Micetro by Men&Mice - 10.6

Men&Mice

Nov 21, 2023

MICETRO BY MENMICE

Welcome to Micetro by Men&Mice, a backend-agnostic DDI orchestration software for complex enterprise network environments.

Deployed in any on-premises, hybrid, or multi-cloud network environment, Micetro acts as a non-disruptive overlay that unifies server management under a single GUI and API. Micetro is a modular, software-defined DDI solution built around a number of components, and accessed through a unified user interface and API.

This documentation is divided into four parts:

1. *Implementation Guide*
2. *Using Micetro*
3. *Admin Guide*
4. *Micetro reference articles*

Use the **Install Guide** to familiarize yourself with Micetro's architecture and installation procedures for components on different platforms. The **User Guide** covers all of Micetro's functionality. The **Admin Guide** is aimed at system administrators managing Micetro.

Tip: Use the search function to quickly locate the information required.

Note: For how-to articles and troubleshooting, see *Micetro reference articles* or visit the Knowledge Base.

Note: If you're using version **9.2 or older** of the Men&Mice Suite, refer to the documentation on https://cdocs.menandmice.com/display/MM/Documentation+Home.

The documentation is open-source, under a modified MIT license (see docs-license), and you're welcome to file issues and improvements on GitHub.

CHAPTER

ONE

TABLE OF CONTENTS

1.1 Release Notes

Note: Major releases are only supported for 2 years.

Jump to: *10.0.8*, *10.1*, *10.1.1*, *10.1.2*, *10.1.4*, *10.1.6*, *10.1.7*, *10.2*, *10.2.1*, *10.2.2*, *10.2.3*, *10.2.4*, *10.2.5*, *10.2.7*, *10.2.8*, *10.3*, *10.3.1*, *10.3.2*, *10.3.3*, *10.3.4*, *10.3.5*, *10.3.6*, *10.3.8*, *10.3.9*, *10.5*, *10.5.1*, *10.5.2*, *10.5.3*, *10.5.4*, *10.6*

1.1.1 10.6

October 19, 2023

New Features

- **BlueCat DNS/DHCP Server Appliance Integration**: You can now seamlessly manage BlueCat DNS/DHCP Server Appliances with Micetro. This combines the signature Micetro intuitiveness and ease-of-use with the robustness and reliability of the BlueCat DNS/DHCP Server appliance for efficient network administration. See *Integrating and Managing Appliances* for details.

Improvements

- **Simplified Zone Creation**: In the Create Zone wizard, if you enter a subnet into **Zone name**, it will automatically be replaced with the corresponding reverse zone, streamlining the zone creation process.
- **Enhanced Session ID Algorithm**: We've updated the algorithm for generating session IDs. It now uses non-deterministic random values that are automatically seeded from the underlying OS, improving security and unpredictability.
- **Improved Screen Reader Support**: We have added a hidden heading to the **Object History** page. This hidden heading provides essential context for screen readers, ensuring a better user experience and improved accessibility for all users.
- **OpenAPI Version Update**: The pi/swagger.json now produces OpenAPI version 3.x for better compatibility and documentation of the APIs.
- **Expanded DNSZoneOptions**: We've introduced enhancements to the DNSZoneOptions functionality. We now publish both the DNSZoneOptions object and its associated child objects, along with providing new APIs for getting and setting DNSZoneOptions.

- **Improved Failover Relationship View**: Our frontend interface now allows you to view existing ISC DHCP failover relationships at the server level. This enhancement provides a clearer and more comprehensive view of your DHCP configurations, making it easier to manage and troubleshoot failover relationships.

Bug Fixes

- **Resolved DNAME Record Creation Issue**: Users can now successfully create DNAME records in the Web Application without encountering any issues.

Note: The Men&Mice Command Line Interface (mmcmd) has been deprecated. We have transitioned away from mmcmd in favor of our powerful and versatile API(s). This change is aimed at providing a more flexible and integrated solution for our users.

1.1.2 10.5.4

September 20, 2023

Improvements

- BIND has been upgraded to v9.16.44 on the Micetro appliance.

1.1.3 10.5.3

September 11, 2023

New Features

- **Default TTL Configuration**: Introducing a new system setting that allows users to customize the default Time To Live (TTL) for records created within zones belonging to xDNS profiles. that are in xDNS profiles. This feature provides enhanced flexibility in managing your DNS records.

Improvements

- Enhanced Central's handling of HTTPS certificates by now supporting multiple Certificate Authority (CA) files. Additionally, you can no longer select the Strict policy without specifying a CA file or directory, reinforcing security practices.
- NS records are now generated correctly when creating AuthServe zones with secondaries, provided that Initial Records are not specified during zone creation. This enhancement streamlines the process of setting up secondary zones.

Bug Fixes

- Fixed an issue that previously prevented users from editing SNMP v2 profiles through the Management Console.
- Fixed a bug where Micetro error messages were not displaying correctly in Windows Event Viewer.
- Fixed a bug that resulted in an error when duplicating a range with certain custom properties.
- Resolved a bug that previously hindered the creation of newly converted DHCP scopes on all relevant DHCP servers.
- Addressed an issue in the Management Console where DHCP scopes on Kea could unintentionally be disabled.
- Resolved an issue where the association between DNS records and IP addresses was not being cleaned up correctly upon zone deletion.
- Fixed a bug where Micetro would not functioning as expected when managing BIND servers with Catalog zones.
- Fixed a bug that previously prevented the successful creation of a DHCP scope on all relevant DHCP servers when converting a range.

1.1.4 10.5.2

July 11, 2023

New Features

- **Duplicate Network**: This feature allows you to easily duplicate networks along with their subranges, DHCP scopes and configurations under a new network address. Please note that this feature is currently not supported for Cisco scopes, Cloud networks, and ranges in a non-CIDR format.

Improvements

- SNMP profiles now support more modern algorithms for authentication and encryption.
- The **Create DNS record** task now automatically defaults to creating PTR records in reverse zones. Record types that are not applicable to reverse DNS are hidden from the list of available record types.
- Users are now able to use passwords with a length between 4 and 100 characters.
- Users can no longer accidentally convert AuthServe primary zones to secondaries when configuring an option template that has a list of primary servers defined.
- Administrators can now specify default TTL values in system settings using BIND shorthand notation
- The ISC configuration file can now be modified through the Web Application.
- When creating ISC Failover scopes, the scope and pool are now created on both servers.
- The **Manage scope instances** task now only allows adding a scope instance to an ISC Failover scope if both servers have the failover peer specified on the scope/pool.
- A new system setting has been added to control whether A/AAAA records at the zone apex are considered apex records for **Edit apex records** access checks on DNS zones.
- The Generic DNS Controller can now be managed through the Web Application.
- We now log a warning only once when the Central host machine does not support certain secure crypto protocols while connecting to AWS Cloud Services.
- The Redundancy tab in the Create zone wizard is now visible by default.

- Users can now define the valid lifetime for Kea DHCPv4 Scopes.
- Users can now edit Kea DHCP Scope Relay IP Addresses directly through Micetro.
- Servers on which users do not have zone creation access are no longer displayed in the Zone Creation Wizard.
- Access for Replicate failover now requires DHCP admin access.

Bug Fixes

- Micetro messages are now logged to files instead of the database to address a performance issue caused by an excessive accumulation of messages. Please note that during the upgrade, all messages in the database will be deleted.
- Broken documentation link to Failover management has been fixed.
- Broken documentation link to AD Sites and Subnets was fixed.
- Fixed a bug that prevented users with read-only access to Active Directory from creating IP ranges.
- Resolved an issue related to configuring a fixed Central server in the web service configuration.
- Fixed an issue where DHCP option values in non-standard user class were not automatically replicated to the partner server in MS DHCP failover relationships.
- When attempting to create a zone with an unknown zone type, a more descriptive error message is now returned.
- We now exclude interfaces configuration from replication between ISC Kea peers.
- Fixed a bug that previously prevented updating AuthServe Options Templates in certain situations.
- Resolved an issue where the order of columns on the Service Management page was not being saved.
- Deleting an Authserve zone that no longer exists will no longer return an error.
- Fixed an issue that occurred when sending an empty HTTP body with utf-8 specified as content-type.
- Fixed multiple time zone related issues in the Web Application.
- Fixed an issue where adding a zone to a new folder wasn't possible
- An issue was fixed where connections to MSSQL databases were not cached on Central running on Linux.
- An issue was fixed where the Micetro Central service installer would not remove all temporary files during installation.
- Various accessibility fixes have been implemented in the system settings.
- Links to actions that are only applicable to primary zones have been updated accordingly.

1.1.5 10.5.1

June 28, 2023

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2023-2828, CVE-2023-2829, CVE-2023-2911.

1.1.6 10.5

April 18, 2023

New Features

- **Micetro Update Management**: Micetro can now be updated to a more recent version directly in the Web Application. In a new and intuitive interface administrators will be notified when new product updates are available. There they can easily review the updates, view the current status of all Micetro components, retry failed updates, and troubleshoot any update.
- **Service Management**: Server Management has been renamed to Service Management and significant improvements have been made to enhance user experience. In addition, we've streamlined the process of adding DNS, DHCP, and IPAM services with a single button that allows you to easily filter by provider or service name.
- **Akamai AuthServe Integration**: Support for Akamai's AuthServe DNS server has been added. Options Templates and the following record types are supported for the server: HTTPS, SVCB, CDS, CDNSKEY, and CSYNC.
- **Support for Kea Client Classes**: We have added support for Client Classifications on Kea DHCP servers (both v4 and v6).
- **Global Object History**: In the Web Application you can now view global object history in one place, which was previously limitied to specific objects only. We have also made some minor improvements to the data available. This helps you to quickly and easily trace system activities in the event of an incident or problem. Additionally, all users can view their own object change history.
- **Event Hooks**: Scheduled Scripts are now called Scheduled Events, while External Scripts has been renamed to Change Events. You can manage these events, along with Subnet Monitoring Events on the Admin page of the Web Application.
- **System Settings**: Administrators can now manage the System Settings for Micetro in the Web Application.
- **Move Objects Between Address Spaces**: In the Web Application, servers and ranges can now be moved between address spaces in Micetro.
- **DHCP Management**: We have added the following DHCP management features to the Web Application:
  - Microsoft DHCP server-to-server failover relationships management.
  - Definition of custom DHCP IPv4 and IPv6 options for individual Microsoft, Kea, and ISC services.
  - Management of DHCP server properties.
- **Zone Creation Workflow**: We have introduced a new intuitive wizard for creating zones. Among other improvements, custom properties can be added to all zone types and zones can be added to folders during the creation process.
- **Primary and Secondary Zones**: Master/Slave terminology has been replaced with Primary/Secondary in the Web Application.

Improvements

- The old web interface is no longer packaged with Micetro.
- OS version display for different DNS and DHCP providers is now more consistent.
- The logging functionality was upgraded to exclude sensitive information when modifying AD Forests, Users, and Cloud Services.
- Better handling of Microsoft DHCP JET Database errors when working with reservations on failover scopes.
- Ordering of grid columns in the IPAM view has been improved so that Discovery properties, when set to be shown, are displayed after custom properties.
- BIND 9.18 is now supported by Micetro.
- Micetro is verified to run on Red Hat Enterprise Linux 9.
- The DHCP remote now supports HTTPS connections to the ISC Kea Control Agent.

Note: This feature was added in Kea 2.0. We officially support version 1.8.

- DHCPv6 Scopes are now displayed in the Management Console.
- Type is now required when importing reservations to a Microsoft DHCP scope.
- Discovery schedule can be configured for multiple ranges at a time.
- When allocating subranges, users can select between 16 options instead of 8 in the Web Application.
- The build date of the Web Application can now be seen when hovering over the version number on the login page.
- xDNS profile grid has been updated to look more like other grids in the system. xDNS Profiles can now be opened by double clicking the relevant row.
- ISC-built packages of BIND are now supported by the Micetro installer.
- We have added a new API command for retrieving multiple free IP addresses located inside a given IP range.
- Various UI/UX and accessibility improvements.

Bug Fixes

- Performance has been improved when opening scopes on Kea.
- Fixed an issue where it was not possible to add change requests for ranges with invalid set of custom properties.
- Fixed a bug where license keys with expiry date were reported as inactive.
- Fixed an issue where promoting a zone would use data from a different primary zone with the same name.
- An issue was fixed where access was not retained when a zone was migrated.
- An issue with setting custom properties with the AddDNSRecords API command was fixed.
- Fixed an issue where submit buttons for change requests in Workflow would render off screen on certain screen resolutions.
- An issue was fixed where it was not possible to add an IPv6 address of a primary server to a secondary zone.
- An issue was fixed where scope name was not updated to reflect the name of the network.

- An issue was fixed where it was possible to get information about a network through an error message, even though the user does not have access to the network.

1.1.7 10.3.9

September 20, 2023

Improvements

- BIND has been upgraded to v9.16.44 on the Micetro appliance.

Bug Fixes

- Fixed an issue where AWS debug log messages were excessively logged to the Micetro log.

1.1.8 10.3.8

June 28, 2023

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2023-2828, CVE-2023-2829, CVE-2023-2911.

1.1.9 10.3.6

January 16, 2023

Improvements

- Improved Azure VPC/subnet synchronization to sync changes to VPC/subnet address space into Micetro
- Accessibility improvements in the UI
- Various UX improvements

Bug Fixes

- Disabling scopes on KEA is no longer possible and has been disabled in the UI
- Fixed issue where it was not possible to add change requests for ranges with invalid set of custom properties
- Fixed a bug where CNAME and TXT records would sometimes be removed when they shouldn't while clearing IP addresses.

1.1.10 10.3.5

October 14, 2022

Improvements

- DHCPv6 scopes are now displayed in the Management Console (Thick Client)

Bug Fixes

- Fixed an issue where removing IP addresses would sometimes result in database errors
- Fixed an issue with the Search and Update functionality for IP addresses in the Management Console which sometimes caused database errors
- Removed /64 limitation from the Allocate Subrange wizard. Users can now allocate IPv6 ranges all the way down to /128.
- Various minor improvements and bug fixes

1.1.11 10.3.4

September 21, 2022

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2022-2795, CVE-2022-2881, CVE-2022-2906, CVE-2022-3080, CVE-2022-38177 and CVE-2022-38178

1.1.12 10.3.3

August 30, 2022

Improvements and Bug Fixes

- Kea DHCP Multi-threading is now supported by Micetro when in High Availability
- Fixed an issue where a user with access to edit IP address properties was unable to Claim IPs
- Improved handling of errors during authentication when further user interaction is required to fulfill additional claims from Azure AD
- Fixed errors related to IIS configuration corrupting location headers

---

Note: The Ansible plug-in for Micetro has been updated and is being maintained here in Galaxy (https://galaxy.ansible.com/ansilabnl/micetro) and in Github (https://github.com/ansilabnl/micetro)

1.1.13 10.3.2

August 18, 2022

Improvements and Bug Fixes

- Improved logging for external authentication
- Improved security of external authentication requests (PKCE and nonce)
- Limited the default requested permission to only current user for authentication with Azure AD
- Improved performance when adding DNS records
- Updated xDNS profile grid to look more like other grids in the system
- Improve UX of create network wizard when no existing folders
- A bug was fixed where importing DHCP reservation on Kea gave an error
- Fixed an issue where some auto suggestion fields would auto select the first suggestion
- Fixed issue where an xDNS zone would not be visible in the Management Console if another zone with the same name in a different view was also added to xDNS
- Fixed a problem with BIND possibly getting stuck when doing a logrotate if the appliance was configured to send the system log messages to a remote server
- Fixed an issue where a view with the name "default" would not behave correctly in the UI
- Fixed an issue where submit buttons for change requests in Workflow would render off screen on certain screen resolutions
- Fixed issue where editing properties of an externally authenticated user would prevent him from logging in
- Fixed an issue where some users were unable to switch between Address Spaces
- Fixed issue where navigating web UI with the keyboard would sometimes clear unrelated fields
- Fixed UI glitch where name of xDNS profile for a zone would sometimes not show up in the sidebar
- Fixed an issue where the Inspector no longer showed complete list of master/slave servers in sidebar for cloud zones
- A bug was fixed where the values were not showing up correctly for the filtering criteria when editing access reports

1.1.14 10.3.1

July 13, 2022

Improvements and Bug Fixes

- An issue was fixed where the schedule date for a scheduled change request wasn't being saved
- Fixed an issue where the quickfilter showed the value [object Object] when searching for a partial string of the word "object"
- An issue with running the DNS Server Agent (Controller) installer for Bind in chroot on some Linux distributions was fixed
- Improved dropdown menus so they may be viewed in smaller window size
- Improved handling of MS DHCP JET Database errors when working with reservations on failover scopes
- Micetro now uses the correct region endpoints when communicating with AWS in setups where the AWS region provider chain is returning the non default region
- Fixed a performance regression when listing and filtering Networks in the Web application
- Fixed a performance regression when viewing object history in large Micetro databases
- Fixed a bug where a white screen error appeared if an IP address was selected on a disabled server
- AD sites can now be sorted alphabetically in the AD sites grid
- Logging was improved and now excludes sensitive information when editing AD Forests, Users and Cloud Services
- Fixed issue where the "Reveal" action had sometimes to be executed twice to select a revealed IP address
- Various improvements and bug fixes

1.1.15 10.3

June 14, 2022

New Features

- Multi-factor Authentication: MFA has been added to Micetro. Supported platforms are Okta and AzureAD.
- Multi-vendor DNS Redundancy: xDNS has been improved and simplified with the introduction of xDNS profiles. Profiles group together two or more DNS services which are designated to share the authority of a list of zones. Changes within Micetro are replicated automatically to all services in the profile.

Note: xDNS functionality has been removed from the Management Console (thick client). xDNS functionality is now only available in the web UI. The API functionality has changed as well. Please check your API calls before upgrading to ensure consistent functionality.

- Custom Properties Select List Enhancement: Manage cascading list options with ease. Configure options for a hierarchy of lists, with a single colon separated raw text list, or navigate and manage the options in a tree view editor.
- KEA DHCPv6 Support: Micetro support added for managing Kea DHCPv6 servers

---

Note: "KEA DHCPv4" has now been changed to "Kea" in the Micetro server enumeration types, and this will need to be changed in all calls to the API

- DHCP administrators can view the lease history for an IPv4 address in the web UI.

Improvements

- IPv6 addresses are now written using shorthand notation from the API
- Improved the error message when DNS/DHCP server controllers are outdated and incompatible with Micetro Central
- BIND has been upgraded to v9.16 on the Micetro appliance
- Role management: Groups are now listed in a single column to prevent problems with displaying very long group names
- UI/UX improvements - Better keyboard event handling
- Micetro now detects, and reports, if Microsoft Server 2022 is the installed operating system
- Access Management: When managing access for multiple networks user can inherit parent access
- Range was renamed to Network in texts where it applied to both ranges and scopes to avoid confusion
- Filter now recognizes potential IPv6 and colon separated Mac Addresses
- Built-in groups are read-only, when managing users in Micetro users cannot be added or removed from built-in groups
- Better visual indication that a High-availability state switch has started and completed
- All Micetro references to “Fast DNS” have been changed to “Edge DNS”
- Managing BIND 9.16 is now supported in Micetro
- Lists of objects do not show a folder indicator when all items in the list are in the same folder
- Admin user can change custom property type when editing custom properties (except for Yes/No properties)
- When installing Linux Bind Controller it is now possible to specify location of named-checkconf
- Improve access to documentation from product empty states
- Access Management enhancement: Users with manage access permissions can view and manage access for multiple objects at the same time
- Added command to reconcile All DHCP scopes on a DHCP server in web UI
- Service options no longer get stale in add zones/scopes forms
- Held IP addresses can be released and claimed
- General UI enhancements

Bug Fixes

- DHCPv4 client identifiers are no longer forced to MAC on Kea services
- Using ISC reservations no longer cause the API command SetIPAMRecord to fail
- Fixed a bug involving the $GENERATE directive in BIND configs
- Fixed a problem when not able to bulk import DNS data when there are required custom fields on record level
- Resolved a problem when RPZ zone records can’t be edited in Web UI
- Adding a DHCP reservation via the REST API now automatically updates both failover scopes

- Improving multi-selection behavior in the web UI
- Changes made to primary servers will now persist as expected
- Improved handling of down Kea servers in the web UI
- Fixed a bug when no initial records shown in grid for new zones on cloud providers
- Error messages no longer appear when leases are removed from split scope
- Fixed a bug involving address pool creation on ISC DHCP servers with no prior pools
- Column width changes are now persistent
- Fixed a bug where under certain conditions Micetro would not communicate correctly to the active Kea server in a HA setup
- Syntax is no longer changed in TTLs of records when using Workflow
- Special characters are now handled in filters
- The authority section of the Inspector is now updated when zones are migrated
- An issue was fixed where the DHCP remote was unable to read reservations with a missing MAC address
- An issue with rearranging columns in the web application was fixed
- Fixed a problem when editing DHCP reservations on a split scope.
- Record custom properties modified with change requests are now properly logged into audit history
- The related DNS data section of the Inspector is now updated when addresses are cleared
- Setting DHCP boot-file-name option is now supported on Kea
- An issue when editing large Kea files was fixed
- Web UI no longer shows error in service configration tab when system does not have an active IPAM license
- SOA records containing number fields/time unit fields with spaces may now be modified
- Users no longer need to refresh page to use a new address space
- New API commands added to create and get reservations from ranges
- Discovery Schedule and Subnet Monitoring settings are now displayed when viewing Scopes/Ranges
- Users may now click Save when converting a lease to a DHCP reservation without editing the Create DHCP Reservation dialog box
- Fixed a bug where in certain conditions Micetro would not communicate correctly with the active Kea server in HA setup
- DHCP agents are now able to read reservations with missing MAC addresses
- An issue with rearranging columns in the web UI was fixed
- Setting DHCP boot-file-name option is now supported on Kea
- An issue with editing large Kea configuration files was fixed.
- New API commands to create and get reservations from ranges
- Various improvements and fixes

1.1.16 10.2.8

September 20, 2023

Improvements

- BIND has been upgraded to v9.16.44 on the Micetro appliance.

Bug Fixes

- Various accessibility improvements were made to the Web Application.

1.1.17 10.2.7

June 28, 2023

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2023-2828, CVE-2023-2829, CVE-2023-2911.

1.1.18 10.2.5

November 29, 2022

Bug Fixes

- Fixed a bug where CNAME and TXT records would sometimes be removed when they shouldn't while clearing IP addresses.
- Fixed an issue where some auto suggestion fields would auto select the first suggestion.
- Fixed a bug where the quickfilter showed the value [object Object] when searching for a partial string of the word "object"
- Fixed a problem with BIND possibly getting stuck when doing a logrotate if the appliance was configured to send the system log messages to a remote server.
- Accessibility improvements in the UI

1.1.19 10.2.4

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2022-2795, CVE-2022-2881, CVE-2022-2906, CVE-2022-3080, CVE-2022-38177 and CVE-2022-38178

1.1.20 10.2.3

July 5, 2022

Improvements

- Micetro now detects, and reports, if Microsoft Server 2022 is the installed operating system.

Note: Microsoft Server 2022 is now supported in versions 10.2.3 and up

Bug Fixes

- Fixed a bug where all DHCPv4 client identifiers were forced to MAC on Kea
- Fixed a bug regarding the $GENERATE directive in BIND configs
- Fixed a performance regression when viewing object history in large Micetro databases
- Fixed disappearing values in scope options while hostnames are being resolved
- Logging was improved to not include sensitive information when editing AD Forests, Users, and Cloud Services
- New API commands to create and get reservations from ranges.
- Various accessibility improvements were made to the Web Application

1.1.21 10.2.2

March 16, 2022.

Bug Fixes

Fixed BIND v9.11 and v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2021-25220 and CVE-2022-0396 from ISC

1.1.22 10.2.1

March 8, 2022.

New Feature

- Users with manage access permissions can view and manage access for multiple objects at the same time.

Improvements

- User can select to inherit parent access when managing access for multiple networks
- Failed login attempts are now throttled to prevent brute force attacks
- Admin users can now change custom property types when editing custom properties (except for Yes/No properties)

Bug Fixes

- Cisco DHCP remote reservation issues fixed when MAC addresses are missing
- Users are able to more easily reorder property columns in the grid of the Web UI
- Editing reservations for split scopes now appropriately modifies the reservation for all servers
- Deleting reservations for split scopes now appropriately deletes reservations for all servers
- Custom properties modified with change requests from DNS Workflow are now properly logged in audit history
- Requiring definition of custom properties which are children of optional properties is no longer possible
- Setting DHCP boot-file-name option is now supported on Kea
- An issue with editing large Kea configuration files is now fixed
- Fixed a problem where users were unable to bulk import DNS data when there are required custom fields on DNS record level
- Resolved a problem where RPZ zone records can't be edited in the web UI
- Web UI no longer shows error in server page when system does not have an active IPAM license
- An issue was fixed where an incorrect error message was displayed when login failed
- Multiple minor improvements and fixes to enhance user experience

1.1.23 10.2

February 3, 2022.

New Features

- DHCPv6 Management: Enjoy the same level of management and visibility for dynamically allocated IPv6 addresses as you have with IPv4 and DHCP in your Windows environments. Toggle DHCPv6 management on or off by server or enable it on multiple servers at once.
- Custom Property Management: Custom Properties can now be managed through the Micetro web interface. Create searchable fields to track information about your DNS zones, DNS records, DHCP scopes, networks, IP ranges and other objects in Micetro. There are two Default Custom Properties built in to the Range object type that come with Micetro which are Title and Description.
- HA Management: Administrators can now manage High Availability for Micetro Central by adding servers, defining priority, and executing failovers via the Web UI.
- Reconcile DHCP Scopes: Manage DHCP scope reconciliation for Microsoft DHCP server from the Micetro Web UI to ensure consistency between the DHCP database and DHCP registry.

Updates

- Microsoft has deprecated support for Windows Server 2008 R2 and therefore Micetro will no longer support this Operating System
- Microsoft has deprecated support for SQL Server 2008 R2 and therefore it will no longer be supported by Micetro
- Micetro will no longer support the 32-bit Linux Operating Systems

Improvements

- Users are now able to create DHCP split scopes in the Web UI for both DHCPv4 and DHCPv6
- When hovering over the folder icon next to a network or DNS zone, the tooltip now shows the full folder path when an object is in a subfolder
- NAPTR records are now supported in AWS Route53
- Colons are now supported when entering hex values in the UI. For example "f1:04:0a:03:e0:0a" is now accepted as an appropriate entry for a field which requires hex.
- Admins may now manually specify a BIND user or BIND group when deploying Micetro to work with BIND
- Folders are now sorted alphabetically in the left sidebar
- The email support address shown under licensing support and error messages is now consistently the same address
- When deleting a folder the folder name is now shown in the popup message confirming deletion
- Improved the order of permissions to be consistent among multiple dialog boxes
- When performing an action on multiple objects, task names are now displayed in plural form
- Read-only Active Directory sites are not shown any longer in the dropdown for setting AD Sites for DHCP scopes or IP ranges
- When there are no DHCP or DNS servers present, the information shown reflects the empty state with helpful information
- For a zone or network that is contained within a folder, users can now click on the folder icon next to that object to view a list of all other objects contained within that folder. Hovering over that folder icon still shows the name of the folder.
- When editing DHCP options to enter a subnet mask value, the IP insight information is no longer displayed as it is when entering IP address information
- Users are no longer given the option to manage read-only forests under AD Sites
- Users with correct permissions may now perform a bulk action of unblocking multiple roles at the same time.
- When running reports users may now specify which DNS servers to include in the filter so as to avoid duplicate information within the report from redundant or testing servers for example.
- By default, when there are no additional address spaces to the default address space, permissions will automatically be assigned to the default address space. When there are additional address spaces, then permissions will need to be managed specifically for each address space.
- When editing a user under the Admin>>Configuration tab the user name will now be displayed in the dialog box.
- Users may be authenticated with read-only domain controllers by setting the ReadOnlyDC preference value.
- Reserved and Leased IP address states are now filterable/sortable in the IPAM grid for a network

- The API call GetAvailableAddressBlocks will now claim subnets for a short amount of time so they can't be used by others

Bug Fixes

- Editing a record in an AD integrated zone will no longer create duplicate records by leaving the old record in the zone
- DHCP Option 43 is now stored as Hex value instead of ASCII making it possible to configure option 43 for ISC DHCP users.
- If the BGPD service is enabled on DDI appliances it will now start automatically after a restart of the appliance
- Increased the size of the externalID column in the mm_users db table to fix an issue where users with longer usernames couldn't login
- In the "Delete Zone" dialog box, when master zones are selected, other unrelated zones are no longer selected as well.
- Double clicking on the meatballs menu of a row in the IPAM or DNS grid only opens menu options instead of following the behavior of double clicking on the row itself to open the properties
- Hovering over an action button in the inspector on the right side of the Web UI no longer displays two tooltips.
- Improved error message is now shown when a user tries to rename an SNMP profile with a name that already exists.
- Labels in the Change Request dialog box under Workflow have been enlarged with legible text
- It's now possible to create multi-string TXT records
- Filtering scopes by server no longer shows scopes from unrelated servers
- Next button will now appear so users may move forward when editing reports to adjust the utilization percentage in the Reports Wizard
- The admin page in the Web UI is no longer visible to those without privileges
- Improved indicator display of subranges inside range folders
- Improved error message shown when a user tried to rename an SNMP profile with a name that already exists
- When using a REST call to add a DHCP reservation the reservation will now be added to the active and failover scope in the case that failover has been configured
- Long DHCP reservation names no longer cause errors when sending requests to the servers
- Renaming Azure accounts without re-entering the client secret management account credentials is now allowed
- Multiple minor improvements and fixes to enhance user experience

1.1.24 10.1.7

September 20, 2023

Improvements

- BIND has been upgraded to v9.16.44 on the Micetro appliance

1.1.25 10.1.6

June 28, 2023

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2023-2828, CVE-2023-2829, CVE-2023-2911.

1.1.26 10.1.4

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2022-2795, CVE-2022-2881, CVE-2022-2906, CVE-2022-3080, CVE-2022-38177 and CVE-2022-38178

1.1.27 10.1.2

December 15, 2021.

Improvements

- Messages when no folders are present under DNS or IPAM are now more human readable and informational.
- Links within the Micetro Management Console and Web UI now direct readers to updated documentation.
- Consistent format shown for read-only Active Directory Sites in all dropdown menus.
- Error message that appears when trying to change an SNMP profile name to an existing name has been improved to be more informational.

Bug fixes

- There's no longer a syntax error that pops up when modifying text records that contain data fields over 255 characters.
- Admins will be able to add AD groups in the Web UI when AD Sites and Services feature has been disabled.
- Selecting A or PTR records no longer intermittently causes unnecessary data fetching from server.
- "PTR Status" column will now always show correct status for IP addresses.
- NAPTR records are now correctly formatted before being sent to AWS Route 53.
- Filtering scopes by server no longer shows scopes on unrelated servers with similar names. Your bulk clean-up operations are safe again!
- Accurate informational error message pops up when trying to create a folder that already exists.
- Fixed alignment issue under Access column when creating/editing permissions list for new Roles.

- Correct SNMP profiles will appear when switching between Micetro Central platforms without having to refresh.
- Find Next Free Address command in the web UI glitched at times but is now guaranteed to work correctly.
- Expand/contract function when viewing nested CIDR boundaries, or "Tree View," under the IPAM tab will work as expected.
- Text for task in Groups under Access Control has been changed from "Remove User" to "Remove Group."
- Create Network Wizard is now more intelligent when checking whether a range can be created.
- Fixed rendering issue in filtering sidebar where two items might appear to be selected at the same time.
- Column alignment in Import DNS Records" list has been corrected.
- TXT records that include quotation marks can now be created on Akamai and Dyn DNS.
- Fixed minor issues when adding, removing, and editing Active Directory Forests.
- Extra comma(s) in the IN operator in the API no longer returns "No Results."
- Multiple minor improvements and fixes to make user experience better.
- Improved string validation in a number of API commands.

1.1.28 10.1.1

October 27th, 2021.

- Fixed BIND vulnerability CVE-2021-25219 on the Men&Mice Virtual Appliances. See *Security announcements* for details.
- Fixed an issue with upgrading to Micetro 10.1 with a Microsoft SQL 2008R2 or earlier database.

1.1.29 10.1

October 19th, 2021.

Important: Version 9.2 will no longer receive bug fixes and feature updates. Please update your Micetro to at least version 9.3.

Known issues

New features

- New Access Control management: access controls in Micetro have been redesigned from the ground-up, and provide a fully role-based, flexible management. Existing configurations will be converted into the new model while preserving backward compatibility. Read *Access Management* and *Role-based access example* for details.
- Folder management is now available in the Web Application. Users can organize DNS and IPAM objects using traditional folders and customizable smart folders (saved filters) to quicken their workflows. "Smart people use folders. Even smarter people use smart folders."
- AD Sites and Subnets management has been streamlined and integrated into the IPAM context of the Web Application.

Improvements

- DNS administrators can manage preferred servers for DNS zones in the Web Application.
- SNMP profile management is available in the Web Application.
- A new slide-in help is available for many functions, offering further details on functionality and syntax for their respective operations. Not a water slide in a theme park, but it is still weirdly satisfying.
- Micetro components will no longer display errors if they're reporting different minor versions. We're all one family here.
- Users can import DHCP reservations to Micetro using the Web Application, including bulk import. Get yer CSV goodness on!
- Lease names are searchable in the Quick Command. So you can have a better leash on them. (We'll see ourselves out.)
- Custom links can be added to the Micetro login screen.
- Improved subnet management, including splitting and merging subnets. Alchemy, almost; although no turning iron into gold with Micetro. Yet.

Bug fixes

- Wildcard policies on AWS will display a descriptive error message (as they're not currently supported in Micetro).
- Users can use relative time (i.e. >=-7d) in the Reporting module. Because time is relative, and E equals m times c squared. Except in quantum, but let's not sweat the small stuff.
- BIND installer will no longer get stuck during installation. Sticks and stones may break our bones, but stuck things are just weird.
- DNS and IPAM data is properly updated when changing address spaces. Multiverse mixup, we've had words with the Sorcerer Supreme.
- Using the Quick Filter properly highlights the query in the name column. As this is how it's supposed to work, this fix is a highlight to share.
- Using the 'View scopes' action on a DHCP server will properly show the scopes on the DHCP server. Because it. Has. One. Job.
- Creating a scope on a Cisco DHCP server no longer fails randomly.
- No longer possible for the logged-in user to remove themselves. Word came down that it created a bunch of variants that bottlenecked the TVA, and who needs that?
- Updating refresh times on SOA records will no longer fail with a cryptic error.
- Tooltips no longer appear erroneously on top of the screen after closing their window. They understand now that they have to respect the boundaries of others, just like all polite UI elements do.
- Editing a DHCP pool will no longer result in a locked up dialog window due to illegal from/to address input.
- Converting a network to a DHCP scope will no longer have a missing field. It's returned safe and sound, we can take it off the milk cartons finally.
- Using the 'View history' action will no longer return an error message when a filter is applied.
- The 'Reserve' button will no longer disappear from the Action menu. This type of hide-and-seek is not appropriate in the workplace.
- Streamlined the Men&Mice Central binary to reduce size. Took a lot of pilates, but now it's in much better shape.

- The 'Import records' task is no longer available in Quick Command. We don't know why it was there in the first place. It's not like we put it there. <whistles innocently>
- Login no longer fails if no DNS license key is activated. Some like IPAM with no pulp, and we don't judge.
- Users can use the 'subType' field as a query parameters within data from cloud providers. Suber!
- Adding a cloud provider to Micetro properly runs synchronization for DNS data.
- Men&Mice Web Services will no longer report unhandled exceptions on a Windows Server. While Micetro is exceptional, we're plenty able to handle it.
- The 'Edit reservation' button once again works as expected. Good button, have a cookie.
- Resizing the Inspector panel will no longer cause sections to lock up. No DataTables left behind.
- You can use 'Add to favorites' on IPAM objects as well. We don't like to play favorites, so we're giving favorites to all.
- Removing a cloud account will properly remove all related data from Micetro. Having your ex's stuff around is never a good idea.
- Men&Mice Central will no longer run out of memory when scanning a large number of SNMP profiles. To paraphrase Lady Liberty: give Micetro your huddled SNMP masses yearning to breathe free.
- Pool indicators are refreshed when editing exclusions for a scope.
- Deleting TXT records containing & in the data field no longer fails in AWS. & all rejoiced & the world was at peace again.
- Using the Quick Filter for Networks will no longer cause loading skeletons to appear.
- Exceeding the retry limit in Azure will properly throw an exception.
- Fixed an issue where DNS administrators would not have access to a DNS record's history. Obviously they should. And now they do.
- The 'Edit configuration' task is no longer enabled for unreachable servers.
- The 'Add DNS Zone' task from Quick Command properly fills out the name for the zone. Otherwise it's not magic, now is it?
- Clicking 'Save' on dialogs with no changes made closes the dialog. Clicking save on dialogs that have been modified validates the input. Save the cheerleader, save the world.

Other

- Various performance improvements and UX tweaks. Micetro does things faster and nicer.

1.1.30 10.0.8

Improvements

- Fixed BIND v9.16 vulnerabilities on the Micetro appliance addressed in CVE-2022-2795, CVE-2022-2881, CVE-2022-2906, CVE-2022-3080, CVE-2022-38177 and CVE-2022-38178

1.2 Security announcements

1.2.1 October 27th, 2021

Vulnerabilities were found in the BIND software running on our virtual appliances.

- CVE-2021-25219: malicious actors can exploit a flaw in the response processing of affected authoritative servers that can cause degradation in BIND resolver performance.

We have updated the Men&Mice Virtual Appliances with the appropriate patches, and recommend all customers to update to the latest 10.1.1 version as soon as possible.

The appliances can be easily upgraded using the Automatic Updates feature of Micetro.

For details on how to update Micetro, see *Update Guide*.

For more information regarding the upgrade, contact Men&Mice Customer Care. See *Contacting Support*.

1.3 Contacting Support

Providing the best possible support to our customers is very important to us. Please help us help you by following these guidelines.

1.3.1 Critical Issues

If you have a valid service contract and the issue is considered critical, please contact our Call Center and clearly state that this is a critical issue. Your Service Contract User Guide contains the necessary Call Center contact information.

1.3.2 Clear Description

It is important that you write a clear description of the issue. Please include the current version number of Micetro and related components and provide detailed information based on the following questions.

- What were the circumstances when the issue came up?
- Did an upgrade take place recently?
- Has anything specific to your DNS/DHCP changed recently?
- Do you have any logfiles or screenshots available that might help diagnose the problem?
- In which part of Micetro did the issue come up? E.g. Management Console, DNS/DHCP Controller, Men&Mice Central, Web Application?

1.3.3 Send an email to us

Send an email to support@menandmice.com with the above information. We will get back to you as soon as possible.

1.3.4 Support Contracts

If you have a Support Contract, please refer to the contract for more information.

1.4 Open-source licenses

Name	License
BIND	isc-license
DHCP	isc-license
Unbound	bsd-license
TinyCore	gplv2-license
SQLite	sqlite-license

1.5 Implementation Guide

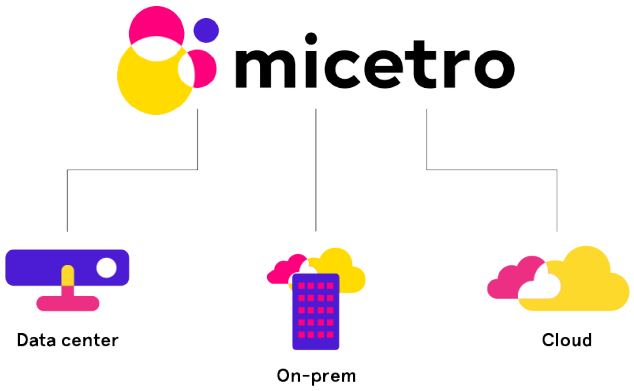
This document is intended to help administrators to install and configure Micetro by Men&Mice. It will help the administrators to identify strategic servers to install the Micetro components on, as they do not have to be installed on all DNS and DHCP servers in the managed environment.

Note: All Micetro components can be installed on virtual machines.

1.5.1 Architecture

Architecture overview

Micetro is a non-destructive, software-defined overlay for managing DNS, DHCP, and IPAM in diverse network environments.



- non-destructive: Micetro does not interfere with network structure or service integrity
- software-defined: Micetro can be deployed using virtual machines (no hardware component is necessary) and is using a single-layer API for orchestration
- overlay: Micetro is capable of managing multiple DNS and DHCP services dynamically, on-premise, in data centers, or in cloud platforms

Components

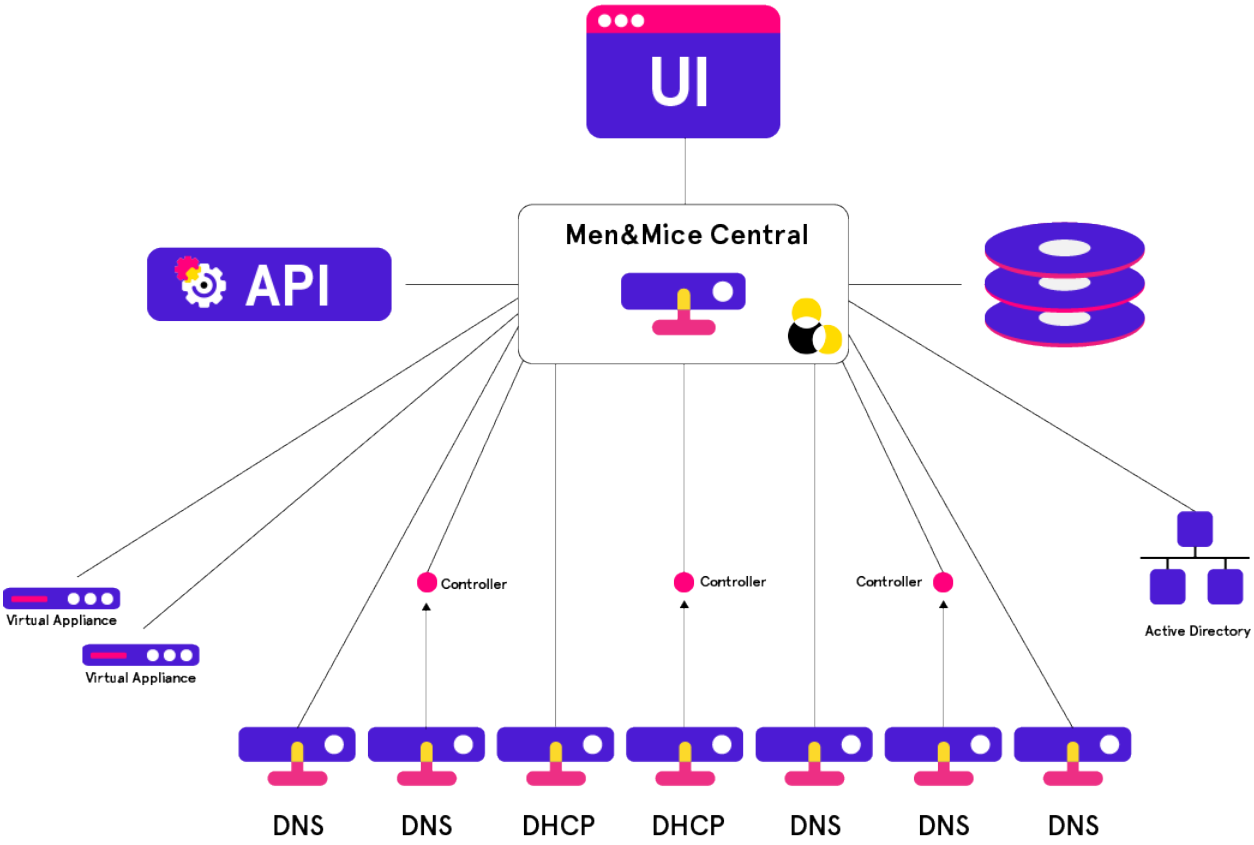
Micetro consists of the following components:

Men&Mice Central
: The server component of Micetro, running the orchestration logic for all configured services. *Can be configured for high availability on certain platforms.*

Data storage
: Accumulating and organizing data from connected services. *Can be configured for high availability on certain platforms.*

Server Controller(s)
: Minimal-footprint service handling communication between Men&Mice Central and the connected services. *Some services can be connected natively to Central and don't need a Server Controller.*

User interface(s)
: Users can manage connected services through a browser-based UI (primary) and a Windows application (transitional, will be deprecated in favor of the web application).



Note: All communications between the Micetro components are encrypted.

Men&Mice Central

Note: At least one copy of Men&Mice Central needs to be installed.

Men&Mice Central, through the connected database, stores all data including user-specific and centrally stored information.

Men&Mice Central handles user authentication and contains information about access privileges for the user. If the Micetro IP Address Management module is activated, Men&Mice Central is responsible for the management and allocation of IP Addresses.

Men&Mice Central listens on TCP port 1231. See *Networking requirements* for more details.

Men&Mice recommends the following table as guidelines for allocating sufficient resources for a smooth operation of Micetro:

Size of environment	Number of objects	Hardware guidelines (per Central instance)
Small to medium	Zones: fewer than 100 IP addresses: fewer than 5000 Subnets: fewer than 1000	Central can be run on a server alongside other services, such as on a DNS/DHCP server or a Domain Controller[1]
Medium to large	Zones: fewer than 1000 IP addresses: fewer than 50000 Subnets: fewer than 10000	4 CPU cores, >= 2 GHz 8 GB of memory 50GB disk space
Large Enterprises and service providers	Zones: Tens of thousands IP addresses: Millions Subnets: Hundreds of thousands	>=8 CPU cores, > 2 GHz >=16 GB of memory 100GB disk space

Additional instances of Micetro's Central can also be installed as a "cold standby". With Micetro's embedded SQLite data storage, the database is periodically copied from the active Central server to the cold standby and, if the active server becomes unavailable, the Central service on the cold standby can be activated. If Central is configured with a different database backend, the database needs it's own high availability setup for redundancy.

See *Configure High Availability for Micetro Central* for running multiple Central instances for high availability.

[1] In smaller installations, Micetro's Central component can be installed on one of the DNS or DHCP servers, as it will not require much resources. More resources are needed as the managed environment gets larger.

Data storage

Note: In case of conflict, the authoritative data is always the data source itself (the DNS or DHCP server).

By default, Men&Mice Central will use an embedded *SQLite* database. The embedded database is suitable for small to medium environments but larger environments should instead use a more robust database backend. Currently supported database platforms are MS SQL and PostgreSQL server.

Information on how to use MS SQL or PostgreSQL as the database for Men&Mice Central can be found in the *Database backend* section.

Note: Deploying Micetro through the Azure Marketplace will use Azure SQL as its database backend automatically. See installation-azure for details.

Server controllers

The Men&Mice Server Controllers are minimal-footprint services running on the DNS/DHCP server or alongside Men&Mice Central and facilitate the communication between the connected service and Central.

DNS Server Controllers

The Men&Mice DNS Server Controller is used to control the DNS server and must be installed on each DNS server machine you want to control. The Men&Mice DNS Server Controller reads and writes zone data and option files, and sends commands to the DNS server. The Men&Mice DNS Server Controller listens on TCP port 1337.

(Unix) BIND DNS environment
: Micetro's DNS Server Controller (i.e., DNS agent) is installed on each DNS server that is to be managed.

(Microsoft) AD environment
: The DNS agent can be installed on some of the DNS servers or they can all be managed agent free. If they are to be managed agent-free, then the DNS Server Controller is typically installed on the machine running Men&Mice Central and when adding the DNS server, the option to add the server as "Microsoft Agent-Free" is chosen. (See *Agent-free management of DNS/DHCP servers*.)

  The DNS Server Controller must be running as a user that has the necessary privileges.

  If the plan is to install the DNS agent on some of the DNS servers in a Microsoft AD environment, and the environment is a pure AD environment (meaning that *all* zones are AD integrated), the DNS agent is typically installed on 2 DNS servers in each AD domain. Micetro will read and write DNS updates to the first server from each AD domain, but if the first server becomes unavailable it will failover to the second server.

  For more information see *Editing Preferred Servers*.

Other environments
: The Men&Mice Server Controller service can also communicate with other DNS platforms, such as PowerDNS. See *Generic DNS Server Controller* for more information.

Note: The Men&Mice DNS Server Controller communicates with the DNS server using RNDC (BIND) or DNSP/RPC (Windows Server 2008 and above).

DHCP Server Controllers

The Men&Mice DHCP Server Controller is used to control the DHCP server.

ISC DHCP
A copy should be installed on each DHCP server machine.

MS DHCP
A copy can be installed on each DHCP server machine, or in certain circumstances it can be installed on another server and connect to the DHCP service over the network. In order for this remote DHCP management to work, the DHCP Server Controller must be installed on a Windows server and must run under an account that has privileges to manage the DHCP service over the network. Operating this way, one DHCP Server Controller can manage several different DHCP servers.

Cisco DHCP
The DHCP Server Controller can be installed on any machine.

The DHCP Server Controller listens for connections from Men&Mice Central on TCP port 4151.

Tip: There are a few strategies to install the Men&Mice DHCP Server Controller (DHCP agent).

- In a Unix ISC DHCP environment, the DHCP agent is installed on all DHCP servers that are to be managed.
- In a Microsoft environment, the administrator can install the DHCP agent on one server, some of the servers, or all the servers. If all the DHCP servers are in the same security realm (maybe in different forests but with trust between them), the DHCP agent can be installed on one server, typically the server running Micetro's Central component.

  Note: If the DHCP agent is to be used to manage DHCP on other DHCP servers, the DHCP agent must be running as a member of the AD DHCP Administrators group.

- If some of the managed DHCP servers are not in the same forest as Micetro's Central component, and there is no trust between the forests, the administrator must install at least one DHCP agent in the foreign forest. That DHCP agent can act as a proxy between Central and the DHCP servers and must be running as a member of the AD DHCP Administrators group in the foreign forest.
- The DHCP agents can be installed on each managed DHCP server. In that scenario, the DHCP agent can be run as the Local System account, which means that no additional configuration is needed after the installation is complete.

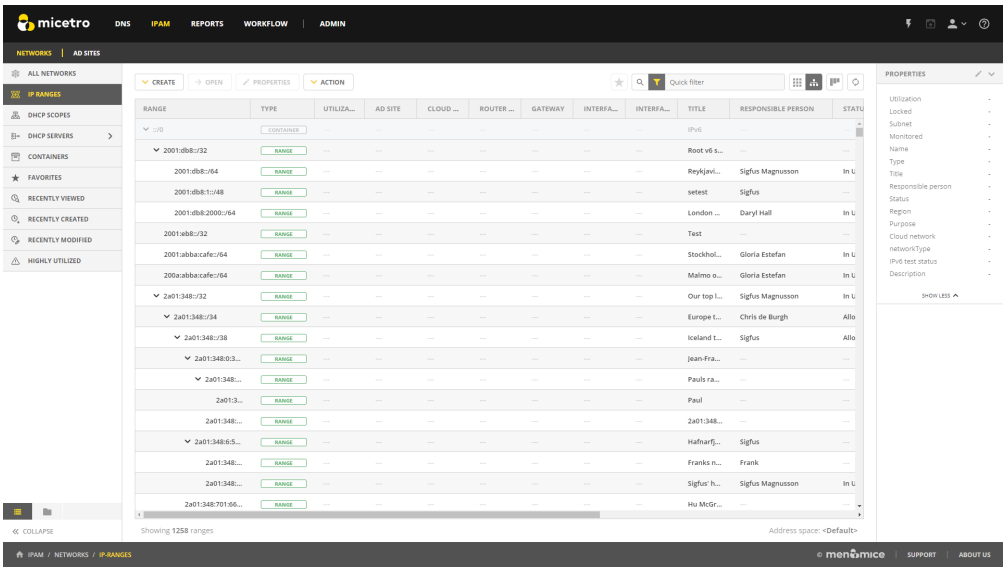
Cisco IOS DHCP servers can be managed using Micetro. A Men&Mice DHCP Server Controller has to be installed on a machine in the environment, which will then act as a proxy to manage the Cisco IOS DHCP servers and will use either plain `telnet` or `ssh` to connect to the managed servers.

User Interface

Note: Of the different user interfaces, multiple copies may be installed, and multiple instances can be logged in at once to manage the environments.

Web Application

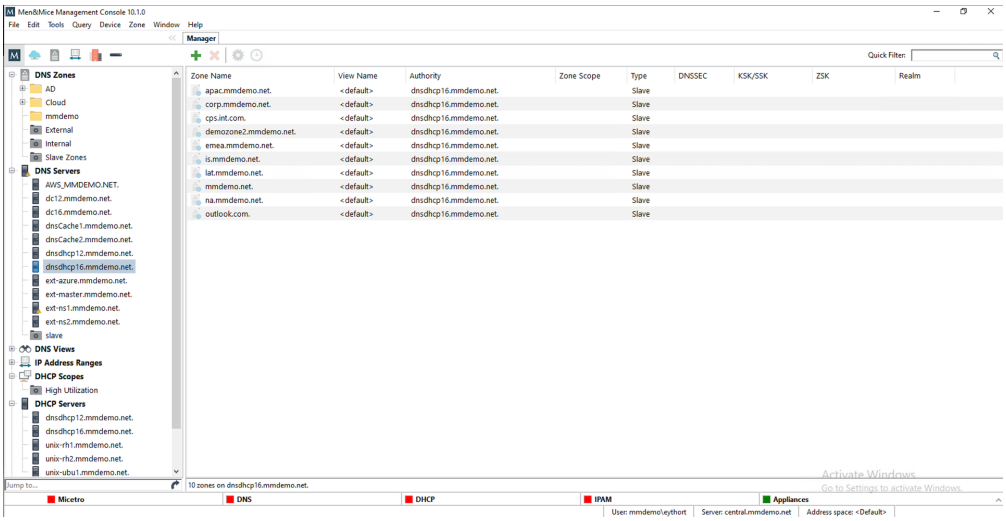
The Men&Mice Web Application can be installed on any server on the network running Microsoft Internet Information Services (IIS) or Apache. The Men&Mice Web Application talks directly to the Web Server (IIS or Apache) which redirects its request to Men&Mice Central through TCP port 1231.



Tip: It is common practice to install the Web Application on the same server that Micetro's Central component is installed on.

Management Console

Micetro's Management Console is a Windows-only rich client that can be installed on as many client computers as required and is typically installed on each administrator's workstation.



Important: The Management Console is being deprecated in favor of the web application. No new features will be added to the Management Console.

Virtual Appliances (Optional)

There are two types of Virtual Appliances: a DNS/DHCP appliance and a DNS Caching Appliance.

The DNS/DHCP Appliance can be used as both a DNS and a DHCP server. Once the DNS/DHCP appliance has been configured, you work with the DNS and DHCP server just as you would work with the BIND and ISC DHCP servers. See *Integrating and Managing Appliances* for more information.

The DNS Caching Appliance contains a high-performance Caching-only DNS server. See *Caching DNS Servers* for more information.

1.5.2 Installation

Networking requirements

Certain ports need to be open for Micetro's different components to communicate with each other.

The following table lists all services and their respective ports to be opened for incoming communications from the source components.

Service name	Port	Protocol	Source(s)
Men&Mice Central	1231	TCP	Management Console, Web Application, SOAP API
Web Application	80/443	TCP	User's browser
PostgreSQL	5432	TCP	Men&Mice Central
PostgreSQL	5000	TCP	PSQL HA nodes
Kea	8000	TCP	Kea Control Agent
DNS Server Controllers	1337	TCP	Men&Mice Central
DHCP Server Controllers	4151	TCP	Men&Mice Central
Men&Mice Updater	4603	TCP	Men&Mice Central

Make sure that the servers running these services have the corresponding ports open in their firewalls.

Micetro by Men&Mice components

Linux

Important: All Micetro non-Windows components (Central, Server Controllers, and the Web Application) require Python (version 3 or above) to be installed on the target server.

Download the following installer packages:

- Men&Mice Central: `micetro-central-10.5.0.linux.x64.tgz`
- Men&Mice Server Controller: `micetro-controllers-10.5.0.linux.x64.tgz`
- Men&Mice Web Application: `micetro-web-10.5.0.linux.x64.tgz`
- Men&Mice AuthServe Agent: `mm-authserve-agent.tar.gz`

Note: Unless noted, all commands are run as *root*.

Windows

Download the following installer packages:

- Men&Mice Central: `Micetro_Central_x64_10.5.0.exe`
- Men&Mice Server Controller: `Micetro_Controllers_x64_10.5.0.exe`
- Men&Mice Web Application: `Micetro_Web_Application_x64_10.5.0.exe`
- Men&Mice Management Console: `Micetro_Management_Console_10.5.0.exe`

Note: Unless noted, all applications are run as *Administrator*.

Location of important config and log files

Important: The paths below represent the default values. Depending on your installation, your environment may be using different paths. See central-non-standard-install.

Linux

Path	Information
`/var/mmsuite/mmcentral/preferences.cfg`	Men&Mice Central configuration file.
`/var/mmsuite/dns_server_controller/preferences.cfg`	Men&Mice DNS Server Controller configuration file.
`/etc/httpd/conf/mmweb.conf`	Men&Mice Web Application configuration file.
`/etc/httpd/conf/mmws.conf`	Men&Mice Web Services proxy configuration file
`./[monitor|nodeX]/postgresql.conf`	PostgreSQL HA cluster database configuration file.
`./[monitor|nodeX]/pg_hba.conf`	Stores client authentication information for the database cluster.
`/var/mmsuite/mmcentral.log`	Men&Mice Central logfile.
`/var/mmsuite/dns_server_controller/logs/`	Men&Mice DNS Server Controller logfile.
`./[monitor]/pg_log/postgresql-[WeekDay].log`	PostgreSQL HA cluster monitor logfile.

Windows

Path	Information
`C:\Program Files\Men and Mice\Central`	Men&Mice Central install directory.
`C:\Program Files\Men and Mice\Console`	Management Console install directory.
`C:\Program Files\Men and Mice\DNS Server Controller`	DNS Server Controller install directory.
`C:\Program Files\Men and Mice\DHCP Server Controller`	DHCP Server Controller install directory.
`C:\Program Files\Men and Mice\Web Services`	Men&Mice Web Application install directory.
`C:\ProgramData\Men and Mice\Central\preferences.cfg`	Men&Mice Central configuration file.
`C:\ProgramData\Men and Mice\Central\mmsuite.db`	Default, built-in database for Micetro.
`C:\ProgramData\Men and Mice\Central\backups\`	Server configuration backups for Men&Mice Central.
`C:\ProgramData\Men and Mice\Central\logs\`	Men&Mice Central logfiles. See central-logging.
`C:\ProgramData\Men and Mice\Central\updates\`	Men&Mice Updater service install directory.
`C:\ProgramData\Men and Mice\DHCP Server Controller\preferences.cfg`	Men&Mice DHCP Server Controller configuration file.
`C:\ProgramData\Men and Mice\DNS Server Controller\preferences.cfg`	Men&Mice DNS Server Controller configuration file.
Logfiles for Server Controllers	Enabled in the controller's `preferences.cfg` file. See *Configuring logging for the Men&Mice Server Controllers*.

Men&Mice Central

Men&Mice Central is the central authentication server. It also serves as the meta-data storage engine, containing data such as zone history logs, user accounts and permissions, etc. You must have at least one copy of Central installed in the environment. Central does not need to be installed on a DNS server.

Important: The installer was designed to be quick and straightforward. Pay attention to the steps, if you'd like to customize your installation. (Such as installing Central to a different path.)

Men&Mice Central on Linux

Note: Before installing Men&Mice Central, decide the following:

- What user account will own the Men&Mice Central process?
- Where do you want everything stored? There are defaults provided.

Extract and run the Men&Mice Central install package:

```
tar -xzvf micetro-central-10.3.5.linux.x64.tgz
cd micetro-central-10.3.5.linux.x64
./install
```

After installation has finished, check for running mmcentral: .. code-block:

```
systemctl status mmcentral
```

Removing Men&Mice Central

Installing Men&Mice Central puts the following files on your system:

Description	File(s) or directory
Men&Mice Central daemon	mmcentrald, usually in /usr/sbin or /usr/local/sbin
Data directory for Men&Mice Central	Usually /var/mmsuite/mmcentral
Update directory	update, located in the data directory
Preferences file	preferences.cfg, located in the data directory
init script, the shell script that can be used to control the service; used by init during system startup	/etc/init.d/mmcentral
settings file used by the init script (Ubuntu Linux only)	/etc/default/mmcentral

To remove Men&Mice Central, first use the init script to stop the service (give it the "stop" argument). Then simply delete the daemon and the init script, and remove any references to the init script in the rest of the boot system if necessary. Also delete the data directory if desired.

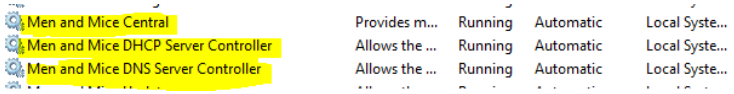
Men&Mice Central configuration files on Linux

See *Linux*.

Men&Mice Central on Windows

Run the downloaded binary and follow the instructions on-screen.

Note: Installing Men&Mice Central does not require special privileges. The service will be started automatically after installation.



Note: Running Men&Mice Central under a privileged user account Running Central as a specific service account affects a few functions when it talks to the Active Directory, such as Integrated Security communications with an SQL server database, communications with AD Sites and Services, authentication of AD users, and ability to ping.

When creating a service account for Central, make sure the user is in the local "administrators" group on the Central machine. Otherwise it will not be able to utilize the ping functionality.

The service account running Central needs to be added to the DNS Admins and/or DHCP Admins group to manage data.

Important: The installer creates the data directories for Men&Mice Central at the default location (C:\Program Files\Men and Mice\Central) even if the installation target is on a different drive or path. See config-files-windows.

Men&Mice Central configuration files on Windows

See *Windows*.

Database backend

Micetro can be used with the following databases:

SQLite

The Men&Mice Central application is shipped with an embedded SQLite database, that will be used if no external database is configured. Customization options for SQLite are not available, Central will use the built-in configuration.

Microsoft SQL Server

Important: We recommend that the network latency between the SQL server and M&M Central is **no more than 5 ms**. Otherwise, the performance of M&M in conjunction with SQL Server can't be guaranteed to be acceptable. We recommend that the SQL Server database is managed and maintained by a database administrator (DBA).

Setting up the Database

Micetro requires that a blank database is created on the database server, with the collation SQL_Latin1_General_CP1_CS_AS, and a login (Windows or SQL server authenticated) that has db_owner access to that database and an effective default schema of mmCentral.

The CreateDatabase.sql script is a suggestion for the database and database server setup. Please note that this script also configures the SQL server itself, which is unnecessary and undesirable in most cases. Therefore, review the script with your database administrator and only run appropriate parts of it.

Before you run the script please go through the script and change the necessary entries accordingly. This includes path strings (default C:/Data) and very important also the password, which is set by default to "1234" in the script!

Warning: The script is preconfigured for an 8 core processor machine, i.e. as a best practice we recommend to create for each processor core one temp file. If you have only a two core machine please comment out the last 6 temp file creation commands in the script.

Danger: The script will, without confirmation, drop the existing database using the name "mmsuite"! Make a manual backup to avoid possible data loss.

Subsequently the script will create:

- a user "mmSuiteDBUser" with the password that you have inserted in the script.
- an empty database with the name "mmsuite" and the following collation: `COLLATE SQL_Latin1_General_CP1_CS_AS`

Note: For further details take a look at the `CreateDatabase.sql` script.

Configuring the connection parameters

Warning: If you're configuring MS SQL on a dedicated server, make sure to enable the TCP/IP protocol with the SQL Configuration Manager.

Warning: An ODBC driver will need to be installed on the Central server to be able to use Microsoft SQL Server.

Men&Mice Central running on Windows

Note: To use Windows Authentication with Micetro and Microsoft SQL Server, make sure Men&Mice Central is running under an Active Directory service account that is a member of the local administrators group.

The `preferences.cfg` file in the data directory contains (beside the fingerprint of Central, i.e. the "password" XML-tag) four additional XML tags: `database`, `databaseserver`, `databaseusername` and `databasepassword`.

The `preferences.cfg` file for normal user/password authentication should look like:

```
<password value="plaintext:PASSWORD"/>
<database value="MSSQL"/>
<databaseserver value="<name or ip of the SQL server>\<name of instance, e.g. SQLEXPRESS>
↪@,<name of database, e.g. micetro"/>
<databaseusername value="mmSuiteDBUser"/>
<databasepassword value="plaintext:DBPASSWORD"/>
```

The `plaintext:` directive in the password inputs allows you to enter the passwords in plaintext, which Central will automatically encrypt and replace with the hash during first startup.

An example `preferences.cfg` file for the Windows Authentication method should look like (`databaseusername` tag must be present and the value attribute must be set to empty string):

```
<password value="the fingerprint hash"/>
<database value="MSSQL"/>
<databaseserver value="<name or ip of the SQL server>\<name of instance, e.g. SQLEXPRESS>
↪@,<name of database, e.g. mmsuite"/>
<databaseusername value=""/>
```

Restart Central and verify it's running. If the database connection fails, the service will fail to start with the appropriate error message.

Men&Mice Central running on Linux

Navigate to the data directory of the Men&Mice Central, usually located in `/var/mmsuite/mmcentral`.

Edit the `preferences.cfg` file with in that directory with the following:

```
<Database value="MSSQL" />
<DatabaseServer value="ip/dns name of SQL server><,port>\<Instance name>@<Database name>
↪" />
<DatabaseUsername value="mmSuiteDBUser" />
<DatabasePassword value="plaintext:<your password here>" />
```

Note: If the `DatabasePassword` value is prefixed by `plaintext:`, it will be replaced by Men&Mice Central for a password hash during start up.

Connecting to the MS SQL database

Restarting the Men&Mice Central service with the new preferences file should connect the Men&Mice Central to your freshly created database. The Men&Mice Central creates the database schema (tables…) during the first connection.

Since the database was freshly created you can now follow the normal installation procedure.

Restart Central and verify it's running:

```
systemctl restart mmcentral
systemctl status mmcentral
```

If the database connection fails, the service will fail to start with the appropriate error message.

PostgreSQL

Men&Mice Central running on Linux

Edit the configuration file for Men&Mice Central:

```
nano /var/mmsuite/mmcentral/preferences.cfg
```

Find (or create) and set the following values:

```
<database value="postgresql"/>
<databaseserver value="HOSTNAME@DATABASE"/>
<databaseusername value="USERNAME" />
<databasepassword value="plaintext:PASSWORD" />
```

Where

- `HOSTNAME` and `DATABASE`: the server's hostname running the PostgreSQL service, and the system user on the server
- `USERNAME`: the user with permissions to read and write the PostgreSQL database
- `PASSWORD`: the database user's password

Note: Once Central starts and reads the configuration file, it'll automatically change the plaintext password to hashed, to increase security.

Restart Central and verify it's running:

```
systemctl restart mmcentral
systemctl status mmcentral
```

If the database connection fails, the service will fail to start with the appropriate error message.

Men&Mice Central running on Windows

The preferences.cfg file in the data directory contains (beside the fingerprint of Central, i.e. the "password" XML-tag) four additional XML tags: database, databaseserver, databaseusername and databasepassword

The preferences.cfg file for normal user/password authentication should look like:

```
<password value="the fingerprint hash"/>
<database value="postgresql"/>
<databaseserver value="<name or ip of the PostgreSQL server>\<name of instance, e.g.␣
↪PSQLDB>@,<name of database, e.g. mmsuite"/>
<databaseusername value="mmSuiteDBUser"/>
<databasepassword value="password hash"/>
```

An example preferences.cfg file for the Windows Authentication method should look like (databaseusername tag must be present and the value attribute must be set to empty string):

```
<password value="the fingerprint hash"/>
<database value="postgresql"/>
<databaseserver value="<name or ip of the PostgreSQL server>\<name of instance, e.g.␣
↪PSQLDB>@,<name of database, e.g. mmsuite"/>
<databaseusername value=""/>
```

Migrating the Micetro database from SQLite to Microsoft SQL Server

Create the database

The knowledge base contains an article that describes the process of creating the database and configuring it: Using Microsoft SQL Server as a database server for the Micetro Suite

The remaining instructions below assume the creation of the Micetro database in MS SQL and that a preferences.cfg file with information on connecting to the MS SQL Server has been created. When Micetro Central connects to the MS SQL server for the first time, it will create the necessary tables.

Preparation

- Create a directory on the Micetro Central server, or if possible, directly on the SQL server (for better performance) and call it "Migrate"
- If SQL Server is not running on the Micetro Central server, download and install the SQL Server Native Client from Microsoft
- Extract the attached ConvertDatabase2.10.zip file and copy the extracted files to the "Migrate" directory. The "Migrate" directory should now contain a PowerShell script used to migrate the database from SQLite to MS SQL as well as two SQLite DLLs (redistributed from system.data.sqlite.org) under the folders x32 and x64
- Stop the Central service on the server
- Copy the mmsuite.db file into the "Migrate" directory. Location of the mmsuite.db file depends on the version of Windows on the Central server (see this Location of Central data directory), but it is typically in either of these locations:

    Windows 2003 - C:Documents and SettingsAll UsersApplication DataMen and MiceCentral

    Windows 2008 and above - C:ProgramDataMen and MiceCentral

Migrate the database to MS SQL

- In the PowerShell window type the following command:

```
> cd C:Migrate > .ConvertDatabase2.ps1 -sourceDbFile .mmsuite.db -database mmsuite -ServerInstance [DATABASE_SERVER] -username [USER NAME]
```

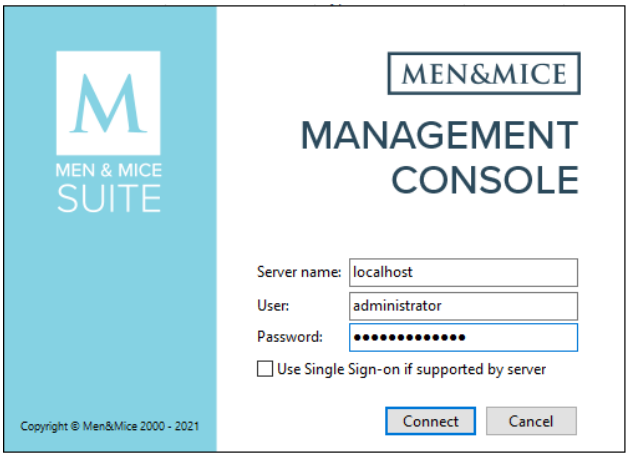
or if your account has access to SQL server, you should use the -useWindowsAuthentication switch:

```
> .ConvertDatabase2.ps1 -sourceDbFile .mmsuite.db -database mmsuite -ServerInstance [DATABASE_SERVER] -useWindowsAuthentication
```

If the script complains about not being able to connect to the database then try adding [Instance_Name] to the -ServerInstance variable like:

```
> .ConvertDatabase2.ps1 -sourceDbFile .mmsuite.db -database mmsuite -ServerInstance 192.168.2.12INSTANCENAME -useWindowsAuthentication
```

```

and/or a custom TCP port to connect to:

```
> .ConvertDatabase2.ps1 -sourceDbFile .mmsuite.db -database mmsuite -ServerInstance 192.168.2.12INSTANCENAME,12345 -useWindowsAuthentication
```

The script may take a few minutes to run, depending on the size of the database.

---

**Note:** If the script returns an error that it can't load the SQLite DLL please check if the DLL is located in the x32 or x64 sub-directory is "Unblocked." Right-click on the DLL and select Properties and press the Unblock button. Please note that Windows might silently refuse the Unblock action. You can check this by re-openeing the Properties and checking to see if it still shows the Unblock buton is blocked. In this case just make a copy of the DLL and delete the original DLL and Unblock the copy.

---

### Start Micetro Central Service

- Ensure the **preferences.cfg** file is using the MS SQL Server
- Go to "Services" and start Central

Central should not connect to the SQL Server and use it as a data store.

---

**Note:** High Availability for the database is only available for MS SQL and PostgreSQL.

---

---

**Note:** Deploying Micetro using the Azure Marketplace configures the environment automatically for Azure SQL. See installation-azure for details.

---

### Installing the Management Console

Men&Mice Management Console is a soon-to-be deprecated, Windows-based user interface of Micetro. As a Windows-based application it needs to be installed on a Windows machine.

---

**Note:** Functionality from the Management Console is in the process of being migrated to the web-application.

---

Run the Men&Mice Management Console installer (with Administrative privileges). Once installed, launch the application:
```



Log in with the default credentials:

- username: `administrator`
- password: `administrator`

The "Server name" field requires the domain or the IPv4/v6 address of the server running the Men&Mice Central application. (This only needs to be defined once, and will autofill on subsequent logins.) Successful login confirms that Men&Mice Central is running, connected to the database, and accessible for the Management Console.

Note: You can disable the "Server name" field: see *Configure the web application to use a fixed M&M Central server*.

Micetro Agents

Micetro uses agents, also known as server controllers, to handle communication between Micetro and the external service. Depending on the type of service and whether it is located on-premises or cloud, the agent is installed on the respective machine, the machine running Men&Mice central or, in some cases, any machine within the same domain as the DNS/DHCP servers. A single agent can handle communication with multiple servers.

Important: The installer was designed to be quick and straightforward. Pay attention to the steps, if you would like to customize your installation, such as installing Central to a different path.

Micetro DNS Agents

Micetro comes with two types of DNS agents:

- the Men&Mice *DNS Server Controller*
- the Men&Mice *AuthServe Agent*

DNS Server Controller

By default, the installer attempts to automatically detect the installed DNS service (e.g., BIND) and install the appropriate controller. If it can't detect the service, it provides hints and additional information.

Note: If you're running BIND DNS, ensure that the DNS Agents run as the same user as BIND (by default, `named`.)

If BIND is running as a different user, or files are updated, ensure that the `mmremote` service is run as the same user and has sufficient access to files and directories.

For machines with multiple services (for example, ISC DHCP and ISC BIND DNS), explicitly specify the desired controllers during installation.

To view available controller options and parameters, run the installer script with the –help parameter:

```
cd archive-name
./install --help

Men&Mice server controller installer.
--help:  Print help.
--quiet:  Suppress output during install.
--auto:  Automatically determine what controllers to install. Default if no␣
↪other option is given.
--bind-dns-controller:  Install a DNS server controller for BIND.
--unbound-dns-controller:  Install a DNS server controller for Unbound.
--generic-dns-controller:  Install a Generic DNS server controller.
--isc-dhcp-controller:  Install a DHCP server controller for ISC dhcpd.
--kea-dhcp-controller:  Install a DHCP server controller for Kea dhcp4.
--update-controller:  Install update controller. Always installed, if another␣
↪Men&Mice service is installed.
```

Running the Installer

- To install controllers automatically (recommended when you have a single service like BIND or Unbound):

```
./install --auto
```

- For a specific set of controllers, run the installer as follows (example with ISC BIND and Generic DNS controller):

```
./install --generic-dns-controller --bind-dns-controller --isc-dhcp-controller
```

- For quiet/unattended installation with no output:

```
./install --generic-dns-controller --bind-dns-controller --quiet
```

Note: The Men&Mice Update Controller is automatically added when another Men&Mice service is installed.

If you plan to use the Generic DNS Controller, refer to the *Generic DNS Server Controller* for more details.

In case of issues with the new installer, the old Perl-based installer is still available in the same archive as `deprecated_installer.pl`. Run it as follows:

```
cd archive-name
./deprecated_installer
```

The installer will ask a series of questions. Be prepared to answer them, as described for each component.

Micetro Controllers Running on Linux

Preliminary Checks

Before installing the Micetro DNS Controller on a Linux system, ensure that you have thoroughly examined your system's configuration. Pay close attention to the following aspects:

- **Configuration File:** Check if there is a valid starting configuration file, typically located at `/etc/named.conf`. If one doesn't exist, you will need to create it.
- **Content of named.conf:** Verify that your `named.conf` file contains all the necessary statements as detailed below.
- **Ownership of Named Data Directory:** Determine if the named init script changes the ownership of the named data directory. This is crucial, especially for certain Red Hat Linux versions and derivatives that may modify the ownership (check for the `ENABLE_ZONE_WRITE` setting).
- **Chroot Environment:** Check if named runs within a chroot environment. If it does, be aware of specific issues that may arise and consult the knowledge base for solutions. Pay attention to the following:
  - Does the named init script copy anything into the chroot jail when starting the service (relevant for SUSE Linux)?
  - Consider potential problems that might occur when the installer rearranges the data directory listed in `named.conf` (relevant for SUSE Linux).
- **User Account for Named:** Identify the user account that owns the named process. Typically, the Men&Mice DNS Controller should run under the same user account. However, it is occasionally possible to use group membership instead.

Installation Steps

1. Extract the Men&Mice Controller installation package (as root):

   ```
   tar -xzvf mmsuite-controllers-10.0.linux.x64.tgz
   ```

2. In the newly created `mmsuite-controllers-10.0.linux.x64` directory, run the installer script to install the Men&Mice Controller (as root):

   ```
   cd mmsuite-controllers-10.1.linux.x64 && ./install
   ```

Installer Questions

During the installation process, the installer will prompt you with questions related to the Men&Mice DNS Server Controller. Be prepared to answer the following:

- Do you want to install the Men&Mice DNS Server Controller?
- Are you running named in a chroot() environment?
- What is the chroot() directory?
- Where is the BIND configuration file?
- Would you like the DNS Server Controller to run `name-checkconf` to verify changes when editing advanced server and zone options?
- Where is `named-checkconf` located?
- The installer needs to rearrange the files in <`directory`> and restart the name server. A backup will be created. Is this OK?
- Enter the user and group names under which you want to run the Men&Mice DNS Server Controller. This must be the user which is running named.
- Where would you like to install the Men&Mice external static zone handling utilities?
- Where do you want to install the Men&Mice Server Controller binaries?
- BIND needs to be restarted. Would you like to restart it now?

Ensure the `named-checkconf` file is readable:

```
chmod a+s /usr/sbin/named-checkconf
```

Required named.conf Statements

The Men&Mice DNS Server Controller requires specific settings within the `named.conf` file (including any files listed in `include` statements in `named.conf`). Ensure the following statements are present:

- `directory`: The `directory` substatement of the `options` statement must be present and must point to a directory that the installer can replace. It should not refer to `/`, `/etc`, the root of a chroot jail, or any partition mount point. If you need to change or add the `directory` statement, be prepared to move files or update paths used elsewhere in your `named.conf`.
- `key`: For BIND, there must be an explicitly defined key in `named.conf` to enable control of named using `rndc` commands. Copy the contents of the key file, such as `rnds.key`, into `named.conf` if it's not explicitly defined.

  To generate a key, consider using the following command (adjust the path if needed):

  ```
  rndc-confgen > /etc/rndc.conf
  ```

  This creates the `rndc.conf` file, which contains configuration for local use and key and controls statements that can be copied into `named.conf`.
- `controls`: The Men&Mice DNS Server Controller uses a `controls` statement for BIND. There must be a `controls` statement with an `inet` substatement that references an explicitly defined key (as mentioned above). The `inet` statement should allow connections from the loopback address, `127.0.0.1`. If no `controls` statement is defined, the installer will prompt you to create one manually.

Changes in named.conf

Note that the installation of the Micetro DNS Server Controller will rearrange your named configuration data, including rewriting `named.conf` and reorganizing the data directory. The new configuration is functionally equivalent to the old one, except that the logging statement may be added or modified to include new channels.

Common Files

The file layout differs slightly between instances with and without BIND views, but there are some common parts:

Description	File(s) or directory
Men&Mice DNS Server Controller daemon	mmremoted, usually in /usr/sbin or /usr/local/sbin
Men&Mice external static zone handling utilities	mmedit and mmlock, usually in /usr/bin or /usr/local/bin
Data directory for Men&Mice DNS Server Controller	Usually /var/named, /etc/namedb, /var/lib/named, or something within a chroot jail; the same location as before the DNS Server Controller was installed
Backup of original data directory	Same as above, with '.bak' appended to the path
New starting configuration file	Usually either /etc/named.conf or /etc/namedb/named.conf; possibly located within a chroot jail
Backup of original starting configuration file	Same as above, with '.bak' appended to the path
logging statement from named.conf	conf/logging, relative to the data directory
key and acl statements from named.conf	conf/user_before, relative to the data directory
options statement from named.conf	conf/options, relative to the data directory
controls, server, and trusted-keys statements from named.conf; also, if present and if not using views, the root hints zone statement	conf/user_after, relative to the data directory
Preferences file	mmsuite/preferences.cfg, located in the data directory
init script, the shell script that can be used to control the service; used by init during system startup	/etc/init.d/mmremote
settings file used by the init script (Ubuntu Linux only)	/etc/default/mmremote

Without Views

If views are not defined, the following files are created inside the data directory:

Table 1: Without BIND views

Description	File(s) or directory
List of include statements, one for each zone statement file	conf/zones
Directory of zone statement files	conf/zoneopt
A sample zone statement file, for the zone 'localhost'.	conf/zoneopt/localhost.opt
Directory of primary master zone files	hosts/masters
Directory of secondary zone files	hosts/slaves
A sample zone file, for the primary master zone 'localhost.'	hosts/masters/localhost-hosts

With views

If views are defined, the following files are created inside the data directory:

Table 2: With BIND views

Description	File(s) or directory
View statements, not including zone statements within each view	conf/zones
List of include statements for a particular view, one for each zone statement file	conf/zones_viewname
Directory of zone statement files for a particular view	conf/zo_viewname
A sample zone statement file, for the zone 'localhost'. in the view 'internal'	conf/zo_internal/localhost.opt
Directory of primary master zone files for a particular view	hosts/view_viewname/masters
Directory of secondary zone files for a particular view	hosts/view_viewname/slaves
A sample zone file, for the primary master zone 'localhost.' in the view 'internal'	hosts/view_internal/masters/localhost-hosts

Removing the DNS Server Controller and Reverting to Original Data

Stopping the Service

Use the init script to stop the DNS Server Controller service. You can achieve this by providing the *stop* argument to the init script. For example:

```
sudo /etc/init.d/dns-controller stop
```

or

```
sudo systemctl stop dns-controller
```

Replace `/etc/init.d/dns-controller` and `dns-controller` with the appropriate paths and service names for your system.

Removing Controller Files

Once the service is stopped, you can proceed to remove the DNS Server Controller files:

- Delete the daemon binary file associated with the DNS Server Controller.
- Delete the init script used to start the DNS Server Controller service.
- If the init script was registered as part of the boot system, remove any references to it. This may involve using system-specific tools or manually editing boot configuration files.

Reverting to Original Data

If you wish to revert to your original DNS configuration and data, follow these additional steps:

1. Stop the BIND or named service, which might have been managed by the DNS Server Controller, using its respective init script. For example:

```
sudo /etc/init.d/named stop
```

or

```
sudo systemctl stop named
```

2. With the BIND or named service stopped, you can proceed to restore your original DNS configuration and data: * Delete the initial configuration file (`named.conf`) created by the DNS Server Controller. * Delete the data directory created by the DNS Server Controller. * If you created backup files by renaming the originals with a ".bak" extension, restore the original files by removing the ".bak" extension from their names.

These steps will effectively remove the DNS Server Controller and revert your DNS setup to its original state. Be cautious when performing these actions, as they may impact your DNS service.

SELinux

Note: The following commands apply to Linux distributions based on RedHat EL 8 or higher. Your distribution may differ.

After installing the DNS Server Controller, run the following commands as root:

```
semanage fcontext -a -t named_cache_t --ftype f "/var/named(/.*)?"
semanage fcontext -a -t named_cache_t --ftype d "/var/named(/.*)?"
semanage fcontext -a -t named_conf_t --ftype f "/var/named/conf(/.*)?"
semanage fcontext -a -t named_conf_t --ftype d "/var/named/conf(/.*)?"
semanage fcontext -a -t named_zone_t --ftype f "/var/named/hosts(/.*)?"
semanage fcontext -a -t named_zone_t --ftype d "/var/named/hosts(/.*)?"
restorecon -rv /var/named
```

These will adjust the SELinux security label for the BIND 9 configuration and zone files.

Note: Due to the complexity of and variation between SELinux configuration files, we are currently unable to officially support SELinux configuration, as SELinux settings can interfere with the normal operation of named after its configuration has been rewritten by the installer for Men&Mice DNS Server Controller. It is possible to make `named`, Micetro, and SELinux all work together, but we cannot currently offer official support for this.

The $INCLUDE and $GENERATE Directives

Refer to the following articles for information about how these directives are handled in Men&Mice Suite.

- *Men&Mice DNS Server Controller and $INCLUDE Directives*
- *Expanding $GENERATE directives into records*

Installation with Dynamic Zones

Men&Mice Suite expects dynamic zones to be made dynamic by allowing signed updates. Any dynamic zone must have an allow-update statement whose ACL contains a key. If you do not otherwise have a need for signed updates, add the rndc key (or any other key) to the list.

Furthermore, after installation, be sure that your server allows zone transfers of dynamic zones to the loopback address, 127.0.0.1, or users will be unable to open dynamic zones from this server. Zone transfer restrictions can be set or changed in the server's and in each zone's **Options** window in the Men&Mice Management Console.

Verify the DNS Server Controller is running

Verify the Controller application is running:

```
systemctl status mmremote
```

Micetrol Server Controller running on Windows

Active Directory Integrated Zones and Other Dynamic Zones

In order to open a dynamic zone, Micetro must read it from the DNS service rather than from a file. The way this is done is via *zone transfer*. On Windows Server 2003 and later, the zone transfer restriction setting in the zone's options window must be set to allow transfers to an explicit list of IP addresses that includes the server's own address. The default setting of allowing zone transfers to any server listed in the zone's NS records will not suffice.

In some cases, Micetro DNS Server Controller will also need to be told specifically which interface to use when requesting zone transfers. If you have trouble opening a dynamic zone after setting the zone's transfer restrictions appropriately, check the Event Log / Application Log for messages from Men&Mice DNS Server Controller. If there is a message indicating that it was unable to get a zone transfer, note the address it tried to use; you can either add that IP address to the transfer restrictions list, or else edit a configuration file for Men&Mice DNS Server Controller.

To configure the DNS Server Controller to use a different address, edit the service's preferences.cfg file on the DNS server computer. The file is located in one of the following two locations, where {Windows} is probably C:\Windows:

- {Windows}\System32\dns\mmsuite\preferences.cfg
- C:\Documents and Settings\All Users\Application Data\Men and Mice\DNS Server Controller\preferences.cfg
- C:\ProgramData\Men and Mice\DNS Server Controller\preferences.cfg

If the file does not exist, create it. The file is a text file in a simple XML-based format. Add the following element, replacing the dummy address here with the server's correct network address:

```
<DNSServerAddress value="192.0.2.1"/>
```

Save the file, and then restart Men&Mice DNS Server Controller using *Administrative Tools → Services* in Windows. Then also restart Men&Mice Central, so that it can cache the zone's contents.

Note: For Active Directory-integrated zones, other domain controllers running Microsoft DNS do not need to get zone transfers. This is because the zone data is replicated through LDAP, rather than through zone transfers. Thus, for an AD-integrated zone, the zone transfer restriction list might need only the server's own address.

Running Micetro DNS Server Controller under a privileged user account / Server type: "Microsoft Server Controller-Free"

Normally, the Men&Mice DNS Server Controller is installed on only *one* host in an Active Directory forest, or one copy per site. That installation can then manage all MS DNS servers in the forest, or in the site, using Microsoft's own DNS management API. In order for this to work, the service needs to run as a user that has DNS management privileges (i.e. the AD service account must be a member of the DNSAdmins group of the domain).

To configure Men&Mice DNS Server Controller to access DNS servers on remote computers, do the following:

1. Start the Windows 'Services' program and open the properties dialog box for Men&Mice DNS Server Controller.
2. Click the *Log On* tab. The *Local System account* radio button is most likely selected.
3. Select the *This account* radio button and enter the name and password of a Windows user that is a member of the Administrators group.
4. Close the dialog box and restart the Men&Mice DNS Server Controller service.

If Men&Mice DNS Server Controller is run as a local system service (the default), it will only be able to manage the MS DNS service on the same host.

Enable the Generic DNS Server Controller functionality

If the Controller should be configured to run a connector script in order to interface with other DNS servers than the natively supported Windows DNS/Unix BIND DNS, the script interpreter and the connector script must be configured in the controllers `preferences.cfg` file.

The file is a text file in a simple XML-based format. Add the following element, replacing the dummy script interpreter and script:

```
<GenericDNSScript value="python /scripts/genericDNS.py" />
```

Configure the DNS Server Controller to work with Microsoft Azure DNS

For information on configuring Microsoft Azure DNS, see configure-azure-dns.

Where to install Men&Mice DNS Server Controller

If Men&Mice Central is installed on a Windows host, one option is to install Men&Mice DNS Server Controller on the same host. If this is not done, the system will need to be told where to find the DNS Server Controller when adding a new DNS server to the system. This will be presented as connecting via proxy.

Note: The Men&Mice communication protocol used to control a DNS server is more efficient than the Microsoft protocol. This means that if a DNS server is separated from Men&Mice Central by a slow network link, it is more efficient to install a copy of the Men&Mice DNS Server Controller in the same local network (the same site, typically) as the DNS server.

AuthServe Agent

Agent Setup

Download

Download the latest package from https://download.menandmice.com/ and extract the installer into `/var/mmsuite`. A different location for the agent can also be chosen if preferred.

```
mkdir -p /var/mmsuite && cd /var/mmsuite

# Assuming the package is in local directory
tar oxzf ./mm-authserve-agent.tar.gz

# Ensure that the user running the service owns the agent files
chown ${SUDO_USER:-$USER}: -R mm-authserve-agent

# Enter the extracted directory and proceed to configure the agent
cd mm-authserve-agent
```

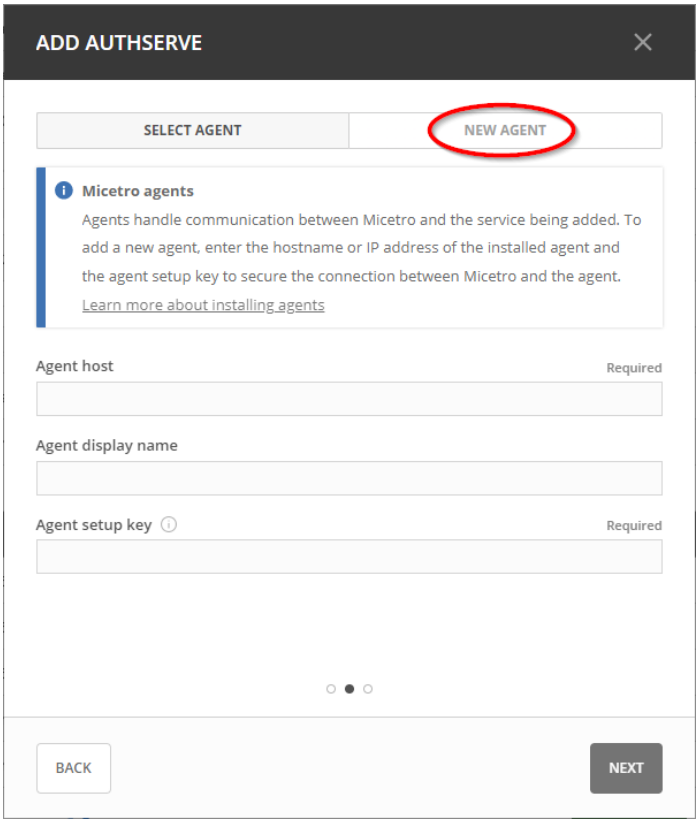
Installing the Agent

1. Install the agent as a service with `sudo ./install`. Note that the install script requires Python. Make sure that the user that runs the install script is the same user that owns the `mm-authserve-agent` folder.
2. Copy the agent setup key that the install script prints out. The Men&Mice AuthServe Agent should now be up and running but you need to connect it to Central to be able to manage it through Micetro.

Note: The Men&Mice AuthServe Agent runs on port 50051 and Central runs on port 1231. Ensure that no firewall settings prevent connection from Central to the agent.

Adding the Agent to Central

1. Select *Admin* on the top navigation bar.
2. Click *Service Management* on the menu bar at the top of the admin workspace.
3. Click *Add Service* above the list of services.
4. On the list of services, select **AuthServe**.
5. Click the *New Agent* tab, and fill in the information.



- **Agent host**: the hostname or IP address of the machine where the agent is located. Note that the Central machine must be able to communicate with the agent machine.
- **Agent display name**: this box is optional and should be filled in if you want your agent to be displayed in the UI under some other name than the hostname/IP address.
- **Agent setup key**: enter the setup key for the agent that you copied earlier from the agent installation script. If you forgot to copy it, you can also find it located in the ssl directory which can be found under the agent directory on the agent machine. The agent also prints it out on startup if it hasn't been added to a Central server yet. The setup key is used to encrypt certificates that Central sends over to the agent. These certificates are then used to allow for a secure encrypted connection to be created between Central and the agent.

Note: If the agent you are adding to Central has been previously added to a Central server, you will have to remove the SSL directory and restart the agent before adding. The restart will generate a new setup key that you should use when adding the agent.

---

6. When you are finished, click *Next*.

7. Enter *Service name* and the Nominum Command Channel used to connect to ANS in the *Channel* box. If you have some custom properties defined for DNS servers in your Micetro setup, you can fill in values for them as well in this panel.
8. Click *Add*. Micetro should now have a secure connection to the Men&Mice AuthServe Agent and you should be able to manage your AuthServe DNS server.

Updating the Agent

Currently, the `mmupdater` service is not capable of updating the AuthServe agent, so the update process must be done manually. To update the agent, an Administrator must unzip the latest agent package and run the `update.sh` script.

Related Topic:

Generic DNS Server Controller

Micetro by Men&Mice manages DNS servers. Native ISC BIND DNS and Windows DNS is supported. As a result of an increase in other DNS servers showing up in production environments, as well as DNS offered as a service by Cloud providers, from Version 6.7 of Micetro, new functions have been added to the DNS Server Controller. This makes the Controller much more flexible and enables Micetro to communicate with such new DNS server types.

How to install and configure the Generic DNS Server Controller:

1. Install:
   - On Windows, run the Controller installer (x32 or x64 - depending on the OS version). There is no special Generic Controller installer - just use the normal Controller installer.
   - On Unix run the Controller installer with the parameter `--generic-dns-controller`.
2. Install a script interpreter. We recommend using Python as we provide example connector scripts for Python (2.7.x).
3. Add the GenericDNSScript XML tag to the preferences.cfg file. If the preferences.cfg file is not present, please create it.

   Note: On Windows 2008/2012 R2 the preferences.cfg file is located under the hidden directory C:ProgramDataMen and MiceDNS Server Controller

   ---

4. Following an example config for the python interpreter and a connector script located on the C drive in the scripts sub-directory:

```
<GenericDNSScript value="c:\python27\python.exe c:\scripts\genericDNS.py" />
```

The genericDNS.py script implements the generic API and interfaces with the DNS server itself.

5. Log in to the M&M Management Console and add the new generic DNS server. Select as Server Type "*Generic*". The name and optional IP address must point to the machine that runs the Generic DNS Server Controller.

Limitations

Reading, modifying zone/server options, reading logs, clearing cache, controlling the server itself is not possible by the API yet. Depending on the connector script, only primary zones are currently supported. That means no secondary zones or special zones like forward or stub zones are supported for Amazon Route53, but secondary zones are supported for *Configuring PowerDNS*.

Of course, the connector script could interface with a secondary zone and return an error when Central tries to update the zone. However, the zone will show up as zone of the type "Primary" in the M&M Suite. In other words, everything else than reading/writing/updating primary zones and their zone data is currently not supported.

Available Connector Scripts

Amazon Route53: see *Configuring Amazon Route53*.

PowerDNS with MySQL database backend: see *Configuring PowerDNS*.

Men&Mice DHCP Agents

Note: For a list of compatible DHCP servers, see *Adding DHCP Service*.

Men&Mice DHCP Agent is the DHCP server agent. It sits on each DHCP server machine (or in case of environments using MS DHCP or ISC Kea servers, on any machine in the network) and manages the DHCP service on your behalf.

Installing Men&Mice DHCP Agent is typically quite straightforward, with far fewer considerations than Men&Mice DNS Agent.

By default, when executed the agent installer tries to figure out the installed service (e.g. BIND) automatically and will try to install it without further user input.

In case it can't install the service it will print out hints and further information.

If the machine has multiple services installed, like ISC DHCP and ISC BIND DNS you want to specify explicitly the Men&Mice Agents that should be installed.

To get the list of available agents/parameters just run the installer script with the `--help` parameter:

```
cd archive-name
./install --help
Men&Mice server controller installer.
--help:  Print help.
--quiet:  Suppress output during install.
--auto:  Automatically determine what controllers to install. Default if no␣
↪other option is given.
--bind-dns-controller:  Install a DNS server controller for BIND.
--unbound-dns-controller:  Install a DNS server controller for Unbound.
--generic-dns-controller:  Install a Generic DNS server controller.
--isc-dhcp-controller:  Install a DHCP server controller for ISC dhcpd.
--kea-dhcp-controller:  Install a DHCP server controller for Kea dhcp4.
--update-controller:  Install update controller. Always installed, if another␣
↪Men&Mice service is installed.
```

Multiple agents can be specified. If you have for instance both ISC Kea and ISC DHCP runnning on the machine just run the installer as follows:

```
./install --kea-dhcp-controller --isc-dhcp-controller
```

Note: If you have only a single service like BIND or Unbound installed we recommend to run the installer without parameter. It will then use the –auto parameter and figure out the service automatically.

Quiet/unattended installation is possible with the `--quiet` parameter (no output at all):

```
./install --isc-dhcp-controller --quiet
```

Note: The Men&Mice Update Controller always gets automatically added to the list when another M&M service is installed, e.g. in the above listed example the –update-controller gets added automatically.

If you run into issues with the new installer, the old interactive Perl based installer is still present in the same archive as:

```
deprecated_installer.pl
```

To execute the deprecated installer for the Men&Mice Agents please run it as follows:

```
cd archive-name
./deprecated_installer
```

The installer will ask a series of questions. Be prepared to answer them, as indicated below for each component.

Note: The Kea DHCP4 Controller can not be installed by the deprecated installer.

Men&Mice Central running on Linux

Here are the questions asked by the installer that pertain to Men&Mice DHCP Agent:

- Do you want to install the Men&Mice DHCP Agent?
- Where is the DHCP server configuration file?
- Where is the DHCP server lease file?
- Where do you want the Men&Mice DHCP Agent to keep its configuration files?
- Enter the user and group names under which you want to run the Men&Mice DHCP Agent. This must be the user which is running dhcpd.
- Where do you want to install the Men&Mice Agent binaries?

Managing Cisco IOS with DHCP support

Men&Mice DHCP Agent can also manage Cisco IOS servers with DHCP support. There is no need to install any software on the Cisco device, but it is necessary to create a user account on the device that has the ability to telnet or SSH in. You will be asked for the username and password when adding the server.

When adding a Cisco IOS server to Men&Mice Suite, the options are very similar to those shown when adding an MS DHCP server; by default, if possible, Men&Mice Central will look for a copy of the DHCP Agent on the same server as itself, but you can also specify a particular installation to use as a proxy. It is recommended to use a copy of the DHCP Agent that is on the same network segment as the Cisco IOS server.

Extract the Men&Mice Agent install package (as root):

```
tar -xzvf mmsuite-controllers-10.0.linux.x64.tgz
```

In the newly created `mmsuite-controllers-10.0.linux.x64` directory run the installer script to install the Men&Mice Controller (as root):

```
cd mmsuite-controllers-10.1.linux.x64 && ./install
```

Ensure the `named-checkconf` file is readable:

```
chmod a+s /usr/sbin/named-checkconf
```

Verify the Controller application is running:

```
systemctl status mmremote
```

Men&Mice Central running on Windows

Running Men&Mice DHCP Agent under a privileged user account / Server type: Microsoft Agent-Free

Normally, Men&Mice DHCP Agent is installed on one host in an Active Directory forest, or one copy per site. That installation can then manage all MS DHCP servers in the forest, or in the site, using Microsoft's own DHCP management API. In order for this to work, the service needs to run as a user that is a member of the Active Directory DHCP Administrators group.

Please note that for the management of the DHCP failover in Windows Server 2012 R2 the service account must also be a member of the local Administrators group of the DHCP servers in order to be able to fetch/manage the failover configuration.

To configure Men&Mice DHCP Agent to access DHCP servers on remote computers, do the following:

1. Start the Windows "Services" program and open the properties dialog box for Men&Mice DHCP Agent.
2. Click the Log On tab. The Local System account radio button is most likely selected.
3. Click the This account radio button and enter the name and password of a Windows user that is a member of either the Administrators group or the DHCP Administrators group.
4. Close the dialog box and restart the Men&Mice DHCP Agent service.

If Men&Mice DHCP Agent is run as a local system service (the default), then it will only be able to manage the MS DHCP service on the same host.

Where to install Men&Mice DHCP Agent

If Men&Mice Central is installed on a Windows host, then one option is to install Men&Mice DHCP Agent on the same host. If this is not done, then the system will need to be told where to find the DHCP Agent when adding a new DHCP server to the system. This will be presented as connecting via proxy.

However, there are other considerations when deciding where to install Men&Mice DHCP Agent.

- The Micetro communication protocol used to control a DHCP server is more efficient than the Microsoft protocol. This means that if a DHCP server is separated from Men&Mice Central by a slow network link, it is more efficient to install a copy of the Men&Mice DHCP Agent in the same local network (the same site, typically) as the DHCP server.
- Starting in Men&Mice Suite 6.0, Men&Mice DHCP Agent can be used to gather lease history data for a DHCP server. However, this requires that the Men&Mice DHCP Agent be installed on the DHCP server machine itself. If this is done for all DHCP servers, then there is never any need to run the DHCP Agent as a privileged user - the DHCP Agent that is only used to control the DHCP service on the same machine as itself can run as a local system service.

Managing Cisco IOS with DHCP Support

Men&Mice DHCP Agent can also manage Cisco IOS servers with DHCP support. There is no need to install any software on the Cisco device, but it is necessary to create a user account on the device that has the ability to telnet or SSH in. You will be asked for the username and password when adding the server.

When adding a Cisco IOS server to Men&Mice Suite, the options are very similar to those shown when adding an MS DHCP server; by default, if possible, Men&Mice Central will look for a copy of the DHCP Agent on the same server as itself, but you can also specify a particular installation to use as a proxy. It is recommended to use a copy of the DHCP Agent that is on the same network segment as the Cisco IOS server.

Agent-free management of DNS/DHCP servers

Kea

Kea DHCP servers can be configured agent-free, without a DHCP Server Controller running on every Kea machine. The *Kea Control Agent* needs to be installed, and available for communication through its defined port (default: 8000). A single DHCP Server Controller is sufficient to communicate with and handle all Kea servers on the network.

Microsoft

Microsoft DNS and DHCP servers in Active Directory environments can be managed agent free, i.e. without running a Men&Mice server controller locally on the DNS/DHCP server.

While agent free management of DHCP servers is possible with any 6.x version of Micetro, version 6.3 or newer is required for agent free management of DNS servers.

Although it is not required to install an agent on the DNS/DHCP server itself, an agent must be installed somewhere in the same domain as the server resides. This agent will be used as a proxy that will handle all communications to the remote DNS/DHCP server(s). Usually, this proxy agent is installed on the same server as Men&Mice Central, assuming the Men&Mice Central server is a member in the domain. If the DNS/DHCP servers are widely distributed geographically, it can also be of performance benefit to install one agent in each geographic location. For instance, if there are datacenters in Iceland, India, and the United States, it is probably best to install one proxy agent in each datacenter that each handles communications with the DNS/DHCP servers in its datacenter. The proxy agent then in

turn feeds all the information back to Men&Mice Central, eventually reaching the end-user in one of the Micetro user interfaces.

Naturally, the Micetro proxy agent must adhere to the security imposed by the Active Directory. Therefore, the proxy agent service must be running with a service account that has sufficient privileges for DNS and/or DHCP management in the domain. If the privileges are restricted, that will translate to the same restriction in Micetro. For instance, if the service account only has privileges to view DNS zones and records but not do any changes what so ever, the zones and records will show up in Micetro, but all changes to those zones will be denied by Micetro. The same applies to the DHCP server management, if the service account has read-only privileges to the scopes, the scopes will show up in Micetro but the end-user will not be able to do any changes.

Limitations:

DNS:

With agent-free management of MS DNS servers, as opposed to using a locally installed agent, you will lose the following ability in static zones only:

- Disable resource record
- Enable resource record
- View and edit resource record comments
- Disable zone

DHCP:

Collection of lease history is only possible when the agent is installed locally. No lease history will be collected from servers that are managed agent-free.

If `netsh` with full dhcp functionality is not installed properly, no scopes will show up in Micetro regardless of the privileges of the service account running the proxy DHCP agent. The proxy DHCP agent must be installed on a machine that has `netsh` with full dhcp capability. This is always the case if the DHCP role service is installed. If not, it can be installed (on Win2008R2) by *Server Manager → Features → Remote Server Administration → Role Administration Tools – >DHCP Server Tools*.

It's recommended (but not required) that Windows 2003 DHCP servers are managed by proxy DHCP agents installed on Windows 2003 servers, and Windows 2008/R2 DHCP servers are managed by proxy DHCP agents installed on Windows 2008/R2 servers, due to some minor differences in the `netsh` between these two operating systems.

Note: Servers in Active Directory environments can be connected without using an agent. For more information, see *Microsoft* in *Agent-free management of DNS/DHCP servers*.

Cloud integration

Overview

Micetro now can integrate natively with cloud based DNS services as well as manage IP address related data for Azure and AWS, including virtual networks and subnets that exist in cloud accounts.

In previous versions to version 8.2, only Azure DNS was natively supported and Amazon Route 53 was supported through the Men&Mice Generic DNS Controller, but as of 8.2 all cloud services are natively supported and all are easily added to Micetro as cloud instances. In version 8.3 partial support for Akamai Fast DNS was added. In version 9.2 support for managing multiple AWS cloud accounts using the same credentials was added.

Supported Cloud Services

Important: To be able to connect and use cloud services, the DNS Server Controller must be installed on the same machine that is running Men&Mice Central. See *Micetro DNS Agents*.

Cloud service	DNS	IPAM
Akamai	Yes (Akamai Fast DNS)	N/A
Azure	Yes (Azure DNS[1])	Yes
Amazon Web Services (AWS)	Yes (Amazon Route 53)	Yes
OpenStack	No	Yes
NS1	Yes	N/A
Dyn	Yes	N/A

DNS

The use of a cloud DNS service in Micetro is transparent to the user. Adding DNS zones, DNS records, or modifying the two is done in the same way as with other DNS servers in Micetro. Currently only primary zones can be created on cloud DNS services.

IPAM

Configure Cloud Integration

To start using the available cloud services, they need to be added and configured through the Men&Mice Management Console.

For detailed instructions on how to configure Men&Mice Cloud integration, see *Configure Cloud Integration*.

[1] see configure-azure-dns

Using Cloud Integration

Using the available cloud services in Micetro is as easy as using DNS Zones, records, or subnets as before.

For detailed instructions on how to use Men&Mice Cloud integration, see *Using Cloud Integration*.

Configure Cloud Integration

Set up and configuration

Before adding a cloud service instance

Micetro communicates with the cloud services through Men&Mice Central (IPAM) and the Men&Mice DNS controller (DNS).

Before continuing, make sure:

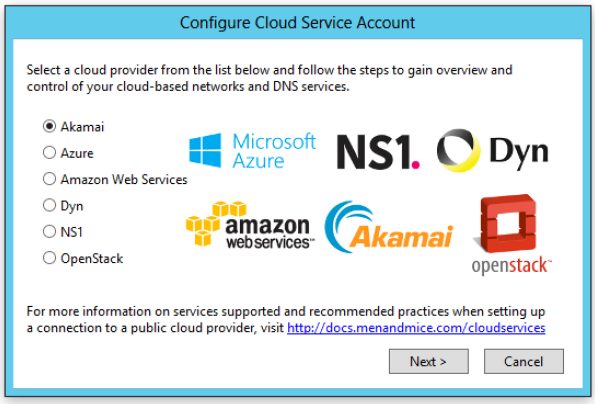
- The DNS controller is installed and set up on the machine running Men&Mice Central. See *Micetro Agents*.
- The machine running central can connect to the specific cloud instance on port 443/TCP. See *Networking requirements*.

If you want to add multiple AWS cloud accounts using single credentials refer to aws-multi-account.

Adding a cloud service

The following are the steps that are needed to start using a cloud service in Micetro.

1. *File* → *New* → *Cloud Service*. Access the Cloud service wizard by right clicking *Cloud Services* in the *Object Browser* of the Management Console and selecting *New Cloud Service* or highlight *Cloud Services* in the *Object Browser* and clicking + sign in the manager window.
2. The following dialog is shown:



Proceed with one of the Cloud providers shown below and click *Next*:

- *Akamai Fast DNS*
- *Azure DNS*
- *Amazon Web Services*
- *Openstack*

- *NS1*
- *Dyn DNS*

Akamai Fast DNS

Fill in the following fields required to connect to Akamai Fast DNS

Name	The name of the cloud service in Micetro
Client Secret	The credentials needed for Micetro to connect to the cloud instance
Host	**Obtaining Access Credentials** Please refer to the following on how to create API Access Credentials for use by Micetro: https://developer.akamai.com/introduction/Prov_Creds.html
Access token	
Client token	

Warning: Server time setting constrictions Akamai OPEN APIs are time sensitive! Ensure that the system your client runs on is synchronized with a Stratum 2 or better time source. (source: https://developer.akamai.com/introduction/Client_Auth.html)

Danger: If the time on the server that the DNS Remote is running on deviates enough from Coordinated Universal Time the authentication will fail and it will not be possible to access/update zone through Micetro.

Go to *Finishing the configuration*.

Azure DNS

Fill in the following fields required to connect to Azure:

Name	The name of the cloud service in Micetro
Subscription ID	The credentials needed for Micetro to connect to the cloud instance
Tenant ID	
Client ID	
Client secret	

Note: See configure-azure-dns.

Go to *Finishing the configuration*.

Amazon Web Services

Fill in the following fields required to connect to AWS:

Name	The name of the cloud service in Micetro
Access Key ID	The credentials needed for Micetro to connect to the cloud instance **Obtaining Access Credentials** Please refer to the following on how to create API Access Credentials for use by Micetro: https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html
Secret Access Key	

Read more: aws-multi-account.

Go to *Finishing the configuration*.

Openstack

Fill in the following fields required to connect to OpenStack:

Name	The name of the cloud service in Micetro
Server Node	The credentials needed for Micetro to connect to the cloud instance
User Name	
Password	
Require HTTPS	

Go to *Finishing the configuration*.

NS1

Fill in the following fields required to connect to NS1:

Name	The name of the cloud service in Micetro
API Key	The credentials needed for Micetro to connect to the cloud instance **Obtaining Access Credentials** Please refer to the following on how to create API Access Credentials for use by Micetro: https://ns1.com/knowledgebase/creating-and-managing-api-keys

Go to *Finishing the configuration*.

Dyn DNS

Fill in the following fields required to connect to Dyn:

Name	The name of the cloud service in Micetro
Customer Name	The credentials needed for Micetro to connect to the cloud instance
User Name	
Password	

Go to *Finishing the configuration*.

Finishing the configuration

After finishing going through the wizard, the DNS service (if applicable) and any subnets defined (if applicable) will be shown in the DNS servers and IP Address Ranges, respectively.

Editing a cloud service instance

To edit the properties for a cloud instance, right click on a cloud instance in the *Object Browser* and select *Properties*.

Removing a cloud service

To remove a cloud service, right click on the specific cloud service in the *Object Browser* and select *Delete*.

> **Warning:** By removing the cloud service, the associated DNS service and the corresponding zones will be removed. Additionally, any subnets and cloud networks will also be removed.

Click *Yes* to remove the cloud service.

Removing a cloud network

To remove a cloud network, right click on the specific cloud network in the object browser or in the manager window and select *Delete*.

Using Cloud Integration

Viewing a cloud service instance

Highlighting a cloud service in the object browser will show the cloud networks residing in that cloud service.

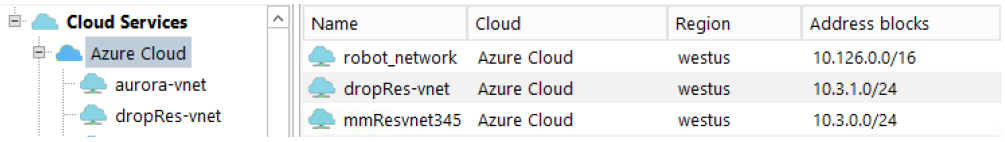
Name
The name of the cloud network

Cloud
The name of the Cloud service

Region
The region where the cloud network is located at.

> **Note:** This field is referred to as Location in Azure.

Address blocks
The address blocks in the specific cloud network.



Using a cloud service

Cloud DNS

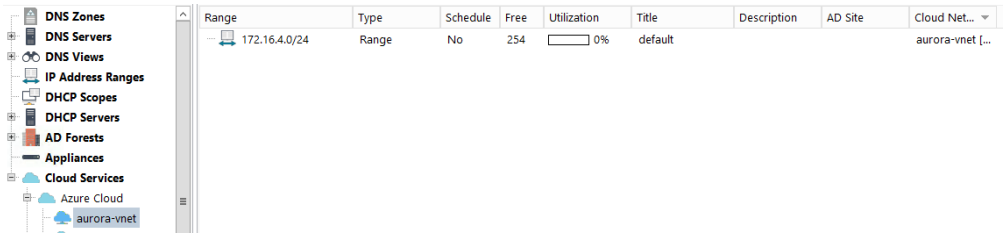
Using and managing a cloud DNS server is very similar as managing and using a local DNS server. Adding zones and records to a zone is transparent for the user.

Cloud IPAM

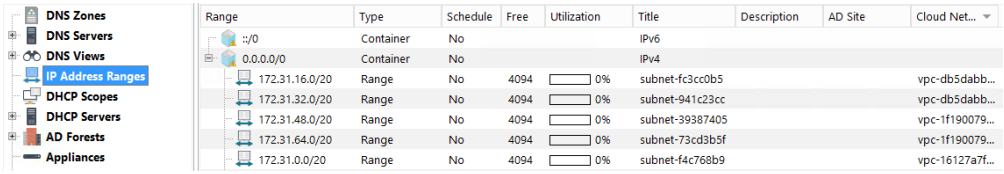
Cloud Networks

The cloud networks can either be viewed in the Object Browser, under the respective cloud service, or in the IP Address Ranges.

In the Object browser, clicking on a specific cloud network will display the subnet residing in that cloud network.



In IP Address ranges, a column named *Cloud Networks* shows the name of the respective cloud network among the other existing subnets.



Custom properties for Cloud services

Custom properties can be specified for cloud services and cloud networks as for other objects.

Web Application

Install the Web Application on Linux

Important: Before you install the the Men&Mice Web Application, make sure you must have a functioning and accessible Apache Web Server running. The Web Application will configure its virtual host.

1. Extract and install the Men&Mice Web Application install package (as root):

```
tar -xzvf micetro-web-application-10.3.5.linux.x64.tgz
cd micetro-web-application-10.3.5.linux.x64 && ./install --web-virtual-host-domain web-
↪application.domain.tld
```

Where `web-application.domain.tld` is the domain on which the Web Application will be accessed.

2. Restart the Apache web server:

```
systemctl restart httpd
```

3. In distributions based on RHEL8 with SELinux enabled, make sure Apache can connect to the web interface service:

```
setsebool httpd_can_network_connect 1 -P
```

Install the Web Application on Windows

Note: On Windows, the Web Application requires IIS to be installed. The installer will check if all required components are available.

Install Men&Mice Web Application by double clicking the Microsoft installer file and follow the instructions there.

> **Warning:** If the web application is not installed on the same server as Men&Mice Central, you need to set the **Web app server host** value to the webserver's hostname through *System settings* → *Advanced* in the Management Console for the auto-update feature to work for the Web Application.

Further configuration

Setup SSL for the Web Application

SSL on Linux (Apache)

By default, the Web Application uses unencrypted http connection on port 80. To use it with https on port 443, follow these steps.

Check that mod_ssl for Apache is installed:

```
yum install mod_ssl
```

If you have existing SSL key files: place the .key file in /etc/pki/tls/private/ and the .crt and .csr files in /etc/pki/tls/certs/.

If you need new SSL keys, generate a keypair:

```
openssl req -new -nodes -keyout mmweb.key -out mmweb.csr -newkey rsa:4096
```

Create self-signed certificate:

```
openssl x509 -req -days 365 -in mmweb.csr -signkey mmweb.key -out externaldns3.crt
```

Place the files in the appropriate directories:

```
cp mmweb.key /etc/pki/tls/private/
cp mmweb.c* /etc/pki/tls/certs/
```

Once the keyfiles are placed in their respective directories, edit the mmweb.conf file in the Apache configuration directory (default /etc/httpd/conf, or use find /etc/ -name "mmweb.conf" to locate the file) with the following changes:

- change <VirtualHost *:80> to <VirtualHost *:443>
- add in the references to the key files (amend the path as necessary):

```
SSLCertificateFile /etc/pki/tls/certs/mmweb.crt
SSLCertificateKeyFile /etc/pki/tls/private/mmweb.key
```

- enable SSL:

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA
```

Note: The default Apache installation may already have a <VirtualHost _default_:443> directive, which can conflict with the `mmweb.conf` file. Comment out this existing VirtualHost block to prevent any errors.

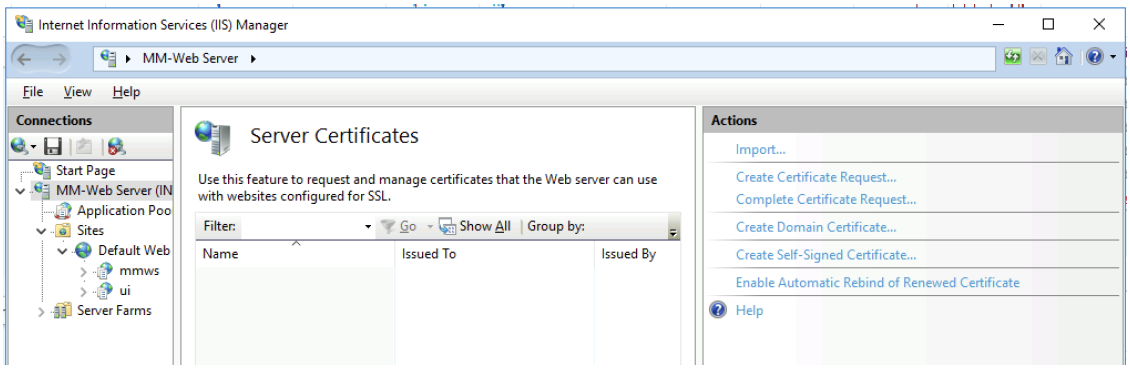
To verify the Web Application is accessible, navigate to `https://web-application.domain.tld`. The Men&Mice Web Application's login panel should appear.

SSL on Windows (IIS)

Configuring SSL Certificate

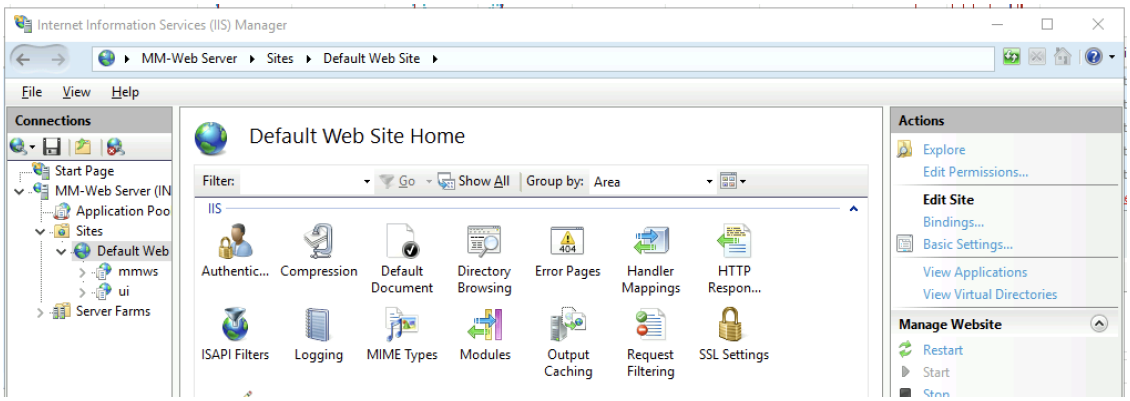
Open the IIS (Internet Information Services) Manager

Select the *Web Server node* in the left sidebar, under "Start Page", and double click on *Server Certificates* in the middle pane

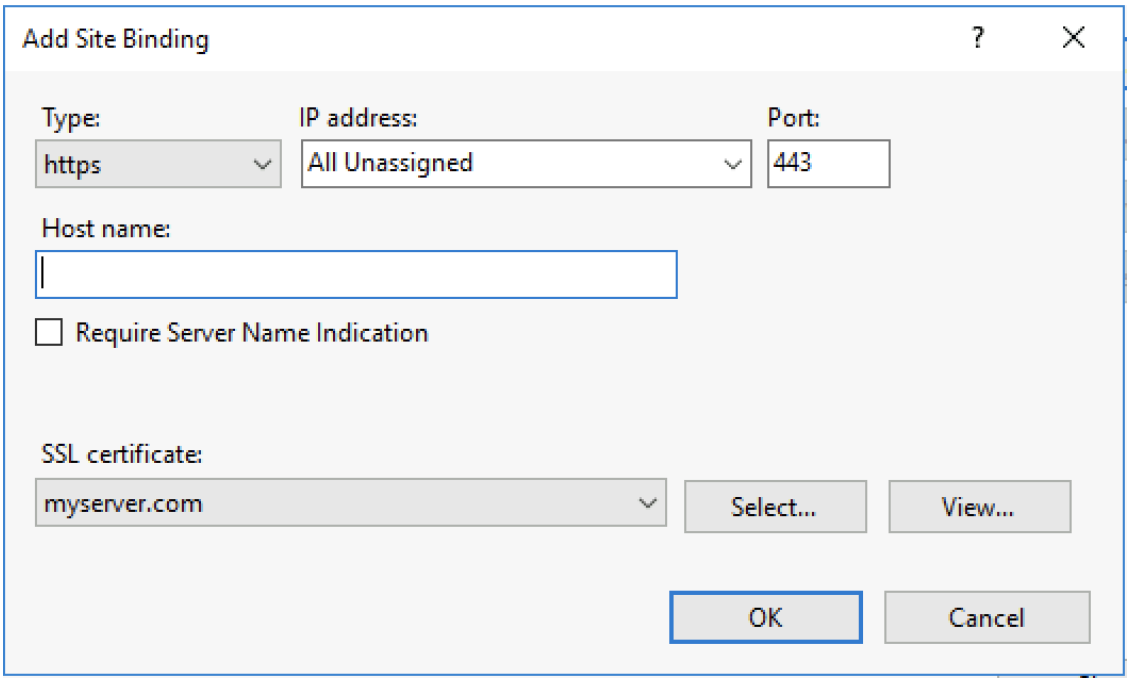


Choose one of the actions in the actions sidebar on the left to import an existing .pfx SSL certificate, or create a self-signed certificate. If your certificate is in a different format than .pfx, please refer to documentation and/or tools that certificate authorities typically provide to convert their certificates to Microsoft's .pfx format

Select your website under *Sites* in the left sidebar (usually Default Web Site) , and click *Bindings...* in the **Actions** sidebar on the right.



In the *Site Bindings* dialog that opened, click *Add*, select **https** from the *Type* menu, and then select the certificate added in step 3 in the SSL certificate picklist. Then click *OK*.



The “Host Name” and “Require Server Name Indication” can be left blank if this the first certificate installed on the server.

Redirect HTTP traffic to HTTPS

Editing web.config

Locate and open the web.config file for your Default Website in notepad. This is typically at C:inetpubwwwrootweb.config

Add the following rule xml to the rewrite > rules section of the xml, at the top below <clear />

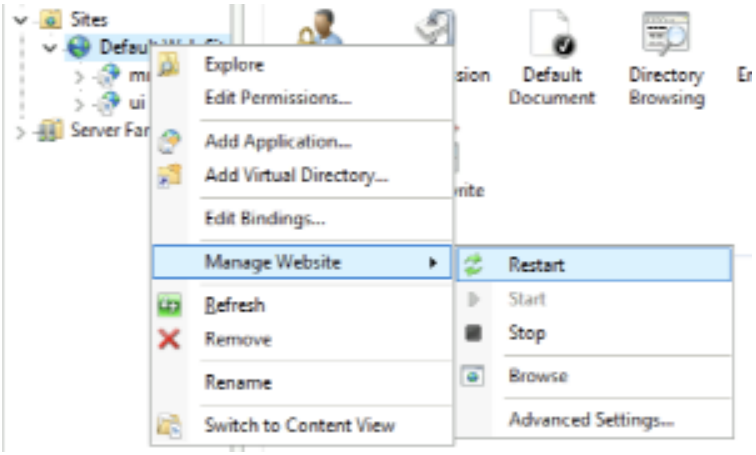
```
<rule name="HTTP to HTTPS redirect" enabled="true" stopProcessing="true">
    <match url="(.*)" />
    <conditions logicalGrouping="MatchAll" trackAllCaptures="false">
```

(continues on next page)

(continued from previous page)

```
        <add input="{HTTPS}" pattern="^OFF$" />
    </conditions>
    <action type="Redirect" url="https://{HTTP_HOST}/{R:1}" appendQueryString="true"␣
↪redirectType="Permanent" />
</rule>
```

In the IIS manager, select the *Default Web site*, right click, and select *Manage Website* → *Restart* to make the changes to the web.config take effect.



With *Default Web Site* selected in the left sidebar, double click on *URL Rewrite* in the middle pane. Verify the rule *HTTP to HTTPS redirect* is at the top of the rewrite rules

Using the IIS manager

With **Default Web Site** selected in the left sidebar, double click on *URL Rewrite* in the middle pane

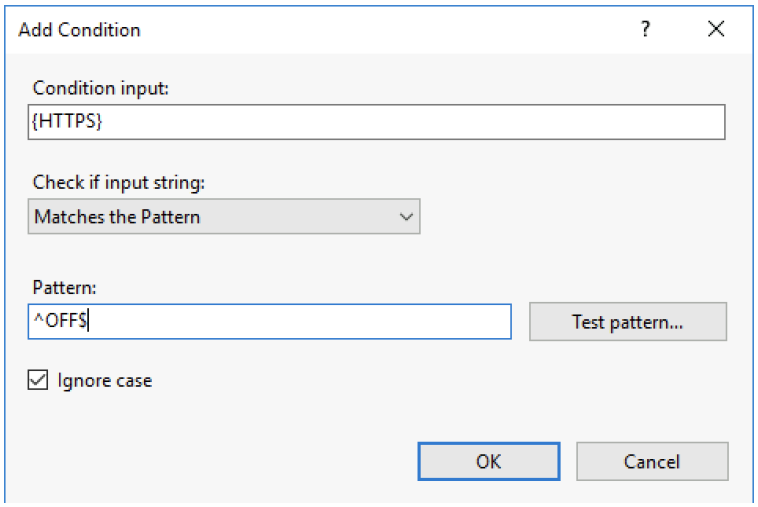
If there's a *HTTP to HTTPS redirect* rule already in place at the top of the list of URL rewrite rules, nothing needs to be done.

Click *Add Rules* in the **Actions** pane on the right, and click OK to create a blank inbound rule.

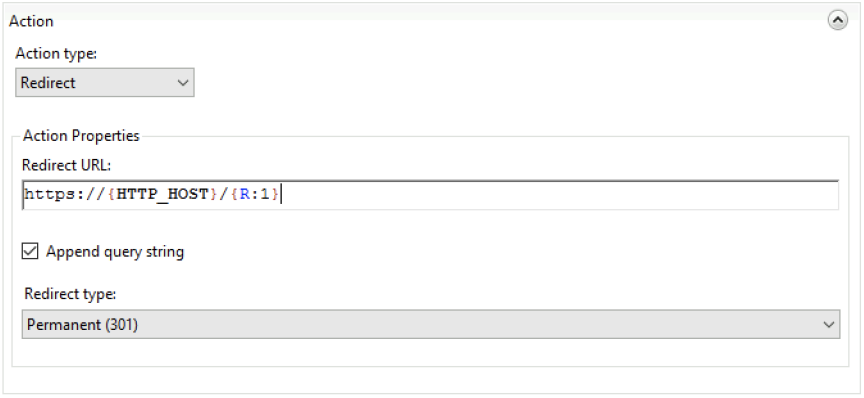
In the name field enter *HTTP to HTTPS redirect*.

In Pattern field enter `(.*)`

Under conditions click *Add* and enter the following condition:



In the **Action** pane on the bottom, choose *Redirect* from the *Action type* dropdown, and set redirect URL to `https://{HTTP_HOST}/{R:1}` and the redirect type to *Permanent (301)*.



Click *Apply* in the **Actions** pane on the left. And click *Back to rules*.

Move the new *HTTP to HTTPS redirect* rule to the top of the rules using the *Move Up* button in the action pane on the right.

Enable content compression for Apache

To speed up response time for large operations, add the following line to `mmws.conf`:

```
AddOutputFilterByType DEFLATE application/json
```

Configure the web application to use a fixed M&M Central server

By default the M&M Web Application allows the user to specify, which M&M Central server is used for the login.

If you want to set a fixed M&M Central Server for the Web App Login dialog follow the steps provided below.

Windows

Steps to configure a fixed Server name for the Web Application login dialog

1. Edit the preferences.cfg file of the M&M Web Services (c:\ProgramData\Men and Mice\Web Services\preferences.cfg). If not already there add a XML-Tag for the default M&M Central server name:

```
<DefaultCentralServer value="your M&M Central DNS name or IP" />
```

2. Add another XML-tag to configure the Web App to use the DefaultCentralServer as fixed server name:

```
<FixedCentralServer value="1" />
```

3. Restart the M&M Web Services Windows service
4. After that the Login dialog shows the DefaultCentralServer name as "Server", greyed out and not editable anymore.

Tip: You might want to clear the browsers cookies that are cached and reload the Web Application site in order to get the right data displayed.

Linux

1. Log in to the server running the web application.
2. Edit the preferences.cfg file of the M&M Web Services (/var/mmsuite/web_services/preferences.cfg). If not already there add a XML-Tag for the default M&M Central server name:

```
<DefaultCentralServer value="your M&M Central DNS name or IP" />
```

3. Add another XML-tag to configure the Web App to use the DefaultCentralServer as fixed server name:

```
<FixedCentralServer value="1" />
```

4. Restart the `mmws` service:

```
systemctl restart mmws
```

Tip: You might want to clear the browsers cookies that are cached and reload the Web Application site in order to get the right data displayed.

Increase timeout for webserver proxy

To ensure that the Web Application works smoothly with larger change request queues (that take longer to process by Central) modify `/etc/httpd/conf` and increase the mmws proxy timeout value:

```
ProxyTimeOut 60
```

Deploying Micetro on Azure

The Azure Marketplace has an offering of Micetro that provides an automated deployment of virtual machines, configured with a database backend using Azure Database. For more information see installation-azure.

1.6 Configuration

1.6.1 Running the Men&Mice components (Central, Controllers)

Linux

After installation, all Men&Mice components are configured as system processes available through `systemctl`. Only use `systemctl` to stop, (re)start, and query the status of the components, i.e.:

```
systemctl status|start|stop|restart mmcentral
systemctl status|start|stop|restart mmremote
```

You can set several options when starting Men&Mice Central (by default `/usr/sbin/mmcentral`):

-ll <level>	Men&Mice Central sends event messages to the system log. You can change the log level for Men&Mice Central by using the –ll command-line option when starting the daemon. Possible levels are 0 - 5 (the default value is 3)
-p <port>	Set port number to listen to (default 1231)
-u <user>	Specifies the user name or user id that the program should run as
-g <group>	Specifies the group name or group id that the program should run as
-d <path>	Sets the path where the data files should be located (the default path is /var/mmsuite/mmcentral)
-v	Displays version information
–h	Displays available command line options for Men&Mice Central

For example:

```
mmcentrald -p 9876 -ll 5 -d /temp/data
```

Windows

Men&Mice Central

Men&Mice Central runs as a service and you can start and stop Men&Mice Central using the Services application. You can also control Men&Mice Central using these command line options:

mmcentral –i	Installs Men&Mice Central as a service
mmcentral –u	Uninstalls Men&Mice Central
mmcentral –start	Starts the Men&Mice Central service
mmcentral –stop	Stops the Men&Mice Central service
mmcentral –v	Displays version information
mmcentral –h	Displays available command line options for Men&Mice Central

Men&Mice Controllers

The Men&Mice DNS Server Controller runs as a service and you can start and stop the Server Controller using the Services application. You can also control the Men&Mice DNS Server Controller using these command line options:

Table 3: widths: 30, 70

mmremote –i	Installs the Men&Mice DNS Server Controller as a service
mmremote –u	Uninstalls the Men&Mice DNS Server Controller
mmremote –start	Starts the Men&Mice DNS Server Controller service
mmremote –stop	Stops the Men&Mice DNS Server Controller service
mmremote –v	Displays version information
mmremote –h	Displays available command line options for the Men&Mice DNS Server Controller

1.6.2 First login

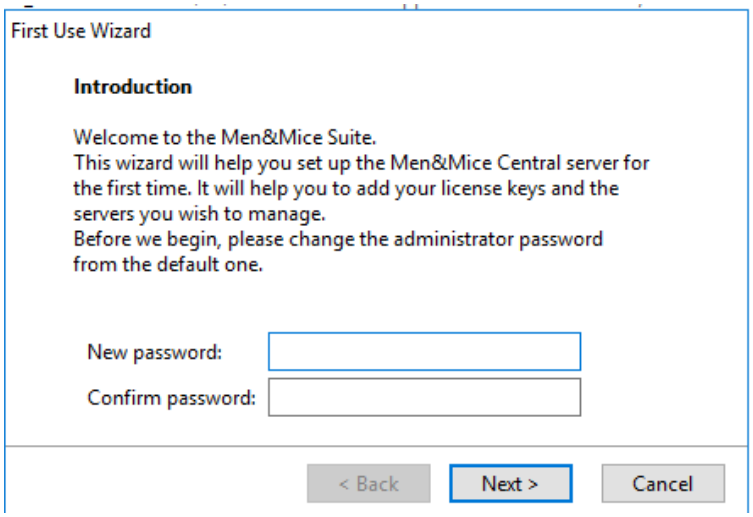
After installing and starting the required components (PostgreSQL, Men&Mice Central, at least one Controller, and the Web Application) administrators must use the Management Console (Windows Client) to log in to and initialize the system.

The default credentials:

- username: `administrator`
- password: `administrator`

After logging in with the default administrator credentials, the system will prompt to change the administrator password.

> **Warning:** Do not lose the password set in this step for the `administrator` user. It cannot be recovered if lost.
>
> Contact Men&Mice Customer Care if the *administrator* user password is lost.



License keys

See *License Management*

Note: The IPAM license key unlocks **both** the DHCP and IPAM functionality of Micetro.

1.6.3 Enable logging for Central

Important: Logging is not enabled by default.

To help troubleshooting, it is highly recommended to enable logging for Men&Mice Central and all Server Controllers. (See *Configuring logging for the Men&Mice Server Controllers*.)

After logging in to the *First login* in the Management Console, navigate to *Tools* → *System Settings* → *Advanced*` and locate the log file settings. (You can use the *Quick Filter* to narrow the options.)

Define the logfile's location (e.g. `/var/mmsuite/mmcentral.log` for Linux) and in '*Logging Level for Men&Mice Central*' set the value.

Note: Men&Mice recommend setting the loglevel to **5** for troubleshooting. Consult the Customer Care team to determine the best loglevel for your environment.

1.6.4 Configuring logging for the Men&Mice Server Controllers

DNS Server Controller

Linux

After installing the DNS Server Controller, *create* the logging directory (`/var/named/mmsuite/` in CentOS or `/var/cache/bind/mmsuite/ in Ubuntu` or specify your own):

```
mkdir /var/named/mmsuite/logs/
```

Edit the `/var/named/mmsuite/preferences.cfg` file and add/edit the following:

```
<LogFileName value="/var/named/mmsuite/logs/mmremote.log" />
<LogDestination value="3"/>
<LogLevel value="5" />
```

(Amend the directory path as needed.)

Restart the DNS Server Controller:

```
systemctl restart mmremote
```

Windows

1. After installing the DNS Server Controller, *create* the logging directory (`C:\ProgramData\Men and Mice\DNS Server Controller\logs` or specify your own).
2. Edit the `C:\ProgramData\Men and Mice\DNS Server Controller\preferences.cfg` file and add/edit the following:

```
<LogFileName value="C:\ProgramData\Men and Mice\DNS Server Controller\logs\mmDnslog.txt"␣
↪/>
<LogDestination value="3"/>
<LogLevel value="5" />
```

(Amend the directory path as needed.)

Restart the DNS Server Controller.

DHCP Server Controller

Linux

After installing the DHCP Server Controller, *create* the logging directory (`/var/mmsuite/dhcp_server_controller/logs/` or specify your own):

```
mkdir /var/mmsuite/dhcp_server_controller/logs/
```

Edit the `/var/mmsuite/dhcp_server_controller/preferences.cfg` file and add/edit the following:

```
<LogFileName value="/var/mmsuite/dhcp_server_controller/logs/mmremote.log" />
<LogDestination value="3"/>
<LogLevel value="5" />
```

(Amend the directory path as needed.)

Restart the DHCP Server Controller:

```
systemctl restart mmremote
```

Windows

1. After installing the DHCP Server Controller, *create* the logging directory (`C:\ProgramData\Men and Mice\DHCP Server Controller\logs` or specify your own).
2. Edit the `C:\ProgramData\Men and Mice\DHCP Server Controller\preferences.cfg` file and add/edit the following:

```
<LogFileName value="C:\ProgramData\Men and Mice\DHCP Server Controller\mmremote.log" />
<LogDestination value="3"/>
<LogLevel value="5" />
```

(Amend the directory path as needed.)

Restart the DHCP Server Controller.

1.6.5 Micetro User Management

Note: Access management has changed in Micetro 10.1. To view the access management used in previous versions, switch to the appropriate version number using the version selector.

For detailed information, see *Access Management*.

Jump to: *Single Sign-On (SSO) and Multi-Factor Authentication (MFA)*

1.6.6 External Authentication

Note: Unless indicated otherwise, instructions here are to be performed in the Management Console.

Overview

This section discusses the available user authentication methods available with Micetro.

In addition to Local User Authentication, Micetro currently supports two methods of AD user authentication using the Windows Active Directory user database and authentication through a RADIUS server.

Micetro also supports multi-factor authentication (MFA) through two methods, Azure and Okta.

Active Directory User Authentication

The Active Directory (AD) User Authentication mechanism allows you to have users authenticate themselves in the AD login system before allowing them to login to Micetro. In large installations, this system has obvious benefits as users do not have to maintain their passwords in multiple locations. The password rules (password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to Micetro.

Active Directory User Authentication vs. Local User Authentication

Even when you are using AD User Authentication, you must create users in the Management Console and assign privileges to them using the Men&Mice access system. The only difference between AD vs. local user authentication is that when AD user authentication is used, users are authenticated using the AD User Authentication system before they can access the Management Console. When AD User Authentication is used, the user password is not stored in the Men&Mice software.

Note: Only one authentication method can be used per user, but different users can have different authentication methods. That means you can have some users log in using AD user authentication, while other users log in using local user authentication.

Enabling AD User Authentication Using Active Directory

AD user authentication using Active Directory is only possible when you run Micetro Central on a Windows machine. The machine running Micetro Central must be a member in an Active Directory domain or forest. No specific configuration is needed for Men&Mice Central for user authentication using Active Directory.

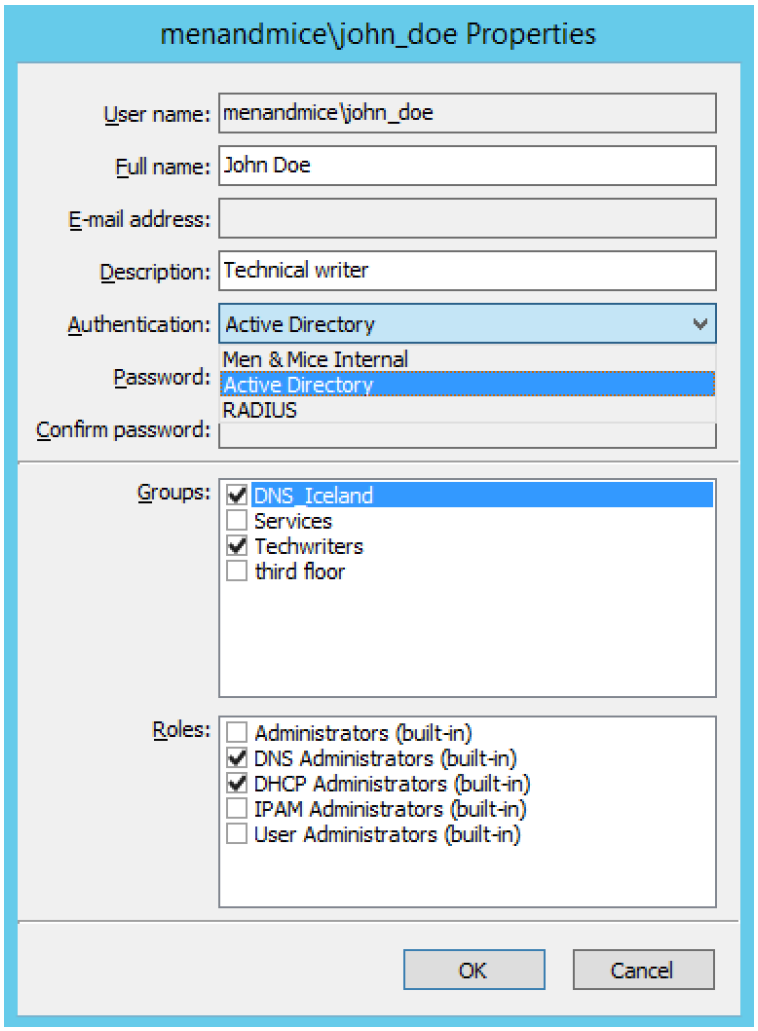
Configuring Users for AD Authentication

To configure a user to use AD user authentication, do the following:

1. From the menu, select *Tools* → *User management*.
2. Select the applicable user from the list. If the desired user is not shown, the user must be added to the application. For more information, see *Users*.
3. When the *Properties* dialog box display, move to the **Authentication** field, click the drop-down list, and select the applicable authentication method. (If Men&Mice Central is not running on a Windows machine, only the Micetro authentication method displays.)
4. Click *OK*.

Note: When the AD authentication method is selected, the **Password** field is disabled, since the password is not stored in Micetro.

Active Directory Single Sign-on



You can enable the Single Sign-on so that Active Directory users do not have to authenticate when logging in through the Management Console.

To enable Active Directory Single Sign-on, do the following:

1. From the menu bar, select *Tools* → *System Settings*.
2. In the *System Settings* dialog box, click the *General Settings* tab.
3. Select the *Allow Single Sign-on* option.
4. Click *OK*.

Web Interface

When single sign-on is enabled, it is possible to enable sign-on in the web interface if the web application is running on a Microsoft Windows Server.

To enable single sign-on in the web application, make sure that Single Sign-on and Single Sign-on for web is enabled in Micetro.

Application Log In

Logging in to Micetro will not change when AD user authentication is used and Single Sign-on is disabled. The only thing to keep in mind is that the user name that is entered must match the user name stored in Micetro. If a distinguished user name is used, it must be entered in the same way when logging in.

Group Level Active Directory User Authentication

The Group Level Active Directory (AD) User Authentication mechanism allows you to set user access privileges by group membership in the AD. In large installations, this system has obvious benefits as the users do not have to maintain their passwords in multiple locations. The password rules (i.e., password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to Micetro.

The login sequence is as follows for users with Group Level AD authentication:

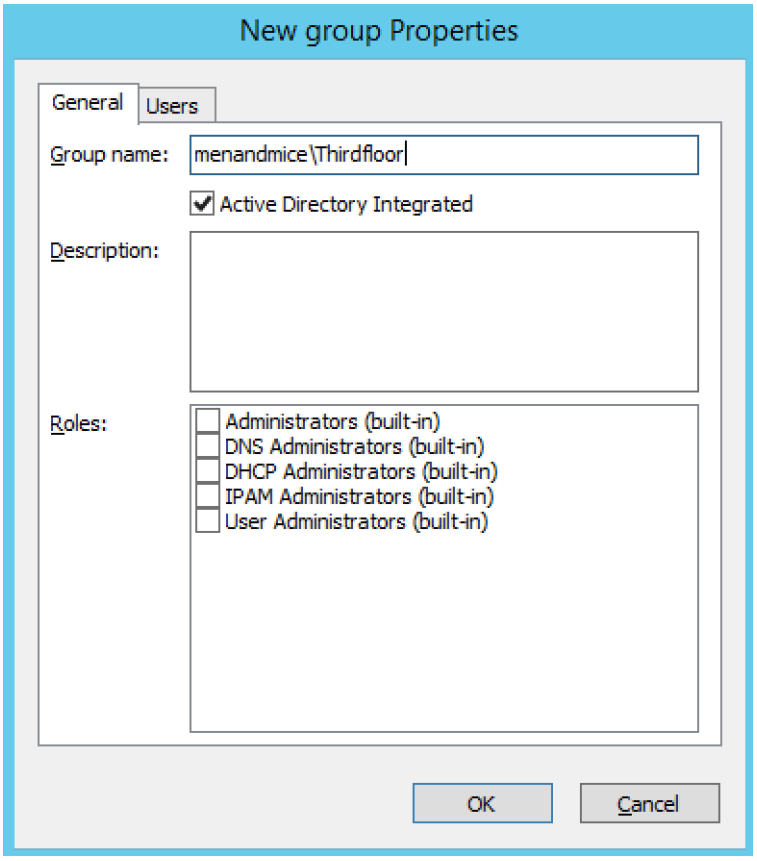
1. The user enters his/her user name and password in Micetro
2. Micetro uses the AD authentication mechanism to validate the user name and password. If the user name and password is correct, Micetro retrieves the group membership of the user from the AD.
3. The AD group list of the user is compared (by group name) to the local group list in Micetro. If a match is found, the user is logged in with the privileges specified in the local group list. If no match is found, the login fails.

To allow a user to log in to Micetro, you must create a group in the AD that has the same name as a group in Micetro and place the AD user in that group. You may create multiple groups in the AD that match group names in Micetro.

Configuring Groups for AD Group Level Authentication

When using AD Group level authentication, you must specify which groups in Micetro should be used to verify group membership.

1. From the menu, select *Tools* → *User Management*. The *Users and groups management* dialog box displays.
2. Click the *Groups* tab.
3. Select the group to which you want to configure AD, and then click *Edit*. If the desired group is not shown, you will need to add the group. See *Groups*.



Group Name

Ensure that the group name is prefixed with the name of the owning domain name. Example: The Active Directory domain "MYDOMAIN" contains the group "MM-ReadOnly". The group name must then be "MYDOMAIN\MM-ReadOnly".

4. Click the checkbox for *Active Directory Integrated*.
5. Click *OK*.

Note: Group Level Active Directory user authentication is only possible when you run Men&Mice Central on a Windows machine. The machine running Men&Mice Central must be a member in an Active Directory domain or forest.

Configuring Users and Access Privileges

You do not have to create users in Micetro when the Group Level AD authentication is used. Instead, user access is controlled by the group membership of the user in the AD.

RADIUS User Authentication

Micetro can authenticate using an external RADIUS server. In large installations, this system has obvious benefits as the users do not have to maintain their passwords in multiple locations. The password rules (password expiry, minimum password length, etc.) that have been applied within the organization automatically apply to Micetro.

RADIUS User Authentication vs. Local User Authentication

Even when you are using RADIUS User Authentication, you must create users in the Management Console and assign privileges to them using the Men&Mice access system. The only difference between RADIUS vs. local user authentication is that when RADIUS user authentication is used, users are authenticated using the RADIUS User Authentication system before they can access the Management Console. When RADIUS User Authentication is used, the user password is not stored in the Men&Mice software.

Note: Only one authentication method can be used per user, but different users can have different authentication methods. That means you can have some users log in using RADIUS user authentication, while other users log in using local user authentication.

Enabling RADIUS User Authentication

To enable RADIUS authentication, you must add several properties to the Men&Mice Central configuration file preferences.cfg. This file is located in the data folder inside the Men&Mice Central data directory:

- Windows: C:\Program Files\Men&Mice\Central\data
- Mac OS X: `/var/mmsuite/mmcentral`
- All others: set during installation. Usually `/var/mmsuite/mmcentral` or `/chroot/var/mmsuite/mmcentral`, where `/chroot` is the location used as a chroot jail for named.

The properties to be added are:

RADIUSServer	Defines the address of the RADIUS server that will do RADIUS authentication.
RADIUSPort	Defines the port that the RADIUS server is listening on. The default value is 1812, which is the port normally used by RADIUS.
RADIUSSharedSecret	The shared secret between the RADIUS server and Micetro.
RADIUSAuthentication	The type of authentication used. 0 = PAP, 1 = CHAP.

Example:

```
<RADIUSServer value="192.168.1.3"/><RADIUSPort value="1515"/><RADIUSSharedSecret value=
↪"MyBigSecret"/><RADIUSAuthentication value="1"/>
```

After editing the file, restart Men&Mice Central.

- Windows: use *Administration Tools* → *Services* to restart Men&Mice Central.

- Mac OS X: Execute the following shell command in a Terminal window (/Applications/Utilities/Terminal):

```
sudo /Library/StartupItems/mmSuite/mmcentral restart
```

- All others: Execute the `mmcentral` init script with the 'restart' argument.

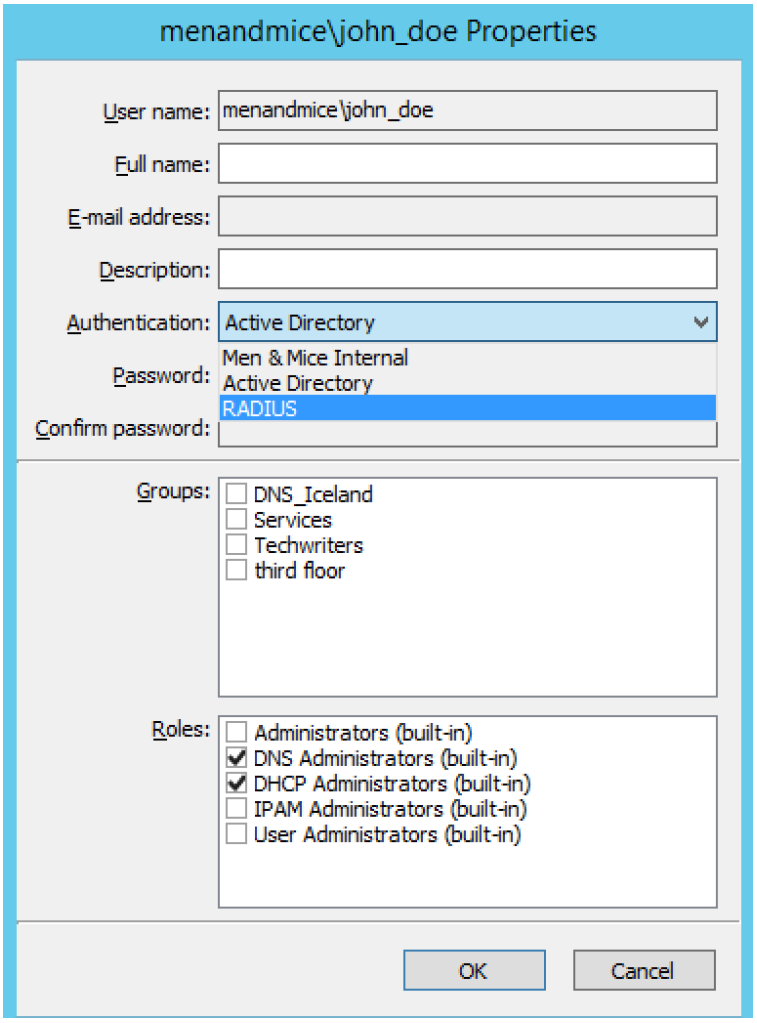
Configuring Users

To allow a user to log in to the Men&Mice system, the user must exist in the Men&Mice user database. If the user does not exist in the Men&Mice user database, they are not allowed to log in, even if they provide a valid user name and password in the RADIUS login system.

To configure a user to use AD user authentication, do the following:

1. From the menu bar, select *Tools* → *User Management*. The *User and group management* dialog box displays.
2. To add a new user, click the *Add* button. Refer to *Users*. Follow the instructions with one exception: select RADIUS on the **Authentication** drop-down list.
3. To modify an existing user, double-click on the user's name to display the user *Properties* dialog box, and select RADIUS on the **Authentication** drop-down list.

Note: When the RADIUS authentication method is selected, the **Password** field is disabled, since the password is not stored in Micetro.



Logging into Micetro

Micetro has integrated with both Azure Active Directory and Okta to allow integration with multi-factor authentication and SSO.

Once configured the frontpage of Micetro will present buttons to redirect the user to the provider's URL for authentication.

Configure LDAP authentication

Introduction

This document describes how to configure LDAP authentication in Micetro.

Installation on Centos Linux

1. Download the Python script and signature file from GitHub.
2. To use LDAP authentication and authorization, start by installing `mm_ldap.py` on the machine where the Men&Mice Central service is run and install the Python extension used by Central when connecting to an LDAP directory:

```
sudo yum install python-ldap
sudo mkdir /var/mmsuite/mmcentral/extensions
sudo cp mm_ldap.py /var/mmsuite/mmcentral/extensions
sudo chown -R root:root /var/mmsuite/mmcentral/extensions
sudo chmod 440 /var/mmsuite/mmcentral/extensions/mm_ldap.py
```

A signature file for the python extension will also have to be installed and placed in the extension directory:

```
sudo cp mm_ldap.signature /var/mmsuite/mmcentral/extensions
```

Note: For security reasons, the Central service will not execute `mm_ldap.py` unless the signature in`mm_ldap.signature` matches the signature calculated for `mm_ldap.py`.

Configuring LDAP

LDAP configurations are stored in a JSON config file that should be stored in the Men&Mice Central service root directory:

```
sudo cp ldapconf.json /var/mmsuite/mmcentral
sudo chown root:root /var/mmsuite/mmcentral/ldapconf.json
sudo chmod 440 /var/mmsuite/mmcentral/ldapconf.json
```

The configuration file has the following schema:

```
{
  "server": {
      "uri": str, // e.g. ldaps://example.com:636
      "reader_dn": str | null,
      "reader_password": str | null,
      "skip_cert_verification": bool | null, // Default: false.
      "ca_cert_file": str | null,
      "disable_referrals": bool | null, // Default: true.
      "use_start_tls": bool | null, // Default: false.
      },
  "user_search_config": {
      "base_dn": str,
      "search_filter": str,
      "scope": "subtree" | "onelevel", // Default: 'subtree'
      "email_attribute": str | null,
      "group_search_config": null | {
          "base_dn": str,
          "scope": "subtree" | "onelevel", // Default: 'subtree'
          "search_filter": str,
```

(continues on next page)

(continued from previous page)

```
        "name_attribute": str // Default: 'name'
      }
    }
  }
```

Name	Description	Example	Required	Default
uri	URI for LDAP service.	ldaps://exa	Yes	None
reader_dn	DN or login name for a user that has permissions to search in the directory. Not needed when all users have permissions to search (for example AD LDAP service).	user@exa	No	None
reader_pa	Password for reader_dn user.		No	None
skip_cert_	If true, then certificates will not be verified. Set to true when using self signed certificates.		No	false
ca_cert_fi	Path of file containing all trusted CA certificates.		No	None
disable_refer	Skip referrals when doing LDAP queries. Should be set to true for AD LDAP services.	No	true	
user_start_	Use TLS when connecting to LDAP service. This is still experimental. Please use LDAPS instead.		No	false
user_searc	DN from where to start searching for a user in the directory.	'dc=corp, dc=examp dc=com'	Yes	None
user_searc	Filter to use for searching for a user. Username will be inserted into placeholder '{username}' if specified.	(&(objectClass=use	Yes	None
scope	Scope to use when searching. Should be either 'subtree' or 'onelevel'. Defaults to 'subtree'.	subtree	No	subtree
email_attr	LDAP attribute used to store users email address.	userPrincipalName	No	None
group_sea	DN from where to start searching for groups in the directory.	'dc=corp, dc=examp dc=com'	If grou authentication is used	None
group_sea	Scope to use when searching. Should be either 'subtree' or 'onelevel'. Defaults to 'subtree'.	subtree	No	subtree
group_sea	Search filter to use when searching for groups. Users DN will be inserted into placeholder '{dn}' if specified. Username will be inserted into placeholder '{username}' if specified.	(&(objectClass=gro	If grou authentication is used	None
group_sea	Attribute used to store name of group.	name	If grou authentication is used	name

Example configuration for connecting to an AD LDAP service:

```
{
  "server": {
      "uri": "ldaps://ldap.example.com:636",
      "skip_cert_verification": false,
      "disable_referrals": true,
      "use_start_tls": false
      },

  "user_search_config": {
      "base_dn":  "dc=corp, dc=example, dc=com",
      "search_filter": "(&(objectClass=user)(userPrincipalName={username}))",
      "scope": "subtree",
      "email_attribute": "userPrincipalName",
      "group_search_config": {
          "base_dn": "dc=corp, dc=example, dc=com",
          "scope": "subtree",
          "search_filter": "(&(objectClass=group)(member:={dn}))",
          "name_attribute": "name"
          }
      }
  }
```

Configuring the Men&Mice Central service to authenticate users using an LDAP service.

To configure the Men&Mice Central service, login as the superuser `administrator` through the Men&Mice Management Console. In the top left-hand corner select *Tools* → *System Settings* → *Advanced* and check the *Enable LDAP integration* checkbox.

Using LDAP with Central running on Windows

To use LDAP with a Men&Mice Central server running on Windows, Python must be installed for all users. See *Installing Python for Men&Mice Central on Windows*.

API Authentication methods

There a few options for authenticating against the M&M API:

- *Login command*
- *Authorization Headers*
- *Single Sign-On*

Login command

This method is available in all versions of M&M, and all the different flavors of the M&M API (SOAP/JSON-RPC/REST). In the REST API, this command is available via the URL commands/Login

The Login command takes in server (for the M&M Central server), user name, and password, and returns a session ID, which should then be used for all other API calls via their session parameter.

The Login command and its parameters is fully documented in the normal SOAP API documentation

---

Note: Remember to configure HTTPS for the mmws and/or _mmwebext sites for this authentication method, since the username and password can easily be extracted for anyone listening in on the communication.

Authorization Headers

With the introduction of Men&Mice Web Services and the REST API in version 7.3, it's now also possible to authenticate via HTTP headers, by adding a Basic Authorization header, or with a Negotiate Authorization header, if the client supports it.

Note: If AuthorizationMethods is not defined in the preference file mmWS will only accept basic authorization.

By using authorization headers for authentication, the Login command becomes unnecessary, and the session ID is not used. The "session" parameter for all the commands must be omitted, and not left blank.

With this authentication method, multiple M&M Web Service instances can be deployed and used simultaneously behind a load balancer to provide a redundancy that is transparent to the API client.

The session IDs, on the other hand, are only valid on the API endpoint (web service) they were created with. So when an API client that uses a session id gets redirected to another Web Service/API Endpoint, the client will get an error that the session id is invalid or expired, and then needs to login again to get a new session id before proceeding.

Basic Authentication

For Basic Authentication, simply include a HTTP header like:

```
Authorization: Basic QWxhZGRpbjpPcGVuU2VzYW1l
```

where the last part is `<user name>:<password>`, base64 encoded

For more information on Basic Authorization headers on the client side, see for example here: https://en.wikipedia.org/wiki/Basic_access_authentication

The authorization header authentication method is only available for JSON-RPC and REST APIs, and only if using M&M Web Services as an endpoint (i.e. the URL is <server>/mmws/api or <server>/mmws/json)

Note: Remember to configure HTTPS for the mmws site for this authentication method since the username and password can easily be extracted for anyone listening in on the communication.

Negotiate Authentication

Negotiate header Authorization (SPNEGO-based Kerberos and NTLM HTTP Authentication) is also supported when the client supports it, and when it has been enabled for the Men&Mice Web Services.

This way, the user name and password are not provided in the header, and the API call is executed in the security context of the user that invokes it. In other words, this is the single sign-on authentication option that the Men&Mice Web Services provides.

To enable the Negotiate header Authorization in M&M Web Services, add the following line to the `preferences.cfg`, and restart the `mmws` service.

```
<AuthorizationMethods value="Kerberos,NTLM" />
```

The order of the methods can be changed, e.g. if NTLM is preferred over Kerberos but in general if you don't want to allow NTLM (which is less secure) as a fallback only specify Kerberos as a value.

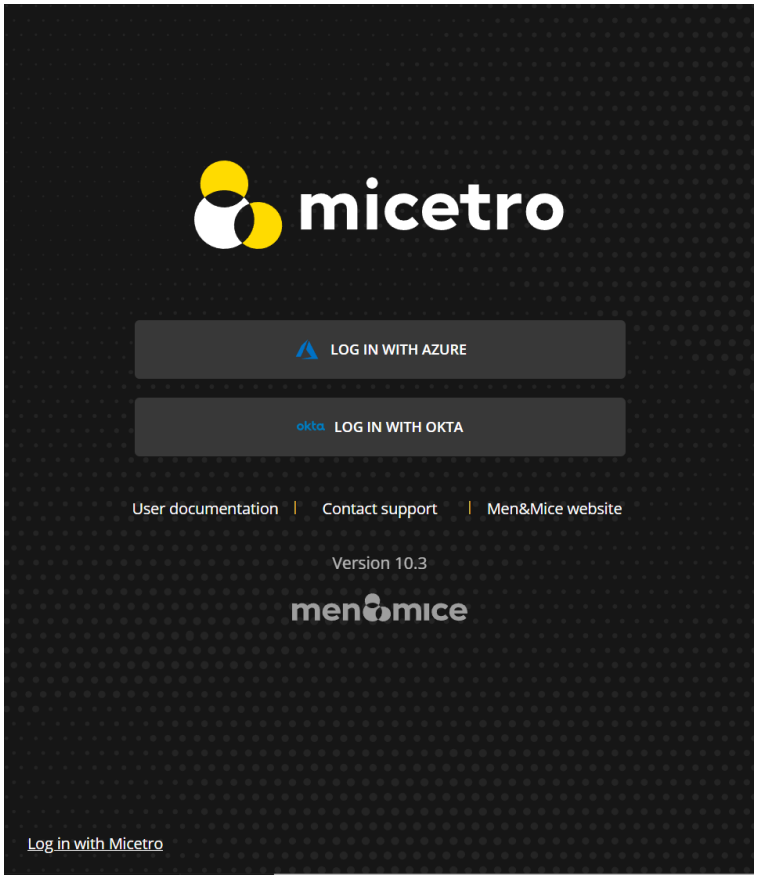
Single Sign-On

To enable single sign-on in the web application, make sure that Single Sign-on and Single Sign-on for web is enabled in Micetro. See *External Authentication*.

Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

Integrating with Identity Provider's SSO/MFA

Micetro is adding support for multifactor authentication via two identity solutions, Azure Active Directory and Okta.



Dependency Checklist

- Configure and enable SSO and MFA in your identity provider
- Micetro web servers must be configured for HTTPS and have a valid certificate
- Central must have internet access to identity provider's endpoints
  - **Azure**
    - login.microsoftonline.com
    - graph.microsoft.com
  - **Okta**
    - *.okta.com
- Python with dependent libraries and requests package is installed on the Central server
  - Azure
    - msal >=1.17 – The Microsoft Authentication Library that enables Micetro to access the Cloud for AAD - https://pypi.org/project/msal/1.17.0/
    - requests - https://pypi.org/project/requests/
  - Okta
    - Python 3 required.

* okta_jwt_verifier >=0.2.3 – Verifies Okta access and ID tokens - okta-jwt-verifier · PyPI
* requests - https://pypi.org/project/requests/

Note: If running Central in HA mode, it is advised to disable the service on one of the partners to ensure installation is successful on each server, and to prevent the servers from failing over during the installation.

Installation and configuration must be done on ALL Central servers in your environment.

Installation/Setup

Setting up the Application (Identity Provider) To get the needed properties for the configuration an application first needs to be set up at the provider.

Azure Active Directory If running Central in HA mode, it is advised to disable the service on one of the During this configuration, you will need to capture your Identity Provider's credentials.

Permissions To be able to fetch the user's profile info and group membership, the application needs to be given permission to do that:

Table 4: Microsoft Graph

API/Permission Name	Type	Description	Admin consent request	Status
GroupMember.Read.All	Delegated	Read group memberships	Yes	Granted for [name]
User.Read	Delegated	Sign in and read user profile	No	Granted for [name]

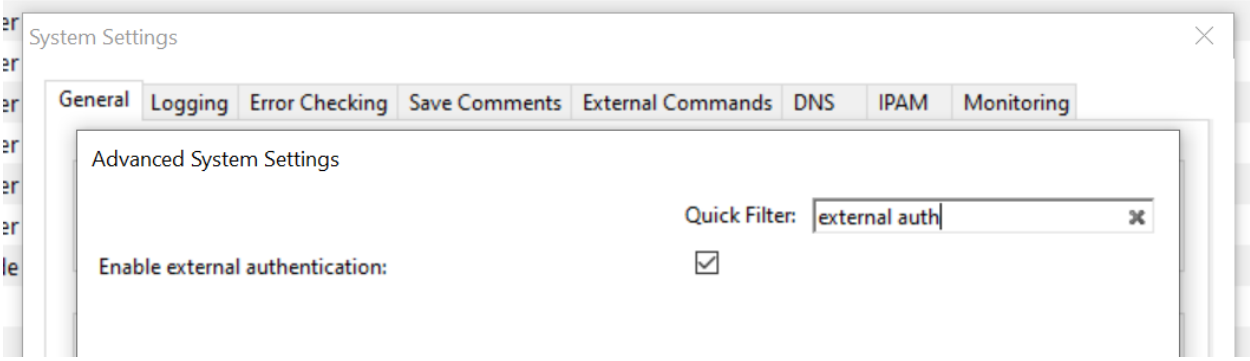
The app asks for `User.Read` from the user, but an administrator needs to grant `GroupMember.Read.All`. Group membership will not be synced if `GroupMember.Read.All` (or some wider groups permission) is not granted to the application by an administrator.

Register the Application

The setup requires navigation to the Azure Portal, and opening AAD.

1. On the left pane, select "App registration" and inside the newly opened "blade" (what Azure calls their subpages) click "New Registration"
2. Type the name, select the proper radio button value for supported authentication types and for the Redirect URI the platform should be web and the field should behttps://micetro.central.fqdn/mmws/auth_cb/microsoft
3. Once the app has been registered, the client ID should be viewable in the essentials panel for the app.
4. Navigate to Certificates and Secrets to generate a new secret for the App to use.

Note: You will need this information for the Central configuration file.



Okta

To get the needed properties for other configuration an application first needs to be set up at the provider.

Table 5: Okta Application

Sign-in method	OIDC - OpenID Connect
Application type	Web Application
Grant type	Authorizationo Code (default)
Sign-in redirct URIs	[Micetro URL]/mmws/auth_cb/okta
Sign-out redirect URIs (optional)	[Micetro URL]

The setup requires opening the Okta Administrator page.

1. On the left pane, expand “Application” and click “Applications”.
2. On the Applications page, click “Create App Integration”.
3. Select OIDC as Sign-in method.
4. Select Web Application as Application type.
5. Grant type: Authorization Code (default)
6. Sign-in redirect URIs: **https://micetro-central-fqdn/mmws/auth_cb/okta**
7. Sign-out redirect URIs: **https://micetro-central-fqdn/**

Okta Authorization Server

An Okta config with server_id set to default means that the Default Custom Authorization Server provided by Okta is used. Otherwise, the value should be the name of the Custom Authorization server that has been setup at Okta or be skipped (or empty) if the Org Authorization Server should be used.

Group authorization

Both new identity solutions can be used in conjunction with group authorization models in Micetro

Group membership is mirrored by matching group names, i.e., the user is added to groups (both AD and Internal, but not Built-in) in Micetro whose names match group names listed by the provider and removed from groups that do not match. If the provider does not list groups, the user’s group membership is not altered.

Note: There are options to filter and transform the provided groups in the setup of the applications at the provider’s end.

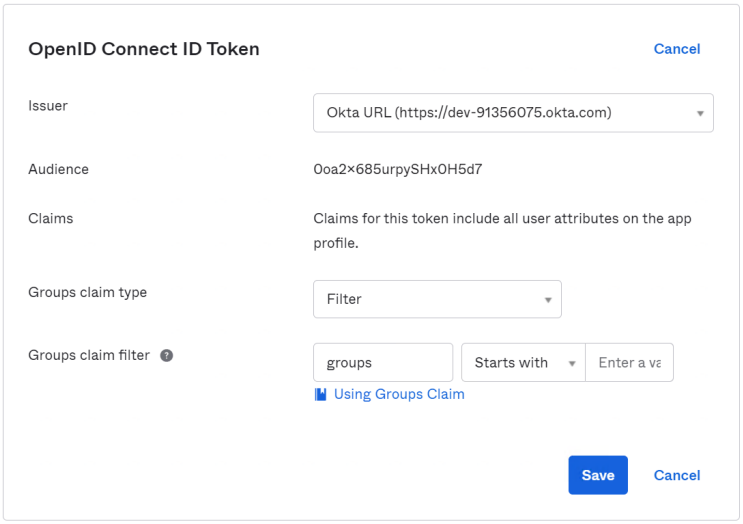
Mapping groups from Microsoft Azure AD

As Azure only returns group ID with the token the script makes an extra call to Microsoft Graph API to fetch the group names. The Graph URI used can be changed in the config (groups_uri), but it should generally not be needed. As there is a limit of about 200 group IDs that can be returned within the JSON Web Token filtering should be used to supply only the necessary groups.

Configure group claims for applications by using Azure Active Directory

Mapping groups from Okta

To map group memberships from Okta an *ID Token Claim* has been created with the name "groups". Add an *OpenID Connect ID Token* to the application of the type "Filter" with the name "groups".



Configure Central Server

1. Install Python and dependent libraries and packages on the Central server.

When installing Python please ensure the following:

- Python is available to "all user" (Windows)
- That you are using a ratified (tested by Men&Mice) version of Python (see dependency checklist)
- Python is installed in the "Default" environment
- Add the below XML-tag to the Preferences.cfg to set the path:

```
<PythonExecutablePath value="C:\\Python39\\python.exe" />

* Windows - C:\ProgramData\Men and Mice\Central\preferences.cfg

* Linux - /var/mmsuite/mmcentral/preferences.cfg
```

Note: A Central restart is required after this statement is added to the Preferences.cfg file.

2. **Create a new directory called "extensions"** in the Central data directory.
   - Windows - C:\ProgramData\Men and Mice\Central\extensions

- Linux - /var/mmsuite/mmcentral/extensions

3. **Download and unzip the Micetro authentication script and signature file** from Github into the newly created extensions directory.

   - mm_auth_cb.py.zip - This Python scripthandles the authentication callback from the external provider. The same script serves both providers.
   - mm_auth_cb.signature.zip

   For security reasons the script is signed and will not be run if there is not a matching signature filemm_auth_cb.signaturefound in the same folder.

4. **Manually create a json configuration file int he Micetro data directory**. At start up the Micetro Central program will search the data directory for a file named"ext_auth_conf.json". It will read the contents of the file and store it in the database along with the timestamp.

The structure of the JSON object inside the configuration file is unique for each customer depending on the identity solution that is being configured.

Micetro data directory:

Windows: C:\ProgramData\Menandmice\Central\ext_auth_conf.json

Linux: /var/mmsuite/mmcentral/ext_auth_conf.json

Add the contents below with credentials obtained from your Identity Provider.

Sample config:

Azure:

```
   "microsoft": {

      "tenant_id": "Company_tenant_id (must match Azure)",

      "client_id": "xxxxxxx-xxxx-xxxx-xxxxx-xxxxxxxxxxx",

      "client_credential": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",

      "redirect_uri": "http://localhost/mmws/auth_cb/microsoft (must match what is␣
↪configured in Azure)"

   }

}
```

Okta:

```
   "okta": {

      "domain": "Company_domain.okta.com",

      "server_id": "xxxxxxxxxxx|'default'", (can be skipped/empty)

      "client_id": "xxxxxxxxxxx",

      "client_secret": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",

      "redirect_uri": "http://localhost/mmws/auth_cb/okta (must match what is configured␣
```

(continues on next page)

(continued from previous page)

```
↪in Okta)"

   }

}
```

This will cache the credentials in the DB (no need to restart Central). Once Authentication through the Service Providers is established, the json configuration file can be deleted.

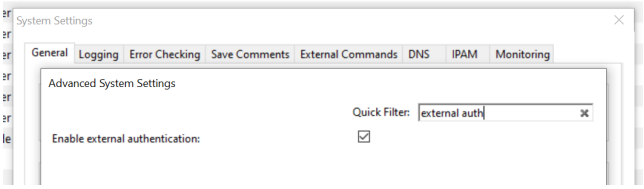
About the credential caching

The contents of the configuration fileext_auth_conf.jsonare cached in the database, therefore the file can be deleted after external authentication is up and running. The cached version is updated automatically based on the file timestamp.

Clear the cached configuration

If for some reason you want to clear the cached configuration file in the database.

1. Empty the .json configuration file.
2. Go to Console Advanced System Settings and ensure that you have the "Default web form" enabled (Tools->System Settings->Advanced).
3. Test with your browser to ensure you can login locally.
4. Disable the external authentication in System Settings.
5. **Enable external authentication in the Micetro system settings** In the Management Console, go to *Tools* → *System Settings* → *Advanced* and search for "external auth".

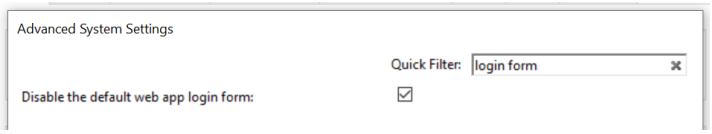


It is also possible to enable it via an API call to SetSystemSettings with a system setting named enableExternalAuthentication and value of 1.

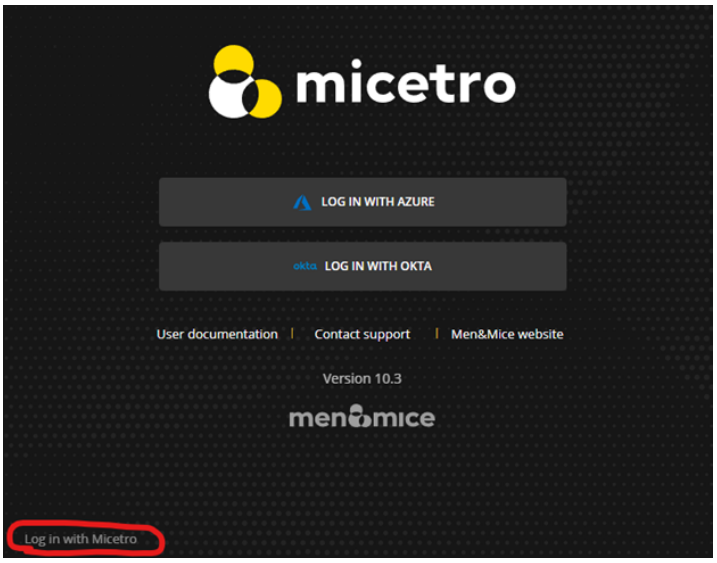
This will enable the SSO login in the web.

6. Turn off default login form (optional)

   If you only want to offer users SSO/MFA login, you can disable the default web app login form.



   This will remove local/onprem login in the Web. However, you still have the option to bypass this at login.



The form will not be hidden if there is no external provider configured. The login form can be found be clicking the "Log in with Micetro" down in the left corner of the login page.

Login and Grant User/Group Access

At first login, when using either Azure Active Directory (AAD) or Okta, **a new user account is created in Micetro**. This user account will appear with the type "External". External changes to user's email, full name and group membership are synced at subsequent logins by matching the external ID.

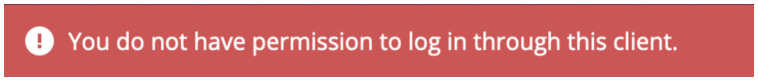
A single user profile is thus not shared between an external user authenticated by Azure AD (or Okta) and AD-integrated SSO, instead they are treated as separate users in Micetro.

By default, all external users are added automatically to the "All users (built-in)" group. If group memberships are among the properties being returned by the identity service, then Micetro will add the user to groups with a matching name inside Micetro.

A few properties are synchronized by Micetro; such as user's email, full name, and group memberships. Any external changes to these properties are updated in Micetro on the next login.

Note: After the new External accounts are added (automatically, when user first logs in), administrators will still need to grant access to the DNS/DHCP/IPAM roles.

If privileges have not yet been granted for the new external accounts, the user will get the below error:



Addendum

Troubleshooting

Logging for External Authentication can be enabled by putting your Central log in ll6.

External changes to user profiles

External changes to user's email, full name, and group membership are automatically replicated in Micetro on next login.

Separate hosts for Micetro Central and Micetro Web Application

The Web Application/Web service is traditionally on the same host as the Micetro Central and by default, the tool will send queries to "localhost".

if Micetro Central is on a different host from the Web Service then you can add the following XML-tag to the preference value to auto-populate the "Server" field at login:

```
<DefaultCentralServer value="IP or DNS name of the Men & Mice Central server" />

* Windows - C:\ProgramData\Men and Mice\Central\preferences.cfg
* Linux - /var/mmsuite/mmcentral/preferences.cfg
```

1.6.7 Adding DNS Service

After installation, Micetro contains no data about DNS servers. These need to be added.

DNS servers require *Micetro Agents* and need to be added using their fully qualified names (such as `dns1.europe.ad.mmdemo.local`).

Note: Servers in Microsoft Active Directory environments can be added without installing a server controller. See *Agent-free management of DNS/DHCP servers*.

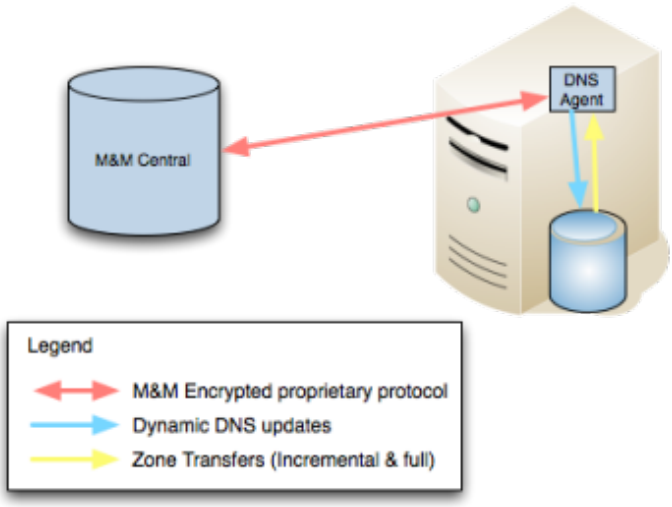
Services are managed on the **Admin** page in the *Service Management* section. There you select *Add Service* to add a new server.

For further details, see *Adding a Service* in the Admin Guide.

Note: To add a new DNS server in the Management Console, select *File* → *New* → *DNS Server*.

DNS Servers in Active Directory Integrated Zones

The DNS agent will use two different methods to retrieve information from Microsoft AD integrated zones. First it will do a zone transfer (both full and incremental) to get the latest records for the zone and then it will use Microsoft APIs to get detailed information for individual records. Due to this it is important that the DNS agent is allowed to do a zone transfer from the local server.



The DNS agent on the DNS server must be able to transfer AD integrated zones from the local DNS server.

Note: There is a global setting in the Management Console that allows Micetro to adjust the zone transfer settings for dynamic or AD integrated zones. It is enabled by default but the administrator can change this setting. See *Disable "Automatic adjustment of Zone Transfer"* for details.

1.6.8 Adding DHCP Service

DHCP servers require *Micetro Agents* and need to be added using their fully qualified names (such as `dns1.europe.ad.mmdemo.local`).

Note: Servers in Microsoft Active Directory environments can be added without installing a server controller. See *Agent-free management of DNS/DHCP servers*.

Note: ISC DHCP servers require a DHCP Server Controller to be installed on each DHCP server. Kea servers require *only one* DHCP Server Controller installed in the system, either on the machine running Kea, or a machine that can connect to the *Kea Control Agent* through the network.

The following table demonstrates the different options when adding a DHCP Server.

Server type	Description
Microsoft Agent-Free[1] (Use proxy not checked)	The DHCP Server Controller has been installed on the machine running the Men&Mice Central Component, and that machine will be used as a proxy. Micetro is not able to track lease history data.
Microsoft Agent-Free[Page 98, 1] (Use proxy checked)	The DHCP Server Controller has been installed on the machine identified in the **Use proxy server** field, and that machine will be used as a proxy. Micetro is not able to track lease history data.
Microsoft with Agent Installed	The DHCP Server Controller has been installed on the remote DHCP server. Micetro is able to track lease history data.
ISC DHCP	Either a Unix server running the ISC DHCPD or a Men&Mice Appliance with the `mm-dhcpd` package installed
ISC Kea (Agent-free)[1]	A server running ISC Kea with the *Kea Control Agent* installed and accessible for the DHCP Server Controller.
ISC Kea	A server running ISC Kea with a DHCP Server Controller and Control Agent installed.[2]
Cisco (Use proxy not checked)	The DHCP Server Controller has been installed on the machine running the Men&Mice Central Component, and that machine will be used as a proxy.
Cisco (Use proxy checked)	The DHCP Server Controller has been installed on the machine identified in the **Use proxy server** field, and that machine will be used as a proxy.

Important: To add Kea servers to Micetro, they need to be configured with the `libdhcp_lease_cmds.so` library. See *Adding Kea to Micetro* for details.

Services are managed on the **Admin** page in the *Service Management* section. There you select *Add Service* to add a new server.

For further details, see *Adding a Service* in the Admin Guide.

Note: To add a new DHCP server in the Management Console, select *File* → *New* → *DHCP Server*.

1.6.9 IP Address Ranges and Devices

Once DHCP services have been added to Micetro, all the scopes from the DHCP servers will be visible in the interface on the **IPAM** page. The organization might also have a spreadsheet or a database with other IP address range (subnet) allocations and details on individual devices (IP addresses). This data can be manually entered in Micetro or more efficiently, imported in bulk.

You can import IPAM data to Micetro using the Web Application. See webapp-import-ipam-data

For importing IPAM data using the Management Console (not recommended), see import-ipam-old.

[1] See *Agent-free management of DNS/DHCP servers*.
[2] Alternatively, you can configure a socket for communication in `kea-dhcp4.conf`.

1.7 Advanced configuration

1.7.1 Advanced System Settings

Note: The *Advanced System Settings* are only available for the built-in "administrator" user.

To access the System Settings:

1. On the **Admin** page, select *Configuration* in the upper-left corner.
2. Select *Advanced* under *System Settings* in the filtering sidebar.

The following table shows a description of the currently available settings.

System Setting	Description
SSL	
SSL Certificate policy	Determines the SSL Certificate policy applied to the Cloud Integration feature and update checks.
Path to SSL Certificate Authority file or directory	Specifies the path to the SSL Root certificate used by the SSL Certificate policy.
SOA record defaults in new zones	
TTL of SOA record	Specifies the default TTL (Time to Live) value to use for the SOA record of new zones.
Hostmaster	Specifies the default value to use for the Hostmaster field in the SOA record of new zones.
Refresch	Specifies the default value to use for the Refresh field in the SOA record of new zones.
Retry	Specifies the default value to use for the Retry field in the SOA record of new zones.
Expire	Specifies the default value to use for the Expiry field in the SOA record of new zones.
Negative caching (BIND)	Specifies the default value to use for the Negative Caching field in the SOA record of new zones. Only applicable for zones on BIND DNS servers.
Minimum TTL (MS)	Specifies the default TTL (Time to Live) value to use for the TTL field in the SOA record of new zones. Only applicable for zones on Microsoft DNS servers.
Web proxy	
Web proxy to use	Specifies a proxy server to be used for outgoing connections for checking for updates and additionally for AWS cloud services.
Web proxy port (defaults to port 80)	Specifies the port of the proxy server to be used for outgoing connections for checking for updates and additionally for AWS cloud services.
Password for web proxy authentication	Specifies a cleartext password for proxy sign in.
Use web proxy settings when connecting to AWS	If selected, the proxy settings configured will be used for connections to AWS.
Directory for scripts that can be run from the API	Specifies the directory that contains scripts that may be run from the API.
Log performance of API calls	Determines whether execution time of API calls should be logged. Mainly used for diagnostic purposes.
Time in minutes between write-outs of API call performance log	If logging of API query performance is enabled, this setting specifies how frequently the log should be written to disk.

continues on next page

Table 6 – continued from previous page

System Setting	Description
Automatically adjust local zone transfer settings for BIND	When enabled, BIND can automatically optimize the settings related to local (within your network) zone transfers.
Automatically create reverse (PTR) records	When selected, Micetro automatically creates reverse (PTR) records. PTR records are used for reverse DNS lookups, which are used to resolve an IP address to a domain name.
Perform backup of MS and ISC DHCP servers	Determines whether to perform a backup of Microsoft (MS) and Internet Systems Consortioum (ISC) Dynamic Host Configuration Protocol (DHCP) servers.
Default TTL to use for DNS records created in zones for all xDNS profiles	Specifies the default TTL (Time to Live) value to use for DNS records created in zones for all xDNS profiles.
Disable all health checks	If selected, all health checks will be disabled.
Disable collection of statistical information	Select to stop the collection of statistical information.
Use Azure activity log to optimize DNS synchronization	When enabled, the Azure activity log is monitored for events related to DNS changes, and those changes are synchronized with the DNS server in real-time.
Use AWS CloudTrail events to optimize DNS synchronization	Determines whether AWS CloudTrail events should be used to optimize DNS synchronization.
IP ranges/scopes inherit access by default	When you create a new IP range or scope, it will ineherit all access bits form its parent by default. If you want to change this behavior, clear this checkbox.
Maximum number of blocks that can be temporarily claimed	Limits the number of blocks that can be temporarily reserved or allocated for use by a specific user.
Enable collection of IP information from routers	Determines whether the system can collect IP information from the ARP cache of routers. If selected, the system can collect this information.
Timeout in seconds for named-checkconf	Specifies the timeout value in seconds for named-checkonf files.
Synchronize DNSSEC signed zones immediately after editing	Determines whether DNSSEC signed zones should be synchronized immediately after they are changed. If selected, the zones are synchronized immediately.[1]
Use case sensitive comparison when updating custom properties from scripts	Specifies whether to take case sensitivity into account when comparing custom properties from scripts.
Include A/AAAA records when checking for *Edit apex records* access	Determines whether A and AAAA records are considered when verifying access to edit apex (root) records.
Web app landing page	By default, the Micetro frontpage is the landing page for the system. Clicking the Micetro logo will take you to the landing page.
Web app server host	Used to specify which host the web application is running on in order for auto update to work for the web application. Default is localhost (same server as Men&Mice Central)

[1] Enabling this feature can affect the performance of the system.

1.7.2 Configure High Availability for Micetro Central

Failover instances of Men&Mice Central can be configured to build a high availability cluster.

Note: To run Micetro in High Availability mode you must be using the MSSQL or PostgreSQL database backend for Micetro. High Availability mode is not available for other database types.

Note: When there are no HA members defined or if Micetro Central has not been configured for HA, a message will appear indicating further configuration is necessary. This documentation shows how to configure HA in the web UI for versions 10.2 and above. If you need to use the management console (thick client), please follow the documentation in [10.1](https://menandmice.com/docs/10.1/guides/implementation/central_ha)

Note: For fine-tuning the settings for the Central High Availability cluster, see *Men&Mice Central HA tweaks*.

Linux

1. On the existing (or designated as *primary*) server running Central, edit the preferences file in `/var/mmsuite/mmcentral/preferences.cfg`, adding

```
<ClusterMemberName value="somename"/>
```

to the end of the file. `somename` is the unique name that will identify the Central instance in the high availability cluster. (E.g. "1", "primary", or "central1")

2. Restart the primary Central application:

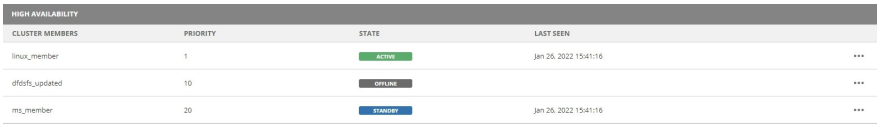
```
systemctl restart mmcentral
```

3. Login to the web UI as "administrator" and go to *Admin* then *Configuration*
4. Select *High Availability*
5. Type in the name of the first member server to match the name given earlier and set the priority to **10**
6. Click *Add Member*

7. Restart Central:

```
systemctl restart mmcentral
```

8. Login to the web UI and verify that the current server is running with state "Active"
9. Repeat steps 3-6 to add another member to the HA configuration, but now use a priority of **20** or higher



10. On the just added secondary server, install the Micetro Central application. If it's already installed, make sure it's stopped by using (as root):

```
systemctl stop mmcentral
systemctl status mmcentral
```

11. Copy the `/var/mmsuite/mmcentral/preferences.cfg` file from the first server to the second, and change the `ClusterMemberName` value to match the one set up previously. Save the file and exit.
12. Start Central on the secondary server:

```
systemctl start mmcentral
```

13. Verify that you now have 2 servers, one primary, one secondary in the HA cluster
14. Create a round robin DNS name for the high availability setup, i.e. two A records with the same name, but each with the IP address of the primary and secondary server respectively.

Note: Repeat these steps for each high availability failover you'd like to add. The priority for each failover member should be unique and higher than the primary.

Proceed to *Micetro Agents*.

Windows

1. In the existing (or designated as *primary*) server running Central, edit the preferences file `preferences.cfg`, adding

```
<ClusterMemberName value="somename"/>
```

to the end of the file. `somename` is the unique name that will identify the Central instance in the high availability cluster. (E.g. "1", "primary", or "central1")

2. Restart the primary Central application from the command line:

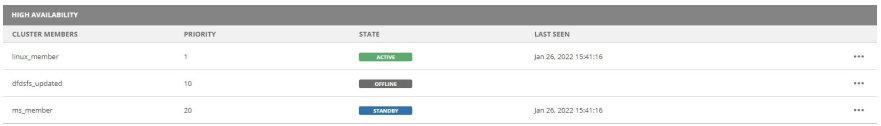
```
mmcentral -stop
mmcentral -start
```

3. Login to the web UI as "administrator" and go to *Admin* then *Configuration*
4. Select *High Availability*
5. Type in the name of the first member server to match the name given earlier and set the priority to **10**
6. Click *Add Member*

7. Restart the Central application from the command line:

```
mmcentral -stop
mmcentral -start
```

8. Login to the web UI and verify that the current server is running with state "Active"
9. Repeat steps 3-6 to add another member to the HA configuration, but now use a priority of **20** or higher



10. On the just added secondary server, install the Micetro Central application. If it's already installed, make sure it's stopped:

```
mmcentral -stop
```

11. Copy the `/var/mmsuite/mmcentral/preferences.cfg` file from the first server to the second, and change the `ClusterMemberName` value to match the one set up previously. Save the file and exit.
12. Start Central on the secondary server:

```
mmcentral -start
```

13. Verify that you now have 2 servers, one primary, one secondary in *Tools → Manage High availability*.
14. Create a round robin DNS name for the high availability setup, i.e. two A records with the same name, but each with the IP address of the primary and secondary server respectively.

Note: Repeat these steps for each high availability failover you'd like to add. The priority for each failover member should be unique and higher than the primary.

Editing HA member options

1. Log in to the web UI and go to *Admin* then *Configuration*
2. Click on *High Availability*
3. Hover over the server member and click on the ellipsis (or meatball) menu
4. There are three options:

Edit Member
: Change the name or priority of the server member in the HA cluster

Set Active
: Set the server to be the Active member of the HA cluster manually

Remove Member
: Remove the server member from the HA cluster

Proceed to *Micetro Agents*.

Updating Central in High Availability setup

Warning: The Automatic Update feature cannot be used when the Central service is in High Availability setup

The procedure for updating the Central servers in High Availability is as follows:

1. Turn off the Central service on each secondary server
2. Upgrade the primary server manually using an installer. An installer can be downloaded from https://download.menandmice.com/

3. Upgrade each secondary server manually using an installer. After the upgrade finished successfully, the service will be started again.
4. Now, both servers should be upgraded and again in High Availability mode.

1.7.3 Men&Mice Central HA tweaks

Changing the default heartbeat timestamp value in Central HA

The local time of the cluster member machines are used to update the heartbeat timestamp in the database. It's crucial that the cluster member machines have a synchronized time.

By default the Central instances update the heartbeat timestamp in the database every 10 seconds, as set in the `/var/mmsuite/mmcentral/preferences.cfg file`:

```
<HeartbeatInterval value="10" />
```

This can be tweaked between values of **5** and **15**.

When a Central instance stops to write the heartbeat timestamp to the DB the *HeartbeatMaxAllowedDowntime* value is used to determine if a failover is done to the next valid Central in the list. (Valid meaning, in this case, that the next Central application is a HA cluster member and is writing its heartbeat timestamp to the database.)

The default maximum downtime is set for 30 seconds. When the current time [UTC – heartbeat timestamp UTC] > [HeartbeatMaxAllowedDowntime] an automatic failover is triggered.

The default maximum downtime can be overwritten in the `/var/mmsuite/mmcentral/preferences.cfg` for each Central instance:

```
<HeartbeatMaxAllowedDowntime value="30" />
```

Values between **20** and **120** are allowed, setting the maximum downtime to 20-120 seconds.

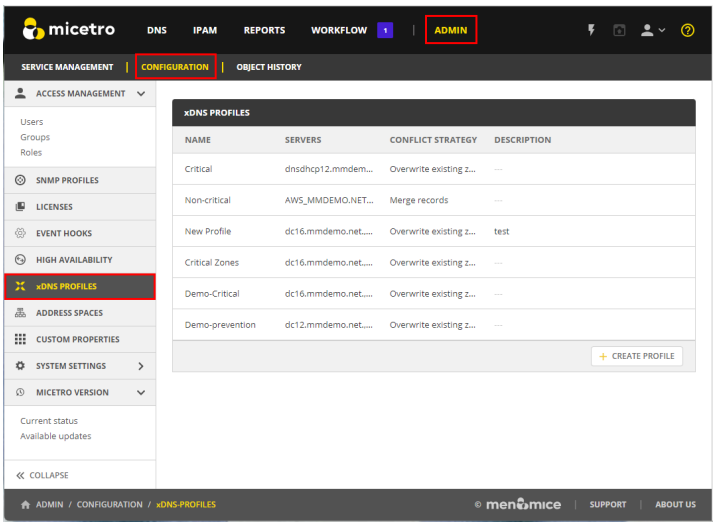
1.7.4 xDNS Redundancy

The xDNS (Cross-Domain Name System) redundancy feature helps ensure the availability and reliability of your DNS infrastructure. It allows you to create backup DNS configurations, so if one DNS server or service fails, another can seamlessly take over, ensuring uninterrupted access to your websites or services.

- **Creating Redundancy Groups**: With xDNS profiles, you can create groups that consist of multiple DNS servers and services. These groups are designed to manage the authority of a specific list of DNS zones.
- **Identical Zone Content**: Once you've set up an xDNS redundancy group, the system assists you in generating identical copies of the DNS zone content across multiple primary zones. This replication ensures that all zones within the group are the same in every aspect.
- **Flexibility**: As your needs evelove, you can add or romeve zones from the xDNS profile.

To access xDNS Profiles:

1. Go to the **Admin** page.
2. Select *Configuration* in the upper-left corner.
3. Select *xDNS Profiles* in the filtering sidebar on the left-hand side.



xDNS Profiles

xDNS Profiles group together two or more DNS services that share the the authority of a list of zones. Any changes made to these zones, within or outside of Micetro, are automatically synchronized across all DNS services within the profile. In case of conflicts, Micetro has a built-in conflict resolution strategy to handle them.

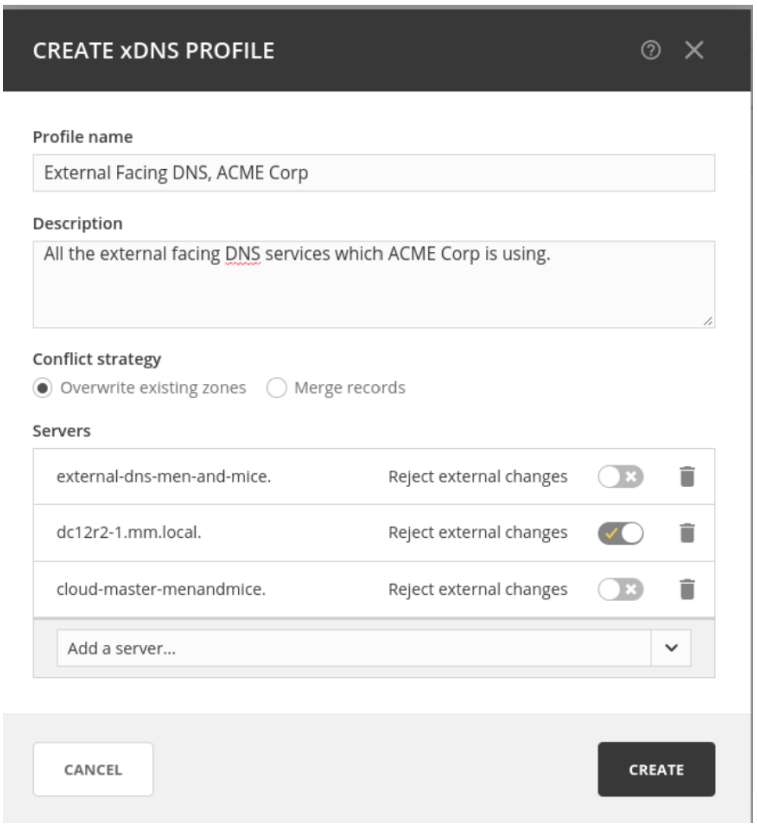
Creating/Modifying xDNS Profiles

To create or edit an xDNS profile, you must have administrative access within Micetro to the DNS Services you want to include.

- To **create** a new profile, click *Create Profile* in the lower-rigt corner of the xDNS Profiles list.
- To **edit** a profile, select the relevant profile, and then select *Edit profile* on the **Row menu (…)**. You can also double-click the profile.

Each profile has the following properties:

- **Name**: A unique identifier for the profile.
- **Description**: An optional field to describe the purpose of the xDNS profile.
- **Conflict Strategy**: Determines whether Micetro overwrites or merges record conflicts that may arise during synchronization. This also serves as the default when adding new zones to the profile.
  - **Overwrite existing zones**: If a zone with the same name exists on any other DNS service included in the xDNS profile, its records will be overwritten with the record data from the zone instance being added to the xDNS profile.
  - **Merge records**: If a zone with the same name exists on any secondary service, its contents will be merged with the contents of the zone on the primary service.
- **Servers**: At least two DNS services must be added to the profile. Each service can also be configured to reject external changes. This means changes to record data made on one service outside of Micetro will not be replicated by xDNS to other services.



Note: The list of servers **cannot** be changed after the profile has been created

Configuring TTL for DNS Records in xDNS Profiles

You can specify the default Time-to-Live (TTL) for DNS records created within zones for all xDNS profiles. This setting determines how long DNS information remains cached by DNS resolvers before requesting updated data.

1. Go to the **Admin** page.
2. Select *Configuration* in the upper left corner.
3. Under **System Settings** in the filtering sidebar, select *Advanced*.
4. Enter your desired TTL value in the appropriate text box.

Deleting xDNS Profiles

To delete an xDNS profile, you must have administrative access within Micetro to all DNS services within the profile.

When an xDNS profile is deleted, each service retains a copy of the zones from the profile, but replication between them will stop.

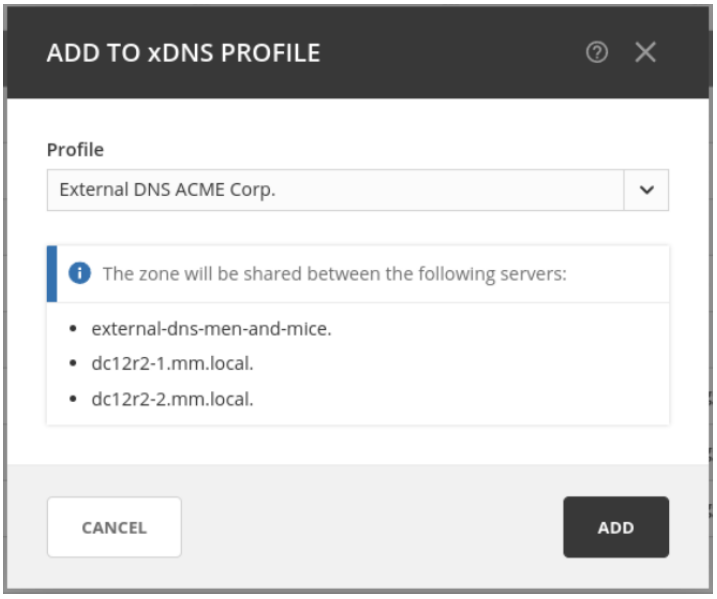
- To delete a profile, select the relevant profile, and then select *Delete profile* on the **Row menu (...)**. You can also double-click the profile.

Adding Zones to xDNS Profiles

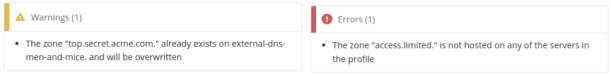
To add a DNS zone to an xDNS profile, you must have “create zone access” on all DNS services included in the xDNS profile. xDNS profiles initially do not include any zones.

To add zones to xDNS profiles>

1. Go to the **DNS** page.
2. In the filtering sidebar, select *Primary Zones*, if not already selected. xDNS only supports primary zones.
3. On the *Actions* menu, select *Add to xDNS profile*. You can also select this option on the **Row menu (…)**.



- When a profile is selected on the *Profile* menu, Micetro runs preflight checks and displays any warnings or potential errors that are detected.



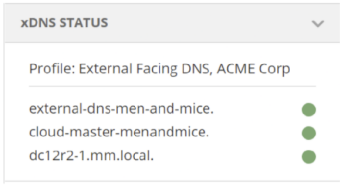
Adding a zone to xDNS will, if necessary, create zone instances on other DNS services included in the selected profile and add delegation records. Afterward, other record data from the source zone will be replicated to the newly created zone instances.

The overview grid for DNS zones will display only one instance, with the authority column showing the name of the profile to which the zone has been added.

xDNS Status on Zones

You can monitor the status of xDNS zones in the inspector. Each underlying zone instance is represented by the name of the DNS service and a traffic light indicator.

In sync	Zone is in sync with other zones in the xDNS zone group.
Out of sync	Zone is out of sync and will be updated when possible
Offline	The server hosting the zone is not available
Missing	The zone has disappeared off the server



Multiselecting is supported if all xDNS zones belong to the same profile, with each entry showing the aggregate state of the zone instances on each DNS service. If zones from multiple profiles are selected, the xDNS status section will be hidden.

Removing Zones from xDNS Profiles

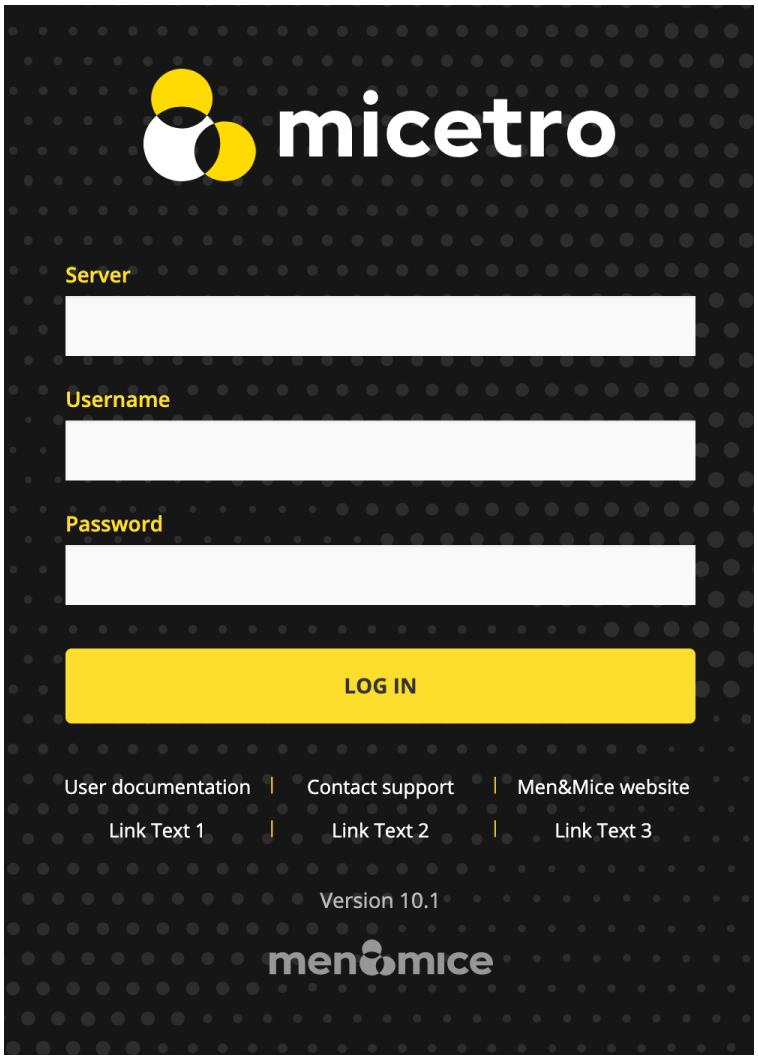
Removing a zone stops all replication between zone instances on each DNS service. Delegation remains unchanged, and no zone instances are deleted.

xDNS zones and the API

xDNS zones are represented as single instances in the API, with the Authority value denoting the profile they belong to. Individual zone instances remain accessible, for example by calling GetDNSZones and filtering for each DNS service via the dnsServerRef parameter.

1.7.5 Custom links in the web application

You can add up to three custom links that show up on the Micetro login page.



To add your custom links (for example internal support channel):

1. Open the `preferences.cfg` file for Men&Mice Web Services.
   - Default location on Windows: `C:\ProgramData\Men and Mice\Web Services\preferences.cfg`
   - Default location on Linux: `/var/mmsuite/web_services/preferences.cfg`
2. To the end of the file, add the links in the following format:

```
<LoginFootnote value="Link Text 1[https://www.example.com/link1],Link Text 2[https://www.
↪example.com/link2],Link Text 3[https://www.example.com/link3]" />
```

3. Restart the MMWS service to pick up the changes:
   - On Windows: `mmws.exe`
   - On Linux:

```
systemctl restart mmws
```

Note: The MMWS service always needs to be restarted after changes to its preferences file.

1.8 Update Guide

Note: These instructions apply to the Micetro web interface. For information about update management in the M&M Management Console, see *Update Guide - Management Console (obsolete)*.

Permissions:

- **Permission**: None (cannot create a custom role to access this)
- **Role**: `Administrators (built-in)`

1.8.1 Micetro Version

Micetro notifies you when a new version becomes available and allows administrators to update to a new version. Versions may contain updates for any number of components, such as Men&Mice Central and the Men&Mice Server Controllers.

- Minor versions often only contain an update for a single component, such as the Micetro Appliances.
- Major version upgrades normally contain an update for every component.

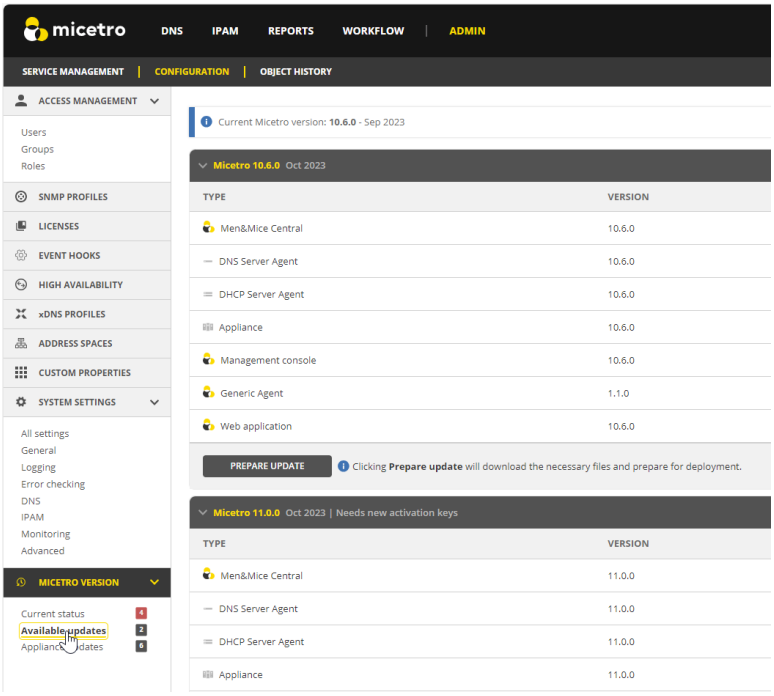
Note: To receive notifications and check for updates, you must be in a group with administrative privileges. Only the Administrator user can perform the actual update.

1.8.2 Updating Micetro

Before updating Micetro, we strongly recommend reading the Release Notes first, see *Release Notes*.

To apply an update:

1. Select *Admin* on the top navigation bar.
2. Select the *Configuration* tab at the top of the admin workspace.
3. Find available updates under *Micetro Version* in the left sidebar.



Preparing the Update

To streamline the updating process, the update is prepared by making sure that update packages are uploaded to the various comopnents before the update is actually deployed.

To prepare an update:

1. Select *Prepare Update* to start the update process.
2. A package for the new version is downloaded and prepared for deployment. This includes uploading a package to each DNS and DHCP server, as well as each appliance, if the new update package includes an update for them.

Deploying the Update

Once the package has been prepared, select *Deploy Update* to deploy the new version.

If the new version includes an updated Central component, it will restart. Otherwise, Micetro seamlessly updates to the new version.

After the update has been deployed, each Micetro component requiring an upgrade is upgraded to the latest version. The update packages that were uploaded during the preparation phase are put into place.

Update Paths

If you're updating Micetro from an older version, refer to the following table:

Origin version	Target version	Update to
9.x	10.x	10.x[1]
8.x	10.x	10.x[Page 112, 1]
7.x	10.x	10.x[1]
6.x	10.x	9.3

1.8.3 Checking the Status of Micetro Components and Appliances

You can see the status of all components at a quick glance so you know everything is up and running smoothly.

To check the current status of Micetro components and appliances:

1. Go to the *Configuration* tab on the **Admin** page.
2. Select *Current status* under *Micetro Version* in the left sidebar.
3. You will see a list of all components, their current version, and status.

Troubleshooting

The *Status* column will highlight if there is an error with the component, or if it is offline. Hover over the Offline or Error status for more details to help you troubleshoot.

1.8.4 Updating Appliances

Appliance updates shows if any Appliances have updates pending. There are three types of updates:

- **Full**: Full updates are the most extensive and involve replacing the entire appliance, typically with the release of a new major version. These updates are versioned and around 700MB in size.
- **Minor**: Minor updates consist of version upgrades, such as 9.4.1, and typically include minor improvements or enhancements. They are executed in the same way as full upgrades, using partition swap. For example, the 9.4.2 update includes all changes made in 9.4.1, so it's okay to go directly from 9.4.0 to 9.4.2. However, for customers with older appliance versions prior to 9.4, it's necessary to first install the 9.4.0 full upgrade before deploying 9.4.1 or 9.4.2. These updates are around 2-300MB in size.
- **Patch**: Patch updates are minor adjustments to individual components, such as BIND or ISC DHCP. They address specific issues or vulnerabilities.

[1] Kea DHCP servers must be updated to 1.6.0 or 1.8.0 *before* updating Micetro to 10.x. See Kea update notice.

Update Status

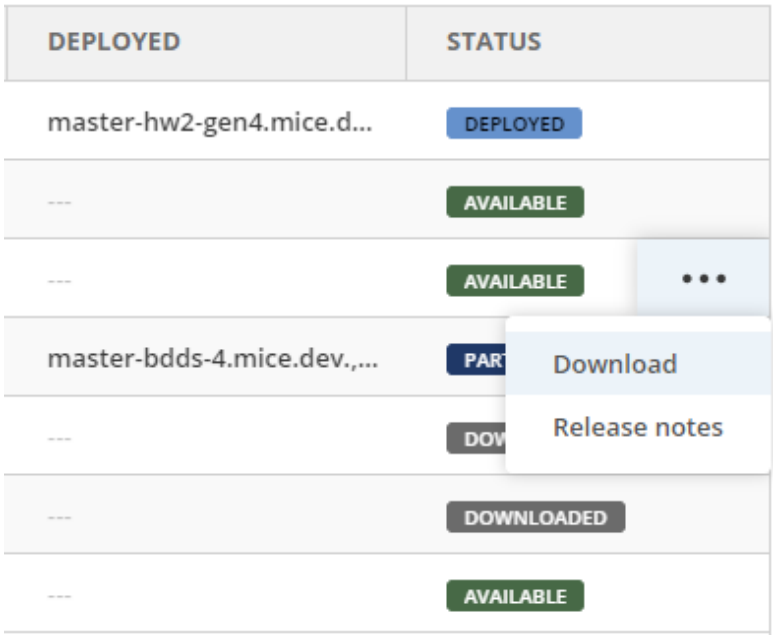
The update process involves downloading and deploying updates, which are reflected in the *Status* column.

- **Available**: Updates are ready for application but have not been downloaded yet.
- **Deployed**: Updates have been applied and fully deployed.
- **Partially deployed**: Updates have been downloaded but not applied to every applicable appliance in the system.
- **Downloaded**: Similar to **Partially deployed**, but updates have not been applied to any appliance in the system.
- **Downloading**: This is a temporary state indicating that the patch or upgrade is currently being downloaded.

Note: It is recommended to update individual appliances one at a time to avoid simultaneous downtime for all appliances.

To update an appliance:

1. Go to the *Configuration* tab on the **Admin** page.
2. Select *Appliance updates* under *Micetro Version* in the left sidebar.
3. On the Row menu ... for the relevant update, select *Download*.



4. Once the download is complete, the update status becomes *Downloaded*. Initiate the update process by selecting *Deploy* on the Row menu.

1.8.5 Update Management in the Management Console

For information about how to update in the M&M Management Console, see:

Update Guide - Management Console (obsolete)

The Update Manager notifies you when a new version of Micetro is available and simplifies the update process for Micetro. Using the Update Manager you can update Men&Mice Central, the Men&Mice Server Controllers and the Men&Mice Appliances with minimal downtime.

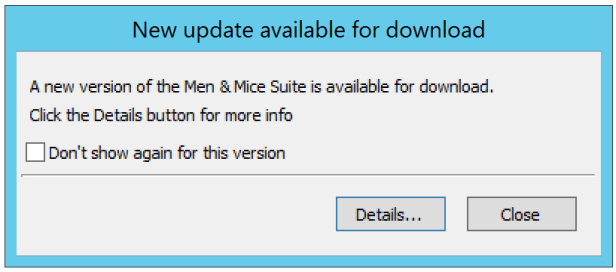
Update paths

If you're updating Micetro from an older version, refer to the following table:

Origin version	Target version	Update to
9.x	10.x	10.x[1]
8.x	10.x	10.x[Page 114, 1]
7.x	10.x	10.x[1]
6.x	10.x	9.3

Checking and Downloading an Update

When you log into the system using the Management Console, an update notification is displayed when a new version of Micetro is available.



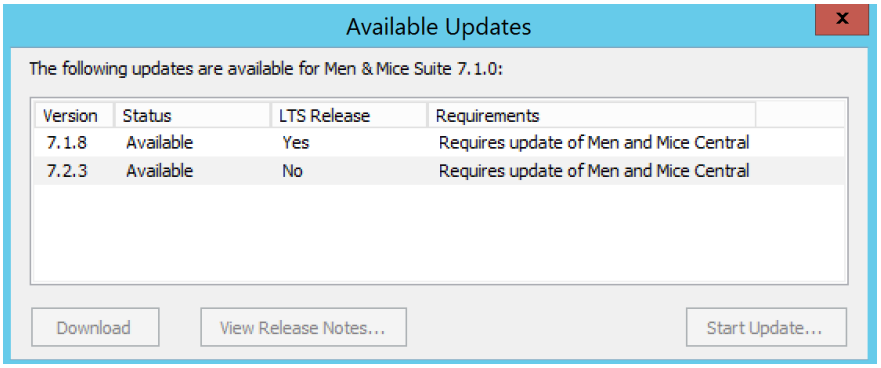
You can also check if an update is available by selecting *Tools* → *Check for Updates*.

Note: To receive update notifications and check for updates, you must be in a group with administration privileges. Only the Administrator user can perform the actual update.

If you are not interested in receiving notifications for the update, select the *Don't show again for this version* checkbox. When the checkbox is checked, a notification for the specific update is no longer displayed, however, if a later update becomes available, the dialog box is displayed again.

Click the Details button to get more information on the update. This displays a dialog box that shows all available updates.

[1] Kea DHCP servers need to be updated to 1.6.0 or 1.8.0 *before* updating Micetro to 10.x. See Kea update notice.



To view the release notes for an update, select the corresponding update and then click the *View Release Notes* button. This will show the release notes in a web browser.

To download the new version, select the version and click the *Download* button. The new version is downloaded and stored on the Men&Mice Central server. Once the download has completed, you can start the update.

Note: To download and perform the actual update you must be logged in as Administrator. If you are not logged in as Administrator, the Download button is disabled.

Installing an Update

Once the update has been downloaded, you can start the actual update process. The Update Manager can update Men&Mice Central, connected Server Controllers and Men&Mice Virtual Appliances. The Men&Mice Web Application must be updated manually.

If you want to perform the update at a later time, you can close the dialog box. To display the dialog box again, select *Tools → Check for Updates*.

The following instructions contain information on how to update Micetro after the update has been downloaded using the Update Manager.

1. To start the update process, click the *Start Update* button in the update details dialog box. When you click *Start Update* the following happens:

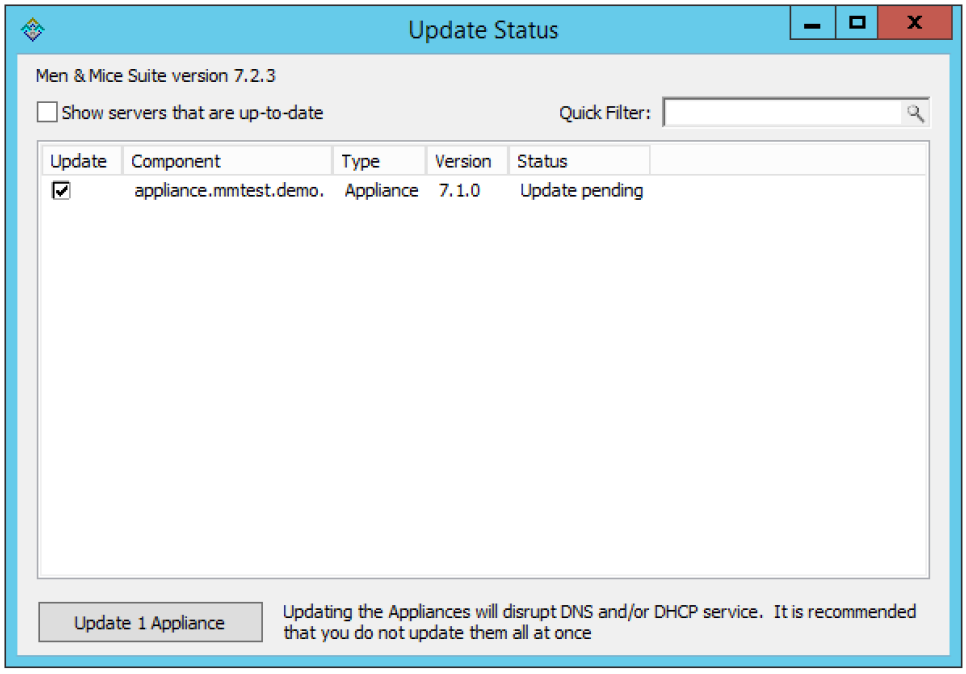
- Men&Mice Central and the DNS and DHCP server controllers are updated. (See *Updating Central in High Availability setup* for updating Central in HA configuration.)
- If the update contains a new version of the Men&Mice Web Application, a dialog box is displayed where you can find instructions on manually updating the Men&Mice Web Application.
- If your environment contains a Men&Mice Appliance, the latest version of the Men&Mice Appliance software is uploaded to the Appliance, but isn't applied automatically.

Updating an Appliance

As an update to the Men&Mice Appliance sometimes requires that the Appliance is restarted, the update is not applied automatically.

To complete an Appliance update, you must manually initiate the update. To minimize service disruption you might want to update your Appliances in several batches.

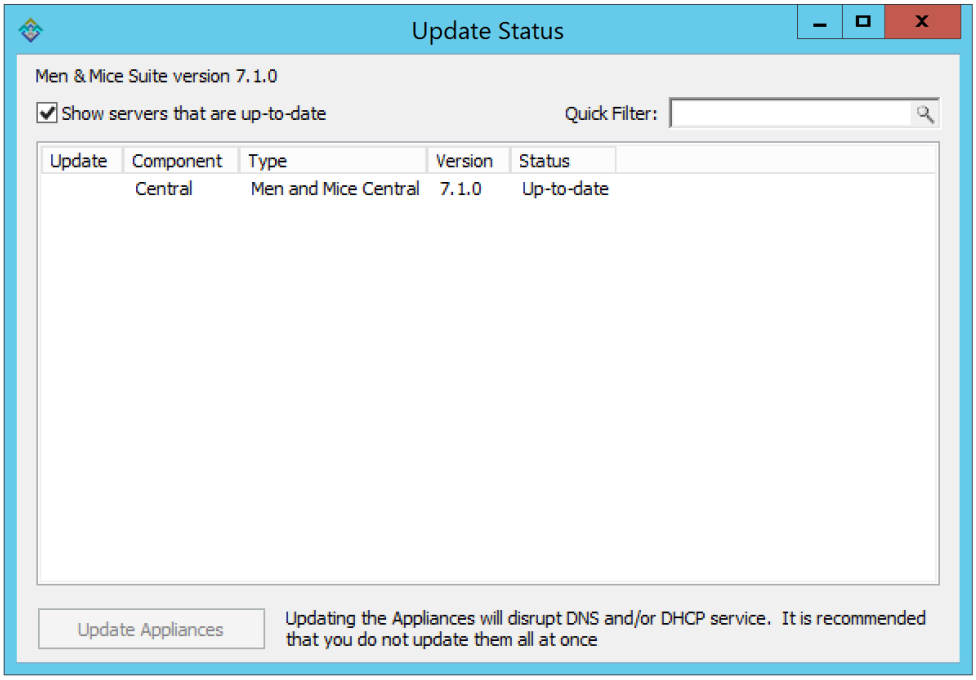
1. From the menu bar, select *Tools* → *Update Status*. The *Update Status* dialog box displays. The dialog box shows the update status for all DNS and DHCP server controllers as well as all Men&Mice Appliances. If an update is pending for an Appliance, the status is listed as *Update pending* and a checkbox is displayed in the Update column.



2. Click the checkbox to select the Appliance(s) you want to update.
3. Click the *Update Appliances* button. This will update the selected appliance(s).

Viewing Update Status

Through the *Update Status* dialog box, you can always view the update status for Micetro components. To display the Update Status dialog box, select *Tools* → *Update Status*.



The dialog box shows the update status for all DNS and DHCP server controllers as well as all Men&Mice Appliances. If an update is pending for an Appliance, the status is listed as Update pending and a checkbox is displayed in the Update column.

Uncheck the *Show servers that are up-to-date* checkbox to only show servers that need to be updated.

Note: The Auto Updater will update *all* connected server controllers along with Central.

Note: If some Controllers can't be updated automatically please check if the M&M Updater daemon or Windows service is running on the server and if the port 4603/tcp is accessible from the machine that runs Central. See *Networking requirements* for more information.

Warning: When Central is in a high availability configuration, the Auto Updater cannot be used. See *Updating Central in High Availability setup* for instructions.

Verifying the updates

In order to verify that the update has propagated to all servers:

1. Log in to the Management Console
2. Navigate to *Tools* → *Update Status*
3. Review the version reported for each of the listed components. The listed version number for Micetro is listed near the top, and should match the version of each component in the list.
4. Log in to the Web Application, click on the *User* icon in the top menu. Verify that the version listed there matches the version of the Men&Mice Central that was installed.

Note: If there's a version mismatch between components, the Management Console and Web Application will report an error when trying to log in.

1.9 Using Micetro

The application is split into 5 main sections:

- **DNS**. On the *DNS* page, you can create, delete, and edit DNS zones. Here you also manage DNS records within the DNS zones.
- **IPAM**. On the *IPAM* page, you have the ability to perform various actions related to network and DHCP management, such as creating a new network range or DHCP scope, managing IP addresses within a network or DHCP scope and creating DHCP reserverations. You can also view related DNS data for IP addresses within a network and add DNS hosts for IP addresses.
- **Reports**. The *Reports Management* is activated with a separate license key and there you can create and save new reporting definitions, as well as schedule reports to be run at specific times.
- **Workflow**. The *Workflow Management* requires a separate license key. The module allows you to submit 'change requests' for creating, modifying, or deleting DNS records.
- **Admin**. The Admin page is the workspace for system administrators where they perform the various tasks to manage Micetro, such as managing user access and services.

Note: The Internet Explorer browser is no longer supported as of version 9.3.0.

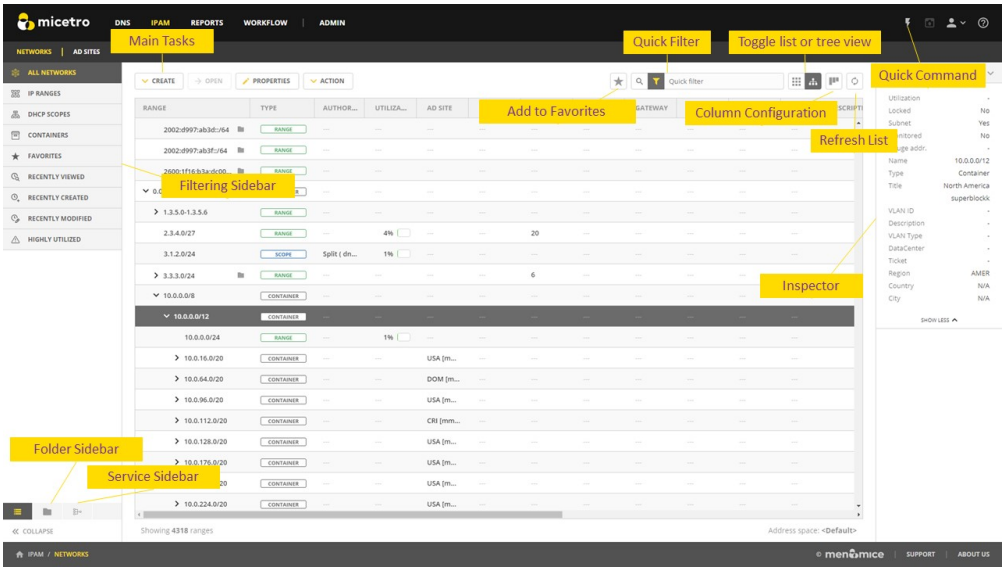
1.9.1 Getting Help or Support

Information about how to get help and access the documentation can be found in the right sidebar on the front page.

You can also access the help sidebar by clicking the *?* icon in the top menu on all pages.

1.9.2 Working with the List View

Micetro is centered around the grid listing objects in the system, such as DNS zones, DNS records, IP address ranges, DHCP scopes, and IP addresses.



Item	Description
Refresh list	Refreshes the list containing a list of zones, ranges, records, or IP addresses
Column configuration	Specifies which columns are visible in the list
Quickfilter	Narrows down the results shown in the list after having selected an item in the filtering sidebar. webapp-quick-filter
Toggle list or tree view	Toggles the list between list and tree view
Refresh list	Refreshes the contents of the list
Add to favorites	Adds the selected item in the list to favorites. The corresponding favorites filter in the sidebar shows all favorited items
Main tasks	The main tasks in each section.
Inspector	Shows various information for the selected item in the list. See webapp-inspector.
Filtering sidebar	Shows a list of possible filters to use for the list. See webapp-filtering.
Quick command	Allows for quickly finding and performing actions. See webapp-quick-command.

1.9.3 Filtering Sidebar

The left-hand filtering sidebar acts as a selector in each context, and helps you to quickly find the zones or networks. You can select pre-defined “filters” or selectors.

By default, the sidebar is open, but you can collapse it to an icon-only mode. In case where a list of clickable items is needed, the sidebar is automatically unfolded.

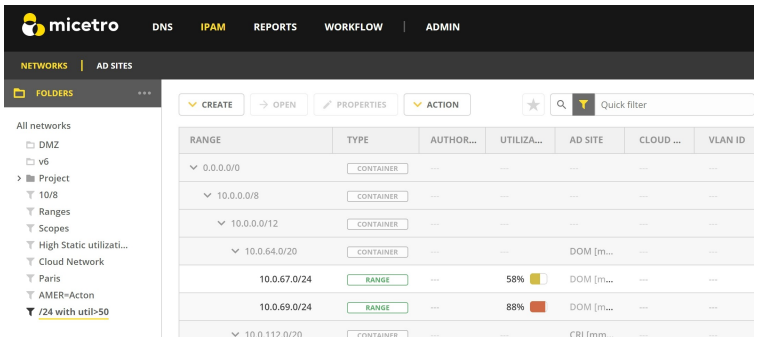
Selecting an item in the filtering sidebar applies the filter for the main work grid. You can further narrow down results with quickfilters from the top menu. (See Quickfilter.)

Tip: When you select a filter in the filtering sidebar, and then select the *Create* operation in the grid, the type of object will be automatically selected based on the active filter.

Folders

You can use folders as containers of objects such as DNS zones and networks.

The available folders, along with the folder hierarchy, can be viewed in the filtering sidebar. Click a folder to display the contents of that folder.



Selecting an item in the list, and then selecting *Add to folder* on the *Action* menu, opens a dialog box where you can move the item from one folder to another, or remove ir from a folder.

1.9.4 The Inspector

The inspector, located to the right of the grid in each context, serves as an infobox for the selected objects, such as the DNS zone list. In some cases it is possible to edit the information, such as DNS zone authority, or the SOA record for each zone.

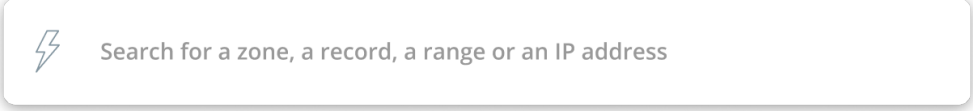
All properties for the selected object are shown in the properties section. These include all custom properties that have been defined for a specific object type.

For IP addresses, where available, the vendor for the specific MAC address is also shown.

1.9.5 Searching by Using the Quick Command

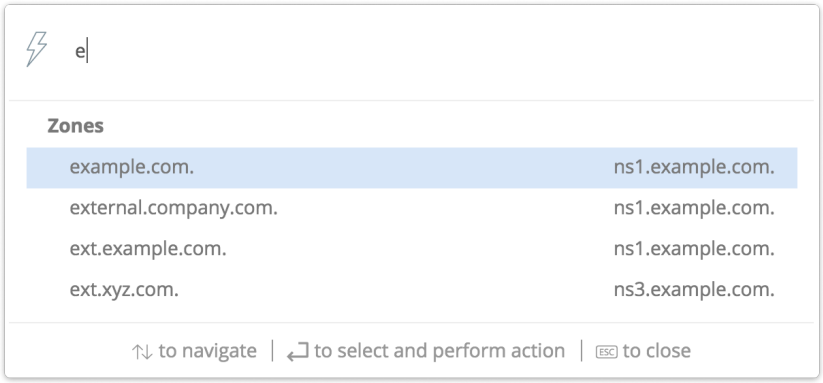
Quick command speeds up common operations in Micetro and helps you quickly find and perform actions on specific objects in the system.

Access quick command by clicking either the lightning icon in the upper-right corner or by using a keyboard shortcut: **Ctrl** + **Space**.

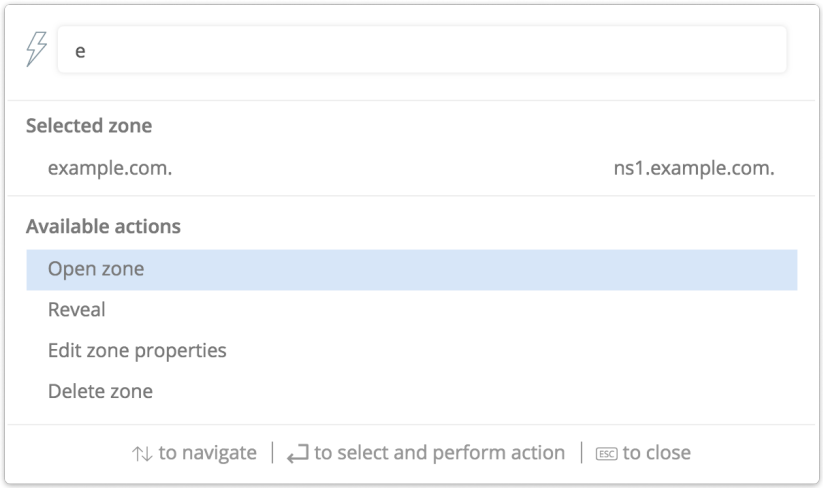


1. Start typing in one of the following:
   - A network
   - A DNS zone name
   - A DNS record name
   - An IP address

   A list of potential results will be displayed:



2. Select the object to work with.
3. Select the action to perform on the object.



1.9.6 Quickfilter

Note: Quicksearch

You can toggle the Quickfilter to Quicksearch. Quicksearch will only highlight matching objects in the grid, but still display all other entries as well.

The Quickfilter can be accessed in all sections that use a list of items, for example, in the DNS zone list in the DNS section.

The Quickfilter helps you narrow down the results displayed after having selected an item in the filtering sidebar. Alternatively, it can be used solely by specifying columns and values for each column to be filtered by.

The Quickfilter can be used as a free text search by simply entering some string into the field. The value is compared to all rows that have columns containing the given string.

You can also provide the name of the column, a condition operator, and the queried string.

```
type=slave
name=^example
name=$arpa.
```

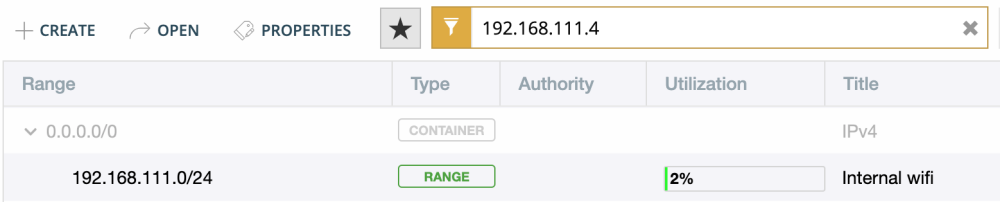
Conditional Operators

Operator		Opposite operator	
=, ==	is equal	!=	is not equal
>, >=	larger than, larger than or equal	<, <=	smaller than, smaller than or equal
=@	contains	!@	does not contain
=^	starts with	!^	does not start with
=$	ends with	!$	does not end with
=~	matches regular expression	!~	does not match regular expression
in(...)	is equal to one of the values in the given list	not in(...)	does not match any of the values in the given list

Two or more conditions can be combined using *and*, *or*, and *()* parenthesis.

Note: Date and time values as well as MAC addresses need to be enclosed in quotes when using the quickfilter.

On the **IPAM** page, one way of finding the network containing a specific IP address is typing the full IP address into the quickfilter.



1.10 DNS

Micetro's access control system provides granular control over who can access DNS information. The system includes the following built-in roles that provide varying levels of access to the DNS page.

- **DNS Administrators**
- **DNS viewers** (allows viewing of DNS information)

To grant other roles access to DNS information, make sure that they include the following permissions:

- **Access DNS module**
- **List (or view) DNS server**
- **List (or view) zone**

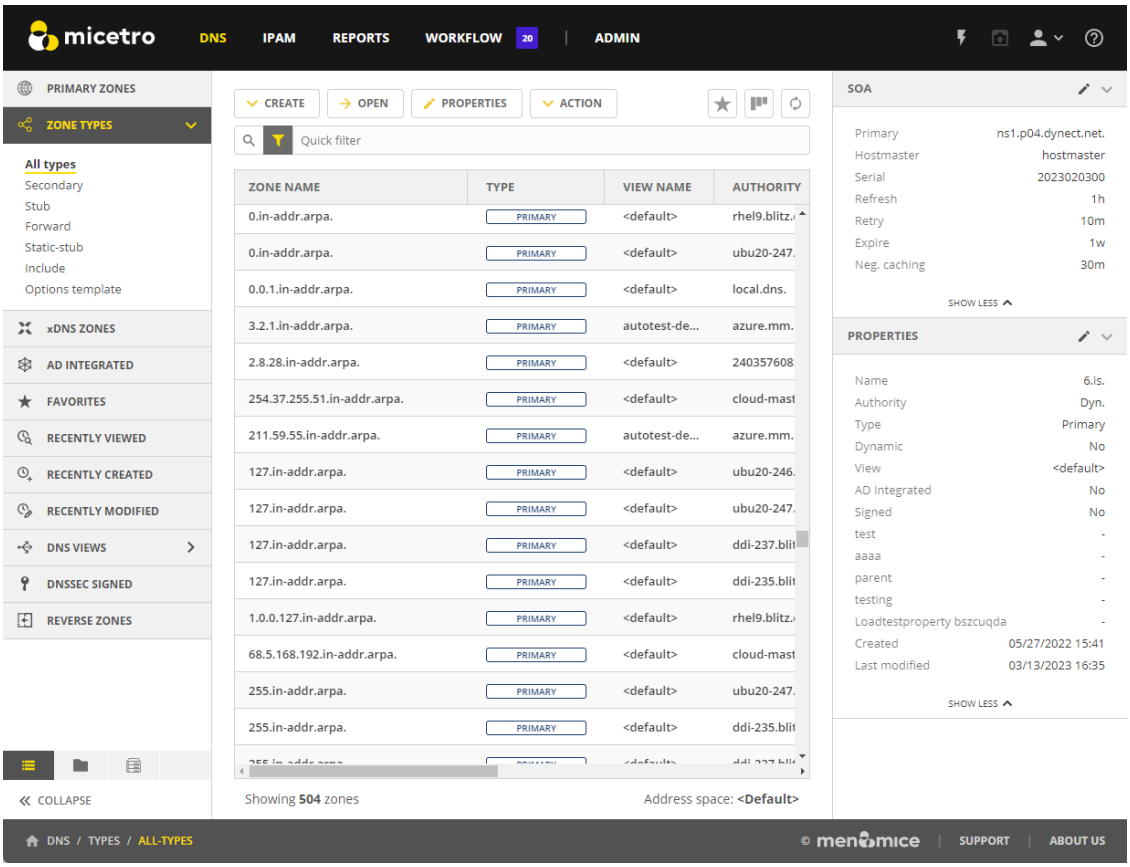
Note: To fully manage zones, additional permissions may be required, and specific access might be defined on individual zones.

1.10.1 DNS Zones

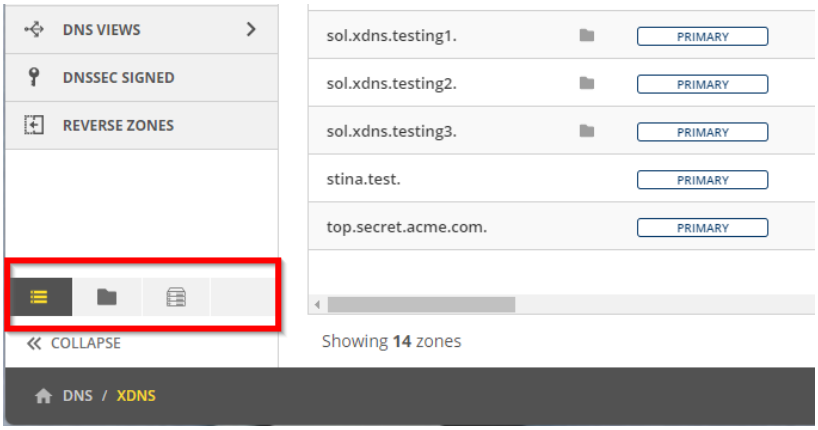
Note: This information applies to the web interface. For information about DNS zone management in the M&M Management Console, see *DNS Zones - (Management Console)*.

Overview

By default, the DNS page displays all primary zones in the system regardless of authority.



The left sidebar offers several options for filtering and organizing the zones. The sidebar has three tabs: **Menu**, **Folders**, and **DNS services**.



- The **Menu** tab offers the most commonly used filtering options for zones, such as zone types, favorites, and reverse zones.
- The **Folders** tab allows you to organize zones and filter queries into folders. For more information about folder management, see *Folder management*.

- On the **DNS services** tab you can view zones by server/service. This can be useful if you have multiple DNS services and want to view the zones associated with each one separately.

Micetro will remember your current tab selection when you navigate away from the DNS page and return to it later.

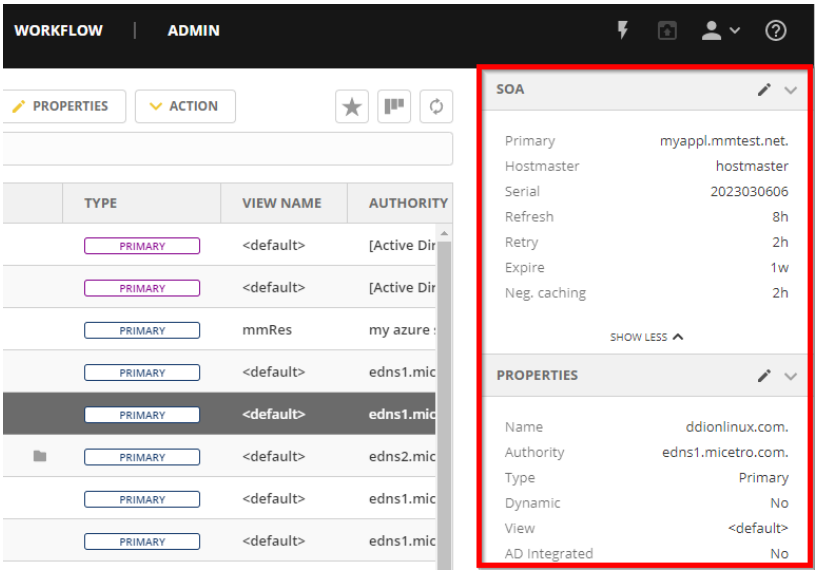
Zone Types

Below are the zone types supported by Micetro.

Type	Description
Primary (blue)	A primary zone, which is always the original copy of the zone, and always present on that zone's primary server.
Primary (yellow)	A dynamic master zone, which is always the original copy of the zone, and always present on that zone's master server.
Primary (purple)	An Active Directory Integrated primary zone.
Secondary	A read-only copy of a primary zone or another secondary zone.
Hint	Root zone used for bootstrapping of recursive DNS servers.
Options template	This configuration template is specific to the AuthServe DNS server and can be used to add templated options configuration to multiple zones. Editing the options template will affect all zones using the template.
Configuration types	*The below zone types are essentially a configuration that tells the (recursive) DNS server how to resolve zones it cannot resolve the normal way.*
Stub	A stub zone is a copy of a DNS zone that contains only resource records that identify the authoritative DNS servers for that zone. Stub zone is dynamically updated from the list of primary DNS servers.
Static-stub	A BIND specific zone type to configure conditional forwarding, similar to Stub but is static, that is, it has a set of preconfigured NS entries.
Forward	A forward zone contains a list of name server addresses, called forwarders, that can resolve queries for the zone. With forward zones queries are forced to go to the specified addresses.

Zone Contents

The Inspector pane on the right provides a look at the SOA record and properties of the selected zone.



You can hide information in the Inspector pane. Simply click a the header of the desired section (or > and *v*) to collapse or expand the section.

SOA

The Start of Authority, or SOA record, is displayed as a collection of fields in the Inspector pane.

Table 7: SOA Information

Field	Description
Primary	The name of the server that acts as primary server for the zone.
Hostmaster	This field is properly formatted by giving the email address of the person responsible for zone with the @ symbol replaced with a period (.). For example, instead of hostmaster@example.com enter hostmaster.example.com. The username part of the email address cannot contain a (verbatim) dot (.). See RFC 1912 'Common DNS Operational and Configuration Errors', Section 2.2 for additional information.
Serial	The serial number is a ten-digit number consisting of the year, the month, the day, and a two-digit daily revision number. (Actually, it is any integer between 0 and ~ 4 billion, but the preceding is the standard convention.)
Refresh	This is the period (in seconds) that determines how often secondary servers will check with the primary server to determine if their zone files are up to date. This is done by checking the serial number. The default value for this field is 28800, which equates to once every 8 hours.
Retry	This determines the period that a secondary server will wait before trying to re-contact the primary zone (in the event that an earlier contact attempt is unsuccessful). The default value is 7200 seconds, or once every 2 hours.
Expire	This value determines how long a secondary server will keep serving a zone after its last successful contact to the primary name server. Once the zone has expired, the secondary server stops giving information about the zone because it is deemed unreliable. The default expiration period is 604800 seconds, or 1 week.
Neg. caching	This field is only available when connected to a BIND server. This value specifies how long a server will retain (cache) the knowledge that something does not exist. The default value is 86400 seconds, 24 hours.

Managing Zones

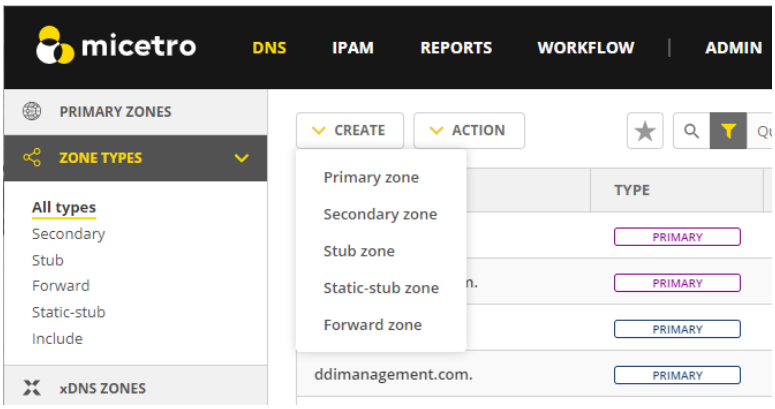
Opening DNS Zones

To view the DNS resource records for a particular zone, you can double-click the zone, or select the zone and then click *Open* on the toolbar at the top or on the row menu (**...**). A list of the zone's resource records is displayed. For more information about DNS Resource Records, see *DNS Resource Records*.

Creating Zones

To create a new DNS zone:

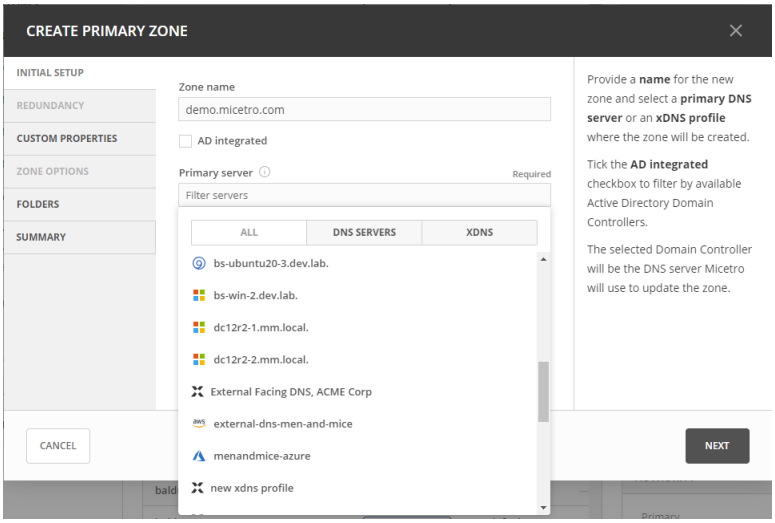
1. Click *Create* on the DNS page toolbar.
2. Select the zone type. For more information about zone types, see *Zone Types*.



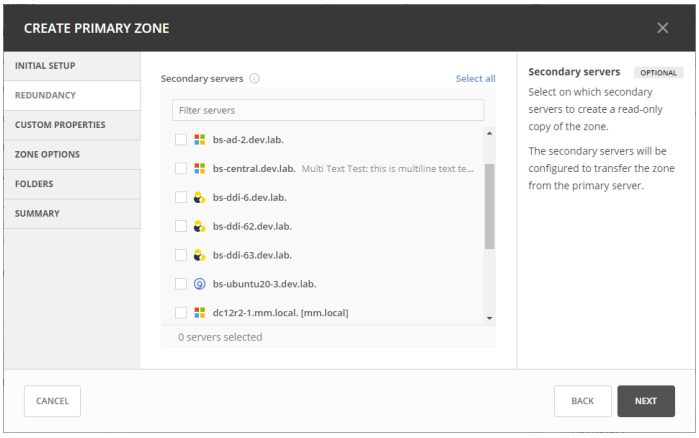
3. Follow the steps of the wizard. The number of steps varies depending on the zone type and how Micetro is configured.

Primary Zone

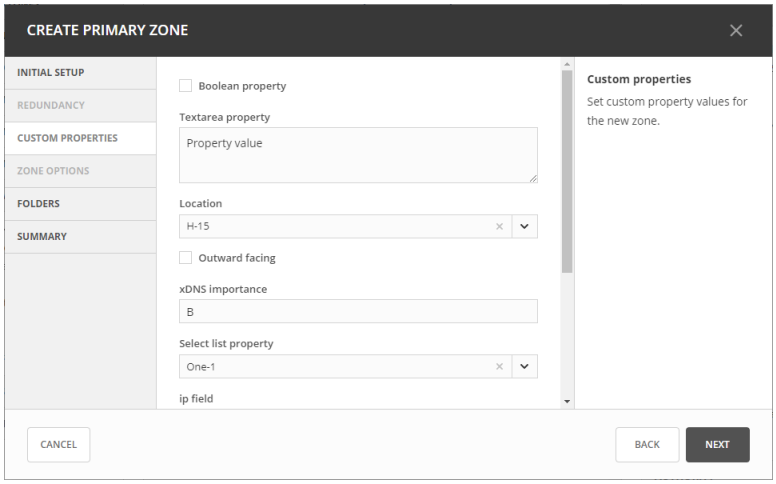
1. Use the server filter to select the DNS server where the zone should be created. If xDNS profiles have been created on the instance, the zone can be added directly to an xDNS profile in the first step of the wizard.



2. Optional. You can select server(s) to host an identical copy of the zone. The zone files from the primary DNS are synced to the secondary DNS through a zone transfer.

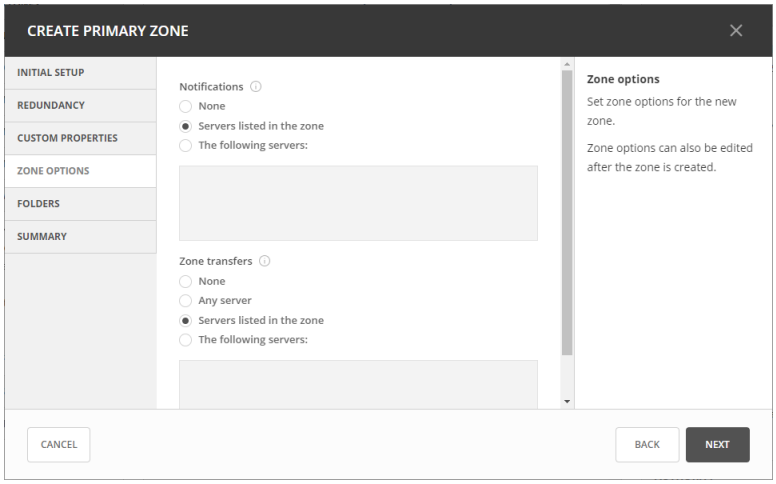


3. If **custom properties** have been defined for zones, they can be edited in a separate step. Custom properties provide additional attributes that enhance the ability to understand, search, and sort zone data in Micetro.

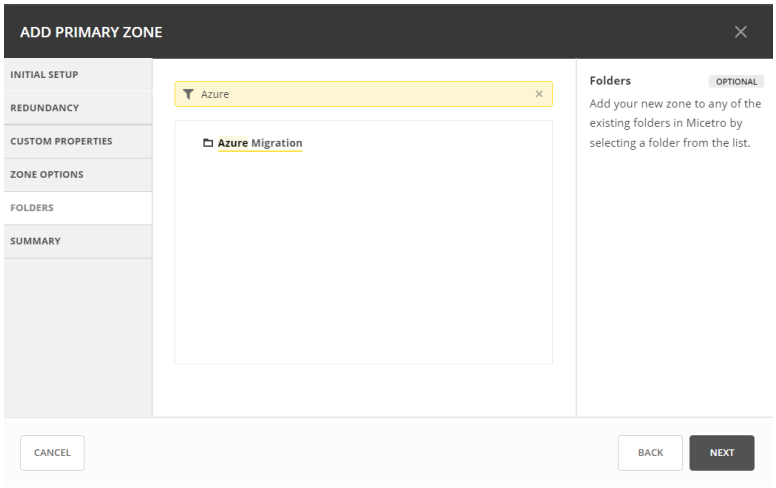


Custom properties are displayed as columns in the DNS grid for each zone.

4. On the **Options** page you can specify which DNS servers should receive notifications when changes are made to the zone and to which servers it is allowed to perform zone transfers.



5. If **DNS folders** have been configured in Micetro, the new zone can be added directly to a folder. DNS folders are a neat way to organise zones in Micetro to have better overview and manageability. For more information about folders, see *Folder management*.



6. The **summary** step summarises the configuration for the new zone before its created. To edit the configuration, go to the respective page of the wizard and make the desired changes.

Secondary Zone

When creating a secondary zone, you need to specify the zone name and either the IP address or hostname of the primary servers that hold the zone you are creating a secondary copy for.

Stub Zone

When creating a stub zone, you must provide the zone name and one or more primary servers for the zone being copied. You can use the toggle control above the text box to turn the address resolution on and off.

Static-stub Zone

When creating a static-stub zone, you must provide the the zone name and a target DNS server. To configure how the resolve the zone, specify either hostnames or IP addresses on the zone options page.

Forward zone

Forward zones are similar to stub zones. You must provide zone name and a list of Forward servers as well as at least one target server for where to create the zone.

Options Template Zone

The template zone option is available only if an AuthServe DNS server is connected to Micetro.

Deleting Zones

To delete a zone from one or more servers:

1. Select the zone(s) you want to delete.
2. On the *Action* menu, select *Delete zone*. You can also select this option on the **Row menu (...)**.
3. The Delete Zone dialog box opens, showing each zone you selected and a list of servers that currently serve that zone. The zone(s) you selected will be deleted from every server that is selected on this list. To keep the zone on a particular server, clear the checkbox for that server.
4. Click *Delete*. The zone is removed from the servers.

Migrating Zones

You can migrate one or more zones from one server to another, including all data in the zone.

To migrate a zone:

1. Select the zone you want to migrate.
2. On the *Action* menu, select *Migrate zone*. You can also select this option on the **Row menu (...)**.
3. The Migrate Zone(s) dialog box opens.
4. Select the DNS service you want to migrate the zone to.
5. If you want remove the zone from the current service, select the *Remove original zone* checkbox. If the checkbox is left unselected, a copy of the zone is left on the current service.

Editing Preferred Servers

Note: This option is only available when working with Active Directory (AD) integrated zones. For more information about AD, see *AD Sites and Subnets*.

DNS administrators can specify the server to use when opening an AD integrated zone, as well as the order of servers to use if the first preferred server becomes unavailable.

1. In the filtering sidebar, select the *AD Integrated*.
2. Select the zone(s) you'd like to set preferred servers for.
3. On the *Action* menu, select *Edit preferred servers*. You can also select this option on the **Row menu (...)**. :
4. Arrange the order of your servers into the preferred order. The server on the top of the list is tried first, then, if that server is unavailable, the second, and so on.
5. Click *Save*.

Warning: If you selected multiple zones, they might have different settings for preferred servers. Saving the configuration will overwrite the previous settings on all selected zones.

Editing Zone Properties

You can click *Edit Properties* on the toolbar to edit custom properties that have been configured for the selected zones.

Promoting Secondary Zones

The Promote Zone feature makes it possible to change a secondary zone to a primary zone. This might be necessary in emergency situations, for example, if the primary zone becomes unavailable for an extended period of time. This feature is only available for DNS Administrators.

When a secondary zone is promoted, the following actions are performed:

- Micetro checks whether the most recent copy of the zone is found in its internal database or on the server hosting the secondary zone, and uses the copy that is more recent.
- The server hosting the secondary zone is configured so that the zone is saved as a primary zone on the server.
- The zone history and access privileges from the old primary zone are applied to the new primary zone.
- The configurations of other instances of the secondary zone are modified so that they will get the updates from the new primary zone.

To promote a secondary zone to a primary zone:

1. Select the secondary zone.
2. On the *Action* menu, select *Promote to primary*. You can also select this option on the **Row menu (...)**.
3. Click *Save* to continue, or *Cancel* to discontinue the process.

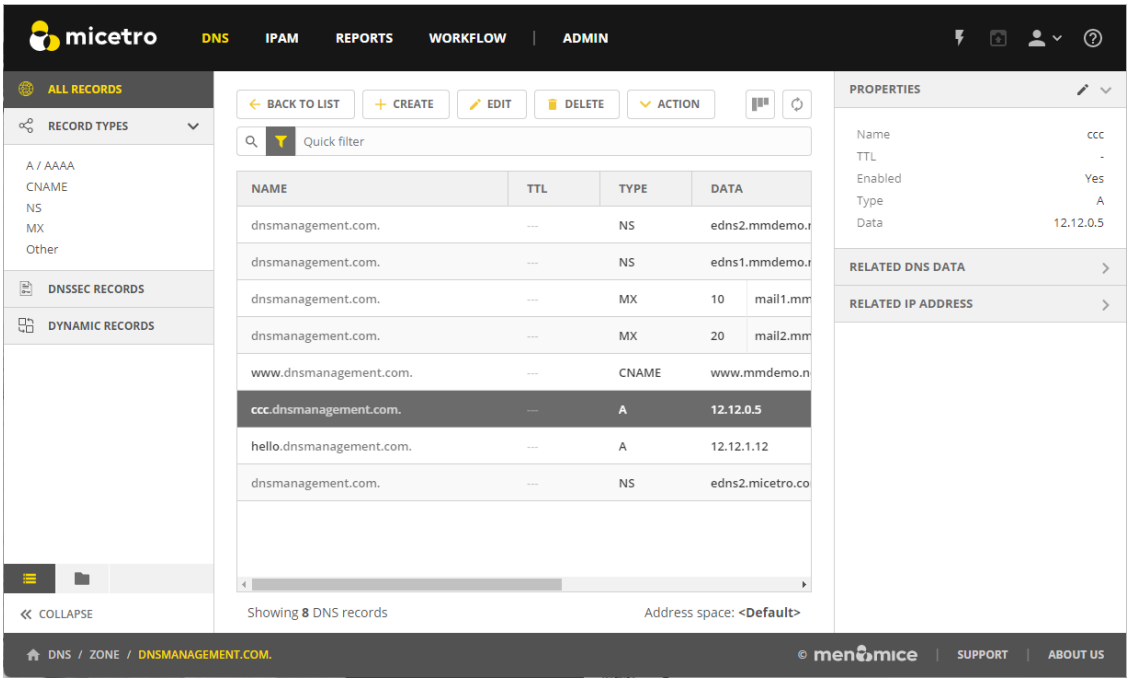
View History

The *View history* option on the *Action* menu opens the History window that shows a log of all changes that have been made to the zone, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user when saving changes to objects. See *Viewing Change History*.

1.10.2 DNS Resource Records

Overview

Each zone in the Domain Name System (DNS) contains a set of resource records that define how requests are processed or delegated within that zone. To view the resource records for a particular zone, you can double-click the zone, or select the zone and then click *Open* on the toolbar at the top or on the row menu (...). Once you have opened the zone, you can view, edit, and manipulate the resource records.



Selecting a DNS record in the list, will display the following details and actions for the record in the *Inspector* pane on the right.

Item	Description
Actions	Lists all available actions for the selected record.
Properties	Lists the properties for the selected DNS record.
Related DNS Data	Lists all related DNS records for the selected DNS record. Related DNS records all DNS records that are somehow associated with the specified record.
Related IP address	Lists the related IP address in case of an A or AAAA DNS record.

Available Record Types

- A / AAAA
- MX
- TXT
- NS
- SOA
- SRV
- HINFO
- CNAME
- TLSA

- CAA
- CERT
- WKS
- RP
- AFSDB
- LOC
- SSHFP
- SPF
- DNSKEY (read only)
- NSEC (read only)
- NSEC3 (read only)
- NSEC3PARAM (read only)
- RRSIG (read only)
- DS
- DLV (read only)
- HTTPS
- SVCB
- CDS
- CDNSKEY
- CSYNC

Creating New DNS Records

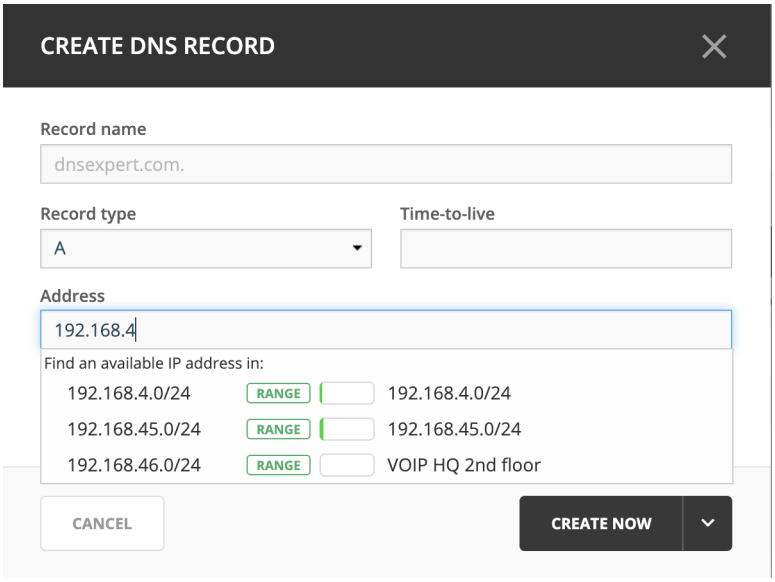
Note: For importing DNS records in bulk, see webapp-import-dns-records.

To create a new DNS record:

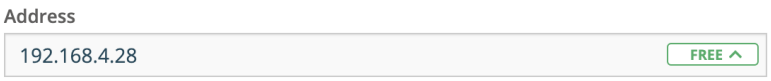
1. Click *Create* in the main toolbar. The Create DNS Record dialog box opens.
2. Enter a name and select the record type. After selecting the type, the relevant fields are automatically displayed.

   Warning: If you save a new DNS record with the wrong type, you cannot change the type later. You have to delete the record and create a new one with the correct type.

3. Fill in the required information and custom fields, if there are any.
   - For A records, an autocomplete behavior helps finding a free IP address in a network.
   - When you enter the first digits of a network, you'll see a list of networks to choose from.



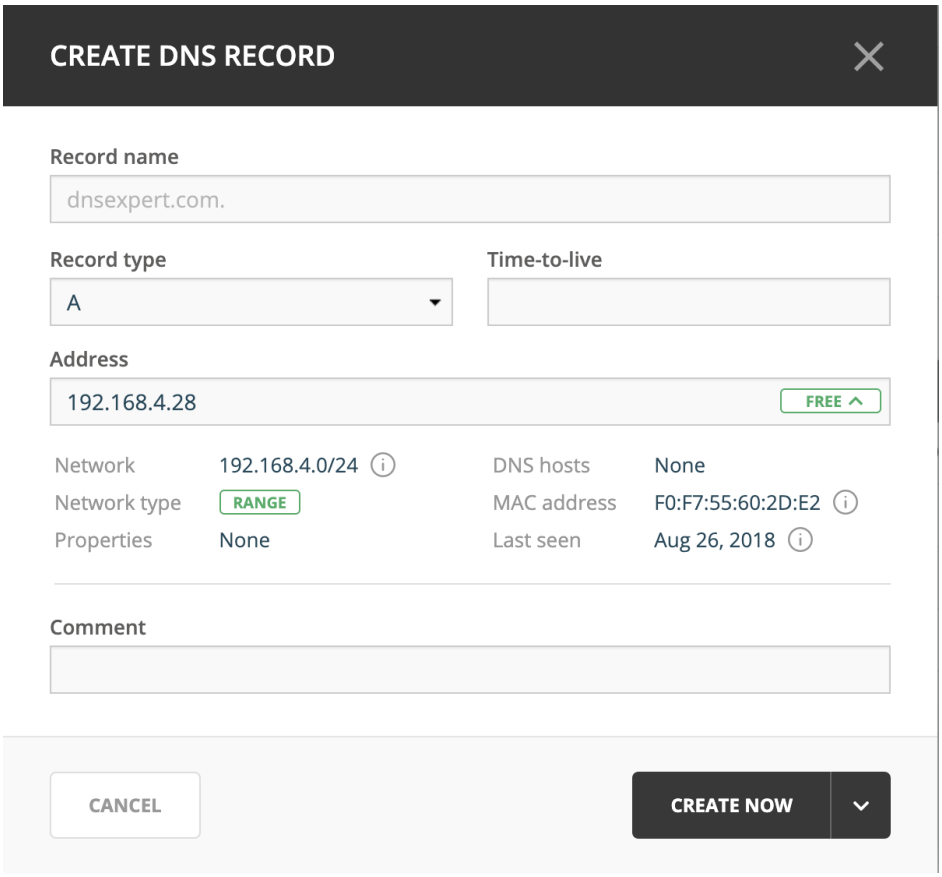
- Selecting an item from the list, will fill in the **Address** field with the next free IP address from that network, along with an indicator on the address state: `Free`, `Reserved`, `Claimed` or `Assigned`. You'll also see insights for the selected IP address.



4. When you are finished, click *Create now* to save the new record to the zone, or *Add to request* to add it to the request queue. For more information about the request queue, see *Workflow Management*.

IP Address Insights

Once you have entered/selected the IP address in the **Address** field, you'll be able to see some insights about the address and related objects. These insights give you more information about the IP address and can help you understand its state better.



Hover over the *i* icon to see more information or a list of objects:

- *Network* will show more details on the network.
- *Properties* will show a list of all defined properties for the specified IP address.
- *DNS hosts* will show a list of all defined DNS hosts for the specified IP address.
- *MAC address* will show a list of additional MAC information for the specified IP address.
- *Last seen* will show a list of additional information for the specified IP address.

Table 8: IPAM Insights

Network	The network containing the specified IP address
Network type	Either an IP address range or a DHCP scope
Properties	Various properties including custom properties, if defined.
DHCP client	
DNS hosts	Lists all DNS hosts that are set for the specified IP address
MAC address	The MAC address of the discovered device
Last seen	The date for which the IP address was last seen

Time-to-live (TTL)

Throughout the system, the TTL value can either be specified in seconds or using the shorthand notation, such as:

- **1s**: 1 second
- **1m**: 1 minute
- **1h**: 1 hour
- **1d**: 1 day
- **1w**: 1 week

Editing a DNS record

1. Select the DNS record in the DNS record list
2. Either click *Edit* in the main task bar, or click on *Edit DNS record* in the row menu (...).
3. A dialog box is displayed where you can modify the DNS record.
4. Click *Save*.

Deleting Records

Deleting a record removes both the data and the physical record from the grid.

1. Select the record(s) that you want to delete. To select multiple records, hold down the Ctrl (or Cmd on Mac) key while making you selections.
2. Click *Delete* on the task bar. The record is immediately deleted from the zone.

1.11 DHCP

Note: To manage DHCP scopes in the Management console, see *DHCP Scopes - Management Console (obsolete)*.

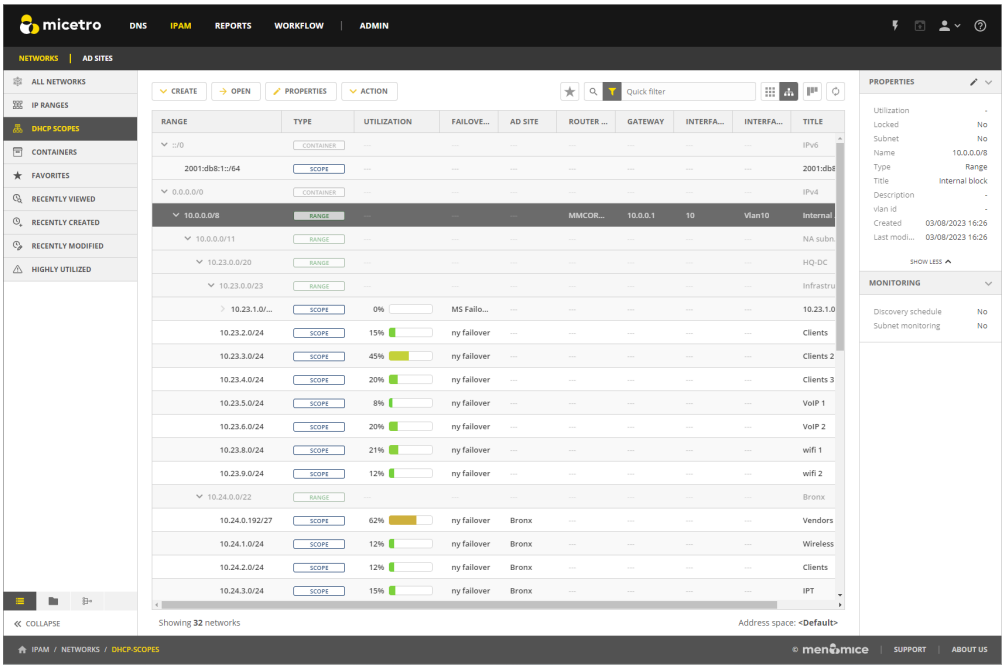
1.11.1 Overview

This section shows you how to perform specific actions in Micetro associated with maintaining your DHCP scopes, such as creating and modifying reservations, setting scope options and working with split scopes.

1.11.2 Viewing DHCP Scopes

All DHCP Scopes on All Servers

You can view all of the existing DHCP scopes at once, regardless of the server to which they belong. On the *IPAM* page, select *DHCP scopes* in the filtering sidebar on the left.



The *Utilization* column in the scope list shows the utilization of available addresses within the address pool(s) of each scope.

Disabled scopes appear dimmed. The number of unassigned addresses is always shown as zero for disabled scopes.

Scopes on a Specific DHCP Server

Adiministrators can view DHCP scopes that reside on individual DHCP Servers that are being managed by Micetro. On the *Admin* page, select the relevant DHCP server in the filtering sidebar under *DHCP Services*. On the *Action* menu, select *View scopes*. You can also select this option on the **Row menu (…)**.

Selected Scope Menus

When working with scopes, selecting one or more scopes enables a row menu (...) and relevant actions from the *Actions* menu on the top toolbar. The available actions change based upon the type of the DHCP server the scope is hosted on.

DHCP Scope Actions

- **Open network**: Opens the selected scope.
- **Edit network properties**: Change the title, description, and vlan id of the selected network.
- **Enable/disable scope**: If you are no longer using a particular scope, but do not want to delete it completely because you may need it in the future, you can disable the scope instead. A scope that is disabled will be ignored by the DHCP server until it is re-enabled.
- **Convert to network**: Converts the DHCP scope to a network.
- **Add to folder**: Adds the scope to a folder for easier access. See *Object folders*.
- **Set discovery schedule**: Sets discovery schedule for the scope.
- **Set subnet monitoring**: Configures subnet monitoring for the scope.
- **Manage DHCP pools**: View and manage DHCP pools.
  - **Add Pool** : Creates an address pool for the selected scope. Fill in the *From* and *To* fields in the dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.
  - **Edit Address Pool**: To edit an existing pool, select it, and then select *Edit* on the **Row menu (...)** .
  - **Delete Address Pool(s)**: To delete an existing pool, select it, and then select *Delete* on the **Row menu (...)**.
  - **Create Exclusion**: *MS DHCP only*. Allows you to exclude a single IP Address or an entire range of addresses from being used. You can only exclude addresses that are already part of an address pool. To create an exclusion, specify the From and To IP Addresses. All the addresses between and including the ones entered will be excluded.
  - **Edit Exclusion**: *MS DHCP only.* To edit an exclusion, select it, and then select *Edit* on the **Row menu (...)**.
  - **Delete Excluded Range(s)**: *MS DHCP only.* To delete an exclusion, select it, and then select *Delete* on the **Row menu (...)**.

DHCP Actions for IP Addresses

To view the IP addresses a DHCP scope contains, double click the scope the grid, select *Open network* on the **Row menu (...)**, or the *Action* menu.

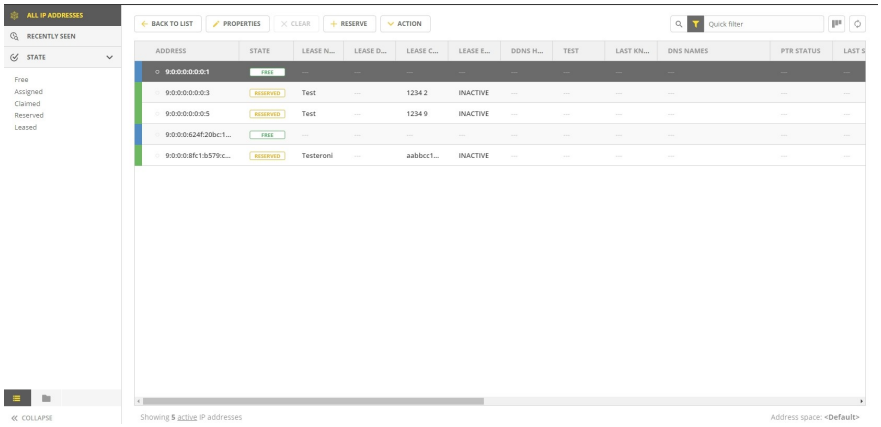
- **Create DNS record**: Creates an A record from the selected IP address. See webapp-create-dns-record.
- **Edit IP address properties**: Define values for any custom properties configured in the system.
- **Claim/release IP address**: Claims and releases the IP address(es).
- **Ping IP address**: Performs a ping on the selected IP address(es).
- **Create DHCP reservation**: Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP Addresses. To create a reservation, do the following:

  - **Name**: Assign a name to identify the reserved address.
    * **Description**: (Optional) User defined description.
    * **Reservation method**: Hardware address or Client identifier
      · **Hardware address**: Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.
      · **Client identifier**: Use the *Ascii* and *Hex* switch on the right to change input type.
    * **Reservation type**: Select whether this reservation should support DHCP, BOOTP (i.e., Bootstrap Protocol), or both (default).

- **Edit DHCP reservation**: Edit an existing reservation.
- **Edit reservation options**: Edit options for a reservation. Refer to dhcp-options for details on this dialog box.
- **Delete DHCP reservation**: To delete an existing reservation, right-click on the reservation you want to remove and select *Delete Reservation(s)*.
- **View history**: Displays the object history for the selected IP address.

1.11.3 Viewing DHCPv6 Scopes

Unlike DHCPv4 scopes which display all the addresses within a scope, a DHCPv6 scope will only display addresses in use or which have been recently used. At the bottom of the view, you will see how many active IP addresses are being shown. If there is an IP address with the status of **free**, that IP address has recently been used. To see more information, select *View History* for that address.



1.11.4 New DHCP Scope

Note: Creating a scope on a Kea server configured for load balancing high availability, Micetro will automatically split the scope evenly between primary and secondary servers. See dhcp-kea-ha.

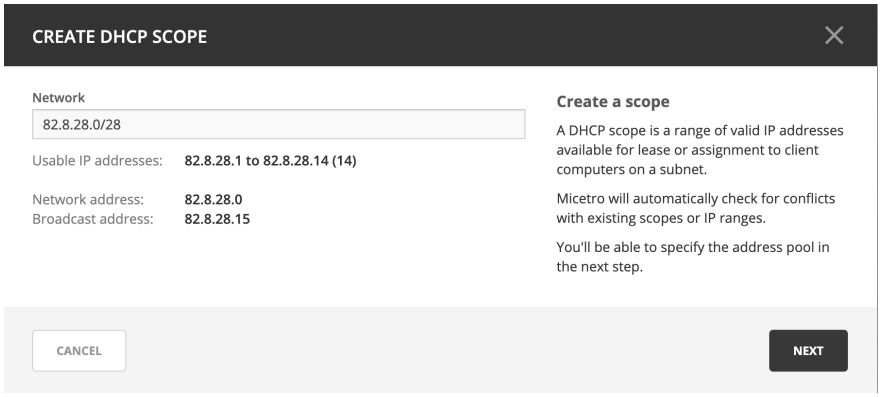
This section describes how to create and edit DHCP scopes with the new *DHCP Scope Creation Wizard*.

Whenever you create a new scope, Micetro automatically checks whether the new scope conflicts with an existing scope or an IPAM range.

The Wizard has additional steps, or skips over some steps, depending on the type of DHCP server the scope is being created on, and whether the *AD Sites and Subnets* integration has been enabled.

To create a new scope on the MS DHCP server, do the following:

1. In *Networks* use the *Create* action and select *DHCP scope* from the dropdown.



2. Click *Next*.
3. Edit the options for the DHCP scope.
   - **DHCP server**: The DHCP server for the scope.
   - **Enabled**: If selected, the DHCP scope will start allocating IP addresses immediately. Clear this option if you want to configure the scope further.
   - **Start/end of address pool**: Adjust the first and last IP address in the pool.
4. Active Directory Site selection. If you have enabled *AD Sites and Subnets*, the Wizard will ask you which AD site the new DHCP Scope should be associated to.

   Note: Leave it empty for no AD site.

5. Scope properties.
6. Summary. The changes the Wizard will perform are summarized here and applied once the user clicks “Finish”.
7. Save comment.

1.11.5 New DHCPv6 Scope

Micetro supports DHCPv6 for Microsoft and Kea DHCP

1. Under *IPAM* click on *Create* and select *DHCP Scope*..
2. Enter the network information and click *Next*.
3. Enter the DHCP Server name and the preference, and put a check next to *Enabled* if you'd like to enable this scope on this server. Click *Next*.

   Note: The preference value is a new parameter required by Microsoft for DHCPv6 scopes. If the scope is assigned to multiple servers, the lowest preference assignment will be selected by the DHCP client

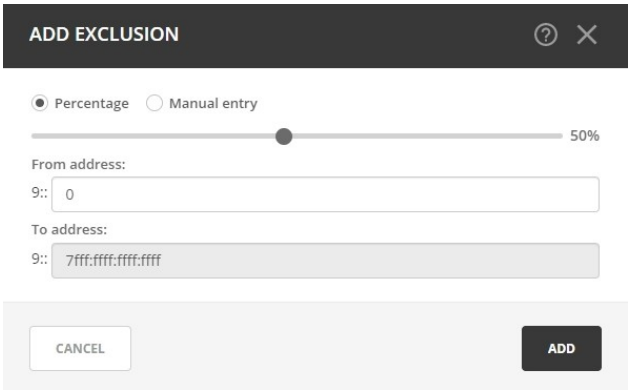
4. Enter the title as an identifier for this scope as well as the description and click *Next*.
5. Verify the information is correct and click *Finish*.

1.11.6 Manage DHCPv6 Exclusions

When managing exclusions within a DHCPv6 pool it is possible to specify a percentage of a DHCPv6 scope rather than specifying a **From address** and **To address**

1. Select a DHCP scope while under *IPAM* >> *DHCP scopes*.
2. Click *Action*, and then select *Manage DHCP Exclusions*.
3. Click *Add Exclusion*.
4. A new pop up will appear. Choose to either create the exclusion range by *Manual Entry* or *Percentage*.
5. If you choose manual entry, enter the **From address** and **To address** for the range you'd like to exclude from the DHCP scope.

   If you choose percentage, drag the percentage bar to the correct percentage of addresses you'd like to exclude, and enter a **From address** only.

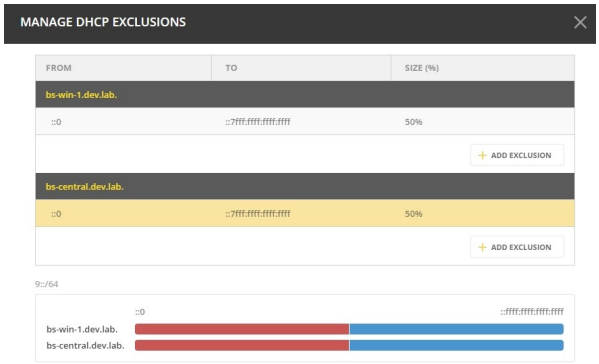


Note: If the exclusion range doesn't have the space to accomodate the percentage of IP addresses specified, it will not allow you to add this exclusion range until you pick an appropriate **From address** or lower the percentage.

6. Click *Add*.

   Red bar: The exclusion range

Blue bar: Address Pool of dynamic allocation addresses



7. Click *Save*

1.11.7 Access

For complete details on this function, refer to *Access Management*.

1.11.8 Folders

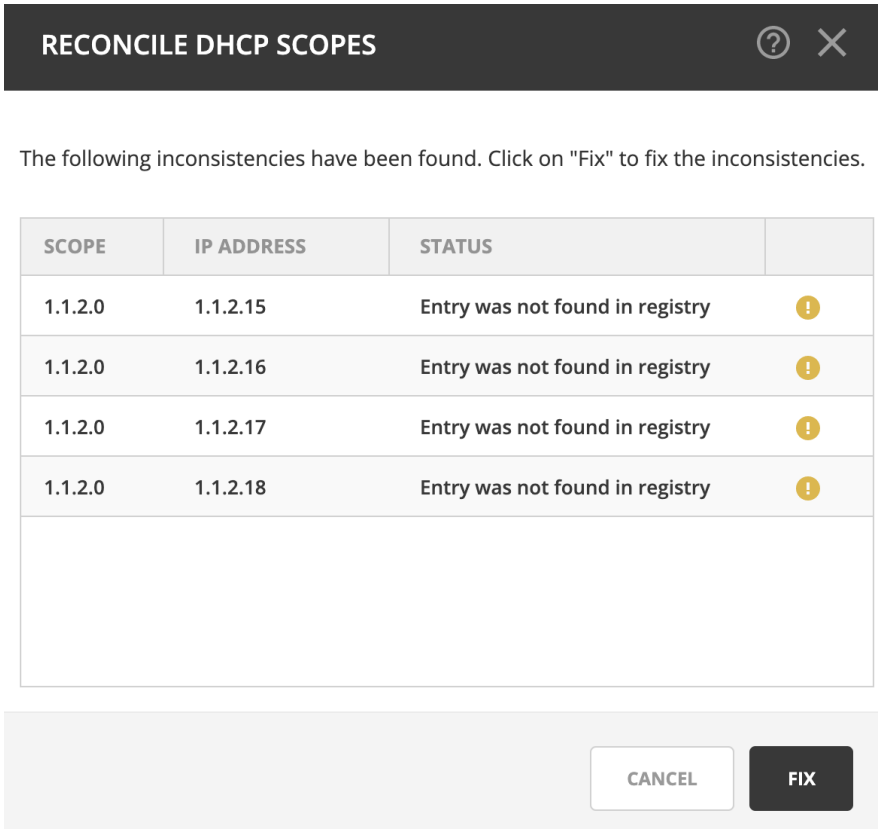
Refer to *Object folders* for details on this function.

1.11.9 Reconcile Scopes

Note: Applies to MS DHCP Servers only.

Use this function to fix inconsistencies between information in the registry and the DHCP database.

1. Go to the *IPAM* page.
2. Select *DHCP Scopes*
3. Select one or multiple DHCP Scopes from *Microsoft Servers*
4. Click on the ellipsis (or meatball) menu on the scope(s).
5. Click on *Reconcile DHCP Scopes*
6. If there are inconsistencies, a list will be presented. Click *Fix* to fix the inconsistincies.



For more information see the Microsoft documentation.

1.11.10 Other Functions

At any time, you can modify the properties for a scope. Simply locate the item, and from the **Row menu (...)** select *Edit network properties*. For split scopes, the scope contents can be examined individually on each server.

Deleting a Lease

To delete a lease in a DHCP scope, do the following:

1. Open the scope containing the lease you want to delete.
2. Select the lease and on the **Row menu (...)** select *Release DHCP lease* or use *Action → Release DHCP lease*.

IP Address Details

The IP Address details window contains all information pertaining to an IP Address in Micetro, including DNS records, DHCP reservations, and custom properties. To access the IP address details select an IP address in the DHCP scope dialog, and all information is displayed in the Inspector, including information on any DNS and DHCP data associated with the IP address. A reservation can be created by clicking the + button in the *Related DHCP data* section of the Inspector.

Renaming a Scope

You can change the name and/or description of a scope in Micetro.

1. Locate and select the DHCP Scope you want to rename.
2. On the **Row menu (…)**, select *Edit network properties*.
3. Enter the **Title**, and any other value you wish to change.
4. Click *Save*.

1.11.11 Host Discovery

With this feature, you can see when hosts were last seen on your network. There are two methods you can use for host discovery – using ping or querying routers for host information.

When host discovery is enabled, two columns are added to the range or scope view.

Last Seen
: This column identifies when a host was last seen on the network and which method was used to discover the host.

Last Known MAC Address
: This column shows the MAC address used by the host the last time it was seen on the network. This column is only populated if the host was seen using a router query.

Configuring Host Discovery Using Ping

1. Select one or more scopes.
2. on the **Row menu (…)**, select *Set discovery Schedule*.
3. Select the *Enable* option.

- **Frequency**: Click the drop-down list and select the frequency (e.g., 1, 2, etc.).
- **Every**: Enter the frequency unit for discovery (e.g. days, weeks, etc.).
- **Next run**: Select the start date and time.

4. Click *Save*.

Once the schedule options have been set and saved, two columns - Last Seen and Last Known MAC Address - are added to the range or scope grid. The Last Seen column identifies when a host was last seen on the network.

Green
: Host responded to the last PING request. The date and time are shown.

Orange
: Host has responded in the past, but did not respond to the last PING request. The date and time of last response is shown.

Red
: Host has never responded to a PING request. The text Never is shown.

At any time if you wish to disable host discovery, do the following:

1. Select the object(s) for which you want to disable discovery.
2. On the **Row menu (…)** , select *Set discovery schedule*.
3. Clear the *Enable* option.

4. Click *Save*.

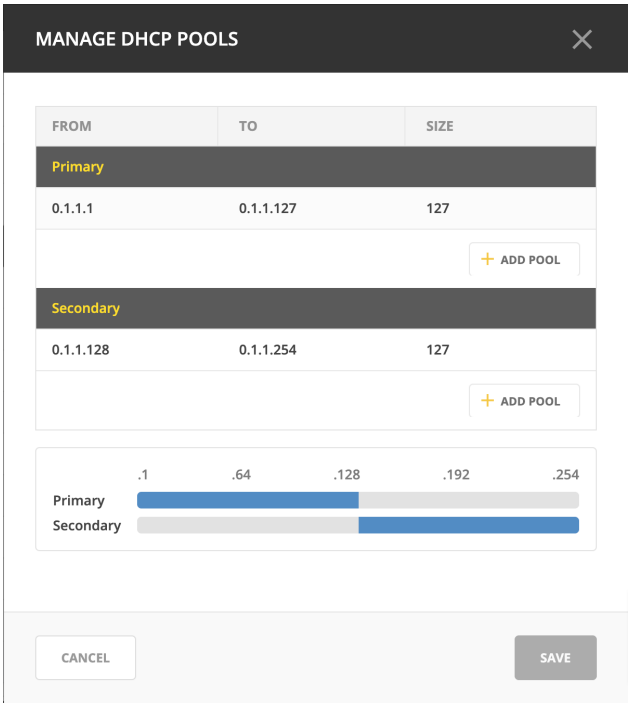
- The DHCP scope window will show every instance of the split scope in a separate tab, making it possible to work with all instances of the split scope in a single window.
- The Overview and Statistics tab in the DHCP scope window will show a graphical overview for all of the split scope instances.
- Reservations are managed automatically. All changes to reservations (creation, modification, and deletion) are applied to all instances of the split scope.

The servers listed in this dialog box all contain the scope to which the user was applying the change. By pressing the Enable button, all instances of the scope would be enabled.

Note: Split scopes are only supported on MS DHCP and ISC Kea servers.

1.11.12 Split Scopes in Load Balancing Mode

When creating scopes on Kea servers configured in load balancing mode for high availability, Micetro will split the available pool evenly between primary and secondary servers.



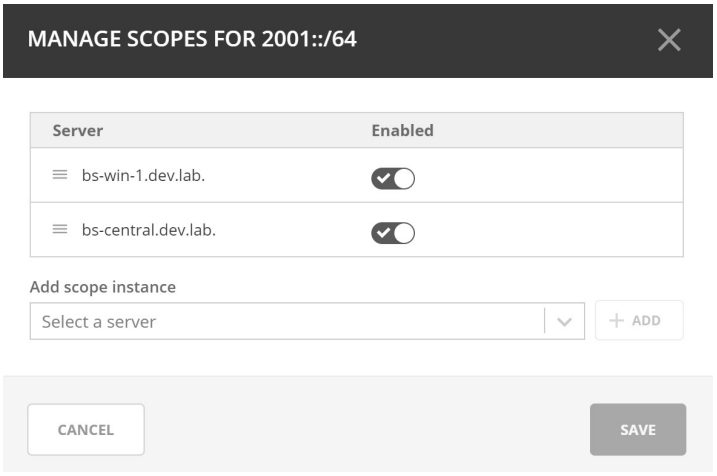
1.11.13 Managing Split Scopes for DHCPv6

1. Select a DHCPv6 scope under *IPAM >> DHCP Scopes*
2. Click *Action*, and then *Manage Scope Instances*
3. In the drop-down menu select a second server to manage the DHCP scope, and then click *Add*. Enable the servers on which the split-scope should reside.

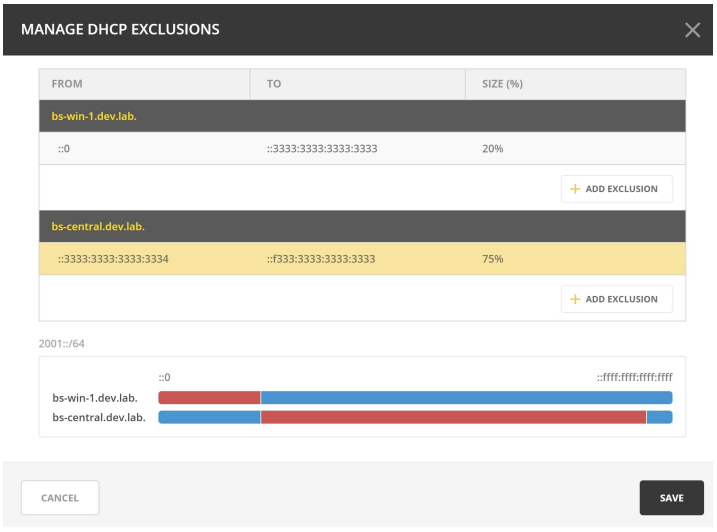
Note: You can change the preference of the servers by clicking and dragging on the hamburger icon (three lines to the left of the server) to change the order of the servers. The second server will always have a preference of the **First Server Preference + 1** and each additional server will increment by 1.

---

4. Click *Save*



5. On the same scope, click the *Action* menu and then select *Manage DHCP Exclusions*
6. Click on *Add Exclusion* for the first server and select the percentage for which you'd like to exclude from the first server and click *Add*
7. Click on *Add Exclusion* for the second server and select the percentage for which you'd like to exclude from the second server and click *Add*



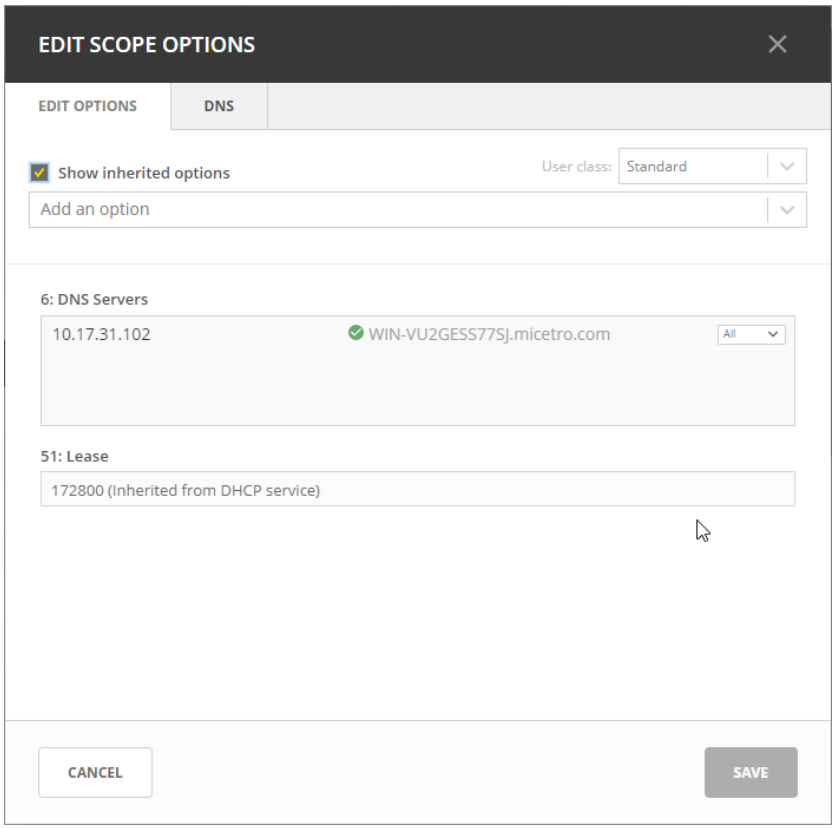
8. Click *Save*

1.11.14 Editing DHCP Options

Note: DHCPv4 and DHCPv6 scopes inherit DHCP and DDNS Options from the parent DHCP server. DHCPv4 and DHCPv6 reservation inherit DHCP and DDNS options from the DHCP scope. However these options may be changed by editing the options for the specific scope or reservation.

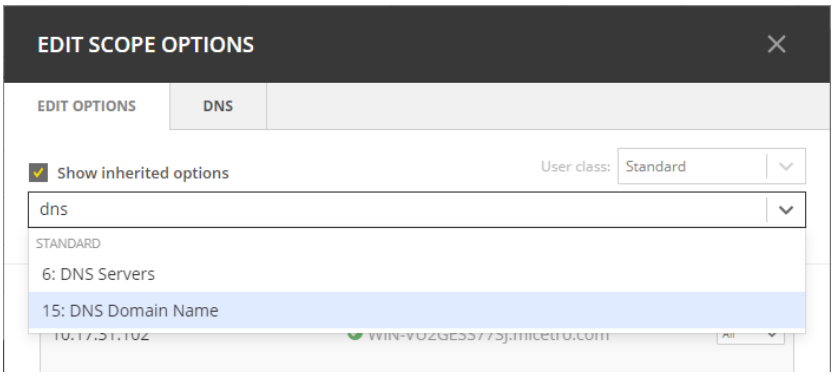
Viewing the configured DHCP options for a DHCP scope

1. Select the DHCP scope in the networks list.
2. On the *Action* menu, select *Edit scope options*. You can also select this option on the **Row menu (...)**.
3. A dialog box is displayed. Note that in order to see the options that have inherited values, you need to select the *Show inherited options* checkbox.



Adding a New DHCP Option

1. Start typing into the *Add an option* field. Either type in the name of the option or the option number.
2. A list of available options will be displayed as you type.



3. Select the option you want to add.
4. The option is now shown in the list and you can add values to the option.

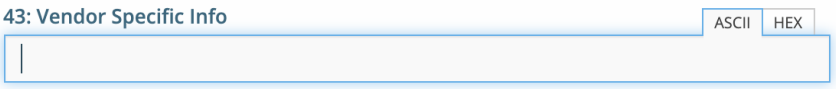
Removing a DHCP Option

Hovering over an option in the Edit Scope dialog box will display a trash can icon to the right of the option.

Clicking the trash can will remove the option.

HEX and ASCII Representation

Some DHCP options, such as DHCP option 43 (Vendor specific info) require the value to be in HEX format. In this case the UI offers the value to be viewed both as HEX and ASCII by selecting each option in tabs above the field, as seen in the figure below.



1.12 IPAM

Note: This information applies to the Web Interface. For information about how to manage IP addresses in the Management Console, see console-ipam.

1.12.1 Overview

Managing IP Addresses entails being able to create assignable ranges within the available address space and determining which users and groups have usage rights to that space. The IP ranges can be created with specific properties that also determine the properties of the IP Addresses contained within them.

Note: In order to use the IP Address Management features in Micetro, you must have entered the license key for the IPAM module.

1.12.2 Multiple Address Spaces

Note: For managing address spaces, see *Address Space Management*. For managing address spaces through the Management Console, see console-address-spaces.

Micetro supports multiple address spaces.

Each address space instance contains its own set of DNS servers, DNS zones, DHCP servers, DHCP scopes, IP Address ranges (including the IPv4 and IPv6 root ranges), IP address entries, and folders.

Note: Changes to data in one address space do not affect data in any other address space.

Items **shared** between address spaces are:

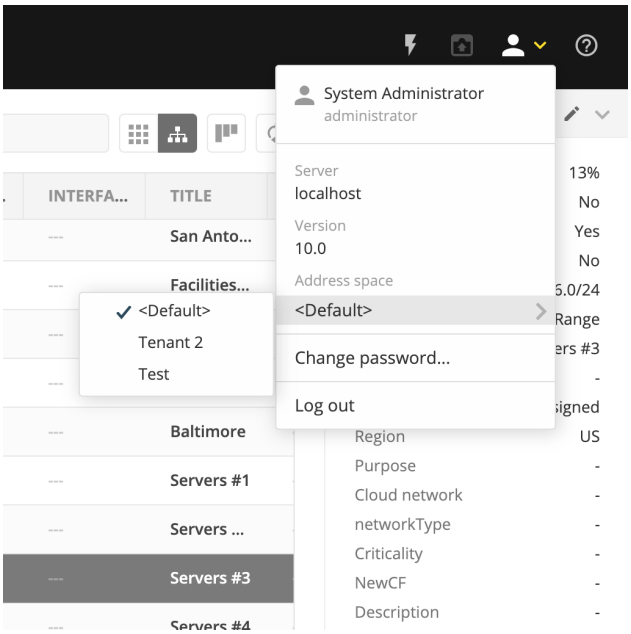
- users, groups, and roles
- custom property definitions (see *Custom Properties*)

Switching to a Different Address Space

You can only work in one address space at a time. You can see the current address space at the bottom of the *Networks* section on the *IPAM* page..

To switch to a different address space:

1. Click the **User** icon in the top right corner.
2. Point to *Address Space*, and then select the address space you want to use.



1.12.3 Address (A) Records in DNS Zone Windows

When the IPAM component is enabled, you may notice some differences when working with Address (A) records in DNS zone windows, such as:

Restriction on allowed IP Addresses
When IPAM is enabled, the system administrator may restrict which IP Addresses you are allowed to use. The system administrator can determine an IP Address range that you are allowed to work with. In addition, he/she can choose whether you can use an IP Address that has already been assigned in DNS.

Automatic assignment of IP Addresses
The system administrator can configure Micetro so that you can create address (A) records without entering IP Addresses. When the zone is saved, the IP Addresses are automatically assigned using free IP Addresses in your IP Address range. If you want to enter an IP Address manually, you can type it in the IP Address field, but if you leave the field unchanged, the IP Address will be automatically assigned when you save the zone. If you have access to more than one IP Address range, a dialog box will be displayed at save time where you can choose the IP Address range for your new address records.

1.12.4 Containers

A Container is a section of the address space that has been reserved but not yet allocated. Containers can contain address ranges and scopes, and you can set address privileges for containers that can be applied to the enclosed ranges and scopes through access inheritance. You cannot allocate IP addresses from within a container unless you have enabled that functionality in System Settings.

New Container

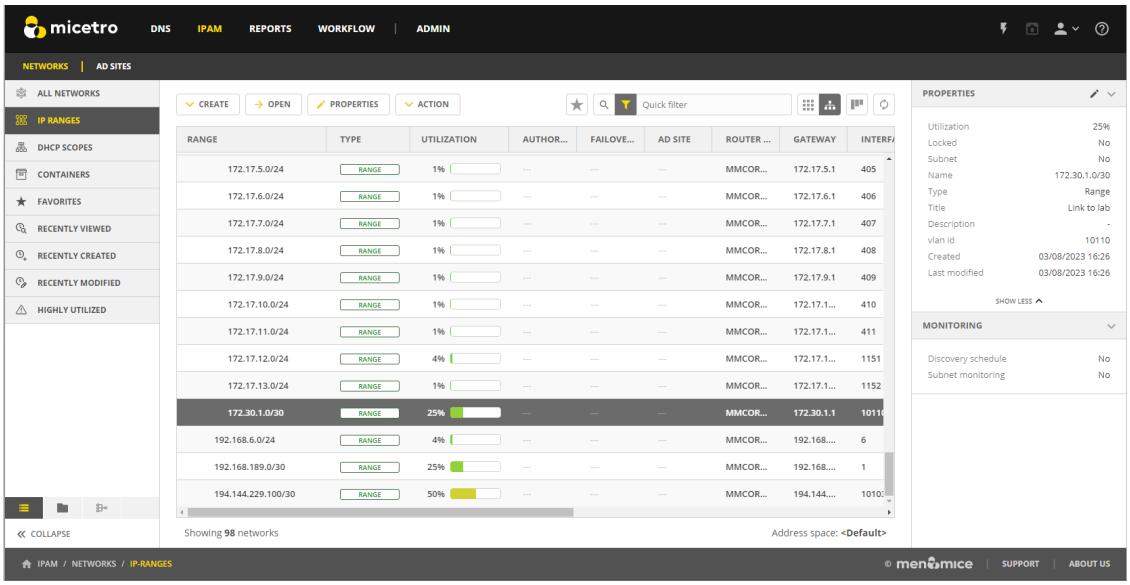
A range that exists on network boundaries (a subnet) can be converted to a Container. Likewise, a Container can be converted to a range.

1. Select *IPAM* on the top navigation bar.
2. Select the range(s) you want to convert.
3. On the *Action* menu, select *Convert to container*. You can also select this option on the **Row menu (…)**.
4. Confirm that you want to convert the selected range(s), and add a save comment.

1.12.5 Viewing IP Address Ranges

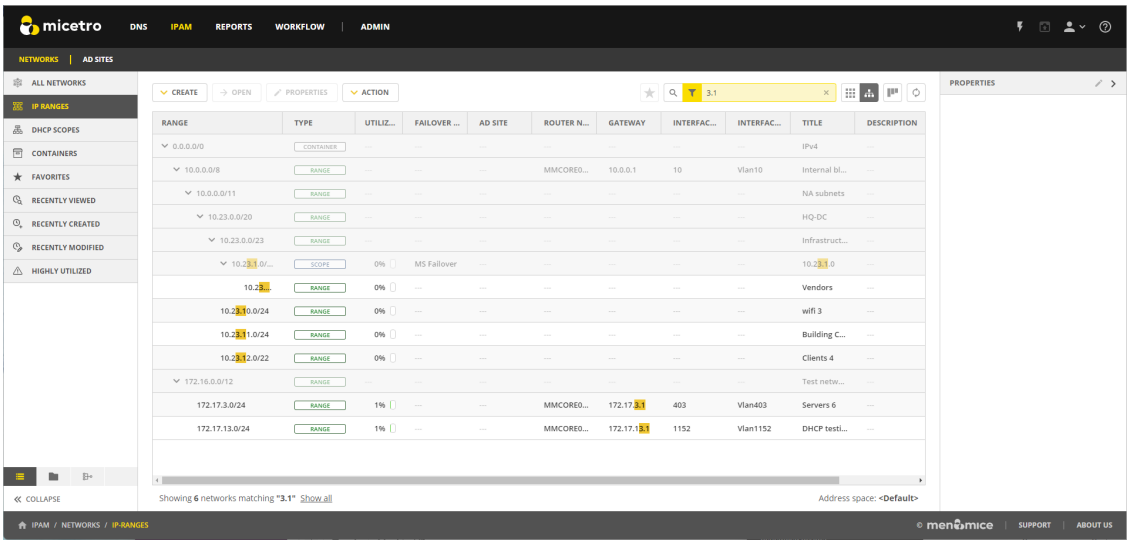
The **IPAM** page shows the section of the IP address space that is accessible to the current user of the system. Micetro allows administrators to manage the IP Address space by dividing it into any number of named sub ranges that can be assigned to specific groups for use by its members.

In the filtering sidebar, select *IP Ranges*.



- Use the buttons on the top right of the grid to choose between a flat and a hierarchical view for the Address Ranges scopes.
- If an Address range has no subranges, the utilization for the range is shown in the range list.

To narrow down the results shown when viewing IP ranges, you can use the webapp-quick-filter. When using the tree view with an active filter, any parent ranges that do not match the search criteria will be faded out while the matches highlighted. For example, in the image below, we searched for the string `3.1`.



1.12.6 New Networks

To create a new network, do the following:

1. Go to the **IPAM** page.
2. Click the *Create* button.
3. Select what type of network (new network, *New DHCP Scope*, *New Container*) you'd like to create.
4. Enter the appropriate values, grouped on pages depending on the type.

Note: The *Create* wizard is different depending on the type selected through the dropdown:

- For a *network*, you can reserve network and broadcast address, and lock the range if needed. You can also assign it to an AD site. (See *AD Sites and Subnets*)
- A *DHCP scope* can be created with the network and broadcast address automatically configured. See *New DHCP Scope*.
- A *container* has no network or broadcast address. See *Containers*.

5. Click *Finish*.

Once a non-reserved IP Address range has been created, it is considered to be managed. A managed IP Address range is being managed by the Networks component of Micetro. When the range is managed, Micetro will allow users with appropriate privileges to work with IP Addresses from the range.

It is possible to create subranges of existing ranges and DHCP scopes.

Note: When you create a new IP Address range, Micetro checks to see if the new range can be logically grouped with other address ranges, and adds the new range in the appropriate address range group.

Network Configuration

When creating a new network, DHCP scope, or container, you must complete the Properties page in the final step.

These properties are defined in *Custom Properties*.

Network Modifications

Once you have created a network, it is easy to make changes.

1. Select the range in the list.
2. On the *Action* menu, select *Edit network properties*. You can also select this option on the **Row menu (..)**.
3. Make the desired changes.
4. Click *Save*.

Network Deletions

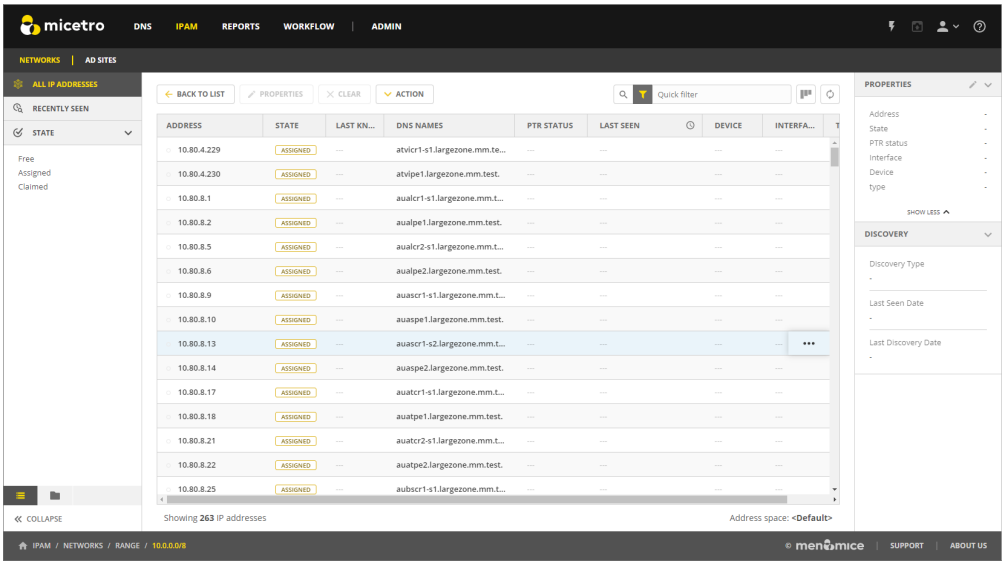
You can always delete a network definition. If you delete a network, the IP addresses that belonged to it will get the attributes of the parent network. If the network you are deleting has subranges, they will become children of the unassigned networks' parent.

To delete a network definition:

1. Select network(s) you want to remove.
2. On the *Action* menu, select *Delete network*. You can also select this option on the **Row menu (..)**.
3. You are prompted to confirm your decision to delete the(se) network(s). Click *Yes* to delete the range, or *No* to leave it.

1.12.7 IP Address List

To view a list of host entries in a particular network, double-click the network. This opens a list where you can view and edit the properties of individual IP address entries.



The *State* section in the filtering sidebar can be used to show only **Free**, **Assigned**, **Claimed**.

The *PTR Status* column shows the status of the Address (A) record and Pointer (PTR) record mappings. This column can have three values:

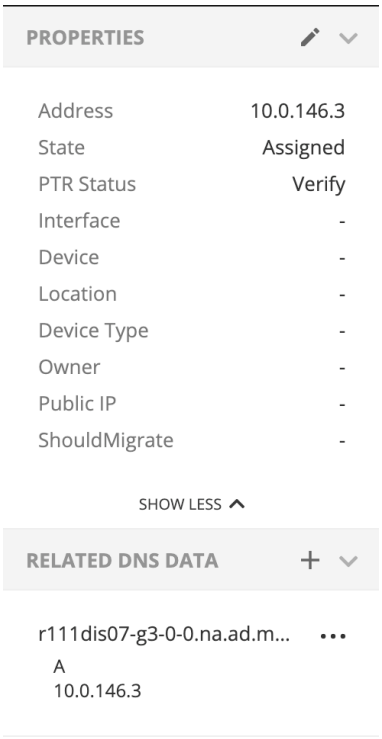
- **Empty**: The status is empty if there are no DNS records for the host. It is also empty if a PTR record exists where the domain in the data section of the PTR record is not managed by the system.
- **OK**: If there is a match between the A and the corresponding PTR record(s) the status is listed as OK.
- **Verify**: If there is not a match between the A and the PTR records for the host, the status is listed as Verify. The most common reasons are:
  - There is an A record but the PTR record is missing.
  - There is a PTR record but the A record is missing.
  - The data section in the PTR record does not correspond to the name of the A record.

When the PTR Status for a host entry shows Verify, you can open the IP Address dialog box for the host to see more detailed information on which DNS host entry is generating this status message.

Note: When working with large IP Address ranges (ranges that contain more than 4096 IP Addresses) the *Show unassigned addresses* will no longer be available and the IP Address List window will only display assigned IP Addresses.

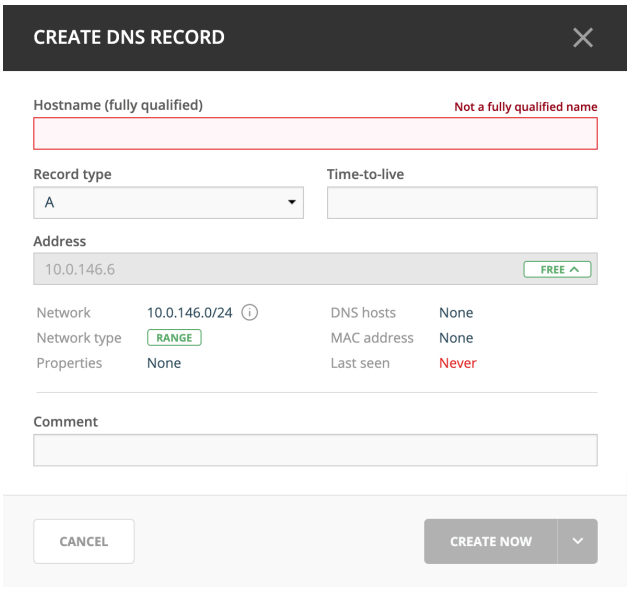
1.12.8 IP Address Inspector

When you add or modify an existing IP address entry, the IP Address dialog box displays. The entries in Inspector can vary, depending on the custom properties defined in Micetro (e.g., "Owner" is a custom property in the example shown below), if DNS or DHCP related data exists, etc.



Adding a DNS Host

While viewing the IP Address Inspector, click the + button in the *Related DNS data*.



The **Address** field is automatically filled with the selected IP address. Fill in the other information and click *Create now* or *Add to request*. (See *Workflow Management*.)

Editing a DNS Host

1. In the Inspector, in the ellipsis menu in the *Related DNS data* section click *Edit*.
2. Make the desired changes and click *Save*. The dialog box closes and the details are updated.

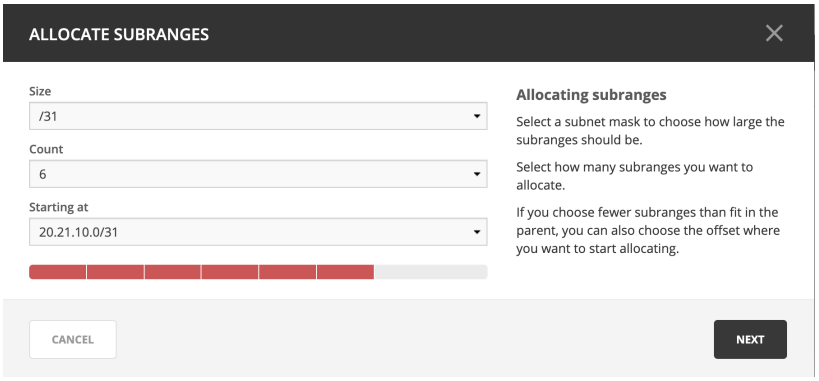
Removing a DNS Host

1. In the Inspector, in the ellipsis menu in the *Related DNS data* section click *Delete*. The host details are deleted and removed from the Inspector.

1.12.9 Split/Allocate Range Wizard

This wizard allows you to create multiple subranges from an existing range. The wizard can only be used on ranges that exist on subnet boundaries and have no subranges already in place.

1. On the **IPAM** page, select the range you'd like to split.
2. On the *Action* menu, select *Allocate subranges*. You can also select this option on the **Row menu (...)**.
3. Configure the new subranges. If you choose fewer subnets that fit in the parent, you can also set the offset from where you want to start allocating. Click *Next* when finished configuring.

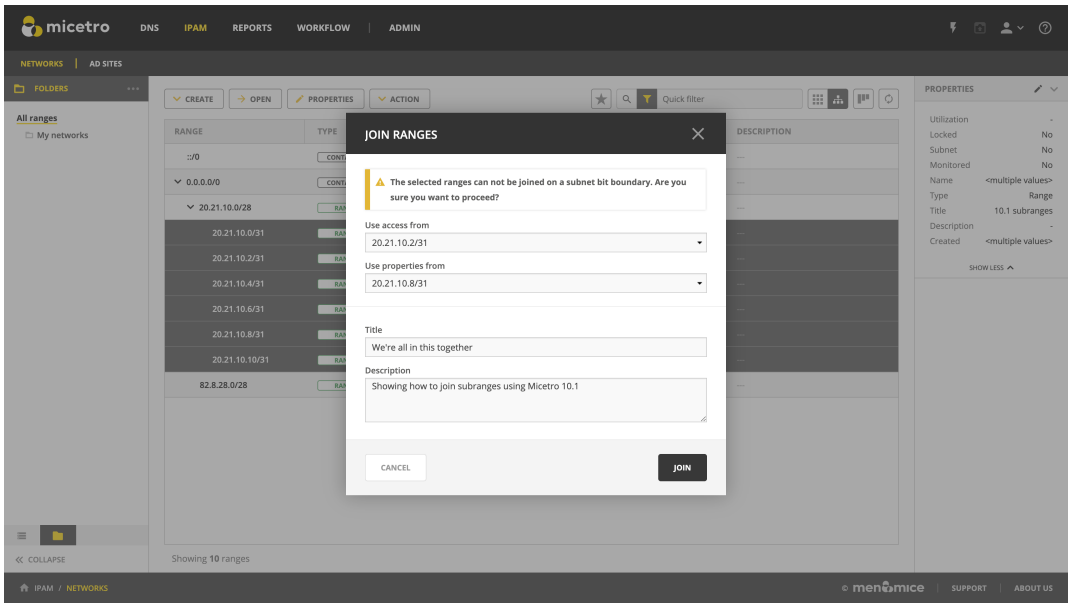


4. Define the title and custom properties for the new subranges. Click *Next* when done.
5. On the summary page verify the new subranges and click *Finish*.

Note: In the web application, the Split Range and Allocate Range wizards are merged together. For information on these wizards in the Management Console, see console-split-range and console-allocate-ranges.

1.12.10 Join Ranges

1. On the **IPAM** page, select the ranges that you want to join.
2. On the *Action* menu, select :guilabel: *Join Ranges*. You can also select this option on the **Row menu (…)**.



3. Set the properties for the joined range:
   - **Use Access from**: Click the drop-down list and specify from which range you will gain access.
   - **Use Properties from**: Click the drop-down list and specify from which range you will use the properties.
   - **Title**: Enter a title for the new range.
   - **Description**: Type a description.
4. Click *Join*.

1.12.11 Host Discovery

With this feature, you can see when hosts were last seen on your network. There are two methods you can use for host discovery – using ping or querying routers for host information.

Configuring Host Discovery Using Ping

1. Select one or more IP ranges.
2. On the *Action* menu, select *Set discovery schedule*. You can also select this option on the **Row menu (…)**.
3. Select the *Enable* option.
   - Frequency: Click the drop-down list and select the frequency (e.g., 1, 2, etc.).
   - Every: Enter the frequency unit for discovery (e.g. days, weeks, etc.).
   - Next run: Select the start date and time.
4. Click *Save*.

Once the schedule options have been set and saved, two columns - Last Seen and Last Known MAC Address - are added to the range grid. The Last Seen column identifies when a host was last seen on the network.

- **Green**: Host responded to the last PING request. The date and time are shown.
- **Orange**: Host has responded in the past, but did not respond to the last PING request. The date and time of last response is shown.
- **Red**: Host has never responded to a PING request. The text Never is shown.

At any time if you wish to disable host discovery, do the following:

1. Select the object(s) for which you want to disable discovery.
2. On the **Row menu (…)**, select *Set discovery schedule*.
3. Uncheck the *Enable* option.
4. Click *Save*.

Configuring Host Discovery by Querying Routers

See *SNMP Profiles*.

1.12.12 Subnet Discovery

The subnet discovery features enables Micetro to obtain information about the subnets on the network through SNMP on the routers. The process is the same as in configuring host discovery, but to enable this feature, make sure the *Synchronize subnets …* is checked in the SNMP profile. See *SNMP Profiles*.

1.12.13 Add to/Remove from Folder

Adds or removes the currently selected IP Address Range from folders.

Danger: Once you remove a range from a folder, there is no "undo" option available.

1. Highlight the range you want to remove.
2. On the **Row menu (…)**, select *Set folder* and add or remove the range from folders.

Set Subnet Monitoring

To change the monitoring settings for a subnet:

1. Select the subnet(s) for which you want to change the monitoring setting.
2. On the *Action* menu, select *Set subnet monitoring*. The Subnet Monitoring dialog box opens.
    - **Enabled**: When selected, the subnet will be monitored.
    - **Script to invoke**: Enter the path of the script to run when the number of free addresses goes below the set threshold. Refer to External Scripts , for information on the script interface and the format for calling the script.
    - **Email addresses**: Enter one or more e-mail addresses (separated by comma, e.g. email@example.com,email@example.net). An e-mail will be sent to the specified addresses when the number of free addresses goes below the set threshold.
- **Dynamic Threshold**: Enter the threshold for the free addresses in a DHCP scope address pool. NOTE: For split scopes and scopes in a superscope (on MS DHCP servers) and address pools using the shared-network feature on ISC DHCP servers, the total number of free addresses in all of the scope instances is used when calculating the number of free addresses.
- **Static Threshold**: Enter the threshold for the free addresses in a subnet.
- **Only perform action once (until fixed)**: When selected, the action is performed only once when the number of free addresses goes below the threshold.
- **Perform action when fixed**: When selected, the action is performed when the number of free addresses is no longer below the threshold.

3. Click *OK* to confirm your settings.

1.12.14 AD Sites and Subnets

Overview

Micetro allows administrators to integrate Active Directory (AD) sites into the IPAM context, view subnets within these sites and add, remove, and move subnets between the sites.

Note: AD sites and subnets integration is only available when Men&Mice Central is running on a Windows server, and it is enabled by default. See *General*.

AD sites are only assigned to and visible in the `Default` address space.

To add/remove a subnet to/from a site, the user must be assigned to a role with the *Edit range properties* permission set and the role applied to the object. See *Access Management* for more details.

AD sites and subnets are displayed in the *IPAM* context:

- subnets in the main *IPAM* → *Networks* grid, along with all other subnets in Micetro (if any). The *AD Site* column displays the site the subnet belongs to.
- sites in a separate *IPAM* → *AD sites* grid, grouped by Forests. The Inspector box on the right displays the subnets (if any) belonging to the selected AD site.

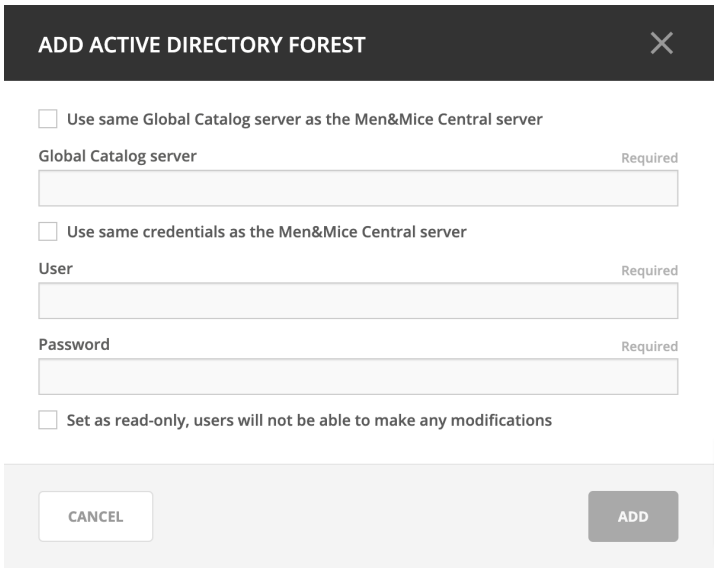
AD Forests

To manage sites and subnets, Micetro needs to be configured with AD Forest(s).

Note: You can manage sites and subnets from multiple forests.

Adding an AD Forest

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Use the *Add Forest* action from the top bar. A dialog box displays.



Use same Global Catalog as the Men&Mice Central server
: If checked, Micetro will use the same Global Catalog server as the Men&Mice Central server is using. If you unselect this checkbox, you must specify the Global Catalog server's FQDN or IP address in the **Global Catalog Server** field.

Global Catalog Server
If you want to specify a Global Catalog server, enter the server's FQDN or IP address in this field. (To unlock this field, the *Use same Global Catalog as the MenMice Central server* checkbox needs to be unchecked.)

Use the same credentials as the Men&Mice Central server
If checked, Micetro uses the same credentials as the Men&Mice Central server when accessing the site information.

User and Password
If you don't want to use the default credentials for the machine running Men&Mice Central, enter the desired user name and password in these fields. (To unlock these fields, the *Use the same credentials as the MenMice Central server* checkbox needs to be unchecked.)

Set as read only
If checked, users will be able to display data from Active Directory, but unable to make any modifications.

3. Click *OK* to save the changes. The forest is added and the sites belonging to the forest are displayed.

Edit AD Forest

To edit an existing AD Forest (to, for example, change the read-only status):

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Select the *Edit AD Forest* action from the top toolbar or the **Row menu (…)**.
3. Update the settings in the dialog box.
4. Click *OK* to save your changes.

Removing an AD Forest

To remove an AD Forest from Micetro:

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Select the AD Forest(s) you want to remove.
3. Select the *Remove AD Forest* action on the top toolbar or the **Row menu (…)**.
4. Click *OK* in the confirmation box to remove the Forest(s).

Reloading the Sites in an AD Forest

Data from AD Forests is synchronized by Men&Mice Central regularly. To manually synchronize forests and reload the data for sites and subnets:

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Select the AD Forest(s) you want to synchronize.
3. Use the *Synchronize* action from the top bar.
4. Click *OK* in the confirmation box to synchronize the Forests.

1.12.15 AD Subnets

View subnets in a site

To view subnets within a specific site:

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Select the AD Forest the site is in, or use the webapp-quick-filter to find it by name.
3. On the *Action* menu, select *View networks*. You can also select this option on the **Row menu (...)**.

This will open the *IPAM → Networks* context with a filter applied to show all subnets that belong to the site.

Note: You can also use the -> *View* button in the Inspector of the selected AD site to open the subnet view.

Moving subnets between AD sites

To add subnet(s) to a site, or move between sites:

1. On the **IPAM** page, select the subnet(s) in the list.
2. Select *Set AD Site* on the *Action* menu or the **Row menu (...)**.
3. Set the (new) AD Site in the dropdown and click *Save*.

Note: Child subnets cannot be moved to a different site than the parent subnet unless the `Enforce site inheritance` checkbox is unchecked in the System Settings dialog box.

Subnets whose AD site settings are inherited from a parent range will have a `<AD Site Name> (inherited)` notation added.

See *General*.

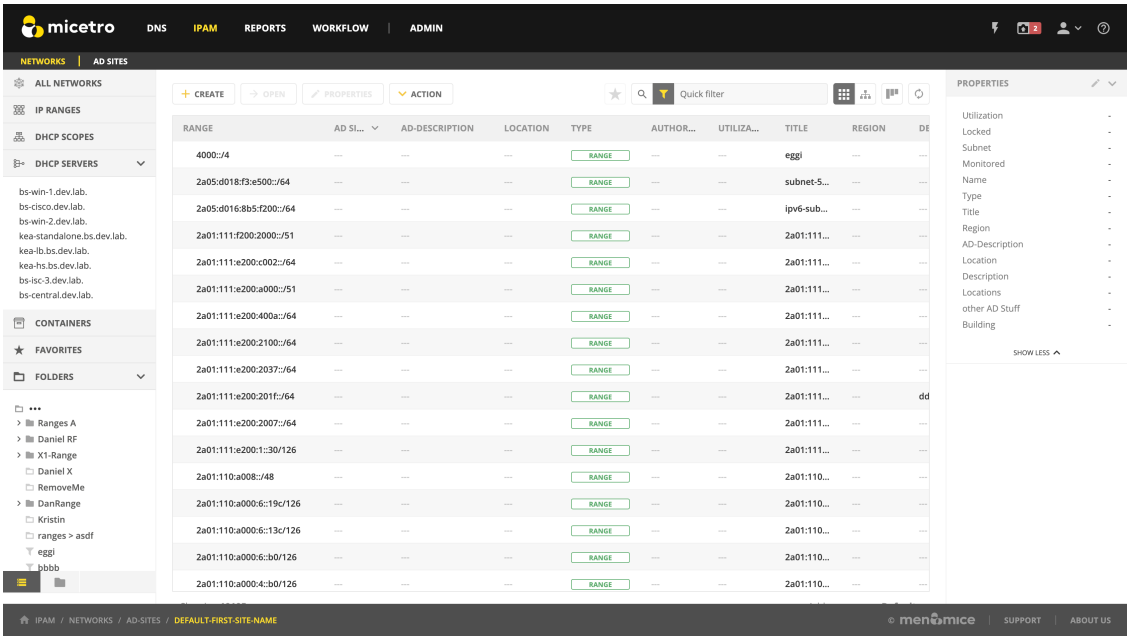
Remove subnet from AD site

1. Select the subnet(s) in the *IPAM → Networks* grid.
2. Select *Remove from AD Site* on the *Action* menu or the **Row menu (...)**.
3. Click *Yes* to confirm the removal.

Subnets outside of sites

To view subnets that don't belong to any AD site:

1. On the **IPAM** page, select *AD sites* in the upper-left corner.
2. Click the `Flat view` button (see webapp-quick-filter) next to the Quick Filter to change the view.
3. Sort the IP address ranges by the **AD Site** column in *ascending* order:



1.13 Folder management

Folder management is an important organizational tool for objects (through *Object folders*) and saved filters (through *Smart folders*).

The list of folders is located in the 'Folders' tab of the webapp-filtering.

Tip: To switch to the 'Folders' tab, click the folder icon on the bottom of the sidebar.

1.13.1 Folders and contexts

Folders are exclusive to their respective contexts, DNS or IPAM. Users cannot place IPAM objects in DNS folders, or vica versa.

Tip: Any object that has been placed in an object folder has an indicator next to its name in the grid. Hovering over the icon will display the name of the folder.

1.13.2 Access to folders

Folders are created globally: only users/groups attached to an Administrator role can create object or smart folders. Folders are visible to all users in the system.

Note: *Objects in folders* are only visible to those that have the correct role to view them. See *Access Management* for details on roles and permissions.

Folders are **not shared** across address spaces and cannot be moved from one address space to another.

1.13.3 Creating folders

1. Locate the parent folder under which you want to create the new folder. (Or the root folder, .)

Note: The "root folder" is called *All zones* in the DNS context and *All ranges* in the IPAM context.

---

2. Click on the ellipsis next to the parent/root folder's name, and select *Create folder* (for *Object folders*) or *Create smart folder* (for *Smart folders*).
3. Fill in the name (for object folders) and the filter query (for smart folders only) and click *Create*.

Note: Folder names don't need to be unique.

1.13.4 Editing folders

You can edit a folder's name or filter query (for smart folder) by clicking *Edit* from its ellipsis menu.

1.13.5 Deleting folders

You can delete a folder by clicking *Delete* from its ellipsis menu.

Warning: Deleting a folder will delete **ALL** subfolders.

1.13.6 Folder types

Object folders

Object folders can group together the following objects:

DNS
: Zones.

IPAM
: Ranges, scopes, and networks.

DNS records and IP addresses cannot be placed in object folders. (But can be filtered with *Smart folders*.)

Note: Objects can be placed in only one object folder.

Access to object folders

See *Access to folders*.

Adding objects to an object folder

1. Select the object(s) you want to add to a folder.
2. Use the Add to folder action from the top bar or the ellipsis menu.
3. Select the folder from the folder tree.

Moving objects between object folders

1. Open the folder in which the item is located. (Or select the object in the grid.)
2. Use the Change folder action from the top bar or the ellipsis menu.
3. Select the new folder from the folder tree.

Removing object from an object folder

1. Open the folder in which the item is located. (Or select the object in the grid.)
2. Use the Remove from folder action from the top bar or the ellipsis menu.
3. Confirm with *Yes*.

Smart folders

Smart folders are saved filters, using the filter query syntax from webapp-quick-filter.

Smart folders can group together the following objects:

DNS
: Zones and records.

IPAM
: Ranges, scopes, containers, and IP addresses.

Note: DNS records and IP addresses can only be filtered with a smart folder placed in the root folder.

Access to smart folders

See *Access to folders*.

Combining smart folders

Smart folders placed inside another smart folder will combine the filtering queries.

Example: user creates a smart folder called *.com TLD** with the filter query `.com` (either in the root folder or inside an object folder). Inside the **.com TLD** smart folder they create another smart folder called *local** with the filter query `authority=example.local.`.

The smart folder *.com TLD* will display all zones that contain the string `.com`, and the smart folder *local* will display all zones that contain the string `.com` **and** whose authority is `example.local.`.

Tip: Using smart folders within smart folders allows you to create powerful and complex filter combinations while preserving each filter element on its own as well.

Object folders are represented by a folder icon (full if there are objects or other folders inside, empty otherwise). Smart folders are represented by a filter icon.

Note: For information on using folders in the Management Console, see console-object-folders and *Saving a Filter*.

1.14 Reports Management

1.14.1 Introduction

Micetro manages vast amounts of DNS, DHCP, and IPAM data. Building reports is easy and can be tailor-made by correlating related data in a few steps, and scheduling the results to be generated daily, weekly or on a custom schedule. There are built-in report definitions that can be used as a reference to build reports. Using custom fields in Micetro further enhances reports by correlating custom fields with the built-in ones. The system then allows you to create reporting definitions that can be run either one time only, or scheduled to run later or at regular intervals.

The reports can be viewed within the Web Application, or downloaded in various formats for further analysis.

When the **Reports** page is opened, you are presented with a list of report definitions. Like every other part of the Web Application, this list can be filtered and searched.

1.14.2 Reporting Module

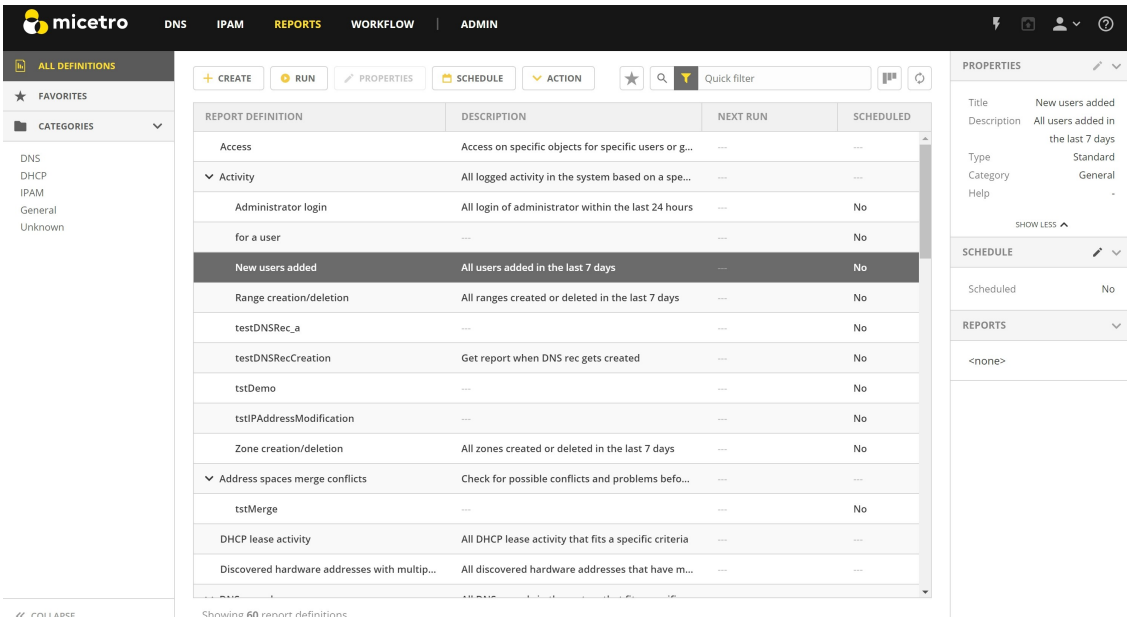
You can:

- create and save new report definitions
- schedule reports to be generated
- run reports
- download reports in various formats

1.14.3 Viewing the Report Definition List

A report definition is a recipe for the actual report. It contains the filter criteria used to build the report, along with scheduling information, and other properties.

The list of report definitions is shown when first opening the **Reports** page.



For help with finding and organizing the reports, use the filtering sidebar on the left-hand side.

All Definitions	Shows all report definitions.
Favorites	Shows report definitions that have been added to favorites. See *Adding a Report Definition to Favorites*.
Categories	Shows all report definitions that belong to a specific category.

1.14.4 Creating a New Report

A new report definition can be created by clicking on the *Create* button above the report list, or by selecting the Create new report in the action list in the Inspector.

With the wizard, you can:

- change the report definition's source
- edit its filter
- select the columns to be included in the output
- and then run the report.

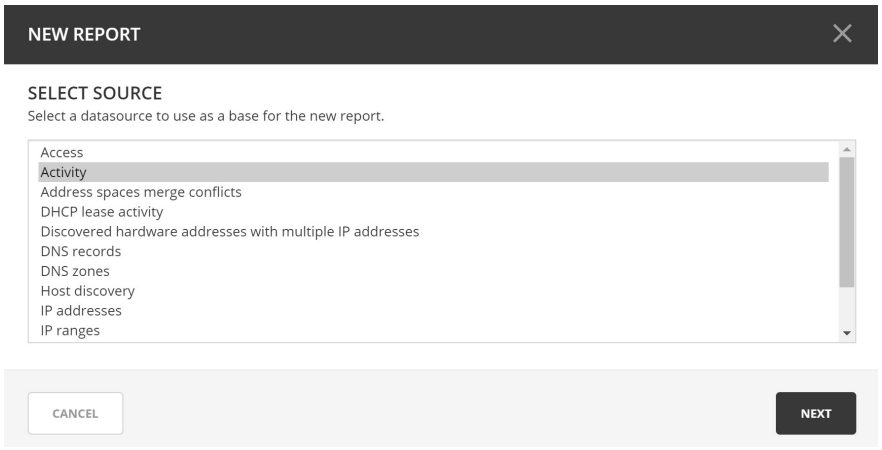
Additionally, it is possible to schedule a report to be generated at specific times or intervals.

After running the report, you are presented with a preview of the results and has the option of saving a copy of the report in a number of different formats. See *Viewing the Report Results*.

A description of each report source is described in *Report Sources*.

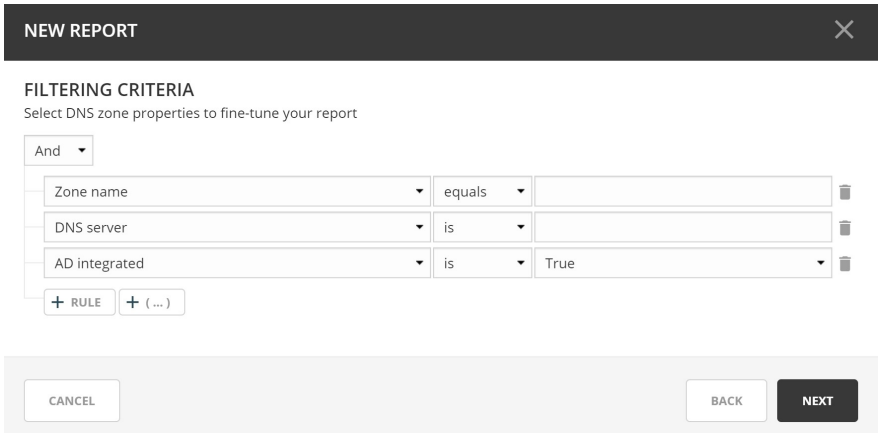
Step 1: Select Source

Select one of the existing reports or a data source as the basis of the new report definition.



Step 2: Edit Filtering Criteria

In the second step, you have the option of editing the filtering criteria. You might want to make some adjustments to the fields in the filter of the selected report definition, for example, extending a time span or selecting a different username. It is also possible to change the filter completely and create a new report definition.



Conditions and Parenthesis

Operator	Description
And	All the conditions have to be met
Or	Sufficient that any of the conditions are met

It is possible to add parenthesis to create sub-conditions with a different operator. The report definition shown in the screenshot above can be read as follows:

> "Last seen must be less than one month ago, lost must be true and either claimed or usage must be true".

This translates into: "*Show me hosts that have not answered during discovery in the last month that are either claimed or in use.*"

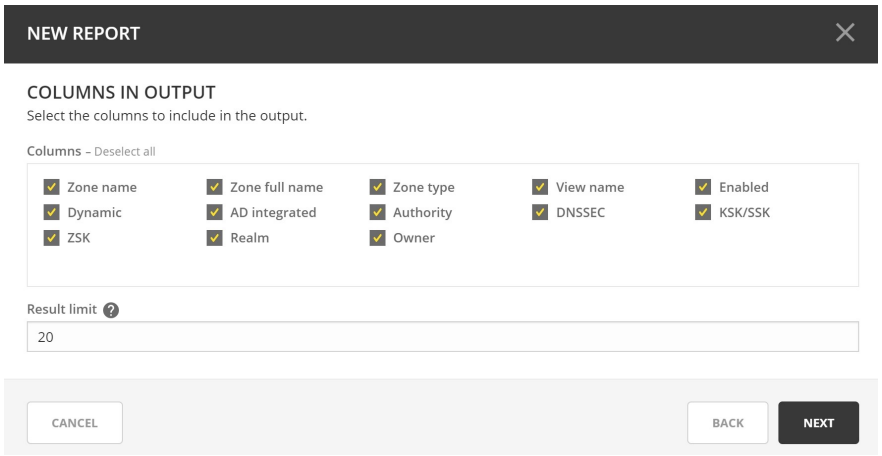
Comparison Operator

Depending on the type of field, you are presented with different comparison operators.

String	Number, timespan, date	Boolean, pick-list, object
equals	=	is
doesn't equal	!=	is not
contains	<	
doesn't contain	>	
starts with	<=	
doesn't start with	>=	
ends with		
doesn't end with		
matches regex		
doesn't match regex		

Step 3: Select Columns

It is possible to select which columns are to be included in the report result.



Note: By default, all available columns are selected.

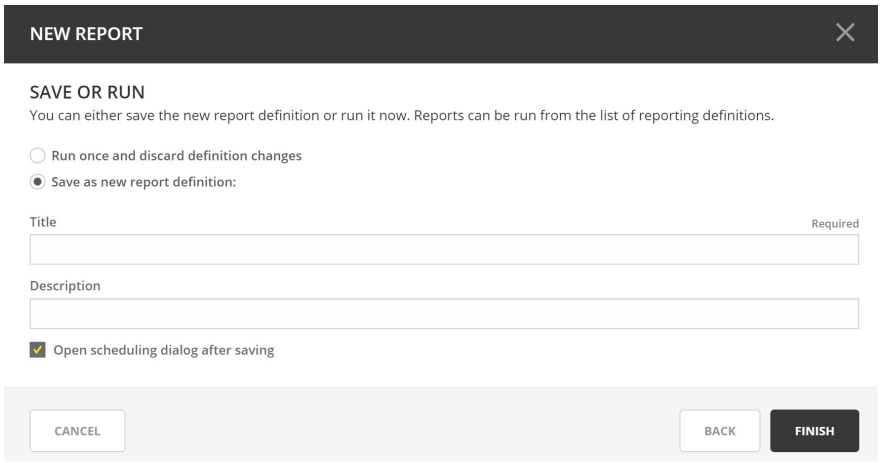
Step 4: Save or Run Report Definition

By selecting *Run once and discard definition changes*, the report definition will not be saved, and you will be presented with a dialog that shows the report results.

By selecting *Open scheduling dialog after saving*, you can schedule periodic executions of the report.

Click *Finish* to run the report and get the results.

Step 5: Schedule



In this step, report generation can be scheduled to run periodically. The frequency and the interval can be specified, and a start date can be set.

For more information, see *Schedule Regular Report Generation*.

Step 6: Run the Report Definition

After the report has been created, it can be generated at any time by selecting the report definition in the list, and then clicking the *Run report* task. (See *Viewing the Report Results*.)

1.14.5 Viewing the Report Results

Viewing the List of Reports

To view a list of all reports that have been generated for a particular reporting definition, double click the reporting definition in the list.

This lists all reports along with how much data is in the report (row count), and how long it took to generate the report (duration).

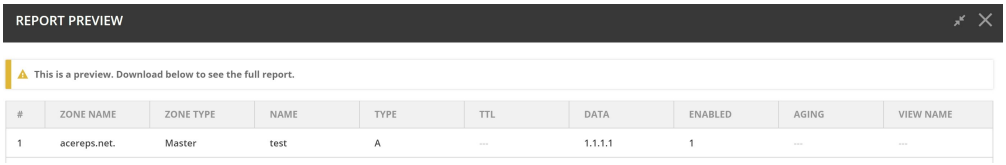
Double clicking on a report in this list allows you to preview a report.

Previewing and Downloading a Report

Previewing the report results can be done in various ways:

- Generating the report instead of saving it after going through the create report wizard.
- Selecting a report definition in the list and clicking the *Run report* task.
- Preview a report result from a scheduled run:
  1. Select a report definition in the list.
  2. Find the "Reports" inspector item.
  3. Find a scheduled run of a report and click on the timestamp or the ellipsis, and then select *Preview* on the menu.

Note: The preview only shows up to the first 150 rows in the report. For the full report it needs to be downloaded.



In all cases, you will be presented with a preview of the report in a separate dialog box. (As shown above.)

The results can then be downloaded by clicking the download button. The drop-down menu offers a number of file formats to select from (ie. CSV, XML, JSON or SYLK).

Tip: Sylk and CSV are handy for importing the data into a spreadsheet application for further processing.

1.14.6 Actions for Reports

In the actions part of the Inspector, the available actions for each selected reports are shown.

Note: In the case of the reporting module not being enabled, the unavailable actions are greyed out.

Run now

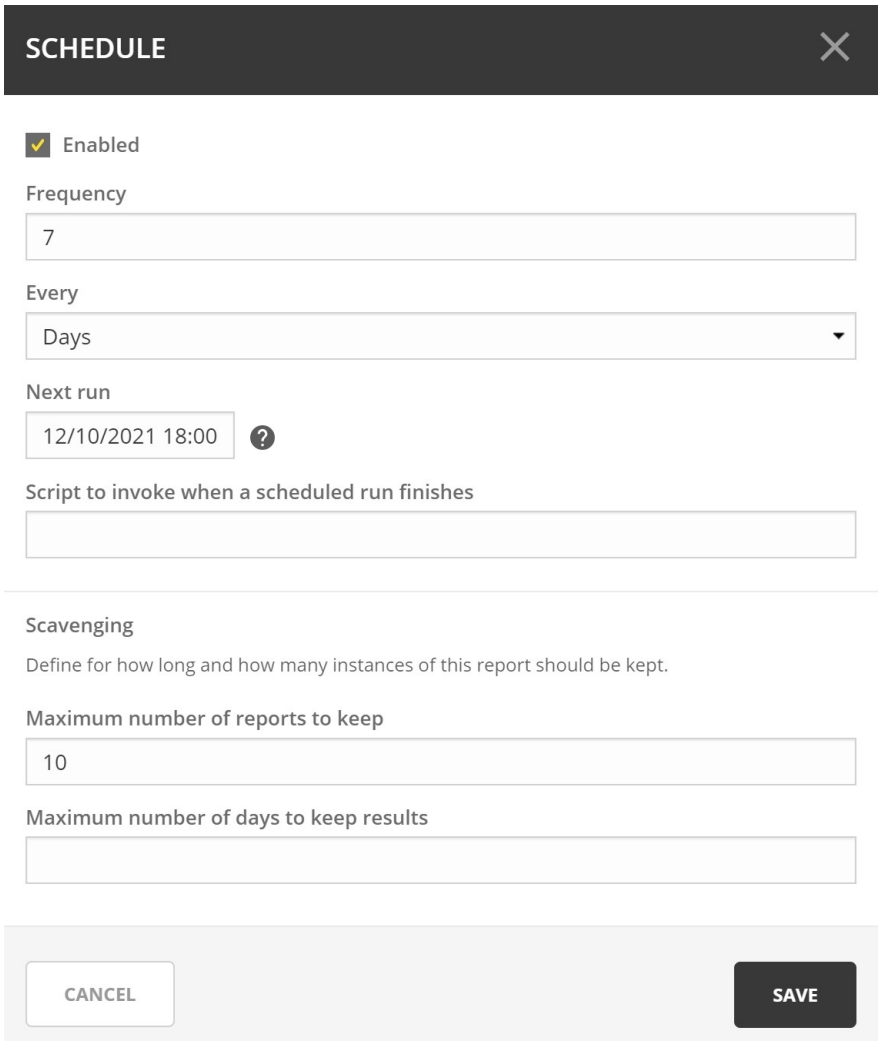
Select a report definition in the list, and then click the Run now action.

A dialog box is displayed showing a preview of the report results. (See *Viewing the Report Results*.)

Schedule Regular Report Generation

In this dialog box a report can be scheduled to be generated at specific intervals. Additionally, it is also possible to specify a path to a script that will be run after the report is generated and also can scavenging be scheduled.

1. Select a report definition in the list, and then click *Schedule*.
2. The following dialog box is shown where scheduling and scavenging can be configured.



Settings for Schedule.

Enabled	When selected, scheduling is enabled for this report
Frequency	Specifies the frequency in which the report is scheduled to run.
Every	Specifies the interval in which the report is scheduled to run.
Starts on	Specifies the starting date for the report to be run on.

By selecting for example '2' and 'Weeks', a new report is generated at the selected start on date/time and then at every 2 weeks afterward.

Note: All dates and times are according to the time zone setting on the Men&Mice Central server.

Settings for Scavenging

Maximum number of reports to keep	Specifies how many reports will be retained in the system. This helps with making sure that disk space does not run out in case many large reports are generated in a small time interval.
Maximum number of days to keep results	Specifies for how many days the reoprts will be retained in the system. This helps with making sure that disk space does not run out in case many large reports are generated in a small time interval.

Duplicate an Existing Report Definition

Use this option to create a new report definition based on an existing one.

1. Select a report definition in the list, and then click *Duplicate*.
2. The create new report wizard will be shown, and you will be allowed to edit the filtering criteria for the new report. (As described in Step 2 in Creating a new report.)

Delete a Report Definition

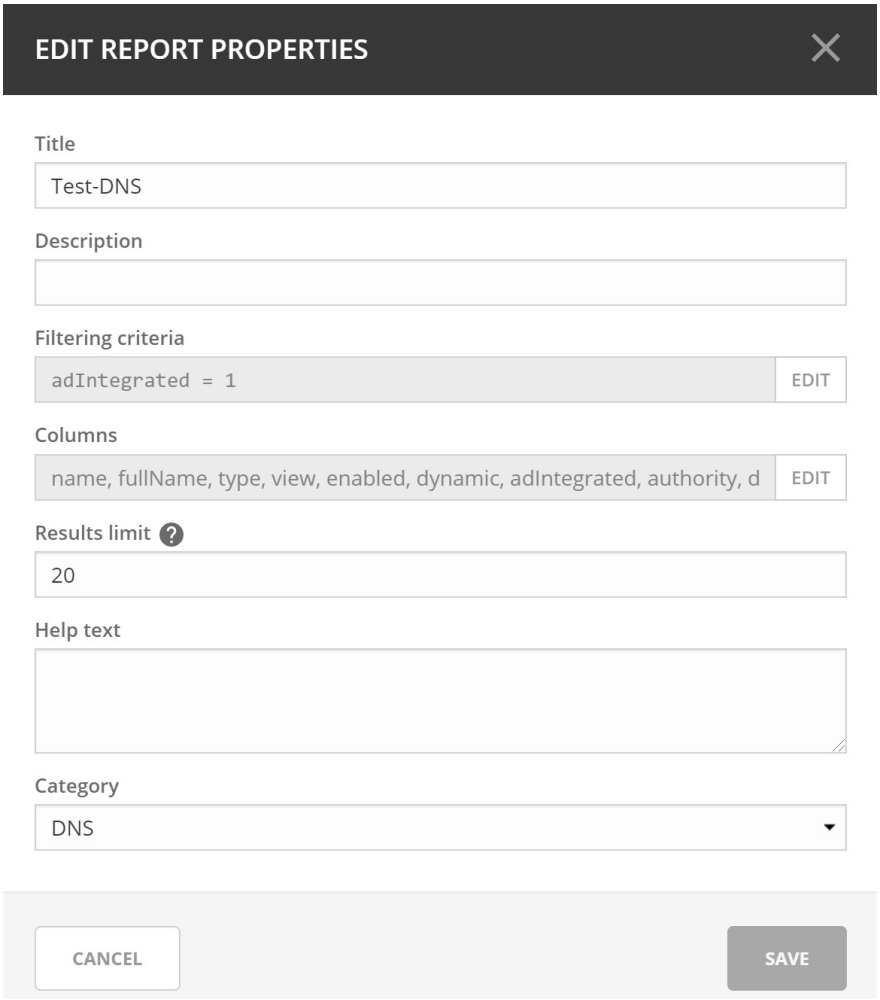
1. Select a user defined report definition in the list, and then click *Delete*.
2. A dialog box is presented prompting you if you want to delete the report definition.

Edit Report Definition Properties

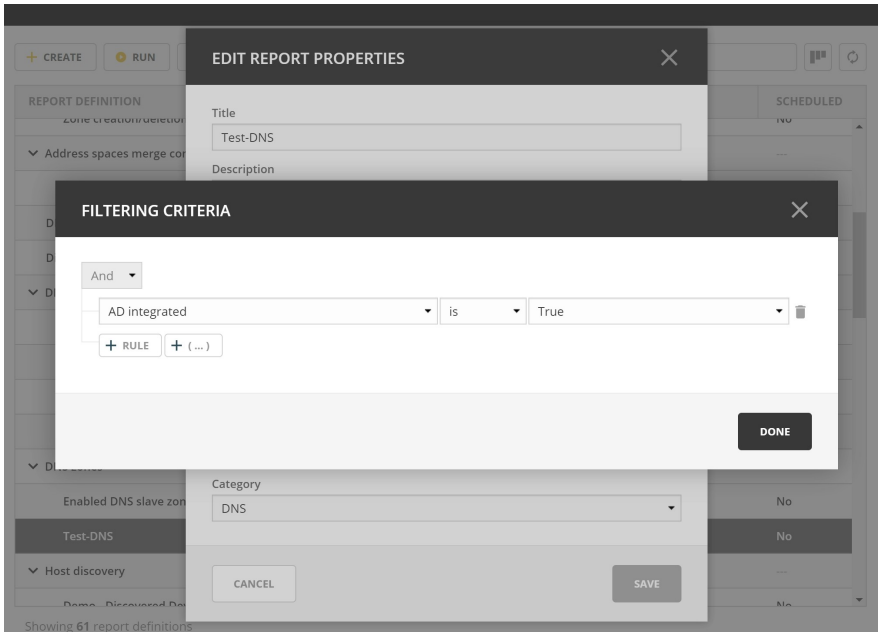
Both the report definition properties, the filtering criteria for the report, and the data columns for the report results can be edited.

Note: Only user created report definitions can be edited.

1. Select a report definition in the list, and then click *Edit report properties*.
2. A dialog box is presented which allows for specifying the properties for the report, along with editing the filtering criteria.



3. Clicking *Edit* for the filtering criteria brings up the following dialog box:



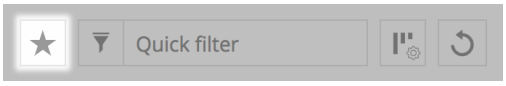
Scavenge Reports

Report results take up disk space on the Men&Mice Central server. The system allows for specifying the maximum number of reports (or the maximum number of days to keep each result) for each report definition. Oldest results are deleted when the limit is reached.

1. Select a report definition in the list, and then click *Scavenge reports*.
2. A dialog box is presented which allows for specifying the properties for scavenging reports.

Adding a Report Definition to Favorites

1. Select a report in the list, and then click *Delete*.
2. Click on the star button to the left of the Quick filter field:



1.14.7 Report Sources

There are 24 reports definitions in the list on the **Reports** page (not counting user defined reports).

12 base report definition sources: sources that either allow you to query one particular object type in the system (for example Activity); or sources that give access to a particular data relation in the system (e.g. Host discovery).

12 derivatives of the base report sources showing the specification possibilities they offer. (Zone creation/deletion building upon Activity and IP reconciliation building upon Host discovery.)

1.14.8 Filter Field Types

String, number	Free text input.
Date and time	Date time string or current time delta shorthand units, e.g. -2w, +1d.
Timespan	Timespan shorthand units, e.g. 24h, 2d, 30m
Object, boolean, options	A dropdown is presented with the available options.

Timespan Formats

```
<num><time unit>
<time unit> ::= s (seconds), m (minutes), h (hours), d (days), w (weeks), M (months), y␣
↪(years)
```

Date Time Formats

General date time format consist of date and/or time (separated by a space).

```
<datetime> ::= <date> <time>
<time> ::= HH:MM[:SS[:TTT]][ AM|PM]
<date> ::= [yy]yy-mm-dd
         | dd.mm.yy[yy]
         | mm/dd/yy[yy]
```

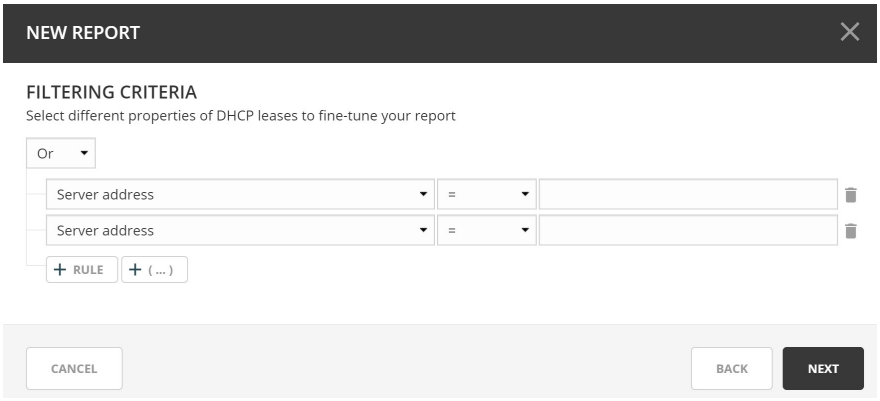
Timestamps formatted according to RFC3339.

```
YYYY-MM-DDTHH:MM:SS[time-secfrac][time-offset]
```

Current time deltas, i.e. a date time relative from now, can also be used.

```
-|+ <num><time unit>
<time unit> ::= s (seconds), m (minutes), h (hours), d (days), w (weeks), M (months), y␣
↪(years)
```

To include more than one value for a particular field the field has to be added again to the filter with an "OR" condition. (For example: the Address records, where the record type field has to be either A or AAAA.)



1.15 Workflow Management

1.15.1 Introduction

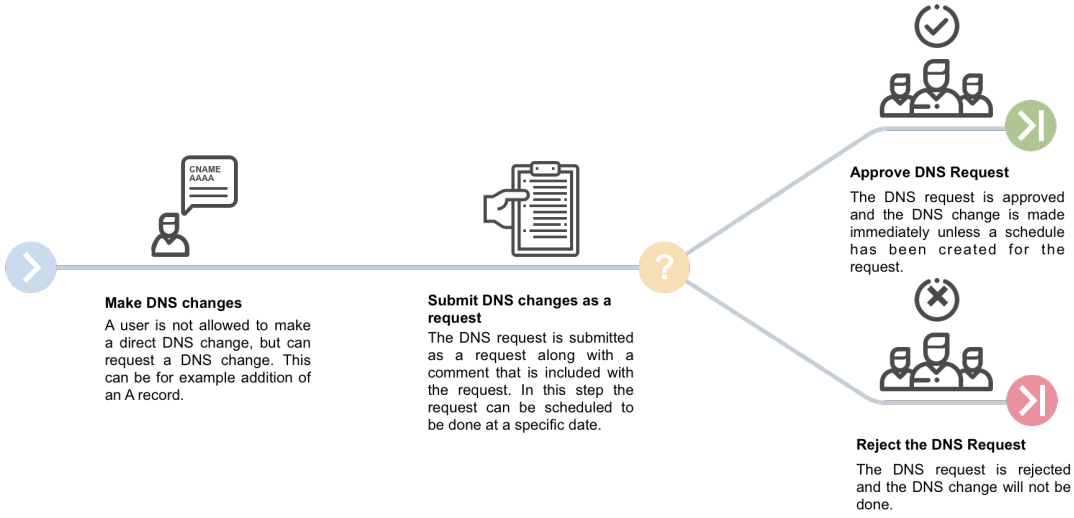
This current version of the Workflow module is focused on DNS changes, so a company can have better control over what changes are done in their DNS infrastructure by approving or rejecting changes. It also helps preventing unintentional changes resulting from human error.

Organizations can give users access within the organization and the ability to request DNS changes, in some or all of the DNS zones available in the organization.

The Workflow module allows the user to submit 'change requests' for creating, modifying, or deleting DNS records:

1. The user makes a change in DNS. This can be adding a new DNS record, or modifying or deleting an existing DNS record. Instead of saving the changes or creating the DNS record immediately, users with limited access have an option of creating a request to approve the change.
2. The request is created and can, be submitted for approval by users with necessary access.

3. User with permission of approving DNS requests can view a list of requests.
4. The request can be either approved or rejected. If the request is approved, the DNS change is made and the DNS zone is updated automatically with the new data, either immediately or at a time specified in the request. If the DNS request is rejected, the request is deleted and the DNS request history will indicate a reason for the rejection.



1.15.2 Getting Started

In order to use the DNS requests, the Workflow module needs to be purchased and enabled. For information about how to add license keys, see *License Management*.

In order to use the Workflow module, two new workflow specific roles in Access Management, “Requesters” and “Approvers”, need to be set. Users have to be added to the “Requesters” role to be able to submit requests. Administrative users have to be added to the “Approvers” role to be able to see and approve requests made by others.

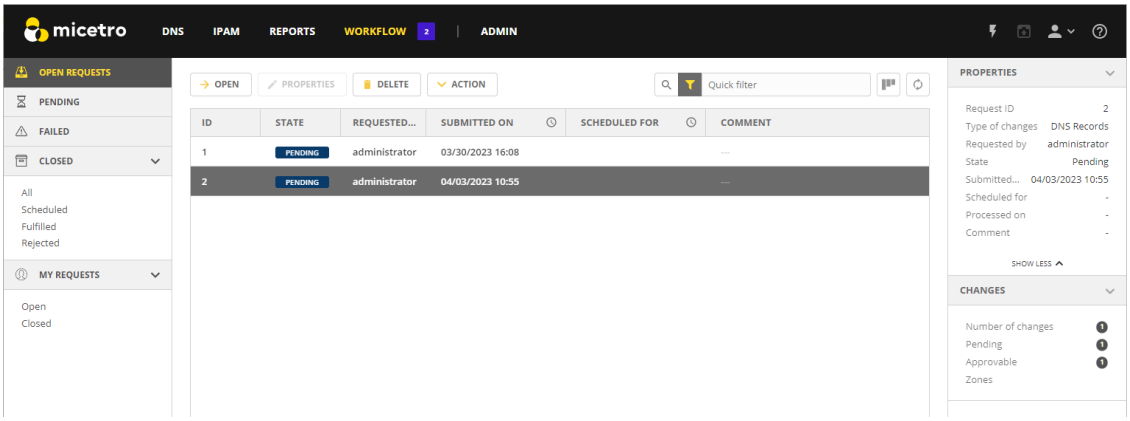
In addition, Approvers are only able to approve requests that involve DNS Zones in which they have access to edit records.

Requesters also need basic read-only access to the DNS Zones (and the containing DNS server) to be able to request changes, as well as the IP address ranges (to find available IP addresses).

1.15.3 Overview of DNS Requests in the System

When the Workflow module license key has been added and enabled, a new top menu item is visible.

Open Requests shows an overview of the change requests in the system. An icon in the upper-right corenr indicates how many pending changes are in the queue. Clicking the icon displays a dialog box for submitting those changes as a request. c



1.15.4 Filtering Sidebar

The filtering sidebar has the following options for open DNS requests:

Pending	Lists all DNS requests that are pending approval or rejection
Failed	Lists all DNS requests that encountered an error while being applied to the DNS servers
Closed	Lists all requests that are closed and have been either **Scheduled**, **Fulfilled**, or **Rejected**
My requests	Lists all requests for the current logged in users that are either **Open** or **Closed**.

1.15.5 Actions

The following actions can be performed for a selected request in the list.

Open request	Opens the request in a dialog where changes in it can be viewed and either approved or rejected
Edit request properties	Opens up a dialog where the properties for the request can be edited, if custom properties for Change Requests have been defined
Delete request	Allows for canceling the selected request
View history	Allows for viewing the history of the selected request

1.15.6 Inspector

The following items are listed in the Inspector's Properties section for a selected request in the list.

Request ID	The ID of the selected request
Type of changes	Currently only DNS Records
Requested by	Username of user that submitted the selected request
State	The current state of the request. Either Pending, Approved (i.e. awaiting scheduling), Rejected, Failed or Applied
Submitted on	Date the request was submitted
Schedule for	Date the request should be fulfilled on
Processed on	Date the request was fully approved and applied
Comment	An optional comment the user provided when submitting the request

1.15.7 Creating a DNS Request

In order to create a DNS request, one of the following can be done:

- Create a DNS record
- Edit a DNS record
- Delete a DNS record

Additional options are available when creating, editing, or removing a DNS record.

Note: Access restrictions will affect which users have these options available.

Authorized users and approvers can also submit change requests, even if they have full access, in order to make scheduled changes.

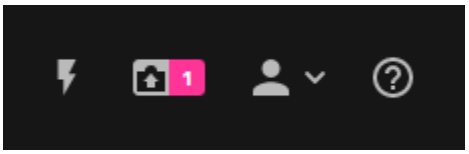
Add to request	Adds the changes to a DNS request. Number in badge on request queue icon in top right corner will increase accordingly
Save now / Delete now	DNS changes are applied immediately to DNS server(s)

Note: After a DNS request for a DNS change has been created, the corresponding IP address will be set in to a pending state and will not be available, for example when requesting the next Free IP address in the subnet.

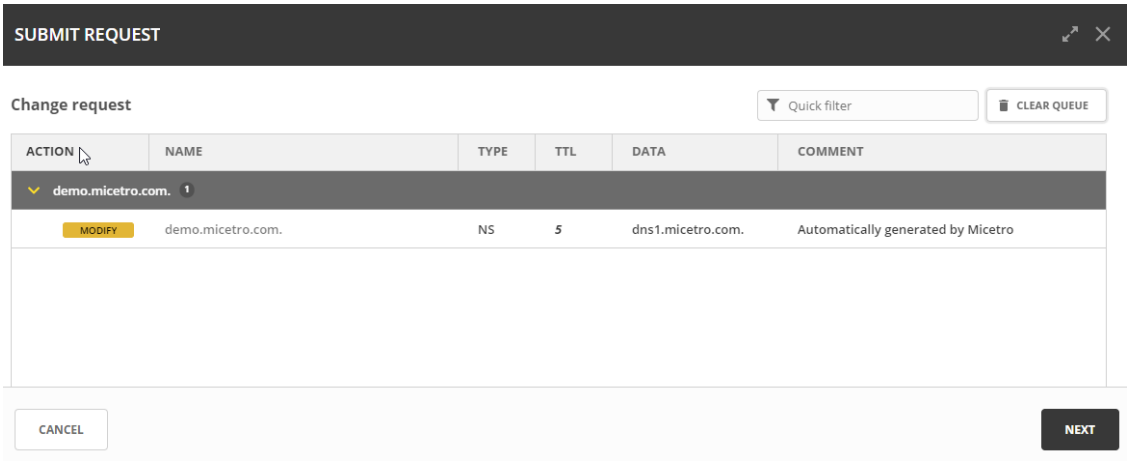
1.15.8 Submitting a Cange Request

Step 1: Open the pending request.

Open the pending request by clicking on the request queue icon in the top menu.



The following dialog box is displayed, where the user can review the DNS changes to submit or remove a DNS change from the queue.

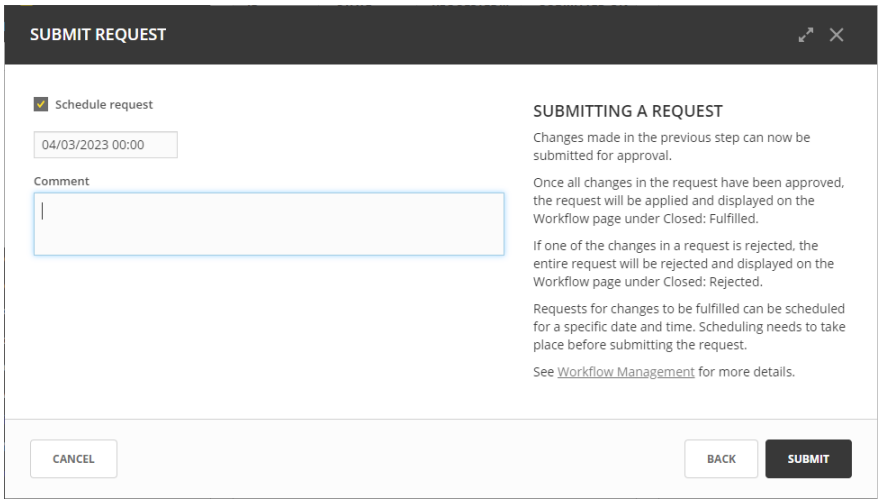


Step 2: Scheduling

If the user want to make a scheduled change (i.e. the records are applied to the DNS server at a specific date and time), they need to select *Schedule request*, and provide the date and time.

Additionally, if custom properties have been defined for Change Requests, the user will be asked to enter those here, along with the optional Comment.

Note: All dates and times are according to the time zone setting on the Men&Mice Central server.

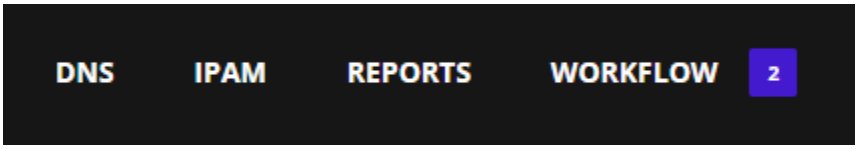


Step 3: Submit the request

Clicking *Submit* will submit the request which is followed by an indication of a successful submission, along with the ID (request number) for the request.

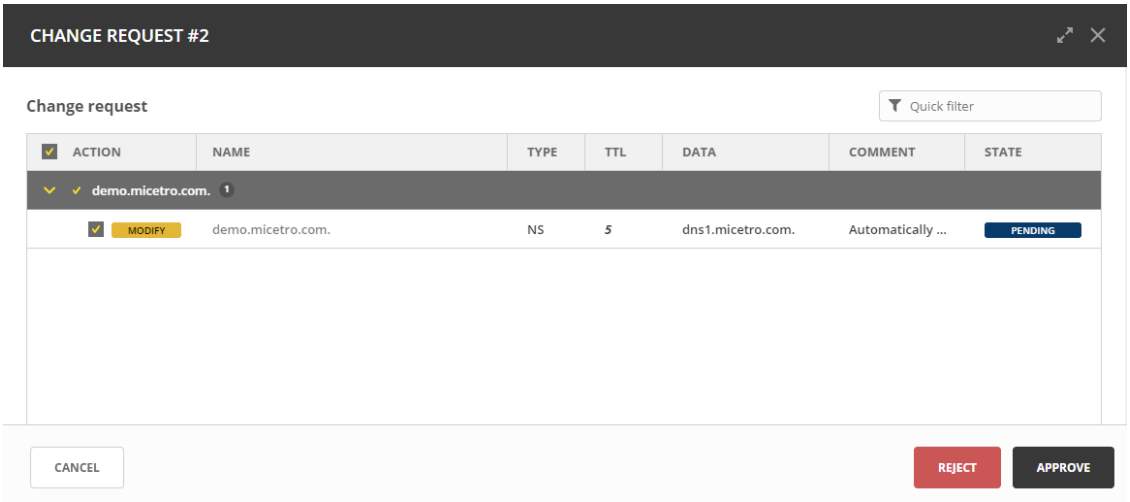
1.15.9 Approving or Rejecting a Change Request

Pending requests are indicated in the top menu.



Selecting *Workflow* in the top menu displays the Workflow page with an overview of all requests that the user has access to view.

Double clicking a pending request opens up the approval dialog box:



The approval dialog box shows the request to be approved or rejected, as well the following details:

Action	Indicates what action is being performed: Add, Modify, or Remove
Name	The fully qualified DNS record name
Type	The DNS record type
TTL	The Time To Live of the DNS record
Data	The data being added. Hovering over the field shows the previous value, if being modified
State	The state of the change request

After clicking *Approve*, the request is approved, and the data propagated accordingly.

If the user clicks *Reject*, they are prompted for a comment and then the request and all changes within the request is rejected.

1.16 Viewing Change History

Permissions:

- Permission: `Access to view history` on Micetro.
- Role: `Administrator (built-in)`

Note: For information about how to view object change history in the Management Console, see *Object Change History*.

You can see a log of all changes made to any object, including the date and time of the change, the name of the user who made it, actions taken, and any comments entered by the user.

All users can view their own object change history, while administrators can see the history of all users.

You can view the history of a specific object or all objects.

To view your own changes:

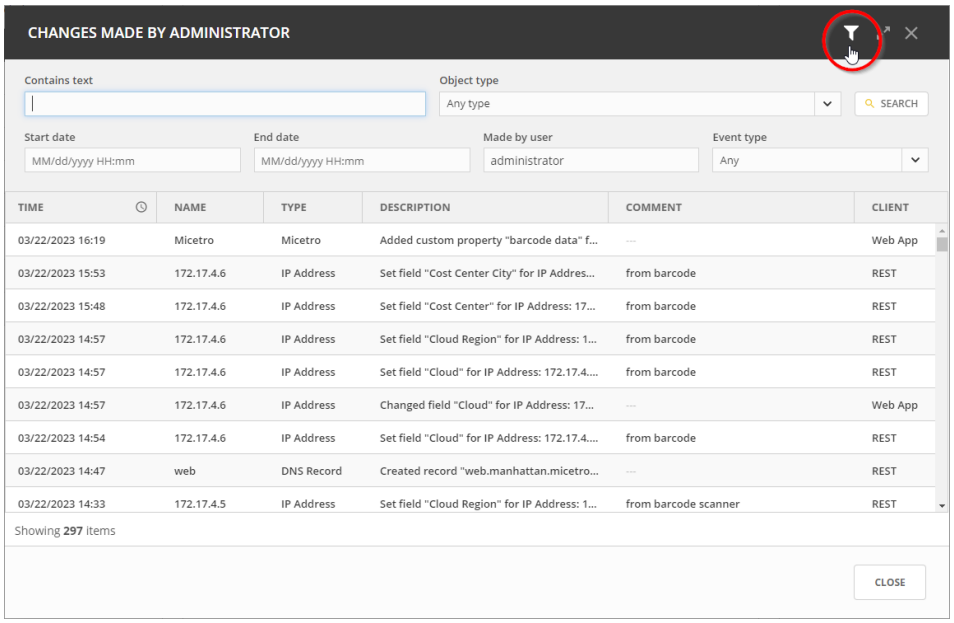
1. Click the User icon in the upper-right corner.
2. Select *View history*.

To view changes to a specific object:

1. Select the object you want to view.
2. On the *Action* menu, select *View history*. You can also select this option on the **Row menu (...)**.

To filter data in the Change History window:

1. Click the filter icon in the top right corner.
2. Enter/select the relevant information and click *Search*.



- If you're viewing global object history, you can select an object type to narrow down the results.
- Administrators have the option to enter a username in the *Made by user* box to view changes by specific users.

1.17 Management Console

Note: Migrating features from the Management Console to the Web Interface is ongoing, and new features are not added to the Console.

1.17.1 Overview

Prior to starting the Men&Mice Management Console, make sure that you have installed and started the other Micetro components, as applicable. For more information about other components, see *Implementation Guide*.

The Men&Mice Management Console is a rich, Windows-only application that boasts a very intuitive interface. It is a central organizational tool of Micetro and provides all the tools you need to oversee the management of your DNS and DHCP servers and IP Addresses.

From the Management Console, you can simultaneously manage DHCP/DNS servers on any supported platform.

Note: Be aware that you will only be able to view the servers to which you have access. The administrator user has access to all servers.

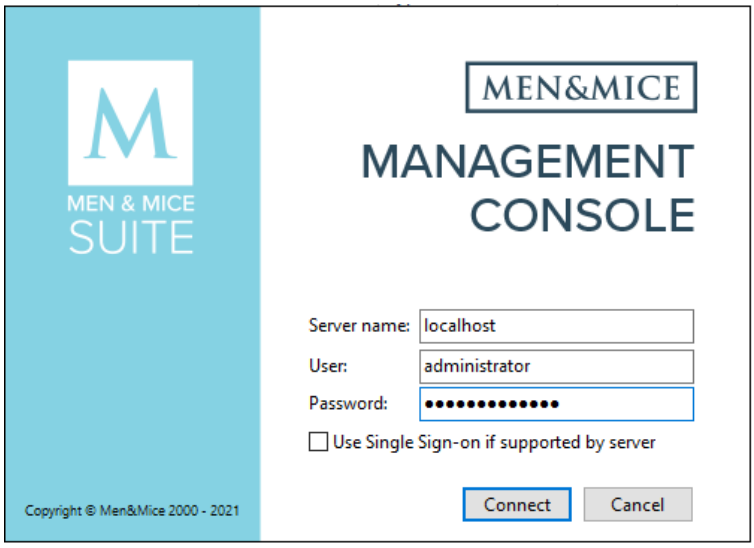
1.17.2 Launching the Management Console

When logging into the Men&Mice Management Console, you have the option to choose "Single Sign-on." This allows those users working on a Microsoft Network with Active Directory to sign on one time only to access all your resources.

Note: If you are the system administrator, you can choose whether to enable this option. On the *Tools* menu, select *System Settings*. On the *General* tab, select the *Allow Single Sign-on* checkbox to enable this option. Then click *OK*.

To start the Management Console:

1. Locate and launch the Men&Mice Management Console. The Men&Mice Management Console login dialog box displays.



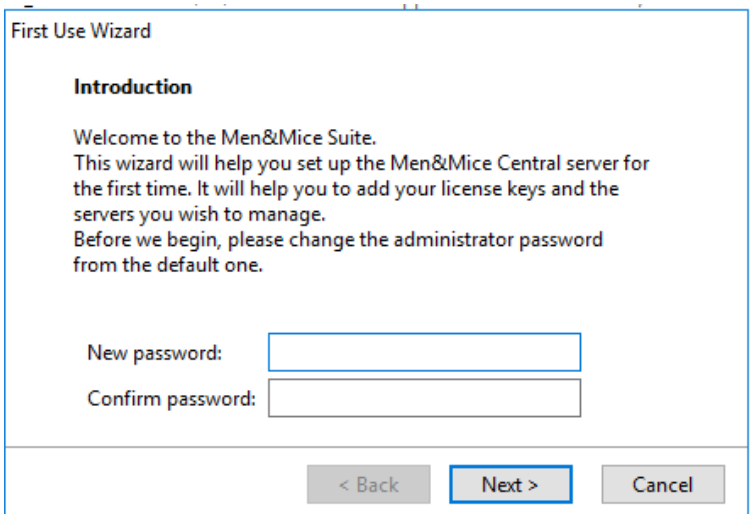
2. In the **Server name** field, enter the name or IP Address (IPv4 or IPv6) of the workstation on which Men&Mice Central is running. This is only required the first time you log in. After a successful connection, this field will be pre-filled with the server name you enter.
3. In the **User** and **Password** fields, enter the applicable information. The default value for both fields is `administrator`.
4. If you want to enable Single Sign-on, select the checkbox.
5. Click *Connect*. If this is the first time any user logs into this particular Men&Mice Central, the first-use-wizard launches. Otherwise, within a few moments, the Men&Mice Management Console will start, and the Manager window will be displayed.

1.17.3 First Use Wizard

The First Use Wizard opens when you connect the Management Console to a newly installed instance of Men&Mice Central or log in for the first time. The wizard is able to discover:

- DNS Servers
- DHCP Server
- AD Subnets

1. Log in using the default credentials (administrator:administrator). Enter a new password for the administrator user, and then click *Next*.

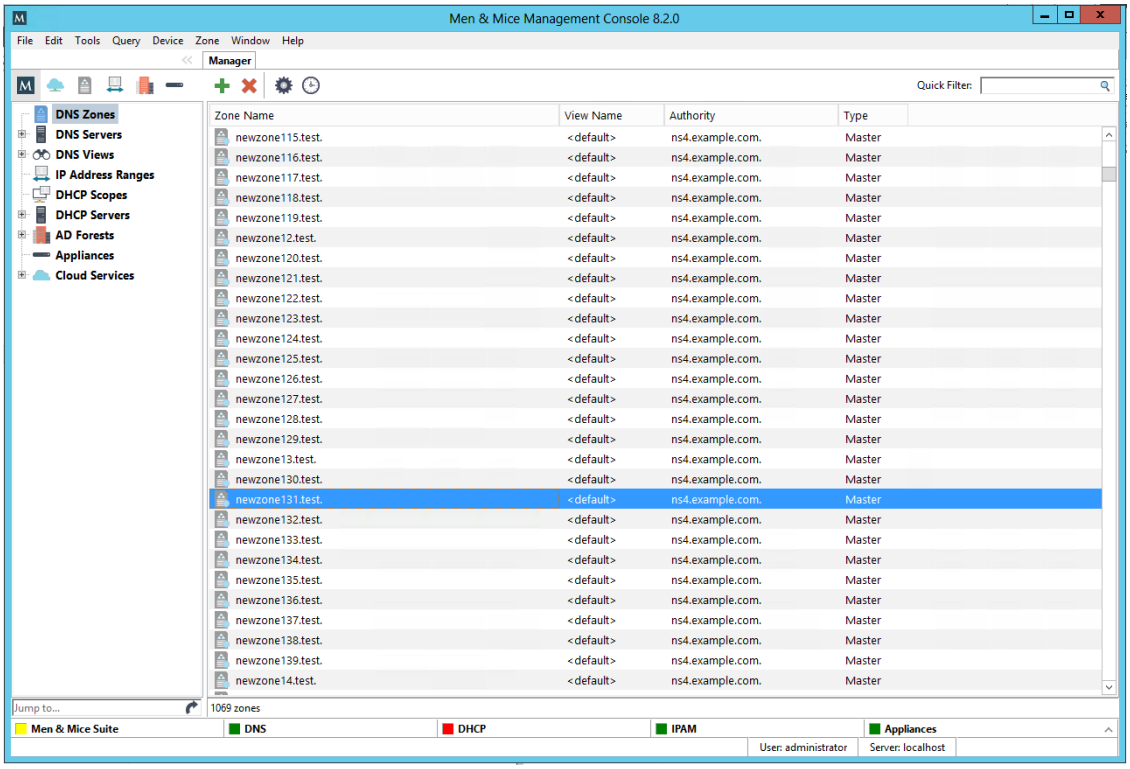


2. Follow the instructions to complete each page, and then click *Finish*.

1.17.4 Console Features and Tasks

Management Console Interface

When the Management Console is started up, the *Manager Window* displays in the center. This window is the heart of the Men&Mice Management Console, providing a single interface with nearly every feature in Micetro.



This window consists of two main areas: the *Object Browser* and the *Detail View*.

Object Browser

The *Object Browser* displays on the left side of the Manager window and contains categories of objects that can be created, modified, and deleted.

Tip: A new feature in version 8.2 is the ability to filter by the type of object in the Object Browser. By clicking on the respective icon at the top of the Object Browser, the Object Browser will show only that type of object. Clicking on the "M" icon to the left will show all types of objects. Note that this applies only to Clouds, DNS, IPAM (Subnets and DHCP), AD Forests and Appliances.

DNS Zones
: Selecting the DNS Zones object will cause the Detail View to display all DNS zones configured in the system and accessible to the current user. This category is accessible with a valid DNS Module License Key.

DNS Servers
: Selecting the DNS Servers category will cause the Detail View to display all DNS servers managed by the system and accessible to the current user. If a DNS server is not reachable, its icon is shown with an exclamation mark. If the DNS Servers category is expanded, the same list of servers will show as sub-categories to the DNS Servers

category. Selecting a server subcategory will cause the Detail View to display the zones managed by that server and accessible to the current user. This category is accessible with a valid DNS Module License Key.

DNS Views

The DNS Views category allows you to see zones on DNS servers that are configured with multiple views. If no views are configured on any server, this category will not appear. The Views feature of the BIND name server allows one server to return different data to different clients; each view has its own separate list of zones, often with the same names. This category behaves similarly to the DNS Servers category.

IP Address Ranges

Selecting the IP Address Ranges category will cause the Detail View to display all IP Address Ranges configured in the system and accessible to the current user. This category is accessible with a valid IP Address Management Module License Key.

DHCP Scopes

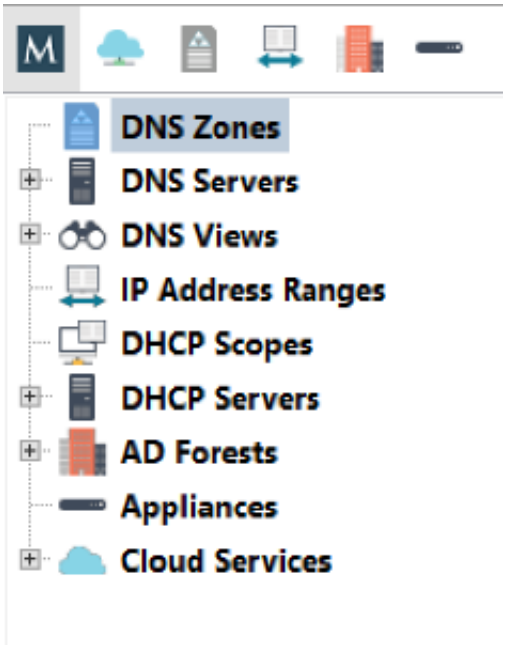
Selecting the DHCP Scopes category will cause the Detail View to display all DHCP scopes configured in the system and accessible to the current user. This category is accessible with a valid DHCP Module License Key.

DHCP Servers

Selecting the DHCP Servers category causes the Detail View to display all DHCP servers managed by the system and accessible to the current user. If a DHCP server is not reachable, its icon is shown with an exclamation mark. If the DHCP Servers category is expanded, the same list of servers will show as sub-categories to the DHCP Servers category. Selecting a server subcategory causes the Detail View to display the scopes managed by that server and accessible to the current user. This category is accessible with a valid DHCP Module License Key.

AD Sites

This category is only displayed if you have enabled *AD Sites and Subnets* integration. Selecting this category will show all AD sites that have been selected for integration in Micetro.



Detail View

Note: A new feature in version 7.2 is that the windows are now 'docked' and therefore they open up in a tab instead of a window.

The *Detail View* displays on the right side of the Manager window and displays the contents of the selected category in the Object Browser. While in this view, you can do the following:

Sort and filter
to allow a more concise view of the contents. Refer to quickfilter.

Display a shortcut or "context" menu
that gives access to other options. Right-click to view this shortcut menu.

Open an object by simply double-clicking
This opens either a property window (such as in the case of DNS/DHCP Servers), or brings you to a new view of the data contained within the object (such as in the case of DNS Zones, DHCP Zones, and IP Address Ranges).

Reorder the columns
Click on the column you want to move and, while holding down the mouse key, drag the column to the new position.

Display or hide columns
Right-click on a column header. All the column names shown with a checkmark are currently displayed. To hide a column, click on the name to remove the checkmark. To display a hidden column, repeat the process. Reset all makes all columns display without having to unhide them individually.

Sorting Records

When viewing information in the Object List – be it DNS zones, Servers, Views, IP Address Ranges, or Scopes – you can instantly sort the displayed information by clicking on the header of any column shown in that view. For instance, click on the *Name* header once to sort the displayed objects alphabetically (A-Z) by name. Clicking on the *Name* header again will resort the list in reverse alphabetic order (Z-A). This can be done with any column of data, including Servers, Addresses, Utilization percentages, etc.

Note: When sorting zone names alphabetically, reverse zones will appear at the bottom of the list (after Z), or at the top of the list when sorted in reverse alphabetic order.

Menu Bars

The *Menu Bar* in the Men&Mice Management Console provides access to nearly all of the program's functionality.

Important: You must have sufficient access privileges in order to use some of the menu items discussed below.

Note: Not every menu option is listed below. Some are detailed in their respective sections. Some of the options discussed below are global across the whole application (e.g., Cut, Copy, and Paste).

File Menu

Save
Saves any changes that have been made in the currently active window. This is only available when a zone has been edited and there is some new data to be saved.

Change Password
Use this command to change your login password to the Management Console. Your current password is required in order to change to a new one.

Page Setup
Opens the Print Setup dialog box, from which you can choose the default printer, paper, page orientation, and other properties to be used when printing from Management Console.

Print
Opens the Print dialog box and allows you to print the contents of the currently selected Zone window. This command is only available when a Zone window is open.

Exit
Closes the Management Console window.

Edit Menu

The commands available from the Edit menu vary, depending on what is currently selected in the Management Console. When working in the Manager window the following functions are offered:

Undo
Reverses the last edits that you made, in the reverse-order that you made them.

Redo
Reverses the effects of the last Undo command.

Cut Removes the currently selected item(s) and stores them in the Windows clipboard.

Copy
Makes a copy of the currently selected item(s) and places it into the Windows clipboard.

Paste
Copies the contents of the clipboard at the location of the insertion point.

Paste Custom Properties
Allows pasting of custom property contents into multiple objects. To use this command, select one object and choose Copy. Then select the objects whose custom properties you want to populate and choose Paste Properties. This will open a dialog box where you can choose which custom properties you want to paste.

Clear
Deletes the currently selected text or record.

Select All
This command selects all of the objects (e.g., zones, servers, scopes, IP Address ranges).

Find
This command initiates a new search.

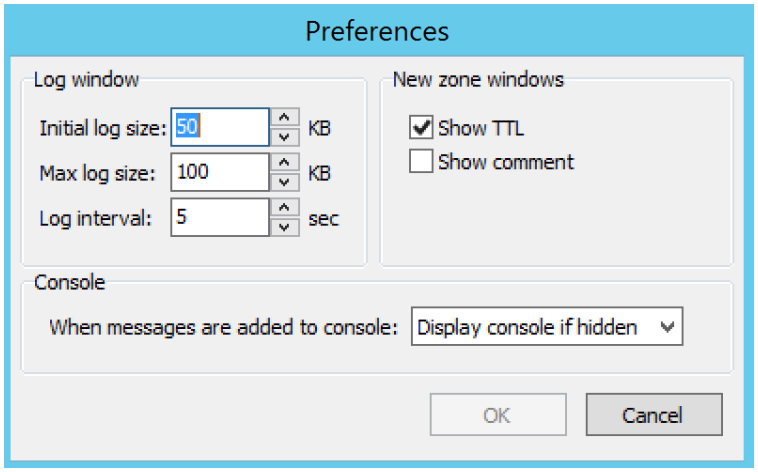
Find Next
This command repeats the last search you performed. For example, if the last search was for A, this automatically locates the next occurrence of A in the object list.

Save Filter/Delete Filter
It is possible to save/delete filters for various object types. Saved filters appear in the list on the left hand side of

the Manager Window and in the Create Zone dialog box. Filters can be local or global in scope. Filters created by the Administrator are global and visible to all users. Filters created by any other user are visible only to that user.

Preferences

Opens the Options dialog box where you can make default selections for various Management Console functions.



When working with a zone, the Edit menu changes and includes additional functions.

Enable Record

Makes the currently selected record(s) active in the zone. Use this command to re-enable a zone that has been disabled. All records are active by default unless they have been manually disabled. You cannot enable records in dynamic zones.

Disable Record

Makes the currently selected record inactive. When a record is disabled, it is ignored in the zone. You cannot disable records in dynamic zones.

Insert Record

Opens a popup menu that lets you specify the type of record you want to create. To insert A, CNAME, MX, NS, or PTR records, choose the corresponding option from the menu. The new record is created directly below the currently selected record or field. For other types of records, select Insert Record. This creates a new blank row above the currently selected record or field.

Duplicate Record

Creates a copy of the selected record(s). The new records appear directly underneath the last record being duplicated.

Delete Record

Deletes the entire record from the zone. Unlike the Clear command, the entire record does not need to be selected for this command to work. It will delete the entire record in which the cursor is currently located.

Show TTL

This menu command can be toggled on and off by selecting it repeatedly. This option is enabled by default. If you disable this option, the TTL column will not be displayed in the zone window. This command is only available when a zone window is open and active.

Show Comment

This menu command can be toggled on and off by selecting it repeatedly. This option is enabled by default. If you disable this option, the Comment column will not be displayed in the zone windows. This command is only available when a Zone window is open and active. This command can only be used for static zones.

Query Menu

Lease History
This function can be enabled through System Settings, Logging. When enabled you can search the DHCP lease history and if desired, export the search results to a file.

Object History
Allows you to query the history throughout the system for all objects or a specific object. Refer to Object Change History for details. You can search all objects or, using the Only show objects of type drop-down list, you can select which object type to search. You can only search all object types or one selected object type.

Men&Mice Suite Log
Displays log messages for Micetro.

Search and Update Wizard
Launches the Search and Update Wizard, a utility that allows you to find, create, modify, or delete records in multiple zones and DHCP Scopes using a single action. Click Next> and follow the instructions onscreen to specify the type of records you want to search, the action you want to perform (e.g., create, replace, delete, edit), etc.

User Activity
Users with user administrative privileges can see this menu item. Selecting this menu item displays a window that shows a list of all users including the user name, authentication type, login status, and last login time.

Window Menu

Cascade
Aligns all currently open windows inside the Console window so that they overlap, showing only their title bars. This allows you to access all currently open windows.

Show Progress
This window shows the progress of operation that can take some time, such as opening and saving large zones. When an operation is in progress (and displayed in the progress window) it can be cancelled by clicking in the progress window and choosing Cancel.

Show Console
Displays errors that may occur during various operations.

Show Manager Window
Displays the Manager Window. Use this function in the event you inadvertently close the Manager window.

Revert to Standard Layout
Returns the program to its standard view, with the Management Console open and the main window displayed on top of any other open windows. Other windows are not affected by this command. Also, shows the progress window if the window is hidden.

Active Window List
At the bottom of the Window menu, there will be a list of every window currently open in the Management Console. You can instantly give a window the focus (i.e., bring it to the top) by selecting it from this list.

Help Menu

Help
Launches the on-line help features of Micetro.

About Men&Mice Management Console
Opens the About window, which contains the full version number of the Men&Mice Management Console that you are running.

Toolbars

The toolbar, which runs along the top of the *Object Section* and *Object List*, provides fast access to commonly performed operations. The function of any given button is always in the context of the currently selected object. Some buttons will not be available (i.e., greyed out) when certain objects are selected.

Button	Name	Description
	**Create**	Lets you create a zone, add a name server, a DHCP scope, or a DHCP server based on the currently selected object.
	**Delete**	Lets you delete a zone, a name server, a DHCP scope, or a DHCP server; based on the currently selected object.
	**Options**	Display the options dialog box for the currently selected object, if applicable (e.g., Zone options, Server options, etc.).
	**Server Info**	Displays a window that provides general information about the selected server—e.g., server type, IP Address, OS, number of zones, number of requests sent/received, etc. Refer to DNS Servers—Server Information .
	**Server Log**	Displays the Server Log window that shows the DNS log of that server. Refer to DNS Servers—Server Log .
	**History**	Opens the History window and displays a log of all changes that have been made to the selected object, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user. Refer to Management Console—Object Change History .
	**Zone Wizard**	Launches the Zone Wizard, which helps you create the desired type of zone by prompting you with a series of questions. Refer to DNS Zones—Zone Migration Wizard .
	**View (Hierarchical)**	When selected, toggles to hierarchical view for the IP Address range.
	**View (Flat)**	When selected, toggles to flat view for the IP Address range.
	Quick Filter	This text field lets you instantly filter out objects that you do not want to display. For example, if you type 'ex' in the field, only objects that contain 'ex' somewhere in their name are displayed in the Object List. When you clear the contents from this field, all available objects are again displayed. Refer to Quick Filter .

Zone toolbar

Button	Name	Description
	**Analyze**	Analyzes the contents of the zone. Refer to DNS Zones—Zone Analysis .
	**History**	Displays the history for the selected zone. Refer to the DNS Zones—View History .
	**Wizard**	Launches the Record Creation Wizard. Refer to DNS Resource Records.
	Zone Controls	Only available for static zones on BIND Opens the Zone Controls dialog box. Refer to the DNS Zones—Zone Controls .
	**Find**	Opens the Find Zone dialog box in which you enter criterion to locate specific information for this zone. Refer to DNS Zones—Search .
	**Options**	Opens the Zone Options dialog box. Refer to the DNS Zones—Zone Options .
	**Print**	Prints the zone information.
	**Save**	Saves the information as entered in the main zone information window.

IP Address Range toolbar

Button	Name	Description
	**Delete**	Removes the currently selected host. Refer to IP Address Management.
	**Edit**	Opens the IP Address dialog box in which you can edit details for the IP Address. Refer to IP Address Management .
	**Claim**	Use this feature to prevent accidental assignment of a reserved address without creating a DNS entry for it.[1]
	**Release**	Use this feature to release assignment of a reserved address.
	**Next Free Address in Range**	Finds the first IP Address in the range that is not in use. When clicked, opens the IP Address dialog box in which you enter the IP Address info.

[1] The workflow is as follows:

- A user with "edit data" privileges can select one or more addresses that have no associated A record(s) and choose "Claim" from the menu. Going forward, no one can create A records for the address(es) through the zone window (neither auto-assign nor manually assign).
- A user can select one or more claimed addresses and select "Release." These addresses are then restored to their previous state.
- A user can edit a Claimed record through the IPAM module. When the user opens a IP Address details window for a claimed address, a dialog prompts, "This address has been claimed. Are you sure you want to edit it?" Yes/No? When Save is selected in the IP Address details window, one of two things happens: (1) If the user only entered non-DNS data (custom properties, MAC address, name), the "claimed" flag says in place. (2) If the user entered one or more DNS hosts for the IP Address, the "claimed" flag is cleared.

Scope toolbar

Button	Name	Description
	**Edit**	Allow you to edit the selected host by opening the IP Address dialog box. Refer to DHCP Scopes.
	**Delete**	Deletes the currently selected IP Address. Refer to DHCP Scopes.
	**Claim**	Use this feature to prevent accidental assignment of a reserved address without creating a DNS entry for it.[Page 191, 1]
	**Release**	Use this feature to release assignment of a reserved address.

Quick Filter (Management Console, obsolete)

Note: The Quick Filter functionality is also available in the Web Application.

Quick Filters provide a simple way to filter out data records you do not want to see. They can be found in most windows that contain a number of objects. A Quick Filter works in real time and searches all items in a list by default. It is also possible to narrow the search by using keywords to specify in which field to search.

Using Keywords

Column Headers
: It is possible to use column headers as keywords in the Quick Filter and to specify in which field to search. For example, if you enter the following filtering criterion when filtering zones - `name:myzone` - the filter only searches in the **Name** field and displays only those results that contain the text `myzone`. When a column header's name contains a space, such as `Lease MAC Address`, you can enclose the name in quotes –e.g. `"Lease MAC Address":11`. See Colons, below.

Colons
: Colons are used to separate a column name from a filter. If the filter contains colons, you can either enclose the filter in quotes or escape the colons with a backslash \. For example, both `"Lease MAC Address":"11:22"` and `"Lease MAC Address":11\:22` search for a MAC address containing `11:22` in a column with a name containing with the name `Lease MAC Address`.

Simultaneous Keywords
: You can use several keywords simultaneously simply by leaving a space between each consecutive filtering criterion. An `AND` condition is used when finding records. For example: `name:myzone type:slave`.

Custom Properties
: When custom properties are used, you can use the name of the custom property as a keyword.

Using Wildcards and Regular Expressions in Filters

When using the Quick Filters, it is possible to use the wildcard characters ^ and $ to narrow the search results.

- The **caret symbol** ^ means **starts with**. For example, the search string ^server finds server1.zone.com and server-north.anotherzone.com, but not myserver.myzone.com.
- The **dollar symbol** $ means **ends with**. For example, the search string 'server$' finds the.best.server and good.nameserver, but not slow.servers.
- The ! operator means **NOT{*}**.

For example, the search string `!^a` finds entries that don't start with 'a'. The exclamation mark can be used with the other wildcards to find non-empty fields. Entering `Description: !^$` finds all entries where the Description field is not empty.

Warning: The & and | operators only work for the SOAP interface and Web Application, but *not* currently for the Management Console. It is a known issue that will be fixed in an upcoming version.

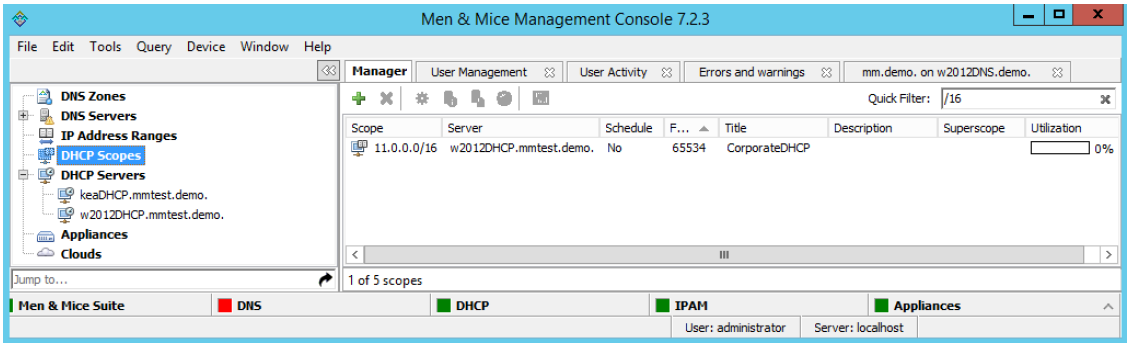
- The & and | operators. The **ampersand** is interpreted as an **AND** operator while the **vertical bar** is used as an **OR** operator. Using these operators, you can combine searches for added control. You can use parenthesis in conjunction with these operators. Examples:
  - `A | B` Finds entries with the text A or the text B
  - `A & B` Find entries containing both A and B
  - `A & (B | C)` Finds entries containing A and either B or C
  - `(A & B) | C` Finds entries containing both A and B or entries containing C

For even more control, you can use regular expressions in filters.

Note: The character `.` must be escaped if it is to be used as a wildcard character. Otherwise, it will be interpreted literally. The same applies to following characters: `(`, `)`, `{`, `}`.

Clearing an Entry

At any time, you can clear the text you have in the Quick Filter field by click the *X* shown at the end of the field.

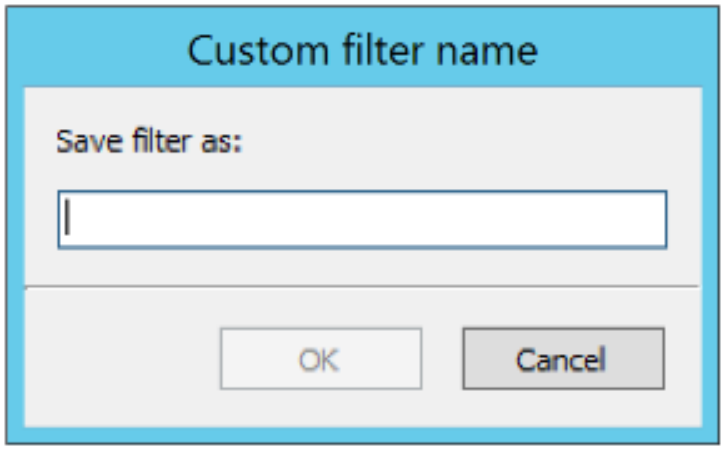


Saving a Filter

It is possible to save filters for various object types. Saved filters appear in the list on the left hand side of the Manager Window and in the Create Zone dialog box. Filters can be local or global in scope. Filters created by the Administrator are global and visible to all users. Filters created by any other user are visible only to that user.

To save a filter, do the following:

1. Type the entry you want to filter by in the Quick Filter field.
2. Move to the menu bar, and select *Edit* → *Save Filter*.
3. In the dialog box, type the desired name for the filter. Then click *OK*.
4. The saved filter shows at the bottom of the Object list for the corresponding object type.

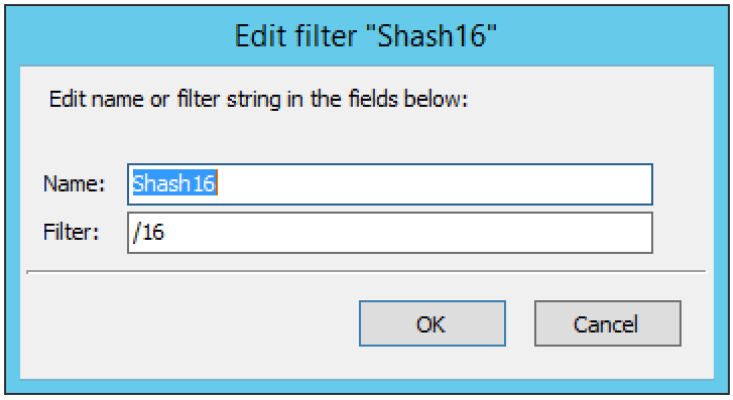


Note: You can also create filters that reside in object folders. To create a filter in a folder, start by selecting the folder before creating the filter. A filter that resides in a folders perform the search within the context of the folder.

Editing a Filter

To edit a filter, do the following:

1. Locate the filter name in the Object list.
2. Right-click the filter and select *Edit Filter*.
3. Make the desired changes to the filter and click *OK* to save the changes.



Deleting a Filter

To delete a filter, do the following:

1. Locate the filter name in the Object list.
2. Right-click the filter and select *Delete Filter*.

Other actions in the Management Console

Jump to Box

The **Jump to Box** is a field that can be used to quickly open a single object in Micetro by entering the object name. Using the 'Jump to Box' you can open the following object types:

- DNS Zone
- DNS Record
- IP Address Range
- DHCP Scope
- IP Address in an IP Address Range or a DHCP Scope

The 'Jump to Box' is located at the bottom of the sidebar on the left. Additionally the shortcut *Shift-J* can be used to move the focus to the 'Jump to Box'.

To use the 'Jump to Box', do the following:

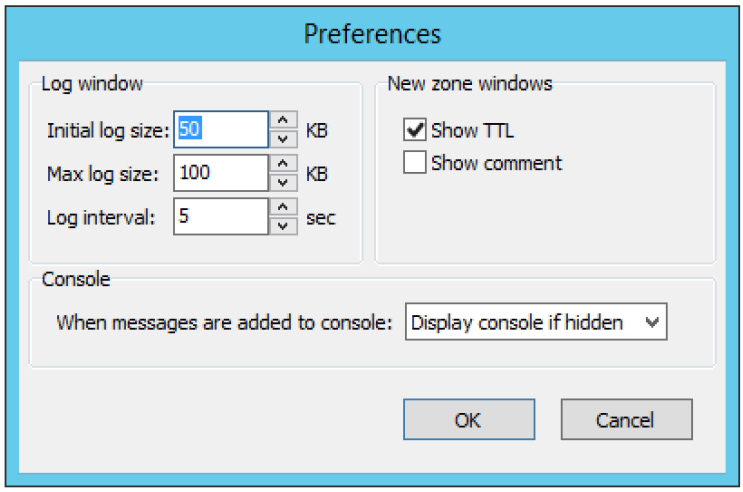
1. Navigate to the **Jump to Box** or press *Ctrl+J*.
2. Enter the name of the object you want to open and click the *Jump to* icon to the right of the field (or press *Enter*). If more than one matching object is found, a dialog box displays in which you can select the object instance you want to open.

Note: You must enter the exact name of the object you want to open. For example, if you want to open a zone by the name myzone.local, it is not sufficient to enter just 'myzone' or 'myzone.lo' – you must enter 'myzone.local'. The same applies for DNS records, IP Address Ranges, DHCP Scopes and IP Addresses.

Program Preferences

You can set some default behaviors for the Men&Mice Management Console using the *Options* dialog box.

On the menu bar, select *Edit* → *Preferences*. The *Options* dialog box displays.



Log Window

Initial log size
The server logs are kept by the servers. When the Management Console connects to a server and the log window is opened, the Manager downloads the most recent portions of the server's log. The amount downloaded (in kilobytes) will be equal to the value set in the Initial log size field.

Max log size
The maximum log size determines how much of a server's log can be retained by the Management Console at any one time. Once the maximum size is reached, the Manager will discard old log entries as necessary to make room for the new ones. Log entries discarded by the Manager Console are retained on the log that the server maintains. The Max log size field can be set to any value between 1 and 1024 KBs. The default value is 100 KB.

Log interval
Whenever the log window is open, it will continually update itself (the log) from the server. The interval between sequential updates can be set to any value between one and thirty seconds. The default value is every five seconds.

New Zone Window

Show TTL
This checkbox is enabled by default. If you clear this checkbox, the TTL column will not be included in any new zones that you create.

Show comment
This checkbox is enabled by default. If you clear this checkbox, the Comment column will not be included in any new zones that you create.

Console

You can configure how the Console Window behaves when new entries are added to the window.

Do nothing
If this option is selected, entries are added 'silently' to the console window. If the window is hidden, it is not displayed when new entries are added.

Display Console if hidden
If this option is selected, the console window will be displayed when new entries are added.

Bring Console to front
If this option is selected, the console window will be displayed as the front-most window when new entries are added.

Search/Update Wizard

This utility allows you to find, create, modify, or delete records in multiple zones and DHCP Scopes using a single action.

There are three search options available:

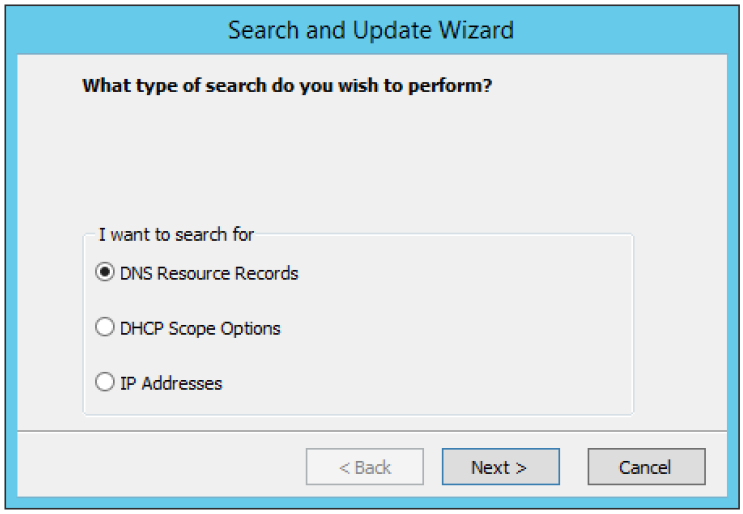
DNS Resource Records
Refer to *DNS Resource Records* for further information.

DCHP Scope Options
Through this function, you replace, delete or search for option values.

IP Addresses
Through this function, you can find an IP Address in any IP Address range and display the results in the IP Address range window.

To launch the *Search and Update Wizard*, do the following:

1. From the menu bar, select *Query* → *Search and Update Wizard*. The *Search and Update Wizard* dialog box displays.
2. Select the type of search you want to perform.
3. Complete each screen as you move through the wizard.



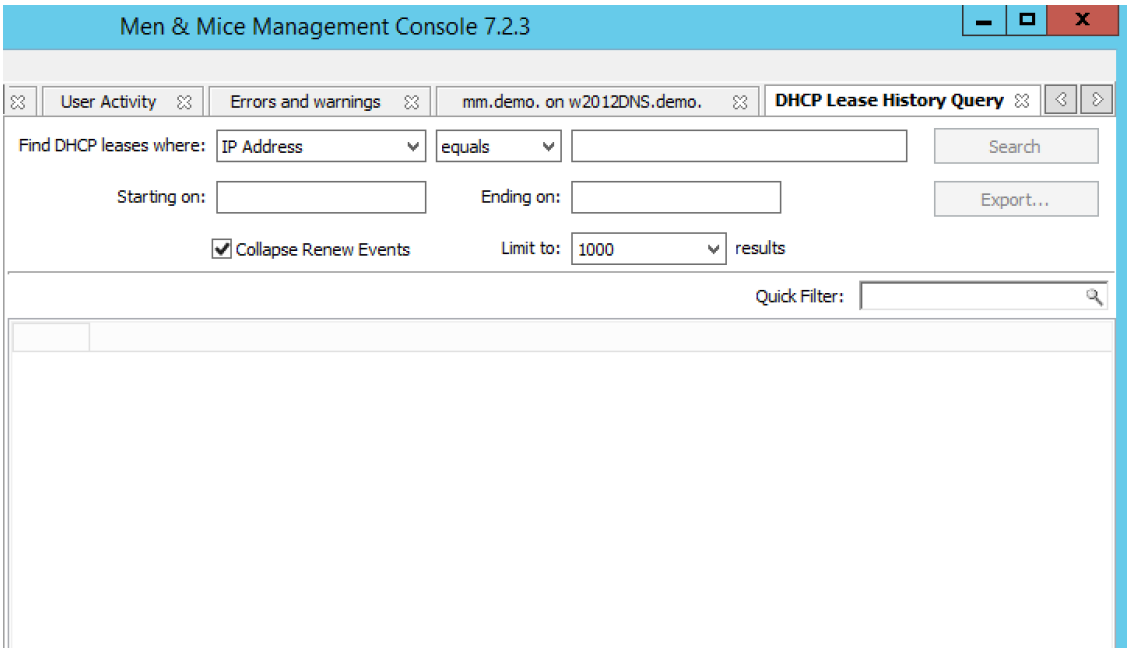
Lease History

Through this function, you view the lease history for your MS and ISC DHCP servers.

Note: You must be a member of the DHCP Administrator group to view the DHCP lease history. Lease history collection must be enabled for this function to work.

To view the DHCP lease history:

1. From the menu bar, select *Query* → *Lease History*. The *Lease History Query* tab displays.



Find DHCP leases where
: Select if you want to query by *IP Address*, *MAC Address*, *Server Address*, *Hostname* or *Description*.

Starting on/Ending on
: To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07.

2. Click *Search*. Any matching results are displayed in the lower portion of the window.

Exporting Search Results

To export the results as a CSV file, do the following:

1. Display the lease history.
2. Search for the desired history.
3. When the applicable change history is shown, click the *Export* button. The *Export records to CSV file* dialog box displays.
4. Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
5. Click *Save*.

Object Change History

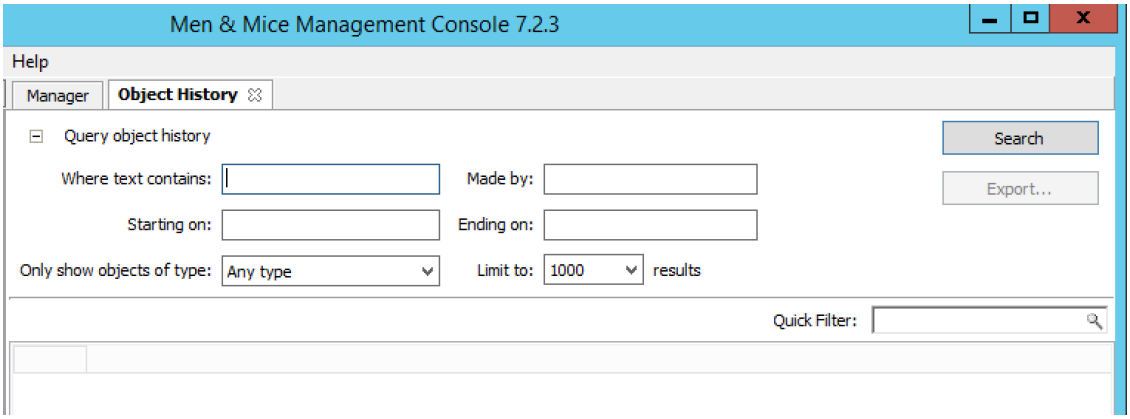
Through this function, you can display a log of all changes that have been made to any object such as the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user.

There are two ways to search/view the object change history:

- From the *Menu Bar*. With this option, you select the type of object to search change history for.
- Through the *Object Browser*. With this option, you select the object first, and then search for the change history.

Accessing via the Menu Bar

1. From the menu bar, select *Query* → *Object History*. The *History Query* tab displays.



Where text contains
Type any words that the text contains.

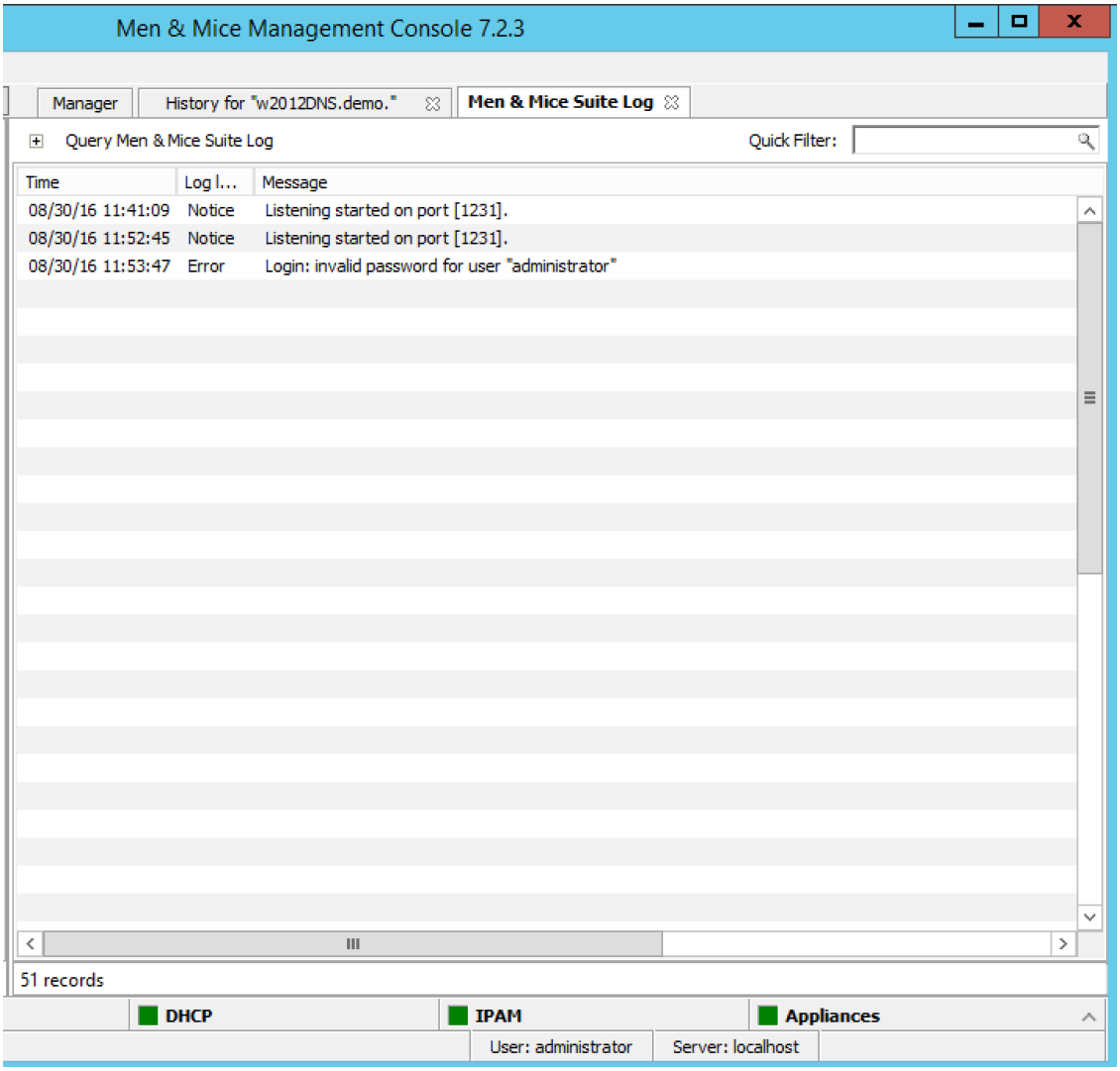
Made by
Type the user login name.

Starting on/Ending on
To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07.

Only show objects of type
Click the drop-down list arrow, and select the type of object for which you want to find change history.

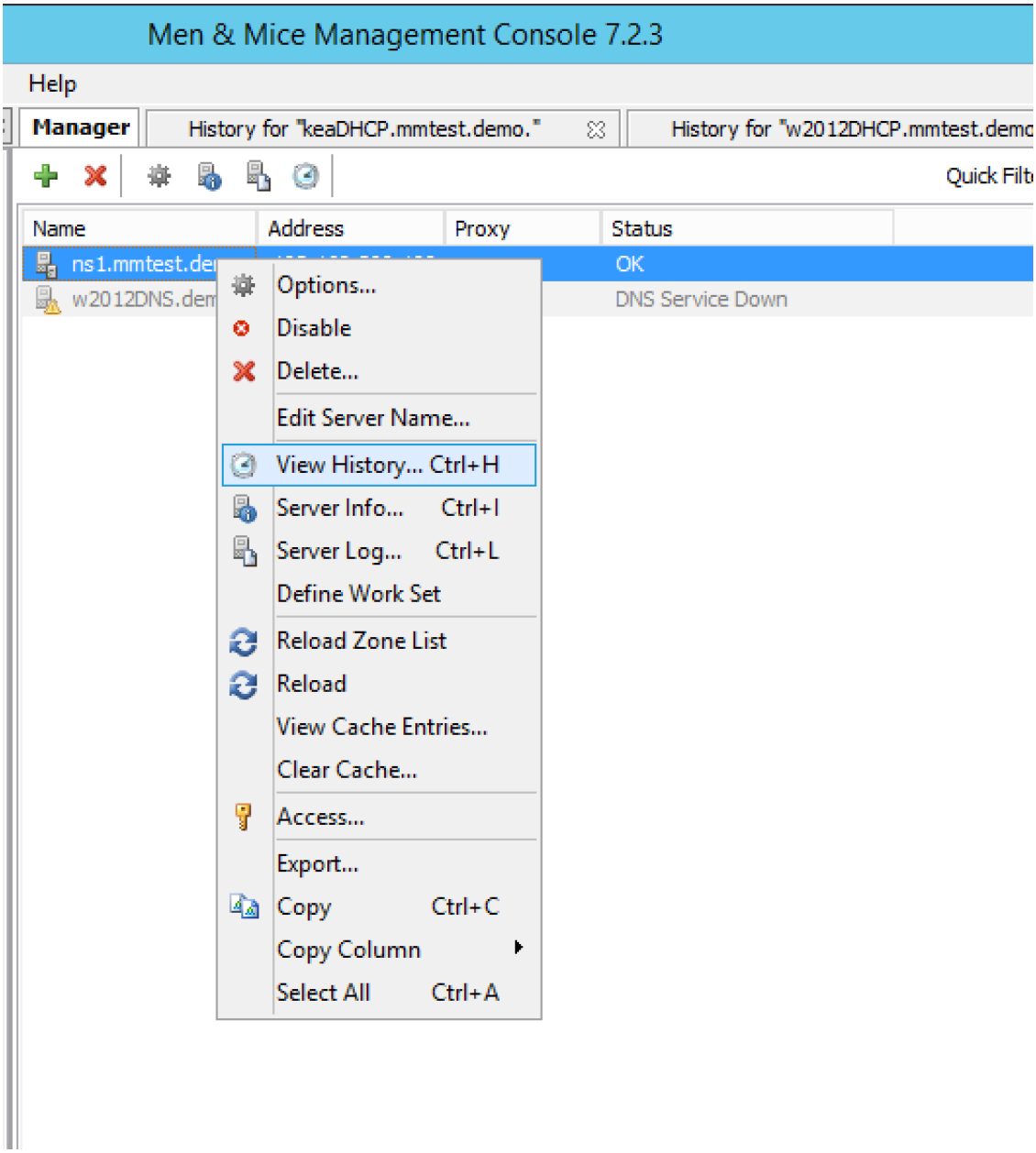
Limit to ____ Results
Enter the maximum number of results to display.

2. Click *Search*. Any matching results are displayed in the lower portion of the tab.

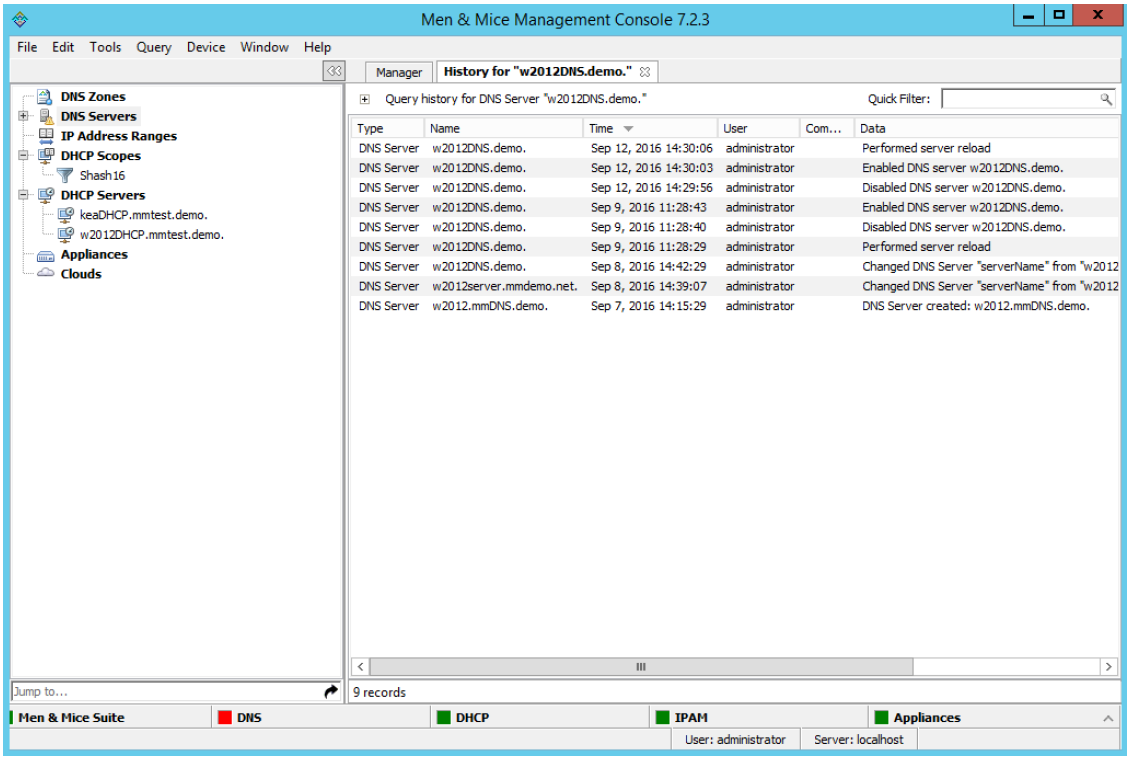


Accessing via the Object Browser

1. In the *Object Browser*, open the desired object category (e.g., DNS Zones, DNS Servers, etc.).
2. Locate the object for which you want to view the history.
3. Right-click and, from the shortcut menu, select *View History*.



The *History* window displays showing all the history for the selected object.



4. If you wish to query the results, click the + in the upper left corner of the dialog box.
5. Following the directions under *Accessing via the Menu Bar* to enter the query information.

Exporting Search Results

To export the results as a CSV file, do the following:

1. Display the object change history.
2. Display the *Query Change History* search criteria fields.
3. Search for the desired change history.
4. When the applicable change history is shown, click the *Export* button. The *Export records to CSV file* dialog box displays.
5. Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
6. Click *Save*.

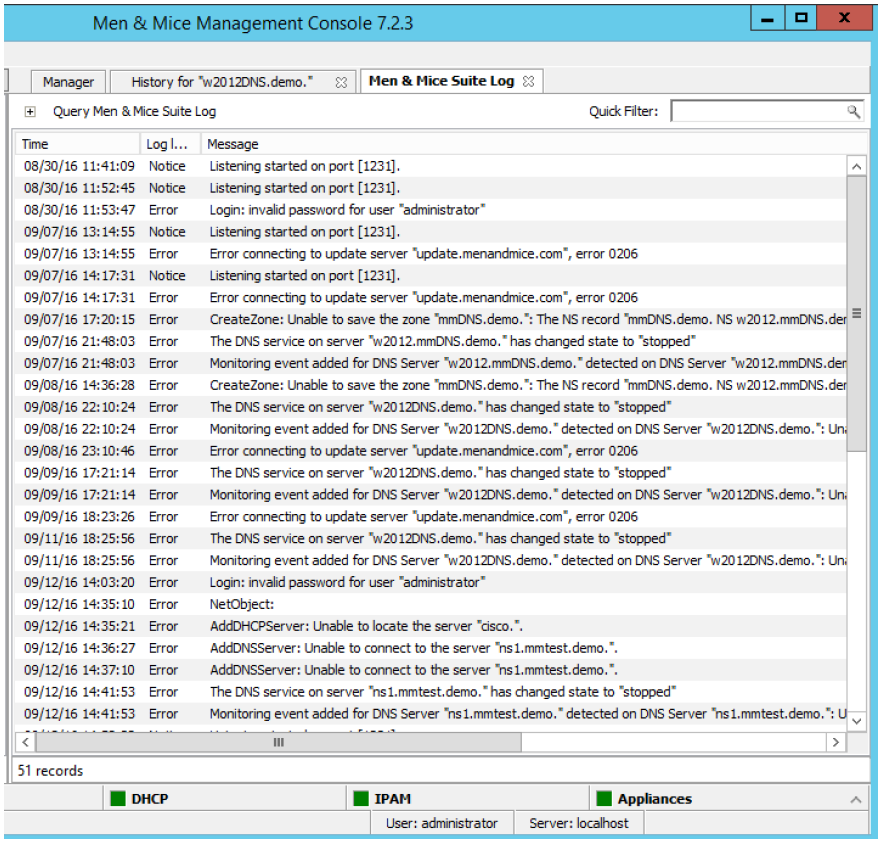
Micetro Log

Through this function, you can display log messages generated by Micetro.

Note: You must be a member of an Administrator group to view the log messages.

To view the log messages, do the following:

1. In the main Men&Mice window, move to the menu bar and select *Query → MenMice Suite Log*. The *Men&Mice Suite Log* tab displays.



Search For
Type the information to query.

Starting on/Ending on
To query based upon a date range, type the starting and ending range dates. For example, to find all changes made in 2007, in the Starting on field type 1/1/2007 and in the Ending on field, type 12/31/07.

Log level
Click the drop-down list, and select the desired level – e.g., Error, Notice or Warning.

2. When all selections/entries are made, click *Search*. Any matching results are displayed in the lower portion of the window.

3. The Quick Filter allows you to further refine the search results. As you type in the field, results that are not applicable are removed. To export the results as a CSV file, do the following:

   - Click the *Export* button. The *Export records to CSV file* dialog box displays.
   - Select the drive, directory, subdirectory, etc. into which you want to save the CSV file.
   - Click *Save*.

Health Monitoring Bar

Overview

The Men&Mice Health Monitoring provides the administrator with valuable information they need to maintain their systems and services. First, a good overview of the general health of Micetro and related services. More importantly, it will give the administrator an indication if there is a problem that needs to be acted on and corrected, for example if there is a secondary zone that is expiring or if there is a zone that has not been loaded on a server due to an error. Both cases can cause outages for users and therefore be a serious impact for the business.

Categories

The health status is displayed on the health bar which is positioned at the bottom of the management console window. The status indicators are split into five categories

- Micetro
- DNS
- DHCP
- IPAM
- Appliance

A color code is used to represent the severity of the error. If an indicator in any of those categories has a warning or error, it is shown as yellow or red, respectively; otherwise as green. The health bar can be expanded and then the indicator subcategories are shown and more details can be obtained about the health indicators. More importantly, details about each error are given in a separate window where a detailed description about the error is given and also the administrator is given the opportunity to navigate to the object that is affected and from there, fix the error.

Fig. 1: The health bar has been expanded by clicking the up arrow in the upper right corner of the health bar. There, it can be seen the there are errors in ‘DNS Zones’ and ‘Server Controllers’ and a warning in ‘Version’.

Indicator details

Category	Subcategory	Description
Mice	Licensing	An indication is given if there is a problem with the license, for example if a module license has been exceeded.
	Datal	An indication is given if the database size exceeds a default threshold of 1GB for SQLite.
	Serve Controlle	An indication is given if * the server controllers have a problem communicating with Men&Mice central * there is a problem communicating with the update agents running beside the server controllers.
	Version	An indication is given if there is a new version available, if there are pending upgrades or if any components are out of date.
DNS	DNS Serve	An indication is given if there is a problem communicating with the servers or if the DNS server is down.
	DNS Zone	An indication is given if * the system is unable to get the zone status * the slave zone will expire in the next 24 hours * the zone can not load on the server
DHC	DHC Serve	An indication is given if there is a problem communicating with the servers or if the DHCP server is down.
	DHC Scop	An indication is given if * the system is unable to get the scope status * the static part of scope is over utilized * the dynamic part of scope is over utilized * a superscope is over utilized * there is a scope pool collision * there is a scope reservation mismatch * scope contains inconsistencies that need reconciling * the system is unable to check whether scope contains inconsistencies * the system is unable to check whether scope is part of a failover relationship on partner server * the DHCP failover partner server is unreachable * the system is unable to fetch scope info from the partner server * if a scope is not part of a failover relationship on the partner server
IPAM	Static	An indication is given if a subnet is over utilized.
	Discovery	An indication is given if there are problems with communicating with routers.
Appliance	Appliance healtl	An indication is given if an appliance is unreachable.

In any case of an warning or error above, there will be a detailed description of the error or warning, and a way to navigate to the proper place to fix an error/warning.

Ignoring indicators

By right clicking a status indicator in the health bar and selecting **ignore**, that status indicator can be ignored.

Viewing error / warning indicators

In this window you can see more details about the status indicator. Following are descriptions about what each column shows.

Message
: Details about the error / warning for this indicator

Object
: Name of the object that the error / warning is related to

First seen
: The date of which the error / warning was first seen

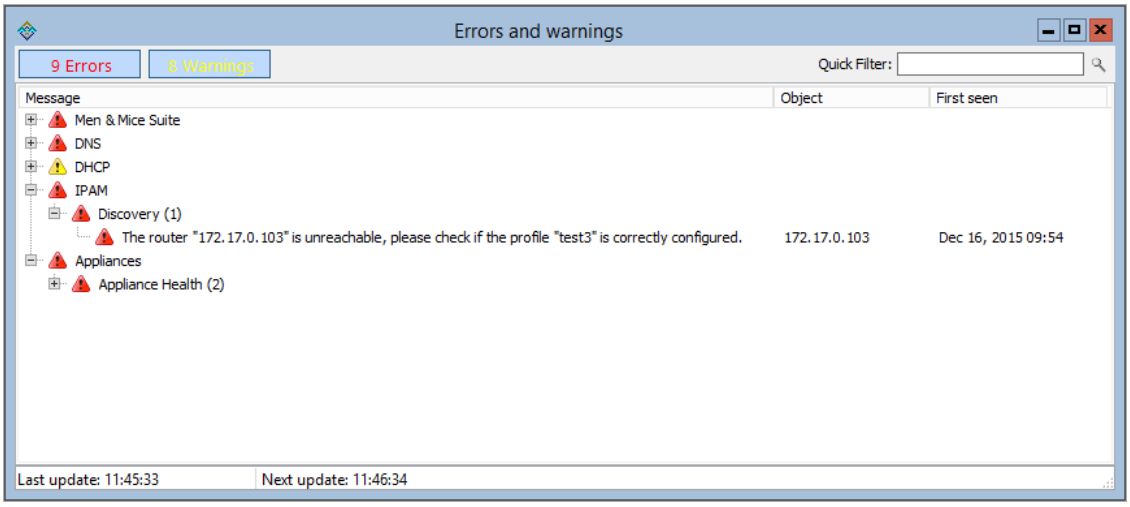


Fig. 2: In the figure above, we have clicked on the 'Discovery' indicator to get more details about the error.

Right clicking an indicator will show a context menu with the following items (where applicable):

- Show in manager window: Show the specific item in the manager window
- Open: Opens a specific object, for example a scope
- Reconnect: Reconnects to an already disconnected server

Disabling health monitoring

The system health monitoring can be disabled completely by setting an advanced system option. See *Advanced System Settings* for more details.

Authoritative DNS Servers (Management Console, obsolete)

Overview

This section shows you how to perform specific actions in the Men&Mice Management Console associated with maintaining your DNS servers, such as adding, and creating and editing zones and records. The commands associated with server management are located in the Server menu and several are accessible from the toolbar. The Server menu is only available when the DNS Servers object is selected in the Object Section of the Management Console.

Server Access on Remote Computers

To manage DNS servers, each must have a DNS Server Controller installed. For the BIND DNS server, a DNS Server Controller must be installed on each DNS server you want to manage.

If you plan to use Men&Mice Suite to manage any Microsoft DNS servers, install the DNS Server Controller on a Windows machine that is a member of the same domain or workgroup as the DNS servers. You may install multiple copies of the DNS Server Controller, for example if you want to manage Microsoft DNS Servers that reside in different forests. A single DNS Server Controller for Microsoft DNS Servers can manage multiple DNS servers. The DNS Server Controller must adhere to whatever restrictions and security standards are set forth in Microsoft Windows.

To configure the DNS Server Controller to access DNS servers on remote computers, do the following:

1. Before you can administer DNS servers, verify that the DNS Controller is running as a Windows User and has the necessary privileges.
2. To enable DNS Management in Micetro, start the Windows Services program and open the properties dialog box for Men&Mice DNS Server Controller.
3. Click the *Log On* tab. The *Local System account* radio button is most likely selected.
4. Click the *This account* radio button and enter the name and password of a Windows User that is a member of the Administrators group.
5. Close the dialog box and restart the Men&Mice DNS Server Controller service.

Note: Some actions for static zones are not available if you are managing Microsoft DNS servers on remote computers using the DNS Server Controller. The following actions are not available:

- Disable resource record
- Enable resource record
- View and edit resource record comments
- Disable zone

If you need to be able to perform these actions, you must install the DNS Server Controller on the server and use the Microsoft with Agent Installed connection method when connecting to the server.

Define Work Set

It is possible to define a Work Set for servers in the Management Console. A Work Set contains a subset of all of the servers in the system and when a Work Set is active, only the servers in the Work Set are visible and the zones on the servers in the Work Set are the only zones visible. This feature is useful when many servers are defined, but you only work with a small number of them on a day-to-day basis.

To define a Work Set, do the following:

1. Select the server(s) you want to include in the Work Set.
2. Right-click the selected server(s) and choose *Define Work Set*.

To clear a Work Set, do the following:

1. Click the *Clear Work Set* button in the Manager window. The Work Set is cleared.

Options

The Management Console's *Server Options* dialog box lets you configure settings for each name server individually, including forwarding servers, logging preferences, transfer and query restrictions, and root servers.

Note: The server options vary depending on the server environment. In the section that follows, the server options are documented twice: once for those using a Windows DNS server, and again for those using BIND.

Accessing Server Options

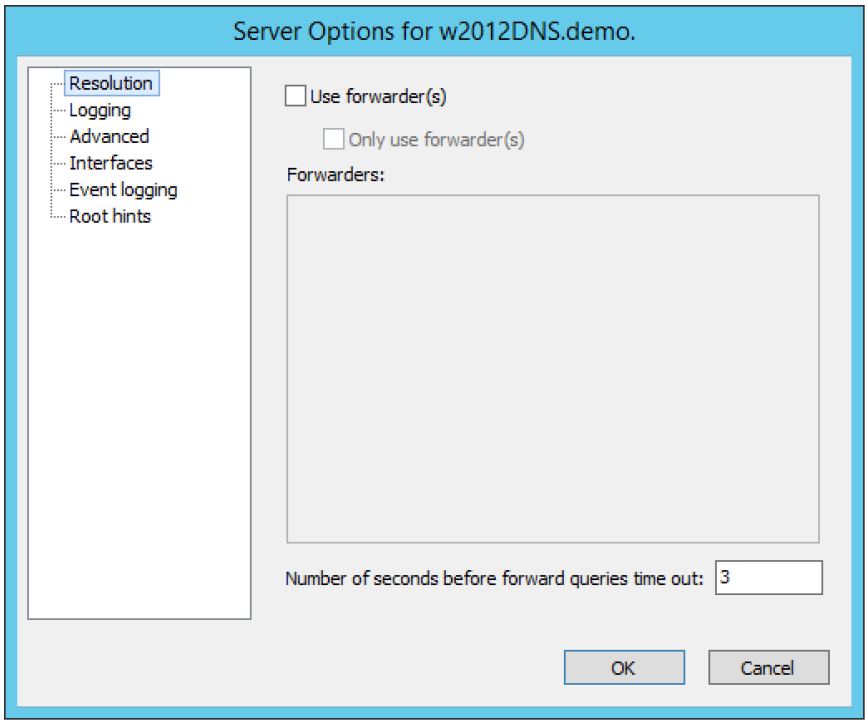
1. In the Object Section, select *DNS Servers* so the servers appear in the Object List.
2. Right-click on the server you want to make changes to and select *Options* from the context menu. The *Server Options* dialog box displays.
3. Choose the desired option (Resolution, Logging, Advanced, Interfaces, Event logging, Root hints) from the menu on the left. The corresponding options display in the right panel of the dialog box.
4. Refer to the appropriate section and server environment below for each option.

Windows DNS servers

This section describes the Server Options as they display in a Windows Server environment.

Resolution (Windows)

The Resolution panel lets you change the method by which this server resolves queries.



Three basic modes can be established:

The server can be set to resolve queries entirely by itself.
If you do not want to use any forwarders with this server, leave the Use forwarder(s) checkbox unchecked.

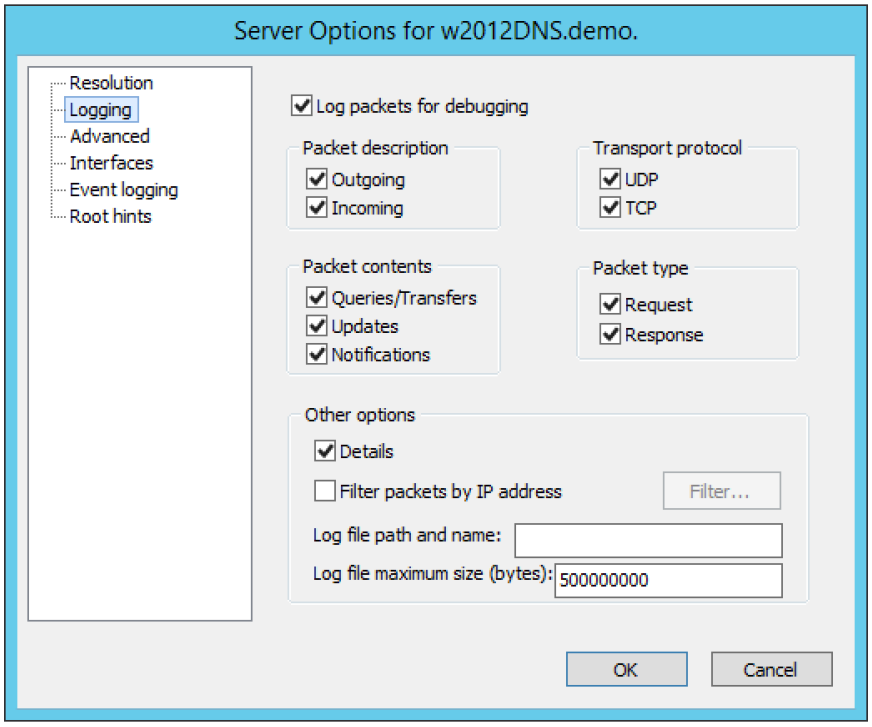
The server can share the task of resolving queries.
If you want to share the task of resolving requests with one or more forwarding servers, select the Use forwarder(s) checkbox and enter the IP Address of the forwarding servers in the Forwarders list. When you enter the IP Addresses to multiple forwarders, all the forwarders are queried simultaneously, and the first response is accepted. Under this shared mode, if a server using a forwarder does not receive a response after a few seconds, it will attempt to resolve the query itself.

The server can forward all requests to other servers.
If you want to forward all requests to other servers (and never use this server), select the Use forwarder(s) checkbox, enter the IP Address of the forwarding server(s) in the Forwarders list, and check the Only user forwarder(s) checkbox.

After making the desired changes, you can choose another category from the left column, or click OK to close the dialog box.

Logging (Windows)

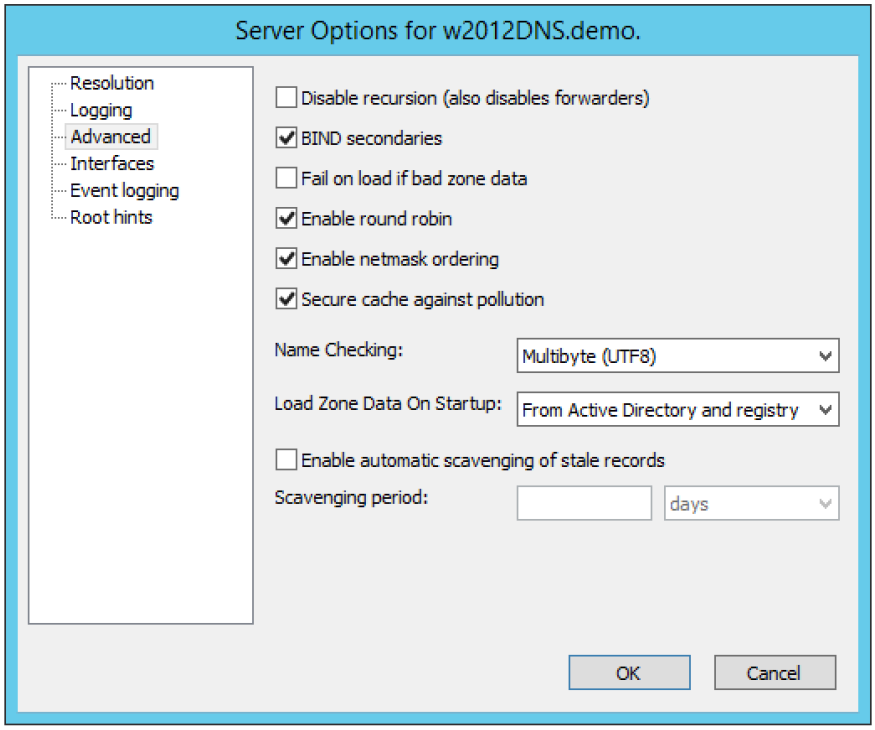
The Logging options consist of a list of checkbox options. Once you enable Log packets for debugging, the other options in the dialog box become accessible and you can choose which types of information you want the program to record in the server's log.



After checking the desired options, you can either choose another category from the left column or click *OK* to close the dialog box.

Advanced (Windows)

Use this panel to set various advanced options for the DNS server. Complete the dialog box based upon the guidelines below. When all selections/entries are made, click *OK*.



Disable recursion.
Determines whether or not the DNS server uses recursion.

BIND secondaries.
Disables fast (compressed) zone transfers for compatibility with old BIND servers (older than 4.9.4).

Fail on load if bad zone data.
Prevents the server from loading a zone when bad data is found.

Enable round robin.
Rotates the order of resource record data returned in query answers when multiple resource records of the same type exist for the queried DNS domain name.

Enable netmask ordering.
Determines whether the DNS server reorders A resource records within the same resource record set in its response to a query based on the IP Address of the source of the query.

Secure cache against pollution.
Determines whether the server attempts to clean up responses to avoid cache pollution.

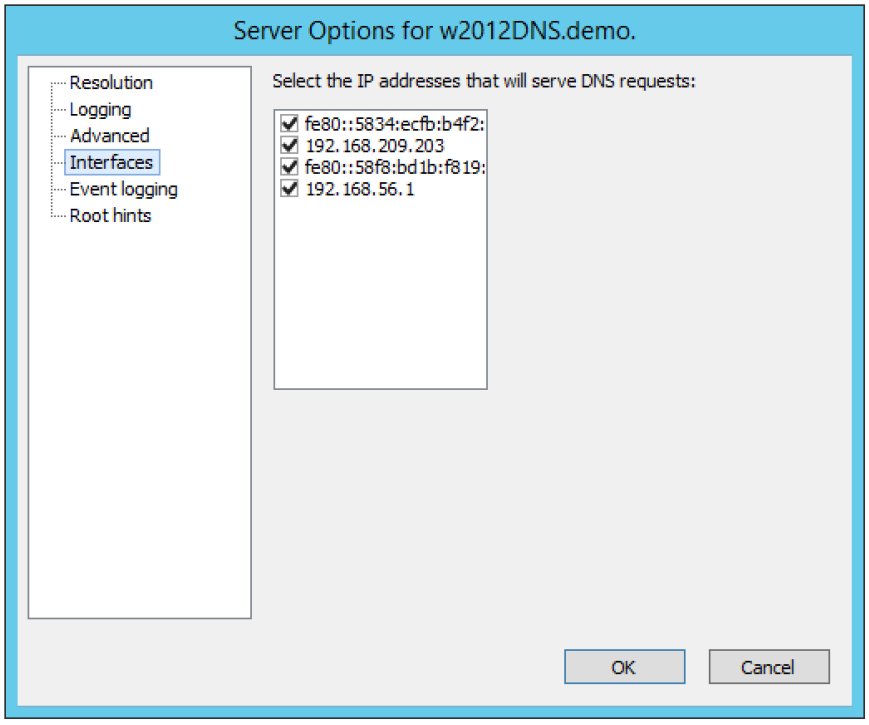
Name Checking.
Determines the type of name checking used for zones on the server. Click the drop-down list and select from the options provided.

Load Zone Data on startup.
Determines from where to load the zone data when the server starts up. Click the drop-down list and select from the options provided.

Enable automatic scavenging of stale records.
Specifies whether scavenging can occur for the selected server. If automatic scavenging is enabled, the scavenging period can be specified. Type the duration in the first field. In the second field, click the drop-down list and select the duration range – e.g., days.

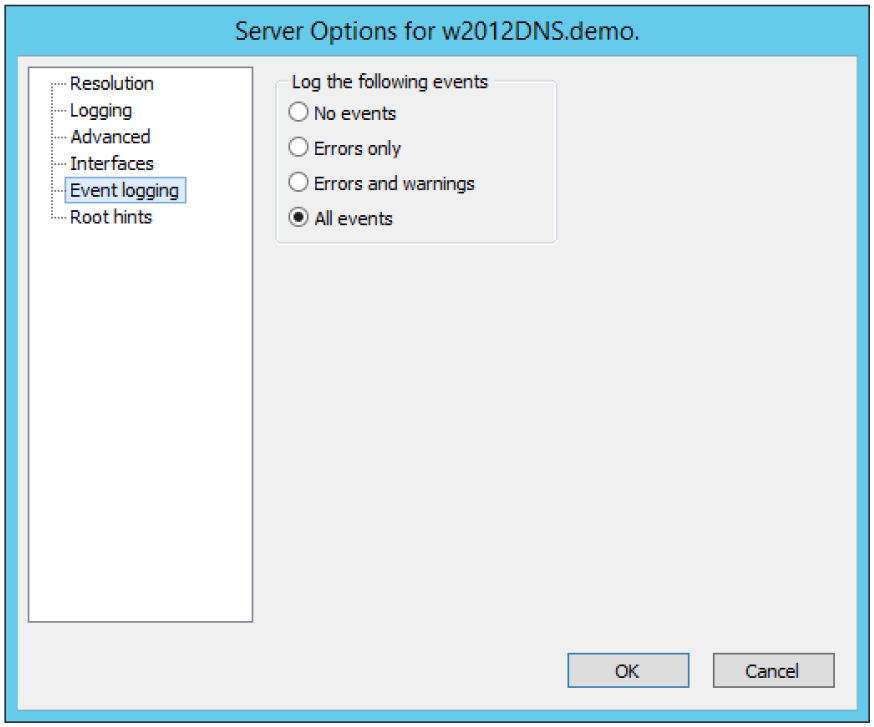
Interfaces (Windows)

Use this panel to specify the IP Addresses this server will use to serve DNS requests. When your selection is made, click *OK*.



Event Logging (Windows)

Specifies what event information should be logged and displayed in the Server log.



Click next to each of the desired items using the guidelines below:

No events.
Specifies that no events will be logged in the DNS Server log.

Errors only.
Specifies that only errors will be logged in the DNS Server log.

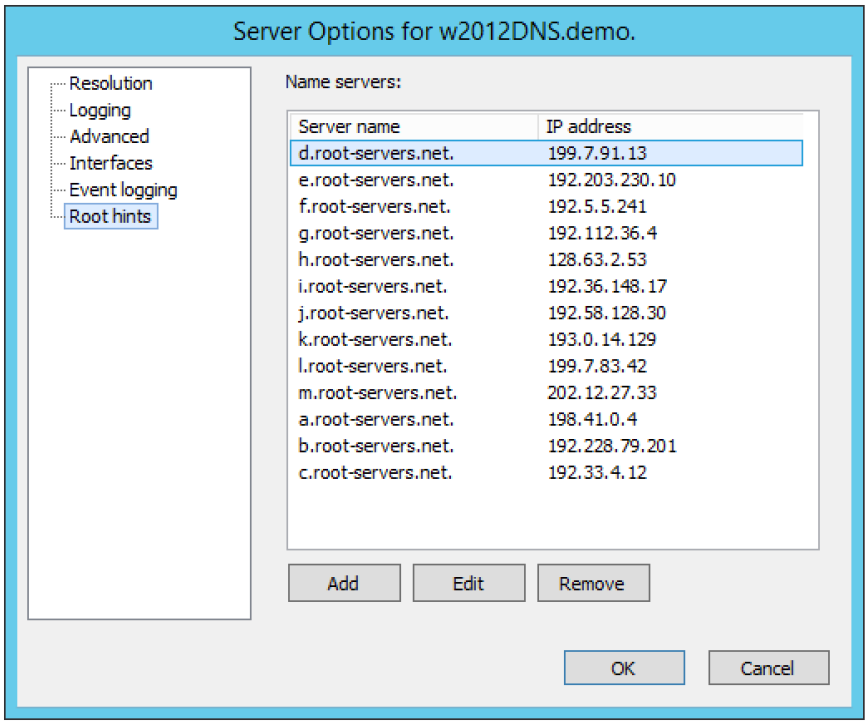
Errors and warnings.
Specifies that only errors and warnings will be logged in the DNS Server log.

All events.
Specifies that all events will be logged in the DNS Server log.

When all selections are made, click *OK*.

Root hints

Allows configuration of suggested root servers for the server to use and refer to in resolving names.



To Add a Root name server, complete the fields as follows:

1. Click the *Add* button.

   Server fully qualified domain name.
   Type the name of the server.

   IP Address.
   Type the IP Address of this server.

2. Click *OK*.

To Edit the Root hint name server data, do the following:

1. Select the server definition you want to edit.
2. Click the *Edit* button.
3. In the *Root hint name server* dialog box, type the updated information.
4. Click *OK*.

To Remove a Root hint name server, do the following:

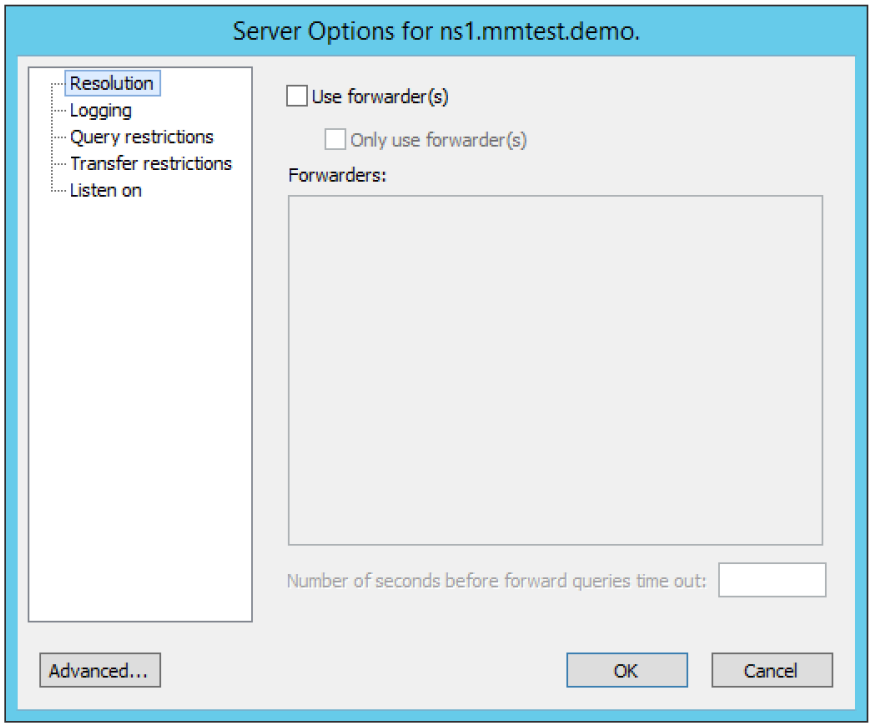
1. Select the server definition you want to remove.
2. Click the *Remove* button.

BIND Environment

This section describes the Server Options as they display in a BIND environment.

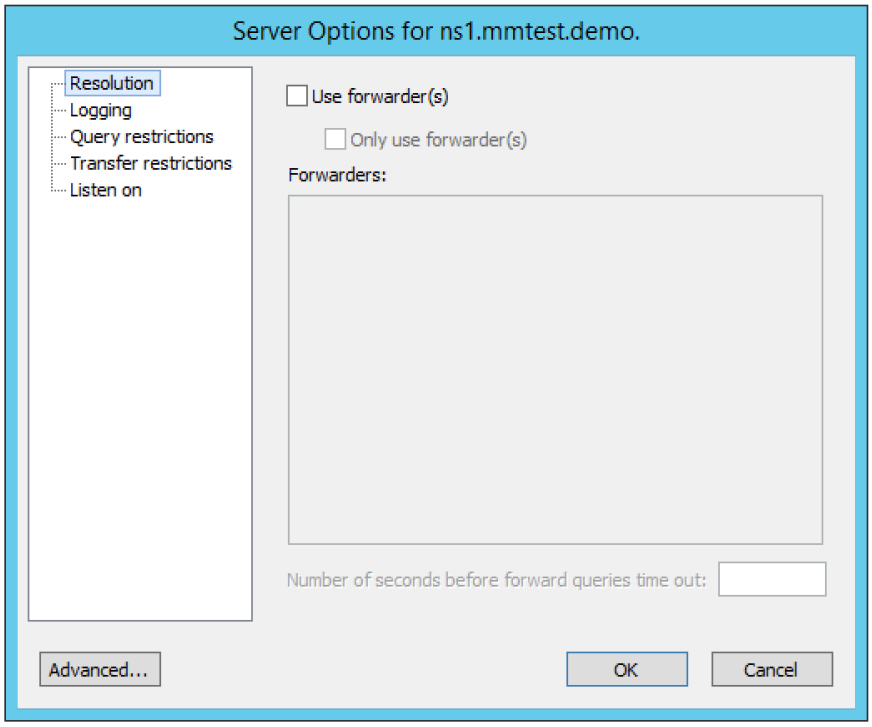
Resolution (BIND)

The Resolution settings in a BIND environment are the same as in a Windows environment.



Logging (BIND)

The Logging Settings control the type of information that is recorded in a server's log.



Channel.
Specifies where your logged data will go. Use the drop-down list to select which log file you want to receive which categories of data.

Category.
Lists the different types of information that can be logged. The System log typically tracks system-level messages, while the Men&Mice log is much more comprehensive and includes information about server interactions and activity. Check the categories you want to include in the log.

Log Level.
The Log Level allows you to filter messages by severity. Select the level of messages that you want to log by choosing the corresponding radio button. There are eight radio buttons. The top five are the standard severity levels used by syslog. The remaining two settings areDebug and Dynamic.

Debug.
Provides name server debugging. When you choose this option, a text box displays next to the radio button allowing you to specify a debug level. If you do not specify a debug level, it is assumed to be 1. If you do specify a level, you will see messages of that level when name server debugging is turned on.

Dynamic.
Causes the name server to log messages that match the debug level. For example, if you send two trace commands to the name server, it will log messages from level 1 and level 2.

Print Category.
When selected, the category of the message displays with the log entry.

Print severity.
When selected, the severity of the message displays with the log entry.

Print time.
When selected, the message includes a time stamp.

Max file size (only shown for log file channels).
Determines how many versions of the log file are maintained. The log file will grow to the size specified in the

Max file size field, after which a new log file is created and the old file is renamed. As this process continues, each file is systematically renamed until it is finally deleted. For example, if the Version field contained the value 2, there would be the 'active' log file, and two older versions. When the active log file becomes too big, a new log file would be created and the previously active log file would be renamed as the version 1 file. The old version 1 file would be renamed as the version 2 file, and the old version 2 file would be deleted.

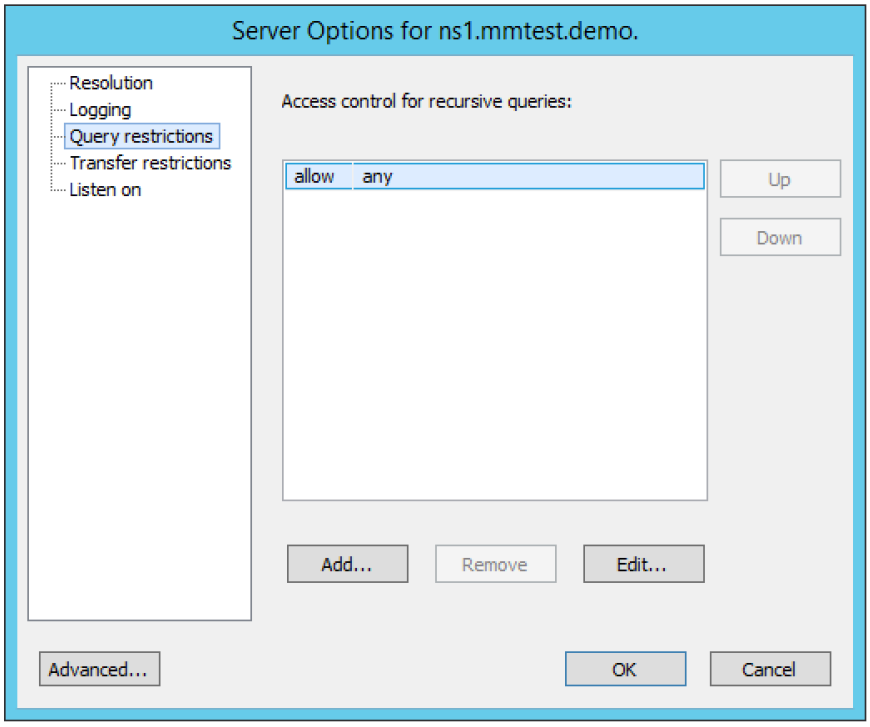
Versions (only shown for log file channels).
Enter the maximum size of the log file and the appropriate units. For example, 100K = 100 kilobytes, 2M = 2 megabytes, and 3G = 3 gigabytes. If no value is specified, the default unit bytes are used.

Facility (only shown for syslog channels).
Allows the user to specify a syslog facility to be used.

Note: For remote logging on the DDI appliance, only the local7 facility is configured to be sent to the remote loghost. See Appliance Management for more information on enabling remote logging on the DDI appliance.

Query Restrictions (BIND)

The Query restrictions panel allows you to restrict recursive DNS queries to only certain IP Addresses or address ranges.

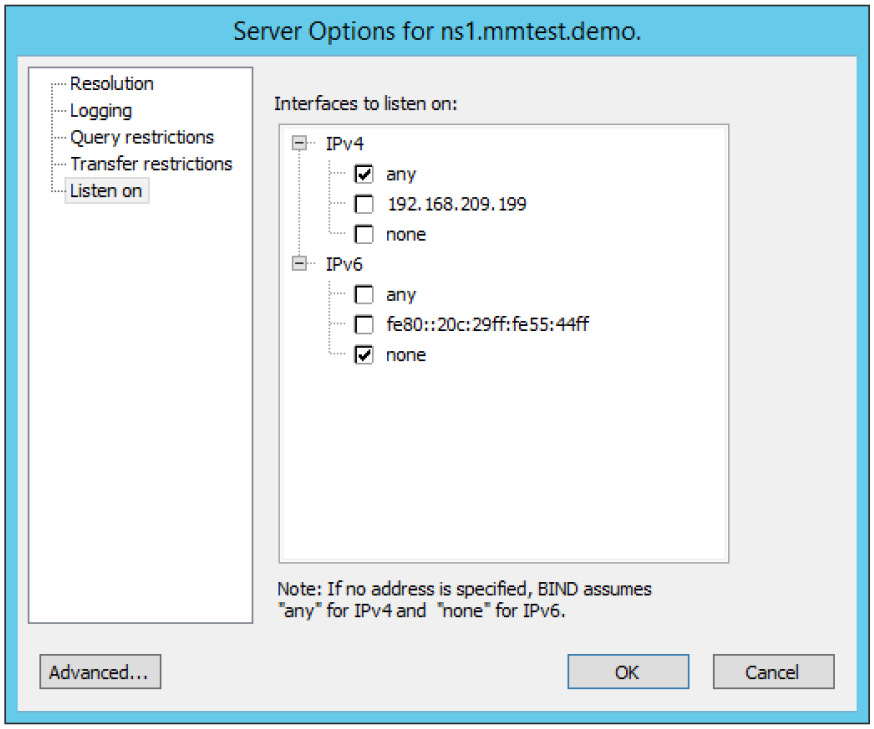


To configure a query restriction, do the following:

1. Click the *Add* button.
2. Enter an IP Address in the field provided. You can choose a predefined range from the drop down list, which gives you the option to select any, none, localhost, or localnets.
3. Choose whether you want to allow or deny this server access control for recursive queries by selecting the appropriate radio button.
4. Click *OK* to add the new restriction to the list.

Transfer Restrictions (BIND)

The Transfer restrictions panel allows you to restrict zone transfers to only certain IP Addresses or address ranges. Restricting access to zone transfers is a marginally effective security measure designed to prevent outsiders from seeing the names and IP Addresses of your hosts. All of this information is available from a reverse zone lookup. However, security through obscurity will keep out amateurs and the merely curious.

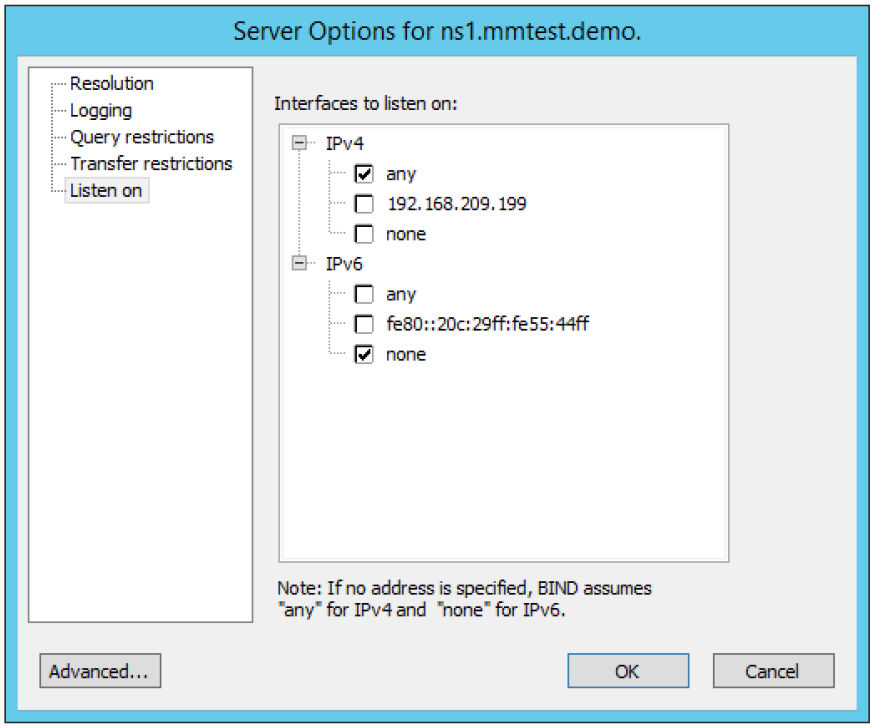


To configure a transfer restriction, do the following:

1. Click the *Add* button.
2. Enter an IP Address in the field provided. You can choose a predefined range from the drop down list, which gives you the option to select any, none, localhost, or localnets.
3. Choose whether you want to allow or deny zone transfers to this IP Address by selecting the appropriate radio button.
4. Click *OK* to add the new restriction to the list.

Listen on (BIND)

The Listen on panel allows specify the IP Addresses this server will use to serve DNS requests.



To specify the listening interfaces, select the checkboxes for the interfaces you want to listen on, both for IPv4 and IPv6.

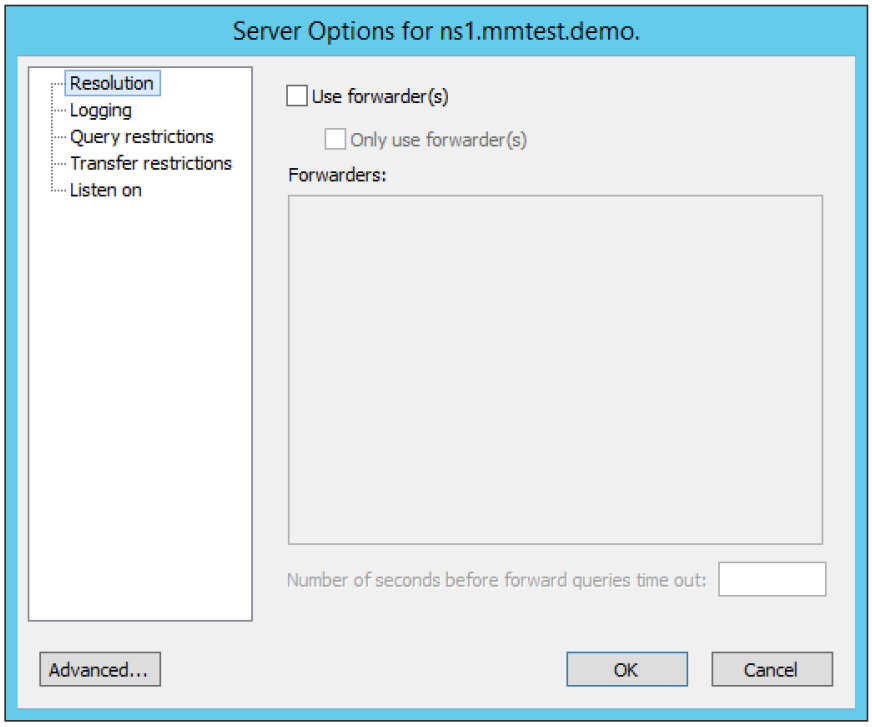
- If you select the any option, the server will listen on all configured IP Addresses.
- If you select the None option, the server will not listen on any IP Address.

Advanced Server Options

DNS Administrators can access the BIND configuration files directly to edit DNS server and zone options that are not available in the GUI.

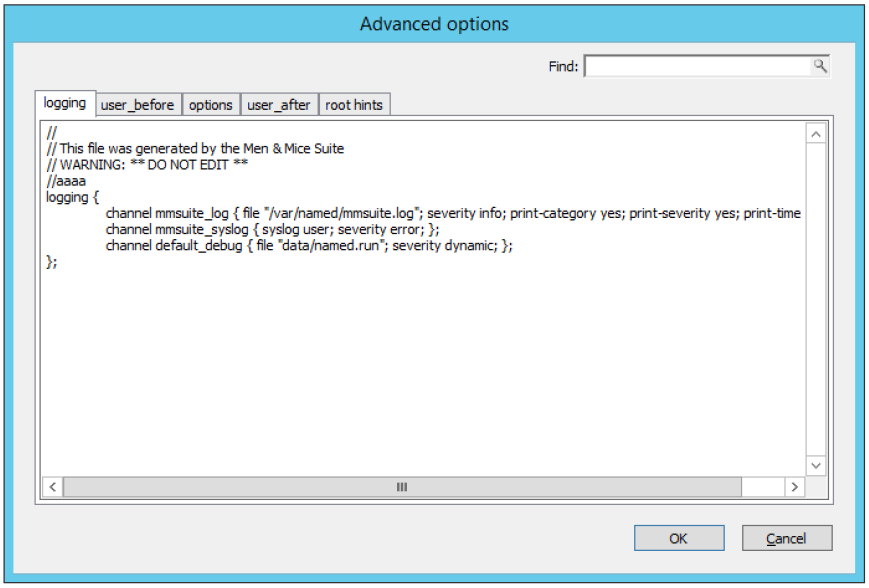
To access the advanced options, do the following:

1. Log in to Men&Mice as the DNS administrator.
2. For a DNS zone or DNS server, right-click and select *Options* from the shortcut menu.
3. When the *Options* displays, click the *Advanced* button.



4. When the Advanced Options dialog box displays, you can edit the options for the zone or server in a text document. The dialog for editing server options contains four tabs where each tab contains a section of the server options (logging, user_before, options, user_after). If the DNS server contains one or more views, each view displays in a separate tab where various settings can be changed for each view.

Note: #include statements are not shown and you cannot add #include statements.



Refer to *BIND DNS File Structure* for more information on each section.

5. Click *OK*. The contents of the files are verified for correctness. If an error is found during verification, an error message displays and the changes are not saved.

Properties

Applies only when custom properties have been defined for DNS servers. Selecting this menu item will display a dialog box where the custom property values can be modified.

1. In the Object browser, select the server for which you want to manage properties.
2. From the menu bar, select *Server* → *Properties*.

Location
Type a location.

4. Click *Apply* or *OK*.

Server Info

This command opens a dialog box that shows information about the history and status of the currently selected server in the Management Console. This includes such things as the server's IP Address, operating system, number of requests & replies received, total uptime, and the number of master and slave zones it has. This command is only available when a server is selected in the Management Console.

In the Object List, right-click on the desired server name and, from the shortcut menu, select *Server Info*.

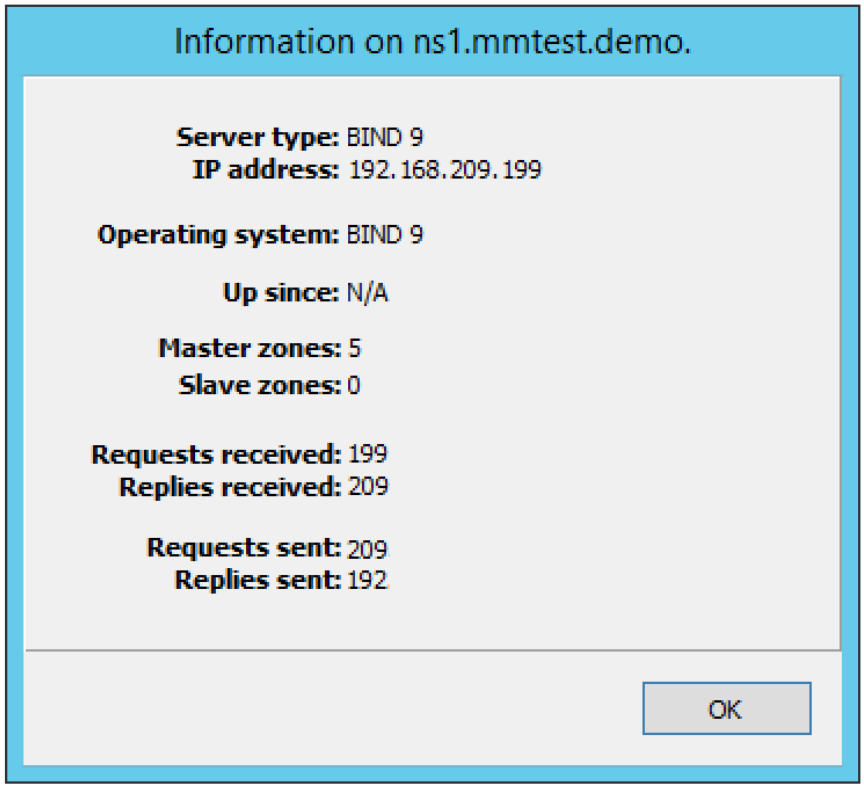
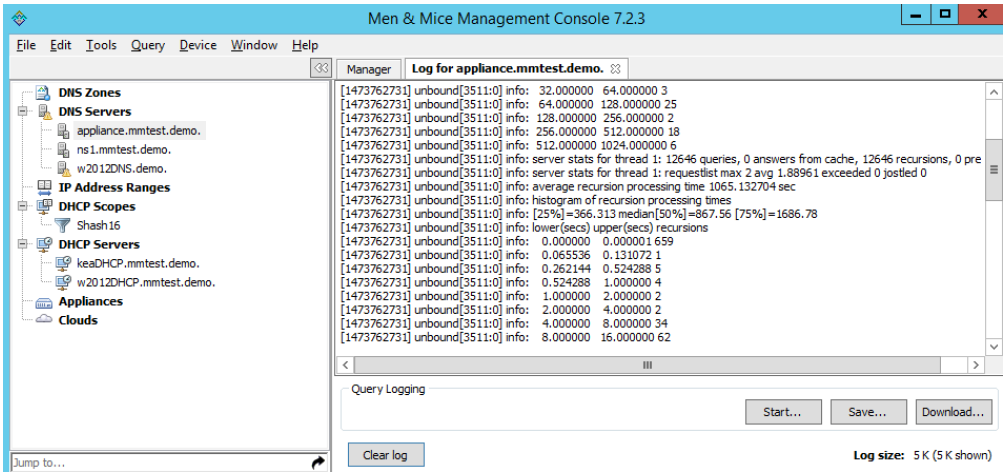


Fig. 3: An Information window opens for the selected server.

Server Log

To view the activity log for a particular server:

In the Object List, right-click on the desired server and, from the shortcut menu, select *Server Log*. A Log tab opens for the selected server that contains a list of activity and maintenance that has occurred on that server since the last time the log was cleared.



You can clear the server log by clicking the *Clear log* button in the server log tab.

Note: For Windows DNS servers, it is not possible to view the server log if connected through an agent-free connection.

Note: If the server log window is opened for a caching DNS server, the window will contain additional buttons related to query logging.

Reload/Reload Zone List

Note: In the Web Application, hitting the browser's 'Refresh' button will reload the data displayed in the context.

There are two reload commands in the Server context and the commands are quite different:

Reload.
: This command reloads the DNS server. On Windows this command has the same effect as the Clear Cache command, but on BIND servers, the command `rndc reload` is sent to the DNS server.

Reload Zone List.
: This command reloads the list of zones from the DNS server. It is useful if a zone has been created outside of Micetro.

To reload the zone list to include zones that have been added/deleted outside of Micetro, do the following:

1. Select the desired server.
2. From the menu bar, select *Server* → *Reload Zone List*. The window grays as the zones are reloaded then displays with the updated zones.

To reload a DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select *Server* → *Reload Zone List*.

Edit DNS Policies

Note: This functionality is only available for Windows Server 2016

For details on how to configure and use DNS Policies, see *DNS policies (Windows)*.

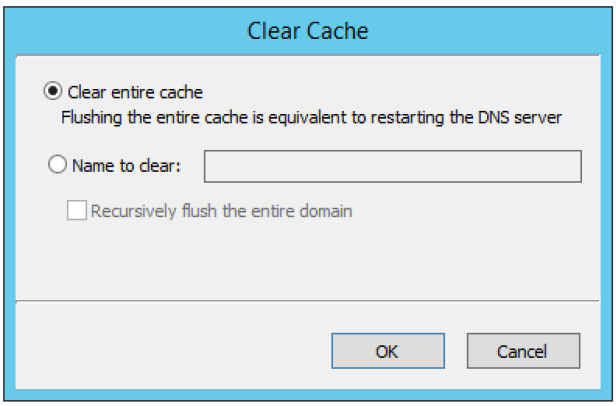
Clear Cache

It is possible to clear the DNS server cache using the Management console's 'Clear Cache' command. The control you have over which cache entries you can clear depends on the DNS server type:

- On BIND, you can choose to clear individual cache entries or the entire cache
- On a Windows DNS server you can only clear the entire cache
- On the DNS Caching Appliance you can clear individual cache entries, an entire domain or clear the entire cache

To clear the cache of a BIND DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select *Server* → *Clear Cache*. The *Clear Cache* dialog box displays.



3. To clear the entire server cache, select *Clear entire cache*. Note that this is the only available option if you are clearing the cache on a Windows DNS server.
4. To clear a specific name, select the *Name to clear* radio button and enter the name you want to clear from the cache. The name is cleared from all views unless you specify the view name after the entry name. Note that this option is not available for Windows DNS servers.

To clear the cache of a Windows DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select *Server* → *Clear Cache*. A confirmation dialog box displays.
3. Click *OK* to clear the cache of the server.

To clear the cache of a DNS Caching Appliance, do the following:

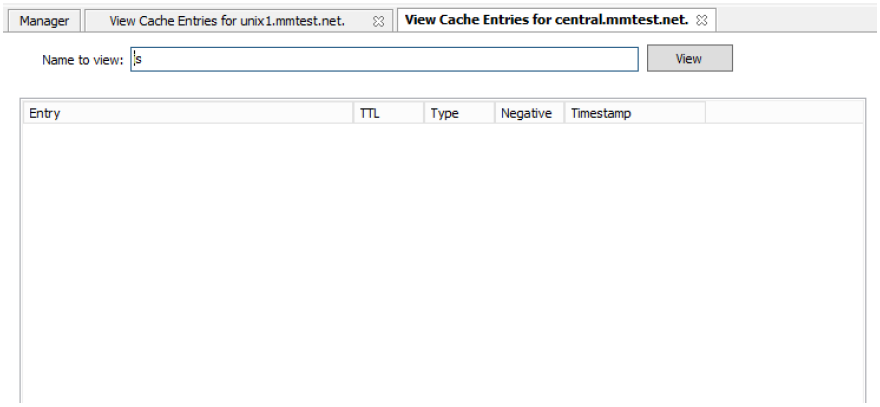
1. Select the desired server.
2. From the menu bar, select *Server* → *Clear Cache*. The *Clear Cache* dialog box displays.
3. To clear the entire server cache, select *Clear entire cache*. Note that this is the only available option if you are clearing the cache on a Windows DNS server.
4. To clear a specific name, select the *Name to clear* radio button and enter the name you want to clear from the cache. If you want to clear an entire domain (the name entered and all names below it), select the Recursively flush the entire domain checkbox.

View Cache Entries (Management Console)

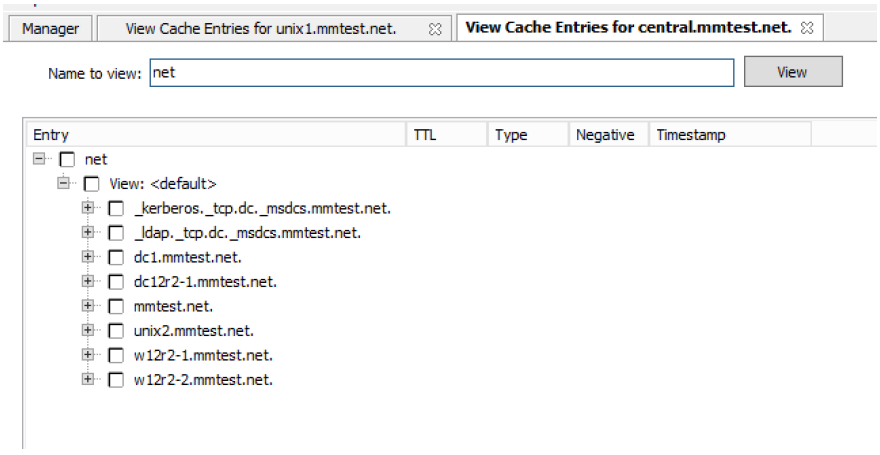
You can view and clear individual DNS cache entries using the View Cache Entries command.

To view the cache of a DNS server, do the following:

1. Select the desired server.
2. From the menu bar, select *Server* → *View Cache Entries*. The *View Cache Entries* tab displays.



3. Enter a name to view and click the *View* button. The entries found are displayed in a tree view.



4. To clear one or more entries from the DNS server cache, select the checkbox for the entries you want to clear.
5. Click the *Clear Selected* button.

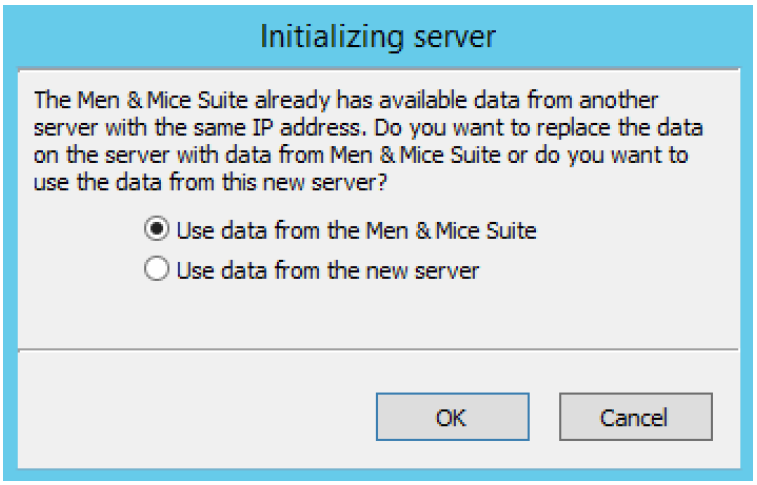
Backup and Restore (BIND Only)

Micetro will automatically backup configuration for all BIND DNS servers it manages. The backup can then be used to restore the DNS server to the backed-up copy of the configuration. The backup is fully automatic and there is no configuration needed.

Automatic backup can be disabled by setting the property `BackupDNSServers` value in Men&Mice central preferences to zero:

```
<BackupDNSServers value="0" />
```

If a DNS server machine crashes and has to be replaced with another machine with the same IP Address, Micetro will detect the new server and consider it to be in an uninitialized state. To be able to work with the server the administrator needs to initialize the server. To initialize the server right-click on the server and select Initialize. This will display a dialog box where the user can choose how the server should be initialized:



- If **Use data from Micetro** is selected, all configurations and DNS zone information on the DNS server will be overwritten with the backed-up data.
- If **Use data from the new server** is selected, all data kept in Men&Mice Central will be ignored and overwritten with current data on the DNS Server.

Basically, the restore scenario is as follows:

1. The DNS server machine crashes and becomes unusable.
2. Configure a new machine to replace the broken machine, using the same IP Address as the old machine.
3. Install the DNS Server Controller on the new machine.
4. When the new machine is up and running, in the Management Console, right-click the server and choose *Reconnect*.

When a connection has been established, Micetro detects that this is a new, uninitialized server. See above for a description on what happens next.

DNS Zones - (Management Console)

Overview

The commands associated with zone management (located on the *Zone menu*) are only available when a specific DNS server or DNS zone is selected. In other words, actions for the DNS zone are only available when DNS zones are listed. When DNS Zones is selected in the Object Browser, all DNS zones are listed on all servers. When a particular name server is selected, only the zones being managed on that server are listed.

Zone Icons

When viewing the zones, you will notice indicators that show the zone type.

The Management Console displays zone type with the following icons:

Table 9: DNS zone icons in the Management Console

Icon	Description
	An icon with a blue dot indicates a static master zone, which is always the original copy of the zone, and always present on that zone's master server.
	An icon with a gold dot indicates a dynamic master zone, which is always the original copy of the zone, and always present on that zone's master server.
	An icon with a purple dot indicates an Active Directory Integrated zone.
	A half page icon represents a stub zone.
	An icon with an arrow pointing to the right represents a forward zone.
	A faded icon without any color marking indicates a slave zone. A slave zone is a duplicate of a master zone that is made on the master zone's slave server(s). Slave zones bring redundancy and stability to the DNS system because it allows more than one server to process domain requests, and allows requests to be processed even if one of the servers becomes unavailable.

Note: These indications are not related to which physical server on which the zone is created. Any server can be the master server. The terms master and slave are only relative to the zones. Whichever server the zone was created on is the master server for that zone. This means that a new zone is always created on the master server.

Zone Viewing

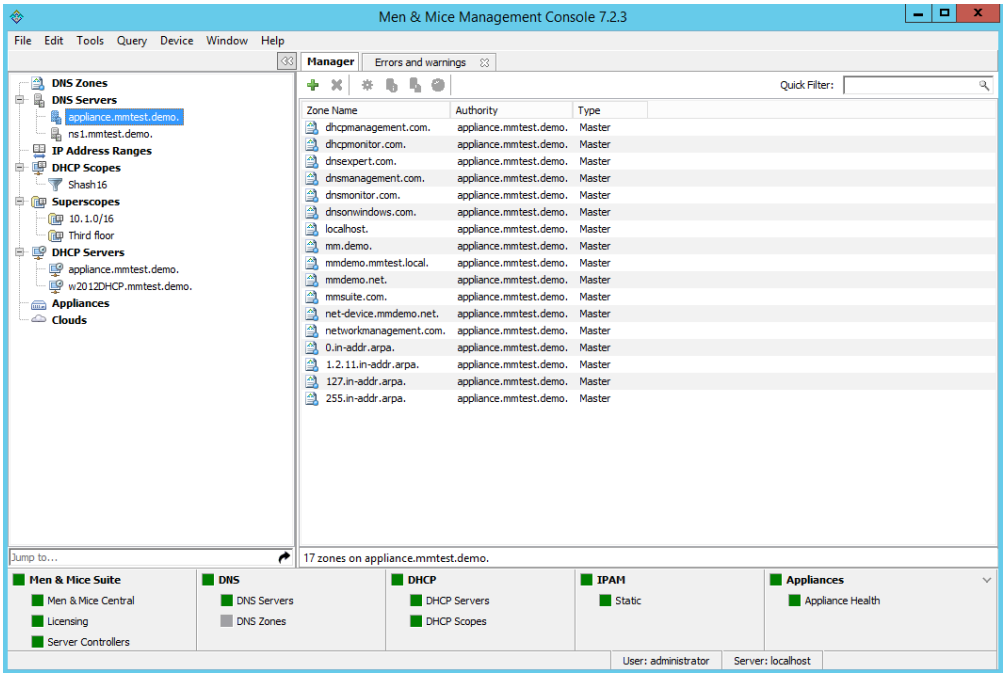
All Zones on All Servers

You can use the Management Console to view all of the existing DNS zones at once, regardless of the server to which they belong.

In the Object Section of the Management Console, click the *DNS Zones* object. This causes all existing zones (to which you have access) to appear in the Object List.

Single Name Server Zones

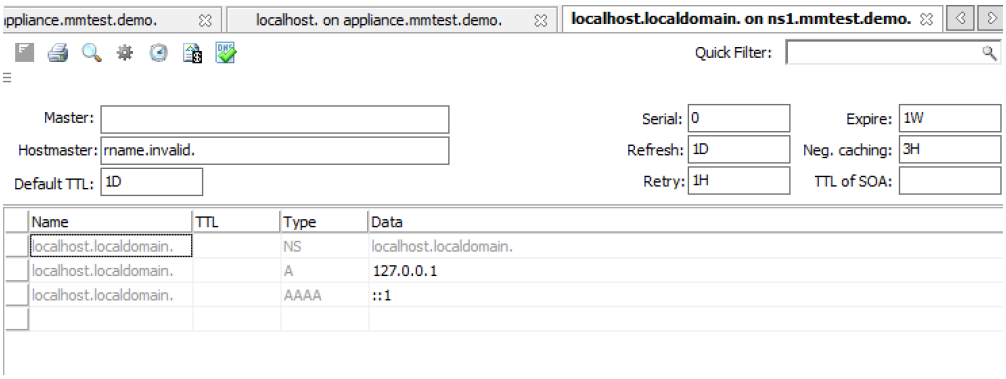
In the Object Section of the Management Console, locate the DNS server that owns the zones you want to view and click on it. (The DNS server(s) will be listed under the DNS Servers object. You may need to click the + sign in order to see it.) When a server is selected, the zone information for that server displays in the Objects List.



Zone Contents

The *Zone* tab provides a detailed look at the data inside of a zone, including its resource records. The name of the zone always displays in the title bar. The header record (a.k.a. Start of Authority or SOA record) displays as a collection of fields above the resource records.

To view the contents of a particular zone, double-click on it. This opens the Zone tab.



SOA Panel

Since the SOA record is seldom modified after it is created, the Zone tab has a built-in control to allow you to conceal the *SOA panel* from view. This allows you to view more of the resource record area below. If you look at the left edge of the Zone tab, just above the record table, you will notice three short horizontal lines, stacked vertically. This is the *Hide/Show SOA panel* control. Click on this control once to hide the SOA panel. Click on it again to make it re-appear.

SOA Fields

Field	Description
Master	This field gives the name of the server that acts as master server for the zone.
Hostmaster	This field is properly formatted by giving the e-mail address of the person responsible for zone with the @ symbol replaced with a period (.). For example, instead of hostmaster@example.com type hostmaster.example.com. The username part of the e-mail address cannot contain a (verbatim) dot (.). See RFC 1912 'Common DNS Operational and Configuration Errors', Section 2.2 for additional information.
Serial Number	The serial number is a ten-digit number consisting of the year, the month, the day, and a two-digit daily revision number. (Actually, it is any integer between 0 and ~ 4 billion, but the preceding is the standard convention.) To create a unique serial number, the Management Console adds 1 to the daily revision number every time the zone is saved.
Refresh	This is the period (in seconds) that determines how often slave servers will check with the master server to determine if their zone files are up to date. This is done by checking the serial number. The default value for this field is 28800, which equates to once every 8 hours.
Retry	This determines the period that a slave server will wait before trying to re-contact the master zone (in the event that an earlier contact attempt is unsuccessful). The default value is 7200 seconds, or once every 2 hours.
Expire	This value determines how long a slave server will keep serving a zone after its last successful contact to the master name server. Once the zone has expired, the slave stops giving information about the zone because it is deemed unreliable. The default expiration period is 604800 seconds, or 1 week.
Neg. caching	This field is only available when connected to a BIND server. This value specifies how long a server will retain (cache) the knowledge that something does not exist. The default value is 86400 seconds, 24 hours.
Default TTL	This value serves as the default time-to-live for all records without an explicit TTL value. The default value is 86400 seconds, 24 hours.
TTL of SOA	This TTL applies to the SOA record. It represents the maximum time in seconds any outside DNS server should cache this data. The default value is 86400 seconds, 24 hours.

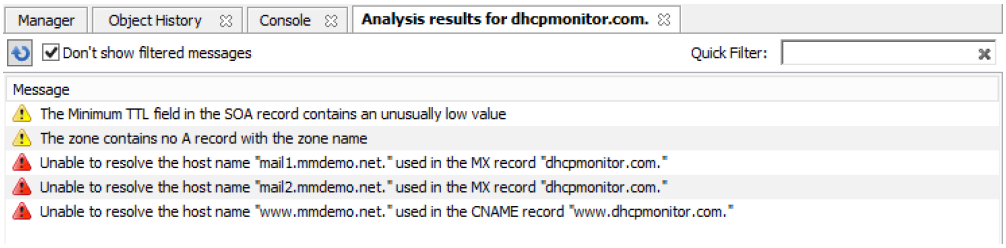
Zone Analysis

The DNS Expert Zone Analysis engine allows zones to be analyzed for correctness in the Management Console.

To analyze a zone, do any of the following:

- Right-click on the zone you want to analyze, and from the shortcut menu select *Analyze*.
- Choose *Zone* → *Analyze*
- Open the zone and click the Analyze button on the toolbar. 

The results of the zone analysis are shown in a new window:



Reanalyze
To perform the analysis again, press F5 or click the *Analyze* button.

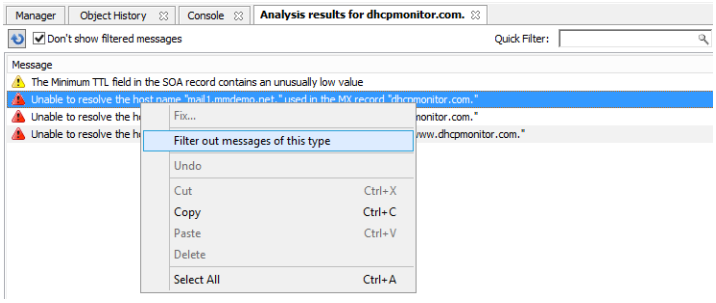
Filtering
It is possible to filter out messages of a certain type. When the checkbox *Don't show filtered messages* is selected, the filtering is active and these messages are not shown in the message list. Deselecting the checkbox disables the filtering and all messages are shown in the message list.

Quick Filter
The Quick filter works the same as it does in other windows.

Messages
The message list shows the results of the zone analysis. Messages are either warnings or errors (as indicated by the icon next to the message). Selecting a message will display detailed information about the message at the bottom of the window.

Fix
When the application can fix an error, the *Fix* menu item becomes available. Selecting this menu item will display more information about the fix for the error.

Filter out messages of this type
Selecting this item, will suppress the display of the selected error type unless the *Don't show filtered messages* checkbox is unselected. NOTE: This setting is global and it is applied to all subsequent analysis in all zones. If you right-click a filtered message, this item will read as Don't filter out messages of this type.



If the zone you are analyzing is open, an icon with an exclamation mark is shown in the bottom left corner of the window. Clicking this icon will display the errors found during the analysis in a list at the bottom of the Zone tab. Closing the analysis window will clear the error message list in the Zone tab.

Access/Access for Non-Master for Zone(s)

Refer to *Access Management*.

Delete zone

Use this command to delete a zone from one or more servers. Before using this command, select the zone you want to delete from the Management Console; the Delete Zone dialog box displays and shows a list of servers on which that zone resides. By default, the zone will be removed from all servers (i.e., all servers are checked). If you want to keep it on one or more servers, clear the checkbox next to that server. Click *Delete* to remove the zone from the selected servers.

1. Select the zone(s) to delete.
2. From the ellipsis menu select *Delete zone* or use *Actions* → *Delete zone*. A confirmation dialog appears.
3. To delete the zone(s) from the selected servers, click the *Yes* button. The zone is removed from the servers.

Warning: The *Delete Zone* dialog, showing each zone you selected and a list of servers that currently serve that zone, is only available in the Management Console. There you are able to keep the zone on particular server(s) by clearing the checkbox next to that server(s).

Note: See console-delete-dns-zone for the zone deletion operation in the Management Console.

Disable/Enable (Management Console)

Note: This function is only available in the Management Console.

Disabling a Zone(s)

This function is only available for static master zones that have no slave zones. (For other types of zones (dynamic or AD integrated) the command is not visible. The Disable command deactivates the entire zone without deleting it. When disabled, the server ignores the contents of the zone. The zone can still be edited while disabled, but changes will not take effect until the zone is re-enabled.

1. In the Object Section, select *DNS Zones* to view all zones, or under the DNS Servers object, select the server containing the zone you want to disable. This displays the zones in the Object List.
2. Select the zone(s) that you want to disable. To select more than one zone, hold down the Ctrl key while making your selections.
3. From the menu bar, select *Zone* → *Disable Zone*. A dialog box prompts you to confirm your decision.
4. To disable the selected zone(s), click the *Yes* button. The zone becomes disabled.

Zones that are disabled appear faded in the Object List. They are still fully accessible and editable, but they will not be active until you re-enable them.

Enabling a Zone(s)

Use the following procedure to re-activate a zone that has been disabled.

1. In the Object List, locate the zone(s) that you want to re-enable. To select more than one disabled zone, hold down the Ctrl key while making your selections.
2. From the menu bar, select *Zone* → *Enable Zone*. A dialog box prompts you to confirm your decision.
3. To enable the zone(s), click the *Yes* button. The Object List refreshes itself and shows that the zone(s) has been restored to active status.

Duplicate

Use the following procedure to create a new zone that is an exact duplicate of an existing one, including master and slave servers, zone data and zone options.

1. In the Object Section, select either *DNS Zones*, or select a specific server under the DNS Servers object. This lists the zones in the Object List.
2. In the Object List, right-click on the zone you want to duplicate and select *Duplicate* from the popup menu. The *Create Zone* dialog box displays.
3. Enter a name for the new zone in the **Zone Name** field.
4. Click the *Create* button. A new zone is created with the same records, Master server, and Slave servers as the original.

Zone Migration Wizard

The *Zone Migration Wizard* allows you to migrate one or more zones from one server to another, including all data in the zone.

To migrate a zone:

1. In the Manager window, select one or more zones.
2. Right-click and, from the shortcut menu, select *Migrate Zone*. The *Migrate Zone(s) Wizard* dialog box displays.
3. For each of the resulting screens, make a selection/entry and move through the wizard.

View Related Servers

This option is used to see on which servers a copy of a particular zone resides.

1. In the Manager window, select one or more zones.
2. Right-click and, from the shortcut menu, select *Related Servers*. A dialog box with information on where a copy of the zone resides displays.
3. Click *OK* to close the dialog box.

Edit Preferred Servers

This option is only available when working with AD integrated zones. (See *AD Sites and Subnets*.) It is used to specify the server to use when opening an AD integrated zone.

It is also possible to specify which server to use if the preferred server becomes unavailable—e.g., the server on the top of the list is tried first and, if that server is unavailable, the second server is tried, and so on.

1. From the menu bar, select *Zone* → *Preferred Server*. The *Edit preferred server list* dialog box displays.
2. Change the order of your servers into the preferred order.
3. Click *OK*.

Export

Use this command to export DNS zone files to standard format.

1. Select the zone you want to export and open the *Zone* tab.
2. From the menu, select *File –> Export*. The *Export zone to text file* dialog box displays.
3. Provide a name and destination for the file and click the *Save* button. All exported files are saved in standard, readable format.

Folders

Refer to *Object folders* for details on this function.

Forward Zone

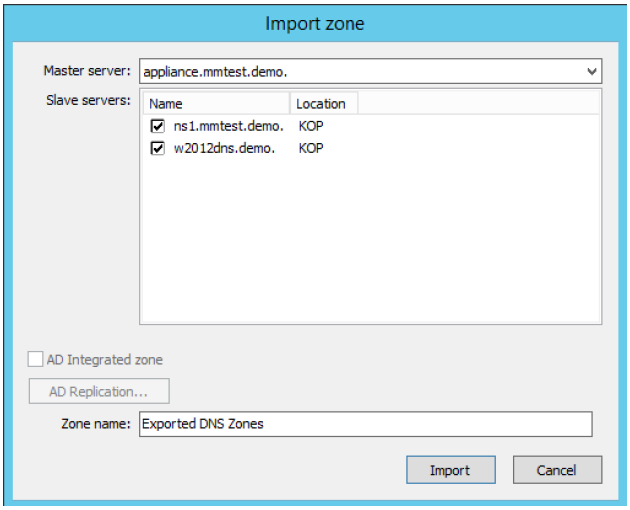
For creating a forward zone in the Management Console, see console-forward-zone.

Import

Note: This is a function that allows importing DNS *zones*. To import DNS *records* see webapp-import-dns-records.)

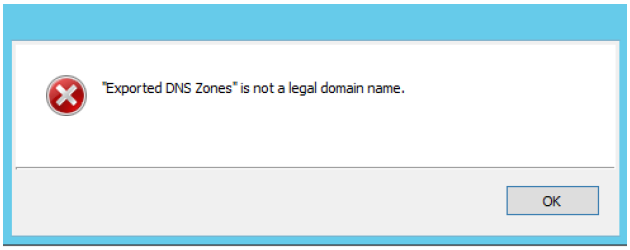
Through this function, you can import multiple DNS zones at one time.

1. Use *File* → *Import Zone*. The *Import* dialog box displays.
2. Locate the zones to be imported. The zones must within the same folder. To select multiple zones, press/hold the Ctrl key. Then click on each zone.
3. Click *Open*. The files are uploaded and the *Import zones* dialog box displays.



4. Click *Import*.

If you happen to select an invalid zone, the following error message dialog box displays:



5. Click *OK* and when you return to the *Import zones* dialog box, clear the field containing the zone.

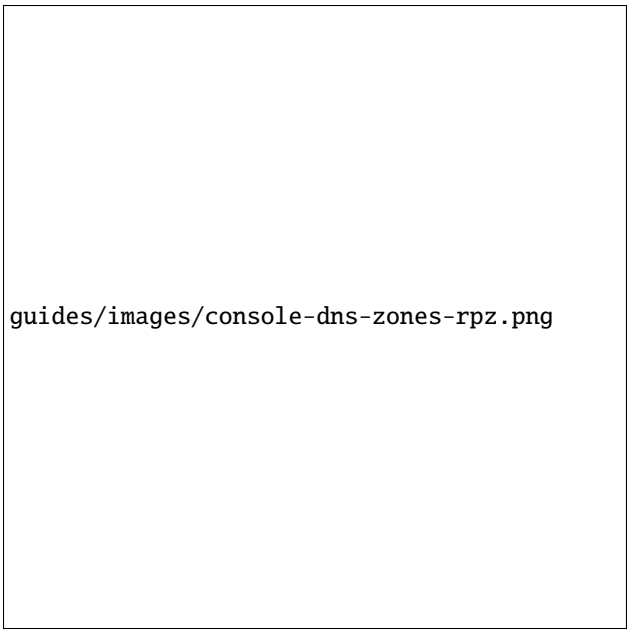
Master Zone

For creating master zones in the Management Console, see console-create-master-dns-zone.

DNS Response Policy Zones (BIND only)

The ISC BIND name server (9.8 or later) supports DNS Response Policy Zones (RPZ). You can find more information on RPZ at dnsrpz.info

You can manage RPZ zones from within Micetro with the Management Console. When you open the *Options* dialog box for a master zone on a BIND server you will see the *Response Policy Zone* checkbox. To specify zone as an RPZ zone, just click the checkbox.



Note: To use RPZ, a response-policy statement must exist in the DNS server options file. The *Response Policy Zone* checkbox is disabled if a response-policy statement is not present. For example

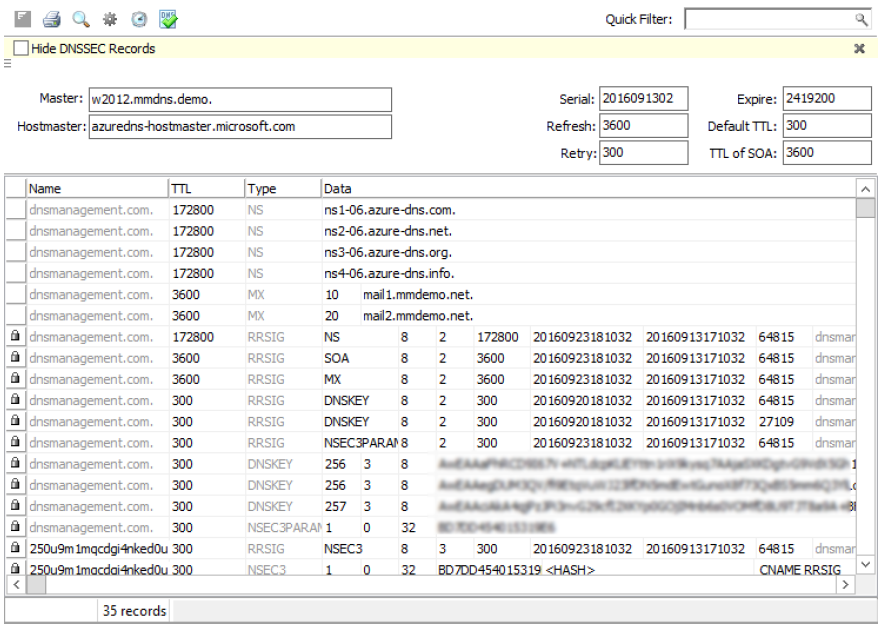
```
options {
  ...
  response-policy {zone "rpzzone.com" ;};
  ...
};
```

DNSSEC Zones

Note: DNSSEC signed zones can be listed in the Web Application by selecting *DNSSEC signed* in the filtering sidebar on the left.

Zones containing DNSSEC records are labeled as "Signed" in the DNSSEC column in the zone list.

When DNSSEC zones are opened, the system ignores most DNSSEC records unless the system setting to include DNSSEC records has been set.



Note: All DNSSEC record types, with the exception of the DS and NSEC3PARAM record types, are read-only.

DNSSEC Management on Windows Server 2012

You can use Micetro to manage DNSSEC on Windows Server 2012. You can sign and unsign zones. You can customize the zone signing parameters and add, edit and remove Key Signing Keys (KSK) and Zone Signing Keys (ZSK).

The details of DNSSEC are beyond the scope of this documentation. For more information on Windows Server 2012 and DNSSEC, see the Microsoft web site http://www.microsoft.com.

Signing Zones using DNSSEC

To sign a zone on a Windows Server 2012, do the following:

1. With the zones displayed in the Object List, select the zone you wish to sign.
2. Do one of the following to display the *Zone Signing* dialog box:

- Right-click on the zone record and select *Sign Zone*.
- From the menu bar, select *Zone* → *Sign Zone*.

3. Select an option for signing the zone:

Customize zone signing parameters.
Signs the zone with a new set of zone signing parameters. When this option is selected you can choose or create new Key Signing Keys (KSK) and Zone Signing Keys (ZSK).

Sign the zone with parameters of an existing zone.
Signs the zone using parameters from an existing signed zone. To use this option, you must enter the name of the zone containing the parameters to use.

Use default settings to sign the zone.
Signs the zone with the default zone signing parameters.

4. Click *Next*. If you chose the *Customize zone signing parameters* option, the zone signing wizard allows you to choose KSK and ZSK for signing the zone. If you chose either of the other options, an overview panel displays in which you can see the zone signing parameters that will be used to sign the zone.
5. Click *Finish* to complete the zone signing process.

Unsigning Zones using DNSSEC

To unsign a zone on a Windows Server 2012, do the following:

1. With the zones displayed in the Object List, select the zone you wish to unsign.
2. Do one of the following to unsign the zone:
   - Right-click on the zone record and select *Unsign Zone*.
   - From the menu bar, select *Zone* → *Unsign Zone*.
3. The zone is unsigned and all DNSSEC records are removed from the zone.

Options

Note: Using the Web Application's *Properties* you can edit custom properties that's been configured for DNS zones.

The Zone Options dialog box is where you can configure individual settings for a specific zone on each server.

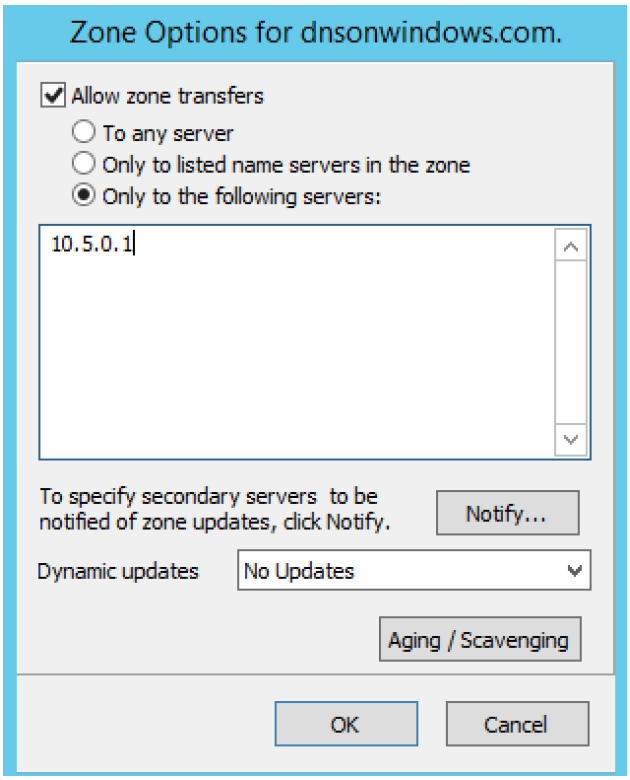
Zone Options (Windows and BIND)

To access the zone options for a specific zone only, do the following:

1. With the zones displayed in the Object List, select the zone you wish to configure.
2. Do one of the following to display the Zone Options dialog box:
   - Right-click on the zone record and select *Options*.
   - From the menu bar, select *Zone* → *Options*.
   - On the toolbar, click the *Options* button.
3. Depending on the type of zone you select, the Option dialog box varies.

Master zones

Allow Zone Transfers.
When enabled, zone transfers will occur according to the method indicated by the radio buttons below. You must select at least one of these methods.



To any server.
When selected, the zone transfer will be performed to any requester.

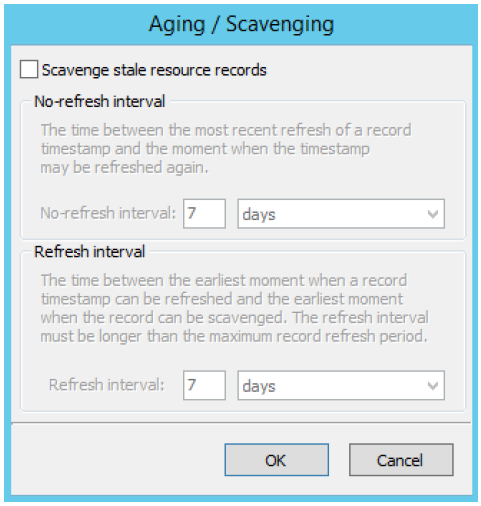
Only to listed name servers in the zone.
When selected, the zone will be transferred from the server to any other name server listed in the zone.

Only to the following servers.
When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP Address.

Dynamic updates.
Specifies whether dynamic updates are allowed for the zone

AD Replication.
Displays a dialog box where you can set the AD Replication options for the zone.

Aging/Scavenging.
Displays a dialog box where aging and scavenging options can be set for the zone.



Slave Zones

Allow Zone Transfers.
When enabled, zone transfers will occur according to the method indicated by the radio buttons below. You must select at least one of these methods.

To any server.
When selected, the zone transfer will be performed to any requester.

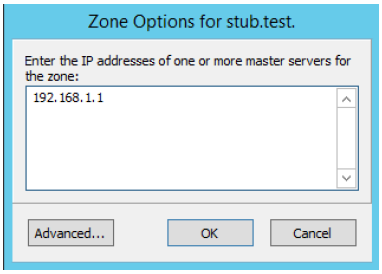
Only to listed name servers in the zone.
When selected, the zone will be transferred from the server to any other name server listed in the zone.

Only to the following servers.
When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP Address.

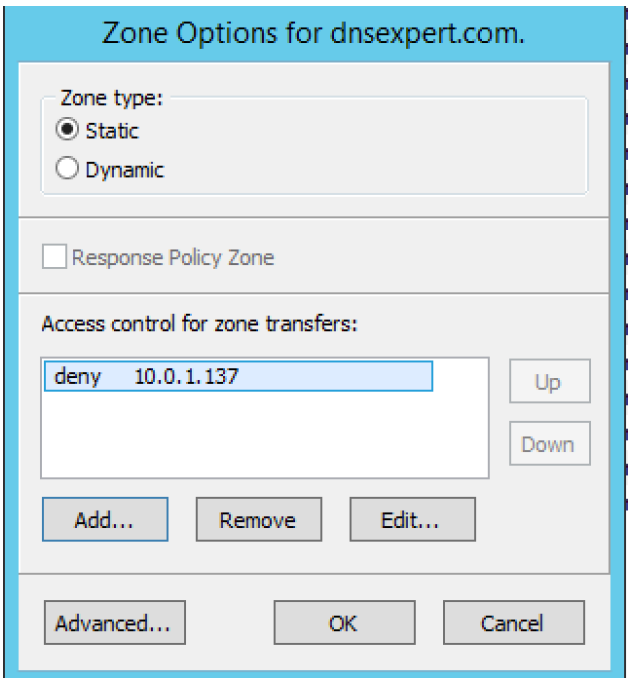
IP Addresses of master.
Type the IP Address of the master servers for the zone.

Stub/Forward Zones

Type the IP Address of the master servers for the zone.



BIND Servers



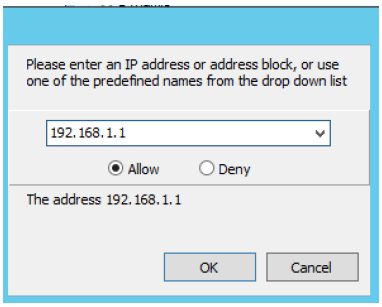
The Zone Options dialog box lets you specify an IP Address (or an address block) from which zone transfers can be allowed, or disallowed.

The top section of the Options dialog box lets you designate the zone as either Static or Dynamic. Newly created zones are static by default, but can be changed to a dynamic zone (and vice versa) using this option. Refer to *Dynamic Zones* for more information on dynamic zones versus static zones.

Addresses that have already been setup to handle (i.e., allow or disallow) zone transfers are listed in the lower area of the Zone Options dialog box. If you want to change the settings associated with an address that is already listed here, select it and click on the Edit button. To remove the access control completely, select it from the list and click the Remove button.

To specify a new address (or block) on which you want to implement access controls, do the following:

1. Click the *Add* button. A small dialog box displays, prompting you to enter the server's IP Address, an address block, or to use one of the predefined names from the drop-down list (any, none, localhosts, localnets).

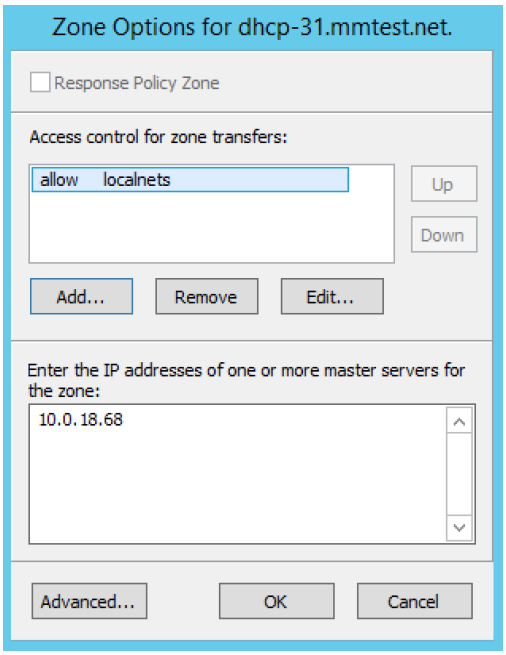


2. After entering the address, select either **Allow** or **Deny** to specify whether to permit or disallow access to/from this address.

3, Click *OK* to save the selection. The new address is now listed in the Zone Options dialog box.

Note: BIND uses journal files to keep track of changes to dynamic zones. The data in the journal files is merged with the zone data file at a designated interval. It is not possible to manually merge the data from the journal files to the zone data file. This means that if there is data in the zone's journal file when the zone type is changed to a static zone, the entries in the journal file will not be visible in the Management Console.

Slave Zones on BIND Servers



When a slave zone is hosted on a BIND server, the Options dialog box will look like the one below.

Besides being able to setup the access control (as described in the previous section), you can also specify the IP Address of one or more master servers for the zone.

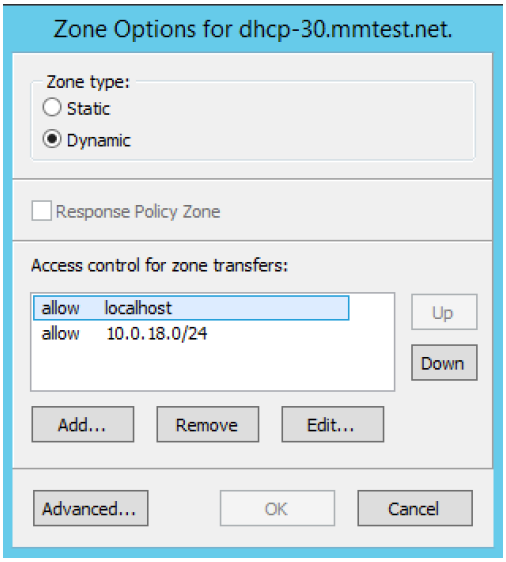
The master servers are specified in the lower half of the Zone Options dialog box. To add a new server to the list, simply click in the white space and enter the IP Address of the master server you are assigning.

To change the address of an existing server, click on it and make the desired edits.

Advanced Options

DNS Administrators can now access the BIND configuration files directly to edit DNS server and zone options that are not available in the GUI. Refer to *Advanced Server Options* for details.

Options for a zone



If a zone exists on more than one server (e.g., in a master/slave configuration), it is possible to select the zone instance for which you want to set options.

1. Select the applicable zone.
2. From the menu bar, select *Zone* → *Options for*.
3. From the submenu, select the desired zone/zone instance (e.g., Master Zones only, Slave Zone only, etc.). The Zone Options dialog box displays.

   Allow zone transfers
   When selected, enables the zone transfer options.

   To any server
   When selected, the zone transfer will be performed to any requester.

   Only to listed name servers in the zone
   When selected, the zone will be transferred from the server to any other name server listed in the zone.

   Only to the following servers
   When selected, the zone will only be transferred to the servers you specify in the list below. To enter a server, click in the first available row and enter its IP Address.

   Dynamic Updates
   Specifies whether dynamic updates are allowed for the zone

   Aging/Scavenging
   Displays a dialog box where aging and scavenging options can be set for the zone.
4. When all selections/entries are made, click *OK*.

Promote Slave to Master

The Promote Zone feature makes it possible to change a slave zone to a master zone. This might be necessary in emergency situations, for example if the master zone becomes unavailable for an extended period of time. This feature is only available for DNS Administrators.

When a slave zone is promoted, the following actions are performed:

- Micetro checks whether the most recent copy of the zone is found in its internal database or on the server hosting the slave zone and uses the copy that is more recent.
- The server hosting the slave zone is configured so that the zone is saved as a master zone on the server.
- The zone history and access privileges from the old master zone are applied to the new master zone.
- The configurations of other instances of the slave zone are modified so that they will get the updates from the new master zone.

To promote a slave zone to a master zone:

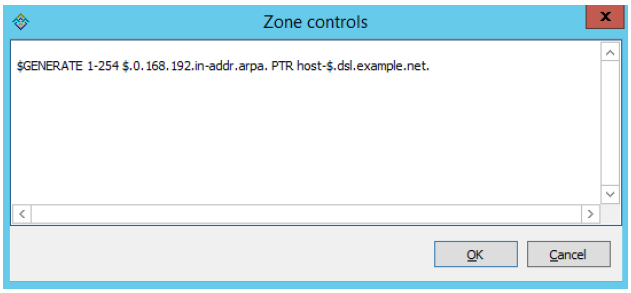
1. Select the DNS server that contains the slave zone.
2. Right-click the slave zone you want to promote and, from the shortcut menu, select *Promote to master*. An information message displays:

3. Click *Yes* to continue, or *No* to discontinue the process.

Zone Controls (BIND only)

The Zone Controls feature allows you to create and edit $GENERATE statements in static zones on BIND DNS servers.

1. Open the zone you want to work with.
2. On the Toolbar click the Zone Controls button  . The Zone Controls dialog box opens, showing any $GENERATE statements that exist in the zone. The $GENERATE statements are shown in a multiline edit field.



3. Make the necessary adjustments to the statements and click OK.

Note: The fields for each $GENERATE statement must be separated by a tab.

Reload

Sends a command to the DNS server instructing it to reload the zone data.

Set Folder

Allows you to add or remove zones from folder.

> **Warning:** If you remove a zone from a folder, there is no way to undo this action.

1. Highlight the zone you want to remove from a folder.
2. From ellipsis menu select *Set folder* or use *Actions* → *Set folder*.

Search

For searching in the DNS zone tab in the Management Console, see console-dns-search.

Slave Zone

For creating slave zones in the Management Console, see console-create-slave-zone.

Stub Zone

For creating stub zones in the Management Console, see console-stub-zone.

View History

Opens the History window and displays a log of all changes that have been made to the zone, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user. See *Object Change History*.

DNS resource records (Management Console)

Overview

Each zone contains DNS resource records that define how requests are processed or delegated by the zone.

Types of Resource Records

There are varieties of resources records that actively affect zones, as well as several informational records that can be used to provide supporting data about a zone. The primary record types are described below.

NS

The Name Server record is used to list a name server for this zone. NS records state the domain name of the zone's name servers. The name of an NS record is the fully qualified domain name of a zone. Every zone must have at least one NS record with the same name as the zone itself.

Example:

Name	Type	Data
example.com.	NS	ns1.example.com.

A

Also known as an Address record, an A record declares the IP Address of a domain name. Defines a Hostname-to-IP Address mapping, or a forward mapping.

Example

Name	Type	Data
example.com.	A	192.168.0.1

PTR

Also known as Pointer records, PTR records define an IP Address-to-Hostname mapping, known as a reverse mapping. A properly configured reverse zone has one PTR record providing the reverse lookup for each IP Address. All reverse zones are traditionally part of the `.in-addr.arpa.` zone. The proper formatting for a PTR record is the 4 octets of the IP Address in reverse order, followed by `.in-addr.arpa.` A properly formatted PTR record for the A record (above) is shown in the following example.

In the event that you have multiple A records concerning the same IP Address, choose one for the PTR record. If one of the host names is used for a mail server, give that hostname preference because a common use of reverse lookup is to check the source of e-mail.

Example

Name	Type	Data
1.0.168.192.in-addr.arpa.	PTR	example.com.

CNAME

Canonical Name records are used to define an alias. The canonical or primary DNS domain name used in the data is required and must resolve to a valid DNS domain name in the namespace. The name of the record is the name of the alias. Thus, if you want www.example.com to bring visitors to example.com, you'd need to add the line shown in following example:

Example

Name	Type	Data
www.example.com.	CNAME	example.com.

MX

Also known as Mail Exchange records, MX records create mail routes. Each exchanger host must have a corresponding host (A) address resource record in a valid zone. The first field in the record data is the preference number; this is the order in which mail hosts will be used by an outside mail server trying to send mail to a domain. Mail hosts will be contacted from the lowest preference number and work up to higher preference number. If two MX records have the same preference number, they will be used in random order. Mail servers with the same preference number will not forward to each other, nor will they forward to a mail server with a higher preference number.

Example

Name	Type	Data
example.com.	MX	10 mail.example.com.

AAAA

Maps a DNS domain name to an Internet Protocol (IP) version 6 128-bit address.

Example

Name	Type	Data
host.example.com.	AAAA	4321:0:1:2:3:4:567:89ab

WKS

Similar in function to MX records, Well-Known Service (WKS) records describe the well-known IP services supported by a particular protocol on a specific IP Address. They provide TCP and UDP availability information for IP servers. Multiple WKS records should be used for servers that support both TCP and UDP for a well-known service or that have multiple IP Addresses that support a service.

Three fields of data are required: IP Address, protocol, and a service list.

Example

Name	Type	Data
host.example.com.	WKS	10.0.0.1 TCP (ftp smtp telnet)

Warning: Please note that the record type WKS was deprecated by RFC1123 - please don't use this record type.

RP

The Responsible Person record specifies the domain mailbox name for the person responsible for that domain. This name is then mapped to a domain name in for which (TXT) resource records exist in the same zone. When RP records are used in DNS queries, subsequent queries are used to retrieve associated text (TXT) resource record information. Two fields of data are required: the domain name you are searching, the domain where TXT resource records exist.

Example

Name	Type	Data
my.example.com.	RP	who.example.com txtrec.example.com

AFSDB

The Andrew File System Database resource record maps a DNS domain name to the host name for a server computer of a server subtype. Two fields of data are required:

The first is a subtype, which can have one of two supported numeric values:

- A 1 indicates that the server is an AFS version 3.0 volume location server for the named AFS cell.
- A 2 indicates that the server is an authenticated name server holding the cell-root directory node for the server that uses either Open Software Foundation's (OSF) DCE authenticated cell-naming system or HP/Apollo's Network Computing Architecture (NCA).

The second field is the server's host name.

Example

Name	Type	Data
abc.example.com.	AFSDB	1 afs-server.example.com.

SRV

Service records are intended to provide information on available services. They allow multiple servers providing a similar TCP/IP-based service to be located using a single DNS query operation.

An SRV record has four fields and a special system for naming. The naming system is an underscore followed by the name of the service, followed by a period, an underscore, and then the protocol (generally TCP or UDP), another dot, and then the name of the domain. The four fields are:

Priority
Used the same way as the preference number in MX records.

Weight
This determines the relative capacity between SRV fields with the same priority. Hits will be assigned proportionately by weight, allowing a powerful and a weak server to share appropriate loads.

Port
The port of the service offered.

Hostname
The name of the domain.

Example

Name	Type	Data
_http._tcp.example.com.	SRV	10 5 80 www.example.com.

HINFO

The Host information resource record specifies the type of CPU and operating system, respectively, for the host DNS domain name. This information is used by some application protocols, such as FTP, which use special procedures when communicating with computers of a known CPU and operating system type. Hardware information belongs in the first data field and OS information in the second field, as shown in the example below.

Example

Name	Type	Data
compname.example.com.	HINFO	Intel-PIII WIN2K

TXT

A Text Record allows you to include up to 255 characters of free-form descriptive text in your zone file. The order of resource records in zone files is not preserved, so it is best to keep messages confined to one record.

Example

Name	Type	Data
random.example.com.	TXT	The quick brown fox jumped over the lazy dog."

LOC

Geographic Location Records provide exact altitude, latitude, and longitude information. There is not much in the way of a practical application for this record, though some industries may find it to be of limited value. The LOC record can accept as few as three or as many as six fields of data:

- Degrees latitude in degrees, minutes, seconds, N or S
- Degrees longitude in degrees, minutes, seconds, E or W
- Altitude in meters. This is single value, you may add an M.
- Size of machine in terms of an enclosing sphere in meters radius. Expressed as a number, or a number immediately followed by an M. (Optional.)
- Horizontal precision of the data in meters, with or without an M. (Optional, not available if 4 is blank.)
- Vertical precision of data in meters, with or without an M. (Optional, not available if 5 is blank.)

Note: The Microsoft DNS server does not support LOC records.

Example

Name	Type	Data
geo.example.com.	LOC	42 21 43.528 N 71 05 06.284 W 12m

NAPTR

NAPTR stands for Naming Authority Pointer and is a resource record type that supports regular expression based rewriting. The NAPTR record accepts six fields of data:

Preference
When there are multiple NAPTR records with the same name, the record with the lowest preference number is picked first.

Weight (Order)
This field specifies the order in which the NAPTR records MUST be processed to accurately represent the ordered list of Rules. This field is only used when there is more than one record with the same preference

Flags
This field contains flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set A-Z and 0-9.

Service
This field contains a character-string that specifies the Service Parameters applicable to this delegation path.

Regexp
This field contains a character-string that contains a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup.

Replacement
This field contains a domain name, which is the next domain name to query for, depending on the potential values found in the flags field.

Example

Name	Type	Data
104	NAPTR	100 10 u sip+E2U !^.*$!sip:info@info.example.test!i .

SSHFP
SSHFP stands for SSH Public Key Fingerprint. This resource record type is used for publishing SSH public host key fingerprints in the DNS System, in order to aid in verifying the authenticity of the host. The SSHFP record accepts 3 fields of data:

Algorithm
Specifies the algorithm number to use.

Fingerprint type
Specifies the fingerprint type to use.

Fingerprint
The fingerprint for the record.

For further information on this record type, see RFC 4255.

Example

Name	Type	Data
random.example.com	SSHFP	1 1 23D3C516AAF4C8E867D0A2968B2EB999B3168216

SPF
SPF stands for Sender Policy Framework. This record type is used in an e-mail validation system designed to prevent e-mail spam. The SPF record accepts a text string that contains the configuration info that should be used.

For further information on this record type, see RFC 4408.

Example

Name	Type	Data
example.com	SPF	v=spf1 a mx -all

TLSA
The TLSA DNS record is used to associate a TLS server certificate with the domain name where the record resides.

For further information on this record type, see RFC 6698

A TLSA record has four fields, which are:

Certificate usage
Specifies the association that will be used to match the certificate.

Selector
Specifies which part of the TLS certificate will be matched against the certificate association data

Matching type
Specifies how the certificate association is presented

Certificate associate data
Specifies the certificate association data to be matched

Example

Name	Type	Data
example.com	TLSA	3 1 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971

CAA
The CAA (Certification Authority Authorization) DNS record is used to specify which Certification Authorities (CA) can issue certificates for the domain.

Example

Name	Type	Data
example.com	CAA	0 issue “letsencrypt.org”

In addition to the supported record types in the table, Micetro supports the following DNSSEC resource record types:

- DNSKEY (read-only)
- NSEC (read-only)
- NSEC3 (read-only)
- NSEC3PARAM
- RRSIG (read-only)
- DS
- DLV (read only)

Note: All DNSSEC specific record types, with the exception of the DS and NSEC3PARAM record types, are read only.

It is beyond the scope of this documentation to discuss DNSSEC management so these record types are not explained in detail. For further information on these resource record types and DNSSEC in general, we recommend the DNS Extensions section on the IETF web site.

Resource Records

To select a *single resource record*, do the following:

- Click on the gray square to the left of the record. This highlights the entire record.

Once a record is selected, you can perform various editing actions on it, such as deleting, cutting, or copying. These are discussed in more detail later in this section. Many editing action can be performed on multiple records simultaneously. Simply select the records you want to operate on and perform the editing action as usual.

To select non-consecutive records, do the following:

- Hold down the Ctrl key and select each record as usual.
- When you are done selecting records, release the Ctrl key.
- To select a contiguous series of records, select the first record in the series as usual, then hold down the [Shift] key and select the last record in the series. All records in between will automatically be selected.

New Records

If you are comfortable editing the record table directly, you can use this procedure to insert a new record directly in the zone tab.

1. Open the zone to display the resource records in the zone you want to edit.
2. In the grid, select the record that is directly *above* where you want to insert the new record.
3. Right-click anywhere in the selected record and, from the shortcut menu, select *Insert Record*. A new, blank record is added.
4. Starting with the Name field, enter the domain name.

> **Warning:** If you enter a domain name that is not fully qualified (i.e., does not end in a trailing dot `.`), Micetro will assume that you are using a local name and will automatically append the name of the zone onto the end of the name, making it a fully qualified domain name. That means when adding the name server `ns1` to the zone `example.com`, you should enter either just `ns1` or `ns1.example.com`. If you leave off the trailing dot Micetro will interpret your intention as `ns1.example.com.example.com`. The information automatically filled in by the Web Application appears greyed out.

5. In the **Type** field select the appropriate type from the dropdown. The following types of resource records can be created: NS, A, PTR, CNAME, MX, AAAA, WKS, RP, SRV, TXT, and SPF. The appropriate number of fields is automatically created in the Data field based on the type you entered. If you enter the wrong record type, you will be unable to change it. You must delete the record, insert a new one, and re-enter the record information.
6. Enter the appropriate data for your record type.
7. Click the *Save* button to save the new record to the zone.

Deleting Records

Deleting a record removes both the data and the physical record from the grid. Records beneath the deleted one are instantly moved up to fill in the space.

1. Select the record(s) that you want to delete. To select multiple records, hold down the Ctrl (or Cmd on Mac) key while making you selections.
2. Right-click anywhere in the zone window, and select Delete Record from the context menu. The record is immediately deleted from the zone.

Clearing Records

When the whole record is selected, the *Clear* command works the same as the *Delete Record* command. The Clear command is really intended for deleting the contents of an individual field of data, leaving the rest of the record's data intact.

1. In the *Zone* window, select the field (cell) whose contents you want to delete.
2. Right-click anywhere in the zone window and select *Clear* from the context menu. The data is removed from the field. (The cell is not removed, and the rest of the record is unaffected.)

Disable/Enable Records

You can disable a record without deleting it. The disabled record performs no function; however, it can be instantly enabled when its services are needed, without having to re-type the record.

Note: You cannot disable and enable records in dynamic zones.

How to Disable a Record

1. Select the record(s) that you want to disable. To select more than one record, hold down the Ctrl (Cmd on Mac) key while making your selections.
2. From the ellipsis menu select *Disable DNS record* or use *Actions* → *Disable DNS record*.

Note: Disabled records are grayed out in the grid, and will show an *Enable DNS record* action instead.

---

3. In the confirmation dialog, click *Save now* to save the changes, or *Add to request* to add it to the request queue. (See *Workflow Management* for details on the request queue.)

Cut, Copy, and Paste

When working with records in the Management Console, there is no need to enter the same records in different zones. All records can be copied (or moved) to other zones simply by copying and pasting them between different zone windows.

To facilitate this, the Copy and Paste functions do not use fully qualified host names, so it is easy to work with records between zones.

This means that if you copy a record from the domain example.com, such as: `www.example.com. CNAME example.com.` and paste the record to sample.com, it displays as: www.sample.com. CNAME sample.com.

To cut, copy, and paste records, do the following:

1. Select the record(s) that you want to move or copy. To select multiple records, hold down the Ctrl key while making your selections.
2. Right-click anywhere in the Zone window and choose either *Cut* (to move the record) or *Copy* (to duplicate the record elsewhere) from the context menu.

Note: The Cut, Copy, Paste, and Clear commands can also be selected from the Edit menu in the main window.

---

3. Open the destination zone in which you want to insert the record(s).
4. In the destination zone, insert a new blank record in the location where you want to paste the records. To do this, right-click on the record immediately above where you want to paste the new one(s), then select *Insert Record* from the popup menu.
5. Select the blank record.
6. Right-click anywhere in the Zone window and choose *Paste* from the context menu. The new record(s) are pasted in the destination zone.The Management Console allows you to undo most editing actions, such as deleting, clearing, cutting, and pasting.
7. When you perform an editing action, the *Edit* menu's *Undo* command is modified to include that action. For example, if you disable a record, the Undo command changes to *Undo Disable*. Selecting this command will reverse the action and restore the previously deleted record. When you perform an Undo action, the Redo command becomes active. Selecting this command reverses the previous Undo action. If you perform multiple editing actions in a row, the Undo command can be used repeatedly to restore each prior action.

Undo/Redo Commands (Management Console)

The Management Console allows you to undo most editing actions, such as deleting, clearing, cutting, and pasting.

When you perform an editing action, the Edit menu's Undo command is modified to include that action. For example, if you disable a record, the Undo command changes to Undo Disable. Selecting this command will reverse the action and restore the previously deleted record.

When you perform an Undo action, the *Redo* command becomes active. Selecting this command reverses the previous Undo action.

If you perform multiple editing actions in a row, the Undo command can be used repeatedly to restore each prior action.

DNS policies (Windows)

Note: Managing DNS policies for Microsoft DNS servers is only available in the Management Console.

DNS Policies and DNS Scopes

DNS policies are processing rules that control DNS operations on the DNS server. Creating a DNS policy enables user control over the details of these DNS operations: query processing, zone transfer, recursion and dynamic update. A DNS policy is always specific to one DNS operation and apply either on the server level or the zone level. This control of DNS operations can, for example, be used to implement the following scenarios:

- High availability of DNS services
- Traffic management
- Split-brain DNS
- Filtering
- Forensics
- Redirection based on date/time

Specific types of policies are:

Zone transfer policies
Controls how zone transfers are processed, either for the DNS server or a specific DNS zone.

Recursion policies
Control how recursive DNS queries are processed by the DNS server.

Query resolution policies
Controls how queries are processed for the DNS server or a specific zone.

Dynamic update
Controls how dynamic updates are processed

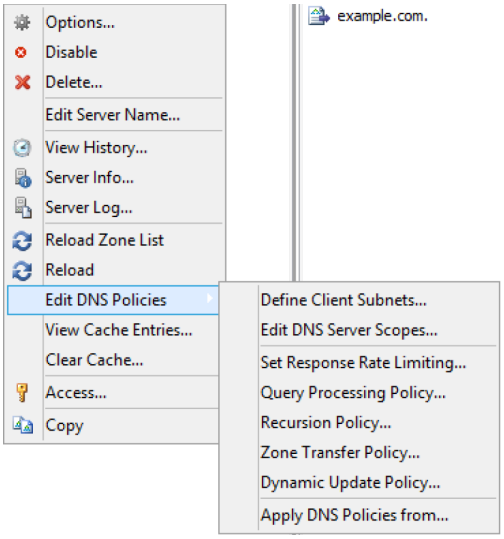
Rate limiting exception list
Controls how rate limiting is configured

DNS policies are used in conjunction with zone scopes and server scopes which are a new concept introduced in Windows Server 2016. A zone scope represents a specific version of an existing zone while a server scope is a collection of DNS server settings that is associated with a unique name.

Edit DNS Policies

Editing or adding DNS policies on Windows Server 2016 is done by

1. Right click on the server in the sidebar as shown in the figure.
2. Select *Edit DNS Policies*.
3. A menu is displayed that offers to do add or edit various types of policies and configure related properties.



Define Client Subnets

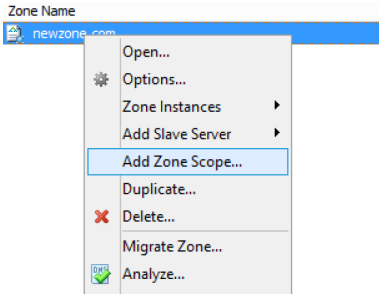
This allows the user to specify those subnets that will be used by the DNS policies to identify where a DNS client is located.

1. Select the *Define Client Subnets* in the submenu of *Edit DNS Policies*.
2. Click the *Add* button to add a new client subnet.
3. Specify the name of the subnet and a list of subnets in CIDR notation, that will be used in the exclusion rules.

Add DNS Zone scopes

To add a new zone scope:

1. Right click on a DNS zone.



2. Select *Add zone Scope* after right clicking the zone.
3. A new dialog appears where you can enter the name of the new zone zone.
4. Click the *Add* button to add the new zone scope.

The newly added zone scope is now shown in the zone list. The name of each zone scope is shown in a separate column.

Edit DNS Server Scopes

This allows the user to add or remove server scopes as well as specifying options for each scope.

1. Select the *Edit DNS Server Scopes* in the submenu of the *Edit DNS Server policies*.
2. Click the *Add* button to add a new server scope. A new dialog is displayed that allows the user to specify a name of the new server scope.
3. Click the *OK* button to add the new server scope.
4. For an existing server scope, select the corresponding server scope and then click the *Remove* button to remove the server scope.
5. To edit the options for a server scope, highlight the corresponding server scope and click the *Options* button. A new dialog window is displayed that allows the user to specify forwarders and select if recursion should be allowed. To disable the use of forwarders for the server scope leave the forwarders list empty.

Note: The forwarders list for the default server scope can still be edited in the Server Options

---

Set Response Rate Limiting

The Response Rate Limiting feature of the Microsoft 2016 DNS server can be used to control the rate in which the server responds to similar requests it will send to clients on the same subnet.

Configuring rate limiting

1. Select the 'Set Response Rate Limiting' in the submenu of the 'Edit DNS Server policies'
2. To enable response rate limiting, make sure the checkbox in 'Enable reponse rate limiting is checked.

For an overview of the configuration and the related fields, see below.

Enable Response Rate Limiting
To enable the Response Rate Limiting

Log only
RRL calculations are performed, but potential actions are logged as if RRL is enabled.

Responses / second
Maximum number of times the servers sends a client the same response within a one second interval.

Errors / seconds
Maximum number of times the servers sends an error response to a client within a one second interval.

Detection window
Specifies the period (in seconds) over which rates are measured and averaged for RRL.

IPv4 prefix length
Specifies the IPv4 prefix length, which indicates the size of the subnet in which the incoming queries are grouped.

IPv6 prefix length
Specifies the IPv6 prefix length, which indicates the size of the IPv6 subnet in which the incoming queries are grouped

Leak rate
Specifies the rate at which the server responds to dropped queries

Truncate rate
Specifies the rate at which the server responds with truncated responses

Max responses / window
Specifies the maximum number of responses that the server sends to a subnet-domain address in a RRL time window.

Exception list
Allows for creating policies that control RRL exceptions.

Adding an exception

In the Response Rate Limiting window, click on the *Add* button.

DNS Policies

To add a DNS policy:

1. Select the type of DNS policy in the submenu of the *Edit DNS Server policies*.
2. Click the *Add* button to add the new policy
3. A new dialog window is displayed. It is a generic window for adding a DNS policy. Refer to *Adding DNS policies* for more details.

Adding DNS policies

1. Each DNS policy must have a name that conforms to the rules of filenames. The name should be chosen to be unique for the zone or among DNS policies on the server level.

   Note: In case the name of the DNS policy does conflict with a DNS policy of a different type it is automatically renamed.

2. A DNS policy can be created enabled or disabled. Policies that are disabled are ignored by the server except for statistics and logging.
3. Each query that matches the policy can result in three actions:

   Allow:
   The query is processed and answered from the server or zone scope referred to.

   Deny:
   The DNS server refuses the query.

   Ignore:
   The DNS server drops the query without informing the client.

   Note: Server level policies other than recursion policies can only have "Deny" and "Ignore" as the action. Recursion policies and all zone level policies can have "Allow", "Deny" and "Ignore" as the action. For the "Allow" action one or more DNS scope must be selected, for a recursion policy these must be sever scopes and for any policy on a DNS zone these must be DNS scopes created on the zone.

4. If the action is 'Allow' select the 'Edit' button. This opens a dialog where you can select the target DNS scopes used for matched queries and the weight for load balancing.
5. Condition decides the condition for matching the Criteria list. Selecting 'And' indicates that all of the criteria should match for the policy to apply and 'Or' indicates that one or more of the criteria is sufficient for the policy to apply.
6. Criteria is a list of rules that the incoming DNS query is compared to. If the query matches the rules the server takes action in accordance. For more details refer to Add DNS policy criteria section.

Adding DNS policy target scope

When the action for a DNS Policy is 'Allow' one or more target DNS scopes must be chosen. Each DNS scope has a name and a weight for load balancing.

1. To add an DNS scope to the list press *Add* button.
2. In the Add Target Scope dialog you can select a scope which you want to be used to answer queries that match the DNS policy criteria list. DNS scopes for the DNS server or the zone will be listed, to create a new DNS scope, refer to Add server scope and Add zone scope, respectively.

   Target scope:
   The DNS scope used to answer the query.

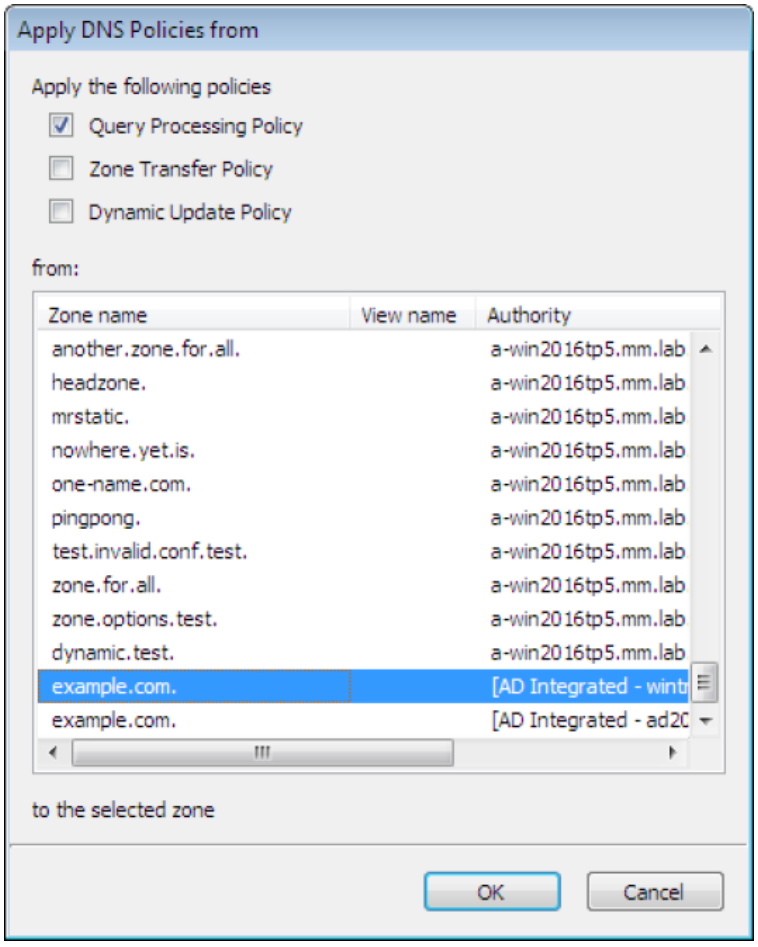
   Note: The DNS server will always have default scope, the name of the default scope is '.', DNS zones also have a default scope with the same name as the zone. In some cases the empty string can be used to referred to the default scope.

Weight:
Is an integer value used for load balancing.

Note: DNS policies can be used to for DNS based load balancing. For zones this can be achieved by adding the DNS records that you want to load balance (typically A/AAAA records) to different DNS scopes and then creating a Query Processing policy that will match the incoming queries and has 'Allowed' as the action, then add the DNS scopes as the target scopes for the DNS policy.

The queries will be answered from the the target scopes in a round-robin fashion based on the weight. If the target scopes are 'example.com' with weight 4 and 'offload' with weight '2', then the first 4 queries that match this policy will be answered from the 'example.com' scope and the next 2 from the 'offload' scope. Similar load balancing can also be achieved with other types of DNS policies.

Adding DNS policy criteria



Each DNS policy has a list of criteria that with the policy condition define how the DNS policy is matched. Depending on the policy type different criteria are allowed.

The DNS policy criteria and their descriptions are:

Type	Dsecription
Client Subnet	A list of subnet names as they are defined on the server. See Define client subnets for details.
Transport Protocol	A list of transport protocols used by the incoming query. The possible transport protocols are UDP and TCP.
Network Protocol	A list of network protocol used by the query. The possible network protocols are IPv4 and IPv6.
Server interface	A list of the IP address that the DNS server is listening on.
Domain Name	A list of domain names with strict wildcards allowed. For example '*.example.com'
Query Type	A list of DNS record types. For example A, NS, SRV, CNAME
Time of Day	A list of time periods in a 24h format. For example 18:00-23:15. The time of day is rounded to the next 15 minutes by MS-DNS. Maybe we should put this in a note and absolutely avoid examples that will be rounded.

Operator:
Supported values are 'is' or 'is not', where is not negates ALL the values supplied in the 'Values' input box.

Values:
The list of values used to match the DNS policy criteria with each item in the list on a newline.

Note: Two criteria of the same type are allowed only if they have a different operator but you can work around this limitation by using a list of values for each operator. If you want the criteria to match on two domain names you can select the type as 'Domain Name', the operator 'is' and enter the two domain name on different lines in the 'Values' field.

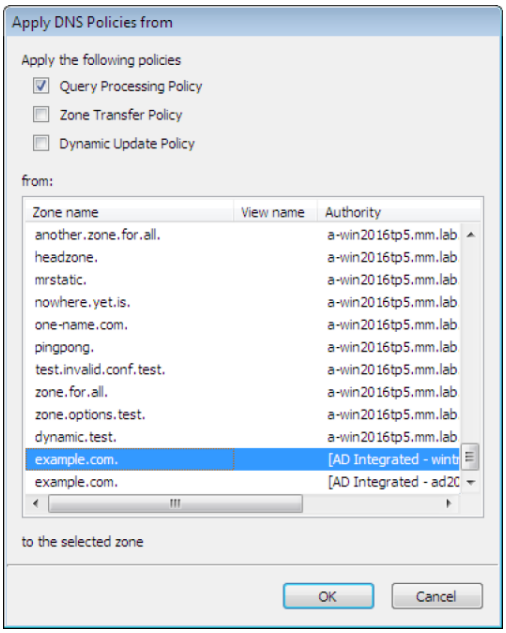
Apply DNS Policy from

It is possible to copy DNS policies between DNS servers and DNS zones. One or more type of DNS policy list can be copied at a time to one or more DNS server or DNS zone. DNS policies can not be copied if they refer to any Client Subnet Lists, DNS scopes or server interfaces that do not exist the targets of the copy operation. The copy operation results in the DNS policy lists for the chosen types of DNS policy to be overwritten with the copied DNS policy lists.

Note: DNS policies will be renamed if necessary when created or copied. You can avoid this by choosing unique names.

---

1. Right click on a DNS Server or DNS zone.
2. Select *Apply DNS Policy From…* ` in the *Edit DNS Policy* submenu.



3. Select the DNS policy type to copy.
4. Select the DNS server or DNS zone to copy DNS policies from

DHCP

DHCP servers - Management Console (obsolete)

Overview

This section shows you how to perform specific actions in Micetro associated with maintaining your DHCP servers, such as adding and deleting servers and setting DHCP server options. In order to use the DHCP functionality of Micetro you need to have a valid DHCP license key.

Note: The functions for this menu option are listed alphabetically after the New DHCP Server section.

This page describes the process for adding new DHCP servers, and generic DHCP management information. For detailed information about the different DHCP platforms, refer to:

- *Microsoft DHCP*
- *ISC Kea DHCP*
- *ISC DHCP*
- *Cisco DHCP*

Inherited Access (Management Console)

You can manage access to scopes just as you can for other object types in Micetro, but there is one important distinction: you can set *Inherited Access* for scopes. When you open the *Access* dialog box for a scope, the dialog box has an extra section for inherited access.

Checking the *Inherit Access* checkbox will have the selected scope inherit all access bits from its parent range. This means that whenever the access privileges for the parent range are changed, they will be applied to the scope as well.

Clicking the *Apply access inheritance in child ranges* button will enable access inheritance for all descendants of the scope. This means that whenever the access privileges in the scope are changed, the changes will be applied of all descendants of the scope.

Regarding other access settings, refer to *Access Management*.

Remove

Note: To remove a DHCP server in the Management Console, see console-delete-dhcp-server.

Options

Note: To manage DHCP server option in the Management Console, see console-dhcp-options.

Properties

Refer to the applicable section based upon the server type: console-ms-dhcp-properties, console-isc-dhcp-properties, console-kea-dhcp-poperties or console-cisco-dhcp-properties.

Advanced ISC Kea Server Properties

Note: To edit advanced DHCP configuration in the Management Console, see console-dhcp-advanced-options.

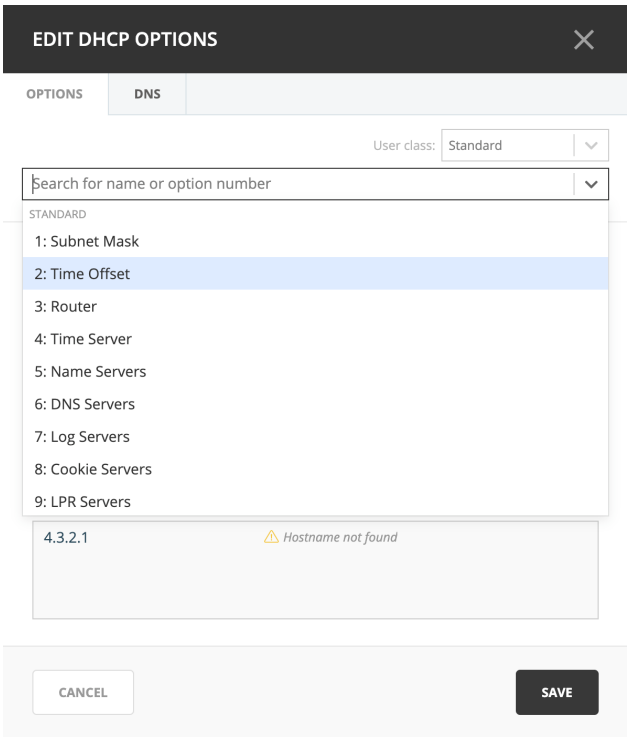
Reload Scope List (Management Console)

Reloads the list of scopes to view additions and/or deletions made by another user.

Microsoft DHCP

Defining Options on MS DHCP Servers

1. In *Admin* → *Server Management* select the applicable DHCP Server and select *Edit DHCP options* from the ellipsis menu or use *Actions* → *Edit DHCP options*. The *Edit DHCP options* box displays. The dialog box shows all options defined on the DHCP server.
2. Use the drop-down menu to select the option you want to define.



3. To add an option, select the option from the list. The option filed is added to the dialog box.
4. To delete an option, hover over its field and click the trash button next to it.
5. Click *Save* to save the updated options.

MS DHCP options (DNS tab)

Enable DNS dynamic updates according to the settings below.
Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.

Dynamically update DNS A and PTR records.
Specifies that the DHCP server update forward and reverse lookups are based on the type of request made by the client during the lease process.

Always dynamically update DNS A and PTR records.
Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.

Discard A and PTR records when lease is deleted.
Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.

Dynamically update DNS A and PTR records for DHCP clients.
Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

Disable dynamic updates for DNS PTR records
Turns off dynamic updates for PTR records.

Reconcile Scopes

See console-dhcp-windows-reconcile.

ISC Kea DHCP

Danger: Starting with Micetro 10.0, older versions of the Kea DHCP server are no longer supported. See system-requirements for a list of supported versions. You need to remove your existing (older) Kea DHCP servers from the system, and update them to a supported version of Kea before updating to Micetro 10.0 from an older version of the Men&Mice Suite. Not doing so could result in lost access to and data from the older Kea servers in Micetro.

Kea Control Agent

The Kea Control Agent is a daemon that exposes a RESTful control interface for managing Kea servers. The Control Agent daemon can receive control commands over HTTP and either forward these commands to the respective Kea servers or handle them commands on its own.

Note: The default port for the Kea Control Agent is `8000`.

Because of the Kea Control Agent, Kea DHCP servers can be added to Micetro without a DHCP Server Controller running on every machine that runs Kea. A *single* DHCP Server Controller, installed on a machine that can access the instances that run Kea services, is sufficient and will communicate with all Kea servers on Micetro's behalf.

Adding Kea to Micetro

Because Micetro uses the Kea API to communicate with the DHCP server(s), it requires (in addition to the DHCP Server Controller) the Kea hook library `libdhcp_lease_cmds.so`.

Note: On certain distributions (like RHEL) check that the kea-hooks package is also installed.

Configuring the Kea hook library

After installing the Kea hook library, open `kea-dhcp4.conf` and locate the `hooks-libraries` array. Add the hook to `libdhcp_lease_cmds.so`:

```
"hooks-libraries":[
    {
      "library" : "/lib64/kea/hooks/libdhcp_lease_cmds.so",
      "parameters" : {}
    }
]
```

The location of the library depends on your distribution, use `whereis libdhcp_lease_cmds.so` to find it.

After adding the library, restart Kea and the Kea Control Agent.

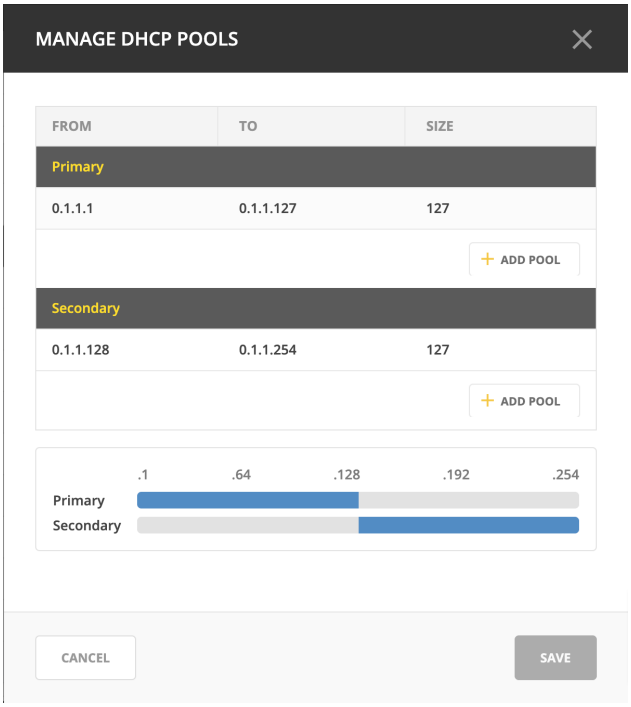
Kea high availability

Kea DHCP servers need to be configured for high availability **before** the primary server is added to Micetro. If the high availability is set up properly, once added to the system Micetro will recognize the failover nodes and the method (load balancing, hot standby, etc.) and configure the server objects accordingly.

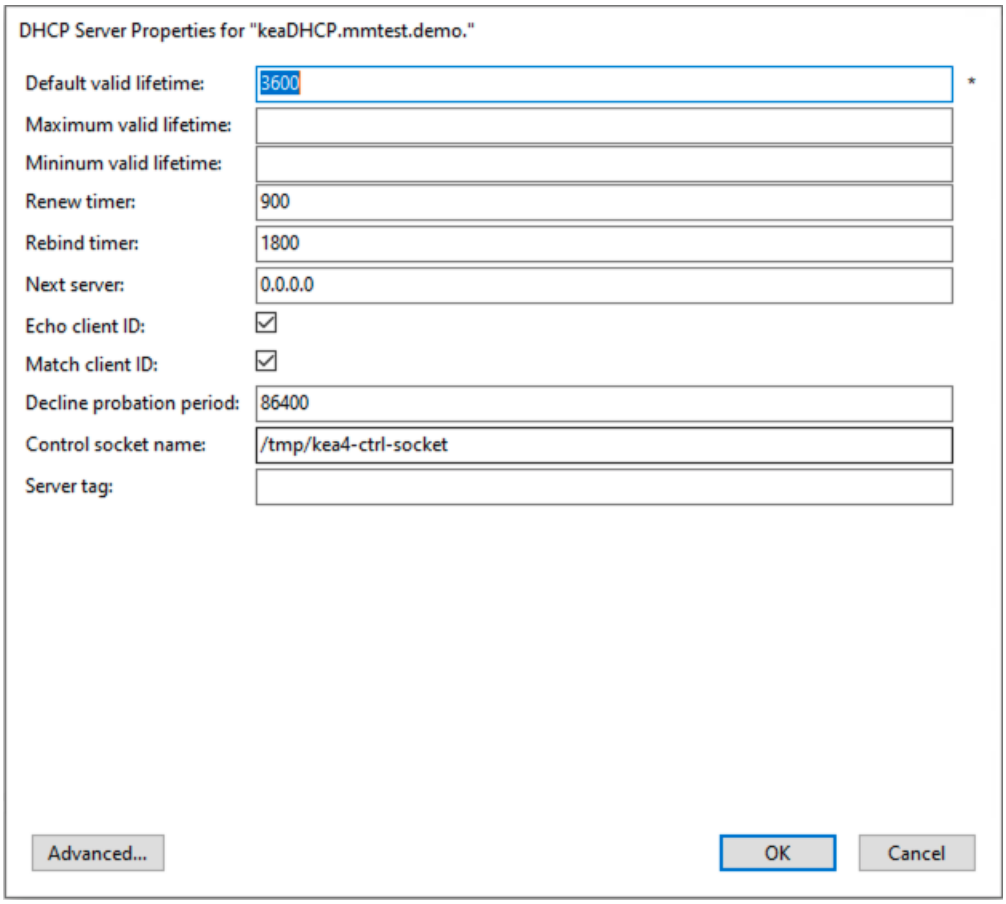
For more information, see dhcp-kea-ha.

Split scopes in load balancing mode

When creating scopes on Kea servers configured in load balancing mode for high availability, Micetro will split the available pool evenly between primary and secondary servers.



Kea DHCP Server Properties



Default/Maximum/Minimum Valid Lifetime
Specifies the time after which a lease will expire if not renewed.

Renew Timer
Specifies the time when a client will begin a renewal procedure.

Rebind Timer
Specifies the time when a client will begin a rebind procedure.

Match Client ID
Specifies if the server should ignore the client identifier during lease lookups and allocations for a particular subnet.

Echo Client ID
Specifies if the server should send back client-id options when responding to clients.

Decline Probation Period
Specifies a probation time that will be set on addresses that are in use by some unknown entity.

Next Server
Specifies the server address to use when clients want to obtain configuration from a TFTP server.

Control Socket

Name
The path to the UNIX socket. Cannot be empty.

Server tag
The name used for this server in a High Availability setup.

Handling external changes with Kea

Warning: You should always edit the Kea DHCP server's configuration file through Micetro to ensure that the synchronization between Micetro and the Kea DHCP server is instant and all changes will immediately updated in the database and reflected in the user interface.

Note: All changes made to the configuration file through Micetro will automatically and instantly be propagated to the secondary/backup servers in a dhcp-kea-ha setup.

Micetro uses the in-memory configuration of the Kea server. If external changes must be made to a Kea DHCP server's configuration file, the changes to the configuration file aren't processed by the server until forced to parse the file to its *in-memory* structure, so Micetro can be made aware of these changes.

To make the Kea DHCP server process changes to its configuration file a call has to be made to either the *Kea Control Agent* or the socket that Kea uses.

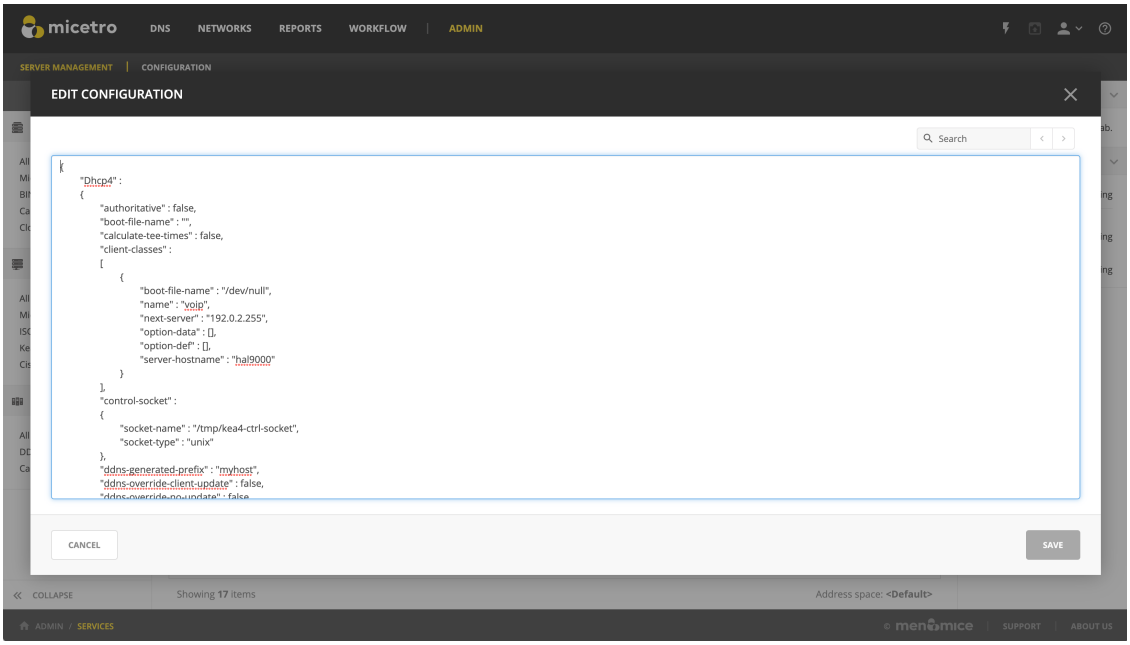
An example of the call to the control-agent:

```
curl -X POST -H "Content-Type: application/json" -d '{ "command": "config-reload",
↪"service": [ "dhcp4" ] }' localhost:8000
```

If successful, the result looks like this:

```
[ { "result": 0, "text": "Configuration successful." } ]
```

After the changes to the configuration file have been accepted and parsed into the Kea DHCP servers memory structure, users can display them in Micetro through the *Edit Configuration* action for the server.



Resolving conflicts

Micetro synchronizes all data between the Kea DHCP servers and its database regularly. Setting the `DHCPSyncInterval` variable in Central's `preferences.cfg` overwrites the default value of 15 minutes.

Note: The values set for `DHCPSyncInterval` are in seconds.

Synchronization occurs based on the configuration to update the database and the user interface, but to prevent overwriting external changes before synchronization is complete, Micetro will check for conflicts with the Kea server's in-memory configuration before writing the changes to the server.

For example, if a scope with subnet 1.3.3.0/29 is manually added to the Kea DHCP servers configuration file, and `config-reload` is successfully called, the Kea server will have parsed the change and added the scope to its in-memory data structure. Synchronization with Micetro may not have been executed yet, and the externally added scope is not yet visible in the user interface. However, if another user would try to add the same or otherwise conflicting scope through Micetro, they will receive a message stating "*A scope with address "1.3.3.0" already exists on the server*" as the configuration file is validated against the Kea DHCP servers in-memory config before each change is applied.

External changes and Kea high availability

See dhcp-kea-ha-external-changes.

ISC DHCP

Note: To manage ISC DHCP servers in the Management console, see console-dhcp-isc.

Defining Options on ISC DHCP Servers

1. In *Admin* → *Server Management* select the applicable DHCP Server and select *Edit DHCP options* from the ellpisis menu or use *Actions* → *Edit DHCP options*. The *Edit DHCP Options* box displays. The dialog box shows all custom options defined on the DHCP server. The available ISC DHCP options can be selected from the dropdown menu.
2. To add an option, select it from the option list. The option field is added to the dialog.
3. To delete an option, hover over its field and click the trash button next to it.
4. Click *Save* to save the changed option definitions.

ISC Server Properties

Authoritative
Specifies whether the server is authoritative to determine if a DHCP request from a client is valid

DDNS Domain Name
Specifies the DNS domain name to use to store the A record for a DHCP client.

DDNS Reverse Domain Name
Specifies the DNS reverse domain name to use to store the PTR record for a DHCP client.

DDNS Update Style
Specifies how the DHCP server does DNS updates. The available styles are:

None
Dynamic DNS updates are not performed

Ad-hoc

> **Warning:** This update scheme is deprecated

Interim
This is the recommended scheme for dynamic DNS updates

DDNS Updates
Specifies whether to perform DNS updates. This setting has no effect unless DNS updates are enabled globally with the DDNS Update Style setting.

DDNS TTL
Specifies (in seconds) the TTL value to use when performing a DNS update.

Default Lease Time
Specifies (in seconds) the default lease time to use for DHCP leases.

Log Facility
Specifies which syslog facility to use when logging DHCP server messages. All possible facilities are listed; however, not all of these facilities are available on all system.

Max/Min Lease Time
Specifies (in seconds) the maximum/minimum lease time to use for DHCP leases.

Get Lease Hostnames
Specifies whether the DHCP server should perform a reverse DNS lookup for each address assigned to a client and send the result to the client in the hostname option.

One Lease per Client
Specifies whether the DHCP server should free any existing leases held by a client when the client requests a new lease.

Ping Check
Specifies whether the DHCP server should send an ICMP echo message to probe an IP Address before offering it to a DHCP client.

Ping Timeout
Specifies for how many seconds the DHCP server should wait for an ICMP echo response when Ping Check is active.

Filename
Specifies the name of the initial boot file to be used by a client.

Server Name
Specifies the name of the server from which the client should load its boot file.

Next Server
Specifies the host address of the server from which the initial boot file (that is specified by Filename) is to be loaded.

Restart

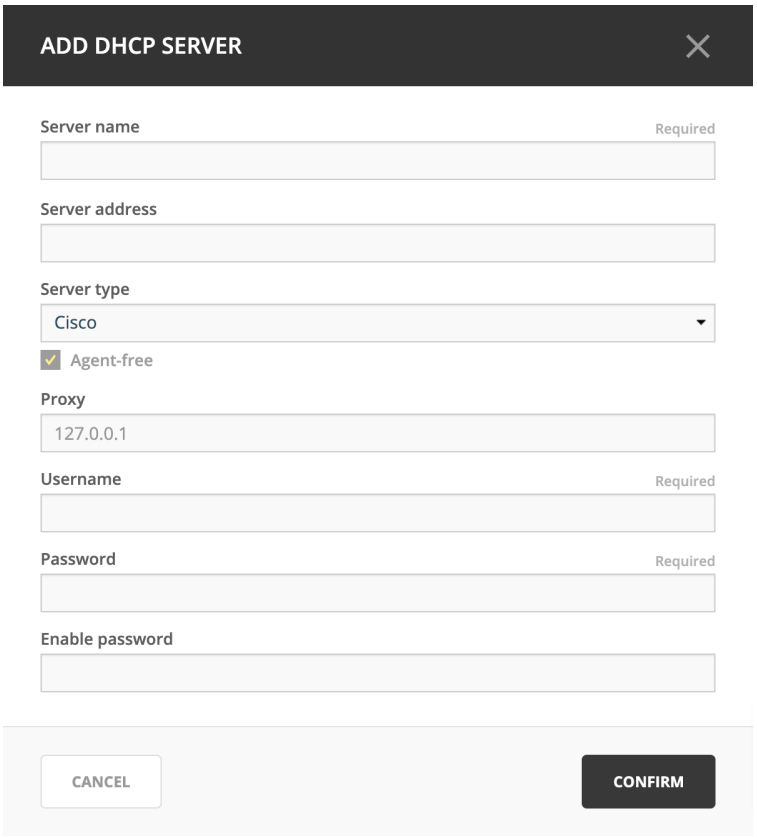
See console-dhcp-isc-restart.

Cisco DHCP

Note: For managing Cisco DHCP servers in the Management Console, see console-dhcp-cisco.

Adding a Cisco DHCP server

When adding a Cisco DHCP server, the following dialog box displays:



Type the **User name** and **Password** that should be used to access the server. This is the user name and password that is used when normally accessing the Cisco device from the command line prompt. If the server requires a separate password to enter privilege level 15, enter the required password in the **Enable Password** field.

DHCP Scopes - Management Console (obsolete)

Overview

This section shows you how to perform specific actions in Micetro associated with maintaining your DHCP scopes, such as creating and modifying reservations, setting scope options and working with split scopes.

Viewing Scopes

Scopes on a Specific DHCP Server

It is easy to view the DHCP scopes that reside on individual DHCP Servers that are being managed by the Management Console. Simply click on the plus + sign next to the DHCP Servers object in the *Object Section*, and select the DHCP server containing the scopes you want to view.

Selected Scope Menus

When working with scopes, a right-click, shortcut menu is offered. The menu options change, based upon the type of DHCP server the scope is hosted on: MS, ISC or Cisco.

MS Shortcut Menu

Open
: Opens the currently selected IP Address.

Delete
: This option is enabled when there is an existing DNS entry for the IP Address or there is custom property data for the IP Address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.

History
: Shows any changes made to the selected item. These changes are displayed in a new window.

Ping
: Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.

Claim
: Allows you to "claim" an address to prevent accidental assignment but without creating a DNS entry for it.

Create Address Pool
: Creates an address pool for the selected scope. Complete the From and To fields in the DHCP Address Pool dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.

Edit Address Pool
: To edit an existing pool, click anywhere in the applicable address pool, right-click, select *Edit Address Pool* and, in the dialog box, make the desired edits.

Options for Pool
: *ISC DHCP only.* To set options for a pool, click anywhere in the applicable address pool, right-click, select Options for Pool and, in the Options dialog box, make the desired changes.

Permits for Pool

ISC DHCP only. Allows you to specify permits for an address pool. To set access pool permits, do the following:

1. Click anywhere in the applicable address pool, right-click and select *Permits for Pool*. The *Pool Permits* dialog box displays.
2. Click *Add* to create a new access pool permit.
3. Enter the permit settings and click *OK* to save the changes and close the dialog box.
4. Use the *Edit* and *Delete* buttons to modify or delete existing permits.

Delete Address Pool(s)

To delete an existing pool, click anywhere in the applicable assigned range, right-click and select *Delete Address Pool(s)*.

Create Excluded Range

MS DHCP only. Allows you to exclude a single IP Address or an entire range of addresses from being used. You can only exclude addresses that are already part of an address pool. To create an excluded range, specify the From and To IP Addresses. All the addresses between and including the ones entered will be excluded.

Edit Excluded Range

MS DHCP only. To edit an existing range, click anywhere in the applicable excluded range, right-click, select *Edit Excluded Range* and, in the dialog box, make the desired edits.

Delete Excluded Range(s)

MS DHCP only. To delete an existing range, click anywhere in the applicable excluded range, right-click and select *Delete Excluded Range(s)*. The entire excluded range is removed.

Create Reservation

Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP Addresses. To create a reservation, do the following:

1. Locate the IP Address you want to reserve, right-click on it, and select *Create Reservation* from the pop-up menu. The *DHCP Reservation* dialog box displays.

   Name
   Assign a name to identify the reserved address.

   MAC Address
   Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

   Description
   (Optional) User defined description.

   Supported Types
   Select whether this reservation should support DHCP, BOOTP (i.e., Bootstrap Protocol), or Both (default).

2. To specify whether the DHCP server automatically updates record in the DNS server or not, click the *DNS* tab.
3. Enable DNS dynamic updates according to the settings below. Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.

   Dynamically update DNS A and PTR records
   Specifies that the DHCP server update forward and reverse lookups be based on the type of request made by the client during the lease process.

Always dynamically update DNS A and PTR records
Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.

Discard A and PTR records when lease is deleted
Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.

Dynamically update DNS A and PTR records for DHCP clients that do not request updates
Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

4. Click *OK*. The address is now listed as reserved in the DHCP Scope dialog box.

Edit a Reservation
To edit an existing reservation, right-click on the reservation you want to change and select *Edit a Reservation*. Then, make the necessary edits.

Options for a Reservation
To select options for a reservation, right-click on the reservation and select *Options for a Reservation*. The DHCP Reservations dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Reservation(s)
To delete an existing reservation, right-click on the reservation you want to remove and select *Delete Reservation(s)*.

ISC Shortcut Menu

Open
Opens the currently selected IP Address.

Delete
This option is enabled when there is an existing DNS entry for the IP Address or there is custom property data for the IP Address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.

History
Shows any changes made to the selected item. These changes are displayed in a new window.

Ping
Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.

Claim
Allows you to "claim" an address to prevent accidental assignment but without creating a DNS entry for it.

Create Address Pool
Creates an address pool for the selected scope. Complete the From and To fields in the DHCP Address Pool dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.

Edit Address Pool
To edit an existing pool, click anywhere in the applicable assigned range, right-click, select *Edit Address Pool* and, in the dialog box, make the desired edits.

Options for Pool
When selected, the *DHCP Options* dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Address Pool(s)
To delete an existing pool, click anywhere in the applicable assigned range, right-click and select *Delete Address Pool(s)*.

Create Reservation
Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP Addresses. To create an address, do the following:

1. Locate the IP Address you want to reserve, right-click on it, and select *Create Reservation*. The *DHCP Reservation* dialog box displays.

   Name
   Assign a name to identify the reserved address.

   MAC Address
   Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

   DDNS hostname
   Specifies the DNS domain name to use to store the A record for a DHCP client.

   IP Address
   Enter an IP Address for the reservation. You can add additional IP Addresses by clicking the plus sign and enter an IP Address in the field that displays.

2. Click *OK*.

Edit a Reservation
To edit an existing reservation, right-click on the reservation you want to change and select *Edit a Reservation*. Then, make the necessary edits.

Options for a Reservation
To select options for a reservation, right-click on the reservation and select *Options for a Reservation*. The *DHCP Reservations Options* dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Reservation(s)
To delete an existing reservation, right-click on the reservation you want to remove and select *Delete Reservation(s)*.

ISC Kea Shortcut Menu

Open
Opens the currently selected IP Address.

Delete
This option is enabled when there is an existing DNS entry for the IP Address or there is custom property data for the IP Address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.

History
Shows any changes made to the selected item. These changes are displayed in a new window.

Ping
Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.

Claim
Allows you to "claim" an address to prevent accidental assignment but without creating a DNS entry for it.

Create Address Pool
Creates an address pool for the selected scope. Complete the From and To fields in the DHCP Address Pool dialog box, typing the range of addresses to be included in the pool. Both of these fields default to the first available address in the range. If this is a split scope (a scope that exists on more than one server) and the address pool overlaps a warning message displays.

Edit Address Pool
To edit an existing pool, click anywhere in the applicable assigned range, right-click, select *Edit Address Pool* and, in the dialog box, make the desired edits.

Options for Pool
When selected, the DHCP Options dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Address Pool(s)
To delete an existing pool, click anywhere in the applicable assigned range, right-click and select *Delete Address Pool(s)*.

Create Reservation
Reservations can be created in unassigned address space, address pools, and excluded addresses. It is possible to set options for reserved IP Addresses. To create an address, do the following:

1. Locate the IP Address you want to reserve, right-click on it, and select *Create Reservation*. The *DHCP Reservation* dialog box displays.

   MAC Address
   Enter the MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

   DDNS hostname
   Specifies the DNS domain name to use to store the A record for a DHCP client.

2. Click *OK*.

Edit a Reservation
To edit an existing reservation, right-click on the reservation you want to change and select *Edit a Reservation*. Then, make the necessary edits.

Options for a Reservation
To select options for a reservation, right-click on the reservation and select *Options for a Reservation*. The *DHCP Reservations Options* dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Reservation(s)
To delete an existing reservation, right-click on the reservation you want to remove and select *Delete Reservation(s)*.

Cisco Shortcut Menu

Open
Opens the currently selected IP Address.

Delete
This option is enabled when there is an existing DNS entry for the IP Address or there is custom property data for the IP Address. When Delete is selected, the additional data is removed; however, the IP Address itself remains intact.

History
Shows any changes made to the selected item. These changes are displayed in a new window.

Ping
Allows you to ping the selected server. If the ping is successful, a green dot displays; if unsuccessful, a red dot displays.

Claim
Allows you to "claim" an address to prevent accidental assignment but without creating a DNS entry for it.

Create Excluded Range
Allows you to exclude a single IP Address or an entire range of addresses from being used. You can only exclude addresses that are already part of an address pool. To create an excluded range, specify the From and To IP Addresses. All the addresses between and including the ones entered will be excluded.

Edit Excluded Range
To edit an existing range, click anywhere in the applicable excluded range, right-click, select *Edit Excluded Range* and, in the dialog box, make the desired edits.

Delete Excluded Range(s)
To delete an existing range, click anywhere in the applicable excluded range, right-click and select *Delete Excluded Range(s)*. The entire excluded range is removed.

Create Reservation
Reservations can be created in address pools, and excluded addresses. It is possible to set options for reserved IP Addresses. To create an address, do the following:

1. Locate the IP Address you want to reserve, right-click on it, and select *Create Reservation*. The *DHCP Reservation* dialog box displays.

   Name
   Assign a name to identify the reserved address.

   Reservation Method
   Choose the reservation method for this reservation. You can choose either Client Identifier or Hardware Address.

   Client Identifier / MAC Address
   Depending on your choice for Reservation Method, enter the Client Identifier or MAC Address (i.e., Media Access Control Address) of the network node for which this address is being reserved.

   DDNS hostname
   Specifies the DNS domain name to use to store the A record for a DHCP client.

2. Click *OK*.

Edit a Reservation
To edit an existing reservation, right-click on the reservation you want to change and select *Edit a Reservation*. Then, make the necessary edits.

Options for a Reservation
To select options for a reservation, right-click on the reservation and select *Options for a Reservation*. The *DHCP Reservations* dialog box displays. Refer to dhcp-options for details on this dialog box.

Delete Reservation(s)
To delete an existing reservation, right-click on the reservation you want to remove and select *Delete Reservation(s)*.

Scope Creation Wizard

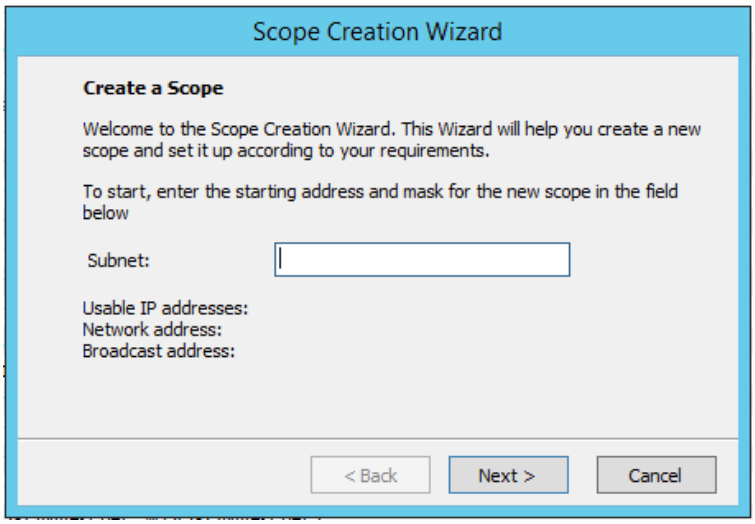
This section describes how to create and edit DHCP scopes with the new *DHCP Scope Creation Wizard*.

Whenever you create a new scope, Micetro automatically checks whether the new scope conflicts with an existing scope or an IPAM range.

The Wizard has additional steps, or skips over some steps, depending on the type of DHCP server the scope is being created on, and whether the *AD Sites and Subnets* integration has been enabled.

To create a new scope on the MS DHCP server, do the following:

1. In the object list, right-click on *DHCP Scopes* and, from the shortcut menu, select *New Scope*. Alternatively, right click on an existing IP address range, and select *Convert To DHCP Scope*.
2. The *Scope Creation Wizard* dialog appears.



Subnet
: Enter the subnet in CIDR notation, e.g. 5.5.5.0/24, and click *Next*.

Server and scope type
: Select the type, either Single scope, Split scope, or Failover scope (only on Windows 2012 and newer DHCP servers) and the DHCP server to create the scope on.

Note: When you change the type to Failover scope, only Windows 2012 and newer servers are shown.

---

3. Select second server (Split scope) or Failover Relationship (Failover Scope).

Note: This step is skipped if Single scope was selected, or if Failover Scope is selected and there is only one Failover Relationship on the selected DHCP server.

---

4. Address pool. Enter the address range for the address pool. By default, it is set to cover the entire scope.
5. Range properties. Enter the custom properties for the IP address range.
6. Enabled or Disabled.
7. Active Directory Site selection. If you have enabled *AD Sites and Subnets*, the Wizard will ask you which AD site the new DHCP Scope should be associated to.

8. Scope properties.

Note: On Microsoft DHCP servers, if the scope is a part of a MS DHCP Superscope, enter the name of the Superscope here, or leave empty.

Note: On Cisco DHCP Servers the only configurable scope property is "Import All". When checked, it imports Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP server database. Refer to the Cisco IOS IP Addressing Command Reference document for more information.

---

9. DNS Update Settings (only Microsoft DHCP servers)
10. Save Comment
11. Summary: The changes the Wizard will perform are summarized here and applied once the user clicks "Finish".

Warning: Once the scope has been created, you must set access privileges for the scope if you want to allow users to make any changes to it, assuming the initial access for Ranges/Scopes has not been set appropriately.

Access

For complete details on this function, refer to global-access.

Delete

Use the following procedure to remove a scope definition from the Management Console.

1. Locate the DHCP Scope you want to remove and right-click on it.
2. From the pop-up menu, select *Delete*. A dialog prompts you to confirm your decision to delete this scope.
3. Click *OK* to delete the scope, or *Cancel* to leave it.

Disable/Enable

If you are no longer using a particular scope, but do not want to delete it completely because you may need it in the future, you can disable the scope instead. A scope that is disabled will be ignored by the DHCP server until it is re-enabled. Use the following procedure to disable/enable a scope.

1. Locate the DHCP Scope you want to disable/enable and right-click on it. Scopes that are currently disabled have faded icons next to them.
2. From the pop-up menu, select *Disable* to disable this scope, or if the scope is already disabled, select *Enable* to reactivate it.

Note: New scopes are always disabled by default so you can configure the properties before the DHCP server begins using it.

Scope Migration Wizard

The *Scope Migration Wizard* allows users to migrate one or more scopes from one server to another, including all data in the scope.

To migrate a scope, do the following:

1. In the Manager window, select one or more scopes.
2. Right-click and, from the shortcut menu, select *Migrate Scope*. The *Migrate Scope(s) Wizard* dialog box displays.

Server
Click the drop-down list and select onto which you want to migrate this scope(s).

4. Click *Next*. The *Migration Options* dialog box displays.
5. For each of the resulting screens, make a selection/entry and move through the wizard.

Duplication Wizard

To duplicate a DHCP scope you should use the Duplicate Scope wizard. The duplicate will initially have the exact same properties as the original, but you will have the option to assign the duplicate to a different DHCP server and modify the duplicated values.

Within this wizard, you can do the following:

- Create a new scope
- Create a split scope interface

To launch the wizard, do the following:

1. In the *Object Section*, click on *DHCP Scopes*.
2. In the *Object List*, right-click on the DHCP Scope you want to duplicate and, from the shortcut menu, select *Duplicate*. The *Duplicate scope wizard* launches.
3. For each of the resulting screens, make a selection/entry and move through the wizard.

Folders

Refer to *Object folders* for details on this function.

Reconcile Scope

Note: Applies to MS DHCP Servers only.

Use this function to fix inconsistencies between information in the registry and the DHCP database.

1. In the *Object List*, select *DHCP Scopes* and then select a scope.
2. Right-click the scope and select *Reconcile Scopes*.
3. Choose whether you want to verify only or fix any inconsistencies and click *OK* to complete the action.

For more information see the Microsoft documentation.

Converting a Scope to a Range

Use this function to convert an existing scope to an IP Address range, while keeping all the settings intact.

1. In the *Object List*, select *DHCP Scopes* and then select a scope.
2. From the menu bar, select *Range* → *Convert to IP Address Range*.
3. When the Men&Mice Management Console confirmation dialog box appears, click *Yes* to convert the range.

Converting a Range to a Scope

Use this function to convert an existing IP Address range to a scope, while keeping all the settings intact.

1. In the *Object List*, select *IP Address Ranges* and then select a range.
2. From the menu bar, select *Range* → *Convert to DHCP Scope*, or right click and select *Convert to DHCP Scope*. The *Scope Creation Wizard* will appear, with the subnet field pre-populated for the selected range.
3. Clicking *Next* will continue with the *Scope Creation Wizard* as normal.

Scope Policies (Windows Server 2012 or newer)

If you are managing DHCP servers on Windows Server 2012 or newer, you can use Micetro to set scope policies for individual scopes.

Activate/Deactivate a Scope Policy

1. In the *Scope List*, right-click a scope that is stored on a Windows 2012 DHCP server.
2. From the shortcut menu, select *Manage Policies*. The *DHCP Scope Policy Management* dialog box displays.
3. The dialog box shows the current status of DHCP scope policies for the selected scope.
4. To activate DHCP scope polices, click the *Activate* button. If DHCP scope polices are active, the button text shows *Deactivate*. To deactivate the DHCP scope policies, click the *Deactivate* button.
5. Click *Close*.

Add a New Scope Policy

1. In the *Scope List*, right-click a scope that is stored on a Windows 2012 DHCP server and, from the shortcut menu, select *Manage Policies*. The *DHCP Scope Policy Management* dialog box displays.
2. Click the *Add* button. The *DHCP Policy* dialog box displays.
3. Enter a name and description for the DHCP policy in the corresponding fields.
4. Click the *Add* button in the *Conditions* section to add a new condition for the DHCP policy. The *DHCP Policy Condition* dialog box displays.
5. Specify the condition you want to use and click *OK* to save the condition and close the dialog box. Note that you can enter multiple conditions for a DHCP policy by clicking the *Add* button in the *DHCP Policy* dialog box.
6. To edit or delete an existing DHCP Policy condition, select the condition from the list of DHCP Policy conditions, and click the corresponding button.

7. If there is more than one condition, you need to specify whether to use the OR or AND operator when evaluating the conditions. Select the corresponding radio button in the DHCP Policy dialog box.

Ranges

1. Click the *Add* button in the ranges section to specify an IP Address range that should be affected by the policy. The *Range specification* dialog box displays.
2. Enter the range using the from and to addresses separated by a hyphen (for example, 192.168.1.10-192.168.1.20).
3. Click the *Add* button to add the range and close the dialog box. NOTE: You can enter multiple ranges by using the *Add Range* dialog box for each range you want to add.
4. To edit or delete an existing range, select the range from the list of ranges, and click the corresponding button.
5. When you have added all conditions and ranges, click the *OK* button to save the DHCP policy.

DNS Dynamic Updates

Options specific to dynamic updates are in the field named **DNS Dynamic Updates**. It can be configured accordingly for the policy.

Lease duration

The lease duration can be specified per policy in those fields.

DHCP Options

To specify DHCP options for this policy, click the *Options* button. That will open a dialog which will allow the user to specify the options.

Note: If this is unconfigured, the options will be inherited from the scope or server.

Change an Existing Scope Policy

You can edit, delete or disable existing DHCP Scope Policies. You can also change the order of DHCP scope policies.

1. In the *Scope List*, right-click a scope that is stored on a Windows 2012 DHCP server and, from the shortcut menu, select *Manage Policies*. The *DHCP Scope Policy Management* dialog box displays.
2. Select the DHCP Policy you want to work with by clicking it in the list of DHCP Policies.

- To edit the policy, click the *Edit* button.
- To delete the policy, click the *Delete* button.
- To disable the policy, click the *Disable* button. If the policy is already disabled, the button text shows Enable. To enable the policy, click the button.
- To move the policy up or down in the list of DHCP Policies, click the *Move Up* or *Move Down* button.

3. When you have completed your changes, click the *Close* button.

Other Functions

At any time, you can modify the properties for a scope. Simply locate the item, right-click and from the shortcut menu select *Properties*. When a scope is opened, the system displays one tab for each server on which the scope is defined. For split scopes, the scope contents can be examined individually on each server.

In addition to the tabs displaying individual scope contents on each server, the DHCP scope dialog contains an *Overview* and *Statistics* tab, with a graphical overview of the scope contents, as well as statistics on pool utilization on all servers.

For each DHCP server containing the scope, there is a bar depicting the placement of reservations, pools, and exclude ranges in different colors.

- The top of the bar represents the IP Address at the start of the scope.
- The bottom of the bar represents the IP Address at the end of the scope.

This overview is useful in verifying that split scope configurations do not contain conflicts, such as overlapping pools or inconsistent reservations.

The table in the lower part of the window contains aggregate statistics for the scope, i.e., effective pool size, the number of pool clients, and the pool utilization, summed up over all servers containing the scope.

Deleting a Lease

To delete a lease in a DHCP scope, do the following:

1. Open the scope containing the lease you want to delete.
2. Right-click on the lease and, from the shortcut menu, select *Release Lease*.

IP Address Details

The IP Address details window contains all information pertaining to an IP Address in the application, including DNS records, DHCP reservations, and custom properties. To access the *IP Address details* window from the DHCP scope dialog you need to double click on an IP Address in the DHCP scope dialog, or right-click on an IP Address and select the Open menu item.

The IP Address details window is documented in *IP Address Inspector*. However, when the IP Address details window is opened from the DHCP scope dialog, information on any DHCP reservation associated with the IP Address displays as well. A reservation can be created by clicking the Create button on the DHCP Panel. You can also create and edit a reservation directly from the DHCP scope dialog by selecting the appropriate menu item when right-clicking on an IP Address. The IP Address dialog box is not available if only a DHCP license key has been entered. In this case, the reservation dialog box will be displayed when double clicking an entry in the DHCP scope.

Subranges of Scopes

It is possible to choose whether the contents of ranges that are created under scopes are displayed in a range view or a scope view. Use the Show DHCP data in subranges of scopes checkbox in the *System Settings* dialog box to choose the preferred display mode.

If the scope view is selected, a window similar to the scope window displays when you open a subrange of a scope. However, the only scope related action available in this window is reservation management. The access dialog box for these subranges will contain an additional access bit, Edit reservations.

If the range view is selected, the subranges are opened in the range view and no scope related actions are available.

Renaming a Scope

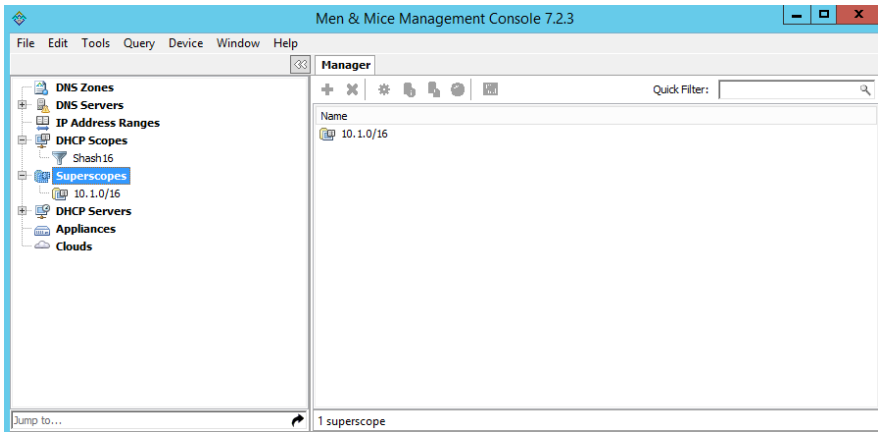
It is very simple to change the name and/or description of a scope in the Management Console.

1. Locate the DHCP Scope you want to rename.
2. Right-click and, from the shortcut menu, select *Properties*. The *DHCP Scope Properties* dialog box displays. NOTE: The dialog box may look different depending on the DHCP server type.
3. Enter the **Title** and **Description**.
4. Click *OK*. The newly renamed scope now displays in the Object List.

Superscopes

Note: Superscopes are only supported on MS DHCP servers on Windows server.

All MS Superscopes are listed in the object section under the heading *Superscopes*.



When you click on the Superscope, all scopes within that superscope display. In addition, a new column, Superscope, is shown in the scope list. It is possible to filter by this column.

To assign an existing scope to a superscope, do the following:

1. In the *Object list*, select a DHCP Scope for which you want to set a Superscope.
2. Right-click and, from the shortcut menu, select *Properties*. The scope dialog box displays.
3. Enter the name of the superscope in the **Superscope** field.
4. Click *OK*. The scope is placed in the superscope. If the superscope did not exist, the new superscope is created and now displays as a new item in the object list.

Moving IP Address Information

IP Address information can be moved to a new IP Address. When the IP Address information is moved, all information about the IP Address is retained, and the associated DNS records are updated. If a reservation is associated with the IP Address, the reservation information is moved with the IP Address if the destination address is in a DHCP scope that is hosted on a DHCP server of the same type. If the destination address is in a scope hosted on a different type of a DHCP server or the destination is in an IP Address range, the reservation information is discarded.

To move IP Address information, do the following:

1. Locate the IP scope containing the IP Address.
2. Double-click on it to display the scope contents.
3. Find the applicable IP Address.
4. Right-click and, from the shortcut menu, select *Move*.
5. In the *Move IP Address Information* dialog box, type the new IP Address.
6. Click *OK*. The IP Address information is moved to the new IP Address.

Host Discovery

With this feature, you can see when hosts were last seen on your network. There are two methods you can use for host discovery – using ping or querying routers for host information.

When host discovery is enabled, two columns are added to the range or scope view.

Last Seen
: This column identifies when a host was last seen on the network and which method was used to discover the host.

Last Known MAC Address
: This column shows the MAC address used by the host the last time it was seen on the network. This column is only populated if the host was seen using a router query.

Configuring Host Discovery Using Ping

1. Select one or more scopes.
2. Right-click and, from the shortcut menu, select Set *Discovery Schedule*. The *Schedule* dialog box displays.
3. Select the *Enable discovery schedule* option.

   Schedule ____ every ___ day(s)/week(s)/month(s).
   : Click the drop-down list and select the frequency (e.g., Daily, Weekly, etc.) and the occurrences (e.g., 1 day, 2 weeks, etc.).

   At ____.
   : Enter the time at which discovery should take place.

   Starting ____.
   : Click the drop-down list and select the start date.

4. Click *OK*.

Once the schedule options have been set and saved, two columns - Last Seen and Last Known MAC Address - are added to the range or scope view. The Last Seen column identifies when a host was last seen on the network.

Green
: Host responded to the last PING request. The date and time are shown.

Orange
Host has responded in the past, but did not respond to the last PING request. The date and time of last response is shown.

Red
Host has never responded to a PING request. The text Never is shown.

The list of ranges contains a column that shows if a discovery schedule has been set for a range. The name of this column is Schedule. To quickly see all ranges that have a schedule set, you can use the Quick Filter and filter by this column by entering `Schedule:Yes` in the Quick Filter search field.

At any time if you wish to disable host discovery, do the following:

1. Select the object(s) for which you want to disable discovery.
2. Right-click and, from the shortcut menu, select *Set Discovery Schedule*. The *Schedule* dialog box displays.
3. Uncheck the *Enable discovery schedule* option.
4. Click *OK*.

Configuring Host Discovery by Querying Routers

To collect information about hosts by querying routers, you must first enable collection of IP information from routers.

To configure host discovery:

1. Select an IP Address Range.
2. Right-click and, from the shortcut menu, select *Configure IP Address Collection*. The *IP Address Collection* dialog box displays
3. Enter the IP Address of the router(s) that you want to use to collect information about hosts in the range.
4. Click *OK*.

Failover Configurations and Split Scopes

Managing Failover Configurations (ISC DHCP)

This function allows you to manage DHCP failover peers on ISC DHCP servers.

Note: When adding a server's first failover peer, all other address pools on the server will be updated to refer to this failover peer.

---

1. On the object menu, select the DHCP Server that contains the scope for which you want to setup failover configuration.
2. From the list of scopes, double-click on the applicable one.
3. From the list of IP Addresses, right-click on the applicable one, and select *Create Address Pool* from the shortcut menu. The *DHCP Address Pool* dialog box displays.
4. Move to the **Failover Peer** field, and click the drop-down list arrow.
5. Select *Add new failover peer*.
6. Click *OK*. The *New Failover Peer* dialog box displays.

Name
Specifies the name of the failover peer.

Role
Specifies the role of the failover peer. The available roles are Primary and Secondary.

Address
Specifies the IP Address or DNS name on which the server should listen for connections from its failover peer.

Port
Specifies the port number on which the server should listen for connections from its failover peer.

Peer Address
Specifies the IP Address or DNS name to which the server should connect to reach its failover peer for failover messages.

Peer Port
Specifies the port number to which the server should connect to reach its failover peer for failover messages.

Max Response Delay
Specifies the number of seconds that may pass without the server receiving a message from its failover peer before it assumes that the connection has failed.

Max Unacked Updates
Specifies the number of messages the server can send before receiving an acknowledgement from its failover peer. According to ISC documentation, 10 seems to be a good value.

Max Client Lead Time
Specifies the number of seconds for which a lease can be renewed by either server without contacting the other. Only specified on the primary failover peer.

Split Index
Specifies the split between the primary and secondary failover peer for the purposes of load balancing. According to ISC documentation, 128 is really the only meaningful value. Only specified on the primary failover peer.

Load Balance Max Seconds
Specifies the cutoff in seconds after which load balancing is disabled. According to ISC documentation, a value of 3 or 5 is recommended.

7. Click *OK*. The DHCP Address Pool dialog box displays and shows the updated information.
8. Click *OK*.

If you need to EDIT or DELETE an existing failover peer, do the following:

1. Locate the relevant ISC DHCP server.
2. Right-click and, from the shortcut menu, select *Manage Failover Peers*. The *Failover Peers for ...* dialog box displays. All failover peers are shown.
3. To EDIT a failover peer, select it and click the *Edit* button. Then modify the *Failover Peers ... properties* dialog box, as needed.
4. To DELETE a failover peer, select it and click the *Delete* button.

Note: In order to finalize the setup of the failover relationship, the scope needs to be migrated to the failover peer.

Note: When deleting a failover peer through this dialog, if it is the last failover peer defined on the server, any references to it will be removed from existing address pools on the server. If there is one other failover peer left on the server, references to the failover peer being deleted will be changed to refer to the remaining failover peer. If, however, there are two or more other failover peers left on the server, the user will be prompted with a list of the remaining failover peers where he will have to choose which failover peer should be referenced by address pools currently referring to the failover peer being deleted.

Note: When changing from one failover peer to another for some specific address pool, if the address pool is the last one referring to the (old) failover peer, the user will be warned that performing the action will result in the deletion of the failover peer.

Managing Failover Configurations (Windows Server 2012)

DHCP failover on Windows Server 2012 enables high availability of DHCP services by synchronizing IP Address lease information between two DHCP servers. It is also possible to use DHCP failover to provide load balancing of DHCP requests.

You can configure failover for a single scope or for multiple scopes on the same server.

Note: To manage failover between two Windows 2012 Servers, the DHCP Server Controller must be running as a service account with enough privileges to manage the DHCP service. For more information, refer to the Men&Mice DHCP Server Controller section in the Installation Guide.

Setting up a Scope Failover

To setup failover for a scope, do the following:

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to setup failover configuration.
2. You have two ways to choose the scopes you want to configure.
    - From the list of scopes, select one or more scopes, right-click and select *Configure Failover*.
    - Right-click the DHCP server and select *Configure Failover*. A dialog box listing all configurable scopes displays. Select the scopes you want to configure and click *Next*. The failover configuration dialog box displays.

Relationship Name
: Select the relationship you want to use for the failover configuration or enter a name if you want to create a new relationship. If you choose an existing relationship, you will not be able to change any of the relationship properties and you can simply click OK to complete the failover configuration for the scope.

Partner Server
: Enter the name or IP Address of the partner DHCP server with which failover should be configured. You can select from the list of Windows Server 2012 machines or you can type the host name or IP Address of the partner server.

Mode
: Select the failover mode you want to use. You can choose between Hot standby and Load balance.

Role of Partner Server
If you chose the Hot standby mode, you must choose the role of the partner server. You can choose between Standby and Active. If you choose Standby the current server will be Active and vice versa.

Maximum Client Lead Time
If you don't want to use the default values, enter the new values in the hours and minutes edit fields.

Addresses reserved for standby server
If you chose the Hot standby mode, you must enter the percentage of addresses that should be reserved to the standby server.

Local server load balance percentage
If you chose the Load balance mode, you need to specify the load balance percentage to use on the local server. The remaining percentage will be used on the partner server.

State Switchover Interval
Select this checkbox if you want to use Automatic State Switchover and specify the interval to use.

Enable Message Authentication
Select this checkbox if you want to use message authentication between the DHCP servers. If the message authentication is enabled, you must provide a shared secret for the message authentication.

Removing a Failover Configuration

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to remove the failover configuration.
2. Select one or more scopes, right-click the selection and select *Deconfigure Failover*. A confirmation dialog box displays.
3. Click *Yes* to confirm the action. The failover configuration for the selected scope(s) is removed.

Replicating Failover Scopes

When using a failover configuration, it is possible to replicate scope information between servers. This is possible for individual scopes, all scopes that share a failover relationship or all scopes on a particular DHCP server. When a scope replication takes place, the scopes on the selected DHCP are considered the source scopes and the entire scope contents are replaced on the destination server.

To replicate individual scopes:

1. On the object menu, select the DHCP Server that contains the scope(s) you want to replicate.
2. Select one or more scopes, right-click the selection and select *Replicate Scope*. A confirmation dialog box displays.
3. Click *OK* to confirm the action. The selected scope is replicated.

To replicate all scopes that share a failover relationship:

1. On the object menu, select the DHCP Server that contains the scopes you want to replicate.
2. Right-click a scope using the desired relationship, and select *Replicate Relationship*. A confirmation dialog box displays.
3. Click *OK* to confirm the action. The scopes that use the same relationship as the selected scope are replicated. Note that this action may take some time if multiple scopes use the relationship.

To replicate all failover scopes on a DHCP server:

1. On the object menu, right-click the DHCP Server that contains the scopes you want to replicate and select *Replicate Failover Scopes* from the menu. A confirmation dialog box displays.
2. Click *OK* to confirm the action. All failover scopes on the selected server are replicated. Note that this action may take some time if the server contains multiple failover scopes.

Managing Failover Relationships

You can view, create, edit and delete existing failover relationships.

Adding a Failover Relationship

1. On the object menu, right-click the DHCP Server and select *Manage Failover Relationships* from the menu. A dialog box listing the current failover relationships displays.
2. Click the *Add* button. A dialog box displays, listing all scopes that are available to be configured for high availability.
3. Select the scope(s) you want to configure. To select all scopes, click the *Select all* checkbox. Click *Next*. The failover configuration dialog box displays.
4. Setup the failover configuration for the selected scopes.

Editing an Existing Failover Relationship

1. On the object menu, right-click the DHCP Server and select *Manage Failover Relationships* from the menu. A dialog box listing the current failover relationships displays.
2. Click the *Edit* button. The failover configuration dialog box displays. Note that some properties are disabled and cannot be changed.
3. Edit the failover configuration and click *OK* to save the settings.

You can delete existing failover relationships. When a failover relationship is deleted, the scopes are not removed from the DHCP server, but they are no longer in a failover configuration. After removing the failover relationship Micetro will handle the affected scopes as split scopes.

Deleting a Failover Relationship

1. On the object menu, right-click on the DHCP Server, and select *Manage Failover Relationships* from the menu. A dialog box listing the current failover relationships displays.
2. Click the *Delete* button and click *Yes* in the confirmation dialog box.

Managing Split Scopes

When a scope is hosted on multiple servers, the scope view lists all the servers that contain a copy of the scope. For scopes on MS servers, the line says 'Split Scope' and then lists the servers. For the ISC DHCP server, the line says 'Multiple Instances' and then lists the servers:

Micetro detects when a split scope configuration is in place. Split scopes are handled as follows:

- In the scope list, split scopes are shown with a different icon and in the server column, the text "split scope" displays

- When performing various actions on scopes (for example enable/disable, scope option changes, scope deletion), a dialog box displays where the user is asked to specify to which instances of the split scope the action should be applied.
- The DHCP scope window will show every instance of the split scope in a separate tab, making it possible to work with all instances of the split scope in a single window.
- The Overview and Statistics tab in the DHCP scope window will show a graphical overview for all of the split scope instances.
- Reservations are managed automatically. All changes to reservations (creation, modification, and deletion) are applied to all instances of the split scope.

The servers listed in this dialog box all contain the scope to which the user was applying the change. By pressing the Enable button, all instances of the scope would be enabled.

Note: Split scopes are only supported on MS DHCP servers.

Devices (Management Console)

Overview

Using the Devices feature, you can create devices, assign interfaces to each device and attach IP addresses to the interfaces.

What is a Device?

A Device is any item that can have an IP address linked to it. A device can, for example, be a computer, a router, a firewall, a phone or a virtual machine. A device has one or more interfaces and each device can have any number of IP addresses linked to it.

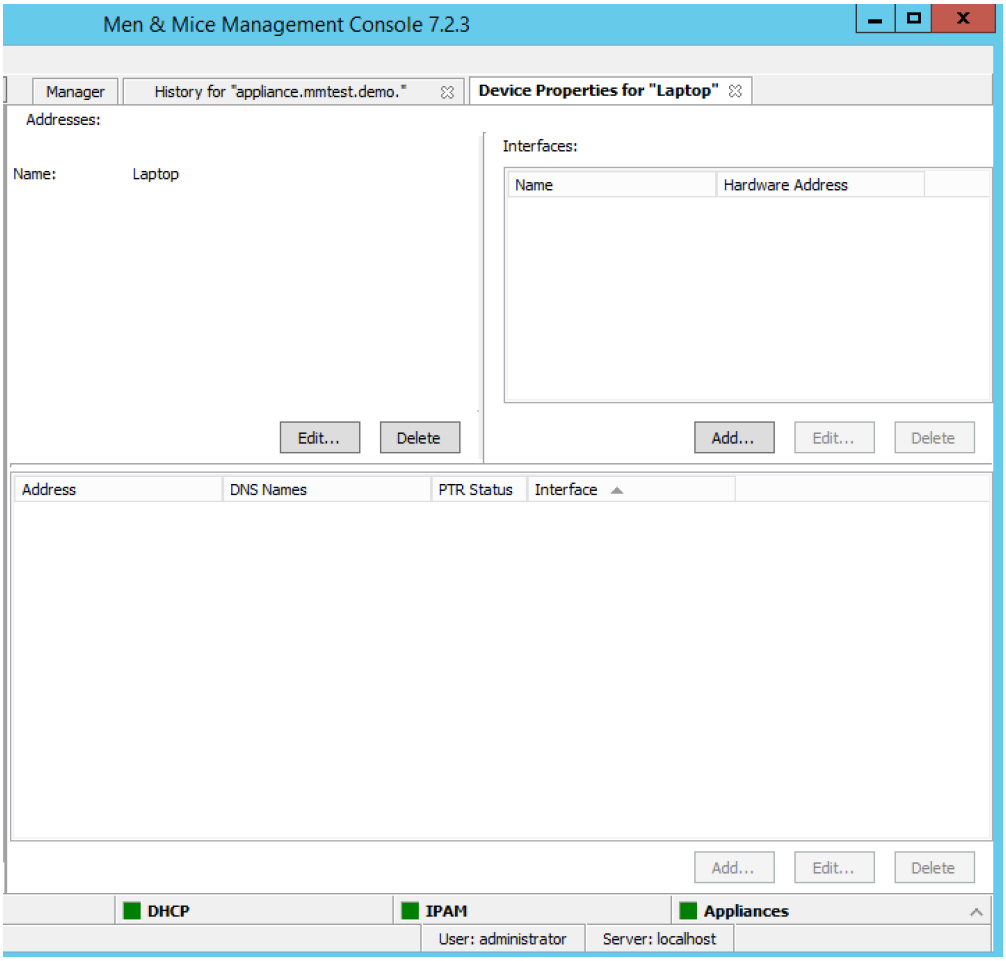
It is common to assign multiple properties to devices. As a default, a device in Micetro only has one property - the device name. However, you can create any number of properties for the devices. To create a property for a device, use the Define Custom Properties feature. For more information on this feature, refer to *Custom Properties*.

Adding a Device

When you add a Device, you start by entering the basic Device information and then you create the relevant interface(s) and optionally link one or more IP Addresses to each interface.

To add a new device:

1. From the menu bar, select *Device* → *New Device*. A dialog box is displayed where you enter the name of the device. The information you enter is based on the properties that have been defined for the device.
2. Enter the name and click *Add* to create the device.
3. Once the device has been created, the *Device Properties* tab displays. Use this tab to manage interfaces for the device and link IP addresses to the device.



To **Add** an interface click the Add button in the Interfaces section and enter the required information for the interface. The **Name** field is mandatory.

The **Hardware Address** field contains the MAC address for the interface. This field is not required. However, if you enter a Hardware Address it must be a valid MAC address and it must be unique – no other device can have an interface with the same Hardware Address.

To add an IP Address to the device, you must first create an interface as the IP Address is attached to an interface on the device. Once an interface has been created, click the Add button in the IP Address section and enter the required information for the IP Address.

Deleting a Device

When you delete a Device, all information about the device is deleted, including the interfaces defined for the device, and all IP addresses linked to the device are unlinked from the device.

To remove a Device:

1. Locate the device you want to remove and open the *Device Properties* window.
2. Click the *Delete* button in the *Device Details* section.
3. Click *OK* in the confirmation box that appears. The device and its associated data is removed.

Linking/Unlinking IP Addresses

Linking an IP Address

You can link an IP Address to a device using two different methods.

Linking an IP Address using the Device Properties window:

1. Locate the device you want to link the address to and open the *Device Properties* window.
2. Click the *Add* button in the *IP Address* section. Note that before you can link and IP Address to a device, you must first create an interface for the device.
3. Enter the required information and click *OK*.

Linking an IP address using the IP Address List window

1. Locate the IP Address Range containing the IP Address you want to link.
2. Double-click on it to display the list window.
3. Find the applicable IP Address.
4. Right-click and, from the shortcut menu, select *Link to Device*. The *Device Linking Wizard* displays.
5. For each of the resulting screens, make a selection/entry and move through the wizard.

Unlinking an IP Address

You can unlink an IP Address from a device using two different methods.

Unlinking an IP Address using the Device Properties window:

1. Locate the device you want to unlink the address from and open the *Device Properties* window.
2. Select the IP Address you want to unlink and click *Delete* in the *IP Address* section. The *Unlink IP Address confirmation* dialog box displays.
3. Select whether you want to only unlink the IP Address or whether you want to delete all data associated with the IP Address.

Unlinking an IP address using the IP Address List window

1. Locate the IP Address Range containing the IP Address you wan to unlink.
2. Double-click on it to display the list window.
3. Find the applicable IP Address.
4. Right-click and, from the shortcut menu, select *Unlink from Device*.
5. Click *OK* in the confirmation dialog box.

Searching for Devices

You can quickly find the device you want to work with using the Find Device command.

To search for a device:

1. From the menu bar, select *Device* → *Find Device*. The *Device Search* dialog box displays.
2. Enter the search criteria for the device you want to find.
3. To add a new search criterion, click the button with the + sign next to the search entry field
4. To remove a search criterion, click the button with the - sign next to the criterion you want to remove
5. Click *OK* to start the search. If the search result only contains one device, the *Device Properties* window displays. If multiple devices are found, the search result is displayed in the *Device List* window.

Device List tab

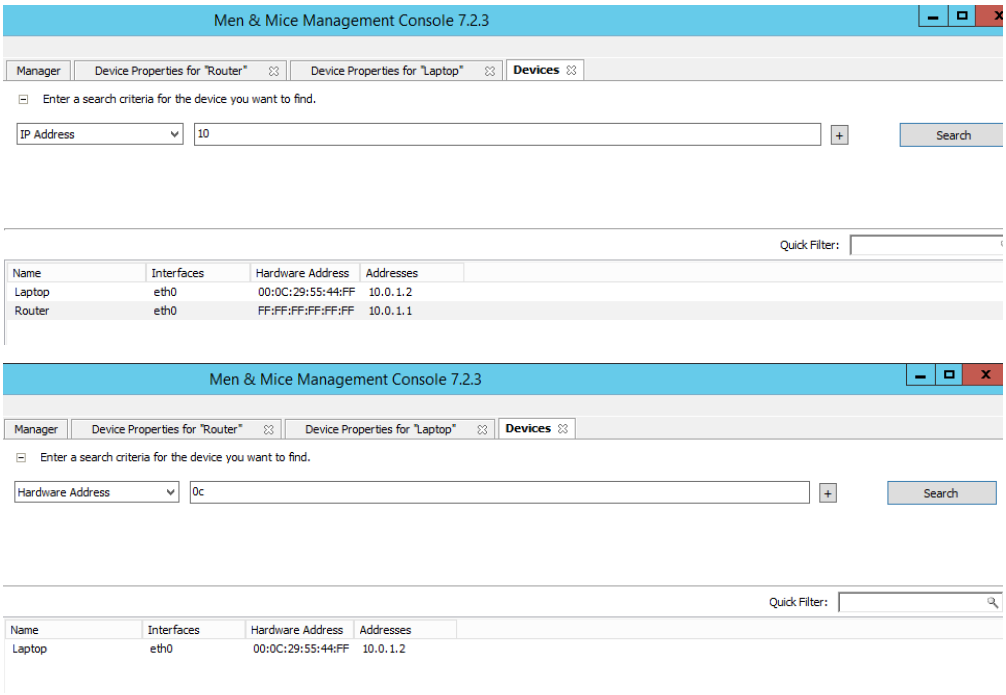
The Device List tab is displayed when you choose *Device* → *Show All Devices* from the menu bar. The tab is also used to display search results when there is more than one device that matches the search criteria.

The *Device List* tab shows all relevant info for the Devices found.

The tab contains a Quick Filter entry field that allows you to refine the search results. As you type in the field, results that are not applicable are removed. The Quick Filter searches within the entries that are displayed in the *Device List* tab.

Clicking the button with the + sign in the top left of the tab will expand the search panel. Using the search panel, you can search for devices based on multiple criteria. A search performed using the search panel will search the entire device list.

- To add a new search criterion, click the button with the + sign next to the search entry field.
- To remove a search criterion, click the button with the - sign next to the criterion you want to remove.



1.18 Automation

Automating your network infrastructure can help you streamline your workflow, save time, and increase efficiency. With Micetro, you have several automation options to choose from, including REST API, SOAP API, and JSON-RPC. These APIs allow you to seamlessly integrate Micetro with other platforms and carry out a vast array of automated operations.

You can also use Ansible for automation. With Ansible modules and plugins, you can connect to the Micetro API and create DNS, DHCP, and IPAM workflows.

Furthermore, Micetro offers a plugin (via the menandmice provider) that allows you to automate Micetro operations via Terraform.

1.18.1 Micetro REST API

With the Micetro REST API administrators and software developers can create custom scripts and applications on top of Micetro to manage DNS, DHCP, and IP address infrastructures of all sizes. Most features available in Micetro are available through the REST API.

Installation

To use the REST API, you must install the Men&Mice Web Services and make sure you have the correct access permission. For more information about installing the application, see *Web Application*.

All APIs are bundled together in the installation of the Web Services. Once the Men&Mice Web Services is installed, you can access the API documentation via:

`http(s)://<micetro.yourdomain.tld>/mmws/api/doc`

Tip: The online REST API documentation can also be viewed on api.menandmice.com.

Getting Started

In REST, the focus is on resources. You specify a resource with a URL (Uniform Resource Location) and then apply an operation on the resource using an HTTP method.

The four most common HTTP methods are GET, PUT, POST, and DELETE.

- `GET` – Retrieves resources
- `PUT` – Modifies an existing resource
- `POST` – Creates a new resource
- `DELETE` – Delete a resource

An example of a resource would be a DNS zone, defined in our REST API as `dnsZones`. The combination of URL and HTTP method to retrieve all DNS zones in Micetro would be:

```
GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones
```

A successful response looks like this:

```
{
 "result": {
     "dnsZones": [
         {
             "ref": "dnsZones/39404",
             "name": "bobo.is.",
             "dynamic": false,
             "adIntegrated": false,
             "dnsViewRef": "dnsViews/143",
             "sourceZoneRef": "dnsZones/39404",
             "authority": "bs-win-2.dev.lab.",
             "type": "Master",
             "dnssecSigned": false,
             "kskIDs": "",
             "zskIDs": "",
             "customProperties": {
                 "Location": "H-15",
                 "Outward facing": "0",
             },
             "created": "May 19, 2023 13:29:15",
             "lastModified": "May 19, 2023 13:29:16",
             "displayName": "bobo.is."
         }
     ],
     "totalResults": 1
   }
}
```


References

Each resource has its own unique identifier. These identifiers can be used to apply operations to a specific object. The format is `<resource>/<ID number>`. The ID number is a unique number for each resource type.

Building on top of our previous example, let's retrieve a specific zone using its unique identifier.

```
GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones/dnsZones/1
```

Tip: Unique identifiers can also be substituted for names as long as they are unique in the system. If a unique name is used instead of an identifier, Micetro will look up the identifier for the user. `GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones/test.menandmice.com`.

Arguments

The Micetro REST API offers a range of arguments that can be included in either the URL or the body of an HTTP request. Regardless of the resource being accessed, several arguments are always available:

- `server` – the name or address of the Micetro Central server that you want to communicate with.
- `loginName` – the username of the user attempting to authenticate.
- `password` – the password of the user attempting to authenticate.
- `session` – the unique ID of a valid user session.
- `pretty` – if set to 'true', the API returns data in a more readable format.

These arguments are all optional. By default, the API assumes that the Micetro Central instance is located on the same machine as the Web Services, which is usually the case. In addition to these arguments, the Micetro REST API also supports other authentication mechanisms, such as Basic Authentication, Windows NTLM, and Kerberos.

Filtering and Sorting Arguments

When using the GET operations in the Micetro REST API, you can take advantage of powerful arguments to filter, sort, or limit the results returned.

- `filter` – specifies the criteria to use when filtering results.
- `offset` – specifies the starting point for returning a list of values
- `limit` – specifies the maximum number of entries to include when returning a list of values.
- `sortBy` – specifies the field to use when sorting values.
- `sortOrder` – specifies whether to sort in ascending or descending order.

Here are some examples of how to use these arguments:

To get all zones with a name starting with `test.menandmice`.

```
GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones?filter=name=^test.menandmice
```

To get all zones sorted alphabetically by name:

```
GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones?sortBy=name&sortOrder=descending
```

To get the first 50 zones in the system in reverse order:

```
GET http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones?sortBy=name&
↪sortOrder=descending&limit=50
```

For a more detailed explanation of filtering and sorting in the Micetro REST API, see our REST API whitepaper.

Creation, Modification, and Deletion Arguments

Creating, modifying and deleting resources require the use of other HTTP methods, such as POST, PUT, and DELETE. These operations typically require more information than other API calls, and the data can be passed either in the URL or in the body of the HTTP request.

For example, to add a DNS record to a zone, you can use the following URL:

```
POST http(s)://<micetro.yourdomain.tld>/mmws/api/dnsZones/test.menandmice.com./
↪dnsRecords?dnsRecord={“name”:”name”, “type”: “A”, “data”: “1.2.3.4”}
```

To modify the newly created DNS record, you can use the following URL:

```
PUT http(s)://<micetro.yourdomain.tld>/mmws/api/dnsRecords/name.test.menandmice.com./?
↪properties={"data":"2.3.4.5"}
```

To delete the DNS record, you can use the following URL:

```
DELETE http(s)://<micetro.yourdomain.tld>/mmws/api/dnsRecords/name.test.menandmice.com.
```

Note: For more complex objects, it's recommended to provide the data in the body of the HTTP request rather than in the URL.

Tip: The API definition can be downloaded from the Web Services and then imported into a 3rd party API development tool such as Postman. To retrieve the API definition in JSON form, navigate to the url `http(s)://micetro.yourdomain.tld/mmws/api/swagger.json`.

1.18.2 SOAP API for Micetro

Introduction

The SOAP interface was introduced in Version 6.2 of the (then) Men&Mice Suite. The web service allows administrators and software developers to create custom scripts and applications on top of Micetro to manage DNS, DHCP and IP address infrastructures of all sizes. Most features available in Micetro are available through the web service interface.

The web service can be used to perform tasks such as:

- Configure and work with Bind, Microsoft and Unbound DNS servers,
- work with DNS zones and records,
- configure ISC and Microsoft DHCP servers,
- work with DHCP scopes, pools and reservations,
- IP address management (IPAM),
- and much more.

SOAP API documentation

The SOAP command reference can be viewed online on api.menandmice.com.

Tip: Documentation for the SOAP API is bundled with the Web Application, and can be viewed on `http(s)://micetro.yourdomain.tld/mmws/wsdldoc` where *micetro.yourdomain.tld* is the url for the Web Application.

If Men&Mice Central is running on a different server from the Web Application, the url to use is `http(s)://micetro.yourdomain.tld/mmws/wsdldoc?server=your.central.server.com`.

1.18.3 Ansible

For the latest Ansible plug-in information please see the documentation and downloads contained on Galaxy and Github. https://galaxy.ansible.com/ansilabnl/micetro https://github.com/ansilabnl/micetro

With the Ansible setup for Micetro by Men&Mice you can manage a Micetro installation through Ansible. The Ansible modules and plugins connect to the Micetro API and perform all needed actions.

See *Ansible configuration example* for an example configuration that you can use with the Ansible modules and plugins for Micetro.

Installation

The modules and plugins need to be installed on the Ansible control node, often called the Ansible controller and Ansible needs to be configured so that the modules and plugins can be found by Ansible.

Installing the Ansible modules and plugins is a straight forward process. Copy the Ansible modules and plugins to a directory on the Ansible control node, let us assume `/tmp/mandm`. Later on these files are copied to the destination directories on the control node.

Requirements

The Ansible integration modules and plugins do not need anything beyond a standard Ansible installation. The minimum Ansible version is 2.7 and up and the required Python version is 2.7+ or 3.5+.

Ansible modules

The Ansible modules can than be placed in a number of directories, depending on your installation and requirements.

`/usr/share/ansible/plugins/modules/`	System wide installation, modules available to all users
`~/.ansible/plugins/modules/`	Modules available only to the current user, as the modules are installed in the users home-directory
`/etc/ansible/library/`	Local installation. As most Ansible installations use the `/etc/ansible` directory as the Ansible top-directory (as this is the default in an Ansible installation), this is probably the best installation option. When installing the modules in this directory, the Ansible library path needs to be set in the `/etc/ansible/ansible.cfg` file, pointing to the module directory.

```
library = /etc/ansible/library
```

After installing the Ansible modules a check can be made to determine if the modules are installed correctly. Run the command:

```
ansible-doc -l | grep '^mm_'
```

This should produce a list with all the Micetro Ansible modules.

Ansible lookup plugins

The set of Ansible Integration modules consists of multiple sets (lookup and inventory) and these should be installed in their own directories.

The lookup plugins can be installed in:

`/usr/share/ansible/plugins/lookup`	System wide installation, modules available to all users
`~/.ansible/plugins/lookup`	Plugins available only to the current user, as the plugins are installed in the users home-directory
`/etc/ansible/plugins/lookup`	Local installation. As most Ansible installations use the `/etc/ansible` directory as the Ansible top-directory (as this is the default in an Ansible installation) this is probably the best installation option. When installing the lookup plugins in this directory, the Ansible lookup path needs to be set in the `/etc/ansible/ansible.cfg` file, pointing to the lookup plugin directory.

```
lookup_plugins = /usr/share/ansible/plugins/lookup:\
                 /etc/ansible/plugins/lookup
```

To check if the modules are installed correctly and are available to Ansible, issue the command:

```
ansible-doc -t lookup -l | grep '^mm_'
```

Which should produce a list with all the Micetro Ansible lookup plugins.

Ansible inventory plugins

The inventory plugins can be installed in:

`/usr/share/ansible/plugins/inventory`	System wide installation, modules available to all users
`~/.ansible/plugins/inventory`	Plugins available only to the current user, as the plugins are installed in the users home-directory
`/etc/ansible/plugins/inventory`	Local installation. As most Ansible installations use the `/etc/ansible` directory as the Ansible top-directory (as this is the default in an Ansible installation) this is probably the best installation option. When installing the inventory plugins in this directory, the Ansible lookup path needs to be set in the `/etc/ansible/ansible.cfg` file, pointing to the lookup plugin directory.

```
inventory_plugins = /usr/share/ansible/plugins/inventory:\
                    /etc/ansible/plugins/inventory
```

To check if the modules are installed correctly and are available to Ansible, issue the command:

```
ansible-doc -t inventory -l | grep '^mm_'
```

Which should produce a list with all the Micetro Ansible inventory plugins.

The `mm_inventory` plugin also needs some extra configuration, see *mm_inventory plugin* for more information.

API user

As the Ansible modules and plugins connect to a Micetro installation, a connection between Ansible and Micetro needs to be made.

API user for Micetro

In Micetro a user needs to be defined that has all rights in Micetro (administrator) so it is able to perform all needed tasks. It is also possible to delegate only certain tasks to certain API users. *Credential matrix* gives an overview which rights a required for every module.

API Provider in Ansible

For the Ansible modules and plugins to function correctly a provider has to be defined. This provider consist of a user, password and connection url (`mmurl`) and this provider needs to be defined in the Ansible setup, either through Ansible Tower/AWX or in the Ansible directory.

As the modules and plugins can be used by all systems under Ansible control, it is advised to define the API provider for the all group. Create a file all in the `/etc/ansible/group_vars` directory, or the `/etc/ansible/inventory/group_vars` directory (if your inventory is a directory instead of a file) which contains something similar to:

```
---
provider:
  mmurl: http://micetro.example.net
  user: apiuser
  password: apipasswd
```

Note: Encrypt the `apipasswd` with `ansible-vault` to prevent plaintext passwords in the Ansible tree.

An example to achieve this is:

```
printf "apipasswd"              | \
    ansible-vault               \
        encrypt_string          \
        --stdin-name="password"
```

Which results in:

```
password: !vault |
  $ANSIBLE_VAULT;1.1;AES256
  34646538383265336162666 53.....643434316266666430
  61396566363835373363653 13.....336161393439666431
  35393130656565313138383 56.....613861623135656634
  63323930636435313390a343 66.....323631613034356565
  6138
```

If an Ansible vault with multiple vault ID's is needed, please have a look at http://www.tonkersten.com/2019/07/151-ansible-with-multiple-vault-ids/ for more information.

The defined provider can be used in Ansible playbooks like:

Run ansible playbook for another host and delegate to the control node

```
- name: Claim IP address
  mm_claimip:
    state: present
    ipaddress: 172.16.12.14
    provider: "{{ provider }}"
  delegate_to: localhost
```

The reason for the `delegate_to: localhost` option, is that all commands can be performed on the Ansible control node. So, it is possible to protect the Micetro API to only accept commands from the Ansible control node and not from everywhere. This can also be achieved by creating a playbook that has localhost as the hosts-setting and is specific for the interaction with Micetro.

Run ansible playbook on the Ansible Control node

```
---
- name: host connection example
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Claim IP address
      mm_claimip:
        state: present
        ipaddress: 172.16.12.14
        provider: "{{ provider }}"
```

Ansible configuration example

Beneath is an example Ansible configuration file (`ansible.cfg`) with the assumption that all Micetro plugins and modules are installed in the `/etc/ansible` directory. Some lines end with a backslash \, which indicates that the following should be appended, but these are split for code clarity.

```
# ==============================================
[defaults]
remote_tmp              = $HOME/.ansible/tmp
inventory               = inventory
pattern                 = *
forks                   = 5
```

(continues on next page)

(continued from previous page)

```
poll_interval           = 15
ask_pass                = False
remote_port             = 22
remote_user             = ansible
gathering               = implicit
host_key_checking       = False
interpreter_python      = auto_silent
force_valid_group_names = true
retry_files_enabled     = False
callback_whitelist      = minimal, dense, oneline
stdout_callback         = default
nocows                  = 0
library                 = /etc/ansible/library
action_plugins          = /usr/share/ansible_plugins/action_plugins
callback_plugins        = /etc/ansible/plugins/callback_plugins
connection_plugins      = /usr/share/ansible_plugins/connection_plugins
filter_plugins          = /usr/share/ansible_plugins/filter_plugins
vars_plugins            = /usr/share/ansible_plugins/vars_plugins
inventory_plugins       = /usr/share/ansible_plugins/inventory_plugins:\
                          /etc/ansible/plugins/inventory
lookup_plugins          = /usr/share/ansible_plugins/lookup_plugins:\
                          /etc/ansible/plugins/lookup

[inventory]
enable_plugins   = mm_inventory, host_list, auto
cache            = no
cache_plugin     = pickle
cache_prefix     = mm_inv
cache_timeout    = 60
cache_connection = /tmp/mm_inventory_cache

[privilege_escalation]
become          = False
become_method   = sudo
become_user     = root
become_ask_pass = False
```

Credential matrix

Table 10: Module and plugin credentials needed

	Page 301, 1	2	3	4	5	6	7
mm_claimip.py				*			
mm_dhcp			*	*			
mm_dnsrecord		*					
mm_group					*		
mm_ipprops			*				
mm_props	*	*	*	*	*		
mm_role					*		
mm_user					*		
mm_zone		*					
mm_inventory				*			
mm_freeip				*			
mm_ipinfo				*			

Note: The `mm_props` module manages custom properties for all types, like DNS servers, DHCP servers, zones, IP ranges etc. When using the module for a type when no modify rights are granted, an error will occur. It is possible to grant less rights and allow only to modify a subset of the record types.

Ansible modules

mm_user

Manage user accounts and user properties in Micetro.

Options

authentication_type:
Authentication type to use. e.g. Internal, AD. Required if `state=present`.

descr:
Description of the user.

email:
The users email address.

groups:
Make the user a member of these groups.

name:
(required) Name of the user to create, remove or modify.

[1] Administrators (built-in)
[2] DNS Administrators (built-in)
[3] DHCP Administrators (built-in)
[4] IPAM Administrators (built-in)
[5] User Administrators (built-in)
[6] Approvers (built-in)
[7] Requesters (built-in)

password:
Users password (plaintext). Required if `state=present`.

provider:
(required) Definition of the Micetro API provider.

roles:
Make the user a member of these roles.

state:
Should the users account exist or not. (`absent`, `present`)

Examples

```
- name: Add the user 'mauricem' as an admin
  mm_user:
    username: mauricem
    password: password
    full_name: John Doe
    state: present
    authentication_type: internal
    roles:
        - Administrators (built-in)
        - DNS Administrators (built-in)
        - DHCP Administrators (built-in)
        - IPAM Administrators (built-in)
        - User Administrators (built-in)
        - Approvers (built-in)
        - Requesters (built-in)
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

```
- name: Remove user 'mauricem'
  mm_user:
    username: mauricem
    state: absent
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_group

Manage groups in Micetro.

Options

descr:
Description of the group.

name:
(required) Name of the group to create, remove or modify.

provider:
(required) Definition of the Micetro API provider.

roles:
List of roles to add to this group.

state:
Should the role exist or not. (`absent`, `present`)

users:
List of users to add to this group.

Examples

```
- name: Add the 'local' group
  mm_group:
    name: local
    desc: A local group
    state: present
    users:
      - mauricemoss
    roles:
      - IPAM Administrators (built-in)
  provider:
    mmurl: http://micetro.example.net
    user: apiuser
    password: apipasswd
  delegate_to: localhost
```

```
- name: Remove the 'local' group
  mm_group:
    name: local
    state: absent
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_role

Manage roles in Micetro.

Options

descr:
Description of the role.

groups:
List of groups to add to this role

name:
(required) Name of the role to create, remove or modify.

provider:
(required) Definition of the Micetro API provider.

state:
Should the role exist or not. (`absent`, `present`)

users:
List of users to add to this role

Examples

```
- name: Add the 'local' role
  mm_role:
    name: local
    desc: A local role
    state: present
  provider:
    mmurl: http://micetro.example.net
    user: apiuser
    password: apipasswd
  delegate_to: localhost
```

```
- name: Remove the 'local' role
  mm_role:
    name: local
    state: absent
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_props

Manage custom properties (see *Custom Properties*) in Micetro.

Options

cloudtags:
Associated cloud tags.

defaultvalue:
Default value of the property.

dest:
(required) The section where to define the custom property.

listitems:
The items in the selection list.

mandatory:
Is the property mandatory.

multiline:
Is the property multiline.

name:
(required) Name of the property.

proptype:
Type of the property. These are not the types as described in the API, but the types as you can see them in the Men&Mice Management Console.

provider:
(required) Definition of the Micetro provider.

readonly:
Is the property read only.

state:
The state of the properties or properties. (`absent`, `present`)

system:
Is the property system defined.

updateexisting:
Should objects be updated with the new values. Only valid when updating a property, otherwise ignored.

Examples

```
- name: Set definition for custom properties
  mm_props:
    name: location
    state: present
    proptype: text
    dest: zone
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
```

(continues on next page)

(continued from previous page)

```
      password: apipasswd
  delegate_to: localhost
```

mm_claimip

Claim IP addresses in DHCP in Micetro.

Options

customproperties:
Custom properties for the IP address. These properties must already exist. See also *mm_props*.

ipaddress:
(required) The IP address(es) to work on.

provider:
(required) Definition of the Micetro API provider.

state:
The state of the claim. (`absent`, `present`)

Examples

```
- name: Claim IP address
  mm_claimip:
    state: present
    ipaddress: 172.16.12.14
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

```
- name: Release claim on IP addresses
  mm_claimip:
    state: present
    ipaddress:
      - 172.16.12.14
      - 172.16.12.15
      - 172.16.12.16
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_ipprops

Set properties on an IP address in Micetro.

Options

deleteunspecified:
Clmicetroperties that are not explicitly set.

ipaddress:
(required) The IP address(es) to work on.

properties:
(required) Custom properties for the IP address. These properties must already be defined.

provider:
(required) Definition of the Micetro API provider.

state:
Property present or not. (`absent`, `present`)

Examples

```
- name: Set properties on IP
  mm_ipprops:
    state: present
    ipaddress: 172.16.12.14
    properties:
      claimed: false
      location: London
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_dhcp

Manage DHCP reservations in Micetro.

Options

ddnshost:
The dynamic DNS host to place the entry in.

deleteunspecified:
Clear properties that are not explicitly set.

filename:
Filename to place the entry in.

ipaddress:
(required) The IP address(es) to make a reservation on. When the IP address is changed a new reservation is made. It is not allowed to make reservations in DHCP blocks.

macaddress:
(required) MAC address for the IP address.

name:
(required) Name of the reservation

nextserver:
Next server as DHCP option (bootp).

provider:
(required) Definition of the Micetro API provider.

servername:
Server to place the entry in.

state:
The state of the reservation. (`absent`, `present`)

Examples

```
- name: Add a reservation for an IP address
  mm_dhcp:
    state: present
    name: myreservation
    ipaddress: 172.16.17.8
    macaddress: 44:55:66:77:88:99
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_zone

Manage DNS zones in Micetro.

Options

adintegrated:
True if the zone is Active Directory integrated.

adpartition:
The AD partition if the zone is Active Directory integrated.

adreplicationtype:
Type of the AD replication.

authority:
Name of the DNS server that contains the zone or the string `[Active Directory]` if the zone is integrated in the Active Directory.

customproperties:
Custom properties for the zone. These properties must already exist. See also *mm_props*.

dnssecsigned:
True if the zone is a DNSSEC signed zone.

dynamic:
Dynamic DNS zone.

kskids:
A comma separated string of IDs of KSKs, starting with active keys, then inactive keys in parenthesis

masters:
The IP addresses of the primary servers if the new zone is not a primary zone.

name:
(required) Name of the zone.

nameserver:
Nameserver to define the zone on. Required if `state=present`.

provider:
(required) Definition of the Micetro API provider.

servtype:
Type of server.

state:
The state of the zone. (`absent`, `present`)

zskids:
A comma separated string of IDs of ZSKs, starting with active keys, then inactive keys in parenthesis.

Examples

```
- name: Create a new zone
  mm_zone:
    state: present
    name: example.com
    nameserver: ns1.example.com
    authority: micetro.example.net
    customproperties:
      location: London
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

```
- name: Release a zone
  mm_zone:
    state: absent
    name: example.com
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
```

(continues on next page)

(continued from previous page)

```
    password: apipasswd
  delegate_to: localhost
```

mm_dnsrecord

Manage DNS records in Micetro.

In DNS it is very common to have multiple entries with the same name, as the example below shows.

```
mail01.example.net.   7200   IN   A      192.0.2.25
mail01.example.net.   7200   IN   A      192.0.2.143
mail01.example.net.   7200   IN   AAAA   2001:db8::25
mail01.example.net.   7200   IN   AAAA   2001:db8::587
```

Tip: To enable multiple records with the same name in the Ansible modules, there is no possibility to change a record, the only way is to add the new record with the updated data and remove the old one after that.

Options

aging:
The aging timestamp of dynamic records in AD integrated zones. Hours since January 1, 1601, UTC. Providing a non-zero value creates a dynamic record.

comment:
Comment string for the record. Note that only records in static DNS zones can have a comment string

data:
(required) The data that is added to the DNS record. The record data is a space-separated list, when the resource type is one of: `MX`, `SRV`, `NAPTR`, `CAA`, `CERT`, `HINFO` or `TLSA`.

Example: data: `"100 10 U E2U+sip !^.*$!sip:customer-service@example.com! ."`

dnszone:
(required) The DNS zone where the action should take place.

enabled:
True if the record is enabled. If the record is disabled the value is false

name:
(required) The name of the DNS record. Can either be partially or fully qualified.

provider:
(required) Definition of the Micetro API provider.

rrtype:
Resource Record Type for this DNS record. Default is `A`.

state:
The state of the properties. (`absent`, `present`)

ttl:
The Time-To-Live of the DNS record.

Examples

```
- name: Set DNS record in zone for a defined name
  mm_dnsrecord:
    state: present
    name: reynholm
    data: 172.16.17.2
    rrtype: A
    dnszone: example.net.
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

```
- name: Set PTR record in zone for a defined name
  mm_dnsrecord:
    state: present
    name: "2.17.16.172.in-addr.arpa."
    data: reynholm.example.net.
    rrtype: PTR
    dnszone: "17.16.172.in-addr.arpa."
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipasswd
  delegate_to: localhost
```

mm_freeip plugin

This Men&Mice FreeIP lookup plugin finds one or more free IP addresses in a certain network, defined in Micetro.

Options

claim:
Claim the IP address(es) for the specified amount of time in seconds

excludedhcp:
exclude DHCP reserved ranges from result

filter:
Micetro filter statement. Filter validation is done by Micetro, not in the plugin. More filter info: quickfilter

multi:
Get a list of x number of free IP addresses from the requested zones.

network:
(required) Network zone(s) from which the first free IP address is to be found. This is either a single network or a list of networks

ping:
ping the address found before returning.

provider:
(required) Definition of the Micetro API provider.

Usage

When using the Men&Mice FreeIP plugin something needs to be taken into account. When running an Ansible lookup plugin, this lookup action takes place every time the variable is referenced. So it will not be possible to claim an IP address for further reference, this way. This has to do with the way Ansible works. A solution for this is to assign all collected IP addresses to an Ansible fact, but here you need to make sure the factname is not used over multiple hosts.

Example usage

Claim IP addresses in one or more ranges

```
---
- name: Men&Mice FreeIP test play
  hosts: localhost
  connection: local
  become: false

  vars:
    provider:
      mmurl: http://micetro.example.net
      user: apiuser
      password: apipassword
    network: examplenet

  tasks:
    - name: Set free IP addresses as a fact
      set_fact:
        freeips: "{{ query('mm_freeip',
                           provider,
                           network,
                           multi=15,
                           claim=60,
                           startaddress='192.168.63.100',
                           excludedhcp=True,
                           ping=True)
                  }}"

    - name: Get the free IP address and show info
      debug:
        msg:
          - "Free IPs          : {{ freeips }}"
          - "Queried network   : {{ network }}"
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Loop over IP addresses
      debug:
```

(continues on next page)

(continued from previous page)

```
        msg:
          - "Next free IP      : {{ item }}"
      loop: "{{ freeips }}"
```

```
# ansible-playbook mmtest.yml

PLAY [Men&Mice FreeIP test play] ************************************

TASK [Gathering Facts] **********************************************
ok: [localhost]

TASK [Set free IP addresses as a fact] ******************************
ok: [localhost]

TASK [Get the free IP address and show info] ************************
ok: [localhost] => {
    "msg": [
        "Free IPs          : ['192.168.63.203', '192.168.63.204']",
        "Queried network   : nononet",
        "Ansible version   : 2.9.7",
        "Python version    : 3.6.8",
        "Python executable : /usr/libexec/platform-python"
    ]
}

TASK [Loop over IP addresses] ***************************************
ok: [localhost] => (item=192.168.63.203) => {
    "msg": [
        "Next free IP      : 192.168.63.203"
    ]
}
ok: [localhost] => (item=192.168.63.204) => {
    "msg": [
        "Next free IP      : 192.168.63.204"
    ]
}

PLAY RECAP **********************************************************
localhost : ok=4  changed=0  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
```

mm_inventory plugin

This plugin generates the inventory from Micetro. It supports reading configuration from both a YAML configuration file and environment variables. If reading from the YAML file, the filename must end with `mm_inventory.(yml|yaml)`, the path in the command would be `/path/to/mm_inventory.(yml|yaml)`. If some arguments in the configuration file are missing, this plugin will try to fill in the missing arguments by reading from environment variables. If reading configurations from environment variables, the path in the command must be @mm_inventory.

Valid configuration filenames are:

- `mm_inventory`
- `mmsuite`

- mandm
- menandmice
- mandmsuite
- mm_suite
- mandm_suite

Options

There are two sets of configuration options, the options for the inventory plugin to function correctly and for Ansible to know how to use the plugin.

Plugin configuration

The mm_inventory plugin is configured through a configuration file, named mm_inventory.yml and the options are:

plugin
: Name of the plugin (mm_inventory)

host
: Micetro to connect to (http://micetro.example.net)

user
: UserID to connect with (apiuser)

password
: The password to connect with (apipasswd)

filters
: Filter on custom properties, can be more than 1 and should be a list. If multiple filters are given, they act as an and function

ranges
: What IP ranges to examine (172.16.17.0/24) Multiple ranges can be given, they act as an or function

---

Note: When both *ranges* and *filters* are supplied that will result in an and function.

Example:

```
filters:
  - location: home
  - owner: tonk
ranges:
  - 192.168.4.0/24
  - 172.16.17.0/24
```

Would result in an inventory for all host that have the location: home and owner: tonk custom properties set and are either a member of the 192.168.4.0/24 or 172.16.17.0/24 range.

An example of the mm_inventory.yml file:

```
plugin: mm_inventory
host: "http://micetro.example.net"
user: apiuser
password: apipasswd
filters:
  - location: London
ranges:
  - 172.16.17.0/24
```

Environment variables:

The `mm_inventory` plugin can also be configured through environment variables

```
export MM_HOST=YOUR_MM_HOST_ADDRESS
export MM_USER=YOUR_MM_USER
export MM_PASSWORD=YOUR_MM_PASSWORD
export MM_FILTERS=YOUR_MM_FILTERS
export MM_RANGES=YOUR_MM_RANGES
```

When reading configuration from the environment, the inventory path must always be `@mm_inventory`.

```
ansible-inventory -i @mm_inventory --list
```

Ansible configuration

Ansible needs to know about the `mm_inventory` plugin and also has some extra configuration options. First the `mm_inventory` plugin needs to be enabled, so Ansible can use it. This is done in the `[inventory]` section in the `ansible.cfg` file.

```
[inventory]
enable_plugins   = mm_inventory, host_list, auto
cache            = yes
cache_plugin     = jsonfile
cache_prefix     = mm_inv
cache_timeout    = 3600
cache_connection = /tmp/mm_inventory_cache
```

With the following meaning:

cache:
: Switch caching on and off

cache_plugin:
: Which caching plugin to use

  - jsonfile
  - yaml
  - pickle
  - …

cache_prefix:
: User defined prefix to use when creating the cache files

cache_connection:
Path in which the cache plugin will save the cache files

cache_timeout:
Timeout for the cache in seconds

Now the inventory plugin can be used with Ansible, like:

```
ansible-inventory -i /path/to/mm_inventory.yml --list
```

Or set the `mm_inventory.yml` as the Ansible inventory in the `ansible.cfg` file.

```
inventory = mm_inventory.yml
```

mm_ipinfo plugin

This Men&Mice IPInfo lookup plugin finds a lot of info about a specified IP address, defined in Micetro.

Options

ipaddress:
(required) The IP address that is examined

provider:
(required) Definition of the Micetro API provider.

Usage

The `mm_ipinfo` plugin delivers a complete set of information about an IP address, as it is delivered by the Micetro API.

Example usage:

Get information on an IP address

```
- name: Get all info for this IP address
  debug:
    var: ipinfo
  vars:
    ipinfo: "{{ query('mm_ipinfo', provider, '172.16.17.2') | to_nice_json }}"
```

With output like (output shortened):

```
ok: [localhost] => {
    "ipinfo": {
        "addrRef": "IPAMRecords/11",
        "address": "172.16.17.2",
        "claimed": false,
        "customProperties": {
            "location": "In the basement"
        },
```

(continues on next page)

(continued from previous page)

```
    }
}
```

Example playbooks

To use the Micetro Ansible Integration you need to create Ansible playbooks that utilize the functionality of Micetro.

Following are a couple of example playbooks for inspiration. These playbooks have been tested extensively with different operating systems, versions of Ansible and Python.

Contents

play-user

```
---
#
# Add, delete and change users in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice users test play
  hosts: localhost
  connection: local
  become: false
```

(continues on next page)

(continued from previous page)

```yaml
tasks:
  - name: Get the free IP address and show info
    debug:
      msg:
        - "Ansible version    : {{ ansible_version.full }}"
        - "Python version     : {{ ansible_facts['python_version'] }}"
        - "Python executable  : {{ ansible_facts['python']['executable'] }}"

  - name: Add the user 'mauricem' as an admin
    mm_user:
      username: mauricem
      password: password
      full_name: Maurice Moss
      state: present
      authentication_type: internal
      roles:
        - Administrators (built-in)
        - DNS Administrators (built-in)
        - DHCP Administrators (built-in)
        - IPAM Administrators (built-in)
        - User Administrators (built-in)
        - Approvers (built-in)
        - Requesters (built-in)
      provider: "{{ provider }}"

  - name: Check idempotency
    mm_user:
      username: mauricem
      password: password
      full_name: Maurice Moss
      state: present
      authentication_type: internal
      roles:
        - Administrators (built-in)
        - DNS Administrators (built-in)
        - DHCP Administrators (built-in)
        - IPAM Administrators (built-in)
        - User Administrators (built-in)
        - Approvers (built-in)
        - Requesters (built-in)
      provider: "{{ provider }}"

  - name: Change the groups
    mm_user:
      username: mauricem
      password: password
      full_name: Maurice Moss
      state: present
      authentication_type: internal
      roles:
        - Administrators (built-in)
```

(continues on next page)

(continued from previous page)

```
        - User Administrators (built-in)
        - Approvers (built-in)
        - Requesters (built-in)
      provider: "{{ provider }}"

  - name: Check idempotency again
    mm_user:
      username: mauricem
      password: password
      full_name: Maurice Moss
      state: present
      authentication_type: internal
      roles:
        - Administrators (built-in)
        - User Administrators (built-in)
        - Approvers (built-in)
        - Requesters (built-in)
      provider: "{{ provider }}"

  - name: Remove the user again
    mm_user:
      username: mauricem
      state: absent
      provider: "{{ provider }}"
```

play-group

```
---
#
# Add, delete and change groups in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice users test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Get the free IP address and show info
      debug:
        msg:
          - "Ansible version    : {{ ansible_version.full }}"
          - "Python version     : {{ ansible_facts['python_version'] }}"
```

(continues on next page)

(continued from previous page)

```
        - "Python executable  : {{ ansible_facts['python']['executable'] }}"

    - name: Add the 'local' group
      mm_group:
        name: local
        desc: A local rgroup
        state: present
        users:
          - mauricemoss
          - jenbarber
        provider: "{{ provider }}"

    - name: Check idempotency
      mm_group:
        name: local
        desc: A local group
        state: present
        users:
          - mauricemoss
          - jenbarber
        provider: "{{ provider }}"

    - name: Add nonexisting user to group
      mm_group:
        name: local
        desc: A local group
        state: present
        users:
          - roy
        provider: "{{ provider }}"
      ignore_errors: true

    - name: Remove the 'local' group
      mm_group:
        name: local
        state: absent
        provider: "{{ provider }}"
```

play-role

```
---
#
# Add, delete and change roles in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
```

(continues on next page)

(continued from previous page)

```
#      password: apipasswd
#
- name: Men&Mice users test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Get the free IP address and show info
      debug:
        msg:
          - "Ansible version    : {{ ansible_version.full }}"
          - "Python version     : {{ ansible_facts['python_version'] }}"
          - "Python executable  : {{ ansible_facts['python']['executable'] }}"

    - name: Add the 'local' role
      mm_role:
        name: local
        desc: A local role
        state: present
        users:
          - mauricemoss
          - jenbarber
        provider: "{{ provider }}"

    - name: Check idempotency
      mm_role:
        name: local
        desc: A local role
        state: present
        users:
          - mauricemoss
          - jenbarber
        provider: "{{ provider }}"

    - name: Add nonexisting user to role
      mm_role:
        name: local
        desc: A local role
        state: present
        users:
          - roy
        provider: "{{ provider }}"
      ignore_errors: true

    - name: Remove the 'local' role
      mm_role:
        name: local
        state: absent
        provider: "{{ provider }}"
```

play-props

```
---
#
# Set, delete and change custom properties in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice Custom Properties test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Set text property
      mm_props:
        state: present
        name: MyProperty
        proptype: text
        dest: dnsserver
        listitems:
          - Paul
          - Daniel
          - April
          - Nolan
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: Check idempotentie
      mm_props:
        state: present
        name: MyProperty
        proptype: text
        dest: dnsserver
        listitems:
          - Paul
          - Daniel
          - April
          - Nolan
        provider: "{{ provider }}"
```

(continues on next page)

(continued from previous page)

```
    delegate_to: localhost

  - name: Change type - not allowed
    mm_props:
      state: present
      name: MyProperty
      proptype: yesno
      dest: dnsserver
      listitems:
        - Paul
        - Daniel
        - April
        - Nolan
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Change list around
    mm_props:
      state: present
      name: MyProperty
      proptype: text
      dest: dnsserver
      listitems:
        - Paul
        - Daniel
        - April
        - Nolan
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Remove property
    mm_props:
      state: absent
      name: MyProperty
      proptype: text
      dest: dnsserver
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Remove property - again
    mm_props:
      state: absent
      name: MyProperty
      proptype: yesno
      dest: dnsserver
      provider: "{{ provider }}"
    delegate_to: localhost
```

play-claimip

```yaml
---
#
# Claim and release an IP address in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
#
- name: Men&Mice ClaimIP test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Claim IP address
      mm_claimip:
        state: present
        ipaddress: 172.16.12.14
        provider: "{{ provider }}"

    - name: Check idempotentie
      mm_claimip:
        state: present
        ipaddress: 172.16.12.14
        provider: "{{ provider }}"

    - name: Unclaim IP address
      mm_claimip:
        state: present
        ipaddress: 172.16.12.14
        provider: "{{ provider }}"

    # This task claims an IP address that cannot exit
    # and returns a warning because of that
    - name: Claim erroneous IP address
      mm_claimip:
        state: present
        ipaddress: 456.978.12.14
        provider: "{{ provider }}"
```

play-dhcp

```
---
#
# Make a DHCP reservation and release it in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice DHCP test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Add a reservation for an IP address
      mm_dhcp:
        state: present
        name: myreservation
        ipaddress: 172.16.17.8
        macaddress: 44:55:66:77:88:00
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: check idempotentie
      mm_dhcp:
        state: present
        name: myreservation
        ipaddress: 172.16.17.8
        macaddress: 44:55:66:77:88:00
        provider: "{{ provider }}"
      delegate_to: localhost

    # Changing the MAC address of a reservation is not allowed, as this
    # would alter the reservation. To achieve this, release the reservation
    # and reclaim it.
    - name: change mac
      mm_dhcp:
        state: present
        name: myreservation
        ipaddress: 172.16.17.8
```

(continues on next page)

(continued from previous page)

```
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: change ip
    mm_dhcp:
      state: present
      name: myreservation
      ipaddress: 172.16.17.9
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: change name
    mm_dhcp:
      state: present
      name: movemyreservation
      ipaddress: 172.16.17.9
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: delete reservation (wrong one)
    mm_dhcp:
      state: absent
      name: movemyreservation
      ipaddress: 172.16.17.9
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: delete reservation (correct one)
    mm_dhcp:
      state: absent
      name: myreservation
      ipaddress: 172.16.17.8
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: create reservation in invalid range
    mm_dhcp:
      state: present
      name: reservationnonet
      ipaddress: 172.16.17.58
      macaddress: 44:55:66:77:88:99
      provider: "{{ provider }}"
    delegate_to: localhost
```

play-zone

```yaml
---
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice DHCP test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Ensure the zone
      mm_zone:
        state: present
        name: example.com
        nameserver: mandm.example.com
        authority: mandm.example.net
        masters: mandm.example.net
        servtype: master
        customproperties:
          owner: Reynholm Industries
          place: London
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: Remove the zone
      mm_zone:
        state: absent
        name: example.com
        provider: "{{ provider }}"
      delegate_to: localhost
```

play-dnsrecord

```
---
#
# Set and change a DNS record in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice DNSRecord test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    - name: Set DNS record
      mm_dnsrecord:
        state: present
        name: reynholm
        rrtype: A
        dnszone: testzone
        data: 192.168.10.12
        comment: From The API side
        ttl: 86400
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: Check idempotentie
      mm_dnsrecord:
        state: present
        name: reynholm
        rrtype: A
        dnszone: testzone
        data: 192.168.10.12
        comment: From The API side
        ttl: 86400
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: Set DNS record with erroneous values
      mm_dnsrecord:
```

(continues on next page)

(continued from previous page)

```
      state: present
      name: reynholm
      rrtype: AAAA
      dnszone: testzone
      data: 192.168.10.127
      comment: From The API side
      ttl: apple
      provider: "{{ provider }}"
    delegate_to: localhost
    ignore_errors: true

  - name: Change record
    mm_dnsrecord:
      state: present
      name: reynholm
      rrtype: A
      dnszone: testzone
      data: 192.168.10.14
      comment: From The API side
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Do something stupid
    mm_dnsrecord:
      state: present
      name: reynholm
      rrtype: A
      dnszone: notthetestzone
      data: 192.168.90.14
      comment: Welcome to the error
      provider: "{{ provider }}"
    delegate_to: localhost
    ignore_errors: true

  - name: Do more something stupid things
    mm_dnsrecord:
      state: present
      name: reynholm
      rrtype: A
      dnszone: testzone
      data: 192.168.390.14
      comment: Welcome to the error
      provider: "{{ provider }}"
    delegate_to: localhost
    ignore_errors: true

  - name: Remove record
    mm_dnsrecord:
      state: absent
      name: reynholm
      dnszone: notthetestzone
      data: 192.168.90.14
```

(continues on next page)

(continued from previous page)

```
        provider: "{{ provider }}"
      delegate_to: localhost

    - name: Remove record - again
      mm_dnsrecord:
        state: absent
        name: reynholm
        dnszone: notthetestzone
        data: 192.168.90.14
        provider: "{{ provider }}"
      delegate_to: localhost
```

play-freeip

```
---
#
# Find a set of free IP addresses in a range in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice FreeIP test play
  hosts: localhost
  connection: local
  become: false

  vars:
    network:
      - examplenet

  tasks:
    - name: Set free IP addresses as a fact
      set_fact:
        freeips: "{{ query('mm_freeip',
                           provider,
                           network,
                           multi=25,
                           claim=60,
                           excludedhcp=True,
                           ping=True)
                 }}"

    - name: Get the free IP address and show info
      debug:
        msg:
```

(continues on next page)

(continued from previous page)

```
        - "Free IPs           : {{ freeips }}"
        - "Queried network(s) : {{ network }}"
        - "Ansible version    : {{ ansible_version.full }}"
        - "Python version     : {{ ansible_facts['python_version'] }}"
        - "Python executable  : {{ ansible_facts['python']['executable'] }}"

    - name: Loop over IP addresses
      debug:
        msg:
          - "Next free IP       : {{ item }}"
      loop: "{{ freeips }}"
```

play-ipinfo

```
---
#
# Get all info for an IP address in Micetro example
#
# The file <ansible_topdir>/group_vars/all contains:
#
#    ---
#    provider:
#      mmurl: http://micetro.example.net
#      user: apiuser
#      password: apipasswd
#
- name: Men&Mice IP Info test play
  hosts: localhost
  connection: local
  become: false

  tasks:
    - name: Get get IP info
      set_fact:
        ipinfo: "{{ query('mm_ipinfo', provider, '172.16.17.2') | to_nice_json }}"

    - name: Show Ansible and Python information
      debug:
        msg:
          - "Ansible version    : {{ ansible_version.full }}"
          - "Python version     : {{ ansible_facts['python_version'] }}"
          - "Python executable  : {{ ansible_facts['python']['executable'] }}"

    - name: Show all infor for this IP address
      debug:
        var: ipinfo

    # This task tries to get the information for a non-existing IP address
    # which results in a fatal `Object not found for reference` error
    - name: Get get IP info for a non existing IP address
```

(continues on next page)

(continued from previous page)

```
    set_fact:
      ipinfo: "{{ query('mm_ipinfo', provider, '390.916.17.2') | to_nice_json }}"
    ignore_errors: true
```

play_it_all

Example of a playbook that combines functionality

```
---
- name: Men&Mice test play
  hosts: localhost
  connection: local
  become: false

  vars:
    network: examplenet

  tasks:
    # Some extra information about Ansible and the used
    # Python version
    - name: Ansible information
      debug:
        msg:
          - "Ansible version   : {{ ansible_version.full }}"
          - "Python version    : {{ ansible_facts['python_version'] }}"
          - "Python executable : {{ ansible_facts['python']['executable'] }}"

    # The `ipaddr` filter needs the Python `netaddr` module, so make sure
    # this is installed
    # The `ipaddr` is used to determine the reverse IP address
    #
    # For example:
    #   vars:
    #     ipa4: "172.16.17.2"
    #     ipa6: "2001:785:beef:1:f2c4:8f9d:b554:e614"
    #
    #   - "Forward IPv4 address : {{ ipa4 }}"
    #   - "Forward IPv4 address : {{ ipa4 }}"
    #   - "Reverse IPv4 address : {{ ipa4 | ipaddr('revdns') }}"
    #   - "Reverse IPv6 address : {{ ipa6 | ipaddr('revdns') }}"
    #   - "Reverse IPv4 zone    : {{ (ipa4 | ipaddr('revdns')).split('.')[1:]  | join('.') }}
↪"
    #   - "Reverse IPv6 zone    : {{ (ipa6 | ipaddr('revdns')).split('.')[16:] | join('.') }}
↪"
    #
    # The reverse zones are split on '.' and only the last part is
    # used (in this example). The reverse for IPv4 assumes a '/24' network
    # and the '16' in the IPv6 zone conversion is for a '/64' network. Adapt these to your
    # own needs (e.g. '2' for a '/16' network on IPv4 or '20' for an IPv6 '/48' net.

    - name: Ensure the netaddr module is installed for Python 2
```

(continues on next page)

(continued from previous page)

```
    pip:
      name: netaddr
      state: present
    when: ansible_facts['python_version'] is version('3', '<')
    become: true

  - name: Ensure the netaddr module is installed for Python 3
    pip:
      name: netaddr
      state: present
      executable: pip3
    when: ansible_facts['python_version'] is version('3', '>=')
    become: true

  - name: define custom properties for IP addresses
    mm_props:
      name: location
      state: present
      proptype: text
      dest: ipaddress
      provider: "{{ provider }}"

  # The above example defines just a single property.
  # Defining multiple properties can be achieved by using
  # the Ansible loop functionality.
  #
  # - name: Example of multiple properties
  #   mm_props:
  #      name: "{{ item.name }}"
  #      state: "{{ item.state }}"
  #      proptype: "{{ item.proptype }}"
  #      dest: "{{ item.dest }}"
  #  loop:
  #    - name: location
  #      state: present
  #      proptype: text
  #      dest: ipaddress
  #    - name: owner
  #      state: present
  #      proptype: text
  #      dest: ipaddress

  # When running an Ansible lookup plugin, this lookup action takes
  # place every time the variable is referenced. So it will not be
  # possible to claim an IP address for further reference, this way.
  # This has to do with the way Ansible works.  A solution for this
  # is to assign all collected free IP addresses to an Ansible fact,
  # but here you need to make sure the factname is not used over
  # multiple hosts.
  - name: get free IP addresses and set it as a fact
    set_fact:
      freeips: "{{ query('mm_freeip', provider, network, claim=60, excludedhcp=True) }}
```

(continues on next page)

(continued from previous page)

```
↪"

  - name: Get the free IP address and show info
    debug:
      msg:
        - "Free IPs           : {{ freeips }}"
        - "Queried network(s) : {{ network }}"

  # Make a DHCP reservation for this address
  # So claim it after DNS setting.
  - name: Reservation on IP address
    mm_dhcp:
      state: present
      name: testhost
      ipaddress: "{{ freeips }}"
      macaddress: "de:ad:be:ef:16:10"
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Set properties on IP
    mm_ipprops:
      state: present
      ipaddress: "{{ freeips }}"
      properties:
        claimed: false
        location: London
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Ensure the zone
    mm_zone:
      state: present
      name: thetestzone.com
      nameserver: mandm.example.com
      authority: mandm.example.net
      masters: mandm.example.net
      servtype: master
      provider: "{{ provider }}"
    delegate_to: localhost

  # The `mm_freeip` plugin always returns a list, but the request was for just 1
  # IP address. The `mm_dnsrecord` only needs a single IP address. That's why the
  # list-slice `[0]` is used.
  - name: Set a DNS record for the claimed IP
    mm_dnsrecord:
      dnszone: testzone
      name: testhost
      data: "{{ freeips[0] }}"
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Set a PTR DNS record for the claimed IP
```

(continues on next page)

(continued from previous page)

```
    mm_dnsrecord:
      dnszone: "{{ (freeips[0] | ipaddr('revdns')).split('.')[1:]  | join('.') }}"
      name: "{{ freeips[0] | ipaddr('revdns') }}"
      data: "testhost.testzone."
      rrtype: PTR
      provider: "{{ provider }}"
    delegate_to: localhost

  # The `mm_ipinfo` returns all known information of an IP
  # address. This can be used to query certain properties, or
  # for debugging.
  - name: Get all info for this IP address
    debug:
      var: freeipinfo
    vars:
      freeipinfo: "{{ query('mm_ipinfo', provider, freeips[0]) | to_nice_json }}"

  - name: Renew properties on IP
    mm_ipprops:
      state: present
      ipaddress: "{{ freeips }}"
      properties:
        claimed: false
        location: Madrid
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Get all info for this IP address
    debug:
      var: freeipinfo
    vars:
      freeipinfo: "{{ query('mm_ipinfo', provider, freeips[0]) | to_nice_json }}"

  - name: Remove properties of IP
    mm_ipprops:
      state: present
      ipaddress: "{{ freeips }}"
      deleteunspecified: true
      properties:
        claimed: false
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Get all info for this IP address
    debug:
      var: freeipinfo
    vars:
      freeipinfo: "{{ query('mm_ipinfo', provider, freeips[0]) | to_nice_json }}"

  - name: Remove reservation on IP address
    mm_dhcp:
      state: absent
```

(continues on next page)

(continued from previous page)

```
      name: testhost
      ipaddress: "{{ freeips }}"
      macaddress: "de:ad:be:ef:16:10"
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Get all info for this IP address
    debug:
      var: freeipinfo
    vars:
      freeipinfo: "{{ query('mm_ipinfo', provider, freeips[0]) | to_nice_json }}"

  - name: Remove DNS record for the claimed IP
    mm_dnsrecord:
      state: absent
      dnszone: testzone
      name: testhost
      data: "{{ freeips[0] }}"
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Remove the PTR DNS record for the claimed IP
    mm_dnsrecord:
      state: absent
      dnszone: "{{ (freeips[0] | ipaddr('revdns')).split('.')[1:]  | join('.') }}"
      name: "{{ freeips[0] | ipaddr('revdns') }}"
      data: "testhost.testzone."
      rrtype: PTR
      provider: "{{ provider }}"
    delegate_to: localhost

  - name: Get all info for this IP address
    debug:
      var: freeipinfo
    vars:
      freeipinfo: "{{ query('mm_ipinfo', provider, freeips[0]) | to_nice_json }}"

  - name: Ensure the zone absent
    mm_zone:
      state: absent
      name: thetestzone.com
      nameserver: mandm.example.com
      authority: mandm.example.net
      masters: mandm.example.net
      servtype: master
      provider: "{{ provider }}"
    delegate_to: localhost
```

1.18.4 Terraform

Installing the Micetro provider for Terraform

Download compiled binaries

Precompiled binaries for Windows and Linux are available on the Men&Mice download server.

Manual Build and Install

Mac or Linux

make install

Windows

1. Build and install the provider:

```
go build -o terraform-provider-menandmice.exe
```

2. Copy the `terraform-provider-menandmice.exe` to:

- for Terraform 0.12: `%APPDATA%\terraform.d\plugins\windows_amd64\`
- for Terraform 0.14: `%APPDATA%\terraform.d\plugins\registry.terraform.io\local\menandmice\0.2.0\windows_amd64\`

3. Initialize:

```
terraform.exe init
```

Run acceptation test

Define the Micetro server:

```
dnsserver: micetro.example.net. micetro.example.com.
dhcpserver: micetro.example.net.
ipam-properties: location
```

Set provider settings that are not set in `main.tf`:

```
export MENANDMICE_ENDPOINT=<api-endpoint>
export MENANDMICE_USERNAME=<your username>
export MENANDMICE_PASSWORD=<your password>
```

And make a test account:

```
make testacc
```

For using the Micetro provider, see *Using the Micetro provider with Terraform*.

Using the Micetro provider with Terraform

menandmice_dhcp_reservation

Schema

Required

name
(String) The name of DHCP reservation you want to query.

Optional

id
(String) The ID of this resource.

Read-Only

addresses
(List of String) A list of IP addresses used for the reservation.

client_identifier
(String) The `client_identifier` of this reservation.

ddns_hostname
(String) Dynamic DNS host name for reservation.

Note: Only applicable for ISC DHCP servers.

---

description
(String) Description for the reservation.

Note: Only applicable for MS DHCP servers.

---

filename
(String) The filename DHCP option.

Note: Only applicable for ISC DHCP servers.

---

next_server
(String) The next-server ISC DHCP option.

Note: Only applicable for ISC DHCP servers.

---

reservation_method
(String) DHCP reservation method, For example: `HardwareAddress`, `ClientIdentifier`. Default: `HardwareAddress`.

servername
(String) The server-name DHCP option.

Note: Only applicable for ISC DHCP servers.

---

type
(String) The type of this DHCP reservation. For example: `DHCP`, `BOOTP`, `BOTH`.

owner_ref
(String) Internal reference to the DHCP group scope or server where this reservation is made.

ref
(String) Internal reference to this DHCP reservation.

Example

```
terraform {
  required_providers {
    menandmice = {
      # uncomment for terraform 0.13 and higher
      version = "~> 0.2",
      source  = "local/menandmice",
    }
  }
}
data menandmice_dhcp_reservation reservation1 {
   name = "reserved1"
}
```

menandmice_dhcp_scope

Schema

Required

cidr
(String) The cidr of the DHCP scope.

Optional

dhcp_server
(String) The DHCP server of this scope.

id
(String) The ID of this resource.

Read-Only

available
(Number) Number of available addresses in the address pool(s) of the scope.

description
(String) A description for the DHCP scope.

enabled
(Boolean) If this scope is enabled.

name
(String) The name of the DHCP scope you want to query.

ref
(String) Internal reference to this DHCP reservation.

superscope
(String) The name of the superscope for the DHCP scope.

Note: Only applicable for MS DHCP servers.

Example

```
terraform {
  required_providers {
    menandmice = {
      # uncomment for terraform 0.13 and higher
      version = "~> 0.2",
      source  = "local/menandmice",
      }
    }
}

data menandmice_dhcp_scope scope1{
  dhcp_server= "micetro.example.net."
  cidr = "192.168.2.0/24"
}
```

menandmice_dns_zone

Schema

Required

name
(String) Fully qualified (with the trailing dot `.`) name of DNS zone.

server
(String) Fully qualified name of the DNS server where the record is stored, ending with the trailing dot `.`.

Optional

id
(String) The ID of this resource.

view
(String) Name of the view this DNS zone is in.

Read-Only

adintegrated
(Boolean) If the DNS zone is AD integrated. Default: `False`.

authority
(String) The authoritative DNS server for this zone. Requires FQDN with the trailing dot `.`.

custom_properties
(Map of String) Map of custom properties associated with this DNS zone.

displayname
(String) A name that can distinguish the zone from other zone instances with the same name.

dnssecsigned
(Boolean) If DNS signing is enabled.

dnsviewref
(String) Internal references to views.

dnsviewrefs
(Set of String) Internal references to views.

Note: Only used with Active Directory.

---

dynamic
(Boolean) If DNS zone Dynamic, default: `False`.

kskids
(String) A comma separated string of IDs of KSKs, starting with active keys, then inactive keys in parenthesis `()`.

lastmodified
(String) Date when zone was last modified Micetro.

ref
(String) Internal references to this DNS zone.

type
(String) the DNS zone type. For example: `Primary`, `Secondary`, `Hint`, `Stub`, `Forward`.

zskids
(String) A comma separated string of IDs of ZSKs, starting with active keys, then inactive keys in parenthesis `()`.

masters
(List of String) List of all masters IP address, for secondary zones.

adpartition
(String) The Active Directory partition if the zone is AD-integrated.

adreplicationtype
(String) Replication types for an AD-integrated zone.

created
(String) Date when zone was created in Micetro.

Import

Import is supported using the following syntax:

```
# import with dnszone ref
terraform import menandmice_dns_zone.resourcename DNSZones/659

# import with readable name
terraform import menandmice_dns_zone.resourcename micetro.example.net::zone1  #<server>:
↪<view>:<dnszone name>
```

Example

```
terraform {
  required_providers {
    menandmice = {
      # uncomment for terraform 0.13 and higher
      version = "~> 0.2",
      source  = "local/menandmice",
    }
  }
}
data menandmice_dns_zone zone1 {
  name = "zone1.net."
  server = "micetro.example.net."
```

menandmice_dns_record

Schema

Required

name
(String) The name of the DNS record.

server
(String) The DNS server where this DNS record is stored.

Note: Requires FQDN, with the trailing dot `.`.

---

zone
(String) The DNS zone where the record is stored.

Note: Requires FQDN, with the trailing dot `.`.

type
(String) The DNS recod type. This can be: `A`, `AAAA`, `CNAME`, `DNAME`, `DLV`, `DNSKEY`, `DS`, `HINFO`, `LOC`, `MX`, `NAPTR`, `NS`, `NSEC3PARAM`, `PTR`, `RP`, `SOA`, `SPF`, `SRV`, `SSHFP`, `TLSA`, `TXT`. Default: `A`.

Optional

id
(String) The ID of this resource.

view
(String) The optional view where this DNS record is in. For example: `internal`.

Read-Only

ttl
(Number) The DNS record's Time To Live value in seconds, setting how long the record is allowed to be cached.

aging
(Number) The aging timestamp of dynamic records in AD integrated zones. Hours since January 1, 1601, UTC.

Note: Providing a non-zero value creates a dynamic record.

comment
(String) Comment string for this record.

Note: Only records in static DNS zones can have a comment string.

Some cloud DNS provides do not support comments.

enabled
(Boolean) If this DNS record should enabled. Default: `True`.

data
(String) The data stored in the DNS record.

dns_zone_ref
(String) Internal reference to the zone where this DNS record is stored.

ref
(String) Internal reference to this DNS record.

Example

```
terraform {
  required_providers {
    menandmice = {
      # uncomment for terraform 0.13 and higher
      version = "~> 0.2",
      source  = "local/menandmice",
    }
  }
}
data menandmice_dns_zone zone1 {
  name = "zone1.net."
  server = "micetro.example.net."
}

data menandmice_dns_record rec1 {
  name = "test"
  zone = data.menandmice_dns_zone.zone1.name  # "zone1.net."
  server = "micetro.example.net."
  type = "A"
}
```

menandmice_ipam_record

Schema

Required

address
(String) The IP address.

Optional

id
(String) The ID of this resource.

Read-Only

claimed
(Boolean) If the IP address is claimed. Default: `true`.

custom_properties
(Map of String) Map of custom properties associated with this IP address.

> **Note:** You can only assign properties that are already defined in Micetro.

device
(String) The device associated with the object.

discovery_type
(String) The discovery method of the IP address. For example: `None`, `Ping`, `ARP`, `Lease`, `Custom`.

extraneous_ptr
(Boolean) Contains `true` if there are extraneous PTR records for the record.

hold_info
(List of Object) Contains information about who holds the otherwise free IP, and for how long. (See *Nested Schema for hold_info*.)

interface
(String) The interface associated with the object.

last_discovery_date
(String) The date when the system last performed IP address discovery for this IP address.

last_known_client_identifier
(String) The last known MAC address associated with the IP address discovery information.

last_seen_date
(String) The date when the address was last seen during IP address discovery.

ptr_status
(String) PTR record status. For example: `Unknown`, `OK`, `Verify`.

ref
(String) Internal reference for the IP address.

state
(String) state of IP address. For example: `Free`, `Assigned`, `Claimed`, `Pending`, `Held`.

usage
(Number) IP address usage bitmask.

Nested Schema for `hold_info`

Read-Only:

expiry_time
(String)

username
(String)

Example

```
terraform {
  required_providers {
    menandmice = {
      # uncomment for terraform 0.13 and higher
      version = "~> 0.2",
      source  = "local/menandmice",
    }
  }
}
data menandmice_ipam_record ipam1 {
```

(continues on next page)

(continued from previous page)

```
  address = "192.168.2.2"
}
```

With the Micetro plugin for Terraform (via the `menandmice` provider), you can automate Micetro operations via Terraform.

1.19 Admin Guide

This guide will walk administrators through managing Micetro by Men&Mice, covering user, service, and system configurations.

You will learn how to effectively manage user accounts, covering tasks such as adding, modifying, and deleting users while also assigning them specific roles and permissions to align with your organization's requirements.

Moreover, the guide will explain how to configure services and you'll gain insights into optimizing your network setup to achieve the highest levels of efficiency and protection.

Additionally, we'll explore the integration of Micetro with Active Directory, allowing you to sync and centralize user data, and configure DNS server settings to ensure seamless communication and resource accessibility.

1.19.1 License Management

The different functionalities of Micetro can be activated by specific license keys.

There are five different keys, one each for:

- DNS
- IPAM

> **Note:** The IPAM license key unlocks **both** the DHCP and IPAM functionality of Micetro.

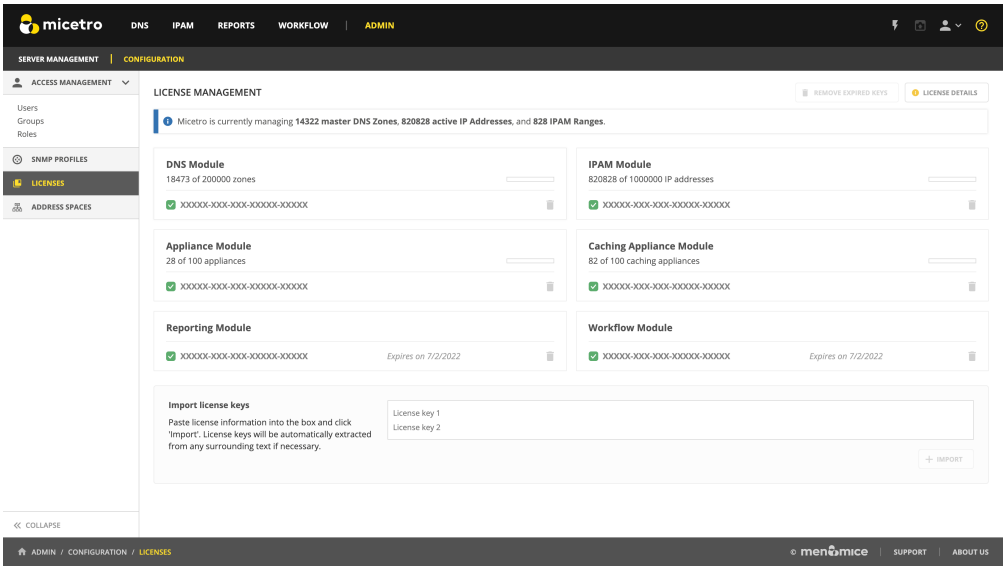
- Men&Mice Virtual Appliances
- Workflow module
- Reporting module

Viewing license keys

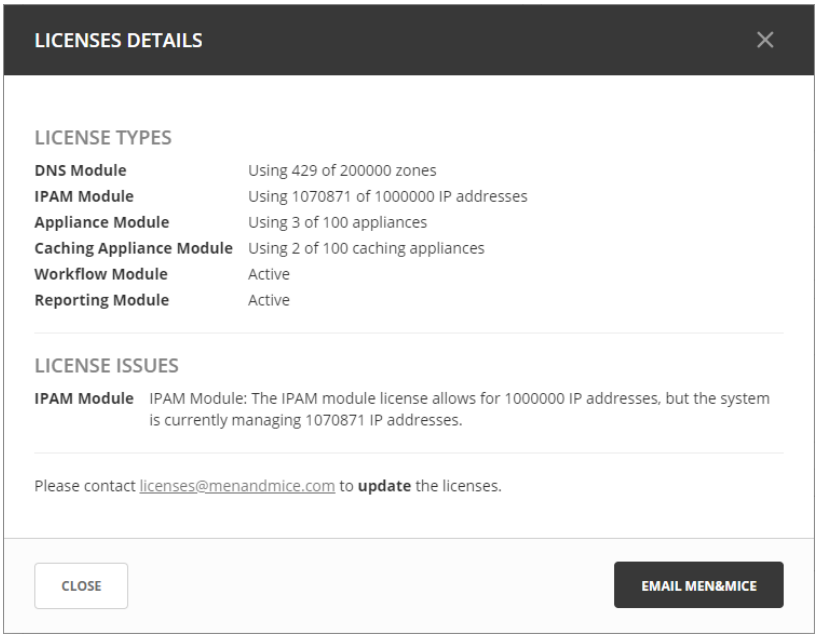
Go to *Admin* → *Configuration* → *Licenses* to see information about the licenses that are currently active on your system. Each active module has a card that shows its associated license keys. These license keys can be either active or expired.

The card also displays how much of the license you have used, for example, the number of DNS zones you have used compared to the limit of the license. This information is shown in a usage bar that is located in the upper right-hand corner of the card.

In addition to this, the card also shows the expiry date for the currently active license key. This information is located in the bottom right-hand corner of the card.



By selecting *License Details*, you can quickly and easily see how much of your licenses are currently being used, as well as any issues related to your licenses.



Expired keys

A notification will be shown when a license key is expired and when a license key is about to expire. This will only be shown to members in the administrators group.

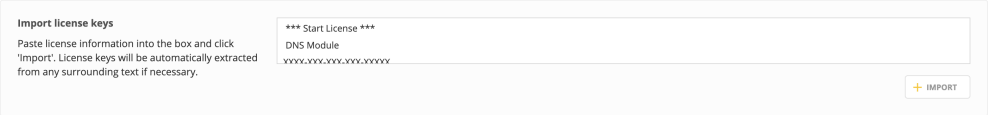
Adding a License Key

Adding license keys for the first time

When logging into a system that has no active licenses, the system will prompt the user and indicate that not active license keys are in the system and offer the user to enter new license keys through the license management page. Additional keys can be added by pasting text containing valid license keys to the textbox at the bottom of the license management page.

1. Navigate to *Admin* → *Configuration* → *Licenses*.
2. To add new key(s), scroll down to the "Import license keys" section and paste in the license key(s).

Tip: You can paste in the email you received from Men&Mice, Micetro will parse the keys from the surrounding text automatically.



3. Click +*Import*.

Removing a License Key

A license key can be removed by clicking on the trashcan icon on the the right.

A confirmation dialog will display, click *Yes* to confirm.

Removing expired license keys

Old, expired license keys can be cleaned up and removed using the *Remove expired keys* action.

Export license data

Active license keys and usage data can be exported from Micetro using the *Export license data* action. This will compile the active keys and usage information into a single text block that can be copied.

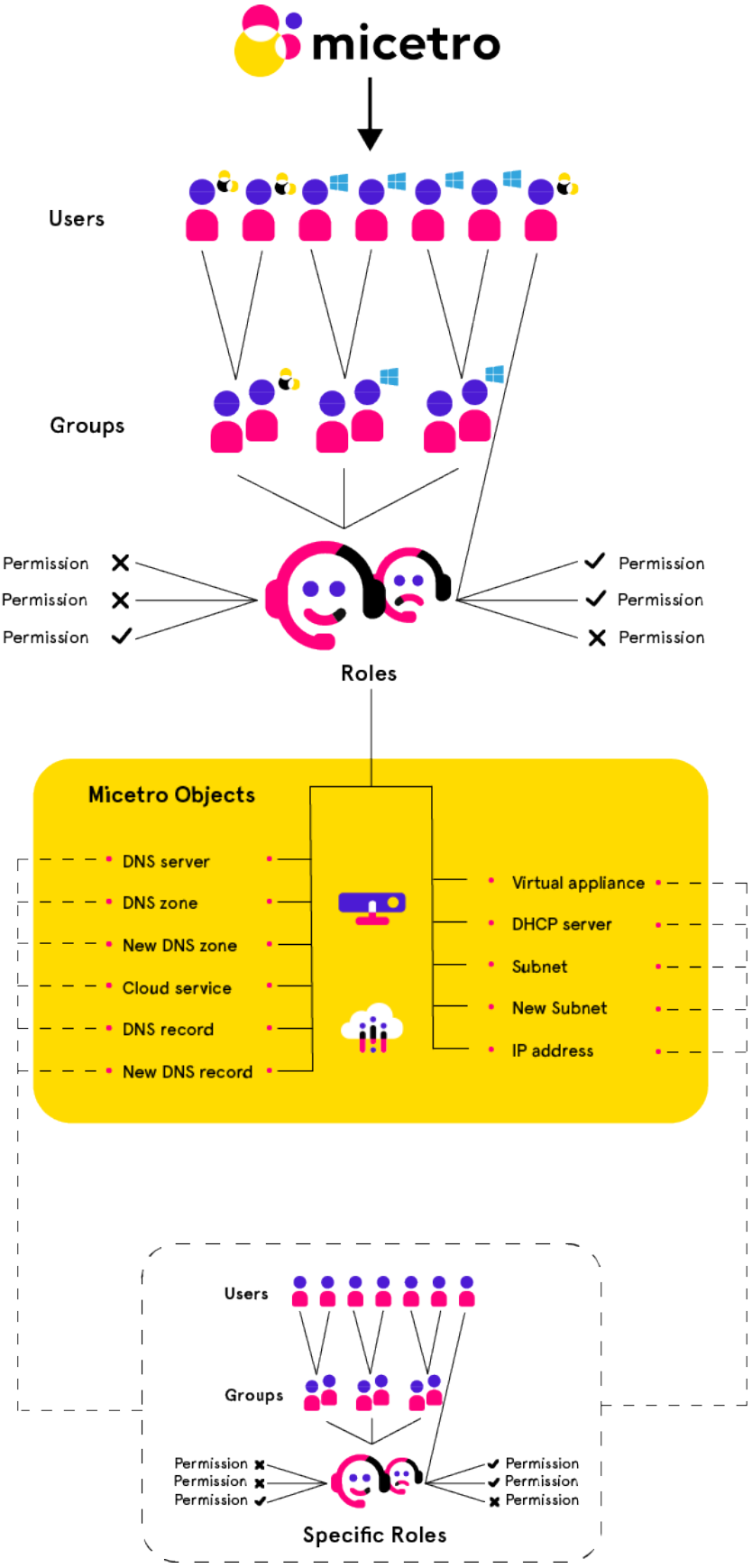
1.19.2 Access Management

Important: Micetro 10.1 (released in September 2021) brought changes to the access management in order to make it more streamlined and easier to use, while keeping the flexibility. This page describes the new access control. If you're using an older version, or would like information on the legacy access control model, see access-control-legacy.

Overview

Access control in Micetro is **role-based**.

Objects (servers, zones, scopes, IP addresses, etc.) in Micetro are accessed through *Roles* configured with *Permissions*. *Users* and *Groups* do not have direct access to objects, only if they're **assigned to roles**. Administrators can control a user or group's access by assigning or removing them from roles.


micetro
Users
Groups
Permission
Permission
Permission
Permission
Permission
Permission
Roles
Micetro Objects
DNS server
DNS zone
New DNS zone
Cloud service
DNS record
New DNS record
Virtual appliance
DHCP server
Subnet
New Subnet
IP address
Users
Groups
Permission
Permission
Permission
Permission
Permission
Permission
Specific Roles

A set of *Built-in roles* are available that should cover most use cases. These are *General roles*, applied to all objects (present and future) in Micetro. *Specific roles* exist for use cases where per-object permissions are required.

Groups, Users, and Roles

The relationship between *Groups*, *Users*, and *Roles* is as follows:

- Users and groups can be assigned to roles.
- Groups can contain users.
- Groups *cannot* contain groups.
- Users from externally managed groups, such as Active Directory, cannot be added to local groups.
- Users and groups can be assigned to any number of roles.

The `administrator` user

The built-in, local `administrator` user exists outside of regular access controls. All permissions are enabled for this user (even if not attached to any role) and its permissions cannot be edited or overriden (see *Block permission*) by any role.

The password for the `administrator` user is configured during the first-run-wizard.

The `administrator` user cannot be removed from Micetro, and is always local (cannot be authenticated by SSO).

New objects

When a user imports or creates a new object (such as DNS zone, record, DHCP scope, IPAM range, etc.) in Micetro, the object is configured for a certain default access based on the permissions for the object type. General roles configured with permissions for the object type will have automatic access to the object.

Access Control Management

Because Micetro's access controls are role-based, permissions are configured *on the role*, and propagated to any user or group attached to the role.

To grant restricted access on a per-object basis, see *Specific roles*.

To check access to a specific object and troubleshoot access control issues, see *Effective access*.

Permissions

Permissions are **access flags**, configured on roles and pertaining to types of objects.

Permissions determine what type of objects the role has access to, and what kind of access it has to them.

For a full list of available permissions see *Permissions reference*.

Setting permissions

Note: Permissions for built-in-roles cannot be modified.

1. Navigate to *Admin* → *Configuration* → *Roles* in the web application.
2. Select the role you want to edit, and double click it. (Or use the *Edit role properties* action from the top bar or ellipsis menu.)

   Note: Permissions can only be edited on individual roles.

3. Switch to the *Access* tab.
4. Edit the permissions as needed.
5. Click *Save*.

Note: When setting access on a role, adding a permission will automatically enable all dependent permissions as well to prevent access problems.

An information button will appear on the top right of the dialog box, providing a summary of dependent permissions enables if hovered over.

Turning off the permission(s) will **not** disable the automatically enabled dependent permissions. Turning off the dependent permission(s) will still allow the role to be saved.

Block permission

When a permission is enabled, it'll set the access flag to `allow`. When you **block** a permission on a role, it is set as `deny` and *prevent any other role* to overwrite that permission.

Example: The role *Worfklow Blocked* has the "Access to Workflow module" permission blocked. The built-in role "DNS approvers" has this permission enabled. Attaching user `janedoe` to both roles will result in the user **not** being able to access the Workflow module. Even though the *DNS approvers* role would allow it, the permission block set in *Workflow Blocked* will prevent it to take effect.

Note: Permissions that are not set are simply returned as "null." These empty access flags are **not** equivalent to 'deny' and **can** be overwritten by access flags configured in other roles.

Roles

Through roles you can manage access control in Micetro.

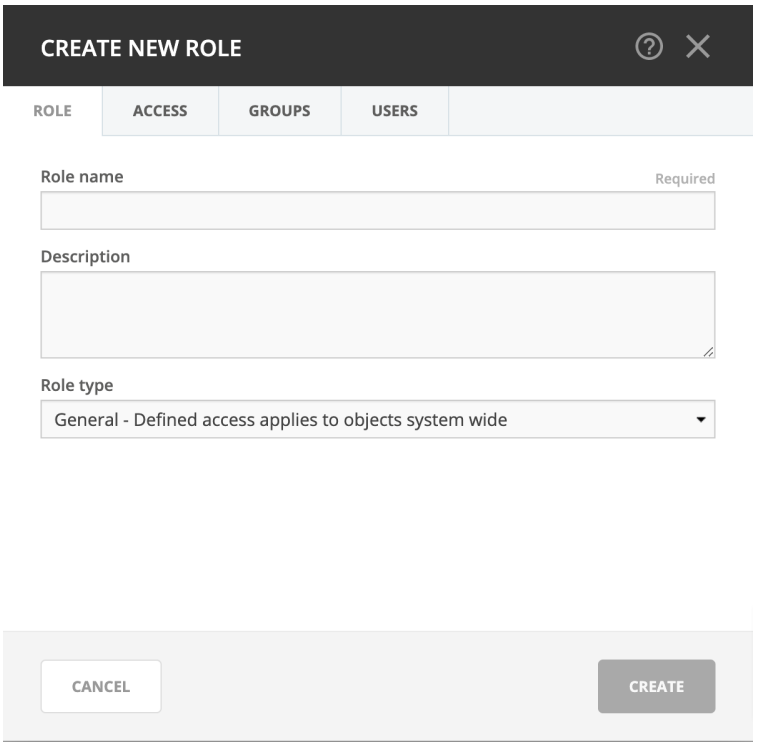
Objects (servers, zones, scopes, IP addresses, etc.) in Micetro are accessed through *Roles* configured with *Permissions*. *Users* and *Groups* do not have direct access to objects, only if they're **assigned to roles**. Administrators can control a user or group's access by assigning or removing them from roles.

Note: This page is for generic management of roles. See *General roles*, *Specific roles*, and *Legacy roles* for the particularities of the different role types.

Adding a new role

Through this function, you add new roles to Micetro.

1. Navigate to *Admin* → *Configuration* and select *Roles* in the filtering sidebar. The built-in roles are displayed here, as well as all other roles that have been added to Micetro already.
2. Click the *Create* button. The *Create role* dialog box displays.



Role name
Give the new role a name.

Description
Brief description for the role.

> **Tip:** Using clear and descriptive names and descriptions makes access management easier.

3. Switch over to the *Access* tab and set the permissions. (See *Permissions*.)
4. When all necessary information and permissions are configured, click *Save*.

Note: The default for new roles is *General roles*.

Tip: See *Example role configuration: DHCP read-only* for an example process for creating a role anew.

Editing a role

Through this function, you can edit the role's name, description, permissions, and attached users/groups.

1. Navigate to *Admin* → *Configuration* and select *Roles* in the filtering sidebar.
2. To select a single role, click on the role's name. To select multiple roles, press/hold the Ctrl (Cmd on Mac) key and then click on each role's name.
3. From the ellipsis menu, select *Edit role properties* or use *Actions* → *Edit role properties*.
4. Make the desired changes to the role's information. In the *Users* and *Groups* tabs you can remove users/groups from the role.
5. Click *Save* to save the changes.

Deleting a role

Through this function, you remove a role from Micetro.

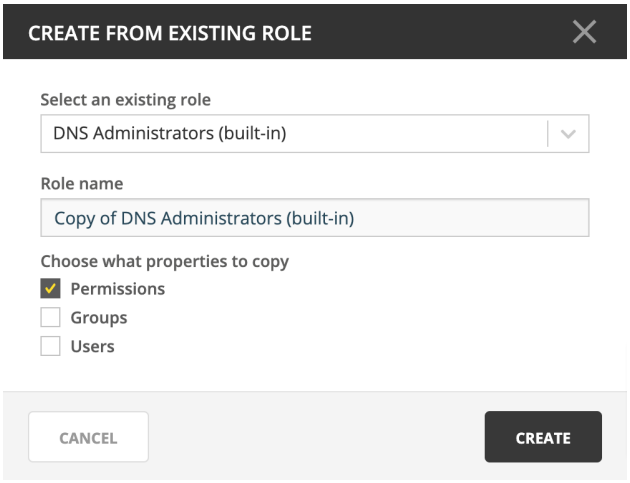
Note: Built-in roles cannot be removed.

1. Navigate to *Admin* → *Configuration* and select *Roles* in the filtering sidebar.
2. To remove a single role, click on the role's name. To remove multiple roles, press/hold the Ctrl (Cmd on Mac) key and then click on each role's name.
3. From the ellipsis menu, select *Remove role* or use *Actions* → *Remove role*.
4. To remove the role, click the *Yes* button. The role is removed.

Duplicating a role

It is possible to duplicate roles and copy the original's configured permissions, users, and groups to a new role.

1. Navigate to *Admin* → *Configuration* → *Roles* in the web application.
2. Use the + *Create* –> *From existing role* action from the top bar.



3. Select the role to duplicate, and name the new role.
4. Select which properties (permissions, groups, roles) to copy.
5. Click Create.

Tip: See *Example role configuration: DNS zone read-write* for an example process for creating a role from an existing template.

General roles

*General roles** are the default role type, whose permissions are automatically applied (if applicable) to all objects in Micetro, present and future.

To create a *General role*, follow the instructions on *Roles*, and **select** the *General* type from the dropdown in the role creation dialog. (The default type is *General*.)

Example: The general role *DNS editor* has the `Edit zone options` permission enabled. Any 'DNS zone' type object in Micetro, whether already existing or added in the future, will be accessible to users/groups attached to this role.

Built-in roles

Micetro has seven built-in general roles that will likely cover most use cases for access control.

The built-in roles are the following:

Administrators
: Full access to all objects

DNS Administrators
: Full access to DNS objects, including zones, DNS servers, etc.

DHCP Administrators
: Full access to DHCP objects, including scopes, DHCP servers, etc.

IPAM Administrators
: Full access to IPAM objects, including IPAM ranges, etc.

User Administrators
: Full access to User and Group objects.

DNS viewers
Can view DNS objects and information, but not make changes.

IPAM viewers
Can view IPAM and DHCP objects and information, but not make changes.

Requesters
Able to make and queue DNS change requests. (See *Workflow Management*.)

Approvers
Able to see and approve/deny submitted DNS change requests. (See *Workflow Management*.)

Note: Built-in roles cannot be deleted.

Permissions for built-in roles cannot be modified.

Note: General roles can be restricted from accessing single objects. See *Object access*.

Specific roles

Specific roles are a role type whose permissions are **not** automatically applied to objects in Micetro. They're intended to allow managing access on a per-object basis.

To create a *Specific role*, follow the instructions on *Roles*, and **uncheck** the *General* checkbox in the role creation dialog. (The default value is checked.)

Example: The specific role *example.com editor* has the `Edit zone options` permission enabled. No 'DNS zone' type object in Micetro, whether already existing or added in the future, will be accessible to users/groups attached to this role **unless specifically added** to the object.

> **Warning:** Specific roles are only intended for edge use cases, and should not be regarded as the preferred method of access control in Micetro.

Using specific roles

Access defined through specific roles isn't applied until explicitly configured on objects.

To use a *Specific role* and control access to an object:

1. Open the context (DNS or IPAM) and select the object to which you'd like to restrict access.

Note: Using specific roles on an object is only possible individually, per object.

---

2. Use the *Access* action from the top bar or the ellipsis menu.
3. On the top of the dialog, remove all unneeded *General roles* and/or users (legacy only) configured.
3. On the bottom of the dialog, search for the *Specific role* and click + *Add*.
4. Click *Save*.

This will restrict access to that particular object to the selected users/groups assigned to the *Specific role*.

Note: Situations may arise that adding a specific role to an object would not take effect because of missing permissions on parent objects. Micetro will calculate the necessary permissions needed, and can automatically add them to the relevant objects.

A notification will display on the *Save comment* dialog, detailing the additional changes. If the user doesn't have the necessary access to set permissions of these objects, an advisory will display.

Note: General roles can be restricted from accessing single objects. See *Object access*.

Legacy roles

Legacy roles were created to maintain backwards compatibility with older Micetro versions and facilitate migration to the new access management model.

Roles (and certain groups and users) in existing Micetro installations (before 10.1) are automatically converted to a legacy role during updating Micetro to 10.1 or later. They will be configured with the same permissions as before.

Legacy roles are treated as *Specific roles*, in that all *existing* objects will have their respective legacy roles associated with them, but *no newly added objects will be automatically assigned to* a legacy role.

After familiarizing yourself with the new access model, you can convert legacy roles to either a *General roles* or *Specific roles*.

Note: Permissions for legacy roles **can** be edited.

Legacy roles **can** be removed from Micetro.

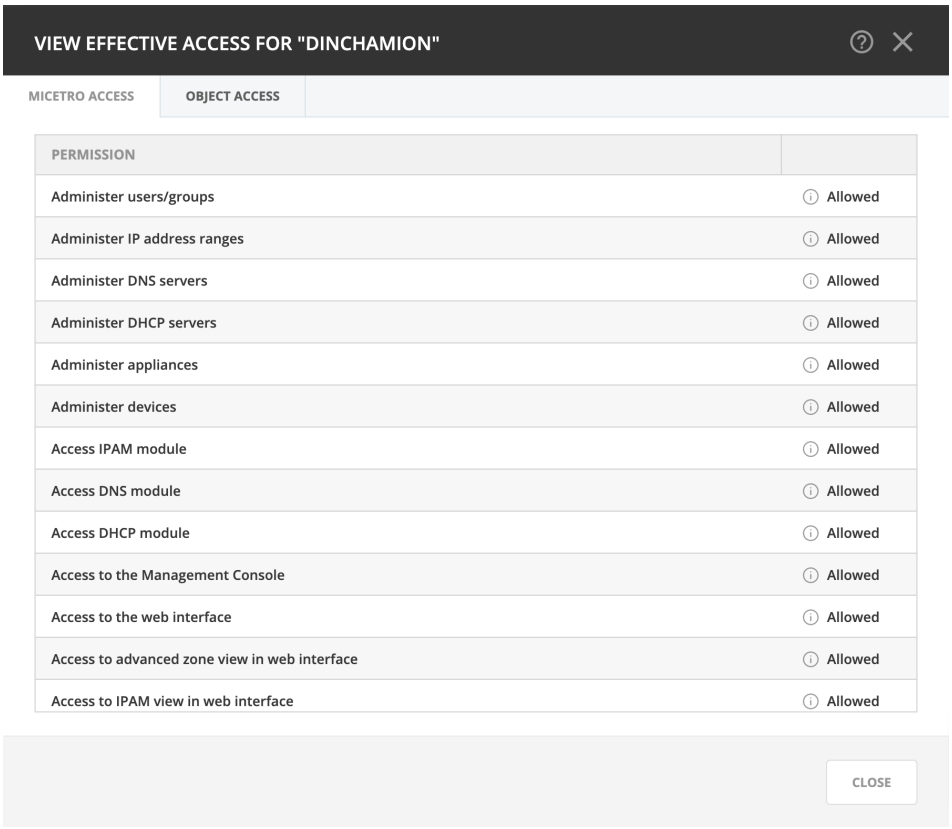
Effective access

The *Effective access* dialog is useful for checking access for a user/group, and to troubleshoot access control problems.

Administrator with access to managing users/groups in Micetro can check the effective access of a user or group based on the role(s) the user/group is assigned to.

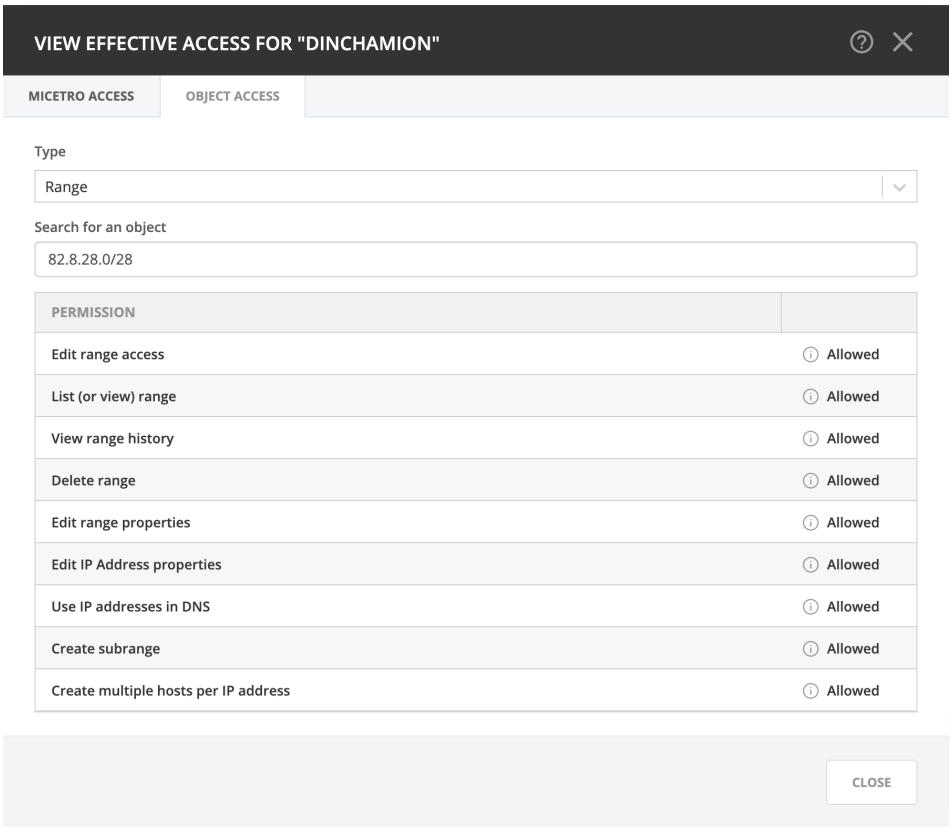
1. Navigate to *Admin* → *Configuration*.
2. Select *Users* or *Groups*, depending on whose access you want to check.
3. Select the user/group in the grid, and use the *Effective access* action from the top bar or the ellipsis menu.

Micetro access
: It shows all *enabled* permissions for the user/group.



Object access

Here you can select an object type and search for a specific object to check the access the selected user/group has, as well as where the access comes from.



Note: The *Effective access* dialog box will display detailed warnings if permissions to the selected object are set, but a parent permission is not.

Example: examining effective access on a DNS zone might reveal that the user is attached to a role that has permission to view DNS zones, but no permission to use the DNS module.

Tip: By hovering over the *i* icon in the permissions list, the role(s) where the permission was set is displayed.

Users

Users represent the individual people working with Micetro.

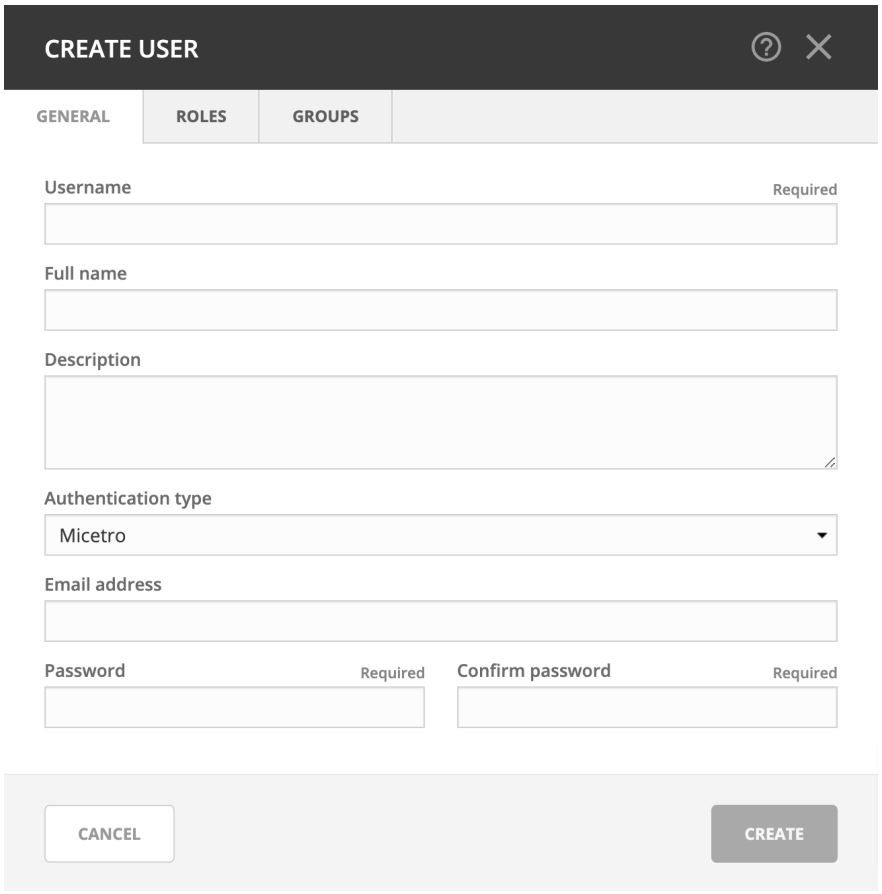
Note: To manage users, you must be logged in as a user who has user management privileges. (Is attached to a role with the `access_adminUser`/"*Administer users/groups/roles*" permission enabled.)

Note: At least one user, the `administrator`, is always configured for Micetro. See *The administrator user*.

Adding User Accounts

Through this function, you add new users who can then be assigned to groups.

1. Navigate to *Admin* → *Configuration* and select *Users* in the filtering sidebar. The default administrator account displays here, as well as any other users you have already added.
2. Click the *Create* button. The *Create user* dialog box displays.



- **Name**
  Type the **username** that you want to as assign to this person.

> **Warning:** Once you have created the user name, it is not possible to change it.

- **Full Name and Description**
  (Optional) Type the user's first and last name and a description of their duties (i.e., job title, department, etc.), respectively.
- **Authentication type**
  Click the drop-down list and specify whether the user's login will be authenticated by Micetro or by an external authentication service (such as existing Active Directory account on the network). See *External Authentication*.
- **Email address**
  The user's email address. Used for sending notifications such as scheduled reports, subnet monitoring updates, etc. Disabled with external authentication.

- **Password/Confirm Password**
  If the **Authentication type** selected is *Men&Mice internal*, you need to provide a password for the user in the Password field. Passwords must be at least four characters in length and no longer than 20 characters. Passwords must be at least 4-characters long and can contain any combination of letters, numbers, and special characters, including spaces. In the Confirm Password field, re-enter the password exactly as you did in the Password field above. Disabled with external authentication.
- On the *Groups* and *Roles* tabs, select the user group(s) and role(s) to which you want to assign this user. Each user can be assigned to none or to multiple groups and roles.

Note: If you have not created your groups, you can always come back and edit the user accounts anytime and change the group assignments.

---

3. When all selections/entries are made, click *Create*. The new user is added to the *Users* list and can now use Micetro.

Editing User Accounts

1. Navigate to *Admin* → *Configuration*, and select *Users* in the filtering sidebar.
2. To select a single user, click on the user's name. To select multiple users, press/hold the Ctrl (Cmd on Mac) key and then click on each user name.
3. From the ellipsis menu, select *Edit user properties* or use *Actions* → *Edit user properties*.
4. Make the desired changes to the user's information.
5. Click *Save* to save the changes.

Removing User Accounts

1. Navigate to *Admin* → *Configuration*, and select *Users* in the filtering sidebar.
2. To remove a single user, click on the user's name. To remove multiple users, press/hold the Ctrl (Cmd on Mac) key and then click on each user name.
3. From the ellipsis menu, select *Remove user* or use *Actions* → *Remove user*.
4. To remove the user, click the *Yes* button. The user is removed.

User Inspector

Selecting a user displays a list of information in the Inspector, including the user name, authentication type, roles, etc. Only users with user administrative privileges can see this information.

Groups

Groups allow you to manage multiple individual users, based on needs for the same access across the system.

Adding a New Group

1. Navigate to *Admin* → *Configuration* and select *Groups* in the filtering sidebar. The default groups are displayed here, as well as any other groups you have already created.
2. Click the *Add* button and select whether to add an external (authenticated and managed through an external source such as Active Directory or LDAP) or create a local group (authenticated and managed through Micetro only).

For **local group** the following dialog box displays:

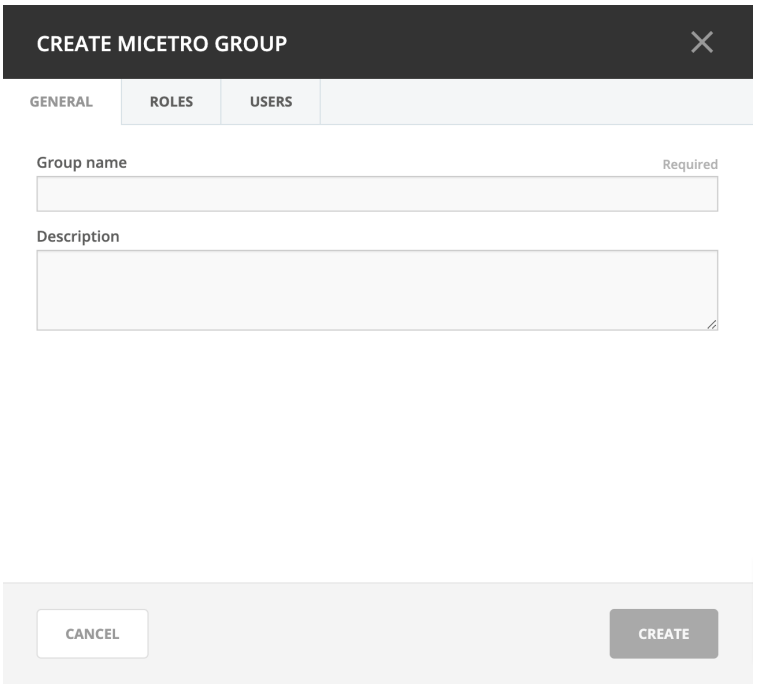
Group name
The name for the group you are creating.

Description field
(Optional) Some information that describes the function of this group.

AD Integrated
Check this box to define this group as an Active Directory Integrated group. When checked this group name will be matched against groups defined in Active Directory. For more information how on this works refer to External Authentication.

Roles
Any roles that members of this group will automatically assume.

Users
Any users that you want to add to this group. (Users can be added/removed at any time.)



3. When all selections/entries are made, click *Save*.

Editing a Group

Through this function, you can edit the group name and/or description, and indicate whether this group is Active Directory integrated.

1. Navigate to *Admin* → *Configuration* and select *Groups* in the filtering sidebar.
2. To select a single group, click on the group's name. To select multiple groups, press/hold the Ctrl (Cmd on Mac) key and then click on each group's name.
3. From the ellipsis menu, select *Edit group properties* or use *Actions* → *Edit group properties*.
4. Make the desired changes to the group's information. In the *Users* tab you can remove users from the group.
5. Click *Save* to save the changes.

Deleting a Group

Through this function, you delete a group.

1. Navigate to *Admin* → *Configuration* and select *Groups* in the filtering sidebar.
2. To remove a single group, click on the group's name. To remove multiple groups, press/hold the Ctrl (Cmd on Mac) key and then click on each group's name.
3. From the ellipsis menu, select *Remove user* or use *Actions* → *Remove user*.
4. To remove the group, click the *Yes* button. The group is removed.

External groups (Active Directory, LDAP)

For external groups, such as those managed in Active Directory, use the *Add –> AD Group* or *Add –> LDAP group*. The **group name** field must match the name in the external authentication. See *External Authentication*.

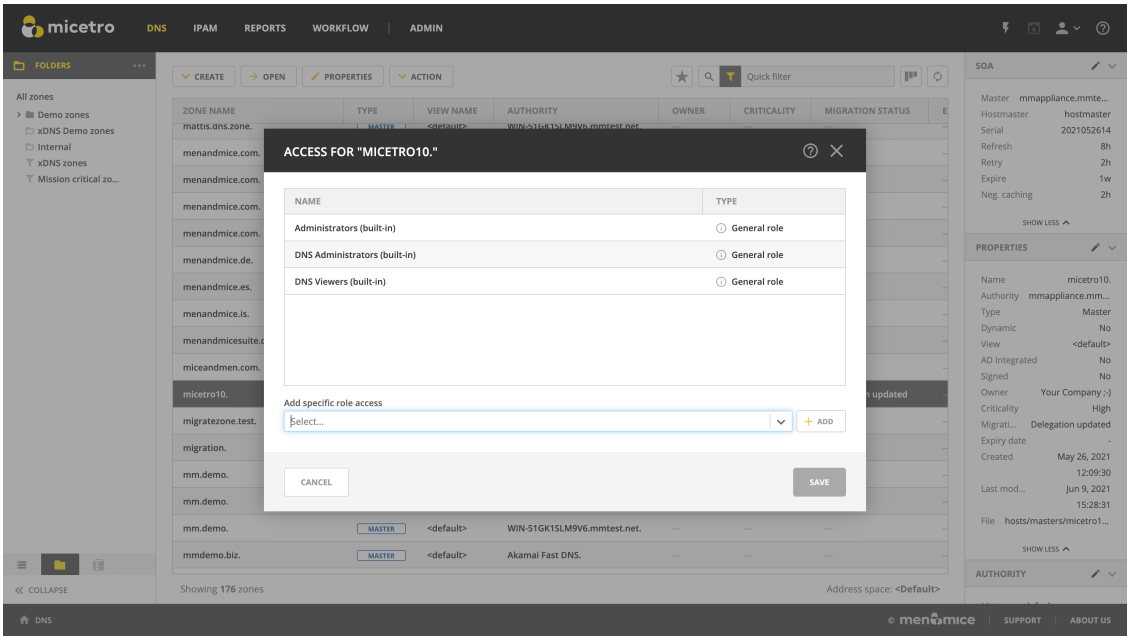
Note: External groups do not have a *Users* tab when adding the group to Micetro.

After the external group is added to Micetro, it will not contain users. Users are only added to the external group after their first login.

For more information, see *AD Sites and Subnets* and *External Authentication*.

Object access

Single objects in the DNS, IPAM, and Admin contexts can be selected to examine and adjust access with the *Action –> Access* task from the top bar or the ellipsis menu.

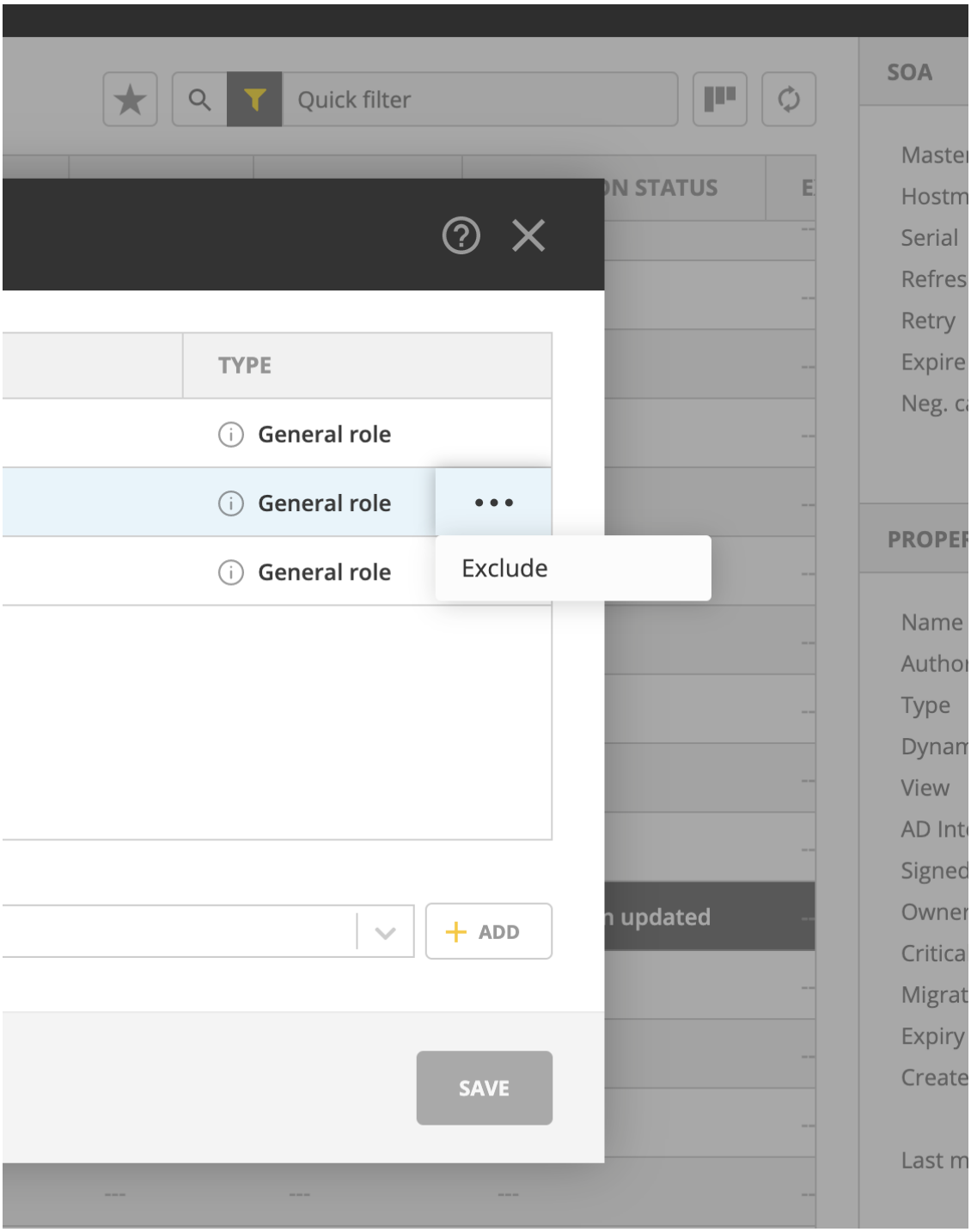


Here you can add *Specific roles* to the object using the dropdown menu.

Note: Only specific roles that have the necessary access enabled are shown in the list.

Exclude roles from object access

If needed, *General roles* can be excluded from access to the single object.



The excluded role will still be shown in the list, but greyed out and struck through.

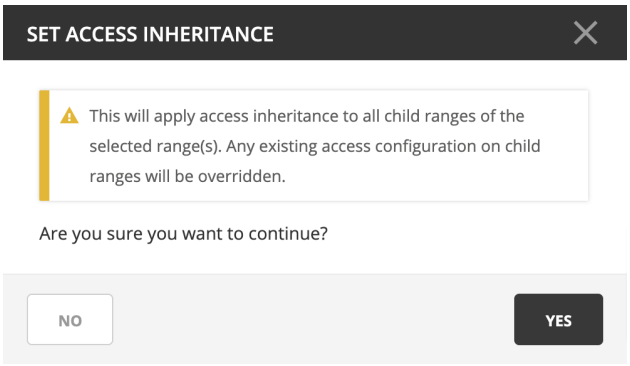
Note: Specific roles cannot be excluded, as they're set on single objects. The 'exclude role' function is available to manage (restrict) object access on a case-by-case basis for general roles.

Access inheritance

Note: Access inheritance is enabled for all applicable IPAM objects by default. You can change this in *System Settings* in the Management Console.

For containers, scopes, and ranges in the IPAM context, users with IPAM administration permissions can configure access inheritance. Access for objects set to inherit access from their parent cannot be edited. Editing access on the parent object will be applied to all child objects.

If disabled, it can be enabled by using the *Action –> Set access inheritance* action from the top bar or ellipsis menu. This will enable access inheritance to all *existing and new* child objects.



Using the *Action –> Access* action from the top bar or ellipsis menu allows you to disable or enable access inheritance by checking the **Inherit access from parent range** checkbox.

Important: Existing access settings are **not** modified by *disabling* inheritance, but **it is overwritten** when *enabling* it.

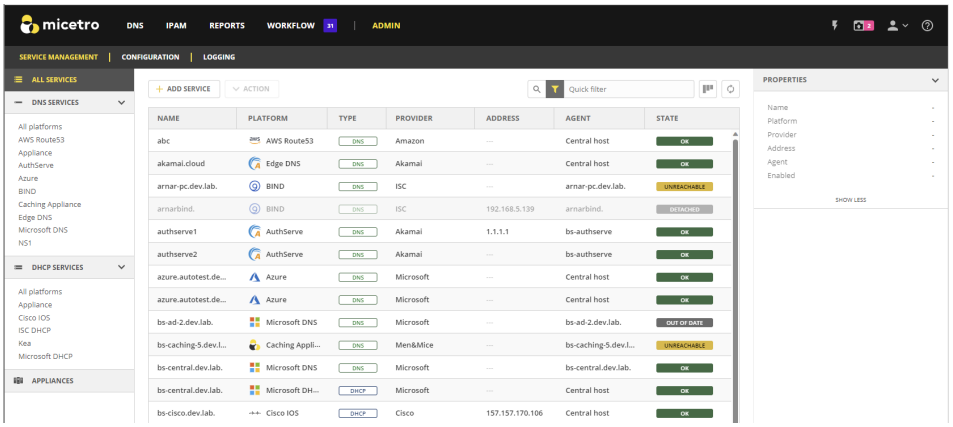
Note: Access inheritance honors *all* roles added to the parent object, including legacy and specific roles. Adding a specific role to a parent object will apply the change to all child objects that have access inheritance enabled.

1.19.3 Service Management

Service Management is the place for connecting and orchestrating DNS, DHCP, and IP Address Management (IPAM) services with Micetro. Your services can be hosted on-premises, deployed on specialized appliances, or reside in the cloud. Connected services are displayed on the **Service Management** tab on the Admin page.

To access Service Management:

1. Select *Admin* on the top navigation bar.
2. Click the *Service Management* tab in the upper-left corner.



- By default, all services configured in the system are shown.
- In the left pane, you can filter the list by type of service or provider.
- In the right pane, the properties of a selected service are shown.

Note: The Micetro web interface does not yet provide full management of IPAM services. Therefore they are not listed here, but you can still enable IPAM services by using the *Add service* function.

User Permissions and Access Management

Depending on user permissions and available license keys, DNS and DHCP services and functions can be disabled or hidden.

Micetro has a granular role-based *Access Management* system. For DNS and DHCP administrators, it is recommended to be members of the built-in **DNS Administrators** and/or **IPAM Administrators** roles. To manage Appliances, it is recommended to be a member of the built-in **Administrators** role.

When not using the built-in roles, users need to be members of a role with the following permissions. Note that additional permissions might be necessary for comprehensive service management. For more information on Micetro's granular role-based access controls, see *Access Management*.

- To manage DNS services: **Administer DNS servers**
- To manage DHCP services: **Administer DHCP servers**
- To manage cloud services: **Access to manage clouds**

- To manage appliance services: **Administer appliances**

Supported Platforms

Micetro supports the following DNS and DHCP platforms:

- DNS
  - AuthServe
  - AWS Route 53 (cloud)
  - Azure DNS (cloud)
  - BIND
  - DynDNS (cloud), (Note DynDNS is EOL May 31st 2023)
  - Edge DNS (cloud)
  - Microsoft DNS
  - NS1 (cloud)
  - Unbound (deprecated, new services cannot be added)
  - BlueCat DNS and DHCP server (BDDS) Appliance
  - Men&Mice Appliance
  - Men&Mice caching Appliance
- DHCP
  - Microsoft DHCP
  - Kea
  - ISC DHCP
  - Cisco IOS
  - BlueCat DNS and DHCP server (BDDS) Appliance
  - Men&Mice Appliance

Micetro Agents

To handle communication between Micetro and the external service, an agent is needed. Depending on the type of service and if it's on-premises or cloud, the agent is either installed on the respective machine, on the machine running Men&Mice central or in some cases, on any machine that is in the same domain as the DNS/DHCP servers. A single agent can handle communication with multiple servers. For more information on agents and how to install them, see *Micetro Agents*.

Note: When managing Microsoft DNS servers on remote computers with the DNS Server Controller, some actions for static zones may not be available:

- Disable resource record
- Enable resource record
- View and edit record comments
- Disable zone

To perform these actions, you need to install the DNS Agent on the server and use that connection when adding the server.

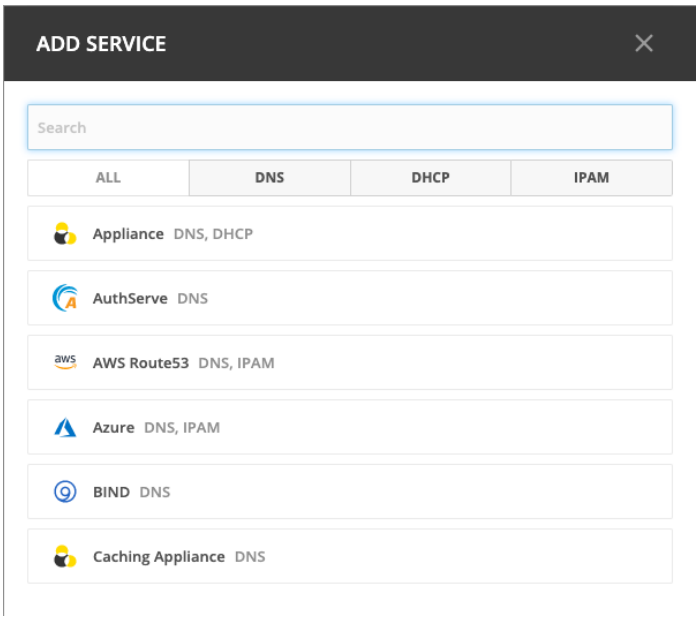
Adding a Service

You must have permission to administer DNS to add a new service to Micetro.

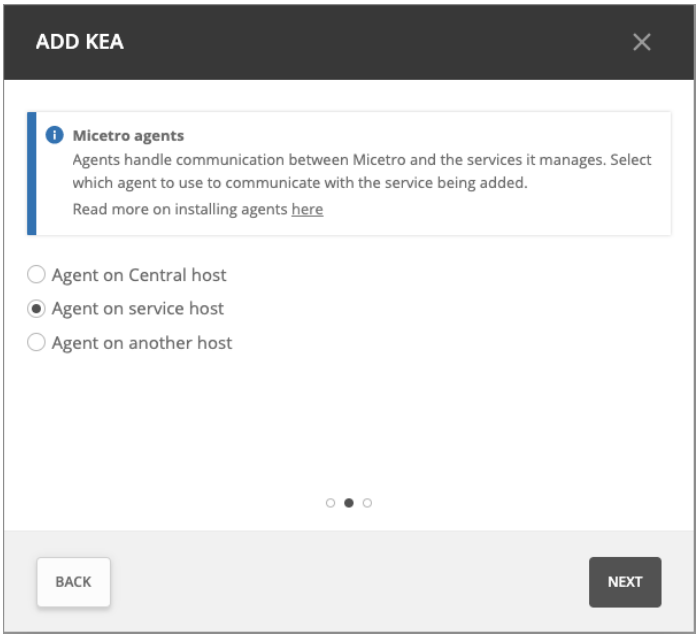
Adding a new service is either a two or three-step process, depending on the type of service being added.

To add a service:

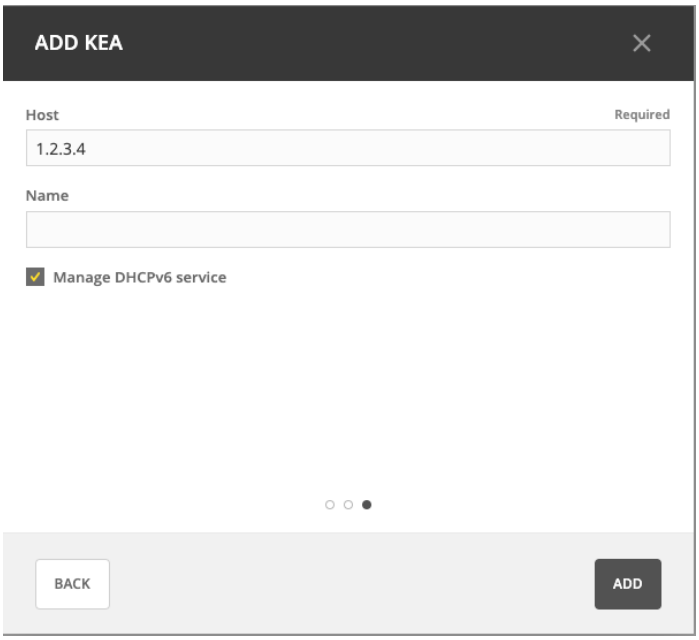
1. On the *Service Management* tab, click *Add Service*. The Add Service wizard opens.



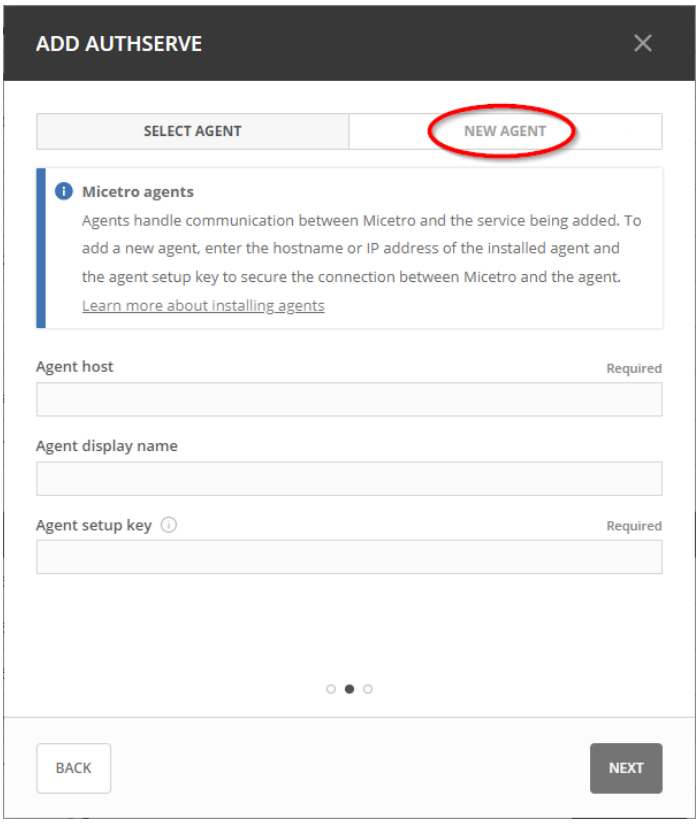
2. Choose the platform you want to use. You'll see a list of options to choose from, based on your license keys. You can use the **DNS**, **DHCP**, and **IPAM** filters at the top to narrow down the list. You can also use the search box to search for the right service.
3. Select an agent:



- This step is skipped for cloud services.
- For ISC BIND and ISC DHCP this step is skipped, as the agent must be installed on the service host.
- With the exception of the service types mentioned above, the agent can be installed on the Micetro Central host, on the Service host, or in the case of MS DNS/DHCP, ISC Kea, and Cisco IOS on a different host. If you have already added a service of this type before, you have the opportunity to either select from existing agents or create a new agent. A single agent can be used to manage multiple connections.



- In the case of **AuthServe**, you can select from a list of available agents that were registered in the installation process.
- For AuthServe git you can also register a new agent on the *New Agent* tab. Enter a hostname for the agent and, optionally, the IP address. If the hostname is not resolvable, an IP address is needed here.



4. Add service:

- Cloud services: Each service type has its set of credentials in addition to the optional service name.
- On-premises services
  - Provide the hostname or IP address of the service/server.
  - AuthServe uses channel as the connection string. Channel name is mapped to a host name in a configuration file on the server. 'ansp' is the default channel name that maps to localhost. To select a different host name the syntax is `"1.2.3.4#<someseceret>"`. Refer to AuthServe documentation for details.

Editing Services

Depending on the service, you can change the name and/or custom properties for the service. For example, if you need to refer to the service by another name or if you are connecting to the service by an IP Address and the IP Address has changed.

To edit a service:

1. Locate the service you want to edit.
2. Select the service, and then select *Edit service* on the *Action* menu. You can also double-click the service.
3. Make the necessary changes. Click *Confirm* to save the changes.

Other Service Actions

Depending on the service, you can modify both the service name and its custom properties. Any actions applicable to a selected server can either be accessed on the *Actions* menu located above the list, or by clicking the row menu ... button that appears when you hover over the right-hand side of a row.

Action	Description
Attach service	Attaches a previously detached server/service.
Detach server	Detaches or disables the server/service. When a server is detached, it is not synchronized with Micetro and is excluded from various checks. When a server is detached, it is greyed out in the service view grid. The server can be attached again for it to be part of the server synchronization again.
Synchronize	Triggers synchronization of zones and records or scopes.
Remove service	Removes the selected server/service from Micetro. This option is only available with the Administrator account.
Access	Shows which roles have access to the service and what actions they are authorized to perform. For more information about how to manage object access, see *Object access*.
View history	Allows you to view history for the selected server/service.

Service States

The list of services shows an indicator of the state of the individual services configured in the system.

The indicators can refer to either the Server Controller (see *Micetro Agents*) running on the DNS/DHCP server, or the DNS/DHCP server service itself.

Use the following table for more information on the indicators:

Indicator	Component	Explanation
Unknown	Controller	The status of the DNS/DHCP Server Controller is unknown.
OK	Server, Controller	The DNS/DHCP Server Controller and service are both OK.
Unreachable	Controller	The DNS/DHCP Server Controller is offline or otherwise unreachable.
Out of date	Controller	The DNS/DHCP Server Controller has a different version than Central.
Updating	Controller	The DNS/DHCP Server Controller is being updated.
Uninitialized	Server	The DNS/DHCP server is uninitialized and needs to be manually initialized.
Detached	Server	The DNS/DHCP server has been detached without removing it from Micetro.
Service Down	Server	The DNS/DHCP server is down and not responding to queries.
Service Impaired	Server	The DNS/DHCP server is running but impaired.[1]

Editing the Raw Configuration on BIND Servers

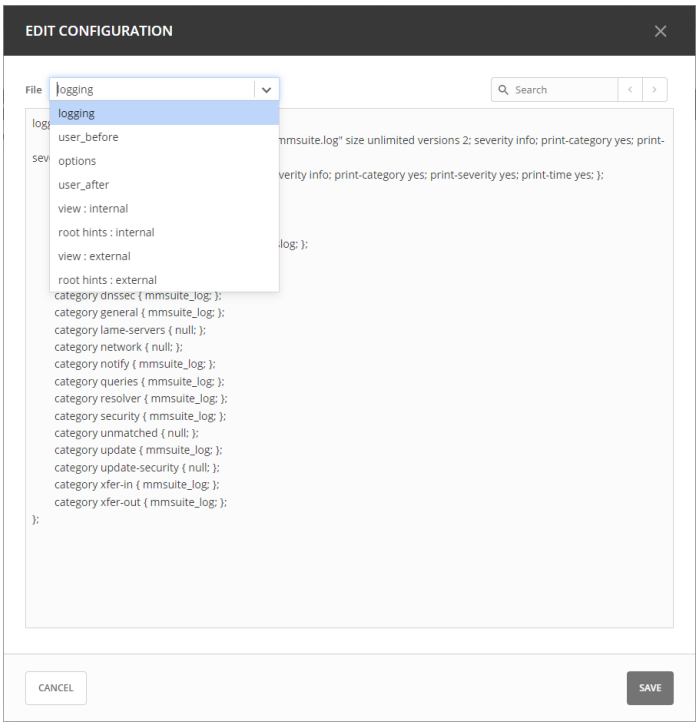
For BIND servers, DNS Administrators can access and modify their raw configuration files directly. This is particularly useful for making changes to the server and zone options that are not yet available through the GUI.

Before you can commit any changes, the configuration file undergoes syntax checks to ensure there are no errors.

Note: To edit the configuration, it's essential to have a good understanding of DNS and BIND configurations, as incorrect changes can affect the server's performance and security.

To edit BIND configuration files:

1. Locate the BIND server that you want to configure.
2. Select *Edit configuration* on the *Action* menu. You can also access this option on the Row menu ....



   - The various configuration files associated with the BIND server are available on the *File* drop-down list. From this list, select the specific configuration file that you want to modify. Configuration files may represent different aspects of the BIND server.
   - If you're looking to make changes to specific settings within the selected configuration file, you can use the search box. Enter keywords or terms related to the settings you wish to modify.
3. Make your edits, and click *Save* when you are done.

[1] In Kea HA configurations. See dhcp-kea-ha.

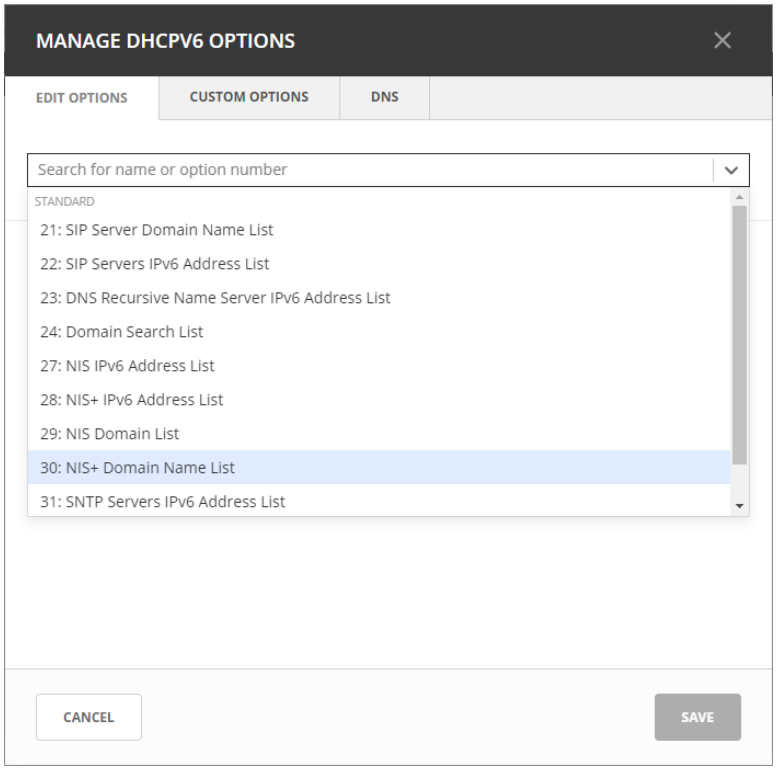
DHCP Services

For detailed information about the different DHCP platforms and their configurations, refer to:

Microsoft DHCP

Defining Options on MS DHCP Servers

1. On the **Admin** page, select *Service Management* in the upper-left corner.
2. Under **DHCP Services** in the filtering sidebar, select the applicable Microsoft DHCP server.
3. On the *Action* menu, select either *Manage DHCPv4 options* or *Manage DHCPv6 options*. You can also select these options on the **Row menu (…)**.
4. The Manage DHCP Options dialog box opens, showing all options defined on the DHCP server.
5. Use the drop-down menu to select the option you want to define.



6. To delete an option, hover over its field, and then click the trash can icon next to it.
7. Click *Save* to save the updated options.

Defining Custom DHCP Options

1. Click the *Custom Options* tab.
2. Select the appropriate *Vendor class* in the drop-down list.

Adding a New Custom Option

1. Select *Add Custom Option*.
2. Enter the desired ID. An error will show if that ID is not available or invalid.
3. Enter a name.
4. Select a Type in the dropdown list. Select the *Array* checkbox if the option is an Array.
5. Click *Add*, and then *Save*.

Note: Once an option has been defined, you can set its value on the *Edit Options* tab.

Removing an Existing Custom Option

1. On the *Custom Options* tab in the Manage DHCP Options dialog box, select the relevant custom option.
2. On the **Row menu (…)**, select *Remove*, and then *Yes* to confirm.

Configuring DNS Options

- In the Manage DHCP Options dialog box, click the *DNS* tab.

Enable DNS dynamic updates according to the settings below.
Specifies whether the DHCP server sends DNS dynamic record updates to the DNS server. Updates are sent to DNS servers configured in TCP/IP client properties for any active network connections at the DHCP server.

Dynamically update DNS A and PTR records.
Specifies that the DHCP server update forward and reverse lookups are based on the type of request made by the client during the lease process.

Always dynamically update DNS A and PTR records.
Specifies that the DHCP server update forward and reverse DNS lookups when a client acquires a lease, regardless of the type of request used to acquire it.

Discard A and PTR records when lease is deleted.
Specifies whether the DHCP server discards forward DNS lookups for clients when a lease expires.

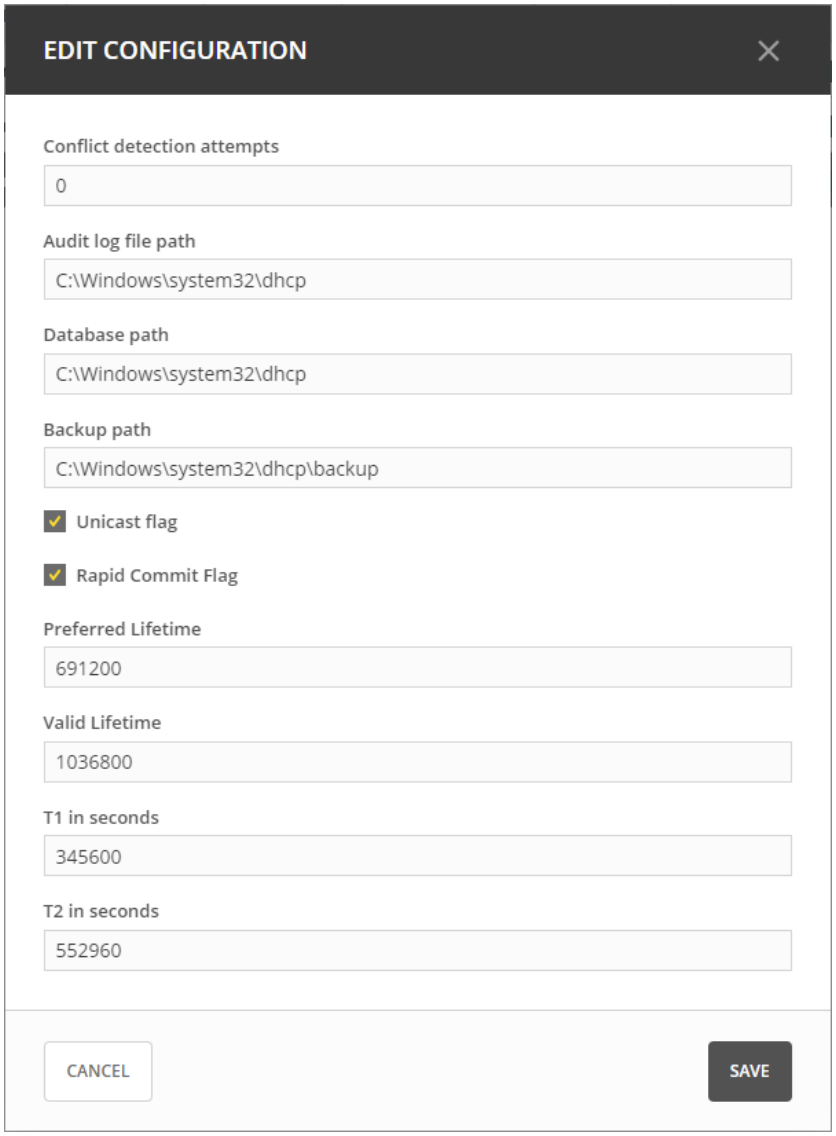
Dynamically update DNS A and PTR records for DHCP clients.
Specifies whether the DHCP server sends dynamic updates to the DNS server for DHCP clients that do not support performing these updates. If selected, clients running earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.

Disable dynamic updates for DNS PTR records
Turns off dynamic updates for PTR records.

Editing Server Properties

You can edit the configuration of Windows servers.

1. Select the relevant Windows server.
2. On the *Action* menu, select *Edit configuration*. You can also select this option on the **Row menu (...)**.
3. In the **Edit Configuration** dialog box, make the desired changes, and then click *Save*.



- **Conflict detection attempts**: Specifies the number of conflict detection attempts you want the DHCP server to make before it leases an address to a client.
- **Audit log file path**: Specifies the location of the DHCP server audit log files.
- **Database path**: Specifies the location of the DHCP server database.
- **Backup path**: Specifies the location for the database backup.

Toggling DHCPv6 Management On and Off

Note: There is only one DHCP service on a Microsoft DHCP server. DHCPv4 and DHCPv6 are not decoupled in Microsoft as they are in Micetro. Any action performed on either DHCPv6 or DHCPv4 that requires a restart of the service will result in a restart of the single DHCP service on the Microsoft server.

1. On the **Admin** page, select the relevant Microsoft DHCP server.
2. On the *Action* menu, select *Edit service*. You can also select this option on the **Row menu (...)**.
3. Select *Manage DHCPv6 service* to enable DHCPv6 management on the server(s) you selected.
4. Click *Confirm*.

Reconciling Scopes

The *Reconcile DHCP Scopes* option is used to fix inconsistencies between information in the registry and the DHCP database. For more information about how to reconcile MS DHCP servers, see *Reconcile Scopes*.

ISC Kea DHCP

Danger: Starting with Micetro 10.0, older versions of the Kea DHCP server are no longer supported. See system-requirements for a list of supported versions. You need to remove your existing (older) Kea DHCP servers from the system, and update them to a supported version of Kea before updating to Micetro 10.0 from an older version of the Men&Mice Suite. Not doing so could result in lost access to and data from the older Kea servers in Micetro.

Kea Control Agent

The Kea Control Agent is a daemon that exposes a RESTful control interface for managing Kea servers. The Control Agent daemon can receive control commands over HTTP and either forward these commands to the respective Kea servers or handle them commands on its own.

Note: The default port for the Kea Control Agent is `8000`.

Because of the Kea Control Agent, Kea DHCP servers can be added to Micetro without a DHCP Server Controller running on every machine that runs Kea. A *single* DHCP Server Controller, installed on a machine that can access the instances that run Kea services, is sufficient and will communicate with all Kea servers on Micetro's behalf.

Adding Kea to Micetro

Because Micetro uses the Kea API to communicate with the DHCP server(s), it requires (in addition to the DHCP Server Controller) the Kea hook library `libdhcp_lease_cmds.so`.

Note: On certain distributions (like RHEL) check that the kea-hooks package is also installed.

Configuring the Kea Hook Library

After installing the Kea hook library, open `kea-dhcp4.conf` and locate the `hooks-libraries` array. Add the hook to `libdhcp_lease_cmds.so`:

```
"hooks-libraries":[
    {
      "library" : "/lib64/kea/hooks/libdhcp_lease_cmds.so",
      "parameters" : {}
    }
]
```

The location of the library depends on your distribution, use `whereis libdhcp_lease_cmds.so` to find it.

After adding the library, restart Kea and the Kea Control Agent.

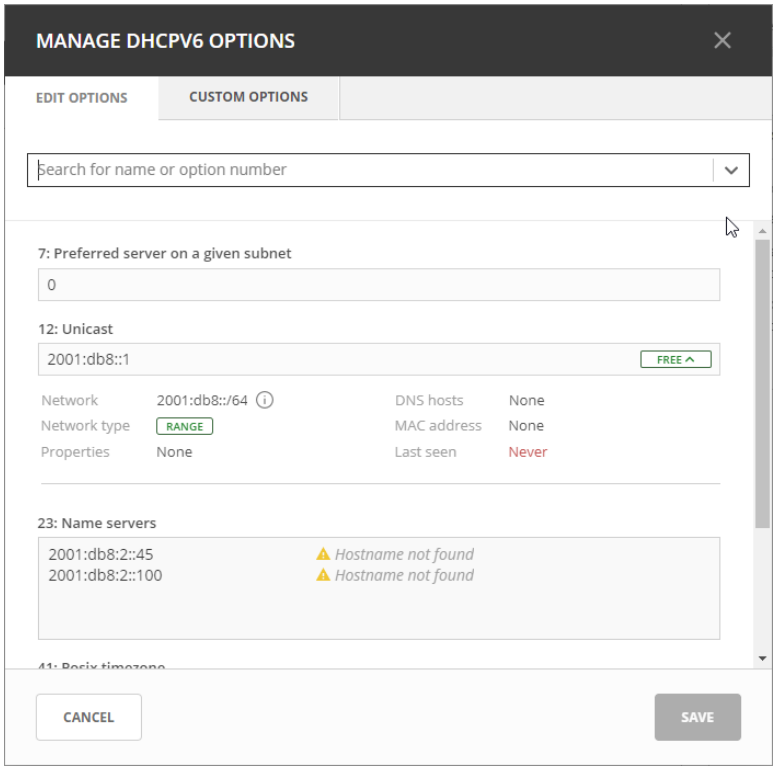
Kea High Availability

Kea DHCP servers need to be configured for high availability **before** the primary server is added to Micetro. If the high availability is set up properly, once added to the system, Micetro will recognize the failover nodes and the method (load balancing, hot standby, etc.) and configure the server objects accordingly.

For more information, see dhcp-kea-ha.

Defining Options on Kea DHCP Servers

1. On the **Admin** page, select *Service Management* in the upper-left corner.
2. Under **DHCP Services** in the filtering sidebar, select the applicable Kea DHCP server.
3. On the *Action* menu, select either *Manage DHCPv4 options* or *Manage DHCPv6 options*. You can also select these options on the **Row menu (...)**.
4. The Manage DHCP Options dialog box opens, showing all options defined on the DHCP server.
5. Use the drop-down menu to select the option you want to define.



6. To delete an option, hover over its field, and then click the trash can icon next to it.
7. Click *Save* to save the updated options.

Defining Custom DHCP Options

1. Click the *Custom Options* tab.
2. Select the appropriate *Vendor class* in the drop-down list.

Adding a New Custom Option

1. Select *Add Custom Option*.
2. Enter the desired ID. An error will show if that ID is not available or invalid.
3. Enter a name.
4. Select a Type in the dropdown list. Select the *Array* checkbox if the option is an Array.
5. Click *Add*, and then *Save*.

Note: Once an option has been defined, you can set its value on the *Edit Options* tab.

Editing an Existing Custom Option

1. On the *Custom Options* tab in the Manage DHCP Options dialog box, select the relevant custom option.
2. On the **Row menu (…)**, select *Edit*.
3. Edit the ID, and then click *Save*.

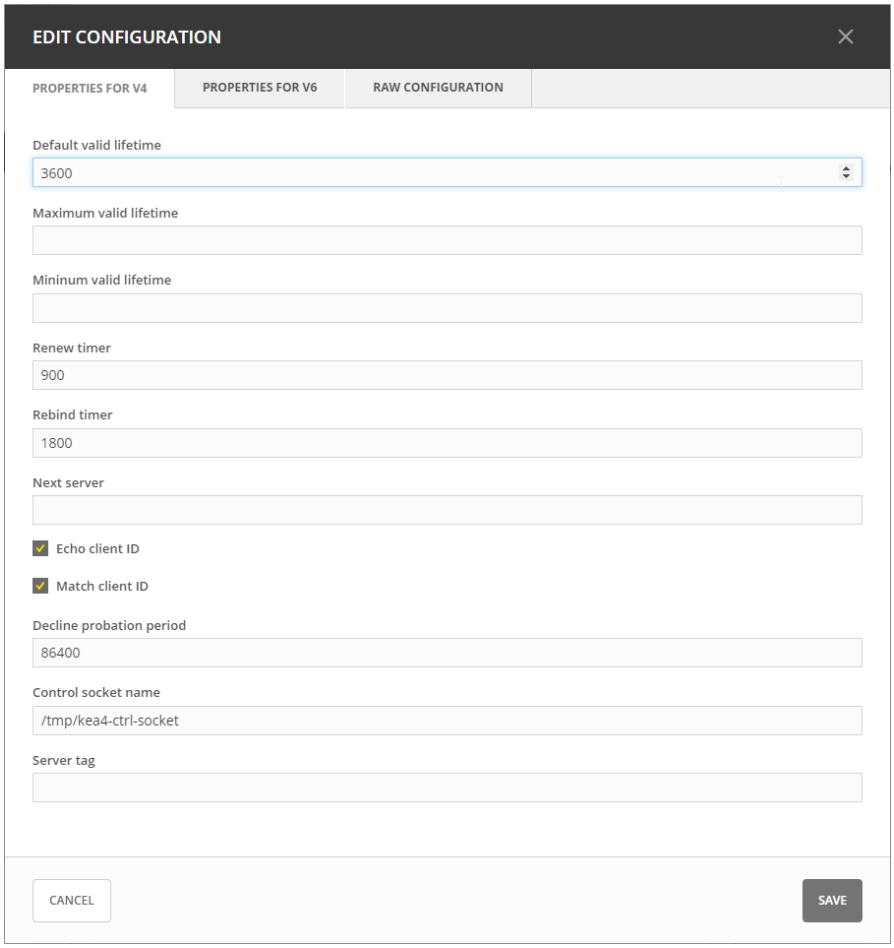
Removing an Existing Custom Option

1. On the *Custom Options* tab in the Manage DHCP Options dialog box, select the relevant custom option.
2. On the **Row menu (…)**, select *Remove*, and then *Yes* to confirm.

Kea DHCP Server Properties

You can edit the configuration of Kea DHCP servers.

1. On the **Admin** page, select the relevant Kea server.
2. On the *Action* menu, select *Edit configuration*. You can also select this option on the **Row menu (…)**.
3. In the Edit Configuration dialog box, make the desired changes, and then click *Save*.



- **Default/Maximum/Minimum Valid Lifetime**: Specifies the time after which a lease will expire if not renewed.
- **Renew Timer**: Specifies the time when a client will begin a renewal procedure.
- **Rebind Timer**: Specifies the time when a client will begin a rebind procedure.
- **Next Server**: Specifies the server address to use when clients want to obtain configuration from a TFTP server.
- **Echo Client ID**: Specifies if the server should send back client-id options when responding to clients.
- **Match Client ID**: Specifies if the server should ignore the client identifier during lease lookups and allocations for a particular subnet.
- **Decline Probation Period**: Specifies a probation time that will be set on addresses that are in use by some unknown entity.
- **Control Socket Name**: The path to the UNIX socket. Cannot be empty.
- **Server tag**: An arbitrary string used to associate configuration elements with specific Kea server instances in a configuration database, allowing for shared or unique configurations among multiple servers.

Raw Configuration

The v4 and v6 properties tabs are the most commonly used properties for configuring Kea DHCP services. For more specialized configurations, you can define additional properties on the Raw Configuration tab. This allows you to edit configuration files directly on the server for both DHCPv4 and DHCPv6. Please note that when editing these files, there is minimal error handling, so caution should be taken when making changes and saving them.

Handling External Changes with Kea

Warning: You should always edit the Kea DHCP server's configuration file through Micetro to ensure that the synchronization between Micetro and the Kea DHCP server is instant and all changes will immediately updated in the database and reflected in the user interface.

Note: All changes made to the configuration file through Micetro will automatically and instantly be propagated to the secondary/backup servers in a dhcp-kea-ha setup.

Micetro uses the in-memory configuration of the Kea server. If external changes must be made to a Kea DHCP server's configuration file, the changes to the configuration file aren't processed by the server until forced to parse the file to its *in-memory* structure, so Micetro can be made aware of these changes.

To make the Kea DHCP server process changes to its configuration file a call has to be made to either the *Kea Control Agent* or the socket that Kea uses.

An example of the call to the control-agent:

```
curl -X POST -H "Content-Type: application/json" -d '{ "command": "config-reload",
↪"service": [ "dhcp4" ] }' localhost:8000
```

If successful, the result looks like this:

```
[ { "result": 0, "text": "Configuration successful." } ]
```

After the changes to the configuration file have been accepted and parsed into the Kea DHCP servers memory structure, you can display them in Micetro through the *Edit Configuration* action for the server.

Resolving Conflicts

Micetro synchronizes all data between the Kea DHCP servers and its database regularly. Setting the `DHCPSyncInterval` variable in Central's `preferences.cfg` overwrites the default value of 15 minutes.

Note: The values set for `DHCPSyncInterval` are in seconds.

Synchronization occurs based on the configuration to update the database and the user interface, but to prevent overwriting external changes before synchronization is complete, Micetro will check for conflicts with the Kea server's in-memory configuration before writing the changes to the server.

For example, if a scope with subnet 1.3.3.0/29 is manually added to the Kea DHCP servers configuration file, and `config-reload` is successfully called, the Kea server will have parsed the change and added the scope to its in-memory data structure. Synchronization with Micetro may not have been executed yet, and the externally added scope is not yet visible in the user interface. However, if another user would try to add the same or otherwise conflicting scope through Micetro, they will receive a message stating "*A scope with address "1.3.3.0" already exists on the server*" as the configuration file is validated against the Kea DHCP servers in-memory config before each change is applied.

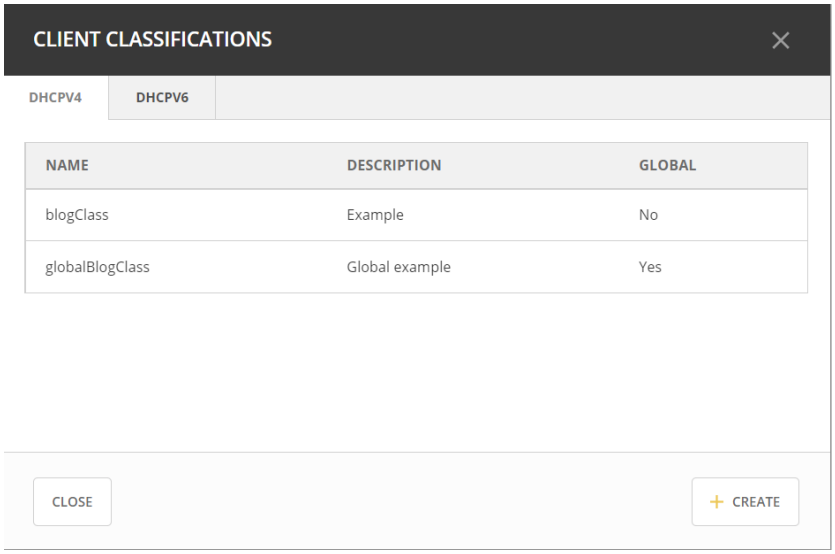
External changes and Kea high availability

See dhcp-kea-ha-external-changes.

Managing Kea Client Classifications with Micetro

You can manage Kea Client Classifications through Micetro.

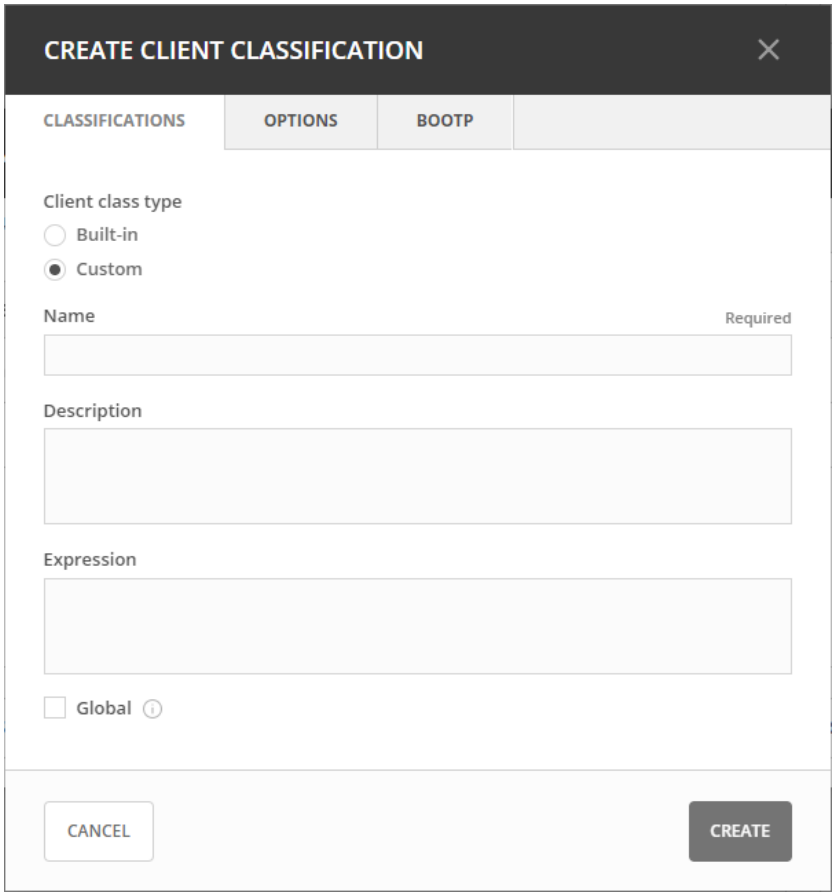
1. On the **Admin** page, select *Kea* under *DHCP Services* in the left sidebar.
2. Select the relevant service, and then select *Manage client classes* on the *Action* menu. You can also select this option on the **Row menu (…)**.



- If you have any client classes already defined on your server, you can find them listed on the respective service type tab (DHCPv4/DHCPv6).
- From here you can create, edit existing, or remove client classes. Any of these actions will add an entry to the audit trail inside of Micetro which can be viewed by selecting the history action of a client class.

Creating Client Classes

1. Click *Create*.
2. In the Create Client Classification dialog box, enter the necessary information.



- Enter a name and create an expression. Each DHCP packet will be evaluated against the expression to determine if it should belong to that client class. For information about how to create expressions, see the Kea documentation.
- Optionally you can add a description. The description is not added to the Kea config, only saved in Micetro. Defining a client class as global is a Micetro-specific feature and is explained in detail below.
- Select the *Global* checkbox if you want to create the client clss on all active Kea servers. Any modification or removal action on that client class will be replicated on all the active Kea servers.

3. Go to the *Options* tab to set DHCP options on the client classes.
4. For DHCPv4 client classes, you can specify BOOTP parameters.
5. When you are finished, click *Create*.

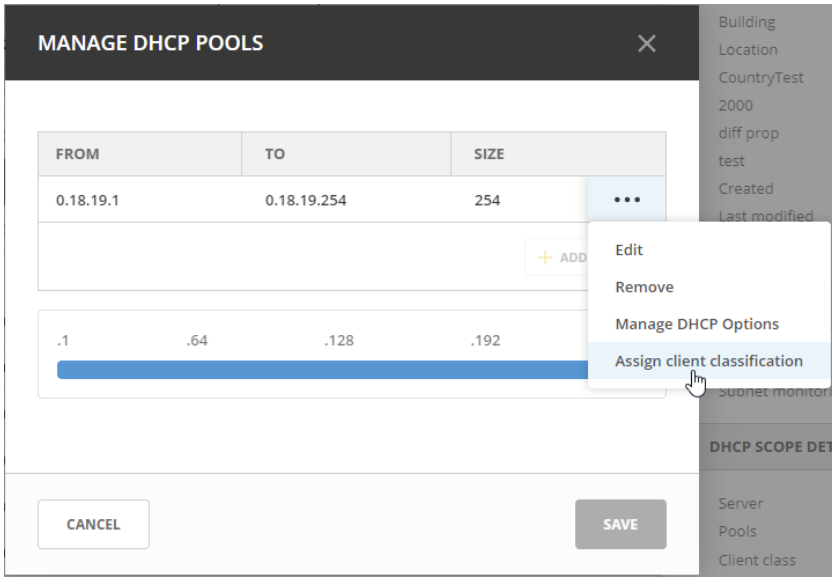
Assigning Client Classes

You can limit the access to specific scopes and address pools by assigning a client class to them. Then only packets that belong to the assigned client class will have access.

To assign a client class to a scope:

1. Go to the **IPAM** page, and select a Kea scope.
2. On the *Action* menu, select *Assign client classification*. You can also select this option on the **Row menu (...)**.
3. In the Manage DHCP Pools dialog box, select the pool.

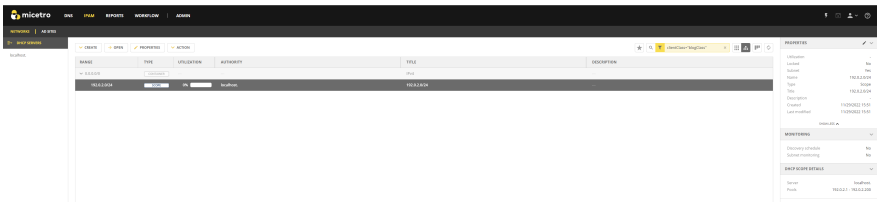
4. On the **Row menu (…)**, select *Assign client classification*.



To assign a client class to a pool:

1. Open a Kea scope.
2. On the *Action* menu, select *Manage DHCP pools*. You can also select this option on the **Row menu (…)**.
3. In the drop-down list, select the client class to assign to the scope. To unassign a client class, select *Unassigned*.

Assigning client classes to scopes/pools shows up in the history of the respective ranges. You can filter ranges based on their assigned client classes with the property *clientClass*.



ISC DHCP

Note: To manage ISC DHCP servers in the Management console, see console-dhcp-isc.

Defining Options on ISC DHCP Servers

1. On the **Admin** page, select *Service Management* in the upper-left corner.
2. Under **DHCP Services** in the filtering sidebar, select the applicable DHCP server.
3. On the *Action* menu, select either *Manage DHCPv4 options* or *Managem DHCPv6 options*. You can also select these options on the **Row menu (…)**.
4. The *Manage DHCP Options* dialog box opens, showing all custom options defined on the DHCP server.
5. Use the **Add an option** dropdown menu to select the ISC DHCP option you want to define.

6. To delete an option, hover over its field, and theb click the trash can icon next to it.
7. Click *Save* to save the changed option definitions.

Defining Custom DHCP Options

1. Click the *Custom Options* tab.
2. Select the appropriate *Vendor class* in the drop-down list.

Adding a New Custom Option

1. Select *Add Custom Option*.
2. Enter the desired ID. An error will show if that ID is not available or invalid.
3. Enter a name.
4. Select a Type in the dropdown list. Select the *Array* checkbox if the option is an Array.
5. Click *Add*, and then *Save*.

Note: Once an option has been defined, you can set its value on the *Edit Options* tab.

Editing an Existing Cusotom Option

1. On the *Custom Options* tab in the Manage DHCP Options dialog box, select the relevant custom option.
2. On the **Row menu (...)**, select *Edit*.
3. Edit the ID, and then click *Save*.

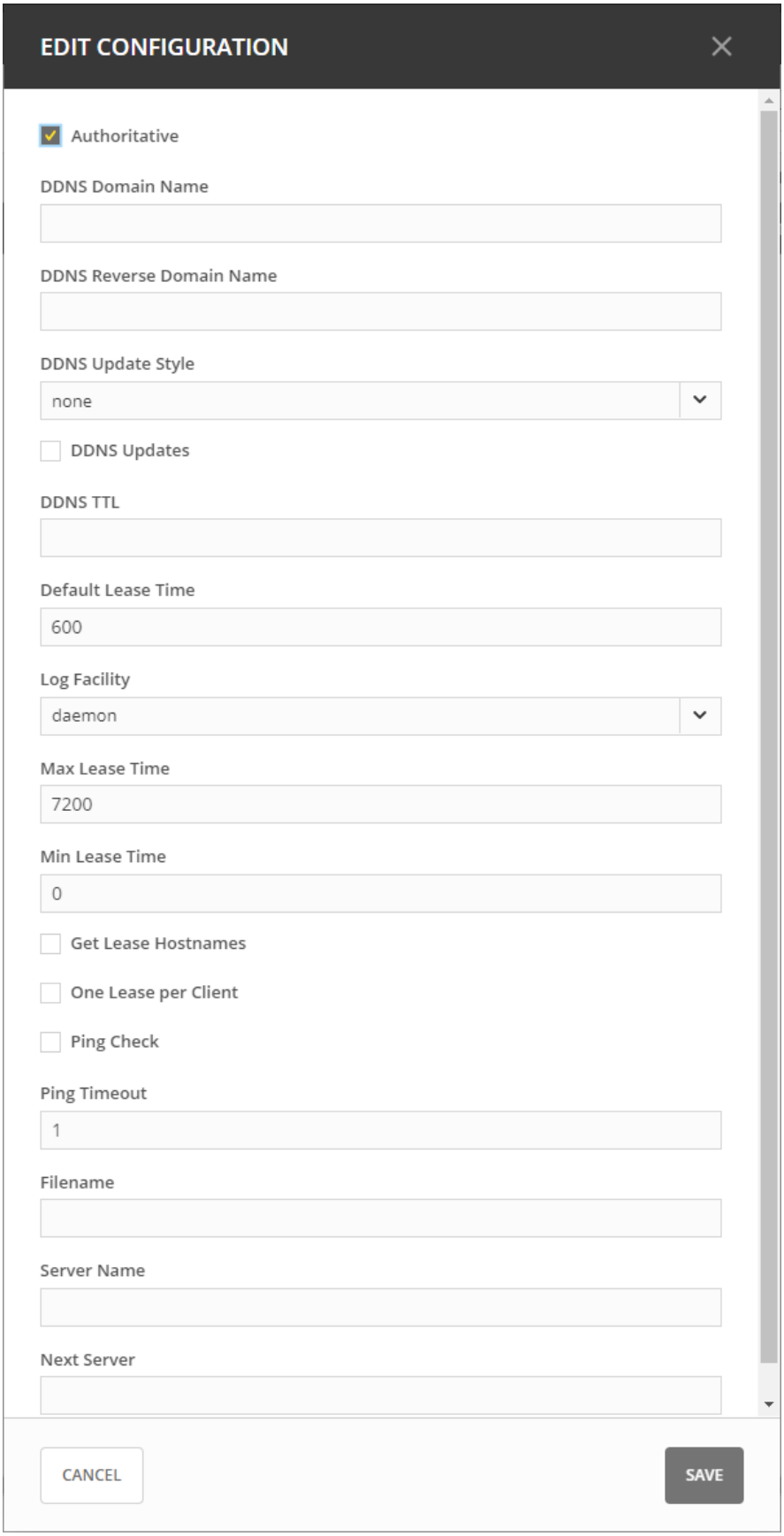
Removing an Existing Custom Option

1. On the *Custom Options* tab in the Manage DHCP Options dialog box, select the relevant custom option.
2. On the **Row menu (...)**, select *Remove*, and then *Yes* to confirm.

ISC Server Properties

You can edit the configuration of ISC DHCP servers.

1. Select the relevant server.
2. On the *Action* menu, select *Edit configuration*. You can also select this option on the **Row menu (...)**.
3. In the **Edit Configuration** dialog box, make the desired changes, and then click *Save*.


EDIT CONFIGURATION
Authoritative
DDNS Domain Name
DDNS Reverse Domain Name
DDNS Update Style
none
DDNS Updates
DDNS TTL
Default Lease Time
600
Log Facility
daemon
Max Lease Time
7200
Min Lease Time
0
Get Lease Hostnames
One Lease per Client
Ping Check
Ping Timeout
1
Filename
Server Name
Next Server
CANCEL
SAVE

- **Authoritative**: Specifies whether the server is authoritative to determine if a DHCP request from a client is valid.
- **DDNS Domain Name**: Specifies the DNS domain name to use to store the A record for a DHCP client.
- **DDNS Reverse Domain Name**: Specifies the DNS reverse domain name to use to store the PTR record for a DHCP client.
- **DDNS Update Style**: Specifies how the DHCP server does DNS updates. The available styles are:
  - **None**: Dynamic DNS updates are not performed
  - **Ad-hoc**:

    Warning: This update scheme is deprecated

  - **Interim**: This is the recommended scheme for dynamic DNS updates.
- **DDNS Updates**: Specifies whether to perform DNS updates. This setting has no effect unless DNS updates are enabled globally with the DDNS Update Style setting.
- **DDNS TTL**: Specifies (in seconds) the TTL value to use when performing a DNS update.
- **Default Lease Time**: Specifies (in seconds) the default lease time to use for DHCP leases.
- **Log Facility**: Specifies which syslog facility to use when logging DHCP server messages. All possible facilities are listed; however, not all of these facilities are available on all system.
- **Max/Min Lease Time**: Specifies (in seconds) the maximum/minimum lease time to use for DHCP leases.
- **Get Lease Hostnames**: Specifies whether the DHCP server should perform a reverse DNS lookup for each address assigned to a client and send the result to the client in the hostname option.
- **One Lease per Client**: Specifies whether the DHCP server should free any existing leases held by a client when the client requests a new lease.
- **Ping Check**: Specifies whether the DHCP server should send an ICMP echo message to probe an IP Address before offering it to a DHCP client.
- **Ping Timeout**: Specifies for how many seconds the DHCP server should wait for an ICMP echo response when Ping Check is active.
- **Filename**: Specifies the name of the initial boot file to be used by a client.
- **Server Name**: Specifies the name of the server from which the client should load its boot file.
- **Next Server**: Specifies the host address of the server from which the initial boot file (that is specified by Filename) is to be loaded.

Cisco DHCP

Note: For managing Cisco DHCP servers in the Management Console, see console-dhcp-cisco.

Editing Cisco DHCP Server Properties

You can edit the configuration of Cisco servers.

1. On the **Admin** page, select the relevant Cisco server.
2. On the *Action* menu, select *Edit configuration*. You can also select this option on the **Row menu (...)**.
3. In the **Edit Configuration** dialog box, make the desired changes, and then click *Save*.

1.19.4 Failover Management

Permissions:

To manage failover relationships

- Permission - DHCP administrator
- Built-in role - `DHCP Administrators (built-in)`

To add/remove a scope to a failover relationship

- Permission bit - `add a scope`.
- Built-in role - `DHCP Administrators (built-in)`

To Replicate Scopes

- Access bits - one or more of the following:
  - `"Read/write scope options"`
  - `"Edit reservations"`
  - `"Edit address pools"`
  - `"Edit exclusions"`
- Built-in roles - `IPAM Administrators (built-in)` and `DHCP Administrators (built-in)`

To Replicate all scopes on a server or in a relationship

- Access bits - `"Administer DHCP servers"`
- Built-in role - `DHCP Administrators (built-in)`

Note: The permissions to replicate scopes are on scope level. This is not to be confused with the "Edit reservation" permission bit on server level that does not apply in this case.

Micetro can be used to manage failover configurations for Windows, ISC and Kea DHCP servers. To help with consistency, the term Failover is used interchangeably with High Availability when referring to Kea DHCP.

DHCP failover synchronizses IP Address lease information between two DHCP servers.

Depending upon the type of server being used, servers can be put into Hot Standby, Load Balancing, or High Availability modes.

You can configure failover for a single scope or for multiple scopes on the same server.

Note: Both servers must be in Micetro for the functionality to work.

As an overlay solution, Micetro is also able to add some additional functionality that is not available natively.

Failover relationships for Windows DHCP servers are created without adding scopes to the relationship on creation. The scopes that should be part of the relationship are added later on with the "Add scope to failover" action.

Note: Windows DHCP Failover Configurations can be managed from the Micetro Web Application.

ISC DHCP and Kea DHCP Failover Configurations can only be managed from the Management Console.

Managing Failover Configurations for ISC DHCP

Note: When adding a server's first failover peer, all other address pools on the server will be updated to refer to this failover peer.

---

1. On the **Object** menu, select the DHCP Server that contains the scope for which you want to setup failover configuration.
2. In the list of scopes, double-click on the applicable one.
3. In the list of IP Addresses, right-click the applicable one, and then select *Create Address Pool* on the shortcut menu. The DHCP Address Pool dialog box displays.
4. Move to the **Failover Peer** field, and click the drop-down list arrow.
5. Select *Add new failover peer*.
6. Click *OK*. The New Failover Peer dialog box displays.
    - **Name**: Specifies the name of the failover peer.
    - **Role**: Specifies the role of the failover peer. The available roles are Primary and Secondary.
    - **Address**: Specifies the IP Address or DNS name on which the server should listen for connections from its failover peer.
    - **Port**: Specifies the port number on which the server should listen for connections from its failover peer.
    - **Peer Address**: Specifies the IP Address or DNS name to which the server should connect to reach its failover peer for failover messages.
    - **Peer Port**: Specifies the port number to which the server should connect to reach its failover peer for failover messages.
    - **Max Response Delay**: Specifies the number of seconds that may pass without the server receiving a message from its failover peer before it assumes that the connection has failed.
    - **Max Unacked Updates**: Specifies the number of messages the server can send before receiving an acknowledgement from its failover peer. According to ISC documentation, 10 seems to be a good value.
    - **Max Client Lead Time**: Specifies the number of seconds for which a lease can be renewed by either server without contacting the other. Only specified on the primary failover peer.
    - **Split Index**: Specifies the split between the primary and secondary failover peer for the purposes of load balancing. According to ISC documentation, 128 is really the only meaningful value. Only specified on the primary failover peer.
    - **Load Balance Max Seconds**: Specifies the cutoff in seconds after which load balancing is disabled. According to ISC documentation, a value of 3 or 5 is recommended.
7. Click *OK*. The DHCP Address Pool dialog box displays and shows the updated information.

8. Click *OK*.

If you need to EDIT or DELETE an existing failover peer, do the following:

1. Locate the relevant ISC DHCP server.
2. Right-click and, in the shortcut menu, select *Manage Failover Peers*. The Failover Peers for... dialog box displays. All failover peers are shown.
3. To EDIT a failover peer, select it and click the *Edit* button. Then modify the Failover Peers ... properties dialog box, as needed.
4. To DELETE a failover peer, select it and click the *Delete* button.

Note: In order to finalize the setup of the failover relationship, the scope needs to be migrated to the failover peer.

Note: When deleting a failover peer through this dialog, if it is the last failover peer defined on the server, any references to it will be removed from existing address pools on the server. If there is one other failover peer left on the server, references to the failover peer being deleted will be changed to refer to the remaining failover peer. If, however, there are two or more other failover peers left on the server, the user will be prompted with a list of the remaining failover peers where he will have to choose which failover peer should be referenced by address pools currently referring to the failover peer being deleted.

Note: When changing from one failover peer to another for some specific address pool, if the address pool is the last one referring to the (old) failover peer, the user will be warned that performing the action will result in the deletion of the failover peer.

Managing Failover Relationships for Windows DHCP Servers

Note: To manage failover between two Microsoft Servers, the DHCP Server Controller must be running as a service account with enough privileges to manage the DHCP service. For more information, see *Men&Mice DHCP Agents*.

Setting up a Failover Relationship

1. On the **Admin** page, select *Service Management* in the upper-left corner.
2. In the left sidebar, under *DHCP Services*, select *Microsoft DHCP*.
3. Select the Windows Server that you want as the primary server in the relationship, and then select *Failover management* on the *Action* menu. You can also select this option on the **Row menu (...)**.
4. Click *Add Relationship*, and set up the relationship as desired. For more information, see *Failover Relationship Parameters*.
5. After confirming the details on the summary tab, click *Add*.

Removing a Failover Relationship

1. On the **Admin** page, select the Windows server that contains the relationship you want to remove, then select *Failover management* on the *Action* menu. You can also select this option on the **Row menu (...)**.
2. Select the relevant relationship, and then select *Remove* on the **Row menu (...)**.
3. If there are scopes associated with the relationship, you will be prompted to select which server you want the scopes to survive on and whether you want the scopes on the other server to be deleted or disabled.

Setting up a Failover Relationship on Management Console (obsolete)

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to setup failover configuration.
2. You have two ways to choose the scopes you want to configure.
   - On the list of scopes, select one or more scopes, right-click and select *Configure Failover*. Right-click the DHCP server, and then select *Configure Failover*.
   - A dialog box listing all configurable scopes displays. Select the scopes you want to configure and click *Next*. The failover configuration dialog box displays.

Removing a Failover Relationship on Management Console (obsolete)

1. On the object menu, select the DHCP Server that contains the scope(s) for which you want to remove the failover relationship.
2. Select one or more scopes, right-click the selection, and then select *Deconfigure Failover*. A confirmation dialog box displays.
3. Click *Yes* to confirm the action. The failover configuration for the selected scope(s) is removed.

Failover Relationship Parameters

- **Failover Name**
  The name for the the relationship.
- **Failover Mode**
  Select the failover mode you want to use. You can choose between Hot standby and Load balance.
- **Partner Server**
  Select the partner server with chich failover should be configured.
- **Addresses reserved for standby server**
  If you chose the Hot standby mode, you must set the percentage of addresses that should be reserved to the standby server.
- **Local Server Load Balance Percentage**
  If you chose the Load Balance mode, you must specify the load balance percentage to use on the local server. The remaining percentage will be used on the partner server.
- **Maximum Client Lead Time**
  If you don't want to use the default values, enter the new values in seonds.

- **State Switchover Interval**
  Specify an interval in seconds if Automatic State Switchover should be used. A value of zero means it's disabled.
- **Shared Secret for Message Authentication**
  If you want to use message authentication between the DHCP servers, you must provide a shared secret for the message authentication.

Replicating Failover Scopes

When using a failover relationship, it is possible to replicate scope information between servers. This is possible for individual scopes, all scopes that share a failover relationship, or all scopes on a particular DHCP server.

When a scope replication takes place, the scopes on the selected DHCP are considered the source scopes and the entire scope contents are replaced on the destination server.

Replicating Individual Scopes

1. On the **IPAM** page, select the Microsoft DHCP server that contains the relationship.
2. On the *Action* menu, select *Replicate failover scope*. You can also select this option on the **Row menu (...)**.
3. Select a source server, and then click *Confirm*.

Replicating All Scopes that Share a Failover Relationship

1. On the **Admin** page, select the Microsoft DHCP server that you want in the relationship.
2. On the *Action* menu, select *Failover management*. You can also select this option on the **Row menu (..)**.
3. Select the relevant failover relationship, and then select *Replicate failover relationship* on the **Row menu (...)**.
4. Click *Confirm*.

Replicating All Failover Scopes on a DHCP Server

Note: When replication takes place, the scopes on the selected DHCP server are considered the source scopes and the entire scope contents for each scope is replaced on the partner server.

---

1. On the **Admin** page, select one of the Microsoft DHCP servers that you want in the relationship.
2. On the *Action* menu, select *Recplicate failover relationships*. You can also select this option on the **Row menu (..)**.
3. Click *Confirm*.

Replicating Individual Scopes on Management Console (obsolete)

1. On the Object menu, select the DHCP Server that contains the scope(s) you want to replicate.
2. Select one or more scopes, right-click the selection, and then select *Replicate Scope*.
3. A confirmation dialog box displays. Click *OK* to confirm the action. The selected scope is replicated.

Replicating All Scopes that share a Failover Relationship on Management Console (obsolete)

1. On the Object menu, select the DHCP Server that contains the scopes you want to replicate.
2. Right-click a scope using the desired relationship, and then select *Replicate Relationship*.
3. A confirmation dialog box displays. Click *OK* to confirm the action. The scopes that use the same relationship as the selected scope are replicated.

Note: This action may take some time if multiple scopes use the relationship.

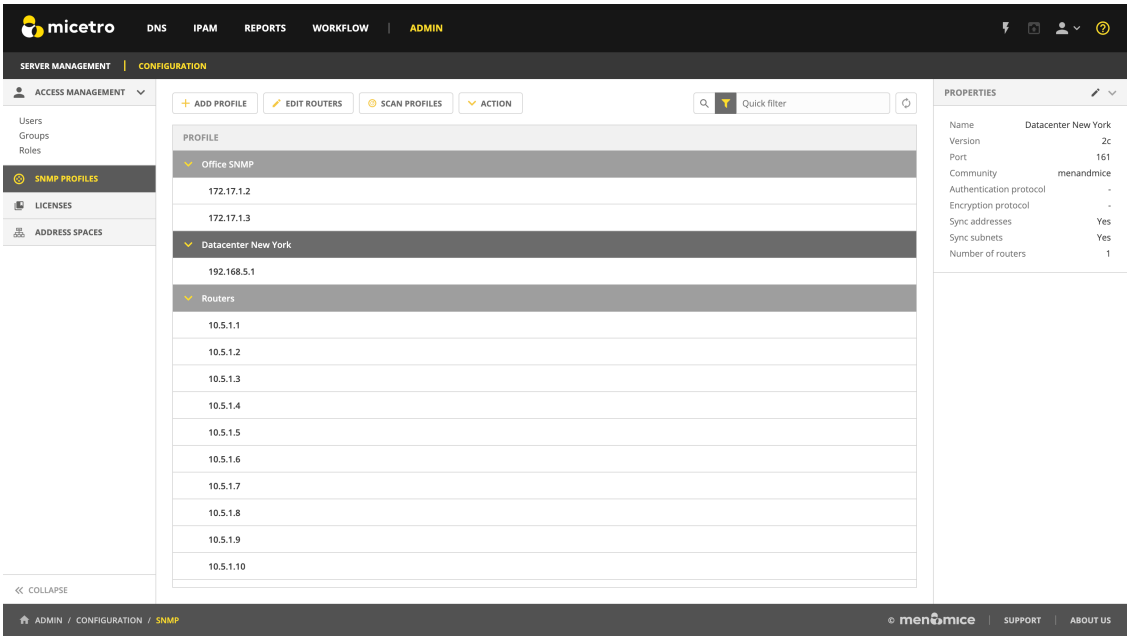
Replicating All Failover Scopes on a DHCP Server on Management Console (obsolete)

1. On the Object menu, right-click the DHCP Server that contains the scopes you want to replicate, and then select *Replicate Failover Scopes* from the menu.
2. A confirmation dialog box displays Click *OK* to confirm the action. All failover scopes on the selected server are replicated.

Note: This action may take some time if the server contains multiple failover scopes.

1.19.5 SNMP Profiles

The SNMP protocol provides a common mechanism for devices on networks to relay management information. Micetro uses SNMP profiles to determine whether devices that have been discovered on networks are active.



Note: For configuring SNMP profiles using the Management Console, see console-snmp-profiles.

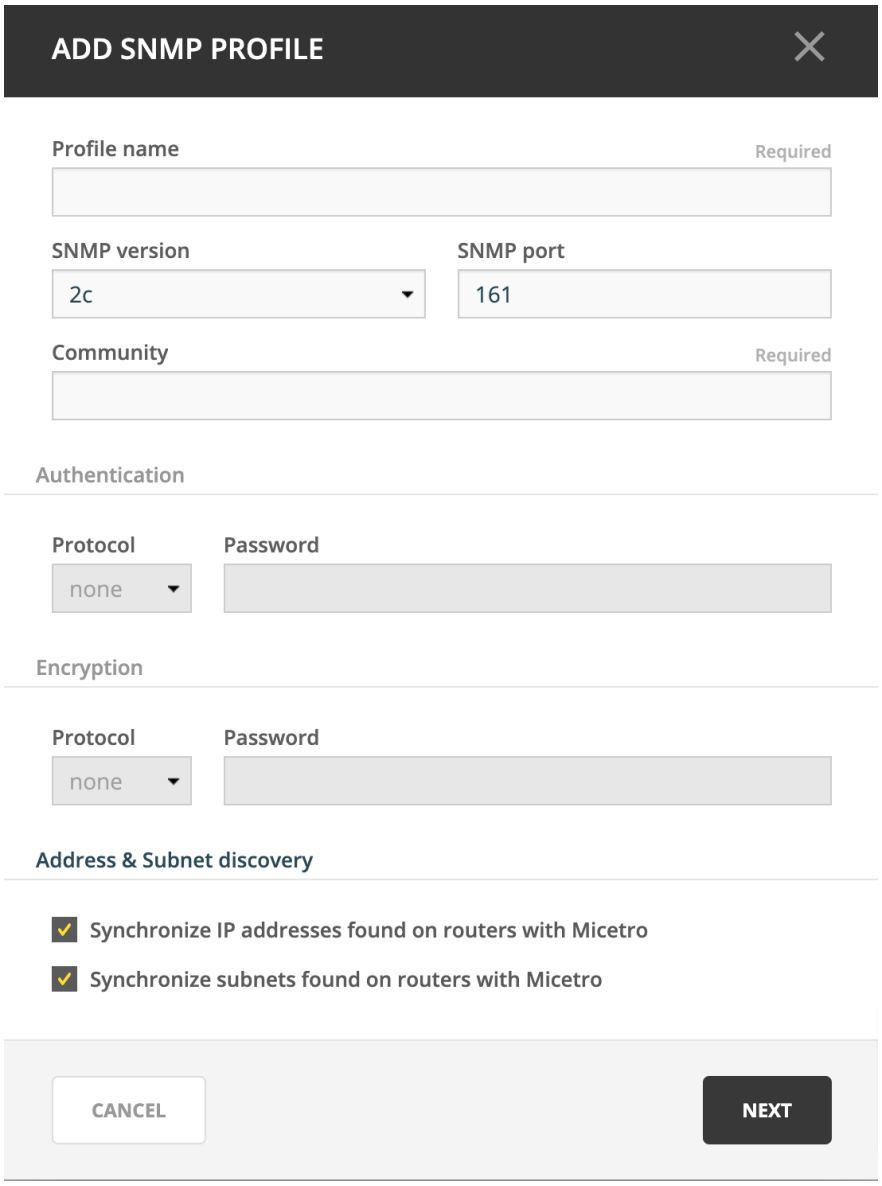
Creating a New SNMP Profile

Before a router can be queried, it must be placed in an SNMP profile containing the parameters necessary to access the SNMP information on the router.

Note: Multiple routers can share the same SNMP profile.

To create an SNMP profile:

1. Navigate to *Admin –> Configuration –> SNMP Profiles*.
2. Select *Add Profile* on the top toolbar.



3. Enter a profile name and choose the SNMP version to use. (Supported versions are SNMP v1, v2c, and v3.) You can also specify a non-standard port to use for SNMP.
4. Enter the necessary information to access the router using SNMP. The information is different depending on the SNMP version selected:

   For SNMP v1 and v2c:

Community	Enter the SNMP community string (password) to use to access the routers using the profile.

   For SNMP v3:

Username	Enter a user name for accessing the routers using the profile.
Authentication	
Protocol	Choose the authentication protocol to use. The available protocols are **MD5** and **SHA**.
Password	Enter the authentication password for the routers using the profile.
Encryption	
Protocol	Choose the encryption protocol to use. The available protocols are **AES** and **DES**.
Password	Enter the authentication password for the routers using the profile.

5. If needed, disable IP address and subnet synchronization.
6. Click *Next*.
7. Paste or enter the IPv4 address of the router(s) that you want to query using this profile.

Note: Each router's IP address needs to be on a separate line in the text area.

8. Click *Add profile* to save the settings and create the profile.

Editing Existing SNMP Profiles

You can edit an existing SNMP profile, to change settings or modify the routers using it.

1. Navigate to *Admin* → *Configuration* → *SNMP Profiles*.
2. Select *Action –> Edit SNMP Profile* on the top toolbar or the **Row menu (...)** to edit a profile's settings. Select *Edit routers* to modify the list of routers using the profile.

Scanning Profiles

SNMP scanning is done automatically in the background by Micetro. Users can initiate a manual scan of all configured profiles to pull ARP cache from the routers if needed.

Select *Scan profiles* on the top toolbar to manually scan all profiles.

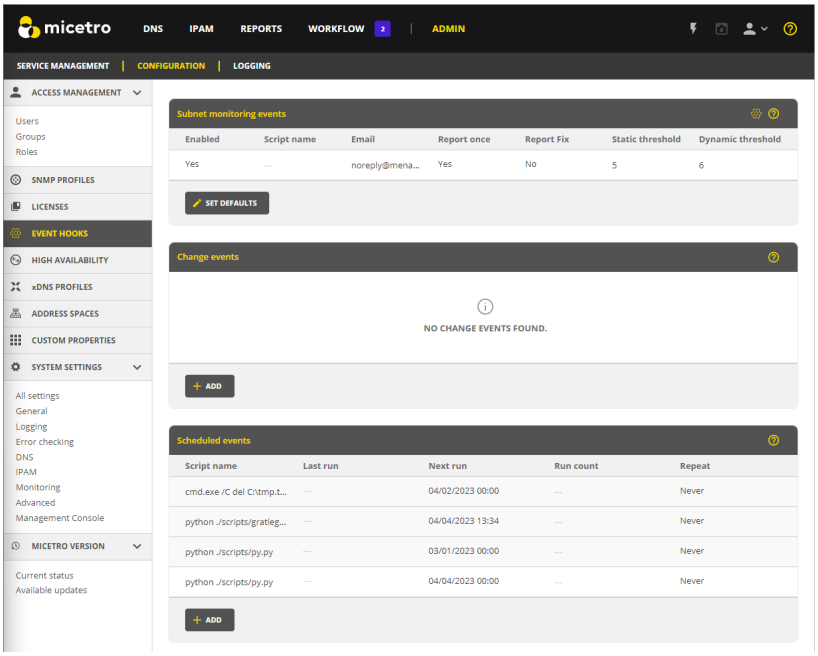
Warning: This might take a long time and can result in higher volumes of traffic.

1.19.6 Event Hooks

Use event hooks to monitor and run specific scripts based on certain events. This gives you the ability to intercept and modify the platform's standard behavior.

Permissions:

- Permission: None (cannot create a custom role to access this)
- Role: `Administrators (built-in)`



Subnet Monitoring Events

To access subnet monitoring events:

1. On the **Admin** page, select *Configuration* in the upper-left corner.
2. Select *Event Hooks* in the filtering sidebar.

Enabling Subnet Monitoring

Subnet monitoring is enabled in the *System Settings*. Click the **Settings** button in the upper-right corner to go to the System Settings where you can enable subnet monitoring in the system and configure email notifications.

When enabled, the system monitors the free addresses in DHCP address pools and subnets, and performs an action if the number of free addresses goes below a user-definable threshold.

When subnet monitoring is enabled, a new column, **Monitoring**, is added when viewing the subnet list. To filter the view by this column and quickly see all subnets that are monitored, you can enter "Monitor: Yes" in the Quick Filter search box.

SMTP Server

The mail server from which notification emails will be sent when the number of addresses goes below a certain threshold.

Mail from

The email address from which notification emails will be sent when the number of addresses goes below a certain threshold.

Subnet Monitoring Defaults

The Subnet monitoring events section lists the current defaults. To change the default values, click **Set Defaults** and make the desired changes in the dialog box.

Enabled
When selected, all subnets are monitored by default. If you only want to monitor a subset of the subnets in the system, clear the checkbox and enable monitoring for the individual subnets instead by selecting the subnet on the **IPAM** page, and then selecting *Set subnet monitoring* on the *Action* menu.

Script to invoke
Enter the path of the script to run when the number of free addresses goes below the set threshold. See *Change Events* for information on the script interface and the format for calling the script.

Email address
The email address that should be the recipient of notification when the number of free addresses goes below the set threshold.

Dynamic threshold
Enter the threshold for the free addresses in a DHCP scope address pool.

Note: For split scopes and scopes in a superscope (on MS DHCP servers) and address pools using the shared-network feature on ISC DHCP servers, the total number of free addresses in all of the scope instances is used when calculating the number of free addresses.

Static threshold
Enter the threshold for the free addresses in a subnet.

Only perform action once (until resolved)
When selected, the action is performed only once when the number of free addresses goes below the threshold.

Perform action when resolved
When selected, the action is performed when the number of free addresses is no longer below the threshold.

Note: The global subnet monitoring setting can be overridden for individual subnets by changing the setting explicitly for the subnet. For information on how to change monitoring settings for individual subnets, see *IPAM*, Set Subnet Monitoring.

Subnet Monitoring Script Interface

The XML schema for a subnet monitoring script is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault=
↪"qualified" xmlns="http://tempuri.org/XMLSchema.xsd" xmlns:mstns="http://tempuri.org/
↪XMLSchema.xsd" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="scopeMonitor">
<xs:complexType>
<xs:sequence>
<xs:element name="scope" type="xs:string" minOccurs="0" maxOccurs="1" />
<xs:element name="server" type="xs:string" minOccurs="0" maxOccurs="1" />
<xs:element name="superscope" type="xs:string" minOccurs="0" maxOccurs="1" />
<xs:element name="threshold" type="xs:integer" minOccurs="1" maxOccurs="1" />
<xs:element name="available" type="xs:integer" minOccurs="1" maxOccurs="1" />
<xs:element name="fixed" type="xs:boolean" minOccurs="1" maxOccurs="1" />
<xs:element name="thresholdType" type="xs:string" minOccurs="1" maxOccurs="1" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

The value of the thresholdType element will be either static or dynamic depending on whether the threshold being crossed is one of dynamically allocatable addresses (that is, available addresses in address pools) or if it is a threshold set for static addresses (that is, available addresses outside of address pools).

Note: The global subnet monitor, set through the *System Settings*, is the only one that takes superscopes into account. When the global subnet monitor actions are performed, due to the conditions being met for a superscope, the XML generated will contain a <server> tag and a <superscope> tag.

An example XML structure for a subnet monitoring script might look as follows for scope:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<scopeMonitor>
<scope>123.45.67.0/24</scope>
<threshold>20</threshold>
<available>8</available>
<fixed>0</fixed>
<thresholdType>dynamic</thresholdType>
<customFields>
<customField customFieldID="1" customFieldName="Title" objectID="526" objectType="6"␣
↪value="Your subnet title"></customField>
<customField customFieldID="2" customFieldName="Description" objectID="526" objectType="6
↪" value="You subnet description"></customField>
<customFields>
</scopeMonitor>
```

The XML structure is slightly different if a superscope (MS DHCP) or a shared-network (ISC DHCP) configuration is used. An example XML structure for a scope monitoring script might look as follows for a superscope / shared-network configuration:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<scopeMonitor>
<server>dhcp1.corp.net.</server>
<superscope>office</superscope>
<threshold>20</threshold>
<available>22</available>
<fixed>1</fixed>
<thresholdType>dynamic</thresholdType>
</scopeMonitor>
```

A subnet monitoring script does not have any return value.

Example PowerShell Script

Note: Powershell scripts can be run natively by Men&Mice by starting the command with `powershell`, `powershell.exe` or simply with the path to the `.ps1` file. Powershell can then read the stdin with `[Console]::In.ReadToEnd()`.

Instructions

1. Copy the `ScopeMonScript.ps1` to `C:\\ProgramData\\Men and Mice\\Central`.
2. In Admin->Configuration->Event Hooks, under **Subnet monitoring events**, click *Set Defaults*.
3. Enter `ScopeMonScript.ps1` in the **Script to invoke** text box.
4. Configure a dynamic threshold.

The monitor will be executed every 10 minutes during the DHCP synchronization interval.

```
param([Parameter(Mandatory=$false,ValueFromPipeLine=$false)]$UserName = "",
[Parameter(Mandatory=$false,ValueFromPipeLine=$false)]$Password = "",
[Parameter(Mandatory=$false,ValueFromPipeLine=$false)]$xmlFileName = "")
$strInput = get-content $xmlFileName
#$strInput = $args
# write output for troubleshooting in file:
#Add-Content -Path .\monitoroutput.xml $strInput

$strXML = [string]::Join(" ", $strInput)
$objXML = [xml]$strXML
$subnetMonitor = (Select-Xml -XML $objXML -XPath "/subnetMonitor").Node

# Check if it's an alert or fixed message
# The script only cares about alerts
if ($subnetMonitor.fixed -eq "0")
{
    $strAlert = "Alert:  The following scope or subnet has fewer IPs available than the␣
↪configured threshold."

    # We could send here an email or generate a trap or...
    #Send-MailMessage -SmtpServer "smpt.example.com" -From "subnetmonitor@example.com" -
↪To "alert1@example.com;alert2@example.net" -Subject "Subnet Monitor Message" -Body
```

(continues on next page)

(continued from previous page)

```
↪$strOutput

    # First handle the superscopes
    if ($subnetMonitor.superscope -ne $null -and $subnetMonitor.superscope -ne "")
    {
    $strOutput = @"

    $strAlert
    Superscope: $($subnetMonitor.superscope)
    Alert Date:    $(Get-Date -Format G)
    Server:        $($subnetMonitor.server)
    Threshold:    $($subnetMonitor.threshold)
    IPs Available:    $($subnetMonitor.available)
    Subnet Type:    $($subnetMonitor.thresholdType)
    "@
        New-EventLog -Source SubnetMonitor -LogName Application
        Write-EventLog -LogName Application -Source SubnetMonitor -EventID 1063 -
↪EntryType Warning -message "$strOutput"
        #Add-Content -Path .\superscopemonitor_msg.txt $strOutput
        }
    else
    {
    # then in the else clause the normal scopes

    $strOutput = @"

    $strAlert
      Alert Date:    $(Get-Date -Format G)
      Scope:        $($subnetMonitor.subnet)
      Threshold:    $($subnetMonitor.threshold)
      IPs Available:    $($subnetMonitor.available)
      Subnet Type:    $($subnetMonitor.thresholdType)
      "@
        New-EventLog -Source SubnetMonitor -LogName Application
        Write-EventLog -LogName Application -Source SubnetMonitor -EventID 1064 -
↪EntryType Warning -message "$strOutput"
        #Add-Content -Path .\scopemonitor_msg.txt $strOutput
    }
  }
  else
  {
  # possible issue fixed message
  }
```

Example Python Script

The following example script, written in Python, shows how a script could return different values depending on the input of custom fields. The script is called when an object property changes and it queries for country and city using a location code. The intended use here is to mark the locations of servers.

```
import sys
import xml.etree.ElementTree as ET

def get_custom_field_element(custom_fields, name):
 element = custom_fields.find(f"./customField[@customFieldName='{name}']")
 if element is None:
     raise KeyError(f"Custom property '{name}' was not found.")
 return element

def get_result(root):
 # username variable is not used but this is how to get the username
 username = root.get('userName')
 custom_fields = root.find("./customFields")

 result = ET.Element("result", {"success": "0"})
 try:
     location_element = get_custom_field_element(custom_fields, 'Location')
     country_element = get_custom_field_element(custom_fields, 'Country')
     city_element = get_custom_field_element(custom_fields, 'City')
 except KeyError as e:
     ET.SubElement(result, "error", {"code": "1", "message": str(e)})
     return result
 location = location_element.get('value')

 # A database could be queried instead here
 LOCATION_MAP = {
     'l1': ('USA', 'Washington'),
     'l2': ('UK', 'London')
 }
 if location not in LOCATION_MAP:
     ET.SubElement(result, "error", {"code": "1", "message": "Unknown location."})
     return result

 result.set("success", "1")
 country, city = LOCATION_MAP[location]
 country_element.set('value', country)
 city_element.set('value', city)
 result.append(custom_fields)
 return result

# Read all input and parse as XML
root = ET.fromstring(sys.stdin.read())
result = get_result(root)

print('<?xml version="1.0"?>')
# This will write the generated result xml to standard output
ET.dump(result)
```

Change Events

Overview

The system can be configured to run scripts in the event that object properties are changed. The script is also run when an object is created, but not on deletion.

Note: Scripts for the DNS Record object type are handled a bit differently. They are not run upon modifying the custom properties of a record, but rather when the content of the zone changes (record added, modified, or deleted.) For more information, see *Zone Content Change Script Interface*.

Scripts associated with object types are often used to perform lookups in external data sources and return data from these sources.

Adding a Change Event

1. On the **Admin** page, select *Configuration* in the upper-left corner.
2. Select *Event Hooks* in the filtering sidebar.
3. Change events are displayed in the **Change Events** section. Click *Add*.
4. In the Add Change Event dialog box, select the **Object type** (Zone, IP Address etc.), and then enter the **Script name** and necessary startup parameters.

   You must enter all information for the script as you would when invoking the script from the command line. It is assumed that the script is located in the same directory as Men&Mice Central; however, if the script is stored in a different location, the path for the script must be entered.
5. When you are finished, click *Add*.

Example 1: Running a python script named mytest.py.

> To run a script named mytest.py that is located in the Men&Mice Central directory using the python interpreter, the following would be placed in the appropriate field: `python mytest.py`.

Example 2: Running an executable named checkdata.exe.

> To run an executable named checkdata.exe that is located in the Men&Mice Central directory the following would be placed in the appropriate field: `checkdata.exe`.

Editing and Deleting Change Events

1. Click the Actions button (**...**) for the event you want to edit or delete.
2. Select the appropriate action on the pop-up menu, and make the desired changes.

Script Interfaces

When Men&Mice Central runs an external script assoicated with a change event, it sends an XML structure as an argument to the script being called. The XML structure contains information about all custom properties that are defined for the object type. The XML structure also contains the login name of the user that triggered the script.

The XML structures differs a little depending on the type of script (property change, zone contents change, scope monitoring).

Note: The API knows change events as External Scripts which is why the element name is externalScriptParameters.

Property Change Script Interface

The XML schema for a property change script is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault=
↪"qualified" xmlns="http://tempuri.org/XMLSchema.xsd" xmlns:mstns="http://tempuri.org/
↪XMLSchema.xsd" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="externalScriptParameters">
<xs:complexType>
<xs:sequence>
<xs:element ref="customFields" minOccurs="1" maxOccurs="1" />
</xs:sequence>
<xs:attribute name="userName" type="xs:string" />
</xs:complexType>
</xs:element>
<xs:element name="customFields">
<xs:complexType>
<xs:sequence>
<xs:element ref="customField" minOccurs="1" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="customField">
<xs:complexType>
<xs:sequence>
</xs:sequence>
<xs:attribute name="customFieldID" type="xs:string" />
<xs:attribute name="customFieldName" type="xs:string" />
<xs:attribute name="objectID" type="xs:string" />
<xs:attribute name="objectType" type="xs:string" />
<xs:attribute name="value" type="xs:string" />
</xs:complexType>
</xs:element>
</xs:schema>
```

An example XML structure with three custom properties named Location, Country and Region might look as follows:

```
<?xml version="1.0"?>
<externalScriptParameters username="administrator">
```

(continues on next page)

(continued from previous page)

```
<customFields>
<customField customFieldID="24" customFieldName="Location"
objectID="27" objectType="4" value="location1"></customField>
<customField customFieldID="25" customFieldName="Country"
objectID="27" objectType="4" value=""></customField>
<customField customFieldID="26" customFieldName="Region"
objectID="27" objectType="4" value=""></customField>
</customFields>
</externalScriptParameters>
```

Upon completion, the script must create a new XML structure and return it to Men&Mice Central. The schema for the XML structure that is returned is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd"
elementFormDefault="qualified" xmlns="http://tempuri.org/
XMLSchema.xsd" xmlns:mstns="http://tempuri.org/XMLSchema.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="result">
<xs:complexType>
<xs:choice minOccurs="1" maxOccurs="2">
<xs:element ref="customFields" />
<xs:element ref="error" />
</xs:choice>
<xs:attribute name="success" type="xs:string" />
</xs:complexType>
</xs:element>
<xs:element name="customFields">
<xs:complexType>
<xs:sequence>
<xs:element ref="customField" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="customField">
<xs:complexType>
<xs:sequence>
</xs:sequence>
<xs:attribute name="customFieldID" type="xs:string" />
<xs:attribute name="customFieldName" type="xs:string" />
<xs:attribute name="objectID" type="xs:string" />
<xs:attribute name="objectType" type="xs:string" />
<xs:attribute name="value" type="xs:string" />
</xs:complexType>
</xs:element>
<xs:element name="error">
<xs:complexType>
<xs:sequence>
</xs:sequence>
<xs:attribute name="code" type="xs:string" />
<xs:attribute name="message" type="xs:string" />
</xs:complexType>
```

(continues on next page)

(continued from previous page)

```
</xs:element>
</xs:schema>
```

An example XML structure with three custom properties named Location, Country and region might look as follows:

```
<?xml version="1.0"?>
<result success="1">
<customFields>
<customField customFieldID="24" customFieldName="loc" objectID="27" objectType="4" value=
↪"location1"></customField>
<customField customFieldID="25" customFieldName="Country" objectID="27" objectType="4"␣
↪value="USA"></customField>
<customField customFieldID="26" customFieldName="Region" objectID="27" objectType="4"␣
↪value="Texas"></customField>
</customFields>
</result>
```

Men&Mice Central uses the information in the XML structure to update other custom properties or to display an error message if the success attribute on the result element is set to 0. The following XML example shows how an error message can be returned by the change event script.

```
<?xml version="1.0"?><result success="0"><error code="1"message="The error message."></
↪error></result>
```

The XML structure is not required to return information about all custom properties, only fields that the script has changed. Unknown property fields are ignored by Men&Mice Central.

Zone Content Change Script Interface

The XML schema for a zone content change script is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema targetNamespace="http://tempuri.org/XMLSchema.xsd" elementFormDefault=
↪"qualified" xmlns="http://tempuri.org/XMLSchema.xsd" xmlns:mstns="http://tempuri.org/
↪XMLSchema.xsd" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="externalScriptParameters">
<xs:complexType>
<xs:sequence>
<xs:element ref="object" minOccurs="1" maxOccurs="1" />
</xs:sequence>
<xs:attribute name="userName" type="xs:string" />
</xs:complexType>
</xs:element>
<xs:element name="object">
<xs:complexType>
<xs:sequence>
<xs:element name="id" type="xs:integer" minOccurs="1" maxOccurs="1" />
<xs:element name="type" type="xs:integer" minOccurs="1" maxOccurs="1" />
<xs:element name="server" type="xs:string" minOccurs="1" maxOccurs="1" />
<xs:element name="view" type="xs:string" minOccurs="1" maxOccurs="1" />
<xs:element name="zone" type="xs:string" minOccurs="1" maxOccurs="1" />
<xs:element name="fqName" type="xs:string" minOccurs="1" maxOccurs="1" />
```

(continues on next page)

(continued from previous page)

```
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

An example XML structure for a zone change script might look as follows for a zone that exists in a view:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<externalScriptParameters userName="administrator">
<object>
<id>2534</id>
<type>13</type>
<server>bind1.corp.net.</server>
<view>internal</view>
<zone>zone.com.</zone>
<fqName>bind1.corp.net.:internal:zone.com.</fqName>
</object>
</externalScriptParameters>
```

An example XML structure for a zone change script might look as follows for a zone that is not in a view:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<externalScriptParameters userName="administrator">
<object>
<id>2635</id>
<type>13</type>
<server>dns1.corp.net.</server>
<view />
<zone>my.zone.com.</zone>
<fqName>dns1.corp.net.::my.zone.com.</fqName>
</object>
</externalScriptParameters>
```

A zone content change script does not have any return value.

Scheduled Events

The administrator can configure the system to run scripts in a schedule, such as collecting a list of all users that performed at least one operation that day at midnight, etc.

To configure scheduled events:

1. On the **Admin** page, select *Configuration* in the upper-left corner.
2. Select *Event Hooks* in the filtering sidebar. In the **Scheduled events** section you can see any already defined events.
3. You can click the Actions (**...**) button to edit or delete an event. There is also an option to run the script immediately.
4. To add a new script, click *Add*. The Add Schedule Event dialog box opens.
5. Enter/select the neccessary information, and then click *Add*.
    - **Enabled**: Select the checkbox to enable the scheduling process for the script. Likewise, at any time if you wish to disable the script, return to this dialog box and clear this option.

- **Script name**: Enter the script name and necessary startup parameters. You must enter all information for the script as you would when invoking the script from the command line. It is assumed that the script is located in the same directory as the Men&Mice Central database file (mmsuite.db). If the script is stored in a different location, you must enter the path for the script.

  Example 1: Running a script named mytest.py.

  To run a script named mytest.py that is located in the Men&Mice Central directory using the python interpreter, enter `python mytest.py` in the appropriate field.

  Example 2: Running an executable named checkdata.exe.

  To run an executable named checkdata.exe that is located in the Men&Mice Central directory, enter `checkdata.exe` in the appropriate field.

  It is possible to create a special user that has permissions to run scripts. When this user exists, it is possible to execute scripts that access Micetro without having to enter a user name and password in the script itself.

  To enable this feature, create a user named ScriptRunner. This user must use the Men&Mice Internal authentication method. When this user has been created, you only have to enter $u as a user name and $p as a password when logging in to Micetro through the script.

  Note: This method only works if the script scheduler invokes the script. When running the script, Micetro uses a temporary password that changes every time the script runs. For example, you could start a python script and pass in the username and password through arguments with `python script.py $u $p`

- **Run on**: Either enter the date and time the script should run, or use the datetime picker to select the date and time.
- **Repeat every**: If this script should repeat at a desired frequency, select the checkbox. Then, in the next two fields, select the interval - for example, 1 week, 1 month, etc.

1.19.7 Address Space Management

Multiple Address Spaces

Note: For managing address spaces through the Management Console, see console-address-spaces.

Micetro supports multiple address spaces.

Each address space instance contains its own set of DNS servers, DNS zones, DHCP servers, DHCP scopes, IP Address ranges (including the IPv4 and IPv6 root ranges), IP address entries, and folders.

Note: Changes to data in one address space do not affect data in any other address space.

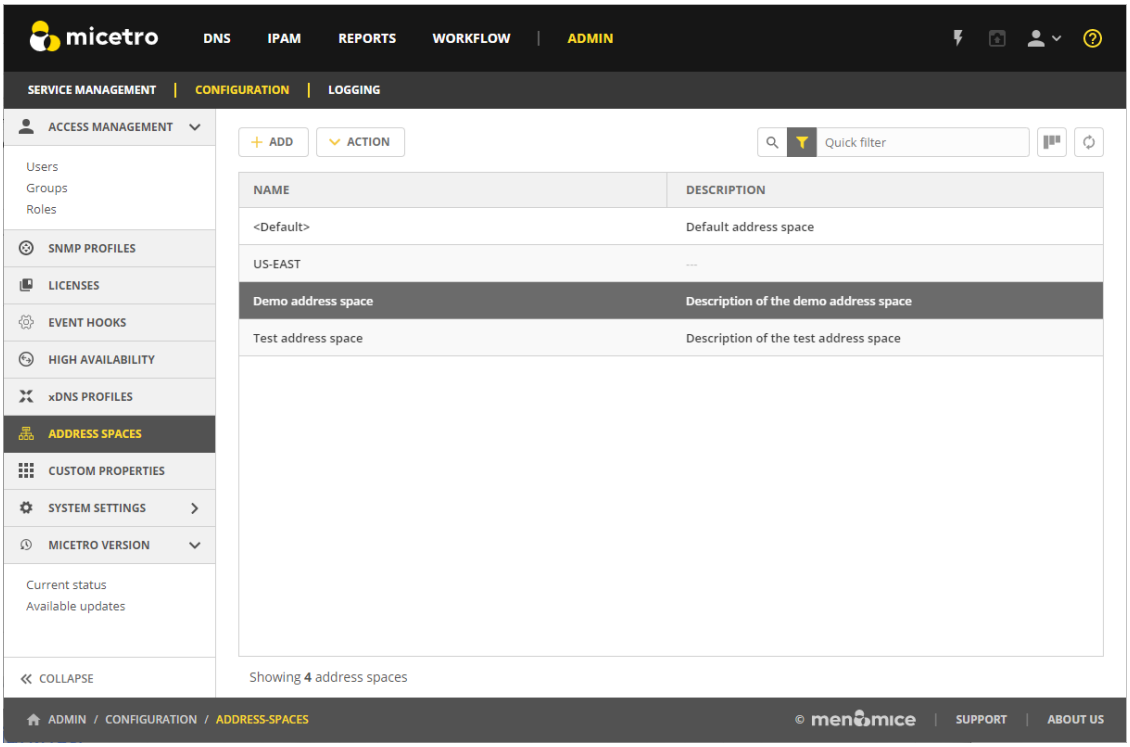
Items **shared** between address spaces are:

- users, groups, and roles
- custom property definitions (see *Custom Properties*)

Address Space Managment

Users with sufficient permissions are allowed to create, modify, or delete address spaces as well as setting access privileges for existing address spaces.

Go to *Admin* → *Configuration* → *Address Spaces*.



- To **create** a new address space, click *Add* at the top of the view, and then enter the name and description for the address space.
- To **edit** the name or description for an address space, select the address space, and then select *Edit address space* on the *Action* menu. You can also select this option on the **Row menu (…)**.
- To **delete** an address space, select the address space, and then select *Remove address space* on the *Action* menu. You can also select this option on the **Row menu (…)**.

> **Danger:** When you delete an address space, all objects contained within the address space are removed (DNS servers, DHCP servers, IP address ranges, IP address entries, and folders). This action cannot be undone.

- To **see and edit the access controls** for an address space, select the address space, and then select *Access* on the *Action* menu. You can also select this option on the **Row menu (…)**.

Note: The first address space is always named `<default>`. It is not possible to rename or delete the *<default>* address space.

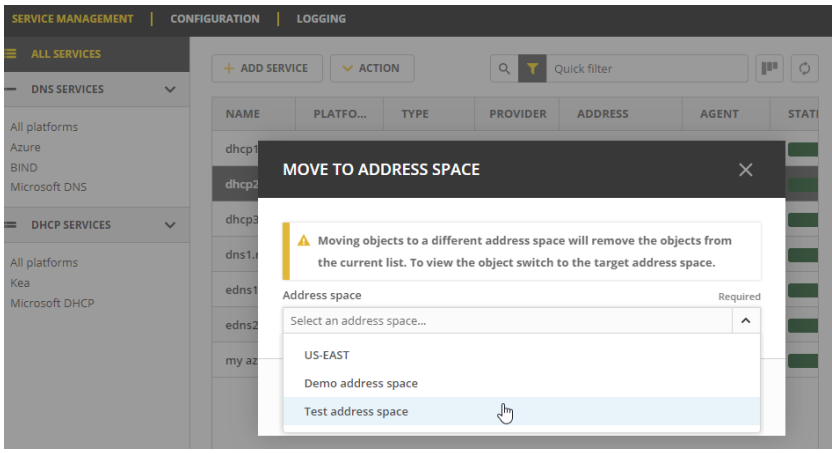
The <*default*> address space is the only address space that shows AD sites if *AD Site and Subnet* integration is enabled.

Moving Objects to a Different Address Space

You can move DNS servers, DHCP servers, and IP Address ranges between address spaces. When an object is moved between address spaces, all properties for the object are retained, including its access settings and change history. You must have the relevant administrator privileges to move objects to a different address space.

To move an object:

1. Select the object you want to move, and then select *Move to address space* on the *Action* menu. You can also select this option on the **Row menu (...)**.
2. Select a different address space in the dropdown list, and then click *Confirm*.

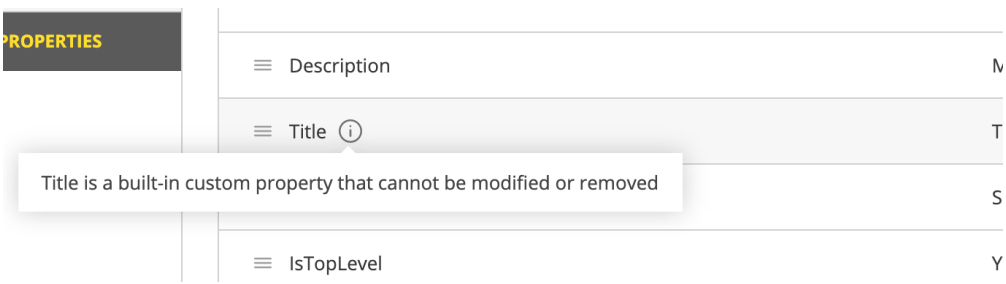


Note: Moving servers in an xDNS profile to separate address spaces, is NOT supported in the Web app. This is also not possible for DHCP servers in a failover relationship.

1.19.8 Custom Properties

As an administrator, you may find that it is necessary to create some custom properties. These properties are used for entry of any data that you feel is relevant for an object. For example, if you want to specify a server is in a specific location, or indicate who is responsible for a particular server, etc. Custom properties can be defined for various object types.

There are two Default Custom Properties built in to the Range object, Title and Description, which may not be changed.



In addition, various properties can be set when working with custom properties objects under DNS, DHCP, and IPAM.

Adding a Custom Property

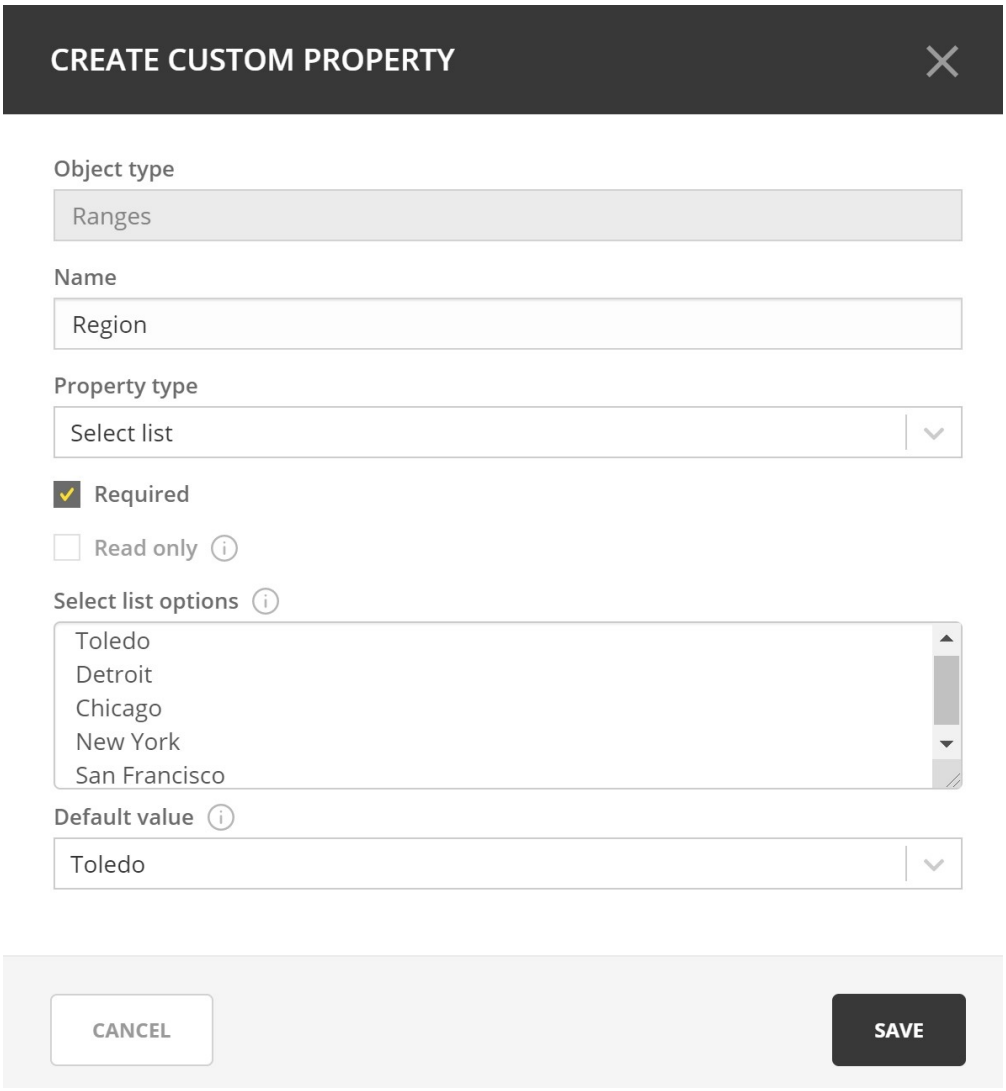
1. Go to *Admin*
2. Click on *Configuration*
3. Select *Custom Properties*
4. Select the object type for which you'd like to create a new custom property
5. Click the action button on the right or the *Add Custom Property* button at the bottom of the property list
6. Specify the name of the new property
7. Fill in the details:

Name:
Type a name for this custom property.

Property Type:
Set the type for the property. By default, "Text" is selected. Click the drop-down list and select the desired property type - e.g., Text, Multiline, Select List, Yes/No, IP Address, or Number.

Required:
When selected, a user must enter a value in this field. If you select this option, you cannot select "Read only."

Read only:
When selected, the field is locked for editing. If you select this option, you cannot select "Required"



8. Enter the appropriate list options and values depending on the property type.
9. Click *Save*

Adding a Cascading List to an Existing List

In some situations nested lists will be necessary, for example when requesting location identity information.

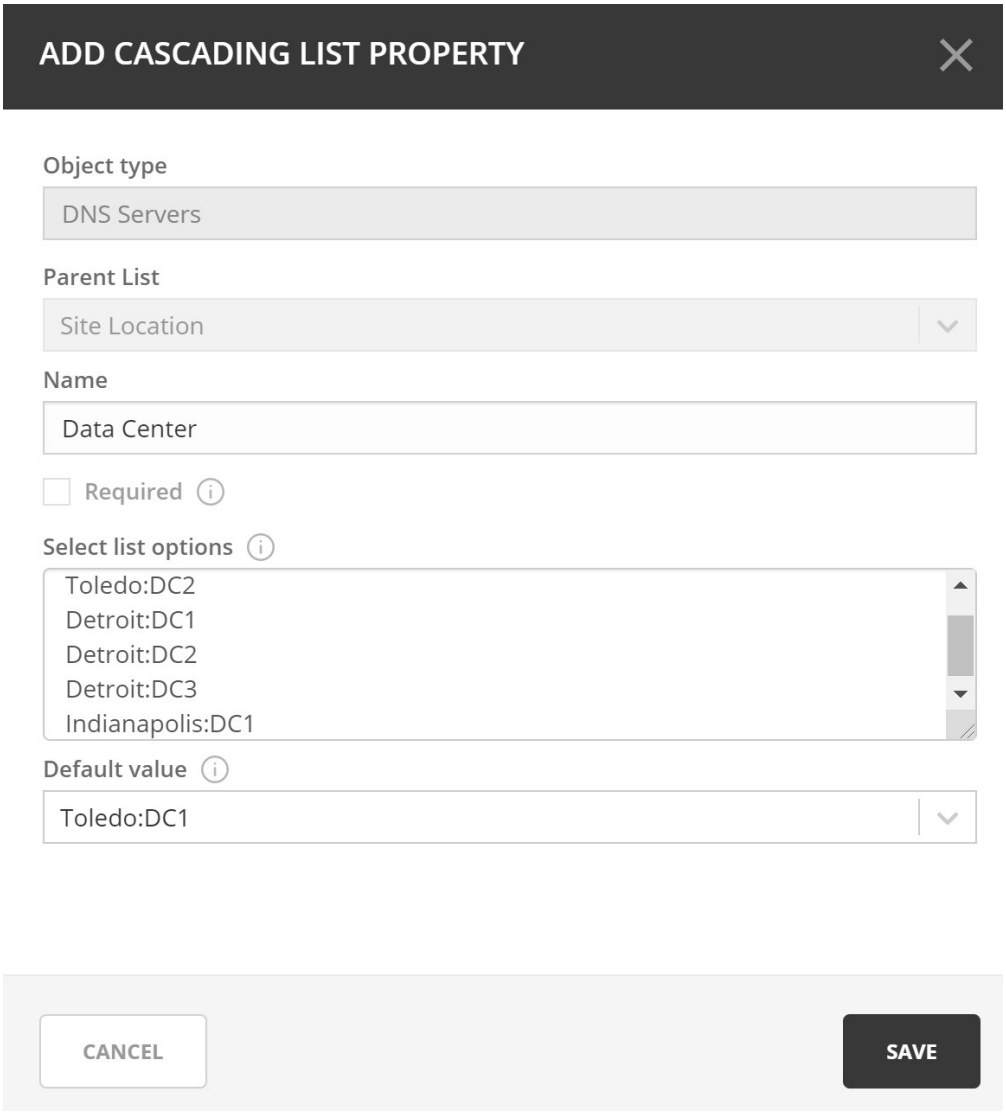
1. Go to *Admin*
2. Click on *Configuration*
3. Select *Custom Properties*
4. Hover over the parent custom property
5. Select *Add Cascading List Property*
6. Fill in the appropriate details in the proper format, where the parent option comes first.

For example:
Site1:DC2

Site1:DC3

Site2:DC1

Site2:DC2

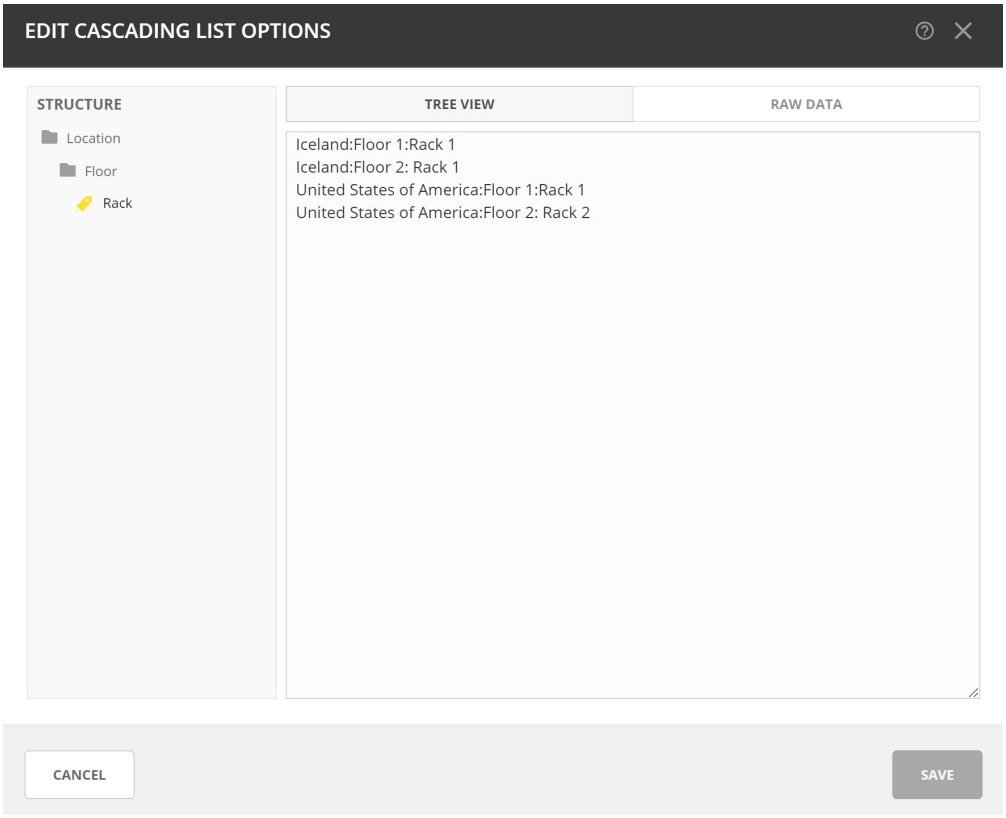


Editing Cascading List Options

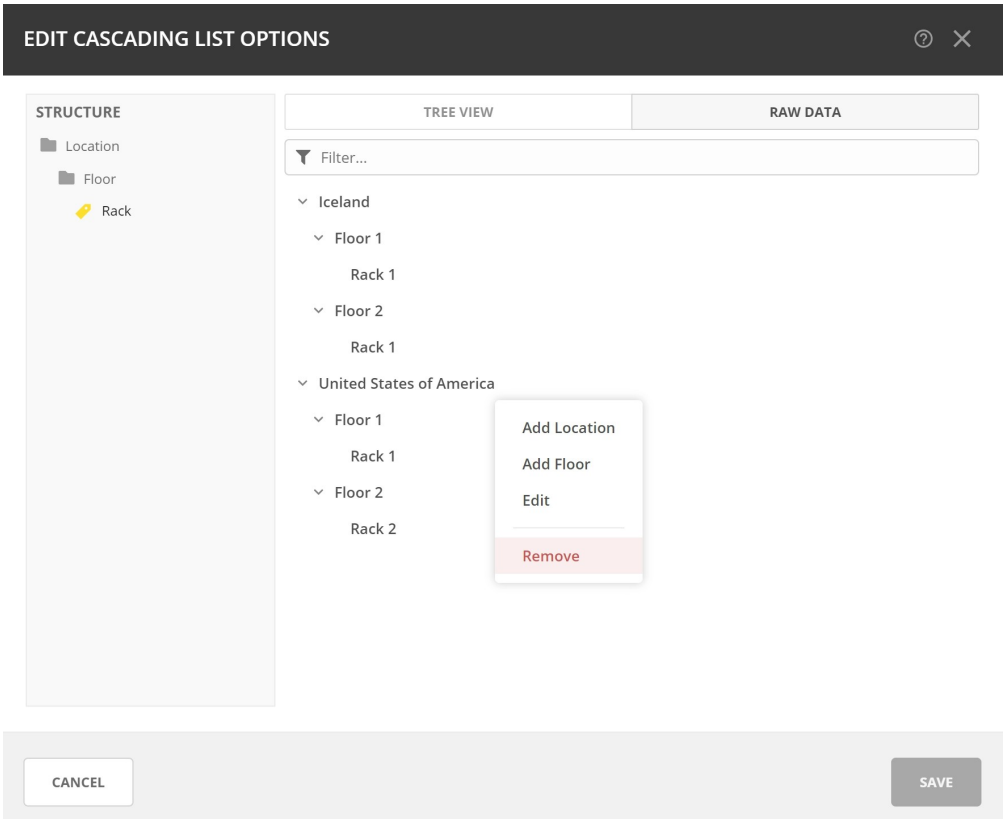
Once cascading list properties have been added to a list you may now edit the list using either *Tree View* or *Raw Data*

1. Click on the meatball menu
2. Select *Edit cascading list options*

The *Raw Data* view may be edited manually, though is most useful when copying and pasting information from an existing CSV document or spreadsheet. The values must be separated by colons with the top level value appearing first before the child. You may have multiple nested lists.



The *Tree View* is useful when editing the nested lists manually. Here you may add, edit, or remove values for each nested list. The *Structure* menu on the left shows which levels are available, with the bottom level, or child list, showing a yellow tag next to it.



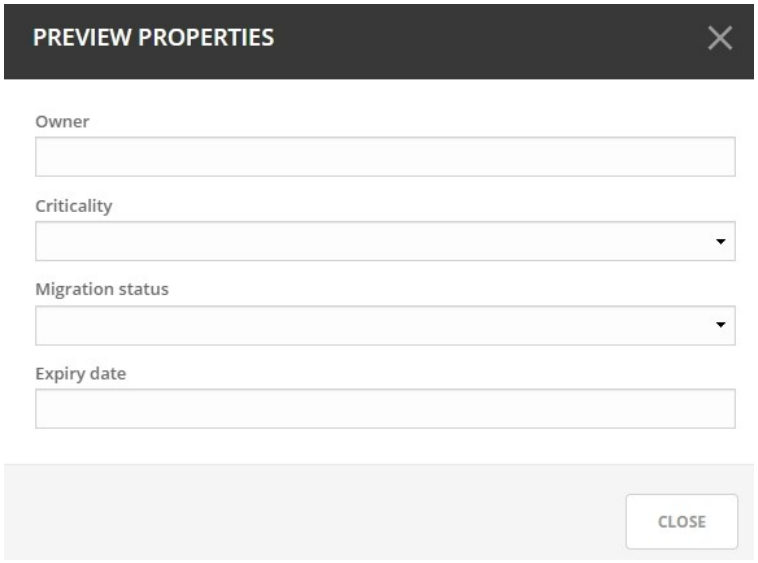
You may also use the *Filter* to narrow down the available options to make it easier to modify the values. You may modify the values within the filtered view.

Note: For complex cascading lists, where there is more than one child property of the same parent, you may only edit one options list at a time.

Reordering Custom Properties

The order in which the custom properties appear in this list will determine the order in which the property fields are displayed in the dialog box when creating or editing the respective object. You may get a preview of the order of fields which will appear in the dialog box by clicking on the preview button (or the eye icon) in the upper right corner as shown in the top picture below.

After clicking on the eye icon, you will see the preview such as the following image



1. Go to *Admin*
2. Click on *Configuration*
3. Select *Custom Properties*
4. Click on the object type for which you'd like to change the property order
5. Click on the pencil (edit) icon on the right
6. Drag the custom properties to the appropriate order

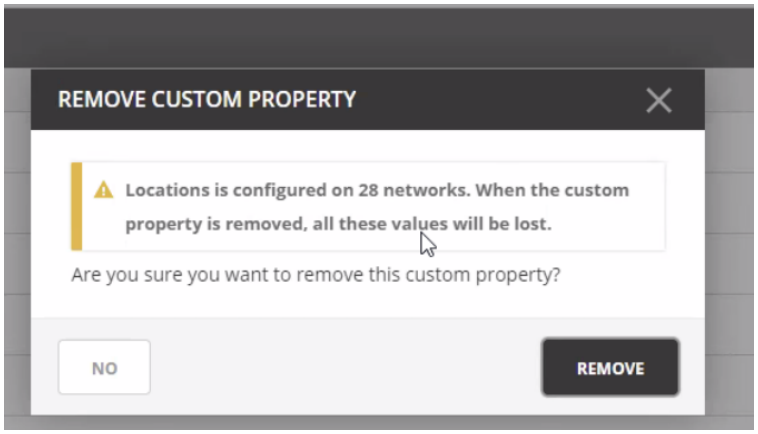
Editing a Custom Property

1. Go to *Admin*
2. Click on *Configuration*
3. Select *Custom Properties*
4. Hover over the Custom Property to change
5. Click the ellipsis (meatball) menu and select *Edit Property*

Deleting a Custom Property

!DANGER!

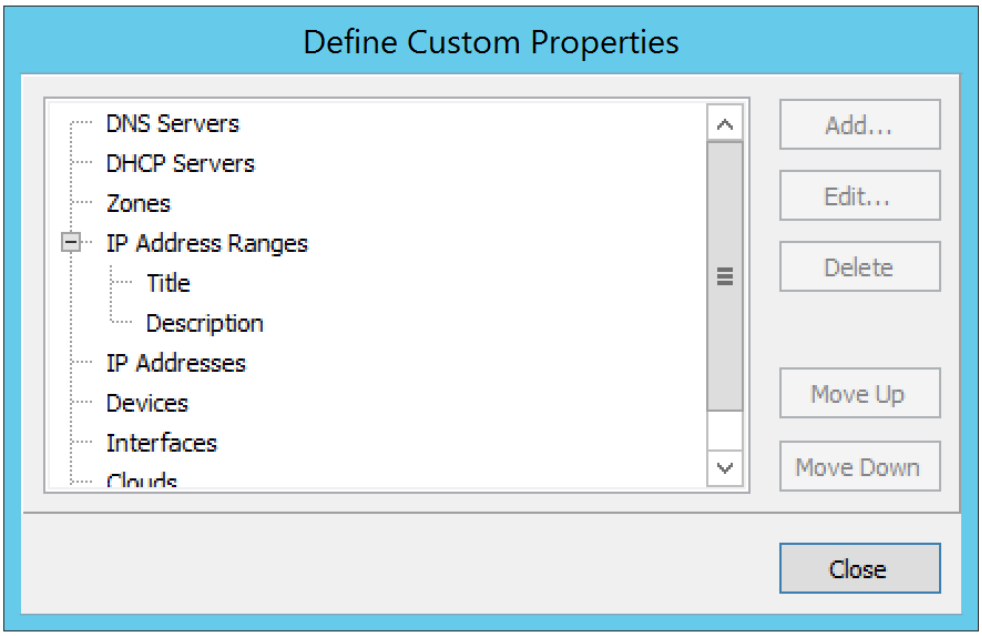
When a custom property is removed that data will be lost for all of the objects on which it was configured.



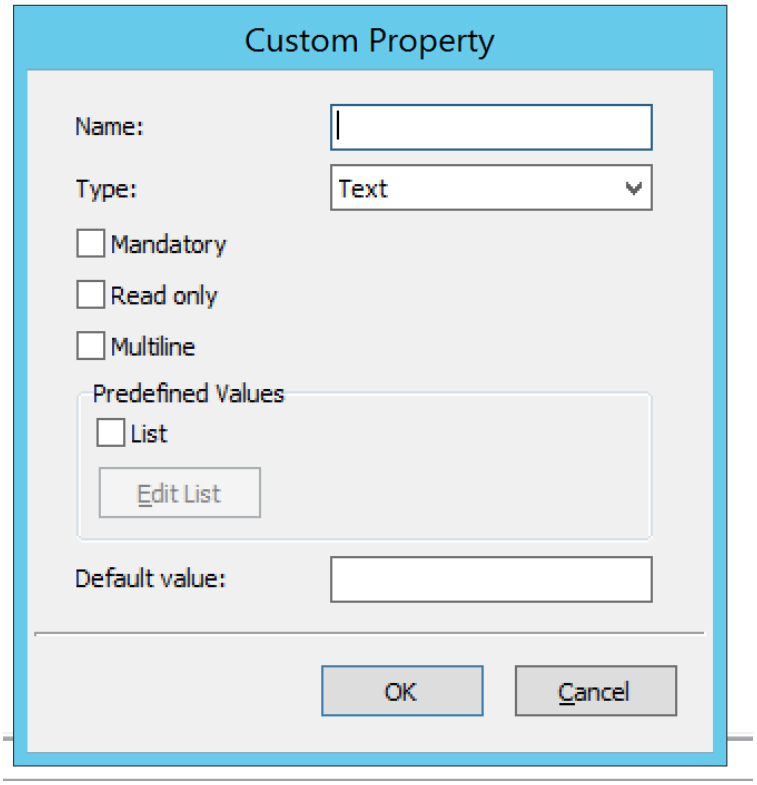
1. Go to *Admin*
2. Click on *Configuration*
3. Select *Custom Properties*
4. Hover over the Custom Property to change
5. Click on the ellipsis (meatball) menu and select *Remove Property*

Adding a Custom Property (Management Console)

1. From the menu bar, select *Tools* → *Define Custom Properties*. The *Define Custom Properties* dialog box displays.



2. Select the object type to which you want to add a custom property.
3. Click the *Add* button. The *Custom Property* dialog box displays.



4. Fill in the details:

Name.
Type a name for this custom property.

Type.
Set the type for the property. By default, "Text" is selected. Click the drop-down list and select the desired property type - e.g., Text, Yes/No, IP Address, or Number.

Mandatory.
When selected, a user must enter a value in this field. If you select this option, you cannot select "Read only."

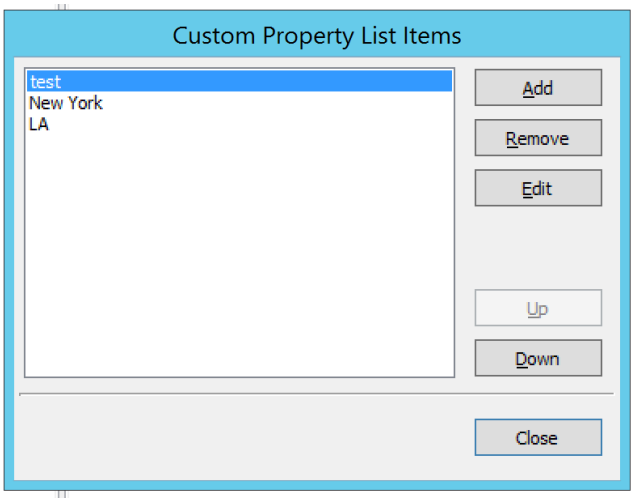
Read only.
When selected, the field is locked for editing. If you select this option, you cannot select "Mandatory."

Multiline.
When selected, the edit field contains multiple lines for entry. If you select this option, you cannot select "List."

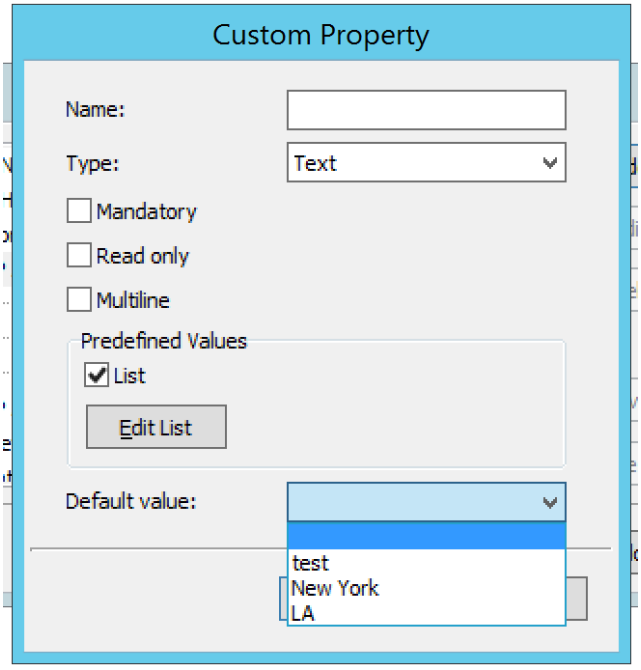
Predefined Values.
When selected, the field displays as a drop-down list. Click the checkbox for List. Then click the Edit List button. The Custom Property List Items dialog box through which you can add, edit, and remove custom properties displays.

Note: If you select this option, you cannot select "Multiline".

- To ADD an item for this property, click Add. The Custom Property List Items dialog box displays.



- Type the item in the field provided.
- Add any additional items. You can move items Up and/or Down in the list, as desired. This designates the order in which they appear in the list.
- Then click *OK*. When you return to the *Custom Property List Items* dialog box, the items entered are shown.



- To edit/remove any values, click Edit List and make the necessary changes.
- When all selections are made, click *OK*.

Default value.
Specifies the default field value to use when an object is created. This field is only a drop-down list if the 'List' checkbox is selected; otherwise, it is an edit field.

5. When all selections/entries are made, click *OK*. When you return to the *Define Custom Properties* dialog box, the new field is shown.

6. If there are multiple custom properties for an object, use the Move Up/Move Down arrows to change the order in which this display in the object window.
7. When all fields are added, click the *Save* button.

Editing a Custom Property (Management Console)

To edit a custom property, do the following:

1. From the menu, select *Tools* → *Define Custom Properties*.
2. Locate and highlight the property to be edited.
3. Click the *Edit* button.
4. Make the necessary changes.
5. Click *OK*.

Deleting a Custom Property (Management Console)

To delete a custom property, do the following:

1. From the menu, select *Tools* → *Define Custom Properties*.
2. Locate and highlight the property to be deleted.
3. Click the *Delete* button.
4. When the confirmation message displays, click *Yes*.
5. Click *OK*.

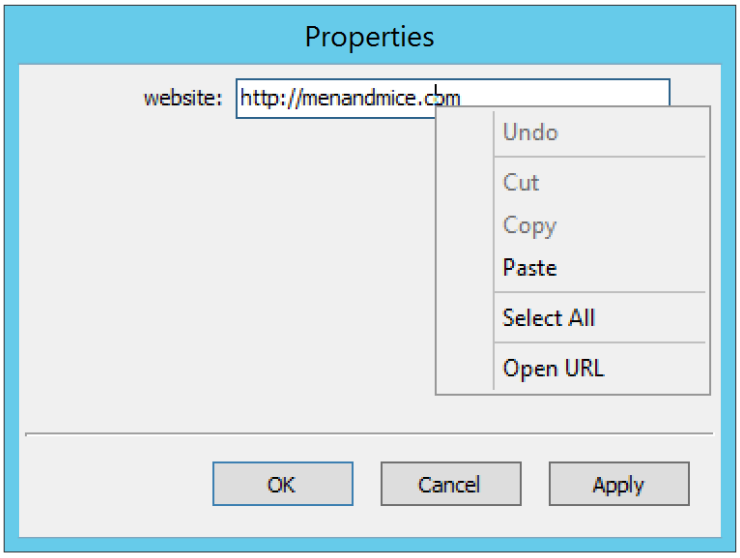
Displaying a Custom Property (Management Console)

Once a custom property has been defined, it is possible to view and edit its contents by opening the Properties dialog for any object of the type for which the custom property has been defined.

Opening a Custom Property URL (Management Console)

Anytime you have specified a URL within a custom property, you can use this option to open the URL.

1. Locate the item containing the URL.
2. Right-click and, from the shortcut menu, select *Properties*.
3. In the *Properties* dialog box, move to the field containing the URL.
4. Place the cursor anywhere in the field and right-click.
5. From the shortcut menu, select *Open URL*.

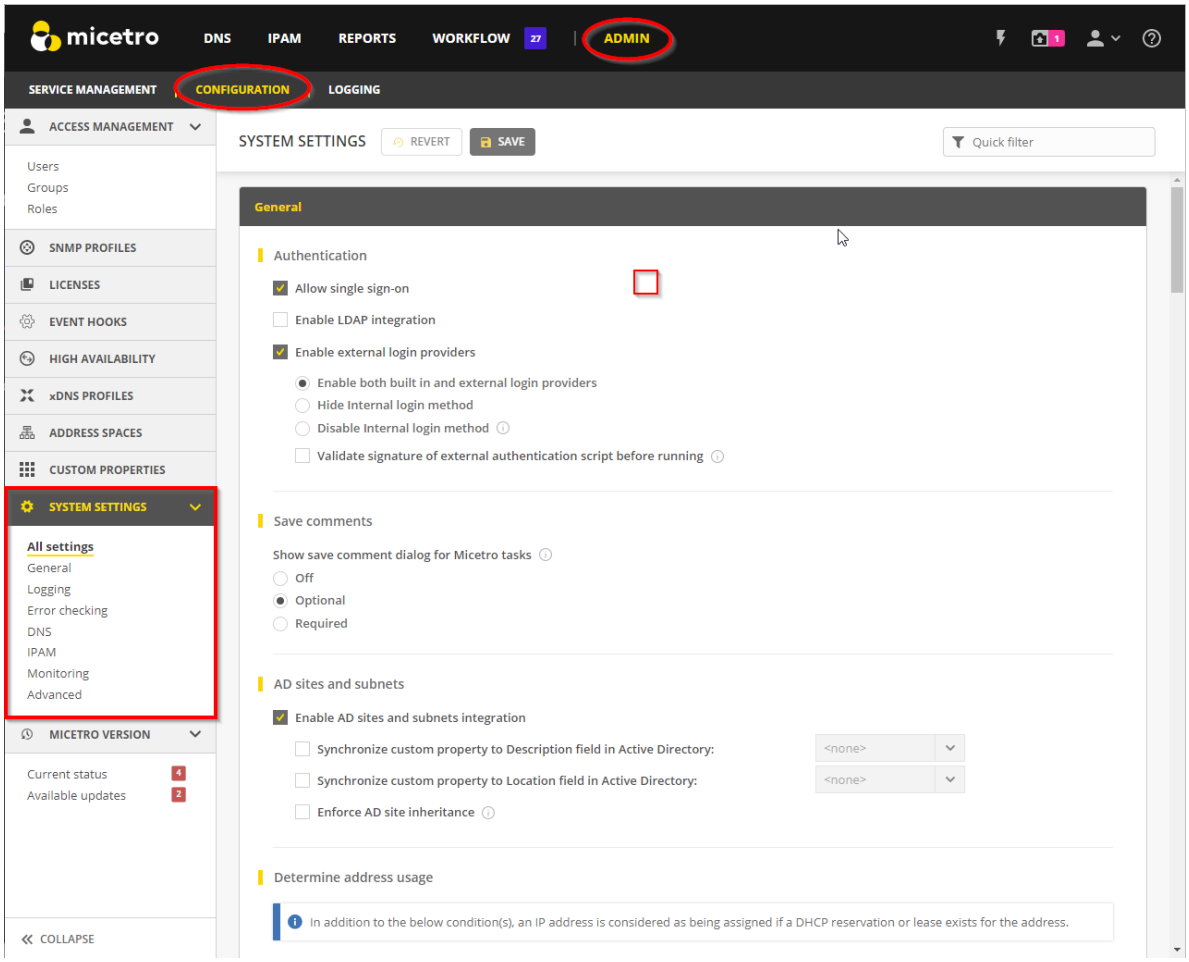


6. Your browser will open and the web site for the URL displays.

1.19.9 System Settings

To access the System Settings:

1. On the **Admin** page, select *Configuration* in the upper-left corner.
2. Browse the categories under *System settings* in the filtering sidebar to find what you're looking for.



The System Settings include the following categories:

- *General*
- *Logging*
- *Error checking*
- *DNS*
- *IPAM*
- *Monitoring*
- *Advanced*

General

Use the General settings to specify the following:

- Authentication methods
- Save Comments for Micetro
- Settings for AD Sites and Subnets integration
- Rules to determine when an IP address is considered as being in use

Authentication

Configure authentication methods, including single sign-on, LDAP integration, and external login providers.

When **single sign-on** is activated, users do not have to authenticate when logging in through the Management Console or the Command Line Interface. For more information about Single sign-on, see *External Authentication*.

Save comments

By default, users can save changes in the system without writing a comment. Here you have the option to set the comment requirements for Micetro tasks, including options to turn off the save comment dialog box, make it optional, or require it.

- When **off** is selected, the save comment dialog box will not appear when users save changes.
- If you choose to make comments **optional**, users can choose whether or not to include a comment when saving changes.
- If you choose to make comments **required**, users will need to include a comment whenever they save changes.

AD sites and subnets

Enable AD sites and subnets integration
: When selected, all AD sites and their corresponding subnets will be displayed in Micetro, and you can add and remove subnets from sites and move subnets between different sites as needed. AD sites and subnets will be listed on the **AD Sites** menu on the IPAM page.

  If you want to synchronize the Location and Description fields of the subnets in Active Directory with custom properties in Micetro, choose the desired custom properties to synchronize against. When synchronization is active, any changes made to the fields in Active Directory will automatically update the corresponding fields in Micetro, and vice versa. See *AD Sites and Subnets*.

Enforce AD site inheritance.
: Select this checkbox if you want to enforce site inheritance in AD. When site inheritance is enforced, child subnets must reside in the same site as the parent subnet. If site inheritance is not enforced, child subnets can be placed in different sites than the parent subnet. See *AD Sites and Subnets*.

Determine address usage

Control how IP addresses are identified as being in use. By default, these settings are all selected. To specify which rules should be applied to IP addresses and get a more granular picture of where the usage is coming from, select/clear the appropriate checkboxes.

Logging

The Logging settings allow you to specify when log messages should be deleted and whether lease history for DHCP servers should be collected.

Micetro log

Logging level for Micetro Central (1-6)
Determines the level of detail to log when logging the output of Micetro Central to a file.

Log file for Micetro Central
Specifies the path and name of the log file to use when you want to log the output of Micetro Central to a file.

Purge log message after (# of days)
Enter the number of days the logs should be kept before they are deleted.

Log extra information when address collection is triggered
When selected, information about the start and duration of the address collection is written in the Micetro log file.

Lease history

Here you can select to start collecting lease history for DHCP servers. By viewing the DHCP lease history, you can quickly identify any potential issues or conflicts.

You can specify the number of days to keep the history before it is deleted, and if you want to save the history to a comma separated text file before it is deleted, enter a name for the file in the **Flush lease history to file before purging** text box.

Error checking

In this section you can specify how the system reports certain errors related to DNS.

Stop A/AAAA records from being created if the name already exists
This setting prevents the creation of A/AAAA records when a name already exists in the system. This can be useful for avoiding conflicts or overwriting existing records in the DNS configuration.

Ignore missing reverse zones.
An error message displays when Micetro is unable to update a reverse record for a changed address record. It is possible to suppress this error message if no reverse zone exists for the given address record by selecting this checkbox.

DNS

Use these settings to specify various DNS related settings.

Delegation records

When activated, Micetro will automatically create delegation records (NS records) in the corresponding parent zones whenever subzones are created. This ensures that the delegation chain between parent and subzones is maintained correctly.

Adjust zone transfer

Allow Micetro to automatically adjust zone transfer settings on Microsoft DNS servers to enable management of dynamic and Active Directory integrated zones.

DNSSEC

Include derived DNSSEC records when viewing DNSSEC signed zones in Micetro. Note that this will significantly increase the size of the Micetro database and may affect overall system performance.

IPAM

Specify various IPAM related settings:

- How the system should handle new subranges if the parent range is in a folder.
- How the system should behave when naming conflicts between existing IP Address ranges and DHCP scopes occur.
- How the system should behave if DHCP scopes are removed outside Micetro.
- Whether the system should allow reservations inside address pools on ISC DHCP servers.

Subranges
The selection made here determines what happens when a user creates a subrange of a range in a folder.

Name conflicts between ranges and scopes
Specify what happens if the name of an MS DHCP scope does not match the name of an existing IP address range.

Apply same rule for scope description as for scope name above.
When selected, the system will use the same rules to update scope description as it does for updating scope names.

Allow reservations inside pools on ISC DHCP servers.
When selected, the system allows users to create reservations inside pools on ISC DHCP servers. When a reservation is created inside a pool, the pool is split to make space for the reservation.

> **Warning:** If a reservation that has been created inside a pool is deleted, the address is not made a part of the pool again.

Allow allocation of IP addresses from IP Address Containers
When selected, the system will allow allocation of IP addresses that reside in IP address Containers. For more information on IP address Containers, refer to *Containers*.

Disable scanning of VRF information
By default, the system does not scan for VRF information. If you clear the checkbox, the system will begin scanning for VRF information. If an overlap is found between different VRFs, the system will log the issue.

Always show discovery info
Determines whether the columns related to host discovery should always be displayed when viewing contents of subnets or scopes.

Monitoring

Use the *Monitoring settings* dialog box to specify various monitoring related settings.

Subnet monitoring

Enable subnet monitoring
When enabled, thesystemmonitors the free addresses in DHCP address pools and subnets and performs an action if the number of free addresses goes below a user-definable threshold. For further configuration, see *Subnet Monitoring Events*.

Note: The global subnet monitoring setting can be overridden for individual subnets by changing the setting explicitly for the subnet. Refer to IP Address Management—Subnet Monitoring and Utilization History for information on how to change monitoring settings for individual subnets.

When subnet monitoring is enabled, a new column, Monitoring, displays when viewing the subnet list. To quickly see all subnets that are monitored, you can use the Quick Filter and filter by this column by entering "Monitor: Yes" in the Quick Filter search field.

Note: Only DHCP scopes that are enabled are monitored. Disabled scopes are ignored.

When subnet monitoring is enabled, you must specify the mail server and the sender e-mail address to use if you want the subnet monitor to send an e-mail. Place the appropriate information in the SMTP Server and Mail from fields.

Enable sending SNMP traps.
When enabled, the system will send SNMP traps when certain events occur:

- When the number of free IP Addresses in monitored subnets goes below a user-definable threshold.
- When a log event of type Error or Notice occurs. Refer to *Logging* for more information on log events.

When enabling sending of SNMP traps, you must provide additional information:

- **Manager name**
  Enter the host name of the computer that should receive the SNMP traps.
- **Manager port**
  Enter the port number the Manager uses for the SNMP traps.
- **Community**
  Enter the community string (password) to use for the SNMP traps.

Service monitoring

When selected, the monitoring tool monitors the DNS and DHCP services on their respective servers. Decide on an appropriate interval for monitoring.

Advanced

Here you can configure advanced system settings, such as specifying a SSL Certificate policy.

Setting	Description
SSL	
SSL Certificate policy	Determines the SSL Certificate policy applied to the Cloud Integration feature and update checks.
Path to SSL Certificate Authority file or directory	Specifies the path to the SSL Root certificate used by the SSL Certificate policy.
SOA record defaults in new zones	
TTL of SOA record	Specifies the default TTL (Time to Live) value to use for the SOA record of new zones.
Hostmaster	Specifies the default value to use for the Hostmaster field in the SOA record of new zones.
Refresch	Specifies the default value to use for the Refresh field in the SOA record of new zones.
Retry	Specifies the default value to use for the Retry field in the SOA record of new zones.
Expire	Specifies the default value to use for the Expiry field in the SOA record of new zones.
Negative caching (BIND)	Specifies the default value to use for the Negative Caching field in the SOA record of new zones. Only applicable for zones on BIND DNS servers.
Minimum TTL (MS)	Specifies the default TTL (Time to Live) value to use for the TTL field in the SOA record of new zones. Only applicable for zones on Microsoft DNS servers.
Web proxy	
Web proxy to use	Specifies a proxy server to be used for outgoing connections for checking for updates and additionally for AWS cloud services.
Web proxy port (defaults to port 80)	Specifies the port of the proxy server to be used for outgoing connections for checking for updates and additionally for AWS cloud services.
Password for web proxy authentication	Specifies a cleartext password for proxy sign in.
Use web proxy settings when connecting to AWS	If selected, the proxy settings configured will be used for connections to AWS.
Directory for scripts that can be run from the API	Specifies the directory that contains scripts that may be run from the API.
Log performance of API calls	Determines whether execution time of API calls should be logged. Mainly used for diagnostic purposes.
Time in minutes between write-outs of API call performance log	If logging of API query performance is enabled, this setting specifies how frequently the log should be written to disk.
Automatically adjust local zone transfer settings for BIND	When enabled, BIND can automatically optimize the settings related to local (within your network) zone transfers.
Automatically create reverse (PTR) records	When selected, Micetro automatically creates reverse (PTR) records. PTR records are used for reverse DNS lookups, which are used to resolve an IP address to a domain name.
Perform backup of MS and ISC DHCP servers	Determines whether to perform a backup of Microsoft (MS) and Internet Systems Consortioum (ISC) Dynamic Host Configuration Protocol (DHCP) servers.
Default TTL to use for DNS records created in zones for all xDNS profiles	Specifies the default TTL (Time to Live) value to use for DNS records created in zones for all xDNS profiles.
Disable all health checks	If selected, all health checks will be disabled.

continues on next page

Table 11 – continued from previous page

Setting	Description
Disable collection of statistical information	Select to stop the collection of statistical information.
Use Azure activity log to optimize DNS synchronization	When enabled, the Azure activity log is monitored for events related to DNS changes, and those changes are synchronized with the DNS server in real-time.
Use AWS CloudTrail events to optimize DNS synchronization	Determines whether AWS CloudTrail events should be used to optimize DNS synchronization.
IP ranges/scopes inherit access by default	When you create a new IP range or scope, it will ineherit all access bits form its parent by default. If you want to change this behavior, clear this checkbox.
Maximum number of blocks that can be temporarily claimed	Limits the number of blocks that can be temporarily reserved or allocated for use by a specific user.
Enable collection of IP information from routers	Determines whether the system can collect IP information from the ARP cache of routers. If selected, the system can collect this information.
Timeout in seconds for named-checkconf	Specifies the timeout value in seconds for named-checkconf files.
Synchronize DNSSEC signed zones immediately after editing	Determines whether DNSSEC signed zones should be synchronized immediately after they are changed. If selected, the zones are synchronized immediately.[1]
Use case sensitive comparison when updating custom properties from scripts	Specifies whether to take case sensitivity into account when comparing custom properties from scripts.
Include A/AAAA records when checking for *Edit apex records* access	Determines whether A and AAAA records are considered when verifying access to edit apex (root) records.
Web app landing page	By default, the Micetro frontpage is the landing page for the system. Clicking the Micetro logo will take you to the landing page.
Web app server host	Used to specify which host the web application is running on in order for auto update to work for the web application. Default is localhost (same server as Men&Mice Central)

1.19.10 Viewing Global Object History

Note: This information applies to the web interface. For information about change history in the M&M Management Console, see *Object Change History*.

Permission:

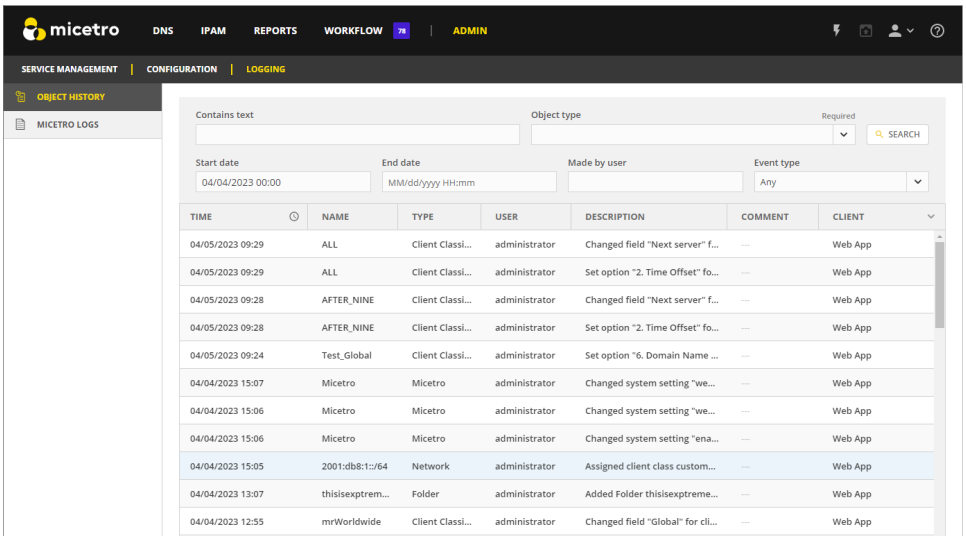
- Permission: `Access to view history` on Micetro
- Role: `Administrators (built-in)`

On the **Object History** tab of the **Admin** page you can view global object history and log messages generated by Micetro.

You can see a log of all changes made to any object, including the date and time of the change, the name of the user who made it, the client used, actions taken, and any comments entered by the user.

[1] Enabling this feature can affect the performance of the system.

1. On the **Admin** page, select the *Object History* tab.
2. Use the search options to filter the results.



- When searching for a change log, you must narrow your search down by *Object type* to make the search more efficient.
- Use *Made by user* to view changes by a specific user.

1.19.11 Configure Single Sign-On

The single sign-on feature in the Men&Mice Web Application allows users to sign in to the web using their active directory credentials.

Note: This article assumes that both an Active Directory group has already been added to Micetro **and** Kerberos/NTLM has been added to the preferences file for Men&Mice Web Services.

Note: For help adding active directory groups to Micetro, see *External Authentication*.

Note: For help adding Kerberos/NTLM to preferences for Men&Mice Web Services, see *API Authentication methods*.

Configuration

1. Make sure the user is a member of the Active Directory group already added to Micetro.
2. Log in to the workstation as the user.
3. Open up Internet Explorer, click the settings button and select *Internet options*.
4. On the *Security* tab, select *Trusted Sites* and open up the *Sites* window.
5. Enter the URL (i.e. https://micetro.example.com) of the Men&Mice Web Application into the **Add this website to the zone** field, and then click *Add*.

Note: It is necessary to clear the *Require server verification for all sides in this zone* checkbox if the Men&Mice Web Application is not running on https.

6. In Internet Options, click *Custom Level* to open *Security Settings → Trusted Sites Zone*.
7. Make sure that under *User Authentication → Logon* the *Automatic logon with current username and password* is selected.
8. Open a web browser[1] that supports Single Sign-On (SSO) and navigate to the Men&Mice Web Application.
9. Enter the FQDN/IP Address of the Men&Mice Central server.
10. Select *Log in with Single Sign-on*, and then click *Log In*.

1.19.12 Maintenance

Micetro contains several options for cleaning up the network space. To access the network maintenance functions, select *Tools → Maintenance* and then the maintenance operation you want to perform.

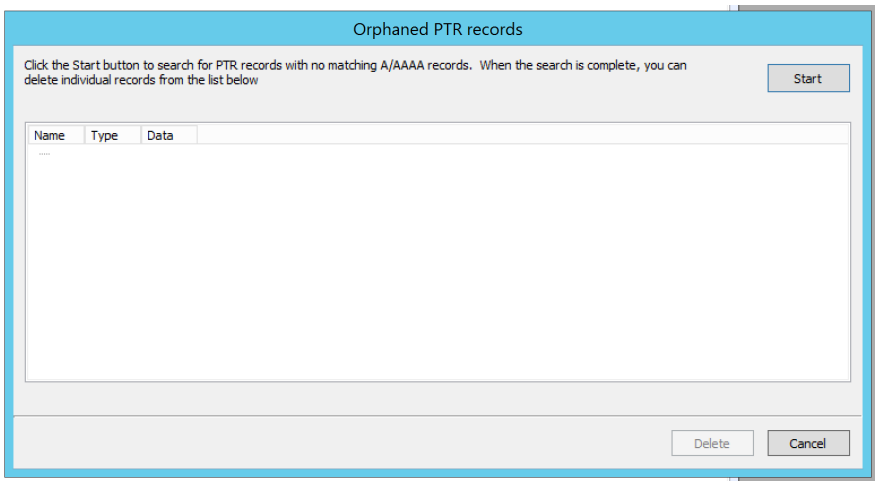
Find Orphaned PTR Records

The *Find Orphaned PTR Records* maintenance operation allows you to see and remove orphaned PTR records in reverse zones. PTR records that have no corresponding address (A) records in the system are considered orphaned.

To find and remove orphaned PTR records, do the following:

1. Select *Tools → Maintenance → Find Orphaned PTR Records*. A dialog box displays.
2. Click *Start* to start looking for orphaned PTR records.

Note: Due to the fact that the result could be a large number of records, there is now a limit of 1000 records being shown.



3. Select the PTR records you want to remove, and click the *Delete* button. The selected PTR records are removed.

[1] Single Sign-On is only supported in Google Chrome.

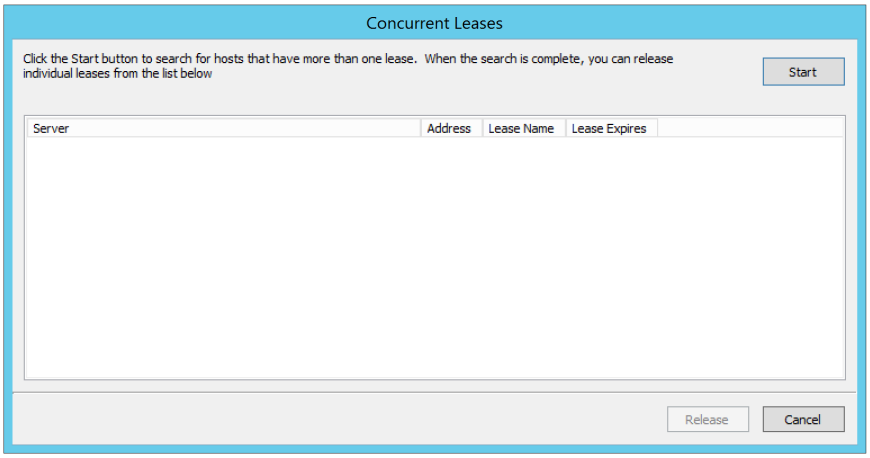
Find Concurrent Leases

The *Find Concurrent Leases* maintenance operation allows you to see and release concurrent DHCP leases. Concurrent DHCP leases are multiple active leases that are assigned to the same MAC address.

To see and remove concurrent DHCP leases, do the following:

1. Select *Tools* → *Maintenance* → *Find Concurrent Leases*. A dialog box opens.
2. Click *Start* to start looking for concurrent DHCP leases.

Note: Finding all concurrent leases might take a while in large environments.



3. Select the leases you want to release, and click the *Release* button. The selected leases are released.

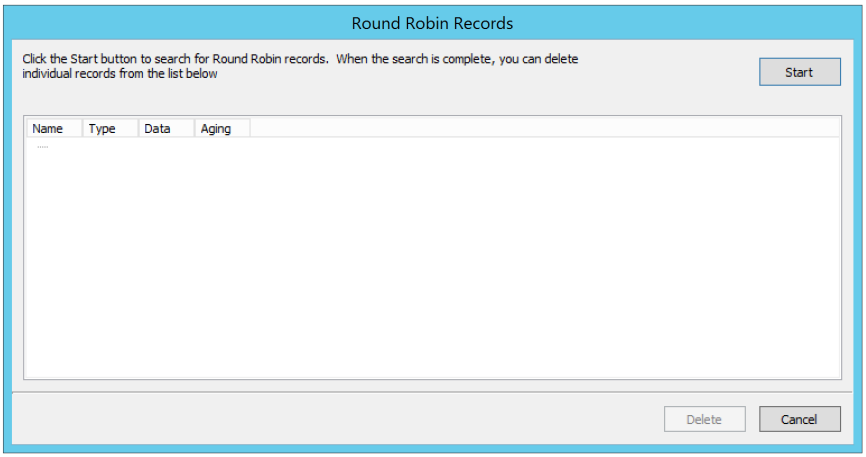
Show Round Robin Records

The *Show Round Robin Records* maintenance operation allows you to see and delete round robin DNS records. Round robin records are multiple address (A / AAAA) records with the same name.

To see and remove round robin records, do the following:

1. Select *Tools* → *Maintenance* → *Show Round Robin Records*. A dialog box displays.
2. Click *Start* to start looking for round robin records.

Note: Finding all round robin records might take a while in large environments.



3. Select the records you want to delete and click the *Delete* button. The selected records are deleted.

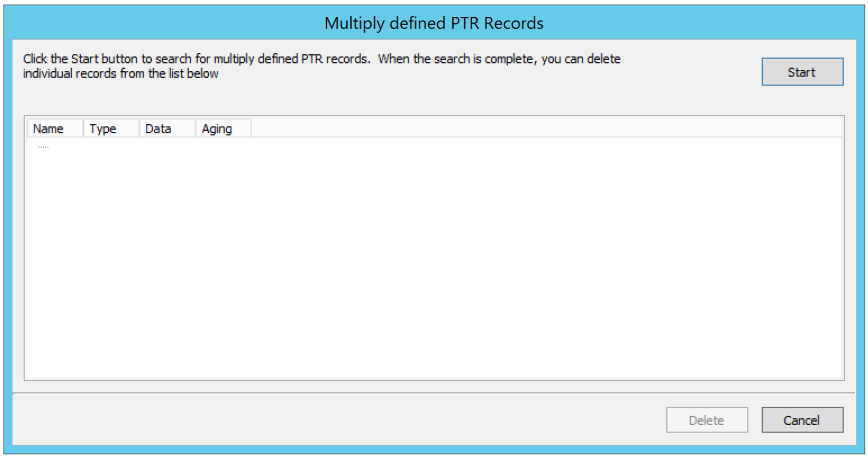
Show Multiply Defined PTR Records

The *Show Multiply Defined Records* maintenance operation allows you to see and delete multiply defined PTR records. Multiply defined PTR records are multiple PTR records with the same name.

To see and remove multiply defined PTR records, do the following:

1. Select *Tools* → *Maintenance* → *Show Multiply Defined PTR Records*. A dialog box displays.
2. Click *Start* to start looking for multiply defined PTR records.

Note: Finding all multiply defined PTR records might take a while in large environments.



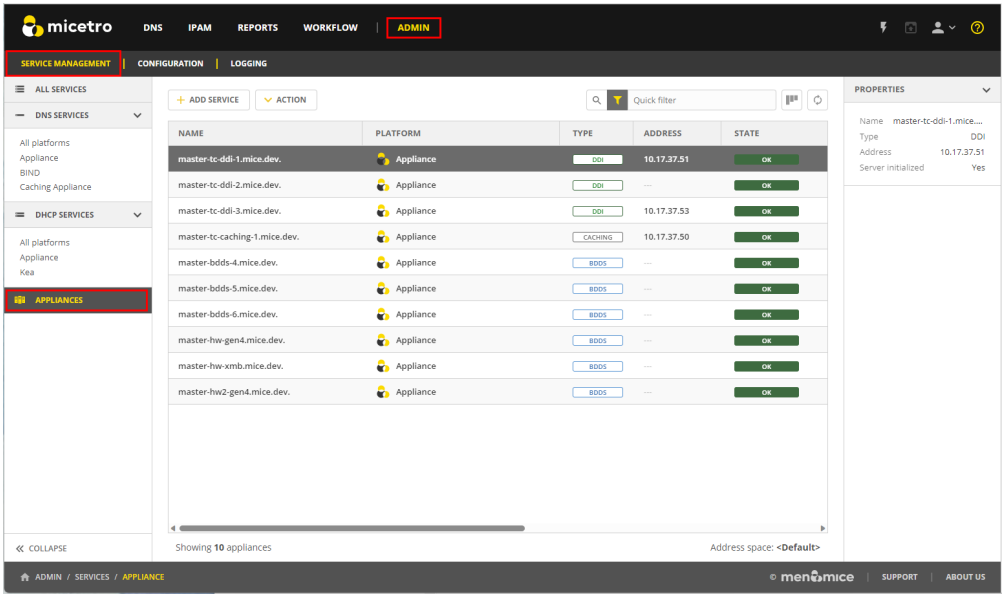
3. Select the records you want to delete, and click the *Delete* button. The selected records are deleted.

1.19.13 Integrating and Managing Appliances

Micetro seamlessly integrates with compatible DNS/DHCP appliances, available in both hardware and virtual machine configuration. By integrating Micetro with appliances, you gain the power to effectively manage services, optimize deployment processes, and oversee day-to-day server operations, all through the intuitive Micetro user interface.

Once you have configured your appliance and added it to your *Service Management*, you can interact with the services just as you would with other DNS and DHCP services within Micetro.

Appliances are accessed and managed in *Service Management* on the *Admin* page.

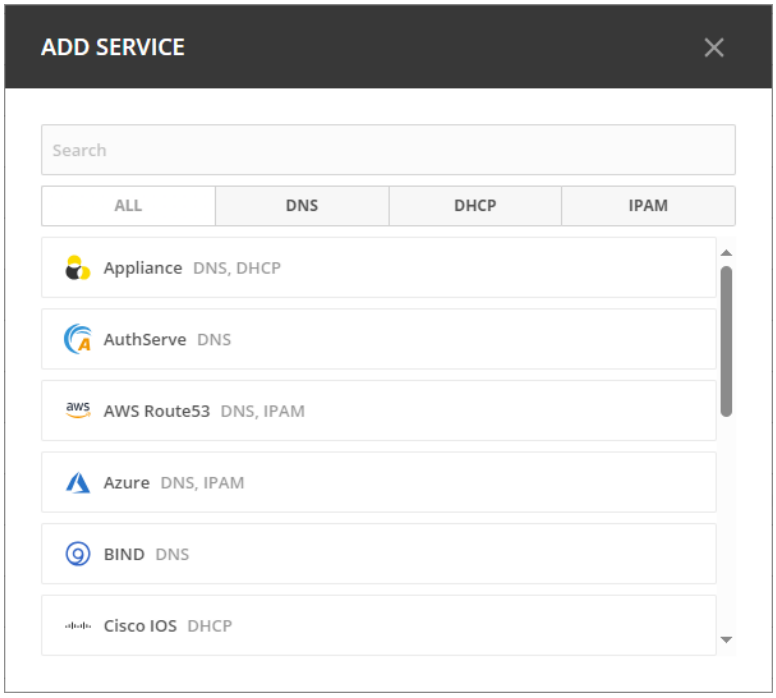


Adding a New Appliance to Micetro

To add an appliance to Micetro, you need to have the Administrator role.

To add an appliance:

1. Go to the *Service Management* tab on the *Admin* page, and select *Add Service*. The Add Service wizard opens.



2. Select *Appliance*.
3. Provide the host name for the appliance, which will also be used for the DNS and DHCP services hosted on the appliance.
4. Optionally, enter the IP address of the appliance. The appliance name will still be used when displaying appliance information.
5. Select *Add*. The appliance is added to the **Appliances** section, and its associated services are listed under **DNS Services** and **DHCP Services**.

Editing Appliance Name

You can change the name or IP address used to connect to your appliance. This is useful if you need to refer to the appliance by another name or if you are connecting to the appliance by an IP address and the IP address has changed.

To change the appliance name:

1. Go to the *Service Management* tab on the *Admin* page.
2. In the filtering sidebar, select *Appliances*, then select the specific appliance you wish to edit.
3. On the *Action* menu, select *Edit appliance*. You can also access this option on the Row menu by selecting ....
4. Modify the appliance's name, and/or IP address (optional).

Note: Changing the name or IP address here only affects how you connect to the appliance. It does not alter the actual IP address of the appliance itself.

---

5. Select *Save* when you are done.

Setting Appliance Services

You can enable or disable various appliance services to configure your appliance.

To enable/disable appliance services:

1. Locate the specific appliance for which you want set services.
2. On the *Action* menu, select *Set appliance services*. You can also access this option on the Row menu ....
    - **SSH (Secure Shell)**: SSH service is enabled by default, providing secure remote access to your appliance. With the SSH client enabled you can connect to and manage the appliance securely. Disabling SSH is not recommended unless you have a specific security requirement. Disabling SSH should only be considered for servers in a highly secure environment, and even then, it should only be done for short periods when absolutely necessary. Always ensure you have alternate secure methods for appliance management.
    - **Firewall**: The firewall is a crucial security measure that protects your appliance against potential attacks. It is strongly recommended to keep the firewall enabled at all times to safeguard your server from threats. Disabling the firewall is NOT recommended. Disabling the firewall temporarily should only be done in situations where you have a deep understanding of the potential risks and have specific security measures in place to compensate for the loss of protection. Even in such cases, minimize the duration of firewall disablement and re-enable it as soon as possible.
3. Select *Save* when you are done.

Setting DNS Resolvers

To ensure optimal performance of your appliance, you can add the IP addresses of DNS resolver servers. This step helps your appliance efficiently resolve domain names and provide accurate network services.

To set DNS resolvers:

1. Locate the specific appliance for which you want to configure DNS resolvers. Ensure you select the correct appliance to avoid any disruptions in network services.
2. On the *Action* menu, select *DNS resolvers*. You can also access this option on the Row menu ....
3. In the DNS resolvers configuration dialog box, enter the IP addresses of the DNS resolver servers you want to set. It's important to ensure the accuracy of the IP addresses, as incorrect entries can lead to DNS resolution issues. You can set multiple DNS resolvers by listing their IP addresses on separate lines. This redundancy ensures uninterrupted DNS resolution even if one resolver becomes unavailable.
4. Select *Save* when you are done.

Configuring SNMP Monitoring

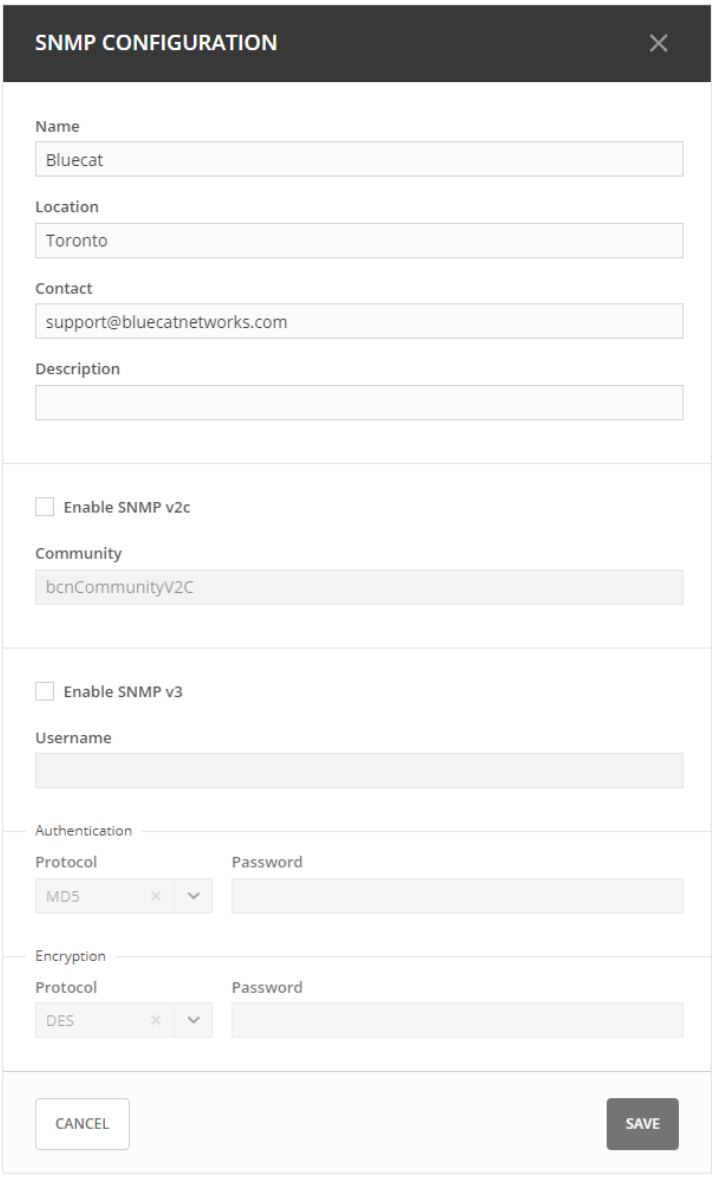
You can use Simple Network Management Protocol (SNMP) monitoring to gather comprehensive information about the appliance. SNMP is enabled by default on appliances, allowing you to access monitoring information without any additional configuration.

Micetro supports SNMP versions v2c and v3. Version v2c is a Community-Based SNMP, which means that it relies on a community string (similar to a password) for authentication, making it relatively simple to set up. Version v3, on the other hand, is a User-Based SNMP and provides enhanced security and authentication mechanisms. It introduces the concept of SNMP users and offers features like user authentication and data encryption.

To configure SNMP Monitoring on appliances:

1. Locate the specific appliance for which you want to configure SNMP monitoring.
2. On the *Action* menu, select *SNMP configuration*. You can also access this option on the Row menu ....

3. The SNMP configuration dialog box opens with several options:



- **Name**: You can enter the name that will be reported through SNMP. By default, this is set as Bluecat.
- **Location**: Enter a description of the system's physical location. By default, this is set as Toronto.
- **Contact**: Enter the email address of the contact person responsible for the system. By default, this is set as the email address for BlueCat's support.
- **Description**: Enter a brief description of the system.
- **Enable SNMP v2c**: Select this option to enable the SNMP v2c protocol.
- **Community**: Enter the community string, which serves as a password for the SNMP v2c protocol.
- **Enable SNMP v3**: Select this option to enable the SNMP v3 protocol.
- **Username**: Enter the SNMP username for the SNMP user.
- **Authentication**: Select either **MD5** or **SHA** authentication and enter the user password for the SNMP user. If you select **None**, the SNMP service doesn't require user authentication and doesn't encrypt the data it

returns.

- **Encryption**: Select either **DES** or **AES 128** encryption types, and provide the password used to encrypt the data. If you select **None**, the SNNMP service doesn't encrypt the data it returns.

4. Select *Save* to save your settings and close the dialog box.

Configuring NTP on Appliances

Use the Network Time Protocol (NTP) service to maintain precise time synchronization across your network infrastructure. Accurate timekeeping ensures proper coordination of network events, security protocols, and compliance with reporting requirements.

To configure NTP:

1. Locate the specific appliance for which you wish to configure NTP.
2. On the *Action* menu, select *NTP configuration*. You can also access this option on the Row menu ....
3. Select the *Enable NTP service* checkbox to activate the NTP service on your appliance.
4. In the text box, enter the hostnames or IP addresses of the NTP servers from which you want to synchronize your appliance's clock.

   Tip: Consider using multiple NTP servers for redundancy and increased reliability, ensuring continued time synchronization even if one server becomes inaccessible.

5. Select *Save* when you are done.

Downloading Support Information for Appliances

To help in troubleshooting, you may be asked to download support information for your appliance. This support information file holds crucial details about your appliance setup, aiding our support team in diagnosing and resolving any issues you may encounter.

To download support information:

1. Locate the specific appliance you are troubleshooting.
2. On the *Action* menu, select *Get support info*. You can also access this option on the Row menu ....
3. Select *Download*.
4. Once the download is complete, forward the downloaded file to support@bluecatnetworks.com.

Note: The support information file is packaged as a .tgz archive and contains various text files. If you wish to view the contents of the support information file, you can use any tool capable of extracting data from .tgz archives to access and review the enclosed text files.

Shutting Down or Restarting Appliances

You can shut down or restart the appliances.

Note: For appliances equipped with an Integrated Dell Remote Access Controller (iDRAC), the iDRAC continues running when the appliance is shut down. This means that it can be accessed via the local network to power on the appliance without requiring physical access. If you shut down an appliance that is not equipped with iDRAC, it will be turned off and you will need physical access to the appliance to turn it on again. Consult the specifications for your appliance for more information on its remote access capabilities.

To shut down or restart appliances:

1. Select the appliance you want to restart or shut down.
2. On the *Action* menu, select *Shut down appliance* or *Restart appliance* and select *Yes* in the confirmation dialog box. The appliance shuts down or restarts, depending on your selection.

Removing Appliances

This command is only available for the Administrator role.

> **Warning:** When you remove an appliance from Micetro, the DNS and DHCP services hosted on the appliance are removed from Micetro as well.

To remove an appliance from Micetro:

1. Select the appliance(s) you want to remove. To select multiple appliances, hold down the **Ctrl** key while making your selection.
2. On the *Action* menu, select *Remove appliance*. Select *Yes* to confirm.

Viewing Appliance History

The *View history* option on the *Action* or the Row menu … opens the History window that shows a log of all changes that have been made to the appliance, including the date and time of the change, the name of the user who made it, the actions performed, and any comments entered by the user when saving changes to objects. For more information about how to view change history, see *Viewing Change History*.

Backup and Restore

Micetro automatically takes a backup of your appliance's configuration every 15 minutes, capturing any changes made since the last backup. Additionally, a full backup is taken once every 24 hours, and all the incremental backups are managed and cleaned up for you.

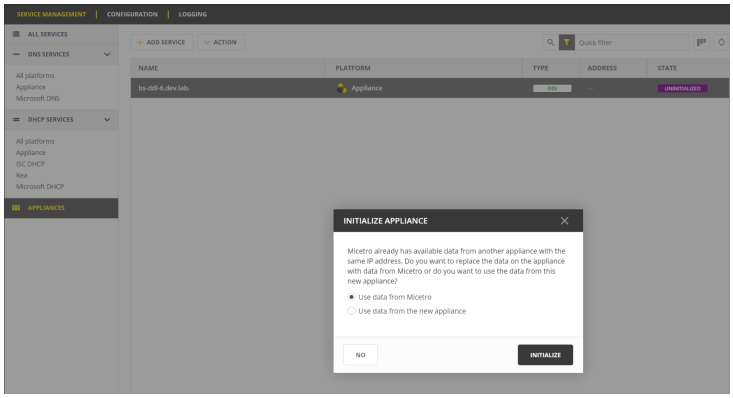
When an appliance experiences a crash and becomes unusable, you can use these backups to set up a new appliance as a replacement, while maintaining the same IP address.

Micetro automatically detects the new server as uninitialized. To begin using the new server, you need to initialize it. uninitialized

To initialize a server:

1. Locate the uninitialized server.

2. On the *Action* menu, select *Initialize appliance*. You can also access this option on the Row menu ....



- **Use data from Micetro**: This option allows you to initialize the server using the data saved in Micetro.
- **Use data from the new appliance**: Use this option if you want to initialize the server with the data from the new appliance itself.

See also:

- *Update Guide*
- *Service Management*
- appliance-management
- *Caching DNS Servers*

1.19.14 Caching DNS Servers

Overview

This section shows you how to perform specific actions in the Men&Mice Management Console associated with maintaining your Caching DNS servers on a Men&Mice DNS Caching Appliance. For some more general options and features of DNS servers in general, please see *Authoritative DNS Servers (Management Console, obsolete)*.

Note: The contents of this section are only relevant if you are using the Men&Mice DNS Caching Appliance.

Options

The *Server Options* dialog box lets you configure settings for each caching DNS server individually. It is also possible to select multiple caching DNS servers and set specific options for all of the selected servers.

To open the caching DNS server Options dialog box, do the following:

1. In the *Object Section*, select *DNS Servers* so the servers appear in the Object List.
2. Right-click on the caching DNS server you want to make changes to and select *Options* from the context menu. The *Server Options* dialog box displays.

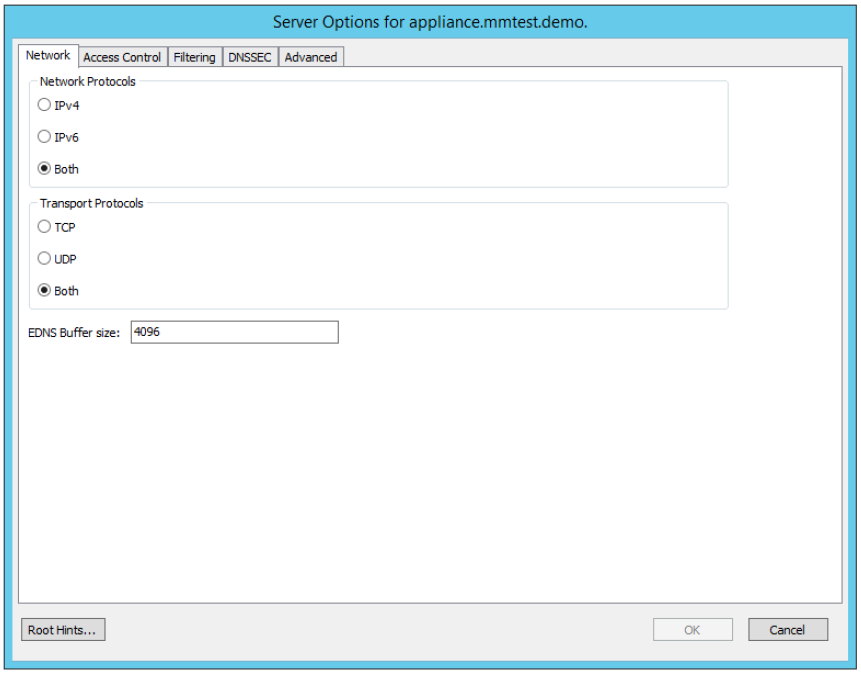
The settings in the following sections are all available from within the caching DNS server options dialog box.

Setting Network and Transfer Protocols

You can choose which network protocols (IPv4, IPv6 or both) and transport protocols (TCP, UDP or both) you want to use and you can also set the EDNS Buffer size.

To set the network and transfer protocols for the caching DNS server, do the following:

1. Select the *Network* tab in the caching DNS server *Options* dialog box.



2. Select the **Network Protocols** to use. You can specify whether you want to enable DNS on IPv4, IPv6 or both.
3. Select the **Transport Protocols** to use. You can specify whether you want to enable DNS on TCP, UDP or both.
4. Set the **EDNS Buffer** size. This is the number of bytes to advertise as the EDNS reassembly buffer size. This is the value put into datagrams over UDP towards peers. The default is 4096 which is RFC recommended.

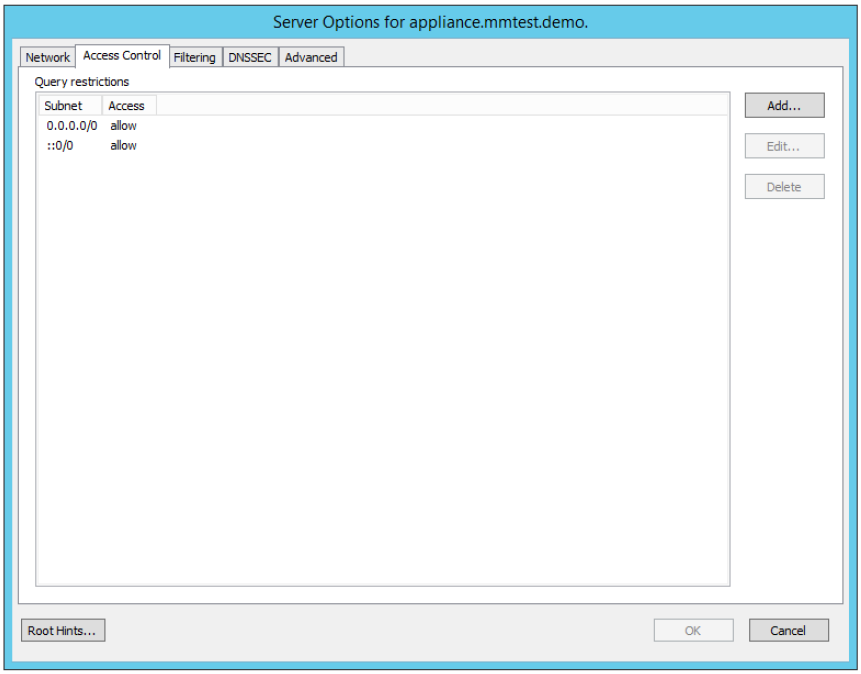
Tip: If you have fragmentation reassembly problems, usually seen as timeouts, then a value of 1480 can fix it. Setting to 512 bypasses even the most stringent path MTU problems, but is seen as extreme, since the amount of TCP fallback generated is excessive (probably also for this resolver, consider tuning the outgoing TCP number).

Setting Access Control for the Caching DNS Server

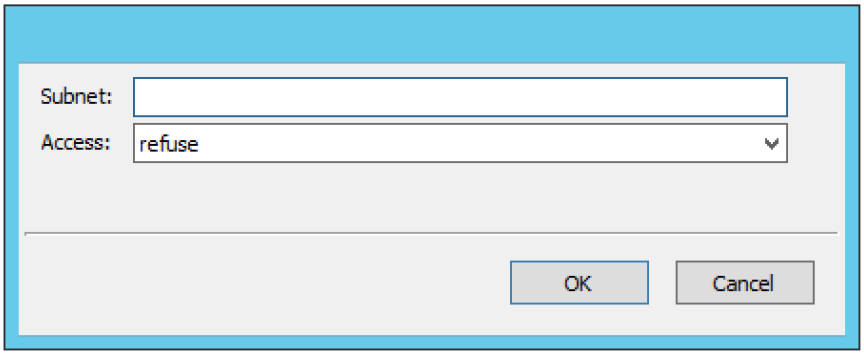
Access control for the caching DNS server is used to specify who can query the server. You can specify access based on individual IP addresses or address blocks and you can create multiple access control entries.

To set access control for the caching DNS server, do the following:

1. Select the *Access Control* tab in the caching DNS server *Options* dialog box.



2. Click the *Add* button to create a new access control entry.



3. Enter the address or subnet in the field provided and choose the access type for the subnet from the drop-down list. There are four access types available:

   refuse
   : Stops all queries from the specified host or network and sends the DNS rcode REFUSED error message back.

   deny
   : Stops all queries from the specified host or network.

   allow
   : Allows the specified host or network to query the server using non-recursive queries.

allow-snoop
: Allows the specified host or network to query the server using both non-recursive and recursive queries.

4. Click *OK* to save the access control entry.

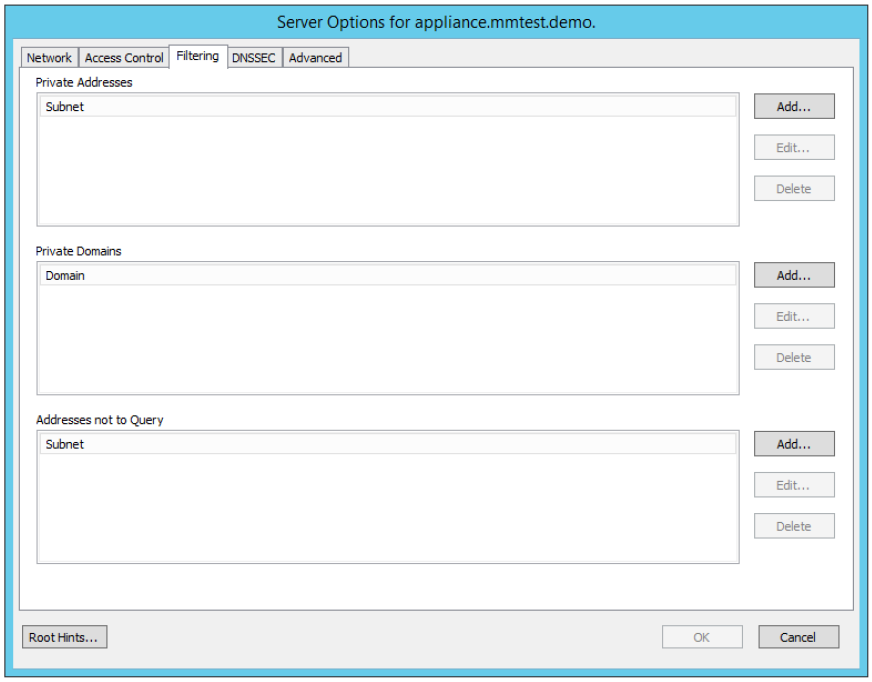
Setting Private Addresses and Private Domains

It is possible to specify private addresses and private domains on the caching DNS server.

- Private addresses are addresses on your private network, and are not allowed to be returned for public Internet names. Any occurrences of such addresses are removed from DNS answers.
- Private domains are domains that may contain private addresses.

To specify private addresses, do the following:

1. Select the *Filtering* tab in the caching DNS server *Options* dialog box.



2. Click the *Add* button in the *Private Addresses* section to create a new private address entry.
3. Enter the address or subnet in the field provided, and click *OK* to save the private address entry.

To specify private domains:

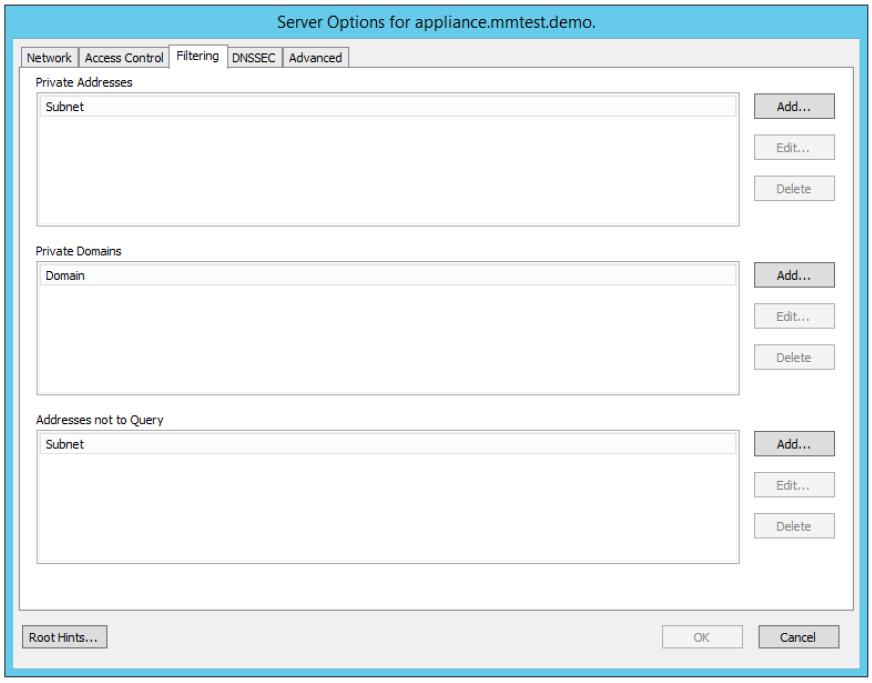
1. Select the *Filtering* tab in the caching DNS server *Options* dialog box.
2. Click the *Add* button in the *Private Domains* section to create a new private domain entry.
3. Enter the domain name in the field provided, and click *OK* to save the private domain entry.

Specifying Addresses not to Query

It is possible to specify IPv4 or IPv6 addresses or subnets that the caching DNS server should not use when querying for DNS information.

To specify addresses that should not be queried, do the following:

1. Select the *Filtering* tab in the caching DNS server *Options* dialog box.



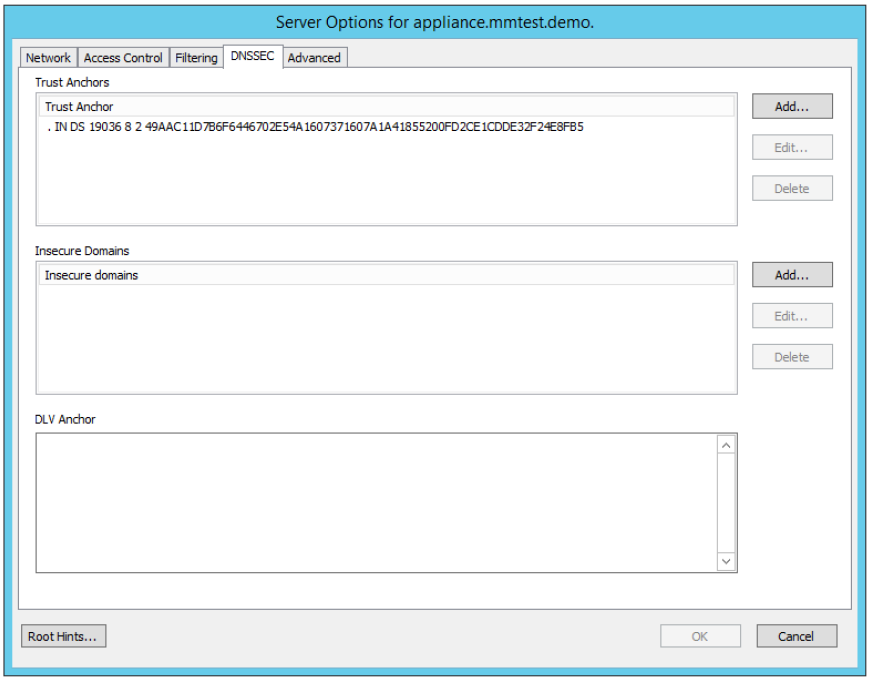
2. Click the *Add* button in the *Addresses not to Query* section to create a new address entry.
3. Enter the address or subnet in the field provided, and click *OK* to save the address entry.

Configuring DNSSEC Settings

Use the DNSSEC section to specify DNSSEC Trust Anchors, DLV Anchors and Insecure Domains

To configure DNSSEC settings, do the following:

1. Select the *DNSSEC* tab in the caching DNS server *Options* dialog box.



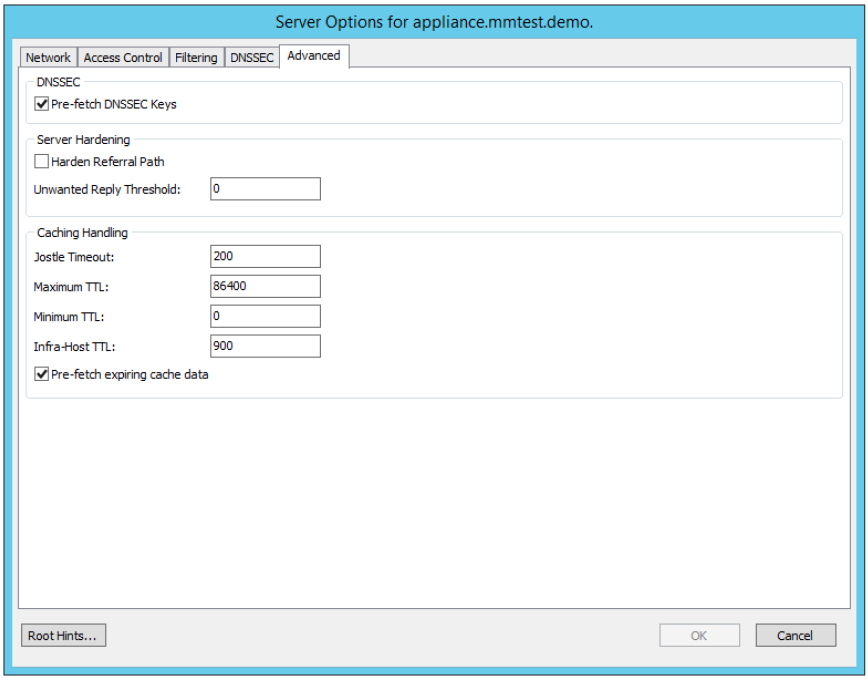
2. Click the *Add* button in the *Trust Anchors* section to create a new trust anchor entry. A trust anchor A is a DS or DNSKEY RR for a key to use for validation.
3. Click the *Add* button in the *Insecure Domains* section to create a new insecure domain entry. This sets the specified domain name to be insecure. The DNSSEC chain of trust is ignored towards the domain name. A trust anchor above the domain name cannot make the domain secure with a DS record and such a DS record is ignored. Also, keys from DLV are ignored for the domain. This can be useful if you want to make sure a trust anchor for external lookups does not affect an (unsigned) internal domain. DS record externally can create validation failures for that internal domain.
4. Enter the relevant DLV Anchor data in the **DLV Anchor** edit field to create a DLV anchor entry. Much like a trust anchor, a DLV anchor is a DS or DNSKEY RR for a key to use for validation. You can only create one DLV anchor entry.

Configuring Advanced Settings

The caching DNS server Options dialog box contains an Advanced tab where you can configure various advanced settings for the server.

To configure advanced settings, do the following:

1. Select the *Advanced* tab in the caching DNS server *Options* dialog box.



2. Configure the desired advanced settings.

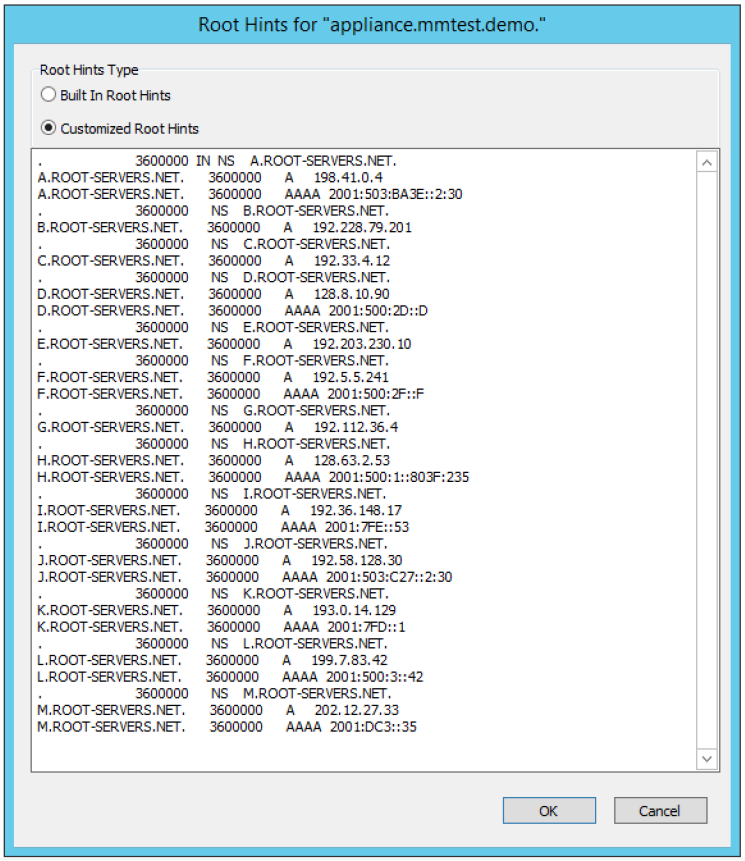
Pre-fetch DNSSEC Keys	If checked, fetches the DNSKEYs earlier in the validation process when a DS record is encountered. This lowers the latency of requests but uses a little more CPU.
Harden Referral Path	If checked, hardens the referral path by performing additional queries for infrastructure data. Validates the replies if trust anchors are configured and the zones are signed. This enforces DNSSEC validation on name server NS sets and the name server addresses that are encountered on the referral path to the answer. Default off, because it burdens the authority servers, and it is not RFC standard, and could lead to performance problems because of the extra query load that is generated.
Jostle Timeout	Timeout used (in milliseconds) when the server is very busy. The default is 200 milliseconds. Set to a value that usually results in one roundtrip to the authority servers. If too many queries arrive, then 50% of the queries are allowed to run to completion, and the other 50% are replaced with the new incoming query if they have already spent more than their allowed time. This protects against denial of service by slow queries or high query rates. The effect is that the qps for long-lasting queries is about (numqueriesperthread / 2) / (average time for such long queries) qps. The qps for short queries can be about (numqueriesperthread / 2) /(jostletimeout in whole seconds) qps per thread, about (1024/2)*5 = 2560 qps by default.
Maximum TTL	Maximum time to live (in seconds) for RRsets and messages in the cache. Default is 86400 seconds (1 day). If the maximum kicks in, responses to clients still get decrementing TTLs based on the original (larger) values. When the internal TTL expires, the cache item has expired. The Maximum TTL can be set lower to force the resolver to query for data often, and not trust (very large) TTL values.
Minimum TTL	Minimum time to live (in seconds) for RRsets and messages in the cache. Default is 0. If the minimum kicks in, the data is cached for longer than the domain owner intended, and thus, fewer queries are made to look up the data. Zero makes sure the data in the cache is as the domain owner intended; higher values, especially more than an hour or so, can lead to trouble as the data in the cache does not match up with the actual data any more.
Infra-Host TTL	Time to live (in seconds) for entries in the host cache. The host cache contains roundtrip timing, lameness, and EDNS support information. Default is 900.
Pre-fetch expiring cache data	If checked, fetches the DNSKEYs earlier in the validation process when a DS record is encountered. This lowers the latency of requests but uses a little more CPU.

Working with Root Hints

The Root Hints file contains information on the root DNS servers. If needed, you can change the contents of this file. After making changes to the Root Hints file you can revert to the built-in Root Hints file.

To configure Root Hints, do the following:

1. Click the *Root Hints* button in the caching DNS server *Options* dialog box. The *Root Hints* dialog box displays.



2. Select the *Customized Root Hints* radio button if it isn't already selected. The contents of the **Root Hints** edit field become editable.
3. Make the desired changes to the Root Hints file and click *OK* to save the changes.

To use the built-in Root Hints file, do the following:

1. Click the *Root Hints* button in the caching DNS server *Options* dialog box. The *Root Hints* dialog box displays.
2. Select the *Built In Root Hints* radio button. The contents of the **Root Hints** edit field become read-only.
3. Click *OK* to save the changes.

Server Log and Query Logging

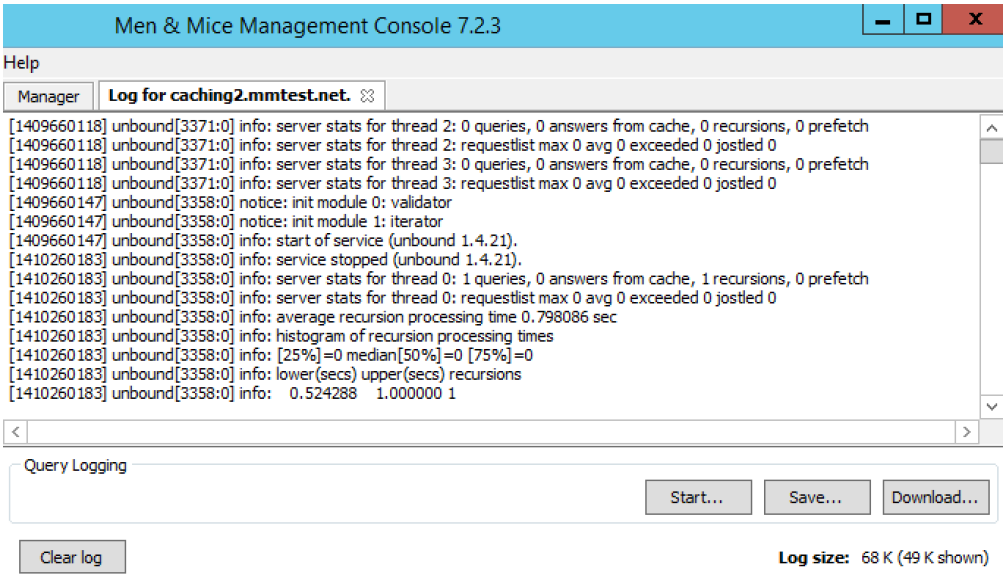
To view the activity log for a particular server, in the Object List, right-click on the desired server and, from the shortcut menu, select *Server Log*. A *Log* tab opens for the selected server that contains a list of activity and maintenance that has occurred on that server since the last time the log was cleared.

You can clear the server log by clicking the *Clear log* button in the server log tab. You can start logging all queries by clicking the *Start* button in the *Query Logging* section in the server log window. If query logging is enabled, the *Start* button changes to a *Stop* button and clicking the button will stop query logging.

> **Warning:** Query logging may impact server performance significantly and should only be used for troubleshooting purposes.

You can save the contents of the server log tab by clicking the *Save* button.

To download the last server log file directly from the DNS Caching Appliance click the *Download* button.



Stopping the DNS Server

The Men&Mice DNS Caching Appliance is configured to keep the DNS service running at all times. This means that if the DNS server is stopped for some reason, it is restarted automatically. However, it is possible to override this setting and stop the DNS server from the Server menu. When the DNS server is stopped, the Men&Mice DNS Caching Appliance withdraws itself from the Anycast setup if Anycast has been configured on the Appliance. When the DNS server is started again, the Appliance re-enables the Anycast configuration. The stopped state for the DNS server is not persistent. If the Appliance is restarted while the DNS server is stopped, the DNS server will be started once the Appliance has restarted.

To stop the DNS server, select the caching DNS server in the DNS Server list and on the *Server* menu select *Stop DNS Server*.

To start the DNS server, on the *Server* menu select *Start DNS Server*.

Stub and Forward Zones

You can create stub and forward zones on the caching DNS server. See *Forward Zone* and *Stub Zone* for more information on creating stub and forward zones.

Note: When creating stub and forward zones on a caching DNS server, some additional settings are available for the zones.

For forward zones, the *Forward only* checkbox displays. Select this checkbox if you want the zone to be a forward only zone.

For stub zones, two additional settings are available:

Prime NS set
: If checked, the server performs NS set priming, which is similar to root hints, where it starts using the list of name servers currently published by the zone. Thus, if the hint list is slightly outdated, the resolver picks up a correct list online.

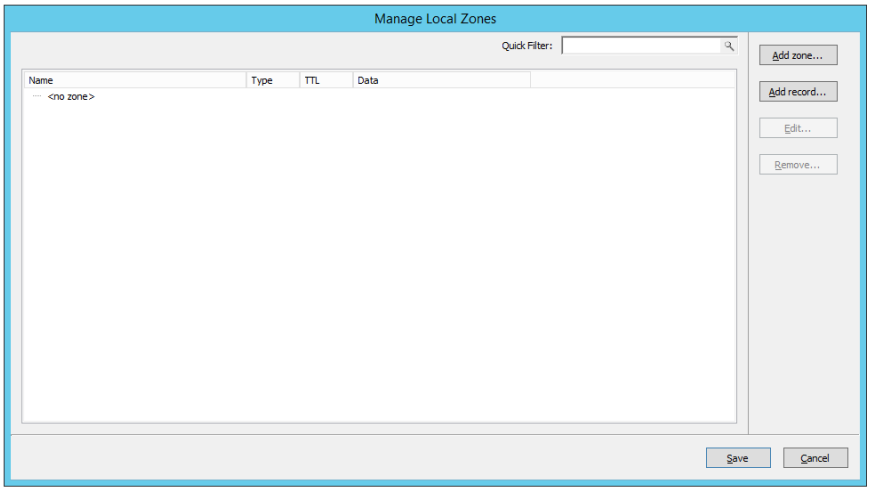
Stub-First
If checked, a query is attempted without the stub clause if it fails.

Managing Local Zones

Using the *Local Zone management* dialog box, you can add, modify and delete local zones and records. Local zones and records are only displayed in the Local Zone management dialog box.

To open the Local Zone management dialog box, do the following:

1. In the *Object Section*, select *DNS Servers* so the servers appear in the Object List.
2. Right-click on the caching DNS server you want to work with and select *Manage Local Zones* from the context menu. The *Manage Local Zones* dialog box displays.



The dialog box is used to work with local zones and records.

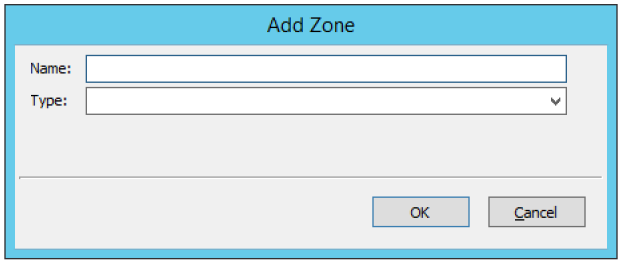
After making changes to the local zone data, click *Save* to save and apply the changes.

The actions in the following sections are all available from within the *Local Zone management* dialog box.

Adding a Local Zone

To add a new local zone:

1. Click the *Add zone* button. A zone properties dialog box displays.



2. Enter the zone name in the field provided and choose the zone type from the drop-down list. There are several zone types available:

   deny
   Do not send an answer and drop the query. If there is a match from local data, the query is answered.

refuse
Send an error message reply, with rcode REFUSED. If there is a match from local data, the query is answered.

static
If there is a match from local data, the query is answered. Otherwise, the query is answered with nodata or nxdomain. For a negative answer a SOA is included in the answer if present as local-data for the zone apex domain.

transparent
If there is a match from local data, the query is answered. Otherwise, if the query has a different name, the query is resolved normally. If the query is for a name given in localdata but no such type of data is given in localdata, then a noerror nodata answer is returned.

typetransparent
If there is a match from local data, the query is answered. If the query is for a different name, or for the same name but for a different type, the query is resolved normally. So, similar to transparent but types that are not listed in local data are resolved normally, so if an A record is in the local data that does not cause a nodata reply for AAAA queries.

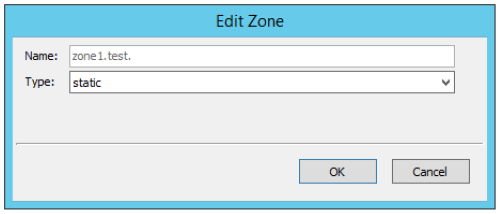
redirect
The query is answered from the local data for the zone name. There may be no local data beneath the zone name. This answers queries for the zone, and all subdomains of the zone with the local data for the zone. It can be used to redirect a domain to return a different address record to the end user, with local-zone: "example.com." redirect and local-data: "example.com. A 127.0.0.1" queries for www.example.com and www.foo.example.com are redirected, so that users with web browsers cannot access sites with suffix example.com.

3. Click *OK* to save the zone entry.

Editing/Deleting a Local Zone

To edit an existing local zone:

1. Select the zone and click the *Edit* button. The zone properties dialog box displays. Note that the server name is disabled and you can only change the zone type.



2. Make the necessary changes and click *OK*.

To delete a local zone:

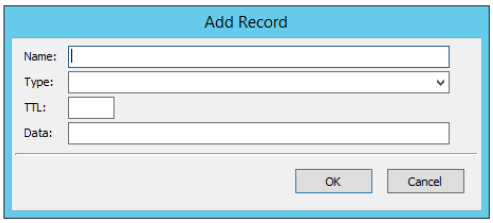
1. Select the zone.
2. Click the *Remove* button. A confirmation box displays.
3. Click *OK* to delete the zone and all of the zone data.

Adding a Record

You can add a record to an existing local zone. It is also possible to add a record that does not belong to a specific local zone. Records that do not belong to any local zones are placed in the <no zone> section in the *Local Zone management* dialog box.

To add a new record:

1. Click the *Add record* button. A record properties dialog box displays. If you selected a zone before clicking the *Add record* button, the name of the selected zone has been added to the **Name** field.

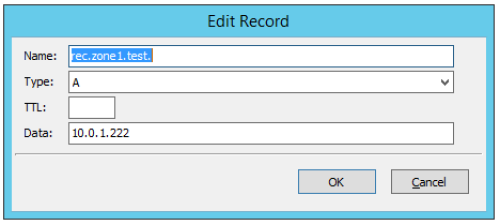


2. Enter a fully qualified record name including the zone name in the **Name** field.
3. Select the record type from the **Type** drop-down list.
4. Enter a TTL for the record in the **TTL** field (optional).
5. Enter the data for the record in the **Data** field.
6. Click *OK* to save the changes.

Editing/Deleting a Record

To edit an existing record:

1. Select the record.
2. Click the *Edit* button. The *Edit Record* dialog box displays.



3. Make the necessary changes and click *OK*.

To delete a record:

1. Select the record.
2. Click the *Remove* button. A confirmation box displays.
3. Click *OK* to delete the record.

See *Update Guide*.

1.20 Micetro reference articles

1.20.1 Permissions reference

Note: License management has no associated permission, and can only be accessed by *The administrator user*.

The following tables list all the permissions in Micetro, as defined in the API and the web application.

Table 12: Micetro

API	Web application	Notes
access_adminU	**Administer users/groups**	Needed to manage Roles.
access_adminI	**Administer IP address ranges**	
access_adminD	**Administer DNS servers**	
access_adminH	**Administer DHCP servers**	
access_adminA	**Administer appliances**	
access_adminD	**Administer devices**	
access_IPAMM	**Access IPAM module**	
access_DNSMo	**Access DNS module**	
access_DHCPM	**Access DHCP module**	Needed to access DHCP functionality in the IPAM view. License for the IPAM module also unlocks the DHCP module.
access_conso	**Access to the Management Console**	
access_comma	**Access to the CLI**	Legacy permission, the CLI (Command Line Interface) is no longer in use.
access_web	**Access to the web interface**	Needed to access the web application.
access_basicZ	**Access to basic zone view in web interface**	Legacy permission, not available in the web application.
access_advan	**Access to advanced zone view in web interface**	Needed to access DNS functionality in the web application.
access_IPAMV	**Access to IPAM view in web interface**	Needed to access IPAM functionality in the web application.
access_basicR	**Access to basic reporting**	Manually run built-in reports.
access_tasksV	**Access to task list view in web interface**	Legacy permission, not available in the web application.
access_viewH	**Access to view history**	
access_webHo	**Access to Host editor**	Legacy permission, not available in the web application.
access_adminA	**Access to manage AD Sites and Site Links**	
access_adminC	**Access to manage clouds**	
access_workf	**Access Workflow module**	
access_advan	**Access to advanced reporting**	Build custom reports, and schedule reports.
access_impor	**Access to 'Import Data' web task**	

Table 13: DNS servers

API	Web application	Notes
access_editA	**Edit DNS server access**	
access_list	**List (or view) DNS server**	
access_viewH	**View DNS server history**	
access_optio	**Edit DNS server options**	
access_addMa	**Add master zones**	
access_addNo	**Add non-master zones**	
access_viewL	**View DNS server log**	
access_clearl	**Clear DNS server log**	
access_editP	**Edit DNS server properties**	
access_manag	**Manage local zones**	

Table 14: DHCP servers

API	Web application	Notes
access_editA	**Edit DHCP server access**	
access_list	**List (or view) DHCP server**	
access_viewH	**View DHCP server history**	
access_readO	**Read DHCP server options**	
access_optio	**Read/write DHCP server options**	
access_addSc	**Add a scope**	
access_editP	**Edit DHCP server properties**	
access_reser	**Edit reservations**	
access_addGr	**Add a group**	
access_readC	**Read DHCP class data**	
access_classl	**Read/write DHCP class data**	

Table 15: DNS zones

API	Web application	Notes
access_editA	**Edit zone access**	
access_list	**List (or view) zone**	
access_viewH	**View zone history**	
access_enabl	**Enable/disable zone**	
access_optio	**Edit zone options**	
access_delet	**Delete zone**	
access_enabl	**Enable/disable apex records**	
access_editA	**Edit apex records**	
access_enabl	**Enable/disable wildcard records**	
access_editW	**Edit wildcard records**	
access_enabl	**Enable/disable other records**	
access_editO	**Edit other records**	
access_editP	**Edit zone properties**	

Table 16: Ranges and DHCP scopes

API	Web application	Notes
access_editA	**Edit range access**	
access_list	**List (or view) range**	
access_viewH	**View range history**	
access_delet	**Delete range**	
access_editP	**Edit range properties**	
access_editD	**Edit IP Address properties**	
access_editDl	**Use IP addresses in DNS**	
access_creat	**Create subrange**	
access_reuse	**Create multiple hosts per IP address**	
access_pingA	**Ping IP addresses**	
access_siteA	**Edit AD site association**	
access_enabl	**Enable/disable scope**	
access_readO	**Read scope options**	
access_optio	**Read/write scope options**	
access_reser	**Edit reservations**	
access_addre	**Edit address pools**	
access_exclu	**Edit exclusions**	
access_relea	**Release leases**	
access_addGr	**Add a group**	Legacy permission for DHCP groups.

Table 17: DHCP groups (legacy only)

API	Web application	Notes
access_editA	**Edit DHCP group access**	
access_list	**List (or view) DHCP group**	
access_viewH	**View DHCP group history**	
access_reser	**Edit reservations**	
access_readO	**Read DHCP group options**	
access_optio	**Read/write DHCP group options**	
access_delet	**Delete DHCP group**	

Table 18: Address spaces

API	Web application	Notes
access_editA	**Edit address space access**	
access_list	**List (or view) address space**	Only needed to switch to an address space other than *Default*.
access_viewH	**View address space history**	

Table 19: Cloud networks

API	Web application	Notes
access_editA	**Edit cloud network access**	
access_list	**List (or view) cloud network**	
access_viewH	**View cloud network history**	
access_editP	**Edit cloud network properties**	
access_delet	**Delete cloud network**	

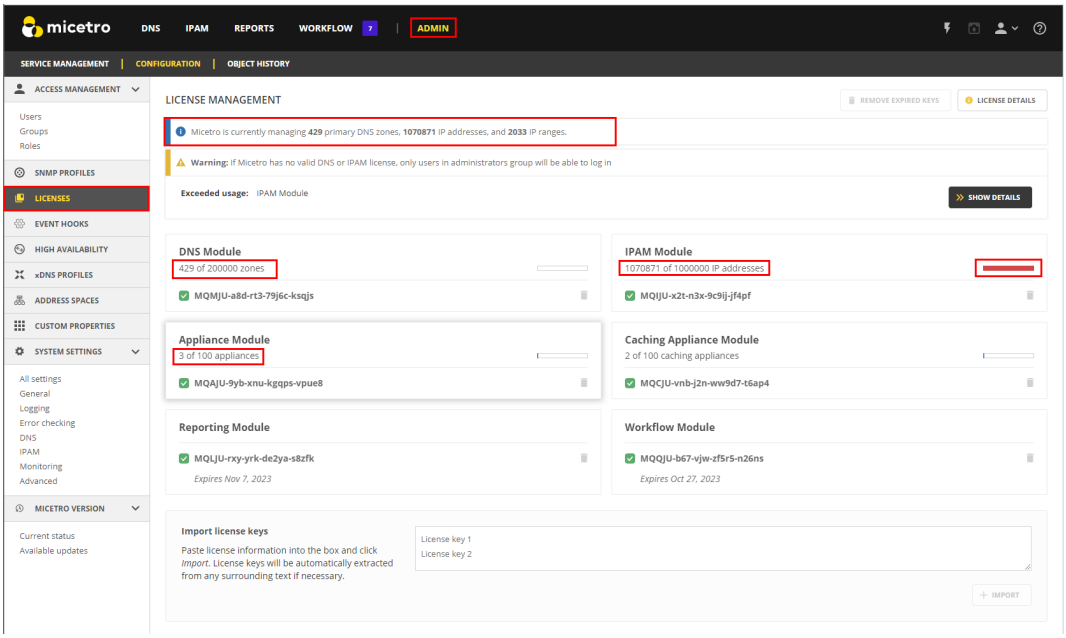
Table 20: Cloud services

API	Web application	Notes
access_editA	**Edit cloud access**	
access_list	**List (or view) cloud**	
access_viewH	**View cloud history**	
access_editP	**Edit cloud properties**	
access_creat	**Create cloud network**	

1.20.2 Calculating IP Usage

As you connect to the services and enable discovery, Micetro reads incoming data to calculate IP address usage. It then compares the usage with the keys provided at the time of purchase to display the number of IP addresses in use, based on the encoded information in the keys. If you are unsure about your IP count, the number can be negotiated with the sales team (best effort).

Note: M&M does not lock the system in any way if the license count is exceeded. Sustaining services is our top priority.



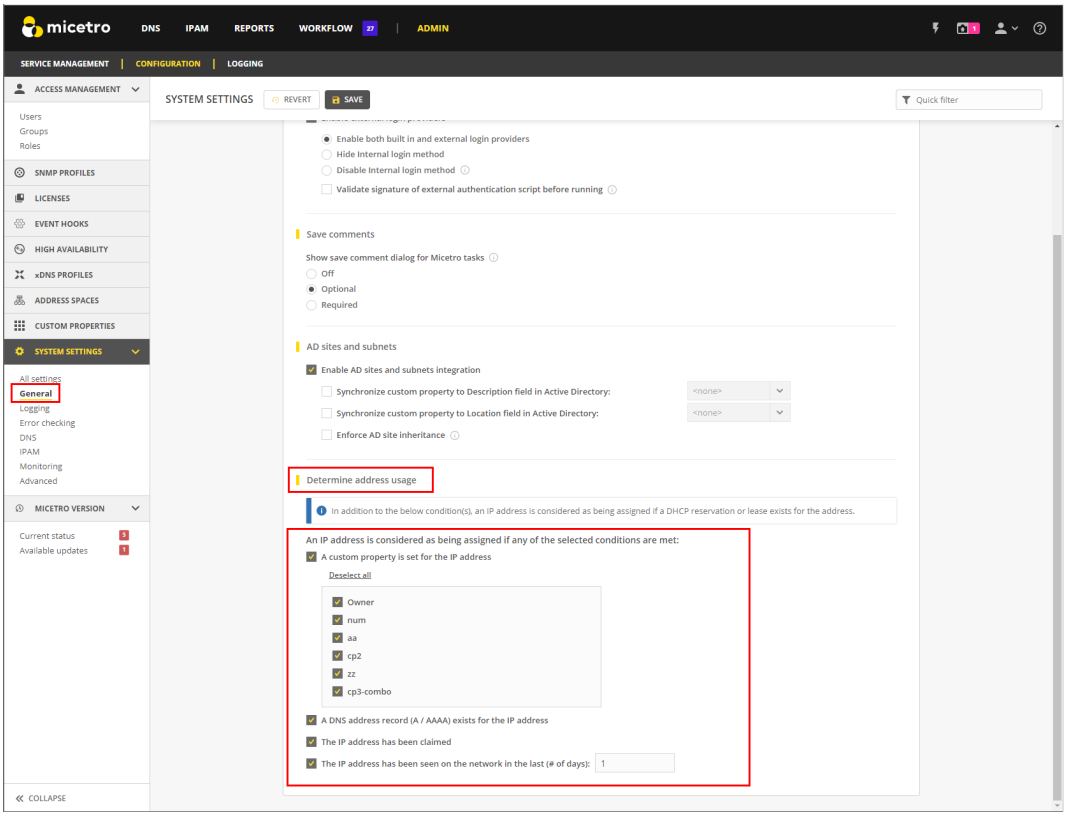
How Micetro Calculates IP Address Usage

Micetro considers an IP address to be “in use” when:

1. There is a DNS record assigned to the IP address (data from the DNS server).
2. There is an active lease in a DHCP pool. This will cause usage to fluctuate in the license count.
3. There is a DHCP reservation configured for the IP address.
4. A custom property is configured for the IP address and it is populated.
5. The IP address has been explicitly claimed using the “Claim IP” feature.
6. Discovery is enabled and there is an active client on the IP address. This feature is configurable by the number of days.

Note: Micetro will only count dual-stacked clients as one IP (IPV4/IPV6).

In the **System Settings**, there is a section called **Determine address usage**.



By deault, all these settings are selected upon installation.

Administrators can toggle the license count configuration on and off to get a more granular picture of where the usage is coming from, which will then allow them to focus on clean-up.

Common Reasons for Excessive IP Usage:

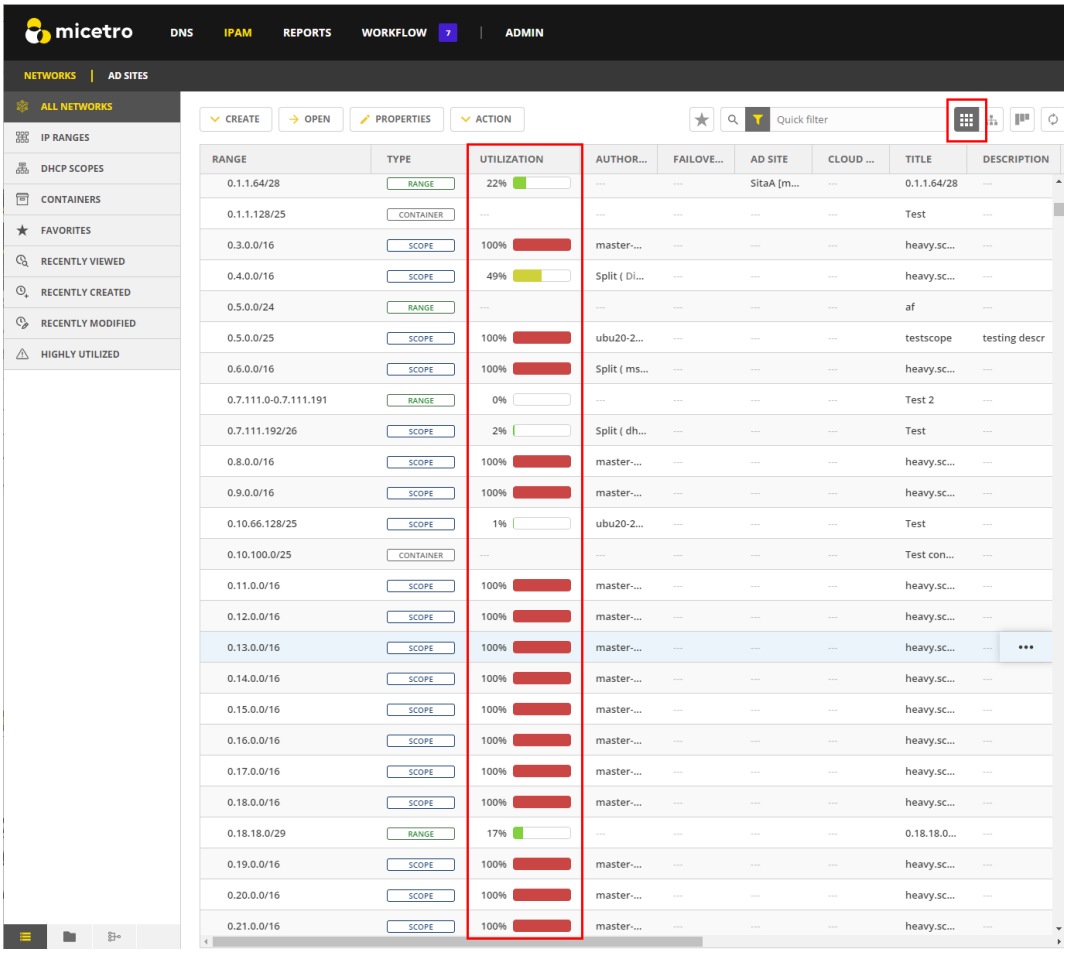
- Stale DNS records (static or missed by AD scavenging).
- Old automation tools that were using the Custom Properties on the IPs, but were not cleaned up.
- Old claims that were not cleaned up.
- DHCP reservations that are not in use.
- DHCP lease times need to be adjusted.

Seeing IP Usage in Micetro

Micetro provides a comprehensive view of your network, allowing you to quickly assess its status and understand what is happening in real-time. As you use Micetro, you will naturally become more knowledgeable about the environment and start to recognize patterns of usage, as well as identifying issues in configurations.

Network Utilization

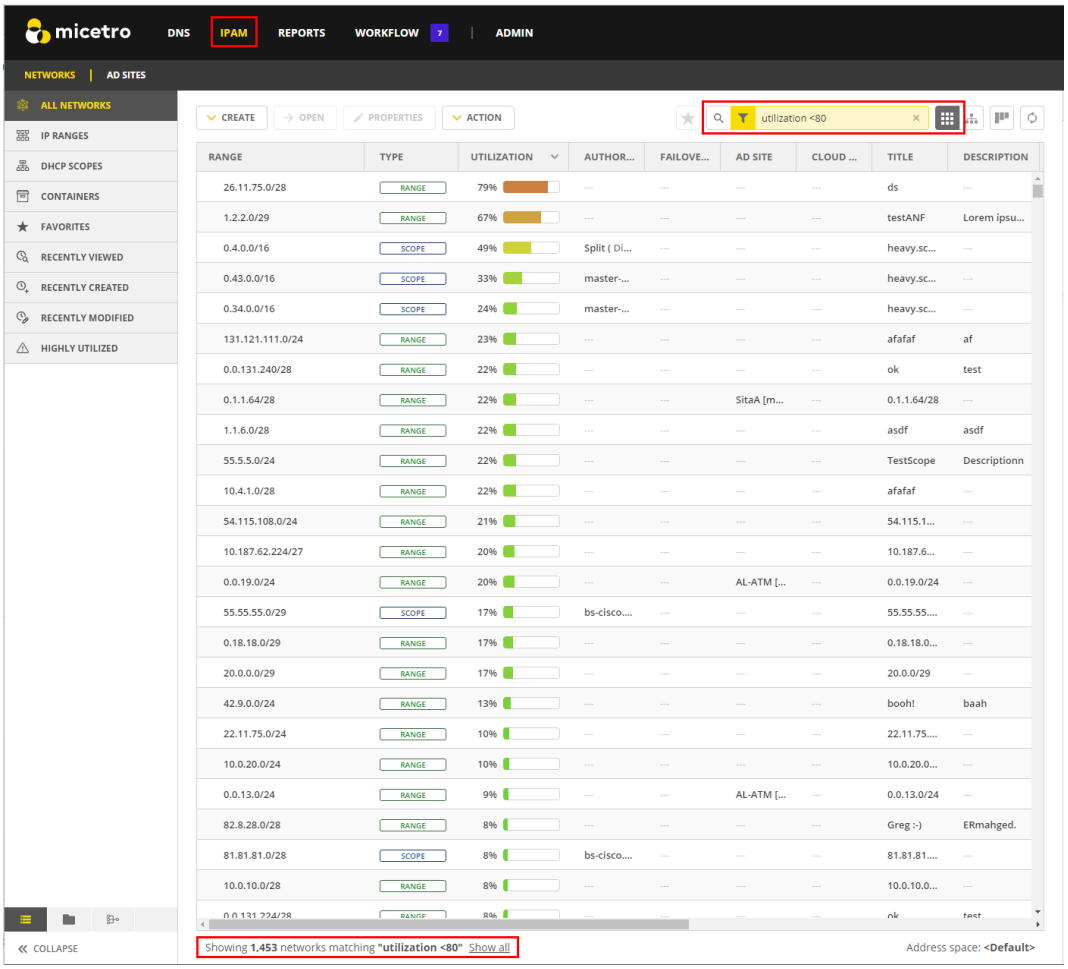
Network Utilization is shown in the IPAM (IP address management) module. For more information about utilization history, see console-ipam-utilization-history.



Tip: You can switch the view to "flat view", and then click the **Utilization** header to sort by most highly utilized networks.

Tip: You can use a quick filter (uses reg-ex) to find all subnets above a certain capacity (utilization < 80). Additional filtering can be added for any of the ranges or scopes (type = Scope and (utilization > 0).

Note: Micetro also gives you the total number of Ranges in the filter.

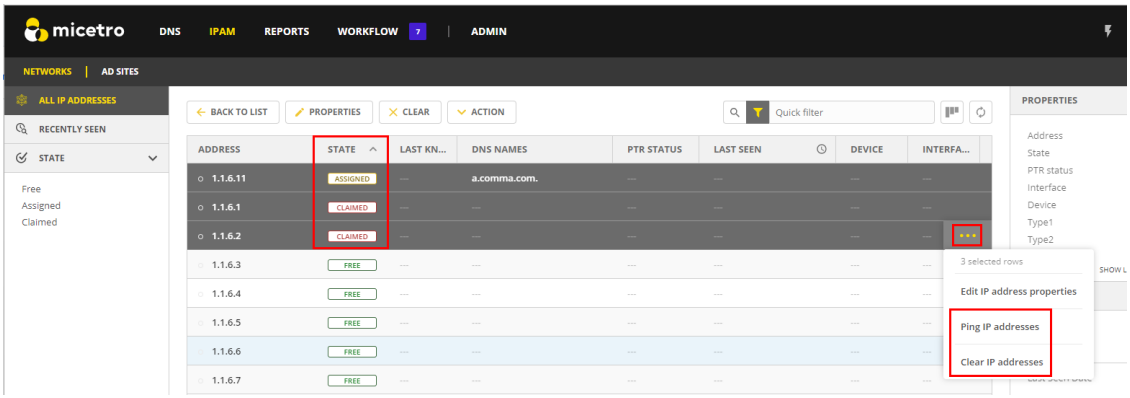


Viewing and Reclaiming IPs at the IP Level

When you open a static Range or a DHCP scope, you can also see the DNS data on the IP.

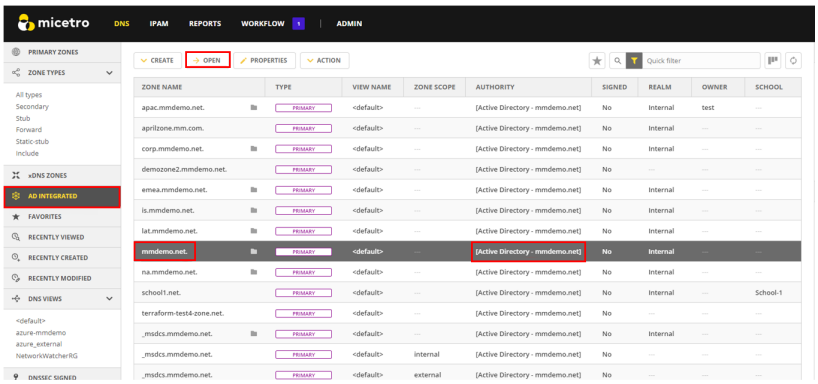
Tip: If you know a DHCP scope or network is not in use, you can safely select all and delete all of the DNS data out of it by selecting *Clear IP address*.

Note: Deleting a range does not delete the DNS data out of the zone. If a new range is created and the DNS data is still in the zone, it will re-populate in the tool.

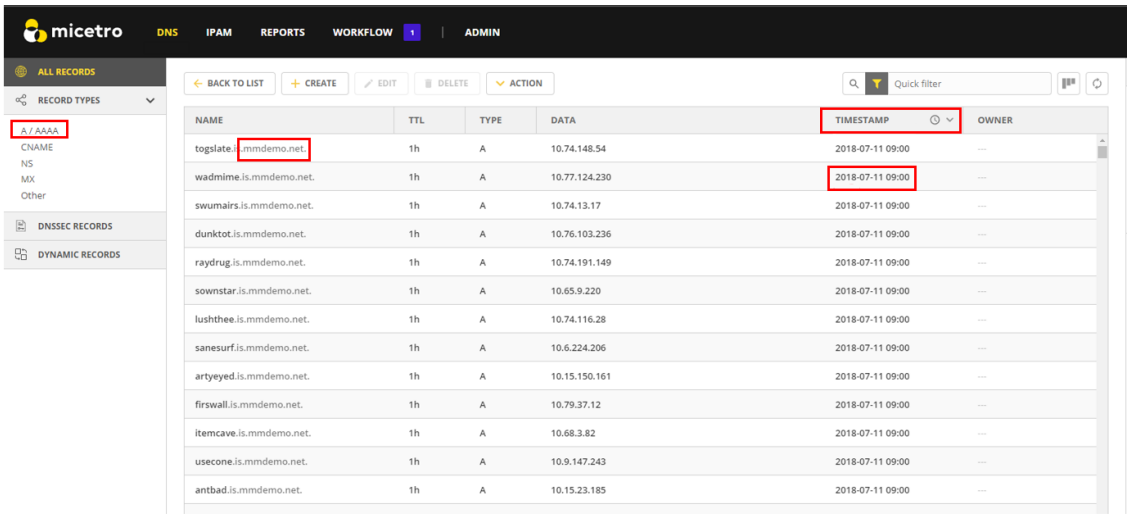


Cleaning up Stale DNS Records

It is not uncommon for AD records to be missed in Scavenging. Micetro gives you the ability to clean stale records up from within the DNS zone. A quick cleanup is to open the AD zone.



Then sort by **TIMESTAMP**. You can choose to delete records in bulk here (shift or ctrl, then select) based on the age of the record. This is a good indicator that the AD Scavenging should also be adjusted.



These are just a few ways that Micetro can be used to assist you in reclaiming IP space. Micetro is designed to help administrators gain a better understanding of their networks and users.

Other useful tools to assist are the Reporting tool (to run simple reports) and the API (if you have an internal Dev/ops team) to automate the cleanup processes once they are identified.

We also offer Professional Services to assist for cleanup or automation projects https://www.menandmice.com/professional-services.

1.20.3 Converting existing access control configurations in Micetro 10.1

Micetro 10.1 updated access control management from an object-based to a role-based model. This page is intended to provide a recommendation for handling access controls in existing environments.

Upgrading to Micetro 10.1

Important: Men&Mice recommends performing a database backup before updating to 10.1.

Environments using a version of Micetro prior to 10.1 will be converted to the new model when you upgrade your Micetro components (see *Update Guide*). The database is migrated automatically. *All existing* access control configuration is preserved, but will use the new model:

- built-in roles are converted into their new *General roles* equivalents
- custom roles previously used for access control are converted into *Legacy roles*
- access settings for legacy roles on objects are preserved, using the *Specific roles* mechanism (i.e. configured on existing objects, and not applied automatically to new objects)

Automatically created Legacy roles

Legacy roles are a transitional role type to help migration and preserve backward compatibility.

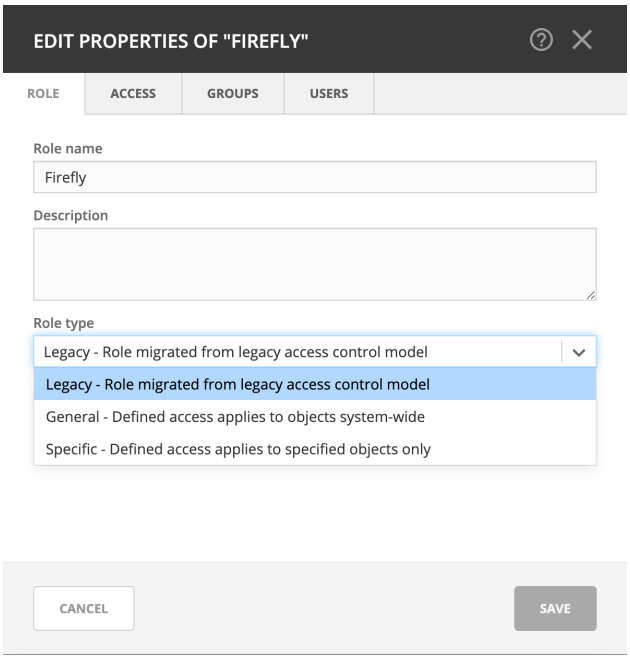
Legacy roles are generated for any user or group previously configured with *Initial access* that had general access for an object type. The legacy roles have the same permissions as their initial access.

The generated legacy roles are named after their original name. E.g. the user *Viola* will become the legacy role `Viola (converted user)` while the group *Illyria* will become the legacy role `Illyria (converted group)`.

Note: Creating legacy roles based on users and groups will leave the existing user and group intact, and automatically assigned to their respective legacy roles.

Converting Legacy roles

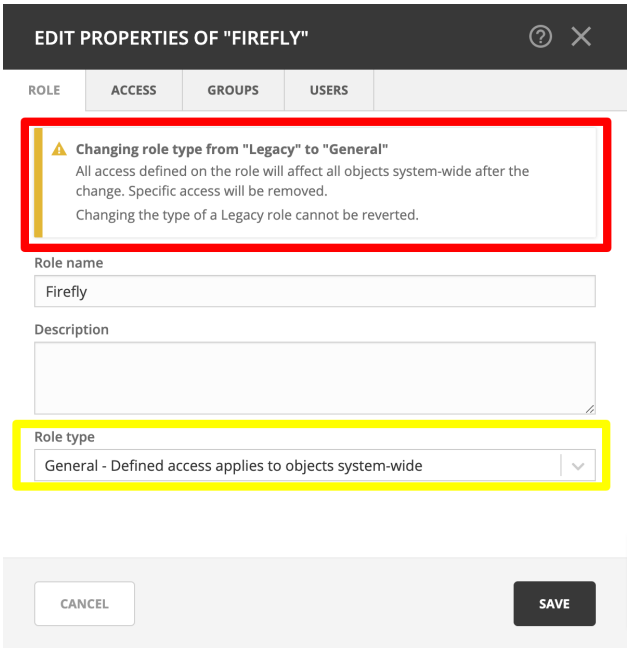
If needed, legacy roles can be converted into a general or specific role, using the dropdown in the *Edit role properties* action.



Danger: Changing the type of a legacy role **cannot** be reverted.

Converting legacy roles into General roles

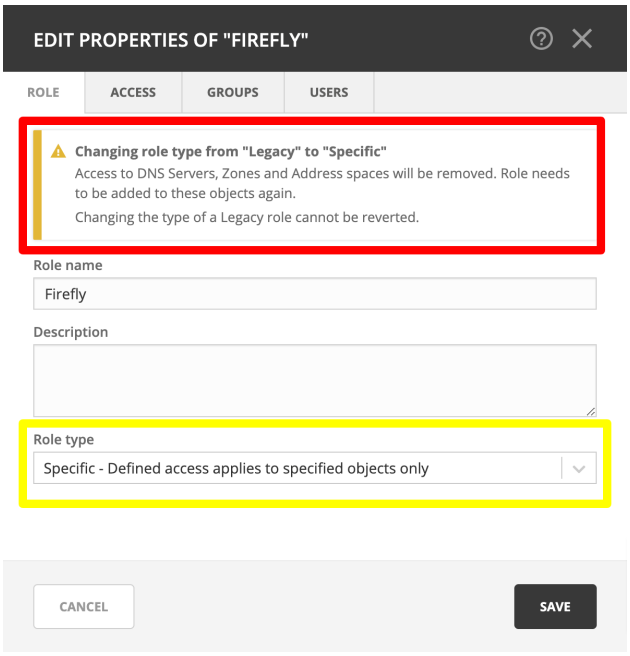
Converting a legacy role into a general role *removes all object-specific access* and makes the legacy role's configured permissions *applicable to all objects* in the system. If the legacy role had general access exclusions on specific objects, these exclusions are also removed.



Converting to Specific roles

If the legacy role was general for some object types it *will not* have access to **any** of the objects of that type after converting to specific.

Any object-specific overrides will inherit the access from the role.



Example of converting legacy role into specific

A legacy role had initial access on DNS servers previously (e.g. *list/view*) but not on zones, but was granted the role access to select zones.

After conversion:

- the role *will not have* access to any servers (even if some servers had overridden/different permissions or were excluded)
- the role *will have* access to the same zones as before, with consistent permissions across these zones

---

Note: Because of the complicated nature of matching access controls between the old and new models, Men&Mice recommends re-creating the configuration of legacy roles as specific roles, instead of changing the type.

1.20.4 Virtual Appliance Guide

Virtual DNS - DHCP Appliance Setup Guide

Introduction

Overview

The Virtual DNS/DHCP Appliance System is an integrated DNS and DHCP server focusing on performance and reliability.

This document contains information about installation and initial configuration of the Virtual DNS/DHCP Appliance.

Software Requirements

- VMWare Workstation 6.5 or higher
- VMWare ESX/ESXi 4 or higher
- VMWare Fusion 2 or higher
- VirtualBox 4.2.18 or higher

Hardware Requirements

Minimal requirements:

- 20 GB of disk space
- 4 GB RAM.
- 1 Processor Core

Recommended:

- 8 GB RAM.
- 4 Processor Cores

Installation

Setting Up the Virtual Machine

Importing the Virtual Appliance

VMWare Fusion/Workstation

1. First, download the OVA file (http://appliance.is/ddi.ova) or use http://download.menandmice.com/Appliance/ for a specific version
2. To setup the Virtual Appliance in VMWare Fusion, either double click the OVA file, or navigate to *File* → *Import*.
3. A dialog box appears that will allow you to specify the location of the OVA file. Confirm by clicking the *Open* button.

4. After specifying the name of the new virtual appliance, clicking *Import* will finalize the importing of the virtual appliance.
5. The Virtual Appliance is now ready to be started up.

VMWare ESX/ESXi

The Virtual Appliance can be imported through a template on the ESX server. As seen in figure 1, the *Deploy OVF template* is selected, and in figure 2, the deployment URL is pasted in. The next steps in the importing wizard should be self-explanatory.

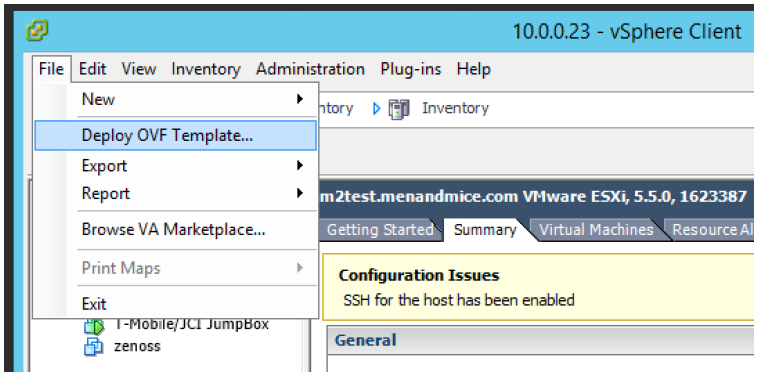


Fig. 4: Select 'Deploy OVF template from the File menu.

VirtualBox

1. First, download the OVA file use http://download.menandmice.com/Appliance/ for a specific version
2. In the VirtualBox Manager open the *File* menu and select *Import Appliance*.
3. Click on the *Open appliance* button and select the Men&Mice Virtual appliance OVA file and click on the *Continue* button.
4. The next dialog page shows an overview of the settings. It's recommended to select the option to re-initialize the MAC addresses of the two virtual interfaces eth0 (Management Interface) and eth1 (Service Interface) as shown in figure 3.

Finally press the *File –> Import Virtual Appliance button* to load the Men&Mice virtual machine into your the VirtualBox environment.

Note:

Change the Guest OS Type to Other Linux (64-bit)
: It's important to change the Guest OS Type to "Other Linux(64-bit). Otherwise the VM might get stuck during startup.

The Virtual Appliance only contains two virtual ethernet interfaces, eth0 and eth1. The eth0 interface serves as a management interface, while the eth1 interface serves as an external interface.

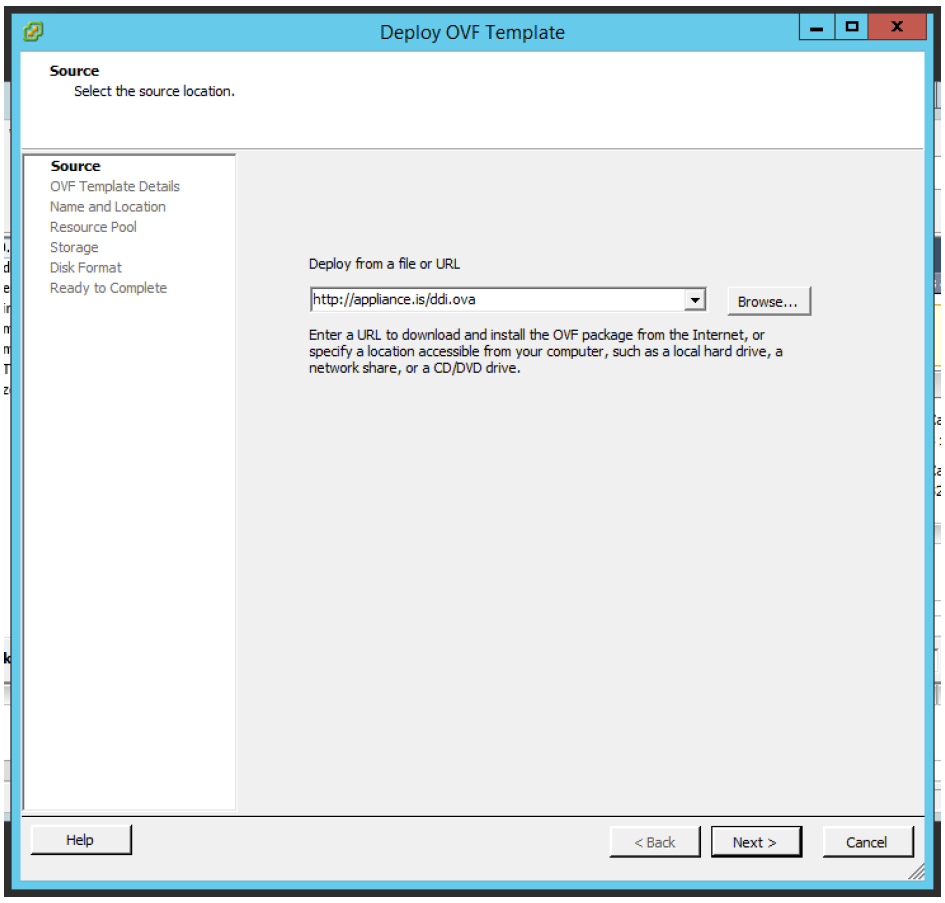


Fig. 5: Paste in the deployment URL (http://appliance.is/caching.ova) as shown and press *Next*.

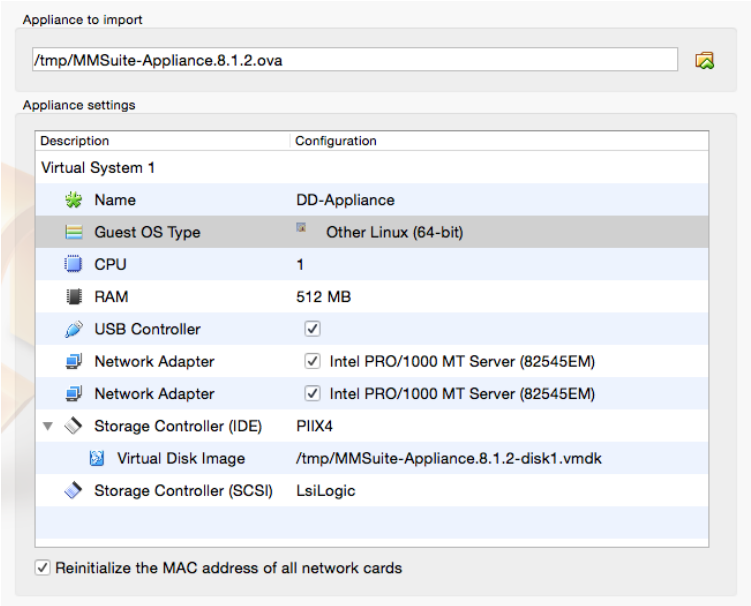


Fig. 6: Importing the Men&Mice Virtual DNS OVA image.

Configuration

Entering Appliance Network Information

This section contains instructions on how to configure the network on the appliance. That is performed through the console on the virtual host.

Once the network information has been entered, you can add the appliance to Micetro. For further information refer to appliance-management in the Micetro User's Guide.

Follow these instructions to configure the network settings:

1. Access the *Appliance* menu by pressing the Escape button and then press the Enter button on the keyboard.
2. From the main menu, select *1. Network*.
3. From the menu, select *1.1IP Address*.
4. Enter the IPv4 address for the Appliance.
5. From the menu, select *1.2 Netmask*.
6. Enter the network mask using a CIDR notation.
7. From the menu, select *1.3 Gateway*.
8. Enter the IP Address of the gateway for the network.

Adding the Appliance to Micetro

Please refer to the appliance-management chapter in the manual for instructions on how to add the appliance to Micetro.

Virtual Caching Appliance Setup Guide

Introduction

Overview

The Virtual Caching Appliance System is an integrated Caching server focusing on performance and reliability.

This document contains information about installation and initial configuration of the Virtual Caching Appliance.

Software Requirements

- VMWare Workstation 6.5 or higher
- VMWare ESX/ESXi 4 or higher
- VMWare Fusion 2 or higher
- VirtualBox 4.2.18 or higher

Hardware Requirements

Minimal requirements

- 20 GB of disk space
- 4 GB RAM.
- 1 Processor Core

Recommended

- 8 GB RAM.
- 4 Processor Cores

Installation

Setting Up the Virtual Machine

Importing the Virtual Appliance

VMWare Fusion/Workstation

1. First, download the OVA file (http://appliance.is/caching.ova) or use http://download.menandmice.com/Appliance/ for a specific version
2. To setup the Virtual Appliance in VMWare Fusion, either double click the OVA file, or navigate to *File* and select *Import*.
3. A dialog box appears that will allow you to specify the location of the OVA file. Confirm by clicking the *Open* button.
4. After specifying the name of the new virtual appliance, clicking *Import* will finalize the importing of the virtual appliance.
5. The Virtual Appliance is now ready to be started up.

VMWare ESX/ESXi

The Virtual Appliance can be imported through a template on the ESX server. As seen in figure 1, the *Deploy OVF template* is selected, and in figure 2, the deployment URL is pasted in. The next steps in the importing wizard should be self-explanatory.

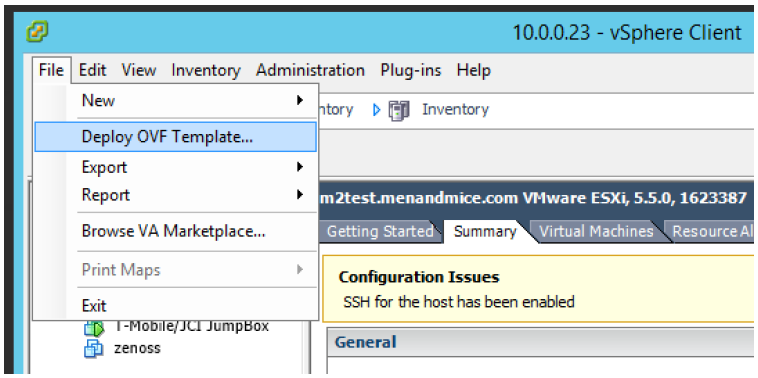


Fig. 7: Select 'Deploy OVF template from the File menu.

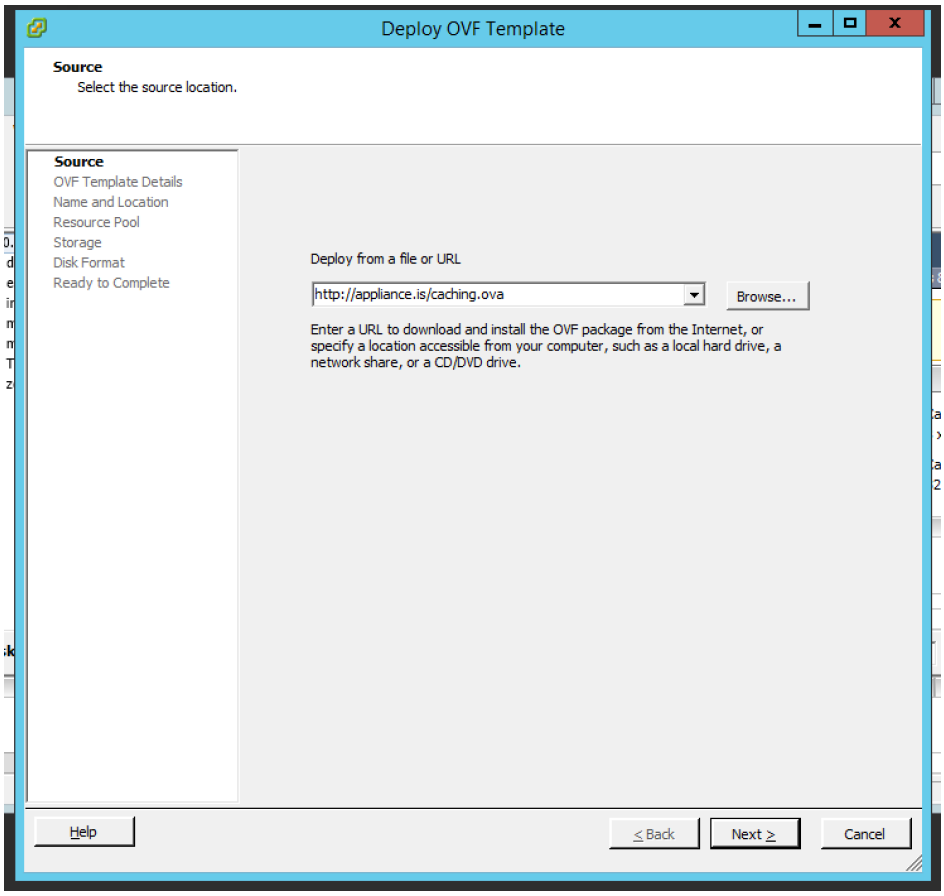


Fig. 8: Paste in the deployment URL (http://appliance.is/caching.ova) as shown and press 'Next'

VirtualBox

1. First, download the OVA file (http://appliance.is/caching.ova) or use http://download.menandmice.com/Appliance/ for a specific version
2. In the VirtualBox Manager open the *File menu* and select *Import Appliance*.
3. Click on the *Open appliance* button and select the Men&Mice Virtual appliance OVA file and click on the *Continue* button (see figure 3).
4. The next dialog page shows an overview of the settings. It's recommended to select the option to re-initialize the MAC addresses of the two virtual interfaces eth0 (Management Interface) and eth1 (Service Interface) as shown in figure 4.

Finally press the *File* → *Import Virtual Appliance* button to load the Men&Mice virtual machine into your the VirtualBox environment.

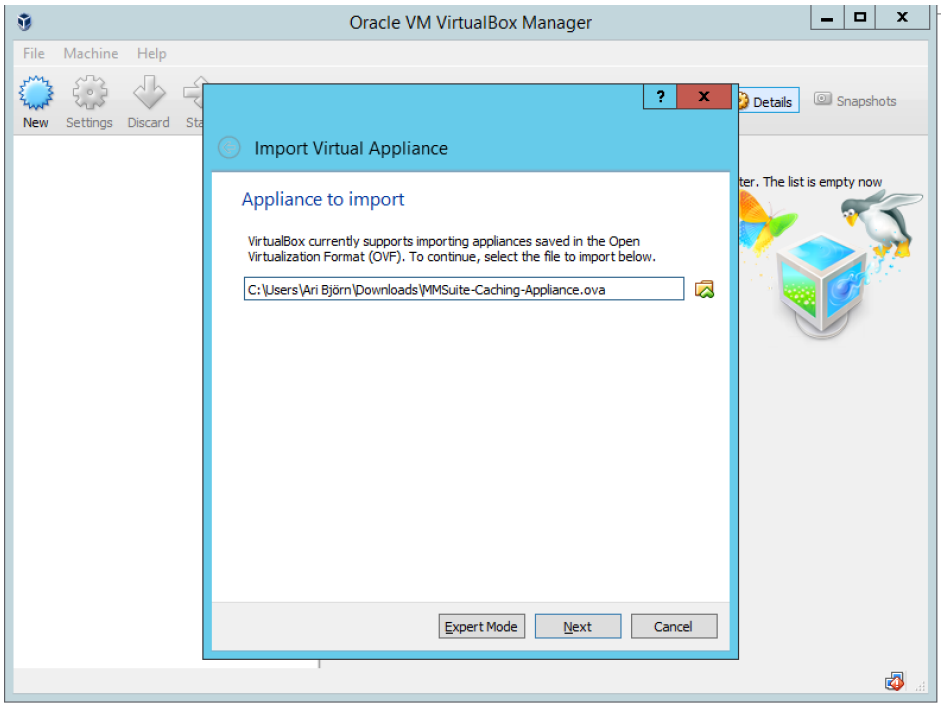


Fig. 9: Importing the Men&Mice Virtual Caching Appliance .ova image.

The Virtual Appliance only contains two virtual ethernet interfaces, eth0 and eth1. The eth0 interface serves as a management interface, while the eth1 interface serves as an external interface.

Configuration

Entering Appliance Network Information

This section contains instructions on how to configure the network on the appliance. That is performed through the console on the virtual host.

Once the network information has been entered, you can add the appliance to Micetro. For further information refer to appliance-management in the Micetro User's Guide.

Follow these instructions to configure the network settings

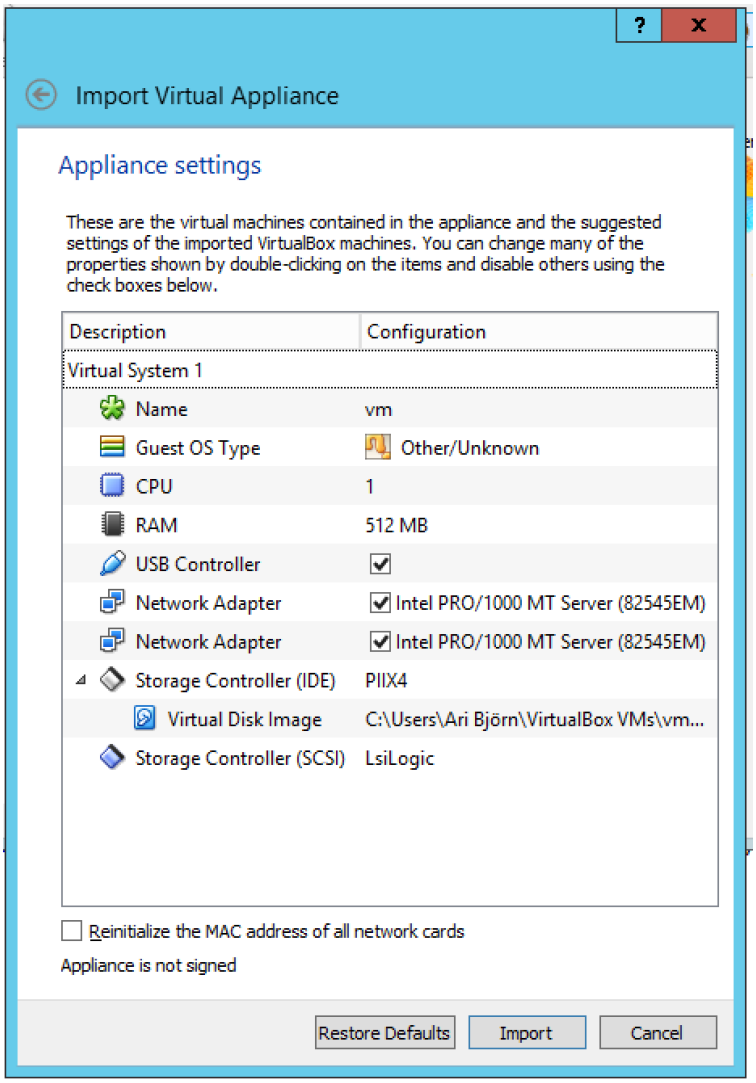


Fig. 10: Importing the Men&Mice Virtual Caching Appliance .ova image.

1. Access the *Appliance* menu by pressing the Escape button and then press the Enter button on the keyboard.
2. From the main menu, select *1. Network*.
3. From the menu, select *1.1IP Address*.
4. Enter the IPv4 address for the Appliance.
5. From the menu, select *1.2 Netmask*.
6. Enter the network mask using a CIDR notation.
7. From the menu, select *1.3 Gateway*.
8. Enter the IP Address of the gateway for the network.

Adding the Appliance to Micetro

Please refer to the appliance-management chapter in the manual for instructions on how to add the appliance to Micetro.

1.20.5 How to export and send license information

Micetro version 10.1 and above

See *Export license data*.

Micetro version *below* 10.1 (10.0, 9.3, 9.2, etc.)

1. Log into the Management console as `administrator`.
2. Open *Tools –> License Management*.
3. Take a screenshot or note down the usage numbers, and send it in an email to finance@menandmice.com.

1.20.6 Health Bar information (Management Console)

On this page, the errors / warnings from the *Health Monitoring Bar* in the Management Console are made available.

The user is able to click a link from the Management Console to get more details about each error / warning that is shown there.

Component out of date

This warning is shown when a Men&Mice component is out of date in the system. This can be confirmed by going to *Tools → Update Status*. It will show all components that are out of date in the system. From this window, they can also be updated.

Component unreachable

This error is shown when the Men&Mice Central cannot communicate with the specified component. It can be due to one of the following reasons:

- The network connection is not functional between the component and the central server. That can be due to firewall issues. See *Networking requirements*.
- The component is not turned on or has been shut down

Database has multiple schemas

This error is displayed when it has been detected that the database has multiple schemas. This can happen if the database has been migrated and not configured properly. Contact Men&Mice Support for further assistance. (See *Contacting Support*.)

Database size exceeded the recommended value

When the database is the default one (SQLite) and the size of the database is higher than the threshold of 1 GB, then this warning is shown. Collecting lease history for DHCP is one of the factors that can increase the size of the database. In cases of that and also when the network environment is considered to be large, it is recommended to use SQL Server or PostgreSQL as a database backend for Micetro. See *Microsoft SQL Server* and *PostgreSQL* for more details.

DHCP failover partner server unreachable

This error is displayed when the defined failover partner server for a DHCP server is not reachable. The reason could be a networking issue or that the DHCP service on the server is down.

Error loading zone

This warning is shown when DNS server (e.g. BIND) is unable to load its zones. This warning is also posted if the server has not successfully finished checking all zones for errors.

Failed to do a SOA request for zone

This error is shown when the Men&Mice DNS Server Controller is able to query the server, but SOA request for the zone failed.

Failed to load ODBC Driver for SQL Server

The preferred version of the Microsoft ODBD Driver for SQL Server failed to load. The latest version can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=53339.

Failover partner Down

High availability failure state

This warning is shown when the active Central server went down and a standby Central server took over the service. For some reasons active server didn't report and therefore the standby server was activated. The Standby server is updated and becomes the active server and vice versa. The former active server will be in failed state until it is fixed or restarted.

License exceeded

This warning is shown when the current license for Men&Mice component has been exceeded. For example, if the appliance license is only valid for a single appliance, and another appliance is added, then the additional appliance is not shown. Please contact sales@menandmice.com to resolve the matter.

Multiple PTR records in zone

Orphaned PTR records in zone

Outdated database server version

For Men&Mice Suite version 8.1 and higher we recommend to use only SQL Server 2014 or higher. Support for older versions will be dropped in version 8.2 of the Men&Mice Suite.

Scope contains inconsistencies that need reconciling

This warning is shown when scope contains inconsistencies and it needs reconciling. See console-dhcp-windows-reconcile and https://technet.microsoft.com/en-us/library/dd183579(v=ws.10).aspx about reconciling a DHCP scope.

Scope is not part of a failover relationship on partner server

This warning is shown when scope is not a part of a failover relationship on partner server, but should be.

Scope pool collision

This warning is shown when one of the following situations occur:

- Scopes in a failover relationship have mismatching address pools or exclusions. Failover scopes should be identical.
- An address pool conflict was detected. Addresses exist in multiple pools without exclusions.
- An address pool conflict was detected. The address pool is not identical across the split scope.
- An address pool conflict was detected.

Cloud Subnet Collision

Scope reservation mismatch

This warning is shown when DHCP reservations do not match, that is name, MAC address and description are not identical.

Slave zone not updated from master or is about to expire

This warning is shown when a slave zone is not receiving an update from its master. This warning could also be shown when a slave zone is not receiving update from its master and is about to expire.

Superscope, subnet, static or dynamic part of scope over utilized

This warning is shown when a specific threshold is reached, that is, not enough IP addresses is available in this range. To fix this issue remove the scope and create a larger one instead or create a super scope which will join together two or more scopes for larger one.

Unable to check whether scope contains inconsistencies

This warning is shown when Men&Mice Central can't connect to the DHCP Server Controller service to check whether scope contains inconsistencies. The reason could be if the DHCP Server Controller is offline or not turned on.

Unable to check whether scope is part of a failover relationship on partner server

This warning is shown when Men&Mice Central can't connect to the DHCP Server Controller service to see if a scope is a part of a failover relationship on partner server. The reason could be if the DHCP Server Controller is offline or not turned on.

Unable to fetch scope info from partner server

This warning is shown when Men&Mice Central can't connect to the DHCP Server Controller service to gather scope info from partner server. The reason could be if the DHCP Server Controller is offline or not turned on.

Unable to get status for DNS or DHCP server

This warning is shown when Men&Mice Central is unable to connect to DNS or DHCP Server Controller to do a status check for the server. This occurs if the Server Controller is offline, not turned on or has been shut down (in some case not installed). To fix this issue get the server online again and turn on the remote or (re)install.

Unable to get status for scope

This error is shown when Men&Mice Central can't connect to the DHCP Server Controller service to get scope status from DHCP server. The reason could be if the DHCP Server Controller is offline or not turned on.

Unable to get status for zones

This warning is shown when Men&Mice Central can't connect to the DNS Server Controller service to get status on the zones. The reason could be if the DNS Server Controller service is turned off or is offline.

Update available

This warning is shown when new version of Micetro is available. To get this new version go to *Tools* → *Check for updates* in the menu bar and run the update wizard.

Update server unreachable

This warning is shown when Men&Mice Central has lost its connection to Men&Mice update server. It is not mandatory to have this connection and it can be turned off. To fix this issue make sure that machine running the Men&Mice Update service and the machine running the Men&Mice Central are listening to the same TCP port. TCP port `4603` is reserved for the update service but it can be changed if there is another software using that TCP port. See *Changing the TCP port for the Men&Mice Update Service* about changing the TCP port.

Zone replication group out of sync

This error is shown when a member of a zone replication group is out of sync.

Zone serial out of date

1.20.7 Dynamic Zones

Overview

Micetro allows you to work with dynamic zones on BIND and the Windows DNS server.

This section describes how Micetro handles dynamic zones and how to configure your DNS server to allow the program to work with dynamic zones.

Static vs. Dynamic Zones

Due to the nature of dynamic zones, the Management Console must handle such zones differently from static zones. Below, you will find information on how the software handles dynamic zones compared to static zones.

Static zones	Dynamic Zones
The zone content is read from disk on the server.	The zone content is retrieved from the server via a zone transfer.
Records can be enabled and disabled. Disabled records are commented out in the zone files.	Disabling records is not possible.
Specifying a TTL value for individual records is optional.	Every record must have a TTL explicitly set.
Every resource record can have a comment associated with it.	Comments are not supported for records.

BIND Server Configuration

The Management Console only supports TSIG signed dynamic updates. Therefore, you will have to create a TSIG key on each of your master DNS servers. If a TSIG key already exists, the program will use the first key it finds in the server configuration files (usually in /var/named/conf/user_before)

To create a TSIG key to use with BIND:

1. Check if there is a key already created in /etc/rndc.key (or its equivalent). If there is, simply copy its contents into the file user_before. Then skip the rest of these instructions.
2. Create a new key using the command rndc-confgen, like this: rndc-confgen -a This will create a file named rndc.key, typically in either /etc or /etc/bind. The contents of the file will look something like this:

```
key rndc-key { algorithm hmac-md5; secret "Qqn05iUpjzmNoXxLJi5vXw=="; };
```

3. (Re)start named (or signal it with either kill –HUP <pid> or rndc reconfig) in order to have it reload its configuration files.
4. Restart mmremoted:

```
/etc/init.d/mmremote stop /etc/init.d/mmremote start
```

When you have configured the server, you can change the zone type from static to dynamic by opening the zone options in the Management Console and changing the zone type to dynamic.

As dynamic zones are transferred from the DNS server using a zone transfer, you should make sure that zone transfers are allowed to localhost.

Windows DNS Server Configuration

- The Men&Mice Management Console can work with dynamic zones on the Windows DNS server, both AD integrated zones and file-based zones.
- A new column, Record timestamp, is shown for dynamic zones that are hosted on Windows DNS servers. The Record timestamp column will show the creation time for records that are added dynamically (dynamic records). Static records will not have a record timestamp.
- Dynamic zones are transferred from the DNS server using a zone transfer. If you restrict zone transfers from your DNS server, you should make sure that zone transfers are allowed to the IP Address of the DNS server itself.
- It is not possible to disable dynamic zones that are hosted on the Windows DNS server. This is the only limitation.

1.20.8 Configuring Amazon Route53

Note: Since the addition of native Route53 support for AWS DNS, the recommended way of adding a Route53 server to Micetro is through *Cloud integration*.

1.20.9 Configuring PowerDNS

The PowerDNS connector script connects directly to the MySQL backend and allows management of zones in PowerDNS. Native mode and Primary/Secondary mode in the authoritative PowerDNS are currently supported.

The installation works as described above. On Linux use the `--generic-dns-controller` parameter when executing the installer.

It will then install the base Generic DNS Server Controller, but there are two things you want to tweak:

1. Create working directory and connector script config:

```
mkdir /var/mmsuite/dns_server_controller
```

and set the correct ownership.

2. Create a file `preferences.cfg` in the `mmsuite` directory and configure the connector script with a XML-tag as described in Generic DNS Server Controller.

E.g. on Linux:

```
<GenericDNSScript value="python /your/script/directory/genericDNSPowerDNS.py" />
```

Download the script from GitHub.

4. Edit the `systemd/init` script of the controller. Open with an editor, e.g. vi the `mmremote` init script, which should be `/etc/init.d/mmremote`.
5. Search for the line `PARAMS="...."`.
6. Add to the begin of the parameter list your created controller working directory with the `-d` parameter, .i.e.:

```
PARAMS="-d /var/mmsuite/dns_server_controller  ...rest of the params"
```

1.20.10 named.conf validation

The Men&Mice DNS Server Controller (`mmremote`) relies on the BIND tool `named-checkconf` to verify if the BIND configuration `named.conf` is valid.

If the `named-checkconf` is not found on any of the standard directories during installation (or if the installation is inside a CHROOT), the *Advanced* button is not shown.

To fix this, add a configuration parameter pointing to the `named-checkconf` tool to the DNS Server Controller configuration file `preferences.cfg` (usually in `/var/named/mmsuite/preferences.cfg`)

```
<fingerprint value="<some-hex-values>"/>
<named-checkconf value="/usr/sbin/named-checkconf"/>
```

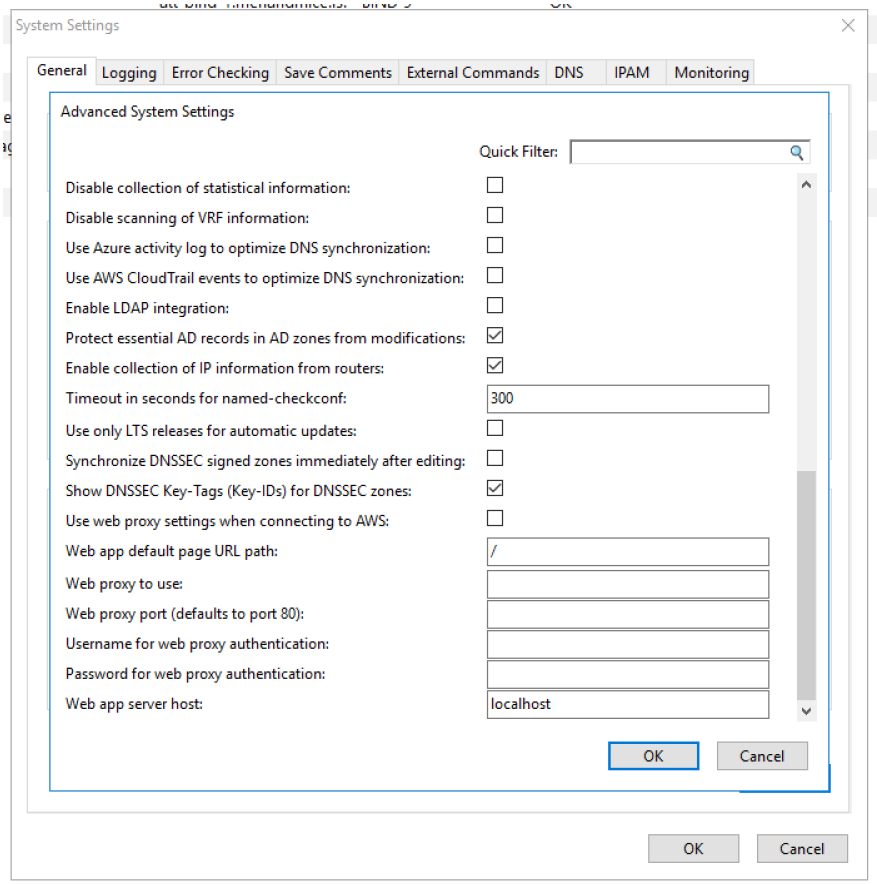
Make sure that the `named-checkconf` tool is executable and reachable for the DNS Server Controller (if the DNSServer Controller is inside a CHROOT environment, the `named-checkconf` must also be inside that CHROOT as well as all dynamic libraries needed).

Note: After changing the configuration file for the DNS Server Controller, the DNS Server Controller process (`mmremoted`) must be started.

1.20.11 Updating timeout value for named-checkconf

To ensure the system runs smoothly, use the Management Console to update the default timeout value for the `named-checkconf` files.

1. Log in to the Management Console
2. Navigate to *Tools* → *System Settings* → *Advanced*.
3. Filter the options with "timeout", and locate the "*Timeout in seconds for named-checkconf*" line.
4. Set the value to **300**.



1.20.12 Changing the TCP port for the Men&Mice Update Service

The Men&Mice update service is listening by default on port `4603/TCP`. Although the port `4603/TCP` is reserved for the Men&Mice Update service in the IANA database, there might be a different software already running on that port.

The TCP port for the updater service can be changed. It must be changed on the `mmupdate` service and also on Men&Mice Central (`mmcentral`). All remote servers must listen on the same TCP port for update messages from Men&Mice Central. It is not possible to run the Men&Mice Update service on different ports for different servers.

1. Stop both services, the Men&Mice Central service and the remote Men&Mice updater service.
2. On the machine running the Men&Mice Update service, append the following line to the Men&Mice Updater's `preferences.cfg` file (create the file if it does not exist):

```
<Arguments value="-p 12345" />
```

Where `12345` is the TCP port number the Men&Mice update service should use.

3. Start the Men&Mice Update service and check that the process in listening on the new port (using `netstat -na` or `lsof -i`).
4. On the machine running the Men&Mice Central service, append the following line to the Men&Mice Central `preferences.cfg` file (create the file if it does not exist):

```
<UpdateAgentPortNumber value="12345" />
```

Where `12345` is the TCP port number the Men&Mice update service is using on the remote system(s).

5. Start the Men&Mice Central service.

1.20.13 Setting up a Managed Service Account to run M&M DNS/DHCP Server Controllers

Managed Service Account was introduced in Windows Server 2008 R2. Managed Service Account is managed domain account that provides the following features to simplify service administration:

- Automatic password management.
- Simplified SPN management, including delegation of management to other administrators. Additional automatic SPN management is available at the Windows Server 2008 R2 domain functional level.

Managed Service Account is good addition to Local Services to run M&M DNS/DHCP Server Controllers. When using MSA you gain managed domain account with isolated privileges to run the application.

Step-by-step guide

1. If you are running Windows Server 2012 or newer then the first step is to run:

```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

This is because Manage Service Account feature came with Windows Server 2008. But in Windows Server 2012 a new service called the Key Distribution Service (KDS) came also and needs to be running to create and use Group Manage Service Accounts.

2. Create new ADServiceAccount:

```
New-ADServiceAccount -DNSHostName "yourserver" -Name "name of the service account" -
↪PrincipalsAllowedToRetrieveManagedPassword "here you list your servers ending with '$'␣
↪and separated with ',' for example: TESTSERVER$, TESTESERVER2$"
```

3. Install the service account:

```
Install-ADServiceAccount "name of the service account"
```

4. Add the right authority to the Managed Service Account:

In Server Manager dashboard click on Tools and choose Active Directory Users and Computers. Click on Users, right click on the group to add the Managed Service Account to. For example DNSAdmins or DHCP Admins.

5. Add the Managed Service Account to M&M DNS/DHCP Server Controllers:

Go to Services and locate the M&M controllers, right click on them and choose Properties. In the Properties window click on Log On tab and choose This Account. Fill in the name of the service that was made in step 2. That is DOMAINServiceAccountName ending with '$' sign. Click OK and restart the M&M DNS/DHCP Server Controller.

To remove Managed Service Account from M&M DND/DHCP Server Controllers run cmd and write in the command:

```
sc.exe managedaccount "Men&Mice DNS/DHCP Server Controller" false
```

Information gathered from this Microsoft article.

1.20.14 BIND DNS File Structure

Overview

When Micetro is installed on a server running BIND, it needs to perform several changes to the server configuration file structure. This section describes these changes and includes an overview diagram that shows how the server configuration files are processed after Micetro has updated the structure.

named.conf

`named.conf` is split into several files. A new `named.conf` file that includes statements for all the new files is created.

When `named.conf` is split up, a new file is created for each zone statement (see *Zone Options Files* files, below).

The options statement goes into a separate file. That file is modified when the user makes changes to the server options in the Men&Mice Management Console.

The current version of the Men&Mice Management Console has no interface to change the values of the following statements: `key`, `acl`, `controls`, `server`, `trusted-keys`. Therefore, they are kept in separate files, `user_before` and `user_after`. Micetro does *not* modify these files.

The hint zone is copied to `/var/named/conf/root.hint`. That file is modified when the user makes changes in the *Root servers* tab in the server options in the Men&Mice Management Console.

Zone Options Files

A new file, `/var/named/conf/zones` is created. It contains a list of includes for zone option files which are stored in the directory `/var/named/conf/zoneopt/`, one for each zone. The zone options (or definitions) files are called `<zonename>.opt`.

Zone Files

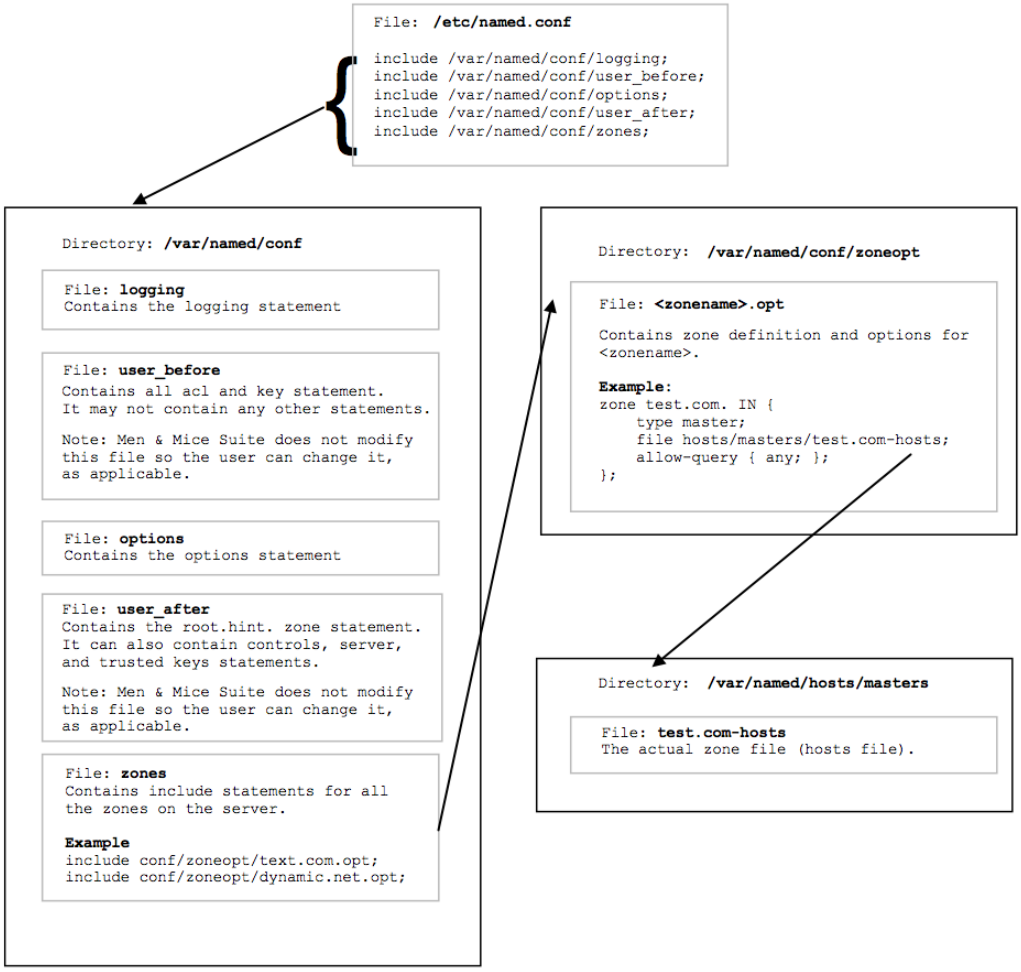
No changes are made to the zone files themselves. The installer copies the zone files to different directories, depending on their types:

- master and forward zones are copied to `/var/named/hosts/masters/`
- slave and stub zones are copied to `/var/named/hosts/slaves/`

The new zone file is named `<zonename>-hosts`.

Configuration Files Diagram

The following diagram provides an overview on how the configuration files are processed after the file structure has been updated by Micetro.



1.20.15 Disable "Automatic adjustment of Zone Transfer"

By default, Micetro automatically adjusts zone transfer settings for slave zones. If this is not a desired behavior for your environment, you can disable it:

1. Log in to the Management Console
2. Navigate to *Tools* → *System Settings* → *Advanced*.
3. Filter the options with "automatically", and locate the "*Automatically adjust local zone transfer settings for BIND*" line.
4. **Uncheck** the box to disable.

1.20.16 Men&Mice DNS Server Controller and $INCLUDE Directives

BIND supports several extensions to the standard zone file format, known as directives or control statements; all directives start with `$`. With one exception, the `$TTL` directive, Micetro doesn't display these directives in the zone window.

Instead, when directives other than `$TTL` are present, the Management Console zone window displays an extra button in the button bar, on the right end. This button, labeled *Zone control statements*, brings up a window showing all of these statements in raw form. The Management Console does not allow these statements to be edited; instead, all editing of such statements must be done by editing the zone file directly, on the server.

The $INCLUDE directive

This directive tells named to load the contents of another file as part of the zone, using the current origin and default TTL. Unfortunately, they often cause problems with Men&Mice Suite.

`$INCLUDE` statements are usually present only if they were present before the DNS Server Controller was installed, since Men&Mice Management Console doesn't provide a way to create them. The Men&Mice DNS Server Controller installer doesn't parse all of the zone files during installation, so it's not aware of `$INCLUDE` directives; therefore, they usually get left behind in the old copy of the data directory (which is renamed to add ".bak" to the end of its name). Furthermore, while most affected users realize this, the common mistake is to copy or move the included file into the same location as the zone file. This is not correct.

Instead, since an included file is usually only specified by name, it must be placed into the root of the data directory tree. For example, if the zone file is in `/var/named/hosts/masters`, the included file must be placed in `/var/named`.

Lastly, it's possible to use an include file in a way that, while perfectly valid as far as `named` is concerned, makes the zone look invalid to Men&Mice Management Console's syntax check. If the zone's authority NS records and/or SOA record are located in an include file, the Management Console will not allow you to save the file. This can be solved by configuring the DNS Server Controller to (permanently) expand control statements.

Using the $INCLUDE directive with Micetro

The Men&Mice DNS Server Controller can be configured to expand `$INCLUDE` statements, so that you see the entire contents of the zone in the zone window.

Note: If you configure Men&Mice DNS Server Controller to expand `$INCLUDE` statements, it will do so globally, for all zones. It will also expand all other control statements (not counting the $TTL directive at the top of each zone). The expansion is permanent, meaning the zone file is actually changed to reflect the effect of the control statement, and the control statement is removed.

To follow these instructions, you'll need to figure out where your named data directory is, which we'll refer to as `$NAMED`. This can be done by examining `named.conf`. If you're not sure where `named.conf` is, examine your DNS Server Controller (`mmremoted`) command line (in the output of the appropriate `ps` command) - it should show the location of `named.conf` after `-c`; if there's a `-t` option as well, the `named.conf` location will be relative to this chroot jail path. If you don't see either of these options, the location is `/etc/named.conf`. (And if this sounds like gibberish to you, please contact us for help.)

`named.conf` contains a set of 5 `include` statements, referring to the absolute path of files in `$NAMED/conf/`. So if your $NAMED directory is `/var/named`, the include statements will look like this:

```
include "/var/named/conf/logging";
include "/var/named/conf/user_before";
include "/var/named/conf/options";
include "/var/named/conf/user_after";
include "/var/named/conf/zones";
```

Edit the file `$NAMED/mmsuite/preferences.cfg`. Add the following line:

```
<ExpandControlStatements value="1"/>
```

Save the file and restart the DNS Server Controller, using its init script (a file named *mmremoted*, such as `/etc/init.d/mmremoted`, or `/Library/StartupItems/mmServerController/mmServerController` - the location is platform-specific). You can then log in with the Management Console to see the effects of this process.

On Mac OS X, use the following shell commands to complete these instructions:

To edit the file:

```
sudo nano /var/named/mmsuite/preferences.cfg
```

Within nano, use the keyboard arrow keys to move around, since there's no mouse support. When you're done editing, type control-o to save, followed by the return or enter key to confirm the filename. Then type control-x to exit.

To restart DNS Server Controller:

```
sudo /Library/StartupItems/mmServerController/mmServerController start
```

1.20.17 Expanding $GENERATE directives into records

BIND supports several extensions to the standard zone file format, known as directives or control statements; all directives start with `$`. With one exception, the `$TTL` directive, Micetro doesn't display these directives in the zone window.

Instead, when directives other than `$TTL` are present, the Management Console zone window displays an extra button in the button bar, on the right end. This button, labeled *Zone control statements*, brings up a window showing all of these statements in raw form. The Management Console does not allow these statements to be edited; instead, all editing of such statements must be done by editing the zone file directly, on the server.

The $GENERATE directive

This directive is a shorthand way of entering multiple similar records. The directive is a line that looks like this:

```
$GENERATE range template
```

Where "range" is a numeric range such as "1-254" and "template" is a record template. A record template looks like a normal record (except it doesn't start on the beginning of a line), but in places where a number from the range is desired, a "$" is used as a placeholder.

For example:

```
$GENERATE 1-254 $.0.168.192.in-addr.arpa. PTR host-$.dsl.example.net.
```

This would create 254 PTR records, all of similar format, looking like this:

```
1.0.168.192.in-addr.arpa. PTR host-1.dsl.example.net.
2.0.168.192.in-addr.arpa. PTR host-2.dsl.example.net.
[...]
254.0.168.192.in-addr.arpa. PTR host-254.dsl.example.net.
```

Of course, while these records are generated by named when the zone is loaded, you won't see them in the zone file. All you'll see is the `$GENERATE` directive.

Using the $GENERATE directive with Micetro

The Men&Mice DNS Server Controller can be configured to expand `$GENERATE` statements, so that you see the records thus generated in the zone window. These will be ordinary records, so you can edit them freely.

Note: If you configure Men&Mice DNS Server Controller to expand `$GENERATE` statements, it will do so globally, for all zones. It will also expand all other control statements (not counting the $TTL directive at the top of each zone). The expansion is permanent, meaning the zone file is actually changed to reflect the effect of the control statement, and the control statement is removed.

To follow these instructions, you'll need to figure out where your named data directory is, which we'll refer to as `$NAMED`. This can be done by examining `named.conf`. If you're not sure where `named.conf` is, examine your DNS Server Controller (`mmremoted`) command line (in the output of the appropriate `ps` command) - it should show the location of `named.conf` after `-c`; if there's a `-t` option as well, the `named.conf` location will be relative to this chroot jail path. If you don't see either of these options, the location is `/etc/named.conf`. (And if this sounds like gibberish to you, please contact us for help.)

`named.conf` contains a set of 5 `include` statements, referring to the absolute path of files in `$NAMED/conf/`. So if your `$NAMED` directory is `/var/named`, the include statements will look like this:

```
include "/var/named/conf/logging";
include "/var/named/conf/user_before";
include "/var/named/conf/options";
include "/var/named/conf/user_after";
include "/var/named/conf/zones";
```

Edit the file $NAMED/mmsuite/preferences.cfg. Add the following line:

```
<ExpandControlStatements value="1"/>
```

Save the file and restart the DNS Server Controller, using its init script (a file named *mmremoted*, such as `/etc/init.d/mmremoted`, or `/Library/StartupItems/mmServerController/mmServerController` - the location is platform-specific). You can then log in with the Management Console to see the effects of this process.

On Mac OS X, use the following shell commands to complete these instructions:

To edit the file:

```
sudo nano /var/named/mmsuite/preferences.cfg
```

Within nano, use the keyboard arrow keys to move around, since there's no mouse support. When you're done editing, type control-o to save, followed by the return or enter key to confirm the filename. Then type control-x to exit.

To restart DNS Server Controller:

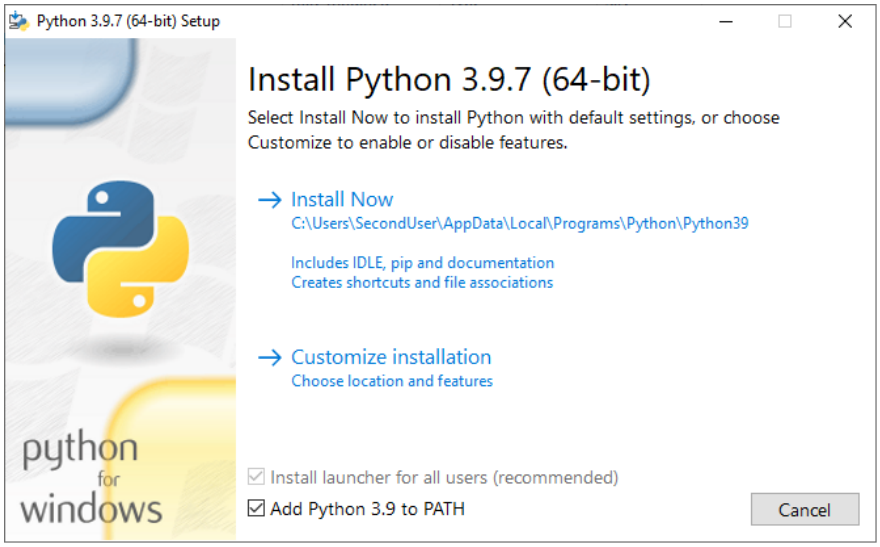
```
sudo /Library/StartupItems/mmServerController/mmServerController start
```

1.20.18 Installing Python for Men&Mice Central on Windows

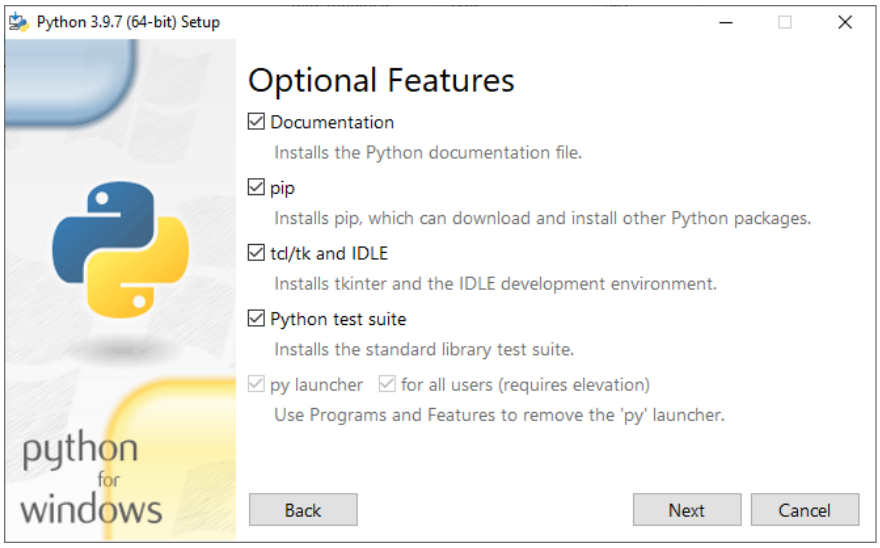
Using LDAP (see *Configure LDAP authentication*) with *Men&Mice Central* on a Windows server requires Python to be installed for all users.

If you haven't yet installed Python, or just for the current user, follow these steps:

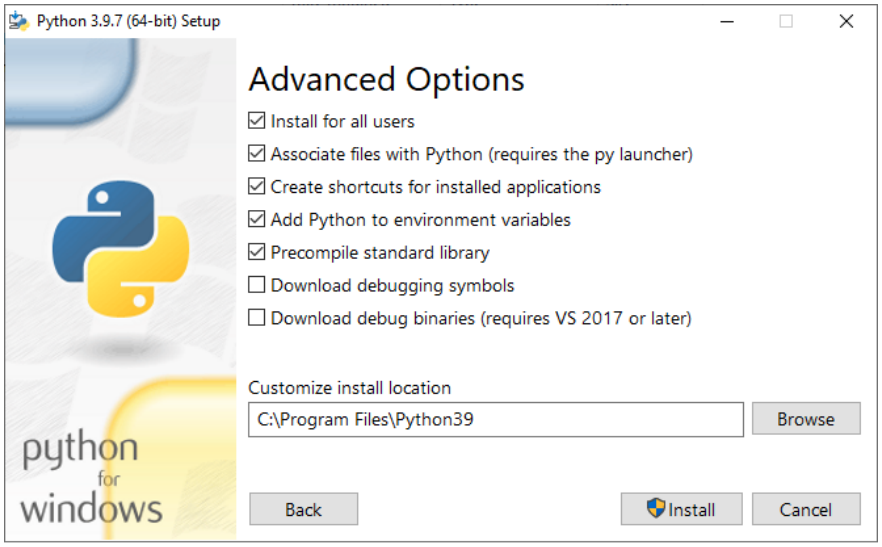
1. Download and run the installer for Python from https://www.python.org/downloads/windows/.
2. On the first screen, select *Add Python 3.x to PATH* and click *Customize installation*.



3. Select the optional features. Central only requires **pip** to be installed.



4. On *Advanced features*, enable *Install for all users*. (Leave the rest unchanged.)



5. Proceed with the installation.
6. Restart Central, if it's already running.

1.20.19 Which SNMP OIDs are used by Micetro in IP address and Subnet Discovery

Micetro has the capability to scan a defined list of routers and retrieve the ARP tables and/or the subnets and their information found on the routers.

To perform this scanning, the following suite of SNMP OIDs are used:

IP-MIB:

- ipNetToMediaPhysAddress: .1.3.6.1.2.1.4.22.1.2
- ipAdEntAddr: .1.3.6.1.2.1.4.20.1.1
- ipAdEntIfIndex: .1.3.6.1.2.1.4.20.1.2
- ipAdEntNetMask: .1.3.6.1.2.1.4.20.1.3

ENTITY-MIB:

- entPhysicalSerialNum: .1.3.6.1.2.1.47.1.1.1.1.11

SNMPv2-MIB:

- sysName: .1.3.6.1.2.1.1.5

CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB:

- cviRoutedVlanIfIndex: .1.3.6.1.4.1.9.9.128.1.1.1.1.3

CISCO-VRF-MIB:

- cvVrfInterfaceType: .1.3.6.1.4.1.9.9.711.1.2.1.1.2
- cvVrfName: .1.3.6.1.4.1.9.9.711.1.1.1.1.2

Note: Each device is only queried once, as the system checks the serial number and the sysName to discover both physical and virtual switches.

For detailed information on the preferred method of access management, see *Access Management*.

1.20.20 Managing access control in the Management Console

Access control management in the Management Console uses the new access control model, but its features are slightly different than those available in the Web Application.

Note: Men&Mice recommends configuring and managing access through the Web Application, as the preferred method. Functionality in the Management Console is mostly implemented in a transitional capacity.

Key differences between the Web Application and the Management Console

Effective access

In the Management Console's *Tools* → *User Management*, the functionality for *Effective access* is not available.

Users and groups

In the Management Console's *Tools* → *User Management*, users and groups cannot be edited to assign roles. Instead, roles need to be configured with users and groups.

Roles

In the Management Console's *Tools* → *User Management*, adding a new role doesn't allow configuring access for it.

Configuring access in the Management Console

Adding a new role

1. Open *Tools* → *User Management* and switch to the **Roles** tab.
2. Click *Add*.
3. Fill in the name and description for the role. Optionally, you can add users and groups to the role.
4. Click *Ok*.

Important: The function for *creating* the role doesn't contain options to set access for it in the Management Console. For configuring access, follow the steps in *Configuring access for a role*.

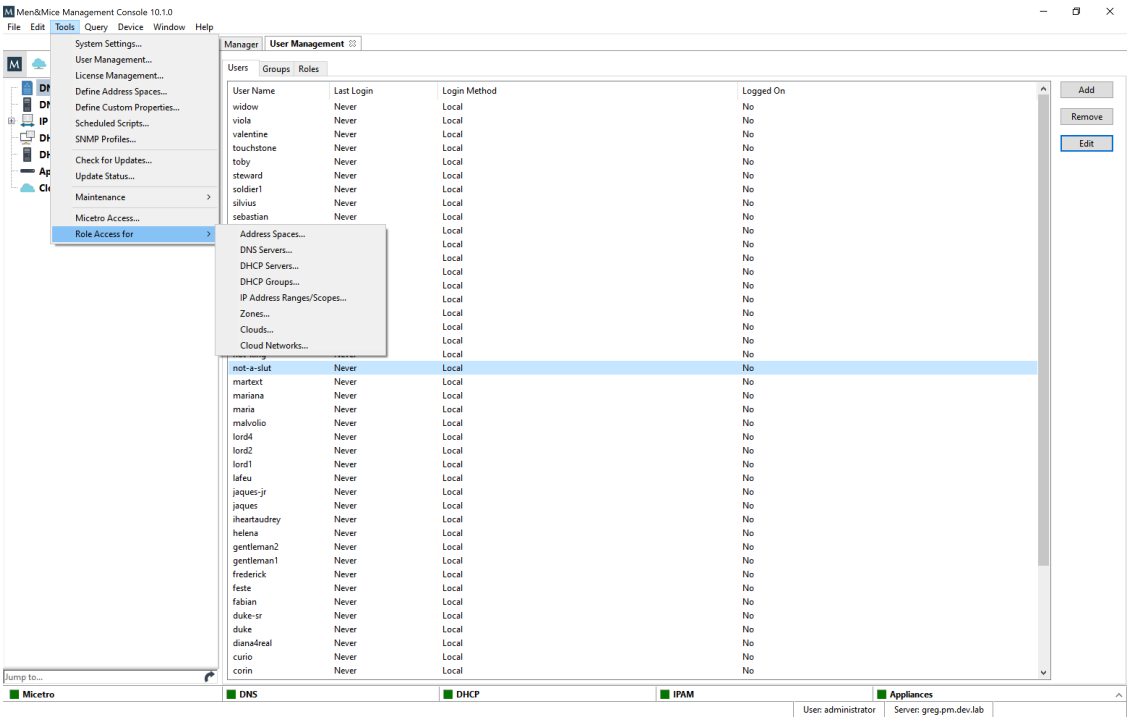
Configuring access for a role

Note: Unlike the in Web Application, configuring access for roles is sectioned by object type (i.e. DNS servers, zones, clouds, etc.).

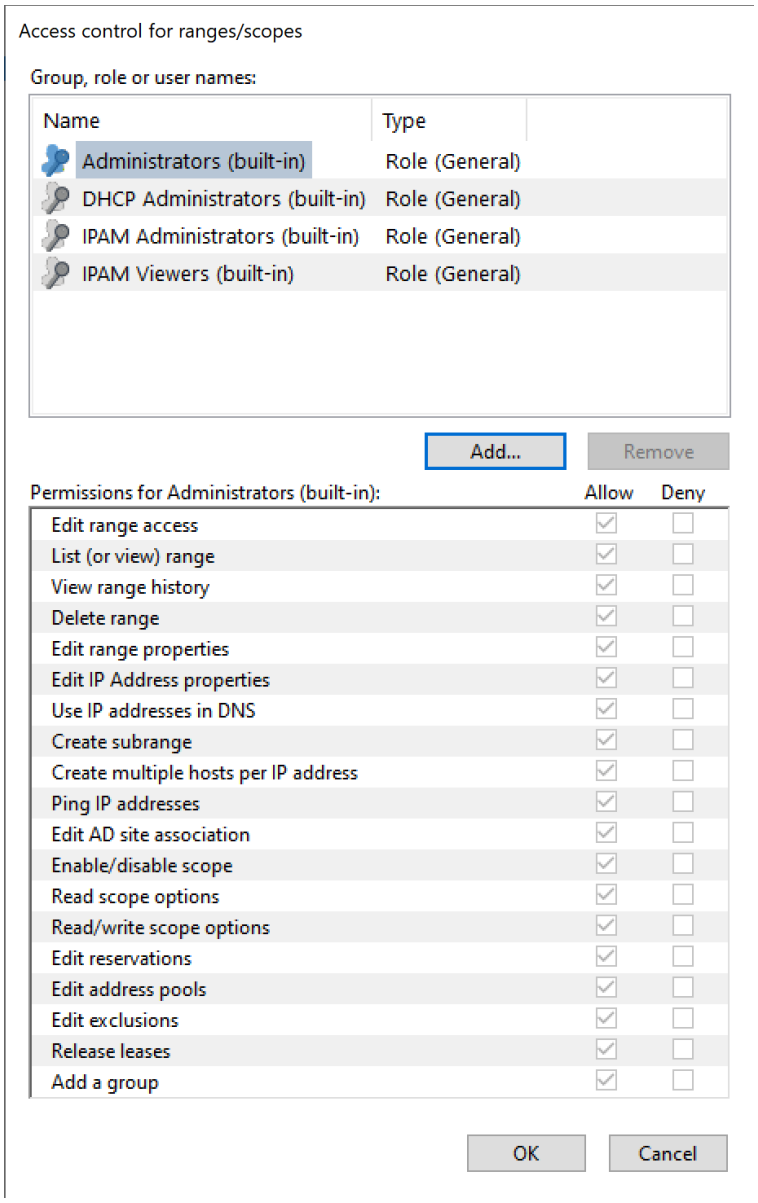
---

1. Open *Tools* → *Role access for* and select the object type from the menu.

Note: To manage access for Micetro (module access, setting user admins, etc.) use *Tools* → *Micetro access*.



2. In the **Access control** dialog, you'll see all roles that have relevant access configured on them.



3. To configure access for the selected object type to a role:

   3/1. Select the role in the top window, or click Add… to add a role that doesn't have access configured for the object type yet.

   3/2. In the bottom panel, select all checkboxes for the access permissions you'd like to enable.

Note: Selecting **Deny** is the equivalent of **Block** in the Web Application. See *Block permission* for more details. Setting 'deny' on a permission will block any other role to overwrite this setting.

---

4. Click *OK* when all the desired access permissions are set.

Removing a role

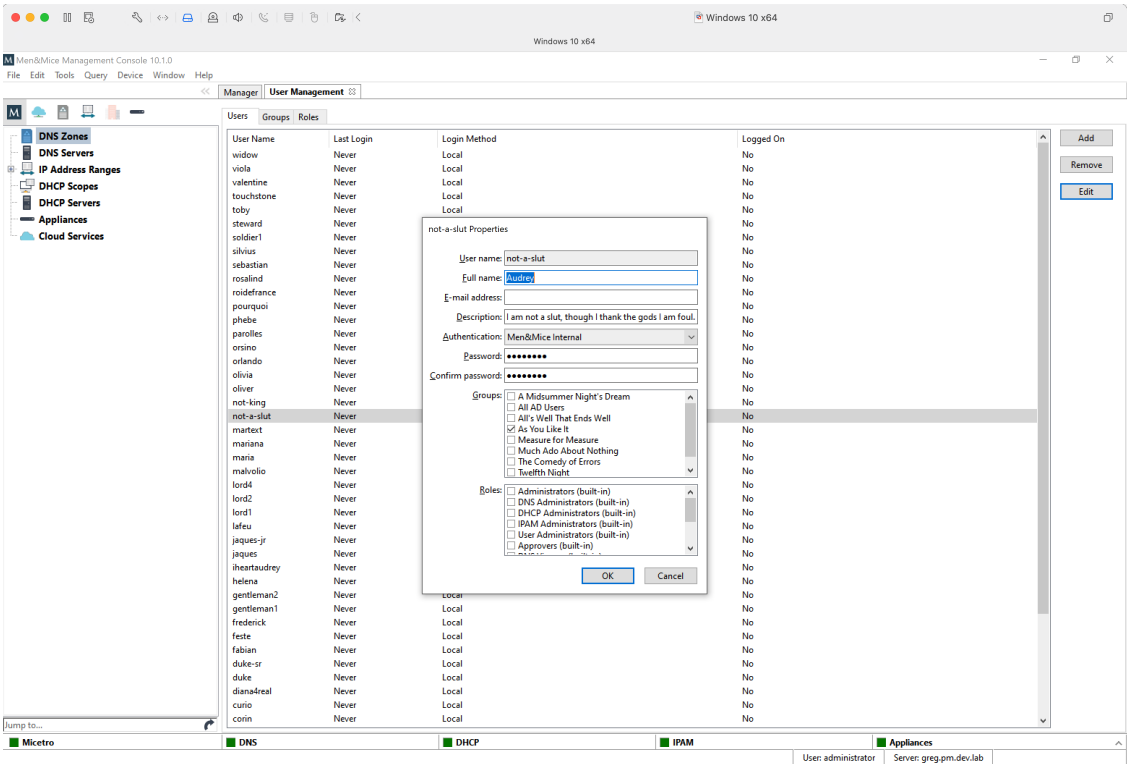
To *remove a role's access permissions from an object type* use the *Tools → Role access for* menu. Select the role in the top panel and click on *Remove*. This will remove all configured access permissions from the role, but **not the role itself**.

To *remove a role from Micetro* use *Tools → User Management* and click on the **Roles** tab. Select the role(s) to remove, and click *Remove*. This will remove **the role and all its configured access permissions** from Micetro completely.

Adding users and groups to a role

To add users or groups to a role:

1. Open *Tools → User Management*.
2. Select the user(s) and/or group(s), click *Edit* and in the bottom panel select the roles to attach the user(s)/group(s) to.



3. Click *OK* to save the new membership settings.

Note: Using the **Roles** tab of *Tools → User Management*, examining a role will display the users and groups attached to the role, but cannot be used for adding users/groups to it.

1.20.21 Role-based access example

Note: Access management has changed in Micetro 10.1. To view the access management example used in previous versions, switch to the appropriate version number using the version selector.

Introduction

This article aims to provide practical information on *Roles* and detailed, step-by-step breakdowns for two scenarios: creating a new, read-only role for DHCP scopes, and using the built-in *DNS viewers* role to set up a DNS read-write role.

The information on this page, and the how-tos presented, will provide a blueprint to customize Micetro to your requirements.

Built-in roles

The seven built-in-roles have been designed to cover most use cases for access control in Micetro. The access settings for the built-in roles can't be modified.

Tip: Built-in roles are all *General roles* and applied to all objects in Micetro, existing or future.

Example: adding a user or group to the *Administrators (built-in)* role, the user (or group members) automatically gain administrative access to all objects in Micetro.

User defined roles

As all DDI environments are different, Micetro allows creating flexible user-defined roles.

Tip: Creating new roles requires the *Administer users/groups* permission.

There are two ways of creating new roles in Micetro:

1. (Preferred) Duplicate an existing role and edit the permissions. See *Duplicating a role*.
2. Create a completely new role. See *Adding a new role*.

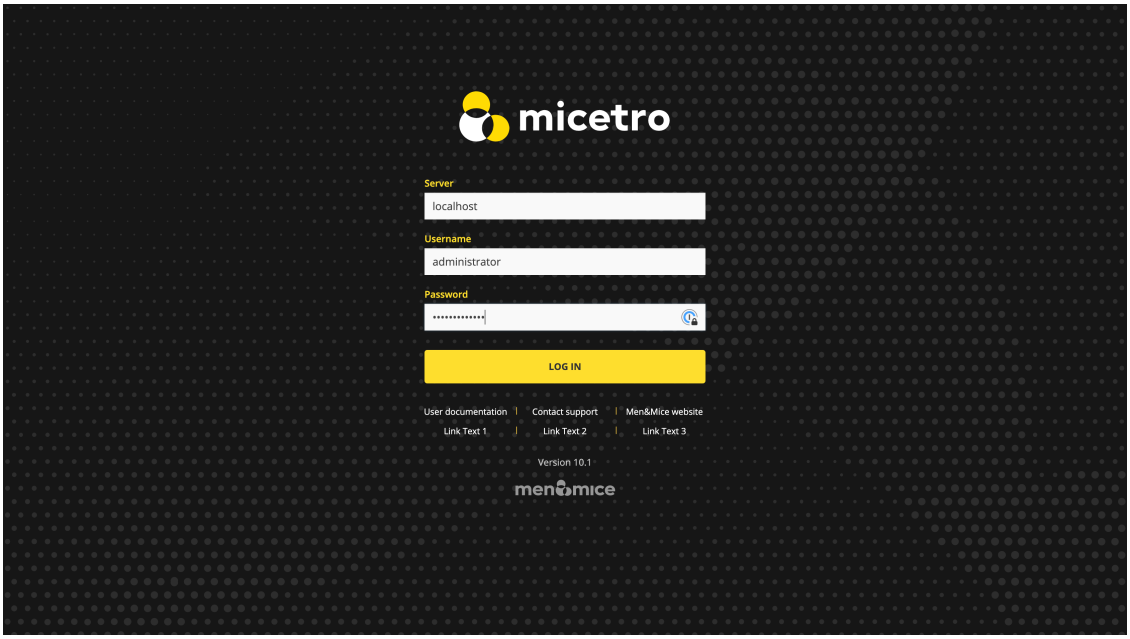
Tip: Men&Mice recommends using the built-in roles as templates and modifying the permission set for the duplicate roles.

Example role configuration: DNS zone read-write

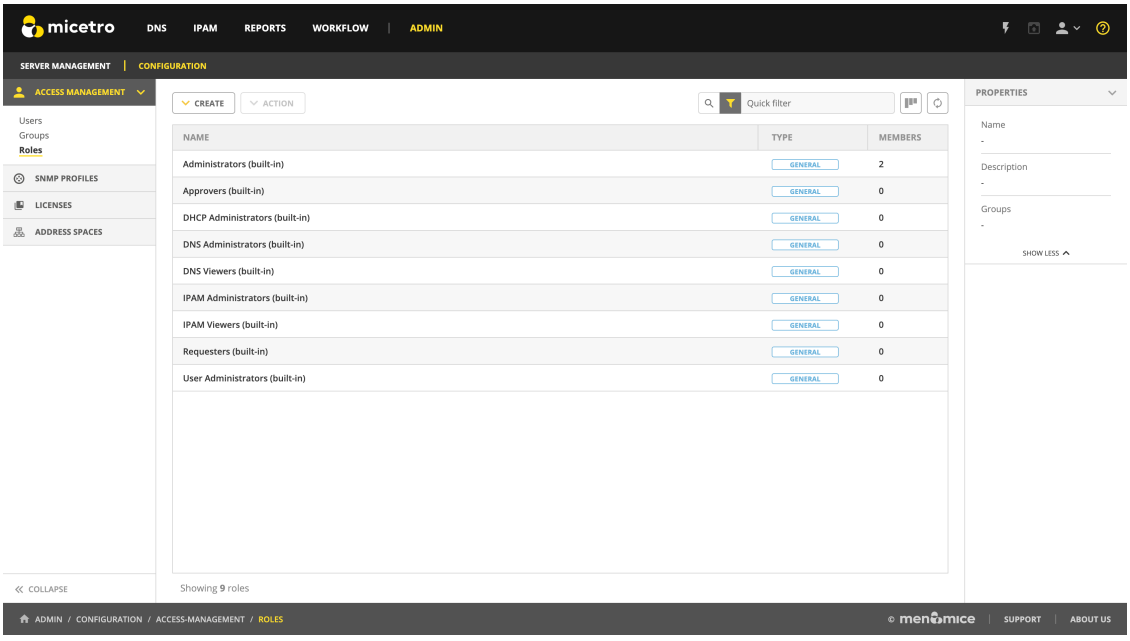
The following steps illustrate how to create a read-write role in Micetro for DNS zones, using a built-in role as a template.

Tip: Using existing roles as templates makes refining access controls easier, as you can both copy over permissions and users / groups.

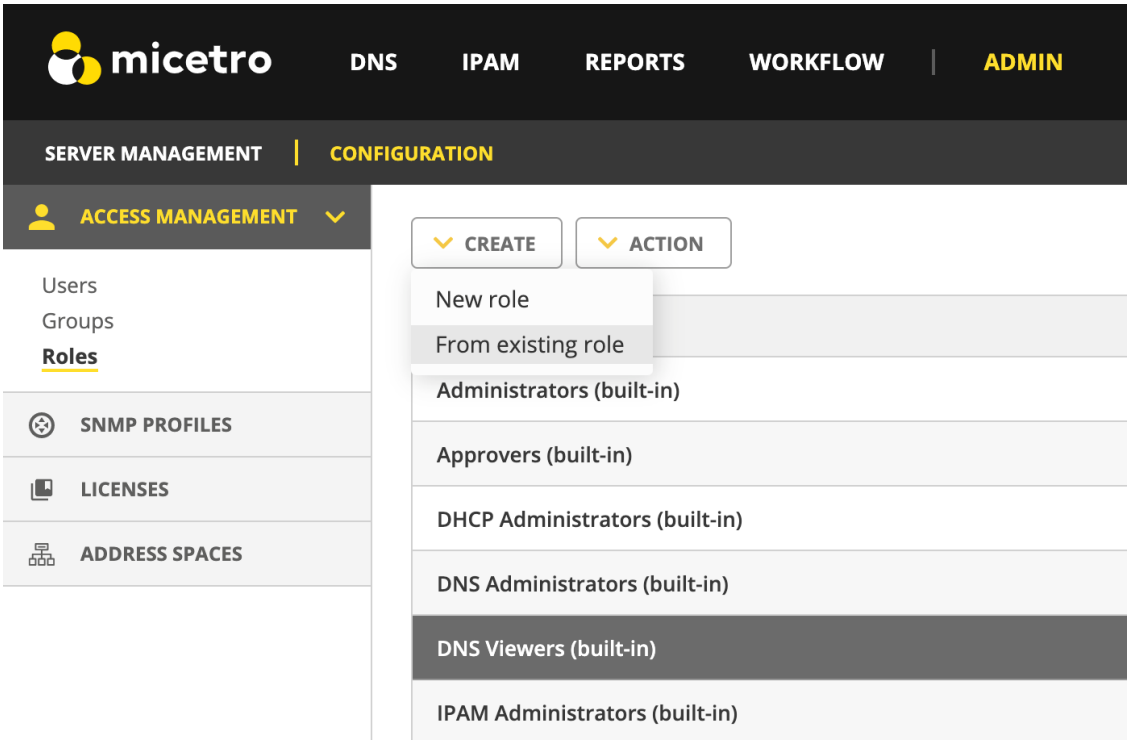
1. Log in to the Web Application.



2. Navigate to *Admin* → *Configuration* → *Access Management* and select *Roles*.

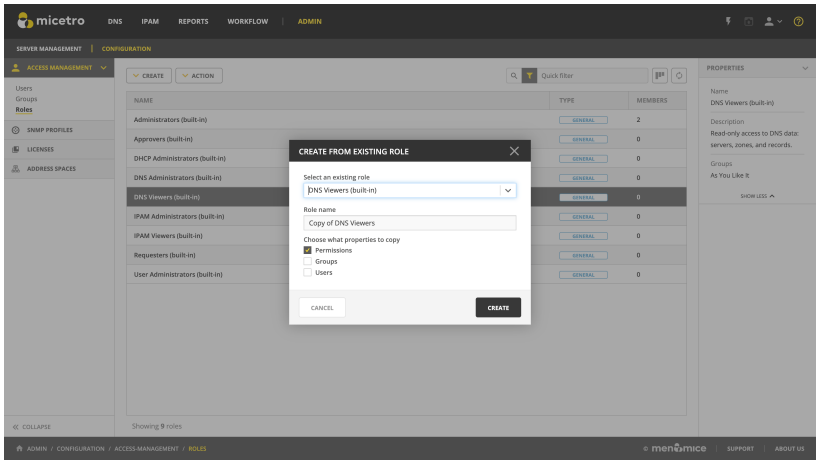


3. Press the *Create* button and select *From existing role*.

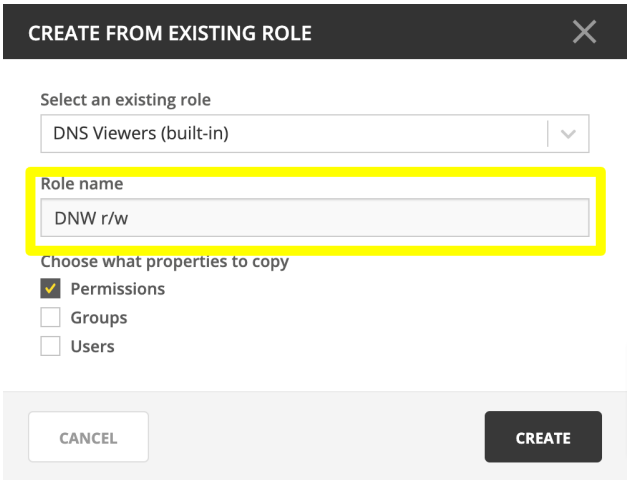


4. From the dropdown **Select an existing role**, click on `DNS Viewers (built-in)`.

Tip: If you have the role selected in the grid, *From existing role* will automatically fill in the value for convenience.

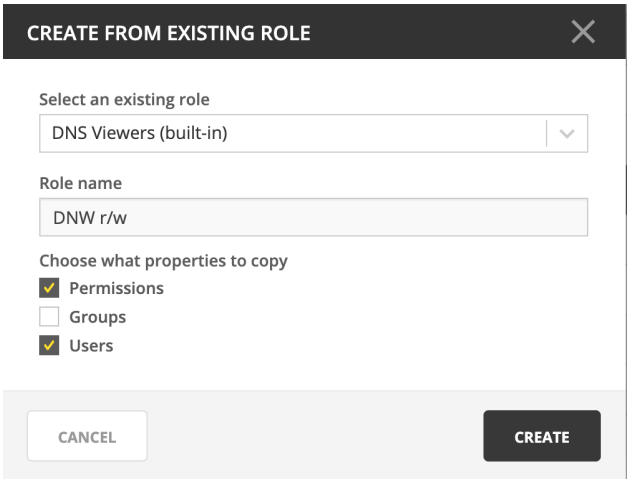


5. Edit the **Role name**.



Note: When duplicating a role, editing the **Description** is not available until the new role is created.

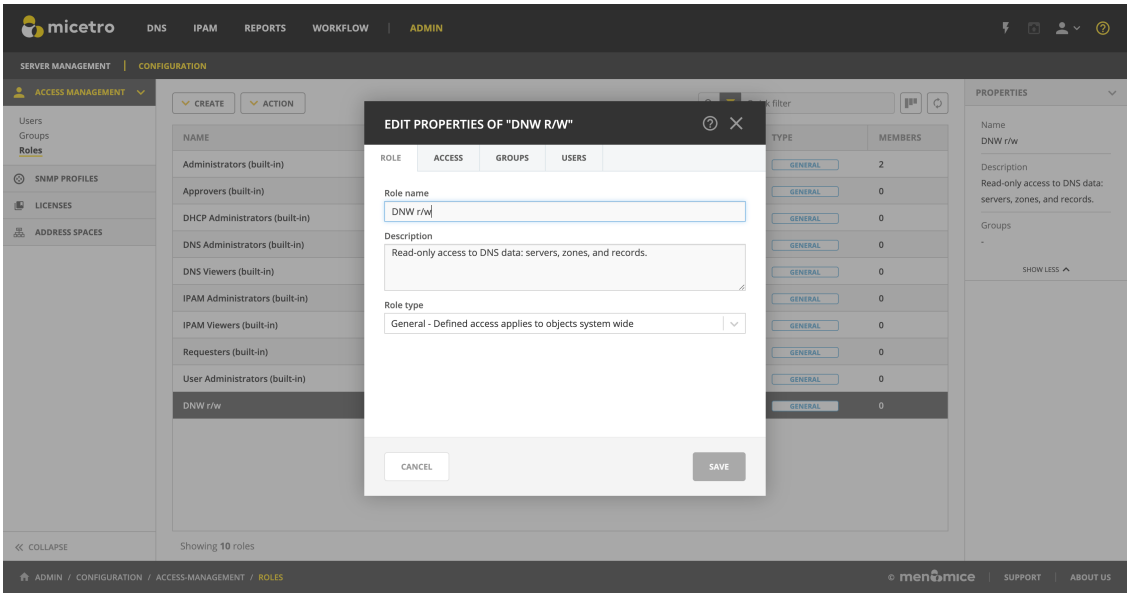
6. Select what to copy from the existing role: **Permissions** (default), *Groups*, and/or *Users*.



Note: Duplicating roles will automatically set the role type to *General*.

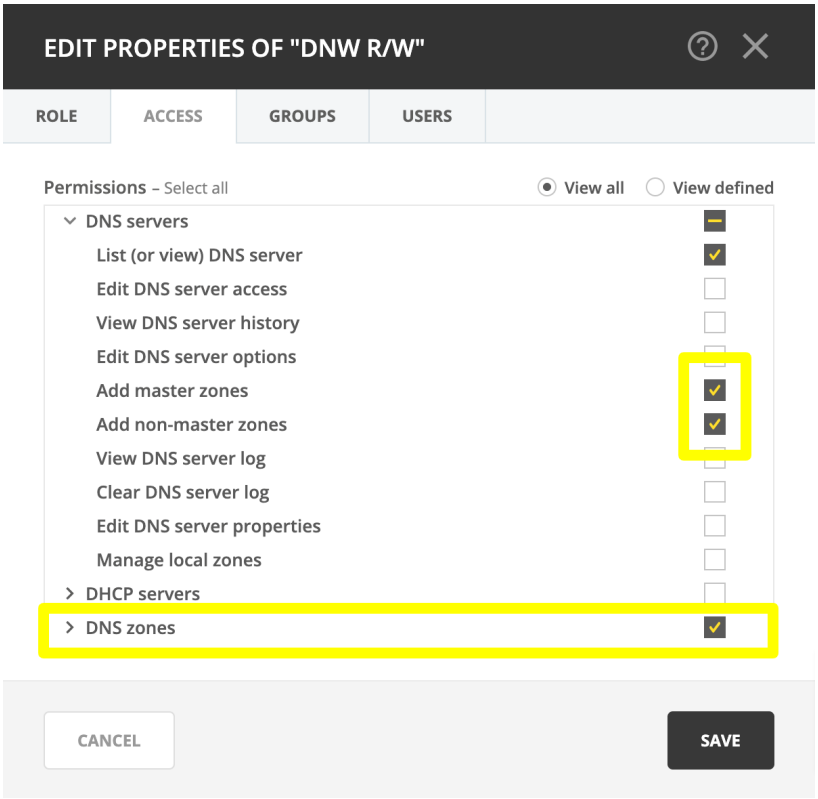
7. Click *Create* to save the new role.

After saving the new role, Micetro will automatically display the *Edit role properties* dialog for it.



8. Switch over to the *Access* tab and enable the following permission:

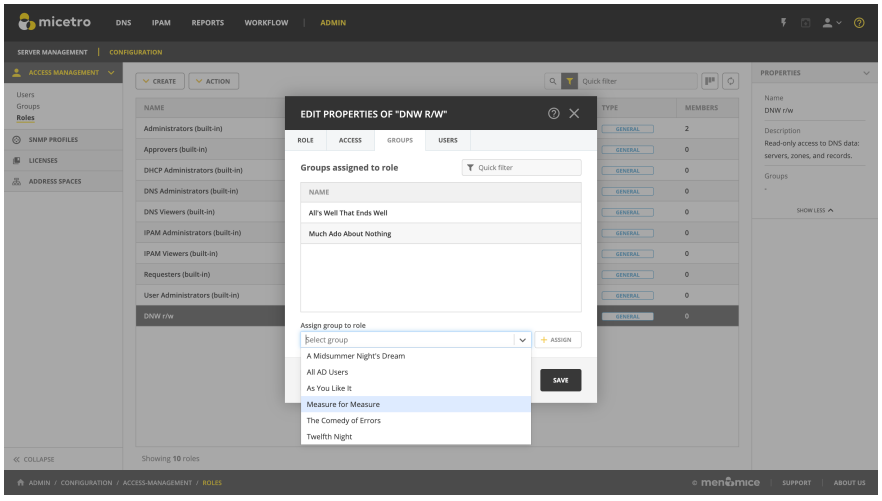
Group	Permission
DNS servers	**Add master zones**
DNS servers	**Add non-master zones**
DNS zones	**Edit zone access**
DNS zones	**List (or view) zone**
DNS zones	**View zone history**
DNS zones	**Enable/disable zone**
DNS zones	**Edit zone options**
DNS zones	**Delete zone**
DNS zones	**Enable/disable apex records**
DNS zones	**Edit apex records**
DNS zones	**Enable/disable wildcard records**
DNS zones	**Edit wildcard records**
DNS zones	**Enable/disable other records**
DNS zones	**Edit other records**
DNS zones	**Edit zone properties**



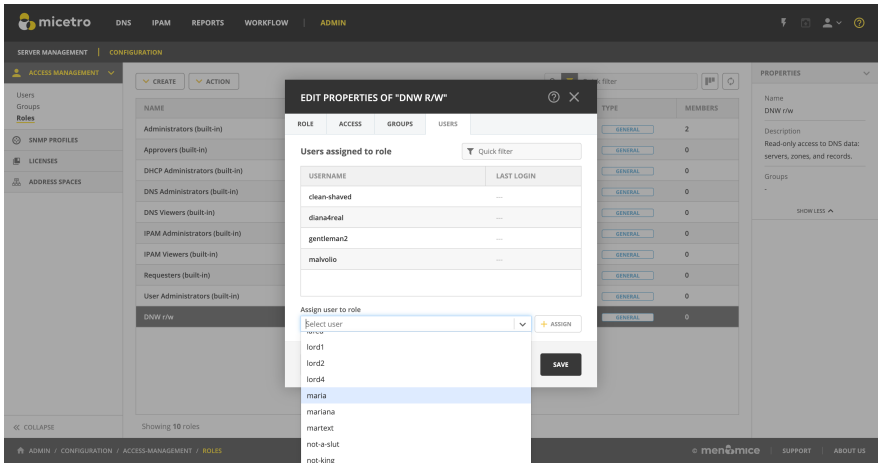
Tip: Clicking the checkbox next to the **DNS zones** group will automatically select all permissions within the group.

Tip: For a handy reference for available permissions, see *Permissions reference*.

9. (Optional) Switch to the *Groups* tab and select the group(s) you'd like to assign to the role.



10. (Optional) Switch to the *Users* tab and select the user(s) you'd like to assign to the role.



Tip: Users and groups can be assigned to and removed from roles at any time.

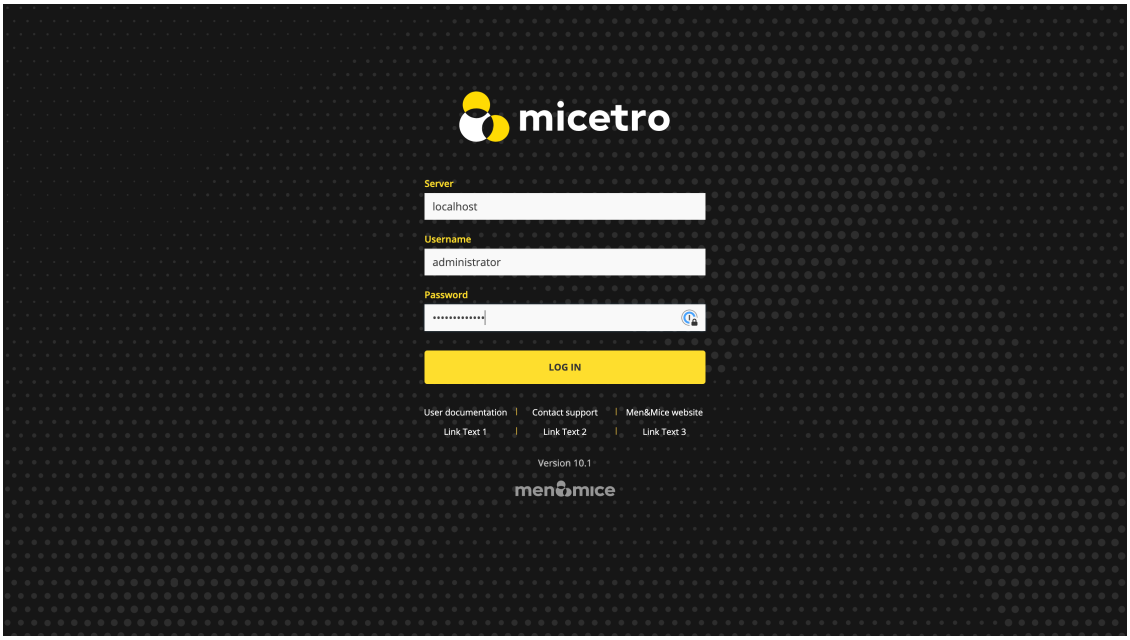
11. Click *Save* to update the role settings.

Example role configuration: DHCP read-only

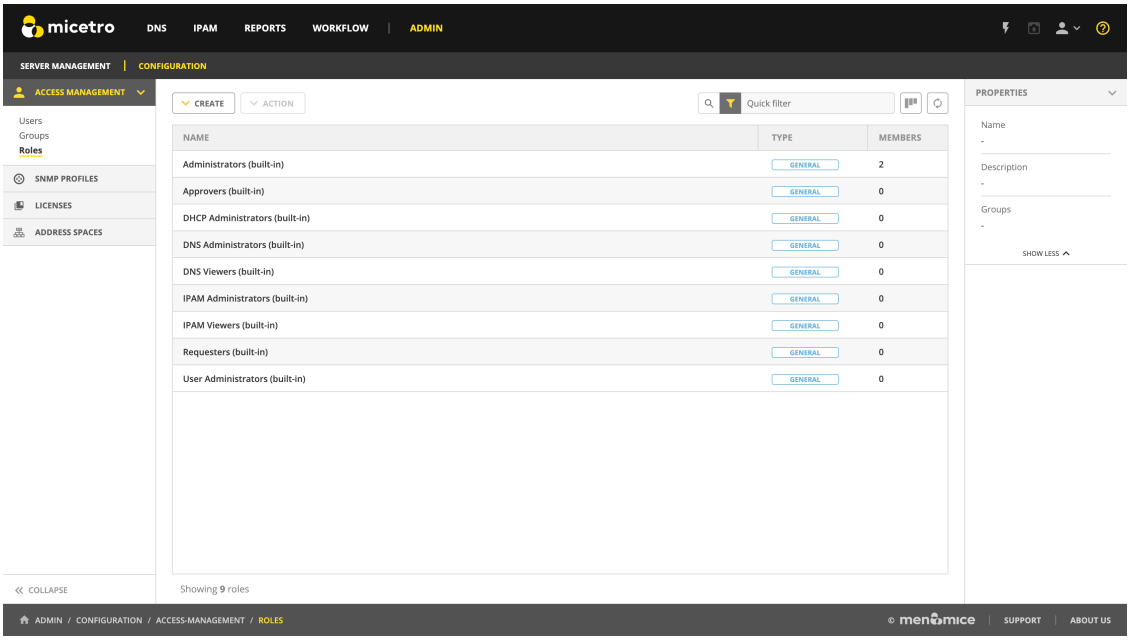
This

The following steps illustrate how to create a new, read-only role in Micetro for DHCP scopes only, without using the built-in role templates.

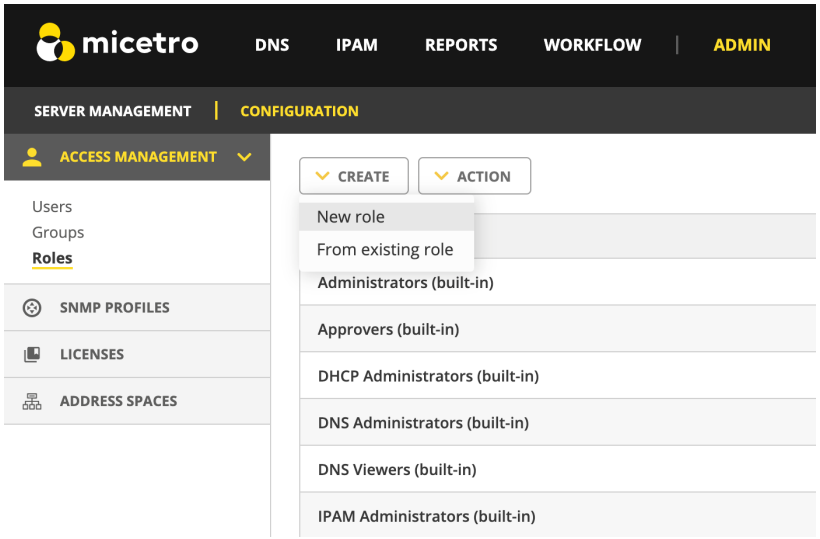
1. Log in to the Web Application.



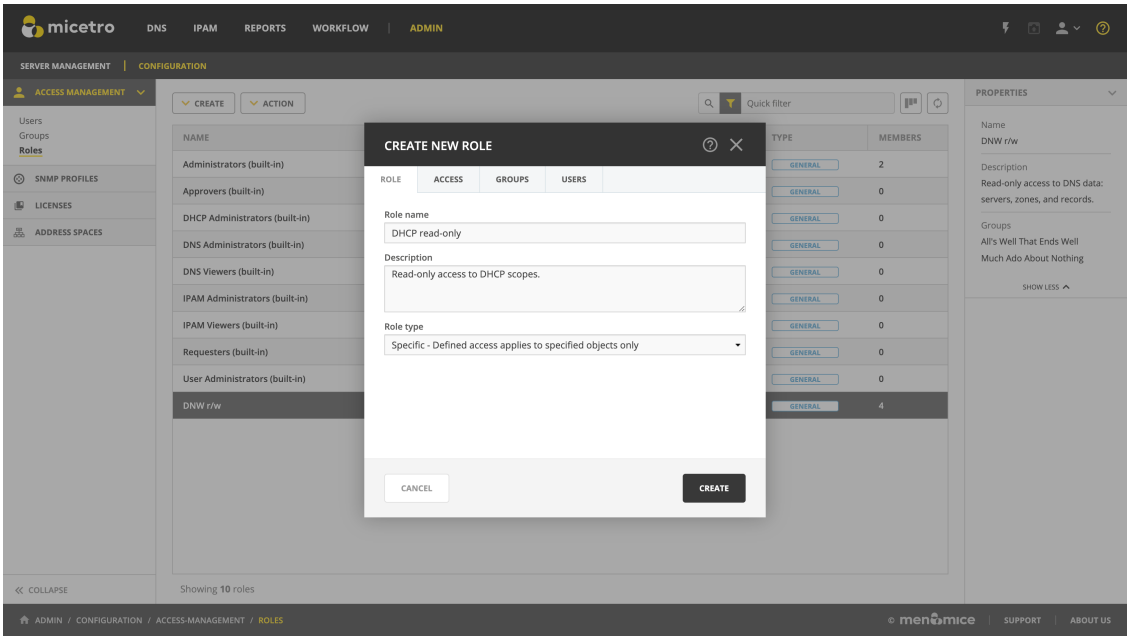
2. Navigate to *Admin* → *Configuration* → *Access Management* and select *Roles*.



3. Press the *Create* button and select *New role*

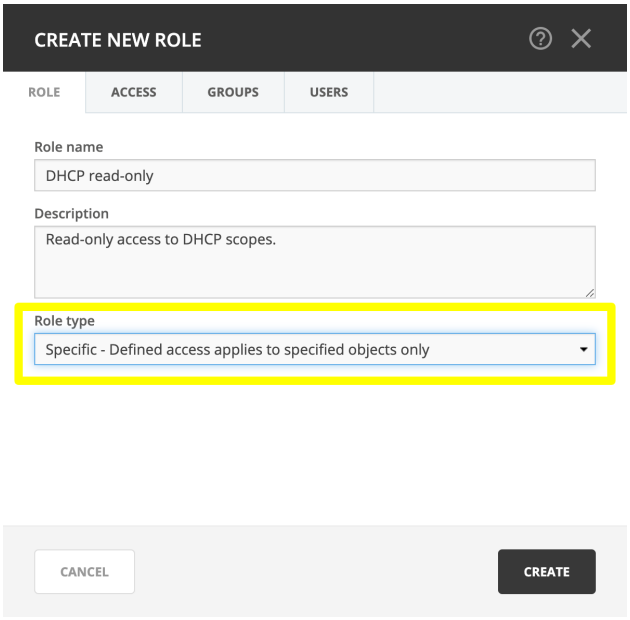


4. Specify the **Role name**, e.g. `DHCP Read-Only` and add a **Description**.



Tip: Using descriptive names and clear text for the description makes access management easier.

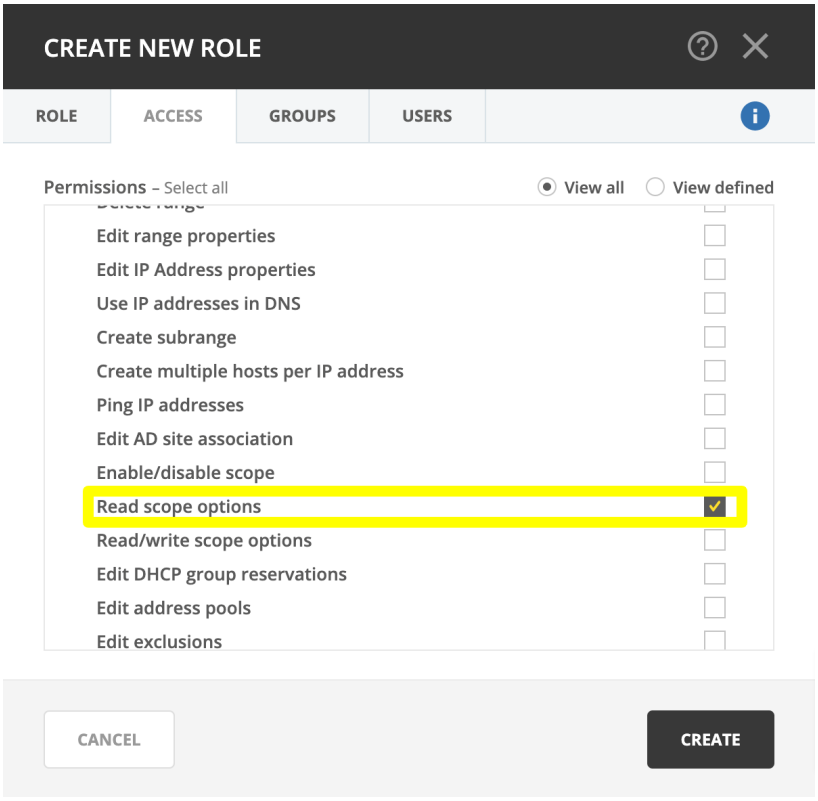
5. Choose between the *General* or *Specific* role types.



Note: The preferred role type in Micetro is the *General roles*. Specific roles exist to preserve backwards compatibility and added flexibility to edge use cases.

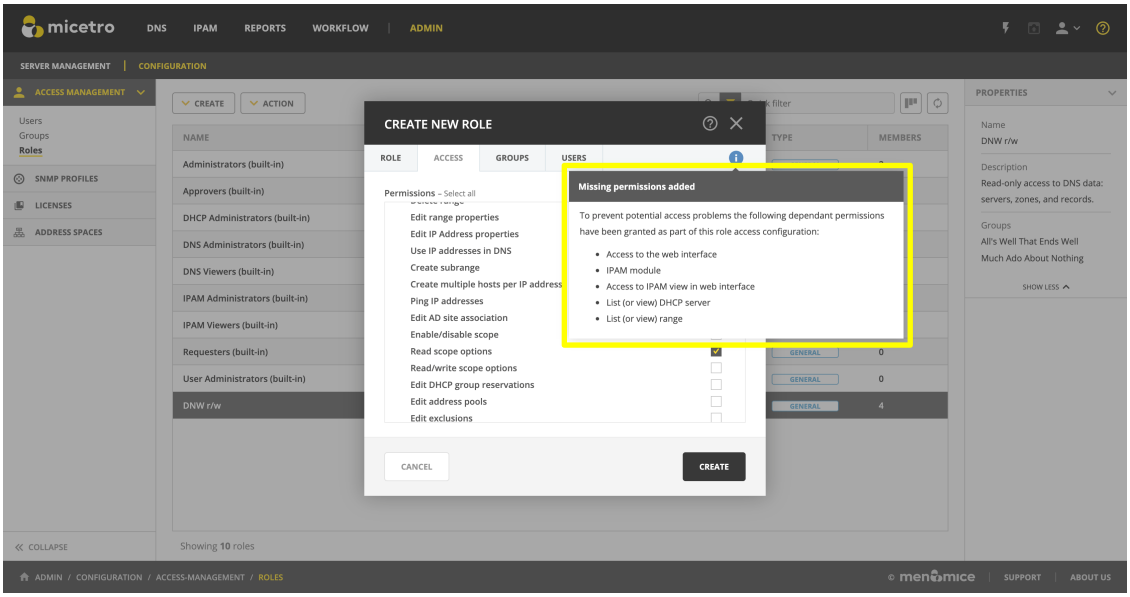
6. Switch over to the *Access* tab and enable the following permission:

Group	Permission
Ranges and DHCP scopes	**Read scope options**



7. Notice that a blue *(i)* indicator appears on the top right. Hovering over will show that in order for the selected permissions to take effect, additional permissions will be set:

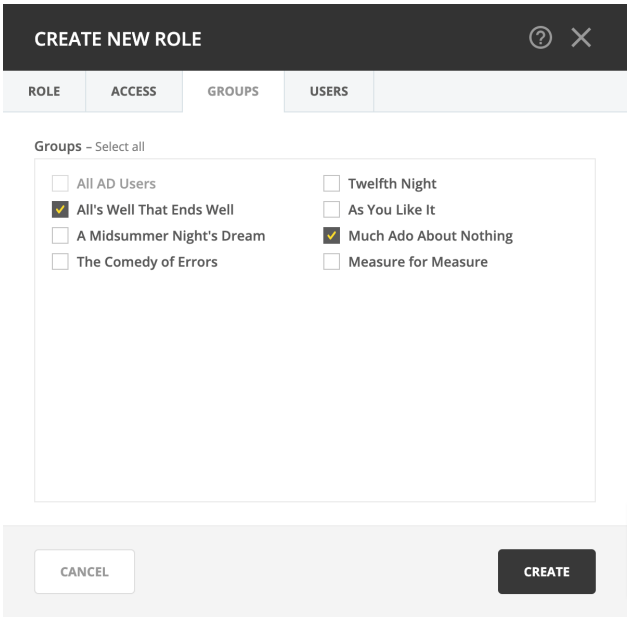
Group	Permission
Micetro	Access to the web interface
Micetro	Access IPAM module
Micetro	Access to IPAM view in web interface
DHCP servers	List (or view) DHCP server
Ranges and DHCP scopes	List (or view) range
Address spaces	List (or view) address space



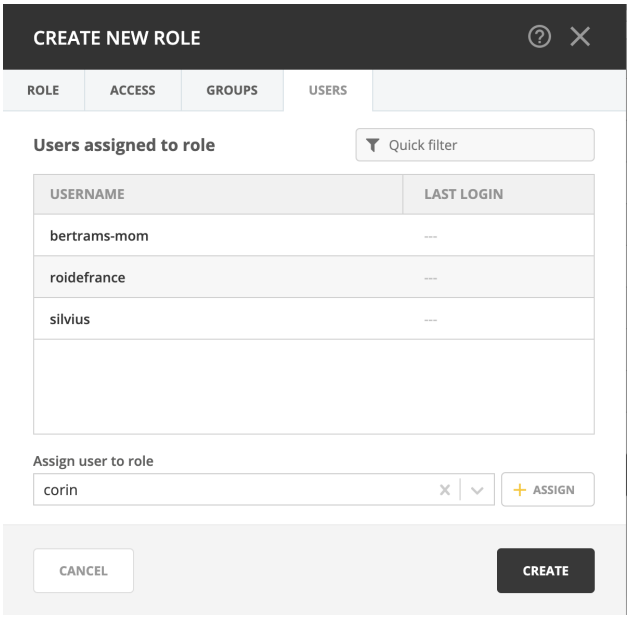
Tip: Micetro will automatically enable these permissions upon saving the new role. You can check the permissions granted to the role by switching to *View defined* using the radio button.

Tip: For a handy reference for available permissions, see *Permissions reference*.

8. (Optional) Switch to the *Groups* tab and select the group(s) you'd like to assign to the role.



9. (Optional) Switch to the *Users* tab and select the user(s) you'd like to assign to the role.



Tip: Users and groups can be assigned to and removed from roles any time.

10. Click *Create* to create the role.

1.20.22 Discontinuation of support for Internet Explorer

As of the 9.3.0 version of Micetro, Internet Explorer will no longer be supported for the Web Application. Customers currently using Internet Explorer to access the Web Application will be redirected to the old Web UI.

Microsoft has discouraged users from using Internet Explorer as their browser. While security and reliability updates are and will be still available for Internet Explorer, in sync with its respective OS version, functionality updates have been discontinued in favor of Edge. Modern web technologies have passed Internet Explorer and are now either unsupported or completely incompatible with it.

Men&Mice has been supporting Internet Explorer to cover environments where legacy systems need to be managed or used. The development to the new Web Application, however, reached a point where Internet Explorer is simply no longer available for reliable use. The Men&Mice Web Application uses web technologies that IE isn't compatible with.

To ensure that your Men&Mice installation can take advantage of all the features Men&Mice offers, please update to Edge or a similar modern browser.

Alternatives

The Men&Mice Web Application supports modern web browsers:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Apple Safari

See system-requirements for a full list of supported systems and applications.

1.20.23 Setting up the PostgreSQL High Availability environment

Important: Configuring high availability for the database is the responsibility of your database team. The following information illustrates a possible setup using `pg_auto_failover` to create a high availability database cluster.

While all possible steps were taken to verify its accuracy, Men&Mice assumes no responsibility for the setup herein.

Install pg_auto-failover

Note: The setup presented here will establish resilience against losing any one of the configured three nodes. Refer to the pg_auto_failover documentation for more details about different configurations.

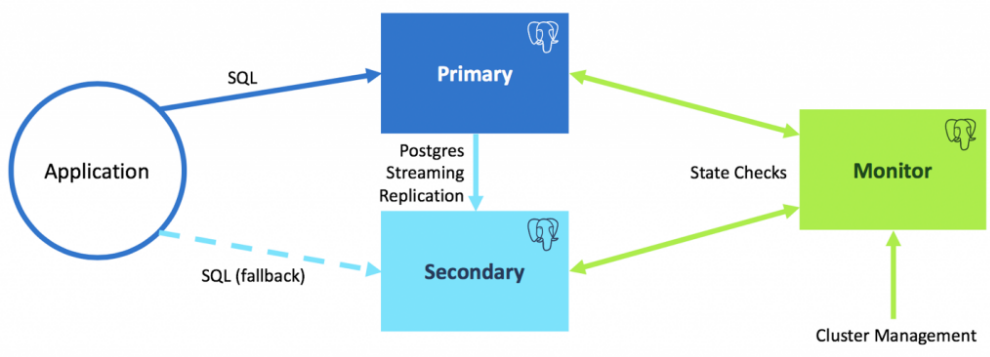


Table 21: Variables

Name	Description	Example value
`[port]`	The port number that will be used for communication between database nodes	5000
`[monitor]`	The monitor node's machine hostname	postgresql-node-0
`[node-1]`	The primary node's machine hostname	postgresql-node-1
`[node-2]`	The secondary node's machine hostname	postgresql-node-2
`[ip-address-monit`	The monitor node's machine IP address	172.17.0.2
`[ip-address-node-`	The machine's IP address of node-1	172.17.0.3
`[ip-address-node-`	The machine's IP address of node-2	172.17.0.4
`[monitor_node_pas`	The monitor node's password to its database. **This password cannot contain the *@* character.**	test123
`[replication-pass`	The password used for replication between nodes	vg8@urenHfhk
`[postgres-passwor`	The password used to access the mmsuite database	postgres
`[ip-address-of-ce`	The IP address of the *primary* machine running Central	172.17.0.5
`[ip-address-of-ce`	The IP address of the machine running the *secondary* Central	172.17.0.6
`[pre-existing-dat`	The port of the pre-existing database (if any)	5432

Make sure that the hostnames are resolvable between all three machines along with the machine running Central (and the second instance if Central is running in HA mode). If that is not possible, using the ip-addresses instead of hostnames is allowed.

Install requirements

Install `sudo` and `which`:

```
yum install sudo
yum install which
```

Enable the package repository that distributes `pg_auto_failover`:

```
curl https://install.citusdata.com/community/rpm.sh | sudo bash
```

Install `pg_auto_failover` for PostgreSQL 12:

```
sudo yum install -y pg-auto-failover10_12
```

If you will be using hostnames, edit `/etc/hosts`:

```
echo "[ip-address-monitor-machine] [monitor]" >> /etc/hosts
echo "[ip-address-node-1] [node-1]" >> /etc/hosts
echo "[ip-address-node-2] [node-2]" >> /etc/hosts
```

Note: You can use the commands `pg_autoctl stop` and `pg_autoctl drop node --destroy` to start with a clean slate and get rid of everything that might have been set up previously.

Machine: monitor

Switch to user *postgres* and export *pgsql path*:

`sudo su - postgres`

`export PATH="$PATH:/usr/pgsql-12/bin"`

Set up a monitor node:

`pg_autoctl create monitor --pgdata ./[monitor] --pgport [port] --nodename [monitor] --auth scram-sha-256`

Next, the `pg_hba.conf` file needs to be edited to allow connection in from the two nodes:

`echo "host pg_auto_failover autoctl_node [ip-address-node-1]/32 scram-sha-256" >> ./[monitor]/pg_hba.conf`

`echo "host pg_auto_failover autoctl_node [ip-address-node-2]/32 scram-sha-256" >> ./[monitor]/pg_hba.conf`

Edit the `postgresql.conf` file to allow *scram-sha-256* authentication:

```
vi ./[monitor]/postgresql.conf
# uncomment the line and set
# password_encryption = 'scram-sha-256'
# uncomment the line and set
# listen_addresses = '*'
# save the file and restart
```

`pg_ctl restart -D ./[monitor]`

Still running as user *postgres*, set the database user password in the monitor database:

```
psql -p [port] -d pg_auto_failover
ALTER USER autoctl_node PASSWORD '[monitor_node_password]';
\q
```

Machine: node-1

Switch to user *postgres* and export *pgsql path*:

`sudo su - postgres`

`export PATH="$PATH:/usr/pgsql-12/bin"`

Set up a primary node:

```
pg_autoctl create postgres --pgdata ./[node-1] --pgport [port] --pgctl `which pg_ctl`
--nodename [node-1] --monitor postgres://autoctl_node:[monitor_node_password]@[monitor]:[port]/
pg_auto_failover --auth scram-sha-256
```

Set up a replication password

`pg_autoctl config set replication.password [replication-password] --pgdata ./[node-1]`

Edit the `postgresql.conf` file to allow *scram-sha-256* authentication:

```
vi ./[node-1]/postgresql.conf
# uncomment the line and set
# password_encryption = 'scram-sha-256'
# uncomment the line and set
# listen_addresses = '*'
# save the file and restart
```

`pg_ctl restart -D ./[node-1]`

Still running as user *postgres*, set the database user password in the database:

```
psql -p [port]
ALTER USER pgautofailover_replicator PASSWORD [replication-password];
ALTER USER postgres PASSWORD [postgres-password];
\q
```

Run the primary node in the background:

`pg_autoctl run --pgdata ./[node-1]/ &`

Machine: node-2

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
pg_autoctl create postgres --pgdata ./[node-2] --pgport [port] --pgctl `which pg_ctl` --
↪nodename [node-2] --monitor postgres://autoctl_node:[monitor_node_
↪password]@[monitor]:[port]/pg_auto_failover --auth scram-sha-256
pg_autoctl config set replication.password [replication-password] --pgdata ./[node-2]
pg_autoctl run --pgdata ./[node-2]/ &
```

Machine: monitor

Show state to verify the setup:

`pg_autoctl show state --pgdata ./[monitor]`

```
Name                        |   Port    | Group |  Node |     Current State |    Assigned␣
↪State
----------------------------+-----------+-------+-------+-------------------+-------------
↪-----
[node-1]                    |   [port] |     0 |     1 |           primary |          ␣
↪primary
[node-2]                    |   [port] |     0 |     1 |         secondary |        ␣
↪secondary
```

Set up the mmsuite database and edit config files

Machine: node-1

Enter the `postgresql` database as user *postgres*:

```
psql -p [port]
> CREATE DATABASE mmsuite ENCODING = 'LATIN1' LC_CTYPE = 'POSIX' LC_COLLATE='POSIX'␣
↪TEMPLATE template0;
> GRANT ALL PRIVILEGES ON DATABASE mmsuite TO postgres;
```

Edit the `pg_hba.conf` to allow access to the database from the outside:

```
echo "host mmsuite postgres [ip-address-of-central-primary]/32 scram-sha-256" >> ./[node-
↪1]/pg_hba.conf
echo "host mmsuite postgres [ip-address-of-central-secondary]/32 scram-sha-256" >> ./
↪[node-1]/pg_hba.conf
psql -p [port] -c 'SELECT pg_reload_conf();'
```

Machine: node-2

Edit the `pg_hba.conf` to allow access to the database from the outside:

```
echo "host mmsuite postgres [ip-address-of-central-primary]/32 scram-sha-256" >> ./[node-
↪2]/pg_hba.conf
echo "host mmsuite postgres [ip-address-of-central-secondary]/32 scram-sha-256" >> ./
↪[node-2]/pg_hba.conf
psql -p [port] -c 'SELECT pg_reload_conf();'
```

Further information

Migrate data from another database

The new PostgreSQL High Availability setup has the database `mmsuite` but with no data. If you have a pre-existing database you need to migrate the data to the new setup.

Create a dump using `pg_dump`:

```
pg_dump -U postgres -p [pre-existing-database-port] -O mmsuite > mmsuite_dump.sql
```

If you've already created the mmsuite database in the HA PostgreSQL server, first drop it and recreate:

```
psql -U postgres -p [port] -c "DROP DATABASE mmsuite;"
psql -U postgres -p [port] -c "CREATE DATABASE mmsuite ENCODING = 'LATIN1' LC_CTYPE =
↪'POSIX' LC_COLLATE='POSIX' TEMPLATE template0;"
```

Finally execute the commands in the dump file to copy the data:

```
psql -U postgres -p [port] -d mmsuite -f mmsuite_dump.sql
```

PostgreSQL HA tweaks

Lower timeout threshold

Machine: monitor

We want to lower the database timeout value, i.e. when the failover should be performed if the primary database is unreachable:

```
psql -p [port] -d pg_auto_failover
# List the health_check variables
SELECT name, setting FROM pg_settings WHERE name ~ 'pgautofailover\.health';
# Check status of database every 5s, setthe timeout to 2s and set the node unhealthy␣
↪timeout to 5s
ALTER SYSTEM SET pgautofailover.health_check_period TO 5000;
ALTER SYSTEM SET pgautofailover.health_check_timeout TO 2000;
ALTER SYSTEM SET pgautofailover.node_considered_unhealthy_timeout TO 5000;
# Reload config:
select pg_reload_conf();
```

(continues on next page)

(continued from previous page)

```
# Verify changes
SELECT name, setting FROM pg_settings WHERE name ~ 'pgautofailover\.health';
SELECT name, setting FROM pg_settings WHERE name ~ 'pgautofailover\.node';
```

Create a startup service

For each machine create a startup service that runs the `pg_autoctl` process:

Machine: monitor

```
pg_autoctl -q show systemd --pgdata /var/lib/pgsql/[monitor]/ | sudo tee /etc/systemd/
↪system/pgautofailover.service
systemctl enable pgautofailover.service
```

Machine: node-1

```
pg_autoctl -q show systemd --pgdata /var/lib/pgsql/[node-1]/ | sudo tee /etc/systemd/
↪system/pgautofailover.service
systemctl enable pgautofailover.service
```

Machine: node-2

```
pg_autoctl -q show systemd --pgdata /var/lib/pgsql/[node-2]/ | sudo tee /etc/systemd/
↪system/pgautofailover.service
systemctl enable pgautofailover.service
```

Configuring PostgreSQL logging

Machine: monitor

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
psql -p [port]
ALTER SYSTEM SET log_truncate_on_rotation = 'on';
ALTER SYSTEM SET log_filename = 'postgresql-%a.log';
ALTER SYSTEM SET log_rotation_age = '1440';
ALTER SYSTEM SET log_line_prefix = '%m - %l - %p - %h - %u@%d - %x';
ALTER SYSTEM SET log_directory = 'pg_log';
ALTER SYSTEM SET log_min_messages = 'WARNING';
ALTER SYSTEM SET log_min_error_statement = 'NOTICE';
ALTER SYSTEM SET log_min_duration_statement = '10s';
ALTER SYSTEM SET log_checkpoints = 'on';
ALTER SYSTEM SET log_lock_waits = 'on';
```

(continues on next page)

(continued from previous page)

```
ALTER SYSTEM SET log_temp_files = '0';
ALTER SYSTEM SET log_connections=on;
ALTER SYSTEM SET log_disconnections=on;
ALTER SYSTEM SET log_duration=on;
SELECT pg_reload_conf();
```

Machine: node-1

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
psql -p [port]
ALTER SYSTEM SET log_truncate_on_rotation = 'on';
ALTER SYSTEM SET log_filename = 'postgresql-%a.log';
ALTER SYSTEM SET log_rotation_age = '1440';
ALTER SYSTEM SET log_line_prefix = '%m - %l - %p - %h - %u@%d - %x';
ALTER SYSTEM SET log_directory = 'pg_log';
ALTER SYSTEM SET log_min_messages = 'WARNING';
ALTER SYSTEM SET log_min_error_statement = 'NOTICE';
ALTER SYSTEM SET log_min_duration_statement = '10s';
ALTER SYSTEM SET log_checkpoints = 'on';
ALTER SYSTEM SET log_lock_waits = 'on';
ALTER SYSTEM SET log_temp_files = '0';
ALTER SYSTEM SET log_connections=on;
ALTER SYSTEM SET log_disconnections=on;
ALTER SYSTEM SET log_duration=on;
SELECT pg_reload_conf();
```

Machine: node-2

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
psql -p [port]
ALTER SYSTEM SET log_truncate_on_rotation = 'on';
ALTER SYSTEM SET log_filename = 'postgresql-%a.log';
ALTER SYSTEM SET log_rotation_age = '1440';
ALTER SYSTEM SET log_line_prefix = '%m - %l - %p - %h - %u@%d - %x';
ALTER SYSTEM SET log_directory = 'pg_log';
ALTER SYSTEM SET log_min_messages = 'WARNING';
ALTER SYSTEM SET log_min_error_statement = 'NOTICE';
ALTER SYSTEM SET log_min_duration_statement = '10s';
ALTER SYSTEM SET log_checkpoints = 'on';
ALTER SYSTEM SET log_lock_waits = 'on';
ALTER SYSTEM SET log_temp_files = '0';
ALTER SYSTEM SET log_connections=on;
ALTER SYSTEM SET log_disconnections=on;
ALTER SYSTEM SET log_duration=on;
SELECT pg_reload_conf();
```

PostgreSQL HA operations

Triggering a failover

To call the function successfully, you need to figure out the formation and group of the group where the failover happens. The following commands when run on a `pg_auto_failover` keeper node provide for the necessary information:

Machine: node-1

Get the variables [formation] and [group] from these commands:

```
su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
# [formation] -> the default value is 'default'
pg_autoctl config get pg_autoctl.formation --pgdata ./[node-1]
# [group] -> the default value is '0'
pg_autoctl config get pg_autoctl.group --pgdata ./[node-1]
```

Machine: monitor

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
psql -p [port] -d pg_auto_failover
> select pgautofailover.perform_failover(formation_id => '[formation]', group_id =>␣
↪[group]);
```

Implementing a controlled switchover

It is generally useful to distinguish a controlled switchover from a failover. In a controlled switchover situation it is possible to organize the sequence of events in a way to avoid data loss and lower downtime to a minimum. In the case of `pg_auto_failover`, because we use synchronous replication, we don't face data loss risks when triggering a manual failover. Moreover, our monitor knows the current primary health at the time when the failover is triggered and drives the failover accordingly. So to trigger a controlled switchover with `pg_auto_failover` you can use the same API as for a manual failover above.

Maintenance of a secondary node

It is possible to put a secondary node in any group in a MAINTENANCE state so that the Postgres server is not doing synchronous replication anymore and can be taken down for maintenance purposes, such as security kernel upgrades or the like.

Machine: node-1 | node-2

To enable maintenance we use:

```
pg_autoctl enable maintenance --pgdata ./[node-1 | node-2]
```

When a standby node is in maintenance, the monitor sets the primary node replication to WAIT_PRIMARY: in this role, the PostgreSQL streaming replication is now asynchronous and the standby PostgreSQL server may be stopped, rebooted, etc.

Note: `pg_auto_failover` does not provide support for primary server maintenance.

To disable maintenance we use

```
pg_autoctl disable maintenance --pgdata ./[node-1 | node-2]
```

Show current state and events

```
$ pg_autoctl show state --pgdata [monitor | node-1 | node-2]
$ pg_autoctl show events --pgdata [monitor | node-1 | node-2]
```

Monitoring `pg_auto_failover` in production

The monitor reports every state change decision to a LISTEN/NOTIFY channel named state. PostgreSQL logs on the monitor are also stored in a table, `pgautofailover.event`, and broadcast by NOTIFY in the channel log.

Machine: monitor

```
sudo su - postgres
tail -f ./[monitor]/pg_log/postgresql-[WeekDay].log
```

Possible disaster scenarios

Failure of:	Machine affected	HA system response
PSQL database service	Primary	Failover, automatic service reboot. Replication stops in the meantime.
	Secondary	Automatic service reboot. Replication stops in the meantime.
	Monitor	Automatic service reboot. Replication continues but no failover possible in the meantime.
Server shutdown	Primary	Failover. Replication stops, waits for a signal from secondary.
	Secondary	Replication on primary stops. Waits for a signal from secondary.
	Monitor	The primary database is still usable. Primary and secondary nodes wait for a connection to monitor. Replication continues.
	All	Database unavailable, no replication, no failover possible.
Server reboot	Primary	Failover, automatic service reboot on startup.
	Secondary	Automatic service reboot. Replication stops in the meantime.
	Monitor	Automatic service reboot. Replication continues but no failover possible in the meantime.
	All	Database unavailable, no replication, no failover possible.
`pg_autoctl` corrupted and/or deleted	All	Database unavailable, no replication, no failover possible.

Controlled switchover

Note: In a controlled switchover situation it is possible to organize the sequence of events in a way to avoid data loss and lower downtime to a minimum. Because the HA cluster described here uses synchronous replication, triggering a manual failover doesn't risk data loss risks. The monitor server keeps the current primary health at the time when the failover is triggered, and drives the failover accordingly.

Triggering a controlled switchover is the same as a manual failover described above.

Recovery

Database service failure

If the PostgreSQL database fails on one of the machines, the system will automatically reboot the affected service, but the replication process is unavailable for the duration.

Server shutdown

If either of the component machines is shut down, a manual restart is required. The failover processes will automatically start with the machine, and reinitialize the connections. If only the monitor server is affected, replication continues and failover is still possible.

Server reboot

The failover system is configured to automatically restart with the server, and no manual intervention is required. If only the monitor server is affected, replication continues but no failover can be triggered until it's available.

`pg_autoctl` setup failure

On the current primary database machine:

```
/usr/pgsql-12/bin/postgres -D /var/lib/pgsql/[node-?] -p [port]
```

Edit the `preferences.cfg file` for Central, and change the following line, using the connection string:

```
postgres://[node-?]:[port]/mmsuite?target_session_attrs=read-write
```

Restart Central:

```
systemctl restart mmcentral
```

Complete shutdown

If the startup scripts are correct in all of the machines a manual boot of the machines in the correct order (1. monitor; 2. primary; 3. secondary) will be enough to reinitialize the cluster. On each machine, use the `ps -ef | grep monitor` (or `primary/secondary`) command after boot to verify the `pg_autoctl` process is running.

If something's not working, or you'd like to manually restart the services to recover, follow these steps.

Note: You can create bash scripts of each step to execute instead of manually running through them.

Start the monitor machine:

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
pg_autoctl run --pgdata ./[monitor]/
```

Start the primary machine:

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
pg_autoctl run --pgdata ./[node-1]/
```

If an error message states an instance is already running, remove the referenced file:

```
rm /tmp/pg_autoctl/var/lib/pgsql/[node-1]/pg_autoctl.pid
```

And re-run the application:

```
pg_autoctl run --pgdata ./[node-1]/
```

Start the secondary machine(s):

```
sudo su - postgres
export PATH="$PATH:/usr/pgsql-12/bin"
pg_autoctl run --pgdata ./[node-2]/
```

If an error message states an instance is already running, remove the referenced file:

```
rm /tmp/pg_autoctl/var/lib/pgsql/[node-2]/pg_autoctl.pid
```

And re-run the application:

```
pg_autoctl run --pgdata ./[node-2]/
```

1.20.24 Always On Availability Groups

Important: Configuring high availability for the database is the responsibility of your database team.

While all possible steps were taken to verify accuracy, Men&Mice assumes no responsibility for the information herein.

Note: Please note that Always On Availability Groups are only supported for Men&Mice Central running on Linux.

Men&Mice Central supports the use of Always On Availability Groups (v9.3.0 and above), In case of a failover the Men&Mice Central will refresh its database connections to the new primary replica.

To use Always On Availability Groups, change the DatabaseServer value in the preferences.cfg to the virtual IP address or the FQDN of the availability group listener:

```
<DatabaseServer value="virtual ip/fqdn of availability group listener><,port>\<Instance␣
↪name>@<Database name>" />
```

1.20.25 Free Trial Best Practices

Configure and size your free trial servers

Note: If you're installing Micetro in a test environment, you're server sizes may be much smaller than what's required from Micetro in a production environment. The following sizes assume you'll keep this version of Micetro in production after testing the free trial.

Micetro may be installed on a Windows or Linux virtual machine on-premises or in the cloud.

CPU Count: 4 Cores

Memory Capacity: 8GB

Disk Space: 50GB

Additional Services Required: Web Services (IIS for Windows Server or Apache 2 Web for Linux Server installation)

Optional Windows Management Console

Starting with version 10.1 of Micetro, the Windows Management Console was replaced with the Web UI. The Web UI is capable of most functionality and therefore the original Management Console is likely not necessary for your Micetro free trial. It is an optional download with features such as a built-in health dashboard. The Free Trial documentation will not address the management console, but you may check the rest of the documentation for more information on how to configure and use.

Active Directory Integration

Active Directory (AD) integration is not required if you're running Linux along with other non-Windows based DNS and DHCP services. However, if you would like to see how AD integration works with Micetro, Micetro Central must be installed on a Windows Server in your AD domain or forest.

Note: You will need an Active Directory (AD) service account with DNS/DHCP administrative privileges (or read-only if preferable) to setup Micetro DNS/DHCP agents. Micetro works by connecting to your current DNS and DHCP services and pulling that information into a centralized UI where you gain visibility and control.

Micetro supports SSO and MFA with Active Diretory, Azure AD and Okta.

For more information on setting up accounts please see the documentation here.

1.20.26 Free Trial Best Checklist

Copy this or print it out to make sure you're getting the most out of your Micetro Free Trial.

[ ] Enter IPAM data either via import, discovery, or through manual entry. For help see video here: https://www.youtube.com/watch?v=RVRDdaOfq5U&t=77s

[ ] Connect to any DNS and/or DHCP services required for testing and/or production. See videos here: https://www.youtube.com/playlist?list=PLg9woNoZKJM1wN3fVjUxLndMwtiIT3FkU

[ ] Add AD Sites (optional). See documentation here: https://docs.menandmice.com/en/latest/guides/user-manual/ipam.html#active-directory

[ ] Integrate with AWS Route 53 and/or Azure DNS (if you are using either in your environment). AWS: https://www.youtube.com/watch?v=ANScAI0ltZA&list=PLg9woNoZKJM1wN3fVjUxLndMwtiIT3FkU&index=10 Azure DNS: https://www.youtube.com/watch?v=DFfp9odIiqE&list=PLg9woNoZKJM1wN3fVjUxLndMwtiIT3FkU&index=13

[ ] Check data quality and explore ways to reclaim IP space utilization. Please see this article for ideas on how to get started: https://docs.menandmice.com/en/latest/guides/reference/ip_count.html

[ ] Setup SNMP profiles for network discovery. See video here: https://www.youtube.com/watch?v=QAXmYRQluz8&t=1s

[ ] Setup discovery schedules. See video here: https://www.menandmice.com/ddi-talks/nU1kcoXnq9w

[ ] Create Micetro accounts and define access permissions. See video here: https://www.youtube.com/watch?v=aMEBxkg3bTQ&list=PLg9woNoZKJM1wN3fVjUxLndMwtiIT3FkU&index=13

[ ] Define and create custom properties for asset management. See webinar here: https://www.youtube.com/watch?v=eHjGYbYqugQ&t=12s

[ ] Familiarize yourself with the APIs (optional). For help see playlist here: https://www.youtube.com/playlist?list=PLg9woNoZKJM0Vgugsm0PFkjs5ll_VQx-a

[ ] Start using DNS Workflow to test automated approval workflows built-in to the UI. This video refers to Microsoft enhancement, but works the same with all DNS services. https://www.youtube.com/watch?v=FwxTcAivsGw&list=PLg9woNoZKJM3cndRlKC8ZScc8kTfJP8-E&index=11

[ ] Start using xDNS for multi-service DNS redundancy. For help see video here: https://www.youtube.com/watch?v=0mhRVOdRZfo&t=8s