
Configure MDM Profiles



For supported software information, click [here](#).

You create a mobile device management (MDM) profile to retrieve device information from a graph server. You can use an MDM profile to retrieve device information from a Microsoft Intune server using the device ID and other information, such as user profile using user ID.

You can associate MDM profiles with a Secure Access Portal or a Secure Access Gateway to verify device information during Versa secure access (VSA) client registration (Portal) and after registration (Gateway).

After you link an MDM profile to a graph server, when a user tries to connect to a Versa gateway using a VPN client, a check verifies whether the device is enrolled with the graph server and if the device is compliant with the policies you have configured. If the device is managed and compliant, the VPN session is established, and the user is allowed to access internal resources.

Configure an MDM Profile

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > MDM Profile in the left menu bar. The main pane displays the MDM profiles that are already configured.

The screenshot shows the Versa Networks configuration interface. The top navigation bar includes tabs for Director View, Appliance View (selected), and Template View. The main navigation menu on the left lists various configuration categories: VLAN IDs, Cloud File Export, Persistent Actions, Schedules, Cloud Profiles, Predefined, Custom Objects, SNAT Pool, TCP Profile, and MDM Profile (highlighted with a red box). The main content area displays a table for MDM Profiles with columns: Name, Activation, Auth Profile, Client ID, Directory ID, Graph Profile, and Default Profile. A message "No Record Added" is shown in the table, along with a "+ Add" button. The right sidebar contains buttons for "Commit Template" and "Build".

4. Click + Add. In the Add MDM Profile popup window, enter information for the following fields.

The "Add MDM Profile" popup window contains the following fields and controls:

- Name ***: Text input field.
- Description**: Text input field.
- Directory ID**: Text input field.
- Auth Profile**: Dropdown menu with "---Please Select---" selected.
- Client ID**: Text input field.
- Client Secret**: Text input field.
- Graph Profile**: Dropdown menu with "---Please Select---" selected.
- Activation**: Checkbox.
- Default Profile**: Checkbox.
- Graph Type**: Section header.
- Provider Name**: Dropdown menu with "---Please Select---" selected.
- Resource**: Dropdown menu with "---Please Select---" selected.
- OK**: Blue button.
- Cancel**: Dark blue button.

Field	Description
Name	Enter a name for the MDM profile.
Description	Enter a text description for the MDM profile.
Directory ID	Enter the tenant or directory ID registered on the graph (Intune) server.
Authentication Profile	Select the authentication profile, which is a cloud profile, to use to retrieve access token for secure access. For more information, see Configure a Cloud Profile in the Configure File Filtering article.
Client ID	Enter the client identifier provided by the graph (Intune) server, in string format.
Client Secret	Enter the client secret provided by the graph (Intune) server, in string format.
Graph Profile	Select the graph server profile, which is a cloud profile, to use to retrieve data from the graph server. For more information, see Configure a Cloud Profile in the Configure File Filtering article.
Activation	Click to enable MDM lookup for the profile.
Default Profile	Click to make this the default MDM profile.
Graph Type (Group of Fields)	
◦ Provider Name	Select the graph provider for which to retrieve information, for example, Microsoft.
◦ Resource	Select the resource or device from which to retrieve information, for example, Device ID.

5. Click OK.

Associate an MDM Profile with a Secure Access Portal

1. In Director view:

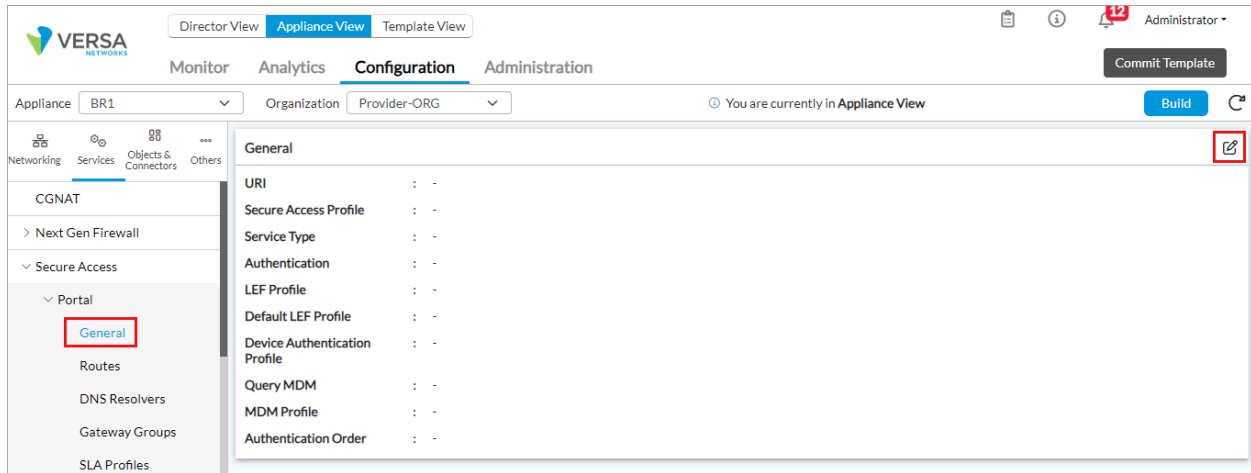
a. Select the Configuration tab in the top menu bar.


https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_MDM...

Updated: Wed, 23 Oct 2024 08:26:38 GMT

Copyright © 2024, Versa Networks, Inc.

- b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > General in the left menu bar. The main pane displays the General settings pane.

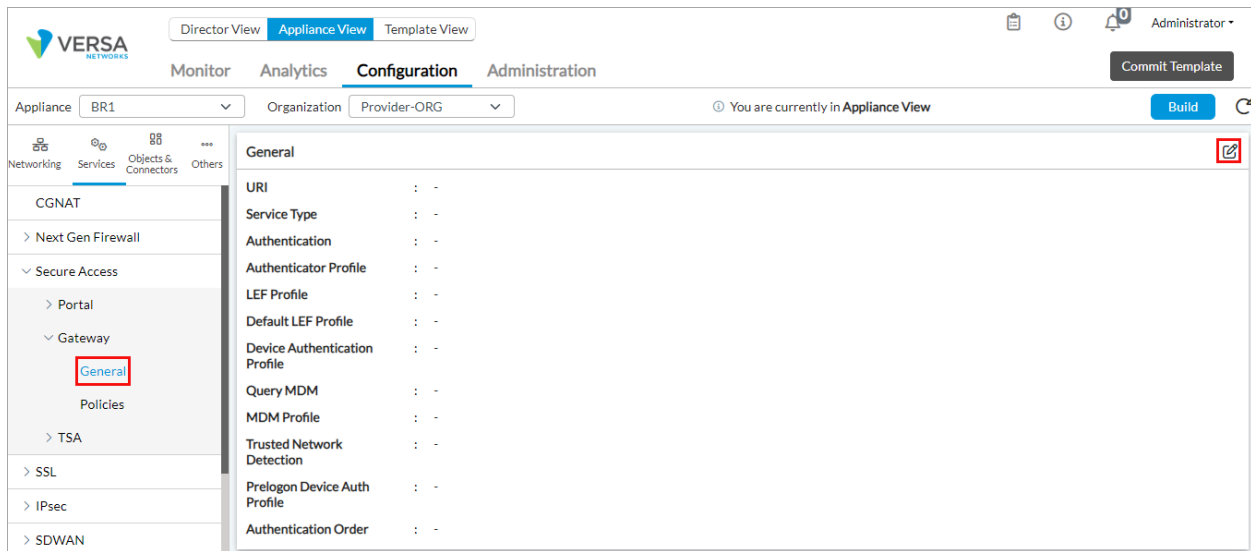



4. In the General pane, click the  Edit icon. The Add Services popup window displays.

5. Click Query MDM to enable MDM checking.
6. Select the MDM profile you configured in [Configure an MDM Profile](#), above.
7. For information about configuring other parameters, see Configure a Secure Access Portal in [Configure Versa Secure Access Gateway](#).
8. Click OK.

Associate an MDM Profile with a Secure Access Gateway

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Gateway > General in the left menu bar.



4. Click the  Edit icon. The Add Services popup window displays.

The screenshot shows the 'Add Services' popup window. It contains the following fields and options:

- URI**: A text field containing 'gateway'.
- Service Type**: A dropdown menu with 'Gateway' selected.
- Authenticator Profile**: A dropdown menu with '---Please Select---'.
- Authentication**: A dropdown menu with '---Please Select---'.
- Device Authentication Profile**: A dropdown menu with '---Please Select---'.
- Prelogon Device Auth Profile**: A dropdown menu with '---Please Select---'.
- Query MDM**: A checkbox that is checked and highlighted with a red box.
- Authentication Order**: A table with a dropdown menu showing '---Please Select---' and a '+' button. Below the table, it says 'No Records to Display'.
- LEF Profile**: A dropdown menu with '---Please Select---' and a checkbox for 'Default LEF Profile'.
- Trusted Network Detection**: A checkbox that is checked.
- MDM Profile**: A dropdown menu with '---Please Select---' highlighted with a red box.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

5. Click Query MDM to enable MDM check.
6. Select the MDM profile you added in [Configure an MDM Profile](#), above.
7. For information about configuring other parameters, see Configure a Secure Access Gateway in [Configure Versa Secure Access Service](#).

8. Click OK.

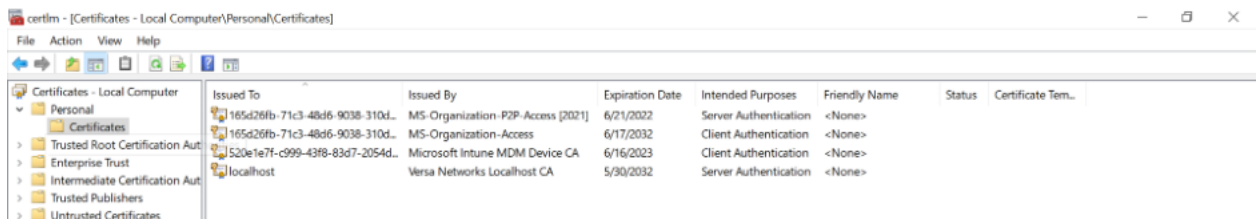
Associate MDM Profiles with Secure Access Portal and Gateway Policies

To ensure that graph server information from devices managed by MDM is in a compliant state, you can create secure access portal and gateway policies to enforce compliance. These policies are checked when a user tries to connect to a Versa gateway using a VPN client. If the managed device is compliant, the VPN session is established, and the user is allowed to access internal resources.

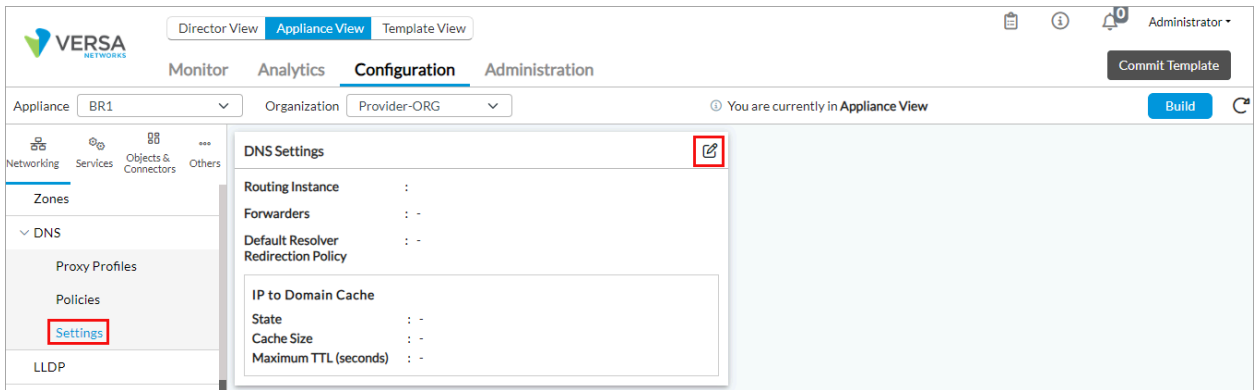
To create the policies, you perform configuration steps both on the VOS device and on Microsoft Intune.


To associate MDM profiles with secure access portal and secure access gateway policies:

1. On Microsoft Intune, check that the device is registered. I
 - a. In the appliance certificate store, go to Certificates - Local Computer > Personal > Certificates.
 - b. Check that the device is registered.



- c. If the device is not registered, an admin user can register the device on Intune by entering the following URL in the browser URI:
ms-device-enrollment:?mode=aadj
2. On the VOS device, add a DNS forwarder so that the cloud profile can connect to Microsoft Graph and the authentication server.
 - a. In Director View, select the Configuration tab in the top menu bar.
 - b. Click Device > Devices in the horizontal menu, select a tenant in the left menu bar, and click a device in the main pane. The view changes to Appliance view.
 - c. Select the Configuration tab in the top menu bar.
 - d. Select Network > DNS > Settings in the left menu bar.



- e. In the DNS Settings pane, click the  Edit icon.
- f. In the Edit DNS Settings popup window, enter information for the following fields.

Edit DNS Settings

Routing Instance

--Select--

Default Resolver Redirection Policy

--Select--

☐ IPv4/IPv6 Address

+

⌵

IPv4/IPv6 Address Not Configured

IP to Domain Cache

☐ Enabled

Cache Size

Maximum TTL (seconds)

OK

Cancel

Field	Description
Routing Instance	Select the routing instance to use to reach the DNS server.
Default Resolver Redirection Policy	Select the default resolver redirection policy to resolve domains
IPv4/IPv6 Address	Click + and enter the IP address of the DNS server.
IP to Domain Cache (Group of Fields)	
◦ Enabled	Click to enable caching of IP address to domain lookup information.
◦ Cache Size	Enter the maximum number for cache entries.
◦ Maximum TTL (Seconds)	Enter the cache TTL upper limit, in seconds.

g. Click OK.

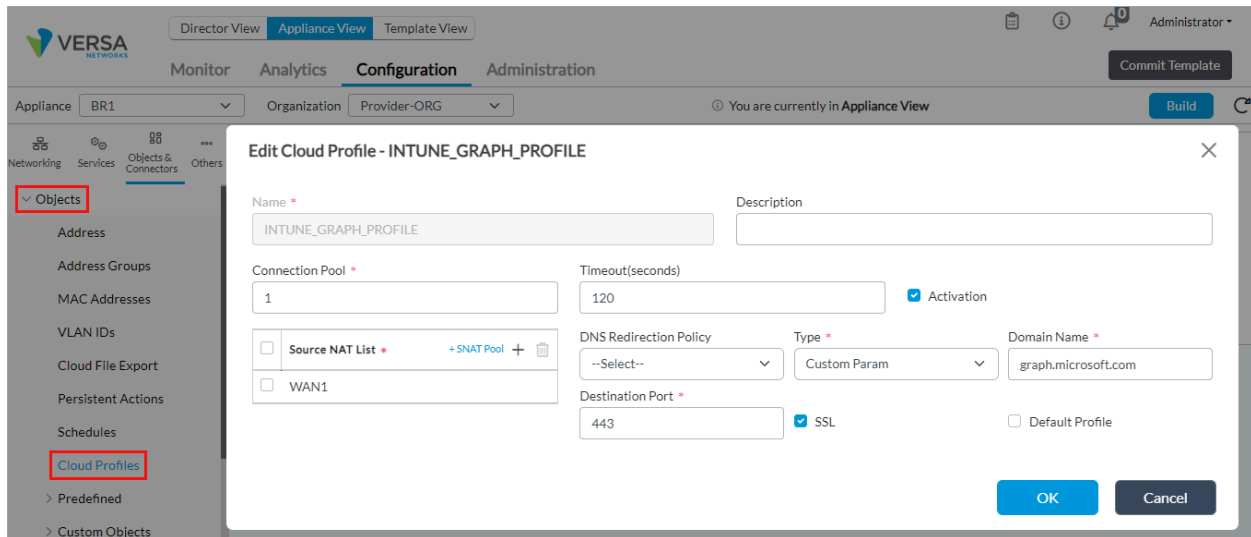
- On the VOS device, create two profiles to use for Intune, an authentication profile and a graph profile. For more information, see [Configure a Cloud Profile](#). The following screenshot shows an example of an authentication profile.

The screenshot displays the Versa Networks configuration interface. On the left, the 'Objects' menu is expanded, and 'Cloud Profiles' is selected. The main window shows the 'Edit Cloud Profile - INTUNE_AUTH_PROFILE' dialog. The dialog contains the following fields and options:

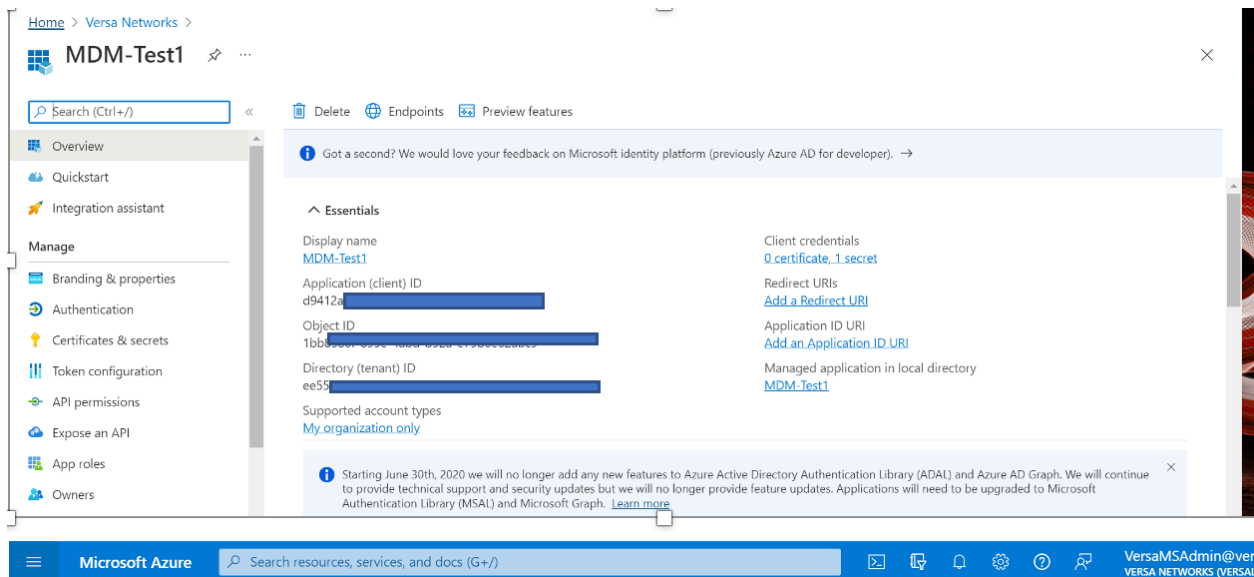
- Name:** INTUNE_AUTH_PROFILE
- Description:** (empty field)
- Connection Pool:** 1
- Timeout(seconds):** 120
- Activation:** ☒
- DNS Redirection Policy:** --Select--
- Type:** Custom Param
- Domain Name:** login.microsoftonline.com
- Destination Port:** 443
- SSL:** ☒
- Default Profile:** ☐

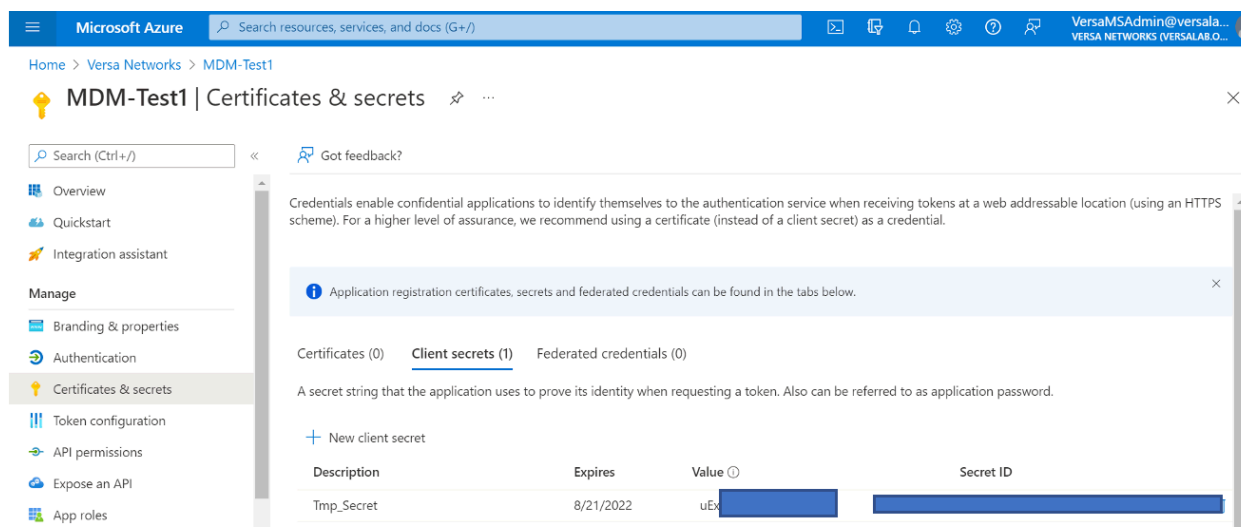
At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

The following screenshot shows an example of a graph profile.

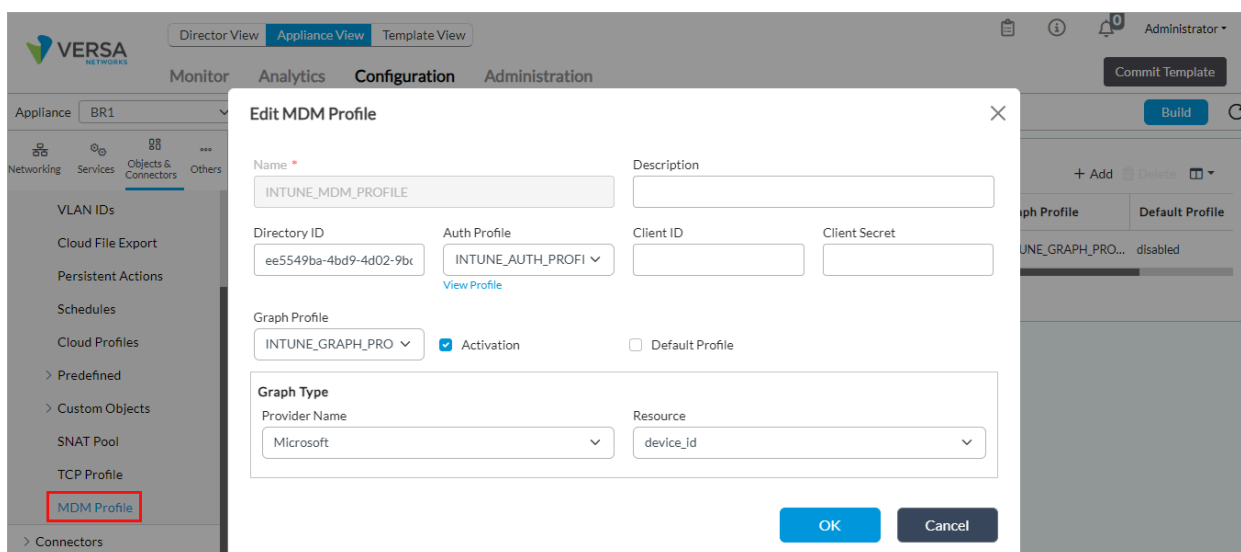


- On Microsoft Intune, create an MDM profile. To fetch the device information from Intune, you create an Intune App for the Azure tenant with permissions that allow Microsoft Graph to provide the data. In the profile, for the Client ID, enter the application ID on the Azure portal. If you need to specify the client secret, use the secret value of the Azure application. Note that this is not a value that you configure. For example:

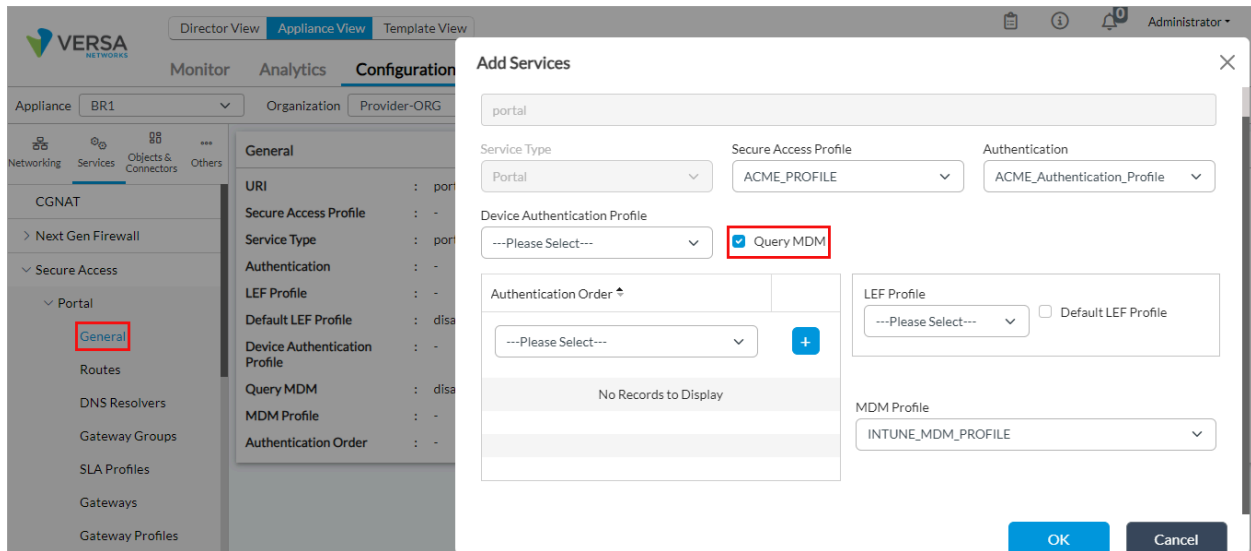




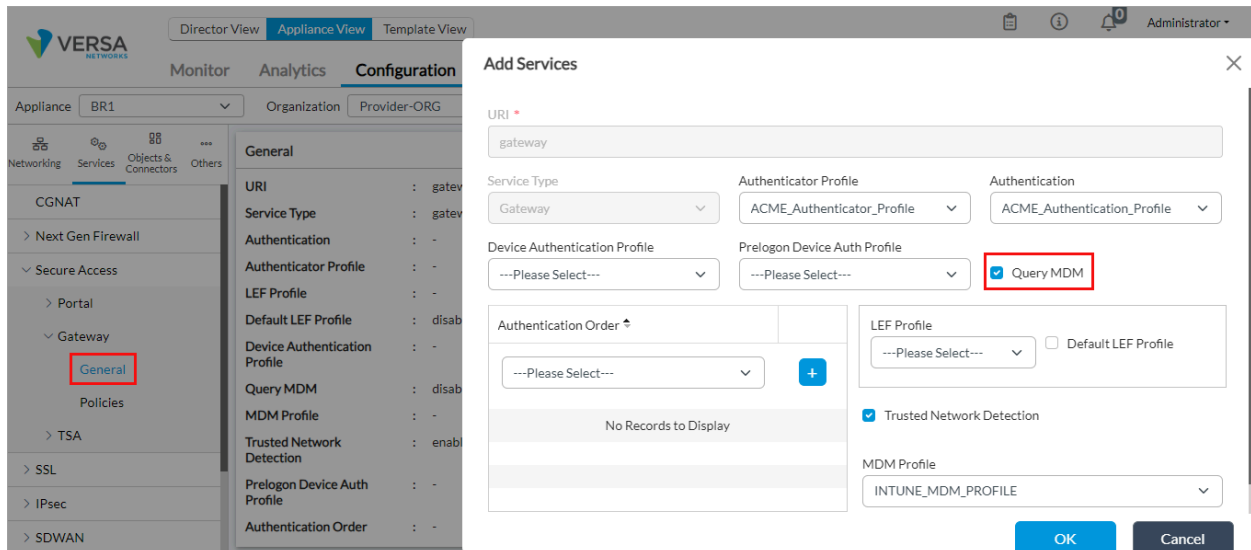
- On the VOS device, configure the MDM profile, as described in [Configure an MDM Profile](#), above. For example:



- On the VOS device, enable a query MDM on the secure access portal and secure access gateway, as described in [Associate an MDM Profile with a Secure Access Portal](#) and [Associate an MDM Profile with a Secure Access Gateway](#), above. The following screenshot shows an example of a query MDM for the secure access portal.



The following screenshot shows an example of a query MDM for the secure access gateway:



7. On the VOS device, create a secure access portal and gateway policy to enforce that graph server information from devices managed by MDM is in a compliant state. For more information, see Add Secure Access Portal Policy in [Configure Versa Secure Access Service](#). In the policy rule, configure the source compliance state and an enforcement message. For example:

Home > Versa Networks > MDM-Test1

MDM-Test1 | API permissions

Refresh
Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

+ Add a permission
Grant admin consent for Versa Networks

API / Permissions name	Type	Description	Admi...	Status	
Intune (1)					...
get_device_compliance	Application	Get device state and compliance information from Microsoft Intu...	Yes	Granted for Versa Netw...	...
Microsoft Graph (22)					...
DeviceManagementConfiguration.Read.All	Application	Read Microsoft Intune Device Configuration and Policies	Yes	Granted for Versa Netw...	...
DeviceManagementManagedDevices.Read.All	Application	Read Microsoft Intune devices	Yes	Granted for Versa Netw...	...
email	Delegated	View users' email address	No		...
openid	Delegated	Sign users in	No		...
profile	Delegated	View users' basic profile	No		...

View MDM Profile Statistics

Note that the MDM statistics display based on the SSL cloud profile settings. For more information, see [Configure a Cloud Profile](#).

To view MDM profile statistics:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select a device in the main pane. The view changes to Appliance view.
- Select the Monitor tab in the top menu bar.
- Select the provider organization in the horizontal menu bar.
- Select the Services tab in the horizontal menu bar.
- Select the Secure Access tab > MDM Profiles tab.

The screenshot shows the Versa Networks Appliance View interface. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. Below this, the 'Monitor' tab is active, with sub-tabs for 'Analytics', 'Configuration', and 'Administration'. The 'Organization' dropdown is set to 'Provider-ORG'. The 'Summary' tab is selected, showing 'Total Appliances: 3' and a filter for 'BR1'. The 'Services' tab is highlighted, showing a list of services including 'Secure Access', 'SD-WAN', 'NGFW', 'CGNAT', 'SD-LAN', 'IPsec', 'Sessions', 'SCI', and 'APM'. The 'MDM Profiles' sub-tab is selected, displaying a table of MDM profile statistics.

Profile Name	Mdm Access Token R...	Mdm Access Token R...	Mdm Access Token R...	Mdm Access Token N...	Mdm Resource Req C...	Mdm Resource Respo...	Mdm Resource Req F...	Mdm Resource Null R...
INTUNE_MDM_PROF...	6	0	0	6	0	0	0	0

The table displays the following information:

Counter Name	Description
MDM Access Token Req Count	Number of times request was sent to fetch an access token.
MDM Access Token Response Count	Number of times an access token response was received successfully.
MDM Access Token Fail Count	Number of times an access token request failed.
MDM Access Token Null Response Count	Number of times an access token request received a null response, which generally occurs because a timeout occurs or a session closes.
MDM Resource Req Count	Number of times an MDM request was sent to fetch a resource (device ID).
MDM Resource Response Count	Number of times an MDM response was received successfully.
MDM Resource Req Fail Count	Number of times an MDM request failed.
MDM Resource Null Response Count	Number of times MDM received a null response, which generally occurs because a timeout occurs or a session closes.

To view MDM profile statistics, using CLI:

```
admin@cli> show orgs org-services tenant-name objects mdm-profile statistics
```

For example:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_MDM...

Updated: Wed, 23 Oct 2024 08:26:38 GMT

Copyright © 2024, Versa Networks, Inc.

```

admin@cli> show orgs org-services AMP objects mdm-profile statistics
objects mdm-profile statistics AMPIntune-ZS
mdm-access-token-req-cnt    430
mdm-access-token-resp-cnt   222
mdm-access-token-req-fail-cnt 0
mdm-access-token-null-resp-cnt 208
mdm-resource-req-cnt        432
mdm-resource-resp-cnt       405
mdm-resource-req-fail-cnt   0
mdm-resource-null-resp-cnt  27

```

The following table explains each counter:

Counter Name	Description
mdm-access-token-req-cnt	Number of times request was sent to fetch an access token.
mdm-access-token-resp-cnt	Number of times an access token response was received successfully.
mdm-access-token-req-fail-cnt	Number of times an access token request failed.
mdm-access-token-null-resp-cnt	Number of times an access token request received a null response, which generally occurs because a timeout occurs or a session closes.
mdm-resource-req-cnt	Number of times an MDM request was sent to fetch a resource (device ID).
mdm-resource-resp-cnt	Number of times an MDM response was received successfully.
mdm-resource-req-fail-cnt	Number of times an MDM request failed.
mdm-resource-null-resp-cnt	Number of times MDM received a null response, which generally occurs because a timeout occurs or a session closes.

Debug MDM Issues

To debug MDM issues, issue the following CLI commands:

- **set debug mdm all-flags level all**
- **set debug success all-flags level all**

Supported Software Information

Releases 21.2.1 and later support all content described in this article.

Additional Information

[Configure File Filtering](#)

[Configure Versa Secure Access Service](#)