FORESCOUT

Forescout

eyeExtend for Microsoft Module

Configuration Guide

Version 1.0.1

Contact Information

Forescout Technologies, Inc.

2400 Dallas Pkwy, Suite 230, Plano, TX 75093

https://www.forescout.com/support-hub/

Toll-Free (US): 1-866-377-8773

Tel (Intl): 1-708-237-6591

About the Documentation

- Refer to the Forescout Documentation Portal for additional technical documentation: https://docs.forescout.com/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2023-08-28 10:27

Table of Contents

About the Microsoft Integration

Microsoft Intune is a cloud-based MDM for all devices (Windows, Mac, Linux and Mobiles).

The Forescout Platform eyeExtend for Microsoft Module provides:

- A single pane of glass for visibility and compliance of all connected devices.
- Network access control and permissions based on Intune enrollment and Intune compliance.
- Automation of compliance and threat response workflows across multi-vendor, multi-tier, policy enforcement points.

Use Cases

The following use cases are supported:

- Validation that the connecting devices are corporate assets on network admission based on Intune enrollment.
- Incorporation of Intune compliance state in Forescout compliance policies and enforcing remediation and restriction actions for non-compliant devices.
- Enrichment of Forescout host properties and classification improvement based on Intune host properties.

Supported Forescout Platform Version

The following table lists the Forescout Platform version that works with each version of the eyeExtend for Microsoft Module that is covered by this guide:

Module Version	Platform Version
1.0.1	Minimum version: 8.4

Microsoft Documentation

Refer to Microsoft online documentation for more information about:

- Microsoft Intune Integration: https://learn.microsoft.com/en-us/mem/intune/
- Microsoft Graph API: https://learn.microsoft.com/en-us/graph/use-the-api
- Microsoft Azure Permissions: https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

How to Work with eyeExtend for Microsoft

This topic describes how to work with the module.

What to Do

Perform the following steps to set up the integration:

1. Download and install the module. See Install eyeExtend for Microsoft.

2. Configure a Microsoft Azure account. See Configure a Microsoft Azure Application.
3. Configure eyeExtend for Microsoft. See Configure eyeExtend for Microsoft.
4. Test eyeExtend for Microsoft. See Test the eyeExtend for Microsoft Module.
5. Create Policies. See Create Microsoft Policies Using Templates

Forescout Platform Requirements

The module requires the following Forescout Platform components:

- A module license for eyeExtend for Microsoft Module. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- Depending on the Operating System: The Endpoint Module with the HPS Inspection Engine/the Linux Plugin/ OS X Plugin running.
- Optional: If 802.1X authentication is used, you need the Authentication Module with the RADIUS Plugin running.

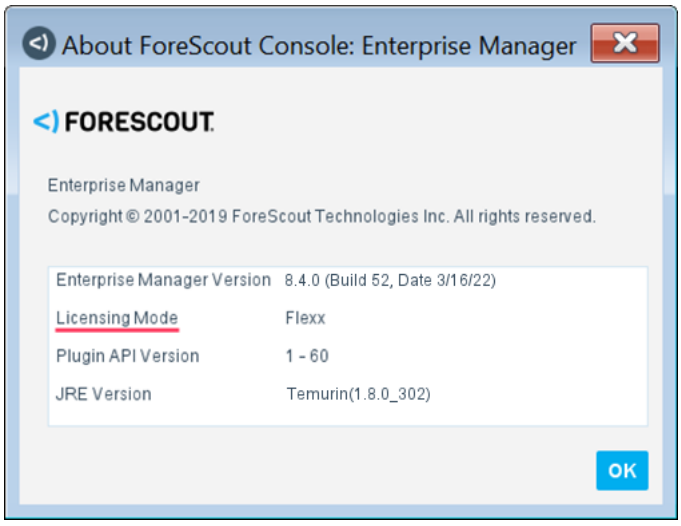
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on the licensing mode of your Forescout Platform deployment.

- For Per-Appliance Licensing
- For Flexx Licensing,

For more information, refer to the Forescout Platform Administration Guide.

To identify the licensing mode of your Forescout Platform deployment, in the Console, select **Help** > **About Forescout**. Then view see the *Licensing Mode* field.



Requesting a License

Refer to the Flexx Licensing Guide.

Install eyeExtend for Microsoft

You need to download and install the module.

To install the module:

1. Navigate to the Downloads page on the Forescout Customer Support Portal.
2. Download the module `.fpi` file.
3. Save the module `.fpi` file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the *Tools* menu.
5. Select **Modules**. The *Modules* pane opens.
6. Select **Install**. The *Open* dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The *Installation* screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

   The installation begins immediately after selecting **Install** *and cannot be interrupted or canceled.*

   In modules that contain more than one component, the installation proceeds automatically one component at a time.

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the *Modules* pane.

    Some components are not automatically started following installation.

Configure a Microsoft Azure Application

eyeExtend for Microsoft Module needs to authenticate against a Microsoft Azure account so that eyeExtend can use APIs to query Intune and obtain endpoint information from Intune.

When you are logged into your Microsoft account, open a file into which you can copy and paste parameters, which you need to save and later use when you configure the eyeExtend for Microsoft Module.

On Microsoft Azure Active Directory (MAAD), you need to:

- Work with a user account with *Global Admin* permissions.

In order that the eyeExtend for Microsoft Module can authenticate against an Intune account via the service principal (the application), you need to register an application and service principal on MAAD, and ensure that you have the required *Global Admin* role, permissions, and owner. See Configure eyeExtend for Microsoft.

You can then log in to an existing Azure *Global Admin* account for your organization which also links to enrolled devices.

Configure eyeExtend for Microsoft

Pre-requisites: Install the eyeExtend for Microsoft Module and complete all of the following Microsoft Azure Active Directory (MAAD) tasks:

- Create a new registered app for this integration: In Azure Active Directory, first create a new app registration to configure the Microsoft Graph Connection for the eyeExtend for Microsoft Module. After registering the app, make sure to copy and save its *Application (client) ID* and its *Directory (tenant) ID*; both these IDs are needed for configuring, in the Forescout Platform Console, the eyeExtend for Microsoft Module.
- Generate (add) a client secret for the app: Next, in Azure Active Directory, generate (add) a new client secret. After generating the client secret, make sure to copy and save its *Value*; the client secret's *Value* is needed for configuring, in the Platform Console, the eyeExtend for Microsoft Module.

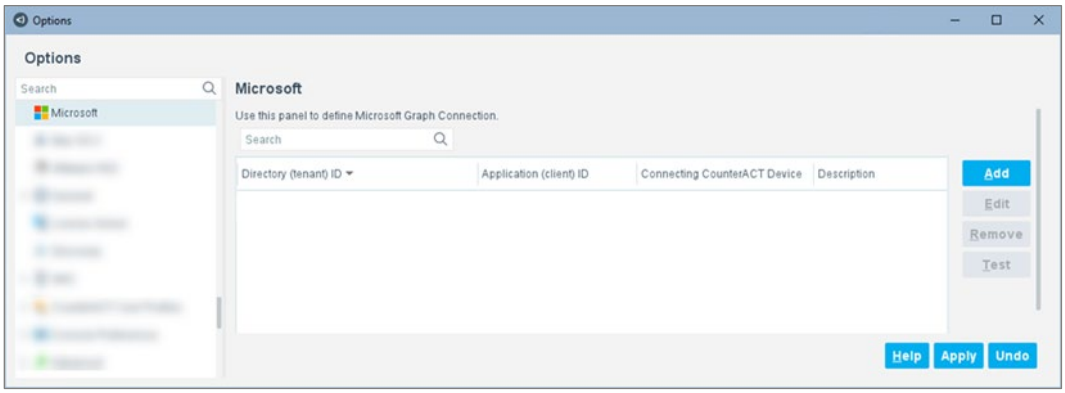
  Immediately copy the client secret's Value because you cannot retrieve it later.

- Configure the following API permissions for the app:
  - For Intune:
    - **`get_device_compliance`** with *Type* = **`Application`**
  - For Microsoft Graph
    - **`Application.Read.All`** with *Type* = **`Application`**
    - **`DeviceManagementManagedDevices.Read`** with *Type* = **`Application`**
    - **`User.Read`** with *Type* = **`Delegated`**
- Admin consent granted for API access by the app
- Get the registered app's *Application (client) ID* and *Directory (tenant) ID* and the generated client secret's *Value*.

Configuring the module means defining the account connection that the eyeExtend for Microsoft Module, via the Forescout Platform, uses to communicate with Microsoft Intune. You can define multiple account connections.

To configure the module:

1. In the Console, select **Options** from the *Tools* menu.
2. In the *Options* navigation pane, select the **Modules** folder.
3. In the *Modules* pane, select **Microsoft**, and select **Configure**. The *Microsoft* pane displays.

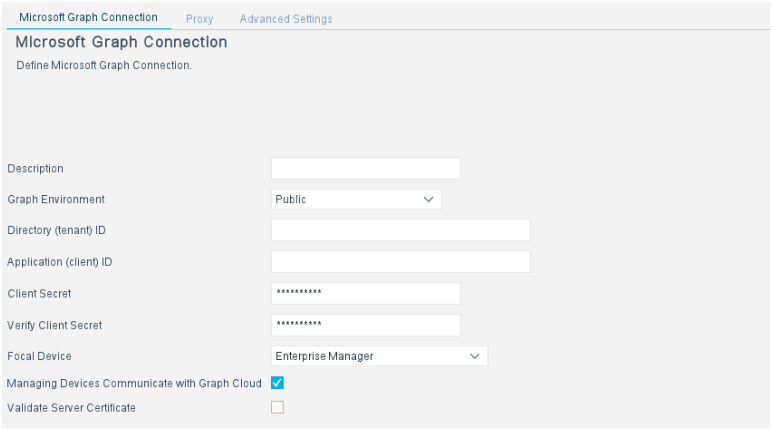


Add Microsoft Graph Connection

Define the Microsoft Graph Connection to configure a connection between the eyeExtend for Microsoft Module, via the Forescout Platform, and Microsoft Intune.

To add a Microsoft Graph Connection:

1. In the *Microsoft* pane, select **Add**. The *Add Microsoft Graph Connection* dialog displays.



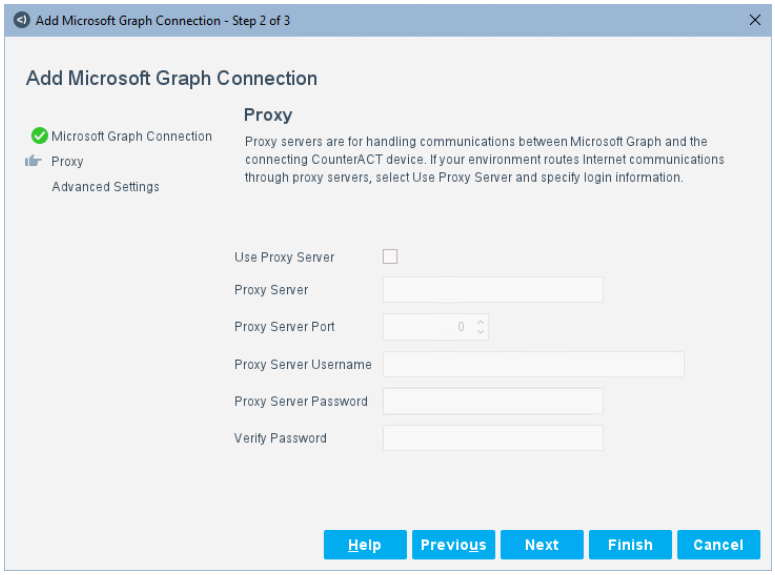
2. In the *Microsoft Graph Connection* pane, configure the following fields:

Description	(Optional) Enter text that describes and qualifies this connection.
Graph Environment	Enter the cloud environment suited to your deployment. For more information, see Available Graph Environments.
Directory (tenant) ID	Enter the *Directory (tenant) ID*. Use the Directory (tenant) ID that you previously saved when creating a new registered app in Microsoft Azure Active Directory. This value is the directory ID in the Azure Active Directory for this account.

Application (client) ID	Enter the *Application (client) ID*. Use the Application (client) ID that you previously saved when creating a new registered app in Microsoft Azure Active Directory.
Client Secret	Enter the *Client Secret*. Use the client secret that you previously saved when generating (adding) a new client secret.
Verify Client Secret	Re-enter the Client Secret to verify it.
Focal Device	Select the connecting CounterACT device that communicates with the Microsoft Graph Connection. This device manages all communication with the Microsoft Graph Connection using the directory ID and the application ID defined for this connection, including requests submitted by other CounterACT devices that you assign to this connection. From the drop-down menu, select the Enterprise Manager or an Appliance IP address.
Managing Devices Communicate with Graph Cloud	Select this option to allow each managing device to communicate with Intune, through the cloud, independently, over the specified **Graph Environment**. If not selected, communication is limited to the Focal Device.
Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ Self-signed server certificate – the server certificate must be installed on the Forescout Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the Forescout Appliance Use the *Certificates* > *Trusted Certificates* pane to add the server certificate to the *Trusted Certificate* list. For more information about certificates, refer to the appendix *The Certificates Pane* in the *Forescout Platform Administration Guide*.

3. Select **Next**. The *Proxy* pane displays.

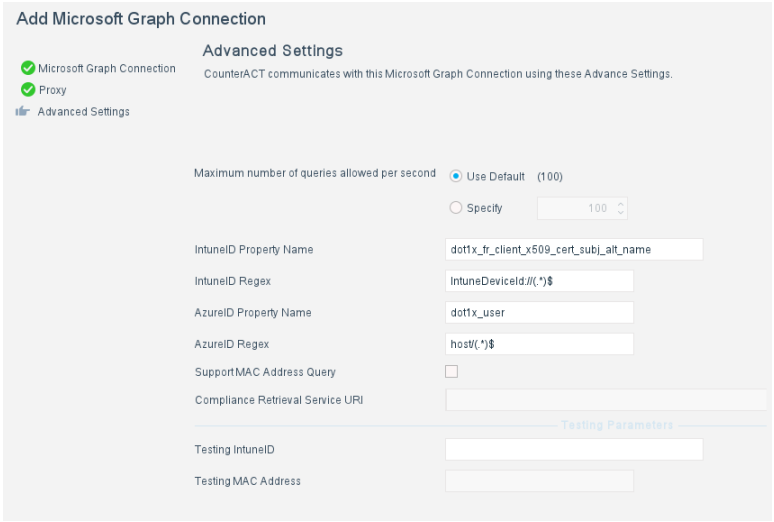
   If your environment routes Internet communications through proxy servers, use this pane to configure the connection parameters for the proxy server that handles communication between the Connecting CounterACT Device and the defined Microsoft Graph Connection.



4. In the *Proxy* pane, configure the following fields:

Use Proxy Server	Select this option to use a proxy server to communicate with the Microsoft Graph Connection.
Proxy Server	Enter the proxy server as a domain name, an FQDN, or an IPv4 address.
Proxy Server Port	Enter the port used to communicate with the proxy server.
Proxy Username	Enter the login name for an authorized account defined on the proxy server, if required.
Proxy Password	Enter the password, if required.
Verify Password	Re-enter the password to verify it.

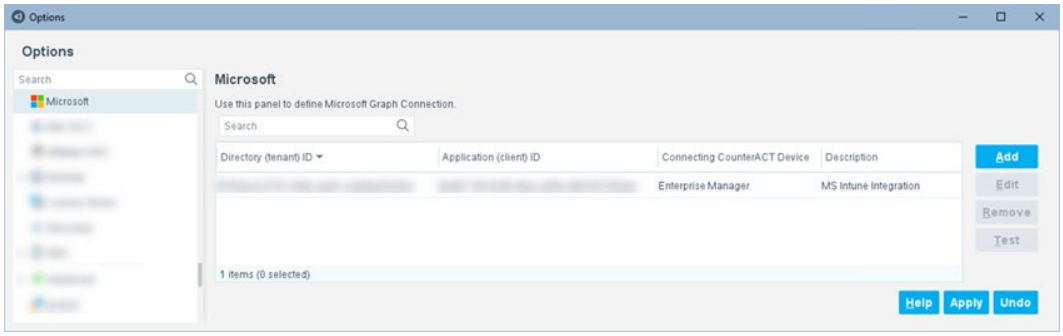
5. Select **Next**. The *Advanced Settings* pane displays.



6. In the *Advanced Settings* pane, configure the following fields:

Maximum number of queries allowed per second	Select the maximum number of queries per second. The range is from 1 to 200. The default is 100. This value limits the number of queries per second for the number of REST API calls to the Microsoft Graph Connection. Set the rate limiting value as follows: ▪ Select **Use Default (100)**. ▪ Select **Specify** and set a value from 1 to 200.
IntuneID Property Name	Enter the IntuneID property name - a host property name that holds a prefix string, appended with the device intune id that is assigned by *Microsoft Intune*. This name is a Forescout internal host property that is obtained by running the following fstool command: `fstool hostinfo $ip` For example: **`dot1x_fr_client_x509_cert_subj_alt_name`** has the value of **`IntuneDeviceId://ca777f24-8d6d-4e35-9f80-e6d3860a1d9f`**
IntuneID Regex	Enter the IntuneID regex. In above **IntuneID Property Name** example, the regex is **`IntuneDeviceId://(.*)$`**. Microsoft Intune recommends using this prefix string as the IntuneID regex.
AzureID Property Name	Enter the AzureID property name – a host property name that holds a prefix string, appended with the *device azure id* that is assigned by *Microsoft Azure*. This name is a Forescout internal host property.
AzureID Regex	Enter the AzureID Regex, which is regular expression. The standard regex is **`AzureDeviceId://(.*)$`**.
Support MAC Address Query	If you activate the checkbox, this allows use of a Microsoft API to get the Intune ID based on the MAC (Media Access Control) hardware address.
Compliance Retrieval Service URI	Per Microsoft Intune documentation, supports access to MAC address endpoints. Requires `Support MAC Address Query`. Example URI: https://some.example.manage.microsoft.com/Traffic*/Traffic*/Resource. This value is copied from the test result shown in the "Test the eyeExtend for Microsoft Module" section.
Testing IntuneID	Verifies connection to Microsoft Intune. You'll see a UUID such as 555abc55-gggg-4ee4-88gg-6e333666999a
Testing MAC Address	Supports the use of Intune to test connections to MAC (hardware) addresses.

7. Select **Finish**. The Microsoft Graph Connection you just configured displays as an entry in the *Microsoft* pane.



8. In the *Microsoft* pane, select **Apply** to save the additions you made to the module's configuration.

After adding a new Microsoft Graph Connection configuration, Forescout recommends that you run a test of the module using this added configuration. See Test the eyeExtend for Microsoft Module.

Available Graph Environments

The plugin supports the following environments:

Cloud	Azure AD Endpoint (to register your app)	Microsoft Graph Root Endpoint
Global	https://login.microsoftonline.com	https://graph.microsoft.com
Azure AD/Microsoft Graph for US Government - L4	https://login.microsoftonline.us	https://graph.microsoftonline.us
Azure AD/Microsoft Graph for US Government – L5 (DoD)	https://login.microsoftonline.us	https://dod-graph.microsoftonline.us
Azure AD/Microsoft Graph Germany	https://login.microsoftonline.de	https://graph.microsoft.de/

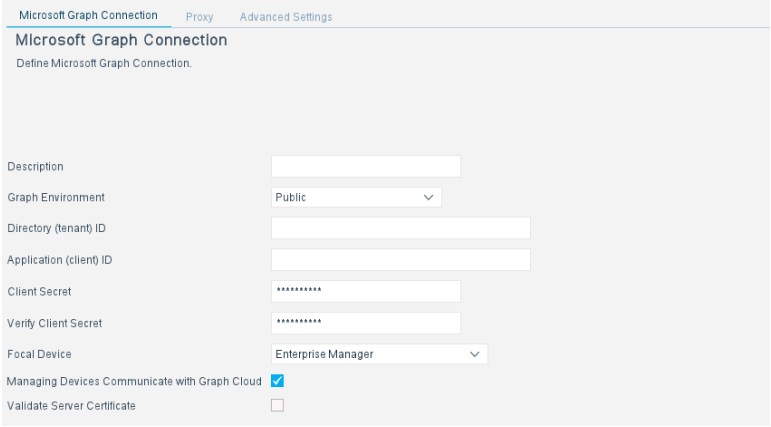
Azure AD/Microsoft Graph China (Operated by 21Vianet)	https://login.chinacloudapi.cn	https://microsoftgraph.chinacloudapi.cn/

Edit Microsoft Graph Connection

You can edit a configured Microsoft Graph Connection.

To edit a configured Microsoft Graph Connection:

1. In the *Microsoft* pane, select a configured Microsoft Graph Connection and select **Edit**.



2. Edit the fields in the **Microsoft Graph Connection** tab, the **Proxy** tab, and the **Advanced Settings** tab.
3. Select **OK**.
4. In the *Microsoft* pane, select **Apply** to save the modifications you made to the module's configuration

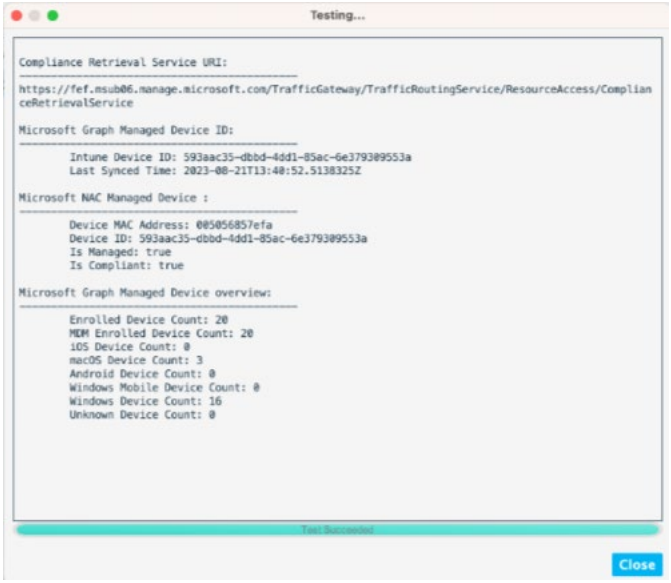
Test the eyeExtend for Microsoft Module

After adding a new Microsoft Graph Connection configuration or editing an existing, Microsoft Graph Connection configuration, Forescout recommends that you run a test of the module using the added or edited configuration. The test uses the selected configuration to check the establishment of a connection between the eyeExtend for Microsoft Module and the Microsoft Graph Connection.

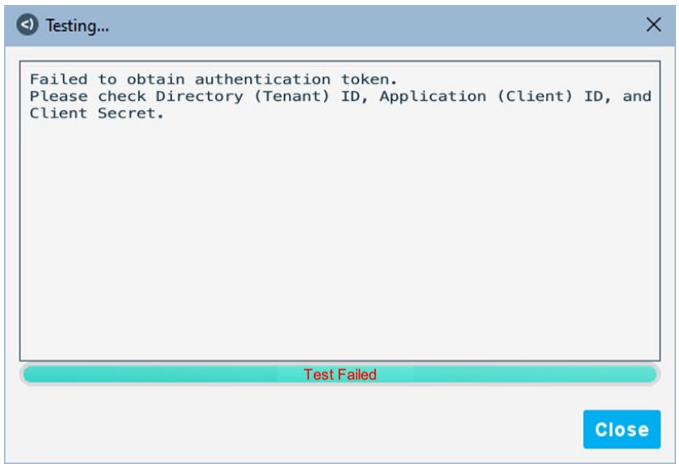
To run a test:

1. In the *Microsoft* pane, select a configured Microsoft Graph Connection and select **Test**.

   If the test is successful, the *Testing* window presents the *Microsoft Graph Managed Device overview*:



   If the test fails, the *Testing* window presents the following message:



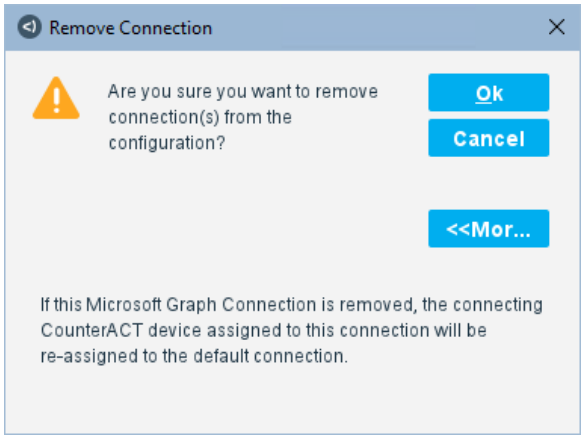
2. Select **Close**.

Remove a Microsoft Graph Connection

You can remove a configured Microsoft Graph Connection from the eyeExtend for Microsoft Module.

To remove a configured Microsoft Graph Connection:

1. In the *Microsoft* pane, select a configured Microsoft Graph Connection and select **Remove**. The *Remove Connection* dialog displays.



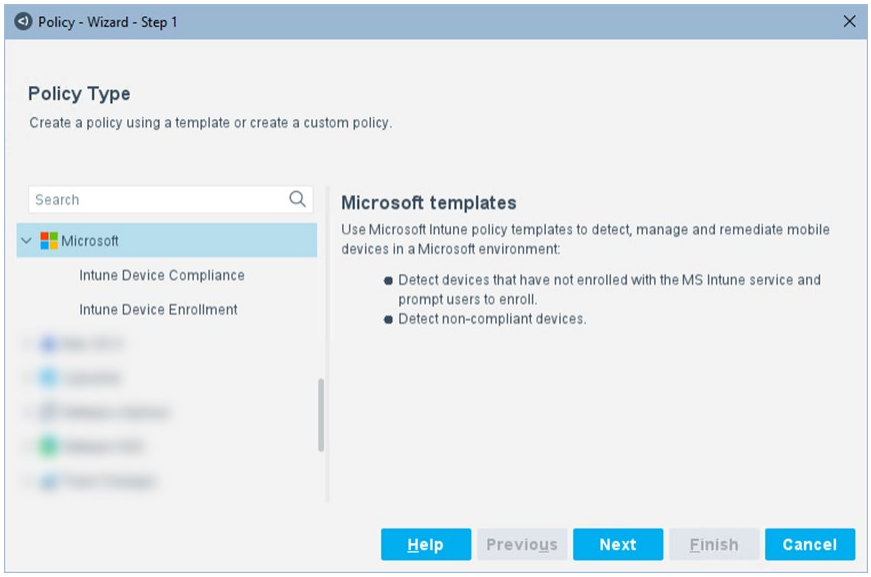
2. If you want to see additional information, select **More Info**.
3. Select **OK**.
4. In the *Microsoft* pane, select **Apply** to save the modification you made to the module's configuration

Create Microsoft Policies Using Templates

Use the Forescout Platform's Microsoft policy templates to create policies that detect, manage, and remediate mobile devices in a Microsoft Intune environment.

See the following topics:

- Create an Intune Device Compliance Policy
- Create an Intune Device Enrollment Policy



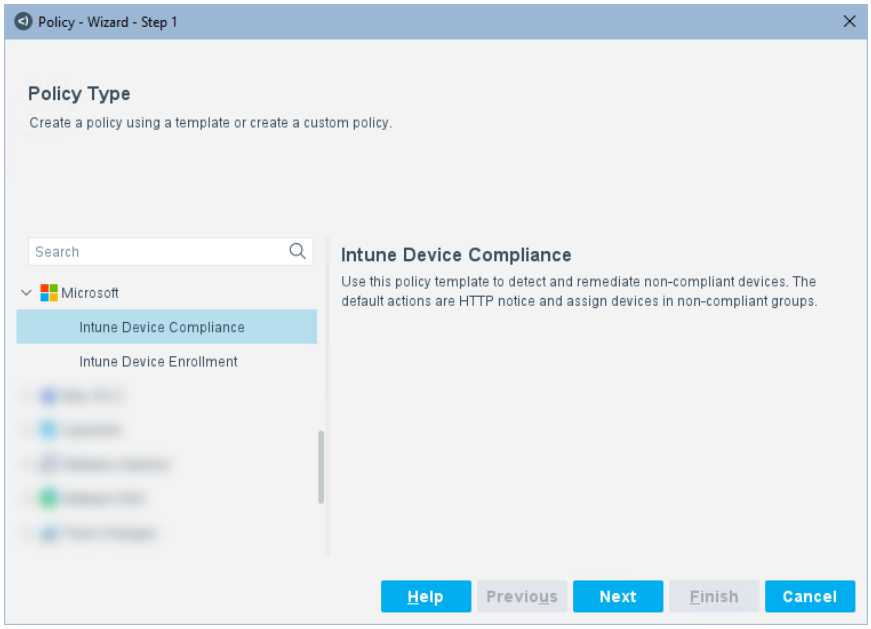
Create an Intune Device Compliance Policy

Use the Intune Device Compliance policy template to accomplish the following network security objective:

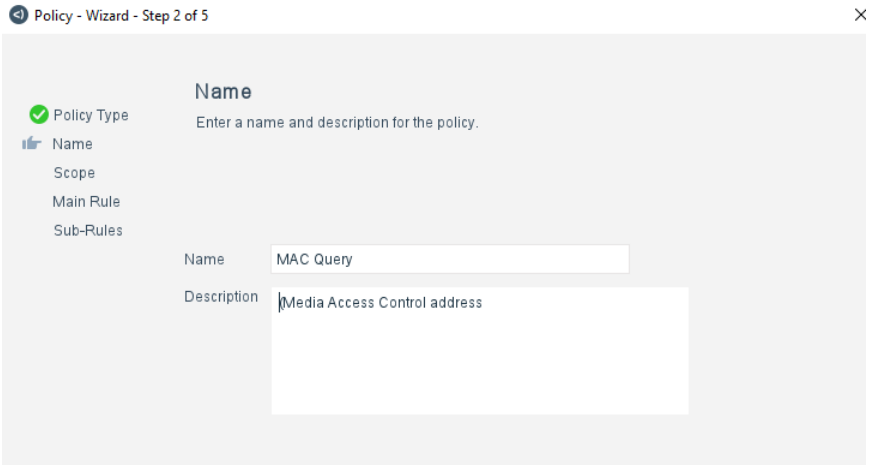
- Create a policy that detects and remediates non-compliant organization endpoints that are connected to the organization's network

To create a policy:

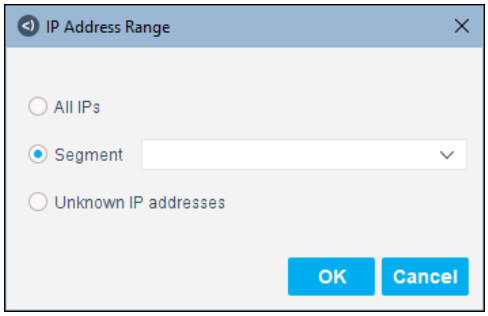
1. Log in to the Console and select **Policy**. The *Policy Manager* pane opens.
2. In the *Policy Manager* pane, select **Add**. The Policy Wizard opens.
3. Expand the **Microsoft** folder and select **Intune Device Compliance**.



4. Select **Next**.



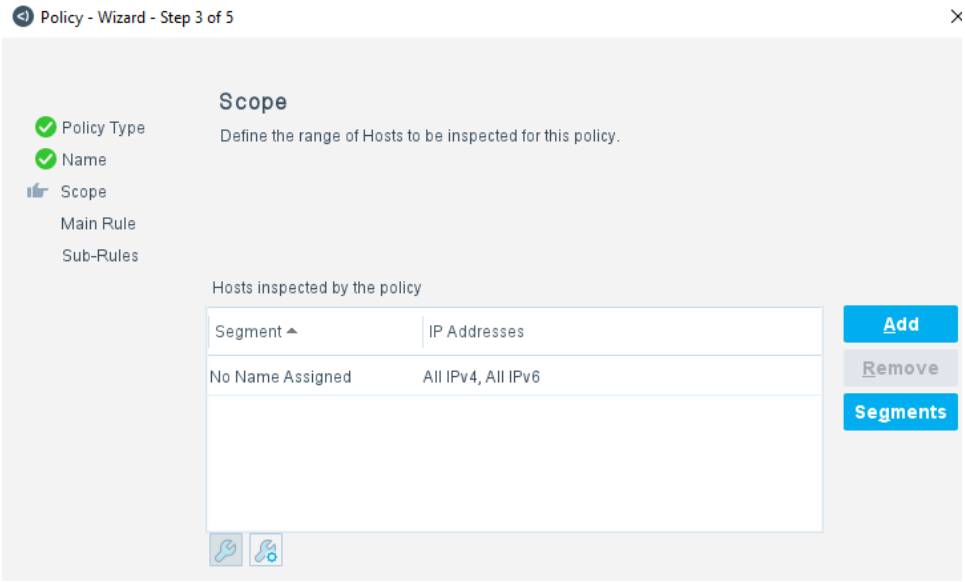
5. Enter a name and optionally add a description.
6. Select **Next**. Both the *IP Address Range* dialog box and the *Scope* pane open.
7. Use the *IP Address Range* dialog box to define which endpoints are inspected.



The following options are available:

a. **All IPs**: Include all IP addresses in the Internal Network.
b. **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the *Scope* pane.
c. **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the *Scope* pane.



9. Select **Next**. You can set up a Policy Main Rule as defined in the Forescout Administration Guide section on Defining a Policy Main Rule.

10. Select **Next** to define **Sub-Rules**.

    The sub-rules check if devices are jailbroken, noncompliant, or compliant. Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

    The three predefined sub-rules have the following conditions:

    - Device Jailbroken - Intune Device is Jail Broken: True
    - Out of Compliance - Intune Device Compliance State: Error, Device is non-compliant and is blocked from corporate resources, Conflicts with other rules, Unknown
    - Compliant - No Conditions

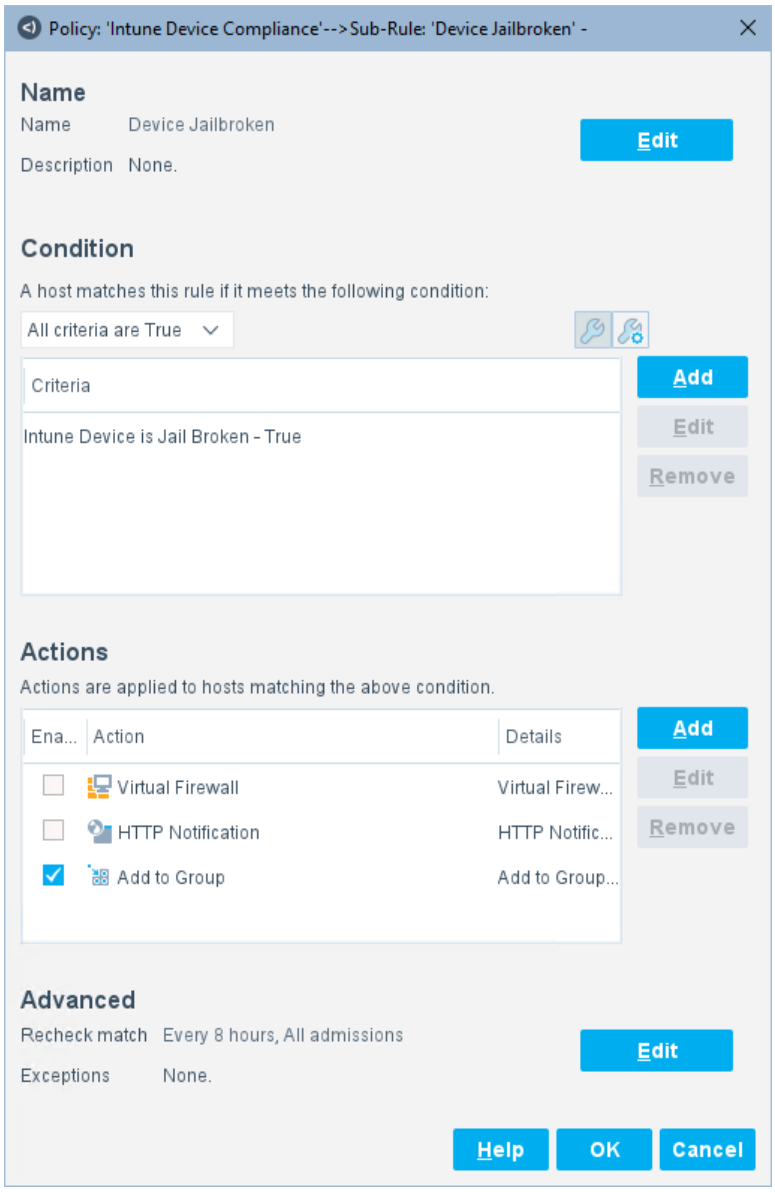
    The *Device Jailbroken* and *Out of Compliance* sub-rules have the following actions:

    - Virtual Firewall (action disabled by default)
    - HTTP Notification (action disabled by default)
    - Add to Group (action enabled by default)

    The *Compliant* sub-rule has the following actions:

    - HTTP Notification (action disabled by default)
    - Add to Group (action enabled by default)

11. Double-click a sub-rule to edit it, for example, to enable an action.



12. To add another condition, select **Add** in the *Condition* area.

13. To add another action, select **Add** in the *Actions* area.

14. In the *Sub-Rule* dialog box, select **OK**.

15. In the *Sub-Rules* pane, select **Finish**.

16. In the *Policy Manager* pane, select **Apply**.

Create an Intune Device Enrollment Policy

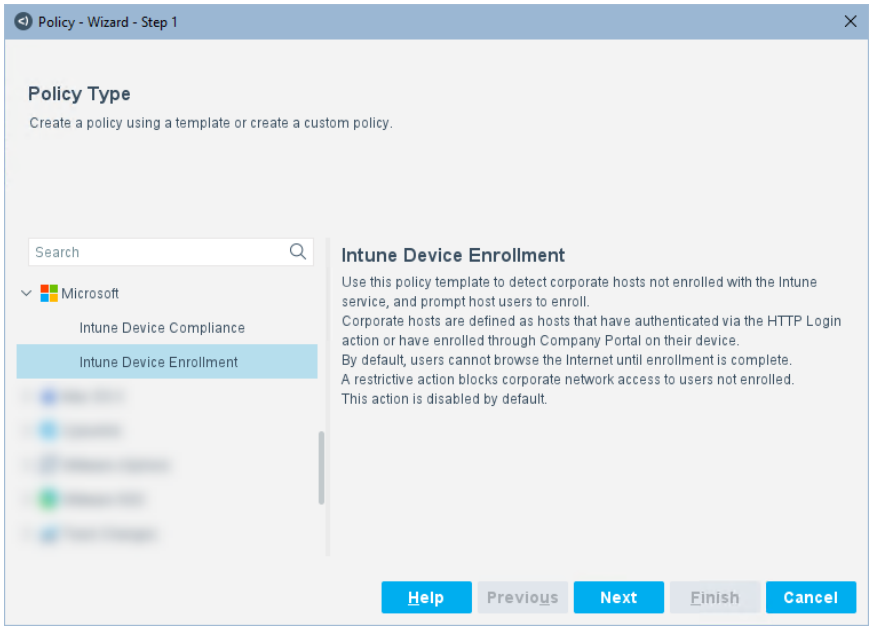
Use the Intune Device Enrollment policy template to accomplish the following network security objectives:

- Detect organization endpoints that are connected to the organization's network and not enrolled in the Microsoft Intune service
- Prompt the users of these detected endpoints to enroll in the Microsoft Intune service

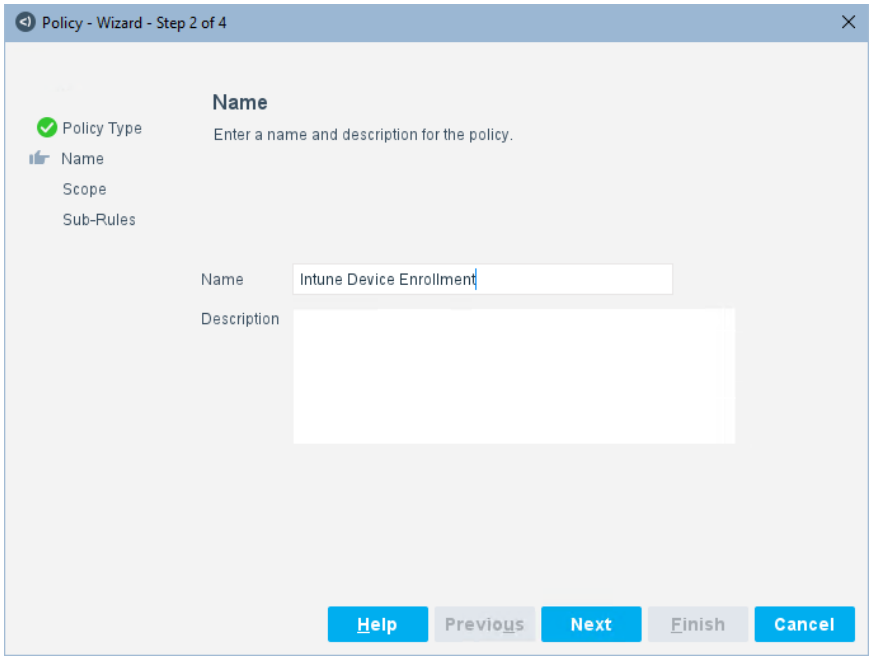
Organization endpoints are defined as endpoints that have authenticated via the *HTTP Login* action or have enrolled by using their endpoint to access the organization portal. By default, users cannot browse the Internet until they complete their endpoint enrollment.

To create a policy:

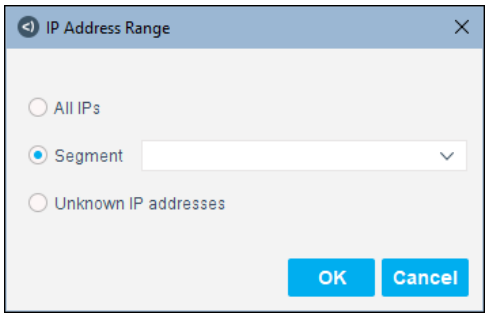
1. Log in to the Console and select **Policy**. The *Policy Manager* pane opens.
2. In the *Policy Manager* pane, select **Add**. The Policy Wizard opens.
3. Expand the **Microsoft** folder and select **Intune Device Enrollment**.



4. Select **Next**.



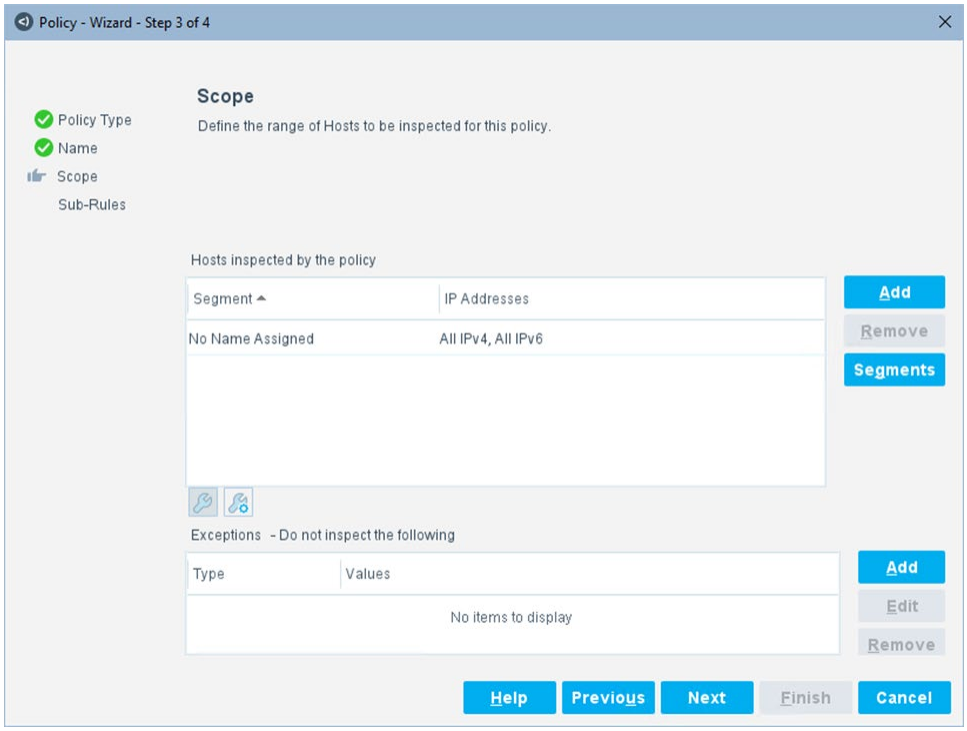
5. Enter a name and optionally add a description.
6. Select **Next**. Both the *IP Address Range* dialog box and the *Scope* pane open.
7. Use the *IP Address Range* dialog box to define which endpoints are inspected.



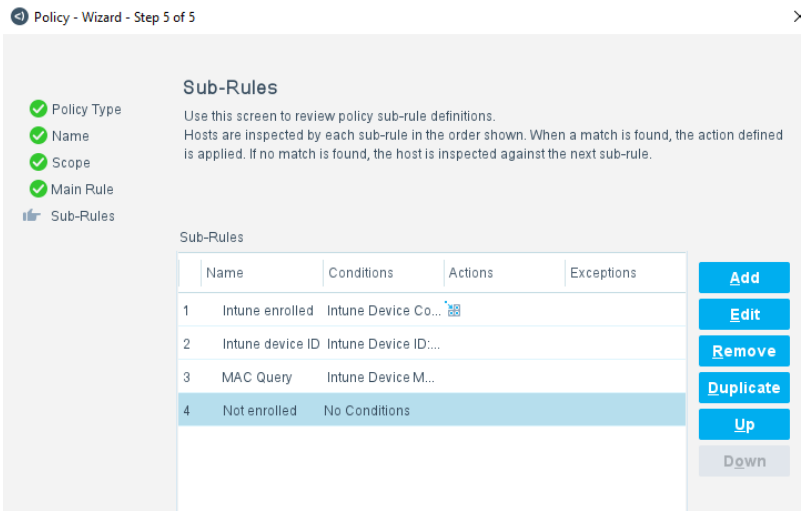
The following options are available:

a. **All IPs**: Include all IP addresses in the Internal Network.
b. **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the *Scope* pane.
c. **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the *Scope* pane.



9. Select **Next** to display the Sub-rules**.**



The sub-rules check if devices are enrolled, not enrolled, unknown, or noncorporate. Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

The predefined sub-rules have the following conditions:

- Intune Enrolled
- Intune Device ID: Any Value (Resolved by prerequisite HPS [Windows] or OSX [Apple] plugins.)

- MAC Query (If you've activated the Support MAC Address Query option.)
- Not Enrolled

The *Intune Enrolled* sub-rule has the following action:

- Add to Group (action enabled by default)

10. Double-click a sub-rule to edit it.

11. To add another condition, select **Add** in the *Condition* area.

12. To add another action, select **Add** in the *Actions* area.

13. In the *Sub-Rule* dialog box, select **OK**.

14. In the *Sub-Rules* pane, select **Finish**.

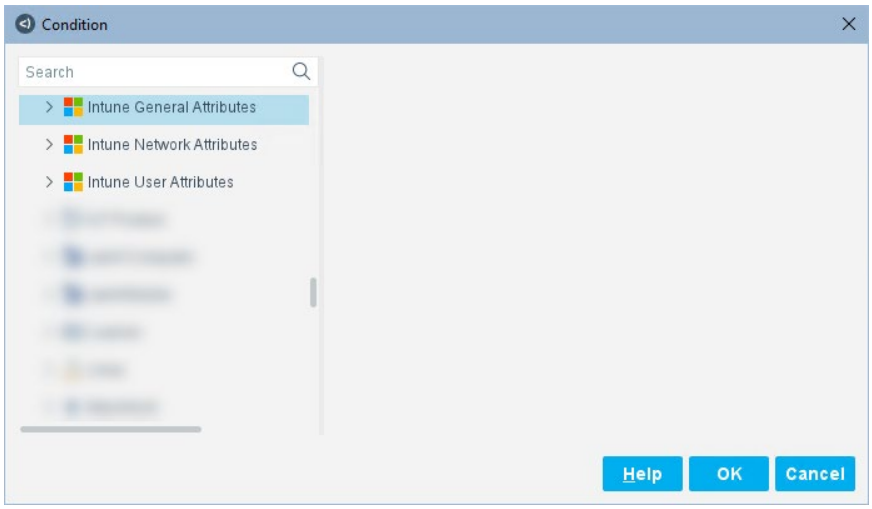
15. In the *Policy Manager* pane, select **Apply**.

Properties for eyeExtend for Microsoft

Properties are used to instruct the Forescout Platform to detect endpoints with specific attributes or conditions. In the policy, whether you are creating or editing it, use properties in a policy main rule and in policy sub-rules to define the appropriate and necessary conditions for evaluating detected endpoints.

To add properties:

- In the search field of the *Condition* window, search for the word **Intune**. In the *Properties* tree, the following Intune property groups are available:
  - *Intune General Attributes*
  - *Intune Network Attributes*
  - *Intune User Attributes*



Open the **Intune General Attributes** group to select a property from among the following available properties:

Intune Device Azure ID	Contains the unique identifier (read-only) of the Azure device.
Intune Device is Registered in AAD	Identifies whether the device is registered in the AAD.
Intune Device Compliance State	Identifies the compliance state of the device. The possible values are: Compliant, Conflicts with other rules, Device is non-compliant and is blocked from corporate resources, Error, In grace period, Managed by configuration manager, and Unknown.
Intune Device Name	Identifies the name of the device.
Intune Device Owner Type	Identifies the owner type of the device.
Intune Device Enrolled DateTime	Identifies the date and time when the device was enrolled.

Intune Device Enrollment Type	Identifies the enrollment type of the device.
Intune Device ID	Contains the unique identifier of the device.
Intune Device is Supervised	Identifies the supervised status of the device.
Intune Device is Jail Broken	Identifies whether a device is jailbroken. The possible values are: False, True, and Unknown.
Intune Device Last Sync DateTime	Identifies the date and time when the device last completed a successful synchronization with Intune.
Intune Device Manufacturer	Identifies the manufacturer of the device.
Intune Device Model	Identifies the model of the device.
Intune Device Operating System	Identifies the operating system of the device, such as Windows or iOS.
Intune Device Operating System Version	Identifies the operating system version of the device.
Intune Device Reported Threat State	Identifies the (read-only) threat state of a device with a Mobile Threat Defense partner in use by the account and device. The possible values are: Activated, Compromised, Deactivated, High Severity, Low Severity, Medium Severity, Misconfigured, Secure, Unknown, and Unresponsive.
Intune Device Serial Number	Identifies the serial number of the device.
Azure Active Directory ID	Identifies the tenant ID of the source AAD account.
Intune Unlock PIN	Identifies the unlock PIN. The remote lock action for macOS devices contains a recovery PIN. When a new remote action is taken, a new PIN is generated and populated on the Platform.

Open the **Intune Network Attributes** group to select a property from among the following available properties:

Intune IMEI	Identifies the International Mobile Equipment Identity (IMEI), which is a unique number that identifies all mobile phones and smart phones.
Intune MEID	Contains the mobile equipment identifier (MEID), which is a unique number that identifies a mobile device.
Intune Device Wi-Fi MAC	Identifies the Wi-Fi MAC address of the device.

Open the **Intune User Attributes** group to select a property from among the following available properties:

Intune Device Email Address	Identifies one or more email addresses for the user associated with the device.

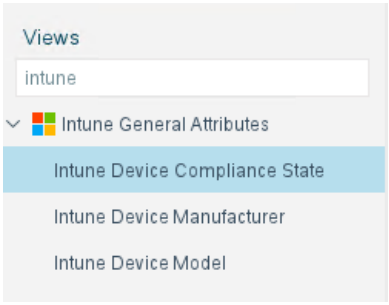
Intune Device Phone Number	Identifies the phone number of the device.
Intune Device User Display Name	Identifies the user display name of the device.
Intune Device User ID	Contains the unique identifier of the user associated with the device.

Display Asset Inventory

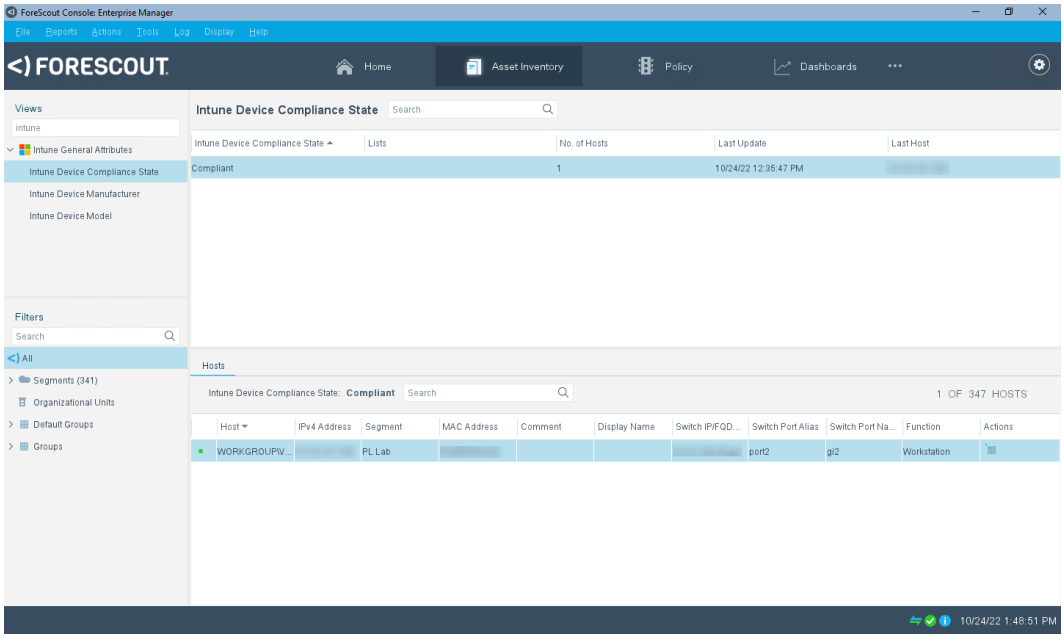
You can view Intune attributes in the *Intune General Attributes* folder of the *Asset Inventory* tab**.**

To access the Intune inventory:

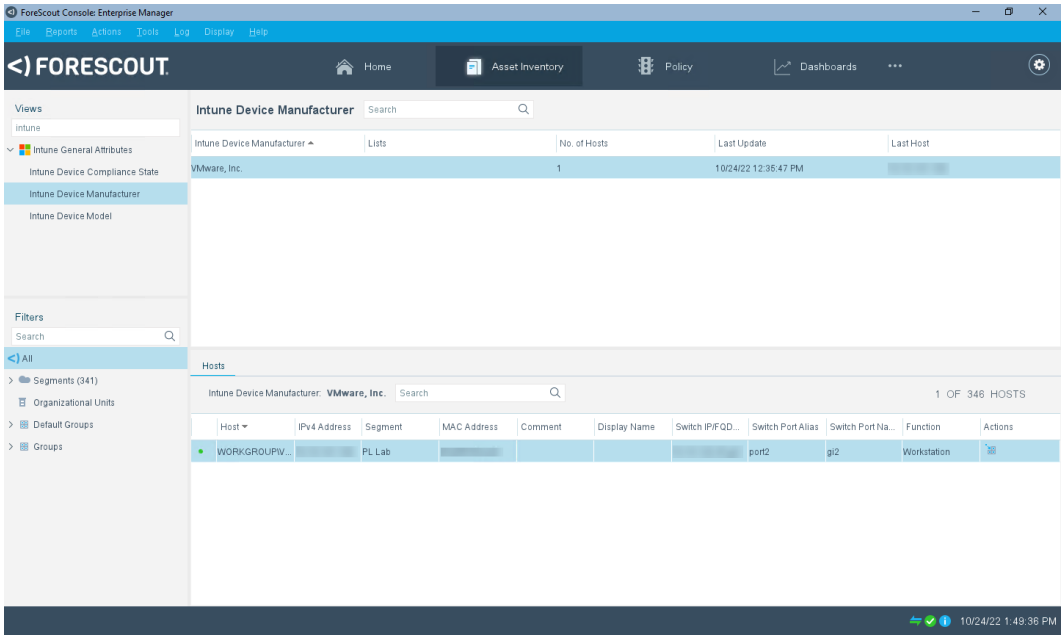
1. Log in to the Console and select **Asset Inventory**.
2. In the search field of the *Views* pane, search for and expand the **Intune General Attributes** folder.



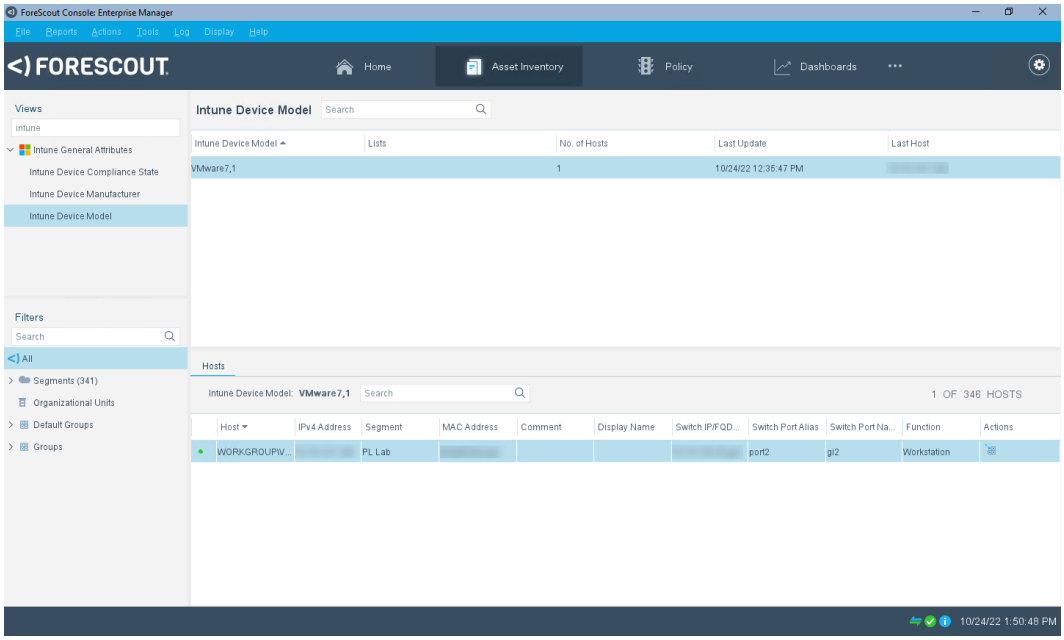
3. Select **Intune Device Compliance State** to view Intune device compliance state information. Select a specific state to view additional details.



4. Select **Intune Device Manufacturer** to view device manufacturer information. Select a specific manufacturer to view additional details.



5. Select **Intune Device Model** to view Intune device model information. Select a specific model to view additional details.



Intune Information Filters

The *Filters* pane, which is available in both the *Asset Inventory* tab and the *Home* tab, provides Intune filters that modify the information being displayed to you in the Console.

To access the Intune information filters:

1. In the Console, select either the **Asset Inventory** tab or the **Home** tab.
2. In the search field of the *Filters* pane, search for the word **Intune**. The *Groups* folder expands to reveal the following Intune information filters:
   - *Intune Compliant Devices*
   - *Intune Enrolled Devices*
   - *Intune Non-Compliant Devices.* Expand this group to reveal the following Intune filter sub-group:
     - › *Intune Jailbroken Devices*
       - *Intune Offsite Devices*
3. Select any of these filters to accordingly modify the information you are viewing in either the *Asset Inventory* tab or the *Home* tab.