

Forescout

eyeExtend for Intune App README.md Version: 2.0.8

Configuration Guide

Version 2.0.8

Contact Information

- Have feedback or questions? Write to us at

connect-app-help@forescout.com

APP Support

- All eyeExtend Connect Apps posted here are community contributed and community supported. These Apps are not supported by the Forescout Customer Support team.
- See Contact Information above.

About Connect APP for Intune

Version 2.0.8 Changes

Added an ACTION request Intune SYNC with the endpoint. Modified the TAG properties to state "PUBLIC" and not "US-PUBLIC". The APP can now connect to the US Government environment. You can select the bet or v1.0 production environments also.

About This Module

Version 2 of the Intune APP has now split the permissions for the discovery/resolve and control actions (wipe/remote lock). *The reason for this is some customer(s) may not require action(s). Actions require a user credential and discovery / resolve only require an application credential.*

The APP now uses *two* APIs.

NAC API was added to enable the resolve of endpoints coming onto the network. The NAC API allows for a query by MAC address.

GRAPH API is used to query for Intune properties and using the “Azure Device ID” learned from the NAC API.

Advantages of using the NAC API.

- Query by MAC address (Enrolled / Not Enrolled, Compliances state)
- Ethernet and Wi-Fi MAC address are handled by the NAC API.

This also means you do not have to enable the host discovery, which will poll for Wi-Fi only devices and all devices that’s Intune has registered, even when not connected to the on-premise network.

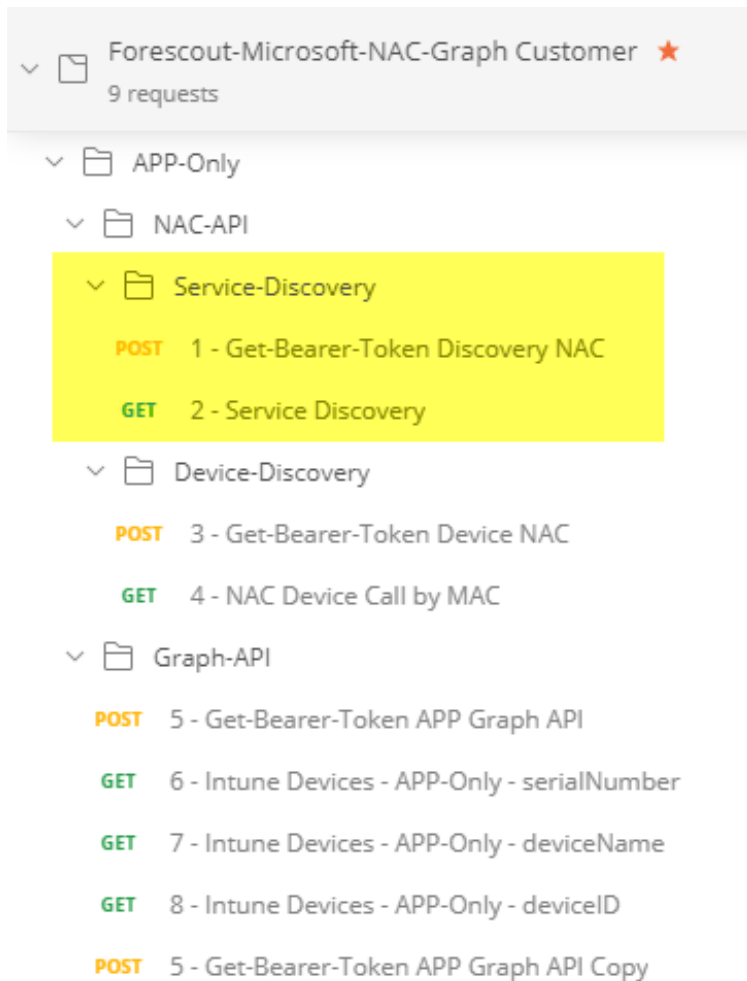
The GRAPH API does not expose the ethernet MAC address in the schema for production Intune environments as of December 2020.

NAC API

To use the NAC API you will have to obtain the NAC API Service Endpoint URI

Example : <https://fef.amsuaXXXX.manage.microsoft.com/StatelessNACService>

Use the POSTMAN collection "Forescout-Microsoft-NAC-Graph-Customer" to help you discover the service endpoint. *See the POSTMAN section below for details.*



Use Cases

This section describes important use cases supported by Forescout eyeExtend for Intune.

Intune NAC API Device Managed

Use this policy template to detect corporate hosts using the NAC API. This should be the first policy to discover devices joining the network. The policy will add the device to a group "Intune Device", used to help other Intune policies.

Intune GRAPH API Device Compliance

Use this policy template to detect corporate compliance status. The policy checks for device(s) if they have been jail broken / Intune compliance status.

How It Works

The following Intune components are required for this integrated solution:

- **Microsoft NAC and Graph API:** The Forescout platform addresses the API exposed by the platform to retrieve endpoint information and perform actions.

The following Forescout platform components support the integration:

- **Forescout eyeExtend for Intune:** This cloud-delivered module handles communication with Intune and provides the properties, actions, and policies described in this guide.
- **Forescout eyeExtend Cloud:** A Forescout cloud service that handles third-party integrations including the integration with Intune, which provides the endpoint properties and actions described in this guide.
- **Forescout eyeExtend Connect Plugin:** An infrastructure for integrating third-party vendors with the Forescout platform.
- **Forescout eyeExtend Intune App:** The Connect App developed by Forescout to implement the integration with Intune.

In a typical deployment, several cloud connections are defined in the Forescout platform. Connections to the cloud may be planned based on anticipated traffic or geographic location. The deployment is as follows:

- A single CounterACT® device connects to each cloud access point, handling communication for a cluster of CounterACT devices. The CounterACT devices in the cluster only work with that Intune cloud instance.
- For each connection, the rate limiting of messaging from the Forescout platform to the Intune cloud can be configured.

What to Do

To set up your system for integration with eyeExtend for Intune, perform the following steps:

1. Verify that the requirements are met. See Requirements.
2. Download and install the module. See How to Install.
3. Configure the module. See Configure the Module.
4. Configure policy templates. See Configure Intune Policy Templates.
5. Configure properties. See Configure Properties.
6. Configure actions. See Configure Actions.

Requirements

- Forescout version 8.1.4, 8.2.1
- Forescout eyeExtend for Microsoft Intune requires the following:
 - An Azure online account for you to log in to <https://portal.azure.com/>.
 - For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Note that Connect App for Microsoft Intune acquires up to 3 authorization tokens and queries device information through the following URLs.

You can whitelist them to allow access.

- <https://login.microsoftonline.com/>
- <https://graph.microsoft.com/>
- <https://fef.amsuaXXXX.manage.microsoft.com/StatelessNACService/devices/>

The API permissions have a specific type

- NAC API, type equals *application*.
- GRAPH API, type equals *application*.
- ACTIONS, type equals *delegated*. **See section Intune Permissions # How to Install**
Get Forescout eyeExtend Connect plugin and Intune App from Forescout.

Ensure That the Plugin is Running

After installing the Connect plugin, ensure that it is running.

To verify:

1. Select **Tools > Options > Modules**.
 2. Navigate to the component and hover over the name to view a tooltip indicating if it is running on Forescout devices in your deployment. In addition, next to the component name, you will see one of the following icons:
 - The component is stopped on all Forescout devices.
 - The component is stopped on some Forescout devices.
 - The component is running on all Forescout devices.
1. If the component is not running, select **Start**, and then select the relevant Forescout devices.
 2. Select **OK**.

Intune Permissions

The Intune APP can use two types of identity.

- User Identity
- Application Identity (Service Principal)

When applying the API permissions you have to select the type.

- Application
- Delegated.

Identity	Permission Type	Forescout Usage	API	Comment
Application (Service Principal)	Application	Discovery / Resolve	NAC / GRAPH	Read only
User	Delegated	Action(s)	GRAPH	Actions (Remote Lock / Wipe)

The reason we use up to three different tokens. NAC and GRAPH, use a different resource, therefore require a bearer token each and a bearer token for the user identity i.e actions.

[Home](#) > [App registrations](#) > [sp-intune-connect-app](#)

[sp-intune-connect-app](#) | API permissions

Search (Ctrl+/)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Forescout Technology Inc - BD

API / Permissions name	Type	Description	Admin consent req...	Status
Intune (1)				...
1 get_device_compliance	Application	Get device state and co...	Yes	✓ Granted for Forescout T...
Microsoft Graph (4)				...
4 Application.Read.All	Application	Read all applications	Yes	✓ Granted for Forescout T...
2 DeviceManagementManagedDevices.PrivilegedOperations.All	Delegated	Perform user-impacting ...	Yes	✓ Granted for Forescout T...
2 DeviceManagementManagedDevices.Read.All	Application	Read Microsoft Intune d...	Yes	✓ Granted for Forescout T...
3 User.Read	Delegated	Sign in and read user pr...	No	✓ Granted for Forescout T...

To view and manage permissions and user consent, try [Enterprise applications](#).

Details for the above application permission

Number	Forescout Usage	API	Type	Forescout Configuration TAB
1	Resolve query for a device coming onto the network. Query by MAC address	NAC	Application	Intune Connection
2	Actions to Remote Lock / Wipe devices	GRAPH	Delegated	Intune ACTION
	<i>Required User Identity with Intune "Intune Administrator" Role</i>			Intune ACTION
3	Resolve query for device, Intune specific data. Query uses " Azure Device ID " from NAC Query (1)	GRAPH	Application	Intune Connection
	Host Discovery	GRAPH	Application	Intune Options
4	Required for Service Endpoint Discovery	GRAPH	Application	Postman

User Identity

If you are using ACTION(S) *remote lock / wipe*, the user identity requires the "Intune Administrator" role.

The screenshot shows the Azure Active Directory user interface for a user named 'test-intune-'. The 'Assigned roles' section is visible, and the 'Administrative roles' tab is selected. The 'Intune administrator' role is listed with the description 'Can manage all aspects of the Intune product.'.

Create User and Application

- On Azure Active Directory (AAD), you need to:

- Create a user account and assign it a role.
- Create an application and assign it an owner.

Before the Forescout platform can authenticate against an Intune account via the service principal (the application), you need to perform the following procedures to register an application and service principal on AAD, as well as ensure that you have the required role, permissions, and owner.

You can obtain the Directory (Tenant) ID and Application (Client) ID from the Azure portal.

Create a New User

Go to <https://portal.azure.com/> and log in to your account. Select **Azure Active Directory > Users New User**

Enter the required information - Name: The of the user, for example: New User

User name: The user name of the user, for example: New.User@domain.onmicrosoft.com

- A temporary password is generated for the user account. Click **Show Password** and copy the temporary password.

Create

- Recommendation: In another browser session, open a New incognito window, log in with the new user and temporary password, then change the password. **Tip:** To find your domain, which ends in onmicrosoft.com, go to Azure Active Directory > Overview

Assign Intune Administrator Role

Select **Azure Active Directory > Users** Locate the new user you created and select it by clicking the user name

Assigned Roles Add assignments Search - **Intune administrator**

Add

Check AAD Permissions

Select **Azure Active Directory > User settings**

Check the setting of **App registrations**

If **App registrations** is set to **Yes**, any user in the AAD tenant, including a non-admin user, can register an app.

If **App registrations** is set to **No**, only global administrators can register AD apps. Check if your account is an admin for the AAD tenant. Select **Overview** and view your user information. If your

account is assigned to the User role, but the setting of **App registrations** is limited to admin users, ask your administrator to assign you to the global administrator role or to enable users to register apps.

Create an AAD Application

Select **Azure Active Directory > App registrations. New registration.**

Enter the **Name** for the application, for example, fs-intune-plugin-app.

- *The application name must be unique across an Azure region*
- *The Redirect URI is not used in the Intune integration*

Register and review the application details in **Overview**.

Authentication and scroll to **Default client type**

For Default client type, select **Yes** to treat application as a public client. (OPTIONAL)

Select **Save**

Assign GRAPH API Permissions

Select **Azure Active Directory > App registrations.**

- Select the app you created, for example, fs-intune-plugin-app.

Add a permission. Microsoft Graph. Delegated.**

In **Type to search**, type DeviceManagementManagedDevices.

Select the following two graph API permissions:

- **DeviceManagementManagedDevices.PrivilegedOperations.All** *Perform user-impacting remote actions on Microsoft Intune devices*

Add Permissions - Microsoft Graph. Type Application.

Search DeviceManagementManagedDevices.

- **DeviceManagementManagedDevices.Read.All** To read Microsoft Intune devices

Add Permissions. The API permissions are displayed.

Assign NAC API Permissions

Select

Add Permissions - Intune.

Type **Application**.

Search - `getdevicecompliance`

Add Permissions. Grant admin consent for XXX.

Yes.

Assign the App an Owner

Select **Azure Active Directory > App registrations**.

Select the app you created, for example, *fs-intune-plugin-app*, and select **Owners**.

Note that the new user is not in the list.

Select **Add owner**.

Select the new user and select **Select**.

Obtain tenant ID, application ID, and application secret:

```
Select **Azure Active Directory > App Registrations**
Select your application, for example, fs-intune-plugin-app
The information is displayed.
Copy the **Application ID** and store it in your application code.
```

The application ID is also referred to as the client ID.

Copy the **Directory (Tenant) ID**. Include it with your authentication request.

Configure the Module

After eyeExtend Connect is installed, **Connect** is displayed under **Options**.

Configure Intune App

To configure eyeExtend for Intune, you import the Intune App and then add a system description.

Initially, the App Configuration tab of the **Connect** pane is blank. The Intune App has not been imported yet and the system description has not been configured yet.

Import an App

You can import the Intune App.

To import the Intune App:

In the App Configuration tab of the **Connect** pane, select **Import**. Apps that can be imported are in .zip or .eca format. They can be in any folder. Select **Import**.

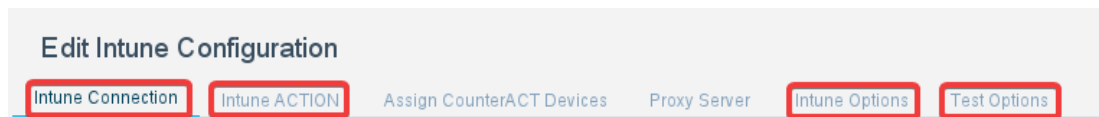
If the app is imported successfully, a message is displayed at the bottom of the **Sending** dialog box.

If the app is not imported successfully, error messages are displayed in the **Sending** dialog box.

Select **Close** when the import has finished. A blank **System Description** dialog box opens. See Add a System Description.

- If you select **Close** before the import has finished, it will fail.

Panels



After the app is imported, the **System Description** dialog box opens. It is initially blank and only the **Add** and **Import** buttons are enabled.

To configure the Intune App, you add a system description to define a connection, which includes login credentials.

If a system description has not been configured and you select **OK** now, a warning message is displayed.

Select **Add**

Intune Connection

Edit Intune Configuration

- Intune Connection
- Intune ACTION
- Assign CounterACT Devices
- Proxy Server

Intune Connection

Intune Connection

Description	<input type="text" value="Test1"/>
Environment	<input type="text" value="Intune Public"/>
GRAPH Environment Version	<input type="text" value="v1.0"/>
Tenant ID	<input type="text" value="256"/>
Application ID	<input type="text" value="d6"/>
Application Secret	<input type="password" value=""/>
Verify Application Secret	<input type="password" value=""/>
NAC API : Service Endpoint URI	<input type="text" value="StatelessNACService"/>

Enter the following information:

- Description: Enter a description for the Intune account.
- Environment: You can now select Intune Public or Intune US Government
- You have the option to select v1.0 production or beta environments.
- Tenant ID: Enter the account tenant ID. See Obtain Tenant ID, Application ID and Secret.
- Application ID: Enter the account application ID. See Obtain Tenant ID, Application ID and Secret.
- Password: Enter the secret for the Intune Application ID.
- NAC API: Service Endpoint URI
 - Example <https://fef.amsuaXXXX.manage.microsoft.com/StatelessNACService>

See the *POSTMAN* section below for details.

Note the user delegated credentials has been moved to "Intune ACTION" panel

Select **Next**.

Intune ACTION

If you are *not* using the action **wipe/remote lock**, skip this panel.

Edit Intune Configuration

Intune Connection **Intune ACTION** Assign CounterACT Devices Proxy Server Intune Options Test Options

Intune ACTION

Intune ACTIONS require delegated permissions
If you are NOT using any actions WIPE / REMOTE LOCK
You can SKIP this tab

Username:

Password:

Verify Password:

- Username
- Password

Select **Next**.

Intune Devices

Connect Configuration [Close]

Edit Intune Configuration

Intune Connection Intune ACTION **Assign CounterACT Devices** Proxy Server Intune Options Test Options

Assign CounterACT Devices

Select the connecting CounterACT device that will communicate with the targeted Intune Account instance, including requests by other CounterACT devices. Specific CounterACT devices assigned here cannot be assigned to another server elsewhere.

If you do not assign specific devices, by default, all devices will be assigned to one server. This server becomes known as the Default Server.

Connecting CounterACT Device: ▾

☐ Assign specific devices ☒ Assign all devices by default

- Initially, the Assign CounterACT Devices panel has only one option, **Assign all devices by default**, and it is selected so that one device is added.

If you want to add a second device, the Assign CounterACT Devices panel has more options.

Enter the following information:

- Connecting CounterACT Device: Select Enterprise Manager or an IP address of the connecting CounterACT device. In an environment where more than one CounterACT device is assigned to a single third-party instance, the connecting CounterACT Appliance functions as a middleman between the third-party instance and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the third-party instance.

- Assign specific devices: This CounterACT Appliance is assigned to a third-party instance, but it does not communicate with it directly. All communication between the third-party instance and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the third-party instance. All the IP addresses handled by an assigned Appliance must also be handled by the third-party instance to which the Appliance is assigned.
 - Select **Available Devices** and then select an IP address or Appliance name from the Available Devices list.
 - Select **Add**. The selected device will send its requests to the third-party instance through the connecting Appliance.
- Assign all devices by default: This is the connecting Appliance to which CounterACT Appliances are assigned by default if they are not explicitly assigned to another connecting Appliance. Select this option to make this connecting Appliance the middleman for all CounterACT Appliances not assigned to another connecting device.

Note the following:

- An error message is displayed if you try to add a device that is already used.
- If you have apps that discover 50,000 or more endpoints, distribute the apps in such a way so that only up to two of the apps share the same focal (connecting) appliance. An alternative is to split the endpoints across multiple user accounts on multiple servers.

Select **Next**.

Proxy Server

Edit Intune Configuration

[Intune Connection](#)
[Intune ACTION](#)
[Assign CounterACT Devices](#)
[Proxy Server](#)
[Intune Options](#)
[Test Options](#)

Proxy Server

Select a Proxy Server device to manage all communication between CounterACT and the Intune server.

Use Proxy Server

☐

Proxy Server

Proxy Server Port

Proxy Server Username

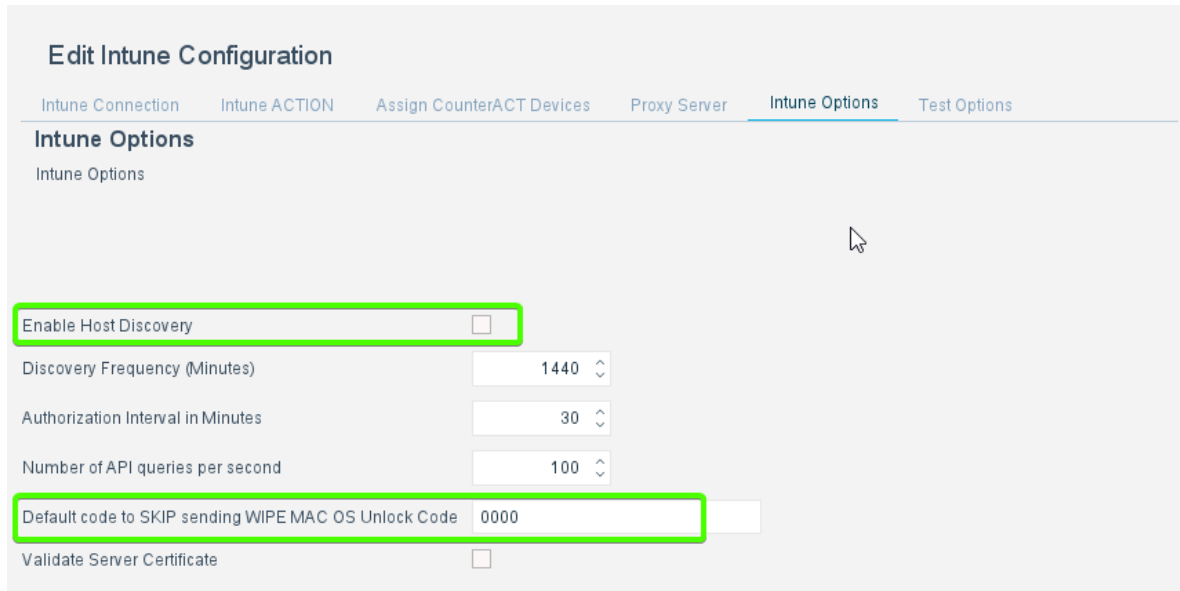
Proxy Server Password

Verify Proxy Server Password

Enter the Proxy Server information similar to any Forescout Extend Module:

Select **Next**.

Intune Options



Edit Intune Configuration

Intune Connection Intune ACTION Assign CounterACT Devices Proxy Server **Intune Options** Test Options

Intune Options

Intune Options

Enable Host Discovery ☐

Discovery Frequency (Minutes) 1440 ^ v

Authorization Interval in Minutes 30 ^ v

Number of API queries per second 100 ^ v

Default code to SKIP sending WIPE MAC OS Unlock Code 0000

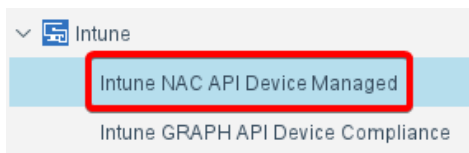
Validate Server Certificate ☐

- Enable Host Discovery: Select this option to enable the **Discovery Frequency** field.

Note : "Host Discovery" is not a requirement now.

The policy "Intune NAC API Device Managed"

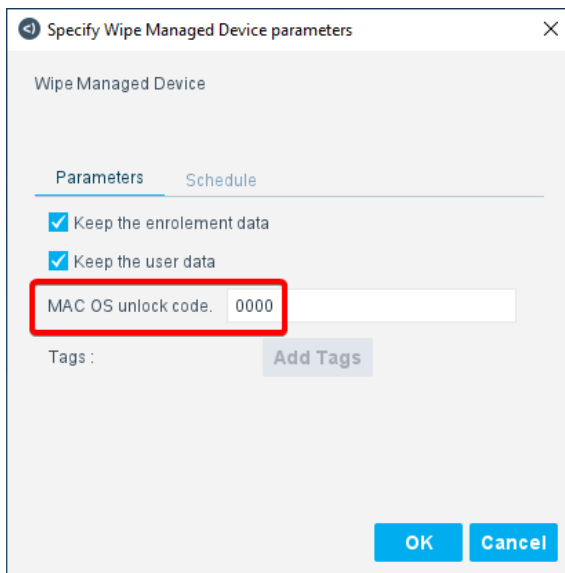
This policy can be used to resolve devices dynamically coming onto the network.



- Discovery Frequency: Select a value for the frequency of host discovery, which is the interval between discoveries. The range is from 1 minute to 2880 minutes. The default is 1440 minutes.
- Authorization interval in Minutes: This value controls the various **bearer** tokens to be refresh.
- Number of API queries per unit time: Select a value for the rate limiter. The range is from 1 to 100 requests per second. The default is 1 request per second. You can rate limit the requests sent to the third-party server. The rate limiter specifies the number of times a script is invoked during the specified time. It is triggered when the app starts.
- Default code to SKIP sending the WIPE MAC OS Unlock code.

MAC OS's can have an optional parameter, unlock code.

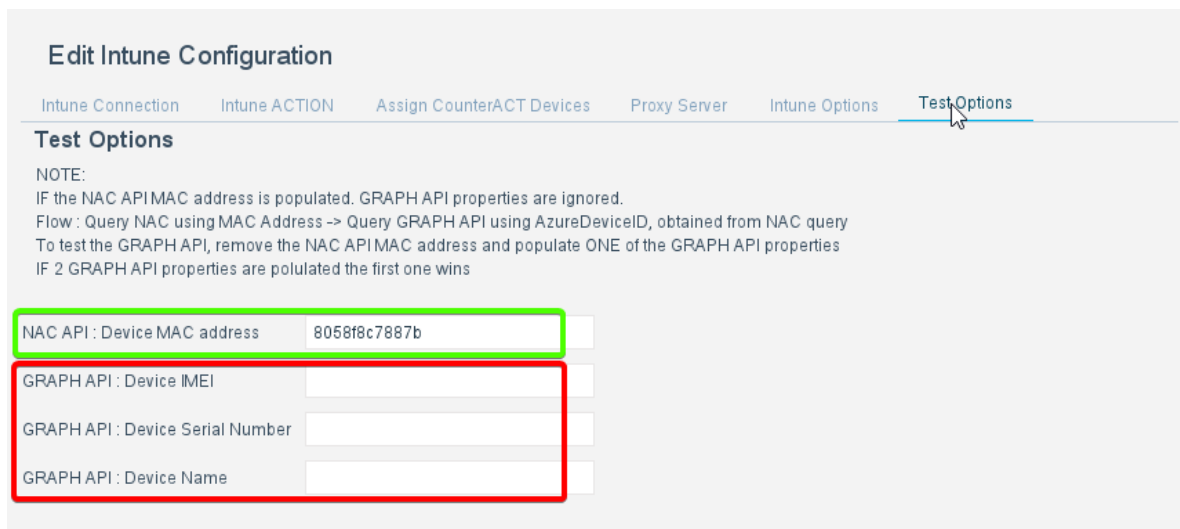
Action parameters can not be empty or null. For this reason, the unlock code has a value of "0000".



When this value is "0000", the unlock code parameter will not be sent.

This value can be changed in "Intune Options"

Test Options



- NAC API: Device MAC address. Query by MAC address. **The GRAPH API properties ignored.**

Query Flow

- NAC API query by MAC address
 - If enrolled (Is Managed)

- GRAPH API query by Azure Device ID
- GRAPH API properties
 - GRAPH API: Device IMEI
 - GRAPH API: Device Serial Number
 - GRAPH API: Device Name

To test the GRAPH only API query, remove the NAC address from the NAC API property

Note only the first property containing a value is queried.

Example

Device IMEI, Device Serial Number, Device Name all have values. - The GRAPH API query will use the Device IMEI

Device Serial Number, Device Name - The GRAPH API query will use the Device Serial Number

Select **Finish**

The configured system description is displayed in the **System Description** dialog box. When the system description is selected, all the buttons on the dialog box are enabled.

To add another system description, select **Add** and repeat the procedure for Add a System Description.

Select **OK** to save the system description to the CounterACT Appliance. The system description is displayed in the App Configuration tab of the **Connect** pane. There are several default columns. See Connect Pane Details.

Edit a System Description

You can edit an existing system description for the Intune App.

To edit a system description:

Select an existing system description and select **Edit**.

There are tabs for each pane. You can edit the settings in the Intune Connection, Assign CounterACT Devices, Proxy Server, and Intune Options tabs.

Select **OK** to save the system description edits to the CounterACT Appliance.

Remove a System Description

You can remove an existing system description.

To remove a system description:

Select An existing system description **Remove**. A confirmation is displayed.

More for details or **Ok**.

Test a System Description

You can test a system description, which tests the connection of the Intune APP to the Intune server. The app must be in the Running state.

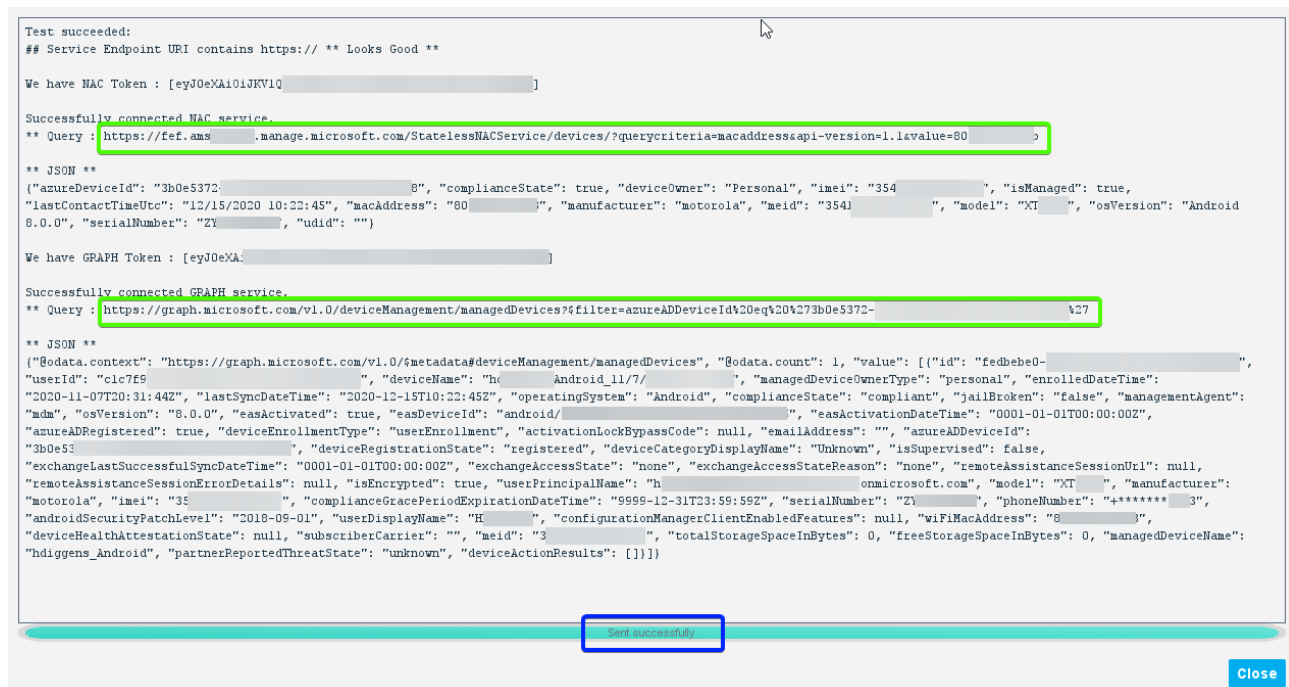
Also, the app must be saved before selecting **Test**. Select **OK** in the **System Description** dialog box and then select **Apply** in the **Connect** pane to save the system description. Please wait about 5-10 seconds after clicking apply.

To test a system description:

Select an existing system description Select **Test**.

If the connectivity of the system description has been tested successfully, a success message is displayed at the top of the dialog box. If the test failed, a failure message is displayed with a reason.

Close.



Configure Intune Policy Templates

There are two Intune policy templates for customers to manage devices in an Intune environment, detect devices that are compliant or non-compliant, and devices that are enrolled or not.

- Intune NAC API Device Managed
 - If you are not using polling and want to dynamically manage device entering the network. Use this policy for initial discovery.
- Intune GRAPH API Device Compliance
 - This policy will require NAC API policy. Dependent on group "Intune Device"
 - Device Jailbroken
 - Device out of compliance
 - Compliant

Intune Properties

Intune properties are available to be used in a policy.

The following properties are available:

GRAPH

- **Intune Device AAD ID:** Indicates the unique identifier (read-only) for the Azure Active Directory (AAD) device.
- **Intune Device Compliance State:** Indicates 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
 - Unknown.
- **Intune Device Enrolled DateTime:** Indicates the date and time when the device was enrolled.
- **Intune Environment TAG :** PUBLIC or US-GOVERNMENT

- **Intune Device ID:** Indicates the unique identifier of the device.
- **Intune Device is Jail Broken:** Indicates whether a device is jailbroken. The possible values are:
 - False
 - True
 - Unknown.
- **Intune Device is Registered in AAD:** Indicates whether the device is registered in the AAD.
- **Intune Device is Supervised:** Indicates the supervised status of the device.
- **Intune Last Sync DateTime:** Indicates the date and time when the device last completed a successful synchronization with Intune.
- **Intune Device Manufacturer:** Indicates the manufacturer of the device.
- **Intune Device Model:** Indicates the model of the device.
- **Intune Device Name:** Indicates the name of the device.
- **Intune Device Operating System:** Indicates the operating system of the device, such as Windows or iOS.
- **Intune Device Operating System Version:** Indicates the operating system version of the device.
- **Intune Device Reported Threat State:** Indicates 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
 - Unresponsive.
- **Intune Device Serial Number:** Indicates the serial number of the device.
- **Intune Directory ID:** Indicates the directory ID of the source Intune account.

- **Intune Managed Device Owner Type:**
- **Intune Device Wi-Fi MAC:** Indicates the Wi-Fi MAC address of the device.
- **Intune IMEI:** Indicates the International Mobile Equipment Identity (IMEI), which is a unique number that identifies all mobile phones and smart phones.
- **Intune MEID:** Indicates the mobile equipment identifier (MEID), which is a unique number that identifies a mobile device.
- **Intune Device Email Address:** Indicates one or more email addresses for the user associated with the device.
- **Intune Device Phone Number:** Indicates the phone number of the device.
- **Intune Device User Display Name:** Indicates the user display name of the device.
- **Intune Device User ID:** Indicates the unique identifier of the user associated with the device.

NAC

- **Intune NAC Azure Device ID :** The Azure device ID
- **Intune NAC Device Compliance Status :** True or False
- **Intune NAC Device Owner :**
- **Intune NAC Device IMEI :**
- **Intune NAC Device Is Managed :** True or False
- **Intune NAC Device Last Connect Time :** UTC Format
- **Intune NAC Environment TAG :** PUBLIC or US-GOVERNMENT
- **Intune NAC Device MAC Address :**
- **Intune NAC Device Manufacturer :**
- **Intune NAC Device MEID :**
- **Intune NAC Device Model :**
- **Intune NAC Device OS Version :**
- **Intune NAC Device Serial Number :**
- **Intune NAC Device UDID :** Maybe be blank

Intune Actions

Intune actions are available to be used in a policy.

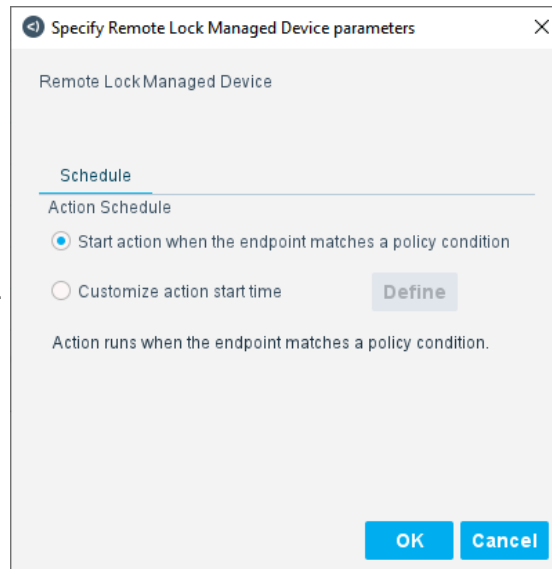
To access the Intune actions:

1. When configuring a policy, select **Add** in the Actions section of the Main Rule or Sub-Rule dialog box.
2. Search for Intune.
3. Select an action in the **Intune** folder.

The following action is available:

Remote Lock

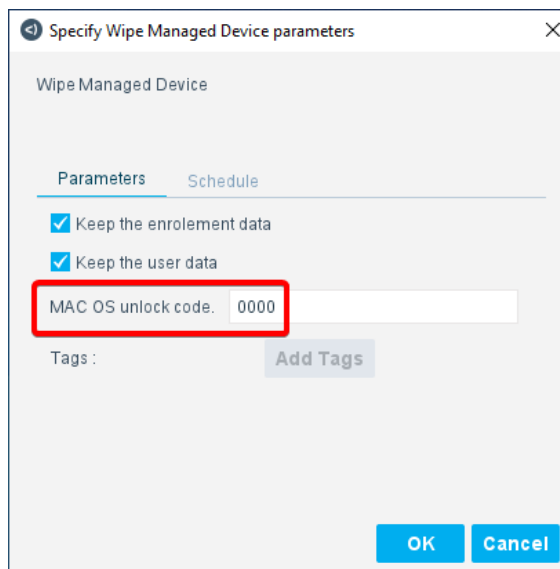
Locks a managed endpoint.



The dialog box is titled "Specify Remote Lock Managed Device parameters". It has a "Schedule" tab selected. Under "Action Schedule", the option "Start action when the endpoint matches a policy condition" is selected with a radio button. There is a "Define" button next to the "Customize action start time" option. Below the options, it says "Action runs when the endpoint matches a policy condition." At the bottom are "OK" and "Cancel" buttons.

Wipe Device

Factory resets a managed endpoint.



The dialog box is titled "Specify Wipe Managed Device parameters". It has two tabs: "Parameters" and "Schedule". The "Parameters" tab is selected. Under "Parameters", there are two checked checkboxes: "Keep the enrolment data" and "Keep the user data". Below these is a text field labeled "MAC OS unlock code." with the value "0000" entered. There is an "Add Tags" button. At the bottom are "OK" and "Cancel" buttons.

If the MAC OS unlock code is the same as defined in the "Intune Options" panel, this parameter will not be sent.

Scripts

There are a few Python scripts.

- **intune_poll.py** : Enable discovery on a specified period to poll endpoint properties.
- **intune_test.py** : Test the connection to the Intune server.
- **intune_resolve.py** : GRAPH API resolve query using Azure Device ID, obtained from " `intune_nac_resolve.py` " - **intuneremotelockmanageddevice.py** : Issue a request to the Intune server to lock a specific managed endpoint.
- **intunewipmanaged_device.py** : Issue a request to the Intune server to wipe a specific managed endpoint.
- **intune_authorization.py** : Fetch an Intune REST API authorization tokens for a specific interval.
- **intunenacresolve.py** : NAC API resolve query by MAC address, use to detect devices entering the network.

POSTMAN

See the Github for the collection "Forescout-Microsoft-NAC-Graph-Customer.postmancollection.json"
 You can use the POSTMAN collection.

- Discover the service endpoint URI.
- Help to debug issues with connecting to NAC and GRAPH API.

After importing the collection into POSTMAN, update the collection variables.

EDIT COLLECTION

Name: Forescout-Microsoft-NAC-Graph-Customer

Description Authorization Pre-request Scripts Tests **Variables**

These variables are specific to this collection and its requests. [Learn more about collection variables.](#)

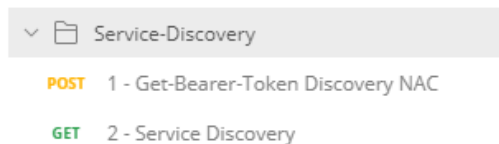
	VARIABLE	INITIAL VALUE ⓘ	CURRENT VALUE ⓘ	...	Persist All	Reset All
<input checked="" type="checkbox"/>	Bearer-Token-GRAPH					
<input checked="" type="checkbox"/>	APP-ID		63f89b			
<input checked="" type="checkbox"/>	APP-Secret		4VWY:			
<input checked="" type="checkbox"/>	Tenant-ID		b01e			
<input checked="" type="checkbox"/>	ServiceEndpoint-URI		https://fef.amsi...manage.microsoft.com/StatelessNACService			
<input checked="" type="checkbox"/>	Bearer-Token-NAC-Discov...		eyJ0eXAiOi...			
<input checked="" type="checkbox"/>	Bearer-Token-NAC-Device					
	Add a new variable					

For your environment update the :-

- APP-ID
- APP-Secret
- Tenant-ID

The remaining variables will be updated via the various REST examples.

Service Endpoint Discovery



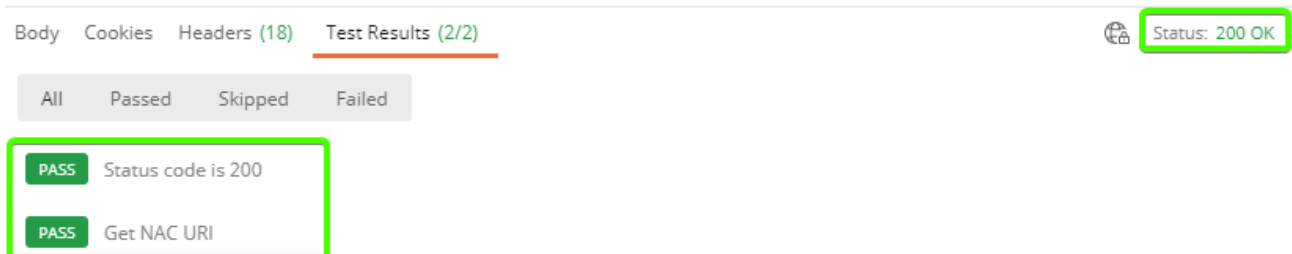
Select **1 - Get-Bearer-Token-Discovery NAC**

Select **SEND** button.

If the "Status 200 OK", this will update the collection variable "Bearer-Token-NAC-Discovery"

Select **2 - Service Discovery**

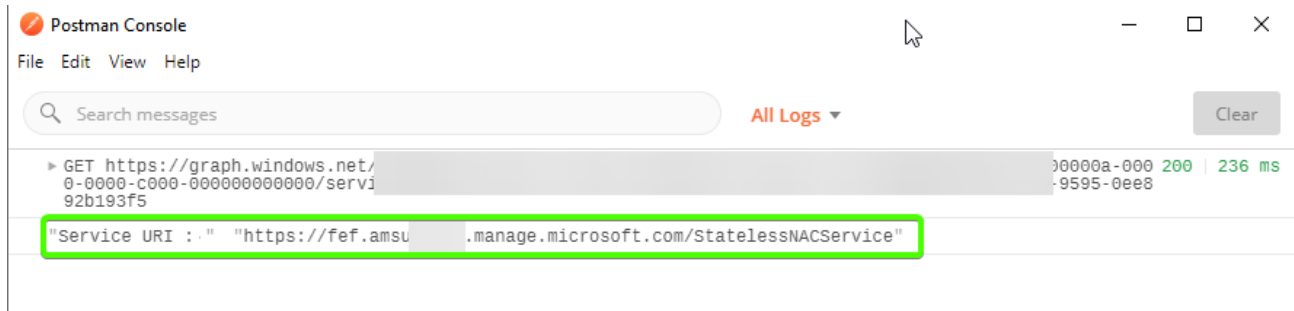
Select **SEND**



This will update the collection variable "ServiceEndpoint-URI"

From the POSTMAN main menu

Select **View/Show Postman Console**



This URI is **required** by "Intune Connection/NAC API: Service Endpoint URI"