About the Network Module

The Forescout® Network Module provides network connectivity, visibility, and control through the following plugin integrations:

- Centralized Network Controller Plugin
- Rogue Device Plugin
- Switch Plugin
- VPN Concentrator Plugin
- Wireless Plugin

The Network Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of Forescout.

The plugins listed above are installed and rolled back with the Network Module.

Refer to the relevant configuration guides for detailed information about how to work with and configure plugins included with this module. See Additional Forescout Documentation for information about how to access these guides, and other documentation.

Forescout Requirements

Minimum of Forescout version 8.1.

Components described in this document may have additional requirements and dependencies.

About This Release

This section describes updates and important information related to the components delivered in this version of the Network Module. This release also includes enhancements and fixes provided in previous releases.

The following table identifies the plugins that are updated in this module version:

Component	Requirements	Feature or Security Enhancements	Fixed Issues	Known Issues	Upgrade Considerations
Centralized Network Controller Plugin 1.1.3	✓	✓	✓		
Rogue Device Plugin 1.0.1					
Switch Plugin 8.13.4		✓	✓		✓
VPN Concentrator Plugin 4.2.2			✓		
Wireless Plugin 1.9.3		✓	✓		

Only components providing new features/enhancements are released with an updated configuration guide (help) that matches the updated version number of the component.

Centralized Network Controller Plugin 1.1.3

Forescout integrates its offering with the following Centralized Network Controller solutions:

- Cisco Application Centric Infrastructure
- Cisco Meraki Cloud-Managed Network

Cisco Application Centric Infrastructure

This section describes important information about the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco ACI software-defined networks. Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Requirements

This section describes requirements for this component.

- Network Requirements
- Third-Party Product Requirements

Network Requirements

Perform the following enterprise firewall configurations to support communication between Forescout and the Cisco ACI:

- Permit communication from the Connecting CounterACT Device(s) to the ACI Application Policy Infrastructure Controllers (APICs) on TCP/443 for the ACI fabrics that are being monitored by the Centralized Network Controller Plugin
- If a proxy server is required for use between Forescout and the ACI APICs, you must permit the proxy server to connect to the APICs on TCP/443

Third-Party Product Requirements

For a complete list of supported hardware and software, see the Forescout Compatibility Matrix.

The CNC Plugin supports Cisco ACI multi-pod and does not support ACI multi-site.

When planning for a single Connecting CounterACT Device to monitor multiple Cisco ACI fabrics, you must make sure to configure each of these fabrics with a unique name.

Authentication

The CNC Plugin requires read-only permissions on an account defined in APIC. This account can be authenticated using any of the following methods:

- Username and password
- TACACS+
- Active Directory

The plugin does not support:

- Username and password authentication with token
- Certificate-based authentication.

Endpoint Requirements

The CNC Plugin supports retrieval and display of information only for endpoints connected directly or indirectly to the ACI fabric and only for endpoints having a 1:1 MAC address-IP address assignment.

The plugin does not support visibility of endpoints that are using the same MAC address for multiple IP Addresses.

Discovery behavior of endpoints having the identical IP address, whether under the same tenant or under different tenants, is not predictable. The last/recent discovered endpoint could overwrite the information/properties of the endpoint having the identical IP address, which was previously discovered.

Feature Enhancements

There are no feature enhancements provided in this release of the Centralized Network Controller Plugin.

Security Enhancements

This release of the Centralized Network Controller Plugin includes updates that address security issues that are identified in, but not limited to, the following Common Vulnerabilities and Exposures (CVE):

Issue	CVE
CN-900	CVE-2018-12545 CVE-2019-10241 CVE-2019-10247 CVE-2019-10246

Merged Hotfixes

The following, previously released hotfixes are merged into this version Centralized Network Controller Plugin:

Hotfix	Fix Content	Up to Version
1.1.1.1	Refer to Hotfix 1.1.1.1 Release Notes	1.1.1.1073
1.1.2.1	Refer to Hotfix 1.1.2.1 Release Notes	1.1.2.1030

Known Issues

This section describes known issues for this version of the Centralized Network Controller Plugin and the plugin's integration with Cisco ACI software-defined networks.

Issue	Description
CN-67	The plugin does not currently support the Forescout platform's Failover Clustering functionality. However, the plugin does support the Forescout platform High Availability functionality.

Cisco Meraki Cloud-Managed Network

This section describes important information about the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco Meraki cloud-managed networks. Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Requirements

- It is recommended that the Centralized Network Controller (CNC) Plugin use received syslog events to detect endpoint connections/disconnections. For this plugin processing to take place, the following is required:
  - Core Extensions Module version 1.1 or above with the Syslog Plugin running
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Known Issues

This section describes known issues for this version of the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco Meraki cloud-managed networks.

Issue	Vendor	Description
CN-15	Cisco Meraki	When the plugin only uses periodic polling of the Meraki Dashboard to retrieve information about monitored Meraki networks, there is a supply delay of +/- a couple of minutes when retrieving information about new endpoint detections. This is Meraki limitation and not a Forescout one. Considering this delay, ForeScout recommends enabling the option **Use Events to Expedite Detection** to expedite plugin endpoint detection via its receipt of syslog events. ***Note***: With *wired-only* cloud-managed networks, even if the **Use Events to Expedite Detection** option is enabled, the plugin might still experience the supply delay.
CN-67		The plugin does not currently support the Forescout platform's Failover Clustering functionality. However, the plugin does support the Forescout platform High Availability functionality.
	Cisco Meraki	Meraki Dashboard does not report IPv6 addresses of connected endpoints to the Forescout platform (the Meraki Dashboard displays these addresses). Given this limitation, the Console only displays the MAC address of connected IPv6-only endpoints that the plugin discovers from Meraki.
CN-113	Cisco Meraki	There can be instances in which the Console cannot report endpoint online/offline in real-time. This issue most typically manifests itself in the following scenario: Endpoint is displayed as online but is actually offline.

Rogue Device Plugin 1.0.1

The solution monitors Forescout platform-managed switches to identify suspicious MAC spoofing events occurring to endpoints that are connected to these switches.

Requirements

This section describes requirements for this component.

Forescout Requirements

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Network Module Requirements

The following plugins and their version must be running in all your CounterACT devices:

- Rogue Device Plugin, version 1.0
- Switch Plugin, version 8.13 or above

Core Extensions Module Requirements

The following plugin and version are ***optionally*** running in all your CounterACT devices:

- DHCP Classifier Plugin, version 2.2 or above
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.

Endpoint Module Requirements

The following plugin and version are ***optionally*** running in all your CounterACT devices:

- HPS Inspection Engine, version 11.0 or above
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.
  - The Rogue Device Plugin requests the HPS Inspection Engine to verify, via Nmap query, the connection status of endpoints.

Feature Enhancements

There are no feature enhancements provided in this release of the Rogue Device Plugin.

Known Issues

This section describes known issues for this version of the Rogue Device Plugin.

Issue	Description
RGD-276	When all the following conditions are true, a small possibility exists that the RGD Plugin makes a false positive, MAC spoofing detection, based on changes in the character of the device: ▪ The Forescout packet engine is either not running or running, but not monitoring specific IP segment(s). ▪ The Flow Collector Plugin is running ▪ Network DHCP server(s) work with a small IP address pool that results in a high frequency of IP address re-allocations ▪ Plugin-managed Layer 3 switches are neither Juniper's nor Cisco's for which the plugin is configured to read the ARP table using CLI. ▪ The plugin's query rate of the ARP table of the managed Layer 3 switches is <= 60 seconds

Switch Plugin 8.13.4

This section describes important information about the Switch Plugin version 8.13.4

Requirements

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Feature Enhancements

This section describes the new features and/or feature enhancements for this release of the Switch Plugin.

Added Assign to VLAN via CLI for Alcatel switches

- Support for Assign to VLAN via CLI for Alcatel switches

Added Forescout eyeSight and eyeControl capabilities for Arista and Extreme X series switches

- Support for Arista switches
- Support for Extreme X-series switches

  VoIP detection is supported for phones connected to ports, where each port is configured with only one untagged VLAN for data traffic and only one tagged VLAN for voice traffic. The Switch Plugin classifies any port having more than one tagged VLAN as a trunk port, for which VoIP detection is not supported.

  PoE bounce on VoIP ports after an assign to VLAN action

  – The following criteria must be met:
    - The Extreme switch must be running XOS
    - The port must have been identified as a VoIP port by the Switch plugin
    - *cli_voip_port_bounce_poe:on* must be added via **Options**>**Switch**>Extreme switch entry>**Edit**>**Permissions**>**Advanced**>**Switch Advanced Settings**>**Configuration flags**.

Added PoE Support and PoE properties resolution for Arista 720 XP

The following basic switch properties are now supported for the Arista 720 XP:

- Switch Port PoE Connected Device
- Switch Port PoE Power Consumption

Added Forescout eyeSight and eyeControl capabilities for the D-Link DGS-1210 switch.

- Support for the SNMP MIB of DGS-1210 functionalities

Switch Port PoE Power ConsumptionAdded Forescout eyeSight and eyeControl capabilities for Moxa (EDS-510A) Switch

- Support for the Moxa (EDS-510A) switch via SNMP

Added Provision VLAN Action

Use the *Provision VLAN* action to assign a connected endpoint to a specific VLAN. The *Provision VLAN* action differs from the *Assign to VLAN* action in the following ways:

- The action's VLAN assignment is permanent; the action changes the VLAN configuration on the switch and does not revert the VLAN assignment.
- Once the plugin applies the action on a connected endpoint, the plugin does not monitor the status of the endpoint; this means that if the endpoint moves to another switch port, the action is not then applied on the endpoint now connected to that other port.
- The applied action cannot be canceled
- If action application fails, the plugin does not re-attempt to apply the action

Added Forescout eyeSight and eyeControl capabilities for VoIP detection

For network environments that include VoIP, the Switch Plugin now provides the following Forescout eyeSight and eyeControl capabilities:

- VoIP detection – detection of connected VoIP endpoints and detection of non-VoIP endpoints that are connected to a connected VoIP endpoint.

Fixed Issues

This section identifies the fixed issues for this version of the Switch Plugin.

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Switch Plugin:

Hotfix	Fix Content	Up to Version
8.11.3.3	Refer to Hotfix 8.11.3.3 Release Notes	8.11.3.3230
8.12.2.2	Refer to Hotfix 8.12.2.2 Release Notes	8.12.2.2594
8.13.2.1	Refer to Hotfix 8.13.2.1 Release Notes	8.13.2.1393
8.13.3.1	Refer to Hotfix 8.13.3.1 Release Notes	8.13.3.1386

Known Issues

This section describes known issues for this version of the Switch Plugin.

Issue	Vendor	Description
SW-4622	H3C	When the Switch Plugin only uses SNMP to manage an H3C S3100-16TP-PWR-EI switch running Hangzhou H3C Comware Platform Software Version 3.10, the *Assign to VLAN* action always fails with the following error message: *Cannot perform the VLAN assignment: The switch port* {port number} *properties were changed by an external source.* ***Workaround:*** To apply the *Assign to VLAN* action, configure the plugin to manage the H3C switch using both CLI and SNMP. Note: Ignore the plugin configuration test step *Assign to VLAN* failure message.
SW-3010		When the plugin is configured with the fully qualified domain name (FQDN) of the managed switch, a switch IP address change might cause plugin management of the switch, using SNMP, to fail. ***Workaround***: If you experience this known issue, restart the Switch Plugin.

Issue	Vendor	Description
SW-190270304	Cisco	While the Switch Plugin is running, if the Forescout user disables the **Enable ACL** option (the option checkbox is cleared) and then saves the updated Switch Plugin configuration, the Switch Plugin does not cancel the ACL rules and port restrictions that it applied on the managed Cisco switch, as a result of ACL actions (*Access Port ACL*, *Endpoint Address ACL*). This issue has the following operational impact: ▪ Affected endpoints remain restricted, even when these endpoints no longer match policy conditions that resulted in the application of ACL actions. The plugin cannot cancel the ACL restrictions. It is ***recommended*** to first stop the Switch Plugin, prior to disabling the **Enable ACL** option (as part of stopping, the plugin removes ACL rules that it applied on managed switches). ***Workaround***: If you experience this known issue, use the Clear ACLs capability to manually clear ACLs from a managed switch. For the procedure to clear ACLs, reference section *Clear ACLs from All Switch Ports* in the *Forescout Network Module: Switch Plugin Configuration Guide*.

Upgrade Considerations

This section describes upgrade considerations for this release.

Use CLI for Brocade and Dell IPv4 Switches Being Managed

After upgrading the Switch Plugin to 8.13.4

- From a plugin version ***below*** 8.11.0 for managed Brocade IPv4 switches

  or

- From a plugin version ***below*** 8.12.0 for managed Dell IPv4 switches

then, during your first edit of the plugin configuration for these managed switches, the Console requires you to enable the **Use CLI** option.

Track to issues SW-1583, SW-2912

VPN Concentrator Plugin 4.2.2

This section describes important information about the VPN Concentrator Plugin version 4.2.2

Requirements

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Fixed Issues

This section identifies the fixed issues for this version of the VPN Concentrator Plugin.

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the VPN Concentrator Plugin:

Hotfix	Fix Content	Up to Version
4.0.9.1	Refer to Hotfix 4.0.9.1 Release Notes	4.0.9.1003
4.1.1.2	Refer to Hotfix 4.1.1.2 Release Notes	4.1.1.2007
4.2.1.1	Refer to Hotfix 4.2.1.1 Release Notes	4.2.1.1008
4.2.2.1	Refer to Hotfix 4.2.2.1 Release Notes	4.2.2.1003

Wireless Plugin 1.9.3

This section describes important information about the Wireless Plugin version 1.9.3. Requirements

This section describes requirements for this component.

Forescout Requirements

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.
- In order for Wireless Plugin *IP address range* to enable Forescout RADIUS-based management of wireless clients, the Authentication Module version 1.1 or above with the RADIUS Plugin running is required.

Networking Requirements

Network connectivity between the Forescout Appliance and a WLAN device is required for plugin management of the WLAN device.

Feature Enhancements

This section describes the new features and/or feature enhancements for this release of the Wireless Plugin.

Added visibility for HP 830 WLC

Added support for Forescout eyeSight capabilities to detect and report the HP 830 Controller WLAN functioning in the network and on endpoints.

Added visibility for Cisco 9800 Controllers

Added support for Forescout eyeSight capabilities to detect and report the Cisco 9800 Controller functioning in the network and on endpoints.

Added WLAN Client VLAN support for Motorola/Extreme WLCs

Added support for the WLAN Client VLAN property on endpoints connected to Motorola/Extreme WLCs for both CLI and SNMP read methods.

Fixed Issues

This section identifies the fixed issues for this version of the Wireless Plugin.

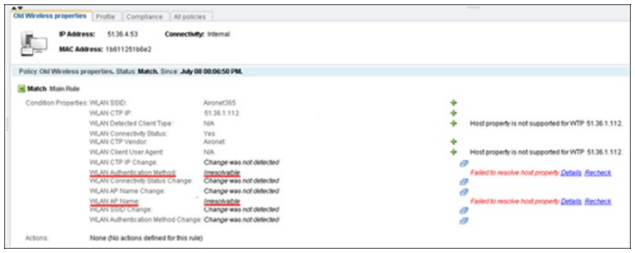
Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Wireless Plugin:

Hotfix	Fix Content	Up to Version
1.7.3.2	Refer to Hotfix 1.7.3.2 Release Notes	1.7.3.2014
1.8.2.2	Refer to Hotfix 1.8.2.2 Release Notes	1.8.2.2047
1.9.1.1	Refer to Hotfix 1.9.1.1 Release Notes	1.9.1.1033
1.9.2.1	Refer to Hotfix 1.9.2.1 Release Notes	1.9.2.1082

Known Issues

This section describes known issues for this version of the Wireless Plugin.

Issue	Vendor	Description
WRL-45672417	Motorola	Whenever the Wireless Plugin is started, it queries the managed WLAN device for some basic information about the device itself, including operating system (OS), location and number of connected wireless clients. With a managed Motorola WLAN device running the WiNG 5.8 OS, the plugin query fails to retrieve the location information of the WLAN device. As a result, in the Console Wireless pane, the **Location** column entry of the managed Motorola WLAN device remains empty.
63473	Cisco Aironet	When the plugin's configured Read method for a managed Cisco Aironet access point is CLI, the plugin does not resolve the properties **WLAN AP Name** and **WLAN Authentication Method** for detected endpoints connected to the access point. The Home tab's Detections pane lists these properties as *Irresolvable*. 

Upgrading the Module

New module releases may become available between Forescout releases. This section describes how to install the module when a new release becomes available.

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Flexx Licensing Mode***

   To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the module `.fpi` file.
3. Save the 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.

Module and Component Rollback

The following rollback/upgrade activities are not supported:

- Rolling back this module (or one of its components) to a version released prior to Forescout 8.1.
- If you are running a version of Forescout lower than 8.1 with the corresponding version of this module installed, you cannot upgrade to this module version (or one of its components).

If you upgrade to a newer module or component version that becomes available after this release, you may be able to roll it back. When rollback is supported, the Rollback button is enabled in the Console.

Modules/components on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules/components on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

To roll back the module or component:

1. Select **Options** from the Console **Tools** menu.
2. Navigate to the **Modules** folder.
3. In the Modules pane, select the module or component to be rolled back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and select **OK**. A dialog box opens showing you the rollback progress.

Previous Module Versions

Installing this module version also installs fixes and enhancements provided in the previous module versions listed in this section. To view Release Notes for previous module versions, see:

https://updates.forescout.com/support/files/plugins/network_discovery/1.1.3/1.1.3-5/RN.pdf

https://www.forescout.com/company/resources/network-module--release-notes-1-1-2/

https://www.forescout.com/company/resources/network-module-1-1-1-release-notes/

https://www.forescout.com/company/resources/network-module-1-1-release-notes/

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-05-14 14:22