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

This module requires Forescout version 8.1.1

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

About This Release

This section describes updates and important information related to components delivered in this version of the Network Module.

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

This release also includes enhancements and fixes provided in previous releases.

Centralized Network Controller Plugin 1.1

With this plugin version, Forescout integrates its offering with the following centralized network controller solutions:

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

Cisco Application Centric Infrastructure

The Forescout platform integrates with a wide range of different data center and cloud platforms to enable operational visibility. Cisco ACI software-defined networking architecture is the last addition data center specific integration. By discovery of ACI connected entities and the associated physical connections and logical networking overlays, the CNC Plugin provides enterprise IT greater data center visibility. This includes context, from basic virtual machine operating system properties to the more advanced services notes and ACI VMM properties for VMware.

The CNC Plugin integration with Cisco ACI software-defined networking architecture, together with the Switch Plugin, expand the Forescout platform's ability to recognize endpoints in different ACI network configurations. For example, CNC Plugin monitoring an ACI fabric for IP address, tenant and endpoint group info, while the Switch Plugin manages downstream L2 switches and obtains their MAC address.

Regarding the ACI networking deployment model (L2 or L3), the Forescout platform gathers a range of operational context directly from the Application Policy Infrastructure Controller (APIC) managing the ACI fabric ESXi hosts. This includes the option to collect context from multiple ACI fabrics.

Visibility use cases include:

- Full data center visibility: CNC Plugin supplies information about all ACI fabric-connected endpoints regardless of networking environment (upstream L3 switch connected to ACI, vSphere integrated with ACI via VMM, ACI endpoints connected to downstream L2 switch)
- Update ServiceNow's CMDB:
  - With new ACI fabric-connected endpoints as they become active
  - With state changes to existing ACI fabric-connected endpoints and the associated tenant, endpoint group and node name, in support of enterprise asset intelligence.
- CNC Plugin supplies information about all ACI fabric-connected endpoints associated with a specific tenant or endpoint group. Then, based on the criticality of these services, run different assessment policies to ensure compliance.

In network environments in which a Switch Plugin-managed switch is connected, as a downstream L2 switch, to an ACI leaf switch, the Switch Plugin resolves the managed switch properties of the connected endpoint and the CNC Plugin resolves the monitored ACI fabric properties of the connected endpoint.

Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Plugin Configuration Highlights

- In the General pane, the **Vendor** field drop-down menu offers you the following options from which to choose:
  - *Cisco ACI*
  - *Cisco Meraki*

  *In the General pane's **Connecting CounterACT Device** field, you can only configure an Enterprise Manager/Appliance as the Connecting CounterACT Device for a single, supported vendor, this being either Cisco ACI or Cisco Meraki.*

- In the Communication pane, configure the login information that the plugin requires in order to access and retrieve information from the Application Policy Infrastructure Controllers (APICs) that manage the ACI fabric.

  When multiple APICs manage the ACI fabric, it is not necessary to provide the IP address/FQDN of all the APICs managing the ACI fabric. Using the entered APIC IP address/FQDN, the Forescout platform discovers/retrieves the IP address of all the APICs that are managing the plugin-monitored ACI fabric.

  Configure plugin ACI fabric monitoring, using any of the following Connecting CounterACT Device assignments:
  - Per Connecting CounterACT Device, a single ACI fabric
  - Per Connecting CounterACT Device, multiple ACI fabrics (each fabric is uniquely named)
  - Multiple Connecting CounterACT Devices, each assigned the same ACI fabric, where:
    - The plugin monitors a mutually exclusive set of tenant groups (load balance plugin processing)
- In the Proxy Server pane, after defining/not defining a proxy server, selecting **Next** triggers the plugin to retrieve from one of the APICs, specified in the **Controller IP/Name** field of the Communications pane, the list of all the tenant groups of the ACI fabric.
- In the Tenants pane, select the ACI tenant groups that the plugin monitors when querying an APIC managing the ACI fabric. The plugin requests information about connected endpoints that belong to the selected tenant groups.
- In the Performance Tuning pane, configure performance-related settings and options that affect plugin processing.

Plugin Information Gathering Methods

The plugin uses REST API to periodically poll the APIC and retrieve information about endpoints, tenants, leaf switch ports and fabric nodes. You can also manually initiate plugin polling by selecting the **Poll** button that is provided in the Controllers tab of the Centralized Network Controller pane.

The plugin also uses the WebSocket notification mechanism to receive information updates about ACI fabric information (endpoint and other APIC-managed object information). The plugin subscribes to the APIC to receive its WebSocket

notifications. This method expedites plugin ability to provide updated ACI fabric endpoint visibility

Property Resolution

The CNC Plugin resolves information for the following properties, per plugin-monitored ACI fabric:

- **Application Profile**
- **Endpoint Group**
- **Endpoint VM Name**
- **Endpoint VMM Controller Name**
- **Endpoint VMM Hypervisor Name**
- **Fabric Domain**
- **Fabric ID**
- **FEX ID**
- **FEX Port**
- **IPv4 Address**
- **IPv6 Address**
- **Leaf Switch Port VLAN**
- **Leaf Switch Port VXLAN**
- **Leaf Switch Port**
- **Leaf Switch Port Description**
- **Life Cycle Control**
- **Node Fabric IP Address**
- **Node ID**
- **Node Name**
- **Node Serial Number**
- **Node Uptime**
- **Node VTEP Address**
- **Node VTEP IP Pool**
- **Pod ID**
- **Role**
- **Tenant Group**
- **VMM Path Group**

In the Forescout Console, find these properties in the **Cisco ACI** property group.

Console Information Displays

The CNC Plugin updates an endpoint's status, based solely on notification it receives from the APIC(s) of the monitored ACI fabric and not based on Forescout platform timers. For example, if the ACI fabric considers an endpoint no longer connected, the managing APIC notifies the CNC Plugin of the endpoint's disconnection and, as a result, plugin deletes the endpoint from display in the Console.

The following Console information displays reflect plugin monitoring of ACI fabrics:

- The **Controllers** tab of the Centralized Network Controller pane – the following columns display information relevant to a plugin monitored ACI fabric:
  - **Connectivity Status**
  - **Vendor**
  - **Connecting CounterACT Device**
  - **Comment**
  - **Controller IP/Name**

  Information presented in the Networks tab of the Centralized Network Controller pane is not relevant for Cisco ACI fabrics. Information presented in this tab is supplied by CNC Plugin monitoring of Cisco Meraki cloud-managed networks.

- The **Devices** tab of the Centralized Network Controller pane - – the following columns display information relevant to a plugin monitored ACI fabric:
  - **Device Name**
  - **Type**
  - **Model**
  - **IP Address**
  - **Total Connected Endpoints**
  - **MAC Address**
  - **Member of Organization/Fabric**
  - **Network Vendor**
  - **Serial Number**
- The All Hosts pane in the **Home** tab display the nodes and connected endpoints that the plugin discovers, via its monitoring of an ACI fabric domain. For node entries [APIC, Leaf Switch, Service Node, Spine Switch], columns providing resolved ACI fabric property information display in the All Hosts pane.
- The **Asset Inventory** contains the new **Cisco ACI** group that provides the following views to group the display of connected endpoints discovered by the plugin in the monitored ACI fabric:
  - **Application Profile**
  - **Endpoint Group**
  - **Fabric Domain**
  - **FEX ID**

- **FEX Port**
- **Leaf Switch Port**
- (Leaf Switch Port) **VLAN ID**
- (Leaf Switch Port) **VxLAN ID**
- **Node ID**
- **Node Name**
- **Pod ID**
- **Role**
- **Tenant Group**
- **VMM Path Group**
- **VMM vCenter**

Known Issues

This section describes known issues for this release.

Issue	Vendor	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 ongoing integration with Cisco Meraki cloud-managed networks. Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Requirements

This section describes requirements for this component.

Forescout 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 with the Syslog Plugin running
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

Feature Enhancements

This section describes feature enhancements for this release.

Additional Meraki Network Devices Monitored

The CNC Plugin monitors the following, additional Meraki network devices:

- Security & SD WAN (model MX65W)
- Teleworker Gateway (models Z1 and Z3)

Plugin Configuration

- In the General pane, the **Vendor** field drop-down menu offers you the following options from which to choose:
  - *Cisco ACI*
  - *Cisco Meraki*

  *In the General pane's **Connecting CounterACT Device** field, you can only configure an Enterprise Manager/Appliance as the Connecting CounterACT Device for a single, supported vendor, this being either Cisco ACI or Cisco Meraki.*

- In the Performance Tuning pane, the following performance setting is now available:
  - **Query for group policies every <n> seconds** – Modify the frequency that the plugin queries the controller to retrieve the names of all the group policies defined per network.

Property Resolution

The CNC Plugin resolves information for the following, additional properties:

- In the **Cisco Meraki** property group:
  - **Assigned Meraki Policy**
  - **Network ID**
  - **Organization ID**
- In the **Track Changes** property group:
  - **Assigned Meraki Policy Change**

Action Control

The CNC Plugin provides the following actions to apply control on connected endpoints:

- *Assign Meraki Policy* – assigns the selected Meraki policy to the connected endpoint. Configure the action to use any one of the following Meraki policy options:
  - *Blocked* – no network access
  - *Whitelisted* - network access allowed
  - Group policy$_{1\text{-}n}$ – user defined group policies obtained from the Meraki Dashboard

  The plugin supports application of the *Assign Meraki Policy* action only on endpoints that are connected to any of the following Cisco Meraki cloud-managed, network devices:
  - Security & SD WAN
  - Teleworker Gateway
  - Wireless Access Point

- *Cancel Meraki Policy Assignment* – cancels the Meraki policy currently assigned to the connected endpoint

In the Forescout Console, find these actions in the **Restrict** action group.

Console Information Displays

The following Console information displays reflect the plugin feature enhancements provided in this release:

- The **Network** tab of the Centralized Network Controller pane – the **Network Type** column is affected as follows:
  - *Appliance* – new network type when the network makeup is exclusively Security & SD WAN and/or teleworker gateway
  - *Combined* – modified network type when the network makeup is any combination of Security & SD WAN, switch, teleworker gateway, wireless
- The **Devices** tab of the Centralized Network Controller pane - the **Type** column includes the following additional device types:
  - Security & SD WAN
  - Teleworker Gateway
- The All Hosts pane in the **Home** tab reports the following network device entries:
  - Security & SD WAN
  - Teleworker Gateway
- The **Asset Inventory** contains the new **Cisco Meraki** group that provides an additional view for resolved, Meraki-related properties:
  - **Assigned Meraki Policy** - use this view to group the display of detected endpoints to which the *Assign Meraki Policy* action is currently applied

Fixed Issues

For information about the following fixed issues from the recently released Centralized Network Controller Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 1.0.0.1:
  - CN-423
  - CN-439
  - CN-451
  - CN-486

  https://forescout.force.com/support/s/article/Centralized-Network-Controller-Plugin-HF-builds-1-0-0-1xxx

Known Issues

This section describes known issues for this release.

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. In light of 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-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.
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.
CN-167	Cisco Meraki	Configure an uplink switch's vacant ports as trunk ports, to prevent the following plugin reporting scenario from occurring: ▪ Plugin alternates between reporting detected endpoints as being connected to a downlink switch [switch IP address and access port information] and, then, reporting these detected endpoints as being connected to an uplink switch [switch IP address and trunk port information].
	Cisco Meraki	Meraki Dashboard does not report IPv6 addresses of connected endpoints to CounterACT (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.

Rogue Device Plugin 1.0

The Rogue Device Detection and Prevention solution addresses the following rogue device, network security problem:

- MAC Spoofing

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

The solution identifies these suspicious events regardless of whether the involved endpoints - the ***spoofing victim*** (legitimate endpoint) and the ***spoofing attacker*** (illegitimate endpoint) - are located on (connected to) the same managed switch or two different, managed switches. Monitoring is continuous. The solution also provides the operator/administrator with the option to take action.

With this solution, Forescout delivers the following value to customers:

- Ensure and demonstrate security compliance
- Reduce the risk of network disruption, due to security incidents/breaches

The solution offers two different methods by which it identifies suspicious MAC spoofing events. The operator/administrator of the Forescout platform, based on their security standards, can activate the use of a single method or both methods. The detection methods are as follows:

- **Detect MAC Address Appearances on Different Ports** – per endpoint connected to a Forescout platform-managed switch, the solution monitors the MAC address appearance at its specific switch location and tracks consecutive changes in/movements of the MAC address switch location. When a configured threshold of MAC address movements is reached within a pre-defined interval, the solution identifies a MAC spoofing event.
- **Detect Changes in Character of Device** - per endpoint connected to a Forescout platform-managed switch, the solution monitors a pre-defined set of fundamental, device properties for changes in their value. When a configured number of these properties experience a change in value within a pre-defined interval, the solution identifies a MAC spoofing event.

Refer to the *Forescout Network Module: Rogue Device Detection and Prevention How-to Guide* for details about this solution.

Requirements

Forescout Requirements

(Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

Network Module

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

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

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

Endpoint Module

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

- HPS Inspection Engine, version 11.0
  - 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.

Property Resolution

The Rogue Device Plugin resolves the following properties:

- **MAC Spoofing Suspected**. This property contains the following information sub-fields:
  - **Spoofing Attacker Network Device Address**
  - **Spoofing Attacker Network Device Port**
  - **Spoofing Victim Network Device Address**
  - **Spoofing Victim Network Device Port**
  - **Endpoint Identity**
  - **Spoofed MAC Address**
  - **Detection Method**
  - **Device Character Changes**
- **MAC Spoofing Suspected – Blocked Locations**

The plugin resolves the **MAC Spoofing Suspected** property upon detection, in your network, of each suspected MAC spoofing event. While the MAC spoofing event remains in effect, the plugin also periodically re-resolves this property.

The plugin resolves the **MAC Spoofing Suspected – Blocked Locations** property as part of its processing of the *Block Suspected MAC Spoofing* action.

In the Forescout Console, find these properties in the **Rogue Device** property group

Policy Evaluation

The Rogue Device Plugin provides the **MAC Spoofing Tracking** policy template. Use this template to create policies that deal with the endpoints involved in suspected MAC spoofing events.

Forescout MAC spoofing detection has the following policy requirements:

- A minimum of one, running (active) MAC Spoofing Tracking policy or an equivalent policy that resolves the **MAC Spoofing Suspected** property.
- ***Only endpoints that fall within the policy's defined scope are subject to MAC spoofing detection***. Therefore, for each MAC Spoofing Tracking policy or equivalent policy, make sure that you define its scope with the IP segments/IP address range(s) that you require the solution to track and detect.

Action Control

The Rogue Device Plugin provides the following actions to apply control on endpoints:

- *Block Suspected MAC Spoofing* - blocks the port of the managed switch to which the targeted endpoint (MAC address) is connected. As part of action processing, the plugin resolves the **MAC Spoofing Suspected - Blocked Locations** property.
- *Undo Rogue Device Block* – Cancels (removes) the block of the port of the managed switch to which the targeted endpoint (MAC address) is connected, which was previously applied using the *Block Suspected MAC Spoofing* action.

In the Forescout Console, find these actions in the **Restrict** action group.

Console Information Displays

In the All Hosts pane in the Console's **Home** tab, entries of connected endpoints that the Rogue Device Plugin determines their identity to be a **MAC Spoofing Attacker**, display the following distinguishing information:

- In the **MAC Address** column, the entry displays the unique, ***fake*** MAC address of the Spoofing Attacker, which the Forescout platform assigns to the endpoint.
- In the **Comment** column, the entry displays the following comment:

  Note: Detected spoofing attacker. Fake MAC address assigned by Forescout.

For a selected endpoint determined to be involved in a MAC spoofing event, MAC spoofing event information displays in the **Profile** tab.

> *When the Rogue Device Plugin identifies detected endpoints that are assigned to the **Ignored host identities** group (ongoing IP address changes) as a **MAC Spoofing Victim**, these endpoints have two, distinct victim entries, one per IP address, in the **Home** tab > **Views** >* <MAC spoofing policy name> *> **Detected Spoofing Victim** group.*

For each, detected MAC spoofing event, the Rogue Device Plugin creates an entry in the Console **Event Viewer** that contains event-specific information

Known Issues

This section describes known issues for this release.

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

Upgrade Considerations

This section describes upgrade considerations for this release.

No Automatic Upgrade of Beta Version Policy

- Customers working with a policy that was created using a 1.0.0 beta version of the MAC Spoofing policy template must upgrade to the current 1.0.0 version of the plugin and then, manually, re-create the policy. There is no automatic upgrade of an existing (1.0.0 beta version) MAC Spoofing policy.

Switch Plugin 8.13.1

This section describes important information about the Switch Plugin version 8.13.1

Requirements

This section describes requirements for this component.

Forescout requirements

- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

Feature Enhancements

This section describes feature enhancements for this release.

Rogue Device Detection and Prevention Support

The Switch Plugin works together with the Rogue Device Plugin to deliver Forescout's *Rogue Device Detection and Prevention* solution. For example, the plugin reports to the Rogue Device Plugin about endpoint MAC address appearances in managed switch locations, for processing of the *Block Suspected MAC Spoofing action,* the Rogue Device Plugin requests the Switch Plugin to either block or cancel the block of a managed switch's **<IP address>:<port>**. For detailed information, refer to the *Forescout Rogue Device Detection and Prevention How-to Guide*.

VoIP Support Expanded

Switch Plugin VoIP support has expanded to include Huawei switches. For this plugin support, the following, additional MIB is required for managed Huawei switches:

- .1.3.6.1.4.1.2011.5.25.42.3.1.2.32.1.2

Auto-Discovery Support Expanded

Switch Plugin auto-discovery is now supported for Huawei switches.

Read VRF ARP Table Support Expanded

The Switch Plugin can be enabled to read the VRF ARP table of managed Juniper switches.

Plugin Management of Layer 3 Devices Expanded

Plugin management of Layer 3 devices has expanded to include the Hirschmann Eagle Industrial firewall, which includes writing to the firewall's ARP table to clear redundant IP addresses to MAC address entries from the ARP table.

Global Option for Managed Switches Renamed

For the purposes of clarity and accuracy, the managed switch global option **Automatically install SecureConnector** is renamed as follows:

- **Install SecureConnector with Assign to VLAN (Windows only)**

Switch Property Available for Use in Vulnerability and Response Policies

The property **Switch Device Vendor and Type** is only available for use in/resolved by policies that are created using a Vulnerability and Response (VR) policy template. The property contains the vendor and the device type of a managed switch device. Examples: *Cisco* (switch) or *Cisco_ASA* (firewall).

New Event Viewer Messages Logged

The Switch Plugin now records messages in the Event Viewer log for the following scenarios:

- When the plugin re-initializes its CLI connection with a plugin-managed switch. This re-initialization occurs, by default, once every 24 hours.
- When the plugin aborts its CLI connection with a plugin-managed switch.
- When the plugin is stopped.

Track to issue SW-3313

Application of the Assign to VLAN Action for VoIP Clarified

In the Configuration Guide, the following clarification is added about plugin application of the *Assign to VLAN* action on detected endpoints connected behind a VoIP device:

> The plugin does apply the *Assign to VLAN* action on detected endpoints that are connected behind a VoIP device (a switch VoIP port with a connected VoIP phone and a PC connected to the VoIP phone), given that the following conditions are met:
>
> – The connected endpoint is either an OS X endpoint or a Windows endpoint
> – SecureConnector is installed on the endpoint, as follows:
> › For OS X endpoints, SecureConnector must be installed as ***permanent***
> › For Windows endpoints, SecureConnector can be installed as either ***permanent*** or ***dissolvable***
> – If SecureConnector is not installed on the endpoint, then the global option **Allow Assign to VLAN VoIP switch ports with no SecureConnector** must be enabled.

Fixed Issues

This section describes the fixed issues for the following Switch Plugin versions:

- 8.13.1 Fixed Issues
- 8.13 Fixed Issues

8.13.1 Fixed Issues

This section describes the fixed issues for Switch Plugin version 8.13.1.

Issue	Description
SW-4283 **SW-4346**	Firewall vendor Palo Alto uses a different method than other plugin-supported firewall vendors to calculate/track ARP table entry aging (minutes connected). The Switch Plugin did not accommodate for Palo Alto's different method and, therefore, reported incorrect endpoint connection times for managed Palo Alto firewalls.

8.13 Fixed Issues

This section describes the fixed issues for Switch Plugin version 8.13.

Issue	Description
SW-3351	When the plugin was configured for use of CLI with an incorrect privileged access password and the plugin was either started/re-started or the plugin configuration test was run, the plugin issued incorrect/duplicated auditing messages
SW-2335	The *Endpoint Address ACL* action's **IP ACL** blocking rule options are corrected to state the following IP address blocking capabilities: ▪ Block TCP traffic that is sent to the detected endpoint IP address ▪ Block TCP/UDP traffic that is sent from the detected endpoint IP address

For information about the following fixed issues from the recently released Switch Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 8.11.2.1:
  - SW-3426
  - SW-3444
  - SW-3468
  - SW-3491

  https://forescout.force.com/support/s/article/Switch-plugin-HF-builds-8-11-2-1xxx
- Hotfix 8.11.2.2:
  - SW-3635
  - SW-3760

  https://forescout.force.com/support/s/article/Switch-plugin-HF-builds-8-11-2-2xxx
- Hotfix 8.11.2.3:
  - SW-3803
  - SW-3824
  - SW-3831

  https://forescout.force.com/support/s/article/Switch-plugin-HF-builds-8-11-2-3xxx
- Hotfix 8.11.3.2:

  https://forescout.my.salesforce.com/kA00H0000010y2y

- Hotfix 8.12.2.1:

SW-3457	SW-3717	SW-3810	SW-3823
SW-3558	SW-3774	SW-3818	SW-3857
SW-3630	SW-3785	SW-3819	SW-3864
SW-3631		SW-3820	

  https://forescout.force.com/support/s/article/Switch-plugin-HF-builds-8-12-2-1xxx

- Hotfix 8.12.2.2:
  - SW-3779
  - SW-3814

  https://forescout.force.com/support/s/article/Switch-plugin-HF-builds-8-12-2-2xxx

Known Issues

This section describes known issues for this release.

Issue	Vendor	Description
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***: In the event that you experience this known issue, restart the Switch Plugin.
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***: In the event that 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 8.13.1 from -

- A version ***below*** 8.11.0 for Brocade IPv4 switches already managed
- A version ***below*** 8.12.0 for Dell IPv4 switches already managed

Then, during the first user edit of the plugin configuration for these managed switches, the Console requires the user to enable the **Use CLI** option for continued plugin management of these switches.

Track to issues SW-1583, SW-2912

VPN Concentrator Plugin 4.2

This section describes important information about the VPN Concentrator Plugin version 4.2.

Requirements

This section describes requirements for this component.

Forescout Requirements

- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

Supported VPN Devices

The VPN Concentrator Plugin supports the following server packages:

- Cisco VPN 3000 software version 4.1.5 or higher
- Cisco VPN ASA 5500 Series Adaptive Security Appliance
- Juniper 5.5R1 (build 11711) or higher
- Nortel V07_00.062 or higher

Supported Authentication Methods

- RADIUS
- Active Directory

Feature Enhancements

This section describes feature enhancements for this release.

Use TLSv1.2 Communication

The **TLSv1.2** checkbox is now available in the **Active Directory Authentication** pane. When configuring the plugin to use Active Directory authentication with a managed VPN device, select this checkbox option to instruct the plugin to communicate with the Active Directory server using TLSv1.2.

Track to issue VPN-133

Fixed Issues

For information about the following fixed issues from the recently released VPN Concentrator Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 4.1.1.1:
  - VPN-172

  https://forescout.force.com/support/s/article/VPN-Plugin-HF-builds-4-1-1-1xxx

Wireless Plugin 1.9

This section describes important information about the Wireless Plugin version 1.9.

Requirements

This section describes requirements for this component.

Forescout Requirements

- In order for Wireless Plugin *IP address range* to enable Forescout RADIUS-based management of wireless clients, the Authentication Module version 1.1 with the RADIUS Plugin running is required.

Networking Requirements

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

Fixed Issues

This section describes fixed issues for this release.

Issue	Vendor	Description
WRL-835		The Wireless Plugin was not reporting wireless clients (endpoints) as being offline, despite its receipt from the WLAN controller (WLC) of client removed trap notification, in the following scenario: ▪ The client connects and then disconnects within 600 seconds (10 minutes) and the WLAN controller deletes the entry from its online clients table. ▪ The Wireless Plugin queries the WLAN controller's online clients table every 600 seconds by default. When the client disconnects, the Wireless Plugin marked it offline. Then, within 10 minutes, that same client reconnected and then disconnected within 1 minute of reconnecting. The Wireless Plugin did not detect this type of rapid wireless client status change.
WRL-789	Cisco Aironet	With some, managed Access Points, the Wireless Plugin failed to retrieve the IP address of connected, wireless clients (endpoints) via SNMP

For information about the following fixed issues from the recently released Wireless Plugin hotfixes that are incorporated into this plugin version, refer to the following:

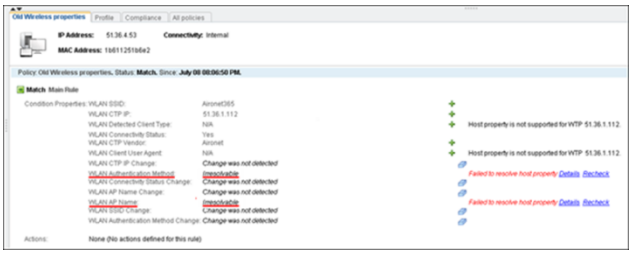
- Hotfix 1.8.2.1:
  - WRL-925
  - WRL-949

  https://forescout.force.com/support/s/article/Wireless-Plugin-HF-builds-1-8-2-1xxx

Known Issues

This section describes known issues for this release.

Issue	Vendor	Description
WRL-456 72417	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.

Issue	Vendor	Description
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 will not proceed if you do not agree to the license agreement.

   - *The installation will begin 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.
- Upgrading to this module (or one of its components) from a version released prior to Forescout 8.1.

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.

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, or 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 will 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.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

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

Plugin Help Files

- After the plugin is installed, 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 Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-05-21 12:33