FORESCOUT

Forescout

Platform and Base Modules

Release Notes

Interim Release 8.2.1

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

2020-07-31 14:08

Table of Contents

About This Release

Version 8.2.1 is a Forescout interim release. This is a new release type that includes feature content in addition to fixed issues that were previously delivered by Forescout platform maintenance releases. This interim release integrates Forescout platform version 8.2 with Forescout platform version 8.1.4 (the last maintenance release) and contains new features and feature enhancements that increase automation and improve usability.

New and enhanced features in Forescout interim release 8.2.1 include:

- Expanded overlapping IP address support to strengthen the handling of both the operational technology (OT) use case and the organization merger & acquisition (M & A) use case.
- Support for multi-home OSX endpoints running SecureConnector
- Enhanced RADIUS Plugin – provides customizable CoA options used in its *RADIUS Authorize* action for Arista, Cisco and other vendors' network devices.
- Support for automated vendor detection of managed L2/L3 switch devices for more accurate Switch Plugin configuration
- Support for Arista Cloud Vision centrally-managed network solutions, both wired and wireless
- The Forescout Limited Appliance mode for enabling on 5110 and CT-R series hardware devices
- Intra-Enterprise Manager and Appliance certificate authentication
- An array of Wireless Plugin feature enhancements that support various vendors' WLAN devices
- Compatibility with eyeExtend Connect 1.6.0; refer to the Forescout eyeExtend Connect Module 1.6.0 Release Notes

Forescout version 8.2.1 delivers New and Changed Features and Fixed Issues both for the core Forescout platform and for Modules Packaged with This Release.

Review information about Known Issues, including any provided workarounds, and Important Considerations for issues to consider before installing/upgrading to the new release.

Installing this release also installs features/fixes provided in Previous Releases. For additional information related to this release that is not included in this document, see Where to Go for More Information.

This version does not support rollback. Forescout interim release 8.2.1 does not support rollback. This means that after the upgrade of your Forescout deployment to 8.2.1, you cannot roll back to a previous release. Returning your Forescout deployment to a previous release would require performing a scratch (new) installation of that release. Therefore, Forescout recommends that you back up your system before performing the upgrade. You can use the *Restore* tool if you need to revert to your previous system settings.

Supported Upgrade Paths

For complete information about supported upgrade paths from earlier Forescout versions and detailed upgrade instructions for this version, including system requirements, refer to the Forescout Installation Guide.

For a complete list of supported models of physical Forescout Appliances and their compatible Forescout platform versions up to and including version 8.2.X, see the Hardware and Software Interoperability Matrix.

What's New in This Release

The following table identifies components that are updated in this release:

Module	Component	New and Changed Features	Fixed Issues	Known Issues
Forescout Platform 8.2.1		√	√	√
Authentication 1.2.1	RADIUS 4.5.1	√		√
	User Directory 6.5.1			√
Core Extensions 1.2.1	Advanced Tools Plugin 2.4.1			√
	CEF Plugin 2.8.2	√		
	Cloud Uploader 1.1.0			
	Dashboards Plugin 1.2.2			√
	Data Publisher 1.0			
	Data Receiver 1.0			
	Device Classification Engine 1.4.1			√
	Device Data Publisher 1.0.1			
	DHCP Classifier Plugin 2.3.1			
	DNS Client Plugin 3.2.2			
	DNS Enforce Plugin 1.4.1	√		
	DNS Query Extension Plugin 1.3.1			
	External Classifier Plugin 2.3.1			
	Flow Analyzer Plugin 1.4.1			
	Flow Collector 1.1.1	√		
	IOC Scanner Plugin 2.4.1			√
	IoT Posture Assessment Engine 1.1.4			√
	NBT Scanner Plugin 3.2.1			
	Packet Engine 8.2.1			√

Module	Component	New and Changed Features	Fixed Issues	Known Issues
	Reports Plugin 5.2.1	√		√
	Syslog Plugin 3.6.1			√
	Technical Support Plugin 1.3.1			
	Web Client Plugin 1.2.1			
Endpoint 1.2.1	HPS Agent Manager 1.2.1			
	HPS Inspection Engine 11.1.1			√
	Hardware Inventory Plugin 1.2.1			
	Linux Plugin 1.5.1			√
	Microsoft SMS/SCCM Plugin 2.4.3			
	OS X Plugin 2.3.1	√		
Hybrid Cloud 2.1.1	Amazon Web Services Plugin 2.2.1			
	Azure Plugin 1.1			√
	VMware NSX Plugin 1.3.1			
	VMware vSphere Plugin 2.5.1	√		√
Network 1.2.1	Centralized Network Controller Plugin 1.2.1	√	√	√
	Network Controller Plugin 1.0.1	√		√
	Rogue Device Plugin 1.1.1	√		√
	Switch Plugin 8.14.2	√		√
	VPN Concentrator Plugin 4.3.1	√		
	Wireless Plugin 2.0.1	√		√

New and Changed Features

This section describes new and changed features in the Forescout platform and Base Modules.

Forescout Platform 8.2.1

This section describes new and changed features in the Forescout platform.

Addition of Security Enhancements

With this version, the Forescout platform incorporates additional security enhancements that ensure more robust platform security and, thereby, reduce an attacker's ability to impose damage and/or take control of platform processing.

Limited Appliance Mode for CT-R/5110 Hardware Devices

In version 8.2.1, Forescout introduces the Limited Appliance mode. Due to memory limitations, 5110 and CT-R series Appliances do not fully support version 8.2.1. For customers owning CT-R or 5110 hardware, the Limited Appliance mode is available to enable on these Forescout hardware devices. Enabling this mode provides a subset of Forescout plugins that run on the Appliance and provide Forescout eyeSight and eyeControl capabilities.

The Limited Appliance mode for version 8.2.1 provides the following plugins:

- DHCP Classifier
- DNS Client
- Device Classification Engine
- Device Profile Library
- HPS Agent Manager
- HPS Inspection Engine
- Hardware Inventory
- NIC Vendor DB
- Packet Engine
- Syslog
- Switch
- Wireless
- User Directory

For more information about Limited Appliance mode, refer to the Forescout Installation Guide.

Inter-Enterprise Manager and Appliance Authentication

The Forescout platform ensures secure communication between Enterprise Managers and Appliances through customer-issued CA certificates. Customers can generate certificate sign requests to a CA Service and import the signed certificate and its certificate chains for each Enterprise Manager and Appliance.

Disabled by default, certificate verification enforcement must be enabled using the **`fs.enforce.cert.verify`** property. Once enabled, the Forescout platform requires

signed certificates of both existing and future Enterprise Managers and Appliances. Before enabling verification, be sure to import signed certificates on each Enterprise Manager and Appliance. For details, refer to either the Forescout Administration Guide or the Forescout Installation Guide.

Authentication Module 1.2.1

This section describes new and changed features in the following components of the Authentication Module:

- RADIUS Plugin 4.5.1

RADIUS Plugin 4.5.1

This release contains the following new and changed features:

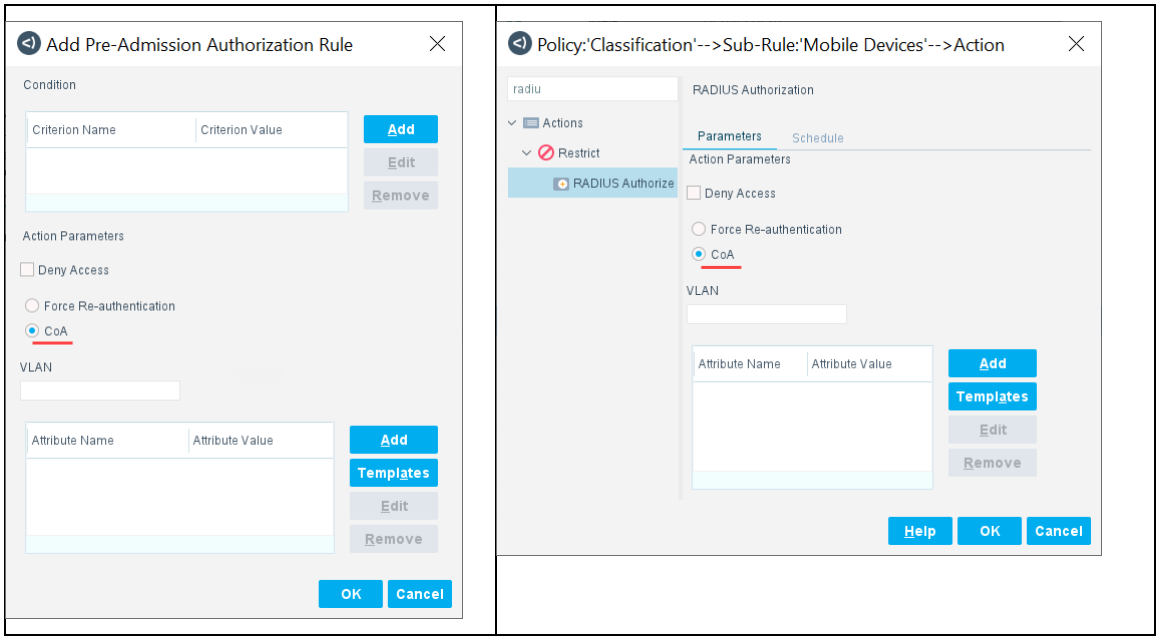
Change of Authorization (CoA) Without Session Disconnect

The RADIUS Plugin can now use CoA messages with all network devices.

Until this release, the RADIUS Plugin could not use CoA messages with network devices of non-Cisco vendors, including Arista and Juniper Mist. For endpoints managed through these devices, CoA required disconnection of existing sessions and re-authorization. With this release, the RADIUS Plugin supports CoA via devices of all vendors. The plugin can be used for role-based endpoint management, including MAB, while maintaining session stability and connectivity.

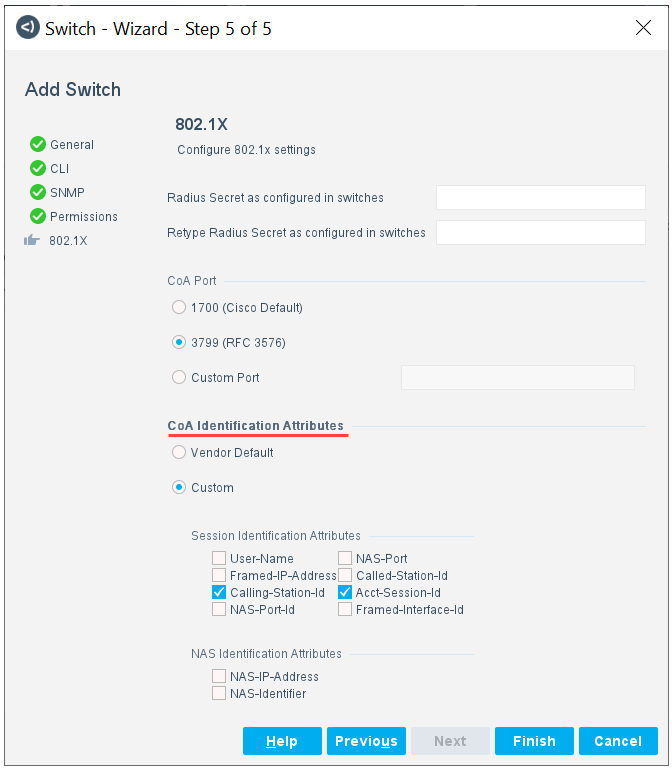
New options let you configure CoA behavior throughout the endpoint lifecycle:

- In Pre-admission Authorization rules
- In policy-based management with the *RADIUS Authorize* action



Use these options to impose a new authorization on endpoints without undesired bounce.

In addition, complementary new options in the Switch Plugin and the Wireless Plugin let you configure per-vendor defaults for session ID and other information used in CoA messages.



For details, refer to the *Forescout Authentication Module: RADIUS Plugin Configuration Guide* and the *802.1X Integration* section of the *Forescout Network Module: Switch Plugin Configuration Guide* and the *Forescout Network Module: Wireless Plugin Configuration Guide*.

Core Extensions Module 1.2.1

This section describes new and changed features in the following components of the Core Extensions Module:

- CEF Plugin 2.8.2
- DNS Enforce Plugin 1.4.1
- Flow Collector 1.1.1
- Reports Plugin 5.2.1

CEF Plugin 2.8.2

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The CEF Plugin supports working with networks that use overlapping IP addresses. When the Forescout platform is enabled to support overlapping IP addresses, the following Console areas of the plugin are affected:

- The *Assigned CounterACT Devices* pane/tab
- The *General* tab of the *Edit SIEM Server* window
- The *CEF* pane

The plugin provides the new CEF Event Field ID **`ird`** (CounterACT property tag **`area_code)`** that is always included in *Audit* action-generated *Compliant* and *Not Compliant* CEF messages.

For plugin details, refer to the *Forescout Network Module: CEF Configuration Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

DNS Enforce Plugin 1.4.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The DNS Enforce Plugin supports working with networks that use overlapping IP addresses. When the Forescout platform is enabled to support overlapping IP addresses, the following Console areas of the plugin are affected:

- The *Select Appliances* dialog. The dialog includes any Appliances in your Forescout deployment that are assigned to IP Reuse Domains (share overlapping IP addresses).

For plugin details, refer to the *Forescout Core Extensions Module: DNS Enforce Plugin Configuration Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Flow Collector 1.1.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The Flow Collector supports working with networks that use overlapping IP addresses. In order for the Flow Collector to support working with networks that use overlapping IP addresses, the following networking requirement must be fulfilled:

- For any given switch device in the enterprise's network, each connected endpoint must be assigned a different, unique IP address.

For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Reports Plugin 5.2.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The Reports Plugin supports reporting information about networks that use overlapping IP addresses. For example, when preparing a report, if the selected IP address segment is assigned an IP Reuse Domain (IRD), the plugin report includes only those network devices whose IPv4 address is located within that IP Reuse Domain (IRD).

For plugin details, refer to the *Forescout Core Extensions Module: Reports Plugin Configuration Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Endpoint Module 1.2.1

This section describes new and changed features in the following components of the Endpoint Module:

- OS X Plugin 2.3.1

OS X Plugin 2.3.1

This release contains the following feature enhancement:

Enhanced Support for Multi-Homed OSX Devices

To manage a device, SecureConnector always uses one network interface of the device.

When a device has multiple network interfaces (such as wired and wireless NICs), the Console lists each of these interfaces as a separate endpoint as they are detected – but only the endpoint corresponding to the interface used by SecureConnector is identified as *Managed by SecureConnector*. For this endpoint the **Manageable SecureConnector** property has the value *Yes*.

The other interfaces of the device are listed in the Console as endpoints *Not Managed by SecureConnector*. For these endpoints the **Manageable SecureConnector** property has the value *No*. This means that network access policies may apply restrictive actions to interfaces of a device that is managed by SecureConnector through another interface.

This release of the OS X Plugin provides the following tools to resolve multi-homed endpoints managed by SecureConnector:

- The new **Manageable SecureConnector via any interface** property can be used to identify the interfaces of a managed endpoint that are not used by SecureConnector. This property has the value *Yes* for *all* interfaces detected on a device managed by SecureConnector. Use this property in policies that handle unmanaged or multi-homed devices. To use this optional property, enable it when you configure the plugin.
- The new Multi Homed SecureConnector for OS X policy template provides basic logic to resolve multi-homed interfaces of endpoints managed by SecureConnector.
- When you view details for an interface of a multi-homed OS X endpoint managed by SecureConnector, the **Macintosh SecureConnector Connection ID** field shows a unique internal identifier used by the Forescout platform to track all interfaces of a single managed endpoint.

For details, refer to the *Forescout Endpoint Module: OS X Plugin Configuration Guide*.

Hybrid Cloud Module 2.1.1

This section describes new and changed features in the following components of the Hybrid Cloud Module:

- VMware vSphere Plugin 2.5.1

VMware vSphere Plugin 2.5.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The VMware vSphere Plugin supports working with networks that use overlapping IP addresses. When the Forescout platform is enabled to support overlapping IP addresses, you can configure the plugin to manage multiple VMware servers all having the same IP address, however for this to be valid, each of these VMware servers must be located within a different IP Reuse Domain (IRD).

The following Console areas of the plugin are affected:

- The *General* pane/tab
- The test results window
- The *VMware vSphere* pane

For plugin details, refer to the *Forescout Network Module: VMware vSphere Configuration Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Network Module 1.2.1

This section describes new and changed features in the following components of the Network Module:

Centralized Network Controller Plugin 1.2.1

This release contains the following new or enhanced features:

Additional Cisco ACI Properties

For Forescout Segmentation view (eyeSegment application) purposes, the Centralized Network Controller Plugin resolves the following three, additional Cisco ACI-related properties:

- Bridge Domain
- Bridge Domain Description
- Endpoint Group Description

Likewise, the *Cisco ACI* view in the *Asset Inventory* provides the above three ACI fabric-related grouping distinctions.

Additional Wireless Property for Cisco Meraki

The Centralized Network Controller Plugin resolves the following, wireless property for a Cisco Meraki cloud-managed network:

- WLAN SSID

and the plugin also resolves the associated wireless track changes property WLAN SSID Change.

Network Controller Plugin 1.0.1

This release contains the following new or enhanced features:

Added Plugin Support of Arista CloudVision Centrally-Managed Networks

Added support of plugin eyeSight and eyeControl capabilities for the following, centrally-managed network solutions:

- Arista CloudVision Wired (premise based)
- Arista CloudVision WiFi (cloud based)

Plugin support for the Arista CloudVision network solutions requires the Network Controller Content Plugin 1.0.1.

Rogue Device Plugin 1.1.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The Forescout rogue device detection and prevention solution, delivered by the Rogue Device Plugin in conjunction with the Switch Plugin, fully functions in networks that use overlapping IP addresses.

In support of overlapping IP addresses (OIP) and rogue device detection and prevention, the Switch Plugin, given specific network conditions, appends a UUID (a randomly generated, unique, hexadecimal number) to the IPv4 address of affected plugin-managed switches, in the format *<IPv4 address@UUID>*. By doing so, the RGDP can then effectively distinguish between the switch location of the connected spoofing attacker and the switch location of the connected spoofing victim. The modified switch IPv4 addresses affect two *sub-fields* of the MAC Spoofing Suspected property.

For plugin details, refer to the *Forescout Network Module: Rogue Device Detection and Prevention How-to Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Switch Plugin 8.14.2

This release contains the following new or enhanced features:

New Auto-Vendor Switch Definition Method

Previous releases of the Switch Plugin provided limited tools for bulk device configuration. This release introduces the first of several enhancements that automate definition and configuration of large numbers of switches.

Many of the Plugin's network device definition settings are vendor-specific. When the new **Add Auto-Vendor** option is used to define new switches, the Switch Plugin automatically resolves the vendor of each new device. This lets you add many switches of various vendors in a single action. You can then select similar devices of the same vendor and configure them in groups.

For details refer to the *Forescout Network Module: Switch Plugin Configuration Guide*.

New Configuration Options for RADIUS Change of Authentication (CoA) Messaging

RADIUS Plugin version 4.5.1 lets users apply the RADIUS CoA message through network devices of all vendors. The Switch Plugin supports this feature with new configuration options for 802.1X integration. See Change of Authorization (CoA) Without Session Disconnect.

Application of Access Port ACL on Arista Switches

When configuring the plugin to manage an Arista switch, the ACL pane/tab is now available and the Enable ACL option can be selected. When the plugin is enabled for

ACL, the plugin can apply its *Access Port ACL* action on targeted endpoints that are connected to a plugin-managed Arista switch. The plugin applies its *Access Port ACL* action using CLI.

Plugin application of its *Access Port ACL* action for managed Arista switches requires the Switch Content Plugin 1.1.0.

Process Juniper MAC Notification Traps

The Switch Plugin has added the processing of SNMP MAC notification traps that it receives from Juniper L2/L3 switches. This is in addition to the plugin already processing these traps sent from Cisco L2/L3 switches. The plugin uses these received traps to detect endpoints and network devices based on new MAC addresses. The plugin requires that the following MIB is present in the Juniper switches:

- .1.3.6.1.4.1.2636.3.48.1

Wireless Plugin 2.0.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The Wireless Plugin supports working with networks that use overlapping IP addresses. When the Forescout platform is enabled to support overlapping IP addresses, you can configure the plugin to manage multiple WLAN devices all having the same IP address, however for this to be valid, each of these WLAN devices must be located within a different IP Reuse Domain (IRD).

The following Console areas of the plugin are affected:

- The *General* pane/tab
- The *Configuration Test* dialog
- The *Wireless* pane

For plugin details, refer to the *Forescout Network Module: Wireless Plugin Configuration Guide*. For information about a network's use of overlapping IP addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

New Configuration Options for RADIUS Change of Authentication (CoA) Messaging

RADIUS Plugin version 4.5.1 lets users apply the RADIUS CoA message through network devices of all vendors. The Wireless Plugin supports this feature with new configuration options for 802.1X integration. See Change of Authorization (CoA) Without Session Disconnect.

Added Plugin Management of Huawei WLAN Controllers

Wireless Plugin management of a WLAN device is now supported for Huawei WLAN Controllers. To work with a Huawei WLAN Controller, the following configuration of the read/write settings in the WLAN device is required:

- SNMP read access to perform queries
- SSH or Telnet write access to apply the WLAN Block action on wireless clients

For a Huawei WLAN Controller, the Wireless Plugin requires that the following MIBs are present on the WLAN devices:

- 1.3.6.1.4.1.2011.6.139.18.1.2.1
- 1.3.6.1.4.1.2011.6.139.13.3.3.1

CLI Added to Resolve the WLAN Authentication Method Property

The plugin expanded its ability to resolve the WLAN Authentication Method property for managed Aruba WLAN devices. The plugin can now use CLI read, in addition to its existing ability to use SNMP read. When the plugin uses CLI read, the WLAN Authentication Method property identifies the encryption method used by the wireless client to authenticate with the access point, instead of the authentication method used.

Added eyeControl WLAN Role Action for Extreme (Motorola) WLAN Controllers

For Extreme (Motorola) WLAN Controllers, the Wireless Plugin now supports CLI Read and Write access to apply the *WLAN Role* action on wireless clients.

To implement the *WLAN Role* action, the Wireless Plugin edits the *Wireless Client Role Policy* in the Motorola WLAN Controller. For Motorola WLAN Controllers, the *WLAN Role* action assigns a VLAN to a wireless client.

The Role Name, as defined on the WLAN device, is the numerical *VLAN ID.*

The *WLAN Role* action to a connected wireless client is enabled per Forescout Appliance on which the Wireless Plugin runs.

For a Motorola WLAN Controller, the Wireless Plugin requires that the following MIBs are present on the WLAN devices:

- 1.3.6.1.4.1.388.50.1.3.17.1.1.1
- 1.3.6.1.4.1.388.50.1.3.4.1.1
- 1.3.6.1.4.1.388.50.1.4.3.2.3.1.1
- 1.3.6.1.4.1.388.50.1.2.1
- 1.3.6.1.4.1.388.50.0.11.0

Added eyeControl WLAN Block Action for HP WLAN Controllers

For HP WLAN Controllers, the Wireless Plugin now supports CLI (SSH or Telnet) write access to apply the WLAN Block action on wireless clients. The Wireless Plugin does not require any MIBs on a WLAN device connected to an HP WLAN Controller.

Added eyeSight Capability for Extreme (Enterasys) WLAN Controllers

Wireless Plugin management of a WLAN device is now supported for Extreme (Enterasys) WLAN Controllers through SNMP read access to perform queries.

For an Extreme WLAN Controller, the Wireless Plugin requires that the following MIBs are present on the WLAN devices:

- 1.3.6.1.4.1.4329.15.3.6.2.1
- 1.3.6.1.4.1.4329.15.3.5.1.2.1
- 1.3.6.1.4.1.4329.15.3.4.1.1.1
- 1.3.6.1.4.1.4329.15.3.3.4.6.1.1
- 1.3.6.1.4.1.4329.15.3.3.4.7.1.1

Added eyeSight and eyeControl Capabilities for Siemens WLAN Controllers

For Siemens WLAN Controllers, the Wireless Plugin now supports the following for management of a WLAN device:

- SNMP or CLI (SSH or Telnet) read access to perform queries
- SSH or Telnet write access to apply the WLAN management actions, *WLAN Block* and *WLAN Role*, on wireless clients

To implement the *WLAN Role* action, the plugin adds a role derivation rule to the WLAN profile used by the wireless client. The rule applies a previously defined Role-based *access-rule* to the connected wireless client.

For a Siemens WLAN Controller, the Wireless Plugin requires that the following MIBs are present on the WLAN devices:

- 1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.1.1
- 1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.3.1
- 1.3.6.1.4.1.4329.20.2.1.2.2.2.3.3.1.2.4.1

VPN Concentrator Plugin 4.3.1

This release contains the following new or enhanced features:

Support for Networks with Overlapping IP Addresses

The VPN Concentrator Plugin supports working with networks that use overlapping IP addresses. When the Forescout platform is enabled to support overlapping IP addresses, you can configure the plugin to manage multiple VPN devices all having the same IP address, however for this to be valid, each of these VPN devices must be located within a different IP Reuse Domain (IRD).

The following Console areas of the plugin are affected:

- The *General* pane/tab
- The *Test* dialog
- The *VPN* pane

For plugin details, refer to the *Forescout Network Module: VPN Concentrator Configuration Guide*. For information about a network's use of overlapping IP

addresses and how the Forescout platform addresses this issue, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access these documents.

Fixed Issues

This section describes fixed issues for the Forescout platform and Base Modules.

Forescout Platform 8.2.1

This section describes fixed issues for this release.

Issue	Description
DOT-4126	With this version, the Forescout CLI command **`disconnect`** is no longer available to execute in the CLI of Forescout devices (Enterprise Manager and Appliances).

Authentication Module 1.2.1

There are no fixed issues for module components in this release.

Core Extensions Module 1.2.1

There are no fixed issues for module components in this release.

Endpoint Module 1.2.1

There are no fixed issues for module components in this release.

Hybrid Cloud Module 2.1.1

There are no fixed issues for module components in this release.

Network Module 1.2.1

This section describes fixed issues for this release.

Component	Issue	Description
Centralized Network Controller Plugin	**CN-866**	With this version, the limitation that the plugin running on the Connecting CounterACT Device does not poll more than 1000 network devices per Meraki Organization is no longer in effect. For additional information, refer to the section Baseline Deployment Guidelines for Cisco Meraki in the Forescout Network Module: Centralized Network Controller Plugin 1.2.1 Configuration Guide.

Known Issues

This section describes known issues for the Forescout platform and Base Modules.

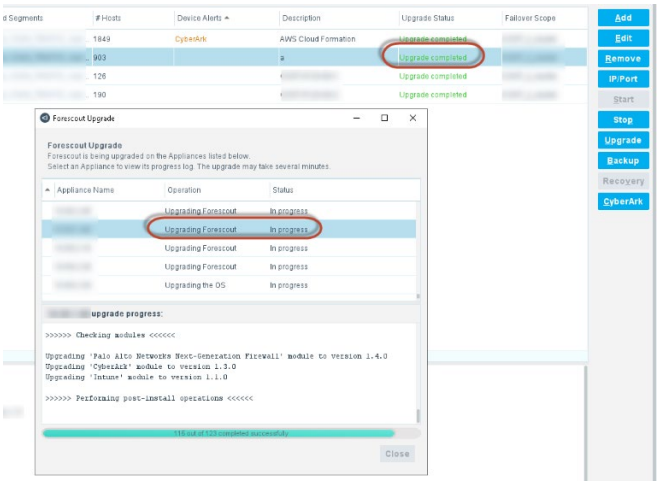
Forescout Platform 8.2.1

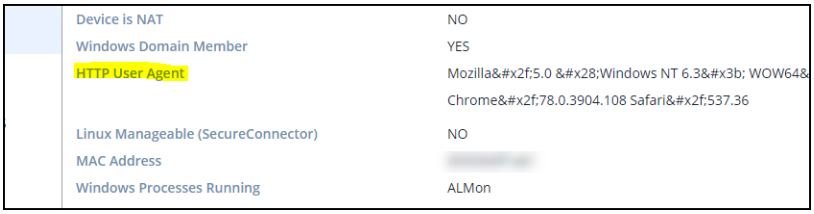
This section describes known issues for this release.

Issue	Description
CA-23249	Navigating away from some plugin's Options pages causes the "Changes not applied. Do you want to continue?" dialog to appear even though there were no changes.
CA-24435	When reassigning segments from one Appliance to another, the message "Loading completed from X out of X Appliances. Appliances omitted due to slow responsiveness" appears.
CA-26296	A "Changes not applied" error appears after applying edits to some plugin's configurations and attempting to leave the configuration page.

Issue	Description
CA-26914	Plugin actions such as the *HTTP Notification* action require the hijack ability on endpoints. Hijack is performed via any of the following Forescout components: ▪ DNS Enforce Plugin (when properly configured) ▪ HPS Inspection Engine ▪ Packet Engine When the DNS Enforce Plugin attempts to apply the *HTTP notification* action on a targeted endpoint and, concurrently, the Packet Engine is stopped (not running), the application of this action fails. Note: Beginning with Forescout platform version 8.2, the Packet Engine became a core plugin that can be started/stopped and is listed in the Console Modules pane. **Workaround:** In order for the DNS Enforce Plugin to apply actions that hijack targeted endpoints, Forescout platform operators/administrators must do the following: ▪ Make sure that both the DNS Enforce Plugin and the Packet Engine are running on the Forescout device (user is not required to enable channels). ▪ The DNS Enforce Plugin and endpoints must be properly configured to enable hijack.
CA-26667	External users - meaning those users whose credentials are authenticated using an external RADIUS server or an Active Directory server - who are logged into the CLI shell of a Forescout device (the Enterprise Manager or an Appliance) are not able to execute ***privileged*** fstool commands. Executing privileged fstool commands requires users to first provide the cliadmin password, which external users typically would not know; as they cannot provide the cliadmin password, privileged fstool commands do not execute.
CA-22726	When you enable support for overlapping IP addresses, failover clusters may not work in branches of the Appliance tree that handle overlapping sites. In particular, failover does not work when you configure a failover cluster in a folder that includes both segments in the global/default network and segments in an IP Reuse Domain.
CA-23249	Navigating away from the Linux or Mac Options pages causes the "Changes not applied. Do you want to continue?" dialog box to appear even though there were no changes.
CA-23920	When support for overlapping IP addresses is enabled, controls in the IP Assignment and Failover pane change. In this release, you cannot reassign segments from Appliances to their parent folder. You must manually move the segments in the Appliance tree. 
CA-24103	Even though there are no changes, a warning about losing changes is displayed when canceling an Option>CEF>Edit for a server in the Forescout Console.

Issue	Description
CA-24180	Java core dumps on Enterprise Manager while adding cloud RM/Appliance to on-premise setup.
CA-24353	HPS Inspection Engine stuck in pending after an Appliance failover. Some properties are not synchronized by the failover mechanism, causing performance issues in the HPS Inspection Engine and delaying the resolution of the Network Function property following a failover.
CA-24475	The number of managed hosts returned by the command **fstool sysinfo** does not match the number of managed hosts displayed in the Console.
CA-24478	During an upgrade, the Enterprise Manager stalls on FSUpgradeStatusConfigParams$FSUpgradeStatusUpdater when an appliance is unresponsive.
CA-24489	The number of hosts in a policy and the total number shown in the host view does not match.
CA-24495	A host stays matched to a policy even if the host is down and remains matched after a manual recheck.
CA-24628	For HTTP Notification hijack redirect action for version 8.x User Portal Builder customization, and enabled Forescout Compliance Center (FCC): The HTTP User Notification web page alternates between the Release 8.x HTTP User Portal Builder customization page (without FCC) and the Release 7.x HTTP legacy customization page (with FCC). This issue is relevant for customers who upgraded from pre 8.x versions and customers who started out with 8.x version.
CA-25285	When you enable support for overlapping IP addresses, the **Log>Host Details** option in the main console menu does not work for endpoints with overlapping IP addresses. To view overlapping endpoint details, right-click the endpoint and select **Information>Details**.
CA-25334	When you enable support for overlapping IP addresses, the site map does not display endpoints in IP Reuse Domains. The map only displays areas of the Internal Network that are in the default/global network.
CA-25438	When you enable support for overlapping IP addresses, endpoints in IP Reuse Domains are not automatically shared with Recovery Manager during continuous updates. After failover to Recovery Manager, these endpoints must be rediscovered.

Issue	Description
CA-25666	From Tools > Options > Guest Management > Registered Guests tab: If you attempt to import a file containing an email address that already exists in a record in the Console table, the import fails. The application is unable to identify any differences between the two records and update the Console table accordingly. Click *Details* in the message dialog box to view the error details. For example, if the file to import contains a record with email address john.smith@abcde.com, and this address already exists for a registered guest in the Console table, the import fails and the application issues the error message "The import guests file contains an existing guest: john.smith@abcde.com" If this error occurs, do one of the following: ▪ Correct the email address of the record in the file if it is incorrect, and then attempt to import the file again ▪ Remove the record with the duplicate email address from the file, and then attempt to import the file again ▪ Delete the registered guest from the table in the Console if the information is out of date, and then attempt to import the file again
CA-25784	When upgrading Appliances, the Forescout Upgrade dialog box gets stuck on a specific step even though the upgrade process completed successfully. The status in the dialog box incorrectly displays *In progress*, while the upgrade status on the device table correctly displays *Upgrade completed*. This asynchrony of display rectifies itself within a brief period. During the upgrade process, the user can minimize the dialog box, but not close it. On closing the Console session, the dialog box closes as well. 
CA-26114	When support for overlapping IP addresses is enabled, **`the fstool devinfo`** command does not work for Appliances with IP Reuse Domains.

Issue	Description
EM2-3386	In the *Assets* view, *HTTP User Agent* details do not parse correctly. To access this property for a device in *Assets* view, click the › icon to the left of the row for the specific device. 

Authentication Module 1.2.1

This section describes known issues for this release.

Component	Issue	Description
RADIUS	**DOT-4176**	There are no new admissions for devices that authenticate using dot.1x. This means that the rule for condition in a policy with *802.1x admission event* (under Condition > Properties > Events > Admissions) cannot match for dot.1x-enabled devices. For example, if you have a clarification policy based on the *802.1x admission event* as a main rule. devices cannot match the main rule. As a result, the system does not inspect advanced sub rules for these devices.
User Directory Plugin	**UD-1427**	The User Directory Plugin does not support IPv6 TACACS authentication servers.

Core Extensions Module 1.2.1

This section describes known issues for this release.

Component	Issue	Description
Advanced Tools	**ADT-219**	When you enable support for overlapping IP addresses, the Segment Path property is not evaluated accurately for endpoints in IP Reuse Domains.
	ADT-234	When you enable support for overlapping IP addresses, Appliances that are assigned to IP Reuse Domains do not resolve the Windows Manageable SecureConnector (via any interface) property for endpoints they manage. The property is evaluated as Irresolvable for these endpoints.
Dashboards	**EM2-2107**	Widgets in the OOTB Device Compliance dashboard do not display data for devices that meet the following criteria: **1.** The policy that the device matches only contains a main rule (no sub-rules). **2.** The policy is categorized as Compliance, with *Unmatched* devices in the main rule labeled as *Not Compliant*.

Component	Issue	Description
Device Classification Engine	**DPL-597**	It is not recommended to perform Set Classification actions after a new Device Profile Library version is installed and before it is applied or rolled back. If these actions are performed: ▪ They are displayed together with the pending classification changes. ▪ Their Set Classification action status is listed as Success. ▪ They do not take effect until the new library version is applied or rolled back.
IOC Scanner	**CA-22258**	If the plugin is not running when you use Search in the IOC Repository tab, the search does not work properly due to the entries in the 'Reported by' column. ***Workaround***: Start the plugin on the Enterprise Manager.
IoT Posture Assessment Engine	**PA-133**	Changes cannot be applied when adding or editing custom credentials for the IoT Posture Assessment Engine. The error "Operation Failed" is shown.
Packet Engine	**PE-521**	When the Forescout platform is deployed on KVM virtual systems, the maximum bandwidth of Packet Engine traffic monitoring is 500 Mb/s. If traffic exceeds this amount, virtual firewall functionality and device discovery may be affected.
	PE-644	Even after SecureConnector was successfully installed in Linux endpoints, application of the HTTP Redirection action on these endpoints results in the following erroneous action status: *Hosts traffic not monitored*
	PE-744	When you enable support for overlapping IP addresses, devices you assign to IP Reuse Domains do not apply Threat Protection logic. Endpoints handled by these devices are no longer covered by Threat Protection features - but this is not indicated in the Console. To restore Threat Protection coverage for specific Appliances: **1.** Open the *Options* window. **2.** In the Options tree, go to **CounterACT Devices > IP Assignment and Failover**. Remove IP Reuse Domain assignments from Appliances and/or folders that must apply Threat Protection: set the **IP Reuse Domain** field to *None*. Select **Apply** to apply changes. **3.** Go to **Options>Threat Protection**. Verify that the **Threat Protection** option is selected and select **Apply**. Appliances without IP Reuse Domains apply Threat Protection logic.

Component	Issue	Description
	PE-852	When you enable support for overlapping IP addresses, Virtual Firewall rules do not always use IP Reuse Domain information. When you define a global virtual firewall rule (**Options>Virtual Firewall**) the rule applies to *all* endpoints with the specified IP ranges, in *all* IP Reuse Domains. To apply a Virtual Firewall to specific instances of an overlapping IP address, create a policy that applies the **Virtual Firewall** action. Limit the overlapping segments in the policy scope, or define a condition based on the IP Reuse Domain host property. The firewall is applied only to endpoints that match policy scope and conditions.
	PE-853	When you enable support for overlapping IP addresses, the **HTTP Redirect** action does not work when Appliances in overlapping sites have a separate management interface to Enterprise Manager. When each overlapping site has a directory server, specify the redirection target using an FQDN.
Reports	**REP-662**	Generating a very large report can fail or cause memory and PDF download problems.
	REP-760	When you run the Registered Guest Analysis web report for selected devices, the result is an empty report. This issue occurs when you run the *Corporate / Guest Control* policy template from the Console in CounterACT version 8.0 and above.
Syslog	**SYS-557**	You can configure the Syslog Plugin to receive syslog messages, via a TCP connection, from a sender source. Any network communication issue that causes dropped packets on the TCP connection without then terminating that connection may result in the Syslog Plugin receiving only a partial message that then causes the plugin to stop operating, because it waits to receive the remainder of that message.

Endpoint Module 1.2.1

This section describes known issues for this release.

Component	Issue	Description
HPS Inspection Engine	**HPS-19276 2969**	The *Disable External Device* action does not work with Seagate portable external drives.
	64724	When the *Start SecureConnector* action is applied to an endpoint running Windows XP, SecureConnector cannot be installed as a *Dissolvable* or *Application* deployment using remote installation.

Component	Issue	Description
	HPS-2806 73636	This release supports Kerberos authentication for Remote Inspection of endpoints. When the Forescout platform has previously logged in successfully to an endpoint using Kerberos, and the endpoint is removed from the Domain and then rejoins, the Forescout platform cannot reconnect to the endpoint until the domain controller renews the Ticket-Granting Ticket (TGT) used for Kerberos authentication; typically the TGT is renewed every 10 hours. During this period, resolution of properties and other Remote Inspection tasks are not performed for the endpoint.
	HPS-5317	SecureConnector is not successfully installed on endpoints running Windows 7 or Windows 10 when the **Endpoint Remote Inspection Method** is set to *Using MS-RRP* and scripts are run using Windows Task Scheduler.
	HPS-5634	When an endpoint running SecureConnector is reassigned to another Appliance, SecureConnector re-creates a secure connection with its new Appliance. However, when support for overlapping IP addresses is enabled, this behavior is not supported in overlapping areas of the network. In these areas: ▪ SecureConnector does not reconnect when an endpoint moves to another Appliance ▪ When SecureConnector is installed on an endpoint in an overlapping site, it can only communicate with the Appliance that downloaded SecureConnector to the endpoint. For more information refer to the *Working with Overlapping IP Addresses How-to Guide*.
Linux Plugin	**LNX-517**	The SecureConnector icon does not display in Ubuntu operating systems when Dissolvable or visible daemon deployment is selected. Upon reboot, the icon is visible with visible daemon deployments.

Hybrid Cloud Module 2.1.1

This section describes known issues for this release.

Component	Defect #	Description
Azure Plugin	**MAZ-146**	The log lists a SocketTimeoutException. The Azure Plugin retries in the next polling interval and recovers.

Component	Defect #	Description
VMware vSphere Plugin	**VMW-868**	When the Forescout platform is enabled to support overlapping IP addresses and in the VMware vSphere Plugin's *General* pane/tab: ▪ The plugin is configured with the FQDN of the VMware server ▪ The *IP Reuse Domain* (IRD) field displays an IRD - identifying that the VMware server's IPv4 address is located within the Connecting CounterACT Device's IP segment assignment (scope) that is assigned to that IRD the following plugin processing issue occurs: After removing that IP segment assignment from the Forescout device, selected as the Connecting CounterACT Device for the VMware server, the VMware server's *IP Reuse Domain* field, in the plugin's General pane/tab, continues to erroneously display the IRD.
VMware vSphere Plugin	**VMW-536**	When the VMware vSphere Plugin sends a full poll request to the vSphere server, a response is not received and after three minutes, a SOAP Request Error message is displayed. When this error occurs, the VMware vSphere Plugin aborts the current operation and starts the full poll at the next scheduled poll.

Network Module 1.2.1

This section describes known issues for this release.

Component	Issue	Vendor	Description
Centralized Network Controller Plugin	**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]. This issue results from a known Meraki API limitation.

Component	Issue	Vendor	Description
	CN-856	Cisco Meraki	When an Appliance that is responsible for a specific group of detected endpoints, based on its configured IP address range, instructs the Connecting CounterACT Device (a different Appliance) to apply the *Assign Meraki Policy* action on a detected endpoint that is connected to a Meraki wireless AP, the following processing behavior has been noticed to occur on ***rare*** occasion: ▪ Some time after the *Assign Meraki Policy* action is successfully applied on the targeted endpoint, the endpoint no longer has the *Assign Meraki Policy* action applied on it, even though there was no active/explicit cancelling of this action. The endpoint does have the Meraki *Normal* policy applied on it, as reported in the Console's *Home* tab. Application of the Meraki *Normal* policy typically occurs upon CNC Plugin cancellation of the *Assign Meraki Policy* action.
Network Controller Plugin	**NC-461**		Any plugin configuration change (select **Apply**) always results in a restart of the NC Plugin, which, as a matter of processing, causes all currently plugin-applied actions to be cancelled and then re-applied on targeted endpoints.
Rogue Device Plugin	**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

Component	Issue	Vendor	Description
Switch Plugin	**SW-1902**	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*.
	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-4584	Brocade	The ACL test fails when testing the plugin configuration for managing a Brocade Stackable Switch running OS Version 08.0.30nT311. The **ACL Status** column in the Switch tab and the **Message** column of the plugin configuration test message both display block symbols (□) rather than readable characters. Plugin application of the *Endpoint Address ACL* action functions as normal.
	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.

Component	Issue	Vendor	Description
Wireless Plugin	**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*. 
	WRL-456	Motorola	When 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.
VPN Concentrator Plugin	**VPN-284**		In an overlapping IP address network environment, the plugin does not support applying its eyeControl actions (the *VPN Block* action and the *Release VPN Block* action cancellation) on targeted endpoints.

Important Considerations

This section describes important considerations and upgrade issues for the Forescout platform and its Base Modules.

Forescout Platform 8.2.1

This section describes important considerations for the Forescout platform.

- In order for the third-party software Medigate Module to work with Forescout interim release 8.2.1, the module must be running Medigate version 1.1.0 or above.
- If any of the following, third-party software components are installed on your Forescout device(s):
  - Attivo Networks
  - Malwarebytes

  - Network Perception (NP-Live)
  - RedSeal
  - Rheinmetall (RSHA)
  - Saint
  - Trapx
  - Tripwire

  Then, before upgrading your Forescout deployment to interim release 8.2.1, you must contact the software vendor(s) and verify the compatibility of these components with Forescout interim release 8.2.1.

CEF Plugin 2.8.2

This section describes important considerations for the CEF Plugin.

- If you have existing policies that were created before Forescout interim release 8.2.1/CEF Plugin 2.8.2 and these policies use any of the CEF Plugin *Audit* actions - *Send Compliant CEF message*, *Send Customized CEF message* or *Send Not Compliant CEF message* - then in order for the new CEF Event Field ID **`ird`** (CounterACT property tag **`area_code`**) to appear in their resulting CEF message, you must edit the policies in which these actions are used; first remove the action and then add the action anew.

Modules Packaged with This Release

When you install or upgrade to Forescout 8.2.1, the following modules are automatically installed. New module releases may become available between Forescout releases. See Module and Component Rollback for rollback information.

Refer to the relevant configuration guides for detailed information about how to work with and configure components included with these modules.

This document contains information about features and fixed/known issues for *Base Modules*. For *Content Modules*, ***refer to the specific Release Notes for each module***.

- Base Modules:
  - Authentication Module 1.2.1
  - Core Extensions Module 1.2.1
  - Endpoint Module 1.2.1
  - Hybrid Cloud Module 2.1.1
  - Network Module 1.2.1
- Operational Technology Module 1.3.1
- Content Modules:
  - Device Profile Library 20.1.5
  - IoT Posture Assessment Library 19.0.12
  - NIC Vendor Database 20.0.4

- Network Controller Content Plugin 1.0.1
- Security Policy Templates 20.0.6
- Switch Content Plugin 1.1.0
- Windows Applications 20.0.5
- Windows Vulnerability DB 20.0.5

Module and Component Rollback

The following rollback/upgrade activities are ***not*** supported:

- Rolling back a base module (or one of its components) to a version released prior to Forescout 8.2.x.
- Upgrading to a base module version (or one of its components) released with 8.2.x when running a version of the Forescout platform lower than version 8.1.1.

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.

Where to Go for More Information

- 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.
- For requirements/specifications related to deployment sizing for physical and virtual Forescout devices, refer to the Forescout Licensing and Sizing Guide.
- For component-specific requirements, refer to the relevant configuration guide. See Additional Forescout Documentation for information about how to access these guides.

- For detailed installation/upgrade instructions for this version, including system requirements and a complete list of supported models for physical Forescout Appliances, refer to the Forescout Installation Guide.

Previous Releases

Installing this release also installs fixes and enhancements provided in the releases listed in this section.

Prior to Forescout version 8.2, Base Module fixes and enhancements were documented in separate Release Notes.

Forescout Platform

https://www.forescout.com/company/resources/forescout-8-2-0-release-notes-platform-and-base-modules/

https://www.forescout.com/company/resources/forescout-8-1-4-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-3-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-2-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-1-release-notes/

https://www.forescout.com/company/resources/forescout-8-1-release-notes/

https://www.forescout.com/company/resources/counteract-version-8-0-1-release-notes/

https://www.forescout.com/company/resources/counteract-8-0-release-notes/

Authentication Module

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

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

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

Core Extensions Module

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

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

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

Endpoint Module

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

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

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

Hybrid Cloud Module

https://www.forescout.com/company/resources/hybrid-cloud-module-release-notes-2-0-2/

https://www.forescout.com/company/resources/hybrid-cloud-module-release-notes-2-0-1/

https://www.forescout.com/company/resources/hybrid-cloud-module-2-0-release-notes/

Network Module

https://www.forescout.com/company/resources/network-module-release-notes-1-1-3/

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 Technical Documentation Page, and from 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 Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based Documentation Portal, as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides 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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support 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

You can access individual documents, as well as the Documentation Portal, directly from the Forescout Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools** > **Options** > **Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.