Forescout

Platform and Base Modules

Release Notes

Version 8.2

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

2020-03-15 14:05

Table of Contents

Forescout 8.2: Identify and Act – Faster

Forescout 8.2 accelerates time to act for organizations wrangling with identifying varied devices, automation, policy enforcement and incident response across their extended enterprises. It delivers a single source of actionable context across diverse network-connected devices.

Security leaders are proactively alerted to areas of security risk and can share that context-rich information, breaking down barriers to action. Teams are empowered to move quickly and with greater confidence to build policies, automate actions and mitigate security exposure.

Highlights of this latest release include:

- A new eyeSight web-based user interface, including out of the box dashboards for device visibility and compliance, expanded personalization and sharing options, and a new assets view enabling users to quickly search for high risk devices across a unified asset inventory. See Enhanced Dashboards View and New Assets View.
- Expanded deployment flexibility for cloud-first organizations. Visibility and control with no on-premises footprint by deploying Forescout appliances on AWS or Azure cloud infrastructure. See Forescout Platform in the Cloud.
- Capacity to uniquely identify and control devices obscured due to cloned networks/overlapping IPs, and devices that are “nested” behind other network-connected devices. See Working with Overlapping IP Addresses and Nested Device Management.
- Enhanced classification coverage with support for an additional 19 healthcare protocols natively in eyeSight.

About This Release

Forescout version 8.2 delivers New and Changed Features and Fixed Issues both for the core Forescout 8.2 platform and for Modules Packaged with This Release.

Review information about Known Issues, including any workarounds, and Important Considerations for installing/upgrading to this version.

Installing/upgrading to this version is not supported on 5110 and CTR (all revisions) model physical Appliances. If you have one of these models, contact your Forescout representative for any questions or concerns. For a complete list of supported models for physical Forescout Appliances, refer to the Forescout Installation Guide Version 8.2.

See Important Considerations for additional install/upgrade related information. Installing this release also installs new 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.

Rollback is not supported by this version. It is recommended 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

Upgrade is supported from the following Forescout versions:

- ***8.1.1***
- ***8.1.2***
- ***8.1.3***

If you are upgrading from a version that is earlier than 8.1.1, you first need to upgrade to one of the above versions before you can upgrade to 8.2. The following table lists supported upgrade paths when upgrading from versions earlier than 8.1.1:

		Upgrading To:					
		8.0	8.0.1	8.1	8.1.1	8.1.2	8.1.3
Upgrading From:	7.0.0, SP 3.0.2.x	✓	✓	✓	✓	✓	✓
	8.0	***N/A***	✓				
	8.0.1		***N/A***	✓	✓	✓	✓
	8.1			***N/A***	✓	✓	✓

For detailed 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 Version 8.2.

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		√	√	√
Authentication	RADIUS 4.5.0		√	√
	User Directory 6.5.0		√	√
Core Extensions	Advanced Tools Plugin 2.4			√
	CEF Plugin 2.8.1			
	Cloud Uploader 1.0 ***NEW***	√		
	Dashboards Plugin 1.2.1			√
	Data Publisher 1.0 ***NEW***	√		
	Data Receiver 1.0 ***NEW***	√		
	Device Classification Engine 1.4	√		√
	Device Data Publisher 1.0 ***NEW***	√		
	DHCP Classifier Plugin 2.3			
	DNS Client Plugin 3.2			

Module	Component	New and Changed Features	Fixed Issues	Known Issues
	DNS Enforce Plugin 1.3.1			
	DNS Query Extension Plugin 1.3			
	External Classifier Plugin 2.3	√		
	Flow Analyzer Plugin 1.4.1			
	Flow Collector 1.1	√		
	IOC Scanner Plugin 2.4			√
	IoT Posture Assessment Engine 1.1.3			
	NBT Scanner Plugin 3.2			
	Packet Engine 8.2	√		√
	Reports Plugin 5.2			√
	Syslog Plugin 3.6			
	Technical Support Plugin 1.3	√		
	Web Client Plugin 1.2			
Endpoint	HPS Agent Manager 1.2			
	HPS Inspection Engine 11.1			√
	Hardware Inventory Plugin 1.2			
	Linux Plugin 1.5			√
	Microsoft SMS/SCCM Plugin 2.4.2			
	OS X Plugin 2.3			
Hybrid Cloud	AWS Plugin 2.2	√		
	Azure Plugin 1.1			√
	VMware NSX Plugin 1.3			
	VMware vSphere Plugin 2.5			√
Network	Centralized Network Controller Plugin 1.2			√
	Network Controller Plugin 1.0 ***NEW***	√		√
	Rogue Device Plugin 1.1	√		√
	Switch Plugin 8.14.1	√		√
	VPN Concentrator Plugin 4.3			
	Wireless Plugin 2.0	√		√
Operational Technology		√		√

New and Changed Features

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

Forescout Platform 8.2

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

Enhanced Dashboards View

The Dashboards view, part of the Forescout Web Client, has been enhanced and now provides:

- Out of the Box Dashboards, including device visibility, device compliance, and health monitoring dashboards with new and enhanced widgets
- Ability to Create Multiple Custom Dashboards
- Improved Workspace Management and Privacy Settings
- Ability to Drill-Down Into a Widget for information about corresponding devices

Refer to the *Forescout Administration Guide* for more information about working with this feature.

Out of the Box Dashboards

The following dashboards are available out-of-the-box with this version:

- **Device Visibility**. View at a glance, real-time inventory, compliance and risk data for devices on your network. Widgets in this dashboard cover:
  - Classification of devices according to function, OS, and vendor/model
  - Compliance overview
  - IoT devices at risk
  - Unauthorized Windows applications installed

  Run the Dashboard Policies template in the Forescout Console to create policies that populate the widgets in this dashboard.

See Running the Dashboard Policies Template – Weak Credentials Policy for an important consideration related to one of the visibility dashboard widgets.

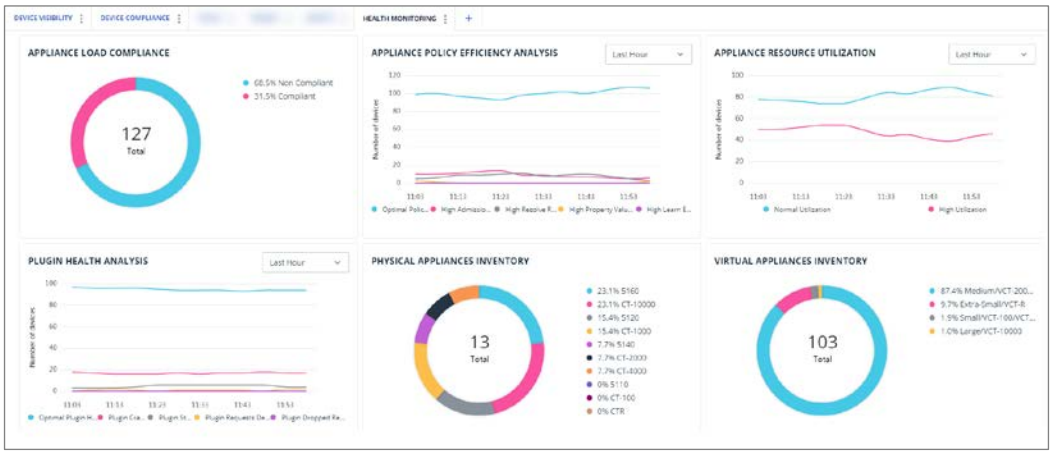
- **Device Compliance**. View at a glance, real-time data for improving compliance hygiene for devices on your network. Widgets in this dashboard cover:
  - Compliance overview
  - Top reasons for noncompliance
  - Highly vulnerable devices
  - Top reasons for noncompliance – IOT devices / Application issues

  Run the Dashboard Policies template in the Forescout Console to create policies that populate the widgets in this dashboard. Also verify that your environment has devices that match 'Not Compliant' sub-rules in running 'Compliance' policies.

- **Health Monitoring**. View at a glance, real-time data that helps you monitor and improve the health of Forescout Appliances in your deployment. Widgets in this dashboard cover:
  - Appliance load compliance

- Appliance policy efficiency
- Appliance resource utilization
- Plugin health analysis
- Physical and virtual Appliance inventory

Run the Health Monitoring templates in the Forescout Console to create policies that populate the widgets in this dashboard. Policies and properties used in this dashboard are provided by the Technical Support Plugin. See Health Monitoring Policies, Properties and Dashboard for more information.

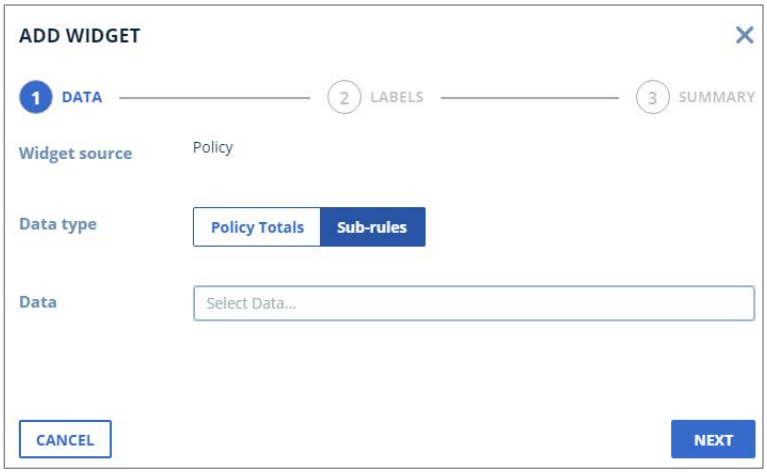


Create Multiple Custom Dashboards

In addition to the Out of the Box Dashboards provided, you can add custom dashboards to your view to address specific use cases. Dashboard views are customizable for each user. For example, you can add:

- New dashboards that you create. You can populate these with widgets of your choosing.
- Public dashboards created by other users.

Add widgets to a dashboard to visualize information about Forescout policies. You can add widgets to any dashboard that you create. Depending on the data you select to populate the widget, different chart type displays are available.



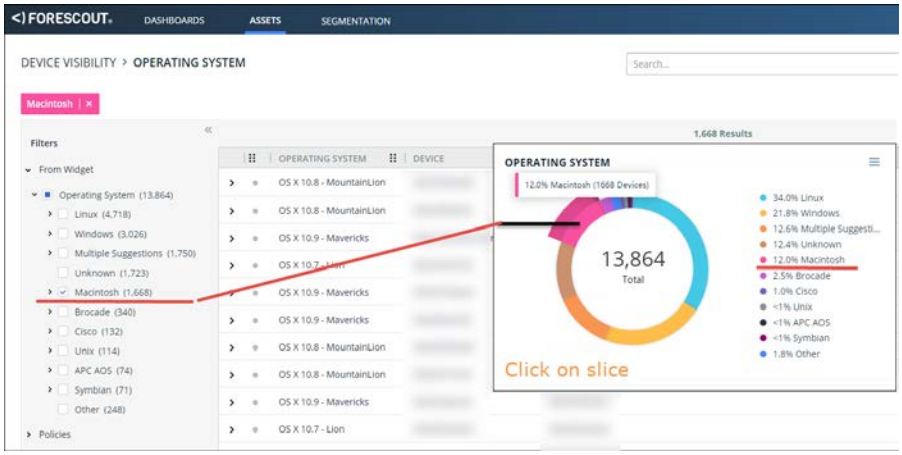
Improved Workspace Management and Privacy Settings

Your ability to work with dashboards and widgets has been enhanced as follows:

- Dashboard workspace management and privacy settings:
  - Hide, rename, duplicate or delete a dashboard.
  - Configure dashboard privacy to determine whether a dashboard you created is public (everyone can add to their view) or private (only you can see).
  - Reorder dashboard tabs
- Widget management:
  - Add custom widgets based on Forescout policy data
  - Edit widget data or delete widgets
  - Reorder widgets in a dashboard
  - Drill-Down Into a Widget

Drill-Down Into a Widget

The Dashboards view is fully integrated with New Assets View. You can drill down into a widget to access tabulated information in the Assets view about the devices corresponding to the widget.

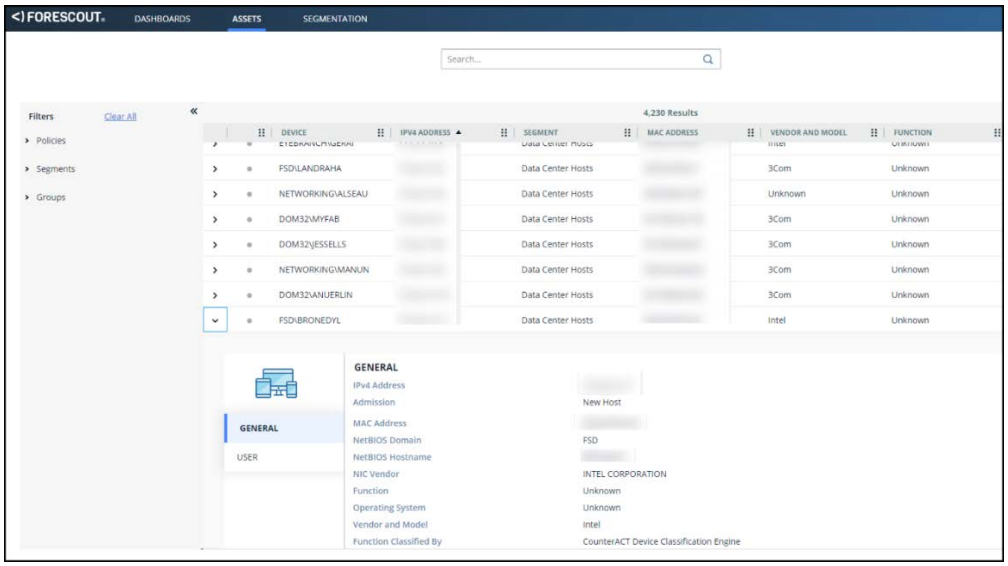


New Assets View

The Assets view, part of the Forescout Web Client, is a web-based search, filter and discovery tool that lets you leverage extensive network and device information collected and correlated by Forescout products. This information is valuable to various groups across your organization, including:

- Security teams: Use device or policy information to quickly locate risky assets.
- IT departments: Use an IP address or other device information to locate and contact users when maintenance is required at the device.
- Help Desk/SOC: Use device information to handle security incidents in real time.

By using the Assets view, crisis management and subsequent remediation time is shortened.



Use this view to display a tabulated list of all the devices that Forescout eyeSight detects, subject to any selected device filters. The *Assets* view provides several device filter methods, which you can apply separately, or in tandem. You can filter the *Assets* view or drill down from a widget into the *Assets* view to list only the devices relevant to a specific area of interest, for example, devices corresponding to a certain policy / sub-rule. You can view information about any device on any segment for which you have permissions, which is defined as part of your user scope.

The Assets view is fully integrated with Forescout Dashboards (see Enhanced Dashboards View), and you can drill down to a view of your devices by clicking objects in dashboard widgets. In addition, you can save your own customized *Assets* view, and you can export any filtered list of devices to a CSV file. The Assets view supports Overlapping IPs.

> *The Assets view does not replace the existing Assets Portal, but instead provides a newer interface with more robust filter/search capabilities. The existing Assets Portal allows users to clear event detections and stop policy actions. Depending on your needs, you may prefer to use one or the other, or both tools.*

Forescout Platform in the Cloud

Forescout Enterprise Managers and Appliances can now be deployed in the cloud via *Amazon AWS* or *Microsoft Azure*.

For hybrid (cloud-based / on-premises) solutions, VPN infrastructure must be deployed between the premises and the cloud. The VPN infrastructure can be a native VPN gateway, or a proprietary VPN service, such as *Amazon AWS Direct Connect* or *Microsoft Azure ExpressRoute* (depending on your service provider).

Our recommended best practices to optimize functionality and minimize costs are to keep Appliances near the assets (devices and switches) with which they interact. So, deploy as follows:

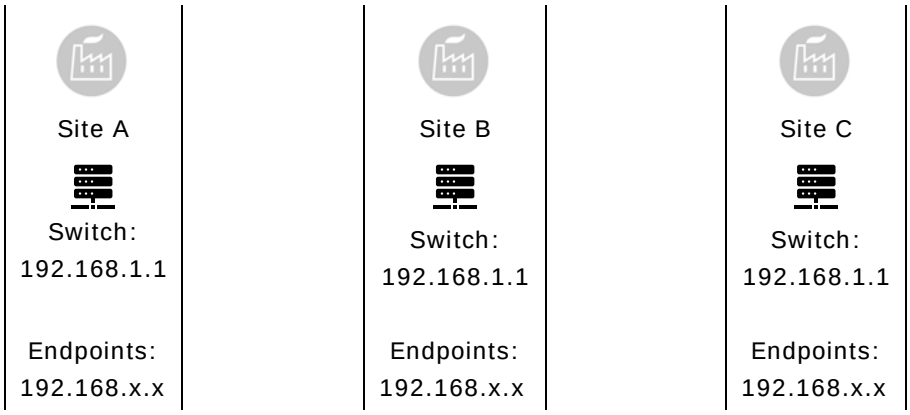
- Use cloud-based Appliances to manage cloud-based assets.
- Use on-premises Appliances to manage on-premises assets.
- Use a mixture of cloud-based and on-premises Appliances to manage hybrid assets.
- Use focal and dedicated Appliances close to the third-party applications with which they interact.

The table below summarizes several available implementations.

Use Case	Cloud Collateral	On-premises Collateral	Connectivity
1	Enterprise Manager	Appliance, switches, and devices	VPN connection (VPN Gateway and Router / Firewall)
2	Appliance and devices	N/A	N/A
3	Enterprise Manager, Appliance, and devices	Appliance, switches, and devices	VPC / Resource Group planning for connection
4	Appliance	Devices	VPN connection (VPN Gateway and Router / Firewall)

Working with Overlapping IP Addresses

Overlapping IP addresses occur when IP addresses repeat across your network, as in retail branches, Operational Technology environments, or merged corporate networks.



By default, the Internal Network defined in Forescout only supports a single domain of unique IP addresses. This guide describes configuration options and tools that support networks with overlapping IPs. When these options are enabled, you can configure segments with overlapping IPs and assign these segments to Appliances.

Part of Forescout's Total Solution for OT/IoT and Automation Networks

Overlapping network structures are commonly used in Operational Technology and other automation environments. In addition to the configuration and usage approach described in this guide, the Operational Technology Module and Forescout SilentDefense components are typically deployed to support these environments. See the *Operational Technology Module Configuration Guide* for detailed information about the Forescout solution for Operational Technology/automation environments.

About IP Reuse Domains

IP Reuse Domains distinguish each instance of an overlapping IP address. Within each IP Reuse Domain, IP addresses are unique and cannot overlap.

When support for overlapping IPs is enabled in the Forescout platform, you define IP Reuse Domains as you assign Appliances to various areas of the Internal Network. Endpoints with overlapping IP addresses are identified by the IP Reuse Domain of the Appliance that discovers and reports them.

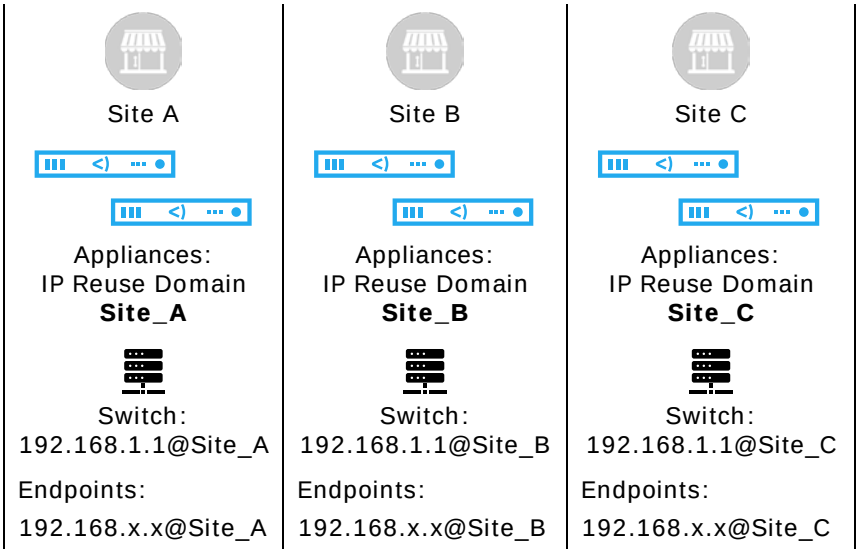
The IP Reuse Domain field appears in relevant areas of the Console, and the IP Reuse Domain is added to IP addresses or segments in Console views, using the following format:

<IPv4>@IP_Reuse_Domain

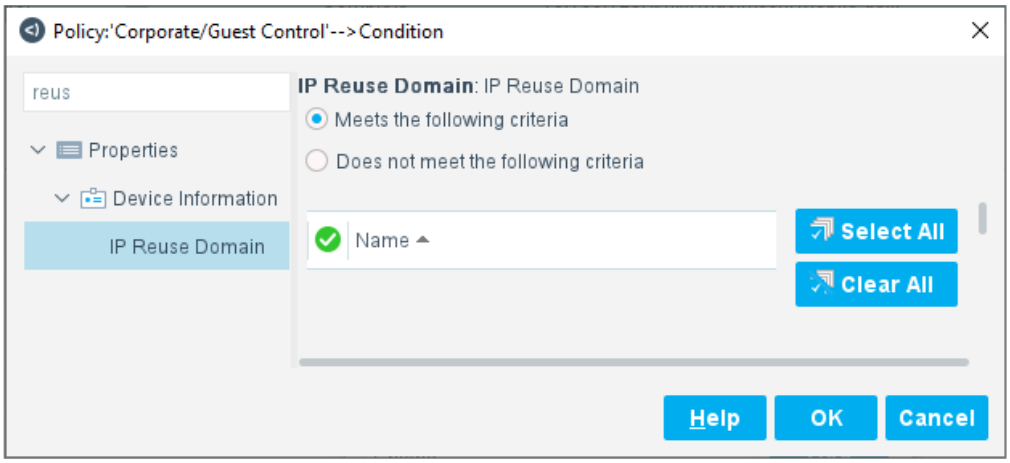
For example:

192.168.0.1@Site_A

IP Reuse Domain settings only appear when this feature is enabled.



The **IP Reuse Domain** host property lets you use the IP Reuse Domain to select endpoints in Forescout policies, and to create filters, lists, and views in the Console.



Deploy Support for Overlapping IP Addresses

This section provides an overview of the procedures you must perform to work with overlapping IP addresses in the Forescout platform. For detailed procedures, refer to the *Working with Overlapping IP Addresses How-to Guide*.

To deploy support for Overlapping IP addresses:

1. Enable the feature: In the Console, open the Options window. Select **Advanced > Overlapping IPs** and select **Allow Overlapping IP Addresses**.

   It is now legal to define multiple segments with the same IP range in the Internal Network. In addition, the **IP Reuse Domain** field and other options are enabled in the console.

2. (Optional) There are additional configuration and deployment steps when SecureConnector is used in your network. See Deploy SecureConnector in Networks with Overlapping IP Addresses.

3. In Segment Manager, define segments that reflect repeated structures while distinguishing each instance. For example, in a simple case of branch offices:

Site A	
Segment Name	**IP Range**
Overlap IPs Site A	192.168.0.0
Admin-Site-A	10.32.3.0

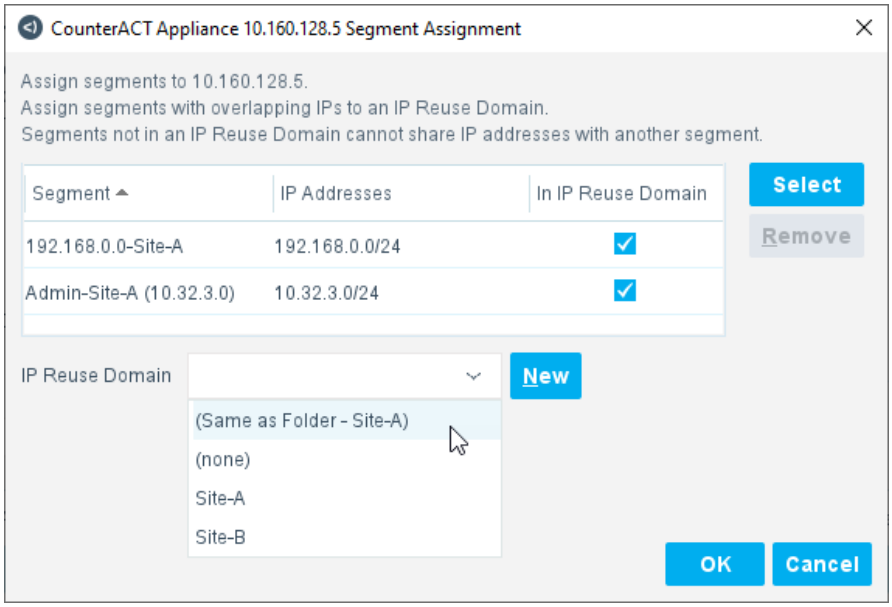
Site B	
Segment Name	**IP Range**
Overlap IPs Site B	192.168.0.0
Admin-Site-B	10.32.6.0

   Segments in Site A and Site B share overlapping IP addresses (192.168.0.0). Each site also has a segment without overlapping IP addresses, that should be configured as part of the default/global network.

4. As you assign segments to Appliances (**Options > CounterACT Devices > IP Assignment and Failover)**, define and apply IP Reuse Domains to distinguish sites with overlapping IP addresses.

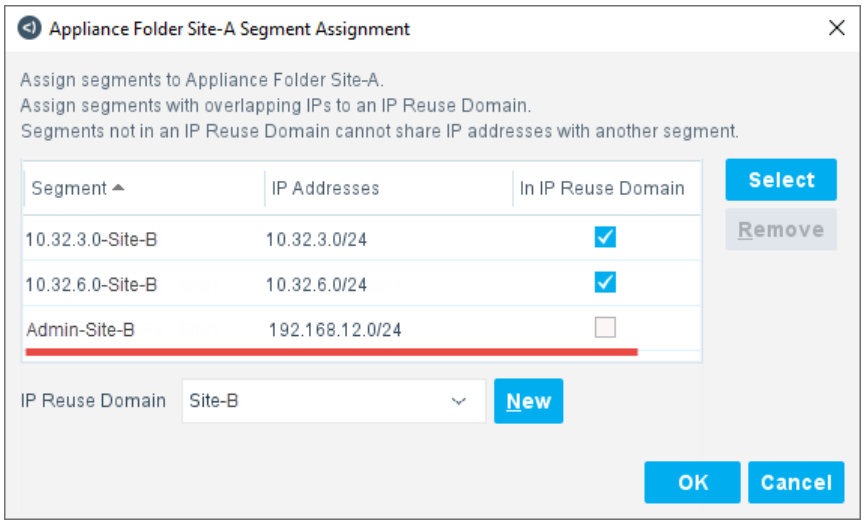
   a. Assign segments of an overlapping site to Appliance(s) or folder(s) dedicated to that site.

   b. In the IP Reuse Domain field, assign an IP Reuse Domain to the Appliance(s) or folder(s).



   c. (Optional) When an Appliance/folder is assigned to an IP Reuse Domain, you can exclude individual segments from the IP Reuse Domain. Clear the **In IP Reuse Domain** checkbox in the list of segments. The segment is in the default/global network.

   In the example shown, segment Admin-Site-B is excluded from the IP Reuse Domain, but is still managed by the Appliances that handle Site B. This segment is in the default/global network.



5. When the overlapping site contains switches, their Connecting Appliance must be within the IP Reuse Domain so that endpoints are reported with the IP Reuse Domain.
6. Repeat this procedure for the other sites. Assign overlapping sites to different Appliances and give Appliances of each site a unique IP Reuse Domain. The IP Reuse Domain uniquely identifies each instance of an overlapping IP address.
7. (In OT/automation environments) Map IP Reuse Domains in Operational Technology Environments. When the Operational Technology Module and other SilentDefense components are deployed in your environment, you must map the IP Reuse Domains you define in the Forescout platform to the IP Reuse Domains defined in Forescout SilentDefense components.
8. (Optional) If you use Splunk to process data from the Forescout platform, you must review and edit Splunk queries. See Reference IP Reuse Domains in Splunk Queries

Note that:

- Only areas of the Appliance tree that have overlapping IPs need to use IP Reuse Domains. All Appliance tree nodes that are *not* assigned to an IP Reuse Domain form a single default/global network. IP addresses must be unique in this default network.
- Segments that include IPv6 addresses cannot be placed in IP Reuse Domains. The larger IPv6 address space does not typically require overlapping addresses.
- Segments discovered based on their MAC address are not assigned to an IP Reuse Domain until their IP address is learned.
- To simplify management, it is strongly recommended to place all instances of overlapping IP addresses in IP Reuse Domains. Technically it is possible to keep a single instance of an overlapping IP address in the default/global network. This may be useful when a merge of new and existing networks causes overlap. The current network definition remains unchanged, and newly incorporated sites are assigned to one or more IP Reuse Domains.

Once you create and use IP Reuse Domains, you cannot disable support for overlapping IPs until you remove all IP Reuse Domain assignments and delete all defined IP Reuse Domains.

Map IP Reuse Domains in Operational Technology Environments

Overlapping network structures are commonly used in Operational Technology and other automation environments. The Operational Technology Module and Forescout SilentDefense components are typically deployed to support these environments. See the *Operational Technology Module Configuration Guide* for detailed information about the Forescout solution for Operational Technology/automation environments.

Both the Forescout platform and the SilentDefense solution use *IP Reuse Domains* to distinguish several instances of an overlapping IP address.

- In the Forescout platform, IP Reuse Domains are assigned to Appliances. Identical segments are distinguished from each other by the IP Reuse Domain of the Appliance that manages each segment.

- In SilentDefense, IP Reuse Domains are defined in the Command Center Console and assigned to selected Sensors.

Map the IP Reuse Domains of Forescout platform to the IP Reuse Domains of SilentDefense in the Operational Technology Module configuration pane.

Define Policy Scope with Overlapping IP Addresses

When you specify a segment with overlapping IP addresses in the scope of a policy, the IP Reuse Domain of the Appliance that manages the segment restricts the policy scope. Endpoints with the same IP addresses that are discovered outside this IP Reuse Domain are *not* in the scope of the policy.

In addition, you can use the **IP Reuse Domain** host property to explicitly match endpoints in specified IP Reuse Domains.

Deploy SecureConnector in Networks with Overlapping IP Addresses

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to the Forescout platform and implements actions on the endpoint.

To deploy SecureConnector on an endpoint, Appliances generate an installer package. This package can be downloaded to the endpoint as part of an interactive session with the end user or distributed in the background to corporate devices by the network administrator.

The installer refers to the address and port that the Appliance exposes for SecureConnector communication from the endpoint.

- In the default/global network, Enterprise Manager or other Appliances can redirect SecureConnector communication to the endpoint's home Appliance. A single installer package can be distributed across the network.
- In the part of the network that is configured with IP Reuse Domains, Appliances cannot redirect SecureConnector communication. In each overlapping site, SecureConnector must be downloaded from an Appliance in the site. Once installed, SecureConnector can only communicate with this Appliance. This is true even for endpoints in a segment that is logically part of the default/global network, and is excluded from the IP Reuse Domain.

Reference IP Reuse Domains in Splunk Queries

eyeExtend for Splunk integrates between the Forescout platform and Splunk. Support for IP Reuse Domains is asymmetrical: Splunk queries can retrieve the IP Reuse Domain value and use it to distinguish endpoints with overlapping IPv4 addresses in retrieved data. However, eyeExtend for Splunk cannot use the IP Reuse Domain to apply actions or adaptive response functions to an endpoint with an overlapping IP address.

Refer to the *Working with Overlapping IP Addresses How-to Guide* for guidelines to modify Splunk queries so they retrieve IP Reuse Domain information.

Feature Scope in This Release

This section summarizes the extent of support for overlapping IP addresses in this release. In subsequent releases, additional areas of the Forescout platform will support overlapping IP addresses.

- This release only supports deployments with up to 200 overlapping locations.
- This release does not support overlapping IP addresses in cloud environments such as AWS and Azure or in virtual environments such as VMWare and Hyper-V.
- You cannot configure multiple Wireless/SDN controllers with overlapping IP addresses, but when these controllers are managed by an Appliance in an IP Reuse Domain, they report endpoints with overlapping IP addresses. These endpoints receive their IP Reuse Domain from the controller's Connecting Appliance.
- Rogue Device detection (introduced in Forescout 8.1) is not supported for areas of the network configured with overlapping IP addresses.
- eyeExtend for Splunk supports use of IP Reuse Domain information in Splunk queries to differentiate endpoints with overlapping IP addresses. Other Extended Modules may not recognize IP Reuse Domains and have not been tested to confirm support for overlapping IP addresses.
- The following Forescout components do not support overlapping IP addresses:

CEF Plugin	DNS Enforce Plugin	eyeSegment Module	IOC Scanner Plugin
Flow Collector	User Scope (RBAC)	VPN Concentrator Plugin	Reports Plugin

Classification Enhancements

eyeSight classification has been enhanced in this version.

Template for Reclassification

Added a Reclassification template to create a policy to reclassify properties on devices connected to your network, following classification. The Reclassification policy template is available in the Classification templates folder. Use this template to correct incorrect classifications and classify unclassified devices. You can reclassify Function, Operating System, and Vendor and Model classification types. For details, refer to the *Forescout Administration Guide*, version 8.2, section "Reclassification Template".

Manual Classification of Vendor and Model

Added support of manual classification of Vendor and Model. You can select **Set Vendor and Model Classification** from the Classify actions. Use the action to override a Vendor and Model property value set by Primary Classification policies. For details, refer to the *Forescout Administration Guide*, version 8.2, section "Set Vendor and Model Classification".

Classification Enabled by Default

Forescout eyeSight automatically discovers classification properties: Function, Operating System, and Vendor and Model through **Options** > **Discovery** > **Inventory**. Classification information is available prior to the Primary Classification

policy template being configured or run. For details, refer to the *Forescout Administration Guide*, version 8.2, section "Classification Enabled by Default".

View How an Endpoint was Classified

Added Profile Sources, which provide a view of how the Primary Classification template and the Device Classification Engine classified an endpoint. In the **Profile** tab of the Primary Classification policy view, the Profile Sources are displayed to the right of the Function, Operating System, and Vendor and Model fields. For details, refer to the *Forescout Administration Guide*, version 8.2, section "How an Endpoint was Classified".

Classify Mobile Devices

Forescout eyeSight classifies mobile devices using a number of classification properties, such as Android, iOS, and Windows Mobile. The conditions and actions used to classify mobile devices are configured on the Sub-Rules pane of the Mobile Classification policy template. For details, refer to the *Forescout Administration Guide*, version 8.2, section "How Forescout eyeSight Detects Mobile Devices – Policy Condition".

Customer Verification

Licensed customers are requested to complete a one-time customer verification process during login. The verification process entails:

- Logging into the Forescout Customer Support Portal.
- Agreeing to allow Forescout to gather endpoint and system information from Appliances in your deployment and send it securely to the Forescout research servers. This information helps Forescout improve the security platform effectiveness.

Opting Out of the Program

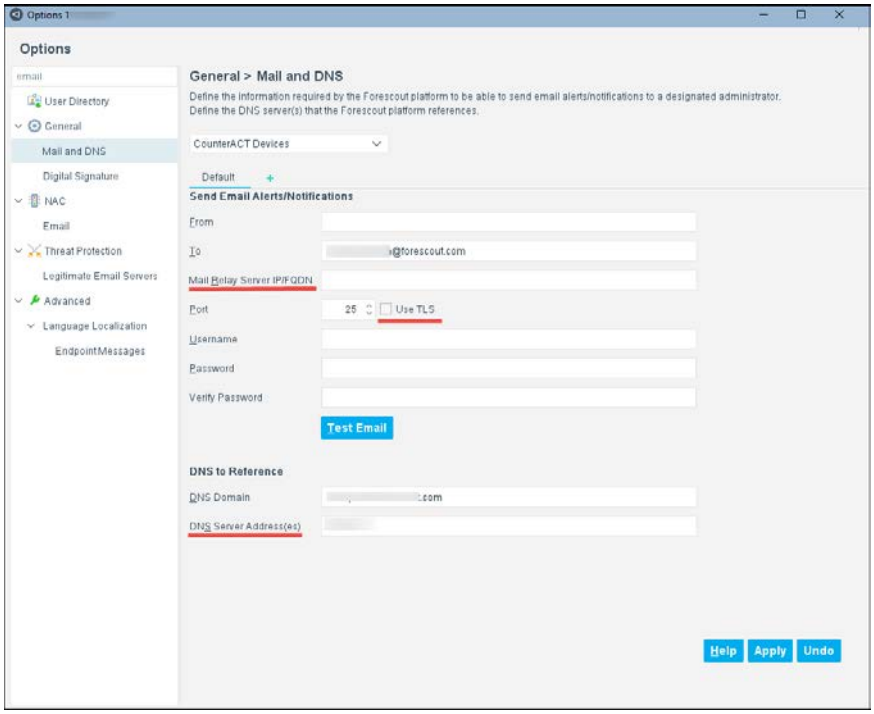
If you do not want to participate in the Forescout Research Program, you can opt out. In the Options pane, select **Advanced > Data Sharing**, and clear the **Share endpoint and system information with Forescout** option. If you completed the customer verification process and you would like to delete data that was already uploaded to the Forescout research servers, please contact Forescout Customer Care.

Cancelling the Verification Request

If there is no Internet connectivity, or if you do not want to complete the customer verification process, you can cancel the Customer Verification prompt. In the Options pane, select **CounterACT User Profiles > Password and Sessions**, select the **Login** tab, and clear the **Request customer verification** option.

Email Notification Enhancements

The following email notification enhancements have been introduced in this version.



- Mail Relay Server IP/FQDN: (optional) If your organization's network security policy requires the routing of incoming email through a mail relay server, enter that server's IP address [IPv4/IPv6] or FQDN.
- Use TLS: (optional) Enable / disable the Use TLS option.
  - If enabled (selected), the Forescout platform SMTP mail server uses TLS secure communication to send email alerts / notifications to the designated mail relay server.
  - If disabled (not selected), the Forescout platform SMTP mail server uses unsecured communication to send email alerts / notifications to the designated mail relay server.
- DNS Server Address(es): (optional) Enter the IP address [IPv4/IPv6] of each DNS server that the Forescout platform references. Comma-separate multiple entries.

Authentication Module 1.2

There are no new or changed features for module components in this release.

Core Extensions Module 1.2

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

- Cloud Uploader 1.0 – New Component
- Data Publisher 1.0 – New Component

Cloud Uploader 1.0 – *New Component*

The Cloud Uploader compresses data from Forescout devices and uses encrypted protocol to send the compressed data to Forescout cloud services where the data is processed and analyzed. The Cloud Uploader manages data upload for the following Forescout components:

- Forescout Research Program
- eyeSegment Module

Data Publisher 1.0 – *New Component*

The *Data Publisher* gathers device policy information from Appliances in your Forescout deployment and sends it to the *Data Receiver*. This information is used by the Device Compliance dashboard, an out-of-the-box dashboard included in the Dashboards view.

Data Receiver 1.0 – *New Component*

The *Data Receiver* receives and stores device policy information sent from the *Data Publisher*. This information is used by the Device Compliance dashboard, an out-of-the-box dashboard included in the Dashboards view.

Device Classification Engine 1.4

This section describes new and changed features for the Device Classification Engine.

Classification Enabled by Default

Forescout eyeSight automatically discovers classification properties: Function, Operating System, and Vendor and Model through **Options** > **Discovery** > **Inventory**. Classification information is available prior to the Primary Classification policy template being configured or run. For details, refer to the *Forescout Core Extensions Module: Device Classification Engine Configuration Guide*, version 8.2, section “Classification Enabled by Default”.

Manual Classification of Vendor and Model

Added support of manual classification of Vendor and Model. You can select **Set Vendor and Model Classification** from the Classify actions. Use the action to override a Vendor and Model property value set by Primary Classification policies. For

details, refer to the *Forescout Core Extensions Module: Device Classification Engine Configuration Guide*, version 8.2, section “Classify Actions”.

Device Data Publisher 1.0 – *New Component*

The Device Data Publisher gathers endpoint and system information from Appliances in your Forescout deployment and sends it securely to Forescout research servers. This information helps Forescout improve the security platform effectiveness.

External Classifier Plugin 2.3

If you use the FTP method to download the file that contains MAC addresses utilized by the External Classification property, the external classification property is now immediately updated every time that information on that file is changed.

Flow Collector 1.1

Flow Collector version 1.1 supports NetFlow v5 protocol, with or without Flexible NetFlow technology. This is in addition to the NetFlow v9, IPFIX, and sFlow protocols supported by the previous version. By default, Flow Collector uses port 9996 UDP to communicate NetFlow v5 data to the Forescout platform.

Packet Engine 8.2

This section describes new and changed features in the Packet Engine.

Support for RSPAN on Cisco Switches

Forescout eyeSight now supports RSPAN and uses it for discovery and endpoint traffic analysis purposes. For more information refer to the *Forescout Core Extensions: Packet Engine Configuration Guide.*

HTTP Actions

HTTP actions are now supported on IPv6 devices.

Configuration

Do one of the following to assign IPv6 devices to your CounterACT Appliance:

- Add the addresses during the installation wizard.
- Run the 'fstool netconfig' command after installation, and then restart the Appliance.

Considerations

For dual-stack endpoints (endpoints identified by both IPv4 and IPv6 addresses):

- Both addresses must be managed by the same Appliance.
- If an HTTP action is configured to use an Appliance DNS name, the DNS name must be the same for both addresses.
- When an IPv4 address is merged with an IPv6 address, an HTTP action that was applied to the IPv4 address replaces any HTTP action that was applied to the IPv6 address.

Automatically Calculated Values Upon Restart

For efficiency and to prevent packet loss, the following values are now automatically recalculated whenever the Packet Engine restarts:

- number of dispatcher threads
- affinity per thread

If you manually change either of these values after installing or upgrading to Packet Engine 8.2, the Packet Engine stops running, and the automatic recalculation of these values is disabled.

Start and Stop

The Packet Engine can now be started and stopped from the Options > Modules pane.

Segment Handling

Packet Engine version 8.2 offers improved action handling for segments that have many non-consecutive ranges.

CAPWAP Support

Packet Engine version 8.2 offers support for CAPWAP traffic and parsing.

Expanded DICOM Support

The DICOM parser now works on more TCP ports without requiring additional configuration. The default ports are:

104	4006	7100	12000
4000	4100	11112	12200

Technical Support Plugin 1.3

This section describes new and changed features in the Technical Support Plugin.

Health Monitoring Policies, Properties and Dashboard

This version of the plugin provides the following functionality related to Health Monitoring:

- ***Health Monitoring Policy Templates***. Use these templates to create health monitoring policies, enable the Health Monitoring Dashboard and populate specific widgets in the dashboard.
- ***Health Monitoring Properties***. Use these properties to help monitor Appliance health. These properties are included in policies created by Health Monitoring Policy Templates. You can also use these properties in custom policies.
- ***Health Monitoring Dashboard***. View at a glance, real-time data that helps you monitor and improve the health of Forescout Appliances in your deployment. Located in the Dashboards view, part of the Forescout Web Client. See Out of the Box Dashboards for more information.

Start and Stop

The Technical Support Plugin can now be started and stopped from the Options > Modules pane.

Endpoint Module 1.2

There are no new or changed features for module components in this release.

Hybrid Cloud Module 2.1

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

AWS Plugin 2.2

This section describes new and changed features in the AWS Plugin.

Support China Account and Regions

Accounts for AWS China can now be configured. If a connection is added using AWS China Account credentials, cn regions, such as cn-north-1, is displayed in the Regions pane.

Support Storage Access

The AWS Plugin now connects to the AWS public cloud environment to retrieve information on Amazon Simple Storage Service (S3).

S3 resources associated with an AWS account and the associated properties, such as name, owner, and tags can be collected. You can use policy templates to verify that an S3 bucket does not have public access. For those S3 buckets that have been misconfigured for public access, an action to block public access is provided.

Support Assume Role

The Assume Role option is supported when integrating the Forescout platform with AWS. The Assume Role provides the IAM user temporary security credentials that enable access to certain AWS resources in your account. The account can be either controlled by you or by a third party.

The Assume Role option is an alternative approach to defining the permissions at the individual account level.

Network Module 1.2

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

- Rogue Device Plugin 1.1
- Switch Plugin 8.14.1
- Wireless Plugin 2.0

Network Controller Plugin 1.0 – *New Component*

The Network Controller Plugin is a new plugin provided in Network Module 1.2. The plugin performs *eyeSight* management of centrally managed networks to:

- Discover (detect) both its network devices and the endpoints that connect to these network devices
- Report both endpoint and network device information in the Forescout Console. See Resolved Properties.

The plugin also provides the operator with the capability to apply *eyeControl* actions on connected, targeted endpoints, either by Forescout policy evaluation or by manual initiation of these actions. See Plugin-Provided Actions. The Network Controller Plugin accomplishes its monitoring and action application by means of communicating with the management interface of the centrally managed network.

A new Forescout content module - the Network Controller Content Plugin - supplies the Network Controller Plugin with product definitions about vendor centrally managed networks/network devices. The installed Network Controller Content Plugin is a required component for Network Controller Plugin operation.

Each set of product definitions supplies the Network Controller Plugin with the necessary information to support integration with specific vendors' centrally managed networks/network devices so that the Network Controller Plugin can manage these devices, using its eyeSight and eyeControl capabilities. Based on product definitions supplied by the Network Controller Content Plugin (NCCP), specific features and capabilities that the Network Controller Plugin (NCP) supports can vary per vendor centrally managed networks/network device.

This content module enables Forescout to release regular, ongoing Network Controller Content Plugin updates for Network Controller Plugin use. These updates always provide additional product definitions that enable the Network Controller Plugin to integrate with additional vendor centrally managed network solutions without having to upgrade the Network Controller Plugin.

For this version, the Network Controller Plugin integrates with the following, vendor centrally managed network solutions:

- Cisco Meraki (cloud based solution)
- Ruckus SmartZone (premise based solution)

This new NCP-NCCP relationship is transparent to NCP configuration and management. For additional information, refer to the *Forescout Content Module: Network Controller Content Plugin Release Notes*. See Additional Forescout Documentation for information on how to access this guide.

Resolved Properties

The plugin resolves the following categories of property information:

- Network Controller Properties

- Switch Properties (a subset of available switch properties)
- Wireless Properties (a subset of available wireless properties)
- Track Changes Properties (Network Controller, Switch and Wireless)

Plugin-Provided Actions

The Network Controller Plugin provides Forescout eyeControl actions that apply control on endpoints. You can incorporate these actions in policies and you can also manually apply these actions on detected endpoints that you select. In the Forescout Console, find these actions in the *Restrict* action group. The plugin provides the following actions:

- Assign to VLAN-Network Controller
- Block Network Access

  Currently, this is the only eyeControl action that the plugin supports for use in Ruckus SmartZone networks

- Restrict Network Access
- Whitelist Network Access

Periodic policy re-evaluation, by the Forescout platform, may cancel currently applied actions; you can also manually cancel currently applied actions. The plugin provides the following cancel actions:

- Cancel Block Network Access

  Currently, this is the only eyeControl cancel action that the plugin supports for use in Ruckus SmartZone networks

- Cancel Restrict Network Access
- Cancel VLAN Assignment-Network Controller
- Cancel Whitelist Network Access

For additional information about plugin configuration and capabilities, refer to the *Forescout Network Module: Network Controller Plugin Configuration Guide*. See Additional Forescout Documentation for information on how to access this guide.

Rogue Device Plugin 1.1

This section describes new and changed features in the Rogue Device Plugin.

Expanded Sub-Rule Specificity for the MAC Spoofing Policy Template

The available MAC Spoofing Tracking policy template provides expanded and more granular specificity to identify and group detected spoofing attackers. With this version, the existing policy template sub-rule *Detected Spoofing Attacker* morphs into and is replaced by the following distinct, policy template sub-rules:

- **Detected Spoofing Attacker - MAC address port changes**: Endpoints matching this sub-rule's condition are the *spoofing attacker* in a suspected MAC spoofing event that the plugin identified using its *Detect MAC Address Appearances on Different Ports* method.

- **Detected Spoofing Attacker - Character of device changes**: Endpoints matching this sub-rule's condition are the *spoofing attacker* in a suspected MAC spoofing event that the plugin identified using its Detect Changes in Character of Device method.

For details about Rogue Device Plugin detection methods, refer to the *Forescout Network Module: Rogue Device Detection and Prevention How-to Guide*. See Additional Forescout Documentation for information on how to access this guide.

Switch Plugin 8.14.1

This section describes new and changed features in the Switch Plugin, as follows:

- New Content Module Facilitates Plugin Integration with Vendor Devices
- Configure Plugin Use of CyberArk Enterprise Password Vault for CLI Access
- Plugin eyeSight Management of Additional Layer 3 Devices
- Plugin Adds Use of Access Port ACL Action on Dell DNOS 9.x Switches
- Plugin Extends eyeSight and eyeControl Capabilities on Arista Switches

New Content Module Facilitates Plugin Integration with Vendor Devices

With this version, a new Forescout content module - the Switch Content Plugin - supplies the Switch Plugin with product definitions about vendor network devices. The installed Switch Content Plugin is a required component for Switch Plugin operation.

Each set of product definitions supplies the Switch Plugin with the necessary information to support integration with specific vendors' network device(s) so that the Switch Plugin can manage these devices, using its eyeSight and eyeControl capabilities. Based on product definitions supplied by the Switch Content Plugin (SCP), specific features and capabilities that the Switch Plugin (SWP) supports can vary per vendor network device.

This content module enables Forescout to release regular, ongoing Switch Content Plugin updates for Switch Plugin use. These updates always provide additional product definitions that enable the Switch Plugin to integrate with additional vendor network devices without having to upgrade the Switch Plugin.

For this version:

- SCP 1.0 supplies the SWP with product definitions for 12 vendor network devices; some are new network device integrations, and some are existing network device integrations.
- All other, existing, vendor network device integrations remain implemented in the Switch Plugin itself.

This new SWP-SCP relationship is transparent to SWP configuration and management. For additional information, refer to the *Forescout Content Module: Switch Content Plugin Release Notes*. See Additional Forescout Documentation for information on how to access this guide.

Configure Plugin Use of CyberArk Enterprise Password Vault for CLI Access

With this version, when configuring the plugin to use CLI commands to manage a network device, you have the option of defining the source that supplies the password for plugin CLI access of the managed device. The *Password source* field is available for defining both CLI access and privileged CLI access. The available password source options are:

- *Local*: The *Local* option is the default selection. If selected, the *Password* field becomes available for data entry.
- *CyberArk*: The *CyberArk* option instructs the plugin to query the CyberArk Enterprise Password Vault to retrieve the required password for CLI access of the managed switch. The *CyberArk Query* dialog opens for data entry.

With this version, the Switch Plugin provides you with the capability to define the *CyberArk Query* to retrieve the required password for plugin CLI access and/or privileged CLI access of multiple, managed switches, for any of the following password scenarios:

- Define Local Password for CLI Access
- Define Local Password for Privileged CLI Access
- Define CyberArk Account Query for CLI Access
- Define CyberArk Account Query for Privileged CLI Access

To perform these password definitions, you must run the new, interactive fstool command **`cli-password`**.

Plugin eyeSight Management of Additional Layer 3 Devices

With this version, the Switch Plugin expands its portfolio of Layer 3 network devices that it can manage to include the following vendor devices:

- Cisco Firepower Firewall
- SonicWall Firewall
- Cisco Viptela SD-WAN
- SilverPeak SD-WAN

Using CLI commands, the plugin provides its Forescout eyeSight management of these devices, as follows:

- Detects the Layer 3 network devices and the endpoints connecting to/disconnecting from these devices (reads device ARP table)
- In the Forescout Console, the plugin reports Layer 3 device and endpoint property information that it obtains by periodic query of the managed Layer 3 devices

Plugin Adds Use of Access Port ACL Action on Dell DNOS 9.x Switches

With this version, the Switch Plugin provides its Forescout eyeControl capability - the *Access Port ACL* action - for use on plugin-managed Dell Networking-DNOS v9.x switches. When adding/editing plugin management of these switches, the *ACL* tab/pane is made available. In this tab/pane, you can enable the plugin to use the *Access Port ACL* action on these switches.

> *Use of the* Access Port ACL *action in your Forescout deployment requires you to globally enable the use of this type of ACL action by configuring the advanced configuration flag* ***acl_action_type***

Use the *Access Port ACL* action to define an ACL that addresses one or more than one access control scenario. Then, either by policy evaluation or manual initiation, the plugin applies the action's ACL on the switch access port of targeted endpoints.

Plugin Extends eyeSight and eyeControl Capabilities on Arista Switches

With this version, the Switch Plugin executes the following Forescout eyeSight and eyeControl capabilities on managed Arista switches:

- Endpoint detection and action application on switch VoIP ports
- Resolution of Power over Ethernet (PoE)-enabled switch port information

Switch VoIP Ports

Using CLI commands, the plugin -

- Detects connected VoIP endpoints and endpoints that connect through the VoIP endpoints to the Arista switch
- Reports detected endpoint information in the Forescout Console.
- Applies the *Assign to VLAN* action and the *Switch Block* action on endpoints connected to Arista switch VoIP ports.

PoE Port Information

Using CLI commands, the plugin resolves property information of Arista PoE-enabled switch ports, as follows:

Property	Description
Switch Port PoE Connected Device	Description of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed switch.
Switch Port PoE Power Consumption	Power consumption of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed switch. The power consumption value provided is in milliwatts (mW). For example, 750. When either a non-PoE device or no device is connected to the PoE-enabled switch port, the property value is zero (0).
Switch Port PoE Connected Device Change	Identifies a change in PoE device that is connected to the PoE-enabled switch port.
Switch Port PoE Power Consumption Change	Identifies a change in power consumption of the PoE device that is connected to the PoE-enabled switch port.

Wireless Plugin 2.0

This section describes new and changed features in the Wireless Plugin.

Added eyeSight Management of HP Controller

With this version, the Wireless Plugin expands its portfolio of wireless network devices that it can manage to include the following vendor device:

- HP 830 WLAN controller

Using CLI commands, the plugin provides its Forescout eyeSight management of this device, as follows:

- Detects the wireless network device and the endpoints connecting to/disconnecting from this device
- In the Forescout Console, the plugin reports wireless device and endpoint property information that it obtains by periodic query of managed HP 830 WLAN controllers.

Operational Technology Module 1.2

This section describes new and changed features in the Operational Technology Module.

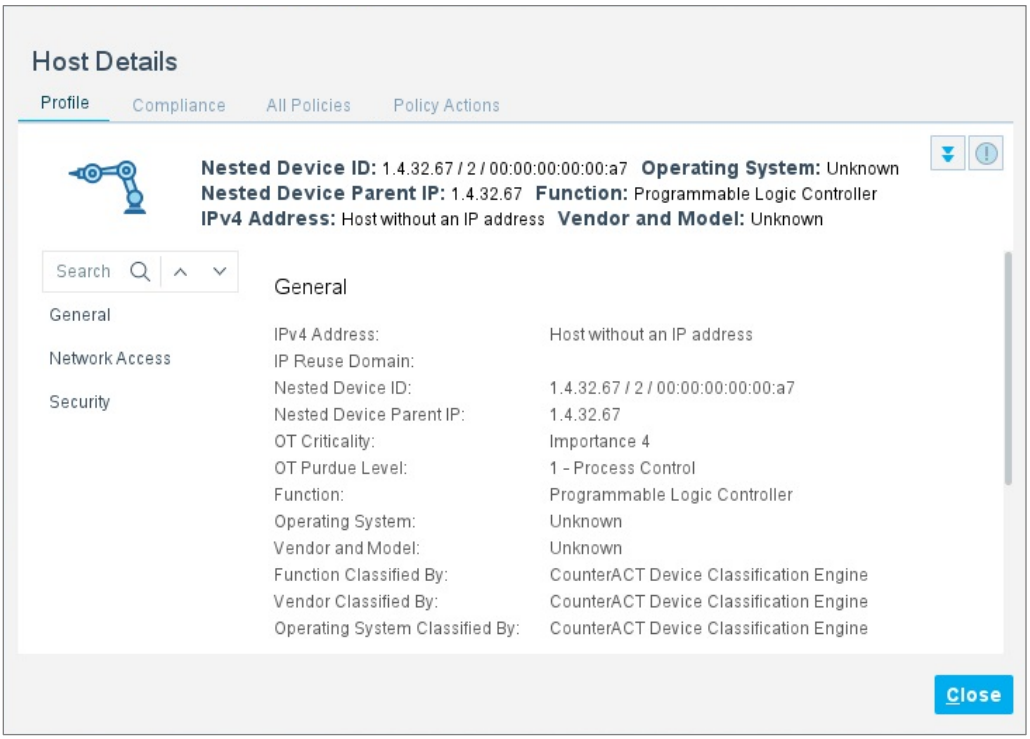
Nested Device Management

SilentDefense detects devices with nested or cascading IP addresses. When a controller or other endpoint integrates sub-modules or PLCs, Deep Packet Inspection of industrial protocols, such as BACnet and EtherNet/IP, identifies these children based on traffic from the parent. Endpoint properties report this information in Forescout. Typical applications include:

- Most Building Automation (BA) deployments nest devices. Typically, the building management system (BMS) monitors and controls controllers within a floor or room (for example, door locks and room temperature controllers) through an intermediate floor or room controller/router.
- In Industrial Control Systems (ICS) nesting provides efficient scalability: DCS/SCADA servers communicate only with the main controller, which then mediates the communication to the secondary nested controllers.

With this release, you can work with nested device information in the Forescout platform. SilentDefense components identify these child devices based on deep analysis of traffic from the parent. Command Center reports information about nested devices via the Operational Technology Module.

In the Console screen shown below, the IP address exposed by the parent device is 1.4.32.67. Sub-modules are identified by strings appended to the parent IP address. The format of these strings varies with the configuration and internal protocol of the nested device.



Use the following host properties to work with this information in Forescout.

Nested Device ID	The full string used to identify a sub-module or nested device, including the parent IP address.
Nested Device Parent IP	The IP address of an endpoint that contains sub-modules or nested devices.

Support for Overlapping IP Addresses

Networks in plant/production, building automation, and other Operational Technology environments often contain duplicate sites and network structures. IP addresses repeat, or *overlap*, across the network.

To support these networks, the Forescout platform and the SilentDefense solution use *IP Reuse Domains* to distinguish several instances of an overlapping IP address. You define a unique IP Reuse Domain for each repeated segment or network branch. IP addresses are unique in each IP Reuse Domain.

- In the Forescout platform, IP Reuse Domains are assigned to Appliances. Identical segments are distinguished from each other by the IP Reuse Domain of the Appliance that manages each segment.
- In SilentDefense, IP Reuse Domains are defined in the Command Center Console and assigned to selected Sensors.

For more information see Working with Overlapping IP Addresses.

New Traffic Inspection Library Module

The Traffic Inspection Library packages regular updates of the knowledge base used for protocol parsing and other aspects of traffic/packet analysis. These regular updates make new insights and developments of the SilentDefense product team immediately available in the Forescout platform, where they work in synergy with other device classification tools.

Fixed Issues

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

Forescout Platform 8.2

This section describes fixed issues for this release.

Issue	Description
CA-24602	The Forescout Specifications Guide did not align with the internally generated capacity calculations.
CA-24585	Machine type capacity presented in the Forescout GUI did not match the capacity stated for each virtual machine in the Forescout Appliance Specifications Guide.

Authentication Module 1.2

This section describes fixed issues for this release.

Component	Issue	Description
RADIUS	**DOT-3159**	The plugin did not support the Protected EAP-TLS (PEAP-EAP-TLS) authentication protocol, and did not extract the supplicant user name (tunneled user name) used for the inner authentication phase of Protected EAP-MSCHAPv2.
	DOT-3650 **DOT-3760**	When Accounting was enabled, the RADIUS Plugin received a Framed-IP-Address from the NAS server as an update to the endpoint address, even when the endpoint was in transition between IP addresses assignments, or was off-line.

Component	Issue	Description
User Directory	**UD-1239**	During switch-over, tags were not copied from the Enterprise Manager to the Recovery Enterprise Manager.

Core Extensions Module 1.2

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

Endpoint Module 1.2

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

Hybrid Cloud Module 2.1

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

Network Module 1.2

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

Operational Technology Module 1.2

There are no fixed issues in this release.

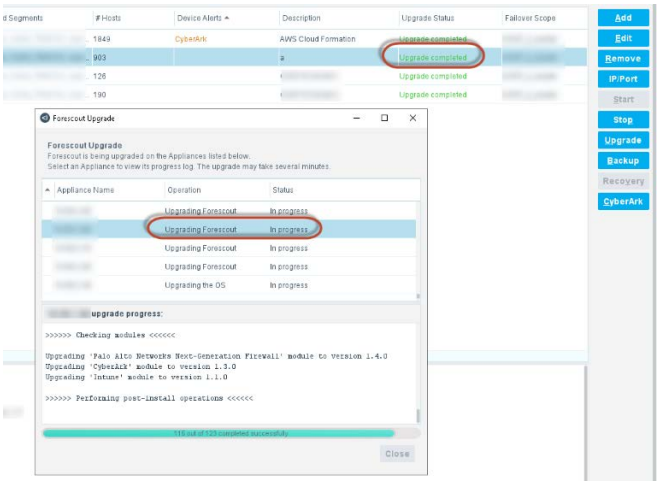
Known Issues

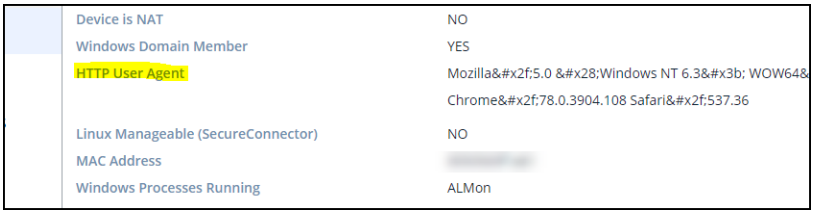
This section describes known issues for the Forescout platform and Base Modules.

Forescout Platform 8.2

This section describes known issues for this release.

Issue	Description
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.
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-24435	When reassigning segments from one appliance to another, the message "Loading completed from X our of X Appliances. Appliances omitted due to slow responsiveness" appears.
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.

Issue	Description
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.
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*. 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. 

Issue	Description
CA-26114	When support for overlapping IP addresses is enabled, **the `fstool devinfo`** command does not work for Appliances with IP Reuse Domains.
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

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

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 Irresolveable for these endpoints.

Component	Issue	Description
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*.
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.
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.
	PE-761	The Packet Engine experiences a core dump in the audit trails due to a segmentation fault. This issue is extremely intermittent.

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-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.

Endpoint Module 1.2

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.
	HPS-28067 3636	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.

Component	Issue	Description
	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

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.
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.

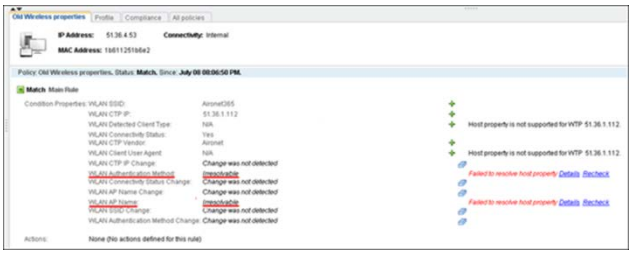
Network Module 1.2

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.

Component	Issue	Vendor	Description
	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.
	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
	SW-4974	Cisco, Arista	For a brief, temporary period after Switch Plugin restart, the plugin inaccurately reports managed switch PoE property information, **Switch Port PoE Connected Device** and **Switch Port PoE Power Consumption**, as N/A and 0 respectively.
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.

Operational Technology Module 1.2

This section describes known issues for this release.

Issue	Description
OT-545	Command Center mistakenly identifies endpoints running some Linux flavors as Windows endpoints. These endpoints appear in the Forescout platform as Windows endpoints.
OT-546	Command Center may not display/update IP Reuse Domain information for some detected endpoints.
OT-562	In rare instances, the OT Module may mistakenly report an endpoint that went offline as online, even though the endpoint was not re-detected online.
OT-565	When Command Center reports information for endpoints with nested devices to the Forescout platform, it does not report the client/server protocols used between the endpoint and its nested devices. ***Workaround***: This information is available in the Command Center console.

Issue	Description
PE-912	COST | V8.2 | Packet Engine reset detected at virtual VMWARE appliance when PE incoming set to Eth1 and OTSM plugin set to Eth3 (Ethernet drivers are e1000)
PE-915	When an Integrated Sensor uses the same interface that the Packet Engine running on the Appliance uses as a monitoring interface, the Packet Engine repeatedly drops a significant number of packets. This packet loss degrades See and Control capabilities. ***Workaround***: To identify the interfaces configured for Packet Engine monitoring: **1.** In the Console, open the Options window. **2.** In the CounterACT Devices pane, double-click the Appliance. In the Details dialog, select the Channels tab. Channels are listed as Monitor-Response pairs. Defined channels are listed under the Channels button. **3.** To view details, double-click a channel or select Channel>Add or Channel>Edit. When you activate an Integrated Sensor, do not select an interface that is configured as a Monitoring interface.

Important Considerations

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

Forescout Platform 8.2

This section describes important considerations for the Forescout platform.

Dashboard Considerations

- Updated Dashboard Policies
- Pre-8.2 Legacy Widgets
- Running the Dashboard Policies Template – Weak Credentials Policy

Updated Dashboard Policies

If you worked with the Dashboard (Web Client) in previous Forescout versions, it is important to run the Dashboard Policies template again in Forescout 8.2 even if you already ran it in a previous version. Be aware that running this template removes outdated policies from your system that were added in previous versions.

The policies this template provides have been updated as followed:

Added in 8.2	Removed in 8.2	Carried over from 8.1
Device Compliance	Device Classification*	Campus Wired
IoT Devices	Non-Compliant Endpoints by Operating System**	Campus Wireless

Added in 8.2	Removed in 8.2	Carried over from 8.1
Cleartext Ports Open	Non-Compliant Endpoints**	OT Network
Weak Credentials		Computer Manageability
Legacy OS		Data Center (previously part of unified Data Center/Cloud policy)
Unauthorized Windows Applications Installed		Cloud (previously part of unified Data Center/Cloud policy)

**The information previously provided by this policy is now provided by Forescout classification properties.*

***The information previously provided by these policies is now provided by any compliance policies containing sub-rules categorized as Not Compliant. These compliance policies populate new widgets in the Device Compliance Dashboard that give additional insight into non-compliant endpoints.*

Pre-8.2 Legacy Widgets

Any custom Dashboard widgets that you created in version 8.1 is retained and moved to a dedicated *Legacy Widgets* dashboard.

Running the Dashboard Policies Template – Weak Credentials Policy

Running the Dashboard Policies template in the Forescout Console creates policies that populate widgets in out-of-the-box dashboards. One of these policies is *Weak Credentials*, which populates the IoT Devices at Risk widget. This policy contains a *Commonly-Used Credentials* sub-rule, which attempts to find devices that use commonly used credentials.

By default, the policy scope includes all devices on the network. Forescout checks for commonly used credentials on SSH and Telnet via login attempts, which may be interpreted as brute force attacks by devices or third-party security systems. If such a concern exists, Forescout recommends limiting the policy scope or adjusting the sub-rule accordingly.

Changes to Password Requirement Default Settings

For enhanced security, the Forescout password requirement default settings have changed in this version. Most settings are now enabled by default, and the default values have changed.

- Upgrade to 8.2:
  - If you made any changes to the default password settings in 8.1.x (pre-upgrade), all your password settings are preserved after upgrade to 8.2. Default settings for 8.1.x are listed below.
  - If you did not change any default password settings in 8.1.x (pre-upgrade), the default settings are changed, as listed in the 8.2 column in the table below.

- Clean install of 8.2:
  - Password default settings are changed, as listed in the 8.2 column in the table below.

Password Setting	8.1.x (Default)	8.2 (Default)
Minimum (min) length	6	15
Min. upper case alphabetic characters	1 Disabled	3 Enabled
Min. lower case alphabetic characters	1 Disabled	3 Enabled
Min. digits	1 Disabled	3 Enabled
Min. special characters	1 Disabled	3 Enabled
Min. forbidden repeated characters/digits	2 Disabled	2 Enabled
Min. characters that password must differ from previous	4 Disabled	4 Enabled
Must not contain user name	Disabled	Enabled
Must not contain commonly user weak passwords	Disabled	Enabled
Last amount of passwords that cannot be reused	1 Disabled	6 Enabled
Password expires after	30 days Disabled	60 days Enabled
Lock user account after days without login	35 days Enabled	15 days Enabled
Lock user account after failed logins	3 failed logins for 30 minutes Enabled	3 failed logins for 15 minutes Enabled
Limit password change to once every	24 hours Disabled	3 days Enabled
User must change password at next login if changed by admin user	Disabled	Disabled

Primary Classification Policy

Upgraded versions of Forescout might include legacy Asset Classification policies that provide limited information about endpoints. To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies.

The Primary Classification policy provides more comprehensive classification in your environment than legacy Asset Classification policies. To use it as your primary classification policy, ensure that the Add to Group actions are enabled in the Primary

Classification policy, and use the Policy Manager to stop your Asset Classification policies.

Legacy NetFlow Plugin Deprecated

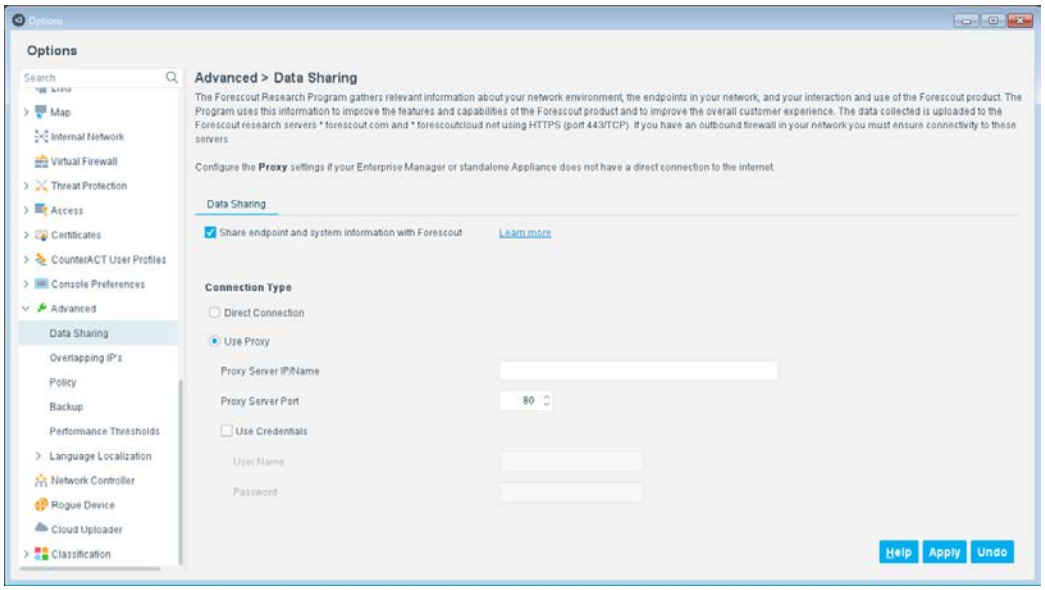
With the availability of the Forescout Flow Collector, the legacy NetFlow Plugin is deprecated. The Flow Collector provides more accurate and stable traffic flow detection and more scalable bandwidth capabilities than the NetFlow Plugin. It is recommended to configure and enable the Flow Collector, and then stop and uninstall the NetFlow Plugin.

VMware Virtual Machine Total Disk Space Requirement

When installing/upgrading VMware virtual Forescout devices to this version, be aware that the virtual machine file requires at least 200 GB of total disk space.

Console Changes

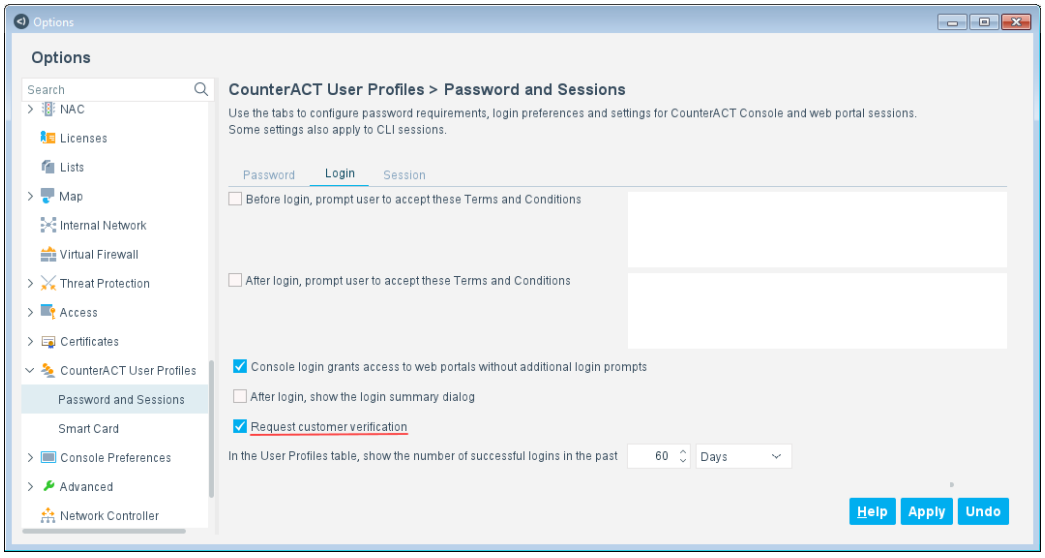
- The **Options > Advanced > Data Sharing** pane has been changed.



  - The *Forescout Research and Intelligent Analytics Program* has been replaced by the *Forescout Research Program version 2.0*.
  - Instead of having different options for sharing different types of data, there is now only one option for sharing all data:

    Share endpoint and system information with Forescout
  - Instead of requiring the user to select checkboxes to opt in to share data, the data sharing checkbox is now selected by default.

- A new **Request customer verification** checkbox has been added to the **Options > CounterACT User Profiles > Password and Sessions > Login** tab.



When this checkbox is selected, a Customer Verification process is initiated at each user login until the user completes the process one time. The checkbox is selected by default.

Core Extensions Module 1.2

This section describes important considerations for the following components of the Core Extensions Module.

- Flow Collector 1.1

Flow Collector 1.1

With the availability of the Forescout Flow Collector, the legacy NetFlow Plugin is deprecated. The Flow Collector provides more accurate and stable traffic flow detection and more scalable bandwidth capabilities than the NetFlow Plugin. It is recommended to configure and enable the Flow Collector, and then stop and uninstall the NetFlow Plugin.

If both plugins run concurrently, ensure that the **Port for NetFlow communication** field in the NetFlow Plugin configuration does not contain any of the ports used by the Flow Collector.

Endpoint Module 1.2

This section describes important considerations for the following components of the Endpoint Module.

- HPS Inspection Engine 11.1

HPS Inspection Engine 11.1

If you have customized the directory to which SecureConnector and/or Remote Inspection scripts are downloaded to and run from, or if you want to customize this directory, consider the following changes:

- Directory Customization for SecureConnector Scripts
- Directory Separator in the Customization of the Script Directory

For more information, refer to the section on *Script Execution Services* in the Forescout Endpoint Module: HPS Inspection Engine 11.1 Configuration Guide.

Directory Customization for SecureConnector Scripts

- A new script is used to customize the directory for SecureConnector scripts: **`config.sc_script_run_folder.value.`**

  (Instead of: **`config.script_run_folder.value)`**
- Unless re-customized by use of the above script, Forescout eyeSight now reverts to the ***default directory*** (***not*** the previously customized directory).
- The above script has the additional requirement of user access.

*These changes do **not** affect the Remote Inspection script directory settings.*

Directory Separator in the Customization of the Script Directory

You now need to use a double backlash (\\) or a single forward slash (/) as a directory separator. This is because the Enterprise Manager reads a single backlash as an escape character.

This change affects both the Remote Inspection and the SecureConnector script directory settings.

Network Module 1.2

This section describes important considerations for the following components of the Network Module.

- Switch Plugin 8.14.1

Switch Plugin 8.14.1

Use CLI for Brocade and Dell IPv4 Switches Being Managed

After upgrading the Switch Plugin to 8.14.1 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

If the plugin is configured to manage any of these switches with either read or read/write ARP table permissions, 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.

Modules Packaged with This Release

When you install or upgrade to Forescout 8.2, 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
  - Core Extensions Module 1.2
  - Endpoint Module 1.2
  - Hybrid Cloud Module 2.1
  - Network Module 1.2
  - Operational Technology 1.2
- Content Modules:
  - Device Profile Library 20.1.1
  - IoT Posture Assessment Library 19.0.12
  - NIC Vendor Database 19.0.12
  - Network Controller Content Plugin 1.0 (***NEW***)
  - Security Policy Templates 19.0.12
  - Switch Content Plugin 1.0 (***NEW***)
  - Windows Applications 19.0.12
  - Windows Vulnerability DB 19.0.12

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

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 Version 8.2.

Previous Releases

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

Prior to this release, Base Module fixes and enhancements were documented in separate Release Notes.

Forescout Platform

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 Forescout Technical Documentation Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

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

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

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

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 Support Portal

The Downloads page on the Forescout Customer Support 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 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

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 **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**.

Documentation Portal

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