Forescout

Enterprise Manager / Appliance

Technical Notes

Forescout versions 8.1.4 and 8.2.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

2020-07-31 11:36

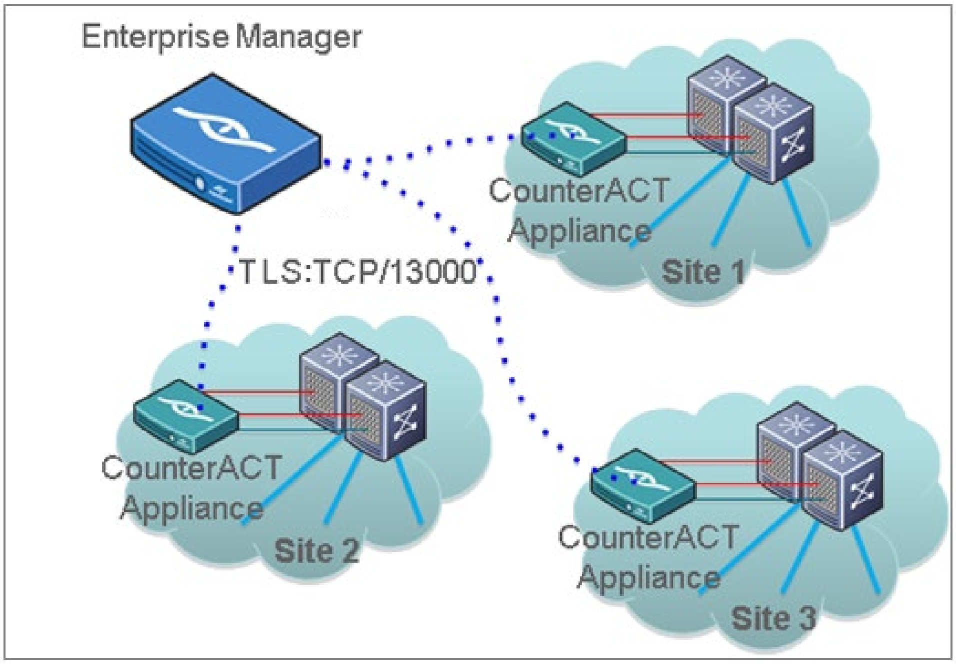
Table of Contents

About this Document

This document presents information regarding Enterprise Manager/Appliance communication. The information refers to Forescout 8.x systems.

Enterprise Manager/Appliance Communication Overview

Communication between the Enterprise Manager and Appliances is performed using a proprietary protocol over TLS on TCP port number 13000. All TCP sessions are initiated by the Enterprise Manager to the Appliances.



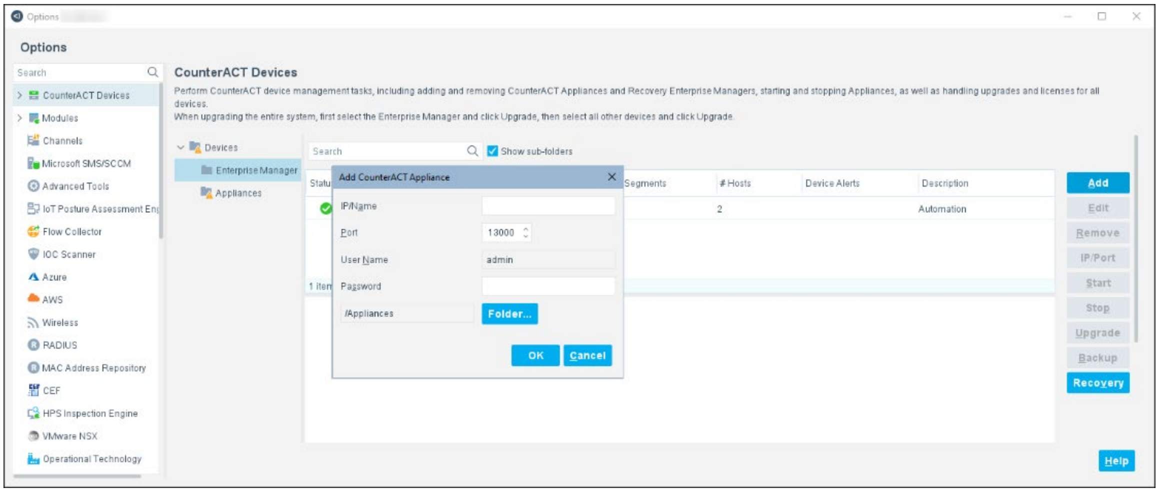
Authentication

When an Appliance is added to the Enterprise Manager, the Enterprise Manager administrator provides the Appliance’s admin username and password.

These credentials are used for the initial authentication. If the authentication is successful, the Appliance stores the Enterprise Manager public key in its keystore.

Future connections from the Enterprise Manager to the Appliance are authenticated using key authentication.

Since Forescout version 8.14, the Forescout platform can also ensure secure communication between Enterprise Managers and Appliances through customer issued CA certificates. Customers can generate certificate sign requests to a CA Service and import the signed certificate, and its certificate chains for each Enterprise Manager and Appliance. See “Inter-Enterprise Manager and Appliance Authentication” in the *Forescout Administration Guide* for complete details.



CounterACT Devices

Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery Enterprise Managers, starting and stopping Appliances, as well as handling upgrades and licenses for all devices.
When upgrading the entire system, first select the Enterprise Manager and click Upgrade, then select all other devices and click Upgrade.

☑ Show sub-folders

Segments	# Hosts	Device Alerts	Description
	2		Automation

Add CounterACT Appliance

IP/Name:
Port: 13000
User Name: admin
Password:
/Appliances [Folder...]
[OK] [Cancel]

Sessions Life Cycle

When the Enterprise Manager connects to an Appliance, it initiates a set of short-lived TCP sessions to perform an extensive range of synchronization tasks. Examples of major tasks performed include:

- Tasks related to disconnected Appliances:
  - Installing plugins that were installed at the Enterprise Manager during disconnection.
  - Copying repository files that were uploaded to the Enterprise Manager during disconnection.
  - Synchronizing the status of remote endpoint actions that were issued or cancelled during disconnection.
  - Synchronizing configurations that changed during disconnection.
- Synchronizing the Appliance status: Running/stopped plugins, packet-engine status etc.
- And more

Once the synchronization sessions are complete, the Enterprise Manager issues a single permanent session that is used to send messages both from the Enterprise Manager to the Appliance and from the Appliance to the Enterprise Manager.

When the Enterprise Manager/Appliance connection disconnects, the Enterprise Manager attempts reconnection to the Appliance every 10 seconds, until it succeeds.

Information and Requests Sent from the Enterprise Manager to Appliances

The Enterprise Manager sends an extensive range of both information and requests to system Appliances. Examples of typical information sent/requested include:

- Information regarding:
  - License distribution
  - Appliance software upgrades
  - Changes to IP assignments at Appliances
  - Configurations, for example policy changes, segments, plugin configuration
  - and more
- Starting and stopping Appliances
- Detections pane information or filtered information. Messages are sent from the Enterprise Manager to all network Appliances requesting that relevant information be returned for display.
- Request to receive system and component backup files
- Requesting information for Web reports
- and more

Refer to the *Forescout Administration Guide* for more information about these features or navigate to the Forescout Console online Help.

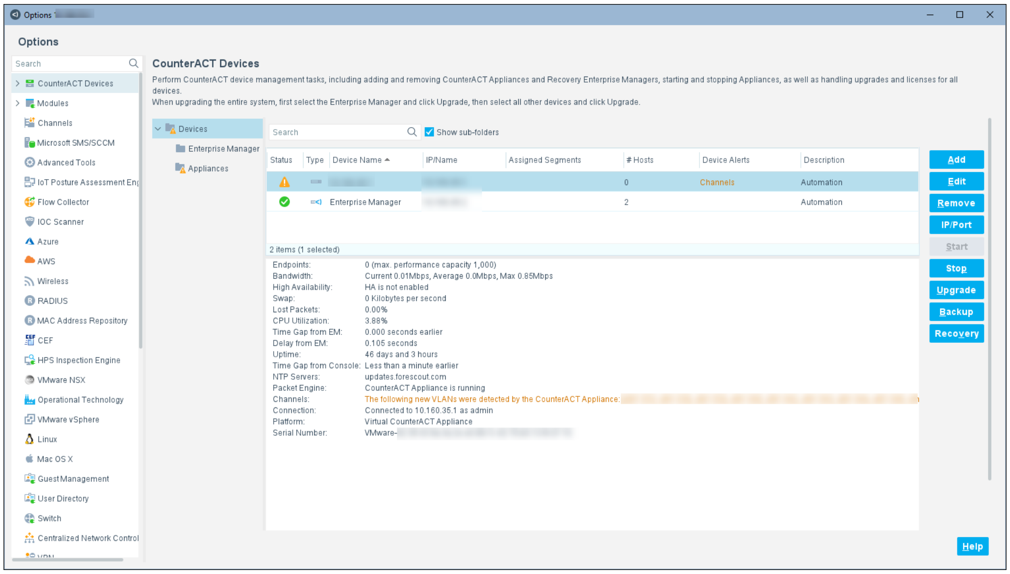
Information Sent from Appliances to the Enterprise Manager

Appliances communicate an extensive range of information to the Enterprise Manager.

> 🗎 *Starting from Service Pack 2.2.0, Appliances can communicate certain information directly with one another when possible instead of through the managing Enterprise Manager. If this service pack is not installed, this information will continue to be routed via the Enterprise Manager. See Direct Inter-Appliance Communication for details.*

Examples of typical information sent include:

- Appliance health information, displayed in the Enterprise Manager Console, CounterACT Devices Status pane.



CounterACT Devices

Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery Enterprise Managers, starting and stopping Appliances, as well as handling upgrades and licenses for all devices.
When upgrading the entire system, first select the Enterprise Manager and click Upgrade, then select all other devices and click Upgrade.

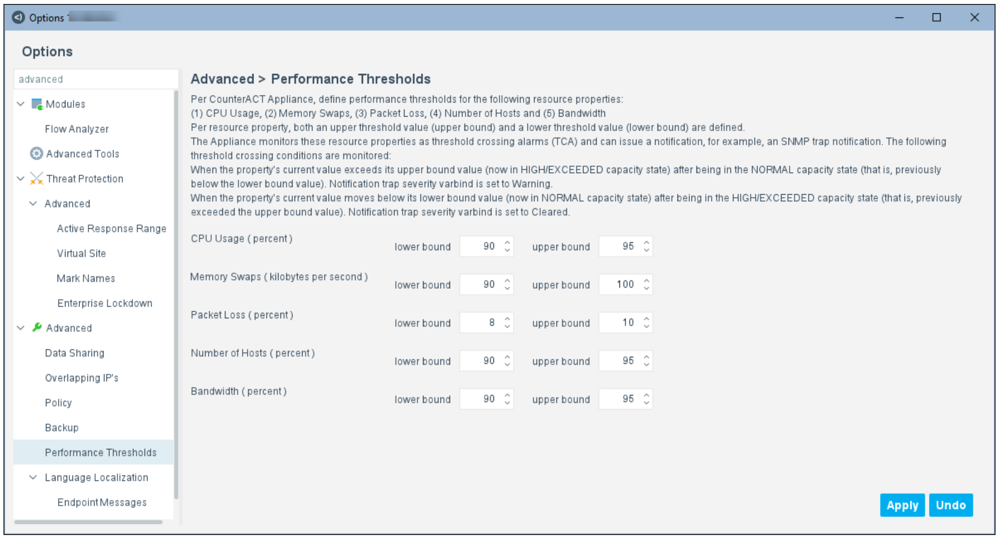
☑ Show sub-folders

Status	Type	Device Name ▲	IP/Name	Assigned Segments	# Hosts	Device Alerts	Description
⚠		[redacted]	[redacted]		0	Channels	Automation
✓		Enterprise Manager	[redacted]		2		Automation

2 items (1 selected)

```
Endpoints:               0 (max. performance capacity 1,000)
Bandwidth:               Current 0.01Mbps, Average 0.0Mbps, Max 0.85Mbps
High Availability:       HA is not enabled
Swap:                    0 Kilobytes per second
Lost Packets:            0.00%
CPU Utilization:         3.88%
Time Gap from EM:        0.000 seconds earlier
Delay from EM:           0.105 seconds
Uptime:                  46 days and 3 hours
Time Gap from Console:   Less than a minute earlier
NTP Servers:             updates.forescout.com
Packet Engine:           CounterACT Appliance is running
Channels:                The following new VLANs were detected by the CounterACT Appliance: [redacted]
Connection:              Connected to 10.160.35.1 as admin
Platform:                Virtual CounterACT Appliance
Serial Number:           VMware-[redacted]
```

This information is also used to populate OIDs in the MIB table object for each of the corresponding CounterACT Appliances. SNMP queries made to the Enterprise Manager return the table containing these per-Appliance MIB values. The Enterprise Manager also uses this information to send SNMP Trap notifications, for example when MIB values pass configurable performance thresholds. These thresholds can be configured by selecting **Tools>Options>Advanced>Performance Thresholds**.



Advanced > Performance Thresholds

Per CounterACT Appliance, define performance thresholds for the following resource properties:
(1) CPU Usage, (2) Memory Swaps, (3) Packet Loss, (4) Number of Hosts and (5) Bandwidth
Per resource property, both an upper threshold value (upper bound) and a lower threshold value (lower bound) are defined.
The Appliance monitors these resource properties as threshold crossing alarms (TCA) and can issue a notification, for example, an SNMP trap notification. The following threshold crossing conditions are monitored:
When the property's current value exceeds its upper bound value (now in HIGH/EXCEEDED capacity state) after being in the NORMAL capacity state (that is, previously below the lower bound value). Notification trap severity varbind is set to Warning.
When the property's current value moves below its lower bound value (now in NORMAL capacity state) after being in the HIGH/EXCEEDED capacity state (that is, previously exceeded the upper bound value). Notification trap severity varbind is set to Cleared.

CPU Usage (percent)	lower bound	90	upper bound	95
Memory Swaps (kilobytes per second)	lower bound	90	upper bound	100
Packet Loss (percent)	lower bound	8	upper bound	10
Number of Hosts (percent)	lower bound	90	upper bound	95
Bandwidth (percent)	lower bound	90	upper bound	95

- NAC policy and segment endpoint counters pushed from Appliances to the Enterprise Manager and forwarded to the Console.

Refer to the *Forescout Administration Guide* for more information about these features or navigate to the Forescout Console online Help.

Disconnected Appliances

If Appliances disconnect from the Enterprise Manager, all features that *do not* require sharing information between the Enterprise Manager or other Appliances continue to work regularly. This includes properties and actions that are not dependent on remote plugins.

Direct Inter-Appliance Communication

Available starting from Service Pack 2.2.0, *Direct Inter-Appliance Communication* allows Appliances to communicate directly with one another when possible instead of through the managing Enterprise Manager. This optimizes communication between Appliances.

Despite the communication changes implemented in this feature, the Enterprise Manager continues to manage Appliance activity, sending an extensive range of both information and requests to system Appliances.

For more information about this feature, including requirements, refer to the *CounterACT 7.0.0 Service Pack 2.2.0 Release Notes*.

Communication Among Appliances

Communication among Appliances is performed using a proprietary protocol over TLS (by default, on TCP port number 13000).

Connections among Appliances are established on demand, whenever one Appliance needs to send a message to another Appliance. If the recipient Appliance is not routable from the source Appliance or if the number of simultaneous connections between Appliances surpasses 100, the information is routed via the Enterprise Manager.

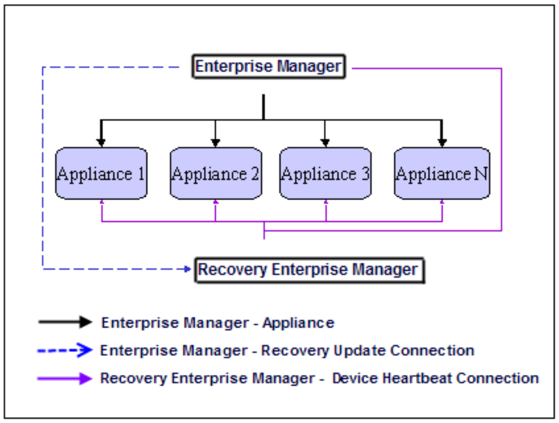
Appliances send the following information directly to other Appliances without first sending to the Enterprise Manager as an intermediary:

- Information about endpoints learned by one Appliance but assigned to another (IP Assignment). These are the most common messages sent by Appliances.
- Information learned by network device plugins configured at one Appliance that needs to be redirected to another Appliance. For example, an *Assign to VLAN* action that is performed on an endpoint connected to a switch managed by a Switch plugin running on a remote Appliance. Also, information sent by a network device to one Appliance that needs to be redirected to another Appliance, such as SNMP traps.
- Information sent between an Appliance and another Appliance that is configured as a Connecting CounterACT Device used to communicate to a third-party server. For example, in the Nessus Plugin, the Connecting CounterACT Device manages all communication with the defined Nessus server, including forwarding scan requests submitted to it by other Forescout devices assigned to this server and dispatching received scan results back to the appropriate Appliances.

Recovery Enterprise Manager Communication

A Recovery Enterprise Manager registered at the Console maintains a lightweight TCP connection with all Forescout devices in the organizational network. The purpose of this connection is to:

- Verify that the Recovery device can connect to other Forescout components
- Transmit primary Enterprise Manager system settings to the Recovery device.


Enterprise Manager
Appliance 1
Appliance 2
Appliance 3
Appliance N
Recovery Enterprise Manager
Enterprise Manager - Appliance
Enterprise Manager - Recovery Update Connection
Recovery Enterprise Manager - Device Heartbeat Connection

This connection is used to manage network Appliances when the recovery Enterprise Manager is switched over as the primary Enterprise Manager. Communication between the Enterprise Manager and the Recovery Enterprise Manager is performed on port 13000/TCP using standard TLS encryption. You may set up one Recovery Enterprise Manager in your enterprise.

Verifying Connections Between Forescout Devices

Connections between Forescout devices use fingerprints for verification purposes. When a connection is established, the fingerprints of the two Forescout devices are compared. If they match, the connection is accepted. This ensures that only trusted Forescout devices are connecting with each other.

This includes connections between:

- Enterprise Managers and Appliances
- Enterprise Managers and Recovery Enterprise Managers
- Appliances and other Appliances (Direct Inter-Appliance Communication)

Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

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

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

🗎 *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

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

To access the Technical Documentation page:

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

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Support Portal

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

To access documentation on the Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

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

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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