ForeScout

Enterprise Manager/Appliance Communication

CounterACT® Technical Note

Version 1.1

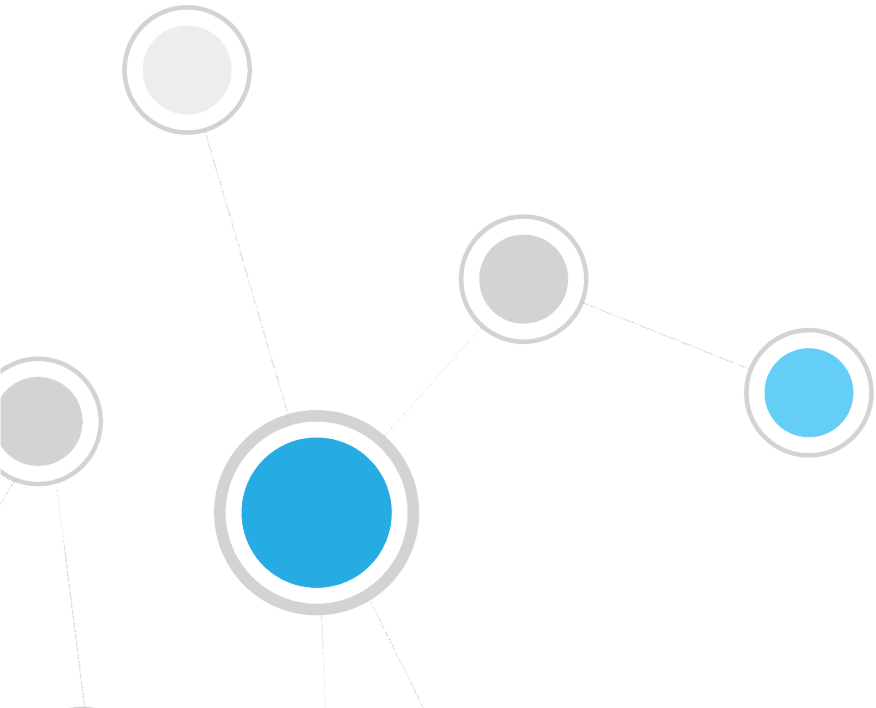


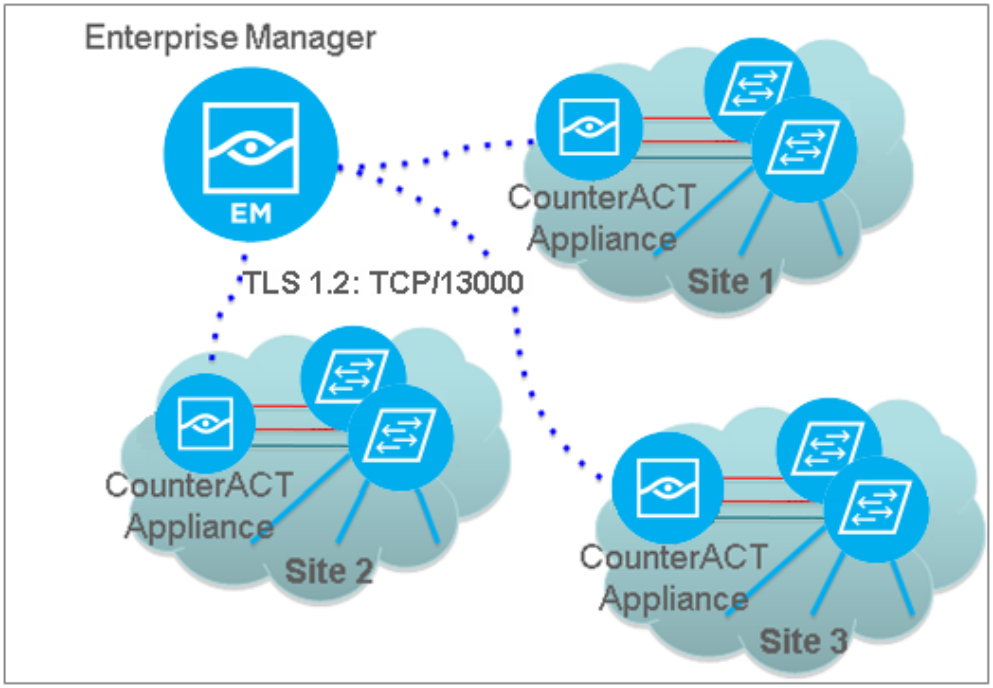
Table of Contents

About this Document

This document presents information regarding Enterprise Manager/Appliance communication. The information refers to ForeScout CounterACT® 8.0 systems.

Enterprise Manager/Appliance Communication Overview

Communication between the Enterprise Manager and Appliances is performed using a proprietary protocol over TLS1.2 on TCP port number 13000. All TCP sessions are initiated by the Enterprise Manager to the Appliances.

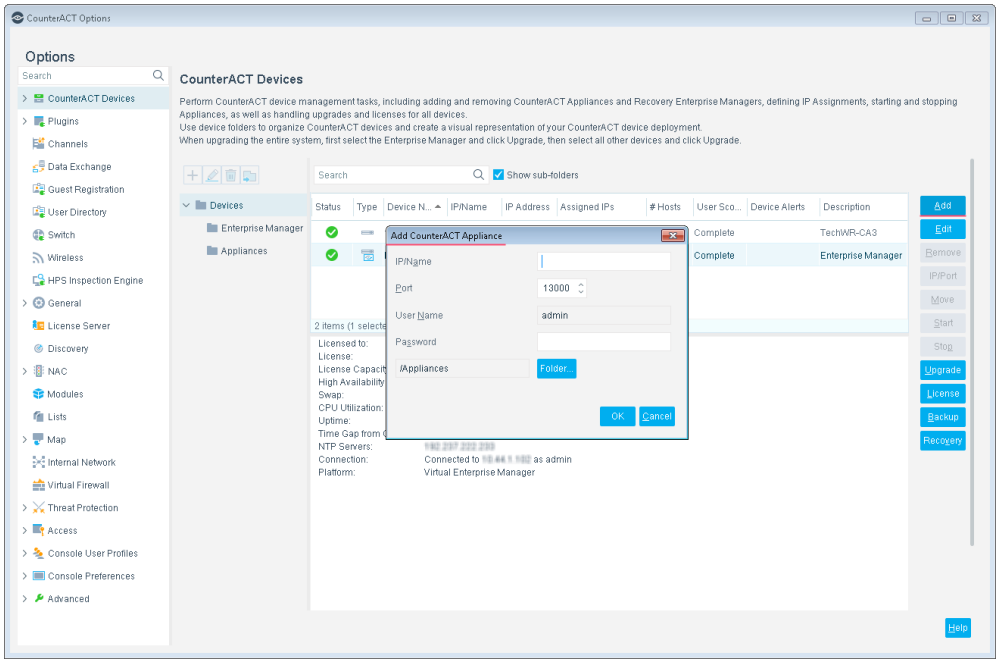


Authentication

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.



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 its managed 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 CounterACT Administration Guide for more information about these features

Information Sent from Appliances to the Enterprise Manager

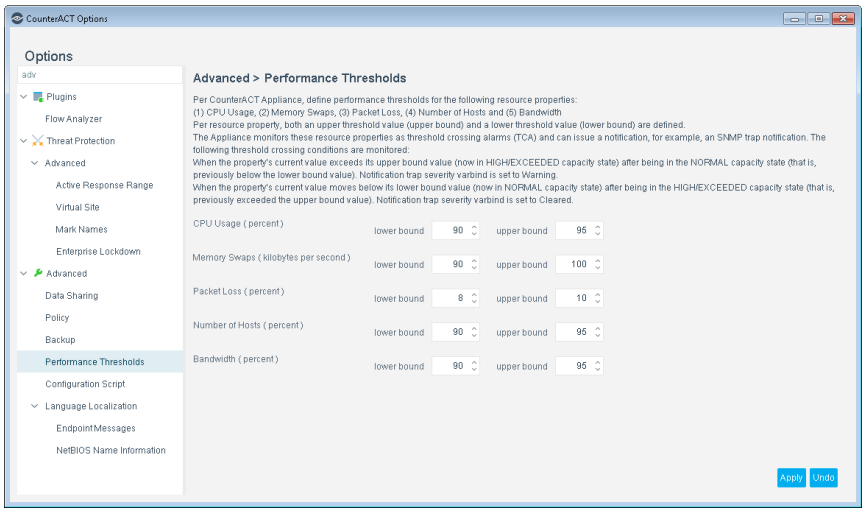
Appliances communicate an extensive range of information to the Enterprise Manager.

> *Appliances can also communicate certain information directly with one another when possible instead of through the managing Enterprise Manager. See Direct Inter-Appliance Communication for details.*

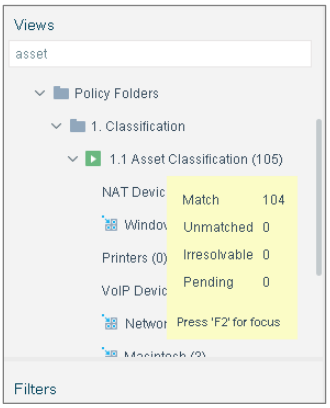
Examples of typical information sent include:

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

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**.



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



- and more

Refer to the CounterACT Administration Guide for more information about these features.

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

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 its managed Appliances.

Requirements

- Appliances should be routable from one another in order to communicate directly.
- Appliance firewalls must be configured to allow communication via port 13000 to other Appliances. By default, port 13000 is open on Appliances for communication with all IP addresses.

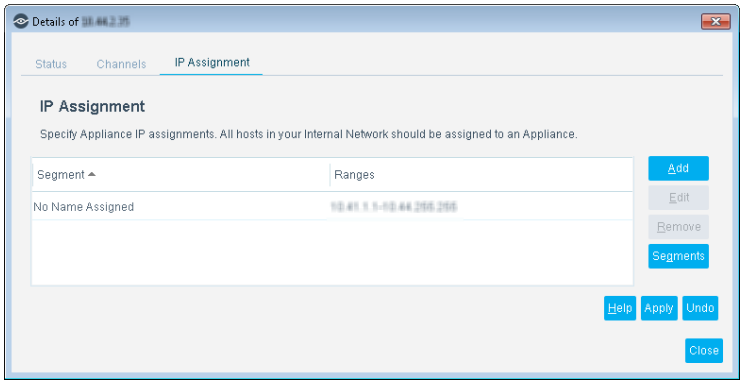
Communication Among Appliances

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 majority of messages sent by Appliances.

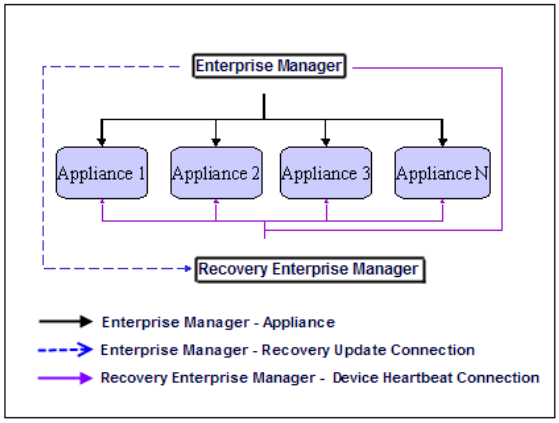


- Information learned by network device plugins configured at one Appliance that needs to be redirected to another Appliance. For example, an *Assign to VLAN* action that is performed on an endpoint connected to a switch managed by a Switch plugin running on a remote Appliance. Also, information sent 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 CounterACT 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 CounterACT devices in the organizational network. The purpose of this connection is to:

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



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.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

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

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

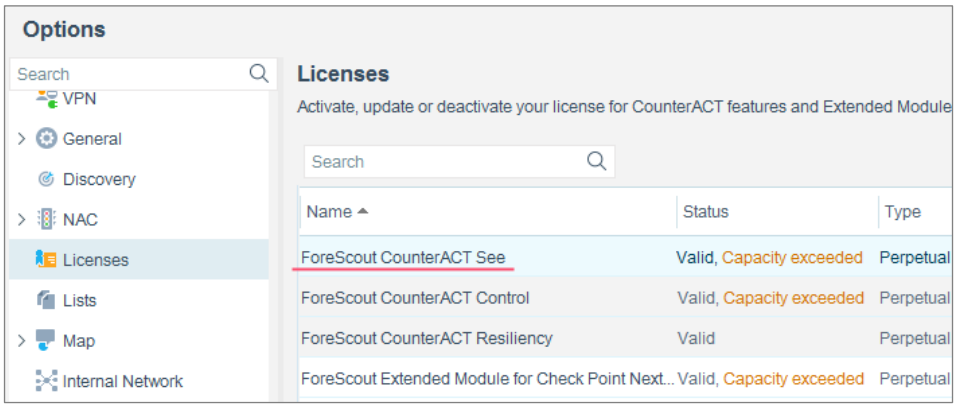
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-16 11:41