ForeScout CounterACT®

Deploying SecureConnector™ as a Service as Part of a Machine Image

How-to Guide

Version 8.0

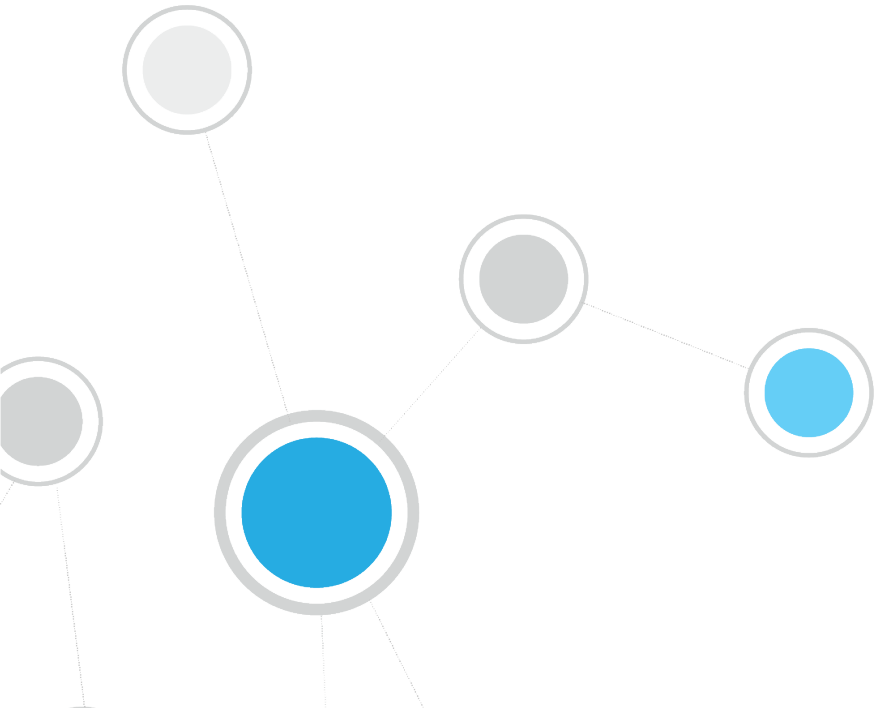


Table of Contents

About this Document

This document discusses distribution of SecureConnector™ on endpoints as part of a machine image. The information is relevant to CounterACT 8.0 systems with the following components installed:

- Endpoint Module version 1.0 with the following components running:
  - HPS Inspection Engine
  - Linux Plugin
  - OS X Plugin

Deploying SecureConnector™ as a Service as Part of a Machine Image - Considerations

Machine images are often used to apply identical installation and configuration settings to numerous corporate endpoints. When SecureConnector is regularly used to manage corporate devices, you may want to include SecureConnector in the machine image to simplify deployment.

However, some security features and implementation options of SecureConnector must be considered when implementing machine image rollout.

- SecureConnector implements various deployment options using separate installer packages. This means that several machine images are needed to support different combinations of the following deployment options:
  - Operating system
  - 32/64 bit system
  - SecureConnector toolbar icon visible/invisible
- When the managed endpoint accesses the network, SecureConnector connects to the Enterprise Manager by default and is assigned to the Appliance that manages the endpoint. Consider the following:
  - To support assignment to a managing Appliance, endpoints created using the machine image must use an IP address within the scope of CounterACT's *Internal Network* definitions. See the *CounterACT Administration Guide* for more information about the Internal Network.
  - If large numbers of endpoints are activated near-simultaneously after image installation, this may cause momentary traffic peaks at the Enterprise Manager that may that impact performance.

Consider creating several machine images, each of which directly addresses a different CounterACT Appliance when SecureConnector runs. This is especially recommended in large, geographically disperse networks. Multiple, targeted images are easily achieved by using the SecureConnector installer package that resides on a chosen target Appliance to install SecureConnector on the corresponding reference image. When machines imaged from that reference access the network, SecureConnector contacts the target Appliance. Refer to detailed deployment procedures below.

In addition, it may be necessary to generate multiple images that contact the same Appliance, but use different SecureConnector deployment settings (such as menu bar visibility).

Deployment Strategies

Consider the following when you deploy SecureConnector as a machine image in your environment:

- Follow these suggested procedures to deploy SecureConnector in the image:
  - Deploying SecureConnector in a Windows Machine Image
  - Deploying SecureConnector in a Mac OS X Machine Image
  - Deploying SecureConnector in a Linux Machine Image
- ***Ongoing Maintenance:*** Update the SecureConnector version in machine images each time you upgrade related CounterACT plugins. This ensures that new endpoints are created with the most current version of SecureConnector in the environment, and prevents unnecessary interactions between new endpoints and CounterACT Appliances.

Deploying SecureConnector in a Windows Machine Image

On Windows endpoints, SecureConnector generates a new, unique ID for itself upon installation. This means that an installer must run on the endpoint after imaging each machine.

Follow this suggested general procedure to deploy SecureConnector as a service as part of a Windows machine image:

1. Download the SecureConnector installer that installs SecureConnector as a service with the deployment options you want. See Download/Install SecureConnector Interactively on the Reference Machine.
2. Configure or deploy the image so that the installer executable is automatically run on machines formatted with the image.
   - When deploying an installer that installs SecureConnector as a service, the installer should run upon first boot of the machine.
   - When deploying an installer that installs SecureConnector as an application, the installer should run upon first login.

For example, on Windows endpoints the RunOnce registry key can be used to launch the installer. Under the following registry location, define a string object whose value is the path of the installer:

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

3. Create the image based on this reference machine.

Deploying SecureConnector in a Mac OS X Machine Image

To deploy SecureConnector as a service as part of a Mac OS X machine image:

1. Install the desired SecureConnector deployment on the reference machine. Do one of the following:
   - Install SecureConnector interactively. See Download/Install SecureConnector Interactively on the Reference Machine.
   - Follow the procedure for background installation described in the *OS X Plugin Configuration Guide*. Use the **`update.tgz`** archive located on a specific Appliance to create a machine image which contacts that Appliance upon first boot.
2. Create the image based on this reference machine.

Deploying SecureConnector in a Linux Machine Image

To deploy SecureConnector as a service as part of a Linux machine image:

1. Install the desired SecureConnector deployment on the reference machine. Do one of the following:
   - Install SecureConnector interactively. See Download/Install SecureConnector Interactively on the Reference Machine.
   - Create a Debian or RPM package that installs SecureConnector. Use this package to install SecureConnector on the reference machine. For details of Debian/RPM package creation, see Appendix 1 of the *CounterACT Macintosh/Linux Property Scanner Plugin Configuration Guide*.
2. Create the image based on this reference machine.

Download/Install SecureConnector Interactively on the Reference Machine

Follow this procedure to download a SecureConnector installer to the reference machine, as described in the OS-specific installation procedures above.

- For a Windows machine image, this installer is embedded in the image and runs upon boot of each endpoint based on the image.

- For Mac OS X and Linux machine images, run this installer on the reference machine to create a SecureConnector instance on the image.

To interactively install SecureConnector on the reference machine:

1. On the reference machine, browse to the following URL:

   `https://<`*`Appliance_IP`***`>/SC`**

   where <*Appliance_IP*> is the IP address of the Enterprise Manager or the Appliance that will manage endpoints created with this image. SecureConnector contacts this Appliance upon first boot of endpoints based on this image.

2. The ForeScout SecureConnector Distribution Tool page opens.
3. Specify deployment options and select **Submit**. The ForeScout Agent Download page opens.
4. (Window only) Select the 32 bit or the 64 bit agent version, depending on the machine image you are creating.
5. Select **Download**. Save the installer on the reference machine.
   - (Windows) Save the .exe file on the reference machine.
   - (Mac OS X) Save the .dmg file on the reference machine.
   - (Linux) Save the .sh file on the reference machine.
6. (Linux and Mac OS X only) Run the installer on the reference machine. You may delete the installer after it runs.

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**.

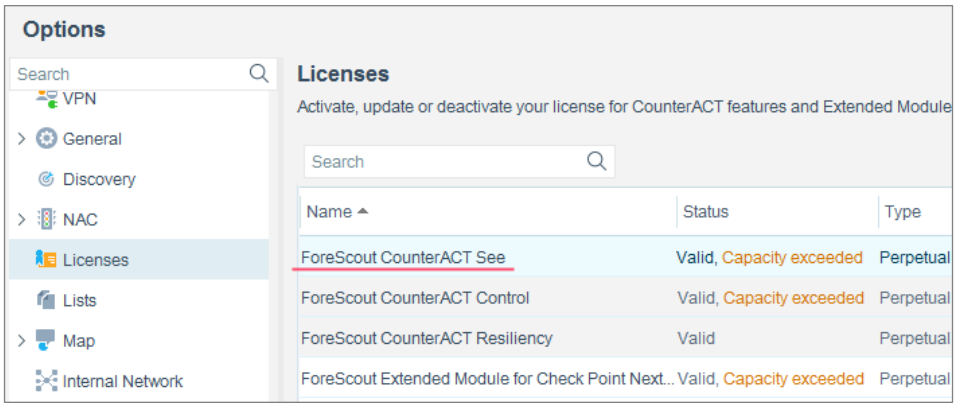
Documentation Portal

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

2018-04-15 14:20