ForeScout™

SecureConnector Advanced Features

How-to Guide

CounterACT Version 7.0.0

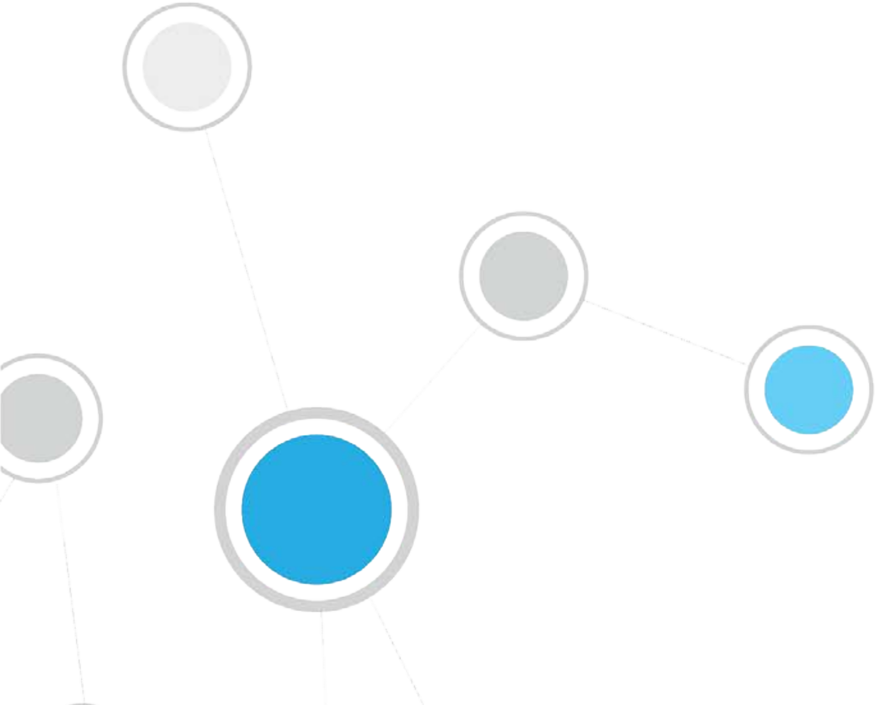


Table of Contents

About this How-to Guide

This guide describes the following advanced SecureConnector features:

- Certificate Based Rapid Authentication of Endpoints
- Endpoint Roaming Among Multiple CounterACT Deployments

Certificate Based Rapid Authentication of Endpoints

Typically CounterACT endpoint detection capabilities are combined with endpoint authentication and compliance policies to enforce network access control: Upon connection, network access of endpoints is restricted (typically to the DHCP and DNS servers and to CounterACT for detection and remediation interactions) until the user/endpoint is authenticated and compliance is proven. Only then is the necessary network access granted. However, authenticating endpoints and verifying compliance can cause a delay during which even legitimate endpoints have only restricted access. If complex compliance policies are in place, this delay in network access may be noticeable, resulting in an unsatisfactory user experience for corporate users.

An alternative access control method for initial connection is to give all endpoints full access by default for a limited period of time. During this time, the endpoint is authenticated and compliance checks are performed in the background. If authentication and/or compliance is not achieved within this ‘grace period’ access is restricted. This provides an improved user experience, but also opens a window during which a rogue user may freely access the network.

Authenticating endpoints can be quite challenging, and often this step is either omitted altogether, or a weak authentication check is performed (such as ensuring manageability). A strong endpoint authentication mechanism supports more immediate network access based on authentication alone, without the need to rely on potentially lengthy compliance checks.

Certificate based rapid authentication provides a strong, secure and extremely fast endpoint authentication mechanism. It uses your corporate PKI (Public Key Infrastructure) to provide immediate, authenticated network access for corporate users and other known endpoints, while providing greater security than the ‘grace period’ access approach.

When endpoints connect to the network:

- Corporate endpoints and other trusted endpoints managed by SecureConnector immediately initiate certificate-based authentication as part of SecureConnector’s TLS interaction with CounterACT. Endpoints are granted immediate network access based on a signed X.509 digital certificate. CounterACT continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.
- Endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, are granted limited network access until normal, policy-driven compliance checks are run.

Requirements for Rapid Authentication

This section describes requirements for working with rapid authentication.

Install the following plugin releases:

- HPS Inspection Engine Plugin version 10.5.0 or above
- Switch Plugin 8.10.0 or above
- (Optional) To support rapid authentication of Linux endpoints managed by SecureConnector, install Macintosh/Linux Property Scanner Plugin 7.0.1 or above.
- (Optional) To support rapid authentication of OS X endpoints managed by SecureConnector, install OS X Plugin 1.1.1 or above.

To use this feature, endpoints must be managed by SecureConnector. Versions of SecureConnector that support this feature identify rapid authentication client certificates on endpoints, and submit them for authentication as part of SecureConnector initial connection. For best performance, SecureConnector should be installed as a service; this ensures that authentication and consequent actions to grant network access can take place before the user has logged on, minimizing the time end users must wait to access the network.

CounterACT authenticates these client certificates based on certificates and CRL files generated by your PKI that are installed on each Appliance.

This feature requires your organization to have an existing Public/Private Key Infrastructure for certificate-based authentication, as described in the X.509 standard, including:

- a trusted Certificate Authority that can generate signed certificates
- support for certificate revocation

Administrators use the PKI in your network to generate signed certificates unique to the rapid authentication feature, and to distribute and manage these certificates on corporate devices and other trusted endpoints. Authentication chain and CRL information for these certificate is also distributed to CounterACT devices to allow authentication of client certificates.

What to Do

Follow this general procedure to implement certificate based rapid authentication.

1. Review the Requirements for Rapid Authentication and plan deployment. You can implement different levels of network access based on certificate details. See Detect and Authenticate Endpoints.
2. Work with the PKI/desktop team in your environment to generate Rapid Authentication Certificate Components.
3. Install Rapid Authentication Files on CounterACT Devices.

   If your environment uses the same CA to generate several certificates, you may Use an Extended Key Usage Object ID to distinguish the rapid authentication certificate from other certificates.

4. Install Rapid Authentication Client Certificates on Endpoints

   SecureConnector on managed endpoints detects these certificates to allow rapid authentication.

5. Create CounterACT policies that Detect and Authenticate Endpoints based on rapid authentication certificates.

Rapid Authentication Certificate Components

This section describes certificates and revocation lists that must be generated by the PKI team in your environment. To support rapid authentication, you must install certificate chain components on CounterACT devices and client-side certificates on endpoints managed by SecureConnector. See Install Rapid Authentication Files on CounterACT Devices and Install Rapid Authentication Client Certificates on Endpoints for details.

The complete certification chain for the rapid authentication certificate takes the form:

`[Certificate_chain][certificate]`

Where

`[Certificate_chain]` is the full certificate chain, including the root CA and any intermediate Certificate Authorities. The chain must be provided as a .pem file.

`[certificate]` is the signed client certificate installed on each endpoint.

In addition, a certificate revocation list **`[CRL]`** for this certificate chain is required. Because this list may be updated at regular intervals, your PKI team should provide a URL that points to the most recent CRL. The CRL file should be in .crl or .pem format.

Install Rapid Authentication Files on CounterACT Devices

The section describes how to install certificate chain and CRL files on CounterACT devices.

🗎 *When Appliances are added to the CounterACT environment, repeat this procedure to distribute certificates to the new Appliances.*

To install rapid authentication files on devices:

1. Log in to the Enterprise Manager or standalone Appliance as root.
2. If necessary, convert the certificate chain (from root CA to certificate issuer) for rapid authentication certificates to .pem format. Copy the .pem file to the Enterprise Manager or standalone Appliance. Note the location to which you copy these files.
3. Verify that the Enterprise Manager or standalone Appliance can access the URL of the CRL.
4. Submit the following command:

```
fstool sc_client_auth -i <cert_path> -c <CRL_URL> [-d <CRL_interval>]
[-win-oid <w_oid>] [-linux-oid <l_oid>]
```

where:

> **-i** installs the certificate chain files you deposited at <*cert_path*>in Step 2 to all Appliances. <*cert_path*> must be an absolute path.
>
> **-c** downloads a CRL file from the URL specified by <*CRL_URL*> to all Appliances.
>
> **-d** <*CRL_interval*> sets the time interval, in hours, at which a new CRL file is downloaded from <*CRL_URL*>. The default value is 24 hours. If you change this setting, specify an integer value.
>
> **-win-oid** and **-linux-oid** set Extended Key Usage Object IDs that identify certificates relevant to this feature. See Use an Extended Key Usage Object ID for details.

To initially configure CounterACT to use this feature, you must use the **-i** and **-c** flags to distribute certificate chain and CRL files to all devices. All other flags are optional.

🗎 *This command requires reboot of the Appliance.*

Use an Extended Key Usage Object ID

In some environments the same issuing CA is used to sign certificates for different purposes. In these environments clients have several certificates issued by the same CA, and an Extended Key Usage extension is used to distinguish each certificate. Typically an Object ID (OID) string is used as the key.

For Windows and Linux endpoints, when the **-win-oid** and the **-linux-oid** flags are added to the **fstool sc_client_auth** command the plugin sets the OID string(s) that SecureConnector uses to identify and authenticate certificates for this feature. For example, the following command sets the OID string 12.5.2.7 to identify authentication certificates on Windows endpoints, and the OID string 10.4.0.1.6 to identify authentication certificates on Linux endpoints.

```
fstool sc_client_auth -i <cert_path> -c <CRL_URL> -win-oid 12.5.2.7
 -linux-oid 10.4.0.1.6
```

🗎 *This command requires reboot of the Appliance.*

🗎 *To roll back use of an extended key usage extension, submit the command with these flags, but with the string* ***none*** *as the OID value. The OID value is removed from CounterACT devices.*

Existing SecureConnector clients receive the OID value the next time they connect to CounterACT.

For OS X endpoints, use the following procedure to work with an Extended Key Usage extension:

To use an Extended Key Usage extension with OS X endpoints:

1. Verify that the **`fstool sc_client_auth`** command has been used to distribute the certificate chain to all CounterACT devices.
2. Log in to the Enterprise Manager or standalone Appliance as root.
3. Submit the following command:

   `fstool osx_pkg -c <`*`o_OID`***`> [-o]`**

   where

   `-c` sets the Extended Key Usage Object ID for OS X endpoints to the value specified in <*o_OID*>. SecureConnector uses this value to identify and authenticate certificates for this feature on OS X endpoints. The OID value is also added to the SecureConnector installers used by the OS X Plugin.

   🗎 *To roll back use of an extended key usage extension, run the command without this flag. The OID value is removed from CounterACT devices, and installers without an extension value are generated.*

   `-o` implements OID changes on all CounterACT devices. Use this flag when you are logged in to Enterprise Manager to apply changes to all Appliances. Omit this flag when you are logged in to an Appliance to apply changes only to that Appliance.

Existing SecureConnector clients receive the OID value the next time they connect to CounterACT. New OS X endpoints receive the OID value during SecureConnector installation.

Install Rapid Authentication Client Certificates on Endpoints

When endpoints access the network:

- SecureConnector connects to CounterACT, making endpoints manageable.
- SecureConnector authenticates using rapid authentication certificates on endpoints, and the plugin reports authentication-related host property values. You can use these properties in CounterACT policies to grant network access to endpoints with valid certificates.

This section describes installation requirements that allow CounterACT to find the rapid authentication certificate on endpoints running different operating systems:

- Install Rapid Authentication Certificates on Windows Endpoints
- Install Rapid Authentication Certificates on Linux Endpoints
- Install Rapid Authentication Certificates on OS X Endpoints

Rapid authentication certificates are installed on endpoints by the team in your environment that is responsible for your PKI or desktop infrastructure. Any valid certificate enrollment procedure may be used to install certificates.

When you Use an Extended Key Usage Object ID to distinguish rapid authentication certificates, the object/OID value should be included in the client-side distribution. SecureConnector on endpoints searches certificate stores for the OID value that was configured during server-side certificate installation on CounterACT devices.

Install Rapid Authentication Certificates on Windows Endpoints

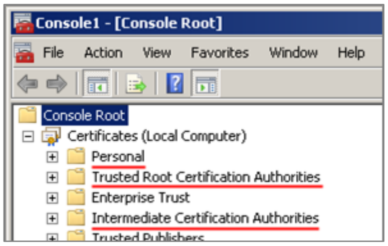
All certificates should be installed in the certificate store of the local computer.

To install rapid authentication certificates on Windows endpoints:

- Install the rapid authentication certificate under the *Personal* certificate store.

– The *Client Authentication* certificate purpose must be enabled.

- Install [root_CA] – the certificate of the root Certification Authority - under the *Trusted Root Certification Authorities* store.
- Install [intermediate_CAs] – the intermediate Certificate Authorities relevant to this feature – under the *Intermediate Certification Authorities* store.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

Install Rapid Authentication Certificates on Linux Endpoints

To install rapid authentication certificates on Linux endpoints:

1. For each client certificate, save the key pair as two files:

   `fs_sc_cert.pem` contains the client certificate.

   `fs_sc_cert_key.pem` contains the private key of the client certificate.

2. Create the following directory, and place both files in the directory:

   – When SecureConnector is run as permanent service or as dissolvable executable under the root user account:

   $HOME**`/etc/forescout/certs/`**

   – When SecureConnector is run as dissolvable executable under another user account:

   <*user_ home***>`/forescout/certs/`**
   Where <*user_home*> is the home directory of the user account.

Install Rapid Authentication Certificates on OS X Endpoints

To install rapid authentication certificates on OS X endpoints:

1. If necessary, convert the client certificate key pair file to .pfx format.
2. Copy the .pfx file to the endpoint.
3. Attach this .pfx file to the System Keychain. For example, the following command attaches a file copied to the desktop to the Keychain.

   ```
   sudo security import ~/Desktop/<client_cert>.pfx –k
   /Library/Keychains/System.keychain –f pkcs12 –A –P <pass>
   ```

   Where <*client_cert*> is the name of the client certificate file in .pfx format, and <*pass*> is the passphrase used to unwrap the file.
4. Verify that SecureConnector can access this client certificate. If necessary, change key permissions.

Detect and Authenticate Endpoints

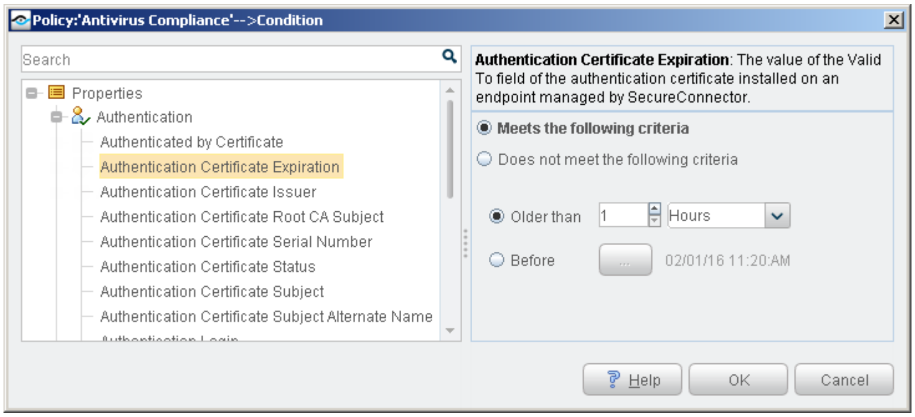
When you install plugin releases that support this feature, new host properties are available. The properties are described in the table below.

Use these properties to create policies that detect endpoints with valid rapid authentication certificates, and to grant them network access. Most of these properties report fields of the client certificate, and several of these properties track the certificate based authentication process.

Consider creating the following policies to support certificate-based rapid authentication. In some cases, you can incorporate new rules in existing policies:

- *Detect and install SecureConnector:* It may be necessary to detect corporate endpoints and other trusted devices that are not yet managed by SecureConnector, and install or upgrade SecureConnector.
- *Manage the rapid authentication process:* Use the **Authentication Certificate Status** and the **Authenticated by Certificate** host properties to track the rapid authentication process, and to troubleshoot endpoints that failed to authenticate.
- *Grant network access based on certificate details:* Use the host properties below to detect endpoints based on the subject or other fields of the certificate, and to provide a specific network access profile based on the information in the certificate on the endpoint. This allows definition of several basic levels of access, determined by the rapid authentication certificate.
- *Handle non-compliant trusted devices:* detect certificate-authenticated endpoints which subsequently fail one or more policy-based compliance checks that are standard in your environment. If endpoints are significantly non-compliant, you may want to revoke the certificates of these endpoints to prevent rapid authentication the next time they connect.

- *Troubleshoot rapid authentication certificates:* Use the host properties below to detect endpoints with invalid or expired certificates.


Policy:'Antivirus Compliance'-->Condition
Search
Properties
Authentication
Authenticated by Certificate
Authentication Certificate Expiration
Authentication Certificate Issuer
Authentication Certificate Root CA Subject
Authentication Certificate Serial Number
Authentication Certificate Status
Authentication Certificate Subject
Authentication Certificate Subject Alternate Name
Authentication Login
Help
OK
Cancel

Authentication Certificate Expiration: The value of the Valid To field of the authentication certificate installed on an endpoint managed by SecureConnector.

● Meets the following criteria

○ Does not meet the following criteria

● Older than 1 Hours

○ Before ... 02/01/16 11:20:AM

Authentication Certificate Subject Alternate Name	The value of the Subject Alternate Name field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Status	Indicates the state of the certificate installed on the endpoint for certificate-based authentication, and any verification errors for the certificate. If a certificate for this feature is not found on the endpoint, this property returns the value *No certificate.*
Authentication Certificate Expiration	The value of the Valid To field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Issuer	The value of the Issuer field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Root CA Subject	The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Serial Number	The value of the Serial Number field of the certificate installed on the endpoint for certificate-based authentication.
Authenticated by Certificate	Indicates whether certificate-based authentication process for the endpoint was successful. If a certificate for this feature is not found on the endpoint, this property returns the value *No.*
Authentication Certificate Subject	The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.

Tuning CounterACT Devices for Rapid Authentication

This section describes information regarding tuning of internal processes to improve performance of the Certificate Based Rapid Authentication feature.

To minimize the time it takes to detect new endpoints on the network and authenticate then, and similarly, to detect their disconnection, use the following procedure to change default settings on CounterACT devices.

To configure CounterACT devices for rapid authentication:

1. Log in to the Enterprise Manager or a standalone Appliance as root.
2. Submit the following commands:

   ```
   fstool va set_property conf.agent_close_state_timeout.value 0
   ```

   This internal parameter specifies the interval, in seconds, which the HPS Inspection Engine Plugin waits before reporting an endpoint as *Not Manageable* after two expected keep-alive messages were not received.

   ```
   fstool va set_property config.kpa_recv_interval.value 60
   ```

   This internal parameter specifies the timeout interval, in seconds, which the HPS Inspection Engine Plugin waits for keep-alive messages from SecureConnector agents on managed endpoints.

   Modifying these values from their defaults precipitates reconnection more quickly if an endpoint managed by SecureConnector fails to connect to its Appliance.
3. Submit the following command to restart the HPS Inspection Engine Plugin with these new settings:

   ```
   fstool va restart
   ```
4. (Enterprise Manager only) Submit the following commands to implement these configuration settings on each CounterACT device in the network:

   ```
   fstool oneach fstool va set_property
   conf.agent_close_state_timeout.value 0
   ```

   ```
   fstool oneach fstool va set_property config.kpa_recv_interval.value
   60
   ```

   ```
   fstool oneach fstool va restart
   ```

To restore default settings for these parameters:

1. Log in to the Enterprise Manager or a standalone Appliance as root.
2. Submit the following commands:

   ```
   fstool va remove_property conf.agent_close_state_timeout.value
   ```

   ```
   fstool va remove_property config.kpa_recv_interval.value
   ```
3. Submit the following commands to restart the HPS Inspection Engine Plugin with these new settings:

   ```
   fstool va restart
   ```
4. (Enterprise Manager only) Submit the following commands to implement these configuration settings on each CounterACT device in the network:

   ```
   fstool oneach fstool va remove_property
   conf.agent_close_state_timeout.value
   ```

   ```
   fstool oneach fstool va remove_property
   config.kpa_recv_interval.value
   ```

   ```
   fstool oneach fstool va restart
   ```

Endpoint Roaming Among Multiple CounterACT Deployments

This feature lets endpoints that are managed by SecureConnector roam to various corporate CounterACT deployments and still remain managed.

For example, in a large organization separate CounterACT deployments may support geographically disperse segments of the corporate network. When an endpoint managed by SecureConnector in one CounterACT deployment roams to a segment of the corporate network managed by another CounterACT deployment, it is recognized, allowed to connect, and is managed by SecureConnector.

This section describes how to configure CounterACT so that SecureConnector can work with several independent Enterprise Managers or standalone Appliances.

🗎 *Endpoints must initially connect to their home CounterACT deployment after defining this configuration to receive the roaming capabilities.*

Requirements

This section describes requirements for working with .

Install the following plugin releases:

- For SecureConnector on Windows: HPS Inspection Engine 10.5.0 or above
- For SecureConnector on OS X: OS X 1.1.1 or above
- For SecureConnector on Linux: Macintosh/Linux Property Scanner 7.0.1 or above

Roaming for Windows Endpoints with SecureConnector

This procedure lets Windows endpoints managed by SecureConnector roam to other CounterACT deployments in your corporate network while remaining manageable.

To support roaming for Windows endpoints managed by SecureConnector:

1. On each Enterprise Manager:

   a. Log in as root.

   b. If roaming endpoints can still connect to their home Appliance over the corporate network, submit the following command:

   ```
   fstool va set_property config.disconnect_unassigned_sc.value true
   ```

   From the CounterACT Console, restart the HPS Inspection Engine plugin.

   c. In the CounterACT Console, select **Options** from the **Tools** menu.

   d. Select **HPS Inspection Engine**.

e. Select the SecureConnector tab. In the **Additional Appliance Connections** field, enter a comma-separated list of IP addresses for the other Enterprise Managers:

   <*EM_IP1*>**,**<*EM_IP2*>,...,<*EM_IPn*>

f. If several configurations are defined for the plugin, repeat step e in all configurations.

g. Select **Apply** to save changes.

Roaming for Linux Endpoints with SecureConnector

This procedure lets Linux endpoints managed by SecureConnector roam to other CounterACT deployments in your corporate network while remaining manageable.

To support roaming for Linux endpoints managed by SecureConnector:

1. Prepare a file named **`multiple_em_ips.conf`**. Each row of the file has the following format:

   <*EM_IP***>;<***EM_public_key***>**

   Where

   <*EM_IP*> is the IP address of an Enterprise Manager

   <*EM_public_key*> is the public key found on the Enterprise Manager at:

   ```
   /root/.ssh/id_rsa.pub
   ```

   This file must contain all Enterprise Managers in all CounterACT deployments.

2. Place this file at the following location on all Enterprise Managers:

   ```
   /usr/local/forescout/plugin/mac/multiple_em_ips.conf
   ```

3. On each Enterprise Manager:

   a. Log in as root.

   b. Submit the following commands:

   ```
   fstool mac set_property config.use_multiple_em.value true
   fstool oneach fstool mac set_property config.use_multiple_em.value
   true
   fstool oneach scp
   /usr/local/forescout/plugin/mac/multiple_em_ips.conf
   ```

   c. If roaming endpoints can still connect to their home Appliance over the corporate network, submit the following command:

   ```
   fstool mac set_property config.disconnect_unassigned_sc.value true
   ```

   d. From the Console, restart all instances of the plugin.

Roaming for OS X Endpoints with SecureConnector

This procedure lets OS X endpoints managed by SecureConnector roam to other CounterACT deployments in your corporate network while remaining manageable.

To define Enterprise Manager roaming for OS X endpoints managed by SecureConnector:

1. On each Enterprise Manager:

   a. Log in as root.

   b. Submit the command **`fstool osx additional_sites`**.

      Output containing a certificate and other information is generated.

   c. Select the information including the curly brackets, as indicated below. Save this information to a file.

```
{
 "resource" : "/sc",
 "client_auth_oid" : "1.3.6.1.4.1.694.21.8.815",
 "servers" :
   [
      {
        …

       "reconnect_interval" : "2",
       "server" : "10.34.1.14",
       "port" : 10005,
       "compliance_center_url" :
        "http://10.34.1.14/status?cc=true&fromsc=true"
      }
   ]
}
```

2. In each CounterACT environment with its own Enterprise Manager:

   Create a file named **`additional_sites`**. Edit the file and paste in the Enterprise Manager data you prepared in Step 1. Do not include data for this Enterprise Manager; the file should contain only data from other Enterprise Managers. The **`additional_sites`** file should have the following structure:

   [{_EM_1_info_**},{**_EM_2_info_**},…,{**_EM_n_info_**}]**

   - Curly brackets enclose information from each Enterprise Manager.

   - A comma separates information from different Enterprise Managers.

   - Enclose the entire comma-separated list in square brackets.

   d. Log in to the Enterprise Manager as root.

e. Save the **`additional_sites`** file you prepared in Step 2 to the following location on the Enterprise Manager:

```
/usr/local/forescout/plugin/osx/
```

f. Submit the following command:

```
fstool oneach scp /usr/local/forescout/plugin/osx/additional_sites
```

g. From the CounterACT Console, restart all instances of the OS X Plugin in this CounterACT environment.

Legal Notice

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout's products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-05-21 17:32