FORESCOUT

CounterAct®

Infrastructure Update Pack

Configuration Guide

Version 2.0.14

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

Legal Notice

2019-12-19 13:13

Table of Contents

About the CounterACT Infrastructure Update Pack

The CounterACT Infrastructure Update Pack lets you take advantage of infrastructure changes made to CounterACT, for example security patches and upgrading of security-related libraries and utilities.

Refer to the CounterACT Infrastructure Update Pack Release Notes on the Product Download page to read about the latest improvements.

What to Do

This section lists the steps you should take to install the update pack and work with new or enhanced features:

1. Verify that you have met system requirements. See Requirements.
2. Install the Plugin.
3. Configure the Plugin.

Requirements

The plugin requires the following Forescout release:

- Forescout version 7.0
- An active Maintenance Contract for CounterACT devices is required.

Install the Plugin

Perform the following steps to download the plugin from the Web site and install it on the Console.

It is recommended to back up the Enterprise Manager and Appliances before installing the pack as the installation cannot be rolled back.

When installing, be aware of the following issues:

- If you install or update a plugin on the Enterprise Manager, it is automatically installed or updated on all registered Appliances. For more information, refer to *Centralized Management* in the *CounterACT Console User Manual*.
- Installing or upgrading the CounterACT Infrastructure Update Pack results in a single service restart, the duration of which depends on your network environment. A typical installation takes about 20 minutes.
- If you are using iDRAC to remotely access the CounterACT device, the connection to iDRAC will be disconnected when you install the plugin and you will need to reconnect afterwards. This does not affect CounterACT functionality.

To install the plugin:

1. Navigate to the Product Updates Portal, Base Plugins page and download the plugin `.fpi` file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin `.fpi` file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

Configure the Plugin

After installation, you can configure and work with the following feature:

- Control Command-line Access to CounterACT Devices

Control Command-line Access to CounterACT Devices

CounterACT devices expose a command-line interface (CLI) that is used by administrators for device installation and setup, or to issue fstool commands, or when file import/export tools are not supported by the Console.

The user accounts defined at the CLI level are not related to Console users.

The following tools support more secure management of CLI level access.

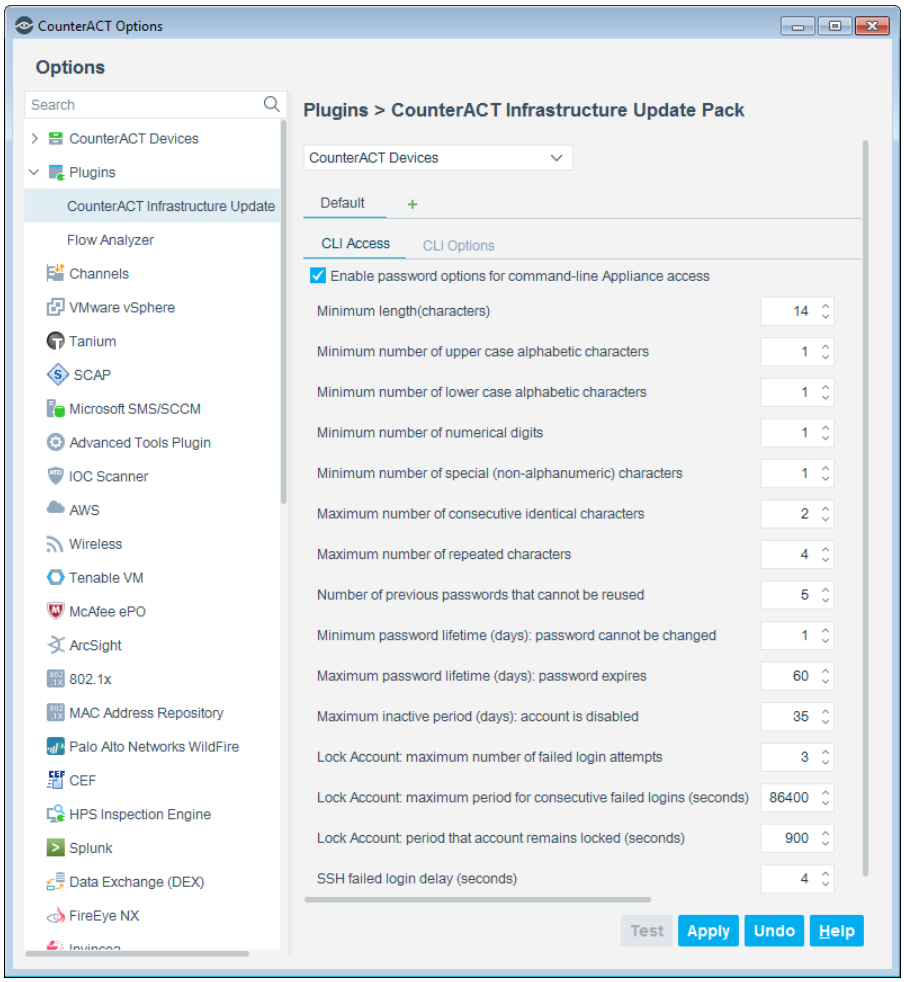
- Configure Access Security Features for Command-Line Users
- Configure Session Security Features for Command-Line Interaction
- Configure Password Protection for the Boot Loader

Configure Access Security Features for Command-Line Users

Use this procedure to define minimum acceptable password requirements for users logging in to CounterACT devices through the command-line interface. In addition, you can configure features such as lockout and inactive account suspension.

To configure password handling for command-line users:

1. In the Console, select **Options** from the **Tools** menu.
2. In the Options pane, select **Plugins** and then select **CounterACT Infrastructure Update Pack**.



CLI Access Tab

3. (Optional) Define or modify a configuration that applies to a subset of CounterACT devices. See *Configuring Features for an Appliance or Group of Appliances* in the *CounterACT Console User Manual*.
4. In the CLI Access tab, select **Enable password options for command-line Appliance access** and configure the following fields.

Minimum length (characters)	Passwords with fewer characters than the number specified are rejected. Longer minimum word lengths enhance security.
Minimum number of upper case alphabetic characters	Passwords that contain fewer characters of each type than specified are rejected. Requiring passwords with different types of characters enhances security.
Minimum number of lower case alphabetic characters	

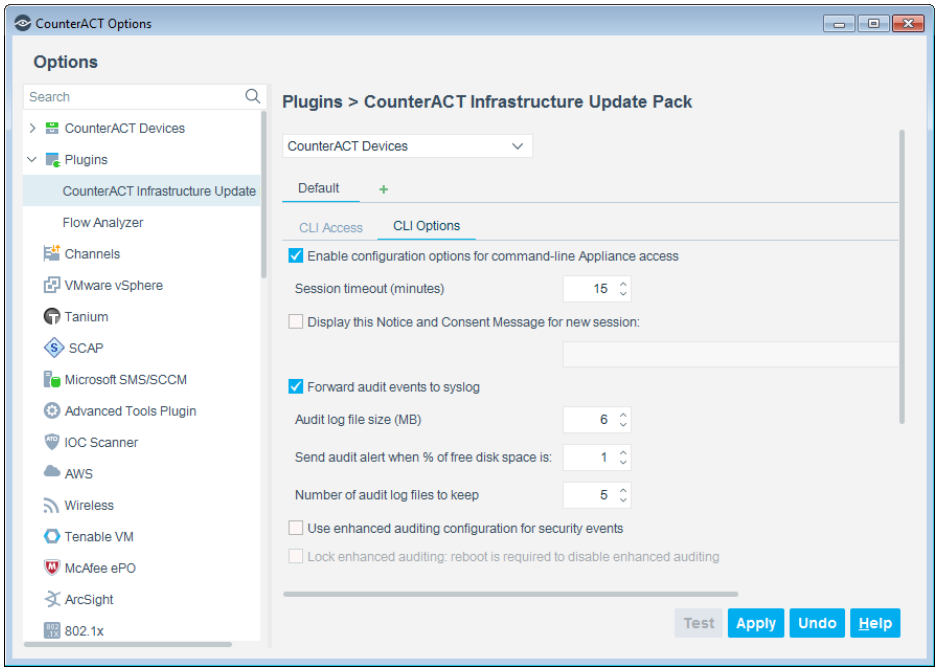
Minimum number of numerical digits	
Minimum number of special (non-alphanumeric) characters	
Maximum number of consecutive identical characters	Passwords with more unique characters are more secure. In the password **`t93AAw7`**, two identical characters (A) appear consecutively.
Maximum number of repeated characters	Passwords with more unique characters are more secure. The password **`fffaA1v22`** contains three repeated characters: f,f,2.
Number of previous passwords that cannot be reused	Requiring users to submit a password not recently used enhances security.
Minimum password lifetime (days): password cannot be changed	Preventing users from immediately changing a new password enhances security.
Maximum password lifetime (days): password expires	Requiring users to change their password regularly enhances security.
Maximum inactive period (days): account is disabled	When a user account has been inactive for the specified time period, it is disabled. Disabling dormant accounts enhances security.
Lock Account: maximum number of failed login attempts	If a user submits the specified number of incorrect passwords within the specified time period, the account is locked for the specified time period. This feature prevents brute-force login attacks.
Lock Account: maximum period for consecutive failed logins (seconds)	
Lock Account: period that account remains locked (seconds)	

Configure Session Security Features for Command-Line Interaction

Use this procedure to define session timeouts, audit log file properties and other security features that apply when users log in to CounterACT devices through the command-line interface.

To configure security features for command-line interaction:

1. In the Console, select **Tools>Options**.
2. In the Options tree, select **Plugins>CounterACT Infrastructure Update Pack**.
3. (Optional) Define or modify a configuration that applies to a subset of CounterACT devices. See *Configuring Features for an Appliance or Group of Appliances* in the *CounterACT Console User Manual*.
4. Select the CLI Options tab.



CLI Options Tab

5. Select **Enable configuration options for command-line Appliance access** and configure the following fields.

Session timeout (minutes)	When a session has been inactive for the specified period, it is closed. Users can log in again immediately. Closing inactive sessions enhances security.
Display this Notice and Consent Message for new session:	The text you enter here is displayed to users when they connect to the device. Do not enter line break characters in this string.
Forward audit events to syslog	Forward a copy of the audit events to the syslog server.
Audit log file size (MB)	The size in MB of the log files to be generated. Maximum size is 50 MB.
Send audit alert when % of free disk space is:	The percentage of free disk space left that triggers an alert. Maximum percentage is 10.
Number of audit log files to keep	The number of recently created audit log files to be kept. Maximum is 20.
Use enhanced auditing configuration for security events	When this option is selected, CounterACT devices monitor additional events and conditions that indicate security exposure.
Lock enhanced auditing: reboot is required to disable enhanced auditing	It may be necessary to disable enhanced auditing, for example if enhanced auditing causes performance issues. When this option is selected, enhanced auditing cannot be disabled from the Console. The device(s) must be rebooted to disable enhanced auditing.

Configure Password Protection for the Boot Loader

CounterACT devices use the GNU GRUB boot loader. To prevent malicious changes to boot settings, you can protect access to these settings by requiring a password.

Once you define a boot loader password, you cannot disable password protection or define a null password.

To configure password protection for the boot loader:

1. Log in to the CounterACT device CLI.
2. Submit the following command:
   `fstool grub –setpassword`
3. The following prompt appears:
   `Enter grub password:`
4. Enter the password. The following prompt appears:
   `Re-type grub password:`
5. Re-enter the password. The following prompt appears:
   `Successfully updated grub password.`

The system prompts for this password when users try to edit boot loader settings.

Configure Use of SHA-1 Hash Algorithm

By default, CounterACT accepts the SHA-1 hash algorithm to secure SSH connections. Use the following procedure to configure CounterACT to accept only more secure SHA algorithms.

To configure use of SHA-1 for SSH:

1. To disable SHA-1:
   a. Log in to Enterprise Manager CLI.
   b. Enter the following command:
      `fstool ciup ssh`
      The following message appears:
      `hmac-sha1 for SSH is currently enabled.`
      `Disable? (yes/no)`
   c. Enter **`yes`** and press Enter. The following confirmation message appears:
      `hmac-sha1 for SSH is disabled.`
   d. Repeat these steps on all Appliances in your environment.
2. To enable SHA-1:
   a. Log in to Enterprise Manager CLI.
   b. Enter the following command:
      `fstool ciup ssh`

The following message appears:

```
hmac-sha1 for SSH is currently disabled.
Enable? (yes/no)
```

c. Enter `yes` and press Enter. The following confirmation message appears:

```
hmac-sha1 for SSH is enabled.
```

d. Repeat these steps on all Appliances in your environment.

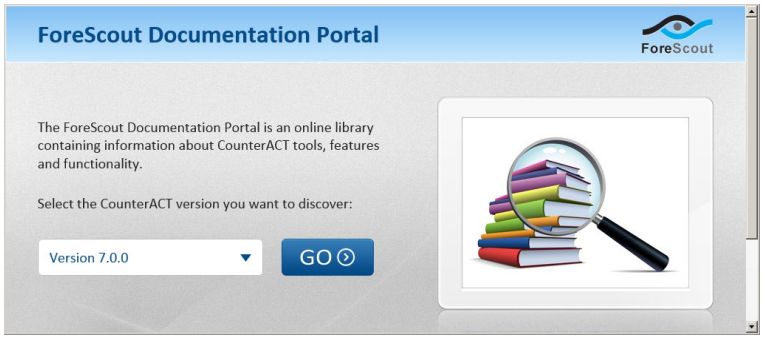
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



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.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:

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

CounterACT Console Online 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.

Console User Manual

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 **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

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