FORESCOUT

Forescout

CLI Commands

Reference Guide

Forescout versions 8.1.x and 8.2.x

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/supporurt/

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

2020-07-16 17:32

Table of Contents

About Command Line Access

This reference guide describes how to use the Forescout® command line interface (CLI) on Forescout devices, meaning either the Enterprise Manager or Appliances.

> *As the former product name* – CounterACT – *still appears in the CLI, this guide continues to reference the name* CounterACT.

FS-CLI

FS-CLI is a proprietary Forescout command line interface that is designed to comply with security certification requirements. When FS-CLI is enabled, you can run FS-CLI Commands via the CLI. When FS-CLI is not enabled, a different set of commands is available (see The fstool Command Set by Categories for available commands).

The FS-CLI is installed by default in all Forescout systems:

- If you performed a clean installation, FS-CLI is installed and running when you access the CLI.
- If you performed an upgrade, FS-CLI is installed, but the Bash shell is still running when you access the CLI. You need to run an fstool command to exit the Bash shell and enter FS-CLI.

To run FS-CLI:

1. Log in to the CounterACT Appliance CLI (Bash shell).
2. Run: **`fstool cli`**

Bash Shell

A special command is available that allows you to exit the FS-CLI and access the operating system's Bash shell. This command is not available when running in Certification Compliance Mode.

To return to the Bash shell:

- Run: shell

User Roles and Permissions

You can add new CLI users and grant user permissions to perform specific operations within the CLI. You can also update permissions for existing users.

See user – Configure User Roles and Permissions for more information.

Certification Compliance Mode

When Forescout platform is running in Certification Compliance mode, FS-CLI is the only command line interface available, and the user cannot access Bash or operating system shell commands. For more information about Certification Compliance mode,

refer to the *Forescout Installation Guide*. See Additional Forescout Documentation for information on how to access this document.

> *When Forescout is installed under Certification Compliance mode, the only option for regaining access to the Bash shell is to reinstall the Forescout Appliance with Certification Compliance Mode disabled.*

CLI User Account

Log in to the command line interface using the *cliadmin* user account. The password for this account is specified during installation. It is not recommended to delete this user from the system.

Entering Commands

After successful login, enter the **?** character to list available commands.

Submit commands in the format shown in this guide and other Forescout documentation. Most commands are shown with the optional fstool prefix. This prefix can be omitted when you enter commands in FS-CLI, but must be included when you enter commands in the Bash shell. For example, the following commands yield the same result in FS-CLI:

```
fs-cli@em1>fstool ntp test
fs-cli@em1>ntp test
```

Entering Privileged Commands

This command execution requirement applies to Forescout versions 8.1.4 and 8.2.x.

When working in the CLI shell (vs. the BASH shell) of a Forescout device, users must provide their Linux sudo password in order to run fstool commands that are classified as *privileged*. This mitigates against a user leaving their terminal open, since someone else must know the user's Linux sudo password in order to abuse the terminal to run privileged fstool commands.

- The password to provide is the user's own Linux sudo password (their login credential)
- When user attempts to execute a privileged fstool command, the user is then prompted to enter their Linux sudo password
- Once the user enters their password, it is cached for 5 minutes per session (the default cache period). There is no caching between SSH sessions.

The following are examples of the message prompt that displays when a user, working in the CLI shell of a Forescout device, attempts to run a privileged fstool command:

```
cliadmin@ em>shell
[sudo] password for cliadmin:

testadmin@ em>user list
[sudo] password for testadmin:
```

File Transfer

Some of Forescout platform's administration and feature configuration tasks are performed by customizing files on the Appliance. Typically each of these features has a dedicated CLI command that generates an archive or makes a file available for download.

A *SecureFTP* CLI user can access Appliances via SFTP only and access log/shared/OS log files. See user – Configure User Roles and Permissions for details.

In addition, you can use the following general procedure to perform these tasks (for shared files only):

1. Log in to the CLI on an Appliance.
2. Use the dedicated CLI command provided by Forescout platform to generate a specific archive or make a file available for download.
3. On your work machine, use the Linux Secure Copy (SCP) command to transfer the downloaded file(s) from the Appliance to the work machine. Use the CLI user **cliadmin** for this command:

   scp <*filename.xyz***> cliadmin@<***CounterACT_device_IP***>:<***filename***>**
4. After editing the files, use the **SCP** command to transfer the file(s) to the Appliance.

   scp cliadmin@<*CounterACT_device_IP***>:<***filename.xyz***> <***localfile***>**
5. Use the dedicated CLI command provided by Forescout platform to process the files.

When you use the SCP command on Appliances, omit standard flags that specify pathnames. These flags are not parsed by Forescout platform.

FS-CLI Commands

The FS-CLI contains a number of commands that are either unique to the FS-CLI, or carry the same command name as in the Bash shell but behave differently.

? – List of Available Commands

View a list of available commands.

Usage: **?**

clear_shared – Clear Shared Directory Content

This command is not available in the Bash shell.

Use this command to empty content from the shared folder.

Usage: clear_shared

crypt – Disk Encryption Tool

Use this command to encrypt log and database partitions.

When you enable disk encryption:

- Forescout services are stopped until the encryption process completes.
- The log partition is deleted. Back up the logs if needed.
- If you have a High Availability pair, verify that you are:
  - Enabling encryption on the Standby node first
  - That the High Availability state is valid.

Usage: **crypt**

- **crypt enable** - enable disk encryption
- **crypt disable** - disable disk encryption
- **crypt status** - disk encryption status

crypt and FIPS

You cannot enable disk encryption in FIPS mode (See also fips - Toggles the current FIPS status).

If you run **crypt enable** and FIPS mode is active, the CLI issues the following warning message:

```
'fstool crypt enable' is not supported in FIPS mode. Before you
enable disk encryption, you must first disable FIPS mode. When
disk encryption has completed, you can enable FIPs mode again.
```

Once disk encryption is enabled (after reboot), the CLI issues the following warning message:

```
FIPS mode is currently disabled, but was enabled prior to
enabling disk encryption. You can enable FIPS mode with the
'fstool fips' command.
```

date – OS Date

Display the current time.

dhclasstest – Test DHCP Fingerprint

You can use this command to troubleshoot DHCP-related issues.

Usage: **dhclasstest** <command> <params>

Commands:

- **testfp** - test specific fingerprint and/or vendor_id

  Syntax: **testfp** [**-h** <ip>] [**-f** <fingerprint>] [**-v** <vendor_id] [**-c**] [**-p**] [**-d**] [**-4**] [**-6**] [**-b**] [**-O**]

- **testdb** - test entire fingerprint database

  Syntax: **testdb** [**-o** <os>] [**-p**] [**-d**] [**-c**] [**-4**] [**-6**] [**-b**] [**-O**]

- **dumpdb** - dump entire database (FP_DB and FP_HASH contents)

  Syntax: **dumpdb** [**-p**] [**-4**] [**-6**] [**-b**]

Parameters:

-h <ip>	Test using dhcp_fingerprint and dhcp_vendor for a specific host <ip>
-f <fingerprint>	Test a <fingerprint> value, e.g., "1,15,3,6,44,46,47,31,33,43,252,12"
-v <vendor_id>	Test a <vendor_id> value, e.g., "MSFT 5.0"
-o <os>	Test an <os> value, e.g., "100"
-c	Show all colliding Class and OS results for blank <fingerprint> or <vendor_id> values
-d	Show detailed output
-4	Use ipv4 database only (default)
-6	Use ipv6 database only
-b	Use both ipv4 and ipv6 databases
-p	Show OS/Class collisions and other database problems - enabled by default for dumpdb and testdb commands
-O	Test using old lookup method

dns – Configure/List CounterACT Name Server(s) (DNS)

You can use this command to check DNS server settings and troubleshoot DNS-related issues.

Usage: dns [-l]

engine – Forescout Packet Engine Control

You can use this command to troubleshoot, configure and maintain the Packet Engine Plugin.

Input parameters: [**kill | reopenlog | dump_stack | dump_core | status | version**]

- **reopenlog** - Request engine to reopen log
- **dump_stack** - Request engine to dump stack logs
- **cycle_core** - Restart core purge cycle
- **dump_core** - Request engine to dump core file
- **kill** - Forcibly terminates engine
- **status** - Engine status
- **version** - Engine version

exit – Exit CLI

Exit the FS-CLI.

fingerprintkey – Verify CounterACT Device Signature

Displays the CounterACT Device signature digest.

The signature is the message digest of the key certificate that is assigned to your CounterACT device. The signature appears in the Authorization Manager dialog box when you transfer your system to the Strong Authentication Mode. Use this command to verify that this key signature and the key signature of your CounterACT device are identical.

Usage: **`fstool fingerprintkey`**

list – List Directories and Log Files

This command is not available in the Bash shell.

Use the list command to list directories and log files saved by Forescout in the 'log' folder, operating system logs saved in the 'oslog' folder, or shared files that were saved in the 'shared' folder.

See also monitor - Monitor Tail of Log File, search – Search For and Within Log Files and view – View Log Files.

Input parameters: **`[log | oslog | shared]`**

- **`log`** - View appliance log files
- **`oslog`** - View log files
- **`shared`** - View upload/download shared folder

Examples:

```
cliadmin@app> list log
d somefolder
- 292K sample_log.txt

cliadmin@app> list log:plugin/va
d store
1.1M va.log
```

* where **`d`** indicates a directory, and **`-`** indicates an individual file

monitor - Monitor Tail of Log File

This command is not available in the Bash shell.

Monitor the tail end of the log files saved by Forescout in the 'log' folder, operating system logs saved in the 'oslog' folder, or shared files that were saved in the 'shared' folder. This allows you to see if anything in the file has changed.

See also list – List Directories and Log Files, search – Search For and Within Log Files and view – View Log Files.

Examples:

```
monitor log:watch_dog.log
monitor log:plugin/va/va.log
monitor oslog:audit/audit.log
```

password – Change CLI Password For Current User

Allows the current user to change their CLI Password. You set the rules for the composition and length of this password in the Console > *Tools* > *Options* > *User Profiles* > *Password and sessions*.

quit – Exit CLI

This command is not available in the Bash shell.

Exit the FS-CLI.

rename_admin_user – Rename Admin User

Use this command to rename the cliadmin (FS-CLI) or admin (Bash shell) user.

Usage: **`rename_admin_user <new admin user name>`**

resolve - Resolve Host Address by Name

Allows an admin user to get the IP address for a specific hostname, which may be helpful for troubleshooting.

Usage: **`resolve [-f] host_name`**

Usage: **`resolve -u name1=ip1 name2=ip2 …`**

search – Search For and Within Log Files

This command is not available in the Bash shell.

Use this command to search inside log files saved by the Forescout platform.

See also list – List Directories and Log Files, monitor - Monitor Tail of Log File and view – View Log Files.

Usage:

cliadmin@app> search <pattern/regex> <parent dir>:filename

cliadmin@app> search <string> <parent dir>:filename

Examples:

cliadmin@app> search test1 log:filename

cliadmin@app> search "Sending.*pid" log:daemon/www.log

cliadmin@app> search "kernel: IPv4:" oslog:messages

cliadmin@app> search support shared:uploaded_file

shell – Return to Bash Shell from FS-CLI

This command allows you to exit the FS-CLI and access the operating system's Bash shell.

ssh -t server -o RekeyLimit – Configure Thresholds for SSH Rekeying

Allows you to configure thresholds for SSH rekeying.

Example:

ssh -t server -o RekeyLimit "1G 1h"

where **1G** is the max amount of data transferred before a rekey happens and **1h** is the max time before a rekey happens. The two numbers must be enclosed in quotation marks. You are then asked to restart the ssh daemon for the change to take effect.

The max amount of data can be specified in bytes (no units), kilobytes (example: **1048576K**), megabytes (example: **1024M**) or gigabytes (example: **1G**).

The max amount of time can be specified as '**<no>h<no>m<no>s**' (example: **1h30m10s** for 1 hour, 30 minutes and 10 seconds) or 'none' to disable time threshold.

To reset to defaults (1 gigabyte and 1 hour) run the command without arguments:

- **ssh -t server -o RekeyLimit**

In a High Availability environment, there are separate settings for the Forescout partition and the miniroot. The command should be run separately on each High Availability node and on the partition.

summary – Detailed Appliance Summary

This command is not available in the Bash shell.

Use the command to display detailed information about the Appliance, for troubleshooting or when contacting Forescout Support.

tech-support – Technical Support Utility

Use the command to send logs to Forescout Customer Support. During communication with Forescout Customer Support, they may recommend that you run this command to help troubleshoot issues.

unmanage – Disconnect CounterACT from Enterprise Manager

Use this command to disconnect an Appliance from the Enterprise Manager.

user – Configure User Roles and Permissions

This command is not available in the Bash shell.

You can add a new CLI user and grant the user permissions to perform specific operations within the CLI. You can also update permissions for existing users.

- CLI Admin. Has full permissions to perform all operations.
- Operator. Similar to CLI Admin, but cannot add users or update permissions.
- Auditor. Can run the tech-support command.
- SecureFTP. Access Appliances via SFTP only and access log/shared/OS log files.

Input parameters: **`[add | add-external | del | list | update | auth]`**

- **`user add`** – Add a new user
- **`user add-external`** - Add a new external user (e.g. RADIUS or LDAP)
- **`user del`** - Delete existing user
- **`user list`** - List CLI users
- **`user update`** - Update user
- **`user auth`** - Authentication configuration

view – View Log Files

Use the command to view log files saved by the Forescout platform in the 'log' folder, operating system logs saved in the 'oslog' folder, or shared files that were saved in the 'shared' folder.

See also list – List Directories and Log Files, monitor - Monitor Tail of Log File and search – Search For and Within Log Files.

Alphabetical Listing of fstool Commands

This section provides an alphabetical listing of fstool commands and a short command description. Items listed in blue are linked to more detailed explanations and related functions.

fstool Command - Description
acpi - Enable/Disable ACPI Shutdown
addradius - Add RADIUS Server to VPN/Switch 802.1X Plugin
anomaly - Display Anomaly IPs or Channels
asymnet - Enable/Disable Network Asymmetry Test
backup/restore - Backup and Restore
chmod – Toggle Appliance Operation Mode
clear_time_data – Clock Issues in
clients - Enable Console Access to
conf - Repeat Forescout Configuration Procedure
config_sum - CounterACT Appliance Configuration Summary
convert_patch_path - Update Location to Display Microsoft Patches
data_reset - Reset System Data
dns - Configure Appliance Name Servers DNS
ethset - Configure Interface Speed/Duplex
ethtest – Identify Ethernet Ports on Appliance
exclude_arp – ARP Exclude List
fips - Toggles the current FIPS status
fw - Control Built-in Firewall
fw delhook - Remove Rules or Commands from Built-in Firewall
ha – High Availability Utilities
ha_setup - High Availability Setup
help – List fstools with Description
hwstat – Test Hardware Status

fstool Command - Description
ifcount – Display Network Traffic
injectnet – Disable Response (Injection) Test
kbd – Change the Forescout Keyboard
key - Verify CounterACT Device MD5 Signature
linktest – Test NIC Connectivity
mail conf - Configure Mail/Mail Relay Values
model - Obtaining Appliance Model Information
netconfig - Changing Operating System Network Configurations
netest - Network Visibility Test Tool
nphalt - Stop the NAC Policy
ntp – Network Time Protocol
passwd – Update Admin Password
plugin – Plugin Control Tool
restore – Restore from FSB File to Another Forescout System
service – Display Service Status
setmapiport – Set MAPI Service Port
sitedb –Backup and Restore Site Table
smime gen - Generating a Certificate Signing Request (CSR)
smime export - Regenerating the Existing Signing Request
smime import pem - Importing a Signed S/MIME Certificate in a PEM file
smime import pfx - Importing a Signed S/MIME Certificate in a PFX file
smtpp - Enable and Disable SMTP Privacy
snapsend – Send to SnapShot Server
snapshot – Create Snapshot
ssh - Update SSH Access to Enterprise Manager
sysinfo - View Extensive System Information about the Appliance

fstool Command - Description
sw netconf – Debug Configured Switches Using NETCONF
sw snmpwalk – Debug Configured Switches Using SNMP
sw traps – Configure Cisco Switches for MAC traps
tty - Manage Built-in tty
tz - Change Time Zone Setting
upgrade – Upgrade Forescout from a File
va_test – Test Remote Host
version – Display Appliance Version
wormdelay - Worm Slowdown Mechanism

The fstool Command Set by Categories

The fstool Command Set was developed by Forescout to help configure options and to help troubleshoot during installation and configuration. It consists of powerful commands given from the command line that make it easier for an experienced user to control the Forescout platform and connected hardware.

These commands are available when you are accessing the Bash shell. Many fstool commands are also available when you are accessing FS-CLI. An indication is given if the command is not available in FS-CLI.

Machine Administration

acpi - Enable/Disable ACPI Shutdown

Enables/disables ACPI (Advanced Configuration & Power Interface). Reboot is required to enable.

When disabled, press the power button, the machine cleanly shuts down the Enterprise Manager service and powers off. The default is Enabled.

Usage: **`fstool acpi`**

To enable/disable ACPI shutdown:

1. Log in to the CounterACT device CLI.

2. Run the following command: **fstool acpi**

   The following message appears:

```
ACPI is currently enabled.
Disable ACPI (will be applied after reboot? (yes/no)
```

3. Type yes and press **Enter**. The following message appears:

```
Disabling ACPI...
Updating boot parameters...
Boot parameters updated successfully.
Reboot is required for changes to take effect.
Reboot now? (yes/no) [yes]
```

4. Press **Enter** to reboot and enable the ACPI shutdown.

asymnet - Enable/Disable Network Asymmetry Test

This command is not available in FS-CLI.

Enable/disable the asymmetry test. The test verifies that Forescout platform is able to see symmetric traffic, for every session, on the monitoring interface(s), both incoming and outgoing.

Usage: fstool asymnet

You can enable/disable the asymmetry test, as required. The test verifies that Forescout platform is able to see symmetric traffic on the monitoring interface(s). That is, for every session, both incoming and outgoing directions are visible.

To disable/enable the test:

1. Log in to the CounterACT Appliance CLI.
2. Run: **fstool asymnet**

   The following message appears:

```
Asymmetric Network Detection is currently disabled.
Enable Asymmetric Network Detection? (yes/no) :
```

3. Type **yes** and press **Enter**. The following message appears:

```
Enabling Asymmetric Network Detection...
Restarting CounterACT Engine...
```

backup/restore - Backup and Restore

This command is not available in FS-CLI.

Backup of a Forescout system and then restore the same system on another machine to replace the existing one. The backup data includes the following:

- Configuration
- License
- Operating System configuration

- Plugins

This includes, for example:

- Forescout platform IP address
- Root password
- License information
- Channel
- E-mail
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

The backup does not include event data.

Usage: **`fstool backup backup-file`**

In order to proceed correctly, the backup procedure requires the following files to be located under **`/usr/local/forescout/lib/perl/forescout/`**:

- **`util.ph`**
- **`db.ph`**
- **`if.ph`**
- **`help.ph`**
- **`event_log.ph`**
- **`plugin.ph`**
- **`getopts.pl`** to be found under **`/usr/lib/perl5/5.6.0/`**

Backup / restore of a Forescout system can be performed using one of following three methods:

- Using the menu option *Restore saved CounterACT configuration* from the menu that appears when accessing a non-configured system
- From the Control Center.
- Using: **`fstool backup | restore`** from the command line.

These options are detailed below:

*It is necessary to stop the Forescout engine before running the fstool backup/restore command (use: **`fstool service stop`**).*

Non-configured system

When accessing a non-configured system or a new system from production, the restore option is available in a menu that appears on the screen, as in the following example:

```
Options:
1) Configure CounterACT-8.1.2
2) Restore saved CounterACT-8.1.2 configuration
3) Identify network interfaces
4) Configure keyboard layout
5) Turn machine off
Choice (1-5) :
```

Choosing the *Restore saved CounterACT-X configuration* option initiates an interactive restore procedure, where the backup file can be searched over a USB storage device, CD-ROM, floppy diskette or to display a shell prompt.

After the restore procedure is completed, the installation log is written to:

`/tmp/CounterACT-install.log`

And the system needs to be rebooted for completing the procedure.

restore – Restore from FSB File to Another Forescout System

Restores from an FSB file to another Forescout system, using the following syntax:

`fstool backup/restore <full path file name>`

The **`fstool backup/restore`** command should be run only after the Appliance has been stopped (use: **`fstool service stop`**)

For details on backup and restore, see: backup/restore.

clear_time_data – Clock Issues in CounterACT device

Forescout platform depends on the clock installed on the CounterACT device to set time-sensitive information, and it should be accurate. This option clears time sensitive data from the CounterACT device database.

If this clock malfunctions or has been incorrectly set, all the dates and times displayed in the Console will be incorrect. For example, you may see dates of host events that were previously blocked, but appear with future times.

If the clock is incorrect, you must stop the CounterACT device, fix the clock and then delete time-related information from the CounterACT device. This information includes the event logs and audit trails reports.

This information includes the event logs and audit trails reports if you are logged in to the Enterprise Manager. If you are logged in to the Appliance, the following information is lost:

- Virtual site host information
- User names and host names for marks
- All information regarding probing, infected and manually added source events
- All lockdown event information (only applicable for Enterprise solution systems)

- Event logs and audit trails reports

In addition to permanently losing this information, all blocked sources are released.

To clear time-related information:

1. Log on to the CounterACT device CLI.
2. Run: **fstool clear_time_data**
3. The following message appears:

```
This command removes time sensitive data from
Management database.

It should be used when the system clock is moved
backwards.
```

The complete procedure is:

```
1. Stop the Enterprise Manager
2. Change the time
3. Run this command
Continue? (yes/no)
```

If you stopped the Enterprise Manager and fixed the clock, select **yes**.

convert_patch_path - Update Location to Display Microsoft Patches

This command is not available in FS-CLI.

By default, Forescout platform continuously displays patch links that reside on the Microsoft website. An option is available, however, to define a local server from which to centrally manage your patch updates. You may want to do this if you are using customized patch packages. If necessary, you can also restore to the original Microsoft path.

This fstool replaces vulnerability patches from **%root%/patch** to **%user_root%/patch**

If necessary, it can also restore original patches.

Input parameters: **[restore | replace user_root]**

Example: **fstool convert_patch_path replace http://my_server/patches**1 **at lib/fstool/commands/convert_patch_path.pl line 17**.

To change the path:

1. Define a location on a local server from which to download the patches.
2. Log in in to the Appliance or Enterprise Manager.
3. Run: **fstool convert_patch_path**

The following prompt appears:

```
This fstool replaces vulnerabilities patches from
%root%/patch to %user_root%/patch
```

If necessary, it can also restore original patches.

Input parameters: **[restore | replace user_root]**

Example: **fstool convert_patch_path replace http://my_server/patches**1
at lib/fstool/commands/convert_patch_path.pl line 17

exclude_arp – ARP Exclude List

This command is not available in FS-CLI.

Add/Remove/Display ARP resolving exclude list.

IP addresses that are included in the ARP domain AND are listed in the Exclude ARP list, will not respond to requests when baiting.

exclude_arp - Add/Remove/Display ARP resolving exclude list.

Use:Add : fstool exclude_arp -s [-m mac] [-i ip] [description]

or

Del: fstool exclude_arp -d [-m mac] [-i ip]

or

List: fstool exclude_arp -l

Example:

fstool exclude_arp -s -m 00:02:B3:8B:02:7E -i 192.168.1.2 hostA mac address

fips - Toggles the current FIPS status

The FIPS option configures Forescout platform to meet FIPS 140-2 (level 2) requirements. This option is only recommended for Forescout platform deployments in the US Federal government, where FIPS is required. SSH cannot be used to connect to Appliances in FIPS mode.

Disk encryption is not supported when FIPS is enabled. See crypt – Disk Encryption Tool.

To enable the machine as FIPS:

1. Log in to the CounterACT Appliance.
2. Run: **fstool fips**

   The following warning message appears requesting command confirmation:

   ```
   You are about to enable FIPS 140-2 on this CounterACT
   machine.
   Note that CounterACT service will be restarted.
   Enable FIPS and restart CounterACT service? (yes/no) :
   ```

3. Enter **yes** or **no** to either confirm or cancel the command, respectively.

To disable the machine as FIPS:

1. Log in to the CounterACT Appliance.

2. Run: **fstool fips**

   The following warning message appears requesting command confirmation:

```
You are about to disable FIPS 140-2 on this CounterACT
machine.
Note that CounterACT service will be restarted.
Disable FIPS and restart CounterACT service? (yes/no) :
```

3. Enter **yes** or **no** to either confirm or cancel the command, respectively.

fw - Control Built-in Firewall

Test connectivity between Appliances with the rest of the network.

The internal firewall that protects Forescout platform can be temporarily disabled to allow all communications or ICMP communication only. This tool is useful for testing connectivity with the rest of the network.

To control the built-in firewall:

1. Log in to the CounterACT Appliance CLI.
2. Run the following command:

   fstool fw

   The following status message appears displaying the current built-in firewall protection status:

```
Status: Only required traffic is enabled
Options:
1) Enable ICMP traffic.
2) Enable all traffic.
3) Enable required traffic only (default).
4) Quit.
Choice (1-4)
```

3. Select an option and press **Enter**.

   Selecting option **1** or **2**, disables the built-in firewall for a specified time period.

   – Select **1** to ping nodes with which Forescout platform must communicate, for example the name server.
   – Select **2**, to allow all traffic. This option is inherently unsecure.

4. At the prompt: Time period (in minutes) [10] :, specify the time period (in minutes) for which traffic will be enabled and press **Enter**. A message appears indicating the current time and date and the time and date the traffic will be allowed. For example:

```
Date  : Wed Jun 16 13:22:56 2004
Status: ICMP traffic is enabled until Wed Jun 16
13:27:56 2004
```

   After the time you entered expires, the default built-in firewall default status is reinstated. This option allows required traffic only.

fw delhook - Remove Rules or Commands from Built-in Firewall

To remove a named set of rules or commands:

1. Log in to the Appliance.
2. Run the following command:

   `fstool fw delhook <hook_name>`

   where **`<hook_name>`** is a text string that identifies a previously applied set of rules or commands.

   The following command removes the previous set of iptable commands:

   `fstool fw delhook newrule`

injectnet – Disable Response (Injection) Test

This command is not available in FS-CLI.

Disable the response (injection) test when network conditions prevent the test from working properly. You know that the test is not working properly when you start observing response failures that are in fact host bites. If specific network conditions prevent the test from working properly, you can disable it.

To disable the test:

1. Log in to the CounterACT Appliance CLI.
2. Run: **`fstool injectnet`**
3. Follow the instructions for disabling the test.

linktest – Test NIC Connectivity

Test NIC connectivity and interfaces.

Usage: **`fstool linktest`**

The following is a sample result of this command:

```
--------------------------
Management interface status
--------------------------

Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half
10baseT/Full
                                100baseT/Half
100baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half
10baseT/Full
                                100baseT/Half
100baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Half
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: puag
        Wake-on: g
        Link detected: yes
-----------------------------------
Pinging default gateway (10.0.4.XXX)
-----------------------------------
PING 10.0.4.251 (10.0.4.251) from 10.0.4.231 : 56(84)
bytes of ata.
64 bytes from 10.0.4.XXX: icmp_seq=0 ttl=64 time=271
usec
64 bytes from 10.0.4.XXX: icmp_seq=1 ttl=64 time=236
usec
64 bytes from 10.0.4.XXX: icmp_seq=2 ttl=64 time=249
usec
64 bytes from 10.0.4.XXX: icmp_seq=3 ttl=64 time=252
usec
64 bytes from 10.0.4.XXX: icmp_seq=4 ttl=64 time=247
usec

--- 10.0.4.XXX ping statistics ---
5 packets transmitted, 5 packets received, 0% packet
loss
round-trip min/avg/max/mdev = 0.236/0.251/0.271/0.011
ms
Success pinging 10.0.4.XXX
------------------------------
Performing Name Resolution Test
------------------------------
Resolving www.forescout.com address...
Success resolving www.forescout.com address.
------------
Test summary
```

```
------------
Default gateway ping test : OK.
Name resolution test      : OK.
```

mail_conf - Configure Mail / Mail Relay Values

This command is not available in FS-CLI.

Change/display mail configuration. The Forescout operator receives emails from Forescout platform on intrusion events and other information. If Forescout platform does not have full access to external SMTP and DNS servers, an internal mail-relay address must be configured. Several options are available updating mail-relay values that you previously defined.

In addition, you can also define a mail relay host and IP address if you have not already done so or test the connectivity to the mail relay. You must restart the Appliance after making changes.

Other options are available to:

- Update addresses that receive e-mail alerts
- Send an e-mail test
- Change the sender address (for example if the address must be changed as a spam protection mechanism, i.e. the mail server reads the default sender address as illegal.)

Defining a Mail-Relay Address / Host Name

To configure a mail-relay address:

1. Log in to the CounterACT Appliance CLI.
2. Run the following command:

   `fstool mail_conf`

   If the mail relay has not yet been defined, the following message appears:

   ```
   Mail-relay is not defined:

   1) Define mail-relay.
   2) Send test E-mail.
   3) Change operator E-mail address(s).
   4) Change sender address.
   5) Done.

   Choice (1-5) :
   ```

3. Type **1** and press **Enter**. At the prompt:

   ```
   Enter mail-relay host name or IP address:, enter the
   required host name or IP address.
   ```

   The current mail relay address is displayed. You can test the connectivity of the address by selecting option **3** in the prompt that appears.

4. Run the **`fstool service restart`** command if you change the host name or IP address.

Updating Current Mail Relay / Mail Configurations

To update the current mail-relay address or other mail configurations:

1. Log in to the CounterACT Appliance CLI.
2. Run the following command:

   `fstool mail_conf`

   If the mail relay has already been defined, the following message appears:

```
Current mail-relay is xx-xxxxx.xxx.xxxxxx.com: (where x
is the address)

1) Disable mail-relay.
2) Change mail-relay settings.
3) Test connectivity to mail-relay.
4) Send test E-mail.
5) Change operator E-mail address(s).
6) Change sender address.
7) Done.
```

3. Select option **1** or **2** to either disable or change the address, or option **3** to test mail relay connectivity.
4. Run the **`fstool service restart`** command if you change the host name or IP address.

model - Obtaining Appliance Model Information

Use this command to view the Appliance model and hardware revision.

To obtain the appliance model and hardware revision number:

1. Log in to the Appliance.
2. Run: **`fstool model`**

```
# fstool model
CT1000-21
#
```

netconfig - Changing Operating System Network Configurations

The network configuration options defined during your Operating System installation can be modified from the CounterACT device

The following configurations can be changed:

- Network Interfaces Card (NIC) configuration, including the interface addresses, Appliance IP address and VLAN configuration
- Default gateway

To redefine the network configuration:

1. Log in to the CounterACT device CLI.
2. Run the following command:

   fstool netconfig

   The following menu opens:

```
CounterACT Machine Network Configuration Options:

1) Configure network interfaces
2) Configure default gateway
3) Restart network services
4) Quit

Choice (1-4):
```

3. Type **1** to reconfigure the Ethernet interface, interface addresses, and VLAN configuration. Type **2** to reconfigure the default gateway.
4. After reconfiguring, you are asked to restart the network service. This applies your changes.
5. Select **yes**.

netest - Network Visibility Test Tool

This command is not available in FS-CLI.

Usage: **fstool netest [options]**

-i input	Colon separated NICs with optional VLAN tags. Such as: **eth0:eth1(1):eth2(2,7-9)** (default is Appliance input interfaces)
-n network	Comma separated network ranges (default is internal network)
-T tags	VLAN id tags (default as defined in Appliance channel)
-t timeout	Time in seconds to monitor network (default fs.netest.timeout=300)
-j timeout	Time in seconds for response (injection) testing (fs.netest.injection=fs.netest.timeout -1 to disable)
-m timeout	Test minimum time in seconds (fs.netest.timeout.min=30)
-c count	Max number of packets to monitor (fs.netest.packet.max=none)
-f cutoff	Seconds to cut off monitoring time (fs.netest.cutoff=1)
-e	Don't ignore Engine's traffic (fs.netest.ignore.engine)
-s	Report open TCP services (**fs.netest.show.services**).
-r seconds	Timeout for address-to-name resolution (**fs.netest.resolve**)
-p	Progress period (default 15 seconds)

-v	Verbose
-o output	Output file (**fs.netest.output=/tmp/netest.out**)
-d	Dup **stderr** to **stdout**
-A	Don't ignore sessions where the server is outside the network (**fs.netest.all_sessions**)
<filter>	pcap filter (**fs.netest.filter=none**)

*For more options see the **fs.netest.*** properties.*

Algorithm:

TCP sessions are checked to see if the acknowledged sequence number has advanced. If it did, then we need to see also traffic in the opposite direction. Exceptions are if some traffic is lost, or if the payload which the second ACK acknowledge has occurred before the monitoring started.

Unless -A is specified, only sessions of which the server side is within the network are considered.

Response (injection) testing is done by observing ARP requests on each of the defined channels. The IP address of the ARP request originator is noted, and an ARP request for this IP address is injected using the corresponding channel's outgoing interface. If an ARP reply for this request is seen, the test is passed for this channel.

nphalt - Stop the NAC Policy

Using this tool stops the trigger detection method and releases all blocked hosts. You may need to use this tool if you cannot access your Console but need to stop the NAC Policy. Policies are saved and not lost.

To stop the NAC Policy:

1. Log in to the CounterACT Appliance.
2. Run: **fstool nphalt**

ntp – Network Time Protocol

Synchronize the Appliance NTP time with a global Network Time Protocol server.

Usage: **fstool ntp setup <list of ntp servers> | configure | test**

fstool ntp setup - shuts down the local NTP server(s), synchronizes time with the global NTP server, and restarts the local NTP server(s).

```
Shutting down ntpd:
[  OK  ]

6 Nov 13:02:34 ntpdate[16297]: adjust time server
212.179.35.137 offset 0.031622 sec

Synchronizing with time server:
[  OK  ]

Starting ntpd:
```

fstool ntp configure <ntp servers>

To configure the local NTP server.

fstool ntp test

Tests connectivity with NTP servers, as in example below:

Remote	refid	st	t	when	poll	reach	delay	offset	jitter
LOCAL(0)	LOCAL(0)	10	l	5	64	1	0.000	0.000	0.008
*geo.forescout.noubliette.mctav		2	u	3	64	1	14.218	-0.588	0.008

oneach - Execute Commands on all Appliances

This command is not available in FS-CLI.

Execute a command on all managed CounterACT Appliances.

This tool works on a management server only, and only if the CounterACT Appliances allow SSH access from the management server.

If the command is "scp <from> <to>", the file will be copied to all Appliances. If <to> is not specified, the file is copied with the same path as <from>.

Usage: **fstool oneach [options] command**

The following options can be specified before the command that you are executing on all Appliances:

-t <timeout>	Timeout before giving up on less responsive systems (default: 30 seconds).
-f <file>	A file containing Appliance IP addresses, one per line, on which to run the command.
-c	Execute the command concurrently on all appliances.
-R	Include Recovery Manager
-o "<ssh options>"	Execute scp with special flags, e.g., -r

serial - Displays Appliance Serial Number

Use this command to display the serial number of the Appliance, for use when troubleshooting or contacting Forescout Support.

sysinfo - View Extensive System Information about the Appliance

Use this command to view extensive system information for an Appliance.

To view system information about the Appliance:

1. Log in to the Appliance.
2. Run: **`fstool sysinfo`**
3. A full printout of system information for the Appliance is displayed.

tz - Change Time Zone Setting

You can change the time zone setting configured during the Forescout installation process.

To change the time zone:

1. Log in to the CounterACT Appliance CLI.
2. Run: **`fstool tz`**

   The following message appears:

   ```
   Current time-zone : XXX/XXXX
   Local time is now : Sun Aug  1 11:47:19 2004
   Universal time is now : Sun Aug  1 08:47:19 2004

   Select different time-zone? (yes/no) :
   ```

3. Type **yes** and press **Enter**. The following message appears:

   ```
   Time zone specification:

   Specify time-zone by geographical location
   Specify time-zone by GMT offset
   ```

4. Follow the instructions for setting the time zone.

upgrade – Upgrade Forescout from a File

This command is not available in FS-CLI.

Upgrade Forescout from a file (fpifile, either downloaded or received on a CD).

Usage: **`fstool upgrade service_pack_file`**

wormdelay - Worm Slowdown Mechanism

This command is not available in FS-CLI.

The worm slowdown mechanism reduces network traffic congestion and provides added protection to hosts within a cell as well as the remaining network by locking an infected machine in static TCP dialog. The worm slow mechanism is enabled by default but can be disabled if required.

To disable the Worm slowdown mechanism:

1. Log in to a CounterACT Appliance CLI.
2. Run: **`fstool wormdelay disable`**

   The following message appears:

   ```
   CounterACT should be restarted for changes to take
   effect.
   Restart CounterACT?
   ```

3. Enter **`yes`**.
4. To enable the worm delay mechanism, run the following command:

   `fstool wormdelay enable`

va_test – Test Remote Host

The **`va_test`** command tests connectivity, interoperability and access rights (whether the host is managed or not) on the remote host. As part of the process it copies two files to the host root drive:

1. **`fs_pro.vbs`**
2. **`fs_outListxx.xx.xx.xx.txt`**

Usage: **`fstool va_test -h host_IP -c command`**

`-h <ip>`	**Tested host IP address**
`-v`	**Verbose**
`-r <registry path>`	**Registry path**
`-c <command>`	**`- all | services | reg_enum | reg_val | reg_walk | smb | copy_file | file_cp | file_rm | sched | nmap | nmapf | banner | member | manage | shared_dirs | version | user | script | fsproc_log | fsproc_dbg`**

For more commands or switches, see the command line help for this command.

Sample Output:

```
[root@root]# fstool va_test -h 10.0.0.37 manage

Starting testing on host[10.0.0.37]

    Port: 445 result[Success] , 139 result[Success]

    Testing user[counteract] domain[fsd]

       registry[HKLM] result[Success] entries[4]

       registry[HKLM\SOFTWARE] result[Failed]
entries[0]

       registry[HKLM\SOFTWARE\CLASSES] result[Success]
entries[4807]


registry[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion
\Uninstall] result[Success] entries[87]

       Result[Success] when getting services.
services [97]

       SMB connect to driver[ipc] result[Success]

       SMB connect to driver[c] result[Success]

       SMB File system on driver[c] result[Success]

Copy file[plugin/va/fs_pro.vbs] to [c\:fs_pro.vbs]
res[Success]

Sched task res[Success]
```

version – Display Appliance Version

The **version** command displays the current CounterACT appliance version number.

Usage: **fstool version**

```
[root@ root]# fstool version
----------------------------------------
CounterACT Appliance version information
----------------------------------------
Version          : 6.3.4.0
Build date       : Sat Oct  9 11:14:08 2010 GMT
HA supported     : No
FIPS enabled     : No
```

Security

key - Verify CounterACT Device MD5 Signature

This command is not available in FS-CLI.

Displays the CounterACT MD5 signature.

The MD5 signature is the message digest of the key certificate that is assigned to your CounterACT device. The signature appears in the Authorization Manager dialog box when you transfer your system to the Strong Authentication Mode. It is recommended that you verify that this key signature and the key signature of your CounterACT device are identical.

To verify the MD5 signature:

1. Log in to the CounterACT device CLI.
2. Run: **`fstool key`**

   A message appears with the MD signature.

config_sum - CounterACT Appliance Configuration Summary

This command is not available in FS-CLI.

Display a summary of the Forescout configuration.

Usage: **`fstool config_sum`**

To generate a summary:

1. Log in to the CounterACT device.
2. Run the following command:

   `fstool config_sum`

The following information is displayed:

```
------------------------------------------------
CounterACT Appliance Configuration Summary
Version Information
Version          : 6.0.0
Build number     : 304
Internal Version : 6.0.0
Build date       : Wed Sep 27 06:20:32 2006 GMT
---------------
Host Information
Hostname         : qcc1
Domain name      : qa.lab.forescout.com
Dns              : 10.0.0.3
------------------
Network Information
Gateway          : 10.0.4.251
eth0      Address: 10.0.4.231        Netmask:
255.255.255.0
Channel Configuration Information
Enterprise Manager Configuration
E-mail Privacy        : no
Mail relay          : No mail-relay configured
Operator mail       : No operator mail configured
Protected net       :
Management Clients  : 10.0.0.0-11.0.0.0
SSH Clients         : 10.0.0.0-11.0.0.0
Send the configuration summary via an email? (yes/no)
[yes] :
```

ethset - Configure Interface Speed/Duplex

Modify the default auto negotiation speed and duplex values of Ethernet ports. The configuration should be set in run time and also for the next boot.

1. Log in to the CounterACT Appliance CLI.
2. Run: **fstool ethset**

```
Interfaces speed and duplex configuration:

Interface           Driver              Cur-
Speed/Duplex    Conf-Speed/Duplex   Link Status

eth0       e100    100baseT/Half  Auto/Auto   link ok

eth1       e100    Auto/Full      Auto/Auto   link ok
```

The current interface speed and duplex configuration appears (as above) along with the following message:

```
CounterACT Interfaces Speed and Duplex Configuration
Options:
1) Edit interfaces speed and duplex options
2) Blink interfaces
3) Quit
Choice (1-3) : 1
```

3. Select option **1** to display a list of available Ethernet ports, as in the example below:

```
Choose interface to configure:
1) eth0
2) eth1
3) eth2
4) eth3
5) eth4
6) eth5
7) eth6
8) eth7
Choice (1-8) : 1
```

4. Choose the interface to configure and select Enter. The current configuration appears along with configuration options. The following displays as an example:

```
Choose eth0 configuration:
1) Auto
2) 10baseT/Half
3) 10baseT/Full
4) 100baseT/Half
5) 100baseT/Full
6) 1000baseT/Full
```

5. Configure as required and press **Enter**.
6. Select **2** Blink Interfaces to identify the Ethernet interfaces (ports). This procedure is the same as that for **`fstool ethtest`** (below).

ethtest – Identify Ethernet Ports on Appliance

Usage: **`fstool ethtest`**

`Blinking eth0. Press ENTER for next interface`

`Blinking eth1. Press ENTER for next interface`

When the first message is displayed (**`Blinking eth0. …`**, check the blinking Ethernet port and mark it. Continue with the other ports.

data_reset - Reset System Data

Remove Forescout platform data by section or All.

Resetting the Enterprise Manager data means that you will release all NAC Policy hosts and undo all actions. Policies continue to function after executing the command.

To reset data:

1. Log in to the Enterprise Manager.
2. Run: **`fstool data_reset`**
3. Choose a reset option, as follows:

Usage: **`fstool data_reset all|orgh|intruder|vsite|npsources`**

`orgh`	remove organizational headsups related tables
`intruder`	remove intruders related tables
`vsite`	remove vsite related tables
`npsources`	remove policy hosts tables
`all`	remove all the above tables

ifcount – Display Network Traffic

This tool continuously displays network traffic on the specified interfaces; it works in two modes - by interface or by VLAN (during the display, the mode can be changed). The tool displays the total bits per second and the percentage of each of the following traffic categories:

- Broadcast - incoming broadcast (destination MAC is broadcast and source MAC is not this Appliance).
- Mirrored - destination MAC is of another machine (not this Appliance's MAC and not a broadcast MAC).
- To my MAC - destination MAC is the Appliance's MAC.
- From my MAC - traffic sent by this Appliance (source MAC is the Appliance's MAC, destination can be broadcast or unicast).

Usage: **`fstool ifcount <interface> [<interface>...]`**

Display commands:

`v – display in VLAN mode`

`I – display in interface mode`

`P – show previous`

`N – show next`

`q – quit displaying`

Example

`fstool ifcount eth0 eth1 eth2 …`

(Separate each interface/VLAN by a space.)

Vlan Mode:

```
update=[13]     [eth0: 14 vlans] [eth1: 1 vlans]
Interface/Vlan   Total       Broadcast   Mirrored    To my MAC   From my
MAC
eth0.untagged    3Kbps        26.9%       0.0%        13.5%       59.6%
eth0.9           0bps         0.0%        0.0%        0.0%        0.0%
eth0.10          0bps         0.0%        0.0%        0.0%        0.0%
eth0.11          0bps         0.0%        0.0%        0.0%        0.0%
eth0.12          0bps         0.0%        0.0%        0.0%        0.0%
eth0.13          0bps         0.0%        0.0%        0.0%        0.0%
eth0.14          0bps         0.0%        0.0%        0.0%        0.0%
eth0.15          0bps         0.0%        0.0%        0.0%        0.0%
eth0.16          0bps         0.0%        0.0%        0.0%        0.0%
eth0.17          0bps         0.0%        0.0%        0.0%        0.0%
eth0.18          0bps         0.0%        0.0%        0.0%        0.0%
eth0.19          0bps         0.0%        0.0%        0.0%        0.0%
eth0.20          0bps         0.0%        0.0%        0.0%        0.0%
eth0.21          475bps       100.0%      0.0%        0.0%        0.0%
eth1.untagged    0bps         0.0%        0.0%        0.0%        0.0%



Show [v]lans [i]nterfaces     <-[p]rev  [n]ext->             [q]uit
```

Interface Mode:

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interface        Total      Broadcast  Mirrored   To my MAC From my MAC
eth0             3Kbps        42.3%       0.0%        14.1%      43.7%
eth1             475bps       0.0%        100.0%      0.0%       0.0%
```

sitedb –Backup and Restore Site Table

This command is not available in FS-CLI.

Usage: **fstool sitedb** <option>

backup - Back up site to file.

restore <from file> - Restore site from file.

version - Display Forescout version information.

Sample display:

```
-----------------------------------------------
CounterACT/Enterprise Manager version information
-----------------------------------------------
Version          : 6.0.0
Build date       : Wed Sep 27 06:20:32 2006 GMT
HA supported     : No
```

Generating CSRs and Importing Signed Certificates

These commands are not available in FS-CLI.

Use the **fstool smime** command to generate Certificate Signing Requests (CSRs) that are submitted to a Certificate Authority (CA). After the CA returns a signed certificate, use this command to import the certificate into Forescout platform. For more information about enabling digital signing of email messages through the Console after a signed S/MIME certificate is imported, refer to the *Forescout Administration Guide*. See Additional Forescout Documentation for information on how to access this document.

The Certificate Authority can return the signed S/MIME certificate in several container file formats. Some of these formats contain just the signed certificate and public key, and some also contain a newly generated private key that must be installed with the signed certificate.

The following commands are only available on the Enterprise Manager:

- smime gen - Generating a Certificate Signing Request (CSR)
- smime export - Regenerating the Existing Signing Request
- To import a container with just the signed certificate and public key, see smime import pem - Importing a Signed S/MIME Certificate in a PEM file.
- To import a container with the signed certificate, public key, and a new private key, see smime import pfx - Importing a Signed S/MIME Certificate in a PFX file.

smime gen - Generating a Certificate Signing Request (CSR)

This command is not available in FS-CLI.

To generate a Certificate Signing Request (CSR):

1. Log in to the Enterprise Manager.
2. Enter the following command:

   $ fstool smime gen
3. If a private key was already generated for the CSR, the following prompt appears:

   A private key already exists. Reuse it? (yes/no) : no

   Choose whether Forescout platform generates a new private key for the CSR, or uses the existing key for the CSR.
4. The following prompts appear. Provide values for the fields as prompted, or press **Enter** to accept previous values, which are displayed in brackets.

   RSA key size [2048] :

   DNS name of this Enterprise Manager [] :

   Organization name [] :

```
Organizational unit name [] :
City or Locality name [] :
State or Province [] :
Two-letter country code for this unit [] :
Email address [] :
```

The email address field represents the Enterprise Manager, which applies the digital signature to emails. The certificate is generated for this email address. Once a signed certificate is installed on the Enterprise Manager, emails are sent with this certificate and the email address configured here appears in the From field. The address should be meaningful, so that users can recognize that it comes from the Forescout Enterprise Manager.

The CSR is generated. A related private key is generated if you opted to generate a new private key.

smime export - Regenerating the Existing Signing Request

This command is not available in FS-CLI.

After you created a CSR, you can regenerate the existing CSR.

To regenerate an existing Certificate Signing Request (CSR):

1. Log in to the Enterprise Manager.
2. Enter the following command:

   `$ fstool smime export`

   The CSR file is generated based on previously entered parameters.

smime import pem - Importing a Signed S/MIME Certificate in a PEM file

This command is not available in FS-CLI.

Use this command to import a signed S/MIME certificate when the Certificate Authority does not generate a new private key. The Certificate Authority returns a container file with the signed certificate and public key, in one of the following file formats:

- PEM
- DER
- P7B

This fstool command supports the PEM file format only. To import a certificate from DER or P7B formatted files, convert it to PEM file format.

To convert from DER to PEM use the following command:

- **`openssl x509 -inform der -in`** <*der_file*> **`-out`** <*pem_file*>

To convert from P7B to PEM use the following command:

- **openssl pkcs7 -print_certs -in** <*p7b_file*> **-text -out** <*pem_file*>

Use the following procedure to import the resulting PEM file:

To import a signed S/MIME certificate in a *.pem file:

1. Log in to the Enterprise Manager.
2. Copy the PEM file to Enterprise Manager.
3. Enter the following command:

   $ fstool smime import pem <*pem_file_full_path*>

   where <*pem_file_full_path*> is the pathname of the PEM file that contains the signed certificate.
4. The following prompt appears:

   Verify that your certificate is in PEM format.

   Continue?(yes/no) [yes] :

   Type **yes**.
5. The certificate is imported and updated.

smime import pfx - Importing a Signed S/MIME Certificate in a PFX file

This command is not available in FS-CLI.

Use this command to import a signed s/mime certificate when the Certificate Authority generates a new private key. When the Certificate Authority generates a new private key, it can return output in several formats:

- A single file in PFX format that contains the certificate and all keys
- A pair of files in PEM or DER format: one file contains the certificate and public key, one file contains the new private key.

This fstool command supports the PFX file format only. To import a certificate and private key from two separate files, first convert them to PFX file format.

To convert a pair of PEM files to a single PFX file, use the following command:

- **openssl pkcs12 -export -out <***pfx_file***> -inkey <***private_pem***> -in <***public_pem***>**

To convert a pair of DER files to a single PFX file, first convert the DER files to PEM files using the following commands:

- **openssl x509 -inform der -in <***public_der***> -out <***public_pem***>**
- **openssl rsa -inform der -in <***private_der***> -outform pem -out <***private_pem***>**

Then convert the PEM files to a single PFX file as described above.

To import a signed S/MIME certificate in a *.pfx file:

1. Log in to the Enterprise Manager.
2. Copy the PFX file to Enterprise Manager.
3. Enter the following command:

   $ fstool smime import pfx <*pfx_file_full_path*>

   where <*pfx_file_full_path*> is the pathname of the PFX file that contains the signed certificate.
4. The following prompts appear:

   Verify that your certificate is in PFX format.

   Continue?(yes/no) [yes] :

   Is the import file protected with a password? (yes/no) : yes

   Enter the import password :

   Is the private key protected with a passphrase? (yes/no) : yes

   Enter the passphrase :

   If the certificate and/or private key have been encrypted, provide password and passphrase values for the imported file and private key as necessary.
5. The certificate and private key are imported and updated.

User Access and Services

clients - Enable Console Access to CounterACT Devices

Edit Forescout Console addresses that are allowed to access CounterACT devices.

IP addresses of the Console that are allowed to connect to the CounterACT device must be listed during the Enterprise Manager installation. These addresses are set up so the Console will be allowed to communicate with the CounterACT device.

If these addresses were defined incorrectly during installation, the Console cannot connect to the CounterACT device. When you try to log in, you will receive a message indicating that the connection timed out. You can correct the Console IP addresses in order to enable access to the CounterACT device.

To update the Console IP address:

1. Log in to the CounterACT device CLI.
2. Run: **fstool clients**
3. A message appears displaying the current list of IP addresses that can connect to the CounterACT device.

Example:

```
Enterprise Manager access list
------------------
192.0.2.0 - 192.0.2.31
192.0.2.63 - 192.0.2.127
(A)dd,(D)elete,(S)ave,(Q)uit :
```

To add an IP address or address range:

1. Type **A** at the command line, and press **Enter**. The following message appears:

   ```
   Range start :
   ```

2. Type in a new start address and press **Enter**. The following message appears:

   ```
   Range end:
   ```

3. Type in a new end address and press **Enter**. Alternatively just press enter to assign one address.
4. Press **S** to save your changes and **Q** to exit the command.

To delete an IP address or address range:

1. Type **D** at the command line, and press enter.
2. Type an IP address range using the conventions shown above.
3. Press **Enter**.
4. Press **S** to save your changes and **Q** to exit the command.

To use an IP address or address range:

1. Log in to the CounterACT device CLI.
2. Run the following command:

   `fstool sw snmpwalk`

ssh - Update SSH Access to Enterprise Manager

To Add, Delete, and Save the list of IP addresses that can access the Enterprise Manager via SSH connection.

SSH access allows you to remotely control the Enterprise Manager. If you specified the wrong list of IP addresses from which SSH access should be allowed during installation, you will need physical access to the machine in order to perform tasks such as re-installation, reboot, and fstool commands.

This has to be done on all Enterprise Managers

To manage the SSH access list:

1. Log in to the CounterACT device CLI.
2. Run: **`fstool ssh`**

3. A message appears displaying the current list of SSH access IP addresses.

   For example:

```
SSH access list
----------------
192.0.2.1
192.0.2.2.
(A)dd,(D)elete,(S)ave,(Q)uit :
```

4. Type **A** at the command line, and press enter.
5. Type in a new IP address.
6. Press **S** to save your changes or **Q** to quit without saving your changes.

To delete an IP address or address range:

1. Type **D** at the command line, and press enter.
2. Type in an IP address.
3. Press **Enter**.
4. Press **S** to save your changes or **Q** to quit without saving your changes.

kbd – Change the Forescout Keyboard

Change the Forescout keyboard layout to support localization (language).

Example:

```
Current keyboard layout is "English"
Select different keyboard layout? (yes/no) [no] :
```

passwd – Update Admin Password

To replace a forgotten administrator password or create a new password.

Your system is installed with a predefined “Admin” user, whose password is set during installation. Admin users who have forgotten their password and as result cannot log in to the Console, can create a new password.

Update the Admin password from the Enterprise Manager. This tool is designed for administrators with root privileges on the Enterprise Manager.

To update the password using the current admin password:

1. Log in to the CounterACT device CLI.
2. Run: **`fstool passwd`**

   The following message appears:

```
Current admin password:
```

3. Enter the current admin password.

   The following message appears:

   ```
   New admin password:
   ```

4. Enter a new password, between 6 and 15 characters (default).
5. Press **Enter**. The following message appears:

   ```
   New admin password (confirm):
   ```

6. Re-enter the password and press **Enter**. The following message appears:

   ```
   User 'admin' password updated
   ```

To reset the password using the root password:

1. Log in to the CounterACT device CLI.
2. Run: **`fstool passwd --reset`**

   The following message appears:

   ```
   Enter 'root' password:
   ```

3. Enter the root password.

   The following message appears:

   ```
   New admin password:
   ```

4. Enter a new password. Use between 6 and 15 characters, including at least one non-alphabetic character.
5. Press **Enter**. The following message appears:

   ```
   New admin password (confirm):
   ```

6. Re-enter the password and press **Enter**. The following message appears:

   ```
   User 'admin' password updated
   ```

service – Display Service Status

CounterACT application control, to start, stop or display status of service.

Usage: **`fstool service start|stop|restart|status|shutdown`**

snapsend – Send to SnapShot Server

This command is not available in FS-CLI.

Send files to Forescout snapshot server.

Usage: **fstool snapsend file [file...]**

snapshot – Create Snapshot

Create and optionally send a snapshot.

The snapshot created is a ZIP file to be sent to Forescout support for analysis. An option allows the snapshot to be sent automatically to the Forescout public server. To enable this, contact Forescout support.

Miscellaneous

addradius - Add RADIUS Server to VPN/Switch 802.1X Plugin

This command is not available in FS-CLI.

Usage: **fstool addradius <vpn|switch802_1x>**

Supported_platforms: UNIX

anomaly - Display Anomaly IPs or Channels

For example, the system thinks it detects unilateral traffic, or unsuccessful response.

Usage: **fstool anomaly -i|-c**

To display anomaly IPs: **fstool anomaly -i**

To display anomaly channels: **fstool anomaly -c**

chmod – Toggle Appliance Operation Mode

This command is not available in FS-CLI.

7.0.0: Enforcement Mode, Partial Enforcement, Full Enforcement (47424, 47464)

The command toggles the Enforcement Node between *Partial Enforcement* and *Full Enforcement*.

Usage: **fstool chmod**

Example:

```
Current Scout operation mode is: Full Enforcement

Change mode to Partial Enforcement? (yes/no) : no.
```

conf - Repeat Forescout Configuration Procedure

Example:

```
*** CounterACT Enterprise Manager Configuration ***

You are about to configure CounterACT Management
Server. When prompted, press <Enter> to accept the
default
```

dns - Configure Appliance Name Servers DNS

The display shows:

```
Either 'yes' or 'no' are acceptable here.
Continue (yes/no)? [yes]:
```

ha – High Availability Utilities

Usage: **fstool ha [-vhH] command [<flags>] [<params>**

To change hostnames on an HA cluster, run: **fstool ha_setup**

Command can be one of the following:

- **install [-f] [-t <template file>] <template arguments>** - Install HA template files.
- **verify [-W(arn only)] [-T(ext format)] <target file> [<Warn only>]** - Check for bad characters in configuration file.
- **properties [-H] [-t <property file>]** - Show HA status properties.
- **status [-t <property file>]** - Show HA status properties.
- **snapshot [-v] [-d <dir>] [<extra files>..]** - Generate a snapshot.
- **template [-f] [-t <template file>] <target file> <template file> [<var1> <value1> ..]** - Configure files using templates, avoid using **$** characters. Use **%..%; -f** for forcing.
- **diag** - diagnoses High Availability status and services and provides advanced log output regarding High Availability status or failure
- **maint [-e]** <enable maintenance>, **[-d]** <disable maintenance task>, **[-s]** <display maintenance task status - enabled/disabled> - to facilitate maintenance operations, this command can disable the cluster/pair mechanism and ignore failover during maintenance procedures.

ha_setup - High Availability Setup

Usage: **fstool ha_setup**

This command is only available from the High Availability miniroot.

help – List fstools with Description

List fstool commands with a brief one-liner description.

hwstat – Test Hardware Status

This command is not available in FS-CLI.

A daemon is periodically activated to collect hardware status data about the Appliance and record the data in the syslog. The **stop** option deactivates the daemon and clears the data. **Restart** stops the daemon to clear the data and restarts the daemon to resume hardware status data collection. The **status** option retrieves the data from the log.

Usage: **fstool hwstat start|stop|restart|status**

Examples

This command was executed after **fstool hwstat start (or restart):**

fstool hwstat status

```
 - hwstat service is up
 - ACPI is enabled:
       * CPU temperature notification - NOT Supported.
       * Power off notification       - Supported.
 - RAID driver install on host - mptscsih:
       * RAID error notification     - Supported.
 - Local disk space usage - reports when usage is above
98%.
 - Interfaces Status:
       eth5:link-ok,100Mb/s Speed,Half Duplex
       eth6:no-link
       eth7:no-link
       eth0:link-ok,100Mb/s Speed,Full Duplex
       eth1:link-ok,100Mb/s Speed,Full Duplex
       eth2:link-ok,100Mb/s Speed,Full Duplex
       eth3:link-ok,100Mb/s Speed,Full Duplex
       eth4:no-link
```

After activating **hwstat**, as indicated above, notifications are recorded in the syslog on the status of ACPI power, RAID, and Ethernet ports status.

To initiate the daemon and collect hardware status data, run:

– **fstool hwstat start**

```
Starting hwstat...
```

To stop the daemon (data remains "as is"), run:

– **fstool hwstat stop**

```
Stopping hwstat...
```

To stop, clear data, and restart the hwstat daemon, run:

– **fstool hwstat restart**

pe – Set Configuration Parameters for Packet Engine

Use this command to configure the behavior of the Packet Engine Plugin on the Appliance.

Usage: **pe**

- **pe get_conf_params** <infix> -- Print conf_params whose names include <infix>
- **pe get_conf_param** <full_name> -- Print (the single) conf_param whose name is <full _name>
- **pe set_conf_param** <full_name> <value> -- Set (the single) conf_param whose name is <full_name> to <value>. Use double-quoted value if it includes shell-characters e.g. '*'

plugin – Plugin Control Tool

Usage: **fstool plugin plugin_name args...**

sc_config - Windows SecureConnector Advanced Log Configuration

Commands for Windows SecureConnector advanced log configuration and other advanced options.

Usage: **sc_config -c <command> [parameters]**

-c	Provide one of the following commands: ▪ **sc_msg –h** <all|none|ip[,ip[,ip..]]> - Enable logging the Protocol messages between SC and HPS. ▪ **close_sc -h** <ip> - Close the connection with the SC running on endpoints with [ip]. ▪ **get_logs -h** <ip> - Copies the zipped log files from the host to the shared path on CA. ▪ **get_dump -h** <ip> - Copies the zipped dump file from the host to the shared path on CA. ▪ **set_config -h** <ip> **-l** <int,0-5> **-m** <int> **-t** <int> - Configure SecureConnector logging mechanism.
-l	Changes the SecureConnector log level
-m	Changes the maximum number of log files that the SecureConnector is allowed to create. A log file's maximum size is ~40MB. If a new log will need to be created after we reached this number, the oldest log will be deleted.

-t	Determines the recording time, after which the log settings will be returned to their original values. By default, the changes are permanent.

Examples:

```
fstool sc_config -c sc_msg -h all
fstool sc_config -c sc_msg -h none
fstool sc_config -c sc_msg -h 10.0.0.1
fstool sc_config -c sc_msg -h 10.0.0.1,10.0.0.2
fstool sc_config -c close_sc -h 10.0.0.1
fstool sc_config -c get_logs -h 10.0.0.1
fstool sc_config -c get_dump -h 10.0.0.1
fstool sc_config -c set_config -h 10.0.0.1 -l 5 -m 4 -t 60
```

setmapiport – Set MAPI Service Port

This command is not available in FS-CLI.

Supported platforms: UNIX.

Usage: **fstool setmapiport [-h|help]**

To set a new list, insert ip:port list. Format the list as follows:

a.b.c.d:port/TCP, e.f.g.h:port/TCP

To clear the current list:

fstool setmapiport clear

smtpp - Enable and Disable SMTP Privacy

By default, e-mail anomalies displayed in the Console and shown in Console reports will hide certain information contained in the mail in order to protect the privacy of the sender. You can disable this mechanism. When disabled the sender and receiver name, and the subject of the mail are not displayed.

To disable the privacy mechanism:

1. Log in to the CounterACT device CLI.
2. Run: **fstool smtpp**

   The following message appears:

   ```
   SMTP Privacy is currently enabled.
   Disable SMTP Privacy? (yes/no) :
   ```

3. Enter **yes**. The following message appears:

   ```
   Disabling SMTP privacy...
   Restarting CounterACT Engine...
   ```

To enable the privacy mechanism:

1. Log in to the CounterACT device CLI.
2. Run: **fstool smtpp**

   The following message appears:

   ```
   SMTP Privacy is currently disabled.
   Enable SMTP Privacy? (yes/no)
   ```

3. Enter **yes**. The following message appears:

   ```
   Enabling SMTP privacy...
   Restarting CounterACT Engine...
   ```

   /tmp/CounterACT-install.log

   And reboot.

Control Center

Select **Tools -> Appliance maintenance -> Backup system settings..**

You are then prompted to provide a file name and a location where to create the backup file:

Command Line

To back up a Forescout system to an FSB file:

- **fstool backup <full path file name>**

To restore a Forescout system from an FSB file to another Forescout system:

- **fstool restore <full path file name>**

sw netconf – Debug Configured Switches Using NETCONF

1. Run: **fstool sw netconf**

   The following sample output is displayed:

```
CounterACT Utility Tool
~~~~~~~~~~~~~~~~~~~~~~
Get NETCONF XMLs from Configured Switches
Please wait, reading switch list from database...
Open database - Success
The following switches are configured to work on the
appliance:
1. 10.39.1.250 using SNMP version [2] vendor [alcatel]
2. 10.39.1.248 using NETCONF vendor [juniper]
3. 10.34.1.250 using SNMP version [2] vendor [extreme]
Select a switch for NETCONF XML query by entering its
number in the list. For multiple switch selection,
separate numbers by commas.
Select switch: 2
```

2. After you select the switch number, the following prompt opens:

```
Open session to switch [10.39.1.248] vendor[juniper]

Take NETCONF XMLs on (a) all XMLs (s)elected XMLs or
XMLs (f)ile:

trying . >>/tmp/10.39.1.248.juniper.walk
```

3. Select (**a**) for all XMLs or (**s**) or (**f**) if you have been instructed to do so by Forescout support.
4. Complete the form that opens up when you run **fstool sw netconf** and submit it to our support team for debugging assistance.

sw snmpwalk – Debug Configured Switches Using SNMP

1. Run: **fstool sw snmpwalk**

The following sample output is displayed:

```
CounterACT Utility Tool
~~~~~~~~~~~~~~~~~~~~~~
Get SNMPWALK from Configured Switches
Please wait, reading switch list from database...
Open database - Success
The following switches are configured to work on the
appliance:
1. 10.33.1.253 using SNMP version [2] vendor [cisco]
2. 10.34.1.250 using SNMP version [2] vendor [extreme]
3. 10.33.1.250 using SNMP version [2] vendor [cisco]
Select a switch for SNMPWALK by entering its number in
the list. For multiple switch selection, separate
numbers by commas.
Select switch: 2
```

2. After you select the switch number, the following prompt opens:

```
Selected switch [10.34.1.250] model [extreme]
Take SNMPWALK on (s)elected OIDs, (a)ll OIDs, or OID
(f)ile:
trying . >>/tmp/10.34.1.250.extreme.walk
```

3. Select (**a**) for all OIDs or (**s**) or (**f**) if you have been instructed to do so by Forescout support.
4. Complete the form that opens up when you run **`fstool sw snmpwalk`** and submit it to our support team for debugging assistance.

sw traps – Configure Cisco Switches for MAC traps

The command configures Cisco switches for MAC notification traps:

```
Cisco SNMP Switch Configuration for MAC Notification
Traps

Usage: fstool sw traps -h hostname -c community -s
state -v version
   -h <ip>               - host ip
   -c <community>        - community
   -s <state>            - 1 = Enable Notification
                           2 = Disable Notification
   -v <version>          - Snmp Version
```

tty - Manage Built-in tty

This command is not available in FS-CLI.

Usage: **`fstool tty command`**

Command can be one of:

`status [<tty dev>]`	Show status
`set [<tty dev> <baud rate>]`	Configure the tty

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 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 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.