



ForeScout CounterACT[®]

Core Extensions Module: Technical Support Plugin

Configuration Guide

Version 1.2

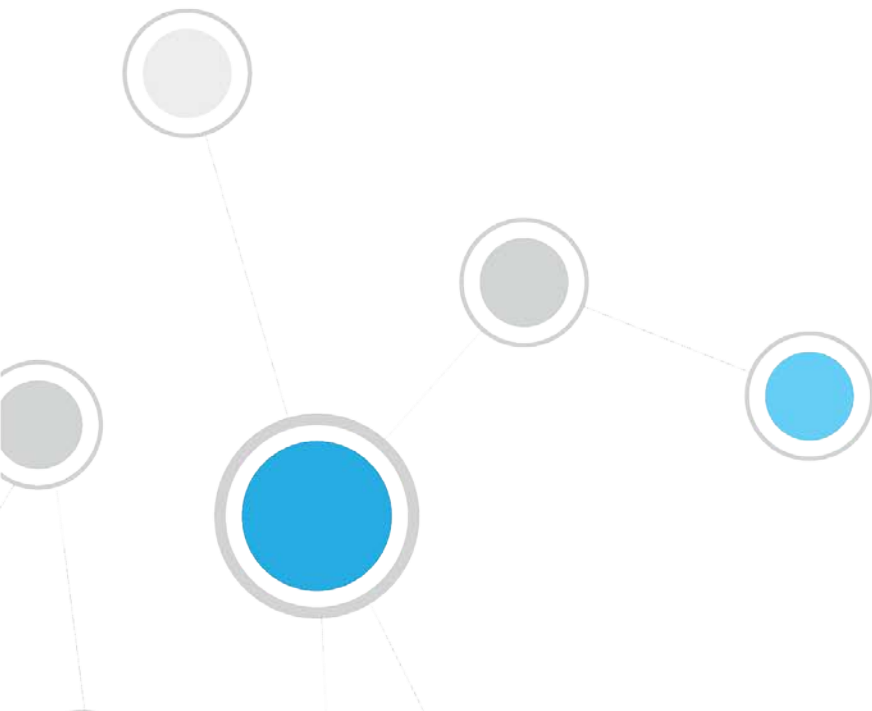


Table of Contents

About the Technical Support Plugin	3
Tool Options	3
What to Do.....	3
Requirements	3
Run the Technical Support Command	4
Send Logs to ForeScout Support	4
Save Logs to a CounterACT Device	5
Map Appliance IP Address to Revision Model	6
Core Extension Module Information	7
Additional CounterACT Documentation	8
Documentation Downloads	8
Documentation Portal	9
CounterACT Help Tools.....	9

About the Technical Support Plugin

The Technical Support Plugin is a component of the ForeScout CounterACT® Core Extensions Module. See [Core Extension Module Information](#) for details about the module.

The Technical Support Plugin provides an infrastructure used to automatically analyze an extensive range of log files on your system and send them to the ForeScout support team for further investigation.

Analysis of log files is carried out on a wide range of issues, for example service restarts, database issues, plugin errors, issues dealing with policies, internal processes, reports or any other issue occurring on your CounterACT system.

The plugin provides a CLI command that analyzes and sends system log files for each of your CounterACT devices. You should run the tool on the device you want to troubleshoot.

By default, information is sent from the last 24 hours.

Installation of the plugin does not initiate the tool. Information is collected, analyzed and sent only when the CLI command is running.

For customers who do not have internet access, an option is available to save the files on an Appliance.

Tool Options

The support team may provide you with additional command-line options to retrieve specific information, for example:

- A time frame for which to send log files. For example the last seven days or a specific date.
- Information about a single plugin or several plugins.
- A specific file.
- Core files and database tables.

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See [Requirements](#).
- Run the tech support command when requested by ForeScout support. See [Run the Technical Support Command](#).

Requirements

The plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0

- An active Maintenance Contract for CounterACT devices is required.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools>Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Run the Technical Support Command

If you have experienced a problem, contact ForeScout Support at support@forescout.com.

If the team member recommends that you run the technical support command, run the command on the CounterACT device you want to troubleshoot.

For customers who do not have internet access, an option is available to save the files on an Appliance.

Send Logs to ForeScout Support

To send files to ForeScout support:

1. Log onto the Appliance/Enterprise Manager CLI.
2. Run the following command: *fstool tech-support*

The following prompts appear.

```
-----  
About to collect snapshot relevant to time period:  
-----
```

```
Since: Sun Feb 9 17:47:20 2014  
Until: Mon Feb 10 17:47:20 2014  
-----
```

Options:

- 1) Send the snapshot directly to ForeScout support
- 2) Pack the snapshot (upload later via <https://upload.forescout.com>)

Choice (1-2) [1] :

3. Type **1** at the **Choice** prompt. You are prompted to enter your company name and a comment.

```
Enter company name [ExampleCompany] :
```

```
Enter one-line comment : My comment
```

4. Enter the company and a comment and press **Enter**. The snapshot is created and sent to ForeScout.

```

-----
Creating the snapshot
-----
Checking CounterACT service : Done
Checking plugins : Done
Checking core files : Done
Collecting CounterACT service logs : Done
Collecting Packet Engine logs : Done
Collecting Portal logs : Done
Collecting events : Done
Collecting stats : Done
Collecting system information : Done
Collecting configuration files : Done
-----
Sending files to ForeScout support...
-----
Connecting to ForeScout Snapshot Server...
Transferring snapshot...
Progress: 12.17% done, ETA: 00:03:05 (217.60 Kbps)

```

Save Logs to a CounterACT Device

If you do not want to automatically send log files to ForeScout, you can save them on the Appliance at which you ran the command. The command prompt output indicates the location the files are saved and the size of the files.

The files can later be uploaded to upload later to <https://upload.forescout.com>.

To save files to on your CounterACT device:

1. Log in to the Appliance/Enterprise Manager CLI.
2. Run the following command: *fstool tech-support*

The following prompts appear.

```

-----
About to collect snapshot relevant to time period:
-----
Since: Sun Feb 9 17:47:20 2014
Until: Mon Feb 10 17:47:20 2014

```

 Options:

- 1) Send the snapshot directly to ForeScout support
- 2) Pack the snapshot (upload later via <https://upload.forescout.com>)

Choice (1-2) [1] :

3. Type **2** at the **Choice** prompt. You are prompted to enter your company name and a comment.
4. Enter the company and a comment and press **Enter**. The snapshot is created.

 Creating the snapshot

Checking CounterACT service : Done

Checking plugins : Done

Checking core files : Done

Collecting CounterACT service logs : Done

Collecting Packet Engine logs : Done

Collecting Portal logs: Done

Collecting events : Done

Collecting stats : Done

Collecting system information : Done

Collecting configuration files : Done

 Packing the snapshot

Storing the snapshot to /tmp/ExampleCompany-appliance.2014_02_10-17.50.23.tgz

...

 Snapshot is ready for upload to <https://upload.forescout.com>

File: /tmp/ExampleCompany-appliance.2014_02_10-17.50.23.tgz

Size: 59.4 Megabytes

Map Appliance IP Address to Revision Model

You can determine the revision models of Appliances in your deployment by running a command prompt on the Enterprise Manager. *N/A* is printed for virtual appliances, or if no model is defined.

To determine Appliance revision models:

1. Log in to the Enterprise Manager CLI.

2. Run the following command: `fstool tech-support oneachmodel`

The following information appears:

```
-----  
| IP          | Appliance Model |  
|-----|-----|  
| 192.168.10.15 | CT1000-30      |  
| 192.168.10.16 | CT1000-30      |  
| 192.168.10.17 | CT2000-30      |  
| 192.168.10.18 | CT4000-30      |  
| 192.168.10.19 | N/A           |  
| 192.168.10.20 | N/A           |  
| 192.168.10.21 | N/A           |
```

Core Extension Module Information

The Technical Support plugin is installed with the CounterACT Core Extension Module.

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin
- NetFlow Plugin
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin

- Web GUI Plugin

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See [Additional CounterACT Documentation](#) for information about how to access the module guide.

Additional CounterACT Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

Documentation Downloads

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

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Portal


The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

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

Documentation Portal

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

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

To access the Documentation Portal:

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

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

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

Plugin Help Files

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

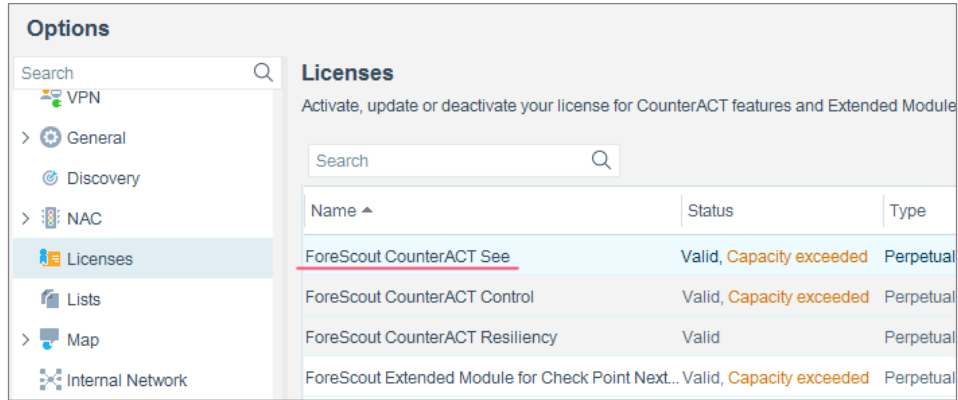
Documentation Portal

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

Identifying Your Licensing Mode in the Console

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

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



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

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-10 09:21