November 2018

Version Information

- CounterACT 7.0.0 Service Pack 3.0.2.5

- The service pack installation includes the following components:

  - Device Classification Engine version 1.1.1
  - Device Profile Library version 2.0.5
  - User Directory Plugin version 6.1.2
  - Reports Plugin version 4.2.0.1001
  - Technical Support Plugin version 1.1.1
  - CounterACT Infrastructure Update Pack version 2.0.8
  - DNS Query Extension Plugin version 1.1.2

  📄 *If you already have a later version of one of these plugins installed, installing this service pack does not override that version.*

- Customers with an active Maintenance Contract for their CounterACT devices can install this service pack.

- *Upgrading from a service pack version lower than 2.3.0 to version 2.3.0 or above results in a purge of the Host Log.*

CounterACT Device Requirements

This section describes CounterACT Appliance and Enterprise Manager requirements.

Physical CounterACT Devices

Service Pack 3.0.2 can be installed on all hardware revisions of CounterACT physical Appliances and Enterprise Managers *except for the following*:

Model	Revisions
CTR	CTR-11, CTR-12, CTR-13
CT100	CT100-20, CT100F-20 CT100-21, CT100F-21
CT1000	CT1000-20, CT1000F-20, CT1000F2-20 CT1000-21, CT1000F-21, CT1000F2-21
CEM-05/CEM-10	CT1000MS-20, CT1000MS-21

To determine the revision of a specific Enterprise Manager, do one of the following:

- Run the **fstool model** command on the Enterprise Manager.

- See the product label on the machine.

To determine the revision of a specific Appliance, do one of the following:

- Run the **fstool model** command on the Appliance.

- Run the **fstool tech-support oneachmodel** command on the Enterprise Manager. (This requires the Technical Support Plugin 1.1.2, available on the CounterACT Base Plugins page.)

- See the product label on the machine.

Contact your ForeScout sales representative for alternative solutions if any of your Appliances are on this list.

Virtual CounterACT Devices

Provision the CounterACT Enterprise Manager and each CounterACT Appliance with at least 3GB of RAM.

What's New

This version contains fixed issues. See Fixed Issues.

Installing this service pack also installs fixes from previous CounterACT 7.0.0 service packs. See Previous Releases for links to previous CounterACT 7.0.0 service packs.

Fixed Issues

This section describes fixed issues in this release. The following issues have been fixed since the release of Service Pack version 3.0.2.3:

Issue	Description
CA-19949	The checksum calculation for connected devices during Enterprise Manager startup has been made more efficient.
CA-20052	The CounterACT Console software was updated with Java 8 support, and now includes JRE 1.8 in the installation package (for clean installation). Upgrading an existing Console installation is not affected.

Issue	Description
CA-20103	The SSL web certificate chain was not being sent out by the CounterACT web server.
CA-20132	Communication between the Enterprise Manager and Appliances has been made more efficient when reporting devices that have been removed from the system.

The following issues were fixed in Service Pack version 3.0.2.3:

Issue	Description
CA-19059	The performance of the Device Classification Engine was enhanced.
CA-18894	CounterACT policy action thresholds have been enhanced to support percentage values at single decimal point granularity

The following issues were fixed since the release of Service Pack version 3.0.1.1001:

Issue	Description
CA-13537	Hardened partition mounting through implementation of the partition mount **nodev** option.
CA-13539	Made user **fshttp** home directory permissions more restrictive.
CA-13700	The CounterACT Service now uses, by default, TLS version 1.2 with the option to fallback to use a lower TLS version, as necessary.
CA-14452	The Apache web server software was updated to address security issues described in CVE-2017-5664.
CA-16095	The CounterACT Console's **Check for Updates** component update facility now communicates using only the HTTPS protocol.
CA-13778	Duplicating a newly discovered switch entry failed if the switch entry had not yet been approved.
CA-14878	In some cases, using the CLI command *hostinfo_all* on an Appliance caused the Appliance to restart
CA-15187	When multiple Appliances try to connect the Recovery Enterprise Manager at the same time after failover from the Enterprise Manager, some Appliances failed to connect to the Recovery Enterprise Manager.
CA-15188	CounterACT appliances were disconnected sporadically from the Enterprise Manager.
CA-15352	The disk cleaning process did not clean up large log files properly, and as a result, CounterACT occasionally restarted.
CA-17114	When a managed Appliance changes a host IP address, but reports a Learn event with a MAC address instead of IP address, an Appliance that receives the Learn event creates an IP Change event, and enters a loop of continually updating the IP Change event with an incorrect IP address.

Issue	Description
CA-17397	When requesting a recheck of compliance status in the ForeScout Compliance Center, the recheck was completed but the on screen progress bar sometimes got stuck.
CA-17792	When an endpoint was added to a group manually, based on the MAC address, the endpoint listing was not saved when the group listings were updated.
CA-18202	A new client-side certificate, *Counteract_cu_client*, has been added to improve the connection authentication for console connections to the Enterprise Manager.
CA-18580	Applying a *Delete Property* action in a policy resulted in endpoints that were offline being reported as online.
CA-18688	A code flow deadlock in the software caused the CounterACT service to stall.

Known Issues

This section describes known issues for this release.

Issue	Description

CA-10022	Web portals are not available on a highly loaded CounterACT device.
	 Workaround:
	 Increase the Tomcat webserver watchdog timeout from the default 60 seconds to 180, by running the following commands:
	 `fstool set_property tomcat5.wd.timeout 180`
	 `fstool www restart`

CA-13192	After switching over from Enterprise Manager to Recovery Enterprise Manager some appliances remain disconnected. Workaround: Run the following command on the Enterprise Manager: `fstool manager_fix`
CA-14299	Unable to see amount of traffic when monitoring high bandwidth traffic (approximately 2Gbps or more). Workaround: Use external tools such as `ethtool` to measure traffic bandwidth

Issue	Description
KB-5140	When using L2 response interfaces with DHCP, CounterACT may inspect/evaluate its own response interface MAC address as an endpoint. This may lead CounterACT to block that interface if it is not compliant, or if that policy contains restrictions
	Workaround:
	Manually set a static IP address for each response VLAN.
	Assign the static IP addresses to CounterACT's **Ignored IPs** group to prevent CounterACT from evaluating these IP addresses.

Upgrade Considerations and Issues

Read the following before you upgrade to the current version.

Upgrade Path to Service Pack version 3.0.2.5010 with CIUP 2.0.10 and OSUP 1.2.4

The following articles describe the upgrade path and requirements for upgrading to Service Pack version 3.0.2.5010 with CounterACT Infrastructure Update Pack (CIUP) version 2.0.10 and CounterACT Operating System Update Pack (OSUP) version 1.2.4

https://forescout.force.com/support/articles/Knowledge/Upgrading-to-CounterACT-Service-Pack-3-0-2-5010-with-CIUP-2-0-10-and-OSUP-1-2-4/p

https://forescout.force.com/support/articles/Knowledge/Supported-Upgrade-Paths-to-CounterACT-Service-Pack-3-0-2-5010-with-CIUP-2-0-10-and-OSUP-1-2-4/p

Host Log Purge

Upgrading from a service pack version that is lower than 2.3.0 to a service pack version 2.3.0 or above results in a purge of the Host Log.

How to Install

This section describes how to install the service pack. See CounterACT Device Requirements for details about physical and virtual CounterACT device limitations.

Perform the following steps to install the service pack:

1. Navigate to the Customer Support Portal, Product Download page and download the plugin `.fpi` file.

2. Save the service pack.

3. Log in to the Console and select the Options icon from the Console toolbar.

4. Navigate to the Plugins folder, and then select **Install**.

5. Install the service pack from the location that you saved it.

After installation you are asked to opt in to the ForeScout Research and Intelligent Analytics Program which uploads sanitized and anonymized endpoint properties. For more information about this program, refer to the *CounterACT Console User Manual.*

Clean Install of the CounterACT Console

A clean install of the CounterACT Console can be performed in one of the following ways.

Download and install the Console installation file for Service Pack 3.0.2.5:

https://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/3.0.2.5010/Install_Management.exe

More Release Information

This section provides the following release information:

- Rollback Support
- Available Releases
- Previous Releases

Rollback Support

Under certain circumstances you may want to roll back this service pack to a previously installed version. This may happen, for example, if your system does not operate as expected after the service pack upgrade.

You can roll back to Service Pack version 3.0.0 and above.

This release cannot be rolled back to Service Pack version 3.0.1.1001.

Rolling back from this version to Service Pack version 2.3.0 and above requires reinstalling the CounterACT Console after performing the rollback.

Rolling back to a previously installed service pack version will *not* roll back the following:

- Console JVM version updates
- External RPMs (e.g. openssl, kernel module RPMs, Java, etc.)
- High Availability miniroot related changes
- Plugins that the service pack itself installed (e.g. Technical Support Plugin)

Rollback on Appliances/Enterprise Manager

Service packs on Appliances connected to the Enterprise Manager are rolled back to the selected version. Service packs on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

Rollback and Plugin Requirements

If your CounterACT environment contains plugins that require a specific service pack version, you will not be able to roll back to a service pack that does not support those plugins. You will need to either uninstall the plugin/s or roll back the plugin/s to an earlier version that is compatible with the service pack you are rolling back to. Uninstall or rollback the plugin/s before rolling back the service pack.

To roll back:

1. Select **Options** from the Console **Tools** menu.
2. Navigate to and select the **Plugins** folder.
3. In the Plugins pane, select the service pack you want to roll back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and then select **OK**. A dialog box opens showing you the rollback progress.
6. After rollback is complete, reinstall the CounterACT Console. Refer to the *CounterACT Installation Guide* for more information.

Available Releases

You can review information about currently available service pack releases at:

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/Updates.pdf

Previous Releases

To view release notes for previous version releases, see:

https://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/3.0.1.1001/3.0.1.1001-30011001/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/3.0.1/3.0.1-30010063/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/3.0.0/3.0.0-30000319/RN.pdf

https://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.4/2.3.4-23040035/RN.pdf

https://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.3/2.3.3-23030080/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.2/2.3.2-23020071/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.1/2.3.1-23010817/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.0.2/2.3.0.2-23010202/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.0.1/2.3.0.1-23010004/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.3.0/2.3.0-23000062/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.2.0.3/2.2.0.3-22030005/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.2.0.2/2.2.0.2-22020007/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.0.3/2.0.3-203032/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.0.2/2.0.2-202024/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.0.1/2.0.1-201018/RN.pdf

http://updates.forescout.com/support/files/plugins/service_pack_for_ca_700/2.0.0/2.0.0-200138/RN.pdf

http://updates.forescout.com/support/files/plugins/hotfix_for_ca_700/1.7.1/1.7.1-171022/RN.pdf

Legal Notice

2018-11-04 15:57