

Patch Release Notes **ArcSight™ ESM**

Version 4.5 SP1, Patch 2
4.5.1.6043.2

September 30, 2009



Patch Release Notes ArcSight™ ESM , Version 4.5 SP1, Patch 2

Copyright © 2009 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
September 30, 2009	ArcSight™ ESM Version 4.5 SP1, Patch 2	Patch Release Notes for ArcSight™ ESM Version 4.5 SP1, Patch 2.

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://protect724.arcsight.com

Contents

ArcSight ESM, Version 4.5 SP1, Patch 2	1
ESM Patch 4.5.1.6043.2	1
Purpose of this Patch	1
Geographical Information Update	1
Vulnerability Updates	1
Oracle Critical Patch Update (CPU) Certification	2
OPatch	2
To Apply the CPU	2
Workarounds for Known Issues in Oracle CPU	3
Installing ESM Version 4.5 SP1 Patch 2	4
Platform-Specific Information for Installing Patch 2	5
Installing ArcSight Console Patch on Mac	16
Logger Integration Commands	17
Enabling Integrated Searches	18
Issues Fixed in this Patch	19
Install and Uninstall	19
Database	19
ArcSight Manager	19
ArcSight Console	21
Known Issues in this Patch	23
Open and Closed Issues in ESM v4.5 SP1	23

ArcSight ESM, Version 4.5 SP1, Patch 2

ESM Patch 4.5.1.6043.2

These release notes describe how to apply the 4.5 SP1, Patch 2 release of ArcSight ESM. Instructions are included for each component, as well as other information about recent changes and open and closed issues.

This patch is for ArcSight ESM v4.5 SP1 only. If you are seeking to set up a fully current ESM v4.5 SP1, Patch 2 installation, install v4.5 SP1 first and refer to those release notes for important additional information.

Purpose of this Patch

This patch addresses:

- Fixes for critical issues
- Oracle CPU certification with the currently available CPU for July 2009
- Updates for geographical information and vulnerability mapping

Geographical Information Update

This patch includes an update to the geographical information used in graphical displays. The update version is GeoIP-532_20090801.

Vulnerability Updates

This patch contains updated vulnerability mapping for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 253	Bugtraq, CVE, X-Force, MSSB
Enterasys Dragon IDS	Bugtraq, CVE, Nessus, CAN, MSSB
Cisco Secure IDS S424	Bugtraq, CVE
McAfee Intrushield	CVE, MSSB
TippingPoint UnityOne DV7755	Bugtraq, CVE, X-Force, CERT, MSKB, MSSB
Fortinet Fortigate	Bugtraq, CVE, X-Force, MSSB
ISS SiteProtector	Bugtraq, CVE, X-Force, MSKB, MSSB, CERT

Device	Vulnerability Updates
Symantec Endpoint Protection	Bugtraq, CVE
Radware DefensePro	CVE
FunkWerk (VarySys Technologies) PacketAlarm	Bugtraq, CVE, X-Force, Nessus, MSSB, MSKB, CERT

Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM has been certified with the Oracle critical patch update (CPU) for July, 2009. Certification has been established with Oracle 10.2.0.4. Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

Platform	CPU July 2009 Patch
Windows 32	p8559466_10204_Win32.zip
Windows 64 (AMD64-EM64T)	p8559467_10204_MSWIN-x86-64.zip
Linux 32	p8534387_10204_Linux-x86.zip
Linux x86-64	p8534387_10204_Linux-x86-64.zip
AIX	p8534387_10204_AIX5L.zip
Solaris 64	p8534387_10204_Solaris-64.zip

OPatch

Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

Platform	OPatch July 2009
Linux 32	p6880880_102000_LINUX.zip
Linux x86-64	p6880880_102000_Linux-x86-64.zip
Solaris 64	p6880880_102000_SOLARIS64.zip
Windows 64 (AMD64-EM64T)	p6880880_102000_MSWIN-x86-64.zip
Windows 32	p6880880_102000_WINNT.zip
AIX	p6880880_102000_AIX64-5L.zip

To Apply the CPU

- From the Product Download section of the ArcSight Customer Support site (<https://support.arcsight.com/>), download both the Oracle CPU and OPatch:
 - Download the correct Oracle CPU package for your platform (see the tables above) and unzip it under your working directory.
 - Download the Oracle 10g OPatch file for your platform.

- 2 Install the OPatch:
 - ◆ Review the [README](#) file in the OPatch zip archive.
 - ◆ Extract the contents of the OPatch zip file under `$ORACLE_HOME`.
- 3 Stop the ArcSight Manager and Partition Archiver, and also stop the Oracle instance and TNS listener.
- 4 Set the OPatch binary in PATH.
- 5 Read the next section in this document, “Workarounds for Known Issues in Oracle CPU” on page 3.
- 6 Install the CPU (that you downloaded in [Step 1](#)) according to the steps outlined in the [README](#) in the CPU zip package for your platform.
- 7 Replace references to “OPatch” in the commands with `$ARCSIGHT_HOME/bin/arcdbutil patch`

where `$ARCSIGHT_HOME` refers to the location where you have installed the ArcSight Database.

For example,

On Windows:

If the [README](#) says:

```
>OPatch apply
```

Then use this command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch apply
```

On UNIX:

If the [README](#) says:

```
>opatch napply -skip_subset -skip_duplicate
```

Then use this command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch napply -skip_subset  
-skip_duplicate
```



More information about Oracle-specific steps is provided in the [README](#) that accompanies the Oracle CPU. Be sure to review the [README](#) carefully and follow those instructions.

- 8 To complete the installation, follow the “Post Installation Instructions...” steps in the [README](#).
- 9 Restart the database and the TNS Listener.
- 10 Restart the Partition Archiver and the ArcSight Manager.

Workarounds for Known Issues in Oracle CPU

The following subsections provide workarounds for issues related to the Oracle CPU on different platforms.

Windows for Oracle 10g

In some cases, the CPU application can fail with this error:

```
OUI-67124:Copy failed from "<source>" to "<destination>"
```

```
OPatch failed with error code 115
```

This error occurs when there are other processes running that lock the file in question. The processes that cause the lock might be related to Oracle. As a workaround, reboot the machine and try the patch application steps again.

Linux - Using a Large Instance

If your ArcSight Database is running on a 32-bit Linux machine with the SMP kernel and your system is configured to use between 2 GB and 4 GB of memory (the default configuration of the Large template), perform the following steps after applying an Oracle Patch or an Oracle Patch Set (for example, a Critical Patch Update or the patch set for 10.2.0.4) to your ArcSight Database.

- 1 Log into the database machine as the Oracle software owner (by default, Oracle).
- 2 Shut down the Oracle database, the TNS listener, and all other Oracle services (if any).
- 3 Run these commands:

```
cd $ORACLE_HOME/rdbms/lib

mv ksms.s ksms.s.org; mv ksms.o ksms.o.org

$ORACLE_HOME/bin/genksms -s 0x15000000 > ksms.s

make -f ins_rdbms.mk ksms.o

make -f ins_rdbms.mk ioracle
```

- 4 Restart the database server and the TNS listener.

Restarting the database server enables the ArcSight database to utilize the extended memory. Oracle cannot restart if this procedure is not followed. If the above commands display errors, call ArcSight Customer Support. If you are using your own Oracle software license, contact Oracle.

Known Issues for AIX

The following error displays when you execute the `opatch` command on AIX: `"UTE011: Active tracepoint array length for HPI is 1036; should be 1030."`

To resolve this issue, add `jre <JRE location>` to the `opatch` command line; for example:

```
./opatch lsinventory -jre < $ORACLE_HOME/jre/*
```

Installing ESM Version 4.5 SP1 Patch 2

You can install this patch release using the platform-specific and component-specific executable files provided. Patch installers are available for all platforms.

Note the following points when installing Patch 2.



- In some Solaris environments, when upgrading the ESM Manager and also when installing the solution packages, these actions do not complete. This problem could occur if your Solaris system does not meet the minimum system requirements. See the *ESM 4.5 Installation and Configuration Guide* for the minimum system requirements for a Solaris system.
- Be sure to execute `arcsight agentsetup -w` on the database component after installing and uninstalling the patch. Refer to the installation and uninstallation steps for the “ArcSight ESM Database” on page 5.
- **For all components and platforms:** Verify that you have enough space (approximately three times the size of the patch installer) available *before* you begin to install the patch. If you run into disk space issues during installation, first create enough disk space, then restore the component base build from the backup, and then resume installation of the patch.
- Backup, patch install, and uninstall procedures require permissions for the relevant components. For example, you need database logon permissions to back up a database installation and install an Oracle critical patch update. To back up the ArcSight Manager installation and install the Manager patch, Manager permissions are required. Before installing a patch, verify that the user who owns the base build installation folder has full privileges on the PATH where the base build is installed.
- Due to issues related to configuration variability (AIX Tech Levels), a small number of users might experience issues with installation and uninstallation. It is good practice to create a backup of the existing product before installation begins.
- Users who uninstall the software need to have the same permissions as the user who originally installed the software.
- For backup, patch install, and uninstall, ArcSight recommends that you log in to the target machine with a specific account name using telnet or SSH. If, instead, you switch accounts after logging in, then be sure to specify the flag `-` for the `su` command; for example: `su - <UserName>`

Platform-Specific Information for Installing Patch 2

Each component has installation and rollback steps.

The patch installation instructions describe installation on all supported platforms. Platform-specific details are provided within the procedures below.

ArcSight ESM Database

This section describes how to install and uninstall ESM v4.5 SP1, Patch 2 for ArcSight Database.

To Install



- Before you install the patch, verify that the ArcSight Database `ARCSIGHT_HOME` and any of its subdirectories are not being accessed by any open shells on your system.
- If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

1 Stop the Partition Archiver Agent.◆ **On Windows:**

Open the Services Console and stop the Partition Archiver Agent service (the default is [Arcsight Oracle Partition Archiver Database](#)).

◆ **On Solaris, AIX, and Linux:**

Run:

```
/etc/init.d/arc_oraclepartitionarchiver_db stop
```



[arc_oraclepartitionarchiver_db](#) is the default service name.

2 Back up the ArcSight Database directory (for example, [c:\arcsight\db](#)) by making a copy. Be sure to back up the database as the Oracle database owner on Solaris, AIX, and Linux. Place the copy in a readily accessible location. Perform this step as a precautionary measure so that you can restore the original state, if necessary.

Arcsight recommends that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3 Download the executable file specific to your platform from the ArcSight Software Download Site. (In the following file names, [xxxx](#) stands for the build number.)

- ◆ [Patch-4.5.1.xxxx.2-DB-Win.exe](#)
- ◆ [Patch-4.5.1.xxxx.2-DB-Solaris.bin](#)
- ◆ [Patch-4.5.1.xxxx.2-DB-AIX.bin](#)
- ◆ [Patch-4.5.1.xxxx.2-DB-Linux.bin](#)

4 As the Oracle Database owner, run one of the following executables specific to your platform.◆ **On Windows:**

Double-click [Patch-4.5.1.xxxx.2-DB-Win.exe](#)

◆ **On Solaris:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-DB-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-DB-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-DB-AIX.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-DB-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-DB-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-DB-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing ArcSight Database [ARCSIGHT_HOME](#) for your v4.5 SP1 database installation in the text box provided, or navigate to the location by clicking **Choose...**
- 7 To restore the installer-provided default location, click **Restore Default Folder**.
- 8 Click **Next**.
- 9 Choose a Link Location (on Solaris, AIX, and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button, and then click **Next**.
- 10 Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
- 11 Click **Install**.
- 12 Click **Done** on the Install Complete screen.

After installation of the database patch is complete **and** after you have installed the ArcSight Manager patch, update the Partition Archiver. These steps are required to upgrade the Partition Archiver version when viewed from the Console. Verify that the Manager is running, and then:

- 1 Run the following command from the Database [bin](#) directory to update the Partition Archiver.

```
arcsight agentsetup -w
```
- 2 Click **Next** through the wizard screens until you reach the screen that prompts you to either review or modify the parameters.
- 3 Select **I do not want to change any settings**, and then click **Next**.
- 4 Click **Finish** in the last screen.
- 5 **On Windows Only:** Click **Cancel** in the Archiver Service Configuration screen.

Start the Partition Archiver Agent.

■ **On Windows:**

Open the Service Console and start the Partition Archiver Agent service (the default is [Arcsight Oracle Partition Archiver Database](#)).

■ **On Solaris, AIX, and Linux:**

Run the following command.

```
/etc/init.d/arc_oraclepartitionarchiver_db start
```



`arc_oraclepartitionarchiver_db` is the default service name.

To Uninstall

If needed, use the procedure below to roll back this patch installation.



Before you begin to uninstall, verify that the Database `ARCSIGHT_HOME` and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Stop the ArcSight Partition Archiver.
- 2 Run the uninstaller program:

On Windows:

- ◆ Double-click the icon you created for the uninstaller when installing the database. For example, if you created an uninstaller icon on your desktop, double-click that icon.
- ◆ Or, if you created a link in the Start menu, click

Start->ArcSight DB SP1 Patch2-> Uninstall ArcSight Database 4.5 SP1 Patch 2

- ◆ Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP1Patch2` directory.

```
Uninstall_ArcSight_DB_Patch.exe
```

On Solaris, AIX, and Linux:

- ◆ From the directory where you created the links (your home folder or another location) when installing the database, run:

```
./Uninstall_ArcSight_Database_4.5_SP1Patch2
```

- ◆ Or, to uninstall in console mode, run

```
./Uninstall_ArcSight_Database_4.5_SP1Patch2 -i console
```

- ◆ If you did not create a link, execute the following command from the Database's `ARCSIGHT_HOME/UninstallerDataSP1Patch2`.

```
./Uninstall_ArcSight_DB_Patch
```

- 3 Click **Done** on the Uninstall Complete screen.

After uninstallation of the database patch is complete, update the Partition Archiver:

- 1 Uninstall the patch on the Manager.
- 2 Start the Manager.
- 3 Run the following command from the Database `bin` directory to update the Partition Archiver.

```
arcsight agentsetup -w
```
- 4 Click **Next** through the wizard screens until you reach the screen that prompts you to either review or modify the parameters.

- 5 Select **I do not want to change any settings** and click **Next**.
- 6 Click **Finish** in the last screen.
- 7 **On Windows Only**, click **Cancel** in the Archiver Service Configuration screen.

Start the Partition Archiver Agent.

■ **On Windows:**

Open the Service Console and start the Partition Archiver Agent service (the default is [Arcsight Oracle Partition Archiver Database](#)).

■ **On Solaris, AIX, and Linux:**

Run the following command.

```
/etc/init.d/arc_oraclepartitionarchiver_db start
```



[arc_oraclepartitionarchiver_db](#) is the default service name.

ArcSight ESM Manager

This section describes how to install or uninstall the Version 4.5 SP1, Patch 2 for ArcSight Manager.

To Install



- Before you install the patch, verify that [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.
- If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

- 1 Stop the ArcSight Manager.
- 2 Back up the Manager directory (for example, [c:\arcsight\manager](#)) by making a copy. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.



Arcsight recommends that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

- 3 Download the executable file specific to your platform from the ArcSight Software Download Site. (In the following file names, [xxxx](#) stands for the build number.)
 - ◆ [Patch-4.5.1.xxxx.2-Manager-Win.exe](#)
 - ◆ [Patch-4.5.1.xxxx.2-Manager-Solaris.bin](#)
 - ◆ [Patch-4.5.1.xxxx.2-Manager-AIX.bin](#)
 - ◆ [Patch-4.5.1.xxxx.2-Manager-Linux.bin](#)
- 4 While logged in as the ArcSight user, run one of the following executables specific to your platform.
 - ◆ **On Windows:**
Double-click [Patch-4.5.1.xxxx.2-Manager-Win.exe](#)

◆ **On Solaris:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-Manager-Solaris.bin
```

To install in console mode, run the following from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Manager-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-Manager-AIX.bin
```

To install in console mode, run the following from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Manager-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./Patch-4.5.1.xxxx.2-Manager-Linux.bin
```

To install in console mode, run the following from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Manager-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing [ARCSIGHT_HOME](#) for your v4.5 SP1 Manager installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer-provided default location, click **Restore Default Folder**.
- 7 Click **Next**.
- 8 Choose a Link Location (on Solaris, AIX, and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button, then click **Next**.
- 9 Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
- 10 Click **Install**.
- 11 Click **Done** on the Install Complete screen.

To Uninstall

If needed, use the procedure below to roll back this patch installation.



Note

Before you begin to uninstall, verify that the Manager's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Stop the ArcSight Manager.
- 2 Run the uninstaller program:

On Windows:

- ◆ Double-click the icon you created for the uninstaller when installing the Manager. For example, if you created an uninstaller icon on your desktop, double-click that icon.

- ◆ Or, if you created a link in the Start menu, click

Start->ArcSight Manager SP1 Patch2-> Uninstall ArcSight Manager 4.5 SP1 Patch 2

- ◆ Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP1Patch2` directory.

`Uninstall_ArcSight_Manager_Patch.exe`

On Solaris, AIX, and Linux:

- ◆ From the directory where you created the links when installing the Manager (your home folder or some other location), run:

`./Uninstall_ArcSight_Manager_4.5_SP1Patch2`

- ◆ Or, to uninstall using console mode, run:

`./Uninstall_ArcSight_Manager_4.5_SP1Patch2 -i console`

- ◆ If you did not create a link, execute the following command from the `ARCSIGHT_HOME\UninstallerDataSP1Patch2` directory.

`./Uninstall_ArcSight_Manager_Patch`

- 3 Click **Done** on the Uninstall Complete screen.

ArcSight Console

This section describes how to install or uninstall the v4.5 SP1, Patch 2 for ArcSight Console on Windows, Solaris, and Linux platforms.



Tip

- Instructions describing how to install or uninstall the Console patch on Macintosh systems are provided in [“Installing ArcSight Console Patch on Mac” on page 16](#).
- The ArcSight ESM Console is not supported on AIX. The following steps do not include information for installing a Console patch on AIX.

To Install

Note

- Before you install the patch, verify that the Console's `ARCSIGHT_HOME` and any of its subdirectories are not being accessed by any open shells on your system.
- If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

- 1 Exit the ArcSight Console.

- 2 Back up the Console directory (for example, `/home/arcsight/console/current`) by making a copy. Place the copy in a readily accessible location. This is a precautionary measure so you can restore the original state, if necessary.



ArcSight recommends that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

- 3 Download the executable file specific to your platform from the ArcSight Software Download Site. (In the following file names, `xxxx` stands for the build number.)

- ◆ `Patch-4.5.1.xxxx.2-Console-Win.exe`
- ◆ `Patch-4.5.1.xxxx.2-Console-Solaris.bin`
- ◆ `Patch-4.5.1.xxxx.2-Console-Linux.bin`

- 4 Run one of the following executables specific to your platform.

- ◆ **On Windows:**

Double-click `Patch-4.5.1.xxxx.2-Console-Win.exe`

- ◆ **On Solaris:**

Verify that you are logged in as the ArcSight user, and then run this command:

```
./Patch-4.5.1.xxxx.2-Console-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Console-Solaris.bin -i console
```

- ◆ **On Linux:**

Verify that you are logged in as the ArcSight user, and then run the following command.

```
./Patch-4.5.1.xxxx.2-Console-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Console-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP1 Console installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer-provided default location, click **Restore Default Folder**.
- 7 Click **Next**.
- 8 Choose a Link Location (on Solaris and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button and click **Next**.
- 9 Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
- 10 Click **Install**.

- 11 Click **Done** on the Install Complete screen.

To Uninstall

If needed, use the procedure below to roll back this patch installation.



Before you begin to uninstall, verify that the Console's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Exit the ArcSight Console.
- 2 Run the uninstaller program:

On Windows:

- ◆ Double-click the icon you created for the uninstaller when installing the Console. For example, if you created an uninstaller icon on your desktop, double-click that icon.

- ◆ If you created a link in the Start menu, click

Start->ArcSight Console SP1 Patch2-> Uninstall ArcSight Console 4.5 SP1 Patch 2

- ◆ Or, run the following from the Console's [ARCSIGHT_HOME\current\UninstallerDataSP1Patch2](#) directory.
[Uninstall_ArcSight_Console_Patch.exe](#)

On Solaris and Linux:

- ◆ From the directory where you created the links when installing the Console (your home directory or some other location), run:

```
./Uninstall_ArcSight_Console_4.5_SP1Patch2
```

- ◆ Or, to uninstall using console mode, run:

```
./Uninstall_ArcSight_Console_4.5_SP1Patch2 -i console
```

- ◆ If you did not create a link, execute the command from the Console's [ARCSIGHT_HOME/current/UninstallerDataSP1Patch2](#) directory:

```
./Uninstall_ArcSight_Console_Patch
```

- 3 Click **Done** on the Uninstall Complete screen.

ArcSight Web Server

This section describes how to install or uninstall ESM v4.5 SP1, Patch 2 for ArcSight Web.

To Install



Note

- Before you install the patch, verify that the Web's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.
- If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

- 1 Stop the Web Server.
- 2 Backup the server directory (for example, `c:\arcsight\web`) by making a copy. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.



Caution

Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

- 3 Download the executable file specific to your platform from the ArcSight Software Download Site. (In the following file names, `xxxx` stands for the build number.)
 - ◆ `Patch-4.5.1.xxxx.2-Web-Win.exe`
 - ◆ `Patch-4.5.1.xxxx.2-Web-Solaris.bin`
 - ◆ `Patch-4.5.1.xxxx.2-Web-AIX.bin`
 - ◆ `Patch-4.5.1.xxxx.2-Web-Linux.bin`
- 4 While logged in as the ArcSight user, run one of the following executables specific to your platform.
 - ◆ **On Windows:**
Double-click `Patch-4.5.1.xxxx.2-Web-Win.exe`
 - ◆ **On Solaris:**
Run the following command.


```
./Patch-4.5.1.xxxx.2-Web-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Web-Solaris.bin -i console
```
 - ◆ **On AIX:**
Run the following command.


```
./Patch-4.5.1.xxxx.2-Web-AIX.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Web-AIX.bin -i console
```
 - ◆ **On Linux:**
Run the following command.

```
./Patch-4.5.1.xxxx.2-Web-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./Patch-4.5.1.xxxx.2-Web-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing [ARCSIGHT_HOME](#) for your v4.5 SP1 ArcSight Web installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer provided default location, click **Restore Default Folder**.
- 7 Click **Next**.
- 8 Choose a Link Location (on Solaris, AIX, and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button, then click **Next**.
- 9 Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
- 10 Click **Install**.
- 11 Click **Done** on the Install Complete screen.

To Uninstall

If needed, use the procedure to roll back this patch installation.



Note

Before you begin to uninstall, verify that the Web's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Stop the ArcSight Web server.
- 2 Run the uninstaller program:

On Windows:

 - ◆ Double-click the icon you created for the uninstaller when installing the ArcSight Web. For example, if you created an uninstaller icon on your desktop, double-click that icon.
 - ◆ Or, if you created a link in the Start menu, click
Start->ArcSight Web SP1 Patch2-> Uninstall ArcSight Web 4.5 SP1 Patch 2
 - ◆ Or, run the following from the Web's [ARCSIGHT_HOME\UninstallerDataSP1Patch2](#) directory.
[Uninstall_ArcSight_Web_Patch.exe](#)

On Solaris, AIX, and Linux:

 - ◆ From the directory where you created the links when installing the ArcSight Web (in your home directory or another location), run:
[./Uninstall_ArcSight_Web_Component_4.5_SP1Patch2](#)
 - ◆ Or, to uninstall using console mode, run:

```
./Uninstall_ArcSight_Web_Component_4.5_SP1Patch2 -i console
```

- ◆ If you did not create a link, execute the command from the `ARCSIGHT_HOME/UninstallerDataSP1Patch2` directory:

```
./Uninstall_ArcSight_Web_Patch
```

- 3 Click **Done** on the Uninstall Complete screen.

Installing ArcSight Console Patch on Mac

The patch installer download and run procedure is slightly different on the Mac than on the other supported platforms.

To Install



If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

- 1 Exit the ArcSight Console.
- 2 Back up the Console directory (for example, `/home/arcsight/console/current`) by making a copy. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.



Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

- 3 Download the file `Patch-4.5.1.xxxx.2-Console-MacOSX.zip` (where `xxxx` stands for the build number) into the directory in which the Console is installed (for example, `/home/arcsight/console/current`). Use the number that matches the specific patch number at the top of this document.



The patch installer file (that shows as a `.zip` on the download site) downloads as `Patch-4.5.1.xxxx.2-Console-MacOSX.app` on the Mac. A single or double-click on this `.app` file launches the patch installer, depending on how you have set these options. There is no need to "extract" or "unzip" the file; it downloads as a `.app` file.

- 4 Launch the patch installer by double-clicking the `ArcSightConsolePatch` file.
- 5 Follow the steps on the patch install wizard, providing the information as prompted:
 - ◆ Choose the location where you want to install the patch. Browse to the same the location of your existing `ARCSIGHT_HOME` for your v4.5 SP1 Console installation.
 - ◆ Choose an alias location for the Console application (or opt to not use aliases). This is the same as a link location on UNIX systems or shortcut location on Windows systems.
- 6 Click **Next**.
- 7 Verify your settings and click **Install**.

To Uninstall

If needed, use the procedure below to roll back this patch installation.



Before you begin to uninstall, verify that the Console's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Exit the ArcSight Console.
- 2 Run the uninstall by clicking the file [Uninstall_ArcSight_Console_4.5_SP1Patch2](#) created during the patch install (see [Step 5](#) above).

Logger Integration Commands

In ESM v4.5 SP1, Patch 2, new integration commands will allow ESM users to run Logger searches within the ESM Console. These commands will be supported with ArcSight Logger v4.0, and will be more fully described in the *ArcSight Logger v4.0 GA Administrator's Guide*.

An integration command has three components:

- The command, which defines the search command the user wants to run on the Logger Appliance.
- The target, which specifies the Logger Appliance to be searched.
- The configuration, which can combine multiple commands in the integration command menu.

Two types of integration commands are introduced in ESM v4.5 SP1, Patch 2: *Logger Search* and *Logger Quick Search*. These commands will be supported with ArcSight Logger v4.0.

Logger Search allows the user to right-click an event in an active channel and then run a search based on one of the fields presented in a list. If there is more than one Logger Appliance accessible from ESM, the user can select which Logger to search.

In summary, Logger Search:

- Displays a pop-up dialog with search options.
- Allows users to search by:
 - ◆ Event Name
 - ◆ Destination
 - ◆ Source
 - ◆ Destination and Source
 - ◆ User
 - ◆ Service Vendor and Product
- Allows users to select the Logger Appliance on which to run the search.

In contrast, Logger Quick Search allows users to right-click a field in an active channel to perform a quick search based on the field and value selected. If there is more than one Logger appliance set up, a pop-up dialog box allows users to choose which appliance to search.

In summary, Logger Quick Search:

- Allows quick search without a pop-up dialog
- Creates a search with the type and value of the field that has been selected

Enabling Integrated Searches

This section describes the configuration steps required to enable integrated searches on Logger.

- 1 Log in to the ESM Console.
- 2 Set up integration targets:
 - a In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Targets**.
 - b Create an integration target for your Logger Appliance, or edit one of the existing entries.
 - c On the **Integration Parameters** tab, add the following parameter:

Parameter: LoggerHost

Type: Text

Value: [IP address or hostname of the Logger Appliance]
 - d If you have more than one Logger Appliance, create an additional integration target for each appliance to be made searchable.
- 3 Set up integration configurations:
 - a In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Configurations**.
 - b Edit the **Logger Search** integration configuration:
 - i Click the **Targets** tab, and then add the integration target(s) you created in [Step 2](#).
 - c Edit the **Logger Quick Search** integration configuration:
 - i Click the **Targets** tab and then add one integration target from the list of targets you just created.
- 4 Set up ESM users:
 - a In the Navigator, click the **Resources** tab, and then navigate to **Users**.
 - b Edit the ESM users that will have access to the Logger Appliance. In most cases, these users should have administrator privileges.
 - c Click the **Integration Parameters** tab, and then create an integration parameter for the Logger user:

Parameter: LoggerUser

Type: Text

Value: [Logger username]

Targets: select targets for that Logger user

- d** Create an integration parameter for the Logger password:
Parameter: LoggerPassword
Type: Password
Value: [Logger password]
Targets: select targets for that Logger user (same as for Logger User).

Issues Fixed in this Patch

The following issues are addressed in Patch 2.

Install and Uninstall

Number	Description
56750	Solaris 64-bit platform: Fresh install of ESM v4.5 SP1 in FIPS mode, or upgrade from v4.0 SP3 Patch 3 in FIPS mode to v4.5 SP 1 FIPS mode failed. Users were not able to start the Manager after installation. Now, the issue has been resolved. After installation, users can start the Manager as expected.
57485	When an existing license key was used during ESM v4.5 SP1 installation, the license keys displayed an error such as Internal license, used for development and QA , followed by the customer name. Now, this issue is fixed.

Database

Number	Description
53530	Running a Partition Archive in standalone mode (using <code>arcsight database pa -i standalone -cn archive</code>) resulted in an error message such as: <code>Error: Cannot initialize the configuration!</code> <code>com.arcsight.common.persist.NoSuchBrokerFactoryException:</code> <code>Broker factory generic is not yet registered</code> Now, the Archive Partition command completes successfully when run in standalone mode.

ArcSight Manager

Number	Description
59167	Reducing the IP range of a zone resulted in an error message, and the workaround was to delete the zone and recreate it. Now, when no assets fall outside the range of the zone, the range can be reduced without generating errors.

Number	Description
58856	<p>If events sent by the ESM FlexConnector had a value set for event annotation, but the audit trail was set to null, then the Manager would drop the event and display a <code>java.lang.NullPointerException</code> error.</p> <p>Now, the issue has been resolved and the error no longer appears.</p>
58643	<p>When users created a query based on an Active List, they were unable to see the <code>get_active_list_value</code> variable function. However, when a query was based on an Event, rather than an Active List, users could see and use the function as expected. This problem prevented users from generating certain critical reports.</p> <p>Now, the problem is solved and users can create queries based on <code>get_active_list_value</code>.</p>
57701	<p>When multiple identical sessions were created with the same start time, some sessions did not expire.</p> <p>Now, this issue has been fixed and entries expire correctly.</p>
59080	<p>In ESM v4.5 SP1, Data Monitors and Dashboards using filters involving IP addresses with <code>IN</code> condition did not populate data correctly.</p> <p>Now, the issue has been resolved and data population occurs as expected.</p>
57702	<p>The Delete and Terminate Session Entry functions did not work properly for huge session lists containing, for example, a million entries. If a new session with a short list was created, the functions behaved as expected.</p> <p>The issue is now fixed, but be aware that the fix is only applicable when the number of live sessions is fewer than the declared maximum size of the session list. When the number of live sessions overflows the cache, termination still might not work in some cases.</p>

ArcSight Console

Number	Description
58715	<p>The Inline filter drop-down list for an active channel showed very few attribute values.</p> <p>Now, the drop-down list shows more distinct attribute values based on the events cached, which depends on pages loaded on the active channel.</p>
58804	<p>Viewing problems occurred when users tried to import a CSV file into an Active List. If more than ~60 items were imported, the Import Viewer pane became too long to be viewed, and users did not have access to the OK button.</p> <p>Now, this issue has been fixed and users can interact with the Import Viewer pane as expected.</p>
58752	<p>After upgrading to ESM v4.5 SP1, Active Lists were forced to fit into the Viewer Panel. The scroll-bars that existed in earlier versions no longer appeared, making it difficult to examine lists with multiple columns.</p> <p>Now, the problem has been resolved and Active Lists display as expected.</p>
57446	<p>When Display Time as GMT was selected, creating an event graph based on a selection of events in an Active Channel would result in no graph, that is, in a value of zero for all sources, destinations, and so on. Upon failure, the Manager logs displayed an error message.</p> <p>The problem was due to a mismatch between the channel ID and timezone stored in the Channel Registry (GMT), and the time in which the Console was started, for example, PST.</p> <p>Now, the mismatch no longer occurs, and event graphs can be created as expected.</p>
58641	<p>When using certain tools, such as nslookup and whois, <code>\$selectedCell</code> or <code>\$selectedItem</code> didn't work correctly on a bucketized data monitor.</p> <p>For example, consider an Active Channel and an Event Graph Data monitor that both show the same IP address. When nslookup was used on the IP address in the Active Channel, the IP address was resolved. However, if the same action was performed on the IP address in the Event Graph Dashboard, the IP address did not always resolve.</p> <p>Now, the issue is fixed.</p>
58546	<p>When users opened multiple Console windows and used different sets of data monitors and dashboards in a multi-monitor environment, display became an issue, especially for users trying to run multiple Dashboard slideshows. For example, multiple dashboards always displayed data in the default monitor. Even when one of the Console windows was dragged to the second monitor, it returned to default monitor. There was no issue when using a single Console window in a multi-Monitor environment.</p> <p>Now, the issue has been resolved and multi-monitor environments behave as expected.</p>

Number	Description
58322	<p>After upgrading to ArcSight Console 4.5.1.5926, the column size reset to the default on all Dashboards. The column size reset every time the Dashboard refreshed. The problem occurred in table view only.</p> <p>Now, the issue has been fixed and the column size is no longer reset upon refresh.</p>
58291 58456	<p>When the Console was used in full-screen mode for slideshows in a multi-monitor environment, pressing F11 and clicking any place on screen resulted in the Console window being minimized. This issue made opening multiple windows impossible, causing problems for users trying to run multiple Dashboard slideshows across multiple monitors.</p> <p>Now, the Console does not minimize when focus is changed to different screen, allowing slideshows to be displayed in full-screen mode on any monitor.</p>
58362	<p>Users could not select multiple rows for any Action under the following circumstances:</p> <ol style="list-style-type: none"> 1 Navigate to All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resource Change Log/Resource Change Log 2 Right-click a Data monitor in the Navigator > Add to Dashboard > Table. <p>When the Shift button was depressed and used in conjunction with the down-arrow keys in the Viewer, multiple selections were not possible. The user could select only one row at a time.</p> <p>Now, using the Shift button and down-arrow keys to select multiple rows works as expected.</p>
58435	<p>Due to an issue in ESM v4.5 SP1, users attempting to use non-time fields, such as Priority, as the first sort field on system tables received an error.</p> <p>Users could work around the issue by specifying specify a time field (MRT or ET) as the first sort field, and then applying a non-time field, such as Priority, as the second sort field.</p> <p>Now, the issue has been resolved and Priority can be specified as the primary sort.</p>
59347	<p>When attempting to access a key for a session list event (and the event's timestamp was older than the in-memory session list cache), the rule engine continued to retry while it waited for an asynchronous notification of lookup completion. This state looped indefinitely, and included an extraneous database lookup with each cycle.</p> <p>Now, the issue has been fixed.</p>
59350	<p>Infinite cycle occurred when processing events for pruned entries in session lists when the session list was not full.</p> <p>Now, extra logging has been added to better analyze this situation if it occurs. Also, a new configuration property was added that prevents unnecessary database access, to protect performance. The property is:</p> <p><code>session.cache.avoidDBLookup</code></p> <p>To enable this property, set it to <code>true</code> in the server.properties file.</p>

Known Issues in this Patch

These open issues in Patch 2 merit your review to avoid difficulties.

Number	Description
60305	Integration command does not pick up value using an event-based field name if the context is an active list or a session list.
60243	<p>During execution of an integration command, quotes are automatically added to values that contain spaces, but not for values that contain a character (for example, values from the <code>deviceEventClass</code> field). This issue can cause problems for ESM Logger integration, in which values with but not quoted are treated as regular expressions.</p> <p>Workaround: Add the quotes manually in the integration command, around the variables.</p>
59649	<p>Linux and Mac OS: Logger integration commands are not available from the context menu on the Channels tab of the ArcSight Console. To run Logger integration command for these operating systems, use an external browser.</p>

Open and Closed Issues in ESM v4.5 SP1

For information about open and closed issues present in ESM v4.5 SP1, see the release notes for that version.

