

Patch Release Notes **ArcSight™ ESM**

Version 4.5 SP2, Patch 1
Build 4.5.2.6088.1

March 17, 2010



Patch Release Notes ArcSight™ ESM , Version 4.5 SP2, Patch 1

Copyright © 2010 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 |
|----------|--|---|
| 03/17/10 | ArcSight™ ESM Version 4.5, SP2, Patch 1 | Release Notes for ArcSight™ ESM Version 4.5, SP2, Patch 1. |

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 SP2, Patch 1 | 1 |
| ESM Patch 4.5.2.6088.1 | 1 |
| Purpose of this Patch | 1 |
| Geographical Information Update | 1 |
| Vulnerability Updates | 1 |
| Oracle Critical Patch Update (CPU) Certification | 2 |
| OPatch | 2 |
| Applying the CPU | 3 |
| Workarounds for Known Issues in Oracle CPU | 4 |
| Installing ESM Version 4.5 SP2, Patch 1 | 5 |
| Platform-Specific Information for Installing Patch 1 | 6 |
| Installing ArcSight Console Patch on a Mac | 17 |
| Issues Fixed in this Patch | 18 |
| ArcSight Manager | 18 |
| ArcSight Console | 20 |
| Open Issues in this Patch | 21 |
| Open and Closed Issues in ESM v4.5 SP2 | 22 |

ArcSight ESM, Version 4.5 SP2, Patch 1

ESM Patch 4.5.2.6088.1

These release notes describe how to apply the 4.5 SP2, Patch 1 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 SP2 only. If you need to set up a fully current ESM v4.5 SP2, Patch 1 installation, install v4.5 SP2 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 January 2010
- 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_20100201**.

Vulnerability Updates

This patch contains updated vulnerability mapping (February 2010 Context Update) 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 |
| Symantec Endpoint Protection | Bugtraq, CVE |

| Device | Vulnerability Updates |
|---|---|
| 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 January, 2010. 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 January 2010 Patch |
|-----------------------------|---------------------------------|
| Windows 32 | p9169457_10204_Win32.zip |
| Windows 64 (AMD64-EM64T) | p9169460_10204_MSWIN-x86-64.zip |
| Linux 32 | p9119226_10204_Linux-x86.zip |
| Linux x86-64 | p9119226_10204_Linux-x86-64.zip |
| AIX | p9119226_10204_AIX5L.zip |
| Solaris 64 | p9119226_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 January 2010 |
|-----------------------------|----------------------------------|
| 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 |

Applying the CPU

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

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

For example,

On Windows:

If the [README](#) says:

```
>OPatch apply
```

use this command instead:

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

On UNIX:

If the [README](#) says:

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

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 might fail and the following error message appears.

```
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.

Installing ESM Version 4.5 SP2, Patch 1

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 1.



- In some Solaris environments, when upgrading the ESM Manager and also when installing the solution packages, these actions do not complete. This problem might 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 6](#).
- **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 1

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 SP2, Patch 1 for ArcSight Database.

To Install the Patch



- 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](#) represents the build number.)

- ◆ [Patch-4.5.2.xxxx.1-DB-Win.exe](#)
- ◆ [Patch-4.5.2.xxxx.1-DB-Solaris.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-DB-AIX.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-DB-Linux.bin](#)

-
- 4 As the Oracle Database owner, run one of the following executables specific to your platform.
- ◆ **On Windows:**
Double-click `Patch-4.5.2.xxxx.1-DB-Win.exe`
 - ◆ **On Solaris:**
Run the following command.

`./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-DB-Solaris.bin -i console`
 - ◆ **On AIX:**
Run the following command.

`./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-DB-AIX.bin -i console`
 - ◆ **On Linux:**
Run the following command.

`./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-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 SP2 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 you have installed both the database **and** 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.
- 6 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 the Patch

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 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 SP2 Patch1-> Uninstall ArcSight Database 4.5 SP2 Patch 1
 - ◆ Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP2Patch1` 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_SP2Patch1
```
- ◆ Or, to uninstall in console mode, run

```
./Uninstall_ArcSight_Database_4.5_SP2Patch1 -i console
```
- ◆ If you did not create a link, execute the following command from the Database's `ARCSIGHT_HOME/UninstallerDataSP2Patch1`.

```
./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.
- 8 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 v4.5 SP2, Patch 1 for ArcSight Manager.

To Install the Patch



Note

- Before you install the patch, verify that [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by 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.



Caution

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` represents the build number.)

- ◆ [Patch-4.5.2.xxxx.1-Manager-Win.exe](#)
- ◆ [Patch-4.5.2.xxxx.1-Manager-Solaris.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-Manager-AIX.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-Manager-Win.exe](#)

- ◆ **On Solaris:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-Manager-Solaris.bin
```

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

```
./Patch-4.5.2.xxxx.1-Manager-Solaris.bin -i console
```

- ◆ **On AIX:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-Manager-AIX.bin
```

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

```
./Patch-4.5.2.xxxx.1-Manager-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-Manager-Linux.bin
```

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

```
./Patch-4.5.2.xxxx.1-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 SP2 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 the Patch

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



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 SP2 Patch1-> Uninstall ArcSight Manager 4.5 SP2 Patch 1
- ◆ Or, run the following from the [ARCSIGHT_HOME\UninstallerDataSP2Patch1](#) 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_SP2Patch1
```

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

```
./Uninstall_ArcSight_Manager_4.5_SP2Patch1 -i console
```

- ◆ If you did not create a link, execute the following command from the `ARCSIGHT_HOME\UninstallerDataSP2Patch1` 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 SP2, Patch 1 for ArcSight Console on Windows, Solaris, and Linux platforms.



- Instructions describing how to install or uninstall the Console patch on Macintosh systems are provided in ["Installing ArcSight Console Patch on a Mac" on page 17](#).
 - 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 the Patch



- 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` represents the build number.)
 - ◆ `Patch-4.5.2.xxxx.1-Console-Win.exe`
 - ◆ `Patch-4.5.2.xxxx.1-Console-Solaris.bin`
 - ◆ `Patch-4.5.2.xxxx.1-Console-Linux.bin`

-
- 4 Run one of the following executables specific to your platform.
 - ◆ **On Windows:**
Double-click `Patch-4.5.2.xxxx.1-Console-Win.exe`
 - ◆ **On Solaris:**
Verify that you are logged in as the ArcSight user, and then run this command:

`./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-Console-Solaris.bin -i console`
 - ◆ **On Linux:**
Verify that you are logged in as the ArcSight user, and then run the following command.

`./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-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 SP2 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 the Patch

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 SP2 Patch1-> Uninstall ArcSight Console 4.5 SP2 Patch 1

- ◆ Or, run the following from the Console's [ARCSIGHT_HOME\current\UninstallerDataSP2Patch1](#) 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_SP2Patch1
```

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

```
./Uninstall_ArcSight_Console_4.5_SP2Patch1 -i console
```

- ◆ If you did not create a link, execute the command from the Console's [ARCSIGHT_HOME/current/UninstallerDataSP2Patch1](#) 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 SP2, Patch 1 for ArcSight Web.

To Install the Patch



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](#) represents the build number.)

- ◆ [Patch-4.5.2.xxxx.1-Web-Win.exe](#)
- ◆ [Patch-4.5.2.xxxx.1-Web-Solaris.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-Web-AIX.bin](#)
- ◆ [Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-Web-Win.exe](#)

- ◆ **On Solaris:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-Web-Solaris.bin -i console
```

- ◆ **On AIX:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-Web-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./Patch-4.5.2.xxxx.1-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-4.5.2.xxxx.1-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 SP2 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 the Patch

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 SP2 Patch1-> Uninstall ArcSight Web 4.5 SP2 Patch 1
- ◆ Or, run the following from the Web's [ARCSIGHT_HOME\UninstallerDataSP2Patch1](#) 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_4.5_SP2Patch1
```

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

```
./Uninstall_ArcSight_Web_4.5_SP2Patch1 -i console
```

- ◆ If you did not create a link, execute the command from the `ARCSIGHT_HOME/UninstallerDataSP2Patch1` directory:

```
./Uninstall_ArcSight_Web_Patch
```

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

Installing ArcSight Console Patch on a Mac

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

To Install the Patch



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-4.5.2.xxxx.1-Console-MacOSX.zip` (where `xxxx` represents 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-4.5.2.xxxx.1-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 SP2 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 the Patch

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_SP2Patch1` created during the patch install (see [Step 5](#) above).

Issues Fixed in this Patch

The following issues have been addressed in this patch.

ArcSight Manager

| Number | Description |
|--------|---|
| 58654 | After a major upgrade, the Manager failed to process any connector events (due to asset conflicts). This issue is now fixed. |
| 59327 | Within a variable, the concatenate function is used to merge two fields. In ESM 4.5 SP1 , if one of the fields was empty, it only displayed the null field. For example, if the string " <code>Agent name (Manager Internal Agent)</code> " is concatenated with " <code>Attacker Dns Name (nothing)</code> ", the result displays as " <code>manager Internal Agentnull</code> ". This issue also appeared in active channels and data monitors. This issue is now fixed. |
| 59537 | The parameter <code>external.export.querygroup.max</code> applies to automatic case search group export. However, this parameter had no effect when manually exporting cases from an Active Channel or when using the rule action " <code>Export to External System</code> ". This issue is now fixed. |
| 59958 | When using a trend as the source in a query and adding a variable, the List functions did not appear within the drop-down menu. This functioned correctly in v4.0 SP3 , but not in v4.5 SP1 . This issue is now fixed. |

| Number | Description |
|--------|--|
| 60799 | <p>There was an issue with the AUP content update mechanism on the Manager. If a connector had incorrect permissions for the ARCSIGHT_HOME/update directory, the Manager continued to open new threads to the connector in an attempt to push the update.</p> <p>This issue is now fixed.</p> |
| 61052 | <p>Using the "In" operator broke rules when using variables.</p> <p>This issue is now fixed.</p> |
| 61637 | <p>When the Manager automatically activated or deactivated a rule, the rule's "Last-Update-Time" was updated while "Last-Updated-By-User" was not.</p> <p>This issue is now fixed.</p> |
| 62460 | <p>MaxEventIdExceededCheckTask stopped the Manager event flow even after resetting the event_id sequence.</p> <p>This issue is now fixed.</p> |
| 64291 | <p>On 4.5 SP1 Patch3, upon expiration of their password, Web users were unable to login to ArcSight Web. The system did not allow them to change their password and the following message appeared:</p> <p>"ArcSight Manager requires you to answer a challenge. This client does not support this feature. Please log in using ArcSight Console or ArcSight Web and try again."</p> <p>Workaround:</p> <p>Use ArcSight Console or ArcSight Web to change your password.</p> |
| 64792 | <p>When creating a join rule with a time-difference based variable, you received an "Invalid field name" error.</p> <p>This issue is now fixed.</p> |
| 64939 | <p>With multiple cases selected in the Navigator under the Cases view, right-clicking and selecting Export To External System from the context menu only exported a single case.</p> <p>This issue is now fixed such that all selected cases are exported.</p> |

ArcSight Console

| Number | Description |
|----------------|---|
| 55822 | <p>An Active Channel Radar Scale did not display values (such as number of events) on the y-axis.</p> <p>This issue is now fixed.</p> |
| 58644 | <p>Under certain conditions, the Resource Graph configuration view did not display.</p> <p>This issue is now fixed.</p> |
| 58803 | <p>If a location was set to German, /All Data monitors/ArcSight Administration/System Health/Connector Status, and /Current Connector Status displayed formats incorrectly within ArcSight Console and Arcsight Web. This may have affected any location that used the European format in interpreting dots and commas in calculations.</p> <p>This issue is now fixed.</p> |
| 58821 | <p>When installing the Console and/or the Manager in FIPS mode, if the version of <code>C:\WINDOWS\system32\nspr4.dll</code> was an older version than the supported version, the following error message appeared.</p> <p><code>"Error Enabling FIPS mode, please make sure NSSDB is in FIPS mode and restart the wizard."</code></p> <p>This error message has now been fixed to correctly represent the actual problem.</p> |
| 59248 | <p>Fixed two display issues related to importing large CSV files:</p> <ul style="list-style-type: none">• When the import list in the CSV files had too many entries, the Active List Import Preview dialog failed to show all entries.• If Creation Time and Last Modified time columns were not defined in the active list, the CSV values for these two columns were displayed as empty strings in the Active List Import Preview dialog. |
| 60660 | <p>After changes in the CCE of the resource editor, the OK/Apply buttons failed to work.</p> <p>This issue is now fixed.</p> |
| 61600 | <p>When configuring a connector through the Console, if you added more than three IP ranges in the 'Dont Reverse-Resolve IP Ranges' box (located in the Default tab of the connector's Inspect/Edit panel), only the first three ranges were displayed.</p> <p>Also, editing a cell resulted in an inability to edit any other cell in this tab.</p> <p>Both issues have been fixed in this release.</p> |
| 61775 | <p>When editing a report and scheduling a new job, if you clicked the Apply button without setting the Frequency, your scheduled job was not saved.</p> <p>This issue is now fixed so that clicking the Apply or OK button without setting the Frequency results in an error message requesting that you set the Frequency.</p> |
| 64725 64903 | <p>The Active Channel did not display fields in the order that they were defined by the field set.</p> <p>This issue is now fixed.</p> |

Open Issues in this Patch

These open issues in Patch 1 merit your review to avoid difficulties.

Installation

| Number | Description |
|--------|---|
| 46995 | In Console mode, the installer sometimes does not validate the Uninstall Links folder. The system successfully validates the Base folder, but without user write permissions it does not create an uninstall link. |
| 47996 | <p>If you start the patch installation wizard, then navigate back and forward using the Previous and Next buttons (for example, to reset configuration options on previous screens), but then exit from the wizard without actually installing, the base component fails to launch. The same launch failure occurs if you cancel the installation at any point.</p> <p>This is because the preparatory step of backing up the files has already occurred.</p> <p>Workaround: If you encounter this situation, you can restore functionality of the base Console by running the following commands to restore the backup files.</p> <p>On Windows: <ARCSIGHT_HOME>\bin\rollbacksp2p1.bat</p> <p>On Unix: <ARCSIGHT_HOME>/bin/rollbacksp2p1.sh</p> |
| 53754 | <p>The Patch Uninstaller for Manager and Web does not remove the link on Unix and the shortcut on Windows.</p> <p>Workaround:</p> <p>Delete this link manually after uninstall is complete.</p> |

Manager

| Number | Description |
|--------|---|
| 55207 | <p>Daily Trends (only existing trends) are out of sync by one hour after the October 2008 DST change. The query interval should be set manually to reflect the correct times for existing trends.</p> <p>For assistance in setting the query interval manually, contact ArcSight Customer Support.</p> |
| 60932 | <p>When an event is aggregated on agent ID, the resulting correlation event shows as the original agent ID from the base event. This occurs even though the agent_type is "arcsight_security_manager" (that of the Manager internal agent).</p> <p>When this happens, an additional entry gets created in the arc_event_agent_side table, which, if multiple such entries are created, could lead to side table performance issues.</p> |

| Number | Description |
|--------|--|
| 62372 | <p>If your time zone is set to Asia/Kolkatta, or if your system time zone is set to America/Toronto, the ESM Manager fails to start after upgrading to ESM installation v4.5 SP1 Patch 3 or later. This is likely due to the difference in how the Java and Oracle handle the GMT offset.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1 Check the Manager <code><ARCSIGHT_HOME>/logs/default/server.log</code> file. This file contains instructions on how to fix the issue, as shown in the following example. <pre>com.arcsight.common.persist.PersistenceException: Default Oracle timezone not found: SELECT tzname FROM v\$timezone_names WHERE tzname='GMT+9:00' Set server property 'oracle.infobroker.default.timezone' with a valid TZNAME from v\$timezone_names</pre> 2 Follow the instructions provided in the <code>server.log</code> file. |

Console

| Number | Description |
|--------|--|
| 65404 | <p>Console on Unix only:</p> <p>Clicking the Help button in the Console displays a blank page. An error message appears in the Console shell window.</p> <p>This issue is slated for resolution in a future release.</p> |
| 65518 | <p>In some European locales, the Database Performance Statistic dashboard displays numbers with decimals incorrectly. It appears in the American style where the number <code>481,17</code> displays as <code>481.17</code>.</p> <p>This issue is slated for resolution in a future release.</p> |

Analytics

| Number | Description |
|--------|---|
| 65253 | <p>When changing the name of an existing trend, the name change does not persist. Instead, the following error message appears. <code>"Resource in broker is newer than modified resource".</code></p> <p>Workaround:</p> <p>Refresh the trend, reedit its name, and recommit it.</p> |

Open and Closed Issues in ESM v4.5 SP2

For information about open and closed issues for ESM v4.5 SP2, see the release notes for that version.