

Patch Release Notes

ArcSight™ ESM

Version 5.0 SP2 Patch 3
Build 5.0.2.6904.3

June 1, 2012



Patch Release Notes ArcSight™ ESM Version 5.0 SP2 Patch 3

Copyright © 2012 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

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

This document is confidential.

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

ESM Patch 5.0.2.6904.3	5
Purpose of this Patch	5
Usage Notes for this Patch	5
Section 508 Compliance	5
Geographical Information Update	6
Vulnerability Updates	6
Installing ESM Version 5.0 SP2 Patch 3	7
ArcSight ESM Database	8
ESM Manager	11
ArcSight Console	14
ArcSight Web Server	17
Upgrade Oracle 11.2.0.1 to 11.2.0.2 on Windows	19
Issues Fixed in this Patch	24
Analytics	24
ArcSight Console	24
ArcSight Manager	24
ArcSight Web	25
General	25
Open Issues in this Patch	26
General	26
Installation and Upgrade	27
Issues Fixed in Patch 2	27
Analytics	27
ArcSight Console	27
ArcSight Database	28
ArcSight Manager	28
General	29
Localization	30
ArcSight Web	31
Open and Closed Issues in ESM v5.0 SP2	31

ArcSight ESM Version 5.0 SP2 Patch 3

ESM Patch 5.0.2.6904.3

These release notes describe how to apply this patch release of ESM. Instructions are included for each component, as well as other information about recent changes and open and closed issues.

This patch is for ESM v5.0 SP2 only. If you are on an earlier version of ESM, refer to the release notes for v5.0 SP2 for information on upgrading. To set up a new ESM v5.0 SP2 installation, refer to the *ArcSight ESM Installation and Configuration Guide*.

After you have upgraded to v5.0 SP2, follow the instructions in ["Installing ESM Version 5.0 SP2 Patch 3" on page 7](#) of these release notes to apply Patch 3.

Refer to *ArcSight Oracle Patch Set Update (PSU) Release Notes* for Oracle Patch Set Update and OPatch information.

If you use time zones in Russia or Belarus, follow the instructions provided in the ESM Hot Fix RDST20111029 to upgrade your environment with Oracle patch updates to support Russia's and Belarus' transition away from Daylight Savings Time.

Purpose of this Patch

This patch:

- Addresses customer reported and other issues in ESM v5.0 SP2
- Provides updates for geographical information and vulnerability mapping.
- Provides a JRE update in Patch 3 to support Russia's and Belarus' transition away from Daylight Savings Time.
- Provides upgrade procedure from Oracle 11.2.0.1 to Oracle 11.2.0.2.

Usage Notes for this Patch

Refer to *ArcSight™ ESM Release Notes Version 5.0 SP2* for usage notes for that service pack.

Section 508 Compliance

HP recognizes the importance of accessibility as a product initiative. To that end, HP continues to make advances in the area of accessibility in its product lines.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20120201.

Vulnerability Updates

This release includes recent vulnerability mappings (January 2012 Context Update) for these devices:

Device	Vulnerability Updates
Snort/Sourcefire SEU 629 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, CERT, MSSB
Entersys Dragon IDS Updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S646 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2132 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
ISS SiteProtector updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
Symantec Endpoint Protection updated	Faultline, Bugtraq, CVE, MSSB, MSKB, CERT
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	Faultline, CVE, Nessus, MSSB

Installing ESM Version 5.0 SP2 Patch 3

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

Please keep the following points in mind when installing Patch 3:



- On Solaris environments, upgrading the ESM Manager and installing the solution packages are unsuccessful if your Solaris system does not meet the system requirements. See the *ESM Installation and Configuration Guide* for the minimum system requirements for a Solaris system.
- **For all components and platforms:** Make sure 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, restore the component base build from the backup, then resume installation of the patch.
- 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 8](#).
- Backup, patch install, and uninstall procedures require permissions for the relevant components. For example, to back up a database installation and install an Oracle critical patch update, you need database logon permissions. To back up the Manager installation and install the Manager patch, you need Manager permissions. To install a patch, make sure 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 a good practice to create a backup of the existing product before installation begins.
- To uninstall the software you must be at the same user level as the original installer.
- For backup, patch install, and uninstall, we recommend that you log in to the target machine with a specific account name via telnet or SSH. If you switch accounts after logging in, then specify the flag "-" for the **su** command (`su - <UserName>`).

Each component has install and uninstall 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 v5.0 SP2 Patch 3 for ArcSight Database.

To Install the Patch



Note

- 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
```



Note

[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.



Note

HP 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 HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, [xxxx](#) represents the build number.

- ◆ [Patch-5.0.2.xxxx.3-DB-Win.exe](#)
- ◆ [Patch-5.0.2.xxxx.3-DB-Solaris.bin](#)
- ◆ [Patch-5.0.2.xxxx.3-DB-AIX.bin](#)
- ◆ [Patch-5.0.2.xxxx.3-DB-Linux.bin](#)

4 As the Oracle Database owner, run one of the following executables specific to your platform:

◆ On Windows:

Double-click [Patch-5.0.2.xxxx.3-DB-Win.exe](#)

◆ On Solaris:

Run the following command:


```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-DB-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-DB-AIX.bin -i console
```

◆ **On Linux:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-DB-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
- 7 Enter the location of your existing ArcSight Database <ARCSIGHT_HOME> for your v5.0 SP2 database installation in the text box provided, or navigate to the location by clicking **Choose...**
- 8 To restore the installer-provided default location, click **Restore Default Folder**.
- 9 Click **Next**.
- 10 Choose a Link Location (on Solaris, AIX, and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button, and then click **Next**.
- 11 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.
- 12 Click **Install**.
- 13 Click **Done** on the Install Complete screen.

After you have installed both the database **and** Manager patch, update the Partition Archiver. These steps are required to update 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
```



Note

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

To Uninstall the Patch

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



Note

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

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

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 > All Programs > ArcSight DB 5.0 SP2 Patch 3 > Uninstall ArcSight Database 5.0 SP2 Patch 3

- ◆ Or, run the following from the [<ARCSIGHT_HOME>\UninstallerDataSP2Patch3](#) directory:

```
Uninstall_ArcSight_DB_Patch.exe
```

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_5.0_SP2Patch3
```

- ◆ Or, to uninstall in Console mode, run:

```
./Uninstall_ArcSight_Database_5.0_SP2Patch3 -i console
```

- ◆ If you did not create a link, execute the following command from the Database's [<ARCSIGHT_HOME>/UninstallerDataSP2Patch3](#):

```
./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 *For Windows Only*, click **Cancel** in the Archiver Service Configuration screen.
- 8 Start the Partition Archiver Agent.

◆ **Windows:**

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

◆ **Solaris, AIX, and Linux:**

Run the following command:

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



`arc_oraclepartitionarchiver_db` is the default service name.

Note

ESM Manager

This section describes how to install or uninstall v5.0 SP2 Patch 3 for the 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 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.



HP 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 HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, `xxxx` represents the build number

- ◆ `Patch-5.0.2.xxxx.3-Manager-Win.exe`
- ◆ `Patch-5.0.2.xxxx.3-Manager-Solaris.bin`
- ◆ `Patch-5.0.2.xxxx.3-Manager-AIX.bin`
- ◆ `Patch-5.0.2.xxxx.3-Manager-Linux.bin`

- 4 While logged in as the ArcSight user, run one of the following executables specific to your platform.

- ◆ **Windows:**

Double-click `Patch-5.0.2.xxxx.3-Manager-Win.exe`

- ◆ **Solaris:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-Manager-Solaris.bin
```

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

```
./Patch-5.0.2.xxxx.3-Manager-Solaris.bin -i console
```

- ◆ **AIX:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-Manager-AIX.bin
```

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

```
./Patch-5.0.2.xxxx.3-Manager-AIX.bin -i console
```

- ◆ **Linux:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-Manager-Linux.bin
```

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

```
./Patch-5.0.2.xxxx.3-Manager-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.

- 7 Enter the location of your existing `<ARCSIGHT_HOME>` for your v5.0 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**.
- 8 Click **Next**.
- 9 Choose a Link Location (on Solaris, AIX, and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button, 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.

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 Manager.
- 2 Run the uninstaller program:

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 > All Programs > ArcSight Manager 5.0 SP2 Patch 3 > Uninstall ArcSight Manager 5.0 SP2 Patch 3
 - ◆ Or, run the following from the
`<ARCSIGHT_HOME>\UninstallerDataSP2Patch3` directory:
`Uninstall_ArcSight_Manager_Patch.exe`

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_5.0_SP2Patch3`
 - ◆ Or, to uninstall using Console mode, run:
`./Uninstall_ArcSight_Manager_5.0_SP2Patch3 -i console`
 - ◆ If you did not create a link, execute the following command from the
`<ARCSIGHT_HOME>\UninstallerDataSP2Patch3` directory:
`./Uninstall_ArcSight_Manager_Patch`
- 3 Click **Done** on the Uninstall Complete screen.

ArcSight Console

This section describes how to install or uninstall the v5.0 SP2 Patch 3 for ArcSight Console on Windows, Mac, Solaris, and Linux platforms.



The ArcSight 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>` directory and any of its subdirectories are not being accessed by any open shells on your system.
- If you need to re-install the patch, run the patch uninstaller before installing the patch again.



HP 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.

- 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.
- 3 Download the executable file specific to your platform from the HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, `xxxx` represents the build number.
 - ◆ `Patch-5.0.2.xxxx.3-Console-Win.exe`
 - ◆ `Patch-5.0.2.xxxx.3-Console-Solaris.bin`
 - ◆ `Patch-5.0.2.xxxx.3-Console-Linux.bin`
- 4 Run one of the following executables specific to your platform:
 - ◆ **On Windows:**
Double-click `Patch-5.0.2.xxxx.3-Console-Win.exe`
 - ◆ **On Solaris:**
Verify that you are logged in as the ArcSight user, and then run this command:

`./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Console-Solaris.bin -i console`
 - ◆ **On Linux:**
Verify that you are logged in as the ArcSight user, and then run the following command:

`./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Console-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
- 7 Enter the location of your existing `<ARCSIGHT_HOME>` directory for your v5.0 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**.
- 8 Click **Next**.
- 9 Choose a Link Location (on Solaris and Linux) or Shortcut location (on Windows) by clicking the appropriate radio button and 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.

To Install the Patch on a Mac

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

- 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.
- 3 Download the file `Patch-5.0.2.xxxx.3-Console-MacOSX.zip` to anywhere on your system. (`xxxx` represents the build number, as shown on the cover.)



The patch installer file (that shows as a **ZIP** file on the download site) downloads as `Patch-5.0.2.xxxx.3-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 an **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:
 - ◆ Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
 - ◆ Choose the location where you want to install the patch. Browse to `<ARCSIGHT_HOME>`, where your previous Console was installed.
 - ◆ 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 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 > All Programs > ArcSight Console 5.0 SP2 Patch 3 > Uninstall ArcSight Console 5.0 SP2 Patch 3
- ◆ Or, run the following from the Console's [<ARCSIGHT_HOME>\current\UninstallerDataSP2Patch3](#) 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_5.0_SP2Patch3`
- ◆ Or, to uninstall using Console mode, run:
`./Uninstall_ArcSight_Console_5.0_SP2Patch3 -i console`
- ◆ If you did not create a link, execute the command from the Console's [<ARCSIGHT_HOME>/current/UninstallerDataSP2Patch3](#) directory:
`./Uninstall_ArcSight_Console_Patch`

On a Mac:

- ◆ From the directory where you created the links when installing the Console, run:
`Uninstall_ArcSight_Console_5.0_SP2Patch3`
- ◆ From the Console's [<ARCSIGHT_HOME>/current/UninstallerDataSP2Patch3](#) directory, run:
`Uninstall_ArcSight_Console_5.0_SP2Patch3`

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

ArcSight Web Server

This section describes how to install or uninstall ESM v5.0 SP2 Patch 3 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.
- 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 HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, `xxxx` represents the build number.

- ◆ `Patch-5.0.2.xxxx.3-Web-Win.exe`
- ◆ `Patch-5.0.2.xxxx.3-Web-Solaris.bin`
- ◆ `Patch-5.0.2.xxxx.3-Web-AIX.bin`
- ◆ `Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Web-Win.exe`

- ◆ **On Solaris:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Web-Solaris.bin -i console
```

- ◆ **On AIX:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Web-AIX.bin -i console
```

◆ **On Linux:**

Run the following command:

```
./Patch-5.0.2.xxxx.3-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-5.0.2.xxxx.3-Web-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
- 7 Enter the location of your existing `<ARCSIGHT_HOME>` directory for your v5.0 SP2 ArcSight Web installation in the text box provided or navigate to the location by clicking **Choose...**

To restore the installer-provided default location, click **Restore Default Folder**.
- 8 Click **Next**.
- 9 Choose a Link Location (Solaris, AIX, and Linux) or Shortcut location (Windows) by clicking the appropriate radio button, 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.

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>` directory 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:

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 > All Programs > ArcSight Web 5.0 SP2 Patch 3 > Uninstall ArcSight Web 5.0 SP2 Patch 3
- ◆ Or, run the following from the Web's `<ARCSIGHT_HOME>\UninstallerDataSP2Patch3` directory:

```
Uninstall_ArcSight_Web_Patch.exe
```

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_5.0_SP2Patch3
```

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

```
./Uninstall_ArcSight_Web_5.0_SP2Patch3 -i console
```

- ◆ If you did not create a link, execute the command from the <ARCSIGHT_HOME>/UninstallerDataSP2Patch3 directory:

```
./Uninstall_ArcSight_Web_Patch
```

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

Upgrade Oracle 11.2.0.1 to 11.2.0.2 on Windows

Upgrading from 11.2.0.1 to 11.2.0.2 on Windows has the following prerequisites:

- Some of these instructions are different than previous Oracle upgrades. Please read them all.
- Upgrade your system to ESM v5.0 SP2 Patch 3 before you upgrade Oracle. That includes the Manager, ArcSight Console, Database, and ArcSight Web.
- Stop all ESM component processes before you start this Oracle upgrade. That includes the Manager, ArcSight Console, Partition Archiver, and ArcSight Web.
- If you configured your Oracle data storage within ORACLE_HOME, reconfigure the data storage to place these files elsewhere. If you do not reconfigure your data storage to place these files somewhere else, the upgrade might not be successful.

For information on finding and moving your database data files and Oracle Control files, look for the KCS articles "Moving Database Datafiles from One Disk to Another Local Disk or SAN Storage" and "How to relocate Oracle control files" on the HP SSO site at <http://support.openview.hp.com>. Search for KCS articles by name on the Self-Solve tab.

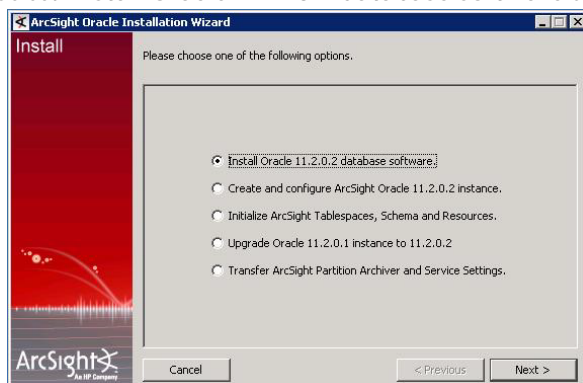
- Do not stop any Oracle services.

Use the following procedure to upgrade your Oracle software from 11.2.0.1 to 11.2.0.2:

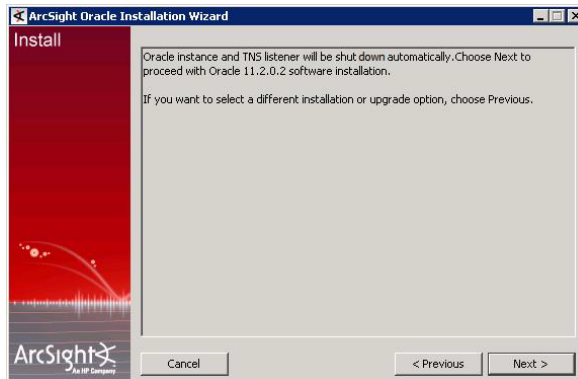
- 1 Run the following command from the bin directory of your ArcSight Database installation:

```
arcsight databasesetup
```

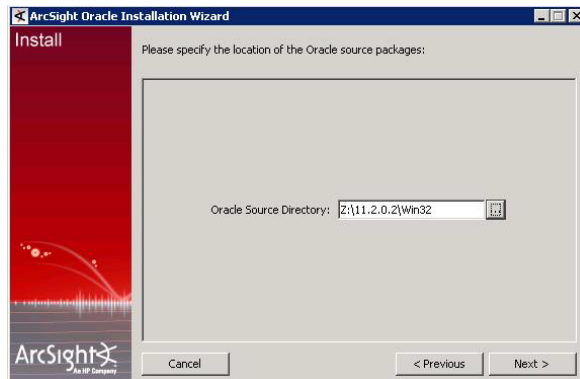
- 2 Select **Install Oracle 11.2.0.2 database software** and click **Next**.



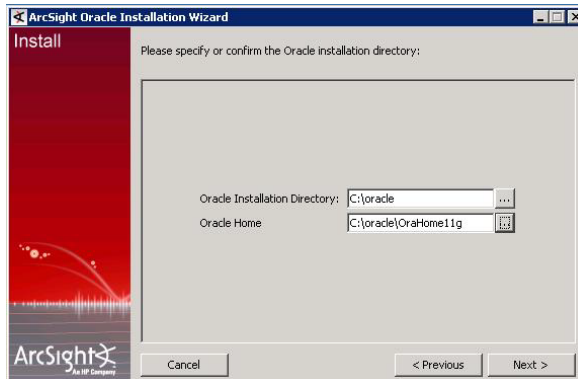
- 3 Do not stop any Oracle services; it is done automatically. Click **Next**.



- 4 Navigate to the location of the Oracle source packages and click **Next**.

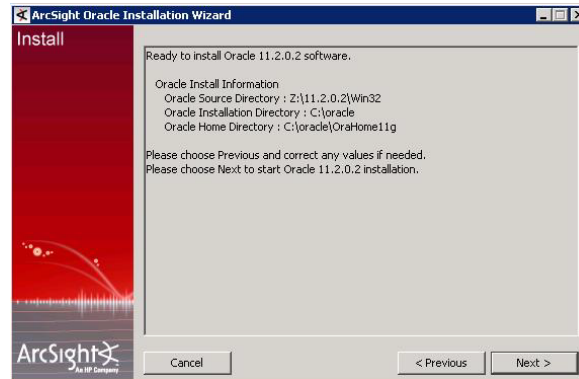


- 5 Enter the same file path for Oracle 11.2.0.2 as you used for 11.2.0.1, then click **Next**.

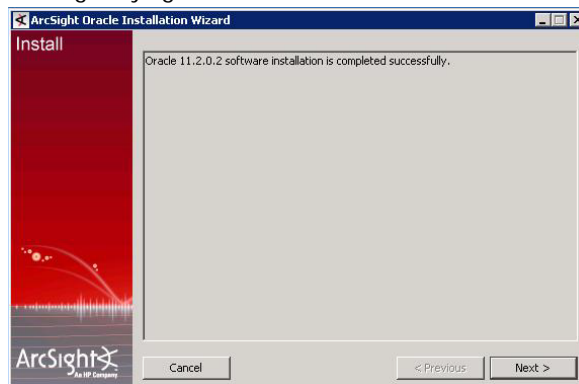
**Caution**

- Verify that the Oracle installation directory path and the ORACLE_HOME path do not contain any spaces.
- If you don't use the same file path as used in your 11.2.0.1 home, it might cause a failure in the upgrade that requires manual steps from HP support to recover from.

- 6 Review the pre-installation information and if satisfied, click **Next**.



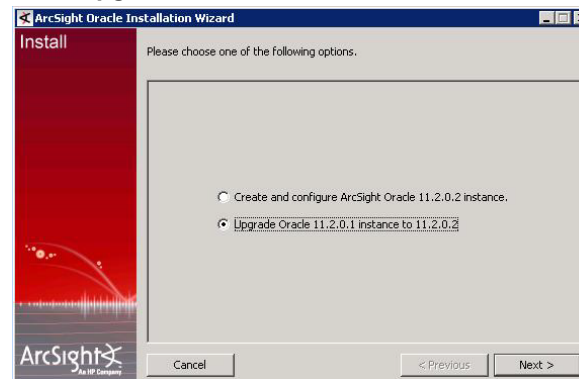
- 7 After the Oracle 11.2.0.2 software has been installed successfully, you will see a message saying so. Click **Next**.



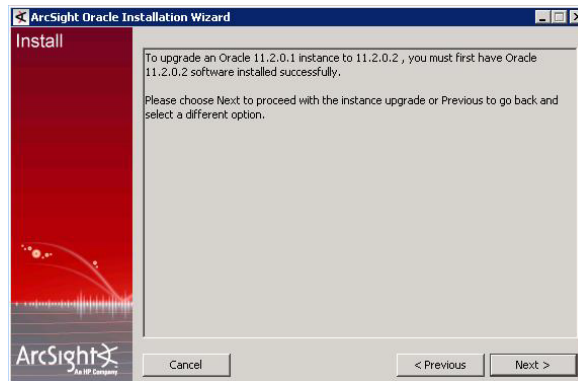
Upgrading a 11.2.0.1 Oracle Instance to 11.2.0.2

To upgrade your Oracle 11.2.0.1 instance:

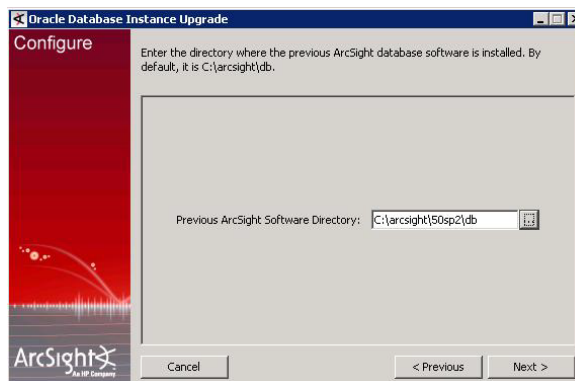
- 1 Select **Upgrade Oracle 11.2.0.1 instance to 11.2.0.2** and click **Next**.



- 2 Click **Next** if the Oracle 11.2.0.2 installation is successful.

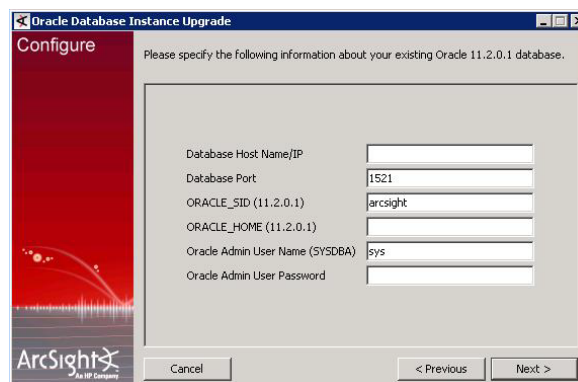


- 3 Enter the location where your current ArcSight Database (v5.0 SP2) exists and click **Next**.



The installation wizard uses this information to retrieve the database host name and port.

- 4 Enter the information about the previously-existing Oracle 11.2.0.1 software and click **Next**.



- 5 Select whether you want to configure the Enterprise Manager and enter the information for DBSNMP and SYSMAN and click **Next**.



Although you can install the Oracle Enterprise Manager client using ArcSight's Oracle 11g Installer, you must acquire licensing and support from Oracle directly.

- 6 The next screen will inform you that the instance upgrade is about to begin. Click **Next**.

- 7 A message appears when the instance has been successfully upgraded. Click **Finish**.

You have upgraded your Oracle database and the instance to 11.2.0.2.

Issues Fixed in this Patch

Analytics

Issue	Description
ESM-49716	<p>There are significant changes from 4.5 to 5.x regarding event fields that made them a resource. In particular, isReviewed, Closed, Hidden, Correlated, inCase, hasAction, and Forwarded have become derived fields of the EventAnnotationFlag. Therefore isReviewed can no longer be saved in a field set.</p> <p>Work around: Since isReviewed is derived from EventAnnotationFlag field, you can use EventAnnotationFlag in place of isReviewed.</p>

ArcSight Console

Issue	Description
ESM-49914	<p>If multiple users have a case open and one has it locked, the update made on the locked case won't appear for the users that have it open but unlocked.</p> <p>Now with the fix, when a user updates a Locked case the update will appear on cases that are opened by other users.</p>
ESM-49107	<p>A change in zone based filtering configuration performed via connector\bin\runagentsetup.sh is not updated when viewed in the ArcSight Console.</p> <p>Now with the fix, an update to zone-based filtering performed using agent setup at connector installation will appear in the ArcSight Console.</p>
ESM-47056	<p>The Data Monitor Editor allowed you to select both the Manager Receipt Time and End time for a data monitor despite these being mutually exclusive options.</p> <p>Now the data monitor only allows one Time Field; either End Time or Manager Receipt Time.</p>
ESM-38983 TTP#63604	<p>When attempting to copy text from a query viewer cell using Ctrl-c, the entire row is copied to the clipboard rather than the individual cell value.</p> <p>Now a copy menu has been added to the right click pop up of the table viewer. You can copy the selected cell (this is only for table viewer). Ctrl+c still copies the entire row.</p>

ArcSight Manager

Issue	Description
ESM-49853	<p>In ESM 5.0 SP2, when the case is linked with the events, and a user tries to get the case by ID or name, a nullpointer exception could be thrown.</p> <p>The issue has been fixed in 5.0 SP2 Patch3.</p>
ESM-48883	<p>When you ran a package uninstall in standalone mode, if the package contained a Pattern Discovery resource, the package uninstall failed.</p> <p>The issue has been fixed in ESM 5.0 SP2 Patch3.</p>

ArcSight Web

Issue	Description
ESM-46538	The ArcSight Web login banner will now show quotes as quotes instead of backslash characters.

General

Issue	Description
ESM-49903	<p>When a Source Manager was set up to forward correlated events to a Destination ESM Manager with a correct filter configuration setting, even though correlation events could be seen from the destination Manager, it was unable to retrieve the correlated base events associated with them in the ArcSight Web UI. Users would see "Event ID either does not exist or you don't have permission to view it" in the Rule Chain Users can perform this operation from the ArcSight Console</p> <p>This issue has been fixed in Patch 3.</p>
ESM-49882	<p>When you opened /All Active channels/Arcsight System/All Events/Last hour in ArcSight Web and ran the channel without modification, if you added an inline filter condition and applied it, it would not accept the filter condition.</p> <p>This issue has been fixed in Patch 3.</p>
ESM-49869	<p>When adding networks to a connector from the connector editor, if there were too many, adding another would give an "Unable to update connector" error.</p> <p>This issue has been fixed in Patch 3.</p>
ESM-49773	<p>In ESM 5.0.0, FIPS mode did not require the write permissions on cert8 and key3 files on the ESM console.</p> <p>Starting in ESM 5.0 SP1, if you put Read only permissions on those files you would receive this error when logon to the ArcSight Console:</p> <p>"The authentication failed. Please verify your credentials and try again."</p> <p>Customers use case is that the workstations are hardened so that all Console files are read-only. This behavior worked in 5.0 GA but does not work from ESM 5.0 SP1 and higher.</p> <p>This issue has been fixed in Patch 3.</p>
ESM-49645	<p>Rules in ESM are generating problematic correlation events. If the action of the rule is to generate correlation events conditioned "on first event," then the generated correlation events always have a start time of epoch GMT (they show up as 31 Dec 1969 18:00:00 CST).</p> <p>This issue has been fixed in Patch 3.</p>
ESM-49626	Connection time-out to e-mail acknowledgement host is now configurable.
ESM-49620	<p>You could not add more than 512 zones to one network.</p> <p>Now you can increase the maximum by adding two properties, both set to a value large enough to accommodate the number of zones you need in a network:</p> <p>In server.properties, add persist.resource.relationship.default.pagesize= In console.properties, add console.ui.maxResourcesIDS=</p>
ESM-49588	<p>Copy feature in the Event Inspector fails to copy to a clipboard.</p> <p>This issue has been fixed in Patch 3.</p>

Issue	Description
ESM-47533	<p>When a Source Manager was set up to forward correlated events to a Destination Manager with a correct filter configuration setting, even though correlation events could be seen from the destination Manager, it was unable to retrieve the correlated base events associated with them in the ArcSight Web UI. Users would see "Event ID either does not exist or you don't have permission to view it" in the Inspect/Edit panel. User can perform this operation from the ArcSight Console</p> <p>This issue has been fixed in Patch 3.</p>

Open Issues in this Patch

This release contains the following open issues. Use the workarounds, where available.

General

Issue	Description
ESM-49587	<p>After upgrading Oracle to 11.2.0.2 on Win 2008, you may get the below exception when starting PA.</p> <p>java.sql.SQLException: ORA-01005: null password given; logon denied</p> <p>The workaround is:</p> <p>Go to ARCSIGHT_DB_HOME\bin and execute "arcsight database pc" and restart the Partition Archiver.</p>
ESM-47237	<p>On AIX, reports will fail to run from ArcSight Web. However, you will be able to run reports on the ArcSight Console.</p>
ESM-34741 TTP#53754	<p>The Patch Uninstaller for Manager and Web does not remove the link on Unix and the shortcut on Windows.</p> <p>The workaround is to delete this link manually after uninstall is complete.</p>
ESM-32088 TTP#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\rollbacksp2p3.bat</p> <p>On Unix: <ARCSIGHT_HOME>/bin/rollbacksp2p3.sh</p>
ESM-31705 TTP#46995	<p>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.</p>

Installation and Upgrade

Issue	Description
ESM-48331	<p>On Macintosh platform only: If your Macintosh machine automatically updates the JVM to version 1.6.0_26, you could encounter a Console login failure, which throws the following exception: "com.arcsight.common.ArcSightException: Could not initialize SSL Client."</p> <p>The workaround is to copy the old cacerts file from the previous JVM installation to the most recent JVM location. Since Mac OS X does not keep the old copies of the JVM, it is a good idea to back up the current JVM in order to preserve the cacerts file. The cacerts file is located via the symbolic link: /System/Library/Java/JavaVirtualMachines/1.6.0_jdk/Contents/Home/lib/security, which points to /System/Library/Java/Support/CoreDeploy.bundle/Contents/Home/lib/security.</p> <p>If you don't have a backup of the cacert file please contact HP Customer Support.</p>

Issues Fixed in Patch 2

Analytics

Issue	Description
ESM-49108 ESM-49040	<p>When a rule that creates cases had to create too many, case processing could not keep up with the rate at which cases were being created, and case processing would slow down and almost stop.</p> <p>Now, case processing is better able to keep up and these case-processing slow-downs no longer occur.</p>

ArcSight Console

Issue	Description
ESM-49624	<p>With the latest version of the JVM, the v5.0 SP2 ESM console could not be launched on a MAC.</p> <p>That issue is fixed in this patch.</p>
ESM-49293	<p>If you deleted cases using the navigator, it asks you if you would like to remove it from this group only or delete the case itself. But similar functionality is not available from the Case channel. Case channel viewer deleted linked cases and the original case without warning.</p> <p>This has now been fixed.</p>
ESM-48275	<p>On the Console after viewing an ancillary file in the web viewer, if you click on an external URL then you cannot close the web viewer.</p>
ESM-48026	<p>Actor names and user IDs consisting entirely of numerals were displayed as numbers instead of strings and incorrectly had commas or periods added. Now such names and IDs are correctly displayed as strings with no additional characters.</p>
ESM-48017	<p>On the ArcSight Web console, If you were in an opened active channel, clicking on the Field Set drop-down menu and choosing Customize, did not work. Now it works correctly.</p>

Issue	Description
ESM-47797	<p>If not configured correctly, the Console is unable to display Chinese, Japanese, or Korean characters.</p> <p>On the ArcSight Console, go to Edit > Preferences > Global Options > Font and set the font to Arial Unicode MS. If that option does not appear, type it in manually.</p>
ESM-47789	<p>If you highlighted an event in an open channel and tried to generate a channel report, you would get a Java null-pointer exception when you tried to save it. This error no longer occurs.</p>
ESM-47528	<p>When creating a filter or adding filter conditions to a rule using CCE, there was an option in the comparison drop down called Correlated By. This option should not be displayed and has been removed.</p>
ESM-47340	<p>When a non-admin user tries to run a channel report from a channel, it could fail, even if they have access to the events. This is a configuration issue.</p> <p>To ensure that it works correctly:</p> <ol style="list-style-type: none"> 1. Log in as Admin and go to Users. 2. Right-click on a non-admin user group and select "Edit Access Control." 3. In the Edit window, select the "Resource" Tab. 4. Add the resource "All Report Templates/ArcSight System" and click OK.
ESM-46156	<p>In Console Mode (non-Windows platforms), a browser window would be opened unnecessarily at the end of the Manager upgrade process. This no longer occurs.</p>
ESM-30538 TTP#43347	<p>Previously, the Acknowledge button would be enabled, even if the notification was undeliverable. Now it is not enabled unless the notification is deliverable.</p>

ArcSight Database

Issue	Description
ESM-48351	<p>Previously, the database super user "SYS" password appeared in clear text within one of the Oracle installation logs.</p> <p>This log file is now automatically deleted after installation.</p>

ArcSight Manager

Issue	Description
ESM-49242	<p>Reports and Active Channels blanked the data in Device CustomString when it began with the "#" character.</p> <p>This is now fixed.</p>
ESM-49166	<p>Out of Memory could occur when processing a very large number of annotated events.</p> <p>This memory leak is now fixed.</p>
ESM-48509	<p>There was a Memory Leak that affected earlier versions of ESM v5.0 SP1.</p> <p>This was fixed in 50SP2P1.</p>
ESM-48498	<p>The Manager stopped processing events because of a race condition while evaluating a threat level formula.</p> <p>This was fixed in 50SP2P1.</p>

Issue	Description
ESM-48034	When an account with less than Admin privileges opened an active channel, the user could get the error "Invalid Combination of sortable fields. Please edit your channel to set new sortable fields." This has now been fixed.
ESM-47198	Previously, importing a CSV file through the Network Model tool would populate the name of assets with what was specified in the CSV, in 5.0 SP1 the name defaults to <hostname - ip>, regardless of what was specified. This is now fixed.
ESM-46694	If you created an event-based Active List, the field size in the list was not as large as the size of the same field in the event, which created errors. The field size in the active list is now the same size.
ESM-48972	Resolved the error handling for over-sized event columns to handle the following error: java.io.IOException: String length '-32761'
ESM-48726	There was a Memory Leak that affected ESM v5.0 SP1. This is now fixed.
ESM-48419	If an Active List was created with the "Allow Multi-Mappings" option enabled, and an entry expired, the activelist:104 event would be repeated every minute until manually clearing entries on the Active List. The activelist:104 event is no longer repeated.
ESM-48327	The ArcSight ESM server, which runs on TCP port 8443 and is based upon the Jetty application server, was vulnerable to a JSP source code disclosure vulnerability. The application server revealed the source code of JSP scripts by adding an encoded NULL-byte character (%00) at the end of the request. This is now fixed.
ESM-46953	An internal error was causing the Forwarding Connector connection to Logger to fail repeatedly with a loss of data. Now this error has been corrected and the connection is stable.
ESM-46307	ESM v5.0, patch 1 installation took a long time. Now performance has been optimized.
ESM-46306	ESM v5.0, patch 1 installation did not create logs. This patch creates logs for the manager component in <ARCSIGHT_HOME>/logs/patch/....

General

Issue	Description
ESM-48158	ArcSight Web Installation fails in FIPS suite B mode. This was fixed in 50SP2P1.
ESM-48130	The server.multizoneengineentrynode.trace property is obsolete and is no longer used, as of v5.0 SP2 P1. You can now go to FilterOptimizedXCPUDMPC MBean link and enable this tracing dynamically by invoking the toggleEnableTrace function.
ESM-48060	You could not sort a column in a channel if you did not have write permission to the Field Set. Sorting now works, even without write permission.

Issue	Description
ESM-47906 ESM-48142	When ESM is upgraded to 5.0, the column size of the event table is increased for several fields. However, other tables, such as the trends table, are not updated. This issue causes ORA-12899 errors when running the Manager. To fix the issue: On the ArcSight Manager host run the following command: <ARCSIGHT_HOME>/bin/arcsight checktrendcolumnsize

Localization

Issue	Description
ESM-49643	During setup, when the ESM manager was set to use 'Traditional Chinese/Taiwan' as the language, ESM 5.0 SP2 (fresh install or upgrade) would not start. This is now fixed.
ESM-48542	Japanese characters of report names were garbled on ArcSight Web. This is now fixed.
ESM-47542	There was a problem with encoding Cyrillic characters in actor names. These characters now display correctly through Console Actors and Actor Audit Events.
ESM-46796	Package import was failing in on Chinese operating systems. This is now fixed.
ESM-48362 ESM-47147 ESM-37144 TTP#59971	There was an issue displaying Chinese, Japanese, Korean (CJK), or Romanian characters in RTF and PDF reports. To generate PDF reports that properly display such characters, use the following procedure: 1. Configure the operating system and the Manager to support the Language you are using. 2. Make sure you have the Adobe Acrobat Reader 9 to view the PDF report. If the Manager is running on Linux, do the following: 1. Download ARIALUNI.TTF font from the Linux support site. 2. Go to the /usr/share/fonts/ directory and create a subdirectory called /aria. 3. Copy ARIALUNI.TTF to /usr/share/fonts/aria. 4. Make a backup of the <ARCSIGHT_HOME>/reports/sree.properties file. 5. Add this property to sree.properties: font.truetype.path=/usr/share/fonts/aria For any Console running on Unix, perform steps 1-3. For Solaris: 1. Download ARIALUNI.TTF font from the Solaris support site. 2. Copy ARIALUNI.TTF to /usr/X11/lib/X11/fonts/TrueType 3. Modify fonts.dir and fonts.scale under the above directory with this line: ARIALUNI.TTF -monotype-arial-regular-r-normal--0-0-0-0-p-0-iso8859-1 and increase the count number in the first line by one. 4. Make a backup of the <ARCSIGHT_HOME>/reports/sree.properties file. 5. Add this property to sree.properties: font.truetype.path=/usr/X11/lib/X11/fonts/TrueType/
Continued...	

Issue	Description
ESM-48362 ESM-47147 ESM-37144 TTP#59971 (continued)	<p>To generate a report in PDF format to display Chinese, Japanese, Korean (CJK), or Romanian characters:</p> <ol style="list-style-type: none"> 1. Log in to the ArcSight Console and open the report. 2. Find the template used by the report. 3. Edit the template and select Open in Designer. 4. Edit the fields that need to display these characters. 5. Set the fonts to Arial Unicode for the fields that display these characters 6. Save the template and click Apply. 7. Run the report with PDF format. 8. Open the generated report (using Adobe Acrobat Reader 9 for PDF) to see the Unicode characters. <p>To generate a report in RTF format to display Chinese, Japanese, Korean (CJK), or Romanian characters:</p> <ol style="list-style-type: none"> 1. Log in to the ArcSight Console. 2. Select Edit > Preferences > Global Options. 3. Set the font to Arial Unicode MS.

ArcSight Web

Issue	Description
ESM-48907	<p>In the ArcSight Web UI there was an error when browsing through "Active Channels" or "Dashboards" from the Home tab.</p> <p>This has now been fixed.</p>
ESM-47460	<p>When viewing a live channel, if you selected a correlation event or a base event and clicked Additional Details, there was an error.</p> <p>Additional Details now works properly.</p>
ESM-46752	<p>There is a limit of 500 cases that can be displayed in the ArcSight Web console. If more than 500 cases are created from the ArcSight Console, when you try to load the cases in ArcSight Web, there is warning message that appears on the top of the page.</p> <p>This is working as designed. If you have more than 500 cases, use the ArcSight Console and not the Web Console.</p>

Open and Closed Issues in ESM v5.0 SP2

For information about open and closed issues for ESM v5.0 SP2, see the release notes for that version.

