Patch Release Notes
ArcSight™ ESM

Version 4.5 SP3, Patch 2
Build 4.5.3.6152.2

December, 2010

Patch Release Notes ArcSight™ ESM ,
Version 4.5 SP3, Patch 2

Revision History

Date	Product Version	Description
12/29/10	ArcSight™ ESM Version 4.5, SP3, Patch 2	Release Notes for ArcSight™ ESM Version 4.5, SP3, Patch 2.

Release Notes template version: 2.0.0

ArcSight Customer Support

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

Contents

ArcSight ESM, Version 4.5 SP3, Patch 2

ESM Patch v4.5.3.6152.2

These release notes describe how to apply the v4.5 SP3, Patch 2 release of ArcSight ESM. Instructions are included for each component, as well as other information about recent changes and open and closed issues.

This patch is for ArcSight ESM v4.5 SP3 only. If you are seeking to set up a fully current ESM v4.5 SP3 installation, please install v4.5 SP3 first and refer to its own 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 October 2010
- Updates for geographical information and vulnerability mapping

Usage Notes

The Network Model Wizard gives an error message if an ampersand (&) appears in an asset name in an import CSV file, because "&" is not a supported character for an asset name. The workaround is to enter two new properties in the file <ARCSIGHT_CONSOLE_HOME>/current/config/console.properties:

1. `console.ui.tools.nmw.remove_invalid_char=[true/false]`

   This property enables the ability to switch out the & character when you set it to True.

2. `console.ui.tools.nmw.replace_invalid_char_with=_AMPERSAND_`

   This property specifies the character(s) to use instead. In this example it substitutes "_AMPERSAND_" for the &.

Geographical Information Update

This patch includes an update to the geographical information used in graphical displays. The update version is GeoIP-532_20101201.

Vulnerability Updates

This patch contains updated vulnerability mapping (December, 2010, Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 398 updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSSB
Enterasys Dragon IDS updated Faultline	CVE, Nessus, MSSB
Cisco Secure IDS S535 updated Faultline	CVE
McAfee Intrushield updated	Faultline, CVE
TippingPoing UnityOne DV8143 updated Faultline	Bugtraq, CVE, MSSB
Fortinet Fortigate updated	Bugtraq, MSSB
ISS SiteProtector Updated	Bugtrag, CVE, X-Force, MSSB
Symantec Endpoint Protection updated Faultline	Bugtraq, CVE, Nessus
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSKB, CERT, MSSB
FunkWerk (VarySys Technologies) PacketAlarm updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSKB, MSSB

Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM has been certified with the Oracle critical patch update (CPU) for October, 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 October 2010 Patch
Windows 32	p10084980_10204_Win32.zip
Windows 64 (AMD64-EM64T)	p10084982_10204_MSWIN-x86-64.zip
Linux 32	p9952272_10204_Linux-x86.zip
Linux x86-64	p9952272_10204_Linux-x86-64.zip
AIX	p9952272_10204_AIX5L.zip
Solaris 64	p9952272_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 October 2010
Linux 32	p6880880_102000_LINUX.zip

Platform	OPatch October 2010
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 SP3, Patch 2

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

Note the following points when installing Patch 2.

- In some Solaris environments, when upgrading the ESM Manager and also when installing the solution packages, these actions do not complete. This problem might occur if your Solaris system does not meet the minimum system requirements. See the *ESM v4.5 SP3 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 2

Each component has installation and rollback steps.

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

ArcSight ESM Database

This section describes how to install and uninstall ESM v4.5 SP3, Patch 2 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-4.5.3.xxxx.2-DB-Win.exe`
- `Patch-4.5.3.xxxx.2-DB-Solaris.bin`
- `Patch-4.5.3.xxxx.2-DB-AIX.bin`
- `Patch-4.5.3.xxxx.2-DB-Linux.bin`

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

- **On Windows**:

  Double-click `Patch-4.5.3.xxxx.2-DB-Win.exe`

- **On Solaris**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-DB-Solaris.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-DB-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-DB-AIX.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-DB-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-DB-Linux.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-DB-Linux.bin -i console
  ```

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing ArcSight Database `ARCSIGHT_HOME` for your v4.5 SP3 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 SP3 Patch2-> Uninstall ArcSight Database 4.5 SP3 Patch2

   - Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP3Patch2` 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_SP3Patch2
  ```

- Or, to uninstall in Console mode, run

  ```
  ./Uninstall_ArcSight_Database_4.5_SP3Patch2 -i console
  ```

- If you did not create a link, execute the following command from the Database's `ARCSIGHT_HOME/UninstallerDataSP3Patch2`.

  ```
  ./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 SP3, Patch 2 for ArcSight Manager.

To Install the Patch

- 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.

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-4.5.3.xxxx.2-Manager-Win.exe`
- `Patch-4.5.3.xxxx.2-Manager-Solaris.bin`
- `Patch-4.5.3.xxxx.2-Manager-AIX.bin`
- `Patch-4.5.3.xxxx.2-Manager-Linux.bin`

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

- **On Windows**:

  Double-click `Patch-4.5.3.xxxx.2-Manager-Win.exe`

- **On Solaris**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Manager-Solaris.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Manager-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Manager-AIX.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Manager-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Manager-Linux.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Manager-Linux.bin -i console
  ```

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP3 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 SP3 Patch2-> Uninstall ArcSight Manager 4.5 SP3 Patch 2

- Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP3Patch2` 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_SP3Patch2
  ```

- Or, to uninstall using Console mode, run:

  ```
  ./Uninstall_ArcSight_Manager_4.5_SP3Patch2 -i console
  ```

- If you did not create a link, execute the following command from the `ARCSIGHT_HOME\UninstallerDataSP3Patch2` 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 SP3, Patch 2 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 16.
- The ArcSight ESM Console is not supported on AIX. The following steps do not include information for installing a Console patch on AIX.

To Install 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-4.5.3.xxxx.2-Console-Win.exe`
- `Patch-4.5.3.xxxx.2-Console-Solaris.bin`
- `Patch-4.5.3.xxxx.2-Console-Linux.bin`

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

- **On Windows**:

  Double-click `Patch-4.5.3.xxxx.2-Console-Win.exe`

- **On Solaris**:

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

  ```
  ./Patch-4.5.3.xxxx.2-Console-Solaris.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Console-Solaris.bin -i console
  ```

- **On Linux**:

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

  ```
  ./Patch-4.5.3.xxxx.2-Console-Linux.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Console-Linux.bin -i console
  ```

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP3 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 SP3 Patch2-> Uninstall ArcSight Console 4.5 SP3 Patch 2
- Or, run the following from the Console's ARCSIGHT_HOME\current\UninstallerDataSP3Patch2 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_SP3Patch2`
- Or, to uninstall using Console mode, run:

  `./Uninstall_ArcSight_Console_4.5_SP3Patch2 -i console`
- If you did not create a link, execute the command from the Console's ARCSIGHT_HOME/current/UninstallerDataSP3Patch2 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 SP3, Patch 2 for ArcSight Web.

To Install the Patch

- 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.

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-4.5.3.xxxx.2-Web-Win.exe`
- `Patch-4.5.3.xxxx.2-Web-Solaris.bin`
- `Patch-4.5.3.xxxx.2-Web-AIX.bin`
- `Patch-4.5.3.xxxx.2-Web-Linux.bin`

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

- **On Windows**:

  Double-click `Patch-4.5.3.xxxx.2-Web-Win.exe`

- **On Solaris**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Web-Solaris.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Web-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Web-AIX.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Web-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command.

  ```
  ./Patch-4.5.3.xxxx.2-Web-Linux.bin
  ```

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

  ```
  ./Patch-4.5.3.xxxx.2-Web-Linux.bin -i console
  ```

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP3 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.

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 SP3 Patch2-> Uninstall ArcSight Web 4.5 SP3 Patch 2
- Or, run the following from the Web's `ARCSIGHT_HOME\UninstallerDataSP3Patch2` 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_SP3Patch2
  ```
- Or, to uninstall using Console mode, run:

  ```
  ./Uninstall_ArcSight_Web_4.5_SP3Patch2 -i console
  ```
- If you did not create a link, execute the command from the `ARCSIGHT_HOME/UninstallerDataSP3Patch2` 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

Note 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.

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 file `Patch-4.5.3.xxxx.2-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.

Tip The patch installer file (that shows as a **ZIP** file on the download site) downloads as `Patch-4.5.3.xxxx.2-Console-MacOSX.`**app** on the Mac. A single or double-click on this **APP** file launches the patch installer, depending on how you have set these options. There is no need to "extract" or "unzip" the file; it downloads as a **APP** file.

4 Launch the patch installer by double-clicking the `ArcSightConsolePatch` file.

5 Follow the steps on the patch install wizard, providing the information as prompted:

- Choose the location where you want to install the patch. Browse to the same the location of your existing `ARCSIGHT_HOME` for your v4.5 SP3 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.

Note 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_SP3Patch2` 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
ESM-41409 TTP#68666	The Time Difference in Minutes function failed when working with notification time stamps. This function now works correctly.
ESM-45716	If your Oracle instance is configured with an 8k block size, then, while importing some packages, the import process would abort with ERROR: ORA-01450. Now this error no longer occurs in that circumstance.
ESM-45845	For Table charts, if you set the Last State Data Monitor's History Function to Maximum, it displayed the most recent value instead of the Maximum value for the History Time Range. The Maximum function now correctly shows the maximum value for the time range.
ESM-45990	When a user selected Investigate on a field in a channel, the filter truncated trailing spaces. This prevented the filter from matching content. The filter no longer truncates training spaces.
ESM-46111	When you moved a sub-folder in the Real-time Rules folder, to another location within the Real-time Rules folder, the rules that were moved stopped firing. The rules are not disabled and there was no visual indicator that they would not fire. Now moving rules within the Real-time Rules folder does not prevent them from firing.
ESM-46504 ESM-46513	ESM was importing the case files out of order. This was causing a problem with the import. Now ESM imports the files in order of the time stamp in the file-name suffix, using a first-in first-out rule.
ESM-46602	Previously, under certain circumstances, the std.log files would fill with debug messages similar to the one shown below due to excessive logging. [<date/time>][ERROR][default.com.arcsight.server.monitor.MonitorEventSender$Sender$1][addMonitorEvent] java.lang.RuntimeException: ####### DUPLICATE MONITOR EVENT: /Monitor/DBTableSpace/Event at com.arcsight.server.monitor.MonitorEventSender$Sender$1.addMonitorEvent(MonitorEventSender.java:237)... Now the problem of logs filling with such messages is fixed.

ArcSight Console

Number	Description
ESM-37327 TTP#60469	While editing a Customer resource or Assets-Locations resource, one of the attributes seen is Country. The drop-down combo box list of countries is not in alphabetical order and includes regions. The country list now shows only countries and they are in alphabetical order.
ESM-41099 TTP#67989	The External Payload Viewer failed to launch correctly on a Linux Console. Now the Launch External Payload Viewer function works correctly on Linux.
ESM-41217 TTP#68190	Copy and paste operations did not work correctly for custom columns. Now the copy and paste works correctly for both cases: it pastes the display value of the custom column if its right-click field has been set to null, otherwise it pastes the same value as the right-click field value set for the custom column.
ESM-41674 TTP#69665	The mail notification message was sent out with a reference to the old product name "myArcSight," and an out-dated message. Now the mail notification message is updated as shown below: “You have received 100 notifications within 24 hours. This destination will temporarily be disabled to prevent flooding. Please visit the ArcSight notification page to view/acknowledge your notifications (if they need acknowledging). If you have not configured Acknowledgement of Notifications then you may contact Administrator to reconfigure notification thresholds.”
ESM-41680 TTP#69700	When importing a CSV file into an active list with field type "Resource Reference" the field always appeared blank. Now when you import a CSV file, the "Resource Reference" is properly populated. If in your active list you have two fields ipAddress and Zones with types address and resource reference, respectively, you need use following format for the import file: 1.2.3.4,"<Resource URI=""/All Zones/cn_zone"" ID=""M1lUr-isBABCDcP2o-fir1g==""/>" Note that you need to include the ID of the resource for the resource reference field. By design, if the ID is not included in the import value, it appears blank in the active list after import.
ESM-45549	In some Locales, custom report start and end times could not be saved correctly. Now report start and end times are saved correctly in all locales.

Correlation

Number	Description
ESM-46149	An active list entry expiration correlated event was showing IP address under deviceCustomStrin4 field instead of the MAC address. It is fixed in this release.

ArcSight Web

Number	Description
ESM-36135 TTP#57261	When starting the web component as a service, the information to the PATH of the log file was displayed incorrectly on the command shell and in the output file. Now this information is displayed correctly.

Known Issues in this Patch

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

Installation

Number	Description
ESM-31705 TTP#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.
ESM-32088 TTP#47996	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. This is because the preparatory step of backing up the files has already occurred. Workaround: If you encounter this situation, you can restore functionality of the base Console by running the following commands to restore the backup files. On Windows: <ARCSIGHT_HOME>\bin\rollbacksp3p2.bat On Unix: <ARCSIGHT_HOME>/bin/rollbacksp3p2.sh
ESM-34741 TTP#53754	The Patch Uninstaller for Manager and Web does not remove the link on Unix and the shortcut on Windows. The workaround is to delete this link manually after uninstall is complete.

Issues Fixed in Previous Patch

The following issues were addressed in patch 1.

ArcSight Manager

Number	Description
ESM-46001	There was an issue that the ESM Manager would run out of memory while opening multiple Active Channels. This issue is now fixed.

Number	Description
ESM-45993	When editing more than one scheduled job at a time, there were issues trying to save them. Now you can save multiple open scheduled jobs.
ESM-41682 TTP#69710	Users in Active Directory groups could not login to ESM when the group name had a space in it. Users can now login even if they are part of an Active Directory group whose name contains a space.
ESM-37471 TTP#60772	When running the “arcsight managerup” command on a FIPS ESM installation, it returned the following improper status even if the Manager was running: No XML RPC response received. Heartbeat received. This now returns a proper message whether the Manager is running or not.

ArcSight Console

Number	Description
ESM-41611 TTP#69402	When editing two reports, the following error occurred when applying changes to the jobs of one of the reports: “Frequency not set for task <Report Name> and will be removed.” You can now edit and save multiple reports.
ESM-41457 TTP#68831	While importing a large number of entries, console would run out of memory, the entries would not be imported, and no error message would appear. Also while importing entries, if one of the entries has more than 512 characters, the entry would not be imported and an exception would appear. Now, the console does not run out of memory while importing large number of entries. Entries with more than 512 characters are skipped, but they are listed in the console status message by the index number of the entry in the CSV file.
ESM-40563 TTP#66863	Requested URL File Name would not display correctly in reports. Now Requested URL File Names display correctly in reports.
ESM-38839 TTP#63318	In the console, Audit event channel:002 had its device event class id and device event category switched. It read: device event class id=/Active Channel/Empty device event category=channel:002 Now the values are placed correctly: device event class id=channel:002 device event category=/Active Channel/Empty
ESM-38502 TTP#62717	The "Is Null" and "Is Not Null" conditions did not work when querying on Request URL File Name field in Active Channels. Now, the "Is Null" and "Is Not Null" conditions work for querying RequestURL in Active Channels.
ESM-37061 TTP#59543	In some cases, text substitution for the $selectedItem place holder did not work correctly in the integration command. Now text substitution for $selecteditem works correctly.

Number	Description
ESM-36977 TTP#59253	Previously, Attacker Zone Resource and Target Zone Resource fields appeared in the CCE for a query on trend, if the trend had those fields. CCE does not support that type of field, so using them generated an error. Now, the fields do not appear in the CCE, even for a query on trend, where the trend contains those fields.
ESM-34742 TTP#53756	When setting up a data monitor bar or pie chart to monitor incoming events, the charts did not draw correctly if the incoming event rate was higher than 400 events per second. Charts now draw correctly when the incoming event rate is higher than 400 events per second.

Analytics

Number	Description
ESM-41510 TTP#69067	When editing the Zone Resource included with Arcsight Standard Content with the following Name: /All Zones/ArcSight System/Dark Address Space Zones/175.0.0.0-185.255.255.255 (IANA), the end address would show 185.55.255.255. Now the proper end address (185.255.255.255) shows when editing.
ESM-36376 TTP#57757	Some dashboards showed an epoch time in certain columns. Now all dashboards show time in a human-readable format.

Localization

Number	Description
ESM-41233 TTP#68233	The Network Model Wizard failed when the CSV file included non-English characters, The error was “Invalid archive: The value of attribute “uri” must not contain the '<' character." Now the Network Model Wizard works when importing non-English characters. However, UTF-8 is still the only format that is supported.

Known and Fixed Issues in ESM v4.5 SP3

For information about known and fixed issues for ESM v4.5 SP3, see the release notes for that version.