

Release Notes

ArcSight ESM 5.5 Patch 1

December 5, 2013



Copyright © 2013 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.hpenterprisesecurity.com/copyright>

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
12/5/2013	ArcSight ESM 5.5 Patch 1	ESM 5.5 Patch 1 Release Notes

Contents

ArcSight ESM Version 5.5 Patch 1	5
ESM 5.5.0 Patch 1, Build 7055	5
Purpose of this Patch	5
Usage Notes for this Patch	5
Section 508 Compliance	5
Geographical Information Update	5
Vulnerability Updates	6
Installing ESM Version 5.5 Patch 1	6
ArcSight Database	7
ArcSight Manager	10
ArcSight Console	12
ArcSight Web	15
Issues Fixed in this Patch	17
Analytics	17
ArcSight Console	17
ArcSight Database	18
ArcSight Manager	18
ArcSight Web	19
Open Issues in this Patch	19
ArcSight Console	19
Installation and Upgrade	20
Open and Closed Issues in ESM v5.5	20

ArcSight ESM Version 5.5 Patch 1

ESM 5.5.0 Patch 1, Build 7055

These release notes describe how to apply this patch 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 v5.5 only. If you are on an earlier version of ESM, refer to the release notes for v5.5 for information on upgrading. To set up a new ESM v5.5 installation, refer to the *ArcSight ESM Installation and Configuration Guide*. The build number for this patch is 7055.

After you have upgraded to v5.5, follow the instructions in ["Installing ESM Version 5.5 Patch 1" on page 6](#) of these release notes to apply Patch 1.

Refer to the latest *ArcSight Oracle Patch Set Update (PSU) Release Notes* for Oracle Patch Set Update (PSU) and OPatch information, available for download from <http://support.openview.hp.com>.

Purpose of this Patch

This patch:

- Addresses critical issues in ESM v5.5.
- Provides updates for vulnerability mapping.

Usage Notes for this Patch

Refer to *ArcSight™ ESM Release Notes Version 5.5*. The usage notes for that release also apply to this patch.

Section 508 Compliance

ArcSight recognizes the importance of accessibility as a product initiative. To that end, ArcSight 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_20131001.

Vulnerability Updates

This release includes recent vulnerability mappings (October, 2013 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 986 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, MSKB, CERT
Enterasys Dragon IDS updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S748 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2312 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, MSSB, CERT
TippingPoint UnityOne DV8483 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
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	CVE

Installing ESM Version 5.5 Patch 1

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

Keep the following points in mind when installing Patch 1:

- **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 or uninstalling the patch. Refer to the installation and uninstallation steps for the ["ArcSight Database" on page 7](#).
- 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 ArcSight 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, 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, 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>`).
- 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. If this happens, use one of the other uninstall options (page 9) to uninstall the patch.

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 Database

This section describes how to install and uninstall ESM v5.5 Patch 1 for the 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 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 Linux:

As root user, 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 that folder as the Oracle database owner on 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` is the build number shown in [ESM 5.5.0 Patch 1, Build 7055](#).

- ◆ `Patch-5.5.0.xxxx.1-DB-Win.exe`

◆ Patch-5.5.0.xxxx.1-DB-Linux.bin

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

◆ **On Windows:**

Run Patch-5.5.0.xxxx.1-DB-Win.exe

◆ **On Linux:**

Run the following command:

```
./Patch-5.5.0.xxxx.1-DB-Linux.bin
```

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

```
./Patch-5.5.0.xxxx.1-DB-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and select **Next**.
- 6 Accept the terms of the license agreement and select **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 v5.5 database installation in the text box provided, or navigate to the location by selecting **Choose...**
- 8 To restore the installer-provided default location, select **Restore Default Folder**.
- 9 Select **Next**.
- 10 Choose a Link Location on Linux or Shortcut location on Windows by selecting the appropriate radio button, and then select **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 Select **Install**.
- 13 Select **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 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 Select **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 select **Next**.
- 4 Select **Finish** in the last screen.
- 5 **On Windows Only:** Select **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 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 ArcSight Partition Archiver.

2 Run the uninstaller program:

Windows:

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

Start > All Programs > ArcSight DB 5.5 Patch 1 > Uninstall ArcSight Database 5.5 Patch 1

- ◆ Or, run the following from the <ARCSIGHT_HOME>\UninstallerData5.5.0.1 directory:

```
Uninstall_ArcSight_DB_Patch.exe
```

Linux:

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

```
./Uninstall_ArcSight_Database5.5.0.1
```
- ◆ Or, to uninstall in Console mode, run:

```
./Uninstall_ArcSight_Database5.5.0.1 -i console
```
- ◆ If you did not create a link, execute the following command from the Database's <ARCSIGHT_HOME>/UninstallerData5.5.0.1

```
./Uninstall_ArcSight_DB_Patch
```

3 Select **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 Select **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 select **Next**.
- 6 Select **Finish** in the last screen.
- 7 **For Windows Only**, select **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`).

◆ **Linux:**

Run the following command:

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



Note

`arc_oraclepartitionarchiver_db` is the default service name.

ArcSight Manager

This section describes how to install or uninstall v5.5 Patch 1 for ArcSight Manager.

To Install the Patch



Note

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

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



Caution

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 shown in [ESM 5.5.0 Patch 1, Build 7055](#).

- ◆ `Patch-5.5.0.xxxx.1-Manager-Win.exe`
- ◆ `Patch-5.5.0.xxxx.1-Manager-Linux.bin`

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

◆ **Windows:**

Run `Patch-5.5.0.xxxx.1-Manager-Win.exe`

◆ **Linux:**

Run the following command:

`./Patch-5.5.0.xxxx.1-Manager-Linux.bin`

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

`./Patch-5.5.0.xxxx.1-Manager-Linux.bin -i console`

The installer launches the Introduction window.

- 5 Read the instructions provided and select **Next**.
- 6 Accept the terms of the license agreement and select **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 v5.5 Manager installation in the text box provided or navigate to the location by selecting **Choose...**

If you want to restore the installer-provided default location, select **Restore Default Folder**.
- 8 Select **Next**.
- 9 Choose a Link Location on Linux or a Shortcut location on Windows by selecting the appropriate radio button, then select **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 Select **Install**.
- 12 Select **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:

Windows:
 - ◆ Select the icon you created for the uninstaller when installing the Manager. For example, if you created an uninstaller icon on your desktop, Select that icon.
 - ◆ Or, if you created a link in the Start menu, select
Start > All Programs > ArcSight Manager 5.5 Patch 1 > Uninstall ArcSight Manager 5.5 Patch 1

- ◆ Or, run the following from the Manager's
<ARCSIGHT_HOME>\UninstallerData5.5.0.1 directory:
`Uninstall_ArcSight_Manager_Patch.exe`

Linux:

- ◆ From the directory where you created the links when installing the Manager (your home folder or some other location), run:
`./Uninstall_ArcSight_Manager5.5.0.1`
- ◆ Or, to uninstall using Console mode, run:
`./Uninstall_ArcSight_Manager5.5.0.1 -i console`
- ◆ If you did not create a link, execute the following command from the Manager's
<ARCSIGHT_HOME>/UninstallerData5.5.0.1 directory:
`./Uninstall_ArcSight_Manager_Patch`

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

ArcSight Console

This section describes how to install or uninstall the v5.5 Patch 1 for ArcSight Console on Windows, Mac, and Linux platforms.

To Install the Patch

**Note**

- 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.

- 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.

**Caution**

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

- 3 Download the executable file specific to your platform from the HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, xxxx represents the build number shown in [ESM 5.5.0 Patch 1, Build 7055](#).
 - ◆ Patch-5.5.0.xxxx.1-Console-Win.exe
 - ◆ Patch-5.5.0.xxxx.1-Console-Linux.bin

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

- ◆ **On Windows:**

Run `Patch-5.5.0.xxxx.1-Console-Win.exe`

- ◆ **On Linux:**

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

`./Patch-5.5.0.xxxx.1-Console-Linux.bin`

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

`./Patch-5.5.0.xxxx.1-Console-Linux.bin -i console`

The installer launches the Introduction window.

- 5 Read the instructions provided and select **Next**.
- 6 Accept the terms of the license agreement and select **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 v5.5 Console installation in the text box provided or navigate to the location by selecting **Choose...**

If you want to restore the installer-provided default location, select **Restore Default Folder**.
- 8 Select **Next**.
- 9 Choose a Link Location on Linux or Shortcut location on Windows by selecting the appropriate radio button and select **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 Select **Install**.
- 12 Select **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-5.5.0.xxxx.1-Console-MacOSX.zip` to anywhere on your system. (xxxx is the build number.)



The patch installer file (that shows as a **ZIP** file on the download site) downloads as `Patch-5.5.0.xxxx.1-Console-MacOSX.app` on the Mac. 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 running the `ArcSightConsolePatch1` file.

- 5 Follow the steps on the patch install wizard, providing the information as prompted:
 - ◆ Accept the terms of the license agreement and select **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 Select **Next**.
- 7 Verify your settings and select **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 uninstaller program:

On Windows:

- ◆ Select the icon you created for the uninstaller when installing the Console. For example, if you created an uninstaller icon on your desktop, select that icon.
- ◆ If you created a link in the Start menu, select:

Start > All Programs > ArcSight Console 5.5 Patch 1 > Uninstall ArcSight Console 5.5 Patch 1

- ◆ Or, run the following from the Console's `<ARCSIGHT_HOME>\current\UninstallerData5.5.0.1` directory:
`Uninstall_ArcSight_Console_Patch.exe`

On Linux:

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

```
./Uninstall_ArcSight_ESM_Console5.5.0.1
```

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

```
./Uninstall_ArcSight_ESM_Console5.5.0.1 -i console
```

- ◆ If you did not create a link, execute the command from the Console's `<ARCSIGHT_HOME>/current/UninstallerData5.5.0.1` directory:
`./Uninstall_ArcSight_Console_Patch`

On a Mac:

- ◆ From the directory where you created the links when installing the Console, run:

```
Uninstall_ArcSight_ESM_Console_5.5.0.1
```

- ◆ From the Console's
<ARCSIGHT_HOME>/current/UninstallerData5.5.0.1 directory, run:
Uninstall_ArcSight_Console_Patch

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

ArcSight Web

This section describes how to install or uninstall ESM v5.5 Patch 1 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.
 - 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 HP Software Support Online site (<http://support.openview.hp.com>). In the following file names, xxxx represents the build number shown in **ESM 5.5.0 Patch 1, Build 7055**.

- ◆ Patch-5.5.0.xxxx.1-Web-Win.exe
- ◆ Patch-5.5.0.xxxx.1-Web-Linux.bin

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

- ◆ **On Windows:**

Run Patch-5.5.0.xxxx.1-Web-Win.exe

- ◆ **On Linux:**

Run the following command:

```
./Patch-5.5.0.xxxx.1-Web-Linux.bin
```

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

```
./Patch-5.5.0.xxxx.1-Web-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and select **Next**.
- 6 Accept the terms of the license agreement and select **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 v5.5 ArcSight Web installation in the text box provided or navigate to the location by selecting **Choose...**

To restore the installer-provided default location, select **Restore Default Folder**.
- 8** Select **Next**.
- 9** Choose a Link Location on Linux or Shortcut location on Windows by selecting the appropriate radio button, then select **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** Select **Install**.
- 12** Select **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> 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:

- ◆ Select the icon you created for the uninstaller when installing the ArcSight Web. For example, if you created an uninstaller icon on your desktop, select that icon.
- ◆ Or, if you created a link in the Start menu, select:

Start > All Programs > ArcSight Web 5.5 Patch 1 > Uninstall ArcSight Web 5.5 Patch 1

- ◆ Or, run the following from the Web's <ARCSIGHT_HOME>\UninstallerData5.5.0.1 directory:
`Uninstall_ArcSight_Web_Patch.exe`

Linux:

- ◆ From the directory where you created the links when installing the ArcSight Web (in your home directory or another location), run:
`./Uninstall_ArcSight_Web5.5.0.1`
- ◆ Or, to uninstall using Console mode, run:
`./Uninstall_ArcSight_Web5.5.0.1 -i console`
- ◆ If you did not create a link, execute the command from ArcSight Web's <ARCSIGHT_HOME>/UninstallerData5.5.0.1 directory:
`./Uninstall_ArcSight_Web_Patch`

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

Issues Fixed in this Patch

The following issues are fixed in this patch.

Analytics

Issue	Description
ESM-51187	A trend would fail to run if the trend query contained a custom conditional evaluation. This issue is now fixed.
ESM-51143	Translation performed by the console for GetDayOfWeek was not being performed in the same way on the Manager. It works fine after the Active List mapping is set as 1 to 7 (1 as Sunday) as expected. This issue is now fixed.
ESM-47280	There was no way to automatically set the initial stage value of a case upon creation by a rule. Now, there is a rule action Add to Case and creating a new case has the option to set the case's stage.

ArcSight Console

Issue	Description
ESM-51245	When user login to ArcSight Console that runs on Mac OS, the "Starting Console" screen remains even though Console is fully loaded. This issue is now fixed.
ESM-51188	In the ArcSight Console advanced editor, if you created a rule in which a FlexString was set in the action, and used a string containing line breaks, the line breaks would be deleted, even if you set "Multi-line Input." Line breaks are now correctly preserved.
ESM-51104	The last field you changed in the case editor would be cleared when you switched tabs. Now all field entries are properly preserved when you switch tabs.
ESM-50749	188.125.82.157 was incorrectly mapped to Iran instead of to Ireland. This is now fixed.
ESM-50673	In the case editor, changes a user made to the text, such as adding more text or deleting existing text in some tabs, were lost after the user switched tabs without selecting the Apply button. This issue is now fixed and user can switch tabs in the case editor without losing the modifications.
ESM-50440	If you created a query by using the Assets subtab to add an assets condition, the query became uneditable and created a null pointer exception. Now you can use the Assets subtab and the query remains editable.
ESM-50398	The last field you changed in the case editor would be cleared when you switched tabs. Now all field entries are properly preserved when you switch tabs.

Issue	Description
ESM-47637	<p>There was a request to add enhancements to make it easier to parse data from an event in pipe-delimited format by making it possible to determine the delimiter and the a value's position in the array.</p> <p>In ESM 5.5 there were two additions that fixed this:</p> <p>ConvertStringToList (new delimiter parameter)</p> <p>GetListElement (new function)</p>
ESM-33294	<p>Previously, there was no way to clear, delete, or remove informational notifications displayed on the Informational tab of the Console's Notifications panel. This issue is now fixed. The Informational tab has a Delete button. To delete informational notifications, select the Notifications icon on the Console toolbar, select the Informational subtab, select the informational notification you want to delete, and select the Delete button. Then confirm the deletion.</p>

ArcSight Database

Issue	Description
ESM-51265	<p>There was an issue with running export_system_tables command on windows. This issue is fixed with 5.5 patch1. Prior to running export_system_tables install 5.5 patch1</p>
ESM-51094	<p>Under some circumstances Trend Partitions were failing.</p> <p>Now Trends are partitioned correctly.</p>
ESM-50465	<p>When the database returned to a normal state the subsystem status change message used the word "Error."</p> <p>Now it uses "OK" when the database returns to a normal state.</p>
ESM-50007	<p>During the archive process on windows the dbf files failed to zip with an unknown exception type.</p> <p>Now these files zip correctly.</p> <p>Compression level can be updated in database.properties by adding partition.archiver.compression.level property with values 1 through 10</p>

ArcSight Manager

Issue	Description
ESM-51210	<p>This was an error that would pop up for the user. When the case channel with a filter containing a date/time field was used, and a new case or an existing case was updated that had the same date/time field set, this exception was thrown.</p> <p>On fixing this issue, the error popup no longer shows up and the user can create new cases or edit existing ones with date/time fields.</p>
ESM-51186	<p>IdentityView 2.5 did not install correctly when log.global.debug property was set to true in manager server.properties file.</p> <p>Now it installs correctly when debug property is set to true.</p>
ESM-50564	<p>Under some circumstances, when the size of the active lists exceeded the defined capacity and the active list was continuously being updated, the event processing could stop and the ESM Manager could become unstable. Now, when the active list grows too large it does not stop event processing, even if the list is being continuously updated</p>

Issue	Description
ESM-50386	Event aggregation set for a number of matches within a time frame would also include matches outside that time frame, Now only matches within the specified time frame are aggregated.
ESM-49794	System automatically deactivates any user account that has been inactive for more than 90 days. This behavior is documented in the "Managing Users and Permissions" topic of the ArcSight Console User's Guide.
ESM-49508	When logging in to the ArcSight Console, you could get an error related to logging in to core services. This issue is now fixed.

ArcSight Web

Issue	Description
ESM-49930 ESM-51258 ESM-51257	Web page headers were cached by proxy servers and web browsers, allowing for exposure of sensitive information. Now these headers are not cached.
ESM-50371	ArcSight Web exposed a scripting vulnerability. Now, the web server version has been updated and the issue is fixed.

Open Issues in this Patch

This release contains the following open issues.

ArcSight Console

Issue	Description
ESM-50790	If you are defining a query for a case and you want to specify the case owner with the owner's name, enter the resource ID of the owner's name instead of the name. If you use the name, you will get an error when you run the query. For example: if Owner=admin, this will not work. if Owner=1UOtZMTkBABCA0qd7zsU1IQ, this will work. You can get the resource ID by viewing the user resource's attributes on the Edit/Panel of the ArcSight Console. Query condition with case owner name is not supported. User can select a query condition with owner ID instead.

Installation and Upgrade

Issue	Description
ESM-34741	<p>The Patch Uninstaller for the Manager and ArcSight Web does not remove the link on UNIX and the shortcut on Windows.</p> <p>If you uninstall the patch and the link or shortcut is not removed, remove it manually.</p>

Open and Closed Issues in ESM v5.5

For information about open and closed issues for ESM v5.5, see the release notes for that version.