Patch Release Notes
ArcSight™ ESM

Version 5.0, SP1 Patch 3
Build 5.0.1.6666.3

June 10, 2011

Patch Release Notes ArcSight™ ESM ,
Version 5.0, SP1 Patch 3

Revision History

Date	Product Version	Description
06/10/11	ArcSight™ ESM Version 5.0, SP1 Patch 3	Created

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://forum.arcsight.com

Contents

ArcSight ESM, Version 5.0 SP1 Patch 3

ESM Patch 5.0.1.6666.3

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 v5.0 SP1 only. If you are seeking to set up a new ESM v5.0 SP1 installation, refer to the *ArcSight ESM Installation and Configuration Guide*.

For instructions on upgrading from v4.5 SP1, SP2 to v5.0 SP1, first see the upgrade guide *Upgrading ArcSight™ ESM; v4.5 SP1 or v4.5 SP2 to v5.0 GA*.
Then see *Upgrading ArcSight™ ESM; v5.0 to v5.0 SP1*.

After you have upgraded to v5.0 SP1, follow the instructions in "Installing ESM Version 5.0 SP1 Patch 3" on page 12 of these release notes to apply Patch 3.

Purpose of this Patch

This patch:

- Provides JRE update CVE-2010-4476
- Addresses customer reported and other issues in ESM v5.0 SP1
- Provides updates for geographical information and vulnerability mapping

Usage Notes

Logger Search Integration Authentication

Note the following Logger integration authentication change with this patch:

If you also have ArcSight Logger 4.0 or later, you can perform a Logger search directly from your ESM Console using ESM integration commands. ESM v5.0 SP1 Patch 2 introduced a "One Time Password" (OTP) option that work in Logger 5.1.

If you are using an earlier version of Logger, continue to use the LoggerUser and LoggerPassword as before for searches. Until you install Logger 5.1, searches display a message that it failed to negotiate a single-use session token and is proceeding with regular authentication. Just click **OK** to continue.

System Table Import and Export - Oracle 11g

The Oracle 11g import and export utilities require a different mechanism for generating the system table dump file (`ArcSight.dmp`). Therefore the dump file generated with this patch is not compatible with the dump files generated with earlier releases.

On Linux, importing system tables in 11g (11.2.0.2) fails with errors, even though the export dump is valid. ESM v5.0 SP1 Patch 3 fixes this with no additional patches.

On Windows, exporting system tables in Oracle 11g (11.2.0.1) only partially succeeds. The export fails to export empty tables and generates many [ORA-00942: table or view does not exist] errors. ESM v5.0 SP1 Patch 3 fixes this. However, for Windows, with Oracle 11g (11.2.0.1), an Oracle patch is required to enable this fix to work. Otherwise, go to Step 10.

If you are on Windows and Oracle 11g, use the following Oracle patch procedure:

1. Visit the ArcSight Customer Support product-download site to get the Oracle patch: `p8795792_112010_Generic.zip`
2. Extract the contents of the Patch zip file
3. Review the `README.txt` file in the Patch zip archive.
4. Stop the ArcSight Manager, Partition Archiver, Oracle instance, and TNS Listener.
5. Set the Patch binary in PATH.
6. Install the patch that you downloaded in Step 1 according to the steps outlined in the `README.txt` file in the zip package.
7. Replace references to "OPatch" in the commands with `$ARCSIGHT_HOME/bin/arcdbutil patch`

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

   For example, if the `README.txt` file says:

   ```
   >OPatch apply
   ```

   Then use this command instead:

   ```
   $ARCSIGHT_HOME/bin/arcdbutil patch apply
   ```
8. Follow the "Post Installation Instructions…" steps in the `README.txt` file.
9. Restart the database, TNS Listener, Partition Archiver, and ArcSight Manager.
10. Use the `import_system_tables` and `export_system_tables` utilities as outlined in the following examples. For additional information see the *ESM Administrator's Guide* for ESM 5.0 SP1.

    ```
    $ARCSIGHT_HOME/bin/arcsight export_system_tables
    <username>/<password>@<TNSName>
    ```

    Export places `arcsight.dmp` in `<ARCSIGHT_HOME>`. Make sure it is still there before doing an import (for example, if you moved it or obtained another one).

    ```
    $ARCSIGHT_HOME/bin/arcsight import_system_tables
    <export_username> <import_username> <import_password> <TNSname>
    <dump_file_name>
    ```

    where `<dump_file_name>` is `arcsight.dmp` file.

System Table Export - Oracle 10g

When you ran the ArcSight export_system_tables script, you might have received the following error:

Error "ORA-39071: Value for TABLES is badly formed."

This is due to an Oracle issue with the `expdp` command of Oracle v10.2.0.4. With this bug, a 10.2.0.4 `datapump` export using transportable tablespaces with a long list of tablespaces fails with ORA-39071 [ID 1131484.1]. To fix the error, set the compatible parameter on the database to 10.2.0.4.

This fix requires you to schedule a database outage and restart the database.

To fix the error, set the compatible parameter on the database to 10.2.0.4.

1. Log in to your database server as an Oracle Software Owner.
2. Navigate to `<ARCSIGHT_HOME>/db/bin` and sqlplus as sysdba.
3. Execute the following SQL statements:

```
alter system set compatible = '10.2.0.4' scope=spfile;
shutdown immediate;
startup;
```

4. To check if the parameter has been set as required, execute the following statement on the SQL prompt:

```
show parameter compatible
```

Example:

```
SQL> show parameter compatible

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
compatible                           string      10.2.0.4
```

5. Restart the database.

To track the progress on this bug, ArcSight has also filed internal bug ESM-47738.

Fixing Misconfigured Connector Severity Filters

If you edited severity filters for a specific Connector from the Console, it might have affected the other un-edited severity filters for that Connector. Because of this, the agent-severity for all events coming from that Connector was set to "very-high."

This issue is fixed in Patch 3, but leaves already-affected severity filters misconfigured. To fix them, manually set the "severity filters" condition to false if you do not intend to use Connector Severity Filters, or modify them to be correct if you do use them.

After you install ESM v5.0 SP1 Patch 3, you can identify misconfigured filters as follows: go to **https://localhost:8443/arcsight/web/manage.jsp > AgentStateTracker**, and look at the **AgentsFilters** table to identify misconfigured Connectors (localhost or IP address, depending on how you registered your Manager). The new Discrepancy column

for a Connector states the reason why a Connector Filter is misconfigured. For this issue, it says "This filter condition is set to True." An empty column indicates that the connector severity filter is not misconfigured.

Section 508 Compliance

ArcSight recognizes the importance and relevance 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_20110301.

Vulnerability Updates

This release includes recent vulnerability mappings (March 2011 Context Update) for these devices:

Device	Vulnerability Updates
Snort Sourcefire SEU 429	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Enterasys Dragon IDS	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
Cisco Secure IDS S552	Faultline, Bugtraq, CVE, Nessus, MSSB
Juniper / Netscreen IDP update 1878	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, CERT, MSSB
TippingPoint UnityOne DV8178	Faultline, Bugtraq, CVE, MSSB
Fortinet Fortigate	Faultline, Bugtraq, MSSB
IBM/ISS SiteProtector	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB, CERT
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, Nessus
McAfee HIPS 7.0	Faultline, CVE
Radware DefensePro	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
FunkWerk (VarySys Technologies) PacketAlarm	Arachnids, Faultline, Bugtraq, CVE, Nessus, MSSB, MSKB, CERT

Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM is certified with the Oracle critical patch update (CPU) for January, 2011. Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment

Oracle 10.2.0.4

Certification has been established with Oracle 10.2.0.4.

Platform	CPU January 2011 Patch for 10.2.0.4
Windows 32	p10349197_10204_Win32.zip
Windows 64 (AMD64-EM64T)	p10349200_10204_MSWIN-x86-64.zip
Linux 32	p10249540_10204_Linux-x86.zip
Linux x86-64	p10249540_10204_Linux-x86-64.zip
AIX	p10249540_10204_AIX5L.zip
Solaris 64	p10249540_10204_Solaris-64.zip

This is the OPatch for 10.2.0.4.

Platform	OPatch January 2011 for 10.2.0.4
Linux 32	p6880880_102000_LINUX.zip
Linux x86-64	p6880880_102000_Linux-x86-64.zip
Solaris 64	p6880880_102000_SOLARIS64.zip
Windows 64 (AMD64-EM64T)	p6880880_102000_MSWIN-x86-64.zip
Windows 32	p6880880_102000_WINNT.zip
AIX	p6880880_102000_AIX64-5L.zip

Oracle 11.2.0.1

Certification has been established with Oracle 11.2.0.1.

Platform	CPU January 2011 Patch for 11.2.0.1
Windows 32	p10432044_112010_WINNT.zip
Windows 64 (AMD64-EM64T)	p10432045_112010_MSWIN-x86-64.zip

This is the OPatch for 11.2.0.1.

Platform	OPatch January 2011 for 11.2.0.1
Windows 64 (AMD64-EM64T)	p6880880_112000_MSWIN-x86-64.zip
Windows 32	p6880880_112000_WINNT.zip

To Apply 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 it under your working directory.
   - Download the Oracle 10g or 11g 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 `$ORACLE_HOME`.
3. Stop the ArcSight Manager and Partition Archiver, and also stop the Oracle instance and TNS Listener.
4. Set the OPatch binary in PATH.
5. Read the next section in this document, "Workarounds for Known Issues in Oracle CPU" on page 11.
6. Install the CPU (that you downloaded in Step 1) according to the steps outlined in the `README` in the CPU zip package for your platform.
7. Replace references to "OPatch" in the commands with `$ARCSIGHT_HOME/bin/arcdbutil patch`

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

   For example,

   On Windows:

   If the `README` says:

   ```
   >OPatch apply
   ```

   Then use this command instead:

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

   On UNIX:

   If the `README` says:

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

   Then use this command instead:

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

   

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

8. Follow the "Post Installation Instructions…" steps in the `README`.
9. Restart the database, TNS Listener, Partition Archiver, and ArcSight Manager.

Workarounds for Known Issues in Oracle CPU

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

Windows for Oracle 10g

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

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

OPatch failed with error code 115
```

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

Linux - Using a Large Instance

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

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

```
cd $ORACLE_HOME/rdbms/lib

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

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


make -f ins_rdbms.mk ksms.o

make -f ins_rdbms.mk ioracle
```

4. Restart the database server and the TNS Listener.

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

Installing ESM Version 5.0 SP1 Patch 3

You can install this patch release using the platform-specific and component-specific executable files provided. Patch installers are available for all 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.
- 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 13.
- **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.
- 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 (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 SP1, Patch 3 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-5.0.1.xxxx.3-DB-Win.exe`
- `Patch-5.0.1.xxxx.3-DB-Solaris.bin`
- `Patch-5.0.1.xxxx.3-DB-AIX.bin`
- `Patch-5.0.1.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-5.0.1.xxxx.3-DB-Win.exe`

- **On Solaris**:

  Run the following command:

```
./Patch-5.0.1.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-5.0.1.xxxx.3-DB-Solaris.bin -i console
```

- **On AIX**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.xxxx.3-DB-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.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 SP1 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** 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. 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 5.0 SP1 Patch 3 > Uninstall ArcSight Database 5.0 SP1 Patch 3

- Or, run the following from the `ARCSIGHT_HOME\UninstallerDataSP1Patch3` 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_5.0_SP1Patch3
  ```

- Or, to uninstall in Console mode, run:

  ```
  ./Uninstall_ArcSight_Database_5.0_SP1Patch3 -i console
  ```

- If you did not create a link, execute the following command from the Database's `ARCSIGHT_HOME/UninstallerDataSP1Patch3`:

```
./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 v5.0 SP1, Patch 3 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-5.0.1.xxxx.3-Manager-Win.exe`
- `Patch-5.0.1.xxxx.3-Manager-Solaris.bin`
- `Patch-5.0.1.xxxx.3-Manager-AIX.bin`
- `Patch-5.0.1.xxxx.3-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-5.0.1.xxxx.3-Manager-Win.exe`

- **On Solaris**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.xxxx.3-Manager-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.xxxx.3-Manager-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.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 SP1 Manager installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer-provided default location, click **Restore Default Folder**.

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 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 5.0 SP1 Patch 3 > Uninstall ArcSight Manager 5.0 SP1 Patch 3

- Or, run the following from the ARCSIGHT_HOME\UninstallerDataSP1Patch3 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_5.0_SP1Patch3

- Or, to uninstall using Console mode, run:

  ./Uninstall_ArcSight_Manager_5.0_SP1Patch3 -i console

- If you did not create a link, execute the following command from the ARCSIGHT_HOME\UninstallerDataSP1Patch3 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 SP1, Patch 3 for ArcSight Console on Windows, Mac, Solaris, and Linux platforms.

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-5.0.1.xxxx.3-Console-Win.exe`
   - `Patch-5.0.1.xxxx.3-Console-Solaris.bin`
   - `Patch-5.0.1.xxxx.3-Console-Linux.bin`
4. Run one of the following executables specific to your platform:
   - **On Windows**:

     Double-click `Patch-5.0.1.xxxx.3-Console-Win.exe`
   - **On Solaris**:

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

     ```
     ./Patch-5.0.1.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-5.0.1.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-5.0.1.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-5.0.1.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` for your v5.0 SP1 Console installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer-provided default location, click **Restore Default Folder**.

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 Delete the existing Console directory after you have made a copy elsewhere. (Essentially, this uninstalls the Console.)

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.

4 Download the file `Patch-5.0.1.xxxx.3-Console-MacOSX.zip` (where `xxxx` represents the build number) into the directory in which the Console is installed (for example, `/home/arcsight/console/current`). Use the number that matches the specific patch number at the top of this document.

The patch installer file (that shows as a **ZIP** file on the download site) downloads as `Patch-5.0.1.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.

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

6 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 the same the location of your existing `ARCSIGHT_HOME` for your v5.0 SP1 Console installation.
- Choose an alias location for the Console application (or opt to not use aliases). This is the same as a link location on UNIX systems or shortcut location on Windows systems.

7 Click **Next**.

8 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 > ArcSight Console 5.0 SP1 Patch 3 > Uninstall ArcSight Console 5.0 SP1 Patch 3

- Or, run the following from the Console's `ARCSIGHT_HOME\current\UninstallerDataSP1Patch3` 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_SP1Patch3
  ```

- Or, to uninstall using Console mode, run:

  ```
  ./Uninstall_ArcSight_Console_5.0_SP1Patch3 -i console
  ```

- If you did not create a link, execute the command from the Console's `ARCSIGHT_HOME/current/UninstallerDataSP1Patch3` 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_SP1Patch3
  ```

- From the Console's `ARCSIGHT_HOME/current/UninstallerDataSP1Patch3` directory, run:

  `Uninstall_ArcSight_Console_5.0_SP1Patch3`

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

ArcSight Web Server

This section describes how to install or uninstall ESM v5.0 SP1, Patch 3 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-5.0.1.xxxx.3-Web-Win.exe`
- `Patch-5.0.1.xxxx.3-Web-Solaris.bin`
- `Patch-5.0.1.xxxx.3-Web-AIX.bin`
- `Patch-5.0.1.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-5.0.1.xxxx.3-Web-Win.exe`

- **On Solaris**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.xxxx.3-Web-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.xxxx.3-Web-AIX.bin -i console
```

- **On Linux**:

  Run the following command:

  ```
  ./Patch-5.0.1.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-5.0.1.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` for your v5.0 SP1 ArcSight Web installation in the text box provided or navigate to the location by clicking **Choose...**

   If you want to restore the installer-provided default location, click **Restore Default Folder**.
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 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 5.0 SP1 Patch 3 > Uninstall ArcSight Web 5.0 SP1 Patch 3

- Or, run the following from the Web's `ARCSIGHT_HOME\UninstallerDataSP1Patch3` 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_5.0_SP1Patch3`

- Or, to uninstall using Console mode, run:

  `./Uninstall_ArcSight_Web_5.0_SP1Patch3 -i console`

- If you did not create a link, execute the command from the `ARCSIGHT_HOME/UninstallerDataSP1Patch3` directory:

  `./Uninstall_ArcSight_Web_Patch`

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

Issues Fixed in this Patch

ArcSight Manager

Issue	Description
ESM-47740 ESM-47205	While performing batch editing, such as modifying the configuration of multiple connectors, some of the connectors would crash.

ArcSight Console

Issue	Description
ESM-47741 ESM-47143	When changes were applied to a User resource, the tree in the Navigator window collapsed.
ESM-47739 ESM-47651	After changing a severity filter on a connector, all as-yet un-changed filters were inadvertently modified to match all events and set them to high Severity. This problem no longer occurs. If you have already edited a filter and need to know which filters were affected, so you can fix them, see "Fixing Misconfigured Connector Severity Filters" on page 7. This information is also available from the ArcSight Support portal in a KB article entitled "Editing Severity Filter For A Connector Changes agent-severity For All Of The Events From That Connector."

Open Issues in This Patch

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

Issue	Description
ESM-47738	There is an bug with the expdp command in Oracle v10.2.0.4 such that a datapump export using transportable tablespaces with a long list of tablespaces fails with ORA-39071. For the workaround for this issue, see "System Table Export - Oracle 10g" on page 7. This information is also available from the ArcSight Support portal in a KB article entitled "export_system_tables Script Error: ORA-39071: Value for TABLES is badly formed."
ESM-47414	A quick logger search using One-Time Password (OTP) in the embedded browser fails after a Logger session has been inactive for 'Logger Session Inactivity Timeout,' for which the default is 15 minutes. The workaround is to use the external browser to see results.
ESM-47209	The Send Logs feature still functions, however it no longer automatically uploads logs to ArcSight support. Send Logs creates a compressed file that you can manually email to ArcSight Support.
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.

Issue	Description
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\rollbacksp1p3.bat On Unix: <ARCSIGHT_HOME>/bin/rollbacksp1p3.sh
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.

Issues Fixed in Patch 2

Analytics

Issue	Description
ESM-45733	While populating the Active List in the Trend Actions tab, the Field Selector was not showing MIN and MAX fields from the Trend, but showing only the AVG and STDDEV fields. It now correctly shows the MIN and MAX functions.
ESM-45530	Under certain circumstances when creating a new trend, an ORA-00904 error occurred in the server and console log files. This error occurred when the query used a variable field that included a Date parameter with the expression "get_day_of_month(Agent Receipt Time, Default Time Zone)." This error no longer occurs in this circumstance.
ESM-38286 TTP#62366	Cyrillic (Russian) characters were not displayed correctly in emails when emailing reports. This is now fixed, however, you must set email.charset.encoding.default=UTF-8 in the server.properties file for it to work.

ArcSight Console

Issue	Description
ESM-47196	In 5.0 GA, we introduced the ability to audit device information for product licensing purposes. The device information is derived from the device side table, based on the device fields in each event. However, there were scenarios where the device information was incorrect, which lead to false alarms during user log in. This has been fixed by disabling the license violation popup dialog for device-count-exceeded scenarios.
ESM-46176	Previously, there was a problem with the format of the Last Modified Time in Query Viewer, if its query was queried on an active list and viewed as a table on the Dashboard, it was displayed with epoch time. The Last Modified Time is now displayed in a proper time format.

Issue	Description
ESM-45714	Users with an unpatched ESM Console v4.5 SP2, in multi-user mode on Linux, got the following message after installing Patch 3 and launching the console: mkdir: cannot create directory `tmp/tuple/remote/classes': Permission denied. This message is benign, but it no longer occurs when installing a patch under these circumstances.
ESM-41190 TTP#68141	If you set the Logger password type to "Password" and ran Logger commands in the external browser, an "Authorization Request" error appeared in your browser. Switching to a password type of "Text" allows the password to appear in plain text in URLs. Now logger passwords of type "Password" work as before, without causing this error.
ESM-36389 TTP#57799	The Console did not recognize Reference Page URLs containing spaces. This is now fixed.
ESM-35926 TTP#56662	There was a problem modifying cases through the web console when there was a large set of data in the "Estimated Impact" field. It would return the following error: "ORA-01461: can bind a LONG value only for insert into a LONG column." This error no longer occurs in this circumstance.

ArcSight Database

Issue	Description
ESM-47068	The character set AL32UTF8 caused the Manager solutions package to fail to upgrade. This problem no longer occurs.

ArcSight Manager

Issue	Description
ESM-47009	ESM was printing redundant log messages and redundant audit events of "Scheduled execution skipped," even though no Scheduled task execution was skipped. These redundant log messages and audit events are fixed.
ESM-46984	After an event was selected from an active channel and added to a case, the Case Detection Time and Estimated Start Time incorrectly showed the same time value. Now this issue has been fixed and these times show the correct values. (Note that the start time is only an estimate.)
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-46909	There was a problem with the ArcRemedy client reading ESM XML files while ESM is still writing them. This problem is now fixed.

Issue	Description
ESM-46868	Under some circumstances, when multiple report queries finished at the same time, it caused an exception in the InetSoft reporting utility and report generation failed. Now ESM ships with a newer version of InetSoft and the problem does not occur.
ESM-46864	Enabling SNMP forwarding was causing the ESM manager to stop persisting events. Now SNMP forwarding does not stop the event flow.
ESM-46807	Under some circumstances, when the size of 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.
ESM-46783	Uninstalling Identity View 2.0 from ESM 5.0 resulted in a conflict error. Users can safely ignore this message, because the conflict is caused by system resources that are correctly locked and cannot be removed anyway.
ESM-46274	Under certain circumstances, the Manager would unexpectedly reject additional threads while waiting to resolve a host during preparation of an internal event. Now thread management has been improved and unexpected thread blocking does not occur.
ESM-46093	The Manager would get unexpected Out of Memory errors on 32-bit platforms. Now, memory usage is more efficient and practical and unexpected Out of Memory errors do not occur.

ArcSight Web

Issue	Description
ESM-45565	When viewing a last state data monitor using ArcSight Web, the dashboard did not render correctly. Instead, it displayed the message, "Error retrieving portlet." The data monitor would display without error when viewed using the ArcSight Console. This problem no longer occurs.

ESM

Issue	Description
ESM-47228	The Custom Layout Dashboards did not allow you to add data monitors or backgrounds when the console user's password included special characters. Now Custom Layout Dashboards work correctly regardless of password characters.

Issue	Description
ESM-47085	Exceptions in updating an Active List batch to the database was causing inconsistency between the Active List cache and database entries. Now all relevant updates are correctly synchronized and active list insertion and failure work correctly. Furthermore, two common sources of Active List entry errors are now handled without causing an exception: - Strings that exceed the maximum length are truncated and the truncated entry is added to the Active list. The part of the string that was cut is recorded in the log. - Unsupported numeric values, such as out of range IP and MAC addresses, are discarded and an "AddToList: Failure" audit event is generated.
ESM-47027	Under some circumstances a Query Viewer would improperly fail with a message about a persistence problem while fetching data. This type of error no longer occurs.
ESM-46945	An event graph from a channel with the domain field set as an event node identifier displayed a NULL value for the domain field. Now the domain field correctly shows the domain field value.
ESM-46621	If a single entry from an Active list update batch failed for any reason, the entire transaction was rolled back and none of the other updates in the batch were written to the database. At the same time the cache had updated entries, which caused inconsistencies with the database entries. This, in turn led to other exceptions and unexpected behavior. Now all the relevant update events are correctly synchronized and individual entry failures are handled more efficiently so that active list insertion and failure work correctly.

Localization

Issue	Description
ESM-35719 TTP#56091	The email of notifications and attached reports sent by ArcSight did not show Chinese characters properly in e-mail or report title. Now Chinese characters display correctly.

Open and Closed Issues in ESM v5.0 SP1

For information about open and closed issues for ESM v5.0 SP1, see the release notes for that version.