Management Console User's Guide

ArcSight Express™ v3.0
Featuring ESM with CORR-Engine Storage

August 2011

ArcSight™
An HP Company

Management Console User's Guide, ArcSight Express™ v3.0

Revision History

Date	Product Version	Description
07/28/11	ArcSight Express v3.0	Management Console Guide initial version

Document template version: 1.0.2.9

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/
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

Introduction

This section provides a general overview of the ArcSight Management Console navigation and functions.

Overview

The ArcSight Management Console provides a streamlined interface that enables you to:

- Manage user accounts and user groups
- Manage data and event storage, archiving, and notifications
- Configure Connectors, notifications, and authentication
- Monitor events and resources from the dashboard
- Update your license
- Access ArcSight Web

In addition, you can install a separate ESM Console on other machines. This ESM Console is documented in the *ESM Console User Guide*. It enables you to create and manage resources, dashboards, and other objects, investigate events and patterns, and perform other necessary functions that the Management Console cannot do.

Streamlined Event Archiving

ArcSight Express's CORR-Engine enables scheduled archiving of daily event data, holding it for a specified retention period, and restoring older archives if they are needed for analysis.

Real-Time Correlation & Analytics

The CORR-Engine provides the foundation for correlation, and draws upon ArcSight's modeling, priority formula, and correlation conditions framework to identify, infer meaning, prioritize, and act upon events of interest.

Real-Time Monitoring

ArcSight Express implements interactive layouts for monitoring data using dashboards. These dynamic layouts enable users to see custom views of event and other data. You can create new custom views in the ESM Console.

CORR-Engine Storage and Retrieval

ArcSight Express v3.0 introduces the Correlation Optimized Retention and Retrieval Engine (CORR-Engine), a proprietary data storage and retrieval framework that enables ArcSight Express to receive events at high rates and perform high-speed searches.

ArcSight Express Start-Up Content

ArcSight Express includes a complete set of coordinated resources that address common security and management tasks to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration.

System Requirements

The Management Console is a Web application that is supported on the following browsers:

- Microsoft Internet Explorer 8 on Windows
- Microsoft Internet Explorer 9 on Windows (use the IE 9 Compatibility View or IE 8 Standard Mode)
- Mozilla Firefox v3.6 and 4
- Safari 5 on Macintosh OS X

Set your screen resolution to at least 1280 x 1024 to avoid cutting off part of the screen.

Starting the Management Console

To start the console from a supported browser enter the following URL:

```
https://<IP address>:8443/
```

Where **<IP address>** is the host name or IP address that you specified when you first configured ArcSight Express.

Log in with your User ID and password. Your user type controls which modules you have access to.

After you have logged in, there is a logout link in the upper right corner of the window.

Management Console Navigation

The Management Console home page appears when you start Management Console or click the Home icon ( ) on the tab bar from any Management Console module.

Hover the mouse over each Management Console module icon to expand it and show a brief description of that module's use.

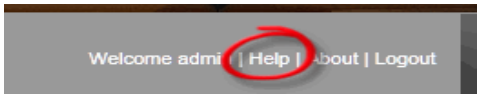
Each Module page has a tab bar at the top that provides access to the other modules.

The navigational elements on each Management Console module page are different and are described in their respective chapters in this guide.

Note

If a Management Console page stops loading or presents a JavaScript error, for example if there is a network interruption during loading, try pressing F5 to refresh the page.

Help Link

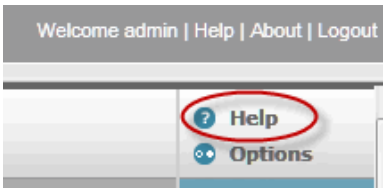


Click the Help link in the upper right corner for a page with links to documents relevant to using ArcSight Express. The documents appear as a comprehensive HTML Help system and there are links to a PDF version of each document.

The *Configuration Guide* for ArcSight Express is available from the customer support download site for ArcSight Express.

The arrow buttons in the upper left of each help page take you back and forth through topics in the order in which they appear in the table of contents, regardless of whether you were looking at them previously.

The **Go Back** and **Go Forward** links in the upper right corner of each page work the same way as the Forward and Back buttons in your browser window. They take you back and forth through the topics you have been looking at, regardless of where they are in the table of contents. (Go Back works after you have visited a second page and Go Forward works after you used Go Back.)



ArcSight Web runs embedded in an ArcSight Express module. It has its own context-sensitive online help link in the upper right corner of the ArcSight Web window.

For ArcSight Web documentation, refer to that help link or the ArcSight Web help and PDF link on the Welcome page of the help link for ArcSight Express shown at the top.

Chapter 2

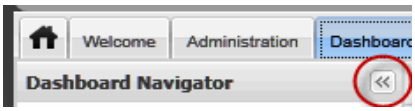
Administration

The Administration module enables you to control administrative functions such as users, storage, connectors and configuration.

Navigation

The accordion panel on the left contains expandable bars for each of the Administrative features in the Administration module.

Click the double arrow in the upper left corner of the accordion panel to hide the whole panel. Click it again to restore it.



When you click each function bar it expands to show the objects in this function that you can administer. For example the User Management function shows the user group hierarchy.

User Management

If it is not already expanded, click the **User Management** bar in the accordion panel to add, edit, or remove users and user groups.The **All Users** list is divided into three groups:

- Administrators
- Default User Groups
- Custom User Groups

You can add and delete users and groups, and perform other user management functions.

Highlighting any group displays its members in the user panel to the right.

In general, when you are first getting started, create groups first. You can only create a new user in an existing group

Add or Edit a User Group

You can add a sub group to any group below the top level. To create or edit a user group, use the following procedure:

1. To add a group: In the hierarchy tree on the left, right-click on the group to which you want to add a new child group and select **New Group**.

   To edit a group, highlight the group you want to edit and either right-click and select Edit or select **Edit Group** at the top right of the group member list panel.

2. Enter a **Name** and a **Description**. The **URI** field specifies the hierarchical location of the group. when adding a group, if you want the new group to be the child of a different group, abandon the operation and add to the other group.

3. In the users box, Select **Add** to add users to this group. This is optional; you can add users later. So you have not yet added any users to your system, see "Add or Edit a User" on page 13, and then come back here to add them to groups.

   - Select a user in one of the boxes use the left or right arrow keys to move the user to the other box. The users in the **Selected Users** box are members of the group.
   - You can start typing in the data entry field above the **Available Users** box to filter the list of available users. Click the X to the right of that field to clear it and restore the list of available users.
   - Use the double arrows (the top-most and bottom-most arrows) to send every user in the box to the other box.

4. Click **Save** to save the group and return to the group page.
   Click **Cancel** to clear any field changes you have made and restore them to the way they were. Cancel does not cancel the operation.

To abandon an edit or add operation, click the **Cancel** button to reset all the fields, then click anywhere in the tree view on the left to close the edit/add panel.

After you add a user group, select the resources and actions to which this group has access. See "Edit Advanced Permissions" on page 11.

Clone a User Group

You can create a copy of a user group using the Clone Group link. Clones are created within the same parent group as the cloned group. You cannot move a group to another group.

1. Highlight the group you want to clone and either right-click and select **Edit Group** or select **Edit Group** at the top right of the group member list panel.

2. Click the **Clone Group** link in the upper right corner of the Edit box. This creates a group with "Copy_" prefix.

3. Change the **Name** and add a **Description**. The **URI** field specifies the hierarchical location of the group. When adding a group, if you want the new group to be the child of a different group, abandon this clone operation and clone an existing child of the other group.

4. In the users box, Select **Add** to add users to this group. This is optional; you can add users later. By default a clone contains the same users as the group you are cloning.

   - Select a user in the available Users box use the right arrow key to move the user to the Selected Users box. The users in the **Selected Users** box are members of the group.

- To filter the list of available users, start typing in the data entry field above the **Available Users** box. Click the X to the right of that field to clear it and restore the list of available users.
- Use the double arrows ( and ) to send every user in the box to the other box.

5 Click **Save** to save the group and return to the group page.
Click **Cancel** to clear any field changes you have made and restore them to the way they were. Cancel does not cancel the operation.

To abandon a clone operation, click the **Cancel** button to reset all the fields, then click anywhere in the tree view on the left to close the Clone panel.

Cloning does not include any sub-groups that the cloned group had. It includes all users and other field values.

You cannot clone the three main groups at the top level.

Delete a User Group

To delete a group, right-click on the group and click **Delete Group**.

- You cannot delete the three main groups at the top level.
- You cannot delete a group of which you are a member, or any of its parent groups.

Delete a User from a Group

There are two ways to delete a user from a group:

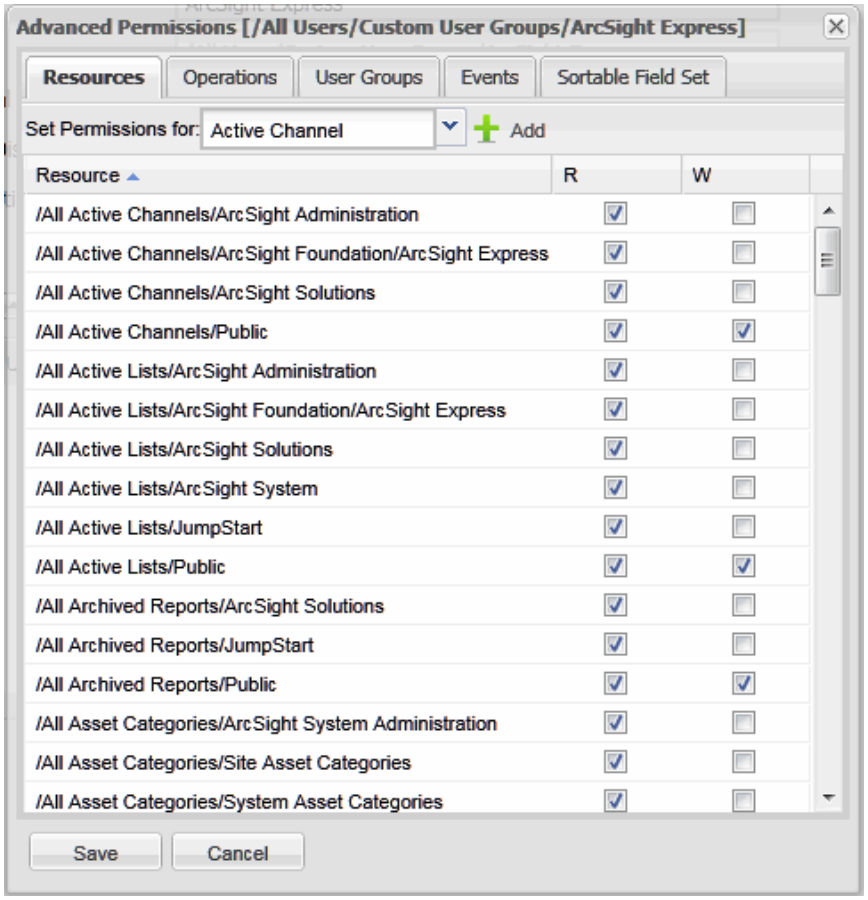
- Edit the user:
  a Select a user.
  b Scroll to the **Groups** box, at the bottom, and click the trash can icon to the right of the group from which you want to remove this user.
  c Click **Save** to save the change.
- Edit the group:
  a Right-click the group and select **Edit Group**.
  b Scroll to the **Users** box and click the trash can icon to the right of the user you want to remove from this group.

A user has to be a member of at least one group. If the trash-can icon is grayed out, add the user to another group before deleting from this group.

Edit Advanced Permissions

For any user group, you can manage what objects and actions they can access, and who can edit that group's permissions. Right-click the group whose permissions you want to change and select **Edit Group**.

Click **Advanced Permissions** at the top right of the Group Edit panel to specify access permissions for this group. You can select the type of data for which you want to assign permissions from the tabs at the top.



The permission tab descriptions are as follows:

- **Resources**: The list in the window shows each resource group to which this user group has Read (**R**) and Write (**W**) permission. To add another resource group:
  - **a** Select the resource category from the pull-down menu at the top of the Resources tab.
  - **b** Click **Add** to the right of the pull-down menu.
  - **c** Expand the resource group hierarchy to find the resource group to which you want to grant access.
  - **d** Check the box to the left of that resource group.
  - **e** Click **OK**.
  - **f** Click **Save**.

  To remove a resource group, uncheck both the Read and Write boxes.
- **Operations**: The list shows each group of operations that this user group can perform.
  - **a** Click **Add** at the top of the Operations tab.
  - **b** Expand the Operations groups to find the one to which you want to grant access.

c Check the box to the left of that operation group.

d Click **OK**.

To remove an operation group, click the trash can icon to the right of it and click **Save**.

- **User Groups**: The list shows each user group that has Read (**R**) and Write (**W**) permission on this user group. That is, groups that can see or change this group.

  a Click **Add** at the top of the User Groups tab.

  b Expand the user groups to find the one to which you want to grant access.

  c Check the box to the left of that user group.

  d Click **OK**.

  e Click **Save**.

  To remove a user group, uncheck both the Read and Write boxes.

- **Events**: The list shows event filters that control what events members of this user group can see. You can create filters from the ESM Console. To add more event filters:

  a Click **Add** at the top of the Event Filters tab.

  b Expand the Event Filters groups to find the event filters that you want to use for this user group.

  c Check the box to the left of those event filters.

  d Click **OK**.

  e Click **Save**.

  To remove an event filter, click the trash can icon to the right of it.

- **Sortable Field Set**: The list shows the sets of sortable fields on which members of this user group are allowed to sort when viewing channels.

  a Click **Add** at the top of the Sortable Field Set tab.

  b Expand the field set groups to find the field sets that you want allow these group members to use.

  c Check the box to the left of those field sets.

  d Click **OK**.

  e Click **Save**.

  To remove a sortable field set, click the trash can icon to the right of it.

Add or Edit a User

You create users within a user group below the All Users level. Use the following procedure to create a new user.

1 In the hierarchy tree on the left, click on the group to which you want to add a user.

2 In the user window, click **New User**, at the top of the list.
To edit a user, click anywhere on the user's row in the list.
The user details fields appear in the lower half of the list.

3 Optionally, fill in the Users **Full Name**.

4 Optionally, you can change the user's **Status** from *Login Enabled* to *Login Disabled*.

5 Optionally supply an **Email** address of the proper form (n@n.n).

6 Create a **User ID** and **Password**. The password must contain at least eight characters. These two are the only fields that are required.

7 By default the **External User ID** is the same as the User ID. An external user ID might be relevant if you have user accounts from other applications.

8 Optionally, expand the **Extended User Attributes** box and specify the users **Alias**, **Role** (Title and Department), and **Phone** numbers.

9 Choose a user **Type** from the drop-down menu. The user types are:

- **Normal User**: Has full privileges to use the Management Console, the ESM Console, and ArcSight Web client, and all tools.
- **Management Tool**: Has only the privileges needed to run certain management tools used in conjunction with network management products. This user cannot log in to any console. This type it is designed for use by software applications.
- **Archive Utility**: Has only the privileges needed to run the `archive` command. (See "ArcSight Commands" in the *Administrator's Guide*.) This command refers to archives of resources, not events. Access to resources is controlled through ACLs. This user type is for programs, not people and cannot log in to a console.
- **Forwarding Connector**: Has only the privileges needed by the Forwarding Connector.
- **Connector Installer**: A user who can add SmartConnectors to the system.
- **Web User**: Has privileges to use the Management Console and ArcSight Web, but not the ESM Console.

The user types confer access permissions that supercede access permissions granted through group membership. For example, a Web User in an Administrative group cannot log in to the ESM Console to perform security functions, because a Web User can only access the Management Console and Arcsight Web.

10 Optionally, expand the **Groups** box and click **Add** to select other groups to which this user should belong. Alternatively, you can edit a group and select users to be members.

11 Click **Save** to save this user and return to the group page.
Click **Cancel** to clear any field changes you have made and restore them to the way they were. Cancel does not cancel the operation.

To **Edit** a user, click on the user entry in the list. The Edit operations are the same as when adding a new user.

To abandon an add or edit operation, click the **Cancel** button to reset all the fields, then click anywhere in the tree view on the left to close the add/edit panel.

Delete a User

To delete a user:

1 Select the user group at the left in which the user appears, or All Users.

2 Select a user in the list on the right.

3 Click **Delete User** at the top.

Also see "Delete a User from a Group" on page 11.

Copy a User

To copy a user, select a user and click **Copy User**, at the top.

Use the copy function to create a new user. The login name is prefixed with “Copy_” but the user name and all other attributes except the password are the same; you must reset the password. Edit the attributes as specified in “Add or Edit a User” on page 13.

When you click **Save**, ArcSight Express creates the new user.

This feature is useful for creating multiple users who have the same group memberships or other similar attributes, without having to re-enter those attributes.

Search for a User

To search for users in the selected group by their user ID, begin to type the user ID in the search field at the top left of the user list. As you type, the user list is filtered to only show users whose User ID starts with the characters you have typed so far.

Click the **X** button to the right of the field to clear the search field and restore the user list.

CORR-Engine Management

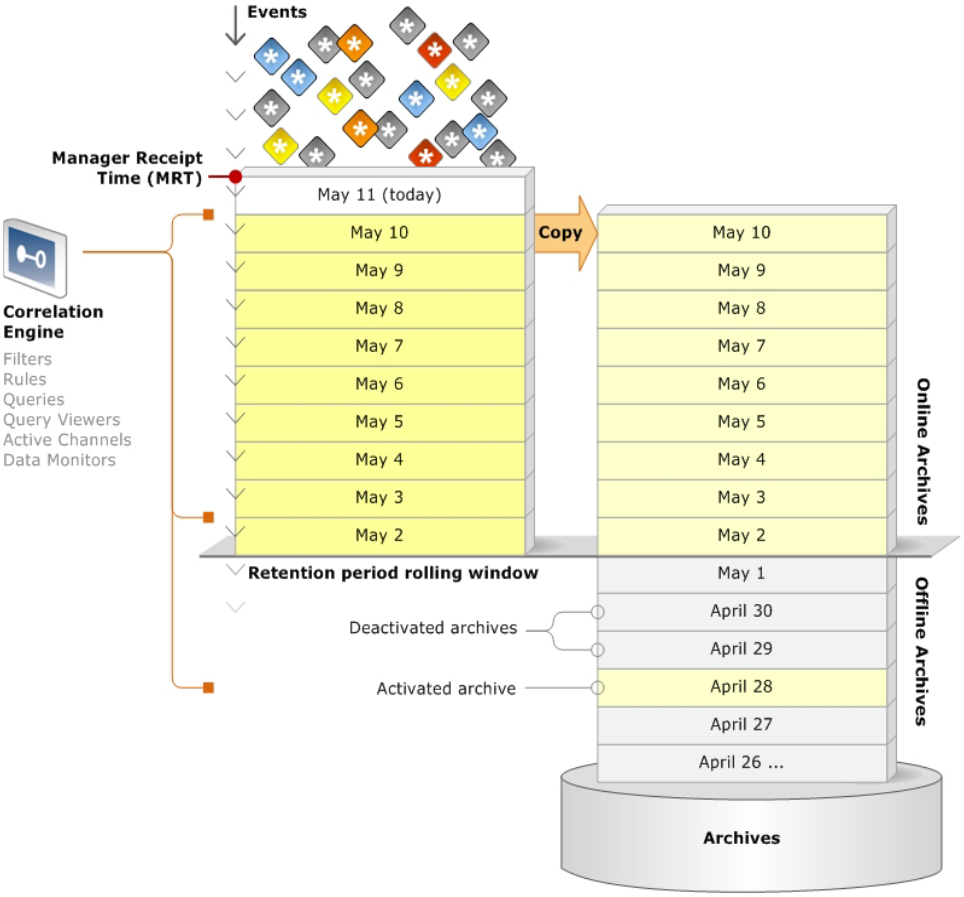
The Correlation-Optimized Retention and Retrieval Engine (CORR-Engine) is a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

To access the CORR-Engine Management function from the **Administration** tab, click the **CORR-Engine Management** bar in the accordion panel at the left.

CORR-Engine Management includes three pages:

- Event & Resource Storage — As events come in they are saved in Event Storage. System resources are stored in System Storage. You can see a summary of storage usage and set the retention period and notifications for usage thresholds.
- Archive Jobs — Provides a list of the daily events that are available for archiving or are already archived. Each day’s events (archived or not) are listed on this page until the age set by the retention period or the limit of available Event Storage space; whichever comes first. After that, they are deleted. If you have archived them, copies are retained and you can access them on the Archives page.
- Archives — Archives are daily events that you have saved, and which have been removed from the Archive Jobs list for lack of Event Storage space or expiration of the

retention period. Archives are deactivated when they are moved to this list, which means they cannot be used for any kind of analysis unless you activate them.



In the figure above, events come in to event storage, on the left. They are kept to the limits of the retention period or space and then deleted. As you archive daily events, they are copied to the archive storage area, on the right. They remain listed in Archive Jobs until their retention period expires and then they are deactivated and the listing is moved to the Archives page.

All the daily events in event storage, plus any activated archives are available for correlation analysis.

Storage allocations and where you can see them are shown in the following table:

Storage Area	Size	Purpose
Event Storage	919 GB (depending on appliance drive space)	Includes collected daily events that accumulate until the end of each day's retention period or until space runs out. At either point the oldest day's events are deleted. You can see the total, used, and available space by clicking on **Event Storage** on the **Event & Resource Storage** page.
System Storage	200 GB	Includes data objects and resources used by the system. You can see the total space and percentage used. By clicking on **System Storage** on the **Event & Resource Storage**, you can see the threshold notification settings in the lower half of the page.

Storage Area	Size	Purpose
Archives	200 GB	Includes daily events that have been archived (copied) from Event Storage. The space that remains available can be seen at the top of both the **Archive Jobs** and **Archives** pages.

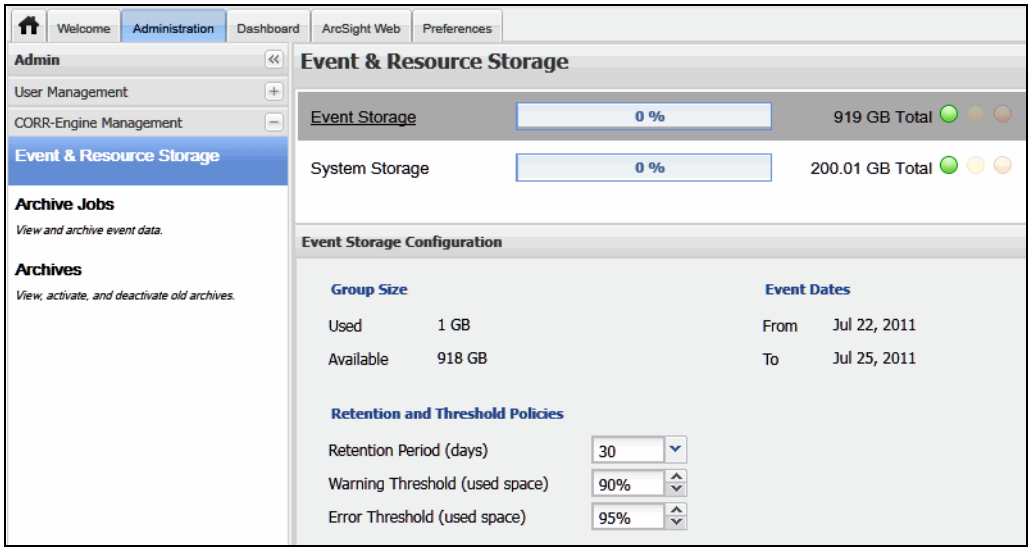
For both Event Storage and Archives, if used space reaches 85 percent and 95 percent (configurable for event storage), and you have configured the Notification List, you get an email warning you that available space is getting low. For archives there is an audit event when it is to full to archive another day's events.

Event & Resource Storage

Select **Event & Resource Storage** in the accordion panel to see a summary of event and system storage. The lower half of the page shows the configuration options for the selected storage area.

Event Storage

Event Storage is for daily events that are younger than the retention period. When they reach the retention period they are deleted, which means they are lost unless you have copied them to an archive (see "Configure Automatic Archiving" on page 21). If Event Storage space runs out the oldest day's events are deleted each day, even if they have yet to reach retention age.



Note

The time stamp on events is based on the time that the event was received by ArcSight Express, in ArcSight Express's time zone.

You can see the total, used, and available space by clicking on **Event Storage** on the **Event & Resource Storage** page. To see a list of all the day's events, see the **Archive Jobs** page.The percentage box shows the used percentage of the total storage space allocated to this storage area.

The colored circles to the right of the total size of event storage act as status lights: they indicate whether the used storage is below the warning threshold (green), above the

warning threshold but below the error threshold (yellow), or above the error threshold (red).

Click the **Event Storage** row in the Event & Resource Storage panel to see the configuration panel below. It shows used and available storage space for this storage area and the date range of included events.

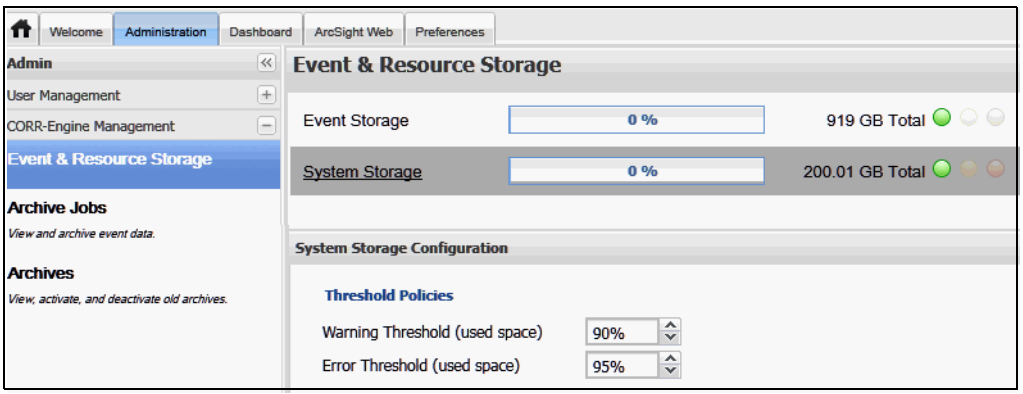
- The event storage **Retention Period** is the number of days that your events are kept in event storage. After that they are deleted. To save daily events, archive them.
- The usage **Warning Threshold** is the percentage of event storage area in use. When used space rises above this percentage, it lights the yellow warning indicator and sends a notification email. This percentage must be lower than the usage Error Threshold.
- The usage **Error Threshold** is a higher percentage of used space. When used space rises above this percentage, it lights the red error indicator and sends a notification email.

  If the number or size of daily events is high or your retention period is sufficiently long, you may run out of space in event storage before the oldest events reach the end of the retention period. If that happens, ArcSight Express deletes the oldest events first.

If you change any configuration options, click **Save** at the bottom to save them.

System Storage

System storage is for data such as ArcSight Express resources. There are 200 GB of disk space for system storage.



The percentage box shows the used percentage of the total storage space allocated to this storage area.

The colored circles to the right of the total size of system storage indicate whether the used storage is below the warning threshold (green), above the warning threshold but below the error threshold (yellow), or above the error threshold (red).

Click the **System Storage** row to see the configuration panel below There is no retention period; this data is always retained.

- The usage **Warning Threshold** is the percentage of system storage area in use. When used space rises above this percentage, it lights the yellow warning indicator and sends a notification email. This percentage must be lower than the usage Error Threshold.
- The usage **Error Threshold** is a higher percentage of used space. When used space rises above this percentage, it lights the red error indicator and sends a notification email.

If you change any configuration options, click **Save** at the bottom to save them.

Notification List

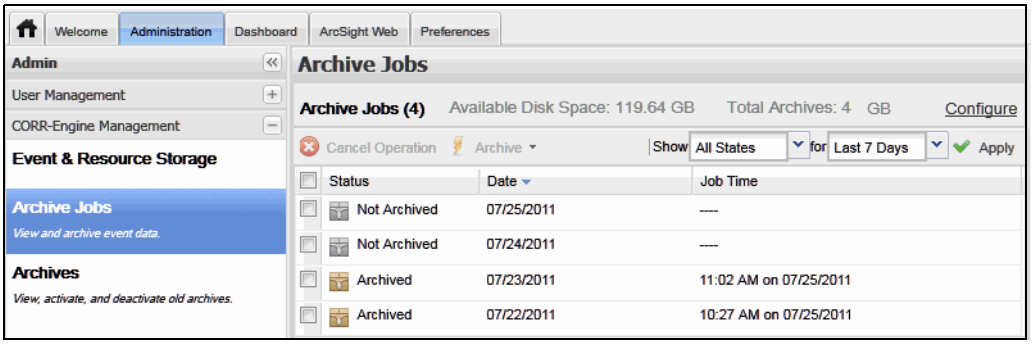
Use the **Notification List** button at the top right of the **Event & Resource Storage** page to add, edit, or remove email addresses of users to notify when any of the data storage thresholds are crossed and when any archive processing operation fails.

For event and system storage, you can separately configure the threshold for warning and error notifications in terms of percentage of used space.

The notification list applies to the Archives area, too. The Archives have a fixed warning threshold that triggers notification when ArcSight Express attempts to add an archive for which there is insufficient storage space.

Archive Jobs

An archive is a copy of a day's events. Archiving daily events is optional. You may allow them to be deleted at the end of the retention period or when Event Storage runs out of space. Alternatively, you can archive daily events manually or you can Configure Automatic Archiving.



Filtering the List

You can select a status and the number of days of archives to display in the status and time range fields at the top of the list.

What are Archive Jobs?

The Archive Jobs page shows each day's events as an archive job. That is, they are available to be archived, in the process of being archived, or already archived. Click on any day's events to see relevant details and available actions.

- Archive Jobs shows all the daily events that reside in event storage. Events that are copied to the archive storage space have the status Archived.
- Archive Jobs shows events that are not archived as Pending, Not Archived, or In Progress. Daily events that are Pending or Not Archived take up space in event storage, but not in the archive storage area.

Date is the day during which ArcSight Express received the events.

Job Time is the time when this day's events most recent activity started. If the status is Pending, the Job Time is when the collection process started at the beginning of the day. For Archived events, it is when the archiving process began.

How this List Works

Events are deleted from event storage and removed from the Archive Jobs list when they reach the age set as the retention period or event storage runs out of disk space,

whichever comes first. If a day's events have been archived when this deletion occurs, the archive listing is moved to the Archives page.

The Available Disk Space shown at the top of the page only reflects space for jobs whose status is Archived. Days' events with other statuses are in Event Storage. When archive space reaches 85 percent full, there is a warning notification, and when it reaches 95 percent full, there is an error notification. When archive storage space is too full to allow addition of another day's events, three things happen:

- An audit event occurs that there is no longer enough space to save another archive.
- Automatic, scheduled archiving stops.
- You are unable to manually archive any jobs.

Statuses and Actions

When you click on an Archive Job, a small box appears showing status details:

The event count and disk space show zero for daily events that are Pending or Not Archived because they are not in Archive storage until they are archived.

The following table describes archive-job statuses and available actions:

Status	Description	Available Actions
Archived	This day's events have been copied to the archive area as a directory. As long as the day's events from which it was copied remain in event storage, this archive is available for analysis. There are about 193 GB of storage set aside for archives.	None
Not Archived	This day's events have either had a problem archiving them or you cancelled the archiving operation, or you have turned off scheduled archiving. Events that are Not Archived are deleted when they reach the retention period age, so make sure to archive any days' events that you want to keep. If you click **Archive > Archive Now**, the status changes to In progress. If you click **Archive > Archive at nest scheduled time**, the status changes to Pending.	Archive: • Archive now • Archive at next scheduled time

Status	Description	Available Actions
Pending	This day's events have not reached the specified time when they are to be archived. This includes today's events, which are still being collected. **Cancel Operation** is available if scheduled archiving is enabled. Cancelling means that collection continues and when it is done at midnight the status changes to Not Archived. If scheduled archiving is not enabled, no action is available.	Cancel Operation
In Progress	This day's events are in the process of being archived, which means being copied to archive storage. If you click **Cancel Operation**, the status changes to Not Archived.	Cancel Operation

Actions are available at the top of the list, when you right-click on a day's events, and in a pop-up that appears when you select a day's events.

Configure Automatic Archiving

Click **Configure** at the right, above the archive list to control archiving.

Parameter	Description
Turn Archiving On	Select this to enable the copying of each day's events to an archive at the specified daily archive time the day following the day the events are received.
Archive Daily at	Select an archive time. Every day at this time the events collected yesterday are copied to an archive.
Archives Stored at	This is the path to the folder where archives are stored. ArcSight Express provides 200 GB of space for archives.

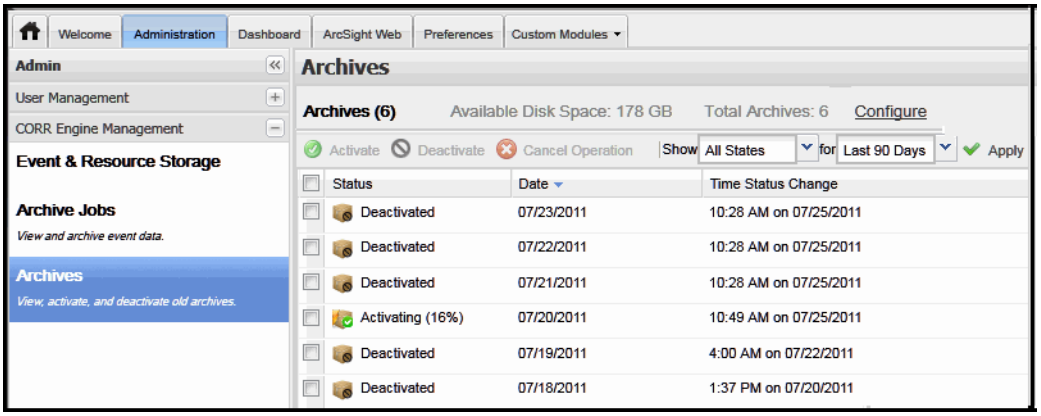
If you do not turn archiving on, events are deleted when they reach the retention period specified for the "Event Storage" on page 17, or when you run out of event storage space, whichever comes first.

When the disk space for archives is full, archiving stops. Events that are deleted from event storage are lost. If you need to save older events, consider these three tasks:

- Turn archiving on so that each day's events are copied to an archive you can back up.
- Regularly back up the **Archives Stored at** folder to another storage device.
- Delete older, deactivated archives as they are backed up, so that the archive area does not fill up.

Archives

When events that have been archived are removed from event storage (by retention period or lack of disk space), they are removed from the Archive Jobs list and moved to the Archives list.



Filtering the List

To filter which archives appear on the list, select a status and the number of days of archives to display in the status and time range fields at the top of the list.

What are Archives?

Archives are files that contain a copy of one day's events. As ArcSight Express creates an archive copy it places it in Archive Storage, which is separate from Event Storage. The term "Archives" includes some archives that are listed on the Archive Jobs list because they have not yet reached the retention limit age. This list only includes the archives that are older than the retention period. There is no copy in Event Storage.

How this List Works

Daily event archives appear on this list at the end of the last day of their retention period. Their status is Deactivated. You can activate an archive for analysis, if necessary.

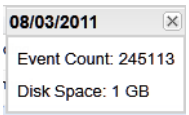
Keep in mind that daily events whose status is Not Archived are deleted when their retention period expires and there is no copy. Be sure to archive any events you need to keep beyond the retention period.

Archives remain on this list until you delete them. When archive storage space is too full to allow addition of another day's events, three things happen:

- The notification list is triggered and everyone is notified that there is no longer enough space to save another archive.
- Automatic, scheduled archiving stops.
- You are unable to manually archive any jobs.

Statuses and Actions

When you click on an Archive, a small box appears showing status details. These include the date, event countand the disk space used in Archive Storage.



The archive statuses are described as follows:

Status	Description	Available Actions
Activated	This archive is available for analysis, as are any other events listed in the Archives Jobs list.	Deactivate
Activating	This archive was deactivated, but is now in the process of being activated.	Cancel Operation
Deactivated	These events are not available for analysis. They are preserved until you delete them.	Activate

Actions are available at the top of the list, when you right-click on a day's events, and in a pop-up that appears when you select a day's events.

Click an archive to see the following:

- The date of the events collected in this archive
- When the archive was last activated or deactivated
- Event count
- Disk space
- A button to activate or deactivate it

Registered Connectors

Registered Connectors enables you to see a list of connectors on the left with their status. By default it shows a summary chart of how many connectors are up and down.

Refresh the Connector Display

Use the **Auto-Refresh** button in the upper right corner of the page to set how often you want ArcSight Express to refresh the Connector Status page. You can also refresh *now.* The Connector status page shows how many connectors are up or down. For information about each connector, click on it in the tree at the left and look at the Connector Editor.

For more information on connectors, refer to the documentation for the individual connector.

Connector Editor

Click a connector to see the connector editor. You can use the editor to view connector details, some of which you can change. You can also send connector commands.

The connector editor shows connector details described in the following table. If you change any values you can **Save** or **Cancel** your changes using the buttons at the bottom.

Field	Description
Connector	
Name	The name of this connector is automatically populated with the name assigned during connector Installation.
Status	Possible statuses are Down, Running, Stopped, and Unknown.

Field	Description
Connector Location	The location of this connector in the connector tree in the left panel.
Device Location	Specify where the connected device is located.
Version	The software version of the connector.
Comment	Enter any text as required.
Model Import User	Select a user from the pull-down menu.
Common	(Fields common to all resources)
Resource ID	The ID code for this connector resource.
Alias	Enter an optional alternate identification string used for referencing resources within ArcSight Express. If given, this alias appears in place of the resource's name everywhere it may be seen.
Description	Enter a text description of the configuration or other related information.
External ID	Enter an identification string suitable for, and which can be referenced by, systems outside ArcSight Express. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system.
Version ID	You can enter a unique version ID for resources.For example, it is useful when exporting or importing a package, if you don't want a newer resource to be overridden by a older version.
Deprecated	Check this box if you want to flag this connector resource as obsolete.
Create/Update Information	
Created By	The user who created this connector (logged-in user during connector installation).
Created on	The date and time of connector installation.
Last Updated by	The user who last updated this connector.
Last Updated on	The date and time this connector was last updated.
Modification Count	The number of times this connector has been changed since it was created or installed.

Connector Commands

For some connectors you can issue basic event-flow-control commands, get their operational status, or issue control commands to network devices through the connector.

Click the **Send Commands** button at the bottom of the connector Editor to select commands to send. The button is grayed out if sending commands is not allowed or if the connector is down. Commands available on this menu vary depending on which connector you are using.

The standard commands are described below.

Command	Description
Status Category	
Get Status	Provides a full report on the selected connector's current operational state.
Get Device Status	Provides the status of the device that reports to the connector. (Currently only available for the CiscoIDS/IPS SmartConnector.)
Agent Process Category	
Restart	Restarts a running connector. **Caution:** Once a connector is terminated, connector commands cannot access it. Therefore, a "restart" works only on a connector that is currently running. Sending a restart command to a running connector terminates and restarts the connector.
Terminate	Shuts down the connector and all processes the SmartConnector started. **Caution:** Once a connector is terminated, connector commands (including connector Process > Restart) cannot access it. The connector must be restarted manually from the machine on which it is installed.
Event Flow Category	
Pause	Stops the connector from sending events to the ArcSight Manager. **Note:** Events received from the target device are saved in the connector cache (even though the connector is in the **Pause** state).
Stop	Stops the connector from sending events to the Manager. **Caution:** A **Stop** command causes the connector to drop all events, including events stored in the connector cache.
Start	Prompts the connector (previously in **Stop** or **Pause** state) to start sending events to the Manager.
Network Category	
Flush Name Resolver Cache	Clears cache for Network name resolver.

Command	Description
Upgrade Category	
Upgrade	Launches a Command Parameters dialog for remote upgrade to newer versions of connectors for managed assets. Provide the version number of the connector to which you want to upgrade and a wait time to verify that the upgrade completed successfully. (If the upgrade is not successful, the system performs an automatic rollback to the previous version of the connector.) Click **OK** to start the upgrade. See the "Managing SmartConnectors" chapter of the *ESM Console User's Guide* for prerequisites for the upgrade process and detailed information on how to upgrade connectors.
Rollback Upgrade	Launches a Command Parameters dialog for remote rollback of connector version to a specified previous version. See the "Managing SmartConnectors" chapter of the *ESM Console User's Guide* for complete information.
Adjust Category	
Rename Mismatched Override Files	Enables you to remotely rename an connector parser override file whose version stamp no longer matches the parser that it was intended to override. Renaming it appends ".1" (or 2, or 3, if earlier numbers are in use), which stops the file from being used. The first parameter is a regular expression you can specify to match specific override files (or blank, the default, for all). The second parameter is a boolean where true, the default, means restart the connecter if any files are renamed.

Tech Support commands are provided for use primarily by ArcSight Customer Support. Brief descriptions of these Tech Support commands are provided for informational purposes, but these commands are not intended for use by customers except as instructed by Technical Support.

Command	Description
Tech Support Category	
Get Support Info	Gets logs and other feedback on connectors.
Get 'agent.properties'	Shows the list of properties for the selected connector.
Get Upgrade Logs	Get upgrade logs on connectors.
Get 'agent.wrapper.conf'	Shows the wrapper configuration for the selected connector.
Get Configuration XML File	Shows the XML configuration file for the selected connector.
Get Thread Dump	Gets one thread dump for the selected connector.

Command	Description
Get Two Thread Dumps...	Gets two thread dumps for the selected connector spaced by the time interval specified. By comparing both thread dumps, ArcSight Customer Support can troubleshoot connectors with threads that are hanging for unknown reasons.
Get Heap Dump	This generates a heap dump, if possible, which in some situations can be useful to ArcSight to analyze problems. The destination ID is used as part of the file name, the file is placed in the same directory as the connector's logs, and normally only 10 such files are kept.
Get last N lines of 'agent.log'...	Shows an excerpt from the connector log file based on the number of lines you specify. The default is 500 lines.
Get System Properties	Shows system properties for the selected connector, including details on variables such as Java runtime name, Java virtual machine (VM) version, operating system name, paths for various Java components, paths for ArcSight Home, user directories, user home, and so forth.
Enable Event Flow Tracing...	Allows you to specify a component and fields to log for initiating an event flow trace. The component should be chosen from the components listed in the Get Status results.
Disable Event Flow Tracing...	Disables event flow tracing on the selected component.
Get Event Flow Tracing Log	When tracing is enabled on the selected connector, the connector logs data about events it receives.
DNS Test	This command takes one parameter, which is either a host name to resolve or an IP address to reverse resolve. This is useful to see what results would normally be expected for the name resolver component of the connector, since it uses the same mechanism to do the lookup as the name resolver uses.
Enable Map File Logging	Directs the AgentNATProcessor component, which processes map files for each event, to log what it is doing for each event. By default the last 100 events are logged.
Disable Map File Logging	Directs the AgentNATProcessor to stop logging.
Get Collected Map File Logging	Gets the collected log messages for the most recent events (100, by default), which may help debug problems with why a map file is not operating as expected.

The following commands provide access to connector component mapping and event categorization for advanced users.

Command	Description
Mapping Category	

Get Additional Data Names	Returns a list of data names seen for each device vendor/product combination since the connector started. For example:
	`Additional Data Names Seen:`
	`Generic (no vendor/product):`
	`test1 [3 times]`
	`test11`
	`test13 [2 times]`
	`Vendor/product [vend/prod]:`
	`test1`
	`test10 [6 times]`
	By default, the command limits the list to show only the most recent 100 device vendor/product combinations and the most recent 100 names for each.
	Tip: You can change this limit by editing the connector property `agent.additionaldata.mapper.track.max.names` in the file `$ARCSIGHT_HOME/ArcSightSmartAgents/current/user/agent/agent.properties` on the machine where the connector is installed. However, in most cases we recommend keeping the defaults. If you do change a property setting such as this, restart the connector.
	If a data name is not a string, its data type is displayed in the list. If the connector saw an additional data name more than once, the command output indicates the number of times the name was seen.

Map Additional Data Name...	Brings up a dialog where you can map an additional data name for the selected connector.
	For a generic mapping, you can leave the **Device vendor** and **Device product** fields blank. For a specific mapping, fill in these fields with the appropriate vendor and product names.
	Typically, the **Additional data name** is one of the names shown in the Get Additional Data Names output (but can be another name not on that list).
	The **ArcSight field** must be a valid ArcSight event field.
	Click **OK** to create the mapping.
	Here is an example of the command output for a successful generic mapping:
	`Successfully mapped additional data name [test11] to event field [message] for vendor/product []`
	A successful device vendor/product-specific mapping returns output similar to this:
	`Successfully mapped additional data name [test10] to event field [message] for vendor/product [vend/prod]`

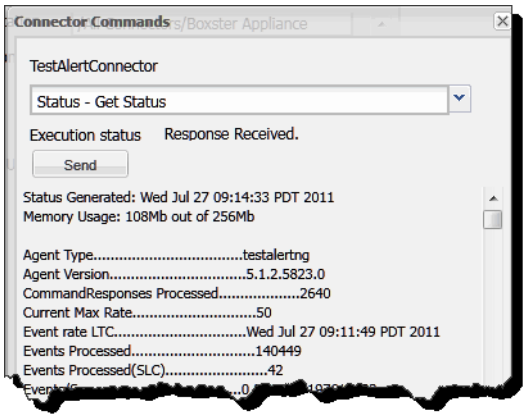
Command	Description

	If the additional data name has not been seen, the name is still mapped, but with a warning like this:
	`Successfully mapped additional data name [foo] to event field [deviceCustomString1] for vendor/product [vend/prod] (note that additional data name [foo] has not been seen for vendor/product [vend/prod])`
	If the ArcSight field is not valid, the error returned is similar to this:
	`Failed to map additional data name [bar] to event field [messages] for vendor/product [vend/prod] (event field [messages] is unknown)`

Unmap Additional Data Name...	Brings up a dialog where you can unmap an additional data name for the selected connector.
	To remove a generic mapping, you can leave the **Device vendor** and **Device product** fields blank. To remove a specific mapping, fill in these fields with the appropriate vendor and product names. The additional data name should be one that was previously mapped for the specified device vendor and product combination.
	Click **OK** to unmap the data name.
	Here is an example of the command output for a successful generic unmapping:
	`Successfully unmapped additional data name [test11] for vendor/product []`
	A successful device vendor/product-specific unmapping returns output similar to this:
	`Successfully unmapped additional data name [foo] for vendor/product [vend/prod]`
	If the specified additional data name was not previously mapped, the output looks like this:
	`Failed to unmap additional data name [foo] for vendor/product [vend/prod] (not previously mapped)`
	Notes:
	• One additional data name can be mapped to more than one ArcSight field for the same device vendor/product combination, and in this case unmapping it unmaps it from all ArcSight fields for that device vendor/product. This is an unlikely scenario, however.
	• The converse case, where multiple additional data names are mapped to the same ArcSight field for the same device vendor/product combination, results in the last mapping taking precedence over any previous mappings to that ArcSight field for that device vendor/product. No warning is generated in this case.

Command	Description
Categorizer / mapper Category	
Reload custom categorizations	There are several ways to set event category information for events. The least common of these is to store custom categorization files (organized by vendor and product) on the connector machine in the `user/agent/aup/acp/categorizer/current` directory (or the `user/agent/acp/categorizer/current` directory). If such categorization files exist and have been changed, this command reloads them without restarting the connector.
Reload custom map files	Rescans and reloads map files in `user/agent/map` directory on the machine where the connector is installed. The map files are named in the form `map.n.properties`, where `n` is a number starting with 0. Use this command to immediately apply the latest changes. Not all connector setups include custom map files. **Caution:** Map files are created on some connector machines to fulfill specific needs. If you are not familiar with the categorizer/mapping setup of an environment, we recommend that you do not use Reload commands.
Reload external map files	Re-scans and reloads external map files in the `user/agent/extmap` directory on the machine where the connector is installed. The map files are named in the form `extmap.n.properties`, where `n` is a number starting with 0. Use this command to immediately apply the latest changes. Not all connector setups include custom external map files. Caution: External map files are created on some connector machines to fulfill specific needs. If you are not familiar with them, we recommend that you do not use Reload commands.

When results are to be returned, the command dialog expands to show progress, and then the results.



Configuration Management

Configuration Management enables you to:

- View license information
- Set manager heap size
- Enable notifications and set your mail server
- Change the Manager authentication method and settings.

License Information

Your current license information appears in the upper part of the page.

To install a new license:

1. In the **License File** field specify or browse to the `lic` or `zip` file containing the license you want to upload.
2. Click **Upload** to upload a new license.
3. After uploading, the Management Console asks you if you want to Restart, which restarts certain ArcSight server processes.

   You can choose to restart later. If so, when you are ready, select **Server Management** in the left panel and click **Restart**, at the bottom. You will have to log in again.

Server Management

Manager Heap Size

In the **Manager Heap Size** field, select one of the possible heap sizes from the pull-down list.

The Manager heap is a special area of memory that ArcSight Express allocates, although the Manager uses some additional system memory as well. The recommended heap size for production deployments is at least 8 GB. Smaller amounts affect performance. It is important that the amount of physical memory available on the system be significantly larger than the amount of heap allocated for the Manager, so that there is additional space available for the operating system and for cache use.

The ArcSight Express B7400 appliance has 36GB of physical memory.

After changing the heap, the Management Console asks you if you want to Restart, which restarts certain ArcSight server processes.

You can choose to restart later. If so, when you are ready, select **Server Management** in the left panel and click **Restart**, at the bottom. You will have to log in again.

Enable Notifications

Set up notification and specify notification recipients to receive system warnings. The importance of this step is sometimes overlooked, leading to preventable system failures.

The following table describes parameters you can enter to set up mail server notification.

Parameter	Description
From Address	The e-mail address from where notification messages originate and are sent, appears in the From field of notification messages
Error Notification Recipients	A comma-delimited list of e-mail addresses to notify of Manager errors.
Preferred Mail Server	Select whether the mail server is internal or external. Using the internal SMTP server requires DNS to be set up correctly on the ArcSight Manager System. Using an external SMTP server requires that the ArcSight Manager system be able to connect to the host via port 25.

Choose whether your **Preferred Mail Server** is Internal or External. The internal mail server is built into ArcSight Express.

External Mail Server Information

If your preferred mail server is external, you must supply this information.

Enter the name of your **Outgoing Mail Server**.

If you check **Use Internal Server as a Backup**, it uses the mail server that is built into ArcSight Express if the external mail server is not available.

Enable Acknowledgements

Enabling acknowledgements mean that notification recipients can reply to the email, and the reply (an acknowledgement) goes to an email account that the ArcSight Express Manager can access.

If you check **Enable Acknowledgements**, fill out the following parameter fields:

Parameter	Description
Incoming Mail Server	The server host name that the Manager uses to receive notification confirmations.
Mail Protocol	Either the Internet Message Access Protocol (IMAP) or Post Office Protocol V3 (POP3), which is used by the Manager to communicate with the Incoming Mail Server.
Account	The user name that the Manager uses to login to the Incoming Mail Server.
Password	The password that the Manager uses to login to the Incoming Mail Server.

Acknowledgements work in conjunction with acknowledgement settings set in the ESM Console for wait-time settings and escalation. Depending on the severity of the notification, if the Manager does not receive acknowledgement within the configured wait time, the notification is escalated. That is, a notification is sent to someone else. Refer to “Changing Notification and Acknowledgement Settings” in the “Managing Users and Permissions” chapter of the *ESM Console User’s Guide*.

Restart

When you make changes that require a restart, a dialog appears that enables you restart immediately. If you choose to wait, you can restart later. Restart does not reboot the computer, it restarts selected ArcSight server processes.

Click **Restart** at the bottom of the **Server Management** panel if you have made changes that require a system restart.

When you click **Restart**, it asks if you are sure you wish to restart. If you click Yes, It issues the restart command and your session loses its connection to ArcSight Express. You can reconnect and log in again after the restart has completed.

Authentication Configuration

In the **Authentication Method** field select the desired authentication method.

The authentication options enable you to select the type of authentication to use when logging into the Manager.

- In order to use PKCS#11 authentication, you must select one of the SSL based authentication methods.
- If you plan to use PKCS #11 token with ArcSight Web, make sure to select **Password Based or SSL Client Based Authentication**.
- PKCS#11 authentication is not supported with Radius, LDAP and Active Directory authentication methods.

See the appendix "Using the PKCS#11 Token," in the *ArcSight Express Configuration Guide*, for details on using a PKCS #11 token such as the Common Access Card (CAC).

By default, the system uses its own, built-in authentication, but you can specify third party, external authentication mechanisms, such as RADIUS Authentication, Microsoft Active Directory, LDAP, or a custom JAAS plug-in configuration.

How external authentication works

The Manager uses the external authentication mechanism for authentication only, and not for authorization or access control. That is, the external authenticator only validates the information that users enter when they connect to the Manager by doing these checks:

- The password entered for a user name is valid.
- If groups are applicable to the mechanism in use, the user name is present in the groups that are allowed to access ArcSight Manager.

Users who pass these checks are authenticated.

Once you select an external authentication mechanism, all user accounts, including the admin account, are authenticated through it.

Guidelines for setting up external authentication

Follow these guidelines when setting up an external authentication mechanism:

- Users connecting to the Manager must exist on the Manager.
- User accounts, including admin, must map to accounts on the external authenticator. If the accounts do not map literally, you must configure internal to external ID mappings in the Manager.

- Users do not need to be configured in groups on the Manager even if they are configured in groups on the external authenticator.
- If user groups are configured on the Manager, they do not need to map to the group structure configured on the external authenticator.
- Information entered to set up external authentication is *not* case sensitive.
- To restrict information users can access, set up Access Control Lists (ACLs) on the Manager.

If you configure the Manager using **Password Based and SSL Client Based Authentication** or **SSL Client Only Authentication**, be aware that ArcSight Web does not support these modes. So:

- If you plan to use ArcSight Web, you will need to configure your Manager to use **Password Based Authentication** or **Password Based or SSL Client Based Authentication** as your authentication method.
- If you plan to use PKCS#11 authentication with ArcSight Web, be sure to select **Password Based or SSL Client Based Authentication** only.

Password Based Authentication

Password-based authentication requires users to enter their User ID and Password when logging in. You can select the built-in authentication or external authentication.

Built-In Authentication

This is the default authentication when you do not specify a third party external authentication method.

If you selected this option, you are done.

Setting up RADIUS Authentication

To configure ArcSight Manager for RADIUS Authentication, choose **RADIUS Authentication** and supply the following parameter values:

Parameter	Description
Authentication Protocol	Which authentication protocol is configured on your RADIUS server: PAP, CHAP, MSCHAP, or MSCHAP2.
RADIUS Server Host	Host name of the RADIUS server. To specify multiple RADIUS servers for failover, enter comma-separated names of those servers in this field. For example, server1, server2, server3. If server1 is unavailable, server2 is contacted, and if server2 is also unavailable, server3 is contacted.
RADIUS Server Type	Type of RADIUS server: • RSA Authentication Manager • Generic RADIUS Server • Safeword PremierAccess
RADIUS Server Port	Specify the port on which the RADIUS server is running. The default is 1812.
RADIUS Shared Secret	Specify the RADIUS shared secret string used to verify the authenticity and integrity of the messages exchanged between the Manager and the RADIUS server.

Setting up Active Directory User Authentication

To authenticate users using a Microsoft Active Directory authentication server, choose **Microsoft Active Directory**. Communication with the Active Directory server uses LDAP and optionally SSL.

The next panel prompts you for this information.

Parameter	Description
Active Directory Server	Host name of the Active Directory Server.
Enable SSL	Whether the Active Directory Server is using SSL. The default is True (SSL enabled on the AD server). No further SSL configuration is required for the AD server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the AD server side, not the manager.
Active Directory Port	Specify the port to use for the Active Directory Server. If the AD server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the AD server, use port 389.
Search Base	Search base of the Active Directory domain; for example, DC=company, DC=com.
User DN	Distinguished Name (DN) of an existing, valid user with read access to the Active Directory. For example, CN=John Doe, CN=Users, DC=company, DC=com. The CN of the user is the "Full Name," not the user name.
Password	Domain password of the user specified earlier.
Allowed User Groups	Comma-separated list of Active Directory group names. Only users belonging to the groups listed here will be allowed to log in. You can enter group names with spaces.

Specify any user who exists in AD to test the server connection.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the AD server.

Configuring AD SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store `<ARCSIGHT_HOME>/jre/lib/security/cacerts`, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the *Administrator's Guide*.

Setting up LDAP Authentication

The ArcSight Manager binds with an LDAP server using a simple bind. To authenticate users using an LDAP authentication server, choose **Simple LDAP Bind** and click **Next**. The next panel prompts you for this information.

Parameter	Description
LDAP Server Host	Specify the host name of the LDAP Server.
Enable SSL	Whether the LDAP Server is using SSL. The default is True (SSL enabled on the LDAP server). No further SSL configuration is required for the LDAP server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the LDAP server side, not the manager.
LDAP Server Port	Specify the port to use for the LDAP Server. If the LDAP server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the LDAP server, use port 389.

Specify any user who exists in LDAP to test the server connection.

Enter a valid Distinguished Name (DN) of a user (and that user's password) that exists on the LDAP server; for example, CN=John Doe, OU= Engineering, O=YourCompany. This information is used to establish a connection to the LDAP server to test the validity of the information you entered in the previous panel.

LDAP groups are not supported. Therefore, you cannot allow or restrict logging into the Manager based on LDAP groups.

If you configure your Manager to use LDAP authentication, ensure that you create users on the Manager with their Distinguished Name (DN) information in the external ID field. For example, CN=John Doe, OU= Engineering, O=YourCompany.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the LDAP server.

Configuring LDAP SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store `<ARCSIGHT_HOME>/jre/lib/security/cacerts`, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the *Administrator's Guide*.

Using a Custom Authentication Scheme

From the Manager Setup Wizard, you can choose the **Custom JAAS Plug-in Configuration** option if you want to use an authentication scheme that you have built. (Custom Authentication is not supported from the ArcSight Management Console.) You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.

Password Based and SSL Client Based Authentication

Your authentication will be based both upon the username and password combination as well as the authentication of the client certificate by the Manager.

Using PKCS#11 provider as your SSL Client Based authentication method within this option is not currently supported.

Password Based or SSL Client Based Authentication

You can either use the username/password combination or the authentication of the client certificate by the Manager (for example PKCS#11 token) to login if you select this option.

SSL Client Only Authentication

You will have to manually set up the authentication of the client certificate by the Manager. See the *Administrator's Guide* for details on how to do this.

You can either use a PKCS#11 Token or a client keystore to authenticate.

Chapter 3

Management Console Dashboards

Dashboards are a graphical display of data gathered from one or more Data Monitors or query viewers. Dashboards can display data in a number of graphical formats, including pie charts, bar charts, line charts, and tables, and you can rearrange the dashboard elements in the window and save the arrangement. The dashboards that appear in the Management Console are those that exist in the ESM Console, where dashboards can be created and customized.

For information on creating and managing dashboards and Data Monitors see chapter 7, “Monitoring Events,” in the *ESM Console User’s Guide*.

For information on query viewers, see chapter 13, “Query Viewers,” in the *ESM Console User’s Guide*.

Dashboard Overview

Dashboards in the Management Console appear as layouts of dashboard data using a browser-based runtime environment. You can see all the dashboards that appear in the ESM Console and you can rearrange the layouts and save them.

- Viewing dashboards requires the Adobe Flash 10 plugin.
- ESM may require additional configurations to display content using Adobe Flash depending on the operating system you are running.

For details about supported browsers and operating systems and the configurations required to display features in a browser, see “Web Browsers (Internal and External),” in the *ESM Console User’s Guide*.

Dashboards in the Management Console can display data monitors and query viewers, but they cannot display data from the following types of data monitors:

- Event Graphs
- Geographic Event Graphs
- Hierarchy Maps

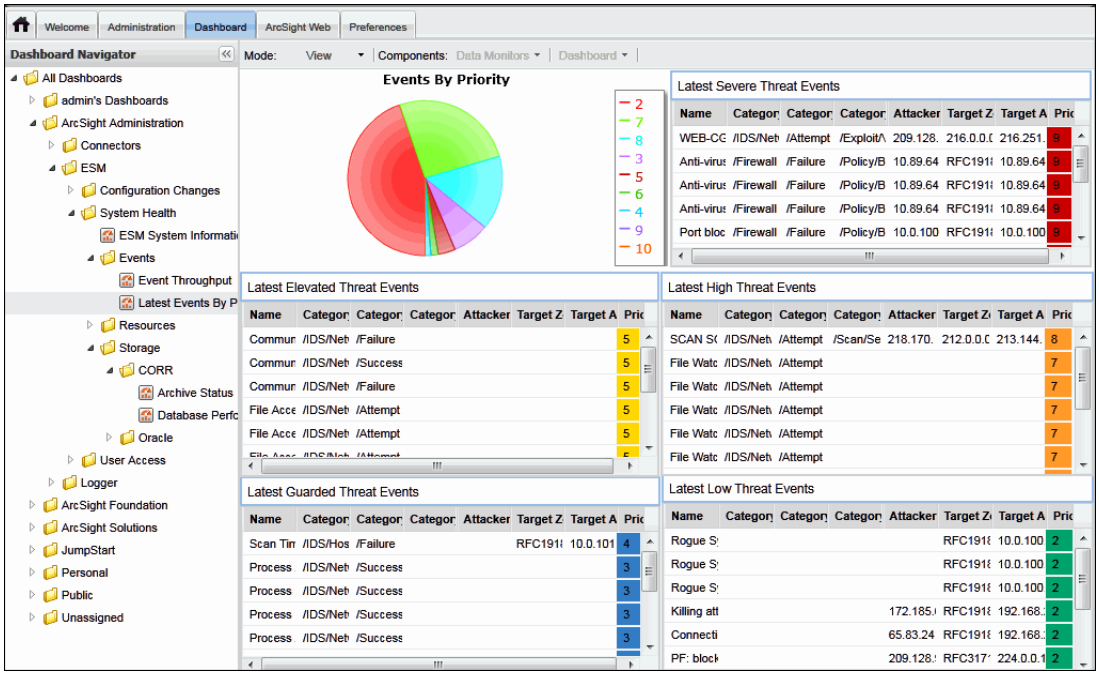
To view dashboards with these types of data monitors, use the regular dashboard view in the ESM Console.

Management Console dashboards do not support drill-down on events.

Dashboards provide two modes: *View* mode for monitoring and investigating events, and *Arrange* mode, for customizing the layout.

Viewing Dashboards

Management Console dashboards open in the *View* mode by default. If the dashboard is not in View mode, select **View** from the Mode drop-down menu in the menu bar above the dashboard.



In the View mode the **Data Monitors** and **Dashboard** pull-down menus are not available. To make any changes to the dashboard, you must change the mode to Arrange mode.

- If you create or edit a custom dashboard in the ESM Console, save and it will then be available to other ESM Consoles and the Management Console.
- User customizations to chart settings and color selections applied to dashboards in the ESM Console are not applied to the Management Console dashboard view.
- The background image scales to fit the available space in the Viewer panel. You may need to adjust the shape of your viewer panel or browser window to preserve the proportions of the background image.

Arranging Dashboards

To re-arrange how the dashboard elements appear on a dashboard, select **Arrange** from the Mode drop-down menu in the menu bar above the dashboard. In *Arrange* mode, you can customize the dashboard layout, toggle dashboard elements on and off, and relocate, resize, and select dashboard elements in the dashboard view.

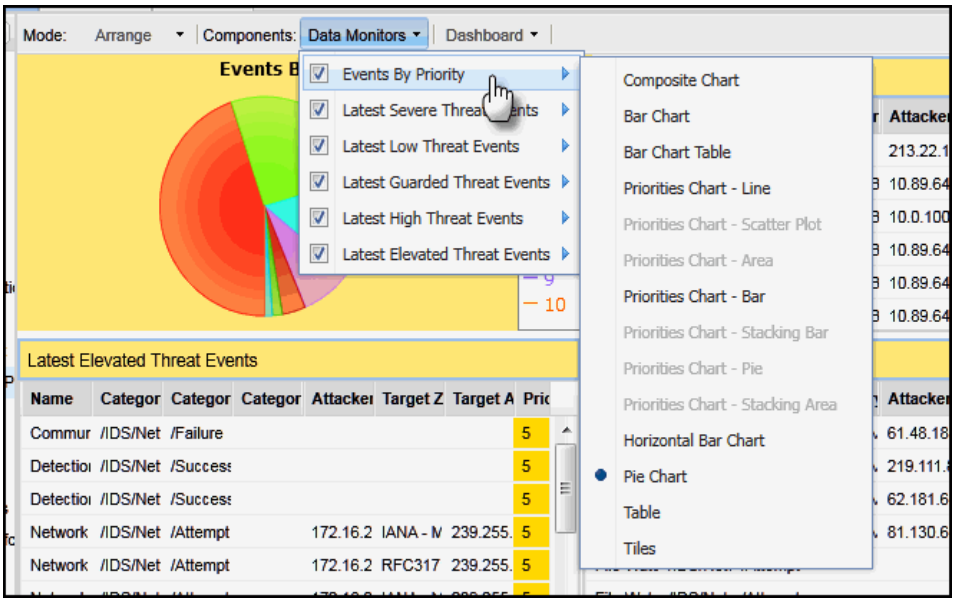
You can move a dashboard element by dragging it.

You can resize a dashboard element by clicking in a corner or side and dragging it.

Data Monitor Menu

The **Data Monitor** menu enables you to select one of the dashboard elements (for example data monitors and query viewers) in this dashboard and choose how you would like to display it. These display options vary according to the type of dashboard element, which depends on selections you made when you created it in the ESM Console. The options include tables, pie or bar charts, scatter plots, and other displays, depending on what the dashboard element supports.

To hide a dashboard element, uncheck the box to the left of its name in the menu.



Dashboard Menu

- **Reset Layout** recalculates an evenly-spaced layout.
- **Save Dashboard** saves the layout. The layout is also saved automatically when you return to the View mode.
- **Close Dashboard** does not function in this release.
- **Export** does not function in this release.

When you are done arranging the layout in Arrange mode, *be sure* to save it and return to the View mode. If you leave the dashboard in Arrange mode and then resize the window, it can scramble your arrangement. Returning to View mode preserves the layout and prevents layout errors.

Chapter 4

Preferences

The Preferences module enables you to control additional links, appearance, logging and your own user account settings.

Custom Modules

A module is one of the icons that appear on the home page. The modules that come with ArcSight Express appear as tabs when you go to one of the module pages. Modules that you create appear on the home page and become menu entries under the **Custom Modules** tab.

Create additional web modules for the Management Console home page. You can simply add links to other web sites or you can link to web applications.

To add a new module:

1. Click **Add** in the action bar at the top of the list.
2. Type in a **Name** for this module. This name appears in the icon for this module and in the box above it when you hover the mouse over the icon.
3. Enter the **URL** for this module.
4. Optionally, enter a **Description** to appear above the module icon and in the box above it when you hover the mouse over the icon.
5. Click **Save** to save this module or **Cancel** to clear the entries and exit the Add mode.

To delete a module highlight the module in the list and click **Delete** in the action bar at the top of the list.

Skins & Effects

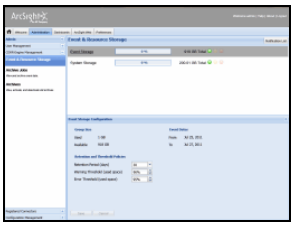
Change the color combinations used in the Management Console display.

1. **Select a Skin** Name from the list.
2. Turn on **Navigation Transition Effects** to introduce a fade effect for page transitions.

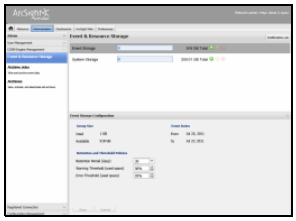
3 Click **Save** in the lower left corner of the panel.

Note

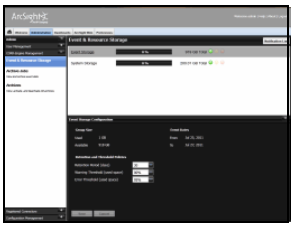
Logging and Skins preferences are both saved in the ArcSight Express system for your user ID. However, if you are sharing a computer with another user, clear the browser cookies before logging in, otherwise you will see the preferences of the last user on this computer.



Blue Theme



Gray Theme



Slickness

Logging

This Logging control is for log entries generated by the Management Console user interface.

Turn **Logging** on to enable the **Logging User Interface** selections:

- The **Logging Panel** is an area at the bottom of the window that shows the most recent events.
- The **Logging Pop-up** is a small pop-up window that you can move around and resize
- The **Logging Debug Support** option shows an increased level of detail in the logged messages.

Click **Save**, at the bottom, if you change any Logging options.

Account Settings

Change your own account settings, except your User ID. You can change your password, name, role, department, and contact information.

Click **Save**, at the bottom, if you change any account settings.

Index