



Hewlett Packard
Enterprise

HPE ArcSight Management Center

Software Version: 2.7x

Administrator's Guide

November 30, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2017 Hewlett Packard Enterprise Development, LP

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

<https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Chapter 1: ArcSight Management Center Overview	16
New Features and Enhancements	16
Chapter 2: Software Installation	18
Overview	18
Installing ArcSight Management Center	20
Prerequisites for Installation	20
Installation Steps	21
GUI Mode Installation	21
Console Mode Installation	23
Silent Mode Installation	24
About Licenses for Silent Mode Installations	24
Generating the Silent Install Properties File	24
Installing Using the Generated Properties File	26
Next Steps After Installation	26
Enabling/Disabling ArcSight Management Center as a System Service	27
Starting Services Automatically for a Non-Root Installation	27
Configuring Firewall Rules	28
Configuring the Firewall on ArcSight Management Center Appliance	29
ArcSight Management Center Operations	30
Connecting to the ArcSight Management Center User Interface	30
ArcSight Management Center Processes	31
The ArcSight Management Center Daemon (arcmcd)	31
Uninstalling Software ArcSight Management Center	32
Uninstalling in GUI Mode	32
Uninstalling in Console Mode	33
Uninstalling in Silent Mode	33
Installing the ArcSight Management Center Agent	33
ArcSight Management Center Agent Operations	35
Uninstalling the ArcSight Management Center Agent	36
Chapter 3: The User Interface	37
Overview	37
The Menu Bar	37

Monitoring Summary	37
Node Management	38
Configuration Management	38
User Management	39
Administration	39
Stats (EPS In/Out)	39
Job Manager	39
Site Map	40
History Management	40
 Chapter 4: Dashboard	 41
Overview	41
ArcSight Management Center Dashboard	41
Drilling Down	42
Details and Health History	42
Data Charts	43
ADP Licensed Usage for the Last 30 Days	43
Monitoring Rules	43
Preset Rules	44
Managing Rules	44
Monitoring Rules Parameters	45
Rule Verification	49
Custom Rules Examples	50
Example 1: Warning Breach	50
Example 2: Critical Breach	50
Configuring Email Notifications	51
Example Email Notification	52
Configuring SNMP Notifications	52
Topology View	54
Deployment View	55
Prerequisites for Instant Connector Deployment	56
For Windows Platforms Only	56
Instant Connector Deployment	57
If the SSH certificate changes... ..	58
About Connectors in Event Broker (CEB)	58
Deploying a Connector in Event Broker (CEB)	59
SecureData Encryption	59
Editing a CEB	60

Undeploying CEBs	60
Chapter 5: Managing Nodes	61
Overview	61
Node Management	62
The Navigation Tree	62
The Management Panel	63
Management Tabs	63
Tab Controls	64
The Locations Tab	64
The Hosts Tab	65
The Containers Tab	66
The Connectors Tab	68
The Connector Summary Tab	69
Connector Data	69
Connector Parameters	69
Table Parameters (WUC Connectors Only)	70
Destinations	70
The ConApps Tab	71
The Loggers Tab	71
The ArcMCs Tab	72
The EB Nodes Tab	73
The Collectors Tab	73
Locations	74
Adding a Location	74
Editing a Location	74
Viewing All Locations	75
Deleting a Location	75
Hosts	76
About Adding a Host	76
Prerequisites for Adding a Host (for each Host Type)	77
Node Authentication Credentials	80
Managing SmartConnectors on ArcMC	81
Preparing to add Event Broker (2.01 or earlier) as a host	81
Adding a Host	82
Adding a Host with Containers	83
Importing Multiple Hosts	83
Prerequisites for Importing Multiple Hosts	83
CSV File Format	83

Host Field Values	84
Import Hosts Procedure	85
Import Hosts Job Logs	86
Exporting Hosts	87
Viewing All Hosts	87
Viewing Managed Nodes on a Host	88
Deleting a Host	88
Moving a Host to a Different Location	88
Updating (or Installing) the ArcMC Agent	89
Scanning a Host	89
The Scan Process	90
Downloading and Importing Host Certificates	91
Updating Host Credentials	91
Regenerating your Marketplace Certificate	92
 Chapter 6: Managing ArcSight Products	 94
Overview	94
Managing Connector Appliances (ConApps)	94
Rebooting a ConApp	95
Shutting Down a ConApp	95
Editing or Removing a Configuration for a ConApp	95
Setting a Configuration on ConApps	96
Managing Other ArcSight Management Centers	97
Rebooting an ArcMC	97
Shutting Down an ArcMC	97
Editing or Removing a Configuration for ArcMC	98
Upgrading ArcMC	98
Remote Upgrade Using Node Management	99
Local Upgrade of ArcMC	99
Setting a Configuration on Managed ArcMCs	100
Managing SmartConnectors on ArcMC	100
Managing Loggers	101
Rebooting a Logger	101
Shutting Down a Logger	102
Editing or Removing a Configuration for a Logger	102
Upgrading a Logger	102
Setting a Configuration on Loggers	104
Managing Containers	104
Viewing All Containers	105

Viewing Connectors in a Container	105
Editing a Container	105
Deleting a Container	106
Updating Container Properties	106
Changing Container Credentials	106
Sending a Command to a Container	107
Upgrading All Connectors in a Container	107
Modifying logger.properties	108
Restarting a Container	109
Viewing Container Logs	110
Deleting a Container Log	110
Enabling FIPS on a Container	111
Enabling FIPS Suite B on a Container	112
Adding a Connector to a Container	112
Running Logfu on a Container	113
Managing Certificates on a Container	113
Adding CA Certificates to a Container	114
Removing CA Certificates from a Container	114
Adding a CA Certs File to a Container	115
Enabling or Disabling a Demo Certificate on a Container	116
Adding Multiple Destination Certificates to a Container	116
Viewing Certificates on a Container	117
Resolving Invalid Certificate Errors	117
Running Diagnostics on a Container	117
Managing Connectors	118
Viewing All Connectors	118
Adding a Connector	119
Prerequisites	119
Editing Connector Parameters	121
Updating Simple Parameters for a Connector	121
Updating Table Parameters for a Connector	122
Updating Simple and Table Parameters for Multiple Connectors	122
Managing Destinations	123
Adding a Primary Destination to a Connector	123
Adding a Failover Destination to a Connector	124
Adding a Primary or Failover Destination to Multiple Connectors	125
Removing Destinations	126
Re-Registering Destinations	127
Editing Destination Parameters	127
Editing Destination Runtime Parameters	128

Managing Alternate Configurations	129
Defining a New Alternate Configuration	129
Editing an Alternate Configuration	130
Editing Alternate Configurations in Bulk	130
Sending a Command to a Destination	130
Deleting a Connector	131
Sending a Command to a Connector	131
Running Logfu on a Connector	131
Enabling SecureData Encryption on Managed Connectors	132
Remote File Systems	132
Managing a Remote File System	132
Changing the Network Interface Address for Events	135
Developing FlexConnectors	135
Editing FlexConnectors	138
Sharing Connectors in ArcExchange	138
Packaging and Uploading Connectors	139
Downloading Connectors	141
Configuration Suggestions for Connector/Collector Types	142
Included FlexConnectors	143
Configuring the Check Point OPSEC NG Connector	143
Adding the MS SQL Server JDBC Driver	146
Adding the MySQL JDBC Driver	146
Chapter 7: Managing Configurations	148
Overview	148
Configuration Management	149
The Configurations Table	149
The Details Tab	150
General	150
Properties	150
The Subscribers Tab	151
Non-Compliance Reports	152
Creating a Subscriber Configuration	152
Editing a Subscriber Configuration	153
Deleting a Subscriber Configuration	153
Importing a Subscriber Configuration	154
Managing Subscribers	155
Viewing Subscribers	156
Adding a Subscriber	156
Unsubscribing a Subscriber	157

Pushing a Subscriber Configuration	157
Push Validation	158
Common Causes for Push Failure	158
Push Remediation	159
Checking Subscriber Compliance	159
Comparing Configurations	160
Configuration Management Best Practices	161
Subscriber Configuration Types	162
Connector Configuration Types	162
BlueCoat Connector Configuration	162
FIPS Configuration	163
Map File Configuration	163
Parser Override Configuration	164
Syslog Connector Configuration	164
Windows Unified Connector (WUC) External Parameters Configuration	164
Limitations to WUC External Parameters Configurations	165
Windows Unified Connector (WUC) Internal Parameters Configuration	166
Limitations to WUC Internal Parameters Configurations	166
ArcMC/Connector Appliance Configuration Types	167
ArcMC/Connector Appliance Configuration Backup Configuration	167
Destination Configuration Types	168
Destination Configuration Parameters	168
Networks and Zones	169
Logger Configuration Types	169
Logger Configuration Backup Configuration	170
Logger Connector Forwarder Configuration	170
Logger ESM Forwarder Configuration	171
Logger Filter Configuration	172
Logger SmartMessage Receiver Configuration	173
Logger Storage Group Configuration	173
Logger TCP Forwarder Configuration	174
Logger Transport Receiver Configuration	175
Logger UDP Forwarder Configuration	176
System Admin Configuration Types	177
Authentication External	177
Authentication Local Password	178
Authentication Session	179
DNS Configuration	179
FIPS Configuration	180
Network Configuration	180

NTP Configuration	180
SMTP Configuration	181
SNMP Poll Configuration	181
SNMP Trap Configuration	181
Initial Configuration Management	182
Importing an Initial Configuration	183
Pushing an Initial Configuration	184
Deleting an Initial Configuration	185
Event History	186
Managing Logger Event Archives	186
Managing Event Archives	187
Managing Logger Peers	188
Viewing Peers or Peer Groups	188
Adding or Removing Peers	189
Importing a Peer Group	189
Edit a Peer Group	190
Pushing a Peer Group	190
Deleting a Peer Group	190
Managing Event Broker	191
About Topics	191
Adding a Topic	191
About Routes	192
Creating a Route	192
Editing a Route	193
Deleting a Route	194
Deployment Templates	194
Managing Deployment Templates	194
Additional Files	195
Managing Collectors	196
Updating Collector Properties	197
Retrieving Collector Logs	197
Updating Collector Parameters	198
Updating Collector Destinations	198
Updating Collector Credentials	198
Restarting Collectors	199
Deleting Collectors	199
Chapter 8: Managing Users on Managed Products	200
Overview	200

User Management Workflow	201
Users and User Lists	201
Permission Groups	203
Roles	205
Node Lists	206
Associations	207
Compliance Report	209
 Chapter 9: Managing Backups and Restores	210
Overview	210
Backup	210
Restore	211
 Chapter 10: Snapshots	213
Overview	213
Creating a Snapshot	213
 Chapter 11: Logger Consumption Report	215
 Chapter 12: Managing Repositories	217
Overview	217
Logs Repository	218
Uploading a File to the Logs Repository	218
CA Certs Repository	218
Uploading CA Certificates to the Repository	219
Removing CA Certificates from the Repository	219
Upgrade Files Repository	220
About the AUP Upgrade Process	220
Uploading an AUP Upgrade File to the Repository	220
Removing a Connector Upgrade from the Repository	221
Content AUP Repository	221
Applying a New Content AUP	221
Applying an Older Content AUP	222
Emergency Restore	222
User-Defined Repositories	223

Creating a User-Defined Repository	223
Retrieving Container Files	225
Uploading Files to a Repository	225
Deleting a User-Defined Repository	225
Updating Repository Settings	226
Managing Files in a Repository	226
Retrieving a File from the Repository	226
Uploading a File from the Repository	226
Removing a File from the Repository	227
Pre-Defined Repositories	227
Settings for Backup Files	227
Settings for Map Files	228
Settings for Parser Overrides	229
Settings for FlexConnector Files	229
Settings for Connector Properties	230
Settings for JDBC Drivers	231
Backup Files	231
Adding Parser Overrides	232
Chapter 13: System Administration	234
System	234
System Reboot	234
Network	235
System DNS	235
Hosts	235
NICs	236
Static Routes	237
Time/NTP	238
SMTP	239
License & Update	240
Updating the Appliance	240
Updating the License File	240
Process Status	241
System Settings	241
SNMP	242
SNMP Configuration	242
Viewing SNMP System Information	243
SSH Access to the Appliance	244
Enabling or Disabling SSH Access	245
Connecting to Your Appliance Using SSH	245

Diagnostic Tools	245
Display I/O Statistics	246
Display file	246
Display network connections	247
Display network interface details	248
Display network traffic	248
Display process summary	249
Display routing table	249
Edit text file	250
List directory	250
List open files	250
List processes	251
Ping host	251
Resolve hostname or IP Address	251
Scan network ports	252
Send signal to container	252
Tail file	252
Trace network route	253
Logs	253
Audit Logs	253
Configuring Audit Forwarding	254
For Software ArcSight Management Center	254
For ArcSight Management Center Appliance	254
Configuring Audit Forwarding to a Specific Destination	255
Storage	255
RAID Controller/Hard Disk SMART Data	255
FTP	256
Models Supporting FTP	257
Enabling FTP	257
Adding a Subdirectory	258
Processing Log Data Received via FTP	259
Using FTPS (FTP over SSL)	259
Using FTPS with Blue Coat ProxySG	259
Security	260
SSL Server Certificate	261
Generating a Self-Signed Certificate	261
Generating a Certificate Signing Request (CSR)	262
Importing a Certificate	264
SSL Client Authentication	265
Uploading Trusted Certificates	265

Uploading a Certificate Revocation List	265
Enabling Client Certificate Authentication	266
FIPS 140-2	266
Users/Groups on ArcMC	267
Authentication	267
Sessions	267
Local Password	268
Users Exempted From Password Expiration	270
Forgot Password	270
External Authentication	271
Local Password	271
Client Certificate Authentication	271
Client Certificate and Local Password Authentication	272
LDAP/AD and LDAPS Authentication	273
RADIUS Authentication	274
Local Password Fallback	275
Login Banner	276
User Management	277
Users	277
Reset Password	279
Groups	280
System Admin Groups	280
ArcSight Management Center Rights Groups for ArcSight Management Center	281
Managing a User Group	281
Change Password	282
Appendix A: Audit Logs	284
Audit Event Types	284
Audit Event Information	284
Application Events	285
Platform Events	291
System Health Events	295
SNMP Related Properties	295
Appendix B: Destination Runtime Parameters	299
Appendix C: Special Connector Configurations	307
Microsoft Windows Event Log - Unified Connectors	307

Change Parser Version by Updating Container Properties	308
SSL Authentication	309
Database Connectors	309
Add a JDBC Driver	310
API Connectors	311
File Connectors	312
Syslog Connectors	312
Appendix D: Setting Up Your ArcSight Management Center Appliance	314
Appendix E: Restoring Factory Settings	318
Overview	318
Factory Restore Using HPE System Restore	318
Factory Restore Using Acronis True Image	320
Appendix F: SuperSchema	322
Appendix G: The Topology View and Unmanaged Devices	328
Send Documentation Feedback	331

Chapter 1: ArcSight Management Center Overview

The following topic is discussed here.

- **New Features and Enhancements**16

ArcSight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective manner.

ArcMC offers these key capabilities:

- **Management and Monitoring:** deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, Collectors, other ArcMCs, and Event Broker.
- **SmartConnector Hosting:** for the hardware appliance, as a platform to host and execute SmartConnectors

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies.
- Increased level of accuracy and reduction of errors in configuration of managed nodes.
- Reduction in operational expenses.

Caution: Customers may not alter any code related to the ArcMC product without direction from ArcSight support, and customization of the code is not supported by ArcSight.

New Features and Enhancements

This version of ArcMC includes the following new features and enhancements:

- **Instant Connector Deployment:** Deploy connectors and Collectors directly in the Deployment View where needed with just a few clicks, using the new Deployment Templates feature.
- **Deployment View:** The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations. As your environment scales to thousands of source devices, you can model subsystems, and datacenters can quickly trace issues and drill down on details.
- **Support for Connectors in Event Broker (CEB):** ArcMC now includes the Connectors in Event Broker (CEB) feature, which collects raw data through a source topic in Event Broker. Raw events are

sent to this source topic from a Collector device. CEBs enable event normalization and processing to be moved directly to Event Broker.

- **ArcSight Secure Data Add-On Integration:** Deploy the ArcSight Secure Data Add-On encryption client to connectors and Collectors as part of Instant Connector Deployment. Events will be displayed in encrypted format on the ESM console.

Note: Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features**. These features are provided for your testing and evaluation only and must not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.** We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

Chapter 2: Software Installation

This chapter describes how to install Software ArcSight Management Center and the ArcSight Management Center Agent.

The following topics are discussed here.

• Overview	18
• Installing ArcSight Management Center	20
• ArcSight Management Center Operations	30
• Installing the ArcSight Management Center Agent	33
• ArcSight Management Center Agent Operations	35

Overview

The complete process of installing Software ArcSight Management Center includes these steps.

Select an Installation Mode

Select a mode in which to install Software ArcSight Management Center on your selected machine. You should plan to install as the root user. In addition, during the installation process, ArcMC will prompt you for a user name, under which the application will be started.

You can install Software ArcSight Management Center in these modes:

- **GUI:** In GUI mode, a wizard steps you through the installation and configuration process. For detailed instructions, see ["Installation Steps" on page 21](#).

Note: If you are using a Windows system to connect to the machine where Software ArcSight Management Center is to be installed, and prefer to install in GUI mode, you must connect using an X Window client, such as **Xming for Windows**.

- **Console:** In Console mode, a command-line process steps you through the installation and configuration process. See ["Installation Steps" on page 21](#) for detailed instructions.
- **Silent:** In Silent mode, the installation process is scripted. There is no need to interact with the installer, as you provide the installation and configuration input through a file. See ["Installation Steps" on page 21](#) for detailed instructions.

Applying your License

A valid license is required for Software ArcSight Management Center. A license file is uniquely generated for each instance of a product; therefore, you cannot use the same license file to install multiple instances of the product.

To obtain your license, follow the instructions in the *Electronic Delivery Receipt* email received from HPE after placing your order.

You will be prompted to install a license during the installation of ArcMC. If no license is provided, an "Instant-On" license will be applied by default. The Instant-On license is valid for 30 days. During this time, you should obtain and apply the correct license from the [HPE Software Entitlement portal](#).

Start as a Service

If installation was performed as a root user, Software ArcSight Management Center can be configured to start as a system service. For more information, see ["Enabling/Disabling ArcSight Management Center as a System Service" on page 27](#)

Make Host Resolvable

For the Apache web process to start, the Software ArcSight Management Center hostname must be resolvable. Add the hostname to either `/etc/hosts` or DNS.

Secure Your Credentials

After initial setup is complete, connect to the application and change the default password to a secure password. To change the default password, follow the instructions in ["Users/Groups on ArcMC" on page 267](#).

Optionally, for additional security, rename the default admin username to a secure name. To change a username, follow the instructions in ["User Management" on page 277](#).

Install the ArcMC Agent (If Required)

Additionally, if you plan to manage one or more Software ArcMCs, Software Connector Appliances or Software Loggers, you will need to install the ArcSight Management Center Agent on each. For more information on manual ArcSight Management Center Agent installation, see ["Installing the ArcSight Management Center Agent" on page 33](#)

No installation is required for ArcMC appliance or the latest versions of software ArcMC and software Logger.

Open Firewall Ports

Open any required ports on your firewall for best functionality. For a list of required open ports, see ["Configuring Firewall Rules" on page 28](#)

Create an Account on the ArcSight Marketplace

The [ArcSight Marketplace](#) is an app store that enables rapid provisioning of your ArcSight SIEM deployment with content updates, trusted security content packages, and best practices.

ArcSight Management Center requires a global administrative account with the ArcSight Marketplace in order to download and perform some content updates. Browse to the Marketplace at <https://marketplace.microfocus.com/arc sight> to set up your administrative account.

Installing ArcSight Management Center

The following section provides instructions to install Software ArcSight Management Center.

- ["Prerequisites for Installation" below](#)
- ["Installation Steps" on the next page](#)
- ["Enabling/Disabling ArcSight Management Center as a System Service" on page 27](#)
- ["Configuring Firewall Rules" on page 28](#)

Prerequisites for Installation

Please note and verify the following prerequisites before beginning the process of installing software ArcMC

Prerequisite	Description
File Descriptors Limit	<p>The host must support a limit of 10240 file descriptors. Perform <code>ulimit -n</code> on the host to determine its current level. If the limit does not equal 10240, then do the following:</p> <ol style="list-style-type: none">1. Open (or create) <code>/etc/security/limits.conf</code>.2. Set these two parameters: * <code>hard nofile 10240</code> * <code>soft nofile 10240</code>3. Save the file.4. Restart your session.
UTF-8 Support	<p>Host must support UTF-8.</p>
Unzip Package	<p>The unzip command path need to be set before installing Software ArcSight Management Center.</p>
Non-Root Account	<p>You can install ArcSight Management Center as a root or non-root user. However, when installing as a root user, a non-root user account is required in order to run some required processes.</p> <ul style="list-style-type: none">• When installing ArcSight Management Center as a root user, you can select the port on which it listens for secure web connections (HTTPS). When installing as a non-root user, the port must be configured to 9000. This value cannot be changed and must be externally accessible.• If ArcSight Management Center is installed as a non-root user, and the host is rebooted, ArcMC services will fail to start automatically. Start them manually with this command: <code><install_dir>/current/arcsight/arcmc/bin/arcmcd start</code> <p>If installed with a non-root account, use an initialization script to launch services automatically. See "Starting Services Automatically for a Non-Root Installation" on page 27.</p>
Time Zone Database	<p>tzdata-2016g or later is required.</p>
OS Upgrade	<p>Upgrade to a supported operating system before performing the ArcMC installation. Refer to the ArcSight Management Center Release Notes, available from the ArcSight software community, for the most current information on supported operating systems, supported browsers, and other technical requirements.</p>

Installation Steps

To begin the installation, select a mode in which to install Software ArcSight Management Center on your selected machine. The three modes available are GUI Mode, Console Mode, and Silent Install.

GUI Mode Installation

In GUI Mode installation, you use the installer wizard to install the application.

To install Software ArcSight Management Center using the GUI mode:

1. Run these 2 commands from the directory where you copied the Software ArcSight Management Center installer:
 - `chmod +x ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin`
 - `./ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin`where <installer_build_number> is the build number of the latest installer.

The installation wizard starts. Review the dialog box, and then click **Next**.

2. Review the License Agreement details, and then scroll down to the end of the License Agreement details. Select **I accept the terms of the License Agreement**. Then, click **Next**.
3. Specify or browse to a folder where you want to install ArcSight Management Center, as shown below. The default installation directory is /opt. However, you should specify a new installation directory in /opt that will easily identify ArcSight Management Center files, such as /opt/arcmc, to distinguish them from files associated with other ArcSight products.
4. Review the summary of installation information on the **Pre-Installation Summary** dialog, and then click **Install**.

The ArcSight Management Center installer begins the installation process.

5. When installation is complete, click **Next** to begin the configuration wizard.
6. If you run the ArcSight Management Center software installer as a root user, the next dialog enables you to specify an existing non-root user and to configure a port through which ArcSight Management Center users will connect through the UI.

For example, you can enter 443, the standard HTTPS port, or any other that suits your needs. If any port other than 443 is specified, users will need to enter the port number in the URL they use to access the ArcSight Management Center UI.

Enter the user name of the non-root user and the HTTPS port number, and then click **Next**. (These values may not be changed later in the process.)

7. After the software is installed, click **Next** to begin ArcSight Management Center initialization.
8. After initialization is complete, click **Done** to launch the ArcSight Management Center Configuration wizard.

Note: The Configuration wizard should launch automatically. If it does not, use this command to launch the wizard:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup
```

9. If you have run the ArcSight Management Center software installer as a root user, the next dialog enables you to configure ArcSight Management Center to run as a system service. By default, ArcSight Management Center runs as a standalone application, requiring a manual launch.

When you install ArcSight Management Center as a root user, a service called `arcsight_arcmc` can be configured, created, and enabled at runlevel 3 and 5.

Additionally, a few libraries are added using `ldconfig`. For a complete list of those libraries, see `/etc/ld.so.conf.d/arcsight_arcmc.conf` and `<install_dir>/current/arcsight/install/ldconfig.out`.

10. You have installed ArcSight Management Center. Click **Start ArcSight Management Center Now**, or click **Start ArcSight Management Center later**, and then click **Finish**.

If you have selected to start ArcSight Management Center later, read the information in "[The ArcSight Management Center Daemon \(arcmcd\)](#)" on page 31 to understand how to start ArcSight Management Center at a later time.

11. If you selected **Start ArcSight Management Center Now**, click **Finish** to exit the wizard. Alternatively, wait for the next dialog which provides the URL to access the ArcSight Management Center interface.

ArcSight Management Center continues to start services and processes in the background. If you have selected to continue within the wizard, follow the instructions on the dialog or use the instructions in "[Connecting to the ArcSight Management Center User Interface](#)" on page 30 to connect to the ArcSight Management Center.

Console Mode Installation

In Console Mode installation, you use a command-line interface to install the application.

After some initial steps in the CLI, the installation sequence is the same as the one described for the GUI mode install in "[Console Mode Installation](#)" above. Follow the instructions provided for the GUI mode install to complete the installation.

To install Software ArcSight Management Center using the Console mode:

1. Run these commands from the directory where you copied the ArcSight Management Center software:

```
chmod +x ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin
./ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin -i console
```

where `<installer_build_number>` is the build number of the latest installer.

The installation wizard starts in command-line mode.

2. Press **Enter** to continue. Then, follow the prompts to complete installation and configuration.

Note: If ArcSight Management Center is installed in Console mode, it will be uninstalled in Console mode as well. See "[Uninstalling in Console Mode](#)" on page 33 for more information.

Silent Mode Installation

Silent mode enables scripting of the installation process. Before you install ArcSight Management Center in silent mode, create two properties files required for the silent mode installation:

- A file to capture the installation properties
- A file to capture the configuration properties

After you have generated the two files, you need to merge them into one file and use the resulting file for silent mode installations.

About Licenses for Silent Mode Installations

As for any Software ArcSight Management Center installation, each silent mode installation requires a unique license file. Obtain licenses from HPE Customer Support and install them on the machines on which you will be installing in silent mode, or ensure that the location where the license is placed is accessible from those machines.

Generating the Silent Install Properties File

This procedure generates the two properties files and then instructs you to combine them into one file. The resulting file is used for future silent installations.

1. Log in to the machine on which you wish to generate the installation properties file.
If you want the silent mode installations to be done as root user, log in as root in this step. Otherwise, log in as a non-root user.

2. Run this command:

```
./ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin -r <directory_location>
```

where `<installer_build_number>` is the build number of the installer file, and `<directory_location>` is the location of the directory where the generated properties file will be placed. This cannot be the same location where ArcSight Management Center is being installed.

The properties file *must* be called `installer.properties`.

3. Install ArcSight Management Center in GUI mode, as described in ["Silent Mode Installation"](#) above until you arrive at step 10.

At Step 10 of the installation procedure, do the following:

- a. Click **Previous** instead of clicking **Done** to proceed further.
 - b. Then, click **Cancel** to stop the installation.
4. When the confirmation message appears, click **Cancel**. Click **Quit** to clear this message.
 5. Navigate to the directory location you specified for the `installer.properties` file earlier.

The following is an example of the generated `installer.properties` file.

```
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.
#Choose Install Folder
#-----

USER_INSTALL_DIR=/opt/<arcmc_installation_folder>/<build number>/installdir
#Install
#-----

-fileOverwrite_/opt/<arcmc_installation_folder>/<build
number>/installdir/UninstallerData/Uninstall_ArcSight_Management_Center_
2.1.1ax=Yes
#Intervention Required
#-----
USER_AND_PORT_1=username
USER_AND_PORT_2=443
```

1. Start the configuration wizard with the option to record configuration properties:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup -i recorderui
```

When prompted to enter a file name to capture the configuration properties, enter a meaningful name; for example, `config.properties`, and then browse to choose the same directory as the `installer.properties` file.

2. Step through the configuration wizard, as described starting at **Step 10** of "[Silent Mode Installation](#)" on the previous page.
3. After the configuration properties file is generated, append the contents of this file to the `installer.properties` file generated in the previous procedure, "[Generating the Silent Install Properties File](#)" on the previous page, to create a combined file.

For example, you can use the `cat` command to concatenate both files:

```
cat installer.properties config.properties > <combinedproperties.properties>
```

4. Include the following property in the combined file:

```
ARCSIGHT_CONAPP_SETUP_PROPERTIES=<directory_location>/
<combined_properties_file>
```

where `<directory_location>` is the path of the directory where the combined file is located, and `<combined_properties_file>` is the file name of the combined file you created earlier.

Use the combined file for future ArcSight Management Center silent mode installations, as described in "[Installing Using the Generated Properties File](#)" on the next page below.

Installing Using the Generated Properties File

To install ArcSight Management Center using Silent mode, do the following.

1. Uninstall the previously installed version of ArcSight Management Center, as explained in ["Uninstalling Software ArcSight Management Center" on page 32](#)
2. Make sure the machine on which you install ArcSight Management Center complies with the requirements listed in the ArcSight Management Center Release Notes, and the prerequisites listed in ["Prerequisites for Installation" on page 20](#).
3. Copy the combined properties file you generated previously to the location where you have copied the ArcSight Management Center software.
4. Do one of the following:
 - Edit the `licensePanel.path` property in the silent mode properties file to include the location of the license file for this instance of the installation. (A unique license file is required for each instance of installation.), OR
 - Set the `licensePanel.path` property to point to a file, such as `arcmc_license.zip`. Then, for each instance of the silent mode installation, copy the relevant license file to the location and rename it to `arcmc_license.zip`. Doing so will avoid the need to update the combined properties file for each installation.
5. Run these 2 commands from the directory where you copied the ArcSight Management Center software:
 - `chmod +x ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin`
 - `./ArcSight-ArcMC-2.7.0.<installer_build_number>.0.bin -i silent -f <combined_properties_file>`where `<installer_build_number>` is the build number of the installer file.

The rest of the installation and configuration proceeds silently without requiring further input.

In some cases, a spurious error message may be displayed: `"SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder"`. This is a harmless error and may be ignored.

Next Steps After Installation

Finally, to get started managing products with ArcMC, you need to add hosts to manage. For more information on adding hosts, see ["About Adding a Host" on page 76](#).

Enabling/Disabling ArcSight Management Center as a System Service

If ArcSight Management Center is installed to run as a system service, you can use `arcmcd` to manage ArcMC processes. For more information, see ["The ArcSight Management Center Daemon \(arcmcd\)" on page 31](#).

To enable or disable ArcSight Management Center as a system service:

1. On the menu bar, click **Administration > System Admin**.
2. In the navigation bar, click **Startup Settings**.
3. Under **Software Startup Options**, select **Start as a Service** to enable starting as a system service, or select **Do not start as a service** to disable.
4. Click **Save**.

After enablement, you can reboot (which will automatically restart the service) or start the service manually without a reboot.

Starting Services Automatically for a Non-Root Installation

If ArcSight Management Center is installed as a non-root user, and the host is rebooted, ArcMC services will fail to start automatically. However, you can set them to start automatically by using an initialization script.

Since the initialization script runs as `su`, it does not log to the console.

An example script is shown here. This is only an example. Your own script will need to be tailored for your environment.

```
#!/bin/sh

# ArcMC                Wrapper script for the Arcsight Management Center
# processname:         arcsight_arcmc
# chkconfig:           2345 99 01
# description:         Arcsight Management Center

DAEMON=/<install_dir>/current/arcsight/arcmc/bin/arcmcd
DAEMON_USER=<NonRootUser-with-which-arcmc-was-installed>

# Exit if the package is not installed

[ -x "$DAEMON" ] || exit 0
```

```
if [ $UID -ne 0 ] ; then
echo "You must run this as root."
exit 4
fi
su $DAEMON_USER -c "$DAEMON $1 $2"
exit $?
```

The DAEMON variable is used to specify the directory where `arcmcd` process is running.

The DAEMON_USER variable is used to specify which non-root user ArcMC will run as.

Finally, the `su` command simply wraps your existing script (defined in the variable DAEMON) and passes any parameters to the \$DAEMON script/

To configure an initialization script:

1. SSH to the VM using root user credentials.
2. Go to `/etc/init.d`
3. Enter the command `vi arcsight_arcmcd` to create a service.
4. Enter the text of your script and save the file.
5. Give execute permission for the script using the command `chmod +x arcsight_arcmcd`
6. Register the script using the command

```
chkconfig --add arcsight_arcmcd
```

7. Enter the command `chkconfig | grep arcsight_arcmcd` to determine what the `chkconfig` will report after you add the init script. Expected results:

```
arcsight_arcmcd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Configuring Firewall Rules

Before ArcSight Management Center can receive data, some ports on must be opened through the firewall.

- For Software ArcSight Management Center, you are responsible for setting up the firewall. HPE ArcSight recommends that you configure your firewall so that only the required ports are open.
- For the ArcSight Management Center Appliance, HPE ArcSight provides a script to configure your firewall. See ["Configuring Firewall Rules" above](#) for more information.

You can configure the firewall on your ArcSight Management Center as you would on any server, by editing `iptables-config` and white-listing the appropriate ports. For ArcSight Management Center Appliances only, you can use the provided script to close all but the appropriate ports in your firewall.

Tip: Be sure to update the firewall configuration when you add or remove any service or function that requires an open port, such as FTP, SNMP, or local connector.

After you first install or upgrade ArcMC, configure the firewall to be open only for the following ports, depending on your form factor and install:

Default Inbound Ports

Service	ArcMC Appliance	Software ArcMC root install	Software ArcMC non-root install
ArcMC Agent	7913	7913	7913
FTP	21	N/A	N/A
HTTPS	443	443	9000
NTP	123	N/A	N/A
Remote management of connectors or Collectors	9001-9008	N/A	9001-9008
SSH	22	22	22

Configuring the Firewall on ArcSight Management Center Appliance

Your ArcSight Management Center Appliance includes a script that you can use to configure the firewall. This script looks at your current ArcSight Management Center configuration and decides what ports to keep open. Alternatively, you can configure the firewall on your appliance as you would on any server, by editing `iptables-config` and white-listing the appropriate ports.

When called without arguments, the `/usr/sbin/arcfirewall` script previews and displays the ports that it will keep open, but takes no action to alter the firewall configuration. To alter firewall configuration, use the `-set` option.

To preview the list of ports the script will open:

1. Log into the appliance as root.
2. Run the following command:

```
/usr/sbin/arcfirewall
```

The script displays the ports that it would open, as shown in the following example.

```
[root@myserver ~]# /usr/sbin/arcfirewall
PREVIEW MODE - NO FIREWALL CHANGES...
List of ports that firewall would allow inbound from any IP address:
21/tcp
22/tcp
443/tcp
```

7913/tcp
9001/tcp
9002/tcp
9003/tcp
9004/tcp
9005/tcp
9006/tcp
9007/tcp
9008/tcp
123/udp

To configure the firewall:

1. Log into the appliance as root.
2. Run the following command:

```
[root@myserver ~]# /usr/sbin/arcfirewall --set
```

The script configures the firewall leaving the previewed ports open.

If you configure an ArcMC appliance local container and assign it a network port, and then run `arcfirewall`, the script will detect that the new port should be opened and list it in the preview of ports. You can then run `arcfirewall` with the `--set` option, as described above, to actually open the port.

If `arcfirewall` is not run, and the port not opened, the connector will not receive any events.

ArcSight Management Center Operations

This section details the operation of ArcSight Management Center: how to connect, which processes run while ArcSight Management Center is active, and commands for using the ArcSight Management Center command-line utility (`arcmcd`).

Connecting to the ArcSight Management Center User Interface

Use this URL to connect to ArcSight Management Center:

`https://<hostname or IP address>:<configured_port>`

where `hostname` or `IP address` is the system on which you installed ArcSight Management Center. If ArcSight Management Center was installed as root and the default port was used, then `<configured_port>` is optional.

To login for the first time, use the following default credentials:

Username: `admin`

Password: `password`

For security, change the default credentials immediately after first logging in. For more information on changing credentials, see ["User Management" on page 277](#).

ArcSight Management Center Processes

The following processes run as part of ArcSight Management Center:

- `apache`
- `aps`
- `postgresql`
- `web`

Logging Into ArcMC If the Web Service is Down

If the web service stops, you can connect to ArcMC to restart it.

1. SSH to the ArcMC host.
2. Enter `<arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd stop all`
3. Enter `<arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd status`. Wait for some time until all process status report "Not monitored".
4. Enter `<arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd start all`. Wait for some time until all the process status report "running".
5. Log into the ArcMC web UI as usual.

The ArcSight Management Center Daemon (arcmcd)

`arcmcd` is available only for the software form factor of ArcMC.

The `arcmcd` utility enables a number of management and control tasks for the ArcSight Management Center software process, including starting, stopping and restarting. The syntax to run `arcmcd` is as follows:

```
<install_dir>/current/arcsight/arcmc/bin/arcmcd <command>
```

Where `<install_dir>` is the installation directory of ArcSight Management Center, and `<command>` is a command listed below.

If ArcSight Management Center is installed to run as a system service, you can use `arcmcd` to manage a specific ArcMCprocess.

arcmcd Commands

Command	Description
<code>start</code>	Starts <code>aps</code> , <code>apache</code> , <code>postgresql</code> , and web processes.
<code>stop</code>	Stops <code>aps</code> , <code>apache</code> , <code>postgresql</code> , and web processes.
<code>restart</code>	Restarts <code>aps</code> , <code>apache</code> , <code>postgresql</code> , and web processes.
<code>status</code>	Displays the current status of all processes.
<code>quit</code>	Stops <code>aps</code> , <code>apache</code> , <code>postgresql</code> , and web processes, as well as the ArcSight Management Center application.
<code>start <process_name></code>	Starts the named process. For example, <code>start apache</code> .
<code>stop <process_name></code>	Stops the named process. For example, <code>stop apache</code> .
<code>restart <process_name></code>	Restarts the named process. For example, <code>restart apache</code> .

Uninstalling Software ArcSight Management Center

Uninstall ArcSight Management Center in the same user mode in which the installation was performed. For example, if you performed the installation as root, then you must perform the uninstallation as root

Uninstalling in GUI Mode

To uninstall Software ArcSight Management Center in GUI mode:

1. In the directory where you installed ArcSight Management Center, enter:
`<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.7.0`
2. The uninstall wizard starts. Click **Uninstall** to start uninstalling ArcSight Management Center and follow the prompts in the wizard.
3. After uninstalling, manually delete the `/userdata` directory.

Note: If using GUI mode and uninstalling ArcSight Management Center software over an SSH connection, make sure that you have enabled X window forwarding using the **-X** option, so that you can view the screens of the uninstall wizard.

If using PuTTY, you also need an X11 client on the host from which you are connecting.

Uninstalling in Console Mode

If you installed ArcSight Management Center in Console mode, then, by default, uninstallation occurs in Console mode.

To uninstall in Console mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.7.0`
2. After uninstalling, manually delete the `/userdata` directory.

At the prompt, press **Enter** again to confirm uninstallation. The application will be uninstalled.

Uninstalling in Silent Mode

If you installed ArcSight Management Center in Silent mode, then, by default, uninstallation occurs in Silent mode.

To uninstall in Silent mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.7.0`.
The application will be uninstalled without further interaction.
2. After uninstalling, manually delete the `/userdata` directory.

Installing the ArcSight Management Center Agent

The ArcSight Management Center Agent runs on managed hosts and enables their management by ArcSight Management Center. Whether you need to install the ArcSight Management Center on a managed host depends on the host's form factor, which is summarized in the table and explained in detail below.

Host Type	ArcMC Agent Required?	Agent Installation
ArcMC, Logger, or Connector Appliance hardware form factor (all versions)	Yes	Automatically performed when adding host.
Software Connector Appliance (all versions)	Yes	Manual installation required; perform before adding host.
Software Logger (before version 6.0)	Yes	Manual installation required; perform before adding host.

Host Type	ArcMC Agent Required?	Agent Installation
Software Logger (version 6.0 or later)	Yes	Automatically performed when adding host.
Software ArcMC (before version 2.1)	Yes	Manual installation required; perform before adding host.
Software ArcMC (version 2.1 or later)	Yes	Automatically performed when adding host.
Connector (any)	No	None. ArcMC Agent is not required.
Collector (any)	No.	None. ArcMC Agent is not required.
Event Broker	No	None. ArcMC Agent is not required.

Automatic Installation

The ArcMC Agent is *automatically* installed when adding any of the following host types to ArcMC:

- Any hardware appliance (ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance)
- Software Logger 6.0 or later
- Software ArcMC 2.1 or later

As part of the Add Host process, ArcSight Management Center automatically pushes the ArcSight Management Center Agent installer to the added host, installs the Agent, and then starts the service. The host is then ready to manage in ArcSight Management Center. You will not need to take any manual installation steps. For more information about the Add Host process, see ["About Adding a Host" on page 76](#).

Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Manual Installation

You must perform a *manual* installation of the ArcMC Agent on any of these host types *prior* to adding them to ArcMC for management:

- Software ArcSight Management Center (before version 2.1)
- Software Logger (before version 6.0)
- Software Connector Appliance (all versions)

An ArcMC used to manage products must have an Agent installed with the same version number as the ArcMC. For example, if your ArcMC 2.1 will be used to manage products, then the ArcMC Agent running on that ArcMC must also be version 2.1.

To manually install the ArcSight Management Center Agent:

1. In the directory to where you transferred the installer, run these 2 commands:
 - `chmod +x ArcSight-ArcMCAGENT-2.7.0.<agent_installer_build_number>.0.bin`
 - `./ArcSight-ArcMCAGENT-2.7.0.<agent_installer_build_number>.0.bin LAX_VM <install_dir>/current/local/jre/bin/java`
where `<agent_installer_build_number>` is the build number of the latest installer and `<install_dir>` is the installation directory of the software product.

The installation wizard starts.

2. Review the dialog box, and then click **Next**. The required installation path is the install directory (that is, the same directory where Software Connector Appliance or Software Logger is installed).
3. Follow the prompts to complete the installation. The ArcMC Agent is automatically started upon completion of the installation process.

If the ArcMC Agent fails to install on the localhost, localhost management will not be enabled. To verify correct installation of the Agent, check on the **Hosts** tab under **Issues**. Follow the instructions shown in the tooltip to install the Agent properly and resolve any issues shown.

Connectors, Collectors, and Event Broker

Connectors, Collectors, and Event Broker do not require the installation of the ArcSight Management Center Agent in order to be managed by ArcMC.

ArcSight Management Center Agent Operations

After installation, the `arcmcagent` process runs on the managed host. This process automatically starts after either automatic or manual installation. However, if the Agent stops for any reason, it can be manually started.

To manually start, stop, or restart the Agent on an appliance host:

1. On the managed host, click **Setup > System Admin > Process status**.
2. Select `arcmcagent` from the list of processes.
3. Click **Start**, **Stop**, or **Restart**, as necessary.

On Software ArcMC, Software Connector Appliance, or Software Logger

To manually start or stop the Agent on Software ArcMC, Software Connector Appliance, or Software Logger:

1. Run `<install_dir>/current/arcsight/<conapp|logger|arcmc>/bin/<conappd|loggerd|arcmcd> <start|stop> arcmcagent`

Agent Verification

To verify that the Agent is running on a host, use one of the following procedures:

- In the managed host's GUI, click **Setup > System Admin > Process Status**. The ArcSight Management Center Agent (arcmcagent) will be shown as a process in the running state.
- (For Software ArcMC, Software Connector Appliance, or Software Logger Only) After you install the Agent, run this command at the command line:

```
<install_dir>/current/arcsight/<conapp|logger>/bin/<conappd|loggerd> status
```

The Agent is shown as a service in the running state.

Uninstalling the ArcSight Management Center Agent

To uninstall the ArcSight Management Center Agent, run the following command:

```
<install_dir>/arcmcagent/UninstallerData/Uninstall_ArcSight_Management_Center_Agent_<version number>
```

where `<install_dir>` is the name of the installation directory, and `<version number>` is the version, of the ArcMC Agent.

The Uninstall Wizard will launch. Click **Uninstall** to begin the wizard. When the uninstallation completes, click **Done**.

- Always stop and then uninstall any previous version of the ArcSight Management Center Agent before installing a new version.
- If uninstalling either Software ArcMC, Software Logger, or Software Connector Appliance, make sure that the ArcSight Management Center Agent is uninstalled from the node before beginning the uninstall of the managed product.

Chapter 3: The User Interface

The following topics are discussed here.

• Overview	37
• The Menu Bar	37
• Stats (EPS In/Out)	39
• Job Manager	39
• Site Map	40
• History Management	40

Overview

This chapter provides a general overview of the ArcSight Management Center interface. ArcSight Management Center uses a browser-based user interface. Refer to the ArcSight Management Center Release Notes for the latest information on supported browsers.

The Menu Bar

The menu bar provides access to the main functional components of ArcSight Management Center. The menu bar includes the **Dashboard**, **Node Management**, **Configuration Management**, **User Management** and **Administration** menus.

Monitoring Summary

The Monitoring Summary page displays information on all monitored products.

- The aggregated health status for products of each type is displayed in pie graph format, showing total number of nodes, as well as the number corresponding to each status. A summary table shows the same data in percentage format.
- The management panel displays the **Monitoring Summary** table, showing all products which are currently reporting issues.
- The navigation panel enables you to display a monitoring summary for individual product types in the management panel. Click the product type to display the product's monitoring summary.

For more information on viewing and configuring monitoring, see ["Dashboard" on page 41](#).

Node Management

Use **Node Management** to manage any of the following node types:

- Connectors or Collectors
- Hardware or Software Connector Appliances
- Hardware or Software Loggers
- Hardware or Software ArcSight Management Centers
- Event Broker

For more information on adding and managing nodes, see ["Managing Nodes" on page 61](#). From the same menu, you can also perform selected management tasks on managed ArcSight products. See ["Managing ArcSight Products" on page 94](#).

Configuration Management

Use **Configuration Management** to create and manage node configurations, synchronization (pushing) of configurations across multiple nodes, and expedite the initial configuration of Loggers. You can manage any of these configuration types:

- Subscriber configurations for:
 - ArcSight Management Center
 - Connectors
 - Connector Appliances
 - Destinations
 - Loggers
 - System administration
- Other configurations:
 - Initial configurations for Loggers
 - Logger event archives
 - Management of Logger peers
 - Management of Event Broker

For more information on subscriber configuration management, see ["Managing Configurations" on page 148](#).

For more information on initial configurations, see ["Initial Configuration Management" on page 182](#).

User Management

User management enables you to manage users across all of your managed nodes. You can create and edit users, user lists, their associations, and roles. You can also check to see if each node complies with a list of authorized users on the managing ArcMC.

For more information about user management, see ["Overview" on page 200](#)

Administration

The **Administration** menu contains these items:

- **Backup** enables you to back up your current ArcSight Management Center configuration. For more information, see ["Managing Backups and Restores" on page 210](#).
- **Repositories** enables you to manage repositories that store files, such as logs, certificates, and drivers. For more information, see ["Managing Repositories" on page 217](#).
- **Snapshot** enables you to take a snapshot image of ArcSight Management Center, to produce logs that are useful in troubleshooting. For more information, see ["Snapshots" on page 213](#).
- **Restore** enables you to restore your configuration from a saved backup. For more information, see ["Managing Backups and Restores" on page 210](#).
- **System Admin** describes the system administration tools that enable you to create and manage users and user groups, and to configure security settings for your system. For more information, see ["System Administration" on page 234](#).
- **Consumption Report:** generates a report on Logger data consumption for selected managed nodes.

Stats (EPS In/Out)

The **Stats** menu item shows the total Events Per Second (EPS) in and out from all managed connectors (standalone SmartConnectors and connectors running on managed hosts).

Job Manager

The Job Manager shows all deployment jobs processed in a specified time frame. Using the Job Manager, you can identify issues that occurred during deployments.


The Job Manager shows the following for each job:

- **Name of the Job:** The job name (must be smaller than 255 characters).
- **Started By:** The user who ran the job.

- **Start/End Time:** The start and end time of the job.
- **Status:** Job status. If the job has a status of *Failed*, click **Retry** to re-run the job.
- **Details:** Job details.

Hover over any field to display details about the field in a tooltip. Click the Up/Down arrows at the top of any column to sort data by the selected parameter.

To view the Job Manager:

1. On the menu bar, click the Job Manager (notepad) icon.  By default, the Job Manager displays all deployment jobs for the last 5 days. A red numeral on the Job Manager icon, if any, indicates the number of jobs currently in the In-Progress state.
- To change the time frame for job data displayed, enter the date criteria in the date boxes in the upper right corner, and then click **Show Results**. You may specify any time frame in the last 180 days (6 months).
 - To search for a specific job, enter the search criteria in the **Search** box.
 - If a job is in progress, you can click **Refresh** on the menu bar to refresh the display.

Site Map

For ease of accessibility and convenience, the Site Map links to all pages in the ArcSight Management Center UI.

To access the site map: on the main ArcMC toolbar, click **Site Map**. Select the desired link to navigate.

History Management

History management enables you to quickly and easily access previously-navigated pages. History management is available for Node Management, Configuration Management, User Management pages, and for some Administration pages.

In Node Management, the **navigation tree** shows the full path for any item selected on the tree. Click any node in the path to navigate directly to the corresponding page.

You also can return to any previously-browsed page by clicking the corresponding link in the breadcrumb trail.

In addition, you can use your browser's **Back** and **Forward** buttons to navigate to previously visited pages.

Chapter 4: Dashboard

The following topics are discussed here.

• Overview	41
• ArcSight Management Center Dashboard	41
• Monitoring Rules	43
• Topology View	54
• Deployment View	55

Overview

Using ArcSight Management Center, you can monitor the health status of all managed nodes. You can also configure warnings and alerts for issues of importance to you.

Note: In order for products to be monitored, they must be added as nodes to ArcSight Management Center. For more information on managing nodes, see ["Managing Nodes" on page 61](#).

Monitoring is displayed on the **Dashboard > Monitoring Summary** page. ArcSight Management Center automatically monitors all managed nodes.

You can also configure notifications (email, SNMP, and through audit forwarding) about the status of managed nodes.

ArcSight Management Center Dashboard

ArcSight Management Center monitoring, on the **Dashboard > Monitoring Summary** page, displays the current health history of all managed nodes, both software and hardware.

- Monitored metrics for software nodes (such as Software Logger) include such software parameters as CPU usage, event flow, and disk usage statistics.
- Monitored metrics for hardware appliances (such as Logger Appliance) include both software as well as hardware-related attributes, such as remaining disk space and hardware status.

You can view a complete list of monitored parameters in ["Monitoring Rules Parameters" on page 45](#), and use them in creating your own custom rules. These rules breaches will also be displayed on the Health History and Hardware Status panels. Note that the layout and selection of the data panels in the Monitoring Summary is not customizable.

Drilling Down

You can view the details of problematic nodes, and then take action to rectify any issues.

To view all details of a problematic node, select it in the upper table. The lower table shows issues associated with that node. Each issue is shown with these identifiers:

- **Metric Type:** Metric assigned to the issue.
- **Metric Name:** Name of the metric.
- **First Occurrence:** Local time of the issue's first occurrence.
- **Last Occurrence:** Local time of the issue's last occurrence.
- **Severity:** Issue severity.
- **Description:** Brief description of the issue.

To view details of nodes by severity:

1. On the menu bar, click **Dashboard > Monitoring Summary**.
2. Click the ring meter corresponding to any of the monitored product types, in the portion of the meter corresponding to the severity you wish to view. (For example, to view all nodes currently with Warning status, click the Warning, or yellow, part of the ring.) The corresponding **Severity Issue Summary** is displayed.

3. On the **Severity Issue Summary** page:

The upper table shows a list of all problematic nodes, with the following identifiers:

- **Name:** Node name.
- **Path:** Path to the node.
- **Type:** Type of node.
- **Lead/Breach:** Short summary of the most severe issue reported by the node. The node may be experiencing less severe issues as well.

Details and Health History

To view further health details of a problematic node, including history and status, click **Details**. The data tables show the detailed parameters of the selected node.

The Health History panel will show any rules breaches, including custom rules you have created yourself.

Note: The layout of the panels and selection of the displayed parameters is not customizable.

Data Charts

Each data chart represents values of the parameter over time. Use the drop-down list to change the interval shown from the last 4 hours, the last day, or the last week. Data charts can include any of the metrics shown under the [Valid Values for Metric Types](#) table.

Click the data legend to toggle display of the corresponding line from the chart. Hiding some lines may be helpful to clarify a chart with many lines.

ADP Licensed Usage for the Last 30 Days

Your ADP license entitles you to a specified number of managed products and amount of managed traffic. The **ADP Licensed Usage for the Last 30 Days** panel shows your ADP data usage for the previous month.

The graph shows all traffic in your ADP environment. The default color is green, which indicates that data usage is within your licensed limit.

- Amber indicates periods when your data usage approached your licensed traffic limit.
- Red indicates periods when your data usage exceeded your licensed traffic limit.

The **Active Loggers** indicates the number of ADP Loggers the data from which contributes to the license monitoring report. For more details, you can export the license report to PDF format, which includes data on the last 365 days.

To enable the display of ADP licensed usage:

1. Enable ArcMC as an ADP license server. In the ArcMC toolbar, click **ADP License Server**, then click **Yes**.
2. Upload a valid capacity license to the ArcMC on the **License and Upgrade** page.

To export the license report to PDF format:

1. Click **Export License Report**.
2. The PDF is downloaded to your local system.

Monitoring Rules

Monitoring rules are defined to generate monitoring warnings for each managed product type. ArcMC includes many [preset monitoring rules](#) for your use. You can use these rules as written, or customize them for your own use. In addition, you can [create your own custom monitoring rules](#).

A monitoring rule comprises a set of logical, performance, health, or other criteria. All criteria in the rule are evaluated together to determine the rule's total effect, which generates an alert from ArcMC.

Rules breaches will be displayed in the Warning Severity Issue Summary, which you can view by clicking one of the ring meters on the [Monitoring Dashboard](#).

For example, a rule could check for the number of *input events per second* (criterion #1) that reach a *certain type of device* (criterion #2). Should this number *exceed* (criterion #3) a specified *level* (criterion #4), then a *warning (alert)* should be returned.

Alerts can be delivered by [email](#) or by [SNMP](#), or can be recorded in [audit logs](#).

If [email notifications are configured](#), even with no monitoring rules defined, automatic email alerts are sent indicating when a managed node has gone down or is not reachable. Email alerts are also sent when a down or unreachable node comes back up or becomes reachable again.

For more information on managing and creating rules, see "[Managing Rules](#)" below.

Preset Rules

ArcSight Management Center includes preset rules to assist in monitoring. You can use these preset rules as written or customize them as needed for your own use. You can also [create custom rules](#) of your own.

By default, ArcMC preset rules are disabled. You must enable a preset rule in order for it to apply and trigger alerts.

For customers with previous versions of ArcMC and who already have a list of existing rules, preset rules included in ArcMC are appended to your existing rules.

To review preset rules:

1. Click **Dashboard > Rules**. The Monitoring Rules summary is shown.
2. To view a rule's settings in detail, in the **Name** column, click the rule name.
3. To enable a disabled preset rule, under **Status**, select **Enable**, and then click **Save**.

Managing Rules

To create a custom rule:

1. Click **Dashboard > Rules**.
2. In the toolbar, click **New**.

3. Select values for the [rule parameters](#).
4. Click **Save**.

To edit an existing rule:

1. Click **Dashboard > Rules**.
2. Under **Monitoring Rules**, locate the rule you wish to edit.
3. In the **Name** column, click the rule name.
4. Select new values for the [rule parameters](#), as needed.
5. Click **Save**. Alternatively, click **Save As** to save the edited rule with a new name.

To enable (or disable) a rule:

1. Click **Dashboard > Rules**.
2. In the management panel, under **Monitoring Rules**, select the rule to enable or disable.
3. In the **Name** column, click the rule name.
4. Under **Status**, toggle the status to **Enable** (or **Disable**).
5. Click **Save**.

To delete a rule:

1. Click **Dashboard > Rules**.
2. Under **Monitoring Rules**, select the rule you wish to delete.
3. Click **Delete**.
4. Click **OK** to confirm deletion.

To export all rules to a text file:

1. Click **Dashboard > Rules**.
2. In the toolbar, click **Export**. Your rules are exported to a local text file called `monitor_breach_rules.properties`. and downloaded locally.

Monitoring Rules Parameters

Monitoring rules are defined by rule parameters. The following table describes monitoring rules parameters and their valid values.

Monitoring Rules Parameters

Parameter	Description
Name	Name of the rule. (Max. length 50 characters)
Metric Type	Criterion being measured. For valid values of Metric Type, see the Valid Values for Metric Type table, below. Each metric type has a Value Type constraining the kind of value which may be assigned to it.
Product Type(s)	Managed product type (or types) to which the rule applies. These are automatically selected based on the Metric Type. For example, if you selected a metric type that applied only to hardware, such as Voltage, only products with hardware form factors would be available for selection. You can also deselect types to which to apply the rule, as applicable.
Specific Node Selector	Click View/Choose , and then select one or more specific nodes to which the rule applies. If none are chosen, then the rule applies to all nodes of the selected Product Types.
Severity	Breach severity. Valid values are Healthy, Warning, Critical and Fatal. Thresholds for each of these values are defined by the administrator.
Aggregation	Aggregation function applied to Metric Type data points. Valid values: <ul style="list-style-type: none"> • ANY: any value • AVG: average value (numeric values only) • MIN: minimum value (numeric values only) • MAX: maximum value (numeric values only)
Measurement	A comparison between two criteria. Valid values: <ul style="list-style-type: none"> • GREATER: One field is greater than the other • LESS: One field is less than the other • EQUAL: One field is equal to the other • NOT_EQUAL: Two fields are unequal
Value	Threshold value for comparison. Valid values are dependent on Metric Type. <ul style="list-style-type: none"> • Percentage: Number from 1-100 (with no %-sign). • Numeric: Numeric string. • Boolean: true/false (case-insensitive) • Literal Status: Status of the appliance component, and can be one of the following values: <i>Ok, Degraded, Rebuilding, Failed, Unavailable</i>.
Notify Me	Select one or more notification mechanisms for alerts about the rule (Email , SNMP , or Audit Forwarding).
Status	If Enabled , the rule will apply and produce alerts, as specified in Notify Me . (ArcMC rule presets are Disabled by default.)
Time Range	Evaluation interval, in hours and minutes. The total of hours and minutes must not exceed 168 hours (7 days).
Description	Brief description of the rule. (Max. length 300 characters.)

Note: Compound rules (AND/OR) are not supported.

Valid Values for Metric Type

Value	Description	Value Type
For Connector Appliances or Loggers only		
CPU Usage	CPU usage, as a percentage.	Percentage
JVM Memory	Memory of Java Virtual Machine.	Numeric
Disk Read	Number of reads of the disk.	Numeric
Disk Write	Number of writes to the disk.	Numeric
Network Received	Network traffic received, in MB/sec.	Numeric
Network Sent	Network traffic sent, in MB/sec.	Numeric
All EPS In	Total Events Per Second in.	Numeric
All EPS Out	Total Events Per Second out.	Numeric
For Connectors only		
EPS In	Events Per Second (EPS) in.	Numeric
EPS Out	Events Per Second (EPS) out.	Numeric
Events Processed	Number of events processed.	Numeric
Events Processed (SLC)	Events processed (Since Last Checked).	Numeric
Events Per Second	Events per second.	Numeric
FIPS Enabled	1= FIPS enabled, 0=FIPS disabled.	Boolean
Command Responses Processed	Number of command responses processed.	Numeric
Queue Drop Count	Queue drop count.	Numeric
Queue Rate (SLC)	Queue rate (Since Last Checked).	Numeric
Active Thread Count	Active thread count.	Numeric
For hardware form factor products only		
Fan	Hardware fan status.	Literal Status

Valid Values for Metric Type, continued

Value	Description	Value Type
Disk Space	Hardware disk space status.	Literal Status
Voltage	Hardware voltage status.	Literal Status
Current	Hardware current status.	Literal Status
Temperature	Hardware temperature status.	Literal Status
Power Supply	Hardware power supply status.	Literal Status
RAID Controller	RAID controller status.	Literal Status
RAID Battery	RAID battery status.	Literal Status
Hard Drive	Hard drive status.	Literal Status
For Loggers Only		
Storage Group Usage	Current storage group usage, in bytes.	Numeric
Storage Group Capacity	Current storage group capacity, in bytes.	Numeric
For Event Brokers Only		
Event Broker All Bytes In	All bytes received by the Event Broker cluster.	Numeric
Event Broker All Bytes Out	All bytes transmitted by the Event Broker cluster. Note that due to the replication of each topic, Bytes Out will always exceed Bytes In.	Numeric
Event Broker Disk Usage	Disk usage of Event Broker's individual nodes.	Numeric
Event Broker Memory Usage	Memory usage of Event Broker's individual nodes.	Numeric
Event Broker SP EPS	Count of events per second received by Event Broker's Stream Processor.	Numeric

Valid Values for Metric Type, continued

Value	Description	Value Type
Event Broker Error	Count of events per second waiting to be processed received by Event Broker's Stream Processor which produced an error.	Numeric
Event Broker Lag	Count of events per second waiting to be received by Event Broker's Stream Processor.	Numeric
Event Broker CPU Usage	CPU usage of the Event Broker's individual nodes.	Numeric
Event Broker EPS In	Events per Second received by the Event Broker cluster.	Numeric
For Collectors Only		
Collector CPU Load Average	Average load of Collector CPU.	Numeric
GC Count	Count of Java garbage collection.	Numeric
Restart Count	Number of restarts. (Not available.)	Numeric
Total Memory	Total JVM memory.	Numeric
Event Volume	Syslog lines received by the Collector, and custom filtering, like messages filtered out.	Numeric
Used Memory	JVM memory in use.	Numeric

Rule Verification

It is possible to create syntactically valid rules that return confusing or meaningless alerts. For example, you could create a syntactically valid rule to trigger an alert if CPU usage is below 101%, but this rule would not return useful alerts (since it would alert you constantly).

Always verify your rules to ensure that they return meaningful values, to help you best detect problems and issues.

Note: Custom Polling Intervals: ArcSight Management Center uses three polling intervals (4 hours, 1 day, and 1 week) associated with metric data archive types across ArcSight products. These intervals can be adjusted for proper usage, if required.

It is strongly recommended that you adjust these intervals only if you fully understand the impact of the changes.

Polling intervals can be specified in the file `logger.properties` using a text editor.

- 4-hour data (minimum allowed interval 1 minute):
`monitoring.data.poll.4hour.cron=10 0/3 * * * ?`
This property indicates a poll at 3 minute intervals.
- 1-day data (minimum allowed interval 5 minutes):
`monitoring.data.poll.1day.cron=15 0/10 * * * ?`
This property indicates a poll at 10 minute intervals.
- 1-week data (minimum allowed interval 1 hour):
`monitoring.data.poll.1week.cron=20 2 * * * ?`
This property indicates a poll at 2 hour intervals.

After making the changes and saving the edited file, a server restart is required for the changes to take effect.

Custom Rules Examples

Shown here are examples of custom monitoring rules.

Example 1: Warning Breach

This example specifies the following Warning condition:

“Generate a Warning breach if the average CPU usage of any ArcMC in the past 30 minutes is greater than 70%.”

Name: ArcMC Warning

Metric Type: CPU Usage

Product Type: ArcMCs

Severity: Warning

Aggregation: AVG

Measurement: GREATER

Value: 70

Timespan: 30 minutes

Example 2: Critical Breach

Example 2 specifies the following Critical condition:

“Generate a Critical breach if the Power Supply fails on any Logger Appliance in the past hour.”

Name: Logger Warning

Metric Type: Power Supply

Product Type: Loggers

Severity: Critical

Aggregation: ANY

Measurement: EQUAL

Value: Failed

Timespan: 60 minutes

Configuring Email Notifications

Email notifications will inform recipients about monitored nodes being down or out of communications.

Note: Email alerts do not include issues with connectors or Collectors. However, containers may be the subject of email alerts.

Before configuring email notifications, ensure that values are specified for your SMTP settings under **System Admin > System > SMTP**. For more information on SMTP settings, see ["SMTP" on page 239](#).

Once configured, email notifications must be configured for each of the notification rules you wish to trigger an alert.

To configure email notifications:

1. In a text editor, open the file `.../userdata/arcmc/logger.properties`. (If the file does not exist, you can create it in a text editor. When creating the file, ensure that it is owned by the non-root user.)
2. Add a new line with the new property named `monitoring.notification.emails` and a value equal to a comma-separated list of email addresses of all administrators you intend to receive notifications. For example, this value would send email alerts to `address1@example.com` and `address2@example.com`:

```
monitoring.notification.emails=address1@example.com,  
address2@example.com
```

3. Save the modified `logger.properties` file.
4. Restart the ArcMC web process.
5. In the rules editor, open the notification rule you wish to trigger an email alert, and under **Notify Me**, select *Email*.

Example Email Notification

An example of the email sent to recipients is shown here.

<URI> refers to the URI of a problematic node.

NodeN is the hostname of a problematic node.

This information is found on the **Hosts** tab under Node Management.

Subject: <Email title>

The following nodes are either down or not reachable from ArcSight Management Center:

//Default/<URI>/<Node1>

//Default/<URI>/<Node2>

Configuring SNMP Notifications

SNMP notifications will send SNMP traps about monitored nodes being down or out of communications.

To configure SNMP notifications on ArcMC appliance:

1. Under **Administration > System Admin > System > SNMP**, enable SNMP. Then, enter values for port, SNMP version, and other required settings for your SNMP environment.
2. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me**, select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Enabling SNMP on Software ArcMC

Software ArcMC does not include UI controls for SNMP configuration. Instead, take these steps to configure Software ArcMC for SNMP notifications and monitoring.

To enable SNMP notifications on a software host:

1. Make sure following RPM packages are installed on the system: `net-snmp`, `net-snmp-utils`, `net-snmp-libs`, `lm_sensors-libs`.
2. Enable the SNMP service by entering: `chkconfig snmpd on`
3. Start the SNMP service by entering: `service snmpd start`

4. In a text editor, create a file `/opt/arcsight/userdata/platform/snmp.properties` with the following parameters. Items in brackets `<>` indicate you should substitute values appropriate for your own environment.

```
snmp.enabled=true

snmp.version=V3

snmp.port=161

snmp.v3.authprotocol=SHA

snmp.v3.authpassphrase=<password>

snmp.v3.privacyprotocol=AES128

snmp.v3.privacypassphrase=<password>

snmp.user=<SNMP username>

snmp.community=public

snmp.system.location=<SNMP location>

snmp.system.name=ArcMC Node 247

snmp.system.contact=<your support email address>

snmp.trap.enabled=true

snmp.trap.version=V3

snmp.trap.port=162

snmp.trap.nms=<IP address of NNMI>

snmp.trap.user=<SNMP trap user name>

snmp.trap.community=public

snmp.trap.v3.authprotocol=SHA

snmp.trap.v3.authpassphrase=<password>

snmp.trap.v3.privacyprotocol=AES128

snmp.trap.v3.privacypassphrase=<password>
```

5. Run the script `arcsight_snmpconf` script as a root user, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home> /userdata/platform/snmp.properties trap
```

6. Run the script a second time, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home> /userdata/platform/snmp.properties poll
```

This script will setup `/etc/snmp/snmpd.conf` file and restart the SNMP service.

7. Restart SNMP services: `service snmpd restart`

8. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me**, select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Topology View

The Topology View displays your end-to-end data flow in browseable format. Shown are the logical relationships between network devices (event producers), connectors and Collectors, and their destinations in each of your ArcMC locations.

As your environment scales to thousands of source devices, you can use logical groupings (locations) to model subsystems, and datacenters can quickly trace issues and drill down on details.

To display the Topology View, click **Dashboard > Topology View**.

The left column highlights the current topology view. The available views are based on the [locations defined in ArcMC](#).

The health status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

Each of monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.

A green bubble shows the active devices, that is devices which are receiving events. A red bubble, if present indicates the number of inactive events.

Click either a green or red bubble to view a details page showing the active or inactive hosts for the Product type.


The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

The **Connectors/Collectors** area shows connectors in the current topology view.

- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any) and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately following adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data

from the new connector is collected.

- Connectors displayed with the  symbol are included in a different location from the one currently selected for viewing.

The **Destinations** area shows connector destinations.

- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Deployment View** to show your environment's [Deployment View](#).

If any are present, unmanaged connectors (or other nodes) in your network are noted as such in the Topology View. ArcMC will have no visibility into unmanaged connectors, nor any visibility of traffic from those nodes. Various scenarios for such views, and the results of each scenario, are detailed [here](#). To get the most complete and accurate picture of your network, you are strongly encouraged to use ArcMC to manage all connectors which are part of your logical topology.

Deployment View

The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations.

To display the Deployment View, click **Dashboard > Deployment View**.

The left column highlights the current deployment view. The available views are based on the physical hosts.

The health status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

Each of monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.


A green bubble shows the active devices, that is devices which are receiving events. A red bubble, if present indicates the number of inactive events.

Click either a green or red bubble to view a details page showing the active or inactive hosts for the Product type.

The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

The **Connectors** area shows connectors and Collectors in the current topology view.

- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any) and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately following adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data from the new connector is collected.
- Connectors displayed with the  symbol are included in a different location from the one currently selected for viewing.

The **Destinations** area shows connector destinations.

- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Topology View** to show the **topological** relationships in your environment.

Prerequisites for Instant Connector Deployment

To enable Instant Connector Deployment, you must first set up one or more **deployment templates**.

In addition, Instant Connector Deployment must be performed by an account with root access to the remote VMs.

Note: One-click instant connector deployment is supported for accounts using SSH key authentication, but not supported for SSH with passphrase authentication. To enable SSH key authentication, the SSH key needs to be set up between a non-root user of ArcMC and a user of the remote host who has the ability to perform some privileged operations using `sudo`, such as creating connector users, or running scripts that allow the connector to run as a service.

For Windows Platforms Only

For Instant Connector Deployment on Windows platforms, only the local admin account is supported for deployment.

In addition, the following preparatory steps are required when deploying on a Windows VM.

1. Enable PowerShell 4.0 or higher

<https://www.microsoft.com/en-us/download/details.aspx?id=40855>

2. Enable and configure PowerShell Remoting, with CredSSP authentication

http://docs.ansible.com/ansible/latest/intro_windows.html#windows-system-prep

Pass the -EnableCredSSP switch to enable CredSSP as an authentication option:

```
ConfigureRemotingForAnsible.ps1 -EnableCredSSP
```

3. Enable TLS 1.2

http://docs.ansible.com/ansible/latest/intro_windows.html#credssp-and-tls-1-2

Instant Connector Deployment

Instant Connector Deployment enables rapid installation of connectors or Collectors where you need them in your environment. You perform instant deployment right from the Deployment View. Ensure you have set up 1 or more [deployment templates](#) before performing instant connector deployment.

Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features**. These features are provided for your testing and evaluation only and must not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.** We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

To instantly deploy a connector or Collector:

1. Click **Dashboard > Deployment View**.
 2. In the **Connectors** column label, click +, then select **Add Connector** or **Add Collector**.
 3. On the **Add Connectors** (or **Add Collectors**) dialog, enter values for the connector to be added. Any fields marked with an asterisk (*) are required. Note that your selected deployment template may populate some fields automatically, but you may overwrite the values in these fields, if needed, for a particular deployment. **Exception:** you may only use the latest version of the connector you have [uploaded to the repository when you set up deployment templates](#). You can add multiple destinations for each connector if needed.
- **Collector Hostname:** The Collector hostname must match the hostname of the remote machine. If the remote machine does not have proper DNS /hostname setup correctly, enter the IP address of the remote machine as the hostname.
 - **Collector Destination:** A Collector's destination must be the eb-con-syslog topic on your ArcMC-managed Event Broker.
 - **ArcSight Secure Data Add-On Enablement:** To enable the ArcSight Secure Data Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. For more information on enabling the SecureData Add-On, see ["SecureData Encryption" on page 59](#).

4. To add multiple connectors (or Collectors) of the same type, click **Clone**. Then enter the information unique to the new connector (or Collector). When deploying multiple connectors, if any specified parameters (such as port number) are invalid, the deployment of all connectors in the job will fail.
4. Click **Install**. The connector or Collector is deployed. Alternatively, click **Add** to add more connectors to the deployment job.

Note: Instant Connector Deployment (including Collectors) is not supported from RHEL/CentOS 6.9 to a remote Windows host.

You can track and manage deployment jobs and issues using the [Job Manager](#).

Note: If you later connect to a host where connectors or Collectors were installed through Instant Deployment, and run the Connector setup wizard from the command line, you should run agent setup by setting the mode with option, -i, such as: `./runagentsetup.sh -i console`, where options are swing, console, silent, and so on. For more information on options, see the SmartConnect User's Guide.

If the SSH certificate changes...

If the connector VM is redeployed, its SSH certificate will change and you will no longer be able to use Instant Connector Deployment to deploy connectors to the VM. In this case, take the following steps to re-enable Instant Connector Deployment to the re-deployed VM.

1. Connect to the ArcMC's VM.
2. Change to the directory `/home/<non root user>/.ssh`
3. Open the file `known_hosts`.
4. Delete the line with the IP or hostname of the Connector's VM.
5. Save the file.

About Connectors in Event Broker (CEB)

Note: Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features**. These features are provided for your testing and evaluation only and must not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.** We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

Deploying a Connector in Event Broker (CEB)

Ensure you have added an Event Broker host for a supported version (2.10 or later) before adding any CEBs. You can deploy up to 3 syslog connectors directly to a managed Event Broker.

To deploy a CEB:

1. Click **Dashboard > Deployment View**.
2. In the **Event Broker** column, next to the managed Event Broker icon, click the **+** icon.
3. On the **Deploy CEB** dialog, in **CEB Name**, enter a name for the CEB. The name must be smaller than 256 characters in length.
4. Under **Destination Topics**, click the down arrow, then select one or more destination topics (CEF or binary) for the CEB.
5. Click **Deploy**. The CEB deployment job status can be viewed in [Job Manager](#).

Once deployed, the CEB will be displayed in Node Management on the Connectors tab, and in the Topology and Deployment View drilldown under the source topic.

Note: Destination topics must always be grouped the same for multiple CEBs. For example, if a CEB is sending events to both eb-cef and eb-esm topics, then any other CEB that sends events to one of these topics must also send events to the other topic, or events will be duplicated.

SecureData Encryption

To enable SecureData encryption, you must provide the SecureData server details in the [Deployment Templates](#) for a connector.

If any proxy settings are required, these must also be provided in the Deployment Template.

To explicitly specify that no proxy be used for the SecureData client, no parameters are needed in the Deployment Template. In addition, edit the file `/etc/profile.d/proxy.sh` (or its equivalent on Windows VM) and add/edit the line “`export no_proxy` and `export NO_PROXY`” with your SecureData server details.

If your SecureData client needs a certificate, then upload the valid certificate to ArcMC's cacerts repository when creating the deployment template.

After all settings are configured, and a connection is ensured from the connector host to the SecureData server, you can deploy the connector using the [Instant Connector Deployment](#) process.

Warning: SecureData settings may only be updated once. Once encryption is turned on, it may not be turned off. Make sure you wish to use encryption before activating it.

Editing a CEB

To edit a CEB:

1. Click **Dashboard > Deployment View**.
2. In the **Event Broker** column, next to the managed Event Broker icon, click the edit (pencil) icon.
3. On the **CEB Parameters** dialog, modify the name or destination topics, as needed.
4. Click **Redeploy**. The CEB is re-deployed. The job progress can be viewed in [Job Manager](#).

Undeploying CEBs

To undeploy one or more CEBs:

1. Click **Dashboard > Deployment View**.
2. Click on the Event Broker box to drill down.
3. Click the edit (pencil) icon.
4. On the **CEB Parameters** dialog, click **X** next to any CEBs to be undeployed.
5. Click **Redeploy**. The job progress can be viewed in [Job Manager](#).

Chapter 5: Managing Nodes

The following topics are discussed here.

• Overview	61
• Node Management	62
• The Navigation Tree	62
• The Management Panel	63
• Locations	74
• Hosts	76

Overview

A *node* is a networked ArcSight product that can be centrally managed through ArcSight Management Center. Each node is associated with a single networked host which has been assigned a hostname, an IP address, or both.

Node types can include any of the following ArcSight products:

- Connector Appliances or Software Connector Appliances
- Logger Appliances or Software Loggers
- Containers, connectors, or Collectors
- Other ArcSight Management Centers, either software or Connector Hosting Appliances
- Event Broker

A single host, such as a single deployed Event Broker, can comprise multiple nodes for management purposes. In addition, a node can be in a parent or child relationship with other nodes.

You can perform any of the following node management tasks:

- View managed nodes by location, by host, or by node type.
- Add, view, edit, and delete locations for hosts.
- Add nodes from a host, import hosts from a CSV file, view and delete hosts, view all hosts in a location, update software on hosts, move hosts to different locations, and scan hosts for new connectors or containers.

For more information on adding hosts, see ["About Adding a Host" on page 76](#).

Node Management

To manage nodes, on the menu bar, click **Node Management > View All Nodes**. The Node Management UI displays. The Node Management UI comprises two panels:

- The left side displays the navigation tree.
- The right side displays the management panel, enabling you to perform management operations on items selected in the navigation tree.

The Navigation Tree

The navigation tree organizes managed nodes into a hierarchy, and comprises the following:



System: System displays the entire set of nodes managed by ArcSight Management Center.



Location: Individual locations are displayed under **System**, listed in the order in which they were added. Locations are logical groupings you can use to organize a list of hosts. For more information, see ["Locations" on page 74](#).



Host: Each location branch shows all hosts assigned to that location, listed by hostname, in the order in which they were added. For more information, see ["Hosts" on page 76](#).

Node Types: Each host branch shows all managed nodes associated with that host. A node can be any of the following types:



Connector Appliance or Software Connector Appliance: Each Connector Appliance (hardware or software) is shown as a separate node.



Logger Appliance or Software Logger: Each Logger (hardware or software) is shown as a separate node.



ArcSight Management Center: Each ArcSight Management Center (hardware or software) is shown as a separate node.



Container: If the host includes any containers, each is shown as a node.



Connector: If a container node contains a connector, the connector is shown under the container node in which it is contained.



Collector: If a container node contains a Collector, the Collector is shown under the container node in which it is contained.



Event Broker: A managed Event Broker is shown as a node.

Since items in the tree are organized hierarchically, each item in the tree includes all branches displayed below it. For example, a **Location** branch includes all hosts assigned to that location. Click the wedge icon to toggle the view of any branch and any items included in the branch.

The Management Panel

Select an item in the navigation tree to display its details on one of the tabs in the central management panel. For example, to display the details of a host shown in the navigation tree, select the host in the tree. The management panel to the right of the tree will display details and controls pertaining to selected host.

Management Tabs

The tabs displayed in the management panel depend on the type of item selected in the navigation tree. The management tabs displayed will show detailed information associated with the selected item, depending on its position in the hierarchy.

Selected Item Type in Navigation Tree	Tabs Shown in Management Panel
System	Locations, Hosts, Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, EB Nodes
Location	Hosts, Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, EB Nodes
Host	Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, EB Nodes
Node	Connectors, Collectors, ConApps, Loggers, ArcMCs, EB Nodes

For example, if you selected a location item from the navigation tree, the **Hosts, Containers, Connectors, Collectors, ConApps, Loggers ArcMCs** and **EB Nodes** tabs would be shown. Each tab would display the items of the named type associated with the selected location, including details on those items.

Working with Items in the Management Panel

Selecting One or Multiple Items: To select an item from a list of items in the management panel, click the item. Use Shift+Click to select multiple adjacent list items, or Ctrl+Click to select multiple non-adjacent items.

Column Settings: Click the gear icon to change column settings:

- **Sorting:** To sort data by a column, select either **Sort Ascending** or **Sort Descending**.
- **Column Display:** To change the columns displayed in a table, select **Columns**. Then toggle one or more columns to display.
- **Filter:** To filter a list of items, select **Filters**. Then enter one or more filter criteria to display items matching those criteria.

Refreshing a List: To refresh the data in a list, click **Refresh** in the upper right corner.

Tab Controls

These controls are commonly displayed on all tabs in the management panel:

- **Toolbar Buttons:** Toolbar buttons enable operations related to the items on the tab.
- **Items Table:** Items corresponding to the tab header are displayed in a table. For example, locations are listed in tabular format on the Locations tab.
- **Bulk Operations Buttons:** On most tabs, bulk operations buttons enable you to perform operations on one or more items. Choose one or multiple items in the list, and then click the button to perform the indicated operation. For example, to delete multiple items such as hosts, select one or more hosts on the **Hosts** tab, and then click **Delete**. The selected hosts would be deleted.

In addition, each tab may have controls individual to that item type. For example, the **Connectors** tab includes controls related to the management of connectors (see ["Managing Connectors" on page 118](#)).

The Locations Tab

The **Locations** tab displays all locations defined in ArcSight Management Center. The **Locations** tab includes these buttons:

Add Location	Adds a new location. For more information, see "Adding a Location" on page 74
Delete	Deletes one or more selected locations from ArcMC. For more information, see "Deleting a Location" on page 75

The **Locations** table displays these parameters for each location.

- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.
- **Action:** Drop-down includes a control for editing a location. For more information on editing a location, see ["Editing a Location" on page 74](#).








For more information on managing locations, see ["Locations" on page 74](#).

The Hosts Tab

The **Hosts** tab displays all hosts associated with the location selected in the navigation tree. The **Hosts** tab includes these buttons:

Add Host	Adds a host. Available on the Hosts tab when a location is selected in the navigation tree. For more information on adding a host, see "About Adding a Host" on page 76 .
Move	Moves selected hosts to a new location. For more information, see "Moving a Host to a Different Location" on page 88
Update Agent	Updates the ArcMC Agent on selected hosts. If the Agent is not currently installed, this button will install the Agent. For more information, see "Updating (or Installing) the ArcMC Agent " on page 89 .
Delete	Deletes selected hosts from ArcMC. For more information, see "Deleting a Host" on page 88

The **Hosts** table displays these parameters for each host:

- **Hostname:** Fully qualified domain name (FQDN) or IP address of the host. The hostname must match the hostname in the host's SSL certificate. (If IP address was used to add the host, then the certificate will match the IP address used.)
- **Path:** Path to the host.
- **Agent Version:** Version number of the ArcSight Management Center Agent running on the host.
- **Issues:** Status of any issues associated with the host. Possible indicators include:
 -  **None:** No issues are associated with the host.
 -  **Internet connection Not Present:** The host is currently not reachable by internet connection. Displayed when ArcMC is not able to connect to the Marketplace for retrieving parser upgrade versions. If the user environment needs a proxy server for an internet connection, [configure the logger.properties file](#). If the user environment is an appliance, save the DNS settings on the **System Admin > Network** page.
 -  **Valid Marketplace Certificate Not Found in ArcMC:** Displayed when the Marketplace certificate does not match the one found in ArcMC's trust store.
 -  **Host Certificate Mismatch:** The hostname does not match the hostname in the SSL certificate. For instructions on downloading and importing certificates for the host, see ["Downloading and Importing Host Certificates" on page 91](#). If this issue is displayed for the localhost, and the certificate cannot be downloaded, please restart the **web** service on the localhost.
 -  **ArcMC Agent Out of Date:** The host's Agent version cannot be upgraded from the managing ArcMC, or the ArcSight Management Center cannot communicate with the ArcSight Management Center Agent on the managed node. You may need to manually install the ArcMC Agent. For requirements and instructions, see ["Installing the ArcSight Management Center Agent" on page 33](#)
 -  **ArcMC Agent Stopped:** The Agent process on the host has been stopped.
 -  **ArcMC Agent Upgrade Recommended:** The host's Agent version is older than the one on the managing ArcMC. An Agent upgrade is recommended.

- **!** *ArcMC Agent Uninstalled:* The Agent on the host has been uninstalled.
- **!** *ArcMC Agent Down:* The Agent on the host is not running.
- **!** *Update the authentication credentials on the localhost, and then install the ArcMC Agent.:* For a localhost added for remote management, [authentication credentials need to be updated](#) to ensure authentication, and then the [ArcMC Agent needs to be installed](#) to enable management. Take both of these steps to correct this issue.
- **!** *Error in REST Authentication.:* The Event Broker node lacks the ArcMC certificate, ArcMC session ID, or ArcMC URL and port. To resolve this issue:
 - Make sure the user has the permission rights for the Event broker operations.
 - Make sure the valid ArcMC certificate (with FQDN and .crt extension) is present in the Event Broker's location: /opt/arcsight/k8s-hostpath-volume/eb/arcmccerts
 - Make sure that the ArcMC URL is updated with correct FQDN and port in ArcSight Installer > Event Broker Configuration > ArcMC_Monitoring field.
 - Note that each time the user replaces the ArcMC certificate to the EB's location, the EB's webservice pod has to be restarted for the new certificate to be read and to be updated in the trust store.
- **Model:** If the host is an appliance, this shows the ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.
- **Type:** Type of installation, either ArcMC Appliance or Software.
- **Version:** Version number of the software on the host.
- **Action:** Drop-down shows controls for executing host management tasks, which include:
 - [Scanning a host](#)
 - [Downloading certificate details](#)
 - [Updating host credentials](#)

For more information on host management, see ["Hosts" on page 76](#).

The Containers Tab

The **Containers** tab displays all containers associated with the item selected in the navigation tree. For example, if you selected a location in the tree, since locations include hosts, the **Containers** tab would display all containers associated with all hosts in the selected location. The **Containers** tab includes these buttons:

Properties	Set properties on selected containers. For more information, see "Updating Container Properties" on page 106 .
Certificates	Manage certificates on selected containers. For more information, see "Managing Certificates on a Container" on page 113 .
FIPS	Enable or disable FIPS on selected containers. For more information, see "Enabling FIPS on a Container" on page 111 .

Upgrade	Upgrades all connectors in selected containers. For more information, see "Upgrading All Connectors in a Container" on page 107 .
Credentials	Manage credentials on selected containers. For more information, see "Changing Container Credentials" on page 106 .
Logs	Manage logs on selected containers. For more information, see "Viewing Container Logs" on page 110 .
Restart	Restart all connectors in selected containers. For more information, see "Restarting a Container" on page 109 .
Delete	Deletes the selected containers from ArcSight Management Center. For more information, see "Deleting a Container" on page 106 .

The **Containers** table includes the following columns:

- **Name:** Name of the container.
- **Path:** Path to the container.
- **Issues:** Status of any issues associated with the container.
- **Port:** Port number through which the container is communicating.
- **Framework Ver:** Framework version number of the container.
- **Parser Ver:** Parser version number of the container.
- **Status:** Status of the container. Possible values for container status are:
 - *Improper configuration:* Initial default state.
 - *Initializing connection:* The connector has a resolvable URL, but ArcSight Management Center has not logged in to the connector yet.
 - *Down:* There was an exception trying execute the login command.
 - *Unauthorized:* The login command was executed, but login has failed.
 - *Connecting:* The login is in progress.
 - *Connected:* The login was successful.
 - *Empty:* Login successful, but the container doesn't have connectors.
 - *Initialized:* Login successful and the container has connectors.
 - *Unknown:* No information on status. To resolve, manually SSH to the system and restart the container.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing container management tasks, which include:
 - [Edit Container](#)
 - [Send Container Command](#)
 - [Add Connector](#)
 - [Run Logfu](#)

- [Download Certificate](#)
- [Display Certificates](#)
- [Deploy \(to ArcExchange\)](#)
- [Run FlexConnector Wizard](#)

For more information on container management, see ["Upgrading All Connectors in a Container" on page 107](#)

The Connectors Tab

The **Connectors** tab displays all connectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Connectors** tab would show all connectors in the selected container. For the details on managing connectors, see ["Managing Connectors" on page 118](#).

The Connectors tab will also show any deployed [CEBs](#).

The **Connectors** tab includes these buttons, which perform operations on one or more selected connectors:

Add Connector	(Only shown when a container is selected in the navigation tree.) Adds a connector to the selected container.
Runtime Parameters	Edit the runtime parameters on selected connectors. For more information, see "Editing Connector Parameters" on page 121 .
Destinations	Sets the destinations of selected connectors. For more information, see "Managing Destinations" on page 123 .
Parameters	Sets parameters for selected connectors. For more information, see "Editing Connector Parameters" on page 121 .
Delete	Deletes connectors from ArcSight Management Center. For more information, see "Deleting a Connector" on page 131 .

The **Connectors** table displays the following parameters for each connector:

- **Name:** Name of the connector.
- **Path:** Path to the connector.
- **Type:** Type of connector.
- **EPS In:** Events per second received by the connector.
- **EPS Out:** Events per second sent by the connector to its destination.
- **Cache:** Connector cache size.
- **Last Check:** Date and time of the last status check.
- **Action:** Drop-down shows a variety of controls for executing connector management tasks. These include:

- [Send Connector Command](#)
- [Share](#) a connector to ArcExchange
- [Edit a FlexConnector](#)

For more information on connector management, see ["Managing Connectors" on page 118](#).

The Connector Summary Tab

To view a single connector in detail, click the connector in the navigation tree. The toolbar on the summary tab includes the following buttons for operations on the connector:

Connector Command	Sends a command to the connector. For more information, see "Sending a Command to a Connector" on page 131 .
Remove Connector	Removes the connector. For more information, see "Deleting a Connector" on page 131 .
Run Logfu	Run Logfu diagnostics on the connector. For more information, see "Running Logfu on a Connector" on page 131 .
Share	Shares the connector through ArcExchange. For more information, see "Sharing Connectors in ArcExchange" on page 138 .

Tables below the toolbar show connector specifics, including basic connector data, parameters, and connector destinations. These tables include the following columns:

Connector Data

- **Type:** Type of connector.
- **Status:** Connector status.
- **Input Events (SLC):** Total number of events received by the connector since it was last checked (generally once per minute).
- **Input EPS (SLC):** Events per second received by the connector since it was last checked (generally once per minute).
- In addition, the columns to the right include tools for [editing a connector](#), [editing runtime parameters](#), [adding a failover destination](#), and [sending a destination command](#).

Connector Parameters

Click **Connector Parameters** to toggle display of this table. **Connector Parameters** includes:


-  Click to edit parameters.
- **Parameters:** Parameters can include connector network port, IP address, and protocol, and other information.
- **Value:** Parameter value.


Table Parameters (WUC Connectors Only)

WUC connectors (only) display these parameters.

- **Domain Name:** Connector domain name.
- **Host Name:** Connector host name.
- **User Name:** Connector user name.
- **Security Logs:** Indicates whether security events are collected.
- **System Logs:** Indicates whether system events are collected.
- **Application:** Indicates whether application events are collected from the Common Application Event Log.
- **Custom Log Names:** List of custom application log names, if any.
- **Microsoft OS Version:** Microsoft operating system for the connector.
- **Locale:** Connector locale.

Destinations

Click **Destinations** to toggle display of this table. The **Destinations** table includes:

-  Click to add additional destinations.
- **Name:** Destination name.
- **Output Events (SLC):** Total number of events output by the connector to the destination since it was last checked (generally once per minute).
- **Output EPS (SLC):** Events per second output by the connector to the destination since it was last checked (generally once per minute).
- **Cached:** Total number of events cached to be transmitted to the destination.
- **Type:** Destination type. Destination types are described in the SmartConnector User's Guide.
- **Location:** Location of the destination.
- **Device Location:** Location of the device on which the destination is located.
- **Comment:** Comments on the destination.
- **Parameters:** Destination-specific parameters, such as IP address , port, and protocol.
- **Action Buttons:** Action buttons enable destination management tasks, such as editing the destination, editing the runtime parameters, adding a new failover destination, sending destination commands and removing the destination.

For more information on managing connectors, see ["Managing Connectors" on page 118](#).

The ConApps Tab

The **ConApps** tab displays all hardware and software Connector Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Connector Appliances** tab would display all Connector Appliances in ArcSight Management Center; if you selected a Location, the tab would display all Connector Appliances in the selected location.

The **Connector Appliances** tab includes the following button, which operates on one or more selected Connector Appliances:

Set Configuration	Sets the configuration for selected Connector Appliances. For more information, see "Setting a Configuration on ConApps" on page 96
--------------------------	---

The **Connector Appliances** table displays these parameters for each Connector Appliance:

- **Name:** Name of the Connector Appliance.
- **Path:** Path to the Connector Appliance.
- **Port:** Port number through which the Connector Appliance is communicating.
- **Version:** Software version of the Connector Appliance.
- **Status:** Status of the Connector Appliance.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing Connector Appliance management tasks, including the following:
 - [Rebooting](#)
 - [Shutting down](#)
 - [Editing or removing a configuration](#)

For more information on Connector Appliance management, see ["Managing Connector Appliances \(ConApps\)" on page 94](#).

The Loggers Tab

The **Loggers** tab displays all hardware and software Loggers associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Loggers** tab would display all Loggers in ArcSight Management Center; while if you selected a Location, you would see all Loggers in that location.

The **Loggers** tab includes the following buttons, which perform operations on one or more selected Loggers:

Set Configuration	Sets the configuration for selected Loggers. For more information, see "Setting a Configuration on Loggers" on page 104 .
Upgrade Logger	Upgrades selected Loggers. For more information, see "Upgrading a Logger " on page 102

The **Loggers** table displays these parameters for each Logger:

- **Name:** Name of the Logger.
- **Path:** Path to the Logger.
- **Port:** Port number through which the Logger is communicating.
- **Version:** Software version of the Logger.
- **Top Storage Use:** Displays the most used storage group and its percentage of storage.
- **Status:** Status of the Logger.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing Logger management tasks, including the following:
 - [Rebooting](#)
 - [Shutting down](#)
 - [Editing or removing a configuration](#)

The ArcMCs Tab

The **ArcMCs** tab displays all Software ArcSight Management Centers and ArcSight Management Center Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **ArcMCs** tab would display all managed ArcSight Management Centers; while if you selected a Location, you would see all ArcMCs in that location.

The **ArcMCs** tab includes the following buttons, which perform operations on one or more selected ArcMCs:

Set Configuration	Sets the configuration for selected ArcMCs. For more information, see "Setting a Configuration on Managed ArcMCs" on page 100
Upgrade ArcMC	Upgrades selected ArcMCs. For more information, see "Upgrading ArcMC" on page 98

The **ArcMCs** table displays these parameters for each ArcMC:

- **Name:** Name of the ArcSight Management Center.
- **Path:** Path to the ArcSight Management Center.
- **Port:** Port number through which the ArcSight Management Center is communicating.
- **Version:** Software version of the ArcSight Management Center.
- **Status:** Status of the ArcSight Management Center.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing ArcMC management tasks, including the following:
 - [Rebooting](#)
 - [Shutting Down](#)
 - [Editing a configuration](#)

For more information on managing other ArcSight Management Centers in ArcSight Management Center, see ["Managing Other ArcSight Management Centers" on page 97](#).

The EB Nodes Tab

ArcMC can only manage a single Event Broker. However, the single managed Event Broker may have any number of Event Broker nodes, each of which can be managed and monitored by ArcMC. When you add an Event Broker as a host to ArcMC, you add all of its nodes.

The **EB Nodes** tab displays all Event Broker nodes present in the managed Event Broker. For example, if you selected **System** in the navigation tree, the **EB Nodes** tab would display all managed Event Broker nodes; while if you selected a Location, you would see all Event Broker nodes in that location.

The tab displays these parameters for each managed Event Broker node:

- **Name:** Name of the Event Broker node.
- **Port:** Port number through which the Event Broker node is communicating.
- **Type:** Type of Event Broker node.
- **Last Check:** Date and time of last status check.

For more information on managing Event Broker in ArcSight Management Center, see ["Managing Event Broker" on page 191](#).

The Collectors Tab

The **Collectors** tab displays all Collectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Collectors** tab would show all Collectors in the selected container. For the details on managing Collectors, see [Managing Collectors](#).

Note: Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production** alpha features. These features are provided for your testing and evaluation only and must not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.** We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

The **Collectors** table displays the following parameters for each connector:

- **Name:** Name of the Collector.
- **Port:** Collector port.
- **Type:** Type of Collector.
- **Syslog Lines Received:**
- **Custom Filtering:** messages filtered out

- **Status:** Collector status.
- **Last Check:** Date and time of the last status check.

For more information on connector management, see ["Managing Connectors" on page 118](#).

Locations

A *location* is a logical grouping of hosts. The grouping can be based on any criteria you choose, such as geographical placement or organizational ownership. Locations are a useful way to organize a set of hosts.

For example, you could group all hosts in New York separately from hosts in San Francisco and assign them to locations named “New York” and “San Francisco”. Similarly, you could group hosts in a location named “Sales” and others in the location “Marketing”.

A location can contain **any number** of hosts. For information on adding hosts to locations, see ["About Adding a Host" on page 76](#).

Note: ArcSight Management Center includes one location by default (called *Default*) but you may add any number of others. The name of the Default location may be edited, and the location itself may be deleted.

Adding a Location

You can add any number of locations.

To add a location:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Add Location**.
4. Enter the name of the new location, and then click **Next**.
5. Click **Done**. The new location is shown in the System tree.

Editing a Location

You can edit the name of a location.

To edit a location:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Locations** tab.
3. On the **Locations** tab, choose a location to rename.
4. In the **Action** drop-down of the selected location, select **Edit Location**.
5. Enter the new name of the location, and then click **Next**.
6. Click **Done**. The location is renamed.

Viewing All Locations

You can see all the locations that exist in ArcSight Management Center.

To view all locations:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Locations** tab to view all locations.

Deleting a Location

When you delete a location from ArcSight Management Center, any hosts in the location (and their associated nodes) are also deleted.

Tip: If you want to delete a location but still want to keep its hosts in ArcSight Management Center, relocate the hosts before deleting the location. See ["Moving a Host to a Different Location" on page 88](#).

To delete a location:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Locations** tab.
3. On the **Locations** tab, choose one or more locations to delete.
4. Click **Delete**.
5. Click **OK** to confirm deletion. The selected locations are deleted.

Hosts

A *host* is a networked system associated with a unique IP address or hostname. A host can be an ArcSight appliance, or a system running an ArcSight software product, such as Software Logger.

For information on adding hosts to manage, see ["About Adding a Host" below](#).

About Adding a Host

After a host is added to ArcSight Management Center, ArcSight products on the host becomes *nodes*, and can be managed. For example, adding a host running Connector Appliance with 4 containers would add 5 nodes to ArcSight Management Center: the Connector Appliance itself, and each container.

In ArcMC 2.2 and later, the ArcMC localhost is added automatically for remote management. You will be able to [manage the localhost as you would any other node](#).

Prerequisites for Adding a Host (for each Host Type)

Connection Information for Adding a Host

Host Type	Required Information
Appliance with Local Connectors (includes ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance (L3XXX))	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. Note: See "Prerequisites for Adding a Host (for each Host Type)" above for more information about authentication credentials. • Authentication credentials (username and password) for any local containers. If the appliance includes multiple containers, then the credentials for each container must be identical. For example, if the username and password for one container managed by a Connector Appliance is <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for all local containers managed by the same Connector Appliance.
Appliance without Local Connectors (includes Logger Appliance (non-L3XXX))	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. Note: See "Prerequisites for Adding a Host (for each Host Type)" above for more information about authentication credentials.
Software Form Factor (includes Software ArcSight Management Center, Software Connector Appliance, or Software Logger)	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials if possible, or use the fall back credentials.` Note: See "Prerequisites for Adding a Host (for each Host Type)" above for more information about authentication credentials. • Port number assigned to the product.

Connection Information for Adding a Host, continued

Host Type	Required Information
Connector (includes SmartConnectors of all types)	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) • Authentication credentials (username and password) for the connector. <p>Note: See "Prerequisites for Adding a Host (for each Host Type)" on the previous page for more information about authentication credentials.</p> <ul style="list-style-type: none"> • Optionally, specify an inclusive port range separated by a hyphen (such as 9004-9008) to scan a port range for all connectors. <p>Note: If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for every connector in the port range.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Prior to adding a software-based SmartConnector as a host, you must prepare the Smart Connector as explained in SmartConnectors on ArcMC.</p> </div>
Collector	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) • Authentication credentials (username and password) for the Collector. <p>Note: See "Prerequisites for Adding a Host (for each Host Type)" on the previous page for more information about authentication credentials.</p> <ul style="list-style-type: none"> • Optionally, specify an inclusive port range separated by a hyphen (such as 9004-9008) to scan a port range for all Collectors. <p>Note: If the port range includes multiple Collectors, then the credentials for each Collector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for every Collector in the port range.</p>

Connection Information for Adding a Host, continued

Host Type	Required Information
Event Broker 2.01 or earlier	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) • Port number for the Event Broker (default 38080) • In order to add Event Broker as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights. <p>Note: Prior to performing the Add Host process, you will need to generate the ArcMC certificate with complete FQDN and download the .crt file, and then copy the certificate file to your Kubernetes master node. See Preparing to Add Event Broker as a Host for details on this process.</p>
Event Broker 2.02 or later	<ul style="list-style-type: none"> • Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) • Port number for the Event Broker (default 38080) • The following Kubernetes cluster parameters: <ul style="list-style-type: none"> • Cluster Hostname • Cluster Port • Cluster Username and Password • Certificate file (contents): To get the certificate file contents, <pre># cat /opt/arcsight/kubernetes/ssl/ca.crt</pre> to the master Kubernetes node. Copy everything from the first dash character (-) before BEGIN CERT to the last dash character after END CERT, then paste it into the Cluster Certificate box. • In order to add Event Broker as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights.

- **An SSL Certificate:** An SSL certificate must be generated for any of the following host types to be managed:

- Connector Appliance or Software Connector Appliance
- Logger Appliance or Software Logger
- Event Broker (any version)
- ArcSight Management Center Appliance or Software ArcSight Management Center

The hostname in the certificate must match the hostname you will add to ArcSight Management Center. For more information on generating certificates for these host types, consult the ArcSight Administrator's Guide for each product. (If a host to be added already has a certificate installed, you can use the existing certificate, as long as the hostname on the certificate matches the hostname of the host you will be adding.)

Note: If the hostname does not match the hostname in the SSL certificate, you can regenerate

a matching certificate by doing one of the following:

- For a hardware appliance, in **System Admin > Network**, click the **NICS** tab. Under **Host Settings**, note the entry in the Hostname field. (This is the value you should use to add the host to ArcSight Management Center.) Click **Restart Network Service**. Then, in the navigation menu, under **Security**, pick **SSL Server Certificate**. Click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.
 - For software form factor, in **System Admin > SSL Server Certificate**, under **Enter Certificate Settings**, verify that the hostname from the NICS tab noted previously is entered in the **Hostname** field. Then, click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.
- **Check for Agent Installation:** Check the table under "[Installing the ArcSight Management Center Agent](#)" on [page 33](#) to determine if the ArcMC Agent needs to be installed on a host prior to adding it to ArcMC. For some host types, the Agent will be installed automatically upon adding a host.

Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Node Authentication Credentials

ArcSight Management Center authenticates to each managed node each time it communicates with the node, using the node's authentication credentials—that is, username and password—you supply when first adding the host. If the host includes connectors or containers, then authentication credentials must also be supplied for these as well. (Exception: Event Broker does not require authentication credentials for individual nodes.) As a result, valid credentials for each node are required when adding a host.

Determining a Node's Credentials:

Consult the system administrator for each managed node to determine its current login credentials. Each ArcSight product ships with a default set of credentials. However, for optimal security, it is expected that the default credentials are changed as soon as possible by the administrator, so the default credentials may no longer be valid for authentication.

- For default credentials for ArcSight products, consult the relevant product administrator's guide. (For SmartConnector default credentials, consult the SmartConnector User's Guide, available from the HPE support community at [Protect724](#).)
- Some products can be configured by administrators to use external authentication, in which case the external authentication credentials or fallback credentials should be provided when adding the host to ArcSight Management Center. (SmartConnectors may not be configured for external authentication.)

Changed or Expired Credentials

If the username or password on a node are changed (or expire) any time after the node is added to ArcSight Management Center, then the node will no longer be managed. However, it will still appear in the list of managed nodes. For example, on some hosts, passwords are set to expire automatically after some time period, which would prevent successful authentication by ArcSight Management Center using the node's initial credentials. To avoid this issue, you may wish to use node credentials that do not expire. To continue management of node on which the credentials have changed or expired, use the [Update Host Credentials](#) feature.

Dynamic Credentials

If authentication credentials are configured to change dynamically (such as with RADIUS one-time passwords), then instead of providing external authentication credentials, you can instead provide the credentials of a local user on the managed node who is permitted to use fallback authentication. ArcSight Management Center will then try to authenticate to the managed node using the external authentication method first, and if this fails, it will try to authenticate to the managed node using the local user credentials.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with ArcMC, you need to enable remote management on each connector, as follows:

1. In a text editor, in the installation directory for the SmartConnector, open the file `/<install_dir>/user/agent/agent.properties`.
2. Add the line: `remote.management.enabled=true`
3. If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: `remote.management.listener.port=<port_number>`, where `<port_number>` is the new port number.
4. Save the file.
5. Restart the SmartConnector for changes to take effect.

Preparing to add Event Broker (2.01 or earlier) as a host

Before you can add Event Broker (version 2.01 or earlier) as a managed host, you will need to generate the ArcMC certificate with complete FQDN and download the .crt file, and then copy the certificate file

to your Kubernetes master node.

To prepare for adding Event Broker as a host:

1. In ArcMC, click **Administration > System Admin.**
2. Under **Security > SSL Server Certificate**, under Hostname, enter the FQDN of the ArcMC.
3. Click **Generate Certificate.**
4. Save the certificate locally.
5. Connect to your Kubernetes master node.
6. Copy the previously generated certificate to `/opt/arcsight/k8s-hostpath/eb/arcmccerts.`
7. Launch the ArcSight Installer.
8. Click **Configuration > ArcSight Event Broker.**
9. On the **ArcMC Monitoring** tab, in **ArcMC URL**, enter the FQDN and port number of the managing ArcMC.

In ArcMC, you can now follow the process outlined under [Adding a Host](#).

Adding a Host

Before adding a host, ensure that that you have the required information for the host on hand. For more information, see "[Prerequisites for Adding a Host \(for each Host Type\)](#)" on page 77.

To add a host to ArcMC:

1. Click **Node Management.**
2. In the navigation tree, select a location to which you plan to add the host.
3. On the **Hosts** tab, click **Add Host.**
4. On the **Add a new Host** dialog, in **Hostname/IP**, enter either the hostname or IP address of the host.
5. In **Type**, select the type of node from the drop-down list.
6. Enter values for the required settings. (Requested information will depend on the node type.)
 - In **Host Credentials** or **Connector Credentials**, enter the username and password required for authentication.
 - In **Port**, if required, enter the value of the port on which ArcSight Management Center will connect to the host.
7. Click **Add.** The host is added to ArcSight Management Center.

You can quickly deploy a connector or Collector directly to a host in the ArcMC Deployment View. For more information, see ["Instant Connector Deployment" on page 57](#).

Adding a Host with Containers

When you add a host that includes containers (such as Connector Appliance), ArcSight Management Center also attempts to retrieve the SSL certificates from any containers that reside on the host, and add each container as a separate node. Containers on the remote host can be managed only if ArcSight Management Center can authenticate using the certificates and supplied credentials. When the certificates are retrieved, you are prompted to import them into ArcSight Management Center.

Note: On ArcSight Management Center Appliance, all local containers are added automatically as hosts of type Software Connector.

Importing Multiple Hosts

To quickly and easily add multiple hosts in bulk, you can import a comma-separated values (CSV) file that lists the names and required attributes of the hosts to be added.

Note: ArcSight Management Center 1.0 used a slightly different file format for importing connector hosts. That file format is not supported by ArcSight Management Center 2.1. Use the file format described here instead.

Prerequisites for Importing Multiple Hosts

The following prerequisites apply to importing hosts.

- **Add Host Prerequisites:** Any prerequisites for the Add Host process also apply to importing multiple hosts by a CSV file. See ["About Adding a Host" on page 76](#).
- **Valid CSV File:** Ensure the values in your CSV file are valid and correct. An import hosts job will fail immediately upon receiving an invalid or incorrect value. The CSV file format is described under ["CSV File Format" below](#).
- **Stop the Agent 1.0 Process:** In addition, if any of the hosts to be imported are running the ArcSight Management Center 1.0 Agent, stop the Agent process on each such host before the import. (This is not needed for later versions of the ArcMC Agent.)

CSV File Format

The CSV (comma-separated value) file requires the following header line to be its first line:

```
location,hostname,type,host_username,host_password,connector_username,connector_password,port/port_range
```

Each subsequent line represents one host to be imported. Each line must include values for the following comma-separated fields for each host:

<Location>, <Hostname>,<Host Type>,<Host Username>,<Host Password>,
<Connector Username>,<Connector Password>,<Port/Port Range>

Some host types require values for all fields, and some are optional. An optional field with no value specified must still include a comma to represent the empty field.

Host Field Values

Valid values for host fields are detailed in the following table. An asterisk (*) indicates a required field. An optional field with no value specified must still include a comma to represent the empty field.

Field	Description
Location*	Location to which the host will be assigned.
Hostname*	Hostname (FQDN) or IP address of the host. <ul style="list-style-type: none">FQDN or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address.If hostname is used, the hostname entered must match the hostname from the host's SSL certificate.For a hardware appliance, DNS must be configured on the managing appliance (System Admin > DNS).
Host Type*	Host type. Valid (case-insensitive) values are: <ul style="list-style-type: none">appliance_with_local_connectors: includes ArcSight Management Center Appliance, Connector Appliance and Logger Appliance (L3XXX)appliance_without_local_connectors: includes Logger Appliance (non-L3XXX).software_form_factor: includes Software ArcSight Management Center, Software Connector Appliance or Software Logger.software_connector: includes all connectors and Collectors.

Field	Description
Host Username/Password*	User name and password used to authenticate to the host. Note: See "About Adding a Host" on page 76 for more information about authentication credentials.
Connector Username/Password	Username and password used to authenticate to the connector. Required for hosts of type Appliance with Local Connector and Software Connector; otherwise optional. Note: See "About Adding a Host" on page 76 for more information about authentication credentials.
Port/Port Range	Starting port or port range for connector scan. Valid values: <ul style="list-style-type: none"> Port number Port range Comma-separated port numbers (for example, 9000,9004,9007) Notes: <ul style="list-style-type: none"> <i>For software form factors</i>, port is required. <i>For appliance form factors</i>, to add all local containers, leave the field blank. However, if any port numbers are entered, then certificates will be downloaded only for the specified port numbers, and only those containers will be imported. <i>For connectors</i>, either a port or port range is required. If using port range, specify an inclusive port range, using a hyphen between starting and ending port. For example, a specified port range of 9001-9003 would scan ports 9001, 9002, and 9003. Note: If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i> , then <i>myusername</i> and <i>mypassword</i> must be the credentials for every connector in the port range.

An example of a valid import file, importing two hosts, is shown here:

```
location,hostname,type,host_username,password1,connector_
username,password2,port/port range

CorpHQ,hostname.example.com,software_connector,username,password,connector__
username,connector_password,9001-9010

EMEA,hostname2.example.com,appliance_without_local_connectors,
logger_user,logger_pword,, ,
```

In this example, the first line would represent the required header line, the second line a Software Connector, and the third line would represent a Logger Appliance.

Import Hosts Procedure

Only a single Import Hosts job may be executed at one time.

To import hosts from a CSV file:

Note: Before beginning the import, stop the Agent processes on any hosts running version 1.0 of the ArcMC Agent.

1. Create and save your CSV file in a text editor.
2. Log into ArcSight Management Center.
3. Select **Node Management > Import Hosts**. The Import Hosts wizard starts.
4. Click **Browse**, and browse to the location of your hosts CSV file.
5. Click **Import**. The hosts are imported as a background job.

If the CSV file is valid, connector certificates are retrieved automatically so that ArcSight Management Center can communicate with each connector in a container. The Upload CSV wizard lists the certificates. (To see certificate details, hover over the certificate.).

Automatic installation of the ArcMC Agent may increase the time required for the Import Hosts job.

- Select **Import the certificates...**, and then click **Next** to import the certificates and continue.
- Select **Do not import the certificates...**, and then click **Next** if you do not want to import the certificates. The Upload CSV wizard does not complete the upload CSV process.

Note: The Import Hosts wizard does not complete the upload if certificate upload failed for any of the connectors in a container, or if any of the certificates failed to import into the trust store.

2. The Import Hosts job executes.

Import Hosts Job Logs

ArcSight Management Center logs the results of all Import Hosts jobs. Each job produces a new log, named `import_hosts_<date>_<time>.txt`, where `<date>` and `<time>` are the date and time of the import hosts job.

- For Software ArcSight Management Center, logs are located in the directory `<install_dir>/userdata/logs/arcmc/importhosts`.
- For ArcSight Management Center Appliance, logs are located in the directory `opt/arcsight/userdata/logs/arcmc/importhosts`.

Log Format

Each entry in the log will show the success or failure of each host import attempt, in the format:

```
<User initiating job>, <CSV filename>, <Time of import host job start>,<Hostname>,<Success/failure result>
```

For example:

```
admin, my_csv_file.csv, Tue Apr 08 14:16:58 PDT 2015, host.example.com, Host
added successfully
```

If the import hosts job has failed due to one or more invalid entries in the CSV file, the result file will show the parsing error details with the line number and error.

For example:

```
Line [1] has [connector password] field empty. [connector password] field is
required for this host type.
```

Exporting Hosts

Exporting hosts from an ArcSight Management Center will create a CSV list of hosts managed by that ArcSight Management Center. (Password information is not included in this file.)

After adding passwords for each host to the file, you can then import this list of hosts into another ArcSight Management Center, using the Import Hosts feature described under ["Importing Multiple Hosts" on page 83](#)

Exporting hosts is most useful when you are reassigning management of hosts from one ArcMC to another.

For example, consider two ArcSight Management Centers, called ArcMC East and ArcMC West. ArcMC East currently manages 50 hosts. However, you are consolidating management of all hosts to the new ArcMC West. To do this quickly and easily, you would export the hosts from ArcMC East into a CSV file. Then, you would add an additional entry for ArcMC East to the CSV file.

After adding in password data for each host, you would import the resulting CSV file into ArcMC West. At the end of the process, all of ArcMC East's hosts, and ArcMC East itself, would be managed by ArcMC West.

To export hosts in ArcSight Management Center:

1. Select **Node Management > Export Hosts**.
2. All hosts managed by the ArcSight Management Center are exported to the local CSV file (`exporthosts.csv`).
3. Optionally, open the file in a CSV editor. Add the password information for each host to the CSV file, and then save the file.

Viewing All Hosts

You can see all the hosts managed by ArcSight Management Center, or view hosts by location.

To view all hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**. (To view by location, click the location you wish to view.)
3. Click the **Hosts** tab. All managed hosts are displayed.

Viewing Managed Nodes on a Host

You can view all the managed nodes on a host, by host type.

To view managed nodes on a host:

1. Click **Node Management**.
2. In the navigation tree, click the location to which the host is assigned. Then, click the host.
3. Click the appropriate tab to view the node types for the managed host: **Containers**, **Connectors**, **Connector Appliances**, **Loggers**, or **ArcMCs**.

Deleting a Host

When you delete a host, any nodes associated with the host are also deleted. Deleting a host removes its entry from ArcSight Management Center, but otherwise leaves the host machine unaffected.

Use caution when deleting a host. Deleting a host will delete its associated nodes from any [node list](#), [association](#), [peers listing](#), or [subscribers listing](#) that includes those nodes. .

To delete one or more hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Hosts** tab.
3. Choose one or more hosts to delete.
4. Click **Delete**.
5. Click **Yes** to confirm deletion. The host (and any associated nodes) are deleted.

Moving a Host to a Different Location

You can assign one or more hosts to a new location. When you move a host, any nodes associated with it are also moved. For example, if you moved a Connector Appliance to a new location, all of its containers and managed connectors would also be moved to the new location.

To move one or more hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Hosts** tab.
3. Choose one or more hosts to move.
4. Click **Move**.
5. Follow the prompts in the **Host Move** wizard. The selected hosts are reassigned to their new locations.

Updating (or Installing) the ArcMC Agent

Hosts running an outdated version of the ArcSight Management Center Agent can be quickly upgraded to the latest version.

Agent installation or upgrade is supported on all versions of ArcMC Appliance, Connector Appliance (hardware) and Logger Appliance, Software Logger 6.0 or later, and software ArcMC 2.1 or later.

Tip: Check the version of the Agent on each host by clicking the **Hosts** tab and reviewing the **Agent Version** column.

To upgrade or install the Agent on one or more hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Hosts** tab.
3. Select one or more hosts to update.
4. Click **Update Agent**. The Agent Upgrade wizard launches. Follow the prompts to complete the Agent Upgrade wizard.

Scanning a Host

Scanning a host will inventory all currently running containers on the host and the connectors associated with them.

To ensure accuracy and currency of container inventory, you will need to manually scan for new containers in any of the following circumstances:

- Additional containers or connectors or Collectors are added to a remote host after it has been added to ArcSight Management Center.
- Containers, connectors or Collectors are removed from a remote host managed in ArcSight Management Center.
- Any containers which were down when the initial, automatic scan was performed have since come

back up.

- The license for a managed ArcSight Management Center (managed by another ArcSight Management Center) is upgraded to increase the number of licensed containers.

Any host that includes containers is scanned automatically when first added to ArcSight Management Center.

You can manually scan any host types that can run containers. These types include:

- Connector Appliances
- Loggers (L3XXX models only)
- ArcSight Management Center Appliances
- Connectors
- Collectors

The Scan Process

A host scan retrieves information on all CA certificates from any running containers on the host. The containers on the remote host can be managed only if ArcSight Management Center can authenticate using the certificates and the credentials. You are prompted to import any retrieved certificates into the ArcSight Management Center trust store.

A manual scan will be discontinued if any of the following are true:

- Any containers on a scanned Connector Appliance host are down.
- If you choose *not* to import any certificates that are retrieved.
- Authentication fails on any of the containers.

Note: When a Collector and connector are intended to run on the same host, add the Collector to ArcMC first, before the connector. Then perform a scan host to correctly detect the connector.

To manually scan a host:

1. Click **Node Management**.
2. In the navigation tree, select the location to which the host has been assigned.
3. Click the **Hosts** tab.
4. In the **Action** drop-down for the host to be scanned, click **Scan Host**. The Host Scan wizard starts.
5. Click **Next** in the Host Scan wizard.
6. Enter values for the parameters in the following table, and then click **Next**.

Parameter	Description
Starting Port	The port number on the host on which ArcSight Management Center starts scanning for containers.
Ending Port	The port number on the host on which ArcSight Management Center ends scanning for containers.
User	The user name to authenticate with the host.
Password	The password for the user name you provide.

- Connector certificates are retrieved automatically so that the ArcSight Management Center can communicate with each connector in a container. The Host Scan wizard lists the certificates. (To see certificate details, hover over the certificate.)
 - To continue the scan, select **Import the certificates**, and then click **Next** to import the certificates and continue.
 - Otherwise, select **Do not import the certificates**, and then click **Next**. The Host Scan wizard discontinues the scan.

Downloading and Importing Host Certificates

In case of a mismatch between the hostname and the hostname in the SSL certificate, you can download and import the host's current certificates.

To download and import host certificates:

- Click **Node Management**.
- In the navigation tree, select the location to which the host has been assigned.
- Click the **Hosts** tab.
- In the **Action** drop-down for the desired host, select **Download Certificate**.
- Click **Next** in the Download wizard.
- Follow the prompts in the wizard to complete the process.

Updating Host Credentials

ArcMC relies on a host's login credentials to connect and authenticate to the managed host. You specify these credentials when adding the host to ArcMC for management. If these credentials ever change, the management link between ArcMC and the host will be broken.

However, you can update the credentials ArcMC uses to authenticate to a managed host, which will prevent the management link from being broken.

Updating host credentials on ArcMC does not change the actual credentials on the managed host. You will need to change those on the host directly, either immediately before or immediately after performing this operation. Updating credentials will only update the credentials that ArcMC uses to authenticate to the host.

To update host credentials:

1. Click **Node Management**.
2. In the navigation tree, select the location to which the host has been assigned.
3. Click the **Hosts** tab.
4. In the **Action** drop-down for the desired host, select **Update Credentials**.
5. In **Username** and **Password**, enter the new credentials that ArcMC will use to connect to the host.
6. Click **Save**.

Regenerating your Marketplace Certificate

On rare occasions, you may need to regenerate ArcMC's certificate with the ArcSight Marketplace. This can sometimes show as a "Host Certificate Mismatch" error.

To regenerate your Marketplace certificate in ArcMC:

1. Delete the existing marketplace certificate in ArcMC.

For software form factor:

```
rm -rf <install_dir>/current/arcsight/arcmc/config/certs/marketplace.microfocus.com
```

For ArcMC appliance:

```
rm -rf /opt/arcsight/arcmc/config/certs/marketplace.microfocus.com
```

2. Download the new Marketplace certificate in your browser. Browse to the Marketplace website (<https://marketplace.microfocus.com/arcsight>). A security exception will be noted.
3. Click **More Information**, then click **View Certificate**

Note: The exact procedure for downloading the certificate will depend on your browser. The procedure given here applies to Firefox. Consult your browser documentation for exact steps.

4. On the **Details** tab, click **Export**, and save the certificate as X.509 Certificate (PEM).
5. Save the downloaded certificate at the following location:

For software form factor:

```
<install_dir>/current/arcsight/arcmc/config/certs
```

For ArcMC appliance:

`/opt/arcsight/arcmc/config/certs`

6. Restart the ArcMC web service.

Chapter 6: Managing ArcSight Products

The following topics are discussed here.

• Overview	94
• Managing Connector Appliances (ConApps)	94
• Managing Other ArcSight Management Centers	97
• Managing Loggers	101
• Managing Containers	104
• Managing Connectors	118

Overview

ArcSight Management Center enables management tasks on a variety of ArcSight products, including the following:

- Hardware and Software Connector Appliances
- Hardware and Software ArcSight Management Centers
- Hardware and Software Loggers
- Containers
- Software connectors
- Event Broker

This chapter discusses the remote management of these products.

Managing Connector Appliances (ConApps)

You can perform any of the following management tasks on managed Connector Appliances or Software Connector Appliances using ArcSight Management Center:

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Set a configuration on one \(or multiple\) Connector Appliances](#).

Note: Not all Connector Appliance functionality is manageable through ArcSight Management Center. For a complete discussion of Connector Appliance features, see the Connector Appliance Administrator's Guide.

Rebooting a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the Connector Appliance to be rebooted.
5. In the **Action** drop-down of the Connector Appliance, select **Reboot ConApp**.
6. Click **Next** to confirm reboot.
7. The Connector Appliance is rebooted. Click **Done**.

Shutting Down a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the Connector Appliance to be shut down
5. In the **Action** drop-down of the Connector Appliance, select **Shutdown ConApp**.
6. Click **Next** to confirm shutdown.
7. The Connector Appliance is shut down. Click **Done**.

Editing or Removing a Configuration for a ConApp

You can edit a configuration on, or remove property values of a list configuration from, a managed Connector Appliance.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.

4. In the list of Connector Appliances, locate the desired Connector Appliance.
5. In the **Action** drop-down of the Connector Appliance, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Note: In order to edit a backup configuration on a Connector Appliance node, the node must have a scheduled backup to begin with.

Setting a Configuration on ConApps

You can set a configuration on one or multiple Connector Appliances using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Connector Appliances. Only new values will be appended. For more information on list configurations, see ["List Configurations" on page 150](#).
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Connector Appliances.

Caution: Setting a configuration on one or multiple Connector Appliances may make each Connector Appliance node non-compliant with its current subscriptions.

To set a configuration on one or more Connector Appliances:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, select one or more Connector Appliances.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected Connector Appliances. Click **Done**.

Managing Other ArcSight Management Centers

You can perform any of the following management tasks on managed Software ArcSight Management Centers or ArcSight Management Center Appliances:

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Remotely upgrade an ArcMC](#).
- [Set a configuration on one \(or multiple\) ArcSight Management Centers](#).

Rebooting an ArcMC

To remotely reboot a managed ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be rebooted.
5. In the **Action** drop-down of the ArcMC, select **Reboot ArcMC**.
6. Click **Next** to confirm reboot.
7. The ArcSight Management Center is rebooted. Click **Done**.

Shutting Down an ArcMC

To remotely shut down a managed ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be shut down.
5. In the **Action** drop-down of the ArcMC, select **Shutdown ArcMC**.
6. Click **Next** to confirm shutdown.
7. The ArcSight Management Center is shut down. Click **Done**.

Editing or Removing a Configuration for ArcMC

You can edit a configuration on, or remove property values of a list configuration from, a managed ArcSight Management Center.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the desired ArcSight Management Center.
5. In the **Action** drop-down, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Note: In order to edit a backup configuration on an ArcMC node, the node must have a scheduled backup to begin with.

Upgrading ArcMC

In ArcMC, you can remotely upgrade any of the following managed ArcMC types and versions.

Form Factor	Upgrade File Name	Can Upgrade From...	Can Upgrade To...	Comments
Appliance	arcmc-<build number>.enc	ArcMC version 2.0 or later	Any later ArcMC version.	
Software	arcmc-sw-<build number>-remote.enc	ArcMC version 2.1	Any later ArcMC version.	Remote operating system upgrade is not supported for software ArcMC, and, if required, must be performed manually.

Remote Upgrade Using Node Management

Remote upgrade first requires that you upload the appropriate file to your ArcMC repository first. You can then apply the upgrade file to managed ArcMCs.

To upload the upgrade file to your repository:

1. Download the ArcMC upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories**.
3. In the navigation tree, pick **Upgrade Files**.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed ArcMCs:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcMCs, select one or more ArcMCs for upgrade. (You may select only the form factor appropriate for the upgrade file type, as outlined above.)
5. Click **Upgrade ArcMC**. The Upgrade wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Local Upgrade of ArcMC

A local upgrade uses the same file as remote upgrades, as described above.

Although the filename for software ArcMC upgrade includes the word 'remote' (`arcmc-sw-
<build number>-remote.enc`), this file should be used for local upgrades as well.

To perform a manual upgrade of an ArcMC local host:

1. Download the upgrade file for your form factor to a secure network location.
2. Click **Administration > System Admin**
3. In the navigation menu, under **System**, click **License & Update**.
4. In the management panel, under **Select File to Upload**, click **Browse**.

5. Browse to the upgrade file you downloaded in Step 1.
6. Click **OK**. The upgrade file is applied to the local host.

In some cases, after the upgrade of a local host with an .enc file completes, an empty page is displayed. You may navigate away from this page as normal.

Setting a Configuration on Managed ArcMCs

You can set a configuration on one or multiple ArcSight Management Centers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple ArcSight Management Centers. Only new values will be appended. (For more information on list configurations, see ["The Configurations Table" on page 149](#).)
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple ArcSight Management Centers.

Caution: Setting a configuration on one or multiple ArcSight Management Centers may make each ArcSight Management Center node non-compliant with its current subscriptions.

To set a configuration on one or more ArcSight Management Centers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, select one or more ArcSight Management Centers for which to set a configuration.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected ArcSight Management Centers. Click **Done**.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with ArcMC, you need to enable remote management on each connector, as follows:

1. In a text editor, in the installation directory for the SmartConnector, open the file `/<install_dir>/user/agent/agent.properties`.
2. Add the line: `remote.management.enabled=true`
3. If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: `remote.management.listener.port=<port_number>`, where `<port_number>` is the new port number.
4. Save the file.
5. Restart the SmartConnector for changes to take effect.

Managing Loggers

You can perform any of the following management tasks on managed Logger Appliances or Software Loggers using ArcSight Management Center.

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Set a configuration on one \(or multiple\) Loggers](#).
- [Remotely upgrade a Logger](#).

Note: Not all Logger functionality is manageable through ArcSight Management Center. For a complete discussion of Logger features, see the Logger Administrator's Guide.

Rebooting a Logger

To remotely reboot a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the Logger to be rebooted.
5. In the **Action** drop-down of the Logge, click **Reboot Logger**.
6. Click **Next** to confirm reboot.
7. The Logger is rebooted. Click **Done**.

Shutting Down a Logger

To remotely shut down a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select the Logger to be shut down.
5. In the **Action** drop-down of the Logger, select **Shut Down Logger**.
6. Click **Next** to confirm shut down.
7. The Logger is shut down. Click **Done**.

Editing or Removing a Configuration for a Logger

You can edit a configuration on, or remove property values of a list configuration from, a managed Logger.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the desired Logger.
5. In the **Action** drop-down of the Logger, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Note: In order to edit a backup configuration on a Logger node, the node must have a scheduled backup to begin with.

Upgrading a Logger

In ArcMC, you can remotely upgrade any of the following managed Logger types.

Form Factor	Upgrade File Name	Can Upgrade From Version...	Can Upgrade To Version...	Comments
Appliance	logger-<build number>.enc	6.0 or later	6.1 or later	The filename format for the remote upgrade file for Logger Appliance is logger-<build number>.enc
Software	logger-sw-<build number>-remote.enc	6.0 or later	6.1 or later	<ul style="list-style-type: none"> The filename format for the remote upgrade file for software Logger is logger-sw-<build number>-remote.enc Remote operating system upgrade is not supported for software Logger, and, if required, must be performed manually.

Upgrading to Logger version 6.0 requires ArcMC Agent 1167.1 or later to be running on the managed Logger. Upgrade the Agent on the managed Logger before performing the upgrade to Logger 6.0.

To upload the upgrade file to your repository:

1. Download the Logger upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories**.
3. In the navigation tree, pick **Upgrade Files**.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers. (You may only select one form factor type to upgrade.)
5. Click **Upgrade Logger**. The Upgrade wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

In some cases, after the upgrade of a localhost with an .enc file completes, an empty page is displayed. You may navigate away from this page as normal.

Setting a Configuration on Loggers

You can set a configuration on one or multiple Loggers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Loggers. Only new values will be appended. For example, if you had a common group of users on three Loggers, you could use the Set Configuration wizard to add the same new user to all three Loggers with a single action. (For more information on list configurations, see ["The Configurations Table" on page 149.](#))
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Loggers.

Caution: Setting a configuration on one or multiple Loggers may make each Logger node non-compliant with its current subscriptions.

To set a configuration for one or more Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers for which to set a configuration.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected Loggers. Click **Done**.

Managing Containers

A *container* is a single Java Virtual Machine (JVM) that can run up to four connectors. The exact number of connectors depends on your current service agreement and the type of connector.

Containers may run on ArcMCs, on Connector Appliances, and on L3XXX model Loggers. The number of containers that can be run at one time is based on the product license. Check under **System Admin > License & Update** for this information.

Scanning a managed host will ensure all currently running containers on the host (and the connectors associated with them) are accurately inventoried. For more information, see ["Scanning a Host" on page 89.](#)

Note: A connector of any of the following types must be the single connector running in its container:

- Trend Micro Control Manager (TMCM)
- Syslog
- Windows Unified Connector (WUC)

Viewing All Containers

You can view all containers managed in ArcSight Management Center.

To view all containers:

1. Click **Node Management**
2. In the navigation tree, click **System**. (Alternatively, to view containers on a specific host, select the host from the navigation tree.)
3. Click the **Containers** tab to display the containers.

Viewing Connectors in a Container

You can see all the connectors in a container.

To view connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container whose connectors you wish to view.
3. Click the tree branch corresponding to the container.
4. Click the **Connectors** tab. The connectors in the container are displayed.

Editing a Container

The default name for a container is *Container N*, where N is a sequential number that indicates the order in which the container was added. However, you can edit a container's default name.

To edit a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host with container you wish to rename.
3. In the list of containers, locate the container you wish to edit.
4. In the **Action** drop-down of the container, click **Edit Container**.

5. In **Name**, enter the new container name, and then click **Next**.
6. Click **Done**. The container is renamed.

Deleting a Container

When you delete a container, the connectors that it contains are also deleted.

To delete a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion. The selected containers are deleted.

Updating Container Properties

You can update existing container properties, delete them, or add new ones.

To update container properties:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to update.
5. Click **Properties**.
6. Follow the instructions in the wizard to update the container properties.

Note: When a property is removed, it is still visible until the container is restarted.

Changing Container Credentials

You can change the user name and password associated with each container.

Caution: A container's default user name is `connector_user` and the default password is `change_me`. ArcSight strongly recommends that for optimal security, you should change each container's credentials to a non-default value before deploying it to production.

To change container credentials:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to change the credentials.
5. Click **Credentials**.
6. Follow the instructions in the wizard to update the credentials for the selected containers.

Sending a Command to a Container

You can run commands on a container to configure memory settings, pull an OPSEC certificate, generate a key, or restart the container.

To run a command on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. In the **Action** drop-down of the container, click **Send Container Command**. The Send Command wizard starts.
5. From the drop-down list, select the command you want to send, and then click **Next**.
6. Enter appropriate values for the parameters and then click **Done**.

Upgrading All Connectors in a Container

You can upgrade all connectors in a container to a specific parser or framework version number.

Before Performing the Upgrade

Prior to performing an upgrade of a container, you will need one of the following:

- You can use a connector AUP file of the new parser or framework version in your ArcMC repository. If you opt to use this method, you will need to upload the version file to your repository as follows:

To upload a version file to your repositories.

1. Click **Administration > Repositories**.
2. In the navigation tree, pick **Upgrade Files**.

3. In the management panel, click **Upload**.
4. Click **Choose File** and browse to your connector AUP file, then click **Submit**. The file is uploaded.
- Alternatively, instead of using a parser AUP file from the repository, you can download and use parser files from the [ArcSight Marketplace](#). (Framework files are not available from the Marketplace.) Create your administrative account on the ArcSight Marketplace. If you have not created your Marketplace account, you will be given an opportunity to sign up for an account during the parser upgrade process.

To perform the parser or framework upgrade on all connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to upgrade.
5. Click **Upgrade**.
6. On the upgrade page, under **Select Upgrade Type**, choose either **Parser upgrade** or **Framework upgrade**.
7. Under **Select Upgrade Version**, from the drop-down list, choose the version to which you want to upgrade the selected containers. (You can control the number of parser upgrade versions displayed in the drop-down, as described in [Modifying logger.properties](#).)
 - a. For a parser upgrade, if the selected parser version is from the Marketplace and not the local repository, save your Marketplace credentials in ArcMC. This is a one-time task unless you wish to update these credentials.
8. Click **Upgrade**. The upgrade is performed on all containers.

If you are performing parser upgrades through a proxy server, additional configuration is required. See [Modifying logger.properties](#) for more information.

Modifying logger.properties

To enable or modify some functionality, such as performing you may need to edit the file `<install_dir>/userdata/arcmc/logger.properties` with additional parameters in any text editor.

General Editing Procedure

If `<install_dir>/userdata/arcmc/logger.properties` does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsight' user, and for software ArcMC, use the non-root account used to install the ArcMC.

The `logger.properties` file may not be readable and writable by all users. Apply the following commands to the file.

```
chown <non-root user>:<non-root user> logger.properties
```

```
chmod 660 logger.properties
```

Finally, *restart the web process* after making any edits to `logger.properties`.

For Parser Upgrades Through a Proxy Server

If performing parser upgrades, and your environment connects to the Marketplace through a proxy server, you will need to modify the `<install_dir>/userdata/arcmc/logger.properties` file with the proxy details.

```
proxy.server=<server address>
```

```
proxy.port=<server port>
```

#Enter the proxy server credentials if the proxy server needs authentication

```
proxy.username=<username>
```

```
proxy.password=<password>
```

For the Number of Parser Upgrade Versions Displayed

You can control the number of parser upgrade versions displayed in the parser upgrade drop-down list. In `logger.properties`, set the parameter

```
marketplace.parser.update.latest.versions.count = <number of parser upgrade versions to be retrieved from Marketplace>
```

To Disable the Marketplace Connection

To disable ArcMC's Marketplace connection, in `logger.properties`, set the parameter

```
marketplace.enable=false
```

If set to false, parser upgrade versions from the Marketplace will not be shown in the drop-down list. In addition, the Parser Out of Date status (on **Node Management > Containers** tab, **Parser Version** column) will not be available.

Restarting a Container

Restarting a container will restart all the connectors in the container. You can restart multiple containers in bulk.

To restart one or more containers:


1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which a container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to restart.
5. Click **Restart**.
6. Click **Yes** to confirm restart. The selected containers are restarted.

Viewing Container Logs

You can retrieve and view the log files for one or more containers. The log files are in .zip format.

Container logs must be uploaded to the Logs repository before they can be viewed. For instructions on how to upload logs, see ["Uploading a File to the Logs Repository" on page 218](#).

To retrieve and view container logs:


1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to view logs.
5. Click **Logs**.
6. Click **Next** to begin the **Retrieve Container Logs** process. When complete, click **Done**.
7. Click **Administration > Repositories**.
8. In the left panel, click **Logs**.
9. In the management panel, click  to retrieve the log files (in .zip format) you want to view.

Deleting a Container Log

You can delete unneeded container logs as necessary.

To delete a container log file:

1. Click **Administration > Repositories**.
2. In the left panel, click **Logs**.

3. In the management panel, on the list of logs, click  next to the log file you want to delete.
4. Click **OK** to confirm deletion.

Enabling FIPS on a Container

FIPS mode is supported on local, and remote connectors and Collectors running version 4.7.5 or later, but certain connectors do not support FIPS mode. For information about which connectors do not support FIPS mode, see the document [Installing FIPS-Compliant SmartConnectors](#), available on [Protect 724](#). Before enabling FIPS on a container that contains connectors running as a service, review the caveats listed in that document.

FIPS is disabled by default on ArcSight Management Center, but can be enabled as described under ["FIPS 140-2" on page 266](#). After FIPS is enabled on the appliance, you can enable FIPS on a container. Any FIPS-compliant connector in that container (or one which is added later) will automatically communicate in FIPS mode.

- If the connector destination is ArcSight Manager, Connector Management automatically imports the ArcSight Manager certificate into its trust store and applies it to the container.
- However, if the connector destination is Logger, the Logger certificate must be uploaded manually and applied to the container.

A FIPS Suite B certificate must be uploaded manually, regardless of the connector destination, as described in under “Enabling FIPS Suite B on a Container”, below.

You enable or disable FIPS by the same procedure.

To enable or disable FIPS mode on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to enable FIPS.
5. Click **FIPS**.
6. Follow the instructions in the wizard to update FIPS status.

Check that the appropriate CA certificates are in the trust store so that the connectors in the container can validate their configured destinations successfully. If necessary, add the appropriate certificates to the container.

A 32-bit FIPS connector enabled cannot be remotely managed if it is installed on a 64-bit Linux system.

Enabling FIPS Suite B on a Container

Managed connectors can communicate in FIPS Suite B mode with their destination. A FIPS Suite B certificate must be imported manually and applied to the container, regardless of the connector destination.

Before you perform the following procedure, make sure FIPS mode is enabled on ArcSight Management Center, as described in ["FIPS 140-2" on page 266](#).

To enable FIPS Suite B on a container:

1. Export the certificate for the connector destination (either ArcSight Manager or Logger) to a temporary directory. For example, on ArcSight Manager, from \$ARCSIGHT_HOME/current/bin, enter the following command: `./arcsight runcertutil -L -n mykey -r -d /opt/arcsight/manager/config/jetty/nssdb -o /tmp/managercert.cer`
2. Upload the certificate from the temporary directory to the CA Certs Repository, as described in ["CA Certs Repository" on page 218](#).
3. Enable FIPS on the container as described above.
4. Add the certificate on the container, as described in ["Managing Certificates on a Container" on the next page](#).
5. Click **Node Management**.
6. In the navigation tree, navigate to the host on which the container resides.
7. Click the **Containers** tab.
8. On the **Containers** tab, select one or more containers for which to enable FIPS Suite B.
9. Click **FIPS**.
10. Follow the instructions in the wizard to update FIPS Suite B status.

Adding a Connector to a Container

Each container may hold up to 4 connectors.

To add a connector to a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container to which you wish to add a connector.
3. On the **Connectors** tab, click **Add Connector**. The **Connector Setup** wizard starts.
4. Click **Next**, and then follow the prompts to set up the new connector.

Note: Always change the default credentials of any new connector to non-default values. For more information, see ["Changing Container Credentials" on page 106](#).

Running Logfu on a Container

The **Logfu** utility is a diagnostic tool that parses ArcSight logs to generate an interactive visual representation of the information contained within the logs. When event flow problems occur, it can be useful to have a visual representation of what happened over time.

To run Logfu on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, locate a container on which to run Logfu.
5. In the **Action** drop-down of the container, click **Run Logfu**.
6. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
 - In the **Group** box, choose which type of data you would like to view. The **Group** box lists all connectors within the chosen container, plus many other types of data such as memory usage and transport rates.
 - Then, choose one of the Group box **data points**. Depending on which data point you chose, a list of fields appears in the Field box below.
 - Choose a **field** to view. A graphic chart appears in the Chart box, providing rate and time information. The key at the bottom of the Chart box defines the data points mapped in the chart.
 - To choose a different data point for analysis, click **Reset Data**.
7. When complete, close the display window.

Managing Certificates on a Container

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The Certificate Management wizard, available from the **Containers** tab, helps you add and remove certificates on a container. Using the wizard, you can:

- Add a certificate to a container.
- Add certificates in bulk, enabling multiple containers at once.
- Enable or disable a demo certificate on a container that is in non-FIPS mode only.

- Add a CA Certs file on a container that is in non-FIPS mode only.
- Remove a certificate from a container.


From the **Containers** tab and the **Connectors** tab, you can view details about the certificates applied to a container. See ["Viewing Certificates on a Container" on page 117](#).

For information about resolving invalid certificates, see ["Resolving Invalid Certificate Errors" on page 117](#).

Adding CA Certificates to a Container

You can add a single CA certificate to a container that is in FIPS mode or non-FIPS mode.

Note: Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Hover over a container name to see the type of certificate applied to it. Click the  icon to display a list of the certificates available on the container.

Before you perform the following procedure, make sure the certificate you want to add is loaded in the CA Certs repository.

To add a single CA certificate to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to add certificates.
5. Click **Certificates**. The Certificate Management wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Add Certificate**, and then click **Next**.
8. Follow the instructions in the wizard to add the certificate.

If a container is down or a connector is running an older build, the wizard reports errors in the progress bar and on the Summary page.

Removing CA Certificates from a Container

You can remove CA certificates from a container when they are no longer needed. When you remove a CA certificate, the certificate is removed from the container's trust store; but it is **not** deleted from the repository.

Caution: Use caution when deleting certificates. When you delete a certificate on a container but the connector destination is still using that certificate, the connector can no longer communicate

with the destination.

To remove CA certificates from a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to remove certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Remove certificate**, and then click **Next**.
8. Select one or more certificates from the certificate list, and then click **Next**. The certificates are removed from the list of certificates and no longer used. When you remove a certificate from a container in FIPS mode, the container restarts automatically.
9. The Certificate Management wizard displays the certificates that are removed successfully in a comma-separated list. Certificates that cannot be removed are shown in a comma-separated list together with a reason why the certificate removal failed.

Adding a CA Certs File to a Container

You can add a CA Certs file to any container that is in non-FIPS mode.

Caution: When you apply a CA Certs file, the entire trust store on the container is overwritten. All previously-added certificates are overwritten.

Before you follow the procedure below, make sure that the CA Certs file you want to add is loaded in the CA Certs repository.

To add a CA Certs file to a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers to which you wish to add a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **CA Cert (Legacy)**.

8. Follow the instructions in the wizard.

After the CA Certs file has been added to a container, the container restarts automatically.

Enabling or Disabling a Demo Certificate on a Container

You can use the demo certificate on a container for testing purposes. By default, the demo certificate on a container is disabled. You can enable the demo certificate temporarily for testing purposes on a container that is non-FIPS mode.

Note: Enable a *demo* certificate on a container in non-FIPS mode for testing purposes only. Using a demo certificate in a production environment is a serious security issue because the demo certificate is not unique.

To enable or disable a demo certificate on a non-FIPS mode container:


1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers for which you wish to enable or disable a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Demo CA (Legacy)**, and then click **Next**.
8. Follow the instructions in the Certificate Management wizard.

After you add the demo certificate on a container, the container restarts automatically.

Adding Multiple Destination Certificates to a Container

You can add multiple destination certificates to a container, whether in FIPS mode or not.

Note: Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Click the  icon to display a list of the certificates available on the container.

To apply multiple destination certificates to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.

4. On the **Containers** tab, containers for which you wish to add multiple destination certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Import destination certificates** to add a certificate.
8. Follow the instructions in the wizard to complete the process.

Viewing Certificates on a Container

You can display a list of the CA certificates applied to a container and view the details for a particular certificate in the list. To view certificates on a container,

- On the **Containers** tab, in the **Action** drop-down for the container whose certificates you want to view, select **Display Certificates**.
- On the **Connectors** tab, click **Certificates** at the top of the page.

The Certificate List wizard displays the certificates applied to a container. To see details of a certificate, select the certificate, and then click **Next** at the bottom of the page.

Resolving Invalid Certificate Errors

If no valid CA certificates exist for the connectors in the container, resolve the invalid certificate error as follows:

To resolve the invalid certificate error:

1. Select the container in the navigation tree.
2. Click the **Containers** tab. The error message is displayed.
3. In the **Action** drop-down of the container showing the issue, select **Download Certificates**.
4. Follow the instructions in the wizard to download and import the valid certificates.

Running Diagnostics on a Container

You can run diagnostics on a container.

Note: Diagnostic tools are also provided under **Administration > System Admin**.

To run diagnostics on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.

4. On the **Containers** tab, select one or more containers for which to run diagnostics.
5. In the **Action** drop-down, click **Run Logfu**. The Diagnostics wizard starts.
6. Select the action you want to take on the selected container:
 - Select **Edit a configuration file** to edit a file in the `user/agent` folder on the container with the extension `.properties`, `.csv`, or `.conf`.
 - Select **Edit a user file** to edit any file (except binary files, such as `.zip`, `.jar`, or `.exe`) in the `user/agent` folder on the container.
7. From the list of available files, select the file you want to edit. The file displays in the Edit File panel. Make your edits, and then click **Next** to save your edits and restart the container.

Note: When you click **Next**, ArcSight Management Center saves the updated file in the `user/agent` folder on the container. The original file is overwritten.
8. Click **Done** to close the Diagnostics wizard.

Managing Connectors

A *connector* (also known as a *SmartConnector*) is an ArcSight software component that collects events and logs from various sources on your network. A connector can be configured on ArcSight Management Center, on a Logger platform with an integrated Connector Appliance, or installed on a computer on your network, managed remotely. For a complete list of supported connectors, go to the ArcSight Customer Support site.

Procedures for managing connectors are described below.

Viewing All Connectors

You can see all currently managed connectors.

To view all connectors:

1. Click **Node Management**.
2. Click **System** in the navigation tree.
3. In the management panel, click the **Connectors** tab. All connectors display on the **Connectors** tab in the management panel.

Adding a Connector

Prerequisites

Before you add a connector, review the following important information.

- Make sure that the container, host, and location to which you want to add the connector exist in ArcSight Management Center. If any of these elements do not exist, create them.
- Follow the configuration best practices described in ["Configuration Suggestions for Connector/Collector Types" on page 142](#).

If you are configuring the Check Point OPSEC NG Connector, see ["Configuring the Check Point OPSEC NG Connector" on page 143](#) and refer to the SmartConnector Configuration Guide for Check Point OPSEC NG.

If you are configuring a database connector that requires the MS SQL Server Driver for JDBC, follow instructions in ["Adding the MS SQL Server JDBC Driver" on page 146](#).

Caution: This connector type has special requirements concerning JDBC and authentication setup. Refer to the SmartConnector Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB for this important information before installing the connector.

- If you are adding a software-based connector, make sure that the username and password for the connector match the username and password for the container to which you are adding the connector. If necessary, refer to ["Changing Container Credentials" on page 106](#).

Caution: Each connector's default user name is `connector_user` and the default password is `change_me`. A connector with these default values still in place should be considered non-secure. ArcSight strongly recommends that for optimal security, you should change each connector's credentials to non-default values before deploying the connector to production.

- File-based connectors use the Common Internet File System (CIFS) or Network File System (NFS). These stipulations apply when creating a local connector to run as part of ArcMC.
 - On a Windows system, a CIFS share needs to be configured before you add a file-based connector.
 - For all other connectors, an NFS mount needs to be established before a file-based connector can be added. In addition, when entering the connector parameters, enter the configuration file name without an extension in the **Configuration File** field. The extension `.sdkrfilereader.properties` is appended automatically.
- For detailed information about individual connector parameters, refer to the specific ArcSight SmartConnector Configuration Guide for the type of connector chosen. The configuration guide also describes how to set up the source device for use with the connector

To add a connector:

Tip: If you are adding a connector for the Check Point FW-1/VPN-1 system, see a more detailed procedure in ["Configuring the Check Point OPSEC NG Connector" on page 143](#).

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the connector will reside.
3. In the management panel, click the **Containers** tab.
4. On the **Containers** tab, locate the container where you will assign the connector.
5. In the **Action** drop-down, click **Add Connector**. The Connector Setup wizard starts.
6. Review the dialog box, and then click **Next**.
7. Select a connector type from the pull-down list of available types, and then click **Next**.
8. Enter basic parameters for the connector. Parameters vary based on the connector type. (Hover over a field for more information on a field.) When all fields have been entered, click **Next**.

Note: When entering parameters that include a file path, enter the path in POSIX format (for example, /folder/filename).

For file-based connectors on Windows systems, specify the name of the CIFS mount point you created for the connector. (You need to specify `/opt/mnt/CIFS_share_name`.)

Some connectors include table parameters. For example, the Microsoft Windows Event Log includes parameters for each host in the domain and one or more log types (security, application, system, directory service, DNS, file replication, and so on). You can import table parameters from a CSV file. You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

Note: For connectors that query Microsoft Active Directory to detect devices (for example, Microsoft Windows Event Log - Unified), if the "Network Security: LDAP Server Signing Requirements" policy is set to "Signing Required" on the Domain Controller, ArcSight Management Center will be unable to connect to the Active Directory or browse for devices. You see an error when selecting **Windows Host Browser** as the connector device browser type.

9. Choose a primary destination for the connector and enter destination-specific parameters on the following page(s), and then click **Next**. Destinations can be:
 - ArcSight Logger SmartMessage (encrypted)
 - ArcSight Manager (encrypted)
 - CEF Syslog (plaintext, that is, unencrypted)

Note: FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination, and then click Next** if you do not want to import the certificate. The destination will not be added.

10. Enter connector details:

Parameter	Description
Name	A descriptive name for this connector.
Location	The location of the connector (such as the hostname).
Device Location	The location of the device that sends events to the connector.
Comment	Additional comments.

11. When complete, click **Done**.

Editing Connector Parameters


ArcSight supports a large number of connector types to gather security events from a variety of sources, including syslog, log files, relational databases, and proprietary devices. Accordingly, configuration parameters vary widely depending on the type of connector being configured.

You can edit parameters (simple and table) for a specific connector, or for multiple connectors of the same type at the same time.

Updating Simple Parameters for a Connector

The following procedure describes how to update simple parameters for a specific connector.

To update parameters for a specific connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector you wish to update.
3. In the management panel, the **Connector** summary tab displays.
4. On the **Connector** tab, next to **Connector Parameters**, click .
5. Modify parameters as necessary, and then click **Next**.


Note: When editing parameters that include a file path, enter the path in POSIX format (for example, /folder/filename).

6. When complete, click **Done**. The updated parameters display in the **Connector Parameters** table of the Connector summary tab.

Updating Table Parameters for a Connector

Certain connectors, such as the Microsoft Windows Event connector, have table parameters. You can update the table parameters for a specific connector when necessary.

To update table parameters for a specific connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector you wish to update. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Table Parameters**, click .
4. Modify parameters as necessary and then click **Next**.
 - To add more rows of parameter information, click the **Add Row** link.
 - You can use an Excel-compatible program to prepare a comma-separated values text file with the information and click the **Import File** button to load the entire table at once. The file needs to be in the same format as the rows shown on the Update Table Parameters page and needs to include a header row with parameter labels in the order shown on that page. For fields that require checkbox values, enter True or False as the value. An example is shown below
5. When complete, click **Done**. The updated table parameters display in the Table Parameters section of the Connector page.

Note: You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

	A	B	C	D	E	F
1	Domain Name	Host Name	User Name	Password	Security Logs	System Logs
2	test	1.1.1.1	admin	password	TRUE	FALSE
3	test2	1.1.1.1	admin	password	TRUE	FALSE

Updating Simple and Table Parameters for Multiple Connectors

If you have multiple connectors of the same type, you can change the simple and table parameters for all the connectors at the same time.

To edit parameters for multiple connectors of the same type:

1. Click **Node Management**.
 2. In the navigation tree, select the host where the connectors reside.:
 3. In the management panel, select the connectors whose parameters you want to update.
 4. Click **Parameters**. The Update Connect Parameters wizard starts.
 5. Review the dialog box, and then click **Next**.
 6. Follow the instructions in the wizard.
 - You can choose to modify the simple parameters for all the selected connectors at once or modify the simple parameters per connector.
 - If the connectors have table parameters, the table parameters are displayed so that you can modify them. If you have many table parameters to modify for multiple connectors, you can import the parameters from a CSV file. You can also export the table parameters to a CSV file for use as a backup or to import on another Connector Appliance.
- Note:** When you update parameters for connectors of different versions, the newer connectors might have additional parameters. In this case, only those parameters shared by all connectors are displayed for updating.
7. Click **Done** when complete.

Managing Destinations

Connectors can forward events to more than one destination, such as ArcSight Manager and ArcSight Logger. You can assign one or more destinations per connector. You can assign multiple destinations to a connector and specify a failover (alternate) destination in the event that the primary destination fails.


The following procedures describe how to perform these actions on a specific connector or for multiple connectors at the same time:

- Add a primary or failover destination
- Edit destination parameters and destination runtime parameters
- Remove destinations
- Re-register destinations
- Manage alternate configurations for a destination
- Send a command to a destination

Adding a Primary Destination to a Connector

When you add a primary destination to a connector, you need to enter details for the destination, such as the destination hostname and port used.

To add a primary destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Destinations**, click . The Add Destination wizard starts.
4. Follow the steps in the wizard. You can either select an existing destination or add a new destination. If you are adding a new destination, select the destination type and enter parameters for the destination. Destination types are described in the SmartConnector User's Guide.

Note: For containers running 5.1.2.5823 and later, ArcSight Management Center retrieves the certificate for the ArcSight Manager destination automatically and displays the certificate summary.

For containers running 5.1.2 and earlier, upload the certificate on the container and then add the destination.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.


5. Click **Done** when complete.

Adding a Failover Destination to a Connector

Each destination can have a failover destination that is used if the connection with the primary destination fails.

Tip: UDP connections cannot detect transmission failure. Use Raw TCP for CEF Syslog destinations.

To add a failover destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click . The Add Destination wizard

starts.

4. Follow the steps in the wizard to select from available destinations and enter the destination details.

Note: FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.


- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Primary or Failover Destination to Multiple Connectors

You can add a primary or failover destination to several connectors at the same time.

To add a primary or failover destination to multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click  **Destinations. The Manage Destinations wizard launches.**
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Add a destination, and then click Next**.
8. Choose between a creating a new destination or selecting an existing destination, and then click **Next**.
 - If you choose to **create a new destination**, select the destination type and then provide the destination parameters. Destination types are described in the SmartConnector User's Guide.
 - If you choose to **select an existing destination**, select a destination from the list.

Note: ArcSight Management Center retrieves the ArcSight Manager certificate for the destination automatically and displays the certificate summary.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from destination**, and then click **Next** to import the certificate and continue.


- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

9. Define the destination function by choosing between a primary or failover destination.
 - If you choose **Primary destination**, click **Next** to update the configuration.
 - If you choose **Failover destination**:
 - a. Select the primary destination that applies to your failover.
 - b. Check the box in the table header to modify all of the displayed connectors.
 - c. Click **Next** to update the configuration.
10. Click **Done** when complete.


Removing Destinations

You can remove a destination from a connector at any time. Each connector must have at least one destination; as a result, you may not remove all destinations from a connector.

To remove a single destination from a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector from which you wish to remove a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click  for the destination you want to remove.
4. Click **OK** to confirm removal.

To remove *multiple* destinations from one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click  **Destinations. The Manage Destinations wizard launches.**
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Remove a destination, and then click Next**.
8. Follow the instructions in the wizard, and click **Done** when complete.

Re-Registering Destinations

At certain times, you might need to re-register the destinations for one or more connectors; for example, after you upgrade ESM, or if a Logger appliance or ESM appliance becomes unresponsive.


To re-register destinations for one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click **Destinations. The Manage Destinations wizard launches.**
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Re-register destinations**, and then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Parameters

The following procedures describe how to edit destination parameters for a specific connector and how to edit destination parameters for multiple connectors.

To edit destination parameters for a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to edit destination parameters.
In the management panel, the **Connector** summary tab displays.
3. In the **Destinations** table, click  next to the destination you want to edit to display the **Edit Destination Parameters** page.
4. Make your changes, and then click **Next**.
5. Click **Done** when complete.

To edit destination parameters for *multiple* connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination parameters.
5. Click **Destinations. The Manage Destinations wizard opens.**


6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Edit a destination**, and then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.


Editing Destination Runtime Parameters

The runtime parameters for a destination enable you to specify advanced processing options such as batching, time correction, and bandwidth control. The parameters you can configure are listed in ["Destination Runtime Parameters" on page 299](#). The user interface automatically displays the parameters valid for a destination.

The following procedures describe how to edit the runtime parameters for a specific connector and how to edit the runtime parameters for multiple connectors at the same time.

To edit destination runtime parameters for a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click next to the destination whose runtime parameters you want to edit.
4. Under **Add Alternate Configurations**, click  next to the alternate configuration that you want to edit.

If you have not set up alternate configurations, click  next to the **Default**. For more information about alternate configurations, see ["Managing Alternate Configurations" on the next page](#).

5. Specify or update values for the listed parameters, and then click **Save**.

To edit destination runtime parameters for *multiple* connectors at the same time:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination runtime parameters.
5. Click **Runtime Parameters** to open the wizard.
6. Follow these steps in the wizard to edit the runtime parameters:
 - a. Select the destinations whose runtime parameters you want to modify.
 - b. Select the configurations to be affected (default or alternate configurations).
 - c. Select the group of parameters you want to modify (for example, batching, cache, network,

processing).

- d. Modify the parameters.

Managing Alternate Configurations

An *alternate configuration* is a set of runtime parameters that is used instead of the default configuration during a specified portion of every day. For example, you might want to specify different batching schemes (by severity or size) for different times of a day. You can define more than one alternate configuration per destination, and apply them to the destination for different time ranges during the day. For example, you can define a configuration for 8 a.m. to 5 p.m. time range and another configuration for the 5 p.m. to 8 a.m. time range.


By default, a configuration labeled **Default** is applied to a destination. Any subsequent configurations you define are labeled **Alternate#1**, **Alternate#2**, and so on. The default configuration is used if the time ranges specified for other alternate configurations do not span 24 hours. For example, if you specify an alternate configuration, **Alternate#1** that is effective from 7 a.m. to 8 p.m., the **Default** configuration is used from 8 p.m. to 7 a.m.

If you need to apply the same alternate configuration for multiple destinations, you need to define an alternate configuration (with the same settings) for each of those destinations.

Defining a New Alternate Configuration

The process of defining a new alternate configuration includes first defining the configuration, and then editing it to specify the time range for which that configuration is effective.

To define an alternate configuration:



1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Under **Add Alternate Configurations**, click **Add**.
5. Specify or update values for the listed parameters.
6. Click **Save**. If this is the first alternate configuration you defined, it is saved as Alternate#1. Subsequent configurations are saved as Alternate#2, Alternate#3, and so on.

To specify the effective time range for which the configuration you just defined, edit the configuration you just defined using the following procedure, ["Editing an Alternate Configuration" on the next page](#).

Editing an Alternate Configuration

In addition to editing an alternate configuration to change parameter values, you can edit it to specify the time range for which it is effective.

To edit an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. From the list of alternate configurations, select the alternate configuration that you want to edit, and then click .
5. Specify or update values for the listed parameters, including the time range in the From Hour/To Hour.
6. Scroll down to the end of the page and click **Save**.


Editing Alternate Configurations in Bulk

If you need to update the same parameters in multiple alternate configurations, follow the procedure described in ["Editing Destination Runtime Parameters" on page 128](#).

Sending a Command to a Destination

You can send a command to a connector destination.


To send a command to a destination on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Select the command you want to run, and then click **Next**.
5. Enter values for the parameters that the user interface displays, and then click **Finish**.

Deleting a Connector

To delete one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors the connectors you want to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion.
7. Reboot the Connector Appliance or Logger system that each connector was associated with.

Note: You can also delete a specific connector from its **Connector** summary tab. Click  at the top of the tab to delete the connector.

Sending a Command to a Connector

You can send a command to a connector.

To send a command to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, click **Connector Command**.
4. From the **Command Type** drop-down list, select the command you want to send to the connector, and then click **Next**.

Running Logfu on a Connector

Run Logfu on a connector to parse ArcSight logs and generate an interactive visual representation of the information contained within the logs.

To run Logfu on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to run Logfu. In the management panel, the **Connector** summary tab displays.

3. On the **Connector** summary tab, click **Run Logfu**.
4. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
 - In the **Group** box, choose a data type to view. The **Group** box lists all connectors within the chosen container, plus many other data types, such as memory usage and transport rates.
 - Next, choose one of the **Group** box **data points**. Depending on which data point you chose, a list of fields appears in the **Field** box below.
 - Choose a **field** to view. A graphic chart appears in the **Chart** box, providing rate and time information. The key at the bottom of the **Chart** box defines the data points mapped in the chart.
 - To choose a different data point for analysis, click **Reset Data**.
5. When complete, close the Logfu display window.

Enabling SecureData Encryption on Managed Connectors

SecureData can be enabled as part of the [Instant Connector Deployment](#) process. However, you can also enable SecureData encryption on connectors or containers you [already manage in ArcMC](#).

To enable SecureData encryption on connectors or containers you already manage in ArcMC:

1. Ensure that the remote VM can communicate with the SecureData server. If not, edit the hosts file or configure DNS to enable communication.
2. If there is a certificate for the SecureData server, make sure the server certificate is successfully imported to the remote VM.
3. Ensure proxy settings allow the SecureData client to communicate with the SecureData server.
4. Install the SecureData client manually on the remote VM where the connectors reside.
5. Finally, in ArcMC, select the connectors or containers. Perform the Modify Property operation and provide the necessary SecureData and proxy details.

Remote File Systems

Your system can mount Network File System (NFS 3.0 only) and CIFS (Windows) shares. As a result, it can read log files and event data from UNIX, Linux, Windows remote hosts, and any Network Attached Storage (NAS) solutions based on these operating systems. You need to establish a CIFS mount before you can add a file-based connector on a Windows system to ArcSight Management Center.

Managing a Remote File System

Make sure the following requirements are met before you mount a share.

File System Type	Requirements
CIFS (Windows)	<ul style="list-style-type: none"> A user account that has access to the shared drive exists on the Windows system. The folder to which you are establishing the mount point is configured for sharing. Note: NTLMv2 and NTLMv2i authentication are supported. NTLMv2i support on Windows 2008 R2 requires installation of Microsoft hotfix KB957441.
NFS	<ul style="list-style-type: none"> Grant your ArcSight system read and write permission on the NFS system. The account used for mounting must use the numeric ids 1500 for uid, or 750 for gid.

To add a Remote File System mount:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Remote File Systems** in the **Storage** section in the left panel.
The Remote File Systems form is displayed.
3. Click **Add** from the top left side of the page and enter values for the following fields in the resulting form.

Parameter	Description
Select File System Type	Whether you want to mount an NFS or a CIFS share.
NFS Settings	
Name	A meaningful name for the mount point. The name cannot contain spaces. This name is used locally on your system to refer to the mount point, and needs to be specified when configuring archive settings for data that will be stored on the share.
Hostname / IP Address	The name or IP address of the host to which you are creating the mount.
Remote Path (for NFS)	<p>The folder on the remote host that will act as the root of the network file system mount. For example, /public/system_logs.</p> <p>Make sure that only this system can write to the location you specify in this field. If multiple systems (or other systems) mount this location and write to it, data on this location will be corrupted.</p>
Mount Options	<p>AutoFS options. For example, ro for read-only from the remote host, rw for read-write, or hard to keep retrying until the remote host responds.</p> <p>Note: Even if you configure rw permission at your mount point, rw permission is not granted to the remote host if the host is configured to allow read-only access.</p> <p>Note: NTLMv2 and NTLMv2i authentication are supported.</p>
Description	A meaningful description of the mount point.
CIFS Settings	

Parameter	Description
Name	A meaningful name for the mount point. The name cannot contain spaces. This name is used locally on your system to refer to the mount point, and needs to be specified when configuring archive settings for data that will be stored on the share.
Location	<p>Enter the share name in one of the following ways:</p> <ul style="list-style-type: none"> Share name in this format: <IP Address> or <Hostname>:<share_name> For example, 198.0.2.160:myshare This folder needs to be configured for sharing. (Typically, to configure a Windows folder for sharing, right click on the folder name > Properties > Sharing.) Caution: when mounting from a Windows Server 2008 in cluster, you must use the Hostname and not the IP address for a successful mount. UNC path For example, //198.0.2.160/myshare
Mount Options	<p>Autofs options. For example, ro for read-only from the remote host, rw for read-write, or hard to keep retrying until the remote host responds.</p> <p>Note: Even if you configure rw permission at your mount point, rw permission is not granted to the remote host if the host is configured to allow read-only access.</p> <p>Important: For log file connectors (for example, the Symantec AntiVirus connector), you need to enable the directio option so that ArcSight Management Center can process new events. Enter rw,directio in the File System Mount Options field.</p>
Description	A meaningful description of the mount point.
Credentials for CIFS	
Username	<p>The name of the user account with read-write privileges to the Windows share.</p> <p>Make sure the username is prefixed with the domain information. For example, tahoe\arcsight.</p>
Password	The password for the user name specified above.

4. Click **Add**.

All mount points are created under /opt/mnt. Note the name of the mount point you create. You need to specify this name when adding a connector that will use this share to ArcSight Management Center.

To edit a Remote File System mount:

Note: You cannot edit a mount point if it is in use. The **Edit** link is displayed only if the mount point can be edited.

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Remote File Systems** in the **Storage** section in the left panel.

3. Select the mount point you want to edit, and click **Edit** from the top left side of the page.
4. Change the field values.
5. Click **Save**.

To delete a Remote File System mount:

Note: You cannot delete a mount point that is in use. The **Delete** link is displayed only if the mount point can be deleted. Once stopped, expect up to a two minute delay before the mount can be edited or deleted.

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Remote File Systems** in the **Storage** section in the left panel.
3. Select the mount point you want to delete, and click **Delete** from the top left side of the page.

Changing the Network Interface Address for Events

ArcSight Management Center has multiple network interfaces. By default, the connector determines which network interface address is used for events displayed in the ArcSight Console or Logger, but typically uses eth0.

To use a specific network interface address for events, add the parameter `connector.network.interface.name` to the Connector's `agent.properties` file. For example, to use the IP address for eth1, specify the following parameter:

```
connector.network.interface.name=eth1
```

Developing FlexConnectors

FlexConnectors are custom, user-designed *SmartConnectors* that can read and parse information from third-party devices and map that information to ArcSight's event schema.

ArcSight Management Center provides a FlexConnector Development wizard that enables you to quickly and easily develop a FlexConnector by creating a parser file, and enables you to test and package your new FlexConnector before deploying it. The wizard generates regular expressions and provides event field mapping suggestions automatically so you do not need to be an expert in regular expression authoring, parser syntax, or ArcSight event schema.

Use the FlexConnector Development wizard to develop FlexConnectors for simple log files. For complex log files, use the FlexConnector SDK (available from the ArcSight Customer Support site)

The FlexConnector Development wizard supports Regex Files, Folder Follower, and Syslog (Daemon, File, Pipe) FlexConnectors only.

The FlexConnector Development wizard does not support the extra processors property or multiple sub-messages. If you need these features, use the FlexConnector SDK to create your FlexConnector.

Caution: A FlexConnector that you develop with the FlexConnector Development wizard might perform more slowly than an ArcSight *SmartConnector*.

To develop a FlexConnector:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where you wish to develop the connector.
3. In the management panel, click the **Connectors** tab.
4. On the **Connectors** tab, in the Action drop-down, click **Edit FlexConnector**. The FlexConnector Development wizard is launched.
5. Provide the vendor and product name of the device for which you are creating a FlexConnector, and then click **Next**.
6. Select the data source type, and then click **Next**:
 - Select **Syslog** to create a Syslog FlexConnector to read events from Syslog messages.
 - Select **File** to create a FlexConnector to parse variable-format log files using regular expressions (ArcSight FlexConnector Regex File) or to parse variable-format log files in batch mode (ArcSight FlexConnector Folder Follower).
7. Upload a sample log file for the data source type you selected in the previous step, and then click **Next**.
8. The wizard finds the first unparsed line in the log file, generates a regular expression to match and extract tokens from that line, and displays the suggested field mappings for each extracted token in the Mappings table.

FlexConnector Development Wizard

Enter regular expression corresponding to text Lines Skipped: 0% Lines Parsed: 0%

Text 2005 Aug 24 13:57:54 EDT -04:00 %SPANTREE-6-PORTFWD: Port 3/16 state in VLAN 203 changed to forwarding

Regex

Mappings table			
	Extracted Value	Type	Format
1	2005 Aug 24 13:57:54	TimeStamp	yyyy MMM dd HH:mm:
2	3/16	String	String
3	203	Integer	String

Extra Mappings table	
Event Field	Value
name	_stringConstant(SPAN)

Note: The mappings are displayed in descending order of probability (based on ArcSight training data). You can change the mappings by selecting from the list.

The percentage of parsed lines in the file is shown in the top right of the panel. You can use this percentage to estimate where you are in the log file. The percentage of unparsed lines skipped in the file is also shown in the top right of the panel.

- To change the regular expression in the **Regex** box and recalculate the mappings, edit the expression and then click the **Recalculate** button. You can set the regular expression back to the suggested value by clicking the **Reset** button.
- Field mappings that do not correspond directly to the extracted tokens in the unparsed line of the log file are displayed in the Extra Mappings table. You can change the Event Field and provide a token operation. To add a new Event Field, click **Add Row**.

You can use extra mappings to:

- Remap an extracted token to a different Event Field in addition to the existing mapping. For example, you can add an Event Field with the value `$3` where `$3` is the third token in the list of suggested mappings.
- Map a modified token or combination of tokens to an Event Field. For example, you can add an Event Field with the value `__operation($1,$3)`.
- Map an Event Field to a constant string or integer. For example, you can add an Event Field with the value `__stringConstant(constant)`.

For a list of the token operations used when tokens are mapped to ArcSight event fields, refer to the FlexConnector Developer's Guide (available from the ArcSight Customer Support site).

9. Click **Next** to save the mapping to the parser file and display the next unparsed line in the log file. After all unparsed lines in the log file have corresponding regular expressions and mappings, the wizard displays the parser file for review.
10. Review the parser file and make changes, if necessary, directly in the Review Parser File panel.
11. Click **Next** to save and package the parser file.
12. Choose how you want to deploy the FlexConnector:
 - Select **Deploy parser to existing connector in container**, and then click **Next** to use the parser file with an existing connector. Click **Done** to close the FlexConnector wizard and re-display the **Container** tab.

Note: The **Deploy parser to existing connector in container** option displays only if the container already contains a connector of the same type.

- Select **Add new connector to container**, and then click **Next** to add the parser as a new connector. Follow the steps to add the connector to the container.

You can share FlexConnectors with other users. See ["Sharing Connectors in ArcExchange" on the next page](#).

Editing FlexConnectors

After you have developed a FlexConnector with the FlexConnector wizard and have deployed it in a container, you can edit the FlexConnector to make changes to the parser file when needed.

The FlexConnector Edit wizard is available on the **Connectors** tab in the **Action** drop-down.

Click **Edit Connector** in the **Action** drop-down for the FlexConnector to open the wizard, then edit the parser file.

Caution: Only edit a FlexConnector that is created with the FlexConnector wizard. Editing manually-created FlexConnectors might produce unpredictable results.

Sharing Connectors in ArcExchange

You can share FlexConnectors and parser overrides with other users.

A FlexConnector is a custom connector that you define to gather security events from log files, databases, and other software and devices. You can share the following FlexConnector types:

- Syslog FlexConnectors (to read events from syslog messages)
- Log File FlexConnectors (to read fixed-format log files)
- Regular Expression Log File FlexConnectors (to read variable-format log files)
- Regular Expression Folder Follower FlexConnectors (to read variable-format log files recursively in a folder)
- Regular Expression Multiple Folder Follower FlexConnectors (to read events in real time or batch mode from multiple folders)
- XML FlexConnectors (to read events recursively from XML-based files in a folder)

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added. You can share parser overrides for all connector types that use a parser.

To share a FlexConnector or parser override, you need to package and upload it to ArcExchange on the ArcSight online community (Protect 724) or to your local machine. You can also download a FlexConnector or parser override that you need from ArcExchange or from your local machine and add it to a container.

Note: ArcExchange will not be able to reach the ArcSight Protect724 Community if access is attempted through a proxy server.

Packaging and Uploading Connectors

Before uploading your FlexConnector or parser override to Protect 724 or to your local computer, you need to package it into a zip file, (called an AUP package) using the upload wizard.

A FlexConnector AUP package contains the connector properties file, categorization file, connector parameters, and a manifest file with all the metadata on the package required for successful deployment. Metadata includes information about the AUP package, such as the package type, connector type, connector description, and so on. You can create only one AUP package per connector per device type. You can package a FlexConnector in Basic or Advanced mode. In **Basic** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package.
- The wizard packages the categorization file automatically *only* if it can be determined based on the device vendor and product information found in the properties file.
- The wizard does not package connector parameters. You are prompted to configure the connector when it is downloaded and deployed.

In **Advanced** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package. (This is same as Basic mode.)
- The wizard packages the categorization file automatically if it can be determined based on the device vendor and product information found in the properties file. If the categorization file cannot be determined, you are prompted to select the categorization file you want to package from the list of files found in the container.
- The wizard displays connector parameters so you can configure the parameters you want to display and set the default values you want to provide during connector deployment (download). The parameters you do not configure for display are pre-configured with the current values and will not be displayed during connector deployment.

A parser override package contains the parser override properties file and the manifest file only.


Follow the steps below to package and upload a FlexConnector or parser override.

- To upload to ArcExchange, you must have a valid username and password for Protect 724.
- Make sure that you have configured network settings under **Administration > System Admin > Network** and that ArcSight Management Center can communicate with the Protect 724 server.

To package and upload a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to upload a package. In the

management panel, the **Connector** summary tab is displayed.

3. On the **Connector** details page, click . The upload wizard is launched.
4. Click **Next** and follow the steps in the wizard to:
 - a. Select the type of AUP package you want to create for the selected connector.
ArcSight Management Center scans the container and displays the relevant files that can be packaged.
 - b. For a FlexConnector, select **Basic** to create a default package or select **Advanced** to customize the package to meet your needs.
 - c. If the connector contains several properties files, you are prompted to select the properties file you want to package. Certain connectors, for example, syslog connectors, can have more than one parser override folder, in this case, you are prompted to select the folder you want to package.
 - d. If you selected Advanced mode for a FlexConnector previously, and the categorization file cannot be determined, you are prompted to select the categorization file you want to package from a list of files found in the container.

Note: Categorization files are not packaged for parser overrides.

- e. If you selected Advanced mode for a FlexConnector previously, select the configuration parameters you want to display when the connector is deployed and then provide default values for these parameters. Parameters you do not select are pre-configured with the current values.
If any advanced connector parameters were previously modified from their defaults, the wizard displays these parameters so that you can select which ones you want to be configured automatically during deployment.

Note: Configuration parameters are not displayed for parser overrides.

If the connector has table parameters, they are not displayed during packaging. However, when the connector is downloaded to a container, you are prompted to provide values for all the table parameters.

- f. Provide a description of the AUP package and instructions on how to configure the device used by the connector.
- g. Provide the vendor, product, and version of the device used by the connector.
If the wizard can determine the vendor, product, and version of the device, the information is displayed in the fields provided. You can change the information to meet your needs.
- h. Upload the created AUP package to ArcExchange or to your local machine. You will require a username and password for Protect 724.

Downloading Connectors

You can download a FlexConnector or parser override that is available from ArcExchange on Protect 724 or from your local computer. You download a FlexConnector or parser override directly to a container.

You can download only one FlexConnector per container using the download wizard. However, there is no limit to the number of parser overrides you can download to a container.

- When downloading a parser override to a container, the download wizard overwrites any existing parser override with the same name in the container without prompting for confirmation. To avoid overwriting an existing parser override, send a **Get Status** command to the existing parser override to check the parser information before you download a new parser override. For information on sending a Get Status command, refer to ["Sending a Command to a Connector" on page 131](#).
- Always back up the container to the Backup Files repository before downloading a connector or parser override so you can revert to the previous configuration if the download produces unexpected results.

Follow the steps below to download a FlexConnector or parser override to a container.

To download to ArcExchange, you must have a valid username and password for Protect 724. Also, make sure that you have configured network settings under **Administration > System Admin > Network** and that the appliance can communicate with the Protect 724 server.

To download a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the container resides.
3. In the management panel, click the **Containers** tab.
4. From the list of containers, locate the container into which you want to download the connector. In the **Action** drop-down, select **Run FlexConnector Wizard**.
5. Click **Next** and follow the steps in the wizard to:
 - a. Select whether you want to download the connector from ArcExchange on Protect 724 or from your local computer.
 - b. Select the AUP package you want to download.

On Protect 724, you can search for a parser override or FlexConnector AUP package using a keyword or a combination of keywords.

Note: You can only download a parser override package to a container that has a connector of the same type as the package.

You can download only one FlexConnector per container using the download wizard. If the container already contains a FlexConnector of the same type as the one you want to download, you can replace the existing FlexConnector with the one you are downloading, but you cannot create a new one.

- c. For a FlexConnector, provide connector configuration parameters, if needed.

Pre-configured and advanced parameters are deployed automatically with the values that were packaged; you are not prompted to configure these parameters. The configurable parameters are displayed with suggested defaults, which you can modify if necessary. The table parameters are displayed with no configured values, you have to provide the values manually, as needed.

- d. Add or select a destination for the connector.

If you are downloading the connector to a container that has an existing connector of the same type, you are *not* prompted for a destination.

The wizard copies the properties and categorization files to the appropriate locations and also installs the zip file for the AUP package in the `user/agent/deployedaups` folder on ArcSight Management Center to keep track of the deployment history.

After a successful download, the container is restarted automatically.

Configuration Suggestions for Connector/Collector Types

The following table provides configuration suggestions for different types of connectors or Collectors.

Connector/Collector Type	Effects of Limited Usage
Syslog	<p>Due to the nature of UDP (the transport protocol typically used by Syslog), these connectors/Collectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache might fill and the operating system drop UDP messages.</p> <p>Note: Do not use the Limit CPU Usage option with these connectors because of the possibility of event loss.</p>
SNMP	<p>Similar to Syslog connectors/Collectors, when the event rate is limited on SNMP connectors, they can potentially lose events. SNMP is also typically UDP-based and has the same issues as Syslog.</p>
Database	<p>Because connectors/Collectors follow the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. However, no events will be lost, unless the database tables are truncated. After the event burst is over, the connector might eventually catch up with the database if the event rate does not exceed the configured limit.</p>

Connector/Collector Type	Effects of Limited Usage
File	Similar to database connectors/Collectors, file-based connectors/Collectors <i>follow</i> files and limiting their event rates causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. The connectors might catch up if the event rate does not exceed the configured rate.
Asset Scanner	All connectors/Collectors on ArcSight Management Center run as a service (not as an application). Therefore, asset scanner connectors running on Connector Appliance are <i>not</i> supported in Interactive mode. To run the asset scanner connector in Interactive mode, install the connector on a standalone system and manage it as a software-based connector.
Proprietary API	The behavior of these connectors depends on the particular API, (for example, OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. These connectors work much like database or file connectors.

Included FlexConnectors

HPE ArcSight Management Center Connector Appliance includes these prototype FlexConnectors:

- ArcSight FlexConnector File
- ArcSight FlexConnector ID-based Database
- ArcSight FlexConnector Multiple Database
- ArcSight FlexConnector Regular Expression File
- ArcSight FlexConnector Regular Expression Folder File
- ArcSight FlexConnector Simple Network Management Protocol (SNMP)
- ArcSight FlexConnector Time-based Database
- ArcSight FlexConnector XML File

You can use these prototypes to develop your own FlexConnectors, and these can be shared with other users. Refer to ["Sharing Connectors in ArcExchange" on page 138](#).

For more information, consult the FlexConnector Developer's Guide, available from ArcSight Customer Support.

Configuring the Check Point OPSEC NG Connector

The Check Point FW-1/VPN-1 OPSEC NG connector can operate in clear channel or sslca mode.

Note: The following stipulations apply to configuring the Check Point OPSEC NG Connector:

- This procedure is supported only for ArcSight connector release 4.6.2 or later.
- A hostname is called an Application Object Name on Check Point. A password is a

Communication Activation Key on Check Point.

To configure a connector to operate in sslca mode:

On the Check Point SmartDashboard:

1. Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object.

Parameter	Description
Name	A meaningful name for the application object you are creating; for example, ArcSightLea-1. This name is used to pull the OPSEC certificate.
Host	The hostname of the ArcSight Management Center system managing the connector.
Client Entities	Select LEA.
Secure Internal Communication	If a DN string is not present, initialize the communication by providing an activation key. The activation key is used when the certificate is pulled. This is the SIC Name. Click Communication > Initialize .

After the object is created, note down the following information, which you will need to provide when continuing configuration.

- *SIC Name*: DN string that you obtain after initializing communication as described below.
 - *SIC Entity Name*: Double-click the Check Point Gateway name in the SmartDashboard to view its general properties. The SIC Entity Name is the SIC string configured in the general properties window.
 - Check Point IP address or hostname.
2. Pull the Check Point certificate.

To do so, run the `Pull OPSEC Certificate` command on the container to which you will be adding the connector. For detailed information about running a command on a container, see ["Sending a Command to a Container" on page 107](#). You need to provide this information when running the command:

Parameter	Description
Server hostname or IP address	The name or IP address of the Check Point server.
Application object name	The OPSEC Application object name you specified in the previous step. This parameter is case sensitive.
Password	The activation key you entered when creating the OPSEC application object in the previous step.

If the certificate is pulled successfully, a message similar to this is displayed:

OPSEC SIC name (CN=ArcSightLea-1,0=cpfw1.5ad8cn) was retrieved and stored in /opt/arcsight/connectors/<container name>/current/user/agent/checkpoint/<name>. Certificate was created successfully and written to "/opt/arcsight/connectors/<container name>/current/user/agent/checkpoint/ArcSightLea-1.opsec.p12".

Note down the OPSEC SIC Name (CN=ArcSightLea-1,0=cpfw1.5ad8cn in the above example) and the file name (ArcSightLea-1.opsec.p12 in the above example).

Tip: If the certificate is not pulled successfully, check to ensure that the Application object name you specified is correct (including the case) and the container on which you are running the command is up and running.

3. Install Policy on the LEA client for the Check Point Gateway using the SmartDashboard.

On Connector Appliance:

1. Add a Check Point connector by following instructions described in ["Adding a Connector" on page 119](#). You need to provide the following information.

Parameters	Values to input
Type	Check Point FW-1/VPN-1 OPSEC NG
Connection Type	SSLCA
Connector Table Parameters	Server IP: The IP address of the Check Point server. Server Port: The port on the server that listens for SSLCA connections. Use the default value 18184. OPSEC SIC Name: The name you noted in "Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object." on the previous page . OPSEC SSLCA File: The name you noted after pulling the certificate in "Pull the Check Point certificate." on the previous page . OPSEC Entity SIC Name: The name you noted in "Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object." on the previous page .

2. An error similar to the following is displayed.

-1:[X] Unable to connect to the Lea Server[10.0.101.185] -1:1 connection test failed!

Select the **Ignore warnings** check box, and then click **Next**.

3. Continue to configure the rest of the connector as described under ["Adding a Connector" on page 119](#).

Adding the MS SQL Server JDBC Driver

When you install and configure database connectors that use Microsoft SQL Server as the database, a JDBC driver is required. This driver does not ship pre-installed; you need to install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1. From the Microsoft web site, download the MS SQL Server JDBC Driver to a computer that can access ArcSight Management Center.
2. Run the setup program to install the driver.
3. Follow the instructions in ["Uploading Files to a Repository" on page 225](#) to add the `sqljdbc.jar` file.

Tip: The name of the `jar` file may be different from that of some JDBC driver versions. Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database.

The new driver file is added to the repository, as shown in the following example.

After you have installed the JDBC driver, you need to upload the driver file to the containers that will contain the SQL Server database Connectors. Follow the instructions in ["Uploading Files to a Repository" on page 225](#).

After the driver file has been uploaded to a container, follow the instructions in ["Adding a Connector" on page 119](#) to add a connector that requires a JDBC driver.

Adding the MySQL JDBC Driver

When you install and configure database connectors that use MySQL as the database, a JDBC driver is required. This driver does not ship pre-installed. Install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1. From the Microsoft web site, download the MySQL JDBC Driver to a computer that can access ArcSight Management Center.
<http://dev.mysql.com/downloads/connector/j/5.0.html>
2. Extract the driver.
3. Follow the instructions in ["Uploading Files to a Repository" on page 225](#) to add the `mysql-connector-java-x.x.x-bin.jar` file. The new driver file is added to the repository.

After you have installed the JDBC driver, you need to upload the driver file to the containers that will contain the MySQL database Connectors. Follow the instructions in ["Uploading Files to a Repository" on page 225](#).

After the driver file has been uploaded to a container, follow the instructions in ["Adding a Connector" on page 119](#) to add a connector that requires a JDBC driver.

Chapter 7: Managing Configurations

The following topics are discussed here.

• Overview	148
• Configuration Management	149
• Managing Subscribers	155
• Pushing a Subscriber Configuration	157
• Checking Subscriber Compliance	159
• Comparing Configurations	160
• Configuration Management Best Practices	161
• Subscriber Configuration Types	162
• Initial Configuration Management	182
• Managing Logger Event Archives	186
• Managing Logger Peers	188
• Managing Event Broker	191
• Deployment Templates	194
• Managing Collectors	196

Overview

A *configuration* is a group of related appliance or software settings and their associated values, which applies to one or more node types. A configuration created for a node can be pushed to nodes of the same type managed by ArcSight Management Center, assuring uniformity across a group of nodes.

Configurations come in these kinds:

- A *subscriber* configuration is for the routine management of multiple managed ArcSight products. You can easily assign values to, propagate, and maintain the same settings across multiple nodes of the same type, including connectors, Collectors, Connector Appliances, Loggers, or other ArcMCs.
- An *initial* configuration is for the rapid, uniform setup of multiple ArcSight Loggers (only). Use an initial configuration to expedite the initial deployment of ArcSight Loggers to a production environment.

Configuration management tasks include:

- *Configuration Creation*: A configuration for a node type can be created (as well as edited or deleted) in ArcSight Management Center.
- *Configuration Import*: A configuration can be created directly on a managed node, exported, and then imported into ArcSight Management Center for sharing with nodes of the same type.

- *Configuration Push*: A configuration can be *pushed* from ArcMC to managed nodes. This copies the configuration from ArcMC and changes the settings on each destination node.
- *Subscriptions*: Managed nodes can be *subscribed* to a subscriber configuration, so they can receive a new or updated configuration pushed from ArcSight Management Center.
- *Compliance Checks*: Check whether the settings and their values on a managed node match the ones for a configuration type specified in ArcSight Management Center. If so, the node is said to be in *compliance* with the configuration.
- *Comparisons*: Compare two configurations of the same type quickly, with a field by field breakdown of each setting, its value, and any differences. You can compare the values of a configuration on a subscriber node to the values of the baseline or reference configuration on an ArcMC which manages it. You can also compare two configurations of the same type on a single ArcMC.

For example, a typical workflow for a subscriber configuration might work as follows: you can create a suitable DNS configuration for an appliance, specifying primary DNS server, secondary DNS server, and search domains for the appliance. (See "[Destination Configuration Types](#)" on page 168.) You can then push your DNS configuration to subscribing appliances, and so ensure that DNS settings for all subscribed nodes are configured identically with a single action.

If you later updated the configuration to use a new primary DNS server, you could push the new configuration to all subscribers, and all of them would be updated for the new DNS server with one action.

At any time, you could verify any managed node's compliance with the configuration to determine if its settings were assigned the desired values.

Configuration Management

To create or manage configurations, on the menu bar, click **Configuration Management**. To manage a specific configuration type, select the configuration type from the sub-menu.

For example, to access subscriber configurations for Loggers, click **Configuration Management > Subscriber Configurations > Logger Configurations**.

The Configurations Table

The **Configurations** table lists all currently available subscriber configurations in ArcSight Management Center. Each listed configuration, whether it was created in ArcSight Management Center or imported from an existing node, is considered the baseline copy of that configuration, for pushing to managed nodes. The table includes the following columns.

- **Name**: The name of the configuration.
- **Type**: The type of configuration.
- **Last Edited By**: The most recent user to edit the configuration.

- **Compliance:** An aggregation of the status of the individual subscribers to that configuration.
 - *Compliant* indicates that all subscribers are in compliance.
 - *Non-Compliant* indicates that at least one subscriber is out of compliance.
 - *Unknown* indicates that the compliance status for one or more subscribers cannot be determined (for example, because connectivity to one or more subscribers is not available).

Tip: You can check the individual compliance of each subscriber on the **Subscribers** tab.

Click any column header to sort the **Configurations** table by that column.

To view the details of any configuration, click its name in the list. The **Details** and **Subscribers** tabs will display additional information.

Tip: To select multiple items from any list, Shift+Click or Ctrl+Click while selecting.

The Details Tab

The **Details** tab shows the specifics of the configuration, including any configured attributes and their values.

Configuration Name

Each configuration has a unique name. A configuration may be up to 255 characters in length.

General

General details describe the basics of the configuration, as follows:

- **Configuration Type:** The type of the configuration. For details of configuration types, see ["Subscriber Configuration Types" on page 162](#).
- **Last Edited By:** The most recent user to edit the configuration.

Properties

A *property* is a group of one or more settings for the configuration. For example, for the NTP Server configuration, the property includes two settings: Enable as NTP Server (a Boolean value indicating whether to enable the product as an NTP server), and NTP Servers (a list of NTP servers).

The specific parameters included in each property are pre-defined for each configuration type. ArcSight Management Center prompts for values of each setting when the property is selected. Each parameter must be assigned a valid value corresponding to its data type. For instance, if the data type is integer, you must specify an integer value. A red asterisk (*) indicates a required parameter.

List Configurations

A configuration type that can include more than one property is known as a *list configuration*. A list configuration represents a configuration with multiple instances of data values of the same kind. Each instance is known as a *property*.

For example, the Connector Map File configuration could include information on multiple map files. Each Property would represent a different map file (with different values for file path and content).

Note: A pushed list configuration will override any existing configuration of the same type on the managed node. To *append* data to an existing configuration, use the bulk management tools (**Set Configuration**)

For a description of supported configuration types, the parameters associated with each type, and their data types, see ["The Configurations Table" on page 149](#).

The Subscribers Tab

The **Subscribers** list shows all managed nodes currently eligible to receive the configuration. (The list is empty if no hosts have been added yet.)

The tab includes these operations buttons:

Add Subscribers	Adds subscribers to the existing configuration.
Push	Pushes the configuration to one or more selected subscribers.
Check Compliance	Checks the compliance of all subscribers with the baseline configuration.
Unsubscribe	Removes one or more selected subscribers from the subscriber list.

The list includes the following columns:

- **Path:** The path of the subscribing node, consisting of location/hostname/node type.
- **Type:** The type of subscribing node.
- **Last Pushed At:** The time and date of the most recent push to the subscriber.
- **Last Push Status:** The status of the most recent push to the subscriber.
 - *Succeeded:* the configuration push was successful.
 - *Failed:* hover over the link to determine the reason for the push failure. An error message is displayed to help in remediation of the issue. For more information, see ["Push Remediation" on page 159](#).
 - *Unknown:* Initial status before the subscriber has received any pushes.
- **Last Compliance Check:** The date and time of the most recent compliance check.
- **Compliance:** Whether the node is in compliance with the configuration.
 - *Compliant* indicates the node is in compliance. The values for *all* settings associated with the configuration type match the values from the configuration.
 - *Non-Compliant* indicates the node is out of compliance. One or more values for the settings

associated with the configuration type do not match the values from the configuration. Hover over *No* to show the cause of the node's non-compliance.

- *Unknown* indicates either that the node's compliance could not be determined at the time of the most recent compliance check, or that the node has not yet undergone a compliance check.

Non-Compliance Reports

You can determine why a compliance status is Non-Compliant.

For a compliance status of *Non-Compliant*, click the status to display the **Configuration Comparison** dialog, which compares all setting values for the configuration on ArcMC and on the managed node.

Click **Push Configuration** to push the configuration to the managed node in order to make it Compliant.

Creating a Subscriber Configuration

You can create a subscriber configuration for pushing to any subscribed nodes.

Note: The following subscriber configuration types cannot be created in ArcSight Management Center, but can only be imported from managed nodes:

- Logger Storage Group
- Logger Filter
- Logger ESM Forwarder, Connector Forwarder, TCP Forwarder, UDP Forwarder
- Authentication External

For more information on importing a configuration from a managed node, see ["Importing a Subscriber Configuration" on page 154](#).

To create a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. Under **Configurations**, click **New**.
3. On the **Details** tab, select a configuration type from the **Configuration Type** drop-down list. (Only the appropriate configuration types are shown in the drop-down list.)
4. In **Configuration Name**, enter a name for the configuration. (Configuration names must be unique and may be up to 255 characters in length.)
5. Enter values for any required parameters, which are indicated with a red asterisk (*).

Note: For a description of valid parameters for each configuration type, and the data type associated with each, see "[Subscriber Configuration Types](#)" on page 162.

6. Optionally, add values for any optional parameters.
7. Optionally, to add an additional property for a list configuration: click **Add Property**, and then enter values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
8. Click **Save**.

Editing a Subscriber Configuration

You can modify or delete values for a subscriber configuration. (You may not edit a configuration currently being pushed.)

To edit a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration to be edited.
3. On the **Details** tab, click **Edit**.
 - Edit the general settings as needed.
 - Optionally, to add an additional property for a list property, click **Add Property**, and then enter values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
 - Optionally, to delete a property from the configuration, click **Delete Property**.
4. When complete, click **Save**. After saving, if the configuration has any subscribers, you are prompted to push the updated configuration to the subscribers.

Deleting a Subscriber Configuration

A deleted subscriber configuration is no longer available for pushes to subscribers. You may not delete a configuration currently being pushed.

To delete a subscriber configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select one or more configurations to be deleted.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Importing a Subscriber Configuration

A subscriber configuration created on a managed node may be imported into ArcSight Management Center, for editing and pushing to other nodes of the same type.

For example, you can define a configuration on a managed Connector Appliance, and then import the configuration into ArcSight Management Center. The imported configuration may then be edited and pushed to other managed Connector Appliances, just the same as you would with a configuration you originally created in ArcSight Management Center.

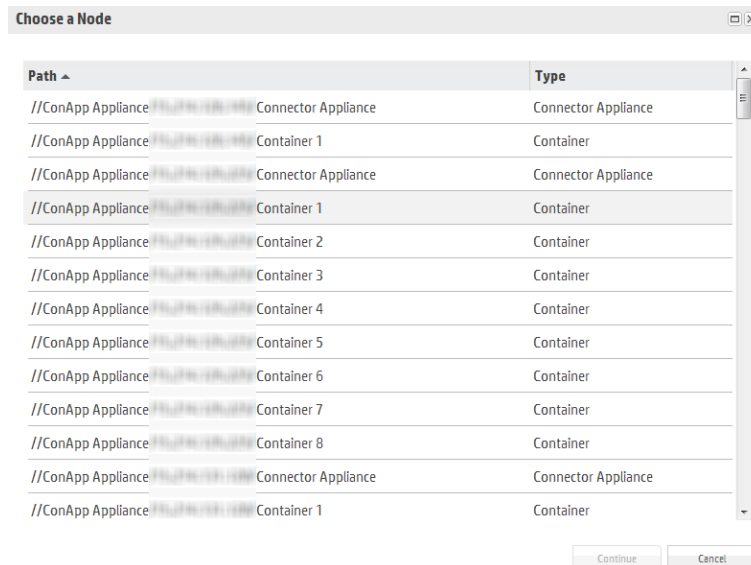
If configuration import to the localhost fails, restart the web service on the localhost.

To import a subscriber configuration from a managed node:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. Under **Configurations**, click **Import**.
3. On the **Choose a Node** dialog, select the node from which you wish to import the configuration.



4. Click **Continue**.
5. On the **Import Configuration** dialog:
 - a. Select a configuration type for the imported configuration from the **Type** drop-down list. (The entries in the list depend on the configuration types which apply to the node chosen in Step 3.)
 - b. In **Name**, enter a name for the imported configuration.
6. Click **Import**. The configuration is imported into ArcSight Management Center and is shown in the **Configurations** table.

Note: In order to import a backup configuration from a Connector Appliance, Logger, or ArcMC node, the node must have a scheduled backup to begin with.

Managing Subscribers

A *subscriber* is a managed node to which a configuration may be pushed. A subscriber to which a configuration is pushed will receive and process the pushed configuration and apply it to the managed node, so that the managed node's settings are the same as the settings specified in the configuration.

Each node can subscribe to *only one* configuration of each configuration type.

For example, a Logger appliance could subscribe to one Logger Storage Group configuration, but the same appliance could also subscribe to a Logger Filter configuration as well as a Logger Transport Receiver configuration.

Viewing Subscribers

To view subscribers for a configuration:

1. Click **Configuration Management > All Configurations**.
2. From the list of configurations, locate the configuration for which you wish to view subscribers.
3. Click the name of the configuration.
4. Click the **Subscribers** tab. The current subscribers are displayed.

Adding a Subscriber

A subscriber (that is, a subscribed node) can receive a pushed configuration.

To subscribe a node to a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration to which you wish to add subscribers.
3. Click the **Subscribers** tab.
4. Click **Add Subscribers**.
5. On the **Add Subscribers** dialog, select a node to add as a subscriber. The list of potential subscribers is determined by the selected configuration type. To select multiple nodes for subscription, Ctrl+Click each node.

Note: A node may only subscribe to one configuration of each type; for example, one DNS configuration.

If you attempt to add a subscriber which is already subscribed to a configuration of the same type, the following message is displayed: *No available subscribers have been found for the selected configuration.*

6. Click **Add Subscribers**.
7. Click **OK** to confirm completion. The subscriber is added to the recipients for the configuration.

Unsubscribing a Subscriber

After being unsubscribed, a node can no longer receive a pushed configuration.

To remove a subscriber from a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration from which you wish to remove subscribers.
3. Click the **Subscribers** tab.
4. Select one or more subscriber from the list of subscribers.
5. Click **Unsubscribe**.
6. Click **OK** to confirm. The selected subscribers are unsubscribed.

Pushing a Subscriber Configuration

A pushed subscriber configuration synchronizes the configuration from ArcSight Management Center to all or a selection of the configuration's subscribers. Pushing must be performed manually.

When selecting subscribers, only valid potential subscribers for the configuration are shown. For example, if pushing a Logger configuration, which only applies to Loggers, only managed Loggers would be shown as potential subscribers, not Connector Appliances or ArcMCs.

If a configuration push to the localhost fails, restart the web service on the localhost.

To push a subscriber configuration to all subscribers:

1. Select **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.
4. Click **Yes** to confirm the push. The configuration is pushed to all subscribers of the selected configuration. A compliance check is automatically performed on each subscriber.

To push a subscriber configuration to selected subscribers:

1. Select **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed, and click the name of the configuration.
3. On the **Configuration Details and Subscribers** page, click the **Subscribers** tab.
4. On the **Subscribers** tab, select one or more subscribers to which to push the configuration.
5. Click **Push**.
6. Click **Yes** to confirm the push. The configuration is pushed to the selected subscribers. A compliance check is automatically performed on each recipient.

Push Validation

During a push to subscribers, the configuration is automatically validated by ArcSight Management Center. Validation ensures that a pushed configuration contains appropriate, meaningful values for all settings. If any configuration values are found to be invalid, the push will fail, and an error message will be returned. Hover over the subscriber's entry on the **Subscribers** tab, in the **Push Status** column, to show the cause of the failed push. In addition, a compliance check is automatically performed after the push.

Common Causes for Push Failure

A push to a subscriber may fail for any number of reasons. These may include:

- **Validation Failure:** A push with invalid content will fail. Verify that your configuration includes valid setting values for the configuration type.
- **Lack of Connectivity:** Network or system issues can cause disrupt connectivity to a subscriber. Verify connectivity with the subscriber.
- **Agent Not Running on Host :** Verify that the ArcMC Agent process is active on the subscribing node. (This does not apply to connectors or Collectors, which do not require the Agent.)
- **Privileges on Subscribing Host:** In order to push a subscription, the ArcSight Management Center user (specified by the user credentials) must have privileges to view, edit, or delete configuration settings on the subscriber nodes.
- **Expired License:** An expired host license will cause a push to the host to fail.

Push Remediation

If a push to a subscriber fails, you may be able to remedy the failure. To remedy a failed push, do the following:

1. Select the configuration from the **Configurations** table.
2. Click the **Subscribers** tab and choose the subscriber to which the push failed.
3. The **Last Push Status** will show *Failed*. Hover over this link to view the error message associated with the push failure.

After viewing the error message, you can take the appropriate steps on the managed node to address the issue. Resolution may require direct or remote access to the node outside of ArcSight Management Center.

After the issue is resolved, you can retry the failed configuration push.

Checking Subscriber Compliance

A subscribed node is in *compliance* with a configuration if the settings for the node match those assigned to the configuration in ArcSight Management Center.

The configuration listed in the managing ArcSight Management Center is considered the baseline copy of the configuration.

For example, you create an SMTP configuration in ArcSight Management Center named *Sample SMTP Configuration*, with these values assigned:

- Primary SMTP Server: *Mailserver1*
- Secondary SMTP Server: *Mailserver2*
- Outgoing Email Address: *admin@example.com*

A node would be in compliance with this configuration if the values for its primary and secondary SMTP servers, and outgoing email address, matched the values in *Sample SMTP Configuration*.

If any one of these values were different (for example, if a node had a primary SMTP Server of *CorporateMail1*) the node would be out of compliance.

You can manually check the compliance of all subscribers to a configuration.

To manually check subscriber compliance for a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.

Tip: To filter for a specific subscriber configuration type, select the desired configuration type

from the **Subscriber Configurations** sub-menu.

2. In the **Configurations** table, select the configuration to be checked for compliance.
3. Click **Check Compliance**. All subscribers to the selected configuration are checked for compliance.
 - On the **Configurations** table, the **Compliance** column shows the aggregated compliance of all subscribers.
 - On the **Subscribers** tab for the configuration:
 - The **Last Compliance Check** column is updated to show the most recent check.

Automatic compliance checks will run every 12 hours. So this will be the date and time of the latest automatic check.

- The **Compliance** column indicates the individual compliance of each node.

Comparing Configurations

You can compare two configurations of the same type to verify whether they contain the same settings. The following two comparisons are possible:


- **Comparing two configurations on a single ArcMC.** You can compare two configurations of the same type on a single ArcMC. For example, you could compare the settings for two different SMTP configurations.
- **Comparing the configuration on a subscriber to the same configuration on its managing ArcMC.** You can quickly check to see how the settings for a configuration on a subscribing node differs from the same configuration on its managing ArcMC.

To compare two configurations of the same type on one ArcMC:

1. Click **Configuration Management**.
2. Select **All Configurations**.
3. In the list of configurations, select two configurations.
4. Click **Compare**.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item in the **Status** column.

To print the comparison as a PDF report, click **Export to PDF**.

Configuration Comparison			
			 Export to PDF
Configuration Field	Authentication2	auth session	Status
Max Simultaneous Logins/User	15	15	✓ Matches
Logout Inactive Sessions After (seconds)	1000	900	✗ Does Not Match
Disable Inactive Account After (days)	3	0	✗ Does Not Match

To compare the configuration on a subscriber to the same configuration on its managing ArcMC:

1. Click **Configuration Management**.
2. Select **All Configurations**.
3. In the configurations list, select the configuration you wish to compare between ArcMC and the subscriber.
4. Under **Configuration Details & Subscribers**, click the **Subscribers** tab.
5. In the **Compliance** column, click the status link.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item.

Optionally, if the subscriber is Non-compliant with the configuration on its managing ArcMC, click **Push Configuration** to push the configuration to the subscriber (which will make it compliant).

To export the comparison as a PDF report, click **Export to PDF**.

Configuration Management Best Practices

Configuration management is a powerful tool for managing ArcSight products in bulk. You can easily implement configurations across multiple appliances with just a few actions.

- **Node management versus Configuration Management:** Use ArcSight Management Center's node management tools for the administration of individual nodes and their day-to-day operations. However, for consistent and wide-ranging changes to the data or settings of managed nodes, use configuration management if the appropriate configuration exists. For example, to change DNS settings across multiple managed nodes, it would be faster and easier to create the configuration in ArcMC and push it out to managed nodes, than to individually change the settings across multiple devices.
- **Implementing data settings across multiple appliances or products in bulk:** Use the Bulk Management (**Set Configuration**) tools to implement data settings across multiple appliances or products. For example, you can quickly configure all of your appliances to use the same hardware settings (such as SMTP server) with a single platform (in this case, SMTP) configuration applied to managed nodes. (Pushing will overwrite any existing data.)

- **Compliance versus Non-Compliance:** If configuration compliance is not relevant to your configuration management, use the bulk management tools under Node Management to manage your node settings. A bulk push can also be performed under Configuration Management.

Subscriber Configuration Types

The following section lists the available subscriber configuration types, the parameters associated with each, their data types, and a brief description of what the parameter represents. When assigning values to parameters:

- Each parameter's value must be of the data type indicated (for example, the String data type indicates that you must enter a string for the value).
- *Required* parameters are marked with an asterisk (*) and must be assigned a value. A configuration missing a value for a required parameter cannot be saved or pushed.
- *Read-only* parameters cannot be edited in ArcSight Management Center.
- For security reasons, all password parameters are displayed with obfuscation.

Tip: For details of each entry field, in edit mode, hover over the field label and view its descriptive tooltip.

Connector Configuration Types

Connector configurations set values for settings on containers, connectors, or Collectors. The available connector configuration types are listed here.

BlueCoat Connector Configuration

A BlueCoat Connector configuration defines settings for one or more BlueCoat connectors. The configuration is only pushed to a target if a BlueCoat connector exists.

To push a BlueCoat Connector configuration from ArcMC to a managed node that already has values defined for all fields listed here, then specify values for all fields in the pushed configuration. Default values may be used if necessary.

BlueCoat Connector Configuration Parameters

Parameter	Data Type	Description
Row Number*	Integer	Row number of the table parameter to which the configuration is pushed.
Log File Wildcard*	String	Log file wildcard.

BlueCoat Connector Configuration Parameters, continued

Parameter	Data Type	Description
Log File Type*	String	Log file type. Valid values are: <ul style="list-style-type: none">• main• im• ssl• streaming
Processing Mode	String	Processing mode. Valid values are Batch and Real time.
Post-Processing Mode	String	Post-processing mode. Valid values are: <ul style="list-style-type: none">• RenameFileInTheSame Directory• PersistFile• DeleteFile
Mode Options	String	Mode options. Required if Post-Processing Mode is chosen as RenameFileInTheSame Directory
Processing Threshold	Integer	Interval, in hours, after which the log file will be marked as processed.
Processing Limit	Integer	Number of files that can be read in the directory at the same time.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a container.

After pushing a FIPS configuration, the destination container will be restarted.

FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If Yes , FIPS is enabled on the container.

Map File Configuration

A map file configuration defines the path and content of one or more container map files. Each Path/Content pair represents a single map file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all *.properties files in the \map directory on the target, then adds the list of map files to the target, replacing any existing map files.
- If the configuration contains an empty list, all *.properties files are deleted.

If importing and uploading a map configuration file, convert the downloaded CSV file into a .properties file before uploading.

Map File Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the map file.
Content*	String	Content of the map file.

Parser Override Configuration

A parser override configuration defines the path and content of one or more container parser override files.

Each Path/Content pair represents a single parser override file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all *.properties files in the \fcp directory on the target, then adds the list of parser override files to the target, replacing any existing parser override files.
- If the configuration contains an empty list, all *.properties files are deleted.

Parser Override Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the parser override file.
Content*	String	Content of the parser file.

Syslog Connector Configuration

A Syslog connector configuration defines values for one or more Syslog connectors. The configuration is only pushed to the target node if a Syslog connector exists.

Syslog Connector Configuration Parameters

Parameter	Data Type	Description
Port*	Integer	Syslog connector port.
Protocol*	Enum	Protocol of the syslog connector (either UDP or Raw TCP).

Windows Unified Connector (WUC) External Parameters Configuration

A WUC External Parameters connector configuration defines the external parameters for one or more WUC connectors. The configuration is only pushed to the target node if a WUC connector exists.

Limitations to WUC External Parameters Configurations

A WUC external parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary.

WUC External Parameters Configuration Parameters

Parameter	Data Type	Description
Domain Name*	String	Windows domain name.
Domain User*	String	Windows domain user name.
Active Directory Host	String	Hostname for the Active Directory server, if one is used. <ul style="list-style-type: none">◦ If specified, values for User, User Password, Base DN, Protocol, and Port must be specified in subsequent entries.
Active Directory Use	String	Username for the AD server. <ul style="list-style-type: none">◦ Required if a value is provided for Active Directory Host.
Active Directory User Password	String	Password for AD server. <ul style="list-style-type: none">◦ Required if a value is provided for Active Directory Host.
Active Directory Base DN	String	Base DN of the Active Directory. <ul style="list-style-type: none">◦ Required if a value is provided for Active Directory Host.
Active Directory Protocol	String	Protocol for Active Directory. <ul style="list-style-type: none">◦ Required if a value is provided for Active Directory Host.
Active Directory Port	String	Port for Active Directory. <ul style="list-style-type: none">◦ Required if a value is provided for Active Directory Host.
Global Catalog Server	String	Hostname for the Global Catalog server, if one is used. <ul style="list-style-type: none">◦ If specified, values for User Name, User Password, and Base DN must be specified in subsequent entries.
Global Catalog User Name	String	Username for the GC server. <ul style="list-style-type: none">◦ Required if a value is provided for Global Catalog server.

WUC External Parameters Configuration Parameters, continued

Parameter	Data Type	Description
Global Catalog User Password	String	Password for the GC server. <ul style="list-style-type: none">Required if a value is provided for Global Catalog server.
Global Catalog Base DN	String	Base DN of the GC server. <ul style="list-style-type: none">Required if a value is provided for Global Catalog server.
WEF Collection*	String	Indicates if Windows Event Format collection is enabled. Valid values are: <ul style="list-style-type: none">DisabledEnabled (use Active Directory for sources)Enabled (do not use Active Directory for sources) Note: WEF collection is only supported for Connector versions 6.0.6 or later. Otherwise, compliance checks for checks for WUC External Parameters configurations will always fail.

Windows Unified Connector (WUC) Internal Parameters Configuration

A WUC Internal Parameters connector configuration defines the internal parameters for one or more WUC connectors. The configuration is only pushed to the target if a WUC connector exists.

Limitations to WUC Internal Parameters Configurations

A WUC internal parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary

WUC Internal Parameters Configuration Parameters

Parameter	Data Type	Description
Enable GUID Translation*	Boolean	If true, Globally Unique Identifier translation is enabled.
Enable SID Translation*	Boolean	If true, Security Identifier translation is enabled.
Enable SID Translation Always*	Boolean	If true, SID translation is used even for events Windows does not translate.
FCP Version	Integer	File Control Protocol version number.
Global Catalog Port	Integer	Port used by Global Catalog server.

WUC Internal Parameters Configuration Parameters, continued

Parameter	Data Type	Description
Global Catalog Security Protocol	Enum	Security protocol used by Global Catalog server.
Host Browsing Threads Sleep Time	Integer	Time in milliseconds between host browsing queries.
Inactivity Sleep Time	Integer	Time in milliseconds to sleep if no events are retrieved from the configured hosts
Log Rotation Check Interval	Integer	Time in milliseconds to wait before checking for log rotation.
Reconnect Interval	Integer	Time in milliseconds after which the connection to a previously down host is to be retried.
Rotation Retry Count	Integer	Number of times to check that log has been rotated.
Rotation Retry Interval	Integer	Interval in milliseconds for rotation retry.
Sleep Time	Integer	Time, in milliseconds, to sleep before collecting more events from hosts (-1 means disable sleep time).
Thread Count	Integer	Number of threads to use for the connector.

ArcMC/Connector Appliance Configuration Types

ArcMC/Connector Appliance configurations set values for settings on Software ArcSight Management Centers, ArcSight Management Center Appliances, and hardware or software Connector Appliances. The currently available ArcMC/Connector Appliance configuration type is listed here.

ArcMC/Connector Appliance Configuration Backup Configuration

An ArcMC/Connector Appliance Configuration Backup configuration sets values for scheduled configuration backups of ArcSight Management Center or Connector Appliance. Backup content includes all backup data.

After a push, the web process is automatically restarted on the subscriber.

For this configuration type, no automatic compliance checks will be performed. [You must check compliance manually.](#)

Note: You can neither create nor import settings related to a one-time configuration backup.

ArcMC/Connector Appliance Configuration Backup Parameters

Parameters	Data Type	Description
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Port*	Integer	Port of the remote system. Default value is 22.
Base Remote Directory*	String	Destination directory on the remote system. Must be manually created on remote system prior to push. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
User*	String	User name on destination.
Password*	String	Password on the destination. (Obfuscated.)
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are <i>Su, M, T, W, Th, F, Sa</i> .
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00 midnight. For example, a value of 14 would correspond to 2 PM.

Destination Configuration Types

A destination configuration sets values for ESM destination settings on connectors/Collectors. The available destination configuration types are listed here.

Destination Configuration Parameters

A Destination Configuration Parameters configuration defines values and behavior for destination configuration parameters.

Note: Destination Configuration Parameters configurations can only be imported from managed connectors/Collectors, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

For a description of the parameters for this configuration type, see ["Destination Runtime Parameters " on page 299](#).

Networks and Zones

A Networks and Zones configuration defines values and behavior for ArcSight ESM networks and zones. For more information on ESM networks and zones, consult the ArcSight Console documentation.

Networks and Zones Configuration Parameters

Parameter	Data Type	Description
Configuration Name*	String	Name of the configuration.
Networks CSV Content*	CSV	<p>Comma-separated Value (CSV) file. Click Upload to upload a valid CSV file, or click Download to download an existing file.</p> <p>Creating a CSV File</p> <p>The CSV must include the literal header line:</p> <p>#Type,Name,Parent Group URI,Customer URI</p> <p>Then, each line describes a Network. Each line must comprise values for the following fields, and end with a hard return.</p> <p><Type>,<Name>,<Parent Group URI>,<Customer URI></p>
Zones CSV Content*	CSV	<p>Comma-separated Value (CSV) file. Click Upload to upload a valid CSV file, or click Download to download an existing file.</p> <p>Creating a CSV File</p> <p>The CSV must include the literal header line:</p> <p>Name,Start Address,End Address,Parent Group URI,Network URI</p> <p>Then, each line describes a Zone. Each line must comprise values for the following fields, and end with a hard return.</p> <p><Name>,<Start Address>,<End Address>,<Parent Group URI>,<Network URI></p>

Logger Configuration Types

Logger configurations set values for settings on hardware and software Loggers. The available Logger configuration types are listed here.

Logger Configuration Backup Configuration

A Logger configuration backup configuration sets values for scheduled configuration backups of hardware and software Logger to a remote system.

Note: You can neither create nor import settings related to a one-time configuration backup.

Logger Configuration Backup Configuration Parameters

Parameter	Data Type	Description
SCP Port*	String	Port of the remote system. Default value is 22.
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Username*	String	User name on destination.
Password*	String	Password on destination. (Obfuscated.)
Base Remote Directory*	String	Destination directory on the remote system. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are <i>Su, M, T, W, Th, F, Sa</i> .
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00. For example, a value of 14 would correspond to 2 PM.
Backup Content*	String	Type of content to be included in the backup. Valid values are: <ul style="list-style-type: none">• <i>All</i>: includes all backup data.• <i>Report_Content_Only</i>: includes only report data.

Logger Connector Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more connector forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.

Note: Logger Connector Forwarder configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger Connector Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If Yes , the forwarder is enabled.
Connection Retry Timeout*	Integer	Time, in seconds, to wait before retrying a connection.
Source Type*	Integer	Source Type. Valid values: <ul style="list-style-type: none">• Apache HTTP Server Access• Apache HTTP Server Error• IBM DB2 Audit• Juniper Steel-Belted Radius• Microsoft DHCP Log• Other

Logger ESM Forwarder Configuration

A Logger ESM Forwarder configuration sets values for one or more ESM destinations on a Logger (version 6.1 or later). Each destination in the configuration is represented by a different Property.

Note: Logger ESM Forwarder configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger ESM Forwarder Parameters

Parameter	Data Type	Description
Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Start of time range for selection.
End Time	DateTime	End of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receiveforwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable	Boolean	If Yes , the forwarder is enabled.

Logger Filter Configuration

A Logger Filter configuration sets values for one or more saved searches on a Logger.

Each filter in the configuration is represented by a different Property.

Note: Logger Filter configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger Filter Configuration Parameters

Parameter	Data Type	Description
Filter Name*	String (Read-only)	Name of the filter.
Filter Category	String	Category of filter. Valid values are <i>Shared</i> , <i>System</i> and <i>SearchGroup</i> .

Logger Filter Configuration Parameters, continued

Parameter	Data Type	Description
Filter Type*	String	Type of filter. Valid values are <i>RegexQuery</i> or <i>UnifiedQuery</i> .
Query*	String	Query string.
Permission Group	String	Permission group which with the Logger filter is associated. When the configuration is pushed: <ul style="list-style-type: none">• If the permission group is not present on the target Logger, the permission group will be created during the push.• If the permission group of the same name is already present on the target, but has different rights, the rights of the permission group on the target Logger will not be overwritten, and the association between the filter and the permission group will be removed.

Logger SmartMessage Receiver Configuration

A Logger SmartMessage Receiver sets values for one or more for SmartMessage Receivers.

A SmartMessage Receiver configuration pushed to a target overwrites any existing SmartMessage receivers on the target; other types of receivers such as UDP and TCP are not affected.

Logger SmartMessage Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Enabled*	Boolean	If Yes , SmartMessage reception is enabled.
Encoding*	String	Encoding type. Valid values are: <ul style="list-style-type: none">• UTF-8• US-ASCII

Logger Storage Group Configuration

A Logger Storage Group configuration sets values for one or more Logger storage groups.

Note: Logger Storage Group configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger Storage Group Configuration Parameters

Parameter	Data Type	Description
Storage Group Name*	String (Read-only)	Name of the storage group. <ul style="list-style-type: none">The pushed configuration must contain the same number of storage groups as configured on the Logger.The names of the storage groups in the pushed configuration must match the names of storage groups on the Logger.
Maximum Age (Days)*	Integer	Maximum age of events in storage, in days.
Maximum Size (GB)*	Integer	Maximum size of the storage group, in gigabytes. <ul style="list-style-type: none">The cumulative size of all storage groups must not be greater than the storage volume size on the Logger.

Logger TCP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more TCP forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.

Note: Logger TCP Forwarder configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger TCP Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.

Logger TCP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Enable*	Boolean	If Yes , the forwarder is enabled.
Preserve System Timestamp*	Boolean	If Yes , the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If Yes , event is sent as is, without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.
Connection Retry Timeout*	Integer	The time, in seconds, to wait before retrying a connection.

Logger Transport Receiver Configuration

A Logger Transport Receiver configuration sets values for one or more UDP, TCP, CEF UDP, or CEF TCP receivers.

Note: In Logger documentation, a *Transport Receiver* is referred to as simply a *Receiver*.

A pushed Transport Receiver type configuration will overwrite any existing UDP, TCP, CEF UDP, or CEF TCP receiver. Any other type of receivers, such as SmartMessage receivers, are not affected.

Logger Transport Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Receiver Type*	String	Receiver type. Valid values are: <ul style="list-style-type: none">• UDP• TCP• CEF UDP• CEF TCP
Receiver Name*	String	Name of the receiver.

Logger Transport Receiver Configuration Parameters, continued

Parameter	Data Type	Description
Port*	Integer	Port number. Must be a non-zero positive number. Ensure this port is open on the destination.
Enabled*	Boolean	If Yes , transport reception is enabled.
Encoding*	String	Encoding type. Valid values are: <ul style="list-style-type: none">• UTF-8• Shift_JIS• EUC-JP• EUC-KR• US-ASCII• GB2312• UTF-16BE• Big5• GB18030• ISO-8859-1• Windows-1252 For CEF UDP and CEF TCP receivers, only UTF-8 and US-ASCII apply. Caution: Selection of the wrong encoding for a CEF receiver will cause a push failure.

Logger UDP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or UDP forwarders on a Logger. Each forwarder in the configuration is represented by a different Property.

Note: Logger UDP Forwarder configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Logger UDP Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.

Logger UDP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If Yes , the forwarder is enabled.
Preserve System Timestamp*	Boolean	If Yes , the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If Yes , event is sent as is, without without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.

System Admin Configuration Types

System Admin configurations set values for system administrative settings. The available System Admin configuration types are listed here.

Authentication External

An Authentication External configuration defines values and behavior for a hardware or software system requiring authentication to an external server, such as LDAP or RADIUS.

After changing the Authentication Method on a host, you must delete the host from ArcSight Management Center, and then re-add it using Node Management.

Note: Authentication External configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See ["Importing a Subscriber Configuration" on page 154](#) for more information.

Authentication External Configuration Parameters

Parameter	Data Type	Description
Authentication Method*	String	System authentication method.
Allow Local Password Fallback for Default Admin Only*	Boolean	If Yes , the authentication server will fall back to local passwords for authentication for administrators.
Allow Local Password Fallback for All Users*	Boolean	If Yes , the authentication server will fall back to local passwords for authentication for all users.
LDAP Server Hostname[port]*	String	LDAP server hostname and port.
LDAP Backup Server Hostname [port]	String	LDAP backup server hostname and port.
LDAP Server Request Timeout (seconds)	Integer	LDAP server request timeout, in seconds.
RADIUS Server Hostname[port]	String	RADIUS server hostname and port.
RADIUS Backup Server Hostname [port]	String	RADIUS backup server hostname and port
RADIUS Shared Authentication Secret	String	RADIUS authentication shared secret.
RADIUS Server NAS IP Address	String	RADIUS server Network Access Server IP address .
RADIUS Request Timeout (seconds)	Integer	RADIUS server request timeout, in seconds.
RADIUS Retry Request	Integer	Number of times to retry RADIUS server requests.
RADIUS Protocol	String	Type of RADIUS protocol.

Authentication Local Password

An Authentication Local Password configuration defines a hardware or software system's local password options and behavior.

Authentication Local Password Configuration Parameters

Parameter	Data Type	Description
Enable Account Lockout*	Boolean	If Yes , account lockouts are enabled after an incorrect password entry.
Lock Out Account after N Failed Attempts*	Integer	Number of failed attempts before lockout.
Remember Failed Attempts For (seconds)*	Integer	Time, in seconds, between failed attempts that will trigger a lockout.
Lockout Account for (minutes)*	Integer	Time, in minutes, that the account will be locked out.
Enable Password Expiration*	Boolean	If Yes , password expiration is enabled

Authentication Local Password Configuration Parameters, continued

Parameter	Data Type	Description
Password Expires in (days)*	Integer	Interval, in days, after which a password expires.
Notify User (Days Before Expiration)*	Integer	Days before password expiration that the user is notified.
Users Exempted from Password Expiration Policy	List of comma-separated strings	Comma-separated list of users whose passwords will never expire.
Enforce Password Strength*	Boolean	If Yes , password strength is enforced.
Minimum Length (characters)*	Integer	Minimum number of password characters.
Maximum Length (characters)*	Integer	Maximum number of password characters.
Numeric [0-9]*	Integer	Minimum number of numeric password characters.
Upper Case [A-Z]*	Integer	Minimum number of uppercase password characters.
Lower Case [a-z]*	Integer	Minimum number of lowercase password characters.
Special [!\$^*...]*	Integer	Minimum number of special password characters.
Password Must Be At Least*	Integer	Minimum number of characters a new password must differ from the user's previous password.
Include "Forgot Password" link on Login Screen*	Boolean	If Yes , a link is provided where the user can recover a password.

Authentication Session

An Authentication Session configuration defines values for a hardware or software system's authentication sessions.

Authentication Session Configuration Parameters

Parameter	Data Type	Description
Max Simultaneous Logins Per User*	Integer	Maximum number of simultaneous logins per user.
Logout Inactive Session After (seconds)*	Integer	Inactivity session timeout, in seconds.
Disable Inactive Account After (days)*	Integer	Number of days of inactivity after which an account will be disabled.

DNS Configuration

A DNS Configuration defines values for a hardware appliance's Domain Name Service.

DNS Configuration Parameters

Parameter	Data Type	Description
Primary DNS*	String	Primary DNS server.
Secondary DNS	String	Secondary DNS server.
DNS Search Domains	List of comma-separated strings	Comma-separated list of DNS search domains.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a managed node.

After pushing a FIPS configuration, the destination node will be restarted.

FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If Yes , FIPS is enabled on the node.

Network Configuration

A Network Configuration defines values for a hardware appliance's default gateway setting.

Note: Values for these network settings cannot be changed through ArcSight Management Center: hostname, IP addresses for the network interfaces, static routes, /etc/hosts file, and time settings.

Network Configuration Parameters

Parameter	Data Type	Description
Default Gateway*	String	Default network gateway.

NTP Configuration

An NTP Configuration defines values for a hardware appliance's Network Time Protocol.

NTP Configuration Parameters

Parameter	Data Type	Description
Enable as NTP Server*	Boolean	If Yes , the system is enabled as an NTP server.
NTP Servers*	List of comma-separated strings	Comma-separated list of NTP servers. Required even if Enable as NTP Server is false.

SMTP Configuration

An SMTP Configuration defines values for a hardware or software system's Simple Mail Transfer Protocol.

SMTP Configuration Parameters

Parameter	Data Type	Description
Primary SMTP Server*	String	Primary SMTP server.
Secondary SMTP Server	String	Secondary SMTP server.
Outgoing Email Address*	String	Outgoing email address.

SNMP Poll Configuration

An SNMP Poll Configuration defines values for a hardware appliance's Simple Network Management Protocol monitoring. ArcMC supports V2c and V3 of SNMP.

SNMP Poll Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If Yes , SNMP polling is enabled.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported. Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.
System Name	String	Name of the SNMP system.
Point of Contact	String	Point of contact.
Location	String	System location.

SNMP Trap Configuration

An SNMP Trap Configuration defines values for a hardware appliance's Simple Network Management Protocol notifications. ArcMC supports V2c and V3 of SNMP.

In previous versions of ArcMC, an SNMP Trap configuration was known as an SNMP Configuration.

SNMP Trap Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If Yes , SNMP polling is enabled.
NMS IP Address	String	IP address of network management server.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported. Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.

Initial Configuration Management

An *initial configuration* is intended for the rapid, uniform setup of multiple ArcSight Loggers of the same model number and software version. Use an initial configuration to expedite the initial deployment of Loggers to a production environment. Initial configuration management is supported on Logger version 6.1 or later.

An initial configuration is not created in ArcMC. Instead, a suitable initial configuration is created on a managed Logger and imported into ArcMC. The configuration may then be pushed to other managed Loggers of the same model and software version number.

The following attributes are shown for each initial configuration:

Attribute	Description
Imported Init-Config Name	Name of the imported initial configuration.
Product Type	Type of Logger to which the configuration may be pushed: either Logger (appliance) or SWLogger (software)
Source Host	IP address of the host from which the configuration was imported.
Imported On	Date of import.

Attribute	Description
Imported By	User who imported the configuration.
SW Version	Software version of the configuration.
Source Model	For appliances, the model number of the source host Logger. (For software Logger, this is shown as Software.)

You can perform the following initial configuration management tasks:

- [Import an Initial Configuration](#)
- [Push an Initial Configuration](#)
- [View the Initial Configuration Event History](#)
- [Delete an Initial Configuration](#)

Importing an Initial Configuration

An initial configuration created on a managed Logger (of version 6.1 or later) may be imported into ArcSight Management Center, for editing and pushing to other Loggers.

ArcMC can store up to 30 initial configurations.

To import an initial configuration from a Logger of version 6.1 or later:

1. Click **Configuration Management > Other Configurations > Logger Configurations**.
2. Under **Configurations**, click **Import**.
3. On the **Import Initial Configuration** dialog, in **Name**, enter a name for the configuration you wish to import.
4. Under **Source Host URI**, select the node from which you wish to import the configuration.
5. Click **Import**. The configuration is imported into ArcSight Management Center and is shown in the **Configurations** table.
6. Optionally, if you wish to push the imported configuration to managed nodes, when prompted to push, click **Yes**.

An initial configuration is not created in ArcMC. Instead, create the initial configuration on a managed Logger, and then import it into ArcMC for pushing to other managed Loggers.

Pushing an Initial Configuration

You can push an initial configuration to selected managed Loggers of version 6.1 or later. The destination Loggers must be of the same software version (and, for hardware appliances, model number) as the Logger on which the initial configuration was created.

The push process overwrites the settings on the destination Loggers.

Pushing an initial configuration must be performed manually.

Before performing a push, ensure that the destination Logger's storage volume is set up, and that it exceeds that of any source Logger.

To push an initial configuration to one or more managed Loggers of version 6.1 or later:

1. Click **Configuration Management > Other Configurations > Logger Configurations**.
2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.
4. On the **Make Selections for Push** dialog, under **Available Nodes**, the nodes eligible for receiving a push are displayed by location. Browse to the recipient node and click **Add**. The selected node is shown under **Selected Nodes**. (To select multiple nodes to receive a push, Ctrl+click each selected node.)
5. Click **Push**.
6. Click **Yes** to confirm the push and change settings on the destinations. The configuration is pushed to the selected destination nodes.

In order to correctly view push status, click **Refresh**, even if the status is shown as In Progress.

Push Results on a Destination Logger

The results of a push of an initial configuration on a given setting of a destination Logger are dependent on the setting, as shown in the following table.

Setting on Destination	Result After Push
<ul style="list-style-type: none">• Archive storage settings• Audit logs• ESM destinations• Event archives• Finished tasks• Forwarders• Peer Loggers	Blank: These settings will be blank on the destination, even if they are included in the pushed initial configuration. Also, all configurations on the destination Logger related to these settings will also be blanked.
<ul style="list-style-type: none">• Alerts• User-created receivers (RFSFileReceiver, FileTransfer, FolderFollowerReceiver)	Disabled: These settings are disabled on the destination Logger, but are editable through the destination Logger's UI.
<ul style="list-style-type: none">• Hosts file• Groups• Users	Copied From Source: These values are copied from the initial configuration and overwritten on the target. This may include user credentials that the Logger uses to authenticate to ArcMC, which could break the management link between ArcMC and the destination Logger (which requires these credentials). If an overwrite of these credentials occurs, to enable management, delete the host from ArcMC, and then re-add the Logger as a host (with the new credentials).
<ul style="list-style-type: none">• All other settings	Copied From Source: Values are copied from the initial configuration and overwritten on the target.

Deleting an Initial Configuration

A deleted initial configuration is no longer available for pushes. You may not delete a configuration currently being pushed.

To delete an initial configuration:

1. Click **Configuration Management > Other Configurations > Logger Configurations**.
2. From the **Logger Configurations** table, select one or more configurations to be deleted.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Event History

The **Event History** list records all imports, pushes, and delete transactions related to initial configuration pushes. Each event in the history displays the following information:

Column	Description
Init-Config Name	Initial configuration's name.
Author	User who performed the action.
Event Type	Type of event recorded for the initial configuration. Event types include Push, Import, and Delete.
Event Occurrence	Local date and time of the event.
Source Host	URI of the host on which the initial configuration was created.
Destination URI for Push	If the event is of type Push, this is the URI of the destination node to which the initial configuration was pushed.
Event Status	Status of the event. Status types include: <ul style="list-style-type: none">• In-progress: the transaction is still in progress.• Successful: the transaction succeeded.• Failed: the transaction failed. Click the failed status to view an indication of the failure reason.

To search for a specific event by any of these criteria, click the drop-down in the corresponding column header. Then, in **Filters**, select or enter the specific criterion for which you wish to show events. Only events matching the filter will be displayed in the **Event History** list.

For example, to see all pushes, in the **Event Type** column, click the header drop-down. Then, in **Filters**, select *Push*.

Managing Logger Event Archives

Logger Event Archives enable you to save the events for any day in the past (not including the current day). In ArcMC, you can view Logger Event Archives on managed Loggers, and perform management tasks including loading, unloading, and indexing archives.

Logger Event Archive management is only available for managed Loggers of version 6.2 or later.

For complete information on managing Logger Event Archives, see the Logger Administrator's Guide.

The following parameters are shown on the Logger Event Archives list:

Parameter	Description
Peers	For Loggers, the number of peers of the Logger. To see the Logger's peers in detail, click the number shown.
Event Status	The status of a current archiving job, where status is one of the following values: <ul style="list-style-type: none">• <i>Loading</i>: The archive is being loaded on the managed Logger.• <i>Loaded</i>: The archive is currently loaded on the managed Logger.• <i>Unloading</i>: The archiving job is currently executing.• <i>Archived</i>: The archiving job is complete.• <i>Failed</i>: The archiving job was not successful.
Index Status	The status of a current indexing job, where status is one of the following values. <ul style="list-style-type: none">• <i>None</i>: No indexing status is available.• <i>Pending</i>: The indexing job is about to begin. A pending job can be canceled by clicking in the Cancel column of the table.• <i>Indexing</i>: The indexing job is in process.• <i>Indexed</i>: The indexing job is complete.• <i>Failed</i>: The indexing job was unsuccessful.
Cancel	Click the X to cancel a pending indexing job before it begins.

To view Logger event archives:

1. Under **Configuration Management**, select **Other Configurations > Logger Event Archive**.
2. On the **Event Archive List** tab, select the criteria you will use to search for Logger Event Archives on managed Loggers.
3. Select a Start and End Date, then select one or more Loggers to search.
4. Click **Search**. All Logger Event Archives matching the search criteria are listed in hierarchical format: by managed Logger, then by Storage Group, and finally by Event Archive.

To toggle the view open or closed, click **Expand** or **Collapse**.

Managing Event Archives

You can perform two management tasks on managed Loggers related to event archives: loading (or unloading) archives, and indexing them.

To load an event archive:

1. On the Event Archive List, select an archive to load.
2. Click **Load Archive**. The selected operation will be performed. The status of the job will be shown in the **Event Status** column.

To index an Event Archive:

1. On the Event Archive List, select an archive to index.
2. Click **Index Archive**. The selected archive will be indexed. The status of the indexing job will be shown in the **Index Status** column.

Viewing Load/Unload History

You can also view your Logger event archive load, unload, and indexing history. This displays the actions taken in ArcMC to view Logger Event Archives.

To view Logger event archive load/unload history:

1. Under **Configuration Management**, select **Initial Configurations > Logger Event Archive**.
2. Click the **Archive Load/Unload History** tab. The activity history is displayed.

Managing Logger Peers

Managed Loggers can be peered with any number of other Loggers. You can manage the peer relationship between Loggers in ArcMC. ArcSight recommends that, if possible, all peer Loggers be managed by ArcMC.

You can view peers; add or remove peers to a Logger; and import, edit, push, and delete peer groups. A *peer group* is a named set of Loggers you can use to organize and administer sets of Loggers more easily.

For more information about Logger peering, please refer to the ArcSight Logger Administrator's Guide.

Viewing Peers or Peer Groups

You can view the peers of a Logger managed by ArcMC, as long as the Logger is version 6.1 or later.

To view peered Loggers in ArcMC:

1. Select **Configuration Management > Manage Logger Peers**. The **Manage Peer Loggers** table is displayed with all managed Loggers of version 6.1 or later.
2. To view the Loggers peered to a specific Logger in the list, in the **Peer Loggers** column, click the link indicating the number of peers. The filterable **Peer Loggers** dialog lists all the Logger's peers.
3. To view peer groups in ArcMC, click **View Peer Groups**.

Adding or Removing Peers

You can add peers to, or remove peers from, a Logger managed by ArcMC, as long as the managed Logger is version 6.1 or later.

If you remove a Logger not managed by ArcMC as a peer, you will not be able to add it back to the group unless you import the peer group including the Logger into ArcMC, or you add the removed Logger to ArcMC management.

To add peers to, or remove peers from, a Logger:

1. Select the Logger whose peers you wish to edit from the **Manage Logger Peers** table.
2. Click **Edit Peers**.
3. All currently peered Loggers are shown.
 - a. To add one or more peers, click **Add Peers**. Then, in the **Add Peers** dialog, select the Loggers to be added as peers. Optionally, to create a new peer group in ArcMC, in **Peer Group Name**, enter a name for the peer group. Then, click **Add**.
 - b. To remove one or more Loggers as peers, select the Loggers to remove, and click **Remove Peers**. Click **Yes** to confirm removal as peers.

For this release, Logger peering is supported using user name and password, not authorization code.

Importing a Peer Group

You can import Logger peer groups into ArcMC. Importing a peer group is only supported on Loggers of version 6.1 or later.

To import a peer group from a Logger (of version 6.1 or later):

1. Select **Configuration Management > Manage Logger Peers**.
2. Click **View Peer Groups**.
3. Click **Import Peers**.
4. On the **Select Peer** dialog, select a managed Logger. (The selected Logger will also be part of the imported peer group.) Then, click **Next**.
5. On the **Select Peer (of the Target)** dialog, select one or more peers to import into ArcMC.
6. In **Peer Group Name**, enter a name for the selected peer group.
7. Click **Import**. The selected peer group is imported into ArcMC.

Edit a Peer Group

You can edit a peer group, including the name, peered Logger hostname, and group members.

To edit a peer group:

1. Select **Configuration Management > Manage Logger Peers**.
2. Click **View Peer Groups**.
3. Click the name of the peer group you wish to edit.
4. On the **Edit Peer Group** dialog, edit the peer group as needed. You can edit the peer group name, and add or remove peers from the group.
5. Click **Save**. Alternatively, click **Save As...** to save the peer group under a new name.

Pushing a Peer Group

You can push a peer group to one or multiple managed Loggers of version 6.1 or later. The Loggers in the group will become peered with the managed Loggers to which you pushed the group.

To push a peer group:

1. Click **Configuration Management > Manage Logger Peers**.
2. Click **View Peer Groups**.
3. From the table, select a peer group to push.
4. Click **Push**.
5. On the **Destination Loggers** dialog, select one or more destination Loggers to which to push the peer group.
6. Click **Push**. The peer group is pushed to the destination Loggers.

Deleting a Peer Group

You can delete a peer group from ArcMC.

To delete a peer group:

1. Click **Configuration Management > Manage Logger Peers**.
2. Click **View Peer Group**.
3. From the list of peer groups, select a group to delete.
4. Click **OK** to confirm deletion.

Managing Event Broker

You can use ArcMC to perform management and monitoring of Event Broker. These functions include adding topics, managing routes, and status monitoring.

About Topics

A *topic* is a metadata tag that you can apply to events in order to categorize them. Event Broker ships with several pre-set topics, and you can define any number of additional topics as needed.

A topic includes these components:

- **Name:** The name of the topic.
- **Partition:** A segment of a topic. There can be one or more partitions for each topic. The number of partitions limits the maximum number of consumers in a consumer group.
- **Replication Factor:** The number of copies of each partition in a topic. Each replica is created across one Event Broker node. For example, a topic with a replication factor of 3 would have 3 copies of each of its partitions, across 3 Event Broker nodes.

You can currently only use ArcMC to add topics, not edit or delete them.

For more information on managing topic partitions and replication, see the Event Broker Administrator's Guide.

Adding a Topic

To add a topic:

1. Click **Configuration Management > > Other Configurations > Manage Event Broker.**
2. On the Event Broker Configurations page, click **Add Topic.**
3. On the Add New Topic dialog, in **Topic Name**, enter a name for the new topic.
4. In **# of Partitions**, enter the number of partitions the topic will have.
5. In **Replication Factor**, enter the number of copies that will be made for each partition.
6. Click **Save.**

Best Practice: When creating a topic, use a value for replication factor of at least 2. In addition, the number of partitions should be equal to the number of consumers which will be subscribed to the topic (now and in future). If Vertica will be a consumer, the number of partitions should be a multiple of the number of Vertica nodes.

About Routes

A *route* is a method of retrieving events in a topic that meet certain criteria and then copying them into a new topic. Use routes to filter events into your topics for your own requirements, such as selecting a group of events for more detailed examination.

A route comprises these components:

- **Name:** Name of the route.
- **Routing Rule:** A logical filter that defines criteria by which events will be categorized into topics. The criteria are defined in terms of CEF fields.
- **Source Topic:** The topic being filtered for events which match the routing rule.
- **Destination Topic:** The topic to which a copy of an event matching the routing rule should be copied. (A copy of the event will remain in the source topic.)
- **Description:** A short description of the route.

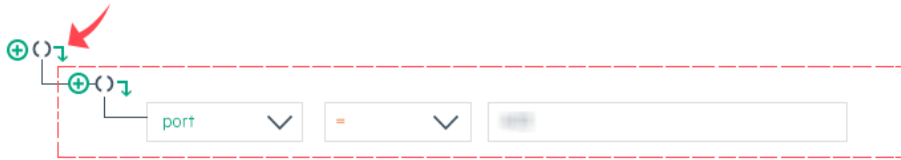
You can add, edit, or delete routes in ArcMC. Routes only apply to CEF topics. Routes created to or from a binary topic (such as eb-esm) will not function.

Creating a Route

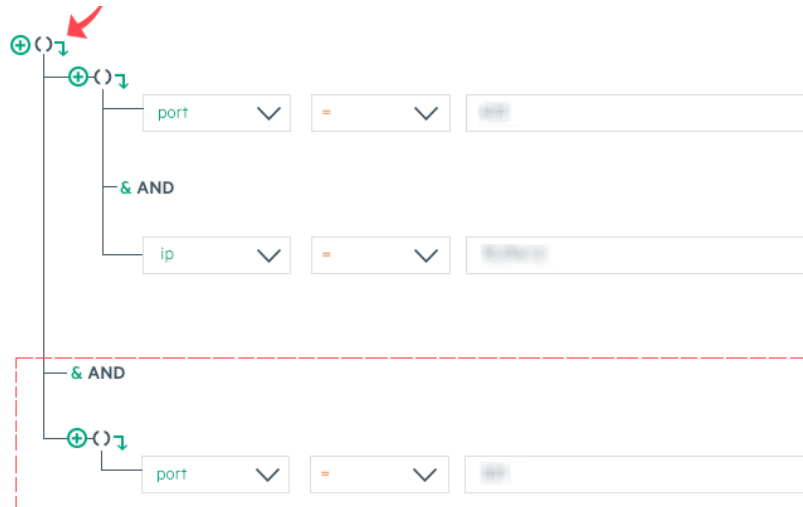
Before creating a route, ensure that your source and destination topics already exist. If not, [create them](#) before creating a route that uses them.

To create a route:

1. Click **Configuration Management > Other Configurations > Manage Event Broker**.
 2. On the Event Broker Configurations page, click **Add**.
 3. In **Route Name**, enter a name for the route.
 4. From the **Source Topic** drop-down list, select the topic from which events will be filtered.
 5. From the **Destination Topic** drop-down list, select the destination to which events will be copied.
 6. In **Description**, enter a short description of the route.
 7. Under **Add Routing Rule**, use the Rule Editor to define the criteria for the routing rule.
- Define a criterion by using the drop-downs to select a **Field**, **Operator**, and **Value** as a filter. Fields are taken from the Event Broker SuperSchema, which are described in detail in ["SuperSchema" on page 322](#).
 - Click + to add a new conjunction (& AND, || OR), or the right arrow to add a dependent conjunction. Then define any new required criteria as needed.



- You can create nested conjunctions by clicking the right arrow at the same level as the current conjunction.



- To change a conjunction, right-click the conjunction and select your choice from the drop-down menu.
- To delete a conjunction, right-click the conjunction and pick Delete. Note that deleting a conjunction will delete all the criteria associated with the deleted conjunction.

The rule is shown in the rule field as you construct it. When the rule is complete, click **Save**.

Editing a Route

To edit a route:

1. Click **Configuration Management > > Other Configurations > Manage Event Broker**.
2. On the Event Broker Configurations page, select the route to edit, and then click **Edit**.
3. Edit the route as needed, and then click **Save**.

Deleting a Route

To delete a route:

1. Click **Configuration Management > > Other Configurations > Manage Event Broker.**
2. On the Event Broker Configurations page, select one or more routes to delete, and then click **Delete.**
3. Click **Yes** to confirm deletion.

Deployment Templates

A *deployment template* is a pre-set collection of settings and parameters for a connector or Collector.

When you deploy that connector or Collector type using the Instant Connector Deployment process, and specify a deployment template, all of the settings you have predefined in the template are applied during the deployment.

You may specify any number of deployment templates for each connector type.

Note: During the deployment process, you are prompted to use the predefined template settings, but may choose to overwrite any of the predefined template settings to custom-fit a particular deployment.

Managing Deployment Templates

You should be familiar with the settings for connectors and Collectors before managing deployment templates. These settings are described in detail in the Smart Connector User's Guide, available from [Protect724](#).

Prior to managing any deployment templates, first upload the appropriate 64-bit connector or Collector installer file to your ArcMC repository. Only the Linux and Windows 64-bit installers are supported. The installer contains a list of currently supported connectors or Collectors and is used in the creation of the connector or Collector list in ArcMC. This upload only needs to be done in preparation to manage deployment templates.

To upload the installer file to ArcMC:

1. Download the connector or Collector installer file to a secure network location.
2. In ArcMC, click **Administration > Application > Repositories.**
3. In the navigation menu, click **Upgrade Files.**

4. Click **Upload**.
5. Under **Upload Upgrade Repository**, click **Choose File**. Then, browse to and select the installer file you previously downloaded.
6. Click **Submit**. The installer file is uploaded to ArcMC.

Additional Files

Note that some connector types may require additional, supplementary files to function correctly, such as Windows DLLs. Such files are not included in the connector installer file.

If additional files are required for a connector type, you must also upload these files to an ArcMC repository before attempting to deploy them using the Instant Connector Deployment process. After uploading the installer file as described, upload additional files (in ZIP format) to the following repositories:

File Type	Repository
SecureData server certificate (Certificate_FPE)	cacert. Note: The certificate must be Base 64 encoded. For Linux platforms (only), it must include the .pem extension.
Windows DLL, JavaLibrary	JDBC Drivers
FlexParsers	Flex Connectors

You will be able to specify the location of these additional files when you create the deployment template.

To create a deployment template:

Click **Configuration Management > Deployment Templates**.

1. In the navigation menu, from the list of supported connectors or Collectors, select the type of connector/Collector for which you wish to create a template.
2. In the management panel, click **New**.
3. Enter values for any required settings (marked with an asterisk *), as well as any settings you wish to apply to all connectors or Collectors of that type when using Instant Connector Deployment. (**Note:** Spaces in file or path names are not supported.)
4. If additional files are needed for operation, such as a Voltage server certificate, under **File Table Fields**, enter values for file name, type, and any other required fields. If more than 1 additional file is needed, click **Add Row**, and then specify the details of the additional file. Repeat for additional files as needed.
5. Click **Save**.

ArcSight Secure Data Add-On Enablement: To enable the ArcSight Secure Data Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. Note that only a

single instance of the add-on is supported on Windows clients. If you wish to move the add-on to a new location, you must first uninstall the previously installed client before launching Instant Connector Deployment.

To delete a deployment template:

1. In the navigation menu, browse to the template you wish to delete. (Templates are sorted by connector/Collector type.)
2. In the management panel, select the template and click **Delete**. Click **Yes** to confirm deletion.

Managing Collectors

Note: Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features**. These features are provided for your testing and evaluation only and must not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.** We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

The **Collectors** tab displays all Collectors associated with the item selected in the navigation tree. For example, if you selected a host in the navigation tree, the **Collectors** tab would show all Collectors associated with that host.

The **Collectors** tab includes the following buttons, which operates on one or more selected Collectors:

Properties	Update the properties of the selected Collectors. For more information, see "Updating Collector Properties" on the next page
Retrieve Logs	Retrieves Collector logs. For more information, see "Retrieving Collector Logs" on the next page
Update Parameters	Update the parameters of the selected Collectors. For more information, see "Updating Collector Parameters" on page 198
Destinations	Manage Collector destinations. For more information, see "Updating Collector Destinations" on page 198
Credential	Manage Collector credentials. For more information on managing Collector credentials, see "Updating Collector Credentials" on page 198
Restart	Restart the selected Collectors. For more information on restarting Collectors, see "Restarting Collectors" on page 199 .
Delete	Deletes the selected Collectors. For more information, see "Deleting Collectors" on page 199

The **Collectors** table displays the following parameters for each connector:

- **Name:** Name of the Collector.
- **Port:** Collector port.
- **Type:** Type of Collector.
- **Syslog Lines Received:**
- **Custom Filtering: messages filtered out:**
- **Status:** Collector status.
- **Last Check:** Date and time of the last status check.

For more information on connector management, see ["Managing Connectors" on page 118](#).

Updating Collector Properties

To update the the properties of a Collector:

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select the Collector you wish to manage.
3. Click **Properties**.
4. On the **Collector Property Update** page, click **Edit**.
5. Edit the Collector properties as needed.
6. To add a new property, click **Add**, then enter the property and a value for the property.
7. When complete, click **Save**.

Retrieving Collector Logs

To retrieve Collector logs:

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors for which you wish to retrieve logs.
3. Click **Retrieve Logs**.
4. Follow the wizard prompts to zip the selected logs into a single file.
5. To view the logs, on the main menu bar, click **Admin > Repositories**. The log zip file is stored in the *Logs* repository.

Updating Collector Parameters

To update Collector parameters:

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors for which you wish to update parameters.
3. Click **Update Parameters**.
4. On the **Collector Parameter Update** page, enter values for the Collector parameters, as needed.
5. Click **Save**. The parameters are updated for the selected Collectors.

Updating Collector Destinations

To update Collector destinations:

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors for which you wish to update destinations.
3. Click **Update Destinations**.
4. On the **Collector Destination Update** page, enter values for the Collector destinations, as needed.
5. Click **Save**. The destinations are updated for the selected Collectors.

Updating Collector Credentials

To update Collector credentials:

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors for which you wish to update credentials.
3. Click **Credential**.
4. On the **Collector Credential Update** page, enter values for the Collector passwords, as needed. (The username is fixed as *Collector*.)
5. Click **Save**. The passwords are updated for the selected Collectors.

Note: Updating Collector credentials does not update the Collector's actual credentials, just the credentials ArcMC uses to authenticate to the Collectors.

Restarting Collectors

To restart one or more Collectors

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors which you wish to restart.
3. Click **Restart**.
4. Click **Yes** to confirm restart. The Collectors are restarted.

Deleting Collectors

1. Click **Configuration Management > Manage Collectors**.
2. On the **Manage Collectors** page, select one or more Collectors which you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm delete. The Collectors are deleted.

Chapter 8: Managing Users on Managed Products

The following topics are discussed here.

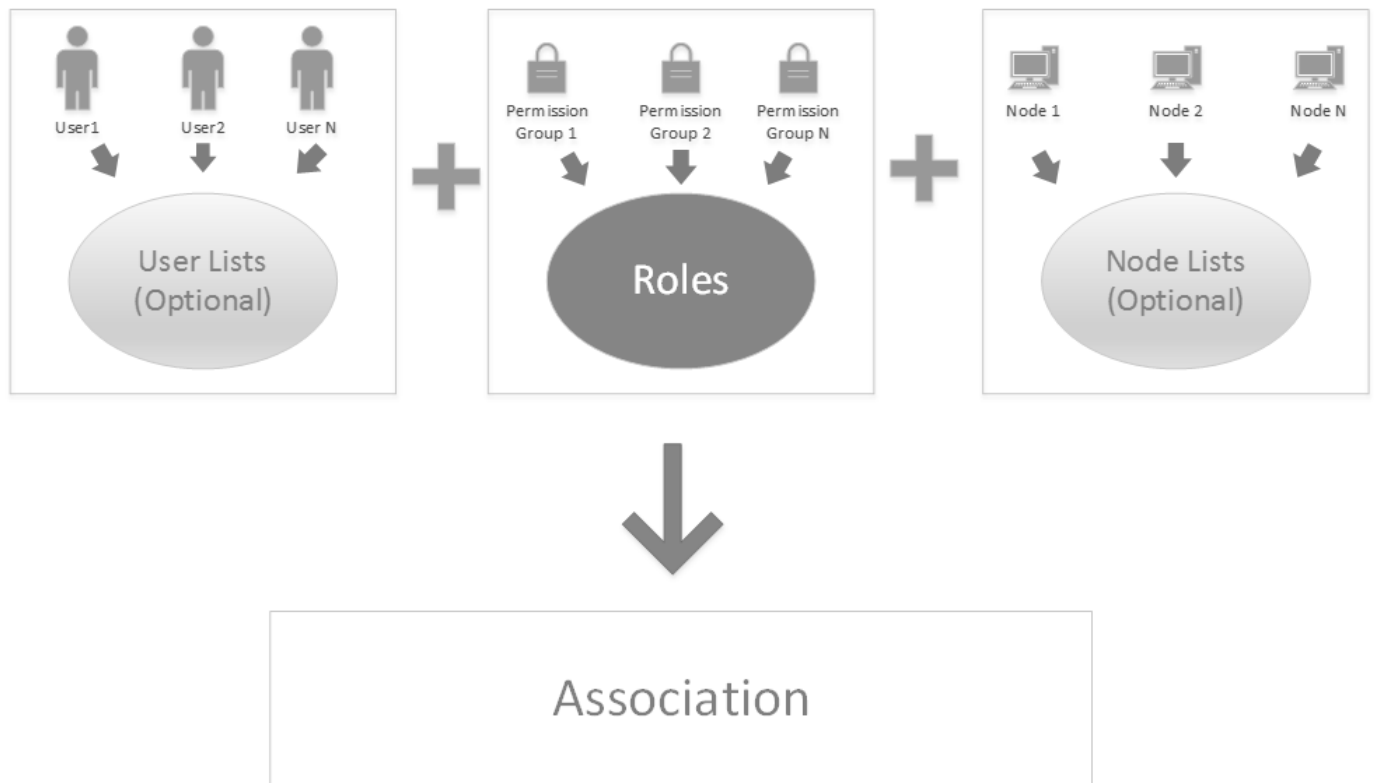
• Overview	200
• Users and User Lists	201
• Permission Groups	203
• Roles	205
• Node Lists	206
• Associations	207
• Compliance Report	209

Overview

Role-based access control (RBAC) user management enables you to manage product user access with custom roles across specified nodes.

Previous versions of ArcMC included user management across nodes as part of Configuration Management (where user information was defined in a Users configuration). In ArcMC 2.1, user management across nodes is now a separate, greatly improved RBAC (role-based access control) functionality.

User Management Workflow



User management in ArcSight Management Center follows this workflow:

1. Create users in ArcSight Management Center, or import them from managed nodes.
2. Optionally, group users into [user lists](#) for ease of organization and management.
3. Create (or import) [permission groups](#) to enable administrative privileges.
4. Create [roles](#) by assigning permission groups to grant functional access to products.
5. Optionally, create [node lists](#) to ease the organization of sets of nodes.
6. Create [associations](#) to associate users (or user lists), nodes (or node lists), and roles.
7. [Push associations to nodes](#) to enable access for users included in the association, with privileges appropriate for the role and access only to the desired nodes.
8. [Check compliance](#) of users on managed nodes with the managing ArcMC.

Users and User Lists

A *user* is defined by a set of values for an individual's credentials and other identifiers, such as first and last name, email, and phone number. On nodes managed by ArcMC, users of those nodes and their permissions can be managed entirely by ArcMC.

Users can be grouped into named *user lists*, which can also be assigned access rights in the same way as individual users.

You can also import users from managed nodes.

Users are defined by these parameters:

Parameter	Description
User Name*	Name used for login credentials.
First Name*	User's first name.
Last Name*	User's last name.
Distinguished Name	User's distinguished directory name, if any.
Email*	User email address. Users pushed to nodes as part of an association will receive email confirmation of their new access to nodes at this address, along with a randomly generated password. (Please verify that this is the correct email address. Once pushed, the password will not be resent to a corrected email address.) Note: To ensure email alerts are sent, enable SMTP services and then restart the web services.
Title	User's job title.
Department	Department of employment.
Phone	Phone number for the user.
Notes	Relevant notes on the user.

To create a user:

1. Click **User Management > Users and User Lists**.
2. Click **New User**.
3. Enter values for the user details.
4. Click **Save**.

To import users from a managed node:

1. Click **User Management > Users and User Lists**.
2. Click **Import User**.
3. On the node list, select the node from which you will import users.
4. On the **Import Users** page, use the arrow keys to move selected users from the **Available Users** list to the **Selected Users** list.
5. Click **Import**. The selected users are imported into ArcMC.

To create a user list:

1. Click **User Management > Users and User Lists**.
2. Click **New User List**.
3. In **User List Name**, enter a name for the user list.
4. The **Selected Users** column shows all users currently selected for the users list. Use the directional arrows to add to, or remove from the **Available Users** list to the **Selected Users** list.
5. Click **Save**.

To edit a user or user list:

1. Click **User Management > Users and User Lists**.
2. On the **Users and User Lists** page, click the name of the user or user group you wish to edit.
3. Edit the user or user list as needed, and then click **Save**. Click **Save As** to save an edited user list under a new name.

To delete users or user lists:

Use caution when deleting users. Deleting a user on ArcMC will delete the user from all nodes where the user was pushed as part of an association.

In order to delete a user, any nodes on which the user is present must be able to communicate with ArcMC.

You can only delete a user list if it is not part of any association. To delete a user list that is part of an association, delete the association first.

1. Click **User Management > Users and User Lists**.
2. On the **Users and User Lists** page, select the users or user lists you wish to delete.
3. On the toolbar, click **Delete**.
4. Click **Yes** to confirm deletion.

For information on how to assign users to roles, see ["Roles" on page 205](#).

Permission Groups

A *permission group* is a set of access privileges. Access privileges are organized functionally, enabling you to assign different functions or different product access across users.

Permission groups are the building blocks of **roles**. In themselves, permission groups do not enable access for any users. Permission groups can be bundled into **roles**, and when users are assigned to those roles, they will gain the privileges which the individual permission groups grant them.

Permission groups can be created, imported from managed nodes, edited, and deleted in ArcMC.

You can create permission groups of the following types in ArcMC.

Group Type	Grants access to...
System Admin	System admin and platform settings.
Logger Rights	Logger general functionality. Does not include Logger Reports and Logger Search permissions.
Logger Reports	Logger report functionality.
Logger Search	Logger search functionality.
Conapp Rights	Connector Appliance general functionality.
ArcMC Rights	ArcSight Management Center general functionality. Note that ArcMC rights <i>View options</i> and <i>Edit, save and remove options</i> can only be granted to groups with either <i>View management</i> or <i>Edit, save, and remove management rights</i> .

You can create different permission groups to reflect different management access levels. For example, you could create two System Admin permissions groups, one with access to reboot and update privileges, and the other with access to global settings. However, a role can only be assigned one permission group per group type.

To create a permission group:

1. Select **User Management > Permission Groups**.
2. On the **Permission Groups** page, click **New**.
3. In **Group Name**, enter a name for the new group.
4. Select a type from the **Group Type** drop-down list.
5. In **Description**, enter a brief description of the permission group.
6. In the **Rights** list, select the rights to which the permission group controls. (Click **Select All** to select all rights in the list.)
7. Click **Save**.

To import one or permission groups from a managed node:

1. Select **User Management > Permission Groups**.
2. On the **Permission Groups** page, click **Import**.
3. From the list of managed nodes, select the node from which to import a group, and then click **Next**.
4. The **Available Permission Group(s)** column shows available permission groups on the managed node. Select one or more groups, and then use the **Add** button to move them to the **Selected**

Permission Group(s) column. (Note that permission groups already present in ArcMC will be shown as disabled and unavailable for selection.)

5. Click **Import**. The groups are imported into ArcMC.

To edit a permission group:

1. Select **User Management > Permission Groups**.
2. From the list of groups, click the name of the group you wish to edit.
3. Enter values or select rights as needed.
4. Click **Save**. (Click **Save As** to save the group under a new name.)

To delete a permission group:

You can only delete a permission group that is not currently assigned to any roles, nor is part of any Filter configuration.

To delete a permission group that is part of a role, delete the role first.

To delete a permission group that is part of a Filter configuration, remove it from the configuration.

1. Select **User Management > Permission Groups**.
2. From the list of groups, select the group you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Roles

Roles

+ New X Delete			
Name	Last Modified On	Last Modified By	Groups
hlu	May 15, 2015 12:14:33 PM	admin	2
role_1	May 15, 2015 12:02:29 PM	admin	3
Brand New Role	May 15, 2015 11:41:49 AM	admin	1
ConApp Manager	May 15, 2015 10:55:50 AM	admin	1

A *role* is a bundled set of [permission groups](#). By assigning a role to an association, you grant all privileges enabled by the role's component permission groups to all of the users or user lists in the association.

You can create and delete roles in ArcMC.

To create a role:

Prior to creating a role, create any [permission groups](#) it will include.

1. Select **User Management > Roles**.
2. Click **New**.
3. In **Role Name**, enter a name for the role.
4. In the **Available Permission Group(s)** column, select one or more permission groups. Use the **Add** button to move selected permission groups from the **Available Groups** column to the **Selected Permission Group(s)** column.
5. Click **Save**.

To delete one or more roles:

Before deleting a role, edit any associations of which it is a part to remove the role from each association.

1. Select **User Management > Roles**.
2. From the list of roles, select one or more roles to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

For information on assigning associations to roles, see ["Associations" on the next page](#).

Node Lists

Node Lists

+ New X Delete			
Name	Last Modified On ▼	Last Modified By	Nodes
New Node List	May 18, 2015 12:15:48 PM	admin	37
nod_list1	May 15, 2015 12:02:54 PM	admin	3

A *node list* is a named set of managed nodes. Using node lists allows you to organize nodes for the purpose of managing users of those nodes in a group.

All nodes in a node list included in an [association](#) will receive pushes of the association from ArcMC.

An association is pushed only to nodes (or node lists) which it includes. To push an association to a particular node, make sure the node is included in the association, either directly or as part of a node list.

You can create, edit, and delete node lists.

To create a node list:

1. Click **User Management > Node Lists**.
2. Click **New**.
3. In the **Available Nodes** column, select multiple nodes or node lists to include. Use the **Add** button to move the selections to the **Selected Nodes** column.
4. Click **Save**.

To edit a node list:

1. Click **User Management > Node Lists**.
2. Select a node list to be edited.
3. Edit the node list as needed.
4. Click **Save**. (Click **Save As** to save the node list under a new name.)

To delete one or more node lists:

You can only delete a node list if it is not assigned to any associations. To delete a node list that is part of an association, first remove it from the association or delete the association.

1. Click **User Management > Node Lists**.
2. From the list of node lists, select one or more node lists to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Associations

An *association* is a bundled group of users (or user lists), along with any number of non-overlapping roles, and any number of nodes (or node lists). Associations are managed in ArcMC and then pushed to managed nodes, in order to grant permissions to users of those nodes.

You can create associations, push them to included nodes, and delete associations.

To create an association:

Prior to creating an association, create all users (or user lists), node lists, and roles to be included in the association.

1. Click **User Management > Associations**.
2. Click **New**.

3. In **Association Name**, enter a name for the new association.
 4. In the **Available Users and User Lists** column, select multiple users or user lists to include. Use the **Add** button to move the selections to the **Selected Users and User Lists** column.
 5. Click **Next**.
 6. On the **Assign Roles** page, in the **Available Roles** column, select one or more roles to include. Use the **Add** button to move the selections to the **Selected Roles** column.
 7. Roles in an association may not overlap in terms of product type.
 8. Click **Next**.
 9. In the **Available Nodes and Node Lists** column, select multiple nodes or node lists to include. Use the **Add** button to move the selections to the **Selected Nodes and Node Lists** column.
 10. Click **Check Conflicts**. A conflict is returned if the permissions assigned in the association conflict with any other association that also assigned the same permission groups types. For example, if an existing association assigns read/write access to User A, and your newly-created new association assigns read-only rights to User A, then a conflict would be returned.
- If a conflict was found in the association, edit the association to correct the conflict shown.
 - If no conflict was found, click **Yes** to push the new association to all nodes included in the association.

To push an association to its included nodes:

1. Click **User Management > Associations**.
2. Click the name of the association you wish to push.
3. Click **Push**. The association is pushed to its included nodes.

An association is pushed only to nodes (or node lists) that it includes. To push an association to a particular node, make sure the node is included in the association, either directly or through a node list.

To edit an association:

1. Click **User Management > Associations**.
2. Click the name of the association you wish to edit.
3. Edit the components of the association as needed.
4. Click **Save**.

To delete one or more associations:

1. Select **User Management > Associations**.
2. From the list of associations, select one or more associations to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Compliance Report

The Compliance Report verifies and displays the compliance status of users on a managing ArcMC with the same users on managed nodes, to which associations including those nodes have been pushed. Compliance status includes permissions, names, and other user data.

To run the Compliance Report:

1. Click **User Management > Compliance Report**. The report displays compliance information.

The **User Info in Managing ArcMC** column displays users (or user groups) currently listed on each managing ArcMC in associations which have been pushed to nodes.

- Click the arrow to expand the column and view the permission groups for each user or user group in detail.
- Click the user name or user group name to view the current permission groups assigned to each user or user group.
- *User N/A* indicates that a user is present on the managed node but not on the managing ArcMC
- *Permission Group N/A* indicates that user or user group currently has permissions on the Managed Node that are not assigned to the destination.
- Users not in associations which have been pushed to nodes are not shown.

The **User Info on Managed Node** column displays the users, user groups, or permission groups currently listed on the managed node being compared.

The **Compliance** column indicates the compliance of the user on the managed node to the user on the managing ArcMC. A status of *Compliant* indicates that all user values match; *Non-Compliant* means one or more values do not match or are missing.

Click the compliance status for a detailed view of each user value.

Matches	Indicates that the value on the managed node matches the value on the managing ArcMC.
Does Not Match	Indicates a discrepancy between the value on the managed node and the managing ArcMC.
Missing Value(s)	The value or values are missing and cannot be compared.

Use the column headers to sort the tabular results across columns.

To export the compliance report results to PDF, click **Export to PDF**.

Chapter 9: Managing Backups and Restores

The following topics are discussed here:

• Overview	210
• Backup	210
• Restore	211

Overview

The **Backup** and **Restore** menu items enable you to back up and restore your ArcSight Management Center configuration. A complete backup includes all data on managed nodes, configurations, system administration, and connector data (in agentdata folders), as well as all repository files. You can also choose to include a selection of this data in a given backup file, to make your backup file smaller and more manageable.

Backup

You can back up the current ArcSight Management Center configuration as often as needed, either to a remote system on the network, or to your local system.

To back up the ArcSight Management Center configuration:

1. Click **Administration > Application > Backup**.
2. Under **Enter Backup Parameters**, supply values for the parameters listed in the following table:

Parameter	Description
Protocol	Select SCP to use Secure Copy to save the backup file on a remote system on your network. You need to specify the IP address or hostname, your user name and password, and the destination directory in the appropriate fields. Select Save to Local to save the backup file on your local system. When you select this option, the Port , IP/Host , User , Password , and Remote Directory fields are disabled (grayed out) as they are not needed.
Port	SCP only. The default port is 22.
Backup Server IP Address	SCP only. The IP address of the destination to receive the backup file.

Parameter	Description
User	SCP only. A user name on the destination.
Password	SCP only. The password for the user name you specify.
Remote Directory	SCP only. The subdirectory on the specified destination to receive the configuration backup file.
Schedule/ One time only	<p>One Time Only SCP only. Allows for a “one time only” backup.</p> <p>Schedule Provides the option to specify backup times in days, hours, or minutes. Note the following rules for this option:</p> <ul style="list-style-type: none"> Valid days of the week are M, Tu, W, Th, Fr, Sa, Su. Letters are not case-sensitive. Minutes must exceed 15 minute intervals. Minute intervals start at the top of the hour, not at the time the request was made. Hour intervals start at midnight, not at the time the request was made.
Backup	<ul style="list-style-type: none"> Select All to create a backup file that contains all data on managed nodes, configurations, system administration, connectors, Collectors, and repositories. Tip: Choosing All can potentially create a .tar.gz file so large that the restoration of data is unsuccessful. To prevent this, you may want to exclude connector data and repository data from your backup file. Select Exclude Repository Data to create a backup file that does not include files in the repositories. Select Exclude Connector Data to create a backup file that does not include connector data. (ArcMC Appliance only.) Select Exclude Connector and Repository Data to create a backup file that does not include repository files and connector data. (ArcMC Appliance only.)

- Click **Save** to back up the configuration, and then select a location to save the file.

Restore

You can restore your ArcSight Management Center configuration from a previous backup. These stipulations apply to restoring:

- The version of ArcSight Management Center used to restore the backup must be the same version used to create it.
- A backup performed on a root installation cannot be used to restore a non-root installation.
- For Software ArcSight Management Center, the install path of a restored Software ArcMC must be the same as the path of the backup, and the same root or non-root user must perform the installation


as did the backup.

- A Restore from one ArcMC backup may be performed to a different IP or hostname, subject to the stipulations above.

To restore the configuration:

1. Click **Administration > Application > Restore**.
2. Under **Upload Backup for Restore**, click **Choose File**.
3. Select your backup file.
4. Click **Upload** to restore the configuration from the specified backup file.

Caution: The version of ArcSight Management Center used to restore the backup must be the same version used to create it.

5. On software ArcMC, restart the ArcSight Management Center web process. On ArcMCappliance, reboot the appliance.
6. Optionally, re-import the SSL certificate for each container. Click the  icon to run the **Certificate Download** wizard and import the valid certificates. In addition, if a certificate mismatch is shown for any remote node, re-import the server certificate for the node.

After restoring the configuration:

- The cache size on the restore may be different from the cache size in the backup file. For example, after restoring the configuration, a managed node might receive more events or consume more cache.
- The container versions on the restore (if any) might be different from those in the backup file.
- The **Cache** column on the **Connectors** tab may take a few minutes to refresh the updated cache size for the connectors/Collectors.

Note: System Restore: For information on restoring an appliance to its factory settings, see ["Restoring Factory Settings" on page 318](#).

Chapter 10: Snapshots

The following topics are discussed here.

- [Overview](#)213
- [Creating a Snapshot](#) 213

Overview

ArcSight Management Center records audit and debug information, including details of any issues that can occur during normal operations. These system logs form a *snapshot* of your ArcSight Management Center activity. System logs are helpful in troubleshooting issues.

ArcSight Customer Support may ask you to retrieve and submit system logs as part of an incident investigation.

Creating a Snapshot

Creating a snapshot of ArcSight Management Center creates a set of zipped log files, which you can download locally.

Retrieve Snapshot Status

Summary		
Name:	Thread-3277	
Request ID:	NsTwAEEBABCqB6y4HDEbw	
Processing Time:	37 sec 462 ms	
Status:	Complete	

Action	Start Time	Time to Complete
Database content	9/8/13 9:18 PM	197 ms
Retrieving logs	9/8/13 9:18 PM	37 sec 264 ms

[Download](#)

To create a snapshot:

1. Click **Administration > Application > Snapshot**.
2. The **Retrieve Snapshot Status** page displays. Depending on the size of the log files, the snapshot may take a few moments to generate.
3. When ready, click **Download** to download the ZIP file locally.

Submit the snapshot file as instructed by ArcSight Customer Support.

Note: An ArcSight Management Center snapshot does not include information on the activity of

the ArcSight Management Center Agent on remotely-managed hosts.

To obtain logs for ArcSight Management Center Agent activity on a managed host, access the remote host. Under **Setup > Appliance Snapshot**, click the **Download** button.

Chapter 11: Logger Consumption Report

The Logger Consumption Report includes information on your Logger data consumption. You can choose which managed Logger 6.1 (or later) nodes to include in the report.

To generate a Logger Consumption report:

1. Click **Administration > Application > Consumption Report**.
2. Use the **Add** and **Remove** arrows to add or remove nodes from the **Available Nodes** column to the **Selected Nodes** column.
3. Click **Run Report**. The report is generated for the selected nodes.
4. Click **+** to expand the data on any node to view licensing specifics.
5. To export the license report to PDF, click **Export to PDF**.
6. Specify a time range for the report.
7. Click **OK** to exit the report.

Report Data

The report displays the licensed value and actual value for data consumption by managed Loggers.

Value	Description
Licensed Consumption	<p>Shows the data consumption to which your license entitles you. For individual ADP Loggers, the license limit will be shown as <i>Not Applicable</i>, since ArcMC tracks the overall ADP data limit, not those of individual Loggers.</p> <p>Note: If an ADP Logger is managed by a version of ArcMC earlier than 2.5, then the license limit will be incorrectly shown in the report as <i>Unlimited</i>.</p>
Actual Consumption	<p>Shows the current value of data consumption. Click the value to display the Consumption Chart, which shows data consumption in detail.</p>
Status	<p>Click any status hyperlink to view individual Logger data for the last 30 days. Status values are shown as follows:</p> <p><i>OK</i> if the actual value is less than or equal to the license value.</p> <p><i>In Violation</i> indicates that the actual value exceeds the license value, which constitutes a violation of the terms of your license. Your license permits you a number of violations for each 30-day period, which is shown on the <i>Violations Last 30 Days</i> line.</p> <p>Click any hyperlink to view individual Logger data for the last 30 days.</p>

Chapter 12: Managing Repositories

The following topics are discussed here.

• Overview	217
• Logs Repository	218
• CA Certs Repository	218
• Upgrade Files Repository	220
• Content AUP Repository	221
• Emergency Restore	222
• User-Defined Repositories	223
• Pre-Defined Repositories	227

Overview

Certain management operations require a specific upgrade or content update (.enc) file, or a certificate. Other operations, such as viewing logs, require you to load the logs to a Log repository. ArcSight Management Center can also maintain centralized repositories for files needed for host configuration and management.

By default, a number of pre-defined repositories are provided. However, you can create more repositories to suit your needs. Any repositories you create are referred to as *user-defined* repositories.

The following controls are used for repository functions:

- **Retrieve Container Files** copies a file from one or more managed hosts to the repository.
- **Upload to Repository** sends a file from your local computer (the computer running the browser) or a network host accessible from your local computer to the repository.
- **Retrieve** downloads a file from the repository.
- **Upload** copies a file from the repository to one or more managed nodes.

You can perform these operations using repositories:

- Manage logs in the Logs repository
- Manage CA certificates in the CA Certs repository
- Upgrade a connector using an upgrade file available in the Upgrade repository
- Apply a Content ArcSight Update Pack (AUP) on one or more connector
- Maintain centralized repositories of files for connector configuration and management

Logs Repository

To view logs, you need to first **Load** the logs of the container that contains the connector to the Logs repository, and then **Retrieve** the logs to view them.

Note: If a container contains more than one connector, logs for all connectors are retrieved.

For information on loading, retrieving, and deleting container logs, see ["Viewing Container Logs" on page 110](#).

Uploading a File to the Logs Repository

Uploading a file into the Log repository is useful for sharing annotated log or other files with other users. An uploaded file needs to be in .zip format.

To upload a ZIP file:

1. Click **Administration > Repositories**.
2. Click **Logs** from the left panel.
3. Click **Upload** from the management panel.
4. Enter the local file path or click **Browse** to select the ZIP file.
5. Click **Submit** to add the specified file to the repository or **Cancel** to quit.

Due to a browser limitation in Internet Explorer 11, the progress of the file upload will not be shown.

CA Certs Repository

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The CA Certs repository (shown below) enables you to store CA Certs files (that contain one or multiple certificates) and single CA certificates. When certificates are stored in the CA Certs repository, you can add the certificates to a container so that the connectors in the container can validate their configured destinations.

You can add a single certificate to a container that is in FIPS or non-FIPS mode. You can only add a CA Certs file to a container that is in non-FIPS mode.

To associate a CA certificate to a connector, you need to:

- Upload the CA certificate or CA Certs file to the CA Certs repository, as described below.
- Add a CA certificate from the CA Certs repository to the container that contains the connector, as

described in ["Managing Certificates on a Container" on page 113](#).

Uploading CA Certificates to the Repository

You can upload a CA Certs file or a single certificate to the CA Certs repository.

Tip: Before you upload a single CA certificate, change the name of the certificate on the local computer to a name that you can recognize easily. This helps you distinguish the certificate when it is displayed in the Certificate Management wizard.

To upload certificates to the repository:

1. Click **Administration > Repositories**.
2. Click **CA Certs** in the left panel.
3. Click **Upload** in the management panel.
4. Enter the local path for the CA Certs file or the certificate, or click **Browse** to select it.
5. Click **Submit** to add the specified CA Certs file or the certificate to the repository, or **Cancel** to quit.


The CA Certs Repositories tab shows all the CA Certs files and single certificates that have been uploaded. The Type column shows CERTIFICATE for a single certificate and CACERT for a CA Certs file.

Removing CA Certificates from the Repository

When you delete a CA Certs file or a single certificate from the repository, it is deleted from ArcSight Management Center.

Note: When you delete a CA Certs file or a single certificate from the CA Certs repository, containers are not affected; the connectors continue to use the certificates, which are located in a trust store after being added to a container. For information about adding a CA certificate to a container, see ["Managing Certificates on a Container" on page 113](#).

To remove a certificate from the repository:

1. Click **Administration > Repositories**.
2. Click **CA Certs** in the left panel.
3. Identify the certificate or the CA Certs file you want to remove and click its associated **Remove** button ().

Upgrade Files Repository

The Upgrade files repository enables you to maintain a number of connector upgrade files. You can apply any of these upgrade files to containers when you need to upgrade to a specific version. As a result, all connectors in a container are upgraded to the version you apply to the container.

Note: Logger ENC files are required for the remote upgrade of a Logger Appliance. For more information, see ["Upgrading a Logger " on page 102](#).

About the AUP Upgrade Process

Note: The process discussed in this section only applies to upgrading connectors and to upgrading a remotely-managed Connector Appliance. If you are upgrading the local ArcSight Management Center (localhost), use an ENC file instead.

To upgrade a connector or to upgrade a remotely-managed Connector Appliance, you need to:

- Upload the appropriate .aup upgrade file to the Upgrade Files repository, as described below.
- Apply the .aup upgrade file from the Upgrade Files repository to the container (see ["Upgrading All Connectors in a Container" on page 107](#)).

Uploading an AUP Upgrade File to the Repository


To upload AUP upgrade files to the repository:

1. Download the upgrade files for the connector or the remote Connector Appliance from the ArcSight Customer Support site at <http://softwaresupport.hpe.com/> to the computer that you use to connect to the browser-based interface.
2. From the computer to which you downloaded the upgrade file, log in to the browser-based interface.
3. Click **SetupConfiguration > Administration > Repositories**.
4. Click **Upgrade AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository or click **Cancel** to quit.
8. You can now use the AUP upgrade file to upgrade a container to a specific version. For instructions, see ["Upgrading All Connectors in a Container" on page 107](#).

Removing a Connector Upgrade from the Repository

You can remove a connector upgrade file from the repository when you no longer need it. When you remove a connector upgrade file from the repository, it is deleted from ArcSight Management Center.

To remove a Connector upgrade from the repository:

1. Click **SetupConfiguration > Administration > Repositories**.
2. Click **Upgrade AUP** from the left panel.
3. Locate the upgrade file that you want to delete and click the associated  icon.

Content AUP Repository

ArcSight continuously develops new connector event categorization mappings, often called *content*. This content is packaged in ArcSight Update Packs (AUP) files. All existing content is included with major product releases, but it is possible to stay completely current by receiving up-to-date, regular content updates through ArcSight announcements and the Customer Support site. The AUP files are located under Content Subscription Downloads.

The ArcSight Content AUP feature enables you to apply an AUP file to applicable connector destinations that you are managing. Only the event categorization information can be applied to the connectors using this feature.

You can maintain a number of Content AUP files in the Content AUP repository. When an AUP file with a version number higher than the ones already in the repository is loaded, it is automatically pushed out to the connector destinations being managed. However, these connectors or connector destinations are skipped:

- Connectors that are unavailable at the time of the AUP file push
- Connectors whose current version does not fall in the range of versions that the Content AUP supports
- The ESM destination on a connector
- All destinations of a connector that have an ESM destination with the AUP Master flag set to Yes

Also, when a new connector is added, the highest number Content AUP is pushed automatically to its destinations.

Applying a New Content AUP

You can add a new content AUP file to the repository and push it automatically to all applicable managed nodes.

To apply a new Content AUP:

1. Download the new Content AUP version from the support site at <http://softwaresupport.hpe.com/> to the computer that you use to connect to the browser-based interface.
2. From the computer to which you downloaded the AUP file, log in to the browser-based interface.
3. Click **Administration > Repositories**.
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository and push it automatically to all applicable connectors, or **Cancel** to quit.


You can verify the current Content AUP version on a connector by performing either of these steps:

- Run the `GetStatus` command on the node destination and check that the value for `aup [acp].version` is the same as the AUP version you applied. For information about running a command on a connector destination, see "[Sending a Command to a Connector](#)" on page 131.
- hover over a host name to see the AUP version applied to all destinations of that connector.

Applying an Older Content AUP

If you need to apply an older Content AUP from the Content AUP repository, delete all versions newer than the one you want to apply in the repository. The latest version (of the remaining AUP files) is pushed automatically to all applicable connectors.

To delete a Content AUP from the Content AUP repository:

1. Click **Administration > Repositories**.
2. Click **Content AUP** from the left panel.
3. Locate the AUP file that you want to delete and click the associated  icon. Repeat for multiple files.

Emergency Restore

The Emergency Restore can be used to restore a severely damaged local container on an appliance. This feature is supported only for containers on the localhost, for the hardware appliance version of ArcSight Management Center

ArcSight recommends that you use this process only when a container is severely damaged and is no longer available. The Emergency Restore process deletes all information about that container and renders it empty. The connector is restored to the AUP version that you select.

To perform an emergency restore:

1. Click **System Admin > Repositories**.
2. In the navigation panel, click **Emergency Restore**.
3. Follow the instructions in the wizard.
4. Re-import the SSL certificate for the container.

User-Defined Repositories

A *user-defined repository* is a user-named collection of settings that control upload and download of particular files from connectors to the repository. Each repository uses a specified path, relative to `$ARCSIGHT_HOME/user/agent`, for files to be uploaded or downloaded. ArcSight connectors use a standard directory structure, so map files, for example, are always found in `$ARCSIGHT_HOME/user/agent`, (that is, the root directory, `$ARCSIGHT_HOME`, of the installation path) in a folder called `map/`.

After they are created, user-defined repositories are listed on the left-side menu, under the **New Repository** heading, and appear with the user-specified display name.

User-defined repositories should be grouped by file type and purpose, such as log files, certificate files, or map files. Each user-defined repository has a name, a display name, and an item display name, which are described under the repository **Settings** tab.

Files viewed in a user-defined repository can be bulk processed with specified hosts and can be exchanged with the user's browser host.

Creating a User-Defined Repository

You can create a new repository at any time.

The repository requires correct directory paths. Your file will be applied to the wrong directory if the entered path contains errors, such as extra spaces or incorrect spellings. You can verify your directory paths by accessing the `Directory.txt` file, which lists the directory structure for every entered path. View the `Directory.txt` file by accessing your container logs and finding the `Directory.txt` file.

To create a new user-defined repository:

1. Click **Administration > Repositories**.
2. Click **New Repository** under the **Repositories** section in the left panel.

3. For the new repository, enter the parameters listed in the following table.

Parameter	Description
Name	A unique name for the repository, typically based on the type of files it contains.
Display Name	The name that will be displayed on the left-side menu and for tabs: Process <i>names</i> , View <i>names</i> , Settings for <i>names</i> . Typically plural.
Item Display Name	The name used to describe a single item.
Recursive	Check to include sub-folders.
Sort Priority	-1 by default
Restart Connector Process	Check to restart the connector process after file operations.
Filename Prefix	An identifying word that is included in the names of retrieved files. For example, map files are identified by Map in the file name: localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip
Relative path (Download)	The path for download, relative to \$ARCSIGHT_HOME, for example, user/agent/map or user/agent/flexagent. Leave this field blank to specify files in \$ARCSIGHT_HOME. Note: The relative path is used for download only.
Include Regular Expression	A description of filenames to include. Use .* to specify all files. The following example selects properties files that consist of map. followed by one or more digits, followed by .properties: map\[0-9]+\..properties\$
Exclude Regular Expression	A description of filenames to exclude. The following example excludes all files with a certain prefix or in the agentdata folder. (agentdata/ cwsapi_fileset_).*
Delete Before Upload	Check to delete earlier copies before upload. CAUTION: If you check Delete Before Upload and do not specify a Relative path (Upload), all files and folders in current/user/agent will be deleted.
Delete Groups	Whether to delete folders recursively in \$ARCSIGHT_HOME/user/agent/map directory.
Relative path (Upload)	The path for upload, relative to \$ARCSIGHT_HOME/current/user/agent/flexagent/<connectorname>
Delete Relative Path	Whether the directory specified in Relative Path (Upload) and its contents should be removed when a file is uploaded from the repository.
Delete Include Regular Expression	Typically the same as the Include Regular Expression.
Delete Exclude Regular Expression	Typically the same as the Exclude Regular Expression.

4. Click **Save** at the bottom of the page.

The new repository displays under the **New Repository** heading in the left-side window panel.

Retrieving Container Files

The **Retrieve Container Files** button copies a file from one or more containers to a repository. The specific files that are retrieved depend on the settings of the repository.

To retrieve a container file:

1. Click **Administration > Repositories**.
2. In the left panel, under **Repositories**, click the name of the repository to which you want to copy connector files.
3. Click **Retrieve Container Files** in the management panel.
4. Follow the instructions in the Retrieve Container Files wizard.

Uploading Files to a Repository

To upload files to a repository:

1. Click **Administration > Repositories**.
2. In the lower left panel (under **Repositories**), click the name of the repository to which you want to upload files.
3. Click **Upload To Repository** from the management panel.
4. Follow the instructions in the Repository File Creation wizard. Select **Individual files** to create a ZIP file with appropriate path information.

Caution: Be sure **not** to change the default sub-folder name `lib` in the **Enter the sub folder where the files will be uploaded** page of the Repository File Creation wizard.

Deleting a User-Defined Repository

To delete a user-defined repository:

1. Click **Administration > Repositories**.
2. From the left panel, click the name of the repository you want to delete.
3. Click **Remove Repository** from the management panel.

Updating Repository Settings.


To update the settings of a user-defined repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository whose settings you want to update.
3. Click the **Settings for Repository_Name** tab from the management panel.
4. Update the settings.
5. Click **Save** at the bottom of the page.

Managing Files in a Repository

Retrieving a File from the Repository

To retrieve a file from the repository:

1. Click **Administration > Repositories**.
2. From the left panel, click the name of the repository in which the file exists.
3. Click  from the management panel for the file that you want to retrieve.
4. Follow the file download instructions to copy the file to your local computer.


Uploading a File from the Repository

To upload a file from the repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click **Upload to Repository** for the file that you want to upload.
4. Follow the Upload Container Files wizard instructions to upload the file to the containers of your choice.
5. Verify that the file was uploaded correctly:
 - If you have SSH access to the connectors, connect to them and check the file structure.
 - Obtain the connector logs and check the contents of the `Directory.txt` file for each connector.

Removing a File from the Repository

To remove a file from the repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click  for the file that you want to delete.

Pre-Defined Repositories

You can define repositories for any connector-related files. The following repositories are pre-defined:

- **Backup Files:** connector cloning (see "[Backup Files](#)" on page 231).
- **Map Files:** enrich event data
- **Parser Overrides:** customize the parser (see "[Adding Parser Overrides](#)" on page 232)
- **FlexConnector Files:** user-designed connector deployment
- **Connector Properties:** agent.properties; subset of cloning
- **JDBC Drivers:** database connectors

To view the settings for a pre-defined repository, click the name of the repository and then click the **Settings** tab in the management panel. Settings for a pre-defined repository are read-only.

Settings for Backup Files

Backup File Default Settings

Name	Default Setting
Name	backup
Display Name	Backup Files
Item Display Name	Backup File
Recursive	Selected (Yes)
Sort Priority	0
Restart Connector Process	Selected (Yes)
Filename Prefix	ConnectorBackup
Download Relative Path	
Download Include regular expression	

Backup File Default Settings, continued

Name	Default Setting
Download Exclude regular expression	(agentdata/lcwsapi_fileset_).*
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	
Delete Include regular expression	
Delete Exclude regular expression	(agentdata/lcwsapi_fileset_).*

Settings for Map Files

This table lists the default settings for map files.

Map File Settings

Name	Default Setting
Name	map
Display Name	Map Files
Item Display Name	Map File
Recursive	Deselected (No)
Sort Priority	5
Restart Connector Process	Deselected (No)
Filename Prefix	Map
Download Relative Path	map
Download Include regular expression	map\[0-9]+\properties
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	map
Delete Include regular expression	map\[0-9]+\properties
Delete Exclude regular expression	

Settings for Parser Overrides

This table lists the default settings for parser overrides.

Parser Override Settings

Name	Default Setting
Name	parseroverrides
Display Name	Parser Overrides
Item Display Name	Parser Override
Recursive	Selected (Yes)
Sort Priority	10
Restart Connector Process	Selected (Yes)
Filename Prefix	Parsers
Download Relative Path	fcp
Download Include regular expression	*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	fcp
Delete Include regular expression	*
Delete Exclude regular expression	

Settings for FlexConnector Files

This table lists the default settings for FlexConnector files.

FlexConnector Settings

Name	Default Setting
Name	flexconnectors
Display Name	FlexConnector Files
Item Display Name	FlexConnector File
Recursive	Selected (Yes)
Sort Priority	15

FlexConnector Settings, continued

Name	Default Setting
Restart Connector Process	Selected (Yes)
Filename Prefix	FlexConnector
Download Relative Path	flexagent
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	flexagent
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for Connector Properties

Connector Default Property Settings

Name	Default Setting
Name	connectorproperties
Display Name	Connector Properties
Item Display Name	Connector Property File
Recursive	Deselected (No)
Sort Priority	20
Restart Connector Process	Selected (Yes)
Filename Prefix	ConnectorProperties
Download Relative Path	
Download Include regular expression	agent\.*
Download Exclude regular expression	
Delete before upload	Deselected (No)
Delete groups	Deselected (No)
Upload Relative Path	

Connector Default Property Settings, continued

Name	Default Setting
Delete Relative Path	
Delete Include regular expression	agent\.*
Delete Exclude regular expression	

Settings for JDBC Drivers

This table lists the default settings for JDBC Drivers.

JDBC Driver Settings

Name	Default Setting
Name	jdbcdrivers
Display Name	JDBC Drivers
Item Display Name	Connector JDBC Driver File
Recursive	Deselected (No)
Sort Priority	25
Restart Connector Process	Selected (Yes)
Filename Prefix	
Download Relative Path	lib
Download Include regular expression	
Download Exclude regular expression	
Delete before upload	Deselected (No)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	lib
Delete Include regular expression	
Delete Exclude regular expression	

Backup Files

Using the **Backup Files** repository, you can quickly copy a container to other containers. As a result, all connectors in the source container are copied to the destination container. This process is called *cloning* a container configuration. You can clone a container to several containers at once. The contents of the source container replace the existing contents of the destination container.

Caution: Containers on ArcSight Management Center are pre-installed with the latest connector release. Do not clone older, software-based connectors (such as build 4.0.8.4964) to containers with newer connector builds (such as 4.0.8.4976 or later).

Cloning a connector using the Backup repository only works if the connector version numbers are the same.

To clone a container using the Backup Files repository:

1. Click **Node Management > View All Nodes**.
2. Click the **Containers** tab to list the containers and determine the source and destination for cloning.
3. Click **Administration > Repositories**.
4. Click **Backup Files** under the **Repositories** section in the management panel.
5. If the backup file that you need to use for cloning exists in the repository, go to the next step. Otherwise, follow the instructions in ["Retrieving a File from the Repository" on page 226](#) to retrieve the container's backup file to the Backup repository.

The retrieved file is named in `<connector name> ConnectorBackup <date>` format.

6. Follow the instructions in ["Uploading a File from the Repository" on page 226](#) to upload the backup file to one or more containers.

The destination containers are unavailable while the backup file is applied and the connectors are restarted.

Note: The backup file does not include the container certificates. You have to re-apply the certificates to the container after you upload the backup file.

After applying the certificates, check the status of the destination container to make sure it is available.

Adding Parser Overrides

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added.

To use parser overrides, you need to:

- Upload a parser override file to the **Parser Overrides** repository.
- Download the parser override file to the container that contains the connector that will use the parser override.

Follow the steps below.

To upload a parser override file:

1. Click **Administration > Repositories**.
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. On the **Parser Overrides** tab, click the **Upload To Repository** button.
4. Follow the wizard to upload the file. When prompted by the wizard, make sure you:
 - Select the **Individual Files** option from the **Select the type of file that you want to upload** field.
 - Add a slash (/) after fcp before adding the folder name in the **Enter the sub folder where the files will be uploaded** field. For example, fcp/multisqlserver_audit_db.When upload is complete, the parser override file is listed in the table on the Parser Overrides tab.

To download the parser override file to a container:

1. Click **Administration > Repositories**.
 2. Click **Parser Overrides** under the **Repositories** section in the management panel.
 3. In the table on the **Parser Overrides** tab, locate the parser override file you want to download and click the up arrow next to the file.
 4. Follow the wizard to select the container to which you want to add the parser overrides.
- When the wizard completes, the parser overrides are deployed in the selected container.

Note: You can download a parser override file from ArcExchange. For more information, refer to ["Sharing Connectors in ArcExchange" on page 138](#).

To verify that the parser override has been applied successfully, issue a Get Status command to the connector. See ["Sending a Command to a Connector" on page 131](#). In the report that appears, check for the line starting with the text ContentInputStreamOverrides.

Chapter 13: System Administration

This chapter describes the System Administration tools that enable you to create and manage users and user groups, and to configure SMTP and other system settings.network, storage, and security settings for your system.

This chapter includes information on the following areas of system administration:

• System	234
• Logs	253
• Storage	255
• Security	260
• Users/Groups on ArcMC	267

System

From the System tab, you can configure system specific settings such as network settings (if applicable) and SMTP.

System Reboot

To reboot or shutdown your system:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **System Reboot** in the **System** section.
3. Select from the following options:

Button	Description
Reboot	Your system reboots in about 60 seconds. The reboot process normally takes 5-10 minutes, during which time the system is unavailable.
Reboot in 5 Minutes	Your system reboots after a 5-minute delay. The reboot process normally takes 5-10 minutes, during which time the system is unavailable.
Shutdown	Automatically shuts down (powers off) the system.

4.

Note: Each of the above actions can be cancelled. “Reboot” and “Shutdown” allow for cancellation within **60 seconds**. “Reboot in 5 Minutes” can be cancelled within **300 seconds**.

5. Click **Reboot**, **Reboot in 5 Minutes**, or **Shutdown** to execute the chosen action.



Network

System DNS

The **System DNS** tab allows you to edit the DNS settings and to add DNS search domains.

To change DNS settings:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **System DNS** tab, enter new values for the IP address of the primary and secondary DNS servers, or edit the list of search domains.

To add a new domain, click the  icon. To remove a domain, click the  icon. To change the search order of domains, select a domain name, and click the up or down arrow until the domain is in the desired position.

4. Click **Save**.
5. Click **Restart Network Service** to put the changes into effect.

Hosts

The **Hosts** tab allows direct editing of your system's `/etc/hosts` file. You can enter data in the System Hosts text box or import it from a local file.

To change the Hosts information:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section, and then click the **Hosts** tab.
3. In the **System Hosts** text box, enter hosts information (one host per line) in this format:

<IP Address> <hostname1> <hostname2> <hostname3>

To import information from a file, click **Import from Local File**, and locate the text file on the computer from which you are accessing your system.

4. Click **Save**.

NICs

The **NICs** tab enables you to set the IP addresses for the network interface cards (NICs) on your system. Additionally, you can configure the hostname and default gateway for your system.

To set or change the NICs settings:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **NICs** tab, enter the following settings. To edit the IP address , subnet mask, or speed/duplex of an NIC, select the NIC and click **Edit** above the NIC Name list.

Setting	Description
Default Gateway	The IP address of the default gateway.
Hostname	<p>The network host name for this system. Make sure that your DNS can resolve the host name you specify to your system's IP address . Performance is significantly affected if DNS cannot resolve the host name.</p> <p>This name must be identical to the domain specified in the Certificate Signing Request, described in "Generating a Certificate Signing Request (CSR)" on page 262.</p> <p>Note: If you previously used a self-signed or CA-signed certificate on this system and are now changing its host name, you must regenerate a new self-signed certificate or CSR. Once obtained, the new certificate should be uploaded to ensure that the connectors which communicate with your system are able to validate the host name. For more information about generating a CSR, see "Generating a Certificate Signing Request (CSR)" on page 262.</p>
Automatically route outbound packets (interface homing)	<p>When this option is enabled (checked box), the response packets are sent back on the same system interface on which the request packets had arrived. Enabling this option can improve performance as the routing decisions do not need to be made (using the default gateway information and static routes) to send packets out from your system. If you have static routes configured, they are ignored when this feature is enabled.</p> <p>When this feature is disabled (unchecked box), the static routes (if configured) are used to determine the interface through which the response packets should leave your system.</p> <p>If you configure only one network interface, this setting does not provide any additional benefit.</p>

Setting	Description
IP Address	<p>The IP address for each network interface card (NICs) in your system.</p> <p>Add NIC Alias</p> <p>You can create an alias for any listed NIC. To do so:</p> <ol style="list-style-type: none">Highlight the NIC for which you want to create an alias.Click Add.Create an alternative IP address for the alias.Click Save. <p>You can identify the alias from its original by an appended colon alongside a digit indicating the number of aliases you have created on a particular NIC.</p> <p>Notes:</p> <ul style="list-style-type: none">You cannot alter the speed of an IP alias.You can create as many aliases as you choose.
Subnet Mask	The subnet mask associated with the IP address you entered for an NIC.
Speed/Duplex	<p>Choose a speed and duplex mode, or let your system determine the network speed automatically:</p> <p>Auto (recommended)</p> <p>10 Mbps - Half Duplex</p> <p>10 Mbps - Full Duplex</p> <p>100 Mbps - Half Duplex</p> <p>100 Mbps - Full Duplex</p> <p>1 Gbps - Full Duplex</p>

- Click **Save**.
- Click **Restart Network Service** to put the changes into effect.

Static Routes

You can specify static routes for the NICs on your system.

To add, edit, or delete a static route:

- Click **Setup > System Admin** from the top-level menu bar.
- Click **Network** in the **System** section.
- In the **Static Routes** tab:
 - To add a new static route, click **Add**.
 - To edit or delete an existing route, select the route first, then click **Edit** or **Delete**.

When adding or editing a static route, you need to configure these settings.

Setting	Description
Type	Whether the static route is to a Network or a Host
Destination	The IP address for the static route destination
Subnet Mask	The subnet mask if you specify a network as the destination
Gateway	The IP address of the gateway for the route

4. Click **Save**.

Time/NTP

The **Time/NTP** tab enables you to configure system time, date, local timezone, and NTP servers. HPE Security strongly recommends using an NTP server instead of manually configuring the time and date on your system.

To set or change the system time, date, or time zone manually:

Caution: If you manually set the date and time settings and are also using an NTP service, the date and time entered manually cannot be more than 16 minutes ahead of or behind the time that the NTP server is providing. If the manually entered time is more than 16 minutes different from the NTP server time, then the NTP service will fail to start.



1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **Time/NTP** tab, configure these settings.

Setting	Description
Current Time Zone	<p>The time zones appropriate to your system's location. To change this setting, click Change Time Zone...</p> <p>Local times zones follow the Daylight Savings Time (DST) rules for that area. Greenwich Mean Time (GMT) + and - time zones are DST agnostic.</p> <p>For example, the America/Los Angeles time zone varies by an hour compared with GMT when DST goes into and out of effect.</p> <ul style="list-style-type: none">• Pacific Standard Time (PST) = GMT-8• Pacific Daylight Time (PDT) = GMT-7
Current Time	<p>The current date and time at the system's location. To change this setting, click Change Date/Time... and then enter the current date and time.</p>

4. The Time Zone change requires that you reboot the appliance. However, the Current Time change takes effect immediately.

To configure your system as an NTP server or for using an NTP server for your system:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. Click the **Time/NTP** tab.
4. Under **NTP Servers**, configure these settings.

To add a new NTP server, click the  icon. To remove a server, click the  icon. To change the order in which the NTP servers should be used, select a server and click the up or down arrow until the NTP server is in the desired position.

Setting	Description
Enable as an NTP server	Check this setting if this system should be used as an NTP server.
NTP Servers	<p>Enter the host name of an NTP server. For example, time.nist.gov.</p> <p>HPE Security recommends using at least two NTP servers to ensure precise time on your system. To enter multiple NTP servers, type one server name per line.</p> <p>Notes:</p> <ul style="list-style-type: none">• An ArcSight system can serve as an NTP server for any other ArcSight system.• If System A serves as an NTP server for System B, System B needs to list System A in its NTP Servers list.• Use the Test Servers button to verify the status of the servers entered into the NTP Servers box.

5. Click **Save**.

Tip: You may need to scroll down to view the **Save** button and **Restart NTP Service**.

6. Click **Restart NTP Service** to put the changes into effect.

SMTP

Your system uses the Simple Mail Transfer Protocol (SMTP) setting to send email notifications such as alerts and password reset emails.

To add or change SMTP settings:

1. Click **Administration > Setup > System Admin**.
2. Click **SMTP** in the **System** section and enter these settings.

Setting	Description
Primary SMTP Server	The IP address or hostname of the SMTP server that will process outgoing email.
Backup SMTP Server	The IP address or hostname of the SMTP server that will process outgoing email in case the primary SMTP server is unavailable.
Outgoing Email Address	The email address that will appear in the From: field of outbound email.

3. Click **Save**.

License & Update

This page displays license information, the version of the components, and the elapsed time since ArcSight Management Center was last rebooted/restarted. From here, you can update ArcSight Management Center and apply a license.

Updating the Appliance

To update your ArcSight Management Center:

1. Download the update file from the HPE Support site at <http://softwaresupport.hpe.com> to the computer from which you can connect to ArcSight Management Center.
2. Click **Administration > Setup > System Admin** from the top-level menu bar.
3. Click **License & Update** in the **System** section.
4. Click **Browse** to locate the file.
5. Click **Upload Update**.

An "Update In Progress" page displays the update progress.

6. Once the update has completed, the Update Results page displays the update result (success/failure) and whether the update requires a reboot. If the update requires a reboot, the ArcSight Management Center reboots automatically.

Updating the License File

To update a license file:

1. Download the license update file from the HPE Support site at <http://softwaresupport.hpe.com> to the computer from which you can connect to the ArcSight Management Center with your browser.
2. From the computer to which you downloaded the license update file, log in to the ArcSight Management Center user interface using an account with administrator (upgrade) privileges.

3. Click **Administration > System Admin.**
4. Click **License & Update** in the **System** section.
5. Browse to the license file you downloaded earlier, and click **Upload Update.**

An “Update In Progress” page displays the update progress.


After the update has completed, the Update Results page displays the update result (success/failure). If you are only installing or updating a license, a reboot/restart is not required.

Note: After updating the license file, refresh the browser to see the current list of features enabled.

Process Status

The **Process Status** page lists all processes related to your system and enables you to view the details of those processes and start, stop, or restart them.

To view the Process Status page:

1. Click **Administration > Setup > System Admin.**
2. In **System** section, click **Process Status.**
3. To view the details of a process, click the  icon to the left of the process name.
4. To start, stop, or restart a process, select the process and click **Start**, **Stop**, or **Restart** at the top of the **Processes** list.

System Settings

If you did not select ArcSight Management Center to start as service during the installation process, you can do so using the **System Settings** page.

To configure ArcSight Management Center to start as a service:

1. Click **Administration > Setup > System Admin.**
2. Click **System Settings** in the left panel.
3. From under **Service Settings**, choose the appropriate option:
 - Start as a Service
 - Do not start as a Service
4. Click **Save.**

SNMP

SNMP (Simple Network Management Protocol) can be used to monitor the health of your appliance. ArcMC supports versions 2c and 3 of SNMP.

SNMP Configuration

You can configure SNMP polling and notifications. If SNMP polling is configured, a manager station can query the SNMP agent residing on the ArcMC. The information retrieved provides detailed information at the hardware and operating system level.

To configure SNMP polling:

1. In the main menu bar, click **Administration > Setup > System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMP Poll Configuration** tab, ensure **Enabled** is selected.
 - For **Port**, the default is 161 but can be any available port. Ensure the specified port is open on your firewall.
 - For **SNMP version**, select V2c or V3.
 - If V2c is selected, specify a community string of between 6 and 128 alphanumeric, underscore, and dash characters.
 - If V3 is selected, specify the username (alphanumeric lower-case string of 4-16 characters, which must begin with an alphabetic characters and may include underscores), authentication protocol, authentication passphrase (4 to 256 characters), privacy protocol, and privacy passphrase (4 to 256 characters).
4. Click **Save**.

If an SNMP destination is configured, ArcMC can send notifications for a limited set of events (see ["Viewing SNMP System Information" on the next page](#))

SNMP notifications differ from those sent by connectors, which are for a generic ArcSight event. The notifications listed here are specific to a single event, making them easier for understanding by a network management system like HPE NMMi.

To configure the destination for SNMP notifications:

1. In the main menu bar, click **Administration > System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMP Destination** tab, ensure **Enabled** is selected. Then, enter values for the other parameters that match your existing NMS SNMP settings.

- For Port, enter 162. (Note: Specifying a non-default port may cause a brief delay. Give the process time to complete.)
- For SNMP version, select V2c or V3, and then enter values for the prompted settings.

4. Click **Save**

Viewing SNMP System Information

SNMP notifications are viewable in any MIB browser. The following SNMP notifications are supported:

- **Application**
 - Login attempt failed
 - Password change attempt failed
 - User account locked
 - Reboot command launched
 - Manual backup failed
 - Enable FIPS mode successful
 - Disable FIPS mode successful
 - Enable FIPS mode failed
 - Disable FIPS mode failed
- **Platform**
 - CPU Usage
 - Memory Usage
 - Disk Almost Full
 - Fan Failure
 - Power Supply Failure
 - Temperature Out of Range
 - Ethernet Link Down

To view system notifications in an MIB browser:

On your appliance:

You can download the ArcSight MIB file and other standard Net-SNMP MIB files using the following URLs:

- https://<system_name_or_ip>/platform-service/ARCSIGHT-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/DISMAN-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/HOST-RESOURCES-MIB.txt

- https://<system_name_or_ip>/platform-service/IF-MIB.txt
- https://<system_name_or_ip>/platform-service/UCD-SNMP-MIB.txt

On any standard MIB browser:

1. Load the MIB.
2. Specify the address and port number of the SNMP agent—your appliance, in this case.
3. Configure the community string that is set on your appliance.
4. Initiate the snmp WALK operation of the OID from the browser.
5. Once the SNMP data is returned, interpret it based on the information described earlier in this section.

MIB Contents

Notifications are written to the following modules of the MIB file:

Module	Notification Types
HOST-RESOURCES-MIB	Standard hardware parameters.
IF-MIB	Objects for network interfaces.
IP-MIB	IP and ICMP implementations.
DISMAN-EVENT-MIB	Event triggers and actions for standard network management.

SSH Access to the Appliance

You can enable SSH access to the appliance. By default, SSH access to your appliance is disabled. For best security, it is strongly recommended that you enable SSH access only when necessary, such as for troubleshooting purposes.

Caution: By default, you are not prompted for a challenge/response when logging in using SSH. (This represents a change from the configuration of Connector Appliance.)

As a result, it is imperative that you change the default password for the “root” account on the ArcSight Management Center Appliance to a new, strong password as soon as possible. To obtain the default root password, contact ArcSight Customer Support.

Enablement options include:

- *Disabled*: No SSH access is enabled. This is the default value.
- *Enabled*: SSH access is always enabled.
- *Enabled, only for 8 hours*: SSH access is disabled automatically eight hours after it was enabled.
- *Enabled, only during startup/reboot*: SSH access is enabled during the time the appliance reboots and is starting up. It is disabled once all processes on the appliance are up and running. This option provides a minimal period of SSH access for situations such as when the appliance does not start successfully after a reboot.

Note: Even if SSH is disabled on your appliance, you can access its console if you have it set up for remote access using the HPE Security ProLiant Integrated Lights-Out (iLO) Advanced remote management card.

Enabling or Disabling SSH Access

To enable or disable SSH access to your appliance:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **SSH** in the **System** section.
3. Select an SSH enablement option.
4. Confirm the option. The change takes place immediately.

Connecting to Your Appliance Using SSH

Once you have enabled SSH access, follow these steps to connect to it using SSH:

1. Connect to the appliance as “root” using an SSH client.
2. When prompted to enter a password, enter a password and press **Enter**.

On an upgraded G9 C6600 appliance, SSH connectivity will be blocked after upgrade. To unblock SSH, disable SSH and then re-enable.

Diagnostic Tools

ArcSight Management Center provides several diagnostic tools that help you set up, manage, and troubleshoot your appliance. You can run these diagnostics on the local appliance only. To run a diagnostic tool on a remote container, refer to ["Running Diagnostics on a Container" on page 117](#).

To access the diagnostic tools:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **Diagnostic Tools** in the **System** section in the left panel to open the Diagnostic Tools page.
3. From the **Tool** drop-down box, select the tool you want to use.
4. Enter the required parameters for the tool you selected and click **Run** (click **Edit** for the Edit text file tool).

Each tool and the parameters and buttons available is described below.

Display I/O Statistics

Use the Display I/O Statistics tool to monitor input/output statistics for devices, partitions, and network file systems on the appliance. This tool is equivalent to the Linux command `iostat`.

This tool uses the parameters described below:

Parameter	Description
Match Expression	Type an expression to display only lines in the file that match that expression. Linux regular expressions are supported. Note: The expression is case sensitive.
Exclude Expression	Type an expression to exclude lines that match that expression from the display. Linux regular expressions are supported. Note: The expression is case sensitive.

Display file

Use Display file to display the contents of a file. This tool is equivalent to the Linux command `cat`.

This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to display.
File	Displays a list of files for the type selected in the Category field (described above). Select the file you want to display from the list. Note: Appliance models Cx400 do not have any boot log files; selecting Boot Log from the File list displays an empty pop-up window.
Match Expression	Type an expression to display only lines in the file that match that expression. Linux regular expressions are supported. Note: The expression is case sensitive.

Parameter/Button	Description
Exclude Expression	<p>Type an expression to exclude lines that match that expression from the display. Linux regular expressions are supported.</p> <p>Note: The expression is case sensitive.</p>
Display	<p>You can limit the number of lines you want to display.</p> <ul style="list-style-type: none"> • Select Beginning of file to limit the display to the number of lines specified in the Number of Lines field (described below) starting from the top of the file. • Select End of file to limit the display to the number of lines specified in the Number of Lines field (described below) starting from the bottom of the file. <p>Note: If you select Beginning of file or End of file, you also need to specify a value in the Number of Lines field, described below.</p> <p>To display all the lines in the file, leave both the Display and the Number of Lines field empty.</p>
Number of Lines	<p>Specify the number of lines you want to display from the beginning or end of the file.</p> <p>If you enter an expression to match or exclude, the display contains or omits the first (if you select Beginning of file) or last (if you select End of file) number of occurrences of that expression. For example, if you enter TCP in the Exclude Expression field, then select Beginning of file from the Display drop-down, and enter 10 in the Number of Lines field, the display contains the first 10 occurrences of the expression TCP found starting from the beginning of the file.</p> <p>Note: To display all the lines in the file, leave this field and the Display field (described above) empty.</p>
Run	<p>Click this button to display the contents of the selected file. The file contents display in a pop-up window.</p>

Display network connections

Use Display network connections to review your network connections and transport protocol statistics. The status information can indicate areas where a protocol is having a problem.

This tool is equivalent to the Linux command `netstat -pn [-t] [-u] [-w] [a] [-l] [-c]`.

This tool uses the parameters described below:

Parameter/Button	Description
Protocol	Leave this field empty to display statistics for all transport protocols or select from these options: <ul style="list-style-type: none">• RAW only displays raw IP protocol statistics. This option is equivalent to the <code>netstat</code> Linux command option <code>-w</code>.• TCP only displays TCP protocol statistics. This option is equivalent to the <code>netstat</code> Linux command option <code>-t</code>.• UDP only displays UDP protocol statistics. This option is equivalent to the <code>netstat</code> Linux command option <code>-u</code>.
Connection	Leave this field empty to display information for all non-listening connections or select from these options: <ul style="list-style-type: none">• All connections displays information for all current connections. This option is equivalent to the <code>netstat</code> Linux command option <code>-a</code>.• Listening connections displays information for listening connections only. This option is equivalent to the <code>netstat</code> Linux command option <code>-l</code>.
Mode	Select Run Continuously to poll the network status continuously every five minutes. This option is equivalent to the <code>netstat</code> Linux command option <code>-c</code> . When Run Continuously is not selected, the network status is polled once.
Match Expression	Enter an expression to display only lines that match that expression in the output. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude lines that match that expression from the output. Linux regular expressions are supported.
Run	Click this button to display the network connection information. The information displays in a pop-up window.

Display network interface details

Use Display network interface details to display the status of a currently active interface on the appliance. This tool is equivalent to the Linux command `ifconfig`.

This tool uses the parameters described below:

Parameter/Button	Description
Interface	Select the network interface on the appliance whose status you want to display. Note: If you leave this field empty, the status of all active network interfaces display.
Run	Click this button to display the status of the selected network interface. The status displays in a pop-up window.

Display network traffic

Use Display network traffic to monitor packets that are transmitted and received on the network. This tool is equivalent to the Linux command `tcpdump`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to monitor.
Match Expression	Enter an expression to show only network traffic that matches that expression in the display; For example, if you specify the expression echo, only network traffic from the specified host that includes the expression echo is displayed. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude network traffic that matches that expression from the display; For example, if you specify the expression echo, all traffic except traffic that contains echo will be displayed. Linux regular expressions are supported.
Run	Click this button to display network traffic between the appliance and the specified host. The information displays in a pop-up window.

Display process summary

Use Display process summary to show a list of the currently running processes and see how long they have been running. This tool is equivalent to the Linux command `top -b -n 1`.

This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Enter an expression to display only processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of currently running processes. The list displays in a pop-up window.

Display routing table

Use Display routing table to see the routes through which traffic flows from the appliance. This tool is equivalent to the Linux command `ip route`.

This tool uses the parameters described below:

Parameter/Button	Description
Destination Host	<ul style="list-style-type: none">• Leave this field empty to see the entire IP routing table.• Specify the IP address or hostname of a host to see IP routing information from the appliance to that host.
Run	Click this button to obtain the routing table. The routing table displays in a pop-up window.

Edit text file

Use Edit text file to edit files on the appliance. This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the type selected in the Category field (described above). Select the file you want to edit.
Edit	Click this button to display the file for editing. After editing the file, click Save or Revert .
Save	Click this button to save the edits you make to the file.
Revert	Click this button to cancel the edits you make to the file. After clicking Revert , click Save to save the reverted text.

List directory

Use List directory to display the contents of a directory on the appliance. This tool is equivalent to the Linux command `ls -al`.

This tool uses the parameters described below:

Parameter/Button	Description
Directory	Specify the directory whose contents you want to display. For example: <code>/opt/arcsight/appliance</code>
Run	Click this button to display the directory list. The list displays in a pop-up window.

List open files

Use List open files to display a list of files in use. This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Enter an expression to display only the top processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of the top processes. The list displays in a pop-up window.

List processes

Use List processes to display the top CPU processes that are currently running together with memory and resource information. This tool is equivalent to the Linux command `ps -ef`.

This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Enter an expression to display only the top processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of the top processes. The list displays in a pop-up window.

Ping host

Use Ping host to test if a particular host is reachable across an IP network and to measure the round-trip time for packets sent from the appliance to the host. This tool is equivalent to the Linux command `ping`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to ping.
Run	Click this button to ping the specified host. The ping results display in a pop-up window.

Resolve hostname or IP Address

Use Resolve hostname to look up a hostname in the Domain Name Server and convert it to an IP address. This tool is equivalent to the Linux command `host`.

This tool uses the parameters described below:

Parameter/Button	Description
Hostname	Specify the hostname you want to resolve to an IP address .
Run	Click this button to look up the hostname in the Domain Name Server. The result displays in a pop-up window.

Scan network ports

Use Scan network ports to scan a specific host on the network for open ports. This tool is equivalent to the Linux command `nmap [-p]`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose ports you want to scan.
Port Range	Optional. Specify a range of ports you want to scan. Separate port numbers in a range by a dash (-) and individual port numbers by a comma. For example, 80-90, 8080. If you do not provide a port range, all ports on the specified host are scanned. This option is equivalent to the <code>netstat</code> Linux command option <code>-p</code> .
Run	Click this button to start scanning ports on the specified host. The result displays in a pop-up window.

Send signal to container

Use Send signal to container to send a terminate command to a container. This tool is equivalent to the Linux command `kill -severity` (where *severity* is either `-15` or `-9`).

This tool uses the parameters described below:

Parameter/Button	Description
Severity	Select the severity of the terminate command you want to send to the container. You can select KILL (Linux <code>kill</code> command option <code>-9</code>) or TERM (Linux <code>kill</code> command option <code>-15</code>).
Container	Select the container to which you want to send the signal.
Run	Click this button to send the signal. The result displays in a pop-up window.

Tail file

Use Tail file to display the last ten lines of a system, application, or log file. This tool is equivalent to the Linux command `tail -f`.

This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the category selected in the Category field (described above). Select the file from which you want to display the last ten lines.
Match Expression	Enter an expression to display only lines that match that expression. Linux regular expressions are supported.
Exclude Expression	Enter an expression to exclude lines from the display that match that expression. Linux regular expressions are supported.
Run	Click this button to display the last ten lines of the file you selected. The lines display in a pop-up window.

Trace network route

Use Trace network route to display the specific network route between the appliance and a specified host. This tool is equivalent to the Linux command `tracert`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose route you want to trace.
Run	Click this button to display the network route. The information displays in a pop-up window.

Logs

Your system can generate audit logs at the application and platform levels. Use the Logs sub-menu to search audit logs and to configure audit forwarding so that the system can send audit events to a destination, such as ESM.

Audit Logs

Your system's audit logs are available for viewing. Audit logs, as Common Event Format (CEF) audit events, can be sent to ArcSight ESM directly for analysis and correlation. For information about forwarding audit events, see ["Configuring Audit Forwarding to a Specific Destination" on page 255](#).

Audit logs are retained permanently by ArcMC.

To view audit logs:

1. Click **Administration > System Admin.**
2. Click **Audit Logs** in the **Logs** section.
3. Select the date and time range for which you want to obtain the log.
4. (Optional) To refine the audit log search, specify a string in the **Description** field and a user name in the **User** field. When a string is specified, only logs whose **Description** field contains the string are displayed. Similarly, when a user is specified, only logs whose **User** field contains the username are displayed.
5. Click **Search**.

Configuring Audit Forwarding

To configure audit forwarding, you must install a single syslog connector in an ArcSight Management Center container. (The connector may be the only connector in the container.)

The procedure for configuring audit forwarding differs for Software ArcSight Management Center and ArcSight Management Center Appliance.

Note: If ArcSight Management Center has been installed by a root user, the syslog connector should also be configured under the root user.

If the installation was by a non-root user, the syslog connector should be configured under the non-root user.

For Software ArcSight Management Center

To configure audit forwarding for Software ArcSight Management Center:

1. Install the local Syslog Daemon connector to `/opt/arcsight/connector`.
2. Configure audit forwarding for the container that has the Syslog Daemon connector. Refer to ["Configuring Audit Forwarding to a Specific Destination" on the next page](#).
3. Click **System Admin** from the menu bar. In the navigation tree, select the newly-installed syslog connector and enable audit forwarding.

For ArcSight Management Center Appliance

To configure audit forwarding for ArcSight Management Center Appliance:

1. In the menu bar, click **Node Management**.
2. In the navigation tree, select the default location. Then, in the management panel, select the local


host.


3. Select the container in which to install the syslog connector.
4. Click **Add Connector** and choose *syslog* as the connector to be installed.
5. Configure audit forwarding for the container that has the Syslog Daemon connector. Refer to ["Configuring Audit Forwarding to a Specific Destination" below](#).
6. Click **System Admin** from the menu bar. In the navigation tree, select the newly-installed syslog connector and enable audit forwarding.

Configuring Audit Forwarding to a Specific Destination

You can forward audit and system health events to an ArcSight ESM destination for correlation and analysis, and to Logger for event collection.

To forward audit events to specific destinations:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Audit Forwarding** in the **Logs** section.
3. Select destinations from the **Available Destinations** list and click the right arrow icon () to move the selected destination to the **Selected Destinations** list.

You can select multiple destinations at the same time and move them, or you can move all available destinations by clicking the () icon.

4. Click **Save Settings**.

Note: Destinations will not be displayed in Software ArcSight Management Center.

Storage

Use the Storage sub-menu to add an NFS mount or a CIFS mount, or SAN (if applicable) and to view the status of the hard disk array (RAID) controller and specific system processes.

RAID Controller/Hard Disk SMART Data

You can view information about the RAID controller or hard disk SMART data in the General Controller Information screen. This information is not needed during normal system operations, but it can be helpful for diagnosing specific hardware issues. Due to the redundant nature of RAID storage, a single drive failure will not disable your system. Instead, performance degrades. Use this report to determine whether a performance issue is caused by a disk failure. Customer support can also use this information to diagnose problems.

To view the General Controller Information screen:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **RAID Controller** in the **Storage** section in the left panel.

Note: On some older models, the Hard Disk SMART Data menu item displays in the left pane instead of the RAID Controller menu item. Click **Hard Disk SMART Data** in the **Storage** section in the left pane to display diagnostic information from the hard drive.

- 3.
4. The information displayed depends on the hardware model of your system. Click the arrows to open and close the sections.

RAID Controller Configuration

RAID Controller Configuration

General Controller Information

Bus Interface: PCI
Slot: 0
Serial Number: 5001438011837E30
Cache Serial Number: PBCDH0CRHZT11S
RAID 6 (ADG) Status: Disabled
Controller Status: OK
Hardware Revision: C
Firmware Version: 3.52
Rebuild Priority: Medium
Expand Priority: Medium
Surface Scan Delay: 3 secs
Surface Scan Mode: Idle
Queue Depth: Automatic
Monitor and Performance Delay: 60 min
Elevator Sort: Enabled
Degraded Performance Optimization: Disabled
Inconsistency Repair Policy: Disabled
Wait for Cache Room: Disabled
Surface Analysis Inconsistency Notification: Disabled
Post Prompt Timeout: 15 secs
Cache Board Present: True
Cache Status: OK
Cache Ratio: 25% Read / 75% Write
Drive Write Cache: Disabled
Total Cache Size: 512 MB
Total Cache Memory Available: 400 MB
No-Battery Write Cache: Disabled
Cache Backup Power Source: Capacitors
Battery/Capacitor Count: 1
Battery/Capacitor Status: OK
SATA NCQ Supported: True

— **Logical Drive #1**

— **Disk #0**

— **Disk #1**

— **Disk #2**

FTP

ArcSight Management Center allows for the use of FTP and FTPS (FTP over SSL) as a method of delivering log files to the appliance. The default state for FTP and FTPS is **disabled**.

Blue Coat ProxySG appliances, in particular, support FTP and FTPS as a means of transferring files to ArcSight Management Center (For details on this and other methods, refer to the SmartConnector Configuration Guide for Blue Coat ProxySG).

FTPS

FTP can also be used over a secure channel, namely SSL. The use of **FTPS** requires that a certificate be generated on ArcSight Management Center. This certificate can be self-signed or signed by a certificate authority (CA). For detailed instructions on this option, see ["Using FTPS \(FTP over SSL\)" on page 259](#).

Models Supporting FTP

The following table lists the ArcSight Management Center models that support the use of FTP. It can also assist in determining the maximum directory size allowed for storing files received over these protocols.

Note: If the maximum directory size is exceeded, FTP is disabled and audit event platform:453, FTP service stopped is sent. Until the directory size is lowered, all FTP connections are denied.

Model Name	Maximum Directory Size (GB)
C1400	275
C3400	275
C3500	475
C5400	235
C5500	475
C6500	500
C6600	500

Enabling FTP

In order to use the FTP protocol, you need to enable it on the appliance and set a maximum directory size for the accumulated files.

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **FTP** under the **Storage** section.
3. From within **FTP Settings**, check the **Enable FTP** check box.
4. If your FTP client is behind a firewall and you need to limit the ports used for passive mode data transfer, check the **Restrict port range...** check box.

- **Port Range** allows you to set either an individual port (e.g., 12345) or a single port range (e.g., 20001-20010). Ensure any ports specified open on your firewall.

Note: When choosing a port or port range, choose a port that is unlikely to already be in use. If a chosen port is already in use, . For this FTP data transfers will fail. For this reason, HPE Security recommends using ports in the range of 10000 and above.

- The number of concurrent passive mode FTP clients is restricted to the number of ports specified. For example, if the specified range is 10 ports, then only 10 concurrent passive FTP clients can be transferring at the same time.

Tip: **Is FTP Running?** verifies (**Yes** or **No**) that your FTP server is running successfully.

5. Enter a maximum directory size.

- The maximum directory size cannot be greater than that allowed on your appliance model (see ["Models Supporting FTP" on the previous page](#)).
- If you change the maximum size, it must be greater than the value in the **Current Size** field.
- **Current Size** includes /opt/arcsight/incoming and all underlying subdirectories.
- If the maximum you have set is exceeded, FTP stops automatically.
- Once the file limitation is back within range, FTP automatically restarts.

6. Enter a password.

Caution: Anonymous FTP is not supported.

7. Click **Save**.

- Only file put operations are supported by the FTP server. There is no capability to retrieve data from the appliance.
- Data is processed faster and more efficiently when transferred in many small files instead of a few large files.

Adding a Subdirectory

Based on naming convention, incoming log files from different devices can potentially conflict within the same directory. To prevent this, you can create subdirectories to separate them. This window also shows the current size of the subdirectory.

Tip: Creating subdirectories is a good practice, as it allows you to verify how much space is being used and to easily delete subsets of file data.

To add files to the subdirectory:

1. From within the appliance, go to **Setup > System Admin > FTP**.
2. In the **Subdirectory** window, click **Add** to name the subdirectory.

The name appears in the window and displays its current size. Ensure that the directory name matches the one configured on the FTP server.

Note: When naming subdirectories, the standard Linux directory naming conventions apply.

Processing Log Data Received via FTP

Receiving input from a connector via FTP requires that some steps be performed outside of the appliance. The following steps allow for the successful transfer of log data.

1. Enable FTP on the appliance. For detailed instructions, see ["Enabling FTP" on page 257](#).
2. Configure the SmartConnector. For instructions on how to do this, see the SmartConnector Configuration Guide for Blue Coat ProxySG.

Tip: When configuring the Blue Coat SmartConnector for use with FTP, set up the SmartConnector to delete files after processing. This step helps to prevent an over accumulation of files on the FTP server.

To do so, in the `agents.properties`, change `agents[0].foldertable[0].mode=RenameInSameDirectory` to `agents[0].foldertable[0].mode=DeleteFile`.

3.

Tip: When configuring the Blue Coat SmartConnector for use with FTP, point the connector to `/opt/arcsight/incoming/<or subdirectory>`.

4. Configure the device. For instructions on how to do this, see the documentation for your device.

Using FTPS (FTP over SSL)

FTPS is FTP used over a secure SSL channel. The use of **FTPS** requires that a certificate is generated on ArcSight Management Center.

Using FTPS with Blue Coat ProxySG

The use of FTPS requires several steps on both ArcSight Management Center and the Blue Coat ProxySG appliance. The first step is that a **self-signed certificate** or **CSR** is generated on ArcSight Management Center. If the certificate is self-signed, it must be imported into the Blue Coat ProxySG

appliance. If signed by a CA, the certificate of the CA must be imported into the Blue Coat ProxySG appliance.

On ArcSight Management Center:

1. **Generate the certificate** (either a self-signed certificate or CSR) on ArcSight Management Center.
 - For a self-signed certificate, see ["Generating a Self-Signed Certificate" on the next page](#).
 - For a CA-signed certificate, see ["Generating a Certificate Signing Request \(CSR\)" on page 262](#) and ["Importing a Certificate" on page 264](#).
2. **Enable FTP** on Connector Appliance. For detailed steps, see ["Enabling FTP" on page 257](#).

On the Blue Coat ProxySG Appliance:

See your current Blue Coat ProxySG documentation for detailed instructions to complete the following necessary steps.

1. **Import the self-signed or the certificate of the CA** into the Blue Coat ProxySG appliance. If importing a self-signed certificate into the Blue Coat ProxySG appliance, click the **View Certificate** button on the **Generate Certificate** page to display the certificate to be used with FTPS. Copy its entire contents and paste it into the Import CA Certificate window on the BlueCoat ProxySG appliance.
2. **Add the imported certificate into the browser-trusted CA Certificates Lists** on the Blue Coat ProxySG.
3. **Configure the FTP upload client** on the Blue Coat ProxySG appliance, ensuring that you **select the option to use secure connections**.
4. **Run an upload test** on the Blue Coat ProxySG appliance to verify that it was able to successfully upload its log files to Connector Appliance over FTPS.

Security

Security settings enable you to configure SSL server certificates, enable and disable FIPS (Federal Information Processing Standards) mode on your system, and configure SSL client authentication for client certificate and Common Access Card (CAC) support.

Tip: For steps on how to create a user DN, see ["Users" on page 277](#), and refer to the section "Use Client DN" in the parameters table.

SSL Server Certificate

Your system uses Secure Sockets Layer (SSL) technology to communicate securely over an encrypted channel with its clients, such as SmartConnectors, when using the SmartMessaging technology and other ArcSight systems. Your system ships with a self-signed certificate so that an SSL session can be established the first time you use the appliance. For more information on this option, see ["Generating a Self-Signed Certificate" below](#).

Although a self-signed certificate is provided for your use, you should use a certificate authority (CA) signed certificate. To facilitate obtaining a CA-signed certificate, your system can generate a Certificate Signing Request. After a signed certificate file is available from the CA, it can be uploaded to your system for use in a subsequent authentication. For detailed instructions, see ["Generating a Certificate Signing Request \(CSR\)" on the next page](#).

Your system generates an audit event when the installed SSL certificate is going to expire in less than 30 days or has already expired. The event with Device Event Class ID “platform:407” is generated periodically until you replace the certificate with one that is not due to expire within 30 days.

Generating a Self-Signed Certificate

Your system ships with a self-signed certificate so that an SSL session can be established the first time you connect. This type of certificate does not require signing from another entity and can be used immediately.

To generate a self-signed certificate:

1. Click **Administration > Setup > System Admin**.
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.
4. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol

Parameter	Description
HTTPS	Choose this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Choose this option only when generating a CSR for use with FTPS.

5. From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	ISO 3166-1 two-letter country code, such as 'US' for the United States.
State/Province	State or province name, such as 'California.'
City/Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	<p>The host name or IP address of this system.</p> <p>When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in "NICs" on page 236.</p> <p>Note: If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.</p>
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Private key length is 2048 bits.

Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

- Click the **Generate Certificate** button to generate the self-signed certificate.
- Click **Ok** after the confirmation message appears.
- Click the **View Certificate** button to view the PEM encoded self-signed certificate.

Generating a Certificate Signing Request (CSR)

The first step in obtaining a CA-signed certificate is to generate a Certificate Signing Request (CSR). The CSR must be generated on the system for which you are requesting a certificate. That is, you cannot generate a CSR for System A on System B or use a third-party utility for generation.

The resulting CSR must be sent to a CA, such as VeriSign, which responds with a signed certificate file.

To generate a certificate signing request:

1. Click **Administration > System Admin.**
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.
4. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol.

Parameter	Description
HTTPS	Choose this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Choose this option only when generating a CSR for use with FTPS.

5. From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	A two-letter country code, such as 'US' for the United States.
State / Province	State or province name, such as 'California.'
City / Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	<p>The host name or IP address of this system.</p> <p>When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in "NICs" on page 236.</p> <p>Note: If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.</p>
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Select the length (in bits) of the private key: 1024 , 2048 , 4096 , or 8192 .

6. Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

7. Choose **Generate CSR** to generate a certificate signing request.
8. If the CSR was successfully generated, a pop-up window appears, allowing you to either download the CSR file or to cut-and-paste its content.

To do so, copy all the lines from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----`.
9. Send the CSR file to your certificate authority to obtain the CA-signed certificate.
10. After the CA-signed certificate file is obtained, continue on to ["Importing a Certificate" below](#).

Importing a Certificate

If you have obtained a certificate from your certificate authority (CA), follow the steps below to import it onto your system.

1. Click **Administration > System Admin.**
2. Click **SSL Server Certificate** under the **Security** section in the left panel.
3. Select the **Import Certificate** tab.
4. From the **Import Certificate For Protocol** field, use the **Network Protocol** drop-down menu to select the appropriate protocol type.

Parameter	Description
HTTPS	Choose to import an HTTPS certificate. (This option may require a reboot).
FTPS	Choose to import an FTPS certificate.

5. Click the **Browse** button to locate the signed certificate file on your local file system.

Note: The imported certificate must be in **Privacy Enhanced Mail (PEM)** format.

6. Click **Import and Install** to import the specified certificate.
7. If using **HTTPS** and depending on your browser, you may need to close and restart the browser for the new certificate to take effect. If you are unsure of your browser's requirements, close and restart it.

SSL Client Authentication

Your system supports client authentication using SSL certificates. SSL client authentication is a form of two-factor authentication that can be used as an alternate or in addition to local password authentication.

Note: CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

To configure ArcMC to support CAC, you need to upload a trusted certificate, and enable client certificate authentication.

Uploading Trusted Certificates

A trusted certificate is used to authenticate users that log in to your system. Uploading a trusted certificate is required if you are using LDAPS authentication. The trusted certificate is used to authenticate the remote LDAPS server. The certificate needs to be in Privacy Enhanced Mail (PEM) format.

To upload a trusted certificate:

1. Click **Administration > Setup > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. On the **Trusted Certificates** tab, click **Browse** to find the trusted certificate on your local file system.
4. Click **Upload**.

The trusted certificate is uploaded and listed in the “Certificates in Repository” list on the same page where you uploaded it.

To view details about a trusted certificate, click the link displayed in the Certificate Name column.

To delete a trusted certificate, select the certificate and click **Delete**.

Uploading a Certificate Revocation List

A certificate revocation list (CRL) is a computer-generated record that identifies certificates that have been revoked or suspended before their expiration dates. To support CAC, you need to upload a CRL file to your ArcSight system. The CRL file needs to be in PEM format.

To upload a CRL file:

1. Click **Administration > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. In the **Certificate Revocation List** tab, click **Browse** to find the CRL file on your local file system.
4. Click **Upload**.

The CRL is uploaded and listed in the Certificate Revocation List.

To view details about a CRL, click the link displayed in the Issuer Name column.

To delete a CRL file, select it and click the **Delete** button.

Enabling Client Certificate Authentication

To enable client certificate authentication, see ["Client Certificate Authentication " on page 271](#).

FIPS 140-2

Your system supports the Federal Information Processing Standard 140-2 (FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards.

If your system needs to be FIPS 140-2 compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS 140-2 for all encrypted communication between its internal and external components.

Note: Do not perform any FIPS-related activity on the appliance while a FIPS mode change is in progress.

To be fully FIPS 140-2 compliant, all components that work together need to be in FIPS mode. For example, when you enable FIPS on ArcSight Management Center, the appliance becomes FIPS enabled and meets the standards for cryptographic algorithms defined by the NIST. However, containers must also have FIPS enabled.

Note: In ArcSight Management Center, enabling FIPS mode will disable the ability to regenerate a self-signed certificate.

To enable or disable FIPS mode:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **FIPS 140-2** in the Security section in the left panel.
3. Click **Enable** or **Disable** for the Select FIPS Mode option.

4. Click **Save**.
5. When the **Application Reboot Restart Required** message displays, restart your system. click the **System Reboot** link.
6. Check that the appropriate CA certificates are present in the trust store so that connectors can validate their destinations (ArcSight ESM or ArcSight Management Center) successfully. If the appropriate CA certificates are not in the trust store, you need to add them. For information on viewing and adding certificates, see ["Sending a Command to a Container" on page 107](#).

Users/Groups on ArcMC

Use the **Users/Groups** sub-menu to configure users and user groups on ArcMC, and to set authentication options.

For managing users of managed products, see ["Managing Users on Managed Products" on page 200](#).

Authentication

Authentication Settings enable you to specify the settings and policies for user login sessions, password rules and lockouts, and external authentication options.

Sessions

The **Session** tab enables you to specify the maximum number of simultaneous sessions for a single user account, and the length of time after which a user session is automatically logged out or a user account disabled. By default, a single user account can have up to 15 simultaneous active sessions, and a user account is logged out after 15 minutes of inactivity.

To change session settings:

1. Click **Administration > Setup > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.

3. On the **Sessions** tab, update the parameters described in the following table.

Parameters	Description
Max Simultaneous Logins/User	The maximum number of simultaneous sessions allowed for a single user account. The default is 15 sessions .
Logout Inactive Session After	<p>The length of time, in minutes, after which an inactive session is automatically ended. The default is 15 minutes.</p> <p>This value does not apply to the user interface pages accessed through the Monitor menu. If a user is on any of the Monitor menu pages and the session has been inactive for the specified number of minutes, the user's session remains active.</p>
Disable Inactive Account After	The number of days after which an inactive user account is disabled. The default is 0 , meaning the account is never disabled.

4. Click **Save** to make the changes, or click another tab to cancel.

Local Password

The **Local Password** tab enables you to set password policies, such as the minimum and maximum number of characters and other password requirements.

To change the password settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **Local Password** tab.

Use the parameters described in the following table to customize your password settings.

Authentication Settings, Local Password tab

Parameter	Description
Lockout Account (policy)	
Enable Account Lockout	Select the checkbox to enable user accounts to be locked out as defined by the following settings. By default, the policy is disabled .
Lockout Account After	Number of failed login attempts after which a user account is locked out. The default is 3 .
Remember Failed Attempts For	The length of time, in minutes, for which a failed login attempt is remembered. The default is 1 .
Lockout Account For	The length of time, in minutes, for which a locked out account cannot be unlocked. The default is 15 .

Authentication Settings, Local Password tab, continued



Parameter	Description
Password Expiration (policy)	
Enable Password Expiration	Select the checkbox to enable user passwords to expire as defined by the following settings. By default, the policy is disabled .
Password Expires in	Number of days after which the password expires. The default is 90 .
Notify User	Number of days before expiration to notify the user. Select this option to allow users to update their password before expiration. The default is 5 .
Users Exempted From Password Expiration Policy	Click the link to set the number of users whose password should never expire. For information on how to use this feature, see "Users Exempted From Password Expiration" on the next page .
Password Strength Rules (policy)	
Enforce Password Strength	Select the checkbox to enforce password policy as defined by the following settings. By default, the policy is disabled .
Minimum Length	Minimum number of characters that a password must contain. The default is 10 .
Maximum Length	Maximum number of characters that a password can contain. The default is 20 .
Password Character Rules	
Password character rules define additional character requirements to ensure password strength.	
Numeric	Minimum number of numeric characters (0-9) in a password. The default is 2 .
Uppercase	Minimum number of uppercase characters (A-Z) in a password. The default is 0 .
Special	Minimum number of non-digit and non-letter characters that are required in a password. The default is 2 .
Lowercase	Minimum number of lowercase characters (a-z) in a password. The default is 0 .
Password Must be At Least N Characters Different From Old Password	Minimum number of characters by which the new password must differ from the previous one. The default is 2 .
Include "Forgot Password" link on Login Screen	<p>Select the checkbox to enable users to reset their local password using a "Forgot Password" link on the login page. By default, the option is disabled.</p> <p>An SMTP server must be configured on the system, and the username must have a correct email address for this feature to work successfully.</p> <p>If an SMTP server is not set, you cannot reset the password because the email containing the temporary password cannot be sent.</p> <p>You must specify an email address in the user settings for the user name. The temporary password is sent to that email address. If no email address is specified or if the email address is incorrect, the user will not receive the email.</p> <p>For information on how to use this feature, see "Forgot Password" on the next page.</p>

- Click **Save** to save the changes, or click another tab to cancel.

Users Exempted From Password Expiration

Even though you have set a password expiration policy for most users, you may want to have a user whose password does not expire automatically.

To exempt a user from the password expiration policy:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **Local Password** tab, and then click **Users Exempted From Password Expiration Policy**.
4. The **Exempt Users From Password Expiration** page displays.
5. Select users from the **Non-exempted Users** list and click the right arrow icon  to move the selected users to the **Exempted Users** list. Do the reverse to remove users from the list of exempted users.
You can select multiple users at the same time and move them over. Or you can move all users by clicking the  icon.
6. Click **Save** to save the policy or **Cancel** to exit.

Forgot Password

This feature is available only if the **Include “Forgot Password” link on Login Screen** setting on the Authentication Settings page (**Setup > System Admin > Authentication > Local Password**) is set to **Yes**. By default, this setting is set to **No**. An SMTP server must be configured in order to use this feature. For more details on how to enable it, see ["Local Password" on page 268](#).

If you forget your system password, use this feature to receive an email that provides a temporary password.

The temporary password is valid until the time specified in the email. If you do not log in within the specified time, only an administrator can reset the password to generate another temporary password.

To reset your password:

1. Click the **Forgot Password** link on the Login screen.
2. Enter a user name on the Reset Password dialog box.
3. Click **Reset Password**.

An automated email with a temporary password is sent to the email address specified for that user.

External Authentication

Besides providing a local password authentication method, your system supports Client Certificate/CAC, LDAP, and RADIUS authentication. It is not possible to enable all authentication methods simultaneously.

Note: CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

From the **External Authentication** tab, use the drop-down menu to choose one of the following authentication methods:

- "Local Password" below
- "Client Certificate Authentication " below
- "Client Certificate and Local Password Authentication" on the next page
- "LDAP/AD and LDAPS Authentication" on page 273
- "RADIUS Authentication" on page 274

Local Password

This option is the default method and implements the local password policies set in the **Local Password** tab. Leave this as the default, or click **Save** if changing from another option.

Client Certificate Authentication

This authentication method requires that users authenticate using a client certificate. For each client certificate, a user account with a Distinguished Name (DN) matching the one in the client certificate must exist on your system.

Caution: All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate authentication:

1. Click **Administration > System Admin.**
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **Client Certificate**.
5. **Allow Local Password Fallback** provides two options:

- **Allow Local Password Fallback for Default Admin Only**

Select this option to allow the default admin user to log in using only a username and password if the client certificate is not available or invalid. This privilege is restricted to the default admin user only. Other users must have a valid client certificate to gain access to the system. This option is enabled by default.

- **Allow Local Password Fallback for All Users**

Select this option to allow all users to log in using their local user name and password if their client certificate is invalid or unavailable.

For more information, see ["Local Password Fallback" on page 275](#).

6. Click **Save**.

Client Certificate and Local Password Authentication

This authentication method requires that users authenticate using an SSL client certificate and a valid local password. *Local Password* refers to the password associated with the user credentials created in **User Management** in the **Users/Groups** section. See ["User Management" on page 277](#) for details.

A user account on your system must be defined with a Distinguished Name (DN) that matches the one in the client certificate.

For instructions on how to create a user DN, see ["Users" on page 277](#) and refer to the section called "Use Client DN" in the parameters table.

Caution: All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate and password authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **Client Certificate AND Local Password**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
This option, always enabled, allows the default admin user to log in using only a username and password.
 - **Allow Local Password Fallback for All Users**
This option is always disabled. You cannot enable it when using the **Client Certificate AND Local Password** authentication method.

For more information, see ["Local Password Fallback" on page 275](#).

6. Click **Save**.

LDAP/AD and LDAPS Authentication

This authentication method authenticates users against an LDAP server. Even when LDAP is enabled, each user account must exist locally on your system. Although the user name specified locally can be different from the one specified on the LDAP server, the Distinguished Name (DN) specified for each user account must match the one in the LDAP server.

Tip: For steps on how to create a user DN, see ["Users" on page 277](#), and the parameter ["Use Client DN" on page 278](#).

To set up LDAP authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **LDAP**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
Select this option to allow the default admin user to log in using only a username and password if LDAP authentication fails. This privilege is restricted to the default admin user only. All others must be authenticated by LDAP. This option is enabled by default.
 - **Allow Local Password Fallback for All Users**
Select this option to allow all users to log in using their local user name and password if LDAP authentication fails.
For more information, see ["Local Password Fallback" on page 275](#).

LDAP Server has the following parameters:

Parameter	Description
Server Hostname [:port] (optional)	(Optional) Enter the host name or IP address and port of the LDAP server in the following format: ldap://<hostname or IP address >:<port> ldaps://<hostname or IP address >:<port> Additional steps are required for the use of LDAPS. See "Using the LDAP over SSL (LDAPS) Protocol" below below.
Backup Server Hostname [:Port] (optional)	(Optional) Enter the backup LDAP server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.
Request Timeout	The length of time, in seconds, to wait for a response from the LDAP server. The default is 10 .

6. When finished, click **Save**.

Using the LDAP over SSL (LDAPS) Protocol

When choosing the LDAPS protocol to authenticate users, make sure the following conditions are true:

- The SSL certificate for the LDAPS server has been uploaded into the trusted store.
- The external authentication method is set to “LDAP”.
- The URL for the LDAPS server(s) starts with “ldaps : / /”.

After uploading the SSL certificate, restart the **aps** process (**Setup > System Admin > Process Status > aps Restart**).

Caution: If the aps process is not restarted, attempts to authenticate using LDAPS will fail.

RADIUS Authentication

This authentication method allows users to authenticate against a RADIUS server. Even when RADIUS authentication is enabled, each user account must exist locally on your system. The username must match the one in the RADIUS server, although the password can be different. A user must present a valid username and (RADIUS) password to be successfully authenticated.

To configure RADIUS authentication settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.

4. From the drop-down menu, choose **RADIUS**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
Select this option to allow the default admin user to log in using only a username and password if RADIUS authentication fails. This privilege is restricted to the admin user only. All others must be authenticated by RADIUS. This option is enabled by default.
 - **Allow Local Password Fallback for All Users**
Select this option to allow all users to log in using their local user name and password, if RADIUS authentication fails. For more information, see "[Local Password Fallback](#)" below.
6. **Update the RADIUS Server** parameters as necessary:

Parameter	Description
Server Hostname [:port]	Enter the host name and port of the RADIUS server.
Backup Server hostname [:port] (optional)	(Optional) Enter the backup RADIUS server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.
Shared Authentication Secret	Enter a RADIUS passphrase.
NAS IP Address	The IP address of the Network Access Server (NAS).
Request Timeout	The length of time, in seconds, to wait for a response from the RADIUS server (in seconds). The default is 10 .
Retry Request	Number of times to retry a RADIUS request. The default is 1 .
RADIUS Protocol:	Use the drop-down menu to choose a protocol option. The default is None .

7. Click **Save**.

Local Password Fallback

You can use this feature to log in using your local user name and password if the external authentication (Certificate, LDAP, or RADIUS) fails, if you forgot your password to the authentication server, or if the authentication server is not available.

The Use Local Authentication allows the default admin to log in even when the remote authentication server is not available, by adding a **Use Local Authentication** checkbox to the login screen. Out-of-box, this option is enabled only for the default administrator. However, it is possible to allow local

password fallback for all users. For example, you could configure the RADIUS authentication method to allow users to log in using local authentication instead of RADIUS should they fail to authenticate to the configured external RADIUS server(s).

For information on how to allow local password fallback for all users for all users, see ["Client Certificate Authentication" on page 271](#), ["LDAP/AD and LDAPS Authentication" on page 273](#), or ["RADIUS Authentication" on page 274](#).

To log in when authentication fails:

1. Select the **Use Local Authentication** checkbox.

Note: This option is only available to the default admin unless it has been enabled for other users.

2. Enter your login and password and click **Login**.

Login Banner

You can customize the message on the login screen to suit your needs. The text you enter in the **Content** field is displayed above the Username and Password fields on the login screen. In addition, you can enter a confirmation message that the user must click to enable the **Username** and **Password** fields.

You must have the "Configure Login Settings" permission enabled for your user account to edit the login banner.

To customize the login banner:

1. Click **Administration > Setup > System Admin**.
2. Click **Login Banner** in the **Users/Groups** section.
3. Enter the text you want to display as the login banner in the **Content** field.
You can enter only unformatted text in this field; however, you can apply standard HTML tags to display formatted text. Loading images in this field is not allowed.
4. (Optional) Enter text in the **Confirmation** field. Any text entered will be displayed in the login banner, accompanied by a check box that the user must click to enable the **Username** and **Password** fields. For example, if you enter "Are you sure?", then the user must click the checkbox in order to confirm log in.
5. Click **Save**.

User Management

The **Users** and **Groups** tabs enable you to manage users and user groups on your system. User groups are a way to enforce access control to various sections of your system.

Users

Open the **Users** tab to manage the users that can log in to your system. You can add a new user, edit user information, or delete a user at any time. You must have the appropriate System Admin group rights to perform these functions.

To add a new user:

1. Click **Administration > Setup > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, click **Add** from the top left side of the page.

4. Enter the following parameters.

Parameter	Description
<i>Credentials</i>	
Login	The user's login name.
Password	The user's password.
Confirm Password	Reenter the users' password.
<i>Contact Information</i>	
Use Client DN	<p>If you enabled SSL client certificate or LDAP authentication, click this link to enter user's the Distinguished Name (Certificate Subject) information. The Distinguished Name should be similar to this format:</p> <p>CN=UserA,OU=Engg Team,O=ArcSight\, Inc.,L=Cupertino,C=US,ST=California</p> <p>To determine the DN, use this URL to display the certificate:</p> <p><a href="https://<hostname or IP address >/platform-service/DisplayCertificate">https://<hostname or IP address >/platform-service/DisplayCertificate</p> <p>OR</p> <p>Obtain the DN information for a user from the browser that the user will open to connect to the system. For example, on Mozilla Firefox, click Tools > Options > Advanced > Encryption > View Certificates > Your Certificates > Select the certificate > View.</p>
First Name	The user's first name.
Last Name	The user's last name.
Email	The user's email address.
Phone Number	(Optional) The user's phone number.
Title	(Optional) The user's title.
Department	(Optional) The user's department.
Fax	(Optional) The user's fax number.
Alternate Number	(Optional) The user's alternate phone number.
Assign to Groups	Select the groups to which this user belongs. This setting controls the privileges a user has on this ArcSight Management Center.

Parameter	Description
System Admin	Select a rights level from the drop-down list: <ul style="list-style-type: none">• <i>Default System Admin Group</i> gives the user rights to change the settings in the System Admin menu. Choosing this option displays all the tabs and menus.• <i>Read Only System Admin Group</i> allows the user read-only access.• <i>Unassigned</i> prevents user access to the System Admin menu.
ArcMC Rights	Select a rights level from the drop-down list: <ul style="list-style-type: none">• <i>Default ArcMC Rights Group</i> gives the user rights to the Dashboard, Node Management, and Configuration Management menus, as well as the Backup/Restore and Repositories menus. Choosing this option displays all the tabs and menus.• <i>Read Only ArcMC Group</i> allows the user read-only access.• <i>Unassigned</i> prevents user access to all ArcMC components.
Notes	(Optional) Other information about the user.

5. Click **Save and Close**.

To edit a user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) you want to edit.
4. Click **Edit** from the top left side of the page.
5. Update the user information as necessary.
6. Click **Save User**.

To delete a user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) you want to delete.
4. Click **Delete** from the top left side of the page.

Reset Password

The Reset Password feature enables you to reset a user's password without knowing their password. If you are using an SMTP-configured server and have permissions to create and update users, you can reset a user's password by clicking the **Reset Password** button. An automated email including the new password string is sent to the user.

An SMTP server must be configured for the automated email containing the temporary password to be sent. If an SMTP server is not configured, the password will not be reset because an email cannot be sent.

To reset a user's password:

1. Click **Administration > System Admin.**
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) whose passwords you want to reset.
4. Click **Reset Password** from the top left side of the page.

The user must use the temporary string to log in within the time specified in the email. If the user does not log in within the specified time, the account becomes deactivated. If the account has been deactivated, the admin must re-activate it before resetting the password.

To activate a user:

1. Click **Administration > System Admin.**
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) that you want to activate.
4. Choose **Edit**.
5. Check the **Active** box.
6. **Save** the changes.

Groups

User groups define privileges to specific functions on your system and serve to enforce access control to these functions. For example, if you want User A to perform system admin related activities that are not Connector Appliance management specific, assign that user to the System Admin group, but not to the Connector Appliance group.

User groups are divided into the following types: System Admin and Connector Appliance Rights Groups. Each type has a pre-defined, default user group in which all privileges for the type are enabled. To authorize a subset of the privileges for a specific group type, create a new user group and enable only the privileges you want to provide for that group. Then, assign restricted users to the newly created group.

System Admin Groups

System Admin Group

The System Admin Group controls the system administration operations for your system, such as configuring network information, setting storage mounts, installing SSL certificates, and user management.

Read Only System Admin Group

In addition to the default System Admin Group that enables all rights (privileges), a Read Only System Admin Group is available on your system. Users assigned to this group can view System Admin settings, but cannot change them.

ArcSight Management Center Rights Groups for ArcSight Management Center

ArcSight Management Center Rights Group

The Connector Appliance Rights Group controls the ArcSight Management Center application operations for your system, such as viewing the ArcSight Management Center dashboards and backup operations.

Read Only ArcSight Management Center Group

In addition to the default Connector Appliance Rights Group that enables all rights (privileges), Connector Appliance provides more controlled authorizations and a “view only” default option. A read-only user can view the tabs and the operations displayed on the tabs, and can perform operations such as refresh, view certificate list, and Logfu.


Refer to your system's user interface for a complete list of rights available to this group.

It is strongly recommended not to modify any rights for the default admin user, as this can cause access issues.

Managing a User Group

To create a new user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Click **Add** from the top left side of the page.
5. Define the new group:
 - a. In the **Group Name** field, provide a name for the group.
 - b. In the **Description** field, provide a description for the group.
 - c. From the Group Type drop-down box, select the group type.

- d. Click the down arrow icon () next to the group type name to view and select privileges that you want to assign to the users in this group.
6. Click **Save and Close** to save the settings of the group, or click **Save and Edit Membership** to add users to this group.

To edit a user group:

1. Click **Administration > System Admin.**
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group that you want to edit, and click **Edit** at the top left side of the page.
5. Update the user group information.

If you need to edit the group's membership:

- a. Click **Save and Edit Membership** to display the Edit Group Membership page.
- b. Click **Add** from the top left of the Edit Group Membership page.
- c. Select users you want to add. By default, you can add only users who do not belong to other groups of the type that you are editing. To add such users, click **Show users that belong to other <group_type> groups**.
When you add a user who belongs to another group of the same group type as the one you are updating, that user is automatically removed from the previous group.
- d. Click **OK**.
- e. Click **Back to Group List**.
6. Click **Save and Close**.

To delete a user group:

1. Click **Administration > System Admin.**
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group (or groups) that you want to delete.
5. Click **Delete** at the top left side of the page.

Change Password

You can use the **Change Password** menu to change your application password. This feature is available to all users for changing their passwords, unlike the Reset Password feature that enables a system administrator to reset the password of users without knowing the password. Passwords are subject to the secure password policy specified by the Admin user, as well as the following restrictions.

- Password reset attempts for the admin user will fail, to prevent an unauthenticated user from resetting the admin account/
- If the password reset attempt fails due to resetting an unknown or admin user, ArcMC will not report the failure.

To change your password:

1. Click **Administration > Setup > System Admin.**
2. Click **Change Password** in the **Users/Groups** section in the left panel to display the **Change Password for <User Name>** page.
3. Enter the Old Password, the New Password, and enter the New Password a second time to confirm.

Appendix A: Audit Logs

The following topics are discussed here.

• Audit Event Types	284
• Audit Event Information	284
• Application Events	285
• Platform Events	291
• System Health Events	295

Audit Event Types

You can forward ArcSight Management Center application audit events, which are in Common Event Format (CEF), to a destination of your choice.

Several types of audit events are generated by ArcSight Management Center:

- **Application events:** related to ArcSight Management Center functions and configuration changes
- **Platform events:** related to the ArcSight Management Center system
- **System health events:** related to ArcSight Management Center health.

Audit Event Information

An ArcSight Management Center audit event contains information about the following prefix fields.

- Device Event Class ID
- Device Severity
- Name
- Device Event Category (cat)

See ["Audit Logs" on page 253](#) for details on how to generate audit logs.

Note: If no Syslog Daemon connector is installed or configured on your local machine, then no audit events will be visible.

Application Events

Application Events

Signature	Severity	Description	deviceEventCategory
Connector			
connector:101	1	Register connector successful	/Connector/Add/Success
connector:102	1	Connector removed successfully	/Connector/Delete
connector:103	1	Update connector parameters successful	/Connector/Parameter/Update/Success
connector:104	1	AUP Package create successful	/Connector/AUP Package/Create/Success
connector:105	1	AUP Package deploy successful	/Connector/AUP Package/Deploy/Success
connector:201	1	Connector add failed	/Connector/Add/Fail
connector:202	1	Connector delete failed	/Connector/Delete/Fail
connector:203	1	Connector parameters update failed	/Connector/Parameter/Update/Fail
ArcSight Management Center			
arcmc:101	1	ConfigurationBackupScheduler add success	/BackupScheduler/Add/Success
arcmc:102	1	ConfigurationBackupScheduler update successful	/BackupScheduler/Update/Success
arcmc:103	1	ConfigurationBackupScheduler delete success	/BackupScheduler/Delete/Success
arcmc:104	1	Scheduled Backup triggered	/Backup/Scheduled/Trigger
arcmc:105	1	Scheduled Backup completed	/Backup/Scheduled/Complete/Success
arcmc:106	1	Manual Backup completed	/Backup/Manual/Complete/Success
arcmc:107	1	Local Backup completed	/Backup/Local/Complete/Success
arcmc:108	1	You have exceeded the maximum number of managed connectors allowed by your license	/RemotelyManagedConnectors/Exceeded
arcmc:110	1	You have attempts to exceed the maximum number of managed products allowed by your license	/managedproducts/exceeded

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:111	1	Reboot command launched successfully	Node/reboot/launched/Success
arcmc:112	1	New configuration created successfully	/Configuration/Add/Success
arcmc:113	1	Edit configuration successful	/Configuration/Edit/Success
arcmc:114	1	Delete configurations successful	/Configuration/Delete/Success
arcmc:115	1	Push configuration successful	/Configuration/Push/Success
arcmc:116	1	Import configuration successful	/Configuration/Import/Success
arcmc:117	1	Add subscriber to configuration successful	/Configuration/Subscribe/Success
arcmc:118	1	Unsubscribe node for configuration successful	/Configuration/Unsubscribe/Success
arcmc:119	1	Check compliance of configuration successful	/Configuration/Check Compliance/Success
arcmc:120	1	Configuration set successfully	/Node/Set/Configuration/Success
arcmc:121	1	Configuration appended successfully	/Node/Append/Configuration/Success
arcmc:122	1	Agent install success	/ArcMCAgent/Install/Success
arcmc:123	1	Upgrade agent successfully	/ArcMCAgent/Upgrade/Success
arcmc:124	1	Add/Push Logger Peers Successful	/Logger/AddPeers/Success
arcmc:125	1	Remove Logger Peers Successful	/Logger/RemovePeers/Success
arcmc:127	1	Create/Import Logger Peer Group Successful	/Logger/AddPeerGrp/Success
arcmc:128	1	Delete Logger Peer Group Successful	/Logger/DeletePeerGrp/Success
arcmc:129	1	Edit Logger Peer Group Successful	/Logger/EditPeerGrp/Success
arcmc:130	1	Import Initial Configuration Successful	/Logger/ImportInitConfig/Success
arcmc:131	1	Pushed Initial Configuration	/Logger/PushInitConfig/Success
arcmc:132	1	Deleted Initial Configuration	/Logger/DelInitConfig/Success
arcmc:133	1	Host upgrade started.	/Node/Upgrade/Start
arcmc:134	1	Host upgrade successful.	/Node/Upgrade/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:138	1	Update rule/s	/ArcMC/UpdateRules/Success
arcmc:201	1	ConfigurationBackupScheduler add failed	/BackupScheduler/Add/Fail
arcmc:202	1	ConfigurationBackupScheduler update failed	/BackupScheduler/Update/Fail
arcmc:203	1	ConfigurationBackupScheduler delete failed	/BackupScheduler/Delete/Fail
arcmc:205	1	Scheduled Backup failed	/Backup/Scheduled/Complete/Fail
arcmc:206	1	Manual Backup failed	/Backup/Manual/Complete/Fail
arcmc:212	1	New configuration creation failed	/Configuration/Add/Fail
arcmc:213	1	Edit configuration failed	/Configuration/Update/Fail
arcmc:214	1	Configuration deletion failed	/Configuration/Delete/Fail
arcmc:215	1	Push configuration failed	/Configuration/Import/Fail
arcmc:216	1	Import configuration failed	/Backup/Local/Push/Fail
arcmc:217	1	Add subscriber to configuration failed	/Configuration/Subscribe/Fail
arcmc:218	1	Unsubscribe node for configuration failed	/Configuration/Unsubscribe/Fail
arcmc:219	1	Check compliance of configuration failed	/Configuration/Check Compliance/Success
arcmc:220	1	Configuration set failed	/Node/Set/Configuration/Fail
arcmc:221	1	Configuration append failed	/Node/Append/Configuration/Fail
arcmc:222	1	Agent install failed	/ArcMCAgent/Install/Failure
arcmc:223	1	Upgrade agent failed	/ArcMCAgent/Upgrade/Fail
arcmc:224	1	Add/Push Logger Peers Failed	/Logger/AddPeers/Fail
arcmc:225	1	Remove Logger Peers Failed	/Logger/RemovePeers/Fail
arc mc:226	1	Alert message payload	/ArcMCMonitor/Breach
arcmc:230	1	Import Initial Configuration Failed	/Logger/ImportInitConfig/Fail
arcmc:234	1	Host upgrade failed.	/Node/Upgrade/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:250	1	Push user assignment <assignment name>	/ArcMCUM/Push
arcmc:251	1	Decommission user <UserName>	/ArcMCUM/DeleteUser
arcmc:252	1	Add user <UserName>	/ArcMCUM/AddUser
Destination			
destination:102	1	Update destination successful	/Connector/Destination/Update/Success
destination:103	1	Remove destination successful	/Connector/Destination/Delete/Success
destination:104	1	Update destination configuration successful	/Connector/Destination/Configuration/Update/Success
destination:105	1	Register destination successful	/Connector/Destination/Registration/Success
destination:106	1	Create destination configuration successful	/Connector/Destination/Configuration/Add/Success
destination:107	1	Destination configuration delete successful	/Connector/Destination/Configuration/Delete/Success
destination:202	1	Destination update to a connector failed	/Connector/Destination/Update/Fail
destination:203	1	Destination delete from a connector failed	/Connector/Destination/Delete/Fail
destination:204	1	Destination configuration update failed	/Connector/Destination/Configuration/Update/Fail
destination:205	1	Register destination failed	/Connector/Destination/Registration/Fail
destination:206	1	Destination configuration add failed	/Connector/Destination/Configuration/Add/Fail
destination:207	1	Destination configuration delete failed	/Connector/Destination/Configuration/Delete/Fail
Container			
container:101	1	Container upgrade successful	/Container/Upgrade/Success
container:102	1	Push user file successful	/Container/UserFiles/Push/Success
container:103	1	User file delete from container	/Container/UserFiles/Delete
container:104	1	CA cert push to a container successful	/Container/CACert/Push/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:105	1	Container demo CA enable successful	/Container/DemoCA/Enable/Success
container:106	1	Container demo CA disable successful	/Container/DemoCA/Disable/Success
container:109	1	Delete property from a container successful	/Container/Property/Delete/Success
container:110	1	Modify properties successful	/Container/Property/Update/Success
container:111	1	Container password update successful	/Container/Password/Update/Success
container:112	1	Container add successful	/Container/Add/Success
container:113	1	Container edit	/Container/Update
container:114	1	Remove container	/Container/Delete
container:115	1	Add certificate for a container successful	/Container/Certificate/Add/Success
container:116	1	Removing certificates successful [addtrust class 1ca]	/Container/Certificate/Delete/Success
container:117	1	Enabling FIPS mode successful	/Container/FIPS/Enable/Success
container:118	1	Disabling FIPS mode successful	/Container/FIPS/Disable/Success
container:119	1	Upgrade was triggered for container that resides on end of life appliance model	Container/FromEndOfLifeModel/Upgrade/Triggered
container:201	1	Container upgrade failed	/Container/Upgrade/Fail
container:202	1	User file push to a container failed	/Container/UserFiles/Push/Fail
container:204	1	CA cert push to a container failed	/Container/CACert/Push/Fail
container:205	1	Enable demo CA for a container failed	/Container/DemoCA/Enable/Fail
container:206	1	Disable demo CA for a container failed	/Container/DemoCA/Disable/Fail
container:209	1	Delete property from a container failed	/Container/Property/Delete/Fail
container:210	1	Update property to a container failed	/Container/Property/Update/Fail
container:211	1	Container password update failed	/Container/Password/Update/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:212	1	Container add failed	/Container/Add/Fail
container:215	1	Add certificate for a container failed	/Container/Certificate/Add/Fail
container:216	1	Delete certificate for a container failed	/Container/Certificate/Delete/Fail
container:217	1	Enable FIPS on a container failed	/Container/FIPS/Enable/Fail
container:218	1	Disable FIPS on a container failed	/Container/FIPS/Disable/Fail
container:219	1	SSL Certificate downloaded successfully	/Container/Certificate/Download/Success
container:220	1	SSL Certificate download failed	/Container/Certificate/Download/Fail
container:221	1	SSL Certificate imported successfully	/Container/Certificate/Import/Success
container:222	1	SSL Certificate import failed	/Container/Certificate/Import/Fail
container:301	1	Container upgrade started	/Container/Upgrade/Start
Event Broker			
eventbroker:146	1	Event broker Add Topic succesful	/EventBroker/Topic/Add/Success
eventbroker:147	1	Event broker delete route/s successful	/EventBroker/Route/Add/Success
eventbroker:148	1	Event broker Add Route/s successful	/EventBroker/Route/Add/Success
eventbroker:149	1	Event broker Update Route successful	/EventBroker/Route/Update/Success
eventbroker:241	1	Event broker Add Topic failed	/EventBroker/Topic/Add/Fail
eventbroker:242	1	Event broker delete route/s failed	/EventBroker/Route/Add/Fail
eventbroker:243	1	Event broker Add Route failed	/EventBroker/Route/Add/Fail
eventbroker:244	1	Event broker Update Route failed	/EventBroker/Route/Update/Fail
Location			
location:101	1	Location add successful	/Location/Add/Success
location:102	1	Location edit	/Location/Update
location:103	1	Remove location	/Location/Delete
location:201	1	Location add failed	/Location/Add/Fail
Host			

Application Events, continued

Signature	Severity	Description	deviceEventCategory
host:101	1	Host add successful	/Host/Add/Success
host:103	1	Remove host	/Host/Delete
host:105	1	Host certificate download and import successful	/Host/Certificate/Download /Import/Success
host:201	1	Host add failed	/Host/Add/Fail
host:205	1	Host certificate download and import failed	/Host/Certificate/Download Import/Fail

Platform Events

Platform Events

Signature	Severity	Definition	Category
platform:200	7	Failed password change	/Platform/Authentication/ PasswordChange/Failure
platform:201	7	Failed login attempt	/Platform/Authentication/Failure/ Login
platform:202	5	Password changed	/Platform/Authentication/ Password
platform:203	7	Login attempt by inactive user	/Platform/Authentication/ InactiveUser/Failure
platform:205	7	Automated password reset attempt made for admin account	/Platform/Authentication/PasswordChange/AdminFailure
platform:206	7	Failed automated password reset attempt for user	/Platform/Authentication/PasswordChange/Failure
platform:207	7	Automated password reset attempted for non-existent user	/Platform/Authentication/PasswordChange/UnknownUser
platform:213	7	Audit forwarding modified	/Platform/Configuration/Global/ AuditEvents
platform:220	5	Installed certificate	/Platform/Certificate/Install
platform:221	7	Certificate mismatch failure	/Platform/Certificate/Mismatch
platform:222	1	Created certificate signing request	/Platform/Certificate/Request

Platform Events, continued

Signature	Severity	Definition	Category
platform:224	5	Re-generate self-signed certificate	/Platform/Certificate/Regenerate
platform:226	7	Uploaded update file damaged or corrupt	/Platform/Update/Failure/CorruptPackage
platform:227	5	Update installation success	/Platform/Update/Applied
platform:228	7	Update installation failure	/Platform/Update/Failure/Installation
platform:230	3	Successful login	/Platform/Authentication/Login
platform:234	7	Failed login attempt (LOCKED)	/Platform/Authentication/Failure/LOCKED
platform:239	1	User logout	/Platform/Authentication/Logout
platform:240	3	Added user group	/Platform/Groups/Add
platform:241	3	Updated user group	/Platform/Groups/Update
platform:242	5	Removed all members from group	/Platform/Authorization/Groups/Membership/Update/Clear
platform:244	3	Deleted user group	/Platform/Groups/Remove
platform:245	3	Added user	/Platform/Users/Add
platform:246	3	Updated user	/Platform/Users/Update
platform:247	3	Deleted user	/Platform/Users/Delete
platform:248	3	Session expired	/Platform/Authentication/Logout/SessionExpiration
platform:249	7	Account locked	/Platform/Authentication/AccountLocked
platform:250	3	Added remote mount point	/Platform/Storage/RFS/Add
platform:251	5	Edited remote mount point	/Platform/Storage/RFS/Edit
platform:252	7	Failed to create remote mount point	/Platform/Storage/RFS/Failure
platform:253	5	Removed remote mount point	/Platform/Storage/RFS/Remove
platform:260	5	Static route modified	/Platform/Configuration/Network/Route/Update
platform:261	5	Static route removed	/Platform/Configuration/Network/Route/Remove
platform:262	5	Appliance time modified	/Platform/Configuration/Time
platform:263		NIC settings modified	/Platform/Configuration/NIC
platform:264		NTP server settings modified	/Platform/Configuration/NTP

Platform Events, continued

Signature	Severity	Definition	Category
platform:265	5	DNS settings modified	/Platform/Configuration/Network/DNS
platform:266	5	Hosts file modified	/Platform/Configuration/Network/Hosts
platform:267	5	SMTP settings modified	/Platform/Configuration/SMTP
platform:268	5	Static route added	/Platform/Configuration/Network/Route/Add
platform:269	5	Updated Platform Settings	/Platform/Configuration
platform:280	7	Appliance reboot initiated	/Appliance/State/Reboot/Initiate
platform:281	3	Appliance reboot canceled	/Appliance/State/Reboot/Cancel
platform:282	9	Appliance poweroff initiated	/Appliance/State/Shutdown
platform:284	5	Enabled SAN Multipathing	/Platform/Storage/Multipathing/Enable
platform:285	5	Disabled SAN Multipathing	/Platform/Storage/Multipathing/Disable
platform:300	5	Installed trusted certificate	/Platform/Certificate/Install
platform:301	5	Installed certificate revocation list	/Platform/Certificate/Revocation/Install
platform:302	5	Deleted trusted certificate	/Platform/Certificate/Delete
platform:303	5	Deleted certificate revocation list	/Platform/Certificate/Revocation/Delete
platform:304	7	Failed installing trusted certificate	/Platform/Certificate/Install/Failure
platform:305	7	Failed installing certificate revocation list	/Platform/Certificate/Revocation/Install/Failure
platform:306	5	Start process	/Platform/Process/Start
platform:307	5	Stop process	/Platform/Process/Stop
platform:308	5	Restart process	/Platform/Process/Restart
platform:310	5	Enabled FIPS mode	/Platform/Configuration/FIPS/Enable
platform:311	7	Disabled FIPS mode	/Platform/Configuration/FIPS/Disable
platform:312	7	Web server cipher strength changed	/Platform/Configuration/WebServer/CipherStrength
platform:313	5	Enable SSH	/Platform/Configuration/SSH/Enable
platform:314	7	Disable SSH	/Platform/Configuration/SSH/Disable
platform: 315	7	Enable SSH only during startup/reboot	/Platform/Configuration/SSH/StartupOnly
platform:316	7	Enable SSH only for 8 hours	/Platform/Configuration/SSH/Enable8Hours

Platform Events, continued

Signature	Severity	Definition	Category
platform:320	3	Appliance poweroff canceled	/Appliance/State/Shutdown/Cancel
platform:371	5	Restarted OS service	/Platform/Service/Restart
platform:400	1	Ran diagnostic command	/Platform/Diagnostics/Command
platform:407	7	SSL certificate expiration warning	/Platform/Certificate/SSL/Expiration
platform:408	5	Appliance startup completed	/Appliance/State/Startup
platform:409	3	Configure login warning banner	/Platform/Configuration/LoginBanner
platform:410	3	Network settings modified	
platform:411	5	Automated password reset	/Platform/Authentication/PasswordChange
platform:412	3	Set locale	/Platform/Configuration/Locale
platform:440	3	SNMP configuration modified	Platform/Configuration/SNMP
platform:450	3	FTP service enabled	
platform:451	3	FTP service disabled	
platform:454	3	FTP service configuration changed	
platform:455	3	Added sub directory	
platform:456	3	Removed sub directory	
platform:460	3	NIC alias added	/Platform/Network/Alias/Add
platform:462	3	NIC alias removed	/Platform/Network/Alias/Remove
platform:500	5	Remove member from group	/Platform/Authorization/Groups/Membership/Remove
platform:501	5	Group member added	/Platform/Authorization/Groups/Membership/Add
platform:502	5	User removed from group	/Platform/Authorization/Users/Groups/Remove
platform:503	5	User added to group	/Platform/Authorization/Users/Groups/Add
platform:530	5	Authentication Session settings successfully changed	/Platform/Configuration/Authentication/Sessions/Success
platform:540	5	Password Lockout settings successfully updated	/Platform/Configuration/Authentication/Password/Lockout/Success

Platform Events, continued

Signature	Severity	Definition	Category
platform:550	5	Password Expiration settings successfully updated	/Platform/Configuration/Authentication/Password/Expiration/Success
platform:560	5	Password Validation settings successfully updated	/Platform/Configuration/Authentication/Password/Validation/Success
platform:570	5	Allow Automated Password Reset settings successfully changed	/Platform/Configuration/Authentication/Password/AutomatedReset/Success
platform:590	5	RADIUS authentication settings successfully changed	/Platform/Configuration/Authentication/RADIUS/Success
platform:600	5	LDAP authentication settings successfully changed	/Platform/Configuration/Authentication/LDAP/Success
platform:610	5	Global authentication settings successfully changed	/Platform/Configuration/Authentication/Global/Success

System Health Events

System health events provide four status indicators:

- OK
- Degraded
- Rebuilding
- Failed

An **OK** event, indicating normal system behavior, is generated once every ten minutes (six events per hour, per sensor). For a status other than **OK** (**Degraded**, **Rebuilding**, or **Failed**), the event is sent every minute until the sensor returns an **OK** status.

SNMP Related Properties

The following list provides the event fields for system health events sent via SNMP traps. For detailed instructions on setting up SNMP traps, see ["SNMP" on page 242](#).

• event.deviceReceiptTime	• event.endTime
• event.deviceVendor	• event.deviceProduct
• event.deviceVersion	• event.deviceEventClassId
• event.name	• event.deviceSeverity
• event.deviceEventCategory	• event.deviceCustomNumber1

• event.deviceCustomNumber1Label	• event.deviceCustomString1
• event.deviceCustomString1Label	• event.deviceCustomString2
• event.deviceCustomString2Label	• event.deviceCustomString3
• event.deviceCustomString3Label	• event.deviceCustomString4
• event.deviceCustomString4Label	• event.deviceCustomString5
• event.deviceCustomString5Label	• event.deviceCustomString6
• event.deviceCustomString6Label	• event.destinationAddress
• event.deviceAddress	

The **snmp.mib.version** is set to 5.0.

System Health Events

Signature	Severity	Definition	Category
CPU			
cpu:100	1	CPU Usage	/Monitor/CPU/Usage
cpu:101	1	Health statistics per CPU	/Monitor/CPU _n /Usage
Disk			
disk:101	1	Root Disk Space Remaining	/Monitor/Disk/Space/Remaining/Data
disk:102	1	Disk bytes read	/Monitor/Disk/drive/Read
disk:103	1	Disk bytes written	/Monitor/Disk/drive/Write
disk:104	1	Disk Space Remaining	/Monitor/Disk/Space/Remaining/Root
Hardware			
hardware:101	1	Electrical (Current) OK	/Monitor/Sensor/Current/Ok**
hardware:102	5	Electrical (Current) Degraded	/Monitor/Sensor/Current/Degraded**
hardware:103	8	Electrical (Current) Failed	/Monitor/Sensor/Current/Failed**
hardware:111	1	Electrical (Voltage) OK	/Monitor/Sensor/Voltage/Ok**
hardware:112	1	Electrical (Voltage) Degraded	/Monitor/Sensor/Voltage/Degraded**
hardware:113	1	Electrical (Voltage) Failed	/Monitor/Sensor/Voltage/Failed**
hardware:121	1	Battery OK	/Monitor/Sensor/Battery/Ok**
hardware:122	5	Battery Degraded	/Monitor/Sensor/Battery/Degraded **
hardware:123	8	Battery Failed	/Monitor/Sensor/Battery/Failed**
hardware:131	1	Fan OK	/Monitor/Sensor/Fan/Ok
hardware:132	5	Fan Degraded	/Monitor/Sensor/Fan/Degraded

System Health Events, continued

Signature	Severity	Definition	Category
hardware:133	8	Fan Failed	/Monitor/Sensor/Fan/Failed
hardware:141	1	Power Supply OK	/Monitor/Sensor/PowerSupply/Ok
hardware:142	5	Power Supply Degraded	/Monitor/Sensor/PowerSupply/ Degraded
hardware:143	8	Power Supply Failed	/Monitor/Sensor/PowerSupply/Failed
hardware:151	1	Temperature OK	/Monitor/Sensor/Temperature/Ok
hardware:152	1	Temperature Degraded	/Monitor/Sensor/Temperature/ Degraded
hardware:153	1	Temperature Failed	/Monitor/Sensor/Temperature/Failed
Memory			
memory:100	1	Platform memory usage	/Monitor/Memory/Usage/Platform
memory:101	1	Health statistics for JVM memory	/Monitor/Memory/Usage/Jvm
memory:102	1	Health statistics for platform buffers memory	/Monitor/Memory/Usage/Platform/ Buffers
memory:103	1	Health statistics for platform cached memory	/Monitor/Memory/Usage/Platform/ Cached
memory:104	1	Health statistics for platform free memory	/Monitor/Memory/Usage/Platform/ Free
memory:105	1	Health statistics for JVM heap memory	/Monitor/Memory/Usage/Jvm/Heap
memory:106	1	Health statistics for JVM non-heap memory	/Monitor/Memory/Usage/Jvm/ NonHeap
Network			
network:100	1	Network usage—Inbound	/Monitor/Network/Usage/iface/In
network:101	1	Network usage—Outbound	/Monitor/Network/Usage/iface/Out
network:200	1	Number of Apache connections	
NTP			
ntp:100	1	NTP synchronization	
RAID			
raid:101	1	RAID Controller OK	/Monitor/RAID/Controller/OK
raid:102	5	RAID Controller Degraded	/Monitor/RAID/Controller/Degraded
raid:103	8	RAID Controller Failed	/Monitor/RAID/Controller/Failed
raid:111	1	RAID BBU OK	/Monitor/RAID/BBU/Ok

System Health Events, continued

Signature	Severity	Definition	Category
raid:112	5	RAID BBU Degraded	/Monitor/RAID/BBU/Degraded
raid:113	8	RAID BBU Failed	/Monitor/RAID/BBU/Failed
raid:121	1	RAID Disk OK	/Monitor/RAID/DISK/Ok
raid:122	5	RAID Disk Rebuilding	/Monitor/RAID/DISK/Rebuilding
raid:123	8	RAID Disk Failed	/Monitor/RAID/DISK/Failed

Appendix B: Destination Runtime Parameters

The following table describes configurable destination parameters. The parameters listed in the table are not available for all destinations. The user interface automatically displays the parameters valid for a destination. For step-by-step instructions on updating the runtime parameters of a destination, see ["Editing Connector Parameters" on page 121](#).

Parameter	Description
Batching	Connectors can batch events to increase performance and optimize network bandwidth. When activated, connectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires, whichever occurs first. You can also prioritize batches by severity, forcing the connector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, 100 , 200, 300 events).
Enable Batching (in seconds)	The connector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is Time Based if the connector should send batches as they arrive (the default) or Severity Based if the connector should send batches based on severity (batches of Highest Severity events sent first).
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the connector to automatically correct the time reported by the device.
Use Connector Time as Device Time	Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. (No Yes)
Enable Device Time Correction (in seconds)	The connector can adjust the time reported by the device Detect Time, using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol. The default is 0 .
Enable Connector Time Correction (in seconds)	The connector can also adjust the time reported by the connector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the connector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and connectors is the NTP protocol. The default is 0 .
Set Device Time Zone To	Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the connector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported. Default: Disabled .
Device Time Auto-correction	

Parameter	Description
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by <code>Past Threshold</code> seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by <code>Past Threshold</code> seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, <code>(ALL)</code> , means all devices.
Time Checking	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking. The default is 5 minutes (300 seconds).
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is 1 hour (3,600 seconds).
Frequency	The connector checks its future and past thresholds at intervals specified by this number of seconds. Default is 1 minute (60 seconds).
Cache	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Cache Size	Connectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the connector receives bursts of events. This parameter specifies the disk space to use. The default is 1 GB which, depending on the connector, can hold about 15 million events, but it also can go down to 5 MB . When this disk space is full, the connector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 150 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is 10,000 .
Notification Frequency	How often to send notifications after the Notification Threshold is reached. (1 minute, 5 minutes, 10 minutes , 30 minutes, 60 minutes.)
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the destination. The default is 10 seconds , but it can go from 5 seconds to 10 minutes . Note that the heartbeat is also used to communicate with the connector; therefore, if its frequency is set to 10 minutes , then it could take as much as 10 minutes to send any configuration information or commands back to the connector.
Enable Name Resolution	The connector tries to resolve IP addresses to hostnames, and hostnames to IP addresses , if required and if the event rate allows. This setting controls this functionality. The Source, Target and Device IP addresses , and Hostnames might also be affected by this setting. By default, name resolution is enabled (Yes).
Name Resolution Host Name Only	Default: Yes .

Parameter	Description
Name Resolution Domain From E-mail	Default: Yes .
Clear Host Names Same as IP Addresses	Default: Yes .
Limit Bandwidth To	A list of bandwidth options you can use to constrain the connector's output over the network. (Disabled , 1 kbit/sec to 100 Mbits/sec.)
Transport Mode	You can configure the connector to cache to disk all the processed events it receives. This is equivalent to pausing the connector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (Normal Cache Cache (but send Very High severity events).
Address-based Zone Population Defaults Enabled	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping. Default: Yes .
Address-based Zone Population	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping.
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	Shows the URI of the zone associated with the connector's source address. (Required for ESM v3.0 compatibility.)
Source Translated Zone URI	Shows the URI of the zone associated with the connector's translated source address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Destination Zone URI	Shows the URI of the zone associated with the connector's destination address. (Required for ESM v3.0 compatibility.).
Destination Translated Zone URI	Shows the URI of the zone associated with the connector's translated destination address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Connector Zone URI	Shows the URI of the zone associated with the connector's address. (Required for ESM v3.0 compatibility.)
Connector Translated Zone URI	Shows the URI of the zone associated with the connector's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Device Zone URI	Shows the URI of the zone associated with the device's address. (Required for ESM v3.0 compatibility.)

Parameter	Description
Device Translated Zone URI	Shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Field Based Aggregation	<p>This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, all the fields of the two events are the same (the only difference being the detect time). However, field-based aggregation implements a less strict aggregation mechanism; two events are aggregated if only the selected fields are the same for both alerts. It is important to note that field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored.</p> <p>Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate “accepts” and “rejects” in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.</p>
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Field Names	Enter one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-hostnames. Names can contain no spaces and the first letter must not be capitalized.
Fields to Sum	Enter one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Preserve Common Fields	Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing No , the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	<p>Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events).</p> <p>Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.</p>
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)

Parameter	Description
Fields to Sum	(Optional) Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Processing	
Preserve Raw Event	For some devices, a raw event can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field. This feature is disabled by default since using raw data increases the event size and therefore requires more database storage space. You can enable this by changing the Preserve Raw Event setting. The default is No . If you choose Yes , the serialized representation of the "Raw Event" is sent to the destination and preserved in the Raw Event field.
Turbo Mode	<p>You can accelerate the transfer of a sensor's event information through connectors by choosing one of two "turbo" (narrower data bandwidth) modes. The default transfer mode is called Complete, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).</p> <p>Complete mode does indeed use all the database performance advances of ArcSight ESM v3.x.</p> <p>The first level of Turbo acceleration is called Faster and drops just additional data, while retaining all other information. The Fastest mode eliminates all but a core set of event attributes, in order to achieve the best throughput.</p> <p>The specific event attributes that apply to these modes in your enterprise are defined in the self-documented <code>\$ARCSIGHT_HOME/config/connector/agent.properties</code> file for the ArcSight Manager. Because these properties might have been adjusted for your needs, you should refer to this file for definitive lists. Only scanner connectors need to run in Complete mode, to capture the additional data.</p> <p>Note: Connector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to Faster will not pass all the data possible for a connector that is set for the default of Complete.</p>

Parameter	Description
Enable Aggregation (in seconds)	<p>When enabled, aggregates two or more events on the basis of the selected time value. (Disabled, 1, 2, 3, 4, 5, 10, 30, 60)</p> <p>The aggregation is performed on one or more matches for a fixed subset of fields:</p> <ul style="list-style-type: none"> • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) <p>The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.</p>
Limit Event Processing Rate	<p>You can moderate the connector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts.</p> <p>The choices range from Disabled (no limitation on CPU demand) to 1 eps (pass just one event per second, making the smallest demand on the CPU).</p> <p>Note: The effect of this option varies with the category of connector in use, as described in the connector Processing Categories table below.</p>
Fields to Obfuscate	
Store Original Time in	Disabled or Flex Date 1.
Enable Port-Service Mapping	Default: No .
Enable User Name Splitting	Default: No .

Parameter	Description
Split File Name into Path and Name	Default: No .
Event Integrity Algorithm	Disabled , SHA-1, SHA-256, SHA-512, or MD5.
Generate Unparsed Events	Default: No .
Preserve System Health Events	Yes, No , or Disabled.
Enable Device Status Monitoring (in minutes)	Disabled or 1, 2, 3, 4, 5, 10, 30, 60, or 120 minutes.
Filters	
Filter Out	NA
“Very High Severity” Event Definition	NA
“High Severity” Event Definition	NA
“Medium Severity” Event Definition	NA
“Low Severity” Event Definition	NA
“Unknown Severity” Event Definition	NA
Payload Sampling	(When available.)
Max. Length	Discard, 128 bytes, 256 bytes , 512 bytes, 1 kbyte
Mask Non-Printable Characters	Default: False .

Appendix C: Special Connector Configurations

Certain connectors require additional configuration when used with ArcSight Management Center. This appendix describes the additional configuration. For general information about installing connectors, see ["Adding a Connector" on page 119](#).

The following topics are discussed here:

• Microsoft Windows Event Log - Unified Connectors	307
• Database Connectors	309
• Add a JDBC Driver	310
• API Connectors	311
• File Connectors	312
• Syslog Connectors	312

Microsoft Windows Event Log - Unified Connectors

The SmartConnector for Microsoft Windows Event Log - Unified is not part of a FIPS-compliant solution. When you add a Windows Event Log - Unified connector, be sure the container is not FIPS-enabled in order for the connector to collect events.

When adding a Windows Event Log - Unified connector, follow the specific instructions in the SmartConnector configuration guide for entering parameters, entering security certifications when using SSL, enabling audit policies, and setting up standard user accounts.

There are currently two parser versions for the Microsoft Windows Event Log - Unified SmartConnector.

- Parser Version 0 is generally available with each SmartConnector release
- Parser Version 1 is available with the Microsoft Windows Monitoring content

The Microsoft Windows Event Log - Unified SmartConnector configured for you during initial configuration uses Parser Version 1.

Detailed Security Event mappings for this parser version can be found in Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1 (MSWindowsEventLogUnifiedMappingsParserVersion1.pdf), available on ArcSight [Protect724](#).

When you install additional Microsoft Windows Event Log Unified connectors, they are installed with the generally available base parser version (Parser Version 0). Mappings for the base parser version are available with each SmartConnector release (Security Event Mappings: SmartConnectors for Microsoft Windows Event Log) and can be found on [Protect724](#), along with the SmartConnector configuration guide. You must use Parser Version 1 if you want the default Windows Monitoring content to work. For

details see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified, or SmartConnector Configuration Guide for Microsoft Windows Security Events - Mappings.

Note: The pre-bundled SmartConnector for Microsoft Windows Event Log - Unified installed using the First Boot Wizard is installed with Parser Version 1. Any Windows Event Log - Unified connectors you add using the connector configuration wizard are installed with Parser Version 0 (the base parser).

Change Parser Version by Updating Container Properties

A parser is a SmartConnector component that specifies how to parse the information contained in the device raw events, and how to map it to ArcSight security event schema fields. Parsers can be in the form of property files, map files, or CSV files. Each SmartConnector has its own parser or set of parsers.

Multiple parser versions enables each SmartConnector parse raw events in many different ways to generate ArcSight security events with appropriate mappings. The SmartConnector for Microsoft Windows Event Log -- Unified, supports two parser versions: Base Parser and Parser Version 1.

With multiple parser versions:

- One SmartConnector build supports multiple parser versions.
- Users can configure their connectors to use the available parser versions of their choice, depending on their event mapping requirements.
- Users can reconfigure connectors to use the appropriate parser version as needed.

Multiple parser versions currently are supported only for the SmartConnector for Microsoft Windows Event Log -- Unified. This functionality is not supported for user-developed ArcSight FlexConnectors.

Each SmartConnector has its own internal `fcv.version` parameter setting to represent its current parser version. The default value for the `fcv.version` parameter is the base (or default) parser version, which is Parser Version 0. Each SmartConnector can support a total of 8 parser versions. The `fcv.version` parameter values range from 0 through 7. Microsoft Windows Unified SmartConnector supports parser versions 0 and 1.

Be sure that when you have content with new mappings, you change the parser version to match that content.

To update container properties (located in the `agent.properties` file) to change the parser version being used when mapping events:

1. Click **Manage** from the top-level menu bar.
2. Select a navigation path.
3. Select the container whose properties you want to update. You can select multiple containers.
4. Click **Properties**.
5. Follow the instructions in the wizard to update connector properties.

The `fcv.version` parameter value 0 designates the base parser. To use parser 1, change the `fcv.version` parameter value to 1. For example:

```
agents[0].fcv.version=1
```

SSL Authentication

If you choose to use SSL as the connection protocol, you must add security certificates for both the Windows Domain Controller Service and for the Active Directory Server. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic. With the First Boot Wizard installation of the connector, the certificates are already imported for you. If you add Windows Event Log - Unified connectors, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for instructions.

Database Connectors

The following database connectors are available for installation with ArcSight Express:

- IBM SiteProtector DB*
- McAfee ePolicy Orchestrator DB*
- McAfee Vulnerability Manager DB*
- McAfee Network Security Manager DB*
- Microsoft SQL Server Audit Multiple Instance DB*
- Oracle Audit DB
- Symantec Endpoint Protection DB*
- Trend Micro Control Manager NG DB*
- Snort DB*

*These connectors extract events from an SQL Server or MySQL databases, which requires a JDBC driver. See ["Add a JDBC Driver" on the next page](#) for instructions.

All of these database connectors require the following information when being added to ArcSight Express; some connectors require additional parameters, such as event types or polling frequency.

Parameter	Description
Database JDBC Driver	If you are using an ODBC DRIVER, select 'sun.jdbc.odbc.JdbcOdbcDriver' driver. For JDBC drivers, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver. If you are using an ODBC DRIVER, select 'sun.jdbc.odbc.JdbcOdbcDriver' driver. For JDBC drivers, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
Database URL	If you are using an ODBC DRIVER, enter: 'jdbc:odbc:<ODBC Data Source Name>', where the <ODBC Data Source Name> is the name of the ODBC data source you just created. If you are using a JDBC DRIVER, enter: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>,' substituting actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.
Database User	Enter the login name of the database user with appropriate privilege.
Database Password	Enter the password for the SiteProtector Database User.

Add a JDBC Driver

The IBM SiteProtector DB, McAfee ePolicy Orchestrator DB, McAfee Vulnerability Manager DB, McAfee Network Security Manager DB, Microsoft SQL Server Audit Multiple Instance DB, Symantec Endpoint Protection DB, and Trend Micro Control Manager NG DB connectors extract events from a SQL Server database. For information about and to download the MS SQL Server JDBC Driver, see the Microsoft web site.

Note: Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

The SmartConnector for Snort DB extracts events from a MySQL database.

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as follows:

1. From ArcSight Express, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, and then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the .jar file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (JDBCdriver, for example). Click **Next**.

10. Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
12. Select the container or containers into which the driver is to be uploaded; click **Next**.
13. Click **Done** to complete the process.

Configuration guides for the database connectors supported with ArcSight Express can be found on the [Protect 724](#) community. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Protect 724:

- IBM SiteProtector DB
- McAfee ePolicy Orchestrator DB
- McAfee Vulnerability Manager DB (formerly FoundScan)
- McAfee Network Security Manager DB
- Microsoft SQL Server Multiple Instance Audit DB
- Oracle Audit DB
- Symantec Endpoint Protection DB
- Trend Micro Control Manager DB
- Snort DB

API Connectors

The following API connectors are available for installation with ArcSight Express. They require a client and authentication credentials, as well as configuring the events types to be sent to the connector by the device.

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

For Cisco Secure IPS SDEE, if you want the SmartConnector to validate the Cisco IPS sensor's authentication certificate, obtain the authentication certificate from the IPS sensor and import it to the appliance.

For Sourcefire Defense Center eStreamer, add an eStreamer client, create an authentication certificate, and select event types to be sent to the connector.

See the individual configuration guides for these connectors for instructions.

Follow the instructions in "Uploading Certificates to the Repository" in the Connector Management for ArcSight Express 4.0 User's Guide to import the trusted certificates to ArcSight Express.

Configuration guides for the API connectors supported with ArcSight Express can be found on the Protect 724 community. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Protect 724:

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

File Connectors

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS).

The following File connector is available for installation with ArcSight Express:

- Blue Coat Proxy SG Multiple Server File

See the configuration guide for device setup, parameter configuration, and mappings information for the SmartConnector for Blue Coat Proxy SG Multiple Server File.

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS). For the file-based connectors on a Windows system, configure a CIFS share before you add the connectors.

For information on creating a CIFS Mount or an NFS Mount, see "Managing a Remote File System" in the Connector Management for ArcSight Express 4.0 User's Guide.

Syslog Connectors

If you selected Syslog Daemon during initial installation with the First Boot Wizard, the Syslog Daemon connector has already been installed.

You can add a Syslog File, Pipe, or Daemon connector in a new container. Syslog connectors for the following devices are available with ArcSight Express:

- Cisco PIX/ASA Syslog
- Cisco IOS Router Syslog
- Juniper Network and Security Manager Syslog
- Juniper JUNOS Syslog
- UNIX OS Syslog

Be sure your device is set up to send syslog events. See your device documentation or the SmartConnector Configuration Guide for device configuration information; the guide also includes specific device mappings to ArcSight event fields as well as further information needed for configuration if you are installing the Pipe or File connectors. Mappings in the SmartConnector for UNIX OS Syslog configuration guide apply to all syslog connectors. Specific mappings per device are documented in the configuration guide for the device.

Configuration guides for these syslog connectors supported with ArcSight Express can be found on the Protect 724 community:

- Cisco PIX/ASA Syslog
- Cisco IOS Syslog
- Juniper JUNOS Syslog
- Juniper Network and Security Manager Syslog
- UNIX OS Syslog

Appendix D: Setting Up Your ArcSight Management Center Appliance

This appendix gives instructions on setting up your ArcSight Management Center Appliance for first use.

Preparation

Prior to first use of your ArcSight Management Center appliance, do each of the following:

1. Unpack the appliance and its accompanying accessories.
2. Read carefully through the instructions, cautions, and warnings packaged with the appliance. Failure to do so can result in bodily injury or appliance malfunction.
3. Note and save the rack-mounting instructions included in the package.
4. Redeem your Management Appliance license key by following the instructions in the “Hewlett Packard Enterprise Entitlement Certificate” document. You will need this key to access Management Appliance functionality.
5. Apply for an account on [Protect 724](#), the ArcSight user community. You will need this account to access product documentation and other community-based resources for your ArcSight products.
6. Follow the rack installation instructions (included in your Appliance package) to securely mount the appliance in its rack and make the back panel connections.
7. Do one of the following to enable local access to the Appliance:
 - Connect a keyboard, monitor, and mouse to the ports on the Appliance.
 - Connect a terminal to the serial port on the Appliance using a null modem cable with DB-9 connector. The serial port requires a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control.
8. Power on the appliance.
9. Optionally, enable your appliance for out-of-band remote access. Download, review, and follow the instructions in the HPE ProLiant Integrated Lights-Out User Guide, available at <http://www.hpe.com/go/iLO>.

You are now ready to begin appliance set up.

Setup

During appliance setup, you will do the following:

1. Configure a new IP address for the appliance at the CLI.
2. Accept the End User License Agreement, and then log in to the appliance.
3. Initialize the ArcSight Management Center appliance.

Each of these steps is described in detail below.

Configure a New IP Address

Use the appliance's Command Line Interface (CLI) to configure a new IP address. ArcSight Management Center Appliance ships with the default IP address 192.168.35.35 (subnet mask 255.255.255.0) on Eth0. You will also need to specify a default gateway, hostname, and DNS and NTP servers.

You will need the following information on hand before beginning:

- The new IP address, plus prefix or subnet mask.
- Your default gateway address.
- Your fully-qualified domain name.
- One or more name search domains and server addresses for DNS resolution.
- One or more NTP server addresses.

To configure a new IP address on the CLI:

1. On the CLI, connect to the appliance using these default credentials:

Login: admin

Password: password

2. Enter the new IP address with one of the following commands:

- `set ip eth0 <ip>/<prefix>`, where <ip> is the new IP address and <prefix> is your prefix, OR,
 - `set ip eth0 <ip> <subnetmask>`, where <ip> the new IP address and <subnetmask> is your subnet mask.
3. Enter `set defaultgw <address>`, replacing <address> with your default gateway IP address.
 4. Enter `set hostname <FQDN>`, replacing <FQDN> with the fully-qualified domain name of the host.
 5. Enter `set dns <search_domain_1>, <search_domain_2>...<search_domain_N> <nameserver1> <nameserver2>...<nameserver_N>`, replacing each <search_domain_N> with a search domain, and each <nameserver_N> with the IP address of a nameserver you wish to use for DNS.

6. Enter `set <ntp_server_1> <ntp_server_2>...<ntp_server_N>`, replacing each `<ntp_server_N>` with the IP address of an NTP server you wish to set appliance time.
7. Enter `show config` and review your settings. If any are incorrect, correct them as described in earlier steps.

You are now ready to accept the End User License Agreement.

Accept the End User License Agreement

Upon first connecting to the appliance through a browser, you are prompted to accept the End User License Agreement (EULA).

To accept the EULA:

1. In a browser, connect to the ArcSight Management Center appliance at `https://<IP>`, where `<IP>` is the new IP address you just configured.
2. Review the license.
3. Select the **I accept the terms of the License Agreement** checkbox, and then click **Accept**.
4. Log in as an administrator using the default credentials.

Login:admin

Password:password

You may now initialize the appliance.

Initialize the ArcSight Management Center Appliance

You can now initialize the appliance by uploading the license file; optionally, setting date and time settings; and then changing the admin login credentials to non-default values.

To initialize the appliance:

1. On the **ArcSight Management Center Appliance Configuration** page, in the **License** field, browse for and upload your current license.
2. Click **Save**.
3. Set your date and time settings for the appliance.
4. Change the admin login credentials from their default values. For instructions, see ["Change Password" on page 282](#).

Your ArcSight Management Center appliance is now ready for use.

Appendix E: Restoring Factory Settings

Overview

You can restore an ArcSight Management Center to its factory settings using a built-in utility on the appliance. Restoration applies to new model ArcSight Management Centers as well as former Connector Appliances that have been migrated to ArcSight Management Center.

Restoring an ArcSight Management Center Appliance to factory settings irretrievably deletes all configuration settings. You should back up your configuration settings before performing a factory restore.

The utility used for the factory restore (and resulting appliance image) depends on the type of appliance being restored. Consult the table below to determine the utility to employ.

Appliance Model	System Restore Utility	Resulting Appliance Image
C6600	HPE System Restore	ArcSight Management Center
Any CX500 (including C6500)	HPE System Restore	ArcSight Management Center
CX400 (running RHEL 5.x pre-Migration)	HPE System Restore	ArcSight Management Center
CX400 (running RHEL 6.x pre-Migration)	Acronis True Image	Connector Appliance

Factory Restore Using HPE System Restore

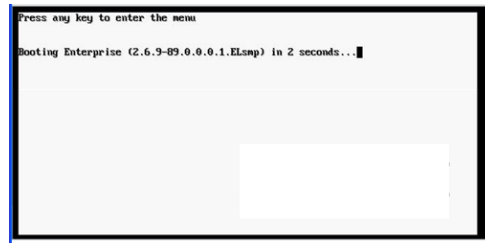
An appliance restored using HPE System Restore will be restored to an ArcSight Management Center image.

To perform a factory restore using HPE System Restore:

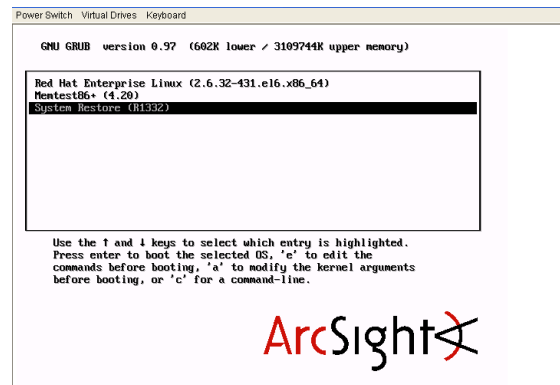
1. Note the IP address, default gateway, and netmask of the appliance.
2. Attach a keyboard, monitor, and mouse directly to the appliance.
3. Reboot ArcSight Management Center from the GUI. Click **Setup > System Admin > Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
4. When the following screen displays, press any key on your keyboard.

Note: This screen is displayed for a very short time. Make sure you press a key on your

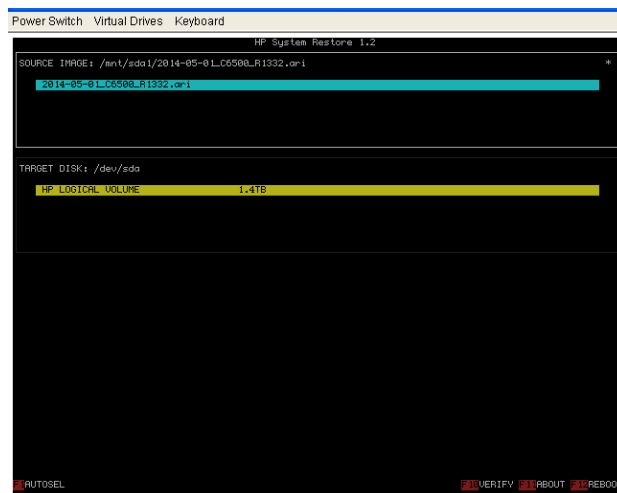
keyboard quickly; otherwise, the appliance continues to boot normally.



5. A screen similar to the one shown below appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press **Enter**. The HPE System Restore utility launches.



6. Press the **F1 (Auto-Select)** key.



7. Press the **F2** key to **Restore** the appliance.
8. When prompted **Proceed with restore?**, press **y**. The restore begins.
9. Allow the restore utility to complete the process.
10. When complete, press **Enter**.
11. Press the **F12** key to reboot the appliance.
12. When prompted **Reboot appliance?**, press **y**. The appliance will be rebooted.

The result of the restore process is a factory restored ArcSight Management Center.

For use, the appliance must now be configured with an IP address, default gateway, and netmask you noted previously. For configuration instructions, see the document *Getting Started with ArcSight Management Center Appliance*, available from ArcSight's online community, [Protect724](#).

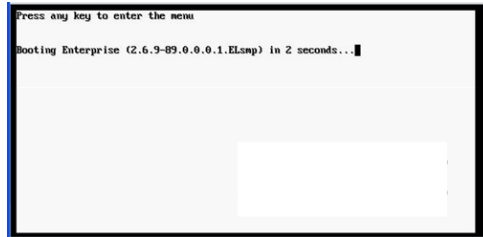
Factory Restore Using Acronis True Image

An appliance restored using Acronis True Image will be restored to a Connector Appliance image.

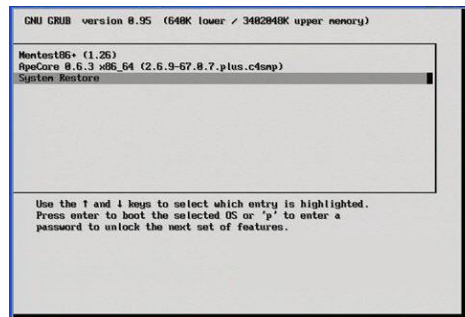
To perform a factory restore using Acronis True Image:

1. Note the IP address, default gateway, and netmask of the appliance.
2. Attach a keyboard, monitor, and mouse directly to the appliance.
3. Reboot ArcSight Management Center from the GUI. Click **Setup > System Admin > Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
4. When the following screen displays, press any key on your keyboard.

Note: This screen is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance continues to boot normally.



5. A screen similar to the one shown below appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press Enter.



6. Click **Acronis True Image Server** to continue.
7. In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press Enter.

8. When the Restore Data Wizard starts, click **Next** to continue.
9. On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.
10. On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.
11. On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** or **sda** (depending on the appliance model) and click **Next**.
12. On the **NT Signature selection for image restoration** page, select how you want the NT signature for the restored disk to be processed and click **Next**.
13. On the **Restored Hard disk Location** page, select the drive to restore (**cciss/c0d0** or **sda**) and click **Next**.
14. On the **Non-empty Destination Hard Disk Drive** page, select **Yes, I want to delete all partitions on the destination hard disk drive before restoring** and click **Next**.
15. On the **Next Selection** page, select **No, I do not** and click **Next** (there are no other partitions or disks to restore).
16. On the **Restoration Options** page, select **Validate backup archive for the data restoration process** if you want to validate the archive before resetting the appliance. Select **Reboot the computer automatically after the restoration is finished** if you want to reboot the appliance automatically. Click **Next**.
17. Review the checklist of operations to be performed and click **Proceed** to begin factory reset. Click **Back** to revisit previous pages.

Caution: Do not interrupt or power down the ArcSight Management Center during the reset process. Interrupting the reset process can force the system into a state from which it cannot recover.

Progress bars show the status of the current operation and the total progress.

18. When you see a message indicating that the data was restored successfully, click **OK**.
19. If you specified automatic reboot previously, the appliance reboots when the reset is complete. Otherwise, reboot manually.

The result of the restore process is a factory restored Connector Appliance.

For use, the appliance must now be configured with an IP address, default gateway, and netmask you noted previously. For configuration instructions, see the document *Getting Started with Connector Appliance*, available from ArcSight's online software community, [Protect724](#).

Appendix F: SuperSchema

The following comprises the superschema used by the CEF to Avro (c2a) stream processor in Event Broker.

Field Name	Data Type	Length
agentAddress	VARCHAR	16
agentDnsDomain	VARCHAR	255
agentHostName	VARCHAR	1023
agentId	VARCHAR	40
agentMacAddress	VARCHAR	DEFINE DEFAULT
agentReceiptTime	DATE	
agentSeverity	VARCHAR	DEFINE DEFAULT
agentTimeZone	VARCHAR	255
agentTranslatedAddress	VARCHAR	DEFINE DEFAULT
agentTranslatedZoneURI	VARCHAR	2048
agentType	VARCHAR	63
agentVersion	VARCHAR	31
agentZoneURI	VARCHAR	2048
applicationProtocol	VARCHAR	40
baseEventCount	INT	
bytesIn	Long	
bytesOut	Long	
categoryDeviceGroup	VARCHAR	1023
categoryDeviceType	VARCHAR	1023
categoryObject	VARCHAR	1023
categoryOutcome	VARCHAR	1023
categorySignificance	VARCHAR	1023
categoryTechnique	VARCHAR	1023
cryptoSignature	VARCHAR	512
customerURI	VARCHAR	2048

Field Name	Data Type	Length
destinationAddress	VARCHAR	16
destinationDnsDomain	VARCHAR	255
destinationGeoLocationInfo	VARCHAR	1023
destinationHostName	VARCHAR	1023
destinationMacAddress	VARCHAR	DEFINE DEFAULT
destinationNtDomain	VARCHAR	255
destinationPort	INT	
destinationProcessId	INT	
destinationProcessName	VARCHAR	1023
destinationServiceName	VARCHAR	1023
destinationTranslatedAddress	VARCHAR	16
destinationTranslatedPort	INT	
destinationTranslatedZoneURI	VARCHAR	2048
destinationUserId	VARCHAR	1023
destinationUserName	VARCHAR	1023
destinationUserPrivileges	VARCHAR	1023
destinationZoneURI	VARCHAR	2048
deviceAction	VARCHAR	63
deviceAddress	VARCHAR	16
deviceAssetId	VARCHAR	DEFINE DEFAULT
deviceCustomDate1	DATE	
deviceCustomDate1Label	VARCHAR	1023
deviceCustomDate2	DATE	
deviceCustomDate2Label	VARCHAR	1023
deviceCustomDescriptorId	VARCHAR	DEFINE DEFAULT
deviceCustomFloatingPoint1	FLOAT	
deviceCustomFloatingPoint1Label	VARCHAR	1023
deviceCustomFloatingPoint2	FLOAT	
deviceCustomFloatingPoint2Label	VARCHAR	1023
deviceCustomFloatingPoint3	FLOAT	

Field Name	Data Type	Length
deviceCustomFloatingPoint3Label	VARCHAR	1023
deviceCustomFloatingPoint4	FLOAT	
deviceCustomFloatingPoint4Label	VARCHAR	1023
deviceCustomIPv6Address1	VARCHAR	DEFINE DEFAULT
deviceCustomIPv6Address1Label	VARCHAR	1023
deviceCustomIPv6Address2	VARCHAR	DEFINE DEFAULT
deviceCustomIPv6Address2Label	VARCHAR	1023
deviceCustomIPv6Address3	VARCHAR	DEFINE DEFAULT
deviceCustomIPv6Address3Label	VARCHAR	1023
deviceCustomIPv6Address4	VARCHAR	DEFINE DEFAULT
deviceCustomIPv6Address4Label	VARCHAR	1023
deviceCustomNumber1	LONG VARCHAR	
deviceCustomNumber1Label	VARCHAR	1023
deviceCustomNumber2	LONG VARCHAR	
deviceCustomNumber2Label	VARCHAR	1023
deviceCustomNumber3	LONG VARCHAR	
deviceCustomNumber3Label	VARCHAR	1023
deviceCustomString1	VARCHAR	4000
deviceCustomString1Label	VARCHAR	1023
deviceCustomString2	VARCHAR	4000
deviceCustomString2Label	VARCHAR	1023
deviceCustomString3	VARCHAR	4000
deviceCustomString3Label	VARCHAR	1023
deviceCustomString4	VARCHAR	4000
deviceCustomString4Label	VARCHAR	1023
deviceCustomString5	VARCHAR	4000
deviceCustomString5Label	VARCHAR	1023
deviceCustomString6	VARCHAR	4000
deviceCustomString6Label	VARCHAR	1023
deviceDirection	VARCHAR	DEFINE DEFAULT

Field Name	Data Type	Length
deviceDnsDomain	VARCHAR	255
deviceDomain	VARCHAR	1023
deviceEventCategory	VARCHAR	1023
deviceEventClassId	VARCHAR	100
deviceExternalId	VARCHAR	255
deviceFacility	VARCHAR	1023
deviceHostName	VARCHAR	100
deviceInboundInterface	VARCHAR	128
deviceMacAddress	VARCHAR	DEFINE DEFAULT
deviceNtDomain	VARCHAR	255
deviceOutboundInterface	VARCHAR	128
devicePayloadId	VARCHAR	128
deviceProcessId	INT	
deviceProcessName	VARCHAR	1023
deviceProduct	VARCHAR	100
deviceReceiptTime	DATE	
deviceSeverity	VARCHAR	63
deviceTimeZone	VARCHAR	255
deviceTranslatedAddress	VARCHAR	DEFINE DEFAULT
deviceTranslatedZoneURI	VARCHAR	2048
deviceVendor	VARCHAR	100
deviceVersion	VARCHAR	16
deviceZoneURI	VARCHAR	2048
endTime	VARCHAR	DEFINE DEFAULT
eventId	Long	DEFINE DEFAULT
eventOutcome	VARCHAR	63
externalId	VARCHAR	40
fileCreateTime	DATE	
fileHash	VARCHAR	255
fileId	VARCHAR	1023

Field Name	Data Type	Length
fileModificationTime	DATE	
fileName	VARCHAR	1023
filePath	VARCHAR	1023
version		
filePermission	VARCHAR	1023
fileSize	LONG	
fileType	VARCHAR	1023
flexDate1	DATE	
flexDate1Label	VARCHAR	128
flexNumber1	LONG	
flexNumber1Label	VARCHAR	128
flexNumber2	LONG	
flexNumber2Label	VARCHAR	128
flexString1	VARCHAR	1023
flexString1Label	VARCHAR	128
flexString2	VARCHAR	1023
flexString2Label	VARCHAR	128
locality	VARCHAR	DEFINE DEFAULT
message	VARCHAR	1023
name	VARCHAR	DEFINE DEFAULT
oldFileCreateTime	DATE	
oldFileHash	VARCHAR	255
oldFileId	VARCHAR	1023
oldFileModificationTime	DATE	
oldFileName	VARCHAR	1023
oldFilePath	VARCHAR	1023
oldFilePermission	VARCHAR	1023
oldFileSize	LONG	
oldFileType	VARCHAR	1023
rawEvent	VARCHAR	4000

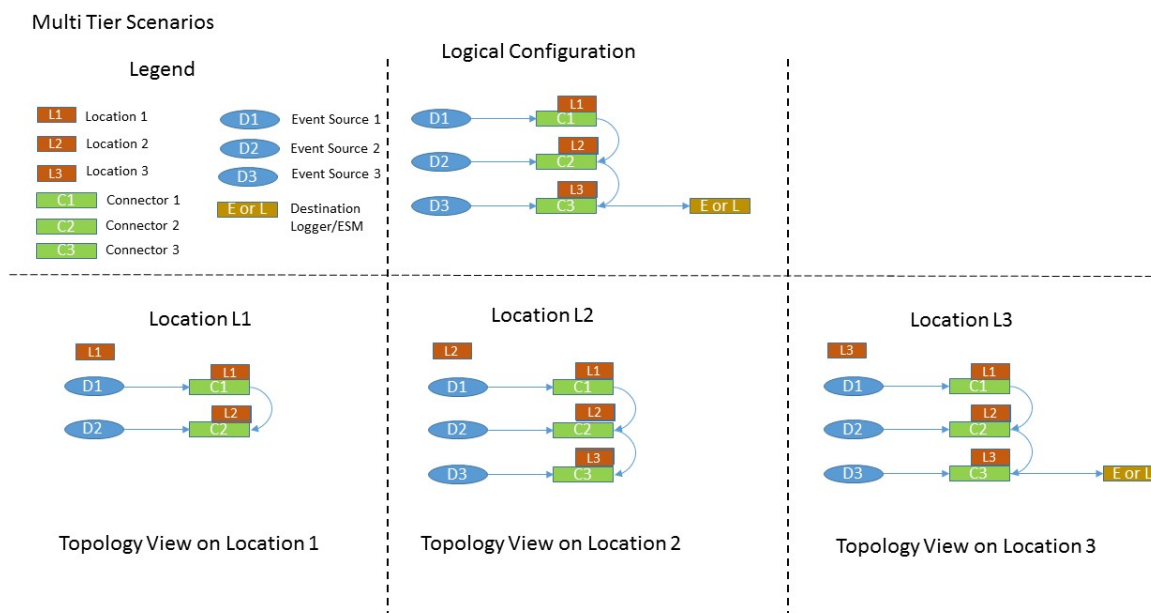
Field Name	Data Type	Length
reason	VARCHAR	1023
requestClientApplication	VARCHAR	1023
requestContext	VARCHAR	2048
requestCookies	VARCHAR	1023
requestMethod	VARCHAR	1023
requestUrl	VARCHAR	1023
requestUrlFileName	VARCHAR	1023
requestUrlQuery	VARCHAR	1023
severity	INT	
sourceAddress	VARCHAR	DEFINE DEFAULT
sourceDnsDomain	VARCHAR	255
sourceGeoLocationInfo	VARCHAR	1023
sourceHostName	VARCHAR	1023
sourceMacAddress	VARCHAR	DEFINE DEFAULT
sourceNtDomain	VARCHAR	255
sourcePort	INT	
sourceProcessId	INT	
sourceProcessName	VARCHAR	1023
sourceServiceName	VARCHAR	1023
sourceTranslatedAddress	VARCHAR	DEFINE DEFAULT
sourceTranslatedPort	INT	
sourceTranslatedZoneURI	VARCHAR	2048
sourceUserId	VARCHAR	1023
sourceUserName	VARCHAR	1023
sourceUserPrivileges	VARCHAR	1023
sourceZoneURI	VARCHAR	2048
startTime	DATE	
transportProtocol	VARCHAR	31
type	VARCHAR	DEFINE DEFAULT

Appendix G: The Topology View and Unmanaged Devices

This section details various scenarios for the inclusion of devices not managed by ArcMC in your network, and the effect of each scenario on the ArcMC Topology View. Particularly when connectors (or Collectors) are chained together in a multi-tier configuration, unmanaged products can block the view from their immediate downstream neighbor.

Scenario 1: No Unmanaged Devices

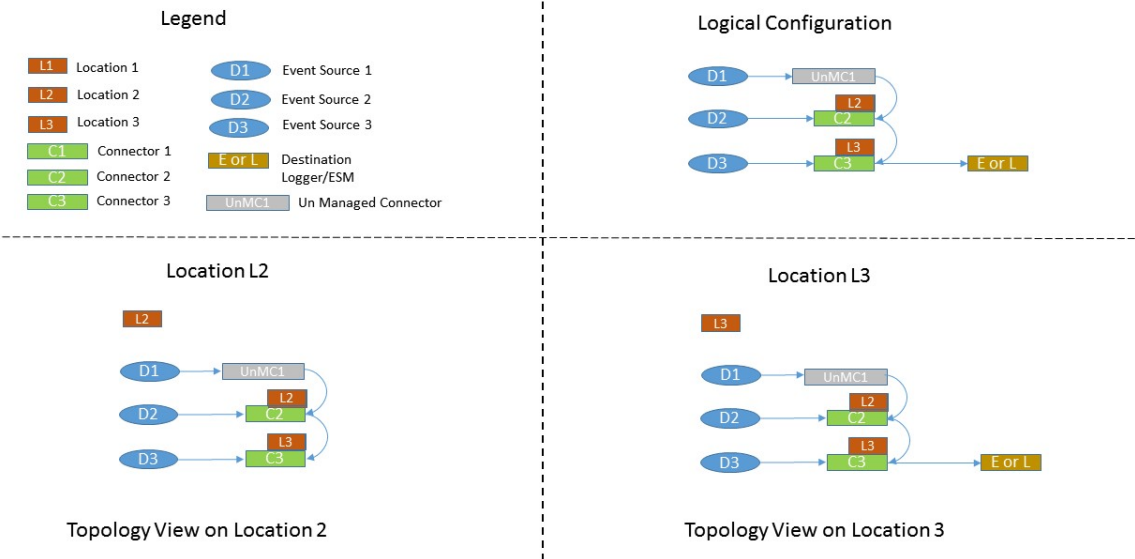
In this scenario, no unmanaged products are included in the network. As a result, the ArcMC Topology view is unimpeded and gives an accurate picture of the logical topology as viewed from any location.



Scenario 2: Unmanaged Connector in Location L1

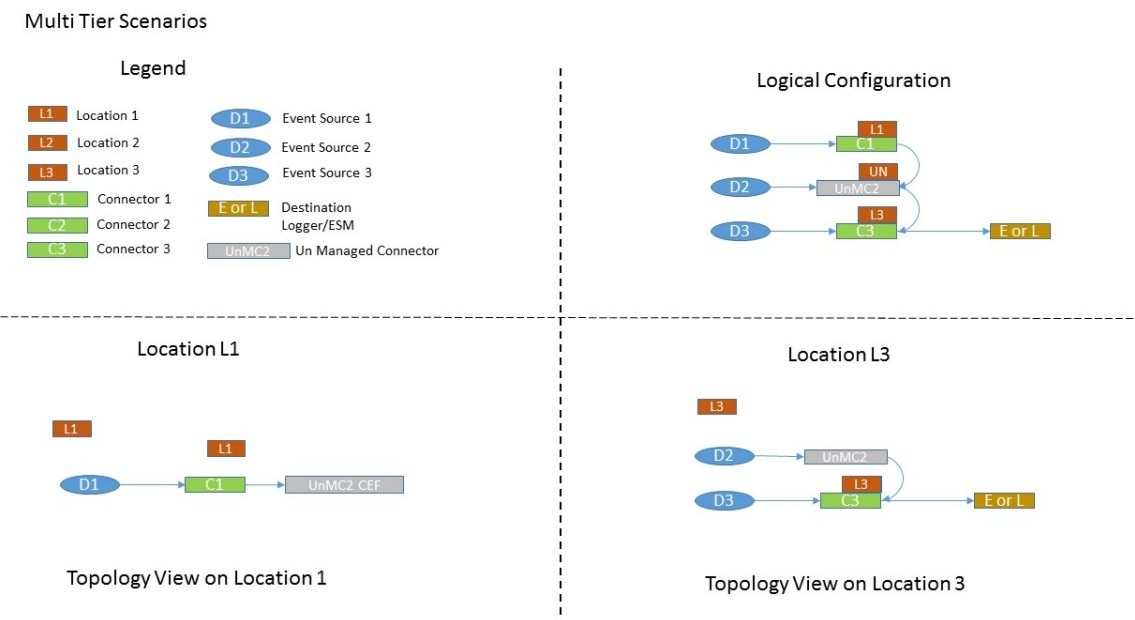
This scenario shows an unmanaged connector in location L1 and the results on the Topology View as seen from locations L2 and L3. No view is seen from L1, since it does not include any managed nodes. The view at the other downstream locations is as expected.

Multi Tier Scenarios



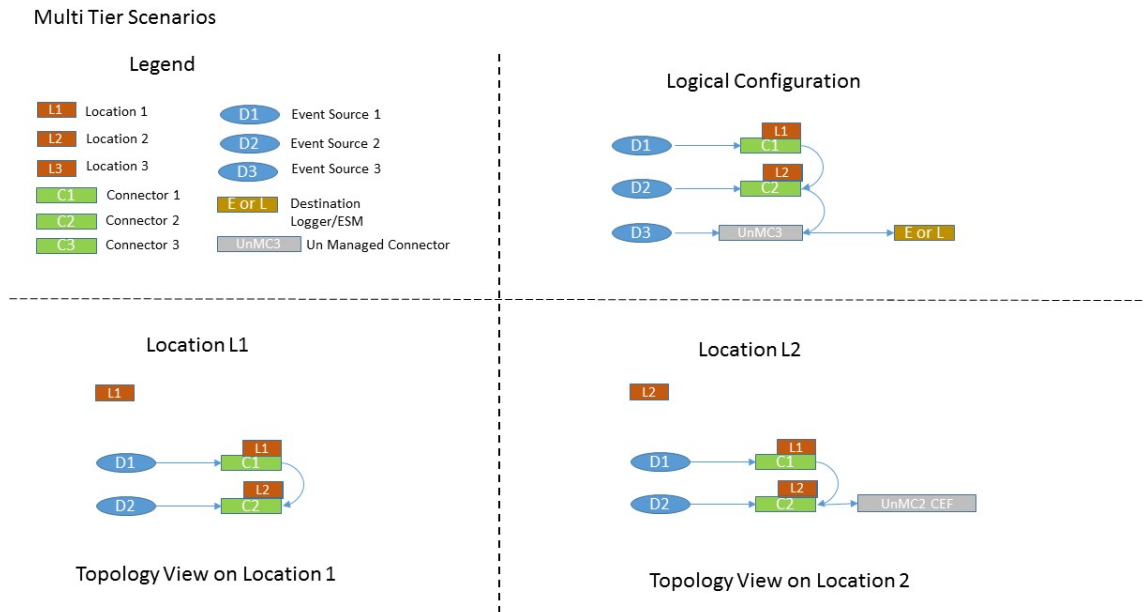
Scenario 3: Unmanaged Connector in Location L2

In this scenario, an unmanaged connector is located in Location L2 and chained to connectors in locations L1 and L2. This blocks the Topology view of L1 as seen from L3. In addition, the destination Logger or ESM shows no traffic from L1.



Scenario 4: Unmanaged Connector in Location L3

In this scenario, an unmanaged connector is in Location L3. This impedes an accurate Topology view of location 3. In fact, no traffic from locations L1 and L2 is shown for the destination Logger/ESM.



To get the most complete and accurate topological view, you are strongly encouraged to use ArcMC to manage all supported connectors (or Collectors) included in your logical topology.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Administrator's Guide (ArcSight Management Center 2.7x)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!