Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Dell EMC Unity and VNXe Storage

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Dell EMC Unity and VNXe Storage

October 17, 2017

Copyright © 2010 – 2017 Hewlett Packard Enterprise Development LP

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 Development LP shall not be liable for technical or editorial 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. Hewlett Packard Enterprise Development LP 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 Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
02/15/2017	Renamed connector from EMC VNXe Storage Systems; changed Device Vendor to 'Dell EMC' and Device Product to 'Unity'. Added mappings for Device Custom Number 1, Bytes In, Bytes Out, and Event Outcome. Added IPv6 support.
11/30/2016	Updated installation procedure for setting preferred IP address mode and for downloading Microsoft Visual C++ Redistributable.
09/30/2013	Formerly "SmartConnector for EMC Celerra Event Publishing Agent", renamed "SmartConnector for EMC VNXe Series Storage Systems". Added VNXe Storage Systems V7.1 support.
05/15/2012	Added new installation procedure.
09/24/2010	General availability of this connector. Updated Windows versions supported.
06/25/2010	First edition of this Configuration Guide.

Contents

Product Overview 4
Configuration Overview 4
Unity and VNXe Configuration 5
Download CEE Software 5
Install the CEE Software 5
Complete the CEE Installation for Windows Server 6
Set Up Consumer Application Access 7
Unity Configuration 8
Enable Event Logging on the SMB/CIFS File System 8
Enable Event Logging for the NAS Server 8
Configure Event Publishing 9
Check CEPA Server Status 12
VNXe Configuration 14
Configure the Event Publishing Agent 14
Manage the Event Publishing Agent 17
Edit the cepp.conf File 17
Start the CEPA Facility 17
Verify the CEPA Status 17
Stop the CEPA Facility 17
Display the CEPA Facility Properties 18
Install the SmartConnector 18
Download Microsoft Visual C++ Redistributable 18
Prepare to Install Connector 18
Install Core Software 19
Set Global Parameters (optional) 19
Select Connector and Add Parameter Information 20
Select a Destination 21
Complete Installation and Configuration 22
Run the SmartConnector 22
Device Event Mapping to ArcSight Fields 22

SmartConnector for Dell EMC Unity and VNXe Storage

This guide provides information for installing the SmartConnector for Dell EMC Unity Storage and configuring the device for event collection. This connector is supported for installation on Windows Server platforms as listed in the SmartConnector Platform Support document. (https://www.protect724.hpe.com/docs/DOC-2281)

The connector works with EMC Unity Storage using the EMC Common Event Enabler for Windows for CIFS audit event collection. Events can also be collected from VNXe storage systems. NFS is not supported by this connector.

Product Overview

Dell Unity Storage comprises Dell EMC UnityVSA virtual storage appliances as well as Unity All-Flash and Hybrid Flash storage devices.

The EMC Common Event Enabler (CEE) framework is used to provide a working environment for the Common Event Publishing Agent (CEPA), which is a facility that resides within the Common Event Enabler (CEE) framework. CEPA delivers both event notification and associated context in one message to the SmartConnector.

The EMC VNXe Series Storage Systems delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata needed to decide business policy.

Configuration Overview

For both Unity and VNXe, configuration includes:

- Installing the Common Event Enabler for Windows
- Setting Up Consumer Application Access

For Unity, further configuration includes:

- Enabling SMB/CIFS Event Logging
- Enabling NAS Server Event Logging
- Configuring Event Publishing

See “Unity Configuration” for these procedures. For complete information about installing, using, and managing the Common Event Enabler for Windows, see the *EMC CEE Using the Common Event Enabler for Windows*.

For VNXe, further configuration includes:

- Configuring the Event Publishing Agent
- Managing the Event Publishing Agent

See “VNXe Configuration” for these procedures. For complete information about installing, using, and managing EMC VNXe Series Storage Systems, see the following EMC Technical Manuals, from which the information in VNXe Configuration has been derived:

- Using VNX™ Event Enabler, P/N 300-011-824
- Using EMC Celerra Event Publishing Agent, P/N 300-006-003
- Using Celerra Event Enabler, P/N 300-006-002

Unity and VNXe Configuration

This section includes:

- Downloading CEE Software
- Installing the CEE Software
- Completing CEE Installation
- Setting Up Consumer Application Access

Download CEE Software

Download the CEE framework software from EMC Online Support:

1. Open a browser window and navigate to https://Support.EMC.com.
2. In the Search EMC Support text box, enter **CEE** and click the Search magnifying glass.
3. Look for the Common Event Enabler <version number> for Windows program file in the list.
4. Click the download icon and save the file.
5. From the iso file, extract the 32-bit or 64-bit EMC_CEE_Pack executable file that you need.

Install the CEE Software

For VNX, before beginning, synchronize the date/time stamps on VNX file systems and domain servers by running the following command:

```
server_date server_# -timesvc start ntp <domain controller ip>
```

Have the following information available to install the Common Event Enabler:

- Account name and password of the user account with local administrator privileges to set up a CEPA account on domain server where CEE will be installed.
- IP address of the Windows Server available where CEE will be installed.
- Domain name and IP address of the Windows domain server.

- IP address of the CIFS server configured for use with the Windows domain server
- File systems names

To install the CEE software:

1. Log in to the domain as an administrator.
2. Run the EMC_CEE_Pack executable file for either the 32-bit (_WIN32) or the 64-bit (_X64) version of the software. Click **OK** to start the InstallShield Wizard.

   The **Welcome** window is displayed. If you have the most current version of InstallShield, the License Agreement window is displayed; skip to step 6. If you do not have the most current version of InstallShield, you are prompted to install it. Continue with step 4.
3. Click **Next**. The **Location to Save Files** window is displayed.
4. Click **Next**.

Do not change the location of the temporary directory. The Extracting Files process runs and returns to the **Welcome to the InstallShield Wizard** window.

5. Click **Next**. The **License Agreement** window is displayed. Click **I accept the terms in the license agreement**, and click **Next**.
6. On the **Customer Information** window displayed, enter a username and organization and click **Next**.
7. On the **Setup Type** window displayed, select **Complete** and then click **Next**. The **Symantec SAV for NAS** window is displayed.
8. If you are using Symantec antivirus software, select **Work with Symantec SAV for NAS** and the option for the SAV version you are using; otherwise, click **Next**. The **Ready to Install the Program** window is displayed.
9. Click **Install**. After the program is installed, the **InstallShield Wizard Completed** window is displayed.
10. Click **Finish**. The **Event Enabler Installer Information** window is displayed and prompts you to restart the server.
11. Click **No**. You will restart the computer during the next procedure. Continue with "Complete the CEE Installation for Windows Server."

Complete the CEE Installation for Windows Server

1. From the Windows taskbar, click **Start -> Settings -> Control Panel -> Administrative Tools -> Services**.
2. Double-click **EMC CAVA** in the **Service** list. The **EMC CAVA Properties** window is displayed.
3. From the **EMC CAVA Properties** window, click **Log On**.

4 Select **This account** and click **Browse**. The **Select User** window is displayed.

5 On the **Select User** window, navigate to the domain where the account for the administrative user who has rights to set up a CEPA server account exists, select the domain location, and click **OK**. The **Select User** window now contains the location.

6 Click **Advanced**.

7 Click **Find Now**.

8 Select the user account that was created to manage CEPA services from the list and click **OK**.

9 For this user account, enter the account's password in both the **Password** and **Confirm password** fields.

10 Click **OK**; the following message is displayed:

```
The new logon name will not take effect until you stop and restart the
service.
```

11 Click **OK**.

12 Restart the computer.

Set Up Consumer Application Access

The SmartConnector should reside on the same local Windows computer where the CEE is installed.

To set up consumer application access:

1 Open a command window on the Windows server where the consumer application is installed and enter `regedit`. The Windows Registry Editor window is displayed.

2 Navigate to **HKEY_LOCAL_MACHINE -> SOFTWARE -> EMC -> CEE -> CEPP -> Audit -> Configuration**.

3 Double-click **EndPoint**.

4 Enter `ArcSightConnector`.

5 Double-click **Enable**.

6 Enter **1** to enable the CEPA function that supports the consumer application being used.

7 Restart the computer.

Any time you modify the CEE section of the Registry, except for Verbose and Debug, the EMC CAVA service must be restarted.

See *EMC CEE Using the Common Event Enabler for Windows* for complete information.

Unity Configuration

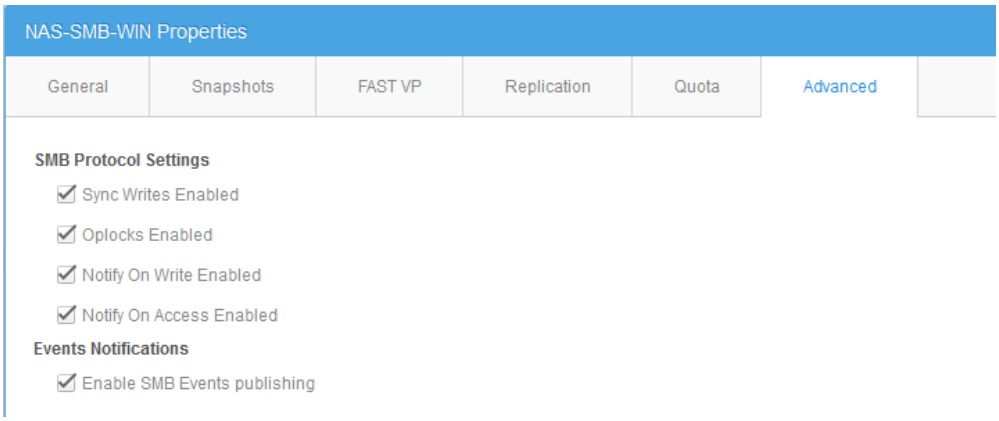
For complete information about installing, using, and managing the Common Event Enabler for Windows, see the *EMC CEE Using the Common Event Enabler for Windows*.

This section includes instructions for:

- Enabling SMB/CIFS Event Logging
- Enabling NAS Server Event Logging
- Configuring Event Publishing
- Checking CEPA Server Status

Enable Event Logging on the SMB/CIFS File System

1. Log in to Unisphere.
2. Select **File** in the left pane under **STORAGE**.
3. Select the **File Systems** tab.
4. Click on the **Advanced** tab.
5. Under **Events Notification**, check **Enable SMB events publishing**.



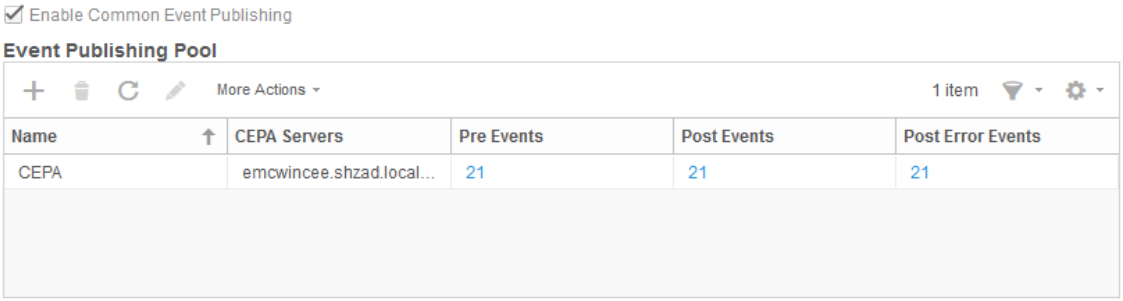
6. Click **Apply**.

Enable Event Logging for the NAS Server

1. Log in to Unisphere VSA.
2. Select **File** in the left pane under **STORAGE**.
3. Select the **NAS Servers** tab.
4. Select the NAS Sever name and click on the edit icon.

5 In the NAS Server Properties window, select the **Protection & Events** tab.

6 Check **Enable Common Event Publishing**.



7 Click **Apply**.

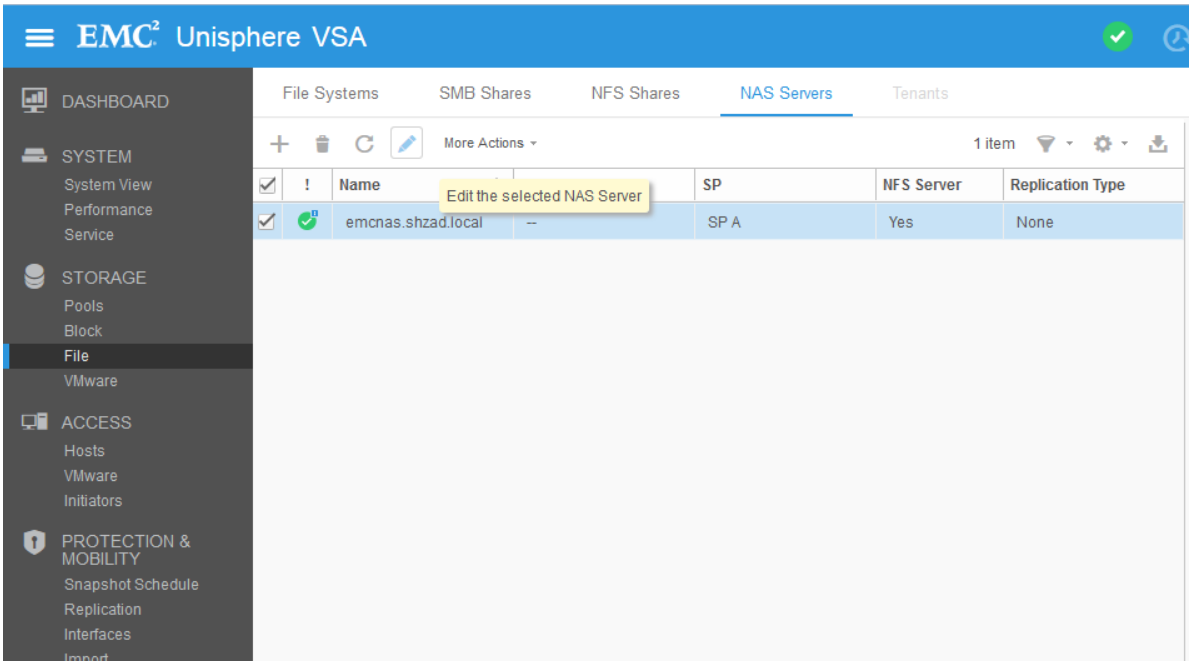
Configure Event Publishing

You can configure and manage Event Publishing for your NAS server through Unisphere.

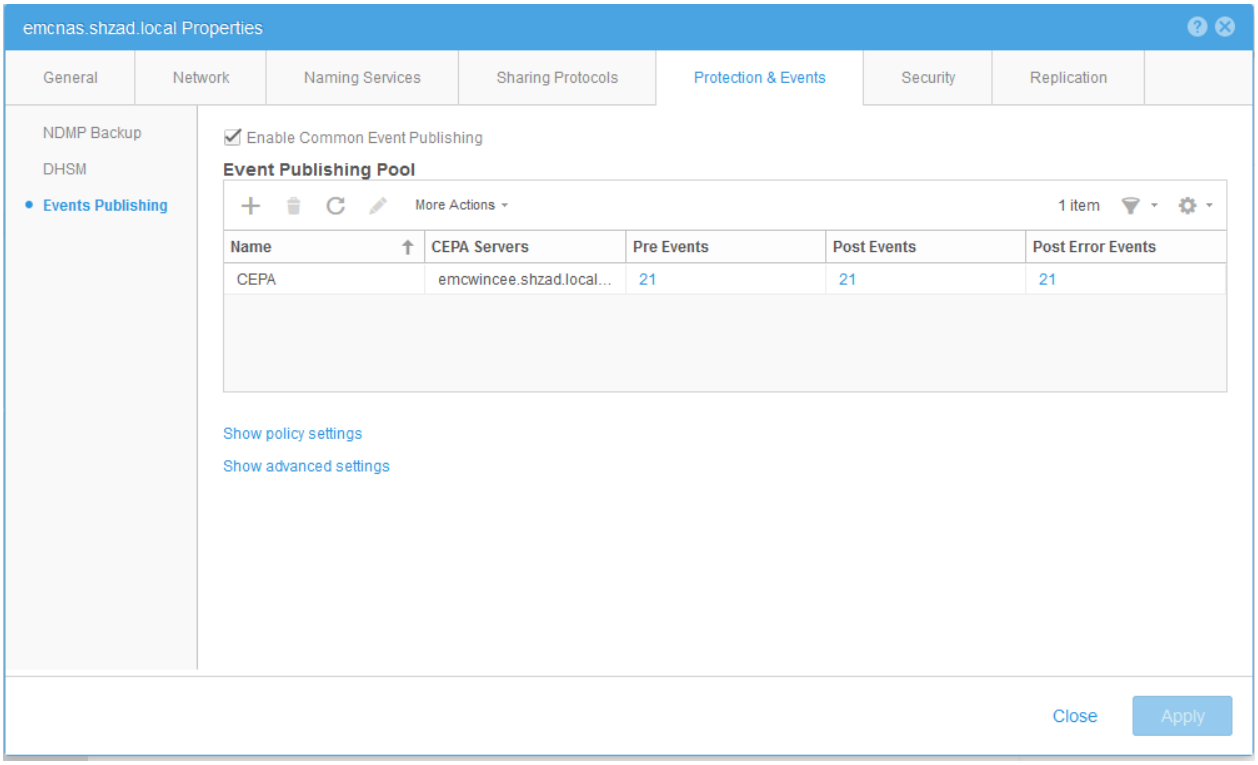
1 After logging in, select **File** under **STORAGE** in the left pane. Select the **NAS Servers** tab.

2 Select the NAS sever.

3 Click the edit icon to edit the properties for the selected server. The server properties window is displayed.

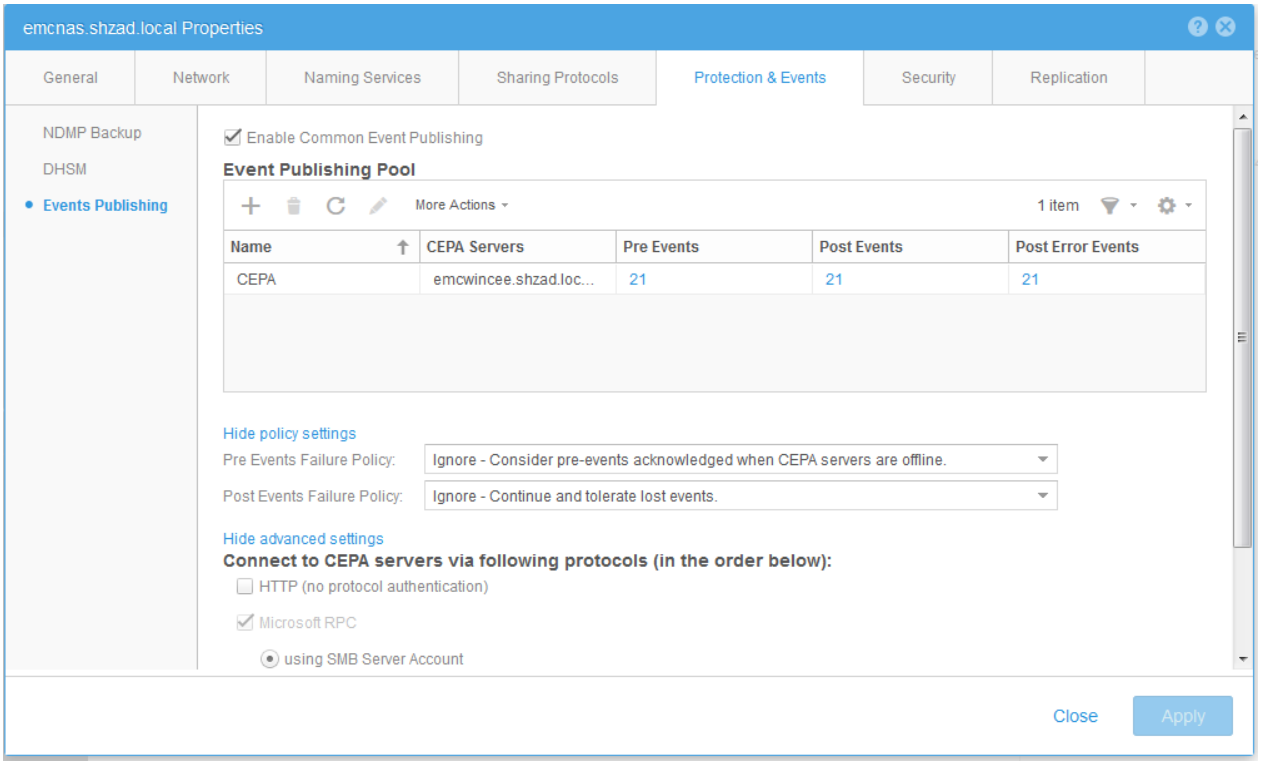


4 Select the **Protection & Events** tab, and select **Events Publishing** from the left pane.



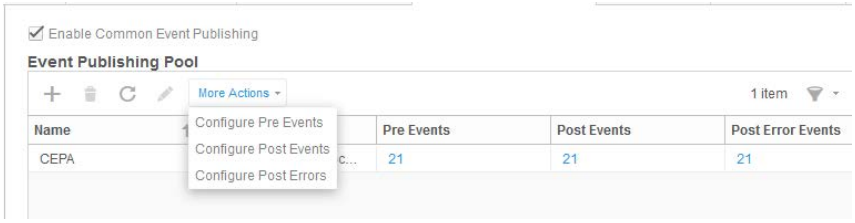
5 Populate the Event Publishing Pool by clicking the plus sign (+) to add the CEPA servers from which events are to be collected.

You can click **Show policy settings** and **Show advanced settings** to edit policies and protocols for the selected server.

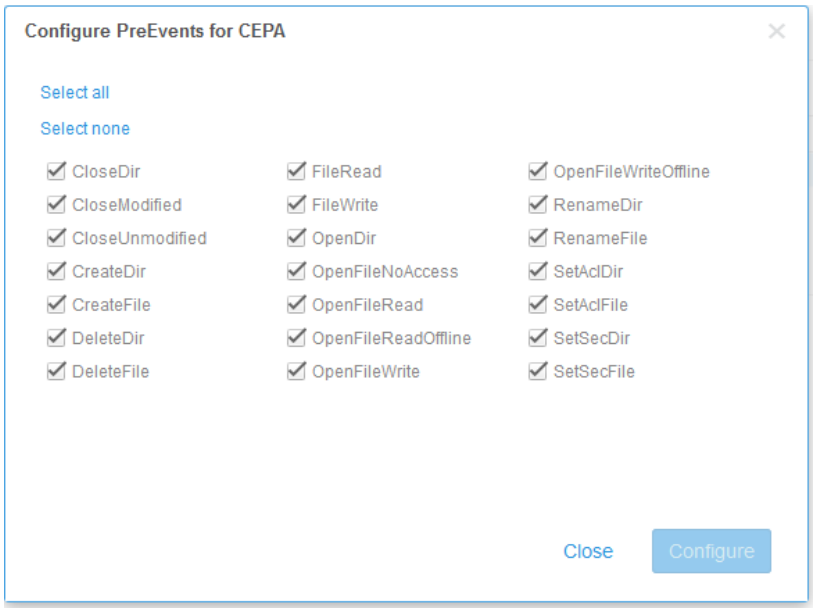


Only the Microsoft RPC protocol is supported for connecting to CEPA servers.

6 To configure the types of events collected, select the CEPA server name and select **Configure Pre Events**, **Configure Post Events**, or **Configure Post Error Events** from the **More Actions** drop-down selection.

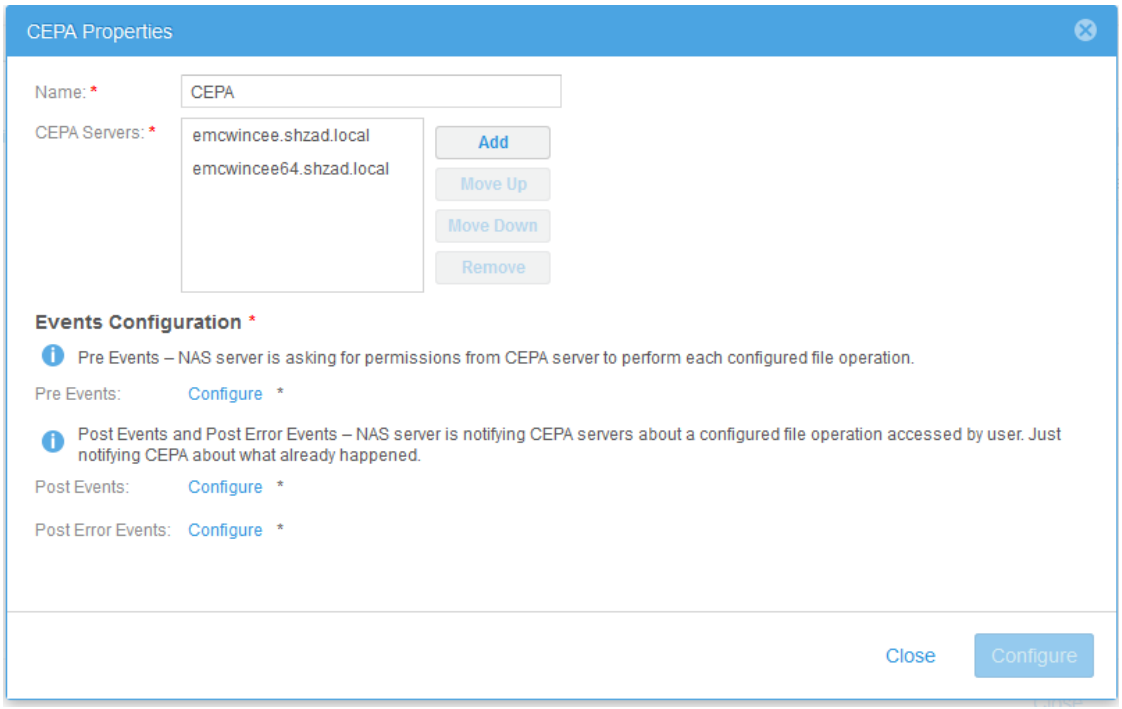


A window such as the following is displayed:



You can choose to **select all events** or check events individually to select them. No events will be collected if you choose **select none**.

You also can access the event configuration windows from the CEPA Properties window (select the CEPA server name and click the edit tool).



Check CEPA Server Status

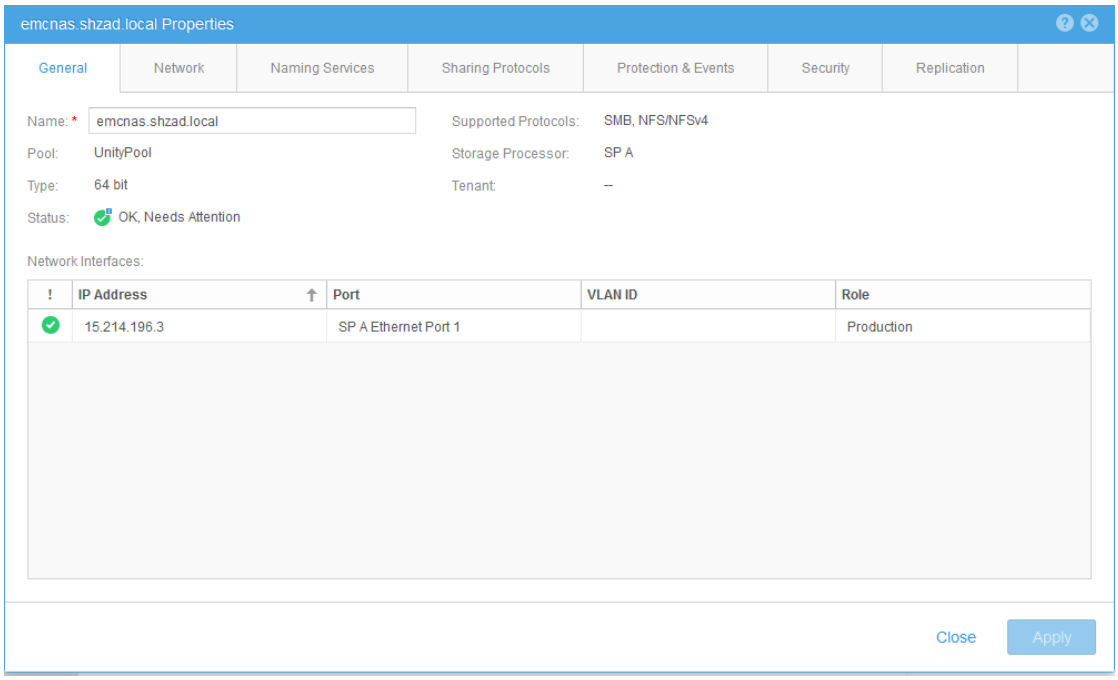
To check the status of the server:

1 Click **File** under **STORAGE** in the left pane.

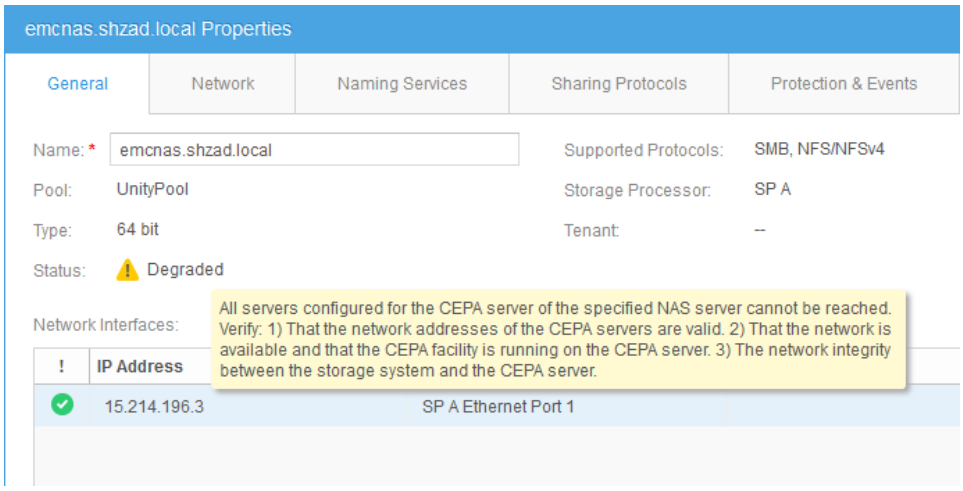
2 Select the **NAS Servers** tab.

3 Select a server and click the edit icon.

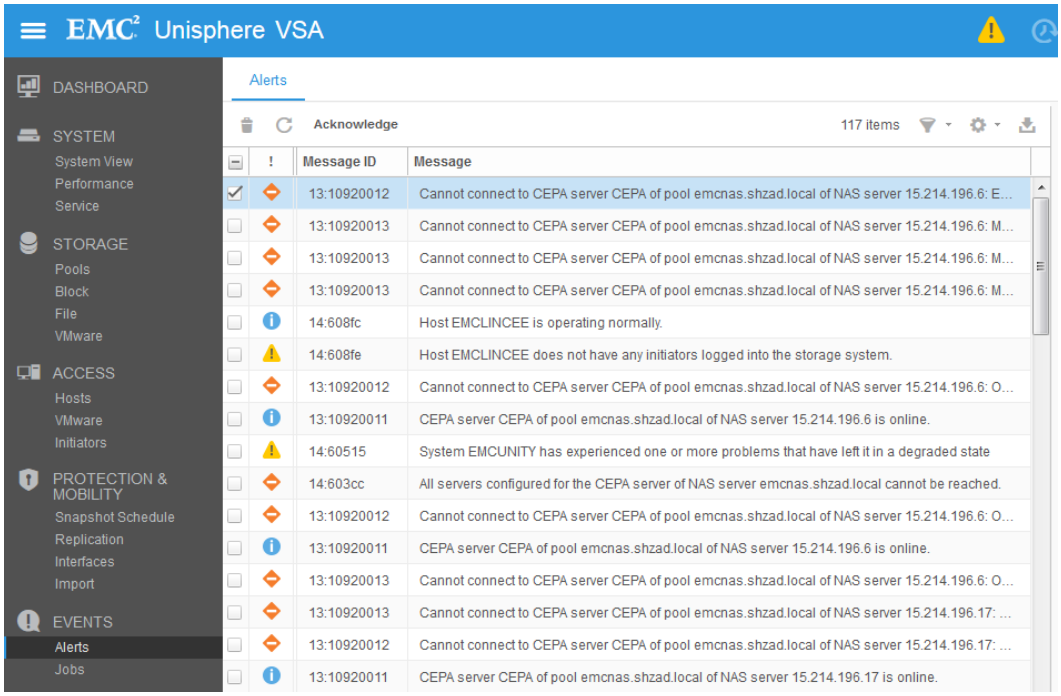
The **Status** is shown on the **General** tab.



Move your mouse over the status to see a description; for example:



You can also check CEPA server status by selecting **Alerts** under **EVENTS** in the left pane.



VNXe Configuration

VNXe configuration includes:

- Configuring the Event Publishing Agent
- Managing the Event Publishing Agent

Configure the Event Publishing Agent

The `cepp.conf` file must be defined with the correct syntax to ensure that the EMC CAVA service starts on the Data Mover. To create the `cepp.conf` file:

1 Log into the system with your administrative username and password:

```
login: <username>
password: <password>
```

where <username> is the username defined for the administrative account (default is **nasadmin**) and <password> is the password defined for the administrative account (default is **nasadmin**).

2 Use a text editor to create a new, blank file in the home directory.

3 Add the CEPA information necessary for your system. This can be on one line or on separate lines by using a space and "\" at the end of each line except for the last line and the lines that contain global options (`cifsserver`, `surveytime`, `ft`, and `msrpcuser`). For example:

```
cifsservers=<cifsserver>
surveytime=<surveytime>
```

```
ft level = [0|1|2|3]  {location=<location>} {size=<size>}
msrpcuser=<msrpcuser>
pool name=<poolname> \
servers=<IP_addr1>|<IP_addr2>| ... \
preevents=<event1>|<event2>| ... \
postevents=<event3>|<event4>| ... \
posterrevents=<event5>|<event6>| ... \
option=ignore or denied \
reqtimeout=<reqtimeout> \
retrytimeout=<retrytimeout>
```

where:

<cifsserver> is the name of the CIFS server used by event publishing agent to access the files in the Celerra Network Server. If you do not include this option, the default CIFS server will be used. If you include this option, the server specified must be a physical Data Mover, not a Virtual Data Mover, in order for the EMC CAVA service to start on the Data Mover.

The use of link-local network addresses for defining CEPA servers is not supported.

<surveytime> is the time to scan each EMC VNXe Series Storage Systems server. The default is 60 seconds and the range is 5 seconds through 120 seconds.

The global ft option has three parts:

- <level> is the fault tolerance level assigned. This option is required. 0 = continue and tolerate lost events (the default); 1 = continue and use a persistence file as a circular event buffer for lost events; 2 = continue and use a persistence file as a circular event buffer for lost events until the buffer is filled and then stop CIFS; 3 = upon heartbeat loss of connectivity, stop CIFS.

- <location> is the directory where the persistence buffer file resides relative to the root of a file system. If a location is not specified, the default location is the root of the file system.

File system that contains the persistence buffer file must have amount of free space available equal to the maximum size of the persistence buffer file. For example, if the persistence buffer file size is 100 MB, the file system must contain at least 100 MB of free space for the temporary file operations.

- <size> is the maximum size in MB of the persistence buffer file. The default is 1 MB and the range is 1 MB to 100 MB.

<msrpcuser> is the name assigned to the user account that the EMC CAVA service is running under on the VEE or CEE machine. For example, if the EMC CAVA service is running under a user called **ceeuser**, the cepp.conf file entry would be **msrpcuser=ceeuser**. If ceeuser is a member of a domain, the entry would be **msrpcuser=domain.ceeuser**.

<poolname> is the name assigned to the set of Windows servers where the VEE or CEE software is installed. The specified Data Mover will use the set of servers to perform round-robin load sharing of events. One pool name must be specified.

<IP_addrx> are the IP addresses of the Windows servers where the VEE or CEE software is installed, or a fully qualified domain name (FQDN). At least one Windows server must be specified. Use the vertical bar (|) or a colon (:) when listing multiple addresses. Note that, if you use a FQDN and the Data Mover cannot retrieve the IP address for it, add the FQDN to the `/.etc/hosts` list in the Data Mover.

IPv6 addresses should be enclosed in square brackets to separate them from the colon delimiter that is used between multiple addresses.

<eventx> are events for which notifications are to be received. At least one error option line (pre, post, or posterr) from the following options must be defined.

```
* (all events), blank (no events), OpenFileNoAccess, OpenFileRead,
OpenFileWrite, OpenDir, FileRead, FileWrite, CreateFile, CreateDir,
DeleteFile, DeleteDir, CloseModified, CloseUnmodified, CloseDir,
RenameFile, RenameDir, SetAclFile, SetAclDir, SetSecFile, SetSecDir
```

Use the vertical bar (|) when listing multiple events.

`ignore =` if the CEPA server is not available, ignore, and return no error to the caller.

`denied =` if the CEPA server is not available, return access denied to the caller. The caller will lose read/write access to the CIFS Share.

<reqtimeout> is the timeout in ms to send a request that allows access to the CEPA server. Wait to receive the response from the CEPA server. The default is 1,000 ms and the range is 500 ms through 5,000 ms.

<retrytimeout> is the timeout in ms to retry the access request sent to the CEPA server. This value must be less than or equal to the `reqtimeout` value. The default is 250 ms and the range is 50 ms through 5,000 ms.

4 Save the file with the name **cepp.conf** and then close the text editor.

5 Move the cepp.conf file to the Data Mover's root file system:

```
$ server_file <movername> -put cepp.conf cepp.conf
```

where <movername> is the name of the Data Mover. Note that each Data Mover than runs CEPA must have a cepp.conf file, but each configuration file can specify different events.

6 Before starting CEPA for the first time, the administrator must issue the following command from the Control Station:

```
/nas/sbin/server_user server_2 -add -md5 -passwd <msrpcuser>
```

where <msrpcuser> is the name assigned to either a simple user account or user account that is part of a domain under which the EMC CAVA service is running on the VEE or CEE machine; for example, ceeuser or CEE1.ceeuser.

Manage the Event Publishing Agent

The tasks to manage the event publishing agent include editing the cepp.conf file, assigning rights in Windows Server 2003 and Windows 2000, starting and stopping the CEPA facility, verifying the CEPA status, and displaying the CEPA facility properties, statistics, and detailed information for a CEPA pool. Before issuing commands, log in as a domain user, not a local user.

Edit the cepp.conf File

1. Copy the current configuration file from the Data Mover, substituting `<movername>` with the name of the Data Mover where the configuration file resides.

   ```
   $ server_file <movername> -get cepp.conf cepp.conf
   ```

2. Edit the cepp.conf file as necessary.

3. Reload the file to the Data Mover, substituting `<movername>` with the name of the Data Mover where the configuration file resides.

   ```
   $ server_file <movername> -put cepp.conf cepp.conf
   ```

Start the CEPA Facility

To start the CEPA facility, use this command syntax, substituting the name of the Data Mover for <movername>:

```
$ server_cepp <movername> -service -start
```

For example, to start the CEPA facility on the Data Mover server_2, enter:

```
$ server_cepp server_2 -service -start
```

Verify the CEPA Status

To verify the CEPA facility status, use this command syntax, substituting the name of the Data Mover for <movername>:

```
$ server_cepp <movername> -service -status
```

For example, to verify the CEPA facility status on the Data Mover server_2, enter:

```
$ server_cepp server_2 -service -status
```

Stop the CEPA Facility

To stop the CEPA facility, use this command syntax, substituting the name of the Data Mover for <movername>:

```
$ server_cepp <movername> -service -stop
```

For example, to stop the EMC VNXe Series Storage Systems facility on the Data Mover server_2, enter:

```
$ server_cepp server_2 -service -stop
```

Display the CEPA Facility Properties

To display information about the CEPA service, use this command syntax, substituting the name of the Data Mover for <movername>:

```
$ server_cepp <movername> -service -info
```

For example, to display CEPA service on the Data Mover server_2, enter:

```
$ server_cepp server_2 -service -info
```

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Download Microsoft Visual C++ Redistributable

The Microsoft C Run-time Library (CRT) distributed with the Microsoft Visual C++ Redistributable for Visual Studio 2012 Update 4 is required to run this connector.

You can download this package from the Microsoft website:

http://www.microsoft.com/en-us/download/details.aspx?id=30679#.

Download and install the VSU_4\vcredist_x86.exe for 32-bit platforms or for installing a 32-bit connector on a 64-bit machine. Download and install VSU4_4\vcredist_x64.exe for 64-bit platforms.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

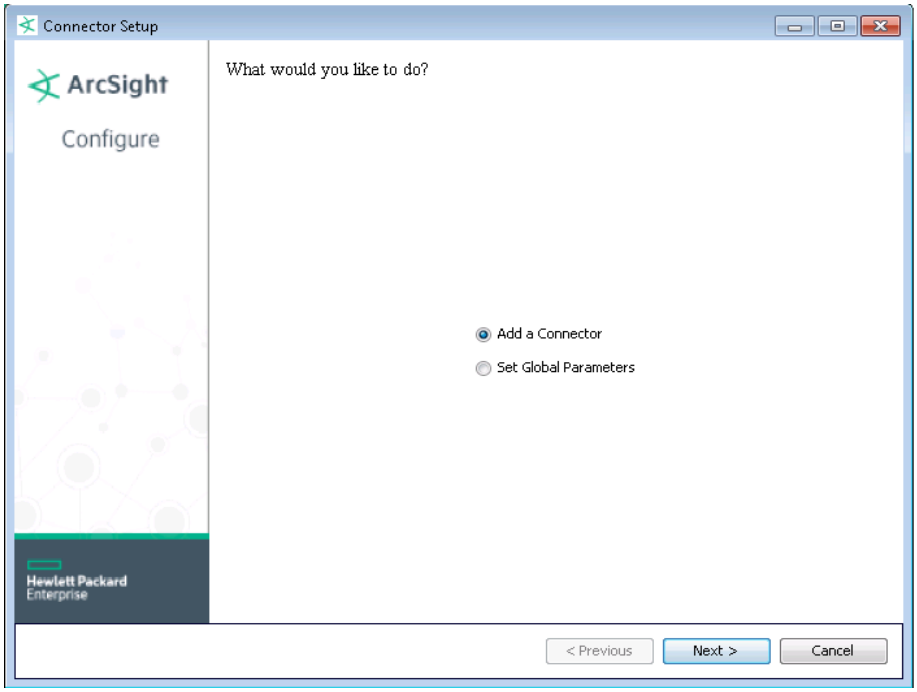
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.

Parameter	Setting
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

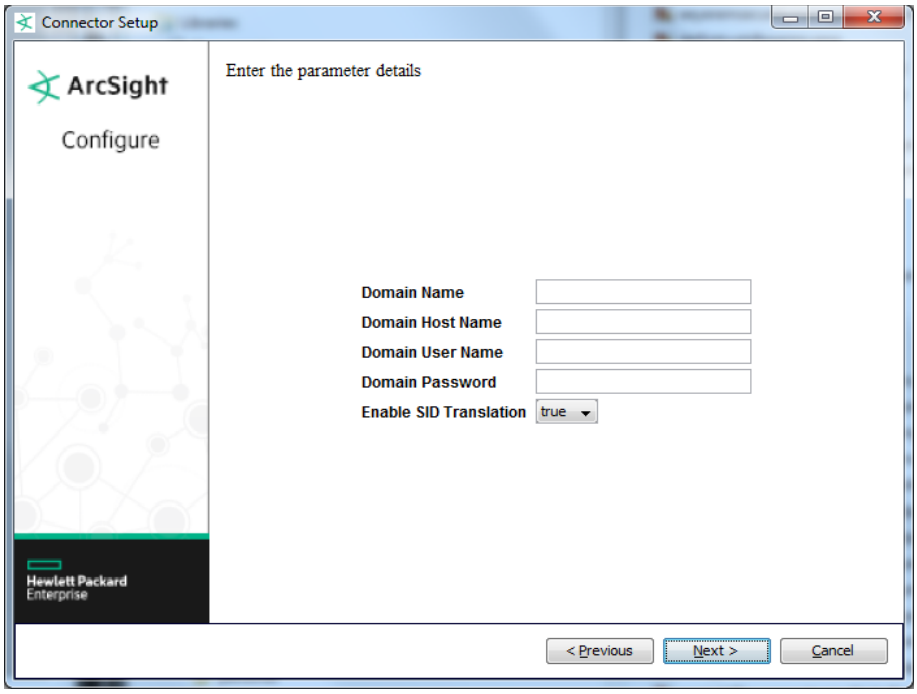
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Dell EMC Unity Storage** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Domain Name	Enter the name of the domain.
Domain Host Name	Enter the Domain Controller's IP address. If not entering the name of the domain host controller, a host (IP address) under the same domain can be used.
Domain User Name	Enter a Domain Controller user name with admin privileges to collect events from the target host.
Domain Password	Enter the password for the Domain Controller user.
Enable SID Translation	The connector can perform SID translation and is configured to translate SIDs by default. Select 'false' if you do not want SID translation enabled.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	protocol
Bytes In	bytesWritten
Bytes Out	bytesRead
Destination Address	serverIp
Destination User Name	ownerSid or the user name from translating ownerSid

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	numberOfReads
Device Custom String 1	userSid
Device Custom String 2	share
Device Custom String 3	flag (0x0=CEPP_FLAG_NONE, 0x1=CEPP_FLAG_PREEVENT, 0x2=CEPP_FLAG_POSTEVENT_SUCCESS, 0x4=CEPP_FLAG_POSTEVENT_FAILURE)
Device Custom String 4	ntStatus
Device Custom String 5	desiredAccess
Device Custom String 6	relativePath or the decoded encodedRelativePath
Device Event Class ID	event
Device Host Name	server
Device Product	'Unity'
Device Receipt Time	timestamp
Device Vendor	'Dell EMC'
Event Outcome	state (0x0=STATE_NONE,0x1=STATE_OFFLINE)
File Path	path or the decoded encodePath
File Size	fileSize
Message	createDispo
Name	0x0=EVENT_UNKNOWN, 0x1=EVENT_FILE_OPEN_NOACCESS, 0x2=EVENT_FILE_OPEN_READ, 0x4=EVENT_FILE_OPEN_WRITE, 0x8=EVENT_FILE_CREATE, 0x10=EVENT_FILE_RENAME, 0x20=EVENT_FILE_DELETE, 0x40=EVENT_FILE_CLOSE, 0x80=EVENT_FILE_CLOSE_MODIFIED, 0x100=EVENT_FILE_SET_ACL, 0x200=EVENT_FILE_READ, 0x400=EVENT_FILE_WRITE, 0x800=EVENT_FILE_SET_SEC, 0x10000=EVENT_DIR_CREATE, 0x20000=EVENT_DIR_RENAME, 0x40000=EVENT_DIR_DELETE, 0x80000=EVENT_DIR_SET_ACL, 0x100000=EVENT_DIR_OPEN, 0x200000=EVENT_DIR_CLOSE, 0x400000=EVENT_DIR_SET_SEC, 0x80000000=EVENT_ADMIN_RESYNC
Source Address	clientIp
Source User Name	userSid or the user name from translating userSid