



Micro Focus Security ArcSight Connectors

SmartConnector for Solsoft Policy Server

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Solsoft Policy Server

June, 2018

Copyright © 2005 – 2017; 2018 Micro Focus and its affiliates and licensors.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/14/2014	Updated parameter screen image.
05/15/2012	Added new installation procedure.
09/24/2010	Updated versions supported.
02/11/2010	Added support for FIPS Suite B and CEF File transport.

SmartConnector for Solsoft Policy Server

This guide provides information for installing the SmartConnector for Solsoft Policy Server and configuring the device to send logged events to the SmartConnector. Solsoft Versions 6.0 and 7 are supported in Windows environments. This SmartConnector may not work with Solsoft version 7.0.2 and later versions.

Product Overview

Solsoft Policy Server centralizes and automates the design, deployment, and documentation of security policies for multi-vendor firewalls, routers, switches, VPN gear, and other security infrastructure. Solsoft Policy Server can generate optimal configuration for network devices and create complete and consistent network security in large and complex multi-device and multi-vendor networks.

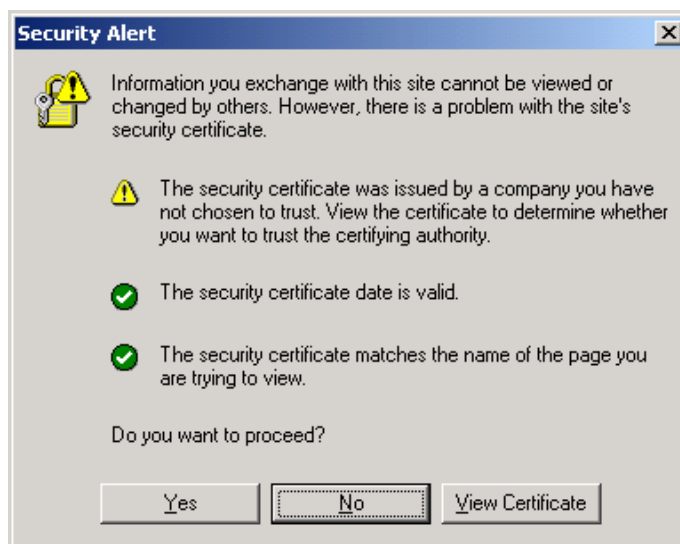
Configuration

Obtaining an Authentication Certificate from the Solsoft Policy Server

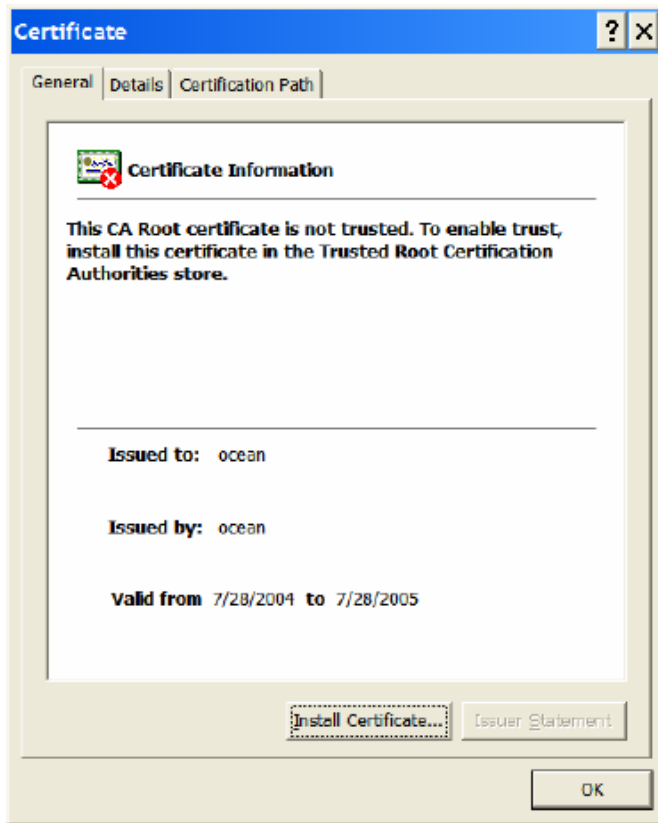
Because the SmartConnector will be validating the Solsoft Policy Server's authentication certificate, first get the certificate from the Solsoft Policy Server and import it into the SmartConnector Java Runtime Environment before running the SmartConnector for Solsoft Policy Server.

This section provides instructions about retrieving, importing, and verifying the authentication certificate. The SmartConnector is to be installed in the folder `c:\ArcSight` on Windows.

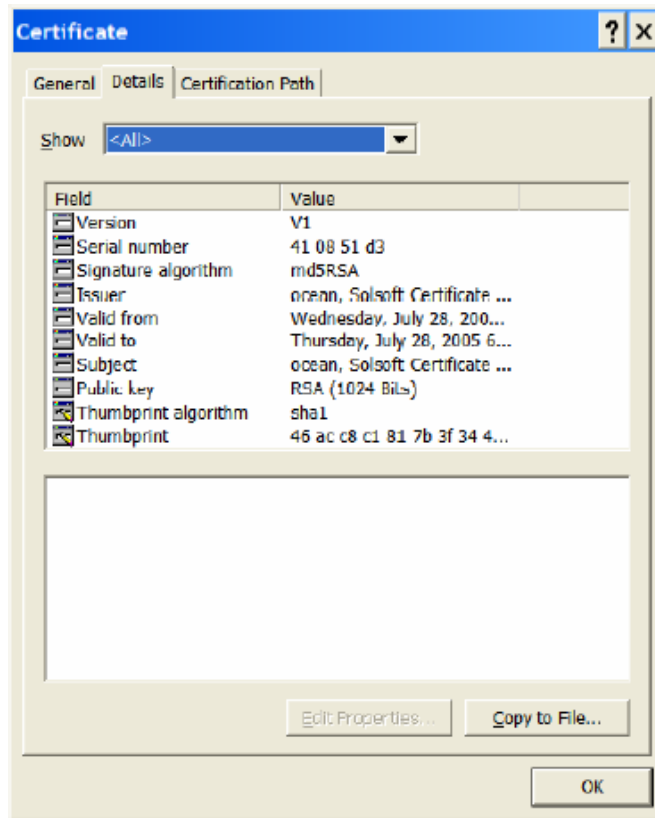
- 1 From Internet Explorer, access site <https://10.0.111.16:8443>; the following dialog box is displayed (with the Solsoft Web Server service running on 10.0.111.16 with port 8443).



- 2 Click **View Certificate**.



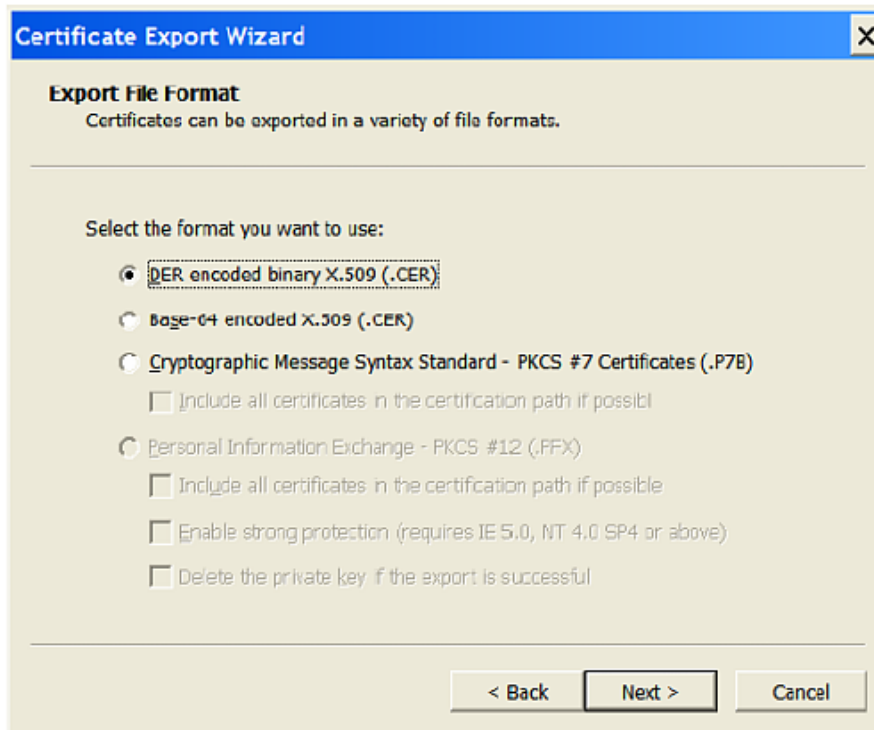
- 3 Click the **Details** tab.



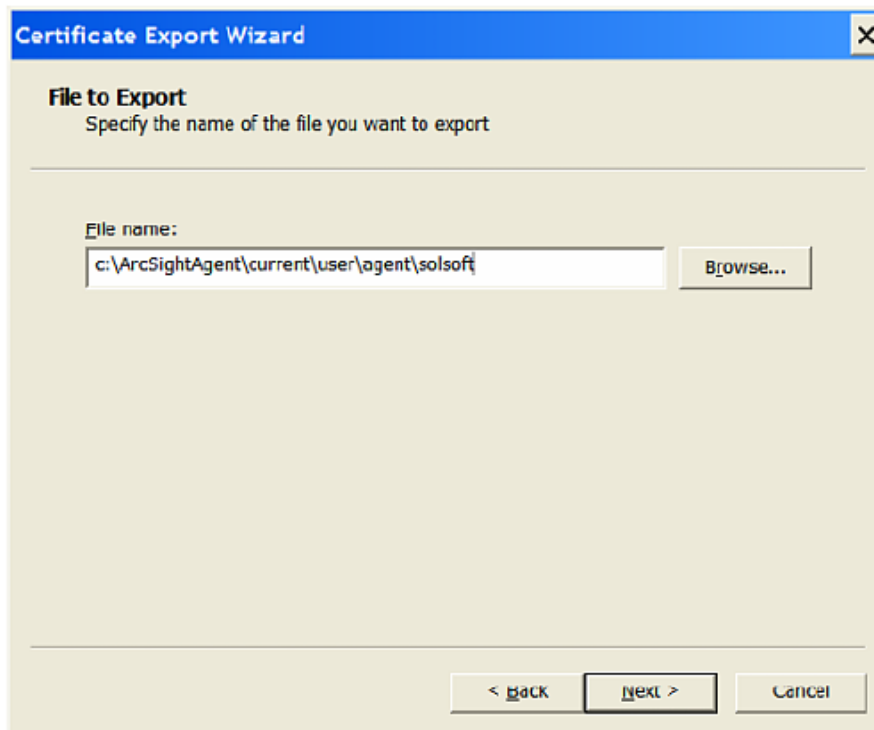
- 4 Click the **Copy to File** button.



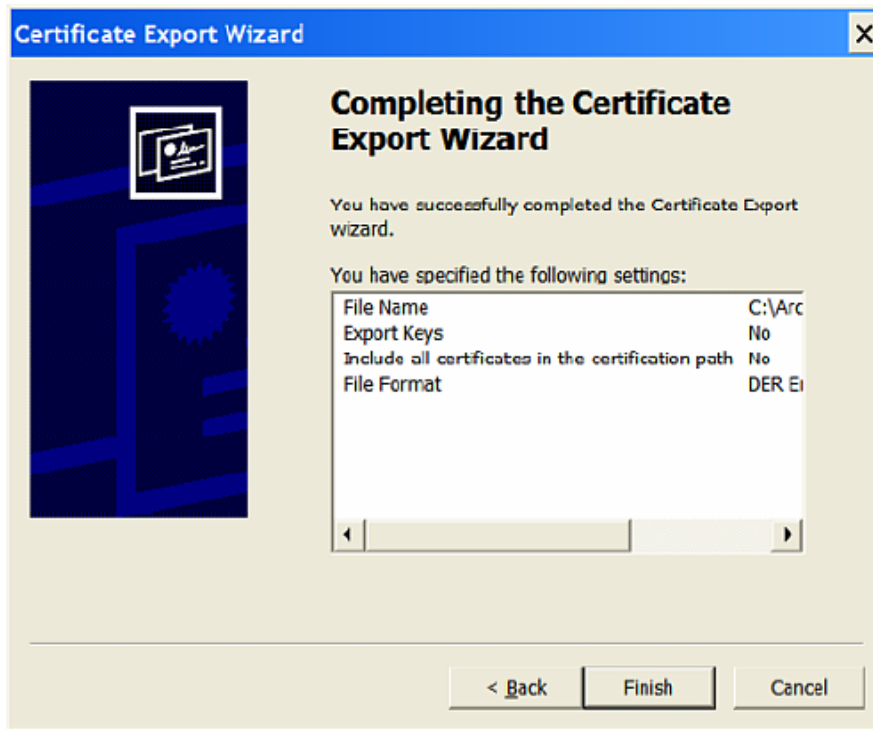
- 5 Click **Next** and select **DER encoded binary X.509 (.CER)**, used by the SmartConnector for Solsoft Policy Server.



- 6 Click **Next** and enter a file name for the new certificate. Remember this file path and name; you will need it later.



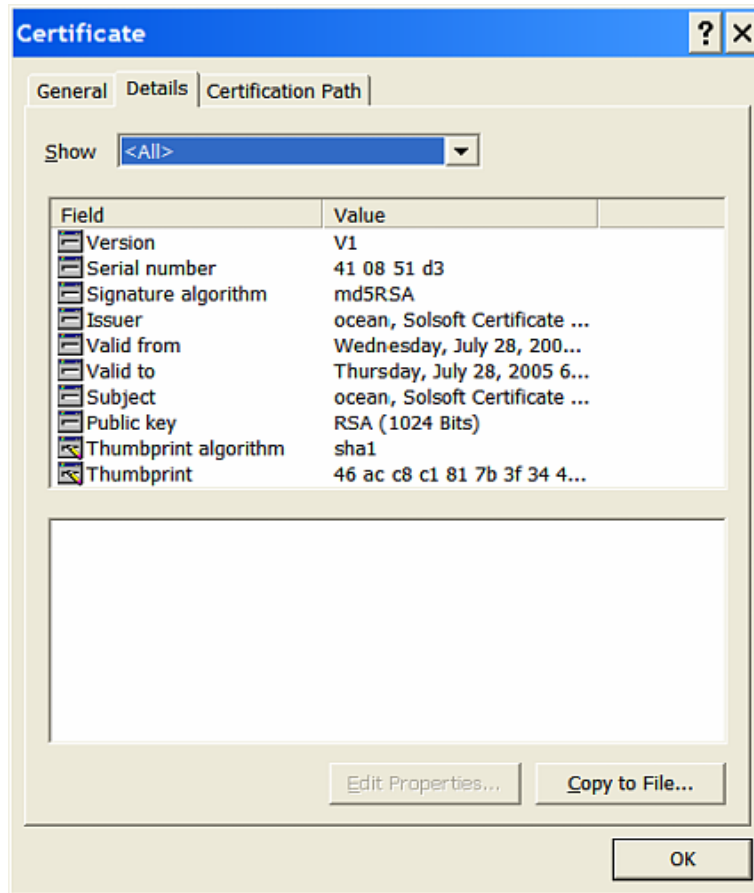
- 7 Click **Next**.



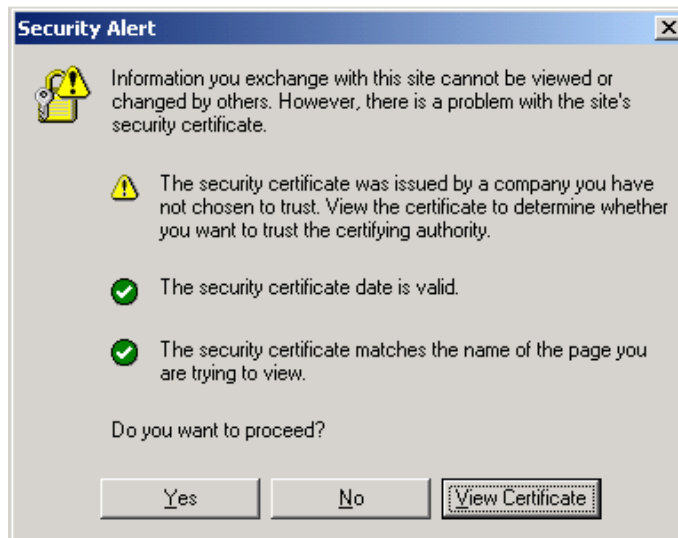
- 8 Click **Finish**. The following confirmation window is displayed.




- 9 Click **OK**.



10 Click **OK**.



11 Click **No** to end the procedure.

-
-  Auto upload is not enabled by default for Solsoft Policy Server version 7.0 or later; in addition, auto upload should never be used for Solsoft Policy Server version 6.0 or earlier.
-

Import the Certificate to the Local Java Runtime Environment

Once the certificate has been created, import it into the Java runtime environment. To do so, open a command window on the SmartConnector machine at `ARCSIGHT_HOME\bin` and follow these steps.

- 1 Execute the keytool application to import the Solsoft Policy Server certificate that we obtained by performing the steps in the previous section.

```
arcsight agent keytool -import -alias solsoft_server -file
c:\ArcSightAgent\current\user\agent\solsoft -store
clientcerts
```

(Enter the keytool command on a single line.)

- 2 Following the prompts, answer 'yes' for prompt **Trust this certificate?**

```
ArcSight Keytool Wrapper 3.1.0.0.0
Using key store: c:\Program
Files\Java\jdk1.5.0_02\jre\lib\security\cacerts (JKS)
Owner: CN=ocean, OU=Solsoft Certificate Authority,
O=Solsoft, C=US
Issuer: CN=ocean, OU=Solsoft Certificate Authority,
O=Solsoft, C=US
Serial number: 410851d3
Valid from: Wed Jul 28 18:24:35 PDT 2004 until: Thu Jul 28
18:24:35 PDT 2005
Certificate fingerprints:
    MD5:  A6:B7:6D:2C:D9:02:E0:FB:89:FC:0F:04:CA:36:FF:83
    SHA1:
46:AC:C8:C1:81:7B:3F:34:4A:40:AB:E9:B4:D0:8D:C2:00:39:43:1F
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Verify the Imported Certificate

You can verify the imported certificate by issuing the following command:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate (alias=solsoft_server) is displayed in the list:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 12 entries:
...
solsoft_server, Apr 7, 2005, trustedCertEntry,
Certificate fingerprint (MD5):
A6:B7:6D:2C:D9:02:E0:FB:89:FC:0F:04:CA:36:FF:83
...
```

Install the SmartConnector

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

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

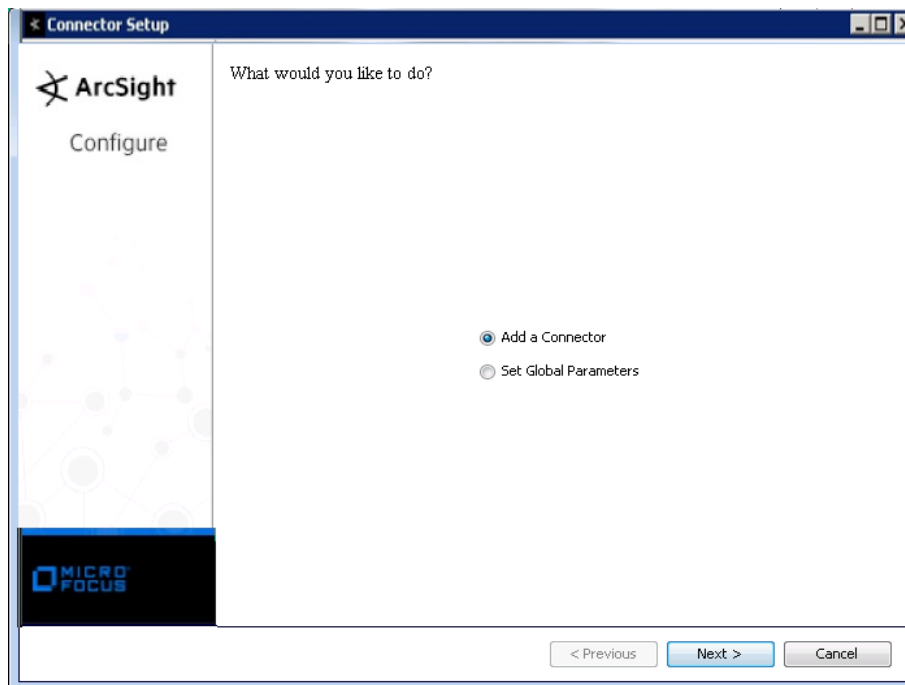
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus 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'.
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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 **Solsoft Policy Server** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Host Name or IP	Host name or IP address of the Solsoft Policy Server.
Web Service Port	Port that will be used for communication with the Solsoft Policy Server Web Server service. The default is 8443.
Login User	User name of login user for Solsoft Policy Server.
Password	Password of the login user for Solsoft Policy Server.
Project Name	The Solsoft project name.

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.

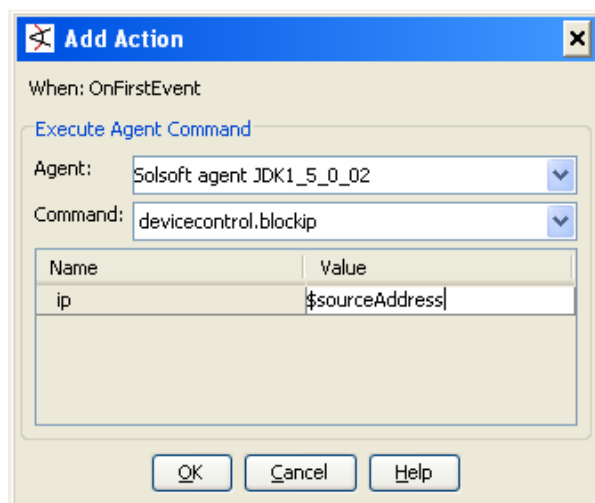
Troubleshooting

This section describes the most common problems you may encounter when installing and configuring the connector. The descriptions include suggested solutions for resolving problems. If you cannot resolve problems using this information, consult ArcSight Support.

Generate the Correct ArcSight Rule

An ArcSight correlation rule action should be generated before you expect the SmartConnector for Solsoft Policy Server Control to work.

When you create or modify a rule, you can add a new action to have the Solsoft Policy Server block an IP or service port. For example, the following 'Action' will block the source address if this rule is triggered:



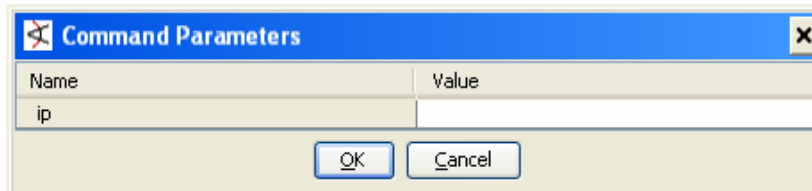
Check Action Manually

For troubleshooting, you can check the action's execution without creating a rule. You can do this through ArcSight ESM Console:

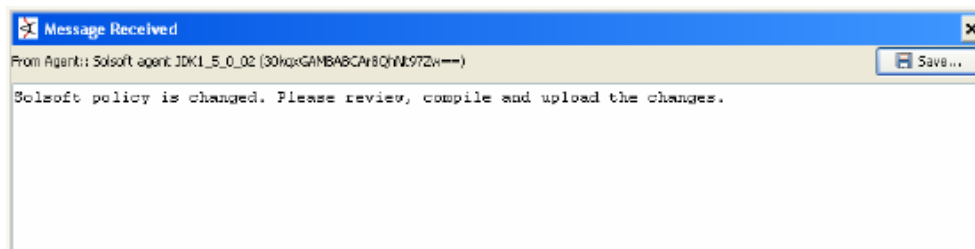
- From the connector list, choose the SmartConnector for Solsoft Policy Server.
- Right click and select **Send Command**.

- Select **Device Policy Control**.
- Choose one of following actions:
 - ◆ Block IP
 - ◆ Block Service
 - ◆ Allow IP
 - ◆ Allow Service
 - ◆ Get Status

For example, you will a windows such as the following when you select 'Block IP':



Enter the IP manually and click **OK** to send the command to the SmartConnector. After a while, the following window is displayed containing the action result:



Current SmartConnector Limitations

- 1 For Policy Server version 6.0, auto upload is not implemented. Changes made to the Solsoft Policy Server's policy are not uploaded to PEP automatically. Instead, an ArcSight internal event `Solsoft policy is changed. Please review, compile and upload the changes.` is sent. The choice to automatically upload policy changes is available with Solsoft Policy Server version 7.0.
- 2 The port field can accept service name only. When you try to block a service port, the following parameter window is displayed:

Name	Value
subnet	
subnet_mask	
port	

Enter the subnet for the first field and subnet mask for the second field. For the third field, enter the service name for the corresponding port rather than the port number.

You can find the service name from Solsoft Security Designer window. If there is no service name for a specific port number, you should create it from Solsoft Security Designer before you use it.

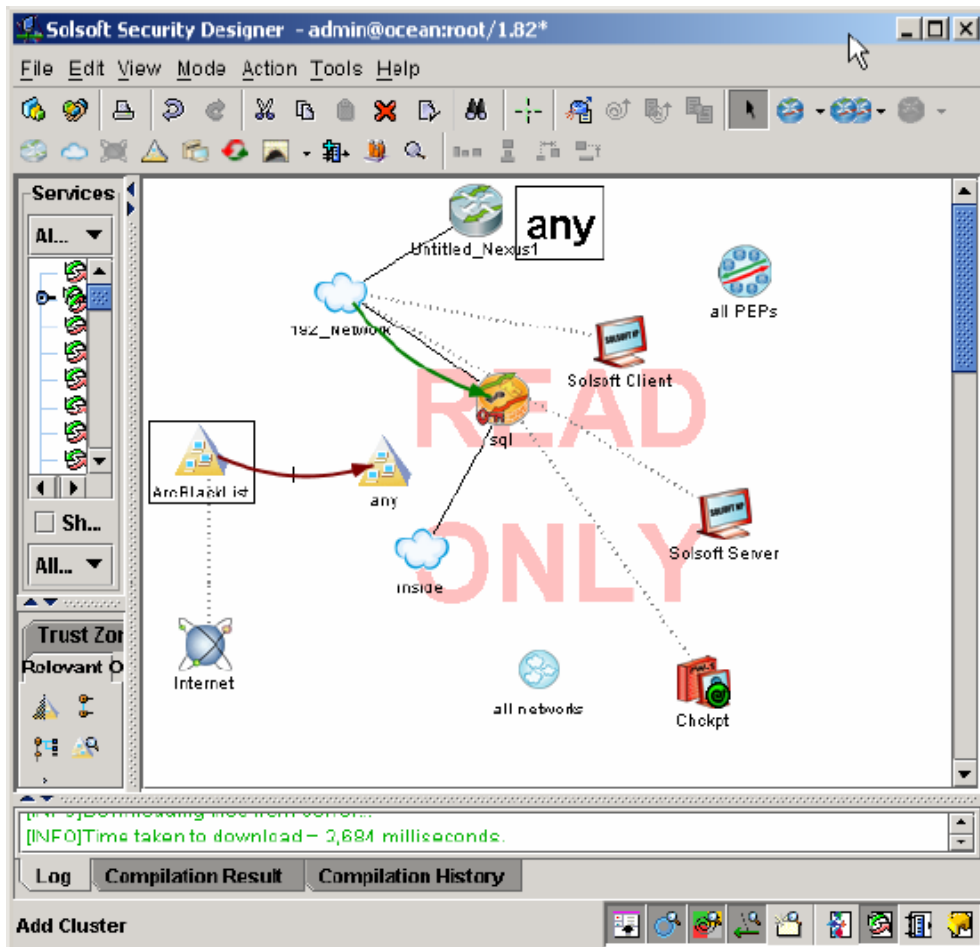
For example, the following parameters block traffic to port 80 of any machine in subnet 192.168.10.0 (255 addresses):

Name	Value
subnet	192.168.10.0
subnet_mask	255.255.255.0
port	http

Check policy changes from Solsoft Security Designer

Any ArcSight change can be reviewed from Solsoft Security Designer before you compile and upload it. We create a class called 'ArcBlackList' to hold all blocked IPs. These blocked IPs will not have permission to access class 'any'.

The following is a screen shot from Solsoft Security Designer about 'ArcBlackList' and its relationship with other classes:



If you double-click 'ArcBlackList', a windows such as the following showing all IPs is displayed:

