Micro Focus Security ArcSight Connectors

SmartConnector for Syslog NG Daemon

Configuration Guide

May 21, 2020

Configuration Guide

SmartConnector for Syslog NG Daemon

May 21, 2020

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202- 3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

* Software Version number

* Document Release Date, which changes each time the document is updated

* Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters. Updated IP Address parameter description.
10/17/2017	Added encryption parameters to Global Parameters. Updated IP Address parameter description.
02/15/2017	Added instructions for using a customer-supplied certificate to setup Syslog NG.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2016	Updated definition of the 'Protocol' parameter.
08/14/2015	Added UDP selection to Protocol parameter for connector configuration.
03/31/2015	General availability of support for IETF standard event collection occurred 9/30/2013.
02/16/2015	Added parameter for Syslog NG Daemon connector configuration.
02/14/2014	Updated parameter screen image.
12/21/2012	Added support for Syslog NG 3.3 and IPv6.
05/15/2012	Added new installation procedure.
02/15/2012	General availability of this connector for BSD syslog format.
05/15/2011	Added support for TLS mutual authentication.
02/15/2011	First edition of this Configuration Guide.

SmartConnector for Syslog NG Daemon

This guide provides information for installing the SmartConnector for Syslog NG Daemon and configuring the device for event collection. Syslog NG versions 3.0 and 3.3 are supported for BSD syslog format. Support is also provided for collection of IETF standard events.

Product Overview

The Syslog NG application is an open source implementation of the syslog protocol for UNIX and UNIX-like systems, extending the original syslogd model and adding important features to syslog, such as using Transport Layer Security (TLS) to encrypt communication and support for IETF Standard (RFC 5424) syslog header.

TLS uses certificates to authenticate and encrypt the communication. The client authenticates the server by requesting its certificate. Optionally, the server can also request a certificate from the client. See "Add TLS Function to the Syslog NG Setup" for more information.

This SmartConnector is capable of receiving events over a secure TLS channel from another SmartConnector (whose destination is configured as CEF Syslog over TLS).

For a list of all mappings supported for all syslog SmartConnectors, see the *SmartConnector Configuration Guide for UNIX OS Syslog*.

Configuration

For information on how to configure Syslog NG, see the *syslog-ng Open Source Administrator Guide*.

Here is one possible installation and configuration workflow for Syslog-NG Daemon. Item 1 should be performed by every customer using this connector. Items 2-4 apply only when TLS is the chosen protocol. When TLS is chosen, item 2 should always be performed in conjunction with item 1. After completing them, the customer should verify the connector is operating properly. Then some customers may decide to complete one of the configuration options in item 3 but never both. Some customers might decide to complete item 4 if they need mutual authentication.

1 Install the Syslog NG Daemon connector as described in "Install the SmartConnector".

2 If you are using TLS protocol, then follow the steps in "Add TLS Function to the Syslog NG Setup" for using the connector-generated certificate. This will verify that the `syslog-ng` machine is correctly configured and communicating with the Syslog NG Daemon connector.

3 If you are using TLS protocol, do one of the following:

- To supply your own certificate for Syslog NG, follow the steps in "Using a Customer-Supplied Certificate for Syslog NG Setup".

- To supply your own certificate for both remote management and Syslog NG, follow the steps in "Using a Customer-Supplied Certificate for Both Remote Management and Syslog NG".

4. If you are using mutual authentication, see "Configure for Mutual Configuration" for additional certificate import information.

5. If you are using TLS as the protocol to receive events from any other SmartConnector, see the *SmartConnector User's Guide*, "CEF Destinations" chapter for more information.

Install the SmartConnector

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

> When installing the syslog daemon connector in a UNIX environment, run the executable as 'root' user.

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.

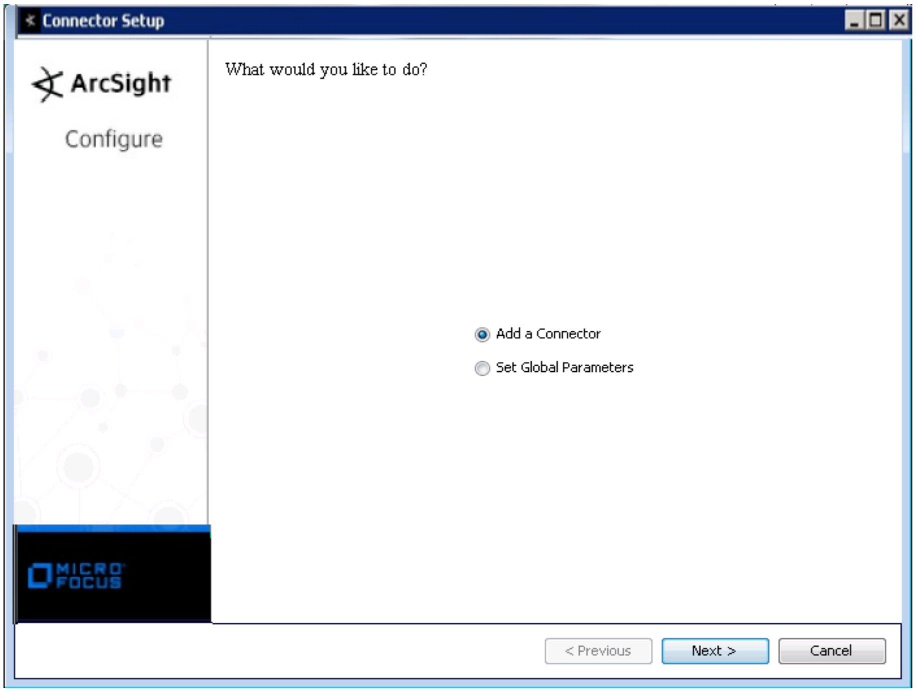
1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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:



What would you like to do?

● Add a Connector

○ Set Global Parameters

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.

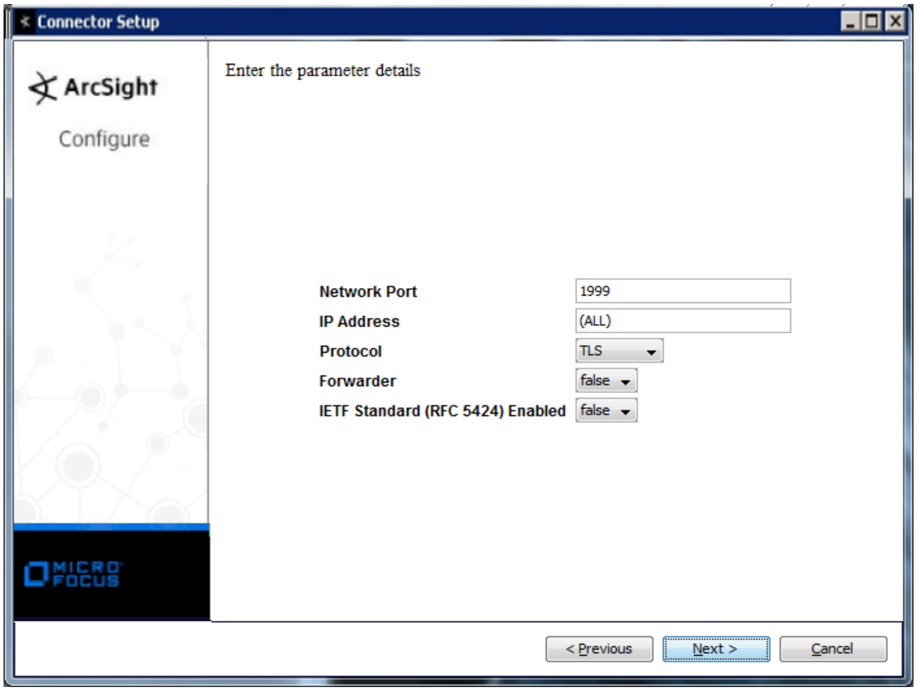
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **Syslog NG Daemon** and click **Next**.

3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the parameter details

Network Port: 1999
IP Address: (ALL)
Protocol: TLS
Forwarder: false
IETF Standard (RFC 5424) Enabled: false

Parameter	Description
Network Port	Specify the port to which the connector is to listen for Syslog NG events. This is generally port 1999 for Syslog NG.
IP Address	Enter the IP address for the device that is receiving the events and to which the connector is to listen exclusively. Accept the default value of (ALL) to bind to all available IP addresses.
Protocol	Select either UDP, TLS or Raw TCP. The default value is TLS. The SmartConnector for Syslog NG Daemon uses the selected protocol to receive incoming messages.
Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
IETF Standard (RFC 5424) Enabled	Select 'true' to enable IETF Standard (RFC 5424); otherwise, leave the default value of 'false'. The Syslog NG connector by default expects the events to be in BSD format, which the syslog connector supports. If the parameter is set to 'true', the connector expects the events to have the IETF Standard (RFC 5424) syslog header.

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*.

Additional Configuration

Add TLS Function to the Syslog NG Setup

The SmartConnector generates a key and a certificate for authentication. The certificate must be copied to the Syslog NG client for the authentication and encryption/decryption of syslog messages, as follows:

1 Make sure you have installed the SmartConnector for Syslog NG Daemon correctly, and that TLS was selected as the protocol during the installation process.

2 Run the connector (see "Run the SmartConnector" for specific instructions).

3 Make sure Syslog NG is installed on the server to be configured to send syslog messages to the Syslog NG Daemon connector. While installing Syslog NG on this server, if you are prompted to "forward your log messages to a remote server, enter the address of the server and select **OK**, otherwise, select **Skip**.

> If an error message is displayed during the installation of the client, you can ignore the message and successfully continue with the installation.

4. Change syslog-ng.conf to create a destination for the Syslog NG Agent. The following is an example /opt/syslog-ng/etc/syslog-ng.conf file. In the example, <connector hostname> is the the DNS name for the Syslog NG Daemon machine, for example, myconnector.acme.com.

   ```
   # destinations

   destination d_tls_syslogNGAgent {
      network("<connector hostname>" port (1999)
      transport("tls")
      tls(ca_dir("/opt/syslog-ng/etc/cert.d"))); };

   log { source(s_sys); destination(d_tls_syslogNGAgent); };
   ```

5. Copy syslog-ng.cert from $ARCSIGHT_HOME/user/agent/ into /opt/syslog-ng/etc/cert.d.

6. From /opt/syslog-ng/etc/cert.d, run the following command to create a hash:

   ```
   openssl x509 -noout -hash -in syslog-ng.cert
   ```

7. Issue the following command: ln -s syslog-ng.cert <hashname>.0, where <hashname> is the name of the hash returned in step 6; for example:

   ```
   ln -s syslog-ng.cert 0968c5ee.0
   ```

8. Start the Syslog NG service, for example: service syslog-ng start. This command might vary depending on your operating system.

Syslog NG should now be sending syslog messages to the connector.

Check the error log to see if syslog-ng startup was successful. On Linux systems, look in /var/log/messages. Here is an example of a successful start message:

```
Jan 24 12:42:00 syslogng syslog-ng[21946]: syslog-ng
starting up; version='3.5.6'
Jan 24 12:42:00 syslogng syslog-ng[21946]: Syslog
connection established; fd='8',
server='AF_INET(15.214.157.159:1999)',
local='AF_INET(0.0.0.0:0)'
```

Using a Customer-Supplied Certificate for Syslog NG Setup

You can provide your own certificate for authentication. You must copy the signed certificate and private key to the machine where Syslog NG Daemon will run, create a keystore, and edit the `agent.properties` file.

The following procedure is an example. You might have alternative procedures for creating the private key and certificate in your environment.

1. Generate a key pair file to be used by Syslog NG, for example:

   ```
   openssl genrsa -out SyslogNGD_key.pem 2048
   ```

2. Generate a certificate signing request for the Syslog NG certificate, for example:

   ```
   openssl req -new -key SyslogNGD_key.pem -out SyslogNGD.csr
   ```

3. Present the certificate signing request to a certificate authority and obtain a signed Syslog NG Daemon certificate.

4. Rename the `.cer file` and `.pem file` to `syslog-ng.cer` and `syslog-ng.pem` and copy them to `$ArcSightHome/current/user/agent`.

5. Create a `pkcs12` keystore on the connector machine where the Syslog NG Daemon connector will run.
   `openssl pkcs12 -export -clcerts -in SyslogNGD.crt -inkey SyslogNGD_key.pem -out syslog-ng.p12 -name "syslogng-alias" -password pass:changeit`. The "changeit" password is used when the connector accesses the keystore.

6. Add the following keystore properties to the `agent.properties` file:

   ```
   syslogng.tls.keystore.file=user/agent/syslog-ng.p12
   syslogng.tls.keystore.alias=syslogng-alias
   ```

Restart the connector so that it will begin using the new keystore and certificate. The certificate must also be copied to the `syslog-ng` machine. See steps 5-8 in "Add TLS Function to the Syslog NG Setup".

The `syslog-ng` machine must have access to the Certificate Authority certificate so that `syslog-ng` can correctly validate the certificate it receives from Syslog NG Daemon connector.

Using a Customer-Supplied Certificate for Both Remote Management and Syslog NG

In the default configuration the connector uses the same self-signed certificate for both remote management and the Syslog NG Daemon connector. You can provide your own certificate and keystore to replace those produced by the connector. You must copy the signed certificate and private key to the machine where Syslog NG Daemon will run and create a keystore.

The following procedure is an example. You might have alternative procedures for creating the private key and certificate in your environment.

1. Start a command prompt/shell window on the machine where the Syslog NG Daemon is installed and navigate to the `user/agent` directory of the connector installation. Display the current `remote_management.p12` keystore to obtain the "Alias name". You will need to use this alias name in subsequent steps.

   ```
   $ARCSIGHT_HOME/jre/bin/keytool -list -v -keystore
   remote_management.p12
   -storetype PKCS12 -storepass changeit
   ```

   The output of this command is similar to:

   ```
   Keystore type: PKCS12
   Keystore provider: SunJSSE

   Your keystore contains 1 entry

   Alias name: cn=n15-214-157-
   h159.my.company.com,ou=jjieufkbabcaarn85auxw,o=arcsight,l=n
   a,st=na,c=us
   Creation date: Jan 26, 2017
   Entry type: PrivateKeyEntry
   Certificate chain length: 1
   Certificate[1]:
   ```
   [remainder of the keytool -list output is omitted]

2. Rename the `remote_management.p12` keystore to `remote_management.p12-self-signed`. The `remote_management.p12` keystore will be replaced so this creates a backup of the original.

3. Generate a private key to be used by Syslog NG, for example:

   ```
   openssl genrsa -out SyslogNGD_key.pem 2048
   ```

4. Generate a certificate signing request for the Syslog NG certificate, for example:

   ```
   openssl req -new -key SyslogNGD_key.pem -out SyslogNGD.csr
   ```

5. Present the certificate signing request to a certificate authority and obtain a signed Syslog NG Daemon certificate.

6. Copy the Syslog NG Daemon certificate and private key to the connector machine where Syslog NG Daemon connector will run. Place these files in the `user/agent` subdirectory of the connector installation.

7. Create a pkcs12 keystore on the connector machine where the Syslog NG Daemon connector will run. Use the alias name obtained in step 1 for the `-name` parameter. The keystore name

is `remote_management.p12`.

```
openssl pkcs12 -export -clcerts -in SyslogNGD.crt -inkey
SyslogNGD_key.pem -out remote_management.p12 -name "cn=n15-
214-157-
h159.my.company.com,ou=jjieufkbabcaarn85auxw,o=arcsight,l=n
a,st=na,c=us" -password pass:changeit
```

8. Verify the `remote_management.p12` keystore. The keystore should be displayed without error and the alias should be the same as obtained in step 1.

   ```
    $ARCSIGHT_HOME/jre/bin/keytool -list -v -keystore
   remote_management.p12 -storetype PKCS12 -storepass changeit
   ```

9. Verify that the certificate for the certificate authority that signed the certificate is present in the Java keystore used by the connector. This command will display the keystore contents:

   ```
   $ARCSIGHT_HOME/jre/bin/keytool -list -storepass changeit -
   keystore $ARCSIGHT_HOME/jre/lib/security/cacerts
   ```

10. If the certificate for the certificate authority is not in the keystore, import it:

    ```
    $ARCSIGHT_HOME/jre/bin/keytool -importcert -file
    <ca_certificate file_name> -storepass changeit -keystore
    $ARCSIGHT_HOME/jre/lib/security/cacerts
    ```

11. Delete the self-signed remote management certificate from both the Java keystore and the FIPS keystore. Use the alias obtained in step 1.

    To delete the self-signed remote management certificate from the Java keystore:

    ```
    $ARCSIGHT_HOME/jre/bin/keytool -delete -alias "cn=n15-214-
    157-
    h159.my.company.com,ou=jjieufkbabcaarn85auxw,o=arcsight,l=n
    a,st=na,c=us" -keystore
    $ARCSIGHT_HOME/jre/lib/security/cacerts -storepass changeit
    ```

    To delete the self-signed remote management certificate from the FIPS keystore:

    ```
    jre/bin/keytool -delete -alias "cn=n15-214-157-
    h159.my.company.com,ou=jjieufkbabcaarn85auxw,o=myCompany,l=
    na,st=na,c=us" -keystore
    $ARCSIGHT_HOME/user/agent/fips/bcfips_ks -storepass
    changeit
    -storetype BCFKS -providername BCFIPS -providerclass
    org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
    providerpath $ARCSIGHT_HOME/lib/agent/fips/bc-fips-
    1.0.0.jar
    -J-Djava.security.egd=file:/dev/urandom
    ```

Restart the connector so that it will begin using the new keystore and certificate. The certificate must also be copied to the `syslog-ng` machine. See steps 5-8 in "Add TLS Function to the Syslog NG Setup".

The `syslog-ng` machine must have access to the Certificate Authority certificate so that `syslog-ng` can correctly validate the certificate it receives from Syslog NG Daemon connector.

Configure for Mutual Authentication

For enhanced security, mutual authentication is now supported. This means the Syslog NG source is authensticated by the connector. This involves generating a key and a certificate on the source. This certificate must be trusted by the connector.

On the Syslog NG Device

The instructions for configuring mutual authentication on the SyslogNG source can be found in the *Syslog NG Administration Guide* in the section "Mutual Authentication Using TLS." The following instructions describe one of the ways to accomplish this.

1. Execute the following command to create the private (`privkey.pem`) and certificate:

   ```
   openssl req -new -x509 -out syslogngclient.pem -days 1095 -
   nodes
   ```

2. Create the following directories:

   ```
   /opt/syslog-ng/etc/cert.d
   /opt/syslog-ng/etc/key.d
   ```

3. Move `privkey.pem` to `/opt/syslog-ng/etc/key.d/syslogngkey.pem`.

4. Move `syslogngclient.pem` to `/opt/syslog-ng/etc/cert.d`.

5. Edit `/opt/syslog-ng/etc/syslog-ng.conf` and update the destination as shown in the following example.

   ```
   destination d_tls_raghu {
           tcp("1.1.1.1" port(1999)
                   tls(ca_dir("/opt/syslog-ng/etc/ca.d")
                       key_file("/opt/syslog-
   ng/etc/key.d/syslogngclient.key")
                       cert_file("/opt/syslog-
   ng/etc/cert.d/syslogngclient.pem")));

   };
   ```

   Note that, for one-way authentication, there is already a directory for ca.d (/opt/syslog-ng/etc/ca.d) containing the certificate of the SyslogNG agent.

On the Syslog NG Agent

Enable Mutual Authentication

After SmartConnector installation, you can modify the `syslogng.mutual.auth.enabled` parameter to enable Mutual Authentication by editing the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent` and changing the value from `false` to `true`. Save your change and restart the connector for the change to take effect.

Copy the Certificate

Copy the `syslogngclient.pem` file to the machine on which the SmartConnector for Syslog NG Daemon is installed. Import the certificate as described in the next section.

Import the Certificate

To import the certificate:

1. From the `$ARCSIGHT_HOME/bin` directory, execute the following command to import the certificate.

   ```
   arcsight agent keytoolgui
   ```

2. Open the keystore in `$ARCSIGHT_HOME/current/jre/lib/security/cacerts` (password will be `changeit`).
3. From the menu bar, select **Tools** and **Import Certificate**. Upload the certificate file.
4. Trust the certificate.
5. Start the connector and the device.

If this SmartConnector is to receive events from another SmartConnector through the CEF Syslog (TLS) destination, copy the `remote_management.cer` from the Syslog NG connector to the source connector `($ARCSIGHT_HOME/current/user/agent` directory. Follow the instructions above to import and trust the `remote_management.cer` certificate.

Syslog NG Sample Configuration

The following is a sample configuration file when the syslog-ng client uses one-way authentication TLS for syslog NG version 3.0. This simple configuration shows how to specify a source, destination, and the certificate. For a description of syslog NG configuration file directives, see the *syslog-ng Administrator's Guide* at http://www.balabit.com/dl/html/syslog-ng-admin-guide_en.html/bk01-toc.html.

```
options {
};
```

```
# sources
source s_local {
# message generated by Syslog-NG
internal();
};

# destinations

destination  d_messages { file("/var/log/messages_tls"); };
destination  d_tls_syslogNGAgent {
                tcp("1.1.1.1" port(1999)
                tls(ca_dir("/opt/syslog-ng/etc/cert.d")));
};

log{
source(s_local);
destination(d_tls_syslogNGAgent);
};
```

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.