



ArcSight SmartConnectors

Software Version: CE 24.3

Configuration Guide for Syslog NG Daemon SmartConnector

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2011 – 2024 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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://www.microfocus.com/support-and-services/documentation>

Contents

- Configuration Guide for Syslog NG Daemon SmartConnector 4
- Product Overview 5
- RFC Compliance Support 6
- Configuration 9
- Installing and Configuring the SmartConnector 10
 - Preparing to Install the SmartConnector 10
 - Installing the SmartConnector to Use the Raw TCP or UDP Protocol 10
 - Installing the SmartConnector to Use the TLS Protocol 12
- Additional Configurations For TLS 16
 - Using a Customer-Supplied Certificate for Syslog NG Setup 16
 - Using a Customer-Supplied Certificate for Both Remote Management and Syslog NG 18
 - Configuring for Mutual Authentication 20
 - On the Syslog NG Device 20
 - On the Syslog NG Agent 21
- Post-Installation Permissions 23
- Device Event Mapping to ArcSight Fields 24
- Appendix - Sample Configuration File 25
- Send Documentation Feedback 26

Configuration Guide for Syslog NG Daemon SmartConnector

This guide provides information for installing the SmartConnector for Syslog NG Daemon and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Syslog NG Daemon SmartConnector is capable of receiving events over **UDP**, **Raw TCP**, and **TLS**. It can receive events over a secure TLS channel from another SmartConnector (where destination is configured as CEF Syslog over TLS).

The syslog SmartConnectors use a sub-connector architecture that allows the SmartConnector to receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall, simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

The Syslog NG application is an open source implementation of the syslog protocol for UNIX and UNIX-like systems. You must install Syslog NG on the server to be configured to send syslog messages to the Syslog NG Daemon SmartConnector. For information on how to configure Syslog NG, see the [syslog-ng Open Source Administrator Guide](#).

For information specific to configuration of devices to send syslog events to ArcSight SmartConnectors for Syslog (for example, Cisco Routers and Netscreen Firewall), see the relevant [SmartConnector Configuration Guides](#) specific to those devices.

RFC Compliance Support

The Syslog NG Daemon SmartConnector currently supports UDP, Raw TCP, and TLS protocols with the following RFC standards or formats:

- RFC 3164 (BSD-style Syslog)
- RFC 5424
- RFCs 6587 (Syslog over TCP)
- RFC 5425 (Syslog over TLS) built on RFC 5424

The following table describes compatibility with the Syslog NG Daemon SmartConnector

Supported Protocol	Supported RFC Standards / Event Formats	Description
UDP	RFC 3164 (BSD-style Syslog)	Supports events from source devices that use the RFC 3164 (BSD-style Syslog) format with the default configuration.
	RFC 5424	<p>Supports events from source devices that use the RFC 5424 format with the following required configuration in the agent.properties file:</p> <p>To enable RFC 5424 parsing support, the following two properties must be set in agent.properties:</p> <ul style="list-style-type: none">• <code>agents[0].syslogng.ietfstandard.format.enabled=true</code>• <code>agents[0].syslogng.subagents.with.ietf= <list of parser types that supports the RFC5424 style format></code> <p>For example: If a Flex Syslog parser is being designed, then you must add <code>flexagent_syslog</code> to this list.</p>

Raw TCP	RFC 6587	<p>Supports the 'Non-Transparent Framing' and 'Octet-Counting Framing' mode standards.</p> <p>After installing the Syslog NG Daemon SmartConnector, to enable the SmartConnector to process Octet-counting enabled syslog messages, you can add the syslog.framing.type property in agent.properties as follows:</p> <ul style="list-style-type: none">• <code>syslog.framing.type=1</code> 1 - This is the default value of the syslog.framing.type property. Only traditional syslog messages are supported (throws an exception for an octet syslog message).• <code>syslog.framing.type=2</code> 2 - Only Octet-counting enabled syslog messages are supported (throws an exception for traditional syslog messages, but still processes those messages).• <code>syslog.framing.type=3</code> 3 - Both traditional syslog and Octet-counting enabled syslog messages are supported. <p>For RFC 6587 compliance, the source device must deliver Syslog message payload in the RFC 5424 format, though the SmartConnector accepts BSD-style Syslog.</p> <p>If an OCF formatted event-stream arrives at the Syslog NG Daemon SmartConnector, the events will be dropped, and therefore will not be available for parsing.</p>
	RFC 5424	<p>Supports events from source devices that use the RFC 5424 format with the following required configuration in the agent.properties file:</p> <p>To enable RFC 5424 parsing support, the following two properties must be set in agent.properties:</p> <ul style="list-style-type: none">• <code>agents[0].syslogng.ietfstandard.format.enabled=true</code>• <code>agents[0].syslogng.subagents.with.ietf= <list of parser types that supports the RFC5424 style format></code> <p>For example: If a Flex Syslog parser is being designed, then you must add <code>flexagent_syslog</code> to this list.</p>

TLS	TLS	<p>The Syslog NG Daemon SmartConnector supports events stream in the NTF format for parsing.</p> <p>If an OCF formatted event-stream arrives at the Syslog NG Daemon SmartConnector, the events will be dropped and therefore will not be available for parsing.</p>
	RFC 5424	<p>Supports events from source devices that use the RFC 5424 format with the following required configuration in the agent.properties file:</p> <p>To enable RFC 5424 parsing support, you must set the following properties agent.properties:</p> <ul style="list-style-type: none"> agents[0].syslogng.ietfstandard.format.enabled=true agents[0].syslogng.subagents.with.ietf= <list of parser types that supports the RFC5424 style format> <p>For example: If a Flex Syslog parser is being designed, then you must add flexagent_syslog to this list.</p>
	RFC 5425	<p>RFC 5425 mandates OCF mode and therefore at this point Syslog NG Daemon SmartConnector is not RFC 5425 compliant.</p>
	RFC 6587	<p>Supports the 'Non-Transparent Framing' and 'Octet-Counting Framing' mode standards.</p> <p>After installing the Syslog NG Daemon SmartConnector, to enable the SmartConnector to process Octet-counting enabled syslog messages, you can add the syslog.framing.type property in agent.properties as follows:</p> <ul style="list-style-type: none"> syslog.framing.type=1 <ul style="list-style-type: none"> 1 - This is the default value of the syslog.framing.type property. Only traditional syslog messages are supported (throws an exception for an octet syslog message). syslog.framing.type=2 <ul style="list-style-type: none"> 2 - Only Octet-counting enabled syslog messages are supported (throws an exception for traditional syslog messages, but still processes those messages). syslog.framing.type=3 <ul style="list-style-type: none"> 3 - Both traditional syslog and Octet-counting enabled syslog messages are supported. <p>For RFC 6587 compliance, the source device must deliver Syslog message payload in the RFC 5424 format, though the SmartConnector accepts BSD-style Syslog.</p> <p>If an OCF formatted event-stream arrives at the Syslog NG Daemon SmartConnector, the events will be dropped, and therefore will not be available for parsing.</p>

Configuration

The Syslog Deamon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port **514** by default. However, You can configure the connector to use another port to recieve syslog events.

You can also configure the connector to use another protocol, such as TCP.

To use the SmartConnector for Syslog Daemon, add the statement in the *rsyslog.conf* file that as follows:

```
*.* @@(remote/local-host-IP):<port>
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@
- To send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the respective machine.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon.

Installing and Configuring the SmartConnector

The following sections provide instructions for installing and configuring the Syslog NG connector to use UDP, TCP or TLS protocols



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

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing the SmartConnector to Use the Raw TCP or UDP Protocol

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Select **Syslog NG Daemon** from the **Type** drop-down list and click **Next**.

5. Enter the following SmartConnector parameters to configure the SmartConnector, then click **Next**.

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 or Raw TCP . The SmartConnector for Syslog NG Daemon uses the selected protocol to receive incoming messages.
Forwarder	Set 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). The default value is 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.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).
13. (Optional) If you selected **true** for the **IETF Standard (RFC 5424) Enabled** parameter, then set the following properties in the **agent.properties** file:

- `agents[0].syslogng.ietfstandard.format.enabled=true`
- `agents[0].syslogng.subagents.with.ietf= <list of parser types that supports the RFC5424 style format>`

For example: If a Flex Syslog parser is being designed, then you must add `flexagent_syslog` to this list.

14. After you install the Syslog NG Daemon SmartConnector, to enable the SmartConnector to process Octet-counting enabled syslog messages, you can add the **syslog.framing.type** property in **agent.properties** as follows:

- `syslog.framing.type=1`
1 - This is the default value of the **syslog.framing.type** property. Only traditional syslog messages are supported (throws an exception for an octet syslog message).
- `syslog.framing.type=2`
2 - Only Octet-counting enabled syslog messages are supported (throws an exception for traditional syslog messages, but still processes those messages).
- `syslog.framing.type=3`
3 - Both traditional syslog and Octet-counting enabled syslog messages are supported.

Installing the SmartConnector to Use the TLS Protocol

The SmartConnector generates a key and a certificate for authentication. After you install and configure the SmartConnector, you must copy the certificate to the Syslog NG Daemon client for the authentication and encryption or decryption of syslog messages.

Perform the following steps install and configure the SmartConnector to use the TLS protocol, and to copy the certificate for authentication:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Select **Syslog NG Daemon** from the **Type** drop-down list and click **Next**.
5. Enter the following SmartConnector parameters to configure the SmartConnector, then click **Next**.

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 TLS . The SmartConnector for Syslog NG Daemon uses the selected protocol to receive incoming messages.
Forwarder	Set 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). The default value is 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.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).
13. (Optional) If you selected **true** for the **IETF Standard (RFC 5424) Enabled** parameter, then set the following properties in the **agent.properties** file:
 - `agents[0].syslogng.ietfstandard.format.enabled=true`
 - `agents[0].syslogng.subagents.with.ietf= <list of parser types that supports the RFC5424 style format>`

For example: If a Flex Syslog parser is being designed, then you must add `flexagent_syslog` to this list.

14. Copy **syslog-ng.cert** from `$ARCSIGHT_HOME/user/agent/` into `/opt/syslog-ng/etc/cert.d`.
15. Open the `/opt/syslog-ng/etc/syslog-ng.conf` file to create a destination for the Syslog NG Agent.

For example:

```
# 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); };
```

Where, `<connector hostname>` is the DNS name for the Syslog NG Daemon machine, such as, `myconnector.acme.com`.

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

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

Note the hash value.

17. Run the following command:

```
ln -s syslog-ng.cert <hashname>.0
```

where `<hashname>` is the name of the hash returned in the previous step For example: `ln -s syslog-ng.cert 0968c5ee.0`.

18. Run the command to start the Syslog NG Daemon service. For example: `service syslog-ng start`.



This command might vary depending on your operating system.

Syslog NG Daemon will start 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`.

Following 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)'
```

19. After you install the Syslog NG Daemon SmartConnector, to enable the SmartConnector to process Octet-counting enabled syslog messages, you can add the **syslog.framing.type** property in **agent.properties** as follows:
- `syslog.framing.type=1`
1 - This is the default value of the **syslog.framing.type** property. Only traditional syslog messages are supported (throws an exception for an octet syslog message).
 - `syslog.framing.type=2`
2 - Only Octet-counting enabled syslog messages are supported (throws an exception for traditional syslog messages, but still processes those messages).
 - `syslog.framing.type=3`
3 - Both traditional syslog and Octet-counting enabled syslog messages are supported.

Additional Configurations For TLS

If you select TLS as the protocol, the SmartConnector uses the certificates generated by the SmartConnector to authenticate and encrypt communication. The client authenticates the server by requesting its certificate. This verifies that the syslog-ng machine is correctly configured and communicating with the Syslog NG Daemon SmartConnector.

However, you can also provide the customer-supplied certificates for authentication for both remote management and Syslog NG Daemon.

For more information:

- To supply your own certificate for Syslog NG, see [Using a Customer-Supplied Certificate for Syslog NG Setup](#).
- To supply your own certificate for both remote management and Syslog NG, see [Using a Customer-Supplied Certificate for Both Remote Management and Syslog NG](#).
- To use mutual authentication, see [Configuring for Mutual Authentication](#) to import additional certificate.
- To receive events from any other SmartConnectors, see the [CEF File](#) topic in the [Installation Guide for ArcSight SmartConnectors](#).

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
```
7. 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 ["Adding TLS Function to the Syslog NG Setup"](#).
8. 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=
na,st=na,c=us
Creation date: Jan 26, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
```

[This is a partial output of `keytool -list`]

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=na,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=na,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 -providertype 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
```

12. Restart the connector to start using the new keystore and certificate. The certificate must also be copied to the syslog-ng machine. See steps 5-8 in ["Adding TLS Function to the Syslog NG Setup"](#).
13. 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.

Configuring for Mutual Authentication

For enhanced security, mutual authentication is now supported. This ensures that the Syslog NG source is authenticated 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

1. Enable Mutual Authentication

- a. After SmartConnector installation, open the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.
- b. Modify the `syslogng.mutual.auth.enabled` parameter from `false` to `true`.
- c. Save your change and restart the connector.

2. Copy the Certificate

Copy the `syslogngclient.pem` file to the machine on which the SmartConnector for Syslog NG Daemon is installed.

3. Import the Certificate

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

```
arcsight agent keytoolgui
```
- b. Open the keystore in `$ARCSIGHT_HOME/current/jre/lib/security/cacerts`. The password is `changeit`.
- c. From the menu bar, select **Tools** and **Import Certificate**. Upload the certificate file.
- d. Trust the certificate.
- e. 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). Import and trust the `remote_management.cer` certificate.

Post-Installation Permissions

The `current/user/agent/agentdata` folder stores raw events data and contains sensitive information which must be restricted using the following permissions:

- For Linux:

The required permissions for the `current/user/agent/agentdata` folder have been modified to reflect the permission set of `chmod 750`. The `chmod 750` sets permissions so that, the user/ owner can read, write, and execute. The group can read, can't write, and can execute. And others can't read, can't write, and can't execute.

- For Windows OS:

The user installing the connector and the system administrator must restrict permission for the `current/user/agent/agentdata` folder so that only they are authorized to access the folder and files present in it. For more information related to the folder permissions, check [Microsoft Documentation](#).



Note: This is applicable to all modes of installation and only for the user and the system administrator.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. For more information about the ArcSight data fields, see the [ArcSight Console User's Guide for ESM](#).

ArcSight ESM Field	Device-Specific Field
Connector Severity	Very High when Device Severity = emerg, crit, ALERT, alert, fatal, Critical, CRITICAL, or VeryHigh; High when Device Severity = err, Error, error, High, or err error; Medium when Device Severity = warn, Warning, warning, WARNING, Medium, or warn warning; Low when Device Severity = info, notice, debug, NOTIFICATION, success, NOTICE, Low
Device Custom IPv6 Address 2 Label	Source IPv6 Address
Device Custom IPv6 Address 3 Label	Destination IPv6 Address
Device Custom Number 1 Label	File Descriptor
Device Custom String 1	Module
Device Custom String 1 Label	Module
Device Custom String 2	One of (Facility1,Facility2,_SYSLOG_FACILITY)
Device Custom String 2 Label	Facility
Device Custom String 4	PID
Device Custom String 4 Label	PID
Device Custom String 6	Module
Device Facility	One of (Facility1,Facility2,_SYSLOG_FACILITY)
Device Process Name	ProcessHeader
Device Product	'Unix'
Device Severity	One of (Priority,severity,_SYSLOG_PRIORITY)
Device Time Zone	DetectTime
Device Vendor	'Unix'
External ID	ID
Name	One of (Message, WholeMessage)
Source User Name	Module

Appendix - Sample Configuration File

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](#).

```
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);  
};
```

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Syslog NG Daemon SmartConnector (SmartConnectors CE 24.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!