



Micro Focus Security ArcSight Connectors

SmartConnector for Blue Coat Proxy SG Multiple Server File

Configuration Guide

March 19, 2020

Configuration Guide

SmartConnector for Blue Coat Proxy SG Multiple Server File

March 19, 2020

Copyright © 2010 – 2020 Micro Focus or one of its affiliates.

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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

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

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.

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
03/19/2020	Added support for BlueCoat MultiServer File Main version 6.7 and 7.x. X-ICAP-Metadata in some token (Content Analysis header values for ICAP), it is a dynamic content that depends on the configurator, hence, additional data is used for them. File Id field is used as a general mapping for all uuid data.
04/16/2018	Added File Type mapping to ASG mappings.
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	Corrected parameter name from monitorinterval to monitoringinterval in Advanced Parameters section.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	Added version 6.6 support.
06/30/2015	Support removed for Blue Coat Proxy SG versions 5.2, 5.4, 5.5, and 6.1, due to product versions no longer supported by vendor. Updated configuration information.
02/16/2015	Added Device Custom Number 1 and Message mappings to support time-taken and x-exception-id events.
06/30/2014	Corrected the process for changing the 'processingthread' and 'monitorinterval' parameters for a folder.
03/31/2014	Added File Type mapping to Main and SSL mappings.
11/15/2013	Added version 6.5 support.
09/30/2013	Updated parameters and mappings.
05/15/2013	Added version 6.4 support.

SmartConnector for Blue Coat Proxy SG Multiple Server File

This guide provides information for installing the SmartConnector for Blue Coat Proxy SG Multiple Server File for log event collection. Blue Coat Proxy OS versions 6.3, 6.4, 6.5, 6.6, 6.7 and 7.x. are supported.

Product Overview

Blue Coat Proxy appliances provide visibility and control of Web communications to protect against risks from spyware, Web viruses, inappropriate Web surfing, instant messaging (IM), video streaming, and peer-to-peer (P2P) file sharing.

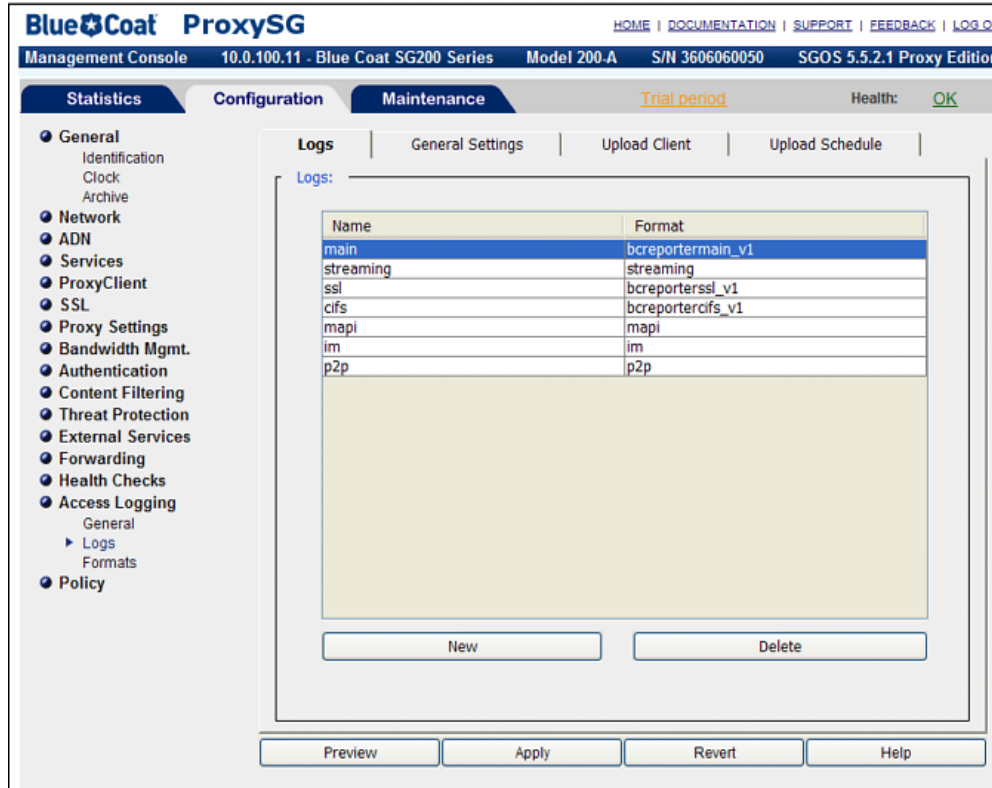
Configure the Blue Coat Proxy SG Device

Blue Coat Proxy SG supports multiple ways to upload access logs from a Proxy SG appliance to any computer running an FTP server or another receiver. In ArcSight's integration environment, Microsoft IIS FTP server is run to receive Blue Coat access logs.

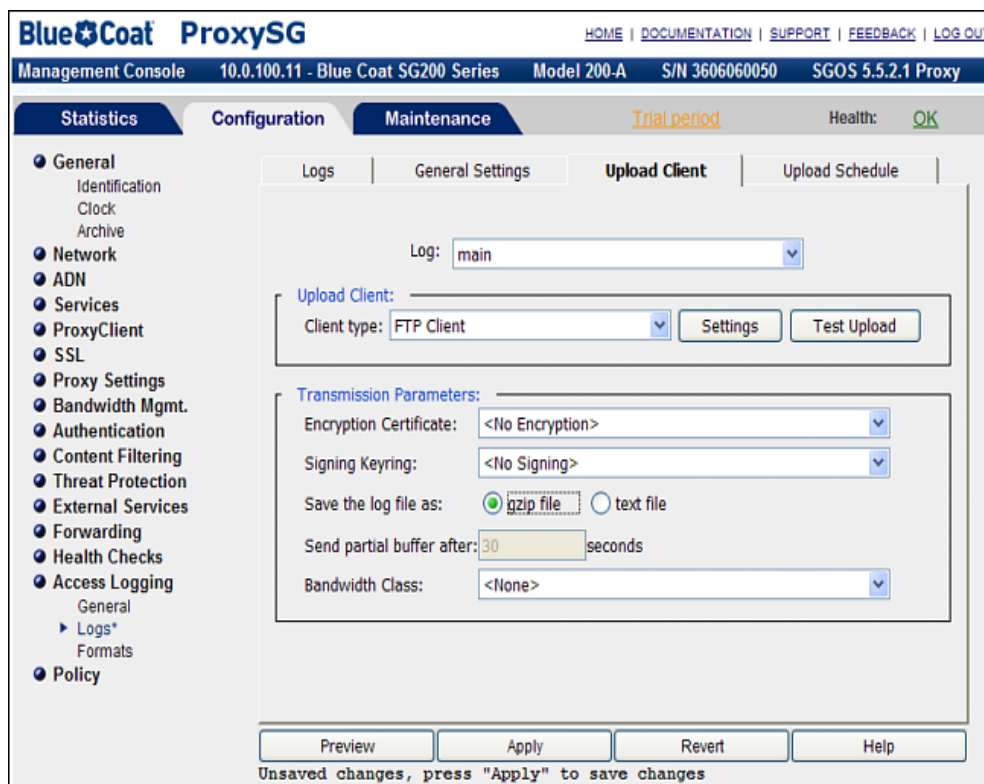


An FTP option is available on the ArcSight Connector Appliance. To use this option, FTP must be enabled on the appliance. See the *ArcSight Connector Appliance Administration Guide* for instructions.

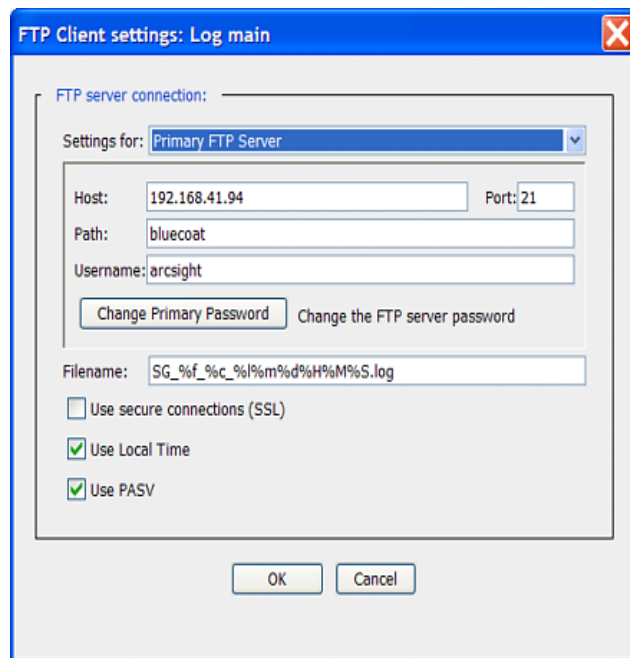
- 1 Using the Web interface, log in to the Proxy SG Management Console through any Web browser.
- 2 Click the **Configuration** tab; then click **Access Logging** and **Logs**.



- Multiple tabs are displayed on the right side. Click **Upload Client** to display the following window:



- 4 Follow these steps for each of the supported log types (main, im, ssl, streaming):
 - a Select the appropriate log type.
 - b Select **gzip file** or **text file** in the **Save the Log file as** field.
 - c Click **Settings**; the **FTP Settings** window is displayed. (In most cases, the FTP server should be your ArcSight SmartConnector machine.)



- d Select the primary or alternate FTP server you want to configure from the **Settings for** drop-down list.
- e Fill in the fields as appropriate:

Host: The name of the upload client host. When the **Use secure connections (SSL)** checkbox is selected, the hostname must match the hostname in the certificate presented by the server. To stop a log from uploading, clear the Host field.

Port: The default is 21; it can be changed.

Path: The directory path where the access log will be uploaded on the server. The full path to the FTP server will be required during Arcsight SmartConnector setup.

Username: This is the username that is known on the host you are configuring.

Change Password: Change the password on the FTP host by clicking this button.

- f Do not change the default value for **filename**; this is the file format that is expected by the SmartConnector. The filename includes specifiers and text that indicate the log name (%f), name of the external certificate used for encryption, if any (%c), the fourth

parameter of the ProxySG IP address (%I), the date and time (Month: %m, Day:%d, Hour: %H, Minute: %M, Second: %S), and the .log or .gzip.log file extension.

Write down what you enter in the **Filename** field; you will need it during ArcSight SmartConnector setup.

- g Click **Apply**, then perform steps a-g for the remaining supported log types.
- 5 When you finish completing step 4 for all four supported log types, click **OK** to return to the **Upload Client** tab.
- 6 Click the **Upload Schedule** tab next to the **Upload Client** tab. For compressed logs, or when installing the connector on the Connector Appliance, select **periodically** for the **Upload the access log** field. For all other types, you can choose either **periodically** or **continuously**.

The screenshot shows the Blue Coat ProxySG Management Console interface. The top navigation bar includes links for HOME, DOCUMENTATION, SUPPORT, FEEDBACK, and LOG OUT. The main header displays system information: Management Console, 10.0.100.11 - Blue Coat SG200 Series, Model 200-A, S/N 3606060050, and SGOS 5.5.2.1 Proxy. The left sidebar contains a tree view of configuration categories, with 'Logs' expanded under 'Access Logging'. The main content area is divided into tabs: Logs, General Settings, Upload Client, and Upload Schedule. The 'Upload Schedule' tab is active, showing a 'Log' dropdown set to 'main'. Below this, the 'Upload type' section has radio buttons for 'continuously' and 'periodically', with 'periodically' selected. Two input fields are present: 'Wait between connect attempts' (60 seconds) and 'Time between keep-alive log packets' (300 seconds). The 'Upload the log file' section has radio buttons for 'Daily at 2:00 a.m.' (selected) and 'Every 0 hours 1 minutes'. 'Upload Now' and 'Cancel Upload' buttons are located to the right. At the bottom, there are 'Preview', 'Apply', 'Revert', and 'Help' buttons, along with a status message: 'Unsaved changes, press "Apply" to save changes'.

- 7 Keep the **minutes** field as **0** if you select **Every** for **Rotate the log file**.
- 8 Click **Apply**.

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

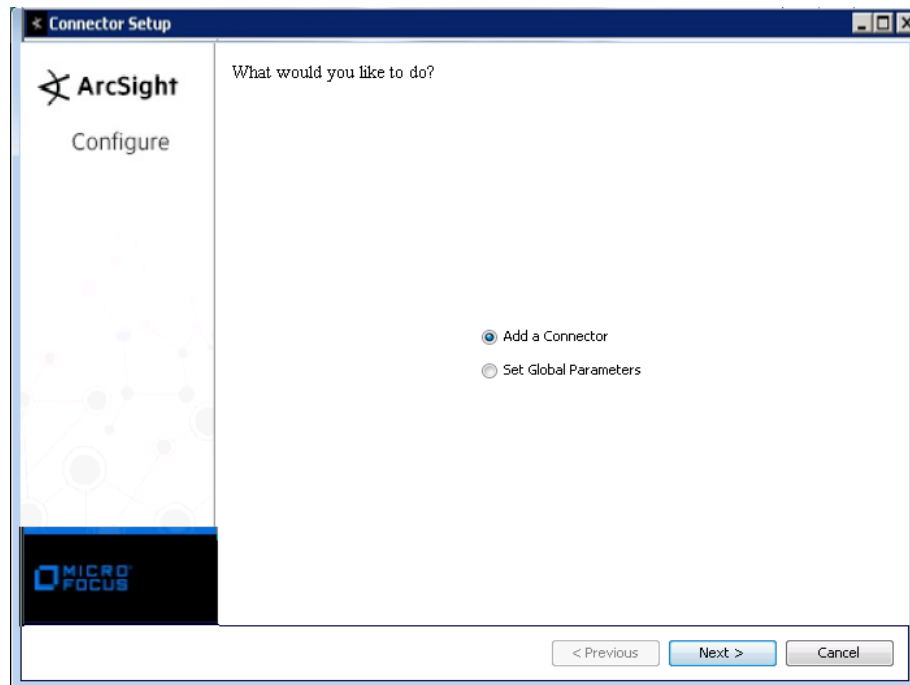
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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.

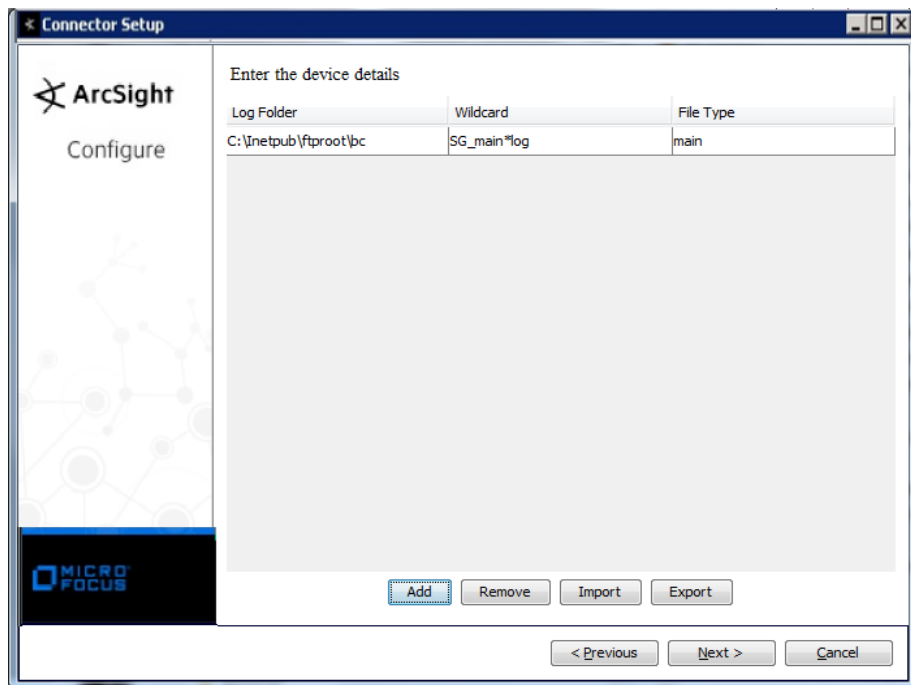
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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.

Parameter	Setting
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 **BlueCoat Proxy SG Multiple Server File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log Folder	Enter the name of the folder on the remote device that contains all Blue Coat access log files. The default value is 'C:\inetpub\ftproot\bc'. For Connector Appliance users configuring the connector with FTP, enter the FTP directory (such as '/opt/arcSight/incoming') from which the connector is to read.
Wildcard	Enter the template the SmartConnector is to use to determine the format of the log files to be uploaded; accept the default value of 'SG_main.*log' for text log file type or change the value to 'SG_main.*gz' for the gzip log type.
File Type	Enter the name of the log file type; possible values are 'main', 'im', 'ssl', and 'streaming'. When you click 'Add', the first line is filled in with default values. First, enter the parameters for the 'main' log, then click 'Add' again. This time, click on the file type (main) and select the next supported file type (im). Enter the parameters for the 'im' log, then click 'Add' again to add the parameters for the 'ssl' log and the 'streaming' log.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

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.

Blue Coat Proxy SG ASG Events Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	cs-uri-scheme
Bytes In	sc-bytes
Bytes Out	cs-bytes
Destination Host Name	
Device Action	sc-filter-result
Device Address	s-ip
Device Custom IPv6 Address 2	c-ip
Device Custom Number 1	time-taken
Device Custom String 1	x-virus-id

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	x-bluecoat-transaction-uuid
Device Custom String 3	cs-threat-risk
Device Custom String 4	cs-categories
Device Custom String 5	x-bluecoat-application-operation
Device Custom String 6	cs-auth-group
Device Event Class Id	oneOf(s-action,"ASG Action")
Device Outbound Interface	r-ip
Device Product	Advanced Secure Gateway
Device Receipt Time	localtime
Device Severity	sc-status
Device Vendor	Blue Coat
File Type	rs(Content-Type)
Message	x-exception-id
Name	oneof(s-action,"Blue Coat Misc. ASG")
Request Client Application	cs(User-Agent)
Request Context	cs(Referer)
Request Method	cs-method
Request Url	concatenate(cs-uri-scheme,":", "/",cs-host,":",cs-uri-port,cs-uri-path,___ifThenElse(cs-uri-query,"-",",cs-uri-query)))
Source Address	oneOf(c-ip,s-supplier-ip)
Source NtDomain	x-cs-auth-domain
Source User Name	cs-username

Blue Coat Proxy SG Main Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additionaldata.xicapReqmodHeader	x-icap-reqmod-header(X-ICAP-Metadata)
additionaldata.xicapRespmodHeader	x-icap-respmod-header(X-ICAP-Metadata)
Agent (Connector) Severity	High = 400 – 599; Medium = 300 – 399; Low = 0 – 299
Application Protocol	cs-uri-scheme
Bytes In	sc-bytes
Bytes Out	cs-bytes
Destination Address	One of (cs-ip, r-supplier-ip)
Destination Host Name	One of (s-supplier-name, cs-host)
Destination HostName	x-bluecoat-appliance-name
Destination Port	s-port
Device Action	sc-filter-result
Device Address	One of (x-bluecoat-proxy-primary-address, s-ip)
Device Custom IPv6 Address 1	s-ip (device IPv6 address)
Device Custom IPv6 Address 2	c-ip (source IPv6 address)
Device Custom IPv6 Address 3	cs-host (destination IPv6 address)
Device Custom Number 1	time-taken
Device Custom Number 2	x-bluecoat-total-time-added

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2 Label	"Total Time Added"
Device Custom Number 3	x-bluecoat-total-policy-evaluation-time
Device Custom Number 3 Label	"Total Policy Evaluation Time"
Device Custom String 1	x-virus-id
Device Custom String 2	sc-filter-category
Device Custom String 3	r-supplier-ip
Device Custom String 4	cs-categories
Device Custom String 5	x-bluecoat-application-operation
Device Custom String 6	cs-auth-group
Device Event Category	'main'
Device Event Class ID	s-action
Device Outbound Interface	r-ip
Device Process Name	s-sitename
Device Product	'Proxy SG'
Device Receipt Time	date, time
Device Severity	sc-status
Device Vendor	'Blue Coat'
File Id	x-bluecoat-transaction-uuid
File Type	One of (rs(Content-Type), cs-uri-extension)
Message	x-exception-id
Name	One of (s-action, 'Blue Coat Misc. Main Event')
Old File Id	rs-service-latency
Request Client Application	cs (User-Agent)
Request Context	One of (cs (Referer), x-bluecoat-application-name)
Request Method	cs-method
Request Protocol	cs-uri-scheme
Request URL File Name	cs-uri-path
Request URL Host	cs-host
Request URL Port	cs-uri-port
Request URL Query	cs-uri-query
Source Address	One of(c-ip,s-supplier-ip)
Source User Name	cs-username

Blue Coat Proxy SG IM Events Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = DENIED, TCP_DENIED, UDP_DENIED; Medium = FAILED, TCP_ERR_MISS, TCP_POLICY_REDIRECT, UDP_INVALID, UDP_MISS; Low = ALLOWED, 0 - 299
Application Protocol	cs-protocol
Destination Address	One of (cs-ip, r-supplier-ip)
Destination User ID	x-im-buddy-id
Destination User Name	x-im-buddy-name
Device Address	One of (x-bluecoat-proxy-primary-address, s-ip)

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	r-supplier-ip
Device Custom String 4	cs-auth-group
Device Custom String 5	x-im-user-state
Device Custom String 6	cs-auth-group
Device Event Category	'im'
Device Event Class ID	One of (x-im-method, both (x-im-method, s-action) when s-action present)
Device Product	'Proxy SG'
Device Receipt Time	date, time
Device Severity	One of (s-action, '0')
Device Vendor	'Blue Coat'
File Path	x-im-file-path
File Size	x-im-file-size
Message	x-im-message-text
Name	One of (x-im-method, 'Blue Coat Misc. Im Event')
Source Address	c-ip
Source Service Name	x-im-client-info
Source User ID	x-im-user-id
Source User Name	One of (x-im-user-name, cs-username)

Blue Coat Proxy SG SSL Events Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = CERT_UNTRUSTED_ISSUER, 400..599, 0; Medium = 300..399, Medium; Low = 100..299, Low
Application Protocol	cs-uri-scheme
Bytes In	One of (x-rs-connection-negotiated-cipher-size, sc-bytes)
Bytes Out	One of (x-cs-connection-negotiated-cipher-size, cs-bytes)
Destination Address	One of (cs-ip, r-supplier-ip)
Destination Host Name	One of (s-supplier-name, cs-host)
Device Action	sc-filter-result
Device Address	One of (x-bluecoat-proxy-primary-address, s-ip)
Device Custom IPv6 Address 1	s-ip (Device IPv6 Address)
Device Custom IPv6 Address 2	c-ip (Source IPv6 Address)
Device Custom IPv6 Address 3	cs-host (Destination IPv6 Address)
Device Custom Number 1	time-taken
Device Custom String 1	x-virus-id
Device Custom String 3	r-supplier-ip
Device Custom String 4	cs-categories
Device Custom String 6	cs-auth-group
Device Event Category	'ssl'
Device Event Class ID	One of (s-action, 'SSL Action')
Device Inbound Interface	c-ip
Device Outbound Interface	One of (cs-host, s-ip)

ArcSight ESM Field	Device-Specific Field
Device Process Name	s-sitename
Device Product	'Proxy SG'
Device Receipt Time	date, time
Device Severity	One of (x-rs-certificate-validate-status, 'Low', sc-status, 'Medium' when s-action is TCP_ERR_MISS)
Device Vendor	'Blue Coat'
File Type	One of (rs(Content-Type), cs-uri-extension)
Message	One of (x-rs-certificate-observed-errors, x-exception-id)
Name	One of (s-action, 'Blue Coat Misc. SSL Event')
Request Client Application	cs(User-Agent)
Request Method	cs-method
Source Address	One of (c-ip, s-supplier-ip)
Source User Name	cs-username

Blue Coat Proxy SG Streaming Events Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400 – 599; Medium = 300 – 399; Low = 0 – 299
Application Protocol	protocol
Bytes In	sc-bytes
Destination Address	One of (cs-ip, r-supplier-ip)
Destination DNS Domain	s-dns
Device Address	One of (x-bluecoat-proxy-primary-address, s-ip)
Device Custom IPv6 Address 1	s-ip (device IPv6 address)
Device Custom IPv6 Address 2	One of (x-client-address, c-ip) (source IPv6 address)
Device Custom IPv6 Address 3	cs-host (destination IPv6 address)
Device Custom String 3	r-supplier-ip
Device Custom String 4	s-session-id
Device Event Category	'streaming'
Device Event Class ID	One of (xs-cache-info, both (s-cache-info, c-status))
Device Product	'Proxy SG'
Device Receipt Time	date, time
Device Severity	One of (c-status, '0')
Device Vendor	'Blue Coat'
File Path	cs-uri-stem
File Size	filesize
Message	x-cache-info
Name	One of (s-action, x-cache-info, 'Blue Coat Misc. Streaming Event')
Request Client Application	cs(User-Agent)
Request Context	cs(Referer)
Request Protocol	cs-uri-scheme
Request URL	cs-uri-stem
Request URL File Name	cs-uri-path

ArcSight ESM Field	Device-Specific Field
Request URL Host	cs-host
Request URL Port	cs-uri-port
Request URL Query	cs-uri-query
Source Address	One of (x-client-address, c-ip)
Source DNS Domain	c-dns
Source Process Name	c-hostexe
Source Service name	Both (videocodec, audiocodec)
Source User Name	x-cache-user
Transport protocol	transport

SmartConnector Advanced Parameters

Parameters can be adjusted that control how long and how often the log file continues to be monitored for additions. The values are in milliseconds; The monitoring interval is set to 30 seconds by default and the processing threshold is set to 24 hours by default. With a processing threshold of 24 hours, the file will be marked as 'processed' only after 24 hours, which is a change from previous behavior.

The `processingthreshold` parameter can be set to a negative value (such as -1), in which the connector processes and deletes or persists in the log file according to the mode set in the parameters for all files but the most recent. The most recent file is considered to be current and continues being watched. If you want to stop watching the most recent file in the directory, reset the `processingthreshold` to a positive value, such as 24 hours (86400000 milliseconds), to be sure the file is no longer updated.

The `monitoringinterval` value determines how often the connector checks to determine whether the file was updated; the checking starts after all records in a file have been read and processed. The monitor interval should be less than the processing threshold. For example, the monitor interval default value is 30 seconds (30000 milliseconds) and the processing threshold could be a few hours.

Update the following parameters in the `user/agent/agent.properties` file in the installation directory of the connector before starting the connector.

- Change the `processingthreshold` parameter value from a negative value (-1, for instance) back to the default 24 hours in milliseconds, shown as:
`foldertable.processingthreshold=86400000.`
- Change the `monitoringinterval` parameter value from the default (30 seconds/30000 milliseconds), to 2 hours in milliseconds, shown as:
`foldertable.monitoringinterval=7200000.`



The above values are applied when the `processingmode` value equals 'realtime' (not batch.)

Connector Appliance Settings

When installing the connector on an ArcSight Connector Appliance, update the following parameters in the `user/agent/agent.properties` file in the installation directory of the connector before starting the connector.

- To indicate to delete the file after processing rather than renaming it in the same directory, change `mode=RenameFileInTheSameDirectory` to `mode>DeleteFile`.
- To have the connector run in batch rather than the realtime default mode, change `processingmode=realtime` to `processingmode=batch`.

SmartConnector Troubleshooting

What if I do not want to use FTP as an Upload Client?

Blue Coat supports other clients for uploading purposes. Discussing each of them is beyond our scope. See the Blue Coat documentation or contact Blue Coat support if you have any problem using other upload clients.

The logs are sent through the network and they should be encrypted.

You are right. Blue Coat also supports secure transmission for your access logs. Again, discussing each of Blue Coat's options is beyond our scope. See the Blue Coat documentation or contact Blue Coat support if you encounter problems using secure transmission.

It seems IIS FTP server buffer logs in somewhere before it writes them to file so the events are not really realtime events.

This is true. Based upon our lab testing, there is a delay of a maximum of about 10 minutes if events are generated at a rate of 6 per second. The delay is a maximum of 20 minutes if events are generated at a rate of 2 per second. You can use other FTP servers if you do not satisfy IIS FTP Server.