



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight Connectors**

SmartConnector for IBM Lotus Domino Web  
Server File

Configuration Guide

November 30, 2016

## Configuration Guide

### SmartConnector for IBM Lotus Domino Web Server File

November 30, 2016

Copyright © 2005 – 2016 Hewlett Packard Enterprise Development LP

#### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

#### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

## Revision History

---

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
09/24/2010	Updated supported versions.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure for FIPS support.
02/14/2008	Added field mapping for Request Method.

---

---

## SmartConnector for IBM Lotus Domino Web Server File

---

This guide provides information for installing the SmartConnector for IBM Lotus Domino Web Server File for log file event collection. This SmartConnector is supported for installation on Windows platforms. IBM Lotus Domino Web Server version 6.5 is supported.

### Product Overview

The IBM Lotus Domino Web Server is an integrated Web application server that can host Web sites that both Internet and intranet clients can access, and can serve pages that are stored in the file system or in a Domino database. When a Web browser requests a page in a Domino database, Domino translates the document into HTML. When a Web browser requests a page in an HTML file, Domino reads the file directly from the file system. Then the Web server uses the HTTP protocol to transfer the information to the Web browser. Using Domino, any change made to a database is automatically reflected on the Web server.

### Preparing for SmartConnector Installation

#### Installing Domino on Windows Systems

- 1 Before installing the Lotus Domino Server program files on a Windows system:
  - ◆ Make sure that the required hardware and software components are in place and working
  - ◆ Read the Release Notes for operating system and network protocol requirements and for any last-minute changes or additions to the documentation.
  - ◆ Temporarily disable any screen savers and turn off any virus-detection software.
  - ◆ Make sure that all other applications are closed. Otherwise, you could corrupt any shared files, and the installation program might not run properly.
  - ◆ If you are upgrading to Lotus Domino from a previous release, see IBM's Lotus Domino *Upgrade Guide*.
- 2 Run the install program **setup.exe**, which is on the installation CD.
- 3 Read the Welcome window and click **Next**. Then read the License Agreement and click **Yes**.
- 4 Enter the administrator's name and the company name.
- 5 Choose whether you want to install partitioned servers.
- 6 Select the program and data directory in which to copy the software; then click **Next**. If you are installing partitioned servers, select only a program directory.
- 7 Select the server type you acquired:

- ◆ Domino Utility Server: Installs a Lotus Domino server that provides application services only, with support for Lotus Domino clusters. The Domino Utility Server is a new installation type for Lotus Domino 6 that removes client access license requirements. Note that it does **not** include support for messaging services.
- ◆ Domino Messaging Server: Installs a Lotus Domino server that provides messaging services. Note that it does **not** include support for application services or Lotus Domino clusters.
- ◆ Domino Enterprise Server: Installs a Lotus Domino server that provides both messaging and application services, with support for Lotus Domino clusters.



All three types of installation support Lotus Domino partitioned servers. Only the Lotus Domino Enterprise Server supports a service provider (xSP) environment.

---

- 8 Click **Customize** to select which components to install, or click **Next** to accept all components.
- 9 If you are installing a partitioned server, specify a data directory for each partition.
- 10 Specify the program folder or accept Lotus Applications as a program folder that will contain the software.
- 11 Click **Finish** to complete the install program.
- 12 Select **Start -> All Programs -> Lotus Applications -> Lotus Domino Server** to start the Server Setup program.

Comprehensive installation instructions for IBM Lotus Domino Web Server can be found in IBM product documentation.

## Installing and Setting Up the Lotus Domino Administrator

When you install and set up a Lotus Domino server, the Server Setup program does not install the Lotus Domino Administrator, which is the administration client. You must run the Lotus Domino Administrator client setup to install the Lotus Domino Administrator client.



Do not install the Lotus Domino Administrator on the same system on which you installed the Lotus Domino server. Doing so compromises Lotus Domino's security and impairs server performance.

---

To set up the Lotus Domino Administrator:

- 1 Make sure the Lotus Domino server is running.
- 2 Start the Lotus Domino Administrator.
- 3 The first time you start the Lotus Domino Administrator, a setup wizard starts. After you answer the questions displayed by the setup wizard, the Lotus Domino Administrator client opens automatically.

## Starting the Lotus Domino Administrator

To start Lotus Domino Administrator:

- 1 Make sure the Lotus Domino server is running.
- 2 Do one of the following:
  - ◆ From the Windows control panel, click **Start -> Programs -> Lotus Applications -> Lotus Domino Administrator**.
  - ◆ Click the **Lotus Domino Administrator** icon on the desktop.
  - ◆ From the Notes client, click the **Lotus Domino Administrator** bookmark button or select **File -> Tools -> Server Administration**.

## Lotus Domino Web Logging

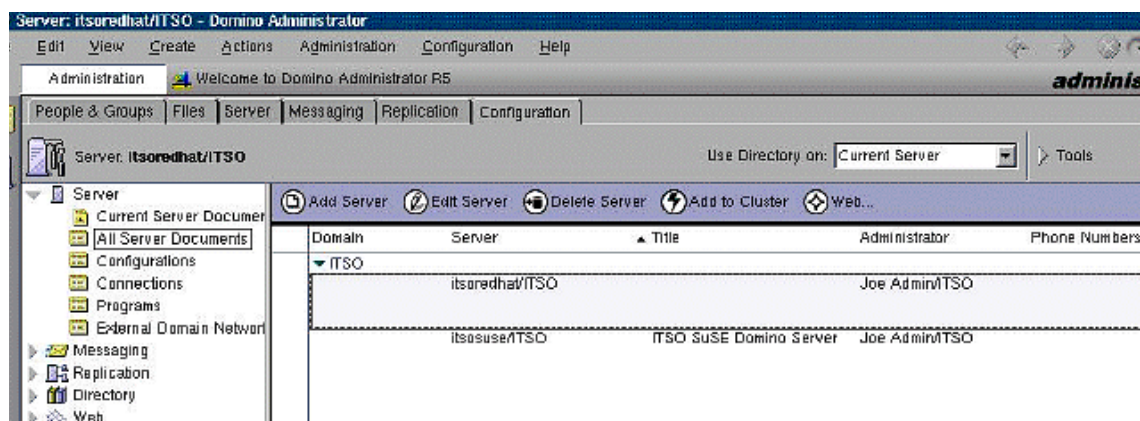
To set up logging on your Lotus Domino server, enable one of the logging methods in the HTTP section of the server document in the Lotus Domino Directory. (Because logging is very server-intensive, it is disabled by default.) When you enable logging to text files and specify a directory for the files, Lotus Domino automatically creates the access log and error log files.

Notice that you can select the format for the access log files (Common or Extended Common) and the time format (LocalTime or GMT). The Common format records only access information. The Extended format tracks access, agent, and referred information in the access log file.

## Changing Settings on the Lotus Domino Web Server

To change the settings of the Lotus Domino Web server:

- 1 Start the Lotus Domino Administrator.
- 2 Choose the server you want to reconfigure.
- 3 Choose the **Configuration** tab.
- 4 Choose **Server -> All Server Documents**.
- 5 Double-click on the name of the Lotus Domino server you want to change or select the server and click **Edit Server**.



- 6 To change the Lotus Domino Web server port, click **Ports -> Internet Ports** in the server document. The **Web** tab should be selected by default. It is best to use the default port 80 for a non-secure Web server and port 443 for a secure Web server.

Here you also can select whether to allow name and password authentication for clients connecting over TCP/IP; the default is **Yes**. Also specify whether to allow anonymous connection over TCP/IP; again, the default is **Yes**. The same is true for the SSL protocol.

- 7 Next, select **Internet Protocols -> HTTP**. In this section, make at least the following changes:
- ◆ In the **Basic** section, enter a **hostname** and enable the **Bind to host name** option if you use a Lotus Domino partitioned environment. Also set the **Maximum request over a single connection** and **Number of active threads**, options.
  - ◆ In the **Mapping** section, customize the **Home URL**. It should be either a Notes database or an HTML file.



The secure server will not run until you create a server certificate.

## Setting up Lotus Domino Web Server Logging to Text Files

To set up logging the Lotus Domino Web Server to text files, you must enable logging (by default, logging is disabled). By default, Lotus Domino stores log files in the data directory. While the Web server is running, it creates new log files depending upon the log file duration settings. If the Web server is not running, it creates log files as needed when the Web server is started.

Some information may increase the size of the log file without providing meaningful information, such as requests for graphics or icons, so you may want to exclude that type of information from the log.

To enable logging to text files:

- 1 From the **Lotus Domino Administrator**, click the **Configuration** tab.
- 2 Open the Server document for the Web server.
- 3 Click the **Internet Protocols - HTTP** tab.
- 4 Under **Enable Logging To**, select the **Enable the Log Files** field.
- 5 Under **Log File Settings**, complete these fields:
  - ◆ Access Log format
  - ◆ Time format
  - ◆ Log file duration
  - ◆ Maximum log entry length
  - ◆ Maximum size of access log
- 5 Under **Log File Names**, complete these fields:

Directory for log files  
The directory to store the log files; if this field is blank, Domino stores the log files in the data directory.

Access log  
The prefix to use when creating the Access log file. The default is access. Do not enter a file extension. For example, with the prefix set to **access**, an access log file name could be `access12072005.log`.
- 7 (Optional) Under **Exclude From Logging**, complete the fields as necessary to exclude certain types of information from the log file.
- 8 Save the document.

## Install the SmartConnector

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



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

## 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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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

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

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

## Install Core Software

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

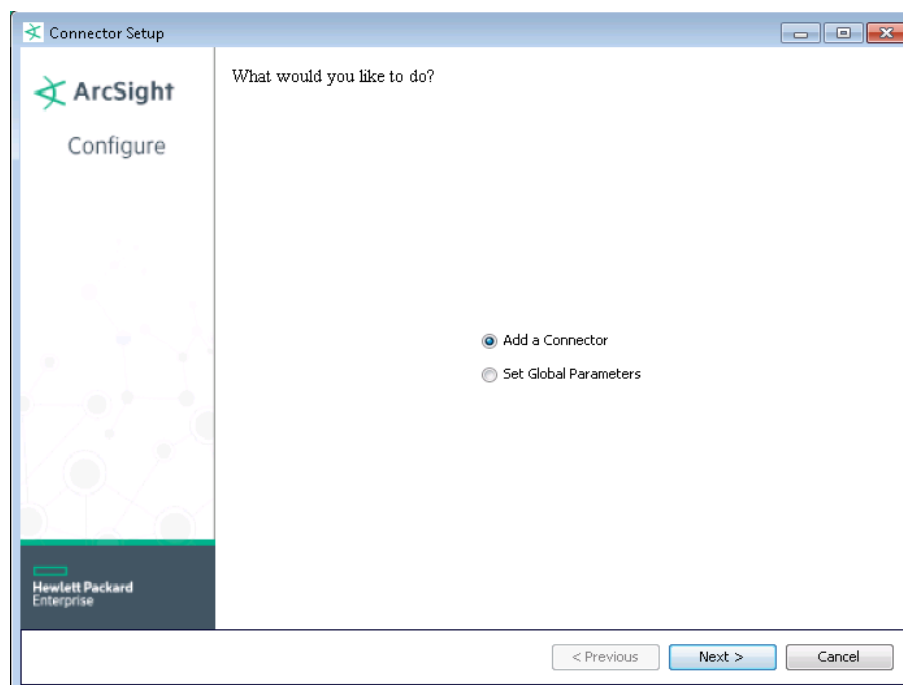
- 1 Download the SmartConnector executable for your operating system from the HPE SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

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

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

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





## Set Global Parameters (optional)

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

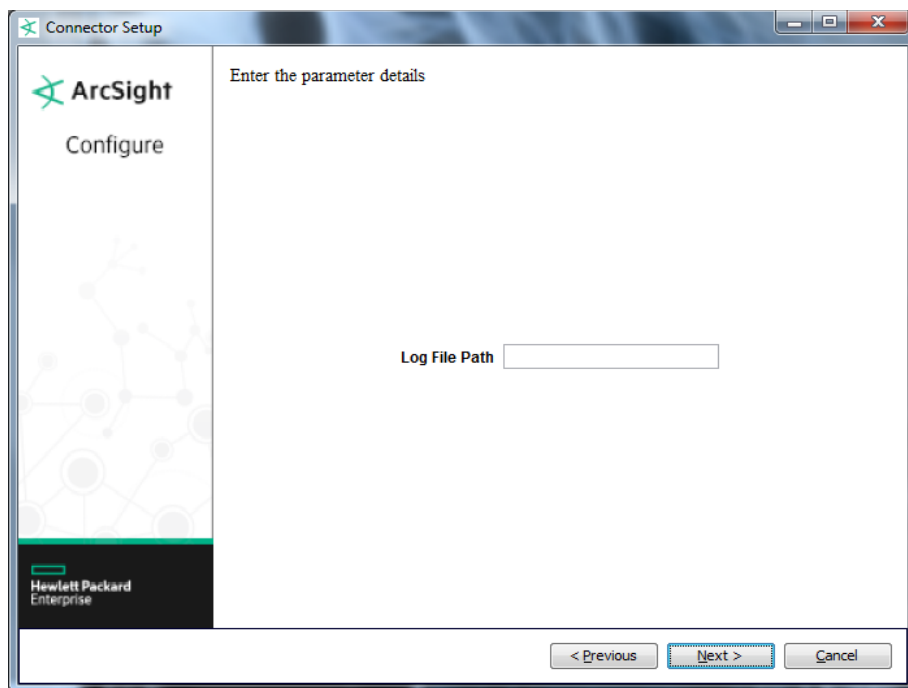
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote 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 'Disable'.
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	If 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. When both values are present, the initial setting is 'IPv4'.

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 the "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 **IBM Lotus Domino Web Server File** and click **Next**.

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



Parameter	Description
Log File	Full path to the log file.

## Select a Destination

- 1 The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)
- 2 Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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 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 some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.



Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

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.

### IBM Lotus Domino Web Server Field Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	Service plus Service Version
Bytes Out	Bytes
Destination Address	Dst Address

**ArcSight ESM Field**

Destination UserID  
Device Custom String 1  
Device Custom String 2  
Device Custom String 3  
Device Event Class Id  
Device Product  
Device Receipt Time  
Device Severity  
Device Vendor  
Name  
Request Client Application  
Request Cookies  
Request Method  
Request URL  
Source Address  
Transport Protocol

**Device-Specific Field**

Auth User  
Elapse Time (ms)  
Translated URL  
Referring URL  
Return Code  
Domino Web Server  
Date  
Return Code  
IBM  
Domino Web Access  
User Agent  
Cookie  
Method  
Request  
Src Address  
TCP

---