Micro Focus Security ArcSight Connectors

SmartConnector for Oracle WebLogic Server File

Configuration Guide

August 21, 2019

Configuration Guide

SmartConnector for Oracle WebLogic Server File

August 21, 2019

Legal Notices

Trademark Notices

Revision History

Date	Description
08/21/2019	Added support for Weblogic Access version 12.1.3.
12/17/2018	Added support for Weblogic Access version 10.3.6.

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2013	Added support for BEA WebLogic v10.3 and Oracle WebLogic v12.0.
05/15/2012	Added new installation procedure.
03/30/2012	Source Host Name rather than Destination Host Name is now mapped to Host Name.
02/15/2012	First version of this Configuration Guide.

SmartConnector for Oracle WebLogic Server File

This guide provides information for installing the SmartConnector for Oracle WebLogic Server File and configuring the device for log event collection. WebLogic Server versions 10.3.3, 10.3.6 and 12.0.0 are supported.

Product Overview

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is a foundation for building applications based on Service Oriented Architectures (SOA). SOA is a design methodology aimed at maximizing the reuse of application services.

System administration of a WebLogic Server environment includes tasks such as creating WebLogic Server domains, deploying applications, migrating domains from development environments to production environments, monitoring and configuring the performance of the WebLogic Server domain, and diagnosing and troubleshooting problems. WebLogic Server provides many tools for system administrators to help with these tasks, including a browser-based Administration Console.

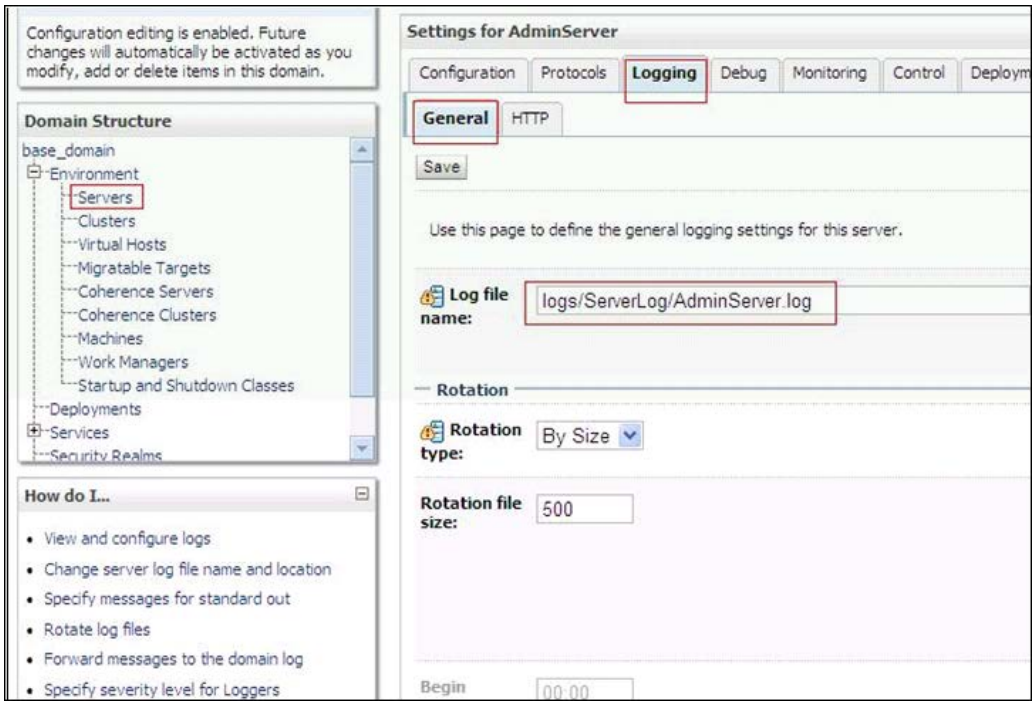
This connector supports event collection from server and access logs. The server log records information about events such as the startup and shutdown of servers, the deployment of new applications, or the failure of one or more subsystems. The messages include information about the time and date of the event as well as the ID of the user who initiated the event. The server log file is located on the computer that hosts the server instance. The HTTP subsystem keeps a log of all HTTP transactions. The default location and rotation policy for HTTP access logs is the same as the server log.

Configuration

For complete information about WebLogic logging, see the Oracle WebLogic Server Administration Console Online Help. You can access the online help either through the Console itself, or online at http://download.oracle.com/docs/cd/E15523_01/apirefs.1111/e13952/core/index.html.

To configure logging prior to connector installation:

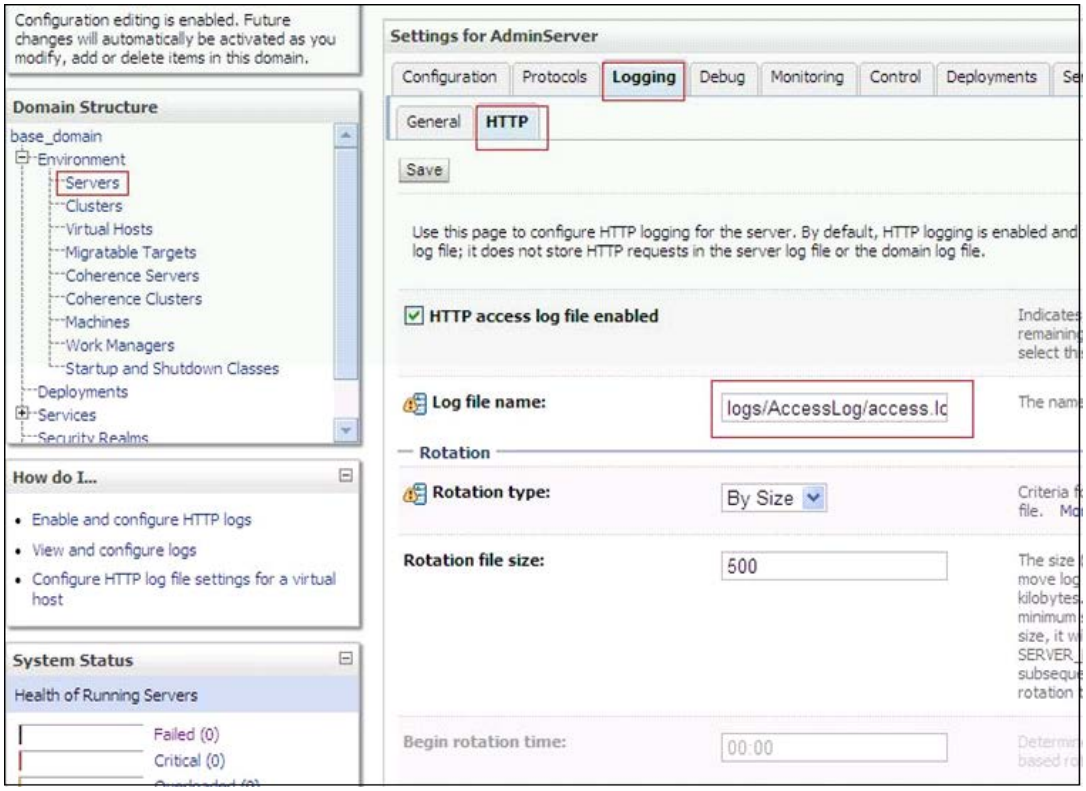
1. In the left pane of the Administration Console, click the name of the domain.
2. In the right pane, click the **Logging** tab and the **General** tab.
3. In the **Log file name** box, enter a path and filename for the server log. Enter an absolute pathname or a pathname that is relative to the server's root directory.



4 Click **Save**.

5 Select the **HTTP** tab.

6 Enter the **Log file name** for the Access log; enter an absolute pathname or a pathname that is relative to the server's Access log directory. Make sure **HTTP access log file enabled** is selected.



7 Click **Save**.

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).

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

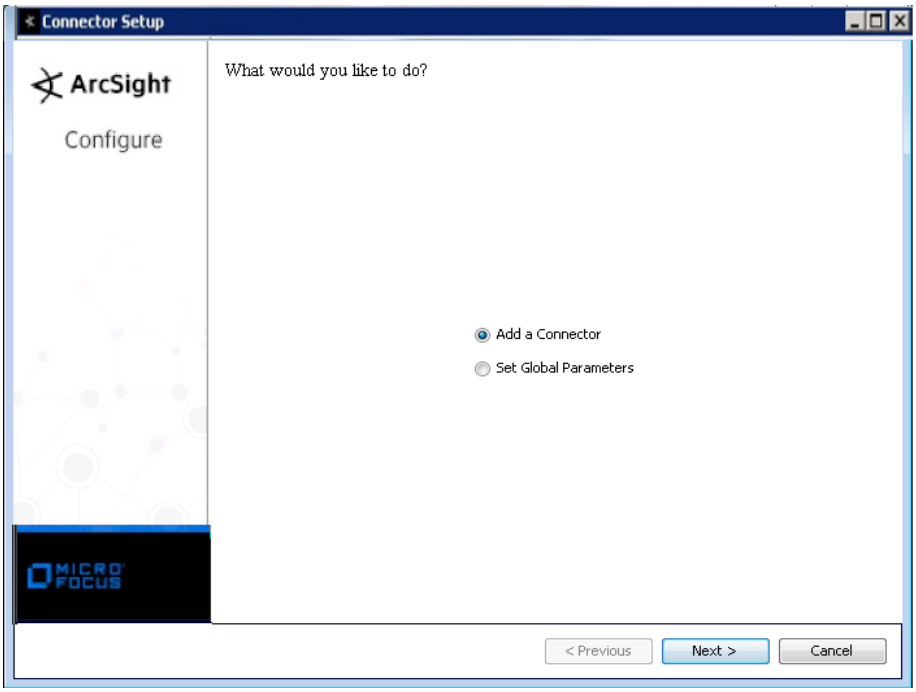
Install Core Software

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.

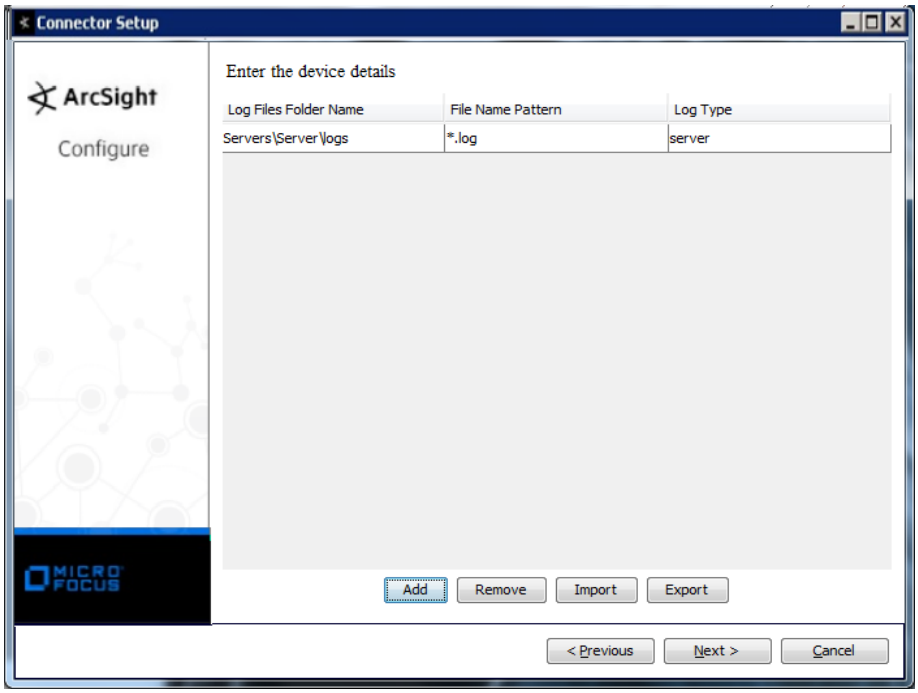
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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 **Oracle WebLogic Server File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log Files Folder Name	Each WebLogic Server instance writes all messages from its subsystems and applications to a log file on its host machine. Enter the full path to the log file folder here; for example, <domain-name>/servers/<server_name>/logs/<server-name>.log
File Name Pattern	For the file name pattern, enter anything that matches files to be processed for real-time mode. For example, if the directory has 'exampleServer.log, exampleServer.log.1, ..., medServer.log, medServer.log1', you want to eliminate processed files (such as 'example.Server.log.1') and process real-time log files. Entering 'ex*.log' as the pattern would cause the example.Server.log to be read; 'med*.log' would cause the medServer.log to be read; '*Server.log' would cause the connector to read all log files with 'Server.log' as the last part of the file name.
Log Type	Select 'access' or 'server' as the log file type. If you have both access and server logs in the same folder, enter a separate line in the table for each log type.

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.

WebLogic Access Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400..599; Medium = 300..399; Low = 100..299
Application Protocol	httpVersion
Bytes Out	bytes
Destination User Id	authUser
Device Action	status
Device Event Class Id	status
Device Product	'WebLogic Server'
Device Receipt Time	date
Device Severity	status
Device Vendor	'Oracle'
Name	All ('Method: ',method,' Error Code:',status)
Request Method	method
Request Url	requestURI
Source Host Name	Host Name
Source User Name	RFC931

WebLogic Server Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector Severity)	High = Critical, Alert, Emergency; Medium = Error, Warning, Notice; Low = Info, Debug
Application Protocol	Protocol
Destination Host Name	machineName
Destination Port	Port
Destination Process Name	threadID
Destination Service Name	Service Name
Destination User Name	user
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom String 1	SubSystem
Device Custom String 2	serverName
Device Event Class ID	One of (messageID, both (Prefix message, messageID))
Device Product	'WebLogic Server'
Device Receipt Time	Timestamp
Device Severity	severity
Device Vendor	'Oracle'
Device Version	WebLogic Server version
External ID	transactionID
File Name	File Name
File Path	File Path
Name	message
Source Address	Address

WebLogic Access v10.3.6 Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400..599; Medium = 300..399; Low = 100..299
Bytes Out	bytes
Destination User Id	verintUserName
Device Action	status
Device CustomString3	timeTaken
Device CustomString3 Label	Time Taken
Device Event Class ID	status
Device Product	'WebLogic Server'
Device Receipt Time	date
Device Severity	status
Device Vendor	'Oracle'
Name	All('Method: ',method,' Error Code:',status)
Request Method	method
Request Url	url
Source HostName	hostName

WebLogic Access v12.1.3 Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity High	400..599; Medium = 300..399; Low = 100..299
Application Protocol	x-Protocol
Bytes Out	bytes
Destination Address	One of (x-ClientIP,x-ForwardedFor)
Destination HostName	x-Host
Destination Port	x-Host
Destination User Name	x-AuthUser
Device Action	sc-status
Device Class ID	sc-status
Device CustomString2	x-AcceptLanguage
Device CustomString3	timeTaken
Device CustomString4	x-Scheme
Device CustomString5	x-Referer
Device Product	stringConstant("WebLogic Server")
Device Receipt Time	date
Device Severity	sc-status
Device Vendor	stringConstant("Oracle")
Name	All of("Method: ",cs-method," Error Code: ",sc-status)
Request Client Application	x-UserAgent
Request Method	cs-method
Request Url	cs-uri
Source Address	c-ip