Micro Focus Security ArcSight Connectors

SmartConnector for Tenable Nessus .nessus File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Tenable Nessus .nessus File

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	Removed Device Custom IPv6 Address 3 mapping.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
10/28/2016	Added support for version 6.8 and updated mappings. Removed support for versions 4.0, 4.2, 4.4, and 5.0 due to end of support by vendor.
09/30/2016	Added support for version 6.6 and updated mappings.
08/12/2015	Added support for version 6.5 and updated mappings.
09/30/2015	Updated screen shot of parameter window.
05/15/2015	Added mappings to support user-defined plug-in IDs for the source of 'Open Ports' data.
03/31/2015	Support ended for Nessus file format v1 and Nessus Vulnerability Scanner version 3.2.

SmartConnector for Tenable Nessus .nessus File

This guide provides information for installing the SmartConnector for Tenable Nessus .nessus File and configuring the device for scan report event collection. This SmartConnector supports Nessus Vulnerability Scanner versions 6.5, 6.6, and 6.8.

Product Overview

The Nessus Vulnerability Scanner features high-speed discovery, configuration, auditing, asset profiling, sensitive data discovery, and vulnerability analysis of your overall security. This connector supports importing Nessus reports in .nessus format.

Configuration

This section provides instructions for configuring the Nessus Vulnerability Scanner to send reports to the ArcSight SmartConnector.

Modes of Operation

The SmartConnector for SmartConnector for Tenable Nessus .nessus File supports the following modes of operation:

- **Interactive Mode:**
  In this mode, a graphical user interface shows the reports available for importing. You can choose reports to send to the SmartConnector by selecting individual report listings and clicking the **Send** button.

- **Automatic:**
  This mode is designed to be used in conjunction with an automated procedure to periodically run scans with the Nessus Vulnerability Scanner.

  To use automatic mode, create a script to schedule the time Nessus should run scans. At the end of the scan, after the report is saved, create an empty file called **{reportname}.nessus_done**, which tells the ArcSight SmartConnector that the report is ready for importing. The connector continues to search for .nessus_done files and process the reports. The processed reports are renamed to {original report file} + "nessus_processed".

Generate and Use .nessus Files

Once you have created a policy and list of scan target addresses, you can save the configuration in the **.nessus** file format from the main NessusClient window by selecting **File** and **Save As...** from the main menu.

To access the saved **.nessus** file, go to **File -> Open**. On Windows systems, the saved **.nessus files** are stored in **C:\Documents and Settings\<username>\My Documents\Tenable\NessusClient**. On Linux systems, the saved **.nessus** files are stored under the user's home directory (such as `/root/my_policy.nessus`).

For information about creating and managing policies and running scans, see Tenable Network Security's *NessusClient User Guide*.

Execute Scripts to Import Nessus Reports in Automatic Mode

The configuration of the SmartConnector for Tenable Nessus .nessus File in automatic mode lets you send Nessus reports automatically to ArcSight. To do this, create a shell script that executes the Nessus Vulnerability Scanner periodically and saves a report in .nessus format. Once the report is created, create a "triggering" file (can be any file) to indicate that the report can be sent to ArcSight. The extension for this file must be defined as `.nessus_done` for .nessus-format report files.

The following is a sample script (`samplenessusscript.sh`) to use as a guideline in creating your own script. This sample directs the Nessus Vulnerability Scanner to generate a .nessus-format report and send it to ArcSight ESM Manager (by automatically creating the `.nessus_done` file).

For more information about creating scripts, see the documentation for the Nessus Vulnerabililty Scanner at http://www.nessus.org/documentation/.

```
#!/bin/sh
NESSUS=/opt/nessus/bin/nessus
usage() {
echo "Usage: samplenessusscript.sh host port(usually 1241) user
password targetsfile reportname-minus-extension format"
}
# Generate an xml report with the params passed in the command line
$NESSUS -q $1 $2 $3 $4 $5 $6.$7 -T $7
#Now create an empty .nessus_done file to trigger the SmartConnector
touch $6.$7_done
```

To run a script to create a report, execute a command such as the following:

```
samplenessusscript <server> 1241 <user> <password> <targets.txt>
<reportname-minus-extension> nessus
```

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

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

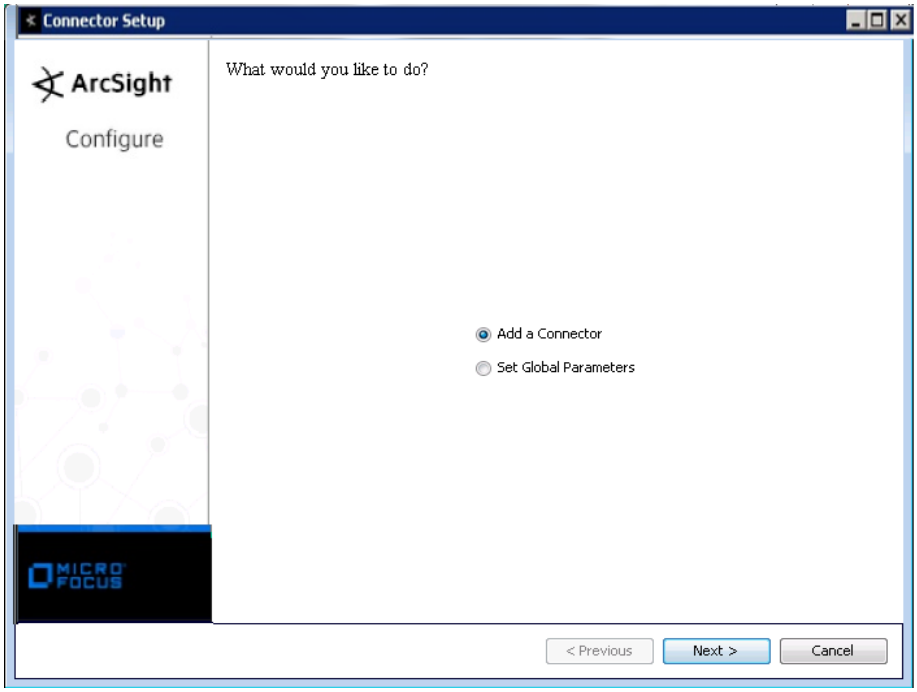
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

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.

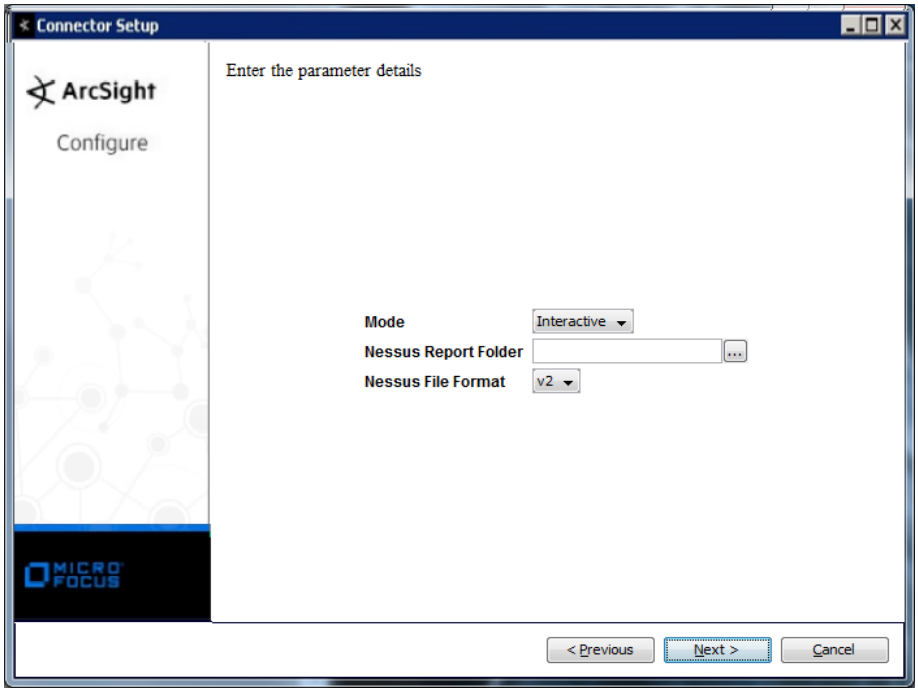
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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.
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 **Tenable Nessus .nessus File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Mode	Interactive Mode or Automatic Mode (see details in "Configuration").
Nessus Report Folder	The folder in which the Nessus reports are located.
Nessus File Format	This represents the Nessus file format version. Currently supported version is v2.

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.

Tenable Nessus .nessus Open Ports Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	EndTime
Additional data	LocalChecksProto
Additional data	netbiosName
Additional data	ReportName
Additional data	smbLoginUsed

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = High or Hole; High = Medium or Warning; Medium = Low or Informational; Low = Open Port
Application Protocol	ServicesName
Category Technique	VulnerabilityCategory(1)
Destination Address	One of (TargetIpAddress, TargetHostName)
Destination Host Name	One of (TargetHostNameFQDN, TargetHostName)
Destination Mac Address	TargetMacAddress
Destination Port	Port
Destination Process Name	ServicesName
Device Custom String 1	cwe (Common Weakness Enumeration)
Device Custom String 2	pluginName (Plugin Name)
Device Custom String 3	Revision
Device Event Category	EventCategory
Device Event Class ID	Both ('Nessus', NessusID)
Device Outbound Interface	One of (TargetHostNameFQDN, TargetHostName)
Device Product	'Nessus'
Device Receipt Time	DetectTime
Device Severity	Risk (0=Open Port, 1=Low or Informational, 2=Medium or Warning, 3=High or Hole)
Device Vendor	'Nessus'
End Time	EndTime
File Name	fname
Message	Description
Name	All of ('Open Port:', ServicesName, Port, Protocol)
Start Time	DetectTime
Transport Protocol	Protocol

Tenable Nessus .nessus Scanner Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of (TargetIpAddress, TargetHostName)
Destination Host Name	One of (TargetHostNameFQDN, TargetHostName)
Destination Mac Address	TargetMacAddress
Device Outbound Interface	One of (TargetHostNameFQDN, TargetHostName)

Tenable Nessus .nessus URIs Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	EndTime
Additional data	localChecksProto
Additional data	netbiosName
Additional data	ReportName
Additional data	smbLoginUsed
Agent (Connector) Severity	Low = Operating System

ArcSight ESM Field	Device-Specific Field
Category Technique	VulnerabilityCategory(4)
Destination Address	One of (TargetIpAddress, TargetHostName)
Destination Host Name	One of (TargetHostNameFQDN, TargetHostName)
Destination Mac Address	TargetMacAddress
Device Event Class ID	Both ('Nessus', NessusID)
Device Outbound Interface	One of (TargetHostNameFQDN, TargetHostName)
Device Product	'Nessus'
Device Severity	Operating System
Device Vendor	'Nessus'
File Path	OS
Name	Both ('Operating System', OS)

Tenable Nessus .nessus Vulnerabilities Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	CVE
Additional data	cvssBaseScore
Additional data	cvssVector
Additional data	Exploitability_ease
Additional data	Exploit_framework_canvas
Additional data	localChecksProto
Additional data	netbiosName
Additional data	PatchPublicationDate
Additional data	PluginModificationDate
Additional data	PluginOutput
Additional data	PluginPublicationDate
Additional data	PluginVersion
Additional data	ReportName
Additional data	RiskFactor
Additional data	smbLoginUsed
Additional data	Solution
Additional data	Synopsis
Additional data	VulnPublicationDate
Agent (Connector) Severity	Very High = 3,4; High = 2, Medium = 1, Low = 0
Application Protocol	ServicesName
Category Technique	VulnerabilityCategory(0)
Destination Address	One of (TargetIpAddress, TargetHostName)
Destination Host Name	One of (TargetHostNameFQDN, TargetHostName)
Destination Mac Address	TargetMacAddress
Destination Port	Port
Destination Process Name	ServicesName
Device Custom Number 1	cert (CERT)
Device Custom String 1	cwe (Common Weakness Enumeration)
Device Custom String 2	CVE

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Revision
Device Custom String 4	XREF
Device Custom String 5	BugtraqID
Device Custom String 6	cvssBaseScore
Device Domain	'Network'
Device Event Category	EventCategory
Device Event Class ID	All of ('Nessus', NessusID, pluginName, Risk, Description, Synopsis, Solution, XREF, URL, CVE)
Device Outbound Interface	One of (TargetHostNameFQDN, TargetHostName)
Device Product	'Nessus'
Device Receipt Time	DetectTime
Device Severity	Risk
Device Vendor	'Nessus'
Device Version	'V2'
End Time	EndTime
File Name	fname
Flex Number 1	DetectTime
Flex Number 2	EndTime
Flex String 1	Description
Flex String 2	Solution
Message	Description
Name	Both ('Vulnerability', Name)
Old File Name	Attachment
Old File Path	_FILE_PATH
Request Client Application	CommonPlatformEnumeration
Request Context	Exploit_available
Request URL	URL
Start Time	DetectTime
Transport Protocol	Protocol