
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Tenable SecurityCenter XML File

Document Release Date: February 2022

Software Release Date: February 2022



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2022 Micro Focus or one of its affiliates

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

Support

Contact Information

| | |
|--------------------------------|---|
| Phone | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| Support Web Site | https://softwaresupport.softwaregrp.com/ |
| ArcSight Product Documentation | https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

Contents

| | |
|--|----|
| Configuration Guide for Tenable SecurityCenter XML File SmartConnector | 6 |
| Product Overview | 7 |
| Configuration | 8 |
| Configure SecurityCenter to Work with Nessus | 8 |
| Modes of Operation | 8 |
| Executing Scripts to Import Nessus Reports in Automatic Mode | 9 |
| Increase Memory Size for XML Reports | 10 |
| Install the SmartConnector | 11 |
| Prepare to Install Connector | 11 |
| Install Core Software | 11 |
| Set Global Parameters (optional) | 12 |
| Select Connector and Add Parameter Information | 14 |
| Select a Destination | 15 |
| Complete Installation and Configuration | 15 |
| Run the SmartConnector | 17 |
| Device Event Mapping to ArcSight Fields | 18 |
| Tenable SecurityCenter XML Open Ports Mappings | 18 |
| Tenable SecurityCenter XML URIs Mappings | 19 |
| Tenable SecurityCenter XML Vulnerabilities Mappings | 20 |
| Tenable SecurityCenter XML Scanner Mappings | 22 |
| Tenable SecurityCenter XML ARF URIs XQuery Mappings | 22 |
| Tenable SecurityCenter XML ARF XQuery Mappings | 23 |
| Tenable SecurityCenter XML ARF Vulnerabilities XQuery Mappings | 24 |
| Tenable SecurityCenter XML ASR XQuery Mappings | 24 |
| Troubleshooting | 26 |

Send Documentation Feedback27

Configuration Guide for Tenable SecurityCenter XML File SmartConnector

This guide provides information for installing the SmartConnector for Tenable SecurityCenter XML File and configuring the device for scan report event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

Product Overview

Tenable's SecurityCenter is a web-based management console that unifies the process of vulnerability detection and management, compliance monitoring, and reporting on all of the above. SecurityCenter enables communication of security events to IT, management, and audit teams.

Using the Nessus API (a custom implementation of the XML-RPC protocol), SecurityCenter communicates with associated Nessus scanners to send scanning instructions and receive results.

Configuration

This section provides instructions for configuring SecurityCenter to work with Nessus. For complete information about configuring Nessus, see Tenable's *Nessus Installation and Configuration Guide*, from which material in this section has been derived.

The SmartConnector for Tenable SecurityCenter XML File supports importing Nessus reports in XML format (not other files) for single or multiple host scans.

Configure SecurityCenter to Work with Nessus

A Nessus Server can be added through the SecurityCenter administration interface. SecurityCenter can be configured to access and control virtually any Nessus scanner.

- 1 Click the **Resources** tab and then click **Nessus Scanners**.
- 2 Click **Add** to open the **Add Scanner** dialog. The Nessus scanner's IP address, Nessus port (default 8834), administrative login ID, authentication type, and password (created while configuring Nessus) are required.

The password fields are not available if **SSL Certificate** authentication is selected. The ability to Verify Hostname is provided to check the CommonName (CN) of the SSL certificate presented by the Nessus server. The state of the Nessus scanner can be set to Enabled or Disabled as needed, with a default of Enabled. Zones to which the Nessus scanner may be assigned can be selected.

For more information, see Tenable's *Security Center Administration Guide*.

Modes of Operation

The SmartConnector for Tenable SecurityCenter XML File supports the following modes of operation:

- **Interactive Mode:**
This mode is valid for connectors installed in stand-alone mode only, not when installed as a service. 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}.xml_done**, which tells the ArcSight SmartConnector that the report is ready for importing. The connector continues to search for .xml_done files and process the reports. The processed reports are renamed to {original report file} + ".xml_processed".

Executing Scripts to Import Nessus Reports in Automatic Mode

The configuration of the SmartConnector for Tenable SecurityCenter XML 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 XML 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 .xml_done for XML-format report files.

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

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

```
#!/bin/sh
XML=xml
XML_DONE=xml_done
NESSUS=/usr/bin/nessus
usage() {
  echo "Usage: samplenessusscript.sh nessusserver port(usually 1241)
nessususer
  nessuspasswd filecontainingtargets reportname xml"
}
# 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 .xml_done file to trigger the SmartConnector
touch <report-filename>.xml_done
```

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

```
./<yourScriptName.sh> <yourServer> 1241 <yourUser> <yourPassword>  
<yourTarget.txt> <YourReport xml>
```

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.

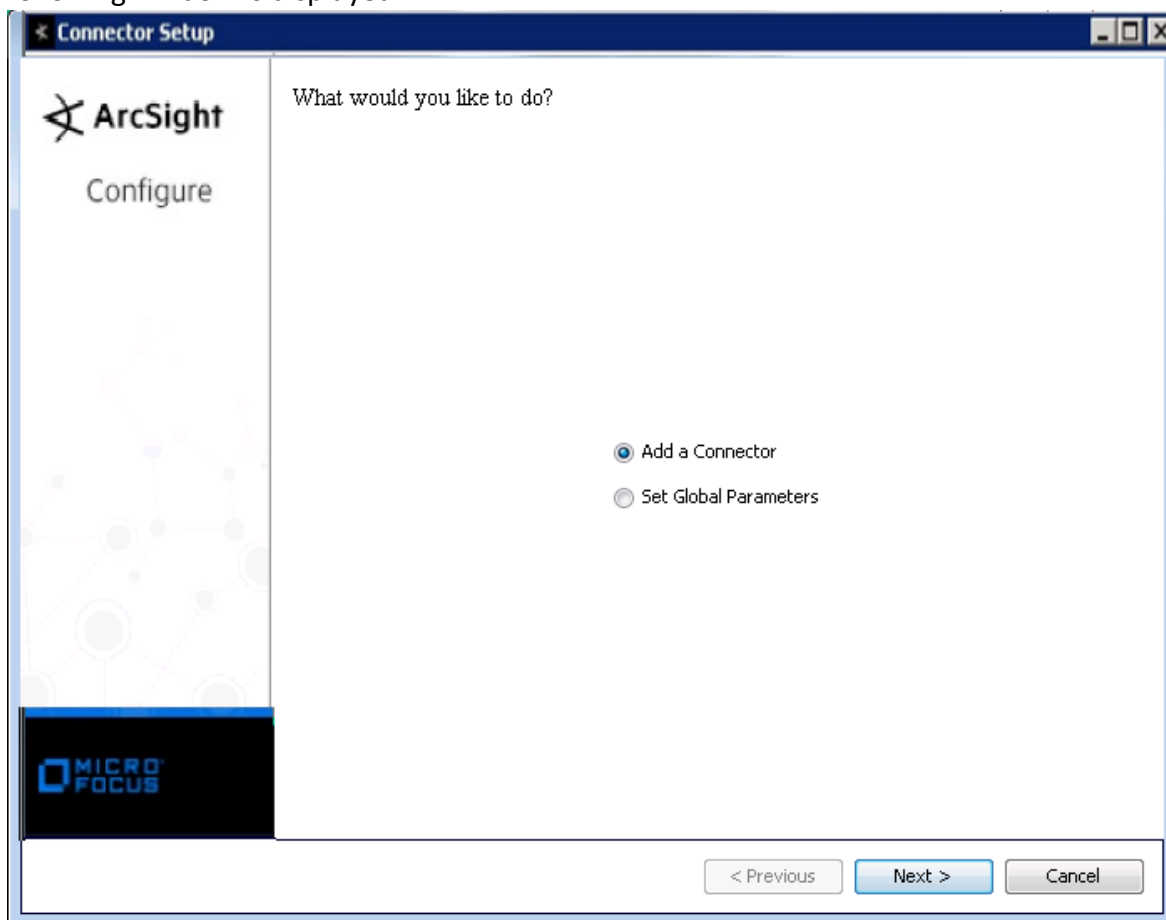
- 1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

- 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 SecurityCenter XML File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

The screenshot shows the 'Connector Setup' window for ArcSight. The window has a title bar with '< Connector Setup' and standard window controls. On the left, there is a sidebar with the ArcSight logo and the word 'Configure'. The main area is titled 'Enter the parameter details'. It contains three fields: 'Mode' with a dropdown menu set to 'Interactive', 'Log Folder' with a text box and a browse button (...), and 'Log Extension' with a dropdown menu showing options: '.xml', '.nessus', and '.xml' (highlighted). At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The Micro Focus logo is visible in the bottom left corner of the window.

| Parameter | Description |
|---------------|--|
| Mode | Interactive Mode or Automatic Mode (see details in "Configuration") |
| Log Folder | The folder in which the Nessus reports are found. |
| Log Extension | The log type file extension (.xml or .nessus). The XML format works for Assessment Summary Results (ASR) and Asset Reporting Format (ARF) logs. Other logs use the .nessus format. |

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 SecurityCenter XML Open Ports 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 | 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' |

| ArcSight ESM Field | Device-Specific Field |
|---------------------|---|
| 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 SecurityCenter XML 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 |
| 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 |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-------------------------------|
| Device Vendor | 'Nessus' |
| File Path | OS |
| Name | Both ('Operating System', OS) |

Tenable SecurityCenter XML 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) |

| ArcSight ESM Field | Device-Specific Field |
|---------------------------|--|
| 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 |
| 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 |

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|------------------------------|
| 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 |

Tenable SecurityCenter XML 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 SecurityCenter XML ARF URIs XQuery Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|-------------------------------|
| Agent (Connector) Severity | low = Low |
| Category Technique | __getVulnerabilityCategory(4) |
| Destination Address | IPV4 |
| Destination FQDN | All of (HostName, REALM) |
| Destination Host Name | HostName |
| Destination Mac Address | mac |
| Device Custom Number 1 | AttributesRecordIdentifier |
| Device Custom String 3 | Resource |

| ArcSight ESM Field | Device-Specific Field |
|--------------------------|---|
| Device Custom String 4 | Assessedname |
| Device Event Class ID | Asset Created |
| Device Inbound Interface | Interface |
| Device Product | 'Nessus' |
| Device Receipt Time | times |
| Device Severity | Low |
| Device Vendor | 'Tenable' |
| File Path | Assessedname |
| Name | All of ("Operating System: (Assessedname, "No OS name available", Assessedname) |

Tenable SecurityCenter XML ARF XQuery Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|-------------------------------|
| Agent (Connector) Severity | low = Low |
| Category Technique | __getVulnerabilityCategory(0) |
| Destination Address | IPV4 |
| Destination FQDN | All of (HostName, REALM) |
| Destination Host Name | HostName |
| Destination Mac Address | mac |
| Device Custom Number 1 | AttributesRecordedIdentifier |
| Device Custom String 3 | Resource |
| Device Custom String 4 | Assessedname |
| Device Event Class ID | Asset report object created |
| Device Inbound Interface | Interface |
| Device Product | 'Nessus' |
| Device Receipt Time | times |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-----------------------------|
| Device Severity | Low |
| Device Vendor | 'Tenable' |
| Name | Asset report object created |

Tenable SecurityCenter XML ARF Vulnerabilities XQuery Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | veryhigh = fail, Fail; medium = Warning; low = success, Success |
| Category Technique | __getVulnerabilityCategory(0) |
| Destination Host Name | record_identifier |
| Device Custom String 2 | all_record_identifiers |
| Device Custom String 4 | ruleID |
| Device Event Class ID | All of (Nessus = ruleID,all of(ruleResult, count, CVE)) |
| Device Product | 'Nessus' |
| Device Severity | ruleResult |
| Device Vendor | 'Tenable' |
| Event Outcome | ruleResult |
| Name | ASR: ruleID |

Tenable SecurityCenter XML ASR XQuery Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | veryhigh = fail, Fail; medium = Warning; low = success, Success |
| Category Technique | __getVulnerabilityCategory(0) |
| Destination Host Name | record_identifier |
| Device Custom String 4 | ruleID |
| Device Event Class ID | All of (Nessus = ruleID,all of(ruleResult,count, CVE)) |
| Device Product | 'Nessus' |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-----------------------|
| Device Severity | ruleResult |
| Device Vendor | 'Tenable' |
| Event Outcome | ruleResult |

Troubleshooting

What if I stop the processing of a vulnerability scan XML file?

When a user kills the SmartConnector in the middle of processing a vulnerability scan XML file, asset population cannot be completed. Restarting the SmartConnector does not resolve this problem. The workaround is to rename the XML file to its original file name and then restart the SmartConnector.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive events.

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 SmartConnector for Tenable SecurityCenter XML File (SmartConnectors 8.3.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!