Upgrading From NetIQ® Security Manager™ 6.5 to Sentinel 7.0

Technical Reference

October 2011

Contents

Security Manager customers upgrading from version 6.5 to the new Sentinel 7.0 release will be able to leverage existing agents and communication infrastructure to provide a smooth transition to the new Sentinel technology platform.

This *Technical Reference* provides information about upgrading from an existing Security Manager 6.5 deployment to a new Sentinel 7.0 installation.

NetIQ Security Manager claims FIPS compliance by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

Overview

NetIQ Security Manager 6.5.4 enables you to easily upgrade your Security Manager installation to Sentinel 7.0 without redeploying large numbers of agents or migrating data to a new Sentinel database.

In addition, Sentinel 7.0 supports direct searches against data in an existing Security Manager log archive. This eliminates the need to migrate data and allows existing data to be groomed using normal grooming procedures while new data is loaded directly into the new Sentinel 7 deployment.

To upgrade from Security Manager 6.5 to Sentinel 7.0, NetIQ recommends that you deploy Sentinel 7.0 alongside an existing Security Manager installation, upgrade to Security Manager 6.5.4, and leverage the integration features described in this document to ease the transition to the new Sentinel 7.0 release.

For detailed information about installing, configuring, and working with Sentinel, see the Sentinel documentation located at www.novell.com/documentation.

Understanding Sentinel 7.0 Architecture

Sentinel 7.0 is similar to the existing version of Security Manager, in that both versions receive event data from various sources, correlate that data, and enable customers to determine whether the collected data indicates a potential threat or risk to their environment. However, the architecture of Sentinel differs from that of Security Manager in several areas.

Sentinel 7.0 gathers events using components called **Connectors**, which receive data from various event sources, known as **Observers** in Sentinel. Observers include operating systems, devices, and third-party products.

Connectors receive and transport event data to components called **Collectors**. Collectors then process the received data and format event messages. Combined, Connectors and Collectors act in a similar way to proxy agents in previous versions of Security Manager.

Sentinel 7.0 includes several Collectors that process different types of data from Security Manager agents.

NetIQ Security Manager Collector
: Processes data received from Security Manager central computers.

NetIQ Change Guardian (Legacy) Collector
: Processes data received from NetIQ Change Guardian for Windows, NetIQ Change Guardian for Active Directory, and NetIQ Change Guardian for Group Policy through the Security Manager communication infrastructure.

NetIQ UNIX Agent Collector
: Processes data received from the NetIQ UNIX Agent.

Note
NetIQ recommends that you configure your UNIX agents to forward data directly to Sentinel, rather than forwarding data through a Security Manager agent. For more information about configuring UNIX data forwarding, see “Configuring UNIX Data Forwarding” on page 6.

IBM iSeries Collector

Processes data received from IBM iSeries environments.

Microsoft Active Directory Identities Collector

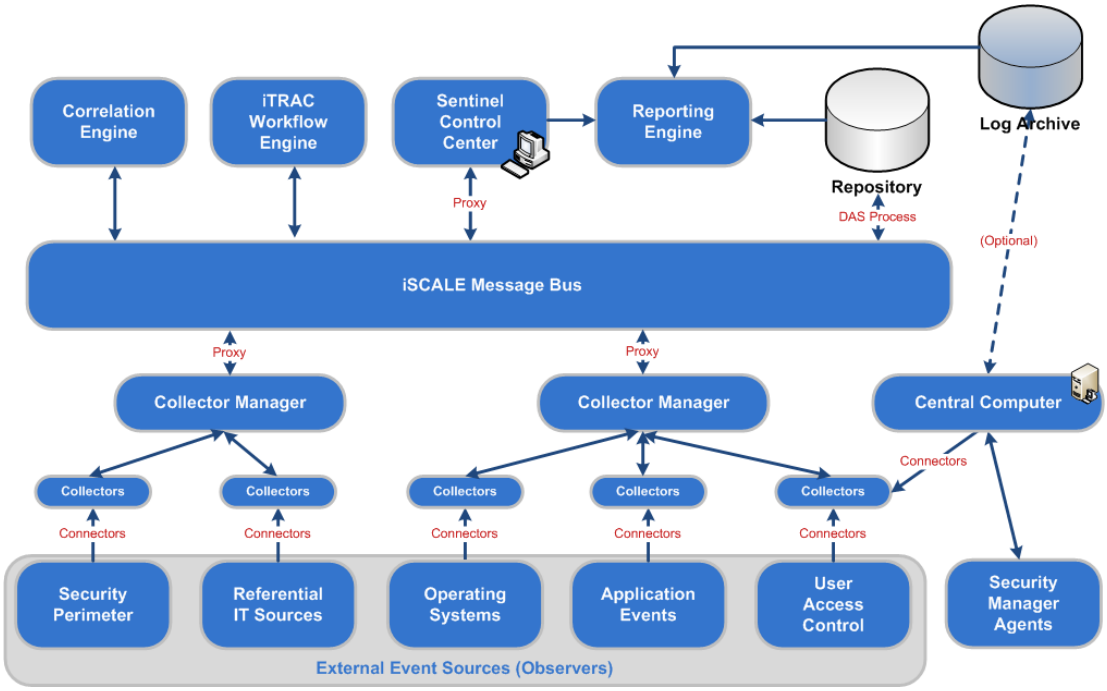
Processes data received from Microsoft Active Directory products installed in Microsoft Windows environments.

For detailed information on a particular Collector, see the appropriate *Collector Guide*.

Each Sentinel environment has multiple Connectors and Collectors, with **Collector Managers** that administer the various Collectors in the environment. Collector Managers transform event data received from data sources into data that can be displayed in a useful way by the **Sentinel Control Center**, which is the primary administrative user interface for Sentinel, and in reports generated by the Sentinel **Reporting Engine**.

All Sentinel components use the iSCALE Message Bus to communicate, sending data and configuration information back and forth among Collector Managers, the Sentinel Control Center, the **Correlation Engine**, and the **iTRAC** incident response system.

The following diagram shows the architecture of Sentinel 7.0 after upgrading from Security Manager 6.5.4.



As displayed above, existing Security Manager customers can integrate existing Security Manager agents in a Sentinel 7.0 installation. Customers can also use Sentinel's reporting capabilities to perform distributed searches across data stored both in the Sentinel repository and in the Security Manager log archive.

For more detailed information about the Sentinel architecture, see the Sentinel documentation located at www.novell.com/documentation. For more information about distributed searching, see "Using Sentinel to Search Log Archive Data" on page 10.

Planning to Upgrade From Security Manager to Sentinel

When upgrading from an existing Security Manager installation to Sentinel, NetIQ recommends you first install and configure Sentinel 7.0 in your environment and transition from your Security Manager 6.5.4 installation. You can either install Sentinel on one or more Linux servers or install a Sentinel virtual appliance in a VMware, Xen, or Hyper-V environment.

Use the following checklist as a guide to the planning, installation, and configuration steps required to upgrade to Sentinel and configure Security Manager to integrate with the new version of the product.

For detailed information on installing and configuring Sentinel, see the *Sentinel 7.0 Installation and Configuration Guide*.

☑	Steps	See Section/Document
☐	**1.** Upgrade your existing Security Manager installation to Security Manager 6.5.4.	*Installation Guide for NetIQ Security Manager*
☐	**2.** Install Sentinel 7.0.	*Sentinel 7.0 Installation and Configuration Guide*
☐	**3.** Configure Sentinel 7.0.	*Sentinel 7.0 Installation and Configuration Guide*
☐	**4.** Configure Security Manager to forward data to Sentinel.	“Enabling Security Manager Data Forwarding” on page 4
☐	**5.** Configure Sentinel to enable log archive searching.	“Enabling Distributed Searching in Sentinel” on page 10
☐	**6.** ***If you want to configure advanced message formatting,*** create custom Match and Filter rules.	“Configuring Custom Message Formatting” on page 17
☐	**7.** ***If you want to configure authenticated communication,*** generate client, server, or log archive server certificates and enable trust.	“Configuring Authenticated Communication” on page 26

Notes

- Both custom message formatting and authenticated communication are optional. NetIQ recommends only advanced users configure message formatting or authenticated communication after upgrading to Sentinel 7.0.
- Before upgrading to Sentinel 7.0, you might want to use the Log Archive Configuration tool to first add a new temporary log archive to your log archive server and mark your existing log archive as read-only. Security Manager will store data in the new log archive and send the same data to Sentinel.

  Once you complete the full transition to Sentinel and no longer want to see duplicate data from Sentinel and your log archive server, you can then detach your temporary log archive and delete the log archive files, since the data is also stored in Sentinel.
- Security Manager does not currently include the capability to migrate existing processing rules into a format usable by Sentinel. After installing Sentinel, you should examine your existing rules in Security Manager to determine which rules you need in Sentinel and recreate that rule functionality in Sentinel.

  To view detailed information about a particular processing rule group in Security Manager, open the Development Console, navigate to the processing rule group, and click **Export Group/Rule Information** in the right pane.

  For information about configuring event collection and processing in Sentinel, see the Sentinel documentation.

Enabling Security Manager Data Forwarding

After deploying Sentinel 7.0 with your existing Security Manager installation, configure Security Manager to forward data received by Security Manager agents to Sentinel. You can then use Sentinel user interfaces, reporting, and search capabilities to view data from endpoints monitored by existing Security Manager agents, as well as data collected by Sentinel itself.

Configuring Data Forwarding

Use the Configuration Wizard in Security Manager to configure your central computers to send data to Sentinel Collector Managers. You can either configure data forwarding globally or for a specific central computer.

Once you configure Security Manager to forward data to Sentinel, you can also decide whether you want to continue to store event and alert data in the log archive and in the OnePoint database or only store data in Sentinel.

For information about configuring data forwarding from UNIX computers, see “Configuring UNIX Data Forwarding” on page 6.

To configure Security Manager data forwarding:

1. Log on to the central computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.

4. On the Tasks menu, click **Global Tasks** > **Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Sentinel Configuration**.
7. Click **Configure Data Forwarding**.
8. ***If you want to configure data forwarding for a particular central computer in your environment,*** select the central computer in the list of computers.
9. ***If you want to configure data forwarding for all central computers in your environment using the same settings,*** select **All central computers forward data to the same Sentinel server**.
10. Select **Forward data to Sentinel**.
11. In the **Sentinel server name** field, specify the name of the Sentinel Collector Manager to which you want the central computer to forward data.

    Note
    You can specify the server name using either the IP address, NetBIOS name, or fully qualified domain name (FQDN) of the computer.

12. In the **Sentinel port number** field, specify the Sentinel syslog connector port where you want the central computer to send data. The default UDP port is `1514`, the default TCP port is `1468`, and the default SSL port is `1443`.

    Note
    Refer to your Sentinel server configuration in the Sentinel Web interface to determine which port to specify.

13. In the **Connection type** field, select the type of connection you want the central computer to use to send data to Sentinel.
14. ***If you no longer want the central computer to store events and alerts in the log archive,*** clear **Store events and alerts on the log archive server**.

    Notes
    - If you clear **Store events and alerts on the log archive server**, you cannot view new events or alerts using Forensic Analysis queries, Summary reports, the Log Archive Resource Kit, or any other interfaces that query the log archive. NetIQ recommends only knowledgeable users modify this setting.
    - You cannot clear the check box above without first selecting **Forward data to Sentinel**. Security Manager 6.5.4 requires that you continue to store data either in the log archive or in the Sentinel repository.
    - If your central computer does not have an associated log archive server, the **Store events and alerts on the log archive server** check box is not selected by default.

      If you want to store data on a log archive server, first use the Configuration Wizard Log Archive Configuration window to specify the log archive server you want to use, then select **Store events and alerts on the log archive server**.

15. ***If you no longer want Security Manager to store event and performance data on the database server,*** clear **Store events and performance data in the OnePoint database**.

Notes

- If you clear **Store events and performance data in the OnePoint database**, you cannot view new events or performance data using the Security Manager Control Center. NetIQ recommends only knowledgeable users modify this setting.
- If you clear this setting, the central computer grooms event and performance data out of the OnePoint database as specified in your Database Server Grooming settings in the Development Console.
- You cannot clear the check box above without first selecting **Forward data to Sentinel**. Security Manager requires that you continue to store event data either in Security Manager or in Sentinel.

16. ***If you want to enable rapid grooming of alerts in the OnePoint database,*** select **Enable daily grooming of alerts (setting applies to all central computers)**.

Notes

- Security Manager always stores alerts in the OnePoint database, in order to enable suppression of duplicate alerts. However, if you select **Enable daily grooming of alerts (setting applies to all central computers)**, Security Manager retains alerts in the database for a maximum of 24 hours. If you enable this setting, Security Manager grooms *all* alerts older than 24 hours out of the OnePoint database, using a grooming job that runs every hour.
- This setting overrides any grooming settings configured in the Database Server Grooming settings in the Development Console.
- This setting applies to *all* central computers in your environment, whether or not you select the **All central computers forward data to the same Sentinel server** option.

17. Click **Next** or **Finish**.

Configuring UNIX Data Forwarding

The NetIQ UNIX Agent sends two streams of data to the Security Manager central computer. The central computer processes one stream and stores the data in the log archive, while the other `syslog_message` stream duplicates some data from the first stream and includes a large amount of data useful only to a limited number of users. The UNIX agent creates the `syslog_message` stream based on the `syslog.conf` file in your UNIX environment.

If you configure your central computer to forward data received from UNIX agents to Sentinel, NetIQ recommends you disable the `syslog_message` stream from the UNIX agent to the central computer and then configure Sentinel to monitor your UNIX syslog data directly using the appropriate Sentinel UNIX collector for your environment.

For more information about configuring the computer to send data to Sentinel, see the *Collector Guide* specific to your UNIX computer.

To configure Sentinel to monitor data from a UNIX agent computer:

1. Log on to the UNIX agent computer using an administrator account.
2. Navigate to the `/etc` folder.
3. Open `vsaunix.cfg` using a text editor.
4. Add the following line to the file:

   ```
   ARCHIVE_SYSLOG=false
   ```
5. Save and close `vsaunix.cfg`.
6. Configure the UNIX computer to send syslog data directly to the Sentinel Collector Manager.
7. Log off of the UNIX agent computer.
8. Log on to the Sentinel server computer using an administrator account that also has access to the Security Manager central computer.
9. Download the latest versions of the Sentinel collector and connector for the type of UNIX syslog data you want to send to Sentinel.
10. Start a Web browser on a computer with access to the Sentinel Web interface.
11. Log in to the Sentinel Web interface using an administrator account.
12. In the top bar, click **collection**.
13. Click the Advanced tab.
14. Launch the **Sentinel Control Center**.
15. In the toolbar, click **Event Source Management** > **Live View**.
16. In the Scripts panel, click the Collectors tab.
17. Click the “Add” icon.
18. Follow the steps in the Import Plug-in Wizard to import the Sentinel collector and connector(s) you downloaded.
19. Configure the collector to receive data from the UNIX computer.
20. Close the Event Source Management Live View.
21. Close the Sentinel Control Center.

For more information about configuring your UNIX computer to send data to Sentinel, see the *Collector Guide* specific to your computer.

Verifying Data Forwarding

After you configure Security Manager to forward data to Sentinel, you can check your configuration using the **Test Connection** button in the Configuration Wizard. Security Manager then checks that the selected central computer can communicate with the specified Sentinel Collector Manager computer using the specified settings, including client or server authentication, if configured.

For more information about configuring authenticated communication with Sentinel, see “Configuring Authenticated Communication” on page 26.

To verify your data forwarding configuration:

1. Log on to the central computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Sentinel Configuration**.
7. Click **Configure Data Forwarding**.
8. ***If you want to verify communication between one central computer and the specified Sentinel server,*** select the central computer and click **Test Connection**.
9. ***If you want to verify communication between all central computers and the same specified Sentinel server,*** select **All central computers forward data to the same Sentinel server** and click **Test Connection**.

   Note
   If you select **All central computers forward data to the same Sentinel server** and click **Test Connection**, Security Manager attempts to verify communication between the specified Sentinel server and either the local central computer or the central computer the Control Center computer uses.
10. Start a Web browser on a computer with access to the Sentinel Web interface.
11. Log in to the Sentinel Web interface using an administrator account.
12. In the **Search** field, type the following query:

    ```
    (sev:[0 TO 5]) AND (evt:"Syslog connection verification
    event")
    ```
13. Click **Search**.

If you configured data forwarding correctly, Sentinel returns a `Syslog connection verification event` confirming that the central computer successfully sent a test message to the Sentinel server through syslog. The event description includes the name of the central computer and the type of connection, whether TCP, UDP, or SSL.

If Sentinel does not return a `Syslog connection verification event`, ensure you have configured your data forwarding settings correctly.

Disassociating the Log Archive Server

After you configure the central computer to forward data to Sentinel and disable log archival storage, you might no longer want to retain the log archive server. If you want to use the central computer strictly for receiving and forwarding data to the Collector Manager, you can use the Configuration Wizard to disassociate the existing log archive server from the central computer.

Notes

- Before you disassociate the log archive server from a central computer, you *must* use the Configuration Wizard to enable data forwarding to the Sentinel server. When you disassociate the log archive server, you can no longer use the Control Center to query any remaining data stored in the log archive. NetIQ recommends only knowledgeable users modify this setting.
- If you disassociate the log archive server, you can still add the log archive server as a search target in Sentinel. For more information about adding search targets, see “Searching Log Archive Data in Sentinel” on page 11.
- After disassociating the log archive server, you cannot re-select the **Store events on the log archive server** check box in the Sentinel Configuration window of the Configuration Wizard.

To disassociate a log archive server from a central computer:

1. Log on to a Control Center computer using an account that is a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Log Archive Configuration**.
7. Select the central computer connected to the log archive server you want to disassociate.
8. Click **Disassociate**.
9. Click **Yes** to confirm.
10. Click **Finish**.
11. Click **OK**.
12. Click **Close**.
13. Open the Services Administrative Tool located in the Control Panel.
14. In the Services pane, click **NetIQ Security Manager Core**.
15. On the Action menu, click **Restart**.
16. Close the Services Administrative Tool.

Using Sentinel to Search Log Archive Data

After you upgrade from Security Manager 6.5.4 to Sentinel 7.0, you can query data collected by both versions of the product using the Distributed Search feature in Sentinel. For example, you can use Sentinel to not only search recent data received by Sentinel but also historical data stored in the Security Manager 6.5.4 log archive.

Understanding Event Searching in Sentinel

Sentinel uses the **Apache Lucene** text search engine to search event data stored either in Sentinel itself or in a separate **search target**, including the Security Manager log archive.

You can search for events in Sentinel by typing a query in the **Search** field in the Sentinel Web interface, using a specific search query syntax.

The basic query structure is as follows:

```
msg:value
```

Where *msg* is the name of the field on which you want to search and *value* is the value against which you want to evaluate data.

For example, if you want to search for any events with a severity level of 4 in Sentinel, type the following query into the Search field and click **Search**:

```
sev:4
```

The Lucene syntax is extremely flexible, allowing you to use wildcards in values, search for values within a specific range, and combine search terms using `AND`, `OR`, and `NOT` operators.

For more information about searching for events using Sentinel, see the *User Guide for Sentinel*. For more information about Lucene search syntax in general, see the Apache Lucene website at lucene.apache.org.

Enabling Distributed Searching in Sentinel

Before you can use Sentinel to search historical data stored in the log archive, you must first enable distributed searching in Sentinel and add the log archive server as a search target to allow Sentinel to search data in the log archive.

For more information about distributed searching, see the *Administration Guide for Sentinel*.

To enable Sentinel to search the log archive server:

1. ***If your log archive server is behind a firewall,*** complete the following steps:
   a. Log on to the log archive server using an account that is a member of the local Administrators group.
   b. Use the **Windows Firewall** tool to open a port on which the log archive server can listen for requests from Sentinel. The default port number is `8443`.
   c. Log off of the log archive server.
2. Start a Web browser on a computer with access to the Sentinel Web interface.

3. Log in to the Sentinel Web interface using an administrator account that is also a member of the OnePointOp ConfgAdms group in your Security Manager configuration group.
4. In the toolbar, click **Search Setup**.
5. ***If distributed searching is not already enabled,*** in the Search Setup tab, select **This local server and other search targets**.
6. Under **Search Targets**, click **Create**.
7. Specify the name or IP address of the log archive server you want to allow Sentinel to search.
8. ***If you want the log archive server to listen for Sentinel requests on a port other than the default port,*** specify the port number you want Sentinel to use to send requests. The default port number is `8443`.

   Note
   The port you specify must be the same as the port you opened on the log archive server.

9. Specify the user name and password you want Sentinel to use to access the log archive server, including the domain to which the server belongs.

   Notes
   - You must specify a user account that is a member of the local Administrators group on the log archive server.
   - You must also specify an account that is a member of the OnePointOp ConfgAdms group in your Security Manager configuration group.

10. Click **Login**.
11. Click **Accept** to accept the default Security Manager certificate.
12. Click **default**.
13. Click **OK**.

Searching Log Archive Data in Sentinel

You can search for log archive data using the Sentinel Web interface the same way you would any other type of data in Sentinel. For detailed information on searching for events using Sentinel, see the *User Guide for Sentinel*.

Mapping Security Manager Platforms to Sentinel Product Names

The current version of Security Manager uses Forensic Analysis report types to specify the particular platform you want to search, filtering log data using the corresponding `analyzer.model` field for each event. Sentinel 7.0 uses a similar field, `pn`, to filter data by product name.

To use Sentinel to search for log archive data related to a specific platform or product, you must specify the product name that corresponds to the platform in Security Manager. Use the following table to map the current `analyzer.model` field to the `pn` field in Sentinel 7.0.

Security Manager Analyzer Model (Platform)	Sentinel Product Name
Windows	Microsoft Active Directory and Windows
TippingPoint	TippingPoint Security Management System
Tripwire Enterprise	Tripwire Enterprise
Trend Micro ScanMail	Trend Micro ScanMail
Trend Micro OfficeScan	Trend Micro OfficeScan
VMware ESXi	VMware ESXi
Type80	Type80
Third Brigade Deep Security Manager	Third Brigade Deep Security Manager
Symantec Endpoint Protection	Symantec Endpoint Protection
Snort IDS	Sourcefire Snort
Oracle On UNIX	Oracle
UNIX	Security Manager for Unix
NetScreen Firewall	Juniper NetScreen Firewall
NetApp Filer	NetApp Filer
Microsoft Exchange Services	Microsoft Exchange
Microsoft Exchange	Microsoft Exchange
Microsoft Exchange Auditing	Microsoft Exchange
McAfee VirusScan Enterprise	McAfee VirusScan Enterprise
Mantra	Netezza Mantra
ISS SiteProtector	IBM ISS SiteProtector
iSeries	iSeries
Imperva SecureSphere	Imperva SecureSphere
IIS	Microsoft Internet Information Services
Cisco IPS	Cisco Intrusion Prevention System
Cisco IOS	Cisco IOS
Cisco Firewall	Cisco Firewall
Cisco Secure ACS	Cisco Secure Access Control Server
Blue Coat ProxySG	Blue Coat ProxySG
Bit9 Parity	Bit9 Parity
Generic Syslog	Generic Syslog

Security Manager Analyzer Model (Platform)	Sentinel Product Name
SM Audit Log	NetIQ Security Manager
Security Manager	NetIQ Security Manager
Security Manager Alert	NetIQ Security Manager
Aegis	NetIQ Aegis
NetIQ Vulnerability Manager	NetIQ Secure Configuration Manager
NetIQ Directory and Resource Administrator	NetIQ Directory and Resource Administrator
Change Guardian	Change Guardian for Windows
Tripwire	Tripwire for Servers
Sidewinder Firewall	McAfee Enterprise Firewall
Cisco IDS	Cisco Intrusion Detection System
Check Point Firewall	Check Point Firewall
Change Guardian for Active Directory	Change Guardian for Active Directory
Group Policy	Change Guardian for Group Policy

Note
If you want a full list of all event fields currently collected by Security Manager, see the `FieldMap.xml` file on the log archive server, located in the following folder by default:

`installation folder``\NetIQ Security Manager\NetIQ Log Archive`

Searching for Change Guardian Data with Sentinel

If you use one or more Change Guardian products with Security Manager and upgrade to Sentinel 7.0, you can use Sentinel to search Change Guardian data stored on a log archive server as you would any other log archive data.

However, Change Guardian users typically need to find very specific change-related information. You can use the following table to determine which Sentinel fields to search for change-related events:

Change Information	Sentinel Field
When	`EventTime`
Who	`InitiatorUserName`
Authorized (Managed or Unmanaged)	`CustomerVar21` (`cv21`)
Where (Host)	`TargetHostName`, `TargetIP`
What > Affected object	`TargetDataName`
What > Action performed	`EventName`, `CustomerVar22` (`cv22`)
What > Original value	`TargetAttributeOriginalValue`

Change Information	Sentinel Field
What > New modified value	TargetAttributeValue
What > Affected object type	CustomerVar23 (cv23)
What > Status	VendorOutcomeCode (0 indicates success, and any failure returns an error code)
What > Affected object information (Change Guardian for Group Policy only)	CustomerVar24 (cv24)
What > Affected section (Change Guardian for Group Policy only)	CustomerVar25 (cv25)
What > Action details (Change Guardian for Group Policy only)	CustomerVar26 (cv26)
Profile type (Low or High; Change Guardian for Active Directory only)	CustomerVar27 (cv27)

In addition, because of the structure of Change Guardian data stored in Security Manager, Change Guardian events forwarded to Sentinel look different from events returned in a Sentinel search on a log archive.

When the central computer forwards a Change Guardian event to Sentinel, some fields are included in the Extended Information (ei) field in Sentinel, while Change Guardian events returned in a Sentinel search retain those separate fields as CustomerVar fields.

For a full list of Change Guardian fields that differ between events stored in the Sentinel datastore and events stored in the log archive, see the following table:

Security Manager Field	Sentinel Field	Distributed Search Results Field
target.object.name (2044) [Parent path]	TargetDataContainer	Not mapped
target.object.name (2044) [Group object] (Change Guardian for Active Directory only)	TargetTrustName	Not mapped
Status (847)	Part of Event Name and VendorOutcomeCode	VendorOutcomeCode
target.object.managed (2061)	Part of Event Name	CustomerVar21
target.object.type (2045)	Part of Extended Information	CustomerVar23
Action (793)	Part of Event Name	CustomerVar22

Security Manager Field	Sentinel Field	Distributed Search Results Field
`userfield_string_001` (2051) to `userfield_string_010` (2060)	Part of `Extended Information` under a named property	Part of `Extended Information` under a property named `CustomField1` to `CustomField10`
classification.name (560) (Change Guardian for Active Directory only)	Used to drive event name in a scripting logic	Event name is always `Change Guardian for Active Directory Event`
userfield_string_001 (2051) (Change Guardian for Active Directory only)	Part of `Event Name`	`CustomerVar27`

Understanding Limitations of Searching Log Archive Data with Sentinel

Sentinel 7.0 handles both events and queries differently from previous versions of Security Manager. Because of those differences, if you search log archive data using Sentinel queries, you may encounter some limitations in terms of what data can be returned.

The following list describes some of the more critical limitations.

Searches for log archive data may require more time in Sentinel

Because the log archive uses a different framework, Sentinel does not search log archive data as quickly as the existing Forensic Analysis query functionality in Security Manager. To optimize searching on log archive data, limit the time range on which you want to search.

In addition, the Sentinel Web interface does not display the results of a log archive search until Sentinel finishes searching all data in the log archive.

You cannot search log archive data with Sentinel using certain words

You cannot use the words “to,” “not,” or “contains” as search parameters when searching log archive data with Sentinel. These words are keywords used by the log archive search function.

If you want to include “to,” “not,” or “contains” as search parameters, you can use proximity indicators in your Lucene query. For example, if you want to search for the text “Service not started,” you can enter the following query in Sentinel:

```
msg:"Service started"~1
```

Sentinel then searches for events where the message field contains the two words “service” and “started” separated by any one word.

For more information about search query syntax in Sentinel, see the *User Guide for Sentinel*.

Sentinel stores some event data in the Extended Information field

Sentinel does not map all data received from the central computer directly to the Sentinel event message structure. Any data forwarded from the central computer to Sentinel that is not mapped to a Sentinel field is stored instead in the `Extended Information` (`ei`) field in Sentinel.

The log archive server stores user information differently from the way Sentinel stores user information

The existing log archive server stores user information in a single field that includes both the domain and user name in the format *`domain\username`*. However, Sentinel stores both the domain and user name as two separate fields, one for the domain and the other for the user. The log archive and Sentinel use these conventions for several sets of fields within the product.

For example, Sentinel stores a logon event (528) in the following way:

```
TargetUserDomain: USDOM01
TargetUserName: bob
```

Security Manager stores the event as follows:

```
TargetUserName: USDOM01\bob
```

Log archive data does not contain taxonomy information

If you search data in the log archive from Sentinel, the returned data does not contain Sentinel taxonomy information. The Sentinel taxonomy is applied only to events collected by or forwarded to Sentinel, and events stored in the log archive have not been processed by Sentinel. However, any data forwarded from the central computer *to* Sentinel does contain taxonomy information.

Sentinel cannot search log archive data using an IP address range or subnet search

Because the log archive stores IP addresses as strings, when you use Sentinel to search data stored in the log archive for a range of IP addresses or within a specific subnet, the log archive returns data incorrectly.

Troubleshooting Sentinel Upgrade Issues

The following section includes information on addressing or mitigating potential issues involved in upgrading from Security Manager 6.5.4 to Sentinel 7.0 or in forwarding Security Manager agent data to Sentinel.

Connectivity Issues Between Central Computers and Sentinel

If you configure a central computer to forward data using either the TCP or SSL connection type, but the central computer cannot communicate with the Sentinel server, whether due to a network outage or some other issue, the central computer automatically stops forwarding data to Sentinel.

In addition, as long as the central computer cannot communicate with Sentinel, the log archive server stops storing data in the log archive.

In the event of a communication disruption, the central computer attempts to continue sending data to the Sentinel server every 30 seconds for 300 seconds, after which Security Manager attempts to send data every five minutes until the connection can be re-established.

Note
Due to the nature of the UDP connection type, the central computer cannot detect whether or not the Sentinel server receives forwarded data. A central computer configured to forward data using a UDP connection continues to forward data without regard to connectivity.

Log Archive Service Restarted During Searching

If you or another user restarts the `NetIQ Security Manager Log Archive` service on a log archive server while Sentinel is attempting to search data stored in the log archive server, the log archive does not resume processing the search request upon restarting.

Once the log archive service restarts, you must re-run the search in Sentinel to find data from the log archive.

Configuring Custom Message Formatting

When configured to forward data to Sentinel, the central computer uses a predefined set of formatting rules to collect standard, commonly-received types of log data from the log archive and format messages sent to Sentinel. These predefined rules serve as a default parse map for all forwarded data and handle most types of data.

However, you can also choose to specify custom formatting rules for data sent from your central computer. Using the Configuration Wizard, you can create your own XML-based rules to filter or forward specific data sent to Sentinel and format forwarded messages in a way that best fits your environment.

You can create custom rules that either filter out data you do not want sent to Sentinel or capture data you want to forward to Sentinel. The Configuration Wizard then concatenates your custom message formatting rules with the predefined set of message formatting rules.

Notes
- If you configure custom message formatting rules for data forwarded to Sentinel incorrectly, you could cause data to be badly formatted when stored in Sentinel. NetIQ recommends that only users with experience configuring Sentinel 7.0 event collection and writing XML configure custom formatting rules.
- The central computer evaluates custom message formatting rules before evaluating predefined message formatting rules. If a message matches a custom rule, the central computer filters or forwards the message and ignores the predefined rules.

Understanding Message Formatting Rule Structure

The basic structure of each formatting rule, predefined or custom, is as follows:

```
<Filter name="RULENAME1" enabled="[true/false]">
   <FieldList>
      <Field id="FIELDIDNUMBER1" dataType="DATATYPE1"
      value="FIELDVALUE1"/>
```

```
   </FieldList>
</Filter>

<Match name="RULENAME2" enabled="[true/false]">
   <FieldList>
      <Field id="FIELDIDNUMBER2" dataType="DATATYPE2"
      value="FIELDVALUE2"/>
   </FieldList>
   <Format><![CDATA[ [FIELDIDNUMBER2] [FIELDIDNUMBER3]
   PLATFORMID: [json-include:{FIELDIDNUMBERS}/json-
   exclude:{FIELDIDNUMBERS}/json:{*}] ]]></Format>
</Match>
```

You can create one or more custom **filter** or **match formatting rules**, specified in XML by `Filter` and `Match` elements.

The following sections define each of the XML elements used in implementing message formatting rules.

Notes

- If you do not specify one or more `Filter` or `Match` formatting rules and elements, the central computer ignores the custom message formatting and uses the predefined set of formatting rules.
- The central computer evaluates data against custom message formatting rules in the order specified in the Configuration Wizard.
- The `<![CDATA[ ]]>` section within the `Format` element above is not required when creating formatting rules. However, NetIQ includes the `CDATA` section by default to allow users to include characters in the `Format` element that could conflict with the XML document as a whole.

  If you do not require the `CDATA` section for your formatting rules, you can remove the section and include only the event fields and JavaScript Object Notation (JSON) tags within the `Format` element.

Filter Rule

When configuring message formatting, you can create one or more filter rules, each defined by a corresponding `Filter` element.

The central computer evaluates each message sent to Sentinel against each filter rule, matching the attributes specified for a particular `Filter` rule against the forwarded data. If a message matches the criteria of the filter rule, the central computer does not forward the message.

Each `Filter` rule contains a `name` attribute that allows you to label a particular rule and an `enabled` attribute that allows you to specify whether a rule is enabled or disabled, as necessary, without removing the rule completely.

Each `Filter` rule also contains a single `FieldList` child element, which then contains one or more `Field` child elements. The central computer uses the attributes of all `Field` child elements within the `Filter` rule to filter out data.

The following XML is an example of a `Filter` rule:

```
<Filter name="FilterRule1" enabled="true">
```

```
   <FieldList>
      <Field id="535" dataType="string" value="test"/>
   </FieldList>
</Filter>
```

In this `Filter` rule, the central computer checks event field `535`, `Target Process ID`, against each forwarded message. If the value of the `Target Process ID` field of any message matches `test`, the central computer does not forward the message to Sentinel.

The following table defines the child elements of the `Filter` rule:

Rule/Element	Child Element	Attribute	Description
`Filter`		`name`	Required attribute that allows you to label the rule. The Configuration Wizard displays the rule name in the Configure Message Formatting tab.
		`enabled`	Required attribute that specifies whether a rule is enabled or disabled. Possible options are `true` or `false`.
	`FieldList`		Required child element that contains one or more `Field` elements. You can include only one `FieldList` child element in a `Filter` rule.

Rule/Element	Child Element	Attribute	Description
FieldList	Field		Optional child element the central computer uses as a criterion for filtering out forwarded data. You can include multiple Field child elements in a FieldList element.
		id	Required numeric attribute that identifies the event ID you want the central computer to match against the specified value attribute.
		dataType	Required string attribute that indicates the type of data being matched. Possible options are datetime, int, uint, short, ushort, string, guid, long, ulong, byte, float, and double.
		value	Required attribute that indicates the value of the specified event ID that you want the central computer to match.

Match Rule

When configuring message formatting, you can create one or more match rules, each defined by a corresponding Match element.

The central computer evaluates each message sent to Sentinel against each match rule, matching the attributes specified for a particular match rule against the forwarded data. If a message matches the criteria of the Match rule, Security Manager formats the data per the Format child element and forwards the message to Sentinel.

Each Match rule contains a name attribute that allows you to label a particular rule and an enabled attribute that allows you to specify whether a rule is enabled or disabled, as necessary, without removing the rule completely.

Each Match rule also contains a single FieldList child element, which then contains one or more Field child elements, and a single Format child element. Security Manager uses the attributes of all Field child elements within the Match rule to find matching data.

The Format child element allows you to specify how you want the message data to look when sent to Sentinel. You can include specific event fields, like the time the agent detected the event or the platform of the computer from which the event originated, either by including each event field as a header field or by using the json-include tag.

You can also use the json-exclude tag to exclude specific fields, if you do not need all data from a particular type of event or want to reduce the size of the message sent to Sentinel.

In addition, you can configure the central computer to include all event fields, if necessary, using the `json:{*}` tag within the `Format` element.

The options within a `Format` element are as follows:

Header fields

A header event field is any field not within a `json-include` or `json-exclude` tag. The central computer includes *all* header fields, even if one or more header fields are also within a `json-exclude` tag. Some Sentinel collectors expect specific header fields to be included at the beginning of any event of a particular type.

Platform identifier

Sentinel requires an identifier for non-header data within a `Format` element. This identifier typically tells Sentinel and the user what type of platform the data comes from. For example, the `Format` element could include the identifier `NQ-UNIX:` to indicate the event data originated in a UNIX environment.

json-include

The `json-include` tag tells the central computer to include only the specified event fields in every event message matching the attributes of the parent `Match` rule. For example, the Format element could include the tag `json-include:{401,501}` to include the `Event Ident` and `Platform` fields in all messages matching the `Match` rule attributes.

json-exclude

The `json-exclude` tag tells the central computer to include all event fields except for the specified fields in every event message matching the attributes of the parent `Match` rule. For example, the Format element could include the tag `json-exclude:{564,565}` to exclude the `Message` and `NetIQ Event Classification` fields from all messages matching the `Match` rule attributes.

json:{*}

The `json:{*}` tag tells the central computer to include all event fields in every event message matching the attributes of the parent `Match` rule.

Notes

- You can only include one JSON tag of any type in a `Format` element.
- The central computer can include or exclude an event field only if that field exists within the event received from the agent.

The following XML is an example of a `Match` rule for a Microsoft Windows event:

```
<Match name="MatchRule1" enabled="true">
   <FieldList>
      <Field id="501" dataType="string" value="Windows"/>
   </FieldList>
   <Format><![CDATA[ [503] [502] MSWinEventLog 2 [561] 11111
   [503] [560] [561] Unknown User N/A [579] [645] 12345 [564]
   11111 ]]></Format>
</Match>
```

In this `Match` rule, the central computer checks event field `501`, `Platform`, against each forwarded message. If the value of the `Platform` field of any message matches `Windows`, the central computer formats the message as follows:

```
[Event Detection Time] [Network Node Address] MSWinEventLog
2 [Log Source Name] 11111 [Event Detection Time] [Native
Classification] [Log Source Name] Unknown User N/A [Event
Type] [Network Node] 12345 [Message] 11111
```

The following message is an example of a real Microsoft Windows event formatted by the `Match` rule:

```
Sep 23 18:05:13 10.12.129.190 MSWinEventLog   2   Security
11111   Sep 23 18:05:13   540   Security   Unknown User   N/
A   Success Audit   HOUTESTSRV001   12345      Successful
Network Logon:    User Name: bob    Domain:  DOM001    Logon
ID:  (0x0,0x427DCE3)    Logon Type: 3    Logon Process:
NtLmSsp    Authentication Package: NTLM    Workstation Name:
HOUTESTSRV002    Logon GUID: -    Caller User Name: -
Caller Domain: -    Caller Logon ID: -    Caller Process ID:
-    Transited Services: -    Source Network Address: -
Source Port: -      11111
```

The Sentinel Windows collector expects all Windows events to follow a particular format, as shown above, and includes only certain event fields. The central computer then forwards the matched, formatted message to Sentinel.

The following XML is an example of a `Match` rule for a UNIX event:

```
<Match name="MatchRule2" enabled="true">
   <FieldList>
      <Field id="501" dataType="string" value="Unix"/>
   </FieldList>
   <Format><![CDATA[ [503] [502] NQ-UNIX: json:{*} ]]></Format>
</Match>
```

In this `Match` rule, the central computer again checks event field `501`, `Platform`, against each forwarded message. If the value of the `Platform` field of any message matches `Unix`, the central computer formats the message as follows:

```
[Event Detection Time] [Network Node Address] NQ-UNIX: [All
Event Fields]
```

The Sentinel UNIX collector does not expect all UNIX events to follow as complex a format as a Windows event but instead looks for the two header event fields above, `503`, `Event Detection Time`, and `502`, `Network Node Address`.

After those two header fields, the `json:{*}` tag tells the central computer to include *all* event fields in the message sent to Sentinel. The `NQ-UNIX:` identifier tells Sentinel the incoming message is UNIX data.

The following table defines the child elements of the `Match` rule:

Rule/Element	Child Element	Attribute	Description
`Match`		`name`	Required attribute that allows you to label the rule. The Configuration Wizard displays the rule name in the Configure Message Formatting tab.
		`enabled`	Required attribute that specifies whether a rule is enabled or disabled. Possible options are `true` or `false`.
	`FieldList`		Required child element that contains one or more `Field` elements. You can include only one `FieldList` child element in a `Match` rule.
	`Format`		Required child element that contains formatting information for the central computer to use when a forwarded message matches the `Field` criteria. You can include only one `Format` child element in a `Match` rule.
`FieldList`	`Field`		Optional child element the central computer uses as a criterion for matching and formatting forwarded data. You can include multiple `Field` child elements in a `FieldList` element.
		`id`	Required numeric attribute that identifies the event field you want the central computer to match against the specified `value` attribute.
		`dataType`	Required string attribute that indicates the type of data being matched.
		`value`	Required attribute that indicates the value of the specified event field against which you want the central computer to match.

Creating Custom Message Formatting Rules

Use the Configuration Wizard to create custom message formatting rules, including either **filter** or **match** rules.

To create a custom message formatting rule:

1. Log on to the central computer as a member of the OnePointOp ConfgAdms group.
2. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
3. In the Navigation pane, click **All Folders**.
4. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
5. Click **Global Settings**.
6. Click **Sentinel Configuration**.
7. Click **Configure Message Formatting**.
8. Click **Edit Custom Formatting Rules**.
9. In the Edit Custom Formatting Rules window, place your cursor where you want to add the new rule.
10. ***If you want to create a filter rule,*** complete the following steps:
    a. Click **Add Filter Rule**.
    b. Replace `set-rule-name` with the name you want to use for the new filter rule.
    c. Use the cursor to select `set-field-id`.
    d. Press **Ctrl+Space**.
    e. Select the event field you want the central computer to use to filter out forwarded messages.
    f. Replace `string` with the type of data received.

    Note
    Possible options are `datetime`, `int`, `uint`, `short`, `ushort`, `string`, `guid`, `long`, `ulong`, `byte`, `float`, and `double`.

    g. Replace `set-field-value` with the event field value that you want the central computer to match.
11. ***If you want to create a match rule,*** complete the following steps:
    a. Click **Add Match Rule**.
    b. Replace `set-rule-name` with the name you want to use for the new match rule.
    c. Use the cursor to select `set-field-id`.
    d. Press **Ctrl+Space**.
    e. Select the event field you want the central computer to use to match forwarded messages.

f. Replace `string` with the type of data received.

> **Note**
> Possible options are `datetime`, `int`, `uint`, `short`, `ushort`, `string`, `guid`, `long`, `ulong`, `byte`, `float`, and `double`.

g. Replace `set-field-value` with the event field value that you want the central computer to match.

h. ***If you want to evaluate data against multiple event field values,*** copy and paste the `Field` line onto a new line below the first `Field` line and repeat Step **c** through **g**.

i. In the `Format` element, delete `[503] [502]`.

j. Press **Ctrl+Space**.

k. Select the header event field you want the central computer to include in the forwarded message.

l. Repeat Step **j** through **k** for each event field you want to include as a header event field.

m. Replace `set-platform-identifier:` with an identifier to differentiate the received data.

n. ***If you want to specifically include a certain set of event fields,*** replace `json:{*}` with `json-include:{`*`FIELDS`*`}` and replace *`FIELDS`* with the numbers of all the event fields you want to include, separated by commas.

o. ***If you want to specifically exclude a certain set of event fields,*** replace `json:{*}` with `json-exclude:{`*`FIELDS`*`}` and replace *`FIELDS`* with the numbers of all the event fields you want to exclude, separated by commas.

p. ***If you want to include all event fields,*** leave `json:{*}` within the `Format` element.

> **Note**
> You can only include one JSON tag of any type in a `Format` element.

q. Add any other characters or information to the formatting instructions, as appropriate for your environment.

12. When finished adding new match or filter rules, click **OK**.

13. ***If you want to view the combined message formatting rules,*** including both custom and predefined rules, click **View Combined Formatting Rules**.

14. ***If you want to export the combined message formatting rules in XML format,*** complete the following steps:

a. Click **View Combined Formatting Rules**.

b. Click **Save As**.

c. Specify the file name you want to use and click **Save**.

d. Click **Close**.

15. When finished configuring message formatting, click **Finish**.

Configuring Authenticated Communication

If you enable data forwarding from a central computer to Sentinel or enable Sentinel to search log archive data, the central computer or log archive server use the default self-signed certificate installed with Security Manager for communication with the Sentinel server.

While the default Secure Sockets Layer (SSL) protocol for communication between the central computer or log archive server and Sentinel encrypts and secures your data using the default certificate, you can also configure an additional level of certificate-based authentication. You can configure client authentication, server authentication, log archive server authentication, or all three, as necessary in your environment.

Warning
Configuring authenticated communication is an operation that requires significant planning and consideration. NetIQ recommends that only users with experience working with certificates and authentication configure authenticated Sentinel communication.

Ensure you install all appropriate certificates before enabling client authentication or server authentication. If you enable authentication without correctly installing all certificates, your central computers and Sentinel servers cannot communicate.

Enabling Central Computer Client Authentication

With data forwarding enabled, you can configure your Sentinel 7.0 environment to authenticate a custom certificate from a Security Manager central computer.

The central computer forwards data to Sentinel as a syslog server. Sentinel provides three options for syslog server client authentication:

Open
Sentinel requires no certificate on the central computer.

Loose
Sentinel requires any valid X.509 certificate on the central computer, whether or not that certificate is signed by a certification authority. The default self-signed certificate installed with Security Manager can be used for this level of authentication.

Strict
Sentinel requires a valid X.509 certificate on the central computer, signed by a trusted certification authority.

If your Sentinel syslog server client authentication setting is **Loose**, Sentinel accepts any valid X.509 certificate, such as the default self-signed certificate installed on the central computer.

If your Sentinel syslog server client authentication setting is **Strict**, you must use a certification authority to issue a custom client certificate for your central computer, then import the root certificate of the certification authority into the **trust store** on your Sentinel server.

Notes

- A trust store in Sentinel is similar to a custom certificate store in a Microsoft Windows environment like the `Trusted Root Certification Authorities` certificate store, in that the trust store contains root-level certificates that Sentinel uses to verify client certificates.
- If you configure a central computer to present an untrusted certificate, including the default certificate, to a Sentinel server using Strict client authentication, Sentinel refuses to accept any data forwarded by the central computer.
- If you select **All central computers forward data to the same Sentinel server** in the Configuration Wizard and want to configure multiple central computers to use client authentication, each central computer must use a client certificate with the same subject DN, stored in the same location and certificate store, to forward data to the Sentinel server. The central computer looks locally for a certificate with the specified name and presents that certificate to the Sentinel server.
- NetIQ recommends storing client authentication certificates in the `LocalMachine` certificate store. If you select `CurrentUser` as the location in the Client Certificate Settings window, note that the `CurrentUser` store is the certificate store of the Security Manager service account on the local central computer.

When you issue a custom Security Manager client certificate, ensure the certificate meets the following requirements:

- The certificate is an X.509 certificate.
- The certificate has a private key.
- The certificate has the `EXCHANGE` key specification, including a public/private key pair used to encrypt session keys so they can be safely stored and exchanged with other users.

For more information about working with certificates and trust stores in Sentinel, see the *Administration Guide for Sentinel*. For more information about configuring data forwarding, see “Enabling Security Manager Data Forwarding” on page 4.

To enable Sentinel client authentication using a custom Security Manager certificate:

1. ***If you have not configured a certification authority for your environment,*** establish a certification authority (CA) to issue client authentication certificates. Ensure your certification authority can issue client computer certificates that meet all authentication requirements.

   Note

   You can use your own internal CA or an outside, well-known CA to issue certificates, as configured in your environment.

   ---

2. Use your certification authority to issue a client authentication certificate for your central computer.
3. Log on to the central computer as a member of the local administrators group.

4. Install the client authentication certificate in the `NetIQ Security Manager` container of the `LocalMachine` certificate store on the central computer.
5. ***If the issuer certificate for the client certificate is not already installed on the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `LocalMachine` certificate store.
6. Export the issuer certificate used to issue the client certificate, in X.509 format, to a location on the central computer.

   Note
   You can use either **DER encoded binary X.509** format or **base-64 encoded X.509** format. The **Cryptographic Message Syntax Standard** format is not valid for certificates used by Security Manager or Sentinel.

7. From the central computer, log on to the Sentinel server computer using an administrator account that also has access to the central computer.
8. Copy the exported issuer certificate to your Sentinel server.
9. Use the `TruststoreCreator.sh` or `TruststoreCreator.bat` tools included with Sentinel to create a new trust store that includes the exported issuer certificate. For more information about creating and working with trust stores, see the Sentinel documentation.
10. Start a Web browser on a computer with access to the Sentinel Web interface.
11. Log in to the Sentinel Web interface using an administrator account.
12. In the top bar, click **collection**.
13. Click the Event Source Servers tab.
14. In the Syslog Servers section, select **Strict**.
15. Click **Import**.
16. Click **Browse** and navigate to the location of the trust store file that includes the issuer certificate.
17. Click **Open**.
18. Specify the password you used when creating the trust store.
19. Click **Import**.
20. Click **Save**.
21. Log back on to the central computer as a member of the local administrators group.
22. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
23. In the Navigation pane, click **All Folders**.
24. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
25. Click **Global Settings**.
26. Click **Sentinel Configuration**.

27. Click **Configure Data Forwarding**.

28. Select the central computer for which you issued a client authentication certificate.

29. In the **Connection type** field, select **SSL**.

30. Click **Set Client Certificate**.

31. In the Client Certificate Setting window, specify the subject, location, and store name for the custom Security Manager certificate you want to use.

32. Click **OK**.

33. Click **Finish**.

Enabling Sentinel Server Authentication

With data forwarding enabled, you can also configure the central computer to require that the Sentinel server present a trusted server certificate.

When you install Sentinel 7.0, the setup program automatically installs a default self-signed certificate, which the Sentinel server presents to all event sources for authentication purposes. You can use tools provided with Sentinel to configure Sentinel to use a custom certificate issued by a certification authority.

To enable Sentinel to present a trusted server certificate to the central computer, generate and send a certificate signing request to your CA to request a new Sentinel certificate. Import the certificate into a trust store and import the trust store into your Sentinel server. Request a root certificate from the CA for your central computer and import that root certificate into the trusted root certificate store on your central computer.

Note
If you configure server authentication and select **All central computers forward data to the same Sentinel server**, all central computers must install the issuer certificate for the certification authority that issued the Sentinel server certificate in the `Trusted Root Certification Authorities` container you use in your environment.

When you issue a custom Sentinel server certificate, ensure the certificate meets the following requirements:

- The certificate is an X.509 certificate.
- The certificate has a private key.
- The certificate has the `EXCHANGE` key specification, including a public/private key pair used to encrypt session keys so they can be safely stored and exchanged with other users.

For more information about generating and validating certificates in Sentinel, see the *Administration Guide for Sentinel*. For more information about configuring data forwarding, see “Enabling Security Manager Data Forwarding” on page 4.

To enable Sentinel server authentication:

1. ***If you have not configured a certification authority for your environment,*** establish a certification authority (CA) to sign server authentication certificates.

   Note
   You can use your own internal CA or an outside, well-known CA to issue certificates, as configured in your environment.

2. Log on to the Sentinel server computer using an administrator account.
3. Use your certification authority to issue a server authentication certificate for your Sentinel server.
4. Import the new server certificate into a trust store. For more information about creating and working with trust stores, see the Sentinel documentation.
5. Log in to the Sentinel Web interface using an administrator account.
6. In the top bar, click **collection**.
7. Click the Event Source Servers tab.
8. In the Syslog Servers section, under **Server key pairs**, select **Custom**.
9. Click **Import**.
10. Click **Browse** and navigate to the location of the trust store file that includes the new certificate.
11. Click **Open**.
12. Specify the password you use for the trust store.
13. Click **Import**.
14. Click **Save**.
15. Restart Sentinel.
16. Log on to the central computer as a member of the local administrators and OnePointOp ConfgAdms groups.
17. Request a copy of the issuer certificate from the certification authority you used to issue the Sentinel server authentication certificate.
18. ***If the issuer certificate for the server certificate is not already installed on the central computer,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `LocalMachine` certificate store.
19. Start the **Security Manager Control Center** in the NetIQ Security Manager program group.
20. In the Navigation pane, click **All Folders**.
21. On the Tasks menu, click **Global Tasks > Launch Configuration Wizard**.
22. Click **Global Settings**.
23. Click **Sentinel Configuration**.

24. Click **Configure Data Forwarding**.

25. Select the central computer you want to authenticate the Sentinel server certificate.

26. In the **Connection type** field, select **SSL**.

27. Select **Require trusted server certificate**.

28. Click **Finish**.

Using a Custom Log Archive Certificate for Sentinel Searching

When you use Sentinel 7.0 to search for log archive data, the Sentinel server sends a request to the log archive server, and the log archive server responds by returning any data matching the request. By default, communication between the log archive server and the Sentinel server is secured with SSL, using the self-signed certificate the Security Manager setup program installs on the log archive server.

However, you can also create a custom certificate for the log archive server using a certification authority in your environment. After you generate a custom log archive server certificate, you must associate the new certificate with the port the log archive server uses to listen for requests from Sentinel.

The default port number is **8443**, but you can use a different port number as long as you configure the new port on the log archive server and in Sentinel.

When you issue a custom log archive server certificate, ensure the certificate meets the following requirements:

- The certificate is an X.509 certificate.
- The certificate has a private key.
- The certificate has the EXCHANGE key specification, including a public/private key pair used to encrypt session keys so they can be safely stored and exchanged with other users.

Note
If you installed your central computer and log archive server on two different computers, you must configure any custom log archive server certificate separately from a custom central computer certificate configured for Sentinel client authentication.

To associate the log archive server port with a custom certificate:

1. ***If you have not configured a certification authority for your environment,*** establish a certification authority (CA) to issue client authentication certificates. Ensure your certification authority can issue client computer certificates that meet all authentication requirements.

   Note
   You can use your own internal CA or an outside, well-known CA to issue certificates, as configured in your environment.

   ---

2. Use your certification authority to issue an authentication certificate for your log archive server.

3. Log on to the log archive server as a member of the local administrators group.
4. Install the authentication certificate in the `NetIQ Security Manager` container of the `LocalMachine` certificate store on the log archive server.
5. ***If the issuer certificate for the authentication certificate is not already installed on the log archive server,*** install the issuer certificate in the `Trusted Root Certification Authorities` container of the `LocalMachine` certificate store.
6. Navigate to the `NqLogArchiveServer.exe.config` file on the log archive server. The file is located in the following location on the log archive server by default:

   `installation folder``\NetIQ Security Manager\NetIQ Log Archive`
7. Using a text editor, open the `NqLogArchiveServer.exe.config` file.
8. Search for the following entry:

   ```
   <RESTServerConfiguration enabled="true" port="8443"
   certStoreName="NetIQ Security Manager"
   certSubjectDN="CN=NetIQ Security Manager Server" />
   ```
9. Modify the existing `certStoreName` and `certSubjectDN` values to match the values of your new custom log archive server certificate.
10. ***If you want the log archive to listen for Sentinel requests on a different port,*** replace `8443` with the new port number.
11. Save and close the modified file.
12. Open the Services Administrative Tool located in the Control Panel.
13. In the Services pane, click **NetIQ Security Manager Log Archive**.
14. On the Action menu, click **Restart**.
15. Close the Services Administrative Tool.