RSA NetWitness Logs

Event Source Log Configuration Guide

Citrix XenMobile EMM Suite

Last Modified: Wednesday, January 25, 2017

Event Source Product Information:

Vendor: Citrix
Event Source: Xenmobile Server (formerly Zenprise MobileManager)
Versions: Zenprise MobileManager 6.6, Xenmobile MDM version 8.6, XenMobile Server 10.x
Additional Download (for Xenmobile MDM version 8.6 only)
sftpagent.conf.zenprisemdm

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: zenprisemdm
Collection Method:

- Syslog for Xenmobile Server 10.x
- File for Xenmobile MDM version 8.6
- Syslog for Zenprise MobileManager 6.6

Event Source Class.Subclass: Network.Configuration Management

Overview

Depending on your version, perform one of the following sets of procedures:

- For Zenprise MobileManager 6.6, XenMobile NetScaler Connector 8.5, and XenMobile 10.x, you use Syslog:

  I. Configure Syslog Output on the XenMobile Event Source

  II. Configure RSA NetWitness Suite for Syslog

- For XenMobile MDM 8.6, you use File collection: Configure File Collection for Xenmobile MDM version 8.6

RSA supports collection of logs from both XenMobile Mobile device management (MDM) and Mobile app management (MAM) modes.

From the Citrix product documentation (https://docs.citrix.com/en-us/xenmobile/10/xmob-arch-overview-con.html):

- Mobile device management (MDM) mode

  XenMobile MDM Edition provides mobile device management for iOS, Android, Amazon, and Windows Phone. You deploy XenMobile in MDM mode if you plan to use only the MDM features of XenMobile. For example, you need to manage a corporate-issued device through MDM in order to deploy device policies, apps and to retrieve asset inventories and be able to carry out actions on devices, such as a device wipe.

- Mobile app management (MAM) mode

  MAM supports iOS and Android devices, but not Windows Phone devices. You deploy XenMobile in MAM mode (also referred to as MAM-only mode) if you plan to use only the MAM features of XenMobile without having devices enroll for MDM. For example, you want to secure apps and data on BYO mobile devices; you want to deliver enterprise mobile apps and be able to lock apps and wipe their data. The devices cannot be MDM enrolled.

- MDM+MAM mode

  Using the MDM and MAM modes together provides mobile app and data management as well as mobile device management for iOS, Android, and Windows Phone. You deploy XenMobile in ENT (enterprise) mode if you plan to use MDM+MAM features of XenMobile. For example, you want to manage a corporate-issued device via MDM; you want to deploy device policies and apps, retrieve an asset inventory, and be able to wipe devices. You also want to deliver enterprise mobile apps and be able to lock apps and wipe the data on devices.

Configure Syslog Output on the XenMobile Event Source

Depending on your version, perform one of the following procedures:

- Configure Citrix XenMobile Suite 10.x for Syslog Collection
- Configure Zenprise MobileManager 6.6 for Syslog Collection

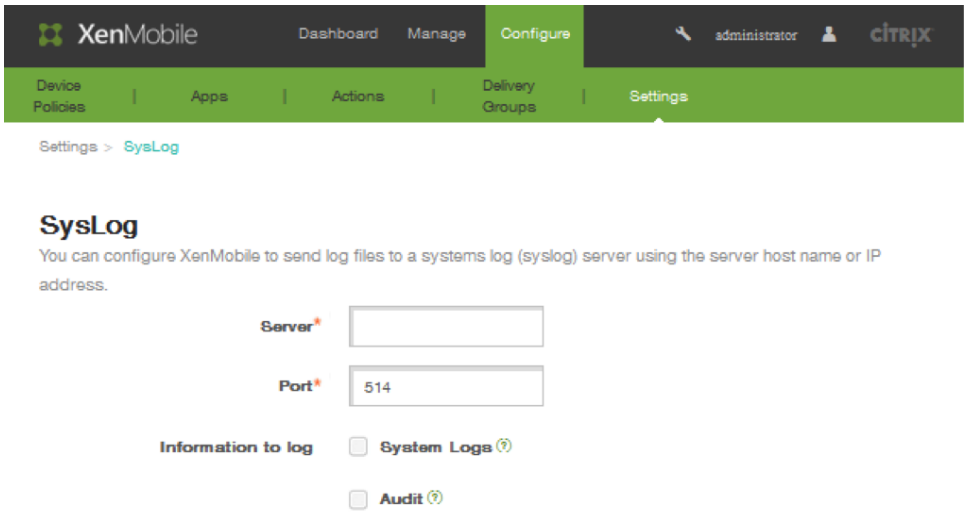
Configure Citrix XenMobile Suite 10.x for Syslog Collection

Use the XenMobile web console to configure a syslog server.

To configure a Syslog server in XenMobile Server 10:

1. In the XenMobile web console, click **Configure > Settings > More > Syslog**.

   The Syslog configuration screen appears.



2. In **Name**, enter either an IP address or the fully qualified domain name (FQDN) of your Syslog server (the RSA NetWitness Log Decoder or Remote Log Collector).
3. 3. In **Port**, enter the port number. By default, the port is set to 514.
4. In **Information to log**, select or clear **System Logs** and **Audit** options, depending on the data you wish to collect.

- **System logs** represent actions taken by XenMobile.
- **Audit logs** represent a chronological record of system activities for XenMobile.

5. Click **Save** to save your settings and close the screen.

Configure Zenprise MobileManager 6.6 for Syslog Collection

To configure RSA support for the Zenprise MobileManager event source, you must edit settings in both the Zenprise Mobile Application Gateway and the Zenprise console (MDM Server).

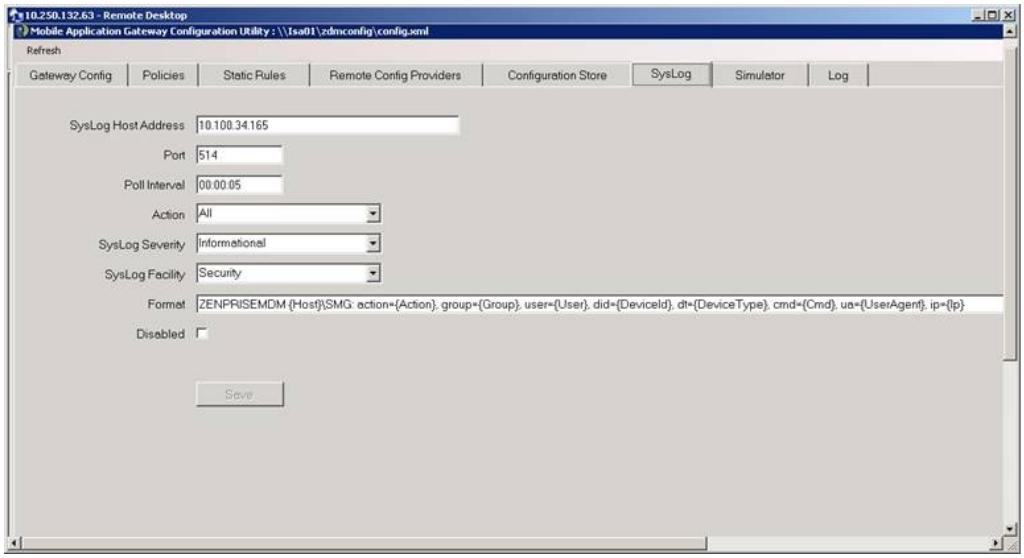
Zenprise Mobile Application Gateway

You set up Syslog format on the Zenprise Mobile Application Gateway.

Note: The instructions vary slightly depending on whether your Zenprise platform is 32- or 64-bit.

To configure the Zenprise Mobile Application Gateway:

1. Start the Zenprise Mobile Application Gateway Configuration Tool (32-bit) or Secure Mobile Gateway (64-bit). The default path for the tool is as follows:
   - For 32-bit: `C:\Program Files\Zenprise\Mobile Application Gateway\Configure.exe`
   - For 64-bit: `C:\Program Files\Zenprise\Secure Mobile Gateway\Configure.exe`
2. Select the **Syslog** tab.
3. Configure the RSA NetWitness Suite server and the syslog string.



- For **Syslog Host Address**, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
- For the **Port**, enter 514.
- For the **Format**, enter the following string:

```
ZENPRISEMDM {Host}\SMG: action={Action}, group=
{Group}, user={User}, did={DeviceId}, dt=
{DeviceType}, cmd={Cmd}, ua={UserAgent}, ip={Ip}
```

4. Save the configuration.
5. Make sure that the Zenprise Gateway Log redirector service is started.

Zenprise MDM Server

On the Zenprise MDM server, you add information to the log4j properties file.

Note: The instructions vary slightly depending on whether your Zenprise platform is 32- or 64-bit.

To configure the Zenprise MDM Server:

1. Open the log4j.properties file in a text editor. The log4j.properties file is in the following folder:

- For 32-bit: `\tomcat\webapps\zdm\WEBINF\classes\`
- For 64-bit: `\zdmtomcat`***x***`\webapps\zdm\WEBINF\classes\`, where ***x*** is the version of Zenprise. For example, for 64-bit version 6, the path is `\zdmtomcat6\webapps\zdm\WEBINF\classes\`.

`\tomcat\webapps\zdm\WEBINF\classes\`

2. Before the ZDM section of the file, add the following text:

```
### SYSLOG ###
log4j.appender.SYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.SYSLOG.syslogHost=LOG DECODER IP ADDRESS
log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.SYSLOG.layout.conversionPattern='ZENPRISEMDM' %d
[%t] %5p %c %x - %m%n
log4j.appender.SYSLOG.Facility=LOCAL1
```

3. Append **,SYSLOG** to lines in the ZDM section of file as follows (text to add is in bold):

```
#### ZDM ####
log4j.logger.com.sparus=info, ZDMLOGFILE,SYSLOG
log4j.logger.com.sparus.nps.SessionPacketQueue=error
log4j.logger.com.sparus.npcommon.Packet= error
log4j.logger.com.sparus.nps.shtp.StartRequest= info
log4j.logger.com.sparus.nps.shtp.ConnectionManager= info
log4j.logger.com.sparus.nps.NetPortalServlet= info
log4j.logger.com.sparus.nps.ios= info
log4j.logger.com.sparus.nps.push= info
log4j.logger.com.sparus.nps.admin.impl.MobileAppGatewayFilterMana
gerImpl=error
log4j.logger.com.sparus.ws.admin.MagConfig=error
log4j.logger.com.sparus.nps.admin.AdmLdapDirectoryProc=error
log4j.logger.com.sparus.nps.ldap=error
log4j.logger.com.sparus.ws.clients.zsmlite.internal.ZMSPServiceMa
nagerImpl=error
log4j.logger.EWSession=error, ZDMLOGFILE,SYSLOG
log4j.logger.com.zenprise.securityfilter.SecurityFilter=info,
ZDMSECURITYLOG
```

```
## set EWSession logging to debug to see packets
#log4j.logger.EWSession=debug, ZDMLOGFILE,SYSLOG
## or set EWSession logging to info to see session state
transitions
#log4j.logger.EWSession=info, ZDMLOGFILE,SYSLOG
log4j.logger.com.zdm.admin.action.Logger=info,
ADMINOPERATIONLOGFILE
log4j.logger.org.drools.xml.ExtensibleXmlParser=error,
ZDMLOGFILE,SYSLOG

## Logging for HTTP requests from Console
log4j.logger.com.sparus.npweb=warn
## AXIS logging ##
log4j.logger.com.sparus.ws=INFO, AXISLOGFILE

##### Tomcat #####
log4j.logger.org.apache=error, ZDMLOGFILE,SYSLOG
log4j.logger.org.apache.commons.digester=error,
ZDMLOGFILE,SYSLOG
# JSP engine/compiler
log4j.logger.org.apache.jasper=error, ZDMLOGFILE,SYSLOG
# JSP pages
log4j.logger.org.apache.jsp=error, ZDMLOGFILE,SYSLOG

##### Hibernate & Spring & EHCache options ####
log4j.logger.org.hibernate=error, ZDMLOGFILE,SYSLOG
log4j.logger.net.sf.ehcache=error, ZDMLOGFILE,SYSLOG
log4j.logger.org.springframework=error, ZDMLOGFILE,SYSLOG
```

4. Restart the Zenprise MDM Server Service.

Configure RSA NetWitness Suite for Syslog

Perform the following steps in NetWitness:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **zenprisemdm**.

Configure Syslog Collection

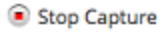
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:

- If you see 

, click the icon to start capturing Syslog.
- If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure File Collection for Xenmobile MDM version 8.6

To configure Xenmobile MDM version 8.6, you must install the SFTP agent, and then configure RSA NetWitness Suite for File event sources.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SA SFTP Agent shell script

Configure the Log Collector for File Collection

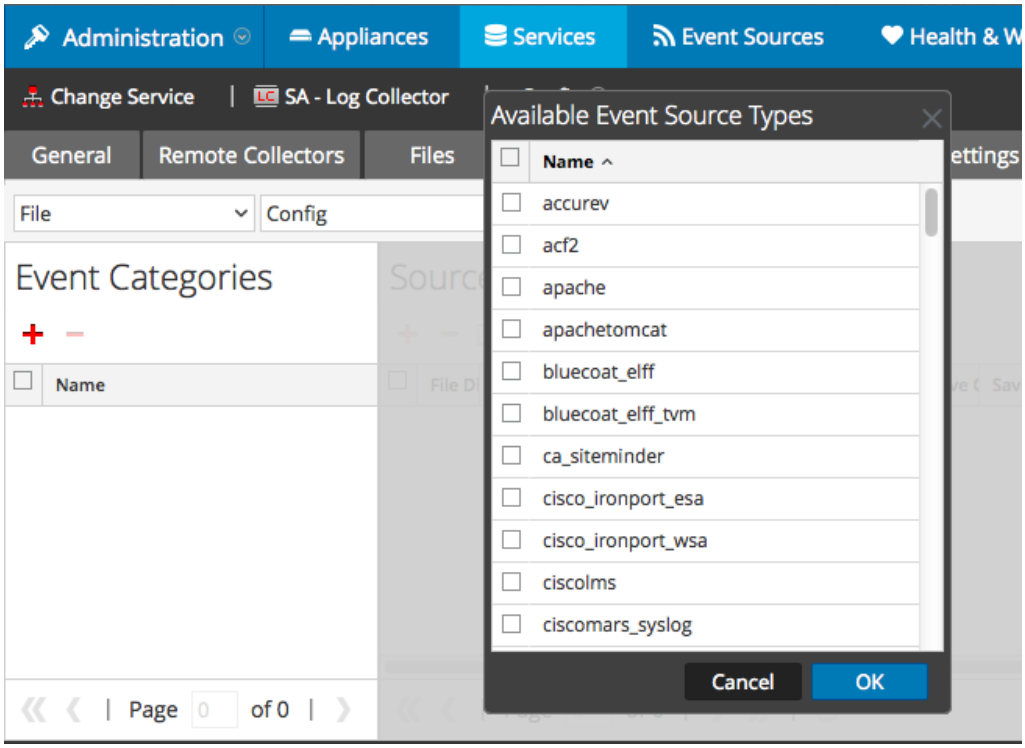
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

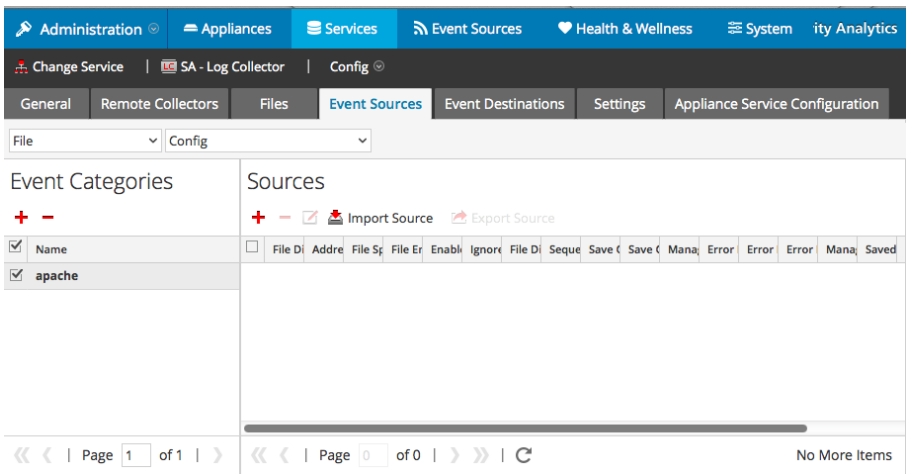
   The Available Event Source Types dialog is displayed.



5. Select the correct type from the list, and click **OK**.

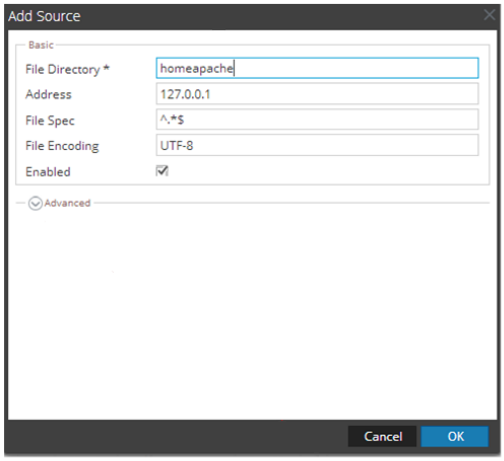
   Select **zenprisemdm** from the **Available Event Source Types** dialog.

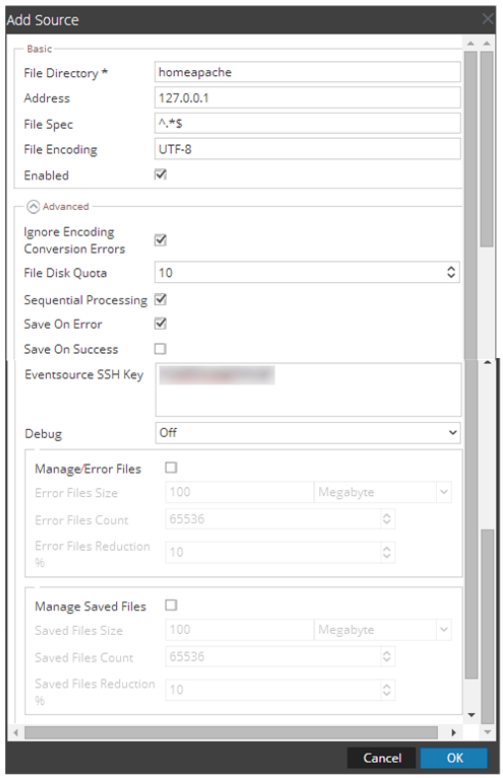
   The newly added event source type is displayed in the Event Categories panel.



6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Trademarks