syslog-ng Premium Edition 6 LTS

Administrator Guide for syslog-ng Agent for Windows

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

> ⊗ **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

> ⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

syslog-ng PE Administrator Guide for syslog-ng Agent for Windows
Updated - 06 October 2023, 11:58
Version - 6 LTS

Contents

Preface

Welcome to the syslog-ng Agent for Windows Administration Guide.

This document describes how to configure and manage syslog-ng Agent for Windows. Background information for the technology and concepts used by the product is also discussed.

Summary of contents

Chapter 1, *Introduction* describes the main functionality and purpose of syslog-ng PE.

Chapter 2, *Installing the syslog-ng Agent* describes how to install syslog-ng Agent for Windows in various scenarios and how to upgrade to new versions.

Chapter 3, *How to configure the syslog-ng Agent* provides detailed description on configuring and managing syslog-ng Agent for Windows.

Chapter 4, *Configuring destinations* provides detailed description on configuring destinations and message rate control.

Chapter 5, *Configuring message sources* describes the configuration of message sources.

Chapter 6, *Using TLS-encrypted connections with syslog-ng Agent* provides detailed description on using TLS-encrypted connections with syslog-ng Agent for Windows.

Chapter 7, *Filtering messages* describes filtering log messages in blacklist or whitelist fashion.

Chapter 8, *Customizing the message format* describes customizing the format of the messages received from the eventlog and the file sources, using templates.

Chapter 9, *Controlling the syslog-ng Agent services* provides details about controlling the syslog-ng Agent for Windows services.

Chapter 10, *Troubleshooting syslog-ng Agent for Windows* describes how to solve common errors and problems.

Chapter 11, *Configuring the auditing policy on Windows* provides descriptions on how to enable auditing on various Windows platforms.

Target audience and prerequisites

This guide is intended for system administrators and consultants responsible for designing and maintaining logging solutions and log centers. It is also useful for IT decision makers looking for a tool to implement centralized logging in heterogeneous environments.

The following skills and knowledge are necessary for a successful syslog-ng PE administrator:

- At least basic system administration knowledge.
- An understanding of networks, TCP/IP protocols, and general network terminology.
- Working knowledge of the Microsoft Windows operating systems.
- An understanding of the legacy syslog (BSD-syslog) protocol) and the new syslog (IETF-syslog) protocol) standard.

Products covered in this guide

This guide describes the use of the following products:

- syslog-ng Agent for Windows (syslog-ng Agent) 6.0.1 and later

Typographical conventions

Before you start using this guide, it is important to understand the terms and typographical conventions used in the documentation. For more information on specialized terms and abbreviations used in the documentation, see theGlossary at the end of this document.

The following kinds of text formatting and icons identify special information in the document.

TIP:

Tips provide best practices and recommendations.

NOTE:

Notes provide additional information on a topic, and emphasize important facts and considerations.

CAUTION:

Warnings mark situations where loss of data or misconfiguration of the device is possible if the instructions are not obeyed.

Command

Commands you have to execute.

Emphasis

Reference items, additional readings.

`/path/to/file`

File names.

`Parameters`

Parameter and attribute names.

Label

GUI output messages or dialog labels.

Menu

A submenu or menu item in the menu bar.

Button

Buttons in dialog windows.

About this document

This guide is a work-in-progress document with new versions appearing periodically.

The latest version of this document can be downloaded from the syslog-ng Documentation page.

Summary of changes

- Starting from syslog-ng Agent 6.0.20, Windows Server 2008 and Windows 7 are not supported.

Feedback

Any feedback is greatly appreciated, especially on what else this document should cover. General comments, errors found in the text, and any suggestions about how to improve the documentation is welcome at bb-pub-documentation@quest.com.

Introduction

This chapter describes how to install and configure the syslog-ng Agent on Microsoft Windows hosts.

The syslog-ng Agent for Windows is a log collector and forwarder application for the Microsoft Windows platform. It collects the log messages of the Windows-based host and forwards them to a syslog-ng server using regular or TLS-encrypted TCP connections.

The features and restrictions of the syslog-ng Agent are summarized below:

- Reads messages from eventlog containers and log files.
- Transfers log messages using TCP.
- Supports TLS encryption.
- Authenticates the server using X.509 certificates. Mutual authentication is also supported.
- The format of eventlog messages can be customized using macros.
- Supports multiple destinations both in parallel and fail-over modes.
- Can be managed from a domain controller using group policies.
- Only basic filtering is supported by the agent, message segmenting, parsing, and classification is not.
-

  Note that the log messages on Windows come from files — either eventlog containers or custom log files — which are already stored on the hard disk, so syslog-ng Agent for Windows does not use additional disk buffering.

Supported operating systems

The central syslog-ng server cannot be installed on Microsoft Windows platforms. The syslog-ng Agent for Windows is capable of forwarding log messages to the central syslog-ng server. It is part of the syslog-ng PE, and is licensed together with it.

The syslog-ng Agent application supports the following operating systems. Unless explicitly noted otherwise, the subsequent releases of the platform (for example, Windows Server 2019 R2 and its service packs in case of Windows Server 2019) are also supported.

- Microsoft Windows Server 2012 (x86_64)
- Microsoft Windows Server 2016 (x86_64)
- Microsoft Windows Server 2019 (x86_64)

- Microsoft Windows Server 2022 (x86_64)
- Microsoft Windows 8 (x86 and x86_64)
- Microsoft Windows 10 (x86 and x86_64)
- Microsoft Windows 11 (x86_64)

> NOTE:
>
> The syslog-ng Agent for Windows application supports the XML-based eventlog format and offers full support for 64-bit operating systems.

Installing syslog-ng Agent for Windows

The syslog-ng Agent for Windows application can be installed in standalone mode on independent hosts. If your hosts are members of a domain, you can install the syslog-ng agent on the domain controller and configure them globally.

- For details on how to install the syslog-ng Agent for Windows application in standalone mode, see Procedure 2.1, "Installing the syslog-ng Agent in standalone mode".
- For details on how to install the syslog-ng Agent for Windows application on the members of a domain, see the section called "Installing the syslog-ng Agent on the domain controller and the hosts of a domain".

> NOTE:
>
> The syslog-ng Agent for Windows application is configured usually using its MMC snap-in (when managed globally from the domain controller or when configuring it in standalone mode). However, it is also possible to use an XML-based configuration file. For details, see the section called "Using an XML-based configuration file".

> **CAUTION:**
>
> **If you are using an XML configuration file, or you have installed syslog-ng Agent with an XML configuration file, it is not possible to use the MMC snap-in for configuring the syslog-ng Agent.**

Installer types:

- `syslog-ng-agent-<version>-setup.exe` is the general installer. This installs an agent that can be configured with a local configuration, XML configuration file and can receive configuration from domain group policy. The installer contains both the 32bit and 64bit versions of syslog-ng Agent.
- `syslog-ng-agent-nosnapin-<version>-setup.exe` is a special installer. .NET environment is not required for it. This installs an agent that can only be configured with an XML configuration file, and can receive configuration from domain group policy. The installer contains both the 32bit and 64bit versions of syslog-ng Agent.
- `syslog-ng-agent-setup-<version>-<amd64/i386>.msi` is an MSI installer for domain clients, installing by group policy.

Procedure 2.1. Installing the syslog-ng Agent in standalone mode

Purpose:

The syslog-ng Agent for Windows application can be installed in standalone mode on independent hosts. If your hosts are members of a domain, install the syslog-ng Agent on the domain controller, as described in the section called "Installing the syslog-ng Agent on the domain controller and the hosts of a domain". The syslog-ng Agent requires about 30 MB hard disk space.

To install the syslog-ng Agent in standalone mode, complete the following steps:

> NOTE:
>
> The regular `.exe` installer of syslog-ng Agent for Windows requires the Microsoft .NET Framework version 3.5 or 4.0. This package is usually already installed on most hosts. If it is not, you can download the .NET package here.
>
> The `nosnapin` and the `.msi` version of the installer does not install the graphical MMC snapin of syslog-ng Agent, and does not require the .NET Framework.

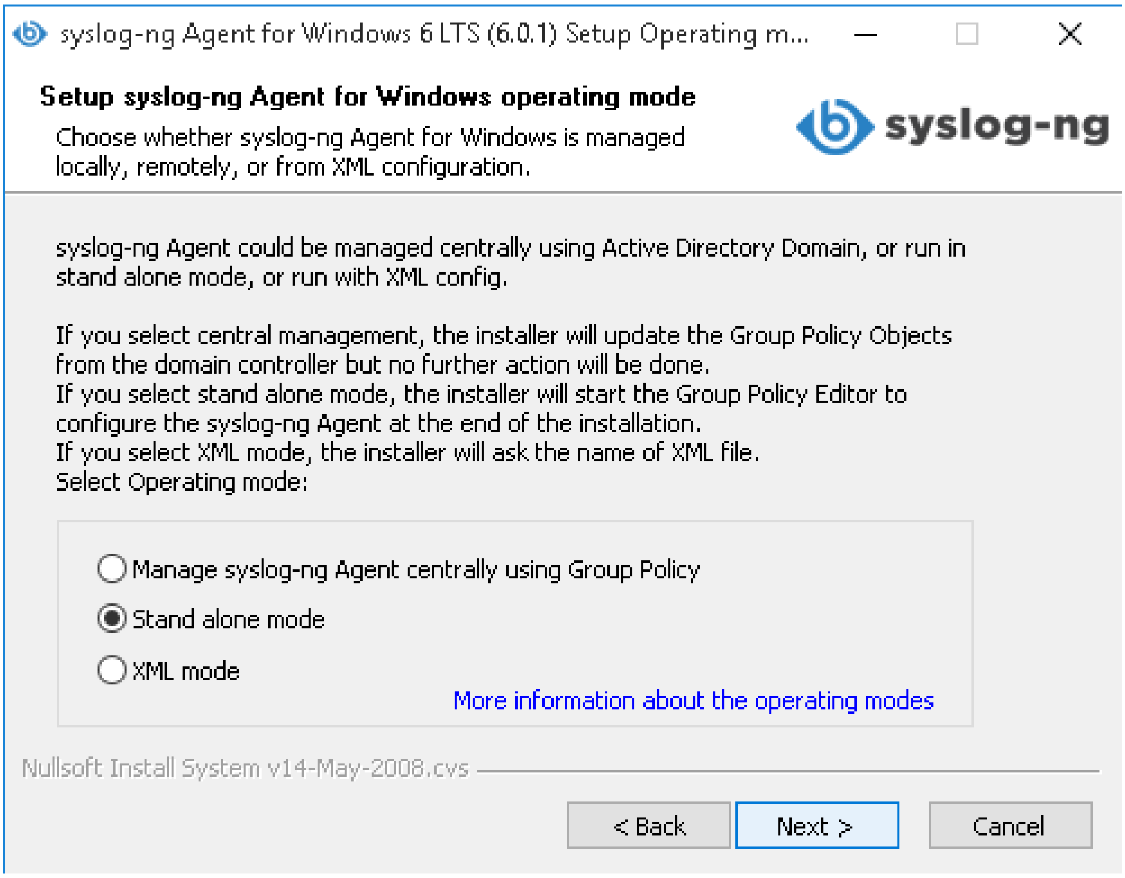
Steps:

1. Start the installer. Run the `syslog-ng-agent-<versionnumber>-setup.exe` file.

   > NOTE:
   >
   > Installing the syslog-ng Agent requires administrator privileges.

2. Read the End User License Agreement and select I Agree.
3. Select the destination folder where you want to install the syslog-ng Agent for Windows application, then select Next.
4. Select Standalone mode, then click Next.

   Figure 2.1. Installing in Standalone mode


syslog-ng Agent for Windows 6 LTS (6.0.1) Setup Operating m...
syslog-ng

Setup syslog-ng Agent for Windows operating mode

Choose whether syslog-ng Agent for Windows is managed locally, remotely, or from XML configuration.

syslog-ng Agent could be managed centrally using Active Directory Domain, or run in stand alone mode, or run with XML config.

If you select central management, the installer will update the Group Policy Objects from the domain controller but no further action will be done.
If you select stand alone mode, the installer will start the Group Policy Editor to configure the syslog-ng Agent at the end of the installation.
If you select XML mode, the installer will ask the name of XML file.
Select Operating mode:

○ Manage syslog-ng Agent centrally using Group Policy

● Stand alone mode

○ XML mode

More information about the operating modes

5. The installer automatically opens the configuration interface of the syslog-ng Agent. As a minimum, you must set the IP address of the destination server, and the agent will automatically start sending eventlog messages to your central log server from the Application, Security, and System eventlog containers.

   NOTE:

   The installation is completed only after you close the configuration interface. For details on how to modify the configuration later, see Procedure 3.1, “Configuring a standalone syslog-ng Agent”.

Installing the syslog-ng Agent on the domain controller and the hosts of a domain

The syslog-ng Agent for Windows application can be installed on the domain controller and the members of a domain from the domain controller, and configured globally using group policies. The syslog-ng Agent requires about 30 MB hard disk space.

- For details on how to install the syslog-ng Agent application in a domain, see Procedure 2.2, "Installing the syslog-ng Agent on the domain controller and the hosts of a domain".
- For details on how to configure the syslog-ng Agents of the domain hosts, see Procedure 3.2, "Configuring the syslog-ng Agents of the domain hosts".
- For details on how to configure the syslog-ng Agents of the domain controllers, see Procedure 3.3, "Configuring the syslog-ng Agents of the domain controllers".

> NOTE:
>
> The *.msi* version of the installer does not install the MMC configuration snap-in of the agent, therefore the *.msi* installer does not require the .NET framework.

Procedure 2.2. Installing the syslog-ng Agent on the domain controller and the hosts of a domain

Purpose:

To install the syslog-ng Agent application on the domain controller and the hosts of a domain, complete the following steps.

This procedure assumes that you install the syslog-ng Agent on the domain controllers in standalone mode, and configure the domain hosts from each domain controller.

> NOTE:
>
> To configure the syslog-ng Agent from domain controllers, you need to install the syslog-ng Agent in standalone mode on at least one domain controller. You can then export the configuration of syslog-ng Agent from the first domain controller and import it to other domain controllers, or you can configure an agent group policy on the other domain controllers, and install syslog-ng Agent in domain mode.

> NOTE:
>
> By default, the syslog-ng Agent for Windows application sends messages as follows:
>
> - From eventlog sources, the syslog-ng Agent application sends only messages that are created after the agent has been installed.
> - From file sources, it sends the entire content of the file.

Steps:

1. Download both the Microsoft Installer (*.msi*) version and the executable (*.exe*) version of the syslog-ng Agent installer to the domain controller host. Make sure to download the executable that includes the MMC snap-in module. Note that separate .msi installers are available for 32-bit and 64-bit operating systems.

   > NOTE:
   >
   > Installing the syslog-ng Agent requires administrator privileges, but configuring the related group policies on the domain controller requires domain administrator or higher (for example enterprise administrator) privileges.

2.

Install the syslog-ng Agent application to your domain controllers using the `.exe` installer.

NOTE:

The regular `.exe` installer of syslog-ng Agent for Windows requires the Microsoft .NET Framework version 3.5 or 4.0. This package is usually already installed on most hosts. If it is not, you can download the .NET package here.

The `nosnapin` and the `.msi` version of the installer does not install the graphical MMC snapin of syslog-ng Agent, and does not require the .NET Framework.

In some rare cases, the syslog-ng Agent service does not start after the installation and you receive the following error message: `"Error 1 : Incorrect Function."`. In this case, open a command prompt and run the `gpupdate /force` command.

3. • Navigate to Start > Control Panel > Administrative Tools > Group Policy Management.

4. • Select and edit the Group Policy object you want to add the syslog-ng Agent configuration to. Alternatively, you can create a new group policy object as well.

5. Select Computer Configuration, right-click on Software Settings, and select New > Package.

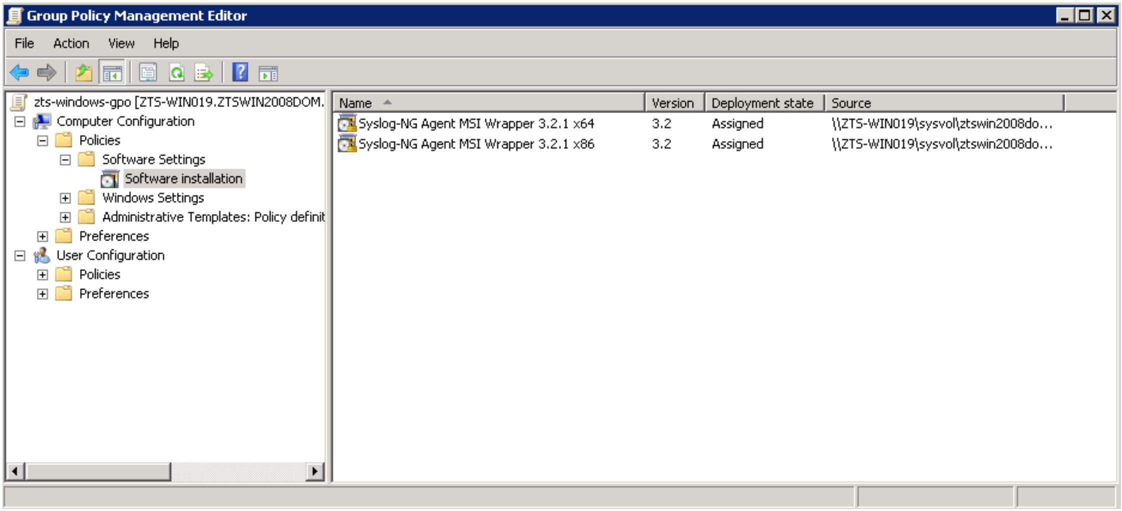
6.

Navigate to the syslog-ng Agent for Windows *.msi* installer and select Open.

7. Select Assigned, then OK.

Select Computer Configuration > syslog-ng Agent Settings and configure the syslog-ng Agent. The members of the domain will use this configuration.

Figure 2.2. syslog-ng Agent Settings



zts-windows-gpo [ZTS-WIN019.ZTSWIN2008DOM.
⊟ Computer Configuration
  ⊟ Policies
    ⊟ Software Settings
        Software installation
    ⊞ Windows Settings
    ⊞ Administrative Templates: Policy definit
  ⊞ Preferences
⊟ User Configuration
  ⊞ Policies
  ⊞ Preferences

Name	Version	Deployment state	Source
Syslog-NG Agent MSI Wrapper 3.2.1 x64	3.2	Assigned	\\ZTS-WIN019\sysvol\ztswin2008do...
Syslog-NG Agent MSI Wrapper 3.2.1 x86	3.2	Assigned	\\ZTS-WIN019\sysvol\ztswin2008do...

8.

9. The syslog-ng Agent for Windows application will be automatically installed on the members of the domain when they are next rebooted.

> NOTE:
>
> If you do not want to install the syslog-ng Agent automatically from the domain controller, skip Steps 5-7, complete Step 8, then install the `syslog-ng-agent-nosnapin-<versionnumber>-setup.exe` file manually on the members of the domain. This method is useful if you do not want to install the syslog-ng Agent on every host of the domain.

10. After the members of the domain have been rebooted, execute the **gpupdate** command on the members of the domain. The syslog-ng Agent for Windows application will receive its configuration during the group policy update, and start processing log messages accordingly.

Procedure 2.3. Installing the MSI package of syslog-ng Agent into a custom folder

Purpose:

The `.msi` installer package of syslog-ng Agent can be modified to install the syslog-ng Agent application into a custom folder.

Steps:

When installing the syslog-ng Agent application from the command line, execute the following command to specify a custom installation folder: **msiexec /i syslog-ng-agent-setup-<version>-<amd64/i386>.msi INSTDIR=C:\<path-to-custom-folder>**

Otherwise, complete the following steps to modify the `.msi` package.

1. Download the Orca MSI editor.
2. Start Orca and load the `syslog-ng-agent-setup-<version>-<amd64/i386>.msi` file to modify.
3. Select Transform > New Transform.
4. Add the *`INSTDIR`* property to the Property Table, and set its value to the full path of the folder where you want to install the syslog-ng Agent application.
5. Select Transform > Generate Transform and save the modifications into a `.mst` file.
6. Close the Orca MSI Editor.
7. Select Start > Control Panel > Administrative Tools > Active Directory Users and Computers and edit the Group Policy object that contains the syslog-ng Agent configuration.
8. Add the saved `.mst` package as a modification to the syslog-ng Agent `.msi` package.

Procedure 2.4. Uninstalling syslog-ng Agent

To uninstall the syslog-ng Agent application, complete the following steps. To uninstall syslog-ng Agent from the command-line, see Procedure 2.5, "Uninstalling syslog-ng Agent in silent mode".

1. Navigate to the installation directory of syslog-ng Agent.
2. Start the `uninstall.exe` file.

3. Follow the on-screen instructions.

Procedure 2.5. Uninstalling syslog-ng Agent in silent mode

To uninstall the syslog-ng Agent application from the command-line, complete the following steps. To uninstall syslog-ng Agent using the graphical interface, see Procedure 2.4, “Uninstalling syslog-ng Agent”.

1. Start a command prompt and navigate to the installation directory of syslog-ng Agent.
2.
   - To uninstall syslog-ng Agent and delete its configuration from the registry, execute the `uninstall.exe /S /DELCONF` command.
   - To uninstall syslog-ng Agent, without deleting its configuration, execute the `uninstall.exe /S` command.

Silent installation

The syslog-ng Agent for Windows application can be installed in silent mode as well, without requiring any user interaction. The various installer options can be specified as command-line options. Using the */S* option is required. The following options are available.

> ⚠ **CAUTION:**
>
> **Write all options in uppercase.**

/D=<path>

Install the syslog-ng Agent into the specified folder. Do not use quotes (`''`) or double-quotes (`""`) around the folder name, even if it contains whitespace characters.

> ⚠ **CAUTION:**
>
> **If you use the */D* option, make sure that this is the last option in the command-line. For example: syslog-ng-agent-nosnapin-<version>-setup.exe /S /XMLCONFIG=c:\test.xml /LOCALUPGRADE /D=c:\Program Files\agent\**

/LOCAL

Install syslog-ng Agent in standalone mode. This is the default installation mode of the syslog-ng Agent. When using this option, you can also set the following two options:

- */GPOUPGRADE*: Upgrade all GPO configuration having syslog-ng Agent settings during the installation.

  > ⚠ **CAUTION:**
  >
  > **Use it only on a domain controller.**

- */LOCALUPGRADE*: Upgrade local settings.

  > 🛈 NOTE:
  >
  > If syslog-ng Agent uses only local configuration and you do not specify this option, it is possible that syslog-ng Agent will not start while you are upgrading its local configuration by opening local configuration with syslog-ng agent MMC snap-in.

/NOMENU

Do not add entries about syslog-ng Agent to the Start menu.

/NOUPGRADE

The installer does not perform upgrade during the installation (default). Use it if the configuration comes from GPO or you are using XML configuration and you do not want to upgrade it (in this case, agent will upgrade it temporarily after starting).

/REMOTE

Install syslog-ng Agent in domain mode.

/S

Start the installer in silent mode. This option is required for the silent installation.

/XMLCONFIG=

Use the specified XML configuration file for the configuration of syslog-ng Agent. When using this option, you can also set the following option:

- *`/XMLUPGRADE`*: Upgrade XML configuration during the installation if XML configuration file is used.

The upgrade operation will be only performed if upgrading is really needed for the specified configuration. For example: If there is no configuration version switching between the current and the previous version of the syslog-ng Agent (for example when upgrading from version 3.0.7 to version 3.0.8) the local settings will not be upgraded even you specify the **/LOCALUPGRADE** option.

The *`/LOCAL`*, *`/XMLCONFIG`*, and *`/REMOTE`* options conflict with each other. If you specify more than one of them, then *`/REMOTE`* takes precedence over the other two options, and *`/XMLCONFIG`* takes precedence over the *`/LOCAL`* option.

Upgrading syslog-ng Agent for Windows to the latest version

The exact upgrading procedure of the syslog-ng Agent for Windows application depends on how you have installed and how you manage the agent.

⚠ **CAUTION:**

- **When upgrading agents running in domain mode, always upgrade the agents running on the domain hosts before upgrading the agent running on the domain controllers.**
- **The hosts of a domain (including the domain controllers) have to run the same version of the syslog-ng Agent, running different versions on the hosts is neither supported nor recommended.**
- **If the Services window of MMC is open, close it before upgrading, because it can prevent the successful registration of the agent service.**

- If a host is running syslog-ng Agent in standalone mode, download and execute the `syslog-ng-agent-<versionnumber>-setup.exe` installer on the host and verify that the displayed information is correct. The agent will be automatically restarted when you close the configuration window.
-

  If a domain host is running the syslog-ng Agent that was installed by the domain controller from the *.msi* installer package, complete the steps described in the section called "Installing the syslog-ng Agent on the domain controller and the hosts of a domain". The system will automatically recognize that the new package will update the syslog-ng Agent for Windows application.
- If a domain host is running the syslog-ng Agent that was installed manually from the `syslog-ng-agent-nosnapin-<versionnumber>-setup.exe` file, run the new `syslog-ng-agent-nosnapin-<versionnumber>-setup.exe` file on the host. After the installation is complete, select Start > Run and execute the **gpupdate** command to refresh the domain settings of the agent.
- If syslog-ng Agent has been installed with an XML configuration file with `syslog-ng-agent-<versionnumber>-setup.exe` or `syslog-ng-agent-nosnapin-<versionnumber>-setup.exe`, download and execute the same installer. It will display the previous XML configuration file, and upgrades it if desired.

How to configure syslog-ng Agent for Windows

This section describes how to configure the syslog-ng Agent application. The exact method depends on the installation scenario and also on the configuration method (regular or XML-based) you want to use. The syslog-ng Agent for Windows application is configured usually using its MMC snap-in (when managed globally from the domain controller or when configuring it in standalone mode). However, it is also possible to use an XML-based configuration file.

- For details on how to configure a syslog-ng Agent that was installed in standalone mode, see Procedure 3.1, "Configuring a standalone syslog-ng Agent".
- For details on how to configure the syslog-ng Agents of the domain hosts, see Procedure 3.2, "Configuring the syslog-ng Agents of the domain hosts".
- For details on how to configure the syslog-ng Agents of the domain controllers, see Procedure 3.3, "Configuring the syslog-ng Agents of the domain controllers".
- For details on how to configure syslog-ng Agent from file, see the section called "Using an XML-based configuration file".

Procedure 3.1. Configuring a standalone syslog-ng Agent

Purpose:

To configure an already installed standalone syslog-ng Agent, perform the following steps.

Steps:

1. Start the syslog-ng PE configuration interface by navigating to Start Menu > Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent.
2. Select Local Settings, and configure the syslog-ng Agent as needed for your environment.
3.

   After modifying its configuration, you have to restart the *syslog-ng Agent* service for the changes to take effect. To restart the syslog-ng Agent service, select Start Menu > Run, enter *services.msc* and restart the syslog-ng Agent service.

Configuring the syslog-ng Agents of a domain

This section describes how to configure the syslog-ng Agent for Windows application in domain mode.

- For details on how to configure the syslog-ng Agents of the domain hosts, see Procedure 3.2, "Configuring the syslog-ng Agents of the domain hosts".
- For details on how to configure the syslog-ng Agents of the domain controllers, see Procedure 3.3, "Configuring the syslog-ng Agents of the domain controllers".
- For details on the relationship of different group-policy levels, see the section called "Domain versus local settings".

Procedure 3.2. Configuring the syslog-ng Agents of the domain hosts

Purpose:

To configure an already installed syslog-ng Agent from the domain controller, perform the following steps.

Steps:

1. Start the syslog-ng PE configuration interface by navigating to Start Menu > Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent.
2. Navigate to Client Group Policy, and select the Group Policy you want to modify (for example, the Default Domain Policy).
3. Configure the syslog-ng Agent as needed for the domain hosts. The changes will take affect when the domain hosts update their settings from the domain controller. By default, this happens every 90 minutes, depending on your domain settings. To download the configuration earlier, execute the **gpupdate** command on the members of the domain.

   > NOTE:
   >
   > When the domain hosts update their settings, the syslog-ng Agent will be automatically restarted to load the new settings, except when there is no difference between the old and the new settings.

Procedure 3.3. Configuring the syslog-ng Agents of the domain controllers

Purpose:

To configure the syslog-ng Agent running on the domain controllers, perform the following steps.

In a domain tree or forest, to configure the syslog-ng Agent for a specific domain, you must be a Domain Administrator of the domain.

Steps:

1. Start the syslog-ng PE configuration interface by navigating to Start Menu > Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent.
2. - To configure syslog-ng PE only on a single domain controller, select Local Settings. Note that if you have configured syslog-ng PE also in a Group Policy that affects domain controllers, the settings of the Group Policy will override

these local settings.

- To configure syslog-ng PE on every domain controller, select Client Group Policy, then select the appropriate Group Policy of your domain controllers (for example, Default Domain Controllers Policy).

3. Configure the syslog-ng Agent as needed for the domain controllers. If you have multiple domain controllers, the changes will take affect when the other domain controllers update their settings from this domain controller. By default, this happens every 5 minutes, depending on your domain settings. To download the configuration earlier, execute the **gpupdate** command on the domain controllers.

> NOTE:
>
> When the domain controllers receive the new settings, the syslog-ng Agent will be automatically restarted to load the new settings, except when there is no difference between the old and the new settings.

Domain versus local settings

The syslog-ng Agent follows the standard policy-inheritance methods of Windows:

GPOs (Group Policy Objects) from parent containers are inherited by default. When multiple GPOs apply to these computers, the settings in the GPOs are aggregated. The final value of a given policy setting is set only by the highest precedent GPO that contains the setting. (However, the final value for a few settings will actually be the combination of values across GPOs.) In this processing order, sites are applied first, but have the least precedence. OUs (Organization Units) are processed last, but have the highest precedence.

When multiple group policy objects are assigned, the group policies are applied in the following order:

1. The local group policy object is applied.
2. The group policy objects linked to sites are applied. If multiple GPOs exist for a site, they are applied in the order specified by the administrator.
3. GPOs linked to the domains are applied in the specified order.
4. GPOs linked to OUs are applied. The OU group policy objects are set from the largest to the smallest organizational unit, that is, first the parent OU and then the child OU. By default, a policy applied later overwrites a policy that was applied earlier. Hence, the settings in a child OU can override the settings in the parent OU.
5. If any group policy is not configured, the syslog-ng Agent checks its local policy settings, and uses the local setting if available.

The following are the rules regarding group policy settings inheritance:

- A policy setting is configured (Enabled or Disabled) for a parent OU, and the same policy setting is not configured for its child OUs. The child OUs inherit the parent’s policy.

- A policy setting is configured (Enabled or Disabled) for a parent OU, and the same policy setting is configured for its child OUs. The child OUs settings override the settings inherited from the parent's OU. There is a specific case, when the type of this setting is list:
    - The syslog-ng Agent will aggregate the contents of these lists and will use the same elements only once.
    - If any policy is not configured (Not Configured), no inheritance takes place.

> NOTE:
>
> Do not use setting Not Configured in local settings, because in that case, it can still use previously configured values. Use settings Enabled or Disabled instead.

Using an XML-based configuration file

Starting from syslog-ng Agent for Windows version 3.2, it is possible to export the configuration of syslog-ng Agent into an XML file. This configuration file can be used as the default configuration when installing the syslog-ng Agent to another host, or can be imported to an existing installation using a command-line utility.

> ⚠ **CAUTION:**
>
> **Do not manually edit or modify the exported XML file.**
>
> **In case you want to validate the XML file, use the `syslog-ng-agent-conf.xsd` file located in the installation directory of syslog-ng Agent for Windows.**

> ⚠ **CAUTION:**
>
> **If you are using an XML configuration file, or you have installed syslog-ng Agent with an XML configuration file, it is not possible to use the MMC snap-in for configuring the syslog-ng Agent.**

Procedure 3.4. Creating an XML configuration file for the syslog-ng Agent

Purpose:

To create an XML configuration file that can be used by other syslog-ng Agent configurations, perform the following steps.

Steps:

1. Install the syslog-ng Agent for Windows application on a host.
2. Create the configuration you want to use on other hosts using the graphical interface. The syslog-ng Agent for Windows application will store this configuration in the registry.
3. Right-click on syslog-ng Agent Settings and select Export to export the configuration of syslog-ng Agent from the registry to an XML file. Select where to save the XML file.

   Alternatively, you can export the configuration of syslog-ng Agent from the command line using the **configmanager.exe -export <source> "destination xml file"** command. The <source> parameter determines which configuration is exported:

   - *`{GPO ID}`*: Export the configuration related to the specified Group Policy Object ID (for example, *`{99AF1185-AB80-40B2-B4B8-41A1E907F329}`*).
   - *`localsettings`*: Export the local settings of the host.
   - *`domainsettings`*: Export the settings the host received from the domain controller.

   > 🛈 NOTE:

> To overwrite the XML configuration file, use the /F option. This will force export even if the file already exists.

4. Use the configuration file on other hosts. For details on the different options, see the section called "Configuring syslog-ng Agent from an XML file".

Configuring syslog-ng Agent from an XML file

How you configure the syslog-ng Agent application to use an XML configuration file depends on your environment. The following list describes the available possibilities.

> ⚠ **CAUTION:**
>
> - **Do not manually edit or modify the exported XML file.**
> - **Do not delete the XML configuration file: syslog-ng Agent for Windows will look for the file every time it is started or restarted. If you need to change the location of the file, edit the *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\syslog-ng Agent\ImagePath* registry key.**

- To use the XML file during the installation of the syslog-ng Agent application, navigate to Setup syslog-ng Agent for Windows operating mode window and select XML mode. In the next window, browse your XML configuration. Note that the XML schema file will be installed in the syslog-ng Agent directory.
- If you want to use the .msi installer with an XML file, use the **syslog-ng-agent-setup-<version>-<amd64/i386>.msi SLNGOPTS="/xmlconfig=fullpath\myconfigfile.xml"** command, or edit the installer with the Orca MSI editor, and add the *SLNGOPTS="/xmlconfig=fullpath\myconfigfile.xml"* to the installation parameters on the Customization tab.
- **Use an XML file as the configuration file of syslog-ng Agent for Windows.** To start an already installed, standalone syslog-ng Agent using an XML configuration file, execute the following steps in a command line. In this case, the configuration of syslog-ng PE is stored in the XML file, it is not imported into the registry (for details on importing a configuration from XML file into the registry, see Import the XML configuration into the registry).
  1. **cd <syslog-ng agent installation directory>\bin**
  2. **net stop "syslog-ng agent"**
  3. **syslog-ng-agent.exe /r**
  4. **syslog-ng-agent.exe /i <PATH>\configuration.xml**
  5. **net start "syslog-ng agent"**

- **Import the XML configuration into the registry.** To import the XML configuration file into the registry of the host, use the following command: **configmanager.exe -import <destination> "source xml file"** command, then restart the syslog-ng Agent service. The <destination> parameter determines which configuration the XML configuration will be converted to:
  - *{GPO ID}*: Import the configuration to the specified Group Policy Object ID (for example, *{99AF1185-AB80-40B2-B4B8-41A1E907F329}*).
  - *localsettings*: Import the configuration as the local settings of the host.
  - *domainsettings*: Import the configuration as the domain settings of the host.

  CAUTION:

  Importing the configuration file from an XML file into the registry of the host has no effect if syslog-ng Agent is configured to use an XML configuration file.

Configuring destinations

The syslog-ng Agent for Windows application can send the log messages of the Windows host to a central log server or relay. It is possible to send the same messages to multiple servers, when each server receives the same messages. You can configure failover servers, when the agent sends the messages to a primary server, or to a failover server if the primary becomes unavailable. If the agent loses the connection to a destination server and the reconnection fails, it will generate an eventlog message. The successful reconnection attempt is also logged. (If the server is unavailable for a long time, the agent generates a log message about the failed connection once in every ten seconds.)

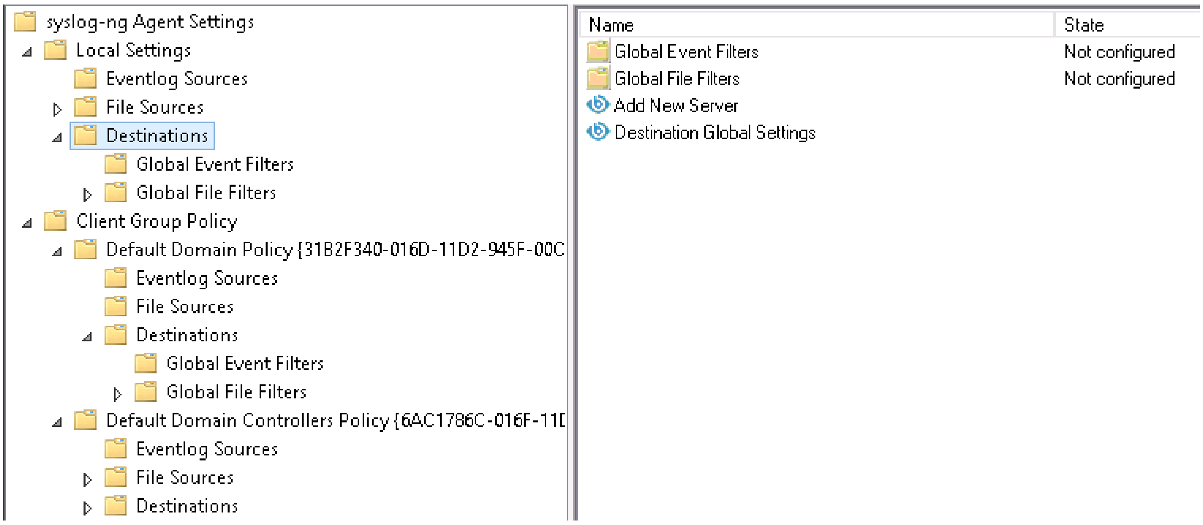
If the failover server also becomes unavailable, the application will switch to the next failover server, and so on. If the last failover server is unavailable, it switches back to the primary. The application does not switch back automatically to the primary server if it becomes available again, only if the syslog-ng Agent for Windows has been restarted.

> NOTE:
>
> The failover servers will use the same options that the primary server uses. Only the name and the address can be configured for the failover servers.

Similarly to the Linux version, the agent now sends MARK messages to the server to indicate that the client host is alive but there are no log messages to send. A MARK message is sent every ten minutes.

> **CAUTION:**
>
> **The syslog-ng Agent for Windows application does not support the unreliable UDP protocol. Configure your central log server to accept logs using TCP or TLS connections. If needed, adjust your firewall configuration to permit such traffic to the log server.**

Figure 4.1. Adding new destinations



Name	State
Global Event Filters	Not configured
Global File Filters	Not configured
Add New Server	
Destination Global Settings	

Procedure 4.1. Configuring the destination log servers

Purpose:

To configure a new destination, complete the following steps:

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Destinations, and double-click on Add new server.

Figure 4.2. Adding new server

Enter the hostname or the IP address of the log server into the Server Name or Address (IPv4) field. If your log server is configured to accept messages on a non-standard port, type the port number into the Server Port field. To use the default port (`35514` when RLTP™ is enabled and `514` when RLTP™ is disabled), click Reset to Default Port.

To enable flow-control, select Enable flow-control. For details, see the section called “Flow-control in syslog-ng Agent for Windows”.

To use SSL encryption, enable Use TLS encryption. For details, see Chapter 6, *Using SSL-encrypted connections with the syslog-ng Agent*.

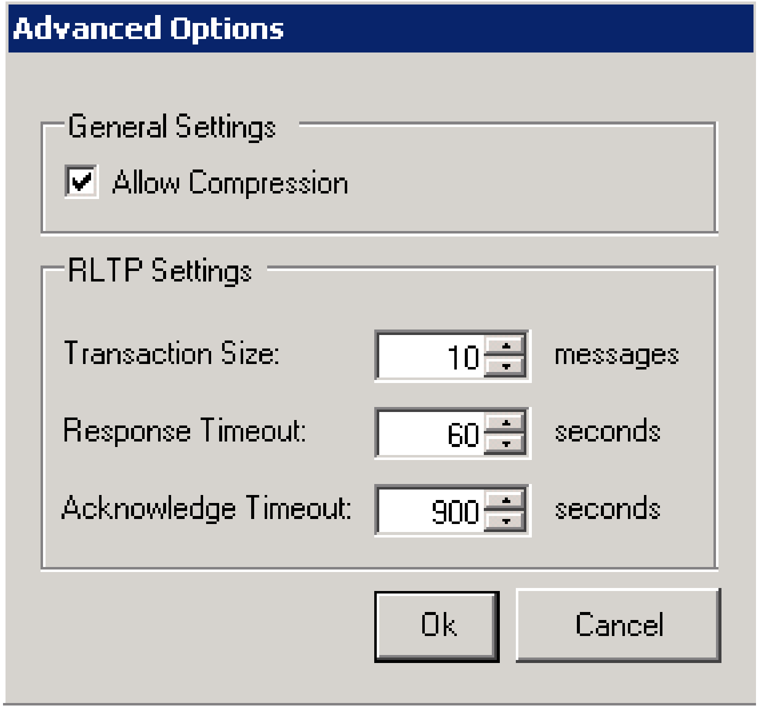
3.

4. *Optional Step*: To use the Reliable Log Transfer Protocol™ (RLTP™), enable Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP).

> NOTE:
>
> You cannot disable flow-control when using the Reliable Log Transfer Protocol™ (RLTP™).

Click Advanced Options.

Figure 4.3. Advanced Options: allowing compression and RLTP settings


Advanced Options

General Settings

☑ Allow Compression

RLTP Settings

Transaction Size: 10 messages

Response Timeout: 60 seconds

Acknowledge Timeout: 900 seconds

a.

To compress the messages during transfer to save bandwidth, select the Allow Compression option. Note that for syslog-ng Agent to actually use compression, the following points must be met.

- The Server > Advanced Options > Allow Compression option must be enabled.
- You must use SSL and/or RLTP to send messages to the logserver (that is, at least one of the Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP) or Use TLS encryption options must be enabled.
- The logserver must be configured to enable compression. If the logserver is syslog-ng PE the proper *allow-compress()* option must be enabled in the source. If the logserver is syslog-ng Store Box, enable the Log > Sources > Allow compression option. Note that to send compressed messages to syslog-ng Store Box, you must use the RLTP™ protocol (for details, see the syslog-ng Documentation page).

b. Change the following options if necessary:

> NOTE:
>
> Do not adjust or modify the following settings unless you know exactly what you are doing.

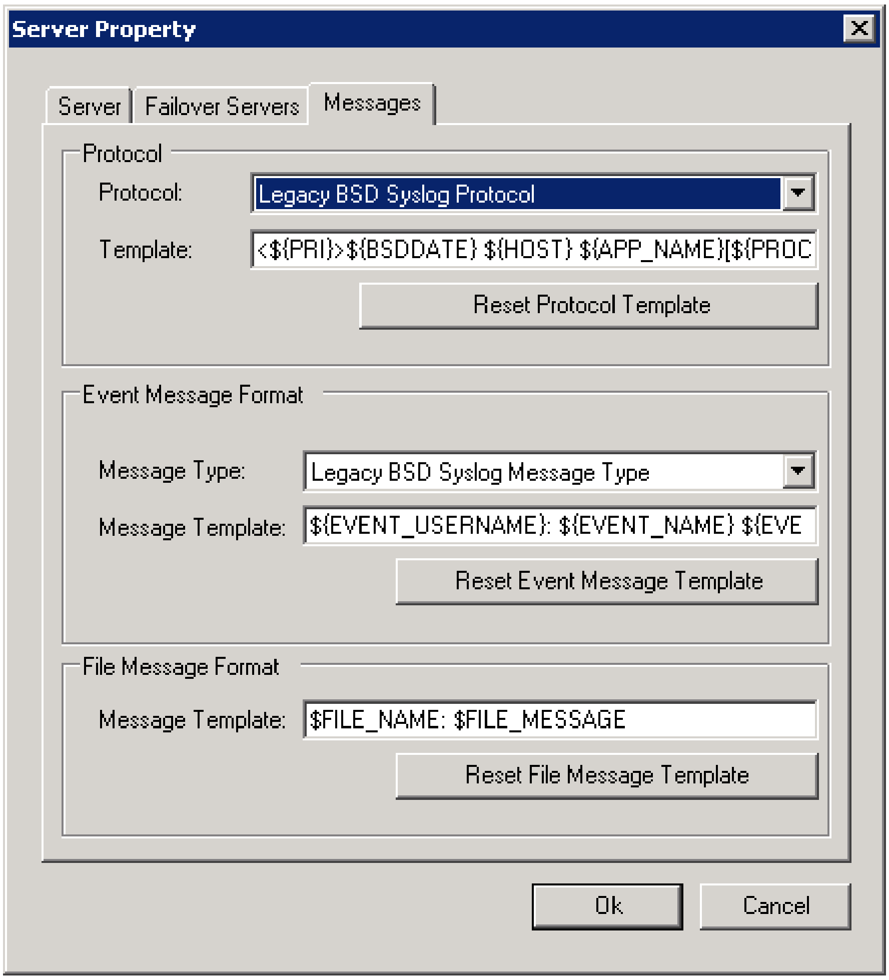
- Transaction Size: The number of messages sent before waiting for acknowledgement from the server.
- Response Timeout: After not receiving any message in the given timeframe, syslog-ng Agent terminates the connection with the server.
- Acknowledge Timeout: After not receiving any reply to the messages in the given timeframe, syslog-ng Agent terminates the connection with the server.

c. Click OK.

5. On Messages tab, select the protocol used to transfer log messages and press Reset to apply the selected template. The following protocol templates are available (for details on the default templates and on customizing the message format, see Chapter 8, *Customizing the message format*):

- Legacy BSD Syslog Protocol: Use the legacy BSD-syslog protocol specified in RFC3164. This option uses the following message template: *<${PRI}>${BSDDATE} ${HOST} ${MSGHDR}${MESSAGE}*. Within the message part, syslog-ng Agent replaces CRLF with 2 spaces and TAB character with 1 space.

Figure 4.4. Legacy BSD Syslog Protocol



Protocol

Protocol: Legacy BSD Syslog Protocol

Template: <${PRI}>${BSDDATE} ${HOST} ${APP_NAME}[${PROC

Event Message Format

Message Type: Legacy BSD Syslog Message Type

Message Template: ${EVENT_USERNAME}: ${EVENT_NAME} ${EVE

File Message Format

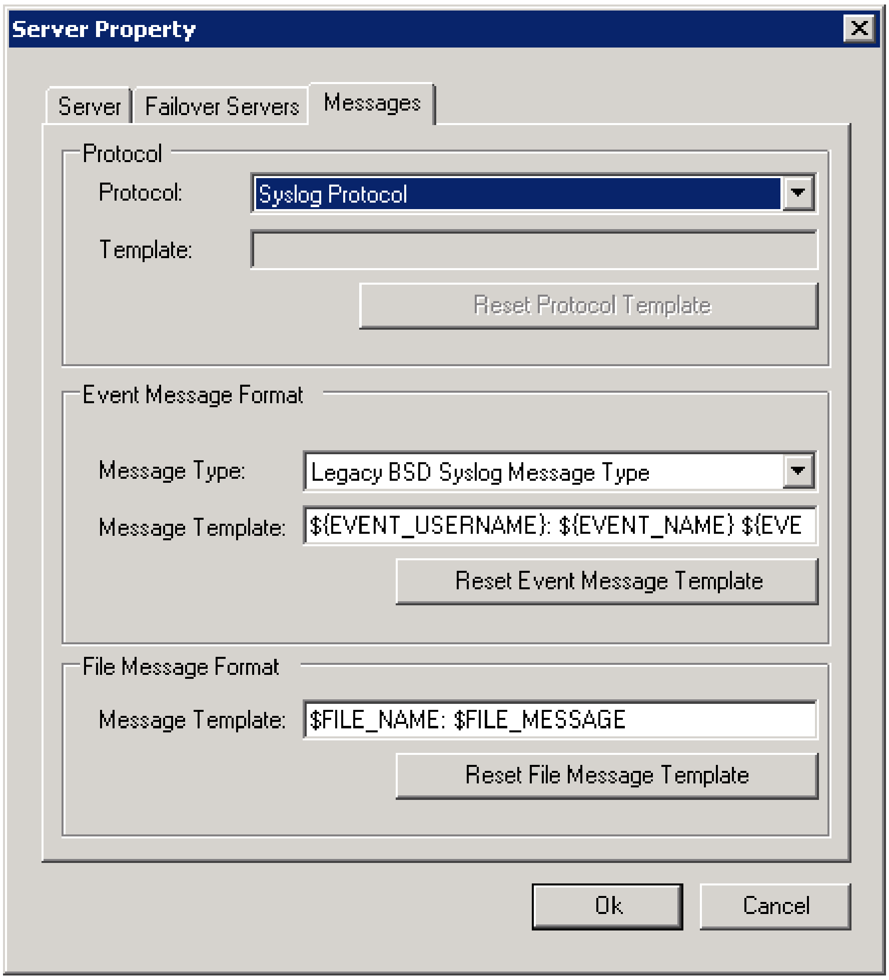
Message Template: $FILE_NAME: $FILE_MESSAGE

Example 4.1. Legacy BSD Syslog Protocol log

```
<134>Oct 04 14:45:33 zts-win019.ztswin2008dom.balabit
Microsoft-Windows-Eventlog[2880]: ZTSWIN2008DOM\balabit: System
Microsoft-Windows-Eventlog: [Information] The Application log
file was cleared. (EventID 104)
```

- Syslog Protocol: Use the new IETF-syslog protocol specified in RFC 5424-5426. This is the default setting.

Figure 4.5. Syslog Protocol



Protocol

Protocol: Syslog Protocol

Template:

Event Message Format

Message Type: Legacy BSD Syslog Message Type

Message Template: ${EVENT_USERNAME}: ${EVENT_NAME} ${EVE

File Message Format

Message Template: $FILE_NAME: $FILE_MESSAGE

When using the IETF-syslog protocol to transfer Eventlog messages, the syslog-ng Agent application includes the macros (name-value pairs) in the SDATA part of the log message by default. This includes every available Event macro, except *EVENT_CONTAINER_COUNTER*, *EVENT_DATA*, *EVENT_GLOBAL_COUNTER*, *EVENT_MSG (EVENT_MESSAGE)*, *EVENT_MSG_XML (EVENT_MESSAGE_XML)*. Macros that do not have a value will not be included in the message.

```
499 <132>1 2010-09-28T12:02:30+02:00 zts-win004.ztswin2003dom.balabit
testapp 1220 - [win@18372.4 EVENT_ID="1000" EVENT_NAME="Application"
EVENT_REC_NUM="1673" EVENT_SID="S-1-5-21-3460971693-970282485-
2299281428-1001" EVENT_SID_TYPE="User" EVENT_SOURCE="testapp" EVENT_
TYPE="Warning" EVENT_USERNAME="ZTS-WIN004\\balabit"][meta
sequenceId="1" sysUpTime="1"] ZTS-WIN004\balabit: Application
testapp: [Warning] test message (EventID 1000)
```

NOTE:

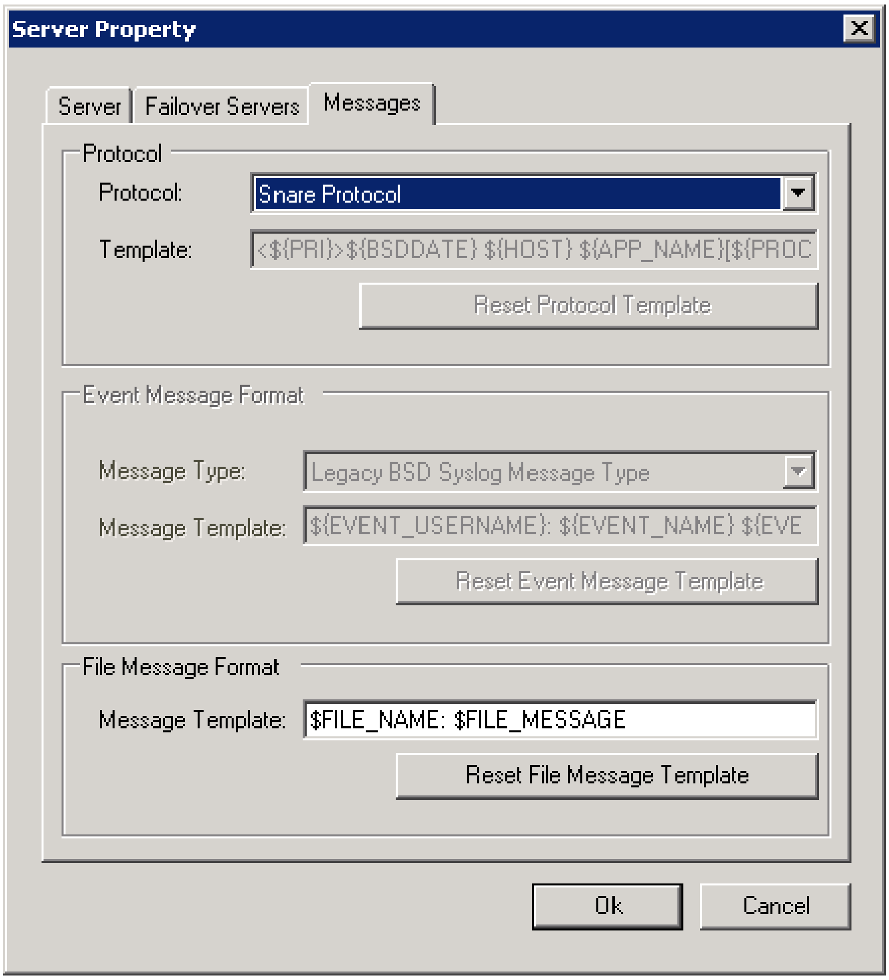
> The names of SDATA fields must be in the following format: name@<private enterprise number>, for example, *mySDATA-field@18372.4*. (18372.4 is the private enterprise number of BalaBit IT Security, the developer of syslog-ng Agent for Windows.)
>
> - Messages received from eventlog sources include the *win@18372.4* SD-ID. For example, on your syslog-ng PE server you can refer to message fields like: *${.SDATA.win@18372.4.EVENT_SOURCE}*
> - Messages received from file sources include the *file@18372.4* SD-ID. For example, on your syslog-ng PE server you can refer to message fields like: *${.SDATA.file@18372.4.name}*

To include only the data mandated by RFC5424, disable Include Eventlog message metadata as SDATA. To do this, navigate to Destinations > Destination Global Settings, select Enable and deselect Include Eventlog message metadata as SDATA. For example, only the following data will be included in the message:

```
[meta sequenceId="value" sysUpTime="value"]
```

- Snare Protocol: Send log messages in a format compatible with the Snare log monitoring tool.

Figure 4.6. Snare Protocol



Server Property

Server | Failover Servers | Messages

Protocol

Protocol: Snare Protocol

Template: <${PRI}>${BSDDATE} ${HOST} ${APP_NAME}[${PROC

Reset Protocol Template

Event Message Format

Message Type: Legacy BSD Syslog Message Type

Message Template: ${EVENT_USERNAME}: ${EVENT_NAME} ${EVE

Reset Event Message Template

File Message Format

Message Template: $FILE_NAME: $FILE_MESSAGE

Reset File Message Template

Ok | Cancel

NOTE:

Snare is a tab-separated message format. Within the message part, agent replaces CRLF with 2 space, TAB character with 1 space.

You cannot modify the log format if you have selected this protocol.

Example 4.2. Snare log

```
<134>Oct 06 13:49:41 zts-win019.ztswin2008dom.balabit
MSWinEventLog   1   Application 1   Wed Oct 06 13:49:41 2010
1   syslog-ng Agent   S-1-5-21-551780264-1021859348-3425375765-
1003   User    Information zts-win019.ztswin2008dom.balabit
None        Application started 1
```

NOTE:

Selecting the Syslog Protocol option is identical to using the *syslog* driver in the Linux/Unix version of syslog-ng. Similarly, selecting Legacy BSD Syslog Protocol is equivalent to the *tcp* driver of syslog-ng.

Changing to the Legacy BSD Protocol does not automatically restore the original template. To do so, click Reset Protocol Template after modifying the protocol.

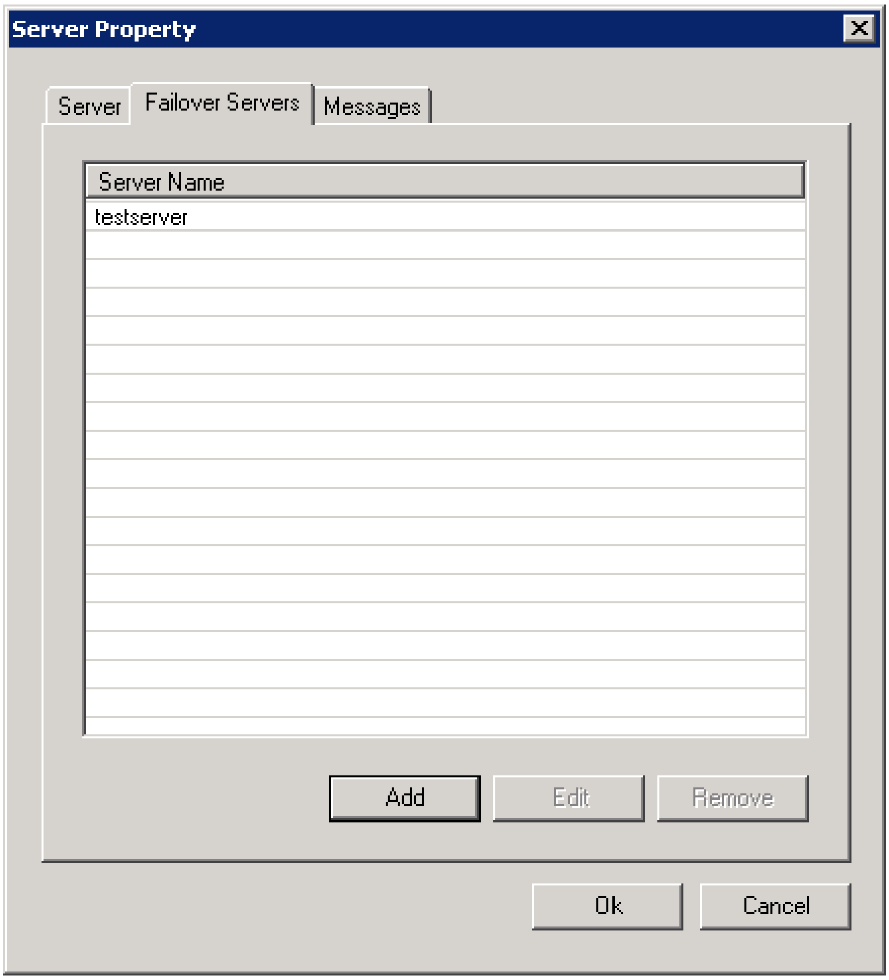
6. If needed, modify the template of the messages. The format of the messages can be different for the eventlog and the file sources.

   CAUTION:

   The maximal length of the template is 1023 characters.

7. If you have a backup server that can accept log messages if the primary log server becomes unavailable, select the Failover Servers tab, click Add, and enter the hostname or the IP address of the backup log server into the Server Name field. Repeat this step if you have more than one backup servers.

   Figure 4.7. Failover Servers



8. If you want to send the log messages to more than on server in parallel, so that every server receives every message, repeat Steps 3-4 to add the other destination servers. These servers may have failover servers as well.

9. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

10. *Optional Step*: If the host running syslog-ng Agent is sometimes logged in into a domain, sometimes not, then its hostname might change depending on its actual domain membership. This can cause that the hostname appearing in the syslog messages depends on the domain membership of the host. To avoid this situation, select syslog-ng Agent Settings > Global Settings > Hostname > Use FQDN. That way syslog-ng Agent resolves the name of its host from the DNS server, and uses the resolved FQDN in the syslog messages.

Procedure 4.2. Limiting the rate of messages

Purpose:

The syslog-ng Agent can control the rate of messages (message per second) sent to the central server. That way sudden message-bursts can be avoided, and the load of the server is decreased.

To limit the number of messages sent to a destination, complete the following steps:

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Destinations.
3. Select Destination Global Settings. To limit the number of messages that the syslog-ng Agent sends to the server per second, enter the desired limit into the Throttle field. By default (*0*), the syslog-ng Agent does not limit the number of messages sent.

   The throttling parameter applies to the total number of messages sent, not to every source independently. The same value applies to every destination.
4. Click OK. To activate the changes, restart the syslog-ng Agent service.

Procedure 4.3. Sending MARK messages

Purpose:

If there are no new messages that have to be sent to the destination server, the syslog-ng Agent for Windows application automatically sends a MARK message every ten minutes to notify the server that the connection is still active. The exact format of the MARK message depends on the protocol:

Legacy BSD protocol (RFC3164):

```
<46>Apr 18 11:34:21 <hostname> -- MARK --
```

Snare protocol:

```
<46>Apr 18 11:34:21 <hostname> -- MARK --
```

Syslog protocol (RFC5424):

```
82 <46>1 2013-04-23T10:51:29+02:00 <hostname> - - - [meta sequenceId="3"] -
- MARK --
```

To change how often the syslog-ng Agent sends these messages, complete the following steps.

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings and double-click on Global Settings.
3. Select Enable, then select Mark Mode Options.
4. Set the frequency of MARK messages that the syslog-ng Agent for Windows application sends.

- *Never*: Do not send MARK messages.
- *When destination idle*: Send MARK messages only if there were no other messages sent to the destination during the specified period.
- *Periodically*: Send MARK messages every time the specified period expires.

5. Set the time between two MARK messages in the The number of seconds between two MARK messages. By default, this is 600 seconds (10 minutes).
6. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Flow-control in syslog-ng Agent for Windows

Starting with version 5 LTS, the flow-control feature of syslog-ng Premium Edition is automatically enabled for the destinations. Using flow-control means that the syslog-ng Agent will stop reading messages from the sources if the destination cannot accept them (for example, because of a network error).

To enable or disable flow-control for a destination, select syslog-ng Agent Settings > Destinations, double-click on the destination, then select Server > Enable flow-control.

NOTE:

You cannot disable flow-control when using the Reliable Log Transfer Protocol™ (RLTP™).

NOTE:

The flow-control of syslog-ng Agent 5 LTS replaces the Primary Server option of earlier versions.

Flow-control and multiple destinations

Using flow-control on a source has an important side-effect if the messages of the source are sent to multiple destinations. If flow-control is in use and one of the destinations cannot accept the messages, the other destinations do not receive any messages either, because syslog-ng stops reading the source. For example, if messages from a source are sent to two remote servers, and the network connection to one of the servers becomes unavailable, neither servers will receive any messages.

NOTE:

Creating separate log paths for the destinations that use the same flow-controlled source does not avoid the problem.

Configuring message sources

The syslog-ng Agent for Windows application can read messages from eventlog containers and text files. The following sections explain how to configure these message sources.

- For details on how to forward messages from eventlog containers, see the section called “Eventlog sources”.
- For details on how to forward messages from plain text log files, see Procedure 5.5, “Managing file sources”.
- Some global settings can apply to both types of sources, these are described in Procedure 5.7, “Configuring global settings”.

Eventlog sources

The syslog-ng Agent for Windows application can collect messages from the standard Windows eventlog containers, as well as from custom containers. The agent automatically forwards the messages from three standard eventlog containers (*`Application, Security, System`*). To enable or disable these sources, or to add custom eventlog containers, complete the following steps:

NOTE:

The syslog-ng Agent for Windows sends its own log messages into the *`Application`* eventlog container.

The agent stores the ID of the last message sent to the destination server, so if the agent is not operating for a time (for example it is restarted), then it starts reading messages from the last stored message ID, sending out all the new messages.

CAUTION:

If an eventlog container becomes corrupt, the agent will stop processing the event source. A log message (*`Eventlog file is corrupt`*) is sent directly to the log server to notify about the error.

CAUTION:

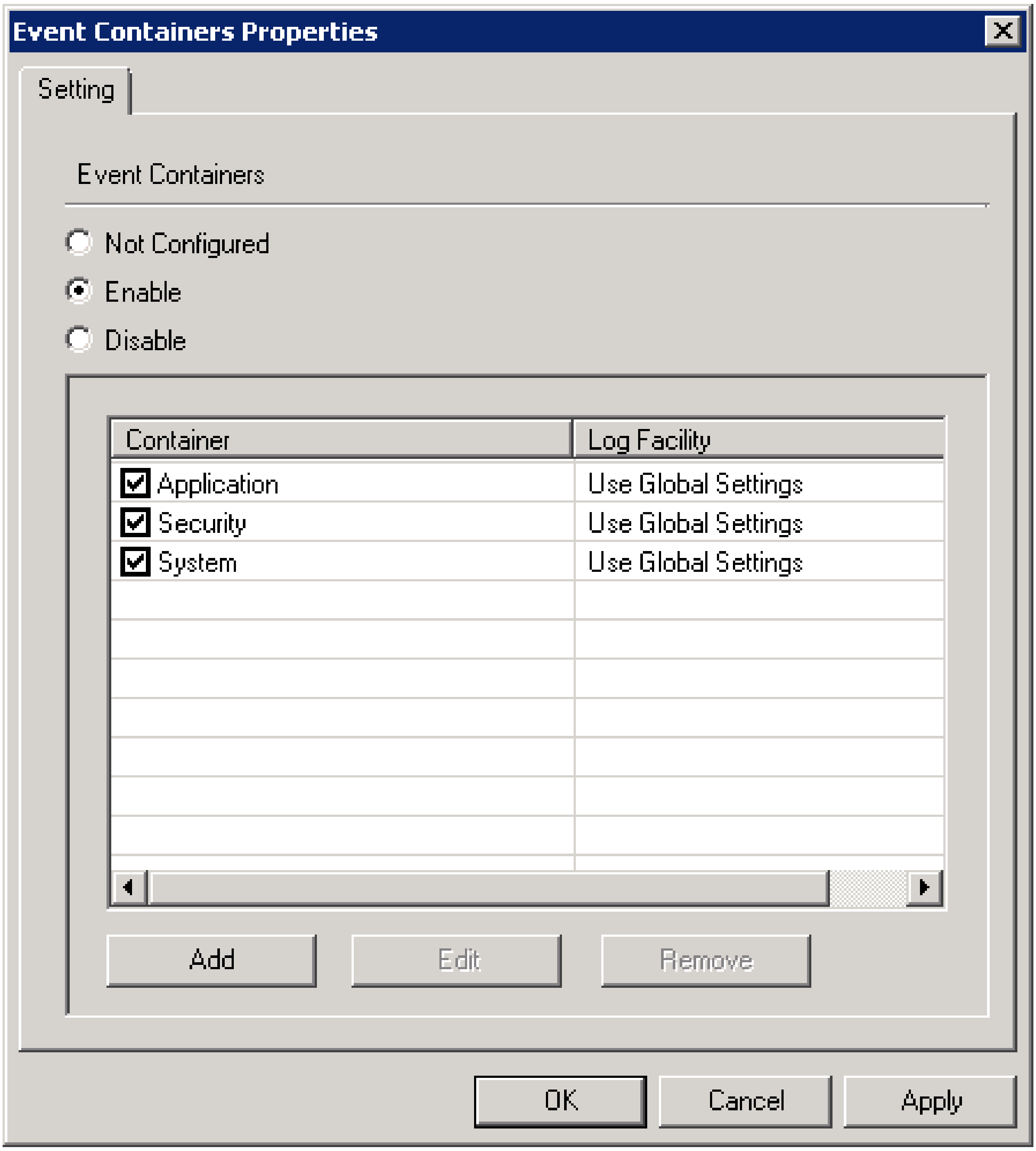
Hazard of data loss! It is not recommended to setup archiving for the event container. It is possible to lose logs if there are non-processed events in the event container when the archiving is started. Windows closes and renames the event container and starts a new one regardless of any reading applications.

To prevent this, enable overwrite events when needed mode in the Windows Event Viewer with the following conditions:

- **The messages are not generated faster than the agent's processing speed.**
- **There is enough window between the first and the last events for planned agent stops. Ensure that new events will not overwrite the event last read by the agent during agent stop.**

Procedure 5.1. Managing eventlog sources

Figure 5.1. Managing eventlog sources



Event Containers Properties

Setting

Event Containers

○ Not Configured

● Enable

○ Disable

Container	Log Facility
☑ Application	Use Global Settings
☑ Security	Use Global Settings
☑ System	Use Global Settings

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Eventlog Sources, and double-click on Event Containers.
3.
    - To disable sending messages from an eventlog container, deselect the checkbox before the name of the container.
    - To modify the log facility associated with the messages of the container, select the container, click Edit, and select the log facility to use in the Log Facility field.
4. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Procedure 5.2. Adding eventlog sources

Purpose:

To forward the messages from an eventlog container to your central log server, complete the following steps.

Prerequisites:

You need to know the name of the eventlog container. If you do not know the name of the container, see Procedure 5.3, "Determining the name of a custom eventlog container" or Procedure 5.4, "Determining the name of a custom eventlog container on Windows XP, or Server 2003".

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Eventlog Sources, and double-click on Event Containers.
3.

    Click Add, and enter the name of the container into the Event Container Name field. You can use the `*` and `?` wildcard characters in the name of the container. That way you can handle multiple eventlog containers in a single source.

    If you use wildcards in the name of the eventlog container, note the following points:

    - If none of the existing eventlog containers match the pattern, the syslog-ng Agent will send a warning message into the debug log. For details on enabling debug logs, see the section called "Debugging syslog-ng Agent".
    - The syslog-ng Agent application checks for new eventlog containers only when it starts or restarts. If a new eventlog container is created with a name that matches the pattern of an eventlog source, restart the syslog-ng Agent service.

    ⚠ **CAUTION:**

    Hazard of data loss! If you use wildcards in multiple eventlog source names, make sure that only one pattern matches every container name. If two eventlog sources match the same container, syslog-ng Agent might ignore the messages of the eventlog container.

4. Click Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

   Expected result:

   The syslog-ng Agent application starts sending new messages from the newly added eventlog container. Note that the syslog-ng Agent will send existing messages from the eventlog container only if you have selected the Read Old Records option.

Procedure 5.3. Determining the name of a custom eventlog container

Purpose:

To determine the name of a custom eventlog container, complete the following steps.

Steps:

1. Open the Event Viewer application.
2. Select the custom container you are looking for (for example `DNS Server`).
3. Right click on the container and select Properties.
4. The name of the container is the name of the file (without the extension) displayed in the Logname field (for example for `C:\WINDOWS\system32\winevt\Logs\Security.evtx` it is `Security`).
5. Use this name as the name of the custom eventlog container during the procedure described in Procedure 5.1, "Managing eventlog sources".

   > NOTE:
   >
   > Some containers are not real containers, but show selected messages collected from multiple containers. To forward such messages to the syslog-ng server, you have to find out which real containers are displayed in the container, and add them to the configuration of the syslog-ng Agent.
   >
   > Some containers have the `%4` characters in their names. When adding these to the syslog-ng Agent, replace `%4` with the `/` (slash) character. For example write `microsoft-windows-bits-client/analytic` instead of `microsoft-windows-bits-client%4analytic`.
   >
   > If you are sending old messages to the server as well, the syslog-ng Agent will not send the very first message stored in the container. This is a bug in the Windows API.

Procedure 5.4. Determining the name of a custom eventlog container on Windows XP, or Server 2003

Purpose:

To determine the name of a custom eventlog container on Windows XP, or Server 2003, complete the following steps.

Steps:

1. On the client host select Start > Run > regedit.
2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\. The custom containers are listed here. For example, the following are valid container names: *`DFS Replication`*, *`File Replication Service`*, *`DNS Server`*.

3. Use this name as the name of the custom eventlog container during the procedure described in Procedure 5.1, “Managing eventlog sources”.

Procedure 5.5. Managing file sources

Purpose:

The syslog-ng Agent for Windows application can collect log messages from text files. It can process messages spanning multiple lines, and supports the use of wildcards (***, *?*) in filenames to be able to follow log files that are automatically rotated. Note that every line of the file that ends with a newline character is considered a separate message. However, if a file contains only a single line that does not end with a newline character, syslog-ng Agent will not process the line.

To configure file sources, complete the following steps:

> ⚠ **CAUTION:**
>
> **Files used as file sources must reside locally on the host the syslog-ng Agent application is running on. Files located on network shares are not supported, because the syslog-ng Agent for Windows application is running as a local service and does not have the privileges to access network shares.**

> ⚠ **CAUTION:**
>
> **If an application deletes a log file, the application must ensure that syslog-ng Agent had enough time to forward the messages from the file to the central server to avoid losing messages.**

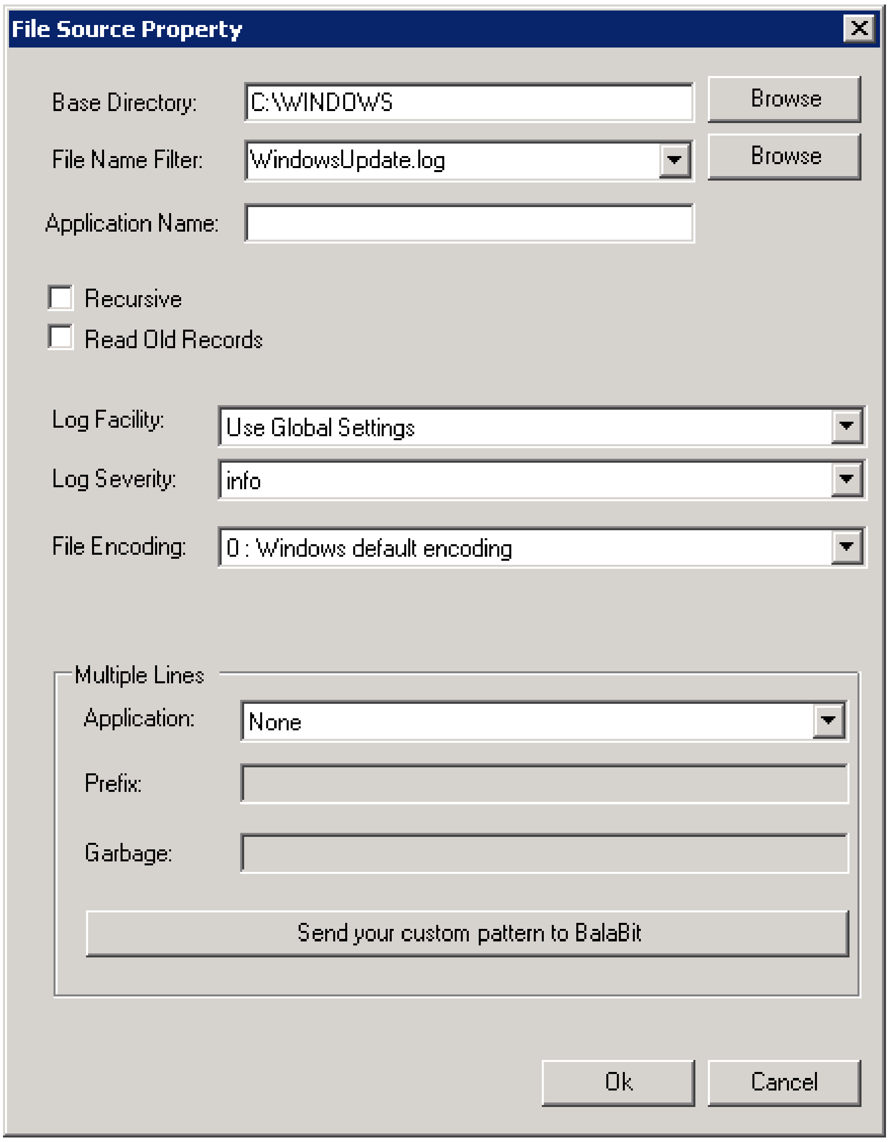
Example 5.1. Collecting the logs of multiple applications from a single folder

If two applications log into the same folder (for example `C:\logs`), you have to create two file sources. For example, if the name of the log files is *`application1-*.log`* and *`application2-*.log`*, respectively, then create two file sources with the `C:\logs` Base Directory, but with different File Name Filter: *`application1-*.log`* and *`application2-*.log`*, respectively.

If other applications log into the `C:\logs` folder, add a separate expression for each application.

By default, the syslog-ng Agent will send every message to the server that arrives into any of the monitored log files.

Figure 5.2. Managing file sources



File Source Property

Base Directory: C:\WINDOWS

File Name Filter: WindowsUpdate.log

Application Name:

□ Recursive

□ Read Old Records

Log Facility: Use Global Settings

Log Severity: info

File Encoding: 0 : Windows default encoding

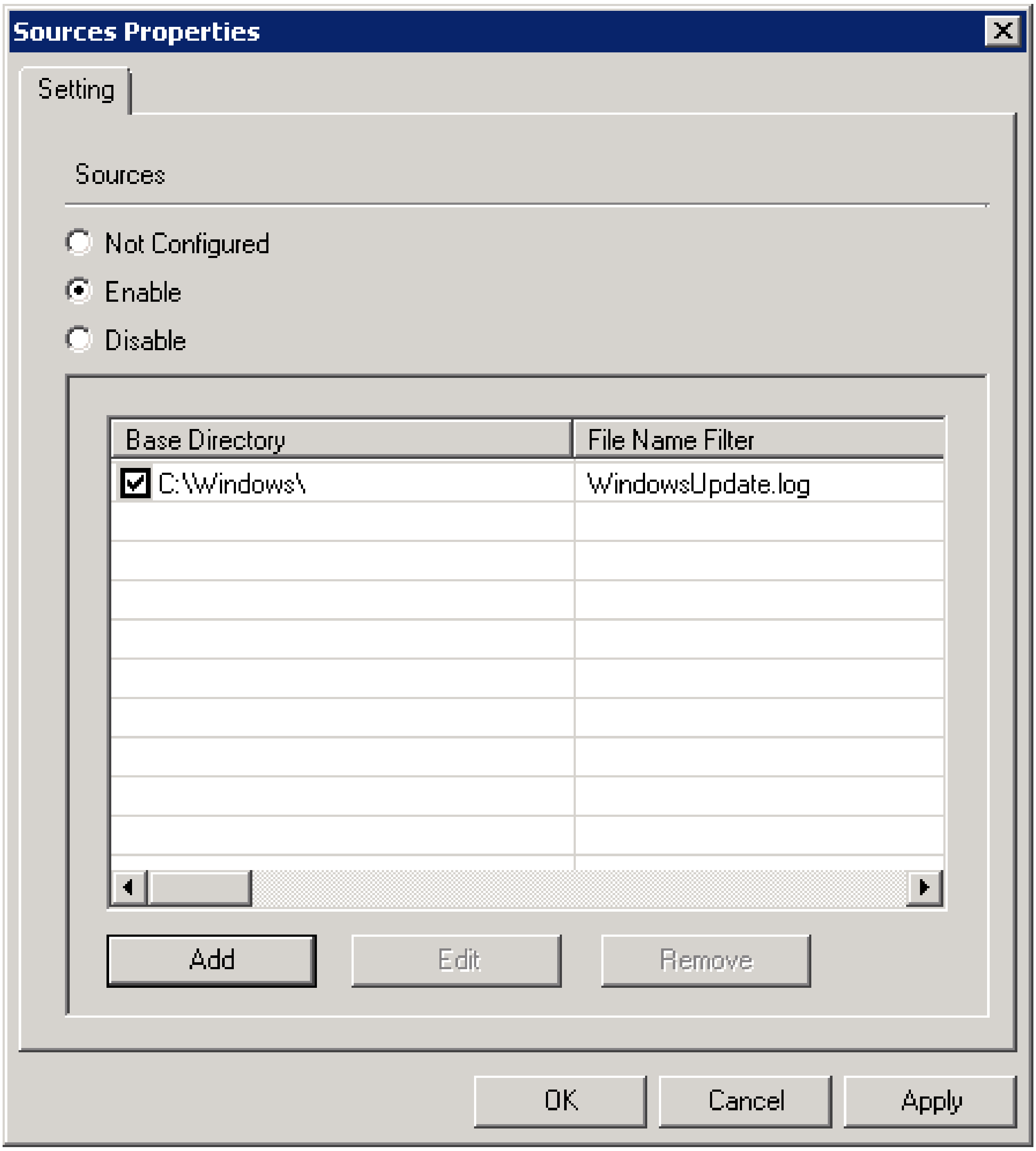
Multiple Lines

Application: None

Prefix:

Garbage:

Figure 5.3. Sources properties



Sources Properties

Setting

Sources

○ Not Configured

● Enable

○ Disable

Base Directory	File Name Filter
☑ C:\Windows\	WindowsUpdate.log

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > File Sources, double-click on Sources, and check the Enable option.
3. Select Add > Browse, and select the folder containing the log files in the Base Directory field. Select or enter the name and extension of the log files in the File

Name Filter field. Wildcards can be used. The syslog-ng Agent will forward log messages from every file that is located in this folder and has a name that matches the filter expression.

> ⚠ **CAUTION:**
>
> **If you use wildcards in multiple file sources, make sure that the files and folders that match the wildcards do not overlap. That is, every file and folder should belong to only one file source. Monitoring a file from multiple wildcard sources can lead to data loss.**

> ⚠ **CAUTION:**
>
> **Files used as file sources must reside locally on the host the syslog-ng Agent application is running on. Files located on network shares are not supported, because the syslog-ng Agent for Windows application is running as a local service and does not have the privileges to access network shares.**

> TIP:
>
> When specifying the Base Directory, you can use the environment variables of Windows, for example *`%WINDIR%`*, *`%SYSTEMROOT%`*, *`%PROGRAMFILES%`*, and so on.

> ⚠ **CAUTION:**
>
> **Note that when managing members of a domain, the selected path must be available on the domain members, for example `C:\logs` must be available on the client hosts and not on the domain controller.**

4.
   - To send messages from the files located in the subfolders of the folder set as Base Directory, select the Recursive option.
   - To change the log facility or the log severity associated to the file source, select the desired facility or priority from the Log Facility or Log Severity fields, respectively.

   > NOTE:
   >
   > Significant changes to the settings of a file source can cause the syslog-ng Agent to resend the entire contents of the matching files. This means that log messages already sent earlier to the syslog-ng server may be resent and thus duplicated in the server logs. Configuration changes that can result in such behavior are:
   >
   > - changing the Base Directory,
   > - changing filter options,
   > - changing the Recursive option.

5. *Optional Step*: By default, the syslog-ng Agent application starts sending messages from the beginning of the file. If you only want to send the messages that are newly added to the file, deselect the Read Old Records option.

> NOTE:
>
> Be careful when Read Old Records is disabled. If a new file(s) is created while syslog-ng Agent is stopped, the content of this file will not be forwarded, only the new records. To avoid message loss, never disable Read Old Records in the configuration.

6. *Optional Step*: By default, the operating system notifies the syslog-ng Agent application when an application modifies a logfile. However, in some cases this does not happen, because the file-monitoring API of Windows does not notice that the file has changed, for example, when monitoring logfiles of the Windows DHCP service.

   In such case, select the Force Directory Polling option. Note that enabling this option decreases the performance of syslog-ng Agent if you monitor lots of logfiles.

7. By default, the syslog-ng Agent application assumes that the source files are encoded using the default windows ANSI code page, specific to the locale of the host. If the files have a different encoding, select it from the File Encoding field. Note that the log messages are sent to the destinations using UTF-8 encoding.

8. If a log messages in the log file consists of multiple lines, that is, the log messages contain newline characters, configure syslog-ng Agent to process the related lines as a single message.

   The syslog-ng Agent application can automatically handle Apache Tomcat Catalina and Oracle SQL log messages. To process such messages, select the name of the application from the Multiple Lines > Application field. Note that the timestamp of Tomcat log messages depends on the locale of the host. The syslog-ng Agent for Windows application automatically removes the last CRLF control character from multi-line messages.

   To process multi-line log messages of a different application, complete the following steps.

   a. Select Multiple Lines > Application > Custom, and set the Multiple Lines > Prefix and optionally the Multiple Lines > Garbage fields.

   b. Specify a string or regular expression that matches the beginning of the log messages in the Multiple Lines > Prefix field. If the Prefix option is set, the syslog-ng Agent ignores newline characters from the source until a line matches the regular expression again, and treats the lines between the matching lines as a single message.

      > NOTE:
      >
      > Use as simple regular expressions as possible, because complex regular expressions can severely reduce the rate of processing multi-line messages.

   c. Use the Multiple Lines > Garbage option when processing multi-line messages that contain unneeded parts between the messages. Specify a string or regular expression that matches the beginning of the unneeded message parts. If the

Garbage option is set, the syslog-ng Agent ignores lines between the line matching the Garbage expression and the next line matching Prefix.

When receiving multi-line messages from a source when the Garbage option is set but no matching line is received between two lines that match Prefix, the syslog-ng Agent application will continue to process the incoming lines as a single message until a line matching Garbage is received.

> ⚠ **CAUTION:**
>
> **If the Garbage option is set, the syslog-ng Agent application discards lines between the line matching the Garbage and the next line matching Prefix expressions.**

d. *Optional Step*: After creating and testing a custom pattern, please consider sending your pattern to One Identity so we can include it in a future version of syslog-ng Agent. To share your pattern with One Identity and other syslog-ng Agent users, click Multiple Lines > Send custom pattern to BalaBit. Your e-mail application will open, with an e-mail containing the application name and the pattern.

9. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Procedure 5.6. Managing the internal source

Purpose:

All messages generated internally by syslog-ng Agent for Windows application use the internal source. The syslog-ng Agent for Windows application can forward messages originating from the internal source to certain destinations. To configure the internal source, complete the following steps:

Steps:

1. Select syslog-ng Agent Settings and double-click on Global Settings.
2. Enable Global Settings.
3. Navigate to Internal Messages.
4. Select the internal message types to forward to the Application event container, or to Remote destinations (meaning all servers that are configured as normal TCP destinations). The message types correspond to the respective message severities. The default setting is internal error and warning messages forwarded to Application event container, and info messages forwarded to Remote destinations.

Only the selected message types will be forwarded.

> ⚠ **CAUTION:**
>
> **If the same message types are selected for both the Application event container and the Remote destinations, and the application event container is also a source, messages can be duplicated.**

> NOTE:
>
> These options will be inherited from GPOs (Group Policy Objects). For details, see the section called "Domain versus local settings". They can also be exported/imported from an XML configuration also.

5. Click Apply.

Procedure 5.7. Configuring global settings

Purpose:

The syslog-ng Agent for Windows application has some global settings that can apply to both eventlog and file sources. To configure the global settings, complete the following procedure:

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings and double-click on Global Settings.
3. Set the default log facility associated to the messages.
4. By default, the filters and regular expressions (see Chapter 7, *Filtering messages*) used in the message filters are case-sensitive. To make them case-insensitive, select the Regular Expressions Ignore Case or the Filters Ignore Case options, or both.

   > NOTE:
   >
   > The Regular Expressions Ignore Case option makes the `Message Contents` filter case-insensitive for both file and eventlog sources. The Filters Ignore Case option makes the `Computers`, `Sources and Categories`, and the `Users` filter case-insensitive.

5. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Procedure 5.8. Configuring the hostname format

Purpose:

The syslog-ng Agent for Windows application can send the hostname macro in different format types (FQDN or short hostname), depending on the domain membership of the host, and the source of the message (eventlog or file). The hostname settings will affect all logs originating from file sources, eventlog sources, as well as MARK messages and internal messages of syslog-ng Agent, for example, start/stop messages.

To prevent using two host licenses from a trusted source, use the same hostname type in every outgoing message.

To determine the hostname, syslog-ng Agent queries the short hostname of the machine at startup, and then attempts to resolve it from the DNS server to receive the FQDN. If DNS resolution is not possible, the hostname will be the short hostname.

> NOTE:
>
> The syslog-ng Agent will never rewrite hostnames.

To configure the hostname format globally, complete the following steps:

Steps:

1. Select syslog-ng Agent Settings and double-click on Global Settings.
2. Enable Global Settings.
3. Navigate to Hostname.
4. Select the hostname type to use globally.
   - To use only the short hostname in the *$HOST* macro of the outgoing message, select Use only hostname. This is the default setting.
     - In case of file sources, MARK messages and internal messages of syslog-ng Agent the outgoing hostname will be the short hostname of the machine.
     - In case of eventlog sources, the hostname will be the short hostname of the event message (for example *mypc*), or syslog-ng Agent will cut the domain name from the FQDN and use the short hostname part (for example *mypc.mycompany.local* becomes *mypc*).
   - To use FQDN (*hostname.domain_name*) in the *$HOST* macro of the outgoing message, select Use FQDN.
     - In case of file sources, MARK messages and internal messages of syslog-ng Agent, the hostname will be the FQDN of the machine.

       > NOTE:
       >
       > If there is no DNS server, or the DNS server cannot resolve the hostname, only the simple hostname of the machine will be used.
     - In case of eventlog sources, if the hostname of event message is already an FQDN, syslog-ng Agent will use it as the hostname (for example *mypc.mycompany.local* will be used as such). If this is not an FQDN, syslog-ng Agent will try to resolve this hostname and use the received FQDN as hostname (for example *mypc* becomes *mypc.mycompany.local*).

       > NOTE:
       >
       > If there is no DNS server, or the DNS server cannot resolve the hostname, only the short hostname of the event message will be used.

- To use a custom domain name that will be appended after the short hostname to receive the FQDN, select Use hostname with custom domain name and enter the domain name to append to the short hostname in the field below. This option affects every outgoing message: eventlog sources, file sources, MARK messages and internal messages of syslog-ng Agent.
    - If the hostname is a short hostname, the custom domain name will be appended after the hostname (for example *mypc* becomes *mypc.customcompany.local*).
    - If the hostname is an FQDN, the domain name part will be replaced with the custom domain name (for example if the FQDN in the forwarded message is *mypc.mycompany.local* and the custom domain name is *customcompany.local*, the hostname in the outgoing message becomes *mypc.customcompany.local*).

> NOTE:
>
> The hostname still can be different in the outgoing messages if in the eventlog message, the hostname in the event is different from the machine hostname:
>
> - In case of a forwarded eventlog: the original machine hostname will be the hostname.
> - The machine hostname is different from what the DNS server provides (if there is a DNS server and it can resolve the hostname).

5. To use lower-case characters in every hostname, enable Convert to lower-case. This is enabled by default. When disabled, mixed lower-case and upper-case characters (if there is any) will be used in hostnames. This option affects every outgoing message: eventlog sources, file sources, MARK messages and internal messages of syslog-ng Agent.
6. Click Apply.

Procedure 5.9. Disabling sources and filters globally

Purpose:

Filters and sources can be disabled globally as well. Disabling filters or sources means that the syslog-ng Agent ignores the disabled settings: that is, if the file sources are disabled, the agent does not send the messages from the files to the server. For details, see the following procedure.

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. - To disable eventlog sources, select syslog-ng Agent Settings, right-click on Eventlog Sources, then select Properties > Disable.
   - To disable file sources, select syslog-ng Agent Settings, right-click on File Sources, then select Properties > Disable.

    - To disable eventlog filters, select syslog-ng Agent Settings > Destinations, right-click on Global Event Filters, then select Properties > Disable.
    - To disable file filters, select syslog-ng Agent Settings > Destinations, right-click on Global File Filters, then select Properties > Disable.
3. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Using TLS-encrypted connections with syslog-ng Agent

When the syslog-ng Premium Edition (syslog-ng PE) server is configured to use mutual authentication, it requests a certificate from the syslog-ng PE clients. The syslog-ng Agent for Windows application can automatically show the requested certificate to the server when the connection is established, provided it is available in the Personal Certificates store of your Local Computer (MMC > Certificates > Computer Account > Local Computer > Personal Certificates).

To import this certificate, use the Certificate Import Wizard. For details, see Importing certificates with the Microsoft Management Console.

> NOTE: The syslog-ng Agent for Windows application only supports this certificate import method for the Windows Certificate Store authentication method.

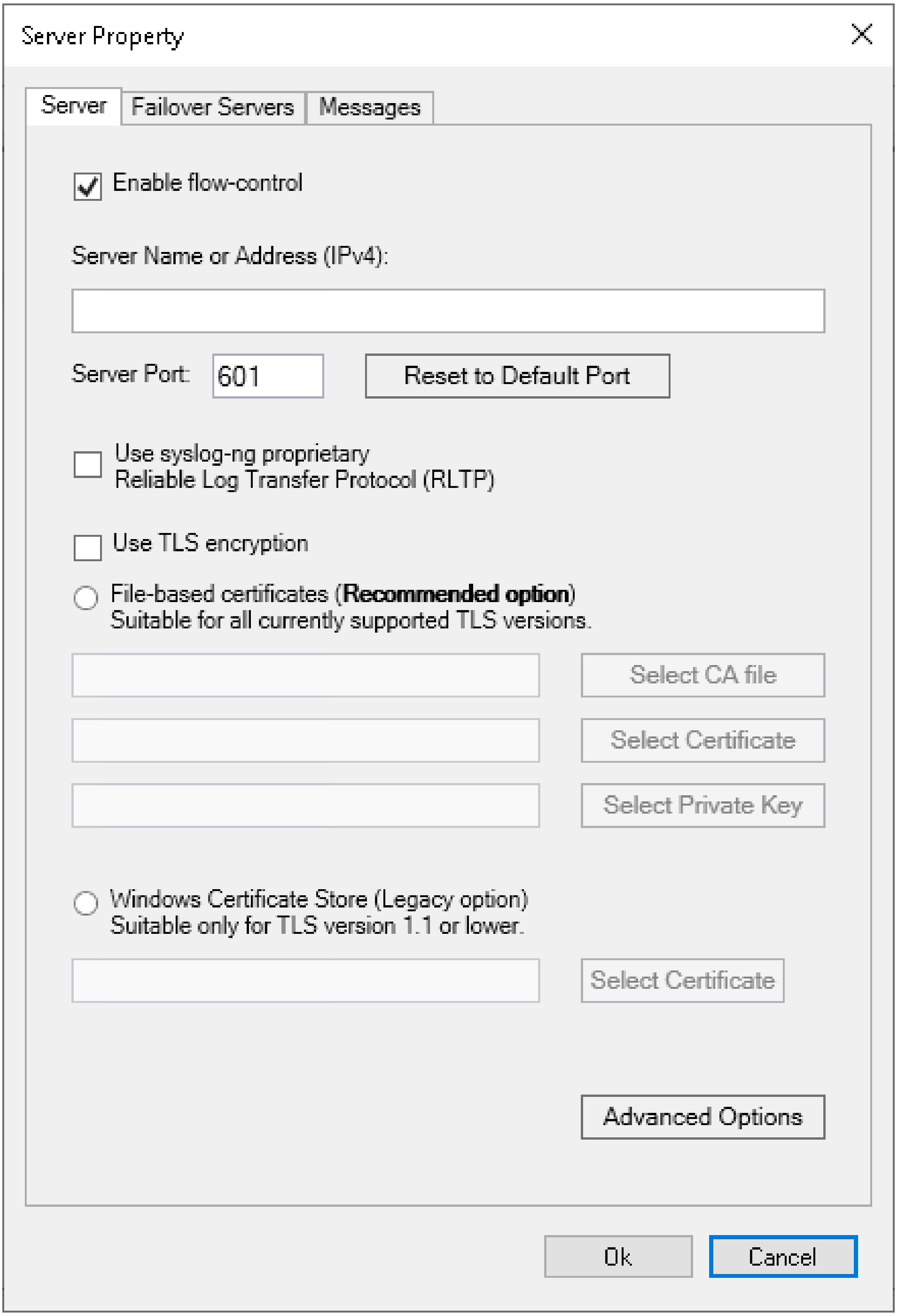
> NOTE: If a certificate revocation list (CRL) is available in the Local Computer > Personal Certificates store, syslog-ng Agent for Windows verifies that the certificate of the syslog-ng PE server is not on this list.

Authentication method options for TLS-encryption

While configuring your server, you have two options to use TLS-encryption:

- Using the File-based certificates authentication method.
- Using the Windows Certificate Store authentication method.

Figure 1: syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property: Authentication methods available for using TLS encryption when configuring your syslog-ng PE server.



Server Property

Server | Failover Servers | Messages

☑ Enable flow-control

Server Name or Address (IPv4):

Server Port: 601

Reset to Default Port

□ Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP)

□ Use TLS encryption

○ File-based certificates (**Recommended option**)
Suitable for all currently supported TLS versions.

Select CA file

Select Certificate

Select Private Key

○ Windows Certificate Store (Legacy option)
Suitable only for TLS version 1.1 or lower.

Select Certificate

Advanced Options

Ok | Cancel

NOTE: When using TLS-encryption on your server, consider the following:

- It is not possible to configure both **File-based certificates**, and **Windows Certificate Store** as an authentication method for newly added destinations.
- For imported configurations that may already be configured for **Windows Certificate Store** authentication method, it is possible to configure **File-based certificates**, but the **File-based certificates** authentication method overwrites the **Windows Certificate Store** method.
- When using **File-based certificate** as an authentication method, uploading a CA file is required.

NOTE: When using TLS-encryption on your server, consider the following:

- The syslog-ng Agent for Windows application supports using the File-based certificate as an authentication method both for TLS version 1.1 or lower, and for TLS version 1.2 or higher. One Identity recommends using this option instead of the legacy Windows Certificate Store option, which only supports TLS versions 1.1 or lower.
- The syslog-ng Agent for Windows application only supports using the Windows Certificate Store as an authentication method for TLS version 1.1 or lower. One Identity does not recommend using this legacy option.

Prerequisites

1. For using file-based certificates as an authentication method:
   - Valid X.509 certificates, in PEM format.
   - Valid non-encrypted keys, in PEM format.
   - The CA file, the Client Certificate, and the Client Key must exist in their respective configured certificate paths before starting syslog-ng Agent for Windows, and must be properly distributed.
2. For using Windows Certificate Store as an authentication method:
   - To use the Windows Certificate Store as your authentication method, you must have certificates available in the Personal Certificates store of your Local Computer (MMC > Certificates > Computer Account > Local Computer > Personal Certificates).

     To import these certificates, you can use the Certificate Import Wizard. For details, see Importing certificates with the Microsoft Management Console.

Limitations

Using TLS-encryption with syslog-ng Agent for Windows has the current limitations:

- For the **File-based certificate** authentication method, the certificates must be valid X.509 certificates, in PEM format.

- For the **File-based certificate** authentication method, the keys must be valid non-encrypted keys, in PEM format.
- For the **File-based certificate** authentication method, the configured new files (that is, the CA-file, the client certificate, and the client key) are not distributed by syslog-ng Agent for Windows, but they must exist in the configured certificate path before starting syslog-ng Agent for Windows. The end-user is responsible for ensuring that the required files exist in the configured certificate paths.

Using the File-based certificates authentication method

When using TLS-encryption with syslog-ng Agent for Windows, using file-based certificates as an authentication method is one of your options.

Figure 2: syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property

> NOTE: The following are the responsibility of the user:
>
> - The user is responsible for ensuring that the certificates are valid X.509 certificates, in PEM format.
> - The user is responsible for ensuring that the keys are valid non-encrypted keys, in PEM format.
> - The configured new files (that is, the CA-file, the Client Certificate, and the Client Key) are not distributed by syslog-ng Agent for Windows, but they must exist in the configured certificate path before starting syslog-ng Agent for Windows. The end-user is responsible for ensuring that the required files exist in the configured certificate paths.

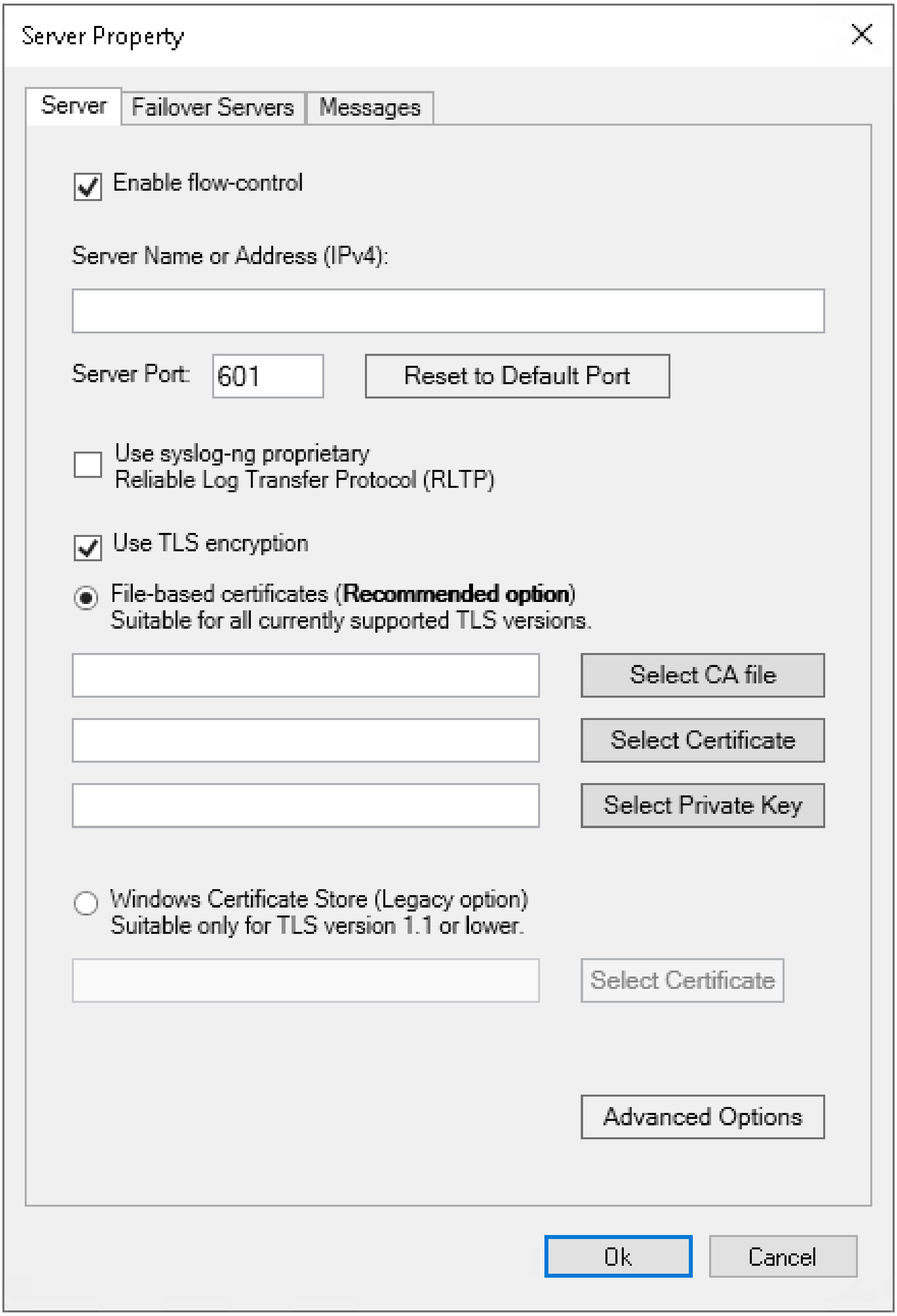
> NOTE: When using TLS-encryption on your server, consider the following:
>
> - The syslog-ng Agent for Windows application supports using the File-based certificate as an authentication method both for TLS version 1.1 or lower, and for TLS version 1.2 or higher. One Identity recommends using this option instead of the legacy Windows Certificate Store option, which only supports TLS versions 1.1 or lower.
> - The syslog-ng Agent for Windows application only supports using the Windows Certificate Store as an authentication method for TLS version 1.1 or lower. One Identity does not recommend using this legacy option.

To configure using File-based certificates as your authentication method,

1. Navigate to **syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property**.

2. Enable **Use TLS encryption**.
3. Select **File-based certificates**.

Figure 3: syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property: Using File-based certificates when using TLS encryption with syslog-ng Agent for Windows



Server Property

☑ Enable flow-control

Server Name or Address (IPv4):

Server Port: 601

□ Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP)

☑ Use TLS encryption

● File-based certificates (**Recommended option**)
Suitable for all currently supported TLS versions.

○ Windows Certificate Store (Legacy option)
Suitable only for TLS version 1.1 or lower.

> NOTE: When using TLS-encryption on your server, consider the following:
>
> - It is not possible to configure both **File-based certificates**, and **Windows Certificate Store** as an authentication method for newly added destinations.
> - For imported configurations that may already be configured for **Windows Certificate Store** authentication method, it is possible to configure **File-based certificates**, but the **File-based certificates** authentication method overwrites the **Windows Certificate Store** method.
> - When using **File-based certificate** as an authentication method, uploading a CA file is required.

4. To select your CA file from your local computer, click **Select CA file**.

   > NOTE: Selecting a CA file is required while using the **File-based certificates method**.

5. (Optional) To select your certificate and private key, click **Select Certificate**, and **Select Private Key**, then select the respective certificate and private key files from your Local Computer.

   > NOTE: When selecting your certificate key and private key, consider that you cannot select only one of them. That is, if you select the Certificate Key, selecting the Private Key is also required. Similarly, if you select the Private Key, selecting the Certificate Key is also required.

6. (Optional). To set compression-related preferences while using TLS-encryption, click **Advanced Options** and configure the server according to your preferences..

Configuring mutual authentication when using the File-based certificates authentication method

If the syslog-ng Premium Edition (syslog-ng PE) server requests authentication from the syslog-ng Agent for Windows, complete the configuration steps referring to selecting your certificate and private key when using the file-based certificates authentication method.

For details, see Using the File-based certificates authentication method.

> NOTE: When using TLS-encryption on your server, consider the following:
>
> - The syslog-ng Agent for Windows application supports using the File-based certificate as an authentication method both for TLS version 1.1 or lower, and for TLS version 1.2 or higher. One Identity recommends using this option instead of the legacy Windows Certificate Store option, which only supports TLS versions 1.1 or lower.
> - The syslog-ng Agent for Windows application only supports using the Windows Certificate Store as an authentication method for TLS version 1.1 or lower. One Identity does not recommend using this legacy option.

For more information about using mutual authentication options when using the Windows Certificate Store authentication method, see Configuring mutual authentication when using the Windows Certificate Store authentication method.

Using the Windows Certificate Store authentication method

When using mutual TLS-encryption with syslog-ng Agent for Windows, using certificates from the Windows Certificate Store as an authentication method is one of your options.

The syslog-ng Agent for Windows application can automatically show the requested certificate to the server when the connection is established, provided it is available in the Personal Certificates store of your Local Computer (MMC > Certificates > Computer Account > Local Computer > Personal Certificates).

To import this certificate, use the Certificate Import Wizard. For details, see Importing certificates with the Microsoft Management Console.

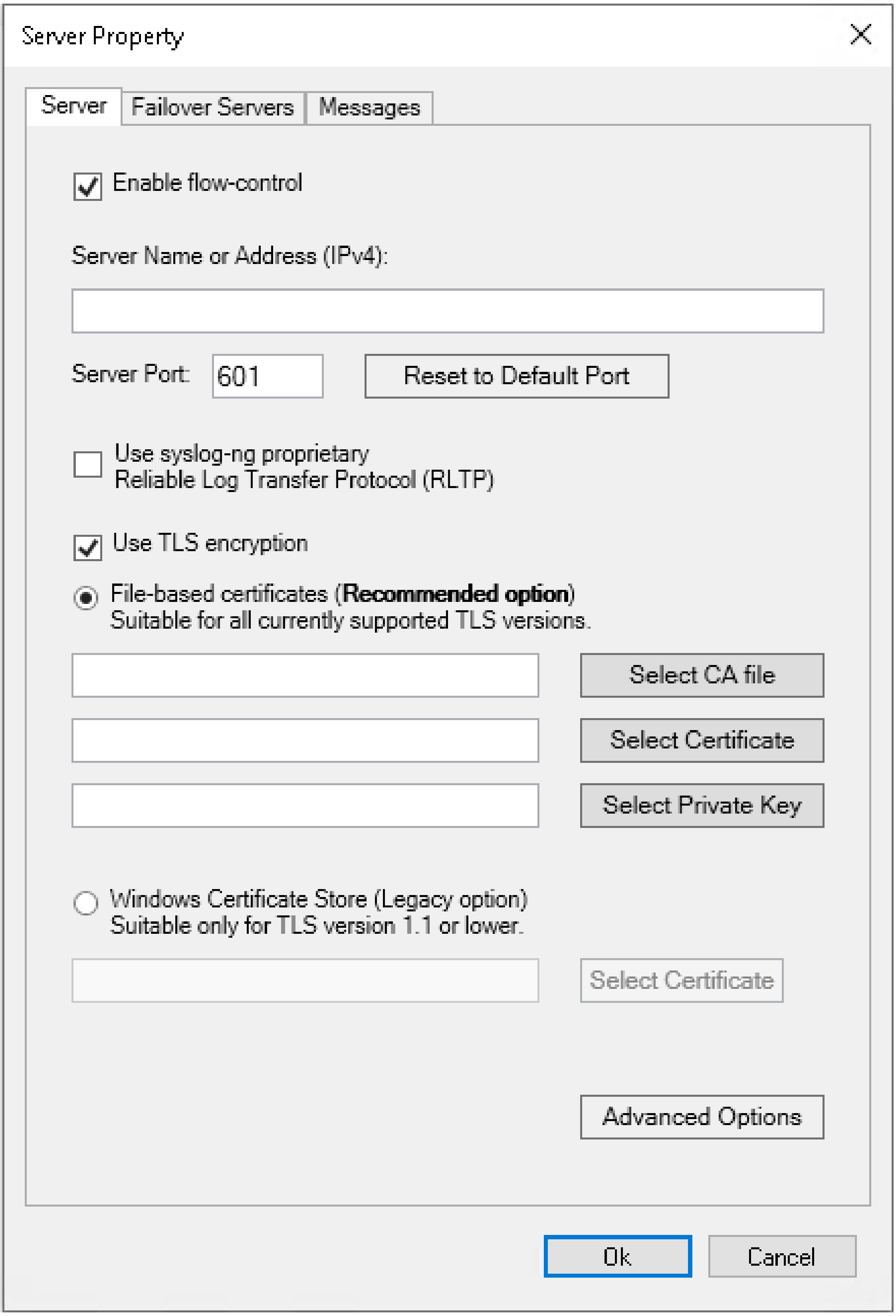
> NOTE: The syslog-ng Agent for Windows application only supports this certificate import method for the Windows Certificate Store authentication method.

For more information about using mutual authentication options when using the Windows Certificate Store authentication method, see Configuring mutual authentication when using the Windows Certificate Store authentication method.

To configure using Windows Certificate Store as your authentication method,

1. Navigate to **syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property**.
2. Enable **Use TLS encryption**.
3. Select **Windows Certificate Store**.

Figure 4: syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property



Server Property

Server | Failover Servers | Messages

☑ Enable flow-control

Server Name or Address (IPv4):

Server Port: 601

Reset to Default Port

□ Use syslog-ng proprietary
Reliable Log Transfer Protocol (RLTP)

☑ Use TLS encryption

● File-based certificates (**Recommended option**)
Suitable for all currently supported TLS versions.

Select CA file

Select Certificate

Select Private Key

○ Windows Certificate Store (Legacy option)
Suitable only for TLS version 1.1 or lower.

Select Certificate

Advanced Options

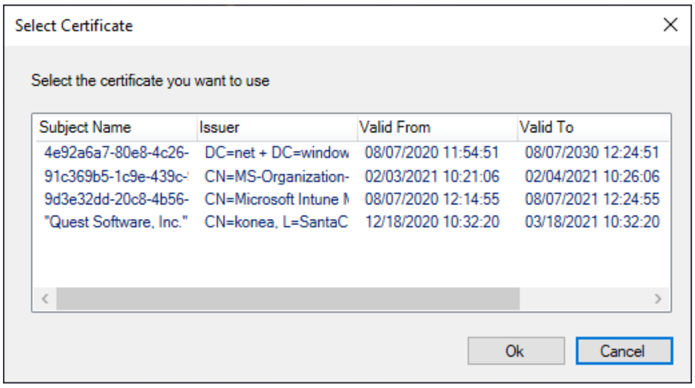
Ok | Cancel

> NOTE: When using TLS-encryption on your server, consider the following:
>
> - It is not possible to configure both **File-based certificates**, and **Windows Certificate Store** as an authentication method for newly added destinations.
> - For imported configurations that may already be configured for **Windows Certificate Store** authentication method, it is possible to configure **File-based certificates**, but the **File-based certificates** authentication method overwrites the **Windows Certificate Store** method.
> - When using **File-based certificate** as an authentication method, uploading a CA file is required.

> NOTE: When using TLS-encryption on your server, consider the following:
>
> - The syslog-ng Agent for Windows application supports using the File-based certificate as an authentication method both for TLS version 1.1 or lower, and for TLS version 1.2 or higher. One Identity recommends using this option instead of the legacy Windows Certificate Store option, which only supports TLS versions 1.1 or lower.
> - The syslog-ng Agent for Windows application only supports using the Windows Certificate Store as an authentication method for TLS version 1.1 or lower. One Identity does not recommend using this legacy option.

4. Click **Select Certificate**, and select the Windows Certificate of your choice.

   Figure 5: syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property > Select Certificate



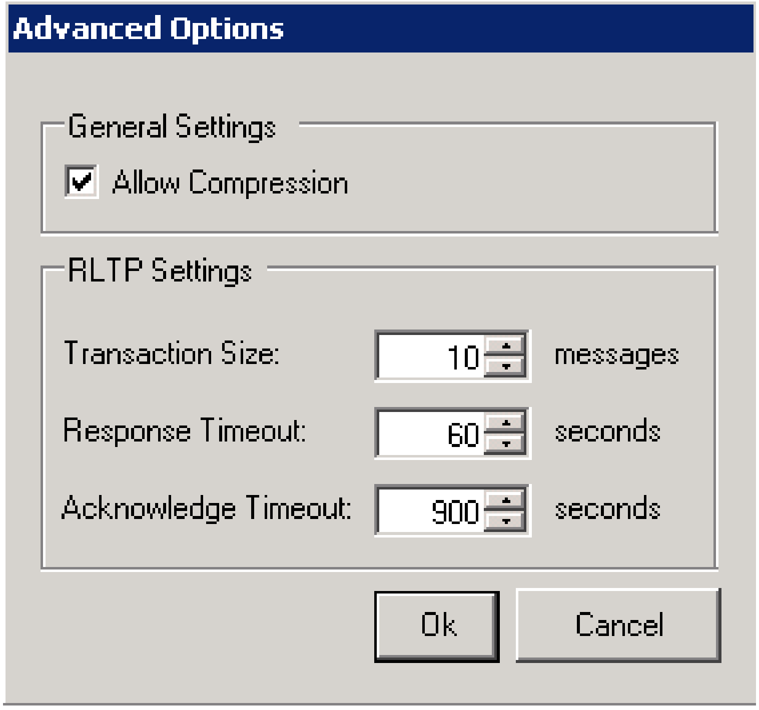
Select Certificate

Select the certificate you want to use

Subject Name	Issuer	Valid From	Valid To
4e92a6a7-80e8-4c26-	DC=net + DC=window	08/07/2020 11:54:51	08/07/2030 12:24:51
91c369b5-1c9e-439c-	CN=MS-Organization-	02/03/2021 10:21:06	02/04/2021 10:26:06
9d3e32dd-20c8-4b56-	CN=Microsoft Intune M	08/07/2020 12:14:55	08/07/2021 12:24:55
"Quest Software, Inc."	CN=konea, L=SantaC	12/18/2020 10:32:20	03/18/2021 10:32:20

5. (Optional) To configure advanced RLTP settings and to allow compression, click **Advanced Options**.

   Figure 3. syslog-ng Agent Settings > Local Settings > Destinations > Add New Server > Server Property > Advanced Options: Allowing compression, and advanced RLTP settings



Advanced Options

General Settings

☑ Allow Compression

RLTP Settings

Transaction Size: 10 messages

Response Timeout: 60 seconds

Acknowledge Timeout: 900 seconds

Configuring mutual authentication when using the Windows Certificate Store authentication method

If the syslog-ng Premium Edition (syslog-ng PE) server requests authentication from the syslog-ng Agent for Windows, complete the following steps.

> NOTE: When using TLS-encryption on your server, consider the following:
>
> - The syslog-ng Agent for Windows application supports using the File-based certificate as an authentication method both for TLS version 1.1 or lower, and for TLS version 1.2 or higher. One Identity recommends using this option instead of the legacy Windows Certificate Store option, which only supports TLS versions 1.1 or lower.
> - The syslog-ng Agent for Windows application only supports using the Windows Certificate Store as an authentication method for TLS version 1.1 or lower. One Identity does not recommend using this legacy option.

1. Create certificates for the clients. By default, syslog-ng Agent for Windows will look for a certificate that contains the hostname or IP address of the central syslog-ng PE server in its Common Name. If you use a different Common Name, do not forget to complete Step 3 to set the Common Name of the certificate.

   The certificate must contain the private key and must be in PKCS12 format.

> TIP:
>
> To convert a certificate and a key from PEM format to PKCS12 you can use the following command:
>
> ```
> openssl pkcs12 -export -in agentcertificate.pem -inkey
> agentprivatekey.pem -out agentcertificatewithkey.pfx
> ```

2. Import this certificate into the Personal Certificate store of the Local Computer using the Certificate Import Wizard. For details, see Importing certificates with the Microsoft Management Console.

   > NOTE: The syslog-ng Agent for Windows application only supports this certificate import method for the Windows Certificate Store authentication method.

3. By default, the syslog-ng Agent for Windows will look for a certificate that contains the hostname or IP address of the central syslog-ng PE server in its Common Name. (The agent will look for the server name or address set in the Server Name field of the destination.) If the certificate of the client has a different Common Name, complete the following steps:

   a. Start the configuration interface of the syslog-ng Agent for Windows for Windows application.

   b. Select **syslog-ng Agent Settings > Destinations**.

   c. Right-click on the server that requires mutual authentication and select **Properties**.

   d. Select the **Use TLS** option, click **Select**, then select the certificate to use. You can also type the Common Name of the certificate into the **Client Certificate Subject** field.

      If you have more than one certificates with the same Common Name, alternatively, you can type the Distinguished Name (DN) of the certificate into the **Client Certificate Subject** field. When using the Distinguished Name, type only the elements of the name, separated with comma, starting with the country. For example *`US, Maryland, Pasadena, Example Inc, Sample Department, mycommonname`*

      > NOTE: A common way is to use the hostname or the IP address of the host running syslog-ng Agent for Windows as the Common Name of the certificate (for example *`syslog-ng-agent1.example.com`*).

4. Select **Apply**, then **OK**. To activate the changes, restart the syslog-ng Agent for Windows service.

Importing certificates with the Microsoft Management Console

In certain cases, you may have to import your certificates for authentication with the Microsoft Management Console.

To import a certificate with the Microsoft Management Console

1. Start the Microsoft Management Console by running `mmc.exe` (Navigate to your Start menu, and select Run application).

   NOTE: Running `mmc.exe` requires administrator privileges.

2. Click on the Add/Remove snap-in item of the File menu.
3. Click Add, select the Certificates module, and click Add.
4. Select Computer account in the displayed window and click Next.
5. Select Local computer and click Close.
6. To import the CA certificate of the syslog-ng Premium Edition (syslog-ng PE) server's certificate, navigate to Console Root > Certificates > Trusted Root Certificate Authorities > Certificates.

   To import a certificate for syslog-ng Agent for Windows to perform mutual authentication, navigate to Console Root > Certificates > Personal > Certificates.

7. Right-click on the Certificates folder and from the appearing menu select All tasks > Import. The Certificate Import Wizard will be displayed. Click Next.

   (Optional): Certificates used to authenticate the syslog-ng Agent for Windows in mutual authentication include the private key. Provide the password for the private key when requested.

8. Microsoft Windows offers a suitable certificate store by default, so click Next.
9. Click Finish on the summary window and Yes on the window that marks the successful importing of the certificate.

Filtering messages

The syslog-ng Agent for Windows application can filter log messages both in blacklist- and whitelist fashion. When using blacklisting, you can define filters, and any message that matches the filters is ignored by the agent — only messages that do not match the filters are sent to the central server. When using whitelisting, you can define filters, and the messages matching the filters are forwarded to the central server — other messages are ignored. By default, blacklist filtering is used.

If you define multiple filters, the messages must match every filter. In other words, the filters are connected to each other with logical AND operations.

Different filters are available for eventlog- and file sources. When the syslog-ng Agent processes a message, it checks the relevant filters one-by-one: for example if it finds a blacklist filter that matches the message, the agent stops processing the message without sending it to the server.

> NOTE:
>
> By default, all filters are case sensitive. For details on how to change this behavior, see Procedure 5.7, “Configuring global settings”.

- For details on how to filter messages received from eventlog sources, see Procedure 7.1, “Filtering eventlog messages”.
- For details on how to filter messages received from file sources, see Procedure 7.2, “Filtering file messages”.
- For details on how to disable filtering globally, see Procedure 5.9, “Disabling sources and filters globally”.

Procedure 7.1. Filtering eventlog messages

Purpose:

The following types of filters are available for eventlog sources. Unless described otherwise, the filters match only if the same string appears in the related field of the message.

> NOTE:
>
> When filtering on the message source, the values of the Source field can be incorrect in some cases. Check the *EVENT_SOURCE* field of a message to avoid any problems.

- *Sources*: Filter on the source (application) that created the message. Corresponds with the *EVENT_SOURCE* macro.
- *Sources and Event ID*: Filter on the source (application) that created the message, and optionally on the identification number of the event. Corresponds with the *EVENT_SOURCE* and *EVENT_ID* macros.
-

Message Contents: Filter the text of the message, that is, the contents of the *EVENT_MESSAGE* macro. In this filter you can use regular expressions.

Sources and Categories: Filter on the source (application) that created the message, and optionally on the category of the event. Corresponds with the *EVENT_SOURCE* and *EVENT_CATEGORY* macros.

Example 7.1. Filtering on Sources and Categories

For example, you want to filter the following message:

```
Source: Microsoft Windows security auditing
Category: Process Creation
New Process Name: C:\Windows\System32\SearchProtocolHost.exe
```

Set the Source to *Microsoft Windows security auditing*, and Category to *Process Creation*.

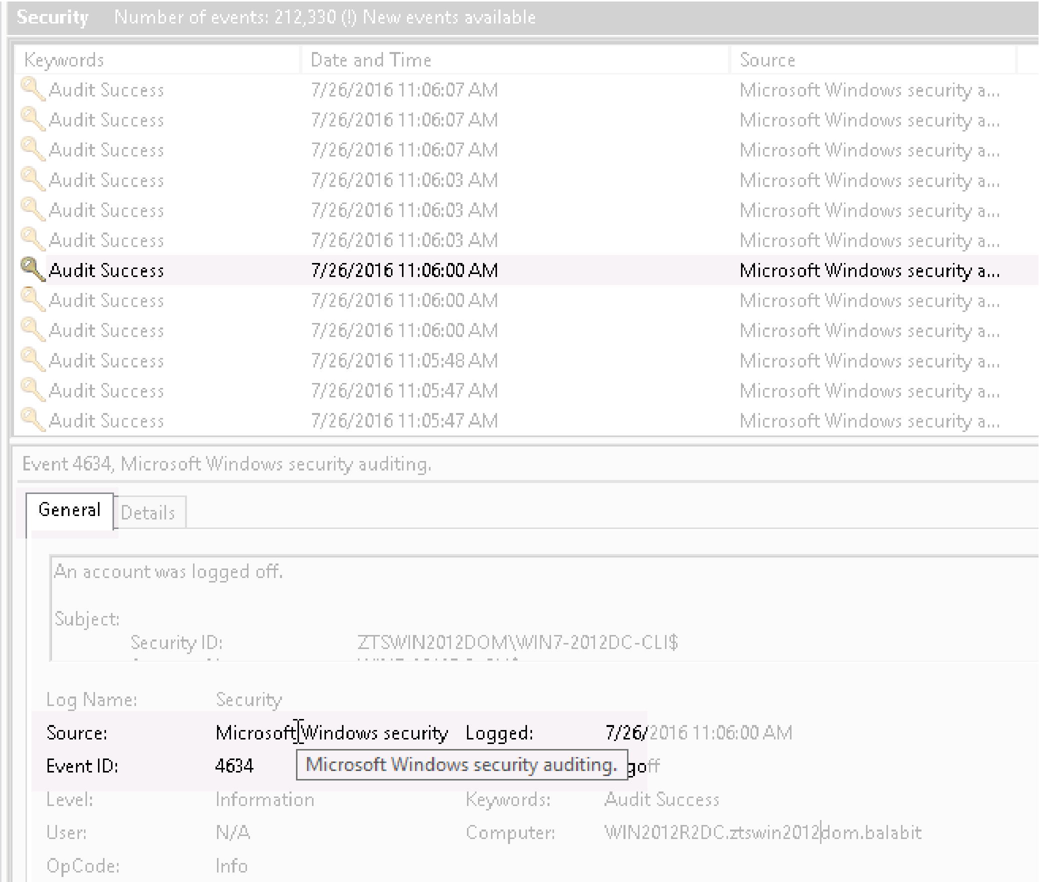
- *Users*: Filter on the username associated with the event. Corresponds with the *EVENT_USERNAME* macro.
- *Computers*: Filter on the name of the computer (host) that created the event. Corresponds with the *HOST* macro.
- *Event Types*: Filter on the type of the event. Corresponds with the *EVENT_TYPE* macro.

To modify the filters used for eventlog messages, complete the following procedure:

Steps:

1. If you want to filter on the source of the message, complete the following steps.
   a. Start the Event Viewer application and find a message from the source that you want to filter.
   b. Select the General tab, and right-click on the value of the Source field.

   Figure 7.1. Finding the name of the Event Source



Security   Number of events: 212,330 (!) New events available

Keywords	Date and Time	Source
Audit Success	7/26/2016 11:06:07 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:07 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:07 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:03 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:03 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:03 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:00 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:00 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:06:00 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:05:48 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:05:47 AM	Microsoft Windows security a...
Audit Success	7/26/2016 11:05:47 AM	Microsoft Windows security a...

Event 4634, Microsoft Windows security auditing.

An account was logged off.

Subject:
Security ID: ZTSWIN2012DOM\WIN7-2012DC-CLI$

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/26/2016 11:06:00 AM
Event ID:	4634	Microsoft Windows security auditing.	goff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN2012R2DC.ztswin2012dom.balabit
OpCode:	Info		

c. Select Copy. Save the saved value somewhere, you will need it later to configure the filter in syslog-ng Agent.

> NOTE:
>
> It is important to use this method, because the actual value of the Source field can be longer than what the Event Viewer displays. (For example, for security messages, the displayed source is often **`Microsoft Windows security`**, while the full name of the source is **`Microsoft Windows security auditing.`** which includes the dot character at the end.)
>
> Hovering your mouse over the value of the Source field also displays the full name of the source.

2. Start the configuration interface of the syslog-ng Agent for Windows application.

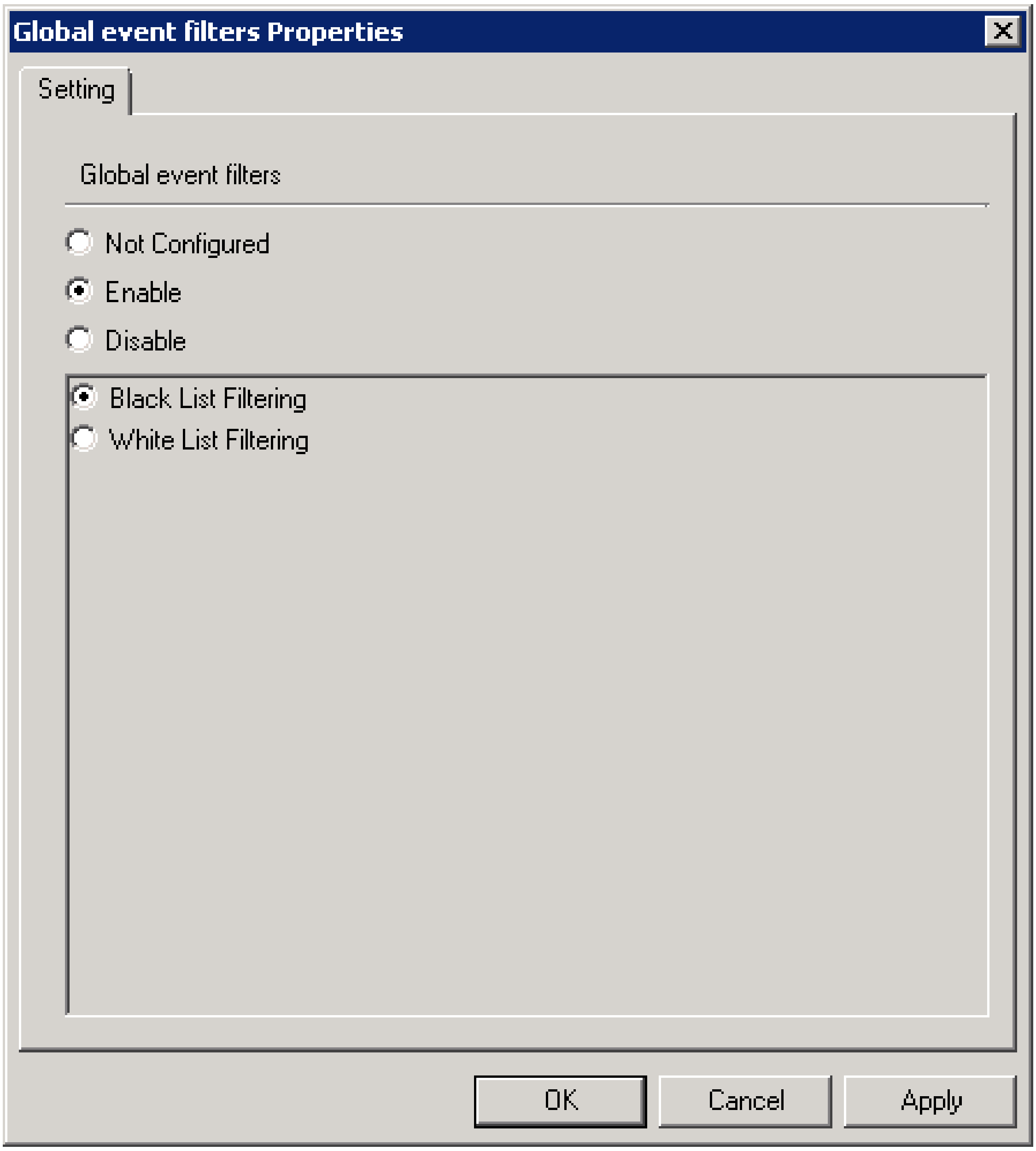
3. - To apply filters globally to every eventlog message, select syslog-ng Agent Settings > Destinations > Global Event Filters, and right-click Global Event Filters.
   - To apply filters only to a specific destination, select syslog-ng Agent Settings > Destinations, select the destination server, then select Event Filters. Right-click Event Filters.

NOTE:

If you want to use both global and local (server side) filtering, first global filters will be applied to the eventlog messages and then the local filters.

Select Properties > Enable > OK.

Figure 7.2. Global event filters



Global event filters

○ Not Configured

● Enable

○ Disable

● Black List Filtering

○ White List Filtering

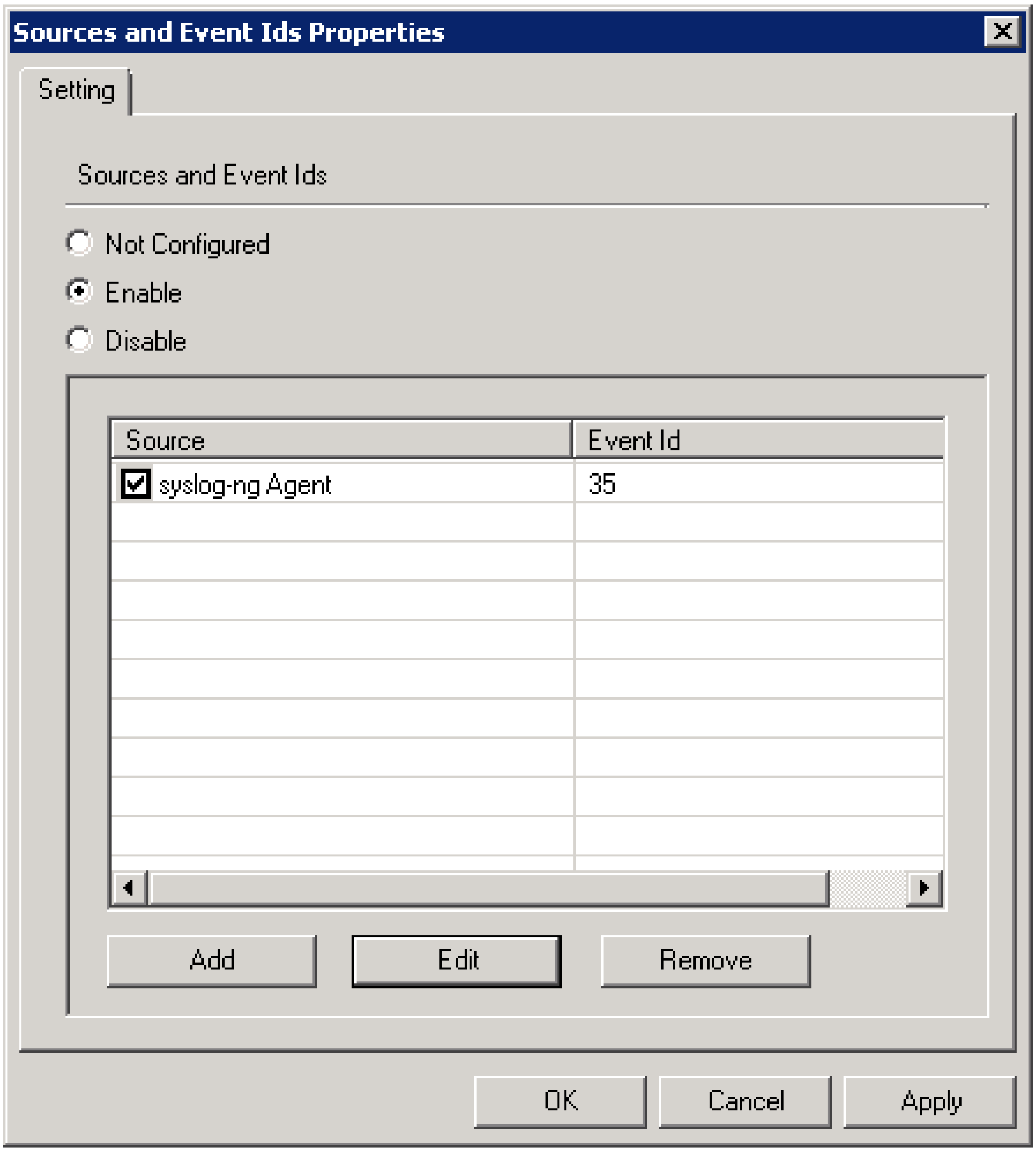
4.

5. To use whitelist-filtering, select White List Filtering. By default, syslog-ng Agent uses blacklist filtering.

6. On the right-hand pane, double-click on the type of filter you want to create.

   To ignore messages sent by a specific application, or messages of the application with a specific event ID, double-click on Sources and Event ID, select Add, and enter the name of the source (application) whose messages you want to ignore into the Source Name field. To ignore only specific messages of the application, enter the ID of the event into the Event ID field. Select Add > Apply.

   Figure 7.3. Sources and Event ID

   Sources and Event Ids Properties

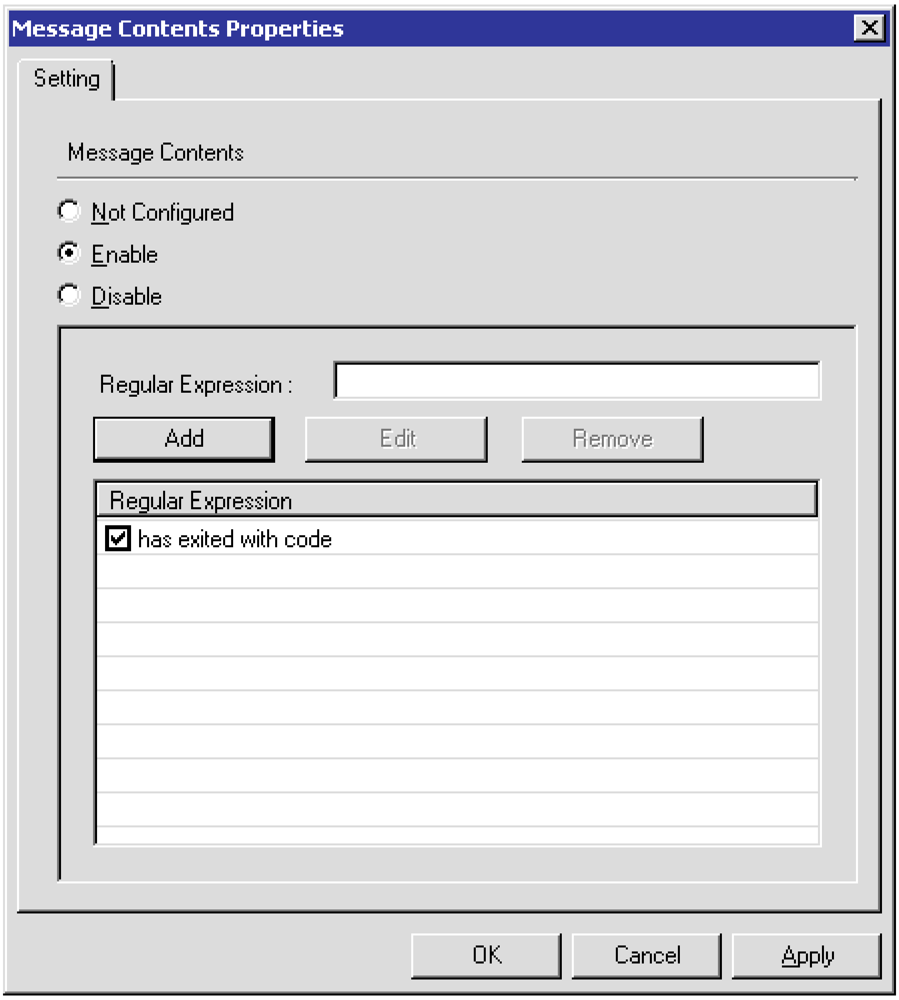
   Sources and Event Ids

   ○ Not Configured
   ● Enable
   ○ Disable

Source	Event Id
☑ syslog-ng Agent	35

7.
   -
   - To ignore messages that contain a specific string or text, double-click on Message Contents, enter the search term or a POSIX regular expression into the Regular Expression field, then select Add > Apply.

Figure 7.4. Message Contents



Message Contents

○ Not Configured
● Enable
○ Disable

Regular Expression :

Regular Expression
☑ has exited with code

- To ignore messages sent by a specific application, or messages of the application that fall into a specific category, double-click on Sources and Categories, select Add, and select the name of the application whose messages you want to ignore from the Application Name field. To ignore only those messages of the application that fall into a specific category, enter the name of the category into the Category field. Select Add > Apply.
- To ignore messages sent by a specific user, double-click on Users, enter the name of the user into the User field, then select Add > Apply.
- To ignore messages sent by a specific computer (host), double-click on Computers, enter the name of the user into the Computer field, then select Add > Apply.
- *Event Types*: To ignore messages of a specific event-type, double-click on Event Types, select the event types to ignore, and select Ok > Apply.

NOTE:

Windows labels certain messages as level 3 and the Event Viewer labels such messages as warnings. This is against the official specification: level 3 should not be used, and only level 2 messages are warnings. To filter these events, you have to manually add a new event type to the registry and set its value to 3, for example *HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\syslog-ng Agent\Local Settings\EventSources\Filter\Type\Rule0\Type=3*

8. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Procedure 7.2. Filtering file messages

Purpose:

The following types of filters are available for file sources:

- *Message Contents*: Filter the text of the message, that is, the contents of the *FILE_MESSAGE* macro. In this filter you can use regular expressions.
- *File Name*: Filter on the file name. Corresponds with the *FILE_NAME* macro. In this filter you can use wildcards (*, ?). Only available for destination file filters.

To modify the filters used for file messages, complete the following procedure:

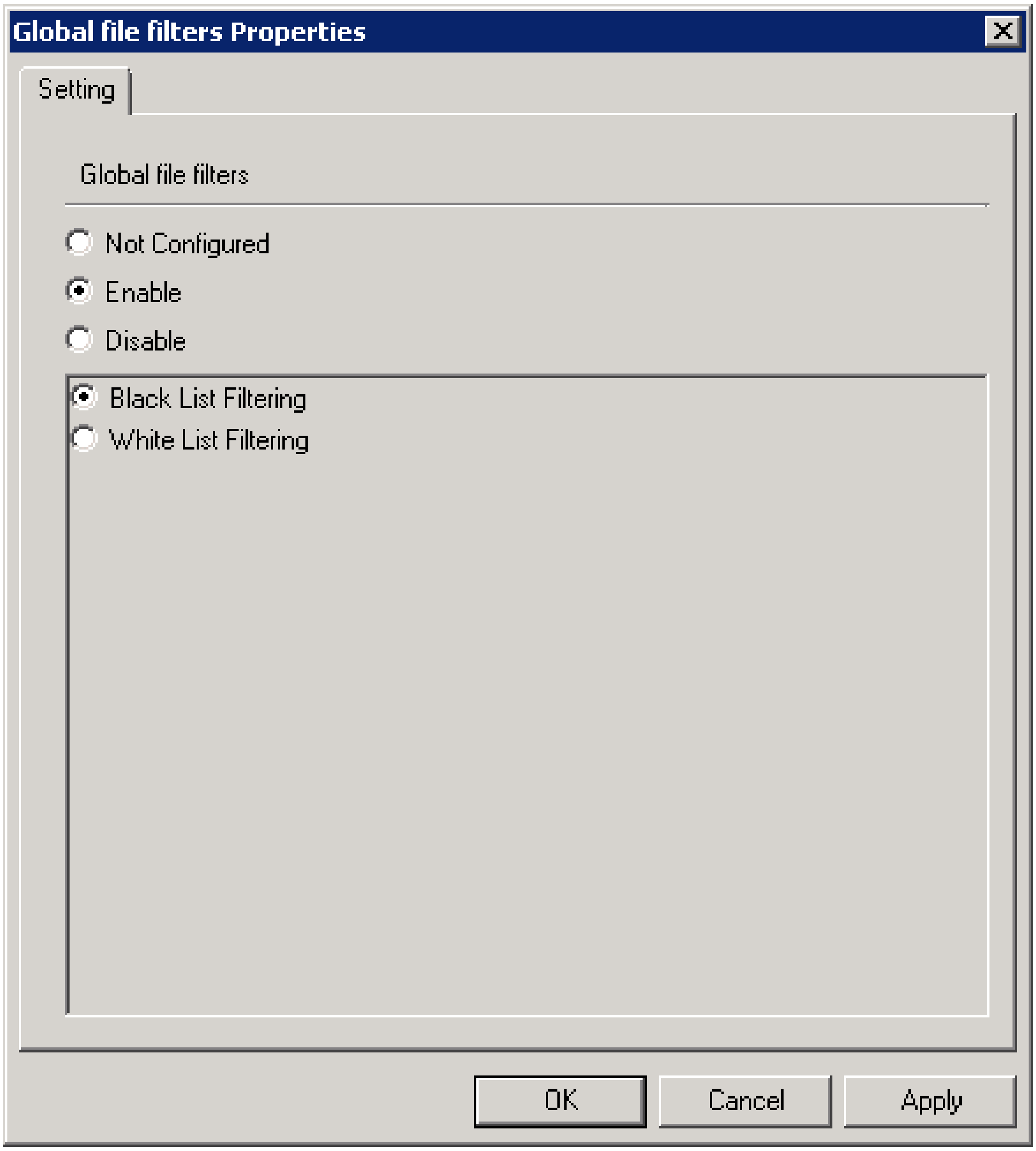
Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2.
   - To apply filters globally to every file message, select syslog-ng Agent Settings > Destinations > Global File Filters, and right-click Global File Filters.
   - To apply filters only to a specific destination, select syslog-ng Agent Settings > Destinations, select the destination server, then select File Filters. Right-click File Filters.

   NOTE:

   If you want to use both global and local (server side) filtering, first global filters will be applied to the file messages and then the local filters.
3. Select Properties > Enable > OK.

Figure 7.5. Global file filters



Global file filters

○ Not Configured

● Enable

○ Disable

● Black List Filtering

○ White List Filtering

4. To use whitelist-filtering, select White List Filtering. By default, syslog-ng Agent uses blacklist filtering.
5. On the right-hand pane, double-click on the type of filter you want to create.
6. - To ignore messages that contain a specific string or text, double-click on Message Contents, enter the search term or a regular expression into the Regular Expression field, then select Add.
7. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

Customizing the message format

The format of the messages received from the eventlog and the file sources can be customized using templates. You can define separate message format for the eventlog and the file sources. If you have multiple destination servers configured, you can define separate templates for each server. When creating a template to customize the message format, you can use macros, all alphanumeric characters, and the following special characters: `<>,():;-+/_`.

By default, syslog-ng Agent uses the following templates to forward messages:

- For the BSD protocol: `<${PRI}>${BSDDATE} ${HOST} ${MSGHDR}${MESSAGE}`
- For messages read from the eventlog, the `$MESSAGE` part is `${EVENT_USERNAME}: ${EVENT_NAME} ${EVENT_SOURCE}: [${EVENT_TYPE}] ${EVENT_MSG} (EventID ${EVENT_ID})` for every protocol.
- For messages read from a file, the `$MESSAGE` part is `$FILE_NAME: $FILE_CURRENT_POSITION/$FILE_SIZE: $FILE_MESSAGE` for every protocol.

Procedure 8.1. Customizing messages using templates

Purpose:

To create a template, complete the following procedure:

CAUTION:

These macros are available only in the syslog-ng Agent for Windows. To recognize Windows-specific elements of the log message (for example eventlog-related macros) on the syslog-ng server, you have to use parsers on the syslog-ng server. The parser must be configured to match the message format set in the syslog-ng Agent.

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Destinations. Select your log server, and click Properties.
3. To change the format of messages received from eventlog sources, type the message format you want to use into the Event Message Format > Message Template field.

   To change the format of messages received from file sources, type the message format you want to use into the File Message Format > Message Template field.

   Do not forget to add the `$` character before macros. For a complete list of the available macros, see the section called “Macros available in the syslog-ng Agent”.

For example, to send the messages in the `DATE HOSTNAME MESSAGE` format, type `Date:$DATE Hostname:$HOST Logmessage:$MESSAGE`.

Note that the $MESSAGE macro contains not only the text of the log message, but also additional information received from the message source, such as the name of the eventlog container, or the file, as set in the eventlog-specific and file-specific templates.

> NOTE:
>
> Templates are assigned to a single destination server, so it is possible to use different templates for different servers. However, a server and its failover servers always receive the same message.

> **CAUTION:**
>
> **If you have more than one destination servers configured (separate servers, not in failover mode), and you want to use the same template for every server, you must manually copy the template into the configuration of each server. Template modifications are not applied automatically to every server.**

4. Click OK.
5. To activate the changes, restart the syslog-ng Agent service.

Customizing the timestamp used by the syslog-ng Agent

The syslog-ng Agent can send the syslog messages using either the ISO or the BSD timestamp format. It is recommended to use the ISO format, because it contains much more information than the BSD format.

Note that in the syslog-ng Agent, the macros without prefix (for example *DATE*) always refer to the receiving date of the message (for example *R_DATE*) when it arrived into the event log container, and are included only for compatibility reasons.

> **CAUTION:**
>
> **If a remote host is logging into the event log of the local host that is running syslog-ng Agent for Windows, both hosts have to be in the same timezone, because the event log message does not include the timezone information of the sender host. Otherwise, the date of the messages received from the remote host will be incorrect.**

Macros available in the syslog-ng Agent

The following sections list the available macros:

⚠ **CAUTION:**

These macros are available only in the syslog-ng Agent for Windows. To recognize Windows-specific elements of the log message (for example eventlog-related macros) on the syslog-ng server, you have to use parsers on the syslog-ng server. The parser must be configured to match the message format set in the syslog-ng Agent.

- Macros related to protocol headers
- Macros related to the date and time of the message
- Macros related to eventlog sources
- Macros related to file sources

ℹ NOTE:

Note that if you use the Syslog protocol template (meaning that messages are sent using the IETF-syslog protocol), only the message part of the log message can be customized, the structure of the headers and other information is fixed by the protocol.

Protocol-related macros of the syslog-ng Agent

APP_NAME

Description: An alias for the *APPLICATION_NAME* macro.

APPLICATION_NAME

Description:

- At event container: Name of the application the message came from
- At file as the name of creator (default value): syslog-ng-agent

HOST

Description: Name of the host sending the message. Hostnames are automatically converted to lowercase.

MESSAGE

Description: The content of the message, including the text of the message and any file- or event-specific macros that are set for the source.

MSG

Description: An alias for the *MESSAGE* macro.

MSGHDR

Description: The name and the PID of the program that sent the log message in `PROGRAM [PID]:` format. Includes a trailing whitespace. Note that the macro returns an empty value if both the PROGRAM and PID fields of the message are empty.

PRI

Description: Priority header of the message, storing the facility and the level of the message.

PROCESS_ID

Description: PID of the application the message came from.

Time-related macros of the syslog-ng Agent

BSDDATE, R_BSDDATE, S_BSDDATE

Description: Date of the message in BSD timestamp format (month/day/hour/minute/second, each expressed in two digits). This is the original syslog time stamp without year information, for example `Jun 13 15:58:00`. If possible, it is recommended to use *ISODATE* for timestamping.

DATE, R_DATE, S_DATE

Description: Date of the message using the BSD-syslog style timestamp format (month/day/hour/minute/second, each expressed in two digits). This is the original syslog time stamp without year information, for example: `Jun 13 15:58:00`.

DAY, R_DAY, S_DAY

Description: The day the message was sent.

FULLDATE, R_FULLDATE, S_FULLDATE

Description: A nonstandard format for the date of the message using the same format as *${DATE}*, but including the year as well, for example: `2006 Jun 13 15:58:00`.

HOUR, R_HOUR, S_HOUR

Description: The hour of day the message was sent.

ISODATE, R_ISODATE, S_ISODATE

Description: Date of the message in the ISO 8601 compatible standard timestamp format (yyyy-mm-ddThh:mm:ss+-ZONE), for example: *2006-06-13T15:58:00.123+01:00*. If possible, it is recommended to use *ISODATE* for timestamping. Note that the syslog-ng Agent cannot produce fractions of a second (for example milliseconds) in the timestamp.

MIN, R_MIN, S_MIN

Description: The minute the message was sent.

MONTH, R_MONTH, S_MONTH

Description: The month the message was sent as a decimal value, prefixed with a zero if smaller than 10.

MONTHNAME, R_MONTHNAME, S_MONTHNAME

Description: The English name of the month the message was sent, abbreviated to three characters (for example Jan, Feb, and so on).

SEC, R_SEC, S_SEC

Description: The second the message was sent.

TZ, R_TZ, S_TZ

Description: An alias of the ${TZOFFSET} macro.

TZOFFSET, R_TZOFFSET, S_TZOFFSET

Description: The time-zone as hour offset from GMT, for example: `-07:00`. In syslog-ng 1.6.x this used to be `-0700` but as *${ISODATE}* requires the colon it was added to *${TZOFFSET}* as well.

UNIXTIME, R_UNIXTIME, S_UNIXTIME

Description: Standard UNIX timestamp, represented as the number of seconds since `1970-01-01T00:00:00`.

YEAR, R_YEAR, S_YEAR

Description: The year the message was sent.

WEEK, R_WEEK, S_WEEK

Description: The week number of the year, prefixed with a zero for the first nine week of the year. (The first Monday in the year marks the first week.)

WEEKDAY, R_WEEKDAY, S_WEEKDAY

Description: The 3-letter name of the day of week the message was sent, for example *Thu*.

Eventlog-related macros of the syslog-ng Agent

EVENT_CATEGORY

Description: The category of the event.

EVENT_DATA

Description: Empty macro, does not contain any data.

EVENT_CONTAINER_COUNTER

Description: The number of received messages per container since the syslog-ng Agent for Windows was started.

EVENT_FACILITY

Description: The facility that sent the message.

EVENT_GLOBAL_COUNTER

Description: A unique ID for messages generated at reception time on the receiving host. It facilitates defining relationships between messages that are potentially distributed to different files on the same host, or different hosts.

EVENT_HOST

Description: The name of the host that sent the log message.

EVENT_ID

Description: The identification number of the event.

EVENT_LEVEL

Description: Importance level of the message represented as a number: 6 - Success, 5 - Informational, 4- Warning, or 3 - Error).

EVENT_MESSAGE

Description: The content of the message.

EVENT_MESSAGE_XML

Description: Contains the entire message in XML format.

EVENT_MSG

Description: The content of the message. This is an alias of the *EVENT_MESSAGE*.

EVENT_MSG_XML

Description: Contains the entire message in XML format. This is an alias of the *EVENT_MESSAGE_XML*.

EVENT_NAME

Description: Name of the Windows event log container (for example Application or Security).

EVENT_PROVIDER

Description: Name of the service that generated the log message.

EVENT_REC_NUM

Description: The record number of the event in the event log.

EVENT_SID

Description: The security identification number of the event.

EVENT_SID_TYPE

Description: The security identification number resolved into name. One of the following: *User*, *Group*, *Domain*, *AliasWellKnownGroup*, *DeletedAccount*, *Invalid*, *Unknown*, *Computer*.

EVENT_SOURCE

Description: The application that created the message.

EVENT_TASK

Description: The task category of the event.

EVENT_TYPE

Description: The importance level of the message in text format.

EVENT_USERNAME

Description: The user running the application that created the message.

File-related macros of the syslog-ng Agent

FILE_CURRENT_POSITION

Description: The position of the message from the beginning of the file in bytes.

FILE_FACILITY

Description: The facility that sent the message.

FILE_LEVEL

Description: Importance level of the message represented as a number: 6 - Success, 5 - Informational, 4- Warning, or 3 - Error).

FILE_MESSAGE

Description: The content of the message.

FILE_MSG

Description: The content of the message. This is an alias of the *FILE_MESSAGE* macro.

FILE_NAME

Description: Name of the log file (including its path) from where the syslog-ng PE received the message.

FILE_SIZE

Description: The current size of the file in bytes.

Customizing the syslog-ng Agent for Windows services

During installation, syslog-ng Agent registers the *syslog-ng Agent* service that is started automatically when the host boots. To disable the automatic startup of the syslog-ng Agent use the Start Menu > Control Panel > Administrative Tools > Services interface. The service is running with the privileges of the *NT AUTHORITY\SYSTEM* user.

To manually start or stop the service use the Start Menu > Control Panel > Administrative Tools > Services interface, or navigate to Start Menu > Programs > syslog-ng Agent for Windows. Note that in the latter case if User Access Control (UAC) is enabled, you need the *Run as Administrator* privilege to start or stop the syslog-ng Agent.

When the syslog-ng Agent service is started or stopped, it sends a syslog message to the central log server and an eventlog message to the Application eventlog container of the host.

⚠ **CAUTION:**

If you change the timezone setting of the host while the syslog-ng Agent is running, you have to restart the syslog-ng Agent. Otherwise, it will not receive the updated timezone information and the date of the events will be incorrect.

NOTE:

It is possible to run the service with an administrator account that has "log on as service" rights (to set user rights, navigate to Local Security Policy > Local Policies > User rights Assignment). These settings are unsupported, use them only at your own risk. Also note that during the next upgrade procedure, these settings will be overwritten by factory default settings.

Command-line options

The syslog-ng Agent for Windows application has the following command-line options:

NOTE:

Command-line options are case-insensitive. The options consist of a single letter introduced by either "-" or "/".

NOTE:

Command-line options will only work with administrator permission.

/c

Start the syslog-ng Agent using the specified XML configuration file.

/d

Start the syslog-ng Agent in debug mode.

/h

Display a help message about the command-line options.

/i

Install the syslog-ng Agent service into the services list.

/r

Remove the syslog-ng Agent service from the services list.

/v

Display version information.

/x

Validate XML configuration file without importing it.

To use these options, select Start > Run > cmd, navigate to the directory where the syslog-ng Agent is installed (for example **cd C:\Windows\Program Files\BalaBit\syslog-ng Agent**), and execute the **syslog-ng-agent.exe** file with the required option.

Example 9.1. Using command line options

To start syslog-ng Agent in debug mode:

```
syslog-ng-agent.exe /d
```

To start syslog-ng Agent with XML configuration file:

```
syslog-ng-agent.exe /c C:\ConfigFiles\syslog-ng-agent-conf.xml
```

To register syslog-ng Agent as a service using XML configuration file:

```
syslog-ng-agent.exe /i C:\ConfigFiles\syslog-ng-agent-conf.xml
```

Troubleshooting syslog-ng Agent for Windows

In case you experience problems with the syslog-ng Agent for Windows application, the following points can be of help.

> NOTE:
>
> The followings address only problems specific to the syslog-ng Agent, and assume that communication between the server and the client is otherwise possible (that is, the server is properly configured to receive messages and is available on the network, and name resolution is properly configured on the client).

Configuration changes do not take effect:

Configuration changes take effect only after restarting the syslog-ng service or rebooting the system. Also restart the system after changing the timezone settings of the host, or importing a certificate that you want to use to authenticate the communication between the agent and the server. If the configuration of the agent has changed since the last restart, the syslog-ng Agent sends a message of the change, including the hmac-sha-1 hash of the new configuration.

Also note that if your clients are managed from a Domain Controller, configuration changes are not instantly downloaded to the client hosts, only at the time of the next group policy update. To update the configuration of a client host earlier, open a command prompt on the client host, and issue the **gpupdate /force** command.

After downloading the configuration from the Domain Controller, the syslog-ng Agent service is automatically restarted if the configuration has changed.

> NOTE:
>
> Certain domain settings that can affect the syslog-ng Agent are downloaded only when the machine is rebooted. For example, moving the computer from one group policy to another requires a reboot to have effect.

The syslog-ng Agent does not send messages to the server:

Check the Application eventlog for messages of the syslog-ng Agent. In case of connection errors and certificate problems, the syslog-ng Agent sends error messages into the eventlog. Ensure that the destination address of the server is correctly set. If you use SSL encryption, verify that the certificate of the Certificate Authority of the server and that the certificate of the client are properly imported. If there are no error messages, check the logs on your log server: the syslog-ng Agent sends a MARK message every ten minutes even if there are no other messages to send (unless you have disabled MARK messages).

The syslog-ng Agent sends only MARK messages to the server:

Verify that you have configured the eventlog and file sources, and that they have not been disabled globally. If these settings are correct but the server still does not send any messages, temporarily disable all filters to see that they are not configured to ignore every message. When using filter, it is also recommended to check the global case-sensitivity settings.

The hostname used in the messages changes: If a host is sometimes logged in into a domain and sometimes it is not, its hostname might reflect this. To avoid this situation, select syslog-ng Agent Settings and double-click on Global Settings. Enable Global Settings, navigate to Hostname and select Use FQDN. This causes syslog-ng Agent to resolve its own hostname from DNS and use the resolved FQDN in the syslog messages. For details, see Procedure 5.8, “Configuring the hostname format”.

Command-line parameters are ignored:

Command-line parameters work only for administrators if User Account Control (UAC) is enabled. To execute syslog-ng Agent with command-line parameters, select Start > Programs > Accessories, right-click on Command prompt > Run as administrator.

If you contact our Support Team about a problem with the syslog-ng Agent for Windows, execute the **syslog-ng-agent -V** command from the command line and include every version and platform information it displays in your support request.

CPU load is high: See the section called “Sending messages and CPU load”.

Losing messages from eventlog containers:
An eventlog container is a special file. The Agent reads this file, formats the messages and sends them to remote log server. Note that the eventlog container can be configured only to a certain size. If the container reaches that size, Windows writes the next message to the beginning of the file. As a result, if the agent is not running (or the destination server is unavailable) so long that the eventlog container is filled up, messages can be lost.

Logs are not forwarded instantly:

For the logs of certain applications (for example, Internet Information Services (IIS) for Windows Server), the syslog-ng Agent for Windows application does not forward the log messages in real time, only in batches after a certain amount of time. The cause of the problem is that the Windows operating system does not immediately flush its buffers to the file when an application sends a log message. The syslog-ng Agent for Windows application immediately starts sending the log messages when they become available in the log file.

Sending messages and CPU load

The syslog-ng Agent application can send messages to the server when the Windows Scheduler provides resources to the syslog-ng Agent. When there are many unsent log messages in the log sources, and there is no other significant activity on the host, syslog-ng will start to send the messages to the server, possibly increasing the CPU load to 100%. After all messages have been sent, or if another application requires the resources, the CPU load decreases back to normal.

TIP:

> To avoid the initial large load on the CPU, limit the rate of message sending temporarily. You can remove the limit after the old messages have been sent. For details, see Procedure 4.2, “Limiting the rate of messages”.

When relaying the messages from multiple sources, the syslog-ng Agent sends one message at a time from each source. That way a single source with a large log traffic does not block other log sources.

Debugging syslog-ng Agent

To enable debug options, create the `debug.ini` file in the syslog-ng Agent install directory.

Example 10.1. Content of the debug.ini file

The `debug.ini` can consist of the following entries:

```
[AgentDbgLog]
enabled=on/off
path=<debug_file_folder_path>[GpoDbgLog]
enabled=on/off
path=<debug_file_folder_path>[WriteMiniDump]
enabled=on/off
```

NOTE:

The `debug.ini` file cannot be distributed. It can only be used on a local machine.

Procedure 10.1. Creating core and memory dumps

Purpose:

The BalaBit support team might request you to send them core dumps of the syslog-ng Agent to investigate a particular problem. When enabled, the syslog-ng Agent for Windows application creates core dumps automatically when it experiences an unexpected shutdown.

Steps:

1. To enable core dumps, enter the following lines in the `debug.ini` file:

   ```
   [WriteMiniDump]
   enabled=on
   ```

   Core dumps are written into the installation folder of the syslog-ng Agent under the `syslog-ng-agent.PID.dmp` filename. The size of a core file is typically about 40-50 MB.

   NOTE:

   By default, this option is enabled. Due to disk space limits you can disable it to prevent hard disk becomes full.

2. To apply the changes, restart the syslog-ng Agent after modifying the *`[WriteMiniDump]`* part of the `debug.ini` file.

Procedure 10.2. Enabling debug logging in syslog-ng Agent

Purpose:

In case you experience problems with The syslog-ng Agent the BalaBit support team might request you to create debug logs for the application to help troubleshoot the problem. Complete the following steps.

> NOTE:
>
> The debug log is not suited to detect the reasons behind why a syslog-ng service could not start. The only way to check a non-starting agent service is to run it manually in debug mode (use the command **syslog-ng-agent.exe /D**). Make sure that if the *[AgentDbgLog]* part of the debug.ini file exists, it is set to *enabled=off*.

Steps:

1. To enable logging debug logs, enter the following lines in the debug.ini file:

   ```
   [AgentDbgLog]
   enabled=on
   ```

   Debug messages are written into the installation folder of the syslog-ng Agent under the syslog_ng_agent_dbg.log filename by default, if no other path is specified. To change the destination folder of the debug log file, enter a path in the path=<debug_file_folder_path> row.

   > **CAUTION:**
   >
   > **When using an optional path, make sure that syslog-ng Agent has the right to write it. Also, make sure that the path exists. Otherwise, syslog-ng Agent will not write into the file.**

   To apply the changes, restart the syslog-ng Agent after modifying the *[AgentDbgLog]* part of the debug.ini file.

   After the restart, a log message is automatically generated about the start of debug logging mode, with a timestamp and the path of the log file.

   Example 10.2. Debug logging enabled log message

   ```
   Apr 16 13:14:02 zts-win015 syslog-ng[252]: syslog-ng Agent debug mode
   is enabled; output file='.\syslog_ng_agent_dbg.log'
   ```

2.
3. Reproduce the error. It will be included in the debug log.
4. After solving the problem, disable debug logging, otherwise the log file will grow and might consume the available hard disk space. The log file contains the log messages received and processed by the syslog-ng Agent as well.

Procedure 10.3. Troubleshooting domain setting problems

Purpose:

If the domain settings are not downloaded to a domain host, the syslog-ng Agent (starting from version 3.0.6) can create a log file to debug why the domain settings are not updated on the client. Complete the following steps:

Steps:

1. To enable logging domain update errors, enter the following lines in the `debug.ini` file:

   ```
   [GpoDbgLog]
   enabled=on
   ```

   Debug messages are written into the installation folder of the syslog-ng Agent under the `syslog_ng_agent_gpo_dbg.log` filename by default, if no other path is specified. To change the destination folder of the debug log file, enter a path in the path=<debug_file_folder_path> row.

   ⚠ **CAUTION:**

   When using an optional path, make sure that syslog-ng Agent has the right to write it. Also, make sure that the path exists. Otherwise, syslog-ng Agent will not write into the file.

2. Select Start > Run > gpupdate to reproduce the error.

3. After solving the problem, disable logging domain update errors, otherwise the log file will grow every time when the domain settings of the client are updated.

Reading eventlog messages is slow

To read the messages from eventlog containers, the syslog-ng Agent for Windows application uses the native Windows API tools. The Windows platforms use an XML-based eventlog format. The API (called EVTX) that reads the XML-messages from the eventlog container and passes them to syslog-ng Agent is inherently slow, severely limiting the performance of syslog-ng Agent.

The API tools that syslog-ng Agent uses on the Microsoft Windows XP and 2003 Server platforms is available on the newer platforms as well, and can increase the speed of reading from eventlog containers, up to 500%. However, using this old API (called EVT) has limitations when used with XML-based eventlog containers.

Limitations of using the EVT API

When using the EVT API to read messages from XML-based eventlog containers, note the following limitations.

- The EVT API supports only containers are listed under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\** key in the registry. The three default containers (Security, Application, System) are listed here by default.
- Derived containers (for example, **microsoft-windows-bits-client/analytic**) are not supported.
- The following macros do not work, that is, their values will be empty: *${EVENT_CATEGORY}*, *${EVENT_MESSAGE_XML}*, *${EVENT_MSG_XML}*, and *${EVENT_TASK}*.
- The way how the EVT API provided by Microsoft reads the values of the XML-based is not perfect. Therefore, filters that use these macros might not work properly. The following list shows the known limitations and errors:
    - *${EVENT_LEVEL}*: The value of this macro can be incorrect. It will always be a number as expected, but not necessarily the correct value.
    - *${EVENT_SOURCE}*: It is possible that the value of this macro will be formatted differently. For example, **Microsoft-Windows-Security-Auditing** instead of **Microsoft Windows security auditing**.
    - *${EVENT_TYPE}*: The value of this macro is known to be incorrect in the following scenarios:
        - For security audit logs, if *${EVENT_LEVEL}* is 4, the value of the *${EVENT_TYPE}* macro will be **Audit Success** instead of **Information**. This is known to happen when the "Audit log cleared" event is generated.
        - For non-security audit logs, if *${EVENT_LEVEL}* is 0, the value of the *${EVENT_TYPE}* macro will be **Undefined** instead of **Information**.
    -

  - *${EVENT_USERNAME}*: The EVT API will always add value of the Username field to this macro. If the Username field of the event is empty, the EVTX API used the TargetUserName or the SubjectUserName instead, but this is not possible with the EVT API. For example, the Username field of events from the security container will be often **N/A**.

  - *${PRI}*: The value of this macro is based on the *${EVENT_LEVEL}*, therefore, it can be incorrect.

Procedure 10.4. Enabling the EVT API

Purpose:

To use the older, but faster EVT API to handle the eventlog containers (instead of the native EVTX API), complete the following steps.

Warnings:

- Hazard of data loss! If you change the API, the position of the last read message can be lost, causing the syslog-ng Agent application to duplicate or lose messages.
- The EVT API is not fully compatible with the EVTX API. Make sure to read the section called "Limitations of using the EVT API" before changing your configuration.
- Changing the API affects every eventlog container on the host. It is not possible to use the EVT API only for selected containers.

Steps:

1. Start the configuration interface of the syslog-ng Agent for Windows application.
2. Select syslog-ng Agent Settings > Eventlog Sources > Eventlog Properties.
3. Select Enable.
4. Select Event API > Event Logging (EVT).

   > NOTE:
   >
   > By default, the syslog-ng Agent for Windows application uses the native API on every platform: EVT on Windows XP and Server 2003, and EVTX on Windows.

5. Select Apply, then OK. To activate the changes, restart the syslog-ng Agent service.

   Expected result:

   The syslog-ng Agent for Windows application uses the EVT API to read messages from the eventlog containers, improving the performance.

Debug bundle on Windows

To create a debug bundle that you can attach to your support ticket, use the **syslog-windebun** application. For details, see syslog-windebun.ps1.

Configuring the auditing policy on Windows

This section describes how to configure the logging and auditing policy on various versions of Microsoft Windows. The syslog-ng Agent can transfer log messages only about those events that are actually logged, so the audit policy has to be configured to log the important events.

Microsoft Windows operating systems can record a range of event types, from a system-wide event such as a user logging on, to an attempt by a particular user to read a specific file. Both successful and unsuccessful attempts to perform an action can be recorded. The audit policy specifies the types of events to be audited. When such an event occurs, an entry is added to the log file of the computer.

Following is a brief overview on how to configure the audit policy on various versions of Microsoft Windows. For details, consult the documentation of your operating system, or visit Microsoft TechNet. For details on configuring the auditing and logging of various applications, like the IIS Server or the ISA Server, consult your product documentation.

Procedure 11.1. Turning on security logging on Windows XP

Purpose:

The following procedure describes how to enable security logging on Windows XP Professional hosts.

Steps:

1. Login as an administrator.
2. Click Start, click Run, and type mmc /a.
3. On the File menu, click Add/Remove Snap-in, and click Add.
4. Under Snap-in, click Group Policy, and click Add.
5. In Select Group Policy Object, select Local Computer, then click Finish, click Close, and click OK.
6. In Console Root, select Local Computer Policy, then click Audit Policy.
7. Right-click the attribute or event you want to audit on the details pane.
8. Set the desired options in the Properties.
9. Repeat Steps 7-8 for every other event you want to audit.

> NOTE:
>
> For details on how to remotely enable security logging for workstations, member servers, and domain controllers, see Procedure 11.2, “Turning on security logging for domain controllers”.

Procedure 11.2. Turning on security logging for domain controllers

Purpose:

The following procedure describes how to enable security logging on a Windows XP Professional domain controller.

Steps:

1. Login as an administrator.
2. Click Start, point to Programs, point to Administrative Tools, and click Active Directory Users and Computers.
3. In the console tree, click Domain Controllers.
4. Click Action, then click Properties.
5. On the Group Policy tab, select the policy you want to change, and click Edit.
6. In the Group Policy window, in the console tree, click Audit Policy.
7. Right-click the attribute or event you want to audit on the details pane.
8. Set the desired options in the Properties.
9. Repeat Steps 7-8 for every other event you want to audit.

Procedure 11.3. Turning on auditing on Windows 2003 Server

Purpose:

The following procedure describes how to configure auditing on a Windows 2003 Server host.

Steps:

1. Login as an administrator.
2. Click Start, point to Programs, point to Administrative Tools, and click Domain Security Policy.
3. In the console tree, click Local Policies, then Audit Policy.
4. Double-click on an event and select the Define these policy settings option.
5. Select the type of event to log: Success or Failure.
6. Repeat Steps 4-5 for every other event you want to audit.

Name

syslog-windebun.ps1 — syslog-ng WINdows DEBUg buNdle generator PowerShell script

Synopsis

```
powershell C:\PATH\TO\syslog-debun.ps1
```

Description

The **syslog-windebun** application is a powershell script that collects information about its environment into a file, to help troubleshoot syslog-ng Premium Edition and syslog-ng Agent for Windows installations.

The **syslog-windebun** application application is distributed with the syslog-ng PE system logging application, and is usually part of the syslog-ng Premium Edition package or the syslog-ng Agent for Windows package. The latest version of the is available at the syslog-ng Downloads page. You can also contact the One Identity Support Team and request the latest version of the script.

Using syslog-windebun

The application requires PowerShell 2.0 or later. Administrator privileges are not required.

To use **syslog-windebun**, run the application in an interactive powershell terminal. On 64-bit Windows, use the 64-bit PowerShell terminal.

Example:

```
powershell -NoProfile -ExecutionPolicy RemoteSigned C:\PATH\TO\syslog-debun.ps1
```

The script collects the information about the syslog-ng PE environment into a file, and displays the location of this file. When creating a support ticket, attach this file to the ticket to help our support team troubleshoot your problem. The following is an example output.

```
PS C:\Users\balabit> C:\Users\balabit\Downloads\syslog-windebun.ps1
syslog-ng Agent is installed
Start gathering Agent related information
Finished gathering syslog-ng Agent information
syslog-ng PE is installed
Start gathering syslog-ng PE related information
Finished gathering syslog-ng PE related information
Starting to gather system related information
Finished gathering system related information.

The resulted zip file is found where you started running the program.

Please send the following file to Balabit Support:
C:\Users\balabit\syslog-windebun-CjZ.zip
```

Data collection policy

The **syslog-windebun** application collects the following information into a file.

- Routing information
- System information
- Network statistics
- Network port information
- IP configuration
- The XML configuration file of syslog-ng Agent for Windows
- Registry information of syslog-ng Agent for Windows
- The content of the `etc` folder of syslog-ng Premium Edition
- PowerShell and .NET version
- syslog-ng Premium Edition and syslog-ng Agent for Windows version
- Installation logs of syslog-ng Premium Edition and syslog-ng Agent for Windows version

Files

```
/opt/syslog-ng/bin/dqtool
```

Author

This manual page was written by the One Identity Documentation Team <documentation@balabit.com>.

Copyright

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product