LogTag Recorders

LogTag® Analyzer

Network Administrator Guide

Software Revision 2.6r9, Document Revision 1.1,

Published 18. March 2016

Table of Contents

Disclaimer

Most techniques described in this guide are directed towards experienced IT professionals who are familiar with the procedures required. Some of the techniques involve:

- editing the registry
- administering Active Directory users
- creating GPO's
- creating msi transforms
- remotely distributing registry keys
- remotely distributing files to users

If you do not have experience with network administration or the techniques described do not attempt these procedures, as they can partially render your infrastructure non-functional if applied incorrectly. Please also consult the help function of your operating system to learn about the consequences of editing the registry.

No representation or warranty is given and no liability is assumed by LogTag® Recorders with respect to the accuracy or use of the information provided or infringement of patents or other intellectual property rights arising from such use or otherwise. LogTag® Recorders shall not be held liable for any consequences arising from the application of these procedures.

http://www.logtagrecorders.com

Who should read this manual?

This User Guide is directed at IT professionals who are tasked with the installation of LogTag® Analyzer and its support software. Some of the procedures apply to stand-alone PC installations, others to both stand-alone and networked PC's.

Before you start deployment we recommend you read the manual in its entirety and familiarise yourself with all concepts presented.

The procedures and techniques described in this manual have been implemented and tested on all Microsoft Windows™ user operating systems currently supported by Microsoft. The network installation methods have been tested in a Microsoft Windows® Server 2008 environment, a Microsoft Windows® Small Business Server 2008 environment and -with small modifications- in a Microsoft Windows® Small Business Server 2003 environment. The same techniques are applicable for other server operating systems, but may require additional steps or further modification.

New in this Version

The USB drivers now include released and signed drivers for Windows 2010.

Previous Changes

The section about copying user data now references the **asxml method** described in Moving User Settings (on page 57) and not the method using the **User Profile.dat**. If you still need to use this older method, please refer to one of the earlier version of this guide.

If you have any questions regarding this manual or the procedures described, please email software@logtagrecorders.com.

Chapter 1
Files and Folders

LogTag® Analyzer uses a number of files during its installation and while it is running. Requirements for these files, their extensions and the folders they are saved in depend on the method of installation and the level of customisation desired. This chapter explains what each of the files does, why you may need it and where it is used.

In this section:

Standard Installer

The standard installer downloaded from the LogTag® Recorders website contains a single executable file, named **logtag_analyzer_2.6r9.exe** or similar. This file includes all files and sub-installers required to install and run the software. The installer language can be chosen on start-up and all required files are included to operate the software in different languages.

You will require local PC administrator permissions to run this installer.

USB Installer Package

Occasionally the USB interface drivers will not install correctly when downloaded from Windows Update. You can download and run the USB driver installation package **USB_Interface_Cradle_Driver_Installation_1.10.exe**, which will uninstall all driver files currently installed, and re-install the latest package for the respective operating system. The standard installer for LogTag® Analyzer includes this package starting with version 2.5r17. It is available through the Start menu shortcut after installation of LogTag® Analyzer has completed.

Microsoft Installer File

To make the process of a network distributed installation easier, LogTag® Recorders have published an installer file **logtag_analyzer_2.6r9.msi**, which is different to the stand-alone installer. This *.msi file allows remote installation without the need to provide local administrator credentials during the installation. It also offers other benefits, for example creation of system restore points before the installation begins.

The file can be downloaded from the software download page on the LogTag® Recorders website at http://www.logtagrecorders.com/.

The installer contains all files to operate the LogTag® Analyzer software in the different supported languages, however the installer is English only, as most network deployments would run this silently. The installer file does not contain the USB interface driver files, which must be downloaded and installed separately.

Depending on your requirements you may also need the files described next.

USB Driver Files

To communicate with LogTag® USB interfaces you will require the following USB driver files. It is likely all driver packages will be required in your organisation.

- **USB32_2.12.10.msi** or **USB64_2.12.10.msi**

  These are the USB interface driver installers for the following 32-bit and 64-bit operating systems:

  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- **USB32_2.8.24.msi** or **USB64_2.8.24.msi**

  These are the USB interface driver installers for the following 32-bit and 64-bit operating systems:

  - Win XP
  - Windows Vista
  - Windows Server 2003
  - Windows Server 2003 R2
  - Windows Server 2008

You need to make sure you deploy the correct driver for the OS of the client computer. The correct driver can also be downloaded from Windows Update at the time the interface is plugged in, but this requires access to the Microsoft Update website and local administrator privileges.

USB Firmware Updater

From time to time LogTag® Recorders will publish firmware updates for its range of USB recorders, allowing the introduction of new features to products already in the hand of users.

The updater software is contained in one or more self-contained executable files called **USB_Firmware_Updater.exe** or similar and can be installed:

- automatically as part of LogTag® Analyzer 2.6 and higher, either via the standard installer or via the *.msi file. Shortcuts will also be installed.
- via a stand-alone installer package, that can be downloaded from LogTag's website. This package is called **LT_UTRIX_Update_6171_11r4.exe** or similar and will not only install the updater, but also check the presence of required operating system features such as .NET 4.0.

The updater can also be used to automatically upgrade recorders that are incompatible with a certain version of software. In this case the software will display a warning and give you a chance to update the product.

You can find more information about the USB Firmware Updater in the on-line help at http://www.logtaganalyzer.net/help/usbupdater/Content/Updater/USB_Firmware_Upgrader.htm

User Profile.dat

LogTag® Analyzer stores most of its settings in a binary file called **User Profile.dat**. This file is unique to each PC user account and located in the corresponding roaming profile location (%APPDATA%\LogTag). This location cannot be changed.

If the file does not exist when LogTag® Analyzer is first started, it is created with default settings.

For installations in languages other than US-English a **User Profile.dat** file is copied to the roaming profile location by the installer. This file contains the default settings plus the setting for the language chosen during installation, so LogTag® Analyzer can show that language when first started.

File and folder names in the User Profile.dat file can contain system variables, so a common file can be used for different users and be created in a lab installation before moving it to production machines. This can be of particular interest with more complicated settings such as FTP and SMTP connection details.

The options configurable in LogTag® Analyzer are detailed in the LogTag® Analyzer User Guide and not explained here.

When you change options via the **Edit - Options** menu, the **User Profile.dat** file will be updated when you exit LogTag® Analyzer.

Profile.ltp

The Profile.ltp file is a binary file that contains one or more recorder configuration profiles. When LogTag® Analyzer is used and the first profile is saved, this file is created and saved to the My LogTag Data\Configuration folder. The file can be moved or copied to different users, folders or installations running the same revision of LogTag® Analyzer, but not earlier versions.

Profile files do not require to be named Profile.ltp, however on creation this name is set by default. LogTag® Analyzer will remember the last file used, unless User Profile.dat is deleted or a new location set via an XML import.

*.asxml Files and AutoImportSettings.asxml

LogTag® Analyzer's customisation options can be set by importing a well formed XML file with an *.asxml (for **A**nalyzer **S**ettings **XML**) file extension. When this file meets certain conditions (amongst others it must be called **AutoImportSettings.asxml**), it can also be automatically imported when LogTag® Analyzer first starts.

Although it is possible to choose a different file extension for importing settings, only *.asxml is registered with the operating system and can be used for automatic import.

Once imported, the settings in this file will replace the settings loaded from the **User Profile.dat** file. When LogTag® Analyzer is closed, the new settings will be saved in the **User Profile.dat** file and become persistent.

Please refer to the sections about Importing Option Settings on page 1 and Automatically Importing Options via XML on page 54.

DftLogo.jpg

This file contains the logo, which is displayed on the report tab both on screen and on the PDF export. Further details about this file are explained in the section about Adding a Custom Logo to Reports and PDF files on page 62.

Folders

Following folders are used in the default configuration of LogTag® Analyzer. Some of these folders can be customised to suit.

- My Documents\My LogTag Data

  Default storage location for the downloaded data files and configuration logs

- My Documents\My LogTag Data\Configuration Profiles

  Default storage location for configuration profile files

- %APPDATA%\LogTag

  Storage location for the User Profile.dat file

- My Documents\My LogTag Data\Templates

  Storage location for the logo file

- Program Files\LogTag Recorders LTD\LogTag® Analyzer

  Default location for the program executable, (x86) on 64-bit PC's

- Program Files\LogTag Recorders LTD\LogTag® Analyzer\Examples

  Storage location for the sample files included with LogTag® Analyzer

LogTag® Analyzer also makes use of the Operating System's temporary folder. This folder must be on the local computer and cannot be on a networked locations. If this folder cannot be local, please follow the instructions about the Temporary Folder on page 73

File Extensions

Following file extensions get registered with the operating system upon installation of LogTag® Analyzer. More information about each file type can be found in the LogTag® Analyzer User Guide. Files with these extensions can be opened with Analyzer by

double clicking in Windows Explorer, drag-and-drop or right-clicking the file in Windows Explorer, then clicking **Open**.

- .ltd

  This is LogTag® Analyzer's native, encrypted data format.

- .sltd

  This is a LogTag® Analyzer native, encrypted data format, which limits the zoom settings to the zoom set at the time of saving the file.

- .multi

  This is a LogTag® Analyzer native, encrypted data format, which contains the settings how individual charts from a multi-chart relate to each other.

- .asxml

  This is an editable file format containing import data.

Following file extensions are used by LogTag® Analyzer, but not registered with the operating system:

- .dat

  For the User Profile.dat file

- .anno

  Contains annotation s for a .ltd file.

- .ltp

  Contains recorder configuration profiles.

- .ehx

  Firmware updater file

Chapter 2

Installing LogTag Analyzer as an Administrator

Local administrator permissions are required when installing LogTag® Analyzer on-site.

If the account used to install Analyzer has administrator permissions, and no other account on the PC requires the software, you can perform the installation with the standard installer, then adjust settings to suit.

If the installation is made using an account with administrator permissions, but additional standard users on the PC also need access to the software, you may need to perform some additional steps once the standard installer has completed:

- The **User Profile.dat** file for non-US English installations will not be copied to standard users. If the start-up language for standard users needs to be non-US English, the techniques described in the section about "Automatically Importing Options via XML" on page 54 need to be used.
- The MRU list for standard users will not be populated with the example files, but users can still browse to the files and open them using **File - Open**.
- USB drivers are always installed for all users.

If the installation is distributed remotely, please follow the instructions in the section about Network Installation of LogTag® Analyzer on page 14.

Chapter 3

Network Installation of LogTag® Analyzer

Network installation requires following steps:

As with many things IT related there are a number of ways software deployment can be achieved. The following procedures describe one specific way, using the tools provided within the operating system. There are others that work equally well, and many 3rd party tools are available for purchase, which assist considerably in deployment.

Before you continue with deployment, please download the files from the Network Administrator section of the LogTag® Analyzer download page.

Setting up Active Directory

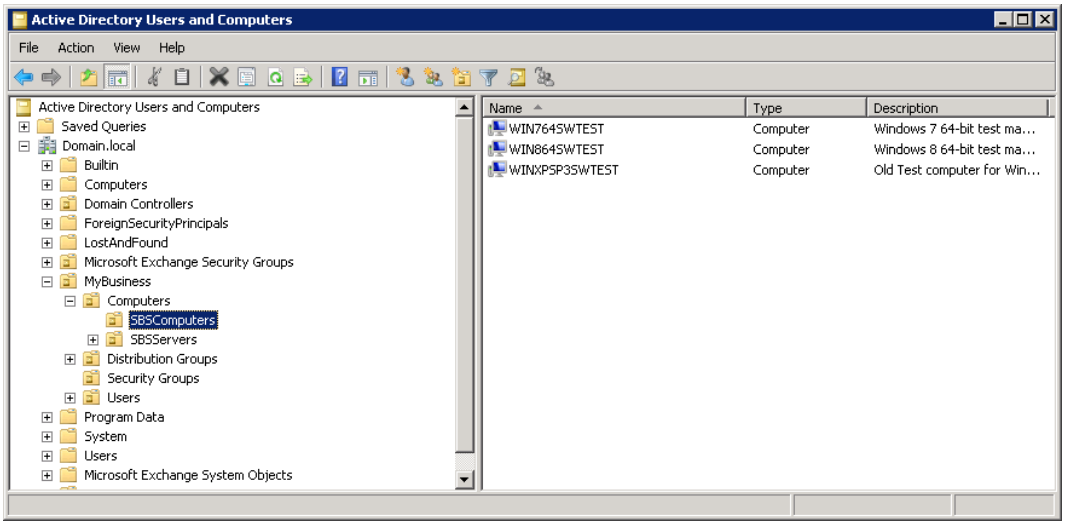
AD governs the rules under which Group Policy Objects are applied. Before you can distribute LogTag® Analyzer remotely, you will need to determine which users and computers will be allowed to receive this software.

There are many ways to achieving this; one of them is described here where the GPO is linked to OU's containing users and computers, and then applying security filters to determine which computers and users the GPO applies to. WMI filters are then used to restrict the GPO to computers with operating systems supported by LogTag®

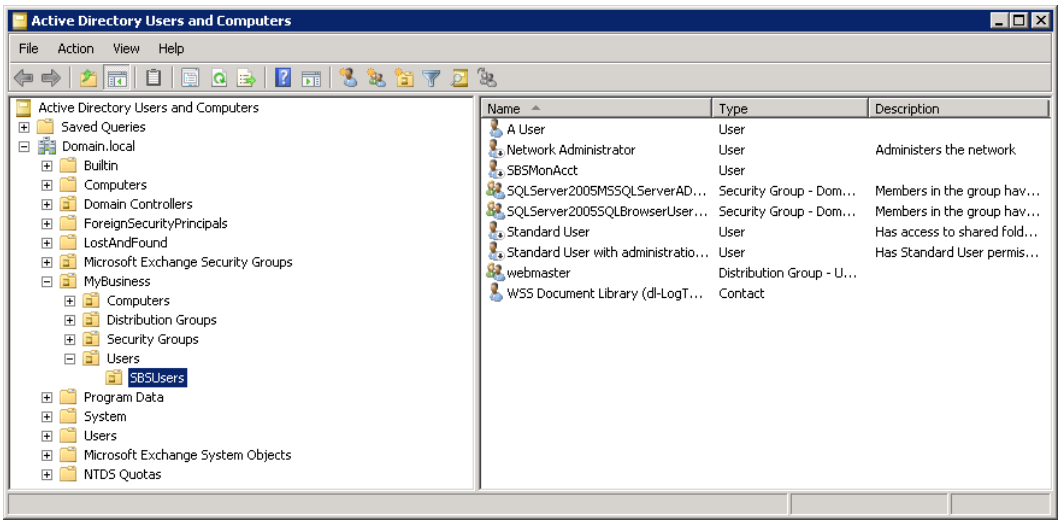
Analyzer. You will likely need to create more than one GPO if you need to deploy USB drivers to a variety of different operating system, as the latest driver is only certified for use with Windows versions 6.1 and later. This requires an earlier driver to be used for 6.0 and below.

Determining Organizational Units

- Choose an OU which contains the computers dedicated to running LogTag® Analyzer. You may wish to create a new OU containing these computers, or you may simply allow all computers in an already existing OU. In this example the OU "SBSComputers" has been selected.



- Determine an OU which contains users which will be allowed to use LogTag® Analyzer. You may create a new OU and add members, or you may choose an existing OU. In this example the "SBS Users" OU has been selected.



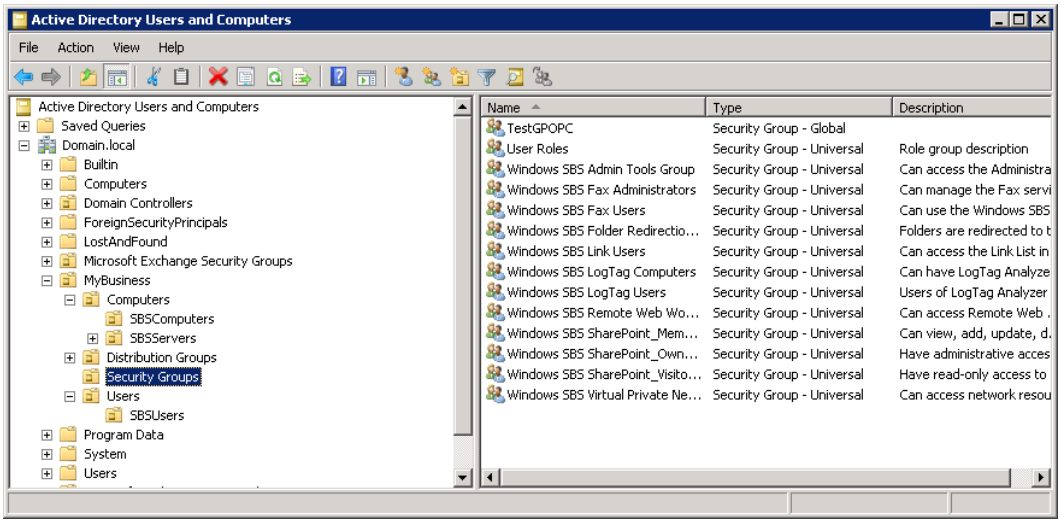
New OUs can be set up through the ADUC management console or through third party applications.

Setting up security groups

You can use security groups to restrict the deployment to a sub-set of computers and users. Please consult the operating system's help for more information on this topic.

In this example two dedicated security groups have been created:

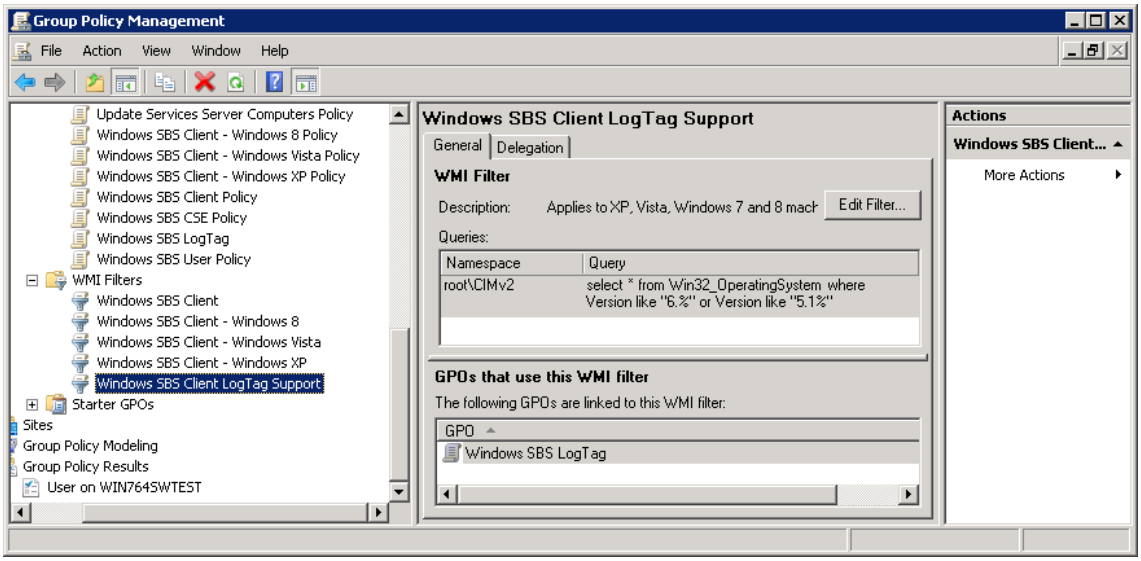
- The Windows SBS LogTag® Computers group, containing all computers on which LogTag® Analyzer will be installed.
- The Windows SBS LogTag® Users group, containing all users who will have access to LogTag® Analyzer.



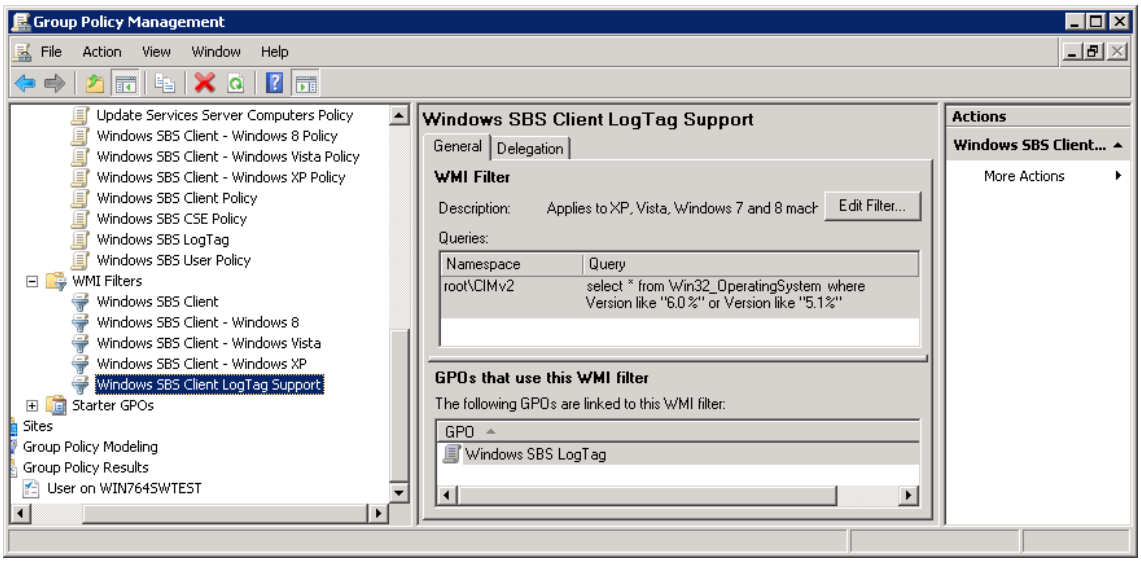
Setting up a WMI filter

It is good practice to limit installations to computers with operating systems who support the application to be installed. LogTag® Analyzer can be installed on Windows XP and later operating systems, so the WMI filter should look like this:

The query statement is **select * from Win32_OperatingSystem where Version like "6.%" or Version like "5.1%"**



To set the WMI filter for Win XP, Windows Vista, Windows Server 2003 and Windows Server 2008 use the query **select * from Win32_OperatingSystem where Version like "6.0%" or Version like "5.1%"**.



To set the WMI filter for Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 use the query **select * from Win32_OperatingSystem where Version like "6.1%" or Version like "6.2%"or Version like "6.3%"**.

You can set up the WMI filter to also include the processor environment by adding a statement **AND NOT OSArchitecture = "64-bit"** or **AND OSArchitecture = "64-bit"** or similar to the end of the query; this, however, will require separate GPOs for each different driver package. Allocating a driver package to an OS Architecture can be defined when you add the USB driver packages to the GPO later, which limits the number of required GPOs.

This concludes the set-up required in AD.

Creating Group Policy Objects

We will be using Group Policy to deploy LogTag® Analyzer to selected computers. You can find more information about the Group Policy Object concept on the Microsoft® Technet and your Windows Server® documentation.

In this step we will create the GPO, link it to the correct OU's and provide for the correct initial policy settings.

This is only one of many ways to achieve this outcome. You can create separate GPO's for user settings and computer settings, limit distribution of 64-bit and 32-bit drivers through different WMI filters or use one of many Microsoft or third party deployment tools.

- Start the Group Policy Management console. Expand the Group Policy Management tree to the domain and select Group Policy Objects

  Create a new Group Policy Object and call it Windows SBS LogTag. Depending on your time table you may wish to set the GPO status to **All settings disabled**, until all your settings have been entered.

- Right click the OU containing the LogTag computers and select **Link an Existing GPO...**. Choose GPO created earlier and make it **enforced**.

- Right click the OU containing the LogTag users and select **Link an Existing GPO...**. Choose GPO created earlier and make it **enforced**.

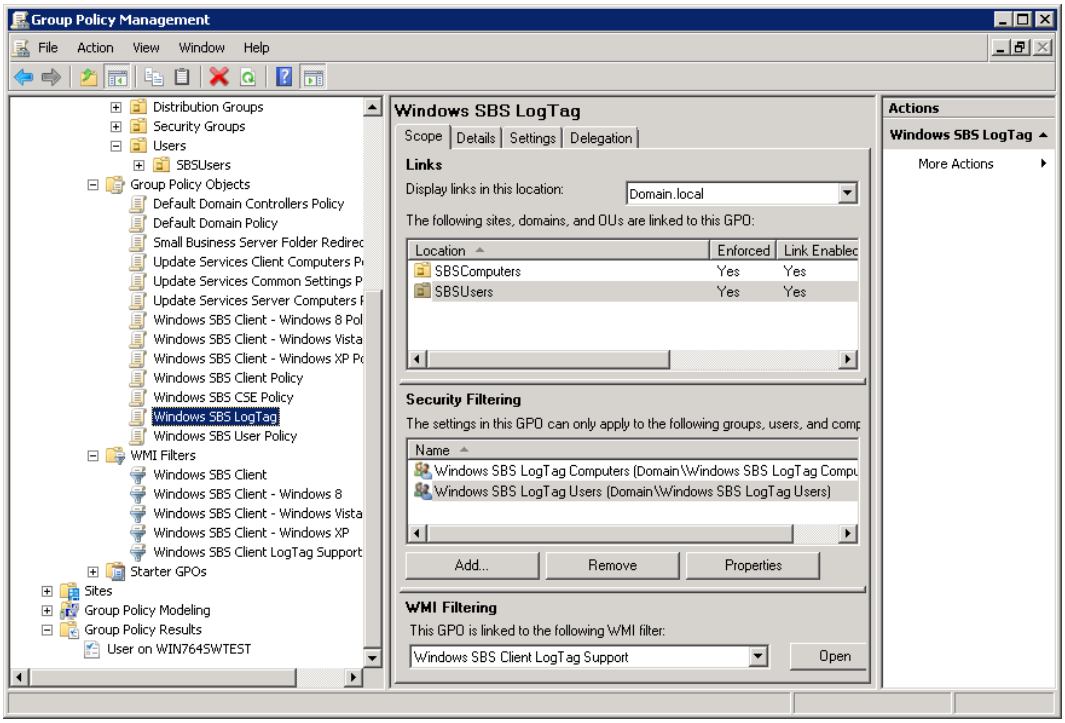
- In the GPMC expand Group Policy Objects and edit the GPO just created.

- In the Group Policy Management Editor expand **Computer Configuration - Policies - Administrative Templates - System - Logon**. Click on **Always wait for network at computer startup and logon** and click **Properties**. Select **Enabled**. This is recommended particularly for computers running Windows XP. Click OK and collapse the node.

- Close the GPME

- The GPO **Links** section in the **Scope** tab will be pre-populated with the previously selected OU's. In the **Security Filtering** section, add the chosen users, groups or computers.

- Add a WMI Filter appropriate for LogTag® Analyzer as created earlier. Supported operating systems are Windows XP Professional and later.



It can be difficult to determine the final outcome of which computer/user combination a GPO is applied to. It is sometimes easier to use two separate GPOs, one for the user, one for the computer, and separate settings associated with computers from settings associated with users.

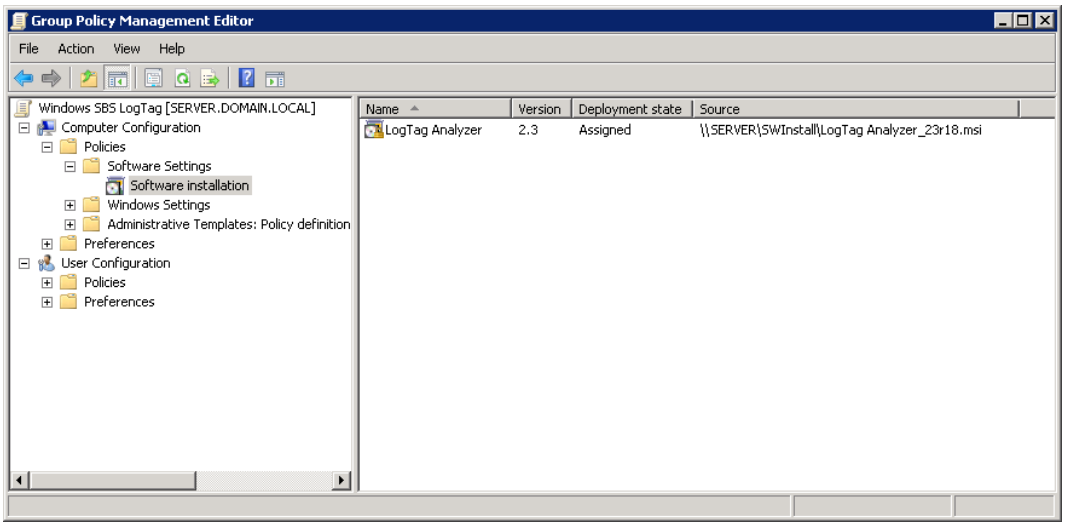
This concludes the initial set-up of the Group Policy Object.

Adding the Application Package

LogTag® Analyzer network distribution uses a different installer file to the stand-alone installation. This *.msi file is a 32 bit, English language only Windows Installer package. The method described does not require domain users to have elevated user privileges to perform the installation.

- Open the previously created GPO in the GPME.
- Expand the node **Computer Configuration - Policies - Software Settings** and click on **Software Installation**.
- Add a new package. Browse to the LogTag® Analyzer *.msi file and click **Open**. Select **Assigned** if you do not require a custom installation path, or **Advanced** if you do. The standard installation path is \Program Files\LogTag Recorders\LogTag Analyzer for 32-bit operating systems and \Program Files (x86)\LogTag Recorders\LogTag Analyzer for 64-bit operating systems. Click **OK**.

Please note you must browse to or enter a UNC location in the form of **\\Computername\Sharedfolder**, **not** the local location of the file, and add -as a minimum- read permissions for the security group for this location, so those users have access to this location via the network.



- Edit the properties of the package. In the **Deployment** tab, click on **Advanced** and select the **Ignore language when deploying this package** option.

  Important: Since this is a 32-bit package you must also ensure the **Make this 32-bit X86 application available to Win64 machines** option is **selected**, so the package is installed for both operating system types.

- Click **OK - OK**

- If you have chosen to use a custom installation path, click on the **Modifications** tab.

  The only time you can apply a modification to the installer package is during the first set-up of the properties.

  Add the transform file (see Creating a Custom Installation Path).

When you have finished, click **OK**. This concludes the application package installation.

Distributing the USB Driver Package

The USB interfaces used for communication between LogTag® recorder products and the LogTag® Analyzer software require a device driver to work. The device driver is available for download from Windows Update, however depending on your specific network policies this may not suit, which is why 64 bit and 32 bit packages of the driver installer have been made available to you for different operating systems. You need to include the package for which a remote installation is targeted; if both

operating system types and both processor architectures will be targeted by the GPO, separate policies need to be created and all packages included.

Regardless of whether you intend to install drivers through Windows Update or the installation package, you will need to allow users without elevated permission level to install the driver. This is achieved through an Administrative Policy, which can be set in the Group Policy Object.

- Open the GPO in the GPME.
- Expand the node **Computer Configuration - Policies - Administrative Templates - System - Driver Installation**. Click on **Allow non-administrators to install drivers for these device setup classes** and click on **Properties**.
- Select **Enable** and click on **Show**.
- Click on **Add**
- In the **Add Item** dialogue window enter the GUID {36fc9e60-c465-11cf-8056-444553540000}, including the braces. Click **OK - OK - OK** and close the node.

You can now add one or both driver packages for the target operating system. Please make sure you choose the correct driver for the operating system.

- Expand the node **Computer Configuration - Policies - Software Settings** and click on **Software Installation**.
- Add a new package. Browse to the USB Interface Cradle Drivers *.msi file and click **Open**. Select **Assigned** and click **OK**.

  Please note you must browse to or enter a UNC location in the form of **\\Computername\Sharedfolder**, **not** the local location of the file, and add -as a minimum- read permissions for the security group for this location, so those users have access to this location via the network.
- Edit the properties of the package. In the **Deployment** tab, click on **Advanced** and select the **Ignore language when deploying this package** option.

  Important: For the 32-bit package you must also **de-select** the **Make this 32-bit X86 application available to Win64 machines** option, or the driver installation will fail.
- Click **OK - OK - OK** and close the node.

Repeat the process for any additional GPOs.

This concludes the driver package installation.

Creating a Custom Installation Path

Unlike with earlier versions (prior to 2.3) you can no longer directly specify a new installation folder for installation of the LogTag® Analyzer software.

You will now need to do this in the GPO context through a **Transform**, created by the Windows Installer package editor "Orca". This editor is available for download from a number of locations on the internet and can be found through common search engines. Please contact LogTag® Recorders if you need assistance locating this software.

- Start Orca and open the *.msi file.
- Create a new Transform
- Browse to "CustomAction"
- Locate the SET_APPDIR property. Edit the "target" column and provide your custom installation path.
- Save the transform in a location accessible to all users/computers for the GPO.

  Please note you must be able to browse to or enter a UNC location in the form of **\\Computername\Sharedfolder**, **not** to a local location, so users have access to this location via the network.

This concludes the creation of a custom installation path.

Distributing Global User Settings

Distributing Global User Settings

Although this method works, we recommend distributing user settings via the Automated XML import function described on page 54 for the following reasons:

- It wraps the deployment of configuration profiles into a single distributed file.
- A set of default options can be imported for new users, and also if users delete their User Profile.dat file
- It allows greater control over individual option settings

Explanations for each of the settings can be found in the LogTag® Analyzer User Guide, in the section about **Customising the software**, so are not repeated here.

Creating the settings file

- Create a test installation of LogTag® Analyzer in the same domain as the users will operate, with access to the same storage locations.
- Open LogTag® Analyzer and make all required settings. Use system variables if desired for the storage folder location of the downloaded files.
- Import any read-only profiles, customisation data or any other data you wish via an XML import file. More information about the XML file option can be found in Importing Option Settings via an XML file on page 34
- Close LogTag® Analyzer, so all changes are written to the file. Locate the **User**

Profile.dat file in the roaming profile (in %APPDATA%\LogTag®) and copy it to a network accessible location.

Distributing the settings file

This file is deployed once when the GPO is applied.

- Open the GPO in the editor. Expand the node **User Configuration - Preferences - Windows Settings** and click on **Folders**.
- Create a new folder. Set its properties as follows:
  - On the **General** tab select the action **Create** and enter **%APPDATA%\LogTag** in the path field.
  - On the **Common** tab enable **Run in logged-on user's security context** and **Apply once and do not reapply**.
- Expand the node **User Configuration - Preferences - Windows Settings** and click on **Files**.
- Create a new file. Set its properties as follows:
  - On the **General** tab select the action **Create** and enter the location of the source file.

    Please note you must browse to or enter a UNC location in the form of **\\Computername\Sharedfolder\User Profile.dat**, **not** the local location of the file, and add -as a minimum- read permissions for the security group for this location, so those users have access to this location via the network.

    In the Destination File field enter **%APPDATA%\LogTag\User Profile.dat**.
  - On the **Common** tab enable **Run in logged-on user's security context** and **Apply once and do not reapply**.

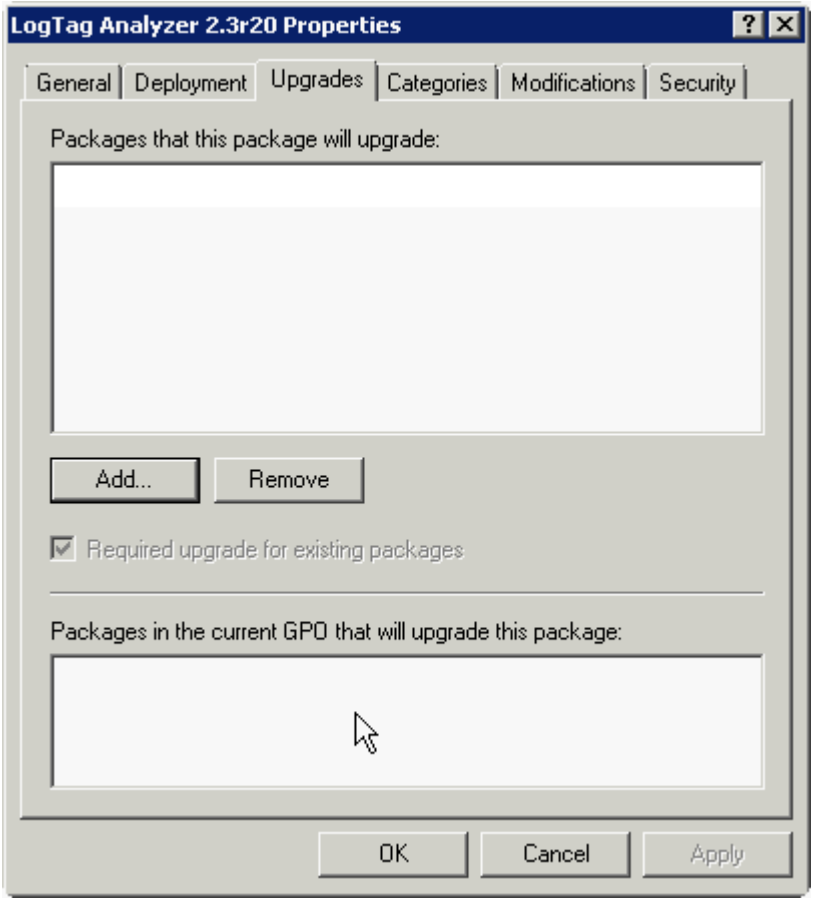
Close the GPME. The custom settings will be distributed when the GPO is deployed.

This concludes editing the GPO for distribution of custom settings.

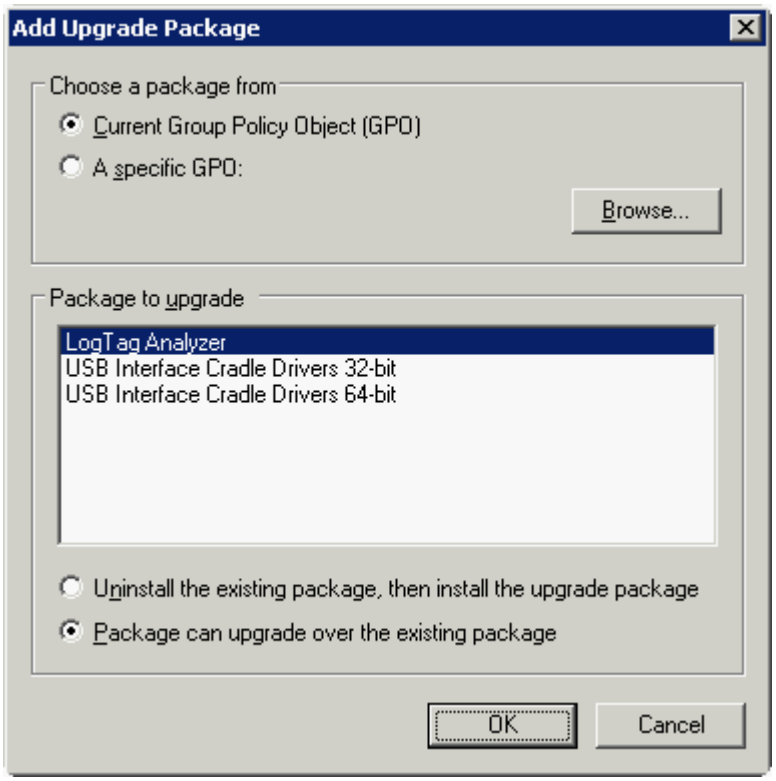
Updates

LogTag Recorders LTD will publish updated software from time to time. You can always download the *.msi package of the latest version from the LogTag Recorders LTD website.

To deploy an update through GPO add the new *.msi package to the **Computer Configuration - Policies - Software Settings** node in the same way you have added the original package, either to a newly created GPO, or to the original GPO.



In addition to the tasks described in Adding the Application Package (on page 19), go to the **Upgrades** tab and click **Add** to choose the previous *.msi file.



Select the GPO containing the old package, and select **Package can upgrade over the existing package**.

Troubleshooting

The software is not being deployed

The number one reason for deployment to fail is the fact the GPO has not been applied to the correct user/computer. To check, either use the **Resulting Sets of Policy snap in (rsop.msc)**, the **gpresult** command line tool or the **Group Policy Results** tool from the GPMC.

It is also possible Group Policy deployment has not bee refreshed. In this case run **gpupdate /force** in a command window with administrator privileges.

The GPO has been set to **All settings disabled**. Enable all settings and refresh Group Policy.

Finding more help

There are many good articles on the Microsoft Technet Website which assist in troubleshooting GPO related issues. Due to the uniqueness of each server installation we can only provide limited assistance.

Chapter 4

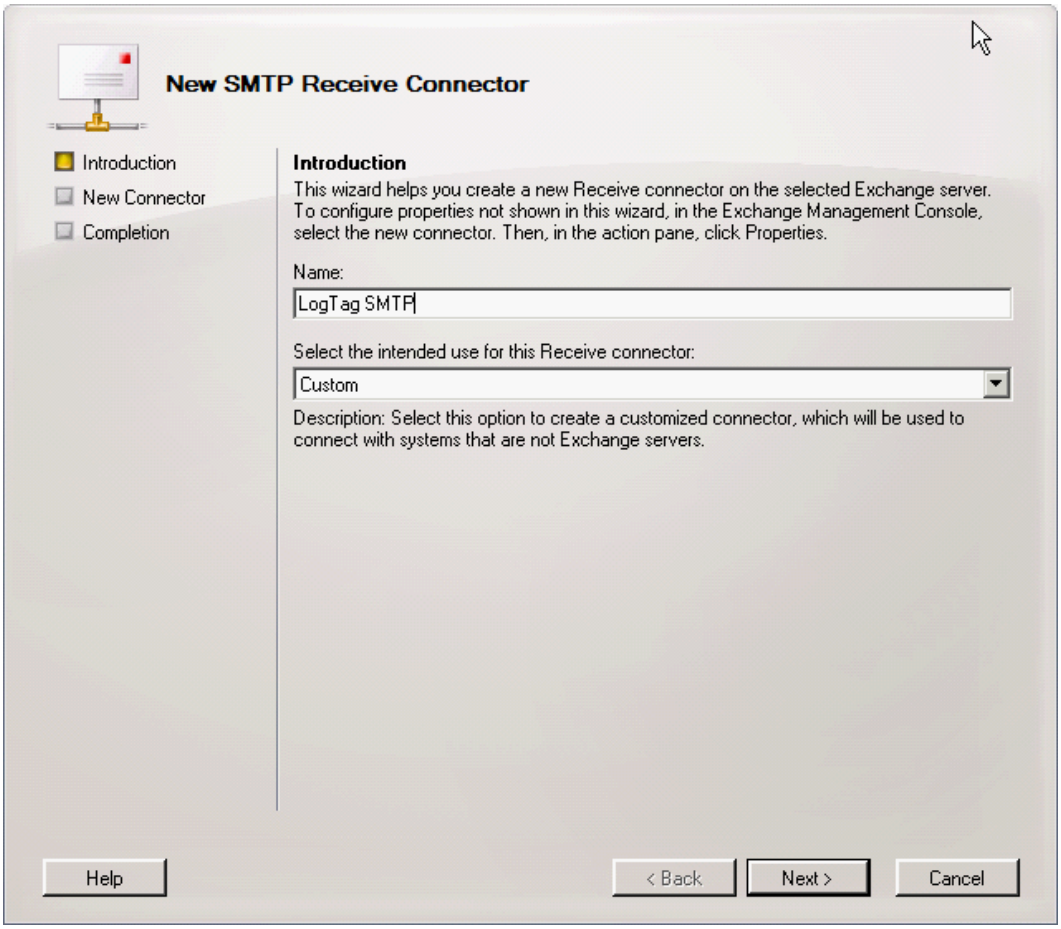
Creating a Microsoft Exchange Connector

In its default settings Microsoft Exchange needs a dedicated SMTP connector or a correctly set up virtual SMTP server to relay any application server's SMTP request to the outside world. This is not a restriction of LogTag® Analyzer, but of the settings in the Exchange server and affects any application sending automated e-mails via Exchange (other examples would be CRM software sending automated e-mails or a photocopier sending e-mail for scans).

Depending on your specific IT network setup this may already have been done in your organisation.

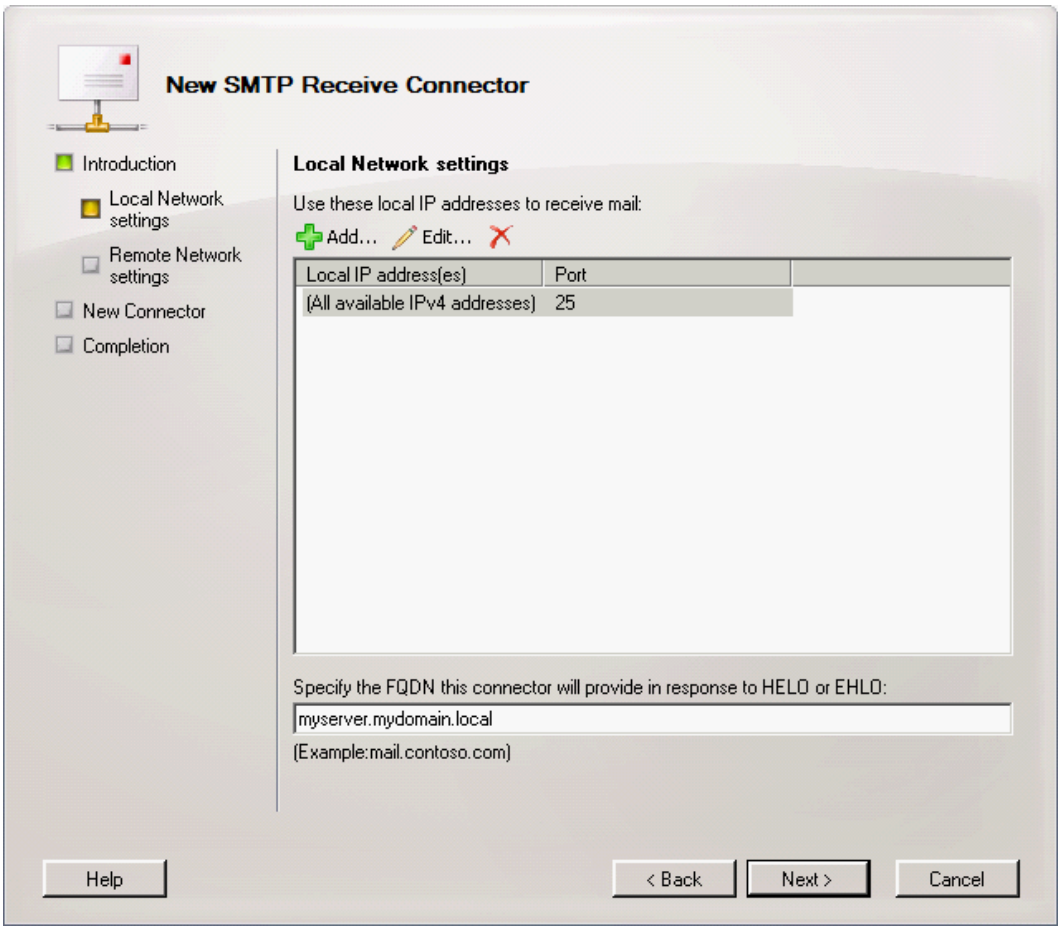
The basic steps to implement are as follows:

1. In the Exchange Management Console, add a new receive connector in the **Receive Connectors** tab of the **Hub transport** node.

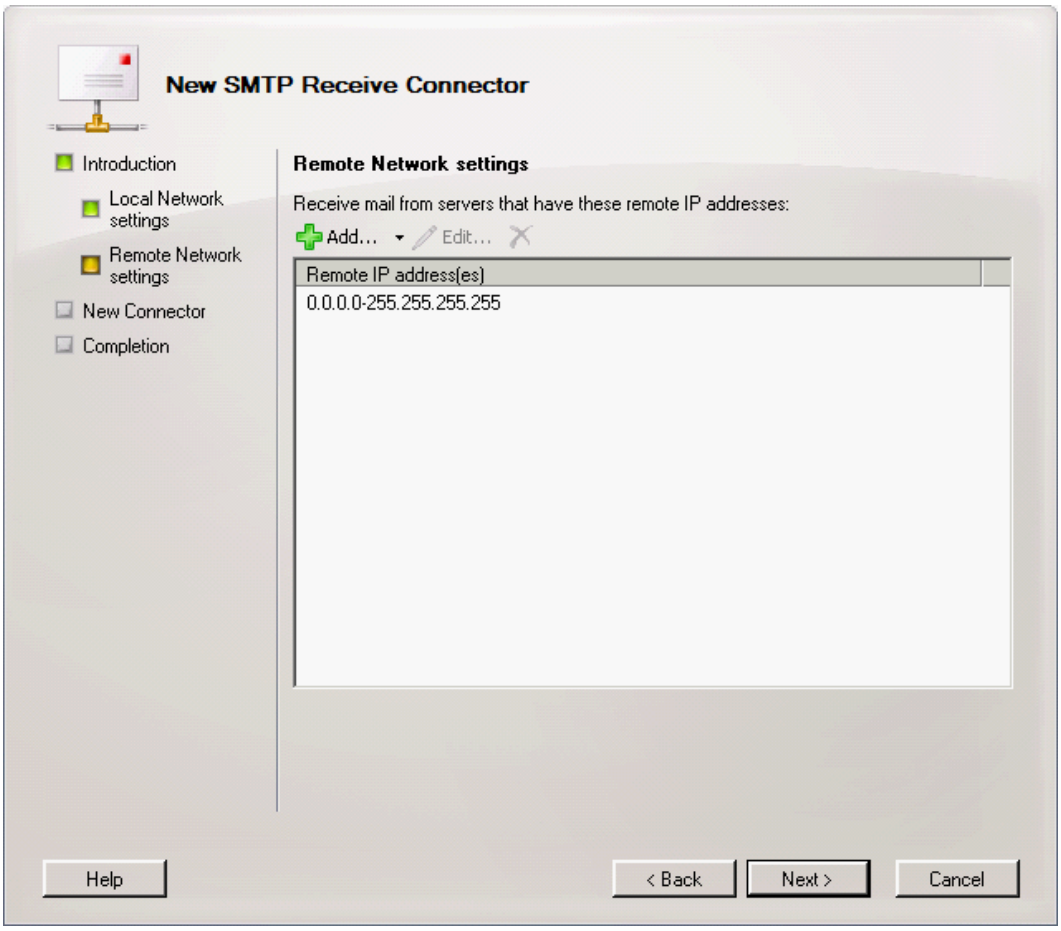


Name it and click next.

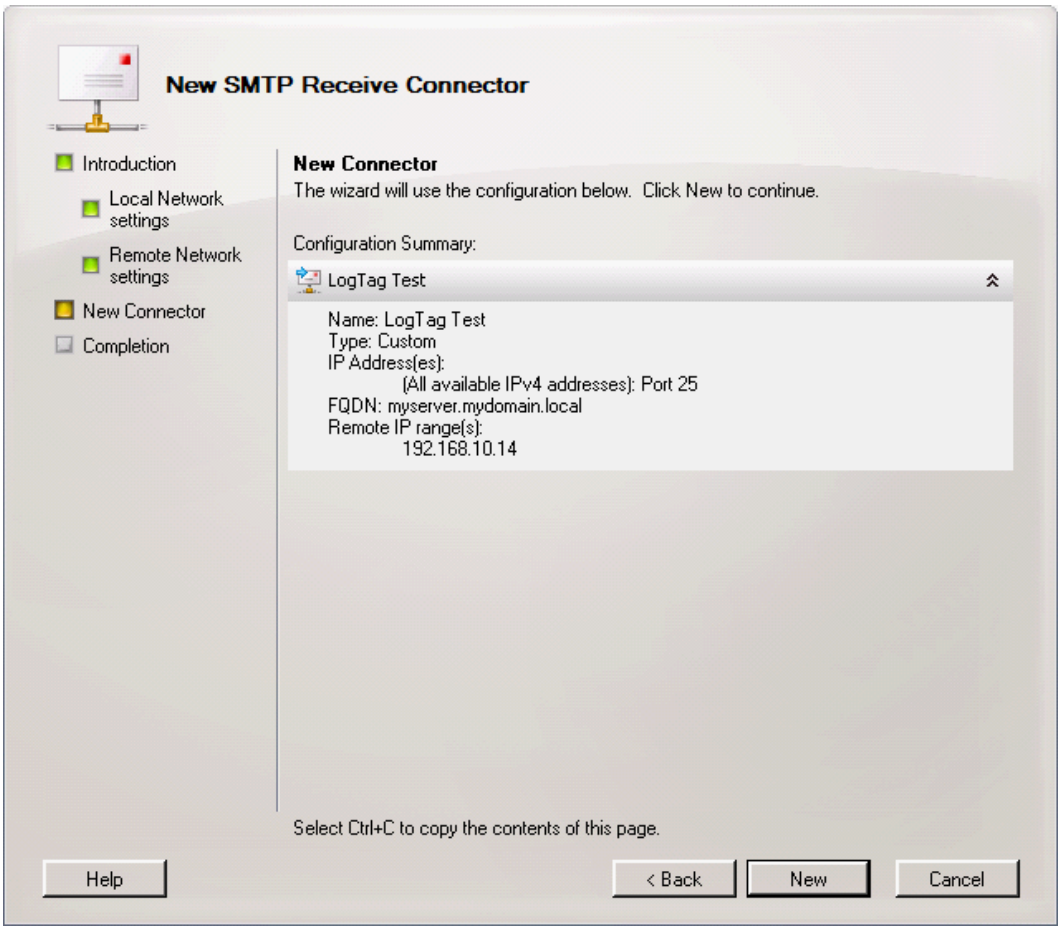
2. In the Local Network settings screen leave the IP addresses as listed. Enter the FQDN for the HELO/EHLO request.



3. In the Remote Network settings screen add the IP addresses for which the connector will be used. This can be a list of single IP addresses, or an address range. If you do not wish to keep the default setting delete it and add your own setting.

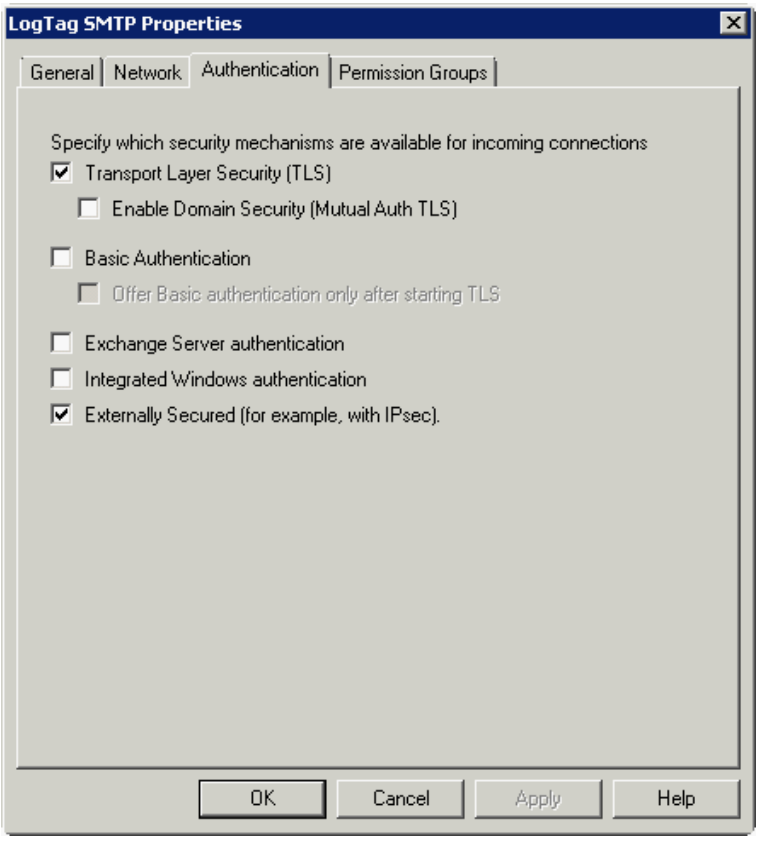


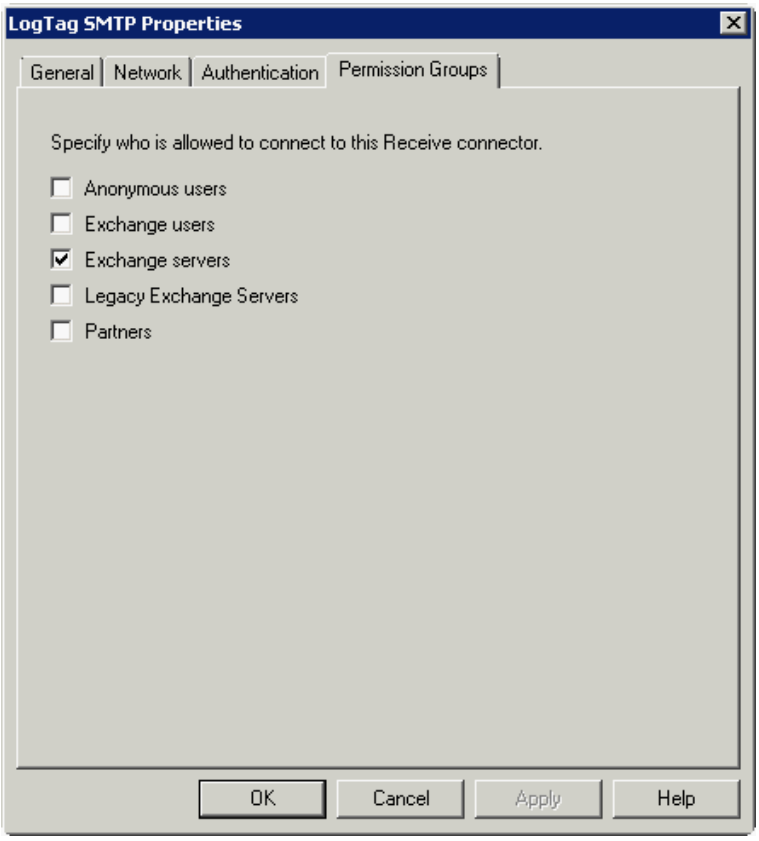
4. Check the summary page, make any amendments if required and click **New**.



Confirm the successful execution of the shell script by clicking **Finish**

The only remaining step is to set Authentication and Permissions for the receive connector.





Please enter the parameters as required for the security settings of your server.

Once you have made all the correct settings it is advisable to re-start the Microsoft Exchange Transport Service from the Services snap-in.

Often when using a Small Business Server e-mail is not hosted on the server but via a smart host, i.e. your ISP. In this case it may be easier to use the SMTP settings for this ISP, rather than changing the settings on your Exchange Server. You can also use a Gmail account and connect through the Gmail SMTP server with the Gmail specific SSL and port settings, however it will highly depend on your organisation's internet and security policies if you are allowed/able to connect to the required ports.

Chapter 5

Connecting to Gmail

You can use Google's SMTP server to send automated e-mail through your Gmail account. This requires special settings, which are slightly different than typically found with other ISP's.

- Enter **smtp.gmail.com** as the SMTP server
- The SMTP connection must be made over a secure connection. Check that SSL is enabled
- In the Authentication section select the **User name and password** check box and enter your Gmail account's user name (your full email address) and password in the text entry fields
- In **Advanced Settings** enter 465 in the Port number field. Please ensure this port is open in your firewall.

Complete the remaining entries in the SMTP section as you would for all other ISP's.

Note that Gmail's SMTP server replaces the email sender address with the Gmail account name used to log in. This is a feature of Gmails SMTP server and cannot be controlled by LogTag® Analyzer's SMTP settings. You can override this account setting by entering a different email address in **Send mail as**, however please note this will also affect all other email sent from this account.

Note Google places certain restrictions on the use of its SMTP server and may block your account if you do not adhere to these restrictions. For details on these restrictions please see Google's SMTP relay policy.

Lately Google has been trying to enforce the new, more secure authentication method OAuth 2.0. This is not supported by LogTag Analyzer. If you wish to use Google's SMTP server you need to enable **Access for less secure apps** on your account page at https://www.google.com/settings/security/lesssecureapps.

Chapter 6

Importing Option Settings via an XML file

LogTag® Analyzer's option settings can be defined by importing a well formed XML file, either see on page 54) on program start-up, or by manually importing the file.

We recommend you edit an existing file created from an export, but you can also create a new file, following the rules below.

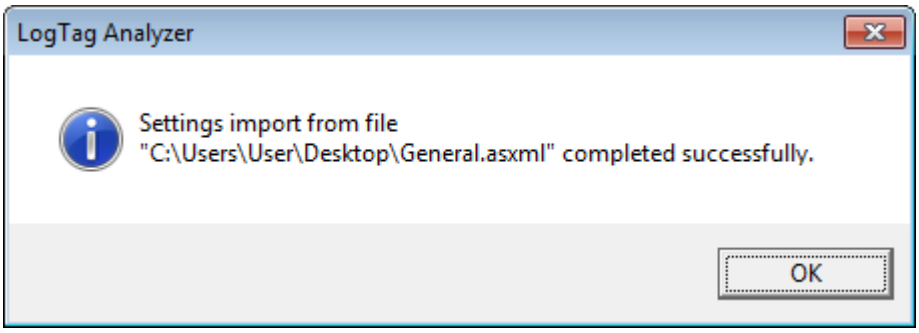
The file should have the extension *.asxml (for **A**nalyzer **S**ettings **XML**). Although it is possible to choose a different extension, only *.asxml is registered with the operating system, so it automatically opens with LogTag® Analyzer when clicked.

The structure of the XML file needs to comply with the following rules:

- The first line must contain the XML declaration:
  `<?xml version="1.0" encoding="UTF-8" standalone="no"?>`
- All tags inside the file (except the declaration) must be properly closed and properly nested, or the XML import validation will fail.
- All settings tags are nested inside a single root element called `<analyzer_options_settings>`, which is closed on the last line of the file.
- The first child tag inside this element is the `<file_version>` element, which contains the current version of the XML file.
- Child tags largely follow the order as displayed in the dialogues of the LogTag® Analyzer options settings, starting with General settings, then summary statistics, then chart statistics and so on. You can find a detailed list of options in the section about Available Settings on page 37
- If you delete a parent tag, but the child tags remain, these will not be imported.
- Not all available tags need to be present in the file for the import to be successful. If for example you wish to only import settings to affect the appearance of the chart, the XML file only needs to contain the section about `<chart_settings>`.
- Standard block comments can be used to prevent parts of the file being imported.

- We recommend you export the desired settings to a template and edit the settings that require changing. You can also download a set of templates (a single file for each option section) from the Network Administrator download page on the LogTag® Recorders website.
- When importing these settings files, error checking at the tag level will prevent importing values not allowed for the specific field they are imported for. This error checking will, however, not prevent you from making settings that are incorrect (for example the entry of incorrect user names, passwords or folder names). We therefore recommend you check the settings by importing them into a lab installation before distributing them to production machines.

On successful import following message will be displayed.



It is possible to suppress or customise this message. To do this you need to include an `<import_success>` tag. If the tag has no children, the message will be suppressed. You can add up to 5 child tags named <line>. Any string inside the `<line>` tag up to 50 characters long will be displayed in the message. An empty `<line>` tag will produce an blank line in the window.

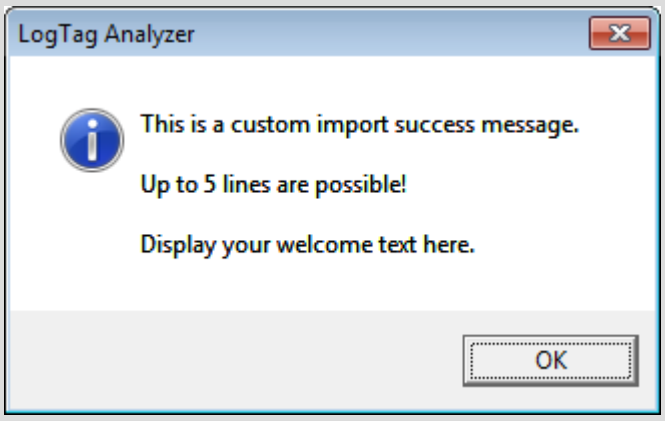
The tag will not be exported, as there is no storage mechanism for the message inside LogTag® Analyzer.

Example:

If a file with the following XML code is imported...

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
   <analyzer_options_settings>
      <file_version>1</file_version>
      <import_success>
         <line>This is a custom import success message.</line>
         <line/>
         <line>Up to 5 lines are possible!</line>
         <line/>
         <line>Display your welcome text here.</line>
      </import_success>
      <general_settings>
         <temperature_unit>Celsius</temperature_unit>
         <language>409</language>
      </general_settings>
   </analyzer_options_settings>
```

...this message is displayed upon successful import:



Editing *.asxml files

Although you can edit *.asxml files with a standard text editor, we recommend using an XML tree editor, making it easier to identify the tags.

Two popular editors are

- **XML Notepad 2007** published by Microsoft
- **XML Tree Edit** available from Sourceforge

Both present the asxml file in a way that makes them easy to view and change. Please note however that when saving both editors may add a *.xml extension to the end of the file name.

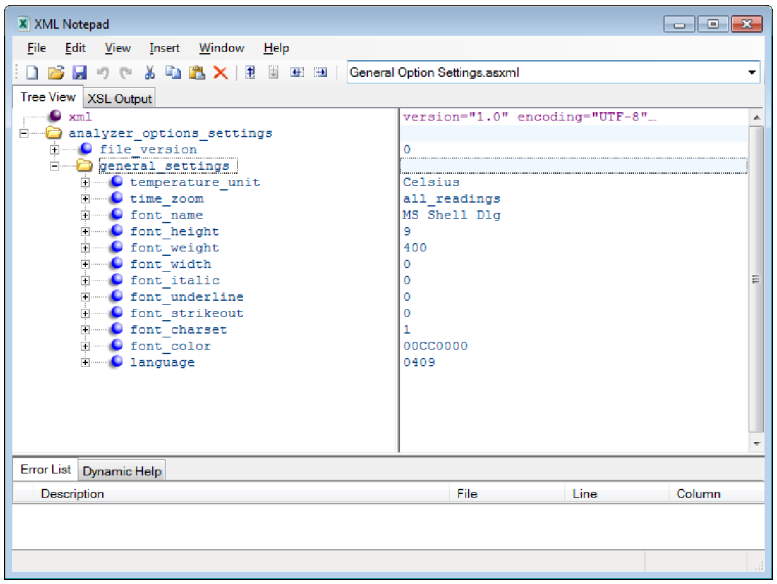


Figure 1: Microsoft's XML Notepad 2007

Password considerations

When exporting a settings *.asxml file, all passwords (for example email and ftp passwords) are stored in an encrypted form in the `<password_encrypted>` tag.

To avoid distributing clear text passwords, administrators can import a settings file into Analyzer containing the clear text password, then export these settings again to a new *.asxml file and either copy/paste the encrypted password or use the new file as the basis for the distributed import file.

Clear text password using the `<password>` tag can also be distributed, but typically company's security procedures don't allow this.

Available Settings

Following tables contain the settings available for import/export. Their meaning is explained only if the settings are not already detailed in the LogTag® Analyzer User Guide, in the section about **Customising the software**.

Please note where colours are referenced, the American spelling **color** is used. The hex values for colours are in the form of 4 octets, rather than the typical 3, the first octet being `00`, the remaining are the BGR values (please note, not RGB!).

The tag syntax and all available settings are in English and must remain in English for all languages.

General Settings

The tag syntax is <general_settings>.

Table 1: General Settings

Setting	Accepted values	Notes
`temperature_unit`	“Celsius”, “Fahrenheit” “Kelvin”	
`time_zoom`	“all_readings” “start_first_mark” “last_mark_end”	
`font_name`	Valid font name	
`font_height`	1-72pt	
`font_weight`	long integer	
`font_width`	long integer	
`font_italic`	0 (attribute not set) 1 (attribute set)	

Setting	Accepted values	Notes
font_underline	0 (attribute not set) 1 (attribute set)	
font_strikeout	0 (attribute not set) 1 (attribute set)	
font_charset	Byte value, values as per definition in wingdi.h: ANSI_CHARSET 0 DEFAULT_CHARSET 1 SYMBOL_CHARSET 2 MAC_CHARSET 77 SHIFTJIS_CHARSET 128 HANGEUL_CHARSET 129 HANGUL_CHARSET 129 GB2312_CHARSET 134 CHINESEBIG5_CHARSET 136 JOHAB_CHARSET 130 HEBREW_CHARSET 177 ARABIC_CHARSET 178 GREEK_CHARSET 161 TURKISH_CHARSET 162 VIETNAMESE_CHARSET 163 BALTIC_CHARSET 186 THAI_CHARSET 222 EASTEUROPE_CHARSET 238 RUSSIAN_CHARSET 204 OEM_CHARSET 255	
font_color	Hex RGB value 00bbggrr	Please note US spelling

Setting	Accepted values	Notes
language	Hexadecimal value corresponding to the Windows language identifier Chinese (Simplified) 404 Chinese (Traditional) 804 Czech 405 Danish 406 Dutch 413 English (UK) 809 English US 409 French 40C German 407 Greek 408 Italian 410 Norwegian 414 Polish 415 Portuguese (Brazil) 416 Portuguese 816 Romanian 418 Russian 419 Spanish 40A Swedish 41D Turkish 41F	Please note due to an earlier issue the language identifiers for Chinese Traditional and Chinese simplified have been transposed from the standard Windows language identifiers.

Summary Statistics Settings

Please note most settings are shared between this section and the chart statistics section. In case of a conflict the setting imported last overwrites the earlier setting.

The tag syntax is <summary_statistics>.

Table 2: Statistics Settings

Setting	Accepted values	Notes
elapsed_time	0: display date/time, 1: display elapsed time	
reading_range	0: don't display 1: display	
average_reading	0: don't display 1: display	
average_decimal_places	1, 2 or 3	The same average parameter settings apply to chart and summary statistics
standard_deviation	0: don't display 1: display	
stdev_decimal_places	1, 2 or 3	The same standard deviation parameter settings apply to chart and summary statistics
stdev_formula	"sample_based" or "population_based"	

Setting	Accepted values	Notes
deg_minutes_below	0: don't display 1: display	
deg_minutes_above	0: don't display 1: display	
mean_kinetic_ temperature	0: don't display 1: display	
mkt_default	0: use default delta H value 1: use delta H specified	The same MKT setting applies to chart and summary statistics
mkt_delta_h	-9999.999 to +9999.999	up to 3 decimal places
mkt_use_logger_delta_h	1: yes 0: no	
time_below_lower	0: don't display 1: display	
time_above_upper	0: don't display 1: display	
time_within	0: don't display 1: display	

Chart Statistics

The tag syntax is <chart_statistics>.

Table 3: Chart Statistics

Setting	Accepted values	Notes
elapsed_time	0: display date/time, 1: display elapsed time	
reading_range	0: don't display 1: display	
average_reading	0: don't display 1: display	
average_decimal_places	1, 2 or 3	The same average parameter settings apply to chart and summary statistics
standard_deviation	0: don't display 1: display	
stdev_decimal_places	1, 2 or 3	The same standard deviation parameter settings apply to chart and summary statistics
stdev_formula	"sample_based" or "population_based"	
deg_minutes_below		
deg_minutes_above	0: don't display 1: display	
mean_kinetic_ temperature	0: don't display 1: display	
mkt_default	0: use default delta H value 1: use delta H specified	The same mkt setting applies to chart and summary statistics, the last setting in the file will override a previous setting

Setting	Accepted values	Notes
mkt_delta_h	-9999.999 to +9999.999	up to 3 decimal places
mkt_use_logger_delta_h	1: yes 0: no	
time_below_lower	0: don't display 1: display	
time_above_upper	0: don't display 1: display	
time_within	0: don't display 1: display	

Chart Settings

A number of chart settings have child tags.

The tag syntax is <chart_settings>.

Table 4: Chart Settings

Setting	Child	Accepted values	Notes
chart_heading		string	use own text, can add variables as listed in the LogTag® AnalyzerUser Guide
temperature_readings	color	Hex RGB value 00bbggrr	
	line_style	"none", "solid", "dash", "dot", "dash_dot", "dash_dot_dot"	
	line_thickness	1 - 15	
temperature_markers	display	0: don't display 1: display	
	color	Hex RGB value 00bbggrr	
	style	"Circle", "Diamond", "Hexagram", "Pentagram", "Square", "Star", "Triangle", "HourGlass", "BowTie"	
humidity_readings	size	1 - 15	
	color	Hex RGB value 00bbggrr	
	line_style	"none", "solid", "dash", "dot", "dash_dot", "dash_dot_dot"	
humidity_markers	display	0: don't display 1: display	
	line_thickness	1 - 15	
	color	Hex RGB value 00bbggrr	
download_marks	display	0: don't display 1: display	
	style	"Circle", "Diamond", "Hexagram", "Pentagram", "Square", "Star", "Triangle", "HourGlass", "BowTie"	
	size	1 - 15	

Setting	Child	Accepted values	Notes
	color	Hex RGB value 00bbggrr	
inspection_marks	display	0: don’t display 1: display	
	style	“Circle”, “Diamond”, “Hexagram”, “Pentagram”, “Square”, “Star”, “Triangle”, “HourGlass”, “BowTie”	
	size	1 – 15	
	color	Hex RGB value 00bbggrr	
above_alert_region	display	0: don’t display 1: display	
	style	“Circle”, “Diamond”, “Hexagram”, “Pentagram”, “Square”, “Star”, “Triangle”, “HourGlass”, “BowTie”	
	size	1 – 15	
	color	Hex RGB value 00bbggrr	
within_alert_region	display	0: don’t display 1: display	
	line_style	“none”, “solid”, “solid_thick”, “dash”, “dot”, “dash_dot”, “dash_dot_dot”	
	color	Hex RGB value 00bbggrr	
below_alert_region	display	0: don’t display 1: display	
	line_style	“none”, “solid”, “solid_thick”, “dash”, “dot”, “dash_dot”, “dash_dot_dot”	
	color	Hex RGB value 00bbggrr	
multi_chart_shade	display	0: don’t display 1: display	
	color	Hex RGB value 00bbggrr	
x_axis_grids	display	0: don’t display 1: display	
y_axis_grids	display	0: don’t display 1: display	
non_validated	display	0: don’t display 1: display	
	display_differently	0: yes, 1: no	
	style	“Circle”, “Diamond”, “Hexagram”, “Pentagram”, “Square”, “Star”, “Triangle”, “HourGlass”, “BowTie”	
	size	1 - 15	
	color	Hex RGB value 00bbggrr	
readings_beyond_specification		0: don’t display 1: display	
annotations		0: don’t display 1: display	
elapsed_time		0: don’t display 1: display	
y_axis_alert_shade		"Humidity”, "Temperature"	

Setting	Child	Accepted values	Notes
default_zoom	Attribute type=""	valid attributes are “readings_range”, “sensor_range”, “custom_range”	
	temperature_unit	“Celsius”, “Fahrenheit”, “Kelvin”	settings for custom range
	temperature_from	-100.0 to 100.0	one decimal point
	temperature_to	-100.0 to 100.0	one decimal point
	humidity_from	0 to 100.0	one decimal point
	humidity_to	0 to 100.0	one decimal point

Automation Settings

The tag syntax is <automation_settings>.

When this section is exported, FTP and SMTP settings are also exported.

Table 5: Automation Settings

Setting	Accepted values	Notes
auto_download	0: false 1: true	
auto_reconfigure	0: false 1: true	
auto_display	0: false 1: true	
display_only_latest	0: false 1: true	
auto_save_readonly	0: false 1: true	
auto_email	0: false 1: true	settings made in the next section
manual_email	0: false 1: true	settings made in the next section
auto_ftp	0: false 1: true	settings made in the section after next
manual_ftp	0: false 1: true	settings made in the section after next

FTP settings

A number of FTP settings have child tags.

Please also see recommendations for dealing with passwords.

The tag syntax is <ftp_settings>.

Table 6: FTP settings

Setting	Child	Accepted values	Notes
server		String	
port_number		0 to 65535	
username		String	
password		String	
password_encrypted		String	encrypted password; where possible use this for distribution. Generated when exported.
security_protocol		"none", "SSL", "TLS1"	
proxy	Attribute settings=" "	values: "proxy_default" "proxy_custom"	
	proxy_server	String	
	proxy_port_number	0 to 65535	
	use_username_password	0: false 1: true	
	proxy_username	String	
	proxy_password	String	clear text password, for importing only
	proxy_password_encrypted	String	encrypted password; where possible use this for distribution. Generated when exported.
	proxy_method	“auto_detect,"site", "user_site", "user_login", "user_pass_acct", "open_site","proxy_username_site", "site_user", "user_proxy_username_site", "socks_v4","socks_v5"	
reconnect_interval		1 to 65535	in minutes
reconnect_retries		0 to 65535	
disconnect_idle_time		0 to 65535	in minutes
log_uploads		0: false 1: true	
log_folder		String	
log_conection_errors		0: false 1: true	
use_outbox		0: false 1: true	
remote_folder		String	
create_remote_folder		0: false 1: true	
upload_file_formats	ltd	0: false 1: true	
	text_tab	0: false 1: true	

Setting	Child	Accepted values	Notes
	text_mac	0: false 1: true	
	csv	0: false 1: true	
	html	0: false 1: true	
	pdf	0: false 1: true	

SMTP Settings

A number of SMTP settings have child tags.

Please also see recommendations in the section about Password considerations on page 37.

The tag syntax is <smtp_settings>.

Table 7: SMTP settings

Setting	Child	Accepted values	Notes
server		String	no enclosing double quotes
port_number		0 to 65535	
use_ssl		1: yes 0: no	
reconnect_interval		1 to 65535	in minutes
reconnect_retries		0 to 65535	
disconnect_idle_time		0 to 65535	in minutes
log_uploads		0: false 1: true	
log_folder		String	no enclosing double quotes, even for folders with spaces
log_conection_errors		0: false 1: true	
use_name_and_password		0: false 1: true	
username		String	
password		String	clear text password, for importing only
password_encrypted		String	encrypted password; where possible use this for distribution. Generated when exported.
sender_name		String	
sender_email		String	

Setting	Child	Accepted values	Notes
email_recipients	recipient	Attributes: name = String, email_address = String	each recipient in separate self closing tag with the attributes
attachment_file_formats	ltd	0: false 1: true	
	text_tab	0: false 1: true	
	text_mac	0: false 1: true	
	csv	0: false 1: true	
	html	0: false 1: true	
	pdf	0: false 1: true	
subject_line		String	use own text, can add variables as listed in the LogTag® AnalyzerUser Guide
use_outbox		0: false 1: true	

File and Folder Settings

The tag syntax is <file_folder_settings>.

Table 8: File and Folder Settings

Setting	Accepted values	Notes
number_mru_files	0 to 16	
initial_display	"Chart", "Data", "Report","Summary"	
file_name	String with placeholder elements	use own text, can add variables as listed in the LogTag® AnalyzerUser Guide
folder	String with placeholder elements, max. length: 260 characters	use own text, can add variables as listed in the LogTag® AnalyzerUser Guide
template_folder	String with placeholder elements, max. length: 260 characters This tag will not be exported.	this folder is used to store the logo file.
file_name_uniqueness	"unique_filename", "overwrite_existing", "prompt_if_exists"	

The string used for file name, folder name and template folder can contain the same placeholder elements that are present in the option settings.

Example:

Following <folder> tag will save all LogTag data files in the user's **Documents** folder, in a subfolder called **My LogTag Data**.

```
<folder>%HOMEDRIVE%HOMEPATH\Documents\My LogTag Data</folder>
```

File Export Settings

A number of file export settings have child tags.

The tag syntax is <file_export_settings>.

Table 9: File Export Settings

Setting	Child	Child	Accepted values	Notes
export_formats	text_tab	Attribute “enabled”	values “on” or “off”	
		include_prestart	1: yes 0: no	
		column_headings	1: included 0: excluded	
		summary	1: yes 0: no	
		readings_beyond_spec_blank	1: yes 0: no	
		show_elapsed_time	1: yes 0: no	either this or the next entry must be '1'
		show_date_time	1: yes 0: no	
	text_mac	Attribute “enabled”	values “on” or “off”	
		include_prestart	1: yes 0: no	
		column_headings	1: included 0: excluded	
		summary	1: yes 0: no	
		readings_beyond_spec_blank	1: yes 0: no	
		show_elapsed_time	1: yes 0: no	either this or the next entry must be '1'
		show_date_time	1: yes 0: no	
	csv	Attribute “enabled”	values “on” or “off”	
		include_prestart	1: yes 0: no	
		column_headings	1: included 0: excluded	
		summary	1: yes 0: no	
		readings_beyond_spec_blank	1: yes 0: no	

Setting	Child	Child	Accepted values	Notes
		show_elapsed_time	1: yes 0: no	either this or the next entry must be '1'
		show_date_time	1: yes 0: no	
		custom_separator	attribute separator="C"	C is one single character
	html	Attribute “enabled”	values “on” or “off”	
		include_prestart	1: yes 0: no	
		column_headings	1: included 0: excluded	
		summary	1: yes 0: no	
		readings_beyond_spec_blank	1: yes 0: no	
		show_elapsed_time	1: yes 0: no	either this or the next entry must be '1'
		show_date_time	1: yes 0: no	
	pdf	Attribute “enabled”	values “on” or “off”	
		day_summary	1: included 0: excluded	
		readings_beyond_spec_blank	1: yes 0: no	
		prestart_chart	1: included 0: excluded	
		prestart_data	1: included 0: excluded	
		prestart_summary	1: included 0: excluded	
		chart_chart	1: included 0: excluded	
		chart_data	1: included 0: excluded	
		chart_summary	1: included 0: excluded	
		all_chart	1: included 0: excluded	
		all_data	1: included 0: excluded	
		all_summary	1: included 0: excluded	
		paper_size	"letter", “legal”, “a3”, “a4”, “b4”, “b5”, “executive”	

Setting	Child	Child	Accepted values	Notes
		paper_orientation	“portrait”, “landscape”	
send_mail_ formats		ltd	1: included 0: excluded	
		text_tab	1: included 0: excluded	
		text_mac	1: included 0: excluded	
		csv	1: included 0: excluded	
		html	1: included 0: excluded	
		pdf	1: included 0: excluded	

Date and Time settings

The tag syntax is <date_time_settings>.

Table 10: Date and Time settings

Setting	Accepted values	Notes
date_format	short long custom: Attribute format="String"	String contains date format string as described in LogTag® Analyzer User Guide
time_format	default custom: Attribute format="String"	String contains time format string as described in LogTag® Analyzer User Guide
display_time_zone	"download", "configuration", "UTC", "display_configuration", "display_ download_date"	

Communication Settings

A number of communication settings have child tags.

The tag syntax is <communication_settings>.

Table 11: Communication Settings

Setting	Child	Accepted values	Notes
disable_all_serial		1: yes 0: no	
The following settings are only included if the COM port settings are selected for export.			
serial_port_ detection		“automatic”, “manual”	
max_com_port_number		1 to 255, default value: 9	determines up to which COM port number the software looks for interfaces

Setting	Child	Accepted values	Notes
com_ports	COMx	List of self closing tags with numbered COM ports that are enabled with x being the port number.	This list is only included if the detection method is “manual”

User Server Settings

The tag syntax is <user_server_settings>.

User server settings can only be imported when a valid user is logged on. That user can only import settings for which change permissions are granted.

The recommended distribution for user settings when User Server is deployed is via Group Policy using the **User Profile.dat** file and registry entries as described in Connecting to LogTag® User Server on page 64.

The XML method can be used to connect a PC to a User Server who has not been connected previously. Please also see the methods described in Automatically Importing Options via XML on page 54

Table 12: User Server Settings

Setting	Accepted values	Notes
connection	"server_on_workstation", "server_name", "server_ip", “no_connection”.	"no connection" will be exported if no User Server connection defined, but importing this setting won’t disconnect from User Server on import
server_name	String	
server_ip	String	
tcp_port_number	0 to 65535	
verify_server_connection	0: false 1: true	recommended setting is 1. Using 0 will create the connection, regardless of whether the server is running or not. Use this with caution.

Updates Settings

The tag syntax is <updates_settings>.

Table 13: Updates Settings

Setting	Accepted values	Notes
enable_check	1: enabled 0: disabled	
check_interval	1 to 365	days
auto_download_updates	1: enabled 0: disabled	

Configuration Log Settings

If configuration logging is disabled, no columns are included in the *.asxml file, if logging is enabled, all columns are included with the "enabled" attribute indicating whether the columns are used or not. The order of the tags starting with <column_...> determines the order in which the export file columns are written to the log file.

The tag syntax is <configuration_logs_settings>.

Table 14: Configuration Log Settings

Setting	Accepted values	Notes
enable_logging	1: enabled 0: disabled	
log_folder	String with placeholder elements, max. length: 260 characters	
field_separator	String, length 1 to 16 characters	
column_date	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_time	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_logger_id	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_user_id	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_enable_prestart	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_wrap_memory	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_start_method	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_log_duration	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_log_interval	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_log_count	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_upper_alerts	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_lower_alerts	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_consec_alert_delay	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_non_consec_alert_delay	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_latch_alert	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute

Setting	Accepted values	Notes
column_clear_alert	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_configure_password	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute
column_download_password	Attribute enabled="on": column included Attribute enabled="off": column not included	switched via tag attribute

Importing and Exporting Configuration Profiles

Starting with LogTag® Analyzer 2.5r17, Configuration Profiles can be exported and imported via a *.asxml file . This allows for example profiles to be imported on start-up, using the same mechanism as for the other option settings, or easy distribution of profiles using email, where users just have to open the *.asxml file. For this to work, the format version of the XML import file must be set to 1.

The actual recorder configuration data are stored in the XML file in binary form in the <data> tag. It is not possible to create a profile manually and then add it via XML. For a profile to be added to an import file, it needs to be first created in LogTag® Analyzer and then exported. You can then copy the section about configuration profiles to a different XML file or edit the settings in the exported file directly.

It is possible to change the way the profile is imported by editing or creating certain tags in the exported XML file.

- You can specify a profile file path and name in which the imported profiles will be stored via the <profile_folder> and <profile_file_name> tags. If the file or path do not exist, they will be created, provided the user importing the XML file has access permissions. If not, the import process will fail.

  The file and folder name tags are not exported to avoid conflict with other installations. Instead, these tags must be created manually.

- You can define whether a profile with an existing name should be skipped or replaced on import with the <overwrite> tag.

  If a *.asxml file contains two profiles with the same name attribute, the same mechanisms apply as if the profiles were imported one after the other from two separate *.asxml files.

- You can define if a profile should be read-only after import, or read/write with the <write_protect> tag. Read-only profiles will be displayed at the top of the profile grid in LogTag® Analyzer and marked in the Attribute column as **RO**. Profiles that can be deleted or changed are marked as **R/W**.

  A read-only profile is stored in the **User Profile.dat** file, rather than in a profile file. It is displayed regardless of the profile file open at the time, can be exported, but not overwritten, and can also not be edited. To delete such a

profile, you need to delete the **User Profile.dat** file. Therefore, you should take care when setting importing Configuration Profiles through automatic import.

Table 15: Profile settings

Setting	Child tags	Child tags	Accepted values	Notes
configuration_ profiles	profile_folder		String	A valid path name
	profile_file_name		String	A valid file name. Combination of folder and file name cannot exceed 255 characters.
	logger_profile			Attribute "name", with the value being the Profile name displayed in the profile grid
		overwrite	0: don't overwrite 1: overwrite	If set to 0, an existing profile with the same name will not be replaced. If set to 1, an existing profile in the will be replaced with the imported one, unless it is read-only.
		write_ protect	1: yes 0: no	If set to 0, the profile will be stored in a Profile file. This will either be the file specified in the XML import, or the defauklt file if no name or folder is specified. If set to 1, the profile will be stored in the User Profile.dat file and cannot be deleted or changed.
		data		Base64 converted binary data, cannot be edited directly

An import file can contain as many <logger_profile> tags as needed.

Example:

The following XML code will add a profile called **TRIX Imported** to the file called **imported profiles.ltp** located in the **Documents\My LogTag Data** folder in a sub-folder called **Configuration Profiles**. If this file does not yet exist, it will be created. If a profile called **TRIX Imported** already exists in this file, it will not be overwritten by the new profile. The profile has read/write access and can be changed or deleted by any user with access to the profile file.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<analyzer_options_settings>
   <file_version>1</file_version>
   <configuration_profiles>
      <profile_folder>%HOMEDRIVE%HOMEPATH\Documents\My LogTag Data\Configuration
Profiles</profile_folder>
       <profile_file_name>imported profiles.ltp</profile_file_name>
       <logger_profile name="TRIX Imported">
       <overwrite>0</overwrite>
       <write_protect>0</write_protect>
<data>B4AAAAgAVABSAEkAWAAAAAAAAAAEABAgAAAAAAAAAAAEAAAAAAAAAAAwdQAA0AcBAAEAAAAA
 AAAAHz8AAAAAAAAIADEAMgAzADQAAAAADQAVABlAHMAdAAgADIALgA1AHIAMQA3ACAAdQBw
 AGcAcgBhAGQAZQAgAHQAbwAgAHIAMQA4AAIAAAAAAABAAAACABoBAAACAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABoBAAAB
 AAAAAAAEAAkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0QAAAAAAAAAAAhAQBAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAADkEB6d</data>
          </logger_profile>
    </configuration_profiles>
 </analyzer_options_settings>
```


Automatically Importing Options via XML

You can set pre-defined options during a one-off automatic import when LogTag® Analyzer starts. To do this, you need to create an XML settings file called **AutoImportSettings.asxml** using the previously described techniques, and save it to one or both of the following locations:

- the roaming profile location of any user for whom the import should take place (%APPDATA%\LogTag).
- the LogTag® Analyzer Program folder, where the executable resides. This is typically the \Program Files (x86)\LogTag Recorders LTD\LogTag® Analyzer or the \Program Files\LogTag Recorders LTD\LogTag® Analyzer folder, depending on OS, but it can also be a user selected folder.

Every time LogTag® Analyzer starts, it will execute the following tasks, in the order listed:

1. Check the roaming profile location of the currently logged in user and try to locate the **User Profile.dat** file. If it finds this file, it will load the settings contained in the file.

2. Check the same location for an **AutoImportSettings.asxml** file.

   If this file is present, its contents will be imported into the current configuration and overwrite the settings of the **User Profile.dat** file. If no **User Profile.dat** file is present, it will first be created with default settings, then the new settings applied. Those settings not present in the **AutoImportSettings.asxml** file remain unchanged.

   Once imported, the **AutoImportSettings.asxml** file will be renamed to **AutoImportSettings.asxml.complete**, and hence not imported again when LogTag® Analyzer starts next.

3. If neither a **User Profile.dat**, nor an **AutoImportSettings.asxml** file is found in the roaming profile location, LogTag® Analyzer will check in the folder where its executable is stored for an **AutoImportSettings.asxml** file.

If this file is present, a new **User Profile.dat** file will be created in the current user's roaming profile location with default settings, then the contents of the **AutoImportSettings.asxml** file will be imported and overwrite the settings of the **User Profile.dat** file. Again, settings not present in the **AutoImportSettings.asxml** file remain unchanged.

When the import is complete, the **AutoImportSettings.asxml** will not be renamed. This allows the file to be imported by multiple users on the same PC, but on the next start of LogTag® Analyzer it will not be imported, as the roaming profile location now contains a **User Profile.dat** file. Only when this file is deleted, will the import be repeated.

When you exit LogTag® Analyzer, any changes made as a result of importing option settings as are written to the **User Profile.dat** and become persistent, until they are either changed again by the User, another *.asxml file is imported or the **User Profile.dat** file is deleted from the roaming profile.

The **AutoImportSettings.asxml** file must contain only valid settings. None of the settings in the **AutoImportSettings.asxml** file will be imported, if even a single invalid tag is found in the file. If no **User Profile.dat** file is present, but the import fails, it will be created with default settings when you exit LogTag® Analyzer.

The previously used LogTag® Settings Editor for FTP and SMTP settings is no longer supported.

Installing LogTag® Analyzer for multiple users

If you are installing LogTag® Analyzer for multiple users on the same PC, but not via network deployment, we recommend the use of a centralised **AutoImportSettings.asxml** file in the Program folder to set-up your specific default settings. This allows you to set common default values, such as display language and temperature units, which would normally be set depending on the language chosen in the installer.

Example:

You need to install LogTag® Analyzer in a language other than US English. On a PC with multiple users, the language selected during installation will only be associated with LogTag® Analyzer's display language for the administrative user installing the software, for all other users the initial language will be US English. To make sure LogTag® Analyzer starts in the desired language, create an **AutoImportSettings.asxml** file with this content:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
   <analyzer_options_settings>
   <file_version>1</file_version>
      <general_settings>
         <temperature_unit>Celsius</temperature_unit>
         <language>40A</language>
```

```
      </general_settings>
</analyzer_options_settings>
```

This file will set the temperature units to Celsius (standard in is Fahrenheit) and the display language to Spanish.

You can also make any other settings such as data storage folders at the same time.

Alternatively you can email all users a *.asxml file once LogTag® Analyzer is installed, which they only need to double-click for the settings to be imported.

Chapter 7
Moving User Settings

Occasionally you may need to transfer LogTag® Analyzer's settings from one user to another user on the same computer, or to a different computer. This section explains how this is done.

Copying data to a different user on the same PC

This section details how settings are copied from User1 to User2 on the same PC.

1. Log on to the computer with the User1 credentials. If LogTag® Analyzer is running, please close it. This ensures any pending changes are saved to the settings file.
2. Start LogTag® Analyzer and click on **Options** in the **Edit** menu. Click **Export...** and place a tick in the box next to **Select all**.
3. Click Export, enter a name for the export file you can remember and store it in a location accessible to all users. A good folder is the Public\Documents folder.

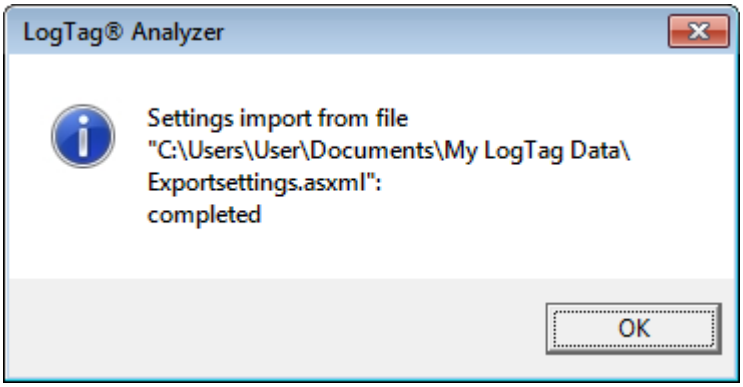
   At this point you may need to edit this file. If your administrator has set the software up correctly, all path names and directories accessed by LogTag® Analyzer are available, even after the settings have been transferred. To achieve this, path names need to point to network locations or incorporate system variables.
   If the file contains path names with your user name, the file needs to be edited. In particular, following path names need to be checked:
   - <log_folder> in <smtp_settings>
   - <log_folder> in <ftp_settings>
   - <folder> in <file_folder_settings>
   - <log_folder> in <configuration_logs_settings>

   You can also add additional information, or remove information not required. For a detailed description about all available settings please see the section about Importing Option Settings on page 1.

   This method also transfers any existing Configuration Profiles.
4. Switch users and log on with the User2 credentials. Start LogTag® Analyzer and

click on **Options** in the **Edit** menu. Click **Import...** and browse to the location where the previously exported file is stored. Select the file and click **OK**.

5. If the import is successful, you will see a message similar to the following:



Now User2 uses the same settings as User1. Please note that from this moment on both users' settings change independently.

You may wish to consider creating default settings for the PC, which are applied to every new user. This information is available in the section about Automatically Importing Options via XML on page 54.the Ne

Copying data to a different PC

This section details how settings are copied from one PC to a different PC.

1. On the PC that contains the correct settings for LogTag® Analyzer create the export settings file with the same procedure as in the previous section, steps 1 to 3.
2. Copy the file you created to a location you can access from the other computer. A good folder would be a publicly shared location on your company network, or a USB stick.

   You can now also edit the file, which is useful if the new PC uses differently named folders.
3. On the other PC install and start LogTag® Analyzer. Click on **Options** in the **Edit** menu. Click **Import...** and browse to the location where the previously exported file is stored, for example the memory stick. Select the file and click **OK**.

The settings have now been transferred, with the following exceptions:

- Any settings that have been disabled via the registry need to be disabled on the new computer.
- The Most recently used file list is not transferred.

Your network administrator will likely copy these registry keys to your new computer, depending on your networking requirements.

Chapter 8

Customising the Installation

You can customise certain settings in the software to apply our corporate branding and information.

Adding Your Company Information to the Help Menu

Starting with LogTag® Analyzer 2.5r17, some of the contact information that is displayed on screen can be imported via a *.asxml file. This process can be used in combination with the automated import to display corporate information in addition to the existing branding of the software. For this to work, the format version of the XML import file must be set to 1.

All of the tags are optional, however if you set some but not other tags the results may not be what you expect.

- Additional text can be shown in the **Help - About** window using the `<help_about_1>` to `<help_about_4>` tags. Each tag represents a line that appears in the **Help - About** window below the company information and above the software version numbers. Any lines longer than 30 characters will be truncated.
- A new support email address using the `<support_contact>` tag. This new address will be used in your email client's recipient field when the user clicks **Request help...** from the **Help** menu. Use it to direct users' requests for support to a company internal address. You need to specify an address in a valid format (a@b.com) for the import to succeed.
- A new home page text and hyperlink via the `<website_menu_entry>` and `<website_address>` tags. A browser window opens with the link, when the user clicks on the home page entry in the **Help** menu.
- Additional text to appear in the window title. This text is defined in the `<window_title>` tag. If the line is longer than 40 characters, it will be truncated on import

Table 16: Customisation settings

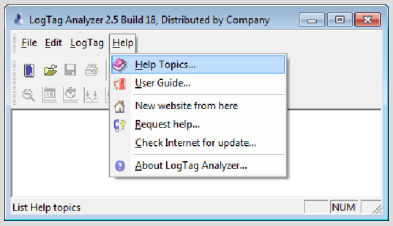
Setting	Child tags	Accepted values	Notes
customisation	help_about_1	String	max 30 characters
	help_about_2	String	max 30 characters
	help_about_3	String	max 30 characters
	help_about_4	String	max 30 characters
	support_contact	String	email format
	website_address	Hyperlink	web address
	website_menu_entry	String	max 30 characters
	window_title	String	max 40 characters

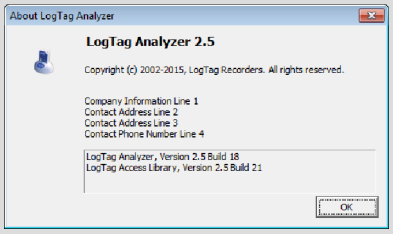
Example:

The following import file ...

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<analyzer_options_settings>
   <file_version>1</file_version>
   <customisation>
      <help_about_1>Company Information Line 1</help_about_1>
      <help_about_2>Contact Address Line 2</help_about_2>
      <help_about_3>Contact address line 3</help_about_3>
      <help_about_4>Contact phone number line 4</help_about_4>
      <support_contact>myemail@someemailprovider.com</support_contact>
      <website_address>http://www.somewebsiteaddress.com</website_address>
      <website_menu_entry>New website from here</website_menu_entry>
      <window_title>, Distributed by Company</window_title>
   </customisation>
</analyzer_options_settings>
```

will create following appearance:





Adding a Custom Logo to Reports and PDF files

You can change the LogTag® logo that appears in the top left corner of the report tab and the PDF export to your own custom logo.

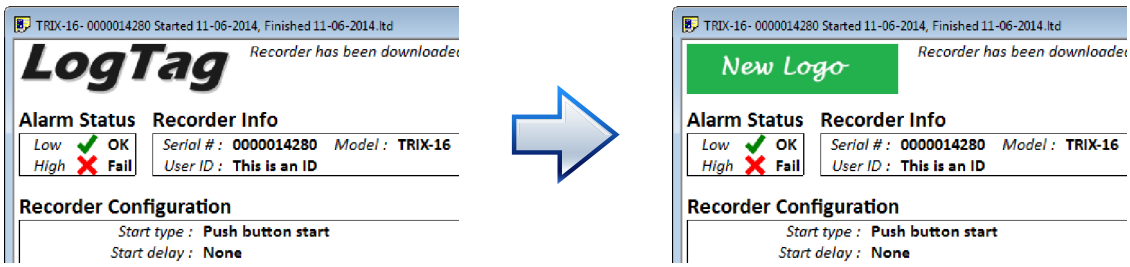


Figure 1: Custom logo for report and PDF export

1. Close LogTag® Analyzer
2. Create your new logo with the following attributes:
   - File format: JPEG
   - File name: `DftLogo.jpg`
   - Dimensions: 588 (W) * 141 (H)

   Any logo file you choose will be resized to these dimensions; for best results you should create a file with the same aspect ratio, ideally the same size.
3. Place the logo file in the folder "[drive letter]:\Users\{user name}\My LogTag® Data\Templates".

   This storage location cannot be changed and is independent of the folder name for the file storage location chosen in **Options - File and Folder Settings**. It is specific to each user, so different users can have different logos.

The custom logo will be stored in the PDF export file on the report page, but not in the *.ltd file used to generate the report. If you open a file on a computer with a different logo, the different logo will be shown on the report tab.

Chapter 9

Connecting to LogTag® User Server

The US Food & Drug Administration has published a set of requirements for Electronic Records and Electronic Signatures, also known as FDA 21 Title 11.

LogTag® Recorders provides the LogTag® Digital Signature Suite to support customers wishing to comply with these requirements.

Once the system is functional, users are required to log on to a central server software when using LogTag® Analyzer. This server software is called LogTag® User Server and:

- administers a user database and provides an authentication method
- stores all user activity such as downloading and configuring recorders
- provides each user with a set of digital signatures, which can be permanently applied to stored files.

You can find more information about the architecture and setup of LogTag® User Server in the "LogTag® Digital Signatures User Guide", which can be found on the LogTag® website.

Connection between the client (LogTag® Analyzer) and the server (LogTag®User Server) is initiated by LogTag® Analyzer through a Registry setting. An encrypted registry key with the connection settings is created when the user clicks on **Options** from the **Edit** menu, clicks on **User Server** and enters the connection details.

For a network distributed setting this method is impractical. Following are the steps required to remotely distribute the connection settings through Group Policy. This requires that LogTag® User Server is installed and running in its permanent location.

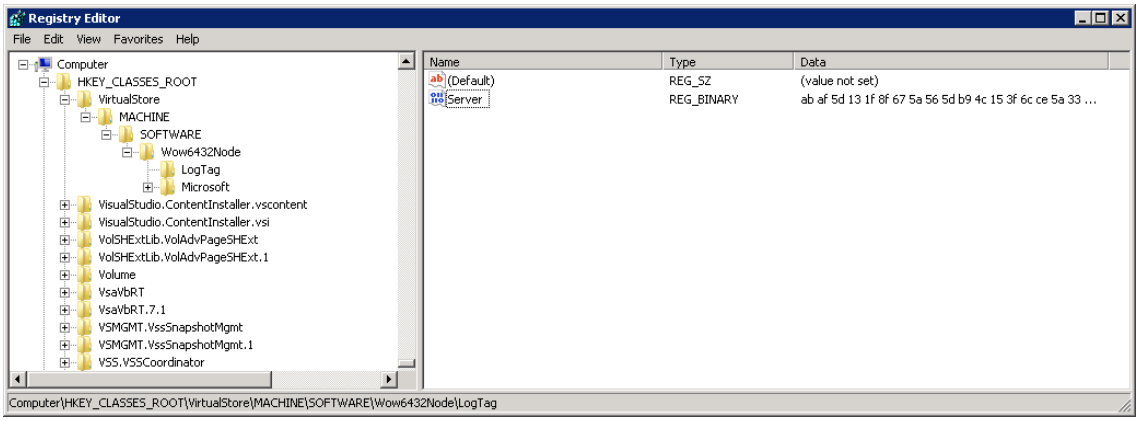
Creating the registry key

Install LogTag® Analyzer on a test computer using local administrator credentials. Connect LogTag® Analyzer to LogTag®User Server by clicking on **Options** from the **Edit** menu and clicking on the **User Server** entry.

Enter the connection details, place a tick in the **I agree** check box and click OK. Verify you can successfully connect to LogTag® User Server by logging on with a valid user name and password.

Start a registry editor and navigate to one of the following nodes, depending on your operating system:

- **XP 32-bit**: HKEY_LOCAL_MACHINE\SOFTWARE\LogTag®
- **XP 64-bit**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\LogTag®
- **Vista 32-bit:** HKEY_CLASSES_ ROOT\VirtualStore\MACHINE\SOFTWARE\LogTag®
- **Vista 64-bit:** HKEY_CLASSES_ ROOT\VirtualStore\MACHINE\SOFTWARE\Wow6432Node\LogTag®
- **Windows 7 32-bit:** (LogTag® Analyzer run with admin privileges) HKEY_ LOCAL_MACHINE\SOFTWARE\LogTag®
- **Windows 7 32-bit** (LogTag® Analyzer run as normal user): HKEY_CLASSES_ ROOT\VirtualStore\MACHINE\SOFTWARE\LogTag®
- **Windows 7 64-bit** (LogTag® Analyzer run with admin privileges): HKEY_ LOCAL_MACHINE\SOFTWARE\Wow6432Node\LogTag®
- **Windows 7 64-bit** (LogTag® Analyzer run as normal user): HKEY_CLASSES_ ROOT\VirtualStore\MACHINE\SOFTWARE\Wow6432Node\LogTag®



If you are creating the test installation on the same computer that is used to distribute the key, you can simply open the key and copy the string to the clipboard. If you are using a different computer to create the key you will need to export it to a text file. Edit the text file and create a continuous string of the hexadecimal data by removing all characters not part of the data, such as line breaks and separation characters.

Creating the Group Policy

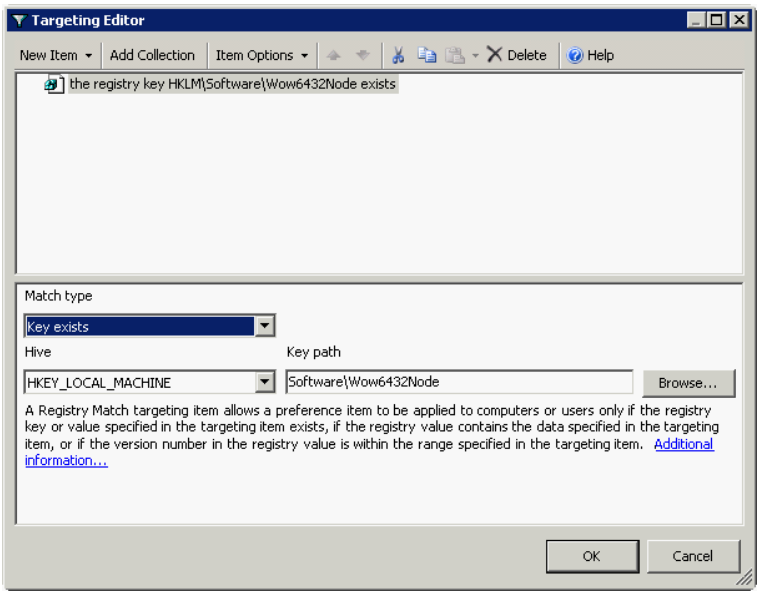
When you distribute this key, you need to ensure you give the local standard user read permissions to this key. If the local user does not have read permissions for

this key, the user will be unable to log into LogTag® Analyzer, as the registry key contains the required connection settings.

Open the GPMC. In this example we are using the same GPO we used earlier to distribute LogTag® Analyzer, but you can also create a new GPO. The settings will be distributed to the computer operating LogTag® Analyzer and therefore it will apply to all users on that computer.

- Edit the GPO **Windows SBS** LogTag. Expand the node **Computer Configuration - Preferences - Windows Settings - Registry**. If the GPO's WMI filter applies the GPO to 64-bit and 32-bit computers you will need to create two registry keys, as they will be distributed to different registry nodes.
- Create a new registry item for the 64-bit key. Set its properties as follows:
  - On the **General** tab select the hive **HKEY_LOCAL_MACHINE**. In the key path field enter **Software\Wow6432Node\LogTag.** In the Value name field enter **Server**. Select **REG_BINARY** as the Value type.

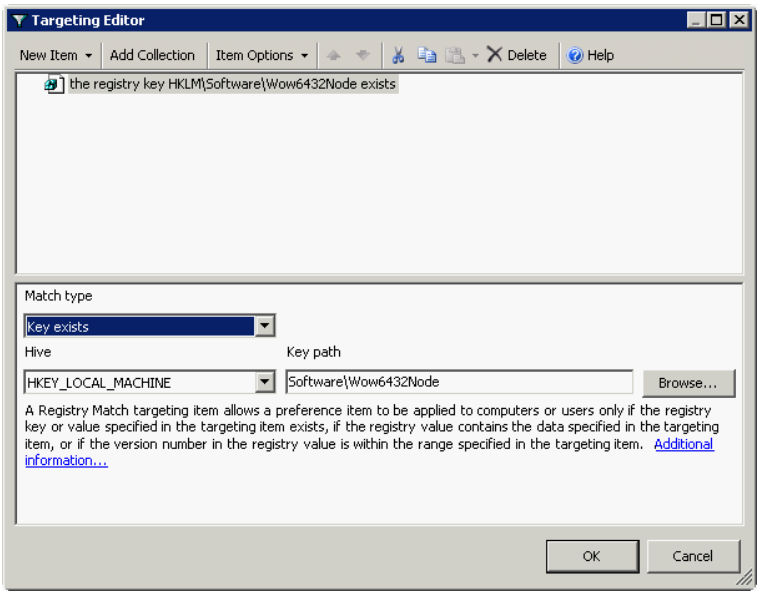
    Open the text file created earlier containing the key and copy/paste the key to the Value data field.
  - On the **Common** tab enable **Apply once and do not reapply** and **Item-level targeting**.
  - Click **Targeting**, and click **Registry Match** from the **New Item** menu. Select **Key Exists** as Match type, **HKEY_LOCAL_MACHINE** as hive and **Software\Wow6432Node** as the key path.



  - Click **OK - OK**.

- Create a new registry item for the 32-bit key. Set its properties as follows:
  - On the **General** tab select the hive **HKEY_LOCAL_MACHINE**. In the key path field enter **Software\LogTag.** In the Value name field enter **Server**. Select **REG_BINARY** as the Value type.

    Paste the key to the Value data field.
  - On the **Common** tab enable **Apply once and do not reapply** and **Item-level targeting**.
  - Click **Targeting**, and click **Registry Match** from the **New Item** menu. Select **Is not** from the **Item Options** menu. Select **Key Exists** as Match type, **HKEY_LOCAL_MACHINE** as hive and **Software\Wow6432Node** as the key path.



  - Click **OK - OK** and close the GPME.

There are a number of different ways to target 64-bit and 32-bit operating systems. For more information please read the corresponding articles on the Microsoft Technet Website.

Chapter 10
Disabling Option Settings

Access to certain option settings can be disabled by network administrators without deploying the Digital Signature Suite. To do this, certain keywords can be added to the registry:

- **DisableConfigure** - User is not permitted to upload new/updated configuration settings
- **DisableHibernate** - User is not permitted to stop loggers recording and place them in hibernation
- **DisableAutomation** – User is not permitted to modify options and preferences that relate to the 'automation' features.
- **DisableChartOptions** – User is not permitted to modify options and preferences that relate to the 'charting' features
- **DisableCommsOptions** - User is not permitted to modify options and preferences that relate to the what communication connections and ports are allowed to be used
- **DisableDateOptions** - User is not permitted to modify options and preferences that relate to the how date and/or times are displayed
- **DisableFolderOptions** - User is not permitted to modify location where files of the recorded readings are stored
- **DisableGeneralOptions** - User is not permitted to modify options for 'general' features
- **DisableUserServer** - User is not permitted to modify options to connect to LogTag User Server
- **DisableExportOptions** - User is not permitted to modify options for export features
- **DisableSoftwareUpdate** - User is not permitted to download new versions of Analyzer (This method is preferred over IP address blocking as it will still allow

users to take advantage of the support they can get from the website at http://www.logtagrecorders.com).

How this is done will be explained with the help of an example below.

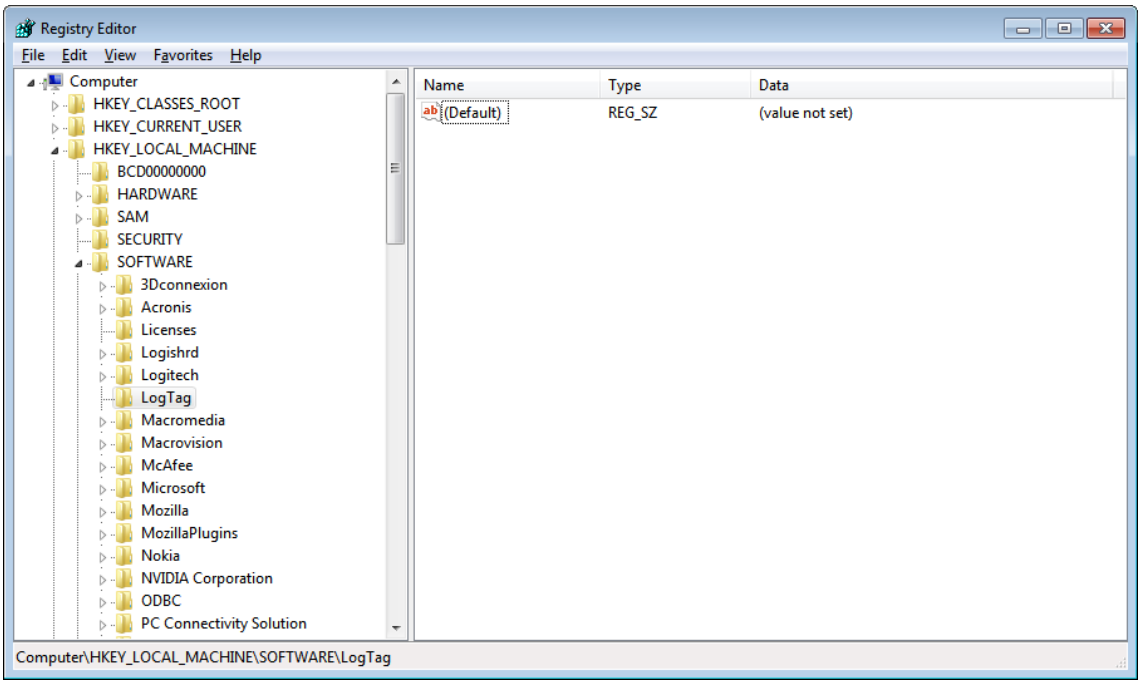
Please note that any settings blocked by a registry key cannot be selected when exporting option settings, but can still be overwritten if a valid *.asxml file is imported.

Disabling Updates

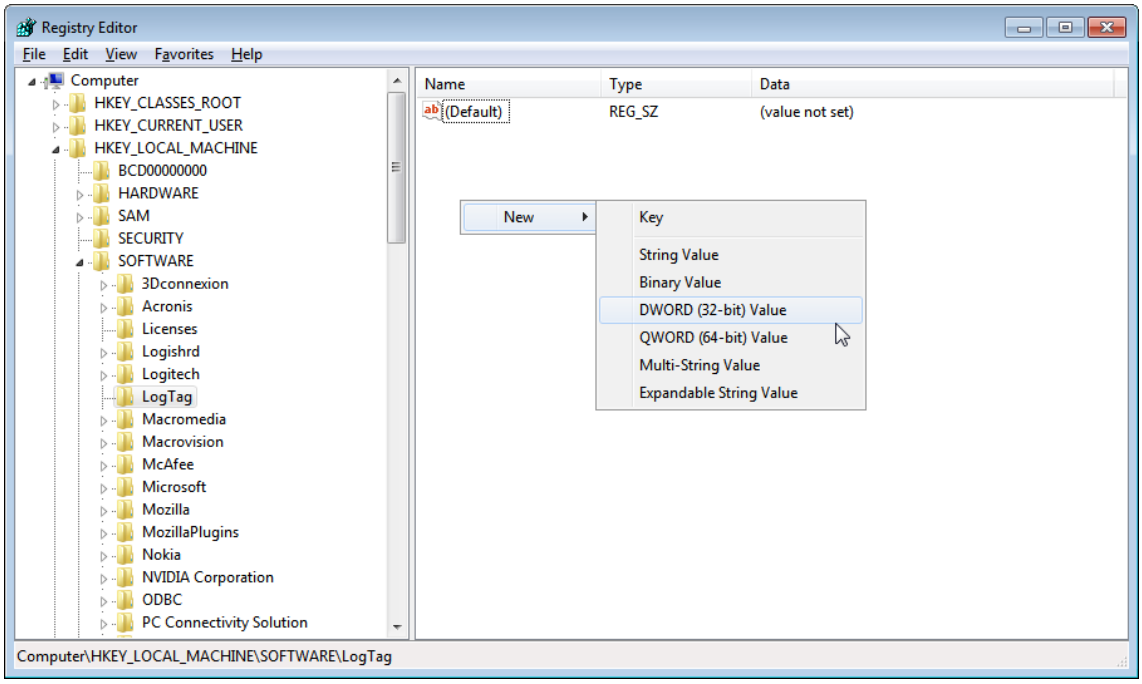
We will show the basic mechanism of editing the registry so certain settings in the software can be disabled by removing the ability to update the LogTag® Analyzer software via the Help menu. This may for example be desirable if the use of LogTag® products is governed by Standard Operating Procedures, which require a certain version of LogTag® Analyzer to be installed.

Open the registry and browse to the following node:

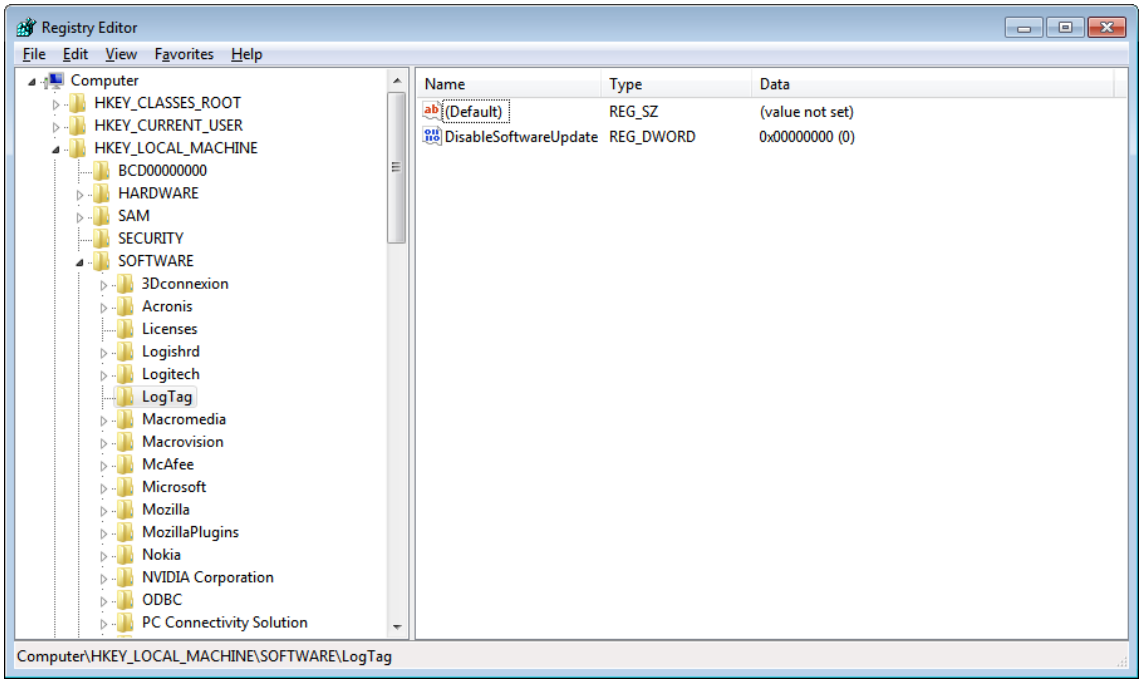
- **64-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\LogTag®
- **32-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\LogTag®



Add a DWORD and name it "DisableSoftwareUpdate". The value of the DWORD is irrelevant.



Once this DWORD is created, the automatic update function is disabled, regardless of the settings made in Options - Updates. Users will also be prevented from accessing the update function manually.



This registry setting can be distributed via GPO to client workstations.

Please note this key may not be written to this specific location, even if the GPO requests it due to the Microsoft Windows registry virtualisation/reflection

mechanisms. LogTag® Analyzer does read the various locations the key may be located in.

The settings for the other options work the same; the DWORD "DisableSoftwareUpdate" is replaced with the respective term from the list of option settings on page 68.

Chapter 11

COM Port Settings

A new registry key can be used to revert the way COM ports are detected to the method used in earlier version of LogTag® Analyzer. A change was made after version 2.1 to better handle COM ports which cannot have interfaces connected, however this influenced the way how virtualised environments detected COM ports, and had issues particularly with the deployment of LogTag® Analyzer in Citrix.

Open the registry and browse to the following node:

- **64-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\LogTag®
- **32-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\LogTag®

Add a new DWORD and name it "LegacyComDetection". The value of the DWORD is irrelevant.

This registry setting can be distributed via GPO to client workstations.

Please note this key may not be written to this specific location, even if the GPO requests it due to the Microsoft Windows registry virtualisation/reflection mechanisms. LogTag® Analyzer does read the various locations the key may be located in.

Once this key is present, the detection mechanism inside LogTag® Analyzer will report all COM ports regardless of what functionality they provide (for example all network COM ports will also be detected, which could lead to substantial delays during detection). We recommend that users open the Communication Options dialogue and disable all RS232 interfaces not used. If the COM port is known, the user settings should be pushed to workstations via GPO.

Chapter 12

Temporary Folder

The PDF creation library used by LogTag® Analyzer requires the temporary folder to be local to the computer on which it is running. In heavily virtualised environments (for example in Citrix deployments) the default temporary folder could be located on the network, which will cause the PDF creation to fail.

From LogTag® Analyzer version 2.5 onward a registry key can be used to define the location of a temporary folder used for PDF creation. This folder must reside on the local computer to successfully create PDF files with the built-in "save as PDF" function.

Open the registry and browse to the following node:

- **64-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\LogTag
- **32-bit OS**: HKEY_LOCAL_MACHINE\SOFTWARE\LogTag

Add a new STRING value and name it "TemporaryFolder".

Modify the string and put the name of the temporary folder you wish to use in the value data field. Close the registry.

This registry setting can be distributed via GPO to client workstations.

Please note this key may not be written to this specific location, even if the GPO requests it due to the Microsoft Windows registry virtualisation/reflection mechanisms. LogTag® Analyzer does read the various locations the key may be located in.

Once this key is present, the PDF creation mechanism will use this folder for temporary storage.

Note: The existence of the folder is not verified, neither is the permission setting to write to this folder. When an incorrect folder is specified, the PDF creation will fail.

Glossary

B

Bootloader
Embedded software that runs inside a product and controls access to other executable software

F

Firmware
Embedded software that runs inside a product and provides its functionality.

G

GPMC
Group Policy Management Console

GPME
Group Policy Management Editor; will be invoked when you edit a GPO

GPO
Group Policy Object

O

OU
Organisational Unit; typically group of computers to which a GPO is applied

Index

R

S

T

U

W