Zorp Authentication Agent Manual

Publication date March 04, 2024

Abstract
This document describes how to install and configure the Zorp Authentication Agent.

BALASYS

Copyright © 1996-2024 Balasys IT Zrt. (Private Limited Company)

DISCLAIMER

Balasys is not responsible for any third-party websites mentioned in this document. Balasys does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. Balasys will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

Table of Contents

List of Procedures

Summary of changes

The following changes have been made to the document between releases Zorp 7.0.18 and Zorp 7.0.19:

Description of the change	Place in the document
The information on which platform ZAA can be installed on has been updated.	For the changes, see *Chapter 3, Installing the Zorp Authentication Agent (ZAA) (p. 4)*.

Table 1. Summary of changes

The following changes have been made to the document between releases Zorp 7.0.17 and Zorp 7.0.18:

Description of the change	Place in the document
The procedures for installing and configuring Zorp Authentication Agent with Group Policy Object (GPO) deployment have been added to the document.	See sections *Procedure 3.1.2, Installing Zorp Authentication Agent with Group Policy Object (GPO) deployment (p. 7)* and *Procedure 4.1.5, Configuring Group Policy Object (GPO) deployment (p. 26)*.
Zorp Authentication Agent installer options have been added to the document.	See section *Procedure 3.1.1, Installing the Zorp Authentication Agent on Microsoft Windows (p. 4)*.

Table 2. Summary of changes

The following changes have been made to the document between releases Zorp 7.0.15 and Zorp 7.0.16:

Description of the change	Place in the document
During authentication, Zorp Authentication Agent requires TLS-encrypted communication from Zorp.	See sections *Section 4.1.3, Configuring SSL connections on Microsoft Windows platforms (p. 15)* and *Section 4.2.2, Configuring SSL connections on Linux platforms (p. 28)*
Editorial changes have been made throughout the document.	

Table 3. Summary of changes

The following changes have been made to the document between releases Zorp 7.0.13 and Zorp 7.0.14:

Description of the change	Place in the document
The steps have been improved and the figures have been exchanged for a more coherent look.	For the changes, see sections: ■ *Procedure 3.1.1, Installing the Zorp Authentication Agent on Microsoft Windows (p. 4)*

Description of the change	Place in the document
	■ *Procedure 4.1.3.2, Importing the CA certificate manually (p. 16)* ■ *Procedure 4.1.4, Configuring X.509 certificate based authentication on Microsoft Windows platforms (p. 25)*

Table 4. Summary of changes

Chapter 1. Introduction

Developed by Balasys, Zorp Authentication Agent (ZAA) is an authentication client, capable of cooperating with the Zorp firewall and the Zorp Authentication Server (ZAS) to identify the users initiating network connections. Zorp Authentication Agent enables the complete network traffic to be audited on the user level.

Chapter 2. Authentication and Zorp

Zorp Authentication Agent (ZAA) is an authentication client, capable of cooperating with the Zorp firewall and the Zorp Authentication Server (ZAS) to identify the users initiating network connections. The authentication process and the related communication between the components is summarized below. For more details, see *Chapter 15, Connection authentication and authorization* in *Zorp Professional 7 Administrator Guide*.

The authentication aims to determine the identity of the user. During the authentication process the user initiating the connection shares a piece of sensitive information (for example, a password) with the other party that verifies the user's authenticity.

Several procedures (so called authentication methods) exist for verifying the identity of the user:

1. The user owns some pieces of sensitive information, for example, a password, PIN code, the response to a challenge, and so on.
2. The user owns a device, for example, a hardware key, chipcard, SecurID token, and so on.

Naturally, the above methods can be combined to implement strong two-factor level authentication in sensitive environments.

2.1. Authentication on the network

The aim of network authentication is to authenticate the connections initiated by the users in order to ensure that only the proper users can access the services. Basically there are two types of authentication:

1. *Inband*: Authentication is performed by the application-level protocol — the data traffic required for the authentication is part of the protocol. Inband authentication is used for example in the HTTP, FTP, or SSH protocols. The protocols usually support different authentication methods — these are usually described in the specifications of the protocol.
2. *Outband*: Authentication is performed in a separate data channel completely independent from the protocol of the accessed service. Outband authentication is realized by the combination of the Zorp Authentication Agent (ZAA), Zorp Authentication Server (ZAS), and Zorp softwares. The advantage of outband authentication is that it can be used to authenticate any protocol, regardless of the authentication methods supported by the original protocol. That way, strong authentication methods (for example, chipcards) can be used to authenticate protocols supporting only the weak username/password method (for example, HTTP).

2.2. Procedure – Outband authentication with Zorp

Purpose:

Zorp implements outband authentication according to the following procedure:

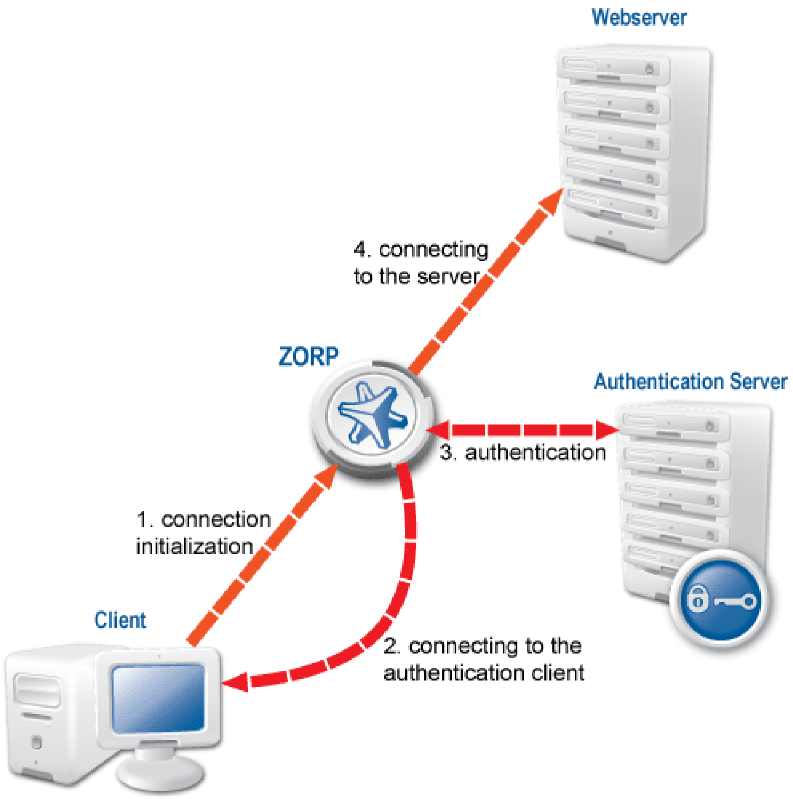

Webserver
4. connecting to the server
ZORP
Authentication Server
3. authentication
1. connection initialization
Client
2. connecting to the authentication client

Figure 2.1. Outband authentication with Zorp

Steps:

Step 1. The client initiates a connection towards the server.

Step 2. Zorp determines the service to be accessed based on the IP address of the client and the server. If authentication is required for the connection (an authentication policy is assigned to the service), Zorp initiates a connection towards the client using the Zorp Authentication Agent protocol.

Step 3. Depending on the authentication methods available (for example, for password-based authentication), the dialog of the Zorp Authentication Agent is displayed on the client machine. The user enters the username that the Zorp Authentication Agent forwards to Zorp.

Step 4. The Zorp firewall connects to Zorp Authentication Server (ZAS) and retrieves the list of authentication methods enabled for the particular user. Multiple authentication methods can be enabled for a single user (for example, x509, Kerberos, password, and so on). The authorization of the user is also performed in this step, for example, the verification of the LDAP group membership.

Step 5. Zorp returns the list of available methods to the client. The user selects a method and provides the information (for example, the password) required for the method.

Step 6. The Zorp Authentication Agent sends the data (for example, the password) to Zorp that forwards it to ZAS.

Step 7. ZAS performs the authentication and notifies Zorp about the result (success/failure).

Step 8. Zorp returns the result to the client and — if the authentication was successful, builds a connection towards the server. In case of a failed authentication it terminates the connection to the client.

Chapter 3. Installing the Zorp Authentication Agent (ZAA)

This section describes the installation and configuration of the Zorp Authentication Agent on Microsoft Windows and Linux platforms. The Zorp Authentication Agent has to be installed on every computer having access to authenticated services. The following platforms are supported:

- Windows 10 or later (x86, x64)
- Ubuntu 18.04 Bionic Beaver (64-bit only)

The agent has two components:

1. *Zorp Authentication Agent Multiplexer*: It is a daemon running in the background, accepting the connections coming from Zorp and verifying the SSL certificates of Zorp (if the communication is encrypted). In a multi-user environment the Multiplexer displays the dialog of the *Zorp Authentication Agent* on the desktop of the user initiating a connection requiring authentication.
2. *Zorp Authentication Agent*: This application collects the information required for the authentication, for example, the username, authentication method, password, and so on.

The installers automatically install both components. The components require approximately 10 MB of free hard disk space.

3.1. Installing the Zorp Authentication Agent on Microsoft Windows platforms

3.1.1. Procedure – Installing the Zorp Authentication Agent on Microsoft Windows

Purpose:

The Zorp Authentication Agent (ZAA) installer is located in the `\windows\satyr\` folder of the Zorp CD-ROM, its latest version is also available from the *Balasys website*.

The following Zorp Authentication Agent installer options are available:

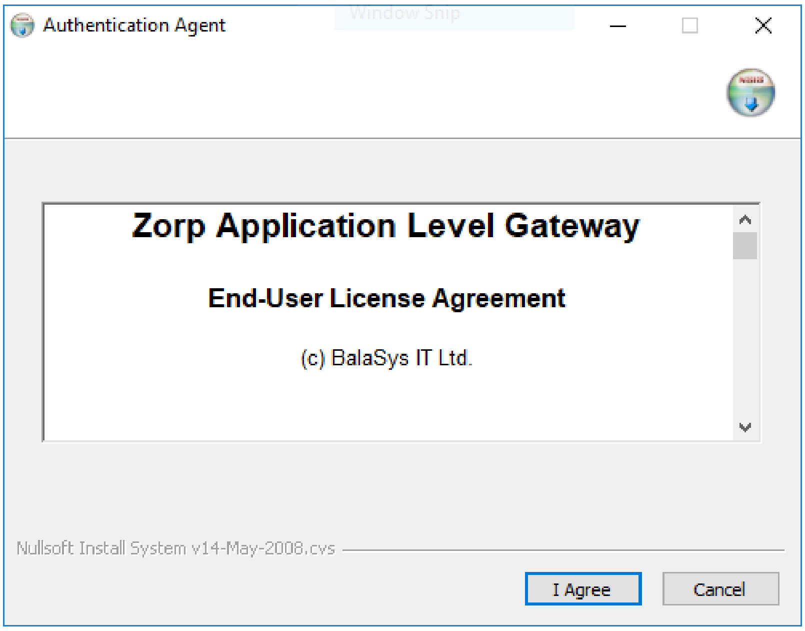
```
/S Silent mode
/D=[path] Set target path
/NO_VCREDIST Do not check/install Visual Studio Redistributable
/log-mpxd=[yes|no] Enable debug logging of AA multiplexer daemon
/log-client=[yes|no] Enable debig logging of AA client
```

Steps:

Step 1. Place the Zorp CD-ROM into the CD drive and start the `satyr-setup.exe` file located in the `\windows\satyr\` folder.

> **Warning**
> Administrator privileges are required to install the application.

Step 2. Click **I agree** to accept the End-User License Agreement, which is displayed after the installer starts. To cancel the installation at any time during the process, click **Cancel**.



Authentication Agent

Zorp Application Level Gateway

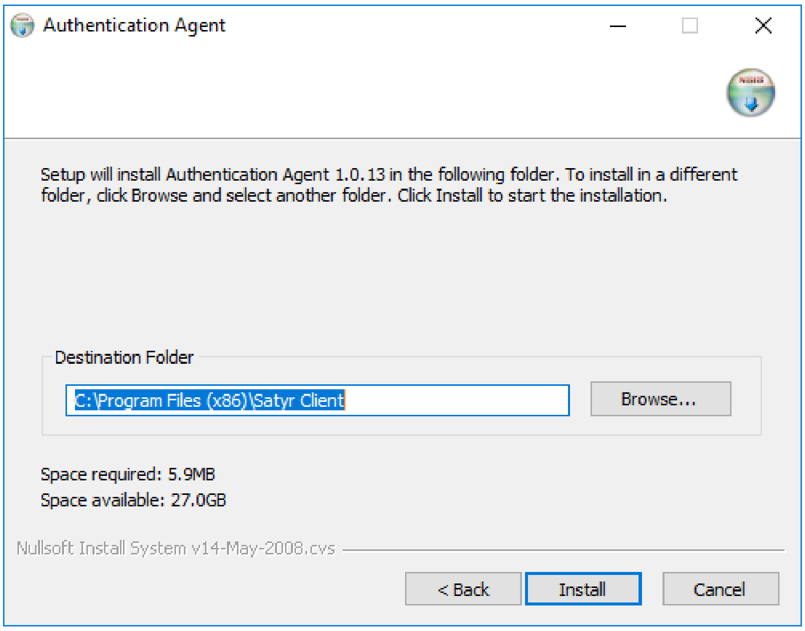
End-User License Agreement

(c) BalaSys IT Ltd.

Nullsoft Install System v14-May-2008.cvs

Figure 3.1. Accepting the EULA

Step 3. Select the destination folder for the application and click **Install**. The default folder in the 64-bit version of Windows is `C:\Program Files (x86)\Satyr Client` (in the 32-bit version of Windows, it is `C:\Program Files\Satyr Client`).



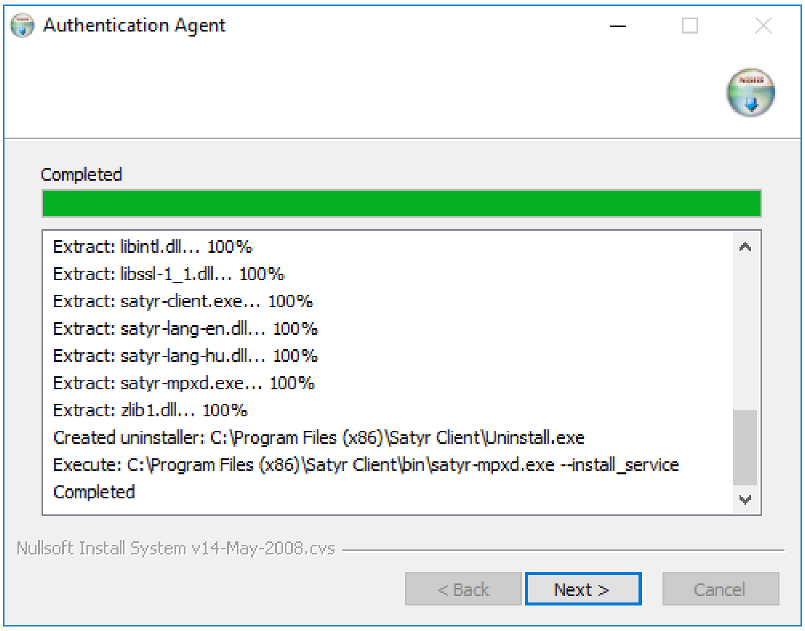
Setup will install Authentication Agent 1.0.13 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files (x86)\Satyr Client

Space required: 5.9MB
Space available: 27.0GB

Figure 3.2. Selecting the destination folder

Step 4. Click **Show details** to display details about the copied files. The installer copies the required files and registers the service called **Zorp Authentication Agent Multiplexer**, which is started after the registration.



Completed

```
Extract: libintl.dll... 100%
Extract: libssl-1_1.dll... 100%
Extract: satyr-client.exe... 100%
Extract: satyr-lang-en.dll... 100%
Extract: satyr-lang-hu.dll... 100%
Extract: satyr-mpxd.exe... 100%
Extract: zlib1.dll... 100%
Created uninstaller: C:\Program Files (x86)\Satyr Client\Uninstall.exe
Execute: C:\Program Files (x86)\Satyr Client\bin\satyr-mpxd.exe --install_service
Completed
```

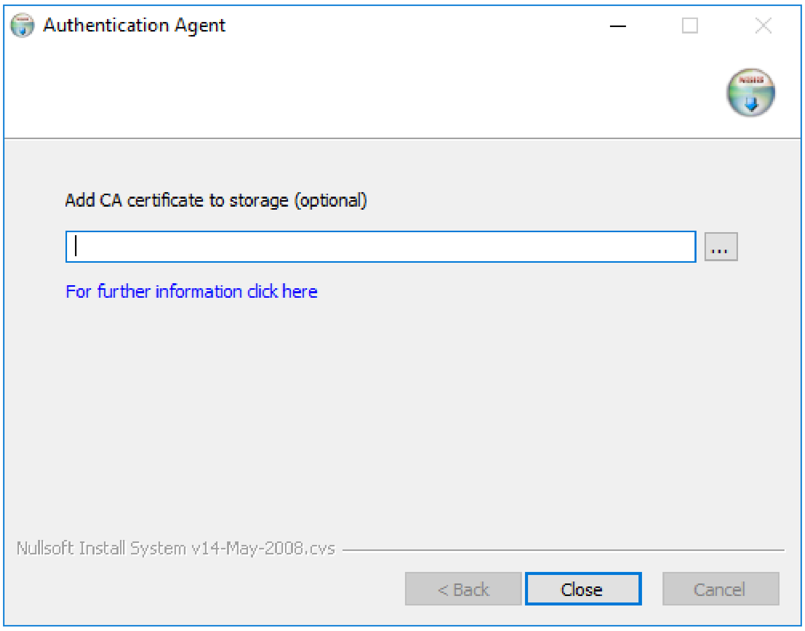
Figure 3.3. Copying the files

Step 5. *Optional step*: Click **Browse**, select the CA certificate to import, then click **Close** to import the CA certificate.

Note
For authentication purposes, when Zorp communicates with ZAA, ZAA expects TLS-encrypted communication. For details, see section *Section 4.1.1, Registry entries on Microsoft Windows platforms (p. 12)* and section *Section 4.1, Configuring Zorp Authentication Agent on Microsoft Windows platforms (p. 12)*.

If the Zorp Authentication Agent and Zorp communicate through an SSL-encrypted channel (recommended), the certificate of the Certificate Authority (CA) signing the certificates of the Zorp firewalls can be imported to the Zorp Authentication Agent.

Note
The CA certificate has to be in `DER` format. It is not necessary to import the certificate during the installation, it can also be done later. For details about encrypting the agent-Zorp authentication, see *Section 4.1.3, Configuring SSL connections on Microsoft Windows platforms (p. 15)*.


Authentication Agent
For further information click here
Nullsoft Install System v14-May-2008.cvs
< Back
Close
Cancel

Add CA certificate to storage (optional)

Figure 3.4. Importing the CA certificate

Step 6. After the installer has completed the above steps, click **Close**.

Step 7. The Zorp Authentication Agent (ZAA) logo is displayed on the system tray, indicating that the application is running. It is also started automatically after each Windows startup.

3.1.2. Procedure – Installing Zorp Authentication Agent with Group Policy Object (GPO) deployment

Prerequisites:

- Create the necessary certificates as instructed in the Zorp Professional Administrator Guide in section *Procedure 11.3.8.2, Creating certificates* in *Zorp Professional 7 Administrator Guide*.
- Set the parameters for the ZAS certificate.
- Export the CA certificate signed by ZAS in .der format for the Windows client.

Steps:

Step 1. Download the .exe format installer. The browser application or the Windows Defender Cloud might send a notification or a warning due to the new and unknown installer program, this can be disregarded.

Step 2. Install the Windows Client and import the CA certificate during the installation. Reboot the system, if it is necessary.

Step 3. Define the preferences with the help of the GUI or via the registry.

Step 4. Test the expected behaviour by initiating traffic.

Step 5. Export the following registries:

- Export the *HKEY_CURRENT_USER\Software\BalaBit\Satyr* registry to the *hlcuzaa.reg* file, which contains the user settings for ZAA. The result shall be as follows:

  ```
  Windows Registry Editor Version 5.00

  [HKEY_CURRENT_USER\Software\BalaBit]

  [HKEY_CURRENT_USER\Software\BalaBit\Satyr]
  "Has preferences"=dword:00000000
  "SSL"=dword:00000001
  "Automatic"=dword:00000001
  "Details"=dword:00000000
  "Can Remember"=dword:00000001
  "Forget Password"=dword:00000000
  "Forget Password Interval"=dword:00000001
  ```

- As ZAA Client is 32 bit executable, and runs on both 32 and 64 bit systems, if the target system is a 32 bit system, as Windows, for example, the following solution is required: Export the *HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr*, which contains the ZAA Multiplexer settings, into the *hklmzaa32.reg* file. The result shall be as follows:

  ```
  Windows Registry Editor Version 5.00

  [HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit]

  [HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr]
  "InstallLang"="1033"
  ```

- If the target system is a 64 bit system, export the *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr* registry to the *hklmzaa64.reg* file, which contains the multiplexer settings. The result shall be as follows:

  ```
  Windows Registry Editor Version 5.00

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit]

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr]
  "InstallLang"="1033"
  ```

Note

If the ZAA Client will be used on both 32 and 64 bit systems, create both registries, adding or removing the *WOW6432NODE* string to the paths. ZAA will use the corresponding one.

For more details, see *32-bit and 64-bit Application Data in the Registry*.

Later at the deployment, the registries can be distributed as duplicated keys on the target system safely, as detailed at the following site: *Registry key WOW6432Node may be listed in system registry in 32 bit (x86) version of Windows 7*.

The *service private certificate store*, used by the ZAA Multiplexer, can also be deployed as a registry key.

- Export the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd` registry to the *hklmzaacert.reg* file. The result shall be as follows:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd]


[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY\Certificates]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY\Certificates\6421DCB8501C2E1F15DB8BD3A94F435C01DB7CD3]
"Blob"=hex:03,00,00,00,01,00,00,00,14,00,00,00,64,21,dc,b8,50,1c,2e,1f,15,db,\
...
...
...
...
...
  64,0a,87,e9,45,99,04,9e,28,cb,c0,6c,2a,e5,c7,cb,ce,29,d8,b1,e1
```

Note

Note that there can be several empty paths created by the system automatically, which can be included safely.

For further details on registries, see *Section 4.1.1, Registry entries on Microsoft Windows platforms (p. 12)*.

As a result, there will be four registries exported.

Step 6. Switch to the GPO administrator system and download the ZAA *`msi flavor`* installer and place it in the Windows share where the other remotely installled applications are stored.

Step 7. Continue with the procedures detailed in section *Procedure 4.1.5, Configuring Group Policy Object (GPO) deployment (p. 26)*

3.2. Procedure – Installing Zorp Authentication Agent on Linux platforms

Purpose:

This section describes the installation of the Zorp Authentication Agent on Ubuntu Linux operating systems.

Steps:

Step 1. Create a mount point for the Zorp installation medium:

```
sudo mkdir -p /media/cdrom
```

Step 2. Mount the Zorp installation medium to the previous mount point.

```
sudo mount /dev/cdrom /media/cdrom -o ro
```

Step 3. Install the Balasys Gnu Privacy Guard (GPG) keys to allow the checking of Zorp package signatures by APT.

```
sudo /media/cdrom/install-balasys-archive-key.sh
```

Step 4. Make sure the following details are added as follows:

- Add the following lines to the `/etc/apt/auth.conf.d/satyr.conf` file:

  ```
  machine apt.balasys.hu
   login {your username}
  password {your password}
  ```

- Also limit the permissions:

  ```
  chmod 600 /etc/apt/auth.conf.d/satyr.conf
  ```

- Add the following lines to `/etc/apt/sources.list.d/zorp.list`

  ```
  deb https://apt.balasys.hu/zorp-os ubuntu-bionic/zorp-7.0latest satyr
  ```

Step 5. Install the Zorp Authentication Agent. Issue the following commands as root:

```
apt update
apt install satyr
```

The above commands install the `satyr` (Zorp Authentication Agent) and the `satyr-mpxd` (Zorp Authentication Agent Multiplexer) packages.

Step 6. Zorp Authentication Agent Multiplexer is automatically started after the installation. It can be stopped or started by issuing the `systemctl stop satyr-mpxd` or `systemctl start satyr-mpxd` commands, respectively.

Step 7. Zorp Authentication Agent is launched on desktop environment startup. It can be started manually by running `satyr-gtk`.

Chapter 4. Configuring Zorp Authentication Agent (ZAA)

4.1. Configuring Zorp Authentication Agent on Microsoft Windows platforms

4.1.1. Registry entries on Microsoft Windows platforms

Some settings of Zorp Authentication Agent (ZAA) can be modified through the Windows Registry. Launch the registry editor by issuing the `regedit` command (either from a command prompt or through the **Start** button).

In the 64-bit version of the Registry Editor, the Zorp Authentication Agent parameters, as the parameters of a 32-bit program, are located under: *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr* for the Multiplexer and *HKEY_CURRENT_USER\Software\BalaBit\Satyr* for the Client application.

The component has to be restarted if a value is modified (that is, the **Zorp Authentication Agent Multiplexer** service for Zorp Authentication Agent Multiplexer, the Authentication Client application for Zorp Authentication Agent).

To restart the Zorp Authentication Agent Multiplexer, select the **Start** button, type **Services** and then press **Enter**. Select **Authentication Multiplexer** on the list, then **Restart** it.

The following settings are available from the registry:

The following table presents the settings available from the *HKEY_CURRENT_USER\Software\BalaBit\Satyr* registry for the Client application.

HKEY_CURRENT_USER\Software\BalaBit\Satyr		
Name	**Description**	**Default value**
Automatic	To enable the automatic Kerberos authentication without user interaction with the Zorp Authentication Agent, set it to `1`. In this case, Zorp Authentication Agent will use the username provided during Windows login.	*dword:1*
Can Remember	To save your credentials so that the client will fill the username and password automatically for later authentication attempts, set this parameter to `1`. If it is set to `0`, the credentials will not be saved and have to be reentered again.	*dword:1*
Details	The Zorp Authentication Agent displays the details of the connection in the popup dialog if this parameter is set to `1`.	*dword:0*

HKEY_CURRENT_USER\Software\BalaBit\Satyr		
Name	**Description**	**Default value**
	The following information is displayed: the name of the application initiating the connection, the IP address and the port of the destination server, the name of the Zorp service started, and the type of the connection (TCP/UDP). If the details are disabled, only the name of the service is displayed.	
Forget Password	To store the authentication password indefinitely in the Zorp Authentication Agent, set this parameter to False. This sets the *Forget Password Interval* parameter to infinite.	*dword:0*
Forget Password Interval	To prevent unauthorized initiation of network connections through unattended machines, configure this parameter. Enter the number of minutes after which Zorp Authentication Agent deletes the stored password and requires authentication for new connection requests.	*dword:1*
Has Preferences	To enable the **Preferences** menu item in the system tray icon of Zorp Authentication Agent, set this parameter to 1. Otherwise, this menu item will not be available.	*dword:0*
LOG_CLIENT	It marks the verbosity level of the authentication client, ranging from 0 (lowest) to 9. Increase the log verbosity only if it is necessary (for example, for troubleshooting purposes), because setting it to higher than 3 can result in very large log files. The log file is stored in the user's home directory.	*dword:0*
InstallLang	The installer generates it.	*string*

Table 4.1. Registry setting options for the Client application

The following table presents the settings available from the *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr* registry in the 64 bit system and from the *HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr* registry in the 32 bit system for the Multiplexer.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr (64 bit system) **HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr (32 bit system)**		
Name	**Description**	**Default value**
`aliasfile`	This is the name and path (for example, `C:\tmp\aliases`) of a text file. Using the information contained in this file, the Zorp Authentication Agent Multiplexer can redirect the authentication of certain users to a different user in multi-user environments. For example, to redirect the connection authentication of the `Administrator` user to `MainUser` enter the following line: `Administrator: MainUser`.	string
`LOG`	It is the verbosity level of the Zorp Authentication Agent Multiplexer, ranging from `0` (lowest) to `9`. Increase log verbosity only if it is necessary (for example, for troubleshooting purposes), because setting it to higher than `3` can result in very large log files. The log file is stored in the `%SystemRoot%\SysWOW64\config\systemprofile` folder.	*`dword:3`*
`SSL`	To configure the Zorp Authentication Agent Multiplexer so that it uses only SSL-encrypted connections, set this parameter to `1`.	*`dword:1`*
`VerifyDepth`	It is the maximum length of the verification chain.	*`dword:3`*

Table 4.2. Registry setting options for the Multiplexer

4.1.2. Command line parameters on Microsoft Windows platforms

To display the version number of the client, enter `satyr-client.exe --version`.

The Zorp Authentication Agent Multiplexer (`satyr-mpxd.exe`) has the following command line options:

`--install_service`	It registers the Zorp Authentication Agent service.
`--remove_service`	It removes the Zorp Authentication Agent service.
`--start_service`	It starts the Zorp Authentication Agent service.
`--stop_service`	It stops the Zorp Authentication Agent service.

4.1.3. Configuring SSL connections on Microsoft Windows platforms

Zorp Authentication Agent Multiplexer and Zorp can communicate through an SSL-encrypted channel. For this, a certificate has to be available on the Zorp firewall that Zorp uses to authenticate the connection to the Zorp Authentication Agent Multiplexer. The Zorp Authentication Agent Multiplexer verifies this certificate using the certificate of the CA issuing Zorp's certificate, therefore the certificate of the CA has to be imported to the machine running the Zorp Authentication Agent.

> **Note**
> During authentication, when Zorp communicates with ZAA, ZAA expects TLS-encrypted communication. In order to disable this and to use the communication without encryption (which is strongly against the recommendation, but useful for debugging purposes), the SSL encryption shall be disabled by setting the *SSL* registry key to value '0'. For details on this parameter, see *Section 4.1, Configuring Zorp Authentication Agent on Microsoft Windows platforms (p. 12)*. Also see, *Procedure 3.1.1, Installing the Zorp Authentication Agent on Microsoft Windows (p. 4)*.

> **Note**
> It is highly recommended to encrypt the communication between Zorp and the Zorp Authentication Agent, because without it, anyone can connect to the Zorp Authentication Agent Multiplexer, resulting in the authentication information obtained by unauthorized people. It is essential to use encryption when password authentication is used. For details on encryption, see *Procedure 3.1.1, Installing the Zorp Authentication Agent on Microsoft Windows (p. 4)*.

4.1.3.1. Procedure – Encrypting the communication between Zorp and the Zorp Authentication Agent on Microsoft Windows platforms

Purpose:

To enable encryption between Zorp and the Zorp Authentication Agent, complete the following steps. For the steps to be completed from Zorp Management Console (ZMC), see *Chapter 11, Key and certificate management in Zorp* in *Zorp Professional 7 Administrator Guide*.

Steps:

Step 1. Create a CA (for example, *ZAA_CA*) using the Zorp Management Console (ZMC). This CA will be used to sign the certificates shown by the Zorp firewalls to the Authentication Agents.

Step 2. Export the CA certificate into DER format.

Step 3. Generate certificate request(s) for the Zorp firewall(s) and sign it with the CA created in Step 1.

> **Note**
> Each firewall shall have its own certificate. Do not forget to set the firewall as the **Owner host** of the certificate.

Step 4. Distribute the certificates to the firewalls.

Step 5. Install the Zorp Authentication Agent (ZAA) application to the workstations and import to each machine the CA certificate exported in Step 2.
There are three ways to import the CA certificate:

1. Import the CA certificate by using the installer of the Zorp Authentication Agent.

2. Import the CA certificate manually by using the addcert and getcert programs (see *Procedure 4.1.3.2, Importing the CA certificate manually (p. 16)*).
3. You can also import the CA certificate by using the Microsoft Management Console (see *Procedure 4.1.3.3, Importing the CA certificate using Microsoft Management Console (MMC) (p. 16)*).

Step 6. Create the appropriate outband authentication policies in ZMC and reference them among the services of Zorp. See *Chapter 15, Connection authentication and authorization* in *Zorp Professional 7 Administrator Guide* for details.

4.1.3.2. Procedure – Importing the CA certificate manually

Procedure:

To import the certificate of the CA using the addcert and getcert programs, complete the following steps.

Steps:

Step 1. The certificate can be imported using the addcert.exe program located in the installation folder of the Zorp Authentication Agent (C:\Program Files\Satyr client by default). The program can be started from a command prompt. Provide the name and the path of the DER-format certificate as an input parameter, for example:

- On 64 bit:

```
C:\Program Files (x86)\Satyr Client\bin\addcert.exe
C:\temp\AuthenticationAgent_CA.crt
```

- On 32 bit:

```
C:\Program Files\Satyr Client\bin\addcert
C:\tmp\AuthenticationAgent_CA.crt
```

Note
Running addcert.exe requires administrator privileges.

Step 2. Verify that the certificate has been successfully imported by running getcert.exe. Running getcert.exe lists the Subject of all imported certificates.

Step 3. Restart the **Zorp Authentication Agent Multiplexer** service.

4.1.3.3. Procedure – Importing the CA certificate using Microsoft Management Console (MMC)

Purpose:

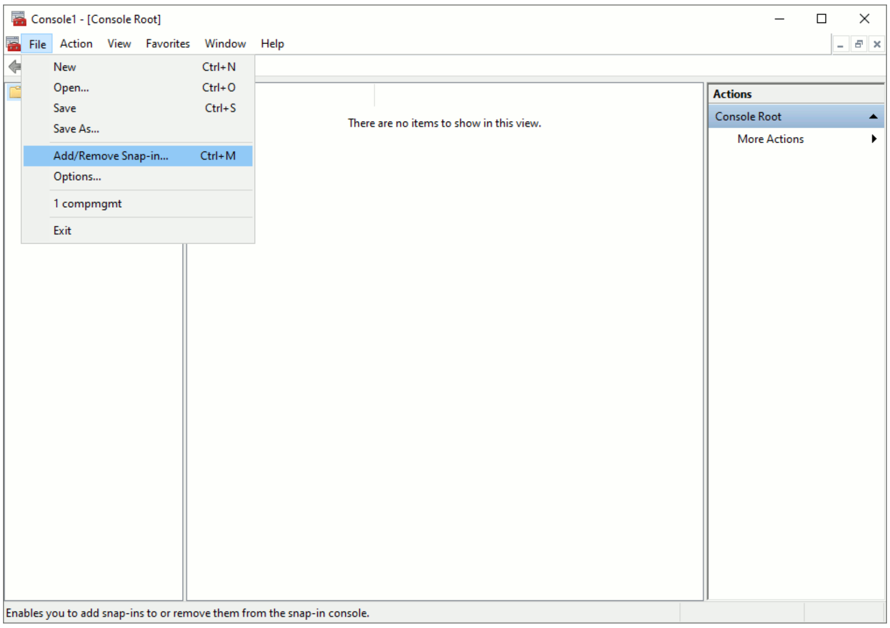
To import the certificate of the CA complete the following steps.

Steps:

Step 1. Start Microsoft Management Console by executing `mmc.exe` after selecting the **Start** button.

> **Note**
> Running `mmc.exe` requires administrator privileges.

Step 2. Select **Add/Remove Snap-in**, from the **File** menu.

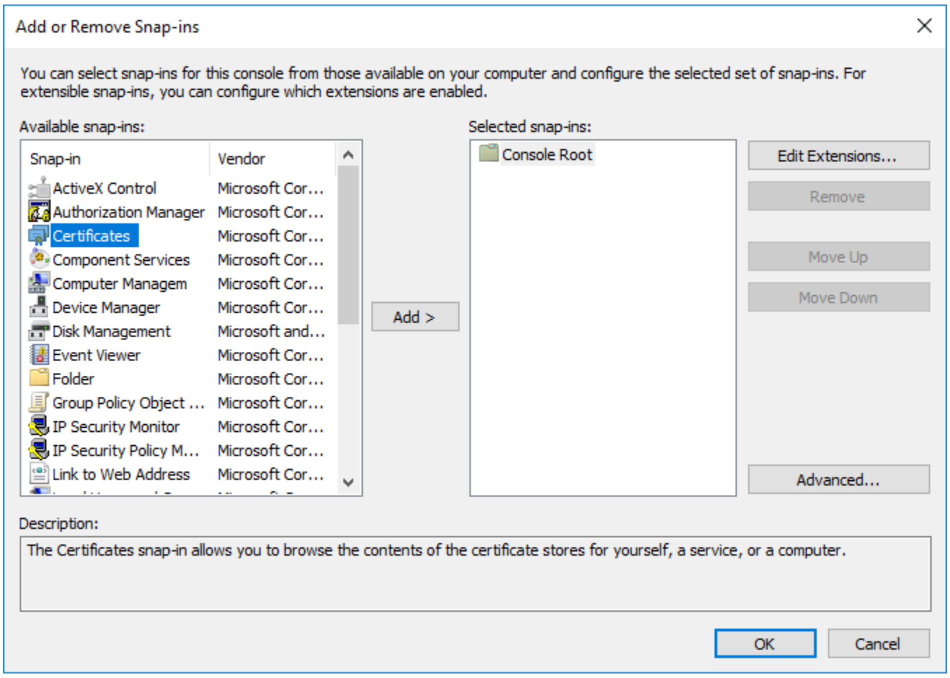


There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

Figure 4.1. Adding a snap-in

Step 3. Select **Certificates** and click **Add** from the **Available snap-ins** list.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

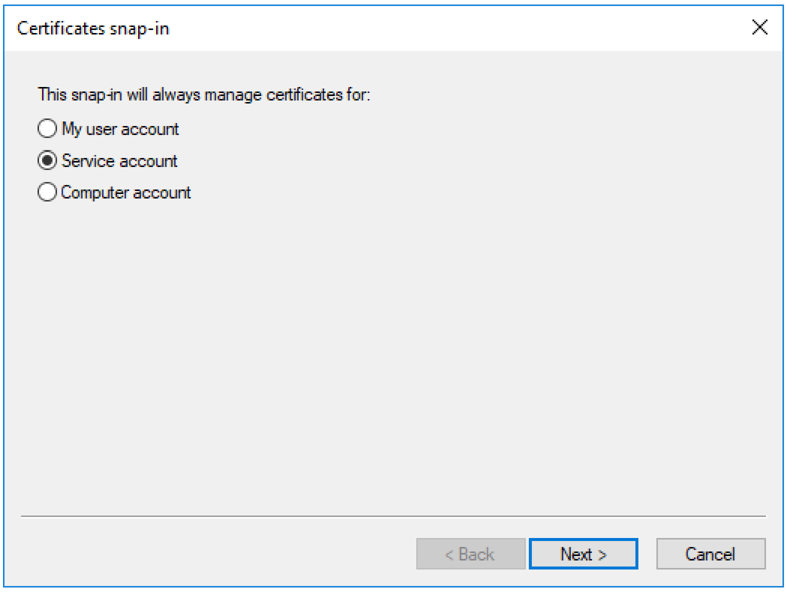
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 4.2. Adding certificates

Step 4. Select **Service account** and click **Next**.



Certificates snap-in

This snap-in will always manage certificates for:

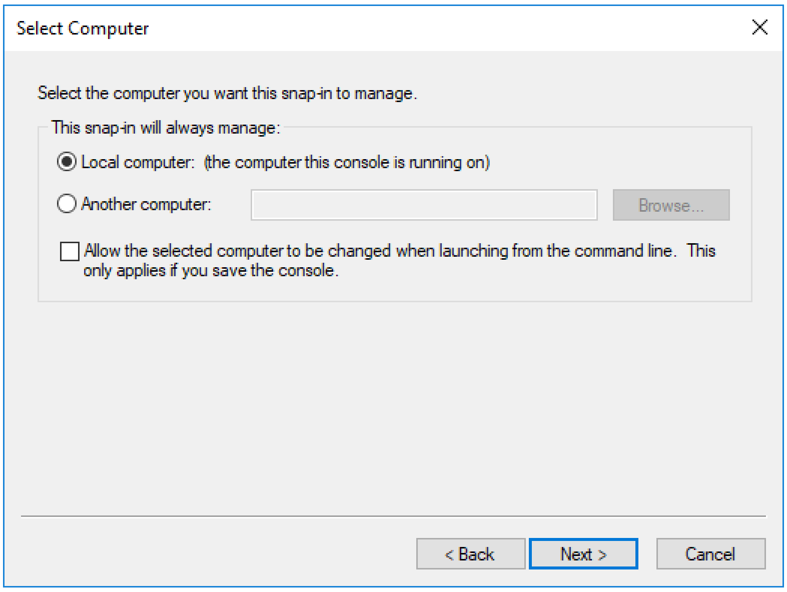
○ My user account

● Service account

○ Computer account

Figure 4.3. Selecting the service account

Step 5. Select **Local menu** and click **Next**.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

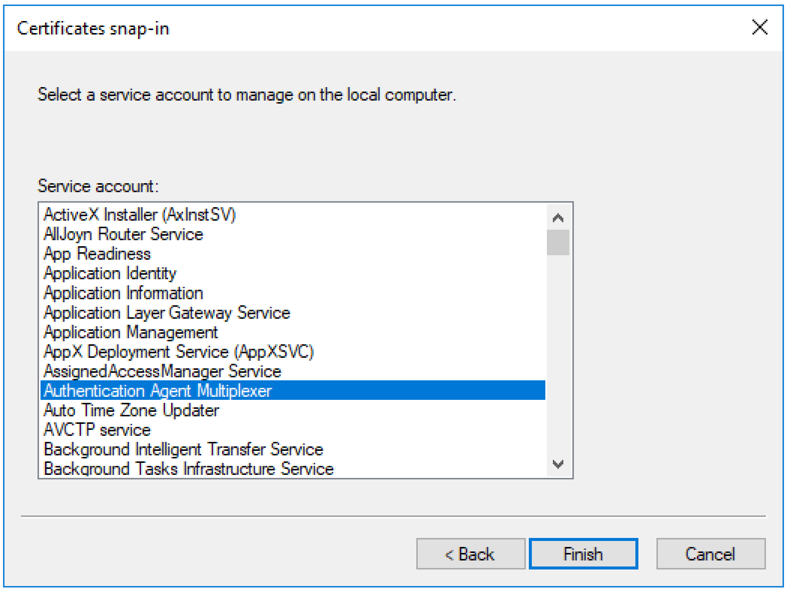
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Figure 4.4. Selecting the managed computer

Step 6. Select the **Zorp Authentication Agent Multiplexer** service and click **Finish**.



Certificates snap-in

Select a service account to manage on the local computer.

Service account:

- ActiveX Installer (AxInstSV)
- AllJoyn Router Service
- App Readiness
- Application Identity
- Application Information
- Application Layer Gateway Service
- Application Management
- AppX Deployment Service (AppXSVC)
- AssignedAccessManager Service
- Authentication Agent Multiplexer
- Auto Time Zone Updater
- AVCTP service
- Background Intelligent Transfer Service
- Background Tasks Infrastructure Service

Figure 4.5. Selecting the service

With the above steps a snap-in module has been configured that enables to conveniently manage the certificates related to the Zorp Authentication Agent Multiplexer.

Step 7. Navigate to **Certificates - Service (Authentication Multiplexer)** > **satyr-mpxd\Personal** > **Certificates**, and click **Add**.

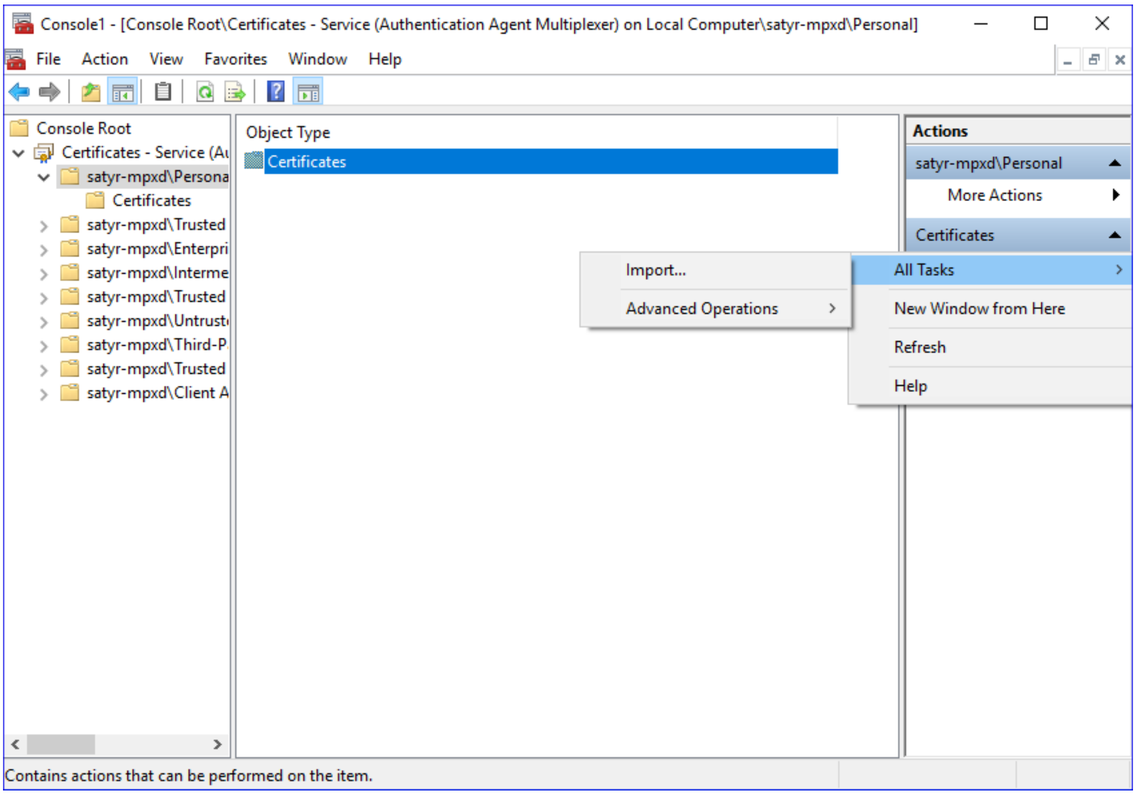
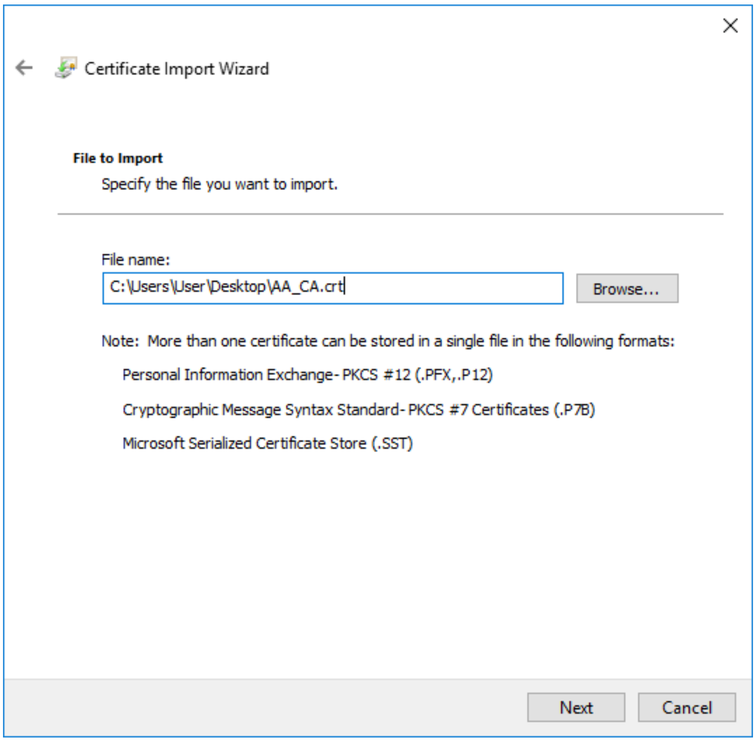


Figure 4.6. Importing the CA certificate

Step 8. Right-click **Certificates**, navigate to **All tasks** > **Import**. The **Certificate Import Wizard** is displayed. Click **Next**.

Step 9. Select the certificate to import and click **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\User\Desktop\AA_CA.crt

Note: More than one certificate can be stored in a single file in the following formats:

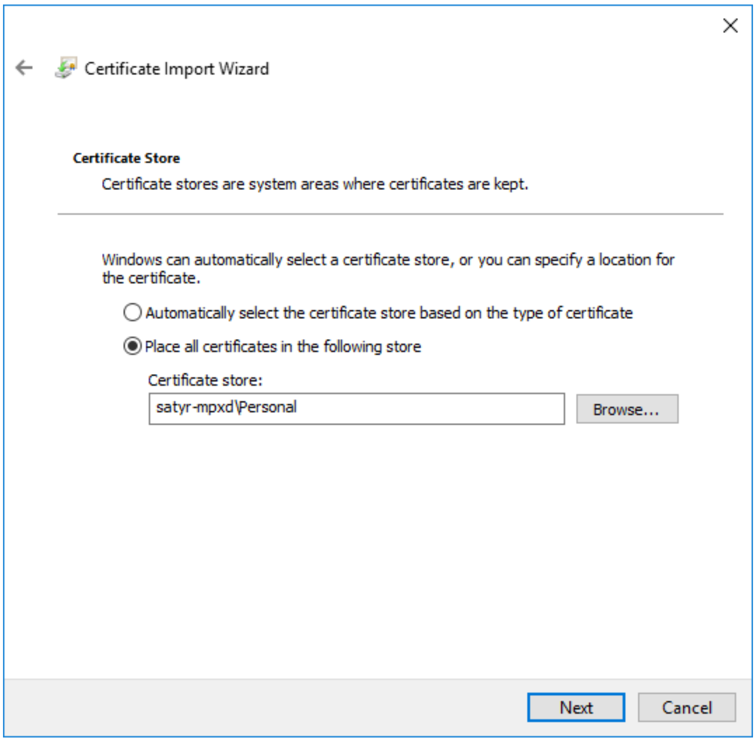
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Figure 4.7. Selecting the certificate to import

Step 10. Click **Next**, when Windows offers a suitable certificate store by default.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

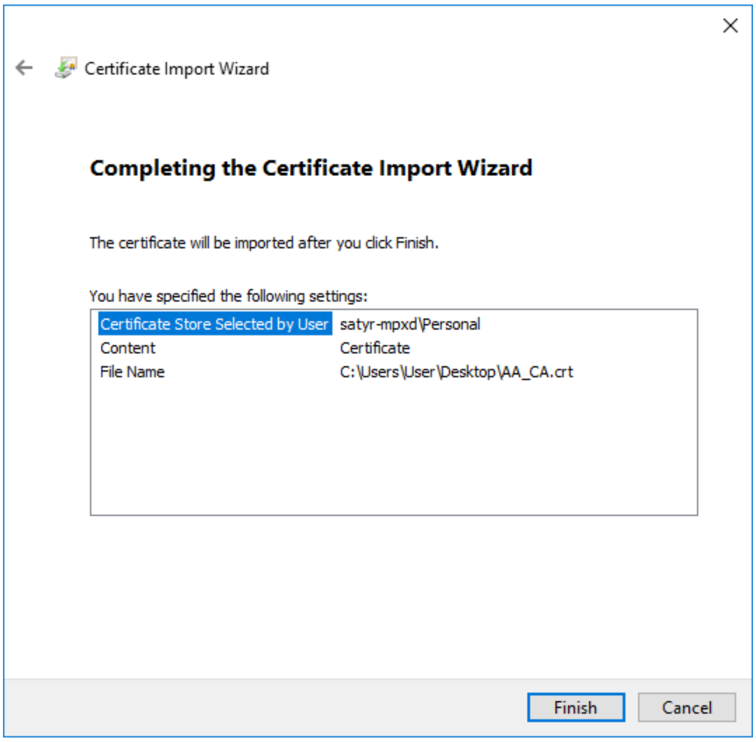
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: satyr-mpxd\Personal

Figure 4.8. Selecting the certificate store

Step 11. Click **Finish** on the summary window and **OK** on the window that marks the successful import of the certificate.



Completing the Certificate Import Wizard

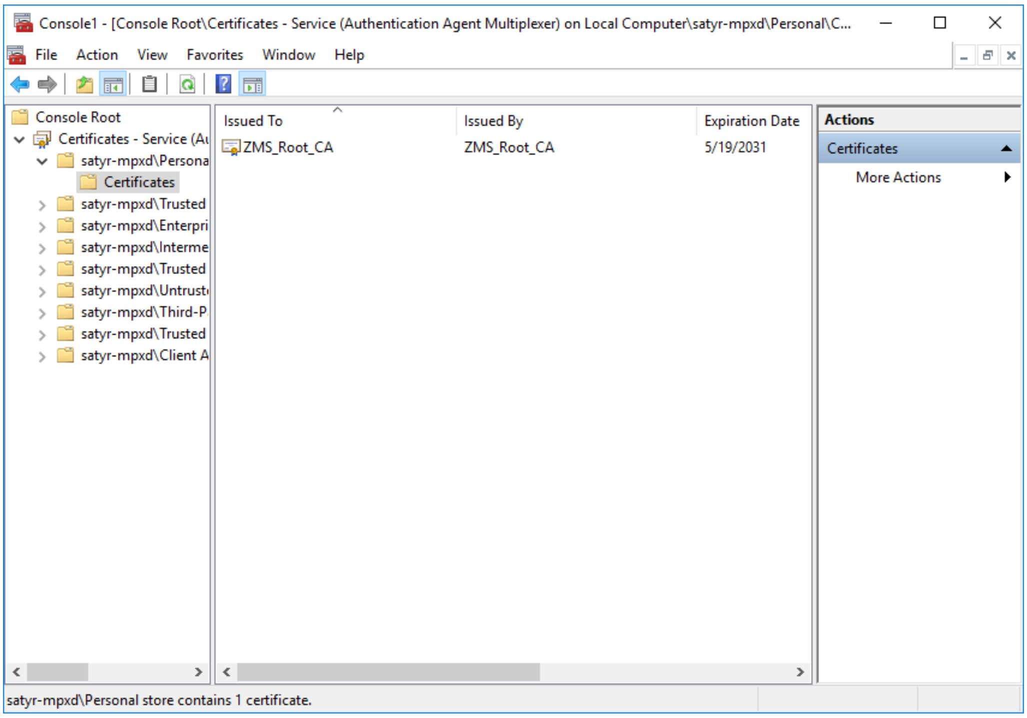
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	satyr-mpxd\Personal
Content	Certificate
File Name	C:\Users\User\Desktop\AA_CA.crt

Figure 4.9. Summary

The main window of MMC is displayed with the imported certificate.



Console1 - [Console Root\Certificates - Service (Authentication Agent Multiplexer) on Local Computer\satyr-mpxd\Personal\C...

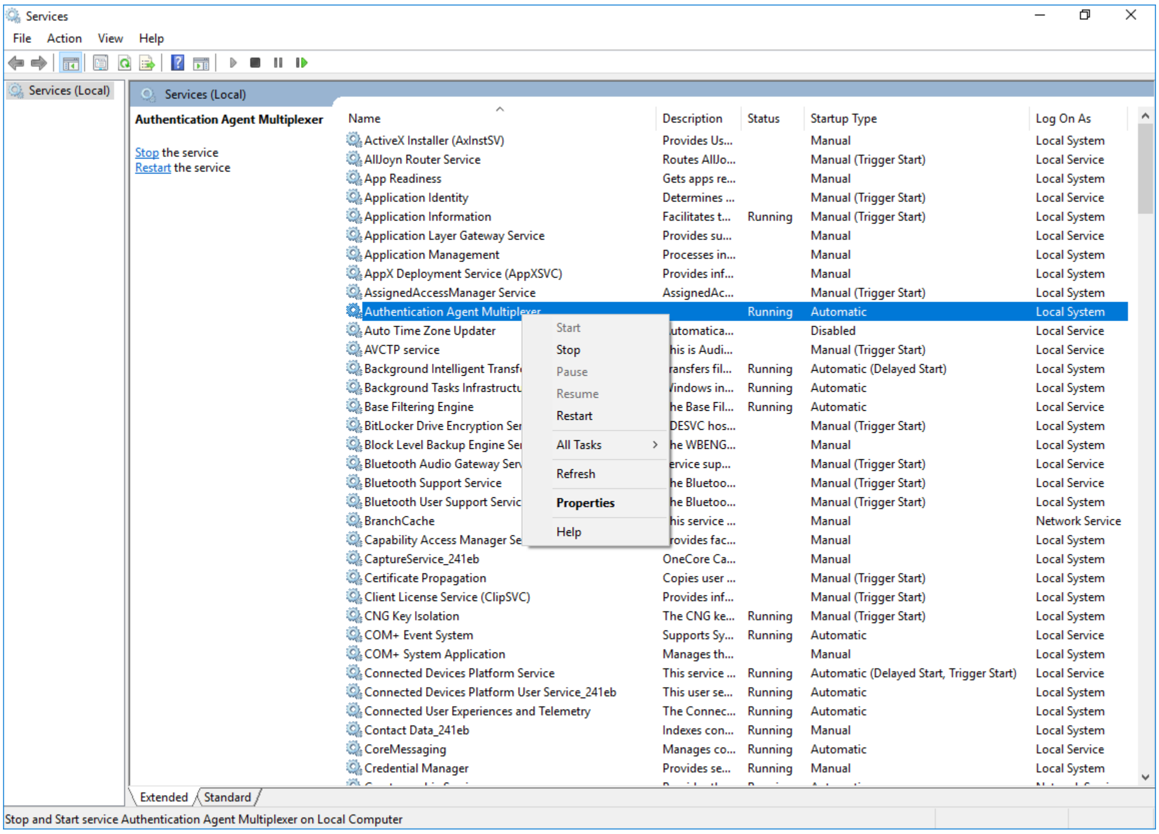
Issued To	Issued By	Expiration Date
ZMS_Root_CA	ZMS_Root_CA	5/19/2031

satyr-mpxd\Personal store contains 1 certificate.

Figure 4.10. The imported certificate

Step 12. Restart the Zorp Authentication Agent service. Scroll to the **Zorp Authentication Agent Multiplexer** among the list of Services and right-click on it. Navigate to **All Tasks** > **Restart**.

It is also possible to start and stop the Zorp Authentication Agent here.



Authentication Agent Multiplexer

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigger Start)	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigger Start)	Local Service
Application Information	Facilitates t...	Running	Manual (Trigger Start)	Local System
Application Layer Gateway Service	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (AppXSVC)	Provides inf...		Manual	Local System
AssignedAccessManager Service	AssignedAc...		Manual (Trigger Start)	Local System
Authentication Agent Multiplexer		Running	Automatic	Local System
Auto Time Zone Updater	utomatica...		Disabled	Local Service
AVCTP service	his is Audi...		Manual (Trigger Start)	Local Service
Background Intelligent Transf	ransfers fil...	Running	Automatic (Delayed Start)	Local System
Background Tasks Infrastructu	Vindows in...	Running	Automatic	Local System
Base Filtering Engine	he Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption Ser	DESVC hos...		Manual (Trigger Start)	Local System
Block Level Backup Engine Ser	he WBENG...		Manual	Local System
Bluetooth Audio Gateway Serv	ervice sup...		Manual (Trigger Start)	Local Service
Bluetooth Support Service	he Bluetoo...		Manual (Trigger Start)	Local Service
Bluetooth User Support Servic	he Bluetoo...		Manual (Trigger Start)	Local System
BranchCache	his service ...		Manual	Network Service
Capability Access Manager Se	rovides fac...		Manual	Local System
CaptureService_241eb	OneCore Ca...		Manual	Local System
Certificate Propagation	Copies user ...		Manual (Trigger Start)	Local System
Client License Service (ClipSVC)	Provides inf...		Manual (Trigger Start)	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trigger Start)	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local System
Connected Devices Platform Service	This service ...	Running	Automatic (Delayed Start, Trigger Start)	Local Service
Connected Devices Platform User Service_241eb	This user se...	Running	Automatic	Local System
Connected User Experiences and Telemetry	The Connec...	Running	Automatic	Local System
Contact Data_241eb	Indexes con...	Running	Manual	Local System
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local System

Stop and Start service Authentication Agent Multiplexer on Local Computer

Figure 4.11. Restarting the Zorp Authentication Agent

4.1.4. Procedure – Configuring X.509 certificate based authentication on Microsoft Windows platforms

Purpose:

For authentication based on X.509 certificates the certificate and the private key of the user has to be deployed onto the workstation. Import the certificate of the user into their personal certificate store. This can be accomplished most easily through the **Certificates** Control Panel item.:

Steps:

Step 1. Click the **Start** button and type **Manage user certificates** then press **Enter**.

Step 2. Navigate to **Certificates - Current User** > **Personal** > **Certificates**.

Step 3. Right-click **Certificates** and navigate to **All tasks - Import**.
The **Certificate Import Wizard** is displayed.

Note
Hardware keys and tokens having a suitable driver for Windows are also displayed in this store and can be used from the Zorp Authentication Agent.

Step 4. Import the certificate, using the **Certificate Import Wizard** tool.

4.1.5. Procedure – Configuring Group Policy Object (GPO) deployment

Step 1. Import all four registry files to the GPO configurator system, so that the Registry Wizard can browse them. Later, remove the registry information if it is no longer required. If it is not possible to remove them, all four files have to be configured as registry keys.

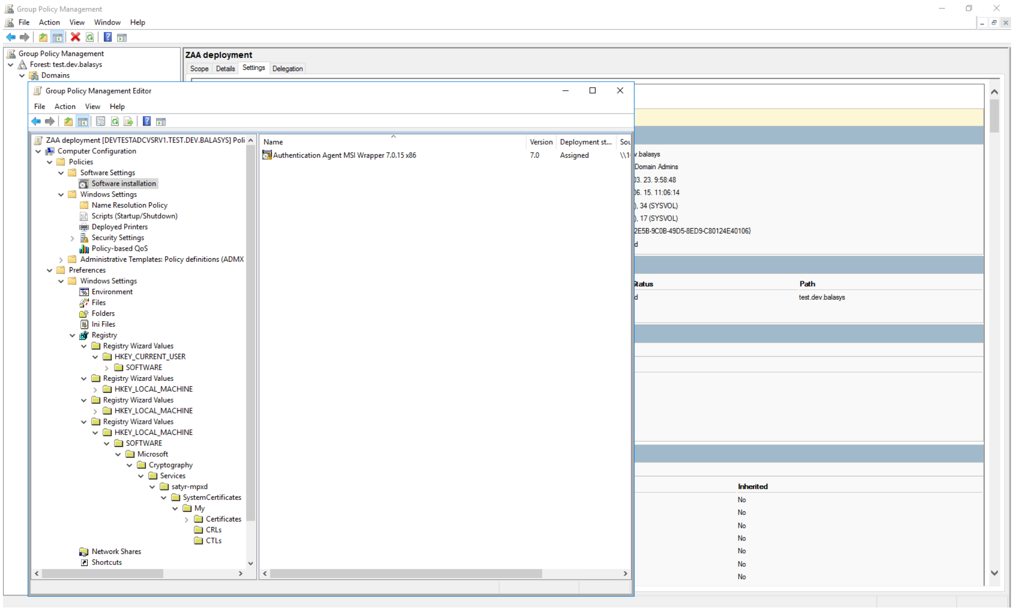
Step 2. Create a new policy to the corresponding forest as *ZAA deployment*.

Step 3. Configure the corresponding parameters, as, for example, target scope or filtering and so on.

Step 4. Edit the *ZAA Deployment* policy.

Step 5. Add the *ZAA msi installer* as a new package under the **Computer Configuration/Policies/Software Settings/Software installation** path.

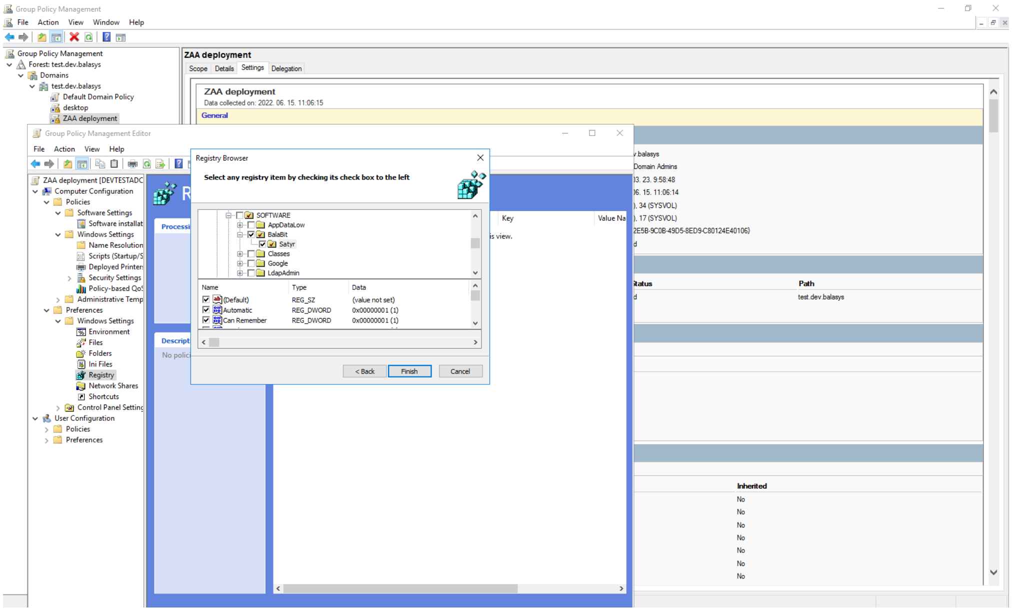
Step 6. Browse the network share for the newly added package, select it, and set it to Auto installation.



Name	Version	Deployment st...	Sou
Authentication Agent MSI Wrapper 7.0.15 x86	7.0	Assigned	\\1

Figure 4.12. The result of auto installation

Step 7. Import all four registry settings with the help of the Registry Wizard. The *HKLM* registries under the **Computer Configuration/Preferences/Windows Settings/Registry** path, and the *HKCU* registries under the **User Configuration/Preferences/Windows Settings/Registry** path.



ZAA deployment

Data collected on: 2022. 06. 15. 11:06:15

Name	Type	Data
☑ (Default)	REG_SZ	(value not set)
☑ Automatic	REG_DWORD	0x00000001 (1)
☑ Can Remember	REG_DWORD	0x00000001 (1)

Figure 4.13. Importing registries

Step 8. Close the GP editor.

4.2. Configuring ZAA on Linux platforms

4.2.1. Command line parameters on Linux platforms

The graphical client (`satyr-gtk`) has the following command line parameters:

`--help` or `-?`	It displays a brief help message.
`--version` or `-V`	It displays version number and compilation information.
`--automatic` or `-a`	It enables automatic Kerberos authentication.
`--no-syslog` or `-l`	It sends log messages to the standard output instead of syslog.
`--verbose <verbosity>` or `-v <verbosity>`	It sets verbosity level to <verbosity>. The default verbosity level is `3`; the possible values are `0`-`10`.
`--logtags;` or `-T`	It prepends log category and log level to each message.

Zorp Authentication Agent Multiplexer (`satyr-mpxd`) has the following command line parameters:

`--help` or `-?`	It displays a brief help message.
`--version` or `-V`	It displays the version number of `satyr-mpxd`.
`--no-syslog` or `-l`	It sends log messages to the standard output instead of syslog.
`--verbose <verbosity>` or `-v <verbosity>`	It sets verbosity level to <verbosity>. The default verbosity level is `3`; possible values are `0`-`10`.
`--logtags;` or `-T`	It prepends log category and log level to each message.

`--aliasfile;` or `-a`

It is the name (including full path) of a text file (for example, `/tmp/aliases`) used by Zorp Authentication Agent Multiplexer to redirect the authentication requests of certain users to a different user in multiuser environments. For example, to redirect all authentication request of the *`root`* user to *`MainUser`* add the following line to the file: *`root: MainUser`*.

`--log-spec;` or `-s`

It sets verbosity mask on a per category basis. Each log message has an assigned multi-level category, where levels are separated by a dot. For example, HTTP requests are logged under *http.request*. The `<spec>` is a comma-separated list of log specifications. A single log specification consists of a wildcard matching log category, a colon, and a number specifying the verbosity level of that given category. The categories match from left to right, for example, `--logspec 'http.*:5,core:3'`. The last matching entry will be used as the verbosity of the given category. If no match is found the default verbosity specified with `--verbose` is used.

`--no-require-ssl;` or `-S`

It turns off the SSL encryption of the communication between Zorp and the Multiplexer.

`--bind-address;` or `-b` and , `--bind-port;` or `-p`

It is the IP address and the port, the Multiplexer is accepting connections on.

`--crt-dir;` or `-t`

It is the path of the directory containing the certificate of the CA that issued the certificate of the Zorp firewall.

`--crl-dir;` or `-r`

It is the path of the directory containing the Certificate Revocation List (CRL) related to the above CA.

4.2.2. Configuring SSL connections on Linux platforms

To enable encryption between Zorp and the Zorp Authentication Agent complete the following steps. For the steps to be completed from ZMC, see *Chapter 11, Key and certificate management in Zorp* in *Zorp Professional 7 Administrator Guide*.

Note
During authentication, when Zorp communicates with ZAA, ZAA expects TLS-encrypted communication. In order to disable this and to use the communication without encryption (which is strongly against the recommendation, but useful for debugging purposes), the SSL encryption shall be disabled by setting the *`--no-require-ssl; or -S`* command line parameter.

4.2.2.1. Procedure – Encrypting the communication between Zorp and the Zorp Authentication Agent on Linux platforms

Steps:

Step 1. Create a CA (for example, *`AA_CA`*) using the Zorp Management Console (ZMC). This CA will be used to sign the certificates shown by the Zorp firewalls to the Authentication Agents.

Step 2. Export the CA certificate into `PEM` format.

Step 3. Generate certificate request(s) for the Zorp firewall(s) and sign it with the CA created in Step 1.

> **Note**
> Each firewall shall have its own certificate. Do not forget to set the firewall as the **Owner host** of the certificate.

Step 4. Distribute the certificates to the firewalls.

Step 5. Install the Zorp Authentication Agent (ZAA) application to the workstations and import to each machine the CA certificate exported in Step 2.
To import the CA certificate complete the following steps:

Step a. Create the `/etc/satyr/ca` directory:

```
mkdir /etc/satyr/ca
```

Step b. Copy the certificate exported into `PEM` format in Step 2 into the `/etc/satyr/ca` directory.

Step c. Create symlinks to the certificate files:

```
c_rehash .
```

Step d. Restart the **Zorp Authentication Agent Multiplexer daemon**:

```
systemctl restart satyr-mpxd.service
```

The authentication client is now ready to accept encrypted connections from Zorp.

Step 6. Create the appropriate outband authentication policies in ZMC and reference them among the services of Zorp. For details, see *Chapter 15, Connection authentication and authorization* in *Zorp Professional 7 Administrator Guide*.

4.2.3. Configuring X.509 certificate-based authentication on Linux platforms

For authentication based on X.509 certificates the certificate and the private key of the user has to be deployed onto the workstation. Create a directory called `.satyr` in the home folder of the user and copy the certificate and private key of the user in `PEM` format into this directory. Use the `cert.pem` and `key.pem` filenames, or create symlinks with these names pointing to the certificate and the key file. The Zorp Authentication Agent will automatically use the certificate found in this directory.

Chapter 5. Using the Zorp Authentication Agent (ZAA)

Purpose:

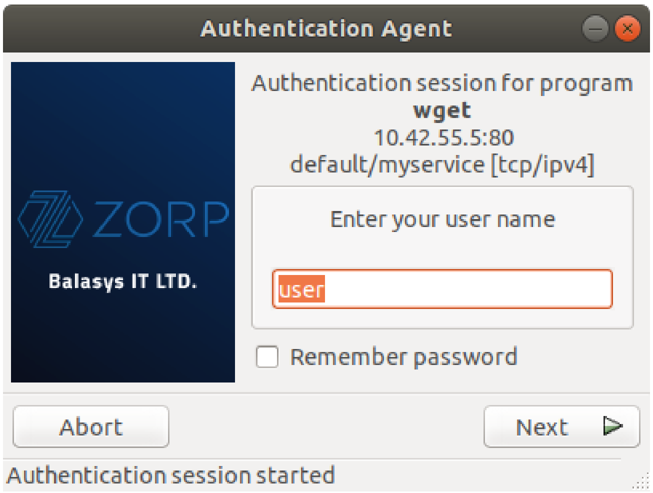
When the user launches an application that requires authentication (for example, a web browser, e-mail client, and so on) the Zorp firewall automatically displays the authentication client on the user's screen.

The client displays the name of the service requiring authentication (`intra_http` in the above example), and — provided that the administrator enabled it — further details of the connection (for example, destination IP address).

Steps:

Step 1. To save your credentials so that the client will fill in the username and password automatically for later authentication attempts, select **Remember password**. For details on configuring password storage period length and deleting a previously saved password, see *Procedure 6., (p. 33)*.
To cancel the authentication at any time, click **Abort**.

Step 2. Enter your user name in the **Enter your user name** field and click **Next**.



Authentication session for program
wget
10.42.55.5:80
default/myservice [tcp/ipv4]

Enter your user name

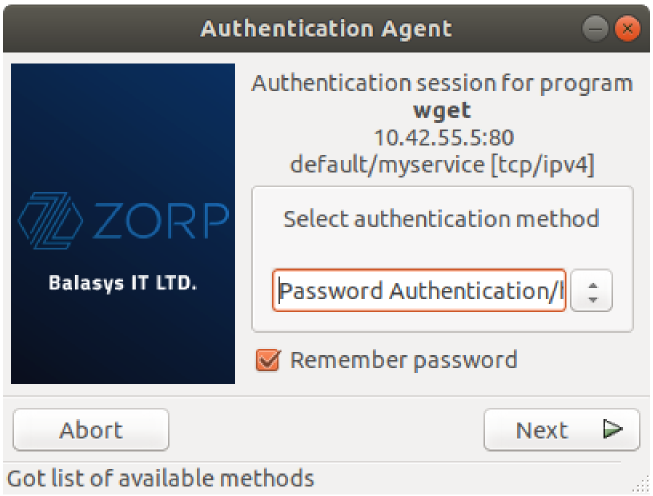
user

□ Remember password

Authentication session started

Figure 5.1. The Zorp Authentication Agent

Step 3. Select the authentication method to use from the **Select authentication method** list. The list displays only the methods that are available for this user.



Authentication session for program
wget
10.42.55.5:80
default/myservice [tcp/ipv4]

Select authentication method

Password Authentication/I

☑ Remember password

Got list of available methods

Figure 5.2. Selecting authentication method

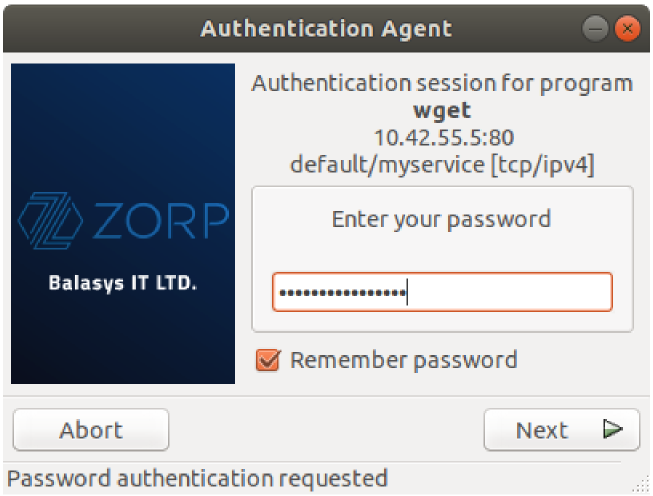
Step a. To authenticate with a password, select **Password authentication**.

Step b. To use Kerberos authentication, select **GSSAPI authentication**.

Note
When using Kerberos authentication the authentication client is not displayed if you have configured **Automatic Kerberos authentication** in **Preferences**. For details, see *Procedure 6., (p. 33)*.

Step c. To authenticate with an X.509 certificate, select **X.509 certificate**.

Step 4. Provide the information required for the selected authentication method. For example, for **Password authentication**, enter your password.



Authentication Agent

Authentication session for program
wget
10.42.55.5:80
default/myservice [tcp/ipv4]

Enter your password

••••••••••••••••

☑ Remember password

Password authentication requested

Figure 5.3. Entering the password

Note
After successful authentication, the window of the authentication client is closed automatically, and the connection to the target server is established. If the authentication fails, the client displays an error message.

Chapter 6. Configuring Zorp Authentication Agent preferences

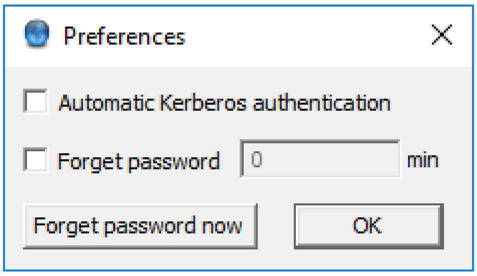
Purpose:

Zorp Authentication Agent is launched on desktop environment startup, and places its icon on the system tray. To configure Zorp Authentication Agent preferences, complete the following steps.

Note
To display the version number and other information about Zorp Authentication Agent, right-click the system tray icon and click **About**.

Steps:

Step 1. Right-click the system tray icon and click **Preferences**.



☐ Automatic Kerberos authentication

☐ Forget password 0 min

Figure 6.1. Preferences

Step 2. To enable automatic Kerberos authentication without user interaction with the Zorp Authentication Agent, select **Automatic Kerberos authentication**. In this case, Zorp Authentication Agent will use the username provided during Windows or Linux desktop session login.

Step 3. To prevent unauthorized initiation of network connections through unattended machines, configure **Forget password**. Enter the number of minutes after which Zorp Authentication Agent deletes the stored password and requires authentication for new connection requests.

Step 4. To immediately delete the stored password from the Zorp Authentication Agent and require authentication for new connection requests, click **Forget password now**.
ZAA stores its preferences in the `~/.config/aa/aa.cfg` configuration file on Linux, and in the Windows Registry on Microsoft Windows platforms, for more information see *Section 4.1.1, Registry entries on Microsoft Windows platforms (p. 12)*.

Chapter 7. Starting and stopping Zorp Authentication Agent

To start or stop Zorp Authentication Agent, perform one of the following steps.

- To stop Zorp Authentication Agent, right-click the system tray icon and click **Exit**.
- To restart the Zorp Authentication Agent select the **Start** button, type **Zorp Authentication Agent** and then press **Enter**.