Authentication Agent Manual

June 04, 2020

Abstract

This document describes how to install and configure the Authentication Agent

Table of Contents

1. Introduction

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

2. Authentication and PNS

Authentication Agent (AA) is an authentication client, capable of cooperating with the PNS firewall and the Authentication Server (AS) to identify the users initiating network connections. The authentication process and the related communication between the components is summarized below. For details, see *Chapter 15, Connection authentication and authorization* in *Proxedo Network Security Suite 1.0 Administrator Guide*.

Authentication aims to determine the identity of the user. During the authentication process the user initiating the connection shares a secret (for example, a password) with the other party that verifies its authenticity.

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

1. The user knows a secret, 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 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 Authentication Agent (AA), AS, and PNS 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 PNS

Purpose:

PNS implements outband authentication according to the following procedure:

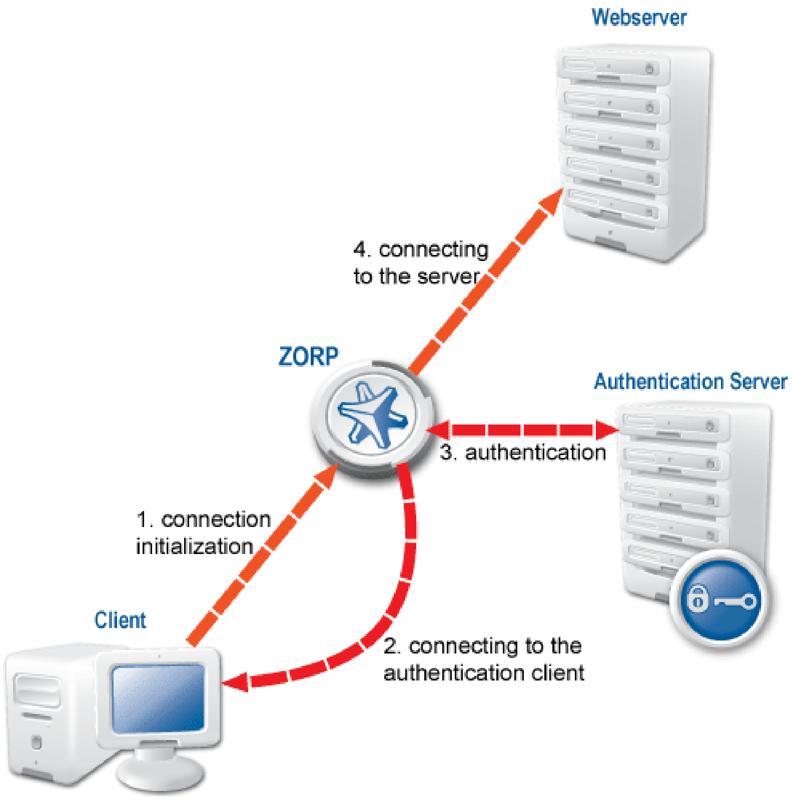

Webserver
4. connecting to the server
ZORP
Authentication Server
3. authentication
1. connection initialization
Client
2. connecting to the authentication client

Figure 1. Outband authentication with PNS

Steps:

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

Step 2. PNS 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), PNS initiates a connection towards the client using the Authentication Agent protocol.

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

Step 4. The PNS firewall connects to Authentication Server (AS) 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. PNS 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 authentication agent sends the data (for example, the password) to PNS that forwards it to AS.

Step 7. AS performs the authentication and notifies PNS about the result (success/failure).

Step 8. PNS 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.

3. Installing the Authentication Agent (AA)

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

- Windows 10 LTSB (Long-Term Servicing Branch)
- Windows Server 2012R2, 2016, 2019
- Ubuntu 18.04 Bionic Beaver (64-bit only)

The agent has two components:

1. *Authentication Agent Multiplexer*: A daemon running in the background, accepting the connections coming from PNS and verifying the SSL certificates of PNS (if the communication is encrypted). In a multi-user environment the Multiplexer displays the dialog of the *Authentication Agent* on the desktop of the user initiating a connection requiring authentication.
2. *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 5 MB of free hard disk space.

3.1. Procedure – Installing the Authentication Agent (AA) on Microsoft Windows platforms

Purpose:

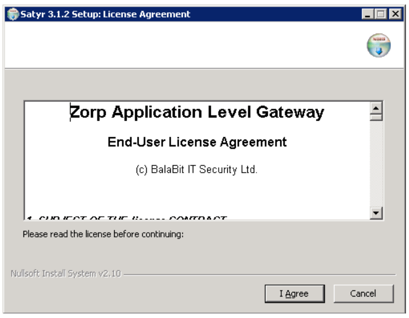
The Authentication Agent (AA) installer is located in the `\windows\satyr\` folder of the PNS CD-ROM, its latest version is also available from the *website*).

Steps:

Step 1. Place the PNS 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.



Satyr 3.1.2 Setup: License Agreement

Zorp Application Level Gateway

End-User License Agreement

(c) BalaBit IT Security Ltd.

1. SUBJECT OF THE license CONTRACT

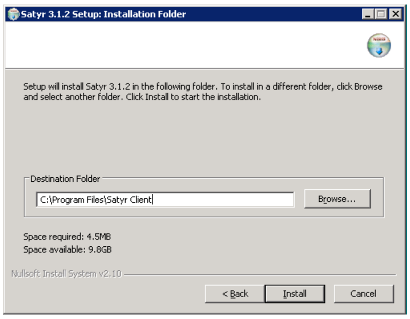
Please read the license before continuing:

Nullsoft Install System v2.10

Figure 2. Accepting the EULA

After the installer starts, the End-User License Agreement is displayed. To accept the End-User License Agreement, click **I agree**. To cancel the installation at any time during the process, click **Cancel**.

Step 3.



Satyr 3.1.2 Setup: Installation Folder

Setup will install Satyr 3.1.2 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\Satyr Client

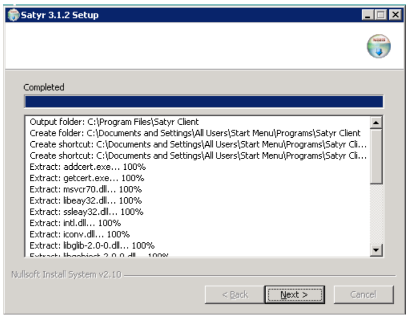
Space required: 4.5MB
Space available: 9.8GB

Nullsoft Install System v2.10

Figure 3. Selecting the destination folder

Select the destination folder for the application and click **Install**. The default folder is `C:\Program Files\Satyr Client`. The Authentication Agent (AA) requires about 5 MB of free disk space.

Step 4.



Satyr 3.1.2 Setup

Completed

```
Output folder: C:\Program Files\Satyr Client
Create folder: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Client
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Cli...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Cli...
Extract: addcert.exe... 100%
Extract: getcert.exe... 100%
Extract: msvcr70.dll... 100%
Extract: libeay32.dll... 100%
Extract: ssleay32.dll... 100%
Extract: intl.dll... 100%
Extract: iconv.dll... 100%
Extract: libglib-2.0-0.dll... 100%
Extract: libgobject-2.0-0.dll... 100%
```

Nullsoft Install System v2.10

Figure 4. Copying the files

The installer copies the required files and registers a service called *Satyr Multiplexer*, which is started after the registration. To display details about the copied files, click **Show details**.

Step 5.

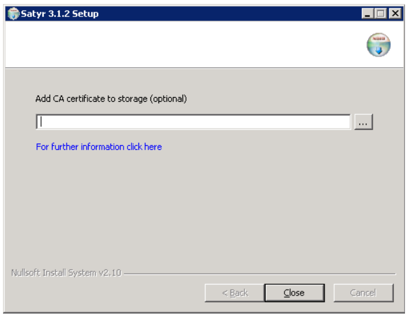

Satyr 3.1.2 Setup
Add CA certificate to storage (optional)
...
For further information click here
Nullsoft Install System v2.10
< Back
Close
Cancel

Figure 5. Importing the CA certificate

Optional step: If the authentication agent and PNS communicate through an SSL-encrypted channel (recommended), the certificate of the Certificate Authority (CA) signing the certificates of the PNS firewalls can be imported to the authentication agent. To import the CA certificate, click **Browse**, select the CA certificate to import, then click **Close**.

> **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-PNS authentication, see *Section 4.1.3, Configuring SSL connections (Windows) (p. 14)*.

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

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

3.2. Procedure – Installing Authentication Agent on Linux platforms

Purpose:

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

Steps:

Step 1. As a first step, upgrade the `apt` package manager to support HTTPS connections. Make sure the following lines are in your `/etc/apt/sources.list` file:

> **Note**
> Replace `username` and `password` with your username and password received from . If you are installing Authentication Agent manually, use your personal account credentials.

- For Ubuntu 10.04:

```
deb
https://USERNAME:PASSWORD@apt.balasys.hu/ubuntu-bionic/zorp-1.0latest
 satyr
```

Step 2. Issue the following commands as root:

```
apt update
apt install apt
```

Step 3. Install the authentication agent. Issue the following commands as root:

```
apt update
apt install satyr
```

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

Step 4. 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 5. Authentication Agent is launched when X11 is started. It is important that it has to be started manually by running `satyr-gtk`.

4. Configuring Authentication Agent (AA)

4.1. Configuring Authentication Agent on Microsoft Windows platforms

4.1.1. Registry entries

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

The parameters of the Authentication Agent are located under *`HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr`*.

The component column contains the name of the component related to the parameter. This component has to be restarted if a value is modified (that is, the Satyr Multiplexer service for Authentication Agent Multiplexer, the Satyr Client application for Authentication Agent).

To restart the Authentication Agent Multiplexer, right-click on the **Satyr Multiplexer** element of the **Start menu** > **Settings** > **Control panel** > **Administrative Tools** > **Services** list and select **Restart**.

The following settings are available from the registry:

Name	Description	Default value	Component
aliasfile	The name and path (for example, `C:\tmp\aliases`) of a text file. Using the information contained in this file, the 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`.	1	Multiplexer
Automatic	To enable the automatic Kerberos authentication without user interaction with the Authentication Agent, set it to `1`. In this case, Authentication Agent will use the username provided during Windows login.	1	Client
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 set to `0`, the credentials will not be saved and have to be re-entered again.	1	Client

Name	**Description**	**Default value**	**Component**
Details	The authentication agent displays the details of the connection in the popup dialog if this parameter is set to `1`. The following information is displayed: name of the application initiating the connection, IP address and port of the destination server, name of the PNS service started, and the type of the connection (TCP/UDP). If the details are disabled, only the name of the service is displayed.	0	Client
Has Preferences	To enable the **Preferences** menu item in the system tray icon of Authentication Agent, set this parameter to `1`. Otherwise, this menu item will not be available.	1	Client
Forget Password Interval	To prevent unauthorized initiation of network connections through unattended machines, configure this parameter. Enter the number of minutes after which Authentication Agent deletes the stored password.	1	Client
Forget Password	To store the authentication password indefinitely in the Authentication Agent, set this parameter to `False`. This sets the *`Forget Password Interval`* parameter to infinite.	1	Client

Name	Description	Default value	Component
LOG_CLIENT	The verbosity level of the authentication client, ranging from `0` (lowest) to `9`. Only increase log verbosity 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 files are stored in the `%SystemRoot%\Debug` folder (for example, `C:\WinNT\Debug` or `C:\Windows\Debug`). **Note** On Windows 7 platforms, if the Authentication Agent is run under a user account, the log files are stored under the `C:\Users\<username>\AppData\Local\VirtualStore\Windows\Debug\` folder. When run as Administrator, the log files are stored under the `C:\Windows\Debug\` folder on Windows 7 too.	0	Client

Name	Description	Default value	Component
LOG	The verbosity level of the Authentication Agent Multiplexer, ranging from `0` (lowest) to `9`. Only increase log verbosity 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 files are stored in the `%SystemRoot%\Debug` folder (for example, `C:\WinNT\Debug` or `C:\Windows\Debug`).	0	Multiplexer
SSL	To configure the Authentication Agent Multiplexer so that it only SSL-encrypted connections, set this parameter to `1`.	1	Multiplexer

4.1.2. Command line parameters (Windows)

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

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

`--install_service`	Register the Satyr Multiplexer service.
`--remove_service`	Remove the Satyr Multiplexer service.
`--start_service`	Start the Satyr Multiplexer service.
`--stop_service`	Stop the Satyr Multiplexer service.

4.1.3. Configuring SSL connections (Windows)

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

Note
It is highly recommended to encrypt the communication between PNS and the authentication agent, because without it anyone can connect to the Authentication Agent Multiplexer, resulting in the authentication information obtained by unauthorized people. It is essential to use encryption when password authentication is used.

4.1.3.1. Procedure – Encrypting the communication between PNS and the authentication agent (Windows)

Purpose:

To enable encryption between PNS and the authentication agent, complete the following steps. For the steps to be completed from MC, see *Chapter 11, Key and certificate management in PNS* in *Proxedo Network Security Suite 1.0 Administrator Guide*.

Steps:

Step 1. Create a CA (for example, `AA_CA`) using the Management Console (MC). This CA will be used to sign the certificates shown by the PNS firewalls to the authentication agents.

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

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

Note
Every firewall should 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 Authentication Agent (AA) 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. Using the installer of the Authentication Agent.
2. Manually using the `addcert` and `getcert` programs (see *Procedure 4.1.3.2, Importing the CA certificate manually (p. 15)*).
3. 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 MC and reference them in the services of PNS. See *Chapter 15, Connection authentication and authorization* in *Proxedo Network Security Suite 1.0 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 Authentication Agent (`C:\Program Files\Satyr client` by default). The program can be started from a command prompt or through **Start menu** > **Run application**. Supply the name and path of the `DER`-format certificate as an input parameter. For example,

```
C:\Program Files\Satyr client\addcert C:\temp\Satyr_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 Satyr Multiplexer service.

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

Purpose:

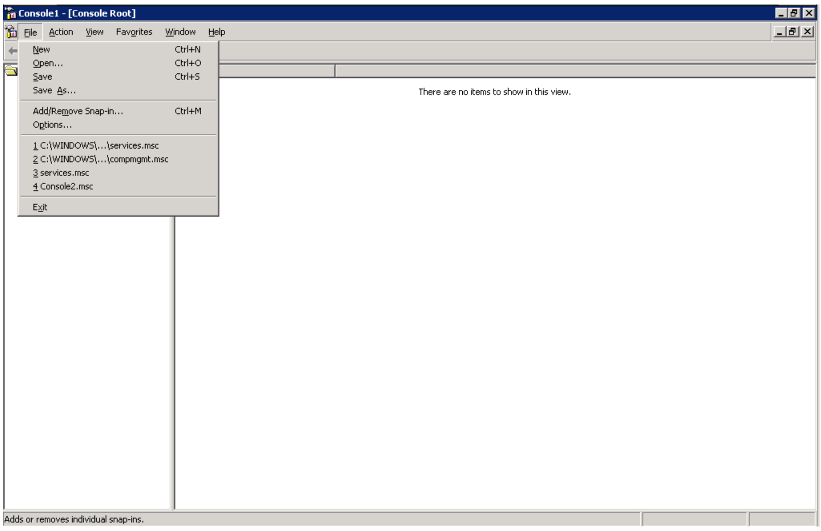
To import the certificate of the CA complete the following steps.

Steps:

Step 1. Start Microsoft Management Console by executing `mmc.exe` in **Start menu** > **Run application**.

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

Step 2. From the **File** menu, select **Add/Remove Snap-in**.

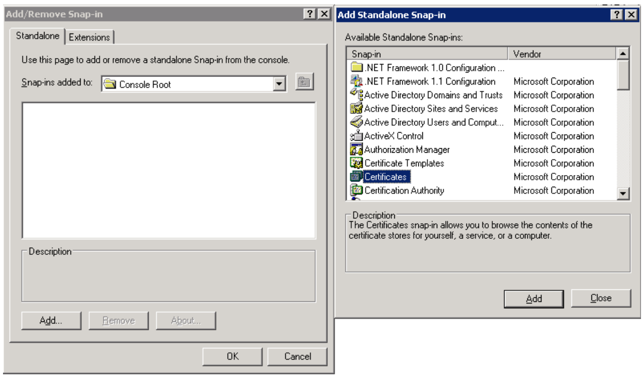


There are no items to show in this view.

Adds or removes individual snap-ins.

Figure 6. Adding a snap-in

Step 3. From the **Available snap-ins** list, select **Certificates** and click **Add**.



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Description

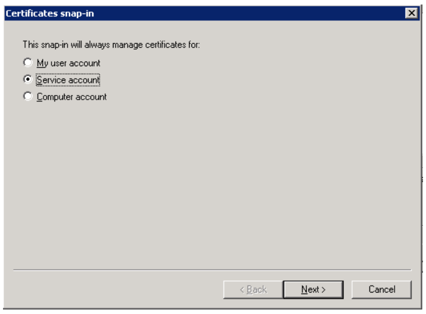
Available Standalone Snap-ins:

Snap-in	Vendor
.NET Framework 1.0 Configuration ...	
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Comput...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation

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

Figure 7. Adding certificates

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



This snap-in will always manage certificates for:

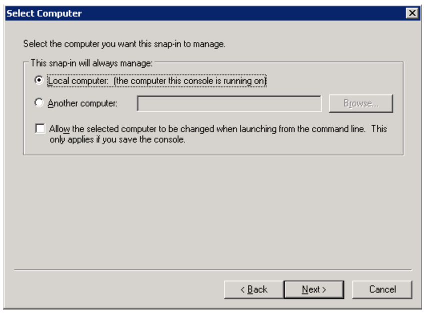
○ My user account

● Service account

○ Computer account

Figure 8. 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:

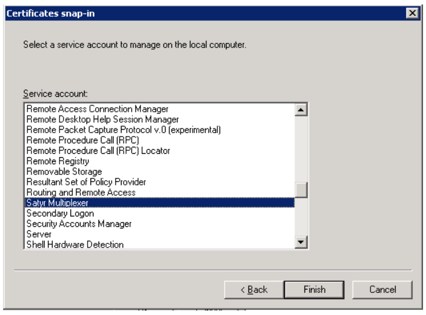
● Local computer: (the computer this console is running on)

○ Another computer:

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

Figure 9. Selecting the managed computer

Step 6. Select the **Satyr Multiplexer** service and click **Finish**.



Certificates snap-in

Select a service account to manage on the local computer.

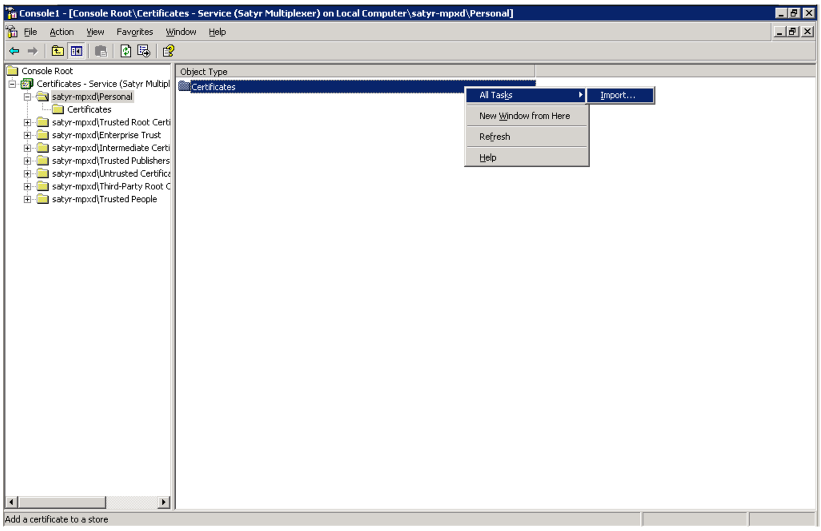
Service account:

Remote Access Connection Manager
Remote Desktop Help Session Manager
Remote Packet Capture Protocol v.0 (experimental)
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Removable Storage
Resultant Set of Policy Provider
Routing and Remote Access
Satyr Multiplexer
Secondary Logon
Security Accounts Manager
Server
Shell Hardware Detection

Figure 10. Selecting the service

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

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



Console1 - [Console Root\Certificates - Service (Satyr Multiplexer) on Local Computer\satyr-mpxd\Personal]

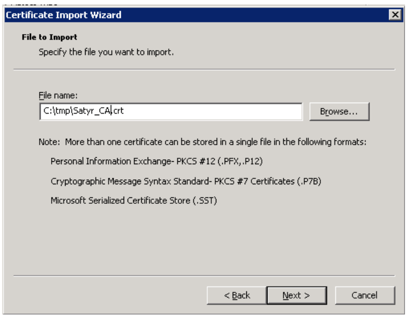
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Service (Satyr Multipl
satyr-mpxd\Personal
Certificates
satyr-mpxd\Trusted Root Certi
satyr-mpxd\Enterprise Trust
satyr-mpxd\Intermediate Certi
satyr-mpxd\Trusted Publishers
satyr-mpxd\Untrusted Certifica
satyr-mpxd\Third-Party Root C
satyr-mpxd\Trusted People
Object Type
Certificates
All Tasks
Import...
New Window from Here
Refresh
Help

Add a certificate to a store

Figure 11. 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 (for example, `C:/tmp/Satyr_CA.crt`) and click **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:
C:\tmp\Satyr_CA.crt

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

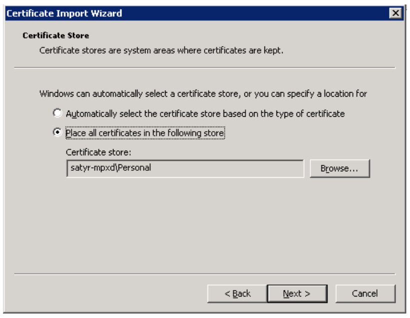
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Figure 12. Selecting the certificate to import

Step 10. Windows offers a suitable certificate store by default, so click **Next**.



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

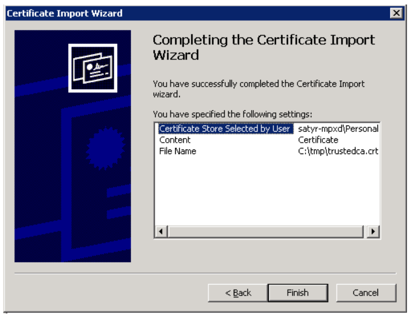
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
satyr-mpxd\Personal

Figure 13. Selecting the certificate store

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



Certificate Import Wizard

Completing the Certificate Import Wizard

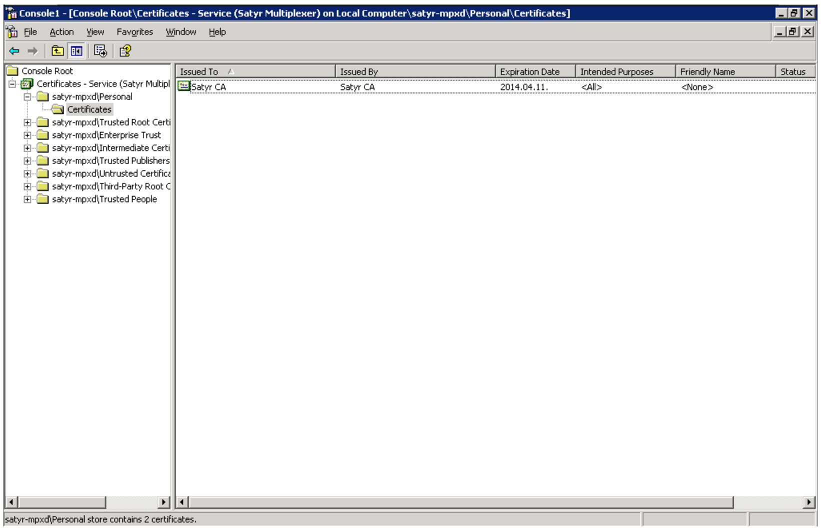
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	satyr-mpxd\Personal
Content	Certificate
File Name	C:\tmp\trustedca.crt

Figure 14. Summary

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



Console1 - [Console Root\Certificates - Service (Satyr Multiplexer) on Local Computer\satyr-mpxd\Personal\Certificates]

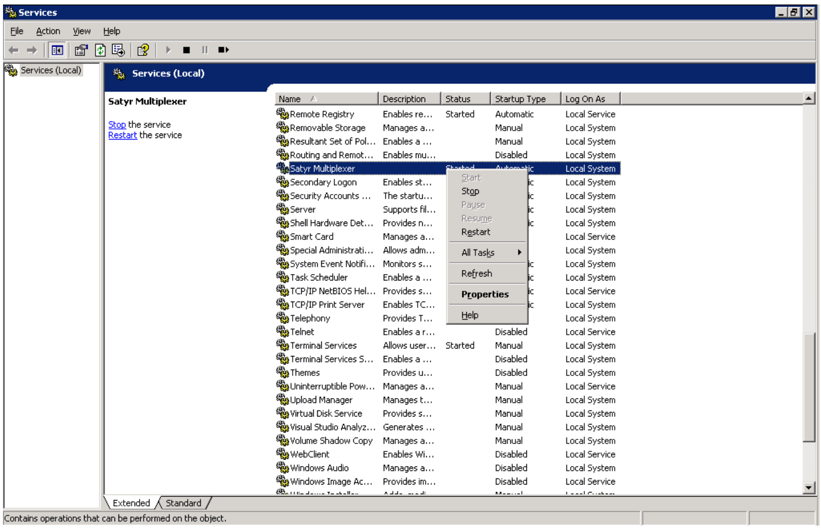
- Console Root
  - Certificates - Service (Satyr Multipl
    - satyr-mpxd\Personal
      - Certificates
    - satyr-mpxd\Trusted Root Certi
    - satyr-mpxd\Enterprise Trust
    - satyr-mpxd\Intermediate Certi
    - satyr-mpxd\Trusted Publishers
    - satyr-mpxd\Untrusted Certifica
    - satyr-mpxd\Third-Party Root C
    - satyr-mpxd\Trusted People

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Satyr CA	Satyr CA	2014.04.11.	<All>	<None>	

satyr-mpxd\Personal store contains 2 certificates.

Figure 15. The imported certificate

Step 12. Restart the Satyr Multiplexer service. Navigate to **Start menu** > **Settings** > **Control panel** > **Administrative Tools** > **Services**. Scroll to **Satyr Multiplexer** and right-click on it. Select **Restart**.



Satyr Multiplexer

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Remote Registry	Enables re...	Started	Automatic	Local Service
Removable Storage	Manages a...		Manual	Local System
Resultant Set of Pol...	Enables a ...		Manual	Local System
Routing and Remot...	Enables mu...		Disabled	Local System
Satyr Multiplexer		Started	Automatic	Local System
Secondary Logon	Enables st...		ic	Local System
Security Accounts ...	The startu...		ic	Local System
Server	Supports fil...		ic	Local System
Shell Hardware Det...	Provides n...		ic	Local System
Smart Card	Manages a...			Local Service
Special Administrati...	Allows adm...			Local System
System Event Notifi...	Monitors s...		ic	Local System
Task Scheduler	Enables a ...		ic	Local System
TCP/IP NetBIOS Hel...	Provides s...		ic	Local Service
TCP/IP Print Server	Enables TC...		ic	Local System
Telephony	Provides T...			Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user...	Started	Manual	Local System
Terminal Services S...	Enables a ...		Disabled	Local System
Themes	Provides u...		Disabled	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Upload Manager	Manages t...		Manual	Local System
Virtual Disk Service	Provides s...		Manual	Local System
Visual Studio Analyz...	Generates ...		Manual	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...		Disabled	Local Service
Windows Audio	Manages a...		Disabled	Local System
Windows Image Ac...	Provides im...		Disabled	Local Service

Contains operations that can be performed on the object.

Figure 16. Restarting the Satyr Multiplexer

4.1.4. Procedure – Configuring X.509 certificate based authentication (Windows)

Purpose:

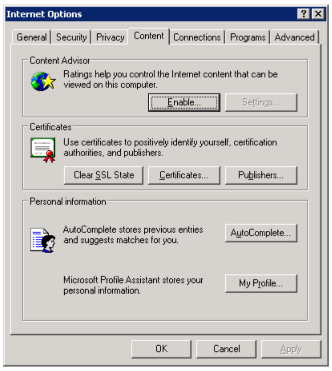
For authentication based on X.509 certificates the certificate and the private key of the user has to be deployed onto the workstation. Import the certificate of the user into their personal certificate store. This can be accomplished most easily through the Internet Explorer:

Steps:

Step 1. Start Internet Explorer from the **Start** menu or from a command prompt by running `iexplore.exe`.

Step 2. From the **Tools** menu select **Internet Options**.

Step 3. On the **Contents** tab click on **Certificates**.



Ratings help you control the Internet content that can be viewed on this computer.

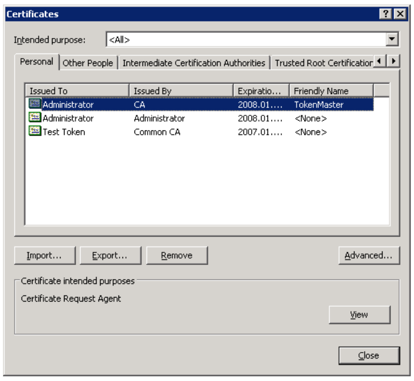
Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Figure 17. The certificates of the user

Step 4. The certificates of the user are displayed on the **Personal** tab. Click **Import**.



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Administrator	CA	2008.01....	TokenMaster
Administrator	Administrator	2008.01....	<None>
Test Token	Common CA	2007.01....	<None>

Certificate intended purposes

Certificate Request Agent

Figure 18. The certificates of the user

Note

Hardware keys and tokens (for example,: Aladdin) having a suitable driver for Windows are also displayed in this store and can be used from the Authentication Agent.

Step 5. Import the certificate using the Certificate Import Wizard.

4.2. Configuration on Linux platforms

4.2.1. Command line parameters (Linux)

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

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

Satyr Multiplexer (`satyr-mpxd`) has the following command line parameters:

`--help` or `-?`	Display a brief help message.
`--version` or `-V`	Display the version number of `satyr-mpxd`
`--no-syslog` or `-l`	Send log messages to the standard output instead of syslog.
`--verbose <verbosity>` or `-v <verbosity>`	Set verbosity level to <verbosity>. The default verbosity level is `3`; possible values are `0`-`10`.
`--logtags;` or `-T`	Prepend log category and log level to each message.
`--aliasfile;` or `-a`	The name (including full path) of a text file (for example, `/tmp/aliases`) used by 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` — Set 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. 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` — Turn off the SSL encryption of the communication between PNS and the Multiplexer.

`--bind-address;` or `-b` and , `--bind-port;` or `-p` — The IP address and the port the Multiplexer is accepting connections on.

`--crt-dir;` or `-t` — Path of the directory containing the certificate of the CA that issued the certificate of the PNS firewall.

`--crl-dir;` or `-r` — Path of the directory containing the Certificate Revocation List (CRL) related to the above CA.

4.2.2. Configuring SSL-encrypted connections (Linux)

To enable encryption between PNS and the authentication agent complete the following steps. For the steps to be completed from MC, see *Chapter 11, Key and certificate management in PNS* in *Proxedo Network Security Suite 1.0 Administrator Guide*.

4.2.2.1. Procedure – Encrypting the communication between PNS and the authentication agent (Linux)

Steps:

Step 1. Create a CA (for example, *`Satyr_CA`*) using the Management Console (MC). This CA will be used to sign the certificates shown by the PNS firewalls to the authentication agents.

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

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

> **Note**
> Every firewall should 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 Authentication Agent (AA) 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. Verify the hash of the CA certificate:

```
openssl x509 -in /etc/satyr/ca/cacert.pem -hash -noout
```

Step d. Create a symlink to the certificate file using the hash received in the above step. Add the `.0` suffix (or the next free suffix if `.0` is already taken) to the file as an extension, for example,

```
ln -s /etc/satyr/ca/cacert.pem /etc/satyr/ca/6d2962a8.0
```

Step e. Restart the Satyr Multiplexer daemon:

```
/etc/init.d/satyr-mpxd restart
```

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

Step 6. Create the appropriate outband authentication policies in MC and reference them in the services of PNS. For details, see *Chapter 15, Connection authentication and authorization* in *Proxedo Network Security Suite 1.0 Administrator Guide*.

4.2.3. Configuring X.509 certificate-based authentication (Linux)

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 authentication agent will automatically use the certificate found in this directory.

5. Procedure – Using the Authentication Agent (AA)

Purpose:

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

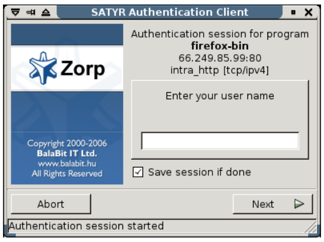
The client displays the name of the service requiring authentication (*`intra_http`* in the above example), and — provided that the administrator enabled it — further details of the connection (for example, destination IP address).

Steps:

Step 1. To save your credentials so that the client will fill the username and password automatically for later authentication attempts, select **Save session if done**. For details on configuring password storage period

length and deleting a prevously saved password, see *Procedure 6, Configuring Authentication Agent preferences (Windows) (p. 26)*.
To cancel the authentication at any time, click **Abort**.

>



Authentication session for program
firefox-bin
66.249.85.99:80
intra_http [tcp/ipv4]

Enter your user name

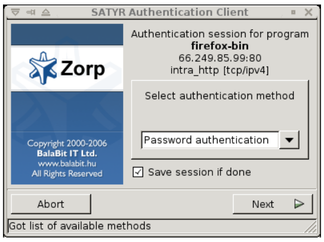
☑ Save session if done

Authentication session started

Figure 19. The Authentication Agent

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

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
firefox-bin
66.249.85.99:80
intra_http [tcp/ipv4]

Select authentication method

Password authentication

☑ Save session if done

Got list of available methods

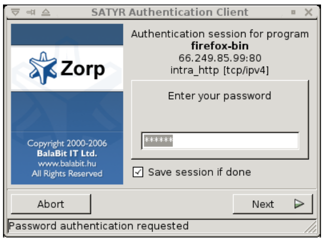
Figure 20. Selecting authentication method

- To authenticate with a password, select **Password authentication**.
- 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, Configuring Authentication Agent preferences (Windows) (p. 26)*.

- 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.



SATYR Authentication Client

Authentication session for program
firefox-bin
66.249.85.99:80
intra_http [tcp/ipv4]

Enter your password

******

☑ Save session if done

Password authentication requested

Figure 21. 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.

6. Procedure – Configuring Authentication Agent preferences (Windows)

Purpose:

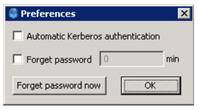
Authentication Agent starts automatically after Windows starts up, and places its icon on the system tray. To configure Authentication Agent preferences, complete the following steps.

Note

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

Steps:

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



Preferences

□ Automatic Kerberos authentication

□ Forget password 0 min

Figure 22. Preferences

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

Step 3. To prevent unauthorized initiation of network connections through unattended machines, configure **Forget password**. Enter the number of minutes after which Authentication Agent deletes the stored password.

Step 4. To immediately delete the stored password from the Authentication Agent, click **Forget password now**.

7. Starting and stopping Authentication Agent

To start or stop Authentication Agent, do one of the following.

- To stop Authentication Agent, right-click the system tray icon and click **Exit**.
- To restart Authentication Agent, navigate to **Start menu** > **Satyr Client** and click **Satyr Client**.