Documentation Area

Using ThinOX Thin Client with Imprivata OneSign 4.6 Environment

Author:	Documentation
Date:	Sep 17, 2012 2:54 PM
URL:	http://wiki.praim.com/display/Imprivata

Table of Contents

This guide will illustrate how to configure ThinOX Thin Client to use Imprivata OneSign 4.6 Environment.

Ver. 1.3 - 17 September 2012

1 Setting up OneSign Environment

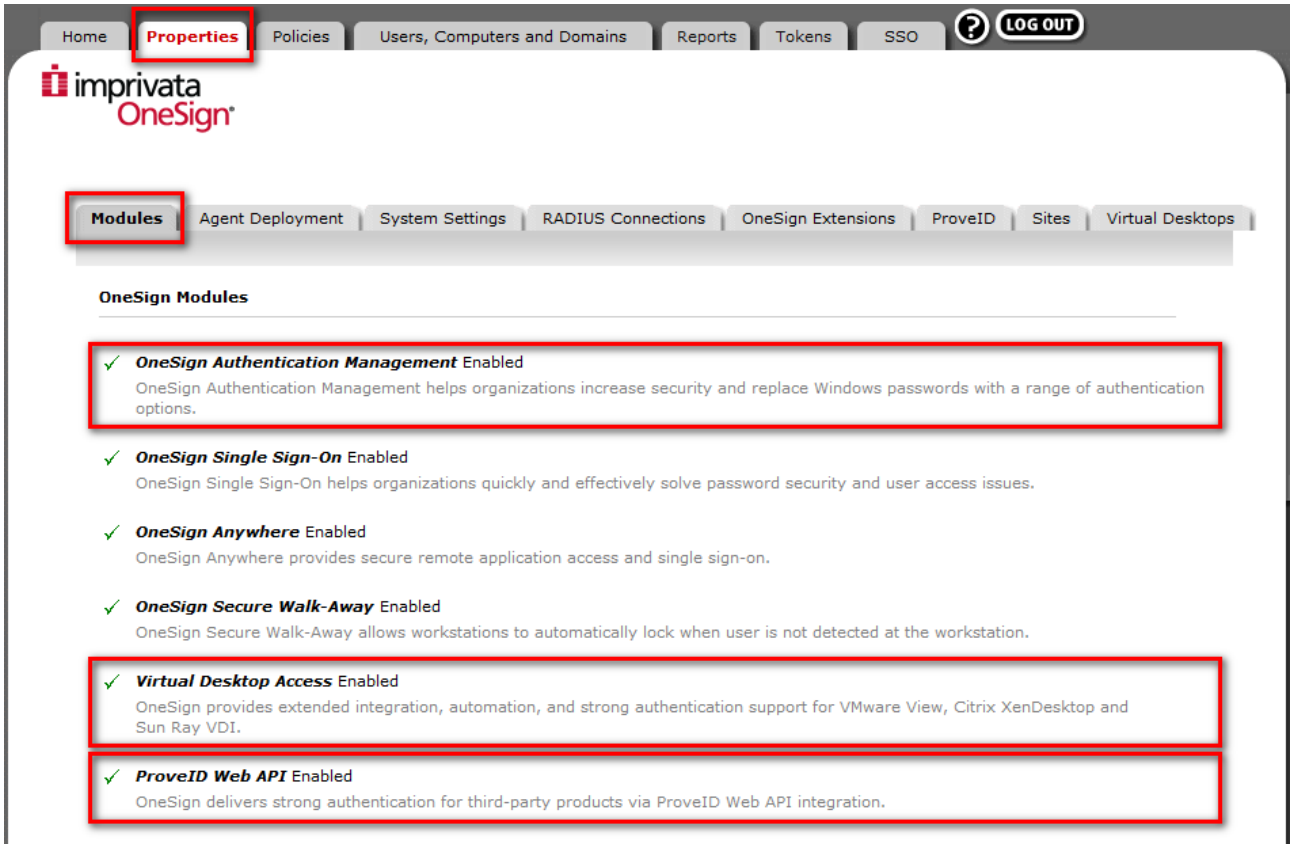
These chapters explain how to configure Imprivata OneSign Environment:

1.1 Check License

To use OneSign Environment you must check the OneSign license.

Follow this procedure to check the installed modules:

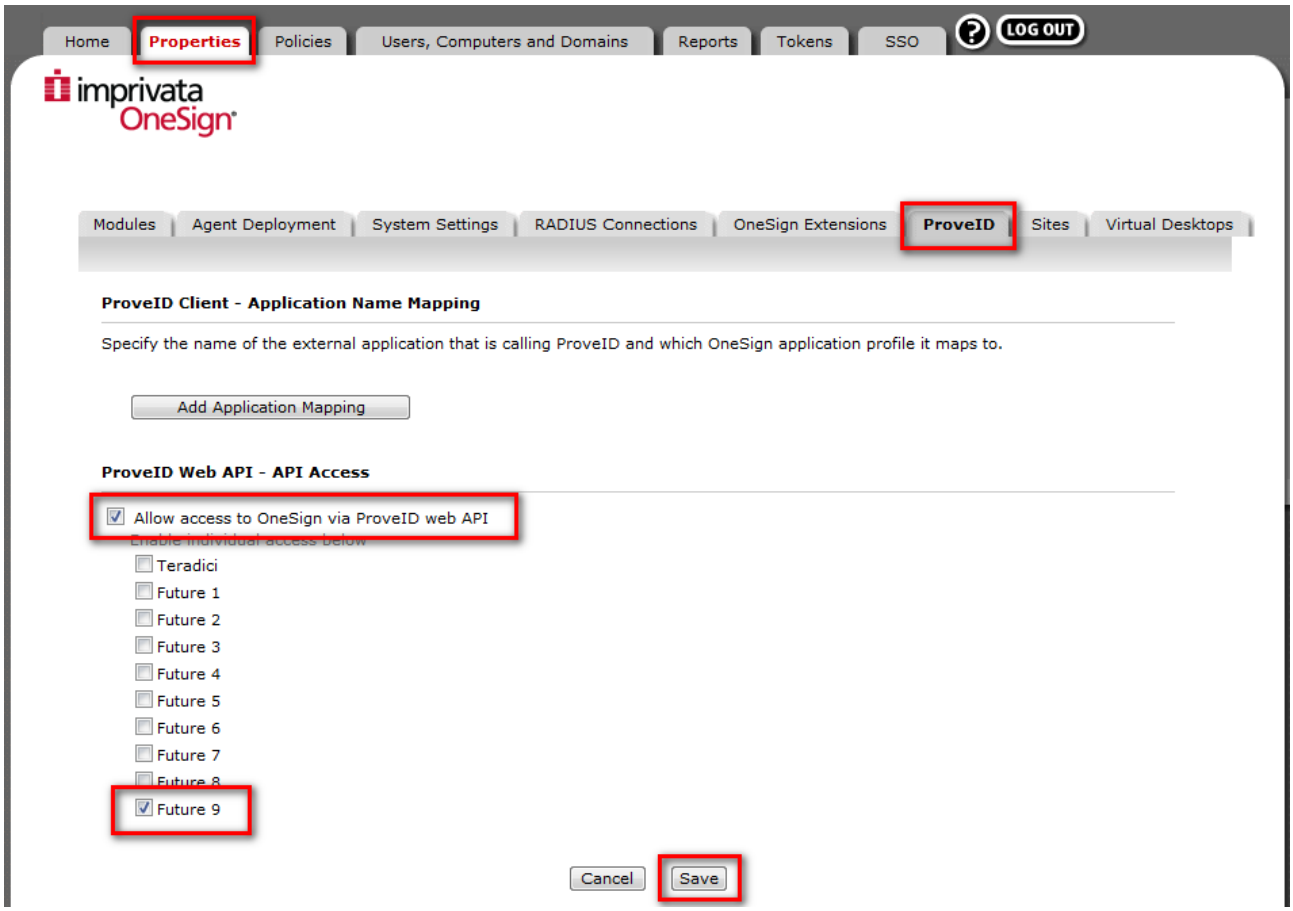
- Open the OneSign Administrator Properties page
- Go to “Modules” tab
- The following modules have to be enabled:
  - OneSign Authentication Management
  - Virtual Desktop Access
  - ProveID Web API (free of charge but it must be requested from Imprivata)



1.2 Enabling ProveID Web API

To set up ThinOX thin client support in your OneSign Enterprise enable the “Future 9” option doing the following:

- Open the OneSign Administrator Properties page
- Go to “ProveID” tab
- Enable “Allow Access to OneSign via ProveID Web API”
- Flag “Future 9” option
- Click on “Save” button to save configuration

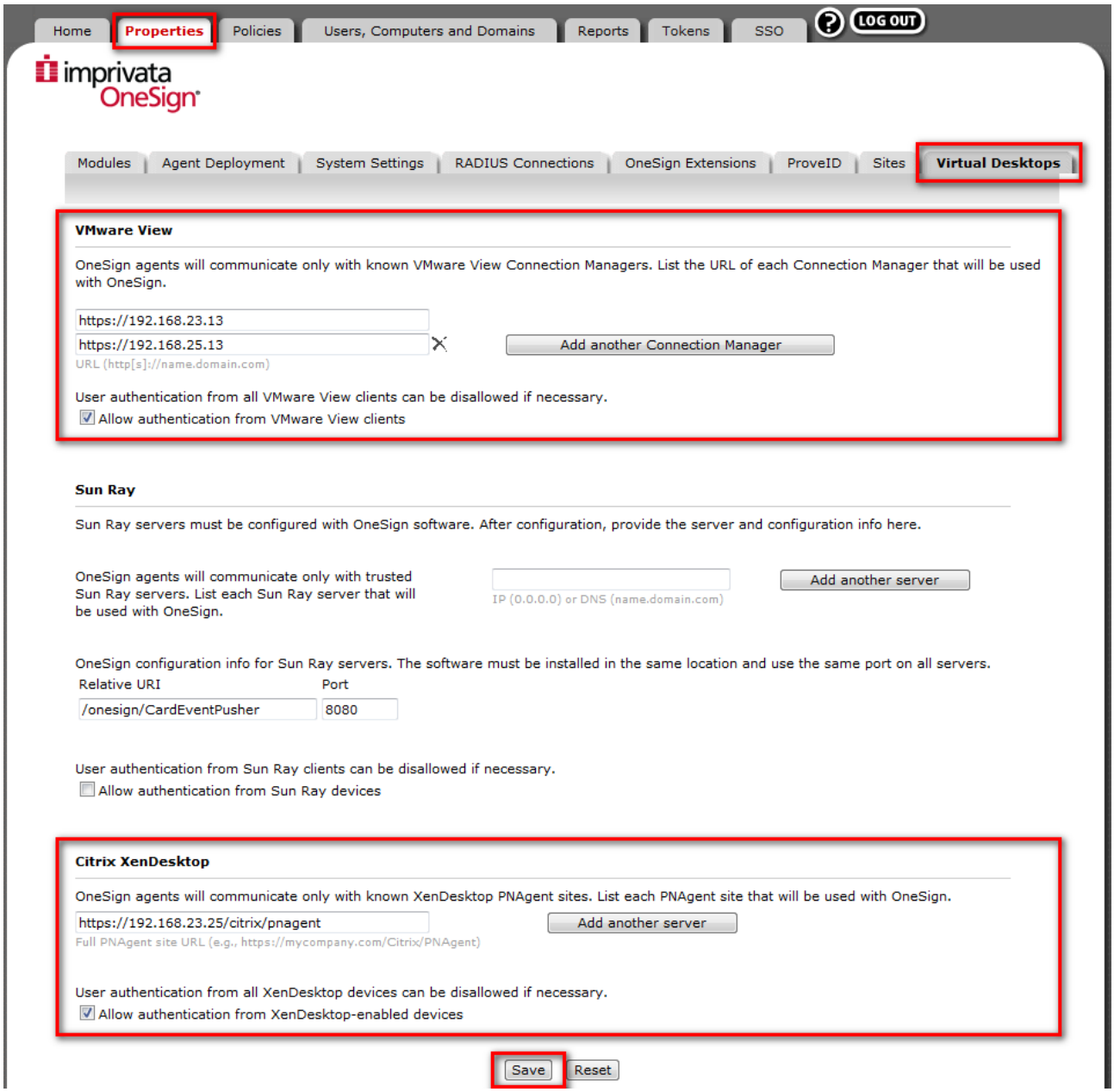


1.3 Configuring VDI Options in OneSign

To use VMware or Citrix infrastructure in OneSign Environment you must insert VMware and Citrix related information. Do this procedure to insert related informations:

- Open the OneSign Administrator Properties page.
- Go to “Virtual desktops” tab.
- Add in the two sections “VMware View” and “Citrix XenDesktop” information related to VMware and Citrix server using the respective “Add server” button.
- Remember to flag the respective “Allow authentication from VMware View Client” and “Allow authentication from XenDesktop-enabled devices” .
- Click on “Save” button to save configuration modification.

See figure below for an example.


Home
Properties
Policies
Users, Computers and Domains
Reports
Tokens
SSO
LOG OUT
imprivata OneSign
Modules
Agent Deployment
System Settings
RADIUS Connections
OneSign Extensions
ProveID
Sites
Virtual Desktops
VMware View
OneSign agents will communicate only with known VMware View Connection Managers. List the URL of each Connection Manager that will be used with OneSign.
https://192.168.23.13
https://192.168.25.13
Add another Connection Manager
URL (http[s]://name.domain.com)
User authentication from all VMware View clients can be disallowed if necessary.
Allow authentication from VMware View clients
Sun Ray
Sun Ray servers must be configured with OneSign software. After configuration, provide the server and configuration info here.
OneSign agents will communicate only with trusted Sun Ray servers. List each Sun Ray server that will be used with OneSign.
Add another server
IP (0.0.0.0) or DNS (name.domain.com)
OneSign configuration info for Sun Ray servers. The software must be installed in the same location and use the same port on all servers.
Relative URI
Port
/onesign/CardEventPusher
8080
User authentication from Sun Ray clients can be disallowed if necessary.
Allow authentication from Sun Ray devices
Citrix XenDesktop
OneSign agents will communicate only with known XenDesktop PNAgent sites. List each PNAgent site that will be used with OneSign.
https://192.168.23.25/citrix/pnagent
Add another server
Full PNAgent site URL (e.g., https://mycompany.com/Citrix/PNAgent)
User authentication from all XenDesktop devices can be disallowed if necessary.
Allow authentication from XenDesktop-enabled devices
Save
Reset

2 Configuring ThinOX Thin Client

These chapter explain how to configure ThinOX Thin Client:

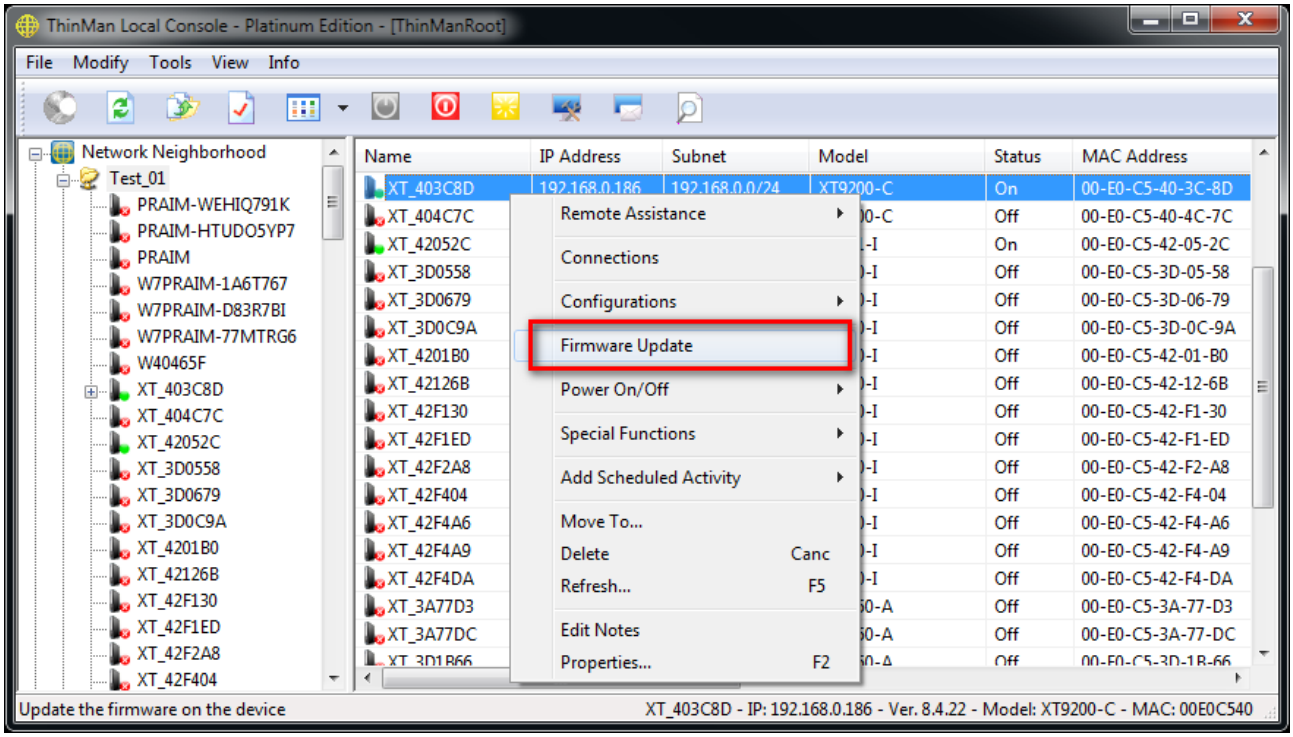
2.1 Update ThinOX ThinClient with Latest Firmware

Imprivata OneSign is available on firmware version 8.5.1 and above.

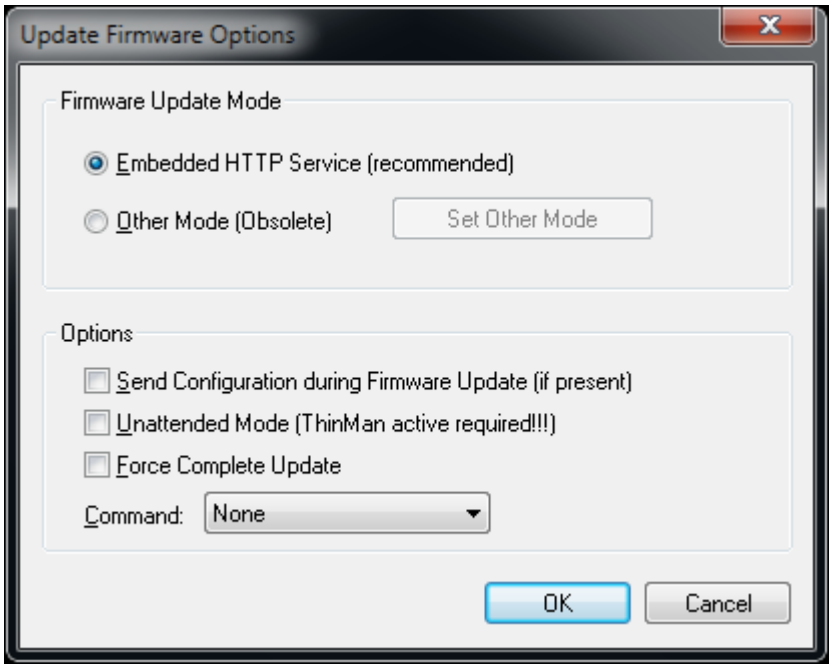
This document and the screenshots are related to ThinOX firmware version 8.5.3.

To check your thin client firmware version open ThinMan Console. In the right side of the graphical interface identify the thin client. Scroll horizontally with horizontal scrollbar until you see the “Version” attribute. In this field you can read the firmware version installed on the thin client.

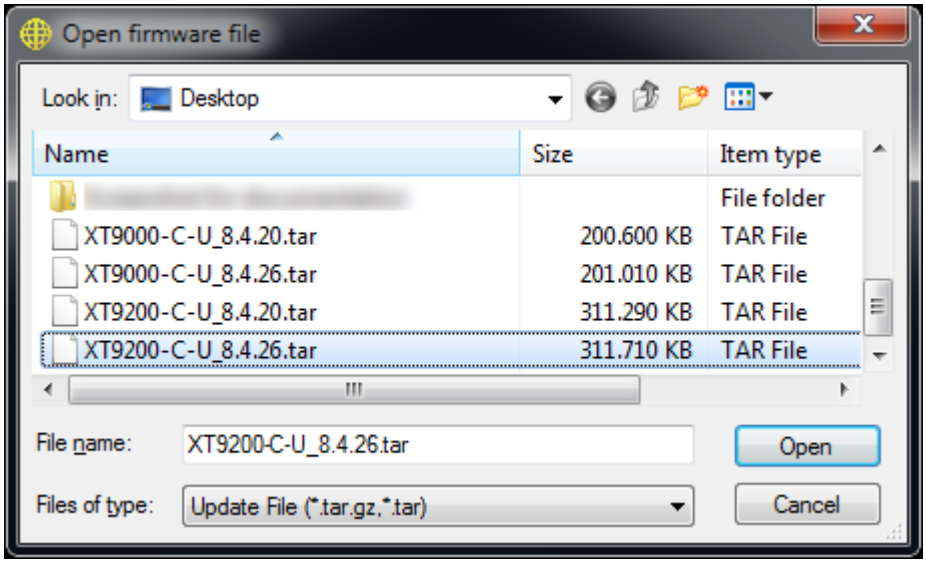
If you need to upgrade firmware version select the thin client you will upgrade and right click with mouse on it.



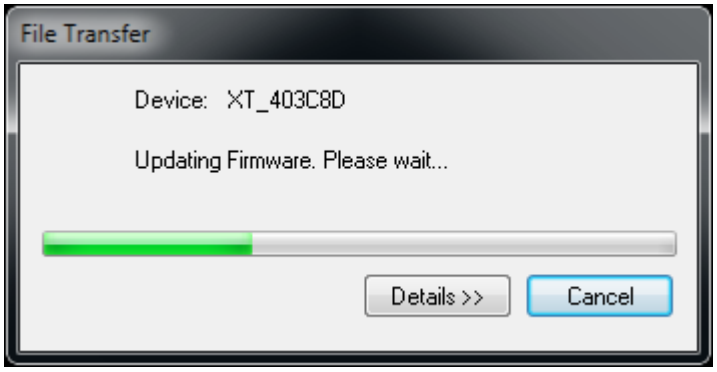
From the menu select “Firmware Update”.



Leave “Embedded HTTP Service” flagged and click on “OK”.



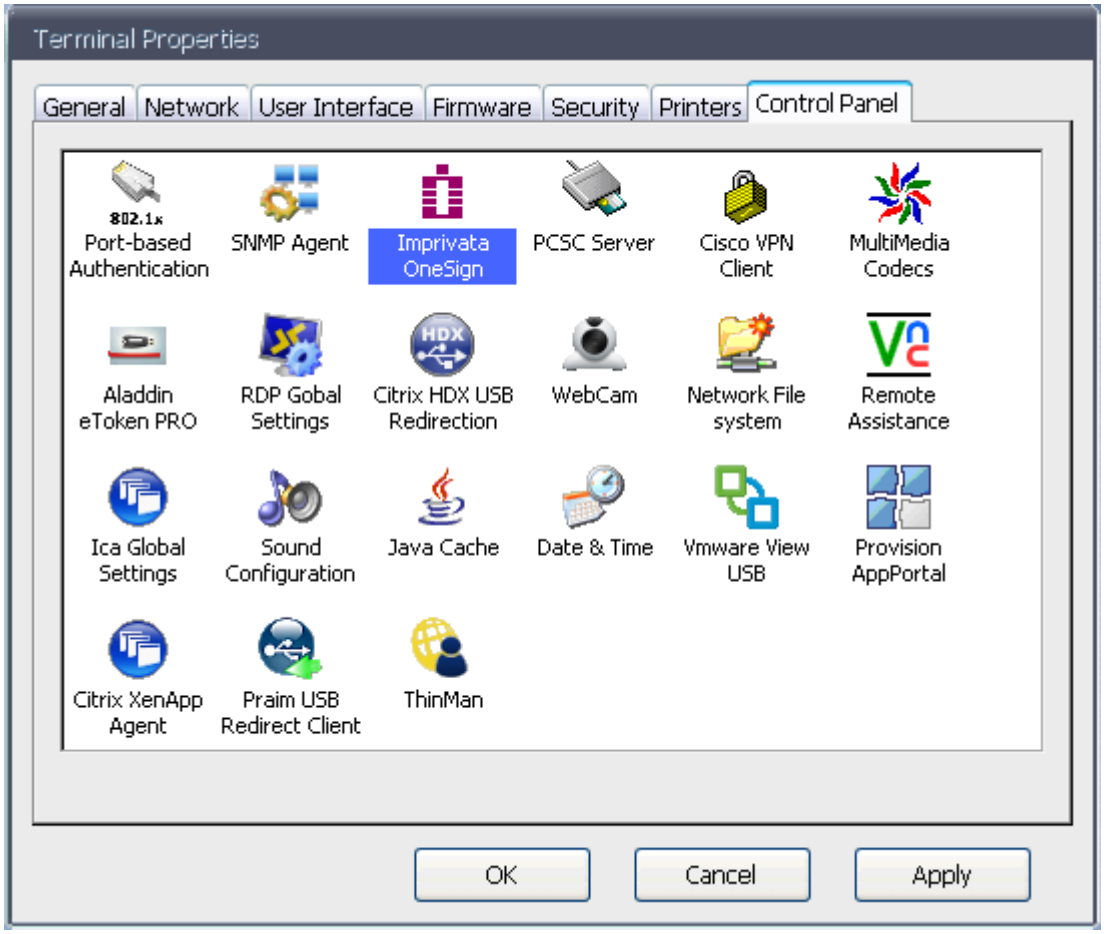
Select the firmware file that is compatible with the thin client model (in case it is not ThinMan will block the operation indicating the error).



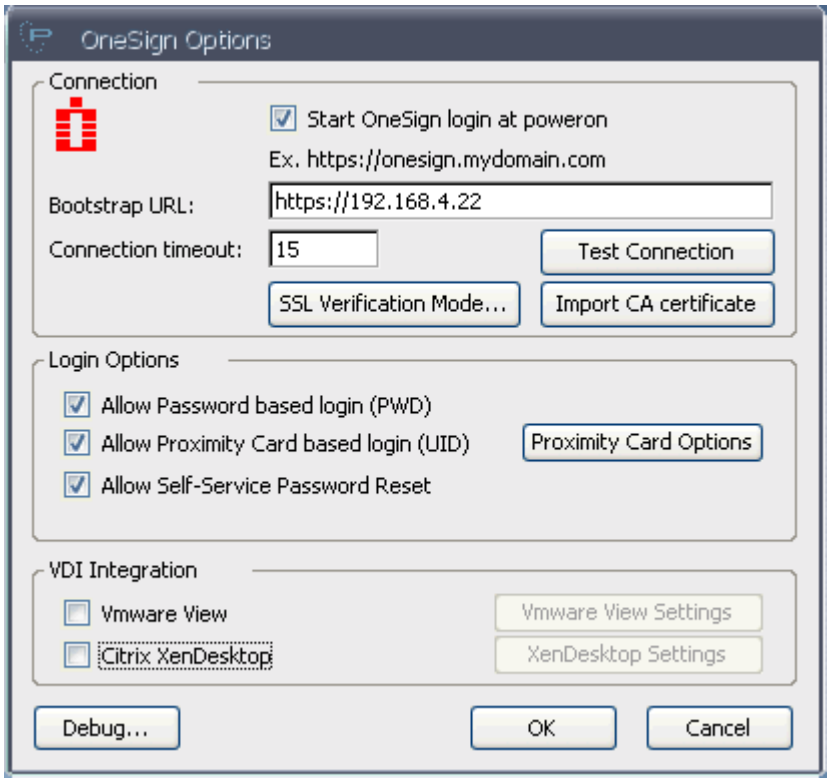
After few seconds ThinMan starts upgrading the thin clients. Once the upgrade is completed the thin client will be rebooted.

2.2 Configure ThinOX Thin Client to Communicate with OneSign

Turn on the thin client. Right-click with mouse on desktop and select “Terminal properties” menu. The “Terminal Properties” window will open, select “Contol Panel” tab.



Double click on “Imprivata OneSign”.



Flag “Start OneSign login at poweron” (this option tell ThinOX to login at OneSign server when the thin client is started).

In the “Bootstrap URL” enter the OneSign Appliance URL in the form “https://<hostname/IPAddress>”.

It is possible to test the inserted parameters related to the connection clicking on "Test Connection". The agent try to connect to the Imprivata server and return a result depending on the connection availability.

Click on “OK” to save Imprivata settings.

Click once again “OK” of “Terminal properties” window to save thin client configuration.

Reboot the thin client.

If the operation was successful the thin client will present the credential login.

2.2.1 SSL Verification Mode

“SSL Verification Mode” permits to define the thin client behavior in case of problem with OneSign server certificate validation.

Clicking on the “SSL Verification Mode“ button a new window will open.

Selecting “Rejecting the unverifiable connection (Secure)…” will close the connection to the server if certificates are not trusted and not valid. Use it in case you have a trusted and valid certificate on the server.

Selecting “Warn if the connection maybe insecure (Default)…” will open a warning window that request a confirmation to proceed with the connection. You can continue or stop the connection. Use it in case you have self-signed or expired certificates on the server.

Selecting “Allow the unverifiable connection (Not Secure)…” will connect to the server even if the certificate is not valid. Don’t use it in production environment.

2.2.2 Import CA Certificate

“Import CA Certificate” permits to load on thin client the Trusted Root CA Certificate used to generate certificate installed on OneSign appliance.

Export CA Certificate from Certification Authority in Base64 format.

Copy the exported certificate on a USB Key, insert the USB Key in the thin client and click on “Import CA Certificates”. A new window will appear and you will able to browse the USB Key, select certificates inside it and import them into the thin client clicking on “Import”.

2.2.3 Copy Thin Client Configuration

When the thin client is configured it is possible to copy its configuration to another thin client.

The copy will include all the configuration made on the thin client included connections, certificates and Imprivata parameters.

For a detailed procedure refer to How to easily copy configuration from a device to another device (see page 54) chapter.

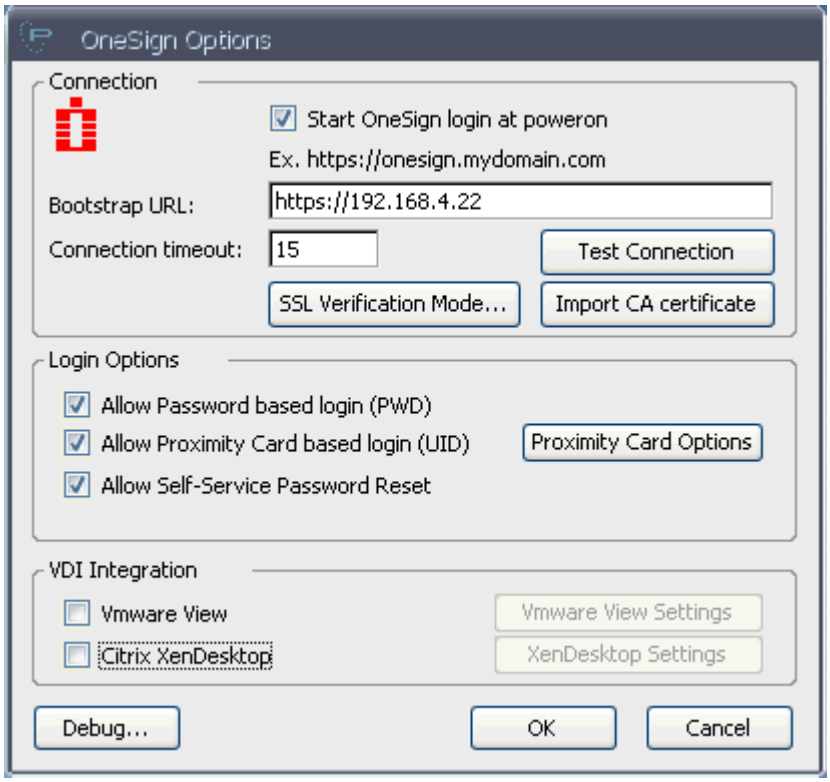
2.3 Use Smart Card as Proximity Card

Smart cards can be used as Proximity Card by using its unique serial number as the Unique ID (UID) of a proximity card.

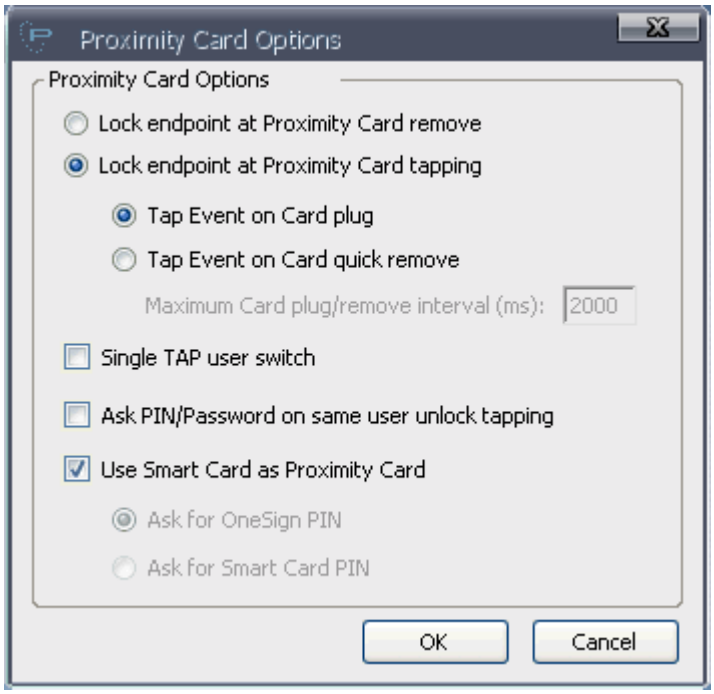
To use a Smart Card as Proximity Card follow this procedure.

Open the “Imprivata OneSign” in the thin client (see previous chapter for details).

Flag "Allow Proximity Card based login (UID)"



Click on "Proximity Card Options" button.

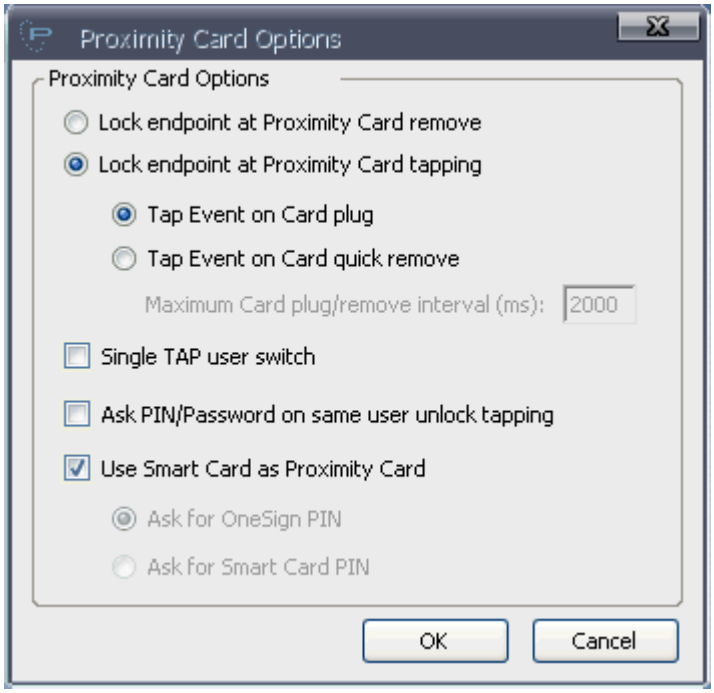


Flag "Use Smart Card as Proximity Card" option.

Click on "OK" to save configuration.

2.4 Proximity Card Options

In this window it is possible to configure the parameters that define the used proximity card workflow.



"Lock Endpoint at Proximity Card Remove" and "Lock Endpoint at Proximity Card Tapping" specify to lock the thin client on card removing or on card tapping.

If you select "Card Tapping" you may specify when the tap event is recognized:

- "Tap Event on Card Plug" consider the tap event the moment when the card is plugged in or leans on the reader
- "Tap Event on Card Quick Remove" means that the tap event is considered when the card leans on or plug in the player and after a short time it is removed. The tap event occurs at the card removing event.
    - In this case you have to indicate what is the time interval in milliseconds, at "Maximum card plug/remove interval" option, in which the two event (plug and remove) must succeed in order to consider a tapping event. If the removing of the card is done after this interval nothing happens. This option is useful when software installed on the Virtual Desktop want use information stored on card (e.g. digital signing, strong authentication, ...).

The "Single TAP user switch" parameter allows the agent, if flagged, to switch user and start its session with a single tap from the user.

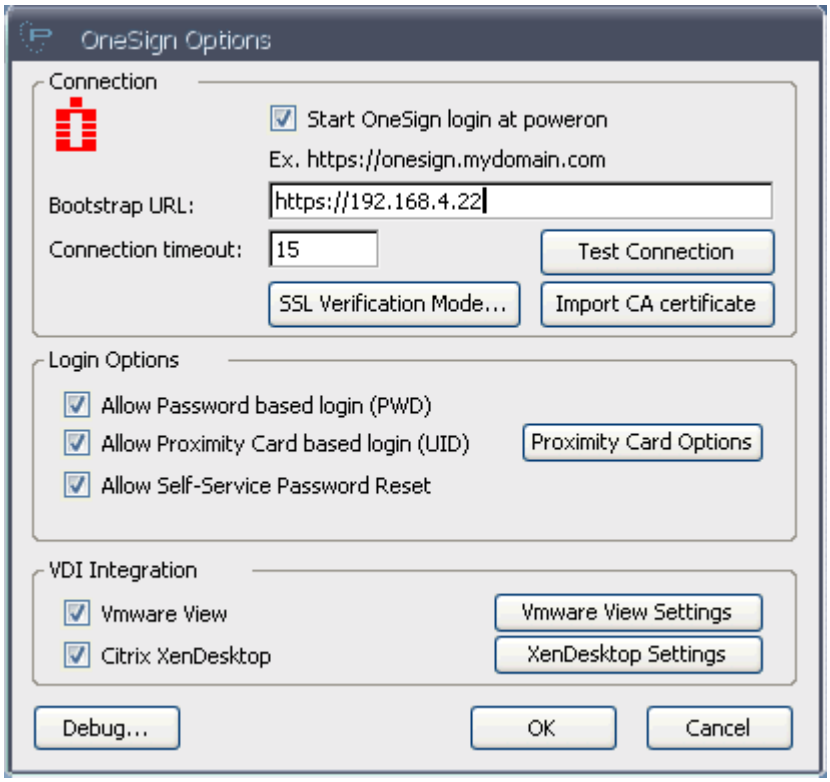
The "Ask PIN/Password on same user unlock tapping" parameter allows a user, if not flagged, to access the locked screen without the needs to digit the PIN or the Password (it is valid only for locked desktop on the same thin client, e.g. a desktop locked by a tap or a desktop locked because screen saver starts).

2.5 Configure ThinOX Thin Client for Imprivata VDI Integration

ThinOX thin client can use Imprivata user policy related information to access the VDI infrastructure specified on the OneSign appliance configuration.

Refer to Imprivata documentation on how to define and configure user policy for VDI integration.

To enable the VDI support access to "Imprivata OneSign Options" window.



2.5.1 VMware View Infrastructure

On the "VDI Integration" section flag "VMware View" option. This flag will indicate the thin client to start a VMware View connection after login using the View Connection manager information provided by the OneSign appliance.

The parameters used in this connection are those specified in the related user policy.

You can also configure specific connection parameters clicking on "VMware View Settings" button. See VMware Client Options (see page 47) for more information.

2.5.2 Citrix XenDesktop/XenApp Infrastructure

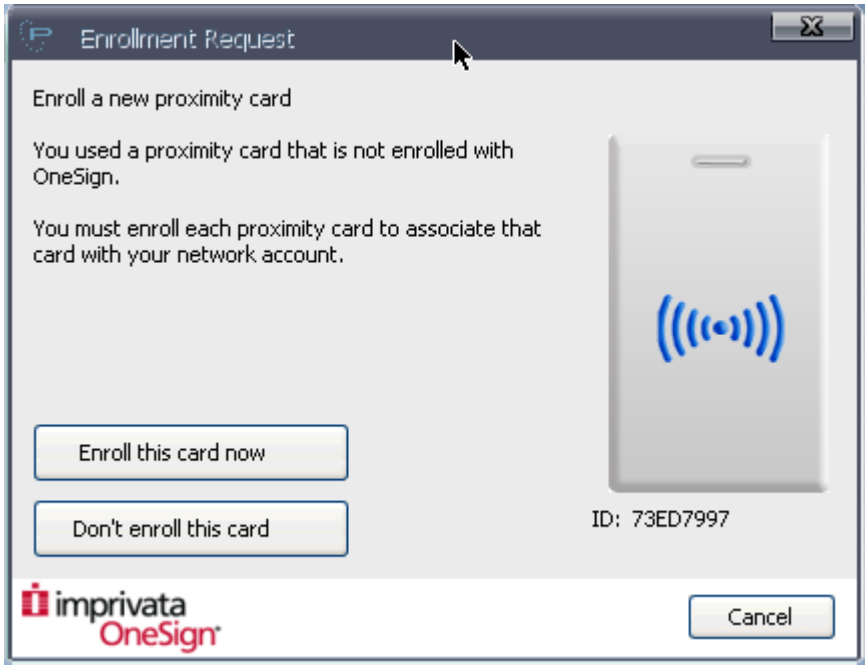
On the "VDI Integration" section flag "Citrix XenDesktop" option. This flag will indicate the thin client to start a Citrix XenDesktop connection after login using the Citrix Farm information provided by the OneSign appliance.

The parameters used in this connection are those specified in the related user policy.

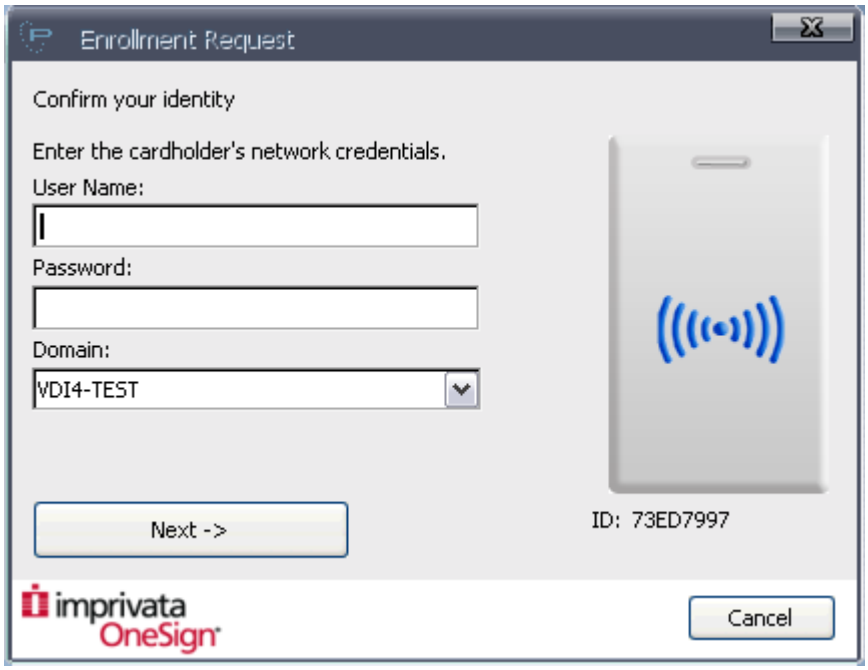
You can also configure specific connection parameters clicking on "XenDesktop Settings" button. See Citrix Client Options (see page 50) for more information.

2.6 Card Enrollment

When a card is tapped on login phase and it is not already enrolled, based on OneSign appliance configuration, the thin client allow the user to enroll it.



Click on "Enroll this card now".



Insert username and password for valid domain credentials and click on "Next".

Click on "Done".

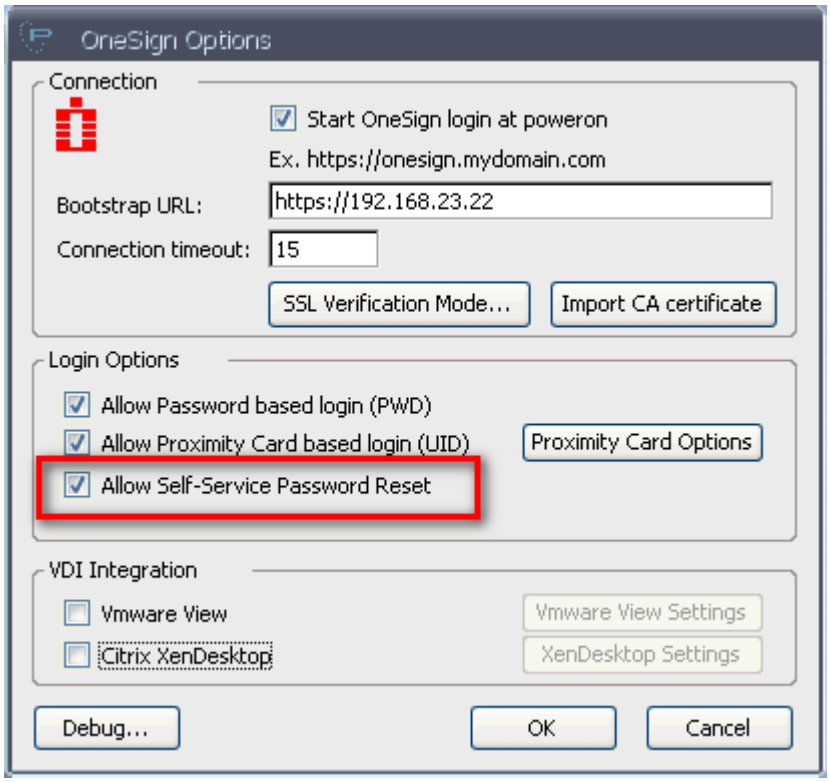
If the user doesn’t have any already enrolled OneSign PIN and the user policy require Secondary Authentication method then the thin client request the OneSig PIN enrollment.

Insert and confirm the OneSign PIN and click "OK".

The card is now enrolled and protected by the OneSign PIN.

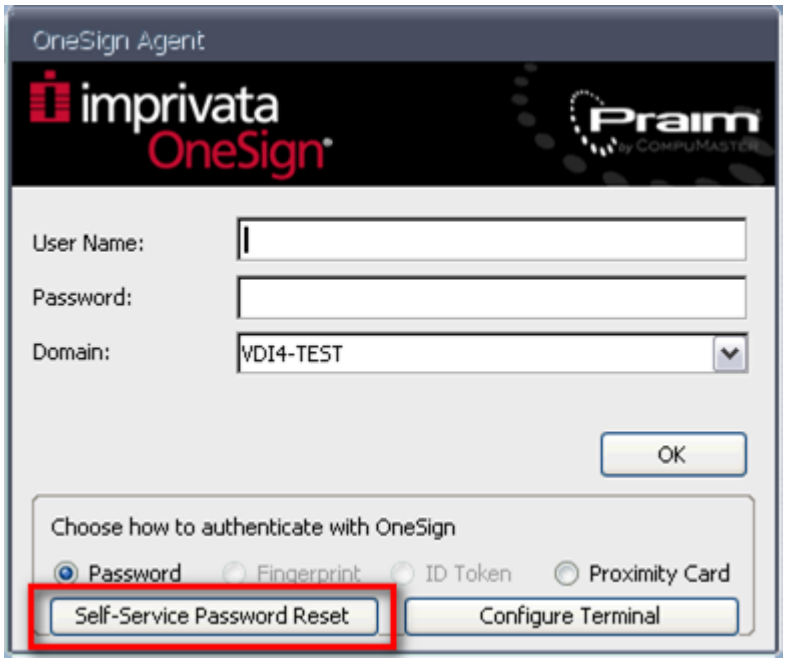
2.7 Self Service Password Reset

The user can be enabled to reset its password by itself when he connect to the thin client.



On "Imprivata OneSign" window (accessed via "Terminal Properties" on thin client) you can flag "Allow Self-Service Password Reset" to allows users to reset their password.

If the option is enabled at thin client startup the "Self-Service Password Reset" button is showed on the OneSign Login window.

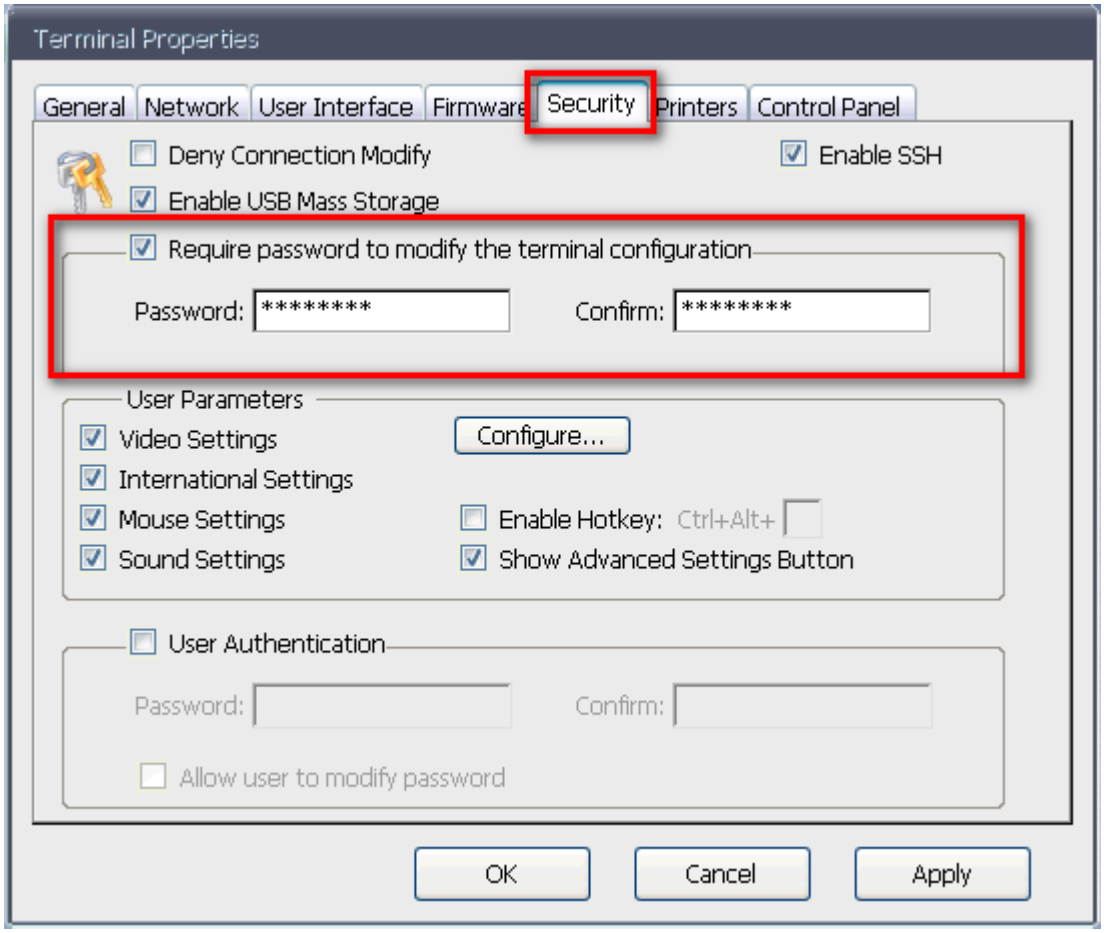


Clicking on the "Self-Service Password Reset" will open a browser window that point to the correct OneSign server that permit the user to reset his password.

2.8 Terminal Properties for Thin Client Users

ThinOX permits to give the user the possibility to change some terminal properties (mouse, video settings, etc.) from Imprivata OneSign login window.

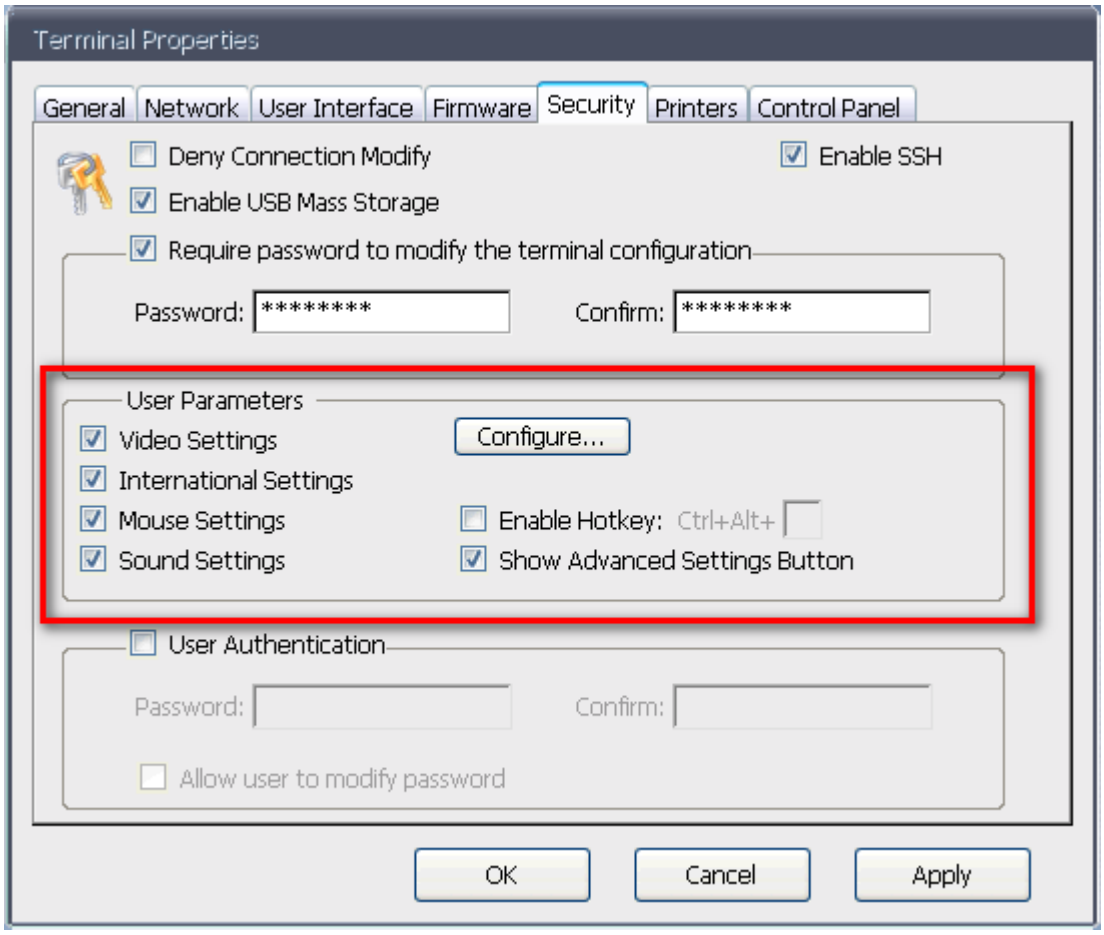
First step to configure this useful feature is to access the "Terminal Properties" window and to select "Security" tab.



Flag "Require password to modify the terminal configuration" options and insert an administrative password (and confirm it). This option tell ThinOX to prevent configuration modification from anonymous users. When the flag is enabled every time you need to change configuration on thin client you are asked to insert the administrative password.

Praim strongly suggest to protect thin client with this administrative password.

Once the thin client is protected from unauthorized modification you can configure to grant some permission to change configuration.



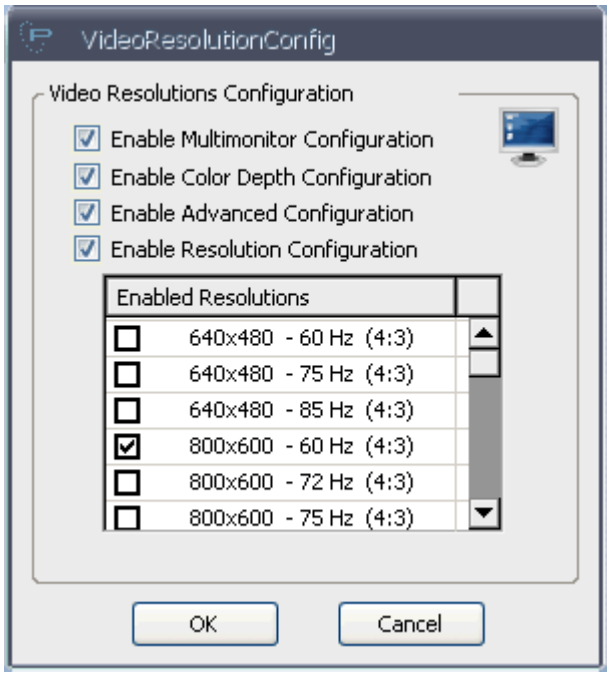
Now flag which properties may be changed from the user. The list of properties is:

- Video Settings: related to monitor/s resolution
- International Settings: related to thin client language and keyboard settings
- Mouse Settings: related to mouse speed, left/right mouse, ...
- Sound Settings: related to volume setting and audio device

Every flagged property will show an icon in the "Terminal Properties” panel and entitles the user to change related thin client option.

The option "Show Advanced Settings Button" tell ThinOX to show in the user limited "Terminal Properties" window a button to access the full "Terminal Properties" window (see below).

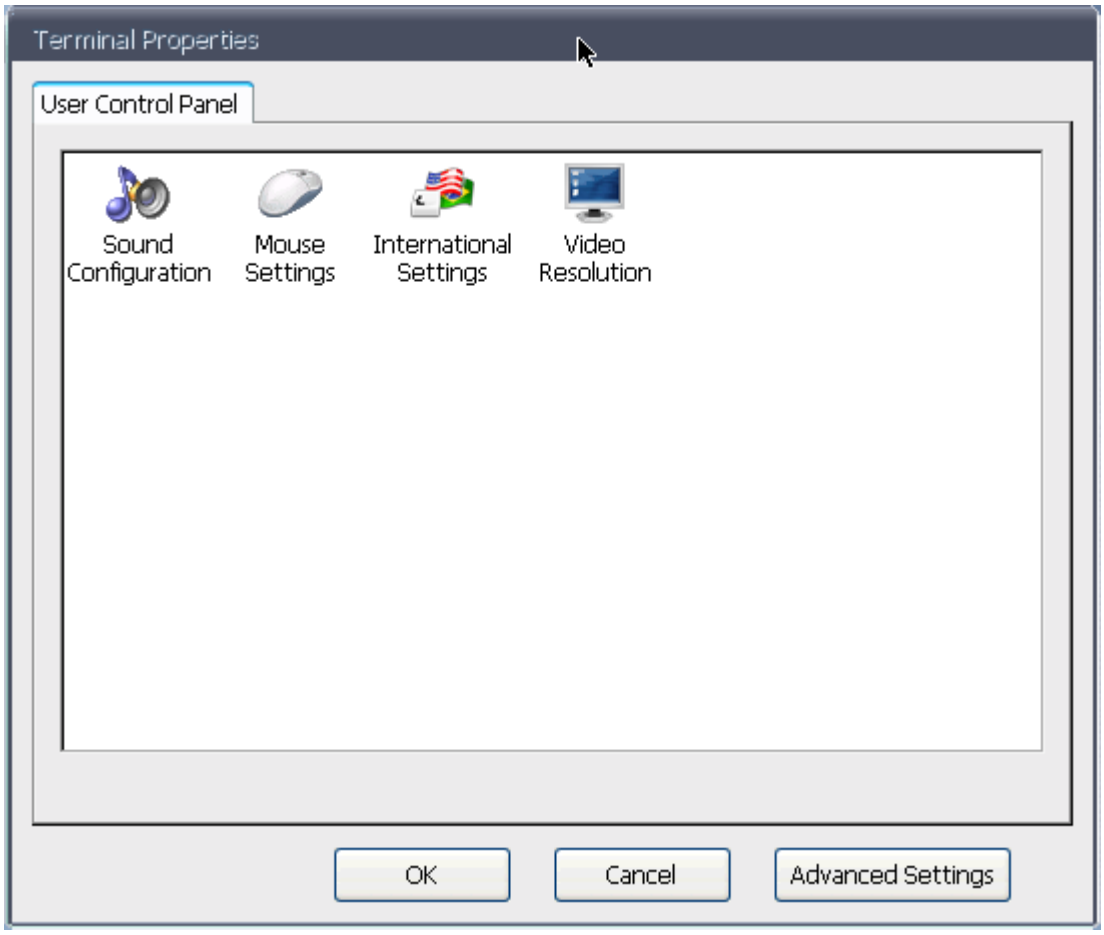
For the "Video Settings" option is furthermore possible to specify which resolutions the user may select from and which properties of the video setting are available to user. Click "Configure" button to access the configuration panel below.



With this panel you can select if user is enabled to modify Multimonitor Configuration, Color Depth Configuration, Advanced Configuration and Resolution Configuration. For Resolution Configuration you can also specify which are the proposed resolution to the user (flag only which resolution will be available to the user).

If at least one of the previously properties is flagged on the OneSign login window a new button is present.

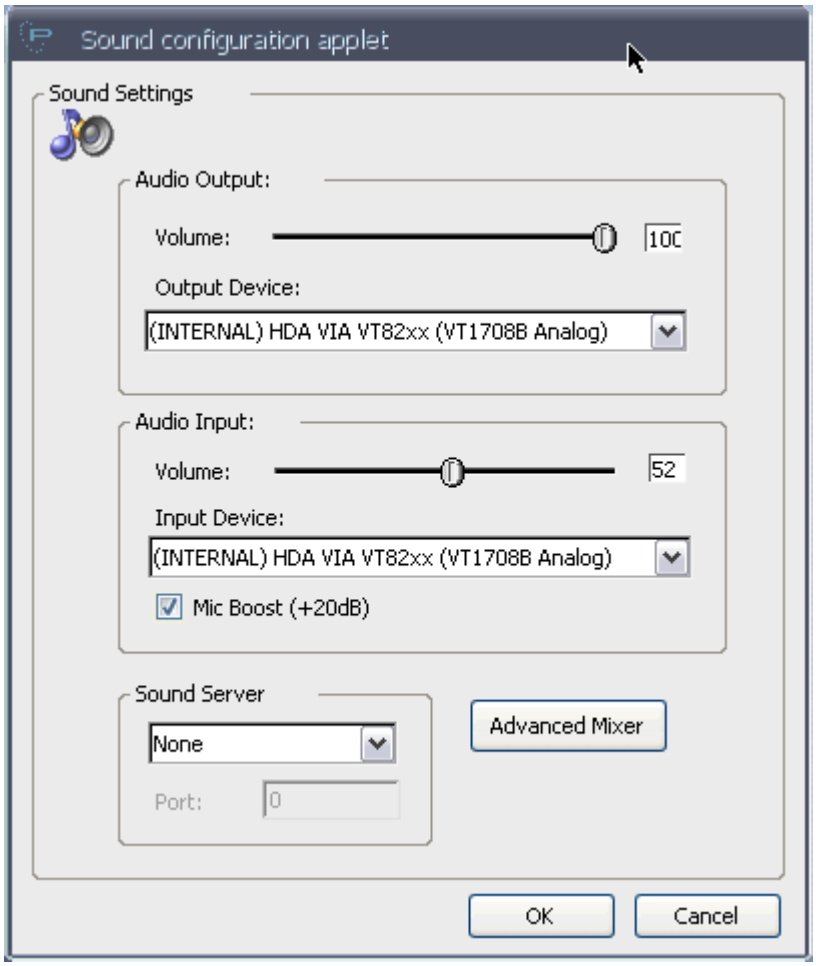
If the user click on "Configure Terminal" button a "Terminal Properties" window will open containing only the configuration items previously specified.



Beware that if the thin client is not protected by an administrative password and "Advanced Settings" button is clicked the full "Terminal Properties" window will open showing all control. In this way the user is enabled to change all thin client configuration with possible disastrous effects on the thin client itself.

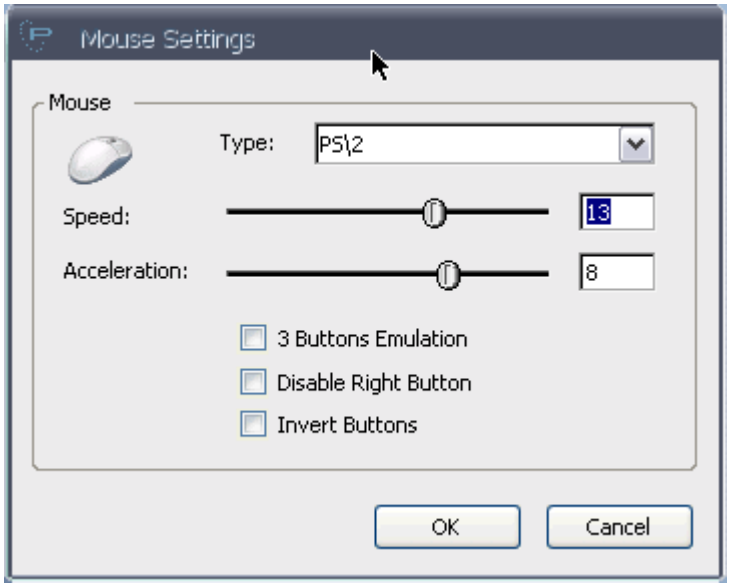
2.8.1 Sound Configuration

This window show the sound configuration possibilities.



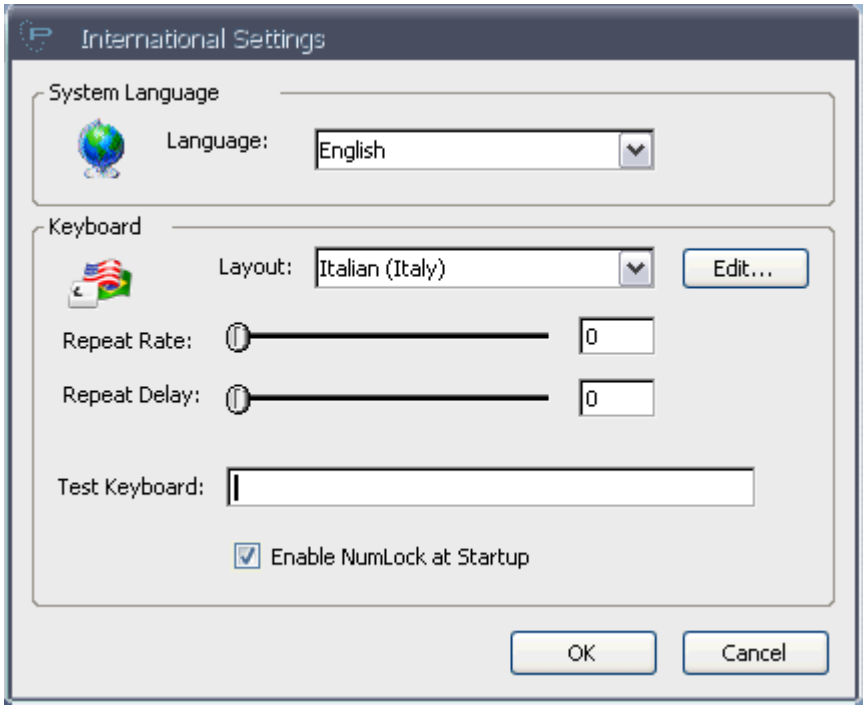
2.8.2 Mouse Configuration

This window show the mouse settings possibilities.



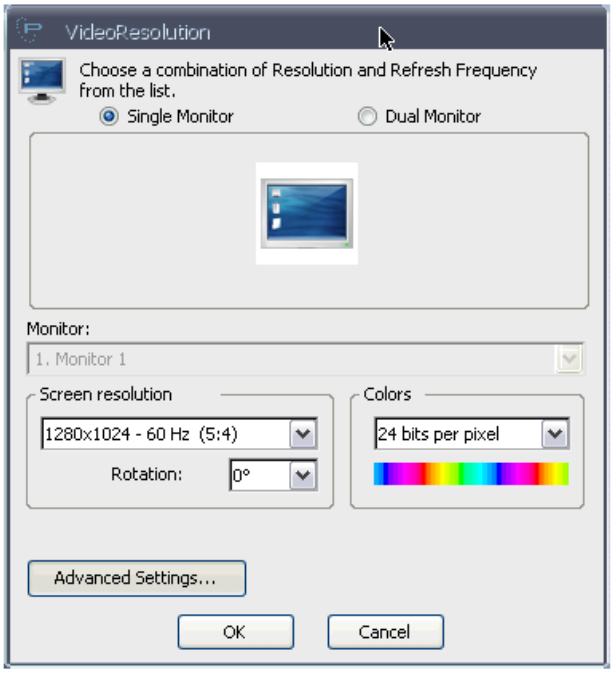
2.8.3 Internationalization Configuration

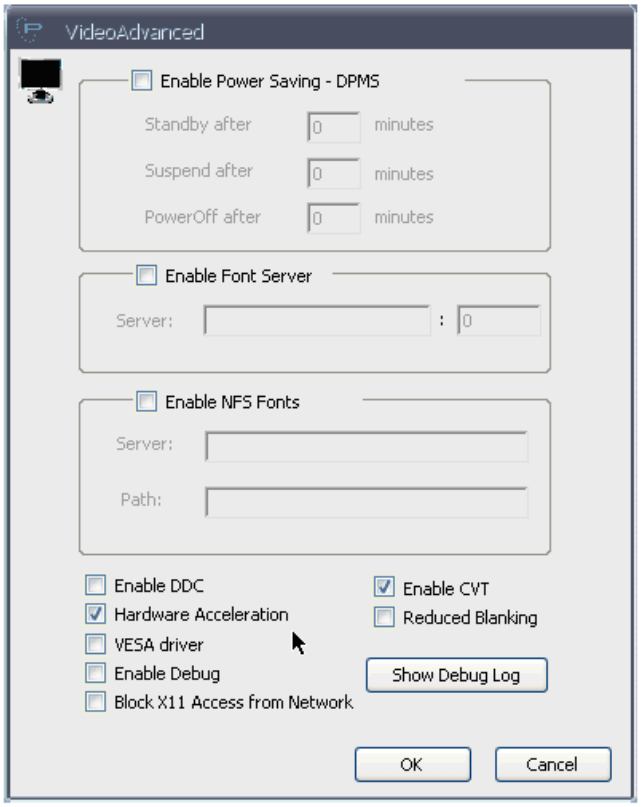
This window show the international settings possibilities.



2.8.4 Video Settings

This window show the video settings possibilities. The second window can be accessed clicking on "Advanced Settings..." button on the first window.


VideoResolution
Choose a combination of Resolution and Refresh Frequency from the list.
Single Monitor
Dual Monitor
Monitor:
1. Monitor 1
Screen resolution
1280x1024 - 60 Hz (5:4)
Rotation:
0°
Colors
24 bits per pixel
Advanced Settings...
OK
Cancel


VideoAdvanced
Enable Power Saving - DPMS
Standby after
0
minutes
Suspend after
0
minutes
PowerOff after
0
minutes
Enable Font Server
Server:
0
Enable NFS Fonts
Server:
Path:
Enable DDC
Hardware Acceleration
VESA driver
Enable Debug
Block X11 Access from Network
Enable CVT
Reduced Blanking
Show Debug Log
OK
Cancel

2.9 Bitmap Customization

Its possible to customize the bitmaps showed in several windows.

There are two logo bitmaps: header bitmap and footer bitmap.

2.9.1 Header Bitmap

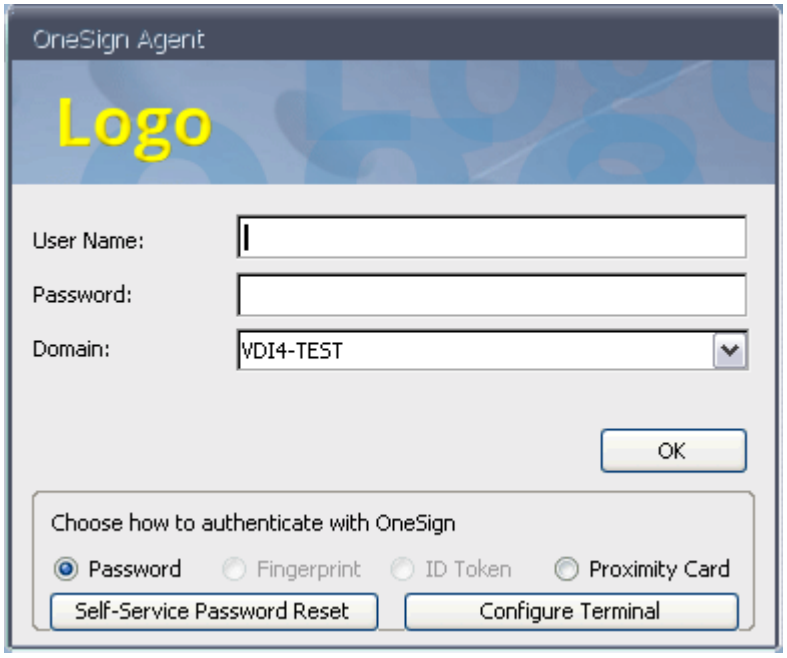
Header bitmap is used in the following windows:

- credentials-based login window
- proximity card login window
- password change window
- password request window
- pin request window
- pin change request window
- pin enrollment window

The header bitmap size is 381 x 62 (h x v) and it must be saved in xpm format (GIMP free software can be used to convert from several graphic formats to xpm).

The custom header bitmap must be copied in thin client "/tmp/config/files" directory. The file name must be "onesign.xpm".

An example of header bitmap customization is in the figure below.



2.9.2 Footer Bitmap

Footer bitmap is used in the following window:

- proximity card enrollment

The footer bitmap size is 425 x 50 (h x v) and it must be saved in xpm format (GIMP free software can be used to convert from several graphic formats to xpm).

The custom header bitmap must be copied in thin client "/tmp/config/files" directory. The file name must be "onesignfooter.xpm".

3 Appendix

3.1 Supported Proximity Card Readers

Supported and tested proximity card readers are:

- ACS ACR122 – P/N ACR122U-A2
- OmniKey 5321 CR
- OmniKey CardMan 5321
- OmniKey CardMan 5321 CLi
- RFIDeas pcProx Plus – P/N RDR-80582AKU

3.2 Troubleshooting

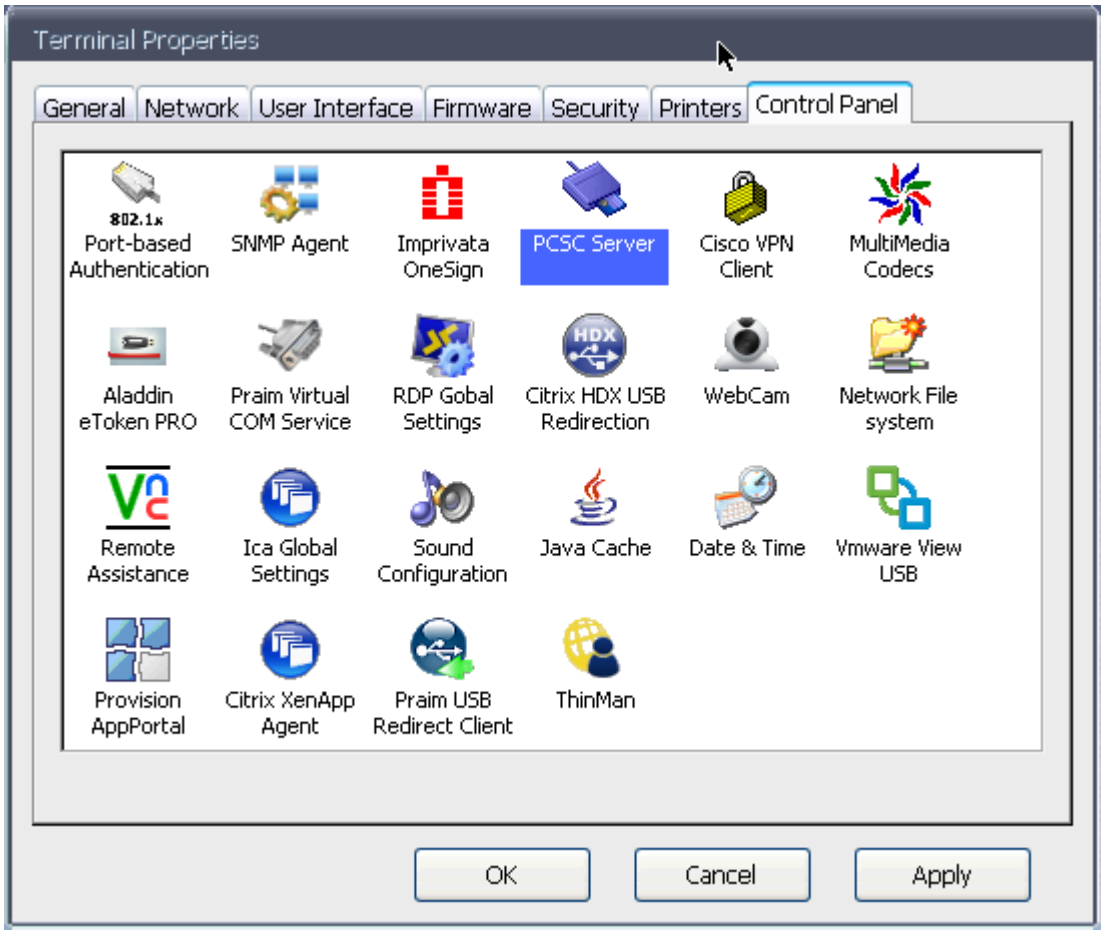
List of Troubleshooting arguments:

- Tapping Proximity Card does not work (see page 38)
- Monitor is not correctly recognized or configured (see page 39)
- Failed connection on start-up due to wrong configured URL (see page 40)

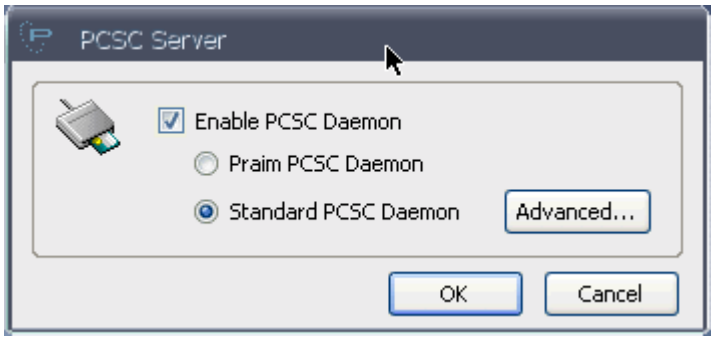
3.2.1 Tapping Proximity Card does not work

Verify on thin client that selected PCSC Server type is "Standard PCSC Daemon"

Access Terminal properties.



Double click on "PCSC Server"



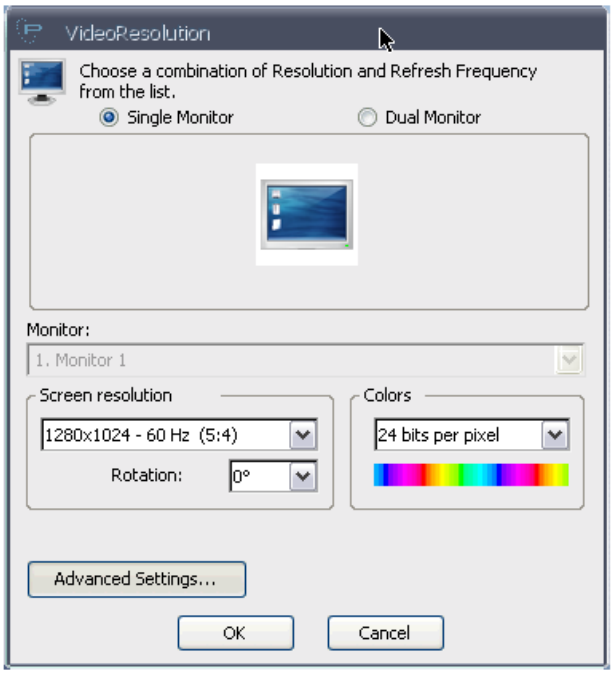
Select "Standard PCSC Daemon" and click "OK" to save changes.

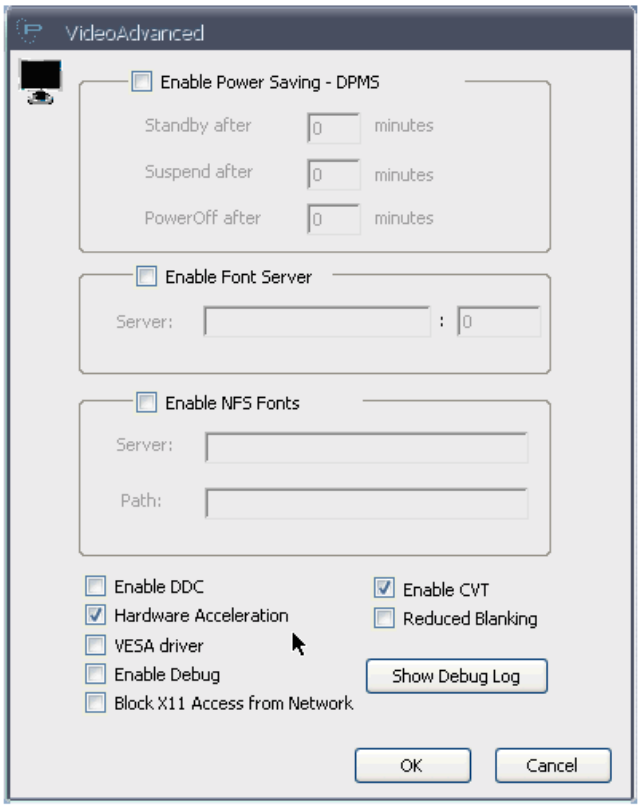
Click once again "OK" to close "Terminal Properties" window.

3.2.2 Monitor is not correctly recognized or configured

In some cases the thin client could not correctly recognize the monitor or could not set the proper resolution. In these cases open the "Terminal Properties" and select the "User Interface" tab.

Double click on "Video Resolution" icon.





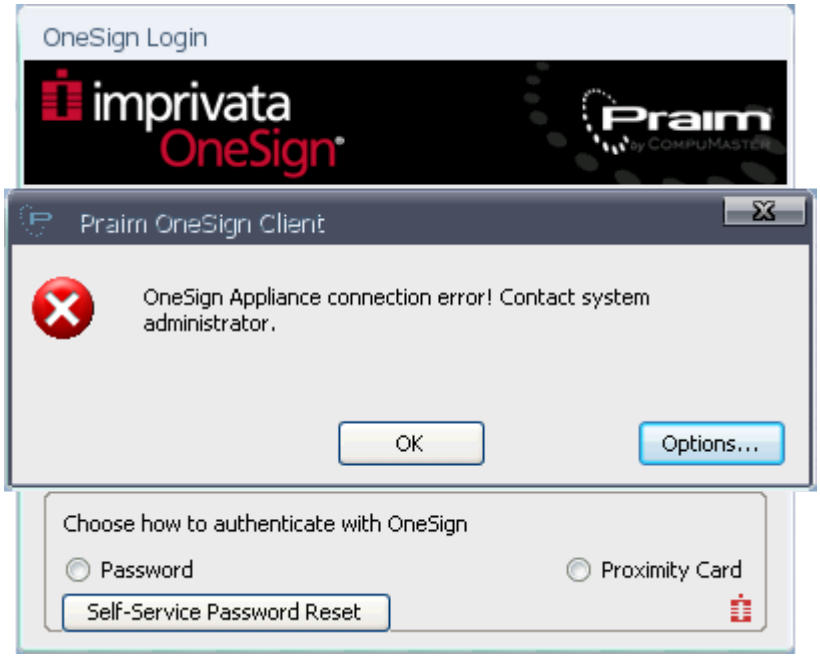
Click on "Advanced Settings..." and try to enable or disable the two parameters "Enable DDC" and "Enabled CVT". To confirm the choice click on "OK" of all the open windows. The terminal will reboot to apply the changes.

For high resolution monitors if the "Enable CVT" parameters is flagged try to tick "Reduced Blanking" parameter.

3.2.3 Failed connection on start-up due to wrong configured URL

A connection error can occurs at the thin client start-up in case of wrong URL configured.

In this case the error window is displayed at the thin client start-up.

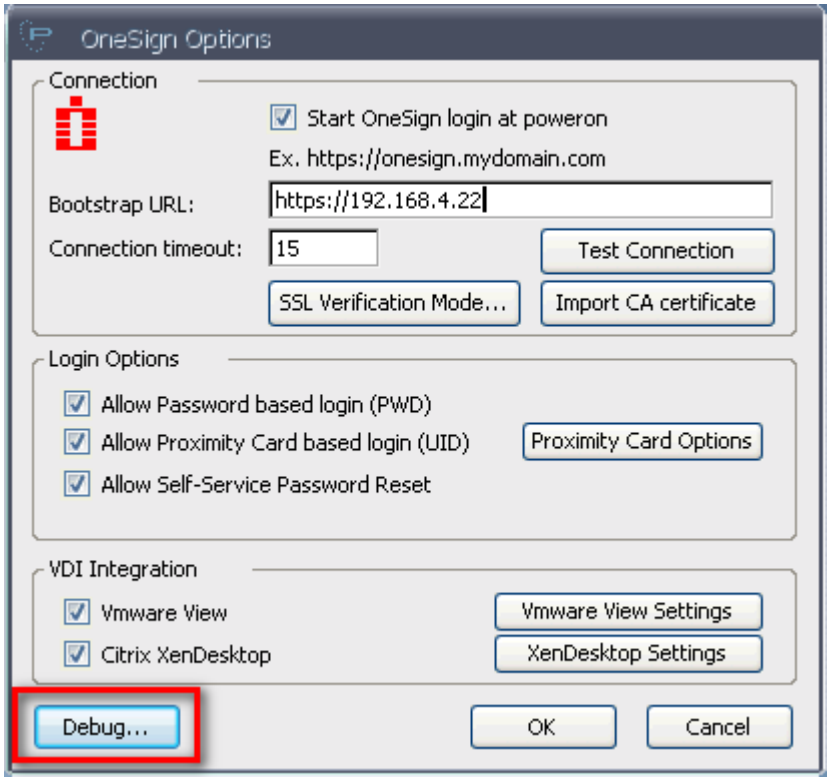


Clicking on "Options..." allows to access the "OneSign Options" window in order to change the Imprivata properties (see Configure ThinOX Thin Client to Communicate with OneSign (see page 13)).

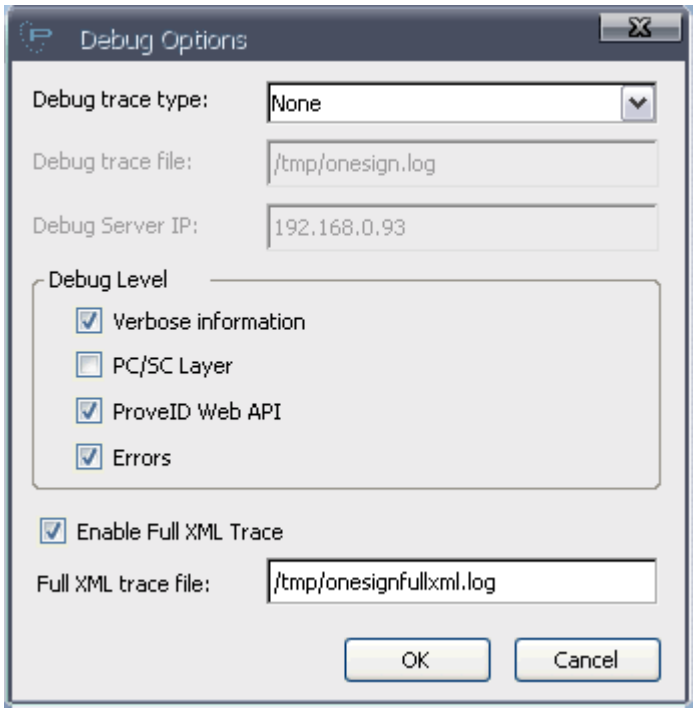
Whether the thin client is protected by a password this is requested in the window. Enter it to gain "OneSign Options" window access.

3.3 How To Create Log File

Some problem can be investigated reading log files on thin client or generating log over network (and captured by ThinMan).



You can specify all debug options clicking on "Debug" button in "Imprivata OneSign" window. It will open a new window with Debug options.

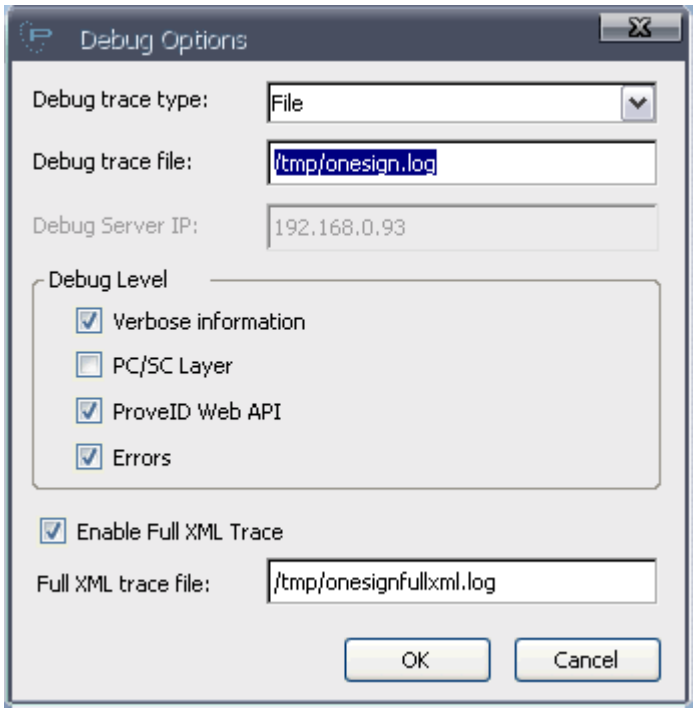


In this window you are able to define which debug trace type use to log events: it can be "None", "File" or "UDP Packet". In case of "None" no debug information are traced. See below for other cases.

In the "Debug Level" section you can define which events collect in the log.

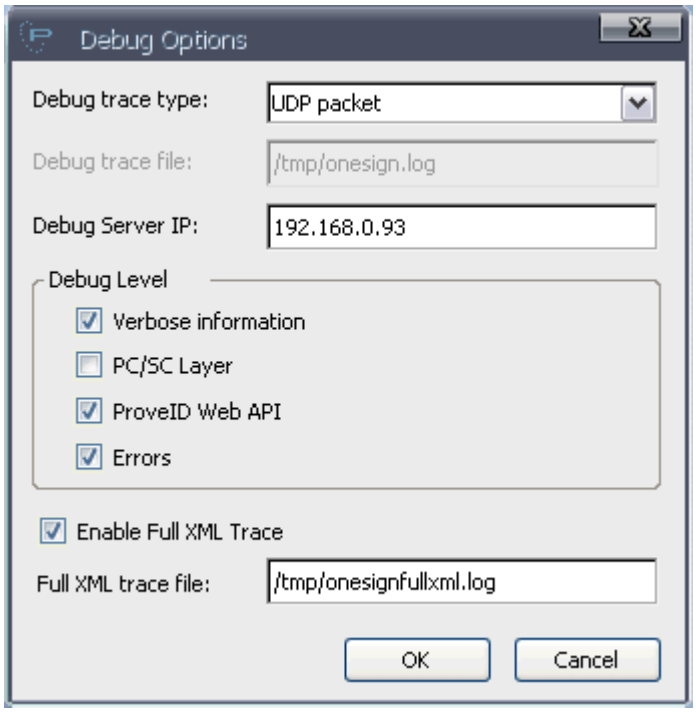
You can also flag "Enable Full XML trace" option: this tell the thin client to trace all XML communication between thin client and the Imprivata appliance and to save in the file defined in the next field (see also below for information about saving it on USB Mass Storage Key).

Trace information are not collected if you set "Debug Trace Type" to "None" and unflag the "Enable Full XML Trace" option.



If you set "Debug trace type" to "File" you have also to define the filename and path where log information are wrote. Filename can be stored in local thin client file system (e.g. "/tmp/onesign.log") or on a USB mass storage key. In the second case put a Usb Key in the thin client, the thin client will mount the Usb Key in the file system and visualize it in the desktop. Under the icon you will find the name of the mounted USB Key.

The Usb storage is mounted under "/tmp/mnt/" directory succeeded by the name of the Usb Key. E.g. in this case the path will be "/tmp/mnt/Volume/" (beware that pathname is case sensitive and will use "/" (slash) character as separator for directory), so a possible file name to provide can be "/tmp/mnt/Volume/onesign.log".

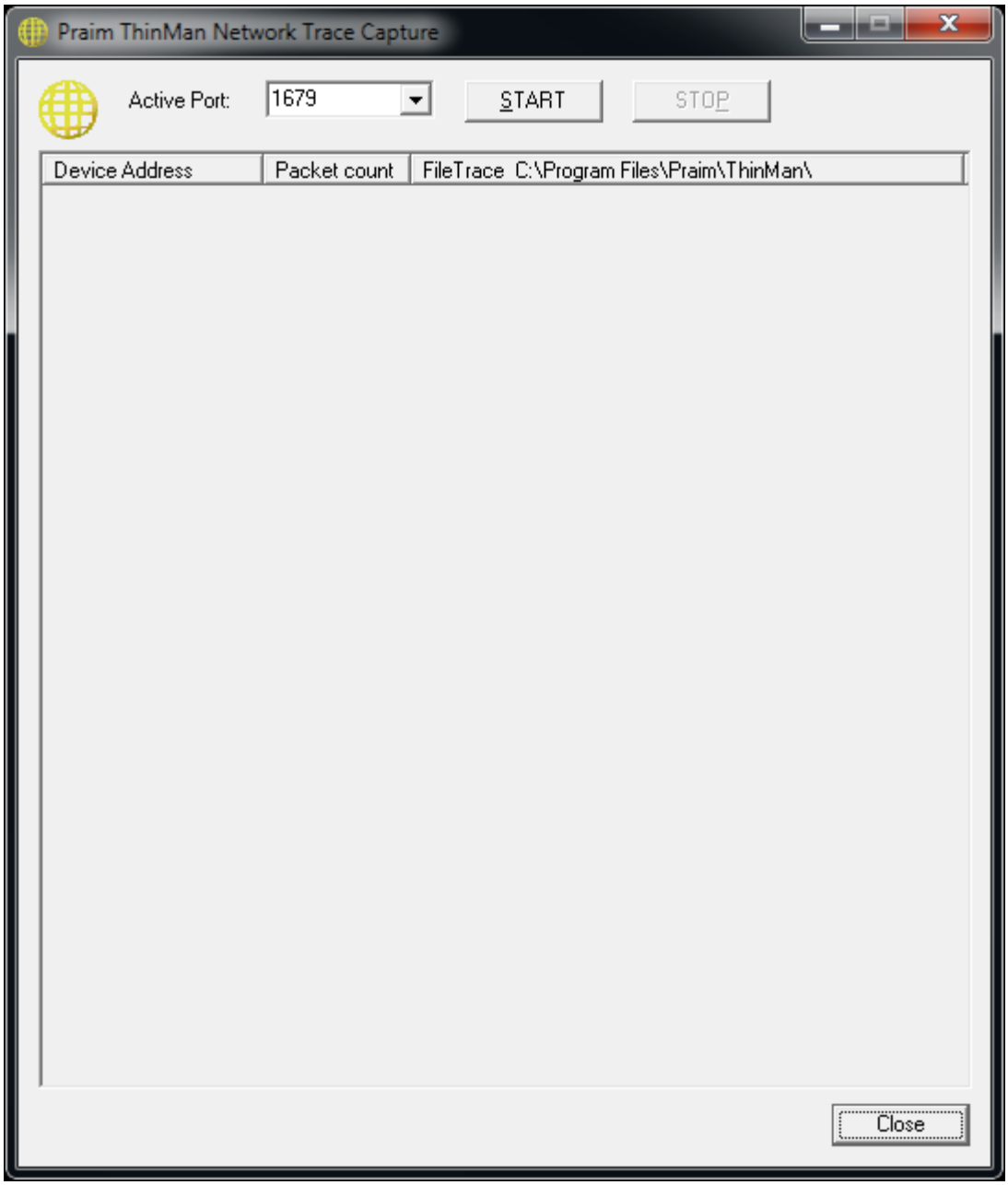


Other possible "Debug trace type" can be "UDP Packet". In this case is requested an IP Address where log information are sent. Insert the ThinMan Server IP Address, save the configuration and restart the thin client. Now follow this instruction on ThinMan Server to configure it.

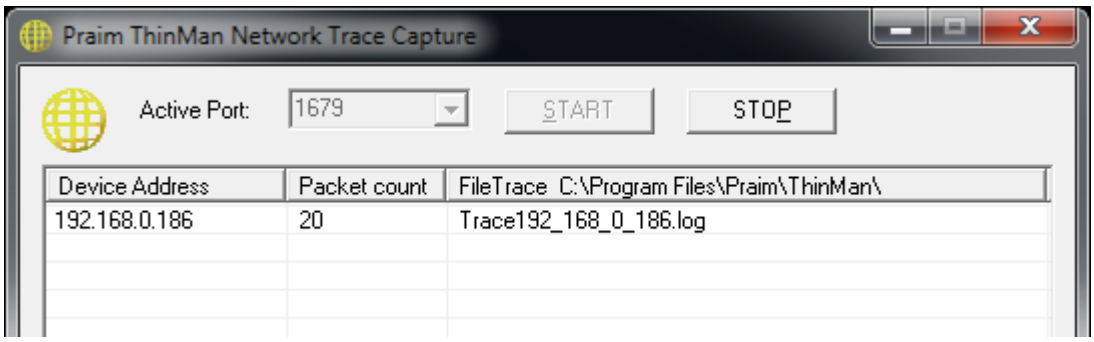
3.3.1 On the ThinMan Server

Access the folder where ThinMan is installed (typically "C:\Program Files\Praim\ThinMan").

Double click on "NetOpenTracer.exe" file. It will show the following window:

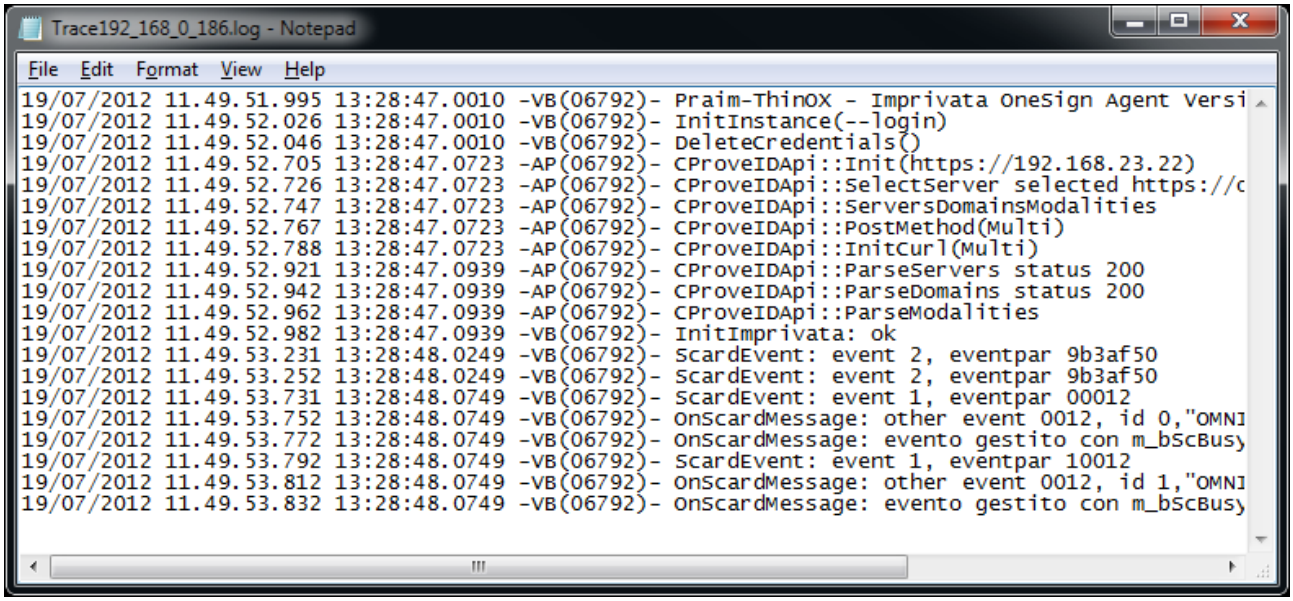


Click on "START" button to active the log collection.



Once the thin client start sending log information you will find a new line with device address, number of packet received and the log filename where log information are stored (path is visualized in the column title, e.g. "C:\Program Files\Praim\ThinMan").

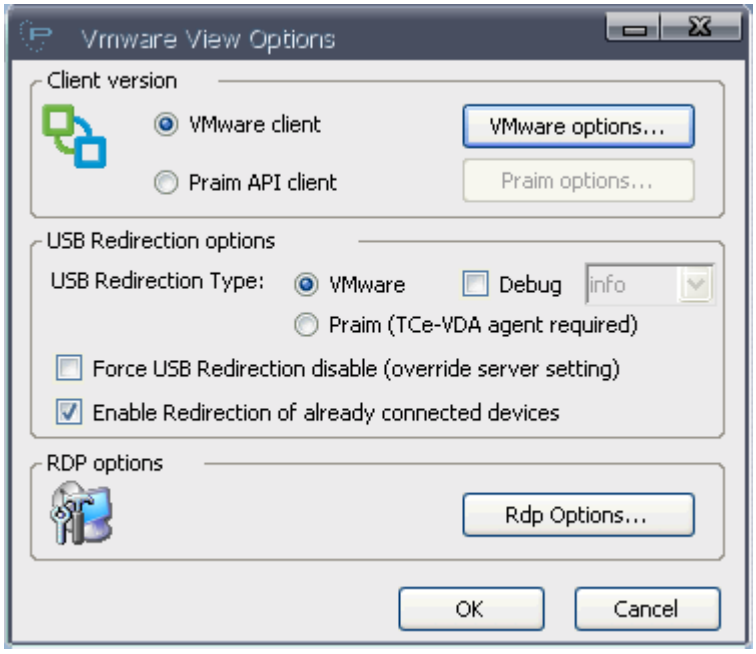
Double-Clicking on the filename will open the log file.



Once the trace information are collected you can close the "Praim ThinMan Network Trace Capture" clicking on "Close".

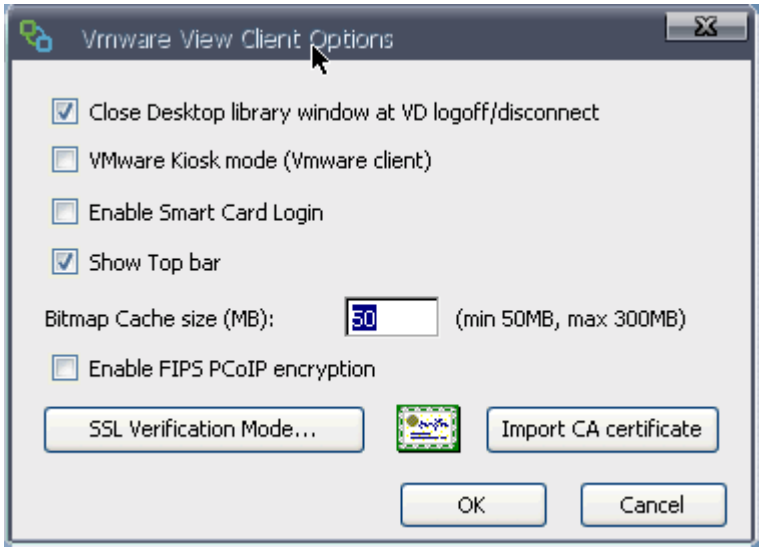
3.4 VMware Client Options

From "OneSign Option" window you can also configure parameters related to the VMware View connection. Click on "VMware View Settings" button. It will open a new window.

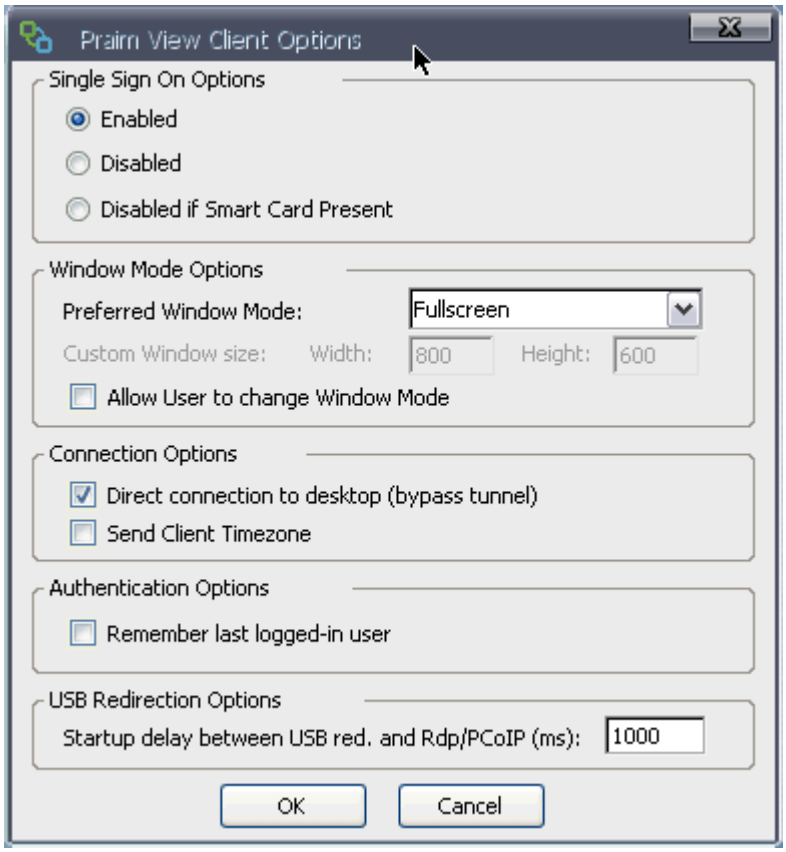


Here you can select options related to USB Redirection and to client version.

You may select to use standard "VMware client" and change related options by clicking on "VMware options".



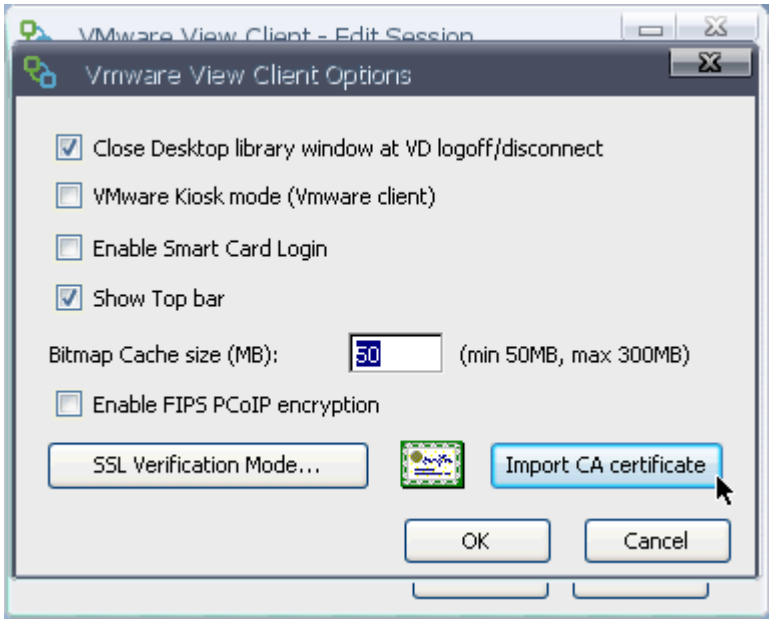
You may select to use "Praim API client" and change related options by clicking on "Praim options".



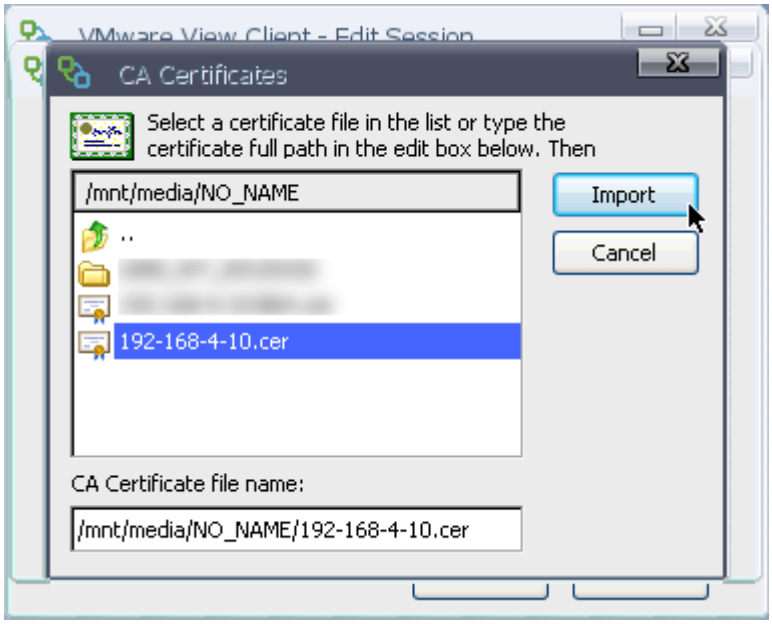
3.4.1 Importing CA Certificate for VMware connection

Export the CA Certificate from Certification Authority in Base64 format.

Copy the exported certificate on a USB Key and insert the USB Key in the thin client.



From "VMware View Client Options" click on "Import CA Certificate".

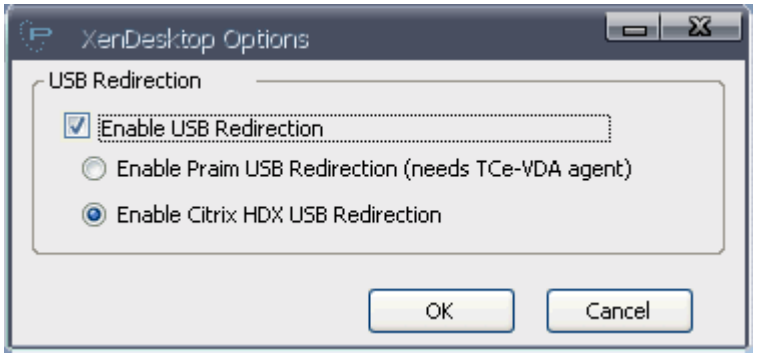


Browse the USB Key, select the certificate and import it into the thin client clicking on “Import”.

3.5 Citrix Client Options

From "OneSign Option" window you can also configure parameters related to the Citrix XenDesktop connection.

Click on "XenDesktop Settings" button. It will open a new window.

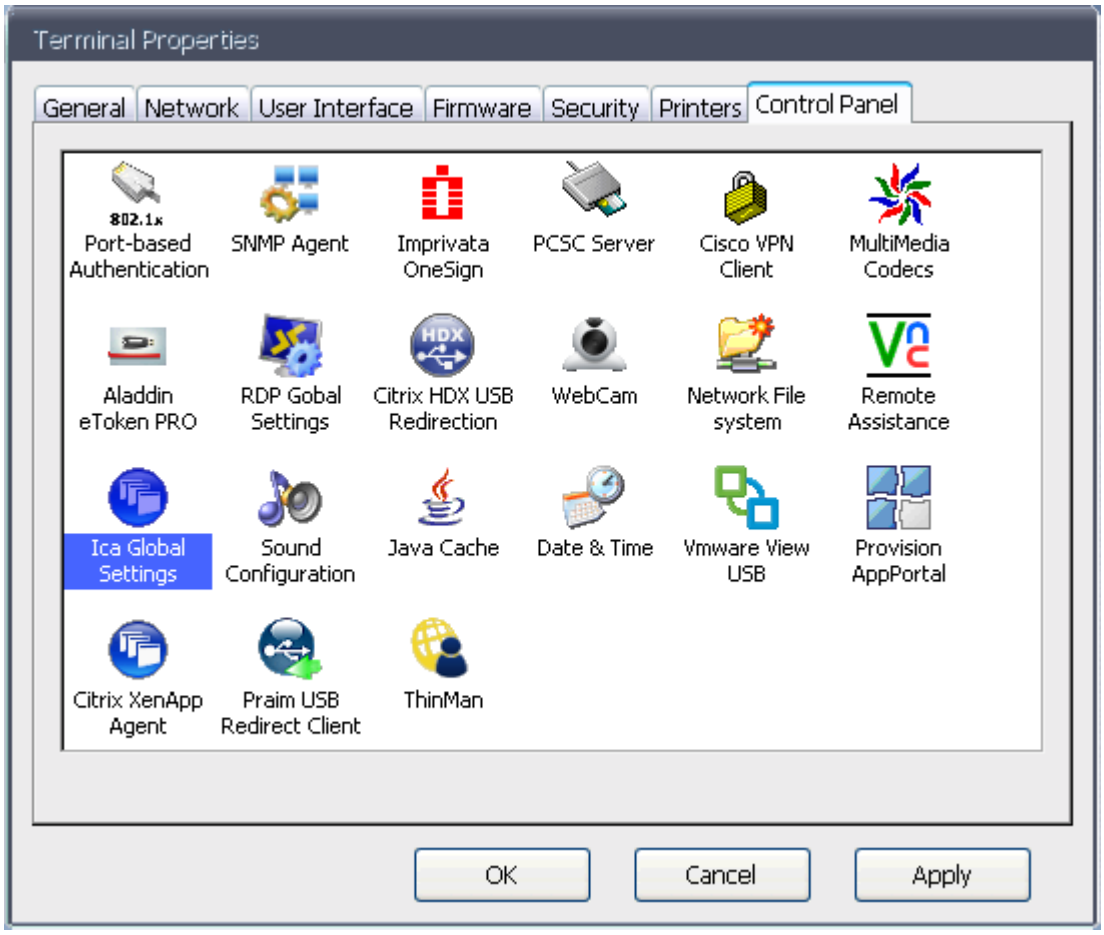


Here you may change option related to USB redirection.

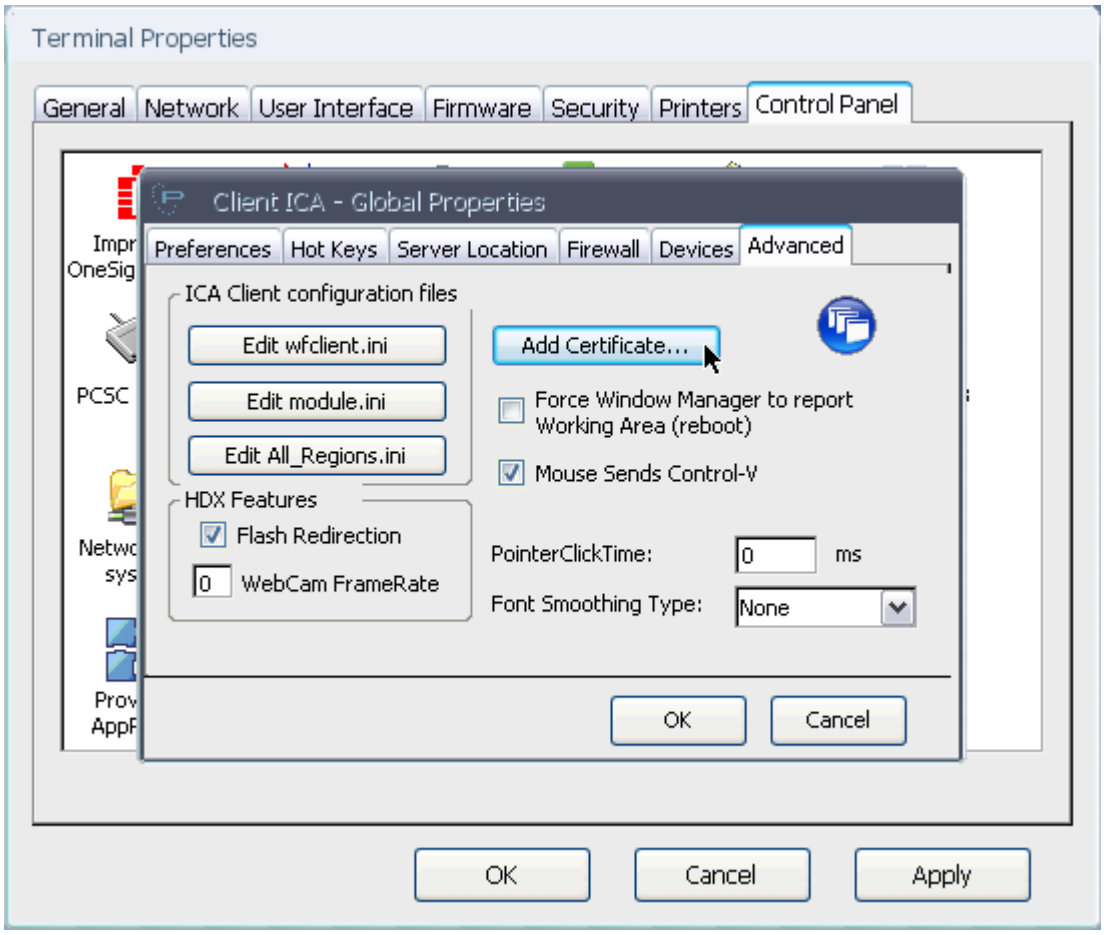
3.5.1 Importing CA Certificate for Citrix Connections

Export the CA Certificate from Certification Authority Server in Base64 format.

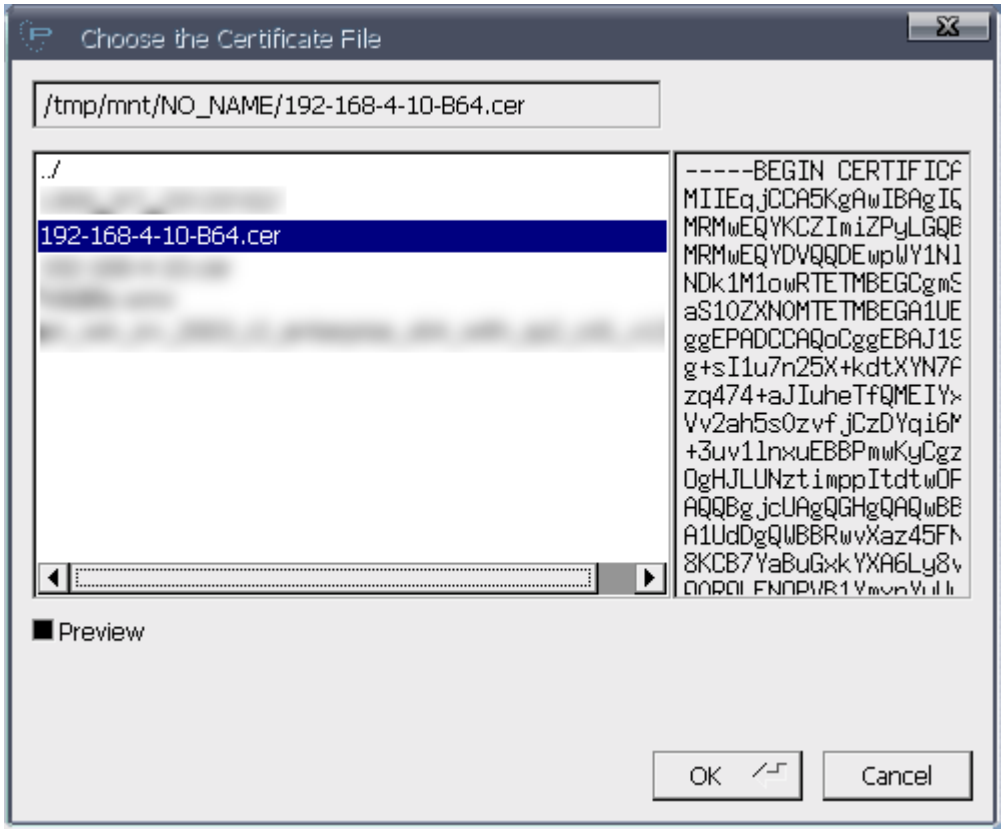
Copy the exported certificate on a USB Key and insert the USB Key in the thin client.



Open the "Terminal Properties" window and select "Control Panel" tab. Double-click on "ICA Global Settings".



Select the "Advanced" tab and click on "Add Certificate...".



Browse the USB Key, select the certificate and import it into the thin client clicking on “OK”.

3.6 How to easily copy configuration from a device to another device

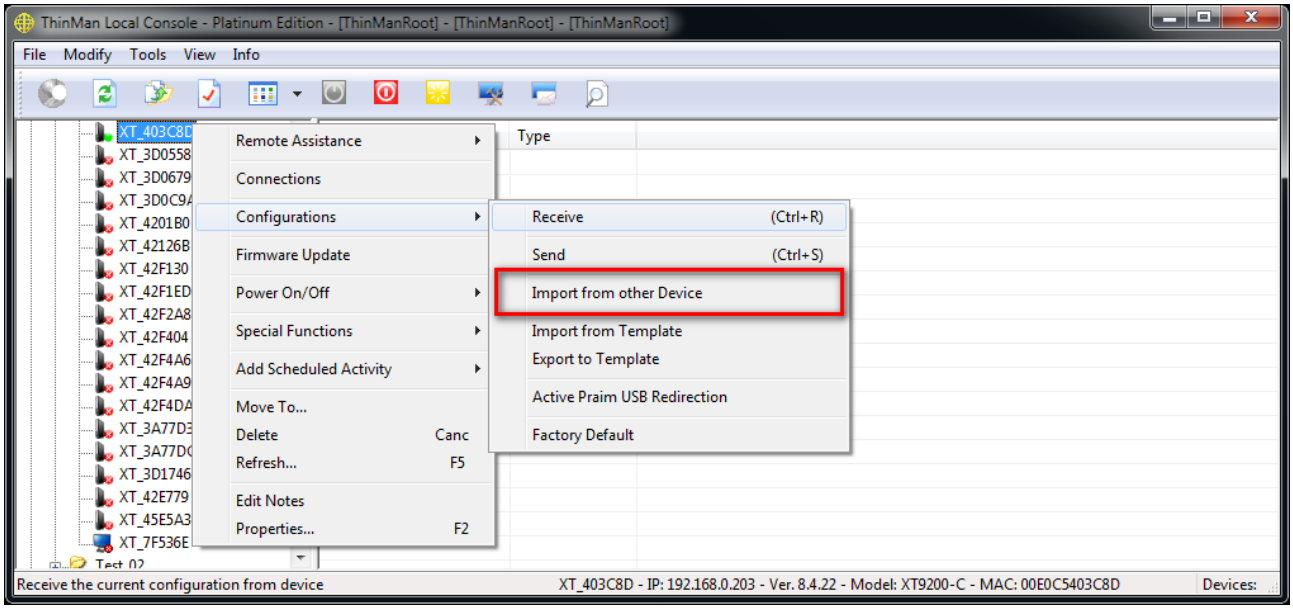
The ThinMan Console is the software provided by Praim that allows an easily management of the thin clients and their configurations.

From the ThinMan Console it is possible to copy the configuration of a thin client (say thinclientsource) to another thin client (say thinclientdestination) in many ways.

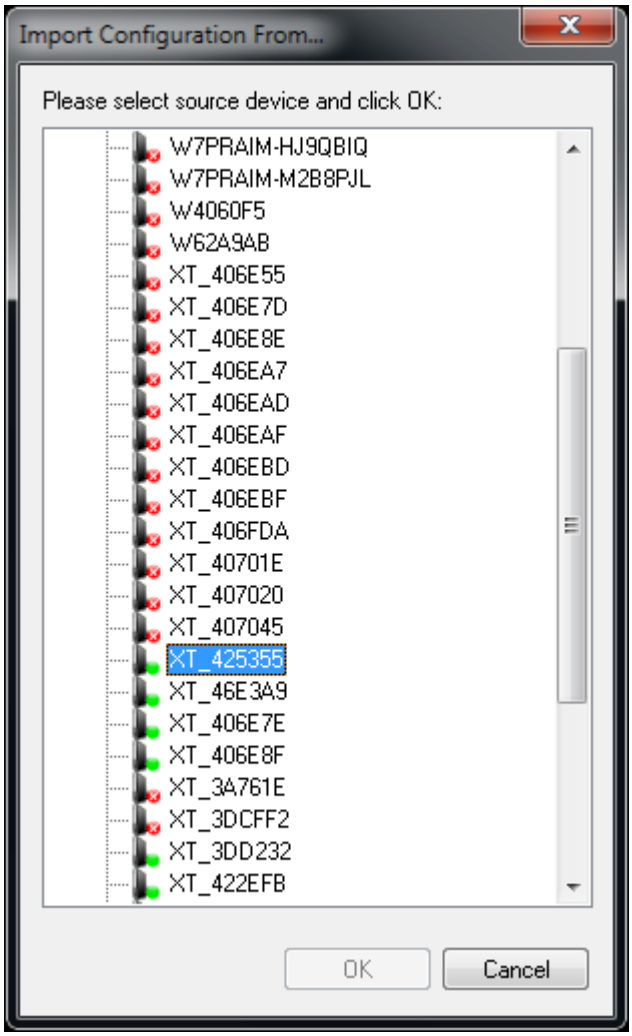
3.6.1 Copy configuration via single command

In this case it is possible to copy the configuration from thinclientsource to thinclientdestination using a single command on the ThinMan Console.

This command is useful if there are very few thin client.



In the ThinMan Console right-click the thinclientdestination and select "Import from other Device" under the menu "Configurations".

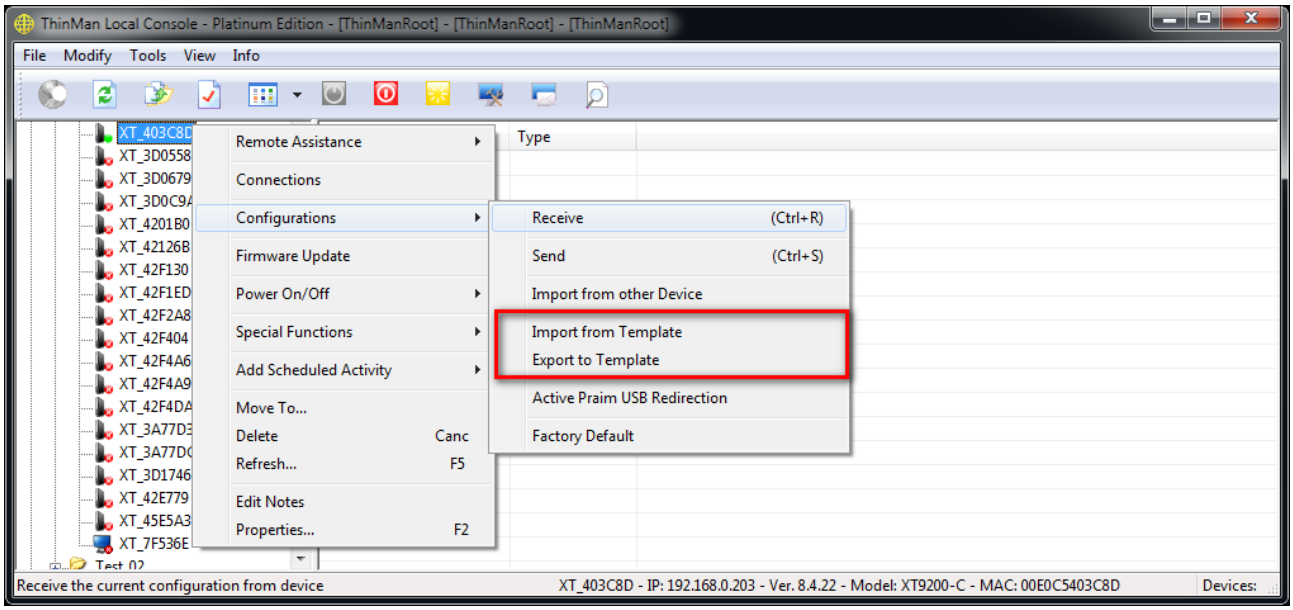


From the window select the thinclientsource and click "OK".

The configuration will be copied from device thinclientsource to device thinclientdestination.

3.6.2 Copy configuration via Template file

In this case the configuration of the thinclientsource is copied to a file for first (called template file), then the template is used to copy the configuration to the thinclientdestination.



Right-click on the thinclientsource and select "Receive" under the menu "Configurations".

Right-click on the thinclientsource and select "Export to Template" under the menu "Configurations".

Enter a name for the template file that will be generated and saved in the file system.

Right-click on the thinclientdestination and select "Import from Template" under the menu "Configurations".

Select from the dialog window the previously saved template. On the subsequent request click on "Yes" to send the configuration to the thin client.