

Documentation Area

Using ThinOX Thin Client with Imprivata OneSign 4.6 Environment

This document is exclusive property of Praim Srl. Permission is granted to print and copy this document for noncommercial distribution.

Author:DocumentationDate:Sep 17, 2012 2:54 PMURL:http://wiki.praim.com/display/Imprivata



Table of Contents

1	Setting up OneSign Environment	4
	1.1 Check License	5
	1.2 Enabling ProveID Web API	6
	1.3 Configuring VDI Options in OneSign	7
2	2 Configuring ThinOX Thin Client	9
	2.1 Update ThinOX ThinClient with Latest Firmware	10
	2.2 Configure ThinOX Thin Client to Communicate with OneSign	13
	2.2.1 SSL Verification Mode	15
	2.2.2 Import CA Certificate	15
	2.2.3 Copy Thin Client Configuration	16
	2.3 Use Smart Card as Proximity Card	17
	2.4 Proximity Card Options	19
	2.5 Configure ThinOX Thin Client for Imprivata VDI Integration	21
	2.5.1 VMware View Infrastructure	21
	2.5.2 Citrix XenDesktop/XenApp Infrastructure	21
	2.6 Card Enrollment	23
	2.7 Self Service Password Reset	25
	2.8 Terminal Properties for Thin Client Users	27
	2.8.1 Sound Configuration	30
	2.8.2 Mouse Configuration	31
	2.8.3 Internationalization Configuration	31
	2.8.4 Video Settings	32
	2.9 Bitmap Customization	34
	2.9.1 Header Bitmap	34
	2.9.2 Footer Bitmap	34
3	Appendix	36
	3.1 Supported Proximity Card Readers	37
	3.2 Troubleshooting	38
	3.2.1 Tapping Proximity Card does not work	38
	3.2.2 Monitor is not correctly recognized or configured	39
	3.2.3 Failed connection on start-up due to wrong configured URL	40
	3.3 How To Create Log File	41
	3.3.1 On the ThinMan Server	44
	3.4 VMware Client Options	47
	3.4.1 Importing CA Certificate for VMware connection	48
	3.5 Citrix Client Options	50
	3.5.1 Importing CA Certificate for Citrix Connections	50
	3.6 How to easily copy configuration from a device to another device	54
	3.6.1 Copy configuration via single command	54
	3.6.2 Copy configuration via Template file	55



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:

- Check License (see page 5)
- Enabling ProveID Web API (see page 6)
- Configuring VDI Options in OneSign (see page 7)



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)

	Properties Policies Users, Computers and Domains Reports Tokens SSO COCOUR
Mod	Agent Deployment System Settings RADIUS Connections OneSign Extensions ProveID Sites Virtual Desktops
Ý	OneSign Authentication Management Enabled OneSign Authentication Management helps organizations increase security and replace Windows passwords with a range of authentication options.
4	OneSign Single Sign-On Enabled OneSign Single Sign-On helps organizations quickly and effectively solve password security and user access issues.
4	OneSign Anywhere Enabled OneSign Anywhere provides secure remote application access and single sign-on.
√	OneSign Secure Walk-Away Enabled OneSign Secure Walk-Away allows workstations to automatically lock when user is not detected at the workstation.
 ✓ 	Virtual Desktop Access Enabled OneSign provides extended integration, automation, and strong authentication support for VMware View, Citrix XenDesktop and Sun Ray VDI.
Ý	ProveID Web API Enabled OneSign delivers strong authentication for third-party products via ProveID Web API integration.



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

Home Properties Policies Users, Computers and Domains Reports Tokens SSO Cocourt imprivata OneSign
Modules Agent Deployment System Settings RADIUS Connections OneSign Extensions ProveID Sites Virtual Desktops
ProveID Client - Application Name Mapping
Specify the name of the external application that is calling ProveID and which OneSign application profile it maps to.
Add Application Mapping
ProveID Web API - API Access
☑ Allow access to OneSign via ProveID web API
Teradici
E Future 1
Tuture 2
E Future 3
Future 4
E Future 5
E Future 6
Future 8 Future 9
Cancel



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.



me Properties Po	licies Users, Computers and Domains Reports Tokens SSO
mprivata	
OneSign	
Modules Agent Deploy	ment System Settings RADIUS Connections OneSign Extensions ProveID Sites Virtual Desktor
VMware View	
OneSign agents will comm	unicate 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	X Add another Connection Manager
URL (http[s]://name.domain.c	om)
User authentication from a	Il VMware View clients can be disallowed if necessary.
Allow authentication fr	om VMware View clients
Sun Rav	
Sun Ray servers must be	configured with OneSign software. After configuration, provide the server and configuration into here.
OneSign agents will comm	Add another server
be used with OneSign.	1 Sun Ray server that will 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/CardEventPush	er 8080
User authentication from s	Sun Ray clients can be disallowed if necessary.
Allow authentication fr	om Sun Ray devices
Citation Management and	
Citrix XenDesktop	
OneSign agents will comm	unicate only with known XenDesktop PNAgent sites. List each PNAgent site that will be used with OneSign.
https://192.168.23.25/cit	ix/pnagent Add another server
Full PNAgent site URL (e.g., h	ttps://mycompany.com/Citrix/PNAgent)
User authentication from a	all XenDesktop devices can be disallowed if necessary.
User authentication from a	all XenDesktop devices can be disallowed if necessary. om XenDesktop-enabled devices



2 Configuring ThinOX Thin Client

These chapter explain how to configure ThinOX Thin Client:

- Update ThinOX ThinClient with Latest Firmware (see page 10)
- Configure ThinOX Thin Client to Communicate with OneSign (see page 13)
- Use Smart Card as Proximity Card (see page 17)
- Proximity Card Options (see page 19)
- Configure ThinOX Thin Client for Imprivata VDI Integration (see page 21)
- Card Enrollment (see page 23)
- Self Service Password Reset (see page 25)
- Terminal Properties for Thin Client Users (see page 27)
- Bitmap Customization (see page 34)



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.

🌐 ThinMan Local Console - Platinum Edition - [ThinManRoot]			×				
File Modify Tools View Info							
🔊 🔹 🏂 🎝 💷 •	- 🔘 🚺 🔀	🔤 🗖	Ì				
P- I Network Neighborhood	Name	IP Address Sul	onet Me	odel	Status	MAC Address	-
🖃 😴 Test_01	XT_403C8D	192.168.0.186 192	.168.0.0/24 XT	<u>1920</u> 0-С	On	00-E0-C5-40-3C-8D	
PRAIM-WEHIQ791K =	LoxT_404C7C	Remote Assistance	e	▶)0-C	Off	00-E0-C5-40-4C-7C	
	L XT_42052C	Connections		-I	On	00-E0-C5-42-05-2C	
	Lo XT_3D0558	Connections)-I	Off	00-E0-C5-3D-05-58	
W7PRAIM-D8387BI	Lo XT_3D0679	Configurations		▶)-I	Off	00-E0-C5-3D-06-79	
	L_XT_3D0C9A])-I	Off	00-E0-C5-3D-0C-9A	
W40465F	▶ ₉ XT_4201B0	Firmware Update)-I	Off	00-E0-C5-42-01-B0	
	↓ XT_42126B	Power On/Off		▶)-I	Off	00-E0-C5-42-12-6B	≡
	Lo XT_42F130)-I	Off	00-E0-C5-42-F1-30	
	by XT_42F1ED	Special Functions)-I	Off	00-E0-C5-42-F1-ED	
	Log XT_42F2A8	Add Scheduled Activity)-I	Off	00-E0-C5-42-F2-A8		
📗 XT_3D0679	Lo XT_42F404	Add Scheduled A	cuvity)-I	Off	00-E0-C5-42-F4-04	
📗 XT_3D0C9A	▶ ₉ XT_42F4A6	Move To)-I	Off	00-E0-C5-42-F4-A6	
🗽 XT_4201B0	by XT_42F4A9	Delete	Canc)-I	Off	00-E0-C5-42-F4-A9	
🗽 XT_42126B	▶ XT_42F4DA	Refresh	F5)-I	Off	00-E0-C5-42-F4-DA	
📙 XT_42F130	LoxT_3A77D3		15	i0-A	Off	00-E0-C5-3A-77-D3	
📕 XT_42F1ED	▶ XT_3A77DC	Edit Notes		i0-A	Off	00-E0-C5-3A-77-DC	
	L XT 3D1866	Properties	F2	i0-A	Off	00-F0-C5-3D-1R-66	Ŧ
Update the firmware on the device		XT_403	3C8D - IP: 192.168.0	0.186 - Ver. 8.4.	22 - Model: XT	9200-C - MAC: 00E0C54	10

From the menu select "Firmware Update".



Update Firmware Options		
Firmware Update Mode		
Embedded HTTP Service (recommended)		
© Other Mode (Obsolete) Set Other Mode		
Options Send Configuration during Firmware Update (if present) Unattended Mode (ThinMan active required!!!) Force Complete Update Command: None		
OK Cancel		

Leave "Embedded HTTP Service" flagged and click on "OK".

💮 Open firm	nware file		 X
Look in: 📘	Desktop	- G 🕸 I	≫
Name	*	Size	Item type 🔺
			File folder
🗋 ХТ9000	-C-U_8.4.20.tar	200.600 K	B TAR File
XT9000-C-U_8.4.26.tar 20			B TAR File
XT9200	-C-U_8.4.20.tar	311.290 Ki	B TAR File 🗏
XT9200	-C-U_8.4.26.tar	311.710 K	B TAR File 🚽
•			Þ
File <u>n</u> ame:	XT9200-C-U_8.4.26.tar		Open
Files of type:	Update File (*.tar.gz,*.tar)	•	Cancel

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).

File Transfer	
Device: XT	_403C8D
Updating Fin	mware. Please wait
	Details >> Cancel



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".



🕝 OneSign Options			
Connection Start OneSign login at poweron Ex. https://onesign.mydomain.com Bootstrap URL: https://192.168.4.22 Connection timeout: 15 SSL Verification Mode Import CA certificate Login Options Allow Password based login (PWD) Allow Proximity Card based login (UID) Proximity Card Options Allow Self-Service Password Reset			
VDI Integration			
Vmware View View Settings			
Citrix XenDesktop XenDesktop Settings			
Debug OK Cancel			

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.



OneSign Agent	R	
impriv Or	∕ata neSign•	
User Name: Password:		
Domain:	VDI4-TEST	~
		ОК
Choose how to	authenticate with OneSign	
Password	🔘 Fingerprint 👘 ID	Token 🔘 Proximity Card
Self-Service	Password Reset	<u>i</u>

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)"

🕒 OneSign Options				
Connection —	Connection			
n 🗋	📝 Start OneSign login at p	poweron		
■■	Ex. https://onesign.mydom	nain.com		
Bootstrap URL:	https://192.168.4.22			
Connection timeout:	15	Test Connection		
	SSL Verification Mode	Import CA certificate		
Login Options —				
📝 Allow Password	based login (PWD)			
🚺 Allow Proximity	Card based login (UID)	Proximity Card Options		
🛛 📝 Allow Self-Servio	Allow Self-Service Password Reset			
VDI Integration				
Vmware View Vmware View Settings				
Citrix XenDeskto	e	XenDesktop Settings		
Debug		OK Cancel		

Click on "Proximity Card Options" button.





🕞 Proximity Card Options		
Proximity Card Options		
C Lock endpoint at Proximity Card remove		
Ock endpoint at Proximity Card tapping		
Tap Event on Card plug		
Tap Event on Card quick remove		
Maximum Card plug/remove interval (ms): 2000		
Single TAP user switch		
Ask PIN/Password on same user unlock tapping		
✓ Use Smart Card as Proximity Card		
Ask for OneSign PIN		
Ask for Smart Card PIN		
OK Cancel		

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.

🕑 Proximity Card Options		
Proximity Card Options		
Lock endpoint at Proximity Card remove		
Ock endpoint at Proximity Card tapping		
Tap Event on Card plug		
Tap Event on Card quick remove		
Maximum Card plug/remove interval (ms): 2000		
Single TAP user switch		
Ask PIN/Password on same user unlock tapping		
Use Smart Card as Proximity Card		
Ask for OneSign PIN		
Ask for Smart Card PIN		
OK Cancel		

"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 <u>not</u> 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.

🕞 OneSign Option	IS		
Connection ——	📝 Start OneSign login at p	oweron	
Bootstrap URL:	Ex. https://onesign.mydomain.com https://192.168.4.22		
Connection timeout:	15	Test Connection	
	SSL Verification Mode	Import CA certificate	
Login Options Allow Password based login (PWD)			
Allow Proximity Card Dased login (UID) Proximity Card Options Allow Self-Service Password Reset			
VDI Integration			
Vmware View		mware View Settings	
Citrix XenDeskto	ip 🔁	KenDesktop Settings	
Debug		Cancel	

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".

🕞 Enrollment Request	<u> </u>
Confirm your identity	
Enter the cardholder's network credentials.	
User Name:	
Password:	
	((um))
Domain:	((((*))))
VDI4-TEST	
Next >	ID: 73ED7997
INEXC ->	
imprivata	Cancel
Unesign	

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.

🕞 Enrollmer	nt Request		
impr C	ivata neSign	4	
PIN: PIN confirm:]
	ОК	Cancel	

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.

🤄 OneSign Option	s		
Connection —			
l n	🔽 Start OneSign login at poweron		
■■	Ex. https://onesign.mydomain.com		
Bootstrap URL:	https://192.168.23.22		
Connection timeout:	15		
	SSL Verification Mode Import CA certificate		
Login Options —			
🛛 📝 Allow Password I	based login (PWD)		
Allow Proximity Card based login (UID) Proximity Card Options			
Allow Self-Service Password Reset			
VDI Integration -			
🔲 Vmware View	Vmware View Settings		
Citrix XenDeskto	KenDesktop Settings		
Debug	OK Cancel		

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.



OneSign Agent			
impriv On	ata eSign•		
User Name: Password:			
Domain:	VDI4-TEST		~
			ОК
Choose how to authenticate with OneSign			
Password) Fingerprint	🔵 ID Token	Proximity Card
Self-Service Pa	ssword Reset	Config	gure Terminal

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.

Terminal Properties
General Network User Interface Firmware Security Printers Control Panel
Deny Connection Modify Enable SSH Storage
Require password to modify the terminal configuration
Password: ****** Confirm: ******
User Parameters
Video Settings Configure
Mouse Settings
Sound Settings Show Advanced Settings Button
User Authentication
Password: Confirm:
Allow user to modify password
OK Cancel Apply

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.



1000	
\mathbf{P}	raim
by	CompuMaster

Terminal Properties
General Network User Interface Firmware Security Printers Control Panel Image: Deny Connection Modify Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration Image: Enable SSH Image: Deny Connection Modify the terminal configuration
User Parameters Video Settings International Settings Mouse Settings Sound Settings Show Advanced Settings Button
User Authentication Password: Confirm: Allow user to modify password
OK Cancel Apply

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.



🕑 v	ideoResolutionConfig
_ Video	Resolutions Configuration
	Enable Multimonitor Configuration 🛛 🧾 🗌
	Enable Color Depth Configuration
	Enable Advanced Configuration
	Enable Resolution Configuration
	Enabled Resolutions
	640x480 - 60 Hz (4:3)
	640x480 - 75 Hz (4:3)
	640x480 - 85 Hz (4:3)
	✓ 800×600 - 60 Hz (4:3)
	800x600 - 72 Hz (4:3)
	□ 800×600 - 75 Hz (4:3) ▼
	OK Cancel

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.

OneSign Agent
imprivata OneSign
Please Tap your Proximity Card on the reader to logon.
Choose how to authenticate with OneSign
Password Fingerprint ID Token Proximity Card
Self-Service Password Reset

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



Terminal Properties	N	
User Control Panel		
Sound Mouse Configuration Settings	International Video Settings Resolution	
]
[OK Cancel Advanced Settings	

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.



🕑 Sound configuration applet
Sound Settings
Audio Output: Volume: Output Device: (VILTERNAL) UDA UTALITOD IN (UT 17000 Angle a)
Audio Input:
Volume: 52 Input Device:
Mic Boost (+20dB)
Sound Server None Port:

2.8.2 Mouse Configuration

This window show the mouse settings possibilities.

🕑 Mouse Settings		
Mouse —	Type: PS\2	
Speed:		
Acceleration:	3 Buttons Emulation	
	 Disable Right Button Invert Buttons 	
	OK Cancel	



2.8.3 Internationalization Configuration

📄 International Settings		
System Language		
Language: English 💽		
Keyboard		
Layout: Italian (Italy) 💽 Edit		
Repeat Rate: 0		
Repeat Delay: 0		
Test Keyboard:		
Enable NumLock at Startup		
OK Cancel		

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.



문 VideoResolution	CP VideoAdvanced
Choose a combination of Resolution and Refresh Frequency from the list.	Enable Power Saving - DPMS Standby after 0
	Suspend after 0 minutes PowerOff after 0 minutes
Monitor:	Server: 0
1. Monitor 1 Screen resolution 1280x1024 - 60 Hz (5:4) Rotation: 0° Colors	Enable NFS Fonts Server: Path:
Advanced Settings OK Cancel	 Enable DDC Enable CVT Hardware Acceleration Reduced Blanking VESA driver Enable Debug Show Debug Log Block X11 Access from Network
	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 381×62 (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.

OneSign Agent		
Logo		6
User Name:	I	
Password:		
Domain:	VDI4-TEST	~
		ОК
Choose how to a	uthenticate with OneSign	
Password	🔘 Fingerprint 🛛 🔘 ID Token	Proximity Card
Self-Service Pa	ssword Reset Confi	igure Terminal

2.9.2 Footer Bitmap



Footer bitmap is used in the following window:

• proximity card enrollment

The footer bitmap size is 425×50 (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

- Supported Proximity Card Readers (see page 37)
- Troubleshooting (see page 38)
- How To Create Log File (see page 41)
- VMware Client Options (see page 47)
- Citrix Client Options (see page 50)
- How to easily copy configuration from a device to another device (see page 54)



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.

🕑 VideoResolution	문 VideoAdvanced
Choose a combination of Resolution and Refresh Frequency from the list.	Standby after 0 minutes
	Suspend after 0 minutes PowerOff after 0 minutes
	Enable Font Server
Monitor:	Server:
Screen resolution I280x1024 - 60 Hz (5:4) Image: Colors Rotation: Image: Operation matching	Enable NFS Fonts Server: Path:
Advanced Settings OK Cancel	 Enable DDC Enable CVT Hardware Acceleration Reduced Blanking VESA driver Enable Debug Show Debug Log Block X11 Access from Network
	OK Cancel



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).

🕒 OneSign Options		
Connection —		
l n	📝 Start OneSign login at poweron	
	Ex. https://onesign.mydomain.com	
Bootstrap URL:	https://192.168.4.22	
Connection timeout:	15 Test Connection	
	SSL Verification Mode Import CA certificate	
Login Options —		
Allow Password based login (PWD)		
Allow Proximity Card based login (UID) Proximity Card Options		
Allow Self-Service Password Reset		
ر VDI Integration		
Vmware View Vmware View Settings		
Citrix XenDesktop XenDesktop Settings		
Debug	OK Cancel	

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



🕒 Debug Options	<u></u>	
Debug trace type:	None	
Debug trace file:	/tmp/onesign.log	
Debug Server IP:	192.168.0.93	
Debug Level Verbose information PC/SC Layer Verbose D Web API Verbose D Web API Verbose D Web API		
C Enable Full XML Trace		
Full XML trace file:	/tmp/onesignfullxml.log	
	OK Cancel	

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.



🕞 Debug Options		
Debug trace type:	File	
Debug trace file:	/tmp/onesign.log	
Debug Server IP:	192.168.0.93	
C Debug Level		
Verbose information		
PC/SC Layer		
🔽 ProveID Web /	API	
V Errors		
🔽 Enable Full XML Trace		
Full XML trace file:	/tmp/onesignfullxml.log	
	OK Cancel	

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".



🖻 Debug Options		
Debug trace type:	UDP packet 💉	
Debug trace file:	/tmp/onesign.log	
Debug Server IP:	192.168.0.93	
r Debug Level		
Verbose information		
🔲 PC/SC Layer		
V ProveID Web API		
📝 Errors		
Enable Full XML Trace		
Full XML trace file:	/tmp/onesignfullxml.log	
	OK Cancel	

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:



🕕 Praim ThinMan N	etwork Trace Capture
Active Port:	1679 ▼ <u>S</u> TART STOP
Device Address	Packet count FileTrace C:\Program Files\Praim\ThinMan\
]	Close

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

I Praim ThinMan Network Trace Capture		
Active Port:	1679	START STOP
Device Address	Packet count	FileTrace C:\Program Files\Praim\ThinMan\
192.168.0.186	20	Trace192_168_0_186.log



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.

Trace192_168_0_186.log - Notepad		
<u>F</u> ile <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp		٦
Inc Edit First 19/07/2012 11.49.51.995 13:28:47.0010 19/07/2012 11.49.52.026 13:28:47.0010 19/07/2012 11.49.52.026 13:28:47.0723 19/07/2012 11.49.52.705 13:28:47.0723 19/07/2012 11.49.52.726 13:28:47.0723 19/07/2012 11.49.52.767 13:28:47.0723 19/07/2012 11.49.52.767 13:28:47.0723 19/07/2012 11.49.52.788 13:28:47.0723 19/07/2012 11.49.52.921 13:28:47.0723 19/07/2012 11.49.52.921 13:28:47.0723 19/07/2012 11.49.52.942 13:28:47.0939 19/07/2012 11.49.52.962 13:28:47.0939 19/07/2012 11.49.52.962 13:28:47.0939 19/07/2012 11.49.53.231 13:28:48.0249 19/07/2012 11.49.53.752 13:28:48.0249 19/07/2012 11.49.53.752 13:28:48.0749 19/07/2012 11.49.53.772 13:28:48.0749 19/07/2012 11.49.53.772 13:28:48.0749	-VB(06792)- Praim-ThinOX - Imprivata OneSign Agent Versi -VB(06792)- InitInstance(login) -VB(06792)- DeleteCredentials() -AP(06792)- CProveIDApi::Init(https://192.168.23.22) -AP(06792)- CProveIDApi::SelectServer selected https://c -AP(06792)- CProveIDApi::ServersDomainsModalities -AP(06792)- CProveIDApi::PostMethod(Multi) -AP(06792)- CProveIDApi::InitCurl(Multi) -AP(06792)- CProveIDApi::ParseServers status 200 -AP(06792)- CProveIDApi::ParseDomains status 200 -AP(06792)- CProveIDApi::ParseModalities -VB(06792)- CProveIDApi::ParseModalities -VB(06792)- ScardEvent: event 2, eventpar 9b3af50 -VB(06792)- ScardEvent: event 1, eventpar 0012 -VB(06792)- OnScardMessage: other event 0012, id 0,"OMNI -VB(06792)- ScardEvent: event 1, eventpar 10012 -VB(06792)- ScardEvent: event 1, eventpar 10012	×
19/07/2012 11.49.53.832 13:28:48.0749	-VB(06792)- OnScardMessage: evento gestito con m_bScBusy	
	-	-
•		#

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.

🕑 Vmware View Options			
Client version			
Whware client	VMware options		
🔵 Praim API client	Praim options		
USB Redirection options			
USB Redirection Type: 💿 VMware	📃 Debug 🛛 info 🛛 🗹		
Praim (TCe-VDA agent required)			
Force USB Redirection disable (override server setting)			
Enable Redirection of already connected devices			
RDP options			
*	Rdp Options		
	OK Cancel		

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".

🗞 Vmware View Client Options 🛛 🔀
Close Desktop library window at VD logoff/disconnect
VMware Kiosk mode (Vmware client)
Enable Smart Card Login
🔽 Show Top bar
Bitmap Cache size (MB): 30 (min 50MB, max 300MB)
Enable FIPS PCoIP encryption
SSL Verification Mode Import CA certificate
OK Cancel

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



Praim View Client Options Single Sign On Options Enabled Dischool		
Disabled Disabled if Smart Card Present		
Window Mode Options Preferred Window Mode: Fullscreen Custom Window size: Width: 800 Height: 600		
Connection Options Image: Connection Options Image: Option Option Options Image: Option Option Option Options Image: Option		
Authentication Options		
USB Redirection Options Startup delay between USB red. and Rdp/PCoIP (ms): 1000		
OK Cancel		

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".

2	VMware View Client - Edit Session
۲	CA Certificates
	certificate full path in the edit box below. Then
	/mnt/media/NO_NAME
	Cancel
	192-168-4-10.cer
	CA Certificate file name:
	/mnt/media/NO_NAME/192-168-4-10.cer

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.

🕒 XenDesktop Options 🗖 🐱
USB Redirection
Enable USB Redirection
Enable Praim USB Redirection (needs TCe-VDA agent)
Enable Citrix HDX USB Redirection
OK Cancel

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.



Terminal Prope	rties					
General Netwo	ork User Inter	face Firmware	e Security F	Printers Contro	l Panel	
802.1x Port-based Authentication	SNMP Agent	Imprivata OneSign	PCSC Server	Cisco VPN Client	MultiMedia Codecs	
Aladdin eToken PRO	RDP Gobal Settings	Citrix HDX USB Redirection	Je Kantan	Network File system	Remote Assistance	
Ica Global Settings	Sound Configuration	近 Java Cache	Date & Time	Vmware View USB	Provision AppPortal	
Citrix XenApp Agent	Praim USB Redirect Client	얱 ThinMan				
		ОК		Cancel	Apply	

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



Terminal Properties
General Network User Interface Firmware Security Printers Control Panel
Import Client ICA - Global Properties Import Preferences ICA Client configuration files ICA Client configuration files Edit wfclient.ini Add Certificate Edit module.ini Force Window Manager to report Working Area (reboot) Working Area (reboot) Edit All_Regions.ini Mouse Sends Control-V HDX Features PointerClickTime: ms WebCam FrameRate Font Smoothing Type: None Prov OK Cancel
OK Cancel Apply

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

🕑 Choose the Certificate File	
/tmp/mnt/NO_NAME/192-168-4-10-B64.cer	
./ 192-168-4-10-B64.cer ■ Preview	BEGIN CERTIFICF MIIEq.jCCA5KgAwIBAgIG MRMwEQYKCZImiZPyLGQB MRMwEQYDVQQDEwpWY1N1 NDk1M1owRTETMBEGCgmS aS10ZXNOMTETMBEGA1UE ggEPADCCAQoCggEBAJ12 g+sI1u7n25X+kdtXYN7F zq474+aJIuheTfQMEIY> Vv2ah5s0zvfjCzDYqi6M +3uv11nxuEBBPmwKyCgz OgHJLUNztimppItdtw0F AQQBgjCUAgQGHgQAQwBB A1UdDgQWBBRwvXaz45FN 8KCB7YaBuGxkYXA6Ly8v ONPOLENOPVR1VmvnVulk
[OK /- Cancel



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.

🌐 ThinMan Local Console - Platinum Edition - [ThinManRoot] - [ThinManRoot] - [ThinManRoot]					
File Modify Tools View Info					
6 2 3 🖓 🖓					
	Remote Assistance	Type			
	Connections				
T_300C9/	Configurations	Receive (Ctrl+R)			
	Firmware Update	Send (Ctrl+S)			
T_42F1ED	Power On/Off	Import from other Device			
	Special Functions	Import from Template			
	Add Scheduled Activity	Export to Template			
XT_42F4DA	Move To	Active Praim USB Redirection			
XT_3A77D3	Delete Canc	c Factory Default			
XT_3D1746	Refresh F5				
📙 XT_42E779	Edit Notes				
₩ XT_45E5A3	Properties F2	2			
Test 02	mag ∧1_/1200				
Receive the current configuration from device XT_403C8D - IP: 192.168.0.203 - Ver. 8.4.22 - Model: XT9200-C - MAC: 00E0C5403C8D Devices:					

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.



🔋 ThinMan Local Console - Platinum Edition - [ThinManRoot] - [ThinManRoot] - [ThinManRoot]					
File Modify Tools View	File Modify Tools View Info				
🔊 💈 🌶 🏹	🐑 🖻 🍺 🛃 🕶 🔟 🔟 🚟 🐺 📼 🔎				
	Remote Assistance	•	Туре		
🛼 XT_3D0679	Connections				
XT_3D0C94	Configurations	•	Receive (Ctrl+R)		
→ XT_42126B	Firmware Update		Send (Ctrl+S)		
XT_42F1ED	Power On/Off	×	Import from other Device		
	Special Functions	•	Import from Template		
	Add Scheduled Activity	+	Export to Template		
📕 XT_42F4DA	Move To		Active Praim USB Redirection		
🗽 XT_3A77D3	🔓 XT_3A77D3 Delete Canc Factory Default	Factory Default			
XI_3A//DC	Refresh	F5			
🛴 XT_42E779	Edit Notes				
	Properties	F2			
XI_/F536E	-		J		
Receive the current configuration from device XT_403C8D - IP: 192.168.0.203 - Ver. 8.4.22 - Model: XT9200-C - MAC: 00E0C5403C8D Devices:					

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.