

Installation Guide

SigIDp-R

Contents

Introduction	2
Installation	2
SigIDp-R Installation	
SigPlus Installation	2
Setup USB Redirection Rules on Citrix Server	3
Setup Procedure on VDA	5
Test Programs	б
SigIDp-R Test	б
SigPlus Test	б

Introduction

Topaz ID pads are bundled with SigIDp-R electronic fingerprint software tools for high-quality, high-resolution fingerprint images and the capture and verification of digital fingerprints.

Follow the steps below for local installation, as well as for Citrix XenDesktop (7.15 and above) environments with the Virtual Delivery Agent (7.15 and above) installed on virtual desktop and server.

Installation

SigIDp-R Installation

After downloading SigIDp-R from <u>www.topazsystems.com/sdks/sigidp-r.html</u>, run the EXE to install the SigIDp-R ActiveX and the fingerprint drivers. A system reboot is required after SigIDp-R installation.

Note: If a Citrix Session will be used, install the Citrix Workspace App, also known as Citrix Receiver.

SigPlus Installation

After downloading SigPlus from <u>www.sigpluspro.com</u>, there is no reboot required. See below for a list of Topaz biometric ID pads and their corresponding SigPlus installation models:

ID Model Number	SigPlus Installation Model
TF-LBK463	T-L(BK)460
TF-S463	T-S460
TF-LBK464	T-L(BK)462

If you are setting up the biometric ID signature pad for a local, standalone application, proceed to the section "<u>Test Programs</u>" below. If you are interested in running a virtualized desktop or application on Citrix XenApp or XenDesktop, continue with the steps below.



Setup USB Redirection Rules on Citrix Server

1. Log-in to the server where Citrix Studio is installed and launch the Citrix Studio. Select "Create Policy" from the Actions panel.

Ħ	Citrix Studio		X
File Action View Help			
 Console Root Citrix Studio (XenDesktop77) Search Machine Catalogs 	CITRIX Policies Templates Comparison	Modeling	Actions Policies
 Delivery Groups Policies Logging Configuration 	Policies	Unfiltered	View View View View View View View View
 Administrators Controllers Hosting ↓ Licensing StoreFront App-V Publishing Ones Intrix StoreFront 	1 Unfiltered	Overview Settings Assigned to This policy has no configured settings by default. Edit the policy to view and configure settings.	Unfiltered Edit Policy Disable Policy Edit Save as Template E Help

2. When the "Create Policy" dialog appears, enter "USB" in the search text box; the settings window shows all the USB related policies:

	Create Policy	
Studio	Select settings	
	(All Versions) All Settings USB	×
	Settings: 0 selected	View selected only
Settings Users and Machines	 Client USB device optimization rules User setting - ICA\USB Devices Not Configured (Default:) 	<u>Select</u>
Summary	Client USB device redirection User setting - ICA\USB Devices Not Configured (Default: Prohibited)	<u>Select</u>
	 Client USB device redirection bandwidth limit User setting - ICA\Bandwidth Not Configured (Default: 0 Kbps) 	Select
	 Client USB device redirection bandwidth limit percent User setting - ICA\Bandwidth Not Configured (Default: 0) 	Select
	 Client USB device redirection rules User setting - ICA\USB Devices Not Configured (Default:) 	Select
	 Client USB Plug and Play device redirection User setting - ICA\USB Devices Not Configured (Default: Allowed) 	Select
	Back	Cancel

3. Press "Select" on the Client USB device redirection. The Edit Setting dialog appears; select the "Allowed" radio button, and then click "OK".



4. Click "Select" on the "Client USB device redirection rules". Click "Add" to create new entries for Topaz Signature pad and fingerprint device. Click "OK" to end this dialog. The following dialog shows Topaz Signature pad and fingerprint devices entered as an example.

alues:	
Allow: VID=06A	\& PID=0043 #Topaz HSB TLBK462/463
Allow: VID=05B	A PID=000A #U.are.U 4500 fingerprint reader
<u>A</u> dd	ue:
Add Use default val Applies to the Virtual Delivery Server OS. 7.5	ue: following VDA versions r Agent: 5.6, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Desktop OS, 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8
<u>A</u> dd Use default val Applies to the Virtual Delivery Server OS, 7.5 Server OS, 7.8 Server OS, 7.12 7.15 Server OS	ue: following VDA versions / Agent: 5.6, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Desktop OS, 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Desktop OS,

Note: The above setting applies for Windows desktop VDAs, such as Windows 11, 10 and 8.1. For Windows Server 2016, 2029 and 2022 VDAs, USB redirection should be denied for the fingerprint reader because there will be a virtual channel established instead:

+ Add	
Value:	
Allow: VID=06A8 PID=0043 # Topaz HSB	
Allow: VID=06A8 PID=0057# Topaz HSB	
Deny: VID=05BA PID=000A # <u>Uare.U</u> 4500	
Use default value:	

Change - Allow: VID=05BA PID=00A to Deny: VID=05BA PID=00A #U.are.U 4500 fingerprint reader in instructions above.

5. Edit "Client USB device optimization rules"; add the Topaz signature pad device into the table for mode set to 4, capture mode.

Client USB device optimization rules	
<u>V</u> alues:	
Mode=00000004 VID=06A8 PID=0043 class=3 #Topaz HSB TLBK462/463	$ \uparrow$ \downarrow

6. Once policies are setup, click "Next" to continue.



- 7. On the "Users and Machines" dialog, select "All objects in the site". Then, click "Next".
- 8. In the Summary dialog, give the Policy a name (for example, "USBPolicy2"). Check the "Enable policy" box, and then click "Finish".
- 9. Then, make the newly created "USB Policy2" higher than any other policy.

Important Step for Citrix VDA 2203 and above:

- 1. Edit "Virtual channel allow list" from policy setting.
- 2. Select "the Disabled" radio button.

Setup Procedure on VDA

The below steps show use of a browser to access the Citrix StoreFront web:

- 1. By double-clicking the group, the VDA will launch. If the group icon is spinning, please check the Citrix Server and restart the Citrix Desktop Service.
- 2. The virtual desktop will display on your system; the Citrix Receiver or Workspace may pop up a dialog to show all of the USB devices on the client machine available for USB redirection.

Citrix Receiver	×
Choose the devices you want to connect to your virtual session	
Unknown HID Device (Vid06A8 Pid0043)	
DigitalPersona, Inc. U.are.U® 4500 Fingerprint Reader	
	_
Connect Cancel	

3. Check the "Unknown Signature Pad (Vid06A8 Pid0043)" item, then click "Connect". If on Windows 10, check the DigitalPersona, 4500 Fingerprint Reader.

Note: For the Windows Server version VDAs 2016, 2019, 2022 and XenApp server, don't check the "Digital Persona" entry. The client/server connection will be established through a virtual channel.

∇

Test Programs

SigIDp-R Test

Launch the SigID Test program. On the QueryStatus button, it will display green if the fingerprint device is detected.

SigID Test Program Capture and Validate Capture - getfingerprintstring Capture - getfingerprintfile Validate - from String Validate - from file	Verification Set Identification Ringerprint V Reset Users
Create FP image Create Bmp Create Bmp Create Jpg Create Jpg Create Tiff Create Tiff	Bmp String Get Bmp String> Set Bmp String File Get Bmp Bytes Burn With
SetWindowPosMoe: AUTOMATIC (0) GetDialogDelay GetDialogDelay	Bmp Write BmpWrite APIs BmpWriteLowRes APIs BmpWriteLowRes APIs

SigPlus Test

Launch the DemoOCX program. Click "Start" and sign on the Topaz signature pad. The signature will appear in the signature area.