



Installation Guide

SigIDp-R

Contents

Introduction	2
Installation	2
SigIDp-R Installation.....	2
SigPlus Installation	2
Setup USB Redirection Rules on Citrix Server	3
Setup Procedure on VDA	5
Test Programs	6
SigIDp-R Test.....	6
SigPlus Test.....	6



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 www.topazsystems.com/sdks/sigidp-r.html, 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 www.sigpluspro.com, there is no reboot required. See below for a list of Topaz biometric ID pads and their corresponding SigPlus installation models:

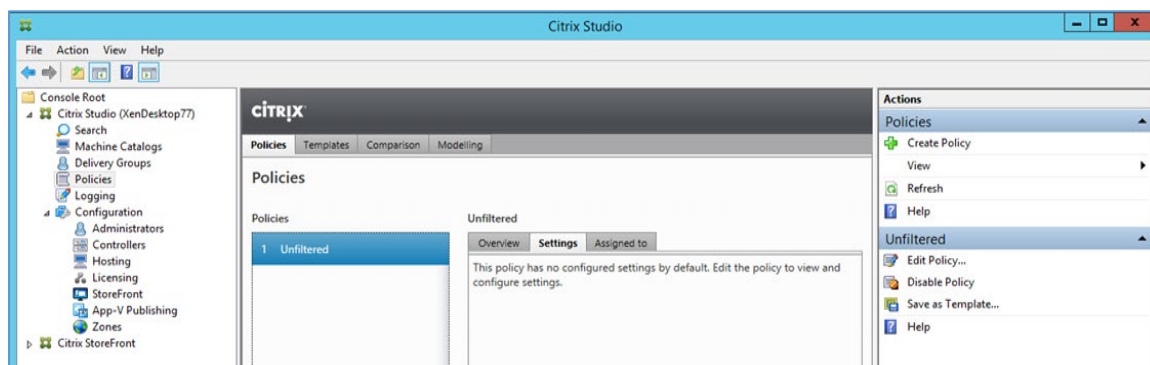
ID Model Number	SigPlus Installation Model
TF-LBK463	T-L(BK)460
TF-S463	T-S460
TF-LBK464	T-L(BK)462

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

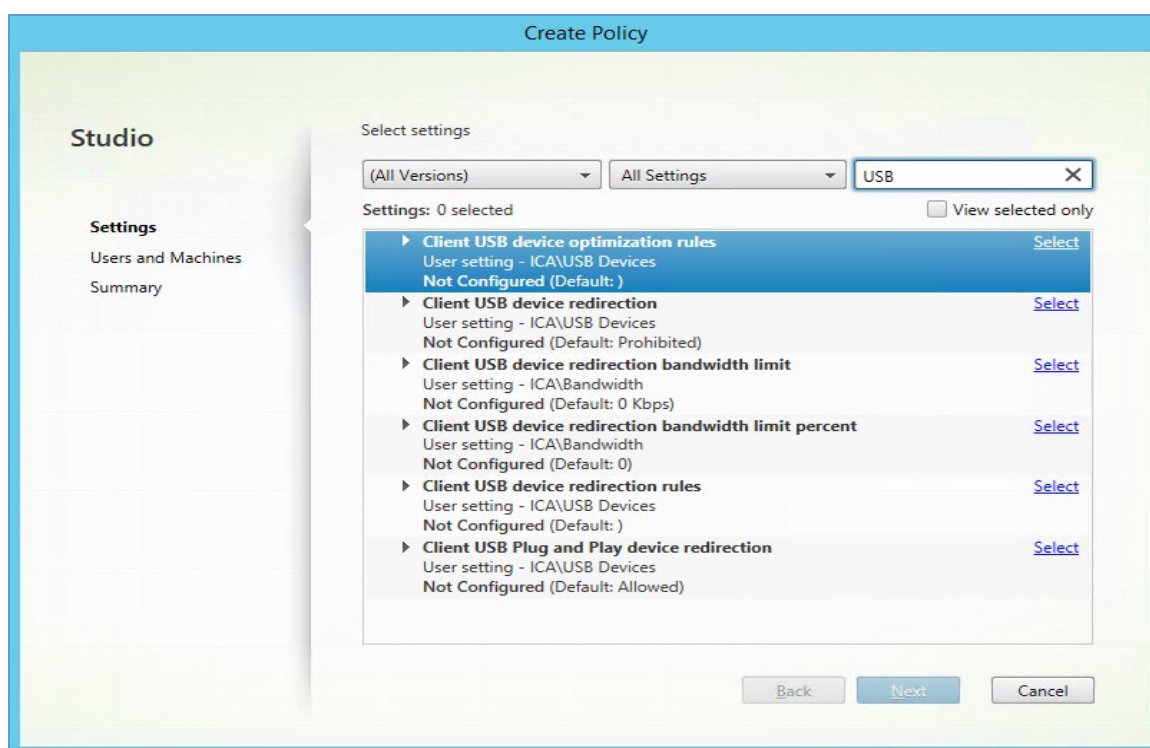


Setup USB Redirection Rules on Citrix Server

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



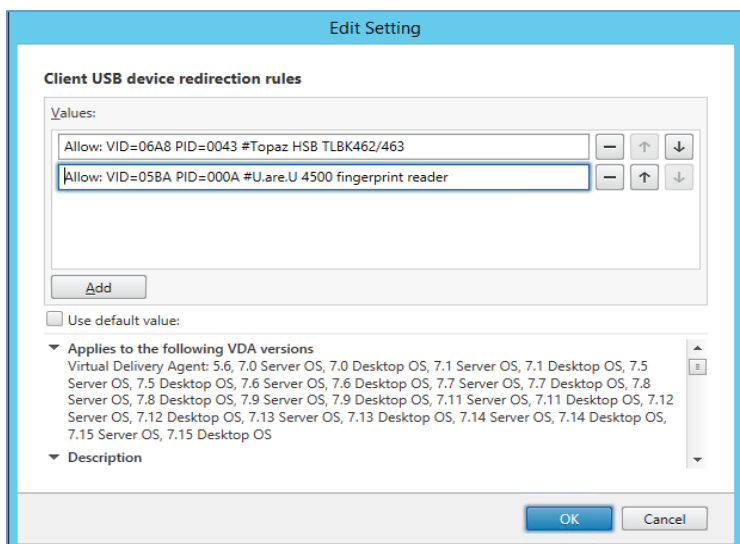
2. When the “Create Policy” dialog appears, enter “USB” in the search text box; the settings window shows all the USB related policies:



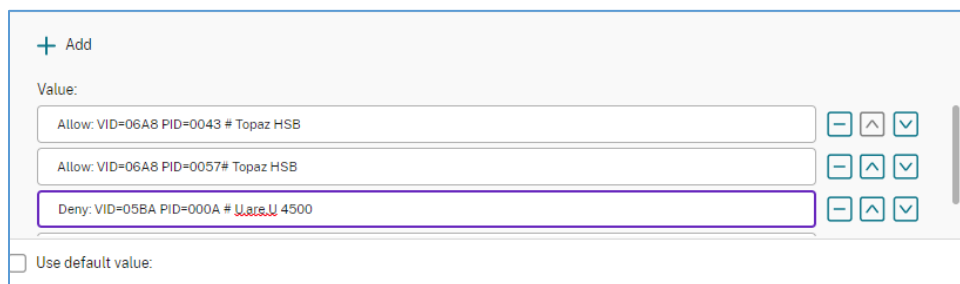
3. Press “Select” on the Client USB device redirection. The Edit Setting dialog appears; select the “Allowed” radio button, and then click “OK”.



- 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.

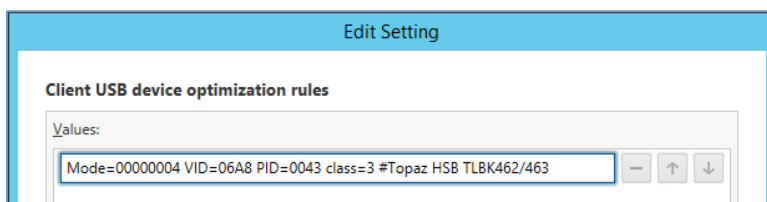


Note: The above setting applies for Windows desktop VDAs, such as Windows 11, 10 and 8.1. For Windows Server 2016, 2029 and 2022 VDAs, USB redirection should be denied for the fingerprint reader because there will be a virtual channel established instead:



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

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



- 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.

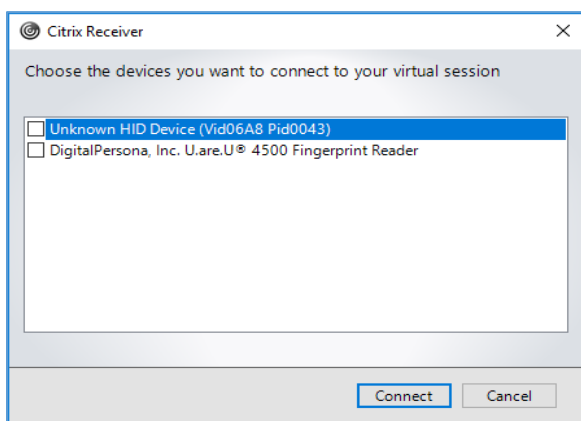
Important Step for Citrix VDA 2203 and above:

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.



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

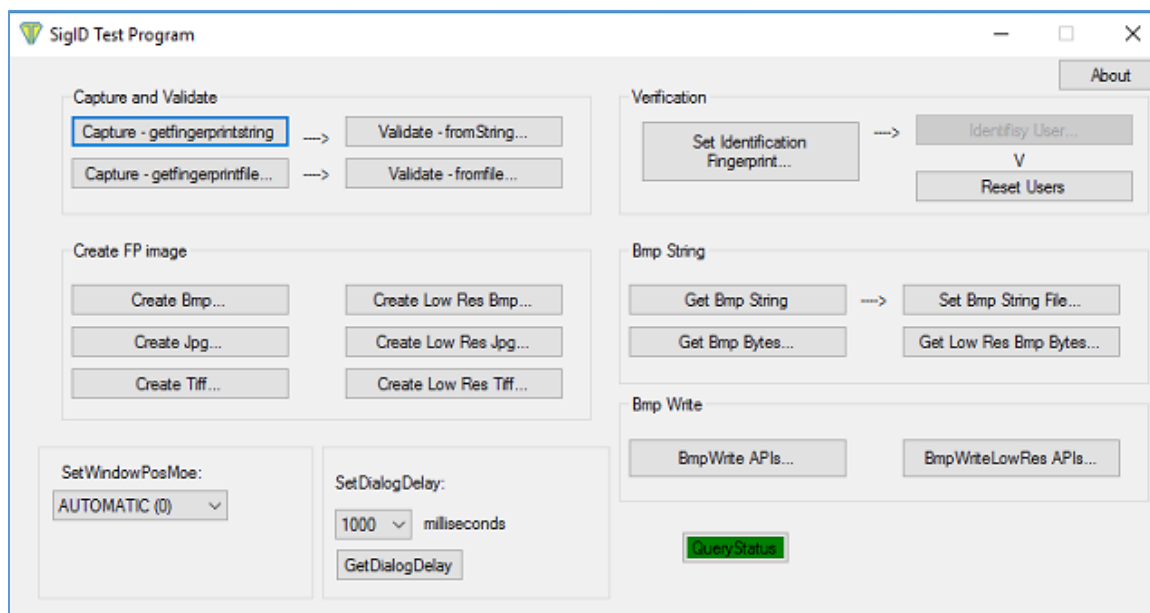
Note: For the Windows Server version VDAs 2016, 2019, 2022 and XenApp server, don’t check the “Digital Persona” entry. The client/server connection will be established through a virtual channel.



Test Programs

SigIDp-R Test

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



SigPlus Test

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