Using Imprivata OneSign with PCoIP Zero Clients Deployment Guide

TER1204004

Issue 1

Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada
p +1 604 451 5800 f +1 604 451 5818
www.teradici.com

The information contained in this document represents the current view of Teradici Corporation as of the date of publication. Because Teradici must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Teradici, and Teradici cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. TERADICI MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Visit http://www.teradici.com/teradici/pat.php for more information.

Revision History

Version	Date	Description
1	May 16, 2012	Document created.

Contents

Table of Figures

1 Introduction

PCoIP® zero clients are ultra-secure, easily managed devices offering the richest user experience in a VMware View environment. With no hard drive or application operating system, PCoIP zero clients are stateless hardware devices that require the least amount of management as there are no virus or new video codecs to update. PCoIP zero clients are also available in a variety of form factors, such as standalone desktop devices, integrated monitors, touchscreen displays, and IP phones.

You can further simplify your large zero client deployments by using the PCoIP® Management Console from Teradici® for your configuration and management needs.

For more information, visit http://www.pcoip.com/zeroclient or access the Teradici Knowledge Base and downloads site at techsupport.teradici.com.

1.1 Overview

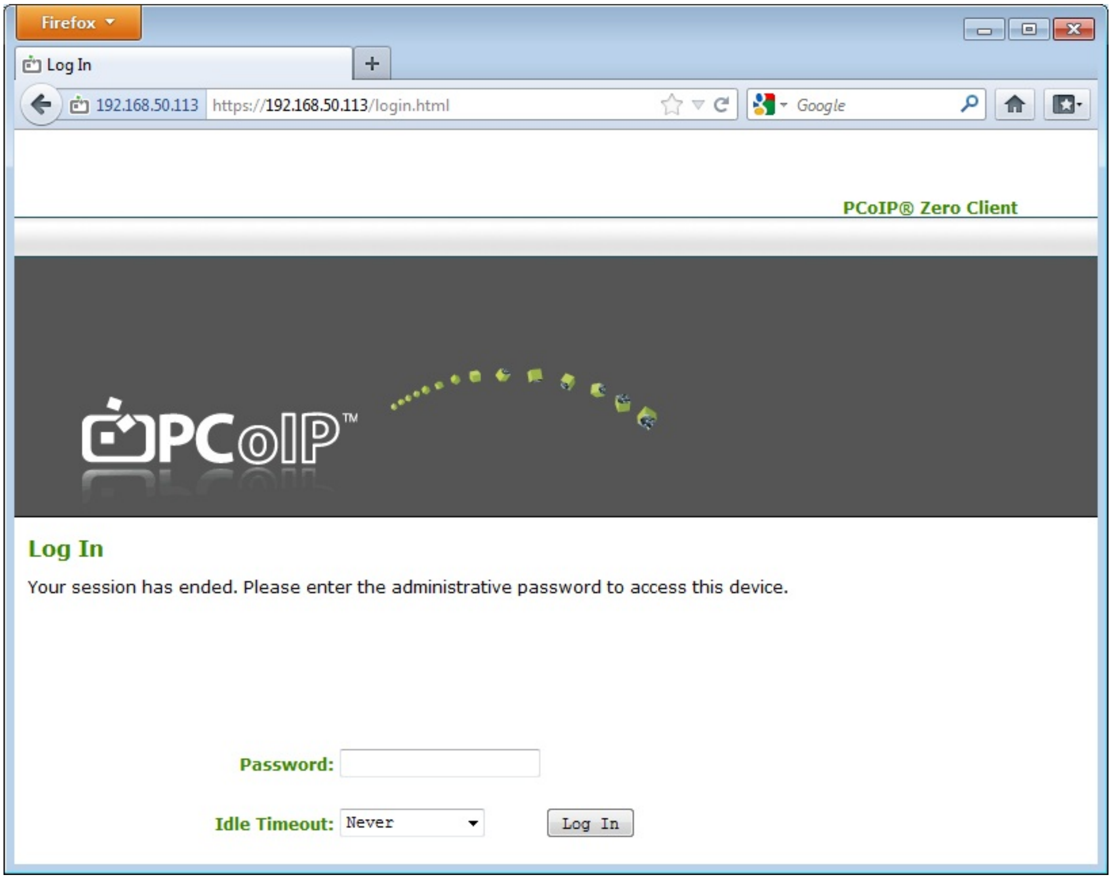
This document shows the steps involved in setting up the OneSign 4.6 within the PCoIP zero client environment. To complete the setup process, you need to:

- Update the zero client with the latest Teradici firmware. See page 8.
- Configure the PCoIP zero client to recognize OneSign. See page 10.
- Configure OneSign to recognize the PCoIP zero client. See page 12.
- Deploy the OneSign agent on the virtual desktop. See page 15.

2 Update the Zero Client with the Latest Firmware

To upload the latest firmware to the zero client, use the Teradici Administrative Web Interface (AWI). The AWI lets you interact remotely with the device through a web browser.

1. To access the AWI, open a web browser to https://<zero client IP Address>.
2. From the **Log In** page, enter your password if requested. (Note that not all zero clients need a password.)



Log In

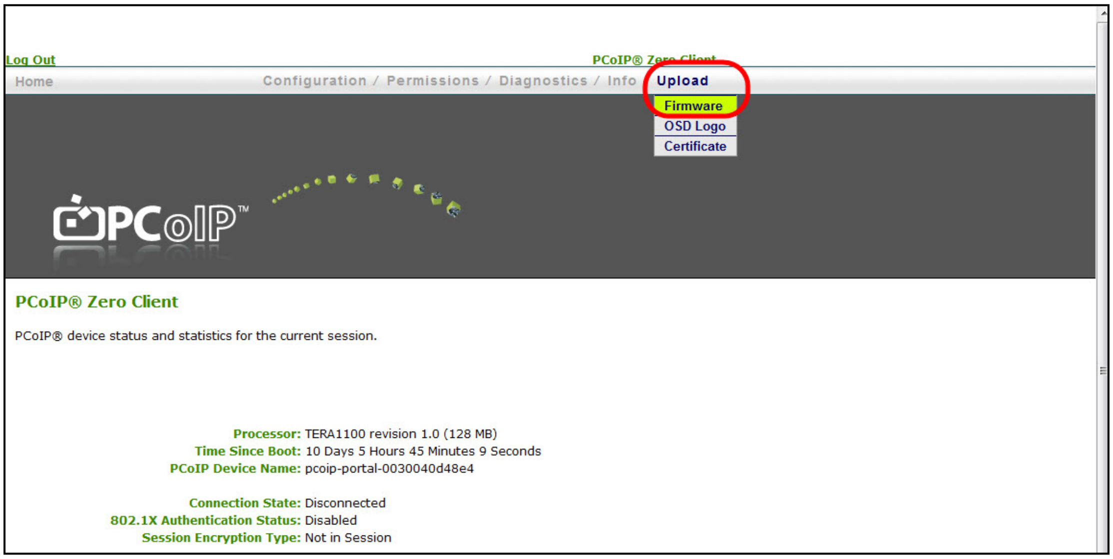
Your session has ended. Please enter the administrative password to access this device.

Password:

Idle Timeout: Never

Figure 1: Log into the Administrator Web Interface (AWI) for the Zero Client

3. From the **Upload** menu, select **Firmware**.



PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

Processor: TERA1100 revision 1.0 (128 MB)
Time Since Boot: 10 Days 5 Hours 45 Minutes 9 Seconds
PCoIP Device Name: pcoip-portal-0030040d48e4

Connection State: Disconnected
802.1X Authentication Status: Disabled
Session Encryption Type: Not in Session

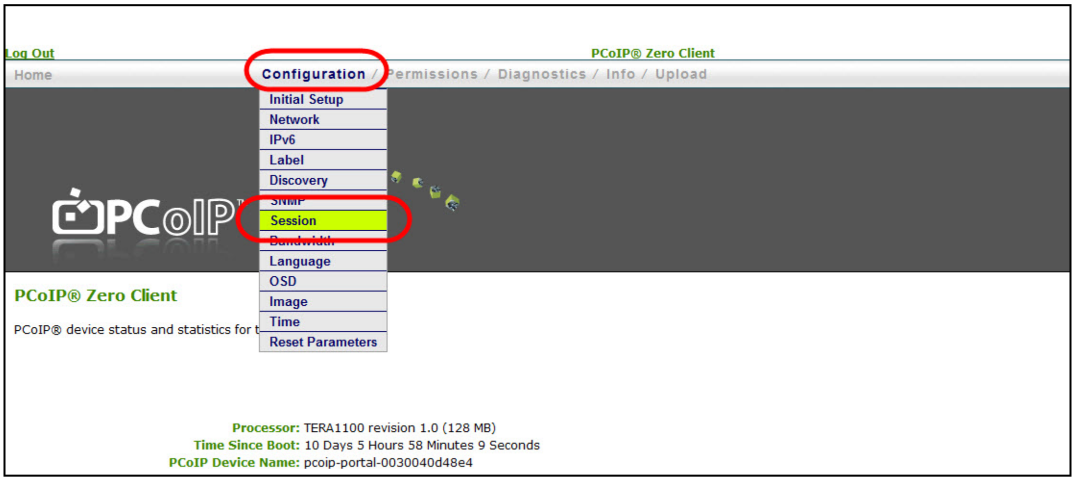
Figure 2: Firmware Upload Page

4. From the **Firmware Upload** page, browse to the firmware ".all" file.
5. Click **Open**.
6. Click **Upload**.
7. Click **OK** to confirm that you want to proceed with the upload. When the firmware upload completes, you must reset the device for the changes to take effect.

3 Configure the PCoIP Zero Client to Recognize OneSign

After uploading the firmware, you can set up the zero client for Imprivata OneSign support. You can use either the zero client AWI or the zero client On Screen Display (OSD).

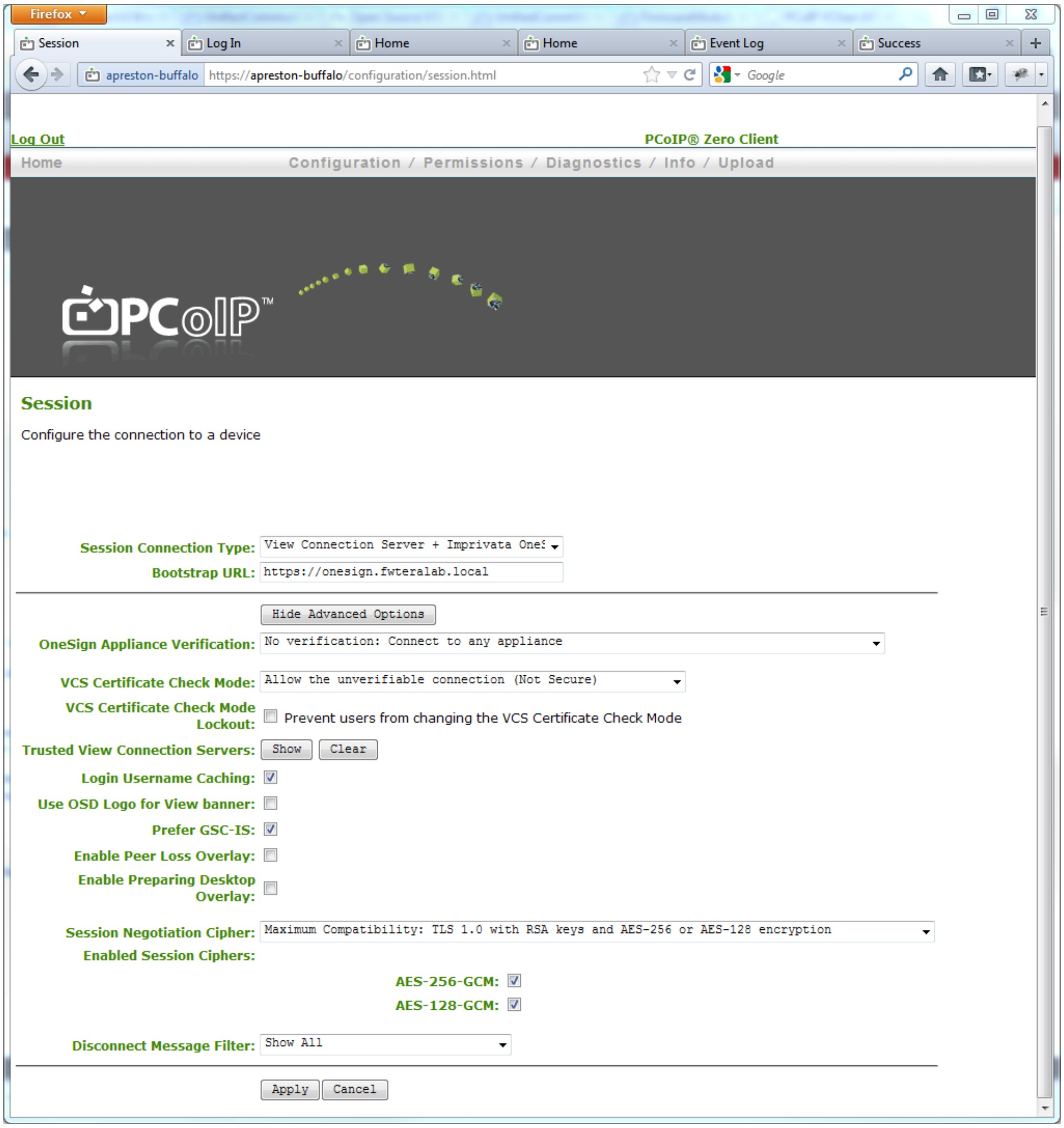
1. Access the AWI of the zero client that you want to connect to OneSign.
2. From the **Configuration** menu, select **Session**.



Processor: TERA1100 revision 1.0 (128 MB)
Time Since Boot: 10 Days 5 Hours 58 Minutes 9 Seconds
PCoIP Device Name: pcoip-portal-0030040d48e4

Figure 3: Select the Session Option from the Configuration Menu

3. In the **Session Connection Type** field, select **View Connection Server + Imprivata OneSign**.
4. In the **Bootstrap URL** field, enter the URL of the OneSign Server.
5. (Optional) For a better user experience, under **Advanced Options**, **set Disconnect Message Filter** to **Show None**.
6. Configure the session settings. For more information about each of the options on the **Session** page, see the TER0606004 *PCoIP Administrator's Guide*. For specific details on the **VCS Certificate Check Mode** and **VCS Certificate Check Mode Lockout** settings, see Teradici Knowledge Base #1020. For specific details on the **OneSign Appliance Verification** setting, see Teradici Knowledge Base #1048


Firefox
Session
Log In
Home
Home
Event Log
Success
apreston-buffalo
https://apreston-buffalo/configuration/session.html
Google
Log Out
PCoIP® Zero Client
Home
Configuration / Permissions / Diagnostics / Info / Upload
PCoIP™

Session

Configure the connection to a device

Session Connection Type: View Connection Server + Imprivata OneS

Bootstrap URL: https://onesign.fwteralab.local

Hide Advanced Options

OneSign Appliance Verification: No verification: Connect to any appliance

VCS Certificate Check Mode: Allow the unverifiable connection (Not Secure)

VCS Certificate Check Mode Lockout: □ Prevent users from changing the VCS Certificate Check Mode

Trusted View Connection Servers: Show Clear

Login Username Caching: ☑

Use OSD Logo for View banner: □

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

Apply Cancel

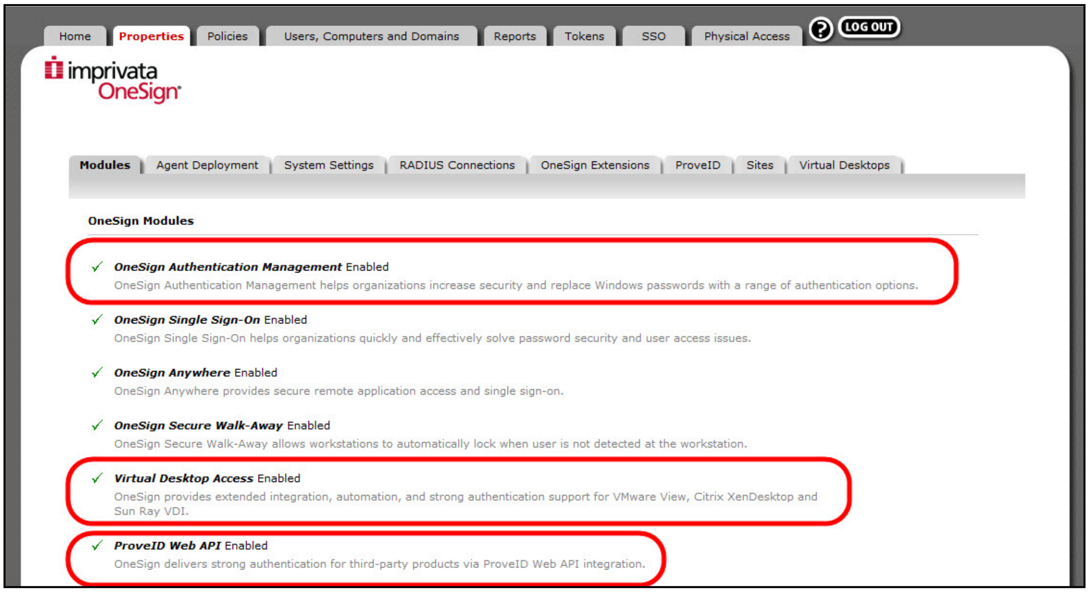
Figure 4: Configure the Session Settings

7. Click **Apply** to save the settings.

4 Configure OneSign to Recognize the PCoIP Zero Client

Within OneSign, you must configure policy to enable the zero client integration. Policy determines the workflow the user experiences with VMware View, as well as configuration settings for the View connection broker itself.

1. Open the OneSign Administrator in an Internet Explorer browser window at: https://<Appliance IP address>/SSO/login.html
2. From the **Properties** page, select the **Modules** tab. Make sure you have three licenses installed:
   - OneSign Authentication Management
   - OneSign VDA
   - OneSign ProveID Web (this is free of charge, but it must be requested from Imprivata)



OneSign Modules

✓ ***OneSign Authentication Management*** Enabled
OneSign Authentication Management helps organizations increase security and replace Windows passwords with a range of authentication options.

✓ ***OneSign Single Sign-On*** Enabled
OneSign Single Sign-On helps organizations quickly and effectively solve password security and user access issues.

✓ ***OneSign Anywhere*** Enabled
OneSign Anywhere provides secure remote application access and single sign-on.

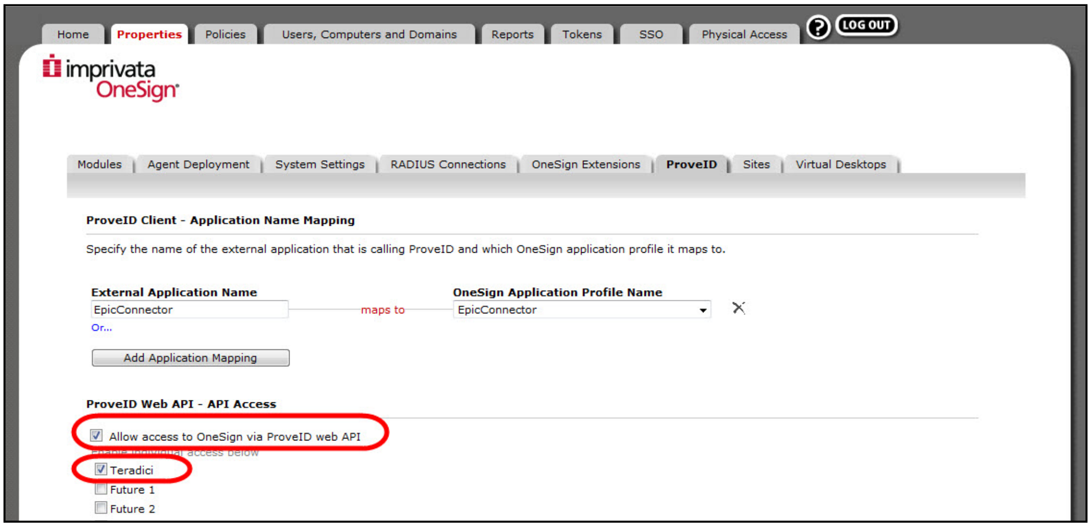
✓ ***OneSign Secure Walk-Away*** Enabled
OneSign Secure Walk-Away allows workstations to automatically lock when user is not detected at the workstation.

✓ ***Virtual Desktop Access*** Enabled
OneSign provides extended integration, automation, and strong authentication support for VMware View, Citrix XenDesktop and Sun Ray VDI.

✓ ***ProveID Web API*** Enabled
OneSign delivers strong authentication for third-party products via ProveID Web API integration.

Figure 5: Check Your OneSign Licenses

3. Select the **ProveID** tab, and then enable **Allow access to OneSign via ProveID Web API and Teradici** under **ProveID web API - API Access**.



ProveID Client - Application Name Mapping

Specify the name of the external application that is calling ProveID and which OneSign application profile it maps to.

External Application Name		OneSign Application Profile Name
EpicConnector	maps to	EpicConnector
Or...		

ProveID Web API - API Access

☑ Allow access to OneSign via ProveID web API

Enable individual access below

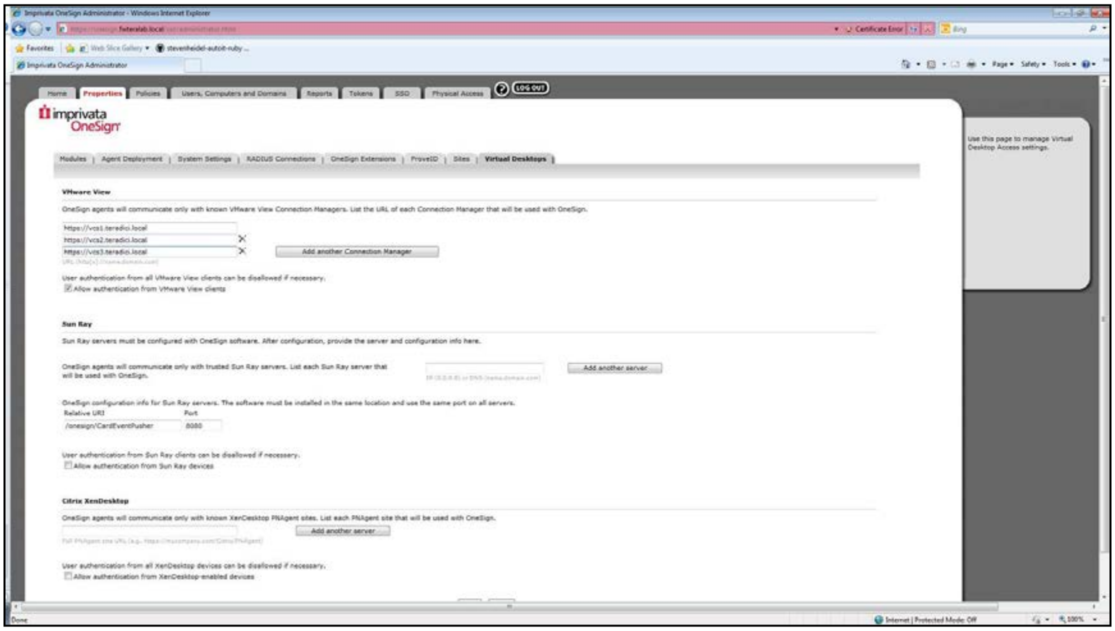
☑ Teradici

□ Future 1

□ Future 2

Figure 6: Enable the ProveID Teradici Option

4. Click **Save**.
5. Select the **Virtual Desktops** tab, and then add your VMware View connection broker as shown next. Enable the box to A**llow authentication from VMware View clients**.



Use this page to manage Virtual Desktop Access settings.

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://vcs1.teradici.local

https://vcs2.teradici.local

https://vcs3.teradici.local

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.

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

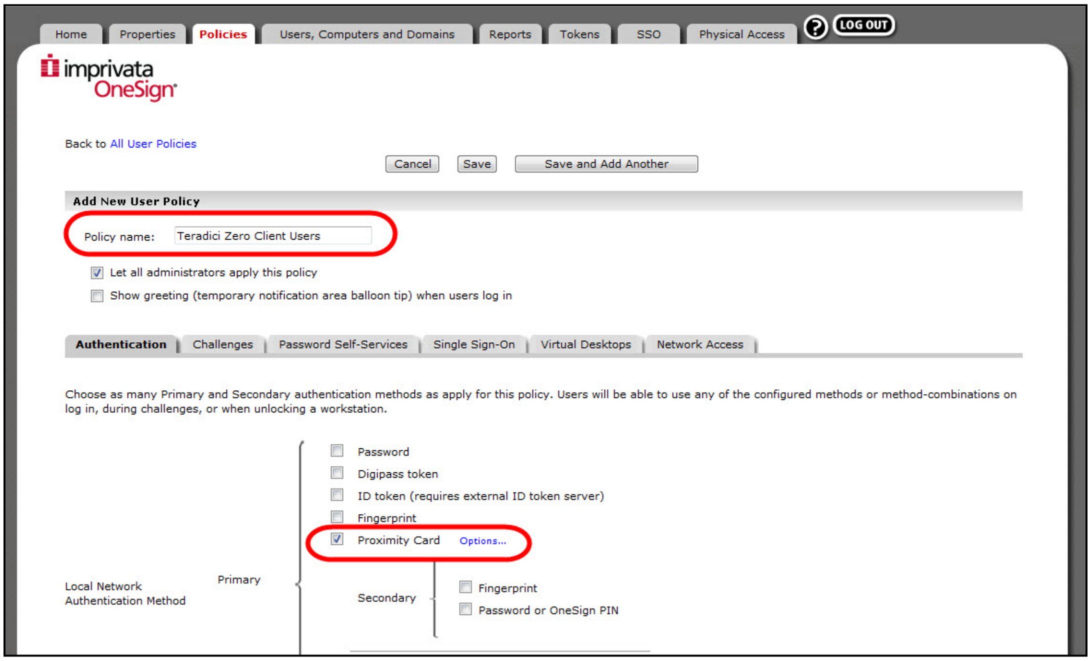
OneSign agents will communicate only with known XenDesktop PNAgent sites. List each PNAgent site that will be used with OneSign.

User authentication from all XenDesktop devices can be disallowed if necessary.

□ Allow authentication from XenDesktop-enabled devices

Figure 7: Add your VMware View Connection Broker

6. Click **Save**.
7. From the **Policies** page, select the **User Policies** tab. Make sure that user policies for PCoIP zero client users allow proximity card authentication.



Add New User Policy

Policy name: Teradici Zero Client Users

☑ Let all administrators apply this policy

□ Show greeting (temporary notification area balloon tip) when users log in

Choose as many Primary and Secondary authentication methods as apply for this policy. Users will be able to use any of the configured methods or method-combinations on log in, during challenges, or when unlocking a workstation.

Local Network Authentication Method

Primary

□ Password
□ Digipass token
□ ID token (requires external ID token server)
□ Fingerprint
☑ Proximity Card

Secondary

□ Fingerprint
□ Password or OneSign PIN

Figure 8: Configure a User Policy for Zero Client Users

5 Deploy the OneSign Agent on the Virtual Desktop

To deploy the OneSign Agent to the virtual desktop:

1. Make sure that View Agent is installed on the virtual desktop. For environments using OMNIKEY proximity card readers, make sure that View Agent is installed with the **PCoIP Smart Card** component disabled.
2. Establish a session with the virtual desktop using an account with administrator privileges.
3. Log on to the OneSign Administrator.
4. From the **Properties** tab, select the **Agent Deployment** tab.
5. Download the appropriate 32 or 64 bit version of the OneSign Agent for installation within the Windows virtual desktop or virtual desktop image.
6. Install the OneSign Agent within the virtual desktop.
7. Set the RedirectionSupported registry key data value to 1 (DWORD) and base Hexadecimal. This can be found under:
   - **Windows 7 64-bit**: HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/SSOProvider/DeviceManager
   - **Windows XP or 7 32-bit:** HKEY_LOCAL_MACHINE/SOFTWARE/SSOProvider/DeviceManager
8. To prevent simultaneous RFideas reader access by two OneSign processes, set the RemoteOnly registry key data value to 1 (DWORD) and base Hexadecimal. This can be found under:
   - **Windows 7 64-bit**: HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/SSOProvider/DeviceManager**Windows XP or 7 32-bit:** HKEY_LOCAL_MACHINE/SOFTWARE/SSOProvider/DeviceManager
9. Reboot the virtual desktop.
10. Deploy to a VMware View pool as necessary.
11. To test this setup, authenticate with a proximity card or password via the OneSign interface on the zero client.