TECH BRIEF

Using the PCoIP Zero Client in a OneSign 4.6 Environment

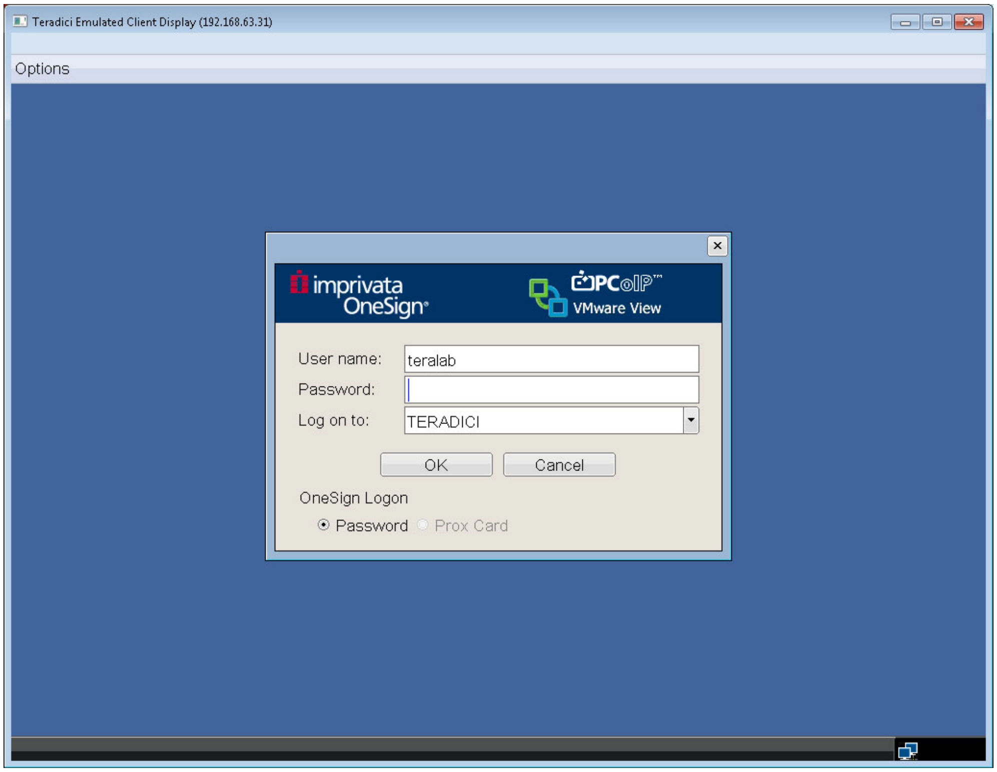
PCoIP® zero clients are ultra-secure, easily managed devices offering the richest user experience in a VMware View™ environment. With no hard drive, and no x86 or Linux operating system, PCoIP zero clients are stateless hardware devices that require the least amount of management as there are no virus or new video codecs to update.

PCoIP zero clients are available in a variety of form factors, including standalone desktop devices, integrated monitors, touchscreen displays, and IP phones. Deployments can be further simplified by using the PCoIP® Management Console from Teradici® to configure and manage large zero client deployments.

For more information, visit www.pcoip.com/zeroclient or access the Teradici knowledgebase and downloads site.

There are two stages to configuring a OneSign 4.6-PCoIP Zero Client environment:

- **Configuring OneSign Support for PCoIP Zero Clients**, in this document
- **Configuring the PCoIP Zero Client to Work with OneSign**



User name: teralab
Password:
Log on to: TERADICI

OneSign Logon
● Password ○ Prox Card

Logging into a PCoIP Zero Client

Configuring OneSign Support for PCoIP Zero Clients

There are three parts to configuring a OneSign 4.6-PCoIP Zero Client environment:

Setting Up the OneSign Environment to Support Zero Client Users on page 2

Creating and Assigning Policies on page 4

Deploying the OneSign Agent on the Virtual Desktop on page 6

Setting Up the OneSign Environment to Support Zero Client Users

Setting up a OneSign enterprise to support zero client users requires three OneSign licenses, the Teradici option enabled, a user policy to support zero client users, a computer policy for the zero clients, and a computer policy auto-assignment to ensure each zero client gets the right computer policy.

Setting up a OneSign enterprise to support zero client users requires.

Checking Your License Support on page 2

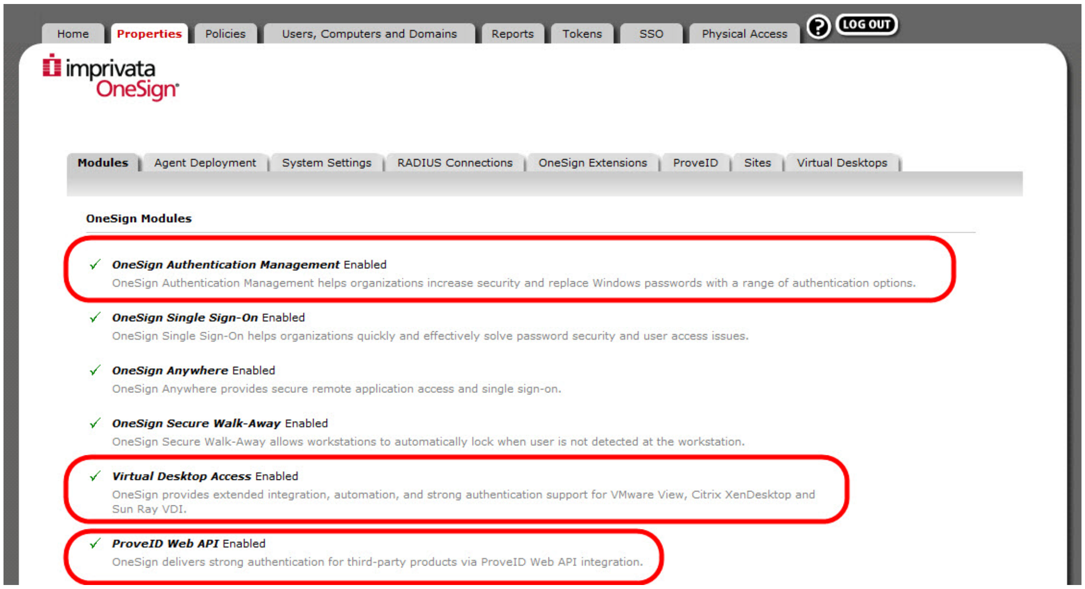
Enabling the ProveID Teradici Option on page 3

Configuring the VMware View Connection Managers in OneSign on page 3

Checking Your License Support

On the OneSign Administrator Properties page, Modules tab, be sure you have:

- OneSign Authentication Management
- Virtual Desktop Access
- ProveID Web API (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.

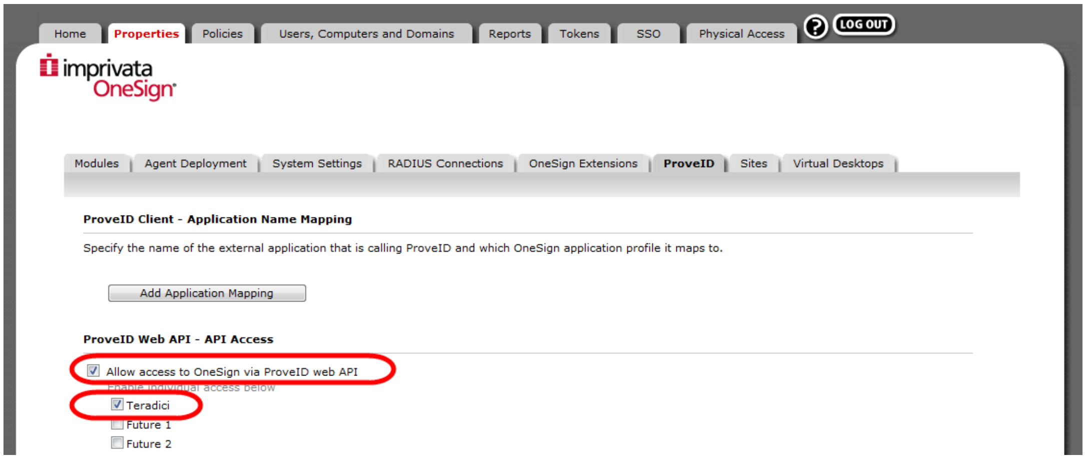
✓ ***ProveID Web API*** Enabled
OneSign delivers strong authentication for third-party products via ProveID Web API integration.

Check Your OneSign Licenses

Enabling the ProveID Teradici Option

The first step to setting up zero client support in your OneSign enterprise is to enable the Teradici option:

1. From the OneSign Administrator Properties page, ProveID tab, enable **Allow access to OneSign via ProveID Web API** and **Teradici** under ProveID web API - API Access and click **Save**.



ProveID Client - Application Name Mapping

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

ProveID Web API - API Access

☑ Allow access to OneSign via ProveID web API

Enable individual access below

☑ Teradici

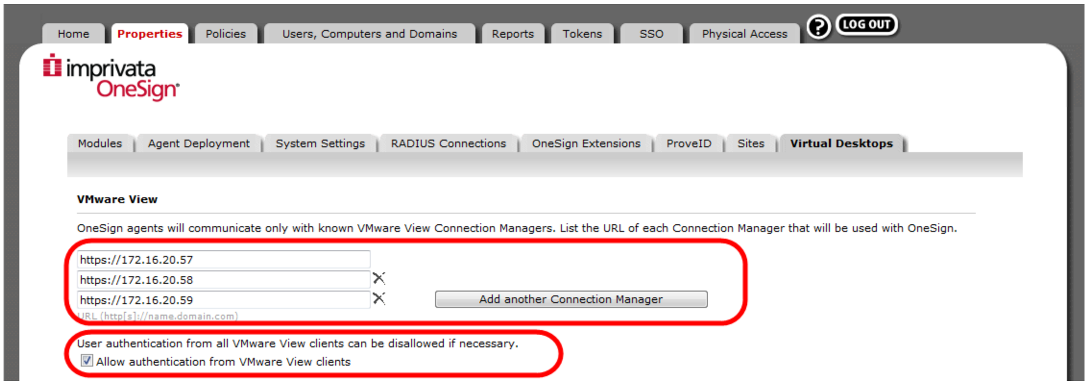
□ Future 1

□ Future 2

Enable the ProveID Teradici Option

Configuring the VMware View Connection Managers in OneSign

2. On the Properties page, Virtual Desktops tab, add your VMware View connection managers. Remember to enable the box to **Allow authentication from VMware View clients**.



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://172.16.20.57

https://172.16.20.58 ✕

https://172.16.20.59 ✕

URL (http[s]://name.domain.com)

User authentication from all VMware View clients can be disallowed if necessary.

☑ Allow authentication from VMware View clients

Add VMware View Connection Managers

The next step is to create user and computer policies for zero clients and their users. This is detailed in **Creating and Assigning Policies** on page 4.

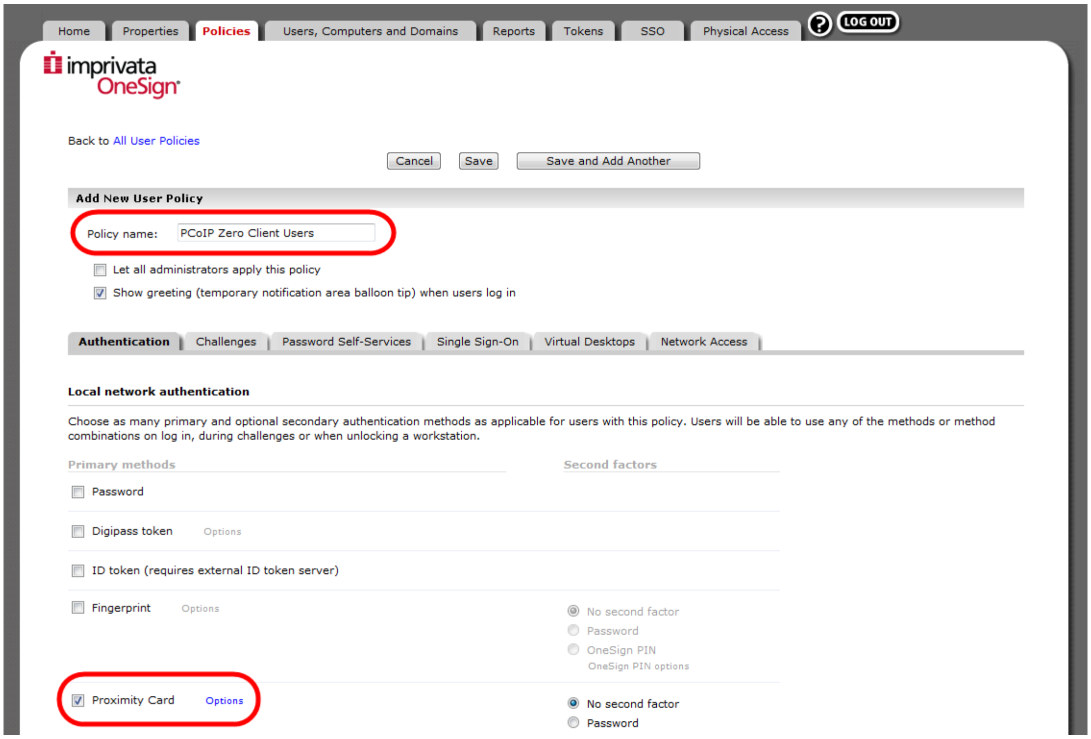
Creating and Assigning Policies

OneSign user and computer policies manage the user workflows. You must configure policies to support zero client users. This involves:

Creating a User Policy on page 4
Creating a Computer Policy on page 5
Configuring Computer Policy Auto-assignment on page 5

Creating a User Policy

1. On the OneSign Administrator Policies page, User Policies tab, make sure that User Policies for PCoIP zero client users allow proximity card authentication.



Back to All User Policies

Add New User Policy

Policy name: PCoIP Zero Client Users

□ Let all administrators apply this policy
☑ Show greeting (temporary notification area balloon tip) when users log in

Local network authentication

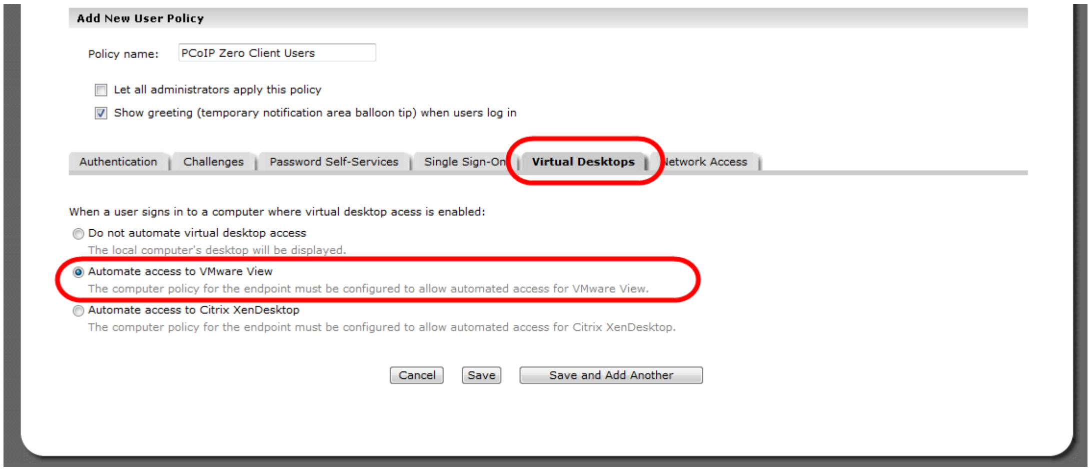
Choose as many primary and optional secondary authentication methods as applicable for users with this policy. Users will be able to use any of the methods or method combinations on log in, during challenges or when unlocking a workstation.

Primary methods | Second factors

□ Password
□ Digipass token
□ ID token (requires external ID token server)
□ Fingerprint — ● No second factor ○ Password ○ OneSign PIN (OneSign PIN options)
☑ Proximity Card — ● No second factor ○ Password

Configuring a User Policy for Zero Client Users

2. On the Virtual Desktops tab, select **Automate access to VMware View** and click **Save**.



Add New User Policy

Policy name: PCoIP Zero Client Users

□ Let all administrators apply this policy
☑ Show greeting (temporary notification area balloon tip) when users log in

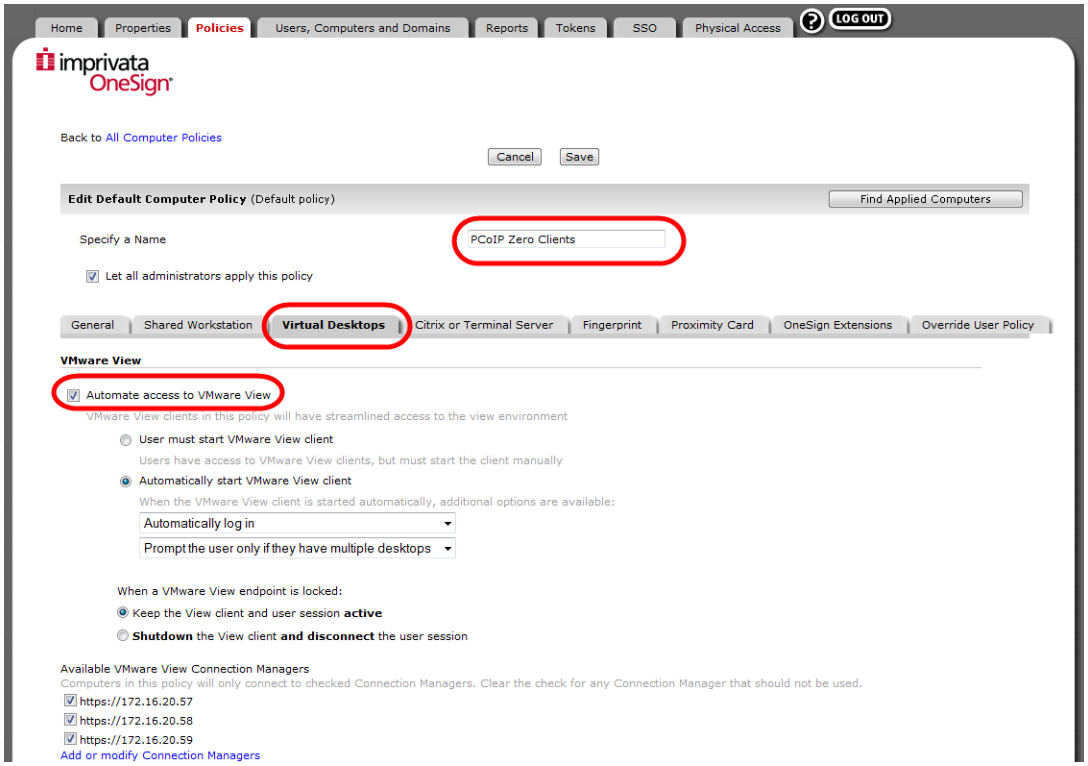
When a user signs in to a computer where virtual desktop acess is enabled:

○ Do not automate virtual desktop access
The local computer's desktop will be displayed.
● Automate access to VMware View
The computer policy for the endpoint must be configured to allow automated access for VMware View.
○ Automate access to Citrix XenDesktop
The computer policy for the endpoint must be configured to allow automated access for Citrix XenDesktop.

Automating VMware View Access

Creating a Computer Policy

3. On the Policies page, Computer Policies tab, create a computer policy for your PCoIP zero clients. On the Virtual Desktops tab, enable **Automate access to VMware View**. Select a workflow, then click **Save**.



Back to All Computer Policies

Edit Default Computer Policy (Default policy)

Specify a Name: PCoIP Zero Clients

☑ Let all administrators apply this policy

VMware View

☑ Automate access to VMware View

VMware View clients in this policy will have streamlined access to the view environment

○ User must start VMware View client

Users have access to VMware View clients, but must start the client manually

● Automatically start VMware View client

When the VMware View client is started automatically, additional options are available:

Automatically log in

Prompt the user only if they have multiple desktops

When a VMware View endpoint is locked:

● Keep the View client and user session **active**

○ **Shutdown** the View client **and disconnect** the user session

Available VMware View Connection Managers

Computers in this policy will only connect to checked Connection Managers. Clear the check for any Connection Manager that should not be used.

☑ https://172.16.20.57

☑ https://172.16.20.58

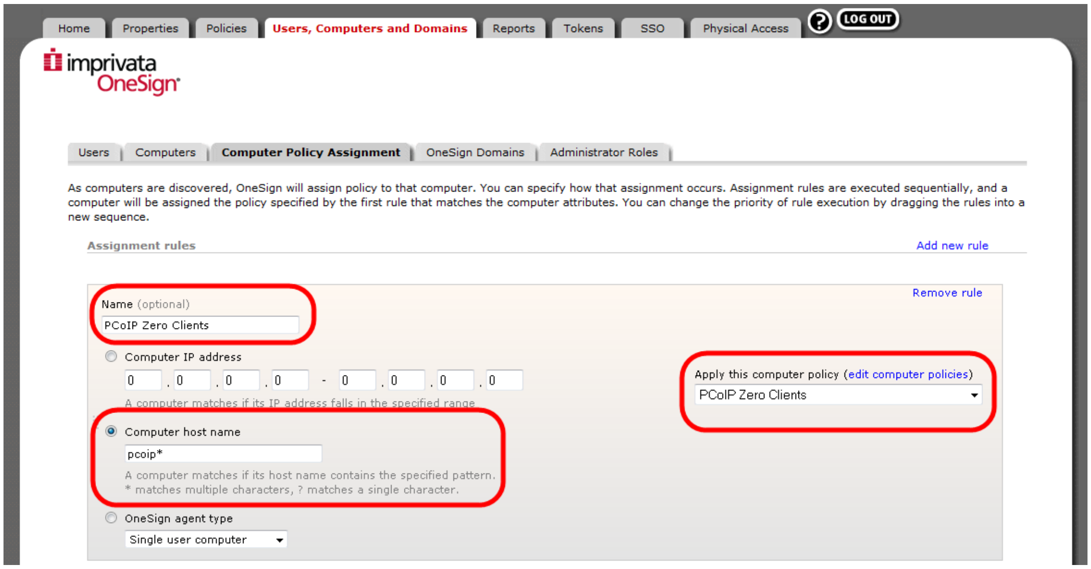
☑ https://172.16.20.59

Add or modify Connection Managers

Creating a Computer Policy for the Zero Clients

Configuring Computer Policy Auto-assignment

4. On the Users, Computers and Domains page, Computer Policy Assignment tab, add a new rule. Give the rule a name, and develop a rule that applies the computer policy to the new zero clients.



As computers are discovered, OneSign will assign policy to that computer. You can specify how that assignment occurs. Assignment rules are executed sequentially, and a computer will be assigned the policy specified by the first rule that matches the computer attributes. You can change the priority of rule execution by dragging the rules into a new sequence.

Assignment rules

Name (optional): PCoIP Zero Clients

○ Computer IP address: 0 . 0 . 0 . 0 - 0 . 0 . 0 . 0

A computer matches if its IP address falls in the specified range

● Computer host name: pcoip*

A computer matches if its host name contains the specified pattern. * matches multiple characters, ? matches a single character.

○ OneSign agent type: Single user computer

Apply this computer policy (edit computer policies): PCoIP Zero Clients

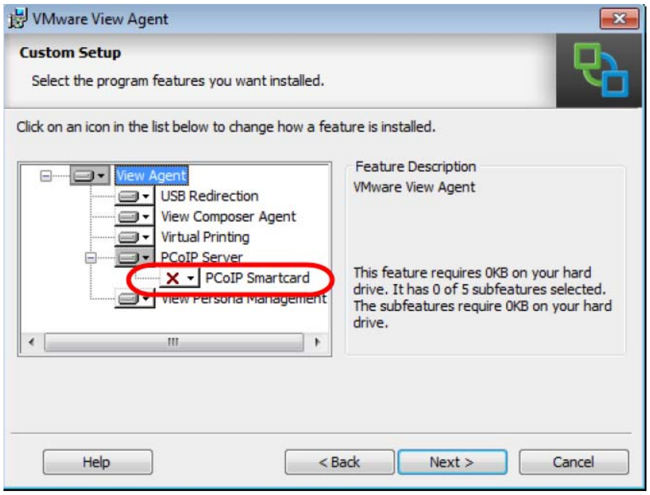
Creating a Computer Policy Assignment Rule

Note: *By default, PCoIP zero client names begin with* ***pcoip-portal-****. If your zero clients are using the default hostnames, enter* ***pcoip**** *in the host name field.*

Deploying the OneSign Agent on the Virtual Desktop

Before you begin, make sure that the View Agent is installed on the Virtual Desktop.

Note: *For end points using the OMNIKEY 5325 proximity card reader, make sure that View Agent is installed with the* ***PCoIP Smartcard*** *component disabled, as shown below.*



VMware View Agent

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- View Agent
  - USB Redirection
  - View Composer Agent
  - Virtual Printing
  - PCoIP Server
    - ✗ PCoIP Smartcard
  - View Persona Management

Feature Description

VMware View Agent

This feature requires 0KB on your hard drive. It has 0 of 5 subfeatures selected. The subfeatures require 0KB on your hard drive.

Disabling PCoIP Smartcard for OMNIKEY 5325 Readers

To deploy the OneSign Agent to the virtual desktop:

1. Establish a session with the Virtual Desktop using an account with administrator privileges.
2. From the OneSign Administrator Properties page, Agent Deployment tab, download the appropriate 32 or 64 bit version of the OneSign Agent for installation within the Windows virtual desktop or virtual desktop image.
3. Install the OneSign Agent within the virtual desktop.
4. Set the **RemoteOnly** registry key data value to `1 (DWORD)` and base `Hexadecimal`. This is at:

`HKEY_LOCAL_MACHINE/SOFTWARE/SSOProvider/DeviceManager` for Windows XP or Windows 7 32-bit.
`HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/SSOProvider/DeviceManager` for Windows 7 64-bit.

5. Set the **RedirectionSupported** value to `1 (DWORD)` and base `Hexadecimal`. This is at:

`HKEY_LOCAL_MACHINE/SOFTWARE/SSOProvider/DeviceManager` for Windows XP or Windows 7 32-bit.
`HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/SSOProvider/DeviceManager` for Windows 7 64-bit.

6. Reboot the Virtual Desktop.
7. Deploy to the VMware View pool as necessary.
8. Test by authenticating with a proximity card or password via the OneSign interface on the zero client.

The next step is to configure the PCoIP zero clients. This is detailed in **Creating and Assigning Policies** on page 4.