

**RSA SECURID<sup>®</sup> ACCESS**

**Standard Agent Client  
Implementation Guide**

**VMware Identity Manager vIDM 3.1**

Daniel R. Pintal, RSA Partner Engineering  
Last Modified: June 25, 2018

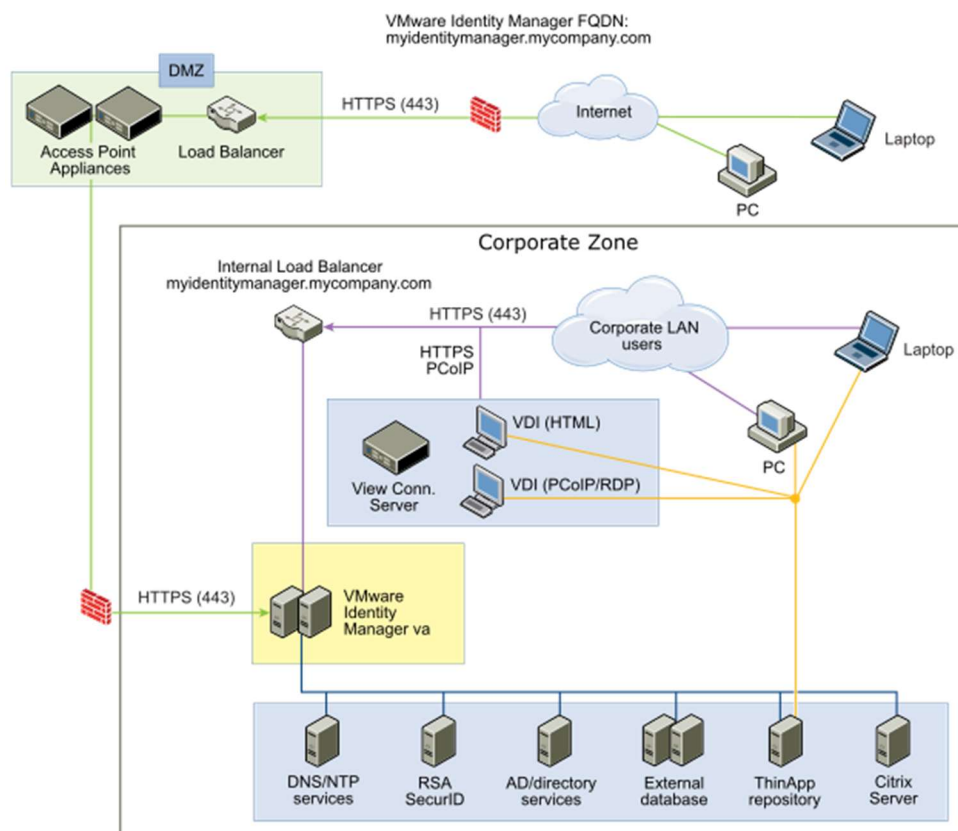
## Solution Summary

VMware Identity Manager provides access to applications from any device, simplifying the end-user experience by combining applications into a single enterprise-class aggregated workspace, securely delivered on any device. IT has a centralized place to manage user provisioning, access policies with enterprise-class directory integration, and identity federation.

RSA SecurID Access Features	
VMware Identity Manager 3.1	
<b>Authentication Manager Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	-

Identity Assurance	
Collect Device Assurance and User Behavior	-



## Partner Product Configuration

---

### ***Before You Begin***

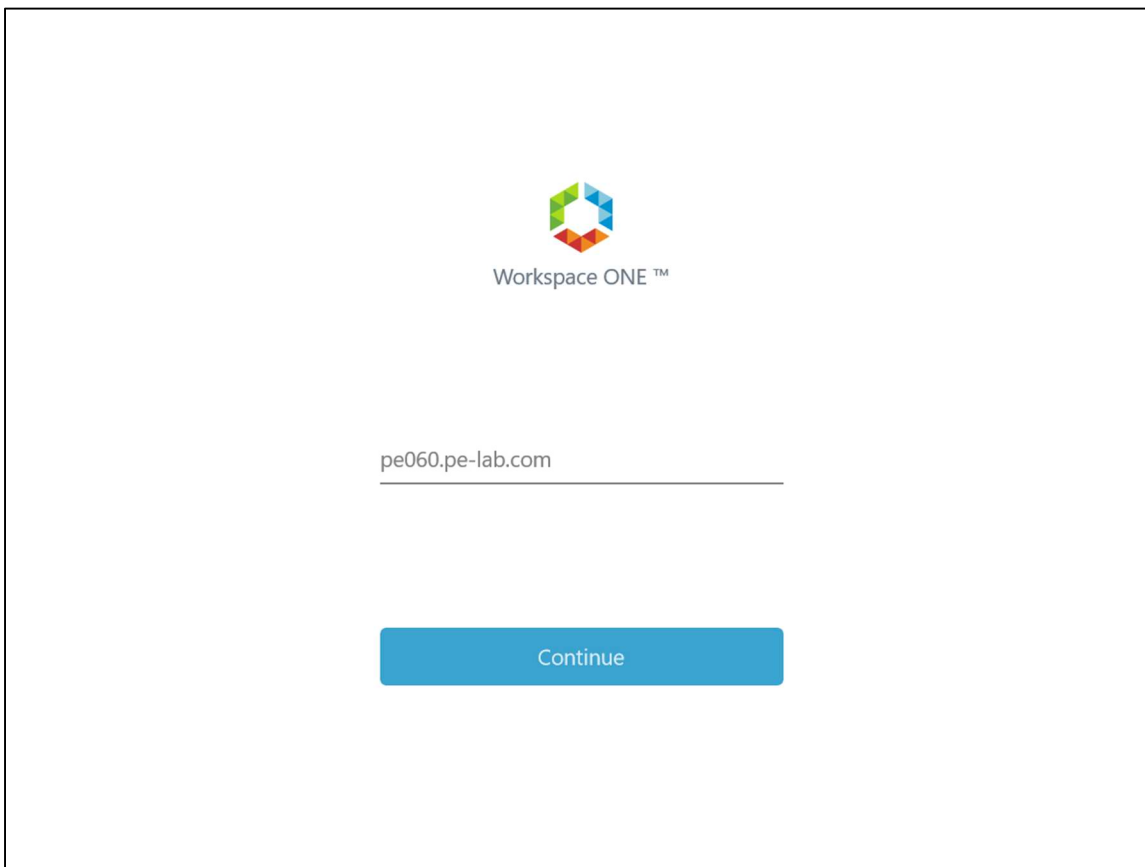
This section provides instructions for configuring the VMware Identity Manager/Workspace One client to work with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All VMware components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***VMware Identity Manager/Workspace One Configuration***

1. Enter the DNS Name of the Identity Manager.



Workspace ONE™

pe060.pe-lab.com

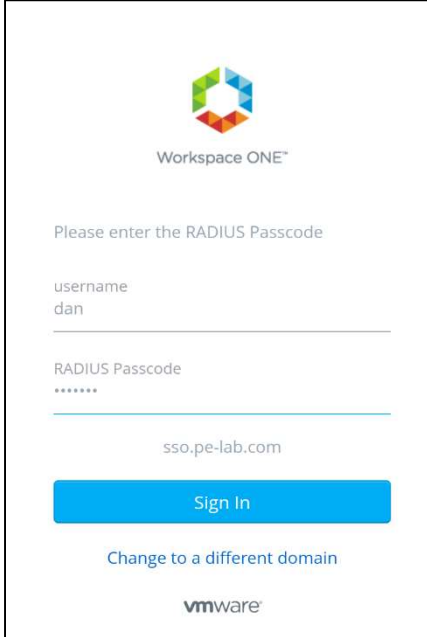
Continue

## Screens

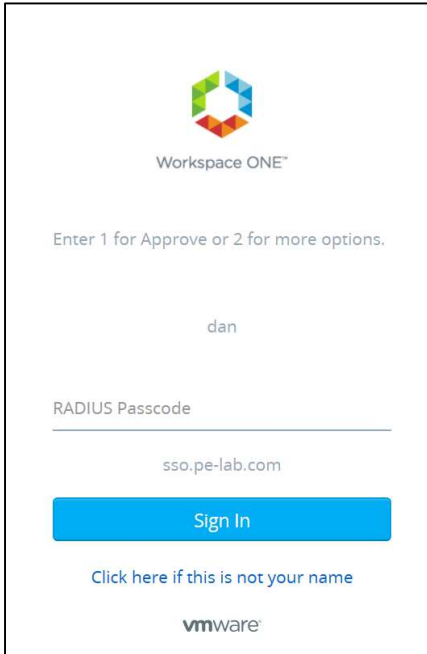
---

### Desktop, iOS and Android

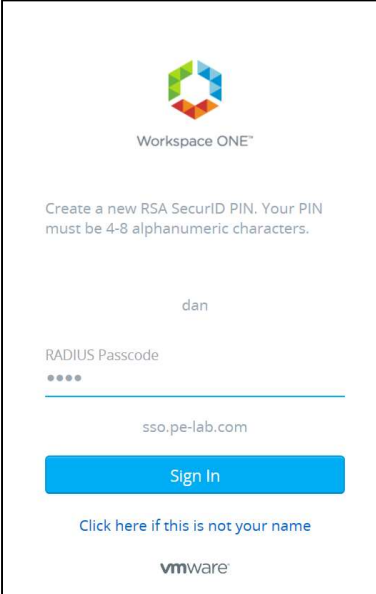
Login Screen (SecurID Access and Cloud RADIUS):



Authenticate Options Screen (SecurID Access Cloud RADIUS only):

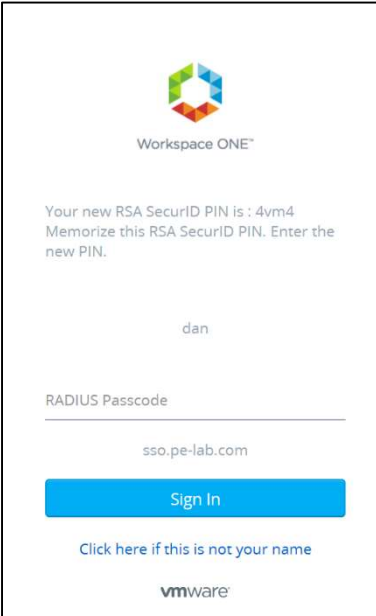


User-defined New PIN (SecurID Access and Cloud RADIUS):



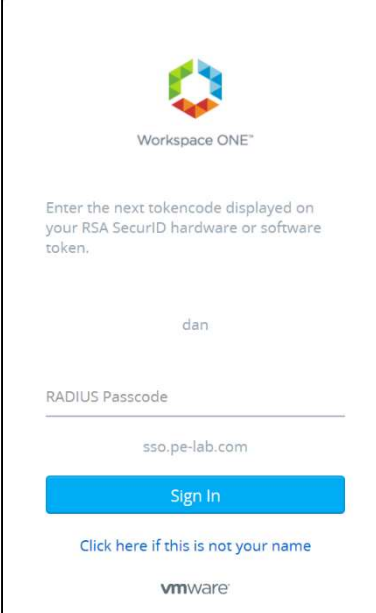
The screenshot shows the VMware Workspace ONE interface for creating a new RSA SecurID PIN. At the top is the Workspace ONE logo. Below it, the text reads: "Create a new RSA SecurID PIN. Your PIN must be 4-8 alphanumeric characters." The user's name "dan" is displayed. There is a "RADIUS Passcode" field with four dots and a blue underline. Below that, the domain "sso.pe-lab.com" is shown. A blue "Sign In" button is present, followed by a link: "Click here if this is not your name". The VMware logo is at the bottom.

System-generated New PIN (SecurID Access and Cloud RADIUS):



The screenshot shows the VMware Workspace ONE interface for a system-generated new RSA SecurID PIN. At the top is the Workspace ONE logo. Below it, the text reads: "Your new RSA SecurID PIN is : 4vm4 Memorize this RSA SecurID PIN. Enter the new PIN." The user's name "dan" is displayed. There is a "RADIUS Passcode" field with a blue underline. Below that, the domain "sso.pe-lab.com" is shown. A blue "Sign In" button is present, followed by a link: "Click here if this is not your name". The VMware logo is at the bottom.

Next Tokencode (SecurID Access and Cloud RADIUS):



The screenshot shows a login interface for Workspace ONE. At the top is the Workspace ONE logo, a colorful hexagon. Below it, the text reads "Workspace ONE®". The main instruction says "Enter the next tokencode displayed on your RSA SecurID hardware or software token." Below this, the name "dan" is displayed. A label "RADIUS Passcode" is positioned above a horizontal input line. The text "sso.pe-lab.com" is shown below the input line. A blue "Sign In" button is centered below the input field. At the bottom, there is a link that says "Click here if this is not your name" and the VMware logo.

## Certification Checklist for RSA SecurID Access

---

### *Cloud Authentication Service*

#### **Certification Environment Details:**

RSA Authentication Manager 8.2, Virtual Appliance

VMware Identity Manager/Workspace One, 3.1, Windows 2016

#### **RADIUS**

Date Tested: May 3, 2018

	<b>Windows</b>	<b>OS X</b>	<b>Android</b>	<b>iOS</b>	<b>Other</b>
RSA SecurID	✓	-	✓	✓	-
LDAP Password	✓	-	✓	✓	-
Authenticate Approve	✓	-	✓	✓	-
Authenticate Tokencode	✓	-	✓	✓	-

✓ = Passed, **X** = Failed, - = N/A

- Reference the Known Issues section of this guide for more details on mobile clients and SAML.

## Certification Checklist for RSA SecurID Access

---

### ***RSA Authentication Manager***

#### **Certification Environment Details:**

RSA Authentication Manager 8.2, Virtual Appliance

VMware Identity Manager, 3.1, Windows 2016

#### **RSA SecurID Authentication**

Date Tested: May 3, 2018

	<b>Windows</b>	<b>Mac</b>	<b>Android</b>	<b>iOS</b>	<b>Other</b>
REST	-	-	-	-	-
UDP Agent	✓	-	✓	✓	-
TCP Agent	-	-	-	-	-
RADIUS	✓	-	✓	✓	-

✓ = Passed, **X** = Failed, - = N/A

- Reference the Known Issues section of this guide for more details on mobile clients and SAML.



## Known Issues

---

Use of the VMware IDM aka.Workspace One Mobile client using RSA SecurID Access SAML is currently under investigation.