

# **RSA SECURID<sup>®</sup> ACCESS**

## **Standard Agent Client Implementation Guide**

### **Cisco AnyConnect Secure Mobility Client**

Peter Waranowski, RSA Partner Engineering  
Last Modified: May 16<sup>th</sup>, 2017

## Solution Summary

---

Cisco AnyConnect leverages Cisco ASA to provide RSA SecurID Access authentication. Cisco ASA integrates with RSA SecurID Access via RADIUS or native UDP agent integration.

Cisco AnyConnect for Windows supports RSA token automation which enhances the end user experience. This feature allows AnyConnect to retrieve Passcodes and Tokencodes from tokens installed in the RSA Software Token application. AnyConnect will then 'listen' for SecurID prompts and programmatically retrieve Tokencodes and Passcodes from the software token behind the scenes.

RSA SecurID Access Features	
Cisco AnyConnect	
<b>Authentication Manager Methods</b>	
RSA SecurID	<input type="text" value="Yes"/>
On Demand Authentication	<input type="text" value="Yes"/>
Risk-Based Authentication	<input type="text" value="No"/>
<b>Cloud Authentication Service Methods</b>	
Authenticate App	<input type="text" value="Yes"/>
FIDO Token	<input type="text" value="No"/>
Identity Assurance	
Collect Device Assurance and User Behavior	<input type="text" value="No"/>
Software Token Automation	
Windows	<input type="text" value="Yes"/>
Mac	<input type="text" value="No"/>
Android	<input type="text" value="No"/>
iOS	<input type="text" value="No"/>

## Partner Product Configuration

---

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

This section provides instructions for configuring the Cisco AnyConnect 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 Cisco components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***Integration Summary***

#### **Configuring RSA SecurID Access Authentication**

- Desktop
- Mobile

#### **Configuring RSA SecurID Software Token Automation**

- Desktop (Windows only)

## Configuring Cisco AnyConnect

When configuring Cisco AnyConnect for use with RSA SecurID Access Cloud Authentication Service via RADIUS, you will need to increase the AuthenticationTimeout value. The default value of 12 seconds does not provide sufficient time for the end user to complete out of band challenges.

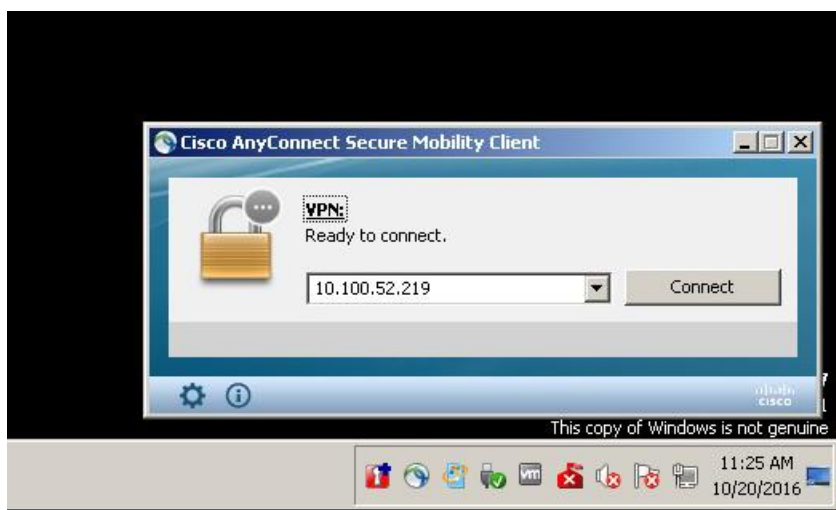
The following example changes the authentication timeout to 120 seconds.

```
<ClientInitialization>  
  <AuthenticationTimeout>120</AuthenticationTimeout>  
</ClientInitialization>
```

## Desktop

RSA SecurID Authentication is configured on the VPN server via RADIUS or Native RSA SecurID agent integration. No additional configuration on the AnyConnect client is required.

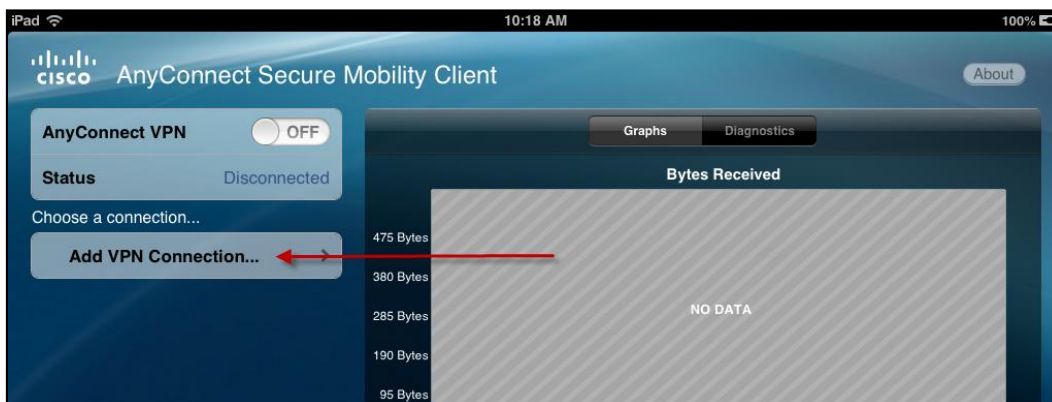
Enter the hostname or IP address of your VPN server in the **VPN:** text field and click **Connect**.



## Mobile

RSA SecurID Authentication is configured on the VPN server via RADIUS or Native RSA SecurID agent integration. No additional configuration on the AnyConnect client is required.

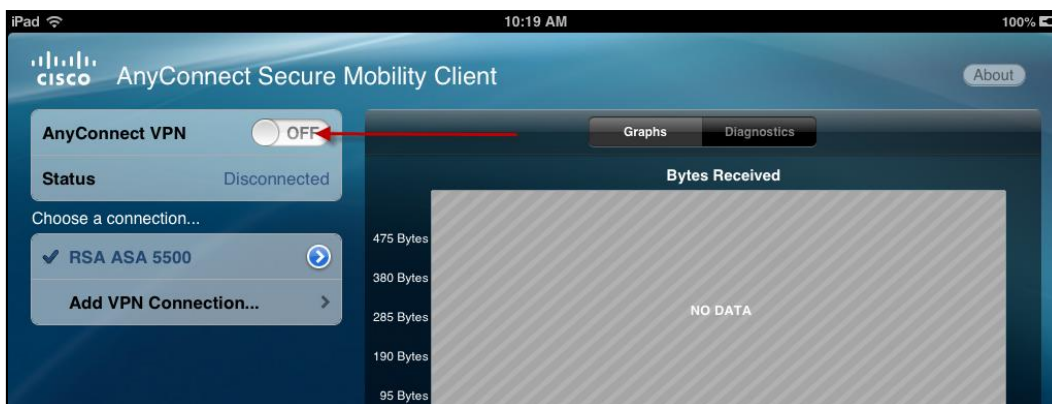
1. Tap **Add VPN Connection...**



2. Enter a **Description** and **Server Address** for your VPN server and tap **Save**.



3. Slide the **AnyConnect VPN** switch to start the connection to your VPN server.



## ***Configuring RSA Software Token Automation***

### **Desktop – Windows**

To enable RSA Software Token Automation:

1. Install the 32-bit RSA Software Token with Automation application on the same system as Cisco AnyConnect.
2. Import RSA Software Token(s) into the RSA Software Token Application.
3. Restart the Cisco AnyConnect client if it is currently running.

---

**! > Important: You must install the 32 bit version of RSA Software Token in order to enable the software token automation feature.**

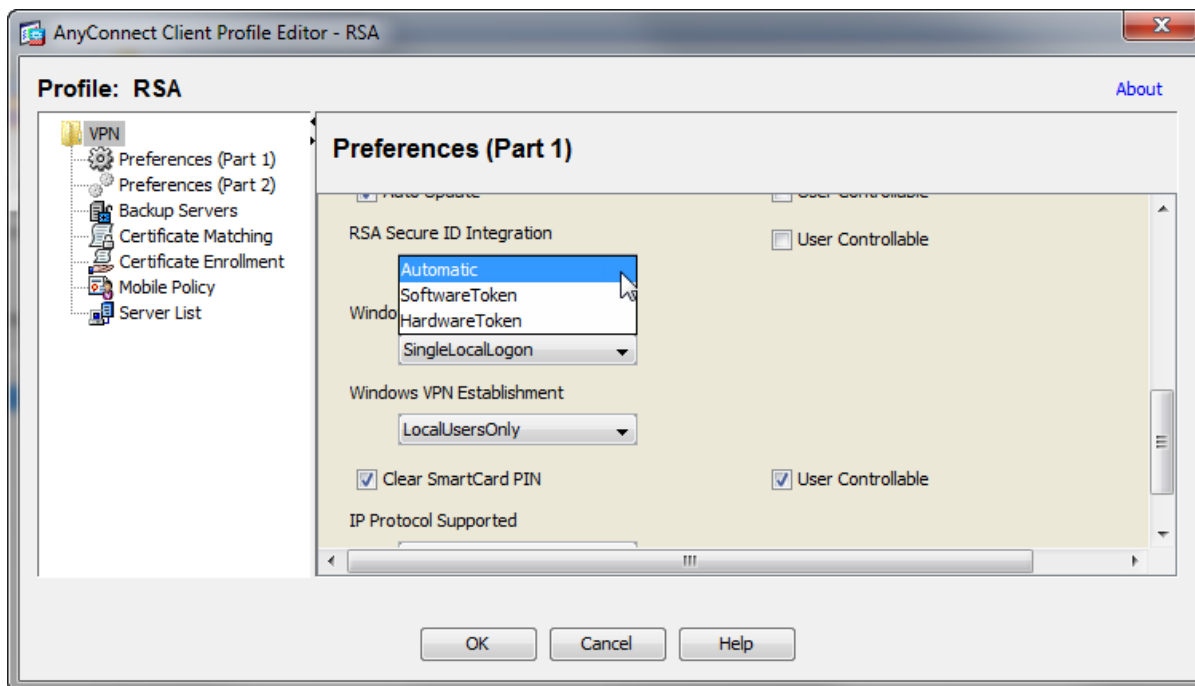
---

The default integration behavior is to prompt for “PIN or Passcode” when the software token is available. The user can authenticate using either a hardware token or an installed software token. The integration can be configured to use only a hardware token (prompt for Passcode) or only a software token (prompt for PIN) by modifying the AnyConnect Client Profile on the Cisco ASA server.

To modify the AnyConnect Client Profile:

1. Open the **Cisco ASDM** administrative console.
2. Browse to **Configuration > Network (Client) Access > AnyConnect Client Profile** and click **Add** or **Edit**.

3. Under **Preferences(Part 1)**, locate the **RSA SecurID Integration** menu and make your selection.



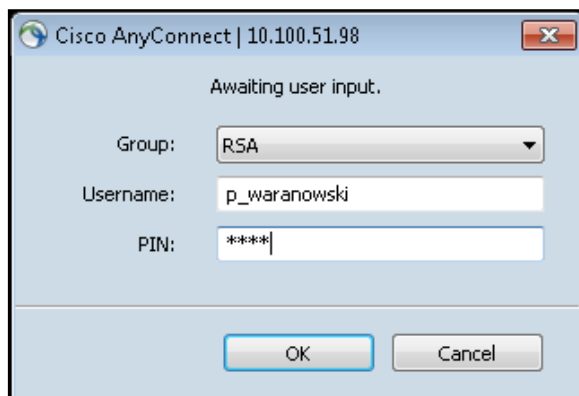
- **Automatic** – Prompts the user for 'PIN or Passcode' and allows for authentication using either a hardware or software token.
- **SoftwareToken** – Prompts the user for 'PIN' and allows for authentication using a software token only.
- **HardwareToken** – Prompts the user for 'Passcode' and allows for authentication using a hardware token only.

## Screens

---

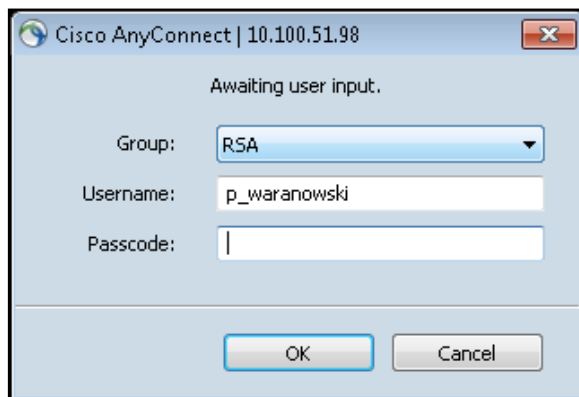
### Desktop - Windows

Software Token PIN Prompt:



A screenshot of a Windows dialog box titled "Cisco AnyConnect | 10.100.51.98". The dialog contains the text "Awaiting user input." and three input fields: "Group:" with a dropdown menu showing "RSA", "Username:" with the text "p\_waranowski", and "PIN:" with the text "\*\*\*\*". At the bottom are "OK" and "Cancel" buttons.

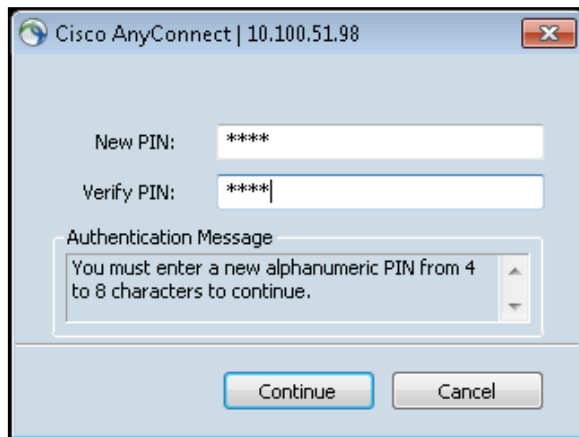
Login screen:



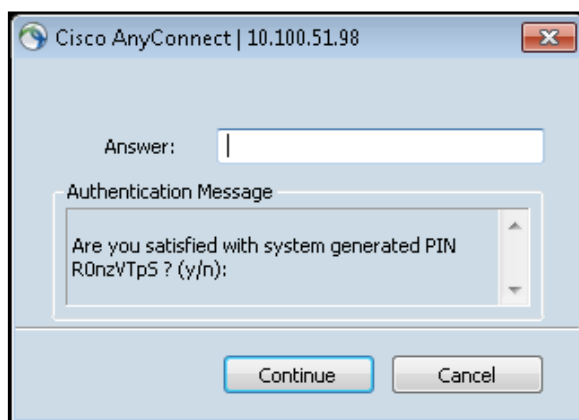
A screenshot of a Windows dialog box titled "Cisco AnyConnect | 10.100.51.98". The dialog contains the text "Awaiting user input." and three input fields: "Group:" with a dropdown menu showing "RSA", "Username:" with the text "p\_waranowski", and "Passcode:" with an empty field. At the bottom are "OK" and "Cancel" buttons.



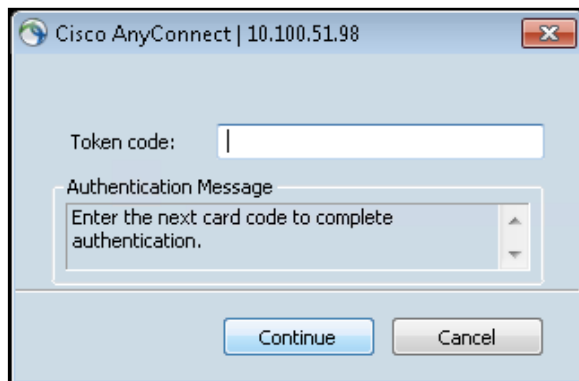
User-defined New PIN:



System-generated New PIN:

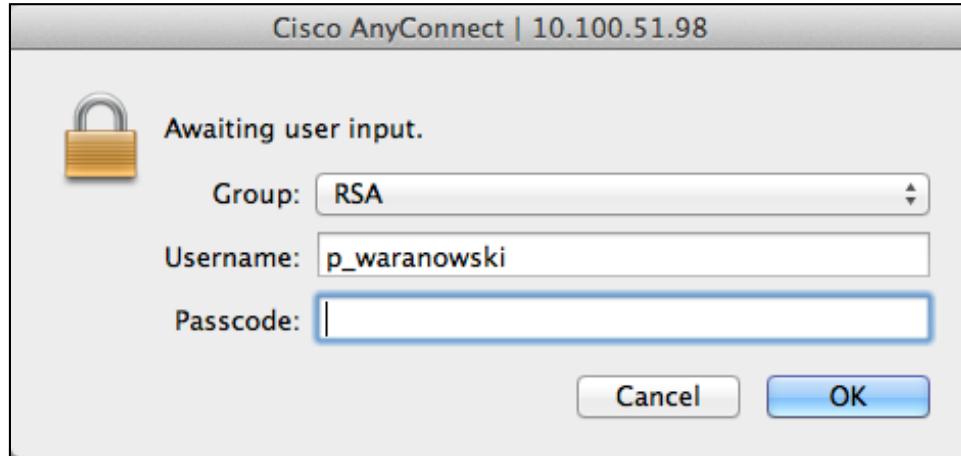


Next Tokencode:




## Desktop - Mac OS

Login screen:



Cisco AnyConnect | 10.100.51.98

 Awaiting user input.

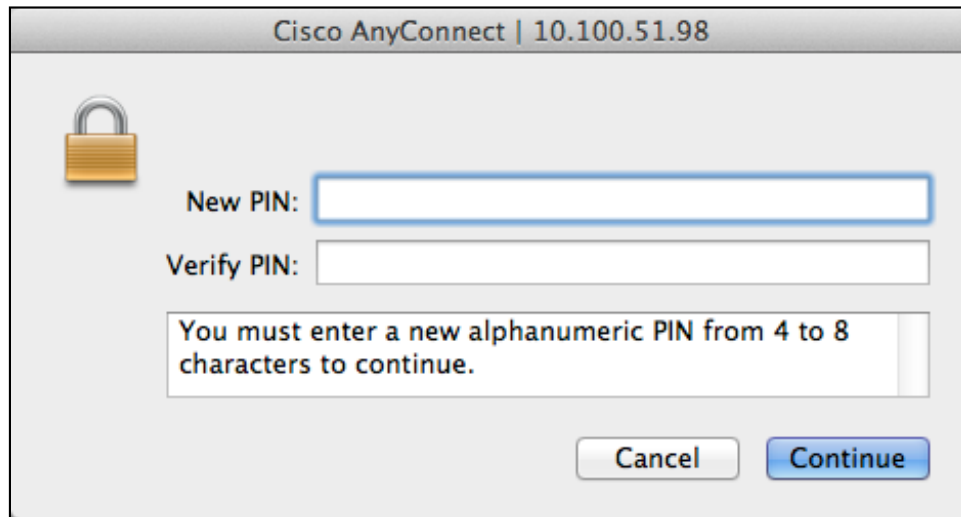
Group: RSA

Username: p\_waranowski


Passcode:

Cancel OK

User-defined New PIN:



Cisco AnyConnect | 10.100.51.98

 New PIN:

Verify PIN:

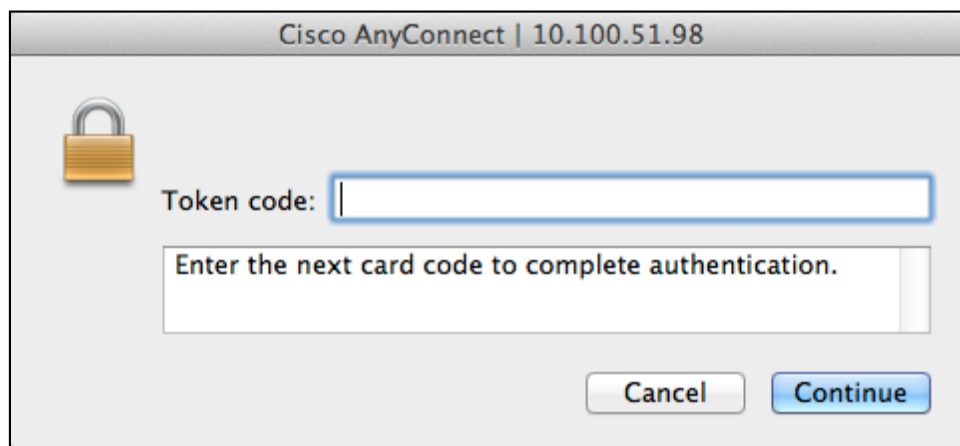
You must enter a new alphanumeric PIN from 4 to 8 characters to continue.

Cancel Continue

System-generated New PIN:

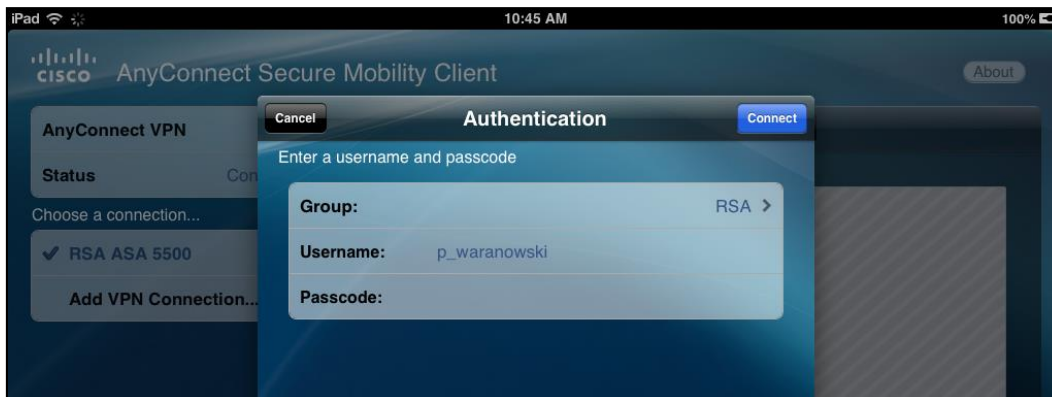


Next Tokencode:

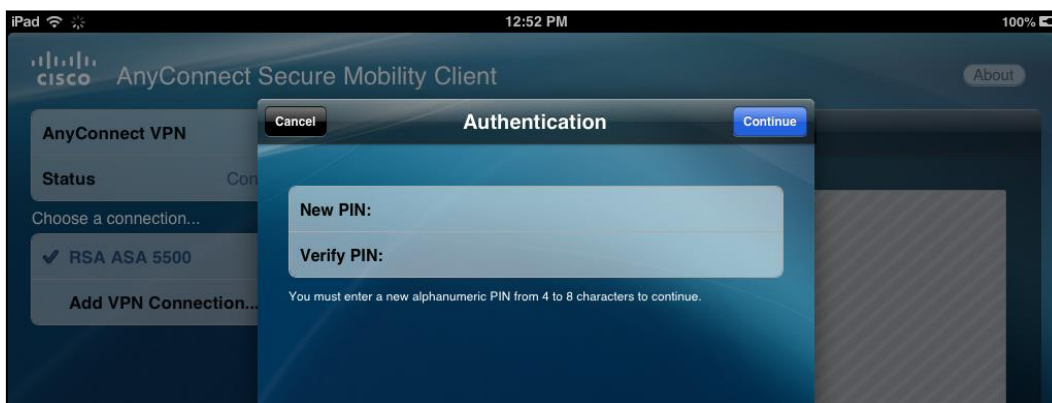


## Mobile – iOS (iPad)

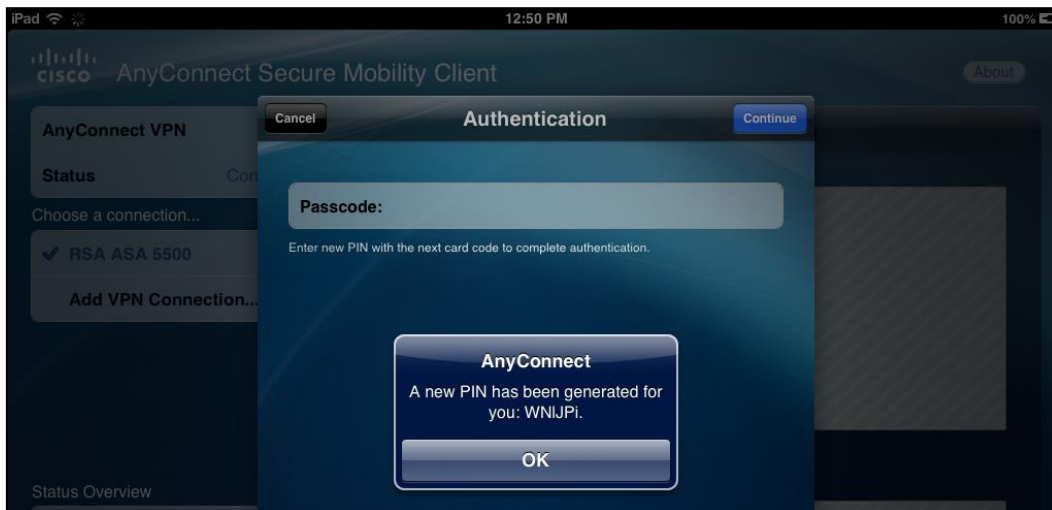
Login screen:



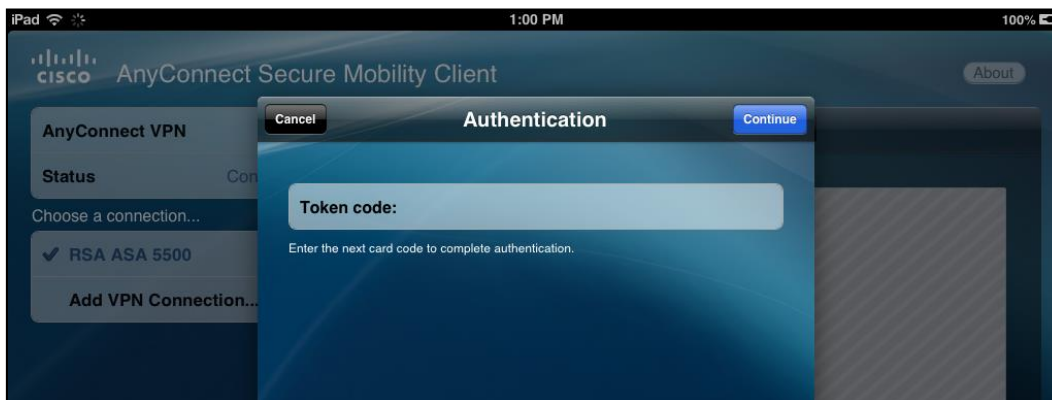
User-defined New PIN:



System-generated New PIN:

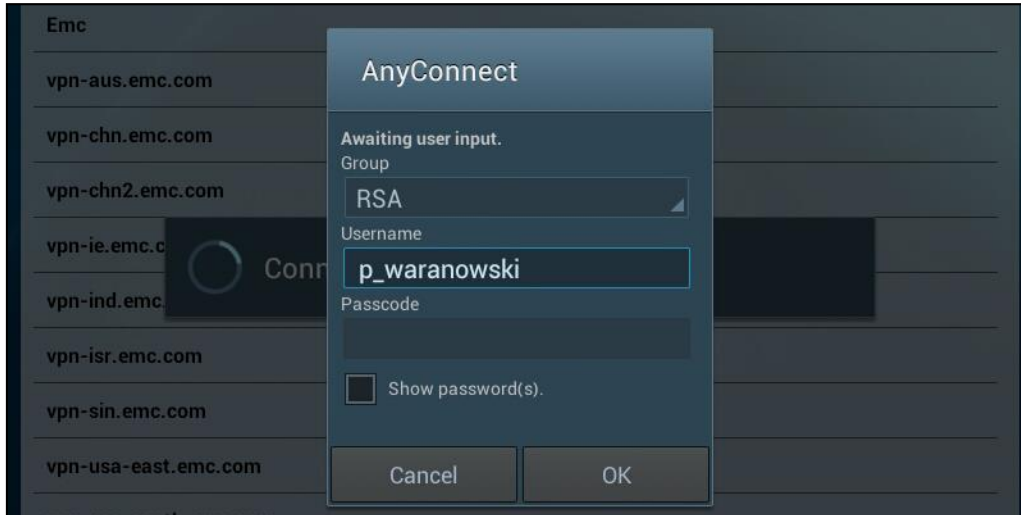


Next Tokencode:

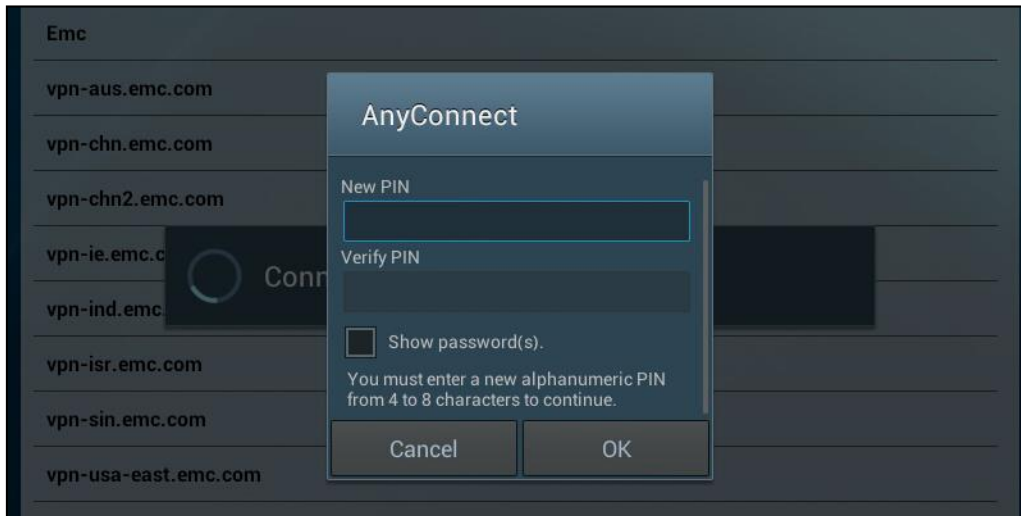


## Mobile - Android

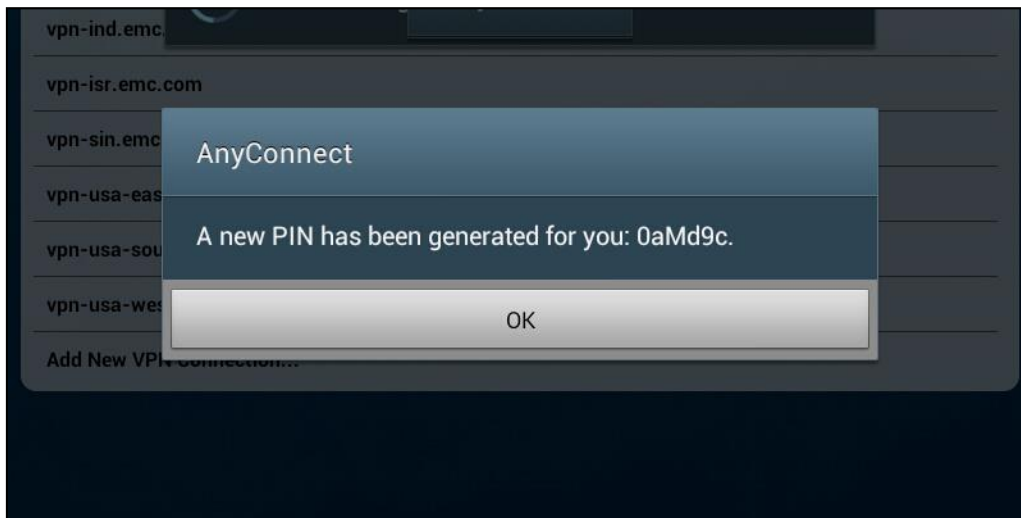
Login screen:



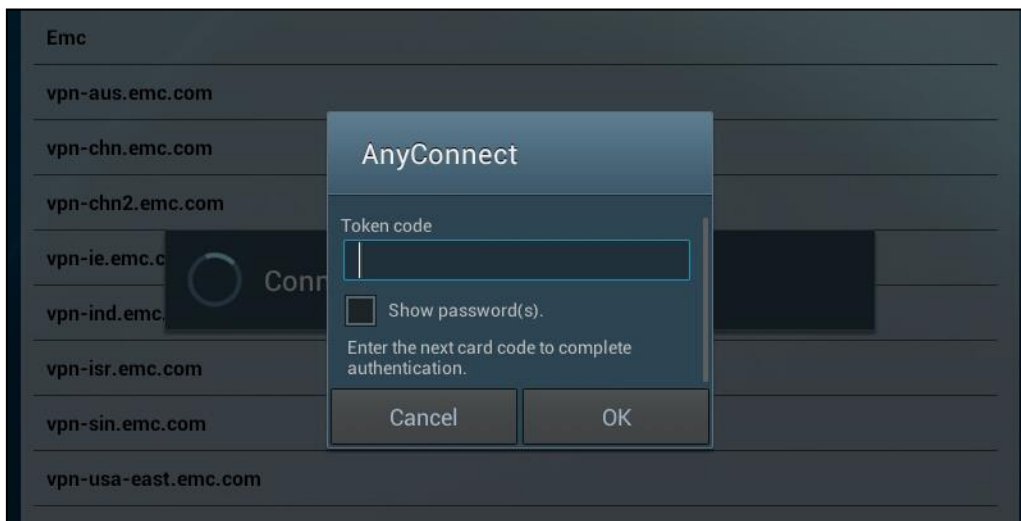
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



## Certification Checklist for RSA SecurID Access

### Cloud Authentication Service

#### Certification Environment Details:

- RSA Authentication Manager 8.2, Virtual Appliance
- RSA Software Token 5.0 (32bit w/ automation), Windows 7 64bit
- RSA Remote Access Client (RAC) 3.6, Windows 7 64bit
- Cisco ASA 9.5(2), Virtual Appliance
- Cisco AnyConnect for Windows 4.2.0439, Windows 7 Enterprise 64bit
- Cisco AnyConnect for Mac 4.2.0439, 10.11 El Capitan
- Cisco AnyConnect for Android 4.0.05057, Android 7.0
- Cisco AnyConnect for iOS 4.0.05055, iOS 10.0.2

✓ = Pass ✗ = Fail N/A = Non-Available Function

#### RADIUS

Date Tested: April 3<sup>rd</sup>, 2017

	Windows	OS X	Android	iOS	Other
RSA SecurID	✓	✓	✓	✓	N/A
LDAP Password	✓	✓	✓	✓	N/A
Authenticate Approve	✓	✓	✓	✓	N/A
Authenticate Tokencode	✓	✓	✓	✓	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function



## Certification Checklist for RSA SecurID Access

### RSA Authentication Manager

#### Certification Environment Details:

- RSA Authentication Manager 8.2, Virtual Appliance
- RSA Software Token 5.0 (32bit w/ automation), Windows 7 64bit
- RSA Remote Access Client (RAC) 3.6, Windows 7 64bit
- Cisco ASA 9.5(2), Virtual Appliance
- Cisco AnyConnect for Windows 4.2.0439, Windows 7 Enterprise 64bit
- Cisco AnyConnect for Mac 4.2.0439, 10.11 El Capitan
- Cisco AnyConnect for Android 4.0.05057, Android 7.0
- Cisco AnyConnect for iOS 4.0.05055, iOS 10.0.2

#### RSA SecurID Authentication

Date Tested: October 20<sup>th</sup>, 2016

	Windows	Mac	Android	iOS	Other
REST	N/A	N/A	N/A	N/A	N/A
UDP Agent	✓	✓	✓	✓	N/A
TCP Agent	N/A	N/A	N/A	N/A	N/A
RADIUS	✓	✓	✓	✓	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

#### Software Token Automation

Date Tested: October 20<sup>th</sup>, 2016

	Windows	Mac	Android	iOS	Other
REST	N/A	N/A	N/A	N/A	N/A
UDP Agent	✓	N/A	N/A	N/A	N/A
TCP Agent	N/A	N/A	N/A	N/A	N/A
RADIUS	✓	N/A	N/A	N/A	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function