



User Experience—How To On-board a BYOD Device

Revised: September 27, 2013

The Cisco ISE allows employees to be in charge of on-boarding their own devices through a self-registration workflow and simplifies the automatic provisioning of supplicants as well as certificate enrollment for the most common BYOD devices. The workflow supports iOS, Android, Windows, and Mac OS devices and assists in transitioning these devices from an open environment to a secure network with the proper access based on device and user credentials.

The simple workflow provides a positive experience to employees provisioning their own device and allows IT to enforce the appropriate access policies.

Apple iOS Devices

The employee connects to the provisioning SSID and is redirected to the Guest Registration portal for registration after opening a browser. The employee logs in using their Active Directory credentials.

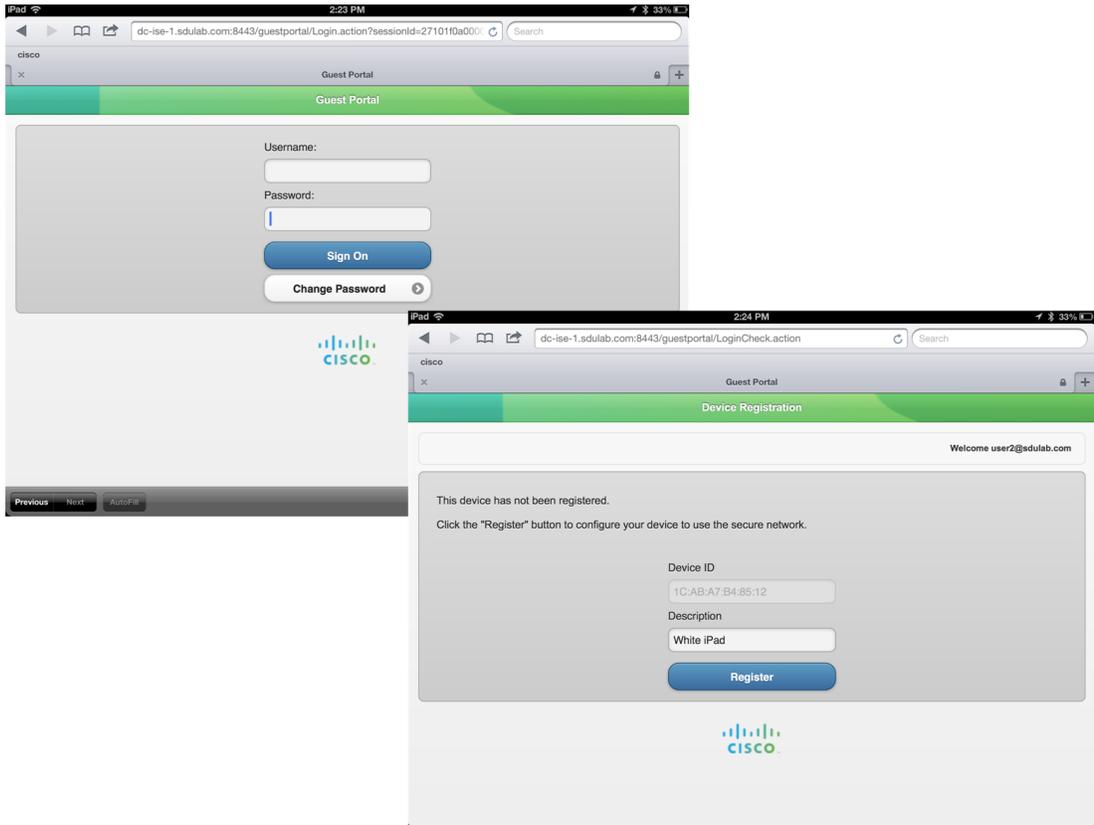
If the device is not yet registered, the session is redirected to the self-registration portal, where the user is asked to enter a description for the new device. The employee is not allowed to change the Device ID (MAC address), which is automatically discovered by ISE.



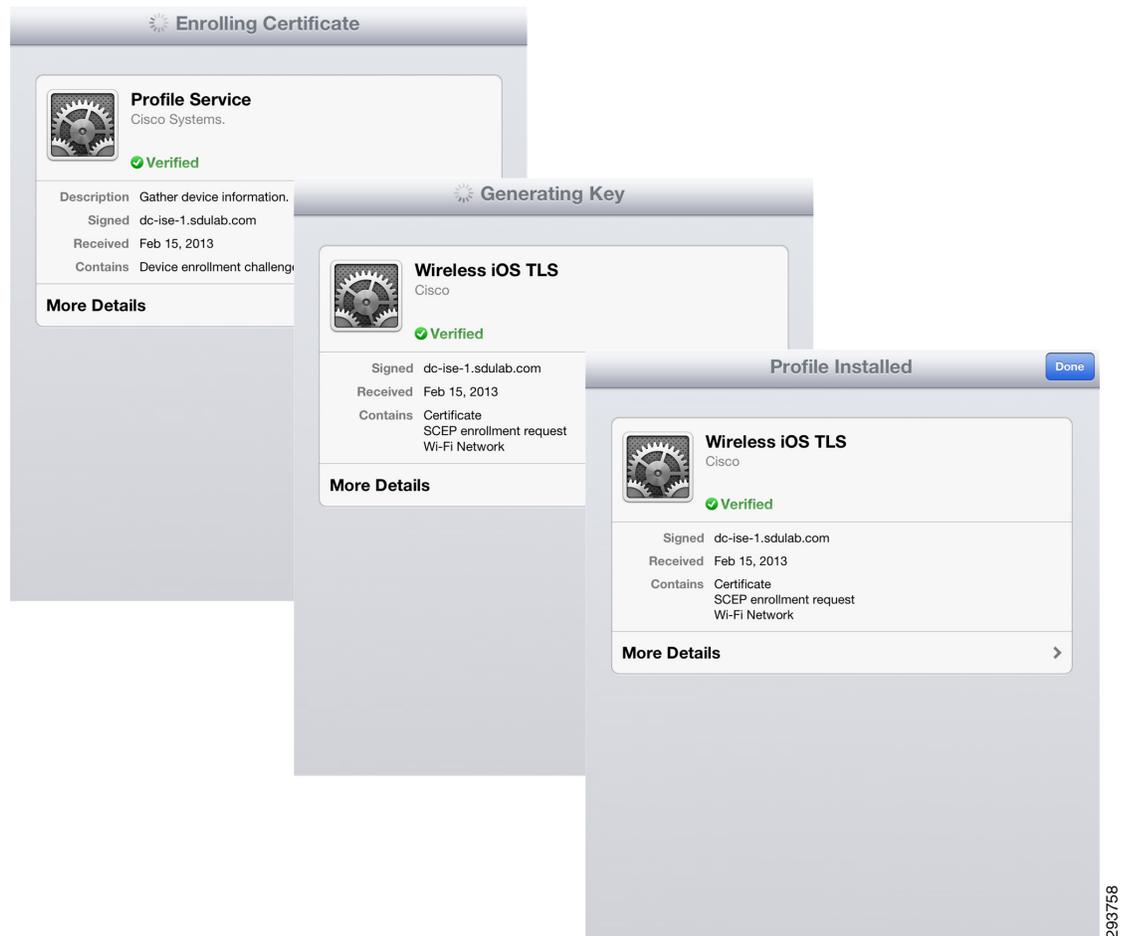
Note

Cisco has been made aware of potential incompatibilities introduced by Apple iOS 7. We are working to understand the limitations and design updates will be made to this publication.

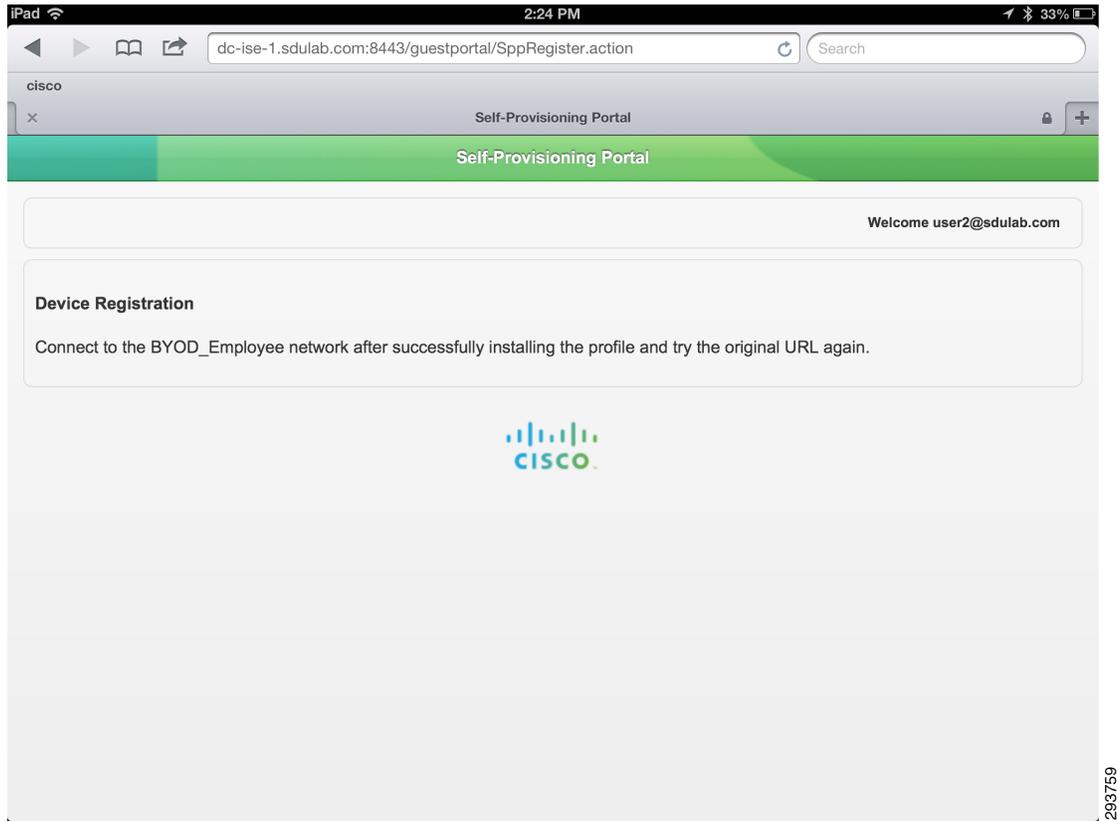
Figure 19-1 Guest Portal and Self-Registration Portal



- The supplicant profile is downloaded and installed on the endpoint.
- Keys are generated and the certificate is enrolled.
- The Wi-Fi profile required to connect to the BYOD_Employee is installed.

Figure 19-2 Enrollment and Profile Installation

The employee is notified that registration is complete and is reminded to manually connect to the BYOD_Employee SSID.

Figure 19-3 Device Registration Complete**Note**

For iOS devices, the employee is required to connect manually to the BYOD_Employee SSID.

The certificates and profile can be viewed by clicking **Settings > General > Profiles** and selecting **Mobile Profile**. [Figure 19-4](#) highlights the Wi-Fi profile to connect to the BYOD_Employee SSID.

Figure 19-4 Mobile Profile Details



As shown in Figure 19-5, the ISE maintains a detailed log of the authentications as they take place:

- The first log shows how the first time the device connects, the MAC address is used for authentication, and the Wireless CWA profile is used for authorization, enabling the redirection to the Guest Registration portal.
- Once the enrollment and provisioning take place, the user connects to the secure BYOD_Employee SSID. ISE grants Partial Access to the device.

Figure 19-5 ISE Authentications Log

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Feb 15,13 04:22:38.055 PM	✓		user2	1C:AB:A7:B4:85:12				Campus WiFi Partial Access	RegisteredDevices
Feb 15,13 04:21:03.764 PM	✓		user2	1C:AB:A7:B4:85:12					Any
Feb 15,13 04:11:22.362 PM	✓		user2	1C:AB:A7:B4:85:12					Any
Feb 15,13 04:10:48.938 PM	✓		1C:AB:A7:B4:85:12	1C:AB:A7:B4:85:12				Wireless CWA	RegisteredDevices

Figure 19-6 shows in more detail the steps that took place and how the rule was evaluated to grant Partial Access.

- Authentication is dot1x and EAP-TLS.
- Username is user2. The Active Directory (AD1) identity store was used.

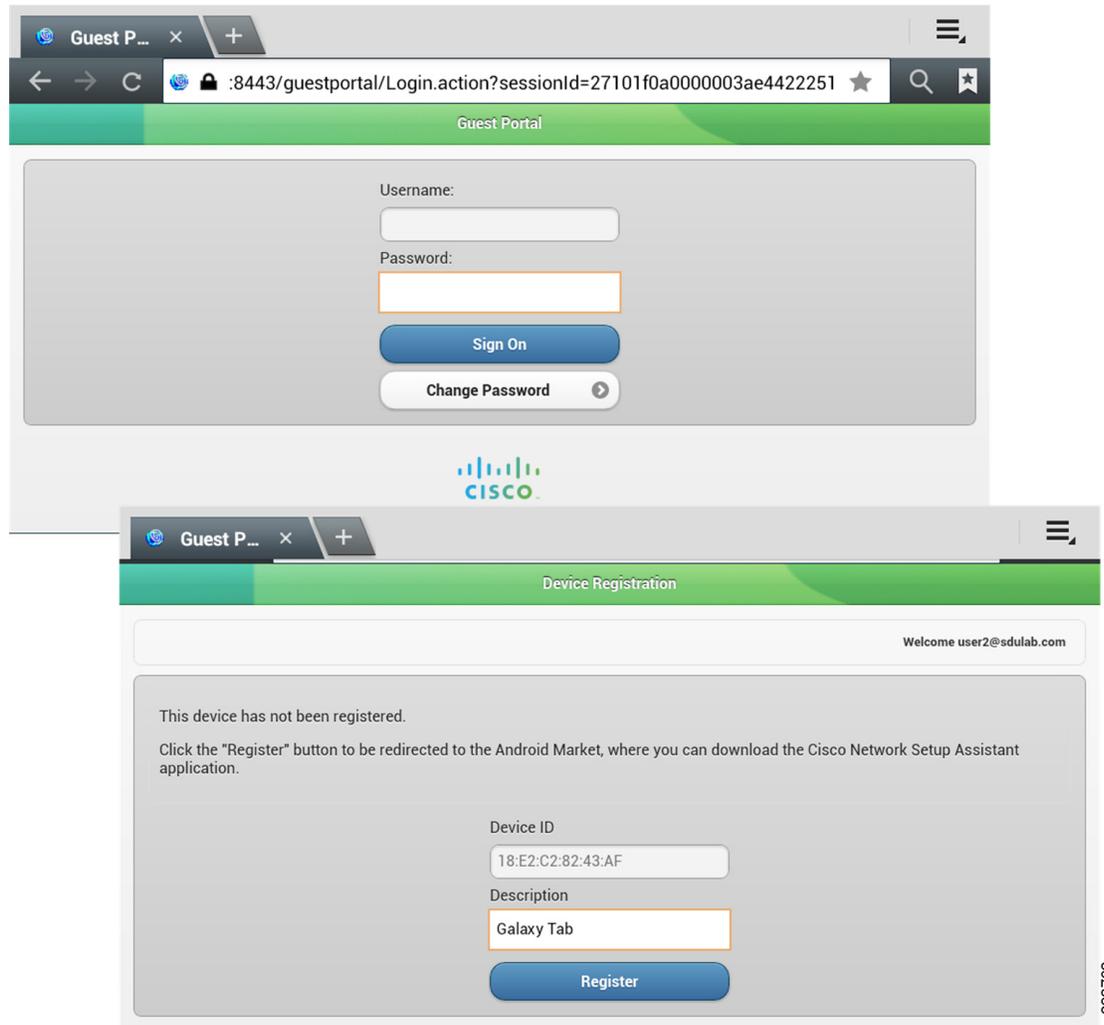
- MAC Address is discovered.
- The Wireless_Dot1X_AuthC authentication rule was used.
- The Campus WiFi Partial Access authorization rule matched. This rule enforces the access list ACL_Partial_Access in the Wireless LAN Controller.

Figure 19-6 ISE Authentication Details

Authentication Details	
Source Timestamp	2013-02-15 16:22:38.055
Received Timestamp	2013-02-15 16:22:38.055
Policy Server	dc-ise-1
Event	5200 Authentication succeeded
Username	user2
User Type	
Endpoint Id	1C:AB:A7:B4:85:12
IP Address	
Identity Store	
Identity Group	RegisteredDevices
Audit Session Id	27101f0a000001a533981e51
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	
Device Type	Network#WLC
Location	Campus_Controllers
NAS IP Address	10.31.16.39
NAS Port Id	
Authorization Profile	Campus WiFi Partial Access
Posture Status	NotApplicable
Security Group	
Failure Reason	
Response Time	381

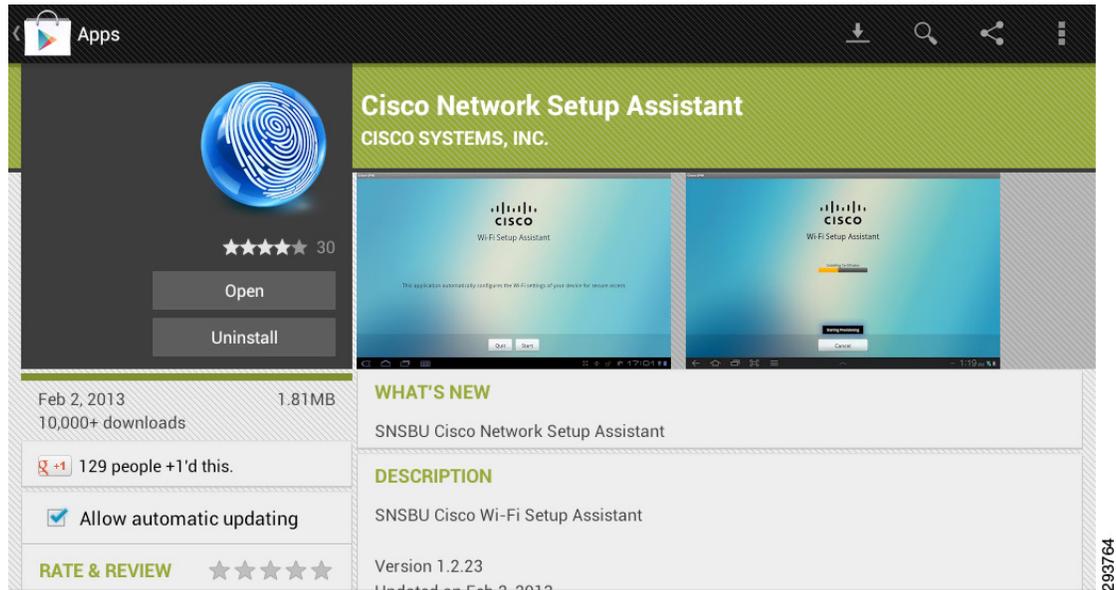
Android Devices

The user experience is very similar when provisioning Android devices. The employee is redirected to the Guest Registration portal and is allowed to enter a description for the new device.

Figure 19-7 Guest Portal and Self-Registration Portal

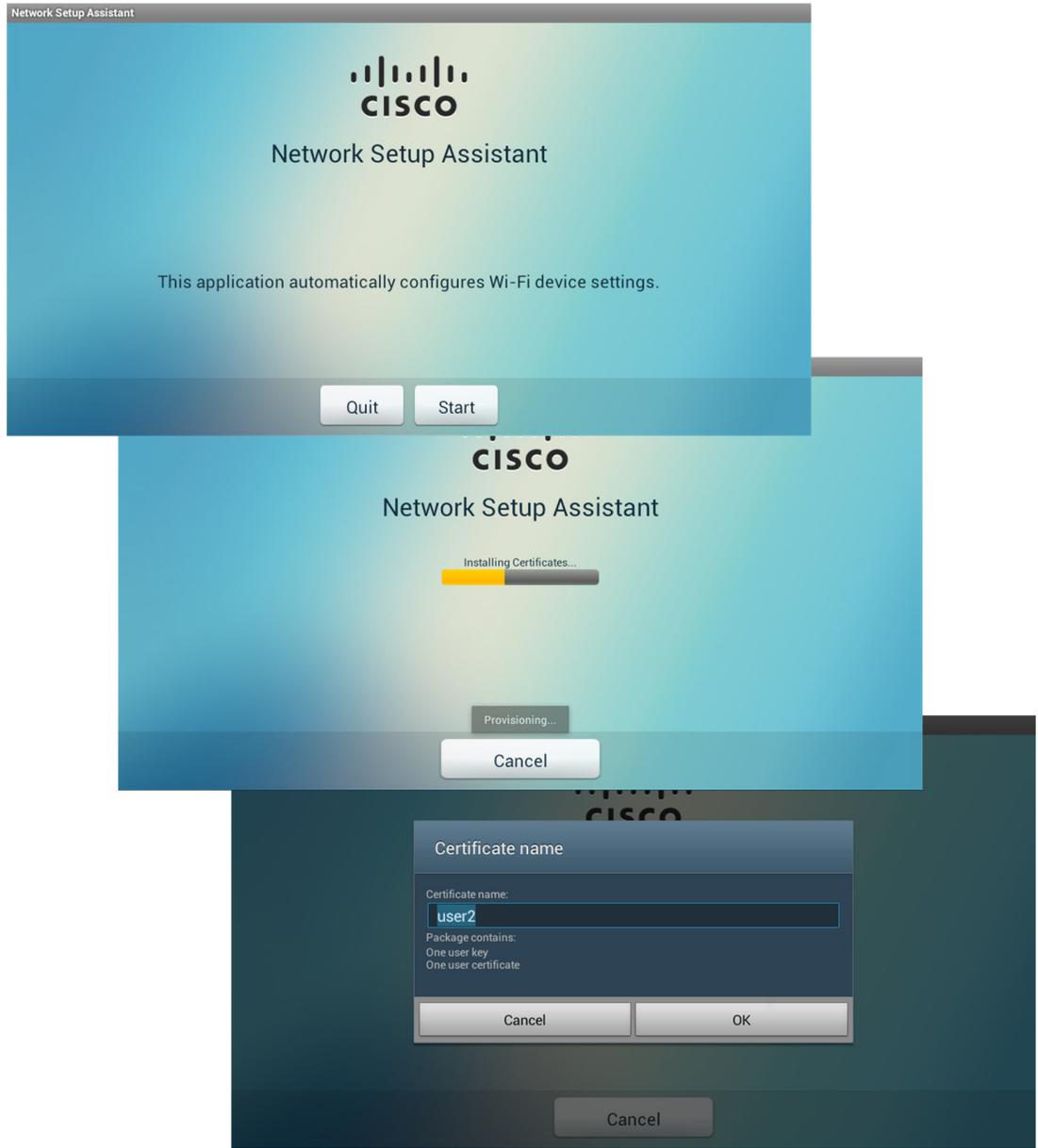
The employee is then redirected to Google Play where the Cisco SPW for Android may be downloaded.

Figure 19-8 Supplicant Provisioning Wizard from Google Play



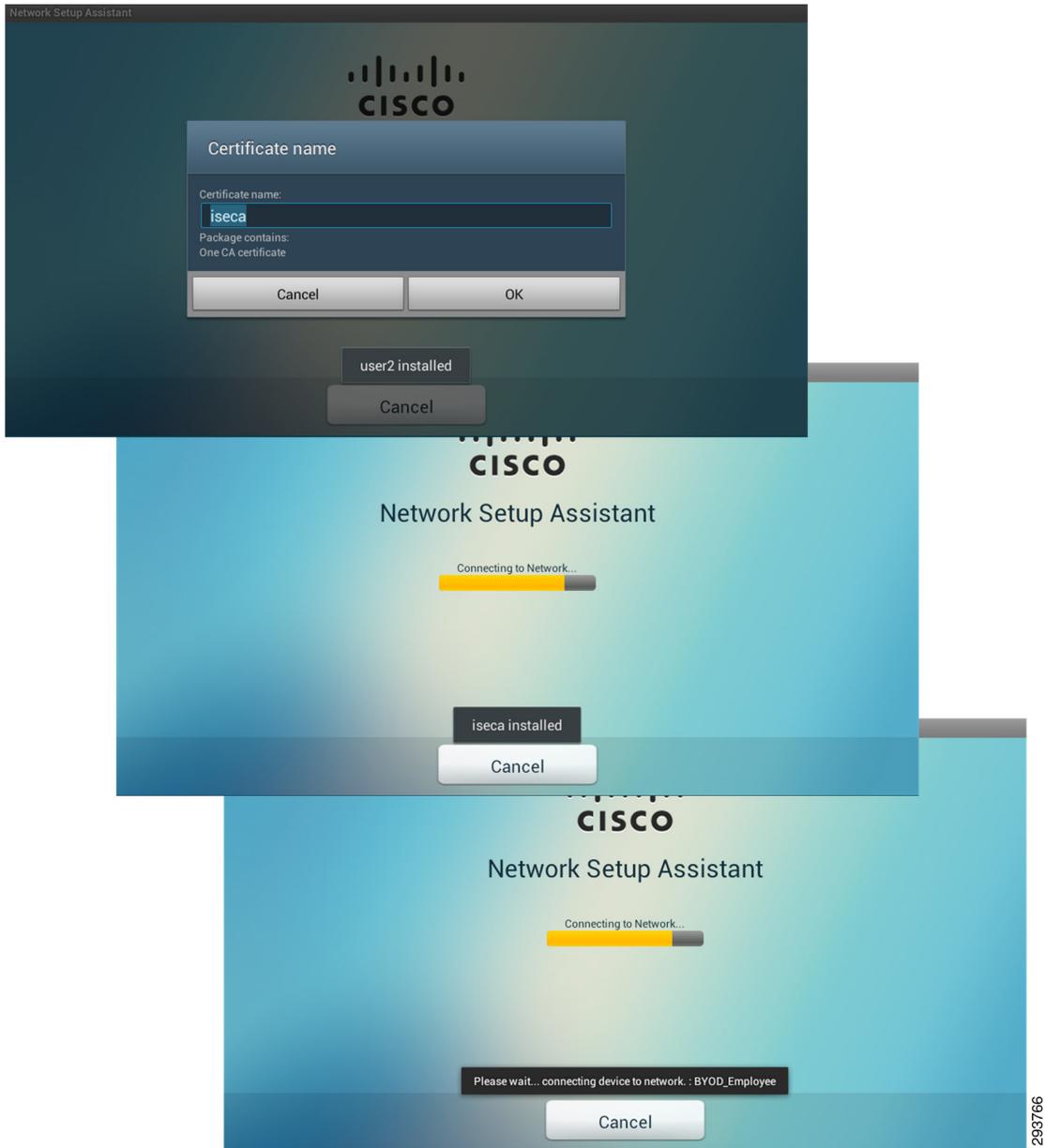
The SPW is launched and the provisioning process begins. The SPW discovers the ISE and begins downloading the profile and installing the certificates.

Figure 19-9 Provisioning Process



The employee is allowed to name the certificate and provides a password for the certificate storage for their device. The Wi-Fi profile to connect to BYOD_Employee is applied.

Figure 19-10 Certificate and Profile



Without employee intervention, the provisioning process automatically connects the Android device to the BYOD_Employee SSID, as shown in [Figure 19-11](#).

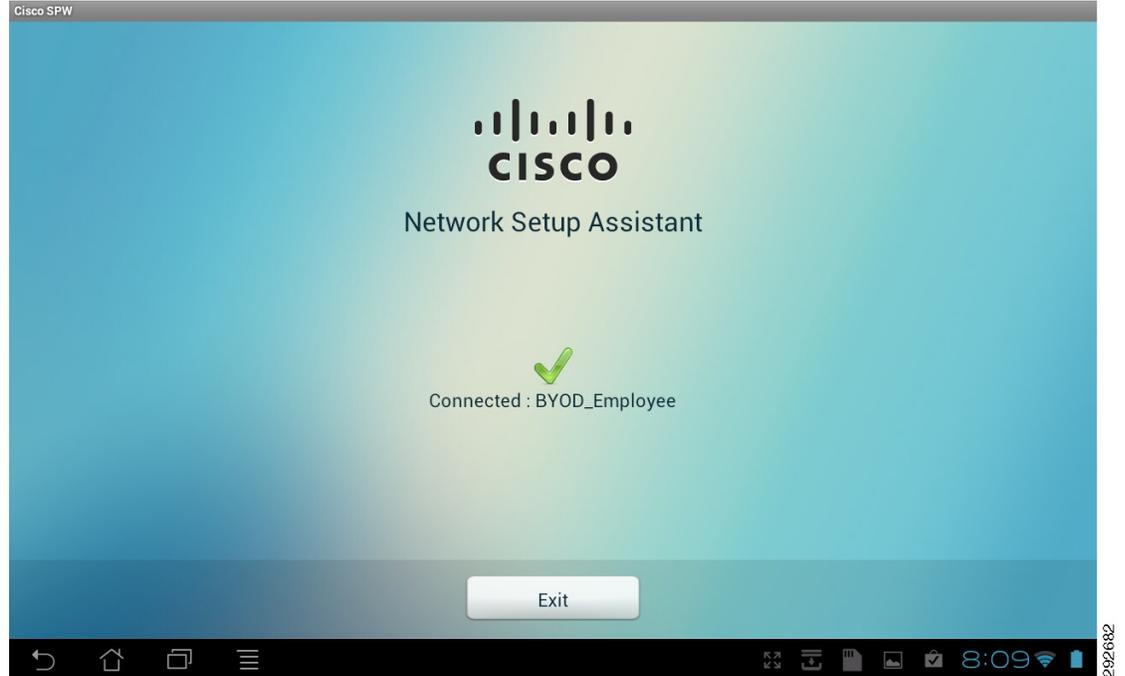
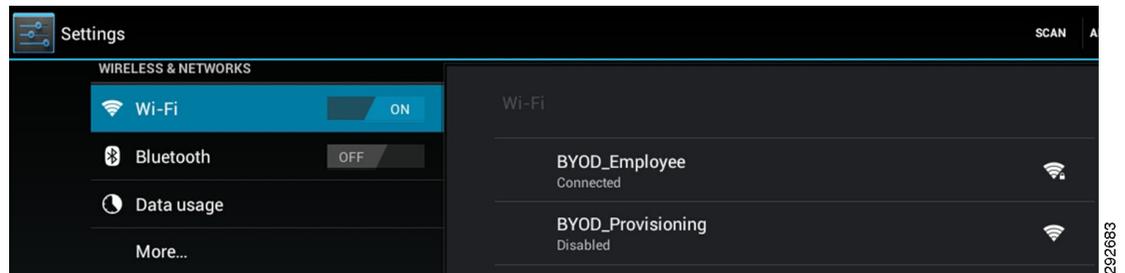
Figure 19-11 Automatic Connection to BYOD_Employee

Figure 19-12 shows how the device is automatically connected to the secure BYOD_Employee SSID.

Figure 19-12 BYOD_Employee Secure SSID

Windows Devices

The user experience while provisioning a Windows device is very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

Some Windows devices have multiple network adapters, for example, a laptop with both wired and wireless adapter. The network security policy checks that the device mac-address (sent using calling-station-id attribute) matches the SAN field of the device digital certificate before allowing access. This is done to prevent spoofing. Since each adapter has a unique mac-address, the anti-spoofing policy check can cause difficulties for devices with multiple adapters. If a device registers with a wired adapter, it will obtain a digital certificate with the mac-address of the wired adapter. If the same device attempts to later authenticate to the secure wireless network, most operating systems will attempt to the

use the wired adapter certificate for authentication and will fail because the mac-address of the wireless adapter will not match the SAN field of the digital certificate. To avoid this problem, a device with multiple adapters must register both the wired and wireless adapter.

There are two methods for provisioning wireless devices:

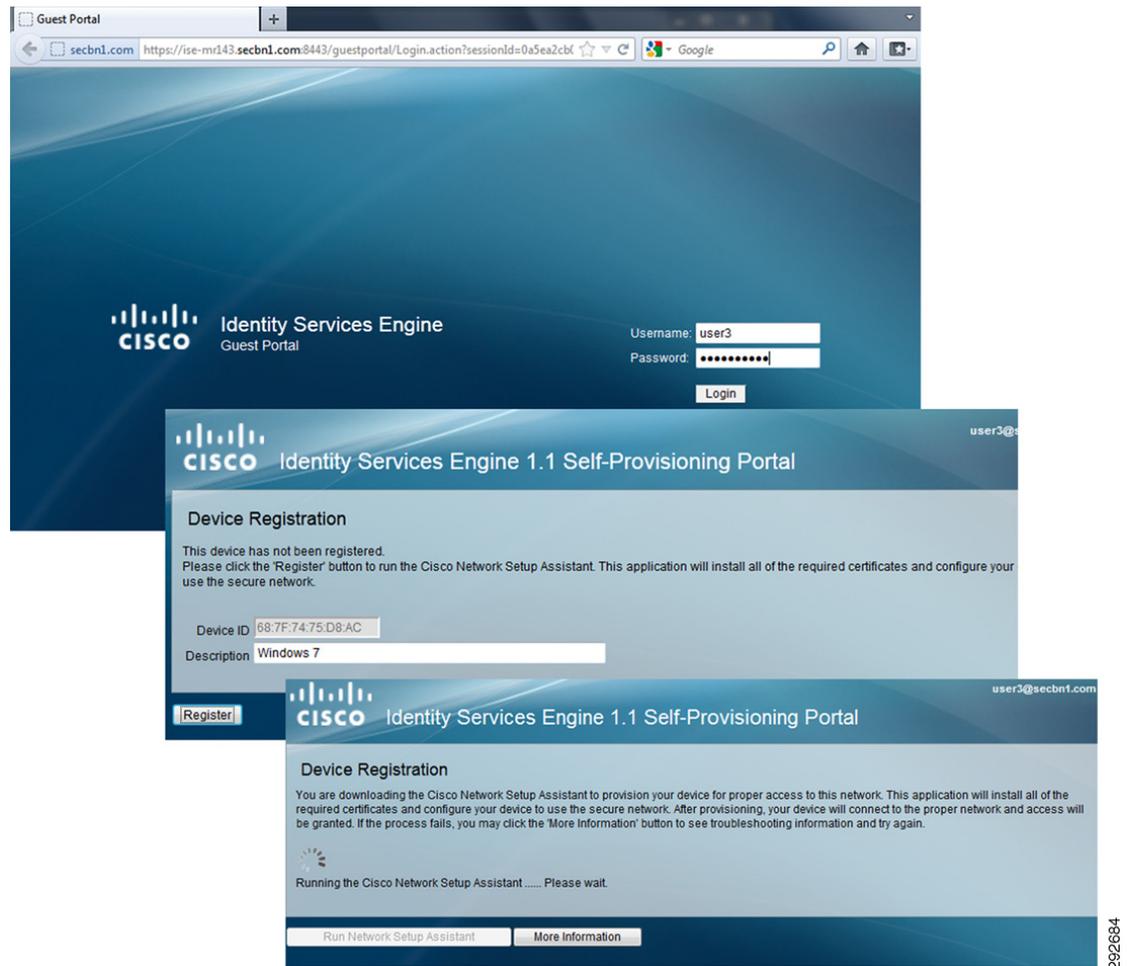
- Dual SSID model, which supports MAB on the provisioning SSID and dot1X on the employee SSID.
- Single SSID model, which supports only the dot1X protocol.

For the Dual SSID method, the wired and wireless adapters may be provisioned in any order. For example, if the device associates with the provisioning SSID (which supports MAB) and is successfully provisioned, then subsequently connects with the wired adapter, 802.1X will fail because of the anti-spoofing check in the policy and the user will be re-directed to complete the provisioning process. Thereafter, the device can access the network with either adapter.

For the Single SSID method, the order in which the wired and wireless adapters are provisioned matters. For example, if the device connects using the wired adapter first and is successfully provisioned, then subsequently connects using the wireless adapter, some operating systems attempt to establish a EAP-TLS connection using the wired digital certificate instead of undergoing the provisioning process. This connection attempt will fail because of the anti-spoofing check in the policy. To prevent this from happening, the user must provision the wireless adapter before connecting with the wired adapter for the single SSID method.

Windows Wireless Devices

After authenticating at the portal and entering a description for the new Windows device, the SPW is downloaded.

Figure 19-13 Guest Registration Portal

The SPW is launched to install the profile, the keys are generated, and the certificate enrollment takes place.

The SPW installs the BYOD_Employee configuration to connect to the secure SSID. The connection is switched automatically to the BYOD_Employee SSID.

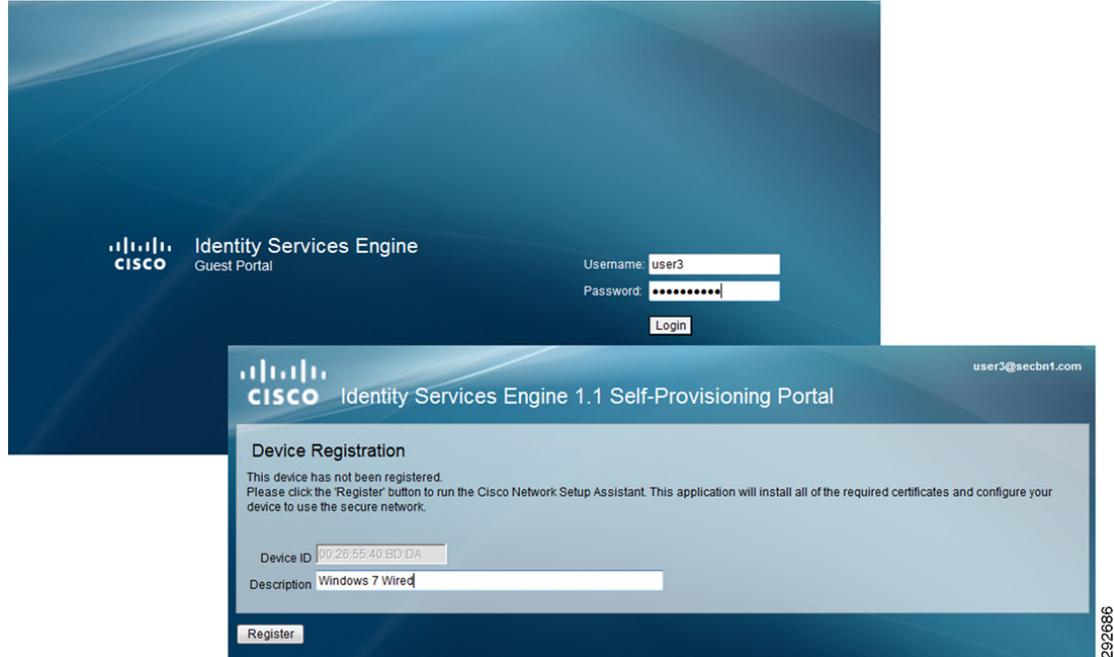
Figure 19-14 SPW and Connection to Secure SSID



Windows Wired Devices

The user experience is very similar, but instead of configuring access to a secure SSID, the SPW configures the devices to connect via a wired connection.

Figure 19-15 Guest Registration Portal



The SPW is downloaded and the proper configurations are applied to the device.

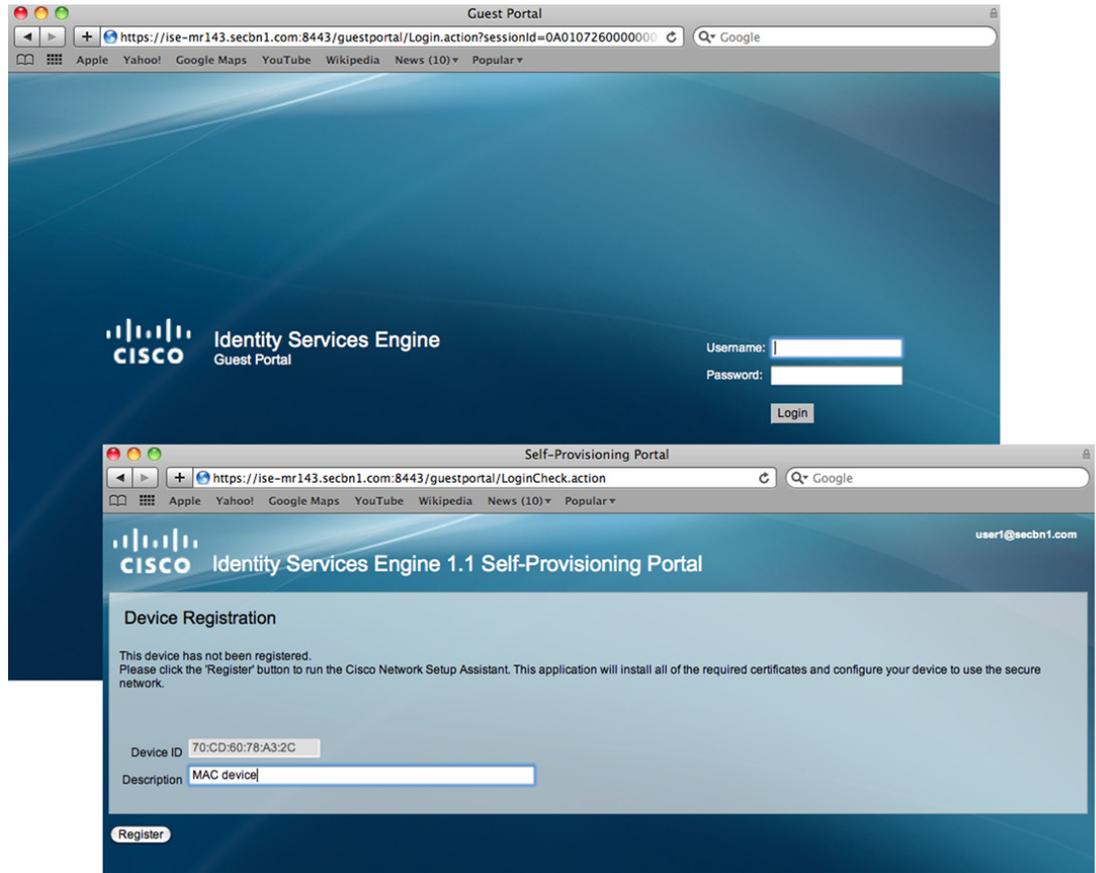
Figure 19-16 SPW and Secure Access



Mac OS/X Devices

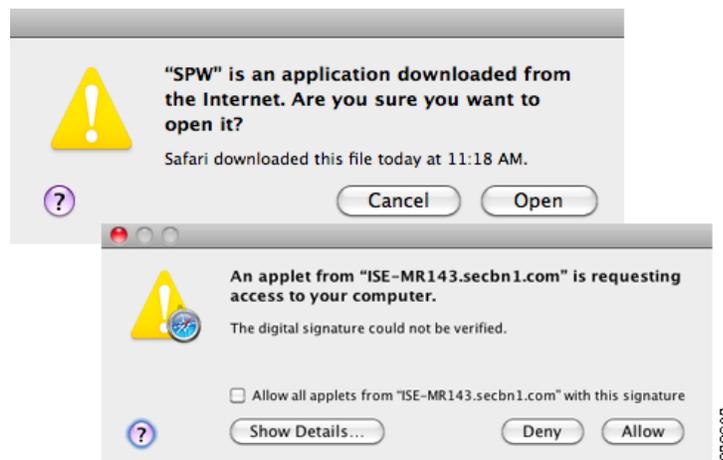
The user experience while provisioning a Mac OS X wired device is also very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

Figure 19-17 Guest Registration and Self-Registration Portals

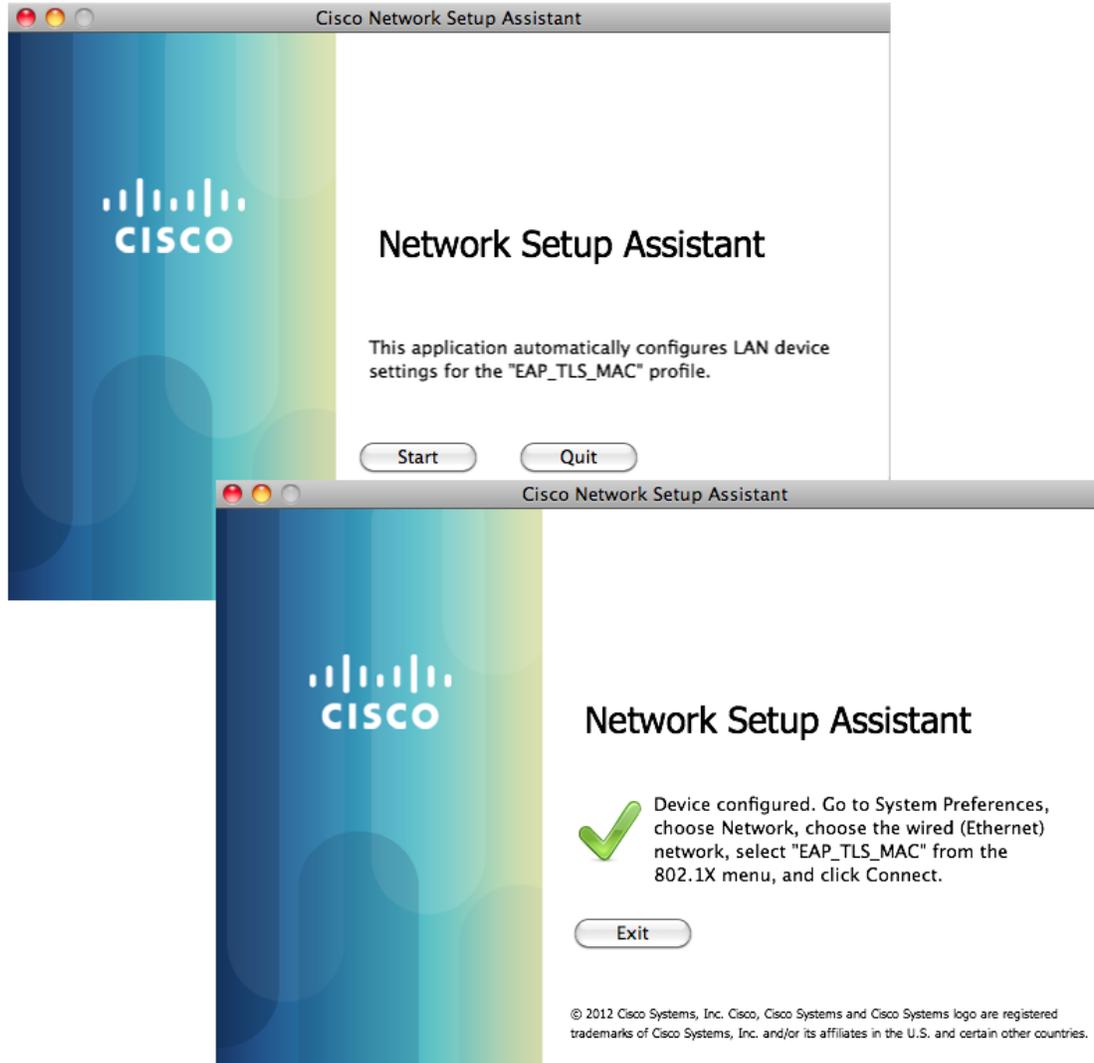


The SPW is downloaded and installed.

Figure 19-18 SPW and Secure Access



The Network Setup Assistant configures the EAP-TLS_MAC profile for secure access.

Figure 19-19 Network Setup Assistant

The network settings in [Figure 19-20](#) show the new EAP_TLS_MAC configuration.

Figure 19-20 Network Settings

