USER GUIDE TO SIMPLIFYING

BYOD with Ruckus

Introduction

Like hot and cold, secure BYOD implementations and ease of use have traditionally been mutually exclusive. Some networking products are intuitive to IT administrators, but they lack the necessary features to solve problems or protect corporate users and data. Other products have all the advanced security, filtering, and access control knobs a government agency could ask for, but no one can figure out how to use them.

This application note describes the technology used and then outlines the steps for how to quickly and easily configure our ZoneFlex system with the right blend of flexibility, security, and simplicity to support BYOD. Instead of adding complexity, we've created smarter security and connectivity mechanisms that ease management and implementation burdens, particularly for mobile devices. In this guide, we'll outline how the following features help streamline a BYOD paradigm:

1. **Dynamic Pre-Shared Key** — Per-user credentials with WPA2-Personal — the best of both worlds
2. **Zero-IT Activation** — Easy, secure onboarding and auto-configuration of client devices
3. **Role-Based Access Control** — Easy ways to manage user connectivity and network authorization.

Strong Security with Dynamic Pre-Shared Key

What is DPSK?

In a traditional WPA2-Personal network, all users on the WLAN share the same passphrase. Dynamic PreShared Key (DPSK) is patented technology that enables unique PSK credentials for each user on the same network. DPSK was developed to provide secure wireless access while eliminating the burdens of manual device configuration and the security drawbacks of shared PSKs.

What are the benefits?

The traditional PSK model (WPA2-Personal) is great for home networks and small offices with only a few users. However, as organizations seek better security or differentiated network policies for each user type, the limitations of a shared PSK become evident pretty quickly. Perhaps the most troublesome problem is passphrase exposure, passphrase sharing, and change management policies. If an employee leaves the organization, the passphrase must be changed and all devices reconfigured.

On the opposite side, WPA2-Enterprise is "recommended," but IT administrators have varying comfort levels with 802.1X and EAP. In turn, many businesses do not implement it. Most companies would like to use 802.1X, but often avoid it because of:

- Lack of expertise
- Lack of time
- Lack of budget
- Lack of backend systems (e.g. AAA server, user database, certificate management)
- Failure to see technical advantages

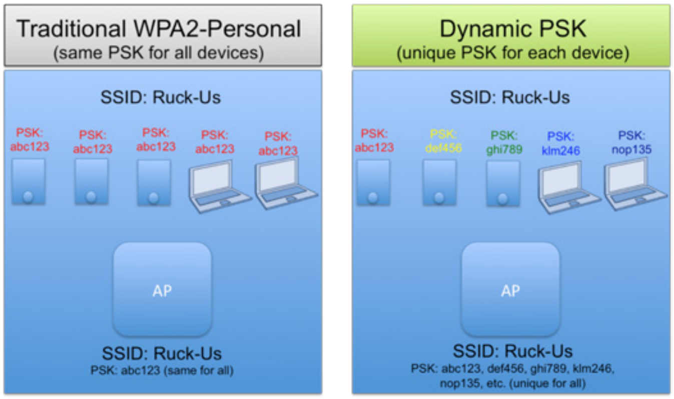
Many organizations don't realize that there is a good alternative to traditional PSKs and 802.1X. DPSK sits right in the happy middle with some of the best advantages of both WPA2-Personal and WPA2-Enterprise:

- Easy to use and administer. Users understand passphrases, but they don't understand 802.1X.
- DPSKs are bound to a specific user/device. Even if PSKs are shared or exposed, they will not work with other devices.
- Compromised DPSKs do not jeopardize all users.
- Single DPSKs can be revoked without impact on the rest of the network.

- DPSKs prevent one valid user from decrypting traffic of other valid users.
- Provides per-user credentials and policies
- Avoids common 802.1X hurdles:
  - — No dependency on RADIUS or backend user databases
  - — No certificates
  - — No complex configuration

How does it work?

Dynamic PSK creates a unique 62-byte preshared key for each device. The PSK is used for network access as well as to create encryption keys, which are unique for each user. DPSKs can be created in bulk and manually distributed to users and devices, or the ZoneDirector can auto-configure devices with a DPSK when they connect to the network for the first time.



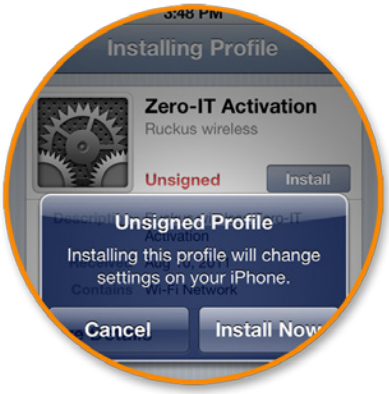
By offering different ways to implement the feature, Ruckus provides the flexibility to bring DPSKs to networks in a way that is secure, intuitive, and IT friendly. Since we're focused on solving BYOD trouble spots, let's look at using DPSK with a unique Ruckus feature called Zero-IT Activation.

Note: The batch DPSK tool is a manual way to create and manage DPSK credentials and users; if that adds value for your unique BYOD situation, see **Appendix A** for step-by-step instructions.

Flexible Onboarding with Zero-IT Activation

What is Zero-IT Activation?

Zero-IT Activation is a unique wireless onboarding feature that enables wireless users to securely access the network without IT staff intervention. Zero-IT works in concert with the DPSK solution, automatically creating and deploying DPSKs to valid users when they connect for the first time



Unsigned Profile

Installing this profile will change settings on your iPhone.

How does it work?

Zero-IT activation automates the DPSK generation and client device configuration steps. When a user connects for the first time, the user enters his/her username/password and downloads a configuration file for their machine. The user runs the configuration file and Zero-IT configures the client machine with a WLAN profile, including a unique PSK. Zero-IT prepares the machine to re-connected to the correct network.

What are the benefits?

Zero-IT offers all of the security benefits of DPSK along with intuitive and flexible onboarding:

- Zero touch wireless configuration of laptops and smart mobile devices
- Support for iPad/iPhone, Android, Mac OS X, Windows XP, Vista, and 7, and Mobile/CE
- One-time device configuration
- Easy for IT staff to setup and maintain
- Unique 62-byte preshared keys generated and automatically installed per device
- Easily deactivated by IT staff if user is no longer valid
- New keys can be generated on-demand
- Can integrate with existing user directories

Configuring and Using Zero-IT Activation

Configuring and using Zero-IT Activation is simple.

1. Start by creating a new WLAN for secure connectivity. Navigate to the **Configure** tab in the ZoneDirector UI and then select **WLANs** in the left pane. When the WLANs page is open, select **Create New** to make a new WLAN.

2. Configure the WLAN as follows:

   Name/ESSID = DPSK-ZERO-IT
   Description = Enter a useful description or leave blank
   Authentication Method = Open
   Encryption Method = WPA2
   Algorithm = AES
   Password = Enter a long, complex passphrase
   (this will not be given to users)
   Zero-IT Activation = Enabled
   Dynamic PSK = Enabled

In the **Advanced Options**, we can also specify VLAN settings for this WLAN. If we want to match this WLAN to a specific VLAN, we can do so. Or, we can assign different users to different VLANs. This is useful if we have VLAN policies on the wired network and we want to extend those policies to our wireless users.

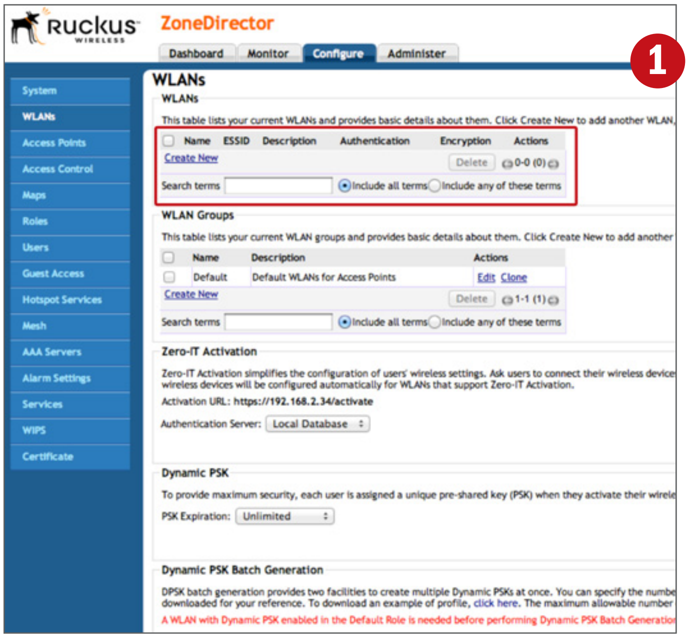
   ACCESS VLAN = Enter VLAN ID (default = 1)
   Enable Dynamic VLAN = Enabled (check in box)

3. Only valid users can receive a DPSK with Zero-IT Activation. To determine which users are valid, we need to decide what user database we'll use for Zero-IT authentication. Scroll near the bottom of the WLANs page where you'll find the Zero-IT authentication server settings and the Zero-IT URL (make a note of the URL).

   Select **Local Database.** (If integrating with an existing user database, this is where we would select our AD or LDAP database)

   Click **Apply** (far right corner, not shown).

   Below the Zero-IT authentication server settings is a configuration section for DPSK expiration. If desired, set a PSK lifetime after which the DPSK will expire.



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN,

□	Name	ESSID	Description	Authentication	Encryption	Actions
Create New					Delete	0-0 (0)

Search terms ● Include all terms ○ Include any of these terms

WLAN Groups

This table lists your current WLAN groups and provides basic details about them. Click Create New to add another

□	Name	Description	Actions
□	Default	Default WLANs for Access Points	Edit Clone
Create New		Delete	1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

Zero-IT Activation

Zero-IT Activation simplifies the configuration of users' wireless settings. Ask users to connect their wireless device
wireless devices will be configured automatically for WLANs that support Zero-IT Activation.

Activation URL: https://192.168.2.34/activate

Authentication Server: Local Database

Dynamic PSK

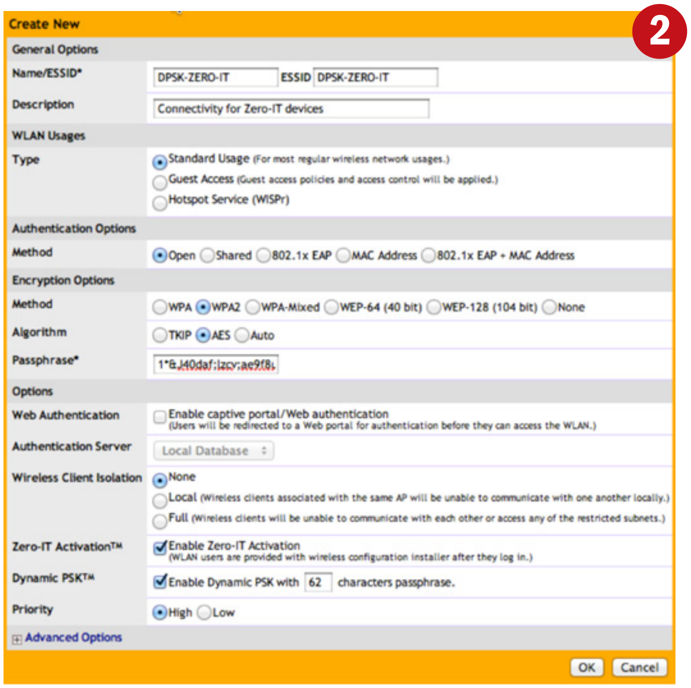
To provide maximum security, each user is assigned a unique pre-shared key (PSK) when they activate their wirele

PSK Expiration: Unlimited

Dynamic PSK Batch Generation

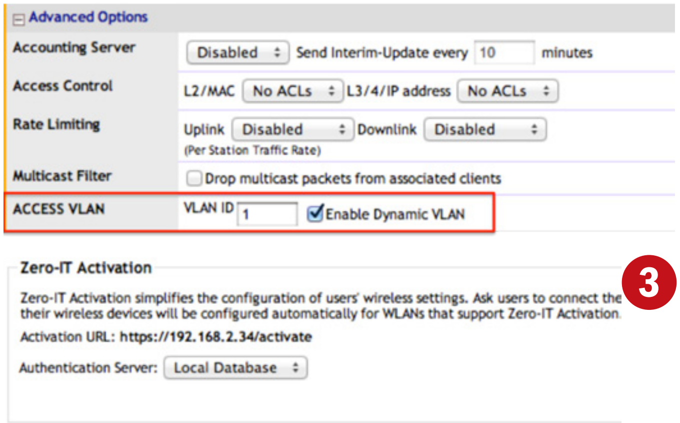
DPSK batch generation provides two facilities to create multiple Dynamic PSKs at once. You can specify the numbe
downloaded for your reference. To download an example of profile, click here. The maximum allowable number

A WLAN with Dynamic PSK enabled in the Default Role is needed before performing Dynamic PSK Batch Generatio



Create New

General Options	
Name/ESSID*	DPSK-ZERO-IT ESSID DPSK-ZERO-IT
Description	Connectivity for Zero-IT devices
WLAN Usages	
Type	● Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ○ Hotspot Service (WISPr)
Authentication Options	
Method	● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Encryption Options	
Method	○ WPA ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None
Algorithm	○ TKIP ● AES ○ Auto
Passphrase*	1*&J40daf;lzcy;ae9f8
Options	
Web Authentication	□ Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.)
Authentication Server	Local Database
Wireless Client Isolation	● None ○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.) ○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)
Zero-IT Activation™	☑ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Dynamic PSK™	☑ Enable Dynamic PSK with 62 characters passphrase.
Priority	● High ○ Low
⊞ Advanced Options	



⊟ Advanced Options	
Accounting Server	Disabled Send Interim-Update every 10 minutes
Access Control	L2/MAC No ACLs L3/4/IP address No ACLs
Rate Limiting	Uplink Disabled Downlink Disabled (Per Station Traffic Rate)
Multicast Filter	□ Drop multicast packets from associated clients
ACCESS VLAN	VLAN ID 1 ☑ Enable Dynamic VLAN

Zero-IT Activation

Zero-IT Activation simplifies the configuration of users' wireless settings. Ask users to connect the
their wireless devices will be configured automatically for WLANs that support Zero-IT Activation.

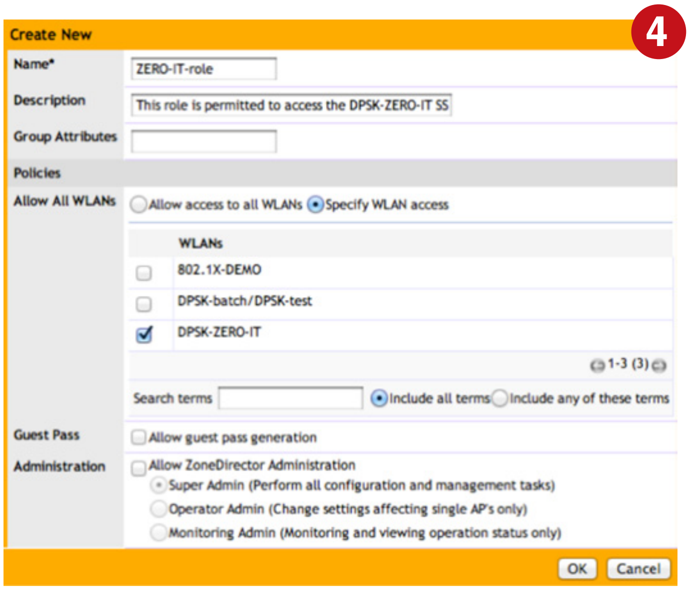
Activation URL: https://192.168.2.34/activate

Authentication Server: Local Database

4. Now create a user group that is permitted to access this WLAN. Select Roles from the left-hand side. Create a new role.

   Name = ZERO-IT-role
   Description = Enter a useful description or leave blank
   Specify WLAN access = Enable the DPSK-ZERO-IT WLAN
   Click **OK.**

4



Create New

Name*	ZERO-IT-role
Description	This role is permitted to access the DPSK-ZERO-IT SS
Group Attributes	
Policies	
Allow All WLANs	○ Allow access to all WLANs ● Specify WLAN access

	WLANs
□	802.1X-DEMO
□	DPSK-batch/DPSK-test
☑	DPSK-ZERO-IT

1-3 (3)

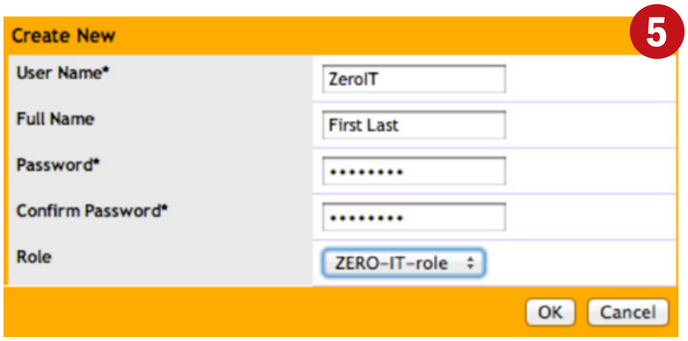
Search terms ● Include all terms ○ Include any of these terms

Guest Pass	□ Allow guest pass generation
Administration	□ Allow ZoneDirector Administration ● Super Admin (Perform all configuration and management tasks) ○ Operator Admin (Change settings affecting single AP's only) ○ Monitoring Admin (Monitoring and viewing operation status only)

5. Use the ZoneDirector's local database and create a new user for this role. Select Users from the left-hand side. Create a new user.

   Name = ZeroIT
   Full Name = First Last
   Password = password
   Confirm Password = password
   Role = ZERO-IT-role
   Click **OK.**

5



Create New

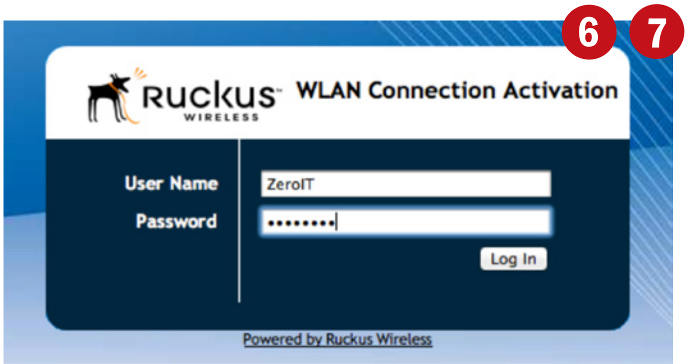
User Name*	ZeroIT
Full Name	First Last
Password*	••••••••
Confirm Password*	••••••••
Role	ZERO-IT-role

So a role has now been created that maps to the DPSK-ZERO-IT WLAN and then we've created a user that belongs to this role. When this user enters his/her username/password, the ZoneDirector will assign a unique DPSK with permission to access the DPSK-ZERO-IT network.

6. To connect a client device, plug in to an Ethernet port with access to the ZoneDirector's subnet/VLAN and use a Web browser to open the "activate" URL. The URL will always be the ZoneDirector IP address followed by **/activate** (e.g. https://192.168.2.34/activate). Note that the URL is TLS encrypted.

7. This Web page serves as the DPSK authentication portal to ensure you are a valid user. When the username/password (ZeroIT / password) created in step 5 is entered, the ZoneDirector will determine the proper role and provision the client accordingly.

6 7

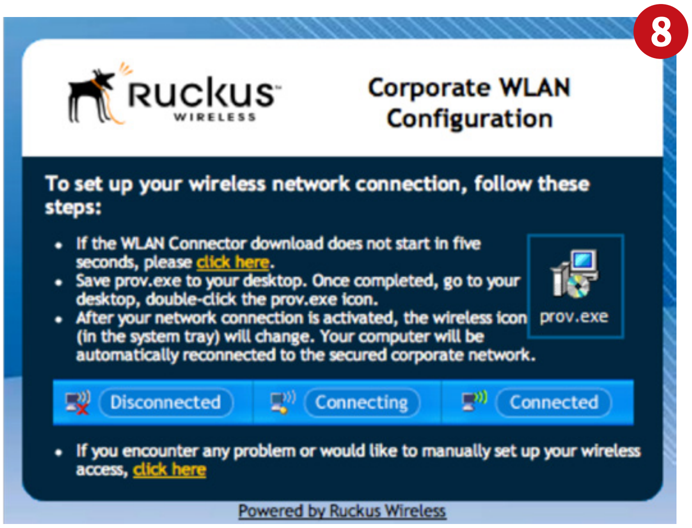


WLAN Connection Activation

User Name	ZeroIT
Password	••••••••

8. Successful authentication will launch a file download called "prov.exe," "prov.apk," or "prov.mobileconfig," depending on the OS type.

8



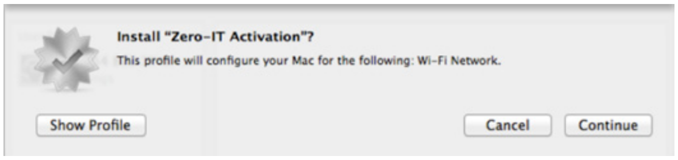
Corporate WLAN Configuration

To set up your wireless network connection, follow these steps:

- If the WLAN Connector download does not start in five seconds, please click here.
- Save prov.exe to your desktop. Once completed, go to your desktop, double-click the prov.exe icon.
- After your network connection is activated, the wireless icon (in the system tray) will change. Your computer will be automatically reconnected to the secured corporate network.

- If you encounter any problem or would like to manually set up your wireless access, click here

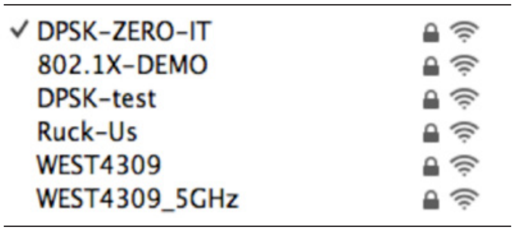
9. Open the file and Zero-IT will auto-configure the WLAN profile (may require administrator privileges).



Install "Zero-IT Activation"?

This profile will configure your Mac for the following: Wi-Fi Network.

10. The configuration script will also automatically connect the wireless client to the network on some devices.



✓ DPSK-ZERO-IT
802.1X-DEMO
DPSK-test
Ruck-Us
WEST4309
WEST4309_5GHz

Zero-IT simplifies network setup for new users, as you can see. Configuring ZoneDirector is straightforward for IT staff and the client experience is intuitive.

BYOD-Provisioning

Now it's important to look at device onboarding without Ethernet. Mobile phones and tablets are the primary devices driving the BYOD trend, but they lack wired interfaces. So there needs to be a way to securely provision them with a clean, intuitive workflow.

How does BYOD Provisioning work?

By relying on the Zero-IT Activation feature, a "provisioning" network can be easily created to automatically redirect users to the Zone Director's activate login screen. The open network is used only for device provisioning; after the ZoneDirector validates user credentials, mobile devices receive a configuration file that auto-configures the WLAN connection manager and re-connects them on the proper WLAN.

Configuring and Using Zero-IT Activation for BYOD

The BYOD setup for this is quite similar to the previous wired Zero-IT setup. In fact, it relies on the DPSK-ZERO-IT SSID already created for device connectivity. Think of *that* WLAN as the corporate network. Now simply create a second WLAN that will serve as our provisioning network.

To start, within the ZoneFlex system, define a new Hotspot Service to use for wireless provisioning. Hotspot Services are a way to control network access on open networks. This helps ensure that the provisioning network is used only for provisioning.

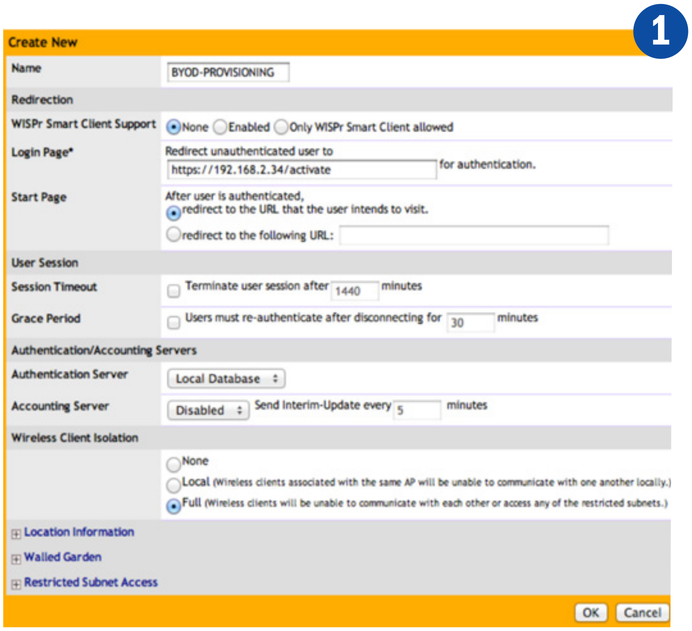
1. Find the Hotspot Services section on the left-hand side and select it. In the main screen, create a new Hotspot Service

   Name = BYOD-PROVISIONING

   Login Page = https://xx.xx.xx.xx/activate, where xx.xx.xx.xx is the IP address of the Zone Director (e.g. https://192.168.2.34/activate). This is the page to which ZoneDirector will redirect users for authentication.

   Authentication Server = Local Database

   Wireless Client Isolation =Full



Create New

Name: BYOD-PROVISIONING

Redirection

WISPr Smart Client Support: ● None ○ Enabled ○ Only WISPr Smart Client allowed

Login Page*: Redirect unauthenticated user to https://192.168.2.34/activate for authentication.

Start Page: After user is authenticated,
● redirect to the URL that the user intends to visit.
○ redirect to the following URL:

User Session

Session Timeout: □ Terminate user session after 1440 minutes

Grace Period: □ Users must re-authenticate after disconnecting for 30 minutes

Authentication/Accounting Servers

Authentication Server: Local Database

Accounting Server: Disabled Send Interim-Update every 5 minutes

Wireless Client Isolation

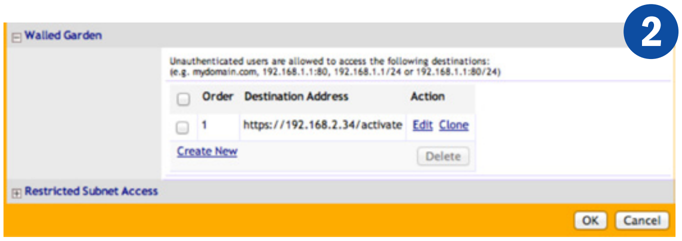
○ None
○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)
● Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

2. It's also important to configure a "walled garden," which is a way to limit the network access on the Open network so it can only be used for provisioning. To do so, expand the walled garden configuration section in our BYOD-PROVISIONING Hotspot Services profile.

   Create a New rule.

   Enter the **"activate" URL** (https://192.168.2.34/activate) address here and **click save**.

   Click OK to save this Hotspot Service.



2

⊟ Walled Garden

Unauthenticated users are allowed to access the following destinations:
(e.g. mydomain.com, 192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

□	Order	Destination Address	Action
□	1	https://192.168.2.34/activate	Edit Clone

3. Now create a new WLAN to offer these Hotspot Services. Navigate back to the WLANs page and create a new WLAN.

Name/ESSID = BYOD-PROVISIONING

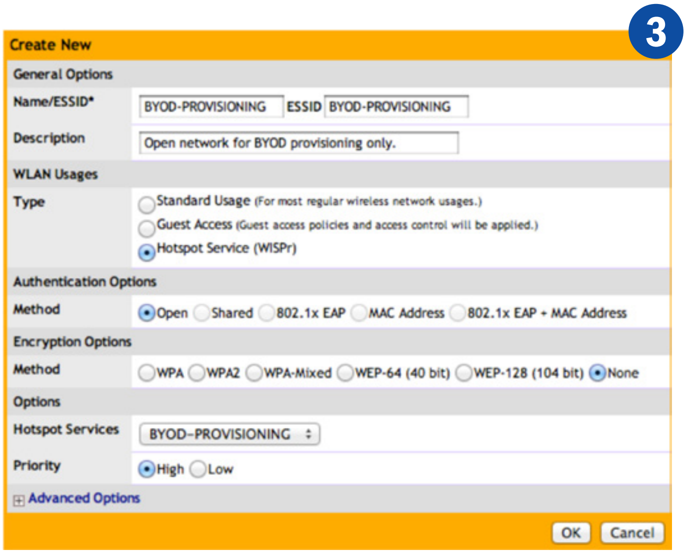
Description = Enter a useful description or leave blank

Type = Hotspot Service (WISPr)

Authentication Method = Open

Encryption Method = None

Hotspot Services = Select BYOD-PROVISIONING from the list.



3

Create New

General Options

Name/ESSID* BYOD-PROVISIONING ESSID BYOD-PROVISIONING

Description Open network for BYOD provisioning only.

WLAN Usages

Type ○ Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ● Hotspot Service (WISPr)

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Hotspot Services BYOD-PROVISIONING

Priority ● High ○ Low

4. In the wired DPSK with Zero-IT demo, a Role titled ZERO-IT-role was already created. This role has permission to access the DPSK-ZERO-IT SSID. Confirm that this role is still present.

5. Now create a new mobile user in the local database that will be a member of the Zero-IT role.

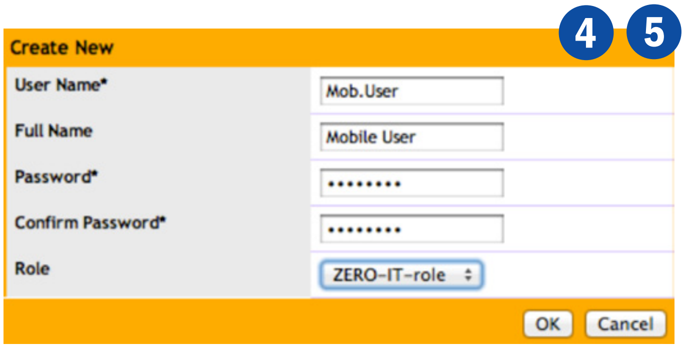
User Name = Mob.User

Full Name = Mobile User

Password = password

Confirm Password = password

Role = ZERO-IT-role

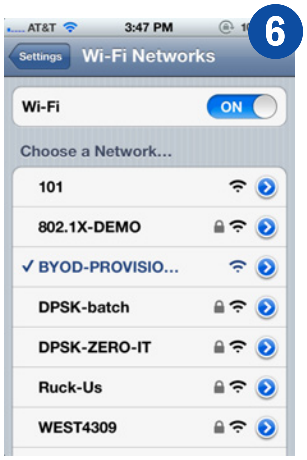


4 5

Create New

User Name*	Mob.User
Full Name	Mobile User
Password*	••••••••
Confirm Password*	••••••••
Role	ZERO-IT-role

6. Now everything is ready to onboard this user and his/her devices.
   a. With a mobile device (iphone shown here), connect to the BYOD-PROVISIONING SSID.
   b. Launch the browser and the URL redirect will occur, taking you to the connection activation page.
   c. Login with the Mob.User user credentials created in step 5.
   d. Successful login will launch the auto-configuration profile. Install the profile.
   e. Now connect to the corporate WLAN (i.e. DPSK-ZERO-IT)



6

AT&T 3:47 PM

Settings Wi-Fi Networks

Wi-Fi ON

Choose a Network...

101

802.1X-DEMO

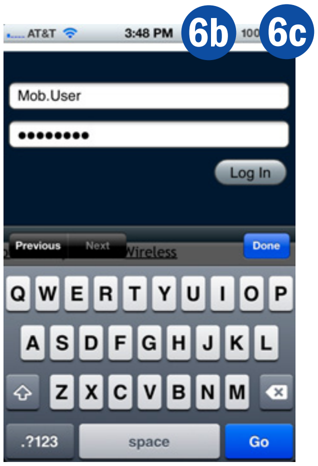
✓ BYOD-PROVISIO...

DPSK-batch

DPSK-ZERO-IT

Ruck-Us

WEST4309

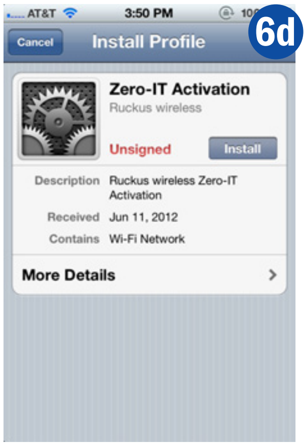


6b 6c

AT&T 3:48 PM 100

Mob.User

••••••••



6d

AT&T 3:50 PM 100

Cancel Install Profile

Zero-IT Activation

Ruckus wireless

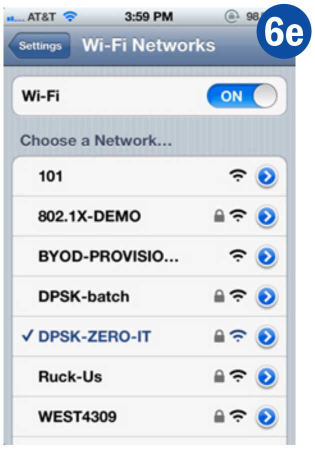
Unsigned Install

Description Ruckus wireless Zero-IT Activation

Received Jun 11, 2012

Contains Wi-Fi Network

More Details



6e

AT&T 3:59 PM 98

Settings Wi-Fi Networks

Wi-Fi ON

Choose a Network...

101

802.1X-DEMO

BYOD-PROVISIO...

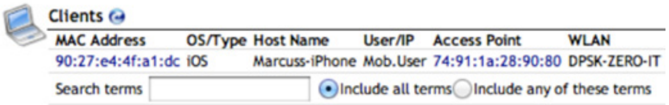
DPSK-batch

✓ DPSK-ZERO-IT

Ruck-Us

WEST4309

7. Using the ZoneDirector's Monitor tab, currently active clients can be easily viewed to check on users. Here, the connected iPhone, the MAC address binding, the user name of the connected user, and some device specific information are all visible. Even with a long list of users, it is easy to find specific clients using the search field.



Clients

MAC Address	OS/Type	Host Name	User/IP	Access Point	WLAN
90:27:e4:4f:a1:dc	iOS	Marcuss-iPhone	Mob.User	74:91:1a:28:90:80	DPSK-ZERO-IT

Search terms ● Include all terms ○ Include any of these terms

The Zero-IT tool creates a quick and easy way to deploy wireless networks and get users connected. Now we'll examine how to use Zero-IT with role-based access to grant network privileges and keep the network properly segmented.

Role-Based Access

In conjunction with Zero-IT Activation and DPSK, Ruckus provides a straightforward way to apply roles to each user, granting access to WLAN policies and VLANs according to the user type. By granting access based on user roles, IT staff can extend specific permissions to users based on wired network design and policy.

So far, we've focused on the internal database of the ZoneDirector to create users, but in live networks, the ZoneDirector seamlessly integrates with an existing user database, such as Active Directory, Open Directory, OpenLDAP, or eDirectory to determine a user's role assignment. The internal database of the ZoneDirector can be used for this feature which is shown in this demo. We'll also discuss how you can use this feature with an external database.

Planning Role-Based Access

By relying on the Zero-IT Activation feature, the "provisioning" network automatically redirects users to the Zone Director's activate login screen.

The first planning step to take is to decide what types of users will use the network, what roles to create for those users, and what permissions should be assigned to these roles.

In this demo, we'll create a mock K-12 education scenario using the following roles:

- Administration
- Staff
- Student

We'll create corresponding WLANs and then map the users/roles to their proper WLAN.

The last step is to evaluate the current wired network as a baseline to decide to what VLAN user groups should be assigned.

If an external user database that has VLAN attributes is being used, this process can be completely automated by enabling the Dynamic VLAN assignment feature. This adds additional flexibility, allowing the use of a single WLAN for different user types.

As an example:

- Administration – VLAN 10
- Staff – VLAN 50
- Student – VLAN 80

Now configure it in the ZoneDirector.

Implementing Role-Based Access

Start by creating the requisite WLANs.

1. Navigate to the WLANs menu in the left pane and then create a new WLAN:

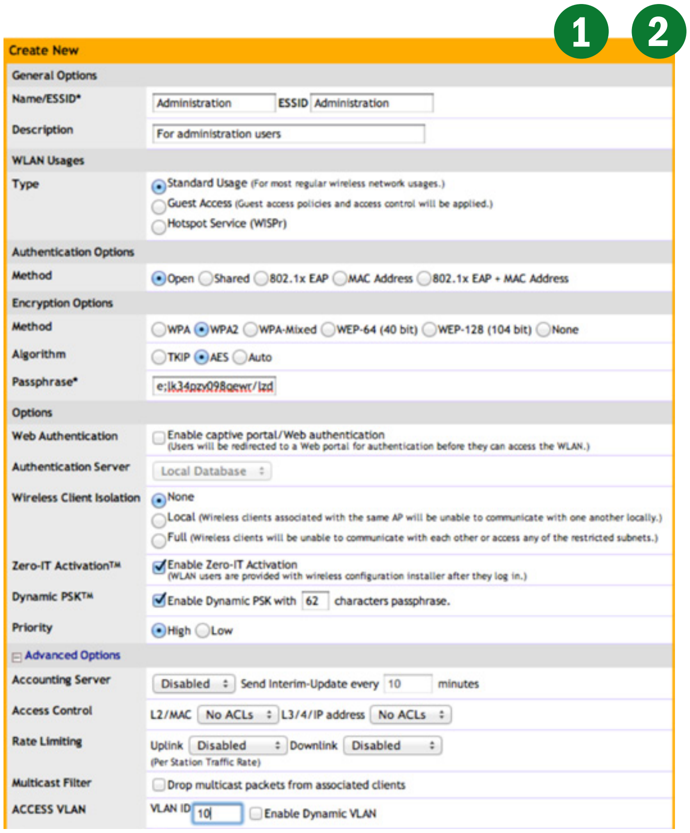
   Name/ESSID = Administration
   Description = Enter a useful description or leave blank
   Authentication Method = Open
   Encryption Method = WPA2
   Algorithm = AES
   Password = Enter a long, complex passphrase (this will not be given to users)
   Zero-IT Activation = Enabled
   Dynamic PSK = Enabled

   In Advanced Options,

   ACCESS VLAN = 10
   Click **OK.**

Now configure administrative users and roles so they are mapped to this WLAN, receiving administrator privileges and policies.

Note: If we're supporting multiple VLANs on each AP, we need to make sure our switch ports are configured to support those VLANs.



Create New

General Options

Name/ESSID*	Administration ESSID Administration
Description	For administration users

WLAN Usages

Type	● Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ○ Hotspot Service (WISPr)

Authentication Options

Method	● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method	○ WPA ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None
Algorithm	○ TKIP ● AES ○ Auto
Passphrase*	e;lk34pzv098qewr/lzd

Options

Web Authentication	□ Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.)
Authentication Server	Local Database
Wireless Client Isolation	● None ○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.) ○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)
Zero-IT Activation™	☑ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Dynamic PSK™	☑ Enable Dynamic PSK with 62 characters passphrase.
Priority	● High ○ Low

⊟ **Advanced Options**

Accounting Server	Disabled Send Interim-Update every 10 minutes
Access Control	L2/MAC No ACLs L3/4/IP address No ACLs
Rate Limiting	Uplink Disabled Downlink Disabled (Per Station Traffic Rate)
Multicast Filter	□ Drop multicast packets from associated clients
ACCESS VLAN	VLAN ID 10 □ Enable Dynamic VLAN

2. Create the **Staff** and **Student** WLANs with the same parameters, changing the VLAN ID accordingly (we'll skip the details here). For the student WLAN (or others, such as guests), you may wish to configure other advanced features:

   - Client Isolation (prevents valid users from communicating directly with one another through the AP) — this is recommended for guest and some student networks
   - Rate limiting policies
   - MAC or IP ACLs to limit network destinations

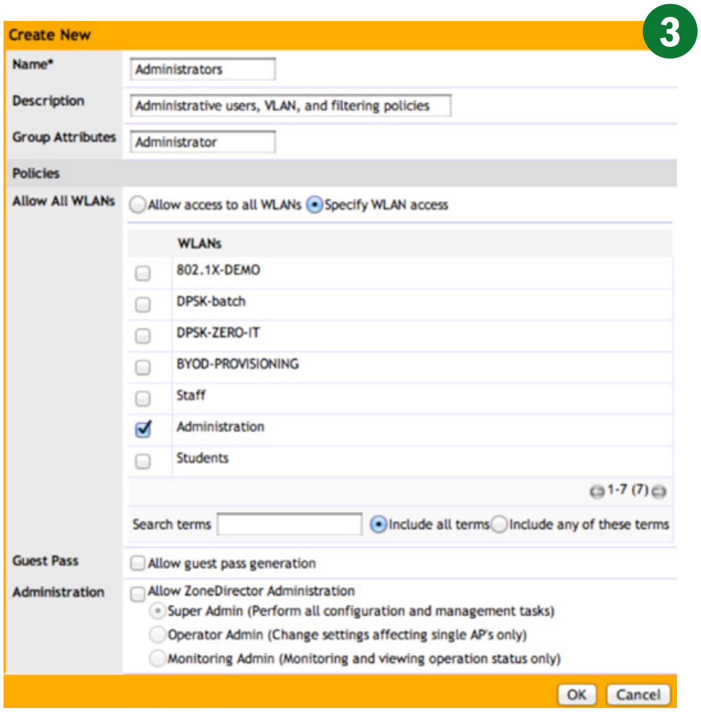
3. Now let's navigate to the **Roles** page and create our respective roles. **Create New**.

   Name = Administrators

   Description = Enter a useful description or leave blank

   WLAN Policies = Enable **Administration** WLAN

   Click OK.



Create New

Name*	Administrators
Description	Administrative users, VLAN, and filtering policies
Group Attributes	Administrator

Policies

Allow All WLANs	○ Allow access to all WLANs ● Specify WLAN access

	WLANs
□	802.1X-DEMO
□	DPSK-batch
□	DPSK-ZERO-IT
□	BYOD-PROVISIONING
□	Staff
☑	Administration
□	Students

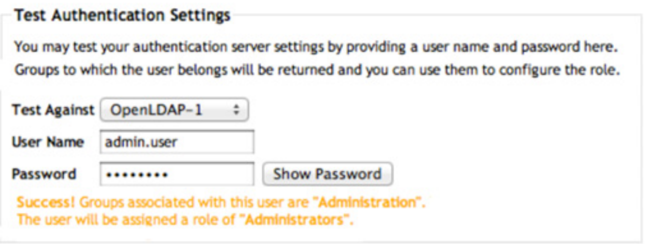
1-7 (7)

Search terms ● Include all terms ○ Include any of these terms

Guest Pass	□ Allow guest pass generation
Administration	□ Allow ZoneDirector Administration ● Super Admin (Perform all configuration and management tasks) ○ Operator Admin (Change settings affecting single AP's only) ○ Monitoring Admin (Monitoring and viewing operation status only)

The **Group Attributes** value for this role (shown above) can be set if integrating with an existing user database (e.g. AD, LDAP, etc.). When the ZoneDirector queries the database for authentication, the user's group attribute automatically maps the user to a ZoneDirector role.

To test this feature, use the **Test Authentication Settings** feature built into ZoneDirector (navigate to the AAA Servers menu). To show how it works in a live environment, we've setup an OpenLDAP user database with an administrative user. In the LDAP database, this user is mapped to an administrator group. In ZoneDirector, pick the database



Test Authentication Settings

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

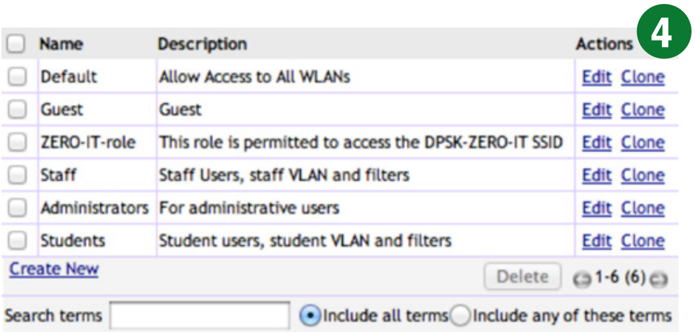
Test Against	OpenLDAP-1
User Name	admin.user
Password	••••••••

Success! Groups associated with this user are "Administration".
The user will be assigned a role of "Administrators".

and enter the credentials. This will test that the database is properly configured and that the user is assigned to the correct role.

As shown, this user authenticated successfully and was assigned to the Administrators role. Zero-IT would then provision this user's DPSK for the proper WLAN and VLAN.

4. Next, create the remaining roles. The role setup should be similar to previous setups.

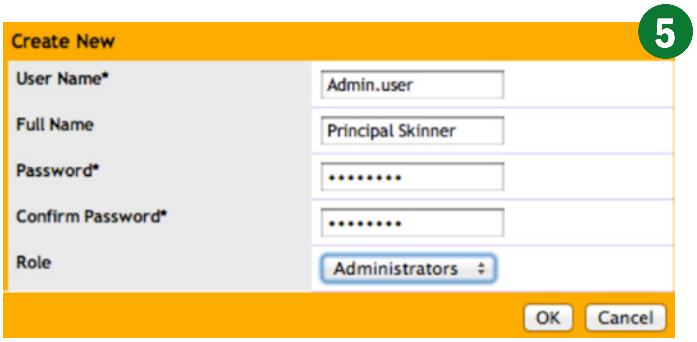


☐	Name	Description	Actions
☐	Default	Allow Access to All WLANs	Edit Clone
☐	Guest	Guest	Edit Clone
☐	ZERO-IT-role	This role is permitted to access the DPSK-ZERO-IT SSID	Edit Clone
☐	Staff	Staff Users, staff VLAN and filters	Edit Clone
☐	Administrators	For administrative users	Edit Clone
☐	Students	Student users, student VLAN and filters	Edit Clone

Create New Delete 1-6 (6)

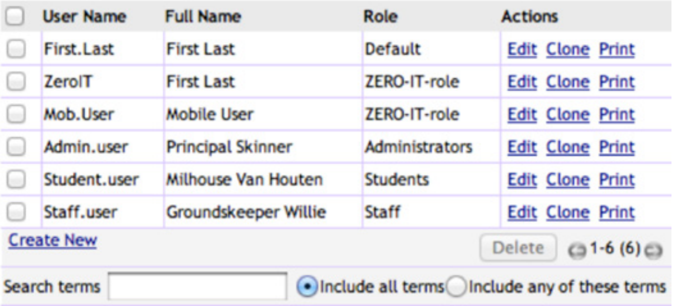
Search terms ● Include all terms ○ Include any of these terms

5. In the local database, we need to create our users next. Enter the name, password, and then select the correct role.



Create New

User Name*	Admin.user
Full Name	Principal Skinner
Password*	••••••••
Confirm Password*	••••••••
Role	Administrators

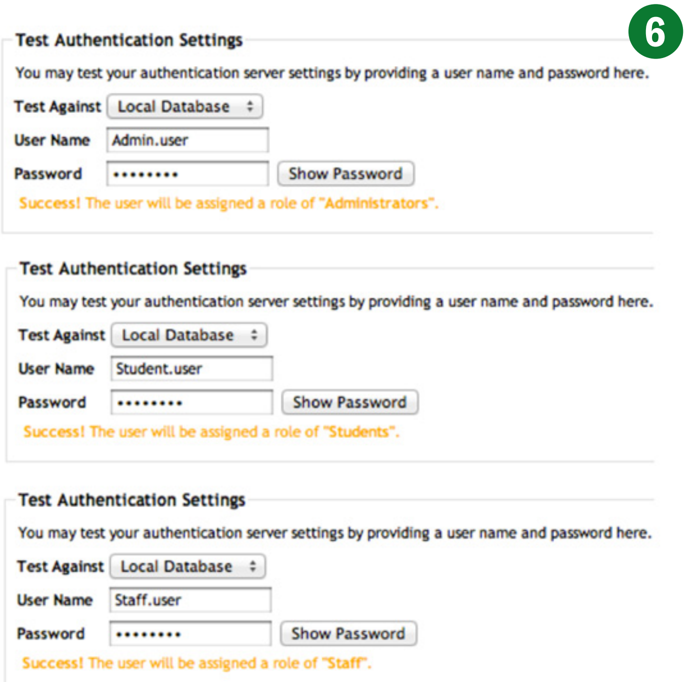


☐	User Name	Full Name	Role	Actions
☐	First.Last	First Last	Default	Edit Clone Print
☐	ZeroIT	First Last	ZERO-IT-role	Edit Clone Print
☐	Mob.User	Mobile User	ZERO-IT-role	Edit Clone Print
☐	Admin.user	Principal Skinner	Administrators	Edit Clone Print
☐	Student.user	Milhouse Van Houten	Students	Edit Clone Print
☐	Staff.user	Groundskeeper Willie	Staff	Edit Clone Print

Create New Delete 1-6 (6)

Search terms ● Include all terms ○ Include any of these terms

A user can be added for each of the roles (admin, staff, student). The final user list will look similar to this.



Test Authentication Settings

You may test your authentication server settings by providing a user name and password here.

Test Against: Local Database

User Name: Admin.user

Password: ••••••••

Success! The user will be assigned a role of "Administrators".

Test Authentication Settings

You may test your authentication server settings by providing a user name and password here.

Test Against: Local Database

User Name: Student.user

Password: ••••••••

Success! The user will be assigned a role of "Students".

Test Authentication Settings

You may test your authentication server settings by providing a user name and password here.

Test Against: Local Database

User Name: Staff.user

Password: ••••••••

Success! The user will be assigned a role of "Staff".

6. Now its important to test the authentication settings for each user to ensure that users will be placed in the proper role and WLAN during authentication.

That's it —role-based access control with Zero-IT activation. It's easy for IT staff, easy for users, and provides flexibility with user policies and segmentation.

Note: To explore this lab in greater detail, use a managed switch and a DHCP server. Create the VLANs on the switch and the DHCP scopes on the DHCP server for each VLAN. Connect a device to each WLAN (admin, staff, student) in turn. Observe the IP settings and VLAN access granted to each user type.

Summary

For organizations trying to solve BYOD challenges, it doesn't have to be complex and cumbersome. With easy to implement features like Zero-IT configuration, Dynamic PSK, and simplified role-based access control, enterprises can leverage their existing network resources to extend policies to their wireless users. Ruckus makes it painless to get users connected and provisioned with the correct network permissions. After that, we keep them happily connected with reliable RF performance.

Appendix A

Configuring and Using DPSK Batch Generation

The DPSK batch generation tool is a way to manually control per-user PSKs. This method of implementing DPSKs creates a DPSK file with multiple PSKs that can be offered to users or pre-configured on their devices. The onboarding process is similar to traditional WPA2-Personal networks, but it provides the added flexibility and security of DPSK.

1. Start by creating a new DPSK WLAN. Navigate to the **Configure** tab in the ZoneDirector UI and then select WLANs in the left pane. When the **WLANs** page is open, select **Create New** to make a new WLAN.

2. Configure the WLAN as follows:

   Name/ESSID = DPSK-batch

   Description = Enter a useful description or leave blank

   Authentication Method = Open

   Encryption Method = WPA2

   Algorithm = AES

   Password = Enter a long, complex passphrase (this will not be given to users)

   Zero-IT Activation = Enabled

   Dynamic PSK = Enabled

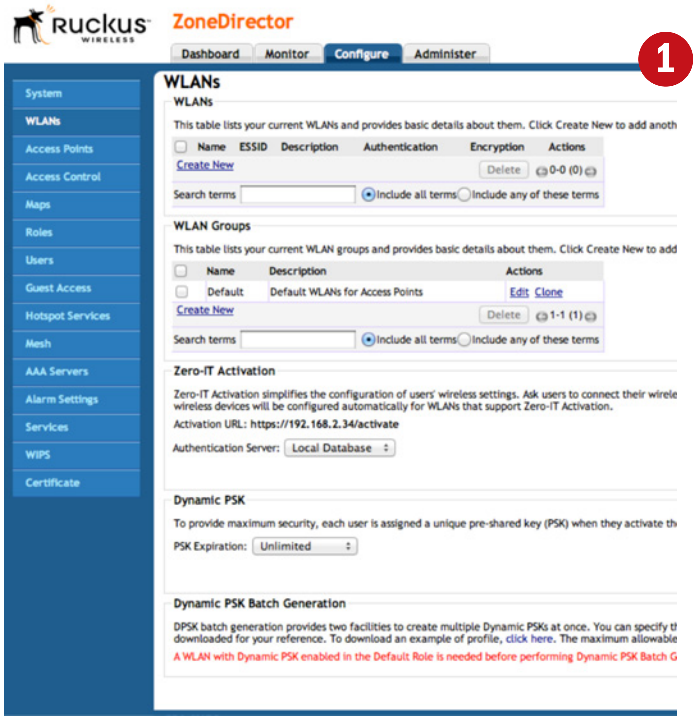
   Click **OK**.

In the advanced options, VLAN settings for this WLAN can also be specified. To match this WLAN to a specific VLAN or assign different users to different VLANs is simple. This is useful if we have authorization policies on the wired network and want to extend those policies to wireless users.

ACCESS VLAN = Enter VLAN ID (default = 1)

Enable Dynamic VLAN = Enabled (check in box)

3. While on the **WLANs** page, scroll to the **Dynamic PSK Batch Generation** section at the bottom.



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add anoth

□	Name	ESSID	Description	Authentication	Encryption	Actions

Create New Delete 0-0 (0)

Search terms ● Include all terms ○ Include any of these terms

WLAN Groups

This table lists your current WLAN groups and provides basic details about them. Click Create New to add

□	Name	Description	Actions
□	Default	Default WLANs for Access Points	Edit Clone

Create New Delete 1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

Zero-IT Activation

Zero-IT Activation simplifies the configuration of users' wireless settings. Ask users to connect their wirele
wireless devices will be configured automatically for WLANs that support Zero-IT Activation.

Activation URL: **https://192.168.2.34/activate**

Authentication Server: Local Database

Dynamic PSK

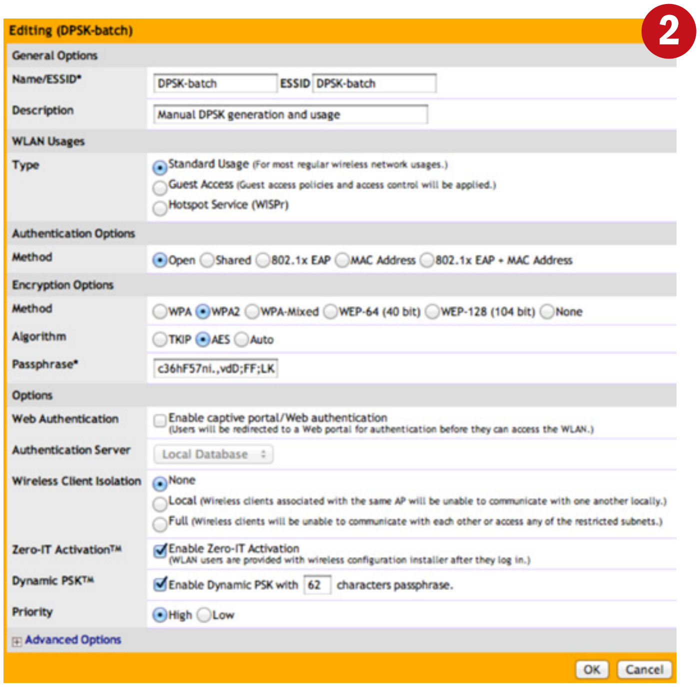
To provide maximum security, each user is assigned a unique pre-shared key (PSK) when they activate th

PSK Expiration: Unlimited

Dynamic PSK Batch Generation

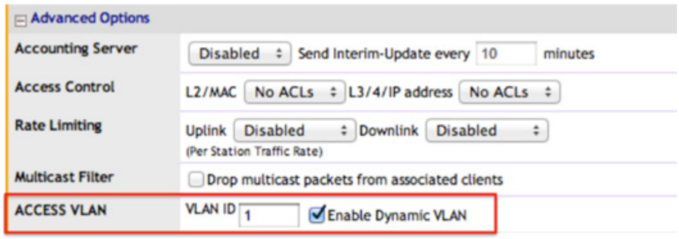
DPSK batch generation provides two facilities to create multiple Dynamic PSKs at once. You can specify t
downloaded for your reference. To download an example of profile, click here. The maximum allowable

A WLAN with Dynamic PSK enabled in the Default Role is needed before performing Dynamic PSK Batch G



Editing (DPSK-batch)

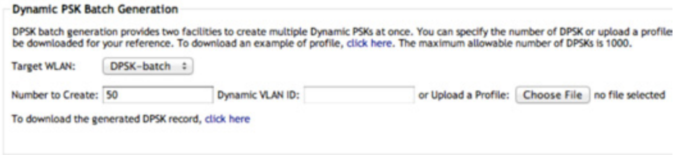
General Options	
Name/ESSID*	DPSK-batch ESSID DPSK-batch
Description	Manual DPSK generation and usage
WLAN Usages	
Type	● Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ○ Hotspot Service (WISPr)
Authentication Options	
Method	● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Encryption Options	
Method	○ WPA ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None
Algorithm	○ TKIP ● AES ○ Auto
Passphrase*	c36hF57ni.,vdD;FF;LK
Options	
Web Authentication	□ Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.)
Authentication Server	Local Database
Wireless Client Isolation	● None ○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.) ○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)
Zero-IT Activation™	☑ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Dynamic PSK™	☑ Enable Dynamic PSK with 62 characters passphrase.
Priority	● High ○ Low
⊞ Advanced Options	



⊟ Advanced Options	
Accounting Server	Disabled Send Interim-Update every 10 minutes
Access Control	L2/MAC No ACLs L3/4/IP address No ACLs
Rate Limiting	Uplink Disabled Downlink Disabled (Per Station Traffic Rate)
Multicast Filter	□ Drop multicast packets from associated clients
ACCESS VLAN	VLAN ID 1 ☑ Enable Dynamic VLAN

The DPSK batch tool is essentially an interface for creating DPSKs. If we have a list of users (and their MAC address and assigned VLANs), we can import a comma separated value (.csv) file here. Otherwise, we can let the ZoneDirector create a file for us with default usernames and the default VLAN. This tool has flexible options, but let's focus on a simple implementation for now.

4. Select the **DPSK-batch** WLAN from the drop-down list. This determines the SSID with which the generated DPSKs will work.



Dynamic PSK Batch Generation

DPSK batch generation provides two facilities to create multiple Dynamic PSKs at once. You can specify the number of DPSK or upload a profile
be downloaded for your reference. To download an example of profile, click here. The maximum allowable number of DPSKs is 1000.

Target WLAN: DPSK-batch

Number to Create: 50 Dynamic VLAN ID: or Upload a Profile: Choose File no file selected

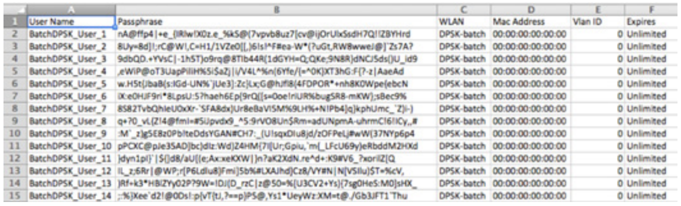
To download the generated DPSK record, click here

5. Enter the number of unique DPSK users to create (e.g. 50) and a VLAN ID if you want this set of users to be auto-assigned to a specific VLAN when they connect.

6. Click Generate in the bottom right corner (not shown in image above). You should see a message indicating success.

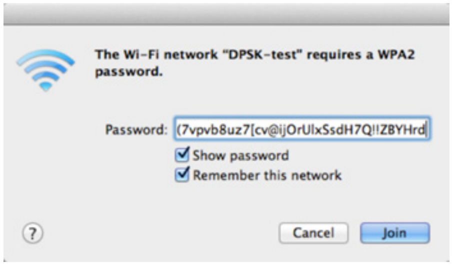
7. Click the link to download the generated DPSK record, which will launch the .csv file download. Open the file.

The default DPSK file has stock user names and empty MAC address bindings (we can customize these settings if we use the DPSK import tool). When a DPSK is used to connect to the network for the first time, the ZoneDirector will bind the device's MAC address to the DPSK.



	A	B	C	D	E	F
1	User Name	Passphrase	WLAN	Mac Address	Vlan ID	Expires
2	BatchDPSK_User_1	nA@ffp4|+e_(lRlw!X0z.e_%k5@(7vpvb8uz7[cv@ijOrUlxSsdH7Q!!ZBYHrd	DPSK-batch	00:00:00:00:00:00	0	Unlimited
3	BatchDPSK_User_2	8Uy=8d]!;rC@W!,C=H1/1VZeO[[,)6!s!^F#ea-W*(?uGt,RW8wweJ@]`Zs7A?	DPSK-batch	00:00:00:00:00:00	0	Unlimited
4	BatchDPSK_User_3	9dbQD.+YVsC|-1h5T)o9rq@8Tlb44R(1dGYH=Q;QKe;9N8R)dNCJSds()U_id9	DPSK-batch	00:00:00:00:00:00	0	Unlimited
5	BatchDPSK_User_4	,eWiP@oT3UapPilIH%5i$aZj|i/V4L^%n(6Yfe/(=^0K)XT3hG:F{?-z|AaeAd	DPSK-batch	00:00:00:00:00:00	0	Unlimited
6	BatchDPSK_User_5	w.H5t(JbaB(s:lGd-UN%`jUe3]:Zc}Lx;G@hJfl8(4FDPOR*+nh8K0Wpe(ebcN	DPSK-batch	00:00:00:00:00:00	0	Unlimited
7	BatchDPSK_User_6	iX:eOHJF9ri*8LpsU:5?haeh6Ep(9rQ([s=0oe!riUR%bugSR8-mKW};sBec9%	DPSK-batch	00:00:00:00:00:00	0	Unlimited
8	BatchDPSK_User_7	8S82TvbQhleUOxXr-`SFA8dx}Ur8eBaVI5M%9LH%+N!Pb4]q}kphUmc_`Z}i-)	DPSK-batch	00:00:00:00:00:00	0	Unlimited
9	BatchDPSK_User_8	q+?0_vL(Z!4@fml=#5iJpvdx9_^5:9rVO8Un$Rm=adUNpmA-uhrmCl6!ICy,,#	DPSK-batch	00:00:00:00:00:00	0	Unlimited
10	BatchDPSK_User_9	:M`_z}g5E8z0PblteDdsYGAN#CH7:_(U!sqxDlu8jd/zOFPeLj#wW(37NYp6p4	DPSK-batch	00:00:00:00:00:00	0	Unlimited
11	BatchDPSK_User_10	pPCXC@pJe35AD]bc)dlz:Wd}Z4HM{7l(Ur;Gpiu,`m(_LFcU69y)eRbddM2HXd	DPSK-batch	00:00:00:00:00:00	0	Unlimited
12	BatchDPSK_User_11	)dyn1pl)`|$()d8/aU[(e;Ax:xeKXW|]n?aK2XdN.re^d+:K9#V6_?xorIZ[Q	DPSK-batch	00:00:00:00:00:00	0	Unlimited
13	BatchDPSK_User_12	IL_z;6Rr|@WP;r[P6Ldlu8}Fmi]5b%#LXAJhd}Cz8/VY#N|N[VSIlu}$T=%cV,	DPSK-batch	00:00:00:00:00:00	0	Unlimited
14	BatchDPSK_User_13	)Rf+k3*HBlZYy02P?9W=IDJ(D_rzC|z@50=%[U3CV2+Ys}{7sg0He5:M0]sHX_	DPSK-batch	00:00:00:00:00:00	0	Unlimited
15	BatchDPSK_User_14	;:%}Xee`d2!@0Ds!:p[vT(tJ,?==p}P5@,Ys1*UeyWz:XM=t@./Gb3JFT1`Thu	DPSK-batch	00:00:00:00:00:00	0	Unlimited

8. Test it and connect a client. Launch your wireless connection utility, scan for the DPSK-batch SSID and, using the first passphrase in the .csv file, connect to the WLAN as you would to a traditional PSK network.



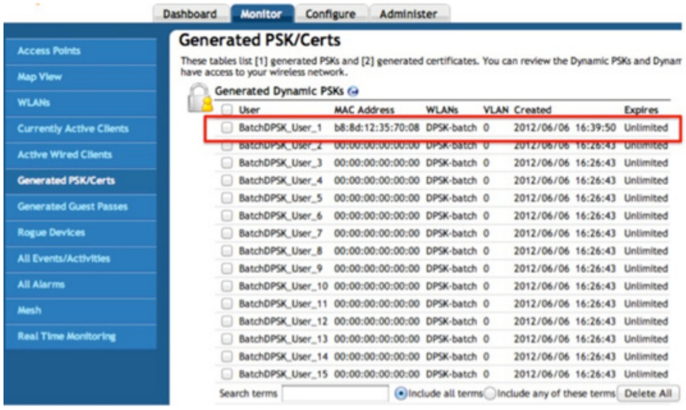
The Wi-Fi network "DPSK-test" requires a WPA2 password.

Password: (7vpvb8uz7[cv@ijOrUlxSsdH7Q!!ZBYHrd

☑ Show password
☑ Remember this network

9. Success!

10. In the ZoneDirector GUI (Monitor > Currently Active Clients), we will now see that BatchDPSK_User_1 is an active client. And, we'll see (Monitor > Generated PSK/Certs) that the user's DPSK has been mapped to the device's MAC address.



Generated PSK/Certs

These tables list [1] generated PSKs and [2] generated certificates. You can review the Dynamic PSKs and Dynam
have access to your wireless network.

Generated Dynamic PSKs

	User	MAC Address	WLANs	VLAN	Created	Expires
□	BatchDPSK_User_1	b8:8d:12:35:70:08	DPSK-batch	0	2012/06/06 16:39:50	Unlimited
□	BatchDPSK_User_2	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_3	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_4	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_5	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_6	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_7	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_8	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_9	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_10	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_11	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_12	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_13	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_14	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited
□	BatchDPSK_User_15	00:00:00:00:00:00	DPSK-batch	0	2012/06/06 16:26:43	Unlimited

Search terms ● Include all terms ○ Include any of these terms Delete All

The manual DPSK model is easy to use and flexible. Avoid the complexities of 802.1X and elude the weaknesses of legacy shared passphrases.

Ruckus Wireless, Inc.
880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA (650) 265-4200 Ph \ (408) 738-2065 Fx

Ruckus®
Simply Better Wireless.