

Dell Networking W-Series Instant Access Point Wireless LAN Deployment Guide for Dell PowerEdge VRTX

Dell Networking Solutions Engineering
June 2013

Revisions

Date	Version	Description	Authors
June 2013	1.0	Initial release	Tracy Alonzo

Copyright © 2013-2016 Dell Inc. or its subsidiaries. All Rights Reserved.

Except as stated below, no part of this document may be reproduced, distributed or transmitted in any form or by any means, without express permission of Dell.

You may distribute this document within your company or organization only, without alteration of its contents.

THIS DOCUMENT IS PROVIDED “AS-IS”, AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE SPECIFICALLY DISCLAIMED. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <http://www.dell.com/learn/us/en/vn/terms-of-sale-commercial-and-public-sector-warranties>

Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell’s recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of Dell. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

Table of contents

- Revisions.....2
- Executive summary.....4
- 1 Introduction.....5
- 2 Network Topology6
- 3 Networking W-Series Instant Access Point (IAP) Configuration7
 - 3.1 Power up and obtain IP address from DHCP server.....7
 - 3.2 Connect to the instant SSID7
 - 3.3 Logging into Dell Networking W-Series IAP8
 - 3.4 Create New Employee SSID9
 - 3.5 New WLAN Settings10
 - 3.5.1 Client IP and VLAN Assignment.....11
 - 3.5.2 Security.....12
 - 3.6 WLAN Access Settings.....13
 - 3.7 Employee WLAN13
 - 3.8 Create New Guest SSID.....14
 - 3.9 Guest WLAN Setting15
 - 3.9.1 Guest Client IP and VLAN Assignment.....16
 - 3.9.2 Guest Security17
 - 3.9.3 Guest Access.....18
 - 3.9.4 Connect to the Guest SSID19
- A Components for this Deployment: (for deployment outside US, equivalent SKU's are available).....20
- B Additional Resources21
 - B.1 Recommended Dell EMC publications:21
 - B.2 Recommended Microsoft publications:21

Executive summary

Remote Office Branch Office can now take advantage of quickly enabling enterprise grade and simple to deploy Wi-Fi access. Dell Networking W-Series Instant Access Points enable a rich Mobility experience for users of notebooks, tablets, phones and other mobile devices.

Dell PowerEdge™ VRTX is a new shared infrastructure product, focused on remote, branch, and small office needs. It combines Dell PowerEdge M520 and M620 server blades, shared storage, and I/O in the form of PCIe and one dedicated I/O Module slot. These elements are combined into a 5U rackable tower, providing a simpler model for Remote Office Branch Office (ROBO) and Small Medium Businesses (SMB) customers to deploy and manage.

1 Introduction

This deployment guide outlines the ease of setting up the Dell Networking W-Series Instant Access Points (IAP) with the Dell PowerEdge VRTX system platform designed for Remote Office Branch Office. The combination of Dell Networking W-Series IAP with Dell PowerEdge VRTX highlights the ability to deliver “Better Together” end –to- end solutions to the Remote Office Branch Office.

The Dell Networking W-Series portfolio is highly scalable and secure, and offers centralized WLAN or Distributed WLAN architectures. You can provide easily managed WLAN, BYOD and Application delivery optimized for your wireless users.

2 Network Topology

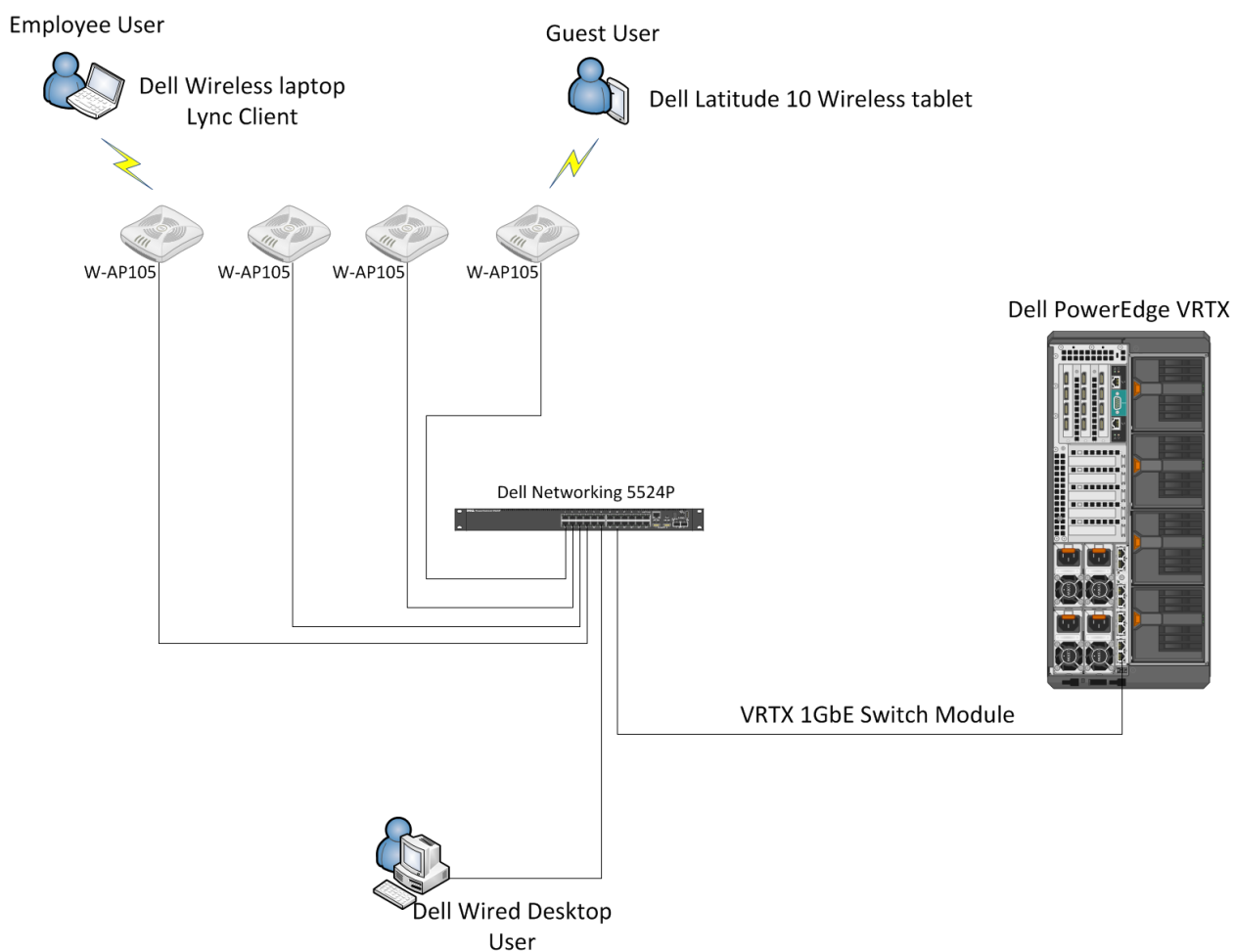


Figure 1 Wireless LAN Mobility for small office/branch office with PowerEdge VRTX

3 Networking W-Series Instant Access Point (IAP) Configuration

3.1 Power up and obtain IP address from DHCP server

Connect the Dell W-Series Instant Access Points (IAP) to the Dell Power-over Ethernet (POE) network switch and verify the unit powers up as shown in Figure 2, indicating the IAP is ready to be configured.



Figure 2 IAP Ready

3.2 Connect to the instant SSID

The Dell W-Series Mobility Instant Access Point (IAP) advertises the default Service Set Identifier (SSID). From a mobile laptop or tablet network connect to the **instant** SSID as shown in Figure 3.

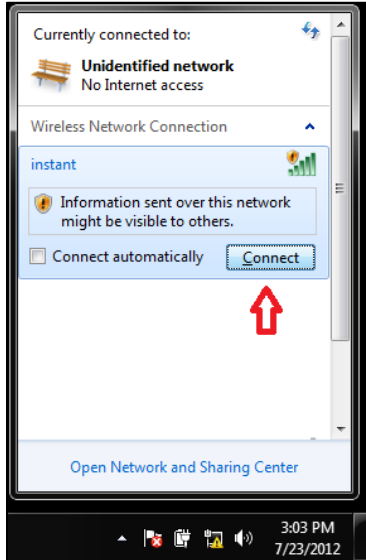


Figure 3 Connecting to Instant SSID

3.3 Logging into Dell Networking W-Series IAP

Open a web browser and navigate to **instant.dell-pcw.com** to access the Dell Virtual Controller login screen. If you enter any other URL, you are redirected to the same Dell Virtual Controller login screen.

Note: Connection to the Internet is required.

Figure 4 shows the Dell Virtual Controller's login screen. Enter Username **admin** and Password **admin**, and then click **Log In**.

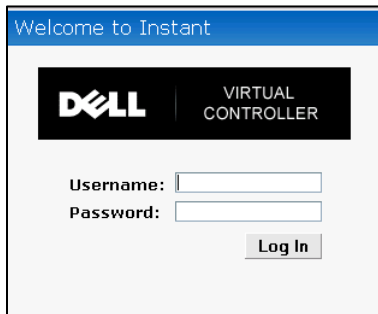


Figure 4 IAP Virtual Controller Login Screen

After logging in, the Virtual Controller main dashboard appears as shown in Figure 5.

Note: This IAP is the only IAP in the network, and is the Master Virtual Controller.

Figure 5 shows the wireless client receiving an IP address from the IAP Virtual Controller. The IAP receives an IP address from the network DHCP in the subnet.

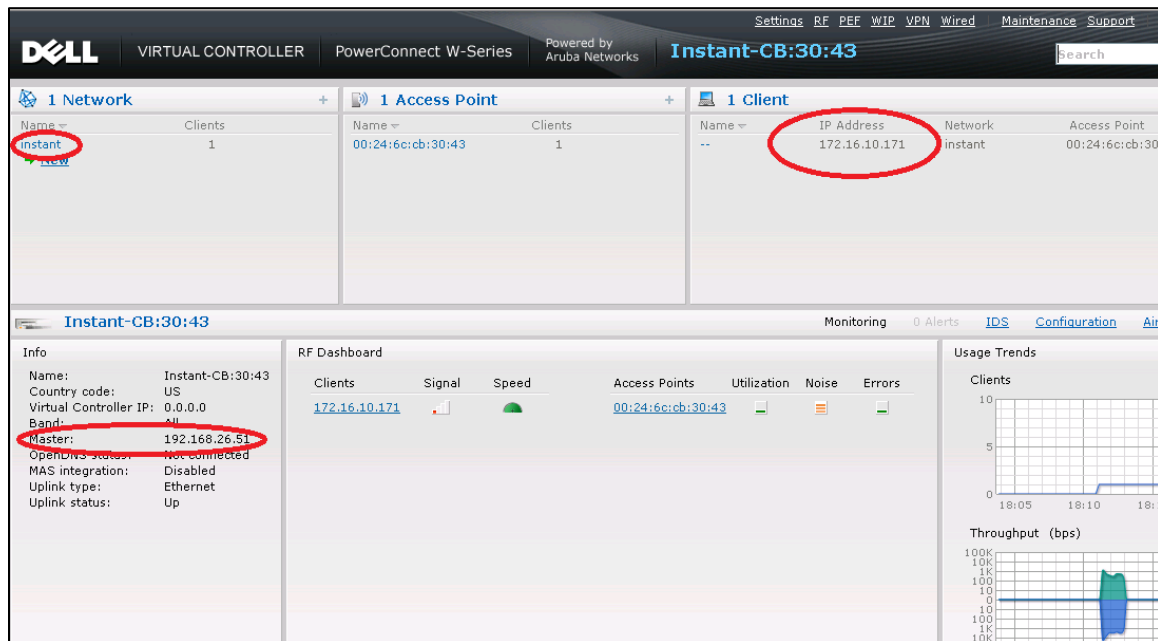


Figure 5 Virtual Controller Main Dashboard

3.4 Create New Employee SSID

From the Virtual Controller main dashboard in Figure 5, under **Network**, click **New** as shown in Figure 6.

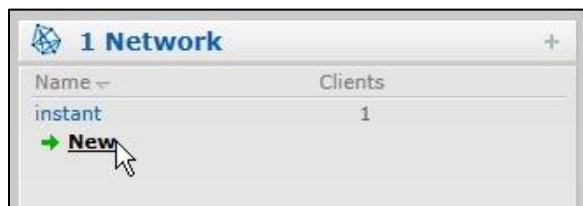


Figure 6 New Employee SSID

3.5 New WLAN Settings

In the **New WLAN** screen, enter a name (SSID). In the example below, the SSID is Dell_ROBO. Next to **Primary usage**, select **Employee**, and click **Next** as shown in Figure 7:

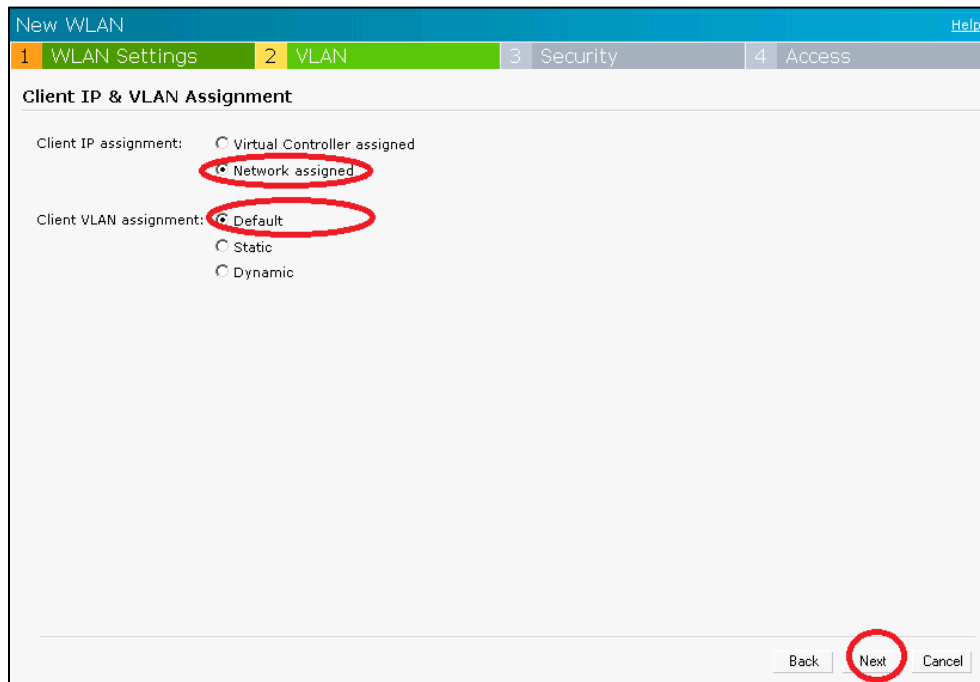
The screenshot shows the 'New WLAN' configuration window. At the top, there is a blue header bar with the title 'New WLAN' and a 'Help' link. Below the header is a tabbed interface with four tabs: '1 WLAN Settings' (active), '2 VLAN', '3 Security', and '4 Access'. The 'WLAN Settings' tab is selected, and its content is displayed below. The 'WLAN Settings' section includes a 'Name & Usage' header. Under this header, there is a 'Name (SSID):' label followed by a text input field containing 'Dell_ROBO'. Below this is the 'Primary usage:' label, followed by three radio button options: 'Employee' (selected), 'Voice', and 'Guest'. At the bottom left of the window, there is a link labeled 'Show advanced options'. At the bottom right, there are two buttons: 'Next' and 'Cancel'. The 'Next' button is circled in red.

Figure 7 New WLAN

3.5.1 Client IP and VLAN Assignment

See Figure 8. **For client IP assignment, Network assigned** is the default setting. This allows wireless clients connecting to the Employee network to be assigned an IP address from the network.

The client VLAN assignment default setting uses VLAN1 for the wireless client.



New WLAN [Help](#)

1 WLAN Settings 2 VLAN 3 Security 4 Access

Client IP & VLAN Assignment

Client IP assignment: ☐ Virtual Controller assigned
☒ Network assigned

Client VLAN assignment: ☒ Default
☐ Static
☐ Dynamic

Back Next Cancel

Figure 8 Client IP and VLAN Assignment

3.5.2 Security

See Figure 9. Set the **Security Level** slide bar to **Personal**. From the **Key management** field drop down menu, select **WPA-2 Personal**. Enter the passphrase then click **Next**.

Note: The IAP Enterprise security setting allows IEEE 802.1x authentication using WPA-2 with AES encryption. Please reference the [Instant Access Point Users Guide](#)

The screenshot shows the 'New WLAN' configuration wizard with four tabs: 1 WLAN Settings, 2 VLAN, 3 Security, and 4 Access. The 'Security' tab is active. On the left, a 'Security Level' slider ranges from 'More Secure' (Enterprise) to 'Less Secure' (Open), with 'Personal' selected in the middle. On the right, configuration options are listed: 'Key management' is set to 'WPA-2 Personal', 'Passphrase format' is '8-63 chars', 'Passphrase' and 'Retype' fields contain masked characters, 'MAC authentication' is 'Disabled', and 'Blacklisting' is 'Disabled'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Figure 9 Security Settings

3.6 WLAN Access Settings

Figure 10 illustrates the Access link. The default is **Unrestricted**, allowing wireless clients access to any and all protocols and destinations. Click **Finish**.

Note: Dell EMC recommends network access rules and policies be set according to the customer's unique security policy requirements.

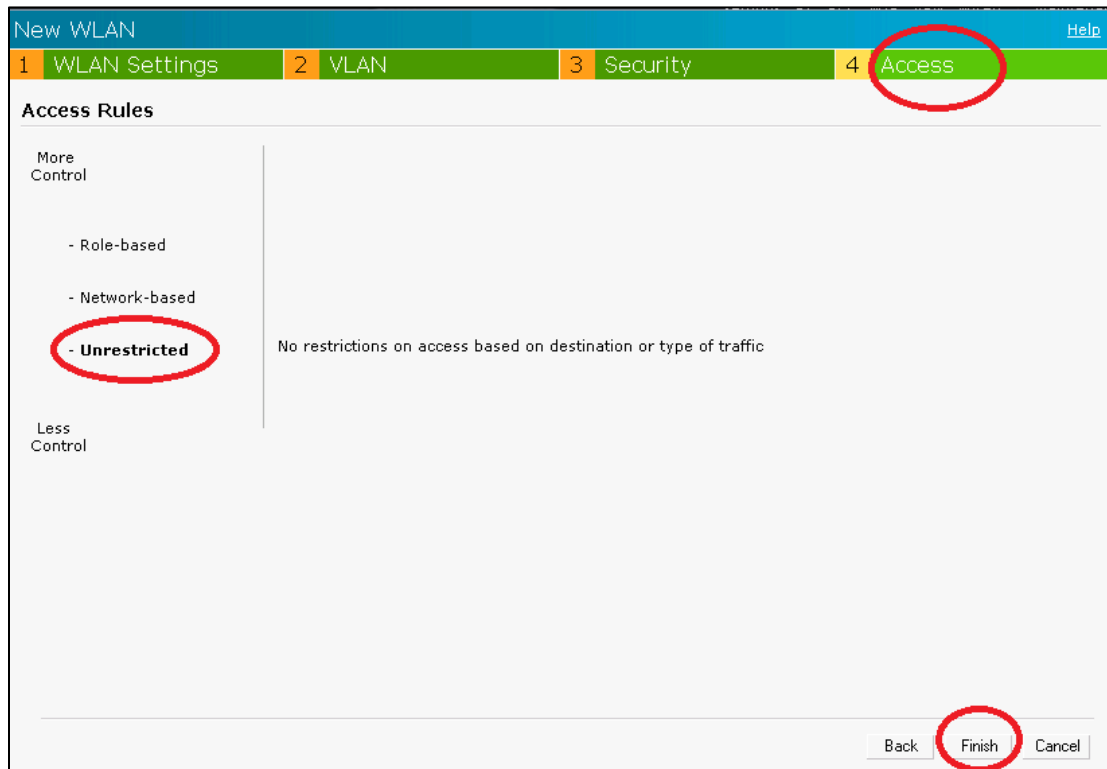


Figure 10 Access Setting

3.7 Employee WLAN

See Figure 11. Disconnect the wireless client from Instant SSID. Connect the wireless client to the new wireless network SSID. Notice a wireless client is now associated with the new WLAN and the IP address for

the wireless client is now assigned by the network DHCP. Once the new WLAN is created and connected to a wireless client, the default Instant SSID is removed.

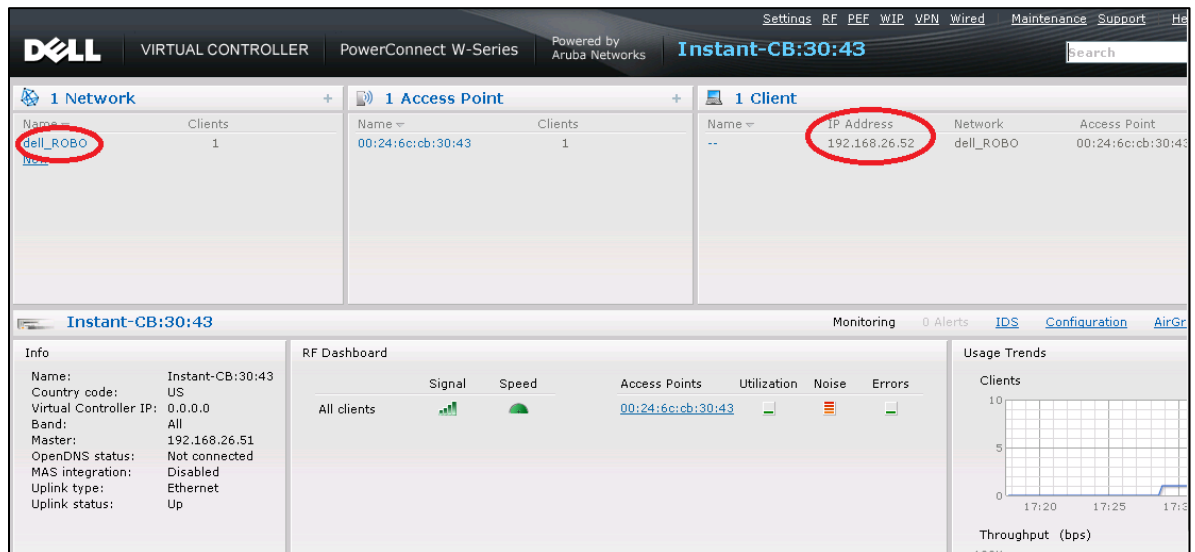


Figure 11 Employee WLAN

3.8 Create New Guest SSID

From the Virtual Controller main dashboard in Figure 11, under **Network**, click **New**, as shown in Figure 12.

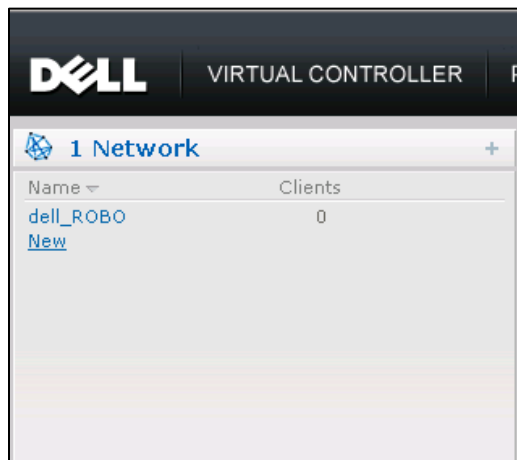


Figure 12 New Guest SSID

3.9 Guest WLAN Setting

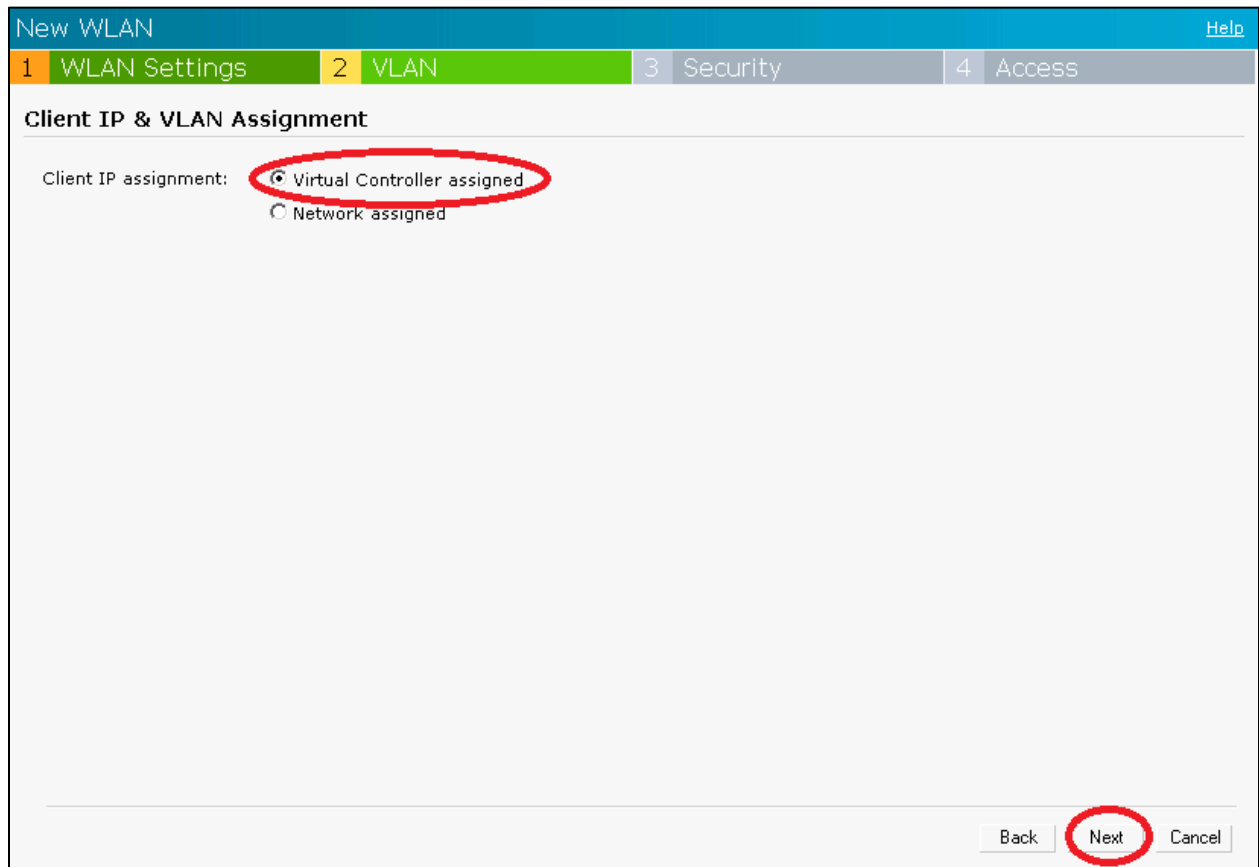
See Figure 13. In the **New WLAN** screen, enter a name in the **Name (SSID)** field. Next to **Primary usage**, select **Guest** and then click **Next**.

The screenshot displays the 'New WLAN' configuration interface. At the top, a blue header bar contains the title 'New WLAN' and a 'Help' link. Below the header is a tabbed navigation bar with four tabs: '1 WLAN Settings' (highlighted in green), '2 VLAN', '3 Security', and '4 Access'. The main content area is titled 'WLAN Settings'. Under the 'Name & Usage' section, the 'Name (SSID):' field contains the text 'guest_ROBO'. Below this, the 'Primary usage:' section has three radio button options: 'Employee', 'Voice', and 'Guest'. The 'Guest' option is selected and highlighted with a red circle. At the bottom right of the form, the 'Next' button is highlighted with a red circle, and the 'Cancel' button is located next to it. A 'Show advanced options' link is visible at the bottom left of the form area.

Figure 13 Guest WLAN

3.9.1 Guest Client IP and VLAN Assignment

See Figure 14. **Virtual Controller assigned** is the default setting. This allows the wireless clients connecting to the Guest network to have the IP address assigned by the Virtual Controller. Click **Next**.



The screenshot shows the 'New WLAN' configuration interface. At the top, there's a blue header bar with 'New WLAN' and a 'Help' link. Below this is a tabbed interface with four tabs: '1 WLAN Settings' (orange), '2 VLAN' (green), '3 Security' (grey), and '4 Access' (grey). The 'VLAN' tab is active. The main content area is titled 'Client IP & VLAN Assignment'. Under the heading 'Client IP assignment:', there are two radio buttons: 'Virtual Controller assigned' (which is selected and circled in red) and 'Network assigned'. At the bottom right of the form, there are three buttons: 'Back', 'Next' (circled in red), and 'Cancel'.

Figure 14 Guest IP Assignment

3.9.2 Guest Security

Figure 15 illustrates the security-level splash page default requiring username and password entries into the internal database. Click the **Users** link.

The screenshot shows the 'Security Level' configuration page, which is part of a sequence of four tabs: 1 WLAN Settings, 2 VLAN, 3 Security (active), and 4 Access. The page is divided into two main sections. The left section, titled 'Security Level', contains several configuration options: 'Splash page type' is set to 'Internal - Authenticated'; 'WISPr' is 'Disabled'; 'MAC authentication' is 'Disabled'; 'Auth server 1' is 'InternalServer'; 'Reauth interval' is set to '0 min.'; 'Internal server' is 'No users' with a link to 'Users'; 'Blacklisting' is 'Disabled'; and 'Encryption' is 'Disabled'. The right section, titled 'Splash Page Visuals', displays a preview of the splash page with a blue header 'Welcome to Guest Network' and a green body containing login fields and a 'Log In' button. Below the preview, there is a 'Click thumbnail above to edit' instruction and a 'Preview' link. At the bottom of this section is a 'Redirect URL' field with '(Optional)' text. At the very bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

Figure 15 Guest Security Level

See Figure 16. In the **Users** screen, add a new user. Enter the username and password, and then click **OK**.

The screenshot shows the 'Users' management screen. It has a blue header with the title 'Users' and a 'Help' link. The main area is divided into two parts. On the left is a table with two columns: 'Users(1)' and 'Type'. It contains one entry: 'ROBO' with the type 'Guest'. Below the table are 'Edit', 'Delete', and 'Delete All' buttons. On the right is the 'Add new user:' section, which includes input fields for 'Username:', 'Password:', and 'Retype:', and a 'Type' dropdown menu currently set to 'Guest'. An 'Add' button is located below the dropdown. At the bottom right of the screen are 'OK' and 'Cancel' buttons.

Figure 16 Guest User Database

3.9.3 Guest Access

Figure 17 shows the network-based access rules to add. Click **New**, and then click **Finish**. The rules will be executed in the order shown.

Note: Dell EMC recommends setting network access rules and policies according to the customer's unique security policy requirements.

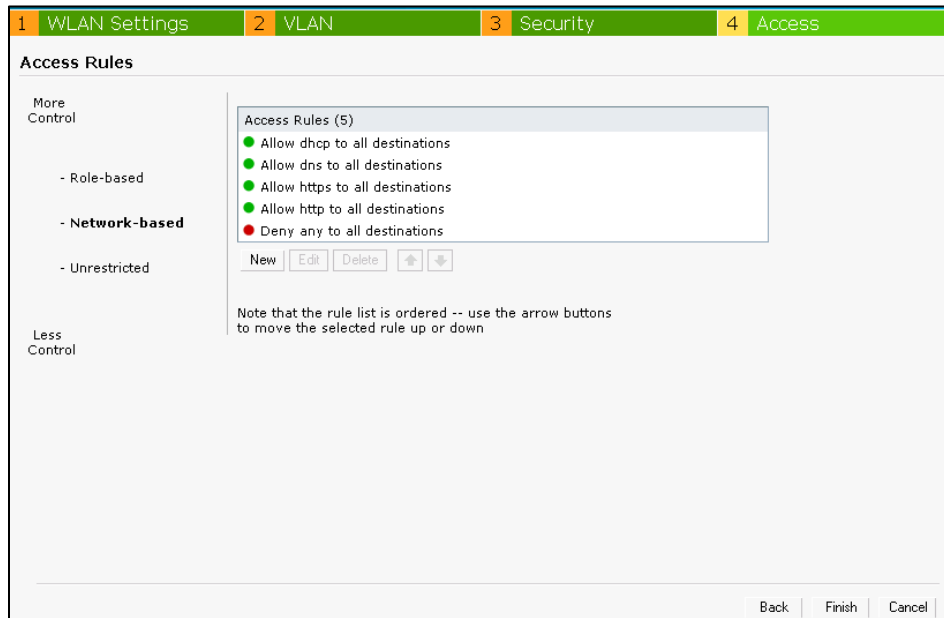
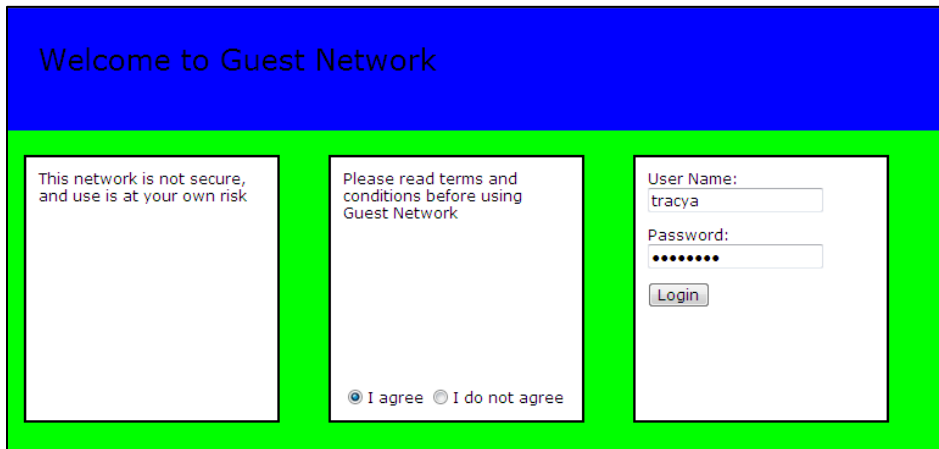


Figure 17 Guess Access Rules

3.9.4 Connect to the Guest SSID

From a mobile device, connect to the Guest SSID. Open a web browser and connect to any internet website. Figure 18 shows the Guest Welcome page that appears. Agree to the terms, and then enter the user name and password for the guest user.

At this point, users now have an Employee and Guest WLAN to which they can connect.

The image shows a web page titled "Welcome to Guest Network" with a blue header. The main content area has a green background and contains three white boxes. The first box on the left contains the text "This network is not secure, and use is at your own risk". The middle box contains the text "Please read terms and conditions before using Guest Network" and two radio buttons at the bottom: "I agree" (which is selected) and "I do not agree". The third box on the right contains a "User Name:" label with a text input field containing "tracya", a "Password:" label with a password input field containing nine dots, and a "Login" button below the fields.

Welcome to Guest Network

This network is not secure, and use is at your own risk

Please read terms and conditions before using Guest Network

☒ I agree ☐ I do not agree

User Name: tracya

Password:

Login

Figure 18 Guest Welcome Page

A Components for this Deployment: (for deployment outside US, equivalent SKU's are available)

Table 1 Dell Networking 5524P

Description	QTY	SKU
5524P, 24 GbE Ports, Managed Switch, 10GbE and Stacking built-in, PoE	1	225-0848
Powercord, 125 Volt, 15Amp, 10 Foot	1	330-6870
Switch includes Lifetime Warranty repair. Choose Dell ProSupport™ for advanced technical support.	1	929-2707, 931-2041, 934-8788, 939-9130, 939-9360
ONSITE INSTALLATION: Hardware Install only	1	989-6188
Asset Recovery, Program Managed	1	960-1848

Table 2 Dell Networking W-IAP105

Description	QTY	SKU
W-IAP105, Instant Wireless Access Point, US	1	225-2051
W-WIAP105, Optional Mounting Kit, Recessed Ceiling, 9/16" or 15/16"	1	331-0211
W-WIAP105 Flat Surface, Wall Box Mount Kit (for PoE only)	1	331-0212
Basic Hardware Warranty Repair: 5x10 HW-Only, 5x10 NBD Parts	1	933-9147, 959-0600, 959-0610, 968-7546, 968-7547
No Installation	1	900-9997
W-IAP Documentation Kit	1	331-5447

B Additional Resources

B.1 Recommended Dell EMC publications:

[Dell Networking W-Series Mobility](#)

[Dell Networking W-Series Mobility Support](#)

[Microsoft Lync Server 2010 on Dell Systems](#)

B.2 Recommended Microsoft publications:

[Microsoft® Lync® Qualified Infrastructure](#)