

RUCKUS SmartZone (ST-GA) Security Guide, 7.0.0

Supporting SmartZone 7.0.0

© 2024 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

| | |
|--|-----------|
| Contact Information, Resources, and Conventions..... | 5 |
| Contacting RUCKUS Customer Services and Support..... | 5 |
| What Support Do I Need?..... | 5 |
| Open a Case..... | 5 |
| Self-Service Resources..... | 6 |
| Document Feedback..... | 6 |
| RUCKUS Product Documentation Resources..... | 6 |
| Online Training Resources..... | 6 |
| Document Conventions..... | 7 |
| Notes, Cautions, and Safety Warnings..... | 7 |
| Command Syntax Conventions..... | 7 |
| About The Guide..... | 9 |
| New in This Document..... | 9 |
| Managing Administrator and Roles..... | 11 |
| Creating User Groups..... | 11 |
| Resource Group Details..... | 13 |
| Creating Administrator Accounts..... | 14 |
| Unlocking an Administrator Account..... | 16 |
| Configuring Administrator Accounts..... | 16 |
| Working with AAA Servers..... | 19 |
| Configuring SZ Admin AAA Servers..... | 19 |
| Configuring Switch AAA Servers..... | 24 |
| Configuring Switch AAA Server Settings..... | 25 |
| AAA Server Authentication..... | 26 |
| About RADIUS Support..... | 27 |
| About LDAP Support..... | 29 |
| Creating Account Security..... | 30 |
| Active Directory (AD)..... | 35 |
| About Active Directory (AD) Support..... | 35 |
| Creating a User Role with Active Directory Authentication..... | 36 |
| 802.1X Authentication..... | 36 |
| Creating a User Role with 802.1x Authentication..... | 36 |
| Access Control..... | 39 |
| Virtual LAN..... | 39 |
| VLAN Pooling..... | 39 |
| VLAN Precedence..... | 41 |
| VLAN Name..... | 42 |
| Restricted Access..... | 43 |
| Overview..... | 44 |
| Creating a Restricted AP Access Profile..... | 45 |
| Configuring a Restricted Access via Access Point..... | 47 |
| Configuring a Restricted Access via Templates..... | 47 |
| Enabling Restricted AP Access Profile..... | 47 |
| Creating Blocked Client..... | 48 |
| Creating a Client Isolation Whitelist..... | 49 |

| | |
|---|------------|
| Creating a Time Based Access Table..... | 50 |
| Creating a Traffic Class Profile | 51 |
| Creating a DNS Server Profile..... | 54 |
| Creating a DNS Spoofing Profile..... | 55 |
| Enabling the Access Control of Management Interface..... | 56 |
| Wireless Intrusion Detection and Prevention Services (WIDS/WIPS)..... | 59 |
| Wireless Intrusion Detection and Prevention System..... | 59 |
| Configuring a Rogue Classification Policy..... | 59 |
| Certificates..... | 63 |
| Importing SmartZone as Client Certificate..... | 63 |
| Assigning Certificates to Services..... | 64 |
| Generating Certificate Signing Request (CSR)..... | 65 |
| Managing AP Certificates..... | 66 |
| AP Certificate..... | 68 |
| Importing SmartZone (SZ) Trusted CA Certificates/Chains..... | 68 |
| DataPlane validates SmartZone..... | 69 |
| AP Validate SmartZone Controller..... | 70 |
| Firewall Profile..... | 75 |
| Managing a Firewall Profile..... | 75 |
| Create an L3 Access Control Policy..... | 76 |
| Creating an L2 Access Control Policy..... | 79 |
| Configuring Application Controls..... | 81 |
| URL Filtering..... | 89 |
| Creating a Device Policy..... | 95 |
| TACACS+..... | 101 |
| About TACACS+ Support..... | 101 |
| ECDSA..... | 103 |
| Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support..... | 103 |
| Cloud Computing Compliance Criteria Catalogue - BSI C5..... | 103 |
| Configuring ECDSA and Keys at Zone Level..... | 103 |
| Mapping Server ECDSA Certificates..... | 105 |
| Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)..... | 108 |

Contact Information, Resources, and Conventions

- [Contacting RUCKUS Customer Services and Support](#)..... 5
- [Document Feedback](#)..... 6
- [RUCKUS Product Documentation Resources](#)..... 6
- [Online Training Resources](#)..... 6
- [Document Conventions](#)..... 7
- [Command Syntax Conventions](#)..... 7

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckusnetworks.com> and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://community.ruckuswireless.com>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckusnetworks.com>.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

| Convention | Description | Example |
|----------------|---|---|
| monospace | Identifies command syntax examples | <code>device(config)# interface ethernet 1/1/6</code> |
| bold | User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names | On the Start menu, click All Programs . |
| <i>italics</i> | Publication titles | Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information. |

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

| Convention | Description |
|--------------------|---|
| bold text | Identifies command names, keywords, and command options. |
| <i>italic text</i> | Identifies a variable. |
| [] | Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets. |
| {x y z} | A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. |
| x y | A vertical bar separates mutually exclusive elements. |
| < > | Nonprinting characters, for example, passwords, are enclosed in angle brackets. |
| ... | Repeat the previous element, for example, <i>member[member...]</i> . |
| \ | Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash. |

About The Guide

- [New in This Document](#)..... 9

New in This Document

TABLE 2 Key Features and Enhancements in SmartZone 7.0.0 Rev A (February 2024)

| Feature | Description | Reference |
|--------------------------------------|--|--|
| Enhance the device policy os vendor. | Updated: The original supported Gaming device type OS vendors have now been merged. | Creating the Device Policy Rules on page 97 |
| Client roaming with AVC info | Updated: AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as ARC and URL Filtering. | <ul style="list-style-type: none">• Configuring Application Controls on page 81• URL Filtering on page 89 |
| ECDSA Certificate | The ECDSA is a digital signature algorithm which uses keys derived from elliptic curve cryptography. | Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support on page 103 |

Managing Administrator and Roles

- Creating User Groups..... 11
- Creating Administrator Accounts..... 14
- Configuring Administrator Accounts..... 16
- Working with AAA Servers..... 19
- Creating Account Security..... 30
- Active Directory (AD)..... 35
- 802.1X Authentication..... 36

The controller must be able to manage various administrators and roles that are created within the network to assign tasks and functions, and to authenticate users.

Creating User Groups

Creating user groups and configuring their access permissions, resources, and administrator accounts allows administrators to manage a large number of users.



Perform the following steps to create user groups.








1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Groups** tab.
3. Select the system domain, and click **Create**.

The **Create User Group** is displayed.

Managing Administrator and Roles

Creating User Groups

4. Configure the following options:
 - a. Permission
 1. Name: Type the name of the user group you want to create.
 2. Description: Type a short description for the user group you plan to create.
 3. Permission: Select one of the access permission for the user group from the drop-down menu. You can also grant admin permission to generate guest passes. Select the **Custom** option to manually assign role-based permission in the **Resource** tab page.
 4. Account Security: Select the account security profile that you created to manage the administrator accounts.
 5. Click **Next**.
 - b. Resource: From **Select Resources**, choose the resources that you want to assign to this user group. If you have selected **Custom** permission option in the previous step, you can assign the required permission (**Read, Modify or Full Access**) to these resources. The resources available are SZ, AP, WLAN, User/Device/App, Admin, Guest Pass, MVNO and ICX. Click the  icon and they appear under **Selected Resources** now. Use the  icon to deselect the resources assigned to the group. To select the right set of resource permission, refer to Resource Group Details.
 - NOTE**

To create User Groups, migrating Domain User Roles prior to 3.5, with DPSK permissions, Users must be granted with "User/Device/App" resource.
 - c. Click **Next**.
 - d. Domain: Select the domain from the list of domains to which this user group will be associated. From **Select Domains**, choose the domains you want to assign to this user group. Click the  icon and they appear under **Selected Domains** now. Use the  icon to deselect the domains assigned to the group.
 - e. Click **Next**.
 - f. Administrator: From **Available Users**, choose the users you want to assign to this user group. Click the  icon and they appear under **Selected Users** now. Use the  icon to deselect the users assigned to the group. You can also create Administrator Accounts by clicking the  icon. The **Create Administrator Account** page appears where you can configure the administrator account settings. You can edit the user settings by clicking the  icon and delete the user from the list by clicking  icon.
 - g. Click **Next**.
 - h. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.
 - i. Click **OK** to confirm.

You have created the user groups.

NOTE

You can also edit and delete the group configuration by selecting the options **Configure**, and **Delete** respectively, from the **Groups** tab.

Resource Group Details

The Resource Group table lists the resources available for each Resource Category. This helps the users to select the right set of resource permission for the Admin type.

TABLE 3 Resource Group Table

| Resource Category | Resources |
|-------------------|--|
| SZ | <ul style="list-style-type: none"> System Settings Cluster Settings and Cluster Redundancy Control Planes and Data Planes Firmware and Patches Cluster and Configuration Backups Licensing Cluster Stats and Health System Events and Alarms System Certificates Northbound Interface SCI Integration |
| AP | <ul style="list-style-type: none"> Zones and Zone Templates AP groups AP Settings AP Stats and Health Maps AP Events and Alarms Bonjour Policies Location Services Ethernet Port Profiles Tunneling Profiles and Settings AP Zone Registration |
| WLAN | <ul style="list-style-type: none"> WLANs WLAN Groups and Templates AAA Services L2-7 Policies Rate Limiting Application Policies Device OS Policies QoS Controls Hotspots and Portals Hotspot 2.0 Service Schedules VLAN Pools |

TABLE 3 Resource Group Table (continued)

| Resource Category | Resources |
|-------------------|---|
| User/Device/App | User Roles Local Users DPSK Guest Passes Application Usage Client and Device Details |
| Admin | Domains Administrators Administrative Groups Administrative Activity AAA for Admins |
| Guest Pass | Guest Pass Guest Pass Template |
| MVNO | MVNO |
| ICX Switch | ICX Switch Switch Group Registration Rule |

Creating Administrator Accounts

The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization. You can also modify the status of the administrator account by locking or unlocking it.

1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Administrators** tab.

3. Click **Create**.

The **Create Administrator Account** page appears.

FIGURE 1 Creating an Administrator Account

The screenshot shows a web form titled "Create Administrator Account". The form contains the following fields:

- * Account Name:
- Real Name:
- * Password:
- * Confirm Password:
- Phone:
- Email:
- Job Title:

At the bottom right of the form are two buttons: "OK" (dark grey) and "Cancel" (light grey).

4. Configure the following:
 - a. Account Name: Type the name that this administrator will use to log on to the controller.
 - b. Real Name: Type the actual name (for example, John Smith) of the administrator.
 - c. Password: Type the password that this administrator will use (in conjunction with the Account Name) to log on to the controller.
 - d. Confirm Password: Type the same password as above.
 - e. Phone: Type the phone number of this administrator.
 - f. Email: Type the email address of this administrator.
 - g. Job Title: Type the job title or position of this administrator in your organization.
 - h. Click **OK**.

NOTE

You can also edit, delete, or unlock the admin account by selecting the options **Configure**, **Delete** or **Unlock**, from the **Administrator** tab.

NOTE

Administrator users mapped to different domain other than system domain have to log in using accountname@domain as the User.

Unlocking an Administrator Account

When multiple user access authentications fail, the administrator account is locked. A super administrator can however unlock the administrator account.

Typically, the account gets locked when the user attempts to login with a wrong user ID or password multiple times, or when the time duration/session time to access the account has ended.

You must login as a super administrator in order to unlock the account.

1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Administrators** tab.
3. From the list of accounts, select the one which needs to be unlocked. The **Status** of such an account is displayed as *Locked*.
4. Click **Unlock**.

The administrator account is now unlocked, the **Status** field against the account now displays *Unlocked*.

Configuring Administrator Accounts

To configure the account security of System Default Super Admin account, you can set session idle timeout, password expiration, and password reuse rules.

You must log in as a **System Default Super Admin** to set the rules.

1. Select **Administration > Administration > Admins and Roles**.
2. Click the **Administrators** tab.

3. Select the administrator account (admin) and click **Configure** to set the additional security enhancements.

The **Edit Administrator Account** page appears.

FIGURE 2 Configuring an Administrator Account

Edit Administrator Account: admin

Account Name: admin

Real Name:

New Password:

Confirm New Password:

Phone:

Email:

Job Title:

Account Lockout: Lock account for 30 (1-1440) minutes after 6 (1-100) authentic attempt

Session Idle Timeout: 15 (1-1440) minutes

Password Expiration: Require password change every 90 (1-365) days

Password Reuse: Passwords cannot be the same as the last 4 (1-6) times

Minimum Password Length: Password must be at least 8 (8-64) characters
When minimum password length is changed, admin should change password well. Minimum password length changes apply for all future passwords on

Password Complexity: Password must be fulfilled as below:
- At least one upper-case character
- At least one lower-case character
- At least one numeric character
- At least one special character
- At least 8-chars within the old password should be changed

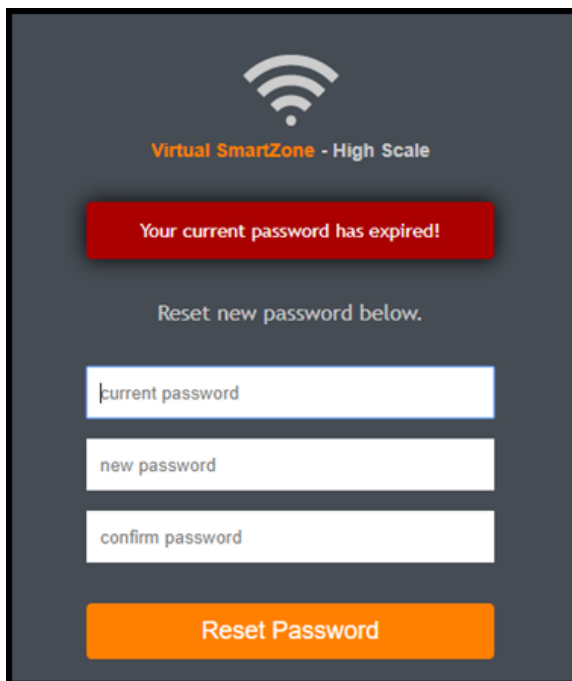
Minimum Password Lifetime: Password should not be changed twice within the 24 hours.

OK Cancel

4. Configure the following fields:
- Real Name: Enter the name of the administrator.
 - Phone: Enter the phone number.
 - Email: Enter the email address.
 - Job Title: Enter the role.
 - Account Lockout: You can configure the security profile to lock the account based on the duration of the session or number of failed attempts to access the account. Provide the values as necessary. Click the button to enable the feature.
 - Session Idle Timeout: Click the button and enter the timeout duration in minutes.
 - Password Expiration: Click the button and type the number of days for which the account's password is valid. After the configured number of days, the password expires, and the account is inaccessible. You must change the password before the expiration day to have continued access to the account. By default, the password is valid for 90 days. It can be configured for validity from a minimum of 1 day, to a maximum of 365 days.

If your password has expired, you are prompted to change or reset your password as soon as you log in. Reset the password as shown in the following figure.

FIGURE 3 Resetting the Old Password



The screenshot displays a dark grey login screen for 'Virtual SmartZone - High Scale'. At the top center is a white Wi-Fi icon. Below it, the text 'Virtual SmartZone - High Scale' is shown in orange and white. A prominent red rectangular box contains the white text 'Your current password has expired!'. Underneath this, the instruction 'Reset new password below.' is centered in white. Three white input fields are stacked vertically, each with a light blue border and a white cursor. The first field is labeled 'current password', the second 'new password', and the third 'confirm password'. At the bottom of the screen, a large orange button with the white text 'Reset Password' is centered.

- Password Reuse: Prevents the reuse of passwords. Click the button to enable this option. By default, the value is 4 (last 4 passwords cannot be reused).
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.
- Password Complexity: Ensures that the password satisfies the following rules:
 - At least one upper-case character
 - At least one lower-case character

- At least one numeric character
- At least one special character
- At least eight characters from the previous password is changed

Select the options you want to apply..

- Minimum Password Lifetime: Ensures that the password is not changed twice within a period of 24 hours. Select the option, if appropriate.

5. Click **OK**.

The **Password Confirmation** page is displayed.

6. Enter the **password**.

7. Click **OK** to apply the new configuration.

Working with AAA Servers

You can configure the controller to use external AAA servers to authenticate users.

Configuring SZ Admin AAA Servers

To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

1. Select **Administration > Administration > Admins and Roles > AAA**.

2. From **AP AAA Servers**, click **Create**.

The **Create Administrator AAA Server** page is displayed.

FIGURE 4 Creating an Administrator AAA Server

3. Enter the AAA server name.
4. For **Type**, select the type of AAA server to authenticate users:
 - **RADIUS**
 - **TACACS+**
 - **Active Directory**
 - **LDAP**
5. For **Realm**, enter the realm or service.
Multiple realms or services are supported. Separate multiple realms or services with a comma.

NOTE

Because the user login format (User Account + @ + Realm) includes a special character, the at symbol (@), the user account must not include the at symbol (@) separately on the AAA server.

6. Enable **Default Role Mapping**.

You can select **auto-mapping** for the system to automatically map between the AAA and SZ accounts.

If **Default Role Mapping** is disabled, the AAA administrator must be mapped to a local SZ Admin user with matching AAA attributes for the RADIUS, TACACS+, Active Directory, or LDAP servers.

- On a RADIUS server, the user data can use the **VSA Ruckus-WSG-User** attribute with a value depending on the SZ users or permissions you want the RADIUS user to map.
- On a TACACS+ server, the user data can use the **user-name** attribute with the **user1**, **user2**, or **user3** value depending on the SZ users or permissions you want the TACACS+ user to map.
- On an Active Directory or LDAP server, the user data can belong to the group **cn=Ruckus-WSG-User-SZAdminName** (for example, **cn=Ruckus-WSG-User-User1**, depending on the SZ users or permissions you want the Active Directory or LDAP user to map.

NOTE

You can use the mapping attributes on AAA and enable **Default Role Mapping** at the same time, but the mapping attributes override **Default Role Mapping**.

7. For **Backup RADIUS**, select **Enable Secondary Server** if a secondary RADIUS server exists on the network. Refer to step 9 for configuration settings.

8. Under **Primary Server**, configure the settings of the primary AAA server.

- **IP Address or FQDN** : Enter the IP address or Fully Qualified Domain Name (FQDN) of the AAA server.

NOTE

The FQDN option can be configured only for the RADIUS server.

- **Port**: Enter the UDP port that the RADIUS server is using. The default port is 1812.
- **Protocol**: Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the PEAP and PAP protocols, you must configure the Trusted CA certificate to support PEAP and EAP connection.

- **Shared Secret**: Enter the shared secret.
- **Confirm Secret**: Re-enter the shared secret to confirm.
- **Windows Domain name**: Enter the domain name for the Windows server.
- **Base Domain Name**: Enter the name of the base domain.
- **Admin Domain Name**: Enter the domain name for the administrator.
- **Admin Password**: Enter the administrator password.
- **Confirm New Password**: Re-enter the password to confirm.
- **Key Attribute**: Enter the key attribute, such as UID.
- **Search Filter**: Enter a filter by which you want to search, such as objectClass=*

For **Active Directory**, configure the settings for the **Proxy Agent**.

- **User Principal Name**: Enter the Windows domain Administrator name
- **Password**: Enter the administrator password.
- **Confirm Password**: Re-enter the password to confirm.

Managing Administrator and Roles

Working with AAA Servers

9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.
 - **IP Address:** Enter the IP address of the AAA server.
 - **IP Address or FQDN:** Enter the IP address or Fully Qualified Domain Name (FQDN) of the AAA server.

NOTE

The FQDN option can be configured only for the RADIUS and Secondary server.

- **Port:** Enter the UDP port that the RADIUS server is using. The default port is 1812.
- **Protocol:** Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the PEAP and PAP protocols, you must configure the Trusted CA certificate to support PEAP and EAP connection respectively.

- **Shared Secret:** Enter the shared secret.
- **Confirm Secret:** Re-enter the shared secret to confirm.

10. Under **Failover Policy at NAS**, configure the settings of the secondary RADIUS server.
 - **Request Timeout:** Enter the timeout period in seconds. After the timeout period, an expected RADIUS response message is considered to have failed.
 - **Max Number of Retries:** Enter the number of failed connection attempts. After the maximum number of attempts, the controller tries to connect to the backup RADIUS server.
 - **Reconnect Primary:** Enter the time in minutes, after that the controller connects to the primary server.

11. Click **OK**.

NOTE

You can also edit, clone, or delete the server by selecting the options **Configure**, **Clone**, or **Delete**, from the **Administrator** tab.

Testing SZ Admin AAA Servers

To ensure that the controller administrators are able to authenticate successfully with the RADIUS server type that you selected, RUCKUS strongly recommends testing the AAA server after you set it up.

The test queries the RADIUS server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

1. Select **Administration > Admins & Roles > AAA**.

2. Select the created AAA server and click **Test AAA**.
An example for testing a RADIUS server is shown in the following figure.

FIGURE 5 Testing an AAA Server: RADIUS

Test AAA Servers

Name: peapIPv6

Protocol: PEAP

User Name: ramu
(Test with username ONLY.)

Password: [masked]
 Show password

AAA testing : Success! Associated with Auto Mapping [CACDEV]

Test Cancel

The **Protocol** field is displayed only for RADIUS server that depends on the SZ AAA server configuration.

3. In the **Name** field, select the AAA server that you created.
4. In the **User Name** field, enter an existing user name that is associated to a user group.

NOTE

For TACACS+ server, test with username appended with configured service.

5. In the **Password** field, enter password for the user name you specified.
6. Click **Test**.

If the username is associated with a user group, the following message is displayed: AAA testing: Success! Associated with Auto Mapping. If the username is not associated with any user group, the following message is displayed: "AAA testing: Success! No SZ User or Default role mapping associated".

Configuring Switch AAA Servers

To add and manage Authentication, Authorization, and Accounting (AAA) servers that the controller can use for authentication, follow these steps.

1. Select **Network > Wired > Switches** The **Switches** window is displayed.
2. Select a **Domain > Switch Group** and scroll down to view the details.
3. In the **Common Configuration** tab, click the **Configure** icon to display the **Common Configuration** dialog box.
4. Click the **AAA** tab.
5. Expand the **AAA Servers** section.
6. Click the **[+Create]** icon.
The **Create AAA Server** page is displayed.
7. Enter the AAA server name.
8. For **Type**, select **RADIUS**, **TACACS+** or **Local User** type of AAA server to authenticate user.

FIGURE 6 Creating a Switch AAA Server with Type as RADIUS

The screenshot shows the 'Create AAA Server' dialog box with the following fields and values:

- Name: [Empty]
- Type: Radius TACACS+ Local User
- IP Address: [Empty]
- Auth. Port: 1812
- Acct. Port: 1813
- Shared Secret: [Empty]
- Confirm Shared Secret: [Empty]
- Purpose: [Default] (dropdown menu is open showing: Default, Authentication, Accounting)

Buttons: OK, Cancel

9. **IP Address:** Enter the IP address of the AAA server.

10. **Auth. Port:** Enter the authentication port that the server is using.

NOTE

The default port number is 1812. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

11. **Acct. Port:** Enter the accounting port that the server is using.

NOTE

The default port number is 1813. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

12. **Shared Secret:** Enter the shared secret.

13. **Confirm Shared Secret:** Re-enter the shared secret to confirm.

14. **Purpose:** When Type=RADIUS, select the purpose for the RADIUS AAA server being created. Values are **Default**, **Authentication** and **Accounting** from the list.

NOTE

Starting with 7.0 release, you can set up multiple RADIUS servers with different options such as **Authentication** and **Accounting**. In earlier releases, the controller could only configure a RADIUS server for a switch with the **Default** option.

NOTE

The switch supports this setting on FastIron release 08.0.90 and later versions.

When Type=TACACS+, select the purpose for the TACACS+ AAA server being created. Values are **Default**, **Authentication**, **Authorization**, and **Accounting**. When Type = Local User, select the privilege for the Local User server being created. Values are **Port Config** , **Read Only** and **Read Write**.

15. Click **OK**.

You can subsequently edit or delete a AAA server by selecting the server from the list in the **AAA Servers** section and selecting **Configure** or **Delete**, respectively.

NOTE

The ICX switch fails to delete the TACACS+ and RADIUS AAA servers when pushed from SmartZone or Virtual SmartZone if SNMP query is disabled in the switch or if the switch is pre-configured before joining SmartZone or Virtual SmartZone.

Configuring Switch AAA Server Settings

To configure and manage AAA servers, complete the following steps.

1. Select **Network > Wired > Switches > AAA** .

2. Select **Switch AAA Setting** > **Select Switch Group** > **Configuration** > **Common Configuration** > **Configure AAA**, configure the following.

Login Authentication

- **SSH Authentication:** Enable the option for secure authentication.
- **Telnet Authentication:** Enable the option to set Telnet authentication. This option requires SSH authentication to be enabled.
- **First Pref:** Select the first preferred authentication system.
- **Second Pref:** Select the second preferred authentication system.
- **Third Pref:** Select the third preferred authentication system.

Authorization

- **Command Authorization:** Enable this option to assign the following authorization services:
 - **Level:** Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
 - **Server 1:** Select the authorization method for the first server.
 - **Server 2:** Select the authorization method for the second server.
- **Exec Authorization:** Enable this option to authorize the user to access the privilege mode.
 - **Server 1:** Select the authorization method for the first server.
 - **Server 2:** Select the authorization method for the second server.

Accounting

- **Command Accounting:** Enable this option to track the following accounting services:
 - **Level:** Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
 - **Server 1:** Select the tracking method for the first server.
 - **Server 2:** Select the tracking method for the second server.
- **Exec Accounting:** Enable this option to track the services in the privilege mode.
 - **Server 1:** Select the tracking method for the first server.
 - **Server 2:** Select the tracking method for the second server.

3. Click **OK**.

AAA Server Authentication

Complete AAA-based authentication for the AAA server by performing one of the following steps.

1. Enable **Default Role Mapping** to map the external AAA users to a single SZ local admin user.

2. Apply the permissions of AAA users on SZ using the corresponding AAA server attributes.

Following is an example:

- a. Create three user groups with the following access permissions in SZ:
 - Group1 with SZ super permission
 - Group2 with SZ AP admin permission
 - Group3 with SZ read-only permission
- b. Create three SZ local users corresponding to the user groups as follows:
 - Bind User1 with Group1
 - Bind User2 with Group2
 - Bind User3 with Group3

NOTE

Following are the attribute values on AAA servers:

- RADIUS: **Ruckus-WSG-User=User1 or User2 or User3.**
 - TACACS+: **user-name=User1 or User2 or User3.**
 - Active Directory and LDAP: **Group cn=Ruckus-WSG-User-User1 or Ruckus-WSG-User-User2 or cn=Ruckus-WSG-User-User3.**
- c. Select **Administrator > Administrator > Admins and Roles > AAA** and click **Create** to create an Admin AAA profile.
Refer to [Configuring SZ Admin AAA Servers](#) on page 19.

About RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is an Authentication, Authorization, and Accounting protocol used to authenticate controller administrators.

In addition to selecting RADIUS as the server type, complete the following steps for RADIUS-based authentication to work on the controller.

1. Edit the RADIUS configuration file (**users**) on the RADIUS server to include the user names.

For example,

```
Peter Cleartext-Password := "user_345"  
      Ruckus-WSG-User = "User2"  
  
Tony Cleartext-Password := "user_456"  
     Ruckus-WSG-User = "User3"  
  
Steve Cleartext-Password := "user_567"  
     Ruckus-WSG-User = "User1"  
~
```

2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 14. In this example, RADIUS can use User1, User2, or User3.

Managing Administrator and Roles

Working with AAA Servers

3. Select **Administration>Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 11.

4. When adding a server type for administrators, select RADIUS as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 19.

5. Test the RADIUS server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 14.

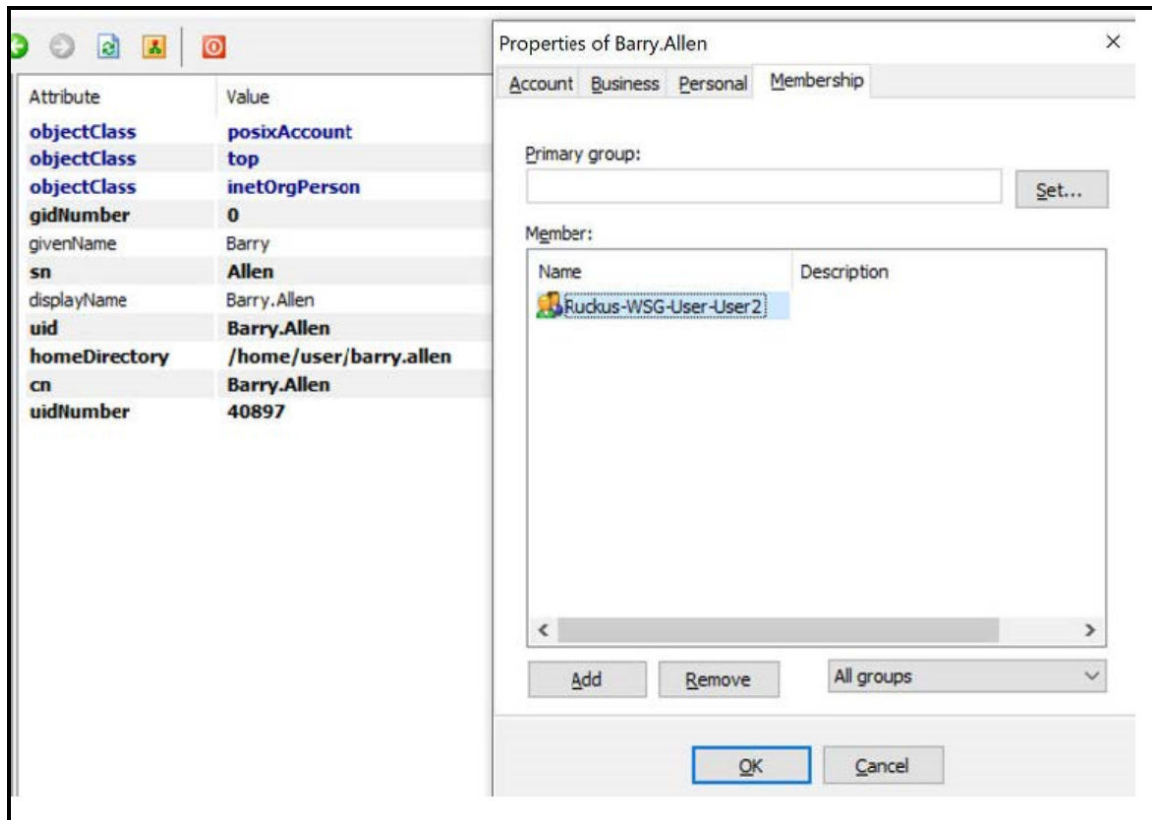
About LDAP Support

Lightweight Directory Access Protocol (LDAP) is an application protocol used to access and maintain directory information services.

In addition to selecting LDAP as the server type, you must also complete the following steps for LDAP-based authentication to work on the controller.

1. Edit the LDAP configuration file on the LDAP server to include the service user name.

FIGURE 7 Supporting LDAP Configuration



2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 14. In this example, LDAP can use User2 only.

3. Select **Administration > Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 11.

4. When you add an AAA server for administrators, select **LDAP** as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 19.

5. Test the LDAP server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 14.

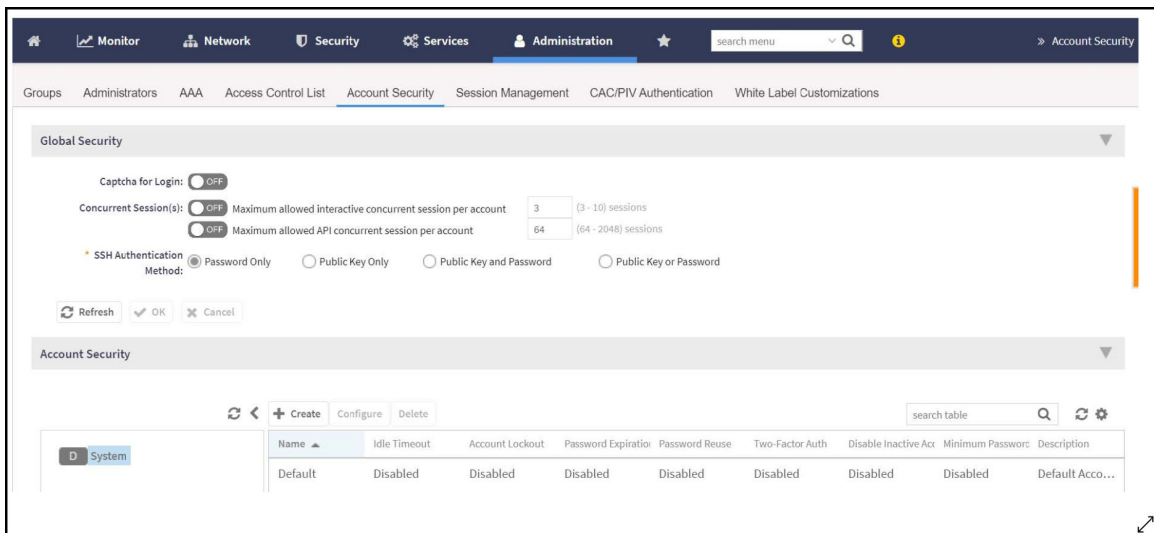
Creating Account Security

Creating an account security profile enables end-users to control administrative accounts to better manage admin accounts, passwords, login, and DoS prevention.

1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Account Security** tab.

The **Global Security** section and **Account Security** section are displayed.

FIGURE 8 Account Security page



3. From Global Security, configure the following:
 - a. **Captcha for Login:** select the option to enable Captcha for log in. The captcha feature provides additional security to ensure a human is signing into the account, and not a robot. If this feature is enabled; when you log into the web interface, the captcha characters are displayed in the login page as shown in the following example.

FIGURE 9 Captcha Enabled in the Login Page



Type the characters as shown in the captcha picture and log in. The characters in the captcha image are case sensitive and can be refreshed if not clear.

- b. **Concurrent sessions:** Click the required options and enter the number of sessions allowed:
 - **Maximum allowed interactive concurrent session per account**
 - **Maximum allowed API concurrent sessions per account**
- c. Click **OK**.

4. From **Account Security**, click **Create**.

The **Create Account Security** page is displayed.

FIGURE 10 Creating Account Security

Create Account Security

Name:

Description:

Session Idle Timeout: ON 15 (1-1440) minutes

Account Lockout: OFF Lock account for 30 (1-1440) minutes after 6 (1-100) failed authentication attempts

ON Lock account forever after 3 (1-100) failed attempts during 15 (1-1440) minute time period.
This option does not apply to AAA Admin Users.

Password Expiration: ON Require password change every 90 (1-365) days

Password Reuse: ON Passwords cannot be the same as the last 4 (1-6) times

Two-Factor Authentication: OFF Require two-factor authentication via SMS
You have to verify your one-time code first to enable it

Disable Inactive Accounts: ON Lock admin accounts if they have not been used in the last 90 (1-1000) days

Minimum Password Length: ON Password must be at least 8 (8-64) characters
When minimum password length is changed, admin should change passwords for all users manually as well. Minimum password length changes apply for all future passwords only

Password Complexity: OFF Password must be fulfilled as below:
When the password complexity is turned from off to on, admin should change all users' passwords manually. The password complexity rule will only be applied to the upcoming password changes.

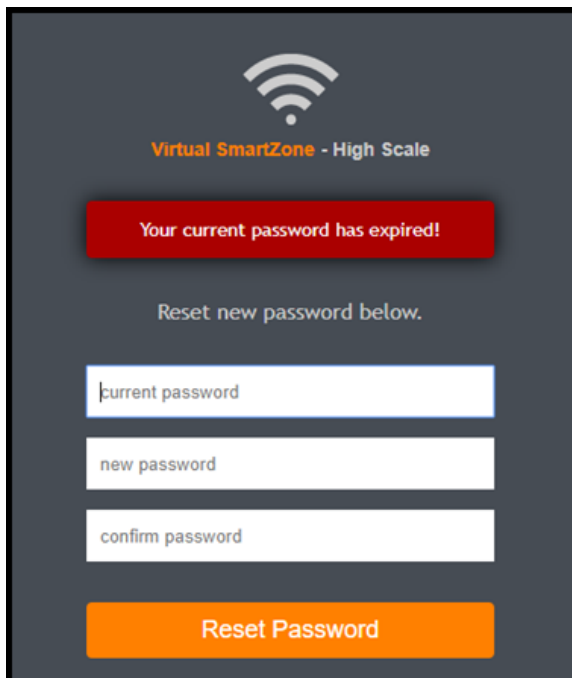
- At least one upper-case character
- At least one lower-case character

5. Configure the following:

- Name: Type the name of the security profile that you want to create.
- Description: Provide a short description for the profile.
- Session Idle Timeout: Click the button and enter the timeout duration in minutes.
- Account Lockout: You can configure the security profile to lock the account based on the duration of the session or number of failed attempts to access the account. Provide the values as necessary. Enable and configure one of the following:
 - Enter the account lockout time and number of failed authentication attempts.
 - Enter the number of failed attempts after which the account is locked and the corresponding time period. After three unsuccessful login attempts in a time interval of 15 minutes, the account is locked and must be released by an Administrator.
- Password Expiration: Click the button and type the number of days for which the account's password will be valid. After the configured number of days, the password will expire and render the account inaccessible. You must change the password before the expiration day to have continued access to the account. By default, the password is valid for a period of 90 days. It can be configured for validity from a minimum of 1 day, to a maximum of 365 days.

If your password has expired, you are prompted to change or reset your password as soon as you log in. Reset the password as shown in the figure.

FIGURE 11 Resetting the Old Password



The screenshot displays a dark gray login screen for 'Virtual SmartZone - High Scale'. At the top center is a white Wi-Fi icon. Below it, a red rectangular box contains the text 'Your current password has expired!'. Underneath this, the text 'Reset new password below.' is centered. There are three white input fields stacked vertically, labeled 'current password', 'new password', and 'confirm password'. At the bottom of the screen is a large orange button with the text 'Reset Password' in white.

- Password Reuse: Prevents the reuse of passwords. Click the button to enable this option. By default, the value is 4 (last 4 passwords cannot be reused).
- Disable Inactive Accounts: Locks the admin user IDs that are inactive for the specified period of time. Click the button and specify the number of days.
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.

Managing Administrator and Roles

Creating Account Security

- Password Complexity: Ensures that the password applies the following rules:
 - At least one upper-case character
 - At least one lower-case character
 - At least one numeric character
 - At least one special character
 - At least eight characters from the previous password is changedSelect the appropriate options.
- Minimum Password Lifetime: Ensures that the password is not changed twice within a period of 24 hours. Select the option.

6. Click **OK** to submit the security profile/form.

The newly created profile is added under the **Account Security** section.

NOTE

You can also edit or delete the profile by selecting the options **Configure** or **Delete**, from the **Administrator** tab.

With new enhancements to account security, SmartZone has a complete feature set to make PCI compliance very simple and straightforward. In addition to local PCI enforcement settings, SmartZone also integrates with SCI for reporting and analytics. SCI version 5.0 and later supports a PCI compliance report, which is based on the relevant PCI-related configuration settings throughout SmartZone. To facilitate the SmartCell Insight PCI report, the SmartZone is capable of sending the following information to SCI:

- Configuration messages as separated GPB messages
- WLAN configuration
- Default configuration changes
- Controller information that identifies the controller model
- Encryption details of communication, for example: CLI, SSH, telnet, Web, API
- Inactive user IDs and session timeout
- Authentication mechanism enforced on user IDs
- Enforcement of password
- Supported mechanism on SZ that can be provided to SCI
- User IDs that are locked after failed attempts
- Authentication credentials that are unreadable and encrypted during transmission
- Enforcement of password standards
- Disallowing duplicate password feature is enabled
- If rogue AP detection is enabled on each AP

To learn more about SCI and the PCI compliance report it provides, check the product page (<https://www.ruckuswireless.com/products/smart-wireless-services/analytics>) and documentation on the RUCKUS support page (<https://support.ruckuswireless.com>).

Active Directory (AD)

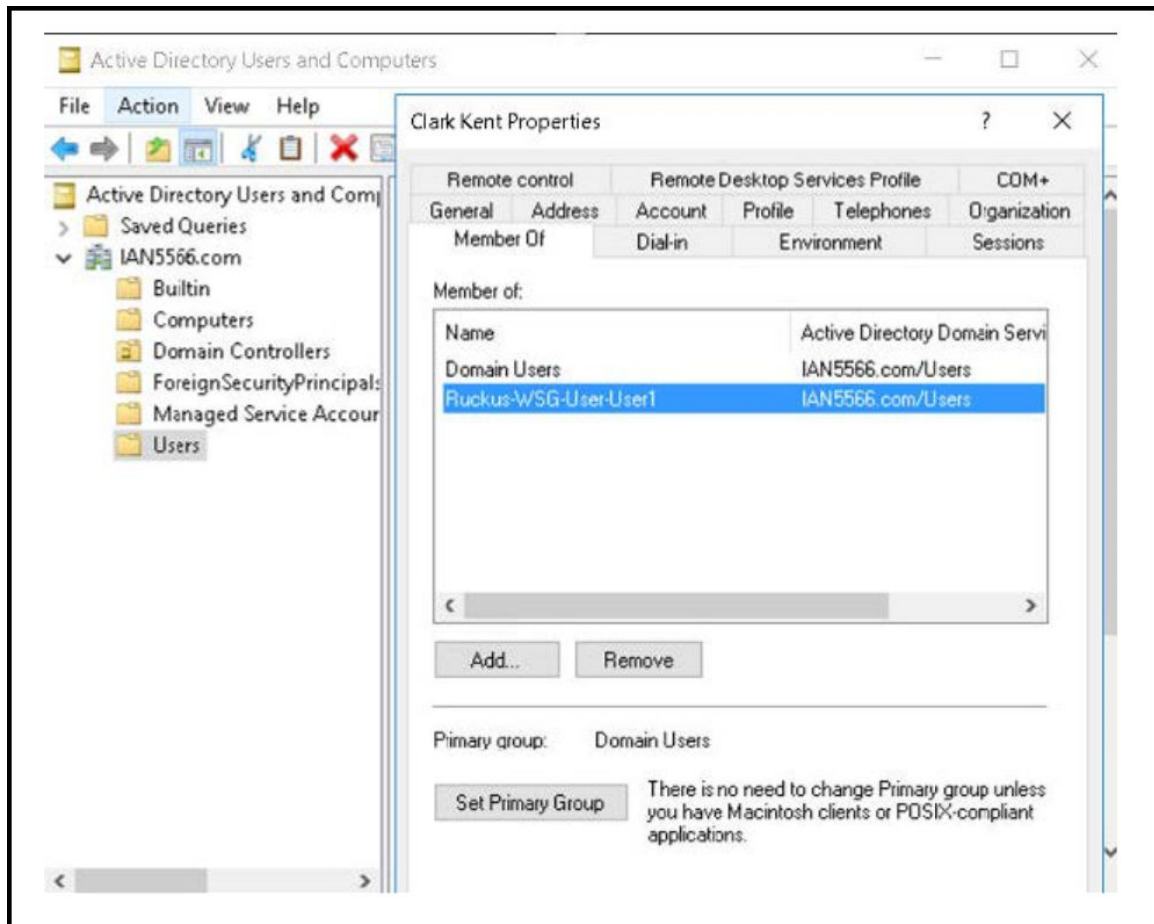
About Active Directory (AD) Support

Active Directory is a domain service that authenticates and authorizes users in a Windows environment.

In addition to selecting AD as the server type, you must also complete the following steps for AD-based authentication to work on the controller.

1. Edit the AD configuration file on the AD server to include the service user name.

FIGURE 12 About Active Directory Support



2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 14. In this example, Active Directory can use User1 only.

3. Select **Administration > Administration > Admins and Roles > Groups**, and then assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 11 .

4. When you add an AAA server for administrators, select **Active Directory** as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 19.

5. Test the AD server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 14.

Creating a User Role with Active Directory Authentication

Configuring user roles using AD authentication provides broad range of directory-based identity-related services.

To create a User Role with AD authentication:

1. Create a new UTP for a particular Role. Refer to [Create an L3 Access Control Policy](#) on page 76.

2. Create a role. Refer to *User Roles*.

3. **NOTE**

Non-proxy Auth servers are not supported.

Create a new Proxy AD server and apply the UTP. Refer *Creating Proxy Authentication AAA Servers*.

4. **NOTE**

In step 4 of the authentication test, for the **Service Protocol** option, choose **Active Directory** and proceed.

Perform an authentication test to ensure that the user gets assigned the correct Role. Refer *Testing AAA Servers*.

5. Create a web authentication portal WLAN configuration and assign the Non-proxy AD server to it. Refer *Creating a WLAN Configuration*.

- a) Choose **WLAN Usage > Authentication Type > Web Authentication**.

- b) Configure the following for **Authentication & Accounting Server**:

Web Authentication Portal: Choose the option from the drop-down.

Authentication Server: Select the Use the Controller Proxy check box and choose the authentication service from the drop-down.

802.1X Authentication

Creating a User Role with 802.1x Authentication

To create a User Role with 802.1x authentication:

1. Create a new UTP for a particular role, see [Create an L3 Access Control Policy](#) on page 76.

2. Create a role. Refer to *User Roles*.

3. **NOTE**
Non-proxy Auth servers are not supported.

NOTE

In step 4 of this procedure, for the **Service Protocol** option, choose **RADIUS** and proceed.

Create a new Proxy RADIUS server and apply the UTP. Refer to *Creating Proxy Authentication AAA Servers*.

4. Perform an authentication test to ensure that the user is assigned the correct Role. Refer *Testing AAA Servers*.
5. Create a web authentication portal WLAN configuration and assign the Non-proxy RADIUS server to it. Refer to *Creating a WLAN Configuration*.
 - a) Choose **WLAN Usage > Authentication Type > Web Authentication**.
 - b) Go to **Authentication Options > Methods**, choose **802.1x EAP** and proceed.

Access Control

- Virtual LAN..... 39
- Restricted Access..... 43
- Creating Blocked Client..... 48
- Creating a Client Isolation Whitelist..... 49
- Creating a Time Based Access Table..... 50
- Creating a Traffic Class Profile 51
- Creating a DNS Server Profile..... 54
- Creating a DNS Spoofing Profile..... 55
- Enabling the Access Control of Management Interface..... 56

Access Control is a data security process. Access control policies are created to identify and verify the users to ensure appropriate access is granted to the user. The main aim of access control is to protect data and assets by reducing the risk of unauthorised intrusions.

Virtual LAN

VLAN Pooling

When Wi-Fi is deployed in a high-density environment such as a stadium or a university campus, the number of IP addresses required for client devices can easily run into the thousands. Allocating thousands of clients into a single, large subnet or VLAN can result in degraded performance due to factors such as broadcast and multicast traffic. VLAN pooling is adopted to address this problem.

VLAN pooling allows administrators to deploy a pool of multiple VLANs to which clients are assigned, thereby automatically segmenting large groups of clients into multiple smaller subgroups, even when connected to the same SSID. As the client device joins the WLAN, the VLAN is assigned to one of the VLANs in the pool based on a hash of the client's MAC address. To use the VLAN pooling feature, you first need to create a VLAN pooling profile, and then you can assign the profile to a specific WLAN or override the VLAN settings of a WLAN group.

NOTE

The 802.11ac wave 2AP models support maximum of 64 VLANs. Other AP models support upto 32 VLANs.

Creating a VLAN Pooling Profile

To create VLAN a Pooling Profile, perform the following:

1. Click **Security > Access Control > VLAN** and select **VLAN Pooling**.
The **VLAN Pooling** screen is displayed.

2. Select the zone and Click **Create**.

The **Create VLAN Pooling Profile** page is displayed.

FIGURE 13 Create VLAN Pooling Profile

Create VLAN Pooling Profile

* Name:

Description:

* [?] VLANs:

Option: MAC Hash

VLAN pooling allows automatic segmentation of large groups of clients into smaller subgroups, even when connected to the same SSID. When a client device joins the Wi-Fi network, a VLAN is assigned based on a hash of the client's MAC address.

OK **Cancel**

3. Enter the following details:

- a. Name: Type a name to identify the VLAN profile.
- b. Description: Type a short description for the VLAN profile.
- c. VLANs: Type the VLAN IDs to be assigned to this pool. VLAN IDs can be separated by hyphens, commas, or a combination (for example, 7-10,13,17,20-28).
- d. Click **OK**.

4. You have created the **VLAN Pooling profile**.

You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **VLAN Pooling** tab.

NOTE

Each VLAN pool can contain up to 64 VLANs, and a maximum of 64 VLAN pools can be created. Each WLAN can be configured with a single VLAN pool. For 802.11ac Wave 1, the dynamic VLAN number is 32. For 802.11ac Wave 2 AP/802.11ax AP, dynamic VLAN number is 64.

VLAN Precedence

Clients are assigned to VLANs by various methods, and there is an order of precedence by which VLANs are assigned and rate limiting is applied. The assignment is commonly from lowest to highest precedence. However, you can create a VLAN Precedence Profile where you can change the order of these precedences.

VLAN Precedence

To create a VLAN Precedence, perform the following:

1. Click **Security > Access Control > VLAN** and select **VLAN Precedence**.

The **VLAN Precedence** page is displayed.

2. Click **Create**.

The **Create Precedence Profile** page is displayed.

FIGURE 14 Create Precedence Profile

Create Precedence Profile

* Name:

Rate Limiting Precedence

↑ Up ↓ Down

| Priority | Description |
|----------|-------------|
| 1 | AAA |
| 2 | DEVICE |
| 3 | WLANUTP |

VLAN Precedence

↑ Up ↓ Down

| Priority | Description |
|----------|-------------|
| 1 | AAA |

OK Cancel

Access Control

Virtual LAN

3. Configure the following:
 - a. Name: Enter a name to identify the profile.
 - b. Rate Limiting Precedence: Use the Up and Down options to set the rate limit priority.

NOTE

When SSID Rate Limiting (restricts total usage on WLAN) is enabled, per-user rate limiting is disabled.

- c. VLAN Precedence: Use the Up and Down options to set the VLAN priority.
- d. Click **OK**.

NOTE

Each VLAN has a default precedence.

You have created a VLAN Precedence profile.

NOTE

You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** from the **VLAN Precedence** tab.

VLAN Name

Virtual LAN (VLAN) is a logical network segmented by function or application without a regard to physical location. A VLAN breaks single network into multiple sections thus effectively creating multiple stand alone networks out of the same network. This is secure and reduces number of broadcasts received on individual device.

VLAN name can be 32 characters in length. You can configure upto 4094 port-based VLANs on a layer 2 and 3 switches. The default VLAN (VLAN1) uses default values and you cannot create, modify, delete or suspend activities on the default VLAN.

TABLE 4 VLAN Ranges

| VLAN Numbers | Range | Description |
|--------------|----------|----------------------------------|
| 1 | Normal | Default |
| 2-1005 | Normal | Configurable VLANs |
| 1006-4094 | Extended | Configurable but with parameters |

Creating VLAN Name Profile

To create VLAN Name Profile, perform the following:

1. Click **Security > Access Control > VLAN > VLAN Name**.

The **VLAN Name** page is displayed.

2. Select a zone from the hierarchy and click **Create**.
The **Create VLAN Name Profile** page is displayed.

FIGURE 15 Create VLAN Name Profile

The screenshot shows a web form titled "Create VLAN Name Profile". It contains the following elements:

- A text input field labeled "* Name:".
- A text input field labeled "Description:".
- A section labeled "* VLAN Mappings:" containing a table with two columns: "* VLAN Name" and "* VLAN Id".
- Buttons for "+ Add", "x Cancel", and a trash icon labeled "Delete" next to the table.
- At the bottom right, there are two large buttons: "OK" and "Cancel".

3. Enter the following fields:
 - a. Name: Enter a name to identify the profile.
 - b. Description: Enter a short description for the VLAN name profile.
 - c. VLAN Mapping: Enter VLAN Name and VLAN ID and click **Add**.

The new VLAN name profile is displayed in the below list .

NOTE

You can also cancel or delete the new VLAN name profile .

Restricted Access

The Restricted Access profile can be created without having any blocked ports or enabling well known and additional entries in the whitelist ports. The Restricted Access Point (AP) profile can be configured multiple ways through SmartZone user interface.

The access point node on the network can be vulnerable to malicious attacks. The AP is a critical node on the network and therefore such an attack can expose the whole network. The Restricted Access profile provides a mechanism to restrict unauthorized access to the AP and allows access only to authorized users, thereby increasing the inherent security of the AP.

NOTE

A maximum of 5 Restricted Access profiles can be created per zone.

The AP currently has the following categories of open ports:

TABLE 5 Well known ports on Access Points

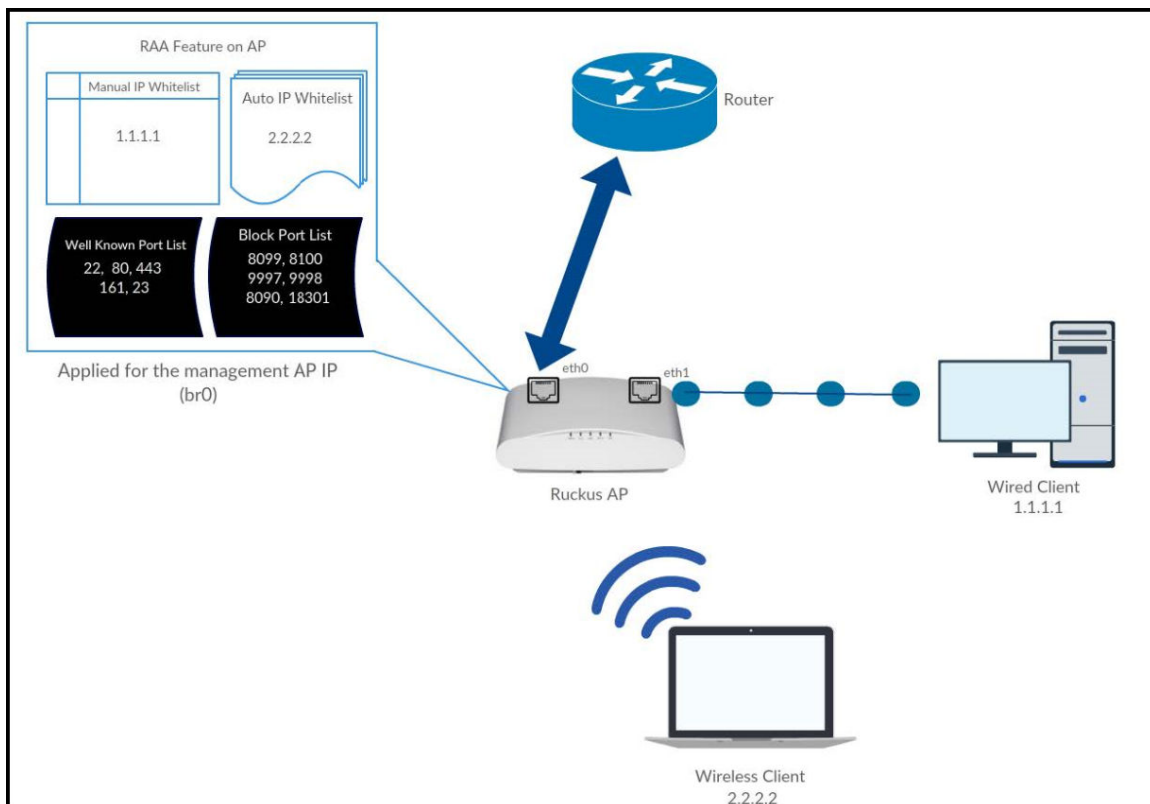
| Sl. No. | Port | Use | Protocol |
|---------|------|--------|-------------------|
| 1 | 80 | HTTP | TCP - IPv4 & IPv6 |
| 2 | 22 | SSH | TCP - IPv4 & IPv6 |
| 3 | 443 | HTTPS | TCP - IPv4 & IPv6 |
| 4 | 161 | SNMP | UDP - IPv4 & IPv6 |
| 5 | 23 | TELNET | TCP - IPv4 & IPv6 |

Overview

The well known port list includes the ports that are most likely to be exploited, with restricted access enabled, any node on the network trying to access the AP using these ports is blocked. This blocking functionality is configurable from the User Interface (UI) by an administrator. The administrator can perform the following functions:

- The administrator can allow temporary or permanent access to these ports for an IP or a list of IPs (IP and Subnet). These IP(s) when configured are added to the Manual White List (Max 10) and these IP(s) are given unrestricted access to the AP.
- The administrator can add ports or a range of ports to the Port Black List (Max 10) as well. These ports will be inaccessible for any node on the network that is not part of the Manual White List as configured by the administrator.

FIGURE 16 Restricted Access Overview



Creating a Restricted AP Access Profile

The Access Point (AP) is a critical node in the network that can be at risk of the malicious attacks as some of its ports are open. The Restricted AP Access Profile addresses this kind of risk and enhances AP security.

Restricted AP Access protects the AP in the following ways.

1. By blocking access to the standard well know open ports on the AP, such as:
 - Port- 22 (TCP -IPv4 & IPv6) - For SSH Operation
 - Port- 23 (TCP - IPv4 & IPv6) - For Telnet Operation
 - Port- 80 (TCP - IPv4 & IPv6) - For HTTP Operation
 - Port- 443 (TCP - IPv4 & IPv6) - For HTTPs Operation
 - Port- 161 (UDP -IPv4 & IPv6) - For SNMP Operation
2. By blocking access to the Internal ports on the AP (used mainly for Ruckus internal communication), such as:
 - Wireless Internet Service Provider roaming (WISPr) internal ports
 - Port 9997 (http) : [Subscriber portal]
 - Port 9998 (https): [Subscriber portal]
 - Port 1997 (http): [Captive Portal Listening Server]
 - Port 1998 (https): [Captive Portal Listening Server]
 - Walled Garden internal Ports
 - Port 8090 (http) : [Subscriber portal]
 - Port 8099 (https) : [Subscriber portal]
 - Port 18090 (http) : Captive Portal Listening Server /Redirect server listen port]
 - Port 18099 (https): Captive Portal Listening Server/Redirect server listen port]
 - Speedflex Port 18301
 - Proxy Web server for Unauthorized UEs 8100
 - DNSMASQ 53
3. By providing a mechanism to block any ports or port range to restrict access.
4. By allowing the AP to be accessed by authorized users.

To create a Restricted AP Access profile, perform the following steps.

1. Click **Security > Access Control > Restricted AP Access**.

This displays the **Restricted AP Access** screen.

2. In the **Restricted AP Access** screen, select a zone from the system tree, and click **Create**. This displays **Create Restricted AP Access Profile** screen.

FIGURE 17 Create Restricted AP Access Profile

Create Restricted AP Access Profile

* Name:

Description:

Blocked Port List: * Protocol: * Port:

| Protocol | Port |
|----------|------|
| | |

OFF Block well known ports

List of well known ports
SSH: 22
TELNET: 23
HTTP: 80
HTTPS: 443
SNMP: 161

IP Address Whitelist: * IP:

| IP |
|----|
| |

The SCG IP (10.1.13.64 / 2005::64) and the DP IP (10.148.124.64 / 2148::71e2:a8a3:5c8a:7fa5, 10.148.124.65 / ::) are whitelisted by default.

3. Enter the following:
 - a. Name: Type a name to identify the Restricted AP Access Profile.
 - b. Description: Type a short description for the Restricted AP Access Profile.
 - c. Blocked Port List: Select the protocol (TCP, UDP or Both) from the **Protocol** drop-down, and enter the port number in the **Port** field and click **Add** to add the entries or click **Cancel** to re-type and add the entry. The protocol and the port get listed in the table below the **Blocked Port** List. Select an entry and click **Delete** to remove the values in the table.
 - d. Block well known ports: Click the toggle button to enable blocking all well known ports.
 - e. IP Address Whitelist: When Restricted AP Access is enabled, network devices may use a non-whitelisted IPv6 IP address for Restricted AP Access related operations, which may cause unexpected result. So, it is recommended to add IPv6 IP addresses manually.
4. Click **OK**.

You have created the Restricted AP Access profile.

Configuring a Restricted Access via Access Point

This topic describes the steps to configure and apply Restricted AP Access Profile through Access Point tab.

1. Click **Wireless > Access Points**.
This displays **Access Points** page.
2. Select a zone from the system tree and click **Configure selected Domain/Zone/Group** icon.
This displays **Edit Zone** page.
3. In the **Edit Zone** page, navigate to **Advanced Options** and locate the **Restricted AP Access Profile** field.
Click the toggle button to **On** and enable the **Restricted AP Access Profile**.
4. Click add icon to **Create Restricted AP Access Profile** from Access Points page.
This displays **Create Restricted AP Access Profile** screen.
5. Enter the details as provided in the [Creating a Restricted AP Access Profile](#) on page 45 topic.
6. The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.
7. Select the Restricted AP Access profile from the drop-down list to apply to the selected zone.

Configuring a Restricted Access via Templates

This topic describes the steps to configure a Restricted AP Access Profile through **Templates** tab.

1. Click **Administration > System > Templates** and select **Zone Template**.
This displays **Zone Templates** page.

NOTE

To create a Restricted AP Access Profile via Templates, you have to create a new zone and map the zone to a group

2. After creating a new Zone, select the new zone and click **Configure**.
This displays the **Edit Zone Template** screen.
3. In the **Edit Zone** page, navigate to **Advanced Options** and locate the **Restricted AP Access Profile** field.
Click the toggle button to **On** and enable the **Restricted AP Access Profile**.
4. Click add icon to **Create Restricted AP Access Profile** from Access Points page.
This displays **Create Restricted AP Access Profile** screen.
5. Enter the details as provided in the [Creating a Restricted AP Access Profile](#) on page 45 topic.
6. The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.
7. Select the Restricted AP Access profile from the drop-down list to apply to the selected zone.

Enabling Restricted AP Access Profile

To enable the Restricted Access, perform the following:

1. Click **Network > Wireless > Access Point**.
2. Select a zone from the system tree and click **Configure selected Domain/Zone/Group** icon.
This displays **Edit Zone** page.

Access Control

Creating Blocked Client

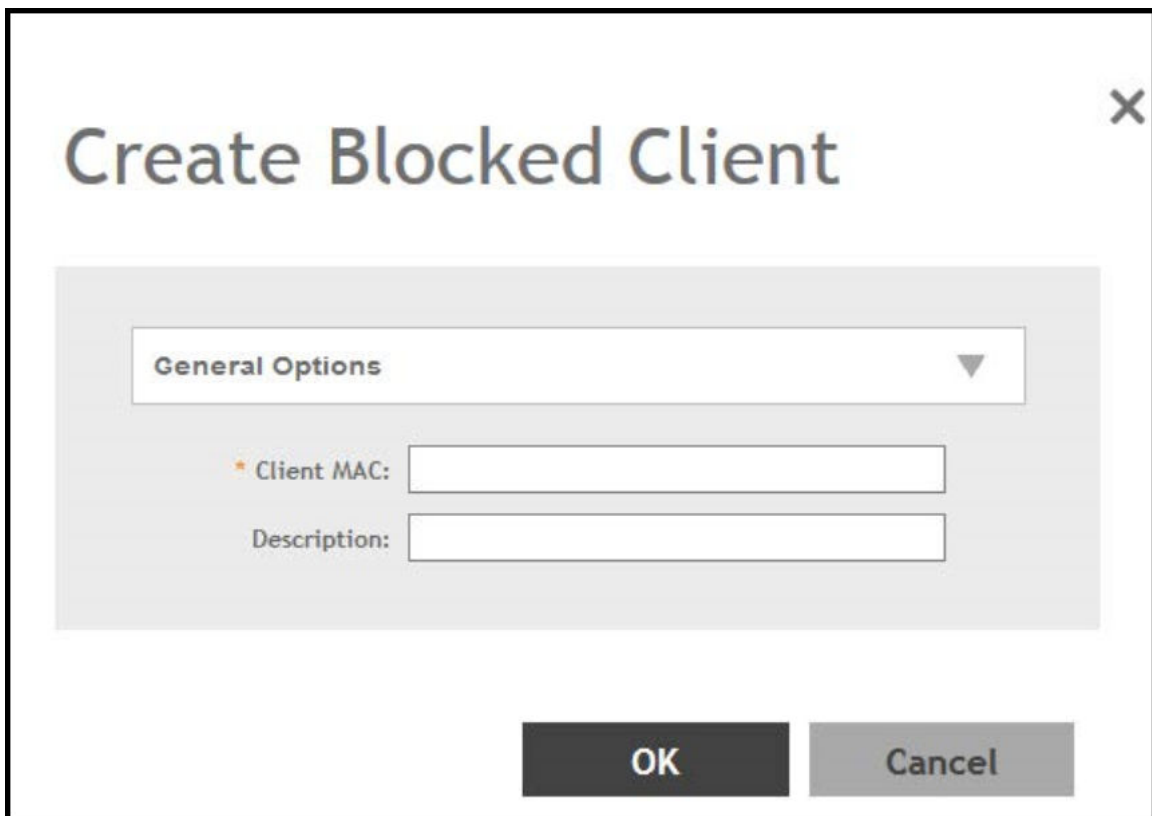
3. In the **Edit Zone** page, navigate to **Advanced Options** and locate the **Restricted AP Access Profile** field. Click the toggle button to **On** and enable the **Restricted AP Access Profile**.

Creating Blocked Client

You can deny access to the network for specific clients by using the block client access control feature. Client blocking is configured on a per-client, per-zone basis.

1. Click **Security > Access Control > Blocked Client**.
This displays **Blocked Client** page.
2. Select a zone from the system tree and click **Create**.
This displays the **Create Blocked Client** page.

FIGURE 18 Create Blocked Client



The screenshot shows a dialog box titled "Create Blocked Client" with a close button (X) in the top right corner. The dialog contains a "General Options" dropdown menu. Below the dropdown are two input fields: "Client MAC:" (with a red asterisk) and "Description:". At the bottom of the dialog are two buttons: "OK" and "Cancel".

3. Enter the following:
 - a. **Client MAC:** Type MAC address of the client that you want to block.
 - b. **Description:** Type a short description for blocking the client.
 - c. Click **OK**.

You have created a blocked client profile for the selected client.

NOTE

You can also edit, clone and delete a list by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Blocked Client** tab.

Creating a Client Isolation Whitelist

This feature allows the administrator to manually specify a list of approved wired destinations that may be reachable by wireless clients.

NOTE

The whitelist applies only to destinations that are on the wired network, and it will not work on wireless destinations.

1. Click **Security > Access Control > Client Isolation Whitelist**.

This displays **Client Isolation Whitelist** page.

2. Select a zone from the system tree and click **Create**.

This displays **Create Client Isolation Whitelist** page.

FIGURE 19 Create Client Isolation Whitelist

Create Client Isolation Whitelist

* Name:

Description:

Auto Whitelist: ON APs will auto-discover gateway devices and add them to the isolation whitelist.

Client Entries

| MAC | IP Address | Description |
|-------------------|--------------|-----------------------------|
| 00:1B:44:11:3A:B7 | 123.89.72.46 | Client MAC and IP Addresses |

Access Control

Creating a Time Based Access Table

3. Enter the following:
 - a. Name: Enter a name to identify the client.
 - b. Description: Enter short description about the client.
 - c. Auto Whitelist: Click on the toggle button to enable the AP to scan for devices automatically and include them in the isolation whitelist.

NOTE

Each VLAN can have only 16 entries in the whitelist and WLAN can have a maximum of 64 client isolation manual entries.

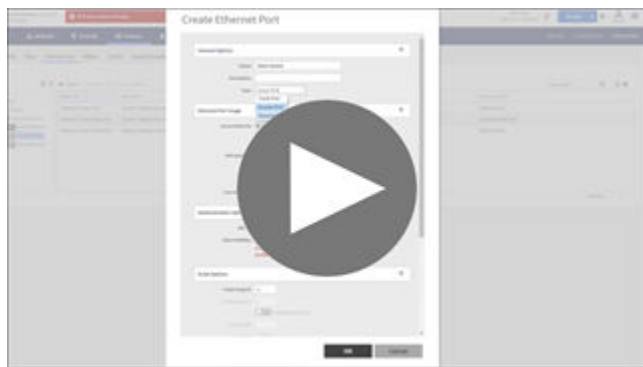
- d. Client Entries: To manually add the clients to the list, click **Create** and provide client information such as MAC address (mandatory), IP address and Description.
- e. Click **OK**.

You have created the list of whitelisted clients that can access the network.



VIDEO

Creating Ethernet Port Profiles. Creating an Ethernet port profile (securing secondary wired port), port types explained



[Click to play video in full screen mode.](#)

Creating a Time Based Access Table

You can control client access to the network by providing a time schedule. This security measure restricts the access based on specific time parameters.

1. Click **Security > Access Control > Time Based Access**.
This displays the **Time Based Access** page.
2. Select a zone from the system tree and click **Create**.
This displays **Create Time Based Access Table** page.
3. Select the **Time Schedule** tab, and then select the zone for which you want to create the schedule.

4. Click **Create**.

The **Create Time Schedule Table** page appears.

FIGURE 20 Create Time Based Access Table

Create Time Based Access Table

General Options

* Schedule Name: Time Schedule

Schedule Description: Short description of the time schedule

Schedule Table

Time Zone: (GMT+0:00) UTC

| Time | AM | | | | | | | | | | | PM | | | | | | | | | | | |
|------|----|---|---|---|---|---|---|---|---|----|----|----|---|---|---|---|---|---|---|---|---|----|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Sun | 0 | | | | | | | | | | | 0 | | | | | | | | | | | 0 |
| Mon | | | | | | | | | | | | | | | | | | | | | | | |
| Tue | 0 | | | | | | | | | | | 0 | | | | | | | | | | | 0 |
| Wed | | | | | | | | | | | | | | | | | | | | | | | |
| Thu | 0 | | | | | | | | | | | 0 | | | | | | | | | | | 0 |
| Fri | | | | | | | | | | | | | | | | | | | | | | | |

OK Cancel

5. Enter the following:
 - a. Schedule Name: Enter a name for the schedule.
 - b. Schedule Description: Enter a short description for this schedule.
 - c. Draw the schedule table.
 - d. Click **OK**.

You have created the schedule.

NOTE

You can also edit, clone and delete the schedule by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Time Schedule** tab.

Creating a Traffic Class Profile

A traffic class allows you to classify traffic according to a set of criteria that you define, such as source and destination IP addresses.

To create a Traffic Class Profile, perform the following:

1. Click **Security > Access Control > Traffic Classes**.

Access Control

Creating a Traffic Class Profile

2. Select the zone from the system tree and click **Create**.

This displays **Create Traffic Class Profile** page.

FIGURE 21 Create Traffic Class Profile

Create Traffic Class Profile

General Options ▼

* Name:

Description:

Traffic Classes ▼

+ Create Configure Delete

| Traffic Class | Destinations |
|---------------|--------------|
|---------------|--------------|

OK Cancel

3. **General Options**
 - a. Name: Enter a name to identify the traffic class profile.
 - b. Description: Enter a short description for traffic class profile.

4. **Traffic Classes**

- a. Click **Create**. This displays **Destination Addresses** window.

Enter a name to identify the destination address.

- b. **Destination Addresses - Access Control Rule Entry**: Enter an access control rule as shown in the format section under the field and click **Add**. The access control address is displayed in the **Access Control Rule Entry** table.

Import CSV Format: Click this field to import a CSV format file from your local computer.

FIGURE 22 Destination Addresses

The screenshot shows a configuration window titled "Destination Addresses". At the top, there is a "Name:" label followed by an empty text input field. Below this is a dropdown menu labeled "Destination Addresses". Underneath the dropdown is an "Access Control Rule Entry" label followed by another empty text input field. To the right of this input field are three buttons: "+ Add", "Import CSV" (with a dropdown arrow), and "Cancel" (with a close icon). Further right are two more buttons: "Cancel" (with a close icon) and "Delete" (with a trash icon). Below the input field is a section titled "Access Control Rule Entry" containing a list of allowed formats:

- The following format are allowed for access control rule entry.
- Format:
- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
 - *.amazon.com
 - *.com

At the bottom right of the window are two large buttons: "OK" and "Cancel".

5. Click **OK**.

NOTE

Only four traffic classes can be added in a single **Traffic Class** profile.

You have created a Traffic Class Profile.

NOTE

The IP destination is reachable only when the IP is not part of traffic class but is present under Split Tunnel. The Split Tunnel policy is effective only when both **Split Tunnel** and **Traffic Class** features are enabled together.

Creating a DNS Server Profile

A DNS server profile allows you to specify the primary and secondary address of the DNS server for devices to identify the host name within the specified zone.

To create a DNS Server Profile, perform the following:

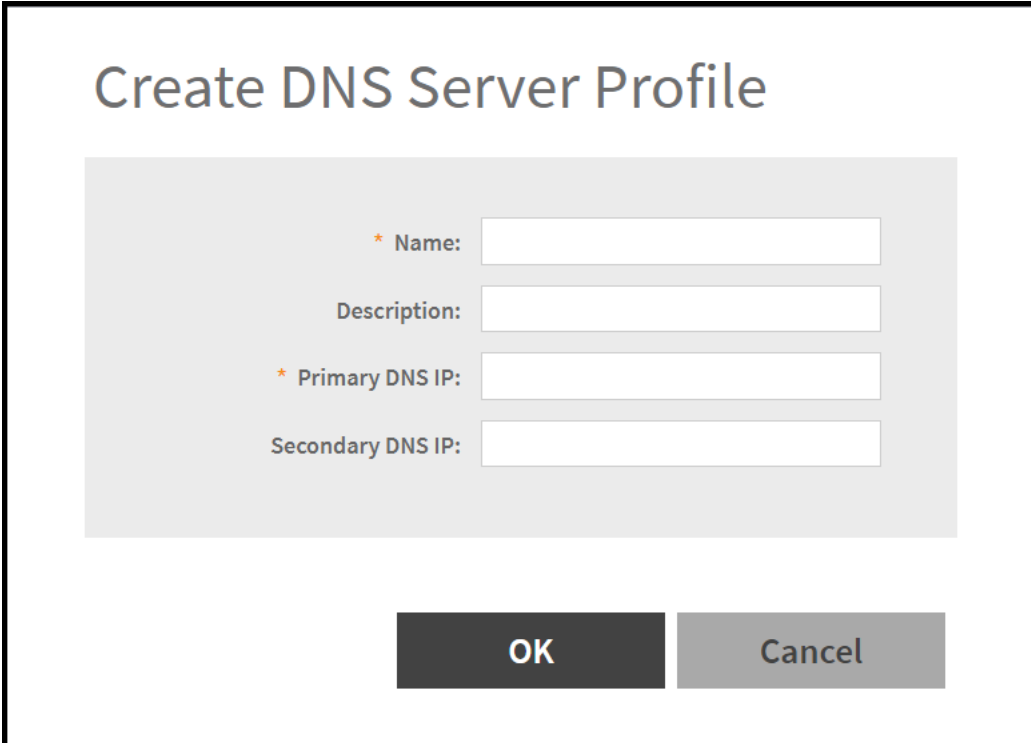
1. Click **Administration** > **System** > **DNS Servers**.

This displays the **DNS Servers** page.

2. Click **Create**.

This displays the **Create DNS Server Profile** page.

FIGURE 23 Create DNS Server Profile



The screenshot shows a dialog box titled "Create DNS Server Profile". Inside the dialog, there is a light gray rectangular area containing four input fields. The first field is labeled "* Name:" and is required. The second field is labeled "Description:". The third field is labeled "* Primary DNS IP:" and is required. The fourth field is labeled "Secondary DNS IP:". Below these fields, there are two buttons: "OK" and "Cancel".

3. Enter the following:
 - a. Name: Type a name to identify the DNS server profile.
 - b. Description: Enter a short description for profile.
 - c. Primary DNS IP: Enter the primary DNS IP address.

NOTE

This feature supports IPv4 address format.

- d. Secondary DNS IP: Enter the secondary DNS IP address.

NOTE

This feature supports IPv4 address format.

- e. Click **OK**.

You have created a DNS Server Profile.

NOTE

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** from the **DNS Servers** page.

Creating a DNS Spoofing Profile

A DNS spoofing profile allows you to specify individual Fully Qualified Domain Name (FQDN) entries to bypass DNS resolution and provide clients with the result specified in the associated rules.

To create a DNS Spoofing Profile, Perform the following:

1. Click **Services > Others > DNS Spoofing**

Access Control

Enabling the Access Control of Management Interface

2. Select a zone to create a DNS spoofing profile and click **Create**.
This displays **Create DNS Spoofing Profile** page.

FIGURE 24 Create DNS Spoofing Profile

The screenshot shows a web-based dialog box titled "Create DNS Spoofing Profile". It is divided into two main sections. The first section, "General Options", contains two text input fields: "Name" and "Description". The second section, "Rules", features three buttons: "+ Create", "Configure", and "Delete". Below these buttons is a table with two columns: "Domain Name" and "IP Address". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

3. Configure the following:
 - a) **General Options**
 1. **Name:** Enter a name to identify the DNS spoofing profile.
 2. **Description:** Enter a short description for the profile.
 - b) **Rules**
 1. Click **Create**, and the **Create Rules** dialog box is displayed.
 2. **Domain Name :** Enter the FQDN of an individual host entry.
 3. **IP List: IP Address:** Enter the and IP Address to resolve the domain name and click **Add**. If the user sends rule with the domain name configured in the DNS Spoofing profile, then the AP responds with the IP address configured in the DNS Spoofing profile for the requested domain name.
 4. e
 - c) Click **OK** to confirm the creation of DNS spoofing profile.

NOTE

You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone** or **Delete** from the **DNS Spoofing** page.

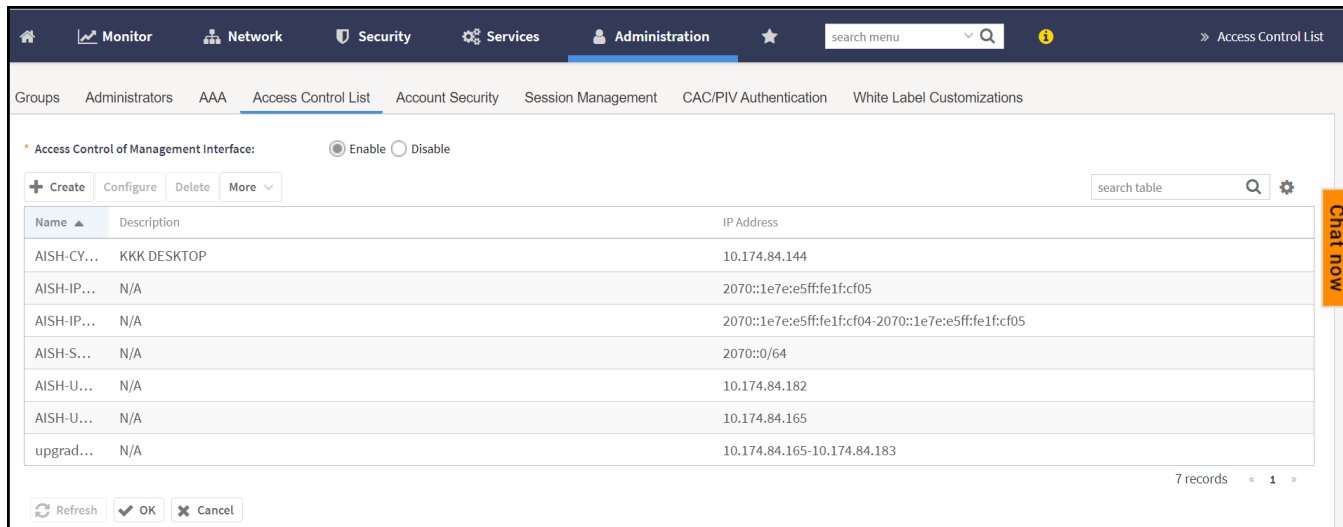
Enabling the Access Control of Management Interface

1. click **Administration > Admins and Roles > Access Control List**.
This displays the **Access Control of Management Interface** page.

- 2. Click **Enable**.

This displays the **Access Control List**.

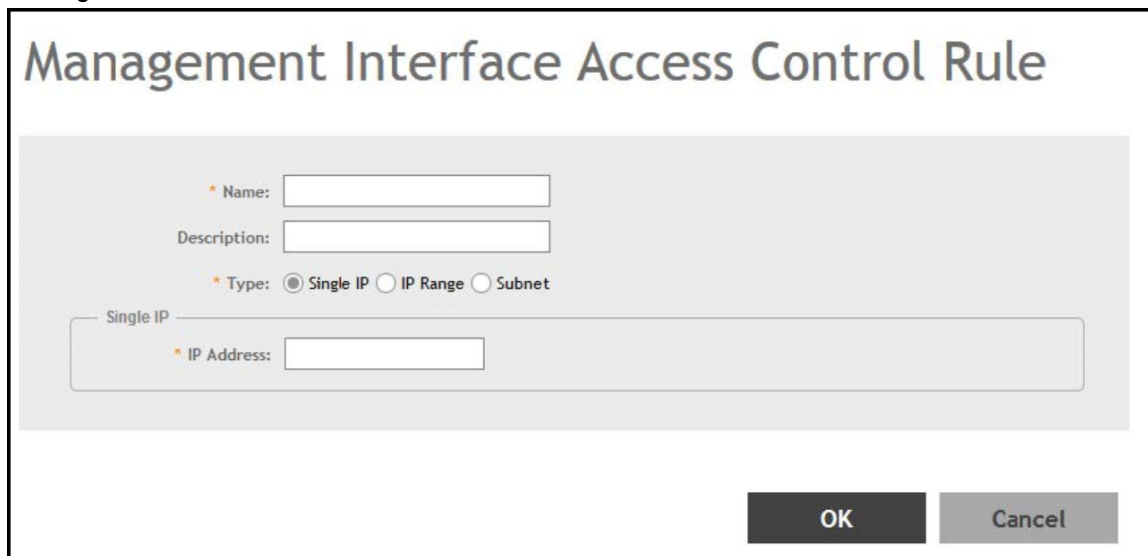
FIGURE 25 Access Control of Management Interface



- 3. Click **Create**.

The **Management Interface Access Control Rule** page appears.

FIGURE 26 Management Interface Access Control Rule



Access Control

Enabling the Access Control of Management Interface

4. Enter the following:
 - a. Name: Type a name to identify the rule.
 - b. Description: Enter a short description for the rule.
 - c. Type: Select one of the following
 - Single IP: Type the IP address of the interface that can be accessed per this rule.
 - IP Range: Type the range of IP address that will be allowed access.
 - Subnet: Type the network address and subnet mask address of the interface that will be allowed access.
 - d. Click **OK**.

NOTE

You can also edit and delete the list by selecting the options **Configure** and **Delete** respectively, from the **Access Control List** tab.

Wireless Intrusion Detection and Prevention Services (WIDS/WIPS)

- [Wireless Intrusion Detection and Prevention System..... 59](#)

Wireless Intrusion Detection and Prevention System

Wireless Intrusion Detection and Prevention System (WIDS/WIPS) is a security structure that monitors a WLAN for any threats from rogue devices.

Configuring a Rogue Classification Policy

A user can create a rogue classification policy with rules at the zone and monitoring-group level. This allows automatic classification when specific rogue detection criteria is met.

Complete the following steps to create a rogue classification policy.

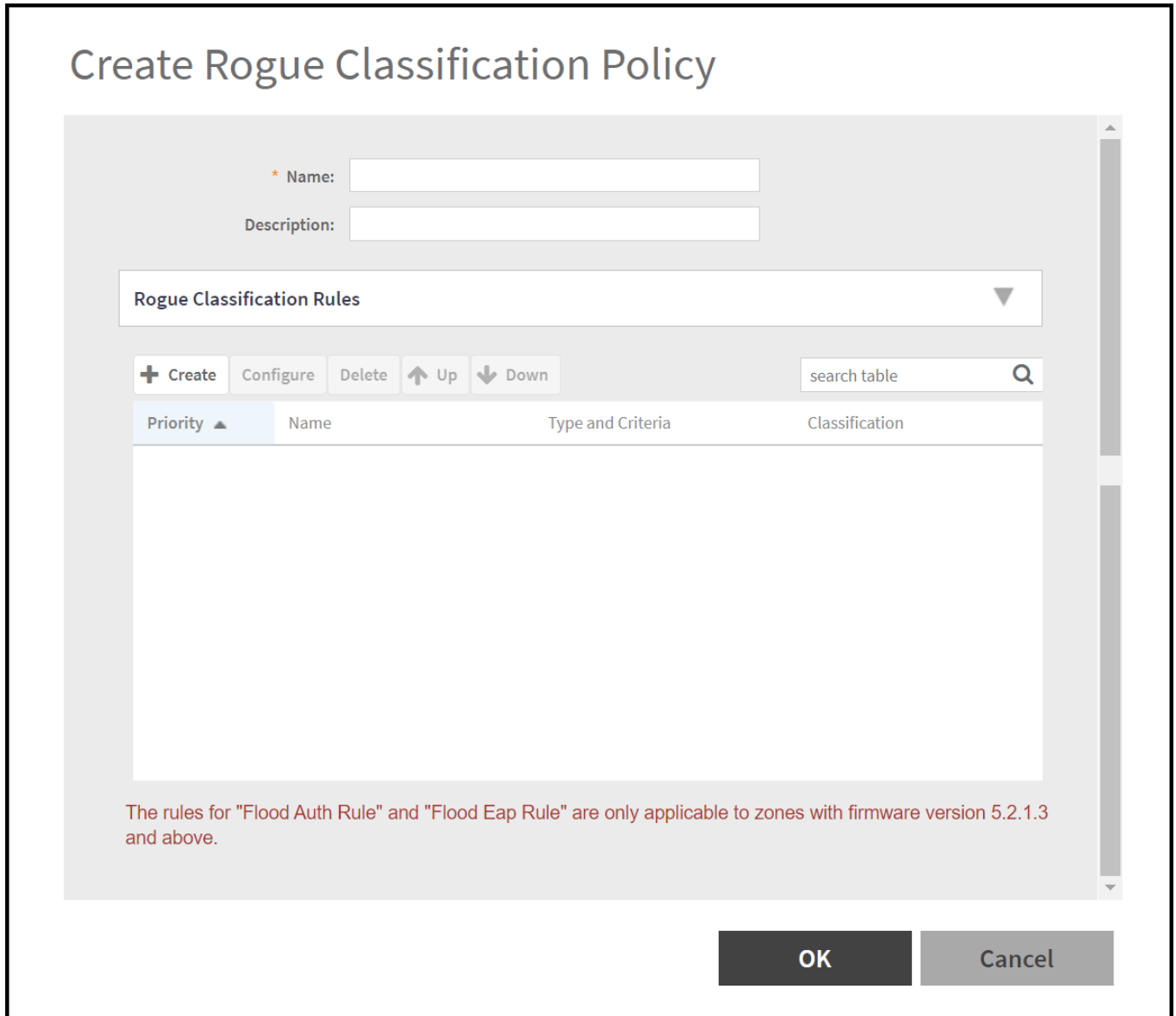
1. Click **Security > Access Control > WIPS & WIDS**.

This displays the **Policy** page.

Wireless Intrusion Detection and Prevention Services (WIDS/WIPS)
Wireless Intrusion Detection and Prevention System

2. Select the zone from the system tree and click **Create**.
This displays the **Create Rogue Classification Policy** page.

FIGURE 27 Create Rogue Classification Policy



Create Rogue Classification Policy

* Name:

Description:

Rogue Classification Rules

+ Create Configure Delete Up Down search table

| Priority ▲ | Name | Type and Criteria | Classification |
|------------|------|-------------------|----------------|
|------------|------|-------------------|----------------|

The rules for "Flood Auth Rule" and "Flood Eap Rule" are only applicable to zones with firmware version 5.2.1.3 and above.

OK Cancel

3. Enter the following:
 - a. Name: Type a name to identify the rogue classification policy.
 - b. Description: Enter a short description for the rogue classification policy.

4. Rogue Classification Rules

- a. Click **Create**. This displays **Rogue Classification Rules** window.
- b. Enter the following:
 - Name: Enter a rule name to identify.
 - Rule Type: Select a rule type for classification policy from the drop-down list.
 - Classification: Select a classification type to match the above criteria.
- c. Click **OK** to create rogue classification rules.

5. Click **OK** to create Rogue Classification Policy.

NOTE

Click **Configure** or **Delete** to edit or delete a rogue classification policy respectively. To prioritize a classification rule, select the rule from the list and click **Up** or **Down** to position the rule.

NOTE

The user can use command line interface in SZ to disable or change threshold packets per seconds for CTS abuse, RTS abuse, Deauth flood, disassociation flood and other detection types.

- To change the threshold detection follow the command: remote ap-cli <ap-mac> "set rogued <attack-type> <number pf packets>". Example: remote ap-cli 8c:fe:74:1c:d6:b8 "set rogued rtsthreshold 10"
- To enable / disable flood detection follow the command : remote ap-cli <ap-mac> "set rogued <attack-type> enable/disable". Example: remote ap-cli 8c:fe:74:1c:d6:b8 "set rogued rtsdetect enable"

FIGURE 28 Classifying a Rogue Policy

```
set rogued : set rogued
-> debug {level} <level: 0~7>
-> rtsdetect {enable|disable} <enable or disable RTS frame detection>
-> rtsthreshold {value} <value >= 1, num of frames per second>
-> ctsdetect {enable|disable} <enable or disable CTS frame detection>
-> ctsthreshold {value} <value >= 1, num of frames per second>
-> deauthdetect {enable|disable} <enable or disable DEAUTH frame detection>
-> deauththreshold {value} <value >= 1, num of frames per second>
-> disassocdetect {enable|disable} <enable or disable DISASSOC frame detection>
-> disassocthreshold {value} <value >= 1, num of frames per second>
-> authdetect {enable|disable} <enable or disable AUTH frame detection>
-> auththreshold {value} <value >= 1, num of frames per second>
-> eapdetect {enable|disable} <enable or disable EAP frame detection>
-> eapthreshold {value} <value >= 1, num of frames per second>
-> maxclientdetect {enable|disable} <enable or disable max client detection>
-> maxclientthreshold {value} <value >= 1, num of clients per AP>
-> ssidlargerthan32 {enable|disable} <enable or disable SSID larger than 32 bytes detection>
-> weakprotocol {enable|disable} <enable or disable weak or outdated protocol detection>
-> packetfloodingdetect {enable|disable} <enable or disable packet flooding detection>
-> pktfloodingthreshold {value} <value >= 1, num of frames per second>
-> failureattempt {enable|disable} <enable or disable failed attempt to join the WLAN detection>
-> failureattemptthreshold {value} <value >= 1, num of failed
```


Certificates

- Importing SmartZone as Client Certificate..... 63
- Assigning Certificates to Services..... 64
- Generating Certificate Signing Request (CSR)..... 65
- Managing AP Certificates..... 66
- Importing SmartZone (SZ) Trusted CA Certificates/Chains..... 68
- DataPlane validates SmartZone..... 69
- AP Validate SmartZone Controller..... 70

Importing SmartZone as Client Certificate

When you have an SSL certificate issued by the certificate provider, you can import it into the controller and use it for HTTPS communication.

To complete this procedure, you will need the following:

- The signed server certificate
- The intermediate CA certificate (at least one)
- The private key file

NOTE

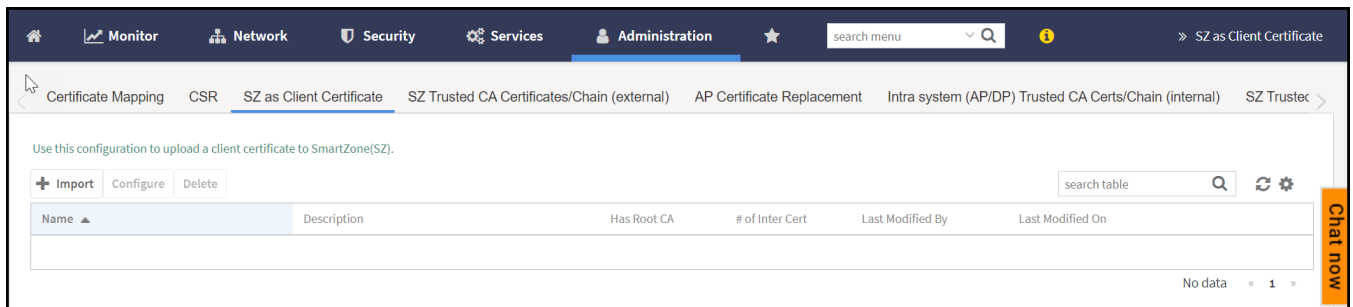
The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

To import a signed server certificate, perform the following:

1. Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.
2. Click **Administration > System > Certificates > SZ as a Client Certificate**.

This displays **SZ as a Client Certificate** page.

FIGURE 29 SZ as Client Certificate



3. Click **Import**, this displays **Import Client Certificate** page.

FIGURE 30 Import client Certificate

Import Client Certificate

* Name:

Description:

Client Certificate

* Client Certificate: Browse Clear

Intermediate CA certificate: Browse Clear

Browse Clear

Browse Clear

Root CA certificate: Browse Clear

* Private Key: Browse Clear

Validate OK Cancel

4. Enter the following:

- Name: Type a name to identify the certificate.
- Description: Enter a short description about the certificate.
- **Client Certificate:** To upload any of the options in this section, select the corresponding check box, click **Browse** and select the location in your local system and upload the certificate.

NOTE

For **Intermediate CA certificates**, if you want to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates. Only CRT or PEM format is supported for the CA certificate.

NOTE

If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate.

NOTE

Private Key can be imported through uploading file or using Customer Signing Request (CSR).

5. Click **OK**.

You can also edit, clone or delete the profile by selecting the options **Configure**, or **Delete** from the **SZ as Client Certificate** page.

Assigning Certificates to Services

You can map certificates to services

To specify the certificate that each secure service will use:

1. In the main menu, click **Administration**. Under **System** menu, hover mouse over the **Certificates** and select **Certificate Mapping**.

2. Select the certificate that you want to use for each of the following services:
 - **Management Web**—Used by Web UI and Public API traffic.
 - **AP Portal**—Used by Web Auth WLAN.
 - **Hotspot (WISPr)**—Used by WISPr WLAN control (Northbound Interface, Captive Portal, and Internal Subscriber Portal) traffic.
 - **Ruckus Intra-device Communication**—Used by AP control traffic.
3. To view the public key, click **View Public Key**, the Certificate Public Key form appears with the public key.
4. Click **OK**.

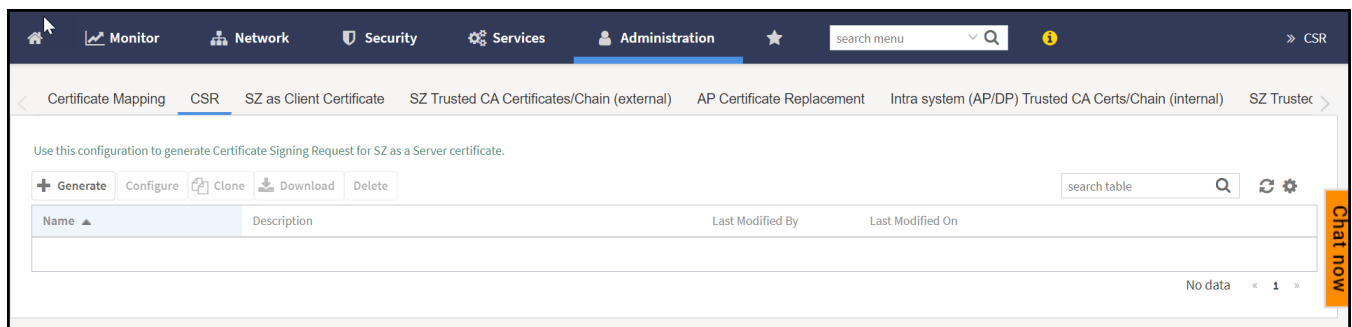
Generating Certificate Signing Request (CSR)

If you do not have an SSL certificate, you will need to create a Certificate Signing Request (CSR) file and send it to an SSL certificate provider to purchase an SSL certificate.

To create a CSR file:

1. Click **Administration > System > CSR**. This displays the Certificate Signing Request (CSR) page.

FIGURE 31 Certificate Signing Request (CSR)



2. Click **Generate**. This displays the **Generate CSR** form.
3. Enter the following:
 - **Name**: Type a name to identify the CSR.
 - **Description**: Enter a short description for this CSR.
 - **Common Name**: A fully qualified domain name of your web server. This must be an exact match (for example, **www.ruckuswireless.com**).
 - **Email**: An email address (for example, joe@ruckuswireless.com).
 - **Organization**: Complete legal name of your organization (for example, **Google, Inc.**). Do not abbreviate your organization name.
 - **Organization Unit**: Name of the division, department, or section in your organization that manages network security (for example, **Network Management**).
 - **Locality/City**: City where your organization is legally located (for example, **Sunnyvale**).
 - **State/Province**: State or province where your organization is legally located (for example, **California**) Do not abbreviate the state or province name.
4. Select the **Country**.

Certificates

Managing AP Certificates

5. Click **OK**, the controller generates the certificate request. When the certificate request file is ready, web browser downloads the file automatically.
6. Go to the default download folder of your web browser and locate the certificate request file. The file name is **myreq.zip**.
7. Use a text editor (for example, Notepad) to open the certificate request file.
8. Go to the website of your preferred SSL certificate provider, and then follow the instructions for purchasing an SSL certificate.
9. When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr, and then complete the purchase.
10. After the SSL certificate provider approves your CSR, you will receive the signed certificate via email.
11. Copy the content of the signed certificate, and then paste it into a text file.
12. Save the file.

NOTE

You can also edit, clone, download or delete a CSR by selecting the options **Configure**, **Clone**, **Download** or **Delete** respectively.

Managing AP Certificates

AP certificates are valid for a period of time and have to be replaced when they expire.

NOTE

Although AP Certificate Expire Check is enabled by default, when an AP with an expired certificate joins the controller, this check automatically gets disabled. To restore security:

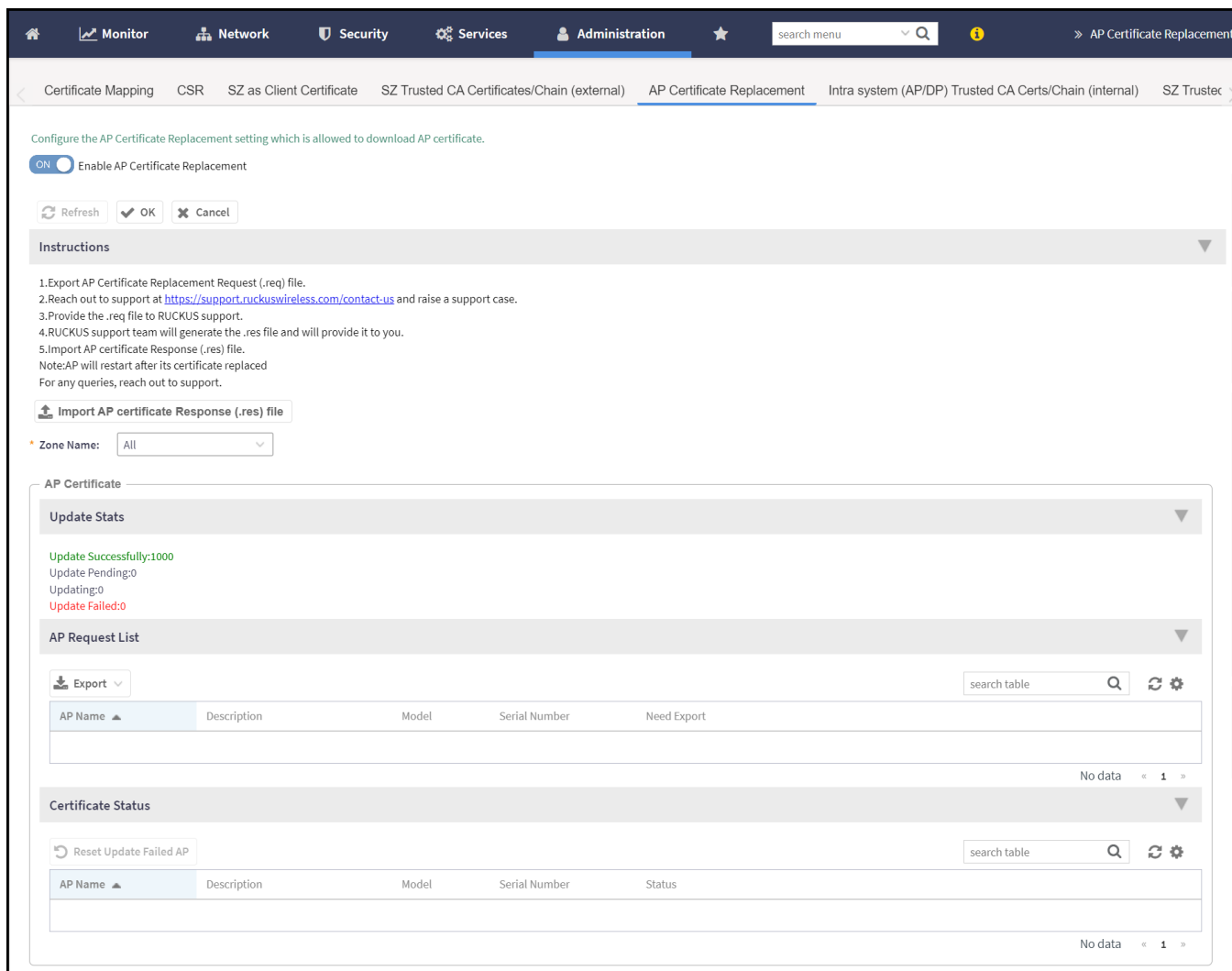
- All APs with expired certificates need to be replaced with a new valid certificate.
- Manually enable certificate check using `ap-cert-expired-check` CLI command in the configuration mode.

You must get AP certificate replacement before your AP certificate expires. The system generates an *apCertificateExpireSystem* alarm and event when an AP certificate expires.

For AP Certificate replacement, perform the following:

1. Click **Administration > System > Certificates > AP Certificate Replacement**. This displays the **AP Certificate Replacement** page.

FIGURE 32 AP Certificate Replacement



2. By default, the Enable AP Certificate Replacement is disabled. Click the **Enable AP Certificate Replacement** button to enable the AP certificate replacement and follow the instructions on the screen.
3. From the AP Certificate Replacement page of the application, click **Import AP certificate Response (.res) file**. The Import AP certificate for replacement form appears.
4. Click **Browse** and select the file.
5. Click **OK**.

NOTE

All APs included in the imported response (.res) file reboot after their certificate is refreshed.

6. Select the **Zone Name** from the drop-down list.

Certificates

Importing SmartZone (SZ) Trusted CA Certificates/Chains

AP Certificate

In the **AP Certificate** section, the following details are displayed.

- **Update Stats:** Displays the status of the AP certificate.
- **AP Request List:** Displays the list of requested APs.
- **Certificate Status:** Displays the certificate status. If the status is:
 - **Updating:** Controller is in the process of updating the certificate.
 - **Update Failed:** Controller failed to update the certificate.

NOTE

The AP reports to the controller at 15-minute intervals. As a result, it may take up to 15 minutes for the AP to update its certificate status on the web interface.

After all the APs are updated with the new certificates, manually enable the `ap-cert-expired-check` CLI command in the config mode to restore security and reject APs that try to connect with expired certificate

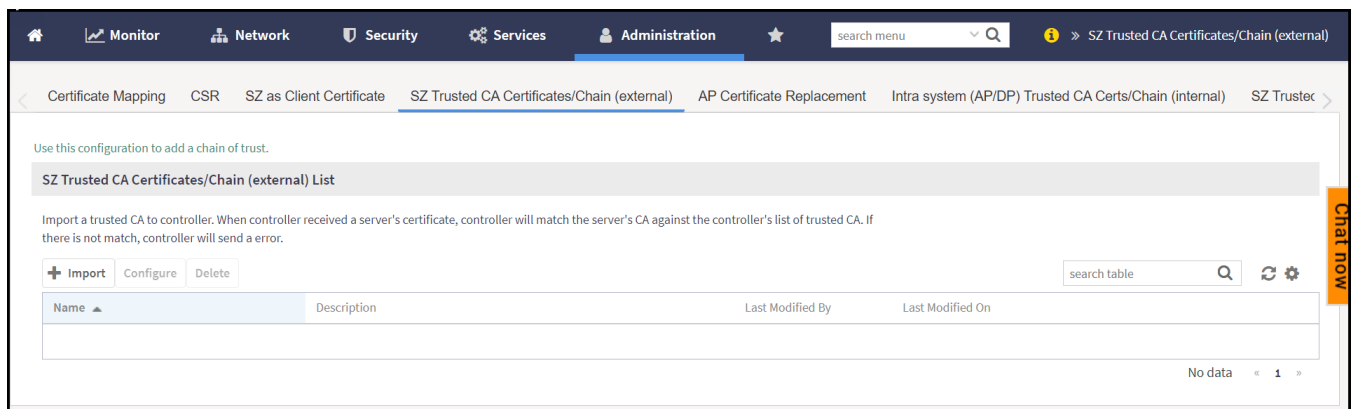
Importing SmartZone (SZ) Trusted CA Certificates/Chains

When a controller receives a server's certificate, it matches the server's CA against the list of trusted CAs it has. If there is no match, the controller sends an error.

To import a CA certificate, perform the following:

1. Click **Administration > System > Certificate** and select **SZ Trusted CA Certificates/Chain (external)**. This displays **SZ Trusted CA Certificates/Chain (external)** page.

FIGURE 33 SZ Trusted CA Certificates/Chains



2. Click **Import**. This displays the **Import CA Certs (Chain)** window.
3. Enter the following details:
 - a. **Name:** Type a name to identify the CA Certificate.
 - b. **Description:** Enter a short description for the CA Certificate.
 - c. **Intermediate CA Certificates:** Click **Browse** and select the file from your local system. If you need to upload multiple intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.

- d. Root CA Certificate: Click **Browse** and select the file from your local system.
 - e. Click **OK** to add the newly imported certificate.
4. Click **OK**.

NOTE

You can also edit or delete a CA certificate by selecting the options **Configure** or **Delete** respectively.

NOTE

The controller does not support the CA certificate with p7b (windows format), only CRT or PEM format is supported. If the Certificates signed by CA chain has more than 5 chain length then you can upload only the Root CA of the certificate.

DataPlane validates SmartZone

DataPlane validates the incoming SmartZone certificate to check if the certificate is valid.

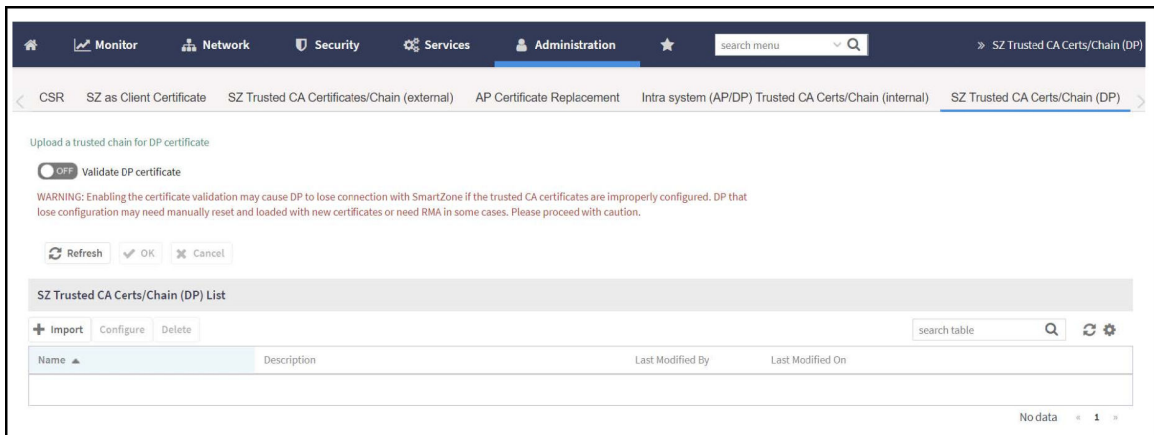
When the Dataplane discovers SmartZone for the first time, Dataplane validates if the SmartZone has the same certificate. If the certificates match then the connection is establishes otherwise it is terminated.

To upload the certificate, perform the below steps:

DataPlane Setup script

1. Import the DataPlane setup script and upload the certificate in SZone Trusted CACerts/Chain (DP).

FIGURE 34 Upload DataPlane Certificate



Certificates

AP Validate SmartZone Controller

- Copy the entire trusted cert content including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

FIGURE 35 Setup Upload Certificate

```
Please make sure SZ/DP certificate are matched
When certificate verification is enabled
If certificate verify fail, DP can't connect to SZ
Do you want to upload vSZ server certificate chain (y/n):y
*****
Paste your certificate sentence including BEGIN/END CERTIFICATE:
*****
Example:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
*****
When you input "-----END CERTIFICATE-----" press enter to finish
Or you can type "###" and press enter to stop
-----BEGIN CERTIFICATE-----
Cert content
-----END CERTIFICATE-----
Verify your certificate format now, wait a moment.
```

- After the setup process, users should be able to enable the server validation via the DataPlane CLI.

The upload command is `enable->config->controller->set_trust_chain`

- For vDP the upload command is `show dp_root_ca`. The root CA is generated in the location `/etc/dp_config/discover` and use this root CA to sign a client cert for vDP TLS connection.
- For physical DP, it should use the MIC cert to do TLS connection. The certificate should pass the validation with Ruckus root CA.

AP Validate SmartZone Controller

Access Point (AP) can validate the SZ by SZ's Public Key or trusted certificates.

Smart Zone can edit the Domain name after the installation

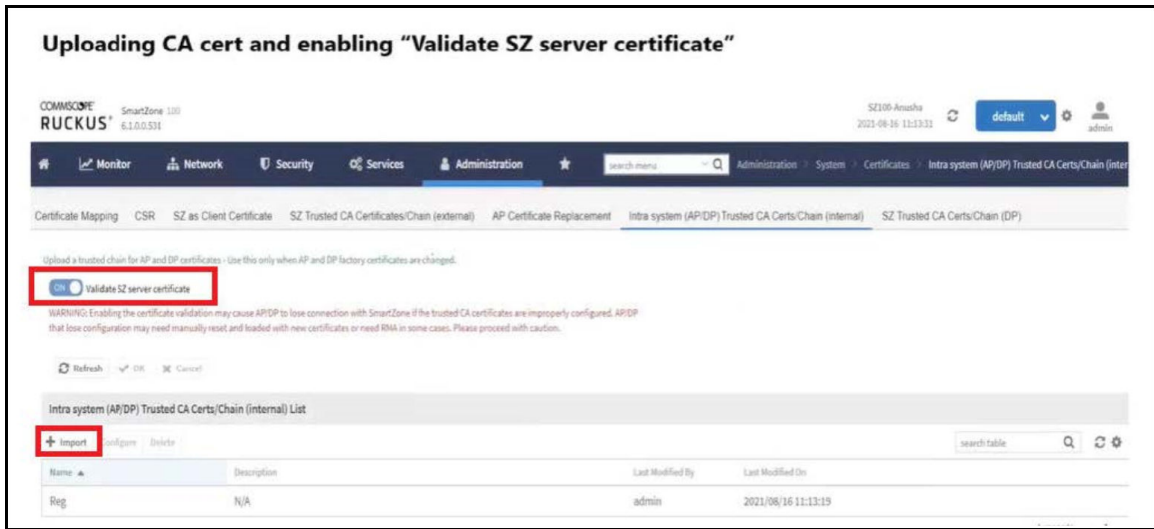
Smart Zone can show the Infra (Communicator) certificate's pem data.

When Server validation is enabled, SZ will push the configurations to AP.

Follow the below steps for the validation of server certificates:

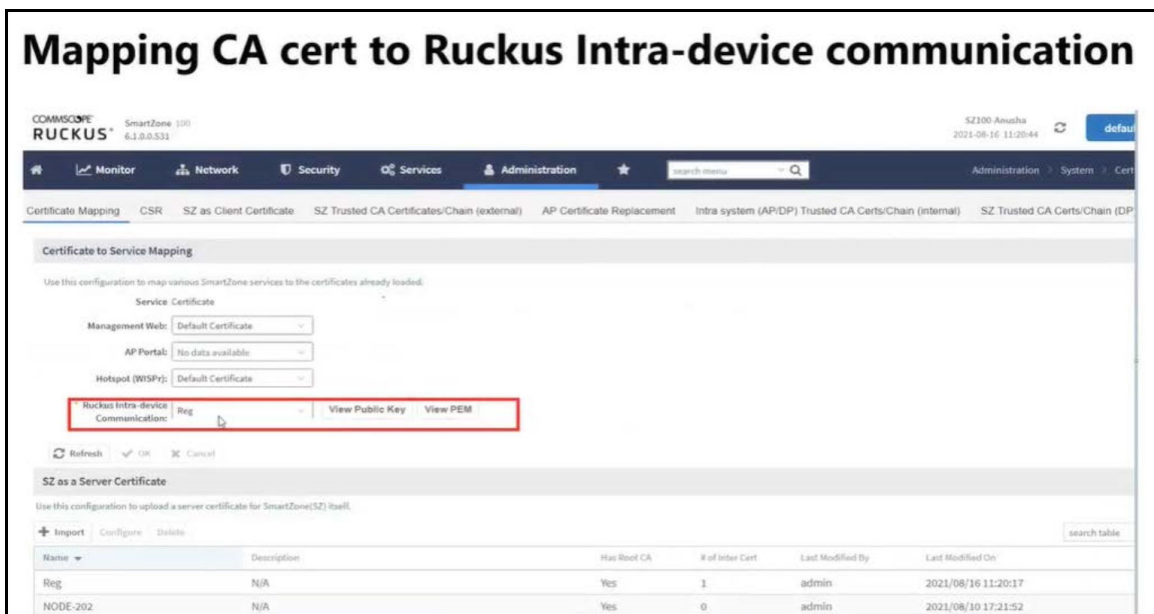
- Go to **Administration > Intra System (AP/DP) Trusted Certs/Chain (Internal)**.

FIGURE 36 SZ Certificate Validation



2. Click "Import" to add valid trusted CA certificate/chain as per the figure above.
3. Enable the "Validate Server certificate".
4. The configuration will be pushed to SCG managed AP's.
5. Upload the certificate in the **Administration>Certificate Mapping> SZ as a Certificate**.
6. Map Server certificate to Ruckus Intra-Device Communication also change the below heading from Mapping CA Cert to Mapping Server Certificate.

FIGURE 37 Mapping CA Certificate



Certificates

AP Validate SmartZone Controller

- The certificate will be validated when AP connects to SCG.
- Configuration Method:

Part 1: Using Public Key

The certificate mapping is done in Administration>System>Certificates> Certificate Mapping.

- Copy the public key from the above marked "View Public key", Enter the Public key in AP CLI using command " set scg pubkey <publickey> ".
- Enable the server cert validation in AP using command "set scg server-validate enable".
- If public key matches The AP will be listed in staging zone.

Success message : ssl_cert_verify_callback:294 SSL Verification OK.

In Ap CLI execute command "get scg ".

```
SCG gwloss|serverloss timeouts: 1800|7200
Controller Cert Validation : enable
Controller Cert Validation Result: success
-----
OK
rkcli: █
```

- If public key is not matching error message,
In Ap CLI execute command "get scg ".

```
Controller Cert Validation : enable
Controller Cert Validation Result: failed
-----
```

SSL certificate verification failed.

ERROR: check_http_status:542 Curl error: Peer certificate cannot be authenticated with given CA certificates."

Part 2: Using CA Cert

- In AP CLI configure ca cert using command "set scg trusted-cert ".


```

rkscli: set scg trusted-cert
*****
Paste your certificate sentence including BEGIN/END CERTIFICATE:
Example:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
*****
When you complete all certificate, please type press "CERT-DONE" to finish
Or you can type "###" and press enter to stop
-----BEGIN CERTIFICATE-----
MIIEjzCAvegAwIBAgIJA0iIFySsSakQMA0GCSqGSIb3DQEBAUAMF4xCzAJBgNV
BAYTAKlOMQwwCgYDVQQIDANLQVIXDTALBgNVBACMBEJscmUxDzANBgNVBAoMB1J1
Y2t1c2EPMA0GA1UECwwGUnVja3VzMRAdDgYDVQDDAadyb290X2NhMB4XDITxMDky
MzEwMTYwMVVoXDTM2MDkxOTEmTYwMVowXjELMAKGA1UEBhMCSU4xDDAKBgNVBAgM
A0tBUjENMA5GA1UEBwwE0mxyZTEPMA0GA1UECgwGUnVja3VzMQ8wDQYDVQQLDAZS
dWNrdXMxEDA0BgNVBAMMB3Jvb3RfY2EwggGIMA0GCSqGSIb3DQEBAQUAA4IBjwAw
ggGKAoIBGQCaNqu0eTLT6Fpa1slxSKeMIJiaaFDJ7AiqhBA7RG5fjZ51zCpicKhJ
AiofLaU+LlQiasLHcejtmR25M9PK6LjLXkxi7tuV6QEkl/xIqIFZzi3K0LgVv9i
p/NaugBIFcGhrJSBw1ch3JOM0TbWT0HFBWeldiF47aqKNqblewUyMQG1JaXoqCzI
hGQudV5a5lFlSaCREwdfayzQ6LeeBsYust4YzeeFD1WIW3iJGfZnZQdeIR9vhtT
jimTMUMnRP1D00T5TA+zFbFwM7kkh6W6cdeFqGzxvk3NT2TiyXfSmVf5ZdJD070L
CE1+fvWAagNzMja9S6G2WtAZmddQR0HRlpfr+zyNS9qj40nfKz6/Tw84kk5kgJu
bgAweu4TJnBc5Kie0c99VWZ2d3FtUbvE3wL3ewhA+YpQ2nh8+m0tdWnCBuKpSx5J
01MjgHusUzIZ3zy+TEg41coHdwZRAz7oR+vh6o+QCGcjVDlq9N4oyVYHpPjPOGfm
fyIlxIC9JgcCAwEAAANQME4wHQYDVR00BBYEFDWSRJDz750MD72vqijxyZ8im2HB
MB8GA1UdIwQYMBaAFDWSRJDz750MD72vqijxyZ8im2HBMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEMBQADggGBAFhXn18/TGfSZUsE0tZ6vNtGThVGIzon8d8aESVG
0g0//le/f0nXmZP2dvmVbStckOUKvAkURxzULVe5d8mxKMYiTwoVGkN+pkllFMn4
chYa2cJ08pCeysHiIdT9RtygvP62CBjppq+a8YjsKXPgiHY0nW0dUKjUJ+z6hg0K
fqtXc8q3ePdu09GJm+ws7K/+CxKW5DKQdLyL/Ew7LfyA2j7ogdXqYmlWbDSzxtFE
3bymmmIx9Lty7Uhn4DoB107yDMoL3Z5rYUzyd3igPf2GD71arhfGkKwCBu04cHgcg
QhCnwatXfXN4Ntb0RU4bvDvxvHCh86LF1LmigrZjRuAyAZn25LdicsffEXWTtChv
2c6B0TQvuucdsIB5K00h1QLsbRmoksMi7BgTVj1Fd1/uAUKS31W/IzaVCNb8S5w1L
gardUR401pXe0MXACR2x1U8CLzC199eFLfk//om7drVnBCR0BgQJy3E0Q6XcP4r
FJncWkB8bvtgt6tQdd7YXa+VsQ==
-----END CERTIFICATE-----
"CERT-DONE"
Set SZ public key/cert done
OK
rkscli: █
    
```

- Enable the server cert validation in AP using command “set scg server-validate enable”.
- If CA certificate is validated the AP will be listed in staging zone.

9. Domain name configuration:

For release 6.1 fresh installation of domain name is mandatory to support AP/DP validate the controller feature. FQDN (Fully Qualified Domain Name) consists of domain name and the host name. The below table is an example of cluster deployment based on the domain name in a cluster deployment.

TABLE 6 Cluster Deployment

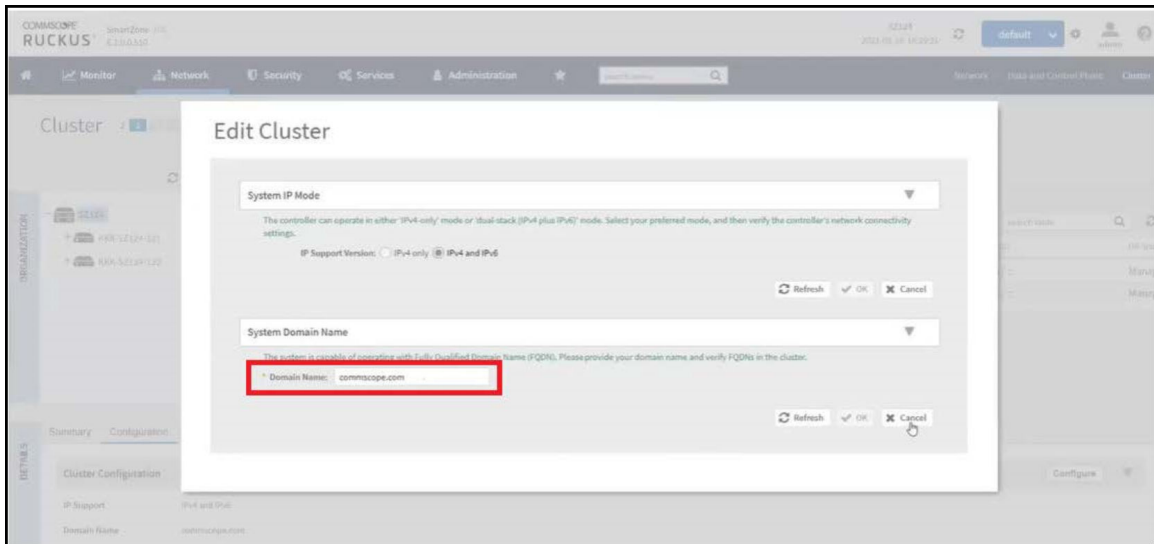
| Cluster Domain Name | Node# | Host Name | FQDN |
|---------------------|--------|-----------|-------------------|
| ruckus.com | Master | Master | master.ruckus.com |
| | Slave1 | Slave1 | slave1.ruckus.com |
| | Slave2 | Slave2 | slave2.ruckus.com |
| | Slave3 | Slave3 | slave3.ruckus.com |

Domain name can be modified after installation by navigating to **Network > Data and control Plane > Cluster > Select the cluster > Configuration > Configure**.

Certificates

AP Validate SmartZone Controller

FIGURE 38 Edit Cluster



Firewall Profile

- [Managing a Firewall Profile.....](#) 75

Managing a Firewall Profile

A firewall profile defines the level of protection. It allows to choose the attributes before applying a policy.

To create a firewall profile, perform the following steps:

1. Select **Firewall**, the **Firewall Profiles** page is displayed.
The **Summary** tab displays the firewall profiles in chart and graph format. You can filter the profiles based on duration and zone.
2. Select **Profiles** tab and click **Create**.
This displays the **Create Firewall Profile** page.

FIGURE 39 Creating Firewall Policy

Create Firewall Profile

Name:

Description:

[?] Rate Limiting: Uplink OFF Rate Limit supports maximum of 100 clients on the wlan

Downlink OFF

L3 Access Control Policy: +

L2 Access Control Policy: +

Application Policy: +

URL Filtering Policy: +

Device Policy: +






OK Cancel

3. In the **Name** field, enter a name for this profile.
4. In the **Description** field, enter a short description for this profile.
5. In the **Rate Limiting** field, select the **Uplink** and **Downlink** options to specify and apply rate limit values for the device policy to control the data rate.

Firewall Profile

Managing a Firewall Profile

6. Configure the following policies:

- a. Select the **L3 Access Control Policy** from the drop-down list or click  to create a new policy. Refer to [Create an L3 Access Control Policy](#) on page 76 for more information.
- b. Select the **L2 Access Control Policy** from the drop-down list or click  to create a new policy. Refer to [Creating an L2 Access Control Service](#) on page 79 for more information.
- c. Select the **Application Policy** from the drop-down list or click  to create a new policy. Refer to [Creating an Application Control Policy](#) on page 82 for more information.
- d. Select the **URL Filtering Profile** from the drop-down list or click  to create a new profile. Refer to [Enabling URL Filtering on the WLAN](#) on page 90 for more information.
- e. Select the **Device Policy** from the drop-down list or click  to create a new policy. Refer to [Creating a Device Policy](#) on page 95 for more information.

7. Click **OK**.

NOTE

You can also edit, clone and delete a firewall profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Firewall Profiles** page.

NOTE

At system level user can create maximum 64 firewall profiles.

Create an L3 Access Control Policy

An L3 Access Control Policy can be created to block or limit user traffic based on a number of factors, including Source IP address, Port, Destination IP address, Protocol, etc. Additionally, an L3 Access Control Policy can be created to shape traffic according to a configurable Application Control Policy.

After L3 Access Control Policy is created, it can be applied to any WLAN from the **Wireless LANs** page.

1. Select **Security > Access Control > L3 Access Control**.

The **L3 Access Control** page is displayed.

2. Click **Create**.

This displays the **L3 Access Control Policy** page.

FIGURE 40 Creating an L3 Access Control Policy

Create L3 Access Control Policy

* Name:

Description:

* Default Access: Default access if no rule is matched: Allow Block

All the unicast, multicast and broadcast traffic, except configured in ACL rules will be allowed. Add rules appropriately

< + Create Configure Delete Up Down >

| Priority | Description | Matching Criteria | Type | Access |
|----------|-------------|--|------|--------|
| 1 | Allow DNS | Direction:Inbound Destination Port:53 | IPv4 | Allow |
| 2 | Allow DHCP | Direction:Inbound Destination Port:67 | IPv4 | Allow |

OK Cancel

3. In the **Name** field, enter a policy name.
4. In the **Description** field, enter a short description for the policy.
5. In **Default Access**, select **Allow** or **Block** if no rule is matched.
6. To assign rules for the policy, click **Create**. The **L3 Access Control** page is displayed.

Refer to [Create an L3 Access Control Policy Rule](#) on page 77 for more information.

NOTE

You can set a priority to the policy by selecting the policy and click **Up** or **Down** to set the desired order.

NOTE

You can edit or delete a policy rule by selecting the options **Configure** or **Delete** respectively.

7. Click **OK** to save the policy.

After the L3 access control policy is created, it can be applied to any WLAN from the Wireless LANs page.

NOTE

You can edit, clone, or delete a policy by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the L3 Access Control page.

Create an L3 Access Control Policy Rule

An L3 Access Control Policy of multiple traffic control rules, which can be enforced in any order you prefer.

To create an L3 access control policy rule:

Firewall Profile

Managing a Firewall Profile

1. From the **L3 Access Control Policy** page, click **Create**. The **L3 Access Control Policy Rule** page is displayed.

FIGURE 41 Creating an L3 Access Control Policy Rule

The screenshot shows a dialog box titled "Create L3 Access Control Policy Rule". The dialog contains several configuration fields: a "Description" text box, an "Access" dropdown menu set to "Allow", a "Protocol" dropdown menu set to "No data available", a "Type" section with radio buttons for "IPv4" (selected) and "IPv6", and sections for "Source IP", "Source Port", "Destination IP", and "Destination Port". Each of these sections has a checkbox labeled "ON" and a "Range" text input field. The "Source IP" and "Destination IP" sections also include "Subnet Network Address" and "Subnet Mask" text input fields. At the bottom, there is a "Direction" dropdown menu set to "Inbound" and two buttons: "OK" and "Cancel".

2. Configure the following:

- **Description:** Type a short description for the access control policy rule.
- **Access:** Select Allow or Block depending on whether you want to set this rule as the default rule.

NOTE

All unicast, multicast and broadcast traffic, except the ACL rules will be allowed or dropped depending on the option selected. Add the appropriate rules.

- **Protocol:** Select the network protocol to which this rule will apply. Supported protocols include TCP, UDP, UDPLITE, ICMP (ICMPv4), ICMPv6, IGMP, ESP, AH, SCTP.
- **Type:** Choose the IP version, IPv4 or IPv6.
- **Source IP:** Enable the option and specify the source **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter **IPv6 Network** address for IPv6 option type.
- **Source Port:** Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
- **Destination IP:** Enable the option and specify the destination **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter **IPv6 Network** address for IPv6 option type.
- **Destination Port:** Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
- **Direction:** Select Inbound, Outbound or Dual indicating the direction of the traffic.

3. Click **OK** to save your changes.

NOTE

Alternatively, in **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall drop-down list which has the L3 access control policy mapped to it.

Creating an L2 Access Control Policy

Creating an L2 Access Control Service

Another method to control access to the network is by defining Layer 2 MAC address access control lists (ACLs), which can then be applied to one or more WLANs or WLAN groups. L2 ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients based on the MAC addresses that are configured. Further, L2 ACLs can also be used to allow-only or deny-only clients based on the ether types of the packet where EtherTypes is a field present in the ethernet header of a packet.

NOTE

If a tagged packet with Tag Protocol Identifier (TPID) value of 0x8100, 0x9100, or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow or block decision against the configured Ether-Types. If the mentioned TPID values need to be treated as Ether-Type to make the allow or block decision, configure the required TPID values in the custom Ether-Type list.

1. Select **Security > Access Control > L2 Access Control**.

2. Click **Create**.
This displays **Create L2 Access Control Service** page.

FIGURE 42 Creating an L2 Access Control Service

Create L2 Access Control Service

General Options

Name:

Description:

Rules

Restriction: Allow only the stations listed below Block only the stations listed below

MAC

MAC

EtherTypes

Restriction: Allow only the EtherTypes listed below Block only the EtherTypes listed below

Standard EtherTypes

Protocol

Protocol

If a tagged packet with TPID(Tag Protocol Identifier) value of 0x8100 or 0x9100 or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow/block decision(s) against configured Standard EtherType(s). If the mentioned TPID value(s) need to be treated as Ether-Type(s) to make allow/block decision(s), please configure the required TPID value(s) in the Use Defined EtherTypes list explicitly.

User Defined EtherTypes

Protocol name EtherType value

Protocol name EtherType value

3. Configure the following options:
 - a. **General Options**
 - **Name:** Enter a name for this policy.
 - **Description:** Enter a short description for this policy.
 - b. **Rules**
 - **Restriction:** Select the default action that the controller will take if no rules are matched. Available options include **Allow only the stations listed below** or **Block only the stations listed below**.
 - **MAC Address:** Enter the MAC address to which this L2 access policy applies and click **Add** or click **Import CSV** to import the MAC address.
 - c. **EtherTypes**
 - **Restriction:** The EtherType in the L2 ACL profile allows or blocks the specified EtherType traffic from the clients toward the network. Available options include **Allow only the EtherTypes listed below** or **Block only the EtherTypes listed below**.
 - **Standard Ether Types:** Select a protocol from the **Protocol** list to which this L2 access policy applies and click **Add**.
 - **User Defined Ether Types:** Enter a protocol name and EtherType value in hexadecimal format and click **Add**. A maximum of ten custom EtherTypes can be configured to be allowed or blocked.
4. Click **OK**.

NOTE

Alternatively, in the **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall list which has the L2 access control policy mapped to it.

NOTE

You can also edit, clone, or delete a policy by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **L2 Access Control** page.

Configuring Application Controls

Using the **Application Control** screen, you can identify, control, and monitor applications that are running on wireless and wired clients associated with managed APs, and you can also apply filtering policies to prevent users from accessing certain applications.

Additionally, you can create your own user-defined applications, import an updated application signature package, and configure rate limiting and QoS traffic shaping policies based on system-defined or user-defined applications.

AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as Application Recognition Control (ARC) and URL Filtering. ARC will work on the destination AP based on its app-id.

Viewing an Application Control Summary

You can view an application-specific or port-specific summary in a chart or table format.

Complete the following steps to view the application control summary.

1. From the main menu, go to **Security > Application Control > Summary**.
The Summary page is displayed.

Firewall Profile

Managing a Firewall Profile

- The **Summary** page can be viewed with following options:
 - Top Applications by: Choose Application or Port from the menu.
 - Click to view by Chart or Table.
 - Count:** Select **10** or **25**.
 - Total, 2.4 GHz, 5GHz, 6(5)GHz.
 - Duration:** Select **Last 1 hour** or **Last 24 hours**.
 - APs: Select a specific AP or **All APs**.
 - All Clients: Select All Clients, Wired or Wireless clients.

Creating an Application Control Policy

An application control policy is created to limit and classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy.

- From the main menu, go to **Security > Application Control > Application Policy**.
The **Application Policy** page is displayed.
- Click **Create**.
The **Create Application Policy** dialog box is displayed.

FIGURE 43 Creating an Application Policy

Create Application Policy

Note: Please ensure that configuration is consistent with URL filtering policy. The URL filtering policy will take precedence.

General Options

Name:

Description:

Rules

+ Create Configure Delete

| # | Rule Type | Content |
|---|-----------|---------|
| | | |

Logging

Send App Logs to SZ: OFF Allow the AP to log every application event and send the events to SmartZone

OK Cancel

- Under **General Options**, enter the policy name and description.

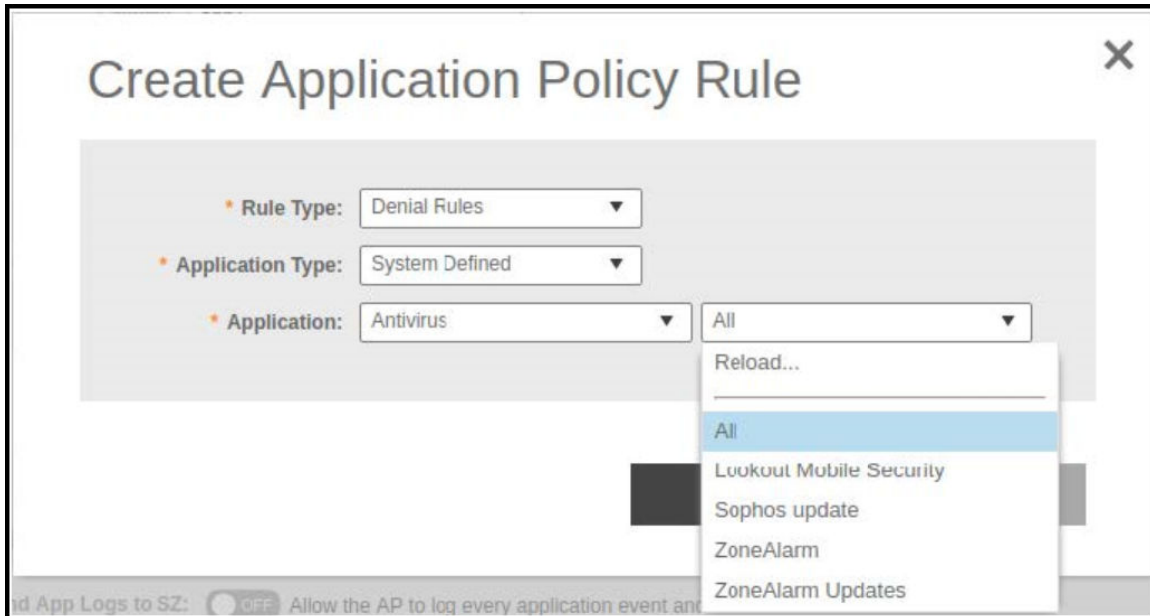
- Under **Rules**, click **Create** to create a new rule.

NOTE

Each application policy can contain up to 128 rules.

The **Create Application Policy Rule** dialog box is displayed.

FIGURE 44 Creating an Application Policy Rule



- From the **Rule Type** list, select one of the following options:
 - **Denial Rules**
 - **QoS**
 - **Rate Limiting**
- From the **Application Type** list, select an application type.
- From the **Application** field, select the application for which you want to create a policy rule.

For example, if you select **All** in the Anitvirus application category and save the application rule, the application rule list reflects all antivirus applications and is selected as a single entry in the rule list. A full category is counted as one rule in the allotment of 128 Layer 7 rules in a Layer 7 policy.

- Click **OK** to save the rule.

NOTE

If a rule is already created, you can edit its configuration settings by selecting the rule and clicking **Configure** in the **Create Application Policy** dialog box.

- Under **Logging**, select the appropriate option for the APs to log events:
 - **Allow the AP to log every application event and send the events to SmartZone**
 - **Allow the AP to log every application event and send the events to external syslog**
- Click **OK** to save the application control policy.

You can continue to apply the application control policy to user traffic.

Firewall Profile

Managing a Firewall Profile

Implementing an Application Control Policy

Deploying an application control policy involves configuring a Firewall Profile with the policy, and then applying that profile to a WLAN.

To implement an Application Control Policy:

1. Go to **Security > Application Control > Application Policy**.

Refer to [Creating an Application Control Policy](#) on page 82 for more information.

NOTE

For SmartZone 5.2.1 or earlier releases, go to **Firewall > Application Control**.

2. Go to **Wireless LANs**.
3. Locate the WLAN for which you want to apply the application policy, and select it from the list.
4. Click **Configure**. The **Edit WLAN [WLAN Name]** page appears.
5. Under **Firewall Options**, select the **Enable WLAN specific** option.
6. From **Application Control**, select an application control policy you created from the drop-down list. Alternatively, click **Create** to create a new application control policy.

7. Click **OK** to save your WLAN changes.

FIGURE 45 Select an Application Policy to apply to the Firewall Profile

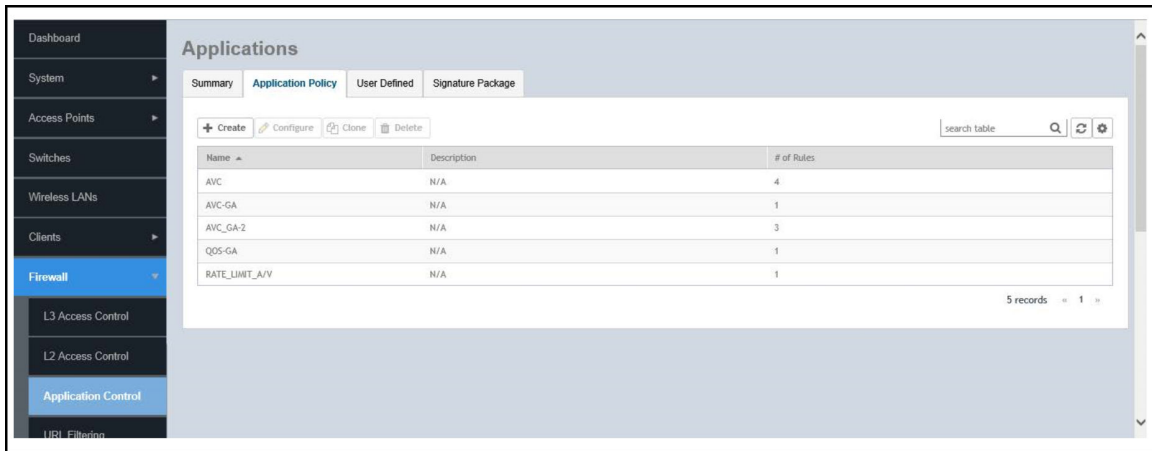
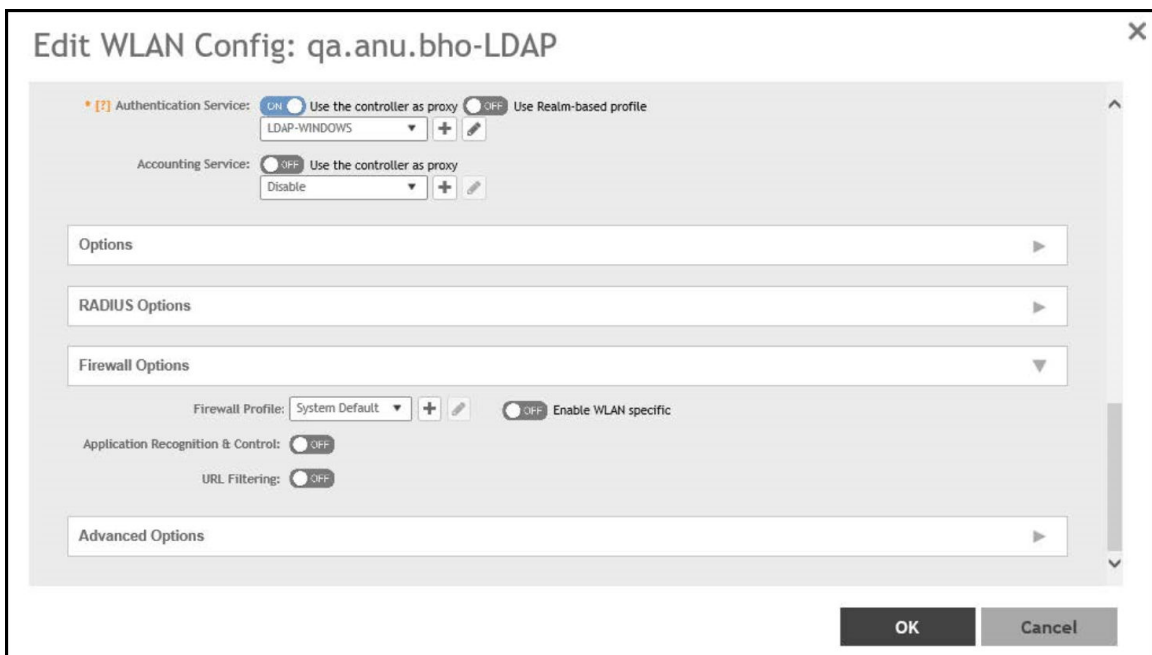


FIGURE 46 Apply the Application Control Policy to a WLAN



Creating a User-Defined Application

When an application is unrecognized and generically (or incorrectly) categorized, the controller is unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address or mask, port, and protocol.

Complete the following steps to configure a user-defined application.

1. From the main menu, go to **Security > Application Control > User Defined Applications**.

Firewall Profile

Managing a Firewall Profile

2. Click **Create**.

The **Create User Defined Application** dialog box is displayed.

3. Configure the following options:

- **Name:** Enter a name for the application. This name that will identify this application on the dashboard.
- **Type:** Select **Default** or **Port Mapping**.
- **IP Mode:** Select **IPv4** or **IPv6** address.
- **Destination IP/Netmask:** Enter the destination IP address of the application and the netmask of the destination IP address.
- **Destination Port:** Enter the destination port for the application.
- **Protocol:** Select the protocol used by the application. Options include **TCP** and **UDP**.

4. Click **OK**.

NOTE

You can also edit, clone, and delete the user-defined application by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **User Defined** tab.

Working with Application Signature Packages

RUCKUS periodically releases and makes new application signature packages available for download.

The controller web user interface displays a notification on the **Dashboard**, when the latest signature application package is available for download.

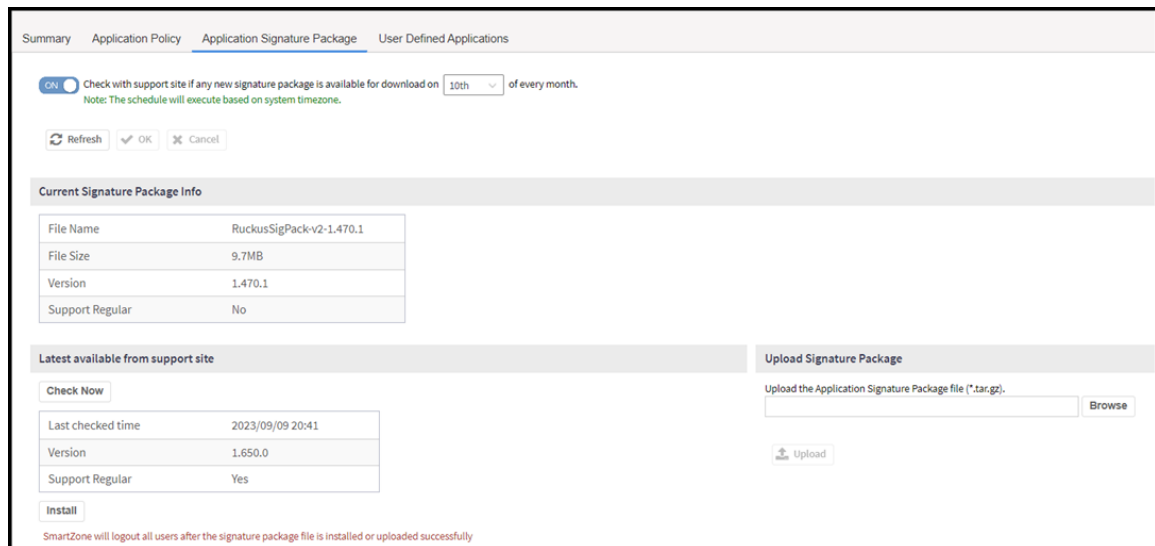
Alternatively, application signature package updates or downloads can be scheduled from the RUCKUS download center.

Complete the following steps to check for application signature package updates.

1. From the main menu, go to **Security > Application Control > Application Signature Package**.

The **Application Signature Package** tab is displayed.

FIGURE 47 Checking the Application Signature Package



2. Switch **ON** the **Check with support site if any new signature package is available for download** option and select the date of the month from the date list to schedule updates every month. A periodic check for the latest available signature package is triggered at a random date.

NOTE

The schedule will run based on the system time zone.

Under **Current Signature Package Info**, the file name, file size, version, and type of signature package are displayed.

3. Under the **Latest available from support site**, click **Check Now** to check for any latest update.
4. Click **Install** to install the latest signature package.

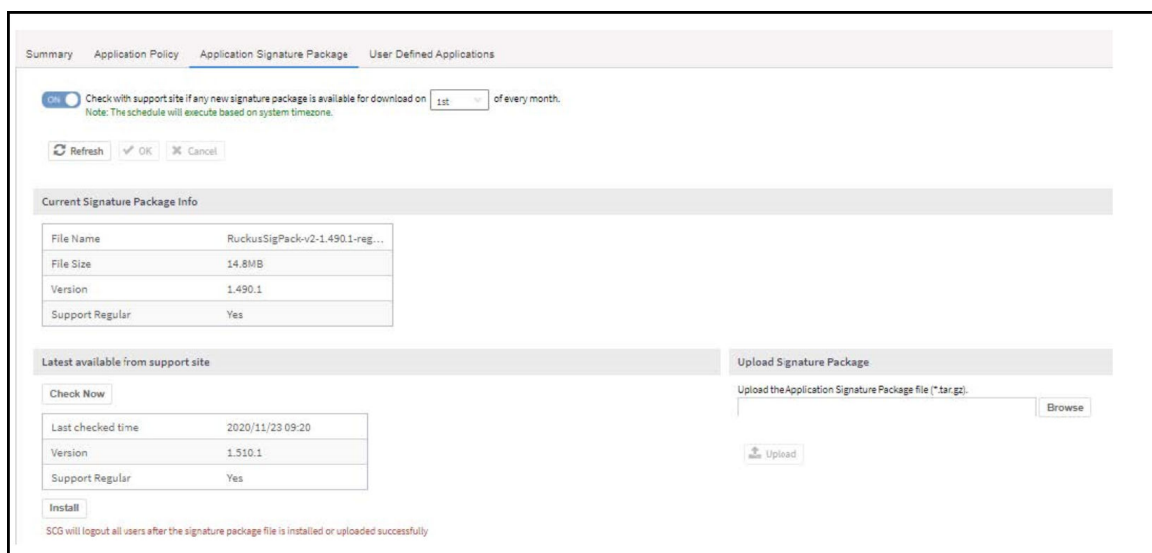
After the signature package file is installed or uploaded successfully, controller logs out all users.

Step 1: Uploading the Signature Package

Once you have downloaded a new signature package, you can import it into SmartZone using the following procedure:

1. Select **Security > Application Control > Application Signature Package**.

FIGURE 48 Viewing and Uploading Signature Package File Information



The **Current Signature Package Info** section displays the information about the file name, file size, version and type of the signature package. For information on the latest signature package, refer to *RUCKUS SmartZone Upgrade Guide*.

2. Select the tab.
3. Under **Upload Signature Package**, click **Browse** to select the signature package file.
4. Click **Upload** to upload the signature package file.

Once the import is complete, the list of system-defined applications is updated immediately.

Firewall Profile

Managing a Firewall Profile

Step 2: Validating the Signature Package

The application updates the latest signature package in all the connected APs. To validate the latest version follow the procedure:

1. In the Access Point, enter the Privileged EXEC mode using CLI.
2. Enter the following CLI command, which displays the latest version of the signature package.

```
get qmdpi-version : get qmdpi-version
                  == get version details of DPI

rkscli: get qmdpi-version
      DPI Signature Version : RuckusSigPack-v2-1.430.1
      DPI Engine Version   : 5.4.0-68.052 (build date Jun  3 2019)
      DPI Bundle Version   : 1.430.0-20 (build date Apr 15 2019)

OK
```

Managing Signature Package Upgrading Conflicts

Upgrading a Signature package from lower version to a higher version fails when an Access Control Policy and an Application Control Policy already exists and the Application Signature in the AVC Policy of lower version conflicts with the one in higher version. In such a case, SZ displays an error message. Perform the following procedure to avoid this error.

To overcome Signature Package upgrade conflicts:

Step 1: Delete the L3 Access Control Policy:

1. Go to **Security > Access Control > L3 Access Control**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > L3 Access Control**

2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the profile and click **Delete**.

Step 2: Delete the Application Control Policy:

1. Go to **Security > Application Control > Application Policy**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > Application Control > Application Policy**

2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the policy and click **Delete**.

Step 3: Upgrade the Signature Package

1. Go to **Security > Application Control > Application Signature Package**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > Application Control > Signature Package**

2. Click **Browse**, and choose the Signature Package file.

3. Click **Upload**.

After the Signature Package is successfully applied the package file name, file size and the version will be visible in the UI.

Step 4: Create a new L3 Access Control Policy with the details of the policy deleted.

Step 5: Create a new Application Control Policy with the details of the policy deleted.

URL Filtering

Administrators can use the URL filtering feature to block access to inappropriate websites. The Web pages available on the internet are classified into different categories, and those identified to be blocked can be configured based on available categories. Administrators can also create policies based on these categories, to allow or deny user access.

After categorizing websites accessed by the clients connected to the AP, a third-party cloud-hosted URL categorization service is used to categorize the live web traffic generated from the client devices. By default, traffic which is not categorized is allowed. The packets from the client device are dropped only after the URL is successfully categorized, and DENY is configured for the client in the policy.

The AP periodically generates statistics such as the Top 10 Denied URLs/categories, Top 10 URLs/categories by traffic and sends them to controller which collects this information and maintains it based on the filters applied per zone and WLAN.

URLs are typically classified by third-party applications to enhance internet security and usage. To categorize the web page or URL, the network packets must be analyzed. In HTTP packets, the complete URL value is extracted and in HTTPS packets, the domain name of the URL is extracted for URL web page categorization. The AP remembers the signature of the packet it forwards and when the packet is identified as HTTP or HTTPS, it receives the domain name/URL from the packet and sends it to the third-party URL categorization engine to verify the Web category. If the retrieved category is blocked as per the configured policy, packets with the same signature are blocked. Blocked HTTP browser traffic redirects the user to a web page that provides information on why the access to the website was denied. This feature is not applicable to HTTPS traffic and mobile application traffic.

The AP maintains a cache of up to 98304 URL entries and attempts to find the URL category from the local cache. It contacts the third-party URL categorization server only when the URL is not available in the local cache.

AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as Application Recognition Control (ARC) and URL Filtering. URL-filtering, based on category and threat level (web reputation) will work on the destination AP depending on the URL domain.

Viewing a Summary of URL Filters

The **Summary** page provides administrators with a view to analyze URL traffic based on the user activity over the network.

You can view the top ten URLs by:

- Traffic - displays all URLs accessed (including blocked URLs) the most
- Categories Traffic - displays all categories accessed (including blocked categories) the most
- Clients Traffic - displays all clients accessed (including blocked clients) the most
- Blocked URLs - displays the URLs that have been denied access the most
- Blocked Categorize - displays the URL categories that have been denied the most
- Blocked Clients - displays the clients that have been denied access the most

Firewall Profile

Managing a Firewall Profile

Enabling URL Filtering on the WLAN

Administrators can create URL filtering policies and reuse them across WLAN controllers. You can define the policy based on the web page categorization, whitelist, blacklist, and web search.

Policies can also be created based on the role assigned to the user. Users can be allowed or denied access to a particular URL based on the role assigned, and the SSID login details for that role.

Complete the following steps to create a URL filtering policy.

1. From the main menu go to **Security > Access Control > URL Filtering > Profiles**.

2. Select the **Profiles** tab, and then click **Create**.
The **Create URL Filtering Policy** page is displayed.

FIGURE 49 Creating URL Filtering Policy

The screenshot shows the 'Create URL Filtering Policy' configuration page. At the top, there is a note: 'Note: Please ensure that configuration is consistent with Application policy. The URL filtering policy will take precedence.' Below this, the 'General Options' section has a dropdown menu and two input fields for 'Name' and 'Description'. The 'Block by Category' section has a dropdown menu. The 'Block by Threat: Level' section has a dropdown menu and a slider control. The slider is currently set to 'High Risk' and is labeled 'ON Enabled'. Below the slider, it says 'Select the threat level to block the URLs and IP'. The slider has five positions: High Risk, Suspicious, Moderate Risk, Low Risk, and Trustworthy. The 'Blacklist & Whitelist' section has two input fields for 'Domain Name' with '+ Add', 'x Cancel', and 'Delete' buttons. The 'Safe Search' section has three sections: 'Google Safe Searches' (ON), 'YouTube Safe Searches' (ON), and 'Bing Safe Searches' (ON). Each section has a radio button for 'Virtual IP' and a corresponding IP address field.

Configure the following options:

- **General Options**
 - Name:** Enter the name of the policy you want to create.
 - Description:** Enter a brief description to identify the policy.
- **Blocked Categories:** Select one of the categories to block. Selecting the **Custom** option allows the administrator to customize the list of categories to block for the user. You can also use **Select All** to choose all of the categories listed, or **None** to set no filters for the user to access (the user can access any URL in this case because no web page is blocked).

Firewall Profile

Managing a Firewall Profile

- **Block by Threat Level:** Enable this option and set the slider bar to a threat level. The web reputation score, from 1 through 100, gives the reputation index or threat level of a URL being browsed by a user. The reputation score can be used to categorize the threat level of URLs according to the following levels:
 - **Trustworthy:** The web reputation score is in the range of 81 through 100. These are well known sites with strong security characteristics.
 - **Low-Risk:** The web reputation score is in the range of 61 through 80. These are generally benign sites and rarely exhibit the characteristics that expose the user to security risks.
 - **Moderate-Risk:** The web reputation score is in the range of 41 through 60. These are benign sites but have exhibited some characteristics that suggest a security risk.
 - **Suspicious:** The web reputation score is in the range of 21 through 40. These are suspicious sites.
 - **High-Risk:** The web reputation score is in the range of 1 through 20. These are high risk sites.

- **Blacklist & Whitelist:** If web content categorization is unable to classify URLs that the user, organization or institution needs, then Whitelist and Blacklist profiles can be created by the administrator. The URLs listed by the administrator under Blacklist are blocked and those listed under Whitelist are allowed access. The domain names under Blacklist and Whitelist take precedence over the default allow or deny action of the URL filter.

The AP matches the URL pattern against all the configured Whitelist and Blacklist profiles through the Extended Global Regular Expressions Print (egrep) program which performs a line-by-line scan of the file and returns lines that contain a pattern matching the given expression. Currently, the exact URL name or a wildcard at the beginning of the URL is used to match the pattern. From R5.2 onwards, the wildcard (*) character is supported in middle and on either start or end, for example, "*.ruckus*.com", [www.ruckus*.co*](http://www.ruckus.co)). This only allows a maximum of two wildcards (*).

Administrators can also add specific IP addresses or wildcard domain names under Whitelist and Blacklist.

In **Domain Name:** Enter the domain name of the web page which you want to deny user access to in the **Blacklist** tab, and enter the domain name of the web page to which you want to provide user access on the **Whitelist** tab. You can define up to 16 domains.

Click **Add**. The domain name or web page is listed in the corresponding tab.

Click **Cancel** to remove the domain name you have entered in the field.

If you want to delete the domain name from the **Blacklist** or **Whitelist** tab, select the URL and click **Delete**.

- **Safe Search:** Administrators can configure the policy to include a safe search option when users access Google, YouTube, or Bing to search on the internet. Select the respective enable option for Google, YouTube, and Bing. Enabling the option will mandate all users using the policy on the network to use safe search on Google, YouTube, and Bing. By default, FQDN-based safe search is enabled. This option provides a secure connection through HTTPS while allowing access to the internet. To use virtual IP (IPv4 and IPv6) address, select the **Virtual IP** option and enter the IP address. If safe search is enabled before upgrading to release 6.1, the old configuration or virtual IP-based safe search will be retained.

3. Click **OK**.

The **URL Filtering Policy** form is submitted with the specified configuration settings.

You have created the URL filtering policy. The newly created policy is displayed on the **Profiles** page.

If you click the policy, the following information is displayed:

- Name
- Managed By
- Description
- Filtering Level
- # of Blocked Categorize
- # of Blacklist

- # of Whitelist
- Threat Level

Click **Configure** to edit the policy. Click **Clone** to create a duplicate of the policy, or to make modifications to the existing settings of the clone.

Click **Delete** to delete the policy from the URL Filtering Profile.

Enabling URL Filtering on the Controller

You can enable the URL filtering feature on the WLAN controller to block or allow access to specific web sites or web pages.

By configuring the controller, administrator can create a wireless network SSID and allow or deny access to a category of websites for all users that join this SSID.

Follow these steps to enable URL filtering on the controller for an available WLAN.

1. From the main menu go to **Network > Wireless LANs** to select a domain or zone.
2. Choose a WLAN from the system tree hierarchy to **Enable URL Filtering** option.

This displays **Edit WLAN Config** page.

NOTE

To enable URL Filtering for a new WLAN, follow the steps to create a new WLAN.

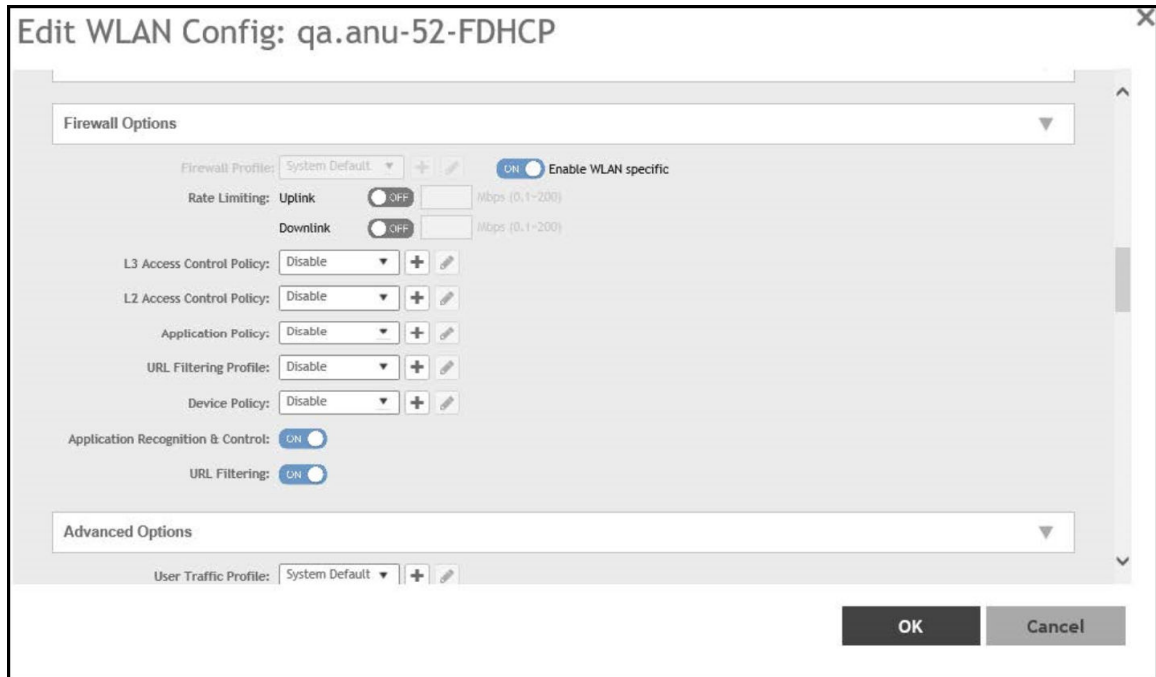
Firewall Profile

Managing a Firewall Profile

3. Scroll down to **Firewall Options**, click **URL Filtering Policy** option.

The **URL Filtering Profile** field appears. Select a URL filtering profile from the drop-down menu. To create a new URL filtering policy, refer [Enabling URL Filtering on the WLAN](#) on page 90.

FIGURE 50 Enabling URL Filtering



NOTE

Application rules are applied based on the following priority:

- a. User defined Access Control Profile
- b. URL Filtering
- c. Application Control Policy

User defined rules take precedence over URL filtering.

You have enabled URL filtering on the controller.

Managing URL Filtering Licenses

URL Filtering license for the selected partners-to use the content database is issued for a duration of one year for an AP. Dashboard warnings are issued thirty days before the end of the license term.

You can add licenses over time. For example, you can purchase 100 one-year licenses on January 1st and add another 200 one-year licenses in May. The controller receives a new expiry date for the combined license count of 300 APs.

To view license details such as start date, end date, and capacity, go to **Administration > Administration > Licenses > Installed Licenses**, for For SmartZone 5.2.1 or earlier releases, go to **Administration > Licenses > Installed Licenses** tab.

For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *Managing Licenses*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated which indicates that the URL filtering server is unreachable. For more information, refer *Managing Events and Alarms*.

NOTE

A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.

Copyright (c) 2005, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

ATTENTION

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

URL filtering feature is supported only on APs that have a minimum of 256MB RAM.

NOTE

The R730 AP is supported only in SZ6.1.0 firmware zone.

TABLE 7 List of APs with 256MB or more

| | | | |
|-----------------|------------|--------------|-------|
| E510 | T811-CM | T310c/d/n/s | H320 |
| R720 | T610/T610s | C110 | R610 |
| R500e | H510 | T710 / T710s | R510 |
| R310 | T504 | R710 | R600 |
| T300 | T301n | T301s | T300e |
| FZM300 & FZP300 | R500 | R700 | R730 |
| R750 | R650 | R550 | R850 |
| H550 | T750 | T750SE | |

Creating a Device Policy

You can control how devices installed with certain OS configurations can be connected to the network, and also control what they can be allowed to do within the network. Using the device policy service, the system can identify the type of client attempting to connect, and perform control actions such as allowing or blocking access, rate limiting, and VLAN tagging based on the OS rule.

To create a device policy:

1. Click **Security > Access Control** and select **Device Policy**.

This displays **Summary** and **Profiles** options.

Firewall Profile

Managing a Firewall Profile

2. Select **Profiles** tab.

This displays **Device Policy Service** page.

NOTE

The Summary tab displays the device policy services in chart and graph format. Profiles can be filtered based on frequency, duration, APs and zone.

FIGURE 51 Create Device Policy Service

The screenshot shows a web interface for creating a device policy service. It includes a 'General Options' section with a 'Name' field, a 'Description' field, and a 'Default Access' section with radio buttons for 'Allow' and 'Block'. Below this is a 'Rules' section with a table for defining rules. The table has columns for Description, Device Type, OS Vendor, Access, Uplink Rate Limit, Downlink Rate Limit, and VLAN. At the bottom are 'OK' and 'Cancel' buttons.

3. Enter the policy service details in the **General Options** section:
 - a. **Name:** Enter a name for the device policy.
 - b. **Description:** Enter a short description for this device policy.
 - c. **Default Access:** Select either Allow or Block. This is the default action that the system will take if no rules are matched.
 - d. Under **Rules** section, define the device policy rules. For more information, refer [Creating the Device Policy Rules](#) on page 97.
 - e. Click **OK**.

NOTE

You can also edit, clone, and delete a service by selecting the options Configure, Clone, and Delete respectively, from the Device Policy tab.

Enabling Device Policy Service

Enable device policy service. To enable the new device policy perform the following steps:

1. Click **Network** tab on the main menu.
2. Select **Wireless LANs**.
3. Select **Create/Configure** tab.
4. Scroll down to **Firewall Options** to enable the firewall profile.

Creating the Device Policy Rules

Complete the following steps to create a device policy rule.

1. From the main menu, go to **Security > Access Control > Device Policy**.
The **Summary** and **Profiles** tabs are displayed on page.
2. Click the **Profiles** tab.
3. Click **Create** to open the **Create Device Policy Service** page.
4. In the **Rules** section, click **Create**.
The **Create Device Policy Rule** page is displayed.

FIGURE 52 Creating a Device Policy Rule

The screenshot shows the 'Create Device Policy Rule' configuration interface. The form contains the following fields and options:

- Description:** Gaming Type Rule
- Action:** Allow
- Device Type:** Gaming
- OS Vendor:** All (with a dropdown menu open showing: All, Gamecube, Wii, Xbox, Nintendo, Playstation)
- Rate Limiting:** Two sections, each with a toggle set to OFF and a text input field for Mbps (0.1~200).
- VLAN:** An empty text input field.

At the bottom of the form are two buttons: **OK** and **Cancel**.

The graph has 3 zones -

- Outer zone - Displays the model names of device types.
- Central zone - Displays information of the operating system used by the device type or the vendor name.
- Inner Zone - Displays the device type.
- Core - Displays the number of clients connected. (Hover the mouse to view the information).

The below table lists the filters available in the **Summary** screen.

TABLE 8 Filters

| Filter Name | Description |
|---------------------------------------|--|
| Total/2.4GHz/5GHz | User can select the radio options from the drop down menu to generate the report. |
| Last report/Last 1 hour/Last 24 hours | User can select the options from the drop down menu generate the report. Last report - Accumlates stats of 180 seconds from the Access Point. Last 1 hour - Accumlates stats of 60 minutes from the Access Point. Last 24 hours - Accumlates stats of 24 hours from the Access Point. |
| All APs | By default displays details of the Access Point selected from Access Points tab. User can select the option from drop down menu to view a particular AP or all APs. |
| All WLANs | Displays the WLANs associated with each AP. User can select the option from drop down menu to view a particular WLAN or all WLANs. |
| Settings - Clients | User can set the preferred display settings. NOTE The maximum clients displayed is 20. |
| Host name - Bytes | This displays traffic consumed per client. |

TACACS+

- [About TACACS+ Support.....](#) 101

About TACACS+ Support

Terminal Access Controller Access-Control System Plus (TACACS+) is one of the Authentication, Authorization and Accounting protocols used to authenticate controller administrators. TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery.

In addition to selecting TACACS+ as the server type, complete the following steps for TACACS+ based authentication to work on the controller.

1. Edit the TACACS+ configuration file (**tac_plus.conf**) on the TACACS+ server to include the service user name.

For example,

```
key = test@1234
accounting file = /var/log/tac_acct.log
user = username {
    member = show
    login = cleartext "password1234!"
}
group = show {
    service = super-login {
        user-name = super <<==mapped to the user account in the controller
    }
}
```

2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 14.

3. Select **Administration > Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 11.

4. When adding a server type for administrators, select TACACS+ as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 19.

5. Test the TACACS+ server using the account **username@super-login**.

ECDSA

- Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support..... 103
- Cloud Computing Compliance Criteria Catalogue - BSI C5..... 103
- Configuring ECDSA and Keys at Zone Level..... 103
- Mapping Server ECDSA Certificates..... 105
- Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)..... 108

Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support

The ECDSA is a digital signature algorithm which uses keys derived from elliptic curve cryptography.

The SmartZone provides an option to disable/enable the ECDSA certification on a per-zone basis. The APs in the zone with ECDSA certificate enabled receives an additional controller-signed certificate from the SmartZone. The 2K MIC (Manufacturer Installed Certificates) on the APs is still used as the trust anchor for the SmartZone. The 2K MIC and corresponding key (2k length) remains untouched, backward compatibility of the zone only allows 2K certificate/key.

The SmartZone managed APs issue ECDSA signed certificates which are valid only among the same SmartZone cluster nodes.

The ECDSA is faster than RSA in key generation and signing operations. Signature algorithms are used in TLS handshake and SSH authentication.

Cloud Computing Compliance Criteria Catalogue - BSI C5

The C5 catalogue specifies minimum requirements for secure cloud computing.

By adhering the BSI C5 requirements and guidelines, RUCKUS AP provides a secure, reliable, and trustworthy communication environment.

The following are the secure features in AP and SmartZone:

- Uses a stronger certificate and key in both client and server authentication.
- Removes weak ciphers and algorithms.
- Replaces DropbearSSH to OpenSSH on AP.

Configuring ECDSA and Keys at Zone Level

To configure ECDSA certificates, enable the **SSH/TLS Key Enhance Mode**.

By default, the **SSH/TLS Key Enhance Mode** is disabled.

This configuration is available only with new installation and upgraded versions of the Access Points. The ECDSA certificates are available only after enabling the **SSH/TLS Key Enhance Mode**. To generate and share the ECDSA certificates, AP should join and be a part of this zone.

To enable **SSH/TLS Key Enhance Mode** at the zone level, perform the following:

1. Click **Network > Wireless > Access Points**

This displays the **Access Points** page.

2. In the system tree, click **Create Domain/Zone/Group (+)** icon.
This displays the **Create Zone** page.
3. In the **Create Zone** page, navigate to **General Options** section and enable the **SSH/TLS Key Enhance Mode**.

FIGURE 54 SSH/TLS Key Enhance Mode

The screenshot shows the 'Create Zone' configuration interface. The 'General Options' section is active, displaying the following settings:

- Name:** [Text Input]
- Description:** [Text Input]
- Type:** Domain Zone
- Parent Group:** System
- Link Switch Group:** OFF
- AP Firmware:** 6.1.2.0.895
- Country Code:** United States
- Location:** [Text Input] (example: Ruckus HQ)
- Location Additional Information:** [Text Input] (example: 350 W Java Dr, Sunnyvale, CA, USA)
- GPS Coordinates:**
 - Latitude:** [Text Input]
 - Longitude:** [Text Input] (example: 37.411272, -122.019616)
 - Altitude:** [Text Input] meters
- AP Admin Logon:**
 - Logon ID:** [Text Input]
 - Password:** [Text Input]
- AP Time Zone:** System defined User defined
(GMT+0:00) UTC
- AP IP Mode:** IPv4 only IPv6 only Dual
- Historical Connection Failures:** OFF
- DP Group:** Default DP Group [Add] [Edit]
- Enforce the priority of DP Group:** OFF
This action will disconnect the already established tunnels to vDPs and re-establish to new vDPs as per the priority defined.
- SSH Tunnel Encryption:** AES 128 AES 256
- SSH/TLS Key Enhance Mode:** OFF (circled in red)

The 'Mesh Options' section is partially visible at the bottom. At the bottom right, there are 'OK' and 'Cancel' buttons.

After enabling the **SSH/TLS Key Enhance Mode**, navigate to **Administration > System > Certificates > Certificate Mapping** to map the server's ECDSA certificates.

Mapping Server ECDSA Certificates

After enabling the **SSH/TLS Key Enhance Mode** at the zone level. You can map the ECDSA certificates to SmartZone (server certificate). This mapping ensures that SmartZone (server) is using 2K/3K RSA or ECDSA certificates during the TLS handshake.

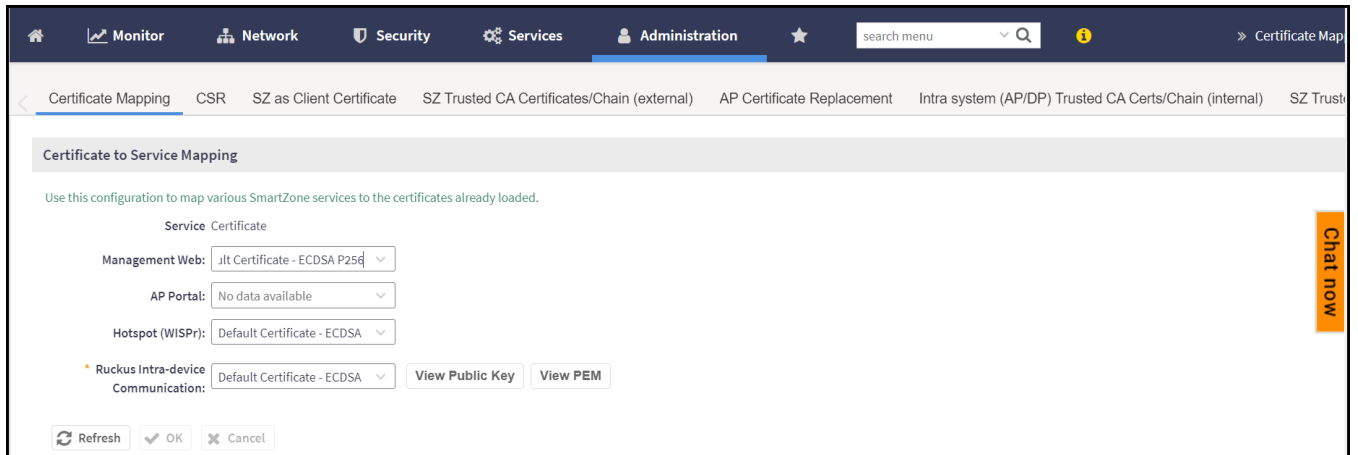
ECDSA Mapping Server ECDSA Certificates

To map the **ECDSA** certificates, perform the following:

1. Click **Administration > System > Certificates > Certificate Mapping**.

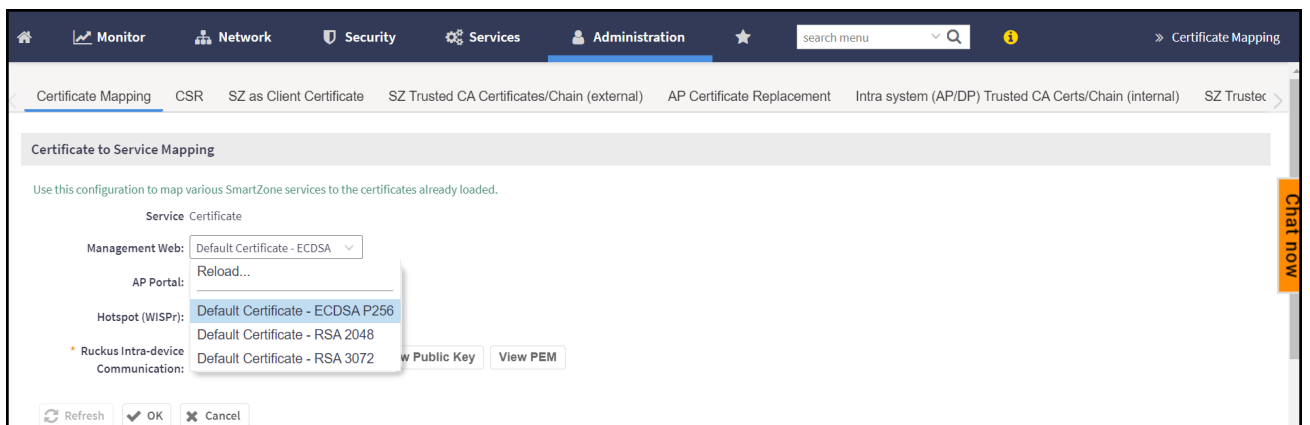
This displays **Certificate Mapping** page.

FIGURE 55 Certificate Mapping



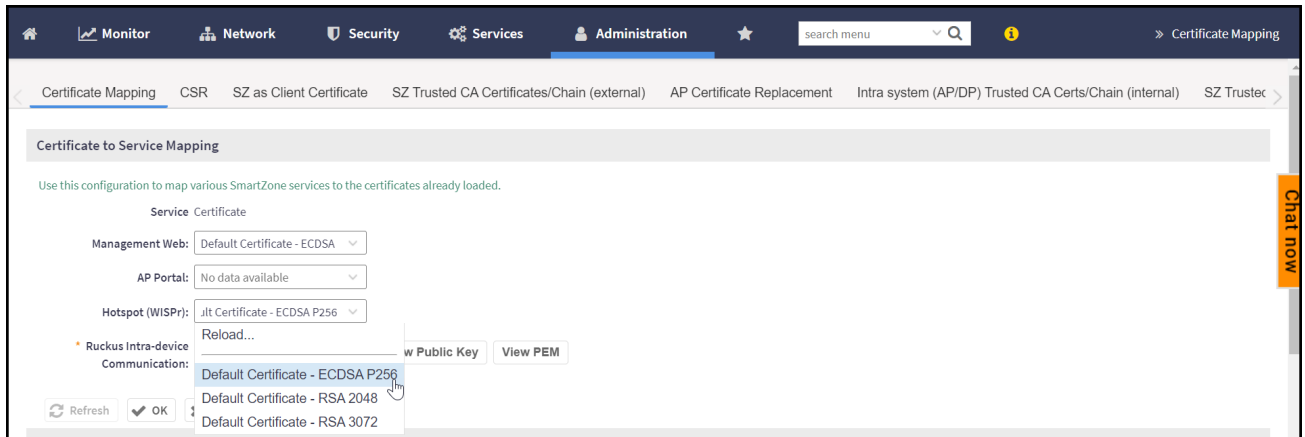
- **Management Web:** SmartZone uses 2K/3K based certificates to map the services when user access SmartZone user interface via web browser.

FIGURE 56 Management Web



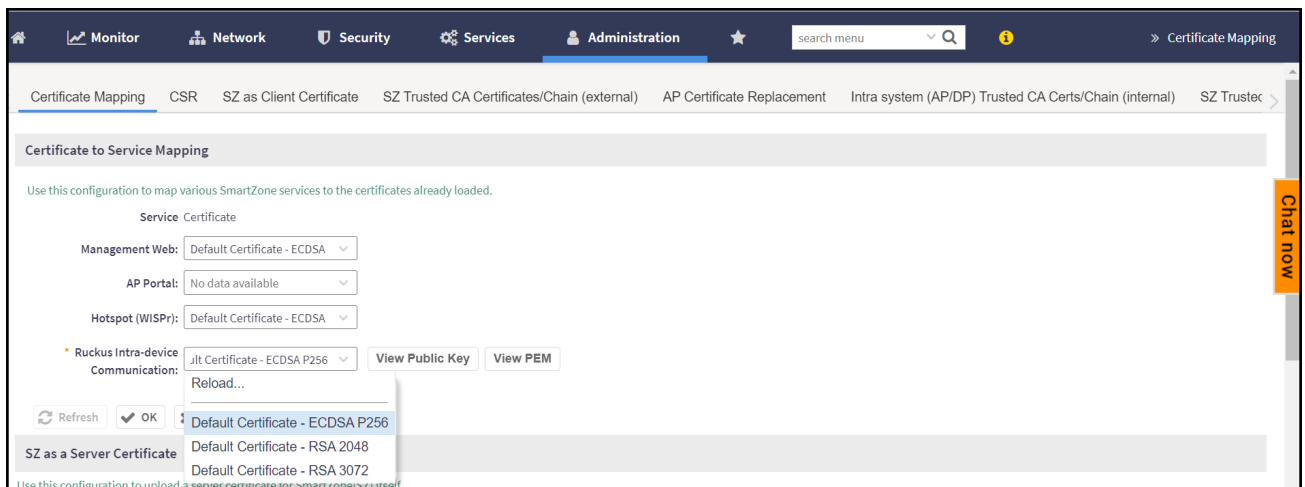
- **Hotspot (WISPr):** SmartZone re-directs the login portal to connected user (via web browser) for authentication.

FIGURE 57 Hotspot (WISPr)



- **Ruckus Intra-device Communications:** SmartZone uses 2K/3K based certificates to map the services when AP/ICX joins the SSH/TLS Key Enhance Mode enabled zone/switch group.

FIGURE 58 Ruckus Intra-device Communication

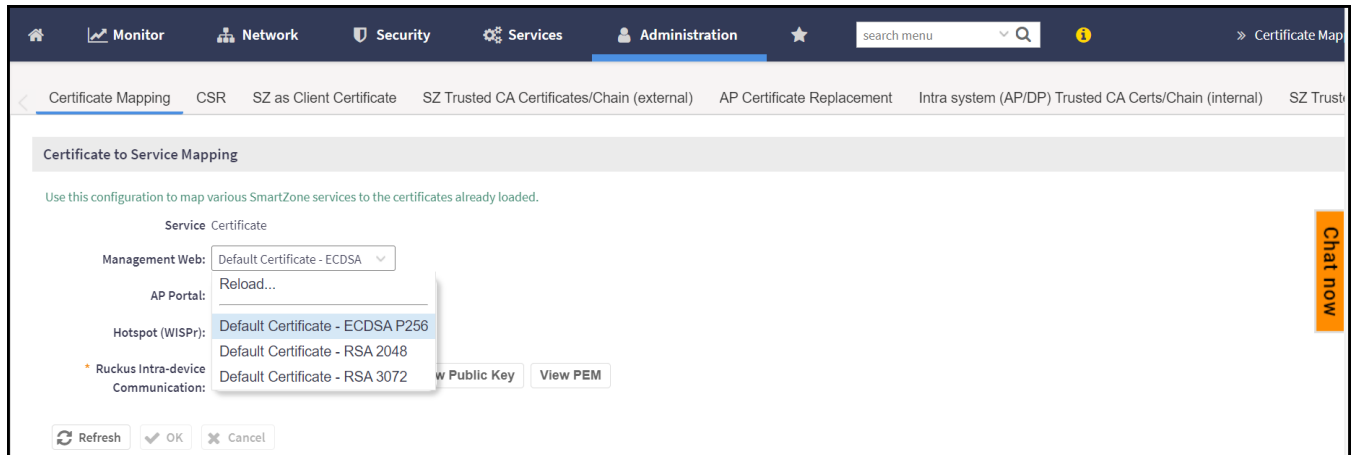


ECDSA

Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)

2. You view the new **ECDSA** certificates in the **Certificate to Service Mapping** section.

FIGURE 59 ECDSA Certificates



3. Click the drop-down menu and select the pre-loaded certificate to map various SmartZone services.
 - **ECDSA P256**: This supports the signing of data with Elliptic Curve methods. The signing and verification is performed using P256 method. The calculation is hash of the message (h), public key (QA) and private key (dA).
 - **RSA 2048**: This is an asymmetric encryption. Each side has a public and private key. The default 2K certificate is renamed as RSA 2048.
 - **RSA 3072**: This is again an asymmetric encryption. RSA can work with keys of different keys of length.
4. Select the certificates and click **OK** and the settings are mapped to various SmartZone services.

Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)

Transport Layer Security (TLS) encrypts communication between a client and server.

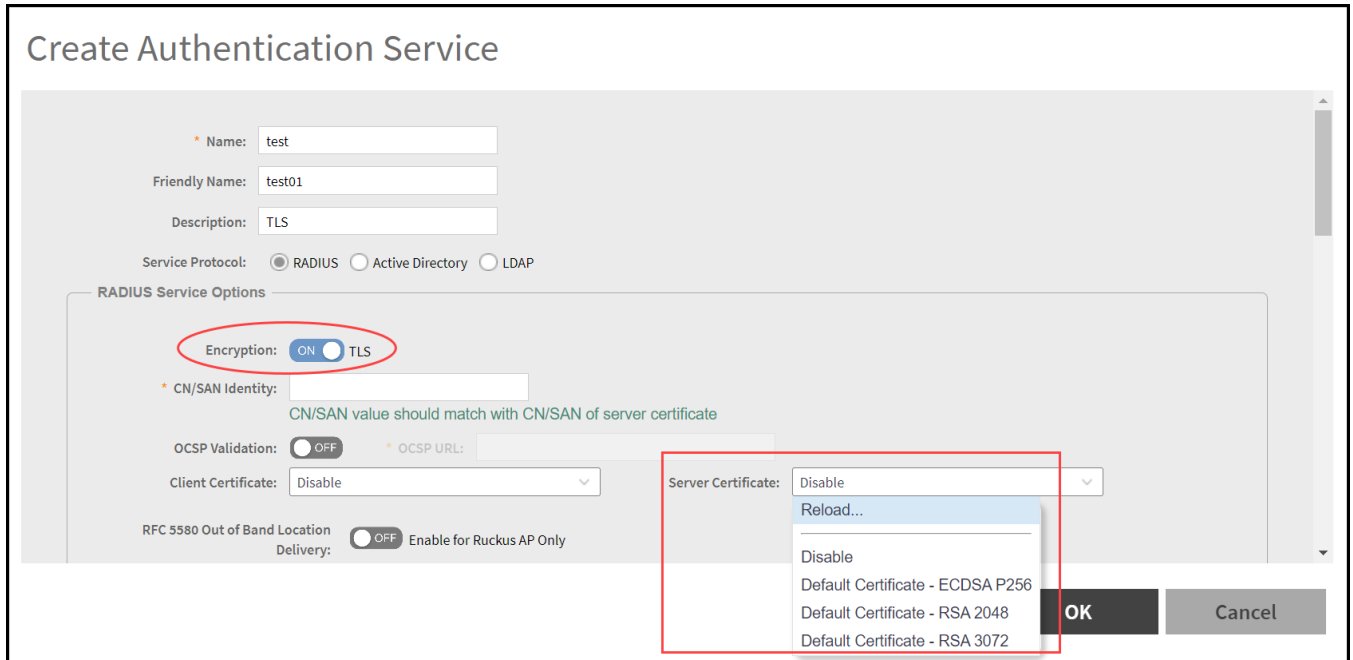
To enable TLS encryption from **Proxy (SZ Authenticator)**, perform the following:

1. Click **Security > Authentication > Proxy (SZ Authenticator)**.
This displays the **Proxy (SZ Authenticator)** page.
2. In the **Proxy (SZ Authenticator)**, click **Create**.
This displays **Create Authentication Service** page.

3. Navigate to **RADIUS Service Options** and enable **Encryption TLS**.

The ECDSA certificates are enabled for RADIUS server.

FIGURE 60 Encryption TLS_Authentication Service



To enable TLS encryption from **Proxy**, perform the following:

1. Click **Security > Accounting > Proxy**.
This displays **Proxy** page.
2. In the **Proxy**, click **Create**.
This displays the **Create Accounting Service** page.
3. Navigate to **RADIUS Service Options** and enable **Encryption TLS**.

The ECDSA certificates are enabled for RADIUS server.

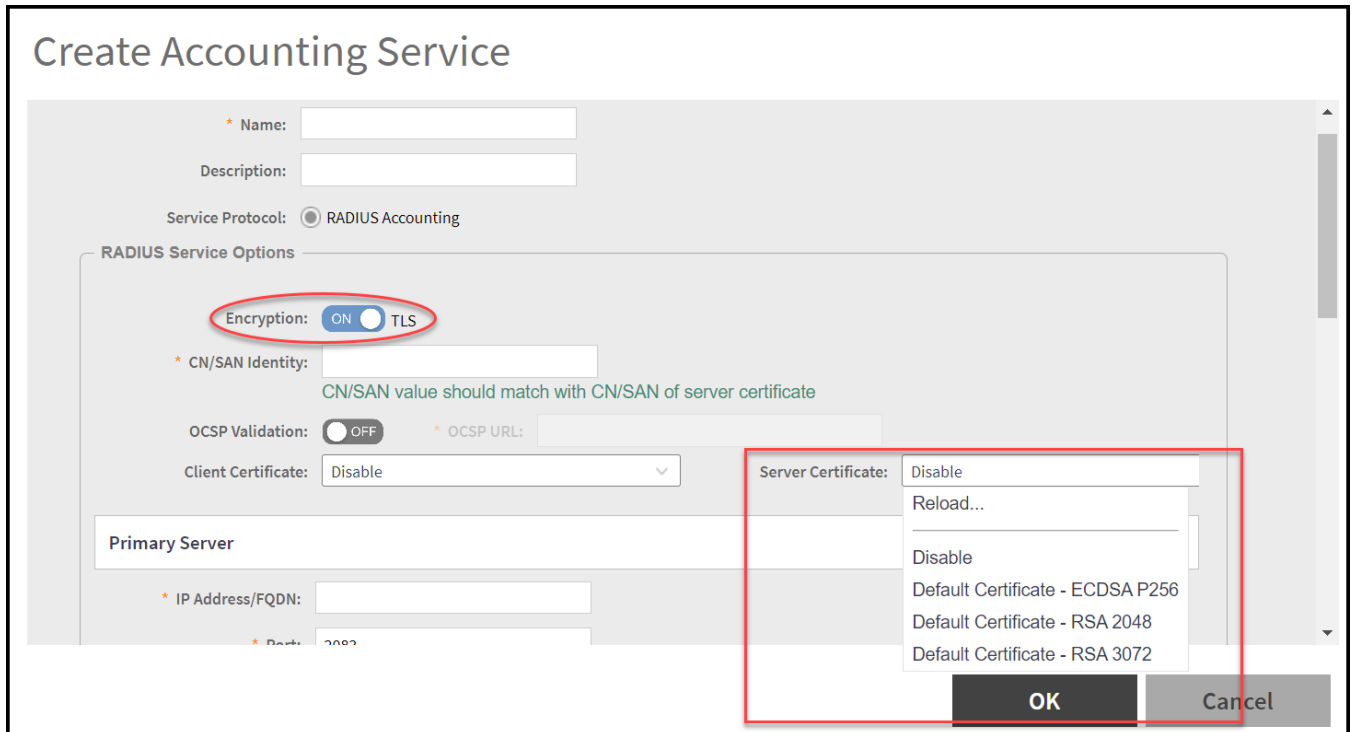
NOTE

The ECDSA certificates is available only for RADIUS service protocol option.

ECDSA

Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)

FIGURE 61 Encryption TLS_Accounting Service





© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>