CONFIGURATION GUIDE



# Cloudpath Enrollment System Multi-Tenant Server Configuration Guide, 5.5

Supporting Cloudpath Software Release 5.5

Part Number: 800-72413-001 Rev A Publication Date: 28 August 2019

# **Copyright, Trademark and Proprietary Rights** Information

© 2019 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

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

Preface	5
Document Conventions	5
Notes, Cautions, and Warnings	5
Command Syntax Conventions	6
Document Feedback	
Ruckus Product Documentation Resources	6
Online Training Resources	7
Contacting Ruckus Customer Services and Support	7
What Support Do I Need?	
Open a Case	
Self-Service Resources	
How to Manage Cloudpath as a Multi-Tenant Server	٥
Multi-Tenant Overview	
VM Specifications	
Root Account	
Tenant Accounts	
Multi-Tenant System Setup Multi-Tenant Activation Code	
Activate Account by Activation Code	
Setting Up the Root Account	
System Setup Wizard	
Select Server Type	
Select System Hostname	
Configure the System WWW Certificate	
Upload the WWW Certificate	
Navigating the Root Account	
Accounts	
Snapshots	
Commands	
Administration - Administrators	
Administration - Company Information	
Administration - System Services	
Administration - System Updates	
Support - Documentation Page	
Support - Licensing	
Support - Diagnostics	
Support - Upload Support File	
Adding Tenant Accounts	
Adding a Tenant Account From the Root Account	
Create Tenant Account	
Tenant Account Admin Password	
Setting Up the Tenant Account	
Tenant Account Setup Wizard	
Tenant Account Login	
Tenant Logs In	
To Do Items	

# Preface

•	Document Conventions	5
	Command Syntax Conventions	
	Document Feedback	
	Ruckus Product Documentation Resources	
	Online Training Resources	
	Contacting Ruckus Customer Services and Support	

# **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	<pre>device(config)# interface ethernet 1/1/6</pre>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
italics	Publication titles	Refer to the Ruckus Small Cell Release Notes for more information.

### Notes, Cautions, and 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
<b>bold</b> text	Identifies command names, keywords, and command options.
<i>italic</i> text	Identifies a variable.
[]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	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, member[member].
١	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.

# **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.ruckuswireless.com.

# **Online Training Resources**

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

# **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.ruckuswireless.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

#### Preface

Contacting Ruckus Customer Services and Support

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- 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.

# How to Manage Cloudpath as a Multi-Tenant Server

•	Multi-Tenant Overview	9
	Multi-Tenant System Setup	
	Setting Up the Root Account	
	System Setup Wizard	
	Navigating the Root Account	
	Adding Tenant Accounts	
	Tenant Account Login	36

# **Multi-Tenant Overview**

Cloudpath supports server configurations in single-tenant and multi-tenant mode. A multi-tenant instance allows you to host multiple customer accounts on your Cloudpath system.

In multi-tenant mode, the server is configured for one root account and up to 128 tenant accounts.

#### NOTE

Each multi-tenant system is provided with 256 RADIUS ports, which equates to one RADIUS authentication port, and one RADIUS accounting port, per tenant account.

### **VM Specifications**

A Cloudpath multi-tenant virtual appliance can be deployed using a VMware ESXI, with an open virtualization archive (OVA) file, or using Microsoft Hyper-V Manager, with a Hyper-V virtual hard disk (vhdx) disk image file.

When deploying a VM for a multi-tenant server, we recommend using 16-18 GB RAM and a 4 vCPUs x 4 Cores configuration to support up to 128 tenant accounts.

### **Root Account**

The root account is the bind account for the entire multi-tenant system. The root account manages the Cloudpath server, can view and manage all tenant accounts and perform system administration tasks, such as upgrades, certificate management, and license information.

### **Tenant Accounts**

Tenant accounts are individual customer accounts hosted and managed by the Cloudpath multi-tenant server. Tenant administrators can only view and manage their own account.

# **Multi-Tenant System Setup**

# **Multi-Tenant Activation Code**

Before setting up a multi-tenant system, you must obtain a multi-tenant activation code from the Cloudpath license server administrator. Request a multi-tenant activation code by emailing cloudpathtrial@ruckuswireless.com, or ask your Ruckus Wireless sales representative to assist with obtaining a multi-tenant activation code.

#### NOTE

If you configure your system for single tenant, it cannot be changed to a multi-tenant system.

# **Activate Account by Activation Code**

A multi-tenant activation code is sent by the Cloudpath license server administrator. Example email with activation code:

An activation code has been generated for an on-premise multi-tenant VM.

Activation Code: CE4E-E533-906A Account: Anna Test BVT Administrator: anna@cloudpath.net

After the VM is deployed, enter the hostname of your system in a browser to access the Cloudpath login page.

#### FIGURE 1 Enter Multi-Tenant Activation Code

CLOUDPATH ENROLLMENT SYSTEM		
	Activate by ac Please provide the activation code Activation Code	
	Luick Start Guide	Activate

Enter your multi-tenant activation code.

# **Setting Up the Root Account**

The initial username and password will be used to bind the root account. You cannot use this account again on the system. No tenant accounts can use the same email and password as the root account.

After the multi-tenant system is activated, you are prompted to set a password for the root account administrator. Use the same email address from the activation code email.

#### FIGURE 2 Create a Password for the Root Account

CLOUDPATH ENROLLMENT SYSTEM	
	Password Setup
	The following credentials will be used to log into this system in the luture.
	anna@cloudpath.net
	Password
	Confirm Password
	Submit

Create a new password for the root account login.

After you enter the multi-tenant activation code, your system is automatically reconfigured as a multitenant system, then restarts.

#### FIGURE 3 Activating a Multi-Tenant System



Reconfiguring the server to be a multi-tenant system takes a few minutes. When complete, enter the administrator email address and new password to finish setting up the system.

#### FIGURE 4 Login After Restart

CLOUDPATH		
	Sign In	
	jeff@arris.com	
Activate Account	Forget Password New to Cloudpath? Sign In	
	Cópyright Xi'y 2015, Ruckus, an ARRIS, company An rights reserved.	

#### NOTE

The credentials entered after a multi-tenant configuration are for the Root Account.

# **System Setup Wizard**

After a successful activation (or login), the system setup wizard takes you through a few steps.

# **Select Server Type**

#### FIGURE 5 System Setup Standard Server

lb at 7	
vhat	Type Of Server Is This?
۲	Standard Server (Default)
	Select this option if this server is your first server or if a cluster will be initialized from this server.
0	Add-On Server For Cluster
	Select this option if this server will be part of a cluster and the cluster will be initialized from a different server. No further configuration will occur on this server until the cluster is established.
0	Replacement Server For Existing Server
	Select this option if this server will import data from an existing server.

In most cases, select **Standard Server**, the default. This selection takes you through a setup wizard, which prompts you for the basic information required for a Cloudpath server.

If you are setting up this server for replication, you can choose to set the server as an **Add-On** or **Replacement** server. These selections provide an alternate set up process, requiring less information for the initial setup. **Add-On** and **Replacement** servers receive most of their configuration from the primary server in the cluster.

If you are setting up this server to replace an existing server, and you are importing the database from the existing server, select **Replacement Server for Existing Server** 

#### NOTE

For add-on or replacement servers, you are not required to go through the full system setup.

# Select System Hostname

#### FIGURE 6 Enter Hostname

lostname Information		
	nultiple locations, including within the URL for OCSP of the root certificate a term. It is okay if the DNS entry is not yet setup.	authority. This should be set based on the
OTE: If you change this, the web serv	ver will restart. If you receive a 404 error, simply refresh the page.	
	anna242.cloudpath.net	
DNS Hostname (FQDN):		

# **Configure the System WWW Certificate**

The system is configured to use HTTPS, but does not currently have a valid WWW server certificate. An invalid WWW server certificate can impact the ability of end-user enrollments, causing 404 errors due to a lack of trust.

#### NOTE

The root account requires a WWW certificate. Tenant accounts will use the WWW certificate of the root account.

#### FIGURE 7 WWW Certificate

	Setup Next >
ww	Certificate for HTTPS
serve enrol prior	Instem is configured to use HTTPS, but does not currently have a valid WWW certificate. An invalid WWW server certificate will impact the ability of end-user ments, causing 404 errors due to a lack of trust. The system can be configured to the WWW server certificate being installed, but it should be installed prior to othing to enroll as an end-user.
The V	WW certificate may be a wildcard certificate (*.company.com) or a named certificate (onboard.company.com). The WWW certificate must mat
the D	WW certificate may be a wildcard certificate (*.company.com) or a named certificate (onboard.company.com). The WWW certificate must mate IS name used by the end-users to enroll. uest a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below.
the D	IS name used by the end-users to enroll.
the D	IS name used by the end-users to enroll. uest a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below.
the D	uest a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below. Generate a Certificate Signing Request (CSR) Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the
the D	IS name used by the end-users to enroll. uest a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below. Generate a Certificate Signing Request (CSR) Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the certificate back, it can be uploaded.
the D	IS name used by the end-users to enroll. uest a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below. Generate a Certificate Signing Request (CSR) Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the certificate back, it can be uploaded. Upload the WWW Certificate

You can skip this step for the initial configuration. However, it should be installed before adding tenant accounts, or enrolling end-users. You can configure the WWW server certificate from **Administration** > **System Services** > **Web Server** service.

Cloudpath supports web server certificates in P12 format, password protected P12, or you can upload the individual certificate components; the public key, chain, and private key or password protected private key.

# **Upload the WWW Certificate**

#### FIGURE 8 Upload WWW Certificate

~	Upload by PEM Files		
	If a p12 file is not available, you may	upload the individual components of the certificate. All files must be in PEM (Base64) format I	f the private key i
	password-protected, specify the pass	sword too. If the private key is not password-protected, leave the password blank.	
1	Public Key (PEM):	Choose File No file chosen	
1	Chain (PEM or P7b):	Choose File No file chosen	
1	Additional Chain (Optional):	Choose File No file chosen	
1	Additional Chain (Optional):	Choose File No file chosen	
1	Private Key (PEM):	Choose File No file chosen	
1	Private Key Password:		
1	Prompt for Password on Boot:		
~	Upload by P12		
	You may upload a server certificate in	n p12 format. To do so, you must also specify the password if the p12 is password protected.	
Ð	P12 File:	Choose File No file chosen	

Browse to locate and upload the web server certificate and click **Next** to continue with the system setup.

#### FIGURE 9 System Restarting After WWW Certificate Upload

System Setup			
Restarting Service			
Applying web server certificate	e to the system and restarting we	veb server. Please wait	
	Processing	×	
	200		

After restarting the web service, the system setup is complete.

The server displays a setup complete page, and a confirmation email is sent to the administrator.

FIGURE 10 Setup Complete for Multi-Tenant System

CLOUDPATH		(	-	U
Multilenant 👻	0			
Accounts	System Setup			
Snapshots	Initialization Task	Status		
Commands	Multi-Tenant Mode:	Activated.		
Administration	System Initialization:	Complete.		
Pannisoalion	Administrator Experience.			
Support >	Administrator UI:	https://anna242.cloudpath.net/admin/		
	Credentials:	The following email addresses have been sent a one-time password along with this information		
		anna@cloudpath.net		
		If you ever forget your password, you can reset it from the login screen.		
	Key Pages:	View Customer Accounts - View list of customers on this system.		
		Add Customer Account - To add a customer to this system.		
		Add/Manage Administrators - This page allows additional administrator logins to be setup.		

#### FIGURE 11 System Setup Confirmation Email

Administrator Experience:	
Administrator UI:	https://anna246.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information: <u>anna@cloudpath.net</u>
	If you ever forget your password, you can reset it from the login screen.
Key Pages:	View Customer Accounts - View list of customers on this system.
	Add Customer Account - To add a customer to this system. Add/Manage Administrators - This page allows additional administrator logins to be setup.

# **Navigating the Root Account**

The root account can view and manage all tenant accounts and perform system administration tasks, such as upgrades, certificate management, and license information.

### Accounts

In the **Accounts** tab view, tenant accounts are displayed according to the **Active**, **Disabled**, or **All** tabs at the top of the page. Click the arrow to the left of the account name to view account details, or click **Expand/Collapse All** button at the top of the page.

#### FIGURE 12 Accounts View

Multitenant	*	Show: Active Disabled All ExpandiCollapse All Publish All Snapshots Add Account	
Accounts			
Snapshots		> Account: Anna Brocade	(†)
Commands		> Account: Anna Ruckus	(±)
Administration	•	> Account: Anna Test BVT (Default)	
Support	•	> Account: Anna_Cloudpath	E
		> Account: TestNewAccount	(L)

#### Changing Into a Tenant Account From the Root Account

From the root account, use the down arrow to the right of the tenant account change into the account as an administrator for the tenant account.

FIGURE 13 Change Into Account from Root Account

Snapshots		> Account	Anna Brocade	Ţ.
Commands		> Account:	Anna Ruckus	Ē.
Administration	•	> Account	Anna Test BVT (Default)	
Support	•	> Account	Anna_Cloudpath	(L)
		> Account	TestNewAccount	Ţ.

# **Snapshots**

This summary view provides a glimpse into successful snapshots and the latest client version for each tenant account.

#### FIGURE 14 Snapshots View

Multilenant -	Show: Publish	ed Outdated No	Snapshot All	Publish All Snapshots
Accounts				
Snapshots	Account	Location	Status	Current Snapshot
-	Anna Brocade	Production	Search Latest Wizard	5.0.668 on 20170531 1616 MDT
Commands	Anna Ruckus	Production	S Latest Wizard	5.0.668 on 20170531 1610 MDT
Administration				
Support 🕨				

# Commands

The multi-tenant commands are shortcuts for root account administration.

- Click **Download** to obtain the email address of all administrators, as needed for system communications, such as upgrade notices.
- If your system is set up for trial accounts, click **Disable Expired Trials** when you want to disable expired accounts and free up RADIUS ports.
- Click **Refresh Licenses** to refresh license information between the multi-tenant system and the Cloudpath license server.

#### FIGURE 15 Commands View

Multitenant -	Multitenant > Commands
Snapshots	Multitenant Commands
Commands Administration	Administrators: Download Trials: Disable Expired Trials (60 Days)
Support	Licenses: Refresh Licenses

## **Administration - Administrators**

During the initial system setup, Cloudpath sets up an administrator for the root account.

Additional administrators for the root account can be added from the left menu **Administration** tab, or you can enable Administrator logins from your authentication servers.

#### FIGURE 16 Administrators for Root Account

Multitenant	•	Administration	> Administrators	Add Admin 🕨
Administration	-			
Administrators		> Admin 1:	anna@cloudpath.net	/ Ov
Company Informatio	n			
System Services				
System Updates				
Replication				
Support	•			

#### **Administrator Roles**

Cloudpath supports the following Administrator Roles for the root account:

- CA Administrator—Allows full configuration access to the Administrative UI. This administrator role can manage all administrative users.
- Administrator—Allows full configuration access to the Administrative UI, except for Certificate Authorities. This administrator can manage Administrator and Viewer administrative users.
- Viewer—Allows view-only access to Enrollment, User, and Certificate records on the Dashboard, the enrollment Workflow, and the Documentation and Licensing pages. This administrator cannot manage other administrative users.

# **Administration - Company Information**

Company Information is typically entered during the initial system setup but can be managed from the **Administration** > **Company Information** screen. The data from this page is used within the URL for enrollments and sponsorships, and included in the onboard CAs.

#### FIGURE 17 Company Information for Root Account

Muttenant	Administration > Company Information
Administration 👻	
Administrators	Company Information
Company Information	Display Name: Anna Test BVT
System Services	() Company Domain:
System Updates	() IT Email:
Replication	() Legal Company Name:
	Department Name:
Support >	City:
	Country:
	Default SMS Country Code: [Default]
	Portal URL
	URL Name:
	Load Balancer Protocol: [Default]
	Support Information
	The following information is included in the wizard in the event that the end-user needs to contact support.
	Support Email:
	Support Phone:
	Support URL:
	Support Message:

# **Administration - System Services**

Navigate to **Administration** > **System Services** to restart or view logs for the application server, web server, configure email or SMS servers, or start up a support tunnel.

#### FIGURE 18 System Services for Root Account

>	Service:	Web Server	1
>	Service:	Network	
>	Service:	SSH	•
>	Service:	Support Tunnel	٠
>	Service:	Outbound Email	1
>	Service:	Outbound SMS	1
>	Service:	Logs	1
>	Service:	External Reporting Server	1
	Service:	Virtual Machine	
2	Service:	Alexa	1
,	Service:	Auto VLAN Assignment	1

System services for the root account include:

- Web Server—Download the Apache Server access and error logs from the Web Server component. You can also Restart the web server, generate a CSR, edit administrative access restrictions, and download or upload the web server certificate, or if needed, upload a code certificate.
- Network—The Network service displays network properties for Cloudpath, and provides access to view or download the diagnostic logs.
- SSH—Use the SSH service to enable, disable or change the access port. SSH runs on ports 22 and 8022. You can set the port number using the command line or from the user interface. Even if you disable SSH access for both ports, SSH can continue to run.
- Support Tunnel—The Support Tunnel service allows you to open a support tunnel to help you in diagnosing issues with your application or configuration.
- Outbound Email—Use the onboard email provider or configure a local email server.
- Outbound SMS—Use the onboard SMS provider, enter a CDYNE account or route SMS message through a customerowned account.
- Logs—Configure where syslog messages are sent. You can enable the syslog, select the protocol over which the syslog messages are sent, and enter a host and port number.
- External Reporting Server—Allows you to integrate Cloudpath enrollment data with a reporting server, such as the ELK stack (Elasticsearch, Logstash, and Kibana).
- Virtual Machine Displays the system clock and system information about the virtual machine. You can also reboot or shut down the virtual machine from this page.

- Alexa Allows you to bind or unbind Alexa, remove old binding data, or get Alexa log files.
- Auto VLAN Assignment Allows you assign available VLAN IDs from a configured range of VLANs to users during their enrollment.

## **Administration - System Updates**

From the **System Updates** page, view and manage your existing build version, scan check for updates, and apply support patches.

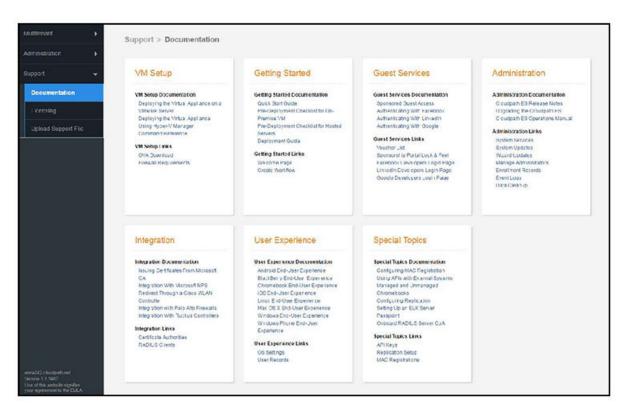
#### FIGURE 19 System Updates for Root Account

Multitenant >	Administration > System Updates
Administration 👻	
Administrators	System Updates
Company Information	
System Services	The system is currently running version 5.1.3467. No updates are currently available for this system.
System Updates	, teo apolena era sontariaz eraneme no era azaren.
Replication	Check For Updates
Support >	

### **Support - Documentation Page**

The **Documentation** page contains technical documents for getting the root system set up, integration with other systems, managing the system, and special configuration instructions. This page also provides links to the most commonly used pages in the Cloudpath Admin UI.

#### FIGURE 20 Documentation View



Cloudpath documentation can also be found on the Ruckus Support site at:

https:// support.ruckuswireless.com/documents?filter=89#documents.

# **Support - Licensing**

The Licensing page displays information about system licenses, active certificates, usage statistics, and copyright notices.

Muttenant F	Support > Licensing	Check For Updates
Administration		
Support 👻	License information	
Documentation Licensing Upicad Support File	Ucense Type: System Utilization	Active trail through [Uninown]. For posistance with licensing or renewate: Contact Sales:
	Statistics:	Users, AutherScations, Certificative IAAC Registrations, Notifications
	License Server	
	License Server; Link Established; Cestamet GUID; System (Senther;	htps://brtoloucpatr.net htps://inex.bi/rec2017053311514.MDT_Advancec (ret1/1966/s5-W/2558/attriff-still-4x38a4-4CQ) [00000C_CA183807_3349_ASPS DF24_77248835137C_58568544_06CD_F26A_12FC]
	Notices	
	Open Source Netices:	This product contains components covered by various open source licenses. These licenses, including the software components, are available at http://www.cloucp.ath.net/opanesource
	Patent Notice:	This product lockades software developed by the Abache Software Foundation (http://www.apache.org/) Protected by one or more of the toxicoerg patients (9,132,4-44,9,193,5-17,9,137,234,5,137,235,9,043,741,5,017,348). Contacts isport tor additional patients
anna242 eloudpoth.not Vorsion 5.1.3407 Upp of this woboils significa your agreement to the EULA	Copyright Notice:	Copyright 2012-2017 Ruckus Networks

# **Support - Diagnostics**

The **Diagnostics** page provides useful tools for system troubleshooting connectivity issues, and verifying certificate information.

FIGURE 22 Cloudpath Connectivity Diagnostics

Multitenant	•	Suppo	ort > Diagno	ostics				
Administration	•							
Support	*	Ping	DNS Lookup	HTTPS & Certificate		RADIUS Certificate	WLAN Controller	Generate Support Bundle
Documentation								
Licensing		()	Server DNS/IP	Address:	[ex. serve	r.domain.com]		Run
Diagnostics								
Upload Support F	File							

The diagnostics includes:

• Ping—Ping an IP address or hostname.

- DNS Lookup—Provide server information and IP address for a given hostname.
- HTTPS & LDAPS Certificate—Query the server certificate used by a secured server (HTTPS, LDAPS, etc.) to verify the certificate currently in use by a server.
- RADIUS Certificate—Query the RADIUS server certificate and the chain presented by the RADIUS server. This is useful to verify the certificate currently in use by a RADIUS server. For this test to work, the Cloudpath ES must be able to reach the IP and port, the shared secret must be correct, and the Cloudpath ES must be an approved client for the RADIUS server.
- WLAN Controller—Query the WLAN controller to check if required ports are accessible.
- Generate Support Bundle: Click **Run** from this tab to generate a zip file that contains log files and metrics information to provide to your Ruckus support representative.

# **Support - Upload Support File**

If Cloudpath Support has provided a support file, you can upload it on this page. This will make changes to the system, so we recommend that you create a VMware snapshot first.

#### NOTE

Only use a support file with the assistance of the Cloudpath Support team.

#### FIGURE 23 Upload Support File for Root Account

Multitenant	Support > Upload Support File
Administration	
Support 👻	Support File Information
Decumentation	Important: A support file should only be uploaded when advised by support.
Licensing	This will make changes to the system, so it is advised to create a snapshot of the $\forall M$ .
Upload Support File	(i) Support File: Choose File No file chosen
Licensing	This will make changes to the system, so it is advised to create a snapshot of the ∨M .

# **Adding Tenant Accounts**

This section describes how to add a tenant account.

# Adding a Tenant Account From the Root Account

A root account administrator adds tenant accounts from the root account Accounts tab.

From the multi-tenant root account **Accounts** page, click the **Add Account** button.

#### FIGURE 24 Add Tenant Account

Accounts			
Snapshots	> Account: Anna B	3rocade	[1]
Commands	> Account: Anna R	Ruckus	[1]
Administration	> Account: Anna Te	Fest BVT (Default)	

# **Create Tenant Account**

Enter tenant account information:

- Company Name
- Company URL Name
- Create Account Administrator
- Admin Display Name
- Admin User Name

#### FIGURE 25 Create Tenant Account Information

Multienant -	Accounts > Create Cancel Save
Accounts	
Snapshots	Account Information
Commands	
Administration	(i) Company Name: Anna Brocade.
, Anni anni anni anni anni anni anni anni	() Company URL Name: AnnaBrocade ·
Support )	(j) Create Account Administrator:
	Admin Display Name:     Anna Brocade
	Admin Userrame: aekhel@brocade.com *
	Specify Password:
	The password specified below will be used. The administrator will not be emailed.
	Password:
	Confirm Password:

### **Tenant Account Admin Password**

Different methods for creating tenant administrator accounts:

• Create an admin account without specifying a password. A system generated password is emailed to the admin.

- Create an admin account with a defined password. The system does not send an email notification for defined passwords.
- Create no account admin. The account is created without an admin. The only way to access the account is by changing into the tenant account from the root account. For details, see the "Changing Into a Tenant Account From the Root Account" section of the Navigating the Root Account on page 20 topic.

# **Setting Up the Tenant Account**

After the tenant administrator account has been created, use the tenant administrator credentials from the new administrator account email to access and log in for the initial system setup.

#### Account Administrator Login

Use the temporary password from the administrator email.

Example email with login credentials:

```
You have been added as an administrator.
URL: https://test245.cloudpath.net/admin/
Username: test_user@cloudpath.net
Temporary Password: Uw6hYcE9vS
```

#### NOTE

If no tenant account admin was specified, the root account user can change into the account for system setup.

#### FIGURE 26 Log In With a Temporary Password

ENROLLMENT SYSTE		
	Sign In	
	Forgot Password Sign Sign Copyright © Ruckus, an ARRIS Company 2019. All rights reserved Activate Account	

#### **Account Admin Setup Credentials**

#### NOTE

If you were assigned a specific password when the tenant account was set up, you will not be prompted to change your password.

#### FIGURE 27 Set up new credentials

System Setup	
Change Password	
Enter information below to esta	ablish an onboard username and password.
(i) Username:	anna@cloudpath.net
(i) New Password:	
(i) Confirm Password:	

## **Tenant Account Setup Wizard**

After the first login to a tenant account (by logging in, or by changing into the account), the system setup wizard guides you through a few basic steps.

#### **Company Information**

Enter **Company Information**. This information is embedded in the onboard root CA certificate.

#### FIGURE 28 Company Information

Cha	inged into account.			
Compa	any Information			
() Co	mpany Name:	Anna Brocade	•	
🕕 Leg	gal Company Name:	[ex. Sample Company, Inc.]		
① Dep	partment Name:	[ex. Information Technology]		
() City	у:	[ex. Westminster]		
i Sta	ate/Province:	[ex. Colorado]		
() Co	untry:	[ex. US] •		
Compa	any Web Presence			
<li>Cor</li>	mpany Domain:	[ex. company.com]		
🕕 Suj	pport Email:	[ex. support@company.com]		
	Email:	[ex. it@company.com]		

#### Select Workflow Template

To initialize the system with a sample configuration, select **BYOD Users & SMS Guests**, or **BYOD Users Only**. This creates an initial workflow for BYOD users and sponsored guests (or BYOD users only) that you can use as a template, or simply add a device configuration and use immediately.

To create your own workflow, select Start with Blank Canvas.

orkfl	ow Information	
The s		figuration or initialized blank. Either way, the system may be fully customized after being initialized. Select your preference
۲		OD and guest users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issu
0	BYOD Users Only. Initializes the system for handling BYO certificate granting them BYOD access	20 users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a s.
0	Start with a Blank Canvas.	

#### **Authentication Server**

#### NOTE

If you selected a **Blank Canvas** for the default workflow, you are not prompted to set up an authentication server during the initial system setup.

If you plan to use an authentication server to authenticate end-users or sponsors, we recommend populating the authentication server information page.

If using multiple authentication servers, additional authentication servers may be added through the workflow or from the **Configuration** > **Authentication Servers** page.

#### FIGURE 29 Set Up Tenant Authentication Server

S.	Connect to Active Directory		
	Select this option to enable end-users to	authenticate via Active Directory.	
	Default AD Domain:	test.cloudpath.local	
	() AD Host:	Idaps://192.168.4.2	
	() AD DN:	dc=test,dc=cloudpath,dc=local	
	() AD Username Attribute:	SAM Account Name	
	Verify Account Status On Each Aut	hentication	
	Perform Status Check:		
	Additional Logins		
	(i) Use For Sponsor Logins:	¥	
	Test Authentication		
	Run Authentication Test?	V	
	() Test Username:	bob	·
	(i) Test Password:		•
0	Connect to LDAP		
	Select this option to enable end-users to a	uthenticate via LDAP (or LDAPs).	
0	Connect to RADIUS		
	Select this option to enable end-users to a	uthenticate via RADIUS using PAP.	
0	Connect to SAML		
	Select this option to enable end-users to a	uthenticate via a SAML 2.0 IdP.	

To setup the initial configuration of the authentication server, select and enter the required fields.

Consider these optional settings for the authentication server:

- Verify Account Status on Each Authentication—If selected, Active Directory is queried during subsequent uses of the certificate to verify the user account is still enabled. You must provide the bind username and password for an authentication server administrator account.
- Additional Logins—If Use for Admin Logins is selected, administrators can log into the Cloudpath Admin UI using credentials associated with this authentication server. If **Use for Sponsor Logins** is selected, sponsors can log into the Cloudpath Admin UI using credentials associated with this authentication server.
- **Test Authentication**—If selected, an authentication will be attempted using the username and password provided to test connectivity to the authentication server. This test can also be run from the workflow.

#### **Authentication Server Certificate**

#### FIGURE 30 Authentication Server Certificate

Tous	e Active Directory via I DAP	S, the system needs to know which server certificate to accept for the authentication server.
	Pin the Current Serve	ALLE IN SUCCESSION IN THE SUCCESSION INTERPORTS ASSION INTERPORTS
		ertificate as a trusted certificate. This is the quickest and easiest but must be updated when the certificate is renewed.
	Common Name:	svr-2 test cloudpath local
	Thumbprint:	QA6EDA55C030F7015DDA34E6664A4568D2F301C3
	Valid Period:	03/05/2017 - 03/05/2018
	leaved By:	Cloupdath Networks MDtCA
	1	

Select **Upload the Chain for the Server Certificate** to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

Select **Pin the Current Server Certificate** to use the current server certificate as the trusted certificate. This setting must be updated if the certificate is renewed.

#### **Publish Tenant Account**

#### FIGURE 31 Publish Tenant Account

stem Setup	
Initialization Task	Status
Create Certificate Authorities:	Completed.
Create Certificate Templates:	Completed.
Create Device Configurations:	Completed.
Configure Workflow:	Completed.
Activate Sponsor Portal:	Completed.
Publish Enrollment Portal:	Completed.
	System is ready to handle enrollments.
Access Point Setup:	
	The following information will be necessary to configure the access point with the appropriate secure SSID configuration.
SSID:	eng-AnnaBrocade (WPA2-Enterprise, AES (CCMP), Broadcast)
RADIUS IP:	anna242.cloudpath.net
RADIUS Authentication Port	14391
RADIUS Accounting Port	14392
RADIUS Shared Secret	q5urhc6x3aj6c6ep5uex
RADIUS Attributes:	BYOD Policy Template - VLAN: '1'
	Guest Policy Template - VLAN: '1'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna242.cloudpath.net/enroll/AnnaBrocade-1/Production/

After the initial setup tasks, the system finishes the initialization process. When the publishing tasks are complete, the system is ready to use. The setup information is also emailed to the system administrator for this account.

# **Tenant Account Login**

This section describes how a tenant can access and manage the tenant account.

# **Tenant Logs In**

Enter the hostname for the tenant account into a browser to access the tenant account and log in using the credentials previously set up. See the "Account Admin Setup Credentials" section of the Adding Tenant Accounts on page 28 topic.

The hostname can be found in the Cloudpath Setup Information emailed to the account administrator.

# **To Do Items**

After account login, the **Cloudpath Welcome** page is displayed. If the **ToDo Items** list displays, the configuration items listed describe what is needed to complete the account setup.

#### FIGURE 32 Cloudpath Welcome Page

Idministrators control by blending traditional employee-centric capabilities (Act apabilities (sponsorship, email, SMS, Facebook, and more).	ive Directory, LDAP, RADIUS, and Integration with Microsoft CA) with guest-centr
Setting Started Ise the left menu tabs to begin setting up your workflow configuration. The Dashboard tab displays reporting information about the enrollments, isers, devices, certificates, and more.	Todo Items A newer wizard version (5.0.776) is available for workflow "Production". Creating a new snapshot that contains the new wizard version is recommended.
The Configuration tab allows you to configure and deploy the enrollment vorkflow, including the look & feel and the device configuration.	System logging is currently running in debug mode.
Ind customize the look & feel of the sponsorship portal. from the Certificate Authority tab, you can manually generate certificates, iew certificate details, revoke certificates, manage the characteristics of ertificates to be issued, and manage certificate authorities (CAs).	The following authentication servers utilize Google's deprecated
he Administration tab allows you to manage administrator accounts, system s	ervices, diagnostics and logs, and system updates.
he Support tab provides access to the Quick Start Guide and several Setup G	Suides to help with common configurations along with licensing information.

### **Enrollment Workflow**

During the initial system setup, a default workflow was configured. Navigate to **Configuration** > **Workflows** to view and manage the enrollment workflow for the tenant account.

#### FIGURE 33 Workflow Setup Page Tenant

	Wo	Warkflows Froduction			Status	Enrollment Portal URL Dienroll/AnnaBrocade-1/Production/			Last Publish Time 20170531 1001 MDT		
Workflows	O Pro				Publishec						
Device Configurations						The second second					
RADIUS Server	Properties	Enrol	Iment Process	Look & Feel	Snapshot(s)	Advanced					
Authent cation Servers	+										
Firewalls & Web Fitters	1	Step 1: Require the user to accept the AUP Welcome Message and AUP						1	×		
MAC Registrations	*										
API Keys	1	Step 2:	All matches in	n: × / vi	sitors Employees	+		1	$\equiv$	×	
onsorship 🕨		Step 3:	Send a verifi	cation code fr	om Guest Vouch	ers			1	×	
tificate Authority											
ministration		Result: Move user to eng-AnnaBrocade and assign certificate using Guest Policy Templat									1

Refer to the complete set of technical documentation for more information about configuring the tenant account enrollment workflows.

Configuration documentation can be found on the **Support** > **Documentation** tab, and also on the Ruckus Wireless Support website at: https://support.ruckuswireless.com/documents?filter=89#documents.



© 2019 CommScope, Inc. All rights reserved. Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc. 350 West Java Dr., Sunnyvale, CA 94089 USA www.ruckuswireless.com