

Cloudpath Enrollment System Private Virtual Machine Pre-Deployment Checklist

Supporting all Cloudpath Software Releases

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	4
Document Conventions.....	4
Command Syntax Conventions.....	4
Document Feedback.....	5
Ruckus Product Documentation Resources.....	5
Online Training Resources.....	5
Contacting Ruckus Customer Services and Support.....	5
Overview	6
Customer Worksheet	7
Information for the Customer to Consider Before Cloudpath is Deployed	7
Initial Setup	8
Who Should Be Involved in the Initial Setup Call	9
Deployment Testing for Cloudpath	9

Preface

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 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.

italic text

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.

Convention	Description
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.

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>
- 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.

Overview

The purpose of this pre-deployment checklist for a virtual machine is to help you plan your Cloudpath deployment by considering various aspects of your network.

This checklist is targeted for both the customer who is performing the deployment and the Cloudpath representative who may be assisting the customer with the deployment.

It is recommended to read through this document thoroughly, and complete any requested information, prior to starting the initial configuration.

Customer Worksheet

To help plan your Cloudpath deployment, it can be helpful to complete the customer worksheet questions to provide some general information about your network.

It is recommended to complete the customer worksheet before starting Cloudpath deployment.

NOTE

If you have purchased White Glove support for your Cloudpath system, you can provide the following information to your Cloudpath deployment representative.

- Customer name (If sending this information to your Cloudpath representative) _____
- Which brand of AP/Controller are you using? _____
- Are you currently utilizing certificate-based authentication in your network? _____
- Are you currently utilizing a RADIUS server in your network for certificate authentication? _____
- Are you using Network Access Control (NAC) in your network? _____
- Do you have a load balancer? _____ If yes, who is the vendor? _____

Information for the Customer to Consider Before Cloudpath is Deployed

Before Cloudpath is implemented into the customer network, the following network configurations should be considered:

- The initial firewall configuration should be set up to allow Internet access for the following:
 - Access from ES -> xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)
 - Access from ES -> dist2.cloudpath.net (used for ES updates TCP 80/443-HTTP/HTTPS)
 - Access from ES -> NTP (UDP 123)

NOTE

You can use **0.centos.pool.ntp.org** on the standard NTP port (123). This can be configured to point to a local server during system setup, if you prefer.

- Internally, the guest/onboarding VLAN needs to be able to access to the wireless controller (this can be locked down to specific ports after the initial setup).
- The WLAN controller requires Layer 3 access to the Cloudpath server.
- If using Active Directory, you need the AD domain information (plus any subdomains) and the IP address of the AD server.

NOTE

AD groups should be set up before the implementation call.

NOTE

The Cloudpath VM should have Layer 3 access to Active Directory (Port 636 for LDAPs, Port 389 for LDAP).

Initial Setup

- Your wireless controller must be WPA2-Enterprise capable.
- You should have knowledge about how to configure a captive portal on your wireless controller(s).
 - The open SSID typically has pre-authentication ACLs defined, which permit access to the VM.
 - The WLAN controller is configured to point to the Cloudpath VM as an external captive portal.
- The WPA2-Enterprise SSID should be set up to delegate authentication to the onboard AAA server or your existing AAA.

NOTE

If using an existing AAA server, it requires Layer 3 access to the Cloudpath VM to verify certificate status (optional).

- A web server certificate is required for HTTPS. The system can be configured prior to the WWW server certificate being installed, but it should be installed before attempting to enroll end-users.
 - The WWW certificate may be a wildcard certificate (*.company.com) or a named certificate (test.company.com).
 - The WWW certificate must match the DNS name used by the end-users to enroll.
 - To request a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, you can download a CSR from ES after the system is set up.
- If using NPS, set up the NPS server role and a RADIUS server.

NOTE

The new RADIUS server certificates and root CA can be uploaded after Cloudpath is configured.

- If using a pre-existing RADIUS server, you need the IP address and access to the RADIUS server-signed certificates.
- If using an existing CA, and you would like to use Cloudpath as an intermediate CA to issue client certificates, you need the public and private key of the existing CA to upload into Cloudpath.
- If using Cloudpath as a proxy for an existing CA (Microsoft CA or Custom External CA) you need the CA URL and CA chain for the remote CA.
- DNS should be configured for Cloudpath and other components appropriate for your network.
- You should have a general idea about your deployment scheme for employees, partners, contractors and guests.

Initial Setup

Before an implementation call between the customer and a Cloudpath representative, the Cloudpath representative should review the customer checklist in this guide as well as the entire *Cloudpath Deployment Guide*.

If deploying to a local VMware server, the customer should download the OVA file prior to the implementation call.

The call should cover the following topics at minimum:

- Discussion about what the customer wants to achieve
- Initial product setup
- Workflow basics

Who Should Be Involved in the Initial Setup Call

Be sure to include anyone in the initial setup call regarding your Cloudpath system who will be involved with administering the network.

Cloudpath implementation affects different aspects of your environment. Therefore, you might want to involve other members of your network team. Suggestions follow:

- Cloudpath is installed as a virtual appliance. If you have a VM team, they should be contacted regarding the deployment.
- The open and secure SSIDs are set up on the wireless controller. The person/team who manages this aspect of your network should be available for making adjustments to the wireless controller.
- Cloudpath can be set up to authenticate users to an Active Directory or LDAP server. Typically, you do not need to make adjustments to the authentication server. However, if there are issues connecting to the secure network, the person/team responsible for the authentication server might be required.
- If you plan to use the onboard RADIUS server, which is recommend, you do not need the RADIUS server team. However, if you plan to use NPS or another external RADIUS server, the RADIUS person/team should attend the setup meeting as user certificates are authenticated to the RADIUS server.

NOTE

After the initial setup, Cloudpath provides a list of the inbound and outbound traffic of your system. Firewall updates may be required for getting Cloudpath up and running in your network.

Deployment Testing for Cloudpath

Ideally, for your deployment testing, you should have devices on hand for each operating system that you plan to support. While the enrollment workflow behaves the same on each device, the Wizard application behaves slightly differently on each operating system. With Android, this issue is compounded by the fact that each vendor can make modifications to the Android operating system, causing the application, in some cases, to behave differently between models.

Contact your Sales or Support representative to review the End-User Experience documentation for your supported operating systems.



© 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