

# Cloudpath Enrollment System TACACS+ Server Configuration Guide, 5.12

**Supporting Cloudpath Software Release 5.12**

© 2023 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](http://www.cs-pat.com).

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>5</b>
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
<b>About This Document.....</b>	<b>9</b>
Acknowledgments.....	9
Purpose of This Cloudpath Configuration Guide.....	9
TACACS+ Features Not Supported in This Release of Cloudpath.....	9
TACACS+ Features Considerations.....	10
New In This Document.....	10
<b>Overview of Using Cloudpath as TACACS+ Server.....</b>	<b>11</b>
Authentication via TACACS+.....	12
Authorization via TACACS+.....	13
Accounting via TACACS+.....	13
<b>Client Configuration Requirements.....</b>	<b>15</b>
<b>Configuring TACACS+ in the Cloudpath Administration UI.....</b>	<b>17</b>
Configuration Overview.....	17
Enabling TACACS+.....	18
Configuring an Authentication Backend.....	19
Configuration Steps.....	19
Adding the Certificate to Secure LDAP SSL or LDAP TLS Backend.....	21
Testing the LDAP Authentication.....	22
Configuring TACACS+ Devices.....	23
Configuration Steps.....	23
Other Actions You Can Perform From Main Device Configuration Screen.....	26
Configuring Time Ranges.....	27
Configuration Steps.....	27
Other Actions You Can Perform From Main Timespec Configuration Screen.....	28
Configuring Access Control Lists.....	29
Configuration Steps.....	29
Other Actions You Can Perform From Main ACL Configuration Screen.....	30
Configuring TACACS+ Services.....	31
Configuration Steps.....	31
Other Actions You Can Perform From Main Services Configuration Screen.....	33
Configuring TACACS+ Groups.....	34
Configuration Steps.....	34
Other Actions You Can Perform From Main Group Configuration Screen.....	36

Configuring TACACS+ Users.....	36
Configuration Steps.....	36
Other Actions You Can Perform From Main Users Configuration Screen.....	38
Creating Configuration Profiles.....	39
Configuration Steps.....	39
Verifying a Configuration Profile.....	42
Other Actions You Can Perform From Main Configuration Profiles Screen.....	43
Testing a Configuration Profile.....	44
Checking and Changing TACACS+ Server Status and Gathering Log Information.....	45
Checking and Changing Status.....	45
Setting the Debug Log Level.....	45
Gathering Log Information.....	46

# 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](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](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](mailto:#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>
<b>bold</b>	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> .
<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
<b>bold text</b>	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 This Document

---

- Acknowledgments..... 9
- Purpose of This Cloudpath Configuration Guide..... 9
- TACACS+ Features Not Supported in This Release of Cloudpath..... 9
- TACACS+ Features Considerations..... 10
- New In This Document..... 10

## Acknowledgments

The Cloudpath implementation of TACACS+ server uses the "pro-bono-publico.de tac plus" project daemon server referenced at the following location: [https://www.pro-bono-publico.de/projects/tac\\_plus.html](https://www.pro-bono-publico.de/projects/tac_plus.html)

This product includes software developed by Marc Huber (Marc.Huber@web.de).

The original tac\_plus code (which Mark Huber's software and considerable parts of his documentation at [https://www.pro-bono-publico.de/projects/tac\\_plus.html](https://www.pro-bono-publico.de/projects/tac_plus.html) are based on) is distributed under the following license: Copyright (c) 1995-1998 by Cisco Systems, Inc.

## Purpose of This Cloudpath Configuration Guide

This guide describes the configuration that you perform in the Cloudpath UI to create your TACACS+ server configuration. It is not intended to cover all aspects of TACACS+. Cloudpath supports TACACS+ in a single-tenant environment only.

### NOTE

**For complete TACACS+ information, refer to the "pro-bono-publico.de tac plus" documentation referenced above in the "Acknowledgments" section.** That document should be referenced for details about TACACS+ including syntax for declarations and statements that you will use while configuring your TACACS+ server in the Cloudpath UI.

## TACACS+ Features Not Supported in This Release of Cloudpath

The following is a list of items not currently supported in Cloudpath:

- Multiple Realms: Cloudpath supports only one realm.
- Global configuration options: The TACACS+ server listening port is configurable (described later). For other global options, the defaults that are provided and documented by the "pro-bono-publico.de tac plus" project are used.
- Logging: Log files, not syslog, are used. Default logging format is used; customizing the reporting format is not supported.

# TACACS+ Features Considerations

The following is a list of considerations:

- Debugging: Three debugging levels are supported: None, Debug, and Packet. Debug level enables most debugging modes allowed by the TACACS+ server except PACKET mode. Packet level provides packet dump and only generates logging files in the server. The packet dump logging files are not accessible through the Web UI. How to set these levels is shown later in this document
- Mavis Backend: Cloudpath supports LDAP backends, including Active Directory and generic LDAP. Cloudpath also supports local user authentication without using Mavis backend. This is described later in this document.

## New In This Document

**TABLE 2** Key Features and Enhancements in Cloudpath 5.12 (July 5, 2023)

Feature	Description	Reference
TACACS+ group membership modification	<b>Updated:</b> When adding a user groups to your TACACS+ configuration, certain characters are restricted.	<a href="#">Configuring TACACS+ Groups on page 34</a>
Modification to TACACS+ debugging	<b>Updated:</b> For TACACS+ debugging within the Admin UI, “Packet” level debugging is no longer an available debugging level option accessible to Admin UI users due to sensitive data considerations.	<a href="#">Checking and Changing TACACS+ Server Status and Gathering Log Information on page 45</a>
Minor editorial updates	<b>Updated:</b> Minor editorial updates were made throughout the Configuration Guide.	All chapter
Updates to address defects	<b>Updated:</b> Minor updates on content throughout to address defects.	All chapters

# Overview of Using Cloudpath as TACACS+ Server

---

You can use your Cloudpath system as a TACACS+ server to manage device access and usage.

Cloudpath Enrollment System is a TACACS+ server which acts as network access control for network devices. TACACS+ provides Authentication, Authorization, and Accounting services for network devices, and specifically provides:

- Centralized authentication and identity for access management to network devices.
- Per-command authorization on network devices.
- Logs for all user-entered commands.

**NOTE**

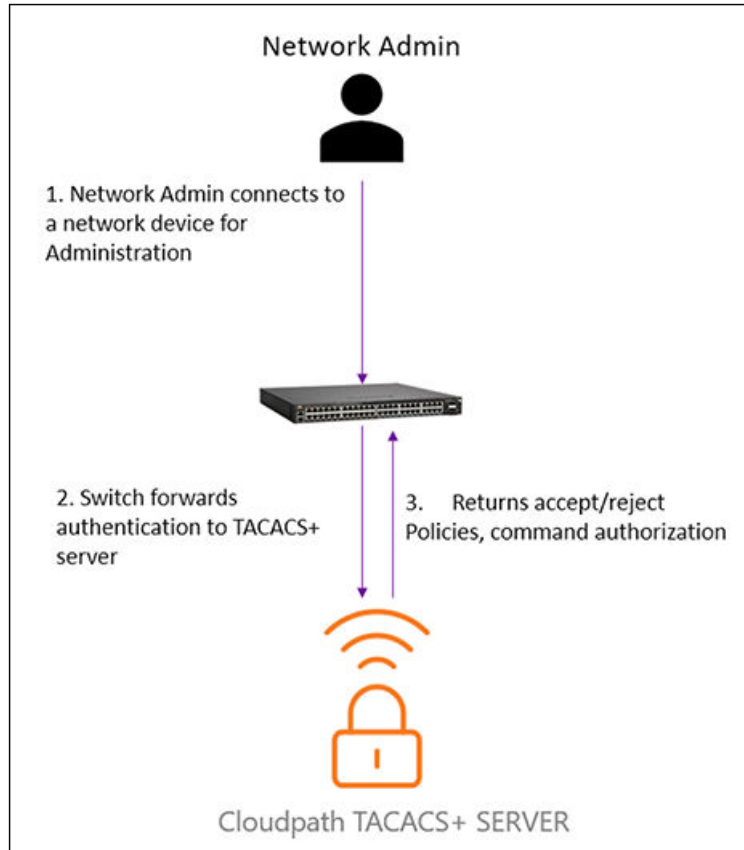
With TACACS+, authentication and authorization are separate processes.

**NOTE**

Cloudpath supports TACACS+ in a single-tenant environment only.

A TACACS+ client can be any device with TACACS+ client support, such as RUCKUS ICX switches, RUCKUS Network Controllers, Cisco switches and routers, and others. All traffic is encrypted. The following figure illustrates the basic flow of device-to-Cloudpath TACACS+ server communication.

FIGURE 1 Flow of Device-to-Cloudpath TACACS+ Server Communication



**NOTE**

Port 49 is used for the TCP connection between a network device and the TACACS+ server.

## Authentication via TACACS+

The steps for how a user such as a network administrator gets authenticated by the Cloudpath TACACS+ server are:

1. The user attempts to gain access to the network device by doing one of the following:
  - Logging into the device using Telnet, console, SSH, or a web management interface.
  - Entering the Privileged EXEC level or CONFIG level of the CLI on the device.
2. The user is prompted for a username and password.
3. The user enters the correct username and password.
4. The device sends a request containing the username and password to the TACACS+ server.
5. The username and password are validated in the TACACS server authentication backend or local user repository.
6. If both username and password are valid, the user gets authenticated.

## Authorization via TACACS+

Two types of TACACS+ authorization are supported:

- Exec authorization. This type of authorization determines the user-privilege level when the user is authenticated, as follows:
  1. A user logs into the network device using Telnet, console, SSH, or a web management interface.
  2. The user gets authenticated.
  3. The device communicates with the TACACS+ server to determine the privilege level of the user.
  4. The TACACS+ server sends a response back to the device that contains an A-V (Attribute-Value) pair with the privilege level of the user.
  5. The user is granted the specified privilege level.
- Command authorization. With this type of authorization, the switch communicates with the TACACS+ server to determine whether the user is authorized to run specific commands, as the following process shows:
  1. A Telnet, console, SSH, or web management interface user who has already been authenticated by the TACACS+ server enters a command on the network device.
  2. The device looks in its configuration file to determine if the command has a privilege level that requires TACACS+ command authorization.
  3. If the command does have a privilege level that requires authorization, the device consults the TACACS+ server to determine if the user is authorized to run the command.
  4. If the user is authorized to run the command, the command gets executed.

## Accounting via TACACS+

The steps for how accounting works on the TACACS+ server are:

1. One of the following events occur on the switch/smartzone device: A user logs into the management interface using Telnet or SSH :
  - A user enters a command for which accounting has been configured.
  - A system event occurs, such as a reboot or reloading of the configuration file.
  - The device checks the configuration to see if the event is one for which TACACS+ accounting is required.
2. If the event requires TACACS+ accounting, the device sends a TACACS+ Accounting Start packet to the TACACS+ accounting server, containing information about the event.
3. The TACACS+ accounting server acknowledges the Accounting Start packet.
4. The TACACS+ accounting server records information about the event.
5. When the event is concluded, the device sends an Accounting Stop packet to the TACACS+ accounting server.
6. The TACACS+ accounting server acknowledges the Accounting Stop packet.



# Client Configuration Requirements

---

For each device, you need to configure the AAA server to use the Cloudpath TACACS+ authentication server.

Refer to the documentation for each device, but keep in mind the following information that you will need to know when configuring the device:

- Port 49 (or a different port number that you configured in the Cloudpath TACACS+ Server Settings) is used for the connection between the device and the Cloudpath TACACS+ server.
- The IP Address to enter for the TACACS+ server is the IP address of your Cloudpath system.
- A shared secret or shared key that is requested on the device-side configuration will also need to be entered during the Cloudpath TACACS+ server device configuration.
- 

For RUCKUS controller and device documentation, go to: <https://support.ruckuswireless.com/>.

For information about configuring the AAA server for a RUCKUS ICX switch as a TACACS+ server, see the *RUCKUS FastIron Security Configuration Guide*, "TACACS+ Server Authentication" chapter.

For information about configuring the AAA server for a RUCKUS SmartZone Controller, see the *RUCKUS SmartZone Controller Administration Guide*, "Working with AAA Servers."





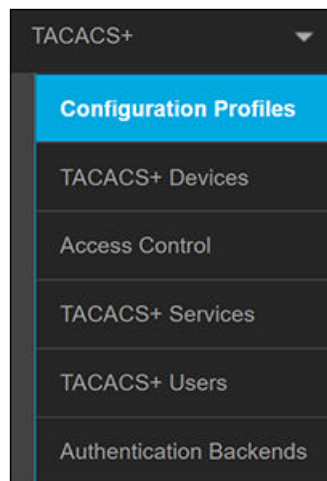
# Configuring TACACS+ in the Cloudpath Administration UI

- Configuration Overview..... 17
- Enabling TACACS+..... 18
- Configuring an Authentication Backend..... 19
- Configuring TACACS+ Devices..... 23
- Configuring Time Ranges..... 27
- Configuring Access Control Lists..... 29
- Configuring TACACS+ Services..... 31
- Configuring TACACS+ Groups..... 34
- Configuring TACACS+ Users..... 36
- Creating Configuration Profiles..... 39
- Checking and Changing TACACS+ Server Status and Gathering Log Information..... 45

## Configuration Overview

All TACACS+ configuration information can be entered in the Cloudpath UI.

**FIGURE 2** TACACS+ Configuration Menu in Cloudpath UI



Because TACACS+ configuration components reference each other, it is recommended to proceed in the following order:

1. [Enabling TACACS+](#) on page 18
2. [Configuring an Authentication Backend](#) on page 19 - This is the LDAP server that must contain all the configuration groups allowed to log in to the various devices you plan to configure. If you plan to add users on an individual basis, then you do not need to select an LDAP server and can instead add each user locally (described later).
3. [Configuring TACACS+ Devices](#) on page 23 - These are the end devices that will be clients to the TACACS+ server.

## Configuring TACACS+ in the Cloudpath Administration UI

### Enabling TACACS+

4. [Configuring Time Ranges](#) on page 27 - Time ranges can be called by reference into ACL configurations; therefore time ranges must be configured before ACLs.
5. [Configuring Access Control Lists](#) on page 29 - ACLs not only call in time ranges, but ACLs themselves can be called by reference into groups and users; therefore ACLs must be configured before groups and users.
6. [Configuring TACACS+ Services](#) on page 31 - Globally configured services can be called by reference into groups and users; therefore such services must be configured before users and groups.
7. [Configuring TACACS+ Groups](#) on page 34 - Groups can call in already-configured ACLs and services.
8. [Configuring TACACS+ Users](#) on page 36 - Users can call in already-configured ACLs and services.
9. [Creating Configuration Profiles](#) on page 39 - Profiles must be configured last because they call in the other previously configured components.

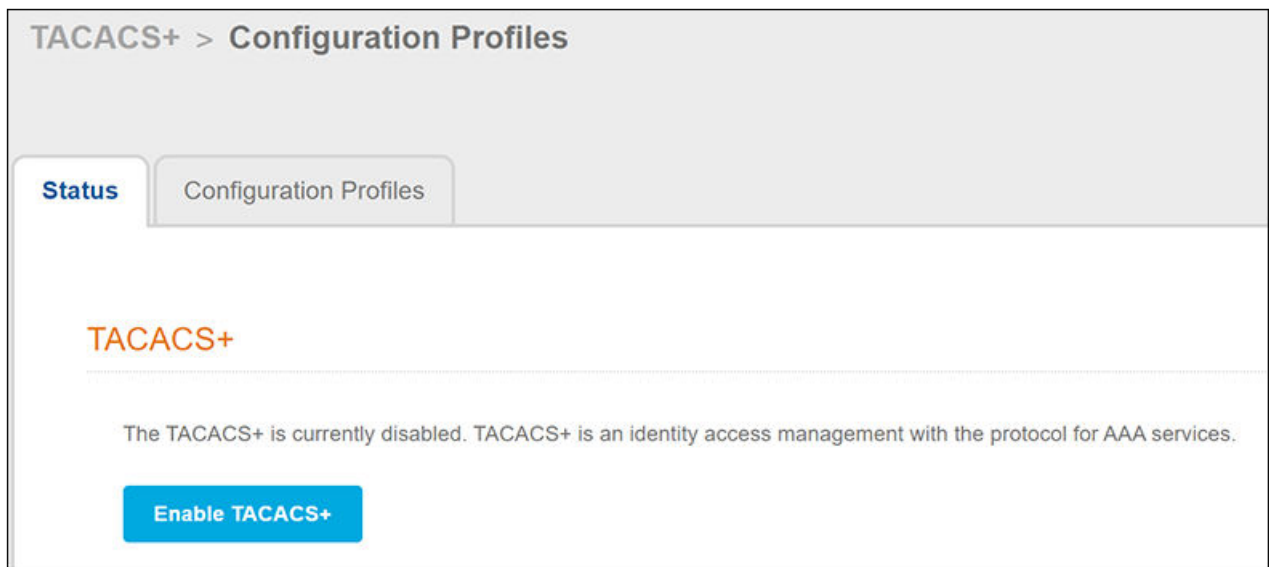
## Enabling TACACS+

TACACS+ is disabled by default, so you must first enable the setting in the Cloudpath UI.

To enable TACACS+, perform the following steps.

1. Navigate to **TACACS+ > Configuration Profiles** to invoke the following screen.

**FIGURE 3** Enabling TACACS+



2. Click the **Enable TACACS** button.

A message indicating that TACACS has been enabled should appear on the screen. However, since no other configuration has yet been performed, the TACACS+ Server Status will show:

Not Running. No Configuration Profile is currently applied to the TACACS+ server.

# Configuring an Authentication Backend

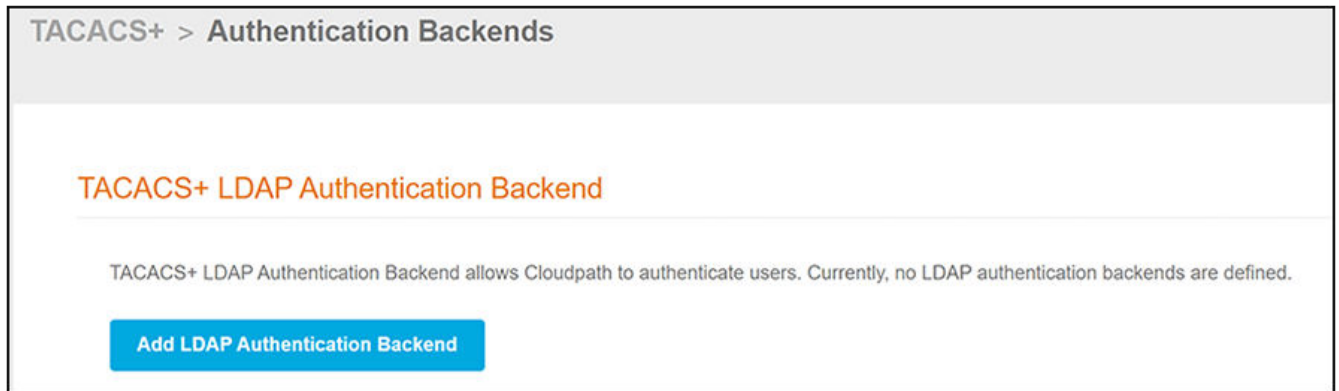
An LDAP server is required for TACACS+ authentication for external users and groups. Both LDAP over SSL (LDAPS) and LDAP over TLS are supported.

## Configuration Steps

Follow these steps to configure an LDAP server:

1. In the Cloudpath UI, go to **TACACS+ > Authentication Backends**. The following screen is displayed.

**FIGURE 4** Adding an LDAP Authentication Server



2. Click the **Add LDAP Authentication Backend** button.
3. Configure the values to create the TACACS+ LDAP authentication backend, as shown in the following example.

FIGURE 5 Creating the LDAP Authentication Backend

The screenshot shows a web interface for creating a TACACS+ LDAP Authentication Backend. The breadcrumb navigation is 'TACACS+ > Authentication Backends > Create'. There are 'Cancel' and 'Save' buttons in the top right. The form title is 'TACACS+ LDAP Authentication Backend Information'. The form contains the following fields:

- Authentication Backend Name: ldap\_SSL
- Description: (empty)
- LDAP Server Type: microsoft (dropdown)
- AD Group Prefix: [ex. tacacs]
- LDAP Host: ldaps://192.168.4.170:636
- Use StartTLS: (checkbox, unchecked)
- LDAP Scope: sub (dropdown)
- LDAP DN: dc=demo,dc=sample,dc=local
- Bind Username: svc\_tacplus@demo.sample.local
- Bind User Password: cpn!00T19

- Authentication Backend Name: A descriptive name for the LDAP server; this name will be used when you build the configuration profile.
- Description: (Optional) Description of the LDAP server.
- LDAP Server Type: Choose one of the following from the drop-down list:
  - microsoft - for Active Directory
  - generic - for a generic LDAP where the user gets authenticated.
  - tacacs\_schema - for a TACACS+ LDAP Schema.

**NOTE**

The TACACS+ LDAP schema is not supported.

- AD Group Prefix (applicable only to AD Microsoft servers): An AD group name that contains this prefix is used to determine a user's TACACS+ group membership, and the prefix is stripped from the TACACS+ group name. **Example:** If the AD Group Prefix is set to "tacacs", members of the AD group called "TacacsNOC" get assigned to the TACACS+ group called "NOC".

**NOTE**

TACACS+ group names are case-sensitive.

- LDAP Host: Space-separated list of LDAP URLs, IP addresses, or hostnames, with the following guidelines:
  - For LDAP over SSL (LDAPS), always use **ldaps://**  
Example: **ldaps://192.168.4.170:636**  
Port 636 is the default for LDAPS.
  - For secure TLS, do not use **ldaps://** in front of the IP address or hostname. If no port is specified, the default port 389 is used.

Example: 192.168.4.170

- Use StartTLS: Check this box only if you are using TLS. If checked, the server is required to support STARTTLS. An LDAP connection on port 389 will be an encrypted connection.
  - LDAP DN: Base DN of the LDAP server.
  - LDAP Scope: Choose one of the following from the drop-down list:
    - base - Search is performed only in the base entry.
    - one - Search is performed only on the children of the base entry.
    - sub - Search is performed on the base and all of its subordinates.
  - Bind Username: Username for LDAP bind.
  - Bind User Password: Password for the Bind Username.
4. Click **Save**.

## Adding the Certificate to Secure LDAP SSL or LDAP TLS Backend

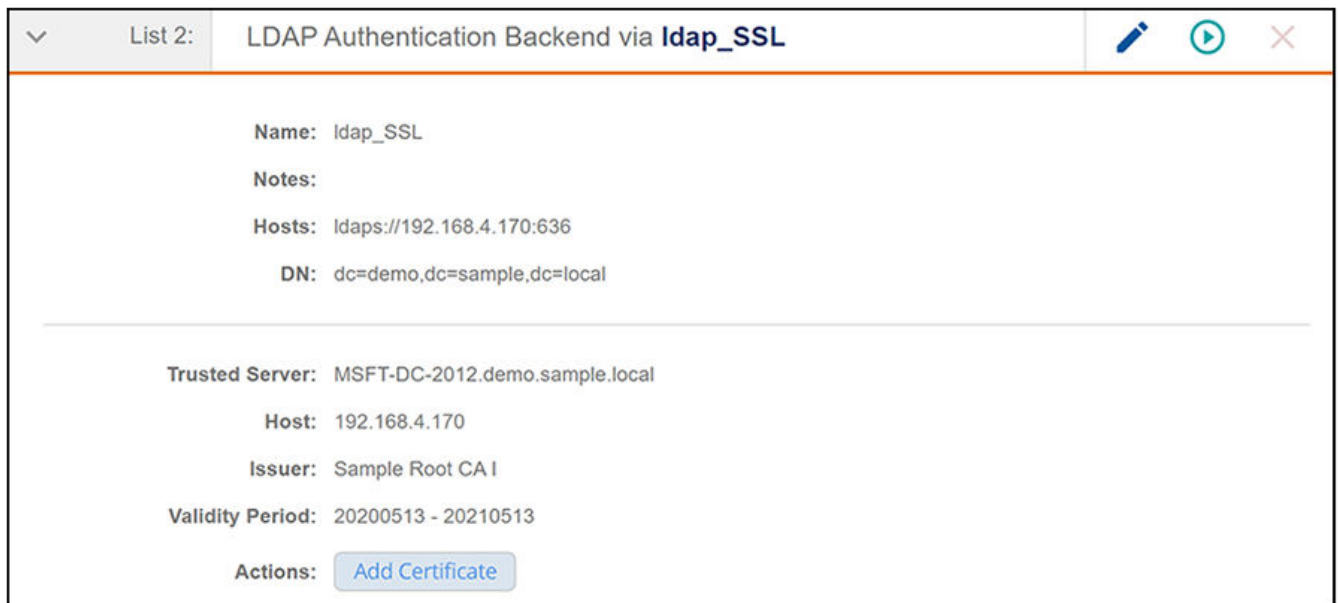
Once you save the LDAP backend, you are returned to the main Authentication Backends screen. If you configured a secure backend (as shown in the SSL example in [Figure 5](#)), you now must add the certificate:

### NOTE

If you are not using a secure LDAP, you can proceed to the next section.

1. Expand the arrow next to the secure LDAP to invoke the full view of the backend configuration:

**FIGURE 6** Backend Configuration From Which You Add the Certificate



2. Click **Add Certificate**.
3. On the ensuing screen, chose to "Pin the Certificate" and click **Save**.

## Testing the LDAP Authentication

After you have added an LDAP backend (and the certificate if applicable), you can test the interaction with the backend by following the steps below:

1. Click the green arrow for the LDAP backend you wish to test.
2. In the ensuing screen, enter credentials for a user to verify interaction with the LDAP authentication backend, then click **Continue**.
3. Check the results on the ensuing screen, an example of which is shown below.

**FIGURE 7** Authentication Test Results

```
TACACS+ LDAP Authentication testing ...

Starting MP5J
Request: /admin/tacacs/authenticationServers/2/testTacacs

Input attribute-value-pairs:
TYPE          TACPLUS
TIMESTAMP     mavistest-6231-1609280010-0
USER          ray@arris.com
PASSWORD      test
TACTYPE       AUTH

Output attribute-value-pairs:
TYPE          TACPLUS
TIMESTAMP     mavistest-6231-1609280010-0
USER          ray@arris.com
RESULT        ACK
PASSWORD      test
SERIAL        ISKIKY6wwEFXINLeDYA+dQ=

Elapsed Time: 425
```

The "Result" field near the bottom of the screen can yield the following values:

**TABLE 3** Possible Values for the "Result" field

"Result" Field Value	Meaning
ERR	LDAP connection error.  <b>NOTE</b> If you receive an error, check the following: <ul style="list-style-type: none"><li>• Use diagnostic tools (go to <b>Support &gt; Diagnostics</b>) to ensure that you can successfully ping and perform a DNS Lookup on the LDAP backend.</li><li>• Check your firewall requirements (go to <b>Administration &gt; Firewall Requirements</b>).</li></ul>
NFD	LDAP user not found.
NAK	LDAP user found, but the password is incorrect or the user is not a member of any TACACS group.
ACK	LDAP user found and successfully authenticated.

## Configuring TACACS+ Devices

You can add one or more devices that can be authenticated by the TACACS+ server.

### Configuration Steps

Follow these steps to add a device:

1. In the Cloudpath UI, go to **TACACS+ > TACACS+ Devices**.
2. Click **Add Device**.
3. Configure the values to create a TACACS+ device, as shown in the following example.

FIGURE 8 Creating a Device

TACACS+ > TACACS+ Devices > Create Tacacs Device

Cancel Save

TACACS+ Device

Device Name: icxOnly

Description: icxOnly

Device Context:

```
address = 192.168.92.244
key = "key4icxOnly"
enable 1 = crypt "ICX123"
template = deviceTemplate
prompt = "device prompt after template"
```

Sample data: Allow-All

- Device Name: A descriptive name for the device; this is used for reference when building the configuration profile. No spaces are allowed in the name.
- Description: (Optional) Description of the device.
- Device Context: Many statements are available to add. Some common ones that are shown in the example screen above are:
  - Address: An **address** statement is used to enter the host IP address of the device. In the example, the host IP address is 192.168.92.244.
  - Key: A **key** statement is used to enter the shared key between the device network and the Cloudpath system that is acting as the TACACS+ server. In the example, the shared key is: **key4icxOnly**. This string must be an exact match of the corresponding key that is configured in the AAA server configuration on the device.

**NOTE**

The value of the key must be in quotation marks.

- Enable: An **enable** statement is used to enable the password and set the privilege level. **enable** passwords may be specified at the host, user, or group level, in that order of precedence.

**Syntax for Enable statement:**

```
enable [ level ] = ( permit | deny | login | ( clear | crypt ) "password" )
```

This statement may be used to set user or group-specific **enable** passwords, to use the login password, or to permit (without password) or deny any **enable** attempt. **enable** passwords defined at the group or user level are given precedence over those defined at the host level. The default for the level is 15.

**NOTE**

The value of the password must be in quotation marks.



The default privilege level for an ordinary user on the NAS is typically 1. A user can reset this level to a value between 0 and 15 by using the **nas enable** statement. If the user does not specify a level, the default level is 15.

The **enable** statement in the example screen above sets the the privilege level to 1, and encrypts the password on the device while setting the password to **ICX123**. This is the password that is requested when logging in to the device.

- Template: A **template** statement is used to pull in another device configuration into this device configuration. In the example, the device configuration called **deviceTemplate** is being called in. **deviceTemplate** is not actually defined as a template itself; however a template statement is needed to call in another device configuration.

An example of the content contained in **deviceTemplate** is:

```
prompt = "Welcome\n"
```

This statement means that the user receives a "Welcome" message upon successful login.

- Prompt: A **prompt** statement is used to display text to the user. In the example, the string "device prompt after template" is shown for testing purposes only and should be replaced by the actual device prompt.

#### NOTE

The value of the prompt must be in quotation marks.

**Allow-All:** If you want to quickly perform a simple device configuration that allows access for any device and creates an entry for you to edit a shared-key value, click **Allow-All** in the lower-left portion of the screen to populate the Device Context field with the following values:

```
address = 0.0.0.0/0  
key = "mysecretsharedkey"
```

#### NOTE

A network address of 0.0.0.0/0 allows access to any device from anywhere.

4. Click **Save**.
5. Add and configure any additional devices. The following screen is an example of the main Devices configuration screen and its information after several device configurations have been performed.

FIGURE 9 Devices Screen Example After Adding Several Devices

	Name	Address	Host	Creation Date	Update Date
	ciscoOnly	192.168.92.10	host = ciscoOnly { address = 192.168.92.10 key = ***** prompt = "device prompt before template" enable 15 = clear ***** template = deviceTemplate}	20201214 1422 MST	20201217 1342 MST
	deviceTemplate		host = deviceTemplate { enable = clear templateSecret prompt = "Welcome\n"}	20201214 1422 MST	20201217 1340 MST
	icxOnly	192.168.92.244	host = icxOnly { address = 192.168.92.244 key = ***** enable 1 = crypt ***** template = deviceTemplate prompt = "device prompt after template"}	20201214 1424 MST	20201217 1341 MST
	smartzoneOnly	192.168.93.179	host = smartzoneOnly { address = 192.168.93.179 key = ***** enable 15 = clear ***** template = deviceTemplate}	20201214 1424 MST	20201217 1342 MST
	testdev	192.168.1.1	host = testdev { address=192.168.1.1 template = deviceTemplate}	20201214 1425 MST	20201214 1425 MST
	world	0.0.0.0/0	host = world { address = 0.0.0.0/0 key = ***** template = deviceTemplate}	20201214 1425 MST	20201214 1425 MST

## Other Actions You Can Perform From Main Device Configuration Screen

Some of the actions you can take from the main Device Configuration screen (Figure 9) include:

- Deleting a device configuration: Click the **X** in the column to the left of the name of the configuration, then confirm the deletion when prompted.

**NOTE**

A minus sign indicates that the device configuration cannot be deleted because it is being referenced by a configuration profile. You would have to first remove the configuration from the configuration profile if you want to be able to delete it from the main Device Configuration screen.

**NOTE**

The icon denotes that the configuration is being referenced by another device configuration. You would have to first remove the configuration from the device configuration if you want to be able to delete it from the main Device Configuration screen.

- Editing a device configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Configuring Time Ranges

You can add one or more time ranges (called time specs in the UI) to your TACACS+ configuration. Time specs allow you to further manage control of the various devices that can use the TACACS+ server by applying time specs to access control lists (ACLs).

### Configuration Steps

Follow these steps to add a time spec:

1. In the Cloudpath UI, go to **TACACS+ > Access Control** .
2. Highlight the **Time Specs** tab.
3. Click **Add Time Spec**.
4. Configure the values to create a the time spec, as shown in the following example.

**FIGURE 10** Creating a Time Spec

The screenshot shows a web form titled "TACACS+ > Access Control > Create Tacacs Timespec". At the top right are "Cancel" and "Save" buttons. The form contains three input fields, each with an information icon (i) to its left:

- Timespec Name:** A text input field containing the value "workinghours".
- Description:** A text input field containing the value "workinghours".
- Timespec context:** A text area containing the value: `** 8-22 14-23 Dec 1-5* # or: ** 8-17 14-23 Dec-Jan Mon-Fri`  
`** 8-12 ** 6* # or: ** 8-12 *** Sat*`

- **Timespec Name:** A descriptive name for the time spec; this is used for reference when building the configuration profile or an access control list. No spaces are allowed in the name.
- **Description:** (Optional) Description of the time spec.
- **Timespec Context:** Declaration that may be used for time-based profile assignments.

#### NOTE

Both cron and Taylor-UUCP syntax are supported. Refer to publicly available documentation for more information on how to use these formats.

5. Click **Save**.
6. Add and configure any additional time specs. The following screen is an example of the main Timespec configuration screen and its information after several time specs have been configured.

#### NOTE

You can reference one or more configured time specs when you configure access control lists.

FIGURE 11 Time Specs Screen Example After Adding Several Time Specs



## Other Actions You Can Perform From Main Timespec Configuration Screen

Some of the actions you can take from the main Time Spec Configuration screen (Figure 11) include:

- Deleting a time spec configuration: Click the X in the column to the left of the name of the configuration, then confirm the deletion when prompted.

### NOTE

A minus sign (not shown in the above example screen) indicates that the configuration cannot be deleted because it is being referenced by a configuration profile. You would have to first remove the time spec from the configuration profile (and remove any corresponding ACLs from the profile as well) if you want to be able to delete the time spec from the main Time Spec Configuration screen.

### NOTE

The icon denotes that the time spec configuration is being referenced with the use of a **time** statement by an ACL configuration. You would have to first remove the corresponding **time** statement from the ACL configuration if you want to be able to delete the time spec configuration from the main Time Spec Configuration screen.

- Editing a time spec configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Configuring Access Control Lists

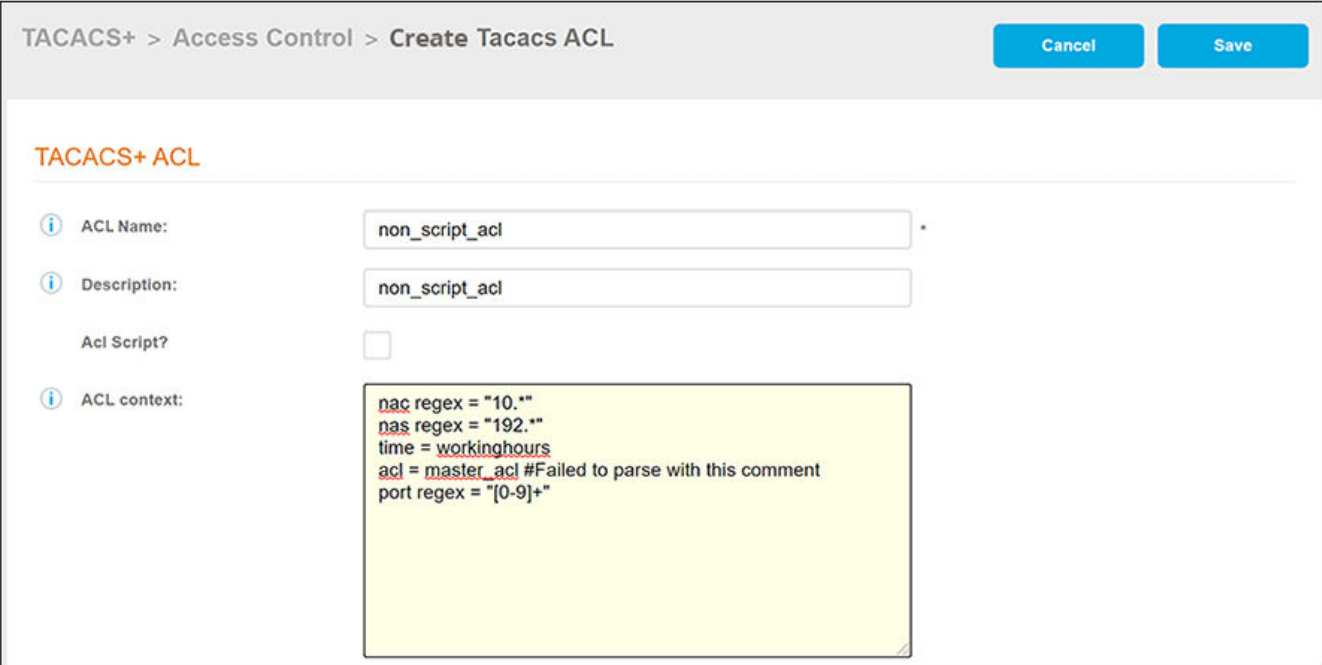
You can add one or more access control lists (ACLs) to your TACACS+ configuration. ACLs allow you to further manage control of the various devices that can use the TACACS+ server by applying ACLs to user groups and individual users.

### Configuration Steps

Follow these steps to add an ACL:

1. In the Cloudpath UI, go to **TACACS+ > Access Control**.
2. Highlight the **Access Control Lists** tab.
3. Click **Add ACL**.
4. Configure the values to create an ACL, as shown in the following example.

**FIGURE 12** Creating an ACL



The screenshot shows the 'TACACS+ > Access Control > Create Tacacs ACL' form. It has 'Cancel' and 'Save' buttons in the top right. The form title is 'TACACS+ ACL'. It contains the following fields:

- ACL Name:** non\_script\_acl
- Description:** non\_script\_acl
- Acl Script?:**
- ACL context:**

```
nac regex = "10.*"  
nas regex = "192.*"  
time = workinghours  
acl = master_acl #Failed to parse with this comment  
port regex = "[0-9]+"
```

- **ACL Name:** A descriptive name for the ACL; this is used for reference when building the configuration profile. No spaces are allowed in the name.
- **Description:** (Optional) Description of the ACL.
- **ACL Script?:** This box should be checked if the ACL is a script.
- **ACL Context:** You can add the access control expressions (ACEs) you desire to build the ACL. The following list describes the ACEs that are shown in the example screen above:
  - nac regex = "10.\*" - Network Access Client (NAC) device IP address begins with "10."

#### NOTE

A network access client is the source host of a telnet connection.

- nas regex = "192.\*" - Network Access Server (NAS) device whose IP address begins with "192."

**NOTE**

A network access server, such as a Cisco box, makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets.

- time = workinghours - Client attempting to connect must do so during the time period allowed in the time spec called *workinghours* configured in the Time Specs tab.
- acl = master\_acl - The ACL called "master\_acl" is being called in.
- port regex = "[0-9]+" - Can be any port number; port is used to access the device.

5. Click **Save**.

6. Add and configure any additional ACLs. The following screen is an example of the main ACL configuration screen and its information after several ACLs have been configured.

**NOTE**

You can reference one or more configured ACLs when you configure user groups or individual users.

**FIGURE 13** Services Screen Example After Adding Several ACLs

	Name	Access Control List	Creation Date	Update Date
	master_acl	acl = master_acl { nas = 192.168.0.0/16}	20201214 1426 MST	20201214 1426 MST
	non_script_acl	acl = non_script_acl { nac regex = "10.*" nas regex = "192.*" time = workinghours acl = master_acl #Failed to parse with this comment port regex = "[0-9]+"}.	20201214 1427 MST	20201214 1657 MST
	script_acl	acl script = script_acl { if ( nac == 192.168.4.237 ) deny}	20201214 1427 MST	20201214 1427 MST

## Other Actions You Can Perform From Main ACL Configuration Screen


Some of the actions you can take from the main ACL Configuration screen (Figure 13) include:

- Deleting an ACL configuration: Click the **X** in the column to the left of the name of the configuration, then confirm the deletion when prompted.

**NOTE**

A minus sign indicates that the configuration cannot be deleted because it is being referenced by a configuration profile. You would have to first remove the ACL from the configuration profile if you want to be able to delete it from the main ACL Configuration screen.

**NOTE**

The  icon denotes that the ACL configuration is being referenced with the use of an `acl` statement by either a user group, individual-user configuration, or another ACL. You would have to first remove the corresponding `acl` statement from the applicable configuration if you want to be able to delete the ACL configuration from the main ACL Configuration screen.

- Editing an ACL configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Configuring TACACS+ Services

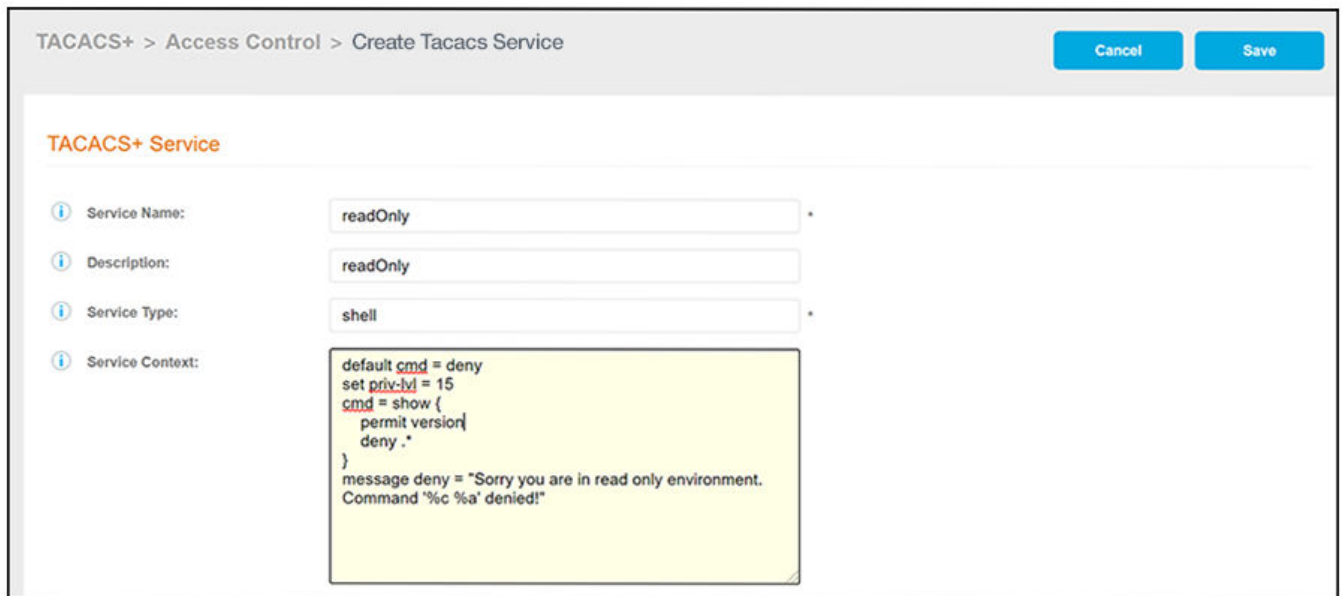
A service allows you to define a set of access rules (such as privilege levels and accessible commands) that can then be assigned to user groups or specific users.

### Configuration Steps

Follow these steps to add a service to your TACACS+ configuration:

1. In the Cloudpath UI, go to **TACACS+ > TACACS+ Services**.
2. Click **Add Service**.
3. Configure the values to create a TACACS+ service, as shown in the following example.

**FIGURE 14** Creating a Service



TACACS+ > Access Control > Create Tacacs Service

**TACACS+ Service**

Service Name: readOnly

Description: readOnly

Service Type: shell

```
default cmd = deny
set priv-lvl = 15
cmd = show {
  permit version|
  deny .*
}
message deny = "Sorry you are in read only environment.
Command '%c %a' denied!"
```

- Service Name: A descriptive name for the service; this is used for reference when building the configuration profile. No spaces are allowed in the name.
- Description: (Optional) Description of the service.

- Service Type: The default is "shell," which gives EXEC service. Other allowed values include "ppp" for PPP, and "junos-exec" for a Juniper Networks-specific authorization service.

#### NOTE

For an ICX switch, always use the service type **shell**.

- Service Context: You can add the entries you desire to build the service. The following list describes the entries that are shown in the example screen above:

- default cmd: A **default cmd** statement is used specify whether or not to accept or reject commands that are not explicitly permitted. In the example, commands will be denied by default.
- set priv-lvl: A **set priv-lvl** statement is used to set the privilege level for the EXEC commands. In this example, the privilege level is set to 15. The allowed range for the privilege level is 0-15; Level 1 is for normal user EXEC mode privileges.

The statement for setting a privilege level for a RUCKUS ICX switch is **set foundry-privlvl** instead of **set priv-lvl**. However, if you use the **set priv-lvl statement** for a RUCKUS ICX switch, Cloudpath automatically translates the privilege value to the corresponding level for an ICX switch, as shown in the table below.

**TABLE 4** Privilege Level Translation for RUCKUS ICX Switches

Value for "set priv-lvl" for Connecting to ICX	RUCKUS Privilege Level (ICX)
15	0 (super-user)
14-1	4 (port-config)
0	5 (read-only)

#### Examples:

- › The statement **set priv-lvl 15** for a user who connects to an ICX switch will be given a privilege level of 0 (super user) on the ICX switch.
- › The statement **set priv-lvl 0** for a user who connects to an ICX switch will be given a privilege level of 5 (read-only) on the ICX switch.
- › The statement **set foundry-privlvl 0** for a user who connects to an ICX switch will be given a privilege level of 0 (super user) on the ICX switch, but in this case Cloudpath would not need to translate the value because the ICX syntax was used to set the privilege level.
- cmd: A **cmd** statement can be used to explicitly list commands that this service will allow the user to run. In the example, the statement shown is:

```
cmd = show {
    permit version
    deny .*
}
```

- message deny: This statement can be used to provide a message to the user when a command is denied. In the example, the user will be presented with the following message:

```
Sorry you are in read only environment. Command '%c %a' denied!
```

#### NOTE

'%c %a' are variables that will be expanded within the device.











4. Click **Save**.
5. Add and configure any additional services. The following screen is an example of the main Services configuration screen and its information after several services have been configured.



**NOTE**

You can reference one or more configured services when you configure user groups or individual users. The group and user configuration screens have a drop-down menu from which you can select configured services.

**FIGURE 15** Services Screen Example After Adding Several Services

+	Name	Service	Creation Date	Update Date
 	genericGroupShell	service = shell { set priv-lvl = 15 default attribute = permit default cmd = permit }	20201214 1435 MST	20201214 1435 MST
 	readOnly	service = shell { default cmd = deny set priv-lvl = 15 cmd = show { permit version deny .* } } message deny = "Sorry you are in read only environment. Command '%c %a' denied!"	20201214 1433 MST	20201214 1433 MST
 	tacuserShell	service = shell { default cmd = deny set priv-lvl = 15  #Allow to run configure command cmd = configure { # can run all configure commands permit .* }  #Allow to run cd command cmd = cd { # can run the following show command permit .* }} }	20201214 1435 MST	20201214 1435 MST
 	usr1ciscoShell	service = shell { default cmd = deny set priv-lvl = 15 #Only allow to run show commands cmd = show { # can run all show command permit .* }} }	20201214 1432 MST	20201216 1236 MST
 	vszService	service = super-admin { set priv-lvl = 1 }	20201214 1431 MST	20201214 1431 MST

## Other Actions You Can Perform From Main Services Configuration Screen

Some of the actions you can take from the main Services Configuration screen (Figure 15) include:

- Deleting a services configuration: Click the X in the column to the left of the name of the configuration, then confirm the deletion when prompted.

**NOTE**

A minus sign indicates that the services configuration cannot be deleted because it is being referenced by from the Services drop-down list in either a group or user configuration. You would have to first remove the reference from the applicable group or user configuration if you want to be able to delete it from the main Services Configuration screen.

- Editing a service configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Configuring TACACS+ Groups

You can add one or more user groups to your TACACS+ configuration.

A group that you configure for TACACS+ must also be configured in LDAP. Any users that belong to that group in LDAP will then be granted the permissions that you assign to the group during TACACS+ group configuration. Therefore, you do not need to define users in the TACACS+ configuration that are part of an LDAP group.

### Configuration Steps

Follow these steps to add a group:

1. In the Cloudpath UI, go to **TACACS+ > TACACS+ Users**.
2. Highlight the **Groups** tab.
3. Click **Add Group**.
4. Configure the values to add a TACACS+ group, as shown in the following example.

**FIGURE 16** Creating a Group

TACACS+ > TACACS+ Users > Create Tacacs Group

Cancel Save

TACACS+ Group

Group Name: ICX

Description: ICX

Group Context: `acl = non_script_acl`  
`enable = login`  
`login = crypt icxPass`  
`template = groupTemplate`

Assign Service to Group: Assign Services to the group.  
genericGroupShell

- **Group Name:** A descriptive name for the group. No white spaces are allowed in the group. If an LDAP authentication backend is specified and used for external authentication in the configuration, the group name must match the name of the group configured in the LDAP active directory. Restricted characters in the group name include # + " < > [ ] \* ,
- **Description:** (Optional) Description of the group.
- **Group Context:** Configure the values to create a TACACS+ group. The following list describes the entries that are shown in the example screen above:
  - `acl`: You can use an `acl` statement to pull an already-configured ACL into the group. In the example, an ACL called `non_script_acl` is being referenced.
  - `enable = login`: Users will need to re-enter their AD password for the **enable** password.

- login: You can use a **login** statement to set and enable a group password. A **login** statement is needed only if an LDAP authentication backend is not being used for external authentication. In this example (see screen above), users in the group are enabled to log in to the devices with the group password *icxPass*. If an LDAP authentication backend is specified and is being used for external authentication, users in the group are enabled to log in to the devices and be authenticated with their own LDAP credentials.
  - template: You can use a **template** statement to call in another group configuration that was created with the intention of being used as a template. In this example, a group configuration called "groupTemplate" is being referenced and will therefore be called into the configuration at the exact point in which it is being referenced.
5. Assign Service to Group: A drop-down list from which you select one of the configured services to be associated with this group. You can add additional services to the group by clicking the + button and selecting another service.

**NOTE**

You can also define a service (locally) by using a **service** statement within the Group context field of the Group configuration screen.

6. Click **Save**.
7. Add and configure any additional groups. The following screen is an example of the main Group configuration screen and its information after several groups have been configured.

**NOTE**

When you add your configuration profiles, you will be able to select any or all of the groups you have configured to be part of a specific profile.

**FIGURE 17** Group Screen Example After Adding Several Groups

Group				
	Name	Group	Creation Date	Update Date
	admin	group = admin { template = groupTemplate login = clear ***** service = shell { set priv-lvl = 15 } default attribute = permit default cmd = permit})	20201214 1438 MST	20201217 1307 MST
	cisco	group = cisco { acl=non_script_acl login = crypt ***** template=groupTemplate  service = shell { set priv-lvl = 15 } default attribute = permit default cmd = permit})	20201214 1440 MST	20201217 1309 MST
	groupTemplate	group = groupTemplate { default service = permit enable = login login = clear ***** login = crypt *****})	20201214 1438 MST	20201217 1327 MST
	ICX	group = ICX { acl = non_script_acl pap = crypt ***** template=groupTemplate service = shell { set priv-lvl = 15 } default attribute = permit default cmd = permit})	20201214 1441 MST	20201217 1309 MST
	smartzone	group = smartzone { acl = non_script_acl pap = clear ***** template=groupTemplate service = shell { set priv-lvl = 15 } default attribute = permit default cmd = permit})	20201214 1442 MST	20201217 1308 MST
	tempray1	group = tempray1 { enable = clear ***** login = clear *****})	20201216 1411 MST	20201216 1411 MST

## Other Actions You Can Perform From Main Group Configuration Screen


Some of the actions you can take from the main Group Configuration screen (Figure 17) include:

- Deleting a group configuration: Click the **X** in the column to the left of the name of the configuration, then confirm the deletion when prompted.

### NOTE

A minus sign indicates that the group configuration cannot be deleted because it is being referenced by a configuration profile. You would have to first remove the configuration from the configuration profile if you want to be able to delete it from the main Group Configuration screen.

### NOTE

The  icon denotes that the configuration is being referenced by a **template** statement from another group configuration. You would have to first remove the **template** statement from the applicable group configuration if you want to be able to delete the configuration from the main Group Configuration screen.

- Editing a group configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Configuring TACACS+ Users

You can add one or more users to your TACACS+ configuration. The reason to add individual users would be if the users do not belong to a group that already exists in your LDAP server.

### Configuration Steps

Follow these steps to add a user:

1. In the Cloudpath UI, go to **TACACS+ > TACACS+ Users**.
2. Highlight the **Users** tab.
3. Click **Add User**.
4. Configure the values to add a TACACS+ user, as shown in the following example.

FIGURE 18 Creating a User

The screenshot shows the 'Create Tacacs User' form in the Cloudpath Administration UI. The breadcrumb navigation at the top reads 'TACACS+ > TACACS+ Users > Create Tacacs User'. There are 'Cancel' and 'Save' buttons in the top right corner. The form contains the following fields:

- User Name:** jeff
- Description:** Jeff R
- User Context:** default service = permit, enable = login, login = clear jeffPass, #member = admin
- Assign Service to User:** readOnly (with a dropdown arrow and a red X icon to the right, and a blue plus icon below it)

At the bottom left, there is a 'Sample data' section with links for 'ICX-Read-Only', 'ICX-Port-Control', and 'ICX-Super-User'.

- **User Name:** A descriptive name for the user; this is used for reference when building the configuration profile. No spaces are allowed in the name. Restricted characters in the name include # + " < > [ ] \* ,
- **Description:** (Optional) Description of the user.
- **User Context:** Configure the values to create a TACACS+ user. The following list describes the entries that are shown in the example screen above:
  - **default service:** You can use the **default service** statement to either permit or deny a service that is not explicitly defined in the user profile. In the example screen above, such services will be permitted.

**NOTE**

You can create a service statement here within the User Context. You do not necessarily need to pre-define it in the **TACACS+ > Services** portion of the UI.

- **enable:** **enable = login** grants enable mode upon successful user login. This omits the secondary password query and allows the user to enter enable mode with the login password, or permit an anonymous enable.
- **login:** You can use a **login** statement to set the user password and choose whether or not to encrypt it. In the example, the password is set to "jeffPass" and the **clear** option denotes to not encrypt this password.

**Sample data:** You can quickly populate the User Context field by clicking any of the "Sample data" options in the lower-left portion of the screen. Each option is named according to what function it will provide to the user. You can click each option to view the statements each provides.

5. **Assign Service to User:** A drop-down list from which you select one of the configured services to be associated with this user. You can add additional services to the user by clicking the + button and selecting another service.

**NOTE**

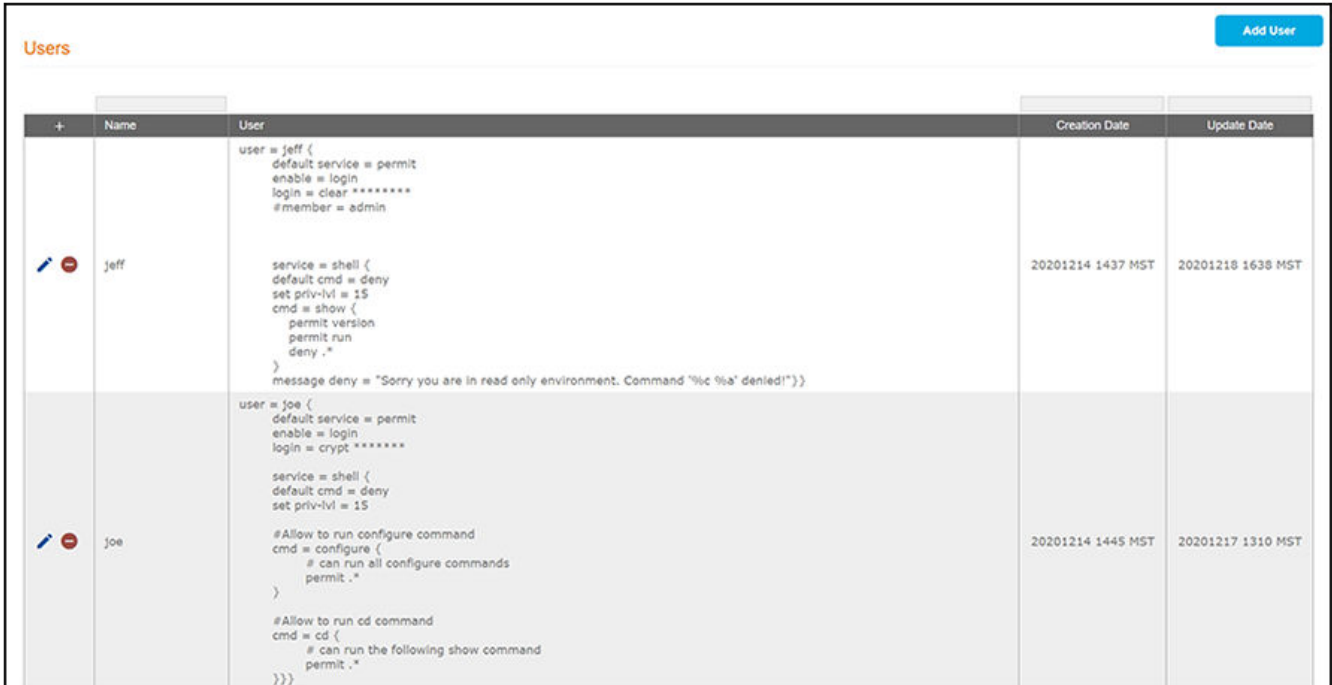
You can also define a service (locally) by using a **service** statement within the User context field of the User configuration screen.


6. Click **Save**.
7. Add and configure any additional users. The following screen is an example of the main Users configuration screen and its information after several users have been configured.

**NOTE**

When you add your configuration profiles, you will be able to select any or all of the users you have configured to be part of a specific profile.

**FIGURE 19** Users Screen Example After Adding Several Users



	Name	User	Creation Date	Update Date
 	jeff	<pre>user = jeff {   default service = permit   enable = login   login = clear *****   #member = admin    service = shell {     default cmd = deny     set priv-lvl = 15     cmd = show {       permit version       permit run       deny .*     }   }   message deny = "Sorry you are in read only environment. Command '%c %s' denied!"; }</pre>	20201214 1437 MST	20201218 1638 MST
 	joe	<pre>user = joe {   default service = permit   enable = login   login = crypt *****    service = shell {     default cmd = deny     set priv-lvl = 15      #Allow to run configure command     cmd = configure {       # can run all configure commands       permit .*     }   }    #Allow to run cd command   cmd = cd {     # can run the following show command     permit .*   } }</pre>	20201214 1445 MST	20201217 1310 MST

## Other Actions You Can Perform From Main Users Configuration Screen

Some of the actions you can take from the main Users Configuration screen (Figure 19) include:

- Deleting a user configuration: Click the **X** in the column to the left of the name of the configuration, then confirm the deletion when prompted.

**NOTE**

A minus sign indicates that the user configuration cannot be deleted because it is being referenced by a configuration profile. You would have to first remove the configuration from the configuration profile if you want to be able to delete it from the main User Configuration screen.

- Editing a user configuration: Click the pencil icon in the column to the left of the name of the configuration, then make and save any edits in the ensuing screen.

## Creating Configuration Profiles

A configuration profile acts as a set of definitions that instruct the TACACS+ server how to manage users and devices. Such a profile contains any combination of already configured TACACS+ server entities, such as authentication backends, devices, groups and users, and so on.

### Configuration Steps

You can add one or more configuration profiles to your TACACS+ configuration. However, only one profile can be in effect at any given time.

Follow these steps to add a configuration profile:

1. In the Cloudpath UI, go to **TACACS+ > TACACS+ Configuration Profiles**.
2. Highlight the **Configuration Profiles** tab.
3. Click **Add Configuration Profile**.
4. The following screen shots each show a portion of the Configuration Profile screen, along with descriptions and examples for each field.

**FIGURE 20** Configuration Profiles: Display Name and LDAP Backend

The screenshot shows the 'Create Configuration Profile' screen in the Cloudpath Administration UI. The breadcrumb navigation at the top reads 'TACACS+ > Configuration Profiles > Create Configuration Profile'. There are 'Cancel' and 'Save' buttons in the top right corner. The main heading is 'TACACS+ Configuration Profile'. Below this, there are three input fields: 'Profile Name' with the value 'allDevices', 'Description' with the value 'allDevices', and 'Listening Port' with the value '49'. Below these fields, there is a section for 'LDAP Authentication Backend' with the text 'Add LDAP Authentication Backend to the configuration profile.' and a dropdown menu showing 'LDAP SSL'. A blue plus sign is visible below the dropdown menu.

- Profile Name: A descriptive name for the the configuration profile. No spaces are allowed in the name. In this example, the profile is named "allDevices" because it will be used to provide access to all devices that have been configured for TACACS+ server authentication.
- Description: (Optional) Description of the configuration profile.
- Listening Port: TCP port number to use when connecting to the TACACS+ daemon. The default port is 49.

- LDAP Authentication Backend: Drop-down list from which you can select an already configured LDAP authentication backend to apply to this configuration profile. Any user groups that you want to allow access to any of the configured devices must exist in the LDAP server selected.

FIGURE 21 Configuration Profiles: Devices, Timespecs, and ACLs

The screenshot shows a configuration interface for TACACS+ profiles. It is divided into three main sections:

- TACACS+ Devices:** Labeled "Add Devices to the configuration profile." It contains a list of four items: "deviceTemplate", "smartzoneOnly", "icxOnly", and "ciscoOnly". Each item has a dropdown arrow and a red "X" icon to its right. A blue "+" icon is located below the list.
- TACACS+ Timespec:** Labeled "Add Timespecs to the configuration profile." It contains a list of two items: "workinghours" and "sundayOnly". The "sundayOnly" item is highlighted in yellow. Each item has a dropdown arrow and a red "X" icon. A blue "+" icon is located below the list.
- Access Control Lists (ACL):** Labeled "Add Access Control Lists to the configuration profile." It contains a list of three items: "master\_acl", "non\_script\_acl", and "script\_acl". Each item has a dropdown arrow and a red "X" icon. A blue "+" icon is located below the list.

- Tacacs Devices: Drop-down lists from which you select already-configured devices to apply to this configuration profile. You can add additional devices by clicking the + button and selecting another device.

**NOTE**

If you are adding a device template to this list, and you want that template to be applied to all devices, you must select the template in the first drop-down, as shown in the example with "deviceTemplate."

- Tacacs Timespec: Drop-down lists from which you select one or more time specs that were already configured in the **TACACS+ > Access Control** area of the UI to apply to this configuration profile. You can add additional time specs by clicking the + button and selecting another time spec.

**NOTE**

Any time specs that are referenced by a **time** statement from an ACL configuration must be selected from the Timespec drop-down list (unless the ACL itself will not be part of the configuration profile). Otherwise, an error message will result.

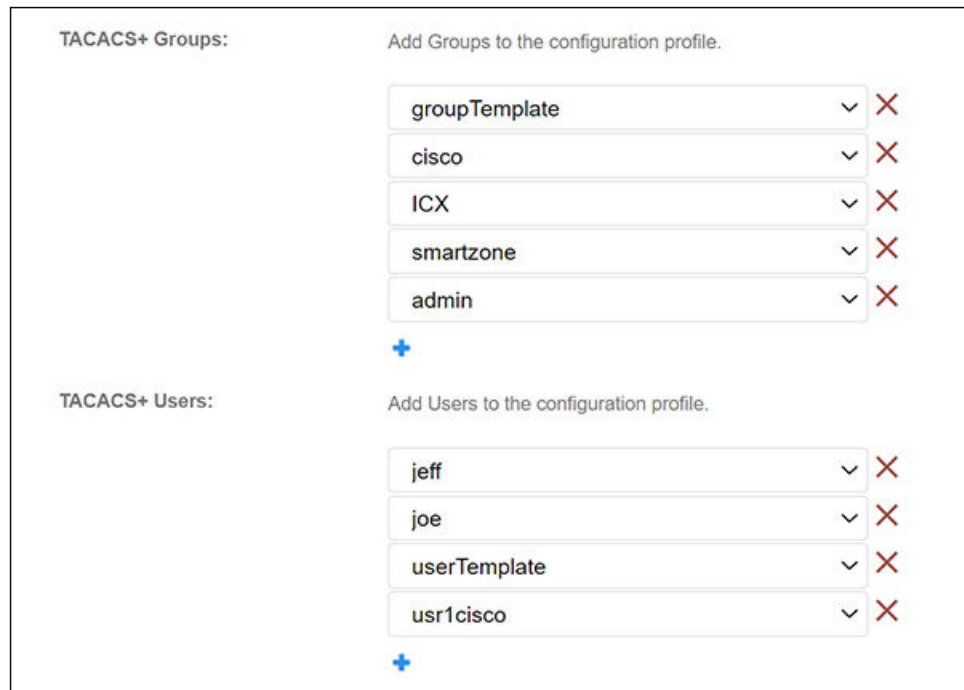
- Access Control Lists (ACL): Drop-down lists from which you select one or more ACLs that were already configured in the **TACACS+ > Access Control** area of the UI to apply to this configuration profile. You can add additional ACLs by clicking the + button and selecting another ACL.



**NOTE**

Any ACLs that are referenced by an **acl** statement from a group or user configuration must be selected from the ACL drop-down list (unless the group or user itself will not be part of the configuration profile). Otherwise, an error message will result. Any ACLs that are referenced by an **acl** statement from different ACLs must be selected prior to the selections of the ACLs referencing them.

**FIGURE 22** Configuration Profiles: Groups and Users



- Tacacs Groups: Drop-down list from which you select groups that were already configured in the **TACACS+ > Users** area of the UI to apply to this configuration profile. You can add additional groups by clicking the + button and selecting another group.

**NOTE**

If you are adding a group template to this list, and you want that template to be applied to all groups, you must select the template in the first drop-down, as shown in the example with "groupTemplate."

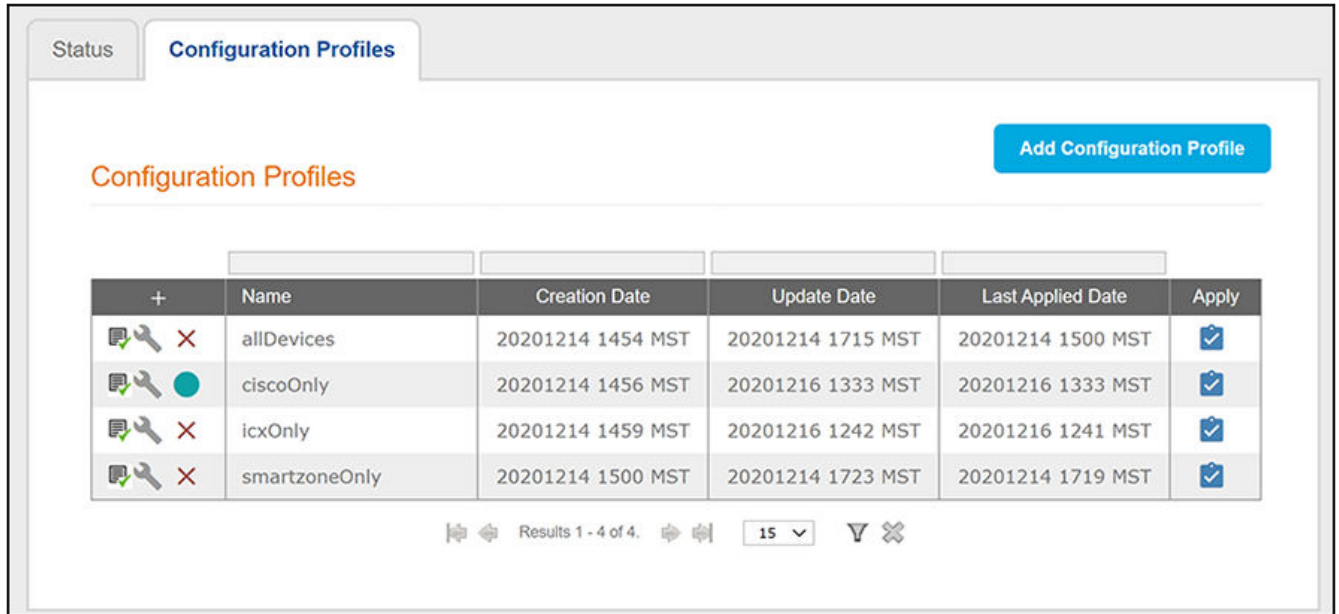
- Tacacs Users: Drop-down list from which you select users that were already configured in the **TACACS+ > Users** area of the UI to apply to this configuration profile. You can add additional users by clicking the + button and selecting another user.

**NOTE**

You only need to add individuals users who are not part of one of the groups in the configuration profile.

5. Click **Save**.
6. Add and configure any additional configuration profiles. The following screen is an example of the main Configuration Profiles screen and its information after several configuration profiles have been created.

FIGURE 23 Configuration Profiles Screen Example After Adding Several Configuration Profiles



## Verifying a Configuration Profile

To verify that a configuration profile is set up properly, such as making sure that all necessary components (time specs, ACLs, devices, and so on) have been added to the profile, click the icon. If successful, the following message will be displayed:

Configurations have been verified.

Following that message is the complete configuration file that has been generated by all the information you entered to create the profile. A portion of this file - the time specs and ACLs - is shown below as an example.

```
timespec = workinghours {
    "* 8-22 14-23 Dec 1-5" # or: "* 8-17 14-23 Dec-Jan Mon-Fri"

    "* 8-12 * * 6" # or: "* 8-12 * * * Sat"
}

acl = master_acl {
    nas = 192.168.0.0/16}

acl = non_script_acl {
    nac regex = "10.*"

    nas regex = "192.*"

    time = workinghours

    acl = master_acl #Failed to parse with this comment

    port regex = "[0-9]+"}

acl script = script_acl {
    if ( nac == 192.168.4.237 ) deny}
```

In the above example the timespec called "workinghours" has been referenced by the ACL called "non\_script\_ACL" with the statement: **time = workinghours**


If workinghours was not selected from the TACACS+ Timespec drop-down, the verification would fail with the following message:

```
Invalid Configurations: Line 70: timespec 'workinghours' not found
```

Therefore, it is strongly recommended to verify your configuration profiles to be sure they return a successful verification message before you proceed further.

## Other Actions You Can Perform From Main Configuration Profiles Screen

Some of the actions you can take from the main Configuration Profiles screen (Figure 23) include:

- Deleting a configure profile: Click the **X** in the column to the left of the name of the profile, then confirm the deletion when prompted.
- Applying a configure profile: This refers to selecting only one of the existing profiles as the profile for the TACACS+ server to use at this particular time. Click the check mark (  ) next to the profile that you want applied to the TACACS+ server, then confirm this selection when prompted. A green circle to the left of the profile name indicates the profile that is currently being applied to the TACACS+ server. The currently applied configuration profile can also be referred to as the *active* profile.

### NOTE

If you edit the active configuration profile, you need to "apply" it again in order for your changes to take effect.


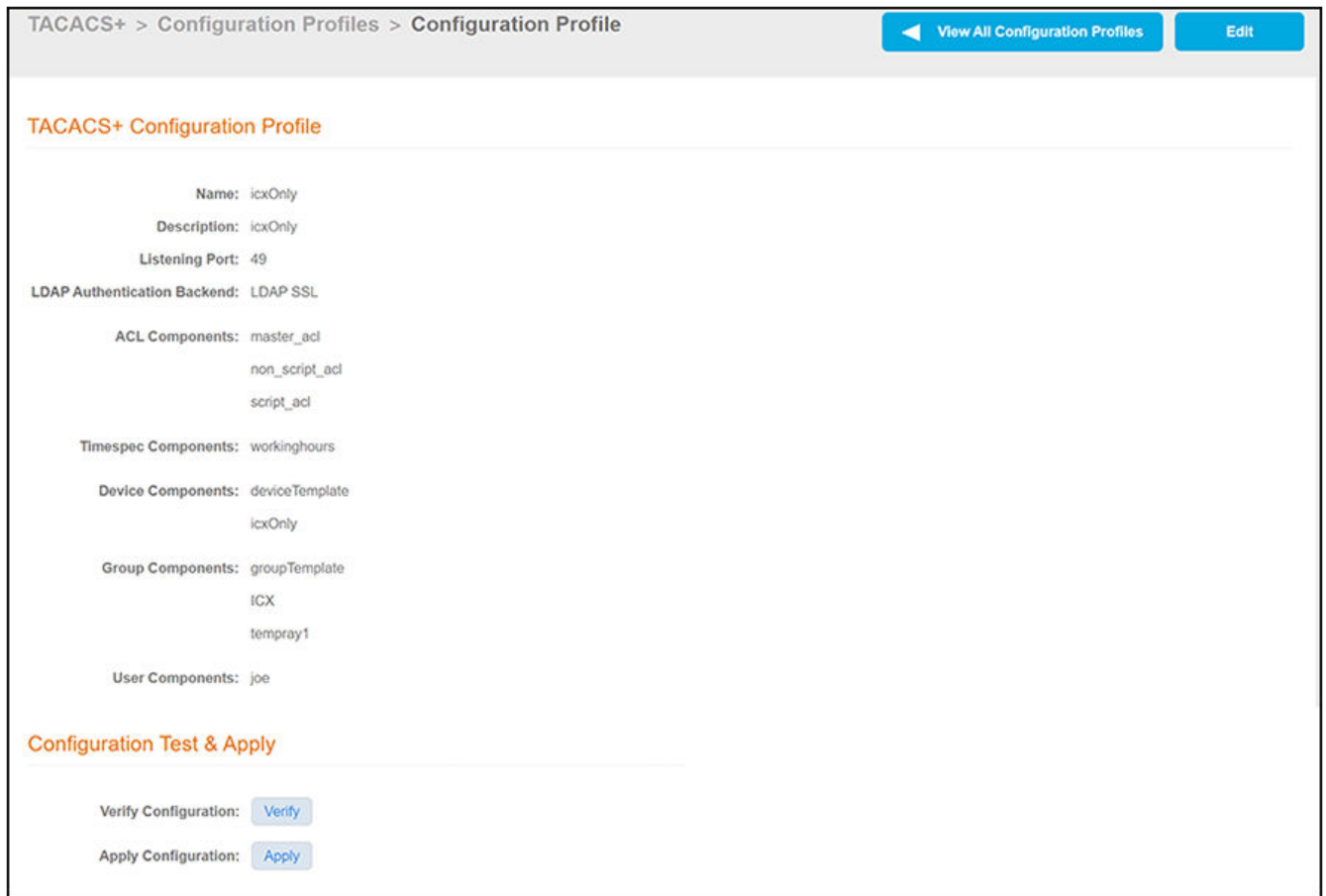
- Managing a configuration profile: Click the wrench icon (  ) to view or edit the configuration profile. The following screen is an example view of a configuration file called "icxOnly" with its currently selected components shown.

FIGURE 24 View of ICX-Only Configuration Profile Example



From the above screen, you can click **Edit** to make any desired changes to the profile.

## Testing a Configuration Profile

You can test a profile to make sure it works as you expect. For example, a few examples of ways to test the active profile could include:

- Try to log in to a device that is not part of the active profile. You should receive an error message. For example, in [Figure 23](#), the profile called "ciscoOnly" is the active file, denoted by the green circle. This profile is named accordingly because the only device selected in the profile is a Cisco device. If you tried to log in to an ICX switch while the "ciscoOnly" profile was active, you would receive an error that the login credentials are not correct.
- Try logging in to a device that is part of the active profile, but attempt to do so outside the hours of a timespec that has been applied. For example, if a "workinghours" timespec is in effect for the device, and you are attempting to log in outside of the time range specified in "workinghours," you should also be denied access.
- Try logging in to a device as a user who is part of a group that has not been added to the active profile; you should again be denied access.
- Try logging in to a device where all criteria in the profile is met, and be sure that you are successful. Then, you can test to be sure that any defined services are working as expected, such as privilege levels and permission levels. For example, if a "read-only" service has been applied, you can test to make sure that the user can only run **show** commands.

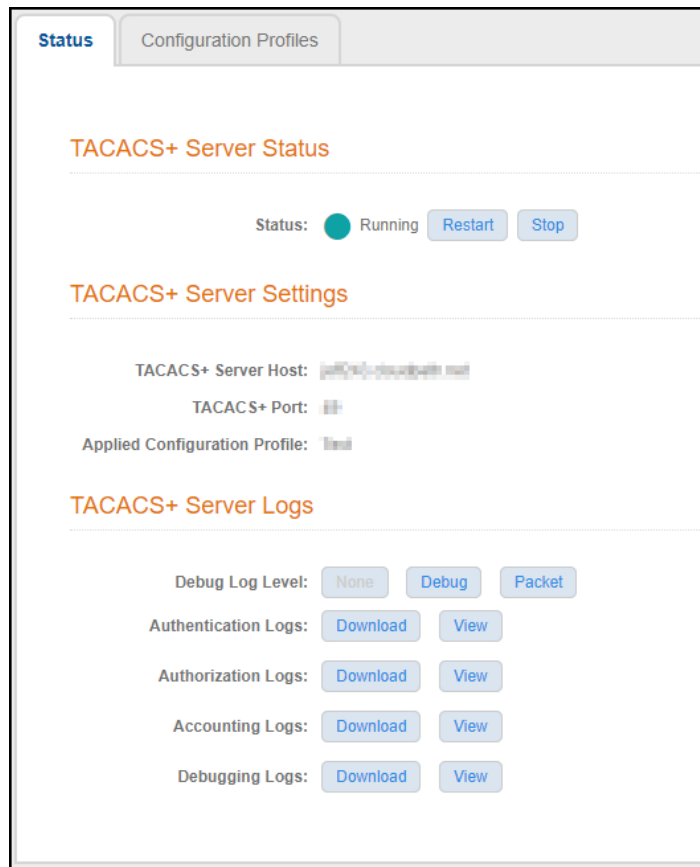
# Checking and Changing TACACS+ Server Status and Gathering Log Information

You can check the status of the TACACS+ server and gather log information in the same screen in the UI.

## Checking and Changing Status

To check the current status of the TACACS+ server, go to **TACACS+ > Configuration Profiles > Status** tab.

FIGURE 25 TACACS+ Server Status Screen



A green circle indicates that the server is running. You can use the Stop and Restart buttons as desired.

## Setting the Debug Log Level

In the TACACS+ Server Status screen, in the "Debug Log Level" field, you can select "None," "Debug", or "Packet." Packet level debugging is excluded from the original debugging levels and its logging contents are hidden from the Admin UI users.

## Configuring TACACS+ in the Cloudpath Administration UI

Checking and Changing TACACS+ Server Status and Gathering Log Information

### Gathering Log Information

In the "TACACS+ Server Logs" section of the screen, you can view and download all the logs shown in [Figure 25](#).



© 2023 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>