9920 v21.2.2.0 Security Configuration Guide

Protocols, Authentication, and Access Control Setup

9039089-00 Rev AA
October 2024

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

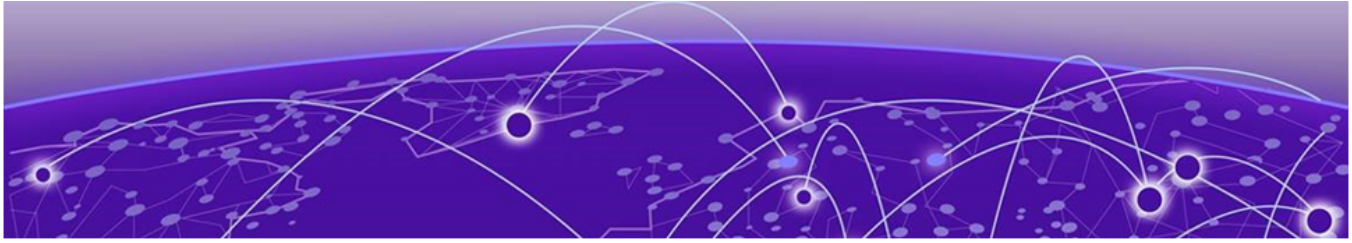
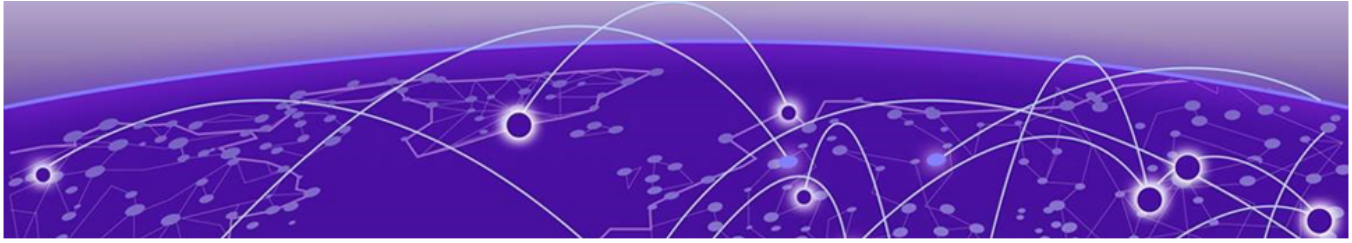


Table of Contents



Abstract

The 9920 Security Configuration Guide for version 21.2.2.0 provides comprehensive instructions for configuring and securing the 9920 platform. It covers essential security protocols, including TLS for encrypted communications, SSH for secure access, and TACACS+ for centralized authentication management. Key configurations include role-based access control (RBAC), user account management, password policies, and integration with external logging systems like Rsyslog for centralized auditing. Additional sections outline steps to secure management interfaces, configure security for IPv4 and IPv6, and implement token-based authentication. Designed for network administrators, this guide ensures the proper configuration of security features to maintain the integrity and compliance of the 9920 platform in enterprise environments.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	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, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

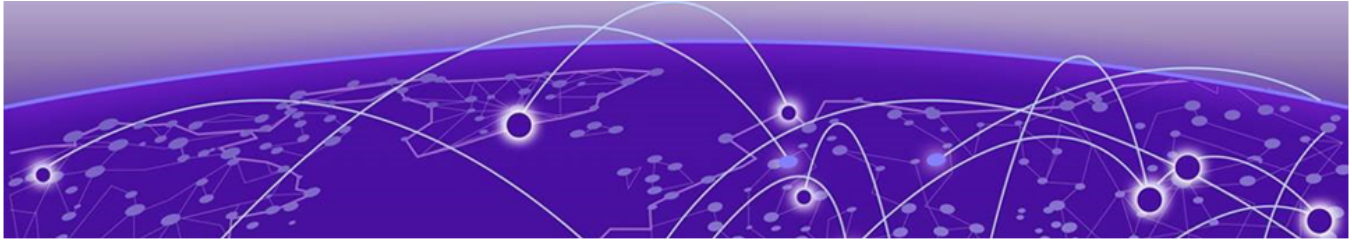
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

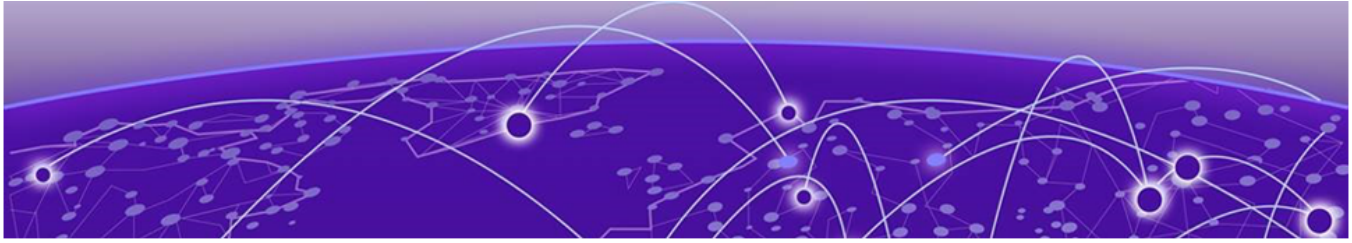
Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



What's New in This Document

There are no changes to this guide for the Extreme 9920 software, release 21.2.2.0.

For more information about this release, see the *Extreme 9920 Software Release Notes, 21.2.2.0*.



Secure Shell

Secure Shell (SSH) is a protocol that encrypts remote access connections to network devices. SSH authenticates clients or servers using encrypted shared keys (RSA/ECDSA) to access the network.

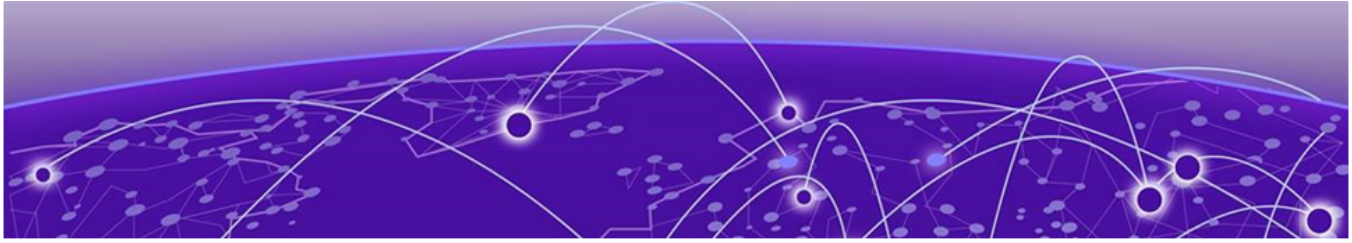
The NPB Application supports only basic SSH authentication based on username and password. A maximum of 32 SSH logins are supported. Both IPv4 and IPv6 SSH logins are supported.

SSH Server Support

- Support for SSH server is available and the device ensures RSA and ECDSA host key pairs are always available for use during SSH operation.
- Remote user authentication and locally stored usernames and passwords are supported for SSH.

Authentication Support (Local + Remote)

- SSH Authentication is supported using basic authentication (username-password) only.



User Accounts and Passwords

The NPB application uses role-based access control (RBAC) as the authorization mechanism for access to resources. A *role* is assigned to a user account and is a container for rules that specify which commands can be executed and with which permissions. When you create a user account you need to specify a role for that account. In general, *user* (as opposed to *user-level*) refers to any account—to which any role can be assigned—user or admin.

The following topics describe accounts and roles and how to configure and manage them.

Default Account Credentials

The NPB application ships with two default user accounts.

When you install the NPB application on Extreme 9920, two default user accounts are provided—**admin** and **user**—with the following case-sensitive default passwords:

- admin account password: **rocks**
- user account password: **password**

As a best practice, log on as the administrator and change the default passwords immediately after the NPB application is installed.

Predefined Accounts and Roles

The NPB application ships with two predefined accounts—**admin** and **user**. The maximum number of user accounts that you can configure is 64, including the predefined accounts.

- **admin**—Accounts with admin role access can execute all commands supported on the device.

- **user**—Accounts with user-level access have read-only permissions. User-level accounts can run the following operational CLI commands.

Table 4: User-level operational commands

Command	Action
dir	List flash files
end	End current mode and change to enable mode
exit	Exit current mode and revert to previous mode
list	Print command list
ping	Ping
quit	Exit current mode and revert to previous mode
show	Show values
terminal	Set terminal timeout parameters
traceroute	Run traceroute
The **ping** and **traceroute** commands are also supported on gNOI and accept both IPv4 and IPv6 addresses.	

User Account and Role Commands

The following tables lists the commands for configuring and displaying user account settings. For more information, see *Extreme 9920 Software Command Reference, 21.2.2.0*.

Table 5: User account and role commands

Command	Description
username <username> role <role> password <password> [encryption-level <0|10>]	Sets the role, password, and encryption level for the specified username.
show role	Displays all role information available in the system.

Account Guidelines and Limitations

Following are the guidelines and limitations for creating user accounts:

- Creating separate user accounts for each user is recommended.
- Rules for the admin or default accounts and roles cannot be modified.
- By default, all account information is stored in the device-local user database.
- By default, user authentication and tracking of logins to the device is local.

- The maximum number of accounts—including the predefined accounts—is 64. If you need more than 64 user accounts, configure Remote Server Authentication. For more information, see Remote Server Authentication on page 15.
- The maximum number of TACACS+ servers is 5.
- The maximum number of simultaneous active SSH sessions is 32.

Create a New User Account

You can create new `user` and `admin` accounts for using the NPB application.

Before You Begin

Note
Only users with `admin` roles can create new user accounts.

Note the following guidelines for creating new user accounts:

Table 6: User-account guidelines

User-defined variables	Values
username	1-40 alphanumeric characters, including underscore and dot. Underscore as first character is not allowed.
rolename	Pre-defined role to be assigned to the user ('admin' and 'user' are the only supported roles).
password	8-40 characters for plain-text password 8-128 characters for hashed passwords
encryption-level	0 = clear-text (default) 10 = encrypted

About This Task

An admin user can run all supported CLI commands. ****user role that can run all show and other basic CLI commands.

Procedure

1. Enter the Config mode.

```
device(config)#
```

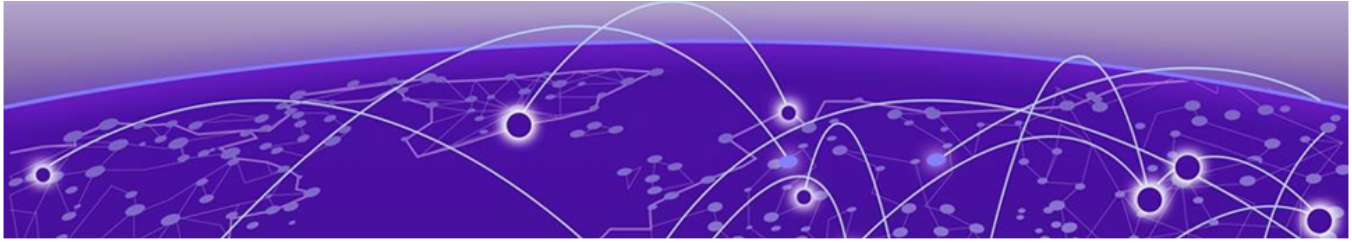
2. Create the required user account with the appropriate role.
   - `admin`
   - `user`

```
username username role rolename password password
```

Example

```
device(config)# username jdoe role user password iKt1Sas*p

device(config)# username jsmith role admin password "uber#p@ssW0^b" encryption-level 10
```



Remote Server Authentication

The NPB application supports two authentication sources to provide external Authentication and Accounting (AA) services for devices. Supported authentication sources are local and Terminal Access Controller Access-Control System Plus (TACACS+).

We recommend that you configure at least two remote AA servers to provide redundancy in the event of failure. For TACACS+, you can configure up to five external servers on the device. Each device maintains its own server configuration.

Login Authentication Mode

The login-authentication mode is defined as the order in which AA services are used on the device for user authentication during the login process. If AA login is not configured, authentication mode defaults to local authentication mode.

The NPB application supports two sources of authentication: primary and secondary. The secondary source of authentication is used in the event of primary source failure. AA login configuration is supported, with TACACS+ as primary and local-auth-fallback as secondary.

You can configure two possible sources for authentication to access the 9920 device:

- TACACS+ — Use an external TACACS+ server as the primary
- local-auth-fallback — Use the fallback local server as the secondary

If login fails through the primary source because of none of the configured servers not responding or because of login rejected by a server, failover occurs and authentication is done again through the secondary source (local).

By default, external AA services are disabled, and AA services default to the device-local user database. An environment requiring more than 64 users, including default and admin users, should adopt AA servers for user management.

Conditions for Conformance

Note the following conditions for Remote Server Authentication:

- By default, the NPB application authenticates with an internal local database.
- The source of authentication and the corresponding server type configuration are dependent on each other. At least one server must be configured before specifying that server type as a source.

Configure Login Authentication Mode

Before You Begin

- Only admin users can perform this procedure.
- The TACACS+ host must be configured on the 9920 device.

About This Task

Perform this procedure to configure TACACS+ as the primary source of authentication and the local-auth-fallback as the secondary source. For additional information, see TACACS+ Configuration on page 19.

Procedure

1. Enter the Config mode.

```
device(config)#
```

2. Configure the login authentication mode.

```
device# configure terminal
device(config)# aaa authentication login tacacs+ local-auth-fallback
device(config)# aaa accounting all default start-stop tacacs+
device(config)# tacacs-server host 1.2.3.4
device(config-tacacs-config)# plain-key testing123
```

   For more information on the `aaa authentication` command, see *Extreme 9920 Software Command Reference, 21.2.2.0*.

   Authentication is attempted first with the TACACS+ server. If that fails, authentication is attempted with the local database.

3. View the configuration.

```
device(config-tacacs-config)# do show run
username testuser2 role user password $6$salt$cevuzTZ/QBjzuZG0/
ebEeedmcTnhyM8ITUu8K032Cp2XvIibq7voqYagm18bwpLBqrg/l/l6YxTmKKibJz5r10
tacacs-server host 1.2.3.4
  encrypted-key QjQkJLQUF3ncI1ooQCOaoEsBn5epVI3GsQwFD6i_BW
aaa authentication login tacacs+ local-auth-fallback
aaa accounting commands default start-stop tacacs+
interface ethernet 1/2
  shutdown
interface ethernet 2/2
  shutdown
```

4. Log into the device using an account with TACACS+-only credentials to verify if the login authentication mode is configured.

Reset the Login Authentication Mode

About This Task

Perform this procedure to reset the login configuration mode to the default value.

Procedure

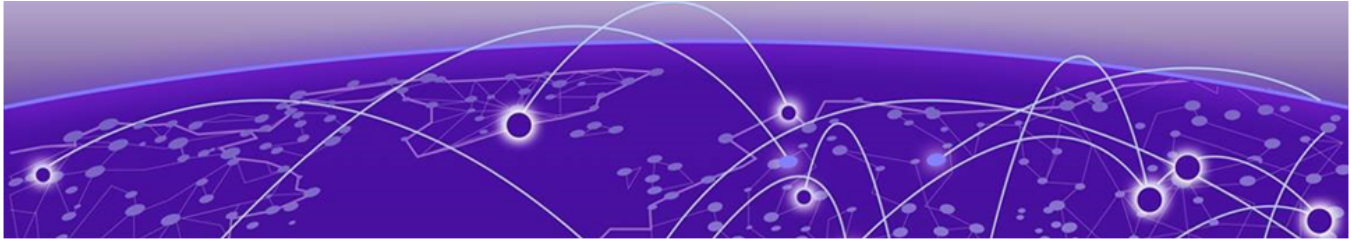
1. Enter the Config mode.

```
device(config)#
```

2. Remove the configured authentication sequence and restore it to the default value (local-only).

```
device(config)# no aaa authentication login tacacs+ local-auth-fallback
```

3. Log into the device using default (local-only) credentials to verify if the login authentication mode is reset.



TACACS+ Server Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) is an AAA server protocol that uses a centralized authentication server and multiple network access servers or clients. With TACACS+ support, management of devices seamlessly integrates into network fabric environments. After a device is configured to use TACACS+, it becomes a TACACS+ client.

The NPB application uses the TACACS+ server for authentication and accounting. You can access the device through SSH. The device goes through the same TACACS+ authentication process with either access method. Both IPv4 and IPv6 addresses are supported.

Note
For more information about configuring remote server authentication, see Remote Server Authentication on page 15. For complete information on login authentication mode, refer to the `aaa authentication` command in the *Extreme 9920 Software Command Reference, 21.2.2.0*.

Supported TACACS+ Packages and Protocols

The NPB application supports the following TACACS+ packages for running the TACACS+ daemon on remote AAA servers:

- Free TACACS+ daemon. You can download the latest package from www.shrubbery.net/tac_plus.
- ACS 5.3
- ACS 4.2

The TACACS+ protocol v1.78 is used for AAA services between the device client and the TACACS+ server.

Challenge Handshake Authentication Protocol (CHAP) authentication protocol is supported for user authentication.

TACACS+ Configuration

Configuring TACACS+ requires configuring TACACS+ support on the client and server.

You must individually configure each client device to use TACACS+ servers. To configure the server IP address and key, use the **tacacs-server** command. You can configure a maximum of five TACACS+ servers on a device for AAA service.

The following table lists the TACACS+ server parameters.

Table 7: TACACS+ server parameters

Parameter	Description
host	IPv4 or IPv6 address or domain name or host name of the TACACS+ server. Host name requires prior DNS configuration. The maximum supported length for the host name is 40 characters.
port	The TCP port used to connect the TACACS+ server for authentication. The port range is 1 through 65535; the default port is 49 and is not configurable. Default value is used.
protocol	The authentication protocol to be used and is not configurable. CHAP is used.
key	Specifies the configurable text string that is used as the shared secret between the device and the TACACS+ server to make the message exchange secure. The plain-text key must be between 1 and 40 characters in length and the encrypted key length must be less than or equal to 128 characters. **Note:** The value of **key** must match the value configured in the TACACS+ configuration file; otherwise, the communication between the server and the device fails.
retries	The number of attempts permitted to connect to a TACACS+ server. The range is 0 through 100, and the default value is 5. Not configurable. Default value is used.
timeout	The maximum amount of time to wait for a server to respond. Options are from 1 through 60 seconds, and the default value is 5 seconds. Not configurable. Default value is used.

Create a TACACS+ Client

The NPB application uses the local database for authentication by default.

Before You Begin

- Only admin users can perform this procedure.
- After configuring the client-side TACACS+ server list, you must set the authentication mode so that TACACS+ is used as the primary source of authentication.

About This Task

You can configure the NPB application to authenticate users with the TACACS+ server as the primary method, with the local database as the fallback if TACACS+ is unavailable or authentication fails.

Procedure

Create a TACACS+ client.

```
# [no] aaa authentication login tacacs+ local-auth-fallback
```

Add a TACACS+ Server

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure to add a TACACS+ server host to the client server list.

Note

When a list of servers is configured, failover from one server to another server happens only when a TACACS+ server fails to respond; it does not happen when user authentication fails.

Procedure

1. Enter the Config mode.

   ```
   device(config)#
   ```

2. Configure the TACACS+ server IP address.

   ```
   device(config)# tacacs-server host 10.2.3.5
   device(config-tacacs-config)#
   ```

3. Configure the required plain-text or encrypted shared secret key string.

   ```
   device(config-tacacs-config)# plain-key "new#hercules*secret*"
   ```

4. Return to the Exec mode and verify the configuration.

   ```
   device(config-tacacs-config)# end
   device# show running-config tacacs-server tacacs-server host 10.2.3.5 encrypted-key
   jahasjikjdoaskjuihuhiaoljsiaknkaiua=
   ```

Modify TACACS+ Server Configuration

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure modify the client-side TACACS+ server configuration.

Procedure

1. Display the configured server IP addresses.

```
device# show running-config tacacs-server tacacs-server host 10.2.3.5 encrypted-key
"jahasjikjdoaskjuihuhiaoljsiaknkaiua="

# tacacs-server host 1.2.3.4 encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo
```

2. Enter the Config mode.

```
device(config)#
```

3. Enter TACACS+ server configuration mode.

```
device(config)# tacacs-server host 10.2.3.5
device(config-tacacs-config)#
```

4. Modify the required the parameters.
   - `host`
   - `plain-key`
   - `encrypted-key`

```
device(config-tacacs-config)# plain-key "changedsec"
```

5. Return to the Exec mode and verify the configuration.

```
device(config-tacacs-config)# end
device# show running-config tacacs-server tacacs-server host 10.2.3.5 encrypted-key
"jahasjikjdoaskjuihuhiaoljsiaknkaiua="
```

Remove the TACACS+ Server Key

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure to remove the configured TACACS+ server key from the client.

Procedure

1. Display the configured server IP addresses and keys.

```
device# show running-config tacacs-server

tacacs-server host 10.2.3.5 encrypted-key "jahasjikjdoaskjuihuhiaoljsiaknkaiua="
tacacs-server host 1.2.3.4 encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo
```

2. Enter the Config mode.

```
device(config)#
```

3. Enter TACACS+ server configuration mode for the selected TACACS+ server.

```
device(config)# tacacs-server host ip-address
device(config-tacacs-config)#
```

4. Remove the key from the server.

```
device(config)# tacacs-server host ip-address
device(config-tacacs-config)# no encrypted-key
```

5. Return to the Exec mode and verify the configuration.

```
device(config-tacacs-config)# end
device# show running-config tacacs-server tacacs-server host host-address
```

Example

The following example removes the key from TACACS+ server on 10.2.3.5.

```
device# configure terminal
device(config)# tacacs-server host 10.2.3.5
device(config-tacacs-config)# no encrypted-key
device(config-tacacs-config)# end

device# show running-config tacacs-server
tacacs-server host 10.2.3.5

tacacs-server host 1.2.3.4 encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo
```

Remove the TACACS+ Server Configuration

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure to remove TACACS+ server configuration from the client.

Procedure

1. Display the configured server IP addresses and keys.

```
device# show running-config tacacs-server
tacacs-server host 10.2.3.5 encrypted-key "jahasjikjdoaskjuihuhiaoljsiaknkaiua="
tacacs-server host 1.2.3.4 encrypted-key "JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo"
```

2. Enter the Config mode.

```
device(config)#
```

3. Remove the selected TACACS+ configuration from the server.

```
device(config)# no tacacs-server host 10.2.3.5
```

4. Return to the Exec mode and verify the TACACS+ server configuration.

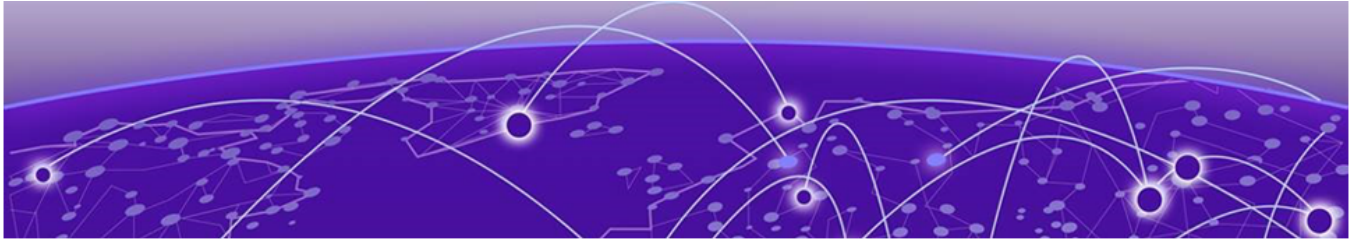
```
device(config-tacacs-config)# end
device# show running-config tacacs-server
tacacs-server host 1.2.3.4 encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo
```

Example

The following example removes the TACACS+ configuration from the server on 10.2.3.5.

```
device# configure terminal
device(config)# no tacacs-server host 10.2.3.5
device(config)# end

device# show running-config tacacs-server
tacacs-server host 1.2.3.4 encrypted-key JMeYDVdBN4Vb-wx35d7HnXIE8BL9KLUcEcePFwMNGo
```



HTTPS Certificates

Extreme 9920 software uses a TLS connection for incoming requests, using a default certificate. Both IPv4 and IPv6 addresses are supported.

The following topics discuss HTTPS certificate management on the 9920 when a default certificate is not used.

Export the Default CA Certificate

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure to export the default CA certificate from the device to the remote host in PEM format.

Procedure

Export the default CA certificate to the remote host.

```
device# crypto export ca-certificate default protocol scp remote-server 10.37.16.211
remote-file /root/temp/test.txt user root password root123
Exporting switch 'default' CA certificate...
Exported switch 'default' CA certificate successfully.
```

Import or Replace an HTTPS Certificate

Before You Begin

- Only admin users can perform this procedure.
- The HTTPS certificate file must be in PEM or PKCS format.

About This Task

Perform this procedure to import or replace an HTTPS certificate on the ingress controller. Applications communicating with the 9920 device are secured with TLS. For additional security, a third-party certificate can replace the default certificates. The third-party certificate can be shared with client applications to validate the server. The

IP address of the 9920 device should present in the SAN and the common name of third-party server certificates.

Note
If an IP address mismatch occurs between the 9920 device and the server certificate SAN IP, authentication fails during TLS connection.

Procedure

Import or replace an HTTPS certificate.

```
device# crypto import type https protocol scp host host address certificate cert.pem key
key.pem user remote-user password remote-password

Installing https certificate will result in a momentary delay and may affect active CLI
connections - please be patient.
```

Remove an Imported HTTPS Certificate

Before You Begin

Only admin users can perform this procedure.

About This Task

Perform this procedure to remove the imported HTTPS certificate so the ingress controller reverts to using the self-signed certificate. You can shut down the HTTPS service without disabling HTTPS certificates. When the Apache web server boots, it enables the HTTPS service only if HTTPS crypto certificates are configured and enabled.

Note
HTTPS certificates must be configured and enabled for web service to function on the device.

Procedure

1. Delete the device certificate.

   ```
   device# no crypto import type https
   ```

2. Verify that the HTTPS certificates were removed.

   ```
   device# show crypto certificates
   ```

Token-Based Authentication

The NPB application supports token-based authentication, where a user provides credentials in the form of a username and password and receives a generated token that facilitates authentication for future access.

The NPB application supports JSON Web token (JWT) token authentication for gRPC requests. The client accesses the RSA key-pair-signed token by presenting the credentials to an authentication API. When the token is stored on the client, it can send additional gRPC/HTTPS requests, with `Authorization: <type> <credentials>`, where the authorization type is Bearer followed by your JWT access token credentials, similar to the following example.

```
headers: {
    Authorization: "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzd......G8p-_cD0"
  }
```

The authenticate request/response includes a long-lived refresh token, which can be used to get a new access-token when the previous access-token expires, as shown in the following code snippet.

```
service Auth {
 rpc Authenticate (AuthenticateRequest) returns (AuthenticateResponse);
 rpc GetAccessToken (RefreshToken) returns (AccessToken);
}
```

For more information about implementing JWT token-based authentication, see the *Extreme 9920 Software YANG Reference, 21.2.2.0*.

Token-Based Authentication Limitations

Note the following limitations for implementing token-based authentication:

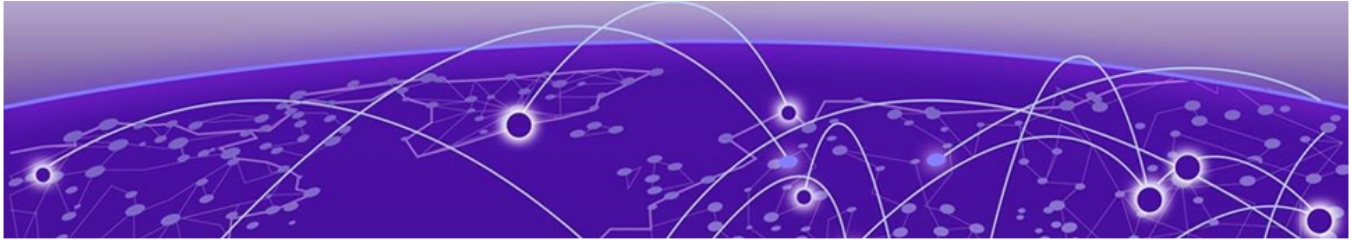
- The access token lifetime is 24 hours. When it expires, a refresh token is used to fetch a new access token.
- The refresh token has a 30-day lifetime. When it expires, the user must reauthenticate and obtain a new access token and then a refresh token.
- The existing tokens become invalid in the following scenarios, and a user must reauthenticate and obtain a new access token.
  - Token expired.
  - Login-authentication method changed.

- User account associated with the token deleted or blocked (local users only).
- Changed user password (local users only).
- Changed user role (local users only).

Token-Based Authentication Flow

The following steps describe the NPB application's token-based authentication process.

1. The client requests an access token from AuthService, using the Authenticate() API method (from AuthClient) to pass user credentials.
2. AuthService issues the token in response, using the following process:
   a. User credentials are validated with the AAA login mechanism configured on the device.
   b. The JWT token is generated and includes role, expiry, and other relevant information.
   c. AuthService signs the token with its private key and sends it as the response to Authenticate() API.
3. The client stores the response token, sending it with every gNMI/gNOI request with the token type and token credential in the Authorization header.
4. AuthService validates the token by performing the following steps:
   a. Validates the signature with the public key from the cert store.
   b. Validates the claims (expiry check, role validation, and any others).
   c. Checks whether the role in the token has permission to access the requested resource.
5. If step 4 fails, the authentication fails, and the request response is an error message.



Remote System Logging

You can configure any Linux server that has the Rsyslog utility installed to accept system logs (syslogs) from Extreme 9920. For more information about installing Rsyslog, see https://www.rsyslog.com/doc/master/installation/install_from_source.html. For all supported system logging commands, see the *Extreme 9920 Software Command Reference, 21.2.2.0*.

Extreme 9920 software supports the following transport protocols for remote system logs:

- UDP
- TCP
- TCP/TLS

Note the following limitations for configuring remote system logging:

- Log filtering is not supported. All syslog types are forwarded to the configured remote server.
- No log-level mapping.

Default CA certificate

A default CA certificate for TLS is provided to verify the certificate that the Extreme 9920 device issues. All gNMI requests to the device are over a secure channel. The Extreme 9920 uses the default HTTPS server certificate if you do not import an HTTPS server certificate.

Use the following CA certificate on the client to verify the certificate generated by the 9920.

```
-----BEGIN CERTIFICATE-----
MIIGPjCCBCagAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgbMxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTELMAkGA1UEBwwCU0oxGTAXBgNVBAoMEEV4dHJlbWUgTmV0
d29ya3MxHzAdBgNVBAsMFkV4dHJlbWUgTmV0d29ya3MgTkdOUEIxIjAgBgNVBAMM
```

```
GW5nbnBiLmV4dHJlbWVuZXR3b3Jrcy5jb20xKjAoBgkqhkiG9w0BCQEWG3N1cHBv
cnRAZXh0cmVtZW5ldHdvcmtzLmNvbTAeFw0yMDA3MDcyMTEzNDNaFw0zMDA3MDUy
MTEzNDNaMIGnMQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExGTAXBgNVBAoMEEV4
dHJlbWUgTmV0d29ya3MxJDAiBgNVBAsMG0V4dHJlbWUgTmV0d29ya3MgTmV4dEdl
bk5QQjEeMBwGA1UEAwwVTkdOUEIgSW50ZXJtZWRpYXRlIENBMSowKAYJKoZIhvcN
AQkBFhtzdXBwb3J0QGV4dHJlbWVuZXR3b3Jrcy5jb20wggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC64lUkRcEvz+jWfm9V9+g/AgZFpDOKL5oR4c3IHdwM
vAA6Rt+Os+6wvOpLysDvzggeVh4L6BWULgFw5SyRhjKJbyz7PaMBg/id5XPqWntU
3MoPOdewdVozyZZf3MRDVqgw8f7nT4Ex55fSnfyYLOx5g2++rUUK3jpQo74vRI/W
SUZdOAvs9hkERcMJIm4DDcj86Z4HuYaB/iBBSqPDhRoErpaX36TOWY+2wCNomkK1
zzCO9PW3HhfZk+GWF10U/7ZkNOBMnd5nVIalf+VsSpaPzQxAJtIKS1xYqmoACW6s
S/myGEPuDqmYhilwSgP+lyRmpkGZEfPbwxZyrhxUAnwQ0+r8HUSvBRavK+utt+JQ
SeFiPPVeo6OoGgwRJ1t9KVid+Sp56+gwMj27Kf26cWYUJsjjHxyJgFFCforcn40M
Kox5idbZkQjdo7ciofK7Twz8U+ip/lyhbycUcz7cG7vimRvu+BpyJ29zL7It/PZX
U8fP3r0ssudasfwZGxl3AO58szhopE0m4eaIQzhotqwqXt6s8Vh/+qj6JMudMxa6
5HVeBVX6BEvLG8TwKaaQiJ4edwI/QY0WZ0wxfeDn05haSiyOhRkmA/F9cqv3h8qM
B5+IZ+nYNpjASyxc1QTtW9Xhn37vp61+7JddU9zxeSVkB43YGOK9Uq1+DXDawlzA
5wIDAQABo2YwZDAdBgNVHQ4EFgQU2Sn6JG7Jo3QzMRBsLHhQkVW8uzQwHwYDVR0j
BBgwFoAUuwS1PNyE3M192izM7zaoJm1vhTQwEgYDVR0TAQH/BAgwBgEB/wIBADAO
BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBAKRIQfsZiiIVZC3jCmBt
cwf3LRN2ESOy8bj4AV0LxgchjMtw/y/Dp7ST5FkUEIAya8HEmL1tjZhHFh0uNfBx
7UcRV2R7ZhGu08TujFbo9sVy2GHd+w1/L6VDauEjV6eUd4oI6kylcDK/OA3UoYwF
vbiiLlDYEFaP3/3MFaqk9osfmkxcmhu3qxOt3QxqevXPiXtXlNxT4w/LrQFXKMcJ
40zjFjgnNsdYlr92c2kwWDE/44xnOWEH7Ar2PuqvqHJi1GFv1lV/Ys+0wkqCyy/K
eAdde8d8ZWcXroSHzlGI34Tql2U9+bZjxNgU9Nc8VJGq+K9LBDTQqFfGg0n9qHYE
eCGGzw5eT+lJMSVompRPEHt44qCk5eKRmEWsMbgeD8d6cisPE4PffIynSV/evjsY
k9gaE0d86uhN5EuNQsqtLn5vsdWN8nBBP+umPLtHpppHATAGSWgW8WGgSLs8gBwS
IABCVCpV7oePXN0LCfzRTd2JwCmUpqxreGw3cuePDMNimOQvwnaAvLfNxFYSoRtp
wU8VGdAUQJxqkeS4xlkpKbOYGGHlntlskSP7VuygLn2ISa3v6xTRLlaTDcLuiu+K
vNGwM33rgKUiPtDFM9oK0CtiydM1TqfQZB3/B1a3RzqX2OmBvR6qB9M5jeNQXd+T
wa/daP9p2G6/lcNRE+AiCpul
-----END CERTIFICATE-----
```

Configure a Remote Logging Server

You can configure any Linux server with the Rsyslog utility to accept syslogs from the NPB application.

Before You Begin

The Rsyslog utility must be installed on the Remote Logging Server.

About This Task

Configure the `rsyslog.conf` file to set up a Remote Logging Server.

Procedure

1. Navigate to the `rsyslog.conf` file and open it in your preferred text editor.

   ```
   $ /etc/rsyslog.conf
   ```

2. Ensure that the following rule is included in the `rsyslog.conf` file.

   ```
   $IncludeConfig /etc/rsyslog.d/*.conf
   ```

3. Save and close the `rsyslog.conf` file.

Configure Remote Logging Server Storage

You can configure the remote logging server to store `client log` files in separate directories.

Before You Begin

The Rsyslog utility must be installed on the Remote Logging Server.

About This Task

By default, system logs are stored in the `/var/log directory`. When system logs are received from other machines, it is a best practice to store the syslogs each client in separate directories.

Procedure

1. Create the following `conf` file.

```
$ /etc/rsyslog.d/directives.conf
```

2. Open the `directives.conf` file in your preferred text editor and add the following content.

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

   The `directives.conf` file does the following:

   - Creates the template `RemoteLogs` and applies it to all logs.
   - Creates a log directory for each client with the local server host name and stores log files with the syslog service name from each sending device to the named directory.
   - Creates a directory with the local server host name and stores local syslogs to this location.
   - Appends logs to the files that already exist.

3. Save and close the `directives.conf` file.
4. Restart the `rsyslog` service to begin logging according to `directives.conf`.

```
$ sudo systemctl restart rsyslog
```

5. Verify the `rsyslog` service status.

```
$ sudo systemctl status rsyslog
```

Configure Remote Logging to Use UDP

You can configure the remote server for logging through UDP.

Before You Begin

The NPB application supports remote logging on Linux, Mac, or Windows operating systems, and the following commands are Linux-specific. See the documentation for the Rsyslog utility for your operating system, as needed.

About This Task

Create a UDP-specific configuration file to enable UDP transport of syslog.

Procedure

1. At the command prompt, create and open the `udp.conf` file in your preferred text editor.

```
$ /etc/rsyslog.d/udp.conf
```

2. Copy the following text into the `udp.conf` file with the appropriate port number.

```
# load UDP listener
module(load="imudp")
# start listener at port 514
input(type="imudp" port="514")
```

3. Save and close `udp.conf` file.
4. Restart the rsyslog service.

```
$ sudo systemctl restart rsyslog
```

5. Verify the rsyslog service status.

```
$ sudo systemctl status rsyslog
```

Configure Remote Logging to Use TCP

You can configure the remote server for logging through TCP.

Before You Begin

The NPB application supports remote logging on Linux, Mac, or Windows operating systems, and the following commands are Linux-specific. See the documentation for the Rsyslog utility for your operating system, as needed.

About This Task

Create a TCP-specific configuration file to enable UDP transport of syslog.

Procedure

1. At the command prompt, create and open the `tcp.conf` file in your preferred text editor.

```
$ /etc/rsyslog.d/tcp.conf
```

2. Copy the following text into the `tcp.conf` file with the appropriate port number.

```
# load TCP listener
module(load="imtcp")
# start listener at port 514
input(type="imtcp" port="514")
```

3. Save and close the `tcp.conf` file.
4. Restart the `rsyslog` service.

```
$ sudo systemctl restart rsyslog
```

5. Verify the `rsyslog` service status.

```
$ sudo systemctl status rsyslog
```

Install TLS Encryption Certificates

Before You Begin

The NPB application supports remote logging on Linux, Mac, or Windows operating systems, and the following commands are Linux-specific. See the documentation for the Rsyslog utility for your operating system, as needed.

About This Task

Perform this procedure to install the three certificates required for using TLS encryption for remote logging. To optionally enable TLS encryption over TCP, you must generate and install three certificates on the remote logging server to enable TLS encryption over TCP. All three certificates are in PEM format:

- CA certificate
- Machine key certificate
- Machine key

Note
The Rsyslog client that sends syslogs to the remote logging server, needs only the current CA certificate on the device.

Procedure

1. Generate the three required certificates, using the instructions at the following Rsylog locations:
   - https://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_ca.html
   - https://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_machine.html
2. Use the **copy** command to copy the certificates to the preferred directory (default is `/etc/ssl/certs`).

   Note
   Note the filepath for each certificate to configure the remote logging server to use TLS encryption.

3. Run the **chmod** command to set file permissions to 0644 on each certificate.

Configure Remote Logging to Use TCP with TLS Encryption

Learn how to configure the remote server for logging via TCP using TLS encryption.

Before You Begin

Generate the certificates required to use TLS encryption and import them to the remove server, making sure they have the proper read permissions (0644). Make sure you have noted the filepaths to each certificate.

About This Task

You install an rsyslog utilities package and add content to tcp.conf on the remote server to enable TLS encryption over TCP.

Procedure

1. If not already installed, run the following command on the remote server to install the package rsyslog-gnutls.

```
$ sudo apt-get install rsyslog-gnutls
```

2. At the command prompt, create and open the following file in your preferred text editor.

```
$ /etc/rsyslog.d/tcp.conf
```

3. Copy and paste the following text into the tcp.conf file, making sure the certificate filepaths are correct and replacing the port number if needed with one you choose.

```
global(
DefaultNetstreamDriver="gtls"
DefaultNetstreamDriverCAFile="/path/to/ca-certificate/ca.pem"
DefaultNetstreamDriverCertFile="/path/to/server-certificate/server-cert.pem"
DefaultNetstreamDriverKeyFile="/path/to/server-key/server-key.pem"
)

# load TCP listener
module(
load="imtcp"
StreamDriver.Name="gtls"
StreamDriver.Mode="1"
StreamDriver.Authmode="anon"
)

# start up listener at port 514
input(
type="imtcp"
port="514"
```

4. Save and close tcp.conf.
5. Run the following command to restart the rsyslog service.

```
$ sudo systemctl restart rsyslog
```

6. Run the following command to verify the rsyslog service status.

```
$ sudo systemctl status rsyslog
```