Configuring Authentication

This chapter describes how to configure authentication on the Cisco LoRaWAN Gateway.

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your LoRaWAN Gateway and viewing configuration information. Typically, you want network administrators to have access to your device while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your LoRaWAN Gateway, you should configure username and password pairs, which are locally stored on the device. These pairs are assigned to lines or ports and authenticate each user before that user can access the LoRaWAN Gateway. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

Configuring Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use the **enable secret** global configuration commands.

The command allows you to establish an encrypted password that users must enter to access privileged EXEC mode (the default).

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable secret passwords:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**enable secret** {*password* | **5** *encrypted_passwd*|**8** *encrypted_passwd*}	Define a secret password for access to privileged EXEC mode. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password. **Note** Special characters cannot be used for the plain password. **Note** While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To remove a password, use the **no enable secret** global configuration command.

Configuring Username and Password for Local Authentication

You can configure username and password pairs, which are locally stored on the LoRaWAN Gateway. These pairs are assigned to lines or ports and authenticate each user before that user can access the LoRaWAN Gateway.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**username** *name* {*password* | **5** *encrypted_passwd* |**8** *encrypted_passwd*}	Enter the username and password for each user. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password.

	Command or Action	Purpose
		Note Special characters cannot be used for the plain password. **Note** While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

Note For enable secret, username, and system admin, use the following characters for the password:

- Lowercase alphabet: [a-z]
- Uppercase alphabet: [A-Z]
- Numbers: [0-9]
- Special Character: [$%{}+_:]

Configuring Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 2 (SSHv2).

Beginning in privileged EXEC mode, follow these steps to configure SSH on the LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

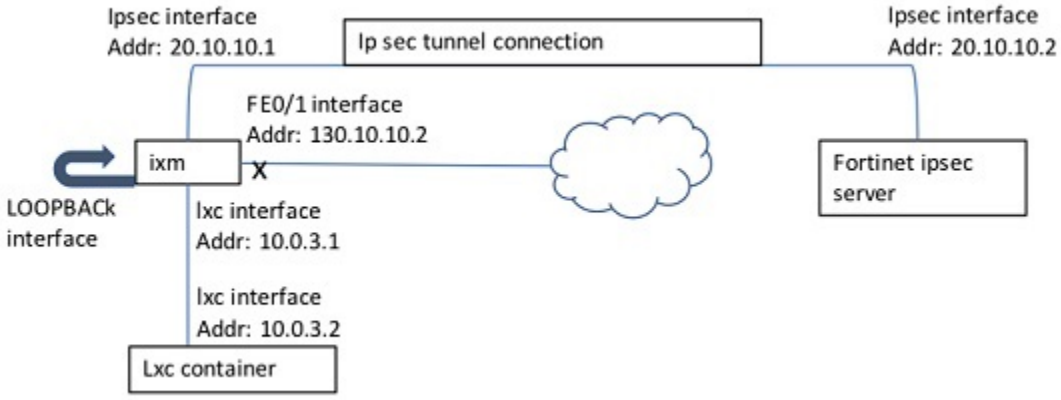
	Command or Action	Purpose
Step 2	**hostname** *hostname*	Configure a hostname for your LoRaWAN Gateway.
Step 3	**ip domain name** *domain_name*	Configure a host domain for your LoRaWAN Gateway.
Step 4	**ip ssh** {**port**|**session**|**authentication-retries**| **time-out**|**admin-access**|**local**| **limit-local**}	Configure the SSH control parameters: • **port** – Configure SSH port. • **session** – Configure number of SSH session. • **authentication-retries** – Configure number of authentication retries. • **time-out** – Configure timeout interval. • **admin-access** – Allow admin access via SSH. • **local** – Restrict user to container and reverse-tunnel SSH access only. • **limit-local** – Permit SSH on local only. Limit the listening address to local address only (for example, 127.0.0.1 or 10.0.3.1). Not listen on LAN interface.
Step 5	**crypto key generate rsa**	Enable the SSH server for local and remote authentication on the LoRaWAN Gateway and generate an RSA key pair. Generating an RSA key pair automatically enables SSH.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	Do one of the following: • **show ip ssh** • **show ssh**	Show and configuration information for your SSH server. Show the status of the SSH server on the LoRaWAN Gateway.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring IP SSH Limit Local

The following figure shows an example of the **IP SSH limit local** command behavior.



When **IP SSH limit local disabled** is configured, the SSH connections to all innterfaces are allowed. When **IP SSH limit local enabled** is configured, the SSH connection to FE0/1 (130.10.10.2) is not allowed.

Note When **IP SSH limit local** is enabled on the IXM, the SSH access from outside is disabled for the unit. The **uboot console disable** option only checks whether SSH is enabled or not, and does not factor the **IP SSH limit local** option. If both commands are configured, it is possible that both the console conntecvity and SSH connectivity are lost. In that case, the only way to access the unit is through container via Thing park.

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 1: Commands for Displaying the SSH Server Configuration and Status , on page 5:

Table 1: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

Using SCP to Upload Files

To copy a local file to a remote location, use the following **scp** EXEC command:

scp local *src_filename username host dst_filename*

To copy a remote file to local flash, use the following **scp** EXEC command:

scp remote *username host src_filename dst_filename*

SSH Access Over IPSec Tunnel

From the primary server and secondary server, you can SSH to IXM over the tunnel.

Example from IR800:

```
IR800# ssh -v 2 -l via 172.27.170.71
```

Configuring Reverse SSH and Connecting to Container

To open a shell to the container for user, use the **request shell container-console** EXEC command. Password is needed when you request shell container. If you have changed the system admin password, you need to use the new password.

Note Admin can change the password by using the **sysadmin security password** command.

Configuring Reverse SSH

Beginning in privileged EXEC mode, follow these steps to create a reverse SSH tunnel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**secure-tunnel create** <*port-no*> <*user-id*> <*remote-host*>	Create a reverse SSH tunnel.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show secure-tunnel**	Show the secure tunnel status.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
configure terminal
 secure tunnel create 30000 vnallamo 10.28.29.226
```

From the 10.28.29.226 server, execute the following command to reverse SSH:

```
ssh -l vik localhost -p 30000
```

Note When IPSec is enabled, secure tunnel may not be working due to gateway reachability. This is a known issue.

Copying Files From the Container

Beginning in privileged EXEC mode, follow these steps to copy files from the container to the host.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container copy** <*filename*> <*path*>	Copy files from the container to the host.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Changing Private Network Between Host and Container

Beginning in privileged EXEC mode, follow these steps to change the private network between the host and the container.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container private-network** <*chosen-private-network-option-from-the-list*>	Change the private network between the host and the container. You can choose one of the following options: 10.0.0.0/28, 172.16.0.0/28, or 192.168.0.0/28. By default, the private network is 10.0.3.0/24, which is configured on startup. To restore the default, use the no form of the command.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show container private-network**	Verify the configuration.

	Command or Action	Purpose
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
Gateway#show container private-network
Container private network: 172.16.0.0/2
```

User Accounts

This section describes the user accounts and their usages.

Use the **request shell host** command to enter the Linux shell and use the **request shell exit** command to exit.

Table 2: User Accounts

userID	SSH connection	Shell	Linux shell access through request shell host	Notes
system	no (default)	/bin/sh	yes	• Use the **ip ssh admin-access** CONF command to allow SSH access. • Use the **sysadmin security password** EXEC command to change system password.
user1	yes	clish	no	-
user2	yes	clish	no	-

Table 3: Linus Shell Access

Request Shell	Exit	Host
SSH	Exit from host	Go into console
console	Go into console	Go into console

Note It is recommended to change the Linux shell password using this command "sysadmin security password".

Table 4: Password Change on Switchover

Switchover Type	Description
From virtual mode to standalone mode	The virtual mode root password is assigned to the standalone mode system password.
From standalone mode to virtual mode	The standalone mode system password is lost during the switchover, and the virtual mode root password remains.

Configuring Logging in Container

Beginning in privileged EXEC mode, follow these steps to configure logging in the container.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container log all**	Enable logging through syslog-ng in the container. To restore the default, use the **no** form of the command.
Step 3	**exit**	Return to privileged EXEC mode.

After the is command is enabled, you can view the logs by logging into the container. The logs are located in **/var/run**.

Example

```
Gateway(config)#container log all
Container syslog has started.
```