Secure Shell—Configuring User Authentication Methods

The Secure Shell—Configuring User Authentication Methods feature helps configure the user authentication methods available in the Secure Shell (SSH) server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Secure Shell—Configuring User Authentication Methods

Secure Shell (SSH) server and SSH client are supported on data encryption software (DES) (56-bit) and 3DES (168-bit) images only.

Information About Secure Shell—Configuring User Authentication Methods

Secure Shell User Authentication Overview

Secure Shell (SSH) enables an SSH client to make a secure, encrypted connection to a Cisco device (Cisco IOS SSH server). The SSH client uses the SSH protocol to provide device authentication and encryption.

The SSH server supports three types of user authentication methods and sends these authentication methods to the SSH client in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method
- Password authentication method

By default, all the user authentication methods are enabled. Use the **no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} command to disable any specific user authentication method so that the disabled method is not negotiated in the SSH user authentication protocol. This feature helps the SSH server offer any preferred user authentication method in an order different from the predefined order. The disabled user authentication method can be enabled using the **ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} command.

As per RFC 4252 (The Secure Shell (SSH) Authentication Protocol), the public-key authentication method is mandatory. This feature enables the SSH server to override the RFC behavior and disable any SSH user authentication method, including public-key authentication.

For example, if the SSH server prefers the password authentication method, the SSH server can disable the public-key and keyboard-interactive authentication methods.

How to Configure Secure Shell—Configuring User Authentication Methods

Configuring User Authentication for the SSH Server

Perform this task to configure user authentication methods in the Secure Shell (SSH) server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
4. **ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
5. **default ip ssh server authenticate user**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
	Example:
	`Device(config)# no ip ssh server authenticate user publickey`
	`%SSH:Publickey disabled.Overriding RFC`
		Disables a user authentication method in the Secure Shell (SSH) server.
		Note A warning message is displayed when the **no ip ssh server authenticate user publickey** command is used to disable public-key authentication. This command overrides the RFC 4252 (The Secure Shell (SSH) Authentication Protocol) behavior, which states that public-key authentication is mandatory.

Step 4	**ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} **Example:** `Device(config)# ip ssh server authenticate user publickey`	Enables the disabled user authentication method in the SSH server.
Step 5	**default ip ssh server authenticate user** **Example:** `Device(config)# default ip ssh server authenticate user`	Returns to the default behavior in which all user authentication methods are enabled in the predefined order.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

- If the public-key-based authentication method is disabled using the **no ip ssh server authenticate user publickey** command, the RFC 4252 (The Secure Shell (SSH) Authentication Protocol) behavior in which public-key authentication is mandatory is overridden and the following warning message is displayed:

  `%SSH:Publickey disabled.Overriding RFC`

- If all three authentication methods are disabled, the following warning message is displayed:

```
%SSH:No auth method configured.Incoming connection will be dropped
```

- In the event of an incoming SSH session request from the SSH client when all three user authentication methods are disabled on the SSH server, the connection request is dropped at the SSH server and a system log message is available in the following format:

```
%SSH-3-NO_USERAUTH: No auth method configured for SSH Server. Incoming connection from
 <ip address> (tty = <ttynum>) dropped
```

Verifying User Authentication for the SSH Server

SUMMARY STEPS

1. **enable**
2. **show ip ssh**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 show ip ssh

Displays the version and configuration data for Secure Shell (SSH).

Example:

The following sample output from the **show ip ssh** command confirms that all three user authentication methods are enabled in the SSH server:

```
Device# show ip ssh

Authentication methods:publickey,keyboard-interactive,password
```

The following sample output from the **show ip ssh** command confirms that all three user authentication methods are disabled in the SSH server:

```
Device# show ip ssh

Authentication methods:NONE
```

Configuration Examples for Secure Shell—Configuring User Authentication Methods

Example: Disabling User Authentication Methods

The following example shows how to disable the public-key-based authentication and keyboard-based authentication methods, allowing the SSH client to connect to the SSH server using the password-based authentication method:

```
Device> enable
Device# configure terminal
Device(config)# no ip ssh server authenticate user publickey
%SSH:Publickey disabled.Overriding RFC
Device(config)# no ip ssh server authenticate user keyboard
Device(config)# exit
```

Example: Enabling User Authentication Methods

The following example shows how to enable the public-key-based authentication and keyboard-based authentication methods:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server authenticate user publickey
Device(config)# ip ssh server authenticate user keyboard
Device(config)# exit
```

Example: Configuring Default User Authentication Methods

The following example shows how to return to the default behavior in which all three user authentication methods are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server authenticate user
Device(config)# exit
```

Additional References for Secure Shell—Configuring User Authentication Methods

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
SSH configuration	*Secure Shell Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 4252	*The Secure Shell (SSH) Authentication Protocol*
RFC 4253	*The Secure Shell (SSH) Transport Layer Protocol*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Secure Shell—Configuring User Authentication Methods

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Secure Shell—Configuring User Authentication Methods

Feature Name	Releases	Feature Information
Secure Shell—Configuring User Authentication Methods	Cisco IOS XE Release 3.10S	The Secure Shell—Configuring User Authentication Methods feature helps configure the user authentication methods available in the Secure Shell (SSH) server. The following command was introduced: **ip ssh server authenticate user**. In Cisco IOS XE Release 3.10, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.