X.509v3 Certificates for SSH Authentication

The X.509v3 Certificates for SSH Authentication feature uses public key algorithm (PKI) for server and user authentication, and allows the Secure Shell (SSH) protocol to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).

This module describes how to configure server and user certificate profiles for a digital certificate.

This module describes the feature and consists of these sections:

- Prerequisites for X.509v3 Certificates for SSH Authentication, page 47-1
- Restrictions for X.509v3 Certificates for SSH Authentication, page 47-2
- Information About X.509v3 Certificates for SSH Authentication, page 47-2
- How to Configure X.509v3 Certificates for SSH Authentication, page 47-3
- Configuration Examples for 509v3 Certificates for SSH Authentication, page 47-5
- Verifying Server and User Authentication Using Digital Certificates, page 47-6
- Additional References for 509v3 Certificates for SSH Authentication, page 47-6
- Feature Information for X.509v3 Certificates for SSH Authentication, page 47-8

Note For complete syntax and usage information for the switch commands used in this chapter, see the Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch.

If a command is not in the *Cisco Catalyst 4500 Series Switch Command Reference* , you can locate it in the Cisco IOS Master Command List, All Releases.

Prerequisites for X.509v3 Certificates for SSH Authentication

The X.509v3 Certificates for SSH Authentication feature replaces the **ip ssh server authenticate user** command with the **ip ssh server algorithm authentication** command. Configure the **default ip ssh server authenticate user** command to remove the **ip ssh server authenticate user** command from the configuration. The IOS secure shell (SSH) server will start using the **ip ssh server algorithm authentication** command.

When you configure the **ip ssh server authenticate user** command, the following message is displayed: "SSH command accepted; but this CLI will be deprecated soon. Please move to new CLI **ip ssh server algorithm authentication**. Please configure the "**default ip ssh server authenticate user**" to make the CLI ineffective."

Restrictions for X.509v3 Certificates for SSH Authentication

- The X.509v3 Certificates for SSH Authentication feature implementation is applicable only on the Cisco IOS Secure Shell (SSH) server side.
- The Cisco IOS SSH server supports only the x509v3-ssh-rsa algorithm-based certificate for server and user authentication.
- The Rivest, Shamir, and Adelman (RSA) 2-factor authentication on Catalyst 4506 SUP7L-E switches and Cisco Identity Services Engine (ISE) does not work correctly, when a user enters the incorrect password. Normal authentication and interworking with Cisco Adaptive Security Appliance (ASA) works fine. Configure the **ip ssh server algorithm authentication keyboard** command for the authentication to work.

Information About X.509v3 Certificates for SSH Authentication

- X.509v3 Certificates for SSH Authentication Overview, page 47-2
- Server and User Authentication Using X.509v3, page 47-2
- OCSP Response Stapling, page 47-3

X.509v3 Certificates for SSH Authentication Overview

The Secure Shell (SSH) protocol provides a secure remote access connection to network devices. The communication between the client and server is encrypted.

There are two SSH protocols that use public key cryptography for authentication. The Transport Layer Protocol, uses a digital signature algorithm (called the public key algorithm) to authenticate the server to the client. And the User Authentication Protocol uses a digital signature to authenticate (public key authentication) the client to the server.

The validity of the authentication depends upon the strength of the linkage between the public signing key and the identity of the signer. Digital certificates, such as those in X.509 Version 3 (X.509v3), are used to provide identity management. X.509v3 uses a chain of signatures by a trusted root certification authority and intermediate certificate authorities to bind a public signing key to a specific digital identity. This implementation allows the use of a public key algorithm for server and user authentication, and allows SSH to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).

Server and User Authentication Using X.509v3

For server authentication, the Secure shell (SSH) server sends its own certificate to the SSH client for verification. This server certificate is associated with the trustpoint configured in the server certificate profile (ssh-server-cert-profile-server configuration mode).

For user authentication, the SSH client sends the user's certificate to the IOS SSH server for verification. The SSH server validates the incoming user certificate using public key infrastructure (PKI) trustpoints configured in the server certificate profile (ssh-server-cert-profile-user configuration mode).

By default, certificate-based authentication is enabled for server and user at the IOS SSH server end.

OCSP Response Stapling

The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. This protocol specifies the data that needs to be exchanged between an application checking the status of a certificate and the server providing that status. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate until a response is received. An OCSP response at a minimum consists of a responseStatus field that indicates the processing status of the a request.

For the public key algorithms, the key format consists of a sequence of one or more X.509v3 certificates followed by a sequence of zero or more OCSP responses.

The X.509v3 Certificate for SSH Authentication feature uses OCSP Response Stapling. By using OCSP response stapling, a device obtains the revocation information of its own certificate by contacting the OCSP server and then stapling the result along with its certificates and sending the information to the peer rather than having the peer contact the OCSP responder.

How to Configure X.509v3 Certificates for SSH Authentication

- Configuring Digital Certificates for Server Authentication, page 47-3
- Configuring Digital Certificates for User Authentication, page 47-4

Configuring Digital Certificates for Server Authentication

	Command or Action	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(config)# ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]}`	Defines the order of host key algorithms. Only the configured algorithm is negotiated with the Secure Shell (SSH) client. **Note** The IOS SSH server must have at least one configured host key algorithm. • **x509v3-ssh-rsa**—certificate-based authentication • **ssh-rsa**—public key-based authentication
Step 4	`Switch(config)# ip ssh server certificate profile`	Configures server and user certificate profiles and enters SSH certificate profile configuration mode.
Step 5	`Switch(ssh-server-cert-profile)# server`	Configures server certificate profile and enters SSH server certificate profile server configuration mode. • The server profile is used to send out the certificate of the server to the SSH client during server authentication.

	Command or Action	Purpose
Step 6	`Switch(ssh-server-cert-profile-server)# trustpoint sign` *PKI-trustpoint-name*	Attaches the public key infrastructure (PKI) trustpoint to the server certificate profile. • The SSH server uses the certificate associated with this PKI trustpoint for server authentication.
Step 7	`Switch(ssh-server-cert-profile-server)# ocsp-response include`	(Optional) Sends the Online Certificate Status Protocol (OCSP) response or OCSP stapling along with the server certificate. **Note** By default, no OCSP response is sent along with the server certificate.
Step 8	`Switch(ssh-server-cert-profile-server)# end`	Exits SSH server certificate profile server configuration mode and returns to privileged EXEC mode.

Configuring Digital Certificates for User Authentication

	Command or Action	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(config)# ip ssh server algorithm authentication {publickey | keyboard | password}`	Defines the order of host key algorithms. Only the configured algorithm is negotiated with the Secure Shell (SSH) client. **Note** The IOS SSH server must have at least one configured host key algorithm. • To use the certificate method for user authentication, the **publickey** keyword must be configured.
Step 4	`Switch(config)# ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]}`	Defines the order of public key algorithms. Only the configured algorithm is accepted by the SSH client for user authentication. **Note** The IOS SSH client must have at least one configured public key algorithm. • **x509v3-ssh-rsa**—Certificate-based authentication • **ssh-rsa**—Public-key-based authentication
Step 5	`Switch(config)# ip ssh server certificate profile`	Configures server certificate profile and user certificate profile and enters SSH certificate profile configuration mode.
Step 6	`Switch(ssh-server-cert-profile)# user`	Configures user certificate profile and enters SSH server certificate profile user configuration mode.

	Command or Action	Purpose
Step 7	`Switch(ssh-server-cert-profile-user)#` **`trustpoint sign`** *`PKI-trustpoint-name`*	Configures the public key infrastructure (PKI) trustpoint that is used to verify the incoming user certificate. **Note** Configure multiple trustpoints by executing the same command multiple times. A maximum of 10 trustpoints can be configured.
Step 8	`Switch(ssh-server-cert-profile-user)#` **`ocsp-response include`**	(Optional) Sends the Online Certificate Status Protocol (OCSP) response or OCSP stapling along with the server certificate. **Note** By default, no OCSP response is sent along with the server certificate.
Step 9	`Switch(ssh-server-cert-profile-user)#` **`end`**	Exits SSH server certificate profile user configuration mode and returns to privileged EXEC mode.

Configuration Examples for 509v3 Certificates for SSH Authentication

- Example: Configuring Digital Certificates for Server Authentication, page 47-5
- Example: Configuring Digital Certificate for User Authentication, page 47-5

Example: Configuring Digital Certificates for Server Authentication

```
Switch> enable
Switch# configure terminal
Switch(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Switch(config)# ip ssh server certificate profile
Switch(ssh-server-cert-profile)# server
Switch(ssh-server-cert-profile-server)# trustpoint sign trust1
Switch(ssh-server-cert-profile-server)# exit
```

Example: Configuring Digital Certificate for User Authentication

```
Switch> enable
Switch# configure terminal
Switch(config)# ip ssh server algorithm authentication publickey
Switch(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Switch(config)# ip ssh server certificate profile
Switch(ssh-server-cert-profile)# user
Switch(ssh-server-cert-profile-user)# trustpoint verify trust2
Switch(ssh-server-cert-profile-user)# end
```

Verifying Server and User Authentication Using Digital Certificates

Displays the currently configured authentication methods. To confirm the use of certificate-based authentication, ensure that the x509v3-ssh-rsa algorithm is the configured host key algorithm.

```
Switch# show ip ssh

SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

Additional References for 509v3 Certificates for SSH Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Catalyst 4500 switch commands	*Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch*
PKI configuration	*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*

Standards & MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2784	Generic Routing Encapsulation (GRE)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for X.509v3 Certificates for SSH Authentication

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for X509v3 Certificates for SSH Authentication

Feature Name	Releases	Feature Information
X509v3 Certificates for SSH Authentication	Cisco IOS Release 15.2(4)E1 Cisco IOS XE Release 3.8.1E	The X.509v3 Certificates for SSH Authentication feature uses the X5.09v3 digital certificates in server and user authentication at the SSH server side. The following commands were introduced or modified: **ip ssh server algorithm hostkey**, **ip ssh server algorithm authentication**, and **ip ssh server certificate profile**.