

在Cisco IOS XE设备上配置SSH的证书身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[部署注意事项](#)

[配置](#)

[IOS-XE设备 \(SSH服务器 \)](#)

[Pragma Fortress CL \(安装在用户机器上的SSH客户端 \)](#)

[验证](#)

[故障排除](#)

[常见问题](#)

[配置错误](#)

[相关信息](#)

简介

本文档根据RFC 6187中定义的指南，概述在Cisco IOS® XE设备上使用X.509v3证书进行身份验证的安全外壳(SSH)配置。

先决条件

要求

思科建议您了解公钥基础设施(PKI)基础设施。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS XE版本17.3.5的C9200L交换机
- Pragma Fortress SSH客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响

背景信息

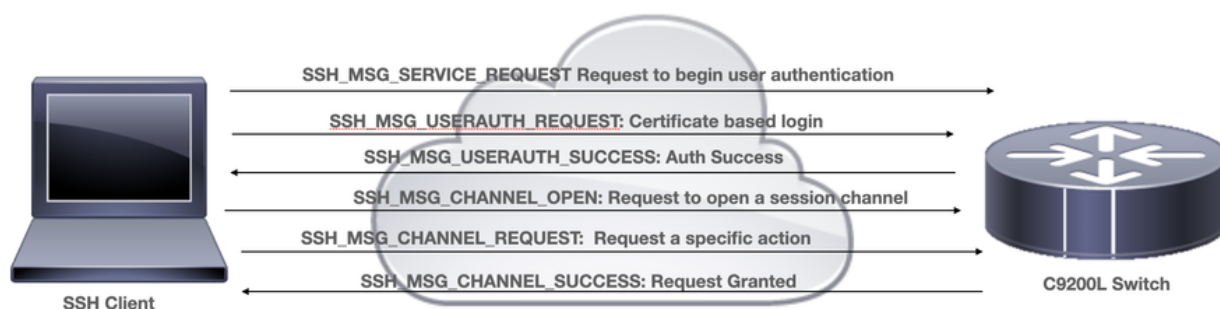
此方法通过启用基于证书的身份验证来增强SSH安全性，从而使SSH密钥管理实践与传输层安全(TLS)中使用的那些实践更紧密地保持一致。

SSH提供相互身份验证，以便在客户端和服务端之间建立安全连接。传统上，服务器使用Rivest-Shamir-Addleman(RSA)密钥对进行身份验证。客户端计算服务器的公钥的指纹，并提示管理员验证该指纹——最好将其与通过安全的带外方法获得的已知值进行比较。但是，由于其复杂性，这种手动验证经常被跳过，增加了中间人(MitM)攻击的风险并削弱了SSH信任模型。

RFC 6187通过启用X.509v3基于证书的身份验证（将SSH与PKI集成）来解决这些问题。此方法允许通过可信证书颁发机构(CA)建立信任，提供类似于TLS的用户体验和信任模型，从而提高安全性和可扩展性。

配置

网络图



部署注意事项

- 需要与RFC6187兼容的SSH客户端才能利用此功能。
- SSH客户端和服务端协商支持的身份验证机制。设备上以前支持的所有身份验证机制可以继续与基于x509的身份验证机制同时运行，以确保平稳过渡。
- 管理员可以选择将基于x509的身份验证方法仅用于服务器、客户端或两者。
- 为了成功验证对方的身份验证数据，客户端和服务端只需要信任一个公共CA。这意味着只有签署路由器证书的CA证书必须安装在客户端设备受信任证书库上。
- 证书提供有关另一方身份的信息（公用名称和主题备用名称通常用于此目的）。客户端必须将作为管理员输入提供的服务器的主机名或IP地址名称与提供的证书中提供的身份数据进行比较。它严重限制了MitM或其他模拟攻击的机会。

配置

IOS-XE设备（SSH服务器）

配置保存CA证书和路由器证书 (可选) 的信任点。

```
crypto pki trustpoint pki-server
    enrollment pkcs12
    subject-name cn=RTR-DC01.cisco.com
    revocation-check none
    rsakeypair ssh-cert
```

```
! The username has to be fetched from the certificate for accounting and authorization purposes. Multip
    authorization username subjectname commonname
```

配置在SSH隧道协商期间使用的允许身份验证机制。

```
! Algorithms used to authenticate server
ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa

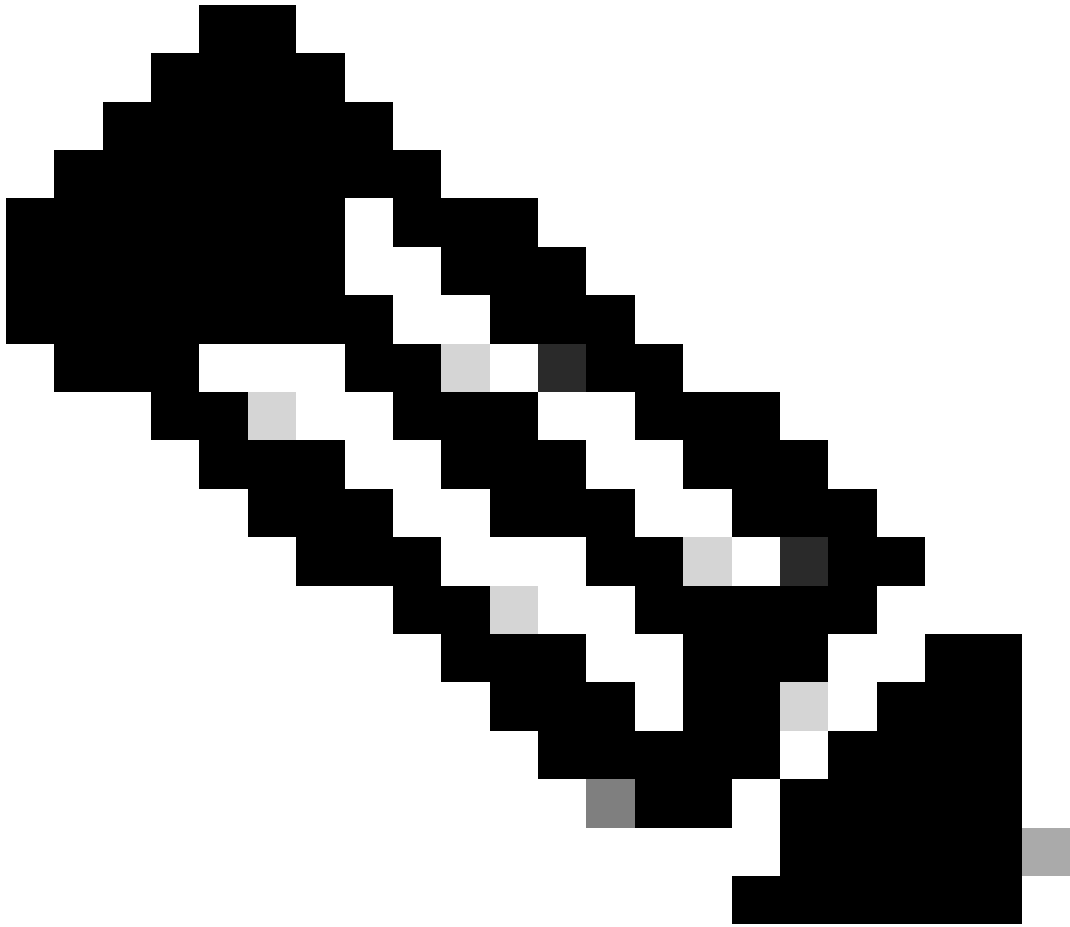
! Acceptable algorithms used to authenticate the client
ip ssh server algorithm authentication publickey password keyboard

! Acceptable pubkey-based algorithms used to authenticate the client
ip ssh server algorithm publickey x509v3-ssh-rsa ssh-rsa
```

配置SSH服务器以在身份验证过程中使用正确的证书。

```
ip ssh server certificate profile
server
    trustpoint sign

user
    trustpoint verify
```



注意：确保SSH服务器和SSH客户端具有由同一CA服务器颁发的ID证书。



注意：如果SSH客户端（例如Windows计算机）具有由其他某个CA颁发的ID证书，则将其导入到SSH服务器（即Cisco交换机）上，并将信任点映射到用户部分下的SSH服务器证书配置文件上方。

Pragma Fortress CL（安装在用户机器上的SSH客户端）

RTR-DC01.cisco.com

Authentication

Logging

Keyboard

Proxy

Serial

Telnet

Terminal

+ Ssh

+ Window

RTR-DC01.cisco.com

Site name:

RTR-DC01.cisco.com

Host address:

RTR-DC01.cisco.com

Host Alias:

Protocol:

ssh2

Port:

22

Comment:

Host address is the Hostname of the Cisco Device mentioned in the ID certificate issued to it by the CA server

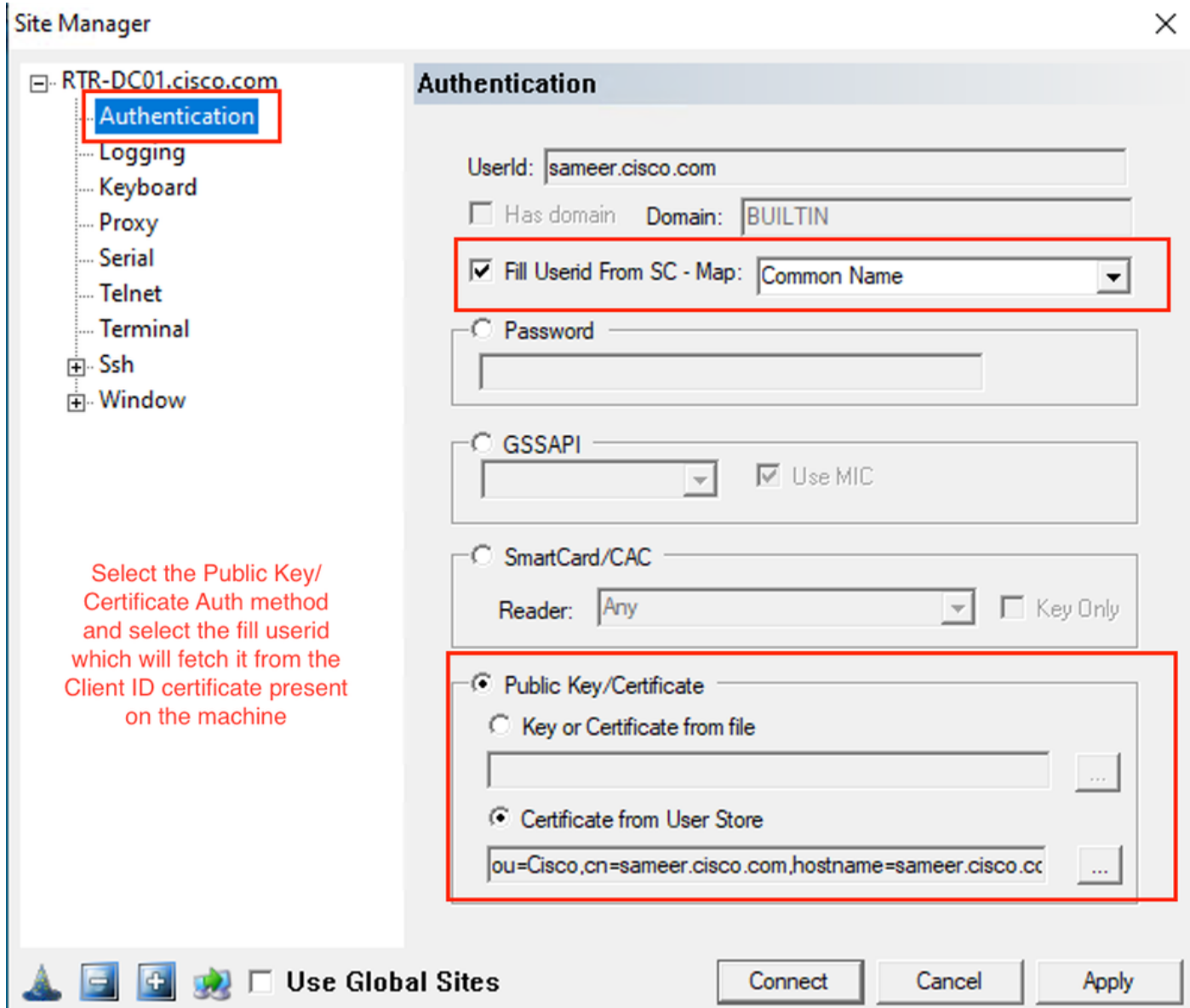


Use Global Sites

Connect

Cancel

Apply



验证

```
show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,password,keyboard-interactive
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
--- output truncated ---
```

```
show users
Line User Host(s) Idle Location
1 vty 0 sameer.cisco.com idle 00:02:37 192.168.1.100
```

故障排除

以下调试用于跟踪成功的会话：

debug ip ssh detail
debug crypto pki transactions
debug crypto pki messages
debug crypto pki validation

Mar 27 15:35:40.103: SSH1: starting SSH control process

! Server identifies itself

Mar 27 15:35:40.103: SSH1: sent protocol version id SSH-1.99-Cisco-1.25

! Client identifies itself

Mar 27 15:35:40.106: SSH1: protocol version id is - SSH-2.0-Pragma FortressCL 5.0.10.4176

! Authentication algorithms supported by server

Mar 27 15:35:40.106: SSH2 1: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-hellman

Mar 27 15:35:40.106: SSH2 1: kexinit sent: hostkey algo = x509v3-ssh-rsa,ssh-rsa

Mar 27 15:35:40.106: SSH2 1: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr

Mar 27 15:35:40.106: SSH2 1: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96

Mar 27 15:35:40.106: SSH2 1: SSH2_MSG_KEXINIT sent

Mar 27 15:35:40.109: SSH2 1: SSH2_MSG_KEXINIT received

Mar 27 15:35:40.109: SSH2 1: kex: client->server enc:aes256-ctr mac:hmac-sha2-256

Mar 27 15:35:40.109: SSH2 1: kex: server->client enc:aes256-ctr mac:hmac-sha2-256

! Client chooses authentication algorithm

Mar 27 15:35:40.109: SSH2 1: Using hostkey algo = x509v3-ssh-rsa

Mar 27 15:35:40.109: SSH2 1: Using kex_algo = diffie-hellman-group-exchange-sha1

Mar 27 15:35:40.109: SSH2 1: SSH2_MSG_KEX_DH_GEX_REQUEST received

Mar 27 15:35:40.109: SSH2 1: Range sent by client is - 1024 < 2048 < 8192

Mar 27 15:35:40.109: SSH2 1: Modulus size established : 2048 bits

Mar 27 15:35:40.121: SSH2 1: expecting SSH2_MSG_KEX_DH_GEX_INIT

Mar 27 15:35:40.121: SSH2 1: SSH2_MSG_KEXDH_INIT received

! SSH Server sends certificate associated with trustpoint "pki-server"

Mar 27 15:35:40.133: SSH2 1: Sending Server certificate associated with PKI trustpoint "pki-server"

Mar 27 15:35:40.133: SSH2 1: Got 2 certificate(s) on certificate chain

Mar 27 15:35:40.135: SSH2: kex_derive_keys complete

Mar 27 15:35:40.135: SSH2 1: SSH2_MSG_NEWKEYS sent

Mar 27 15:35:40.135: SSH2 1: waiting for SSH2_MSG_NEWKEYS

Mar 27 15:35:40.214: SSH2 0: channel window adjust message received 49926

Mar 27 15:35:41.417: SSH2 1: SSH2_MSG_NEWKEYS received

Mar 27 15:35:41.436: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive

Mar 27 15:35:41.437: SSH2 1: Using method = none

Mar 27 15:35:41.437: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive

Mar 27 15:35:41.438: SSH2 1: Using method = publickey

! Client sends certificate

Mar 27 15:35:41.438: SSH2 1: Received publickey algo = x509v3-ssh-rsa

Mar 27 15:35:41.438: SSH2 1: Verifying certificate for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQUEST

Mar 27 15:35:41.439: SSH2 1: Verifying certificate for user 'sameer.cisco.com'

Mar 27 15:35:41.439: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.439: SSH2 1: Received 0 ocsp-response

Mar 27 15:35:41.439: SSH2 1: Starting PKI session for certificate verification

! Client certificate is verified by the SSH-Server

Mar 27 15:35:41.444: SSH2 1: Verifying certificate for user 'sameer.cisco.com'

Mar 27 15:35:41.444: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.444: SSH2 1: Received 0 ocsp-response

Mar 27 15:35:41.444: SSH2 1: Starting PKI session for certificate verification

Mar 27 15:35:41.445: SSH2 1: Verifying signature for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQUEST

Mar 27 15:35:41.445: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.445: SSH2 1: Received 0 ocsp-response

! Certificate status verified successfully

```
Mar 27 15:35:41.446: SSH2 1: Client Signature verification PASSED
Mar 27 15:35:41.446: SSH2 1: Certificate authentication passed for user 'sameer.cisco.com'
Mar 27 15:35:41.446: SSH2 1: authentication successful for sameer.cisco.com
Mar 27 15:35:41.448: SSH2 1: channel open request
Mar 27 15:35:41.451: SSH2 1: pty-req request
Mar 27 15:35:41.451: SSH2 1: setting TTY - requested: height 25, width 80; set: height 25, width 80
Mar 27 15:35:41.452: SSH2 1: shell request
Mar 27 15:35:41.452: SSH2 1: shell message received
Mar 27 15:35:41.452: SSH2 1: starting shell for vty
Mar 27 15:35:41.464: SSH2 1: channel window adjust message received 9
Aug 21 20:07:32.311: CRYPTO_PKI: ip-ext-val: IP extension validation not required
```

常见问题

配置错误

用户的证书验证成功，但是，由于配置中缺少强制命令 `authorization username subjectname commonname`，用户的证书身份验证失败。

```
Apr 26 01:35:32.222: SSH1: starting SSH control process
Apr 26 01:35:32.222: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
Apr 26 01:35:32.224: SSH1: protocol version id is - SSH-2.0-Pragma FortressCL 5.0.10.4176
Apr 26 01:35:32.224: SSH2 1: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-hellman
Apr 26 01:35:32.224: SSH2 1: kexinit sent: hostkey algo = x509v3-ssh-rsa,ssh-rsa
Apr 26 01:35:32.224: SSH2 1: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr
Apr 26 01:35:32.224: SSH2 1: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-9
Apr 26 01:35:32.224: SSH2 1: SSH2_MSG_KEXINIT sent
Apr 26 01:35:32.234: SSH2 1: SSH2_MSG_KEXINIT received
Apr 26 01:35:32.234: SSH2 1: kex: client->server enc:aes256-ctr mac:hmac-sha2-256
Apr 26 01:35:32.235: SSH2 1: kex: server->client enc:aes256-ctr mac:hmac-sha2-256
Apr 26 01:35:32.235: SSH2 1: Using hostkey algo = x509v3-ssh-rsa
Apr 26 01:35:32.235: SSH2 1: Using kex_algo = diffie-hellman-group-exchange-sha1
Apr 26 01:35:32.235: SSH2 1: SSH2_MSG_KEX_DH_GEX_REQUEST received
Apr 26 01:35:32.235: SSH2 1: Range sent by client is - 1024 < 2048 < 8192
Apr 26 01:35:32.235: SSH2 1: Modulus size established : 2048 bits
Apr 26 01:35:32.246: SSH2 1: expecting SSH2_MSG_KEX_DH_GEX_INIT
Apr 26 01:35:32.246: SSH2 1: SSH2_MSG_KEXDH_INIT received
Apr 26 01:35:32.259: SSH2 1: Sending Server certificate associated with PKI trustpoint "pki-server"
Apr 26 01:35:32.259: CRYPTO_PKI: (A0049) Session started - identity selected (pki-server)
Apr 26 01:35:32.259: SSH2 1: Got 3 certificate(s) on certificate chain
Apr 26 01:35:32.259: CRYPTO_PKI: Rcvd request to end PKI session A0049.
Apr 26 01:35:32.260: CRYPTO_PKI: PKI session A0049 has ended. Freeing all resources.
Apr 26 01:35:32.260: CRYPTO_PKI: unlocked trustpoint pki-server, refcount is 0
Apr 26 01:35:32.273: SSH2: kex_derive_keys complete
Apr 26 01:35:32.274: SSH2 1: SSH2_MSG_NEWKEYS sent
Apr 26 01:35:32.274: SSH2 1: waiting for SSH2_MSG_NEWKEYS
Apr 26 01:35:45.664: SSH2 1: SSH2_MSG_NEWKEYS received
Apr 26 01:35:45.665: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive
Apr 26 01:35:45.666: SSH2 1: Using method = none
Apr 26 01:35:45.666: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive
Apr 26 01:35:45.675: SSH2 1: Using method = publickey
Apr 26 01:35:45.675: SSH2 1: Received publickey algo = x509v3-ssh-rsa
Apr 26 01:35:45.676: SSH2 1: Verifying certificate for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQ
Apr 26 01:35:45.676: SSH2 1: Verifying certificate for user 'sameer.cisco.com'
```

Apr 26 01:35:45.676: SSH2 1: Received a chain of 3 certificate
Apr 26 01:35:45.676: SSH2 1: Received 0 ocsrp-response
Apr 26 01:35:45.676: SSH2 1: Starting PKI session for certificate verification
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Session started - identity not specified
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (1249) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (1215) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (921) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: ip-ext-val: IP extension validation not required
Apr 26 01:35:45.677: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 37
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) validation path has 1 certs
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Check for identical certs
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Validating non-trusted cert
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Create a list of suitable trustpoints
Apr 26 01:35:45.677: CRYPTO_PKI: Found a issuer match
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Suitable trustpoints are: pki-server,
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Attempting to validate certificate using pki-server policy
Apr 26 01:35:45.677: CRYPTO_PKI: ECU validation successful. Cert matches configuration.
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Using pki-server to validate certificate
Apr 26 01:35:45.677: CRYPTO_PKI: Added 1 certs to trusted chain.
Apr 26 01:35:45.677: CRYPTO_PKI: Prepare session revocation service providers
Apr 26 01:35:45.677: CRYPTO_PKI: Deleting cached key having key id 50
Apr 26 01:35:45.677: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Apr 26 01:35:45.677: CRYPTO_PKI: Peer's public inserted successfully with key id 51
Apr 26 01:35:45.678: CRYPTO_PKI: Expiring peer's cached key with key id 51
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate is verified
Apr 26 01:35:45.678: CRYPTO_PKI: Remove session revocation service providers
Apr 26 01:35:45.678: CRYPTO_PKI: Remove session revocation service providers
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate validated without revocation check
Apr 26 01:35:45.678: CRYPTO_PKI: Populate AAA auth data
Apr 26 01:35:45.678: CRYPTO_PKI: Unable to get configured attribute for primary AAA list authorization.
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) chain cert was anchored to trustpoint pki-server, and chain val
Apr 26 01:35:45.678: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 37, ref
Apr 26 01:35:45.678: CRYPTO_PKI: ca_req_context released
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Validation TP is pki-server
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate validation succeeded
Apr 26 01:35:45.678: SSH2 1: Could not find username field configured for certificate in trustpoint Err
Apr 26 01:35:45.678: CRYPTO_PKI: Rcvd request to end PKI session A004A.
Apr 26 01:35:45.678: CRYPTO_PKI: PKI session A004A has ended. Freeing all resources.
Apr 26 01:35:45.679: SSH2 1: Can not decode the certificate Err code = 7
Apr 26 01:35:45.679: SSH2 1: Certificate authentication failed for user 'sameer.cisco.com'

相关信息

- [PKI配置指南](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。