

Cisco IOS XEデバイスでのSSH用の証明書認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[導入に関する考慮事項](#)

[コンフィギュレーション](#)

[IOS-XEデバイス \(SSHサーバ\)](#)

[Pragma Fortress CL \(ユーザマシンにインストールされたSSHクライアント \)](#)

[確認](#)

[トラブルシュート](#)

[一般的な問題](#)

[設定の誤り](#)

[関連情報](#)

はじめに

このドキュメントでは、RFC 6187で定義されているガイドラインに従って、X.509v3証明書を認証に使用するCisco IOS® XEデバイスでのセキュアシェル(SSH)の設定について説明します。

前提条件

要件

公開キーインフラストラクチャ(PKI)インフラストラクチャに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS XEバージョン17.3.5を実行するC9200Lスイッチ
- Pragma Fortress SSH クライアント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください

背景説明

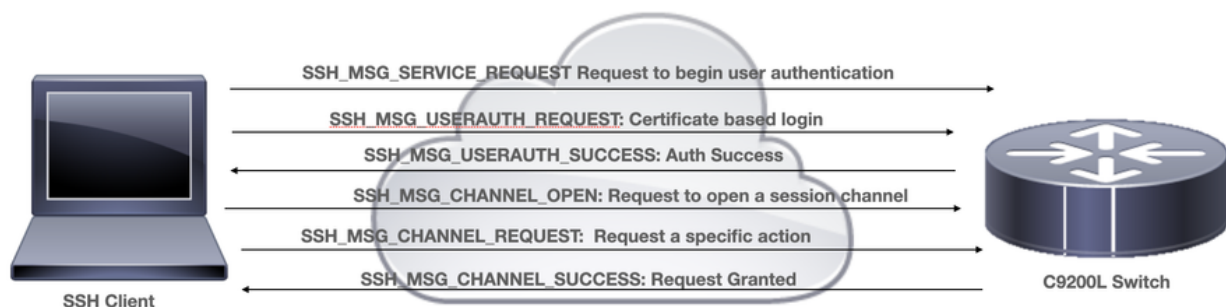
このアプローチでは、証明書ベースの認証を有効にすることでSSHセキュリティが強化され、SSHキー管理の方法がTransport Layer Security(TLS)で使用方法とより密接に連携します。

SSHは、クライアントとサーバの間でセキュアな接続を確立するために、相互認証を提供します。従来、サーバはRivest-Shamir-Addleman(RSA)キーペアを使用して認証を行っていました。クライアントはサーバの公開キーのフィンガープリントを計算し、管理者に確認を求めます。理想的には、これを安全なアウトオブバンド方式で取得した既知の値と比較します。ただし、この手動による検証は、複雑さが原因でスキップされることが多く、Man-in-the-Middle(MitM)攻撃のリスクが高まり、SSH信頼モデルが弱体化します。

RFC 6187では、SSHとPKIを統合するX.509v3証明書ベースの認証を有効にすることで、これらの問題に対処しています。このアプローチでは、信頼された認証局(CA)を通じて信頼を確立し、TLSと同様のユーザエクスペリエンスと信頼モデルを提供することで、セキュリティとスケーラビリティを向上させます。

設定

ネットワーク図



導入に関する考慮事項

- この機能を利用するには、RFC6187互換のSSHクライアントが必要です。
- SSH クライアントおよびサーバは、サポートされている認証メカニズムをネゴシエートします。デバイスで以前にサポートされていたすべての認証メカニズムは、移行を円滑にするために、x509ベースの認証メカニズムと同時に実行し続けることができます。
- 管理者は、x509ベースの認証方式をサーバのみ、クライアントのみ、またはその両方に使

用できます。

- 相手側の認証データを正しく確認するために必要なのは、クライアントとサーバが共通のCAを信頼することだけです。これは、ルータ証明書に署名したCAの証明書のみがクライアントデバイスの信頼できる証明書ストアにインストールされる必要があることを意味します。
- 証明書は、相手側のアイデンティティに関する情報を提供します（一般に、共通名とサブジェクト代替名がこの目的に使用されます）。クライアントは、管理者によって入力されたサーバのホスト名またはIPアドレス名と、提示された証明書で使用可能なIDデータを比較する必要があります。これにより、MitMやその他のなりすまし攻撃の機会が大幅に制限されます。

コンフィギュレーション

IOS-XEデバイス (SSHサーバ)

CA 証明書とルータ証明書 (オプション) を保持するトラストポイントを設定します。

```
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
```

SSHトンネルネゴシエーション中に使用される、設定許可認証メカニズム。

! 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

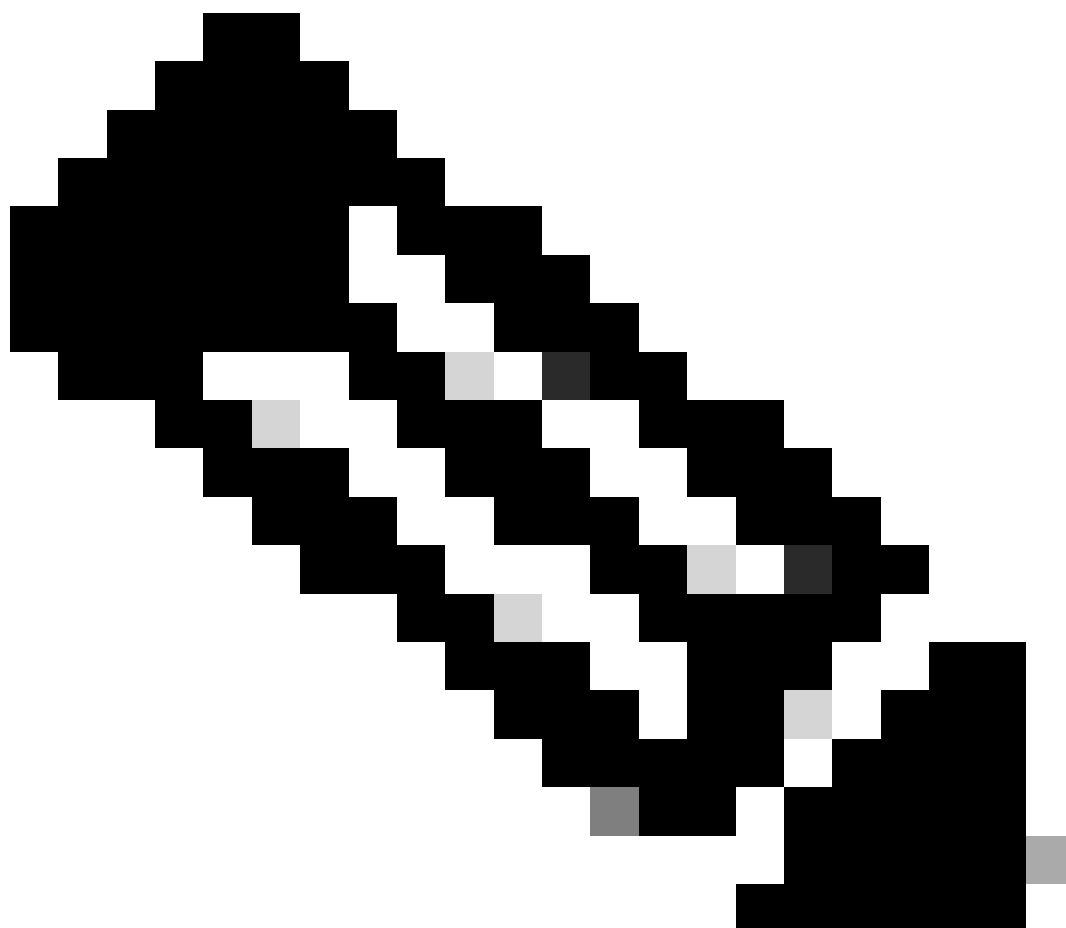
```
ip ssh server algorithm publickey x509v3-ssh-rsa ssh-rsa
```

認証プロセスで正しい証明書を使用するようにSSHサーバを設定します。

```
ip ssh server certificate profile  
server
```

trustpoint sign

user
trustpoint verify



注:SSHサーバとSSHクライアントに、同じCAサーバによって発行されたID証明書があることを確認してください。



注:WindowsマシンなどのSSHクライアントに他のCAによって発行されたID証明書がある場合、その証明書をSSHサーバ、つまりCisco Switchにインポートし、ユーザセクションでトラストポイントをSSHサーバ証明書プロファイルの上にマッピングします。

Pragma Fortress CL (ユーザマシンにインストールされたSSHクライアント)

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

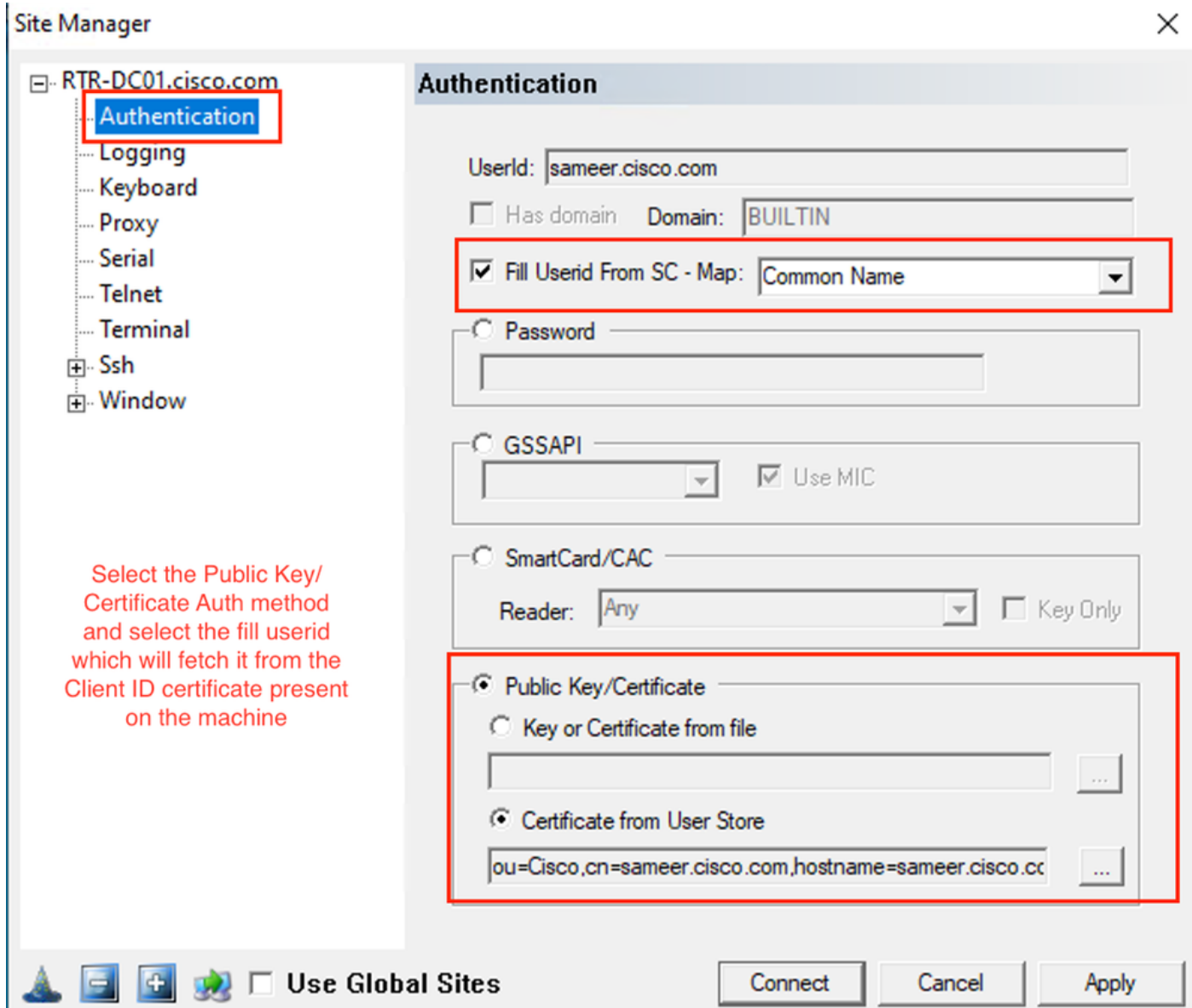


Use Global Sites

Connect

Cancel

Apply



確認

```
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
```

トラブルシューティング

成功したセッションを追跡するには、次のデバッグを使用します。

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
```

一般的な問題

設定の誤り

ユーザの証明書検証は成功しますが、設定に必須コマンド `authorization username subjectname commonname` が指定されていないため、ユーザの証明書認証は失敗します。

```
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-sha1-96
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_REQUEST
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'

関連情報

- [PKI設定ガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。