

Cisco IOS XE 디바이스에서 SSH를 위한 인증서 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[구축 고려 사항](#)

[설정](#)

[IOS-XE 디바이스\(SSH 서버\)](#)

[Pragma Fortress CL\(사용자 시스템에 설치된 SSH 클라이언트\)](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반적인 문제](#)

[컨피그레이션 오류](#)

[관련 정보](#)

소개

이 문서에서는 RFC 6187에 정의된 지침에 따라 인증을 위해 X.509v3 인증서를 사용하는 Cisco IOS® XE 디바이스의 SSH(Secure Shell) 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

PKI(Public Key Infrastructure) 인프라에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS XE 버전 17.3.5를 실행하는 C9200L 스위치
- Pragma Fortress SSH 클라이언트

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다

배경 정보

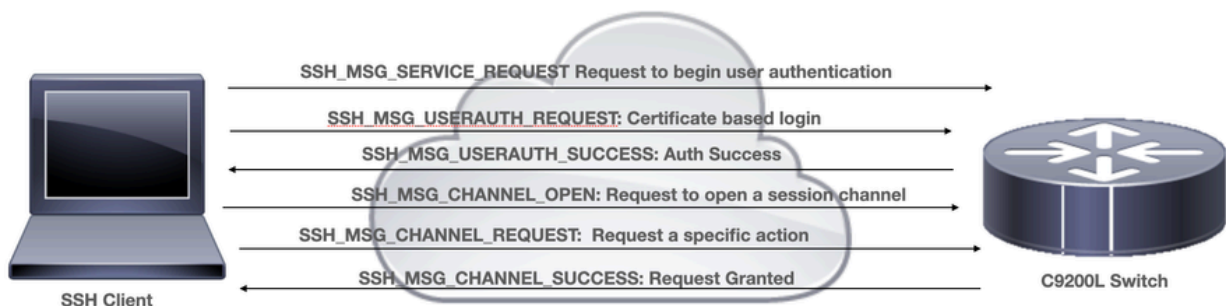
이 접근 방식은 인증서 기반 인증을 활성화하여 SSH 보안을 강화함으로써 SSH 키 관리 방식을 TLS(Transport Layer Security)에 사용되는 방식과 더욱 긴밀하게 연계합니다.

SSH는 클라이언트와 서버 간의 보안 연결을 설정하기 위해 상호 인증을 제공합니다. 일반적으로 서버는 RSA(Rivest-Shamir-Addleman) 키 쌍을 사용하여 인증합니다. 클라이언트는 서버의 공개 키의 핑거프린트를 계산하고 관리자에게 확인 메시지를 보냅니다. 이는 안전한 대역 외 방법을 통해 얻은 알려진 값과 비교하는 것이 가장 좋습니다. 그러나 이 수동 검증은 복잡성 때문에 건너뛰고 MitM(man-in-the-middle) 공격의 위험을 높이며 SSH 신뢰 모델을 약화시키는 경우가 많습니다.

RFC 6187은 SSH를 PKI와 통합하는 X.509v3 인증서 기반 인증을 활성화하여 이러한 문제를 해결합니다. 이 접근 방식은 신뢰할 수 있는 CA(Certificate Authority)를 통해 신뢰를 설정할 수 있도록 함으로써 TLS와 유사한 사용자 환경과 신뢰 모델을 제공함으로써 보안과 확장성을 향상시킵니다.

구성

네트워크 다이어그램



구축 고려 사항

- 이 기능을 사용하려면 RFC6187 호환 SSH 클라이언트가 필요합니다.
- SSH 클라이언트 및 서버는 지원되는 인증 메커니즘을 협상합니다. 디바이스에서 이전에 지원되었던 모든 인증 메커니즘은 원활한 전환을 위해 x509 기반 인증 메커니즘과 동시에 계속 실행될 수 있습니다.
- 관리자는 x509 기반 인증 방법을 서버 전용, 클라이언트 전용 또는 둘 모두에 사용하도록 선택할 수 있습니다.
- 상대방의 인증 데이터를 성공적으로 확인하려면 클라이언트와 서버가 공통 CA만 신뢰하면 됩니다. 즉, 라우터 인증서를 서명한 CA의 인증서만 클라이언트 디바이스의 신뢰할 수 있는 인증서 저장소에 설치해야 합니다.

- 인증서는 상대방의 ID에 대한 정보를 제공합니다(일반적으로 Common Name 및 Subject Alternative Name이 해당 용도로 사용됨). 클라이언트는 관리자가 입력으로 제공한 서버의 호스트 이름 또는 IP 주소 이름을 제공된 인증서에서 사용 가능한 ID 데이터와 비교해야 합니다. MitM 또는 다른 가장 공격의 기회를 심각하게 제한합니다.

설정

IOS-XE 디바이스(SSH 서버)

CA 인증서 및 선택적으로 라우터 인증서를 보유하는 신뢰 지점을 구성합니다.

```
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 터널 협상 중에 사용되는 허용되는 인증 메커니즘을 구성합니다.

! 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
```

인증 프로세스에서 올바른 인증서를 사용하도록 SSH 서버를 구성합니다.

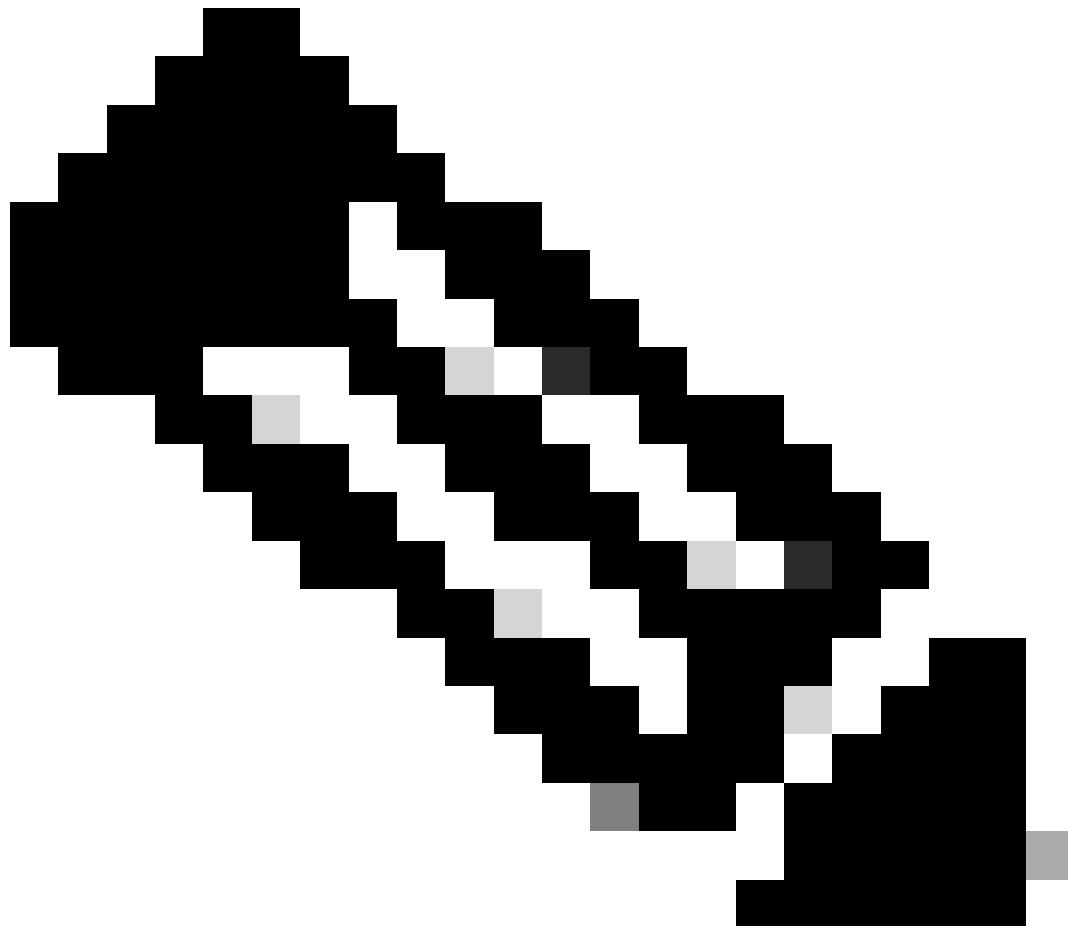
```
ip ssh server certificate profile
```

```
server
```

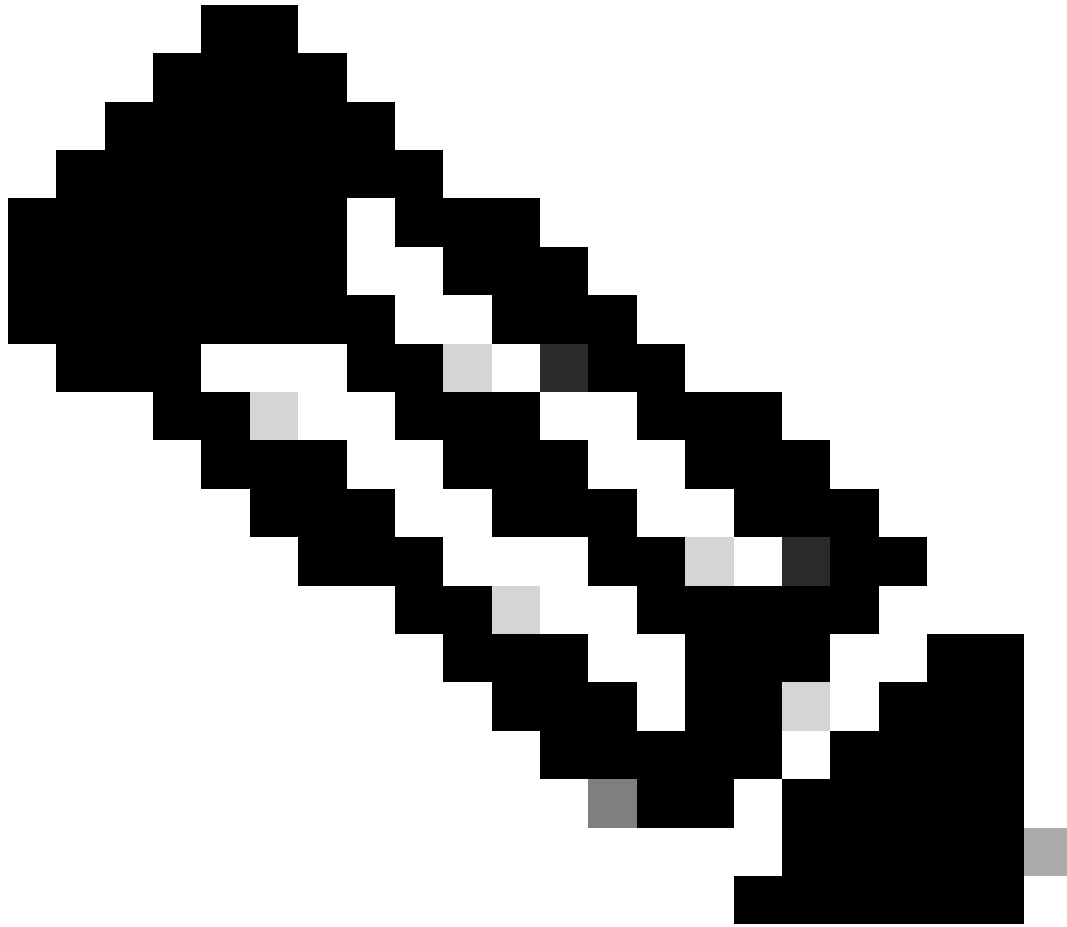
```
trustpoint sign
```

```
user
```

```
trustpoint verify
```



참고: SSH 서버와 SSH 클라이언트에 동일한 CA 서버에서 발급한 ID 인증서가 있는지 확인합니다.



참고: Windows 시스템과 같은 SSH 클라이언트에 다른 CA에서 발급한 ID 인증서가 있는 경우, SSH 서버, 즉 Cisco 스위치에서 가져온 인증서를 가져오고 사용자 섹션의 위 SSH 서버 인증서 프로필에 신뢰 지점을 매핑합니다.

Pragma Fortress CL(사용자 시스템에 설치된 SSH 클라이언트)

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:

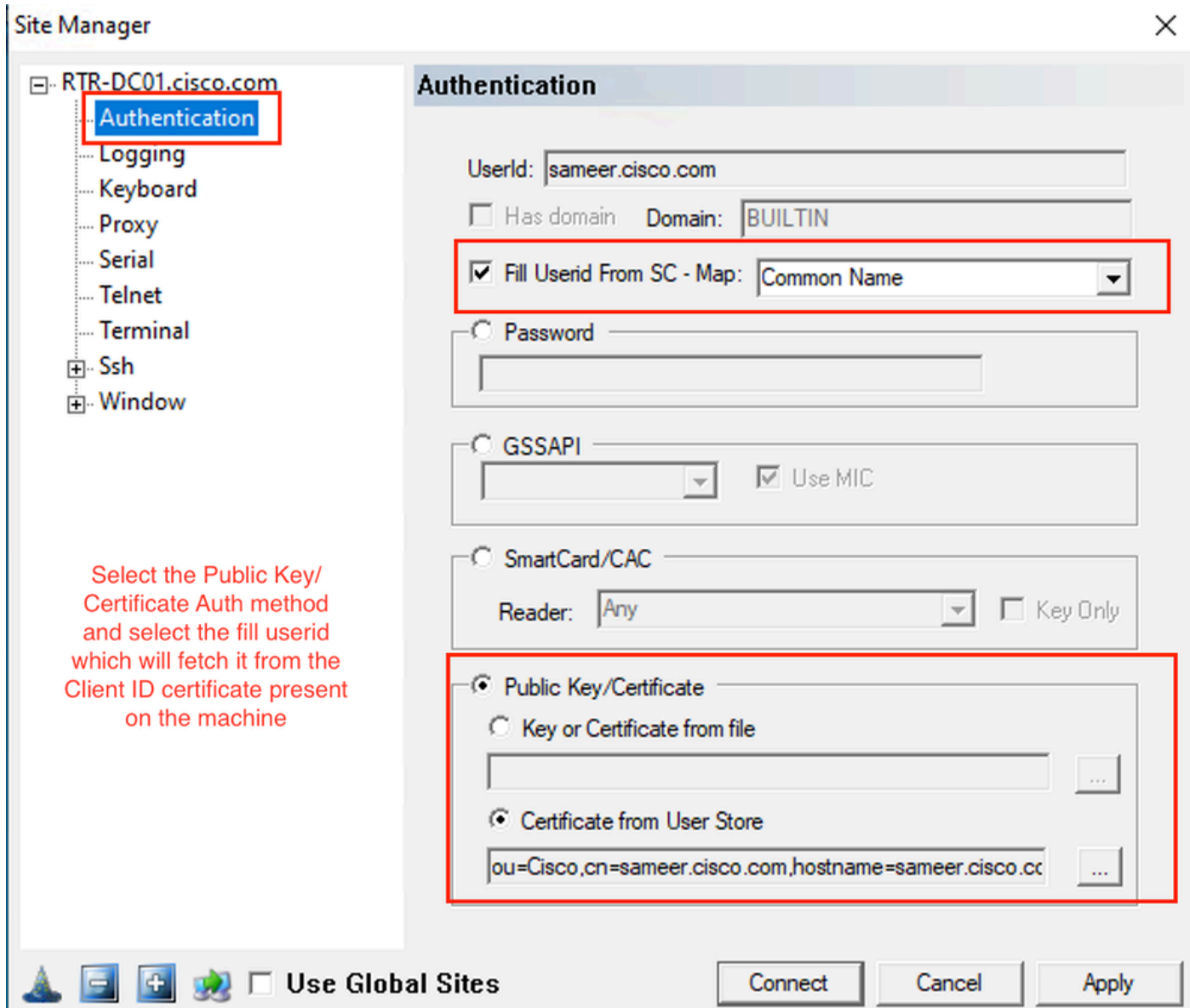
Host address is the Hostname of the Cisco Device mentioned in the ID certificate issued to it by the CA server

☐ Use Global Sites

Connect

Cancel

Apply



다음을 확인합니다.

```
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
```

문제 해결

이러한 디버그는 성공적인 세션을 추적하기 위해 사용됩니다.

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
```

일반적인 문제

컨피그레이션 오류

사용자에 대한 인증서 검증에 성공했지만 컨피그레이션에 필수 명령 권한 부여 사용자 이름 subjectname commonname이 없기 때문에 사용자에게 대한 인증서 인증이 실패합니다.

```
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 oosp-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'

관련 정보

- [PKI 컨피그레이션 가이드](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.