Using Two-Factor Authentication Configuration to Combat Cybersecurity Threats

Guidelines for Deploying Cisco IOS SSH with X.509v3 PIV and CAC Smartcards

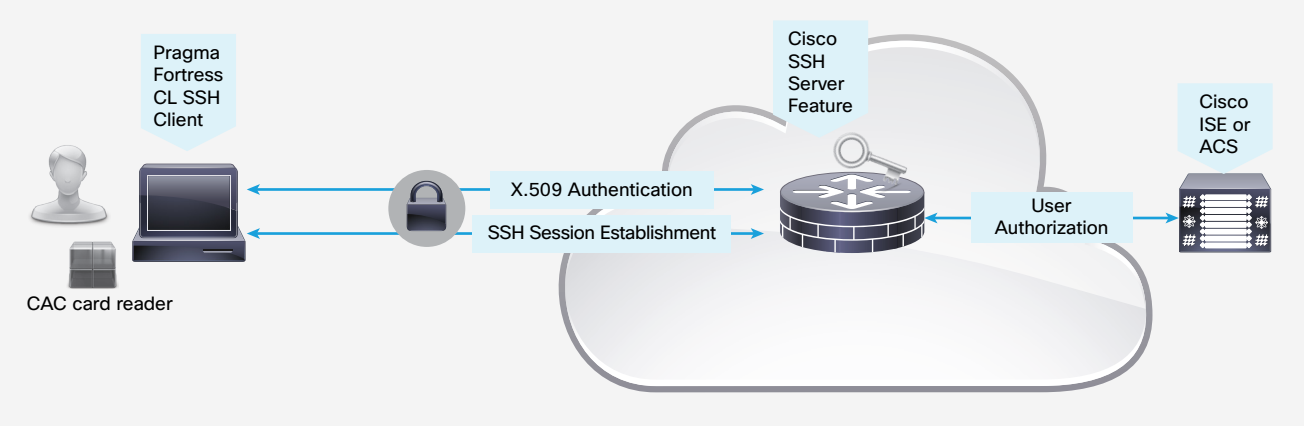
Contents

Introduction

Cybersecurity threats continue to evolve, compromising sensitive and confidential information across the network. To combat this threat, enterprises are taking mitigating actions to strengthen device access across their critical IT infrastructure. Two-factor authentication can significantly reduce the risk of adversaries penetrating strategic networks and systems. This approach requires the use of a Personal Identity Verification (PIV) card or Common Access Card (CAC). In this document, we will detail the basic procedures required to enable two-factor authentication for the Secure Shell Protocol (SSH) using government-issued PIV or CAC cards.

Figure 1 illustrates this process.

Figure 1. Two-Factor Authentication Using SSH



Requirements

Table 1 shows the Cisco® product families that support the X.509v3 certificates for the SSH authentication feature. The versions of Cisco IOS® Software shown in the table, or later, are recommended. These releases include the bug fixes identified in the next section.

Table 1. Recommended Cisco IOS Software Releases

Product Family	Cisco IOS Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) (1900, 2900, or 3900 Series)	Cisco IOS 15.5(3)M2 or later
Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE 3.16.2 S or later
Cisco 4000 Series ISRs	Cisco IOS XE 3.16.2 S or later
Cisco Cloud Services Router (CSR) 1000V Series	Cisco IOS XE 3.16.2 S or later
Cisco Catalyst® 2000, 3000, and 4000 Series Switches	Cisco IOS 15.2(4)E1 or later
Cisco Catalyst 3850 Series Switches	Cisco IOS XE 16.1.2 or later
Cisco Catalyst 3650 Series Switches	Cisco IOS XE 16.1.2 or later

Pragma Fortress CL SSH Client (version 5, build 10, rev 292 or later)

You can purchase or download a 14-day trial from http://www.pragmasys.com/ssh-client/download.

Department of Defense (DoD) CA certificates
Note for DoD customers: You can obtain the CA certificate here:
http://dodpki.c3pki.chamb.disa.mil/rootca.html

Cisco Identity Services Engine (ISE) 2.0 or Cisco Secure Access Control Server (ACS)

DoD CAC card or PIV card for civilian agencies

Smartcard reader

Resolved Bugs

The following defects have been resolved:

CSCuv89417: Cisco IOS SSH not prompting user PIN for verifying signature from client with X.509 certificate-based authentication.

CSCuw91205: PKI needs support for UPN extraction using OID.

Cisco IOS Software Configuration

1. Set up Network Time Protocol (NTP) with the proper time zone for the device This step is critical for the operation of the public key infrastructure (PKI).

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
clock timezone EST -5 0
clock summer-time EDT recurring
ntp server 192.5.41.40
```

Configure PKI trustpoint for the certificate authority (CA). Specify the field from the user certificate that will be used as the SSH username that will pass to the TACACS server for authorization. The example below uses the common name from the subnet field for the username. The user principal name (UPN) from the Subject-Alternative name can also be used as a username for SSH login.

```
crypto pki trustpoint CA2
 enrollment terminal
 revocation-check none
 authorization username subjectname commonname
```

2. Manually authenticate and install the root CA's public certificate. It is not necessary to install the subordinate CA's certificate if the user's computer has the proper DoD certificate chain installed. See the Troubleshooting section for a screenshot example of the DoD certificate chain.

```
Router(config)#crypto pki authenticate CA2

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDcDCCAligAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJVUzEY
MBYGA1UEChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsT
…<snip>
tX3h4NGW56E6LcyxnR8FRO2HmdNNGnA5wQQM5X7Z8a/XIA7xInolpHOZzD+kByeW
qKKV7YK5FtOeC4fCwfKI9WLfaN/HvGlR7bFc3FRUKQ8JOZqsA8HbDE2ubwp6Fknx
v5HSOJTT9pUst2zJQraNypCNhdk=
-----END CERTIFICATE-----

Certificate has the following attributes:
    Fingerprint MD5: 477892DB 8AEC1B53 68F01D00 9C34775E
    Fingerprint SHA1: 8C941B34 EA1EA6ED 9AE2BC54 CF687252 B4C9B561

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

3. Generate RSA signing and encryption keys for the SSH server.

```
Router(config)#crypto key generate rsa modulus 2048 label SSH-RSA usage-keys
The name for the keys will be: SSH-RSA

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
```

4. Enable the SSH server and specify the RSA keys to be used for signing and encryption.

```
ip ssh rsa keypair-name SSH-RSA
ip ssh version 2
```

5. Specify the number of authentication retries and the timeout interval for the SSH server (optional).

```
ip ssh time-out 60
ip ssh authentication-retries 2
```

6. Configure the Cisco IOS SSH server to verify the user's X.509v3 digital credential for two-factor authentication.

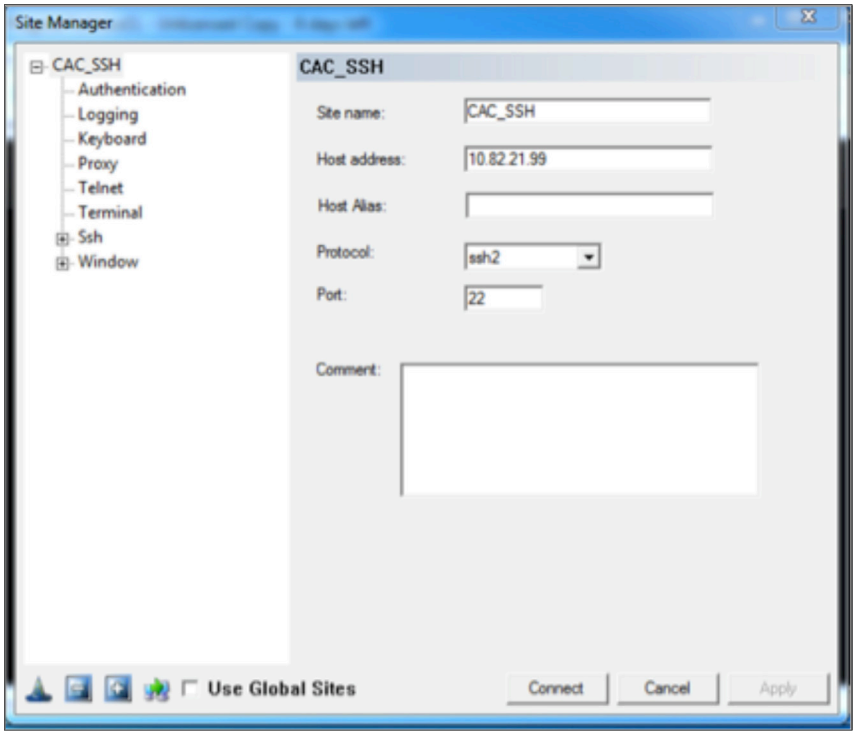
```
ip ssh server certificate profile
user
  trustpoint verify CA2
ip ssh server algorithm hostkey ssh-rsa
ip ssh server algorithm authentication publickey
ip ssh server algorithm publickey x509v3-ssh-rsa
```

7. Enable SSH for terminal line access, and enable X.509v3 validation.

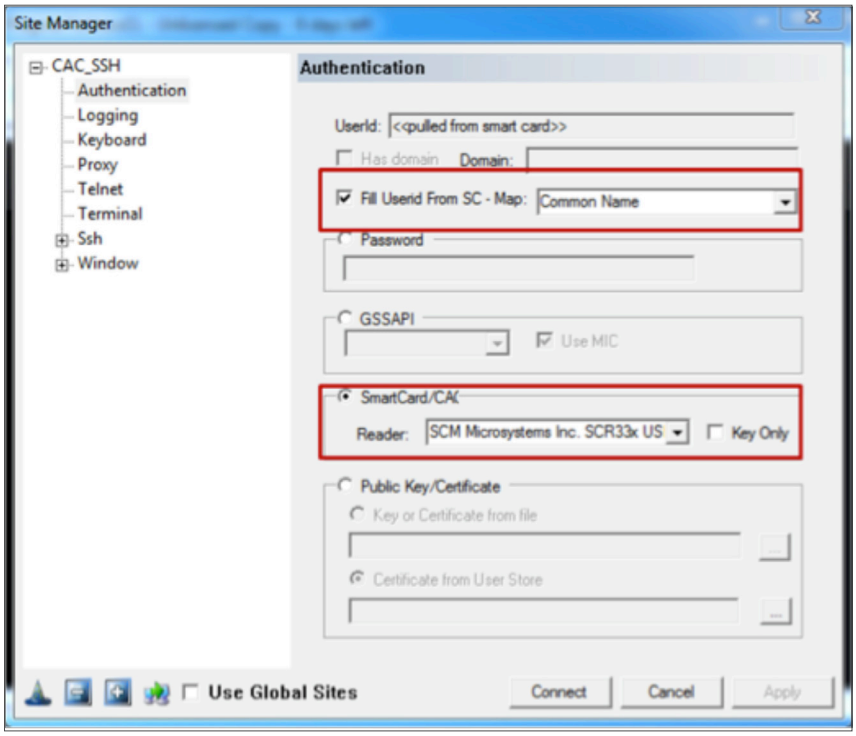
```
aaa new-model
!
line vty 0 4
login
transport input ssh
```

SSH Client Setup

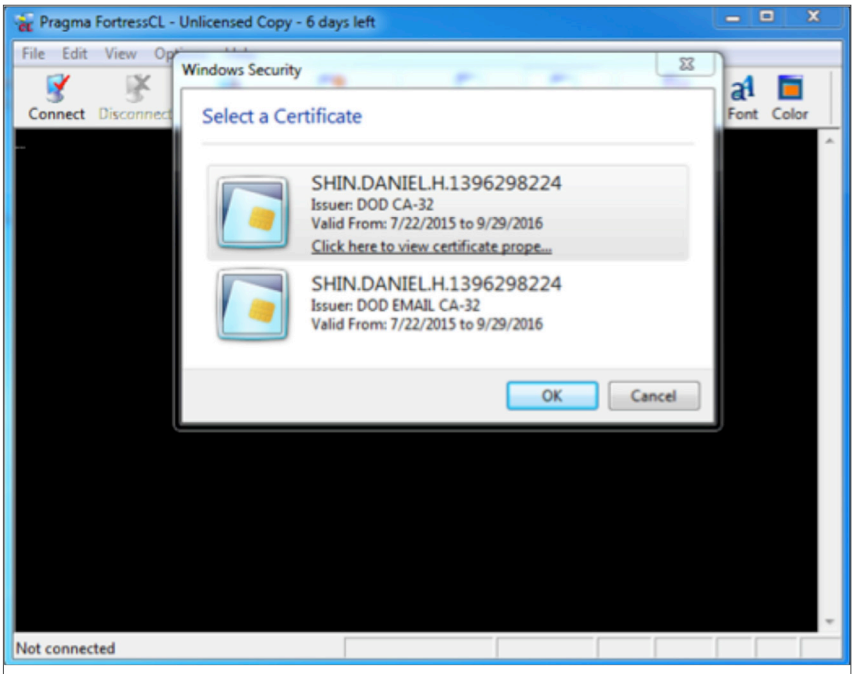
1. Start up the Pragma Fortress CL SSH client (FortressCL.exe), and enter the Site Name and Host Address. Select ssh2 as the protocol.



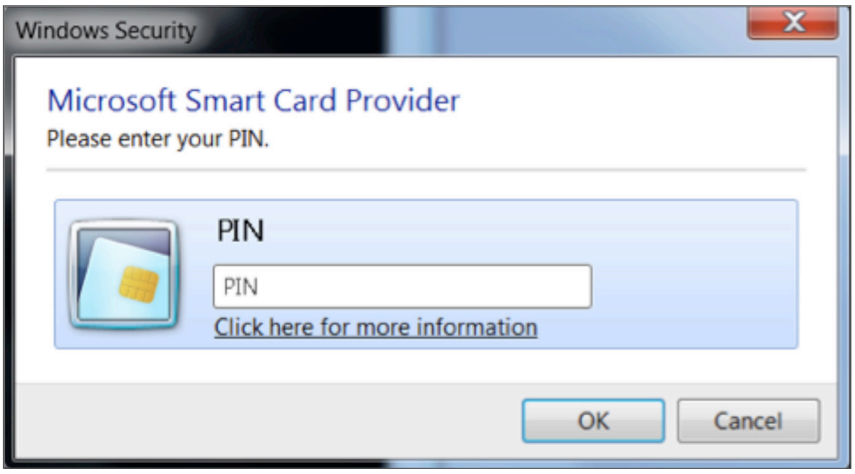
2. Select **Authentication** from the left panel. Click **SmartCard/CAC.** Check the **Fill UserID from SC** box, and select the field (Common Name or Principal Name) to use as the user ID. DO NOT check the **Key Only** box. Click **Connect.**



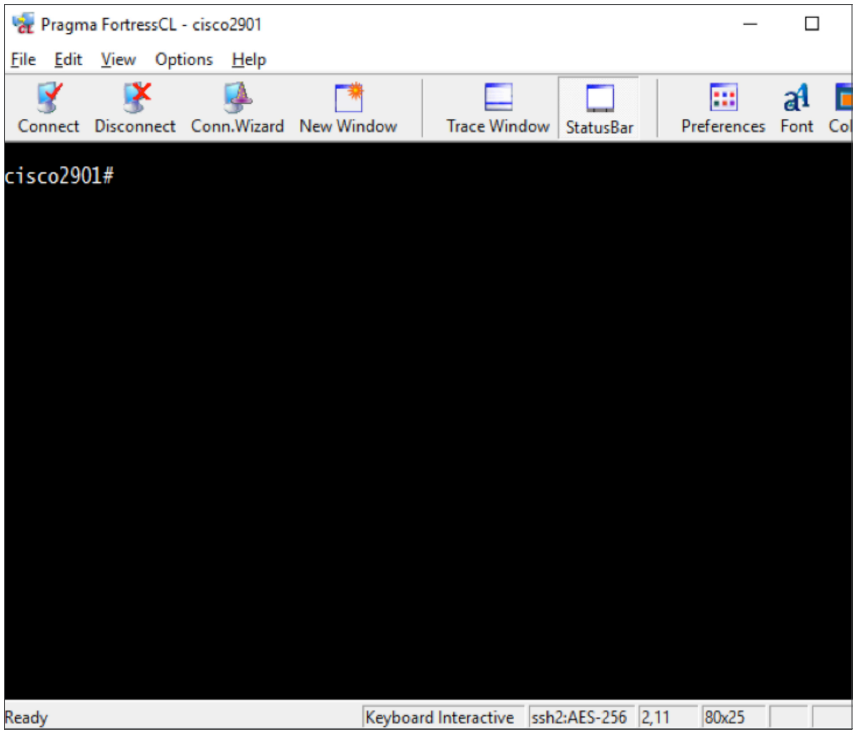
3. Select the proper user certificate from the CAC card in the popup window..



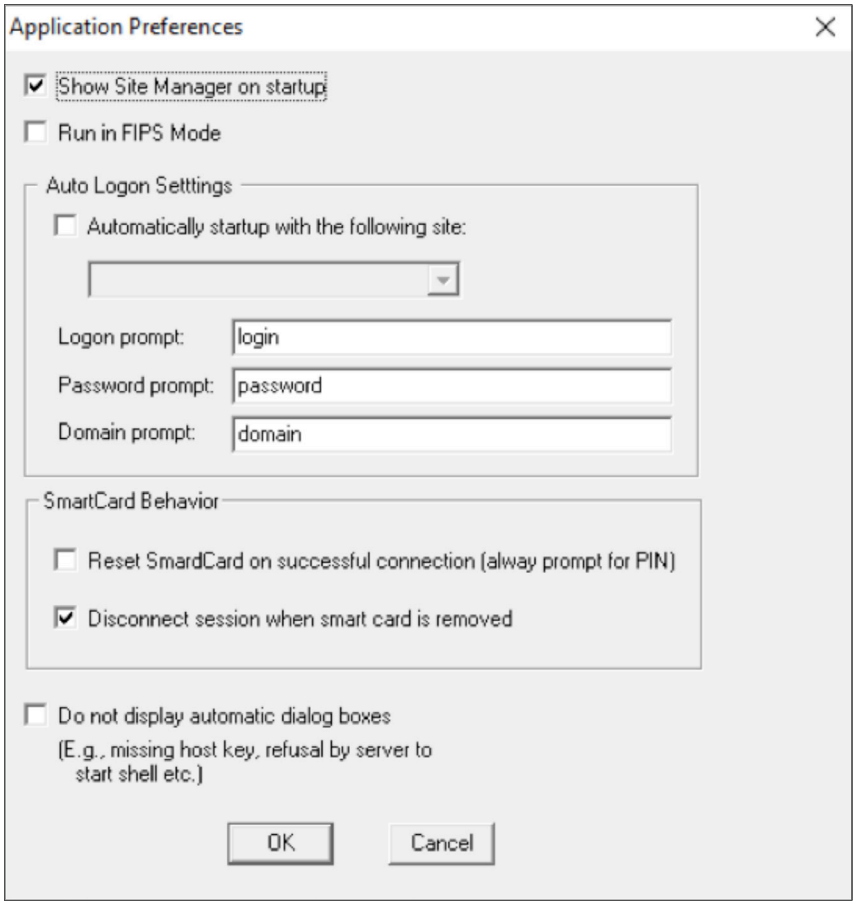
4. Enter the PIN associated with the smartcard credential.



5. You are now at the router prompt.



6. (Optional) There are two settings that govern smartcard/CAC behavior. These settings are in the **Application Preferences** dialog, which can be invoked from the **Options** menu.



The two options are:

1. Reset SmartCard on successful connection (always prompt for PIN). This option will reset the smartcard after successfully connecting, clearing the PIN cache.
2. Disconnect session when smart card is removed. This option will monitor the smartcard and will disconnect the session if the card is removed.

These values can also be set by a domain policy, using the following registry value:

HKEY_CURRENT_USER\SOFTWARE\Pragma Systems\Pragma FortressCL\Preferences\SCardReset	DWORD	1 – Enabled 0 – Disabled
HKEY_CURRENT_USER\SOFTWARE\Pragma Systems\Pragma FortressCL\Preferences\SCardMonitor	DWORD	1 – Enabled 0 – Disabled

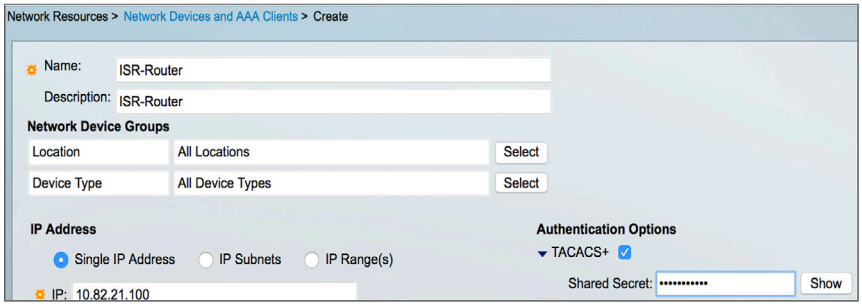
TACACS+ Authorization Setup

This section includes ISE 2.0 and ACS 5.x authentication, authorization, and accounting (AAA) setup procedures. Choose from one of the options for AAA server setup, depending on the AAA method used.

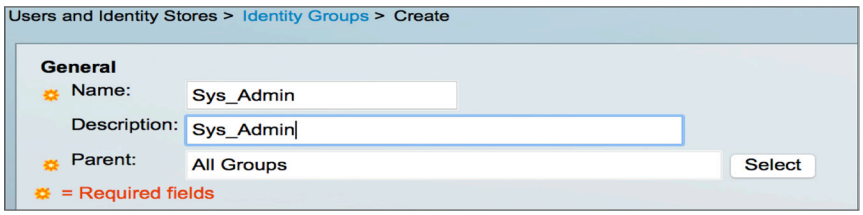
Cisco ACS 5.x Configuration (Option 1)

The following procedures outline the ACS 5.x or later TACACS+ configuration to support PKI AAA integration for SSH login.

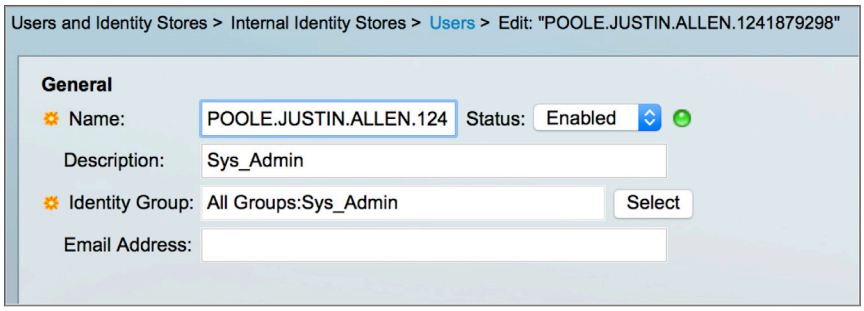
1. Configure the TACACS+ authentication settings for a network device. **In ACS, go to Network Resources > Network Device Groups > Network Devices and AAA Clients > Create**. Enter the device information and shared secret.



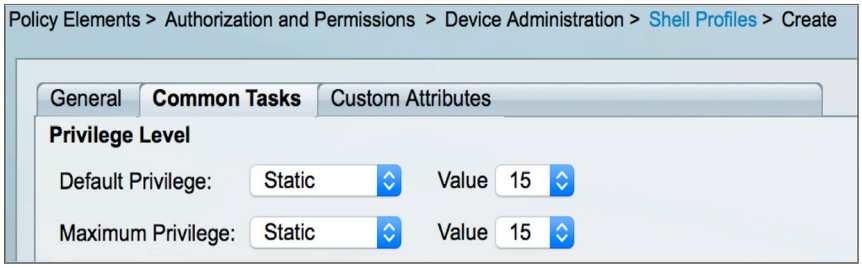
2. Create user identity groups for the various user groups. In ACS, go to **Users and Identity Stores > Identity Groups > Create**. Create a System Administration group.



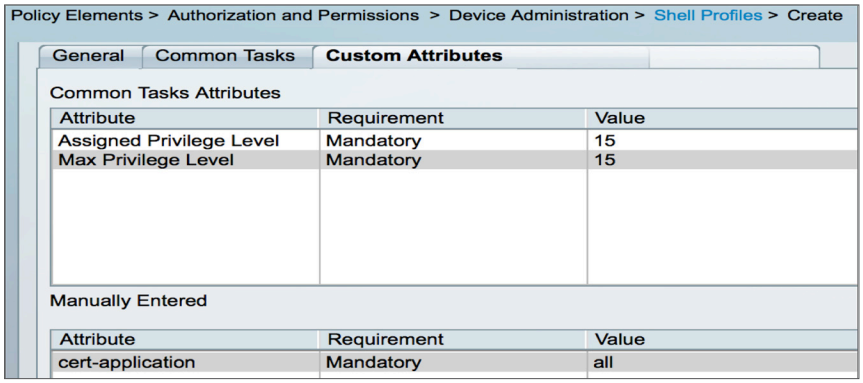
3. Create the users and include them in the proper user identity group. In ACS, go to **Users and Identity Stores > Internal Identity Stores > Users > Create**. The Name field is case sensitive and must match the field from the certificate exactly (for example, the common name, UPN). The password configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication). Select the user group from the list previously configured for the user.



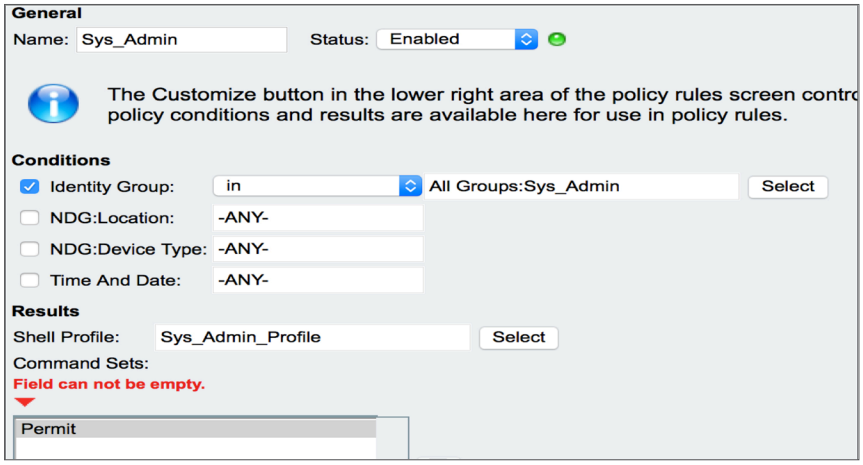
4. Define the shell profile for the System Administrator group. In ACS, go to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create**. Enter the Name. Under Common Tasks, set the **Default Privilege** and **Maximum Privilege** for the System Administrator profile.



5. Select the **Custom Attributes** tab, and add the following Cisco-av-pair to the profile: **"cert-application=all"**. This is needed for AAA integration with the PKI service to authorize the particular user or user group. The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.



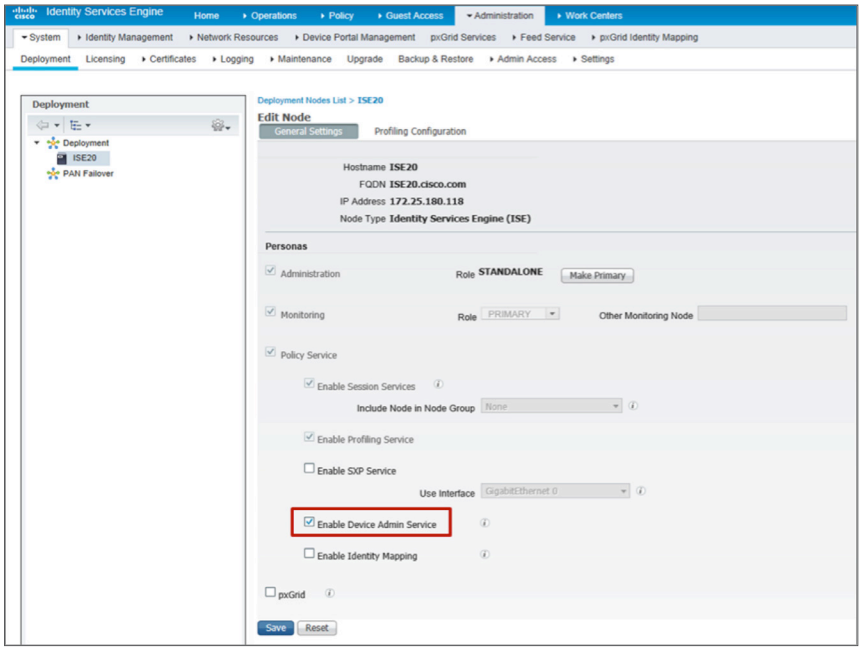
6. Create the device authorization policy for the System Administrator group. In ACS, go to **Access Policies > Access Services > Default Device Admin > Authorization > Create**. Name the rule, reference the identity group previously created, select the System Administrator shell profile, and select or create the command set required



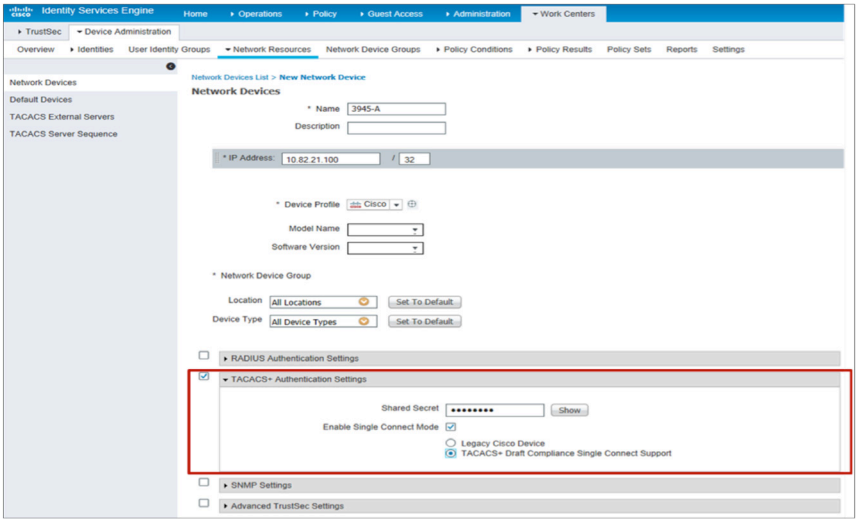
Cisco ISE 2.0 Configuration (Option 2)

The following procedures outline the ISE 2.0 or later TACACS+ configuration to support PKI AAA integration for SSH login.

1. Enable TACACS+ operation on the ISE 2.0 server. Go to the **Administration > System > Deployment > General Settings** page and check the **Enable Device Admin Servic**e check box. Click Save to **save** the configuration.

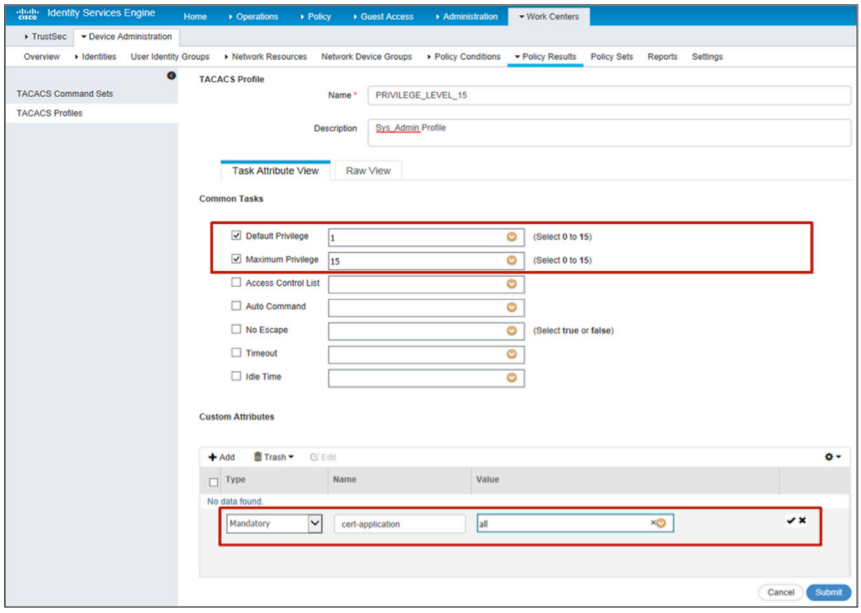


2. Configure the TACACS+ authentication settings for a network device. Go to **Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS+ Authentication Settings**. Enter the device information and shared secret.

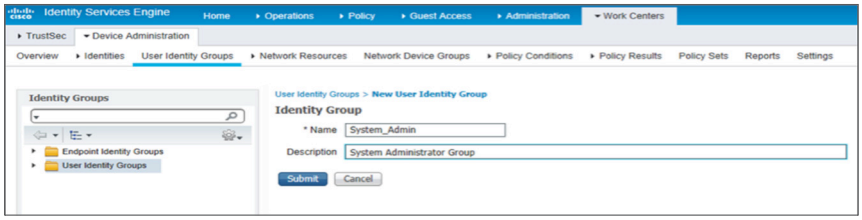


3. Define the TACACS+ profile for System Administrator. Go to **Work Centers > Device Administration > Policy Results > TACACS Profiles > Add**. Enter the **Name** and the **Default Privilege** and **Maximum Privilege** for the System Administrator profile.

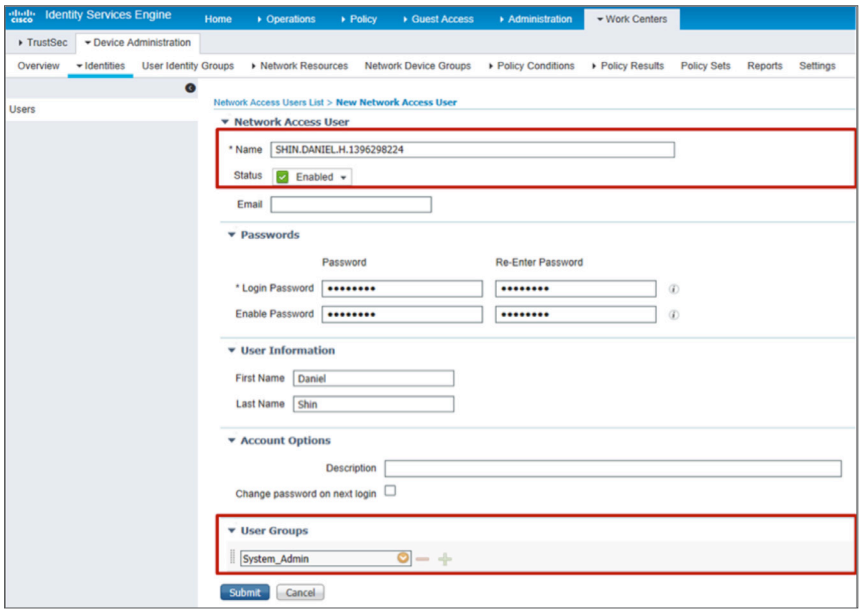
   On the same page, under **Custom Attributes**, add the following Cisco-av-pair to the profile: **"cert-application=all".** This is needed for AAA integration with the PKI service to authorize the particular user or user group. The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.



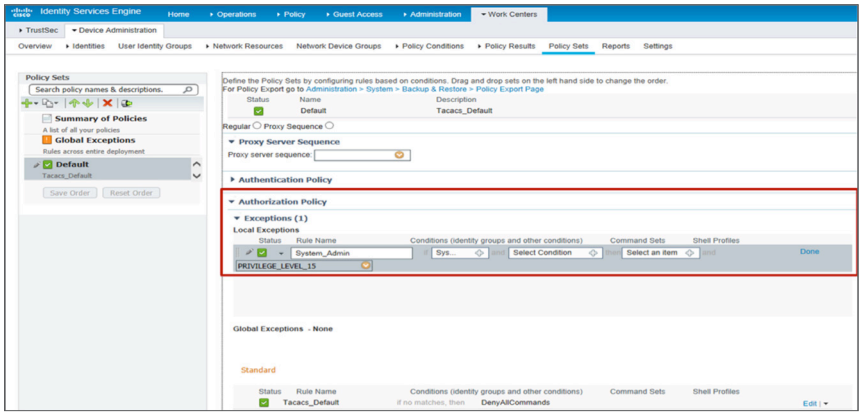
4. Create user identity groups for the various user groups. Go to **Work Centers > Device Administration > User Identity Groups > Add**. Add the user groups for role-based access; for example, System Admin, Helpdesk, and more.



5. Create the member users and include them in the proper user identity group. Go to **Work Centers > Device Administration > Identities > Users**. The Name field is case sensitive and must match the field from the certificate exactly (for example, the common name, UPN). The password configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication). Select the user group from the list previously configured for the user.



6. Add TACACS policy for the user group defined. Go to **Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Exceptions > Create a New Rule**. Enter the name of the rule (for example, System_Admin), select a condition (User Identity Group > System_Admin), and then select shell profiles (e.g. PRIVILEGE_LEVEL_15). Click the **Save** button at the bottom of the page.



Cisco IOS Configuration (Mandatory)

1. Add the TACACS+ server and provision the shared secret and IP address of the TACACS+ server.

```
tacacs server ACS
 address ipv4 172.25.180.117
 key cisco123
```

2. Configure TACACS+ for user authorization. TACACS+ uses the AAA architecture, which separates the authentication, authorization, and accounting functions. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. In this case, with TACACS+, we are using PKI for user credential validation and TACACS+ for authorization and accounting.

```
aaa group server tacacs+ ACS
  server name ACS
!
aaa authorization config-commands
aaa authorization exec ACS group tacacs+
aaa authorization commands 0 ACS group tacacs+ if-authenticated
aaa authorization commands 1 ACS group tacacs+ if-authenticated
aaa authorization commands 15 ACS group tacacs+ if-authenticated
aaa authorization network ACS group tacacs+
aaa authorization configuration ACS group tacacs+
```

3. Enable authorization on the PKI trustpoint CA for the user certificate.

```
crypto pki trustpoint CA2
  authorization list ACS
```

Troubleshooting

Commonly Used show Commands

Verify the status of the SSH server.

show ip ssh

```
Router#sh ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey
Authentication Publickey Algorithms:x509v3-ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 60 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SSH-RSA
ssh-rsa
```

Verify that the certificate for the root CA (CA2) is properly installed.
show crypto pki certificates

```
Router#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 05
  Certificate Usage: Signature
  Issuer:
    cn=DoD Root CA 2
```

```
        ou=PKI
        ou=DoD
        o=U.S. Government
        c=US
    Subject:
        cn=DoD Root CA 2
        ou=PKI
        ou=DoD
        o=U.S. Government
        c=US
    Validity Date:
        start date: 10:00:10 EST Dec 13 2004
        end date: 10:00:10 EST Dec 5 2029
        Associated Trustpoints: CA2
```

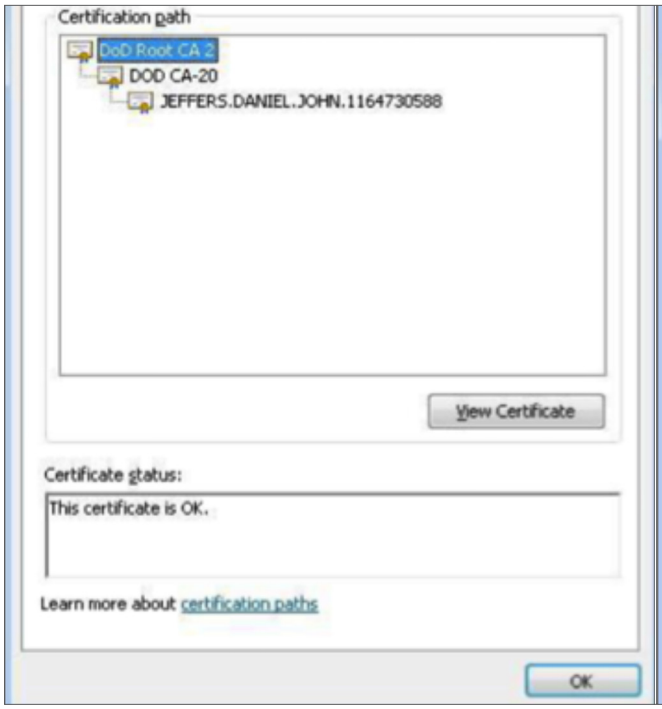
Commonly Encountered Problems

IOS SSH server failed to validate the user certificate without the intermediate CA

The issue is that the workstation has an improperly configured certificate chain. When the PKI CA certificates are not properly installed in the correct locations on the workstation, Microsoft CryptoAPI (CAPI) will attempt to build a path to a known issuer (such as Common Policy) and will automatically install cross-certificates obtained during path processing into the user trust store. This will cause the wrong certificate chain to be sent to the Cisco IOS SSH server and will result in the failed certificate validation. Figure 2 shows examples of correct and incorrect certificate chains.

Figure 2. Correct and Incorrect Certificate Chains

Correctly Installed DoD Certificate Chain



Improperly Configured Certificate Chain

Commonly Used debug Commands

debug crypto pki callbacks

debug crypto pki messages

debug crypto pki transactions

debug crypto pki validation

debug ip ssh detail

debug ip ssh packet

debug tacacs authentication

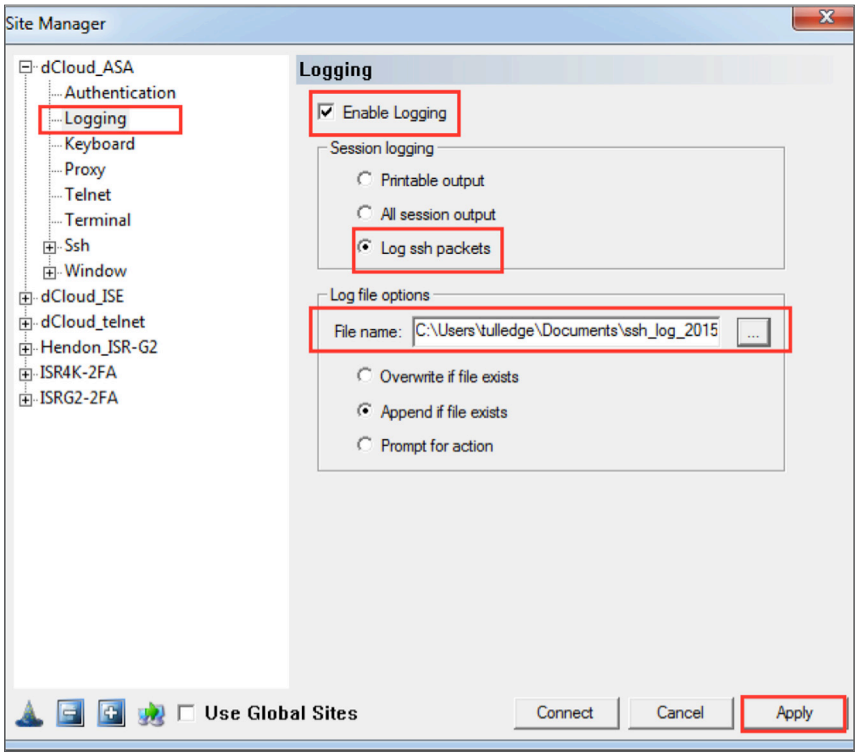
debug tacacs authorization

debug tacacs events

debug tacacs packet

Using Pragma Fortress Client Logging

1. The Pragma client has an SSH logging capability that allows you to see the SSH packet interchange with a server in the clear. Click Logging to enable.
2. Check Enable Logging.
3. Click Log ssh packets, and set the log filename.
4. Click Apply.



Example Configuration

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
aaa new-model
!
aaa group server tacacs+ ACS
  server name ACS
!
aaa authorization config-commands
aaa authorization exec ACS group tacacs+
aaa authorization commands 0 ACS group tacacs+ if-authenticated
aaa authorization commands 1 ACS group tacacs+ if-authenticated
aaa authorization commands 15 ACS group tacacs+ if-authenticated
aaa authorization network ACS group tacacs+
aaa authorization configuration ACS group tacacs+
!
clock timezone EST -5 0
clock summer-time EDT recurring
!
crypto pki trustpoint CA2
  enrollment terminal
  revocation-check none
  authorization list ACS
  authorization username subjectname commonname
!
crypto pki certificate chain CA2
  certificate ca 05
!
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh rsa keypair-name SSH-RSA
ip ssh version 2
ip ssh server certificate profile
  user
    trustpoint verify CA2
ip ssh server algorithm hostkey ssh-rsa
ip ssh server algorithm authentication publickey
ip ssh server algorithm publickey x509v3-ssh-rsa
!
tacacs server ACS
  address ipv4 172.25.180.117
  key cisco123
!
line vty 0 4
  login
  transport input ssh
!
ntp server 192.5.41.40
```

About Pragma Systems

Pragma Systems Inc. is a leading provider of enterprise-class remote access and secure file transfer software for Microsoft Windows platforms and is a Microsoft Gold Certified Partner. Pragma is an industry leader of SSH, SFTP, SCP, and Telnet technologies. Pragma's SSH product line has FIPS 140-2 (certificate #1500), U.S. DoD UCAPL, and U.S. Army TIC lab certifications. Pragma offers its services to build secure infrastructure, data centers, mobile, cloud, and IT delivery solutions for government and corporate enterprises. Pragma's software solution is deployed in the majority of Fortune 500 companies in the United States and in over 4500 companies worldwide in 70 countries, with millions of licensed nodes. To learn more, visit www.pragmasys.com.

C11-737065-00 05/16