Pulse Secure®

PCS/PPS NDcPP and JITC Certification: Deployment Guide

Published Date	April, 2018
Document Revision	1.0

Pulse Secure, LLC

2700 Zanker Road, Suite 200
San Jose, CA 95134

http://www.pulsesecure.net

Pulse Secure assumes no responsibility for any inaccuracies in this document. Pulse Secure reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

PCS/PPS NDcPP and JITC Certification: Deployment Guide

Printed in USA.

Contents

Purpose of this Document

This document is written for administrators configuring the PCS/PPS. To use this guide, you need a broad understanding of networks in general and the internet in particular, networking principles, and network configuration. It highlights the specific PCS/PPS configurations and administration functions and interfaces that are necessary to configure and maintain PCS/PPS in the evaluated configuration as defined in the NDcPP and JITC standards.

NDcPP Mode

Steps to Setup the PCS/PPS for NDcPP

Prerequisites for PCS/PPS Configurations

- External DNS Server should be able to resolve the hostnames used in the testing
- External Syslog server is up and running.
- External CRL is up and running.
- If you plan to integrate with Pulse One, Pulse One server is up and running.

Password Minimum Length Configuration

On Administrator Web Console, follow below instruction to set administrator minimum password length to be 15.

1. Set in Admin Realm:
   a. Navigate to Administrators > Admin Realms
   b. Click on Admin Users.
   c. Click on the Authentication Policy tab.
   d. Click on Password tab
   e. Click on Only allow users that have passwords of a minimum length.
   f. Enter 15 as Minimum Length.
2. Set in local auth server configuration:
   a. Navigate to Authentication -> Auth. Servers.
   b. Click on Administrators.
   c. On the Settings tab, click on Password Options section.
   d. Configure 15 characters as Minimum length.
   e. Configure Maximum Length greater than or equal to 15 characters set as Minimum Length
3. Review all previously configured administrator passwords, update to ensure all are at least 15 characters.

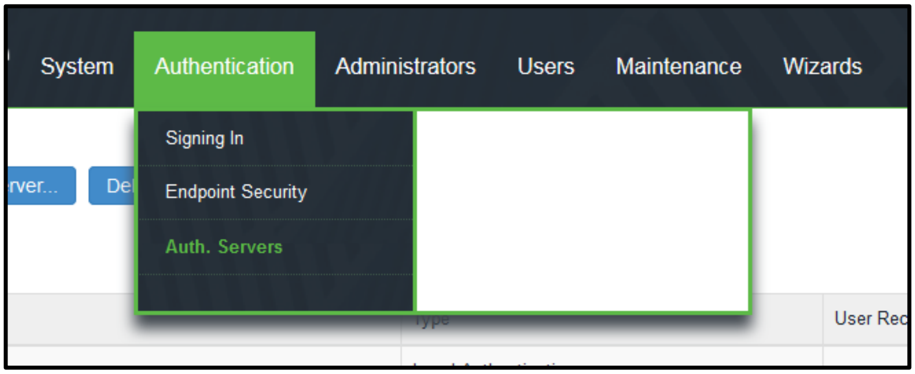
Serial Console Access Control Configuration

Configure administrator access control for the local serial console is a two-step process.

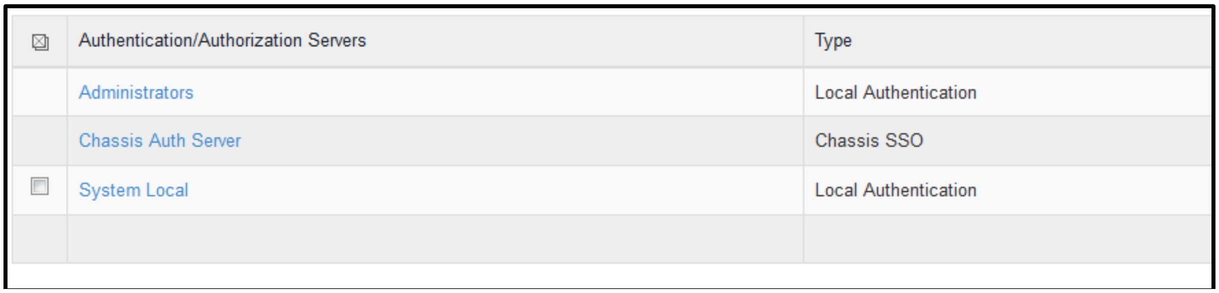
1. Enable allow console access for the administrator.

   In Administrator Web Console,

   a. Go to Authentication -> Auth. Servers



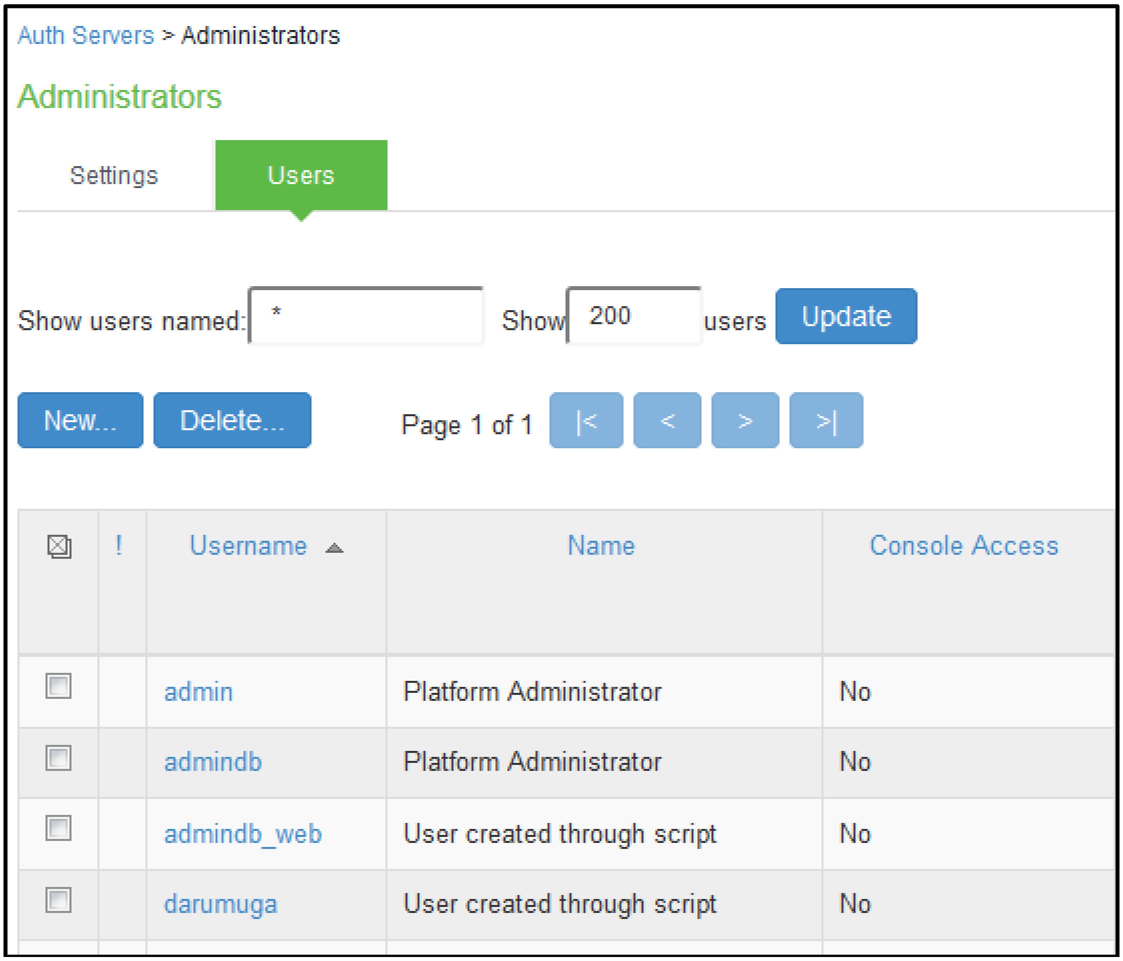
b. This screen is shown.



☒	Authentication/Authorization Servers	Type
	Administrators	Local Authentication
	Chassis Auth Server	Chassis SSO
□	System Local	Local Authentication

c. Select Administrators.

d. Click on Users tab.



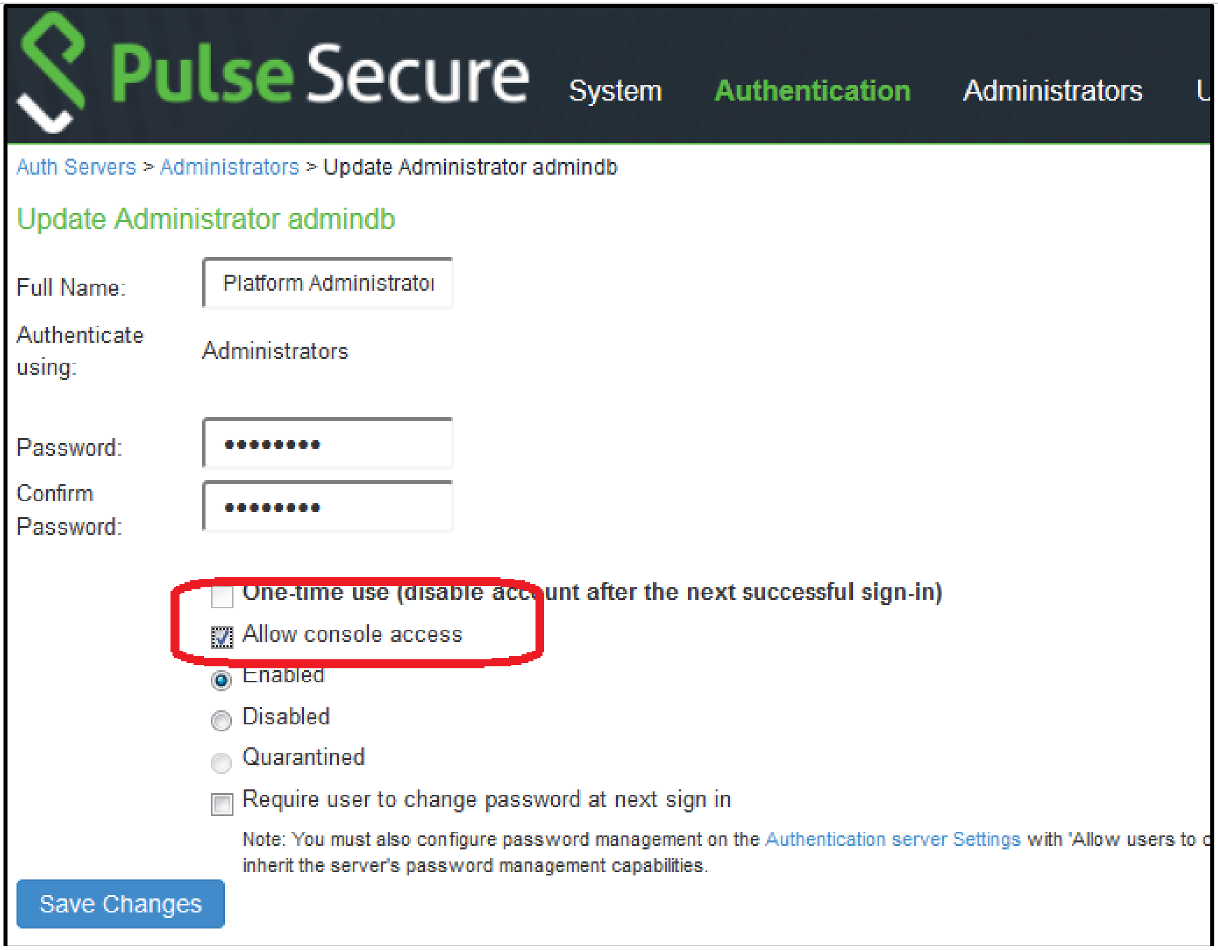
Auth Servers > Administrators

Administrators

Show users named: * Show 200 users

☒	!	Username ▲	Name	Console Access
□		admin	Platform Administrator	No
□		admindb	Platform Administrator	No
□		admindb_web	User created through script	No
□		darumuga	User created through script	No

e. Click on administrator name configured in Initial Setup



Auth Servers > Administrators > Update Administrator admindb

Update Administrator admindb

Full Name: Platform Administrator

Authenticate using: Administrators

Password: ••••••••

Confirm Password: ••••••••

□ One-time use (disable account after the next successful sign-in)

☑ Allow console access

● Enabled

○ Disabled

○ Quarantined

□ Require user to change password at next sign in

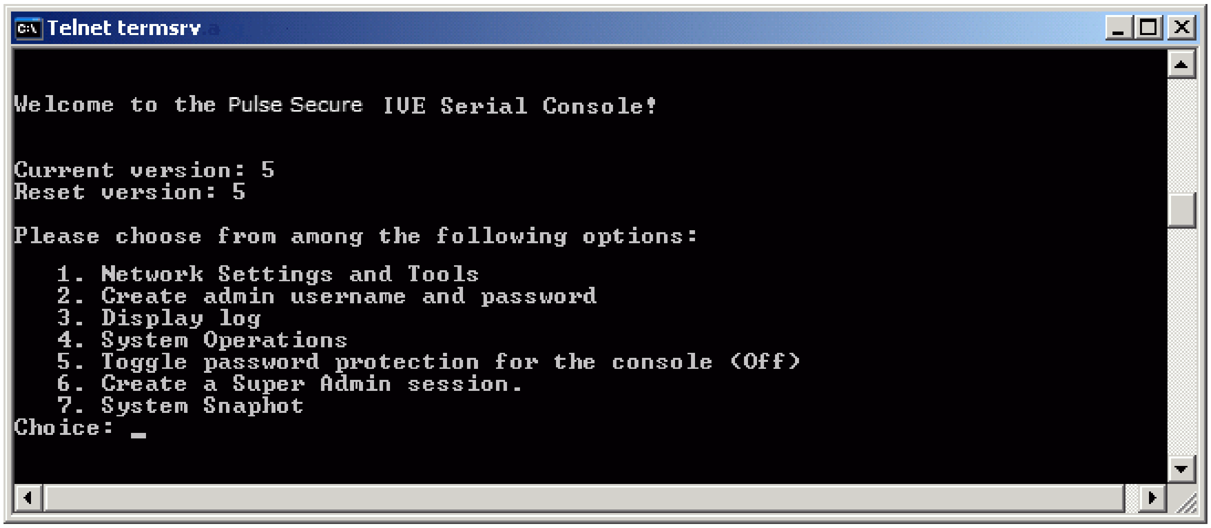
Note: You must also configure password management on the Authentication server Settings with 'Allow users to c inherit the server's password management capabilities.

f. Click on the Allow console access checkbox

g. Click on Save Changes.

2. Enable password protection for the console.

a. Connect to the local serial console, the serial console menu is shown as below.



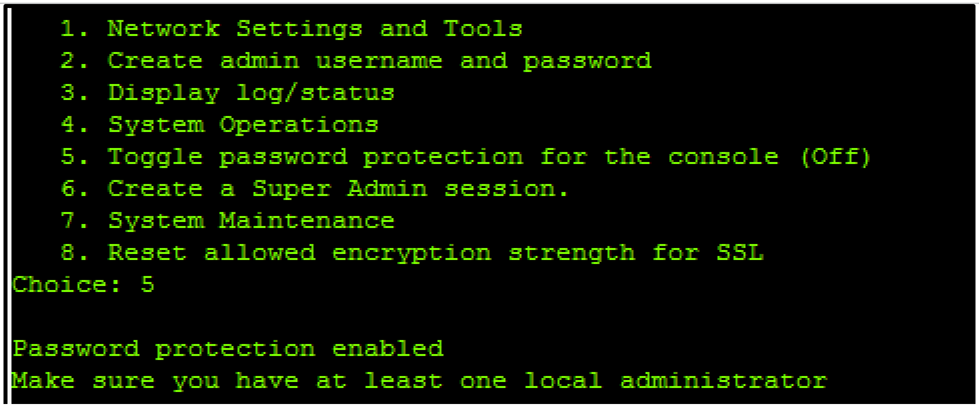
```
Welcome to the Pulse Secure IVE Serial Console!

Current version: 5
Reset version: 5

Please choose from among the following options:

   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snaphot
Choice: _
```

b. Choose option 5 on the local serial console. You should see a confirmation: "Password protection enabled, make sure you have at least one local administrator".

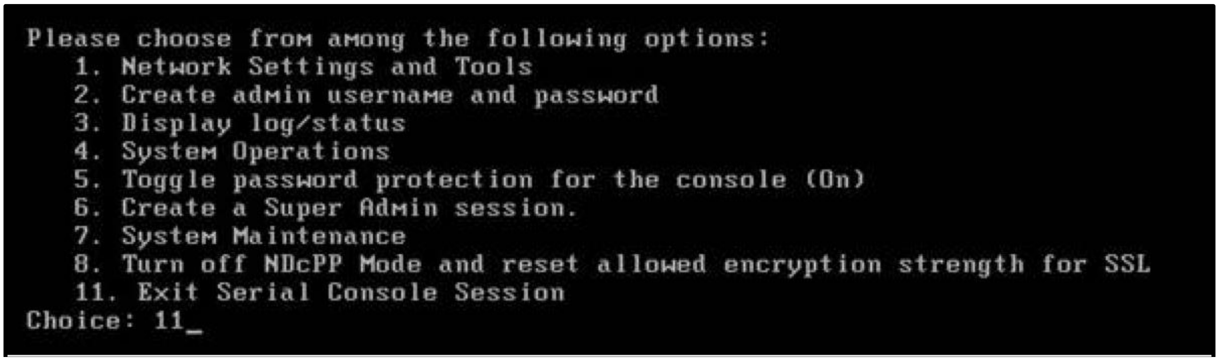


```
     1. Network Settings and Tools
     2. Create admin username and password
     3. Display log/status
     4. System Operations
     5. Toggle password protection for the console (Off)
     6. Create a Super Admin session.
     7. System Maintenance
     8. Reset allowed encryption strength for SSL
Choice: 5

Password protection enabled
Make sure you have at least one local administrator
```

Terminating a Local Console Session

To exit a console session, choose option 11 on the local serial console.

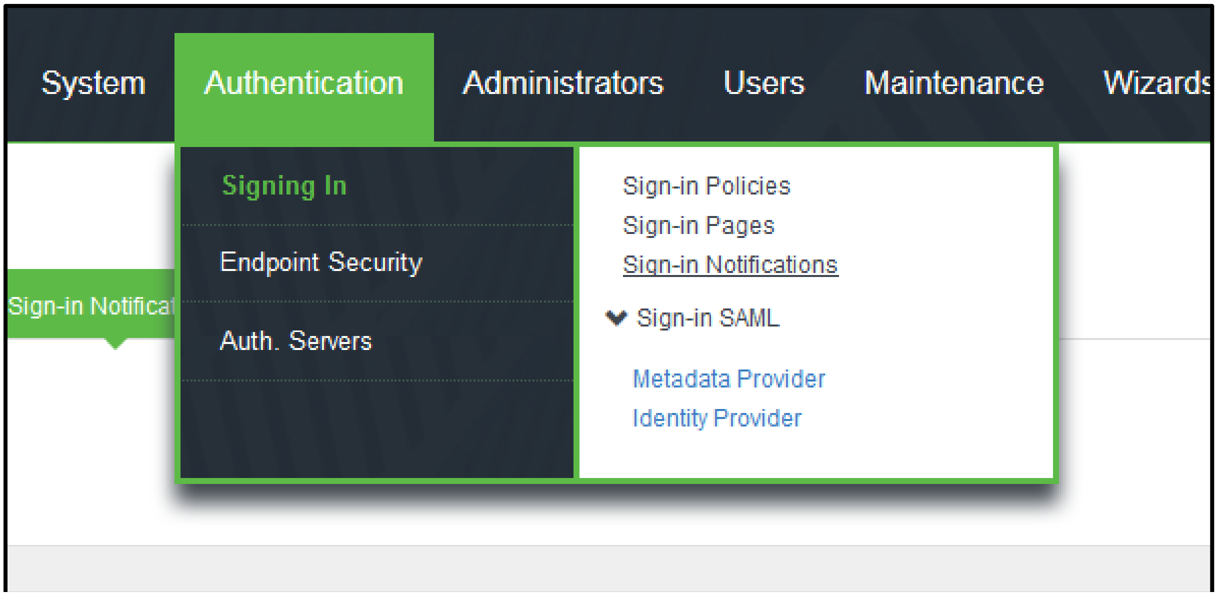


```
Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (On)
   6. Create a Super Admin session.
   7. System Maintenance
   8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
   11. Exit Serial Console Session
Choice: 11_
```

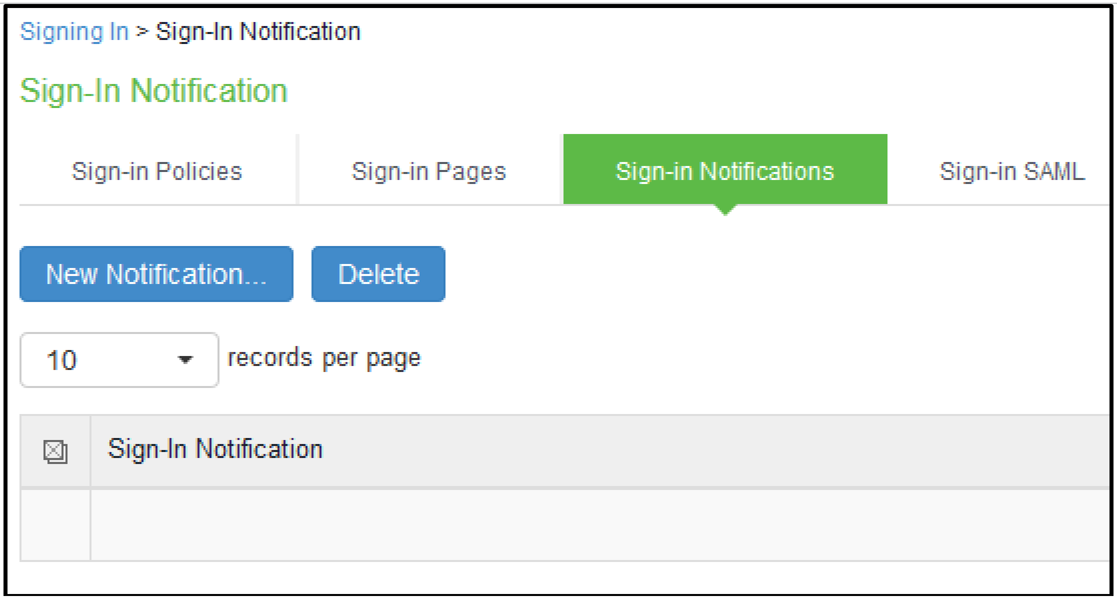
Administrative Banner Configuration

Configuring administrator banner for the Administrator Web Console and the local serial console is a two-step process.

1. Create a Sign-in notification. On Administrator Web Console:
   a. Navigate to Authentication -> Signing In -> Sign-in Notifications



   b. This screen is shown



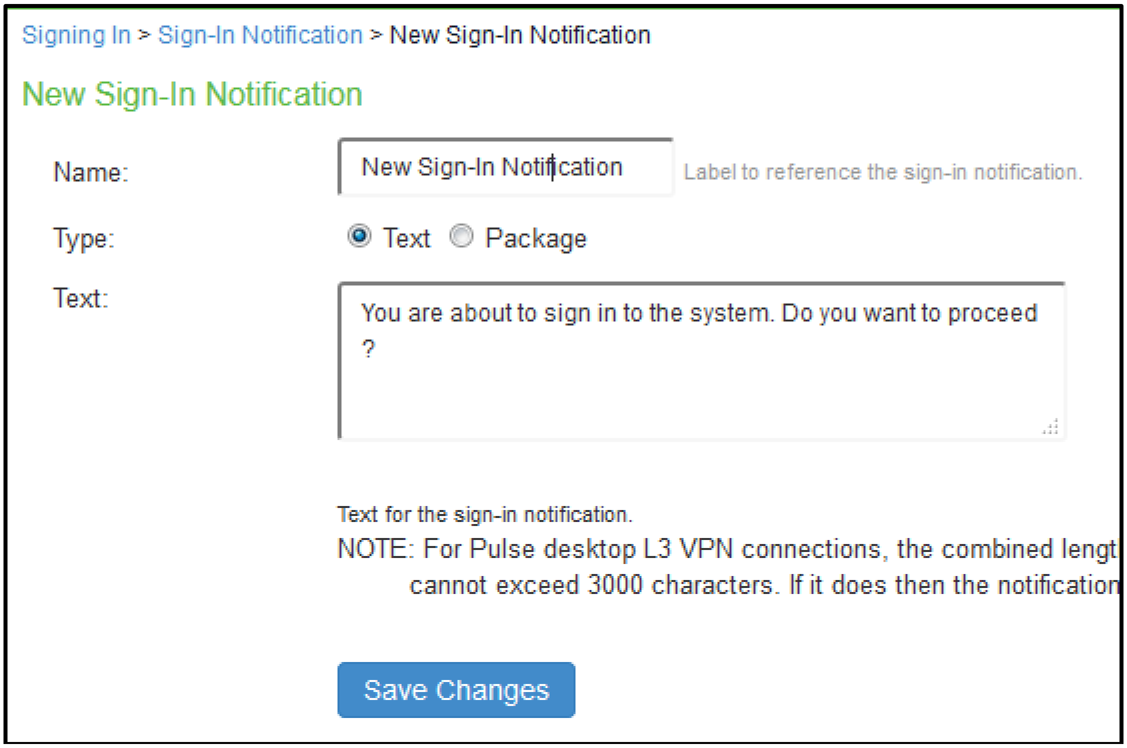
Signing In > Sign-In Notification

Sign-In Notification

10 records per page

☒	Sign-In Notification

c. Click on New Notification



Signing In > Sign-In Notification > New Sign-In Notification

New Sign-In Notification

Name: New Sign-In Notification Label to reference the sign-in notification.

Type: ● Text ○ Package

Text: You are about to sign in to the system. Do you want to proceed ?

Text for the sign-in notification.

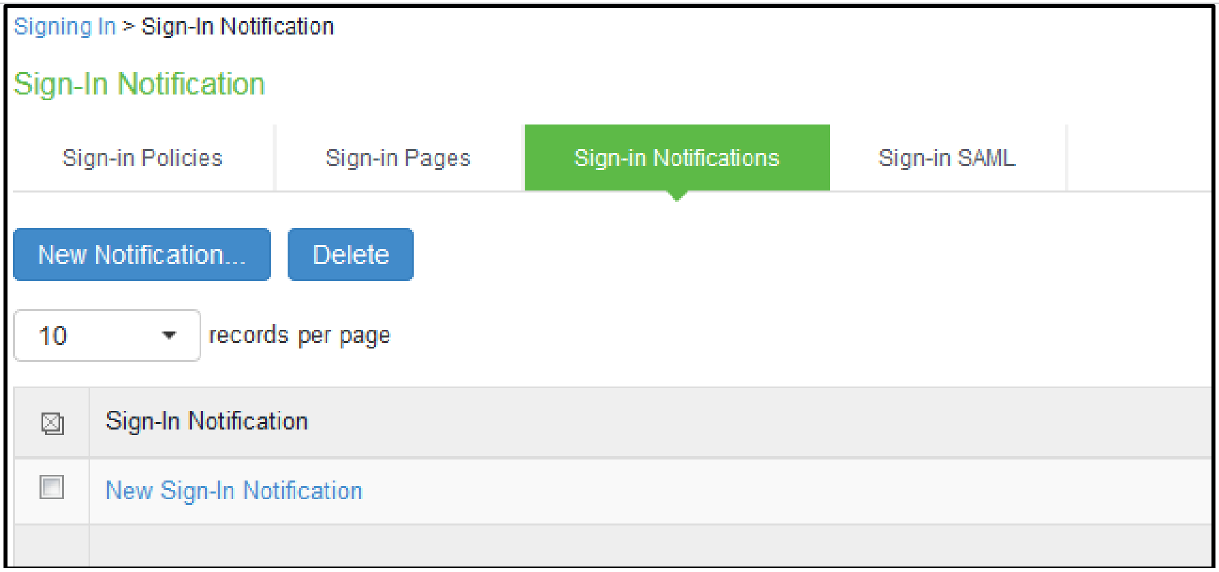
NOTE: For Pulse desktop L3 VPN connections, the combined lengt
cannot exceed 3000 characters. If it does then the notification

d. Enter a name for the new notification in the Name:

e. In Type:, select Text

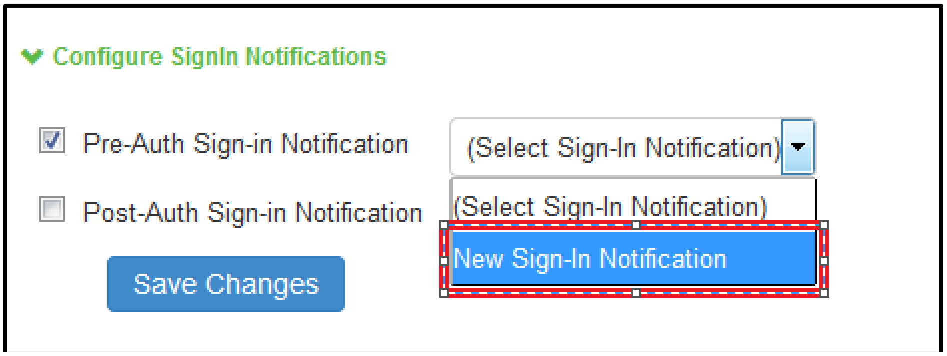
f. Enter banner message in the Text:

g. Click on Save Changes



☒	Sign-In Notification
□	New Sign-In Notification

2. Associate the notification with an admin URL. On Administrator Web Console,
    a. Navigate to Authentication -> Signing In -> Sign-In Policies
    b. Click on admin URL */admin/
    c. In the Configure SignIn Notifications section, select the check box Pre-Auth Sign-in Notification.


Configure SignIn Notifications
☑ Pre-Auth Sign-in Notification
□ Post-Auth Sign-in Notification
Save Changes
(Select Sign-In Notification)
(Select Sign-In Notification)
New Sign-In Notification

    d. A drop down box appears next to Pre-Auth Sign-in Notification once it is selected, in the drop down box, select the notification you created in Step 1 above.
    e. Click on Save Changes

Configure GUI Inactivity Timeout Period

1. Navigate to Administrators -> Admin Roles -> <Role Name> -> Session Options
2. Under the 'Session lifetime' section, enter the Idle timeout in minutes.

Terminating a GUI Session

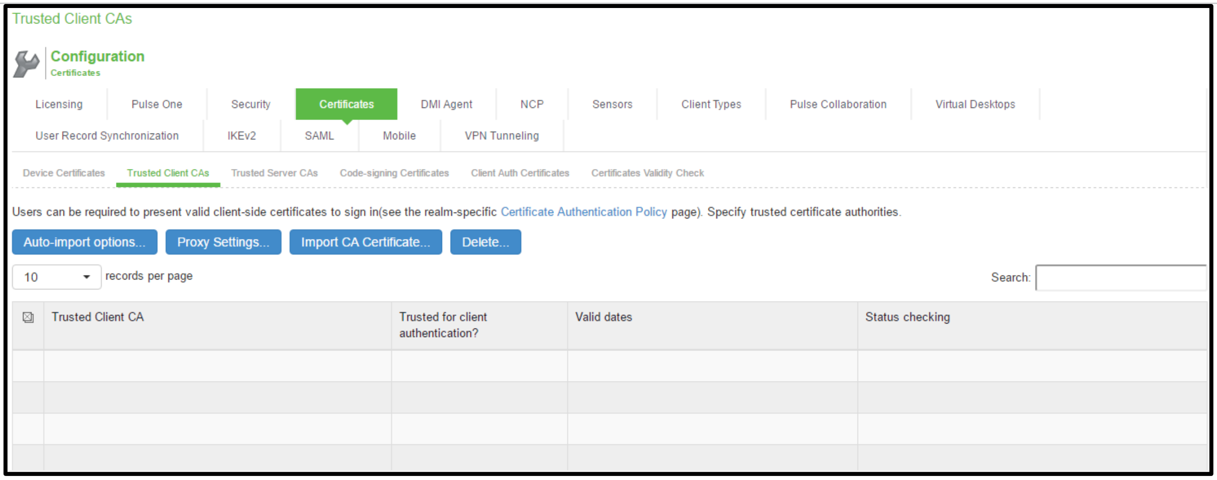
To log out of the web administrative session, on any screen click on the "Sign Out" link at the top right of the screen.

Import Trusted Client CA

Trusted Client CA is required in order to validate the client certificate that is used by the PCS/PPS to authenticate to syslog server.

On Administrator Web Console,

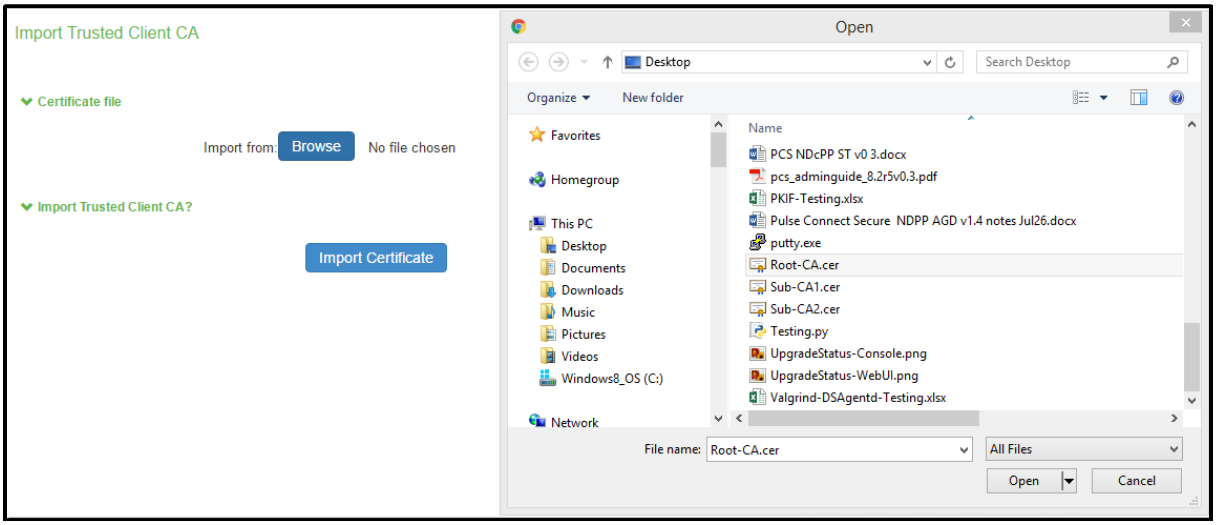
1. Navigate to System -> Configuration -> Certificates -> Trusted Client CAs



Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

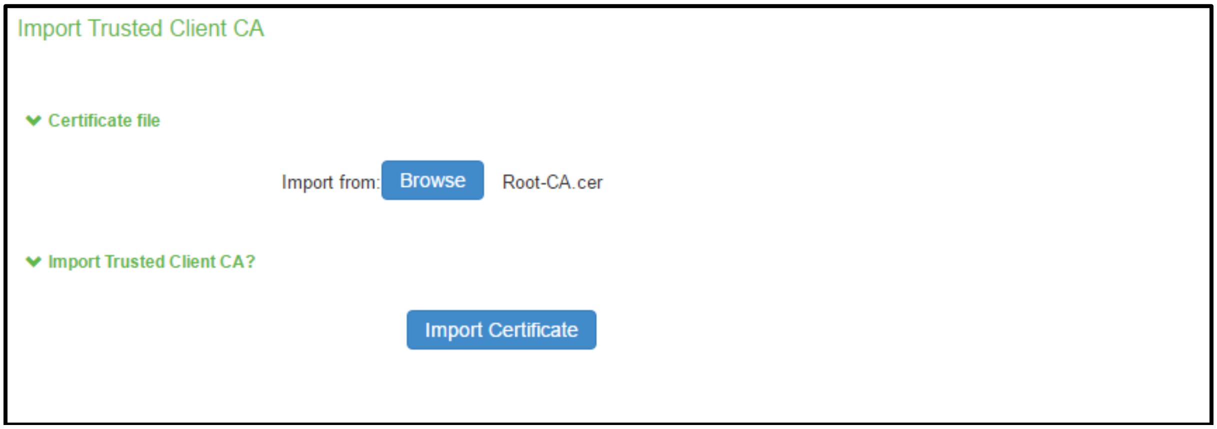
□	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking

2. Click **Import CA Certificates**... button to import CA or Chain of CAs one by one as explained below in different Screenshots



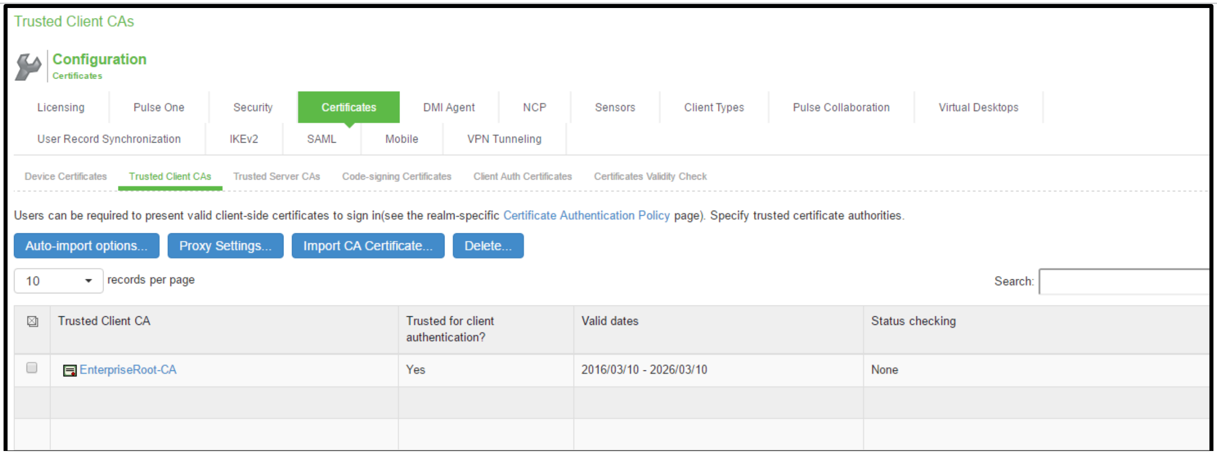
File name: Root-CA.cer

3. Click on **Import Certificate**.



Import from: Root-CA.cer

4. The imported trusted client CA is shown in the Trusted Client CAs table



Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

☐	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
☐	EnterpriseRoot-CA	Yes	2016/03/10 - 2026/03/10	None

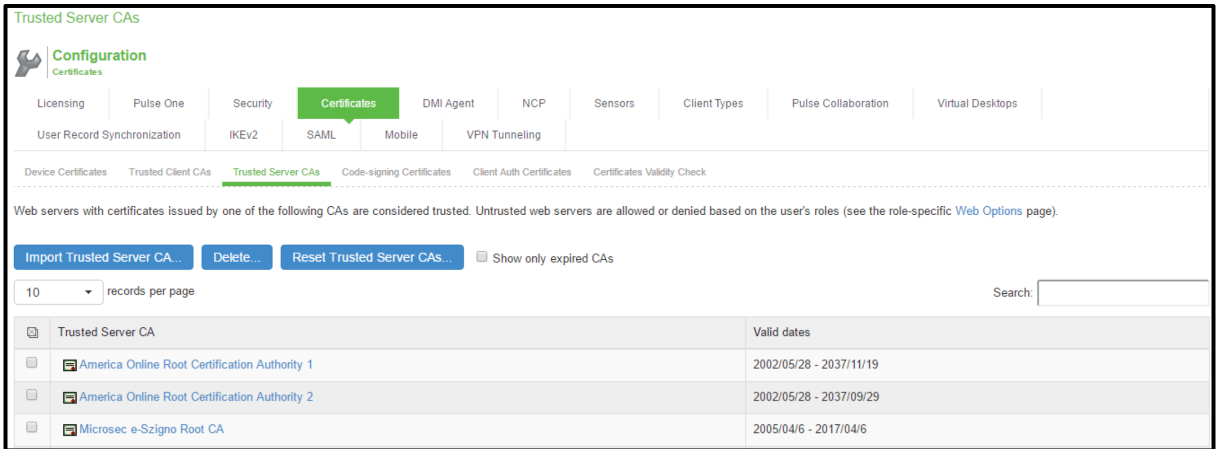
Import Trusted Server CA

Trusted Server CA is used in two situations:

- To validate the device certificate that is generated for TLS handshake when a TLS client is connecting to the PCS/PPS.
- To validate the server certificate received in TLS handshake when the PCS/PPS connects to syslog server and Pulse One.

On Administrator Web Console,

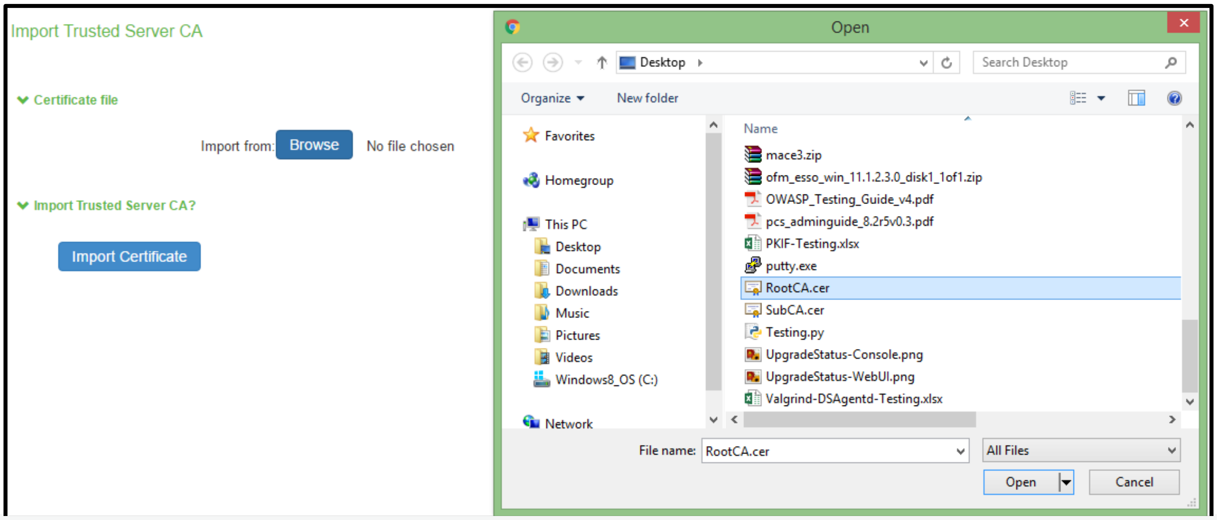
1. Navigate to System -> Configuration -> Certificates -> Trusted Server CAs.



Web servers with certificates issued by one of the following CAs are considered trusted. Untrusted web servers are allowed or denied based on the user's roles (see the role-specific Web Options page).

☐	Trusted Server CA	Valid dates
☐	America Online Root Certification Authority 1	2002/05/28 - 2037/11/19
☐	America Online Root Certification Authority 2	2002/05/28 - 2037/09/29
☐	Microsec e-Szigno Root CA	2005/04/6 - 2017/04/6

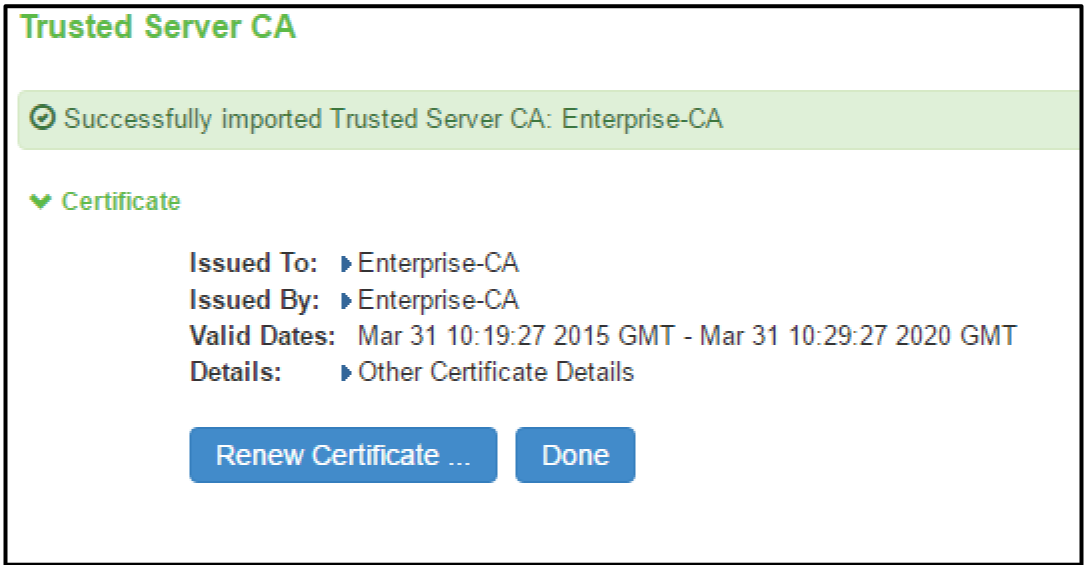
2. Click on Import Trusted Server CA...
3. On the Import Trusted Server CA screen, click on Browser, import the root CA certificate file.



File name: RootCA.cer

Note: In order to import CA Chain, all Sub CAs must be imported one by one.

4. Once CA or CA Chain is Imported, click Done



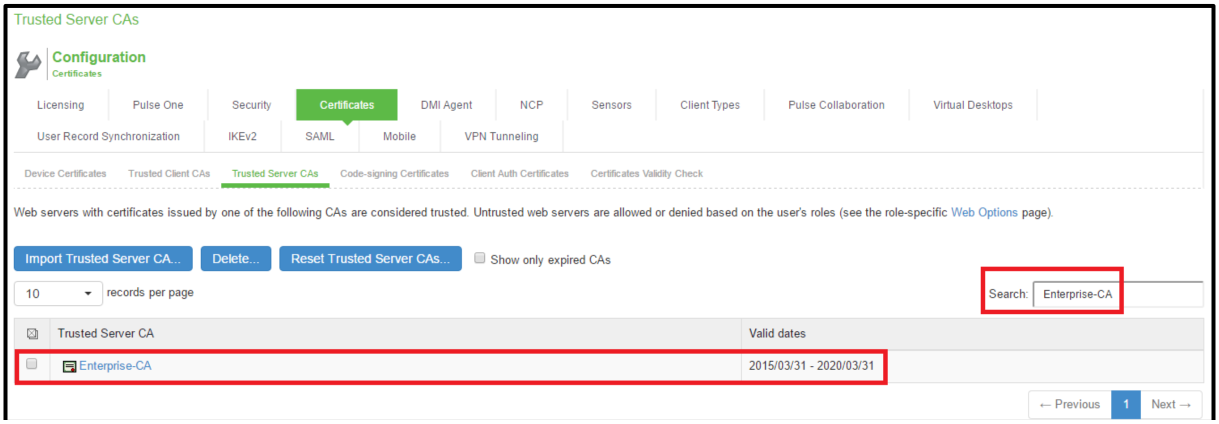
Trusted Server CA

Successfully imported Trusted Server CA: Enterprise-CA

Certificate

Issued To: Enterprise-CA
Issued By: Enterprise-CA
Valid Dates: Mar 31 10:19:27 2015 GMT - Mar 31 10:29:27 2020 GMT
Details: Other Certificate Details

5. The CA Common Name of the imported trusted server CA should be shown in the Trusted Server CA table on screen System -> Configuration -> Certificates -> Trusted Server CAs.



Web servers with certificates issued by one of the following CAs are considered trusted. Untrusted web servers are allowed or denied based on the user's roles (see the role-specific Web Options page).

Search: Enterprise-CA

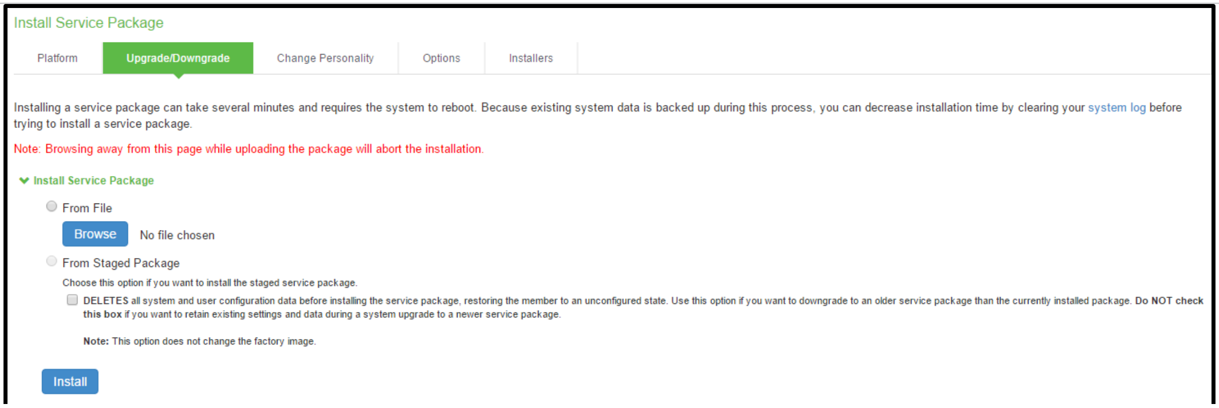
	Trusted Server CA	Valid dates
□	Enterprise-CA	2015/03/31 - 2020/03/31

Note: The CRL configured in the certificate is used, thus no additional configuration is required to configure CRL for trusted server certificate.

Software Updates

If a new NDcPP compliant software package is available, follow instructions in this section to update the software package on the PCS/PPS. The verification of the authenticity of the software package is performed by digital signature verification.

1. Download the PCS/PPS software package from Pulse Secure Licensing and Download Center onto a trusted computer system.
2. On Administrator Web Console.
3. Navigate to Maintenance -> System -> Upgrade/Downgrade.



Install Service Package

Installing a service package can take several minutes and requires the system to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system log before trying to install a service package.

Note: Browsing away from this page while uploading the package will abort the installation.

Install Service Package

○ From File

Browse No file chosen

○ From Staged Package

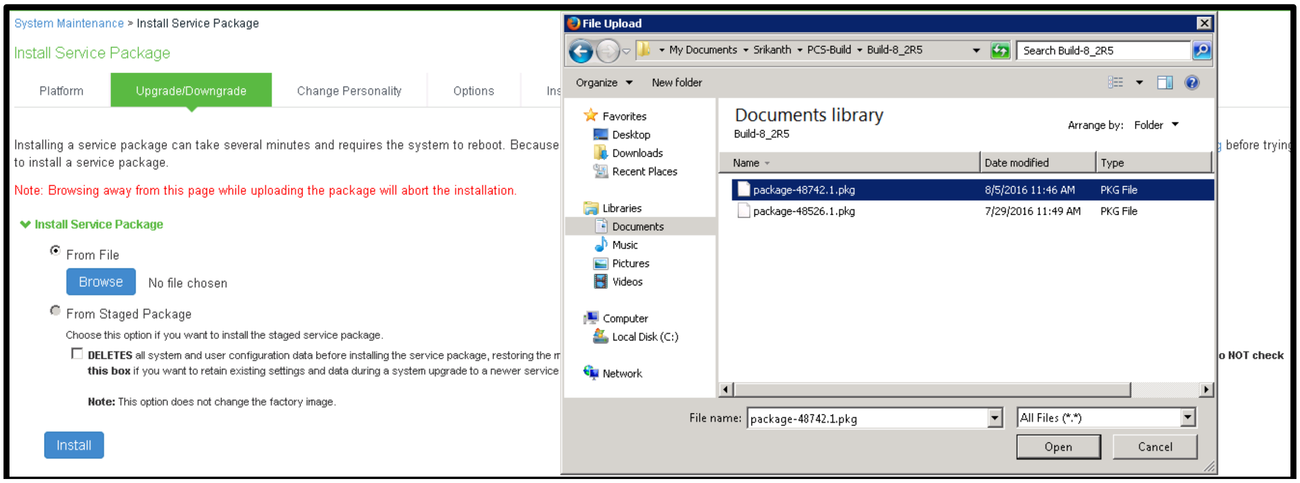
Choose this option if you want to install the staged service package.

□ **DELETES** all system and user configuration data before installing the service package, restoring the member to an unconfigured state. Use this option if you want to downgrade to an older service package than the currently installed package. **Do NOT check this box** if you want to retain existing settings and data during a system upgrade to a newer service package.

Note: This option does not change the factory image.

Install

4. In the expanded **Install Server Package** section, click on **From File** option, then click on **Browse** to select the server package downloaded earlier.

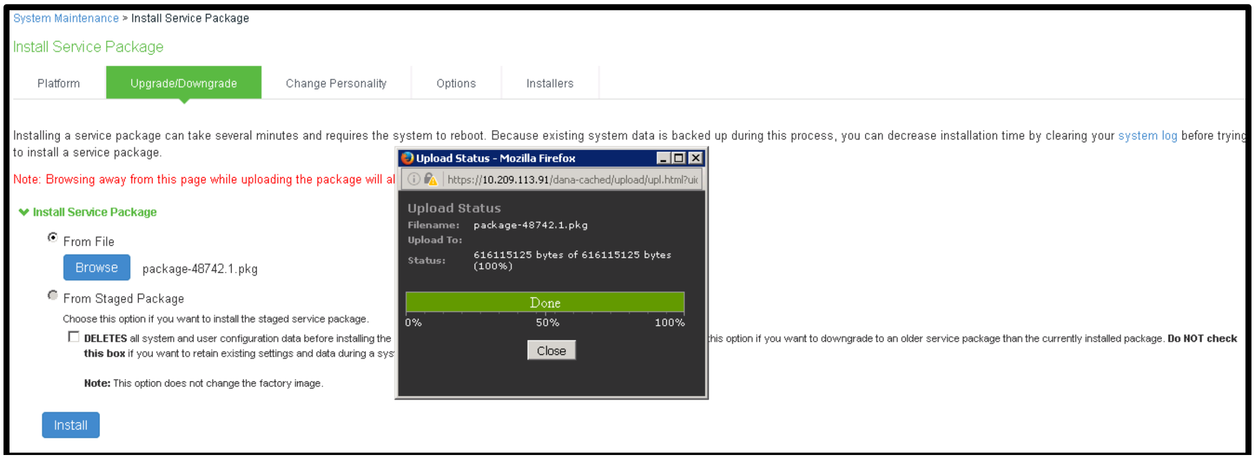


Name	Date modified	Type
package-48742.1.pkg	8/5/2016 11:46 AM	PKG File
package-48526.1.pkg	7/29/2016 11:49 AM	PKG File

File name: package-48742.1.pkg

All Files (*.*)

5. Click **Install** to start the installation process.


System Maintenance > Install Service Package
Install Service Package
Platform
Upgrade/Downgrade
Change Personality
Options
Installers
Upload Status - Mozilla Firefox
https://10.209.113.91/dana-cached/upload/upl.html?ui
Done
0%
50%
100%
Close
Install

Upload Status

Filename: package-48742.1.pkg

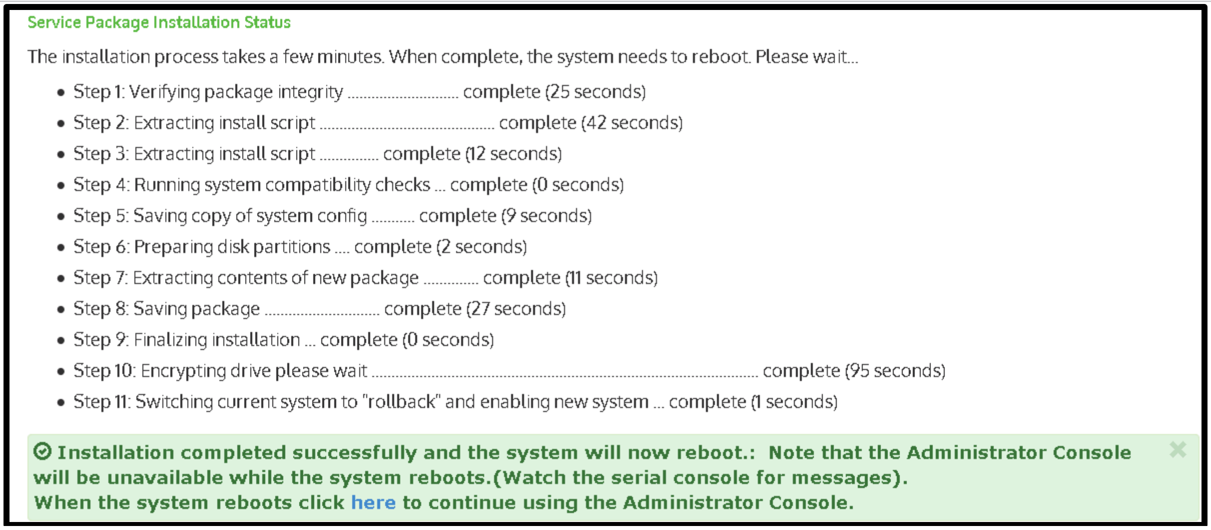
Upload To:

Status: 616115125 bytes of 616115125 bytes (100%)

● From File

Browse package-48742.1.pkg

6. Below information is shown during installation.



Service Package Installation Status

The installation process takes a few minutes. When complete, the system needs to reboot. Please wait...

- Step 1: Verifying package integrity .... complete (25 seconds)
- Step 2: Extracting install script .... complete (42 seconds)
- Step 3: Extracting install script .... complete (12 seconds)
- Step 4: Running system compatibility checks ... complete (0 seconds)
- Step 5: Saving copy of system config .... complete (9 seconds)
- Step 6: Preparing disk partitions .... complete (2 seconds)
- Step 7: Extracting contents of new package .... complete (11 seconds)
- Step 8: Saving package .... complete (27 seconds)
- Step 9: Finalizing installation ... complete (0 seconds)
- Step 10: Encrypting drive please wait .... complete (95 seconds)
- Step 11: Switching current system to "rollback" and enabling new system ... complete (1 seconds)

Installation completed successfully and the system will now reboot.: Note that the Administrator Console will be unavailable while the system reboots.(Watch the serial console for messages). When the system reboots click here to continue using the Administrator Console.

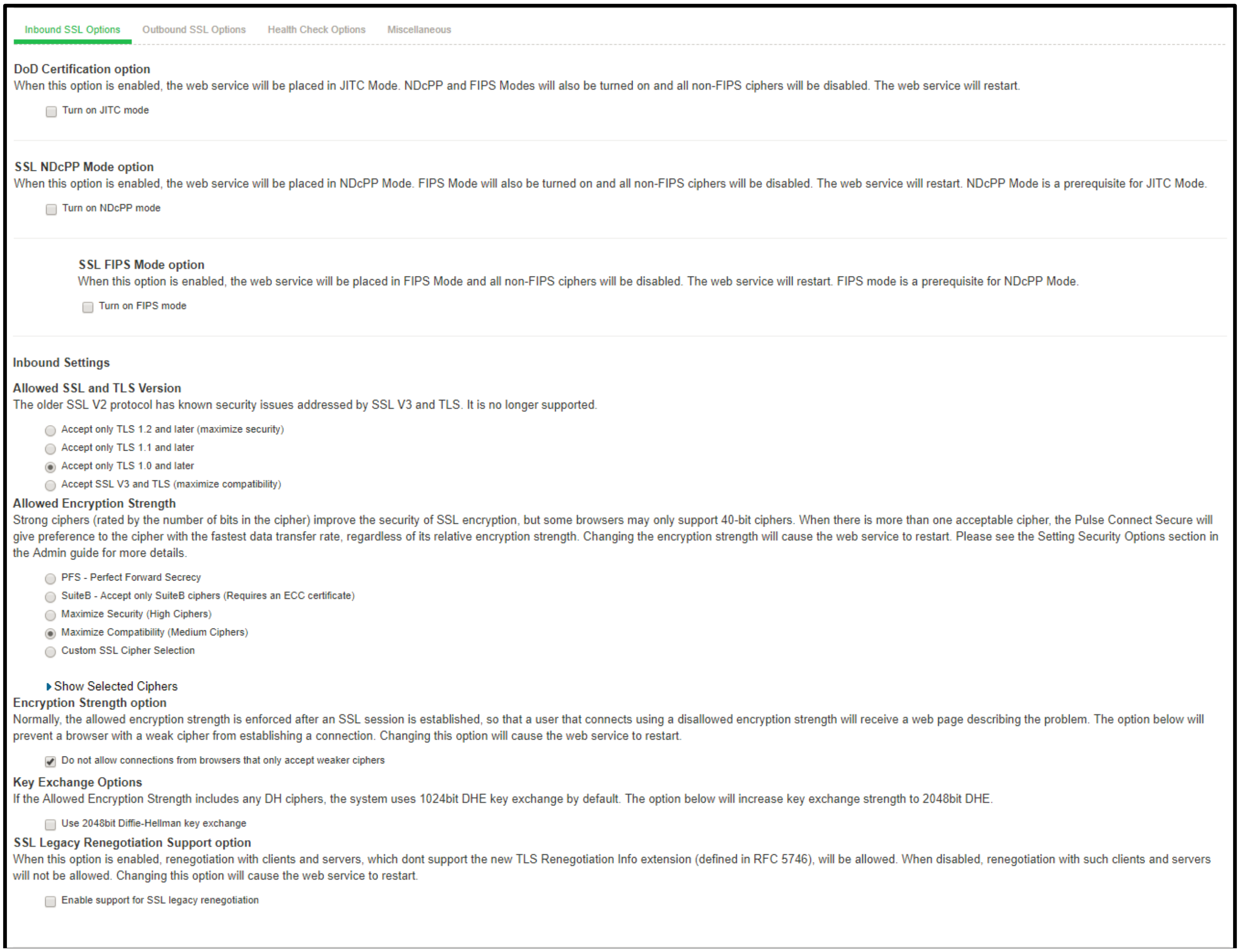
7. Confirm current software version

   After system boot up, go to System Maintenance > Platform screen, verify Current version: displays the correct software version.

Enabling NDcPP Mode

On Administrator Web Console,

1. Navigate to System -> Configuration > Security > Inbound SSL Options.



DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

□ Turn on JITC mode

SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

□ Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode and all non-FIPS ciphers will be disabled. The web service will restart. FIPS mode is a prerequisite for NDcPP Mode.

□ Turn on FIPS mode

Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

○ Accept only TLS 1.2 and later (maximize security)
○ Accept only TLS 1.1 and later
● Accept only TLS 1.0 and later
○ Accept SSL V3 and TLS (maximize compatibility)

Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Connect Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

○ PFS - Perfect Forward Secrecy
○ SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
○ Maximize Security (High Ciphers)
● Maximize Compatibility (Medium Ciphers)
○ Custom SSL Cipher Selection

▸ Show Selected Ciphers

Encryption Strength option
Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using a disallowed encryption strength will receive a web page describing the problem. The option below will prevent a browser with a weak cipher from establishing a connection. Changing this option will cause the web service to restart.

☑ Do not allow connections from browsers that only accept weaker ciphers

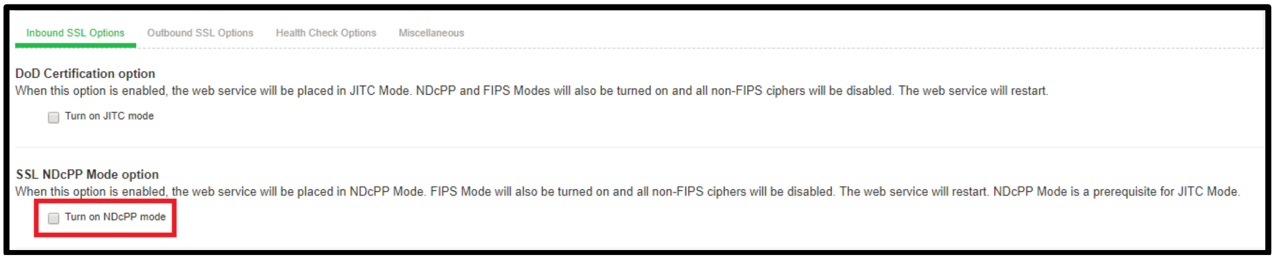
Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

□ Use 2048bit Diffie-Hellman key exchange

SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension (defined in RFC 5746), will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. Changing this option will cause the web service to restart.

□ Enable support for SSL legacy renegotiation

2. Click on the **Turn on NDcPP mode** checkbox highlighted to make the PCS/PPS common criteria compliant



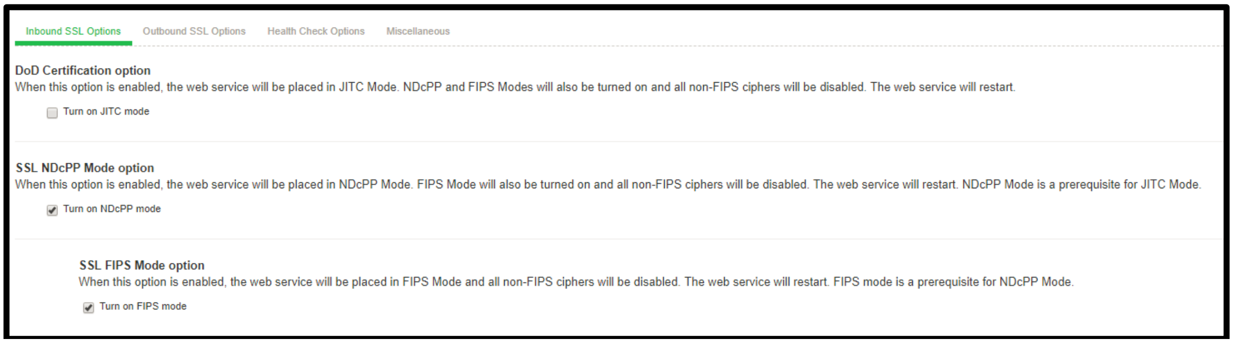
DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

☐ Turn on JITC mode

SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

☐ Turn on NDcPP mode

3. Once **Turn on NDcPP mode** is enabled, **Turn on FIPS mode** is also automatically enabled.



DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

☐ Turn on JITC mode

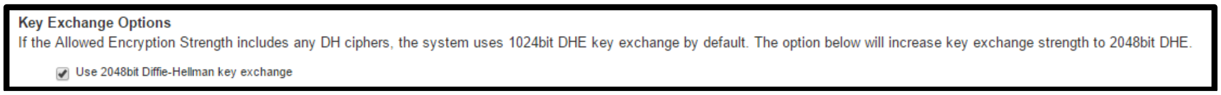
SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

☑ Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode and all non-FIPS ciphers will be disabled. The web service will restart. FIPS mode is a prerequisite for NDcPP Mode.

☑ Turn on FIPS mode

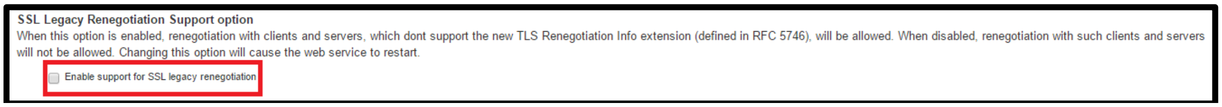
4. Enable the **Use 2048 bit Diffie-Hellman key exchange** checkbox.



Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

☑ Use 2048bit Diffie-Hellman key exchange

5. Uncheck SSL Legacy Renegotiation Support option.



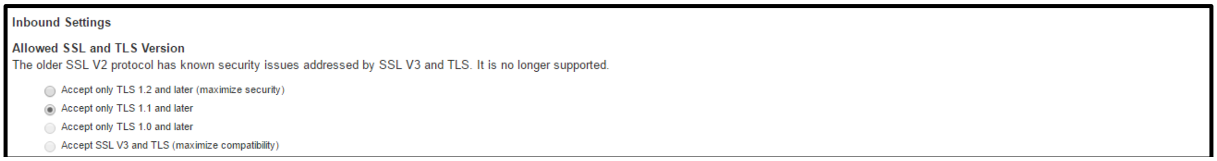
SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension (defined in RFC 5746), will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. Changing this option will cause the web service to restart.

☐ Enable support for SSL legacy renegotiation

6. Click on **Save Changes**.

7. At this point, the **Turn on NDcPP mode** is enabled for both Inbound SSL Options and Outbound SSL Options and the following is shown:

   a. Accept only TLS1.0 and later and Accept SSL V3 and TLS (maximize compatibility) are disabled in the NDcPP mode. Accept only TLS 1.1 and later is selected by default.

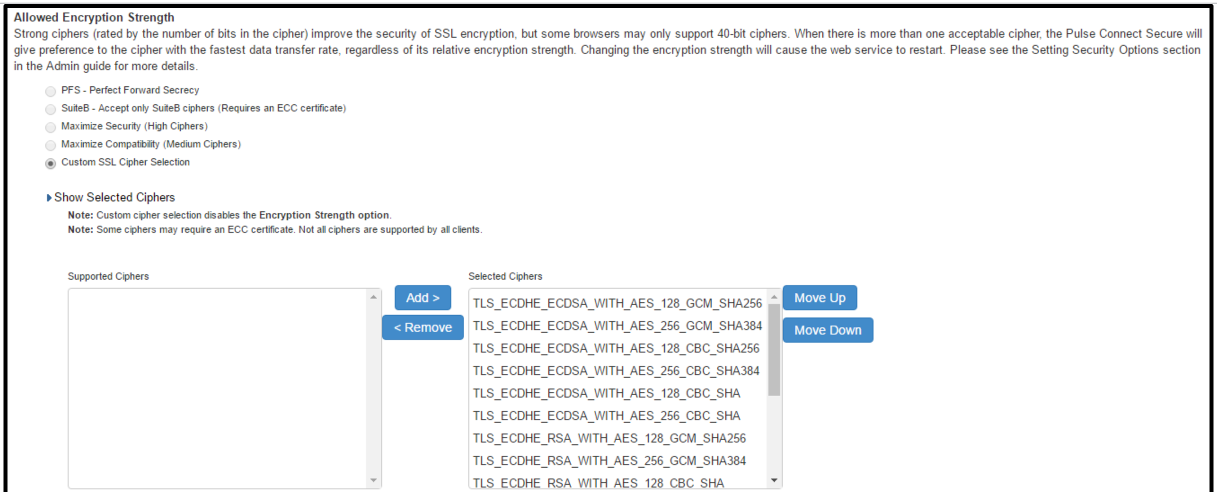


Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

○ Accept only TLS 1.2 and later (maximize security)
● Accept only TLS 1.1 and later
○ Accept only TLS 1.0 and later
○ Accept SSL V3 and TLS (maximize compatibility)

   b. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on Show Selected Ciphers displays below 16 Ciphers in the right panel labelled Selected Cipher.



Allowed Encryption Strength

Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Connect Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

○ PFS - Perfect Forward Secrecy
○ SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
○ Maximize Security (High Ciphers)
○ Maximize Compatibility (Medium Ciphers)
● Custom SSL Cipher Selection

▸ Show Selected Ciphers

Note: Custom cipher selection disables the **Encryption Strength option**.
Note: Some ciphers may require an ECC certificate. Not all ciphers are supported by all clients.

Supported Ciphers

Selected Ciphers

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

c. Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel, and click “Remove” button to remove it from the “Selected Ciphers”.

d. Navigate to System -> Configuration > Security > outbound SSL Options

e. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on Show Selected Ciphers displays below 16 Ciphers in the right panel labelled Selected Cipher.

f. Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel, and click “Remove” button to remove it from the “Selected Ciphers”.

8. Optionally, you may check below log to confirm NDcPP mode is enabled:

   Navigate to System -> Log/Monitoring -> Admin Access -> Logs and Check for the Logs mentioned in the section **NDcPP Mode Enable Configuration Admin Logs**

9. Optionally, you may check below log to confirm that DHE2048 Key Exchange Option is enabled:

   Navigate to System -> Log/Monitoring -> Admin Access -> Logs and Check for the Logs mentioned in the section **DH2048 Key Exchange Enable Configuration Admin Logs.**

Audit Logs For NDcPP Mode

NDcPP Mode Enable Configuration Admin Logs

Configuration change to enable NDcPP mode on the PCS/PPS.

Info	ADM23434	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – Allowed SSL and TLS changed from 'TLSv1 and above' to 'TLS1.1 and above'.
Info	ADM31354	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – Changed Allowed Encryption Strength from <ciphersuite> to <ciphersuite>.
Info	ADM30965	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – FIPS mode is now turned on. The web server will restart.
Info	ADM31273	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – NDcPP mode is now turned on. The web server will restart.

NDcPP Mode Disable Configuration Admin Logs

Configuration change to disable NDcPP mode on the PCS/PPS.

Info	ADM31273	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – NDcPP mode is now turned off. The web server will restart.

DH2048 Key Exchange Enable Configuration Admin Logs

Configuration change to enable DH2048 Key Exchange Option on the PCS/PPS.

Info	ADM31287	<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – DHE2048 option is now enabled

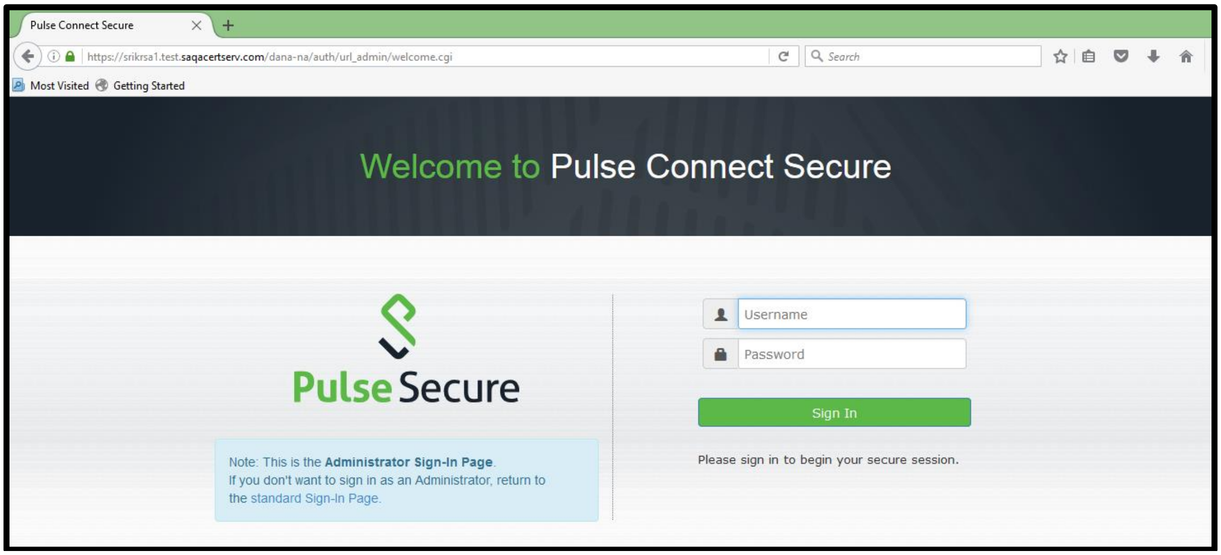
JITC Mode

Prerequisites for enabling JITC Mode

Before enabling the JITC Mode, admin must make sure to import the Trusted Server CAs. If not done yet, perform the following steps before enabling the JITC mode.

1. Login to PCS/PPS from any Browser: **https://a.b.c.d/admin** using admin credentials.

   Note: The admin credentials are configured during the initial setup via console.

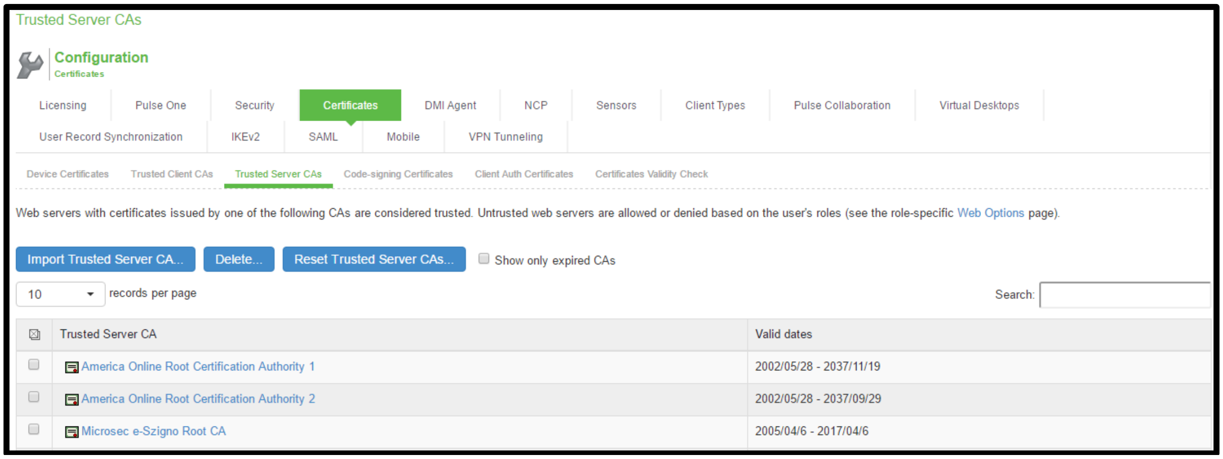

Pulse Connect Secure
https://srikrsa1.test.saqacertserv.com/dana-na/auth/url_admin/welcome.cgi
Search
Most Visited
Getting Started
Welcome to Pulse Connect Secure
Pulse Secure
Username
Password
Sign In

Note: This is the **Administrator Sign-In Page**. If you don't want to sign in as an Administrator, return to the standard Sign-In Page.

Please sign in to begin your secure session.

2. Import Trusted Server CA. For this, on the administrator web console:

   a. Navigate to System -> Configuration -> Certificates -> Trusted Server CAs.

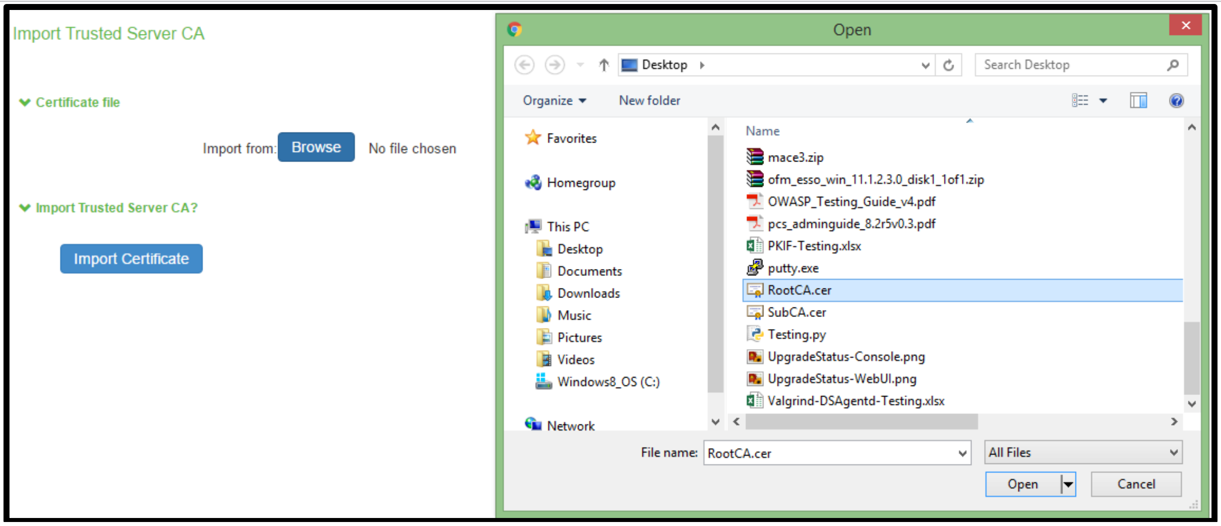


Web servers with certificates issued by one of the following CAs are considered trusted. Untrusted web servers are allowed or denied based on the user's roles (see the role-specific Web Options page).

☐	Trusted Server CA	Valid dates
☐	America Online Root Certification Authority 1	2002/05/28 - 2037/11/19
☐	America Online Root Certification Authority 2	2002/05/28 - 2037/09/29
☐	Microsec e-Szigno Root CA	2005/04/6 - 2017/04/6

   b. Click on Import Trusted Server CA.

   c. On the Import Trusted Server CA screen, click on Browser, import the root CA certificate file.



Import Trusted Server CA

Certificate file

Import from: Browse No file chosen

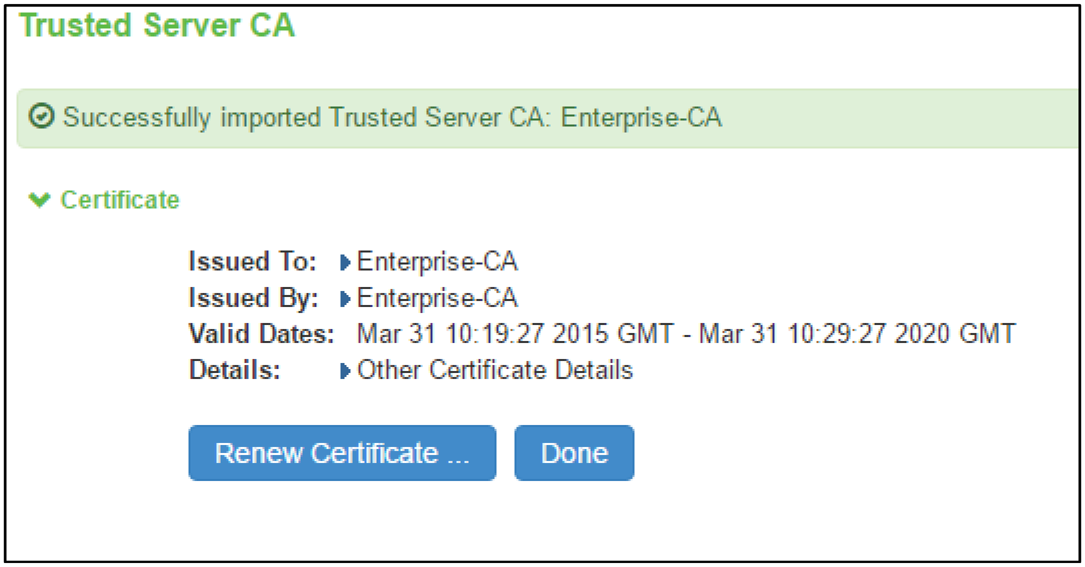
Import Trusted Server CA?

Import Certificate

File name: RootCA.cer

Note: In order to import CA Chain, all Sub CAs must be imported one by one.

d. Once CA or CA Chain is imported, click **Done**.



Trusted Server CA

Successfully imported Trusted Server CA: Enterprise-CA

Certificate

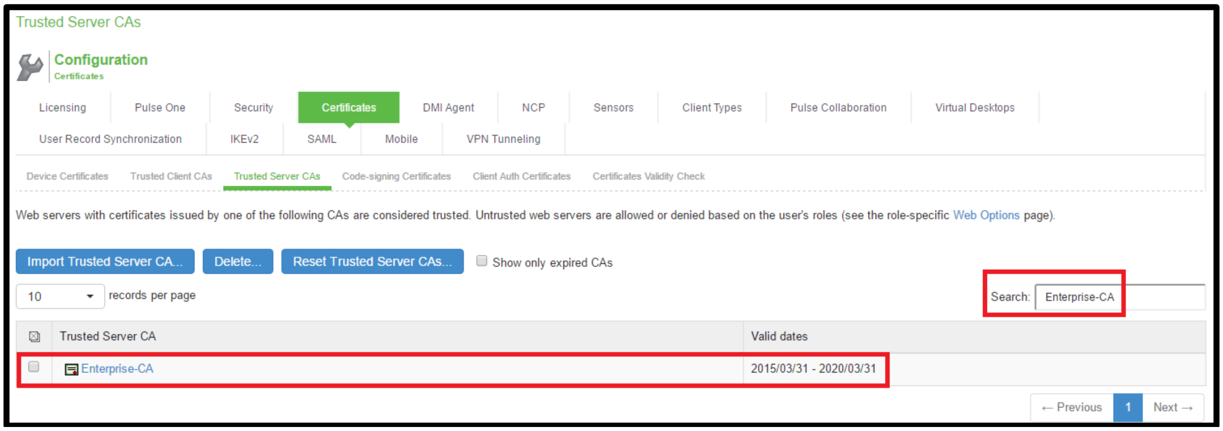
Issued To: Enterprise-CA

Issued By: Enterprise-CA

Valid Dates: Mar 31 10:19:27 2015 GMT - Mar 31 10:29:27 2020 GMT

Details: Other Certificate Details

e. The CA Common Name of the imported trusted server CA should be shown in the Trusted Server CA table on screen **System -> Configuration -> Certificates -> Trusted Server CAs**.



Trusted Server CAs

Web servers with certificates issued by one of the following CAs are considered trusted. Untrusted web servers are allowed or denied based on the user's roles (see the role-specific Web Options page).

□ Show only expired CAs

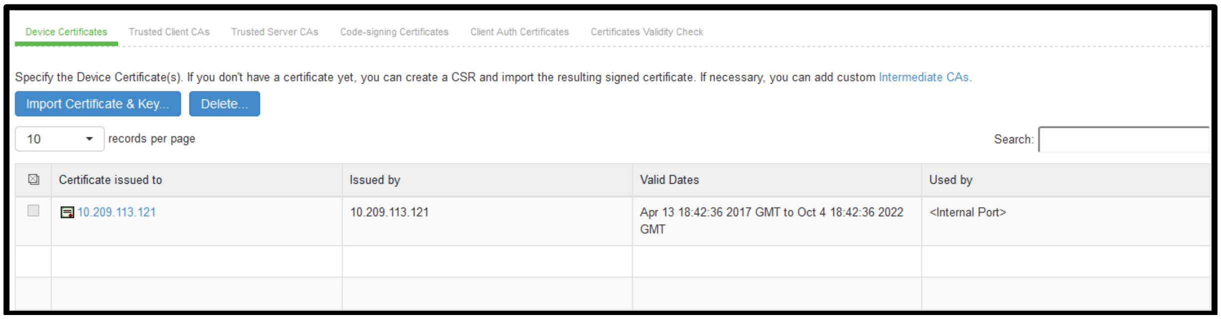
10 records per page

Search: Enterprise-CA

□	Trusted Server CA	Valid dates
□	Enterprise-CA	2015/03/31 - 2020/03/31

3. Import Device Certificate

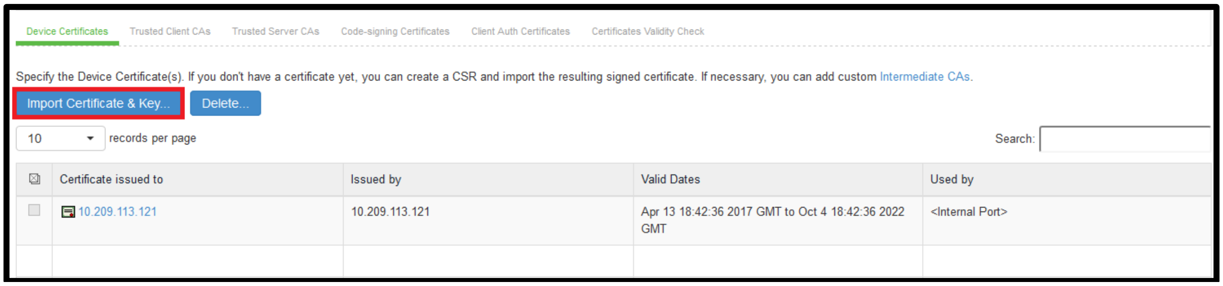
a. Navigate to **System > Configuration > Certificates > Device Certificate.**



Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

	Certificate issued to	Issued by	Valid Dates	Used by
□	10.209.113.121	10.209.113.121	Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT	<Internal Port>

b. Click on **Import Certificate & Key.**



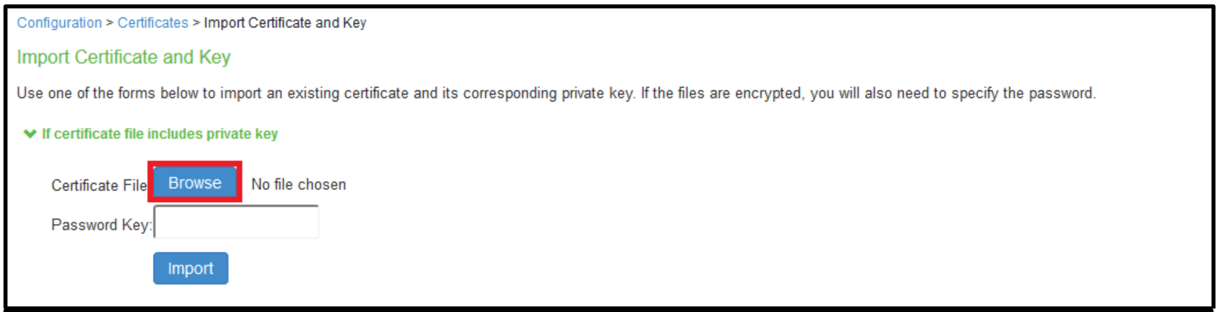
Device Certificates
Trusted Client CAs
Trusted Server CAs
Code-signing Certificates
Client Auth Certificates
Certificates Validity Check

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

Import Certificate & Key...
Delete...
10 records per page
Search:

	Certificate issued to	Issued by	Valid Dates	Used by
□	10.209.113.121	10.209.113.121	Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT	<Internal Port>

c. On the **Import Certificate & Key Page**, click on **Browse** to select the device certificate file having extendedKeyUsage field set for Server Authentication purpose.

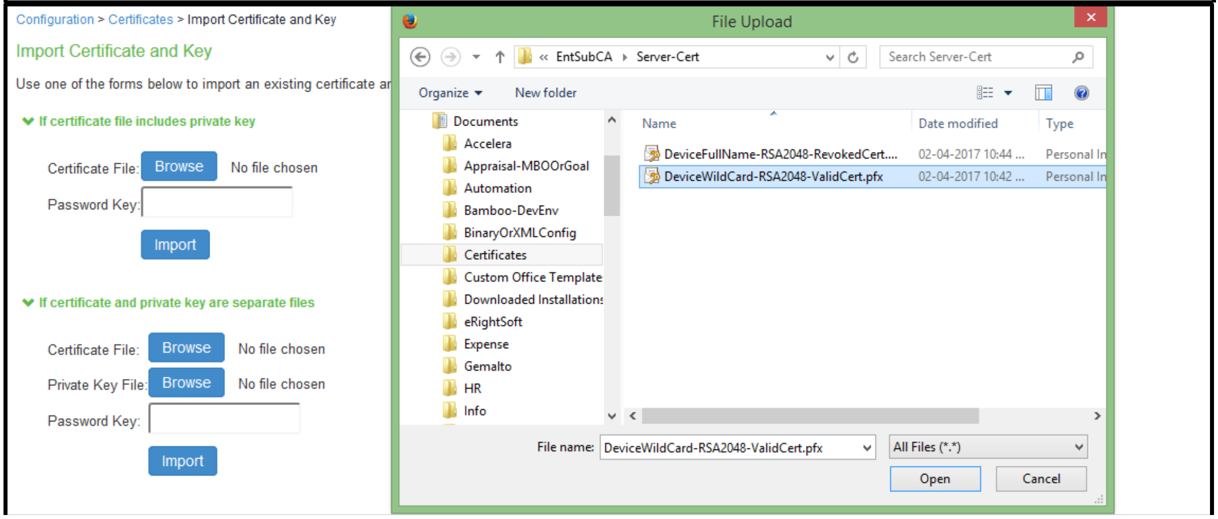


Configuration > Certificates > Import Certificate and Key

Import Certificate and Key

Use one of the forms below to import an existing certificate and its corresponding private key. If the files are encrypted, you will also need to specify the password.

If certificate file includes private key
Certificate File: Browse No file chosen
Password Key:
Import



Configuration > Certificates > Import Certificate and Key

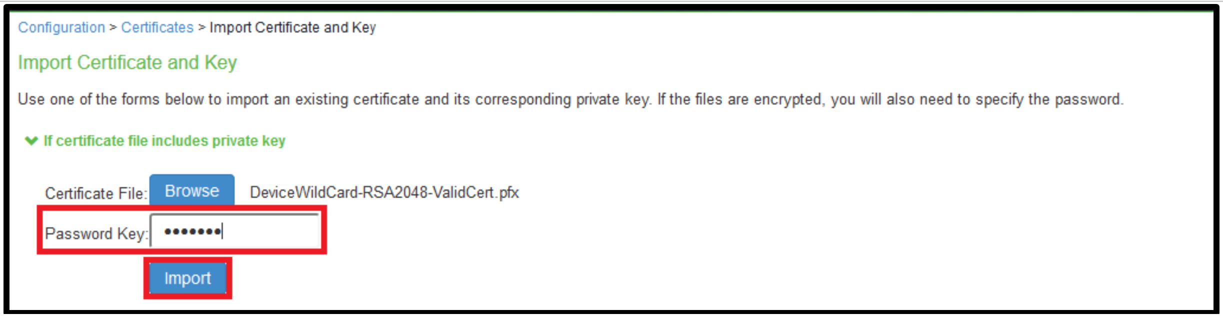
Import Certificate and Key

Use one of the forms below to import an existing certificate ar

Name	Date modified	Type
DeviceFullName-RSA2048-RevokedCert....	02-04-2017 10:44 ...	Personal In
DeviceWildCard-RSA2048-ValidCert.pfx	02-04-2017 10:42 ...	Personal In

File name: DeviceWildCard-RSA2048-ValidCert.pfx

d. Enter private key protected password in **Password Key** Textbox and click **Import.**



Configuration > Certificates > Import Certificate and Key

Import Certificate and Key

Use one of the forms below to import an existing certificate and its corresponding private key. If the files are encrypted, you will also need to specify the password.

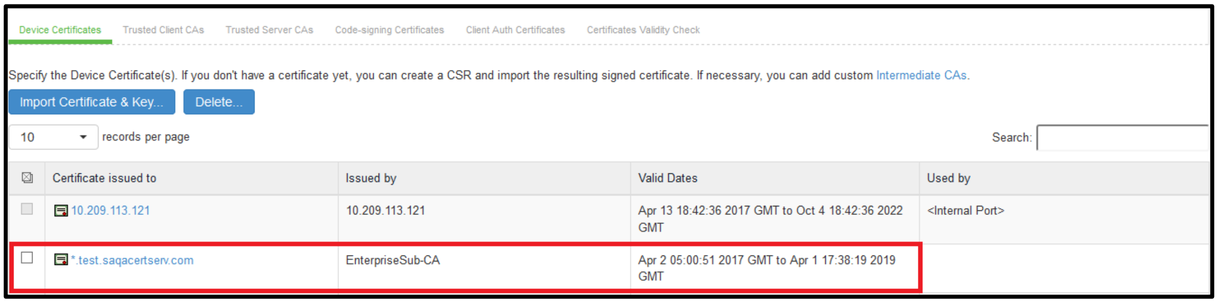
If certificate file includes private key

Certificate File: Browse DeviceWildCard-RSA2048-ValidCert.pfx

Password Key: •••••••

Import

e. The new certificate is shown in System -> Configuration -> Certificates -> Device Certificates.



Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

Import Certificate & Key... Delete...

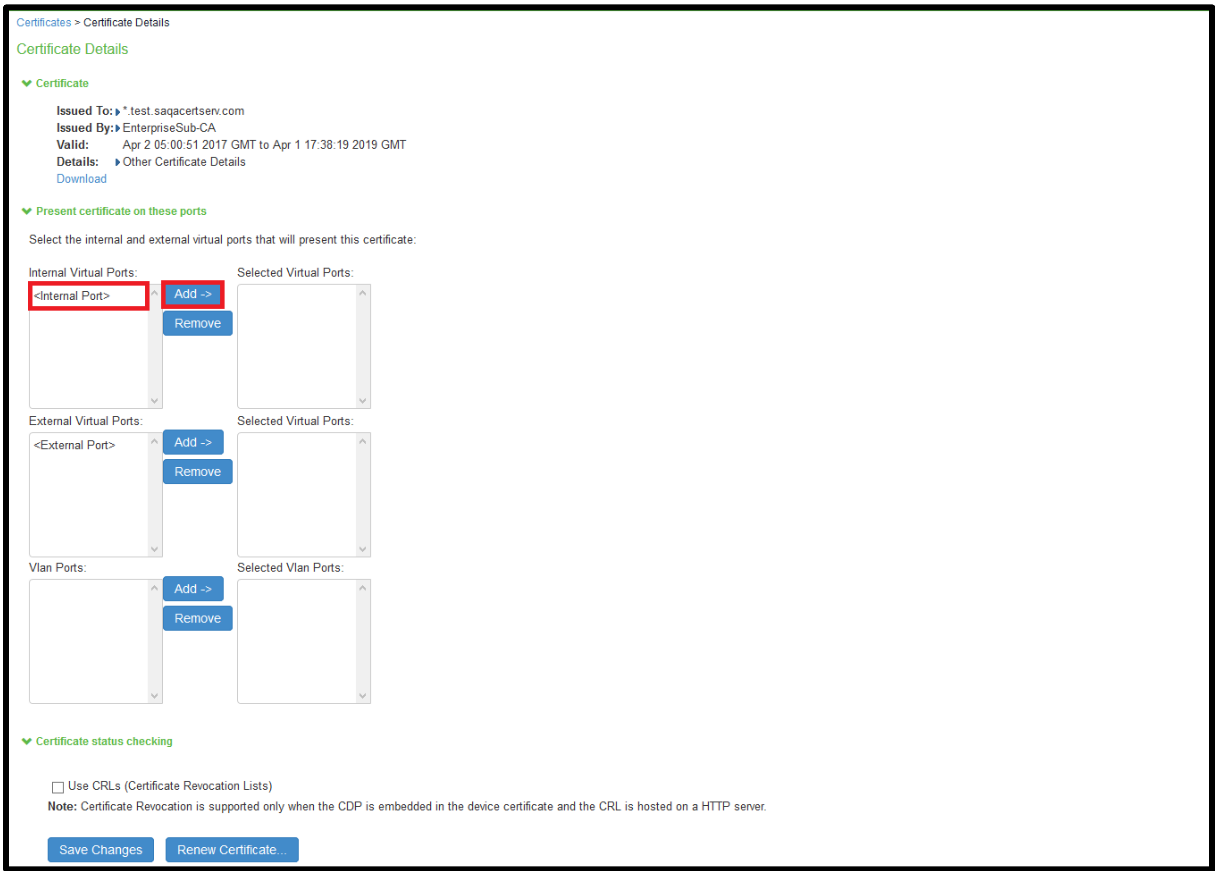
10 records per page Search:

□	Certificate issued to	Issued by	Valid Dates	Used by
□	10.209.113.121	10.209.113.121	Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT	<Internal Port>
□	*.test.saqacertserv.com	EnterpriseSub-CA	Apr 2 05:00:51 2017 GMT to Apr 1 17:38:19 2019 GMT	

f. Click on the certificate name that was created

g. The Certificate Details screen is shown, in the expanded Present certificate on these ports section, select <Internal Port> in the left panel that is labelled Internal Virtual Ports, click on Add -> to map it to the new device certificate.

If the <Internal Port> is not available in the left panel that is labelled Internal Virtual Ports, then the internal port is already mapped to a different device certificate, please see NOTE on instructions to remove the internal port from the currently mapped device certificate.



Certificates > Certificate Details

Certificate Details

Certificate

Issued To: *.test.saqacertserv.com
Issued By: EnterpriseSub-CA
Valid: Apr 2 05:00:51 2017 GMT to Apr 1 17:38:19 2019 GMT
Details: Other Certificate Details
Download

Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

Internal Virtual Ports: <Internal Port> Add -> Remove Selected Virtual Ports:

External Virtual Ports: <External Port> Add -> Remove Selected Virtual Ports:

Vlan Ports: Add -> Remove Selected Vlan Ports:

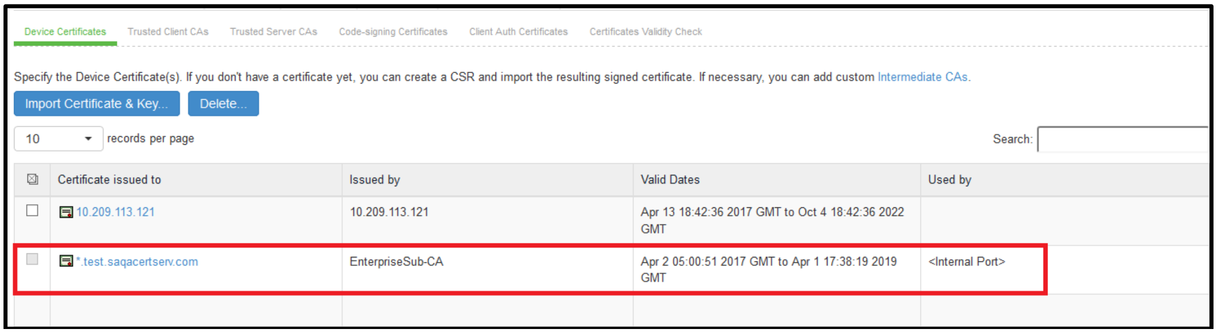
Certificate status checking

□ Use CRLs (Certificate Revocation Lists)

Note: Certificate Revocation is supported only when the CDP is embedded in the device certificate and the CRL is hosted on a HTTP server.

Save Changes Renew Certificate...

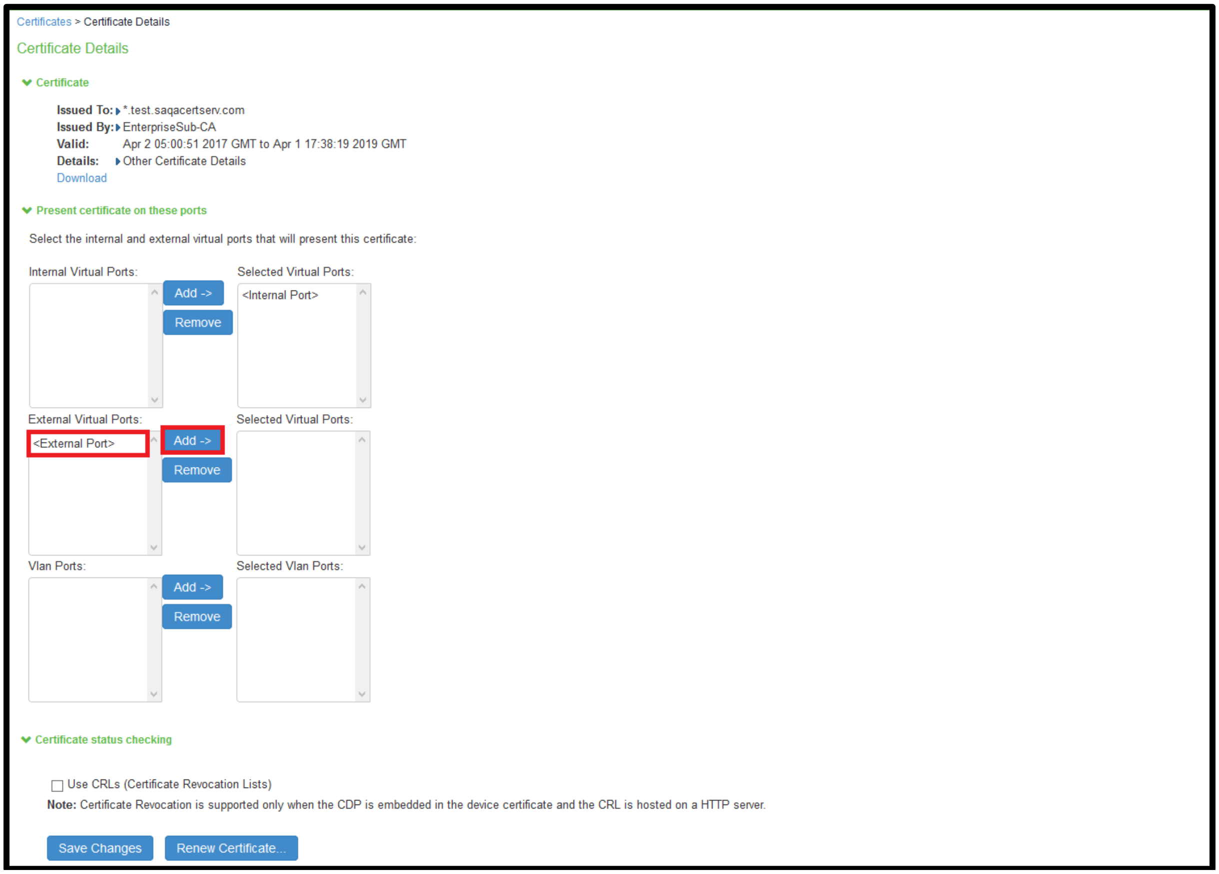
h. Click on Save Changes, the selected port in step 11 is shown in the Used by field for the new certificate.



Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

☐	Certificate issued to	Issued by	Valid Dates	Used by
☐	10.209.113.121	10.209.113.121	Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT	
☐	*.test.saqacertserv.com	EnterpriseSub-CA	Apr 2 05:00:51 2017 GMT to Apr 1 17:38:19 2019 GMT	<Internal Port>

i. The **Certificate Details** screen is shown, in the expanded **Present certificate on these ports** section, select **<External Port>** in the left panel that is labelled External Virtual Ports, click on **Add ->** to map it to the new device certificate.



Certificate Details

Certificate

Issued To: *.test.saqacertserv.com
Issued By: EnterpriseSub-CA
Valid: Apr 2 05:00:51 2017 GMT to Apr 1 17:38:19 2019 GMT
Details: Other Certificate Details
Download

Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

Internal Virtual Ports:

Selected Virtual Ports: <Internal Port>

External Virtual Ports: <External Port>

Selected Virtual Ports:

Vlan Ports:

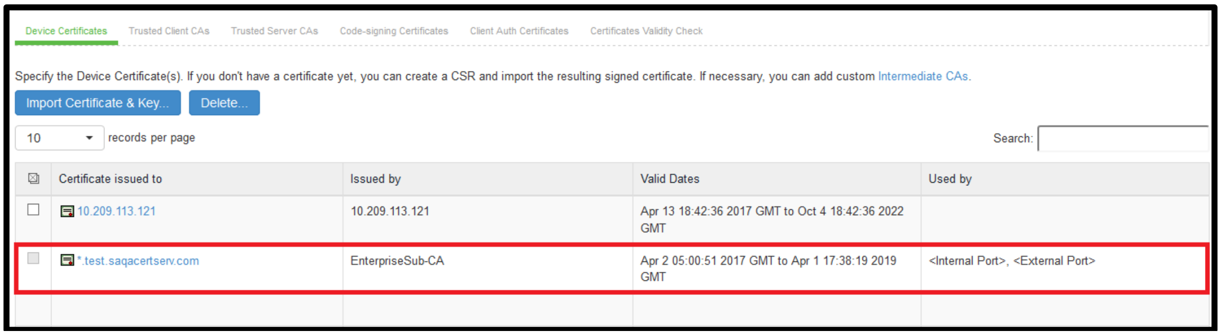
Selected Vlan Ports:

Certificate status checking

☐ Use CRLs (Certificate Revocation Lists)

Note: Certificate Revocation is supported only when the CDP is embedded in the device certificate and the CRL is hosted on a HTTP server.

j. Click on **Save Changes**, the selected port in step 6 is shown in the **Used by** field for the new certificate.

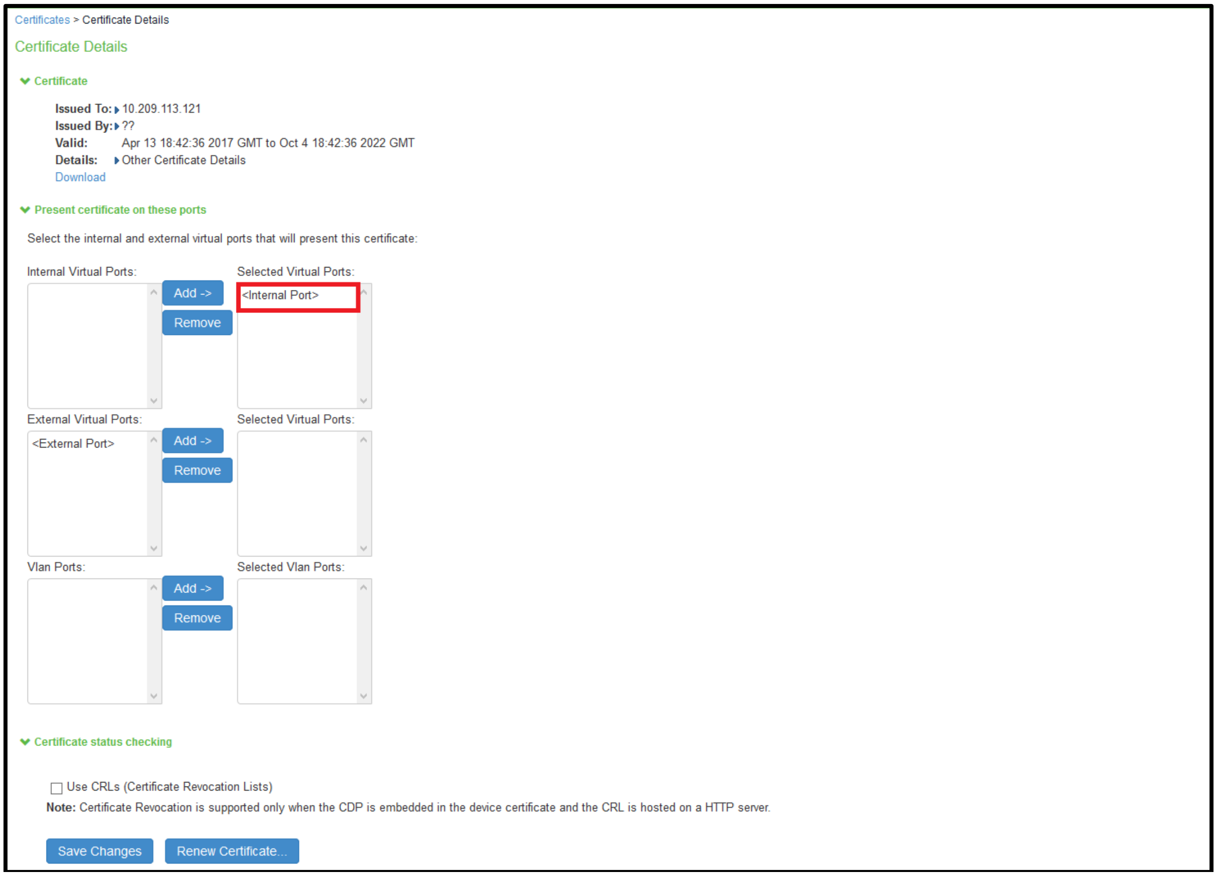


Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

☐	Certificate issued to	Issued by	Valid Dates	Used by
☐	10.209.113.121	10.209.113.121	Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT	
☐	*.test.saqacertserv.com	EnterpriseSub-CA	Apr 2 05:00:51 2017 GMT to Apr 1 17:38:19 2019 GMT	<Internal Port>, <External Port>

NOTE: If the internal port is already mapped to a different device certificate, do the following:

k. Click the device certificate that is mapped to the internal port and select <Internal Port> from Selected Virtual Ports box



Certificates > Certificate Details

Certificate Details

Certificate

Issued To: 10.209.113.121
Issued By: ??
Valid: Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT
Details: Other Certificate Details
Download

Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

Internal Virtual Ports:	Selected Virtual Ports:
	<Internal Port>

External Virtual Ports:	Selected Virtual Ports:
<External Port>	

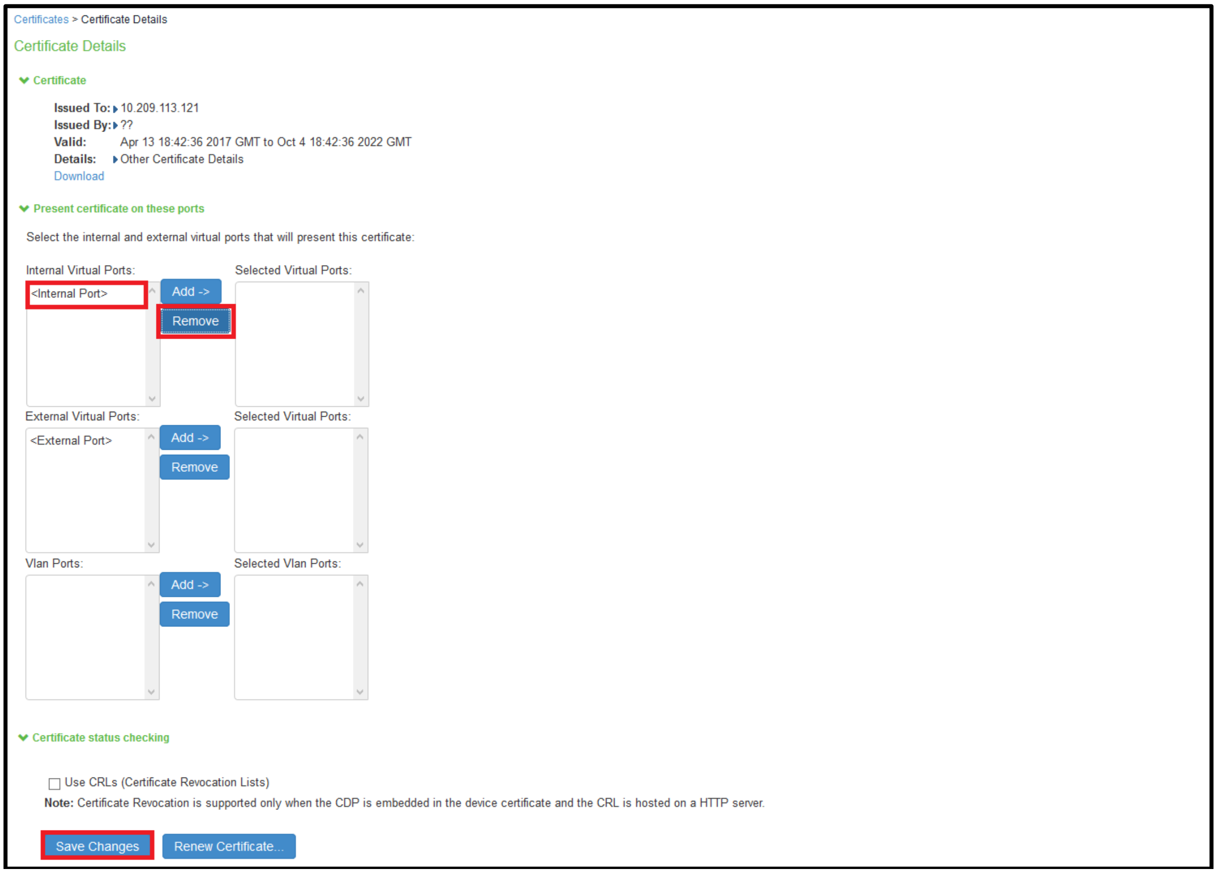
Vlan Ports:	Selected Vlan Ports:

Certificate status checking

□ Use CRLs (Certificate Revocation Lists)

Note: Certificate Revocation is supported only when the CDP is embedded in the device certificate and the CRL is hosted on a HTTP server.

l. Click on Remove to unmap the device certificate from the Internal port and Save Changes.



Certificates > Certificate Details

Certificate Details

Certificate

Issued To: 10.209.113.121
Issued By: ??
Valid: Apr 13 18:42:36 2017 GMT to Oct 4 18:42:36 2022 GMT
Details: Other Certificate Details
Download

Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

Internal Virtual Ports:	Selected Virtual Ports:
<Internal Port>	

External Virtual Ports:	Selected Virtual Ports:
<External Port>	

Vlan Ports:	Selected Vlan Ports:

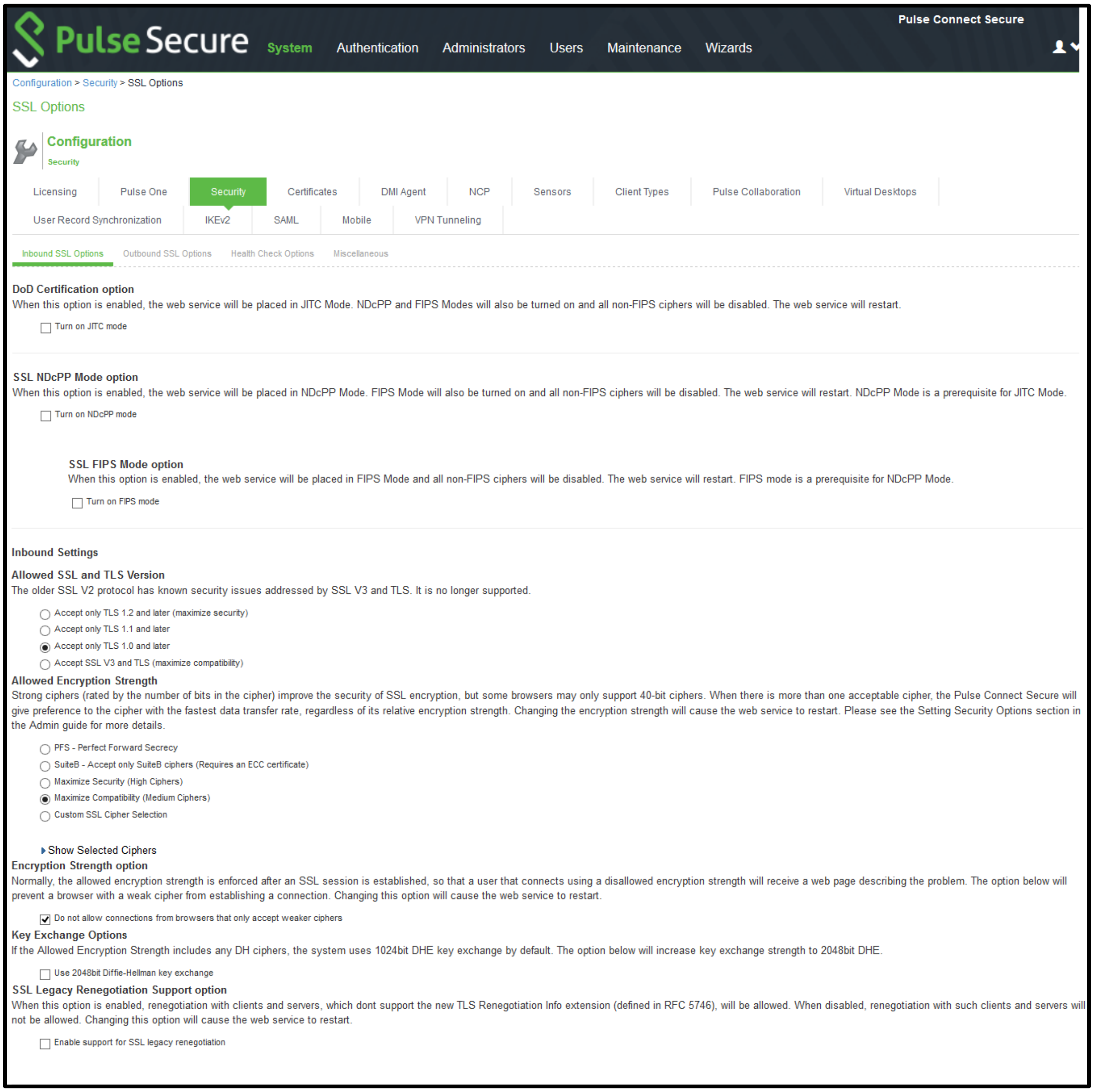
Certificate status checking

□ Use CRLs (Certificate Revocation Lists)

Note: Certificate Revocation is supported only when the CDP is embedded in the device certificate and the CRL is hosted on a HTTP server.

Enabling JITC Mode

1. On the PCS/PPS web console, navigate to System -> Configuration > Security > Inbound SSL Options.



DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

□ Turn on JITC mode

SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

□ Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode and all non-FIPS ciphers will be disabled. The web service will restart. FIPS mode is a prerequisite for NDcPP Mode.

□ Turn on FIPS mode

Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

○ Accept only TLS 1.2 and later (maximize security)
○ Accept only TLS 1.1 and later
● Accept only TLS 1.0 and later
○ Accept SSL V3 and TLS (maximize compatibility)

Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Connect Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

○ PFS - Perfect Forward Secrecy
○ SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
○ Maximize Security (High Ciphers)
● Maximize Compatibility (Medium Ciphers)
○ Custom SSL Cipher Selection

▸ Show Selected Ciphers

Encryption Strength option
Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using a disallowed encryption strength will receive a web page describing the problem. The option below will prevent a browser with a weak cipher from establishing a connection. Changing this option will cause the web service to restart.

☑ Do not allow connections from browsers that only accept weaker ciphers

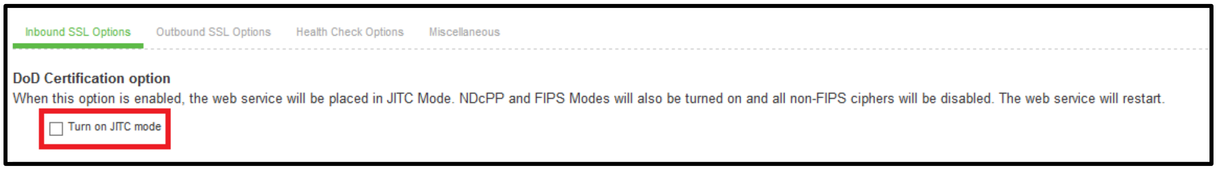
Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

□ Use 2048bit Diffie-Hellman key exchange

SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension (defined in RFC 5746), will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. Changing this option will cause the web service to restart.

□ Enable support for SSL legacy renegotiation

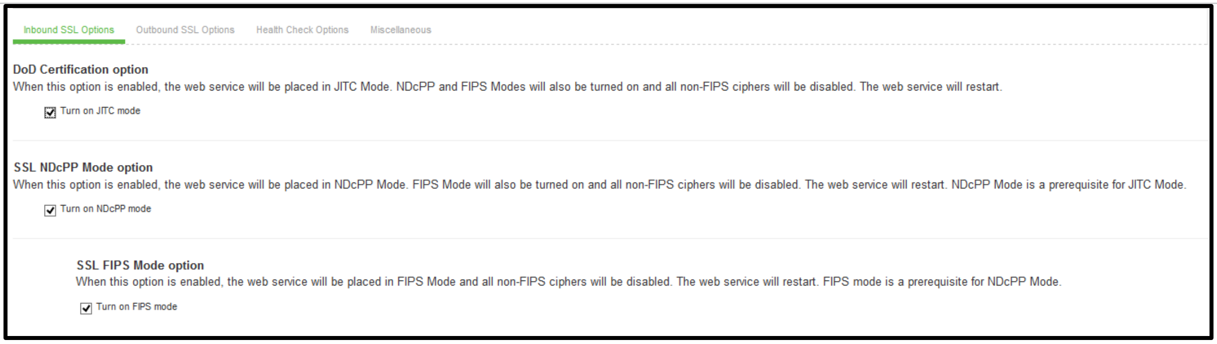
2. Click on Turn on JITC mode checkbox highlighted to make the PCS/PPS common criteria compliant.



DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

□ Turn on JITC mode

3. Once Turn on JITC mode is enabled, Turn on NDcPP mode and Turn on FIPS mode is also automatically enabled.



DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

☑ Turn on JITC mode

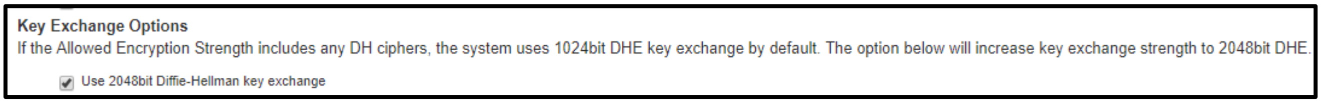
SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

☑ Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode and all non-FIPS ciphers will be disabled. The web service will restart. FIPS mode is a prerequisite for NDcPP Mode.

☑ Turn on FIPS mode

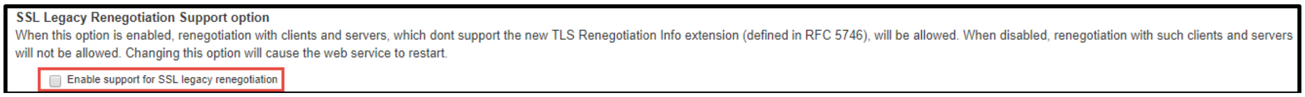
4. Enable Use 2048 bit Diffie-Hellman key exchange checkbox.



Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

☑ Use 2048bit Diffie-Hellman key exchange

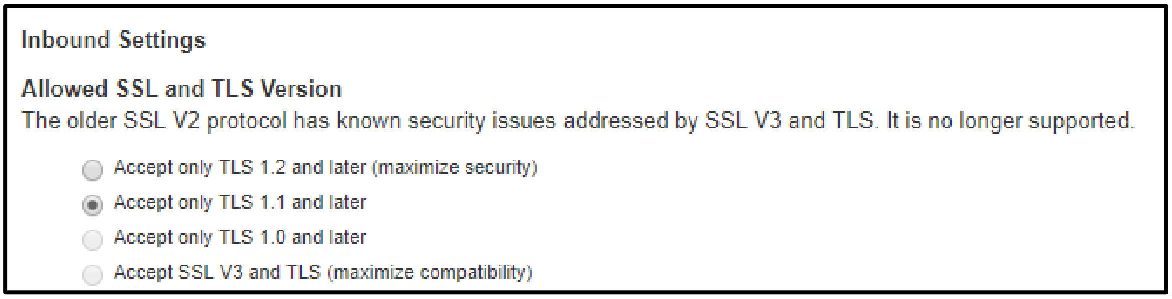
5. Uncheck SSL Legacy Renegotiation Support option.



SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension (defined in RFC 5746), will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. Changing this option will cause the web service to restart.

☐ Enable support for SSL legacy renegotiation

6. Click on Save Changes.
7. At this point, the Turn on JITC mode is enabled for both Inbound SSL Options and Outbound SSL Options and the following is shown:
   a. Accept only TLS1.0 and later and Accept SSL V3 and TLS (maximize compatibility) are disabled in the JITC mode. Accept only TLS 1.1 and later is selected by default.

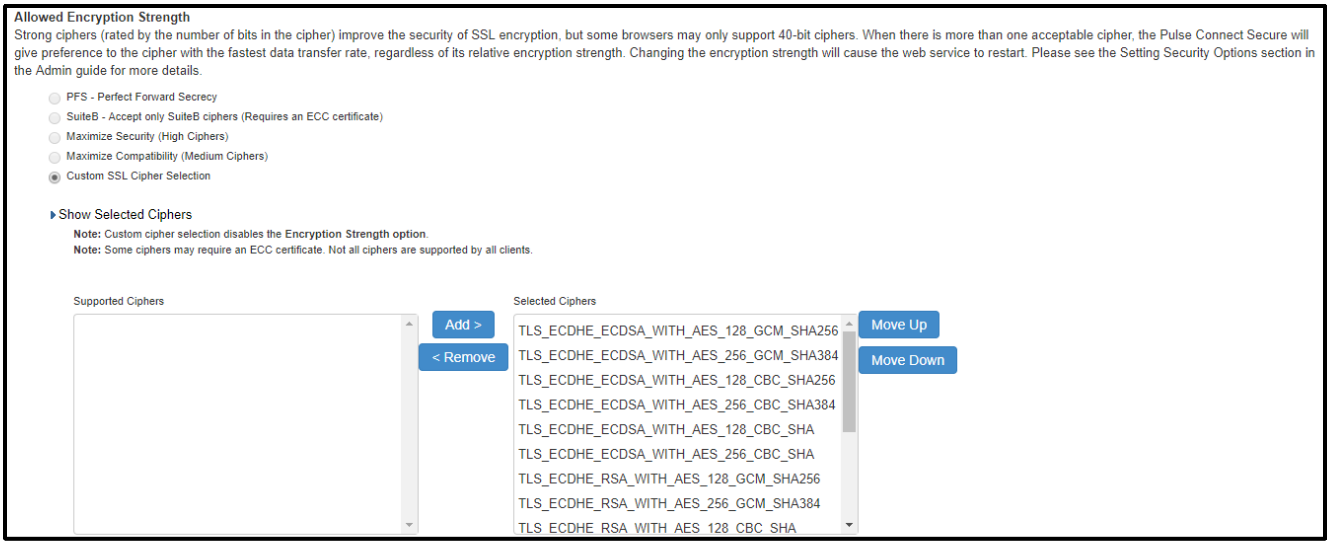


Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

○ Accept only TLS 1.2 and later (maximize security)
● Accept only TLS 1.1 and later
○ Accept only TLS 1.0 and later
○ Accept SSL V3 and TLS (maximize compatibility)

   b. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on Show Selected Ciphers displays below 16 Ciphers in the right panel labelled Selected Cipher.



Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Connect Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

○ PFS - Perfect Forward Secrecy
○ SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
○ Maximize Security (High Ciphers)
○ Maximize Compatibility (Medium Ciphers)
● Custom SSL Cipher Selection

▸ Show Selected Ciphers

Note: Custom cipher selection disables the **Encryption Strength option**.
Note: Some ciphers may require an ECC certificate. Not all ciphers are supported by all clients.

Supported Ciphers

Selected Ciphers

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

   c. Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel, and click “Remove” button to remove it from the “Selected Ciphers”.

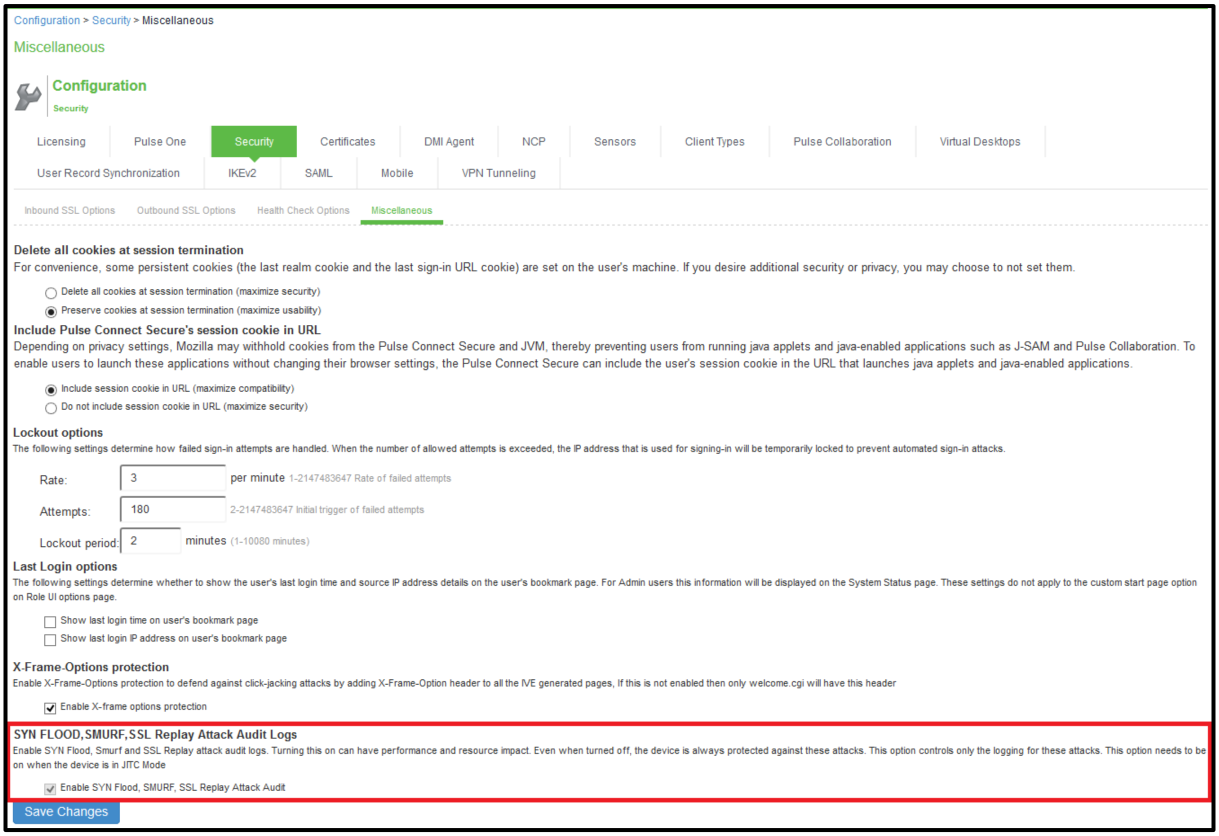
d. Navigate to **System -> Configuration > Security > outbound SSL Options.**

e. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on **Show Selected Ciphers** displays below 16 Ciphers in the right panel labelled **Selected Cipher**.

f. Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel, and click "Remove" button to remove it from the "Selected Ciphers".

g. Navigate to **System -> Configuration > Security > Miscellaneous.**

h. **Enable SYN Flood, SMURF, SSL Replay Attack Audit** checkbox will be automatically enabled.



Delete all cookies at session termination

For convenience, some persistent cookies (the last realm cookie and the last sign-in URL cookie) are set on the user's machine. If you desire additional security or privacy, you may choose to not set them.

○ Delete all cookies at session termination (maximize security)
● Preserve cookies at session termination (maximize usability)

Include Pulse Connect Secure's session cookie in URL

Depending on privacy settings, Mozilla may withhold cookies from the Pulse Connect Secure and JVM, thereby preventing users from running java applets and java-enabled applications such as J-SAM and Pulse Collaboration. To enable users to launch these applications without changing their browser settings, the Pulse Connect Secure can include the user's session cookie in the URL that launches java applets and java-enabled applications.

● Include session cookie in URL (maximize compatibility)
○ Do not include session cookie in URL (maximize security)

Lockout options

The following settings determine how failed sign-in attempts are handled. When the number of allowed attempts is exceeded, the IP address that is used for signing-in will be temporarily locked to prevent automated sign-in attacks.

Rate: 3 per minute 1-2147483647 Rate of failed attempts
Attempts: 180 2-2147483647 Initial trigger of failed attempts
Lockout period: 2 minutes (1-10080 minutes)

Last Login options

The following settings determine whether to show the user's last login time and source IP address details on the user's bookmark page. For Admin users this information will be displayed on the System Status page. These settings do not apply to the custom start page option on Role UI options page.

□ Show last login time on user's bookmark page
□ Show last login IP address on user's bookmark page

X-Frame-Options protection

Enable X-Frame-Options protection to defend against click-jacking attacks by adding X-Frame-Option header to all the IVE generated pages, If this is not enabled then only welcome.cgi will have this header

☑ Enable X-frame options protection

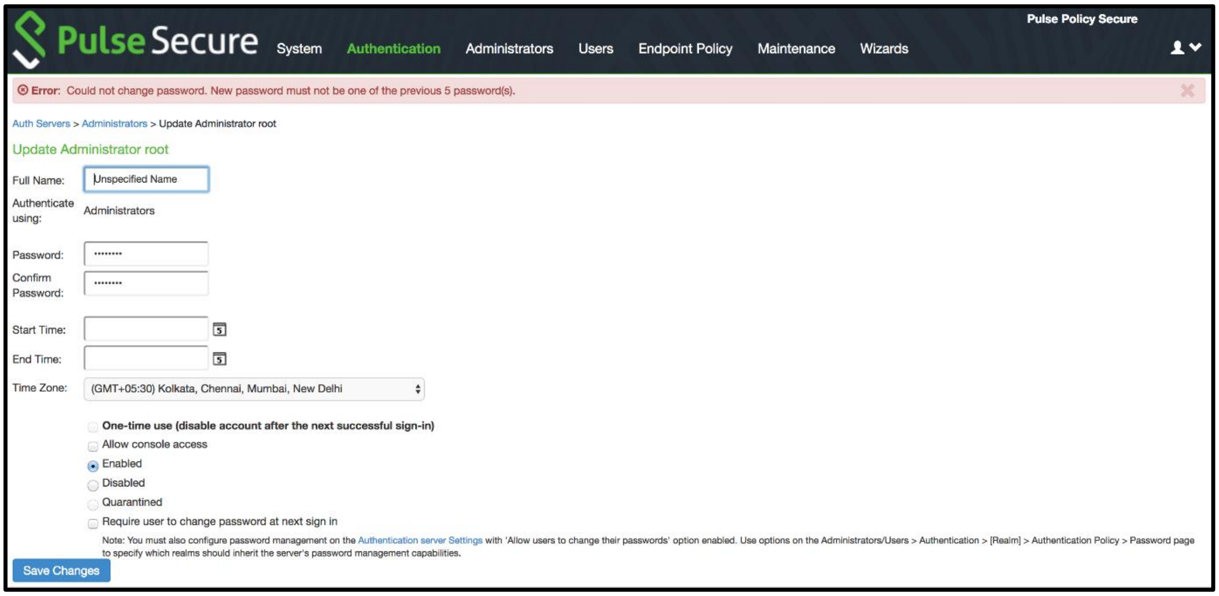
SYN FLOOD,SMURF,SSL Replay Attack Audit Logs

Enable SYN Flood, Smurf and SSL Replay attack audit logs. Turning this on can have performance and resource impact. Even when turned off, the device is always protected against these attacks. This option controls only the logging for these attacks. This option needs to be on when the device is in JITC Mode

☑ Enable SYN Flood, SMURF, SSL Replay Attack Audit

Password Strengthening

When JITC is enabled, PCS/PPS does not allow an administrator to configure a password exactly same as previously configured 5 passwords. An error message is displayed in this case.



⊗ **Error:** Could not change password. New password must not be one of the previous 5 password(s).

Auth Servers > Administrators > Update Administrator root

Update Administrator root

Full Name: Unspecified Name

Authenticate using: Administrators

Password: ••••••••

Confirm Password: ••••••••

Start Time:

End Time:

Time Zone: (GMT+05:30) Kolkata, Chennai, Mumbai, New Delhi

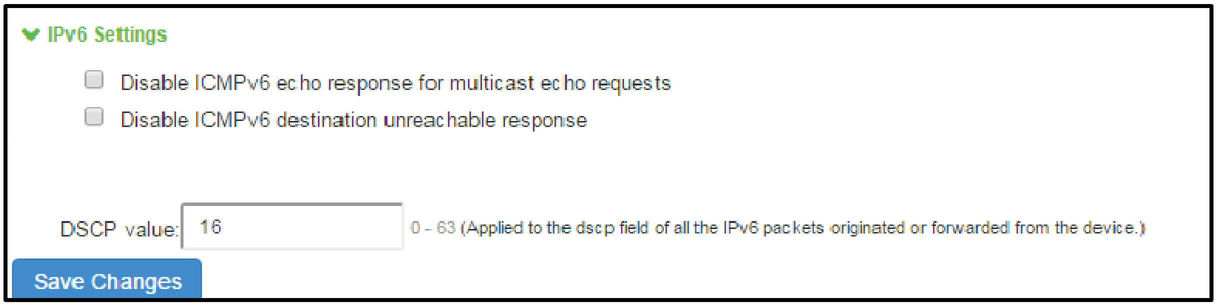
□ **One-time use (disable account after the next successful sign-in)**
□ Allow console access
● Enabled
○ Disabled
○ Quarantined
□ Require user to change password at next sign in

Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

Configuring JITC IPv6 Settings

To enable IPv6 settings and to configure DSCP value:

1. Navigate to **system->network->overview** and scroll down to see IPv6 settings.
2. Select both the check boxes under IPv6 settings.



□ Disable ICMPv6 echo response for multicast echo requests

□ Disable ICMPv6 destination unreachable response

DSCP value: 16 0 - 63 (Applied to the dscp field of all the IPv6 packets originated or forwarded from the device.)

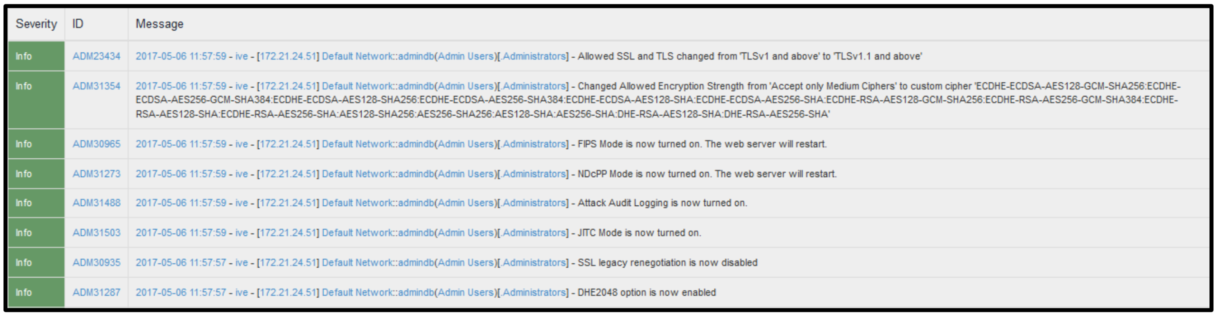
3. Configure the DSCP value by entering the value in the space provided below the check boxes.
4. Click on **save changes**.

IPv6 Settings	
Disable ICMPv6 echo response for multicast echo	Used to enable/disable echo reply. If the check box is enabled, the multicast echo request will be dropped in the PCS/PPS.
Disable ICMPv6 destination unreachable response	Used to enable/disable destination unreachable message. If the check box is enabled, a destination unreachable message is dropped in the PCS/PPS.
DSCP Value	Specify the value from 0-63 for the traffic sourced by the device. When applied, all traffic from the PCS/PPS will be using same DSCP value. The specified value is applied to every IPV6 packets originated from the PCS/PPS to the destination.

Audit Logs For JITC Mode

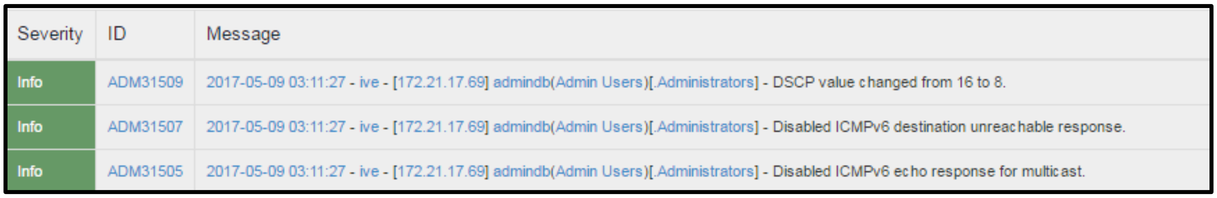
JITC Mode Enable Configuration Admin Logs

Navigate to System -> Log/Monitoring -> Admin Access -> Logs and Check for the logs mentioned in Audit logs



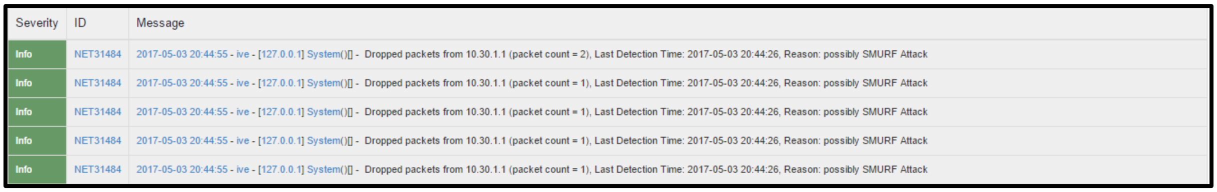
Severity	ID	Message
Info	ADM23434	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - Allowed SSL and TLS changed from 'TLSv1 and above' to 'TLSv1.1 and above'
Info	ADM31354	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - Changed Allowed Encryption Strength from 'Accept only Medium Ciphers' to custom cipher 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA'
Info	ADM30965	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - FIPS Mode is now turned on. The web server will restart.
Info	ADM31273	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - NDcPP Mode is now turned on. The web server will restart.
Info	ADM31488	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - Attack Audit Logging is now turned on.
Info	ADM31503	2017-05-06 11:57:59 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - JITC Mode is now turned on.
Info	ADM30935	2017-05-06 11:57:57 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - SSL legacy renegotiation is now disabled
Info	ADM31287	2017-05-06 11:57:57 - ive - [172.21.24.51] Default Network::admindb(Admin Users)[.Administrators] - DHE2048 option is now enabled

IPv6 Settings to be Verified in Admin Logs



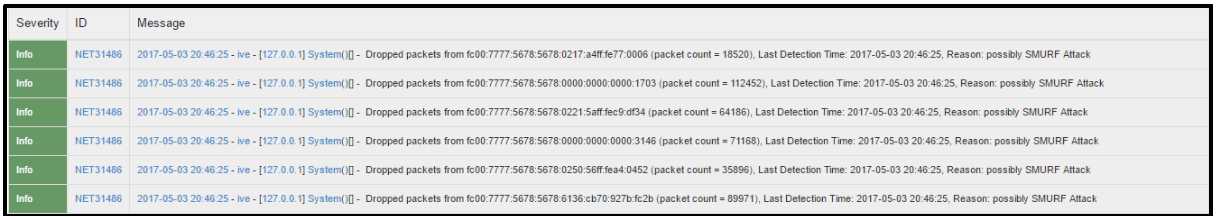
Severity	ID	Message
Info	ADM31509	2017-05-09 03:11:27 - ive - [172.21.17.69] admindb(Admin Users)[.Administrators] - DSCP value changed from 16 to 8.
Info	ADM31507	2017-05-09 03:11:27 - ive - [172.21.17.69] admindb(Admin Users)[.Administrators] - Disabled ICMPv6 destination unreachable response.
Info	ADM31505	2017-05-09 03:11:27 - ive - [172.21.17.69] admindb(Admin Users)[.Administrators] - Disabled ICMPv6 echo response for multicast.

Detection and Prevention of SMURF Attack IPv4 Event Logs



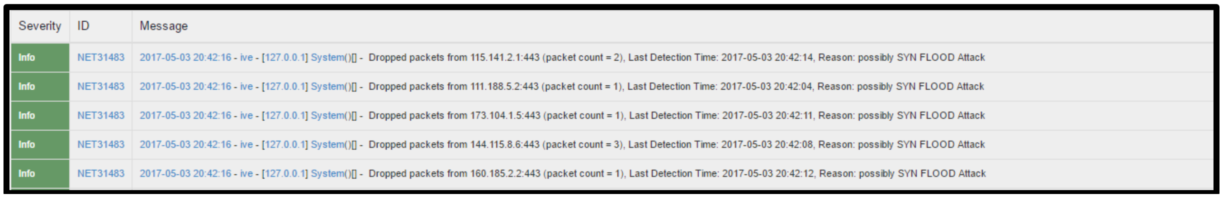
Severity	ID	Message
Info	NET31484	2017-05-03 20:44:55 - ive - [127.0.0.1] System()[] - Dropped packets from 10.30.1.1 (packet count = 2), Last Detection Time: 2017-05-03 20:44:26, Reason: possibly SMURF Attack
Info	NET31484	2017-05-03 20:44:55 - ive - [127.0.0.1] System()[] - Dropped packets from 10.30.1.1 (packet count = 1), Last Detection Time: 2017-05-03 20:44:26, Reason: possibly SMURF Attack
Info	NET31484	2017-05-03 20:44:55 - ive - [127.0.0.1] System()[] - Dropped packets from 10.30.1.1 (packet count = 1), Last Detection Time: 2017-05-03 20:44:26, Reason: possibly SMURF Attack
Info	NET31484	2017-05-03 20:44:55 - ive - [127.0.0.1] System()[] - Dropped packets from 10.30.1.1 (packet count = 1), Last Detection Time: 2017-05-03 20:44:26, Reason: possibly SMURF Attack
Info	NET31484	2017-05-03 20:44:55 - ive - [127.0.0.1] System()[] - Dropped packets from 10.30.1.1 (packet count = 1), Last Detection Time: 2017-05-03 20:44:26, Reason: possibly SMURF Attack

Detection and Prevention of SMURF Attack IPv6 Event Logs



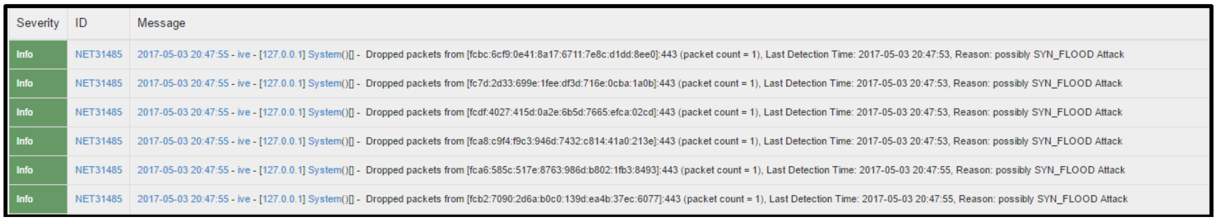
Severity	ID	Message
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:0217:a4ff:fe77:0006 (packet count = 18520), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:0000:0000:0000:1703 (packet count = 112452), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:0221:5aff:fec9:df34 (packet count = 64186), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:0000:0000:0000:3146 (packet count = 71168), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:0250:56ff:fea4:0452 (packet count = 35896), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack
Info	NET31486	2017-05-03 20:46:25 - ive - [127.0.0.1] System()[] - Dropped packets from fc00:7777:5678:5678:6136:cb70:927b:fc2b (packet count = 89971), Last Detection Time: 2017-05-03 20:46:25, Reason: possibly SMURF Attack

Detection and Prevention of SYN Flood Attack IPv4 Event Logs



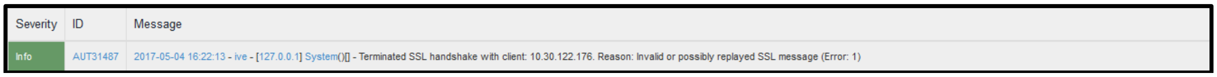
Severity	ID	Message
Info	NET31483	2017-05-03 20:42:16 - ive - [127.0.0.1] System()[] - Dropped packets from 115.141.2.1:443 (packet count = 2), Last Detection Time: 2017-05-03 20:42:14, Reason: possibly SYN FLOOD Attack
Info	NET31483	2017-05-03 20:42:16 - ive - [127.0.0.1] System()[] - Dropped packets from 111.188.5.2:443 (packet count = 1), Last Detection Time: 2017-05-03 20:42:04, Reason: possibly SYN FLOOD Attack
Info	NET31483	2017-05-03 20:42:16 - ive - [127.0.0.1] System()[] - Dropped packets from 173.104.1.5:443 (packet count = 1), Last Detection Time: 2017-05-03 20:42:11, Reason: possibly SYN FLOOD Attack
Info	NET31483	2017-05-03 20:42:16 - ive - [127.0.0.1] System()[] - Dropped packets from 144.115.8.6:443 (packet count = 3), Last Detection Time: 2017-05-03 20:42:08, Reason: possibly SYN FLOOD Attack
Info	NET31483	2017-05-03 20:42:16 - ive - [127.0.0.1] System()[] - Dropped packets from 160.185.2.2:443 (packet count = 1), Last Detection Time: 2017-05-03 20:42:12, Reason: possibly SYN FLOOD Attack

Detection and Prevention of SYN Flood Attack IPv6 Event Logs



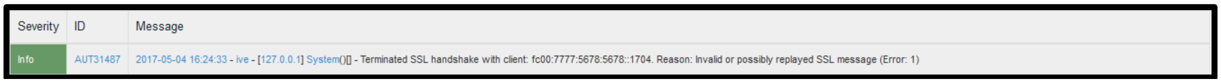
Severity	ID	Message
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fcbc:6cf9:0e41:8a17:6711:7e8c:d1dd:8ee0]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:53, Reason: possibly SYN_FLOOD Attack
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fc7d:2d33:699e:1fee:df3d:716e:0cba:1a0b]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:53, Reason: possibly SYN_FLOOD Attack
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fcdf:4027:415d:0a2e:6b5d:7665:efca:02cd]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:53, Reason: possibly SYN_FLOOD Attack
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fca8:c9f4:f9c3:946d:7432:c814:41a0:213e]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:53, Reason: possibly SYN_FLOOD Attack
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fca6:585c:517e:8763:986d:b802:1fb3:8493]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:55, Reason: possibly SYN_FLOOD Attack
Info	NET31485	2017-05-03 20:47:55 - ive - [127.0.0.1] System()[] - Dropped packets from [fcb2:7090:2d6a:b0c0:139d:ea4b:37ec:6077]:443 (packet count = 1), Last Detection Time: 2017-05-03 20:47:55, Reason: possibly SYN_FLOOD Attack

Detection and Prevention of SSL Replay Attack IPv4 Event Logs:



Severity	ID	Message
Info	AUT31487	2017-05-04 16:22:13 - ive - [127.0.0.1] System()[] - Terminated SSL handshake with client: 10.30.122.176. Reason: Invalid or possibly replayed SSL message (Error: 1)

Detection and Prevention of SSL Replay Attack IPv6 Event Logs:



Severity	ID	Message
Info	AUT31487	2017-05-04 16:24:33 - ive - [127.0.0.1] System()[] - Terminated SSL handshake with client: fc00:7777:5678:5678::1704. Reason: Invalid or possibly replayed SSL message (Error: 1)

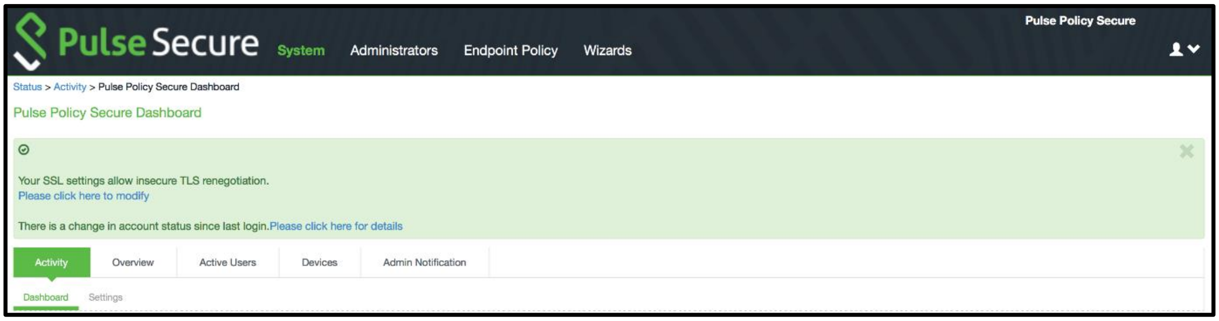
Notification for Unsuccessful Admin Login Attempts

With JITC Mode on, PCS/PPS shows a banner with the count of unsuccessful login attempt. This includes any change in the admin status that has happened since the last successful login.

Upon clicking the banner, the administrator is directed to the status page, which provides more details about the status or configuration change since last the log-in.

These configuration changes will be cleared before the next login, so that the admin can see different set of configurations changes, if anything has happened from the last login.

Banner for Unsuccessful Admin Login Attempts:



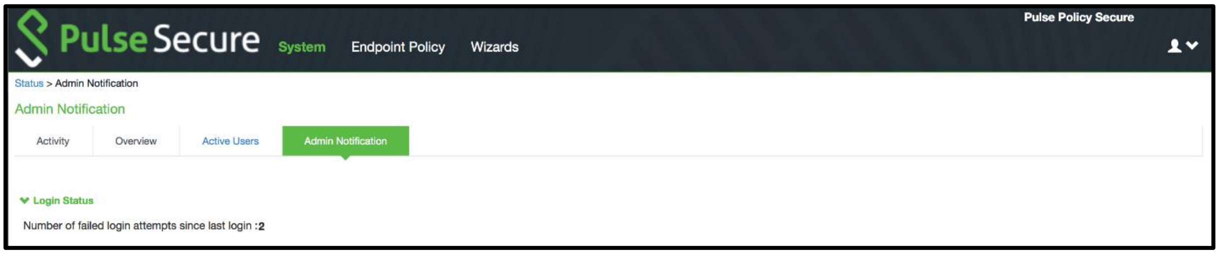
Status > Activity > Pulse Policy Secure Dashboard

Pulse Policy Secure Dashboard

Your SSL settings allow insecure TLS renegotiation.
Please click here to modify

There is a change in account status since last login.Please click here for details

Admin Notification for Unsuccessful Admin Login attempts



Status > Admin Notification

Admin Notification

Login Status

Number of failed login attempts since last login :2