PCS/PPS NDcPP and JITC Certification: Deployment Guide
Contents

PURPOSE OF THIS DOCUMENT ............................................................................................................................. 4
NDCPP MODE ..................................................................................................................................................... 5
STEPS TO SETUP THE PCS/PPS FOR NDCPP .................................................................................................... 6
  Prerequisites for PCS/PPS Configurations ........................................................................................................ 6
  Password Minimum Length Configuration ....................................................................................................... 6
  Serial Console Access Control Configuration .................................................................................................. 6
  Terminating a Local Console Session .............................................................................................................. 9
  Administrative Banner Configuration .............................................................................................................. 9
  Configure GUI Inactivity Timeout Period ......................................................................................................... 11
  Terminating a GUI Session ............................................................................................................................. 11
  Import Trusted Client CA ................................................................................................................................ 11
  Import Trusted Server CA ................................................................................................................................ 13
SOFTWARE UPDATES ..................................................................................................................................... 14
ENABLING NDCPP MODE ................................................................................................................................ 16
AUDIT LOGS FOR NDCPP MODE ...................................................................................................................... 19
  NDCPP Mode Enable Configuration Admin Logs ............................................................................................. 19
  NDCPP Mode Disable Configuration Admin Logs ........................................................................................... 19
JITC MODE ......................................................................................................................................................... 20
PREREQUISITES FOR ENABLING JITC MODE .................................................................................................... 21
ENABLING JITC MODE ....................................................................................................................................... 27
PASSWORD STRENGTHENING ............................................................................................................................. 30
CONFIGURING JITC IPv6 SETTINGS .................................................................................................................. 31
AUDIT LOGS FOR JITC MODE ........................................................................................................................... 32
  JITC Mode Enable Configuration Admin Logs ................................................................................................ 32
  IPv6 Settings to be Verified in Admin Logs ...................................................................................................... 32
  Detection and Prevention of SMURF Attack IPv4 Event Logs ......................................................................... 32
  Detection and Prevention of SMURF Attack IPv6 Event Logs ......................................................................... 32
  Detection and Prevention of SYN Flood Attack IPv4 Event Logs ................................................................. 32
  Detection and Prevention of SYN Flood Attack IPv6 Event Logs ................................................................. 32
  Detection and Prevention of SSL Replay Attack IPv4 Event Logs ............................................................... 33
  Detection and Prevention of SSL Replay Attack IPv6 Event Logs ............................................................... 33
NOTIFICATION FOR UNSUCCESSFUL ADMIN LOGIN ATTEMPTS ..................................................................... 33
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
- Software Updates
- Enabling NDcPP Mode
- Audit Logs For 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:
   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.

<table>
<thead>
<tr>
<th>Authentication/Authorization Servers</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Local Authentication</td>
</tr>
<tr>
<td>Chassis Auth Server</td>
<td>Chassis SSO</td>
</tr>
<tr>
<td>System Local</td>
<td>Local Authentication</td>
</tr>
</tbody>
</table>

- Select **Administrators**.
- Click on **Users** tab.

```markdown
**Auth Servers > Administrators**

**Administrators**

Settings  Users

Show users named: *  Show 200 users  Update

New...  Delete...  Page 1 of 1  <  <  >  >|

<table>
<thead>
<tr>
<th></th>
<th>Username</th>
<th>Name</th>
<th>Console Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin</td>
<td>Platform Administrator</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>admindb</td>
<td>Platform Administrator</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>admindb_web</td>
<td>User created through script</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>darumuga</td>
<td>User created through script</td>
<td>No</td>
</tr>
</tbody>
</table>
```

- Click on administrator name configured in Initial Setup.
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.

   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”.
Terminating a Local Console Session

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

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
c. Click on New 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
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 Sign In Notifications section, select the check box Pre-Auth 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
2. Click **Import CA Certificates** button to import CA or Chain of CAs one by one as explained below in different Screenshots

![Import Trusted Client CA](image1)

3. Click on **Import Certificate**.

![Import Trusted Client CA](image2)

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

2. Click on **Import Trusted Server CA**...

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

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**.

![Trusted Server CAs]

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.
3. Navigate to **Maintenance -> System -> Upgrade/Downgrade.**
4. In the expanded Install Server Package section, click on From File option, then click on Browse to select the server package downloaded earlier.

5. Click Install to start the installation process.

6. Below information is shown during installation.
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**.
2. Click on the *Turn on NDcPP mode* checkbox highlighted to make the PCS/PPS common criteria compliant.

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

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

5. Uncheck *SSL Legacy Renegotiation Support option*.

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.
   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.
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.

<table>
<thead>
<tr>
<th>Info</th>
<th>ADM23434</th>
<th>&lt;current timestamp&gt; &lt;node name&gt; &lt;IP Address&gt; &lt;user id&gt; &lt;Realm&gt; &lt;Role&gt; – Allowed SSL and TLS changed from ‘TLSv1 and above’ to ‘TLS1.1 and above’.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>ADM31354</td>
<td>&lt;current timestamp&gt; &lt;node name&gt; &lt;IP Address&gt; &lt;user id&gt; &lt;Realm&gt; &lt;Role&gt; – Changed Allowed Encryption Strength from &lt;ciphersuite&gt; to &lt;ciphersuite&gt;.</td>
</tr>
<tr>
<td>Info</td>
<td>ADM30965</td>
<td>&lt;current timestamp&gt; &lt;node name&gt; &lt;IP Address&gt; &lt;user id&gt; &lt;Realm&gt; &lt;Role&gt; – FIPS mode is now turned on. The web server will restart.</td>
</tr>
<tr>
<td>Info</td>
<td>ADM31273</td>
<td>&lt;current timestamp&gt; &lt;node name&gt; &lt;IP Address&gt; &lt;user id&gt; &lt;Realm&gt; &lt;Role&gt; – NDcPP mode is now turned on. The web server will restart.</td>
</tr>
</tbody>
</table>

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
- Enabling JITC Mode
- Password Strengthening
- Configuring JITC IPv6 Settings
- Audit Logs For JITC Mode
- Notification for Unsuccessful Admin Login Attempts
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](https://a.b.c.d/admin) using admin credentials.
   
   Note: The admin credentials are configured during the initial setup via console.

   ![Welcome to Pulse Connect Secure](image)

2. Import Trusted Server CA. For this, on the administrator web console:
   a. Navigate to System -> Configuration -> Certificates -> Trusted Server CAs.

   ![Trusted Server CAs](image)

   b. Click on Import Trusted Server CA.

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

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.

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

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

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

d. Enter private key protected password in **Password Key** textbox and click **Import**.
e. The new certificate is shown in **System -> Configuration -> Certificates -> Device Certificates.**

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.**

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

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

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.

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

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

   ![Screen shot showing System -> Configuration > Security > Inbound SSL Options]

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

   ![Screen shot showing 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.
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 1024 bit DH key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

Use 2048 bit 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 don’t 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.

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.

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.”

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.
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.
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.

3. Configure the DSCP value by entering the value in the space provided below the check boxes.

4. Click on **save changes**.

<table>
<thead>
<tr>
<th>IPv6 Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable ICMPv6 echo response for multicast echo</td>
<td>Used to enable/disable echo reply. If the check box is enabled, the multicast echo request will be dropped in the PCS/PPS.</td>
</tr>
<tr>
<td>Disable ICMPv6 destination unreachable response</td>
<td>Used to enable/disable destination unreachable message. If the check box is enabled, a destination unreachable message is dropped in the PCS/PPS.</td>
</tr>
<tr>
<td>DSCP Value</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

IPv6 Settings to be Verified in Admin Logs

Detection and Prevention of SMURF Attack IPv4 Event Logs

Detection and Prevention of SYN Flood Attack IPv4 Event Logs

Detection and Prevention of SYN Flood Attack IPv6 Event Logs
Detection and Prevention of SSL Replay Attack IPv4 Event Logs:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>20190419 00:24:20, 10.2.3.4:443: [Client] - Terminated SSL handshake with client: 10.30.122.179. Reason: Invalid or possibly replayed SSL handshake (Error: 1).</td>
</tr>
</tbody>
</table>

Detection and Prevention of SSL Replay Attack IPv6 Event Logs:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>20190419 00:24:20, 10.2.3.4:443: [Client] - Terminated SSL handshake with client: 10.30.122.179. Reason: Invalid or possibly replayed SSL handshake (Error: 1).</td>
</tr>
</tbody>
</table>

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 login.

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: