Oracle® Communications Convergent Charging Controller

Provisioning Interface Help

Release 12.0.6
F43257-01
August 2022

Oracle Communications Convergent Charging Controller Provisioning Interface Help, Release 12.0.6

F43257-01

Contents

6 PI Password Expiry

1 PI Commands

The **Commands** tab of the PI Administration screen enables you to set the security level for PI commands.

Note: Commands cannot be added to or removed from the list of available commands.

Commands fields

This table describes the function of each field.

Field	Description
Name	The PI command name.
Security Level	The security level required to execute the command.
Subscriber Domain	Indicates the command applies to an account that belongs to the subscriber domain, that is, the account exists on the SMS, the account wallet may be on a VWS or on a third party billing engine.
Wallet Domain	Indicates the command applies to an account that belongs to the wallet domain, that is, both the account and wallet exists on the SMS and VWS.
Voucher Domain	Indicates the command applies to a voucher that belongs to the voucher domain, that is, a voucher that exists on the VWS.

Editing PI commands

Follow these steps to edit a PI command.

1. From the list of PI commands on the **Commands** tab, select the command you want to edit.
2. Click **Edit**.

   Result: The edit dialog box for the selected command appears. See Commands fieldsCommands fields for a description of each field.
3. Change the **Security Level** as required.

   Note: Range is 1 to 99 (highest) inclusive.
4. Click **Save**.

   Result: The details are saved to the database.
5. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI Commands

2
PI Hosts

The **Hosts** tab of the PI Administration screen enables you to configure the hosts from which PI commands can be run. Before a new client can connect, it must be added to the database.

Hosts fields

This table describes the function of each field.

Field	Description
IP Address	The unique IP address of the host which will be allowed to run commands in the PI. **Note:** You cannot modify the IP address after it is first saved.
Description	A description of the host defined in the **IP Address** field, such as the hostname. The PI does not use the description value when connecting to the host.

Adding hosts

Follow these steps to add new hosts to the PI.

1. On the **Hosts** tab, click **New**.

   Result: The PI Hosts screen displays. See Hosts fields for a description of each field.
2. In the **IP Address** field, type the IP address of the host.
3. In the **Description** field, type a description for the host, such as the hostname.
4. Click **Save**.

   Result: The new host details are saved in the database.
5. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI Hosts

Editing hosts

Follow these steps to edit host information in the PI.

1. On the **Hosts** tab, select from the list the host to edit.
2. Click **Edit**.

Result: The PI Hosts screen appears showing the data for the selected host record. See Hosts fields for a description of each field.

3. Change the host **Description** as required.
4. Click **Save**.

   Result: The details are saved to the database.
5. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI Hosts

Deleting hosts

Follow these steps to delete a host from the PI.

1. In the **Hosts** tab, select from the list the host to delete.
2. Click **Delete**.

   Result: The Delete Confirmation screen displays.
3. Click **OK**.

   Result: The host is removed from the database.
4. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI Hosts

3
PI MAC Pairs

The **MAC Pairs** tab of the Administration screen enables you to configure the MAC pairs from which commands can be run in PI. MAC pairs are the security keys to encode and decode encrypted data.

MAC Pairs fields

This table describes the function of each field.

Field	Description
MAC Pair	The unique MAC pair number for this MAC pair. **Note:** This field cannot be changed after it is first saved.
MAC #1	The MAC address of the first MAC address in this MAC pair. This must be an 8 digit number.
MAC #2	The MAC address of the second MAC address in this MAC pair. This must be an 8 digit number.

Adding MAC Pairs

Follow these steps to add new MAC pairs to the PI.

1. On the **MAC Pairs** tab, click **New**.

   Result: The PI MACS screen displays. See MAC Pairs fields for a description of each field.
2. Enter in the **MAC Pair** field the unique MAC pair number.
3. Enter in the **MAC #1** field the MAC address of the first entry for the MAC pair.
4. Enter in the **MAC #2** field the MAC address of the second entry for the MAC pair.
5. Click **Save**.

   Result: The new MAC pair details are saved in the database.
6. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI MAC Pairs

Editing MAC Pairs

Follow these steps to edit MAC pair information in the PI.

1. On the **MAC Pairs** tab, select from the list the MAC pair to edit.

2. Click **Edit**.

   Result: The PI MACS screen fields will be populated with the data for the selected MAC pair record. See MAC Pairs fields for a description of each field.

3. Change the MAC pair details as required.
4. Click **Save**.

   Result: The details are saved to the database.

5. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI MAC Pairs

Deleting MAC Pairs

Follow these steps to delete a MAC pair from the PI.

1. On the **MAC Pairs** tab, select from the list the MAC pair to delete.
2. Click **Delete**.

   Result: The Delete Confirmation screen displays.

3. Click **OK**.

   Result: The MAC pairs are removed from the database.

4. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI MAC Pairs

4
PI Users

The **Users** tab of the PI Administration screen enables you to add new PI users and to edit and delete existing PI users.

When you add a new PI user you select the service providers to associate with the user. The PI user can run PI commands only for those service providers. This allows you to restrict the data that the PI user can query or modify through the PI. The PI returns a NACK if a PI user attempts to run a PI command for a service provider that they are not associated with.

In addition, you specify the connection details and security level of the PI user. The first command sent to the PI by the PI user will be a connect command, specifying the username and password. PI users can access only those commands that have a security level less than or equal to their security level. Users can use only the MAC pair specified in their profile and are restricted to using the port specified on the screen.

Users fields

The following table describes the function of each field in the PI Users screen.

Field	Description
User	The unique username for this user. **Note:** This field cannot be changed after it is first saved.
Enter Password	Sets the password for this PI user.
Confirm Password	Confirms the user's password.
Security Level	The security level for this user. Specify a value between 1 and 99 (inclusive) The user will be able to run PI commands with security levels equal to or lower than this number.
Allow CCSVR1 Private Secret Decryption	Permission for the user to decrypt voucher private secret to obtain HRN.
Port Number	The port number this user can connect from.
MAC Pair	The MAC pair this user can connect from. MAC pairs are the security keys to encode and decode encrypted data.
Currency	The reporting currency for this user.
Last Password Change	Date of the last successful password change for this PI User.
Failed Logins	The number of login failures since the last successful login.

Field	Description
Lock Reason	Displays the reason that a user has been locked out of the system. You can unlock a locked PI user by clearing this field. If a user fails to log in to the system in three successive attempts, the system locks the account and the following text is displayed: `LOCKED: Failed login, maximum attempts exceeded.` For more information about locked accounts, see Unlocking locked PI users. **Warning:** When you create a user, leave this field blank to avoid creating a locked account.
Available Service Providers	The list of service providers that you can associate with this user.
Associated Service Providers	The list of service providers associated with this user. For PI commands that allow a service provider to be specified, the data that this user can update or query through the PI is restricted to data that is managed by a service provider in this list.

Adding PI users

Follow these steps to add a new PI user.

1. On the **Users** tab, click **New**.

   Result: The PI Users screen appears. See Users fields for a description of each field.
2. In the **User** field, type a unique username for the PI user you want to add.
3. In the **Enter Password** field, type the user's password.
4. In the **Confirm Password** field, retype the user's password to confirm.
5. In the **Security Level** field, type the command security level for this user. Specify a value between 1 and 99 (inclusive). The user will be able to run PI commands with security levels equal to or lower than this number.
6. From the **Port Number** list, select the port the user can connect from. To allow the user to connect from any port, select `Any`.
7. From the **MAC Pair** list, select the MAC pair the user will connect from.
8. From the **Currency** list, select the reporting currency for the user.
9. Add the service providers the PI user will be able to run PI commands for to the list of associated service providers:
   - To add a service provider to the list, select the service provider in the **Available Service Providers** box and click **Add**.

- To remove a service provider from the list, select the service provider in the **Associated Service Providers** box and click **Remove**.

10. Click **Save**.

    Result: The new user details are saved in the database.

Related topic

PI Users

Editing PI users

Follow these steps to edit the details of a PI user.

1. From the list of PI users on the **Users** tab, select the user whose details you want to edit.
2. Click **Edit**.

   Result: The PI Users screen is populated with the data from the selected user record. See Users fields for a description of each field.
3. Change the user details as required.
4. Click **Save**.

   Result: The details are saved to the database.

Related topic

PI Users

Deleting PI users

Follow these steps to delete a PI user.

1. From the list of PI users on the **Users** tab, select the user you want to delete.
2. Click **Delete**.

   Result: The Delete Confirmation dialog box appears.
3. Click **OK**.

   Result: The PI user is removed from the database.
4. Soft restart the PI. For details, see *Soft PI Restart* in *PI User's and Technical Guide*.

   Result: The updated configuration details will be loaded by the PImanager.

Related topic

PI Users

Unlocking locked PI users

PI users could be locked for the following reasons:

- By using an incorrect user name or password combination in three successive attempts.
- When their account has expired.

When an account is locked for any reason, the **Lock Reason** field in the PI Users screen displays the reason.

You can unlock locked PI users by resetting the password or clearing the **Lock Reason** field.

Follow these steps to unlock a locked PI user's account by resetting the password:

1. From the list of PI users on the **Users** tab, select the user account you want to unlock.
2. Click **Edit**.

   Result: The PI Users screen is populated with the data from the selected user record. See Users fields for a description of each field.
3. Specify a new password for the PI user.

> **Note:**
>
> Ensure that the new password you specify complies with the configured password policy.

4. Click **Save**.

   Result: The new password is saved and the PI user account is unlocked.

Related topic

PI Users

5
PI Ports

The **Ports** tab of the PI Administration screen enables the configuration of the ports the PIprocesses listens on.

Ports fields

This table describes the function of each field.

Field	Description
Port	The unique port number which will have a PIprocess listening on it. **Note:** This field cannot be changed after it is first saved.
Secure	If **Y**, the port will be secure. If **N**, the port will be insecure.
Max. Connections	The maximum number of concurrent connections to the port.
Type	The type of PI commands which can be run on this port.

Adding ports

Follow these steps to add new ports to the PI.

1. On the **Ports** tab, click **New**.

   Result: The PI Ports screen appears. See Ports fields for a description of each field.
2. Enter in the **Port** field the port number.
3. Select the **Secure** check box if this port should be secure.

   Deselect the **Secure** check box if this port is not required to be secure.
4. In the **Max. Connections** field, type the maximum number of concurrent connections this port will support.
5. From the **Type** list, select the type of commands that can be run on this port.
6. Click **Save**.

   Result: The new port details are saved in the database.
7. Hard restart the PI. See *Hard PI Restart* in *PI User's and Technical Guide*.

   Result: The new configuration details are loaded by the PImanager.

Related topic

PI Ports

Editing ports

Follow these steps to edit port information in the PI.

1. On the **Ports** tab, select the port you want to edit.
2. Click **Edit**.

   Result: The PI Ports screen is populated with the data from the selected port record. See Ports fields for a description of each field.
3. Change the port details as required.
4. Click **Save**.

   Result: The details are saved to the database.
5. Hard restart the PI. See *Hard PI Restart* in *PI User's and Technical Guide*.

   Result: The new configuration details are loaded by the PImanager.

Related topic

PI Ports

Deleting ports

Follow these steps to delete a port from the PI.

1. On the **Ports** tab, select the port to delete.
2. Click **Delete**.

   Result: The Delete Confirmation dialog box appears.
3. Click **OK**.

   Result: The port is removed from the database.
4. Hard restart the PI. See *Hard PI Restart* in *PI User's and Technical Guide*.

   Result: The new configuration details are loaded by the PImanager.

Related topic

PI Ports

6
PI Password Expiry

The **Password Expiry** tab of the PI Administration screen enables you to configure the number of days after which PI user's password should expire. You can also disable password expiration from this tab.

Password Expiry fields

This table describes the function of each field.

Field	Description
Duration(In days)	Number of days after which password should expire.
DisablePassword Expiry	Selecting this checkbox disables password expiry and password will never expire for PI users.

Configuring password expiry

Follow these steps to configure password expiry for PI users.

1. Click on the **Password Expiry** tab.
2. In the **Duration(In days)** field, enter the number of days after which the password should expire.

> **Note:**
>
> Select **Disable Password Expiry** checkbox if you do not want the PI user password to expire.

3. Click **Save**.

   Result: The password expiry configuration is saved.
4. Hard restart the PI. For details, see *Hard PI Restart* in *PI User's and Technical Guide*.

   Result: The new configuration details are loaded by the PImanager.

Related topic

PI Password Expiry