



## Tools Menu

---

The Tools menu of the Unified CCX Administration web interface provides access to system tools you can use to perform a variety of administrative tasks and contains the following menu options:

- **Plug-ins**—to download plug-ins that you can use to enhance the Unified CCXEngine.
- **Real-Time Reporting**—to generate reports that provide detailed information about the status of your Unified CCX system.
- **Real-Time Snapshot Config**—to configure the Unified CCX database connection to a wallboard display.
- **Historical Reporting**—to perform Historical Reporting tasks, including configuring the database server, synchronizing data, configuring users, installing client software, and purging your database.
- **User Management**—to assign access levels to administrators and supervisors.
- **Password Management**—to reset passwords for external database access users like workforce management, historical reporting user and so on.
- **W1 Upgrade**—to show if you have selected "Upgrade from a previous Unified CCX release" option during initial Appadmin setup in a single-node or high availability deployment.

The following sections describe the various menu options.

- [Plug-Ins Menu, on page 1](#)
- [Real-Time Reporting Tool, on page 2](#)
- [Real-Time Snapshot Config Menu, on page 3](#)
- [Historical Reporting Menu, on page 7](#)
- [User Management Menu, on page 9](#)
- [Password Management, on page 13](#)

## Plug-Ins Menu

The Unified CCX system includes software components called *plug-ins* that you can use to enhance the Unified CCXEngine. You can download these plug-ins from the Plug-ins web page.

To access the Plug-ins web page, choose **Tools** > **Plug-ins** from the Unified CCXAdministration menu bar.

The Plug-ins web page contains one or more of the following hyperlinks (depending on the Unified CCX package you have purchased):

- **Cisco Unified CCX Editor**—Click this hyperlink to install the client-side Unified CCX Editor. For more information, see the *Cisco Unified Contact Center Express Getting Started with Scripts and Cisco Unified Contact Center Express Editor Step Reference Guide*.
- **Cisco Unified CCX Real-Time Monitoring Tool for Windows**—Click this hyperlink to install client-side Unified CCX Serviceability Real-Time Monitoring Tool (RTMT) for Windows. This tool monitors real-time behavior of the components in a Unified CCX cluster. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug in is available only for users with administrator capability.




---

**Note** To download on Windows, right-click **Download** hyperlink and select Save Target As option.

---

- **Cisco Unified CCX Real-Time Monitoring Tool for Linux**—Click this hyperlink to install client-side Unified CCX Serviceability Real-Time Monitoring Tool (RTMT) for Linux. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug in is available only for users with administrator capability.
- **Cisco Unified CCX Real-Time Reporting Tool**- Click this hyperlink to download and launch the Real-Time Reporting Tool. This provides real-time reports to monitor Unified CCX system activity. RTR client tool is a Java application and hence requires Java Runtime Environment (JRE) to be installed on the client machine. It runs outside the web browser and prompts for user authentication. **Note** : To download, right click on Download hyperlink and select Save Target As option.

## Real-Time Reporting Tool




---

**Caution** While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for RmCm configuration, and Real-Time Reporting.

---

The Real Time Reporting (RTR) client is a Java application that is used to generate various reports that provide detailed information about the status of the Unified CCX system.

You can download and access the RTR client from the Unified CCX Administration, Tools menu at the following paths:

- **Tools > Real Time Reporting.**
- **Tools > Plug-ins.**

To run the Real Time Reporting client,

- In the **Security** tab of the **Java Control Panel**, add the fully qualified domain name (FQDN) of the Unified CCX server to the **Exception Site List**. For a high availability deployment, add the FQDN of both the Unified CCX servers to the **Exception Site List**.

- In the **Advanced** tab of the **Java Control Panel**, select the **Use TLS 1.2** option in the **Advanced Security Settings**.

The RTR client is a Java application. You can double-click the downloaded RTR file to run the client on the client machine. You can access the RTR client with the Unified CCX Administrator or Supervisor credentials. You must close it after you have run the reports for the Unified CCX system. The RTR client requires Java 1.7.0\_80 or later to run on the client machine.




---

**Note** The Real Time Reporting (RTR) client online help requires user authentication, if the Cisco Unified CCX Administration user interface is not currently active in the web browser.

---

## Real-Time Snapshot Config Menu

Many call centers use wallboards to display their real-time reporting status. Wallboards can display data such as available agents in CSQs, call volumes, talk times, wait times, and number of handled calls. You can enable the Unified CCX system to write Unified CCX real-time information to a database that can then be displayed on a wallboard.




---

**Note** You must purchase the wallboard separately, and configure and control it with its own wallboard software. Wallboard software and hardware are supported by the third-party wallboard vendors, not by Cisco.

You must install the wallboard software on a separate machine or desktop, not on the Unified CCX server. During installation of your wallboard software, you must configure your wallboard software to access the Unified CCX database. To do this, you must assign a DSN, User ID, and password.

---

Use the Real-Time Snapshot Writing Configuration for Wallboard web page to enable the system to write data to the wallboard system.

To access the Real-Time Snapshot Writing Configuration for Wallboard web page, choose **Tools > Real Time Snapshot Config** from the Unified CCX Administration menu bar.

The following fields are displayed on the Real-Time Snapshot Writing Configuration for Wallboard web page.

Field	Description
Data Writing Enable	If checked, the system writes the data to the database. If not checked, the system does not write the data to the database.  The default is disabled.
Data Writing Interval	Sets the refresh interval for the wallboard data. Valid options: 5, 10, 15, 20, 25, 30, 60, 90, 120, 150 and 180.
Cisco Unified CCX CSQs Summary	If checked, writes information about each CSQ to the RtCSQsSummary table in the Unified CCX database.

Field	Description
Cisco Unified CCX System Summary	If checked, writes overall Unified CCX system summary to the RtICDStatistics table in the Unified CCX database.
<b>Wallboard System</b>	
Server Name	IP addresses of the servers running the Wallboard software pointing to the HDS Database Server, which contains the Wallboard Real-Time Snapshot data. If you have multiple Wallboard servers, you can list their IP addresses in this field separated by commas.



**Note** For details about the information written to the RtCSQsSummary and RtUnified CCXStatistics database tables, see the *Cisco Unified Contact Center Express Database Schema Guide*. Only the RtCSQsSummary and RtICDStatistics statistics tables can be used in wallboard queries. Use of historical reporting tables in wallboard queries is not supported.

See the Unified CCX Compatibility related information, located at: <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html>

## Create System DSN for Wallboard

You can create a system Data Source Name (DSN) on your Windows server by performing the following procedure.

### Procedure

**Step 1** Install the wallboard software and IBM Informix ODBC Driver (IDS Version 3.0.0.13219 and above) on the wallboard client desktop.

- Note**
- You can download the Informix ODBC driver from the following URL: <https://www-01.ibm.com/marketing/iwm/iwm/web/pickUrxNew.do?source=ifxd1>. Download the IBM Informix Client Software Development Kit (CSDK) Version 3.00 or higher for the operating system you are installing with the wallboard client. More information about the CSDK can be found at the following URL: <http://www.ibm.com/software/data/informix/tools/csdk/>.
  - The ODBC connections to Unified CCX do not support encryption.

**Step 2** Select **Start > Settings > Control Panel**.

**Step 3** From the Control Panel menu, select **Administrative Tools > Data Sources ODBC** to launch the ODBC Data Source Administrator.

**Step 4** Click the **System DSN** tab. Then click **Add** to open the Create New Data Source dialog box.

**Step 5** Scroll down to locate and select the IBM INFORMIX ODBC DRIVER.

**Step 6** Click **Finish** to open the IBM Informix Setup dialog box.

**Step 7** On the **General** tab, enter and apply a Data Source Name and Description.

**Step 8** On the **Connection** tab, enter the values for the fields as shown in the following table:

Field	Description
Server Name	<p>This is the instance name of the Informix database.</p> <p>Informix database instance name can be formed using Host Name of the Unified CCX server by following these conventions:</p> <ul style="list-style-type: none"> <li>• Convert all upper case letters to lower case.</li> <li>• Replace hyphens with underscore.</li> <li>• Add the letter “i” as a prefix to the instance name, if the hostname starts with a number.</li> <li>• Append the letters “_uccx” to the instance name.</li> </ul> <p>For example, if the hostname is “802UCCX-Ha-Node1”, enter “i802uccx_ha_node1_uccx” in the Server Name field.</p>
Host Name	Enter the hostname of the primary Unified CCX server.
Service	Enter <i>1504</i> .
Protocol	Enter <i>onsoctcp</i> .
Options	Leave blank.
Database Name	Enter <i>db_cra</i> .
User ID	Enter <i>uccxwallboard</i> . This is the user id of the Unified CCX database created for wallboard.
Password	The password for the wallboard user that has been configured. You can change the password by going to <b>Tools &gt; Password Management</b> submenu option from the Unified CCX Administration menu bar.

**Step 9** Click **Apply**.

**Step 10** Click the **Environment** tab and enter the values for the following fields:

Field	Description
Client Locale	Enter <i>en_US.UTF8</i> .
Database Locale	Enter <i>en_US.UTF8</i> .

**Step 11** Click **OK**.

**Step 12** Return to the **Connection** tab and click **Apply and Test Connection**.

If the phrase “Test completed successfully” is returned, click **OK**.

If the test is unsuccessful, return to the configuration sequence and fix any errors.

---

## Wallboard Software in High Availability (HA) Deployment

If you use wallboard software in an High Availability (HA) deployment of Unified CCX and do not want any manual intervention in case of failover, you must upgrade your wallboard software.

Upgraded wallboard software should have a new service which periodically requests Unified CCX server for database mastership information using REST API (URL - *http://<Unified CCX server IP Address>/uccx/isDBMaster*). During failover, this new service in wallboard will update DSN registry to use new database master server.

REST API can be requested only from wallboard servers configured through **Tools > Real Time Snapshot Config** web page from the Unified CCX Administration menu bar.

### Use Upgraded Wallboard Software with New Service in HA Deployment

If you use wallboard software in a High Availability (HA) deployment of Unified CCX, you must work with your wallboard vendor to use the new API exposed by Unified CCX.

Wallboard software with the new service ensures that the wallboard server always displays data from the master database server of Unified CCX and no manual intervention is required. Follow this procedure to complete the setup:

#### Procedure

---

- Step 1** Create DSN using secondary server information and modify the same DSN using primary server information. This will create sqlhost entries for both the servers in a registry at *HKEY\_LOCAL\_MACHINE\SOFTWARE\Informix\SqlHosts*.
  - Step 2** Configure the wallboard software with new service as described in the wallboard software documentation.
  - Step 3** Configure information of both the Unified CCX servers with new service of wallboard as described in the wallboard software documentation.
- 

#### What to do next

After you complete this procedure, no manual intervention is required in case of failover.

### Use Wallboard Software (without New Service) in HA Deployment

If you use the existing wallboard software without the new service in an High Availability (HA) deployment of Unified CCX, you must complete the following actions:

#### Procedure

---

- Step 1** Create DSN using secondary server information and modify the same DSN using primary server information. This will create sqlhost entries for both the servers in a registry at *HKEY\_LOCAL\_MACHINE\SOFTWARE\Informix\SqlHosts*.

- Step 2** Configure the wallboard software as described in the wallboard software documentation.
- Step 3** Whenever there is a failover, you must manually change the DSN registry entry as follows:
- Enter `http://<Unified CCX server IP Address>/uccx/isDBMaster` in a web browser from any wallboard client to know whether the requested Unified CCX IP address server has a database master or not.
  - On failover, change SERVER value to master DB instance name in registry of DSN under `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI`
  - You can find the exact database instance name at `HKEY_LOCAL_MACHINE\SOFTWARE\Informix\SqlHosts`
- 

## Historical Reporting Menu



**Caution** While Unified CM supports Unicode characters in first and last names, those characters become corrupted in Unified CCX Administration web pages for RmCm configuration, and Real Time Reporting.

---

Use the areas of the Historical Reporting Configuration web page to perform a variety of tasks, including configuring users, installing client software, and purging your database.

To access the different Historical Reporting Configuration options, choose **Tools > Historical Reporting** and click any of the following submenu options from the Unified CCX Administration menu bar:

- **Database Server Configuration**—to configure the database server to specify the reporting options provided to the user.
- **SMTP Configuration**—to configure the email server used to email scheduled Cisco Unified Intelligence Center (CUIC) reports.
- **Purge Schedule Configuration**—to automatically purge data as per the following configurations:
  - Timing of the purge
  - Automatic purge configuration
- **Purge Now**—to manually purge data.
- **File Restore**—to restore database records written to HR files when the database goes down.

### Database Server Configuration

Use the Database Server Configuration area to specify the maximum number of client and scheduler connections that can access the database server.

### SMTP Configuration

Use SMTP Server Settings area to configure the email server used to email scheduled Cisco Unified Intelligence Center (CUIC) reports.

The following fields are displayed in the SMTP Server Settings area:

Field	Description
Host/IP Address	The host name or IP address of the SMTP server
From email address	The email address that is to appear in the From field of emails sent by the Scheduler  <b>Note</b> Unified CCX supports alphanumeric IDs and special characters (only hyphen "-", underscore "_", and dot ".").
Use Email Proxy	Check this if you use a proxy server to reach your SMTP server.  Only HTTPS is supported as an email proxy type. SOCKS proxy is not supported.
Email Proxy Hostname	The hostname or IP address of the proxy server used to reach the SMTP server
Email Proxy Port	The port used to connect to the SMTP proxy server
Use SMTP Authentication	Check this if your SMTP server expects to receive username/password credentials
SMTP Username	If you check the Authenticate checkbox, enter the username that is to be authenticated
SMTP Password	If you check the Authenticate checkbox, enter the password that is to be authenticated



**Note** You will not be able to save the SMTP configuration if Cisco Unified Intelligence Center service on the publisher node is down.



**Note** The Unified Intelligence Center email client does not support SSL/TLS based SMTP servers to email the scheduled Unified Intelligence Center reports.

## Purge Schedule Configuration Option

Use the Purge Schedule Configuration area to select a user for whom you want to choose a reporting package for the Unified CCX Historical Reports system.

Choose **Tools > Historical Reporting > Purge Schedule Configuration** from the Unified CCX Administration menu bar to access the Purge Schedule Configuration web page.

The Historical Reporting Configuration web page opens, enabling you to configure the following:

- Daily purge schedule
- Automatic purge (you can specify how long records should persist before the system purges them)

## Purge Now Option

Use the Purge Now area to manually purge data.



Choose **Tools > Historical Reporting > Purge Now** from the Unified CCX Administration menu bar to access the Purge Now area.

## File Restore Option

Use the File Restore area to restore the database records written to HR files when the database goes down.

In case of an High Availability setup, files from both the nodes are restored to the HR Database of the first and second node respectively. If it is unable to connect to the second node, you will see an alert message stating that the remote node is not reachable. When the second node comes up, the restored data will be replicated but you must repeat this Restore operation to restore the HR files, if any, on the second node.

### Procedure

- 
- Step 1** Choose **Tools > Historical Reporting > File Restore** from the Unified CCX Administration menu bar to access the Historical Reporting Configuration web page.
- Note** **Restore Now** radio button is enabled by default on this page.
- Step 2** Click the **Start** icon that displays in the toolbar in the upper left corner of the window or the **Start** button that displays at the bottom of the window to restore the database records.
- You can view the status of the restore operation on this page.
- 

## User Management Menu

The User Management menu option allows you to assign access levels to Unified CCX system administrators and supervisors.

When you configure a Unified CCX supervisor, you are configuring users who can access the Unified CCX Supervisor web pages. You are not creating a supervisor for Unified CCX.



---

**Note** Only administrators can update the Unified CCX system. You must select at least one administrator, so that someone is available to perform updates.

---



---

**Attention** Do not edit users, teams and permissions in Unified Intelligence Center. The Unified CCX to Unified Intelligence Center sync runs as part of daily purge and synchronizes these settings on Unified Intelligence Center according to Unified CCX settings.

---

## Procedure

---

Choose **Tools > User Management** and click any of the following submenu options from the Unified CCXAdministration menu bar to assign administrative privileges to administrators and supervisors:

- [User Configuration, on page 10](#)
  - [Name Grammar Generator Configuration, on page 10](#)
  - [Spoken Name Upload Submenu, on page 11](#)
  - [Administrator Capability View Menu, on page 12](#)
  - [Supervisor Capability View Menu, on page 12](#)
  - [Reporting Capability View Menu, on page 12](#)
  - [Agent Capability View Menu, on page 13](#)
- 

## User Configuration

From the Unified CCXAdministration menu bar, choose **Tools > User Management > User View** to access the User Configuration web page.

Use this page to view existing users and assign administrative privileges to administrators and supervisors. You can provide a search string based on a user ID; for example, if you provide the search string as

- “\*Agent1”, it will display user IDs ending with Agent1
- “Agent1\*”, it will display user IDs starting with Agent1
- “Agent1”, it will display user IDs that contain Agent1.

All the columns are hyperlinked to the user configuration page.



---

**Note** This search bar will search the users only by last name or user ID. Do not use the first name for searching.

---

## Name Grammar Generator Configuration

Use the Name Grammar Generator Configuration web page to define scheduling information for the Name Grammar Generator.

From the Unified CCXAdministration menu bar, choose **Tools > User Management > Name Grammar Generator Configuration** to access Name Grammar Generator Configuration area.

Name Grammars must be generated if you wish to use the Name to User Step with ASR. The Name Grammar Generator scans the User Directory and creates a speech recognition grammar containing every user in the directory. These grammars are saved in the grammar repository.

You may use the Name Grammar Generator Configuration page to run the Name Grammar Generator or schedule it to run at some later time. The page also displays the date and time that the Name Grammar Generator was last run and the completion status of that run.

The following fields are displayed on the Name Grammar Generator web page.

Field	Description
Frequency	How often Name Grammar Generator is automatically run. Valid options: Never, Daily, and Weekly. This is a mandatory field.
Run task on (hrs of day)	Time of day to run the task. This is a mandatory field.
Run task on (day of week)	Day of week to run the task. This is a mandatory field.
Last Completed on	Date of last generation of name grammar.
Last Completion Result	The status after the last name grammar generation. (Display only.)
Grammar Variant	Select one or more grammar variants to generate from the check box next to the following three options: <ul style="list-style-type: none"> <li>• OSR 3.1.x</li> <li>• 2003 SISR</li> <li>• Nuance</li> </ul>
Current Status	Running status of the Name Grammar Generator. (Display only.)

Click the **Generate Name Grammar Now** icon or button to trigger the Name Grammar Generator.



**Note** Clicking **Generate Name Grammar Now** will not apply changes to the scheduling configuration; you must click **Update** to apply scheduling changes.

## Spoken Name Upload Submenu

When a caller requests to be transferred to a specific extension, Unified CCX applications can playback a recording of the spoken name of the person to whom the caller has called. These spoken name recordings are stored as .wav files and managed by the Spoken Name Upload tool of the Unified CCXAdministration web interface.

To access the Spoken Name Prompt Upload web page, choose **Tools > User Management > Spoken Name Upload** from the Unified CCXAdministration menu bar.

The Spoken Name Prompt Upload web page also contains the **Click Here for Recording Information** icon and button, which displays a .htm page in your browser with more information on recording spoken name prompts.

## Administrator Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools > User Management > Administrator Capability View** to access the capability view for the Administrator User Management area.

This web page contains a pane for users identified as Unified CCX Administrator and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction. Click **Update** to save the changes.

**Note**

- You cannot assign Administrator capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation. If you assign Administrator capability to such a user ID, an error appears.
- In Single Sign-On (SSO) mode the **Application User** created during installation will not be able to access the **Cisco Unified Intelligence Center** application with administrator privileges. To enable the Cisco Unified CCX Administrator to have administrator privileges in **Cisco Unified Intelligence Center** as well, follow the steps below:
  1. Assign the reporting capability to the user.
  2. Execute the CLI command, **utils cuic user make-admin**.
  3. Restart the **Cisco Unified Intelligence Center Reporting Service** for the changes to reflect.

## Supervisor Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools > User Management > Supervisor Capability View** to access the capability view for the Supervisor User Management area.

This web page contains a pane for users identified as the Unified CCX Supervisor and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction.

**Note**

For a supervisor to access Unified Intelligence Center Live Data reports, an extension should be assigned to the supervisor.

**Note**

You cannot assign Supervisor capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation. If you assign Supervisor capability to such a user ID, an error appears.

## Reporting Capability View Menu

From the Unified CCXAdministration menu bar, choose **Tools > User Management > Reporting Capability View** to access the capability view for the Historical Report Users area.

The capability view for the Reporting Management web page contains a pane for users identified as Unified CCX Historical Report Users and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction.



**Note** You cannot assign Reporting capability to a user ID that is the same as the application administrator user ID created during the Unified CCX installation. If you assign Reporting capability to such a user ID, an error appears.

The following users can access Unified Intelligence Center:

Roles	Access	Available reports
Application administrator	Super user	<ul style="list-style-type: none"> <li>• Historical reports</li> <li>• Live Data reports</li> </ul>
Reporting user	Unified CCX administrator must assign this role to a user.	<ul style="list-style-type: none"> <li>• Historical reports</li> <li>• Live Data reports</li> </ul>
Supervisor	Unified CCX administrator must assign this role to a user.	Live Data reports
Agent	Unified CCX administrator must assign this role to a user.	Agent-specific Live Data reports

## Agent Capability View Menu

From the Unified CCX Administration menu bar, choose **Tools > User Management > Agent Capability View** to access the capability view for Unified CCX agents.

The capability view for the Agent User Management web page contains a pane for users identified as Unified CCX Agents and another pane with the list of Available Users. Based on your requirements, you can move users back and forth between these two panes by clicking the arrows in either direction.

## Password Management

From the Unified CCX Administration menu bar, choose **Tools > Password Management**.

You can set the passwords for the following system users using this web page:

User	Username	Description
Wallboard	uccxwallboard	This user can connect to Configuration and Historical databases and has read-only access to RtICDStatistics and RtCSQsSummary tables.

User	Username	Description
Recording SFTP	uccxrecording	
Workforce Management	uccxworkforce	
Historical Reporting	uccxhruser	<p>This user can connect to Configuration, Historical and Repository databases and has the following privileges:</p> <ul style="list-style-type: none"> <li>• read-only access to Historical, Configuration, and Repository tables</li> <li>• execute stored procedures</li> <li>• create new stored procedures.</li> </ul> <p>This user is used by coresident Unified Intelligence Center and Standalone Unified Intelligence Center (if configured) to connect to Unified CCX Database and execute historical reports.</p> <p>This user is also used during initialization of Live Data gadgets in Finesse and Live Data reports in Unified Intelligence Center.</p>
System Call Tracking (part of Real Time Monitoring Tool/ Analysis Manager)	uccxsct	

Click **Save** icon that displays in the toolbar in the upper left corner of the window or the **Save** button that displays at the bottom of the window. Click the **Clear** button to remove the data entered and to retain the existing passwords. You will see an error message if the old and new passwords are the same for any of the users. Click **Check Consistency** to confirm.



**Note**

- The maximum length of the password entered is limited to 80 characters.
- A new password cannot be one of the last five passwords used.
- There is no default password set. You must manually reset it for the first time.

In case of a High Availability deployment, the password change will not be propagated to the second node. You must access the AppAdmin web interface of the second node manually to change the password. In an HA setup, you will be able to see **Check Consistency** icon or button in the Password Management page. Use this button to check and confirm whether the passwords between the two nodes match or not. You will be able to see the status of the password check in the Password Management page.



---

**Note** If passwords are not same across the nodes, applications using these user credentials, such as Wallboard, Historical Reports and Live Data reports in Unified Intelligence Center and Finesse may not function. Ensure that the user passwords are same in both the nodes.

---

When one or more user passwords are not same across both the nodes, the following alert would be generated, **UserPasswordMismatchAcrossNodes**.

