Cluster Configuration

Configure Active Directory Settings

Fields on the Active Directory tab configure the Active Directory server to authenticate reporting users as they log in to the Unified Intelligence Center Web application.

Configure Active Directory for the Unified ICM/CC supervisors so that they can sign in as Unified Intelligence Center Reporting users.

Note Cisco Unified Intelligence Center uses LDAP V2 which does not support all Unicode characters that are used in the first name or surname of LDAP users.

Active Directory is not used to authenticate Administration Super Users. These Super Users can only be authenticated through the local database. The first Super User is added during installation. All other Super Users are added through the **User Management** interface, and their credentials are encrypted into the local database.

To navigate to this page, choose **Cluster Configuration** > **Active Directory Settings**.

Table 1: Fields on This Tab

Field	Description
Host Address and Port for Primary Active Directory Server	Provide the hostname or IP address and the port of the Primary Active Directory server. The port defaults to 389.

Field	Description
Host Name and Port for Secondary Active Directory Server	Provide the hostname or IP address and the port of the Secondary Active Directory server. The port defaults to 389.
Use SSL	Check these boxes if you want the connection from the Unified device to the Active Directory connection to be encrypted with SSL while doing authentication.
Manager Distinguished Name	Enter the Manager Distinguished Name used to sign in to the Active Directory server. For example, on a default installation of Microsoft AD: `CN=Administrator, CN=users, DC=MYSERVER, DC=COM`. Replace *MYSERVER* and *COM* with your respective hostname. **Note** If users other than the LDAP administrator are configured as Manager Distinguished Name in the OAMP LDAP configurations, they should have the following rights: 1. User search permissions on the domain. 2. Read access to the user objects and their attributes. 3. Read access to the base DN 4. Permission to bind to LDAP.
Manager Password	Enter the Active Directory manager password.
User Search Base	Specify the user search base. For example, on a default installation of Microsoft AD, `CN=users, DC=MYSERVER, DC=COM`, replace *MYSERVER* and *COM* with your respective hostname. **Note** This example assumes that you placed the users in the USERS subtree of AD. If you created a new organizational unit within your subtree, then the syntax would be: `OU=MYUSERS, DC=MYSERVER, DC=COM`, instead of "CN=MYUSERS".

Field	Description
Attribute for User ID	Whenever a user signs in, Unified Intelligence Center searches for that user in the LDAP (Lightweight Directory Access Protocol) using the sign-in attribute specified in the LDAP configuration. After the user is found, the full DNS of the user is extracted and used for authenticating the user. The sign-in attribute specified in the LDAP configuration is the property against which LDAP search is issued to find the matching username. If you do not know which attribute to use, use *sAMAccountName*, which is the default Microsoft username attribute. Different organizations settle on different LDAP attributes to identify the username across the organization, depending on the tools used to administer LDAP within their organizations. This attribute allows you to customize the sign-in depending on the attribute used. Even a custom attribute can be specified using this dialog. *sAMAccountName* indicates the user attribute to search the user for is the *userPrincipalName*. *sAMAccountName* contains just the short username. For example, jDoe for the user John Doe. *userPrincipalName* indicates the user attribute to search the user for is the *userPrincipalName*. This attribute contains the username in the email format, **`user@compay.com`**. This entire string becomes the username and not just user. Therefore when this attribute is selected, the user has to type the full email format in as the username in the sign-in box. **Custom User Attribute** allows you to specify the attribute used for searching the user in LDAP. **Note** Custom User attributes are not validated and are used as is. Ensure that the correct case and attribute name are used. Contact your Active Directory Administrator for the correct attribute to use.

Field	Description
User Name Identifiers	Users are stored in Unified Intelligence Center in the format <UserName Identifier>\<username> The username Identifiers are used to identify the different kinds of users within Unified Intelligence Center. For example, local, LDAP, user-synced user, users from different LDAP domains, nETBIOSName, and so on. Before you can use it, the username identifier has to be declared for use on this page. When LDAP is configured, at least one identifier must be configured and set as default to enable the system to identify LDAP users. UserSychronization brings in users in format <syncdomain>\username and collections have users in the same format. Therefore, these users must sign in to Unified Intelligence Center using the <syncdomain>\user syntax. To enable, add <syncdomain> or @<syncdomain> (if you are using *userPrincipalName*) to the list of valid identifiers. The maximum allowed length of a username identifier is 128 characters. **Example:** When nETBIOSName and userPrincipalName are same or different: *For sAMAccountName:* Configure in Username Identifiers: <UserNameIdentifier> Login in cuic : UserNameIdentifier\user *For userPrincipalName:* Configure in Username Identifiers: @<UserNameIdentifier> Login in cuic : userPrincipalName This list box is pre-populated with the username Identifiers based on the list of usernames stored in the Unified Intelligence Center database. The most frequently occurring identifier in the list of username is auto-selected as the default. **Note** You cannot save LDAP configuration unless you choose a default Identifier from the **User Name Identifiers** list box and clicking the **Set Default** button.
Default User Name Identifier	Default identifiers allow users to sign-in without typing the full domain identifier (<domain>\user) or the *userPrincipalName* suffixes to usernames (user <@company.com>) on the sign-in page. It can be set by choosing one of the Identifiers from the list box and by clicking the **Set Default** button. Users who use any other identifier can still sign-in by typing their full identifier in the sign-in box. For example, domain2\user or netbiosname\user, provided those identifiers are already configured.

Field	Description
Test Connection	Click to test the connection to the primary and secondary LDAP servers and display the connection status.

- **Save** saves the configuration information you entered for the Active Directory. Clicking **Save** *does not validate the configuration*.

Configure Active Directory with SSL

Perform the following steps if you want the connection from the Unified Intelligence Center to the Active Directory server to be encrypted with SSL while doing authentication.

Procedure

Step 1 Perform the tasks outlined in the Microsoft Active Directory documentation to set up and generate the Certificate Authority.

Step 2 Save the certificate in *Base-64 encoded X.509 (CER)* file format.

Step 3 Log in to the Cisco Unified Operating System Administration User Interface.

Step 4 From the **Security** menu, select **Certificate Management**.

Step 5 Select the certificate name as `tomcat-trust`.

Step 6 Click **Browse** to browse and select the certificate that you have generated from the AD server.

Note You can leave the **Root Certificate** field as blank. This is an optional field.

Step 7 Click **Upload File** to upload the certificate.

Step 8 Use the `utils service restart Cisco Tomcat` and the `utils service restart Intelligence Center Reporting Service` CLI commands to restart the *Cisco Tomcat* and *Intelligence Center Reporting* services respectively.

Configure SMTP Settings

Use SMTP Settings to configure the email server used to email scheduled reports.

The actual schedules for reports (for example, schedule daily at 10AM) are defined and maintained from the Unified Intelligence Center web application. The report scheduler emails scheduled reports at the exact time they are scheduled.

To navigate to this page, choose **Cluster Configuration** > **SMTP Settings**.

Table 2: Fields on This Tab

Field	Description
SMTP Host Name / IP Address	Enter the Hostname or IP address of the SMTP Server.

Field	Description
From Email Address	Enter the email address that is to appear in the From field of emails sent by the Scheduler.
Use SMTP Authentication	Check this if your SMTP server expects to receive username / password credentials.
SMTP User Name	If you check the **Use SMTP Authentication** check box, enter the user name that is to be authenticated.
SMTP Password	If you check the **Use SMTP Authentication** check box, enter the password that is to be authenticated.
Test Connection	Click to test the connection. Unified Intelligence Center attempts to send an email to check for open connections. The connection status displays next to the button.

- **Save** saves the configuration information you entered for SMTP settings.

Note Clicking **Save** *does not validate the configuration*. Use the **Test Connection** button to test the connection.

Note To manage the TLS version used by Unified Intelligence Center to connect with the SMTP server, refer **set tls client min-version**. By default, it uses TLSv1.2. For more information, see Set Commands.

Upload Self-Signed Certificates

If you are using a self-signed certificate in your email server, upload the certificate to **tomcat-trust** using *cmplatform*. Perform the following steps:

Procedure

Step 1 Log in to *cmplatform* and navigate to **Security > Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**. The **Upload Certificate/Certificate Chain** dialog box opens.

Step 3 To upload the certificate chain, select **tomcat-trust** from the **Certificate Purpose** list.

Step 4 Select the file to upload. Click the **Choose File** button and navigate to the file; then, click **Open**.

Step 5 Click **Upload File**.

Step 6 Use the `utils service restart Cisco Tomcat` and the `utils service restart Intelligence Center Reporting Service` CLI commands to restart the *Cisco Tomcat* and *Intelligence Center Reporting* services respectively.

Unified CCE User Integration

> **Note** The **UCCE User Integration** option is not applicable for Packaged CCE deployments.

The Unified CCE User Integration feature imports supervisors and their teams from Unified ICM/CCE from the Unified ICM Configuration Manager and database into Unified Intelligence Center.

Supervisors are automatically given Unified Intelligence Center user roles and can log in to Unified Intelligence Center to access collections for - and run reports for - their agent team(s).

> **Note** There are five tasks in the initial setup for Unified CCE User Integration. Some are performed in the Administration interface. Some are performed in the Reporting interface. As Super Users have access to both interfaces, it is efficient for a Super User to set up Unified CCE User Integration.

- Enable Unified CCE User Integration in the Administration interface.
- Complete the configuration of the Unified CCE Historical Data Source in the **Configure** > **Data Sources** of the Reporting Interface.
- Synchronize Users in the Administration Interface.
- Validate Collections of Agents and Agent Teams in the Reporting Interface.
- Set up a synchronization schedule in the Administration Interface.

- Integrated Supervisors can sign in to Unified Intelligence Center Reporting (provided their Active Directory authentication has been configured.
- Integrated Supervisors are added to the Unified Intelligence Center Reporting User List with the User Roles of Report Designer and Dashboard Designer.
- The Unified Intelligence Center Value Lists page is updated with *Agents* and *Agent Teams* collections.
- Integrated Supervisors can view their *Agents* and *Agent Teams* collections (**Unified Intelligence Center Reporting** > **Value Lists**).
- Integrated Supervisors are granted permissions to *Agents* and *Agent Teams* collections only .

After Unified CCE User Integration schedule is set up, Unified Intelligence Center is updated with changes to supervisors and their teams every time the synchronization updates.

> **Note** Renaming an existing Unified CCE user to a name that is identical to the locally created Unified Intelligence Center user and performing user integration results in the following:
>
> - All the entities that are owned by the locally created Unified Intelligence Center user are assigned to the synched Unified CCE user in Unified Intelligence Center.
> - The locally created Unified Intelligence Center user is deleted.

Related Topics

Configure Unified CCE User Integration, on page 8

Configure Unified CCE User Integration

> **Note** After upgrading to Cisco Unified Intelligence Center 12.6, perform the User Integration operation (Cluster Configuration > UCCE User Integration) manually to import the Supervisors with the required roles. This setting is required to view gadgets in the Cisco Finesse Desktop for Supervisors.
>
> If the changes made to the Supervisors or teams are to be reflected immediately, then manually synchronize using the **Synchronize Now** option.

To navigate to this page, choose **Cluster Configuration** > **UCCE User Integration**.

The User Integration feature facilitates the automatic import of reporting supervisors who are added or modified in Unified ICM Configuration Manager and stored in the Unified ICM/CCE/CCH database.

Once integrated (imported), supervisors are added as users to the Unified Intelligence Center database and can sign into Unified Intelligence Center with their User ID and Password. They are created as users in Unified Intelligence Center with the User Roles of Dashboard Designer and Report Designer and with the rights to view the collection(s) for their agent team(s).

When Unified CCE User Integration runs, data is retrieved from the Unified CCE Data Source and two stock Value Lists (Agents and Agent Teams) are updated.

> **Warning** Schedule Unified CCE User Integration at off-peak hours and several hours after the database purge. By default, the purge runs at midnight (12:00:00 AM). Database tables are locked during the purge and are unlocked when the purge completes. If the Unified CCE User Integration runs at the same time as the purge, the user integration will fail.

Table 3: Fields on this Tab

Field	Description
Enable UCCE User Integration at...	Check this to: • Enable Unified CCE User Integration • Set the time and the day of week when it is to occur. **Note** Leave this field blank if you do not want to run Unified CCE User Integration. For more information, see *Unified CCE User Integration*.
Hour | Minute | AM or PM	Click the arrows to the right of the Hour, Minute, and AM|PM fields to select the time of day you want the Unified CCE Integration synchronization to occur.

Field	Description
Day of the week	Select one, several, or all days that you want the Unified CCE User Integration synchronization to occur.
Last Run Status	Shows the status of the last synchronization. Shows PENDING if the that synchronization is still in progress.
Duration (HH:MM:SS)	Shows how long the synchronization process took.
Unified CCE Supervisors imported	Shows the number of new supervisors imported since the last import. You can view supervisors on the **Configure** > **Users** in the Unified Intelligence Center Reporting Interface . Supervisors are imported with their Active Directory credentials and can sign in to Unified Intelligence Center Reporting with those credentials.
Team Collections Updated	Shows a count of all teams updated. Teams are re-synchronized on each run. Supervisors can view their Agents and Agent Teams collections in Value Lists in the Unified Intelligence Center Reporting interface.
Synchronize Now	Click this to run the user integration immediately. If the scheduled integration is configured to run later in the day, this action runs the job now and still runs it at the scheduled time. Clicking this button changes its appearance to *Cancel Active Synchronization*. A message appears if another user is already running a synchronization.
Save	Click to save your time and date settings.

Cluster Configuration for JVM Using Hazelcast

Cisco Unified Intelligence Center uses Hazelcast for application clustering. Hazelcast provides a second-level cache for the Unified Intelligence Center application layer. When any entity (for example: report, report definition, and so on) cached by Hazelcast is updated in one of the Unified Intelligence Center nodes, it must be invalidated and reloaded in all the other Unified Intelligence Center nodes in the cluster. The Hazelcast cluster automatically takes care of it by publishing clusterwide notifications containing the identifiers of such entities which must be invalidated.

In Unified Intelligence Center, the default mechanism for Hazelcast cluster discovery or formation is UDP multicast. Unified Intelligence Center uses the Multicast group IP address 224.2.2.3 and port 54327. You cannot change these settings in Unified Intelligence Center.

The UDP multicast based discovery mechanism will not work for the customer in the following scenarios:

- When the network has multicasting disabled.
- If the nodes in the Unified Intelligence Center cluster are in different subnets.

In such scenarios, you can change the discovery mechanism to TCP/IP. You can form the CUIC application cluster using TCP/IP instead of the default UDP Multicast based discovery mechanism.

Use the following CLI commands to manage the cluster mode (UDP Multicast vs TCP/IP). That is, use the following CLI commands to switch to TCP/IP only if the customer's network does not support Multicasting:

- **utils cuic cluster show**—This command shows the current cluster mode that is enabled on this node and the other member details.

Note The member details are available only in the TCP/IP mode. The member details displayed are of the configured members and does not represent the cluster in real time.

- **utils cuic cluster mode**—This command is used to switch the Hazelcast cluster join configuration from Multicast to TCP/IP and the opposite way.

Note After changing the cluster mode in all the nodes, restart "Intelligence Center Reporting Service" in all the nodes starting from the publisher sequentially.

- **utils cuic cluster refresh**—This command refreshes the cluster member information only when run in the TCP/IP mode. Run this command when there is an addition or deletion of nodes to the CUIC cluster, which is already in TCP/IP.

Usage

You can use these commands using to switch to TCP/IP only when the customer's network does not support the Multicasting requirements that are specified in *Port Utilization Guide for Cisco Unified Contact Center Solutions* > *Intracluster Ports Between Cisco Unified Intelligence Center* section available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Note

- Stop the "Intelligence Center Reporting Service" on all the Unified Intelligence Center nodes before performing cluster configuration changes using these CLI commands.
- When you have completed the cluster configuration changes on all nodes, use the "utils cuic cluster show" command to ensure that all nodes have identical configuration before starting "Intelligence Center Reporting Service" on any one of them.
- Unified Intelligence Center cluster / application will work only if all the nodes use the same mode–that is, either Multicast or TCP/IP. Mixed mode is not allowed.
- If the network is disconnected and after the cluster nodes retain the network, ensure to perform "synchronize cluster" from all the nodes after logging into the Unified Intelligence Center reporting application.

Steps

Run the following CLIs on all nodes in the given sequence starting from the Publisher node:

Note Run every step on all nodes before performing the subsequent step.

Procedure

Step 1 utils service stop Intelligence Center Reporting Service

Step 2 utils cuic cluster mode

Step 3 utils cuic cluster show

Note Ensure that all nodes have identical configuration.

Step 4 utils service start Intelligence Center Reporting Service

Troubleshooting Cluster Configuration

Verify the Hazlecast Cluster Formation using Hazelcast REST client. To verify, replace <CUIC-IP> with the IP address of any CUIC member in the following URL.

http://<CUIC-IP>:57011/hazelcast/rest/cluster

The Unified Intelligence Center application cluster can be down in the following cases:

- Common Cases:
  - Node is not reachable
  - Unified Intelligence Center Reporting Service is down
  - Member/subscriber node is added in OAMP and the node installation is in progress
  - Hazelcast default Port 57011 is not enabled in Unified Intelligence Center nodes in the customer environment, which is used to communicate between cluster members.
- When multicasting is being used for the member discovery (Default method):
  - Network has UDP multicast disabled
  - UDP port 54327 used for Hazelcast member discovery is disabled
  - Multicast default group IP 224.2.2.3 is not allowed in the network
  - CUIC nodes are distributed across different subnets

Note If any of the above mentioned cases cause issue because of the restrictions on multicasting in the customer environment, you can use TCP/IP for Hazelcast discovery.

- When TCP/IP is being used for the member discovery:
    - Member/subscriber node is added in OAMP, but the cluster mode in the newly added node is not switched to TCP/IP from the default method ‘multicasting’.

For more information, contact Cisco support to troubleshoot and reset the cluster.