



Database Config Guide

Embrava Connector Service

©2019 Embrava Pty Ltd

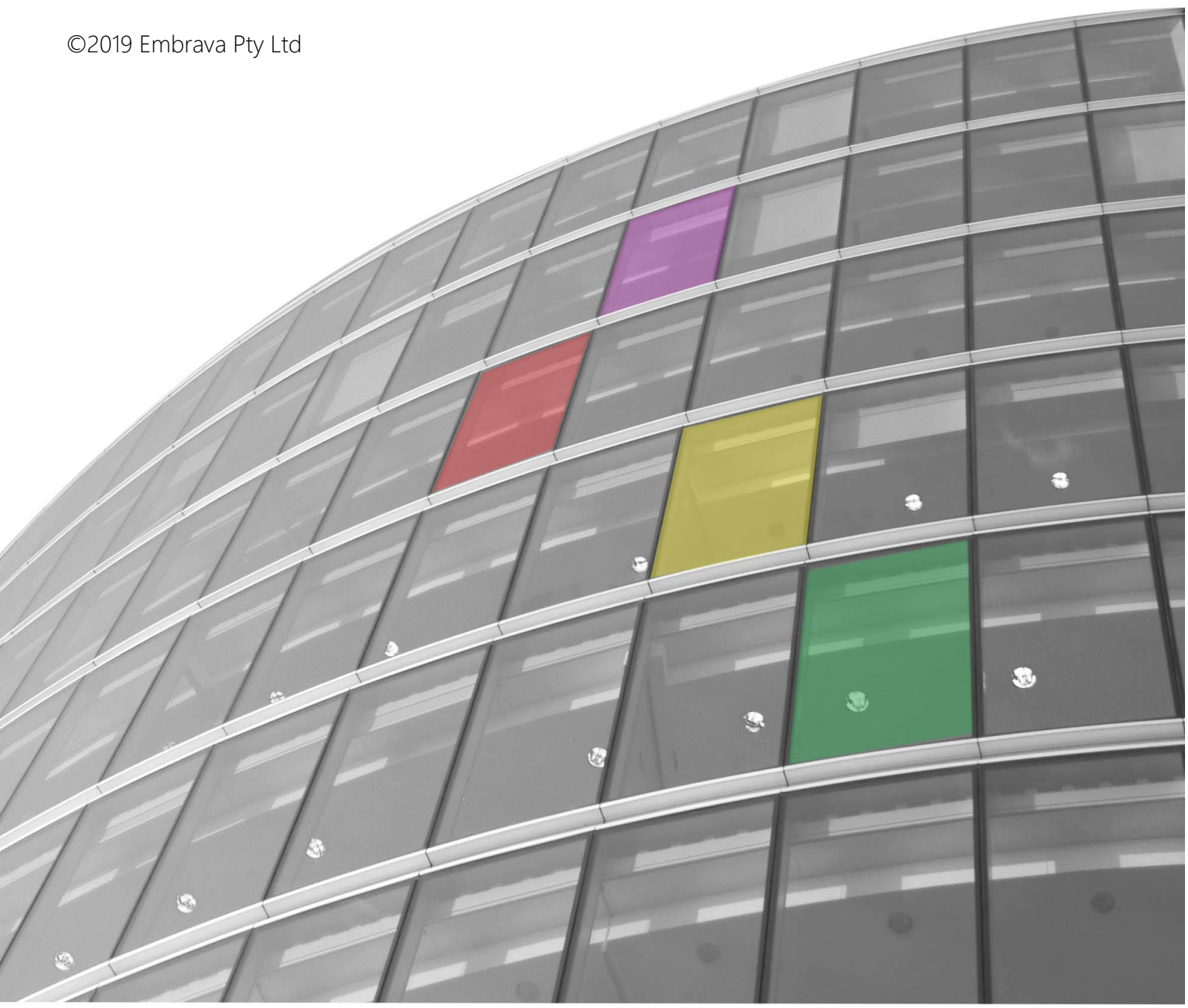


Table of Contents

- Overview..... 3
- UCCE/PCCE configuration..... 3
 - Enabling SQL Server Authentication Mode 3
 - Before you begin – Security Warning 4
 - Enabling SQL Server Authentication using SQL Server Management Studio 4
 - Enabling the sa login using SQL Server Management Studio 5
 - Enabling the sa login using Transact-SQL 5
 - Creating Database User for Embrava Connector 5
- UCCX Configuration 9

Overview

The purpose of this document is to describe how to setup database access for *Embrava Connector*. It needs to connect to *UCCE/PCCE* or *UCCX* database to retrieve statistics data.

UCCE/PCCE configuration

There are a few possible ways to deploy *UCCE/PCCE*. Steps described in this document need to be completed on one of the following servers which depends on the deployment type:

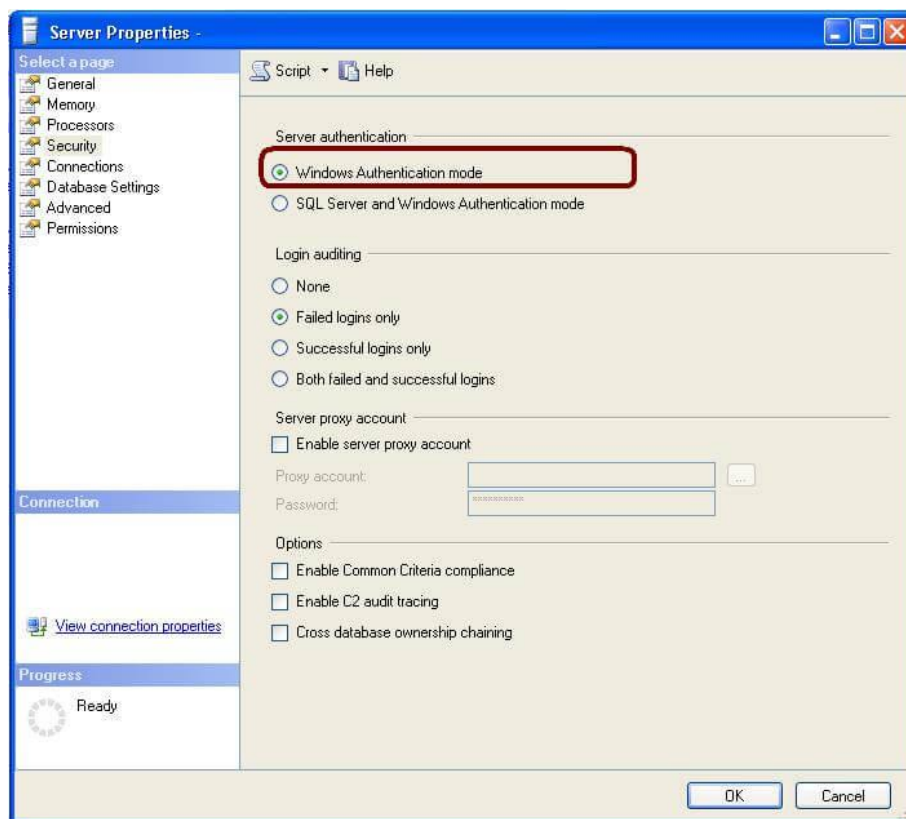
1. In UCCE deployments – AW-HDS system component
2. In PCCE deployments without HDS – DataServer component (Logger database)
3. In PCCE deployments with HDS - AW-HDS system component

Please ask your system administrator to add the following configuration on one of the above servers.

Enabling SQL Server Authentication Mode

During installation, SQL Server Database Engine is set to either **Windows Authentication mode** or **SQL Server and Windows Authentication mode**. *Embrava connector* requires **SQL Server Authentication mode** to be enabled.

To check authentication mode currently set on the MSSQL database open SQL Server Management Studio Object Explorer, right-click on the server name, click Properties and go to Security page to check the SQL Server Authentication. Complete below steps only if “Windows Authentication mode” is selected.



If **Windows Authentication mode** is selected during installation, the sa login is disabled and a password is assigned by setup. If you change authentication mode later to **SQL Server and Windows Authentication mode**, the **sa** login remains disabled. To use the **sa** login, use the ALTER LOGIN statement to enable the **sa** login and assign a new password. The **sa** login can only connect to the server by using SQL Server Authentication.

Before you begin – Security Warning

The sa account is a well-known SQL Server account and it is often targeted by malicious users. Do not enable the sa account unless your application requires it. It is very important that you use a strong password for the sa login.

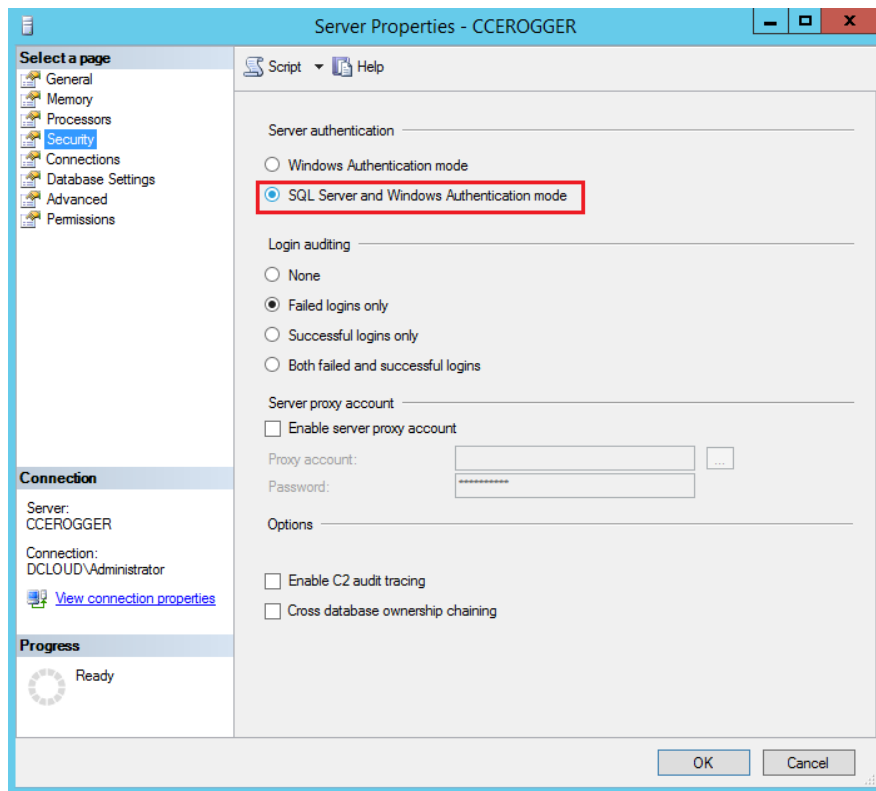
Enabling SQL Server Authentication using SQL Server Management Studio

Note!!!

The procedure presented below requires that the SQL Server process will need to be restarted. This will impact PCCE/UCCE environment. The procedure should be executed and planed in maintenance Window.

To change security authentication mode:

1. In SQL Server Management Studio Object Explorer, right-click the server, and then click **Properties**.
2. On the Security page, under **Server authentication**, select the **SQL Server Authentication Mode**, and then click OK.
3. In the SQL Server Management Studio dialog box, click **OK** to acknowledge the requirement to restart SQL Server.
4. In Object Explorer, right-click your server, and then click **Restart**. If SQL Server Agent is running, it must also be restarted.



Enabling the sa login using SQL Server Management Studio

To enable the sa login:

1. In Object Explorer, expand **Security**, expand Logins, right-click **sa**, and then click **Properties**.
2. On the **General** page, you might have to create and confirm a password for the login.
3. On the **Status** page, in the **Login** section, click **Enabled**, and then click **OK**.

Enabling the sa login using Transact-SQL

To enable the sa login:

1. In Object Explorer, connect to an instance of Database Engine.
2. On the Standard bar, click **New Query**.
3. Copy and paste the following example into the query window and click **Execute**. The following example enables the **sa** login and sets a new password.

```
ALTER LOGIN sa ENABLE ;
GO
ALTER LOGIN sa WITH PASSWORD = '<enterStrongPasswordHere>' ;
GO
```

Creating Database User for Embrava Connector

The following procedure describes steps that need to be completed in order to create user that will be used to pull statistic data from UCCE/PCCE system to *Embrava Connector*.

Please note !!!

Embrava Connector can be treated as a reporting server same as Cisco Unified Intelligence Center (CUIC) application. Database users require same configuration set of parameters as users used in data source configuration. If system administrator doesn't allow to configure additional user accounts CUIC logins can be reused for *Embrava Connector*.

Please note !!!

In the procedure the created user name is **embrava_connector_user**. The name can be change based on the environment owner requirements.

Please Note !!!

In the procedure we assumed that the UCCE/PCCE installation instance name is **embrava**. This means that the all database names will have prefix of **embrava_**. Instance name is different for each deployment models. Please ask your system administrator for the *UCCE/PCCE* instance name before going through the guide.

To create a user:

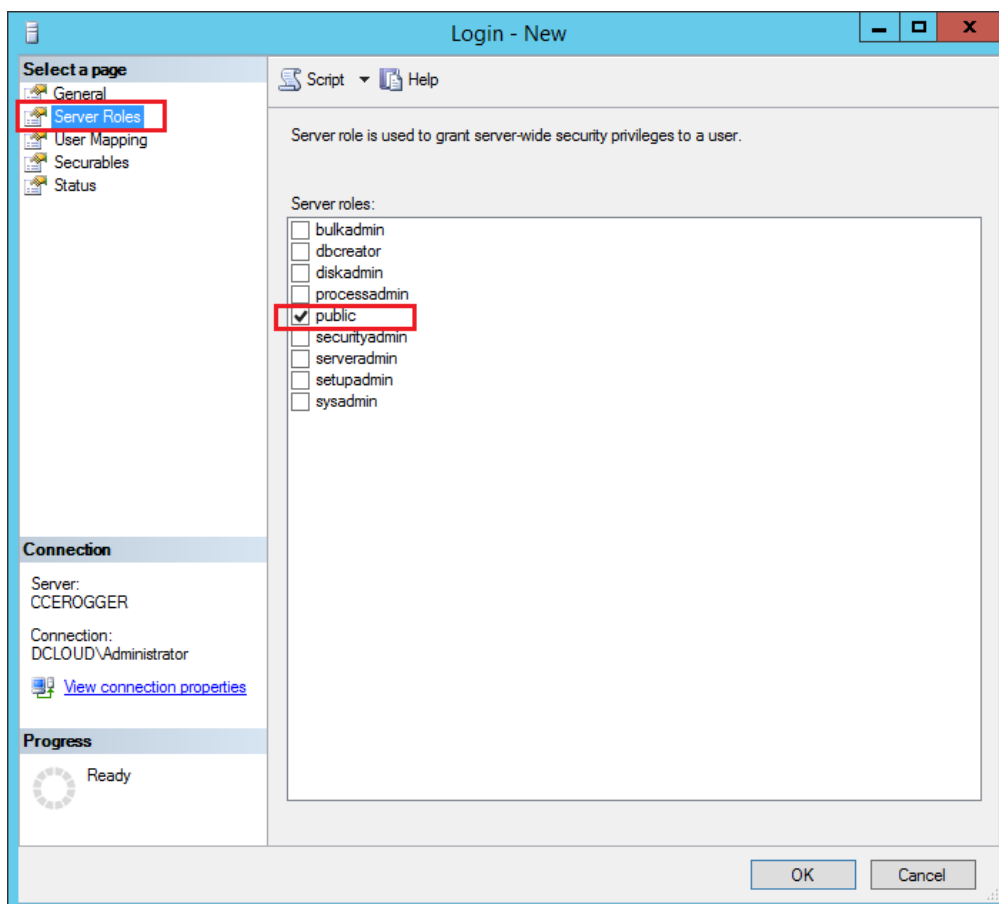
1. In Object Explorer, expand the folder of the server instance in which you want to create the new login.
2. Right-click the **Security** folder, point to **New**, and select **Login....**
3. In the **Login – New** dialog box, on the **General** page, enter the name of a user (**embrava_connector_user**) in the Login name box

The screenshot shows the 'Login - New' dialog box with the following fields and values:

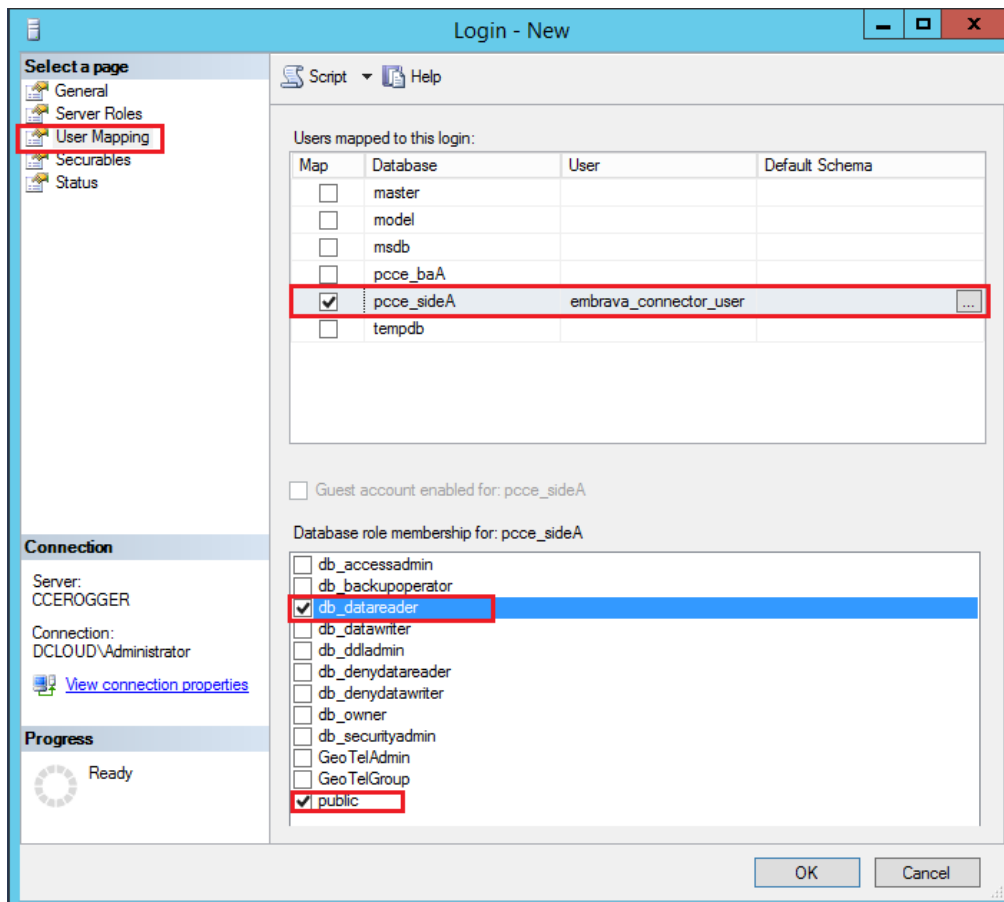
- Login name:** embrava_connector_user
- Authentication:** SQL Server authentication (selected)
- Password:** [masked]
- Confirm password:** [masked]
- Default database:** pcce_sideA
- Default language:** <default>

4. To create a login that is saved on a SQL Server database, select **SQL Server authentication**.

5. In the **Password** box, enter a password for the new user. Enter that password again into the **Confirm Password** box.
6. When changing an existing password, select **Specify old password**, and then type the old password in the **Old password** box.
7. (Optional) If system owner requires enforced password policy:
 - a. To enforce password policy options for complexity and enforcement, select **Enforce password policy**. For more information, see [Password Policy](#). This is a default option when **SQL Server authentication** is selected.
 - b. To enforce password policy options for expiration, select **Enforce password expiration**. **Enforce password policy** must be selected to enable this checkbox. This is a default option when **SQL Server authentication** is selected.
 - c. To force the user to create a new password after the first time the login is used, select **User must change password at next login**. **Enforce password expiration** must be selected to enable this checkbox. This is a default option when **SQL Server authentication** is selected.
8. From the **Default database** list, select a default database for the login. For the Embrava Connector please select **embrava_awdb** for UCCE deployments or **embrava_sideA** or **embrava_sideB** for PCCE deployments.
9. From the **Default language** list, select a default language for the login.
10. Click on the **Server Roles** tab. The **Server Roles** page lists all possible roles that can be assigned to the new login. For the Embrava Connector ensure that the following options are selected:
 - a. **public** check box - all SQL Server users, groups, and roles belong to the public fixed server role by default.



11. Click on the User Mapping tab. The User Mapping page lists all possible databases and the database role memberships on those databases that can be applied to the login. The databases selected determine the role memberships that are available for the login. For the Embrava Connector ensure that the following options are selected:
- a. Users mapped to this login - select the databases that this login can access. When you select a database, its valid database roles are displayed in the Database role membership for: database_name pane.
 - i. For UCCE deployments - select **embrava_awdb** and **embrava_hds** databases
 - ii. For PCCE deployments without HDS – select **embrava_sideA** or **embrava_sideB**
 - iii. For PCCE deployments with HDS - **embrava_awdb** and **embrava_hds**
 - b. For each database listed above ensure that the following roles are selected from the role memberships list: **db_datareader**, **public**.

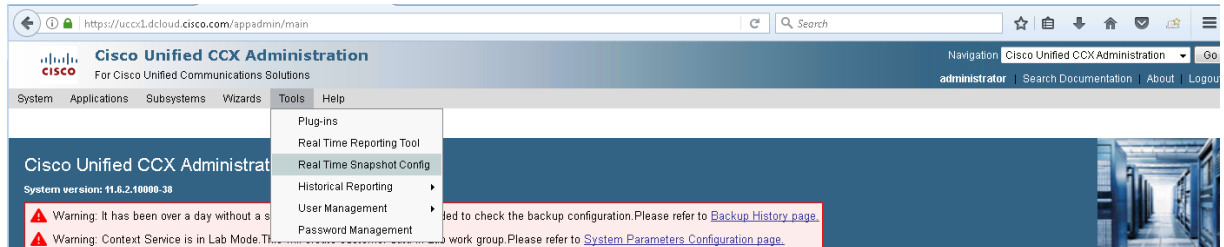


12. Once everything is done – please click **OK** to save the user configuration.

UCCX Configuration


UCCX as opposite to UCCE/PCCE doesn't have a real-time table mechanism. Therefore, data for the provided queries can be gathered based on the snapshot tables that need to be enabled during setup phase. To enable Snapshot mechanism please go through the following steps:

1. Open UCCX Administration page
2. Navigate to **Tools > Real Time Snapshot Config**



3. New window will be presented



4. Please ensure that:
 - a. Data Writing Enabled – is checked/selected
 - b. Data Writing Interval – please select the lowest possible value – 5 seconds. If you feel that this can cause performance issues, then select higher values. Lower value gives more precise statistics.
 - c. Cisco Unified CCX CSQs Summary – is checked/selected
 - d. Cisco Unified CCX System Summary – do not touch this parameter
 - e. Server Name - do not touch this parameter
5. Save the changes by clicking the Update button ().

UCCX is ready to store snapshot statistics.

END OF DOCUMENT