



CMP 8.23

Security Guide

Version 1.0

Classification: **Customer Confidential**



Copyright

© MDS Global 2026

THE CONTENTS OF THIS DOCUMENT ARE THE COPYRIGHT OF MDS GLOBAL LTD. ALL RIGHTS RESERVED. THIS DOCUMENT OR PARTS THEREOF MAY NOT BE REPRODUCED IN ANY FORM WITHOUT THE WRITTEN PERMISSION OF MDS GLOBAL.

Confidentiality

This document contains information that is proprietary to MDS Global and is confidential. The original recipient of this document may duplicate this document in whole or in part for internal distribution only, provided that this entire notice appears in all copies. This document and its contents may not otherwise be reproduced, distributed or disclosed. The recipient agrees to make every effort to prevent the unauthorised use, distribution or disclosure of the proprietary information contained in this document.

Disclaimer

No representation or warranty is contained in, made or given by this document or the information contained within it and no warranty or representation is made or to be implied that the information contained in this document is complete, up to date, accurate or fit for the purpose for which this document is supplied. In no event shall MDS Global be liable for incidental or consequential damages or loss in connection with, or arising from its use, whether MDS Global was made aware of the probability of such damages or loss arising or not.

Trademarks

The teal symbol above is an unregistered trademark of MDS Global Ltd. Other trademarks referred to within this document are the property of their respective trademark holders.

Contact Details

Please visit www.mdsglobal.com for further information on MDS Global products, solutions and services.

ISO 22301 standard is applicable to MDS Global Business Operations.



Table of Contents

Table of Contents	ii
Version Control	iii
Terms Used in this Document	iv
1.0 Security Technical Architecture	1
1. 1 Identity Server	1
1. 2 Administration Console	1
1. 3 Single Sign-On	1
1. 4 Role Extender	2
2.0 About CMP Role-Based Security	3
3.0 Security Groups	5
3. 1 AgentView Groups and Parent Roles	6
3. 1. 1 AgentView Parent and Child Roles	8
3.1.1.1 Bulk Orders	8
3.1.1.2 Comms	8
3.1.1.3 Credit Control	8
3.1.1.4 Customer Data	9
3.1.1.5 Customer Orders	9
3.1.1.6 Enterprise Data	9
3.1.1.7 Enterprise Orders	9
3.1.1.8 Finance	10
3.1.1.9 Hierarchy Management	10
3.1.1.10 Payment Handling	10
3.1.1.11 Problem Resolution	11
3.1.1.12 View Customer Data	11
3.1.1.13 View Enterprise Data	11
3.1.1.14 Workflow Handling	12
3. 2 Administration Console Groups and Roles	12
3. 3 Aurora Console Groups and Roles	16
3. 4 Bulk Action Console Groups and Roles	18
3.0 Creating Users and Assigning Group Roles in CMP	19
3. 5 Create a User in Admin Console	19
4.0 Password Recovery and Reset	21
4. 1 Password Reset Templates	21
4. 2 Enable Password Recovery and Reset	23
4. 2. 1 Prerequisites	23
4. 2. 2 Enable Password Recovery	24
4. 3 Password Policies	26
4. 3. 1 Set Password History Policy	26

Version Control

Version	Issue Date	Author	Comments
Version 1.0	20 August 2026	MDS	CMP 8.23 Release - Added the latest groups and roles, and replaced WSO2 tasks with CMP tasks.

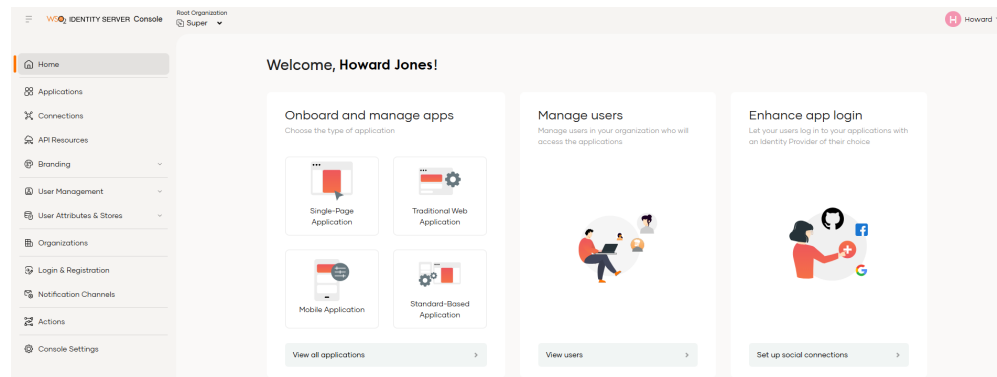
Terms Used in this Document

For definitions and explanations of the terms, abbreviations and acronyms used in this document, please see the *CMP Glossary* document.

1.0 Security Technical Architecture

1.1 Identity Server

CMP is built to use industry standard OAuth2 for authorisation. The WSO2 Identity Server is deployed as part of CMP to provide the Identity and Access Management.



Identity Server Interface

In a standalone CMP installation, users and roles can be maintained directly in the Identity Server however, it can also be configured to use an external identity provider. You can also create users in the Administration Console, which is the preferred method of adding and maintaining users and roles.

For information on installing and configuring the Identity Server, see the *CMP Installation Guide*.

1.2 Administration Console

You create users and assign them access to CMP applications and functionality in the Administration Console. You also perform more granular maintenance, for example assigning roles and permissions, from the Administration Console. See the **Users** screen and the online help for more information.

1.3 Single Sign-On

CMP security architecture supports [single sign-on](#)¹ when all applications are registered with the Identity Server in the same domain.

¹Single sign-on is a property of access control of multiple related, yet independent, software systems or components. With this property, a user logs in with a single ID and password to gain access to any of several related systems.

1.4 Role Extender

The authorisation implementation in many parts of CMP uses very granular level roles for maximum flexibility and future proofing. It would be too cumbersome to have to grant access to all of these granular roles directly to users. A number of granular roles are therefore mapped to higher level business roles and access is granted to these business roles.

For more information, see ["Security Groups" on page 5](#).

The Role Extender takes a role to which access has been granted in the Identity Server and returns the full list of lower level roles that this maps to. CMP components use roles to which that access has been directly granted and the corresponding extended lists of roles returned by the Role Extender to determine whether to allow an action to be performed.

The mapping of business roles to granular roles is factory configuration that is not designed to be modified when CMP is installed.

2.0 About CMP Role-Based Security

CMP employs a multi-level role-based security model in which each user who has rights to access a CMP component is assigned zero or more roles that define which functional area or resource they can access once they are successfully authenticated. Roles can give access to:

- Functionality - such as adding subscribers or configuring communications.
- Applications - roles can allow users to login to particular applications, such as AgentView or Business Configuration.
- Web Services - roles can govern which SOAP or RESTful web services can be used or viewed by a user.

Roles are organised in a hierarchy:

Groups

Groups are the roles at the topmost level of the hierarchy and represent different types of users, for example Customer Service Agent (CSA) or Manager. CMP has a number of different groups for the different features within the different components of CMP, such as Business Configuration, batch server, web services, AgentView and so on. For more information, see "[Security Groups](#)" on page 5. A group can include zero or more parent roles.

Parent roles

Parent roles group other roles and represent functional areas, for example functional areas in AgentView such as View Customer Data, Comms or Enterprise Orders. A parent group comprises zero or more roles.

Roles

Roles represent distinct functionality on a more granular level, for example the Comms parent role includes the roles Maintain Communications, Send Communications and View Communications.

Example

Suppose user JoeSmith has two group roles assigned:

- Consumer User
- BackOffice

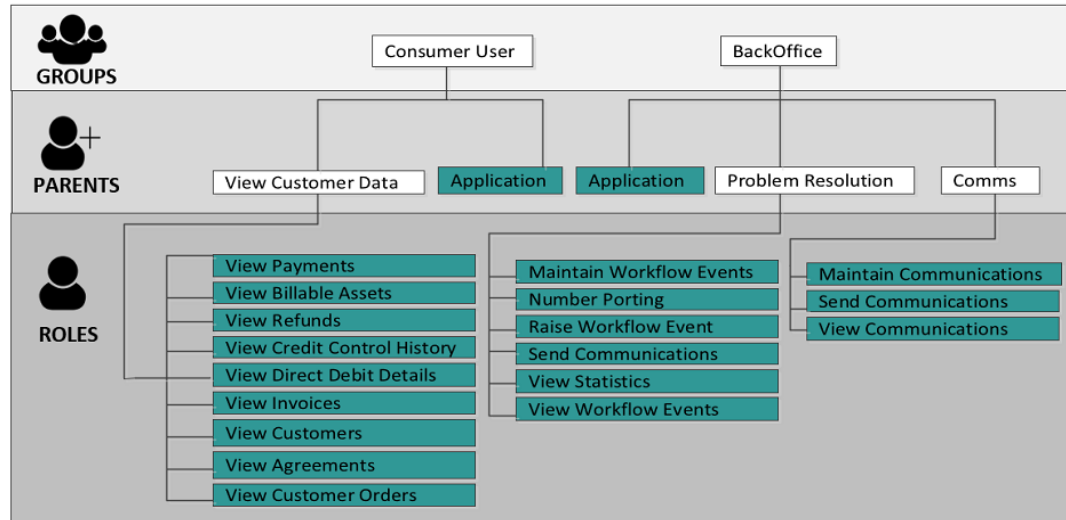
For the purposes of this example, the Consumer User and Back Office groups each have parent roles assigned. Both groups have an AgentView Application role that allows access to an application and is not extended any further - that is, it has no child roles assigned to it. However, the two groups also have parent roles:

- Consumer User has the parent role View Customer Data.
- Back Office has the parent role Problem Resolution and Comms.

Each of these parent groups has a number of roles assigned as children. For example, the Comms parent role has the following child roles:

- Maintain Communications.
- Send Communications.
- View Communications.

The hierarchy of group, parent and child roles is as follows:



From a CMP perspective, the list of roles associated with the JoeSmith are those coloured teal in the diagram.

Groups are controlled by the Identity Server. The relationship between groups and roles is defined by the role-extender service. For more information, see "[Security Technical Architecture](#)" on page 1.

3.0 Security Groups

The security groups that control access to CMP applications are defined against the users defined in the Administration Console. These groups include:

AgentView Groups

The following group roles control access to AgentView and Back Office functionality:

- Administrator
- Back Office
- Consumer CSA
- Consumer User
- Enterprise Admin
- Enterprise CSA
- Enterprise User
- Manager
- Read Only

For more information, see ["AgentView Groups and Parent Roles" on the next page](#).

Admin Console Jobs Groups

The following group roles grant access to CMP batch jobs and the Administration Console and control what functionality the user can access:

- Administrator
- Advanced Operations
- Basic Operations
- Read Only
- Super Administrator

For more information, see ["Administration Console Groups and Roles" on page 12](#).

Aurora Console Groups

The following group roles control which services the user can access: The following group roles control access to Aurora functionality:

- Aurora Admin
- Aurora Basic
- Aurora Read Only

For more information, see ["Aurora Console Groups and Roles" on page 16](#).

Bulk Action Console Groups

The following group roles control access to Bulk Action functionality:

- Bulk Add Package
- Bulk Apply CPI
- Bulk Create Subscription
- Bulk Edit Subscription
- Bulk Number Change

- Bulk Price Plan Change
- Bulk Porting Requests
- Bulk Sales Ledger Adjustment
- Bulk Subscription Feature
- Bulk Subscription Service
- Bulk Update Attributes
- Bulk Workflow

For more information, see ["Bulk Action Console Groups and Roles"](#) on page 18.

Web Service Groups

The following group roles control which services the user can access:

- RESTful Web Services all
- All Web Services
- Basic Web Services
- Billing Web Services
- Customer Web Services
- Financial Web Services
- Orders Web Services

Users with the *RESTful Web Services all* role have access to the RESTful web services. The remaining roles listed provide access to the SOAP web services.

3. 1 AgentView Groups and Parent Roles

The following table lists the CMP AgentView groups and the parent roles that are assigned to them. Click each parent role to view the child roles that belong to them. These child roles represent the functionality that the user assigned this parent role will be able to access.

For more information on access control to AgentView panels, popups and functionality, see the [AgentView Function Security Guide](#).

Parent Role	Group							
	Consumer User	Enterprise User	Consumer CSA	Enterprise CSA	Enterprise Admin	Manager	Back Office	Administrator
View Customer Data	✓		✓			✓	✓	✓
View Enterprise Data		✓		✓	✓	✓	✓	✓
Problem Resolution							✓	✓
Workflow Handling			✓	✓	✓	✓	✓	✓
Comms			✓	✓	✓	✓	✓	✓
Credit Control						✓		✓
Customer Orders			✓	✓	✓	✓		✓
Payment Handling			✓	✓	✓	✓		✓
Finance						✓		✓
Customer Data			✓	✓	✓	✓		✓
Hierarchy Management					✓	✓		✓
Enterprise Orders				✓	✓	✓		✓
Enterprise Data				✓	✓	✓		✓

Parent Role	Group							
	Consumer User	Enterprise User	Consumer CSA	Enterprise CSA	Enterprise Admin	Manager	Back Office	Administrator
Bulk Orders					✓	✓		✓
Maintain Agreement Administrator	✓	✓	✓	✓	✓	✓	✓	
Maintain Shared Group	✓	✓	✓	✓	✓	✓	✓	
View Agreement Administrator	✓	✓	✓	✓	✓	✓	✓	
View Shared Group	✓	✓	✓	✓	✓	✓	✓	
Login	✓	✓	✓	✓	✓	✓	✓	✓

3. 1. 1 AgentView Parent and Child Roles

Groups, parent roles and roles form a hierarchy of permissions that controls the functionality that a user can access. In CMP, the following parent roles handle AgentView functionality. Each parent role has a number of child roles.

3.1.1.1 Bulk Orders

This parent role has the following child roles:

- Add Orders
- Apply Bulk Changes
- View Orders

3.1.1.2 Comms

This parent role has the following child roles:

- Add Communications
- Maintain Communications
- Send Communications
- View Communications

3.1.1.3 Credit Control

This parent role has the following child roles:

- Credit Control Management
- View Credit Control History

- Write-offs

3.1.1.4 Customer Data

This parent role has the following child roles:

- Maintain Agreements
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Invoices
- Maintain Subscription Services
- Maintain Usage Limits

3.1.1.5 Customer Orders

This parent role has the following child roles:

- Add Customers
- Add Orders
- Add Purchases
- Maintain Agreements
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Payment Details
- Maintain Payments
- Maintain Purchases
- Maintain Subscription Services
- Maintain Usage Limits
- Number Porting

3.1.1.6 Enterprise Data

This parent role has the following child roles:

- Maintain Bonds
- Maintain CUGs
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Enterprises
- Maintain Invoices
- Maintain Subscription Services
- Maintain Usage Limits

3.1.1.7 Enterprise Orders

This parent role has the following child roles:

- Add Customers
- Add Orders

- Maintain Bonds
- Maintain CUGs
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Enterprise Orders
- Maintain Orders
- Maintain Payment Details
- Maintain Subscription Services
- Maintain Usage Limits
- Number Porting

3.1.1.8 Finance

This parent role has the following child roles:

- Add Adjustments
- Add Refunds
- Maintain Adjustments
- Maintain Discounts
- Maintain Refunds
- Reverse Payments
- View Direct Debit Details
- View Discounts
- View Payments
- View Refunds
- Write-offs

3.1.1.9 Hierarchy Management

This parent role has the following child roles:

- Maintain Agreements
- Maintain Customers
- Maintain Enterprises

3.1.1.10 Payment Handling

This parent role has the following child roles:

- Add Payments
- Add Purchases
- Maintain Payment Details
- Maintain Payments
- Maintain Purchases
- View Payments

3.1.1.11 Problem Resolution

This parent role has the following child roles:

- Maintain Workflow Events
- Number Porting
- Raise Workflow Event
- Send Communications
- View Statistics
- View Workflow Events

3.1.1.12 View Customer Data

This parent role has the following child roles:

- View Agreements
- View Communications
- View Credit Control History
- View Customer Orders
- View Customers
- View Direct Debit Details
- View Discounts
- View Invoices
- View Orders
- View Payments
- View Purchases
- View Refunds
- View Usage Details
- View Usage Limits
- View Weblinks
- View Workflow Events

3.1.1.13 View Enterprise Data

This parent role has the following child roles:

- View Agreements
- View Communications
- View Credit Control History
- View Customer Orders
- View Customers
- View Direct Debit Details
- View Discounts
- View Enterprises
- View Invoices
- View Orders
- View Payments
- View Purchases

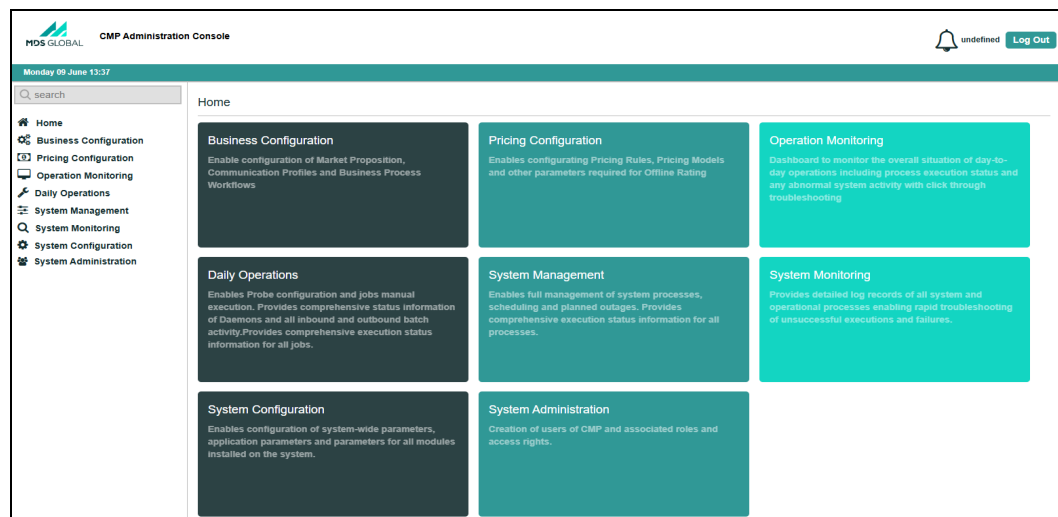
- View Refunds
- View Usage Details
- View Usage Limits
- View Weblinks
- View Workflow Events

3.1.1.14 Workflow Handling

This parent role has the following child roles:

- Maintain Workflow Events
- Raise Workflow Events
- View Workflow Events

3.2 Administration Console Groups and Roles



Administration Console Home Page

Security groups for the batch server, batch jobs and the Administration Console are as follows:

- Read Only

Users in this group have read only access to Daily Operations and System Monitoring in the Administration Console. They cannot perform any actions. They have no access to System Management or System Configuration.

- Basic Operations

Users in this group have the same access as the Sabre Read Only group users and also have full access to System Management in the Administration Console.

- Advanced Operations

Users in this group role have full access to all functionality except for System Configuration, to which they have read-only access.

- Administrator

Users in this group role have full access to all Administration Console functionality.

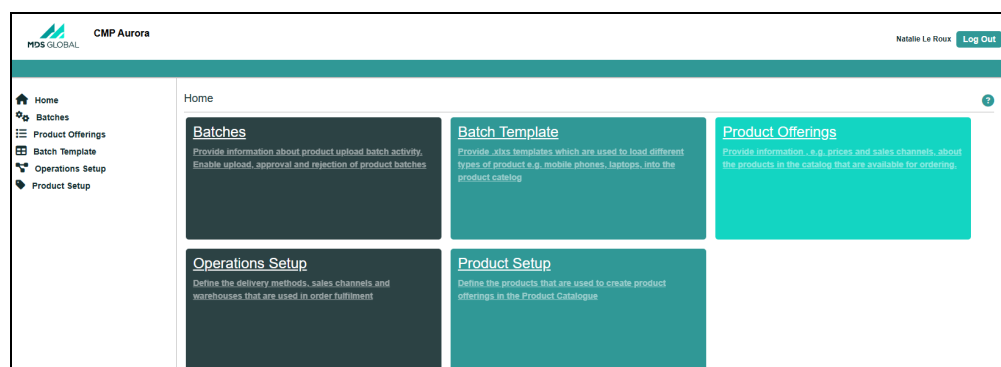
The following table shows in more detail how the security groups control access to Administration Console functionality:

Administration Console Functionality	Groups (sabre-console)			
	Read Only	Basic Ops	Advanced Ops	Admin
Batch server authentication	✓	✓	✓	✓
View Configuration Centre	✓		✓	✓
View Operation Monitoring Dashboard	✓	✓	✓	✓
View Daily Operations screen	✓		✓	✓
View Daily Operations > Probes	✓		✓	✓
View Daily Operations > Daemons	✓		✓	✓
View Daily Operations > Interfaces	✓		✓	✓
View Maintenance screen	✓	✓	✓	✓
View Daily Operations > Jobs	✓		✓	✓
View System Management > Outages	✓	✓	✓	✓
View System Management > Schedules	✓	✓	✓	✓
View System Management > Exclusion Calendars	✓	✓	✓	✓
View System Monitoring screen	✓		✓	✓
View System Monitoring > Executions	✓		✓	✓
View System Monitoring > Logs	✓		✓	✓
View System Monitoring > Outage Misfire Log	✓		✓	✓
View System Monitoring > Network Requests	✓		✓	✓
View Administration			✓	✓

Administration Console Functionality	Groups (sabre-console)			
	Read Only	Basic Ops	Advanced Ops	Admin
Operation Monitoring Dashboard > Control Process Flow			✓	✓
Daily Operations > Select Probes			✓	✓
Daily Operations > Manage Probes (run, enable/disable)			✓	✓
Daily Operations > Probes Details > Select Version			✓	✓
Daily Operations > Probes Details > Add/Remove Versions			✓	✓
Daily Operations > Probes Details > AddNotes			✓	✓
Daily Operations > Probes Details > Select Recipient			✓	✓
Daily Operations > Probes Details > Add/Delete Recipient			✓	✓
Daily Operations > Probes Details > Filter/Export History			✓	✓
Daily Operations > Select Daemons			✓	✓
Daily Operations > Start/Stop Daemons			✓	✓
Daily Operations > Select Jobs			✓	✓
Daily Operations > Manage Jobs (run, enable/disable)			✓	✓
Daily Operations > Job Details > Add Notes			✓	✓
System Management > Select Outages		✓	✓	✓
System Management > Manage Outages		✓	✓	✓
System Management > Select Schedules		✓	✓	✓

Administration Console Functionality	Groups (sabre-console)			
	Read Only	Basic Ops	Advanced Ops	Admin
System Management > Manage Schedules		✓	✓	✓
System Management > Exclusion Calendars > Select Calendar		✓	✓	✓
System Management > Exclusion Calendars > Edit Calendar		✓	✓	✓
System Management > Exclusion Calendars > Edit Weekly Calendar		✓	✓	✓
System Management > Exclusion Calendars > Select Holiday Calendar		✓	✓	✓
System Management > Exclusion Calendars > Edit Holiday Calendar		✓	✓	✓
System Configuration > View Modules			✓	✓
System Configuration > Modules > Edit Properties				✓
System Configuration > Modules > Set Logging Level				✓
System Configuration > Logging > Edit Logging Level				✓
System Configuration > Logging > Edit Days To Retain				✓

3.3 Aurora Console Groups and Roles



Aurora Console Home Page

Security groups for the Aurora Console are as follows:

- Read Only

Users in this group have read only access to all products in the Aurora Console. They cannot perform any actions.

- Basic Operations

Users in this group have the same access as the Administrator group users, except they cannot publish any products.

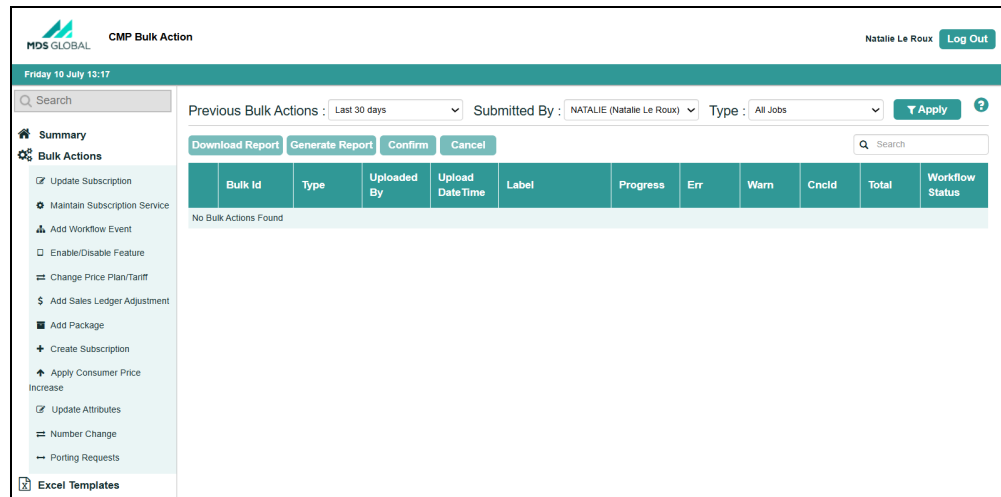
- Administrator

Users in this group role have full access to all Aurora Console functionality.

The following table shows in more detail how the security groups control access to Aurora Console functionality:

Aurora Console Functionality	Groups (aurora-console)		
	Read Only	Basic Ops	Admin
Approve Product Batch		✓	✓
Edit Product Batch		✓	✓
View all Product Offerings	✓	✓	✓
Publish Product Batch			✓
Reject Product Batch		✓	✓
Upload Product Batch		✓	✓

3.4 Bulk Action Console Groups and Roles



Bulk Action Summary Page with Bulk Actions Menu

The following lists the Roles for the Bulk Action Console:

- Bulk Add Package
- Bulk Apply CPI
- Bulk Create Subscription
- Bulk Edit Subscription
- Bulk Number Change
- Bulk Price Plan Change
- Bulk Porting Requests
- Bulk Sales Ledger Adjustment
- Bulk Subscription Feature
- Bulk Subscription Service
- Bulk Update Attributes
- Bulk Workflow

3.0 Creating Users and Assigning Group Roles in CMP

When CMP is first installed, use the Administrator username and password defined as part of the installation process to create and administer users in the Admin Console. Users granted the admin role then in turn can create and administer users.



Note: Only the original Administrator account can grant full admin rights to another account.

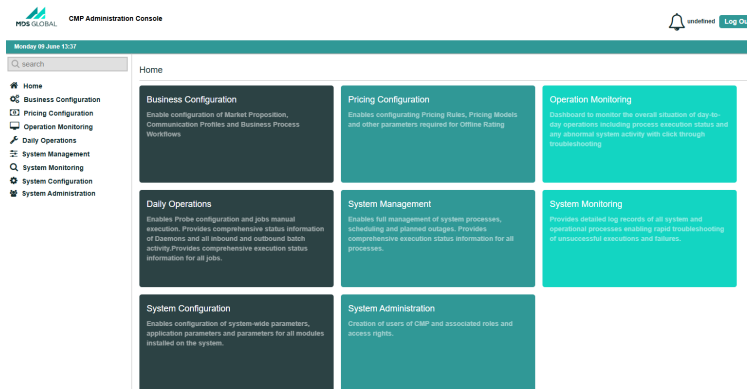
From the Admin Console, you can [create a new user and assign them roles](#).

3.5 Create a User in Admin Console

To create a user and assign them one or more group roles, follow these steps:

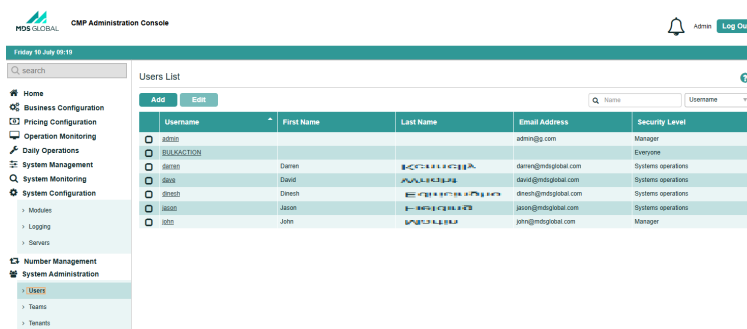
1. Log in to the Admin Console.

The console opens on the **Home** page.



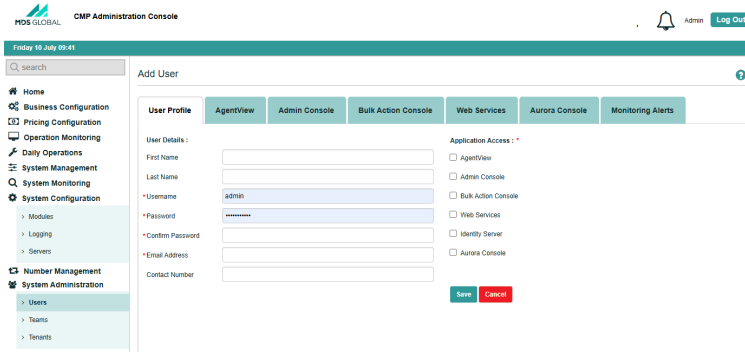
2. Select **System Administration > Users** from the left-hand menu.

The **Users List** page opens.



3. Click **Add**.

The **Add User** screen is displayed.

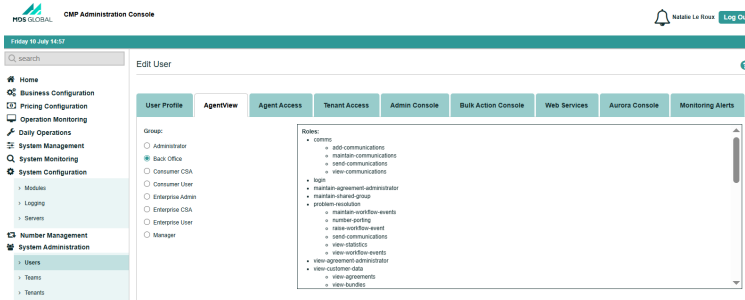


4. On the **User Profile**, enter the user details, including the username, password, and email address.
5. To grant the new user access to CMP applications, select the checkbox to the left of the required application.



This enables the tab for the selected application.

6. To assign the new user to a group, select the relevant tab, and select the groups required.



7. Return to the **User Profile** tab, and click **Save**.

The new user is added to the Users List.

4.0 Password Recovery and Reset

The email address and password is configured for the user in the Admin Console. Forgotten passwords can be reset by an Administrator.

From CMP 8.1.2, all new installations will have these options enabled by default. If you are upgrading from an earlier version to CMP 8.1.2 or above, see the following sections to enable and configure these options:

- "Password Reset Templates" below
- "Enable Password Recovery and Reset" on page 23

4.1 Password Reset Templates

The email templates send to the user and used for the password reset or change are deployed to the directory `/etc/mdsglobal/wso2is-login/templates` on the JBoss Web Server host.



For more information on hosts and deployment, see the *CMP Technical Architecture Overview* and *CMP Installation Guide* documents.

The email templates are standard HTML and can contain a number of parameter placeholders that will be populated at runtime.

The following templates are available:

- `password-reset-subject.vm` - Subject for the password reset email:

```
1 CMP - Password Reset
```

- `password-reset-body.vm` - Body for the password reset email:

```
1 <html>
2 <body>
3 <h1>Password Reset</h1>
4 <p>Hi ${givenName},<br/>
5 We received a request to reset the password for the ${username} account that is associated with this email
6 address.
7 If you made this request, please click the button below to securely reset your password.</p>
8 <p>
9 <a href="${recoveryUrl}" target="_blank" style="width: 230px; font-family: 'Nunito Sans', Arial, Verdana,
10 Helvetica, sans-serif; font-size: 18px; line-height: 21px; font-weight: 600; color: #fff; text-decoration:
11 none; background-color: #e30613; text-align: center; display: inline-block; cursor: pointer;">Reset Password</a>
12 </p>
13 If clicking the button doesn't seem to work, you can copy and paste the following link into your browser.
14 <br/>
15 ${recoveryUrl}
16 </p>
17 If you did not request to have your ${username} password reset, disregard this email and no changes to your
18 account will be made.
19 </p>
20 Thanks,<br/>
21 The CMP Team
22 </p>
23 <p></p>
24 </body>
25 </html>
```

- `password-changed-subject.vm` - Subject for the password changed confirmation email:

```
1 Your CMP password has been changed
```

- `password-changed-body.vm` - Body for the password changed confirmation email:

```
<html>
<body>
<h1>Password Changed</h1>
<p>Hi ${givenName},<br/><br/>
Your CMP password was changed for the ${username} account that is associated with this email address.
<br/>
If you did not perform this action, you should immediately go to ${wso2LoginUrl}/ssologin and use the
forgotten password functionality to reset your password.</p>
<p>Thanks,<br/>
The CMP Team
</p>
<p></p>
</body>
</html>
```

The placeholders include the following:

- `${givenName}` - First name of user
- `${lastName}` - Last name of user
- `${username}` - Username of user
- `${wso2LoginUrl}` - Base URL of the WSO2-login application that initiated the password change, for example AgentView, Administration Console, Business Configuration
- `${recoveryUrl}` - URL of link to change password (reset email only).

The email server settings are defined in the properties file: `/etc/mdsglobal/wso2is-login/application.properties`.

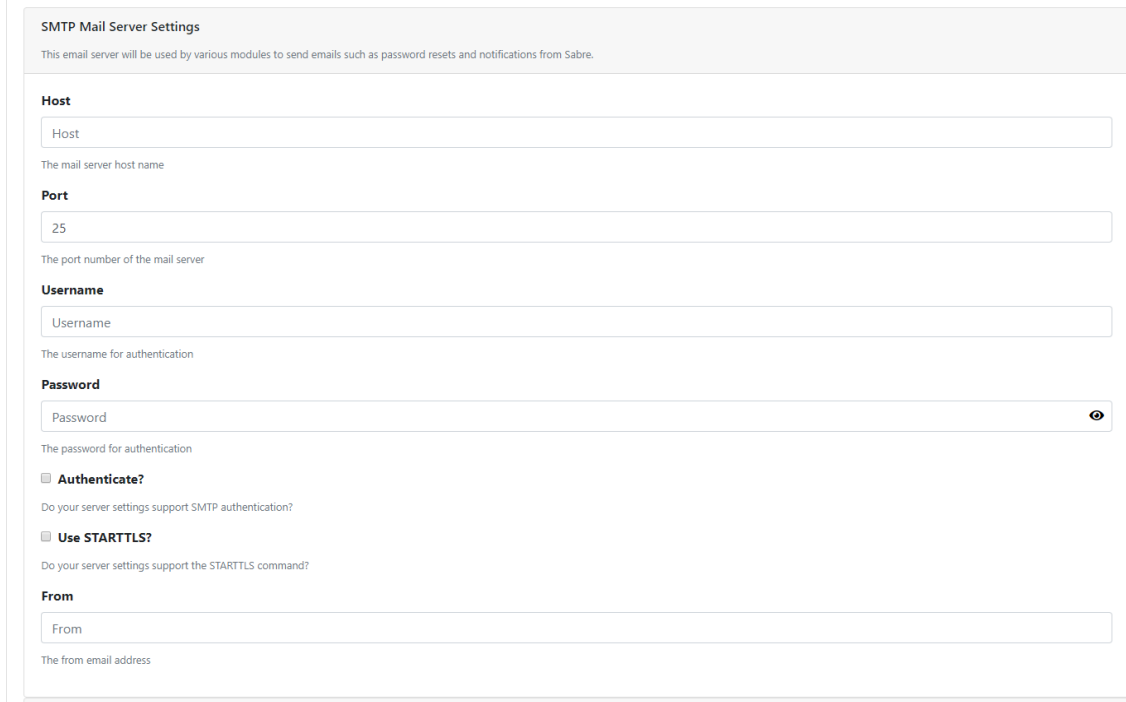
These are populated based on values defined in the inventory file:

```
spring.mail.host={{ mail_server.smtp_host | default('false') }}
spring.mail.port={{ mail_server.smtp_port | default('25') }}
spring.mail.username={{ mail_server.smtp_username | default('') }}
spring.mail.password={{ mail_server.smtp_password | default('') }}
spring.mail.properties.mail.smtp.auth={{ mail_server.smtp_auth | default('false') }}
spring.mail.properties.mail.smtp.starttls.enable={{ mail_server.smtp_starttls | default('false') }}
wso2is.mail.from={{ mail_server.smtp_from | default('') }}
```



If the `spring.mail.host` property is set to `false`, the **Forgot Password** link will not display in the login box.

A new panel has been added to the **Global** tab of the Installation Configuration Tool to support this:



SMTP Mail Server Settings

This email server will be used by various modules to send emails such as password resets and notifications from Sabre.

Host

Host

The mail server host name

Port

25

The port number of the mail server

Username

Username

The username for authentication

Password

Password

The password for authentication

☐ **Authenticate?**

Do your server settings support SMTP authentication?

☐ **Use STARTTLS?**

Do your server settings support the STARTTLS command?

From

From

The from email address



For more information on the inventory file and the Installation Configuration Tool, see the *CMP Installation Guide*.

The `application.properties` file also specifies the location of the template files, as follows:

```
wso2is.mail.subject.template=file:/etc/mdsglobal/wso2is-
login/templates/password-reset-subject.vm
wso2is.mail.body.template=file:/etc/mdsglobal/wso2is-login/tem-
plates/password-reset-body.vm
wso2is.mail.confirm.subject.template=file:/etc/mdsglobal/wso2is-
login/templates/password-changed-subject.vm
wso2is.mail.confirm.body.template=file:/etc/mdsglobal/wso2is-
login/templates/password-changed-body.vm
```

This location can be changed if necessary.

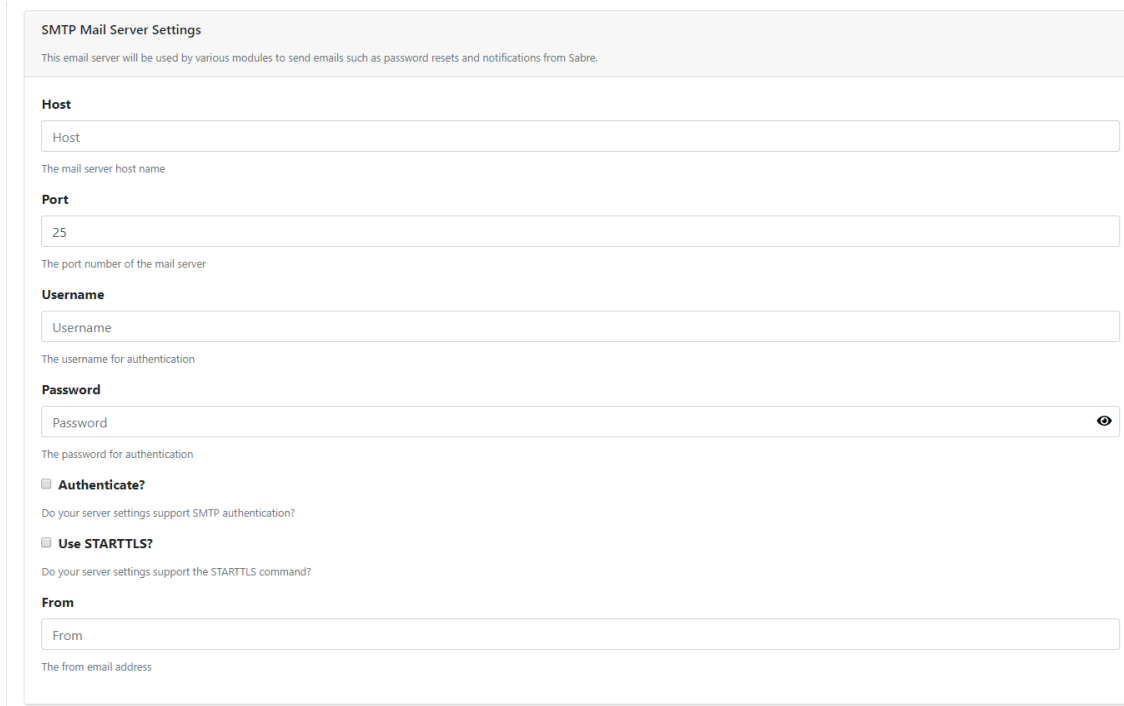
4.2 Enable Password Recovery and Reset

4.2.1 Prerequisites

Ensure the following are in place:

1. A valid SMTP mail server has been configured in your installation configuration prior to deployment. This can be done in the **SMTP Mail Server Settings** panel in

the **Global** tab of the Installation Configuration tool:



SMTP Mail Server Settings

This email server will be used by various modules to send emails such as password resets and notifications from Sabre.

Host

Host

The mail server host name

Port

25

The port number of the mail server

Username

Username

The username for authentication

Password

Password

The password for authentication

☐ **Authenticate?**

Do your server settings support SMTP authentication?

☐ **Use STARTTLS?**

Do your server settings support the STARTTLS command?

From

From

The from email address

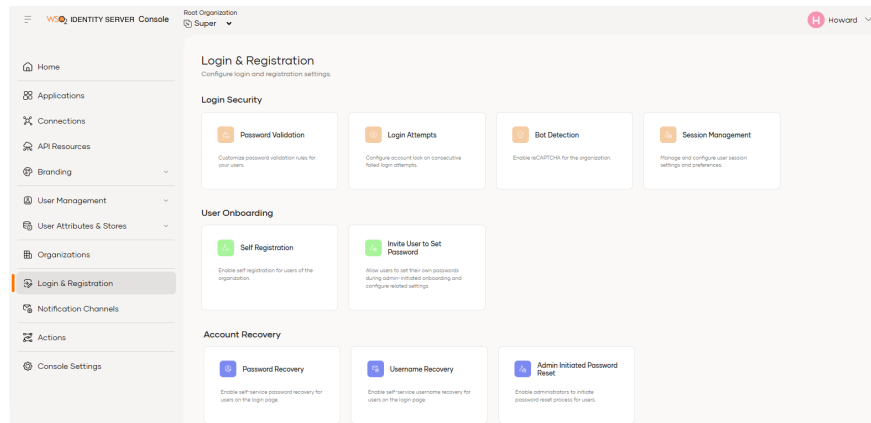
For more information on the inventory file and the Installation Configuration Tool, see the *CMP Installation Guide*.

- Every user must have an email address defined against their profile in CMP.
For information on how to do this, see [Add a User's Email in CMP](#).

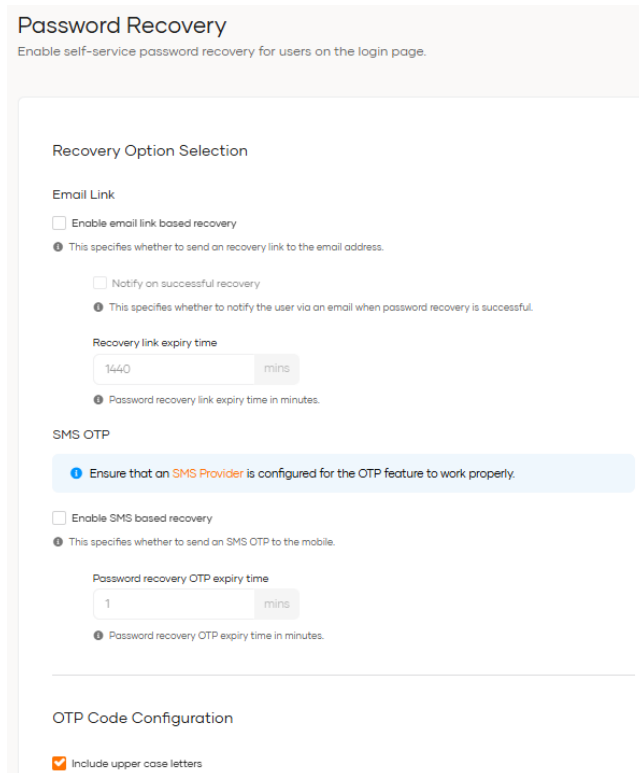
4. 2. 2 Enable Password Recovery

To enable password recovery in Identity Server:

- Log into the Identity Server Management Console.
The console opens on the **Welcome** page, with the **Home** menu tab selected.
- Select **Login & Registration** from the left-hand menu.
The *Login & Registration* page displays.



3. Under *Account Recovery*, select the **Password Recovery** tile. The *Password Recovery* page displays.



Password Recovery
Enable self-service password recovery for users on the login page.

Recovery Option Selection

Email Link

☐ Enable email link based recovery
This specifies whether to send a recovery link to the email address.

☐ Notify on successful recovery
This specifies whether to notify the user via an email when password recovery is successful.

Recovery link expiry time
1440 mins
This specifies the password recovery link expiry time in minutes.

SMS OTP

Ensure that an **SMS Provider** is configured for the OTP feature to work properly.

☐ Enable SMS based recovery
This specifies whether to send an SMS OTP to the mobile.

Password recovery OTP expiry time
1 mins
This specifies the password recovery OTP expiry time in minutes.

OTP Code Configuration

☒ Include upper case letters

4. Tick the required checkbox based on your email recovery requirements:
 - **Enable email link based recovery** - to allow users to reset their password using a recovery link sent to their email address.
 - **Enable SMS based recovery** - to allow users to receive a one-time password (OTP) by SMS.
5. If you selected **Email Link**, you can:
 - select **Notify on successful recovery** to send an email confirming that the password has been successfully reset.

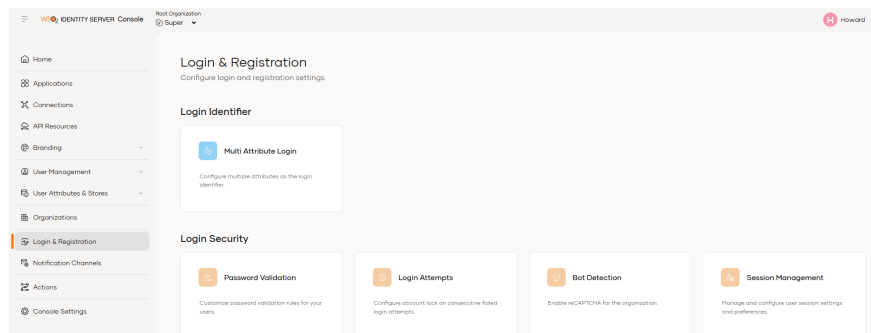
- Enter the Recovery link expiry time to specify how long the email recovery link remains valid
- 6. If you selected the **SMS OTP**, you can enter the *Password recovery OTP expiry time* to specify how long the OTP remains valid.
- 7. Configure the OTP code requirements in the **OTP Code Configuration** section.
- 8. Enter the recovery attempt limits in the **Recovery Attempts Limitation** section.
- 9. Click **Update** to save your changes.

4.3 Password Policies

CMP supports restricting reuse of previous passwords and defining password pattern policies. These can be enabled and configured through the Identity Server Management Console.

4.3.1 Set Password History Policy

1. Log into the Identity Server Management Console.
The console opens on the **Welcome** page, with the **Home** menu tab selected.
2. Select **Login & Registration** from the left-hand menu.
The *Login & Registration* page displays.



3. Under *Login Security*, select the **Password Validation** tile.
The *Password Validation* page displays.

Password Validation

Customize password validation rules for your users.

Password Expiration ☐

Apply

30

days password expiry if no other rules match to the user.

Rules will be applied in the order listed below, from top to bottom. Use the arrows to adjust the priority.

+ Add Rule

Password History Count

Specify the number of unique passwords that a user should use before an old password can be reused.

☒ Must be different from the last

5

 passwords.

Password Input Validation

Must be between

8

 and

30

 characters

Must contain at least

1

 numbers (0-9).

1

 upper-case characters (A-Z).

1

 lower-case characters (a-z).

0

 special characters (!@#%*^&').

☐ Must contain at least

1

 unique characters.

☐ Must not contain more than

1

 repeated characters.

Update

4. From this page, you can configure password policies, including password expiry, password history, and password complexity requirements.
 5. Click **Update** when you are done.
- A success message is displayed.