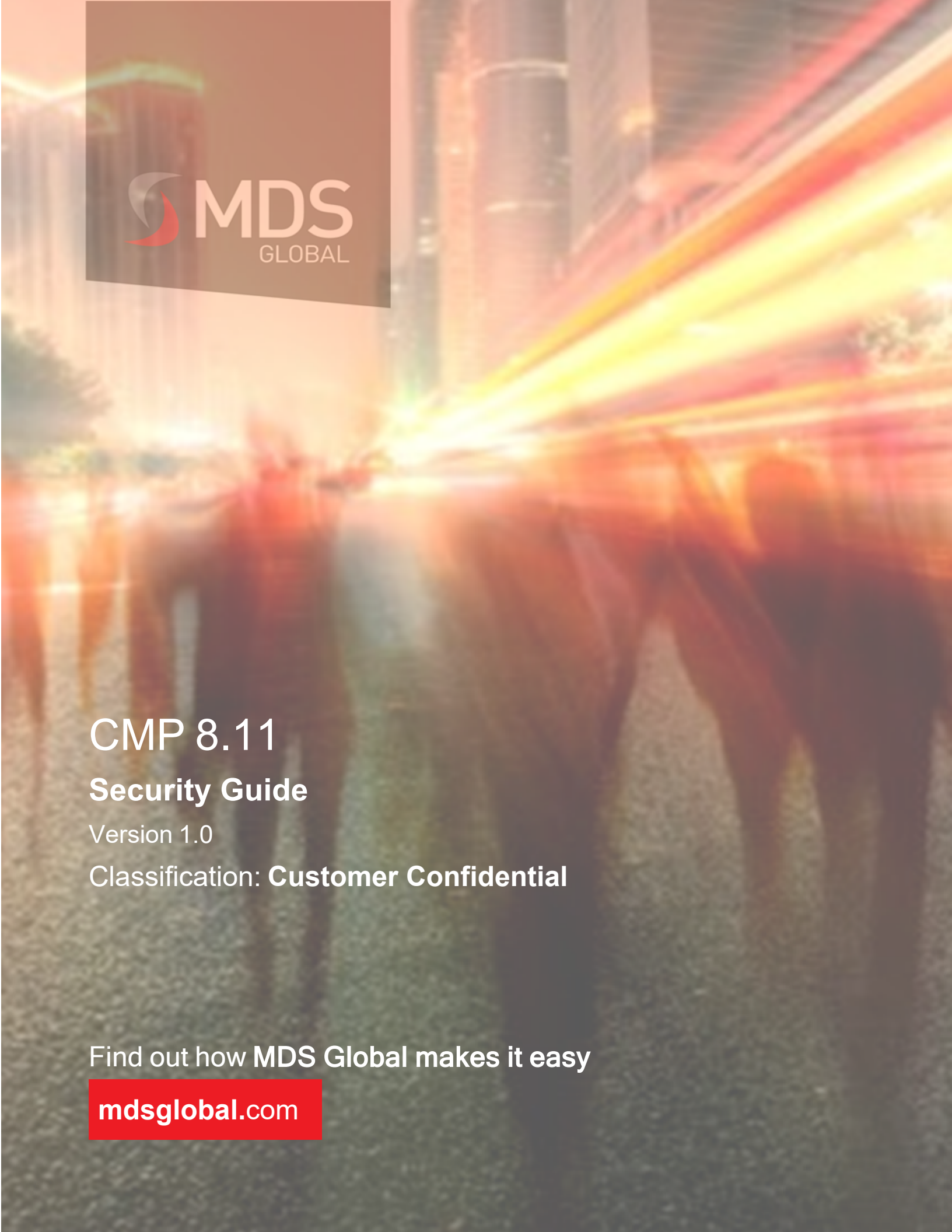


CMP 8.11

Security Guide

Version 1.0

Classification: **Customer Confidential**

Find out how **MDS Global makes it easy**

mdsglobal.com

Copyright

Confidentiality

Disclaimer

Trademarks

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

Version Control

Version	Issue Date	Author	Comments
Version 1.0	29 May 2023	MDS	CMP 8.11 Release - No changes since the last release.

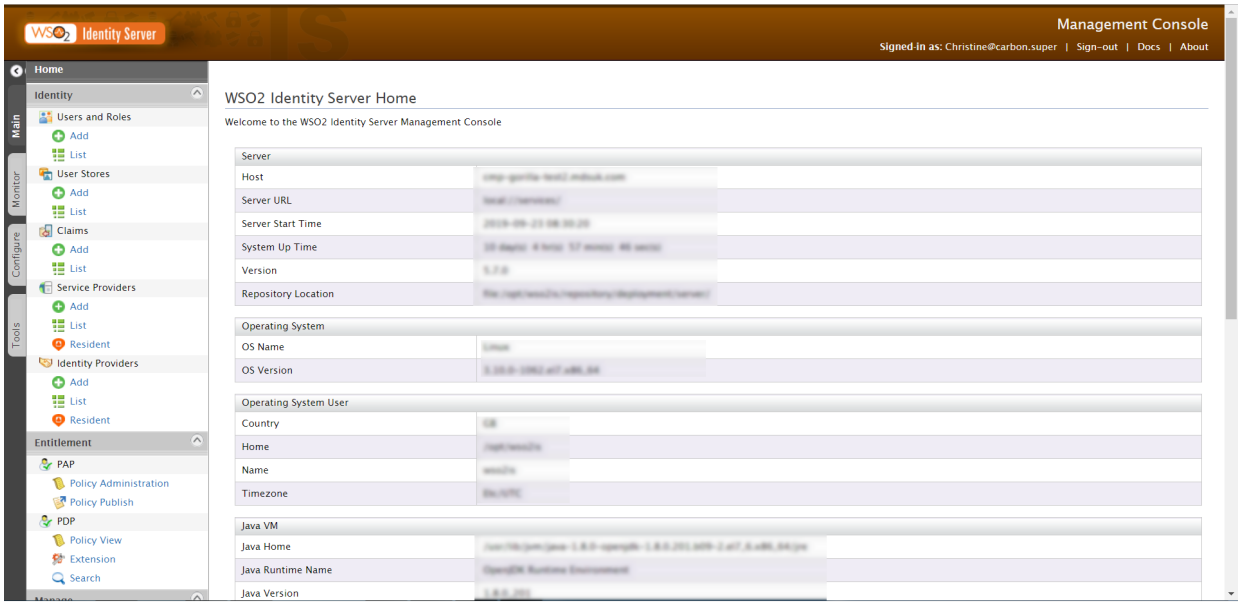
Terms Used in this Document

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.

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

1. 2 Administration Console

You can create users and assign them access to CMP applications and functionality in the Administration Console. See the **Users** screen and the online help for more information. More granular maintenance, for example assigning roles and permissions, takes place directly in Identity Server.

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.

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.

.

[1] Single 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.

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 three group roles assigned:

- Everybody
- Consumer User
- BackOffice

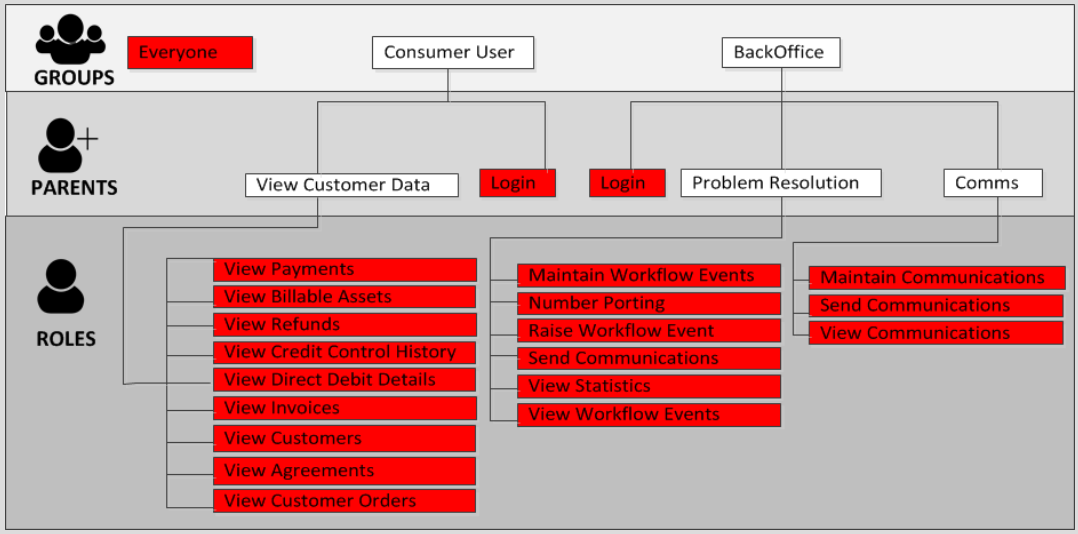
For the purposes of this example, the Everybody role is not extended any further, but the Consumer User and BackOffice groups each have parent roles assigned. Both groups have an Agent View Application role that allows access to an application and is not extended any further - that is, it has no child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

- Consumer User has the parent role View Customer Data.
- BackOffice 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 red 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 CMP Identity Server provides the following security groups to control access to CMP components:

Internal Groups

- Internal/everyone - Every user is assigned this role.
- Application groups - The Application roles are internal to WSO2 IS. They are a special case of internal roles, created for a single service provider (SP) application and only users in this role can manage relevant SP application. A Service Provider is an item in the WSO2 IS that defines an external application that uses WSO2. It defines what claims the application has access to, what type of inbound authentication mechanism does it use, etc. A user assigned to such a role can modify a specific Service Provider. The Application roles for CMP are:
    - Application/agent-view
    - Application/agent-view-interfaces-layer
    - Application/configuration-centre
    - Application/rest-ws
    - Application/role-extender
    - Application/sabre-console
    - Application/soap-ws

AgentView Groups

The following group roles control access to AgentView and BackOffice functionality:

- agent-view-backoffice
- agent-view-consumer-csa
- agent-view-consumer-user
- agent-view-enterprise-admin
- agent-view-enterprise-csa
- agent-view-enterprise-user
- agent-view-manager

For more information, see "AgentView Groups and Parent Roles" on the next page.

Business Configuration Groups

The following groups control grant access to the Business Configuration console and API and control what functionality the user can access:

- configuration_centre_read_only
- configuration_centre_admin
- config_centre_admin_user

Batch Server/Batch Jobs Groups

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

- sabre_console_admin
- sabre_console_advanced_ops
- sabre_console_basic_ops
- sabre_console_read_only

For more information, see "Batch Server and Administration Console Groups and Roles" on page 11.

Web Service Groups

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

- soap-ws-all
- soap-ws-basic
- soap-ws-billing
- soap-ws-customer
- soap-ws-financial
- soap-ws-order

Users with the Application/rest-ws role have access to the RESTful web services.

For more information, see "Web Service Groups and Parent Roles" on page 14.

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							
	agent-view-consumer-user	agent-view-enterprise - user	agent-view-consumer-CSA	agent-view-enterprise-CSA	agent-view-enterprise-admin	agent-view-manager	agent-view-back-office	agent-view-admin
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				✓	✓	✓		✓
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 Comms

This parent role has the following child roles:

- Maintain Communications
- Send Communications
- View Communications

3.1.1.2 Credit Control

This parent role has the following child roles:

- Credit Control Management
- View Credit Control History
- Write-offs

3.1.1.3 Customer Data

This parent role has the following child roles:

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

3.1.1.4 Customer Orders

This parent role has the following child roles:

- Add Customers
- Maintain Agreements
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Orders
- Maintain Payment Details
- Maintain Payments
- Maintain Subscription Services

3.1.1.5 Enterprise Data

This parent role has the following child roles:

- Maintain Customers
- Maintain Direct Debit Details
- Maintain Enterprises
- Maintain Invoices
- Maintain Subscription Services

3.1.1.6 Enterprise Orders

This parent role has the following child roles:

- Add Customers
- Maintain Customers
- Maintain Direct Debit Details
- Maintain Payment Details
- Maintain Subscription Services

3.1.1.7 Finance

This parent role has the following child roles:

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

3.1.1.8 Hierarchy Management

This parent role has the following child roles:

- Maintain Agreements
- Maintain Customers
- Maintain Enterprises

3.1.1.9 Payment Handling

This parent role has the following child roles:

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

3.1.1.10 Problem Resolution

This parent role has the following child roles:

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

3.1.1.11 View Customer Data

This parent role has the following child roles:

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

3.1.1.12 View Enterprise Data

This parent role has the following child roles:

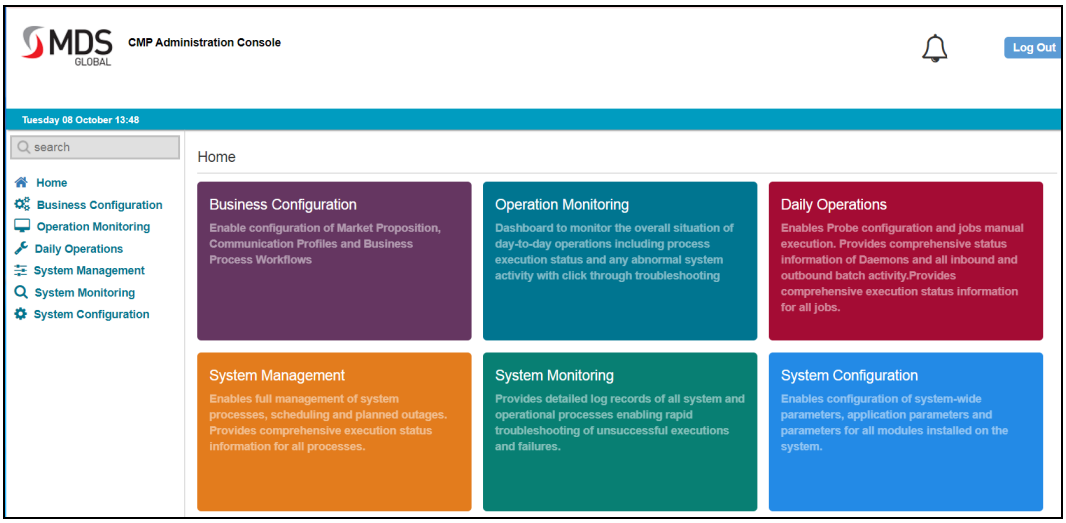
- Send Communications
- View Agreements
- View Communications
- View Credit Control History
- View Customers
- View Direct Debit Details
- View Discounts
- View Enterprises
- View Invoices
- View Payments
- View Refunds
- View Usage Details
- View Weblinks
- View Workflow Events

3.1.1.13 Workflow Handling

This parent role has the following child roles:

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

3. 2 Batch Server and Administration Console Groups and Roles



Administration Console Home Page

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

- sabre-console-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.

- sabre-console-basic-ops

  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.

- sabre-console-advanced-ops

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

- sabre-console-admin

  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-comsole-)			
	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			✓	✓
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 Recip-			✓	✓

Administration Console Functionality	Groups (sabre-comsole-)			
	read-only	basic-ops	advanced-ops	-admin
ient				
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		✓	✓	✓
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				✓

Administration Console Functionality	Groups (sabre-comsole-)			
	read-only	basic-ops	advanced-ops	-admin
System Configuration > Logging > Edit Days To Retain				✓

3. 3 Web Service Groups and Parent Roles

The following table lists the web service security groups and the roles that belong to the groups. These roles represent the web services that a user who is assigned to a group can access.

Parent Role	Group (soap-ws-)					
	all	basic	customer	financial	billing	orders
accountservice-addregisteredcard	✓		✓			
accountservice-cancelregisteredcard	✓		✓			
accountservice-createaccount	✓		✓			✓
accountservice-queryaccount	✓	✓	✓			✓
accountservice-query-customerpreferences	✓	✓	✓			
accountservice-querynamesfornumbers	✓	✓	✓			
accountservice-setcustomerpreferences	✓		✓			
accountservice-setnamesfornumberslist	✓					
accountservice-updateaccount	✓		✓			✓
accountservice-updateaccountdetails	✓	✓	✓			✓
accountservice-updateac-countpaymenttype	✓		✓			✓
additionalofferservice-expire-additionaloffer	✓					
addressservice-createaddress	✓		✓			
addressservice-createemailaddress	✓		✓			✓
addressservice-queryemails	✓	✓	✓			
addressservice-removeemail	✓		✓			
addressservice-updateaddress	✓		✓			✓
agreementservice-createagreement	✓		✓			✓
agreementservice-cre-ateagreementcostcentre	✓		✓			✓
agreementservice-queryagreement	✓	✓	✓			
agreementservice-query-agreementcostcentres	✓		✓			
agreementservice-query-agreementsbycustomerlevel	✓	✓	✓			
agreementservice-updateagreement	✓		✓			✓
billingservice-createbundle	✓				✓	✓

Parent Role	Group (soap-ws-)					
	all	basic	customer	financial	billing	orders
billingservice-createbundlelink	✓				✓	
billingservice-createcugnumbers	✓				✓	
billingservice-querybundle	✓	✓	✓		✓	
billingservice-queryrecentusage	✓	✓	✓		✓	
billingservice-queryunbilledunitattributes	✓	✓	✓		✓	
billingservice-queryunbilledunits	✓	✓	✓		✓	
billingservice-setattributes	✓				✓	
billingsservice-creatediscount	✓				✓	✓
billingsservice-updatediscount	✓				✓	✓
compositeservice-manageservice	✓		✓			
confirmmigration-setmigrationdetails	✓					
confirmmigration-val-idatemigrationdetails	✓					
corporateservice-createcorporate	✓		✓			✓
corporateservice-querycorporate	✓	✓	✓			
corporateservice-updatecorporate	✓		✓			✓
featuresservice-queryfeaturehistory	✓	✓	✓			
featuresservice-setfeature	✓					
financialsservice-cre-ateinvoicequeryamount	✓			✓		
financialsservice-queryaccountbalance	✓	✓	✓	✓		
financialsservice-queryinvoicedetail	✓	✓	✓	✓		
financialsservice-query-invoicequeryamounts	✓	✓	✓	✓		
financialsservice-queryinvoices	✓	✓	✓	✓		
financialsservice-querytransactions	✓	✓	✓	✓		
financialsservice-veri-fybankaccountnumber	✓			✓		
groupservice-creategroup	✓		✓			✓

Parent Role	Group (soap-ws-)					
	all	basic	customer	financial	billing	orders
groupservice-querygroup	✓	✓	✓			
groupservice-updategroup	✓		✓			✓
networkfeaturesservice-set-networkfeature	✓		✓			
networkprovisioningservice-updaten-etworkprovisioningstatus	✓					
paymentservice-createpayment	✓			✓		✓
paymentservice-getpaymenterrors	✓			✓		
paymentservice-paymenthistory	✓			✓		
paymentservice-recordpayment	✓			✓		
paymentservice-releasepayment	✓			✓		
pricingparamsservice-querytariffs	✓	✓	✓			
search-searchaccountsbyserialnumber	✓		✓			
search-searchbyattributevalue	✓	✓	✓			
search-searchbynameandaddress	✓	✓	✓			
search-search-subscriptionsbyserialnumber	✓	✓	✓			
securityservice-querysecuresession	✓	✓	✓			
servicesservice-createservice	✓				✓	✓
servicesservice-queryaccountservices	✓	✓	✓		✓	
servicesservice-querysub-scriptionservices	✓	✓	✓		✓	
servicesservice-updateservice	✓				✓	✓
structureservice-query-agreementstructure	✓	✓	✓			
structureservice-querycustomerstructure	✓	✓	✓			
structureservice-querykeycustomerinfo	✓	✓	✓			
structureservice-setkeycustomerinfolist	✓					
subscriptionservice-createsubscription	✓		✓			✓

Parent Role	Group (soap-ws-)					
	all	basic	customer	financial	billing	orders
subscriptionservice-linksubscriptions	✓					
subscriptionservice-querysubscription	✓	✓	✓			
subscriptionservice-updatesubscription	✓		✓			✓
subscriptionservice-update-subscriptionserialnumbers	✓					✓
subscriptionservice-updatetariff	✓		✓			✓
workflowservice-cre-atesalesledgeradjustment	✓			✓		
workflowservice-createworkflow	✓	✓				
workflowservice-delete-salesledgeradjustment	✓			✓		
workflowservice-queryworkflow	✓	✓	✓			
workflowservice-queryworkflows		✓				
workflowservice-queryworklist	✓	✓	✓			
workflowservice-queryworklists	✓	✓	✓			
workflowservice-updateworkflow	✓	✓				

4.0 Creating Users and Assigning Group Roles in Identity Server

When CMP is first installed, use the Administrator username and password defined as part of the installation process to connect to the Identity server to create and administer users. 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.

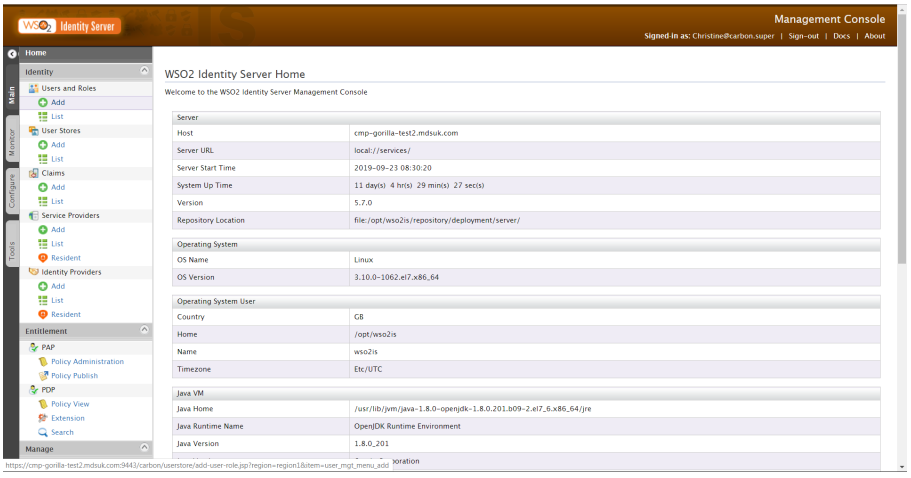
You can create users and assign them group roles in the Management Console of the Identity Server. You can:

- Create a new user and assign them roles.
- Manage the groups roles and passwords for users.

4. 1 Create a User in Identity Server

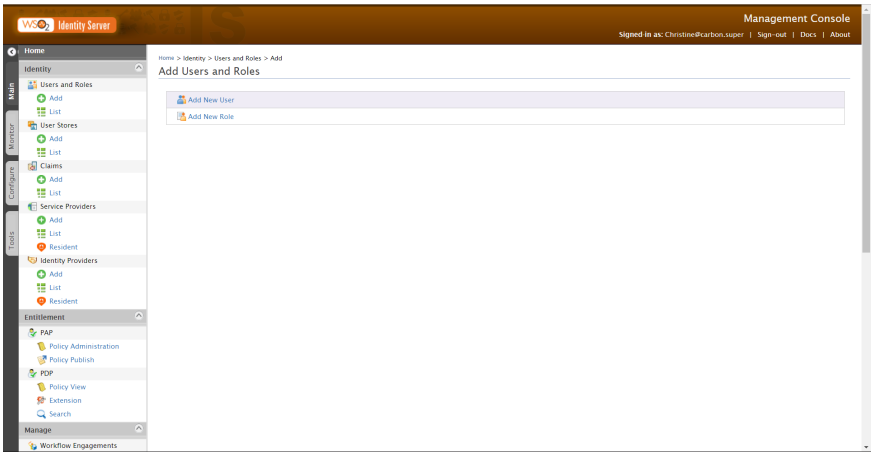
To create a user and assign them one or more group roles, follow these steps:

1. Log in to the Identity Server Management Console.
2. The console opens on the **Home** page. By default, the **Main** menu tab is selected.



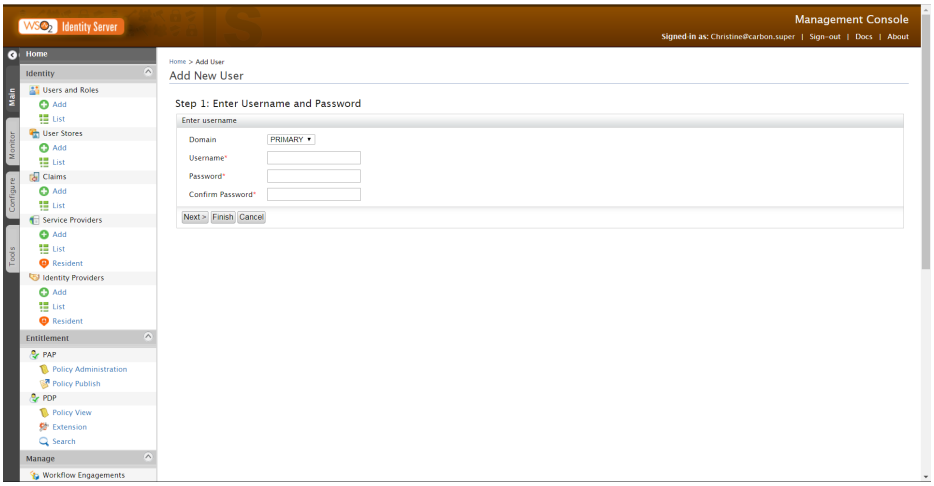
3. In the **Main** menu in the **Identity** section, under **Users and Roles**, click **Add**.

   The **Add Users and Roles** screen opens.



4. Click **Add New User**.

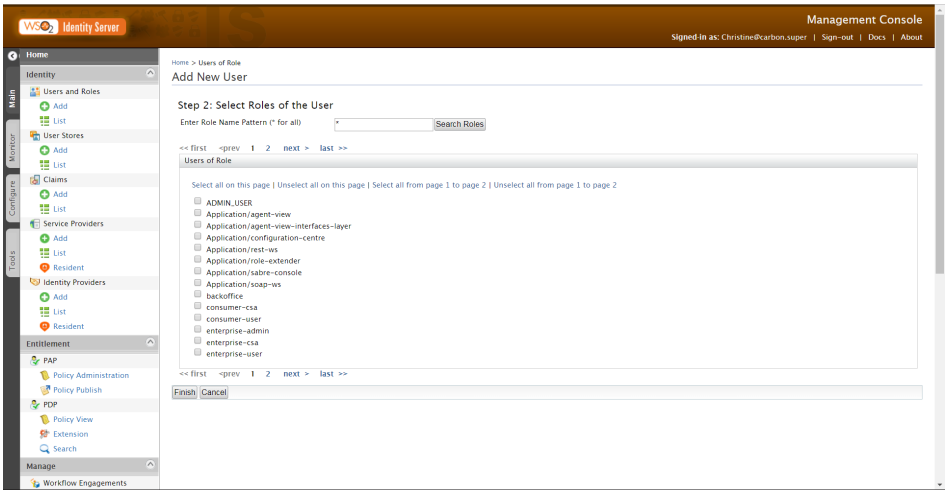
   The **Add New User - Step 1** screen is displayed.



5. In the **Domain** drop-down, accept the default selection of the **PRIMARY** domain.
6. Enter a **Username** and **Password**. Confirm the password.
7. Click **Next** to assign group roles to the new user.

> If you click **Finish** at this point the user will be created but will not have any roles assigned.

8. The **Add New User - Step 2** screen is displayed.



Tips:

Use the **Select** hyperlinks at the top of the roles list to select/deselect multiple roles at a time.

You can search for roles using a pattern, for example `*admin`.

Use the pagination links to scroll through the pages of roles, if required.

9. When you have added all the roles for the user, click **Finish**.

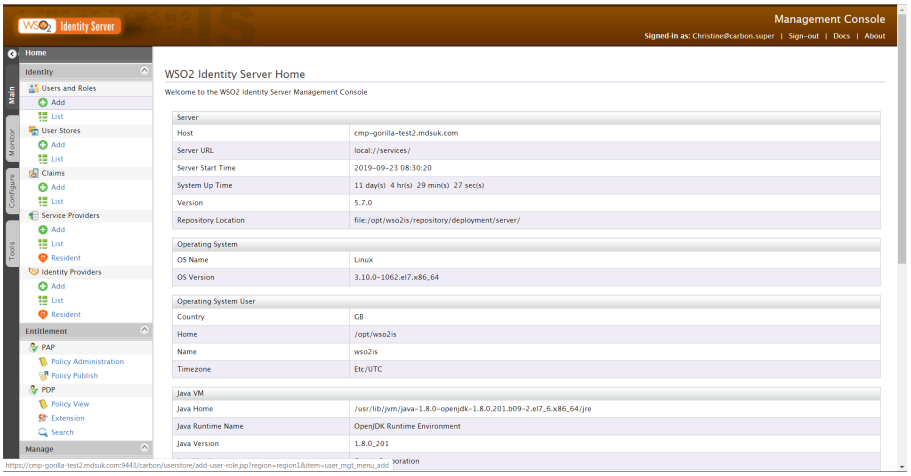
   A success message is displayed and you return to the Users screen where the new user is listed.

4. 2 Manage a User's Role in Identity Server

To manage a user and their roles, follow these steps:

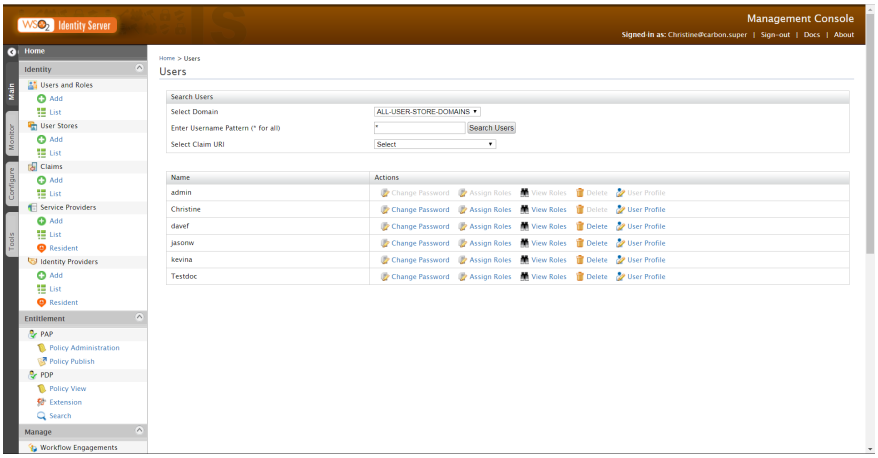
1. Log in to the Identity Server Management Console.

   The console opens on the **Home** page. By default, the **Main** menu tab is selected.

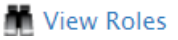


2. In the **Main** menu in the **Identity** section, under **Users and Roles**, click **List**.

   The **Users and Roles** screen opens.
3. Click **Users**
4. The **Users** screen is displayed.



5. Manage a user and their roles as follows:

To change a password:	1. Click **Change Password**  for that user. 2. In the **Change Password** screen, enter the **Current Password**. 3. Enter the **New Password** and **Confirm New Password**. 4. Click **Change**.
To assign roles:	1. Click **Assign Roles**  for that user. 2. Select the roles to assign. 3. Click **Update** to update the user and remain in the screen. 4. Or, click **Finish** to update the user and return to the **Users** screen.
To view/unassign roles for the user:	1. Click **View Roles**  for that user. The **Role List of User <Name>** screen displays all assigned roles. 2. Deselect roles to unassign them. 3. Click **Update** to update the user and remain in the screen. 4. Or, click **Finish** to update the user and return to the **Users** screen.
To delete a user:	1. Click **Delete**  for that user. 2. Click **Yes** in the Confirmation box.

Important: The Identity Server Management Console has many other menu options and screens. Only Administrators who understand the impact of their actions should access and use them.

5.0 Password Recovery and Reset

Users can request a password reset via the **Forgot Password** link in the login box on the Identity Server login screen:

Clicking this link launches the **Recover Password** box, where the user can enter their username and click **Submit** to send a password reset request.

In response, CMP sends an email to the user's email address configured in WSO2 (Identity Server). The email contains a link to reset their password. When the user clicks the link they are redirected to a screen to enter a new password. If the new password matches any security policy in place then the new password is stored in Identity Server.

For information on how to enter a user's email in Identity Server, see the section "Add a User's Email in Identity Server" on page 33.

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 27

5. 1 Password Reset Templates

The email templates 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:

```
CMP - Password Reset
```

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

```
<html>
<body>
<h1>Password Reset</h1>
<p>Hi ${givenName},<br/>
We received a request to reset the password for the ${username} account that is associated with this email address.
If you made this request, please click the button below to securely reset your password.</p>
<p>
<a href="${recoveryUrl}" target="_blank" style="width: 230px; font-family: 'Nunito Sans', Arial, Verdana, Helvetica, sans-serif;  font-size: 18px; line-height: 21px; font-weight: 600; color: #fff; text-decoration: none; background-color: #e30613; text-align: center; display: inline-block; cursor: pointer;">Reset Password</a>
</p>
<p>
If clicking the button doesn't seem to work, you can copy and paste the following link into your browser.
<br/>
${recoveryUrl}
</p>
<p>
If you did not request to have your ${username} password reset, disregard this email and no changes to your account will be made.
</p>
<p>Thanks,<br/>
The CMP Team
</p>
<p><img src="${wso2LoginUrl}/resources/static/img/CMP%20Full%20logo.png" height="50" width="125"/></p>
</body>
</html>
```

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

```
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 ${wso2LoginUrl}/ssologin and use the
forgotten password functionality to reset your password.</p>
<p>Thanks,<br/>
The CMP Team
</p>
<p><img src="${wso2LoginUrl}/resources/static/img/CMP%20Full%20logo.png" height="50" width="125"/></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).

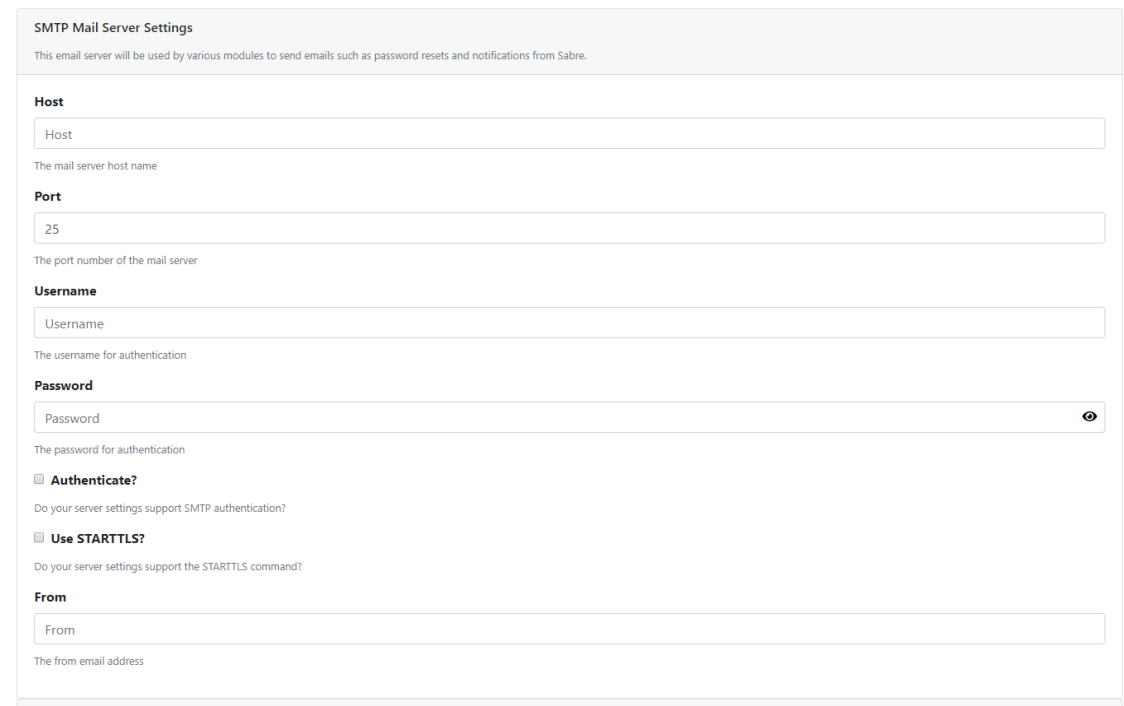
The email server settings are defined in the properties file: `/etc/mdsglobal/wso2is-login/application.properties`.

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:



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/templates/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
```

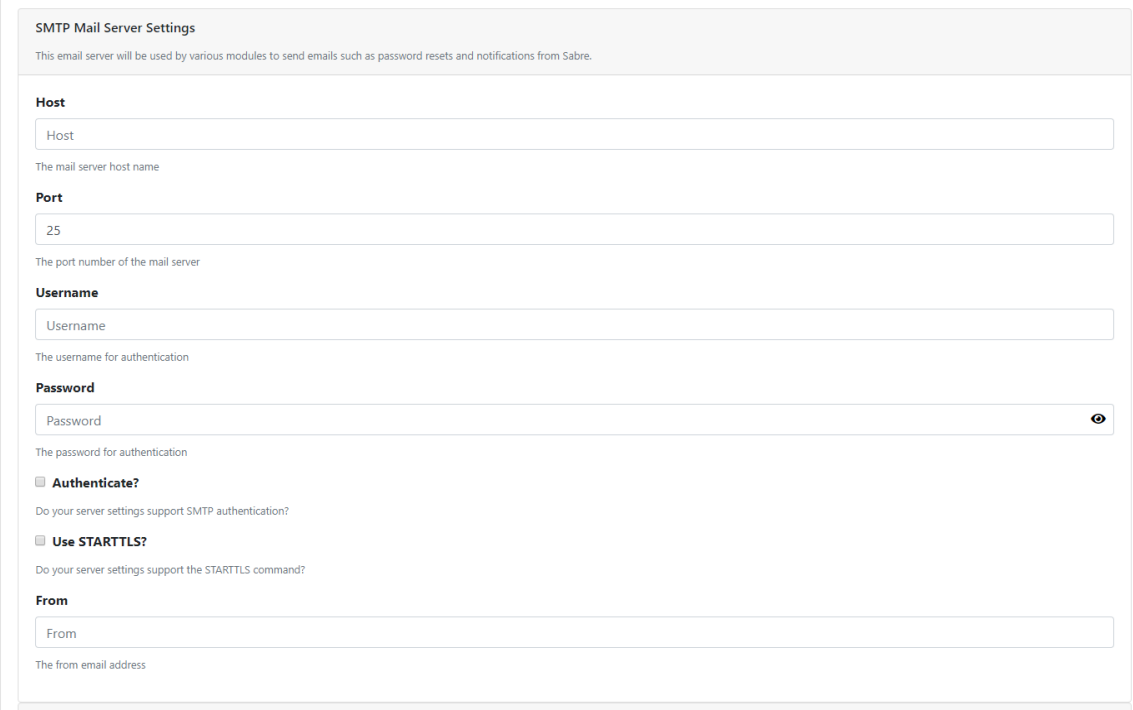
This location can be changed if necessary.

5. 2 Enable Password Recovery and Reset

5. 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:



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

2. Every user must have an email address defined against their profile in WSO2.

   For information on how to do this, see "Add a User's Email in Identity Server" on page 33.

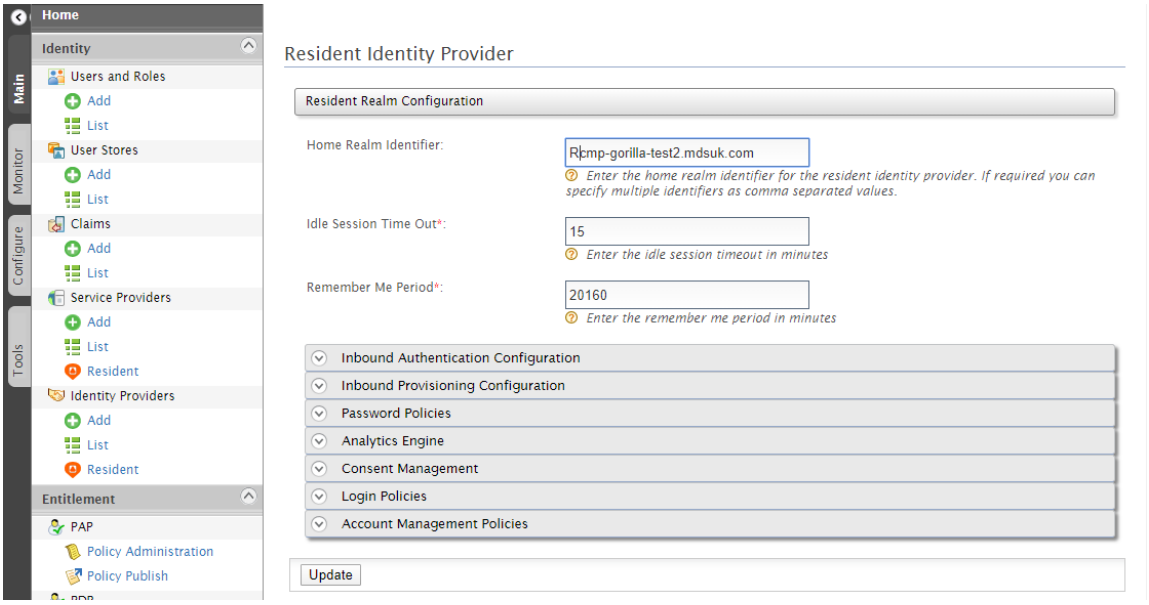
5. 2. 2 Enable Password Recovery

To enable password recovery in Identity Server:

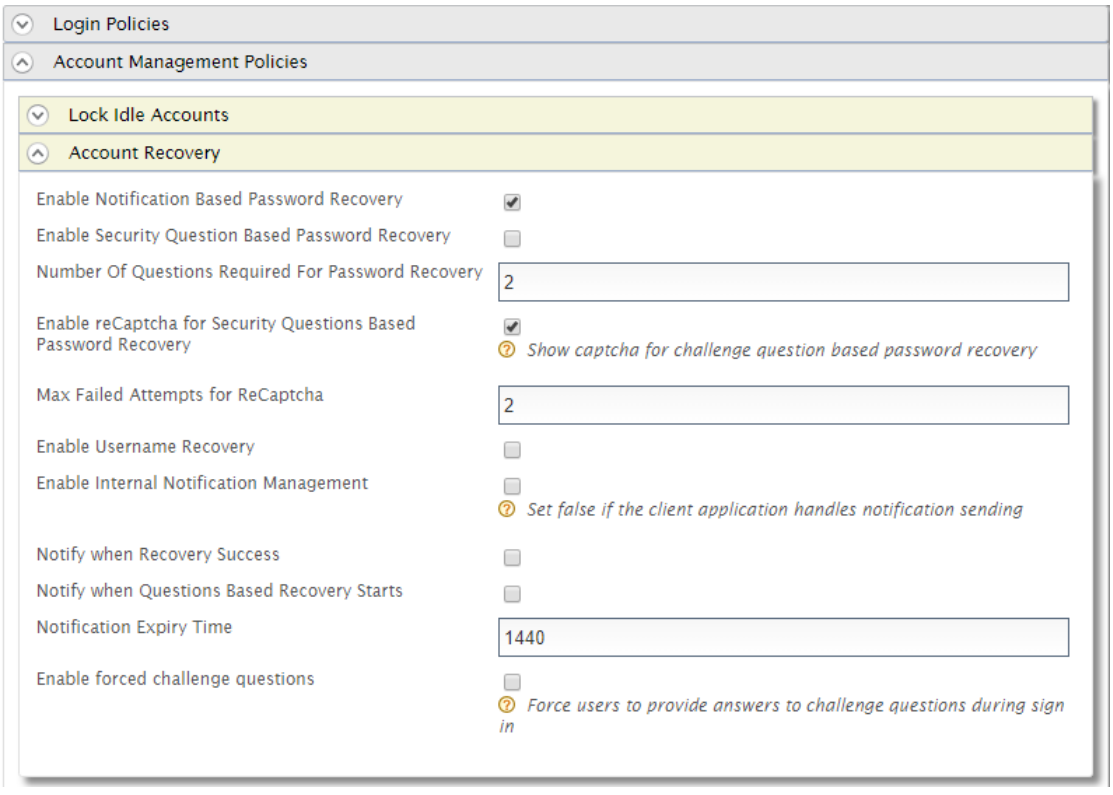
1. Log into the Identity Server Management Console.

   The console opens on the **Home** page. By default, the **Main** menu tab is selected.

2. In the **Identity** section of the tab, locate **Identity Providers** and click **Resident**.



3. In the **Resident Identity Provider** screen, expand **Account Management** Policies.
4. Ensure that **Enable Notification Based Password Recovery** is selected and that **Enable Internal Notification Management** is deselected:



CMP supports the other options in this screen.

5. Click **Update**.

   A success message is displayed.

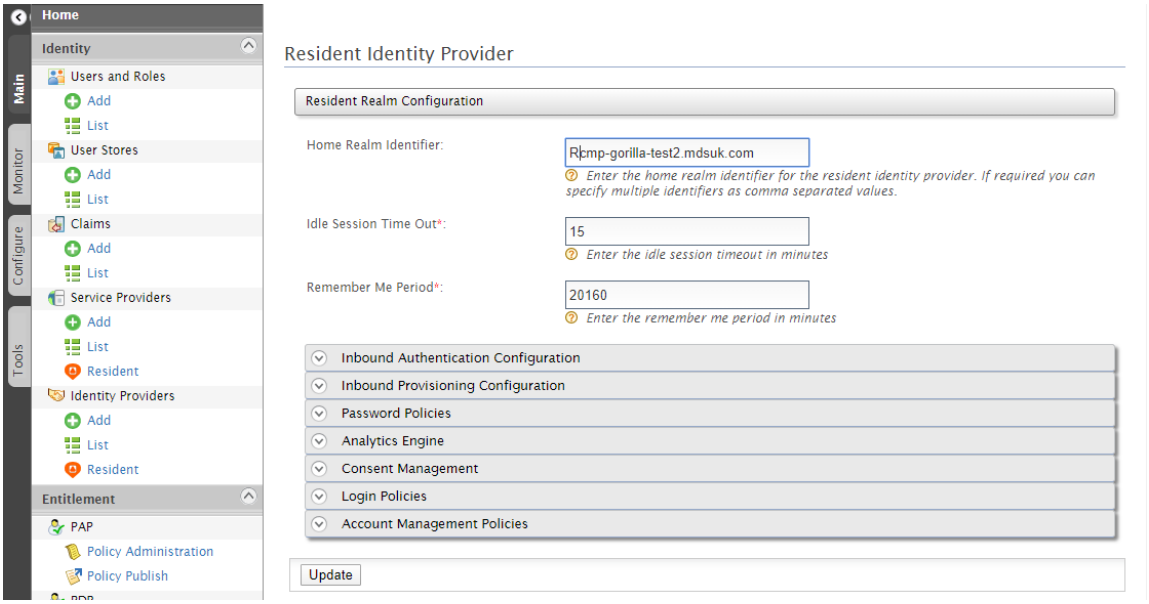
5. 3 Password Policies

CMP 8 supports restricting reuse of previous passwords and defining password pattern policies. These can be enabled and configured through the Identity Server Management Console.

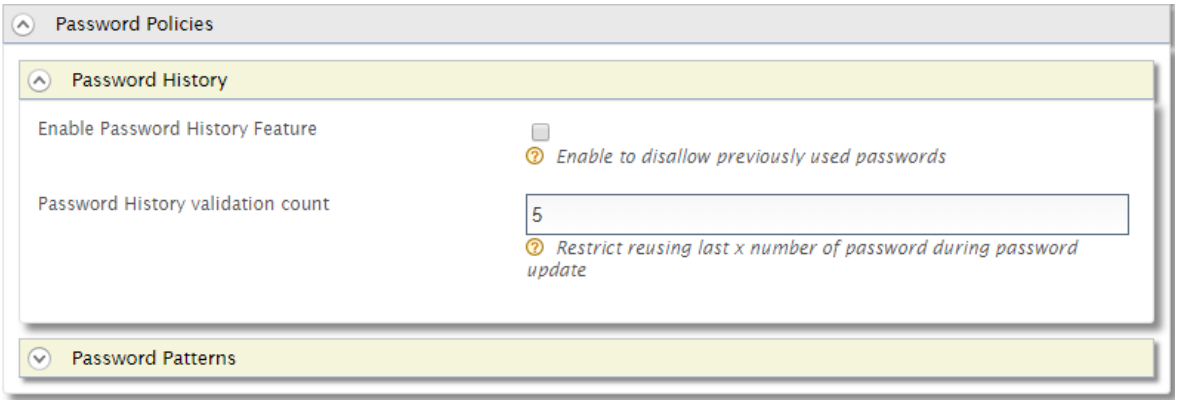
5. 3. 1 Set Password History Policy

1. Log into the Identity Server Management Console.

   The console opens on the **Home** page. By default, the **Main** menu tab is selected.
2. In the **Identity** section of the tab, locate **Identity Providers** and click **Resident**.



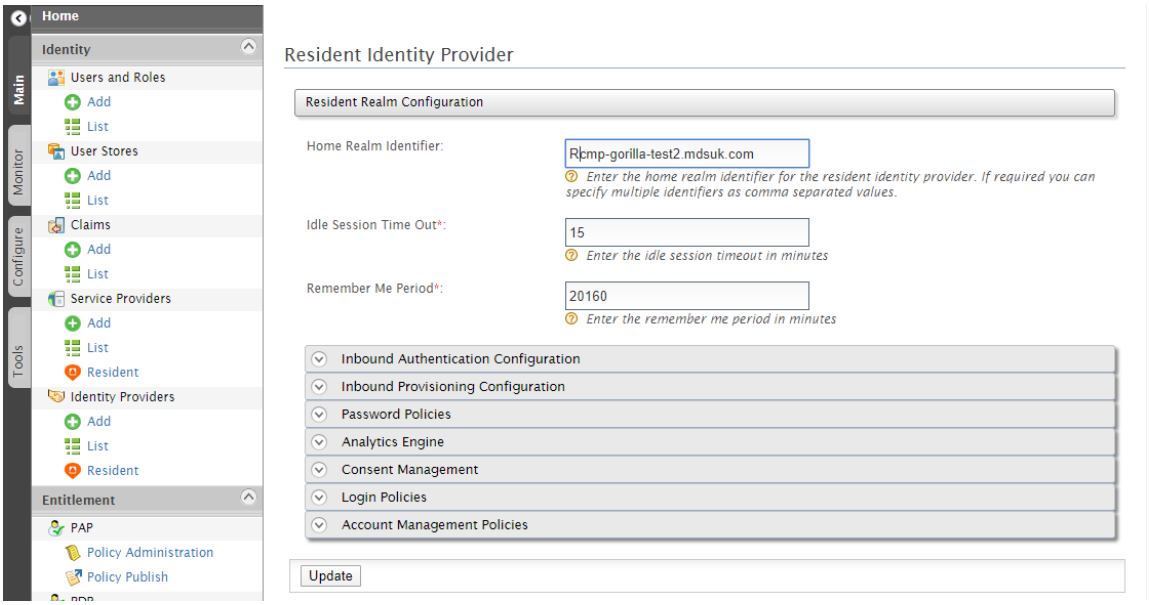
3. In the **Resident Identity Provider** screen, expand **Password Policies** > **Password History**.
4. You can **Enable Password History Feature** and enter a **Password History validation count**.



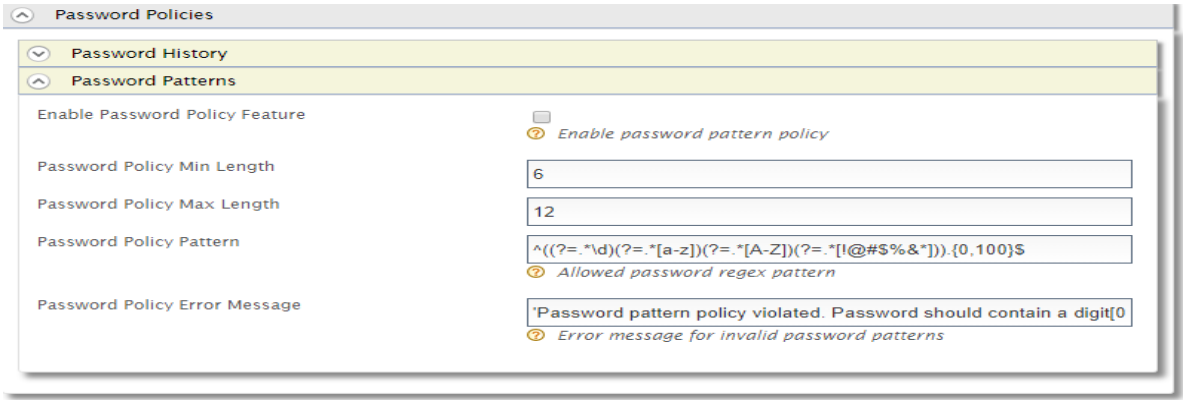
5. Click **Update**.
   A success message is displayed.

5. 3. 2 Set Password Patterns Policy

1. Log into the Identity Server Management Console.
   The console opens on the **Home** page. By default, the **Main** menu tab is selected.
2. In the **Identity** section of the tab, locate **Identity Providers** and click **Resident**.



3. In the **Resident Identity Provider** screen, expand **Password Policies** > **Password Patterns**.
4. To define a password pattern policy, you can:
   a. Enable **Password Policy Feature**
   b. Enter a **Password Policy Min Length**
   c. Enter a **Password Policy Max Length**
   d. Specify a **Password Policy Pattern**
   e. Define a **Policy Error Message** for when a user enters a password that doesn't meet the policy requirements
   .



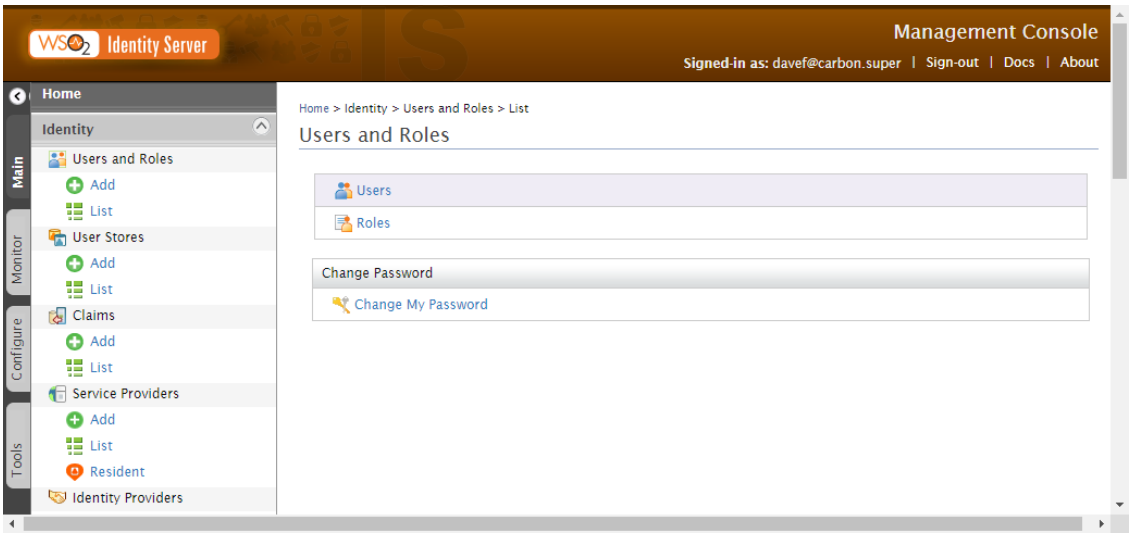
5. Click **Update**.
   A success message is displayed.

5. 4 Add a User's Email in Identity Server

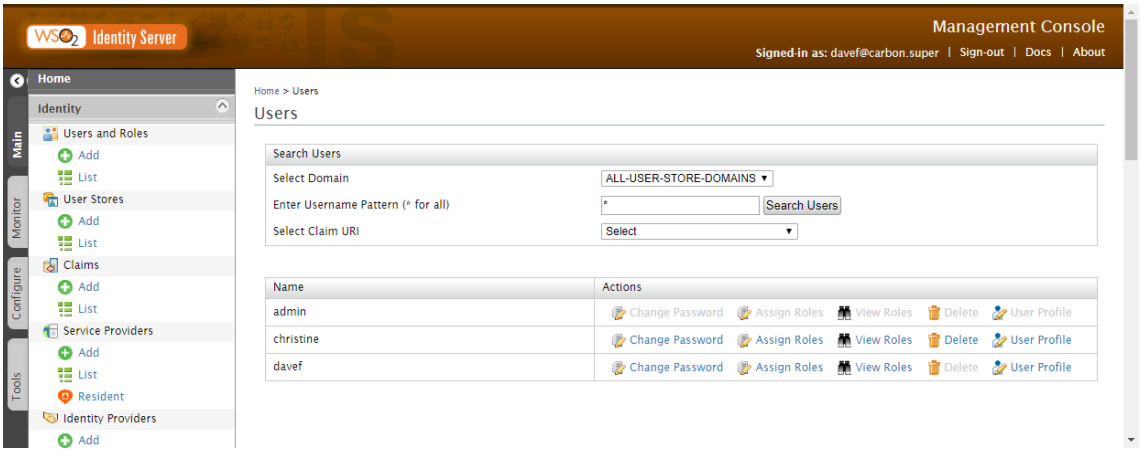
Once a user has been added to Identity Server, you can edit the user profile to add information such as an email address or phone number.

For information on adding a user see "Create a User in Identity Server" on page 19.

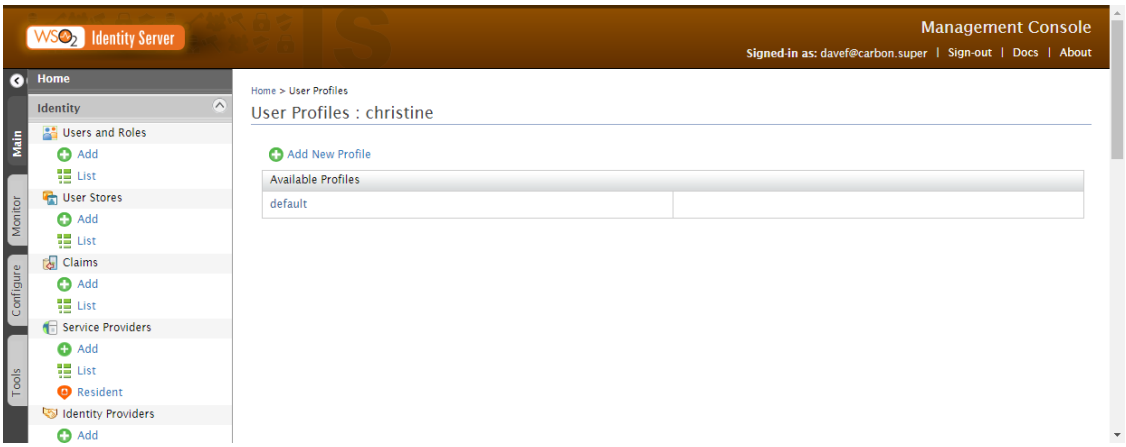
1. Log in to the Identity Server Management Console.
   The console opens on the **Home** page. By default, the **Main** menu tab is selected.
2. In the **Main** menu in the **Identity** section, under **Users and Roles**, click **List**.
   The **Users and Roles** screen opens.



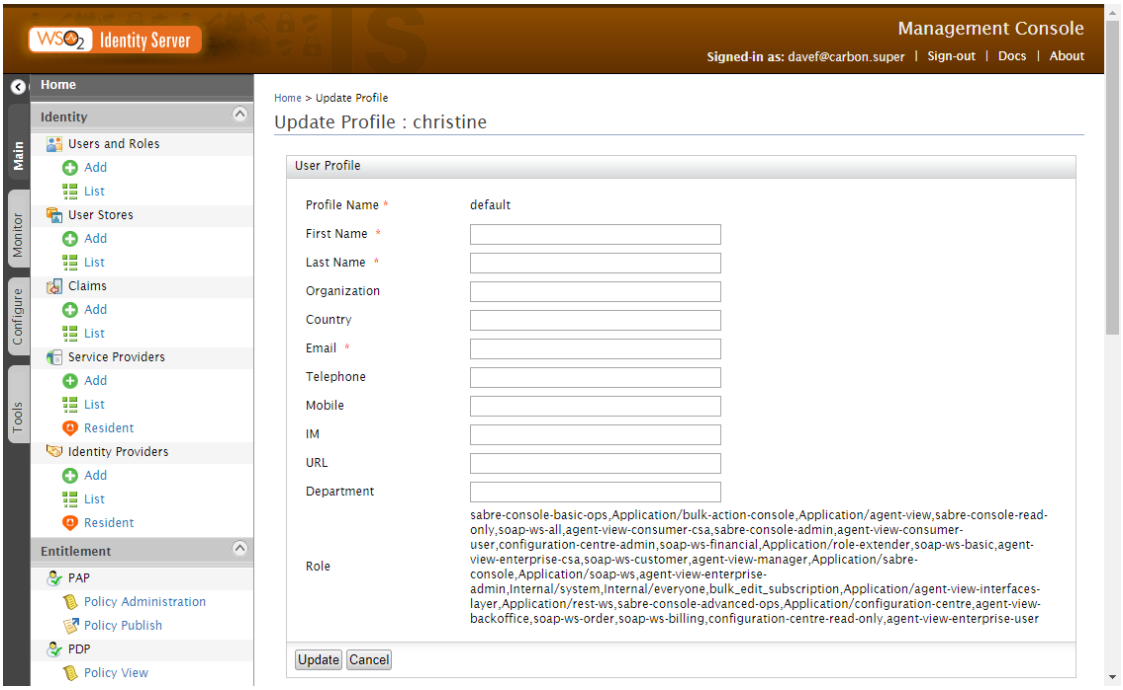
3. Click **Users**.
   The **Users** screen is displayed.



4. Click **User Profile** of the user for whom you want to add an email address.
   The **User Profiles** screen is displayed for that user.



5. Click the user profile to edit. In this case it is **default**.
   The **Update Profile** screen displays the settings for the profile.



6. Enter an **Email** for the user and click **Update**.
   A success message is displayed.