

GUIDE

erwin Mart Portal and erwin ER360

Installation Guide 15.0



Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the "Documentation"), is for your informational purposes only and is subject to change or withdrawal by Quest Software, Inc and/or its affiliates at any time. This Documentation is proprietary information of Quest Software, Inc and/or its affiliates and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Quest Software, Inc and/or its affiliates

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Quest Software, Inc and/or its affiliates copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Quest Software, Inc and/or its affiliates that all copies and partial copies of the Documentation have been returned to Quest Software, Inc and/or its affiliates or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, QUEST SOFTWARE, INC. PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL QUEST SOFTWARE, INC. BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF QUEST SOFTWARE, INC. IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Quest Software, Inc and/or its affiliates.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c) (1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2026 Quest Software, Inc and/or its affiliates All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact erwin

Understanding your Support

Review [support maintenance programs and offerings](#).

Registering for Support

Access the [erwin support](#) site and register for product support.

Accessing Technical Support

For your convenience, erwin provides easy access to "One Stop" support for all editions of [erwin Data Modeler](#), and includes the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- erwin Support policies and guidelines
- Other helpful resources appropriate for your product

For information about other erwin products, visit [erwin by Quest Products page](#).

Provide Feedback

If you have comments or questions, or feedback about erwin product documentation, you can send a message to techpubs@erwin.com.

News and Events

Visit [News and Events](#) to get up-to-date news, announcements, and events. View video demos and read up on customer success stories and articles by industry experts.

Contents

erwin Mart Portal Architecture	7
Setting up erwin Mart Portal	9
Reviewing Prerequisites	10
Install a Mart or Upgrade a Mart?	18
Character Limitations	19
Mart Portal Version Validation	21
Configuring Database	22
Creating Oracle Database	23
Creating PostgreSQL Database	27
Creating SQL Server Database	29
Specify Use of Foreign Characters With Microsoft SQL Server	30
Installing erwin Mart Portal and erwin ER360	31
Create a Pluggable Database	33
Install erwin Mart Portal with a Pluggable Database	35
Configuring erwin Mart Portal	36
Configuring Database Settings	37
Configuring Mart Portal Settings	40
Configuring Advanced Settings	41
Configuring Authentication Settings	45
Configuring Proxy Settings	49
Configuring erwin Mart Portal- CLI Commands	55
Entra ID OAuth2	60

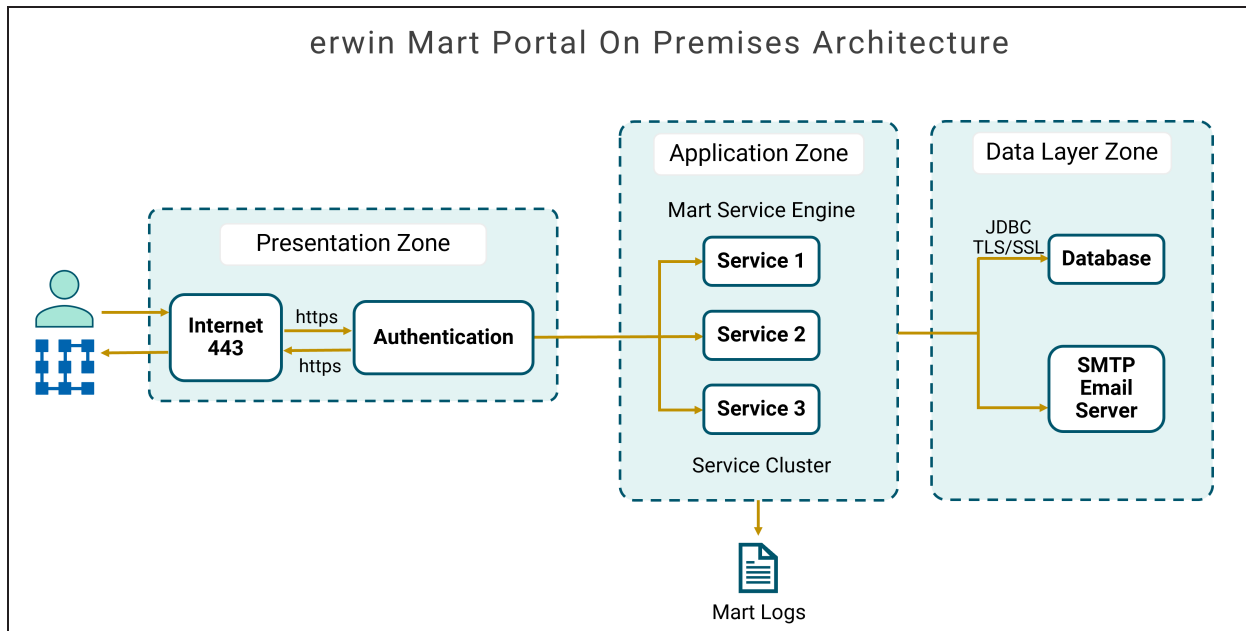
Adding Users in erwin Mart Portal	87
Adding Groups in erwin Mart Portal	88
SAML with Entra ID	89
Adding Groups in erwin Mart Portal	108
SAML with PingIdentity	111
Adding Groups in erwin Mart Portal	130
SAML with Okta	134
Adding Groups in erwin Mart Portal	155
SAML with WSO2	159
Adding Groups in erwin Mart Portal	172
Initializing erwin Mart Portal and erwin ER360	176
erwin Mart Portal	176
erwin ER360	179
Logging in to erwin Mart Portal and Configuring Settings	183
Use a Pluggable Database	185
Logging in to erwin ER360 and Configure Settings	187
Enabling IIS	190
Change the Mart Database Server	197
Upgrading Mart	198
Upgrade Performance Considerations	200
Upgrading erwin Mart Portal	202
Restarting the erwin Mart Portal Service	203
Viewing Log Files	204
Use erwin Mart Portal as a Windows Service	205
Enable Logging in Local AppData	206

Troubleshooting	207
Chinese characters are replaced with question marks in Postgre SQL Mart	212

erwin Mart Portal Architecture

erwin Mart Portal architecture follows a JAR-based, multi-product structure.

The following diagram explains erwin Mart Portal architecture:



The mart comprises the following components:

Database

Stores the user data for the Workgroup Edition.

Database	Versions	Additional Details
Oracle	18c, 19c, 21c, and Oracle Cloud	
PostgreSQL	12.x, 13.x, 14.x, 15.x, and 16.x	You can also use PostgreSQL for Amazon RDS.
SQL Server	Microsoft SQL Server 2017, 2019, 2022, and 2025	You can also use Microsoft SQL Azure and Amazon RDS SQL Server.

Applications

Includes the following web-based components, erwin Mart Portal and erwin ER360 that helps you manage the Mart and manage, review, and govern data models through a web console respectively.

Web server

Hosts erwin Mart Portal and erwin ER360. By default, erwin Mart Portal installation process installs Apache Webserver.

Setting up erwin Mart Portal

When you access the Mart database through erwin Mart Portal for the first time, you must choose the database. You can choose the database using a database authenticated user or a Windows-authenticated user.

Before you proceed, verify that you have installed a DBMS, created the mart database, and configured Mart Portal. If the Mart is already initialized, the Login page appears.

Upon selecting the database, it is necessary to ensure that the database requirements are met. Next, proceed with the installation and initialization of the erwin Mart Portal and erwin ER360.

To install and configure erwin Mart Portal and erwin ER360, follow these steps:

1. [Review prerequisites](#)
2. [Configure database](#)
3. [Install erwin Mart Portal and erwin ER360](#)
4. [Configure erwin Mart Portal](#)
5. [Initialize erwin Mart Portal and erwin ER360](#)
6. [Log in to erwin Mart Portal and configure settings](#)
7. [Log in to erwin Mart Portal and configure settings](#)

Reviewing Prerequisites

You can use any of the following combinations to install erwin Data Modeler (erwin DM), the Mart database, and erwin Mart Portal:

- Install erwin DM, the Mart database, and erwin Mart Portal on the same computer.
- Install erwin DM, the Mart database, and erwin Mart Portal on different computers.
- Install erwin DM and the Mart database on one computer, and install erwin Mart Portal on a different computer.
- Install erwin DM on one computer, and install the Mart database and erwin Mart Portal on a different computer.

Refer to the following tables for minimum system requirements.

Parameter	Requirement	Additional Information
Hardware/Workstation	• VM or Dedicated Physical Server • Windows-based workstation • 100 GB of disk space or more as required to support your specific mart • Processor - 64-bit, minimum 4 cores • RAM: • Only erwin Mart Portal: 16 GB • Both erwin Mart Portal and erwin ER360: 32 GB 16 GB RAM is the basic configuration for erwin Mart Portal, and 32 GB RAM is the basic configuration for erwin Mart Portal and erwin ER360.	
Operating System	• Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 • Microsoft Windows Server 2025 • All current Microsoft Windows critical updates	
Database	• Microsoft SQL Server 2017, 2019, 2022, and 2025. You can also use Microsoft SQL Azure and Amazon RDS SQL Server. • Oracle 18c, 19c, 21c, and Oracle Cloud	SQL Server: • The Mart Portal can use a stan-

Review the Prerequisites

Parameter	Requirement	Additional Information
	• PostgreSQL 12.x, 13.x, 14.x, 15.x, 16.x, and 17.x. You can also use PostgreSQL for Amazon RDS. • For DM Connect for DI, the minimum SQL Server version requirement is SQL Server 2016 SP2	dalone or share an existing database server for a Microsoft SQL Server. • The SQL Server 2017, 2019, 2022, and 2025 TRUSTWORTHY database property is no longer required for the mart. After you install this product, you can optionally reset this property to OFF. • The database user account that is used to configure the Mart must have the db_owner role assigned. • (Optional) To use the Korean language, use the Korean_wansung_CI_AS character set. Select the character set while creating the Mart database (in the Collation field). For

Parameter	Requirement	Additional Information
		more information, see the SQL Server documentation. Oracle: • The Mart Portal can use a standalone or can share an existing database server for an Oracle database. You can also use a plugable database. • To create the Mart, you must be the database schema owner user and you must have the DBA role in the target database on the Oracle server. The DBA role is required for the user who is specified in the Configure Mart Portal dialog. If the DBA privilege of this user is revoked, then erwin DM users will not

Review the Prerequisites

Parameter	Requirement	Additional Information
		be able to save model changes to the Mart. • (Optional) You have modified the following parameters in the initialization file (InitSID.ora): Remote_OS_Authent=T OS_Authent_Prefix=TRUE • (Optional) To use the Korean language with the Mart database, use KO16MSWIN949 or AL32UTF8 character set depending on your operating system language pack. For more information, see the Oracle documentation. • If the Mart database is an Oracle database, the default tablespaces that were used

Review the Prerequisites

Parameter	Requirement	Additional Information
		for initializing any earlier release of r9 series Mart are available for the latest release. PostgreSQL: • The Mart Portal can use a standalone or can share an existing database server for PostgreSQL. • The database user account that is used to configure the Mart must have super user permissions.
erwin Mart Portal Web Client - Browser	Latest versions of the following browsers: • Microsoft Edge • Mozilla Firefox • Google Chrome • Apple Safari	
Web Client Workstation	• Processor - i3 or higher • RAM - 8 -16 GB • Minimum Free Space - 8 - 16 GB	
Web Server	Apache Server 2.4.65	
JDK	21.0.7	
MartPortal Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs:	The required RAM size ranges from 2 to 10 GB for all services.

Review the Prerequisites

Parameter	Requirement	Additional Information
	<pre>reg add "HKLM\SYSTEM\CurrentControlSet\Services\erwinMartPortal\Parameters" /v Application /d "\"%JRE_HOME%\bin\java.exe\" - Xms2048m -Xmx10240m -Dlogging.config=file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-portal.xml" -jar \"%C:\Program Files\erwin\Mart Portal\MartApp\MartPortal.jar\" /f</pre>	
ER360 Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs: <pre>reg add "HKLM\SYSTEM\CurrentControlSet\Services\erwinER360\Parameters" /v Application /d "\"%JRE_HOME%\bin\java.exe\" - Xms2048m -Xmx10240m -Dlogging.config=file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-er360.xml" -jar \"%C:\Program Files\erwin\Mart Portal\MartApp\ER360.jar\" /f</pre>	
Vault Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs: <pre>reg add "HKLM\SYSTEM\CurrentControlSet\Services\erwinVaultService\Parameters" /v Application /d "\"%JRE_HOME%\bin\java.exe\" - Xms2048m - Xmx10240m -Dlogging.config=file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-vaultservice.xml" -jar "%C:\Program Files\erwin\Mart Portal\MartApp\ vaultservice.jar\" /f</pre>	
Job Scheduler Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs: <pre>reg add "HKLM\SYSTEM\CurrentCon- trolSet\Ser- vices\erwinMartJobSchedulerService\Parameters" /v</pre>	

Review the Prerequisites

Parameter	Requirement	Additional Information
	<code>Application /d "%JRE_HOME%\bin\java.exe" -Xms2048m -Xmx10240m -Dlogging.config="file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-mart-jobschedulerservice.xml" -jar "C:\Program Files\erwin\Mart Portal\MartApp\MartJobScheduler.jar" /f</code>	
Search Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs: reg add "HKLM\SYSTEM\CurrentControlSet\Services\erwinSearchService\Parameters" /v Application /d "%JRE_HOME%\bin\java.exe" -Xms2048m -Xmx10240m -Dlogging.config="file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-searchservice.xml" -jar "C:\Program Files\erwin\Mart Portal\MartApp\search-service.jar" /f	
Cache Service	In the C:\Program Files\erwin\Mart Portal\create_service.cmd, update the RAM size setting to increase the RAM in MBs: reg add "HKLM\SYSTEM\CurrentControlSet\Services\erwinCacheService\Parameters" /v Application /d "%JRE_HOME%\bin\java.exe" -Xms2048m -Xmx10240m -Dlogging.config="file:C:\Program Files\erwin\Mart Portal\MartApp\config\log4j2-cacheservice.xml" -jar "C:\Program Files\erwin\Mart Portal\MartApp\cache-service.jar" /f	

Ensure that you always install erwin Mart Portal on Windows operating system.

Other requirements

Ensure that the following additional requirements are met:

Review the Prerequisites

- The DBMS is installed and prepared for creating the Mart Database.
- The Mart database is created. At least one user with administrator privileges is present. You have run the initial queries on the Oracle database. For more information about the initial queries, see the Implementation Guide.
- If you want to add Windows Group users as Mart users, you have the Active Directory Server details.

You can add Windows Group users as normal Mart users, but not as Mart administrators. A Mart administrator must be a server or Windows user.

Important disclaimer notice on all requirements:

1. The requirements that are mentioned previously define the minimum requirements which permit the application to run with reasonable performance based on a small business use case scenario. The actual requirements for an enterprise-wide use case based on larger models and configurations require significantly greater resources to obtain acceptable performance.
2. These requirements are based on actual physical hardware (no virtual environment) and the following assumptions:
 - Minimal to no network overhead (both the database and application servers are locally installed)
 - Vendor's default install of the current version of their software (with all current service or fix packs)
 - No other applications sharing the defined hardware configuration (for example, a clean machine)

Any other hardware/software configurations are acceptable as long as they provide the same (or better) performance characteristics identified.

Install a Mart or Upgrade a Mart?

Use the following guidelines to determine if you must install or upgrade Mart Portal:

- If you are new to erwin Data Modeler and have purchased the current version of Workgroup Edition, then install the current version of the Mart. Use the How to Install and Configure a Mart procedure that is appropriate for your Mart database.
- If you have any earlier release of r9 series Mart, then upgrade the Mart to the current version. Use the How to Upgrade any r9 Series Mart to the Current Version procedure to upgrade your Mart. The models that are created in any earlier release of r9 series are upgraded when a user connects to the current version Mart and opens the models.
- If you have an existing Mart and the version is r7.3 through r8.2.9, install the current version Mart. Use the How to Install and Configure a Mart procedure that is appropriate for your Mart database. After installing the Mart, use the Upgrade Mart utility to upgrade the Mart models from r7.3 through r8.2.9 to the current version.

Character Limitations

There is a limitation on the number of characters you can use for certain Mart Portal parameters. The following table gives information about such parameters:

Parameter/Field	Character Limitations
Username	450 (Server User, Windows User, and Group) Also, refer to the special character limitations below. For international OS (I18N), if the character set being used is Double byte Character Set (DBCS) then the character limit is 225.
Password	130
Email Address	130 Also, refer to the special character limitations below.
Profile Name	130
Profile Description	2000
Catalog Name	255
Catalog Description	4000

Apart from the above character limits, for username and email address, following are the permitted special characters:

Parameter/Field	Permitted Special Characters	
Username	Server User for Mart Portal: . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark), ` (back tick) Windows User for Mart Portal: \ (backslash), . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), #	Server User for ER360: . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark), ` (back tick), (pipe), { (flower brackets) Windows User for ER360: \ (backslash), . (dot), _ (underscore), - (hyphen), ~ (tilde), ^

Character Limitations

Parameter/Field	Permitted Special Characters	
	(hash), ! (exclamation mark), ` (back tick), (pipe), {}(flower brackets) Group User: . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark), + (plus), % (percent)	(carat), # (hash), ! (exclamation mark), ` (back tick), (pipe), {} (flower brackets)
Email Address	Server User for Mart Portal: @ (at sign), - (hyphen), % (percent), _ (underscore), + (plus), . (dot), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark) Windows User for Mart Portal: @ (at sign), % (percent), + (plus), . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark) Group User for Mart Portal: . (dot), - (hyphen), %(percentage), _ (underscore), +(plus), @(at the rate)	Server User for ER360: @ (at sign), - (hyphen), % (percent), _ (underscore), + (plus), . (dot), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark) Windows User for ER360: @ (at sign), % (percent), + (plus), . (dot), _ (underscore), - (hyphen), ~ (tilde), ^ (carat), # (hash), ! (exclamation mark) Group User for ER360: . (dot), - (hyphen), %(percentage), _ (underscore), +(plus), @(at the rate)

Mart Portal Version Validation

Starting with version 15.0, erwin Data Modeler (erwin DM) supports version validation, allowing connectivity with higher erwin Mart Portal 15.x versions.

erwin DM 15.x can connect to the same or higher erwin Mart Portal 15.x repository versions.

To maintain model integrity in shared environments, avoid using different erwin DM 15.x versions (for example, erwin DM 15.0 and 15.2) when connecting to the same erwin Mart Portal 15.x repository, as this can lead to inconsistencies or unexpected issues.

Configuring Database

Configure your DBMS environment before you can install and use erwin Mart Portal and erwin ER360.

- [Oracle](#)
- [PostgreSQL](#)
- [SQL Server](#)

Creating Oracle Database

Before installing and using the software, perform the following setup tasks in your DBMS environment:

1. Install the DBMS on the server where you plan to store the Mart.
2. Ensure that you can create tables, indexes, stored procedures, and public synonyms. For more information about memory and disk space requirements, see the system requirements for each DBMS (Microsoft SQL Server, PostgreSQL, and Oracle).
3. Create a database to use as the Mart. To use a pluggable database, refer to the [Use a Pluggable Database](#) topic.
4. Use the DBMS features to create or identify the required storage objects and the mart. The specific requirements vary depending on your DBMS type.

To create, update, or delete a Mart in erwin Data Modeler Workgroup Edition, you must be the database schema owner and have the DBA role.

Additional Tasks

The DBA and the system administrator responsible for installing the software on an Oracle database management system perform the following tasks.

Use graphical tools or SQL *Plus (all versions), SQL *DBA, or the Oracle Enterprise Management Console to perform these tasks. Some SQL commands are included where appropriate. The Data file paths, data file sizes, role names, and user names are included as examples only.

1. Check the SYSTEM tablespace.

The installation creates several stored procedures. All triggers, stored procedures, and packages are kept in the Oracle SYSTEM tablespace. The standard size of the SYSTEM tablespace assumes that you are not using procedural options, so you may need to expand the SYSTEM tablespace. If other Oracle applications are not using procedural code, then expand the SYSTEM tablespace to 32 MB. If other Oracle applications are using procedural code, expand the SYSTEM tablespace to at least 32 MB.

2. Check the Rollback Segment tablespace.

If your instance uses UNDO tablespace, do not create rollback segments.

Significant rollback space is required for installing and use. The rollback segments must be in their own separate tablespace, and each have at least 16 MB of available space. There

Creating Oracle Database

must be one rollback segment for every four concurrent users, with a maximum of 50 rollback segments. The available space must scale upward with increasing numbers of rollback segments. Finally, the rollback segment optimal parameter must be set to control rollback segment growth and space consumption.

For Steps 3, 4, and 5, use the Dictionary-managed tablespaces.

3. Create a data tablespace of at least 32 MB.

For example:

```
CREATE TABLESPACE MyMart
DATAFILE '/db01/oracle/rdbms9i/data/mymart.ora' SIZE 100M;
```

Or For Locally Managed extents:

```
CREATE TABLESPACE Mymart
DATAFILE '/db01/oracle/rdbms9i/data/mymart.ora' SIZE 100M
EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

4. Create an index tablespace of at least 32 MB.

For example:

```
CREATE TABLESPACE MMARTINDEX
DATAFILE '/db02/oracle/rdbms9i/data/mmartindex.ora' SIZE 75M;
```

Or For Locally Managed extents:

```
CREATE TABLESPACE MMARTINDEX
DATAFILE '/db02/oracle/rdbms9i/data/mmartindex.ora' SIZE 75M
EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

5. Create a temporary tablespace.

For example:

```
CREATE TEMPORARY TABLESPACE MMTEMP TEMPFILE '/db03/oracle/rdbms9i/data/mmarttemp.ora' SIZE 50M;
```

Or For Locally Managed extents:

```
CREATE TEMPORARY TABLESPACE MMTEMP TEMPFILE '/db03/oracle/rdbms9i/data/mmarttemp.ora' SIZE 50M
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1M;
```

For more details about tablespace creation syntax and options, refer to the appropriate Oracle documentation.

6. Create an Oracle user with DBA privileges for use by the erwin Data Modeler Workgroup Edition Installer or designated schema owner.

Assign the data tablespace as the default tablespace and the temporary tablespace as the temporary tablespace for this user.

For example:

```
CREATE USER STEVE IDENTIFIED BY STEVE

DEFAULT TABLESPACE MyMart

TEMPORARY TABLESPACE MMTEMP

QUOTA UNLIMITED ON MyMart

QUOTA UNLIMITED ON MMARTINDEX;

GRANT DBA TO STEVE;
```

7. Create the erwin Data Modeler Workgroup Edition Installer role.

The following example is the role that the Oracle user requires to install erwin Data Modeler Workgroup Edition.

```
CREATE ROLE MMINSTALL;
```

8. Grant the Oracle privileges to the Installer role.

The following example shows the Oracle privileges that the erwin Data Modeler Workgroup Edition Installer must install on Oracle. For the last command, log in as sys with the sysdba role in the user-name or the command will fail.

```
grant create sequence to MMINSTALL;

grant create table to MMINSTALL;

grant create view to MMINSTALL;

grant create materialized view to MMINSTALL;

grant drop public synonym to MMINSTALL;

grant create public synonym to MMINSTALL;

grant create procedure to MMINSTALL;

grant select on dba_data_files to MMINSTALL;
```

Creating Oracle Database

```
grant create session to MMINSTALL;
```

To use the database, an Oracle user needs only the create session privilege.

9. Select the erwin Data Modeler Workgroup Edition tablespaces and Installer role.

When prompted for tablespace and role information, select the Workgroup Edition data tablespace, the Workgroup Edition index tablespace, and the Workgroup Edition Installer role.

[▲ Back to Top](#)

Creating PostgreSQL Database

If you are a DBA or a system administrator responsible for installing the software on a PostgreSQL database management system, perform the following tasks:

Use a graphical user interface (GUI) tool, such as pgAdmin or a similar tool, to create the erwin Data Modeler Workgroup Edition database. If a GUI tool is not available, you can use SQL Shell to type in the appropriate commands manually.

Configure PostgreSQL:

You can configure PostgreSQL database to accept any IP address.

Follow these steps:

1. Set the IP address to 0.0.0.0/0
2. Select the server.
3. Click Tools, Server Configuration, pg_hba.conf. Alternately, you can find the file at C:\Program Files\PostgreSQL\<version>\data.
4. Double-click the last empty column.
5. Complete the following fields:

Type

host

Database

all

User

all

Ip_Address

0.0.0.0/0

Method

md5

6. Select Enable and click Ok.
7. Click Save.
8. Click Reload Server.

Creating PostgreSQL Database

The PostgreSQL database configuration is complete.

[!\[\]\(9ec46ccf39110b98e9de4be0362c59b6_img.jpg\) **Back to Top**](#)

Creating SQL Server Database

If you are a DBA or a system administrator responsible for installing the software on a Microsoft SQL Server database management system, perform the following tasks:

1. Use a graphical user interface (GUI) tool, ISQL (all versions), SQL Administrator, or Enterprise Manager to create the Mart database. If a GUI tool is not available, you can use ISQL to type in the appropriate commands manually.

Your database should meet the following criteria:

- The initial size of the database file should be set to 60 MB.
- The initial size of the transaction log file should be set to 50 MB.
- Set the maximum file size to unrestricted file growth for both files (recommended, but not required).
- Increase the Set Auto grow file by 10 percent (recommended, but not required).

The new database is *owned* by the user who created it.

Set the Truncate Log on Checkpoint option and have the server generate checkpoints frequently. By selecting this option, the log is emptied periodically and should not fill up and cause rollbacks.

For best performance ensure that separate devices are used to store the data and the transaction log.

2. Verify tempdb size.

Significant temporary space is required for installation and use. The temporary segments need at least 16 MB of available space. You should also increase available space as the number of concurrent users increase.

[▲ Back to Top](#)

Specify Use of Foreign Characters With Microsoft SQL Server

For Microsoft SQL Server modify your registry settings to have certain foreign language characters in your models recognized.

Follow these steps:

1. Click Run on the Start menu.
2. Enter *regedit*.

The Registry Editor opens.

3. Verify or add the following registry entry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\DB-Lib]

"AutoAnsiToOem"="ON"

"UseIntlSettings"="ON"

4. Click File, Exit.

Your configuration is set to recognize foreign language characters in your models.

▲ [Back to Top](#)

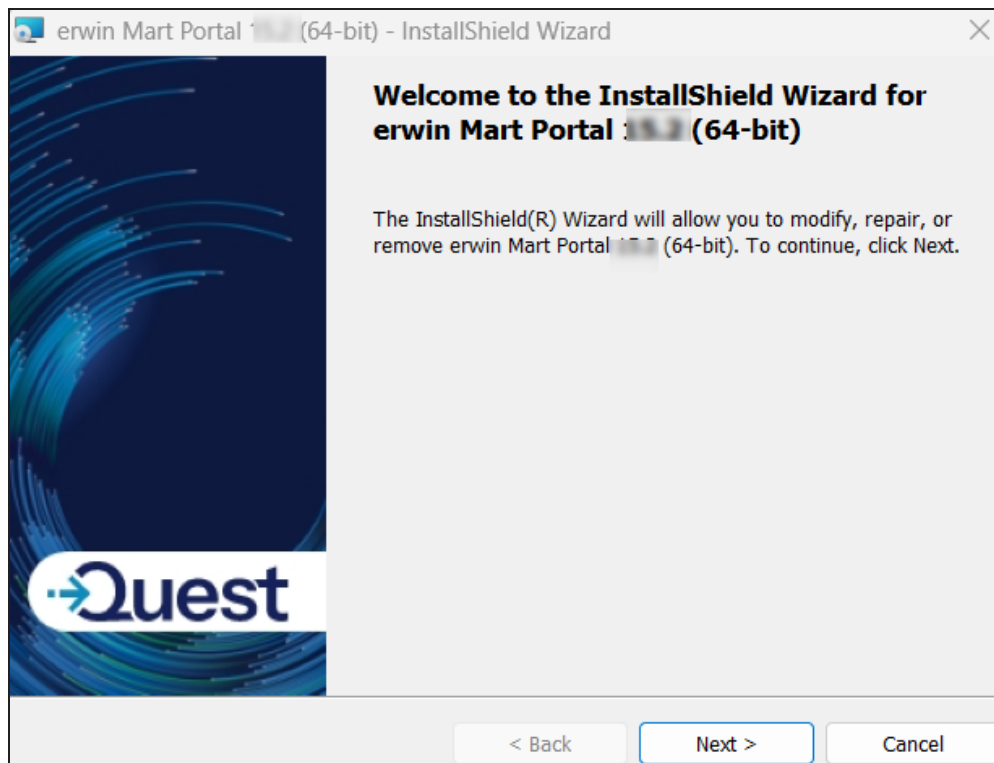
Installing erwin Mart Portal and erwin ER360

The erwin Mart Portal installer contains and installs three microservice JAR files, vaultservice.jar, MartPortal.jar, and ER360.jar. Along with mart, it also installs erwin ER360 by default. You can either use an existing web server or the default web server provided through the installation wizard.

You must install and configure erwin Mart Portal regardless of whether you use Mart Portal as a server or as a Windows service.

To install erwin Mart Portal and erwin ER360, follow these steps:

1. Download the erwin Mart Portal installer file from the [product page](#).
2. Start the installer.
The erwin Mart Portal Installation Wizard appears.



Install erwin Mart Portal

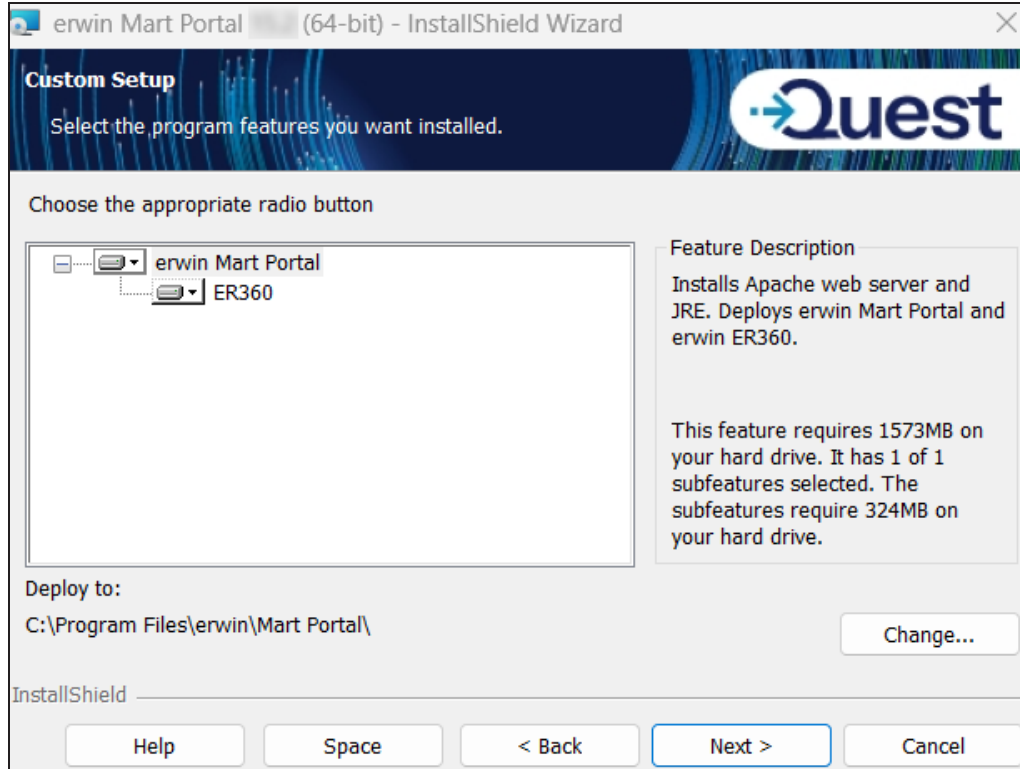
3. Click **Next** and accept the Software Transaction Agreement.

4. Click **Next** and enter your name and organization.

5. Click **Next**.

The applications and components list appears. Observe that under erwin Mart Portal, ER360 is available by default as a component.

Although erwin ER360 is installed by default, you need a license to use it. Contact your license administrator for a license.



6. Click **Next** and then click **Install**.

The installation process starts.

7. Once the installation process is completion, click **Finish** to exit the wizard.

Depending on the options you select, erwin Mart Portal and/or erwin ER360 are installed.

If you want to connect to an SSL enabled Mart through API, you must first install the security certificate on the corresponding computer. Install the certificate through erwin DM. Without the security certificate, the API cannot connect to the SSL enabled Mart.

Create a Pluggable Database

You can use the pluggable database concept in Oracle 12c and create multiple Marts of the same Mart release.

Follow these steps:

1. Create a pluggable database in Oracle 12c.

For example, provide the Global Database Name as erwin and the Pluggable Database Name as erwin_test.

For more information on how to create a pluggable database, see the Oracle documentation.

2. Run the following script on the computer where Oracle 12c is installed:

```
DROP TABLESPACE MMDATA INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;

DROP TABLESPACE MMINDEX INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;

DROP TABLESPACE marttemp INCLUDING CONTENTS AND DATAFILES CASCADE
CONSTRAINTS;

ALTER SESSION SET CONTAINER=erwin_test;

CREATE TABLESPACE MMDATA datafile 'c:\r9mart2\MMDATA.dbf' size 300m
autoextend on;

CREATE TABLESPACE MMINDEX datafile 'c:\r9mart2\MMINDEX.dbf' size 300m
autoextend on;

CREATE TEMPORARY TABLESPACE marttemp tempfile 'c:\r9-
mart2\tempdata.dbf' size 300m autoextend on;

DROP USER MMADMIN CASCADE;

CREATE USER MMADMIN IDENTIFIED BY MMADMIN DEFAULT TABLESPACE MMDATA
TEMPORARY TABLESPACE MARTTEMP QUOTA UNLIMITED ON MMDATA QUOTA
UNLIMITED ON MMINDEX;

DROP ROLE MMINSTALL;

CREATE ROLE MMINSTALL;
```

Create a Pluggable Database

```
GRANT CREATE SEQUENCE TO MMINSTALL;  
GRANT CREATE TABLE TO MMINSTALL;  
GRANT CREATE VIEW TO MMINSTALL;  
GRANT CREATE MATERIALIZED VIEW TO MMINSTALL;  
GRANT DROP PUBLIC SYNONYM TO MMINSTALL;  
GRANT CREATE PUBLIC SYNONYM TO MMINSTALL;  
GRANT CREATE PROCEDURE TO MMINSTALL;  
GRANT CREATE SESSION TO MMINSTALL;  
  
GRANT MMINSTALL TO MMADMIN;  
GRANT DBA TO MMADMIN;
```

Install erwin Mart Portal with a Pluggable Database

The procedure to install erwin Mart Portal for a pluggable database is same as the procedure for a normal database. This topic describes only those fields that need different values for a pluggable database. For more information on how to configure the erwin Mart Portal, see the Install erwin Mart Portal topic.

The following fields on the Configure the erwin Mart Portal dialog need different values:

Server Name

Specifies the name of the database server where you have installed the Mart database.
Enter the name of the computer where Oracle 12c is installed and the pluggable database erwin_test is created.

Database Name

Specifies the name of the pluggable Mart database. For example, erwin_test.

User Name

Specifies the user name to connect to the Mart database. Enter mmadmin or any other user account that you have created when you ran the script.

Password

Specifies the password to connect to the Mart database. Enter mmadmin or any other password that you have created when you ran the script.

Configuring erwin Mart Portal

The next step after installing erwin Mart Portal is to configure it using either of the two ways:

- [via erwin Mart Portal configuration](#)
- [via command line interface \(CLI\)](#)

Configuration via CLI is available from erwin Mart Portal 12.5.2 onwards.

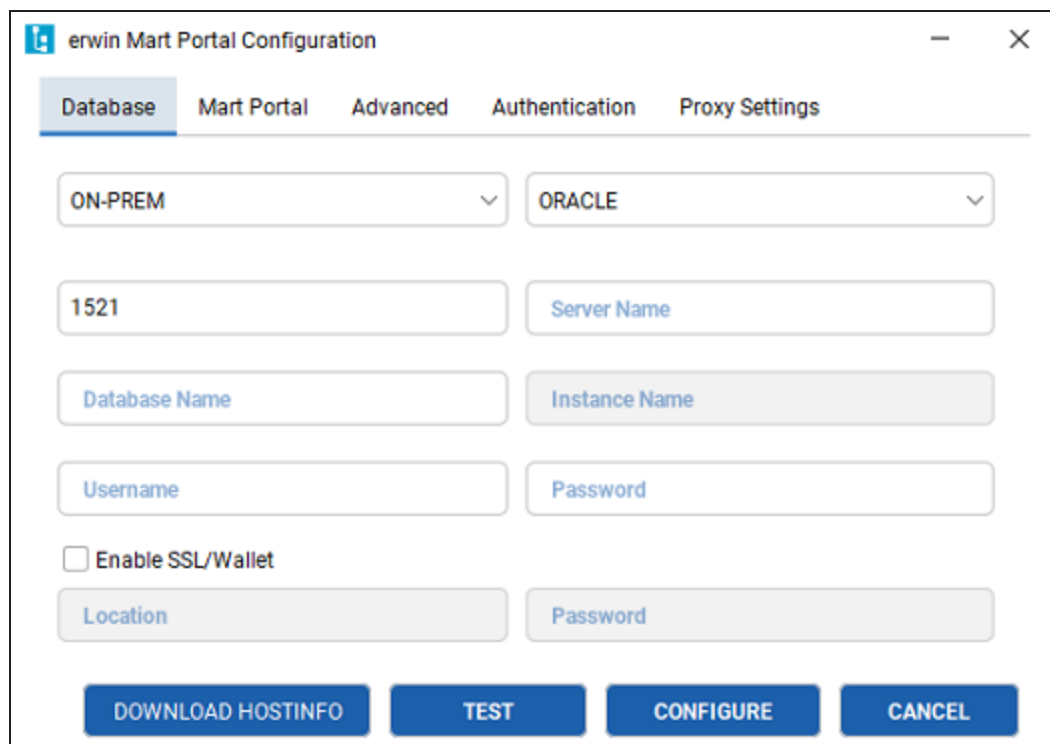
To use the same database that you have used for the r9.0.0 Mart (or any earlier release of r9 series Mart), upgrade your mart. Refer to the [Upgrading Mart](#) topic before proceeding.

Configuring via erwin Mart Portal Configuration

To configure erwin Mart Portal, follow these steps:

1. On the Windows Start menu, click **erwin > Configure Mart Portal**.

The erwin Mart Portal Configuration screen appears.



Configure the Mart Portal

2. [Configure database settings.](#)
3. [Configure mart portal settings.](#)
4. [Configure advanced settings.](#)
5. [Configure authentication settings.](#)
6. [Configure proxy settings](#) (only applicable to erwin ER360).
7. Click **Test** to validate the configuration.
8. On successful validation, click **Configure**.

Configuring Database Settings

On the Database tab, configure the following settings:

Field	Description	Additional Information
Database Connection Method	Specifies whether the mart connects to an on-premises database or to a database via a JDBC connection string.	
JDBC Connection String	Specifies the JDBC connection string to connect to a database	This option becomes available only when the Database Connection Type is set to Custom JDBC URL. For example: • For SQL Server Authentication: jdbc:sqlserver://localhost:1433; databaseName=MyDatabase; user=myUser;password=myPassword • For Windows Authentication: jdbc:sqlserver://localhost:1434; databaseName=MyDatabase; integratedSecurity=true;
Database	Specifies the mart database provider	Available options are: • Oracle • PostgreSQL

Configure the Mart Portal

Field	Description	Additional Information
		SQL Server
Port No	Specifies the port number of the database server	
Server Name	Specifies the name of the database server where you have installed the Mart database. For example, suppose that you are using SQL Server as the Mart database. Enter the name of the computer where SQL Server is installed.	
Database Name	Specifies the database to which the mart must connect	If you are installing the Mart for the first time, use a new database. Do not use an existing database. If you are upgrading the Mart from any earlier release of r9 series to the latest release, use the corresponding Mart database. For an Oracle mart, ensure that appropriate permissions for a materialized view are assigned to the installer role (GRANT CREATE MATERIALIZED VIEW TO MMINSTALL;). For more information, refer to the Creating Oracle Database topic.
Instance Name	Specifies the name of the database instance	Enabled only when the Database is set to SQLServer.
Authentication	Specifies whether user authentication is done via database or Windows authentication	Enabled only when the Database is set to SQLServer. Windows authentication works only for on premises SQL Server database.
Schema Name	Specifies the database schema that you want to use for mart	Enabled only when the Database is set to PostgreSQL. By default, it is set to use public schema.
Username	Specifies the user name to	This username must be is authenticated by the

Configure the Mart Portal

Field	Description	Additional Information
	connect to the Mart database	Mart database. Windows authentication (User Name field) is not supported for connecting to the Mart database from the Configure Mart Portal window. Ensure that the user is server authenticated.
Password	Specifies the password to connect to the Mart database	
Enable SSL/Wallet	Specifies whether SSL or Wallet (in case of Oracle database) is enabled	
Location	Specifies the location of the wallet file	Enabled only when you select the Enable SSL/Wallet check box.
Password (For SSL/Wallet)	Specifies the password that you set for the wallet	Enabled only when you select the Enable SSL/Wallet check box.
Download Hostinfo	Downloads the host machine's information for erwin ER360 offline license.	Downloads the following information in the JSON format. • OS Name • OS Version • Time Zone • System Locale • IP • System Type • NIC • Host Name • MAC • Input Locale The erwin licensing team uses this information to configure an offline license for erwin ER360. For more information on offline licenses, contact license support.

Configuring Mart Portal Settings

On the Mart Portal tab, configure the following settings:

The screenshot shows the 'erwin Mart Portal Configuration' dialog box with the 'Mart Portal' tab selected. The dialog has five tabs: Database, Mart Portal, Advanced, Authentication, and Proxy Settings. The Mart Portal tab contains the following fields and controls:

- A text field for 'localhost'.
- A text field for '18170'.
- A text field for 'MartServer'.
- A checkbox labeled 'Secure Sockets Layer(SSL) Enabled' which is unchecked.
- A disabled text field for 'SSL File Location'.
- A disabled text field for 'SSL Key File Location'.
- A text field for '300'.
- Four buttons at the bottom: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

On the Mart Portal tab, configure the following settings:

Field	Description	Additional Information
Server Name	Specifies the name of the computer where the Web Server is present. For example, if you are using Tomcat, enter the name of the computer where Tomcat is installed. Default: localhost	

Configure the Mart Portal

Field	Description	Additional Information
Port Number	Specifies the port number on which the Web Server is running.	You can now configure erwin Mart Portal on any port except 18172, 18174, and 18176 (These ports are used as proxy ports.). If you use SSO, ensure that you configure the correct port number here according to your SSO configuration. If you select the Secure Sockets Layer (SSL) Enabled check box, Port Number is set to 443 by default.
Secure Sockets Layer (SSL) Enabled	Specifies whether you want to connect to the Mart through a secured connection (SSL)	Using a self-signed SSL certificate may result in an error about certificate authority while connecting to erwin Mart. In that case, click OK to continue connecting to erwin Mart
SSL File Location	Specifies the location of SSL certificate file	Enabled only when the Secure Sockets Layer (SSL) Enabled option is selected. The certificate is available at C:\Program Files\erwin\Mart Portal\Apache\my-erwin.mart.crt.
SSL Key File Location	Specifies the location of the SSL Key file	Enabled only when the Secure Sockets Layer (SSL) Enabled option is selected. The key is available at C:\Program Files\erwin\Mart Portal\Apache\my-erwin.mart.key.
Account Lockout Duration (in seconds)	Specifies the duration (in seconds) for which an account should be locked whenever an incorrect password is entered five consecutive times	By default, it is set to five minutes (300 seconds). At the most, you can set it to 30 days (2592000 seconds).

Configuring Advanced Settings

The Advanced tab specifies mart upgrade settings.

Configure the Mart Portal

The screenshot shows the 'erwin Mart Portal Configuration' dialog box with the 'Advanced' tab selected. The dialog has four tabs: 'Database', 'Mart Portal', 'Advanced', 'Authentication', and 'Proxy Settings'. Under the 'Advanced' tab, there are five unchecked checkboxes: 'Rerun Count Upgrade', 'Rerun Report Upgrade', 'Rerun Report Upgrade For All Models', 'Update Mart Portal Path', and 'Update ER360 Path'. Below these are three text input fields containing the values '8', '64', and '14400'. A text box contains the instruction: 'Ensure that the mart database has the following: m9ReportUpgrade and m9ReportListData tables. m9Catalog with entcnt, attcnt, relcnt and countblob columns. For more information about the advanced tab kindly refer the documentation.' At the bottom are four buttons: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

erwin Mart Portal Configuration

Database Mart Portal **Advanced** Authentication Proxy Settings

☐ Rerun Count Upgrade

☐ Rerun Report Upgrade

☐ Rerun Report Upgrade For All Models

☐ Update Mart Portal Path

☐ Update ER360 Path

8

64

14400

Ensure that the mart database has the following: m9ReportUpgrade and m9ReportListData tables. m9Catalog with entcnt, attcnt, relcnt and countblob columns. For more information about the advanced tab kindly refer the documentation.

DOWNLOAD HOSTINFO TEST CONFIGURE CANCEL

In case of failures in upgrade, before you rerun the upgrade, on the Advanced tab, configure the following settings:

Field	Description	Additional Information
Rerun Count Upgrade	Specifies that the model count upgrade should run while running the Mart database upgrade	
Rerun Report Upgrade	Specifies that the report upgrade should run while running the Mart	

Configure the Mart Portal

Field	Description	Additional Information
	database upgrade	
Rerun Report Upgrade For All Models	Specifies that the report upgrade should run for all models while running the Mart database upgrade	
Update Mart Portal Path	Specifies that the Mart Portal catalog path should run for all models while running the Mart database upgrade	This option updates the root path for each catalog in Mart. Accurate paths are required to validate user permissions for accessing catalogs, models, and libraries. Use on installation, upgrading, or when permissions do not apply as expected.
Update ER360 Path	Specifies that the ER360 catalog path should run for all models while running the Mart database upgrade	This option updates the root path for each catalog in ER360. Accurate paths are required to validate user permissions for accessing catalogs, models, and libraries. Use on installation, upgrading, or when permissions do not apply as expected.
Database Initial Size	Specifies the initial mart database size in MB By default, this is set to 8 MB	
Database Max Size	Specifies the maximum size the mart database can take in MB By default, this is set to 64 MB	
Rest API Token Lifetime(in seconds)	Specifies the duration (in seconds) for which your REST API token will be valid By default, this is set to 14400 seconds (four hours)	

Configure the Mart Portal

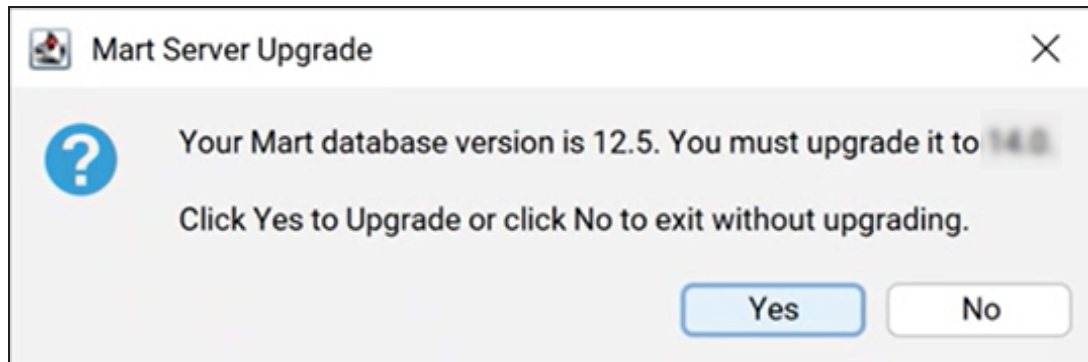
Ensure that the Mart database has the following:

- m9reportUpgrade and m9ReportListData tables
- m9Catalog table with entcnt, attcnt, relcnt, and countblob columns

To upgrade Mart, for example from 12.5 to the latest version follow these steps:

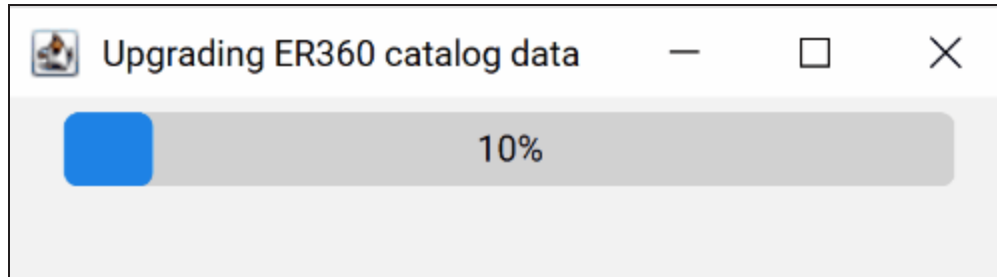
1. Click **Configure**.

The Mart Server Upgrade dialog box appears.



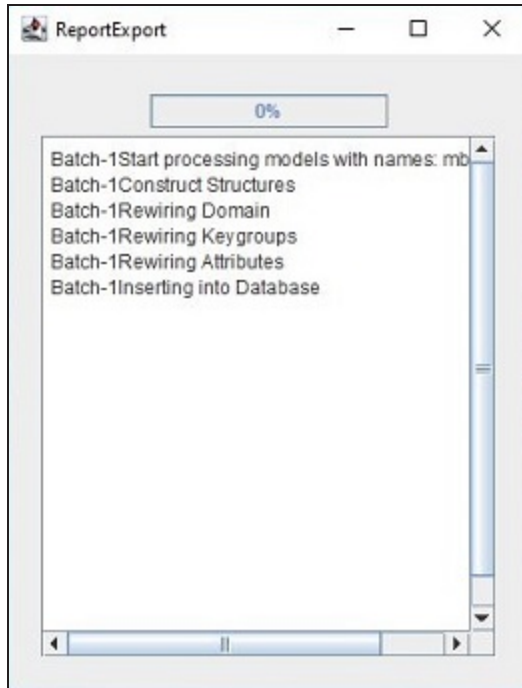
2. Click **Yes**.

The ER360 catalog data screen for count info appears.



Once the count upgrade process is complete, the ReportExport screen appears.

Configure the Mart Portal



This screen does not appear when you upgrade from 2020 R1 Mart to higher versions or when you upgrade for the first time.

On completion of report export process, the upgrade process is complete.

Configuring Authentication Settings

The Authentication tab specifies user account authentication settings for erwin Mart Portal and erwin ER360. The available settings differ based on the selected authentication method. Also, the type of users you can add to erwin Mart Portal differs based on the selected authentication method. For more information on adding users, refer to the [Manage Users](#) topic.

Configure the Mart Portal

erwin Mart Portal Configuration

Database

Mart Portal

Advanced

Authentication

Proxy Settings

SERVER

MartCloudServer

DOWNLOAD HOSTINFO

TEST

CONFIGURE

CANCEL

On the Authentication tab, configure the following settings:

Authentication Method	Field	Description	Additional Information
Server		Specifies that authentication is server-based	
Active Directory Details	Domain Title	Specifies the title of domain to be used in the AD list	You can add up to 10 domains to the list. Enter domain information and click Add Domain. As a best practice, add only those domains that you use in mart. Do not add all your domains.

Configure the Mart Portal

Authentication Method	Field	Description	Additional Information
	Domain Base	Specifies comma separated domain base specification for search. For example, CN=Users,DC=erwin,DC=com Here, <i>cn-users,dc=erwin,dc=com</i> is the distinguished-name. The distinguished name is the full path of the object.	
	Domain Server Name	Specifies server name or the IP address of the server	
	Domain Server Port	Specifies the port number to which the server listens	
	Domain user name	Specifies the domain name and user name in the <domain name>/<user name> format	
	Domain user password	Specifies the password of the domain user	
	Use SSL	Specifies whether you want to connect to the Mart through a secured connection (SSL)	
	Save password	Specifies whether you want to save domain user password	

Configure the Mart Portal

Authentication Method	Field	Description	Additional Information
Entra ID (OAuth2)	Tenant Id	Specifies your Entra ID environment properties for connection	Configure these settings based on your provider and the protocol. For more information on configuring Entra ID OAuth on Microsoft, refer to the Entra ID OAuth2 topic.
	Graph Scope		
	Client Id		
	Client Uri		
	Client Secret		
SAML (SAML 2.0)	Metadata XML method	Specifies your SAML environment properties for connection	erwin Mart Portal is certified for SAML with: • Entra ID • PingIdentity • Okta • WSO2 You can also use any other SAML supported identity provider. To use any of these identity providers, ensure that you do the following: - On the Mart Portal tab, set up Secure Sockets Layer (SSL), SSL Certificate, and SSL Key. - On the Authentication tab, click Download SP Metadata and upload the metadata XML file to your provider's portal. Then, configure these settings based on your provider and the protocol.

Configure the Mart Portal

Authentication Method	Field	Description	Additional Information
	Metadata XML		If switching authentication from LDAP to SAML, remove all LDAP-based user groups. Any remaining user groups will convert to the SAML user type after the change.
	Group Attribute Name		
	User Email Attribute Name		
	User Display Name Attribute Name		
	User Display Name Attribute Name		
	Download SP Metadata	Downloads the service provider metadata file that is required for your SSO setup	

Based on your configuration here, the available options to add users in erwin Mart Portal change.

Configuring Proxy Settings

The Proxy Settings tab is applicable only to erwin ER360 and specifies proxy server settings.

Configure the Mart Portal

erwin Mart Portal Configuration

Database

Mart Portal

Advanced

Authentication

Proxy Settings

☐ Enable Proxy

Proxy server address (DNS/IP Address)

Proxy server port number (eg. 3128)

Proxy username (optional)

Proxy password (optional)

DOWNLOAD HOSTINFO

TEST

CONFIGURE

CANCEL

On the Proxy Settings tab, configure the following settings:

Field	Description	Additional Information
Enable Proxy	Specifies that a proxy server should be used for erwin ER360 configuration	
Proxy server address (DNS/IP Address)	Specifies the proxy server's address, either DNS or an IP address	
Proxy server port number	Specifies the port number on the proxy server that you want to use	
Proxy username	Specifies the proxy server credentials	
Proxy password		

Configuring via CLI

To configure erwin Mart Portal via CLI, open command line interface and run following commands, for example, for Oracle:

```
>cd C:\Program Files\erwin\Mart Portal\MartUpgrade
>SET PATH = %JRE_HOME%\bin
>java -jar ./MartConfiguration.jar configure
--conntype=ON-PREM
--dbname=orcl
--dbport=1521
--dbpwd=mmadmin
--dbserver=localhost
--dbssl=false
--dbtype=ORACLE
--dbuser=mmadmin
--dbschemaname=public
--walletlocation=
--walletpwd=
--adminport=8081
--iisport=80
--locktime=300
--martappname=MartServer
--martserverhost=localhost
--martuseiis=false
--martusessl=true
--sslfilelocation="C:\Program Files\erwin\Mart Portal\Apache\myerwin.mart.crt"
--sslkeyfilelocation="C:\Program Files\erwin\Mart Portal\Apache\my-
erwin.mart.key"
--authorizationType=LDAP
--dcname="ldap://10.250.28.4:389/DC=quest,DC=com"
--domainuser=quest\sysadm
--domainpwd=Erwin12345
```

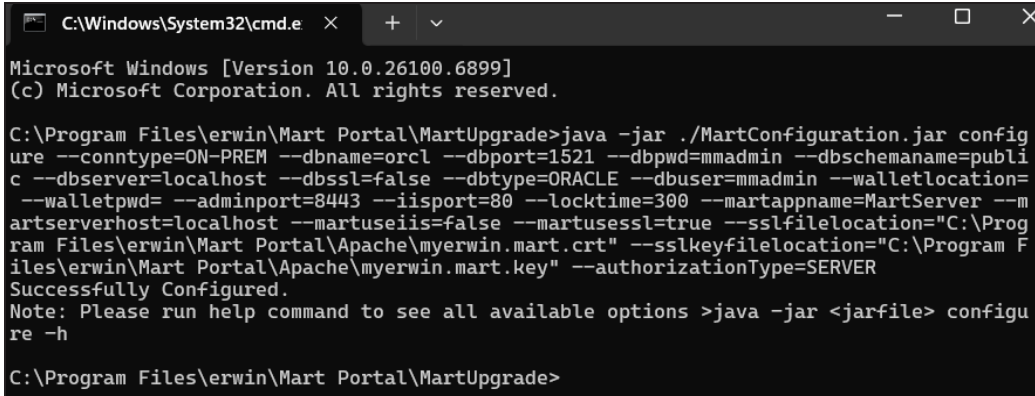
For example, to configure erwin Mart Portal with Oracle database, follow these steps:

1. Open command line interface and navigate to C:\Program Files\erwin\Mart Portal\MartUpgrade.
2. Run the following command:

```
java -jar ./MartConfiguration.jar configure --conntype=ON-PREM --
dbname=orcl --dbport=1521
--dbpwd=mmadmin --dbschemaname=public --dbserver=localhost --dbssl-
l=false
--dbtype=ORACLE --dbuser=mmadmin --walletlocation= --walletpwd=
--adminport=8443 --iisport=80 --locktime=300 --martappname=MartServer
```

Configure the Mart Portal

```
--martserverhost=localhost --martuseiis=false --martusessl=true  
--sslfilelocation="C:\Program Files\erwin\Mart Portal\Apache\my-  
erwin.mart.crt"  
--sslkeyfilelocation="C:\Program Files\erwin\Mart Portal\Apache\my-  
erwin.mart.key"  
--authorizationType=SERVER
```



```
C:\Windows\System32\cmd.e  X  +  v  
Microsoft Windows [Version 10.0.26100.6899]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Program Files\erwin\Mart Portal\MartUpgrade>java -jar ./MartConfiguration.jar config  
ure --conntype=ON-PREM --dbname=orcl --dbport=1521 --dbpwd=mmadmin --dbschemaname=publi  
c --dbserver=localhost --dbssl=false --dbtype=ORACLE --dbuser=mmadmin --walletlocation=  
--walletpwd= --adminport=8443 --iisport=80 --locktime=300 --martappname=MartServer --m  
artserverhost=localhost --martuseiis=false --martusessl=true --sslfilelocation="C:\Prog  
ram Files\erwin\Mart Portal\Apache\myerwin.mart.crt" --sslkeyfilelocation="C:\Program F  
iles\erwin\Mart Portal\Apache\myerwin.mart.key" --authorizationType=SERVER  
Successfully Configured.  
Note: Please run help command to see all available options >java -jar <jarfile> configu  
re -h  
  
C:\Program Files\erwin\Mart Portal\MartUpgrade>
```

Once done, this configuration is updated in configuration file, MartConfiguration.json, located at C:\ProgramData\erwin\Mart Portal. It is also available on the erwin Mart Portal Configuration screen.

Configure the Mart Portal

erwin Mart Portal Configuration

Database

Mart Portal

Advanced

Authentication

Proxy Settings

ON-PREM

ORACLE

1521

localhost

orcl

Instance Name

mmadmin

Password

☐ Enable SSL/Wallet

Location

Password

DOWNLOAD HOSTINFO

TEST

CONFIGURE

CANCEL

Configure the Mart Portal

erwin Mart Portal Configuration

Database Mart Portal Advanced Authentication Proxy Settings

localhost

8443

MartServer

☒ Secure Sockets Layer(SSL) Enabled

C:\Program Files\erwin\Mart Portal\Apache\myerwin.mart.crt

C:\Program Files\erwin\Mart Portal\Apache\myerwin.mart.key

300

DOWNLOAD HOSTINFO TEST CONFIGURE CANCEL

For the full list of commands, refer to the [erwin Mart Portal Configuration- CLI Commands](#) topic.

Configuring erwin Mart Portal- CLI Commands

Section	Command	Description
Database	--conntype=<conntype>	Provide ON-PREM or CUSTOM-JDBC-URL
	--dbinstance=<dbinstance>	Provide database instance name. [Required, if --conntype=ON-PREM]
	--dbname=<dbname>	Provide database name. [Required, if --conntype=ON-PREM]
	--dbport=<dbport>	Provide database port. [Required, if --conntype=ON-PREM]
	--dbpwd=<dbpwd>	Provide database password. [Required]
	--dbschemaname=<dbschemaname>	Provide database name. [Required, if --conntype=ON-PREM and database is Postgres]
	--dbserver=<dbserver>	Provide database server name. [Required, if --conntype=ON-PREM]
	--dbssl	Provide true or false. [default value is false]
	--dbtype=<dbtype>	Provide SQLSERVER or POSTGRESQL or ORACLE.
	--dbuser=<dbusername>	Provide database username. [Required]

Configuring erwin Mart Portal- CLI Commands

Section	Command	Description
	--jdbc_url=<jdbc_url>	Provide jdbc url. [Required, if --conntype=CUSTOM-JDBC-URL]
	--walletlocation=<walletlocation>	Provide wallet location path. [Required, if --dbssl=true][default value is empty]
	--walletpwd=<walletpwd>	Provide wallet password. [Required, if --dbssl=true] [default value is empty]
Mart Portal	--adminport=<adminport>	Provide port number. [default value is 80]
	--iisport=<iisport>	[default value is 80]
	--locktime=<locktime>	Provide locktime in seconds. [default value is 300]
	--martappname=<martappname>	[default value is MartServer]
	--martport=<martport>	
	--martserverhost=<martserverhost>	Provide mart portal hostname. [default value is localhost]
	--martuseiis	[default value is false]
	--martusessl	Provide true or false. [default value is false]
	--sslfilelocation=<sslfilelocation>	Provide SSL File Location. [default value is empty]
	--sslkey-filelocation=<sslkeyfilelocation>	Provide SSL Key File Location. [default value is empty]
Advanced	--dbinitialsize=<dbinitialsize>	Provide database initial size.

Section	Command	Description
		[default value is 8]
	--dbmaxsize=<dbmaxsize>	Provide database max size. [default value is 64]
	--docountupgrade	Provide true or false. [default value is false]
	--doreportupgrade	Provide true or false. [default value is false]
	--doreportupgradeforallmodels	Provide true or false. [default value is false]
	--domartpathupgrade	Provide true or false. [default value is false]
	--doer360pathupgrade	Provide true or false. [default value is false]
	--tokenvalidity=<tokenvalidity>	Provide token validity in secs. [default value is 14400]
Active Directory Options	--dcname=<dcname>	Provide domain controller name. [Required, if --authorizationType=LDAP/LDAPS]
	--domainpwd=<domainpwd>	Provide domain user password. [Required, if --authorizationType=LDAP/LDAPS]
	--domainuser=<domainuser>	Provide domain user name. [Required, if --authorizationType=LDAP/LDAPS]
Azure OAuth Options	--oauth2-provider-client-id=<oauth2_provider_client_id>	Provide oauth provider client id. [Required, if

Section	Command	Description
		--authorizationType=AZURE]
	--oauth2-provider-client-secret=<oauth2_provider_client_secret>	Provide oauth provider client secret. [Required, if --authorizationType=AZURE]
	--oauth2-provider-client-uri=<oauth2_provider_client_uri>	Provide oauth provider client uri. [Required, if --authorizationType=AZURE]
	--oauth2-provider-graph-scope-e=<oauth2_provider_graph_scope>	Provide oauth provider graph scope. [Required, if --authorizationType=AZURE]
	--oauth2-provider-tenant-id=<oauth2_provider_tenant_id>	Provide oauth provider tenant id. [Required, if --authorizationType=AZURE]
SAML Options	--saml-auth-request-signed=<saml_auth_request_signed>	Provide true or false. [default value is true]
	--saml-group-attribute-name=<saml_group_attribute_name>	Provide saml group attribute name. [Required, if --authorizationType=SAML]
	--saml-idp=<saml_idp>	Provide saml provider file path. [Required, if --authorizationType=SAML]
	--saml-user-email-attribute-name-e=<saml_user_email_attribute_name>	Provide saml user email attribute name. [Required, if --authorizationType=SAML]
Authentication	--authorizationType=<authorizationType>	Provide authorization type as SERVER or LDAP or LDAPS or AZURE or SAML. [default value is SERVER]
	--tempServerName=<tempServerName>	[default value is MartServer-Cloud]

Configuring erwin Mart Portal- CLI Commands

Section	Command	Description
Proxy Settings	--proxy-setting-hostName=<proxy_setting_hostname>	Provide proxy hostname. [Required, if --proxy-setting-isEnable=true]
	--proxy-setting-hostPort=<proxy_setting_hostPort>	Provide proxy port. [Required, if --proxy-setting-isEnable=true]
	--proxy-setting-isEnable=<proxy_setting_isEnable>	Provide true or false. [default value is false]
	--proxy-setting-password=<proxy_setting_password>	Provide proxy password. [default value is empty]
	--proxy-setting-username=<proxy_setting_username>	Provide proxy username. [default value is empty]
General Options	--clienthostname=<clienthostname>	[default value is erwinLocal]
	--console=<console>	
	--env-cloud=<env_cloud>	[default value is false]
	--wrapper-ip=<wrapper_ip>	[default value is empty]

Entra ID OAuth2

Based on your application type, refer to the appropriate section for Entra ID OAuth2 configuration:

- [erwin Mart Portal on-cloud](#)
- [erwin Mart Portal on-premises](#)

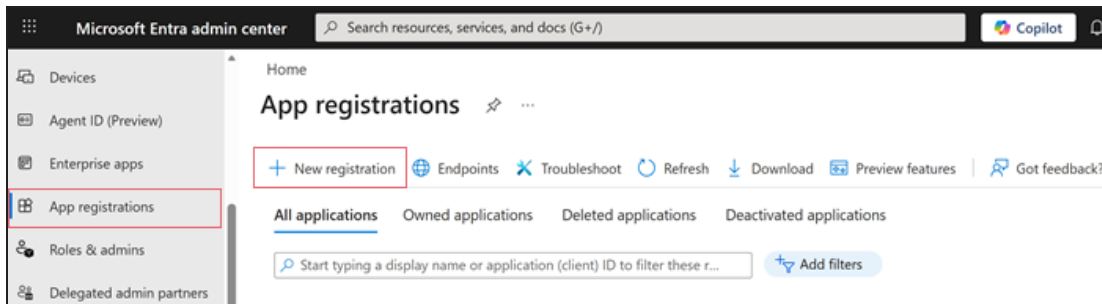
Once the Entra ID OAuth2 configuration is ready, you can add [users](#) and [groups](#) to erwin Mart Portal.

erwin Mart Portal On-Cloud

Before you configure Entra ID OAuth2, ensure that you have responded to the questionnaire from your Quest Support representative so that they can provide the Redirect URI for your instance. If you did not receive the questionnaire, reach out to your Quest Support representative.

To configure Entra ID OAuth2 for erwin Mart Portal on-cloud authentication, follow these steps:

1. Log in to the Microsoft Entra admin center and go to the App registrations page.



2. Click **New registration**. On the Register an application page, enter an appropriate name, supported account type, and the Redirect URI provided by Quest Support.

Home > App registrations

Register an application ...

*** Name**
The user-facing display name for this application (this can be changed later).

MartQuest ✓

Supported account types
Choose the account types that can use this application or access this API

Single tenant only - Contoso ✓ [Help me choose](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓ [http://localhost:3000/](#) ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

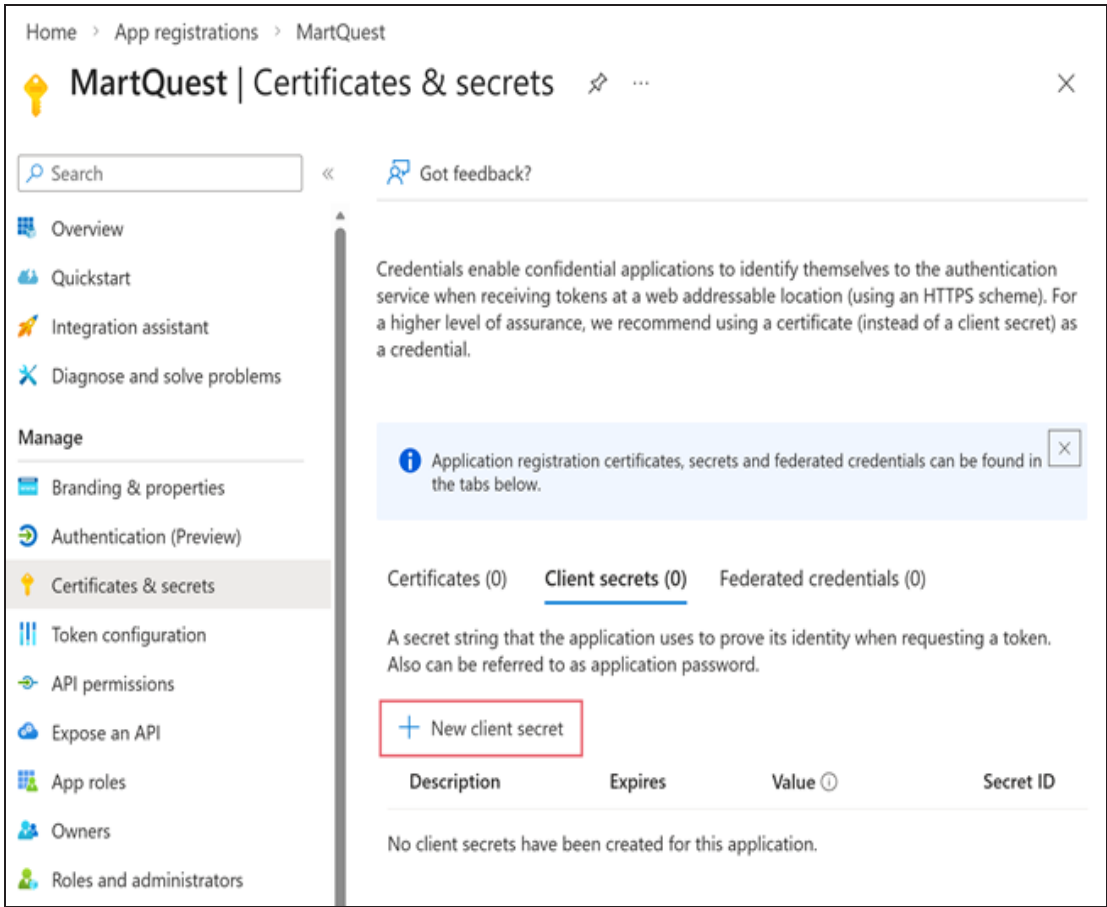
By proceeding, you agree to the [Microsoft Platform Policies](#) ↗

Register

The Contoso support account type is used for registration.

Adding the Redirect URI is optional at this stage and can be updated later.

3. Click **Register**.
4. Go to **Certificates & secrets**.



5. Click **New client secret**.

Home > App registrations > Ma

Add a client secret

Description:

Expires:

MartQuest | Certi

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

6. Enter a Description. Then, click **Add**.
7. Copy the auto-generated value highlighted in the following image.

Home > App registrations > MartQuest

MartQuest | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

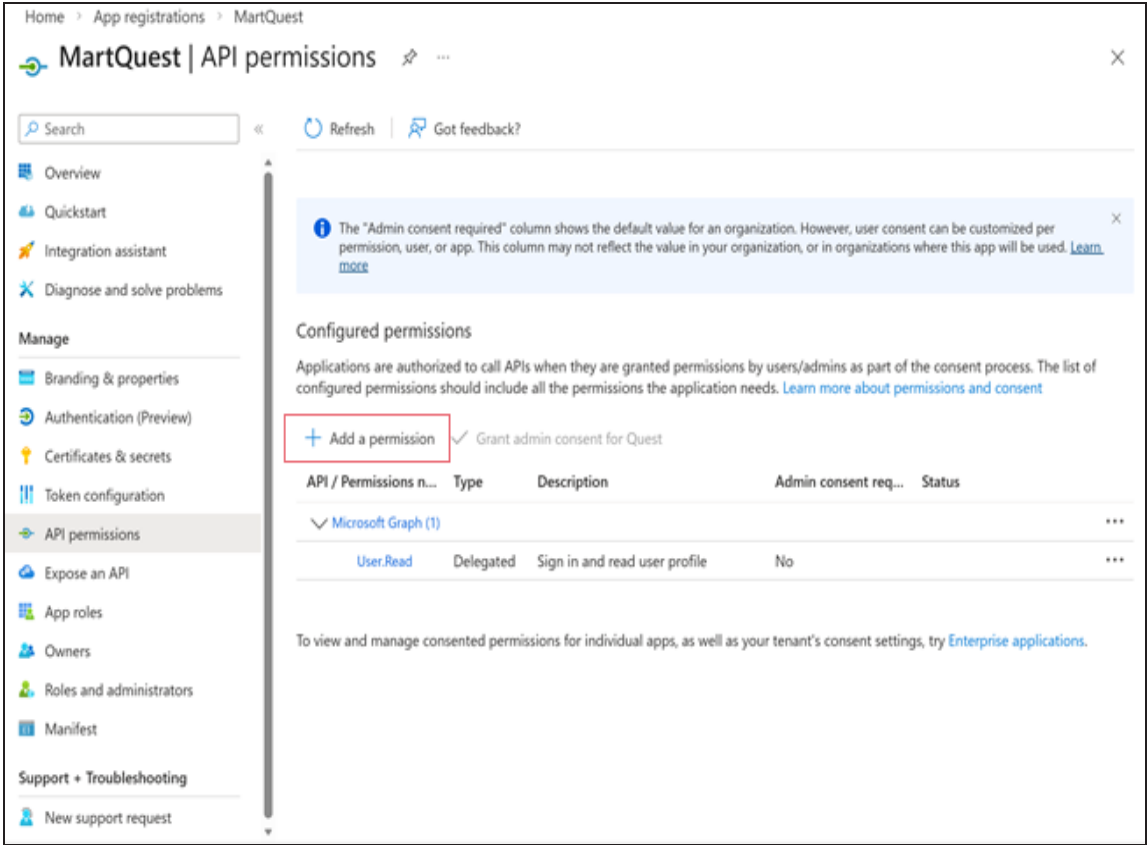
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

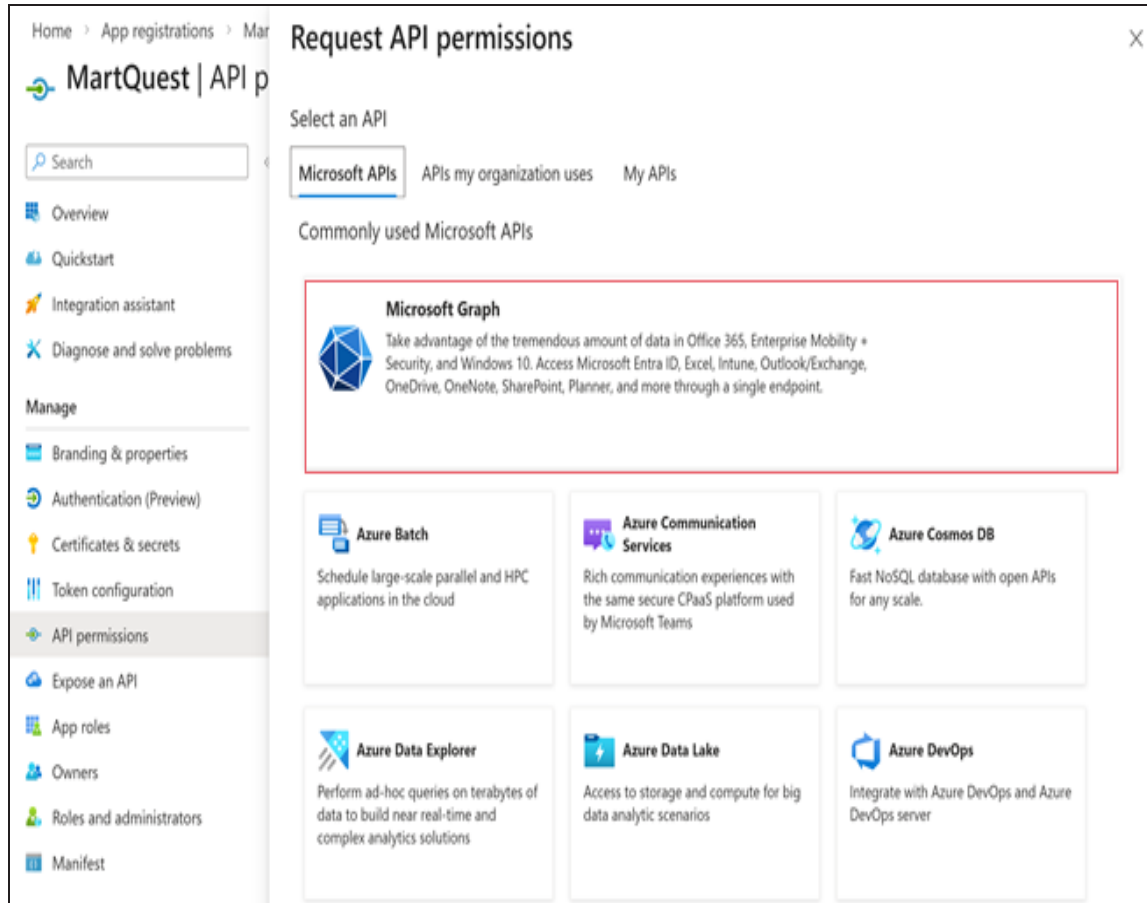
+ New client secret

Description	Expires	Value	Secret ID
Martsecretkey	9/13/2026	WYk8Q~3WH7TGNF...	284fe48d-3877-4faf-...

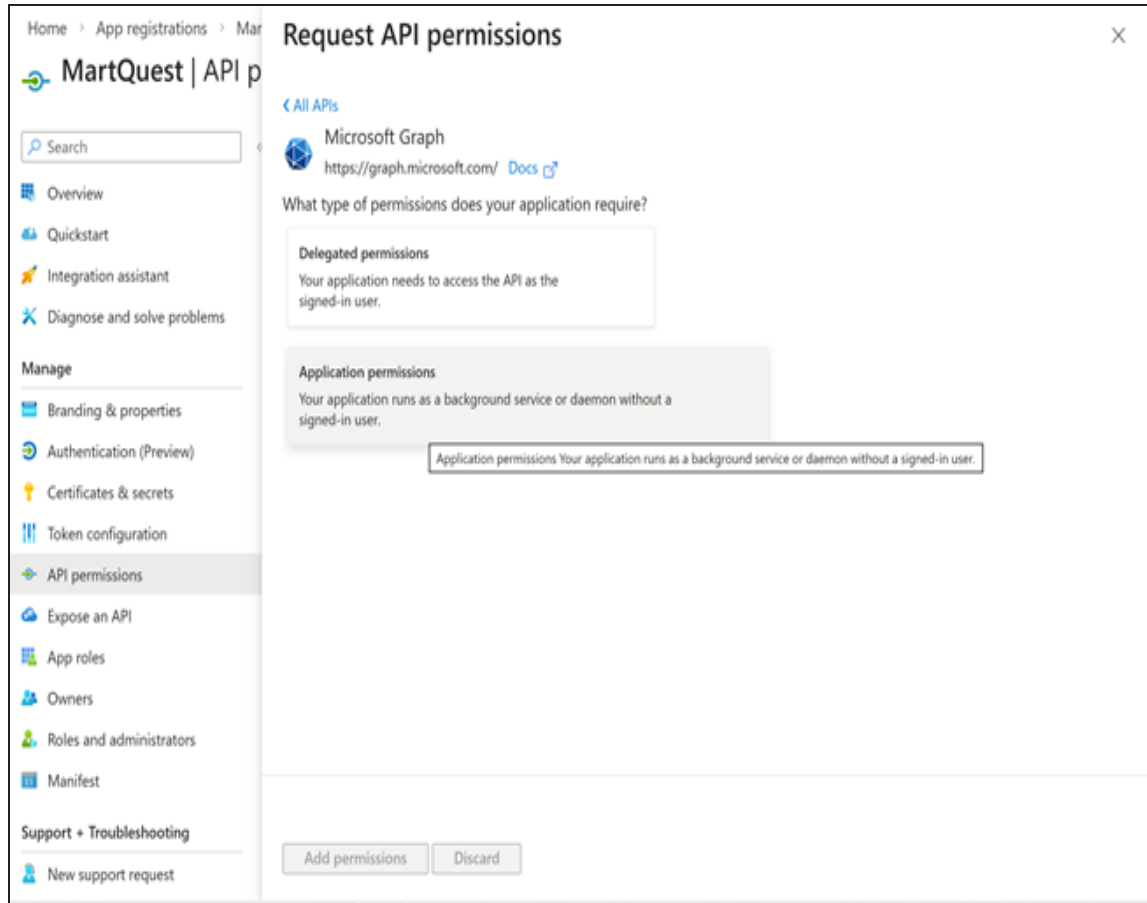
8. Go to **API permissions**.



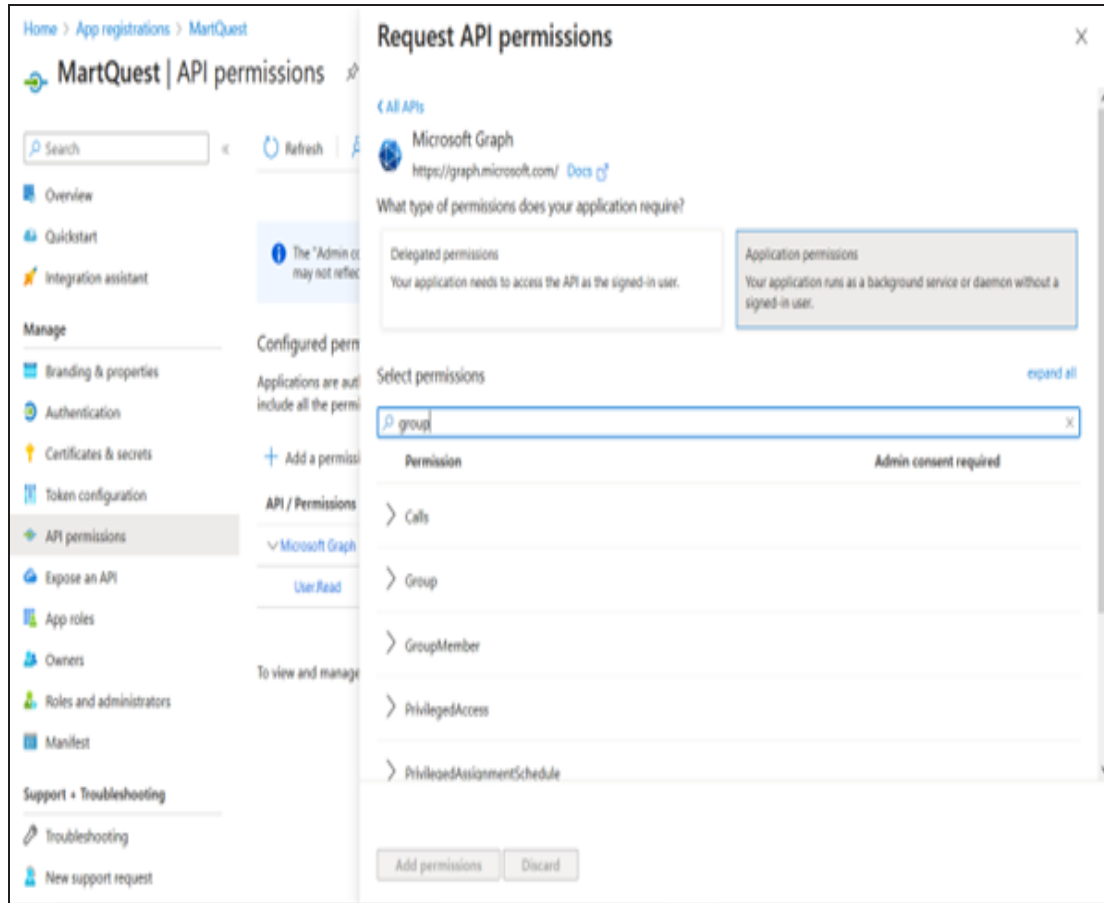
9. Click **Add a permission**.



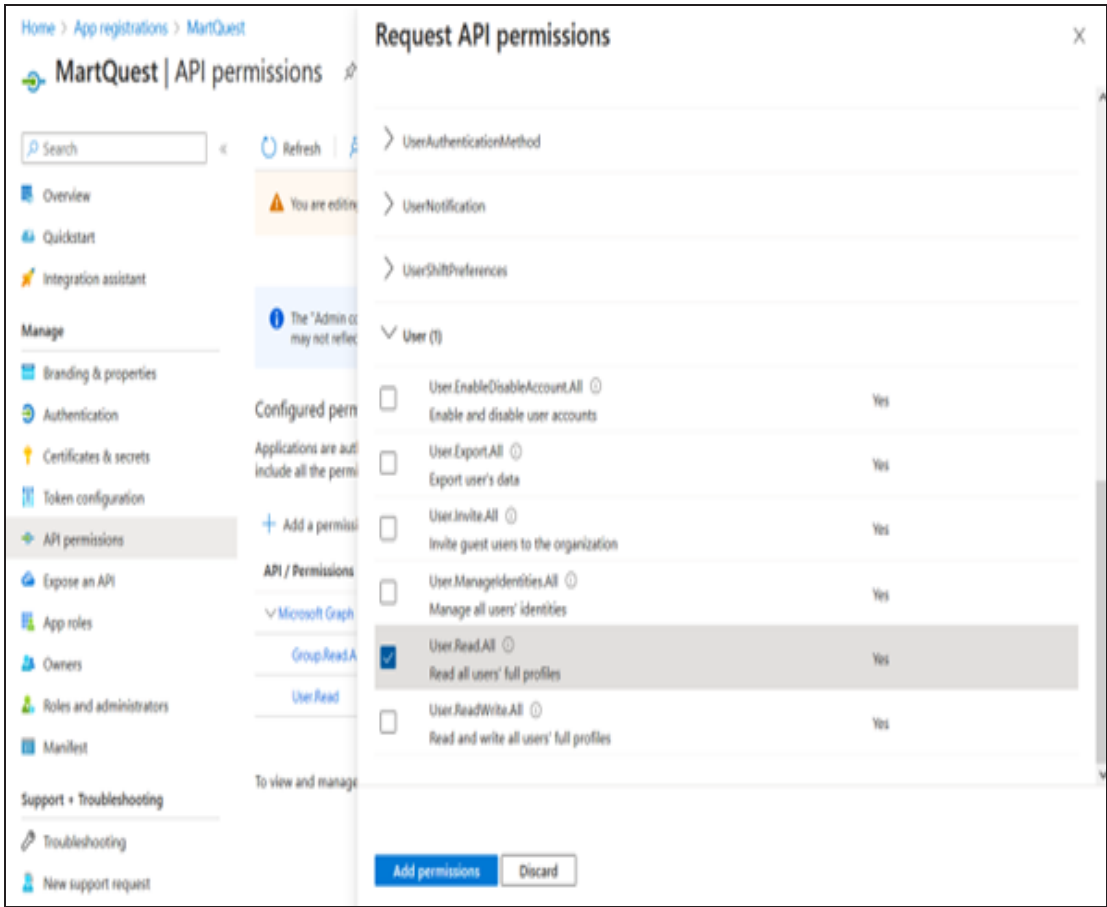
10. Click **Microsoft Graph**.



11. Select **Application permissions**.
12. Search and expand Group and select **Group.Read.All** permission. Then, click **Add permissions**.



13. Go to **Add a permission** > **Microsoft Graph** > **Application permissions** again. Search and expand **User** and select **User.Read.All** permission. Then, click **Add permissions**.



14. On the API permissions page, under the Configured permissions section, click **Grant admin consent for Contoso**.

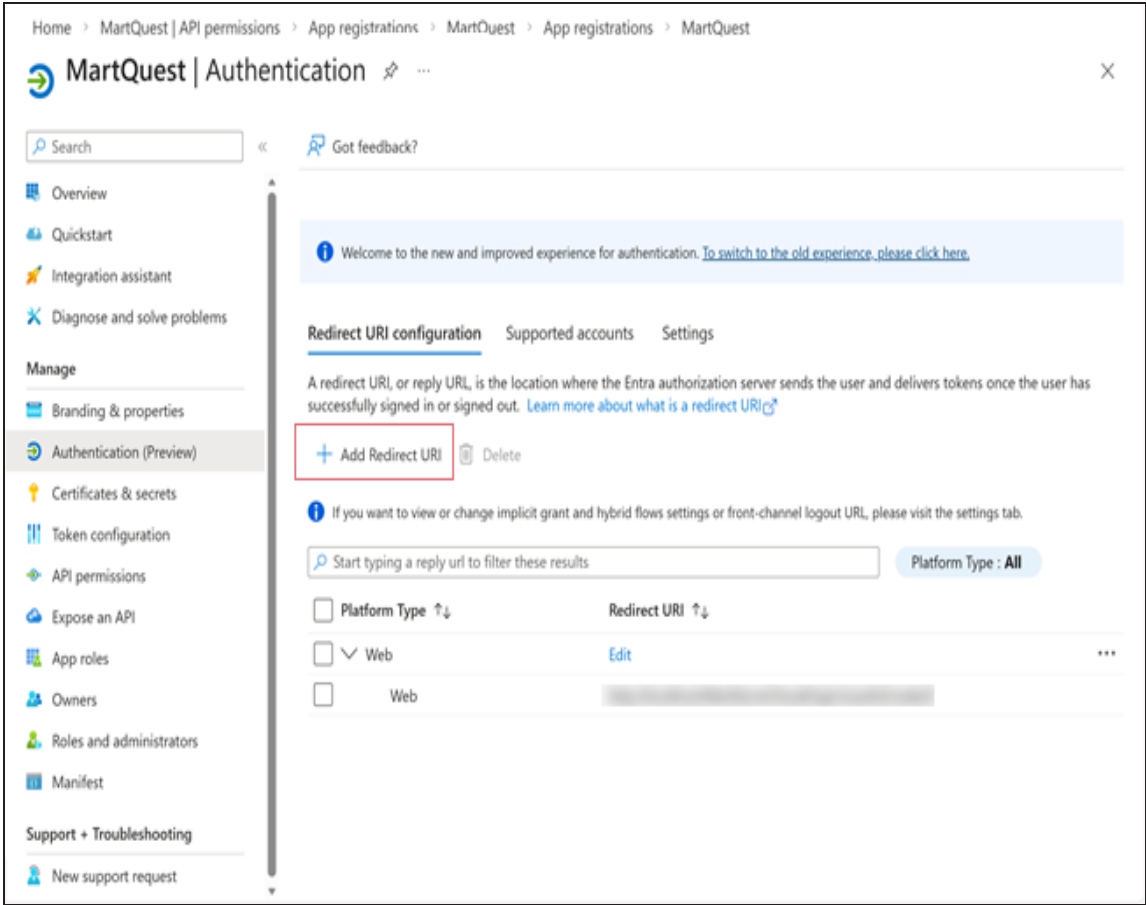
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions includes all the permissions the application needs. [Learn more about permissions and consent](#)

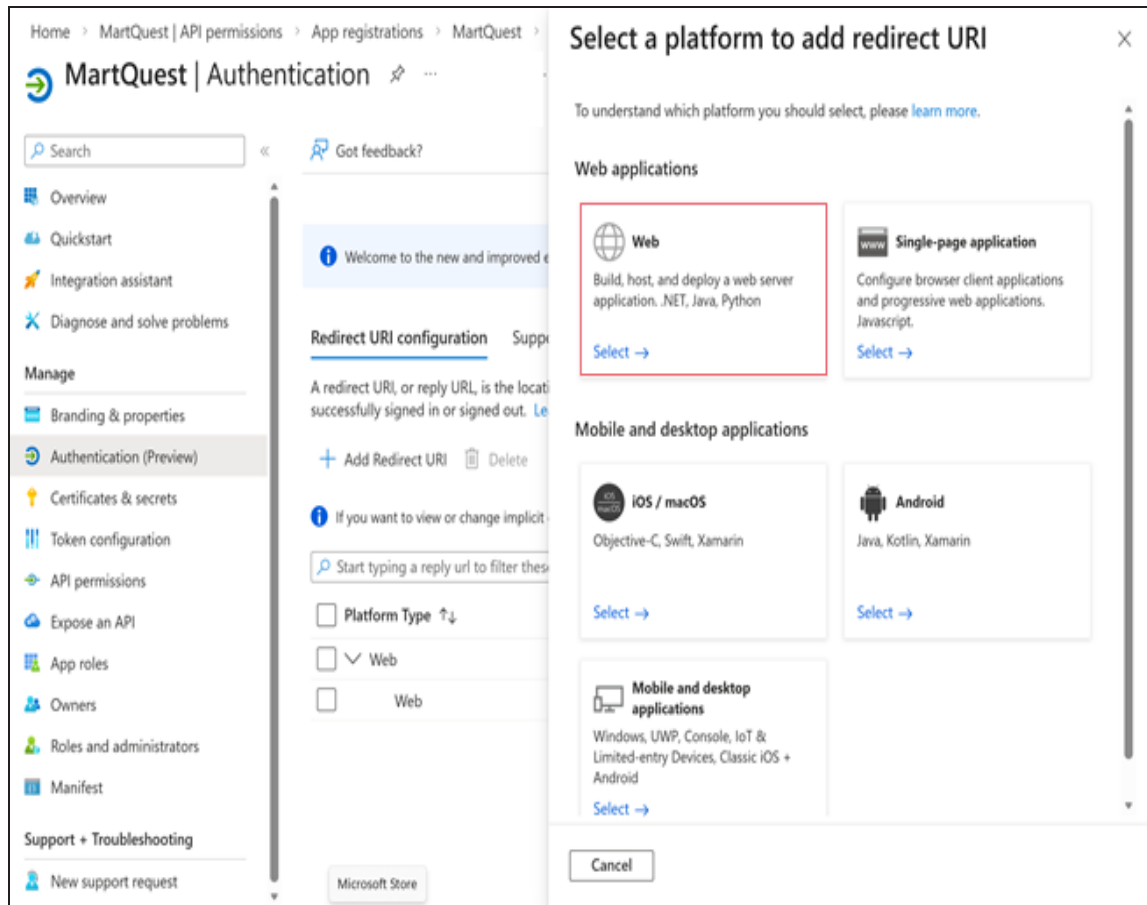
+ Add a permission ✓ Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (3)				...
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Contoso ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Contoso ...

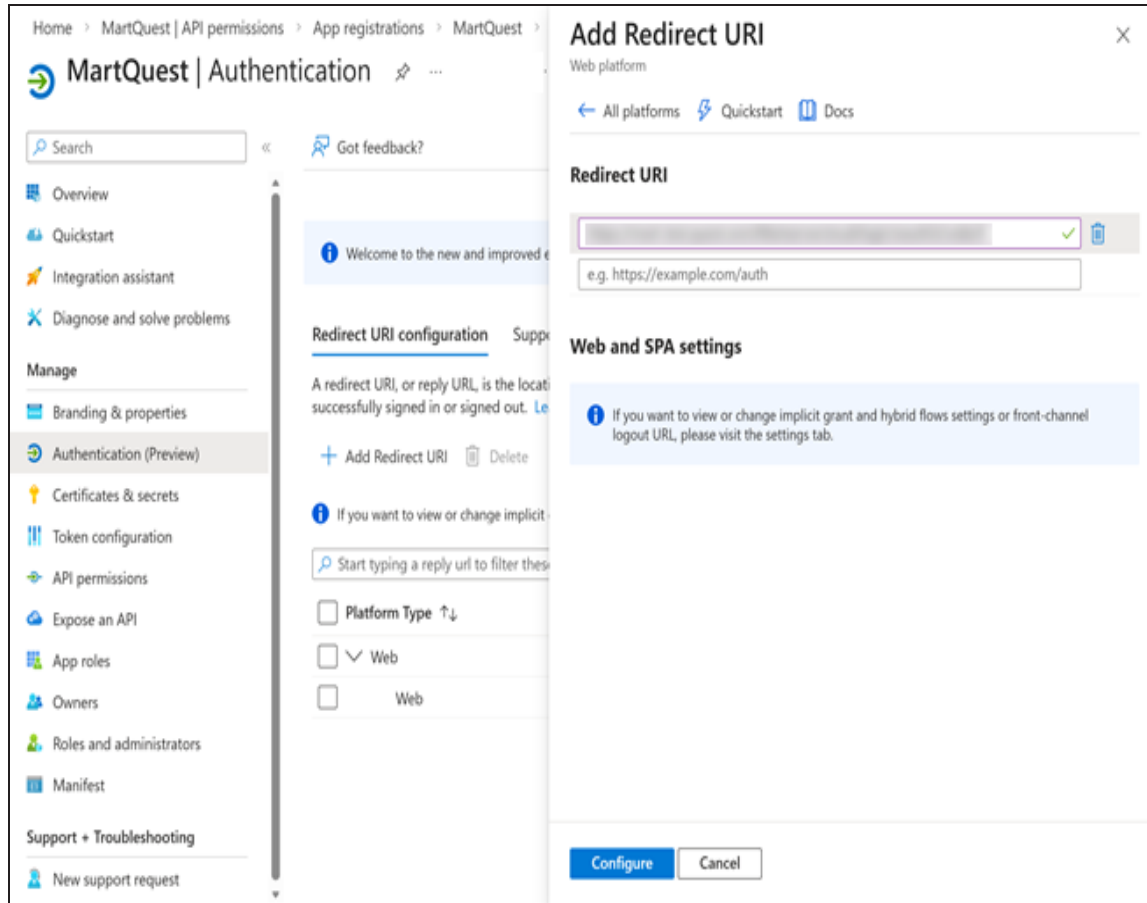
15. Go to the Authentication page and click **Add Redirect URI**.



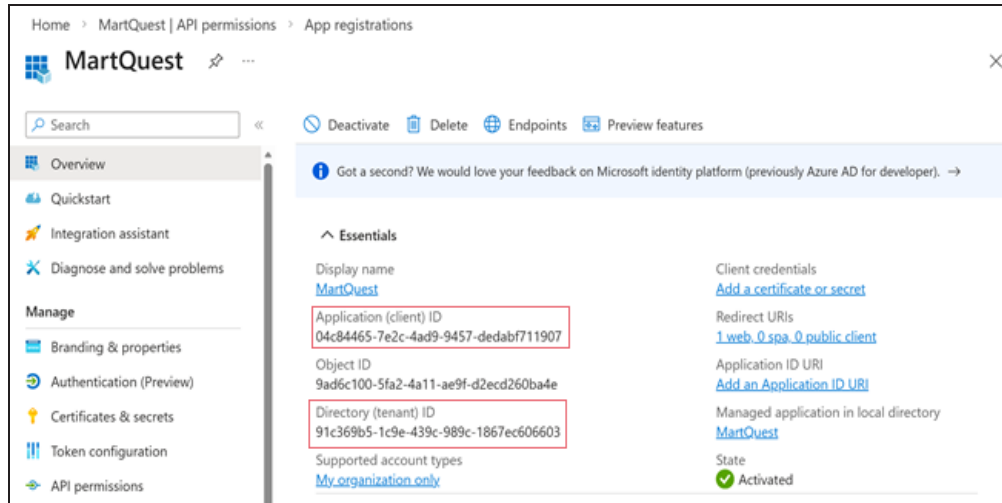
16. Click **Web**.



17. Enter the Redirect URI, and then click **Configure**.



18. Go to the Overview page and note the Application (client) ID and Directory (tenant) ID. Graph scope and Client URI are default.



19. Share the following details with the Mart Cloud Support team:

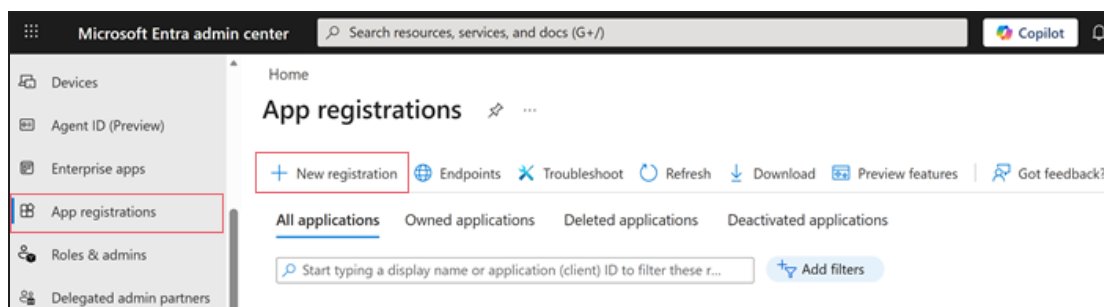
- **Tenant ID:** The Directory (tenant) ID copied in step 18.
- **Graph Scope:** The Microsoft Graph permission scope requested for acquiring an access token. For example, <https://graph.microsoft.com/.default>.
- **Client ID:** The Application (client) ID copied in step 18.
- **Client URI:** The base URI. For example, <https://login.microsoftonline.com/>
- **Client Secret:** The auto-generated value copied in step 7.

Once the support team authenticates erwin Mart Portal for you, you can move to [users](#) and [groups](#) in erwin Mart Portal at https://<your_instance>.myerwin.com/MartPortal.

erwin Mart Portal On-Premises

To configure Entra ID OAuth2 for erwin Mart Portal on-premises authentication, follow these steps:

1. Log in to the Microsoft Entra admin center and go to the App registrations page.



2. Click **New registration**. On the Register an application page, enter an appropriate name, supported account type, and the Redirect URI provided by Quest Support.

The screenshot shows the 'Register an application' page in the Microsoft Entra ID portal. The breadcrumb navigation at the top is 'Home > App registrations'. The page title is 'Register an application' with a three-dot menu icon to its right. The first section is labeled '* Name' and includes the instruction 'The user-facing display name for this application (this can be changed later)'. Below this is a text input field containing 'MartQuest' with a green checkmark icon on the right. The second section is 'Supported account types' with the instruction 'Choose the account types that can use this application or access this API'. It features a dropdown menu showing 'Single tenant only - Contoso' and a blue link 'Help me choose'. The third section is 'Redirect URI (optional)' with the instruction 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It includes a dropdown menu set to 'Web' and a text input field containing a placeholder URL with a green checkmark icon. Below these sections is a note: 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).' At the bottom, there is a link 'By proceeding, you agree to the Microsoft Platform Policies' with an external link icon, and a blue 'Register' button.

The Contoso support account type is used for registration.

Adding the Redirect URI is optional at this stage and can be updated later.

3. Click **Register**.
4. Go to **Certificates & secrets**.

The screenshot shows the 'Certificates & secrets' page for the 'MartQuest' application in the Microsoft Entra ID portal. The left-hand navigation pane includes links for Overview, Quickstart, Integration assistant, Diagnose and solve problems, and a 'Manage' section with options like Branding & properties, Authentication (Preview), Certificates & secrets (which is currently selected), Token configuration, API permissions, Expose an API, App roles, Owners, and Roles and administrators. The main content area has a breadcrumb 'Home > App registrations > MartQuest' and a title 'MartQuest | Certificates & secrets'. Below the title is a search bar and a 'Got feedback?' link. A descriptive paragraph explains that credentials enable confidential applications to identify themselves to the authentication service. A blue information box states that application registration certificates, secrets, and federated credentials can be found in the tabs below. There are three tabs: 'Certificates (0)', 'Client secrets (0)' (which is selected and underlined), and 'Federated credentials (0)'. A text block explains that a secret string is used by the application to prove its identity when requesting a token, also referred to as an application password. A red rectangle highlights a '+ New client secret' button. Below this is a table with headers: 'Description', 'Expires', 'Value' (with a help icon), and 'Secret ID'. The table content shows the message 'No client secrets have been created for this application.'

5. Click **New client secret**.

Home > App registrations > Ma

Add a client secret

Description:

Expires:

Add **Cancel**

MartQuest | Certi

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

6. Enter a Description. Then, click **Add**.
7. Copy the auto-generated value highlighted in the following image.

Home > App registrations > MartQuest

MartQuest | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

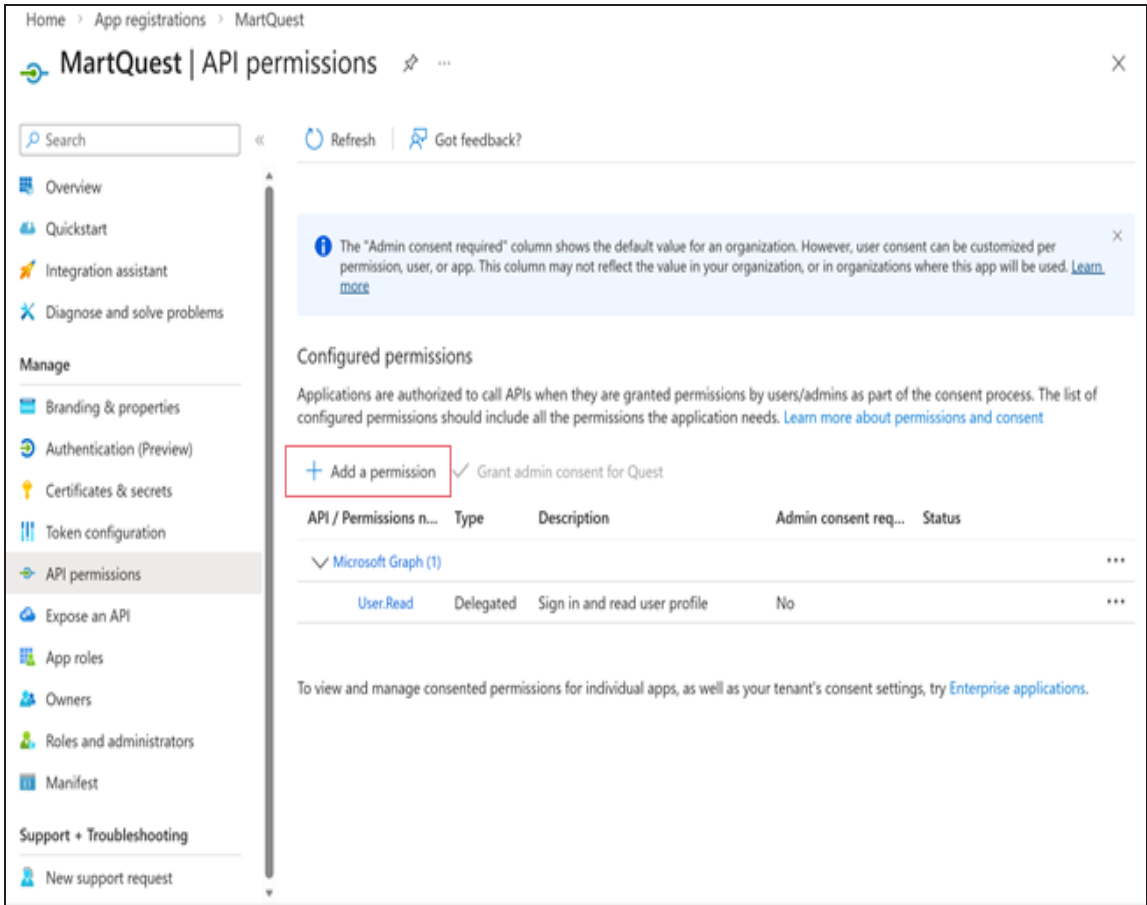
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

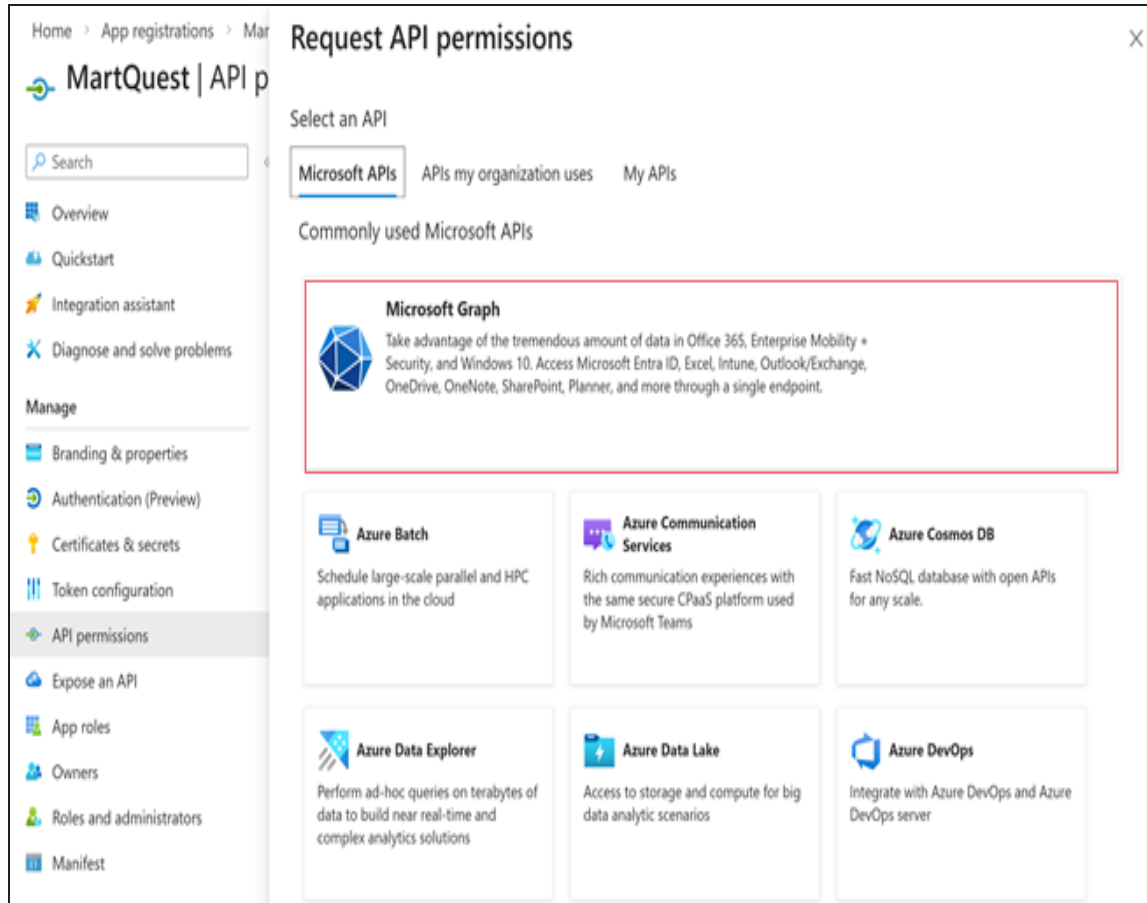
+ New client secret

Description	Expires	Value	Secret ID
Martsecretkey	9/13/2026	WYk8Q~3WH7TGNF...	284fe48d-3877-4faf-...

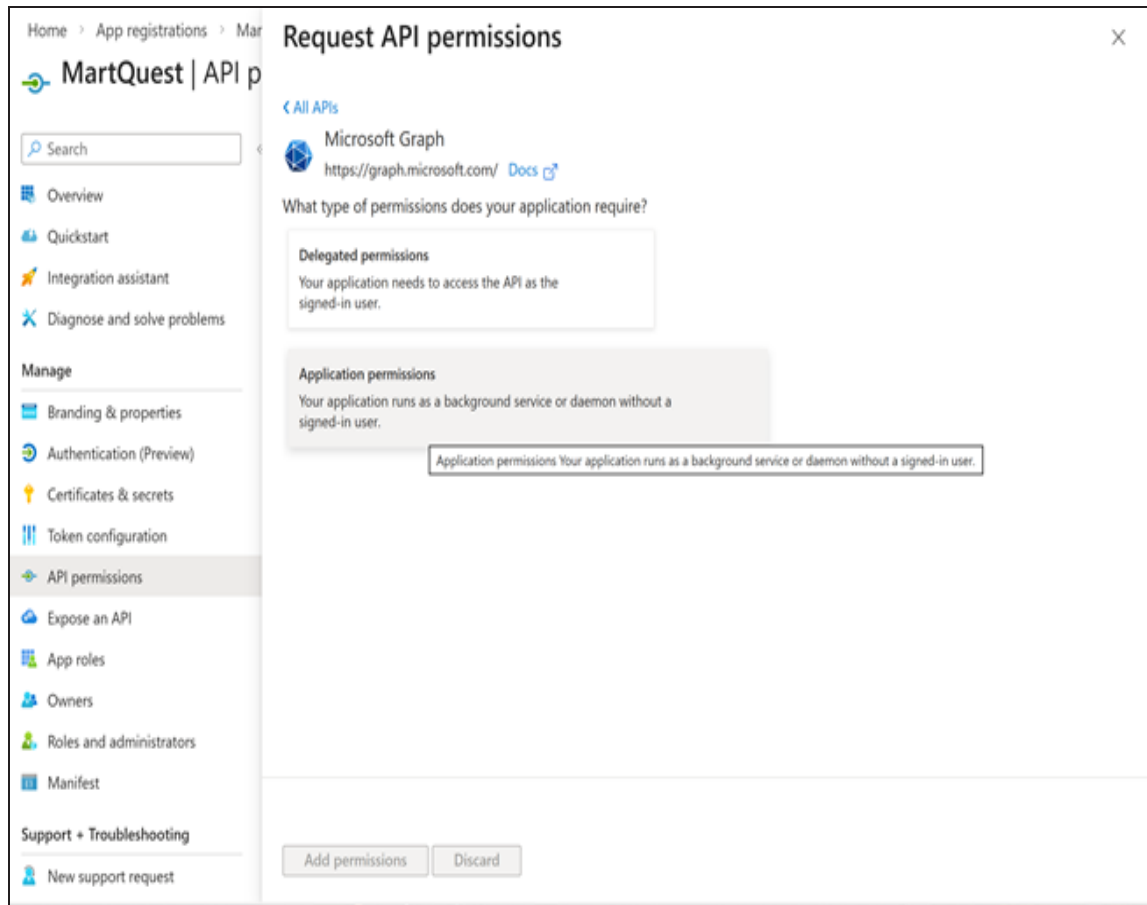
8. Go to **API permissions**.



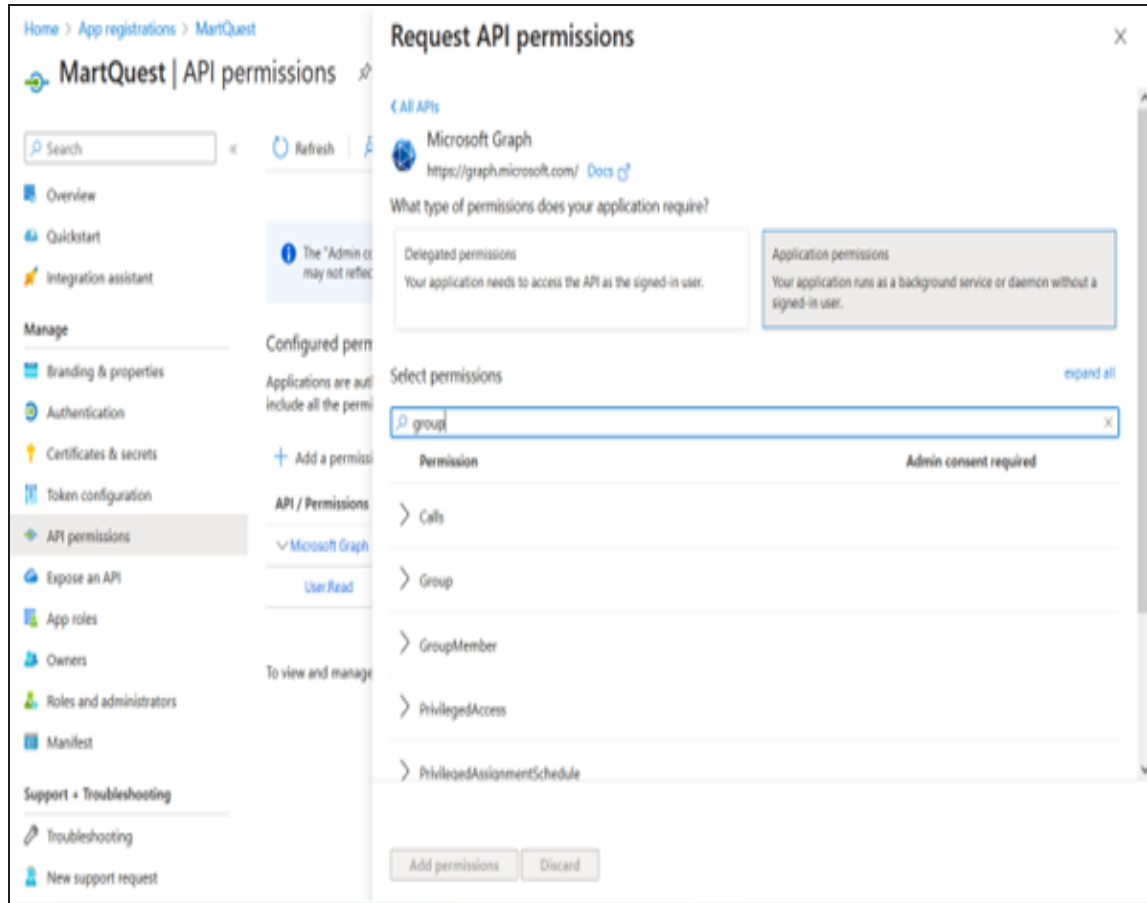
9. Click **Add a permission**.



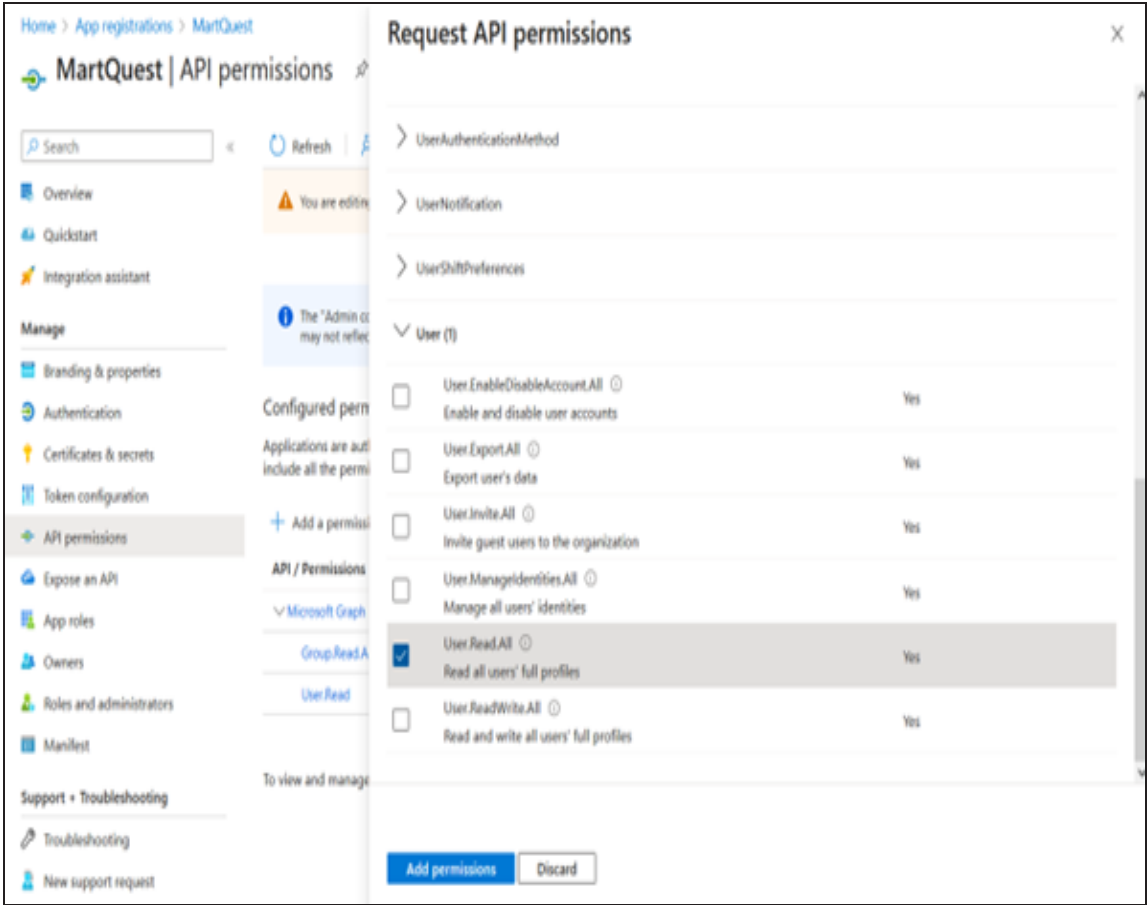
10. Click **Microsoft Graph**.



11. Select **Application permissions**.
12. Search and expand Group and select **Group.Read.All** permission. Then, click **Add permissions**.



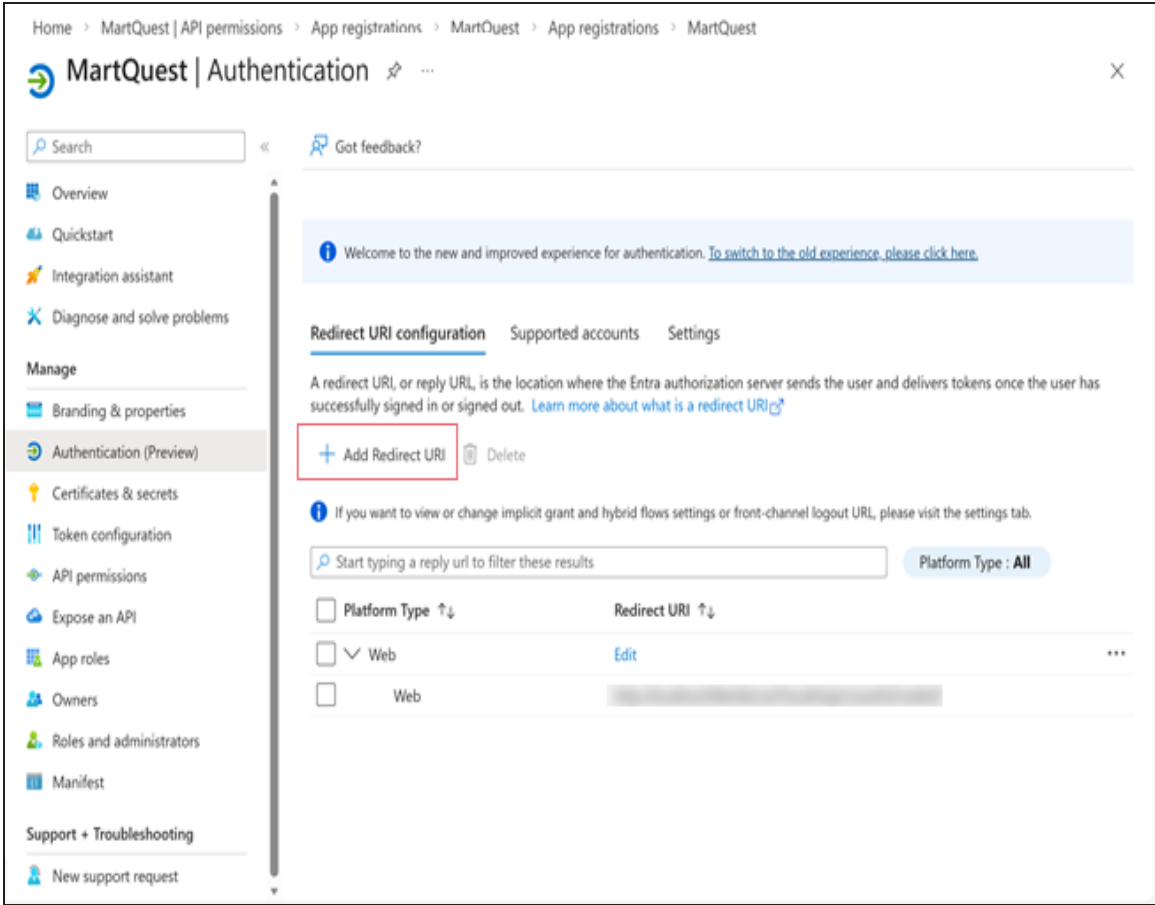
13. Go to **Add a permission** > **Microsoft Graph** > **Application permissions** again. Search and expand **User** and select **User.Read.All** permission. Then, click **Add permissions**.



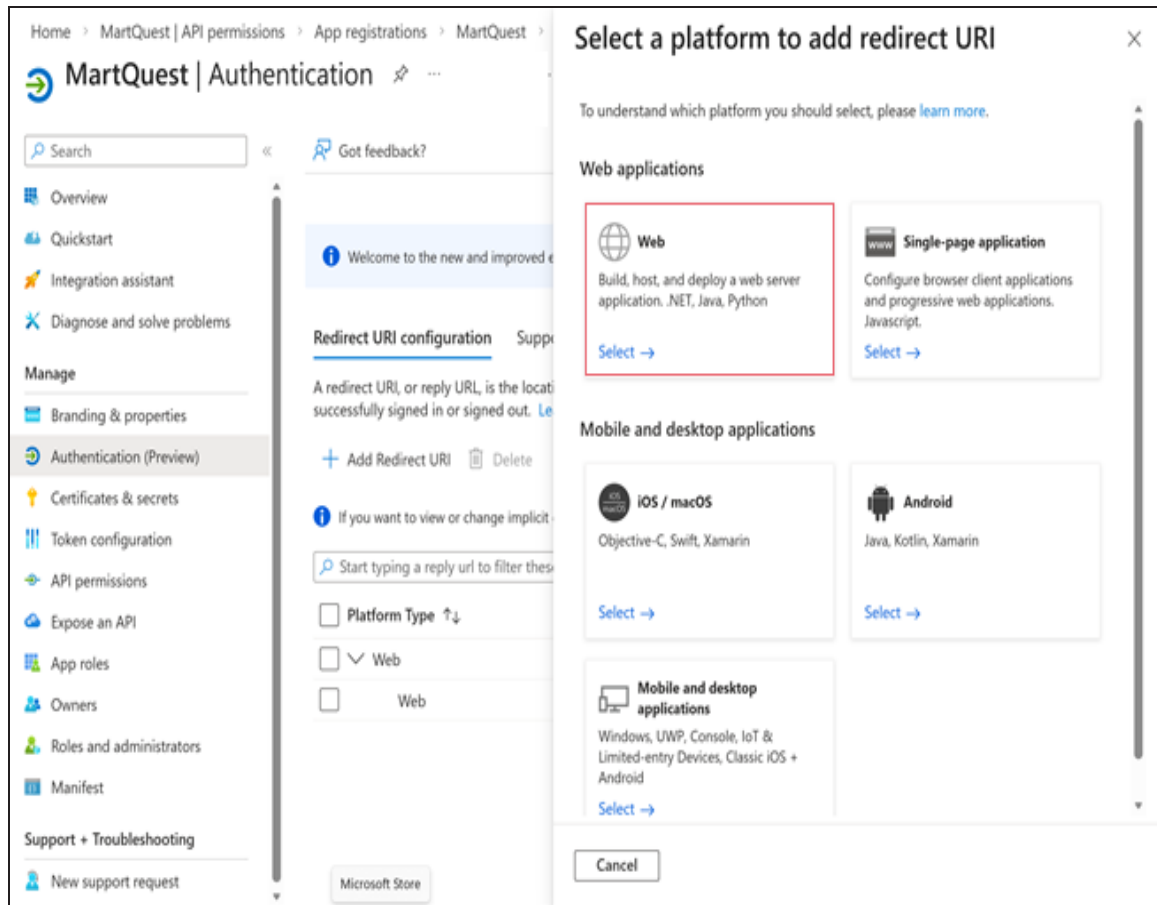
14. On the API permissions page, under the Configured permissions section, click **Grant admin consent for Contoso**.

Configured permissions					
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions includes all the permissions the application needs. Learn more about permissions and consent					
+ Add a permission ✓ Grant admin consent for Contoso					
API / Permissions name	Type	Description	Admin consent required	Status	
▼ Microsoft Graph (3)					
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Contoso	...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso	...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Contoso	...

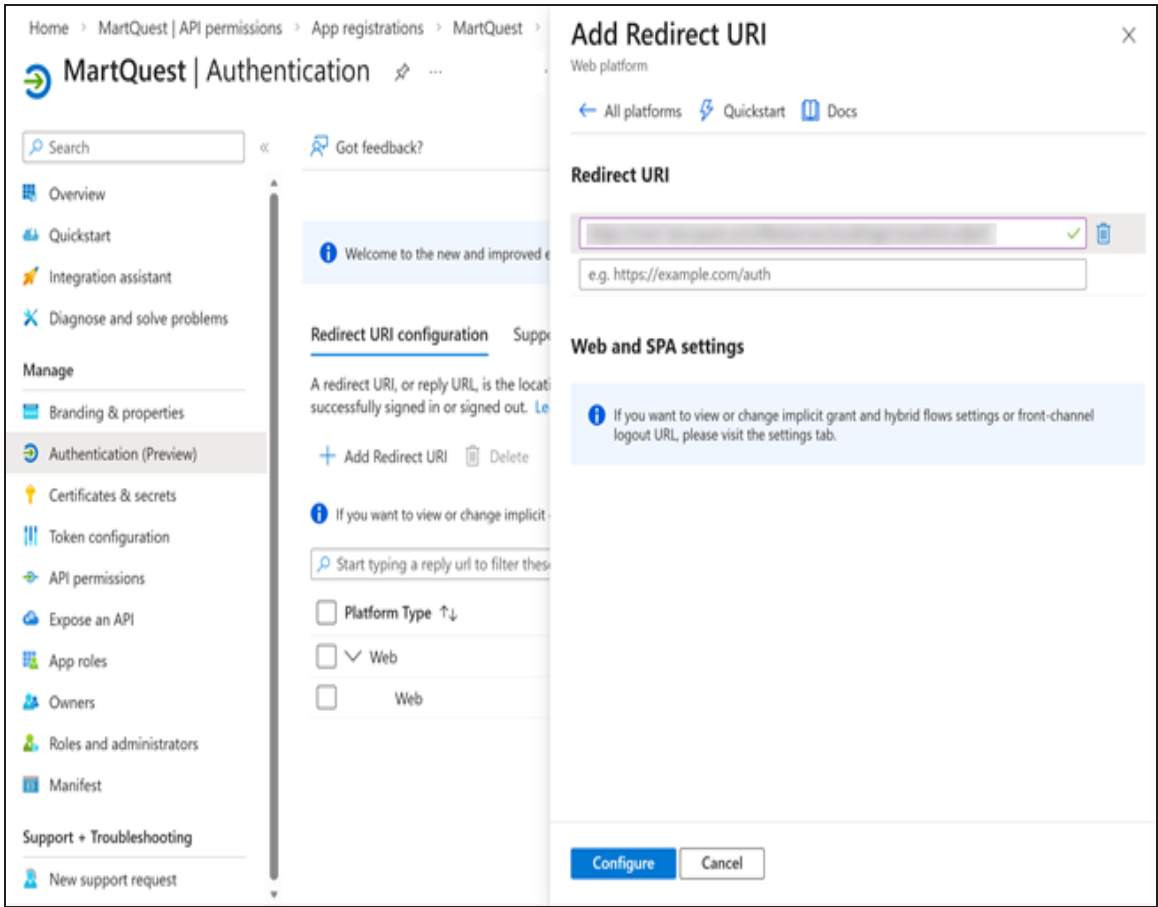
15. Go to the Authentication page and click **Add Redirect URI**.



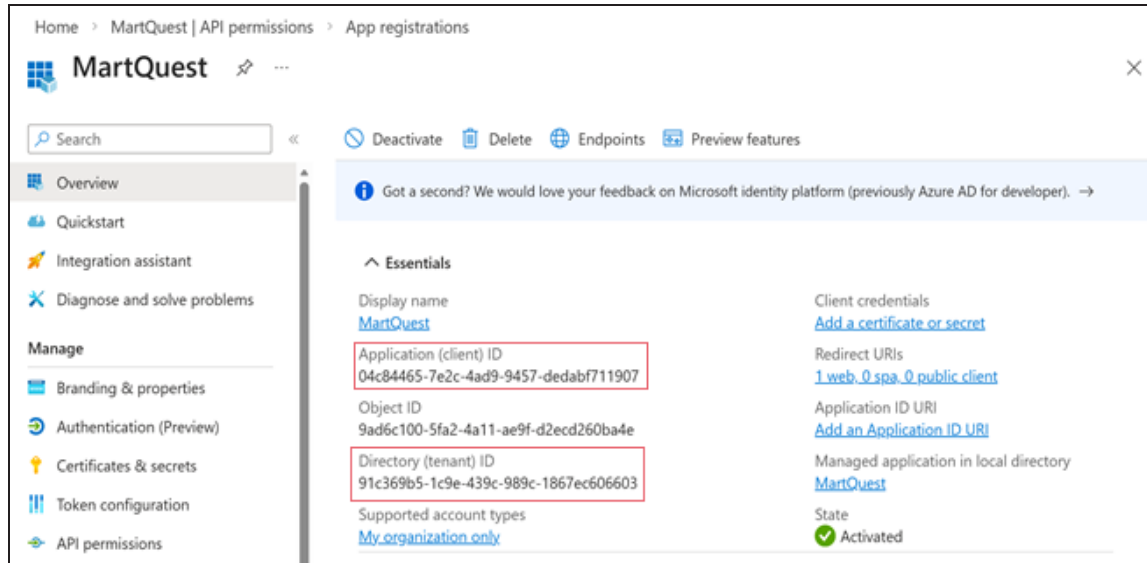
16. Click **Web**.



17. Enter the Redirect URI, and then click **Configure**.

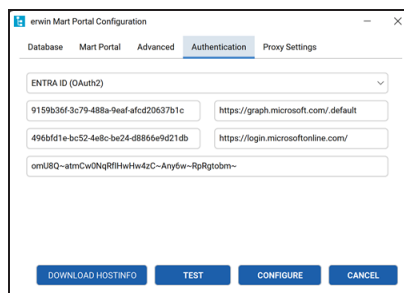


18. Go to the Overview page and note the Application (client) ID and Directory (tenant) ID. Graph scope and Client URI are default.



19. For Mart Portal on-premises, on the erwin Mart Portal Configuration screen, click the Authentication tab, select **Entra ID OAuth2**, and configure the following parameters for SSO:

- **Tenant ID:** Paste the Directory (tenant) ID copied in step 18.
- **Graph Scope:** Enter the Microsoft Graph permission scope requested for acquiring an access token. For example, *https://graph.microsoft.com/.default*.
- **Client ID:** Paste the Application (client) ID copied in step 18.
- **Client URI:** Enter the base URI. For example, *https://login.microsoftonline.com/*
- **Client Secret:** Paste the auto-generated value copied in step 7.



20. Click **Configure**.

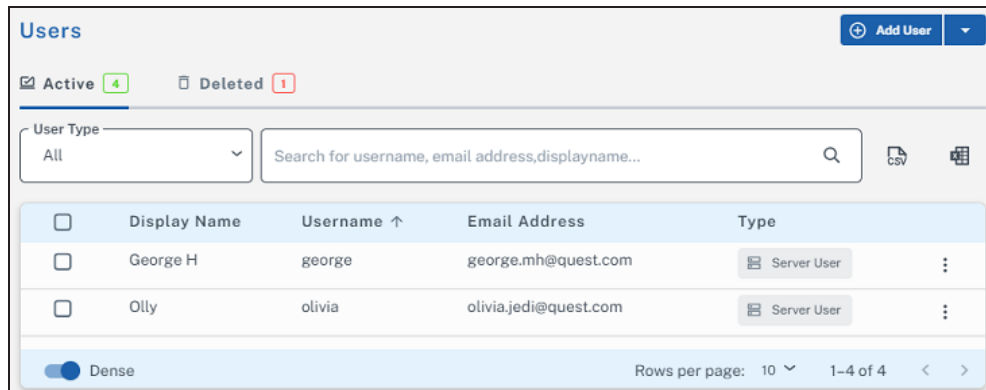
Your erwin Mart Portal is now authenticated via Entra ID OAuth2.

You can move to [users](#) and [groups](#) in erwin Mart Portal

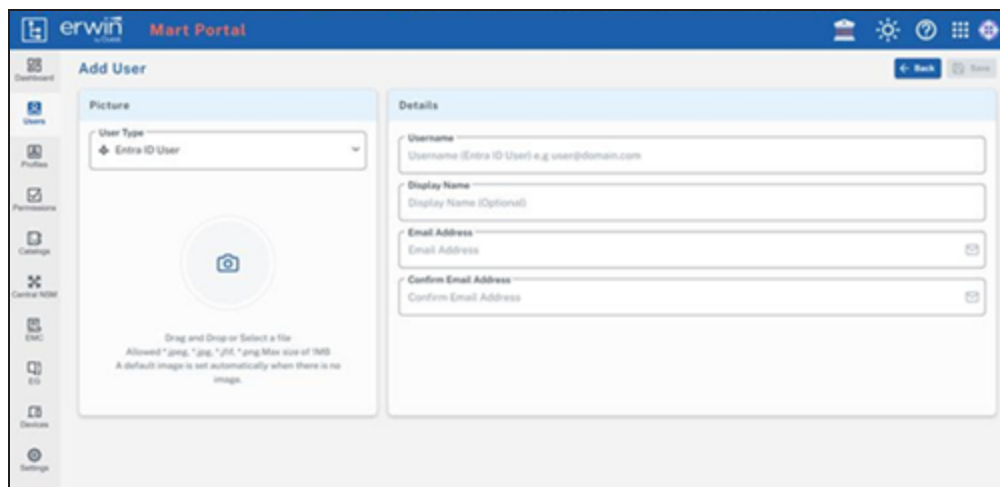
Adding Users in erwin Mart Portal

To add your Entra ID users to erwin Mart Portal, follow these steps:

1. Log in to the erwin Mart Portal as an administrator.
2. Go to **Application Menu > Users**.
The Users page appears.



3. Click **Add User**.
The Add User page opens.



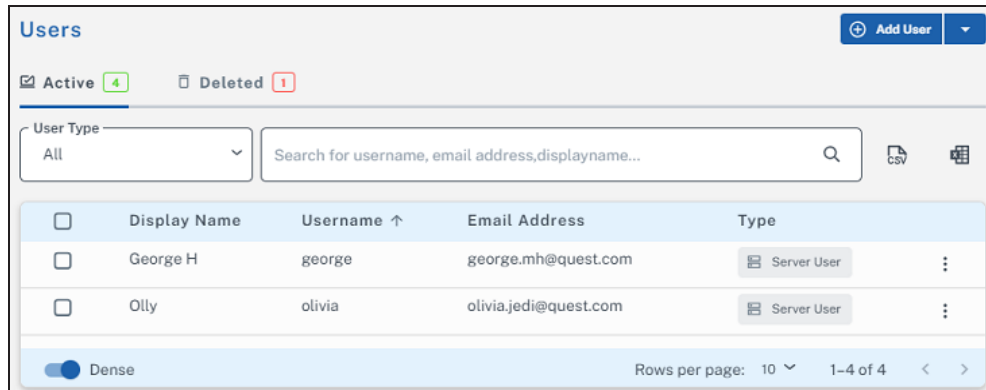
4. In the User Type field, select **Entra ID User** and add details in the Username, Display Name, Email Address, and Confirm Email Address fields.
5. Click **Save**.

The user has been added.

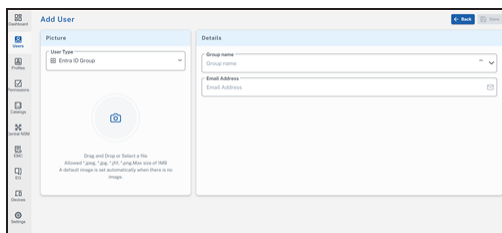
Adding Groups in erwin Mart Portal

To add your Entra ID groups to erwin Mart Portal, follow these steps:

1. In the Microsoft Entra admin center, click **Groups > All groups > Download groups**.
2. Log in to the erwin Mart Portal as an administrator.
3. Go to **Application Menu > Users**.
The Users page opens.



4. Click **Add User**.
The Add User page appears.
5. Under User Type, select **Entra ID Group**.



6. Under Group name, select the group that you want to add.
7. In the Email Address field, enter your email address.
8. Click **Save**.

The group has been added.

SAML with Entra ID

Based on your application type, refer to the appropriate section for SAML configuration:

- [erwin Mart Portal on-cloud](#)
- [erwin Mart Portal on-premises](#)

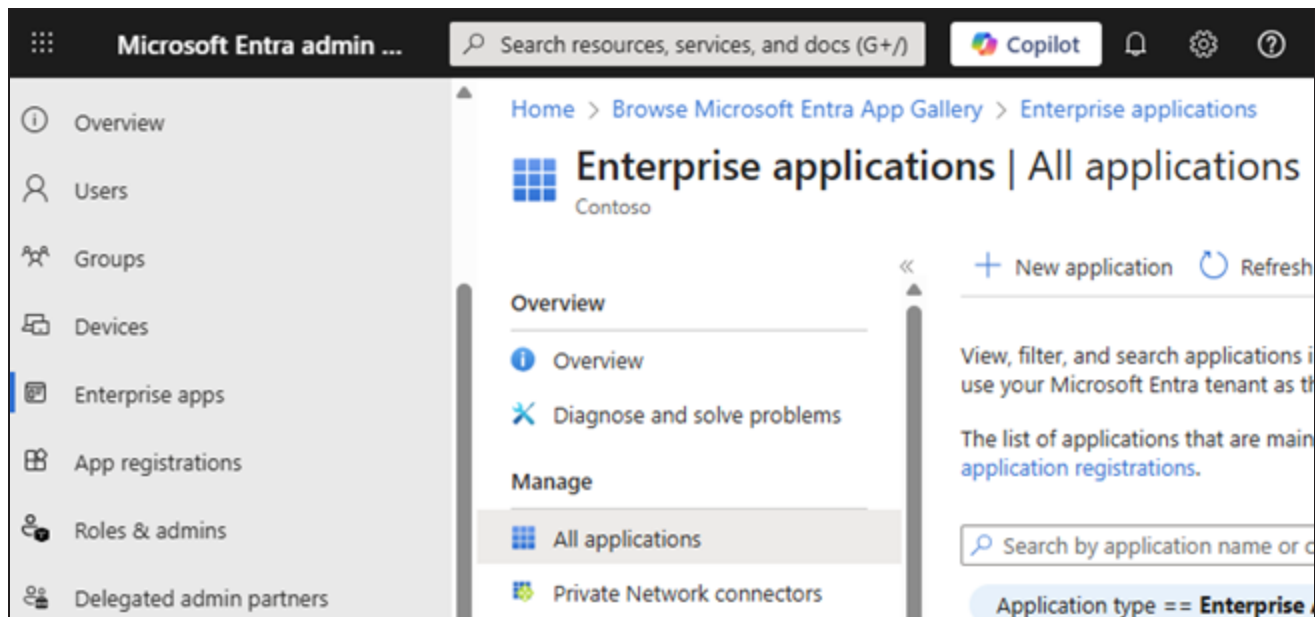
Once SAML configuration is ready, you can [add user groups](#) to erwin Mart Portal.

erwin Mart Portal On-Cloud

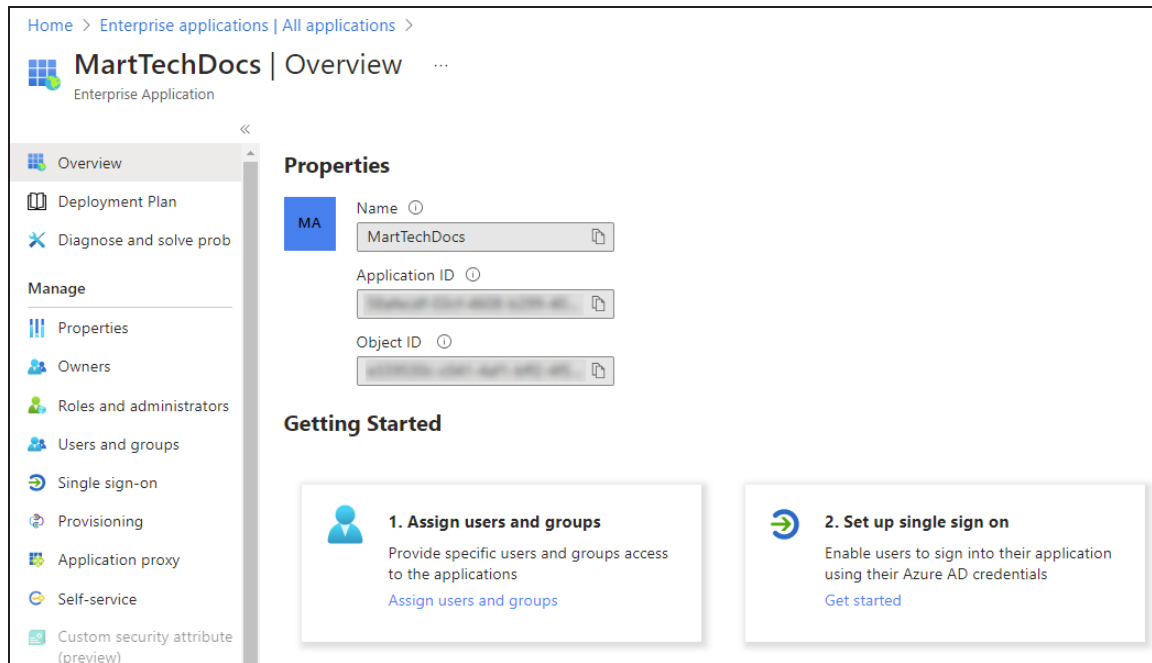
Before you configure Entra ID SAML, ensure that you have responded to the questionnaire from your Quest Support representative so that they can provide you with the Identifier and Reply URL for your erwin Mart Portal instance. If you did not receive the questionnaire, reach out to your Quest Support representative.

To configure Entra ID SAML for erwin Mart Portal on-cloud authentication, follow these steps:

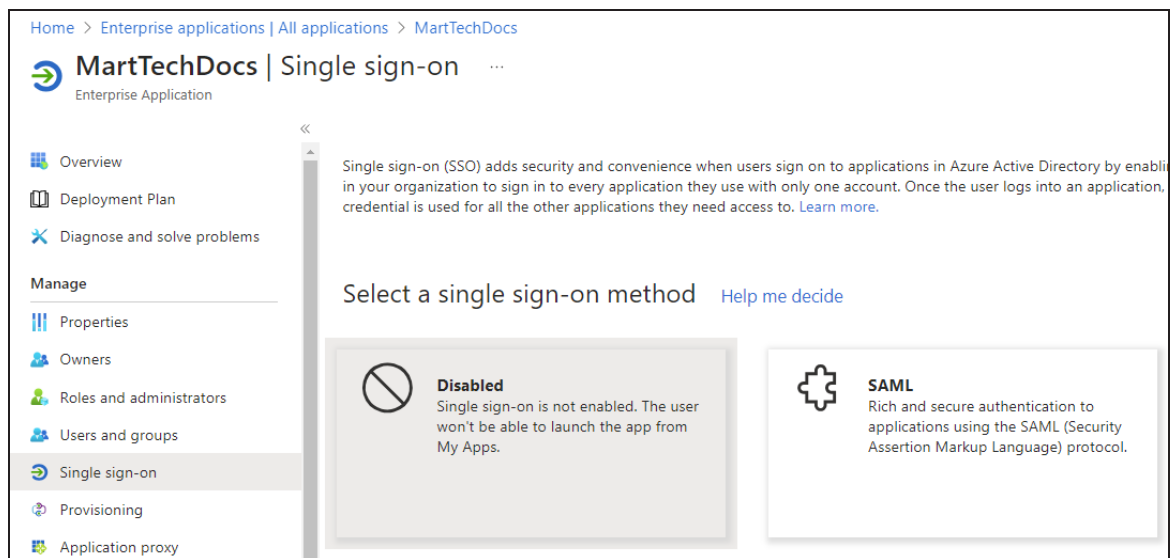
1. Log in to the Microsoft Entra admin center.
2. Click **Enterprise apps**.



3. Click **New application** and create your non-gallery application with an appropriate name.
4. Open your newly created application.



5. Click **Set up single sign on**.



6. Under single sign-on method, click **SAML**.

[Upload metadata file](#)
[Change single sign-on mode](#)
[Test this application](#)
[Got feedback?](#)

1

Basic SAML Configuration

[Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate

[Edit](#)

Status	Active
Thumbprint	C84530997588D74EC273EED06765926DE39BDEC4
Expiration	10/1/2030, 10:46:36 AM
Notification Email	sdhake@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- In the Basic SAML Configuration section, click **Edit**.

The Basic SAML Configuration page opens.

Basic SAML Configuration

 Save |  Got feedback?

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
	0	☒

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

8. Enter the Identifier and Reply URL that you received from Quest Support in the respective fields and click **Save**.

For example, your Identity and Reply URL would follow the `https://<Customer>.myerwin.com/MartServerCloud` format.

For the Reply URL, enter your `https://<Customer>.myerwin.com/MartServerCloud` URL. Once your erwin Mart Portal instance is configured, you will need to change it to the correct URL shared by Quest Support.

[↑](#) Upload metadata file | [↶](#) Change single sign-on mode | [☰](#) Test this application | [🗨](#) Got feedback?

[more.](#)

Read the [configuration guide](#) for help integrating erwinMartOnPremSAML.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://localhost:8443/MartServerCloud
Reply URL (Assertion Consumer Service URL)	https://localhost:8443/MartServerCloud/saml2/login/sso/erwin
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://localhost:8443/MartServerCloud/saml2/SingleLogout

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate

Edit

Status	Active
Thumbprint	A4C4BDAD73605B904814E8E8BE348EBB71E65C3D
Expiration	9/19/2027, 4:54:48 PM
Notification Email	admin@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36f-3c79-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

9. In the Attributes & Claims section, click **Edit**.

The Attributes & Claims page opens.

10. Click **Add a group claim**. In the Group Claims pane, click **Groups assigned to the application** and in the **Source attribute** list, select **Group ID**.

...

MartTechDocs | SAML-E

Attributes & Claim

+ Add new claim

+ Add a

Required claim

Claim name

Unique User Identifier (Name ID)

Additional claims

Claim name

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None

☐ All groups

☐ Security groups

☐ Directory roles

☒ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups ⓘ

Advanced options

Save

11. Click **Save**.
- This configures the group attribute name (user.groups [ApplicationGroup]). This is a necessary property.
- Apart from this, you can configure email (user.mail) and display name (user.givenname) values here. However, they are optional.

Additional claims		
Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [ApplicationGroup]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

12. Go back to the Set up Single Sign-On with SAML page.
- Under Attributes & Claims, the user.groups claim is available now.

[Upload metadata file](#)
[Change single sign-on mode](#)
[Test this application](#)
[Got feedback?](#)

more.

Read the [configuration guide](#) for help integrating erwinMartOnPremSAML.

- ### Basic SAML Configuration

[Edit](#)

Identifier (Entity ID)	https://localhost:8443/MartServerCloud
Reply URL (Assertion Consumer Service URL)	https://localhost:8443/MartServerCloud/saml2/login/sso/erwin
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://localhost:8443/MartServerCloud/saml2/SingleLogout
- ### Attributes & Claims

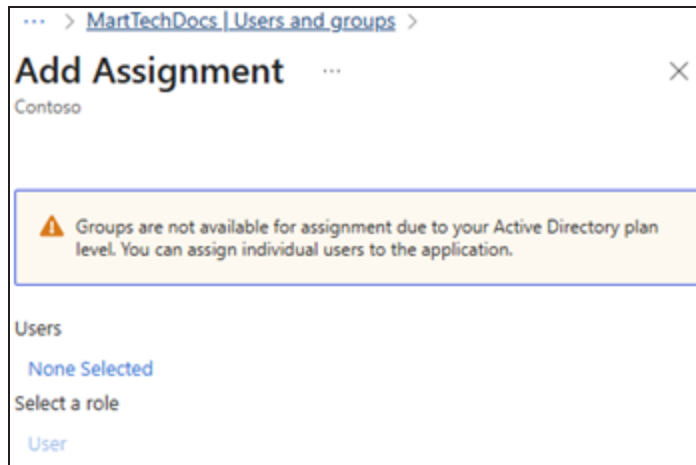
[Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
groups	user.groups
- ### SAML Certificates

[Edit](#)

Token signing certificate	
Status	Active
Thumbprint	A4C4BDAD73605B904814E8E8BE348EBB71E65C3D
Expiration	9/19/2027, 4:54:48 PM
Notification Email	admin@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36f-3c79-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- Copy the App Federation Metadata URL and save it for use later, in step 16.
- Click **Users and groups** > **Add user/group**. Initially, under Users, it displays None Selected.



15. Click the **None Selected** link.

Select the required users or groups and click **Select**. Then, click **Assign**.

Home > Enterprise applications | All applications **Users**

Add Assignment

Contoso

 Groups are not available for assignment due to the application.

Try changing or adding filters if you don't see what you're looking for

Search
mart

Users
3 users selected.

Select a role
User

	Name	Type
☒	mart	User
☐	Mart Test	User
☐	mart_test_user1	User
☐	mart_user_test	User
☐	mart1	User
☒	martuser	User
☒	martuser1	User
☐	martuser2	User

Assign Select

Your SAML SSO setup for the required users is complete.

16. Finally, share the following information with your Quest Support representative along with the detailed questionnaire that you receive at the beginning of the engagement:

- App Federation Metadata URL (copied in step 14)
- Group Attribute Name (Available under Attributes & Claims. For example, user-groups <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>)

Group Attribute Name is case-sensitive.

SAML with Entra ID

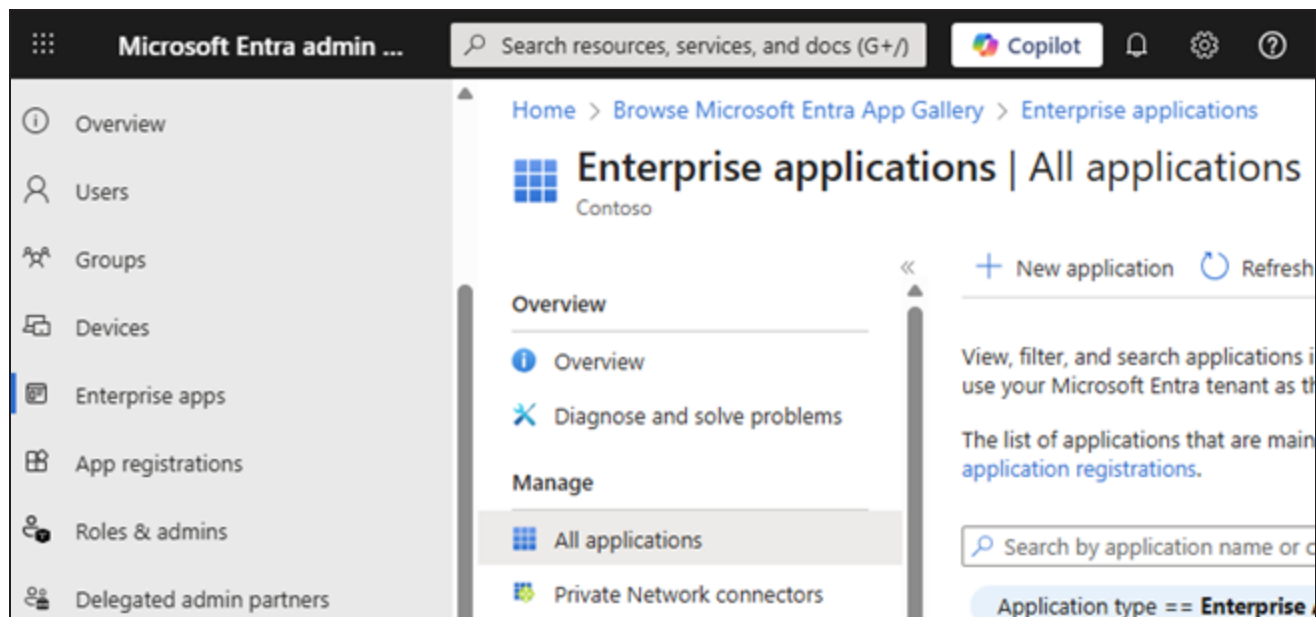
- **Optional**-User Email Attribute Name (Available under Attributes & Claims, For example, user.mail http://s-chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)
- **Optional**-User Display Name Attribute Name (Available under Attributes & Claims, For example, user.givenname http://s-chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname)

Once the support team authenticates erwin Mart Portal for you, you can move to [adding groups in erwin Mart Portal](#) at https://<your_instance>.myerwin.com/MartPortal.

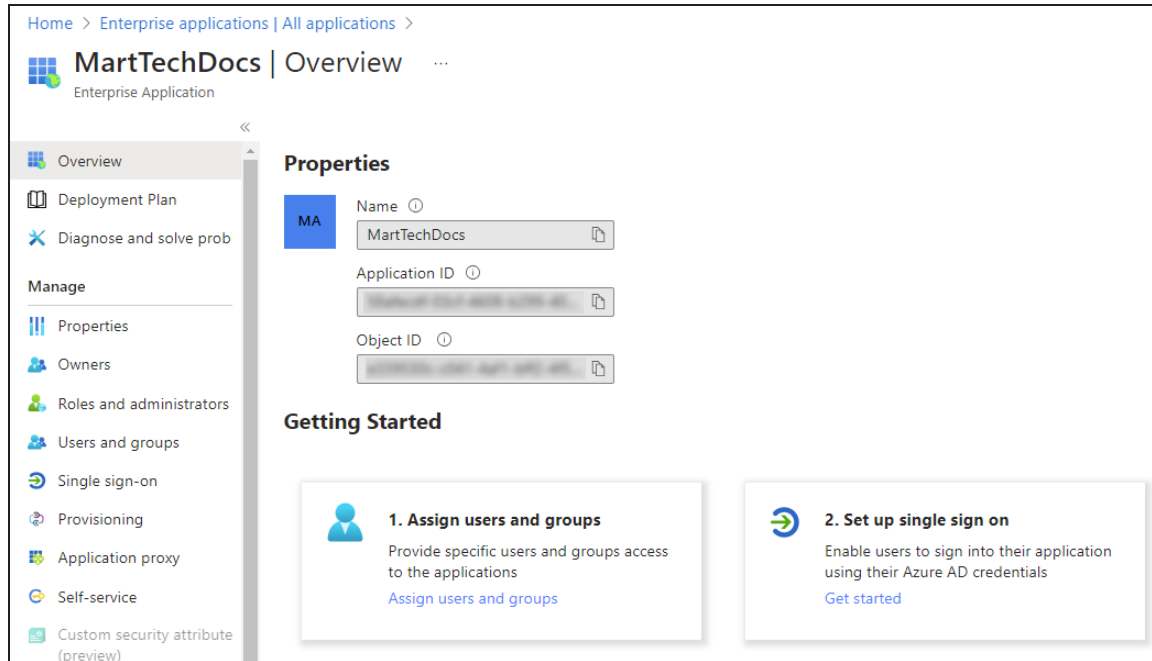
erwin Mart Portal On-Premises

To configure Entra ID SAML for erwin Mart Portal authentication, follow these steps:

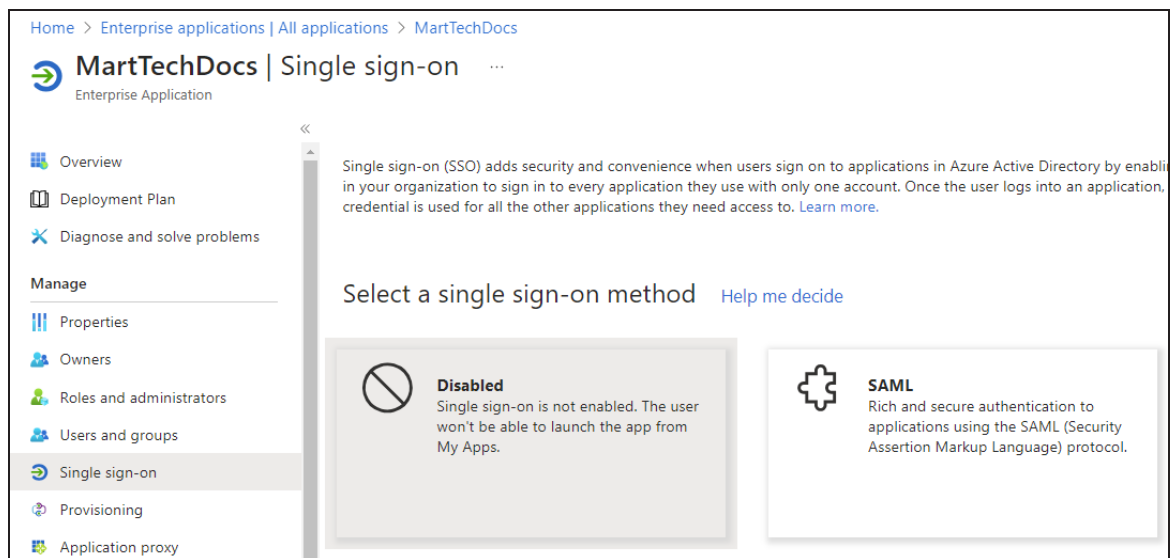
1. Log in to the Microsoft Entra admin center.
2. Click **Enterprise apps**.



3. Click **New application** and create your non-gallery application with an appropriate name.
4. Open your newly created application.



5. Click **Set up single sign on**.



6. Under single sign-on method, click **SAML**.

[↑ Upload metadata file](#) [↩ Change single sign-on mode](#) [☰ Test this application](#) | [🗨 Got feedback?](#)

1

Basic SAML Configuration

[✎ Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate

[✎ Edit](#)

Status	Active
Thumbprint	C84530997588D74EC273EED06765926DE39BDEC4
Expiration	10/1/2030, 10:46:36 AM
Notification Email	sdhake@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

7. Click **Upload metadata file**.

Upload metadata file.

Values for the fields below are provided by MartTechDocs. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by MartTechDocs.



8. Select the SP Metadata file (mart-sp-metadata.xml) that you downloaded (**erwin Mart Portal Configuration > Authentication tab > Download SP Metadata**) during erwin Mart Portal configuration.

Then, click **Add**.

Doing this retrieves the Identifier, Reply URL, and Logout URL.

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://localhost:443/MartServerCloud	☒ ⓘ 

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://localhost:443/MartServerCloud/saml2/login/sso/erwin	0	☒ ⓘ 

[Add reply URL](#)

9. Click **Save**.

The necessary metadata is saved under the Basic SAML Configuration section.

[↑ Upload metadata file](#) [↶ Change single sign-on mode](#) [☰ Test this application](#) [🗨 Got feedback?](#)

[more.](#)

Read the [configuration guide](#) for help integrating erwinMartOnPremSAML.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://localhost:8443/MartServerCloud
Reply URL (Assertion Consumer Service URL)	https://localhost:8443/MartServerCloud/saml2/login/sso/erwin
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://localhost:8443/MartServerCloud/saml2/SingleLogout

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate

Edit

Status	Active
Thumbprint	A4C48DAD73605B904814E8E8BE348EBB71E65C3D
Expiration	9/19/2027, 4:54:48 PM
Notification Email	admin@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36f-3c79-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

10. In the Attributes & Claims section, click **Edit**.

The Attributes & Claims page opens.

11. Click **Add a group claim**. In the Group Claims pane, click **Groups assigned to the application** and in the **Source attribute** list, select **Group ID**.

...

MartTechDocs | SAML-E

Attributes & Claim

+ Add new claim

+ Add a

Required claim

Claim name

Unique User Identifier (Name ID)

Additional claims

Claim name

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

http://schemas.xmlsoap.org/ws/

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None

☐ All groups

☐ Security groups

☐ Directory roles

☒ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups ⓘ

Advanced options

Save

12. Click **Save**.

This configures the group attribute name (user.groups [ApplicationGroup]). This is a necessary property.

Apart from this, you can configure email (user.mail) and display name (user.givenname) values here. However, they are optional.

Additional claims		
Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [ApplicationGroup]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

13. Go back to the Set up Single Sign-On with SAML page.

Under Attributes & Claims, the user.groups claim is available now.

[↑ Upload metadata file](#) [↶ Change single sign-on mode](#) [☰ Test this application](#) [🗨 Got feedback?](#)

[more.](#)

Read the [configuration guide](#) for help integrating erwinMartOnPremSAML.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://localhost:8443/MartServerCloud
Reply URL (Assertion Consumer Service URL)	https://localhost:8443/MartServerCloud/saml2/login/sso/erwin
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://localhost:8443/MartServerCloud/saml2/SingleLogout

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
groups	user.groups

3

SAML Certificates

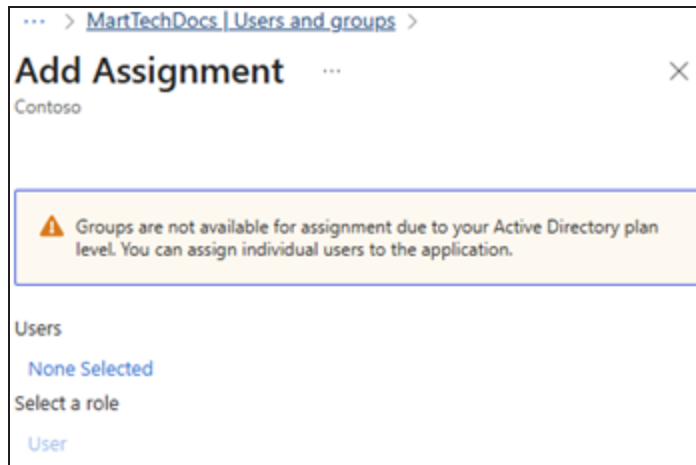
Token signing certificate

Edit

Status	Active
Thumbprint	A4C4BDAD736058904814E8E8B348EBB71E65C3D
Expiration	9/19/2027, 4:54:48 PM
Notification Email	admin@M365x11048911.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9159b36f-3c79-... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

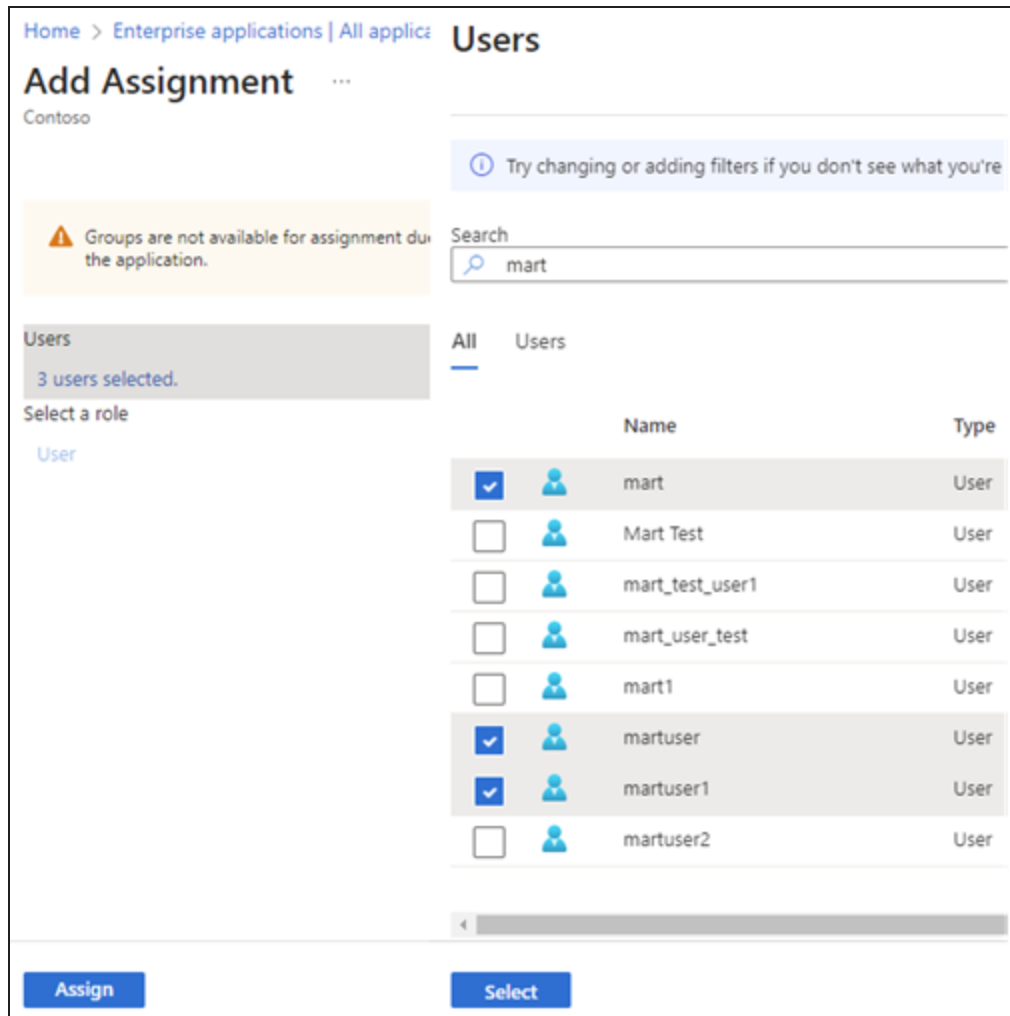
14. Copy the App Federation Metadata URL.

15. Click **Users and groups** > **Add user/group**. Initially, under Users, it displays None Selected.



16. Click the **None Selected** link.

Select the required users or groups and click **Select**. Then, click **Assign**.



Your SAML SSO setup for the required users is complete.

17. On the erwin Mart Portal Configuration screen, click the **Authentication** tab, and then follow these steps:
 - a. In the MetaData XML field, paste the App Federation Metadata URL copied in step 14.
 - b. In the Group Attribute Name, User Email Attribute Name, and User Display Name Attribute Name fields, configure values as follows:

SAML with Entra ID

- Group Attribute Name (Available under Attributes & Claims. For example, user.groups http://schemas.microsoft.com/ws/2008/06/identity/claims/groups)
- **Optional**-User Email Attribute Name (Available under Attributes & Claims, For example, user.mail http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)
- **Optional**-User Display Name Attribute Name (Available under Attributes & Claims, For example, user.givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname)

The screenshot shows the 'erwin Mart Portal Configuration' window with the 'Authentication' tab selected. The configuration is set to 'SAML'. Below this, there is a 'URL' dropdown and a 'Metadata XML' text field. Three attribute name fields are provided: 'Group Attribute Name', 'User Email Attribute Name', and 'User Display Name Attribute Name'. The 'Authentication Request Signed' checkbox is checked. A 'Download SP Metadata' button is present. At the bottom, there are four buttons: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

18. Click **Configure**.

Your erwin Mart Portal is now authenticated via SAML EntraID.

Adding Groups in erwin Mart Portal

To add your Entra ID SAML groups to erwin Mart Portal, follow these steps:

1. Create a CSV file containing the <group_attribute_value> and <group_display_name>.

You can also use the [sample template for groups](#) and replace the sample values with the actual Group Attribute Name and Group Display Name.

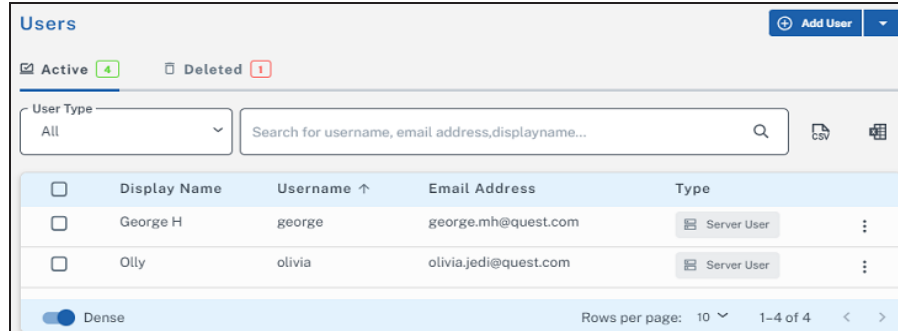
	A	B
1	id	displayName
2	01628af3-3e91-43a0-a9df-ad5a6155f62f	QA53
3	Admin	Mart Admin

```
id,displayName
01628af3-3e91-43a0-a9df-ad5a6155f62f,QA53
Admin,Mart Admin
```

2. Log in to the erwin Mart Portal as an administrator.

3. Go to **Application Menu > Users**.

The Users page appears.



4. Click **Add User**.

The Add User page appears.

The screenshot shows the 'Add User' form in the Quest software interface. The left sidebar contains navigation links: Dashboard, Users, Profiles, Permissions, Catalogs, Central NSM, EMC, EG, Devices, and Settings. The main form is divided into two sections: 'Picture' and 'Details'. In the 'Picture' section, the 'User Type' dropdown is set to 'Server User'. Below it is a large circular area with a camera icon and text: 'Drag and Drop or Select a file. Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB. A default image is set automatically when there is no image.' The 'Details' section contains several input fields: 'Username' (Enter Username), 'Display Name' (Enter DisplayName), 'Email Address' (Enter EmailAddress), 'Confirm Email Address' (Enter Confirm email Address), and 'Password' (Enter Password). A checkbox labeled 'User must change password at next login' is checked. At the top right of the form are 'Back' and 'Save' buttons. At the bottom of the form are links for 'About', 'Privacy', 'Legal', 'Contact', and 'Impressum', along with social media icons and a copyright notice: '© 2025 Quest Software, Inc. All rights reserved. Version 15.2'.

5. Under User Type, select **SAML Group**

The screenshot shows the 'Add User' form in the Quest software interface. The left sidebar contains navigation links: Dashboard, Users, Profiles, Permissions, Catalogs, Central NSM, EMC, EG, Devices, and Settings. The main form is divided into two sections: 'Picture' and 'Details'. In the 'Picture' section, the 'User Type' dropdown is set to 'SAML Group'. Below it is a large circular area with a camera icon and text: 'Drag and Drop or Select a file. Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB. A default image is set automatically when there is no image.' The 'Details' section contains a large area for uploading a file with text: 'Drag and Drop or Select a file. Drop file(s) here or [browse](#). Allowed text/csv. Max size of 2MB'. Below this is a 'Group name' dropdown menu with 'Select Group' as the selected option. At the bottom is an 'Email Address' field with the placeholder text 'Email Address'. At the top right of the form are 'Back' and 'Save' buttons.

6. Drag and drop the CSV file that you created in step 1.
7. Under Group name, select the required group.
8. In the Email Address field, enter your email address.

9. Click **Save**.

The group has been added.

SAML with PingIdentity

Based on your application type, refer to the appropriate section for SAML with PingIdentity configuration:

- [erwin Mart Portal on-cloud](#)
- [erwin Mart Portal on-premises](#)

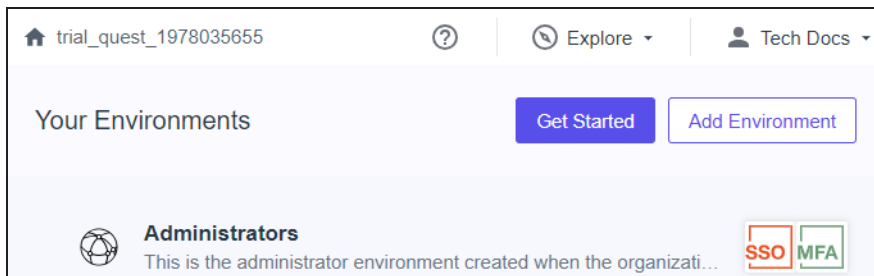
Once SAML configuration is ready, you can add [user groups](#) to erwin Mart Portal.

erwin Mart Portal On-Cloud

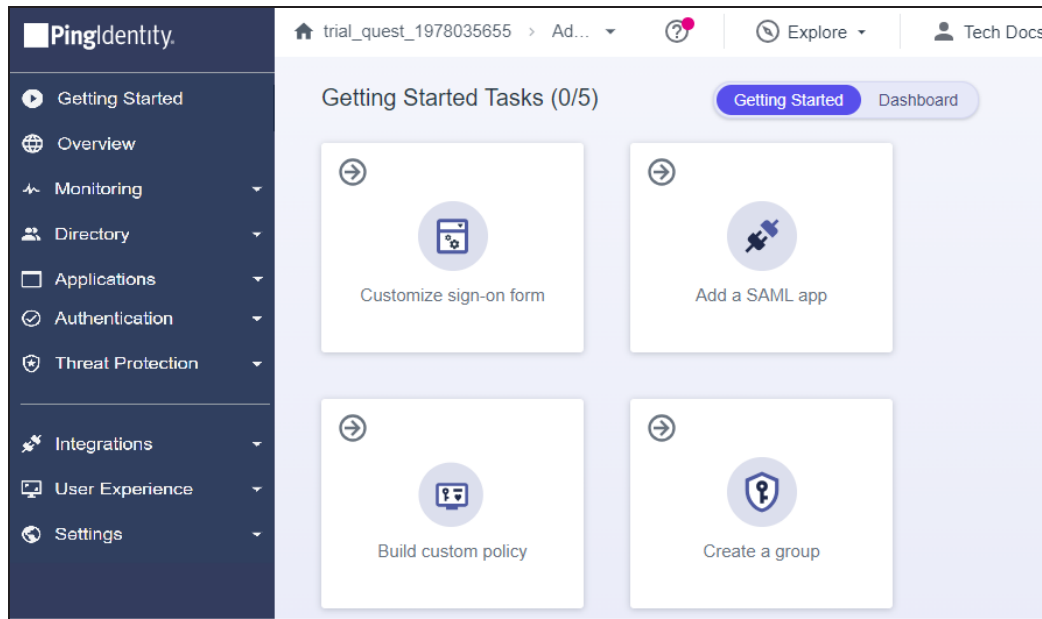
Before you configure SAML with PingIdentity, ensure that you have responded to the questionnaire from your Quest Support representative so that they can provide you with the Identifier (Entity ID) and Reply URL (ACS URL) for your erwin Mart Portal instance. If you did not receive the questionnaire, reach out to your Quest Support representative.

To configure SAML with PingIdentity for erwin Mart Portal on-cloud authentication, follow these steps:

1. Log in to PingIdentity Console.



2. Click **Administrators** to set up your environment.



3. Click **Directory** > **Users** > .

 Add User

Given Name

Family Name

Username *

Email

☐ Require Email to be Verified

Population *

Authoritative Identity Provider ?

PingOne (default)

Password

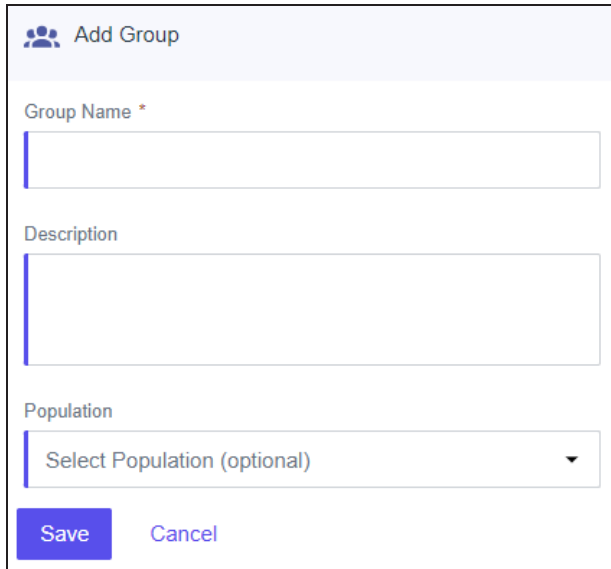
[Generate Password](#)

Save

Cancel

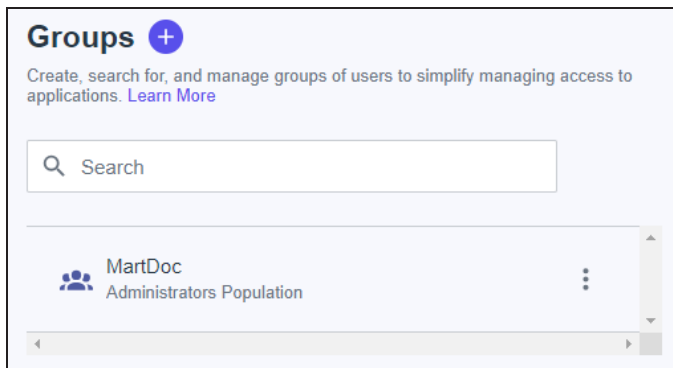
4. Enter user's information and click **Save**.

5. Click **Directory > Groups > **.



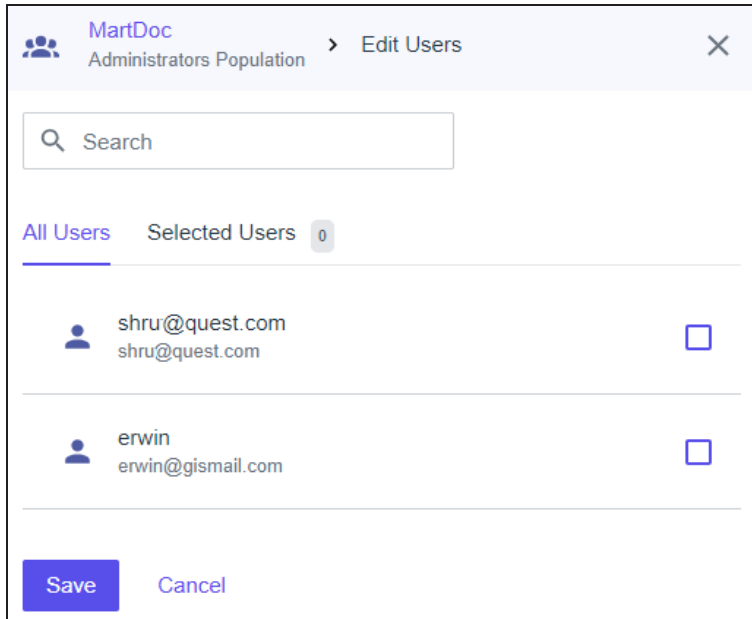
The screenshot shows the 'Add Group' form. At the top, there is a header with a group icon and the text 'Add Group'. Below this, there are three input fields: 'Group Name *' (required), 'Description', and 'Population' (a dropdown menu). The 'Population' dropdown is currently set to 'Select Population (optional)'. At the bottom of the form, there are two buttons: 'Save' (in blue) and 'Cancel'.

6. Enter **Group Name** and select **Population**.
7. Click **Save**.



The screenshot shows the 'Groups' page. At the top, there is a header with the text 'Groups' and a plus icon. Below this, there is a sub-header with the text 'Create, search for, and manage groups of users to simplify managing access to applications. [Learn More](#)'. Below the sub-header, there is a search bar with the text 'Search'. Below the search bar, there is a list of groups. The first group is 'MartDoc Administrators Population' with a group icon and a three-dot menu icon to its right. The list is scrollable, as indicated by the scrollbar on the right.

8. Click . Then, click **Add/Remove Users**.



9. Select the users that you want to add to your group and click **Save**.
10. Click **Applications > Applications > +**.

Add Application [X]

Application Name *

Description

Icon

Max Size 1.0 MB

Application Type [Show Details](#)

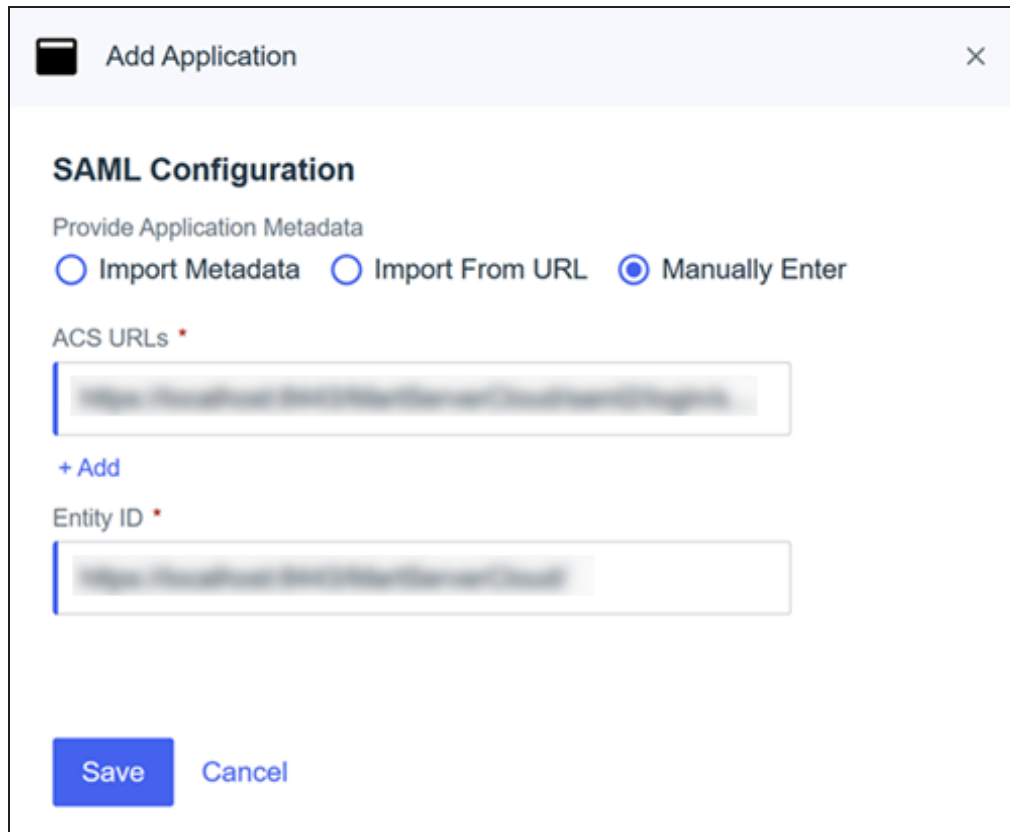
Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

SAML Application **OIDC Web App** **Native**

Single-Page **Worker**

Save Cancel

11. Enter an Application Name.
12. Click **SAML Application** and click **Save**.



Add Application [Close]

SAML Configuration

Provide Application Metadata

☐ Import Metadata
 ☐ Import From URL
 ☒ Manually Enter

ACS URLs *

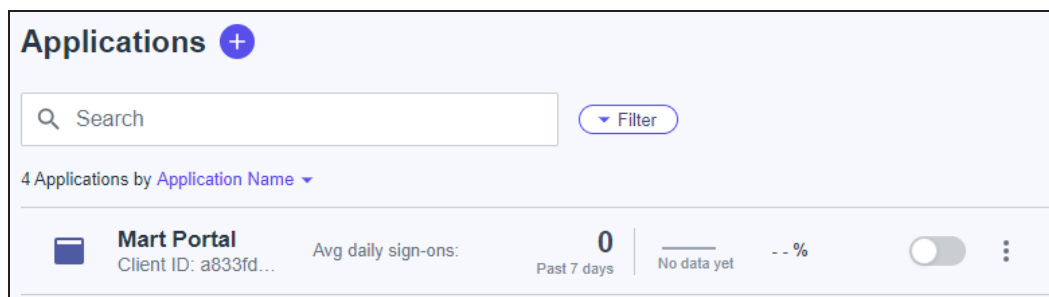
[Text Input Field]

+ Add

Entity ID *

[Text Input Field]

13. Click **Manually Enter** and enter the Entity ID and ACS URL provided by the Quest Support team.
14. Click **Save**.



Applications +

Search [Filter]

4 Applications by Application Name ▾

Application Name	Client ID	Avg daily sign-ons:	Filter	Toggle	More
Mart Portal	Client ID: a833fd...	0 Past 7 days	No data yet	-- %	☐ ⋮

15. Click ☐ against your application name to enable user access to your application.
16. In the list of applications, click your application name.

SAML with PingIdentity

Mart Portal
Client ID: a833fd2b-e7b2-4bf2-87f3-14024feb820

Overview Configuration Attribute Mappings Policies Access

Protocol SAML Attributes 1 Mapped Policies None Selected Access All Users

App Type
Advanced Configuration (SAML)

Description
Not Set

Client ID
a833fd2b-e7b2-4bf2-87f3-14024feb820

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

17. Click **Attribute Mappings** > > **Add**.

Mart Portal > Edit Attribute Mappings

If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Attribute Mapping + Add

Attributes	PingOne Mappings	Required
saml_subject	User ID	☒
		☐

Save **Cancel**

18. Add another attribute and map as shown in the following image.

Mart Portal > Edit Attribute Mappings

You map the identity attributes to the application attributes. The application attributes are listed on the right.

Attribute Mapping + Add

Attributes	PingOne Mappings	Required
saml_subject	User ID	☒
email	Email Address	☐
group	Group Names	☐

Save **Cancel**

Similarly, you can add a display name here.

19. Click **Save**.
These attributes are to be shared with the Quest Support team for configuration.
20. From the Overview tab, copy **IDP Metadata URL**.

Overview Configuration Attribute Mappings Policies Access

Client ID
715de852-122f-4493-9ef3-b788587daa1d

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

Connection Details

Issuer ID
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d

Initiate Single Sign-On URL
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/idp/startssso?spEntityId=https://localhost:8443/MartServerCloud/

IDP Metadata URL
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/metadata/715de852-122f-4493-9ef3-b788587daa1d

Single Signon Service
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/idp/sso

Single Logout Service
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/idp/slo

Download Metadata Download Signing Certificate

21. Share the following details with the Quest Support team:

- **Metadata XML URL:** The IDP Metadata URL copied in step 20.
- **Group Attribute Name:** The value configured in step 18.
- **User Email Attribute Name:** The value configured in step 18.
- **User Display Name Attribute Name:** The value configured in step 18.

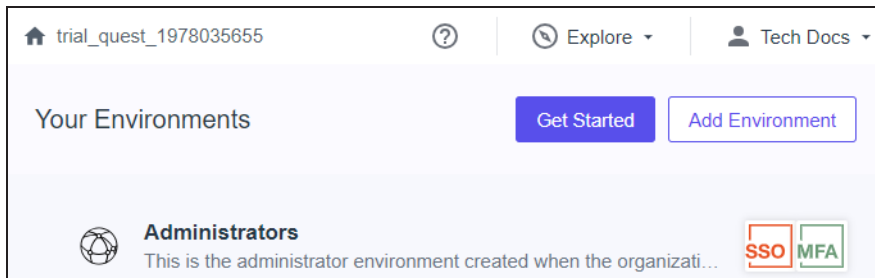
Once the support team authenticates for you, you can move to [adding groups](#) in at https://<your_instance>.myerwin.com/MartPortal.

erwin Mart Portal On-Premises

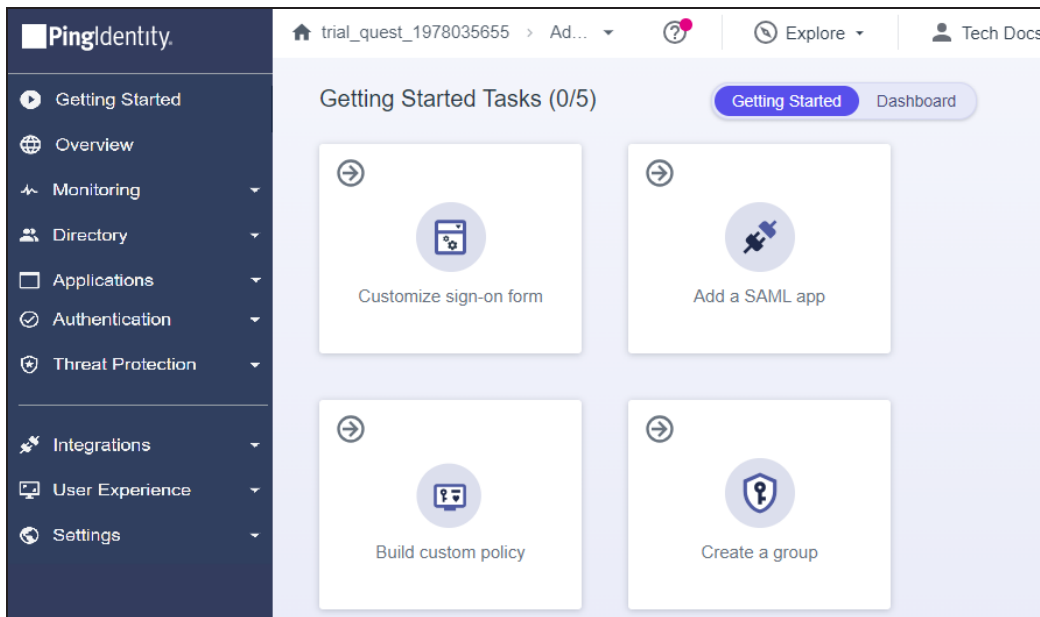
To configure SAML with PingIdentity for erwin Mart Portal on-premises authentication, follow these steps:

SAML with PingIdentity

1. Log in to PingIdentity Console.



2. Click **Administrators** to set up your environment.



3. Click **Directory** > **Users** > .

 Add User

Given Name

Family Name

Username *

Email

☐ Require Email to be Verified

Population *

Authoritative Identity Provider ?

PingOne (default)

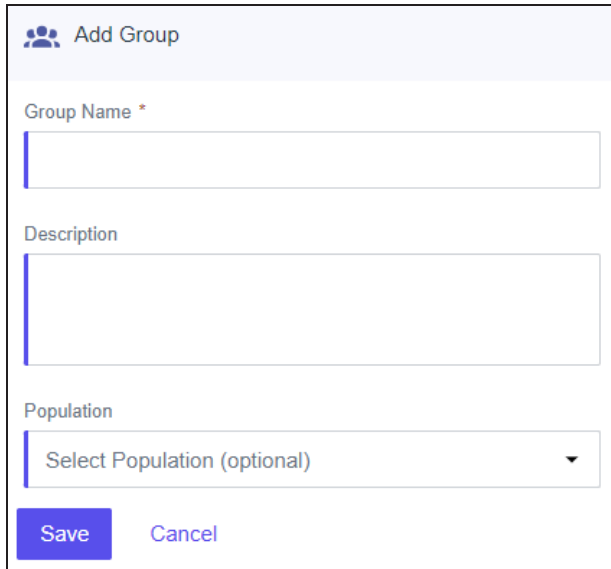
Password

[Generate Password](#)

Save

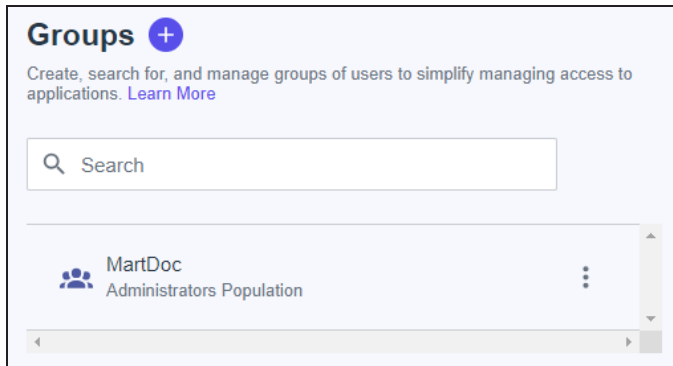
Cancel

4. Enter user's information and click **Save**.
5. Click **Directory > Groups > **.



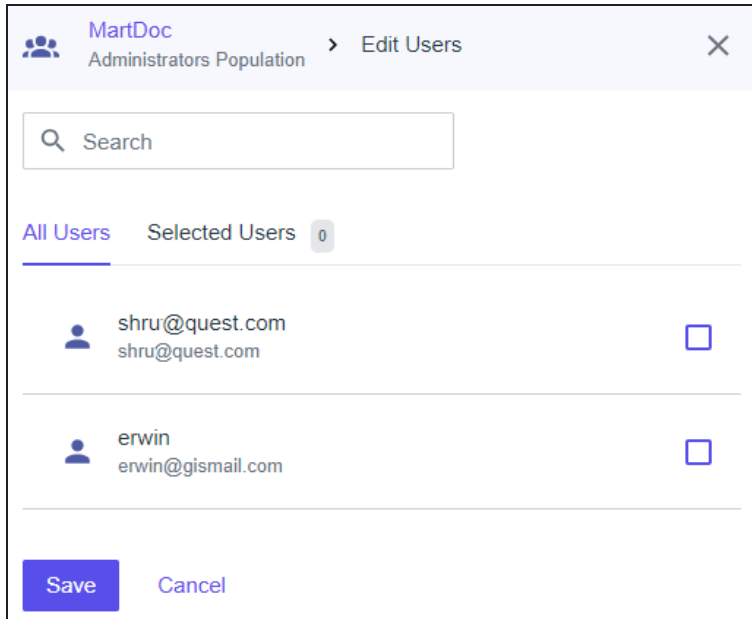
The screenshot shows the 'Add Group' form. At the top, there is a header with a group icon and the text 'Add Group'. Below this, there are three input fields: 'Group Name' with an asterisk indicating it is required, 'Description', and 'Population' which is a dropdown menu. The 'Population' dropdown currently shows 'Select Population (optional)'. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

6. Enter **Group Name** and select **Population**.
7. Click **Save**.



The screenshot shows the 'Groups' management page. At the top, there is a header with the text 'Groups' and a plus icon. Below this, there is a sub-header with the text 'Create, search for, and manage groups of users to simplify managing access to applications. [Learn More](#)'. Below the sub-header, there is a search bar with the text 'Search'. Below the search bar, there is a list of groups. The first group in the list is 'MartDoc Administrators Population' with a group icon and a three-dot menu icon to its right. The list is scrollable, as indicated by the scrollbar on the right.

8. Click . Then, click **Add/Remove Users**.



9. Select the users that you want to add to your group and click **Save**.
10. Click **Applications > Applications > +**.

Add Application

Application Name *

Description

Icon

Max Size 1.0 MB

Application Type [Show Details](#)

Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

SAML Application **OIDC Web App** **Native**

Single-Page **Worker**

Save **Cancel**

11. Enter an Application Name.
12. Click **SAML Application** and click **Save**.

Add Application

SAML Configuration

Provide Application Metadata

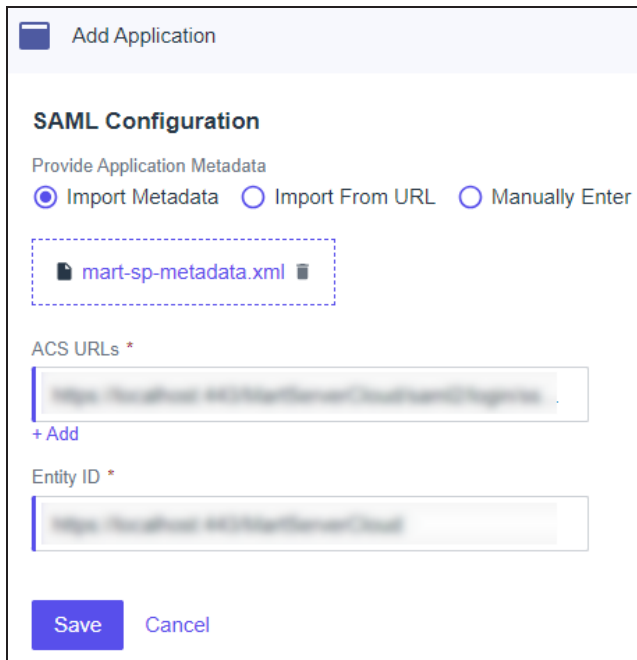
☒ Import Metadata ☐ Import From URL ☐ Manually Enter

Select a file

Save **Cancel**

SAML with PingIdentity

- Click **Import Metadata** and select the file that you downloaded (**erwin Mart Portal Configuration > Authentication tab > Download SP Metadata**) during erwin Mart Portal configuration.



Add Application

SAML Configuration

Provide Application Metadata

☒ Import Metadata ☐ Import From URL ☐ Manually Enter

 mart-sp-metadata.xml 

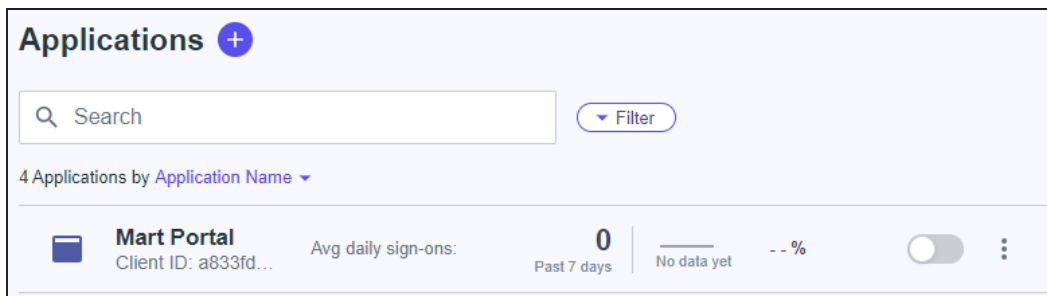
ACS URLs *

+ Add

Entity ID *

Save **Cancel**

- Click **Save**.



Applications 

Filter

4 Applications by **Application Name** ▼

	Mart Portal Client ID: a833fd...	Avg daily sign-ons: Past 7 days	0 No data yet	-- %	☐	
---	--	------------------------------------	-------------------------	------	--------------------------	---

- Click  against your application name to enable user access to your application.
- In the list of applications, click your application name.

SAML with PingIdentity

Mart Portal
Client ID: a833fd2b-e7b2-4bf2-87f3-14024feb820

Overview Configuration Attribute Mappings Policies Access

Protocol SAML Attributes 1 Mapped Policies None Selected Access All Users

App Type
Advanced Configuration (SAML)

Description
Not Set

Client ID
a833fd2b-e7b2-4bf2-87f3-14024feb820

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

17. Click **Attribute Mappings** > > **Add**.

Mart Portal > Edit Attribute Mappings

If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Attribute Mapping + Add

Attributes	PingOne Mappings	Required
saml_subject	User ID	☒
		☐

Save **Cancel**

18. Add another attribute and map as shown in the following image.

Mart Portal > Edit Attribute Mappings

you map the identity provider attributes to the application attributes. The application attributes are listed below.

Attribute Mapping + Add

Attributes	PingOne Mappings	Required
saml_subject	User ID	☒
email	Email Address	☐
group	Group Names	☐

Save **Cancel**

Similarly, you can add a display name here.

19. Click **Save**.
These attributes will be used on the erwin Mart Portal Configuration screen.
20. From the Overview tab, copy **IDP Metadata URL**.

The screenshot displays the 'Overview' tab of a configuration interface. At the top, there are navigation tabs: 'Overview' (selected), 'Configuration', 'Attribute Mappings', 'Policies', and 'Access'. Below these, the 'Client ID' is listed as '715de852-122f-4493-9ef3-b788587daa1d'. The 'Home Page URL' is 'No Home Page Configured', and the 'Signon URL' is 'Default Signon Page'. A section titled 'Connection Details' is expanded, showing the 'Issuer ID' as 'https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d'. The 'Initiate Single Sign-On URL' is shown as 'https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/startssso?spEntityId=https://localhost:8443/MartServerCloud/'. A 'Copy to clipboard' button is overlaid on this URL. The 'IDP Metadata URL' is 'https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/metadata/715de852-122f-4493-9ef3-b788587daa1d'. The 'Single Signon Service' URL is 'https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/sso', and the 'Single Logout Service' URL is 'https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/slo'. At the bottom of the 'Connection Details' section, there are two buttons: 'Download Metadata' and 'Download Signing Certificate'.

Overview Configuration Attribute Mappings Policies Access

Client ID
715de852-122f-4493-9ef3-b788587daa1d

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

Connection Details

Issuer ID
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d

Initiate Single Sign-On URL
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/startssso?spEntityId=https://localhost:8443/MartServerCloud/

IDP Metadata URL
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/metadata/715de852-122f-4493-9ef3-b788587daa1d

Single Signon Service
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/sso

Single Logout Service
https://auth.pingone.com/d6cd149a-e097-48c9-9dd5-733942ef0f7d/saml20/ldap/slo

Download Metadata Download Signing Certificate

21. On the erwin Mart Portal Configuration screen, click the **Authentication** tab, and then follow these steps:
 - a. In the Metadata XML field, paste the copied SAML Metadata URL copied in step 20.
 - b. In the Group Attribute Name, User Email Attribute Name, and User Display Name Attribute Name fields, enter the values that are configured in step 18.

The screenshot shows the 'erwin Mart Portal Configuration' window with the 'Authentication' tab selected. The configuration is for SAML. The 'URL' dropdown is set to 'SAML'. The 'MetaData XML' field is empty. Below these are three optional fields: 'Group Attribute Name', 'User Email Attribute Name', and 'User Display Name Attribute Name'. The 'Authentication Request Signed' checkbox is checked. A 'Download SP Metadata' button is present. At the bottom are four buttons: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

erwin Mart Portal Configuration

Database Mart Portal Advanced **Authentication** Proxy Settings

SAML

URL MetaData XML

Group Attribute Name

User Email Attribute Name

User Display Name Attribute Name

☒ Authentication Request Signed

Download SP Metadata

DOWNLOAD HOSTINFO TEST CONFIGURE CANCEL

The User Email Attribute Name and User Display Name Attribute Name fields are optional.

22. Click **Configure**.

Your erwin Mart Portal is now authenticated via PingIdentity.

Adding Groups in erwin Mart Portal

To add your PingIdentity SAML groups to erwin Mart Portal, follow these steps:

SAML with PingIdentity

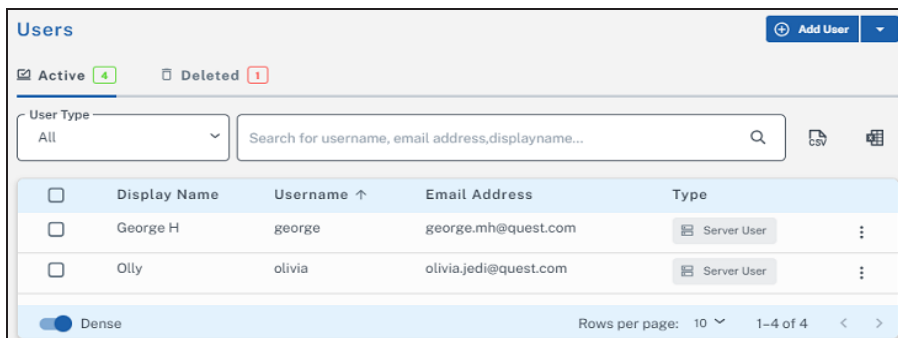
1. Create a CSV file containing the <group_attribute_value> and <group_display_name>.

You can also use the [sample template for groups](#) and replace the sample values with the actual Group Attribute Name and Group Display Name.

	A	B
1	id	displayName
2	01628af3-3e91-43a0-a9df-ad5a6155f62f	QA53
3	Admin	Mart Admin

```
id,displayName
01628af3-3e91-43a0-a9df-ad5a6155f62f,QA53
Admin,Mart Admin
```

2. Log in to the erwin Mart Portal as an administrator.
3. Go to **Application Menu > Users**.
The Users page appears.



Users					Add User
☒ Active	4	☐ Deleted	1		
User Type	Search for username, email address, displayname...				
All					
☐	Display Name	Username ↑	Email Address	Type	
☐	George H	george	george.mh@quest.com	Server User	⋮
☐	Olly	olivia	olivia.jedi@quest.com	Server User	⋮
Dense					Rows per page: 10 1-4 of 4

4. Click **Add User**.
The Add User page appears.

Add User [Back] [Save]

Picture

User Type: Server User

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Username: Enter Username

Display Name: Enter DisplayName

Email Address: Enter EmailAddress [Email Icon]

Confirm Email Address: Enter Confirm email Address [Email Icon]

Password: Enter Password [Password Icon]

☒ User must change password at next login

About Privacy Legal Contact Impressum © 2025 Quest Software, Inc. All rights reserved. Version 15.2

5. Under User Type, select **SAML Group**

Add User [Back] [Save]

Picture

User Type: SAML Group

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Drag and Drop or Select a file
Drop file(s) here or [browse](#)

Allowed text/csv. Max size of 2MB

Group name: Select Group

Email Address: Email Address

6. Drag and drop the CSV file that you created in step 1.
7. Under Group name, select the required group.
8. In the Email Address field, enter your email address.

9. Click **Save**.

The group has been added.

SAML with Okta

Based on your application type, refer to the appropriate section for SAML with Okta configuration:

- [erwin Mart Portal on-cloud](#)
- [erwin Mart Portal on-premises](#)

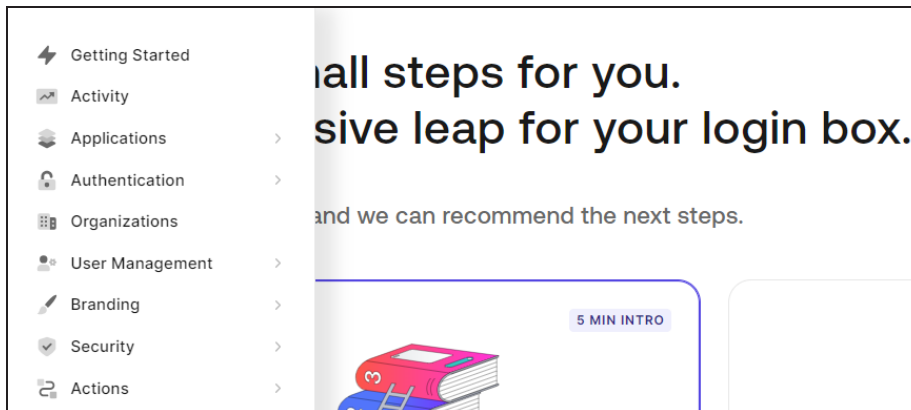
Once SAML configuration is ready, you can add [user groups](#) to erwin Mart Portal.

erwin Mart Portal On-Cloud

Before you configure SAML with Okta, ensure that you have responded to the questionnaire from your Quest Support representative so that they can provide you with the Application Callback URL for your erwin Mart Portal instance. If you did not receive the questionnaire, reach out to your Quest Support representative.

To configure SAML with Okta for erwin Mart Portal on-cloud authentication, follow these steps:

1. Log in to the Okta environment.



2. Click **Applications > Applications > Create application**.

Create application

Name *

My App

You can change the application name later in the application settings.

Choose an application type



Native

Mobile, desktop, CLI and smart device apps running natively.

e.g.: iOS, Electron, Apple TV apps



Single Page Web Applications

A JavaScript front-end app that uses an API.

e.g.: Angular, React, Vue



Regular Web Applications

Traditional web app using redirects.

e.g.: Node.js, Express, ASP.NET, Java, PHP



Machine to Machine Applications

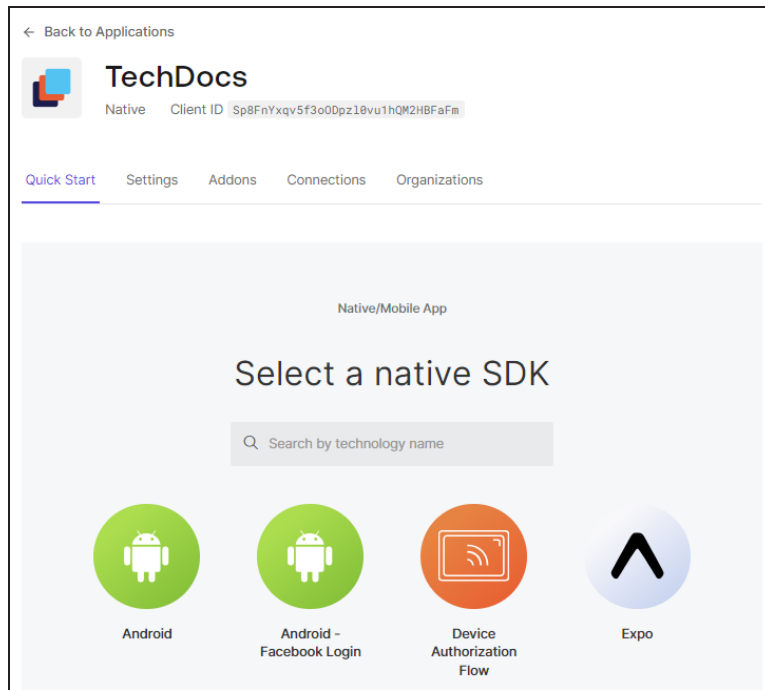
CLIs, daemons or services running on your backend.

e.g.: Shell script

Cancel

Create

3. Enter **Name** for your application.
4. Under application type, select **Regular Web Applications**.
5. Click **Create**.



6. Click **Addons > SAML2 Web App**.

Addon: SAML2 Web App

SettingsUsage

SAML Protocol Configuration Parameters

- SAML Version: 2.0
- Issuer: `urn:dev-6jtub654067xyi4o.us.auth0.com`
- Identity Provider Certificate: [Download Auth0 certificate](#)
- Identity Provider SHA1 fingerprint:
`F0:57:C4:37:C9:16:1D:43:72:FB:C8:47:E4:C9:30:62:BF:9C:B3:29`
- Identity Provider Login URL: <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm>
- Identity Provider Metadata: [Download](#)

Alternatively, you can add a connection parameter:

- <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm?connection=google-oauth2>
- <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm?connection=Username-Password-Authentication>

In this case, Auth0 will redirect users to the specified `connection` and will not display the Login Widget. Make sure you send the SAMLRequest using `HTTP POST`.

7. Click **Settings**.

Addon: SAML2 Web App

Settings Usage

Application Callback URL

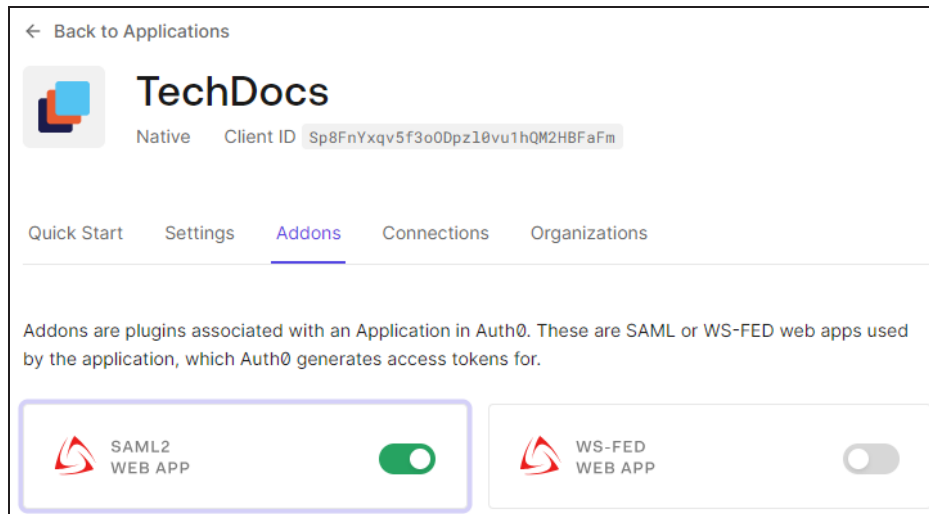
SAML Token will be POSTed to this URL.

Settings

```
3 // "recipient": "http://foo",
4 // "mappings": {
5 //   "user_id": "http://schemas.xmlsoap.org/ws/2005/
6 //   "email": "http://schemas.xmlsoap.org/ws/2005/
7 //   "name": "http://schemas.xmlsoap.org/ws/2005/
8 //   "given_name": "http://schemas.xmlsoap.org/ws/2005/
9 //   "family_name": "http://schemas.xmlsoap.org/ws/2005/
10 //   "upn": "http://schemas.xmlsoap.org/ws/2005/
11 //   "groups": "http://schemas.xmlsoap.org/claims/0
12 // },
13 // "createUpnClaim": true,
14 // "passthroughClaimsWithNoMapping": true,
15 // "mapUnknownClaimsAsIs": false,
16
```

Debug

8. Uncomment line number 4, 6, 11, and 12.
9. On the Addon: SAML2 Web App screen, enter the URL provided by Quest Support team in the Application Callback URL field.
10. Scroll down and click **Enable**. Then, click **Save**.



11. On the menu, click **User Management > Users > Create Users**.

The screenshot shows the 'Create user' form in Okta. It contains the following fields and controls:

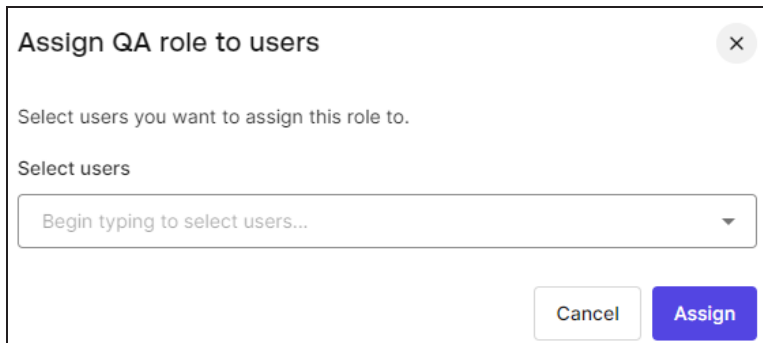
- Email ***: A text input field containing 'email@example.com'. Below it is a red error message: '"email" must be a valid email'.
- Password ***: A password input field with masked characters (asterisks).
- Repeat Password ***: A second password input field with masked characters.
- Connection ***: A dropdown menu currently showing 'Username-Password-Authentication'.
- Buttons**: 'Cancel' and 'Create' buttons at the bottom right.

12. Enter appropriate values in the required fields and click **Create**.
13. On the menu, click **User Management > Users > Roles > Create Roles**.



A dialog box titled "New Role" with a close button (X) in the top right corner. It contains two required fields: "Name *" and "Description *". The "Name" field is currently active, showing a vertical cursor. At the bottom right, there are two buttons: "Cancel" and "Create".

14. Enter appropriate values in the required fields and click **Create**. Then, click **Save**.
15. On the Roles page, click **...**. Then, click **Assign To Users**.



A dialog box titled "Assign QA role to users" with a close button (X) in the top right corner. It contains the text "Select users you want to assign this role to." followed by a "Select users" section. This section has a search input field with the placeholder text "Begin typing to select users..." and a dropdown arrow. At the bottom right, there are two buttons: "Cancel" and "Assign".

16. Under Select users, select the required user and click **Assign**.
17. On the Users page, click a user.
18. On the Details tab, scroll to the Metadata section.

Metadata

user_metadata

```
1 {  
2  
3 }
```

Data that the user has read/write access to (e.g. color_preference, blog_url, etc.)

app_metadata

```
1 {  
2  
3 }
```

Data that the user has read-only access to (e.g. roles, permissions, vip, etc)

Save

19. Under `app_metadata`, add the following and click **Save**.
- ```
"groups": [
 "QA",
 "Modeler"
]
```

```
app_metadata
1 {
2 "groups": [
3 "QA",
4 "Modeler"
5]
6 }
7 }
```

Data that the user has read-only access to (e.g. roles, permissions, vip, etc)

20. On the menu, click **Applications > Applications** and open your application.
21. Scroll down to the Advanced Settings section.

**Advanced Settings** ^

Application Metadata   Device Settings   OAuth   Grant Types   WS-Federation   Certificates   Endpoints

Application metadata are custom string keys and values (max 255 characters each), set on a per application basis. Metadata is exposed in the `Client` object as `client_metadata`, and in Rules as `context.clientMetadata`

**Metadata**

+ Add

10 metadata slots free

| Key                  | Value |
|----------------------|-------|
| There is no metadata |       |

22. Click **Endpoints** and scroll to the **SAML** section.

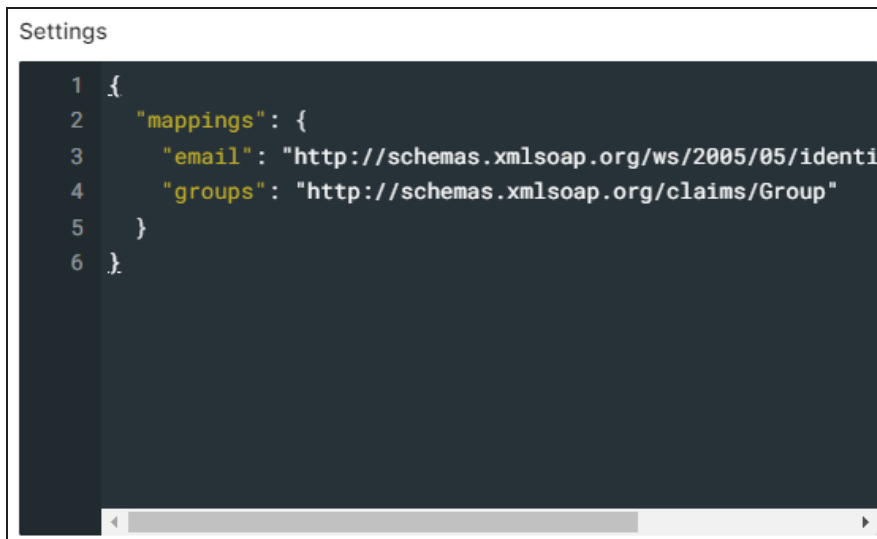


SAML

SAML Protocol URL

SAML Metadata URL

23. Copy the **SAML Metadata URL**.
24. Go to your Okta Auth0 environment. Open your application, and then click **Addons**.
25. Click **SAML2 Web App > Settings**.
26. Copy the email and groups values.



Settings

```
1 {
2 "mappings": {
3 "email": "http://schemas.xmlsoap.org/ws/2005/05/identity
4 "groups": "http://schemas.xmlsoap.org/claims/Group"
5 }
6 }
```

Similarly, you can add a display name here.

27. Share the following details with the Mart Cloud Support team:
  - **Metadata XML URL:** The URL copied in step 23.
  - **Group Attribute Name:** The value configured in step 26.
  - **User Email Attribute Name:** The value configured in step 26.
  - **User Display Name Attribute Name:** The value configured in step 26.

## SAML with Okta

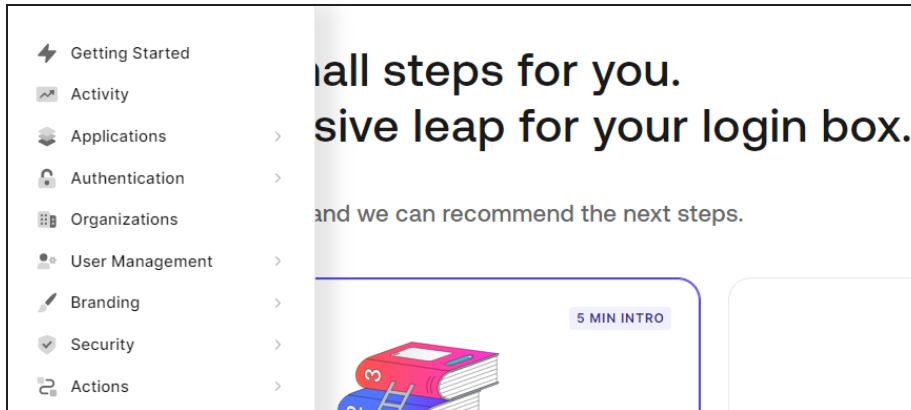
---

Once the support team authenticates erwin Mart Portal for you, you can move to [adding groups in erwin Mart Portal](#) at [https://<your\\_instance>.myerwin.com/MartPortal](https://<your_instance>.myerwin.com/MartPortal).

## erwin Mart Portal On-Premises

To configure SAML with Okta for erwin Mart Portal on-premises authentication, follow these steps:

1. Log in to the Okta environment.



2. Click **Applications > Applications > Create application**.

### Create application

Name \*

My App

You can change the application name later in the application settings.

Choose an application type



**Native**

Mobile, desktop, CLI and smart device apps running natively.

e.g.: iOS, Electron, Apple TV apps



**Single Page Web Applications**

A JavaScript front-end app that uses an API.

e.g.: Angular, React, Vue



**Regular Web Applications**

Traditional web app using redirects.

e.g.: Node.js, Express, ASP.NET, Java, PHP



**Machine to Machine Applications**

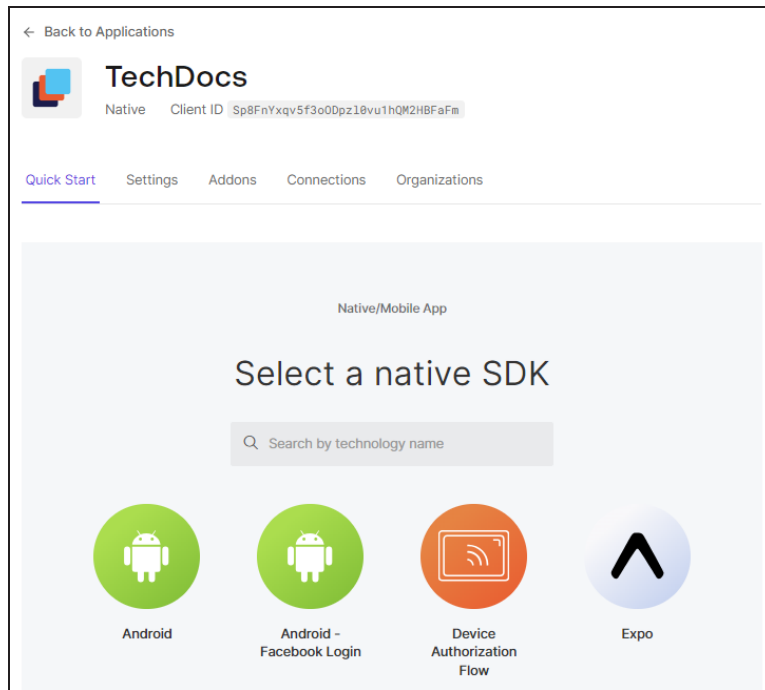
CLIs, daemons or services running on your backend.

e.g.: Shell script

Cancel

Create

3. Enter **Name** for your application.
4. Under application type, select **Regular Web Applications**.
5. Click **Create**.



6. Click **Addons > SAML2 Web App**.

Addon: SAML2 Web App

SettingsUsage

### SAML Protocol Configuration Parameters

- SAML Version: 2.0
- Issuer: urn:dev-6jtub654067xyi4o.us.auth0.com
- Identity Provider Certificate: [Download Auth0 certificate](#)
- Identity Provider SHA1 fingerprint:  
F0:57:C4:37:C9:16:1D:43:72:FB:C8:47:E4:C9:30:62:BF:9C:B3:29
- Identity Provider Login URL: <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm>
- Identity Provider Metadata: [Download](#)

Alternatively, you can add a connection parameter:

- <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm?connection=google-oauth2>
- <https://dev-6jtub654067xyi4o.us.auth0.com/samlp/Sp8FnYxqv5f3oODpzl0vu1hQM2HBFaFm?connection=Username-Password-Authentication>

In this case, Auth0 will redirect users to the specified connection and will not display the Login Widget. Make sure you send the SAMLRequest using HTTP POST.

7. Click **Settings**.

Addon: SAML2 Web App

Settings Usage

Application Callback URL

SAML Token will be POSTed to this URL.

Settings

```
3 // "recipient": "http://foo",
4 // "mappings": {
5 // "user_id": "http://schemas.xmlsoap.org/ws/2005/
6 // "email": "http://schemas.xmlsoap.org/ws/2005/
7 // "name": "http://schemas.xmlsoap.org/ws/2005/
8 // "given_name": "http://schemas.xmlsoap.org/ws/2005/
9 // "family_name": "http://schemas.xmlsoap.org/ws/2005/
10 // "upn": "http://schemas.xmlsoap.org/ws/2005/
11 // "groups": "http://schemas.xmlsoap.org/claims/0
12 // },
13 // "createUpnClaim": true,
14 // "passthroughClaimsWithNoMapping": true,
15 // "mapUnknownClaimsAsIs": false,
```

Debug

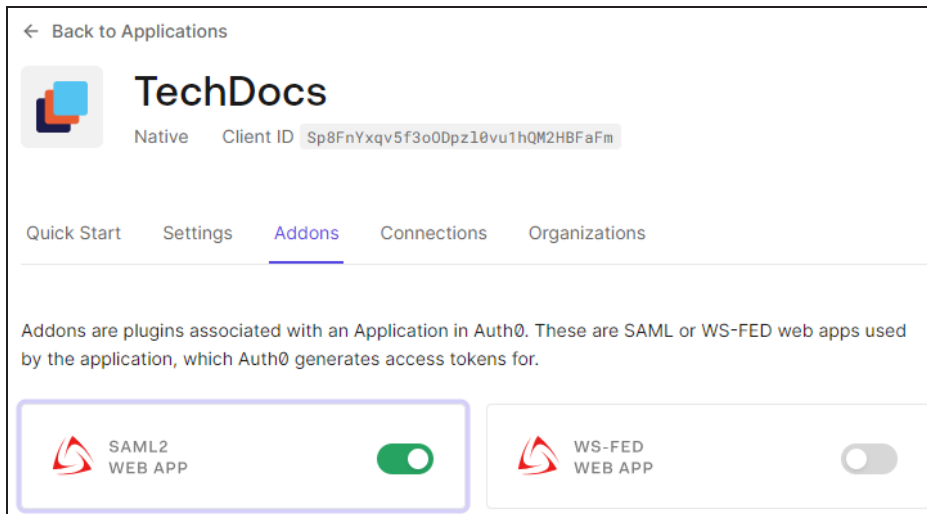
8. Uncomment line number 4, 6, 11, and 12.
9. Download the SP Metadata file (**erwin Mart Portal**) **Configuration > Authentication > Download SP Metadata** and open it in any text editor and copy the URL in the last line as highlighted in the following image.

```

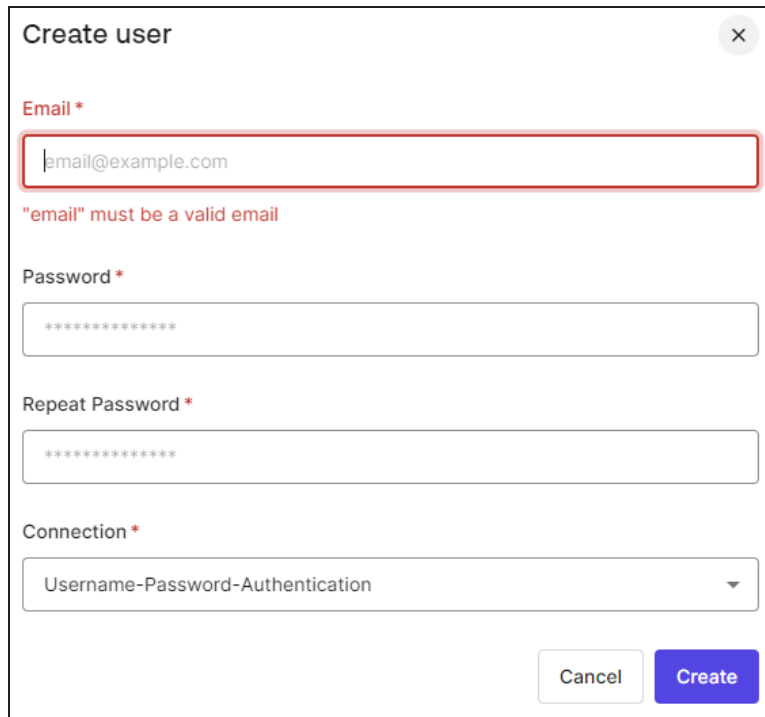
b2Z0d2FyZTEOMAwGA1UECwFZXXJ3aW4xDjAMBGNVBAAMBBWVyd21uMSAwHgYJKoZIhvcNAQkBFhFz
dXBwb3J0QHFI1ZXN0LmNvbTAeFw0yMzAzMTMxMjU2NDZaFw0yNDZaMTI0MjU2NDZaMIIGLMQswCQYD
VQQGEwJVUzBLMAkGA1UECAwCQ0ExFzFASBgnVBAcMC0FsaXNvIFZpZPwvMRcwFQYDVQQKDA5rdWVz
dCBTh2Z0d2FyZTEOMAwGA1UECwFZXXJ3aW4xDjAMBGNVBAAMBBWVyd21uMSAwHgYJKoZIhvcNAQkBFhFz
dXBwb3J0QHFI1ZXN0LmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMxdWbVz
3B1OV0+v28BKJb3UgksXUF+hMIzG9VrV726LuxtdWp2nI991MR5pSNm3xgpBdk2Rrgg7q7kLGye
MMzWIsqgA8GhU25M/xoJaZqIYQAVvtOe9QwDghYYZ2s4K47xFKMp9fUYcwjapfSlfFHWiiccm3WP
3zNOW6JxtDUo5xt9H7xlvV0r9a+Lpet8uH5SbCvYG5TyKS2XYtBnXj2RXLjwqq5av96v8X4b0nKD
q0Hzm0/R6bGTdbNoto64osNOxxvLDzHU8fBkWRtIjMFEPlv7Xco4oX4Lp1fNYcoyju1bf6f6EvG/
FuY8eOECIZ71twsUGmLGWYntKvnFq0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAhI+xpwdNLGbV
vCo72mhg9Giy8396kSve7icX/Ahg6+gZUq9uPpDFhpqBqGprczimQ/Z1fXB4CeRXizWMTNw6pzK
U+X9Es/Nqc+QzdquagxofpxxFNipAWSXz9K95mNfVfYcR+JwuC00ylof1ZZDYnNacOnD1D8F6RtOi
xxqS8lUI8qJj7doJB7XHFgnjZ5Hunqr/owlaBtX6keJGFaQmWt79qDOZPbmrv5g3dUOn7487WbZM
AF0A4H17m2pCeWfa+RUKBCRjPjt8byg0fLXRO24yG1+yDH+sazq5pq3EbTz1119u7ZrNEK6ad70x
zCR991NFs/DqoogQKJV4LKgdQ==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService Binding=
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
"https://localhost:443/MartServerCloud/saml2/SingleLogout"/><md:SingleLogoutService Binding=
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=
"https://localhost:443/MartServerCloud/saml2/SingleLogout"/><md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat><md:NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
</md:NameIDFormat><md:AssertionConsumerService Binding=
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
"https://localhost:443/MartServerCloud/saml2/login/sso/saml2-mart" index="0"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location=
"https://localhost:443/MartServerCloud/saml2/saml2/login/sso/saml2-mart" index="1"/>
</md:SPSSODescriptor></md:EntityDescriptor>

```

10. On the Addon: SAML2 Web App screen, paste the copied URL in the **Application Callback URL** field.
11. Scroll down and click **Enable**. Then, click **Save**.

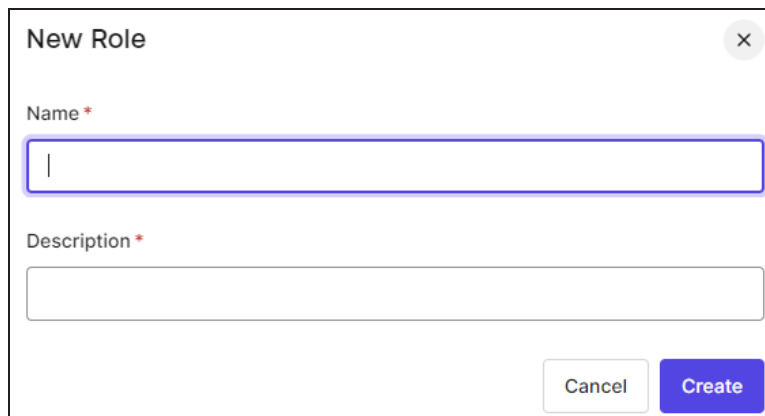


12. On the menu, click **User Management > Users > Create Users**.



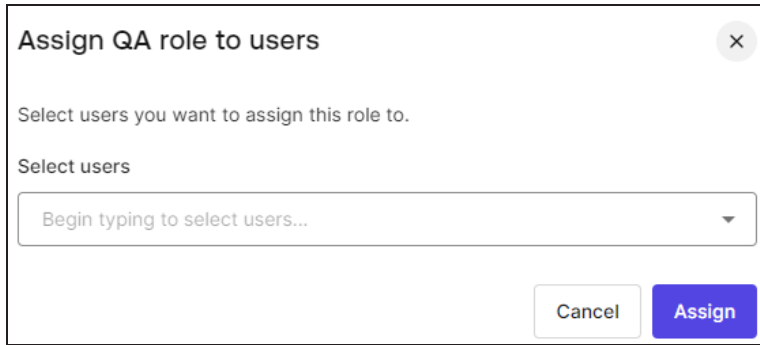
A dialog box titled "Create user" with a close button (X) in the top right corner. It contains four required fields: "Email \*" with the value "email@example.com" and a red error message below it stating "'email' must be a valid email"; "Password \*" with masked text "\*\*\*\*\*"; "Repeat Password \*" with masked text "\*\*\*\*\*"; and "Connection \*" with a dropdown menu showing "Username-Password-Authentication". At the bottom right are "Cancel" and "Create" buttons.

13. Enter appropriate values in the required fields and click **Create**.
14. On the menu, click **User Management > Users > Roles > Create Roles**.



A dialog box titled "New Role" with a close button (X) in the top right corner. It contains two required fields: "Name \*" with an empty text input field and "Description \*" with an empty text input field. At the bottom right are "Cancel" and "Create" buttons.

15. Enter appropriate values in the required fields and click **Create**. Then, click **Save**.
16. On the Roles page, click . Then, click **Assign To Users**.



A dialog box titled "Assign QA role to users" with a close button (X) in the top right corner. The dialog contains the text "Select users you want to assign this role to." followed by a section labeled "Select users". Below this label is a search input field with the placeholder text "Begin typing to select users..." and a downward arrow on the right. At the bottom right of the dialog are two buttons: "Cancel" and "Assign".

17. Under Select users, select the required user and click **Assign**.
18. On the Users page, click a user.
19. On the Details tab, scroll to the Metadata section.

**Metadata**

**user\_metadata**

```
1 {
2
3 }
```

Data that the user has read/write access to (e.g. color\_preference, blog\_url, etc.)

**app\_metadata**

```
1 {
2
3 }
```

Data that the user has read-only access to (e.g. roles, permissions, vip, etc)

**Save**

20. Under `app_metadata`, add the following and click **Save**.
- ```
"groups": [  
  "QA",  
  "Modeler"  
]
```

```
app_metadata
1 {
2   "groups": [
3     "QA",
4     "Modeler"
5   ]
6 }
7 }
```

Data that the user has read-only access to (e.g. roles, permissions, vip, etc)

21. On the menu, click **Applications > Applications** and open your application.
22. Scroll down to the Advanced Settings section.

Advanced Settings ^

Application Metadata Device Settings OAuth Grant Types WS-Federation Certificates Endpoints

Application metadata are custom string keys and values (max 255 characters each), set on a per application basis. Metadata is exposed in the `Client` object as `client_metadata`, and in Rules as `context.clientMetadata`

Metadata

+ Add

10 metadata slots free

Key	Value
There is no metadata	

23. Click **Endpoints** and scroll to the **SAML** section.

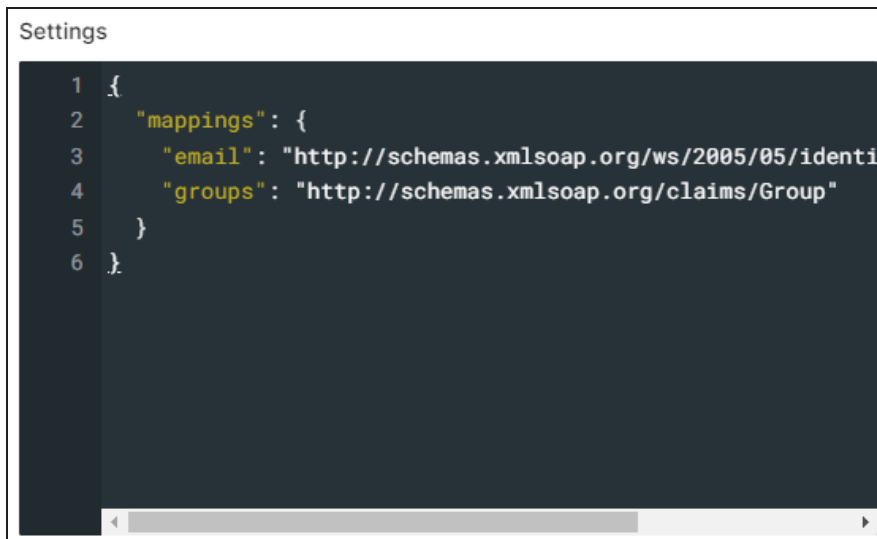


SAML

SAML Protocol URL

SAML Metadata URL

24. Copy the **SAML Metadata URL**.
25. Go to your Okta Auth0 environment. Open your application, and then click **Addons**.
26. Click **SAML2 Web App > Settings**.
27. Copy the email and groups values.



```
1 {  
2   "mappings": {  
3     "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/  
4     "groups": "http://schemas.xmlsoap.org/claims/Group"  
5   }  
6 }
```

Similarly, you can add a display name here.

28. For Mart Portal on-premises, on the erwin Mart Portal Configuration screen, click the **Authentication** tab, and then follow these steps:
 - a. In the Metadata XML field, paste the copied SAML Metadata URL copied in step 24.
 - b. In the Group Attribute Name, User Email Attribute Name, and User Display Name

Attribute Name fields, enter the values that are configured in step 27.

The screenshot shows the 'erwin Mart Portal Configuration' window with the 'Authentication' tab selected. The 'SAML' dropdown is highlighted. Below it, the 'URL' dropdown is set to 'URL' and the 'MetaData XML' field is empty. A group of three text input fields for 'Group Attribute Name', 'User Email Attribute Name', and 'User Display Name Attribute Name' is shown. The 'Authentication Request Signed' checkbox is checked. A 'Download SP Metadata' button is present. At the bottom, there are four buttons: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

The User Email Attribute Name and User Display Name Attribute Name fields are optional.

29. Click **Configure**.

Your erwin Mart Portal is now authenticated via Okta.

Adding Groups in erwin Mart Portal

To add your Okta SAML groups to erwin Mart Portal, follow these steps:

SAML with Okta

1. Create a CSV file containing the <group_attribute_value> and <group_display_name>.

You can also use the [sample template for groups](#) and replace the sample values with the actual Group Attribute Name and Group Display Name.

	A	B
1	id	displayName
2	01628af3-3e91-43a0-a9df-ad5a6155f62f	QA53
3	Admin	Mart Admin

```
id,displayName
01628af3-3e91-43a0-a9df-ad5a6155f62f,QA53
Admin,Mart Admin
```

2. Log in to the erwin Mart Portal as an administrator.

3. Go to **Application Menu > Users**.

The Users page appears.

4. Click **Add User**.

The Add User page appears.

Add User [Back] [Save]

Picture

User Type: Server User

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Username: Enter Username

Display Name: Enter DisplayName

Email Address: Enter EmailAddress [Email Icon]

Confirm Email Address: Enter Confirm email Address [Email Icon]

Password: Enter Password [Password Icon]

☒ User must change password at next login

About Privacy Legal Contact Impressum © 2025 Quest Software, Inc. All rights reserved. Version 15.2

5. Under User Type, select **SAML Group**

Add User [Back] [Save]

Picture

User Type: SAML Group

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Drag and Drop or Select a file
Drop file(s) here or [browse](#)

Allowed text/csv. Max size of 2MB

Group name: Select Group

Email Address: Email Address

6. Drag and drop the CSV file that you created in step 1.
7. Under Group name, select the required group.
8. In the Email Address field, enter your email address.

9. Click **Save**.

The group has been added.

SAML with WSO2

Based on your application type, refer to the appropriate sections for SAML with WSO2 configuration:

- [erwin Mart Portal on-cloud](#)
- [erwin Mart Portal on-premises](#)

Once SAML configuration is ready, you can add [user groups](#) to erwin Mart Portal

erwin Mart Portal On-Cloud

Before you configure SAML with Okta, ensure that you have responded to the questionnaire from your Quest Support representative so that they can provide you with the Reply URL for your instance. If you did not receive the questionnaire, reach out to your Quest Support representative.

To configure WSO2 SAML for erwin Mart Portal on-cloud authentication, follow these steps:

1. Download WSO2 Identity Server [here](#).
2. Extract the installer and open the extracted folder.
3. Run command prompt and run the `wso2server.bat` command.

Ensure that the path for the JAVA_HOME environment variable is configured.

4. Copy the Mgt Console URL, highlighted in the following image.

```

[2023-08-17 16:35:32,097] [ ] INFO {org.wso2.carbon.humantask.core.HumanTaskSchedulerInitializer} - Starting HumanTasks Scheduler
[2023-08-17 16:35:32,106] [ ] INFO {openjpa.Runtime} - Starting OpenJPA 2.2.0-wso2v1
[2023-08-17 16:35:32,150] [ ] INFO {openjpa.jdbc.JDBC} - Using dictionary class "org.apache.openjpa.jdbc.sql.H2Dictionary".
[2023-08-17 16:35:32,816] [ ] INFO {org.wso2.carbon.core.transports.http.HttpTransportListener} - HTTP port : 9763
[2023-08-17 16:35:32,817] [ ] INFO {org.wso2.carbon.core.transports.http.HttpsTransportListener} - HTTPS port : 9443
[2023-08-17 16:35:32,979] [ ] INFO {org.wso2.carbon.bpel.core.ode.integration.BPELSchedulerInitializer} - Starting BPS Scheduler
[2023-08-17 16:35:32,981] [ ] INFO {openjpa.Runtime} - Starting OpenJPA 2.2.0-wso2v1
[2023-08-17 16:35:32,983] [ ] INFO {openjpa.jdbc.JDBC} - Using dictionary class "org.apache.openjpa.jdbc.sql.H2Dictionary" (H2 2.1.210 (2022-01-21.210 (2022-01-17)))
[2023-08-17 16:35:33,032] [ ] INFO {org.wso2.carbon.core.internal.StartupFinalizerServiceComponent} - Server : WSO2 Identity Server-
[2023-08-17 16:35:33,034] [ ] INFO {org.wso2.carbon.core.internal.StartupFinalizerServiceComponent} - WSO2 Carbon started in 50 sec
[2023-08-17 16:35:33,050] [ ] INFO {org.wso2.carbon.healthcheck.api.core.internal.HealthMonitorServiceComponent} - Carbon health monitoring ser
[2023-08-17 16:35:33,634] [ ] INFO {org.wso2.carbon.ui.internal.CarbonUIServiceComponent} - Mgt Console URL : https://localhost:9443/carbon/!
[2023-08-17 16:35:34,045] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - My Account URL : https://localhost:944
[2023-08-17 16:35:34,046] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - Console URL : https://localhost:9443/c
[2023-08-17 16:35:34,047] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - Identity apps common service component
lly.
[2023-08-17 16:35:34,308] [ ] INFO {org.wso2.callhome.CallHomeExecutor} -
.....
The latest update level is 'wso2is-6.1.0.54'.
This consists of 91 updates
applied on top of 'wso2is-6.1.0.0'
[WARNING]
The update level
'wso2is-6.1.0.54' consists of 24 critical security updates applied on top of
'wso2is-6.1.0.0'.
WSO2 strongly recommends to use 'wso2is-6.1.0.54'
distribution in production as soon as possible.

```

5. Open the URL in a web browser and log in using the following credentials:

- **username:** admin
- **password:** admin

6. Under Service Providers, click **Add**.

The screenshot shows the 'Add New Service Provider' form. On the left is a navigation pane with 'Service Providers' selected. The main area has a breadcrumb 'Home > Identity > Service Providers > Add'. Below the title, there are two radio buttons for 'Select Mode': 'Manual Configuration' (selected) and 'File Configuration'. A 'Basic Information' section contains three fields: 'Service Provider Name' (with a hint 'A unique name for the service provider'), 'Description' (with a hint 'A meaningful description about the service provider'), and 'Management Application' (a checkbox with a hint 'If this is enabled, the application can be used to access the server management APIs.'). At the bottom are 'Register' and 'Cancel' buttons.

7. Enter an appropriate Service Provider Name and click **Register**.

The screenshot shows the 'Service Providers' configuration page. The 'Service Provider Name' field now contains 'mart'. The 'Description' field is empty. Under 'Select SP Certificate Type', 'Upload SP certificate' is selected. The 'Application Certificate' section shows a 'Choose File' button and the text 'No file chosen', with a hint 'The certificate (in PEM format) of the application'. The 'SaaS Application' checkbox is unchecked, with a hint 'Applications are by default restricted for usage by users of the service provider's tenant. users of all the tenants.'. The 'Discoverable Application' checkbox is also unchecked, with a hint 'Applications flagged as discoverable are visible for end users.'. The left navigation pane shows 'Entitlement' as the current section.

8. Enter your Reply URL provided by Quest Support.
9. Expand Claim Configuration and click **Use Local Claim Dialect**.
10. Click **Add Claim** and add email address and groups.

The screenshot shows the 'Claim Configuration' dialog box. It has a title bar with an expand/collapse icon and the text 'Claim Configuration'. Inside, there are two radio buttons for 'Select Claim mapping Dialect': 'Use Local Claim Dialect' (selected) and 'Define Custom Claim Dialect'. Below this is a section for 'Requested Claims' with a green plus icon and the text 'Add Claim URI'. This section contains a table with two rows, each with a 'Local Claim' header and a dropdown menu. The first dropdown shows 'http://wso2.org/claims/emailaddress' and the second shows 'http://wso2.org/claims/groups'. At the bottom, there are two dropdown menus: 'Subject Claim URI' (showing '---Select---') and 'Service Provider Claim Dialect' (showing '---Select---'). To the right of the second dropdown is an 'Add' button.

Similarly, you can add a display name here.

11. Under Inbound Authentication Configuration, click **SAML2 Web SSO Configuration > Configure**.
12. Configure properties as shown in the following image.

Register New Service Provider

Edit Service Provider

Issuer *

https://localhost:8443/MartServerCloud

Assertion Consumer URLs *

https://localhost:8443/MartServerCloud/saml2/login/sso/saml2-mart

Add

Delete

Default Assertion Consumer URL *

https://localhost:8443/MartServerCloud/saml2/login/sso/saml2-mart

NameID format

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Certificate Alias

wso2carbon

Response Signing Algorithm *

http://www.w3.org/2000/09/xmldsig#rsa-sha1

Response Digest Algorithm *

http://www.w3.org/2000/09/xmldsig#sha1

Assertion Encryption Algorithm *

http://www.w3.org/2001/04/xmlenc#aes256-cbc

Key Encryption Algorithm *

http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p

☒ Enable Response Signing

☐ Enable Signature Validation in Authentication Requests and Logout Requests

☐ Enable Assertion Encryption

☒ Enable Single Logout

SLO Response URL

Single logout response accepting endpoint

SLO Request URL

Single logout request accepting endpoint

Logout Method

☒ Back-Channel Logout

☐ Front-Channel Logout (HTTP Redirect Binding)

☐ Front-Channel Logout (HTTP POST Binding)

☒ Enable Attribute Profile

☒ Include Attributes in the Response Always

13. Click **Download IDP Metadata**.
14. Click **Register**.
15. Under Users and Roles, click **Add > Add New User**. Then, enter the necessary information.

Home > Add User

Add New User

Step 1: Enter Username and Password

Enter username

Domain

Username*

Password*

Confirm Password*

16. Under Users and Roles, click **Add > Add New Role**. Then, enter the necessary information.

Home > Add New Role

Add New Role

Step 1: Enter Role Details

Enter role details

Domain

Role Name*

17. Click **Finish**.

Home

Roles

Search Roles

Select Domain: ALL-USER-STORE-DOMAINS ▾

Enter Role Name Pattern (* for all): * Search Roles

Name	Actions
admin	Rename Permissions Assign Users View Users Delete
demo_role	Rename Permissions Assign Users View Users Delete
Internal/admin	Assign Users View Users
Internal/everyone	Permissions
Internal/system	Rename Permissions Assign Users View Users Delete
martadmin	Rename Permissions Assign Users View Users Delete

18. For the required role, click **Assign Users**.

Home > Users of Role

User List of Role : demo_role

Enter Username Pattern (* for all) * Search Users

Unassigned Users

Select all on this page | Unselect all on this page

☐ admin

☒ demo

☐ sameer

Update Finish Cancel

19. Click **Finish**.

20. Share the following details with the Mart Cloud Support team:

- IDP Metadata File
- Group Attribute Name
- User Email Attribute Name
- User Display Name Attribute Name

Once the support team authenticates erwin Mart Portal for you, you can move to [adding groups](#) in erwin Mart Portal at https://<your_instance>.myerwin.com/MartPortal.

erwin Mart Portal On-Premises

To configure WSO2 SAML for erwin Mart Portal on-premises authentication, follow these steps:

1. Download WSO2 Identity Server [here](#).
2. Extract the installer and open the extracted folder.
3. Run command prompt and run the `wso2server.bat` command.

Ensure that the path for the JAVA_HOME environment variable is configured.

4. Copy the Mgt Console URL, highlighted in the following image.

```
[2023-08-17 16:35:32,097] [ ] INFO {org.wso2.carbon.humantask.core.HumanTaskSchedulerInitializer} - Starting HumanTasks Scheduler
[2023-08-17 16:35:32,106] [ ] INFO {openjpa.Runtime} - Starting OpenJPA 2.2.0-wso2v1
[2023-08-17 16:35:32,150] [ ] INFO {openjpa.jdbc.JDBC} - Using dictionary class "org.apache.openjpa.jdbc.sql.H2Dictionary".
[2023-08-17 16:35:32,816] [ ] INFO {org.wso2.carbon.core.transports.http.HttpTransportListener} - HTTP port : 9763
[2023-08-17 16:35:32,817] [ ] INFO {org.wso2.carbon.core.transports.http.HttpTransportListener} - HTTPS port : 9443
[2023-08-17 16:35:32,979] [ ] INFO {org.wso2.carbon.bpel.core.ode.integration.BPELSchedulerInitializer} - Starting BPS Scheduler
[2023-08-17 16:35:32,981] [ ] INFO {openjpa.Runtime} - Starting OpenJPA 2.2.0-wso2v1
[2023-08-17 16:35:32,983] [ ] INFO {openjpa.jdbc.JDBC} - Using dictionary class "org.apache.openjpa.jdbc.sql.H2Dictionary" (H2 2.1.210 (2022-01-21.210 (2022-01-17))).
[2023-08-17 16:35:33,032] [ ] INFO {org.wso2.carbon.core.internal.StartupFinalizerServiceComponent} - Server : WSO2 Identity Server-
[2023-08-17 16:35:33,034] [ ] INFO {org.wso2.carbon.core.internal.StartupFinalizerServiceComponent} - WSO2 Carbon started in 50 sec
[2023-08-17 16:35:33,050] [ ] INFO {org.wso2.carbon.healthcheck.api.core.internal.HealthMonitorServiceComponent} - Carbon health monitoring ser
[2023-08-17 16:35:33,634] [ ] INFO {org.wso2.carbon.ui.internal.CarbonUIServiceComponent} - Mgt Console URL : https://localhost:9443/carbon/!
[2023-08-17 16:35:34,045] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - My Account URL : https://localhost:944
[2023-08-17 16:35:34,046] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - Console URL : https://localhost:9443/c
[2023-08-17 16:35:34,047] [ ] INFO {org.wso2.identity.apps.common.internal.AppsCommonServiceComponent} - Identity apps common service component
lly.
[2023-08-17 16:35:34,308] [ ] INFO {org.wso2.callhome.CallHomeExecutor} -
.....
The latest update level is 'wso2is-6.1.0.54'.
This consists of 91 updates
applied on top of 'wso2is-6.1.0.0'
[WARNING]
The update level
'wso2is-6.1.0.54' consists of 24 critical security updates applied on top of
'wso2is-6.1.0.0'.
WSO2 strongly recommends to use 'wso2is-6.1.0.54'
distribution in production as soon as possible.
```

5. Open the URL in a web browser and log in using the following credentials:
 - **username:** admin
 - **password:** admin
6. Under Service Providers, click **Add**.

Home > Identity > Service Providers > Add

Add New Service Provider

Select Mode

☒ Manual Configuration

☐ File Configuration

Basic Information

Service Provider Name:*

A unique name for the service provider

Description:

A meaningful description about the service provider

Management Application: ☐

If this is enabled, the application can be used to access the server management APIs.

7. Enter an appropriate Service Provider Name and click **Register**.

Home > Identity > Service Providers

Service Providers

Basic Information

Service Provider Name:*

A unique name for the service provider

Description:

A meaningful description about the service provider

Select SP Certificate Type

☐ Use SP JWKS endpoint

☒ Upload SP certificate

Application Certificate:

No file chosen

The certificate (in PEM format) of the application

SaaS Application ☐

Applications are by default restricted for usage by users of the service provider's tenant. users of all the tenants.

Discoverable Application ☐

Applications flagged as discoverable are visible for end users.

8. Click Upload SP certificate and upload the myerwin.mart.crt file available at C:\Program Files\erwin\Mart Portal\Apache\.

Select SP Certificate Type	☐ Use SP JWKS endpoint ☒ Upload SP certificate
Application Certificate:	<pre>-----BEGIN CERTIFICATE----- MIIDnzCCAocCFD8SioP0B1Vqb8sxm1R6/BfVGTtyMA0GCSqGSIb3DQEBCwUAMIGL MQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExFDASBgNVBAcMC0FsaXNvIFZpZWpv MRcwFQYDVQQKDA5RdWVzdCBTb2Z0d2FyZTE0MAwGA1UECwwFZXJ3aW4xZjAMBGNV BAMMBWVyd21uMSAwHgYJKoZIhvcNAQkBFhFzdXBwb3J0QHF1ZXN0LmNvbTAeFw0y MzAzMTMxMjU2NDZaFw0yNDZaMTIxMjU2NDZaMIGLMQswCQYDVQQGEwJVUzELMAkG A1UECAwCQ0ExFDASBgNVBAcMC0FsaXNvIFZpZWpvMRcwFQYDVQQKDA5RdWVzdCBT </pre> Choose File myerwin.mart.crt The certificate (in PEM format) of the application
SaaS Application	☐ Applications are by default restricted for usage by users of the service provider's users of all the tenants.
Discoverable Application	☐ Applications flagged as discoverable are visible for end users.
Access URL	Access URL for the Service Provider
Logo URL	Link to the logo of the Service Provider. A 150x150px or higher square image is r
Logout Return URL or regex	External return to URL during a direct IdP logout
Management Application	☐ If this is enabled, the application can be used to access the server manage
Claim Configuration	

9. Expand Claim Configuration and click **Use Local Claim Dialect**.
10. Click **Add Claim** and add email address and groups.

The screenshot shows the 'Claim Configuration' dialog box. It has a title bar with an expand/collapse icon and the text 'Claim Configuration'. Inside, there are two radio buttons for 'Select Claim mapping Dialect': 'Use Local Claim Dialect' (selected) and 'Define Custom Claim Dialect'. Below this is a section for 'Requested Claims' with a green plus icon and the text 'Add Claim URI'. A table with the header 'Local Claim' contains two rows: the first row has the value 'http://wso2.org/claims/emailaddress' and a dropdown arrow; the second row has the value 'http://wso2.org/claims/groups' and a dropdown arrow. At the bottom, there are two dropdown menus: 'Subject Claim URI:' with the value '---Select---' and 'Service Provider Claim Dialect:' with the value '---Select---'. To the right of the second dropdown is an 'Add' button.

Similarly, you can add a display name here.

11. Under Inbound Authentication Configuration, click **SAML2 Web SSO Configuration > Configure**.
12. Configure properties as shown in the following image.

Register New Service Provider

Edit Service Provider

Issuer *

https://localhost:8443/MartServerCloud

Assertion Consumer URLs *

https://localhost:8443/MartServerCloud/saml2/login/sso/saml2-mart

Add

Delete

Default Assertion Consumer URL *

https://localhost:8443/MartServerCloud/saml2/login/sso/saml2-mart

NameID format

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Certificate Alias

wso2carbon

Response Signing Algorithm *

http://www.w3.org/2000/09/xmldsig#rsa-sha1

Response Digest Algorithm *

http://www.w3.org/2000/09/xmldsig#sha1

Assertion Encryption Algorithm *

http://www.w3.org/2001/04/xmlenc#aes256-cbc

Key Encryption Algorithm *

http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p

☒ Enable Response Signing

☐ Enable Signature Validation in Authentication Requests and Logout Requests

☐ Enable Assertion Encryption

☒ Enable Single Logout

SLO Response URL

Single logout response accepting endpoint

SLO Request URL

Single logout request accepting endpoint

Logout Method

☒ Back-Channel Logout

☐ Front-Channel Logout (HTTP Redirect Binding)

☐ Front-Channel Logout (HTTP POST Binding)

☒ Enable Attribute Profile

☒ Include Attributes in the Response Always

13. Click **Download IDP Metadata**.
14. Click **Register**.
15. Under Users and Roles, click **Add > Add New User**. Then, enter the necessary information.

Home > Add User

Add New User

Step 1: Enter Username and Password

Enter username

Domain

Username*

Password*

Confirm Password*

16. Under Users and Roles, click **Add > Add New Role**. Then, enter the necessary information.

Home > Add New Role

Add New Role

Step 1: Enter Role Details

Enter role details

Domain

Role Name*

17. Click **Finish**.

Home

Roles

Search Roles

Select Domain: ALL-USER-STORE-DOMAINS ▾

Enter Role Name Pattern (* for all): * Search Roles

Name	Actions
admin	Rename Permissions Assign Users View Users Delete
demo_role	Rename Permissions Assign Users View Users Delete
Internal/admin	Assign Users View Users
Internal/everyone	Permissions
Internal/system	Rename Permissions Assign Users View Users Delete
martadmin	Rename Permissions Assign Users View Users Delete

18. For the required role, click **Assign Users**.

Home > Users of Role

User List of Role : demo_role

Enter Username Pattern (* for all) * Search Users

Unassigned Users

Select all on this page | Unselect all on this page

☐ admin

☒ demo

☐ sameer

Update Finish Cancel

19. Click **Finish**.
20. On the erwin Mart Portal configuration screen, click the **Authentication** tab, and then follow these steps:
- In the Metadata XML field, select File, and then add the IDP metadata file downloaded in step 13.
 - In the Group Attribute Name, User Email Attribute Name, and User Display Name Attribute Name fields, enter the values that are configured in step 10.

The screenshot shows the 'erwin Mart Portal Configuration' window with the 'Authentication' tab selected. The 'SAML' protocol is chosen from the dropdown menu. The 'File' option is selected for the metadata source, with a 'MetaData XML' button next to it. There are three input fields for attribute names: 'Group Attribute Name', 'User Email Attribute Name', and 'User Display Name Attribute Name'. The 'Authentication Request Signed' checkbox is checked. A 'Download SP Metadata' button is present. At the bottom, there are four buttons: 'DOWNLOAD HOSTINFO', 'TEST', 'CONFIGURE', and 'CANCEL'.

erwin Mart Portal Configuration

Database Mart Portal Advanced **Authentication** Proxy Settings

SAML

File MetaData XML

Group Attribute Name

User Email Attribute Name

User Display Name Attribute Name

☒ Authentication Request Signed

Download SP Metadata

DOWNLOAD HOSTINFO TEST CONFIGURE CANCEL

The User Email Attribute Name and User Display Name Attribute Name fields are optional.

21. Click **Configure**.

Your erwin Mart Portal is now authenticated via WSO2.

Adding Groups in erwin Mart Portal

To add your WSO2 SAML groups to erwin Mart Portal, follow these steps:

SAML with WSO2

1. Create a CSV file containing the <group_attribute_value> and <group_display_name>.

You can also use the [sample template for groups](#) and replace the sample values with the actual Group Attribute Name and Group Display Name.

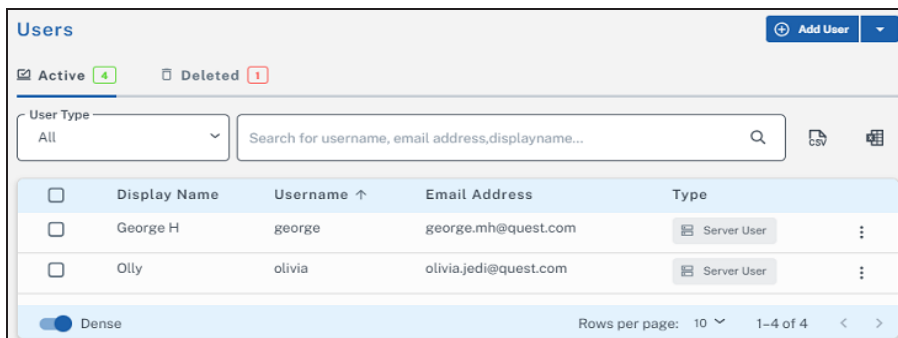
	A	B
1	id	displayName
2	01628af3-3e91-43a0-a9df-ad5a6155f62f	QA53
3	Admin	Mart Admin

```
id,displayName
01628af3-3e91-43a0-a9df-ad5a6155f62f,QA53
Admin,Mart Admin
```

2. Log in to the erwin Mart Portal as an administrator.

3. Go to **Application Menu > Users**.

The Users page appears.



Users				Add User
☒ Active 4	☐ Deleted 1			
User Type All	Search for username, email address, displayname...			
☐	Display Name	Username ↑	Email Address	Type
☐	George H	george	george.mh@quest.com	Server User
☐	Olly	olivia	olivia.jedi@quest.com	Server User
☒ Dense				Rows per page: 10 1-4 of 4

4. Click **Add User**.

The Add User page appears.

Add User [Back] [Save]

Picture

User Type: Server User

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Username: Enter Username

Display Name: Enter DisplayName

Email Address: Enter EmailAddress [Email Icon]

Confirm Email Address: Enter Confirm email Address [Email Icon]

Password: Enter Password [Password Icon]

☒ User must change password at next logon

About Privacy Legal Contact Impressum © 2025 Quest Software, Inc. All rights reserved. Version 15.2

5. Under User Type, select **SAML Group**

Add User [Back] [Save]

Picture

User Type: SAML Group

Drag and Drop or Select a file
Allowed *.jpeg, *.jpg, *.jif, *.png. Max size of 1MB
A default image is set automatically when there is no image.

Details

Drag and Drop or Select a file
Drop file(s) here or [browse](#)

Allowed text/csv. Max size of 2MB

Group name: Select Group

Email Address: Email Address

6. Drag and drop the CSV file that you created in step 1.
7. Under Group name, select the required group.
8. In the Email Address field, enter your email address.

9. Click **Save**.

The group has been added.

Initializing erwin Mart Portal and erwin ER360

To start using erwin Mart Portal and erwin ER360, you first need to initialize the database. You can initialize the database using a database authenticated user.

Before you proceed, verify that you have installed a DBMS, created the database, and configured Mart Portal. If the application is already initialized, the Login page appears.

erwin Mart Portal

When you open erwin Mart Portal for the first time, the Initialize Mart Portal page appears.

If you are using Mart Portal as a Windows service, ensure that the service is started. If not, from the Windows Start menu, click **erwin > Start as Service** to start the Mart Portal. A Windows command prompt window appears and indicates when the server starts.

To initialize mart, follow these steps:

Initializing Mart

1. On the Windows Start Menu, click **erwin** > **erwin Mart Portal**.

erwin Mart Portal opens in your default browser.

Welcome to Mart Portal
Empower data model governance! Quest

Initialize Mart Portal

Username
Username

Password
Password

Confirm Password
Confirm Password

Email Address
Email Address

Mart Roles
Select a Mart role

Table Spaces
Select a table space

Index Table Spaces
Select a index table space

☐ I read, understand, and accept the [Terms of Use](#), [Privacy Policy](#), [Software Transaction Agreement](#), and [Data Processing Addendum](#).

Initialize

2. Complete the following fields:

Field	Description	Additional Information
Username	Specifies the username with which you want to access the Mart. If you are using a Windows-authenticated user, enter the name in the <domain name>/<username> format.	

Field	Description	Additional Information
Password	Specifies the password for the username	A password must fulfil the following criteria: ♦ Contains at least 1 lowercase character ♦ Contains at least 1 uppercase character ♦ Contains at least 1 number ♦ Is minimum 6 characters in length ♦ Is maximum 130 characters in length Apart from the above criteria, special characters are optional.
Confirm Password	Confirms the password that you entered in the previous field.	
Email Address	Specifies the email address for the user account that you are creating.	
Mart Roles	Specifies the database role that grants privileges to	

Initializing Mart

Field	Description	Additional Information
	manage models, users, and repository access in Mart. For example, MMINSTALL.	
Table Spaces	Specifies the default storage location for Mart data objects such as models and metadata. For example, MMDATA.	
Index Table Spaces	Specifies the storage location for database indexes to optimize query performance and retrieval. For example, MMINDEX.	

3. Click **Initialize**.

The username is added as an administrator of Mart, the Mart is initialized, and the Login page appears. Initializing is a one-time task. After initialization, the user who initialized must log in first. Later, any other user who wants to use erwin Mart Portal can log in.

The username that is entered here is an application-level user and not a database user. Remember the password that you have entered here. Without the password you cannot log in to erwin Mart Portal for the first time.

In the previous releases, only a server user was allowed to initialize a Mart. From release r9.6, a Windows-authenticated user can also initialize a Mart. Further, a Windows-authenticated user can log in to a Mart as a Windows user.

erwin ER360

When you open erwin ER360 for the first time, the Initialize ER360 page appears.

To initialize erwin ER360, follow these steps:

1. On the Windows Start Menu, click **erwin** > **erwin ER360**.
erwin ER360 opens in your default browser.

Initializing Mart

**Initialize ER360**
Collaborate to share models and metadata!

Initialize

☐ I read, understand, and accept the [Terms of Use](#), [Privacy Policy](#), [Software Transaction Agreement](#), and [Data Processing Addendum](#).

→ Initialize

2. Complete the following fields:

Field	Description	Additional Information
Username	Specifies the username with which you want to access the application. If you are using a Windows-authenticated user, enter the name in the <domain name>/<user-name> format.	

Field	Description	Additional Information
Password	Specifies the password for the username	A password must fulfil the following criteria: - Contains at least 1 lowercase character - Contains at least 1 uppercase character - Contains at least 1 number - Is minimum 6 characters in length - Is maximum 130 characters in length Apart from the above criteria, special characters are optional.
Confirm Password	Confirms the password that you entered in the previous field.	
Email Address	Specifies the email address for the user account that you are creating.	
ER360 Roles	Specifies the database role that grants privileges to manage models, users, and repository access in Mart. For example, MMINSTALL.	
Table Spaces	Specifies the default storage location for Mart data objects such as models and metadata. For example, MMDATA.	
Index Table Spaces	Specifies the storage location for database indexes to optimize query performance and retrieval. For example, MMINDEX.	
License	Specifies your erwin ER360 license code.	If you need help with the license code, contact your license administrator.

Initializing Mart

Field	Description	Additional Information
		You can initialize erwin ER360 with an offline license. For more information on offline licenses, contact license support .

3. Select the terms of use, privacy policy, and software transaction agreement check box.
4. Click **Initialize**.

The username is added as an administrator of ER360, ER360 is initialized, and the Login page appears. Initializing is a one-time task. After initialization, the user who initialized must log in first. Later, any other user who wants to use erwin ER360 can log in.

Logging in to erwin Mart Portal and Configuring Settings

After the Mart is initialized, the user who initialized must log in first. When you log in for the first time, configure it according to your requirements. You can configure the following settings:

- Default profile for the model creator
- Default selector for user
- Email notification
- Device tracking

To log in to mart, follow these steps:

1. On the Windows Start Menu, click **erwin > erwin Mart Portal**.

The log in page appears.

2. Enter the credentials with which you initialized the mart and log in.

If you enter an incorrect password five consecutive times, your account will be locked for five minutes (300 seconds) by default. To change the default lock out time, refer to the Change [Default Account Lockout Duration](#) section.

3. On the application menu, click  **Settings**.
4. Complete the following fields:

Default profile for model creator

Specifies the profile that is assigned to a user on a model. This profile is assigned whenever a user creates a model and saves it to Mart for the first time. The user inherits the permissions of the default profile selected here on the model that is saved. For example, suppose that User1 is assigned with Modeler profile and the System Administrator selects Architect as the default profile for model creator. If User1 creates Model1 and saves it to Mart, for Model1, User1 inherits the permissions of Architect. Now, suppose that the System Administrator selects Viewer as the default profile for model creator, and suppose that User1 creates Model2 and saves it to Mart. For Model2, User1 inherits the permissions of Viewer.

Default Selector for User

Log In to [%=General.erwin Mart Portal%] and Configure Settings

Specifies whether the default display selector for users is username, email address, or both. Based on the settings here, users' username and/or email is displayed in the Permissions module.

Use SMTP Settings

Specifies whether SMTP settings are configured for email notification through the application.

SMTP host name

Specifies the name of the SMTP host. Enter the name in the mail.domain.com format. Notification emails are sent from this server.

Port number

Specifies the port number of the SMTP server. The default port number is 25. If your company is using an alternate port number for the mail server, specify that port number.

Authenticate

Specifies whether transactions with the SMTP server are authenticated. Select the check box to authenticate.

Use TLS Connection

Specifies whether transactions with the SMTP server use a Transport layer Security (TLS). If you intend to use a TLS connection, ensure that the User name and Administrator email correspond to each other.

Select this option only if you want to use a TLS connection.

Username

Specifies the user name to authenticate the SMTP server. Select the Authenticate check box to enable authentication.

Password

Specifies the password to authenticate the SMTP server. Select the Authenticate check box to enable authentication.

Administrator email

Specifies the email ID of the Mart administrator. Notifications to Mart users are sent from this ID.

No-reply email from

Specifies the email ID from which administrative emails such as the password reset email are sent.

Enable Device Tracking

Specifies whether the devices on which you log in to your mart account are tracked and logged.

5. Click **Submit**.

Mart options are configured.

If SMTP server is not configured, an Administrator can reset a user's password manually via the Users Page. On the Users page, select a user and click . Enter a new password and click **Submit**.

To log in as a Windows-authenticated user, follow these steps:

This procedure describes how to enable a Windows-authenticated user log in to a Mart that is already initialized. Use this procedure if the Mart is initialized with either a server user or a Windows-authenticated user.

1. In erwin Mart Portal configuration, on the Authentication tab, ensure that you have provided Active Directory details.
2. While adding users, search and add the required user corresponding to the necessary Windows user.

Now, the Windows-authenticated user can log in to erwin Mart Portal by providing the user name in the <domain name>/<user name> format.

A local Windows user who does not belong to an Active Directory group cannot log in to the Mart as a Windows user.

Use a Pluggable Database

This information applies to Oracle 12c.

You can use the pluggable database concept of Oracle 12c and create multiple Marts of the same Mart release in a single Oracle instance. For example, you can create two pluggable databases `erwin_test` and `erwin_production` in an Oracle global database `erwin`. You can configure these databases with the Mart Portal one after the other and connect to one of them at a time.

Follow these steps to use multiple pluggable databases:

Log In to [%=General.erwin Mart Portal%] and Configure Settings

1. Create multiple pluggable databases, for example, erwin_test and erwin_production.
2. Install erwin Mart Portal for the first pluggable database, for example, erwin_test.
3. Initialize the Mart for the first pluggable database, erwin_test. For more information on how to initialize the Mart, see the Initialize an Oracle Mart topic.
4. Log in to the Mart and create the models that you want to store in the test Mart.
5. To use the second pluggable database, follow these steps:
 - a. Stop the Mart Portal or the Mart Portal service.
 - b. Repeat Steps 1, 2, and 3 for the second pluggable database, erwin_production.
 - c. Start the Mart Portal or the Mart Portal service.
 - d. Log in to the Mart and create the models as required.

Logging in to erwin ER360 and Configure Settings

After the erwin ER360 is initialized, the user who initialized must log in first. When you log in for the first time, configure it according to your requirements. You can configure the following settings:

- Default user selector
- Email notification
- Device tracking
- Search permissions
- License

To log in to ER360, follow these steps:

1. On the Windows Start Menu, click **erwin** > erwin ER360.
The log in page appears.
2. Enter the credentials with which you initialized ER360 and log in.

If you enter an incorrect password five consecutive times, your account will be locked for five minutes (300 seconds) by default. To change the default lock out time, refer to the Change [Default Account Lockout Duration](#) section.

3. On the application menu, click Settings.
4. Complete the following fields:

Default User Selector

Specifies whether the default display selector for users is username, email address, or both. Based on the settings here, users' username and/or email is displayed in the Permissions module.

Use SMTP Settings

Specifies whether SMTP settings are configured for email notification through the application.

SMTP host name

Logging in to [%=General.erwin ER360%]

Specifies the name of the SMTP host. Enter the name in the mail.domain.com format. Notification emails are sent from this server.

Port number

Specifies the port number of the SMTP server. The default port number is 25. If your company is using an alternate port number for the mail server, specify that port number.

Authenticate

Specifies whether transactions with the SMTP server are authenticated. Select the check box to authenticate.

Use TLS Connection

Specifies whether transactions with the SMTP server use a Transport layer Security (TLS). If you intend to use a TLS connection, ensure that the User name and Administrator email correspond to each other.

Select this option only if you want to use a TLS connection.

Username

Specifies the user name to authenticate the SMTP server. Select the Authenticate check box to enable authentication.

Password

Specifies the password to authenticate the SMTP server. Select the Authenticate check box to enable authentication.

Administrator email

Specifies the email ID of the Mart administrator. Notifications to Mart users are sent from this ID.

No-reply email from

Specifies the email ID from which administrative emails such as the password reset email are sent.

Enable Device Tracking

Specifies whether the devices on which you log in to your mart account are tracked and logged.

License

Logging in to [%=General.erwin ER360%]

Specifies your erwin ER360 license code that you used to initialize the application.
You can change and validate the license code here.

5. Click **Save**.

erwin ER360 options are configured.

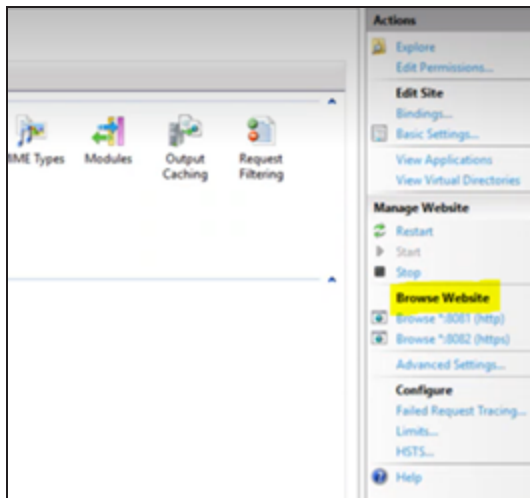
If SMTP server is not configured, an Administrator can reset a user's password manually via the Users Page. On the Users page, select a user and click . Enter a new password and click **Submit**.

Enabling IIS

In IIS-enabled environments, erwin Mart Portal and the configuration will work automatically.

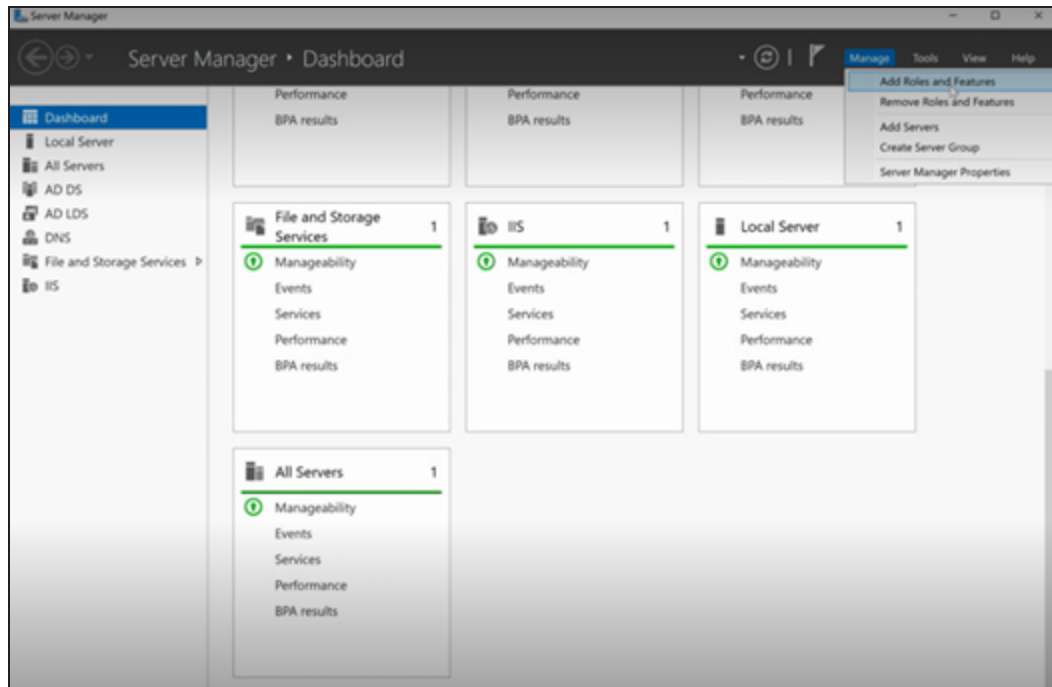
For environments where IIS is not enabled, to enable IIS, follow these steps:

1. On the machine where you have installed and configured erwin Mart Portal, open Internet Information Services (IIS) Manager.
2. Under Browse Website, click the appropriate option.



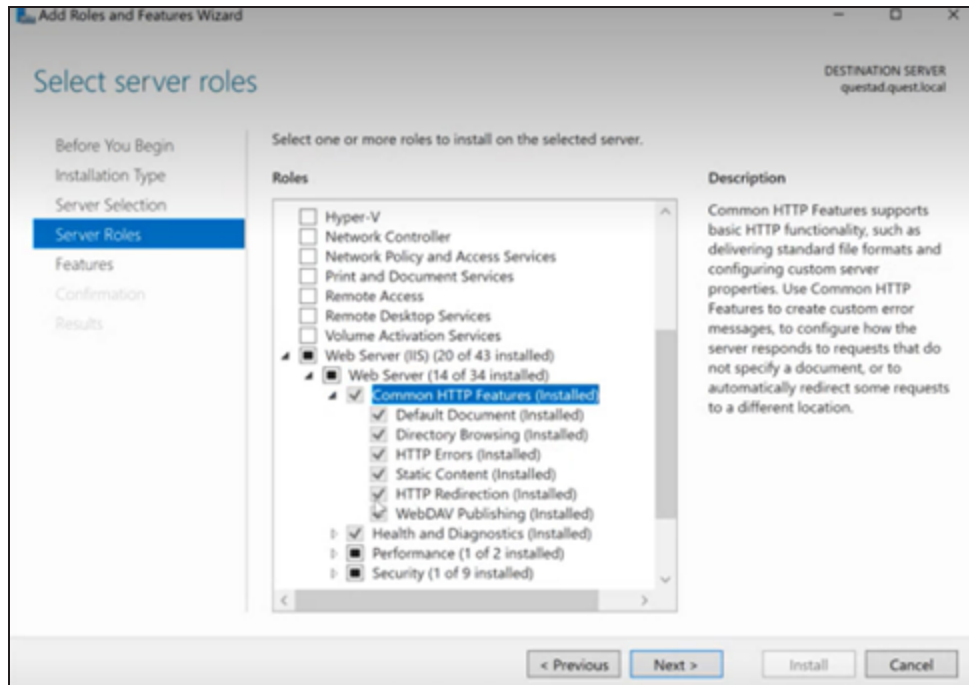
3. Open Server Manager and click **Manage**.

Enabling IIS



4. Click **Add Roles and Features**.

The Add Roles and Features Wizard appears.

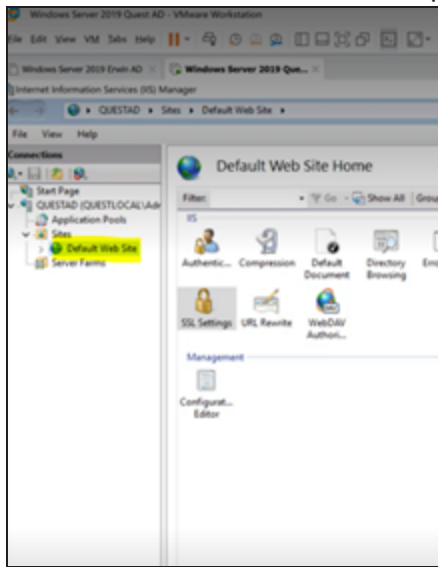


Follow these steps:

1. On the Before you Begin tab, click **Next**.
2. On the Installation Type tab, click **Role-based or Feature-based Installation**.
3. On the Server Selection tab, click **Default**.
4. On the Server Roles tab, select **Web Server (IIS) > Common HTTP Features (Installed)**. Also, ensure that **HTTP Redirection** is selected.
5. Click **Install**.

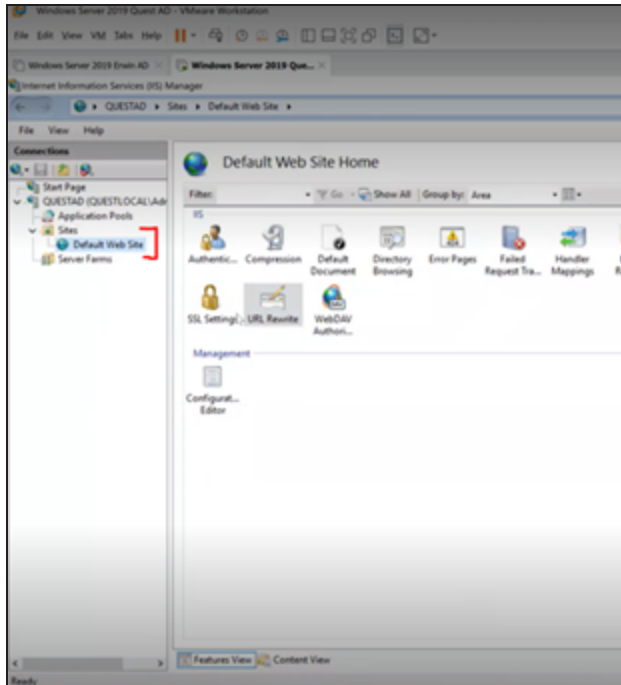
Enabling IIS

Once done, the Default Web Site option is available.

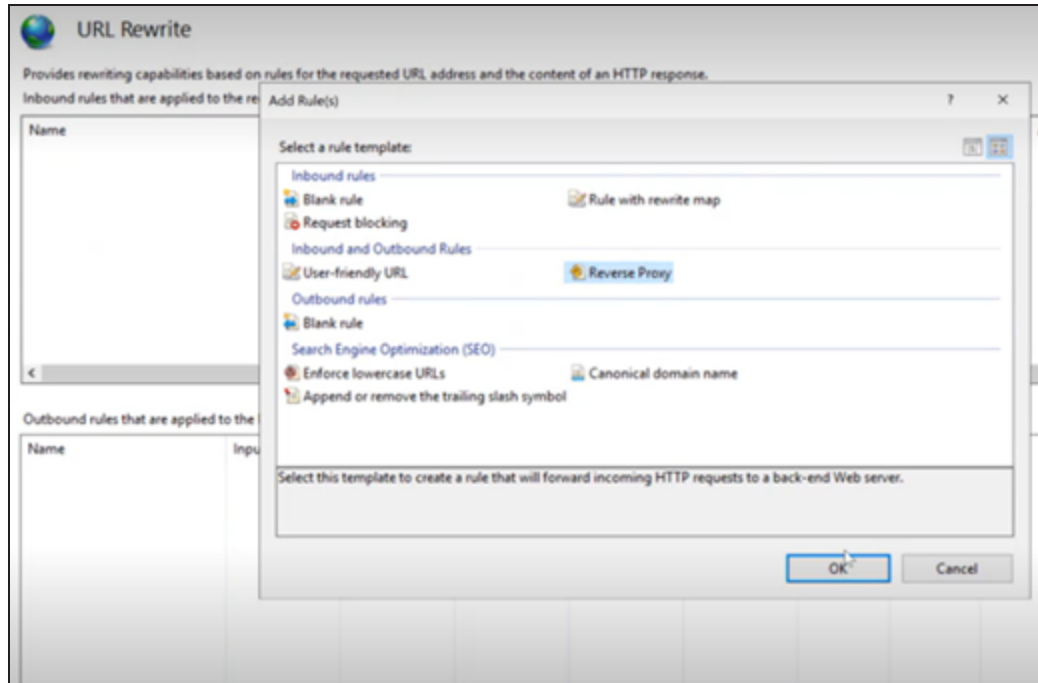


5. Download and install [ARR 3.0](#).
Ensure that you use the 64-bit installer.
6. Download and install [URL Rewrite Module 2.1](#).
Ensure that you use the 64-bit installer.
7. In the Internet Information Services (IIS) Manager, click **Default Web Site**.

Enabling IIS

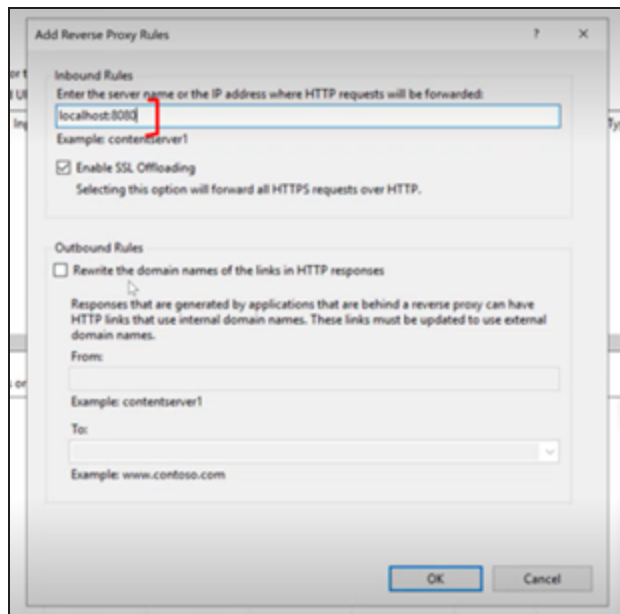


8. Click **URL Rewrite**.
9. Under **Actions**, click **Add Rules**.



10. Click **Reverse Proxy**.

The Add Reverse Proxy Rules screen appears.



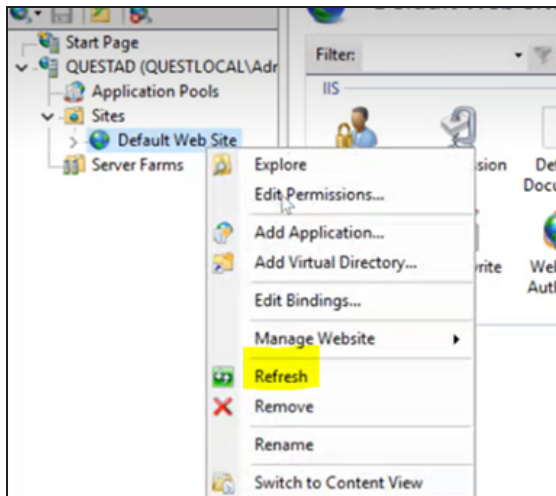
Enabling IIS

11. Under Inbound Rules, add the server name or the IP address and port number of the server where you have installed and configured erwin Mart Portal.

For example, localhost:8080.

It will work with any IP address/port number and not just localhost and 8080. Do not use port that is already in use for another purpose.

12. Under Outbound Rules,
 - a. In the **From** field, add the server name or the IP address and port number of the server where you have installed and configured erwin Mart Portal. For example, localhost:8080.
 - b. In the **To** field, add the server name or the IP address of the server where you have installed and configured erwin Mart Portal. For example, localhost.
13. Click **OK**.
This will redirect you to Apache Server console.
14. In the Internet Information Services (IIS) Manager, right-click **Default Web Site** and click **Refresh**.



15. Right-click **Default Web Site** and click **Manage Website > Restart**.
This completes IIS configuration.

Change the Mart Database Server

Sometimes, you may change the server on which the mart database is installed, or you may restore the mart database with a new name. When there is a change the server name or database name, reconfigure the erwin Mart Portal.

To change your mart database server, follow these steps:

1. Back up your mart database.
2. Restore the database on the designated server.
3. If you use the same computer for erwin Mart Portal and restore the database in a different name, include the new database name in the erwin Mart Portal Configuration screen.

From the Windows Start menu, open the erwin Mart Configuration dialog. On the **Database** tab > **Database Name** field, enter the new name with which the database is restored. Enter the current user name and password to access the database.

4. If you use a different computer for erwin Mart Portal and restore the database in the same name, install the erwin Mart Portal on the new computer.

Install the erwin Mart Portal. On the **Database** tab > **Server Name** field, enter the name of the new server where the database is restored. Enter the current user name and password to access the database.

5. Stop the erwin Mart Portal service and start it again.
6. On the Windows Start Menu, click **erwin** > **erwin Mart Portal**.

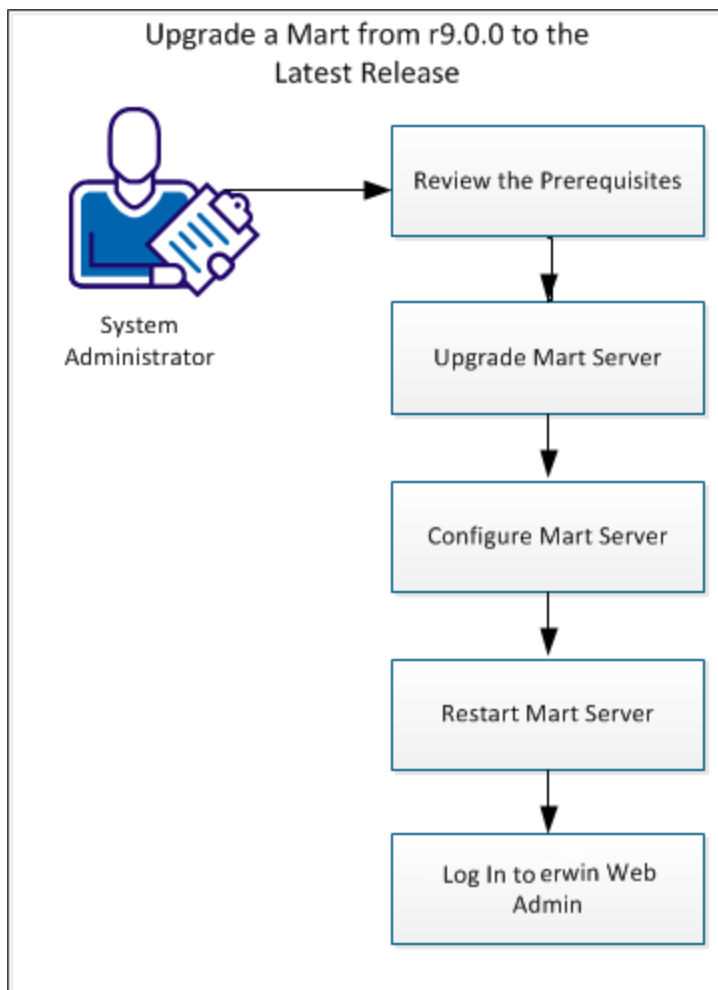
Enter the credentials and log in.

Upgrading Mart

If you are using any earlier release of r9 series and you want to upgrade it to the latest release, upgrade the Mart Portal application and the Mart database. Once the Mart Portal program is upgraded, you must implement the upgraded software.

Important! The current Mart is designed to work with only the current version of erwin Data Modeler. If you try to connect the current Mart with an older version erwin Data Modeler such as r9.0.0, it may corrupt the Mart and cause unexpected behavior.

The following diagram illustrates how System Administrators can upgrade a Mart from any earlier release of r9 series to the latest release:



How to Upgrade any r9 Series Mart to the Current Version

Complete the following tasks to upgrade a Mart of any earlier release of r9 series to the latest release:

1. [Review the prerequisites](#)
2. [Upgrade erwin Mart Portal](#)
3. [Configure erwin Mart Portal](#)
4. [Restart the service](#)
5. [Log in to erwin Mart Portal](#)

▲ [Back to Top](#)

Upgrade Performance Considerations

Ensure that you consider mart size, model count, and associated versions while upgrading a mart from an earlier version to the latest version. The following table provides sample data of the upgrade process. You can use this information as a guideline.

Mart Database	Machine Configuration	Time Taken (Upgrade from lower version to erwin Mart 2021 R1 and above)
Oracle 12c R2 (1221 Models , 42108498 million rows present in M9Object Table)	8 GB RAM 1 CPU	50 minutes
SQL Server 2017 (1277 Models, 44294824 million rows present in M9Object Table)	8 GB RAM 1 CPU	142 minutes
Postgresql 9.6.15 (1020 Models, 33594468 million rows present in M9Object Table)	16 GB RAM 4 CPUs	15 minutes
Oracle 12c R1 (10784 Models, 505178719 million rows present in M9Object Table)	32 GB RAM AWS Machine	15 hours
Oracle 12c R1 (11980 Models, 520732699 million rows present in M9Object Table)	32 GB RAM 4 CPU	20 hours 40 minutes

Following are a few tips to ensure a smooth upgrade:

- Before upgrading, ensure that you double the number of data files in tablespaces for MMDATA and MMINDEX in an Oracle mart.
- Check the Report Upgrade status in the MartServerUpgrade.log file.
- If the M9Object Table has high volume of data and models over 100 MB, run the upgrade on a machine that has 64 GB or more RAM.
- In case of failures in upgrade, before you rerun the upgrade, ensure that you select the following check boxes on the Advanced tab on the erwin Mart Configuration dialog:

Upgrade Performance Considerations

- Rerun Count Upgrade
- Rerun Report Upgrade
- Rerun Report Upgrade For All Models

For more information, refer to the [Configuring erwin Mart Portal](#) topic.

Upgrading erwin Mart Portal

If you are upgrading a Mart from any earlier release of r9 series to the latest release, upgrade the Mart Portal application.

Refer to the [Install a Mart or Upgrade a Mart](#) topic before proceeding.

Follow these steps:

1. If you are running Mart Portal as a Windows service, stop the service and delete it.

If you upgrade erwin Mart Portal without stopping the service, it may not start after you complete the upgrade process.

2. Download and run the installer file from the [erwin Support site](#).

The erwin Mart Portal Installation Wizard appears.

3. Follow the wizard.
4. Restart your computer.

[▲ Back to Top](#)

Restarting the erwin Mart Portal Service

When you modify the details of the mart database and Mart Portal application, restart the erwin Mart Portal service.

Follow these steps:

1. On the Windows Start menu, click **erwin > Stop as Service**.
2. On the Windows Start menu, click **erwin > Start as Service**.

Viewing Log Files

You can find erwin Mart Portal log files at the following locations:

- **erwin Mart Portal as server:**
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/martportal.log
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/martportalupgrade.log
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/vaultservice.log
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/er360.log
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/search_service.log
 - {user.home}/AppData/Local/erwin/Mart Portal/logs/mart_job_scheduler.log
- **erwin Mart Portal as Windows service:**
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\martportal.log
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\martportalupgrade.log
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\vaultservice.log
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\er360.log
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\search_service.log
 - C:\Windows\System32\config\systemprofile\AppData\Local\erwin\Mart Portal\logs\mart_job_scheduler.log

You can configure how the log is generated. For more information about how to configure logging, refer to the [erwin Mart Portal user guide](#).

Use erwin Mart Portal as a Windows Service

There are two ways to start the web server that hosts erwin Mart Portal and erwin ER360:

- Start the web server manually.
- Use a Windows service to start the web server.

For example, if you have used Apache webserver as the server to host Mart Portal, you can start it in two ways:

- Start Apache through the startMartServer.cmd file or through a shortcut to this file.
- Use a Windows service to start Apache.

The benefits of using a Windows service to start a web server are as follows:

- Any user with administrative privileges on a computer can start the Windows service, whereas, only designated users can start a web server manually.
- A Windows service runs regardless of whether a user has logged in. A manually-started web server shuts down when the user who started it logs out.

Follow these steps:

1. On the Windows Start Menu, click **erwin > Create Mart Services** to create erwin Mart Portal Windows services.

Creating the service is a one-time task. After the service is created, you only have to start and stop the service.

2. On the Windows Start Menu, click **erwin > Start as Service** to start the web server.
The necessary services are created

 erwin Apache Server	Apache/2.4.6...	Running	Automatic	Local System
 erwin DM Scheduler Service	erwin Autom...		Manual	Local System
 erwinCacheService		Running	Automatic	Local System
 erwinDMCollibra	erwinDMColl...	Running	Automatic	Local System
 erwinER360		Running	Automatic	Local System
 erwinMartJobSchedulerService		Running	Automatic	Local System
 erwinMartPortal		Running	Automatic	Local System
 erwinSearchService		Running	Automatic	Local System
 erwinVaultService		Running	Automatic	Local System

Use Mart Portal as a Windows Service

You can find the log files, martportal.log, er360.log, and vaultservice.log, at {user account}\AppData\Local\erwin\Mart Portal\logs\.

Enable Logging in Local AppData

To enable logging in a user's AppData while using erwin Mart Portal as a Windows Service, follow these steps:

1. Once the service is created, go to service properties.
2. On the Log On tab, click **This Account**.
3. Enter the credentials.
4. Start the service.

Logging is now enabled for your instance of erwin Mart Portal as a Windows service. The log files, martportal.log, er360.log, and vaultservice.log will be created at {user account}\AppData\Local\erwin\Mart Portal\logs.

Troubleshooting

This section explains the errors that you can encounter while installing and configuring erwin Mart Portal, and how you can troubleshoot them.

The Mart Portal log files are available at C:\Program Files\erwin\Mart Portal\MartApp\config.

Unable to Create Mart Portal Service

Symptom:

If Mart Portal is upgraded to the latest version without stopping and deleting the Mart Portal service of the earlier version, creating a new Mart Portal service does not work.

Solution:

Run the *sc Delete Mart Portal* command to delete the Mart Portal Service from command prompt and then try to create a Mart Portal Service in the new version.

Port out of range

Symptom:

Whenever I connect to the web server, I get the following error message:

```
java.lang.IllegalArgumentException: port out of range 80821.
```

Solution:

Type the correct port number in the Configure erwin Mart Portal's Server dialog and then restart your web server.

Call failed on the server

Symptom:

When I try to connect to the Mart Portal, I get the following error:

```
500 The call failed on the server; see server log for details
```

Solution:

The probable reasons for this error could be one of the following reasons:

Troubleshooting

- The server name is not correct.
- The application name is not correct. By default, the application name is Mart Portal and it is case-sensitive.

Type the correct server name and application name in the erwin Mart Portal's Server dialog and the Configure Mart Portal Details dialog. Restart the web server.

Application Internal Error

Symptom:

When I try to connect to the database, I get the following error:

```
Application Internal Error
```

Solution

You get this error when the Mart Portal application is unable to connect to the required database. The following reasons are probable for this error:

- The database details that are provided in the Configure Mart Portal Details dialog are incorrect.
- The username and the password for the database are incorrect.
- The database is not present.
- The port number for the database is incorrect.
- The network is down.

Ensure that you enter the correct details of your database in the Mart Portal tab of the erwin Mart Configuration dialog.

ORA-12514 TNS listener does not currently know of service requested in connect descriptor

Symptom:

When I try to open the erwin Mart Portal page, I get the Application Internal Error. The Tomcat windows shows the following error message:

```
ORA-12514, TNS:listener does not currently know of service requested in connect descriptor
```

Solution:

Use a fully qualified instance name when starting the Mart Portal.

Note: This section is applicable only for Oracle and SQL Server.

Use a fully qualified instance name when starting the Mart Portal.

Mart already exists. Specify another database name

Symptom:

When I try to connect to the Mart, I get the following error message:

```
An earlier mart is already present in the database you are trying
to initialize. This process can not be continued. Please specify
another database name to continue.
```

Solution:

You get this error when you connect to an old Mart that you have used for erwin DM Release r7 series, r8 series, or Beta release of any r9 series release.

Create a database and provide its details in the Configure Mart Portal Details dialog.

Initialize page is not loading in Internet Explorer

Symptom:

When I type the URL to initialize my Mart in Internet Explorer, the Initialize Mart page is taking a long time to load.

Solution:

The Initialize Mart page does not load because the Active Scripting option in Internet Explorer is disabled.

To enable Active Scripting, follow these steps:

1. In Internet Explorer, click Tools, Internet Options.
2. In the Security tab, click the Custom Level button.
The Security Settings Local Intranet Zone window opens.
3. From the list of options, locate Scripting, Active Scripting, and select Enable. Click OK.
4. Restart Internet Explorer and enter the URL to initialize Mart.
The Mart Initialize page opens.

The Tomcat server is not starting properly. The Configure button is disabled.

Symptom:

My administrator has given me the Administrator rights and when I start the Tomcat server, I get a series of errors. Also, I cannot click the Configure button in the configuration dialog because it is disabled.

Solution:

Right-click Start Server, and click Run as Administrator.

The Tomcat server starts without any error, and the configuration button is enabled.

A connection with the server could not be established

Symptom:

When I try to connect to the web server from erwin Data Modeler, I get the following error message:

```
A connection with the server could not be established
```

Solution:

Verify that you have provided the correct port number and then reconnect to the web server.

The server name or address could not be resolved

Symptom:

When I try to connect to the web server from erwin Data Modeler, I get the following error message:

```
The server name or address could not be resolved
```

Solution:

Verify that the server name where the web server is installed is correct and then reconnect to the server.

If erwin Data Modeler and the web server are installed on the same computer, you can give the server name as localhost. Suppose that erwin Data Modeler and the web server are installed on

different computers. The server name is the name of the computer where the web server is installed.

Invalid user ID or password

Symptom:

When I try to connect to the server, I get the following error message:

```
Invalid user ID or password. Please try again to login.
```

Solution:

Type the correct user name and password.

The user must be an application level user and not a database user.

Error 12029

Symptom:

When I connect to the web server, I get the following error message:

```
Error 12029
```

Solution:

Restart the web server.

Unable to load the web page from my web browser

Symptom:

When I type the URL in Internet Explorer or Google Chrome to connect to the web server, I get the following error messages:

For Internet Explorer

```
Internet Explorer cannot display the webpage
```

For Google Chrome

```
Oops! Google Chrome could not connect to localhost:18170
```

Solution:

Restart the web server.

Internet Explorer Redirects to a Different Link

Symptom:

Suppose that I install erwin Mart Portal on a fresh machine. If I enable the SSL option and I invoke erwin Mart Portal, Internet Explorer redirects the page to `res:///ieframe.dll/`.

Solution:

Internet Explorer versions 8 through 10 have a security enhancement that blocks the following types of sites:

- Sites that have self-signed certificates
- Sites that have self-signed certificates where the certificate does not match the URL

Follow any of these steps:

- Install the certificate in the Trusted Root Certification Authorities store.
- Add the site to trusted sites.
- Set the Internet Explorer Security level to Medium Low.

Chinese characters are replaced with question marks in Postgre SQL Mart

Symptom:

I type Chinese characters in the Version Description dialog in erwin Mart Portal. If I open erwin Data Modeler and go to the Catalog Manager window, I see that the Chinese characters are replaced with ?????.

Solution:

Follow these steps:

1. Select Chinese for the Format, Location, and Locale fields in the computer where you have installed erwin Data Modeler, Mart Portal, and Mart database. (You can access these settings through the Control Panel.)
2. Open the Database Properties dialog for the Mart database and verify the value for the Collation field.
3. If the value is other than `SQL_Latin1_General_CP1_CI_AS`, create a database and assign this value for Collation. Initialize the Mart again.

I have a very long Windows user name and I cannot log in to the Mart through erwin Data Modeler

Symptom:

I have added a very long Windows user name similar to "Magdalena.Chalamalasetti" using the Mart Portal. When the user tries to log in to the Mart through erwin Data Modeler, the name is truncated to "US\Magdalena.Chalamas" and the user cannot log in.

Solution:

The name is truncated due to a limitation with Windows. The Windows API returns the legacy user name that is limited to 20 characters. If the length of a user name exceeds 20 characters, for example, "US\Magdalena.Chalamalasetti", the name is displayed as "US\Magdalena.Chalamas" in the Connect to Mart dialog.

You can resolve this in one of the following ways:

- Type the first 20 characters of the user name when you add the user as a Windows User, in the Mart Portal. For example, instead of typing "US\Magdalena.Chalamalasetti", type "US\Magdalena.Chalamas".
- Use a Windows Group instead of the user's domain name. Using your Windows domain controller software, add the user to a Windows Group, and then add the group as a User Group in the Mart Portal. For more information about how to add a User Group, see [erwin Data Modeler r9 Workgroup Edition: Support for Directory Services](#) video.

SSL Certificate Error

Symptom:

When you open Mart Portal from Mart Portal that is configured with an SSL certification, an SSL certificate error appears.

Solution:

1. Replace localhost in the Mart Portal URL with your computer name.
`https://localhost:12345/MartAdmin/`
`https://<computer_name>:12345/MartAdmin/`
2. Use the updated URL to access the Mart Portal

Unable to save a model to Mart with an existing model name

Symptom:

When you save a model to Mart with an existing model name, a dialog with the following text appears.

Model '<model name>' already exists in library '<mart name>'. Rename the new model name

Solution:

Save the model with a different name.