

## UMT Tool Configuration

This article guides you through your User Management Tool (UMT) SQL server sign on and database basics. It also instructs you on how to perform administrative functions, such as adding or modifying users.

### Prerequisites

Before beginning, you need the following prerequisites:

- Have SQL Server Management Studio (SSMS) installed.
- Obtain SQL credentials to log into the database.
  - Request access and approval from a Global Admin [REDACTED]

Once your approved, the credentials are provisioned by an SQL Admin [REDACTED]

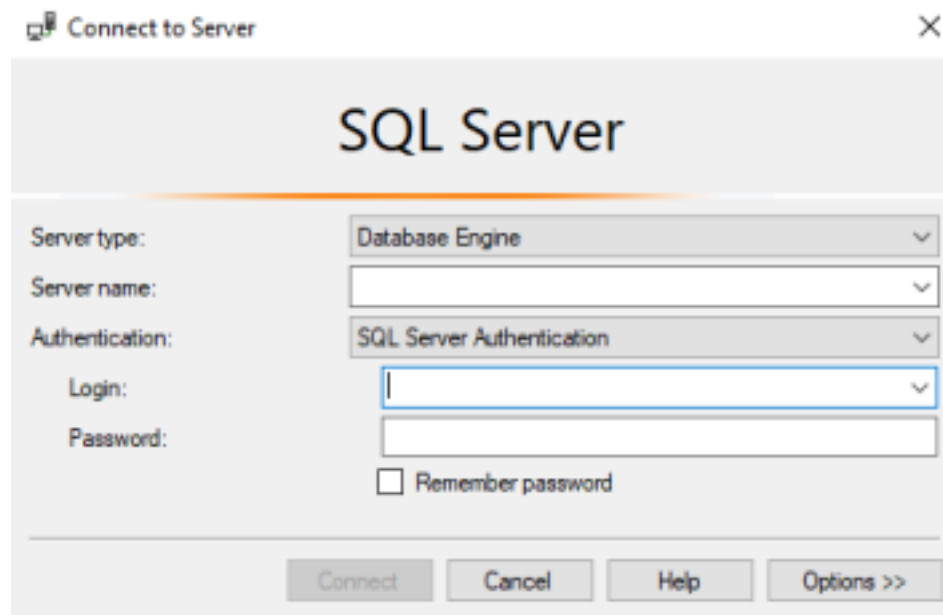
**Note:** If you are using a Torus account, you will have to go through an onboarding process:

- Get started with Torus - Substrate Dev Center (microsoft.net)

### Log into SQL

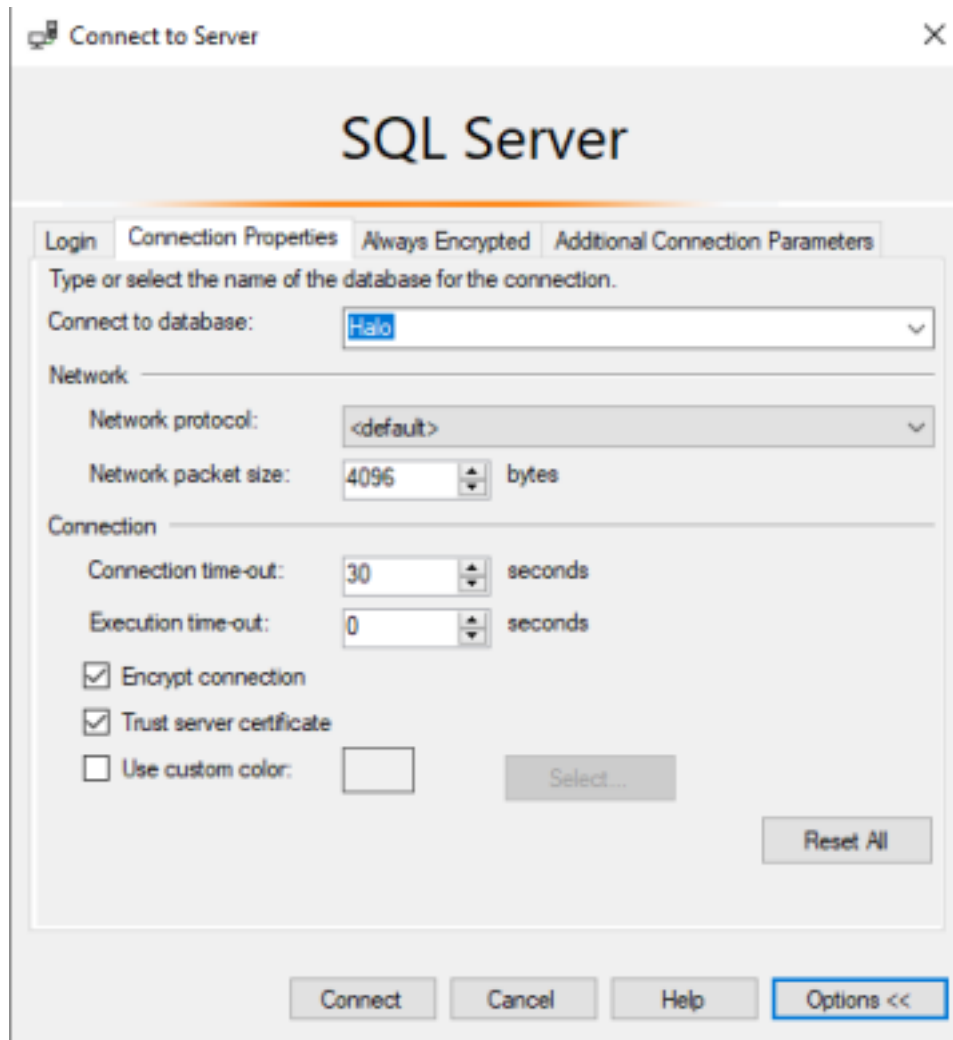
Open SSMS and launch the object explorer.

1. Select **File**, and then **Connect Object Explorer...**
2. In **Server name**, enter the server address to UMT SQL Server you were provisioned.
3. Enter your SSMS sign on credentials in the **Login** and **Password** fields.



Connecting to the SQL server

4. Select **Options**. The **Connection Properties** tab opens.



SQL Server Connection Properties window

5. In **Connect to database**, enter Halo into the field.
6. Ensure **Encrypt connection** and **Trust server certificate** are both checked.
7. Select **Connect**.

## Audit

This table is purely for audit purposes and is treated as a view only table. Only users with authorization to edit this table and task should make changes.

All UMT actions are catalogued to this table. The table provides:

- The user who modified the table.
- The action this user performed in UMT. Possible actions in UMT include add, modify, or delete a user.
- The user on whom the editor performed the action.
- When the action was performed.
- The results of the action.

**Note:** It is not possible to unblock an account that was hard blocked (blocked by an outside entity), such as being blocked by security. Any attempt to unblock a hard blocked account results in a Failure shown the Status column.

### Table schema

The Audit table is named Cortana in the SQL database. The following table outlines all possible columns of the table.

Acronyms in the following table are:

- UPN: User Principle Name

Column Name	Data Type	Description
Id	int	Unique row Id.
AdminUpn	nchar(100)	The user who performed an action in UMT, displayed as their Azure UPN.
Action	nchar(1500 )	The action the user performed.
PerfomedOn	nchar(100)	What user they performed the action on, displayed as their Azure UPN.
PerformedAt	datetime	When the action was performed, displayed as timestamp.
Status	nchar(1500 )	The result of the action taken. This is displayed as either <b>Success</b> or <b>Failure</b> . If it results in a failure, it will often have the resulting error message.

## Administrators

The Administrators table is like the User table but has a few key differences, such as not having a last change or edit by and it is edited by filling a form in excel and running a script. Anyone in the administrator table can also be in the Users table since administrators are not exclusive. It is recommended that the administrators also exist in the users table to avoid any permissions issues.

Administrators can edit only select users based on their UMT supplier approvals.

**Additional\_Supplier\_List** allows administrators to edit outside of their own supplier.

Currently, there are two types of administrators:

- Delegate Administrators:
  - Can only manage users from their own supplier.
  - Is the default administrator role that will be assigned.
- Super Administrators:

- Can manage all users within UMT, regardless of their supplier.
- Should not be created unless approved by [REDACTED]

## Adding delegate administrators

In order to add administrators to the table, use the **Add admins** script.

1. Open the script in SMSS.
2. Fill in the required values.

VALUES

```
('ID','Full Name','Delegate Admin','Standard user administator  
for outsource partner','', 'Azure UPN','Site','Supplier','Suppliers  
Allowed To Edit(comma seperated)')
```

3. **Execute (F5)** the script in SSMS.

**Note:** A new administrator can only view and edit users from their own supplier-set of users, leave 'Suppliers Allowed to Edit(comma separated)' blank.

## Table schema

The Administrator table is named ForeRunners in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	nchar(46)	Unique administrator Id.
Name	text	Administrator's name.
Role	text	Type of administrator: Delegate or Super.
Description	text	Description of administrator role.
Last_Accessed_Time	datetime	The most recent UMT admin access and timestamp
UPN	nchar(100)	Administrators Azure UPN account.
Site	nchar(300)	Administrator's location.
Supplier	nchar(300)	Administrator's supplier.
Managed_Suppliers	nchar(1000)	Any other suppliers the administrator can view and manage in a semicolon separated list.

## Users

The users table contains information on every user in UMT. This table is managed via the UMT front end.

**Important:** Do not edit any fields in the table unless there is a specific error with the user entry. If the data is changed in the table and it does not match with Azures data, it can cause errors and poses security risks.

### Modifying users

If a user needs to be modified, it should be done through UMT front-end and not the SQL back-end. As a best practice, modifying users in SQL is generally avoided. The following are the only reasons that a user should be modified:

- Only minor details need to be changed, such as a wrong site or business unit. •

If the user has the wrong supplier, contact [REDACTED] for verification and then edit the user in UMT.

**Note:** Only the User ID cannot be modified through UMT. If this needs to be changed, then the user will need to be verified, deleted, and then reinstated.

### Table schema

The User table is named Humans in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	nchar(50)	Unique row Id.
DFM	nchar(5)	User's Dynamics for Microsoft
UserPrincipalName	nchar(113)	User's name.
UserPrincipalName_LastChangedBy	nchar(113)	Administrator who changed <b>UserPrincipalName</b> last.
UserPrincipalName_ChangedTime	datetime	Timestamp of the last change.
AccountVerified	nchar(5)	If the user account is verified.
AccountEnabled	nchar(5)	If the user account is enabled.
AccountEnabled_LastChangedBy	nchar(113)	Administrator who changed <b>AccountVerified</b> last.
AccountEnabled_ChangeTime	datetime	Timestamp of the last change.
DisplayName	nchar(70)	User's display name.
DisplayName_LastChangedBy	nchar(113)	Administrator who changed <b>DisplayName</b> last.
DisplayName_ChangeTime	datetime	Timestamp of the last change.

FirstName	nchar(70)	User's real first name.
FirstName_LastChangedBy	nchar(113)	Administrator who changed <b>FirstName</b> last.
FirstName_ChangeTime	datetime	Timestamp of the last change.
LastName	nchar(70)	User's real last name.
LastName_LastChangedBy	nchar(113)	Administrator who changed <b>LastName</b> last.
LastName_ChangeTime	datetime	Timestamp of the last change.
Password_ChangeTime	datetime	Timestamp of the last change.
Company_Email_Address	nchar(113)	User's company email address.
Company_Email_Address_LastChangedBy	nchar(113)	Administrator who changed <b>Company_Email_Address</b> last.
Company_Email_Address_ChangeTime	datetime	Timestamp of the last change.
Site	nchar(300)	User's home site.
Site_LastChangedBy	nchar(113)	Administrator who changed <b>Site</b> last.
Site_ChangeTime	datetime	Timestamp of the last change.
Supplier	nchar(300)	User's supplier they work for.
Supplier_LastChangedBy	nchar(113)	Administrator who changed <b>Supplier</b> last.
Supplier_ChangeTime	datetime	Timestamp of the last change.
BusinessUnit	nchar(100)	User's business unit they belong to.
BusinessUnit_LastChangedBy	nchar(113)	Administrator who changed <b>BusinessUnit</b> last.
BusinessUnit_ChangeTime	datetime	Timestamp of the last change.
LineOfBusiness	nchar(1000) )	User's line of business.

LineOfBusiness_LastChangedBy	nchar(113)	Administrator who changed <b>LineOfBusiness</b> last.
------------------------------	------------	---

LineOfBusiness_ChangeTime	datetime	Timestamp of the last change.
Telephone_Number	bigint	User's work telephone number
Unblock_Count	int	How many times this user has been unblocked.
Soft_Block	nchar(5)	If the user is soft blocked.

## License

This table contains the license groups that are assigned to each supplier. Licenses are assigned by groups and are semicolon-separated if they include more than one license group. A single consumer or commercial supplier can have multiple license groups.

### Add a license

If you need to adjust the license(s) assigned to the supplier's business unit manually, ensure that the group licenses you assign are spelled exactly as shown in the License Groups table. Note the following when manually editing this table:

- The only acceptable options for the **BusinessUnit** is Commercial or Consumer.
- Multiple licenses can be added to a single supplier's business unit for the supplier by separating values with semicolons.
- Leaving the value of **Groups** blank will not add any licenses to the supplier's business unit.

### Table schema

The License table is named License in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	int	Unique row id.
Supplier	varchar(MAX)	Name of the supplier.
BusinessUnit	varchar(MAX)	Commercial or Consumer license identifier.
Groups	varchar(MAX)	A semicolon delineated list of the license groups assigned to the supplier.

## License Groups

This table contains the license groups that are available for the supplier's business units.

**Do not edit this table.** Any modifications to this table will be performed by [REDACTED]

### Table schema

The License Groups table is named LicenseGroups in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Group ID	varchar(50)	License id for the group.
Group Name	varchar(100)	License group name.

## Locations

The Locations table contains the list of sites and suppliers for any users of UMT. The only way for new sites and suppliers to be entered into this table is by manually editing through the SQL Manager.

### Add a new site and supplier

To add a new site and supplier, you will need to use the **Add new locations** script. The script will automatically add a new location id for the data set.

1. Open the script in SMSS.
2. Fill in the **Supplier** and **Site** values. Leave **@NewLocationId** as is.

```
VALUES
    (@NewLocationId
    , '[Supplier]'
    , '[Site]')
```

3. **Execute (F5)** the script in SSMS.

**Note:** Each row is a unique combination of the Supplier and Site. When adding a new entry, ensure that it does not already exist in the table.

### Table schema

The Locations table is named Locations in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	int	Unique row Id. The value of this column is automatically added. Do not edit this column manually.



Supplier	nchar(100) )	The supplier's name.
Site	nchar(200) )	The supplier's location.

## Group Additions

The Group Additions table contains a list of groups and the users assigned to them. This table gives administrators the ability to add a user to groups on an update or creation.

Adding a user to a group(s) is done based on the user's supplier, site, and/or business unit.

### Table schema

The Group Additions table is named GroupAdditions in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	int	Unique row Id. The value of this column is automatically added. Do not edit this column manually.
GroupId	varchar(50)	The group's unique id.
Supplier	varchar(MAX)	The supplier's name.
Site	varchar(MAX)	The supplier's location
BusinessUnit	varchar(MAX)	User's business unit they belong to.

## Human Authentication

The Human Authentication table contains a list of user's Self-Service Password Reset (SSPR) and Multi Factor Authentication (MFA) registrations.

### Table schema

The Human Authentication table is named HumanAuthRecords in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	int	Unique row Id. The value of this column is automatically added. Do not edit this column manually.

UserPrincipalName	nvarchar(MAX)	The user's email address.
SSPR_Enabled	nvarchar(MAX)	True or False value to enable SSPR for the user.
MFA_Enabled	nvarchar(MAX)	True or False value to enable MFA for the user.
Supplier	nchar(300)	The supplier's name.

## Line of Business

The Line of Business (LOB) table contains a list of the LOB's that are used in UMT. This table allows administrators to swap out LOB's when necessary.

### Table schema

The Line of Business table is named LineOfBusiness in the SQL database. The following table outlines all possible columns.

Column Name	Data Type	Description
Id	int	Unique row Id. The value of this column is automatically added. Do not edit this column manually.
LoB	nvarchar(MAX)	The Line of Business name.
BU	nvarchar(MAX)	The Business Unit the LOB belongs to.

## Other

The Other table holds information that does not need its own table, such as the Banner and Alert messages that will appear.

### Change the banner or alert messages

To change the messages shown in the banners and alerts that appear in UMT, change the text contained in the Value column. Only change the text that is wrapped by the HTML.

### Change the banner/alert visibility

This table allows you hide or show the banner or alert messages that can appear in UMT by changing the value of the **hidden** column. Changing the value to:

- **True** will hide the banner/alert.
- **False** or anything besides **True** (within the limit of five characters) will display the banner/alert.

### Table schema

The Other table is named Other in the SQL database. The following table outlines all possible.

Column Name	Data Type	Description
Id	int	Unique row Id.
Type	varchar(MAX) )	The type of information that is being stored.
Value	varchar(MAX) )	The information to be stored.
Hidden	nchar(5)	Allows you to hide the information by setting this field to True.

## Need help?

For questions on the content of this article, reach out to [REDACTED]  
[REDACTED]

To request that content be updated or added to this wiki, submit a Documentation Bug via [REDACTED]  
[REDACTED] or contact [REDACTED]