User Migration Tool

- User Migration Tool Prerequisites, on page 1
- User Migration Tool Features, on page 2
- Migration Scenarios, on page 2
- Internationalization (I18n) and Localization (L10n) Considerations, on page 3
- Security Considerations, on page 3
- User Migration Steps, on page 3
- User Migration Tool Modes, on page 5
- Users from Trusted Domains, on page 10
- User Migration Tool Troubleshooting, on page 11

User Migration Tool Prerequisites

You must meet the following prerequisites before you run the User Migration Tool:

- In the target domain, run Domain Manager. Lay out the Unified ICM OU hierarchy and create the Unified ICM security groups for each Unified ICM instance before you run the User Migration Tool.
- Import the exported Unified ICM registry from the source Logger system to the target Logger system.
- Back up the Logger database from the source Logger system and restore it on the target Logger system before you run the User Migration Tool in the target domain.
- If users from an external domain are members of the Unified ICM security groups at the source domain, use the“Active Directory Domains and Trusts” tool to establish the trust relationship. Establish the trust relationship between the target domain and the external domain that corresponds to the trust relationship that existed between the source domain and the external domain.
- If you move the Unified ICM server to a new domain, make sure that the SQL Server migrates to the new domain before you run the User Migration Tool.
- In the source domain, the user who runs the User Migration Tool must be a domain user and a member of the local system administrator group.
- In the target domain, the user who runs the User Migration Tool must have the following privileges:
  - The user must be a member of the local system administrator group.
  - The user must be a domain user.

- The user must have at least one of the following privileges set:
  - a domain administrator
  - a member of the Cisco_ICM_Setup (Root) security group

- Access the external domain to migrate the membership of Unified ICM users who belong to an external domain. Access requires external domain user account credentials with read privileges.

User Migration Tool Features

The User Migration Tool provides the following features:

- Migrates AD user accounts from an old (source) domain to a new (target) domain to the same, or a different, Unified ICM facility.
- Adds the user account in the corresponding Unified ICM security groups in the target domain.
- Updates the Logger database with the Globally Unique Identifier (GUID) of the user account from the target domain.
- Migrates the Unified ICM security group membership of Foreign Security Principals to the new domain.
- Migrates the Unified ICM security group membership of user accounts to another facility in the current domain.

Note User Migration Tool is not applicable for SSO users.

Migration Scenarios

Use the User Migration Tool in the following migration scenarios:

- Technology Refresh upgrades on machines in a target domain.
- Technology Refresh upgrades on machines in a different Unified ICM Facility OU in a target domain.
- Moving machines with pre-installed Unified ICM components to a target domain.
- Moving machines with pre-installed Unified ICM components to a different Unified ICM Facility OU in the target domain.
- Moving machines with pre-installed Unified ICM components to a target domain and performing a Common Ground (CG) upgrade.
- Moving machines with pre-installed Unified ICM components to a different Unified ICM Facility OU in the target domain and performing a Common Ground upgrade.
- Migration of user accounts to a different Unified ICM Facility OU in the same domain.

Internationalization (I18n) and Localization (L10n) Considerations

In the localized version of Unified ICM/CCE, you can store the usernames in non-Western European characters (but not in Unicode) in the Unified ICM/CCE database, but the Active directory Common Name (First, Last, Middle), sAMAccount Name, User Principal Name, Organizational Unit (OU) and domain names are always in Western European character set and must not include Unicode or multi-byte characters.

The User Migration Tool is able to perform user migration for localized systems.

Security Considerations

The User Migration Tool connects to the Logger Database using Windows Authentication.

In the source domain, the user running the User Migration Tool must be a domain user and a member of the local system administrator group.

In the target domain, the user running the User Migration Tool must have the following privileges:

- The user must be a member of the local system administrator group.
- The user must be a domain user.
- In addition, at least one of the following privileges must be set. The user must be:
    - a domain administrator
    - a member of the Cisco_ICM_Setup (Root) security group

Migration of the membership of system users who belong to an external domain with one-way trust, requires credentials of an external domain user account with read privileges (such as a domain user account) to access the external domain.

User Migration Steps

The User Migration Tool first runs in the source domain in Export mode. In this mode, it reads the users from the Logger database and the nine (9) security groups, then exports the user information (such as Username and UserGroupID) and the security group membership from the source AD folder. The UMT looks at the Logger database for each user found and looks at all nine (9) security groups to find the user group memberships (the Setup and Config security groups in the Root, Facility, and Instance OUs). The user information found is added to the flat file.

For users belonging to the external domain, the User Migration Tool needs credentials to connect to the external domain. The UMT looks for the users in the external domain. If the UMT finds them, it determines the security group membership for the user in the source domain and exports the information.

The UMT also looks at the Instance security groups (Setup and Config) to find any user accounts. If the UMT finds user accounts, it adds that user information to the flat file as well.

The User Migration Tool then runs in the target domain in an Import mode. In this mode, it reads the file that was generated during Export mode and does the migration for all the users that belong to the source domain. During this mode, it looks for the users in the target domain and, if they are not found, creates the user accounts

in the Instance OU. It fixes the group membership for the user and updates the database (if necessary) with the target domain name and the user's GUID from the target domain. In order to perform migration of the users belonging to an external domain, the User Migration Tool needs credentials to connect to the external domain. It looks for the users in the external domain and, if they are found, it fixes the security group membership for the user in the target domain.

The following are the steps involved when using the User Migration Tool.

Export Users from the Source Domain

Procedure

Step 1 Back up the Logger database for each Unified ICM/CCE instance using Microsoft SQL Server tools.

Step 2 On the Logger system, for each installed Logger instance, run the User Migration Tool in Export mode.

An output file (umt_<*Facility name*>_<*logger database name*>.bin) is generated in the directory from which the tool is run.

Step 3 In a Technology Refresh upgrade scenario:

a) Copy the output file to the Logger system in the target domain (to the folder from which you run the User Migration Tool on the target system).
b) Back up and export the registry on the source system.
c) Check the log file for any errors.

Import Users into the Target Domain

Procedure

Step 1 If the Unified ICM/CCE services are running, shut them down.

Step 2 If you need to change the domain name in a Common Ground upgrade scenario, see Change Domain Name, on page 5 and proceed to Step 4.

Step 3 In a Technology Refresh upgrade scenario:

a) Make sure that the exported file exists in the Logger system.
b) Restore the Logger database that was copied from the source Logger system using Microsoft SQL Server tools.
c) Import the Unified ICM/CCE registry exported from the source domain.

Step 4 Run the User Migration Tool in Import mode for each Logger instance to migrate users.

Step 5 (Optional) Run the User Migration Tool in verify mode to validate the migration.

Step 6 For duplex Logger systems, run the ICMDBA tool to synchronize sides A and B.

Step 7 Restart the Unified ICM/CCE services if they were previously running.

Change Domain Name

To change the domain for a system, you must have the necessary permissions. To change the domain for all instances on the computer, complete the following steps:

Procedure

Step 1 Open the Web Setup tool.

Step 2 Click the **Instance Management** tab.

Step 3 Delete any instances and facilities that you don't want to use in the new domain.

Step 4 Open the Cisco Domain Manager tool. Ensure that the instances and facilities that are defined match what is actually on the system. A mismatch can cause the Web Setup Change Domain operation to fail.

Step 5 Select the instance that you want to modify, and then click **Change Domain**.

The Change Domain page opens, displaying the currently configured domain and the new domain name of the system.

Step 6 Click **Save**. Confirm whether you want to change the domain.

Step 7 Click **Yes**. If successful, you'll return to the Instance List page.

If the instance doesn't exist, then create it using the Cisco Domain Manager. Be sure to create the instance under the selected facility in the new domain.

Note Make sure that the certificates in the keystore pertain to the fully qualified domain name (FQDN) of the servers. If you have changed the domain name or hostname, be sure to update the certificates in the keystore.

User Migration Tool Modes

The User Migration Tool provides functions in the following modes:

- Export
  - Runs on the Logger system in the source domain.
  - Exports user account details from the Logger database and Instance security groups to a file generated in the same directory in which the tool was run.

    Names the exported file by combining the tool name (umt), the ICM Facility name, and the Logger database name (umt_<*Facility name*>_<*Logger database name*>.bin).

    The exported file contains the source domain name. It also contains Unified ICM instance specific parameters such as the Unified ICM Facility name, Unified ICM instance name, and Logger database name. You do not need to specify these parameters during the Import mode because they are contained in the exported file.

- Import
  - Imports user account details from the exported file.

- Updates AD and the Logger database (if necessary).

Note Due to the need to replicate new user accounts and AD security group memberships, wait 15 minutes after an Import completes before you run the User Migration Tool in Verify mode.

- Verify
  - Runs on the Logger system in the target domain after you perform an Import.
  - Validates the import.

Note Help is available by entering **`usermigration.exe`** with either no arguments or the **`/help`** argument. This command displays the command line syntax, and all modes and parameters are displayed.

The User Migration Tool also generates a report file in the same directory that the tool is run. The name of the report file consists of the name of the exported file suffixed with ".rpt" (umt_<*Facility name*>_<*Logger database name*>.rpt).

The report file contains the following information:

- In the **Export** mode:
  - the name of the user account that is exported
  - all the Unified ICM security groups that the user account is a member of
- In the **Import** mode:
  - the name of the user account that is created in AD
  - all the security groups added to the user account.

In addition, every time the User Migration Tool runs, it generates a log file in `C:\temp`. The name of the log file contains the current time-stamp and is prefixed with "UMT" (for example: UMT2008619141550.log).

The log file contains results in three categories:

- Info
- Warning
- Error

Runtime messages are also displayed in the command window while the User Migration Tool runs.

Related Topics

Import Mode, on page 8
Verify Mode, on page 9

Mode Considerations

The username created can not log on for Internet Script Editor pages, without first logging into the new domain and then changing the password.

Use your Windows logon to login using the AD account. A prompt appears asking to change the password. Provide a new password, then use the Internet Script Editor interface to login.

Export Mode

The Export mode exports the user information from the source domain and external domain into a file.

When you run the User Migration Tool in Export mode, it exports the following information to the file:

- Unified ICM Facility and Instance name
- Logger database name
- AD user account name and the domain name
- Unified ICM security group that the user is a member of
- UserGroupID from the Logger database

The following table provides the command and parameter information for the User Migration Tool operating in Export mode.

Table 1: Export Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Export	[/DBname <*Logger Database name*>]
		[/Facility <*ICM Facility name*>]
		[/Instance <*ICM Instance name*>]

The Export mode command syntax is: usermigration.exe /Export /DBname <*Logger Database name*> /Facility <*ICM Facility name*> /Instance <*ICM Instance name*>.

Note

- For each external domain, the UMT command-line interface solicits the credential details to connect to that domain. If it fails to connect to the domain, it does not export the users belonging to that domain.
- The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as you include all of them in the command.

Related Topics

Content Parameter Descriptions, on page 9

Import Mode

The Import mode migrates users from the source domain, and external domain, to the target domain; and then updates the Unified ICM database.

In the Import mode, the User Migration Tool gets the username from the input file, and searches for a user account in the AD, and creates one if not found. The user account is created in the Instance OU using the password supplied in the command-line interface. The password is set to expire to force the user to change the password during the next login.

The User Migration Tool adds the user account to the Unified ICM security group based on the information from the exported file. The Logger database then updates with the user account AD Globally Unique Identifier (GUID) and the target domain name.

The following information imports from the exported file:

- Logger database name
- Unified ICM facility
- Instance name

In the Import mode, you can run the User Migration Tool with an optional /Facility parameter to import the user accounts to a different facility name. If the new facility migration is in the same domain:

- You do not need to create the user accounts or update the Logger database.
- Only the Unified ICM security group membership of the user account updates.

The following table provides the command and parameter information for the User Migration Tool operating in Import mode.

Table 2: Import Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Import	[/FileName <*Exported file name*>]
		[/SetPassword <*Default password for newly created AD user accounts*>]
		[/Facility <*Different ICM Facility name*>] (Optional.)

The Import mode command syntax is: usermigration.exe /Import /FileName <*Exported file name*> /Setpassword <*Default password for newly created AD user accounts*> /Facility <*Different ICM Facility name*>.

In the Import mode, the User Migration Tool searches for a user account in the AD, and creates a user account if it does not find one. The user account is created in the Instance OU using the password supplied in the command-line interface. The password is set to expire to force the user to change the password during the next logon.

Note The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as you include them all in the command.

Related Topics

Content Parameter Descriptions, on page 9

Verify Mode

The Verify mode validates the import in the target domain by validating the AD and Unified ICM database migration done in the Import mode.

The User Migration Tool performs the following verification with the data from the exported file:

- Verifies the existence of the user account in AD.
- Verifies the membership of the user in the Unified ICM security groups.
- Validates the user's AD Globally Unique Identifier (GUID) and the domain name with the information in the Logger database (Unified ICM only).

The command and parameter information for the User Migration Tool operating in Verify mode are provided in the following table.

Table 3: Verify Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Verify	[/FileName <*Exported file name*>]
		[/Facility <*Different ICM Facility name*>] (Optional.)

The Verify mode command syntax is: **`usermigration.exe/Verify/FileName <Exported file name>/Facility <Different ICM Facility name>`**.

Note The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as they are all included in the command.

Related Topics

Content Parameter Descriptions, on page 9

Content Parameter Descriptions

The following table provides descriptions of the parameters used by the User Migration Tool.

Table 4: User Migration Tool Parameters

Parameter	Description
/DBName	The Logger database name.

Parameter	Description
/Facility	The Unified ICM instance facility name. When you optionally specify this parameter during the import or verify mode, the User Migration Tool migrates users to a different Unified ICM facility.
/Instance	The Unified ICM instance name.
/FileName	The filename that has the user information exported from the source domain.
/SetPassword	The default password used for the user account created in the target domain. The User Migration Tool sets it to “Change password at next logon” so that the user is forced to change the password when they log in for the first time.

Users from Trusted Domains

User accounts from trusted AD domains with authorization in the current domain are possible. These user accounts are authorized in the current domain because the users are members of Unified ICM security group. The User Migration Tool performs migration of Unified ICM security group membership of such user accounts.

For one-way trusted domains, the User Migration Tool needs Domain User credentials from the external domain in order to:

- Connect to the external domain and find a user account.
- Determine the Unified ICM security group membership in the current domain.

The command-line interface to solicit credentials is as follows:

1. Enter username on domain <*DomainName*>.
2. Enter <*password*>.

For users of a trusted domain, the Unified ICM security group membership is migrated only if the user is a direct member of the Unified ICM security group.

For example:

- *ExtUser1* is a user account belonging to the trusted domain *ExtDomainA*.
- *ExtUser1* is a **direct** member of the Cisco_ICM_Setup and Cisco_ICM_Config security groups.
- *ExtUser1* is a member of the security group FOO.

Note This restriction does not exist for users belonging to the current (source) domain.

As a result, when the Unified ICM security group membership of *ExtUser1* is migrated, only the Cisco_ICM_Setup and the Cisco_ICM_Config security groups are selected.

To migrate Unified ICM security group membership of users belonging to a one-way trusted domain, there must be at least one user from that domain in the Logger database. Otherwise, the UMT skips migration for the one-way trusted domain.

The UMT knows that it needs to connect to a one-way trusted domain only if it is referenced in the Logger database. Unless it connects/authenticates to the one-way trusted domain, it cannot determine if users from that domain are a member of the Unified ICM security groups.

User Migration Tool Troubleshooting

This section provides troubleshooting information for the User Migration Tool.

User Migration Tool Error Messages

The following table provides solutions for User Migration Tool error messages.

Table 5: User Migration Tool Error Messages

Error Message	Solution
Cannot connect or authenticate to the Logger database.	Verify that the Logger database exists and that you can authenticate it using Windows authentication.
Cannot connect or authenticate to the Current domain.	Verify that the Domain controller is up and running and the logged-in user is a member of the Domain Users group.
Cannot add the user account to a Unified ICM security group.	Verify that the logged-in user has the required permissions to run in Import mode. The logged-in user must be a Local Administrator and a member of the Setup security group in the domain. The specified password in the /Setpassword parameter must satisfy the domain's password policy requirements.
Cannot create user account in the target domain.	Verify that the logged-in user has the required permissions to run in Import mode. The logged-in user must be a local administrator and a member of the Setup security group in the domain.
The exported binary file is corrupted.	Run the User Migration Tool again on the source system to generate a new export file.
The exported binary file could not be found in the directory where the User Migration Tool is running.	Ensure that the exported file is available in the directory from where the tool is run.
Failure while reading from the Logger database.	Verify that the Logger database is not corrupted.
Failure while updating the Logger database.	Verify that the logged-in user has writable permissions for the database. The logged-in user must be a local administrator and a member of the Setup security group in the domain.

Error Message	Solution
Failure while reading from the exported binary file.	The exported binary file is corrupted. Run the User Migration Tool in Export mode again on the source system to generate a new export file.
Failure while writing to the binary file during export.	Ensure that the logged-in user has write permissions in the current directory.
One or more of the Unified ICM OU is missing in the current domain.	Run Domain Manager tool and create Setup security groups, and re-run the User Migration Tool.
One or more of the Unified ICM security groups do(es) not exist in the current domain.	Run the Domain Manager tool and create the Setup security groups, then re-run the User Migration Tool.
The logged-in user has insufficient credentials.	The logged-in user must be a Local Administrator. The logged-in user must be a member of the Domain Users group in the current domain. For import, the logged-in user must be a member of Cisco_ICM_Setup security group.
The Logger database is corrupted.	Fix the Logger database and re-run the User Migration Tool.
The system is either running stand-alone, or in a workgroup.	The User Migration Tool must be run on a system that is in a domain.
Mismatch of version between the User Migration Tool and the exported file.	You must use the same version of the User Migration Tool for both modes of the migration.
The User Migration Tool could not disable configuration changes.	Disable the configuration changes manually, then run the tool.
Incorrect usage of the User Migration Tool.	You cannot run the User Migration Tool in Import mode under the same Unified ICM facility and domain that it was exported from. You must run it under a different Unified ICM facility in the same domain, or on a different domain.
The Router system is not reachable for remote registry access.	Ensure the hostname or IP address of the router is correct.