

TELUS AD Sync

An identity management solution



An important historic challenge faced by small and mid-sized businesses when opting for the TELUS Business Email Service is the requirement to have two sets of credentials; one to log on to their computer and on-premises applications, and one for their TELUS-hosted applications.

The situation

The internet has matured, both business and consumers are now dependent on internet connectivity, hosting of business applications has become a reality and offers great advantages to businesses of all sizes.

Nonetheless, having more than one set of credentials results in more forgotten login ids, passwords and lower all-round productivity. Provisioning also adds complication; when a new user is added to an organization the user now has to be created twice. Procedures to delete accounts for departing employees and contractors become more complex leading to potential for accounts to be left open, posing security concerns.

This White Paper presents a new solution by TELUS for automated provisioning and synchronization of user account details between customer-premise and TELUS-hosted Active Directory environments.

TELUS' solution

The TELUS AD Sync service allows customers to synchronize their own localized Domain Controller to the TELUS-hosted Domain Controller. The customer's ID in the TELUS-hosted Domain Controller will be regularly updated with any user changes that have been saved in the customer's domain controller.

The service is a customer only service. Once provisioned to a customer, the customer's administrator will have access to download and configure the TELUS AD Sync tool to their existing Domain Controller. The interface is a one way connection, where any user updates that are made on the Customer Domain Controller are synchronized to the TELUS Hosted environment.

Customers using the TELUS AD Sync service will no longer change their users' properties through the UC Management Centre; any user change must be completed in the customer's existing domain controller.

This allows a customer to add, change, and remove users in their local AD Forest/Domain and have this action replicated automatically in the TELUS Hosted services domain. This service means that shared hosted Unified Communications clients will only have to update their ID credentials in one place, their local Active Directory, not in two places, their local Active Directory and the TELUS Hosting AD.

The TELUS AD Sync Service monitors password changes in the client Active Directory forest and replicates these changes to the TELUS Hosted Active Directory.

TELUS Hosted Services

- Business Email
- Instant Connect
- Workspace

TELUS AD Sync

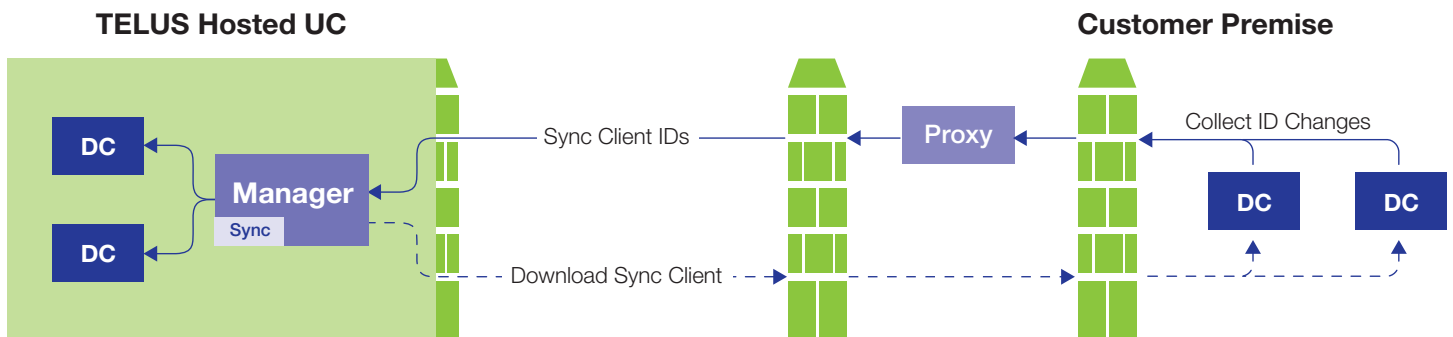


Figure 1 Physical Architectural View

User lifecycle management

The following features are supported by the solution.

■ Exclude and include groups

Users in the Customer AD can be selected for synchronization based on security group membership. Any users in the “include” groups will be synchronized, conversely, if exclude groups are specified, users in the exclude groups will never be synchronized. This gives the customer easy control over the users to be replicated into the hosting environment. Typically, the purpose would be to exclude service and computer accounts or to have control over a migration process from on-premises to hosted Exchange. In the scenario where a user has membership of both an include and an exclude group, the exclude group will take precedence. This works in a similar way to most permission systems, where a “Deny” always takes precedence over an “Allow” permission.

Note: TELUS recommends that the Domain Controller contain a group labeled “TELUS AD SYNC” which will be used as an include group for the service

■ User creation

As soon as a user is created and added to the include group, the user will be replicated in the hosted environment. A template is used for creation that can be used to control which AD attributes are transferred to the new hosted user. When a user is created the SID (globally unique user identifier) from the Customer AD is also stored in The UC Management Centre against the user.

■ User update

Any subsequent changes made to a user in the Customer Active Directory will be replicated across to the TELUS hosted Active Directory. Support is also included for disabling of accounts; a disabled account in the customer AD will disable the account in the TELUS hosted Active Directory.

■ User deletion

Deletion of the user in the customer Active Directory will send another request to The UC Management Centre automatically removing the user from the TELUS hosted environment.

This minimizes cost to the customer by minimizing the amount of resource used in the hosted environment.

Password change detection

TELUS AD Sync implements a Windows password filter DLL, which is registered on each domain controller to receive password change events. This is a standard and recommended approach for detecting password changes and is the approach used by nearly all identity integration products.

Use of NT logon name/sAMAccountName

Active directory supports two logon names or identifiers for each user, the sAMAccountName or Username (simple logon name), and the uPN (User Principal Name). The simple logon name is used to support pre-Windows 2000 operating systems. The uPN (internet-style logon name) is available in current Windows operating systems.

Enterprise customers may use the simple logon name (this is a limited length string, and typically a naming convention is applied, e.g. firstname + first character of lastname, as an example, “John Smith” may have a username of “johns”), the User Principal Name is commonly used in hosting scenarios and looks similar in format to an email address (e.g. user@domain).

In a shared hosting environment, the use of traditional Usernames (simple logon name) is difficult due to duplicate name conflicts that increase with the high volume of users.

TELUS AD Sync

TELUS recommends that users utilize the same uPN (internet-style logon name) from their customer premises AD.

Users will be encouraged to use the uPN for logging on to any system, internal or hosted, this will ease logon problems. Aligning the uPN with the users primary email address will also ease this process.

User Principal Name (uPN) generation and mapping

The UC Management Centre can be configured to generate a "hosting" username for each user based on a pre-determined template; this is needed to ensure that usernames are guaranteed to be unique.

TELUS AD Sync service will perform the following:

1. If the customer domain exists within the TELUS Hosted environment, then the user's current uPN will be preserved into the hosting environment.
2. If the customer domain doesn't exist in the TELUS Hosted environment, the users sAMAccountName (simple logon name) will be pre-pended to the primary domain for the customer (e.g. if the sAMAccountName is johns and the primary domain is domain.com, the hosting uPN would be johns@domain.com).

Security

Security of the solution has been a prime consideration in order to ensure the privacy of data and safe transfer of passwords into the hosting environment.

■ Configuration

Sensitive information in the configuration is encrypted. Furthermore, all configuration files and registry data have permissions that restrict access to an Administrator or the Local System user on the Domain Controller.

■ Password change detection

A password filter DLL is installed onto each Domain Controller. When a password is changed, the user's unique identifier (SID) and the password are immediately encrypted (Windows DPAPI) and stored to a file on the Domain Controller. Encrypted data can only be decrypted on the same machine by an Administrator or the Local System user. The data in the file is also hashed (SHA1) to prevent unauthorized changes. The files have permissions that restrict access to an Administrator or the Local System user.

■ API secure requests

Requests are sent to the UC Management Centre infrastructure using HTTPS (or HTTP). The secure API request utilizes a combination of a public/private key and a symmetric key (RSA and AES) to securely transfer data and credentials. This ensures the data cannot be intercepted or diverted to another source. The data in the request is also hashed (SHA1) to prevent unauthorized changes.

■ Request transfer

The transfer of data to the hosting environment can also be sent over HTTPS (SSL), adding an additional layer of security.

UC Management Centre – features for TELUS AD Sync

The UC Management Centre user interface has been adapted to assist in the management and deployment of the TELUS AD Sync tool as well as restricting the changes that can be made for synchronized users.

■ TELUS AD Sync service

The addition of a new service in The UC Management Centre allows access to the TELUS AD Sync utility to end-customers. This allows TELUS to quickly enable TELUS AD Sync for a customer or reseller and also easily track usage for billing purposes.

■ Configured setup

Any TELUS AD Sync service administrator (or customer level administrator) can gain access to download a customized setup file for installing the TELUS AD Sync customer Active Directory agent. The setup file includes core information needed to connect to The UC Management Centre, including the public key needed for secure API calls and the instance specific connection information needed for the agent to send information back to the UC Management Centre.

■ User control

Users in The UC Management Centre that have been synchronized by the TELUS AD Sync utility are flagged and the UC Management Centre user interface will display non-editable user information. This is to avoid user information being updated in the UC Management Centre and then being overwritten by changes made via the customers Active Directory. User Services can still be provisioned and managed through the UC Management Centre.

TELUS AD Sync

Connectivity

The connection between the TELUS host and the TELUS AD Sync client is encrypted with public/private key technology using a technique similar to that of SSL. This allows the connection between TELUS and the client to use any available connection solution, HTTP, HTTPS, VPN, and dedicated circuit.

This public/private key solution also makes sure that the TELUS AD Sync client can only connect with the TELUS host that contains the private key. This information is contained in the MSI package.

TELUS does not recommend using HTTP connectivity.

There are no special ports required or used other than those used by the various technology setups. The TELUS AD Sync client uses whatever HTTP configuration that the Domain Controller uses.

Managing password policies

The password complexity and expiry policy are essentially controlled by the customers on-premises AD. In order for the solution to work, the TELUS hosted Active Directory must have either the same or a more lenient password policy than the customer password policy in order for passwords to be successfully synchronized.

The password policies of the supplied credentials are dependent on the TELUS host Active Directory password policy. This means that if the credentials from the client do not meet the policy requirements of the TELUS hosted Active Directory, then the password sync will fail.

Summary

The TELUS AD Sync utility is a simple solution that makes it easier for end-users to consume hosted services. The solution is designed to help businesses that have an existing Active Directory infrastructure.

Some of the key benefits include:

- IT Administrators can continue to use the same tools for managing their users.
- Automatic creation and deletion of users in the hosting environment based on the customers own Active Directory. This minimizes costs and maintenance to the customer.
- Users no longer need to remember an additional password for their hosted services; they can manage their credentials in one place.
- This is a cost effective and practical solution for identity management that is designed for professional hosting environments managed by TELUS.

TELUS Whitepaper
Version 2.0
Updated: May 2010

C2301-7/10