# Teams Direct Routing - Tenant Configuration

Document Definition:

This document describes the High-Level architecture and implementation provided by the HALO platform in a customer's Microsoft Tenant. This implementation facilitates the requirements for Microsoft Teams Direct Routing and Service Management using the HALO platform.

Tenant Configuration Overview:
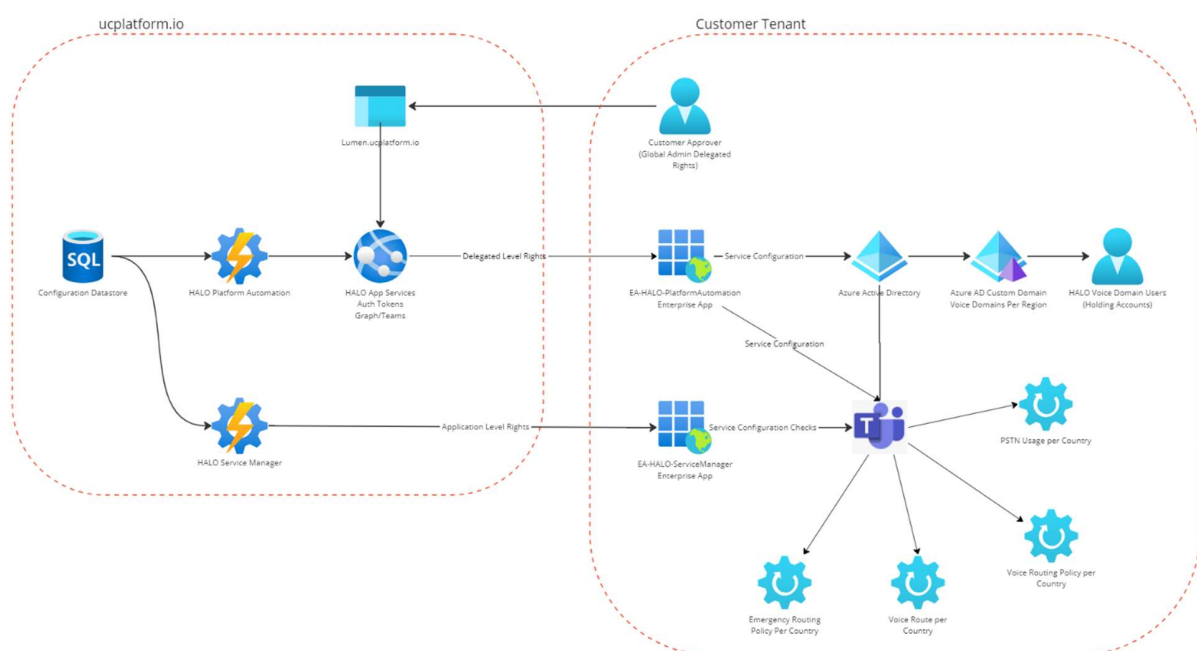
High Level HALO Service Details:

The below sections detail out the specific elements implemented in the customer's Tenant and the standards they were implemented to:

Enterprise Applications:

Enterprise applications have two access types:

> **Delegated**: The customer's global admin must log in to allow the application the rights to perform the actions. Actions can only happen during the customer's login

Application: The global admin approves application level rights to the customer's Tenant. From this point on the application can perform these approved rights whenever required.

The HALO Platform users three different Enterprise Applications to control permissions used while performing different actions in the platform.

Enterprise Application 1 – Tenant Configuration Changes:

HALO performs all Microsoft Tenant configuration changes, using an Enterprise App. You are asked to perform a login to this Enterprise Application, only when changes are required. The actions then performed in your Tenant, utilise the account details you have just logged in with, in most cases this requires a Global Administration Role.

**** This Enterprise Application automatically removes itself, after the configuration changes in your Microsoft Tenant have completed ****

Element	Detail
Name	EA-HALO-PlatformAutomation
Role	All required Tenant changes including base Teams Voice configuration, Custom Domain Creation and Service Account Creation and Licensing
Access Type	**Delegated**

Rights:

Name	Platform	Type	Permission
Application.Read.All	Microsoft Graph	Delegated	Find Enterprise App (Self)
Application.ReadWrite.All	Microsoft Graph	Delegated	Remove Enterprise App (Self post configuration)
offline_access	Microsoft Graph	Delegated	Maintain access to data you have given it access to
openid	Microsoft Graph	Delegated	Sign users in

profile	Microsoft Graph	Delegated	View users' basic profile
User.Read	Microsoft Graph	Delegated	Sign in and read user profile
User.Read.All	Microsoft Graph	Delegated	Read all users' full profiles
User.ReadWrite.All	Microsoft Graph	Delegated	Read and write all users' full profiles
Domain.ReadWrite.All	Microsoft Graph	Delegated	Read and write domains. Create domains
Organization.Read.All	Microsoft Graph	Delegated	Read organization information
Organization.ReadWrite.All	Microsoft Graph	Delegated	Read and write organization information
Directory.Read.All	Microsoft Graph	Delegated	Read directory data
Directory.ReadWrite.All	Microsoft Graph	Delegated	Read and write directory data
RoleManagement.ReadWrite.Directory	Microsoft Graph	Delegated	Read and Write Directory RBAC Settings
user_impersonation	Microsoft Teams	Delegated	Access Microsoft Teams and Skype for Business data as the signed in user

Enterprise Application 2 – Service Management:

HALO performs continuous checks on your Microsoft Tenant, against the Service Profile we have for your Service in our Systems. If your Service Profile changes (Add numbers in a new site or region globally) or something is removed by mistake in your Tenancy, then Service Manager will detect the misconfiguration and inform your technical contacts to perform a repair / update in your Microsoft Tenancy using ucplatform. The repairs will be fully automated and use Enterprise Application 1 listed above and its rights. The Service Manager

Enterprise Application is only used to Read and will never make changes in your Microsoft Tenant

Element	Detail
Name	EA-HALO-ServiceManager
Role	Configuration Health Checks and read User Management Information for Number and License Assignment
Access Type	**Application**

Rights:

Name	Platform	Type	Permission
Domain.Read.All	Microsoft Graph	Application	Read Domain Info (Check voice domains)
GroupMember.Read.All	Microsoft Graph	Application	Read group members (Find members assigned Voice Routes via Groups)
User.Read.All	Microsoft Graph	Application	Read User Info (Find users assigned Voice Routes directly)
Organization.Read.All	Microsoft Graph	Application	Read organization information (Required for Teams API access)
Teams Administrator	RBAC	Role	Access to Teams voice settings

Enterprise Application 3 – Teams User Management:

HALO has a feature to allow the assignment of Microsoft Licenses and Direct Routing Telephone Numbers to Users in your Microsoft Tenant through the UCPlatform. This utilises a specific Enterprise App with the rights to perform the required actions in your Microsoft Tenant. It is delegated right and requires a user to login and perform the actions on the portal. Without that login the Enterprise App is dormant.

Element	Detail
Name	EA-HALO-TeamsUserManagement

Role	Assign users with Microsoft Licenses and Direct Routing Telephone Numbers
Access Type	**Delegated**

Rights:

Name	Platform	Type	Permission
RoleManagement.Read.Directory	Microsoft Graph	**Delegated**	Read directory RBAC settings (Check user has correct RBAC role to perform actions)
User.Read	Microsoft Graph	**Delegated**	Sign in and read user profile
User.ReadWrite.All	Microsoft Graph	**Delegated**	Read and write all users (Change Microsoft licenses eg Teams Phone Addon License)
User_impersonation	Teams Admin API	**Delegated**	Access to Teams voice settings (Change Voice Routing Policies for users)

Teams Direct Routing:

During the Teams Voice configuration process, various elements are created in your Microsoft Tenant. HALO automatically picks up what your Service Profile is and Configures your Tenant in line with this. This will include National and International Call Policies in every country you have Telephone Numbers active for this Teams Direct Routing Service.

Below is a Service Elements table that breaks down the standards in which we configure settings in your Microsoft Tenant. An LLD will be automatically provided to you at the end of the configuration processes, that will have Tables detailing out all the exact names of the Elements configured in your Microsoft Tenant.

Service Elements:

Element	Detail

Number of PSTN Domains	Two Per Region (Maximum 6 if active Globally)
PSTN Domain Prefix	HALOCustomerID + OneNumber + RegionCode
PSTN Domain Suffix	halo.sipcom.cloud
Number of Users	One Per PSTN Domain (Maximum 6 if active Globally)
Number of Licenses	One Per User (Maximum 6 if active Globally)
AD Users Name	Name: HALO.EnterpriseVoice
AD Users Display Name	Name: HALO.EnterpriseVoice DO NOT DELETE
AD Users Permissions	None - Base Account Only
AD Users Password	Randomly generated complex password - Not saved (cache only)
National Call Policy Identity	CountryISO2Code + " National Calls"
International Call Policy Identity	CountryISO2Code + " International Calls"
Emergency Call Policy Identity	CountryISO2Code + " Emergency Calls"
Domestic Voice Routing Policy Identity	"VRP_" + CountryISO2Code + " National_Calling"
International Voice Routing Policy Identity	"VRP_" + CountryISO2Code + " International_Calling"

Tenant Configuration process:

When following the automated provisioning process for a customer's Tenant, a number of actions are performed by the HALO provisioning platform. These actions are detailed below:

1. **Approval to implement Teams Direct Routing in the Customers Tenant**
   - Global admin approved the access to the customers Tenant, to complete the Teams Direct Routing provisioning process.
   - An Enterprise Application is added to the Tenant for authentication and access control via permissions embedded in the application.
2. **Custom domains added to the customer's Tenant based on PSTN Gateway requirements**
   - Based on the countries in the customer's order, two domains are configured in each region for high availability purposes. As an example, If the customer has

UK and US presence, then four domains will be configured, two for EMEA to provide service to the UK and two for AMER to provide services in the US.

3. **Customer selects which Licenses are used in their Tenant to active the Custom Domains used as PSTN Gateway.**
   - These choices are made in the HALO provisioning portal, during the provisioning process

4. **Domain Users added and Licensed to each Custom Domain initializing the Microsoft services including PSTN Gateways.**
   - For a Domain to be live and used for Teams Direct Routing, it must have an active user and that user must have a valid license. As soon as the license is added, the Tenant begins automatic configuration of Microsoft Services. This allows the domain to be used as a valid PSTN Gateway

5. **Microsoft Teams is configured for Direct Routing**
   - Global PSTN Usage updated to add Usage locations for all the customers countries in the order, for domestic dialling, international dialling (if selected) and for the default emergency dialling policy per country
   - Voice Routing policies are configured for each country in the order that link to the specific PSTN Usage Location, both National and International
   - Voice Routes added for each country linking the polices togethers and adding the specific dial codes for that country. For example, if the customer is in the US the US voice route will link any calls for +1 to the AMER PSTN gateways

6. **Emergency Dialling Policies configured based on the countries in the customer's order**
   - Country specific emergency dial policies added, linked to country specific PSTN gateways.
   - Global Emergency policies updated to link country specific emergency dial codes to Country specific emergency policies. For example in the US 911 is linked directly to the AMER PSTN gateways.

7. **Configure HALO Service Manager**
   - Enterprise Application added to the domain with basic rights to monitor the service configuration and pull back user information for User management inside the platform
   - The Application must be approved by a Global Administrator to be Added
   - Service Manager then perform initial health checks to confirm your configuration is correct

After the above actions are completed, the Tenant is ready for Direct Routing with Service Management