

Call2Teams Access and Data Handling Overview

dstny

Table of Contents

Scope 3
Definitions 3
Service Access 3
Microsoft 365 Administrator Scope and Impact 3
Microsoft 365 Admin Rights 3
Service “Sync Now” Feature Scope and Impact 3
Logging 4
Service Diagnostics 4
Media Capture 4
Personally Identifiable Information Scope 5
Data Fields 5
Customer Configuration 5
Admin User Configuration Data 5
Teams Configuration Data 5
PBX / Trunk Configuration Data 6
Customer Logs 7
Billing Data 7
Data Retention 8
Network Facility Locations 8
Additional Services and Features 9
Call2Teams Go Feature 9
Dynamic Emergency Trunk Service 9
Version Control 9

Scope

This document provides information regarding the security and data retention of The Service in line with the Dstny Security White Paper[1].

As The Service is under continuous development, the scope of data stored, and configuration elements relating to these may change at any time.

Definitions

“Partner”, “The Partner”: Any entity entering into a contractual relationship with Dstny to resell The Service.

“Customer”: Any entity consuming The Service.

“Customer tenant”: A Microsoft term used to describe a specific instance of an Microsoft Active Directory containing accounts and groups, specifically a Customer’s Microsoft 365 or Azure tenant for the purposes of this document.

“The Service”: The Call2Teams product and all aspects pertaining to it.

“The Portal”: The Service’s browser-based web interface.

“User“: Any entity who consumes a service license for administration or usage of The Service.

Service Access

Microsoft 365 Administrator Scope and Impact

Set-up and use of The Service requires specific changes to be made to a Customer’s Microsoft 365 tenant.

There are two ways these changes are performed:

- Use of the The Service’s ‘Sync Now’ function, accessed by the Portal.
- By direct PowerShell instructions to manually configure the Customer tenant.

The choice of manual or automated configuration is at the discretion of the Customer.

Microsoft 365 Admin Rights

- Customers must grant The Service *Global Admin* rights to their Microsoft 365 tenant for the initial setup and any changes to regions.
- Customers must grant The Service *Teams Admin* rights for subsequent user provisioning.

Service “Sync Now” Feature Scope and Impact

The Sync Now function uses the Microsoft Graph API and Remote PowerShell to make the changes on the customer’s tenant.

1 https://26142657.fs1.hubspotusercontent-eu1.net/hubfs/26142657/Files/dstny-security-white-paper.pdf

To achieve the access level required by the automated functions, a user with the required admin rights on the target Microsoft 365 account will invoke the process.

When the user clicks the Sync Now function two requests are made of the user to grant permission to make changes to the Microsoft 365 account using *MicrosoftTeams PowerShell* functions.

By accepting these requests, an access token is taken from the user's session by the Portal and is used by the automatic configuration process. The access token is time limited and currently Microsoft have set a 1-hour life to this token.

No administrator access credentials are stored by the Portal.

The automation makes several changes to the Customer tenant. These are mainly to configure Direct Routing in Carrier Mode and manage users.

Full details of the initial setup part of the process can be found in Microsoft's deployment guidance here: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants

The initial configuration changes include:

- Adding custom domains to the Microsoft 365 account.
- Using a spare licence in order to create a user to activate the domains for voice services,
    - Removing these temporary users after the process is complete.
- Creating dial-plans.
- Creating SBC Voice Routing Policies.

The Sync Now automation also reads data from the Customer tenant to discover Users that are licenced for Phone System and voice services.

Additional functions such as setting user's voice routing policy, phone numbers and voicemail/ forwarding policy are performed by the Sync now function.

The only pertinent to the configuration of the Microsoft Phone System functions and the Direct Routing set-up are made to the Customer tenant.

A log of all activities performed by the automatic configuration process is provided for the Customer to review.

Logging

Service Diagnostics

Sync Now activity is logged and retained as described below. Customers may be asked to perform a 'Diagnostic Sync' if there is a problem that requires more information to be made available by the support desk.

The diagnostic sync collects data about the Customer's tenant, users, and licencing for this purpose. This sync data can be deleted from the Portal manually, or will be automatically removed after 14 days.

Media Capture

Call media can be captured in line with the Dstny media capture policy to assist with diagnosing issues. This is only done through dialog with, and approval from, the Partner.

Media captures are only kept as long as is necessary to resolve the reported issue.

Personally Identifiable Information Scope

With respect to Customer data, Dstny is a data processor.

Partners are granted access to the the Portal and may grant access to additional authorized users, including granting access to specific organizations within a Partner's estate (such as allowing a Customer's User administrator level access to their own account).

The majority of data is entered by an authorized User within the Portal and can be amended and deleted in the same way.

Some data is in the form of logs, which are collected automatically based on use of The Service and made available to authorized Users within the Portal for the purposes of auditing, billing reconciliation and troubleshooting purposes.

The level of personally identifiable information entirely depends on that which is entered by authorized Users. This includes use of the 'Sync' functionality to bulk load data from a Microsoft 365 directory into The Service.

The Service is a gateway that maps PBX users to Teams users. The minimum of information that is required depends on the specific PBX but can be as little as the telephone number of each Teams user.

Additional information can be entered in order to simplify the task of administering the mapping between PBX users and Teams users. This includes individual end user's names and email addresses.

Data Fields

The data is split into three components:

- Customer Configuration
- Customer Logs
- Billing Data

It is up to each Partner to determine whether each of the fields below constitutes personally identifiable information based on their own usage.

Customer Configuration

Admin User Configuration Data

For Single Sign-on with Azure Active Directory (AAD) the following user information is stored:

- AAD Tenant Id & AAD Object Id
- AAD Display Name
- AAD Email
- AAD UserPrincipalName

Teams Configuration Data

The following fields are stored for Teams Users.

- When the 'sync' feature is **not** used then the only users stored are those selected by the Partner according to their Customer's specification.
- When the 'sync' feature **is** used then all eligible Teams users are stored.

Field	**Without 'sync' feature**	**With 'sync' feature**
Display Name	Required. Entered by The Customer	Auto-populated from AAD *User.Name*[2]
UserPrincipalName	Not required	Auto-populated from AAD *User.UserPrincipalName*
Email	Not required	Auto-populated from AAD *User.Email*
External Id	Not required	Auto-populated from AAD *Tenant Id & User.Object Id*
Phone Number	Required. Entered by The Customer	Required. Entered by The Customer
Country	Not required	Auto-populated from AAD UsageLocation

PBX / Trunk Configuration Data

The following fields are stored for all users of The Service. All records created by The Customer are stored at the point of creation, either when entered into the Portal or when pre-populated by the API.

Field	**Purpose**
SIP Realm	Required configuration data.
SIP Username	Required configuration data.
SIP Auth Username	Optional (depends on PBX/trunk requirements)
SIP Password	Optional (depends on PBX/trunk requirements)
Display Name	Optional (API-only). Used to cross-reference Teams data to link user parts

2 http://User.Name

Email	Optional (API-only). Used to cross-reference Teams data to link user parts
Phone Number	PBX: Optional (API only). Used to cross-reference Teams data to link user parts Trunk: Required
Country	Required. Used to select the closest media POP

Customer Logs

- SIP messages (registrations and call logs)
- Sync logs - contains details of changes made which may include user configuration data
- “Debug” Sync logs contain details of every user in the Partner’s customer’s Azure Active Directory, not just users with a qualifying license
- Registration logs – records of recent registration attempts and their success status
- Call logs – records of recent calls and their success status

Billing Data

For Partners, the following fields are stored to add meaning to historic billing transaction data:

- Organization Name
- External Reference

Data Retention

Data Type	**Retention Period**	**Grounds for Retention**
Customer Configuration data	Retained indefinitely unless the Partner's account(s) have no active subscriptions, in which case data is deleted 14 days after the last active subscription ends.	Necessary for operation and maintenance of The Service.
Customer Sync logs	Logs are deleted when the Partner disables sync or when configuration data is deleted.	Necessary for diagnostics, operation, and maintenance of The Service.
Sync debug logs	Deleted 14 days after collection.	Necessary for diagnostics, operation, and maintenance of The Service.
Billing Data	Retained indefinitely.	Necessary for financial reporting.
Service logging	Deleted up to 90 days after collection.	Necessary for diagnostics, operation, and maintenance of The Service.

Network Facility Locations

The Service operates with global presences from the following locations. Service presence is generally based on geographic availability, unless specified by customer requirement:

Location
US East
US West
Singapore
Australia Central
Australia East

Japan East
Japan West
EU North
EU West

Additional Services and Features

Call2Teams Go Feature

As Call2Teams Go is wholly dependent on the Service to be able to function, all features of this document also apply to it. The following additional data is handled when the feature is consumed:

- To enable the Go feature, the Service needs to make license assignments in the Partner's Customer's tenant.
    - This uses a Teams Phone Resource Account license which must be obtained by the Partner's Customer.
    - This persists for the duration of the use of the Service, and is necessary for the operation of the Service.
- Where the end user makes changes to their private contact list, the Partner's Customer's tenant is modified to store these changes.
    - This is handled as per the *Customer Configuration data* section of the Data Retention table above.
- Service logging is performed for the Go feature.
    - This is handled as per the *Service Logging* section of the Data Retention table above.

Dynamic Emergency Trunk Service

Where the DET feature is consumed by a Partner’s customer, the following additional data can be handled when the User makes an emergency call:

- Location data for dispatch in PIDF-LO format
    - This data is also logged for billing and service reporting as per the Data Retention table above, where applicable.

Version Control

Version	Purpose	Prepared By	Approved	Date
1.0	Updates	AD	RF	14 March 2024



Call2Teams Access and Data Handling Overview