

 Board Connect
System Architecture Design

Vendor Engage Squared
Details: (03) 9111 0082
 engagesq.com

Date: 9 June 2021

Prepared By: James Di Blasi
 CTO
 +61 412 352 272
 James.diblasi@engagesq.com

Contents

1	Technical overview	3
1.1	Overview	3
1.2	Terminology.....	3
2	High-level Architecture	4
2.1	Overview	4
2.2	Components	5
2.3	Installation	8
2.4	Data	9
2.5	Access management.....	10
2.6	System Management.....	11
2.7	Removing Board Connect	12
3	Appendix A.....	13

1 Technical overview

1.1 Overview

Board Connect helps organisations to run smarter, more effective meetings.

As a Microsoft Teams Application, Board Connect brings together documentation and meeting details relating to board or committee meetings into one easy-to-use location.

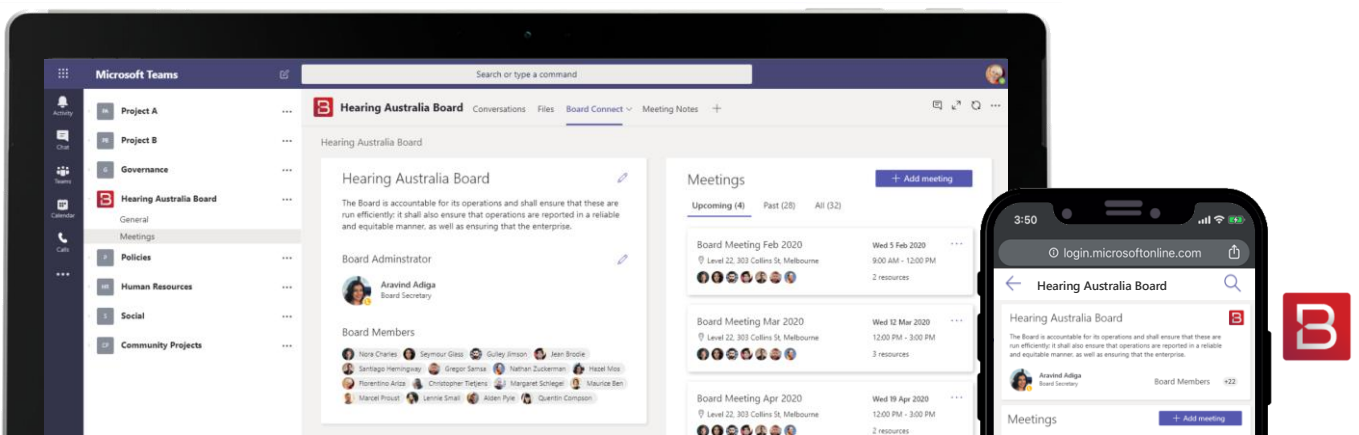
The application has been approved and published to the [Microsoft AppSource Store](#), making it one of the only Microsoft Teams-based meeting management applications on the market.

The Board Connect application is currently hosted out of Microsoft's Australia Southeast Azure data centre. We have the flexibility to host Board Connect in *any* Azure data centre, based on our customers' needs.

This document's purpose is to provide an overview of the system architecture and processes that are in place for Board Connect, to describe how we ensure a secure and intelligent application.

1.2 Terminology

Term	Description
Azure	Microsoft Azure, Microsoft's cloud computing services for application and data management.
Azure AD / AAD	Azure Active Directory – Microsoft's cloud-based identity and access management service.
RBAC	Role-based access control.
Home tenant	Azure AD tenant where the Azure AD application registration resides.



2 High-level Architecture

2.1 Overview

Board Connect makes use of four main components:

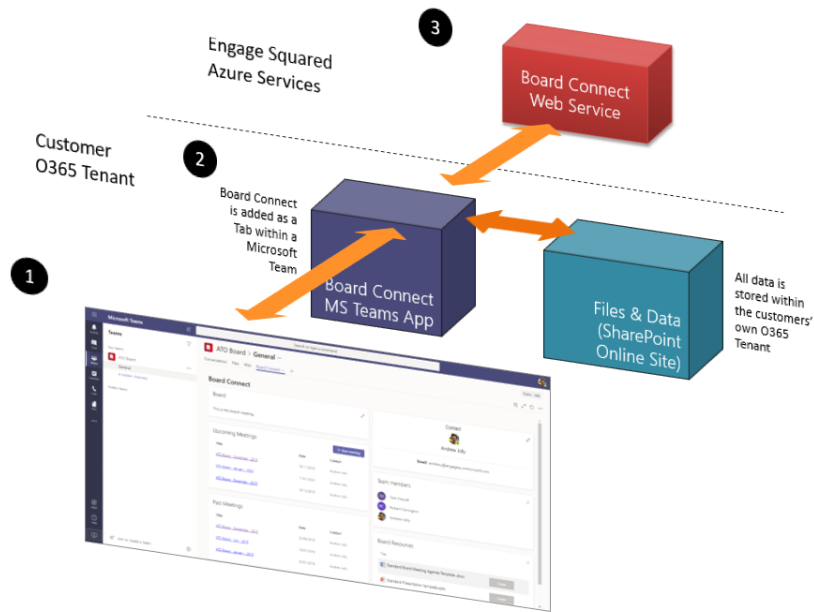
1. **Microsoft Teams:** Board Connect runs within Microsoft Teams (in the desktop application, web browser or mobile application)
2. **Teams App (hosted in your Teams tenant):** Board Connect is installed in Teams as a 3rd Party App. The App can be installed from the [Microsoft AppSource store](#), or as a custom application provided to you by us and installed into your local Teams app gallery.

The app 'registers' Board Connect in Teams, respects the Teams policies and settings that you have configured, and provides users with access to the Board Connect web application via a tab within their Teams channel, and / or using an app in the Teams app bar.

3. **Web Application (hosted in Azure):** the user interface of Board Connect is hosted as a web application in Azure. When users load Board Connect in Teams, the web application is called, the user is authenticated, and then the user can then interact with the web application.

The web application is hosted in Azure and uses the Microsoft Graph API to access resources within your Office 365 tenant on behalf of the logged in user (using delegated permissions); resources accessed by the application include:

- Information about the current Team, including the team name and membership
 - Files and list data stored in the SharePoint site associated with the team
 - Profile information about the current user and other members of the Board
4. **Azure Active Directory:** Azure Active Directory is used to secure Board Connect; two key features are used:
 - User access to Board Connect is controlled through Azure Active Directory user authentication (and respects advanced features, such as conditional access policies)
 - Data in your tenant is accessed using access tokens supplied by the Azure Active Directory App Registration (based on permissions that you grant during installation)



2.2 Components






2.2.1 SharePoint

All content in Board Connect is stored within the SharePoint site that sits behind the Team. All of your Board and Committee data is therefore housed within your tenant, and the Board Connect service does not transmit any meeting data outside of this area.

When Board Connect is first added to a team (including when it is first installed), the application creates the following *hidden* lists in the SharePoint site associated with the team:

- **Meetings** (internal name: E2BCMeetings): stores metadata related to meetings that are scheduled in Board Connect, including meeting title, time and date, attendees etc..
- **Meeting Topics** (internal name: E2BCMeetingTopics): stores agenda items
- **Config List** (internal name: E2BCConfigList): captures and stores settings configured for Board Connect through the settings / admin menu
- **Votes** (internal name: E2BCVotes): stores poll questions and motions
- **Vote Responses** (internal name: E2BCVoteResponses): responses to poll questions and motions from board members
- **Templates** (internal name: E2BCTemplates): a hidden document library where templates loaded into Board Connect are stored

When a new meeting is created in Board Connect, the application creates a new folder in the Shared Documents library in the SharePoint site associated with the Team, for example:

 Name ▾	Modified ▾	Modified By ▾	+ Add column ▾
 August Board Meeting	June 14	Justin McPhee	
 Board Meeting August	May 21	Andrew Jolly E ²	
 Board meeting November 2020	Tuesday at 3:31 PM	Thomas Lalor E ²	
 Board meeting October 2020	September 8	Andrew Jolly E ²	

2.2.2 Board Connect Web Application

The Board Connect Web Application provides the smarts for logic and processing, applying configuration to your Teams, creating and managing data structures and applying security to your SharePoint data store. All data is stored in your tenant, and not accessed by the web application.

2.2.3 Authentication and Authorization

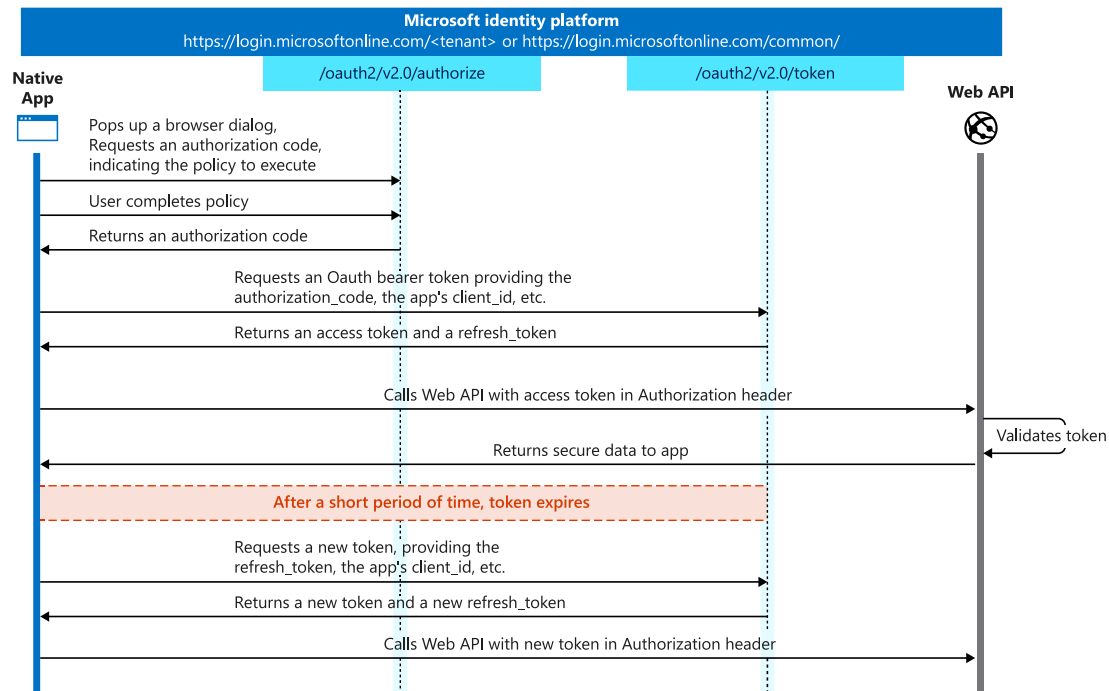
Board Connect has been implemented as an Azure AD application, with a service principal created in each customer's tenant, providing the ability to sign in and grant access to the application to access resources within the tenant.

When Board Connect is given permission to access resources in the customer tenant – that is, once tenant-wide administrator consent to the application is received – the service principal object is created.

This is managed via AAD Enterprise Applications, located within the Microsoft Azure portal, where you can see and manage the service principal permissions.

Board Connect uses the OAuth 2.0 Authorization Code grant type to securely access required protected resources, in particular the Microsoft Graph API and SharePoint REST APIs. The OAuth 2.0 Authorization Code flow is used to perform authentication and authorization, with the flow enabling Board Connect to securely acquire access tokens that can be used to access resources secured by the Microsoft identity platform endpoint. This method also supports Board Connect acquiring refresh tokens to get additional access tokens and ID tokens for the signed in user.

At a high level, the entire authentication flow for the application can be represented by the below diagram:



2.2.3.1 API Permissions

When granting tenant-wide administrator consent to the Board Connect service principal to access protected resources within your tenant, the following delegated permissions are requested.

API	Permissions	Used for	Admin Consent Required
Microsoft Graph	User.Read	To allow users to sign-in to the app and allow the app to read the profile of the currently signed-in user.	No
Microsoft Graph	User.ReadBasic.All	To allows the app to read a basic set of profile properties of other users on behalf of the signed-in user, in order to display this in the app. This includes display name, first and last name, email address and photo.	No

Microsoft Graph	offline_access	To enable the app to get a refresh token, which it can use to get a new access token when the current one expires.	No
Microsoft Graph	Group.ReadWrite.All	To allow the app to create, update and delete group calendar events.	Yes
Microsoft Graph	Sites.Manage.All	To allow the app to create lists and libraries, manage list items and manage documents on a team site collection.	No
Microsoft Graph	Calendars.ReadWrite	To allow the app to update user calendars to reflect their board meeting attendance responses submitted via the app.	No
Microsoft Graph	Notes.ReadWrite.All	To create, update, delete OneNote entities	No
Microsoft Graph	TeamsActivity.Send	Send Teams Activity Feed notifications	No

2.3 Installation

The Board Connect Teams application has been approved and published in the Microsoft Office Store for Teams applications, and into Microsoft AppSource.

The Teams application has been set up as an Azure AD application registration, with a globally unique instance of the app that resides in a secure 'home tenant'.

When Board Connect is added to a customer's tenant, a service principal is created which is a *local* representation in a specific tenant.

The service principal is created in each customer tenant where Board Connect is used, to establish an identity for sign-in and access to resources secured by the tenant.

Please see section Authentication and Authorization for more information.

2.4 Data

2.4.1 Data stored by Board Connect in Azure

Next customer-related information is stored in the app telemetry and logs:

Name	Description
Tenant Id	It is a globally unique identifier (GUID) of a Microsoft 365 tenant, that is different than organization name or domain name.
Team Id	It is a globally unique identifier (GUID) of a Microsoft Teams team, which has a Board Connect Tab installed.
User Id	It is a globally unique identifier (GUID) of a user, who interacts with any instance of Board Connect app.

2.4.1.1 Storage location

Board Connect is hosted and managed on Microsoft's highly secure and universally trusted Azure platform, and all Azure-based services and data used for Board Connect are currently hosted out of the Australia Southeast Azure data centre. It is possible for a customer to choose a different data centre for hosting their Board Connect instance should that be required.

2.4.2 Encryption in transit and at rest

All data is encrypted in transit via HTTPS (port 443). The storage service encryption protects your data at rest. The Azure Storage utilised by the app encrypts your data as it is written to Microsoft Azure data centres, and automatically decrypts it as the application accesses it.

For data transmitted via HTTPS the encryption method and strength are negotiated between the browser and the server. Board Connect has been given an A rating measured by SSL Labs - <https://ssllabs.com>

For encryption at rest, Azure Storage employs Azure Storage Service Encryption (SSE). This employs 256-bit AES encryption. For more details on Azure Storage encryption, refer to: <https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption>

2.5 Access management

2.5.1 Access Controls

Engage Squared access to the Azure Console (i.e. to access Application Insights or the Azure App Service) is protected using two-factor authentication and RBAC.

Role/Group	Function	Location	Access Rights
Board Connect – System Administrator	To administer the application	Australia	Full access to Application Insights, storage tables and the App Service
Board Connect – Support	Providing end-user support	Australia	Access to sanitised logging information, which primarily highlights any errors that may occur

2.5.2 Board Permissions

From an end user perspective within Board Connect, Board Connect currently operates with four key roles:

- **Teams Owner;** has access to complete all available board wide configuration actions within the board.
- **Meeting Owner;** has access to key functionality within the meeting such as completing roll call
- **Primary Administrator;** Is added as a Microsoft Team Owner, and can do everything a Microsoft Teams Owner can do, as well as the meeting owner.
- **Secondary Administrator;** Is added as a Microsoft Team Owner, and can do everything a Microsoft Teams Owner can do, as well as the meeting owner.
- **Normal user;** can interact with the board, create agenda items, meetings etc.

2.6 System Management



2.6.1 Storage Redundancy

Azure Storage redundancy and geo-redundant storage

Azure Storage replicates multiple copies of your licensing and subscription data so that it is protected from events such as transient hardware failures, network or power outages, and natural disasters. Data is replicated three times in the primary region (primary data centre), and in addition the storage that Board Connect uses for licensing and subscription data is configured for geo-redundant storage, with data copied in a second geographic region (secondary data centre). If an outage renders the primary endpoint unavailable, then we can initiate a failover to the secondary endpoint to rapidly restore access. [Learn more](#)

For Board Connect, the default primary region (data centre) is Australia Southeast and the default secondary region is Australia East, but with the flexibility for Board Connect to be hosted in any Azure data centre, based on our customers' needs.



Location	Data center type
 Australia Southeast	Primary
 Australia East	Secondary

2.6.2 Backup Management

Organisation data

All the data you interact with while using Board Connect is stored within your Microsoft 365 tenant (primarily in SharePoint Online). Other than licensing and sanitised logging information, we do not take any of your data out of your tenant.

Please note: Data in your Microsoft 365 tenant will be subject to Microsoft's standard data storage and backup methods.

Board Connect Application

The Board Connect application service(s) are backed up daily at 11am (AEST) and backups are retained for 30 days.

All backups are retained within the Australia Southeast data centre.

2.6.3 Logging

Board Connect currently utilises Microsoft Application Insights, hosted within Azure, for monitoring and logging.

Only sanitised diagnostic data is logged to our hosted Application Insights service. The data that is transferred does not include any content that is added to a customer's Board Connect instance – that is, no specific user, meeting, file or configuration data is stored as it is written within the application; rather, we log correlation IDs that relate to events. Events logged by the application, including user access, errors etc. Please See Appendix A for all data stored by Board Connect.

2.7 Removing Board Connect

To fully remove Board Connect from your tenant, in addition to removing the installed Microsoft Teams application, you should also remove the Azure service principal used to facilitate resource access for the application. The steps to do so are described in [this support article](#) on the Board Connect website.

3 Appendix A

The information that is to be stored within our telemetry.

- **timestamp**: time of the event
- **name**: name of the event
- **user_AccountId**: Id (GUID) of the customer's tenant
- **customDimensions.teamId**: Id (GUID) of the team/group on the target tenant, where the BC app installed.
- **user_AuthenticatedId**: Id (GUID) of the user on the target tenant