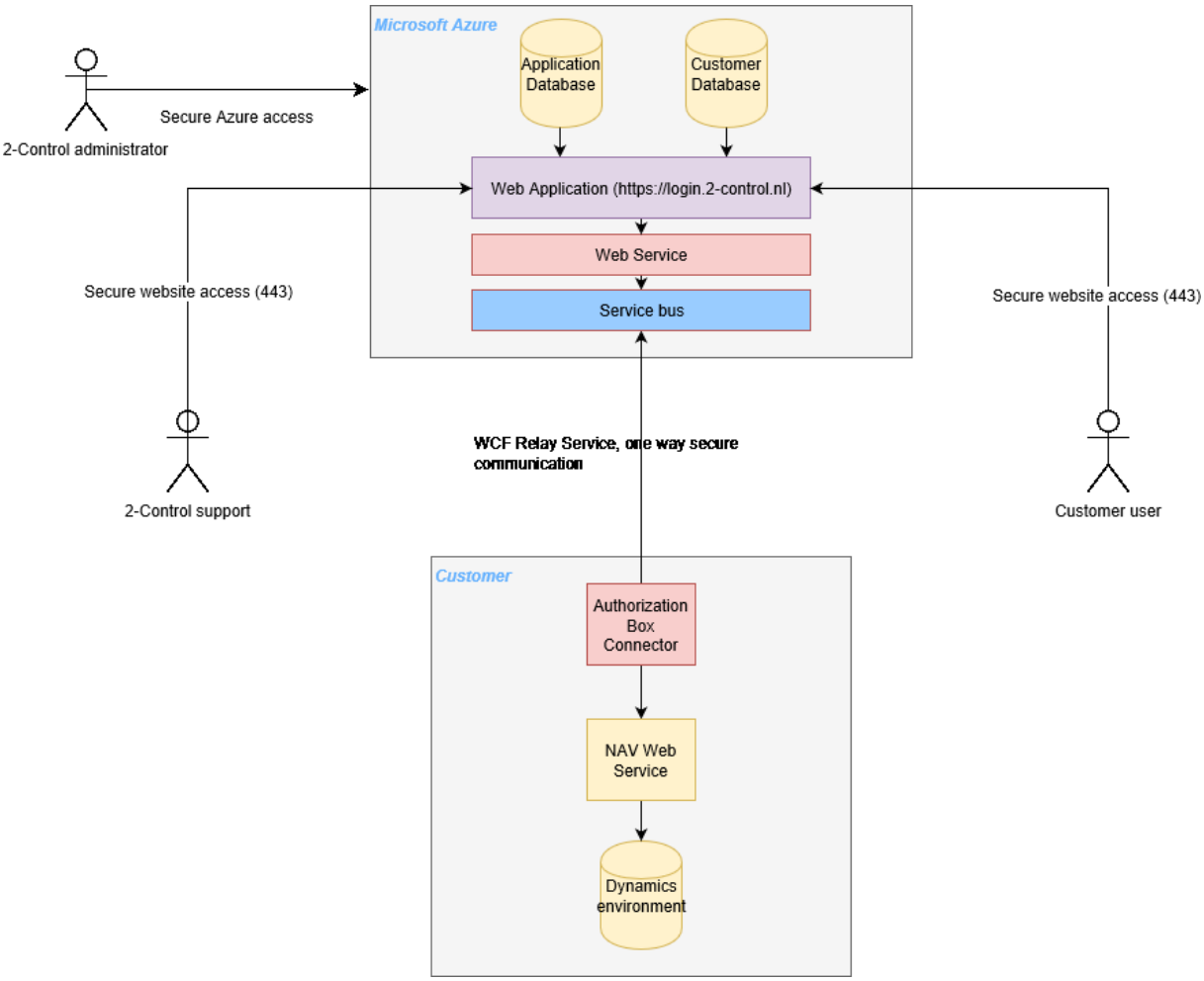
1 Security Authorization Box on Azure

This document describes the technical security aspects of Authorization Box on Azure in relation to your Dynamics environment. If you have any further questions, please contact us at support@2-control.nl or +31 76 501 9470.

2 Architecture

The architecture of Authorization Box on Azure is depicted in the following image. Each component is described below the image.



The application consists of the following components:

1. ***Microsoft Azure***:
    a. *Azure SQL Databases*: we maintain two SQL databases, an Application Database and a Customer Database. The Application Database is for maintaining data that is consistent for all users, the Customer Database is used to store specific customer content. See below in this document for a description on which data this concerns;
    b. *Azure Web App*: we use an Azure Web App to deploy our website https://login.2-control.nl. This website is secured with our company certificate and communication (and mutations) to the Azure SQL Databases is only established through this web application;
    c. *Azure Relay Service*: inside the Azure Web App we have created a web service endpoint which can communicate with the Service Bus. This web service cannot be reached from the outside internet. The communication protocol is WCF Relay (see https://docs.microsoft.com/en-us/azure/service-bus-relay/relay-what-is-it);

   d. *Azure Service Bus*: we use an Azure Service Bus as communication bus. This service bus receives and distributes all messages from our web app and from the customer;
2. ***Customer environment***:
   a. *Authorization Box Connector*: this is the other end of the WCF Relay implementation. The Authorization Box Connector is a Windows Service which communicates with the Azure Service Bus in a one way construction: the service only pulls messages from the service bus. The service bus does not know where the WCF Relay is located and cannot push any data. The communication for a specific customer is secured by a unique customer security id;
   b. *Dynamics NAV / Dynamics 365 Business Central web service*: in the Dynamics environment there is a web service which can be called by the Authorization Box Connector. This web service is used to retrieve data related to permissions and to perform mutations in the authorization setup;
   c. *Dynamics NAV / Dynamics 365 Business Central database*: the web service can retrieve and modify authorization related data in the Dynamics NAV / Dynamics 365 Business Central database;
3. ***Users:*** we distinguish the following users (actors):
   a. *End users:* end users can access the web application via https://login.2-control.nl and only use the functionality the application provides;
   b. *2-Control support users:* every 2-Control employee can access the web application via https://login.2-control.nl and access the environment for support reasons. We only connect to your environment after your consent;
   c. *2-Control administrators:* 2-Control administrators can access the Azure management environment and maintain the technical aspects of the Azure deployment. Only the managing directors of 2-Control can access this environment. Access to the Azure environment is based on the Azure Active Directory security settings which is default two-factor authentication.

3 Communication

All communication between the Authorization Box Azure environment and the customer site is securely established through the earlier described WCF Relay mechanism. Communication between the web application and end users is always via https secure communication.

4 Data

As mentioned before we maintain two databases: Application Database and Customer Database. See below a description of which data is stored in those databases.

1. Application Database:
   a. Customer general information: name, address, city, contact person, contact mail, contact phone no.
   b. Customer contract information: which products of 2-Control, starting / ending dates, prices;
   c. Customer user information: username, name, phone no. and password of the users that have access to Authorization Box (maintained by the customer). The password is stored based on a best practice encryption method of ASP.Net and cannot be decrypted by 2-Control;
   d. Customer database information: address of the Dynamics web service with credentials of the user that is used to consume the web service. The password is stored based on a strong best practice encryption method (for security reasons we do not mention the used method). This password has to be decrypted for the web service call but is transferred encrypted over a secured connection;
2. Customer Database:
   a. Organizational information: departments and functions and the assigned permissions to those functions;
   b. User information: Dynamics users and their functions and assigned permissions.