# EB Security – On-Premise Setup Guide

This guide is to assist users to install the On-Premise software that will communicate with EB Security Website, and pass traffic through to the EntityBox Security Mobile Solution (EB Security)

Should you require more assistance, kindly send us an email:
support@entitybox.co.za

This product is the link between On-Premise and the EntityBox Security Website.

Required Steps to complete before making use of this guide:

1. EntityBox Website Registration

This guide will assume the above configuration has been completed.

## Table of Contents

# Software Prerequisites

The following software should be installed on your Windows Server platform:

- Latest version of EBSS Server downloaded from our website portal
- Microsoft Windows Operating System: Server 2012-2019
- Microsoft .Net Framework 4.8
  https://go.microsoft.com/fwlink/?linkid=2088631
- Microsoft SQL Server / Express
- Active Directory Service Account / gMSA Account.
- Firewall Static NAT, Reverse Proxy such as Web Application Proxy or Azure AD Web-Proxy.
- Internet Access to communicate with EBSS Website over HTTPS

## Permission Requirements

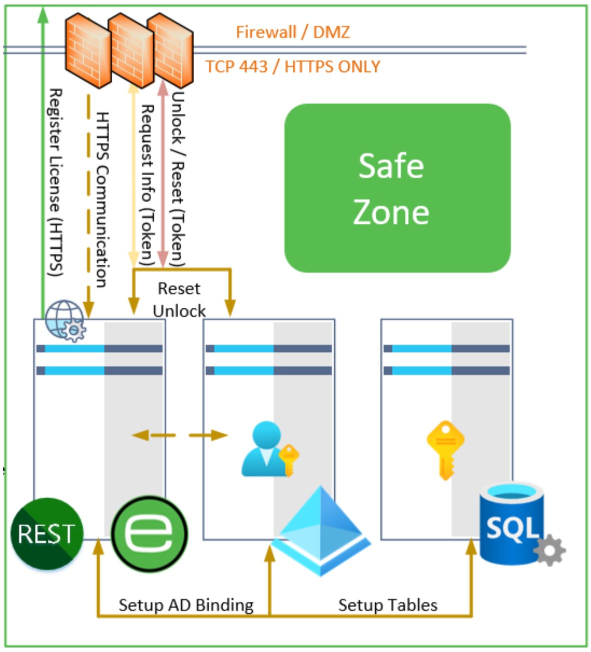
- The installer account should be an Administrator on the Server where the software will be installed.
- The installer account should have SQL Server dbOwner access in order to create the tables, unless Basic Authentication is used.
- Active Directory Service Account / gMSA Account should have Delegated Authority in order to reset and unlock user accounts in the organisation (Account Operators Permission)
- Assistance from the Domain Administrator team should the service run under a gMSA account to setup.
- Assistance from the Networking team to setup the reverse proxy or Static NAT on the firewalls.

## Install Steps Overview

1. Create Active Directory Service Account (or gMSA Account)
2. Delegate permissions in Active Directory as Account Operators for the chosen account.
3. Install SQL Server and Create a new database (EBSS_Server)
4. Assign SQL Permissions to Installer and Service Account as dbOwner on the Database
5. Ensure Internet connectivity settings from the server to the Internet on HTTPS
   https://ebss.entitybox.co.za must be accessible.
6. Install the latest version of EBSS Software downloaded from the portal.
   Current version: EBSS_Setup_1.0.22.exe
7. Configure the Service Startup (if gMSA Account is used)
8. Configure the Service Using Administrator Utility (Enable logging to start)
9. Start the services
10. Test Internal and External Access.

# Architecture (Logical Layout)

Below image indicates the component that will be used in this document:



| System | Description |
|---|---|
| Active Directory | On-Premise Active Directory Domain Controller Instance |
| SQL SERVER 1 | Installed SQL Server or SQL Server Express Instance. Could be installed together with EntityBox Server (SERVER 1) |
| SERVER 1 | EntityBox Security Solution Server that should be installed. |
| NETWORKS | Reverse Proxy Configurations and/or Static NAT Information |

# Active Directory

## Service Account

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-on-premises#choose-the-right-type-of-service-account

## User Account Method

- Create a normal user account in Active Directory Users and Computers (ADUC).
- Create the account with an exceptionally strong password
  ***Recommendation:*** Use at least 18 characters strong with all levels of complexity.
- Remember that User Accounts require password changes, and could lead downtime if the password is set to expire.

## Managed Service Account Method

- Create a gMSA Account on a Domain Controller using PowerShell command
  https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts
- Install the gMSA Account on the Target Server for usage

## Account Delegation

Delegate the permissions for the above Service Account to enable at a minimum:

- Password Reset
- Unlock Account

Larger organisations could already have Active Directory Groups that are delegated with the service desk functions and the service account could just be added to such a group.

If the account is to be added to the "Account Operators" Group, ensure the AdminSDHolder is also updated accordingly.
https://learn.microsoft.com/en-us/previous-versions/technet-magazine/ee361593(v=msdn.10)

***Recommendation***: Do NOT add the service account as a Domain Administrator, either use the Account Operators Group or use the Delegation Wizard in Active Directory.

# SQL Server

a SQL Server is used as the back-end and transactional logging of all activities in the system.
https://www.microsoft.com/en-us/sql-server/sql-server-downloads

Most organisations already have SQL Servers installed. An existing server can be used, or a new one setup. The same server hosting EntityBox Security Solution can also be used as a single server instance.

Database size is depending on the amount of users using the system, and SQL Server Express is more than sufficient to accommodate the database as a start and transition later to a higher version.

1. SQL DB Administrators are required to create the a new database.

2. Assign the dbOwner security role to the Service account created

3. Assing the dbOwner security role to the Installer account (User installing EntityBox)
   (This permission can be removed after installation and functionality is completed)

4. Provide the SQL connection string / information to the installer to use during the setup process.

***Recommendation***: Although the database name could be anything, we recommend to call it "**EBSS_Server**" for conformity of the application, and identification of the system using it.

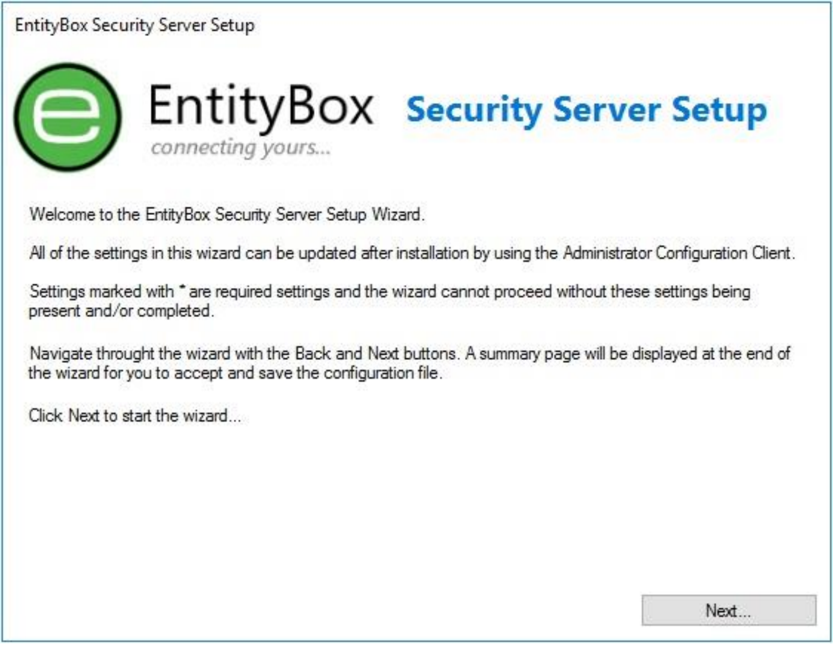
# EntityBox Server

## Software Setup Steps

- Ensure .Net Framework 4.8 is installed on the Server
  https://go.microsoft.com/fwlink/?linkid=2088631
- Download the latest software version from the EBSS Website
  https://ebss.entitybox.co.za | Login | Settings
- Start the EBSS_{VERSION}.exe Setup Software

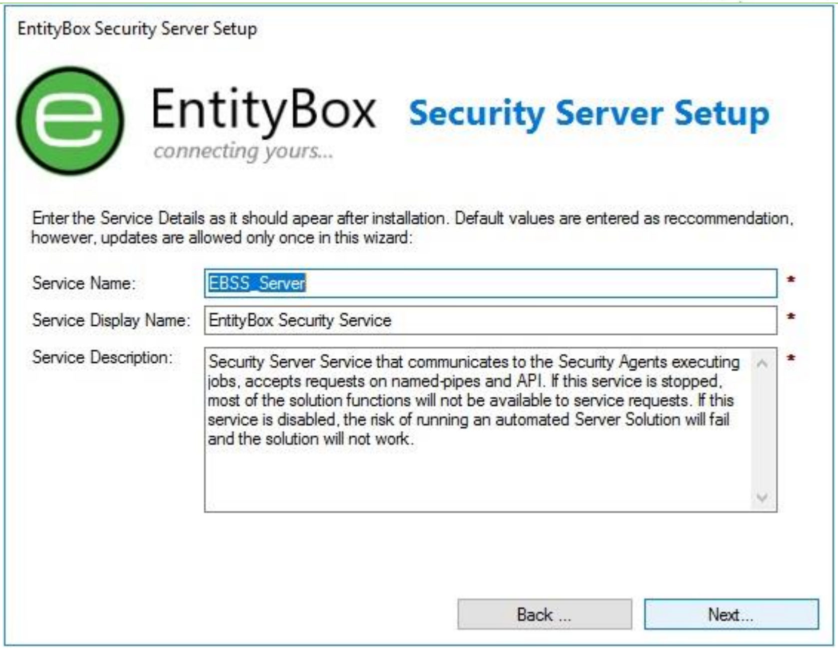
EBSS_1.0.1.22.exe

Below the setup wizard steps explained with relevant configuration information:

| Step | Screen / Description |
|---|---|
| Welcome | <br>EntityBox Security Server Setup<br>EntityBox connecting yours... Security Server Setup<br>Welcome to the EntityBox Security Server Setup Wizard.<br>All of the settings in this wizard can be updated after installation by using the Administrator Configuration Client.<br>Settings marked with * are required settings and the wizard cannot proceed without these settings being present and/or completed.<br>Navigate throught the wizard with the Back and Next buttons. A summary page will be displayed at the end of the wizard for you to accept and save the configuration file.<br>Click Next to start the wizard...<br>Next... |

### Service Details

Service details could be changed although it is not recommended.



EntityBox Security Server Setup

Enter the Service Details as it should apear after installation. Default values are entered as reccommendation, however, updates are allowed only once in this wizard:

Service Name: EBSS_Server *

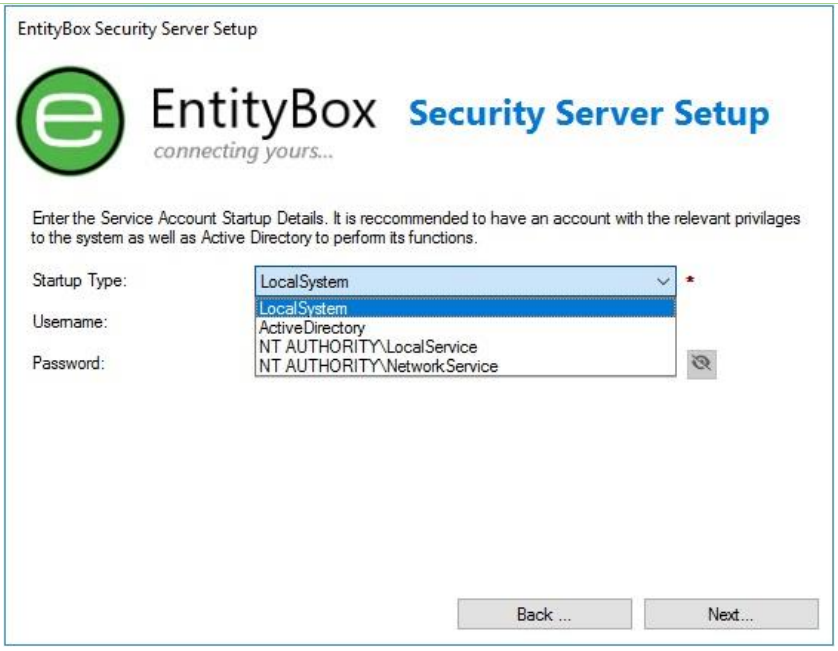
Service Display Name: EntityBox Security Service *

Service Description: Security Server Service that communicates to the Security Agents executing jobs, accepts requests on named-pipes and API. If this service is stopped, most of the solution functions will not be available to service requests. If this service is disabled, the risk of running an automated Server Solution will fail and the solution will not work. *

- Click **Next**

### Service Startup

Use **LocalSystem** if gMSA Account will be used, alternatively select **ActiveDirectory** in order to configure the integrated account.



EntityBox Security Server Setup

Enter the Service Account Startup Details. It is reccommended to have an account with the relevant privilages to the system as well as Active Directory to perform its functions.

Startup Type: LocalSystem *

Username:

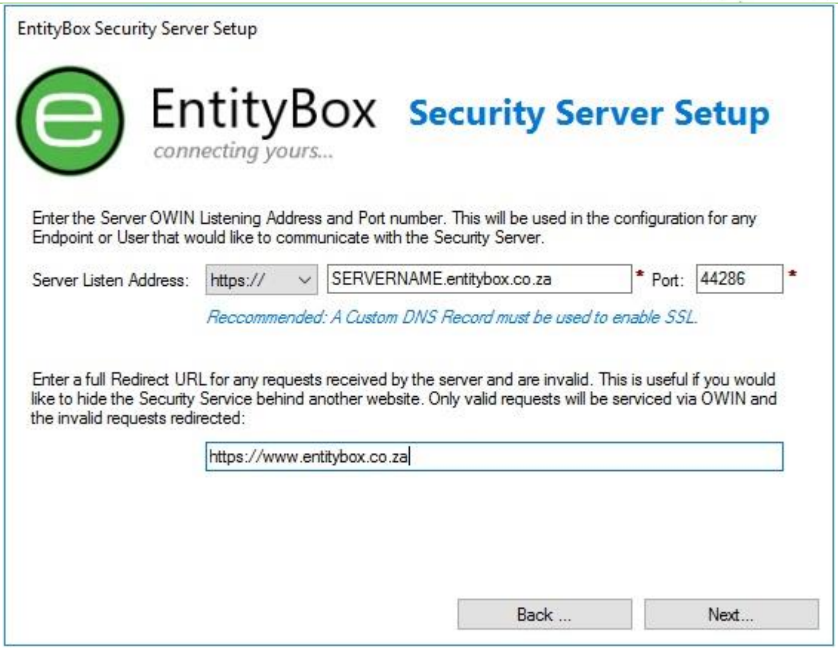
Password:

- Select Service Startup Type
- Configure the Service Login Username and Password
  (Click the "eye" button to ensure password is typed correctly)
- Click **Next**

## OWIN Server Details

Configure the internal listening details on the server.

Default port can be used and changed on the reverse proxy, alternatively change this to https:// & port 443 for SSL.
See SSL Configuration Below



EntityBox Security Server Setup

EntityBox connecting yours... Security Server Setup

Enter the Server OWIN Listening Address and Port number. This will be used in the configuration for any Endpoint or User that would like to communicate with the Security Server.

Server Listen Address: https:// SERVERNAME.entitybox.co.za * Port: 44286 *

*Reccommended: A Custom DNS Record must be used to enable SSL.*

Enter a full Redirect URL for any requests received by the server and are invalid. This is useful if you would like to hide the Security Service behind another website. Only valid requests will be serviced via OWIN and the invalid requests redirected:

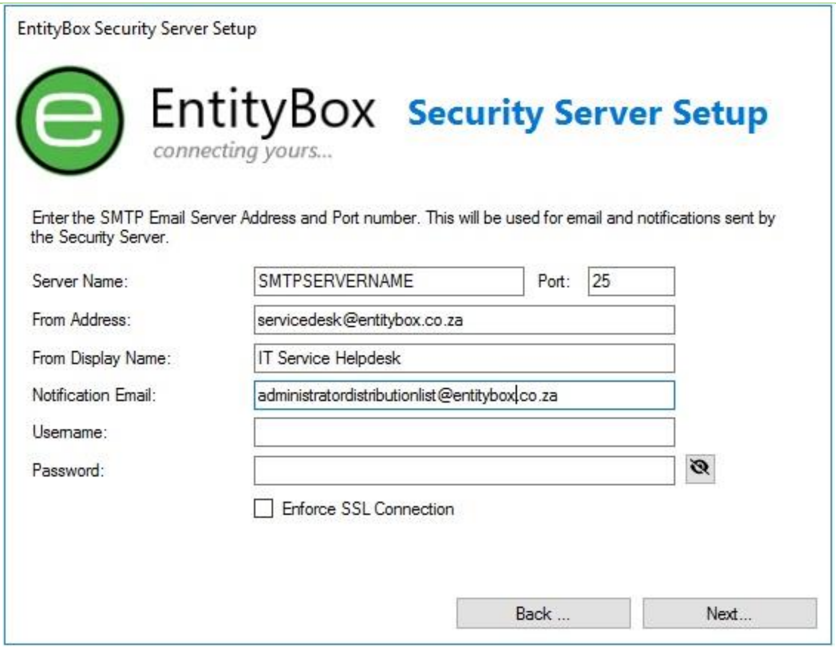
https://www.entitybox.co.za

- Enter Listen Address for OWIN Server
- Enter the company external website address, in the event of someone "snooping" for the API, they will be redirected to the value entered in this URL to "hide" the API from exposure. Only valid request routes will respond
- Click **Next**

## SMTP Server

Emails are sent on notification events, job failures.

Enter your local SMTP Server or Exchange details together with the notification Email address of the administrators.



EntityBox Security Server Setup

EntityBox connecting yours... Security Server Setup

Enter the SMTP Email Server Address and Port number. This will be used for email and notifications sent by the Security Server.

Server Name: SMTPSERVERNAME Port: 25
From Address: servicedesk@entitybox.co.za
From Display Name: IT Service Helpdesk
Notification Email: administratordistributionlist@entitybox.co.za
Username:
Password:

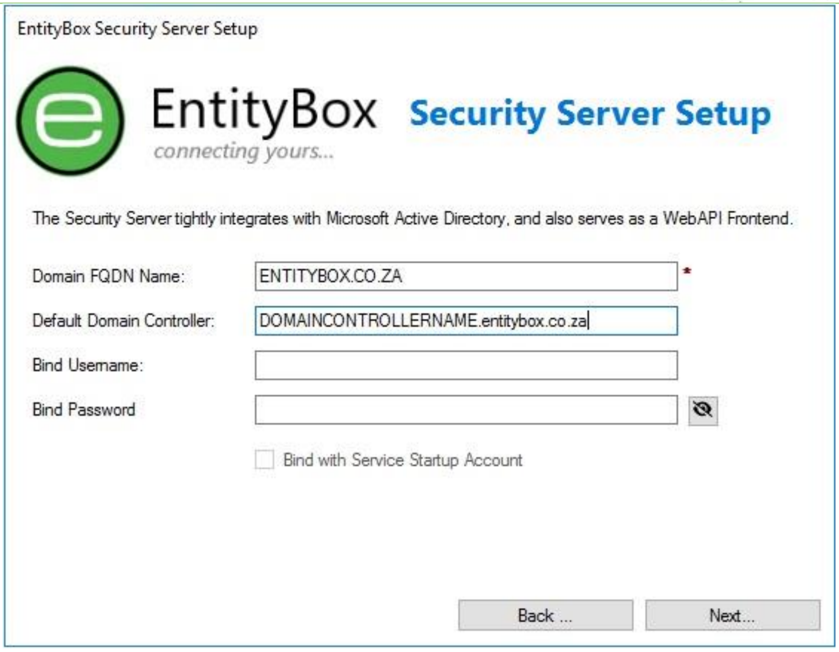
□ Enforce SSL Connection

- Server Name: Enter the FQDN Server name of SMTP
- Port Number: Default 25, custom ports number if required
- From Address: Address that should be used in the From field
- From Display Name: The Friendly name for the From Address
- Notification Email: Administrator email for system notifications
- Username: If SMTP Server requires authentication
- Password: If SMTP Server requires authentication
- Enforce SSL: If SMTP connection is a Only over SSL
- Click **Next**

### Active Directory

If Service is ActiveDirectory, or gMSA Account, it will automatically be integrated.

Set the bind Username and Password if an alternative account should be used to the service account.



EntityBox Security Server Setup

The Security Server tightly integrates with Microsoft Active Directory, and also serves as a WebAPI Frontend.

Domain FQDN Name: ENTITYBOX.CO.ZA *

Default Domain Controller: DOMAINCONTROLLERNAME.entitybox.co.za

Bind Username:

Bind Password

□ Bind with Service Startup Account

- Domain FQDN: Domain Name of the Environment
- Default Domain Controller: DC to be used on LDAP connections
- Bind Username: Username of the account to bind on LDAP
- Bind Password: Password of the account to bind on LDAP
- Bind with Service Startup: Only available if Service is of type ActiveDirectory.
- Click **Next**

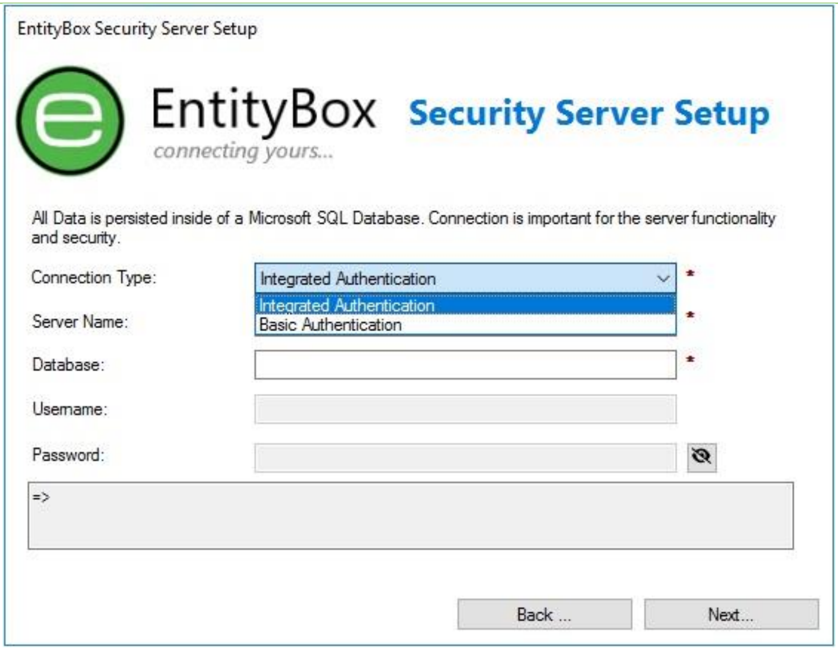
### SQL Server Connection

SQL is used as the default back-end.

Installer account should have permissions to complete the setup.

Integrated security used if the Service Account is ActiveDirectory or gMSA Account.

Basic Authentication could be selected as an alternative, but not recommended.



EntityBox Security Server Setup

All Data is persisted inside of a Microsoft SQL Database. Connection is important for the server functionality and security.

Connection Type: Integrated Authentication *

Integrated Authentication
Basic Authentication

Server Name: *

Database: *

Username:

Password:

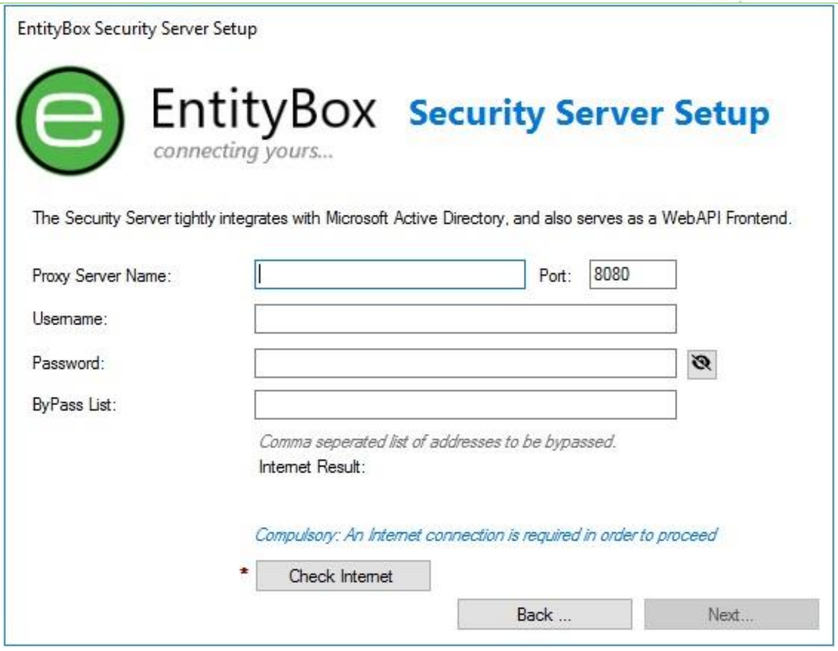
```
=>
```

- Connection Type: Integrated or Basic Authentication
- Server Name: FQDN of the SQL Server used.
- Database: EBSS_Server or what the Database is called as per the SQL Server section.
- Username & Password: Only available on Basic Autentication for connection string.
- Click **Next**

### Proxy Server

Internet is a requirement for this product to function.

Enter the Proxy server if used for outbound connections to the internet.



EntityBox Security Server Setup

EntityBox connecting yours... Security Server Setup

The Security Server tightly integrates with Microsoft Active Directory, and also serves as a WebAPI Frontend.

Proxy Server Name: | Port: 8080

Username:

Password:

ByPass List:

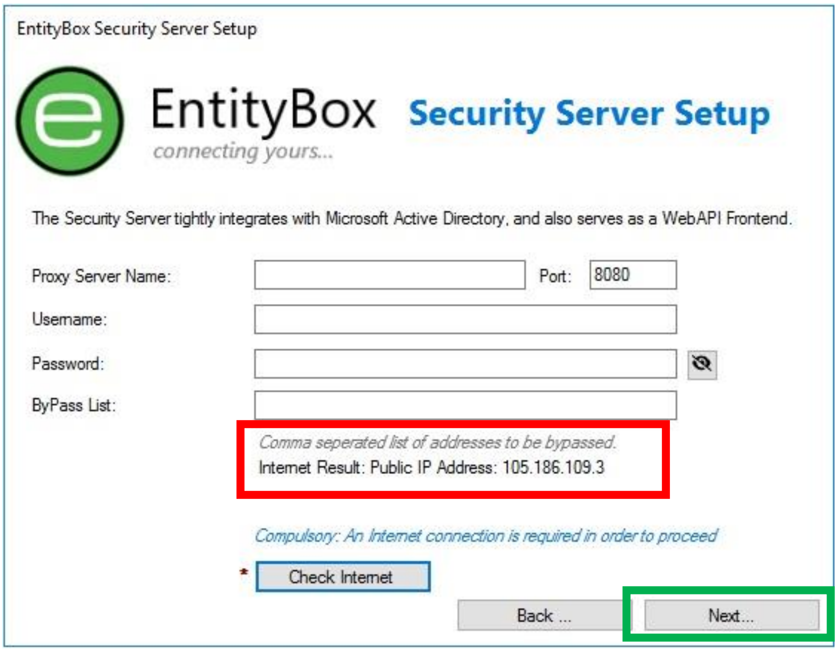
Comma seperated list of addresses to be bypassed.

Internet Result:

Compulsory: An Internet connection is required in order to proceed

- Proxy Server Name: FQDN or IP of the Proxy Server
- Port Number: Port number used for proxy connection
- Username: If Proxy requires Authentication
- Password: If Proxy requires Authentication
- ByPass List: list of internal IPs and domain names to bypass and keep traffic local not to the proxy.
- Click Check Internet

***Note: the Next button will not be available until internet is tested. 3 Tests will still allow the setup to proceed, but will require setup later.***



EntityBox Security Server Setup

EntityBox connecting yours... Security Server Setup

The Security Server tightly integrates with Microsoft Active Directory, and also serves as a WebAPI Frontend.

Proxy Server Name: | Port: 8080

Username:

Password:

ByPass List:

Comma seperated list of addresses to be bypassed.

Internet Result: Public IP Address: 105.186.109.3

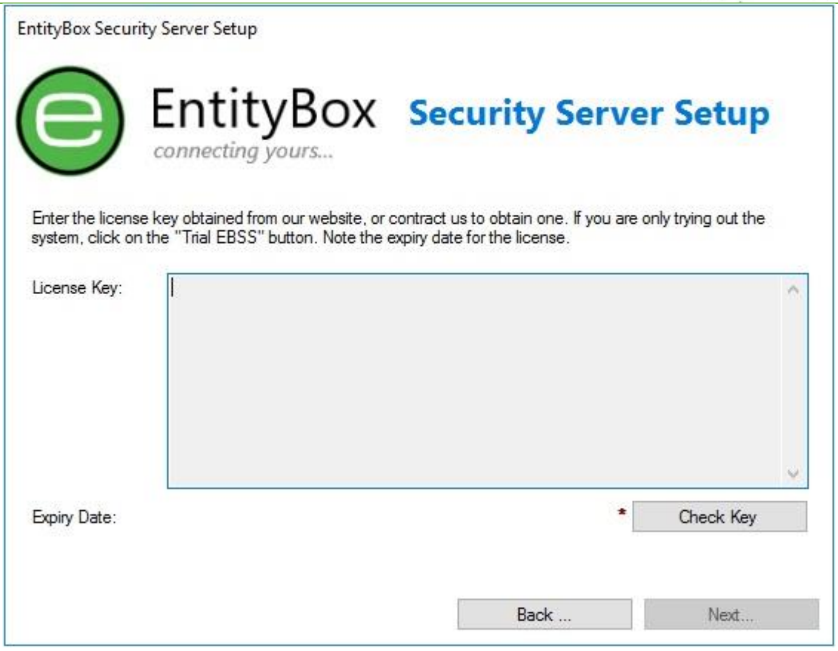
Compulsory: An Internet connection is required in order to proceed

- Click Next

### System License

Software license is checked on the Internet from the EBSS Website, hence the importance of the Internet connection on the previous step.

Once the Software is checked after a new registration, the Trial period would start.


EntityBox Security Server Setup

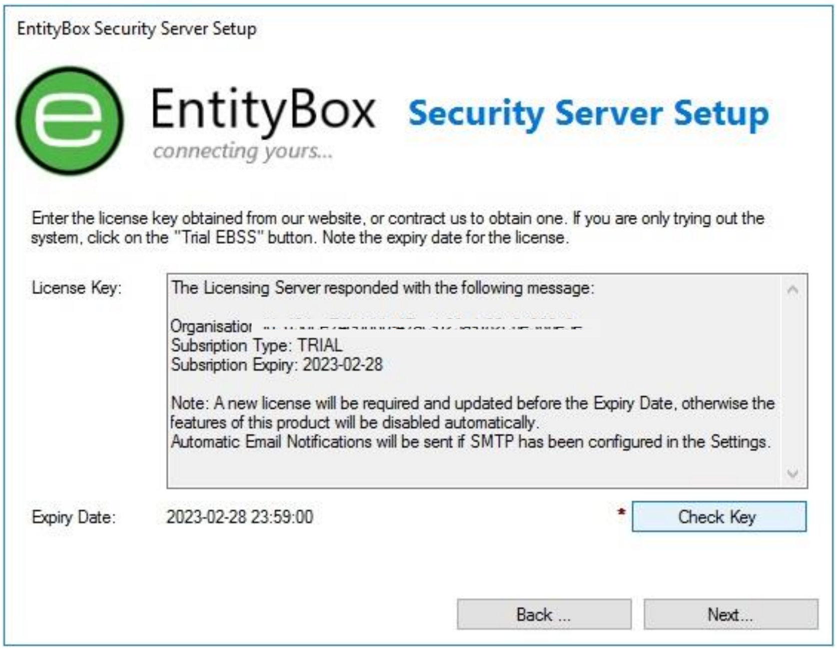
Enter the license key obtained from our website, or contract us to obtain one. If you are only trying out the system, click on the "Trial EBSS" button. Note the expiry date for the license.

License Key:

Expiry Date:

- Click **Check Key**

***License key information and Expiry Date will be shown. Initial setup should show a Trial information.***


EntityBox Security Server Setup

Enter the license key obtained from our website, or contract us to obtain one. If you are only trying out the system, click on the "Trial EBSS" button. Note the expiry date for the license.

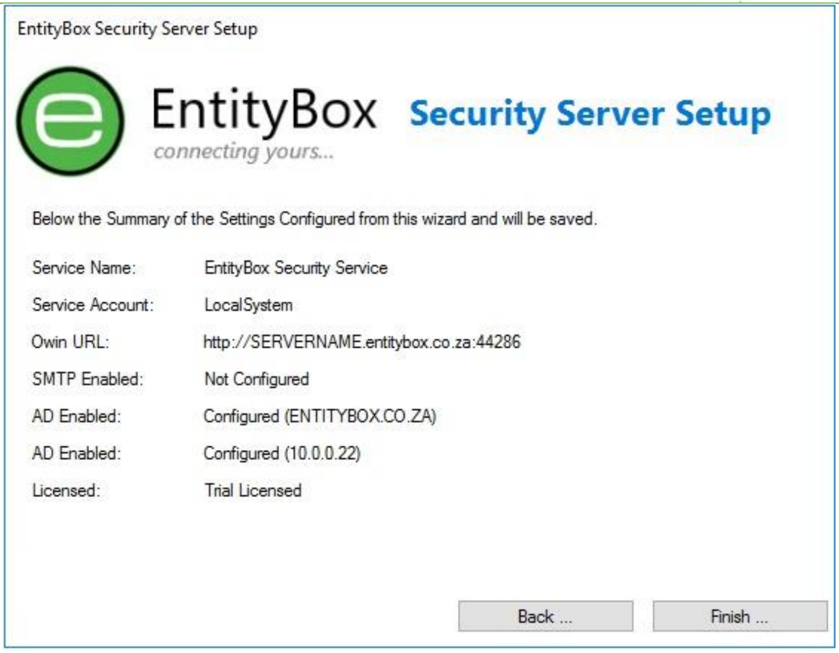
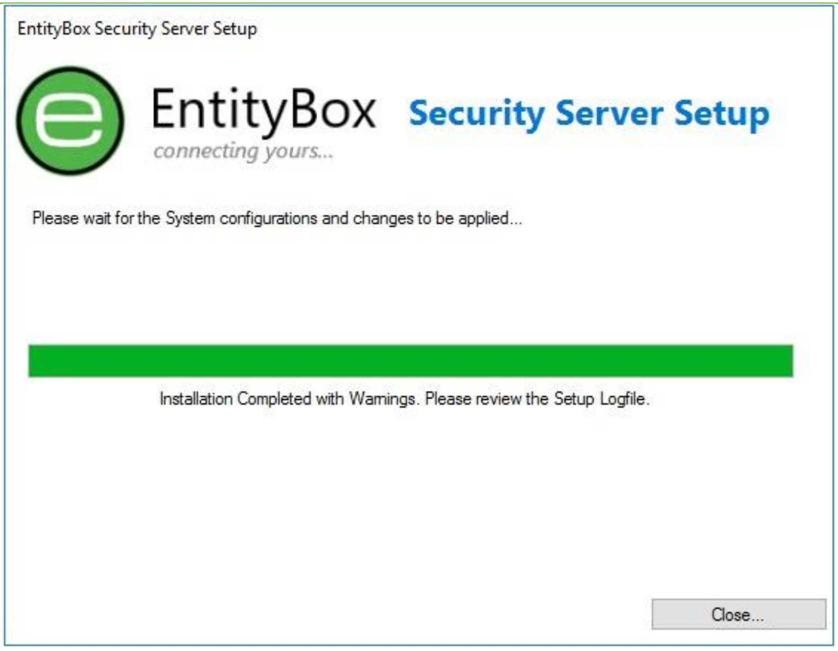
License Key: The Licensing Server responded with the following message:

Organisatior [redacted]
Subsription Type: TRIAL
Subsription Expiry: 2023-02-28

Note: A new license will be required and updated before the Expiry Date, otherwise the features of this product will be disabled automatically.
Automatic Email Notifications will be sent if SMTP has been configured in the Settings.

Expiry Date: 2023-02-28 23:59:00

- Click **Next**

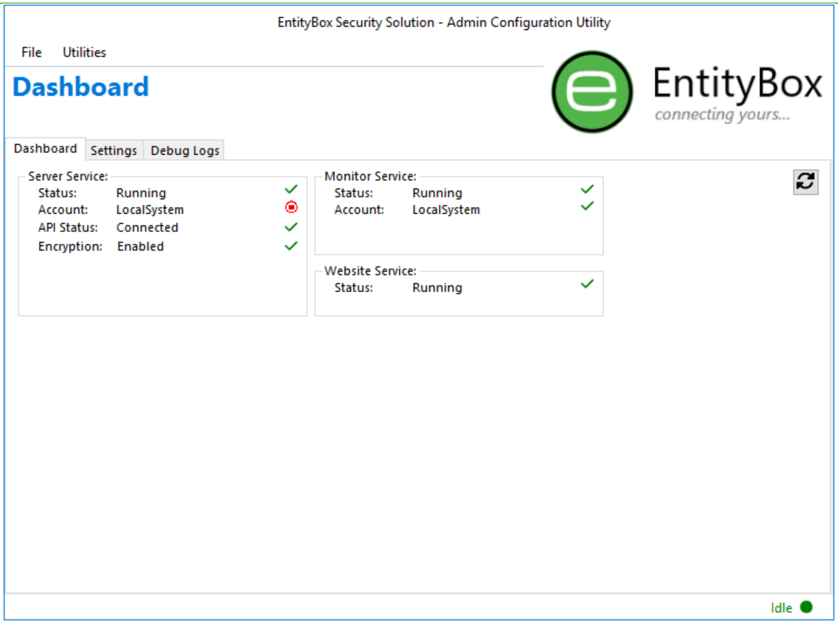
| | |
|---|---|
| **Setup Summary**<br><br>Summary will be shown as configured through the wizard pages. | <br>EntityBox Security Server Setup<br>EntityBox connecting yours... Security Server Setup<br>Below the Summary of the Settings Configured from this wizard and will be saved.<br>Service Name: EntityBox Security Service<br>Service Account: LocalSystem<br>Owin URL: http://SERVERNAME.entitybox.co.za:44286<br>SMTP Enabled: Not Configured<br>AD Enabled: Configured (ENTITYBOX.CO.ZA)<br>AD Enabled: Configured (10.0.0.22)<br>Licensed: Trial Licensed<br> <br>• Click **Finish** |
| **Installation Steps**<br><br>Different stages will show as the application is setup and configured.<br><br>Once completed, you can Navigate to the Install Path: %Program Files%\EntityBox\Security Solution\Data\Logs to review the Setup Log: EBSS_Setup.log for errors. | <br>EntityBox Security Server Setup<br>EntityBox connecting yours... Security Server Setup<br>Please wait for the System configurations and changes to be applied...<br>Installation Completed with Warnings. Please review the Setup Logfile.<br> <br>• Click **Close** |

## Administrator Utility

After the setup, the Administrator Utility can be used to configure the Service.

Stopping and Starting of the Service is still done in the Service Configuration utility (services.msc) of the operating system.

Administrators can launch the Admin Configuration from the Install Path: **AdminConfig.exe**

| | |
|---|---|
| **Dashboard**<br>The Dashboard will provide a quick overview of the status on the Service.<br>Note the Red Stop images and follow the best practice.<br>Initial launch will not show the Services are running as they still require possible configuration.<br>Start the services once configuration is completed and perform an API Browser test. | <br>EntityBox Security Solution - Admin Configuration Utility<br>File Utilities<br>**Dashboard**<br>Dashboard Settings Debug Logs<br>Server Service:<br>Status: Running ✓<br>Account: LocalSystem ●<br>API Status: Connected ✓<br>Encryption: Enabled ✓<br>Monitor Service:<br>Status: Running ✓<br>Account: LocalSystem ✓<br>Website Service:<br>Status: Running ✓<br>Idle ● |
| **Settings** | General<br>• Set the Debug Level to Debug = 1 for the period of Configuration.<br>***Reccomendation***: Set the Debug Level to Warning<br>Server Settings:<br>• Basic information on the Server.<br>OWIN Api<br>• Server URL and Port Number<br>• External URL for invalid route connections<br>Active Directory<br>• Active Directory Configuration<br>***Reccomendation***: If a separate account is used, Test your Binding from here to ensure connectivity<br>SMTP Settings<br>• SMTP Server Configuration<br>***Reccomendation***: Test your SMTP Server and receive an email on the notification email address specified. |

| | |
|---|---|
| | Proxy Settings<br>• Proxy Server and Internet Configuration ***Reccomendation***: Test your internet from this page, and ensure you have a successful connection.<br><br>Extra Settings<br>• This section can be skipped as this is for future use on our current programming of the configuration utility.<br><br>License<br>• License settings can be updated from this section. Should this step failed, or the Expiry Date of the License changed, updating the inforamtion is dependant on the Internet settings working.<br>***Reccomendation***: Ensure Internet is working and the Expiry Date is shown as a future date.<br><br>Maintenance<br>• System Log files and Job files in the Data Directory are automatically cleaned after the amount of days specified.<br>Trim the days in order to suite organisational and system disk requirements.<br><br>EBSS Security (Mobile)<br>• Default URL to be used for communication to our EBSS Website. https://ebss.entitybox.co.za<br><br>**Do not change this value without instruction as your system license will be affected** |

## SSL Configuration

Should the internal application be configured with SSL, it must be taken into account that the OWIN Service runs with the Microsoft HTTP.SYS protocol that will conflict with Internet Information Services (IIS). Do not Install EntityBox Services along with other IIS Websites that will make use of 443 HTTPS Protocol.

Configure the SSL Protocol with the NETSH Command and bind the certificate Thumbprint from the Command-line.
https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificate

## Testing Steps

Testing the system functionality before opening the Networking from external is very important. Once your configuration is complete, the Service can be started from the Services Console (services.msc) -> EntityBox Security Service.

- Monitor the Eventlog of the system (Debug Level minimum Information).
- Browse to http{s}://{OWIN URL}:{PORT}/api/status to receive a Response (example: http://servername.domain.co.za:44286/api/status )
- Use the Admin Configurator and refresh the Dashboard. Monitor the Green Check-marks
- Check the Logfiles created under the Data\Logs directory for any failures and problems.

# Endpoint Mappings

EntityBox allows the following Endpoint mappings that the OWIN Server listens on:

## Anonymous Access Endpoints:

Anonymous access are endpoints that will always be available without authentication. The below table shows these endpoints. For security, these endpoints do not return any valuable information

| Endpoint | Method | Description |
|---|---|---|
| /api/status | **GET** | Get the status of the Service API after configuration or to check if the system responds and listens on OWIN. |
| /Defaults/Index | **GET** | Any URL not in the routing table will be redirected to this URI. If the External Website URL link is configured under the OWIN Settings, redirection will occur to the set value. |

## Protected Access Endpoints:

Protected access endpoints are exposed with a proprietary designed encryption token placed in the header of each request. Access Tokens are first decrypted and checked by the system before any endpoint is executed.

| Endpoint | Method | Description |
|---|---|---|
| /api/~~~/Register/{MobileDevice.EmailAddress} | **PUT** | Registration of new Mobile Device Users into the application.<br>Response Attribute contains:<br>• EBSS Database: UserID GUID<br>• Active Directory: Display Name |
| /api/~~~/User/Info | **GET** | Get information from the Mobile Device User's Active Directory Account Status.<br>Response Attributes contains:<br>• Active Directory: Display Name<br>• Active Directory: UAC Int<br>• Active Directory: Lockout Time<br>• Active Directory: Password Last Set Date |
| /api/~~~/User/Unlock | **PUT** | Performs an Unlock of the Active Directory Account<br>Response includes the same values as GetInfo |
| /api/~~~/User/Reset?EncryptedBase64PasswordString as parameter | **PUT** | Performs a Reset of the Active Directory Account<br>Response includes the same values as GetInfo |

# Networks

Once the EntityBox Server, SQL Server and Active Directory integration is complete, networking towards the server should be allowed from the Internet for inbound access through the organisation's preferred channel.

Below table list a few options used in practice:

| Solution | Description |
|---|---|
| **Static NAT** | Static Network Address Translation (NAT) with TCP Port 443 redirecting to the internal server on port 443 (Server Configuration is also TCP 443 HTTPS) |
| **Static NAT with Port Mapping** | Static Network Address Translation (NAT) with TCP Port 443 redirecting to the internal server on port 44286 (Server Configuration is TCP 44286 HTTP) |
| **Web Application Proxy** | Pass-through Authentication on TCP Port 443 redirecting to the internal server on port 443 (Server Configuration is also TCP 443 HTTPS) |
| **Azure Web Application Proxy** | Pass-through Authentication on TCP Port 443 redirecting to the internal server on the configured port URL. |

***Recommendation:*** Azure Web Application Proxy or Web Application Proxy is recommended so that changes on the organisation firewall is limited and traffic always routes through reverse proxies.

# Support & Errors

## Internet Requirement

Internet is a requirement for this application to function. Encrypted traffic is sent over a secure channel to EntityBox Servers and On-Premise. Without internet the application will indicate a connection error.

## General Errors

Common Errors made whilst configuring the application could be:

- SQL Server Could not connect – Configure this afterwards on the Admin Configuration
- AD Bind Account – If gMSA account is used with LocalSystem, this is expected as the integration should still be configured.
- Internet Connection – EBSS Website could not be contacted to provide an IP.
- SMTP Server Configuration – Authentication is used on port 25 by most Exchange Servers
- Firewall is ON – Ensure the firewall is configured with the following rules:
    - Outbound Traffic tcp: 443 Allowed (Internet Communication), or
    - Outbound Traffic tcp: 8080 Allowed (Proxy Port configuration)
    - Outbound Traffic tcp: 25 Allowed (SMTP Server configuration)
    - Inbound Traffic tcp: 443 / 44286 Allowed (OWIN Port configuration)

## Disclaimer

Although EntityBox try our best to deliver a robust and secure application, we try to keep mobile data consumption to an absolute minimum. EntityBox cannot assume any liability for damages, user negligence or any event that occurs on our platform. We recommend performing a trial period with selected technical users to ensure proper configuration before distribution to all users are done.

EntityBox complies with all legislative requirements in protection of personal information and no sensitive information is stored on our Servers, merely passed through our services between device and On-Premise, processed only to ensure delivery of our services as advertised. No information is forwarded to Third-parties without the customers' explicit consent in writing.

EntityBox is a registered trademark and should not be used without our consent.

Send your comments, requests and feature suggestions to our support: support@entitybox.co.za .