

TRBOnet Enterprise | PLUS Authentication Methods User Guide

Version 6.5

Last revised on 7 August 2026

USA Office

Neocom Software
150 South Pine Island Rd., Suite 300
Plantation, FL 33324, USA

Sales

EMEA: +44 203 608 0598
Americas: +1 872 222 8726
APAC: +61 28 607 8325

www.trbonet.com
info@trbonet.com

Contents

- 1 Introduction 3
 - 1.1 About This Guide 3
 - 1.2 About TRBOnet..... 3
 - 1.3 Contacts..... 3
- 2 TRBOnet Authentication 4
 - 2.1 Multi-Factor Authentication 5
- 3 Windows Authentication..... 7
 - 3.1 Important Notes..... 8
- 4 Microsoft Entra ID Authentication 9
 - 4.1 Important Notes..... 11
 - 4.2 Registering Apps in Microsoft Entra ID 12

1 Introduction

1.1 About This Guide

This document is intended for TRBOnet administrators and Dispatch Console operators. The document describes authentication methods used to connect to TRBOnet Dispatch Console. In addition to its built-in authentication method, TRBOnet uses two more authentication methods that allow users to securely connect to TRBOnet Dispatch Console.

For more comprehensive information on the Neocom TRBOnet family of radio network software tools, refer to our [website](#).

1.2 About TRBOnet

TRBOnet is a suite of professional applications for MOTOTRBO digital two-way radio networks. TRBOnet manages voice and data communication paths across network endpoints. It provides a unified graphical dispatcher workbench interface for the entire range of workforce fleet management tasks.

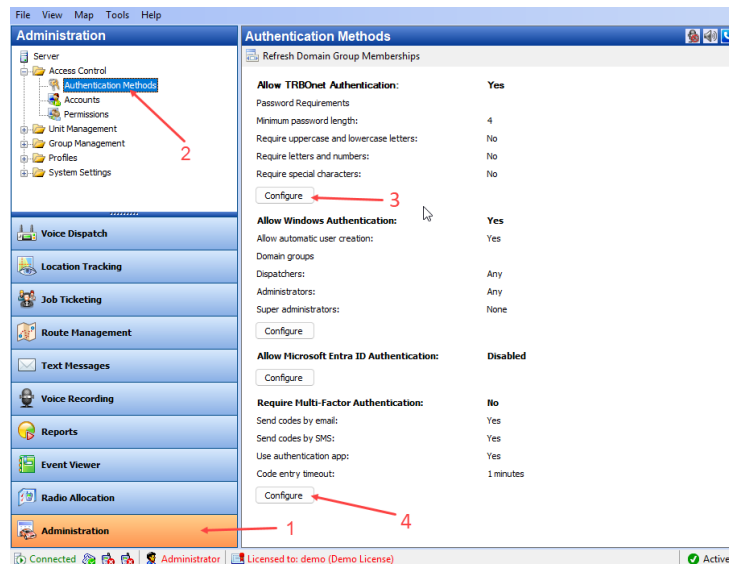
1.3 Contacts

Region	Phone	Email & Support
EMEA	+44 203 608 0598	info@trbonet.com — general and commercial inquiries
Americas	+1 872 222 8726	support@trbonet.com — technical support
APAC	+61 28 607 8325	https://trbonet.com/kb/ — online knowledge base

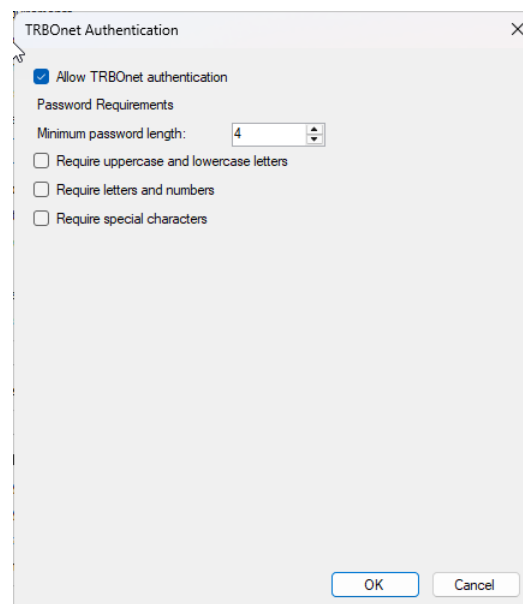
2 TRBOnet Authentication

TRBOnet Authentication is a passport-based method used to authenticate a user's identity. TRBOnet administrator can configure password policy to ensure that all passwords are strong and secure.

- Go to **Administration (1), Access Control > Authentication Methods (2)**.



- Click the **Configure** button (3) under the **Allow TRBOnet Authentication** section.
- In the dialog box that opens, specify the following parameters:

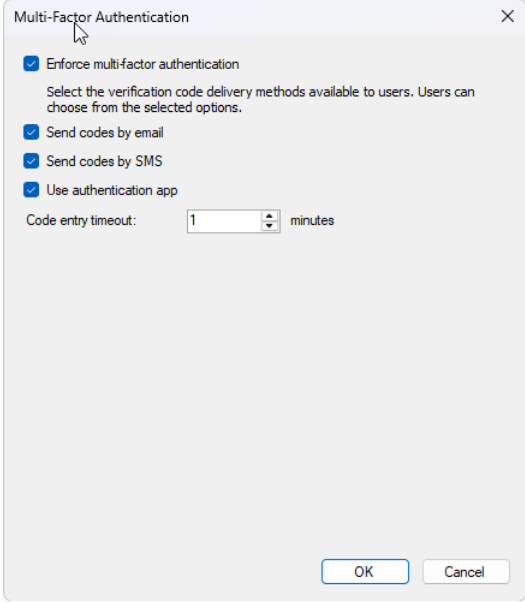


- Allow TRBOnet Authentication**
 Select this checkbox to allow TRBOnet Authentication.
- Password Requirements**

- **Minimum length**
Enter the minimum password length, in characters.
- **Require uppercase and lowercase letters**
Select this checkbox to require that a password include at least one uppercase letter (A-Z) and one lowercase letter (a-z).
- **Require letters and numbers**
Select this checkbox to require that a password include at least one character from [A-Za-z] and at least one from [0-9].
- **Require special characters**
Select this checkbox to require that a password include at least one non-alphanumeric character.

2.1 Multi-Factor Authentication

- Click the **Configure** button (4) under the **Require Multi-Factor Authentication** section.
- In the dialog box that opens, specify the following parameters:



The image shows a 'Multi-Factor Authentication' dialog box. It has a title bar with a close button (X). Inside, there is a section titled 'Enforce multi-factor authentication' with a checked checkbox. Below this is a text label: 'Select the verification code delivery methods available to users. Users can choose from the selected options.' There are three more checked checkboxes: 'Send codes by email', 'Send codes by SMS', and 'Use authentication app'. At the bottom, there is a 'Code entry timeout:' label followed by a spinner box containing the number '1' and the text 'minutes'. At the very bottom are 'OK' and 'Cancel' buttons.

- **Enforce multi-factor authentication**
Select this option to enforce multi-factor authentication.
Select at least one of the code delivery methods that will be available to the users.
- **Send codes by email**
Select this option to send a verification code by email.
- **Send codes by SMS**
Select this option to send a verification code by SMS.

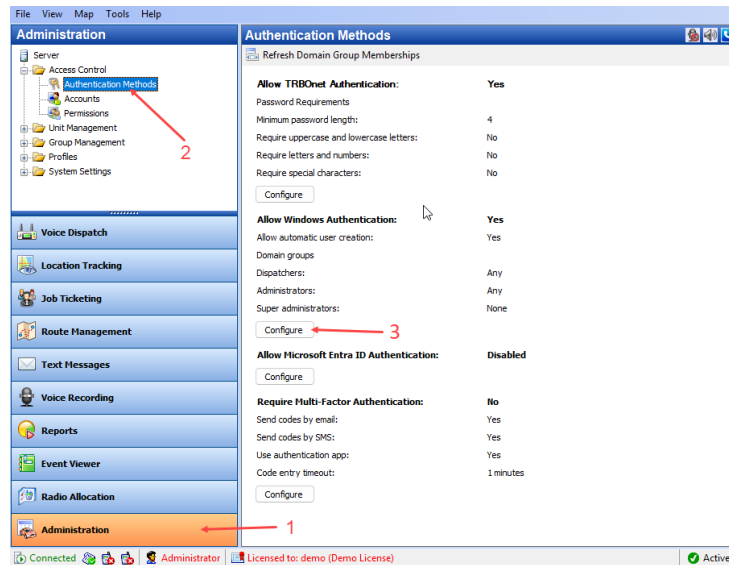
- **Use authentication app**
Select this option to generate a verification code by an authentication app.
- **Code entry timeout**
Enter the time period during which the user must enter a verification code to complete logging in.

3 Windows Authentication

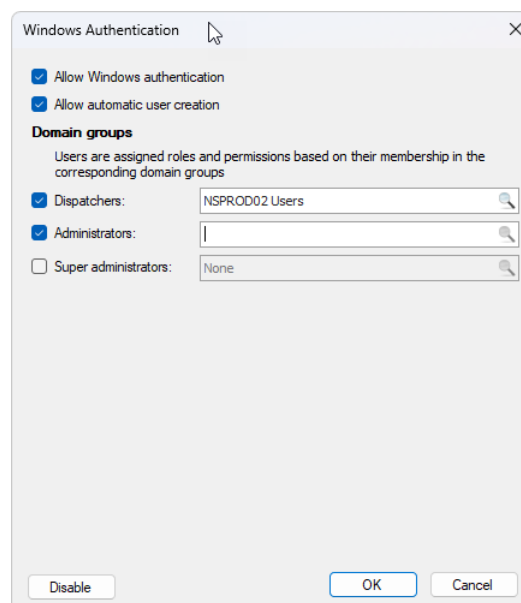
Windows Authentication is a Microsoft security mechanism that authenticates users against an Active Directory domain or local machine database using protocols like Kerberos or NTLM.

Note: Make sure that Windows domain groups are appropriately configured.

- Go to **Administration (1), Access Control > Authentication Methods (2).**



- Click the **Configure** button (3) under the **Windows Authentication** section.
- In the dialog box that opens, specify the following parameters:



- Click the **Enable** button on the bottom of the dialog box to enable Windows authentication in TRBOnet.
- **Allow Windows authentication**
Select this option to allow Windows authentication.
- **Allow automatic user creation**
Select this option to create TRBOnet accounts based on the Windows user membership in the corresponding domain groups.

Domain groups

- Specify the domain groups whose members will be assigned the corresponding roles (**Dispatchers / Administrators / Super administrators**).

Notes: If the **Allow automatic user creation** option is selected, the domain groups of the checked roles must be specified. In addition, the role and access profile must be created and assigned to the corresponding domain group (**Permissions > Add Dispatcher Role/Add Administrator Role/Add Access Profile > General > Domain group**).
Or uncheck the role, if its domain group is not specified. Otherwise, the 'Access Denied' error will appear, and the dispatcher won't be created, or the dispatcher won't be able to log in if the account has been already created.

3.1 Important Notes

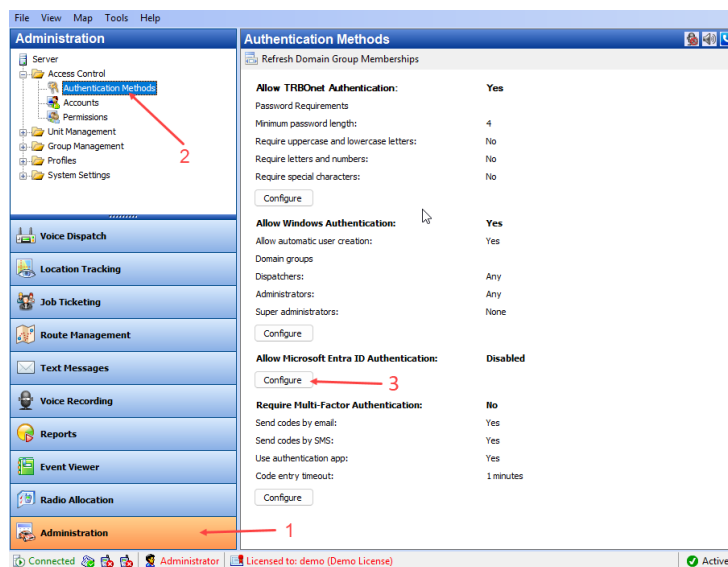
- The computer running TRBOnet Server must be added to the organization's domain. Otherwise, it won't have access to domain groups and won't be able to log in to TRBOnet using domain accounts.
- If the Dispatchers or Administrators role's checkbox is unchecked (reads 'Any'), then the first group in alphabetical order is taken from the domain controller. Therefore, if, in **Permissions > Roles**, you have specified the domain group which is not the first one in alphabetical order, access will be denied for a member of this domain group.
- To update information about user membership in Windows AD, click the **Refresh Domain Group Memberships** button on the top of the right pane.

4 Microsoft Entra ID Authentication

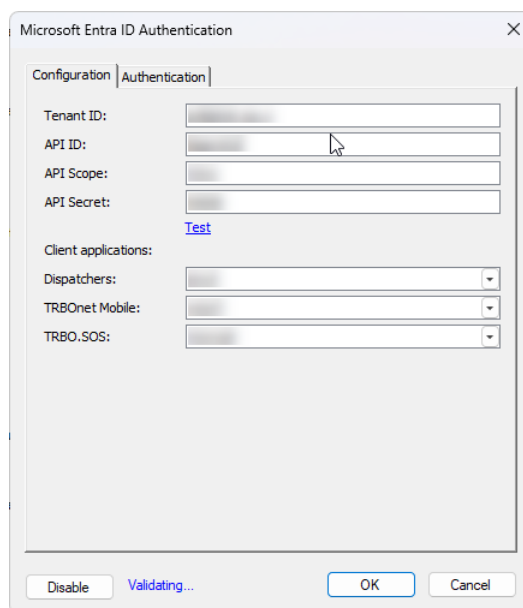
Microsoft Entra ID (formerly Azure AD) Authentication provides secure, token-based access for users and applications. It supports multi-factor authentication (MFA), managed identities for Entra ID resources, and integrations with external providers to verify identity and secure access to services.

Note: Make sure that Microsoft Entra ID Authentication is appropriately configured.

- Go to **Administration (1)**, **Access Control > Authentication Methods (2)**.

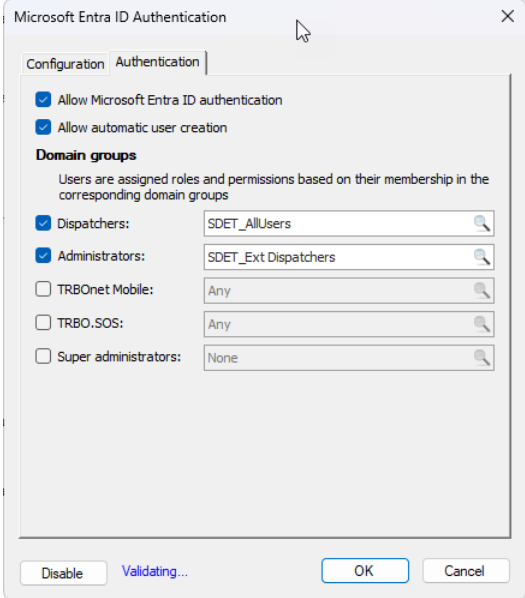


- Click the **Configure** button (3) under the **Microsoft Entra ID Authentication** section.
- In the dialog box that opens, specify the following parameters:



- Click the **Enable** button on the bottom of the dialog box to enable Microsoft Entra ID authentication in TRBOnet.
- Fill in the form according to the Entra ID settings you have specified when you configured Microsoft Entra ID Authentication.

Click the **Authentication** tab, and specify the following parameters:



- **Allow Microsoft Entra ID authentication**
Select this option to allow Microsoft Entra ID authentication.
- **Allow automatic user creation**
Select this option to create TRBOnet accounts based on the Entra ID user membership in the corresponding Entra ID groups.

Domain groups

- Specify the Entra ID groups whose members will be assigned the corresponding roles (**Dispatchers** / **Administrators** / **Super administrators** and **TRBOnet Mobile** / **TRBO.SOS**).

To update information about user membership in Entra ID groups, click the **Refresh Domain Group Memberships** button on the top of the right pane.

4.1 Important Notes

The computer running TRBOnet Server must have access to the MS Entra ID domain controller. Otherwise, it won't have access to domain groups and won't be able to log in to TRBOnet using domain accounts.

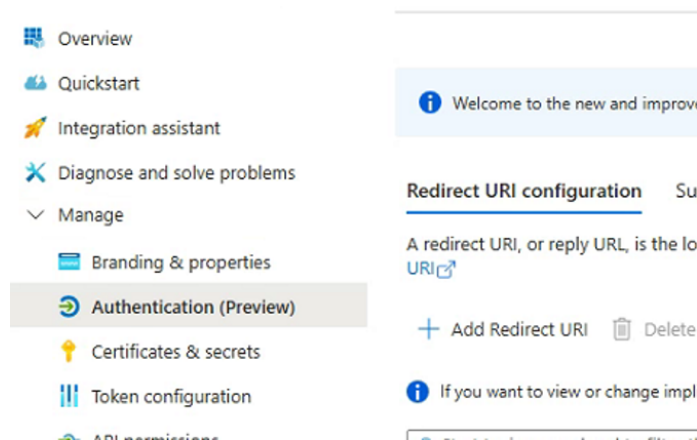
- MS Entra ID domain controller is a cloud-based equivalent of a local domain controller. The logic is similar to that of Active Directory.
- The 'Allow Microsoft Entra ID Authentication' option must be enabled.
- This option is disabled by default because TRBOnet Server sends real-time requests to the cloud domain controller whenever any changes are made to verify the parameters.

The MS Entra ID authentication can be used for Dispatch Console accounts as well as for TRBOnet Mobile and TRBO.SOS devices. Note that TRBOnet Mobile and TRBO.SOS users cannot be created automatically. In addition, unlike Dispatch Console accounts, TRBOnet Mobile and TRBO.SOS users don't have roles.

4.2 Registering Apps in Microsoft Entra ID

This section describes how to appropriately configure Microsoft Entra ID authentication so that it can be used in TRBOnet.

- Log in to the Microsoft Entra admin center at <https://entra.microsoft.com/>.
- From the left navigation menu, browse to **Identity > Applications > App registrations** and click on your specific application.
- Open **Authentication settings**.
 - On your application overview page, at the left sidebar menu, browse to **Manage > Authentication**.

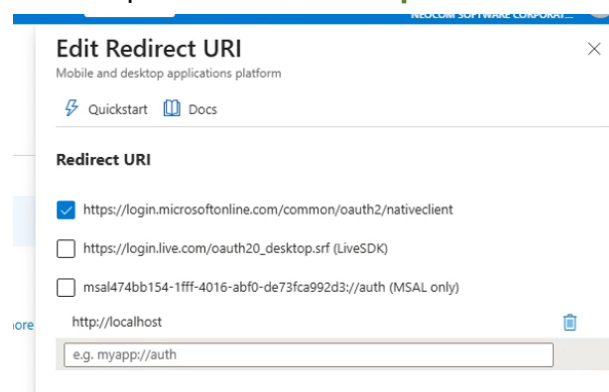


Add the Redirect URI

- Click **Add a platform** at the top of the page.
- Choose your application type (e.g., iOS / macOS, Android or Mobile and desktop applications).

Mobile and desktop applications platform

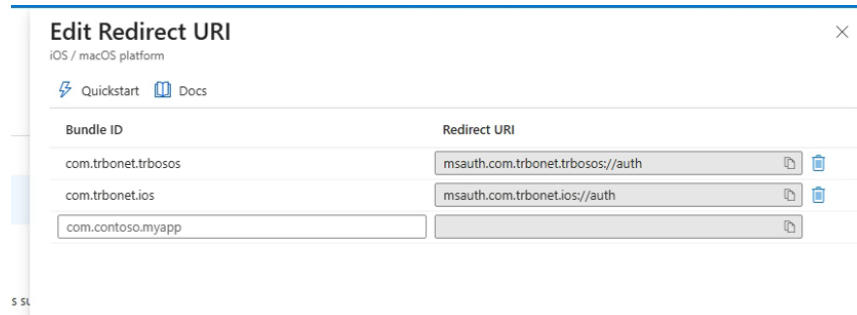
- TRBOnet Enterprise Console > "**http://localhost**"



- Enter your application's parameters (**Bundle ID, Signature Hash**) and click **Configure**.

iOS platform

- TRBOnet Mobile > Bundle ID > **"com.trbonet.ios"**
- TRBO.SOS > Bundle ID > **"com.trbonet.trbosos"**



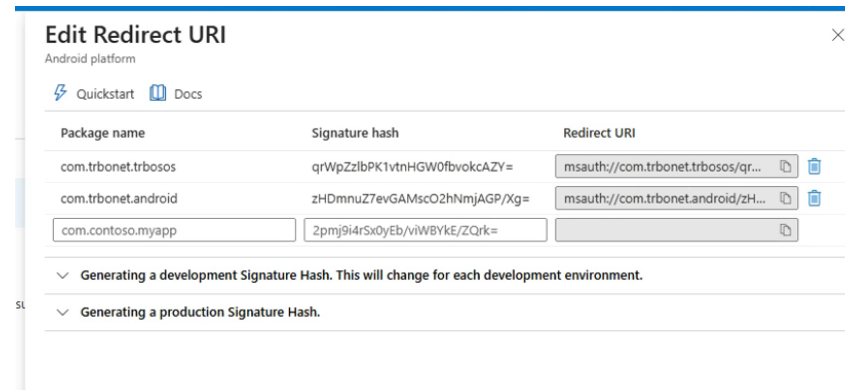
Edit Redirect URI
iOS / macOS platform

Quickstart Docs

Bundle ID	Redirect URI
com.trbonet.trbosos	msauth.com.trbonet.trbosos://auth
com.trbonet.ios	msauth.com.trbonet.ios://auth
com.contoso.myapp	

Android platform

- TRBOnet Mobile > Bundle ID > **"com.trbonet.android"**
+ Signature Hash > **"zHdmnuZ7evGAMscO2hNmjAGP/Xg="**
- TRBO.SOS > Bundle ID > **"com.trbonet.trbosos"**
+ Signature Hash > **"qrWpZzlbPK1vtnHGW0fbvokcAZY="**



Edit Redirect URI
Android platform

Quickstart Docs

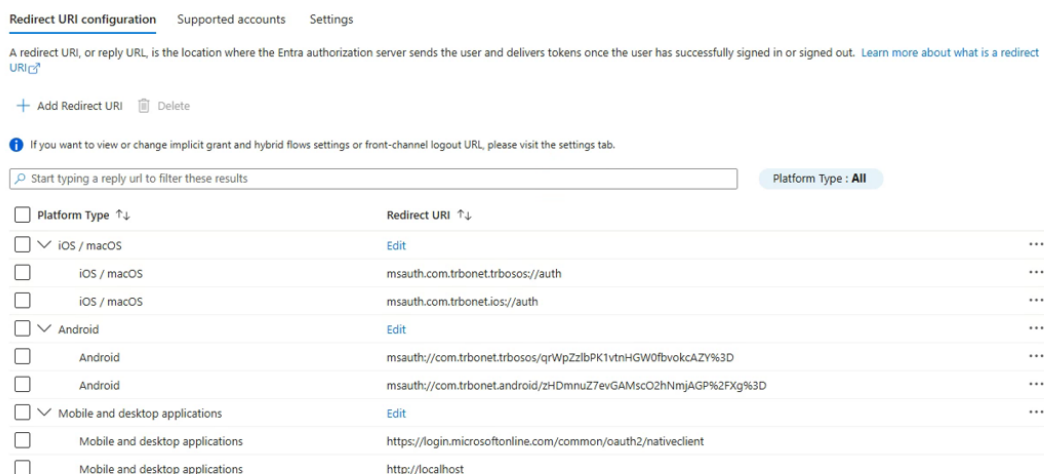
Package name	Signature hash	Redirect URI
com.trbonet.trbosos	qrWpZzlbPK1vtnHGW0fbvokcAZY=	msauth://com.trbonet.trbosos/qr...
com.trbonet.android	zHdmnuZ7evGAMscO2hNmjAGP/Xg=	msauth://com.trbonet.android/zH...
com.contoso.myapp	2pmj9i4rSx0yEb/viWBYkE/ZQrk=	

Generating a development Signature Hash. This will change for each development environment.

Generating a production Signature Hash.

Save your changes

- Scroll to either the top or bottom of the screen and click the **Save** button.



Redirect URI configuration Supported accounts Settings

A redirect URI, or reply URL, is the location where the Entra authorization server sends the user and delivers tokens once the user has successfully signed in or signed out. [Learn more about what is a redirect URI](#)

+ Add Redirect URI Delete

If you want to view or change implicit grant and hybrid flows settings or front-channel logout URL, please visit the settings tab.

Start typing a reply url to filter these results Platform Type: All

Platform Type	Redirect URI	
iOS / macOS	Edit	...
iOS / macOS	msauth.com.trbonet.trbosos://auth	...
iOS / macOS	msauth.com.trbonet.ios://auth	...
Android	Edit	...
Android	msauth://com.trbonet.trbosos/qrWpZzlbPK1vtnHGW0fbvokcAZY%3D	...
Android	msauth://com.trbonet.android/zHdmnuZ7evGAMscO2hNmjAGP%2FXg%3D	...
Mobile and desktop applications	Edit	...
Mobile and desktop applications	https://login.microsoftonline.com/common/oauth2/nativeclient	
Mobile and desktop applications	http://localhost	