SSO User Guide

Xiid Corporation

Contents

SSO User Setup

Introduction to Xiid

What is Xiid?

Xiid is a technology company that enables secure access to your directory, remote machines, data, applications, and more without trusting anyone with a copy – even us.

At the core of Xiid's technology is secure access to your directory services. Directories store and manage the users, usernames, and passwords for your company. When you sign in to your company computer, you are usually authenticating against your company's directory service, which is a central location that ensures that your username and password are up-to-date and your credentials are correct.

These directory services are quintessential to business operations. Every user interacting with your company's ecosystem has permissions to do different things under your company's "domain". The domain is the umbrella ecosystem where all of your company's applications are housed, users are created and managed, email servers may be integrated, and various other parts of your software environment are maintained. The majority of things you do on your company computer operate under your company's "domain".

This is where Xiid comes in. Xiid's software secures your company's directory so that unauthorized bad actors cannot hijack anyone's user to compromise your domain. Xiid aims to make your company's directories more secure, so your username and password stay safe, all while making it easier to access your favorite applications and important data.

Most of Xiid's software operates "under-the-hood", or hidden from what normal users will see.

However, the Xiid Single Sign-On Portal is one major place where users interact with Xiid's software directly to access their resources securely while keeping their credentials safe!

How does Xiid Work?

Your system administrator will handle the details of installing and deploying the necessary components to set up Xiid's software to run in the background. This will lock down your company's directory service and make your credentials more secure. Nothing is needed on your end to make this happen.

Once your system administrator has set up Xiid's software on your company's domain/network, all you need to do is follow these instructions to download and install the XOTC Mobile Application onto your mobile device/smartphone and then register it. After that, when you come to the Xiid Single Sign-On Portal, simply scan the QR code with the Xiid Mobile Application on your mobile device, and you're ready to go! **It's really that easy! No usernames, no passwords, no problems!**

What is XOTC?

XOTC (Pronounced *Exotic*) is an acronym for Xiid One-Time-Code. The *XOTC Authenticator* is the name of Xiid's Mobile Application for generating and using Xiid One-Time-Codes.

Mobile Phone Requirements

To use the XOTC Mobile Application, your phone must meet the minimum operating system version requirements:

iOS Operating System: - iOS Version 13.3 or above

Android Operating System: - Android 11 - Android 12

To check your phone's operating system version, follow these instructions for iPhone and these instructions for Android.

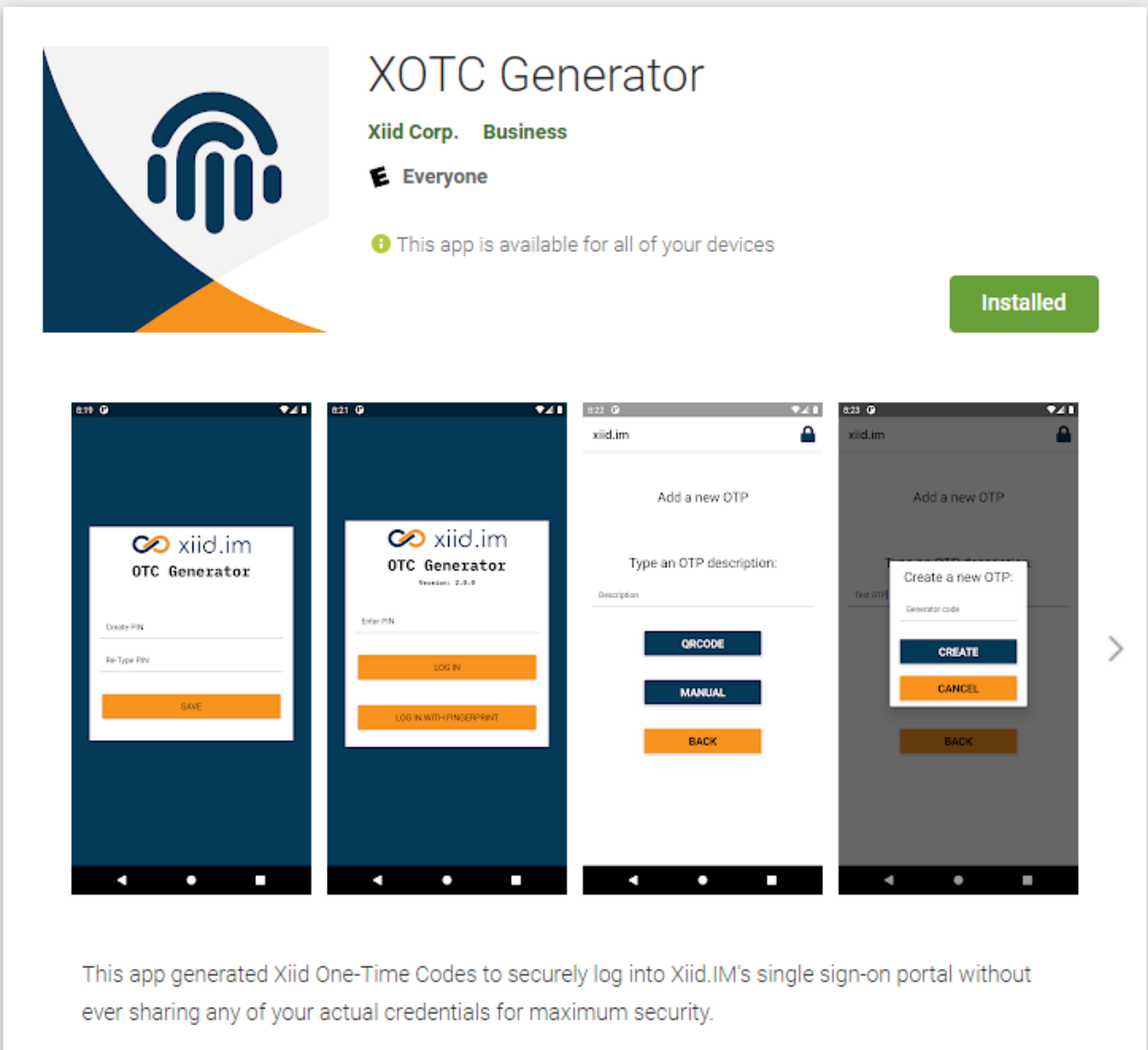
Download and Install the Xiid Mobile App

Start by downloading the XOTC Mobile Application either from the Google Play Store, the App Store, or (Android-only) directly from the Xiid Global Management Portal (ask your System Administrator for help accessing the app from the Portal).

If you choose to download the Android app directly from Xiid's website, tap the **.apk** file to install the app. You may need to adjust your system settings to allow applications from outside official stores to be installed.

When downloading from the Google Play Store or the App Store:

Search for *"xiid"* or *"XOTC"* in the mobile app store and tap the Install button to download the mobile app.



Register your App

Set the PIN

One you have installed the XOTC Authenticator App, we need to register your application with Xiid so that the system understands who you are.

Find the XOTC Application in your list of installed apps on your mobile device/smartphone.

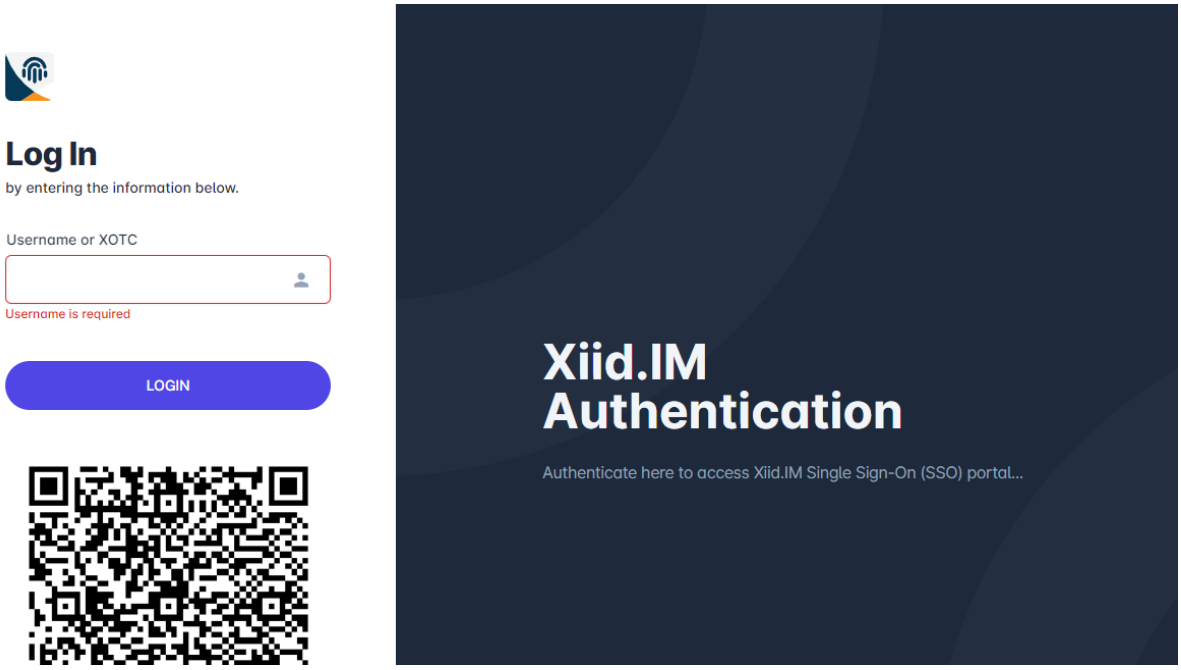
Tap the icon to open the mobile application.

The first time that you open the XOTC Authenticator App you will be asked to set a 6-digit PIN. This PIN is an added layer of security to ensure that nobody but you can access your Xiid Mobile App.

The app will take you to a mostly blank screen with a few buttons in the top right.

Sign Into the Single Sign-On Portal

On your desktop computer, sign in to your company's Single Sign-On Portal that your System Administrator has established for use with Xiid.IM. The URL for the Single Sign-On Portal is **company-specific**, so if you do not know your SSO URL, contact your System Administrator. Your Single Sign-On URL will look similar to this: https://example.us.xiid.im/home/apps/login



Enter your **company username** in the **Username or XiidID** box and click **Login**. You may need to provide the full name of your username within your domain. i.e. username@example.com.

Next you will be prompted for your **company password**. This is the ***only*** time Xiid will ever ask for your username and password.

After entering your password, you will be prompted to provide an email address. This email address is used to recover your Xiid credentials if your phone is lost, stolen or broken.

After entering your email address, you will receive an One-Time-Password to the email address provided which you will need to copy and paste in the **OTP** field on the Single Sign-On Portal.

Once your email address is verified, a QR code will pop up on the screen for you. Pause here on your desktop and switch back to your mobile phone.

Note: You will also receive another email from Xiid with a button for you to reset your password. **Do Not Lose This Email**. This is the only way to recover your XOTC Authenticator if you lose your phone.

Note: Once your initial registration has been completed, each time you want to log into your company's secure network you will only need to browse from your computer to your company's Single Sign-On Portal where a new QR code will be displayed.

Associate Your Account

On your mobile device within the XOTC Authenticator App, click the **plus "+"** button to get started with registration. (Shown below in red)

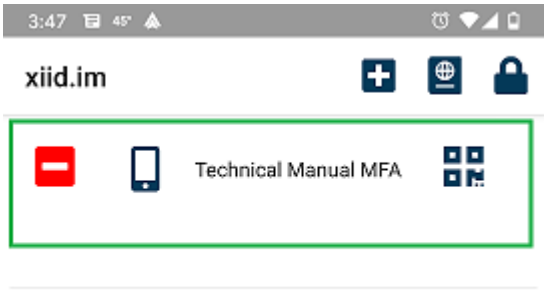
You will be taken to a new screen which will ask for a **Description** as well as a **QRCode**, **Manual**, and **Back** button.

For the **Description** section, enter a description of your company account (i.e. Example Xiid Login) to help you associate the entry in the mobile app to your company User account.

Next, tap the **QRCode** button. This will bring up a camera for you to scan a QR code.

Scan the QR code from the Single Sign-On Portal shown on the browser of your **desktop computer**.

The Xiid Mobile Application will redirect you to the app's main screen where you will now see your new security profile. (Shown below in green)



Your mobile device and XOTC Authenticator App are now registered with your company. Once registered, you will not need to repeat these steps for associating your XOTC App with your company's network unless you change your mobile device for whatever reason. For each new mobile device, you will need to associate the device once with your company network.

Now you're all set up to use the Xiid Single Sign-On Portal with the XOTC Authenticator!

Sign In Using the XOTC Authenticator App

Now that you have activated your account with your company's Single Sign-on Portal and have associated your XOTC Authenticator with your company's secure network, you are ready to use Xiid.IM on a continuous basis. The steps to do this are easy and straight-forward.

Each time you use the Xiid.IM system:

Start by navigating your computer's browser to your company's Single Sign-On Portal.

On the Single Sign-On Portal Screen, you will see a QR Code available under the **Username or XiidID** text box.

Now, on your mobile device, open the XOTC Authenticator App, then find your security profile created when you associated your mobile device with your company's secure network (in the previous section).

Tap the four black box icons on the right side of the screen to bring up the QR scanner. (Shown below in green)

Using the QR scanner, scan the QR Code on the Single Sign-On Portal (found on your computer's browser) and the XOTC Authenticator will automatically log you in.

That's it! No usernames, no passwords, no problems!

SSO Usage Instructions

For most applications in the Single Sign-On Portal, you will only need to click the icon corresponding to the Application and you will be automatically signed in and directed to the Third Party Application.

However, some applications may require additional steps to sign in. Below are the applications which require non-standard sign-in.

Connect to RDP/VDI

To start, sign in to the SSO Portal for your company or organization.

You will be taken to the home screen where you will see your available SSO-enabled applications.

Locate the card for your RDP Connection or RDP App (VDI).

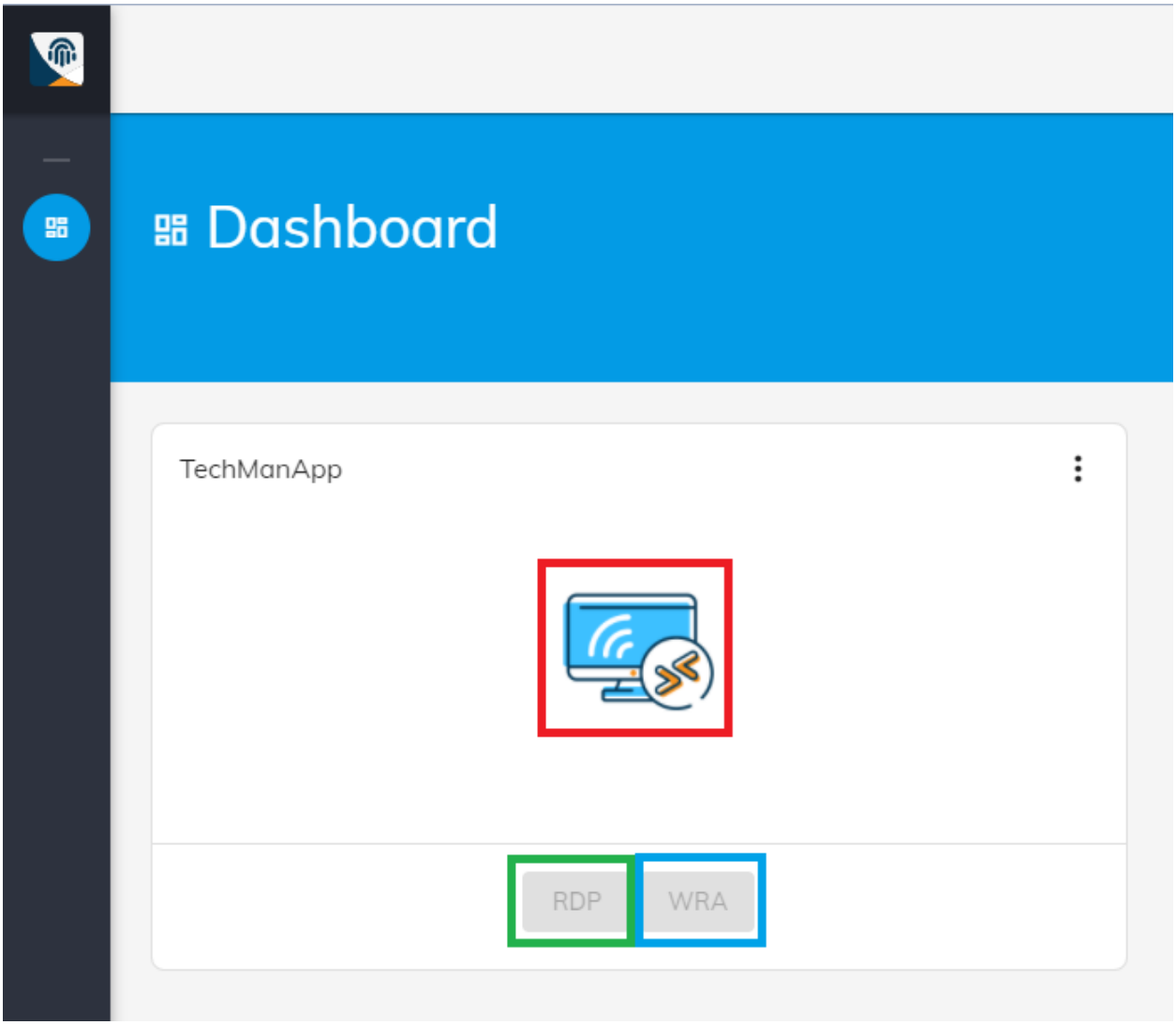
Notice that the **RDP** and **WRA** buttons are grayed out initially.

To access your RDP Application, start first by clicking the blue Monitor button in the center of the Application card (shown below in red). This will generate your dynamic RDP credentials and start an **RDP Session**.

After clicking that icon, the **RDP** and **WRA** buttons should change to a darker color indicating they are no longer disabled.

Click the **RDP** button to download the RDP connection file to connect to your instance. (shown below in green)

You can also click the **WRA** button to download the Xiid RDP Wrapped connection with additional security. (shown below in blue)



Click the downloaded RDP or WRA file to connect to your remote machine.

If you downloaded the RDP file, you will be prompted to sign in to the user account defined in the Xiid Agent Management Portal RDP Application. The password was copied to your clipboard when you created the **RDP Session** above. Paste the password and you will connect to the remote machine.

The one time password must be used within 30 seconds and is only valid **once**.

Reset your XOTC Authentication

If you lose your phone or it is stolen, follow these instructions to reset your XOTC Authenticator and regain access to your SSO Portal.

Start by locating the recovery email sent during the SSO User Setup.

Click the orange **Reset Your Second Factor Authentication** button within the email and a browser will open.

On the **Reset OTP** screen, click the red **Reset** button.

When the prompt pops up for confirmation, click the red **RESET** button.

After you see the green text confirming that your XOTC has been reset, go to the main page of the SSO Portal.

On the home page of the SSO Portal, enter your full username including the domain (User Principle Name) and hit **Login**.

From the next screen, enter your password in the **Password** field and click **LOGIN**.

You will be prompted to enter an email address to recover your XOTC Authenticator. You may re-use the same email address as previously.

Next you will be prompted for the One-Time-Password sent to your recovery email address. Copy the OTP from your email and paste it in the SSO Portal.

Last, a window will pop up with a QR code. Switch to your XOTC Mobile App, hit the **"+"** ("plus sign") button in the top right, enter a description for your new XOTC Security Profile, hit the QR Code button, and scan the code shown on the SSO Portal.

Now your account is reset with your new XOTC Authenticator on your new phone!