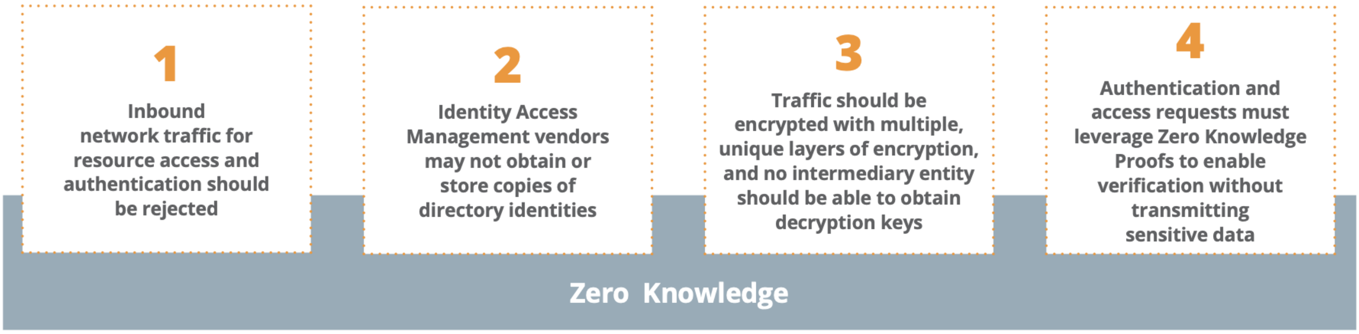
Xiid Zero Knowledge Networking Documentation

Zero Knowledge Networking Introduction

Increased risk of cyberattacks on the enterprise network and cloud-connected users is proving to be more difficult than ever, despite the rise of Zero Trust.

Xiid's Zero Knowledge Networking (ZKN) is a new networking architecture that meets and vastly exceeds the NIST Zero Trust Tenets through the following:

- **All parties – including endpoints and the Zero Trust vendor in-between – are guaranteed to have no excessive knowledge of each other's sensitive data or location**
- **Open inbound ports are never used, eliminating network attack surface**
- **All traffic is wrapped in multiple layers of encryption**
- **Zero Knowledge Proofs authenticate users without transmitting sensitive information or credentials**


1
Inbound network traffic for resource access and authentication should be rejected
2
Identity Access Management vendors may not obtain or store copies of directory identities
3
Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys
4
Authentication and access requests must leverage Zero Knowledge Proofs to enable verification without transmitting sensitive data
Zero Knowledge

This documentation describes the installation, configuration, and operation of Xiid's product offerings, as well as a guide for deploying a sandbox environment that can be used for testing and to gain familiarity with Xiid.

Xiid Products

Product	Description
Identity Access Management (IM)	Xiid's in-house Identity Access Management solution is credential-less and uses Zero Knowledge Proofs to authenticate users. Unlimited numbers of easy-to-use Xiid-provided SSO portals may be provisioned.

Product	Description
	Trust Relationships allow external users easily-revokable access to specific resources without needing to onboard them to your domain. Xiid never stores directory identities but provides the same level of functionality as traditional federated identity providers.
SealedTunnel™ (ST)	SealedTunnel™, Xiid's resource access solution, are triple-encrypted, outbound-only secure tunnels. Backed by Xiid IM and optimized at the lowest levels of the OSI model, any type of internet traffic can be wrapped and secured. Resources located anywhere in the world can connect without ever needing to accept inbound network traffic or even having public IP addresses.

More Information

For more information on **Zero Knowledge Networking**, read our seminal whitepaper.

If you're looking for information on how Xiid conforms to and exceeds **NIST's Zero Trust Tenets**, check out our NIST compliance guide.

Technical Overview

Xiid's **Zero Knowledge Networking (ZKN)** products consist of a variety of components that are spread throughout different areas within and outside the enterprise network. It is helpful to understand what these components are and where they reside.

Birds-Eye View

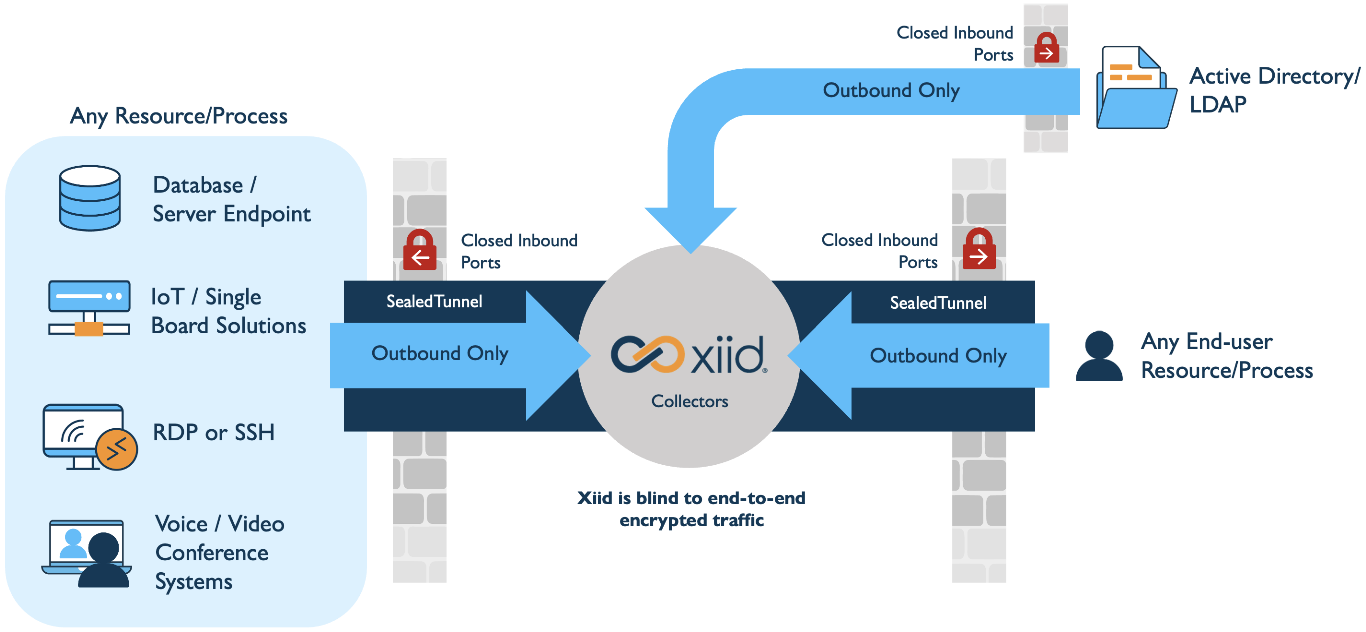
At a high level, the technology underpinning Xiid's products can be split into four major components:

- Xiid One Time Code Authenticator (XOTC™)
- Collectors
- SealedChannels and SealedTunnels™
- Agents

These four components work together to form the Zero Knowledge Network.

▶ **Click for a metaphorical description of Xiid's ZKN**

Here's a high-level diagram describing Xiid's implementation of ZKN from a more technical (and less metaphoric) perspective.



Xiid One Time Code Authenticator (XOTC™)

The Xiid One-Time-Code Authenticator (XOTC, pronounced "exotic") Authenticator, is an application which allows users to create and bind security profiles for various credentials to a credential-less one-time-code.

By default, authentication is performed using **Zero Knowledge Proofs**, ensuring that sensitive, stealable identity information is never transmitted across the internet.

The XOTC Authenticator is available for Android and iOS devices.

Xiid Collectors

TIP

For most deployments, Xiid Collectors are hosted and managed by Xiid as a SaaS service. Xiid Collectors may be licensed and self-hosted for sensitive, high-risk deployments.

Xiid Request Collectors and SealedTunnel Collectors are the front-lines of Xiid's technology. Collectors are one of only two components (the XOTC Authenticator App being the other) that "reside" outside the network perimeter.

Xiid Collectors never require inbound network access to enterprise networks and all authentication data that they receive is encrypted and anonymized, ensuring that even if a Collector were to be comprised, an attacker still would be unable to access private resources.

Request Collector

Request Collectors collect requests from identity providers, convert them to our patented Smart Hybrid Protocols (SHyPs™), and place them into a queue to be picked up by an Xiid Agent. Request Collectors managed by Xiid have built-in redundancy across regions and cloud providers, top-of-the-line security, and protections at every level to minimize attack surface.

SealedTunnel Collector

SealedTunnel Collectors (STCollector) are a variation of Request Collectors that are purpose-built for the SealedTunnel product.

The STCollector operates similarly to a standard Request Collector except that it does not leverage an inner SHyPs layer, since SealedTunnels support unstructured data such as an RDP connections or web traffic. Thus, the SealedTunnel Collector does not use SHyPs to transform data before placing it in the collector's queue.

SealedChannels and SealedTunnels™

Traditionally, careful opening of inbound ports was necessary to provide access to corporate resources. This is risky, however, as open inbound ports vastly increase the attack surface of your domain.

Xiid, through its SealedChannel and SealedTunnel, are able to deliver the same levels of resource access without ever requiring open inbound ports.

SealedChannel solves this problem by creating an encrypted and secured communication channel that utilizes outbound ports and efficient, consistent polling. The messages polled from within the network are stored in memory on the Xiid Request Collector with multiple layers of strong encryption, including with Xiid's own patented technology, **Smart Hybrid Protocols (SHyPs)**.

SHyPs are Xiid's collection of communication protocols in which only a portion of the actual protocol is known by either side (hence the word "hybrid"). The Request Collector side only understands a portion of how to encrypt the incoming requests before putting them into a queue.

Xiid Agents understand the other half of the encryption protocol and use passive transport mechanisms to only fetch the data they need. If any request wrapped in a SHyP in the queue looks suspicious, the request will be immediately discarded.

SHyPs work by leveraging the *structure* of data. This means that purpose-built SHyPs are made for specific types of data and cannot be used with general, unstructured data.

Layering these technologies creates a tightly locked-down communication channel through which your internal network can safely communicate with the outside world.

The SealedTunnel operates similarly to the SealedChannel but without using SHyPs, and is used for process-to-process tunneling between remote resources. The SealedTunnel, along with all Xiid software, also allows for all inbound ports to be closed and efficiently polls a SealedTunnel Collector to function.

Xiid Agents

Xiid Agents handle communication via SealedChannels and SealedTunnels.

Agents never require inbound network access and function outbound-only.

Different Xiid Agents service different types of requests and connections from Xiid Collectors:

Agent	Function
IM	Authentication requests
RDP	RDP/VDI connections

Agent	Function
STLink	SealedTunnel connections

IM Agent

IM Agents are deployed on or near your directory (or Active Directory) server.

You can deploy multiple IM Agents within a single domain via Trust Relationships, and the Agents will work together to handle authentication requests.

An IM Agent can also connect to multiple directories and set up application restrictions based on your Active Directory Security Groups, for example.

RDP Agent

RDP Agents are deployed onto machines that you wish to connect to remotely, either through a direct Remote Desktop Protocol connection or to an application on the machine that you would like to access. RDP Agents function seamlessly with the STLink, wrapping RDP connections in multiple layers of encryption via the SealedTunnel.

For added security, RDP Agents randomize and cycle user passwords on each access attempt.

RDP Agents can be provisioned in the Xiid Global Management Portal.

STLink

Though not an "Agent", as it must be installed on both endpoints of a connection, the STLink acts similarly to an Agent and enables SealedTunnel connections.

STLinks can forward web traffic (HTTP/S), RDP and SSH traffic, or any other TCP/UDP data and connect to SealedTunnel Collectors.

The STLink may be deployed onto any machine you wish to connect to remotely, similarly to the RDP Agent, and is used for process-to-process, encrypted tunnelling that is sent to and from `127.X.X.X` (the loopback address) and is dramatically more secure than traditional RDP or VPNs. Only outbound port `443` is required for it to function.

Xiid Portals and Applications

Xiid offers several web portals that serve important functions for both users and system administrators.

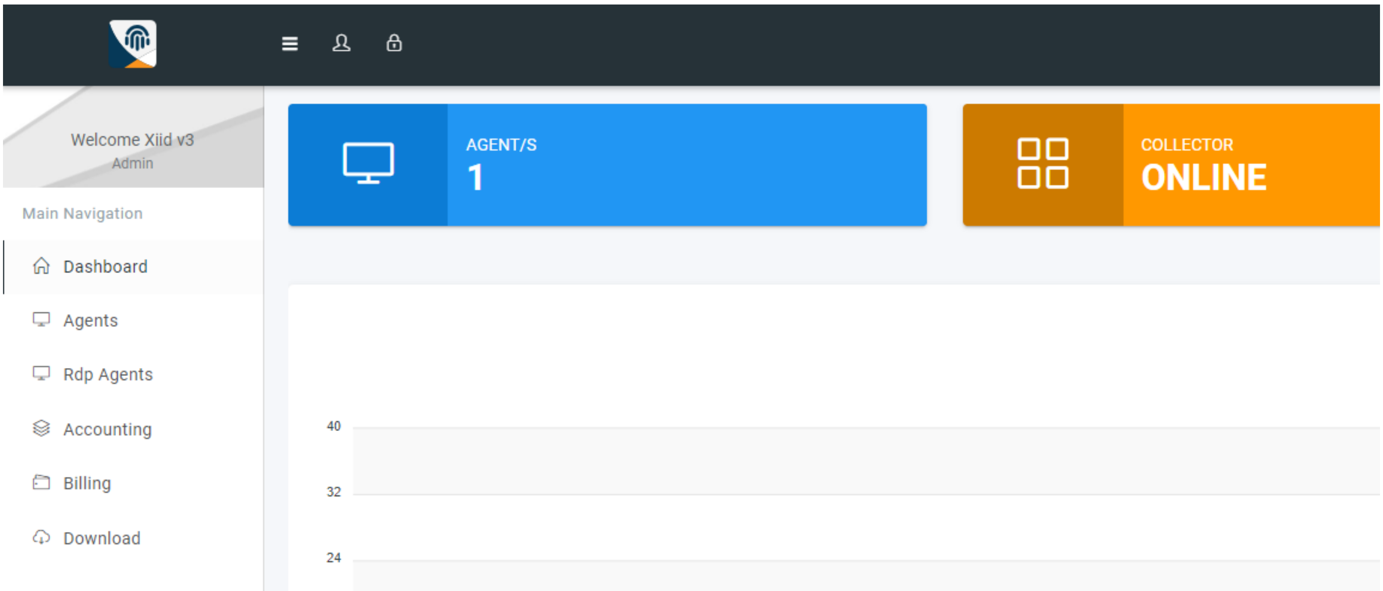
These portals include the Xiid Global Management Portal, the Xiid Agent Configuration Portal, and Single Sign-On (SSO) Portals.

Xiid also provides the XOTC Mobile Application for secure access to your SSO Portals.

Xiid Global Management Portal

The **Xiid Global Management Portal** is used by the system/account administrator(s) to set up an account with Xiid, manage company accounts, view and manage billing information, and track users and API usage.

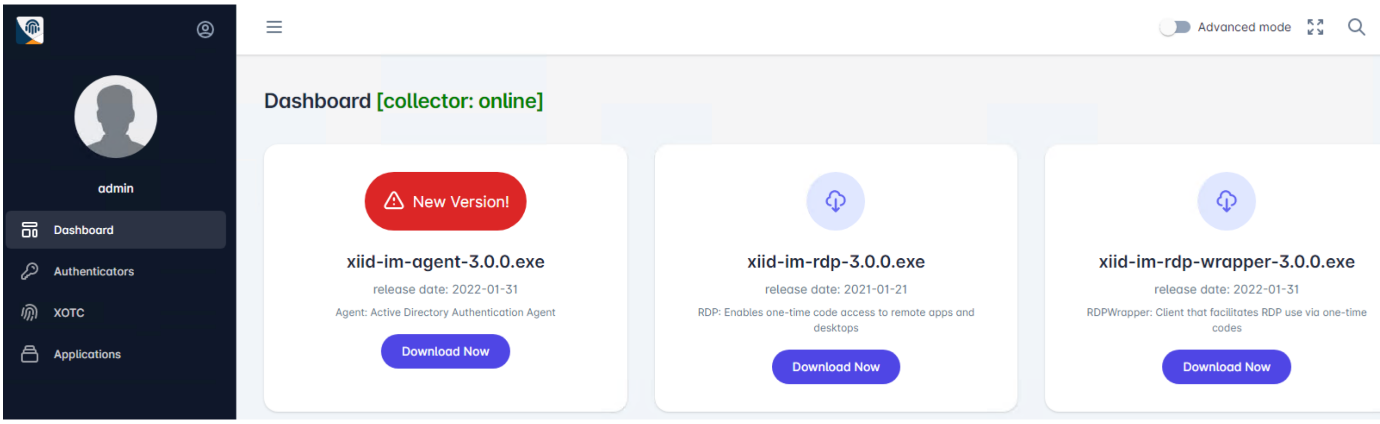
The Global Management Portal also allows administrators to configure Xiid IM Agents to integrate Xiid with their company directory services for authentication.



Xiid Agent Configuration Portal

The **Xiid Agent Configuration Portal** allows system administrators to configure their applications, users, SealedTunnel connections, authentication mechanisms, RDP access, and more.

The Xiid Agent Configuration Portal is typically used by both system administrators and security administrators to configure which users have access to what resources within their environment.



Dashboard [collector: online]

xiid-im-agent-3.0.0.exe
release date: 2022-01-31
Agent: Active Directory Authentication Agent

xiid-im-rdp-3.0.0.exe
release date: 2021-01-21
RDP: Enables one-time code access to remote apps and desktops

xiid-im-rdp-wrapper-3.0.0.exe
release date: 2022-01-31
RDPWrapper: Client that facilitates RDP use via one-time codes

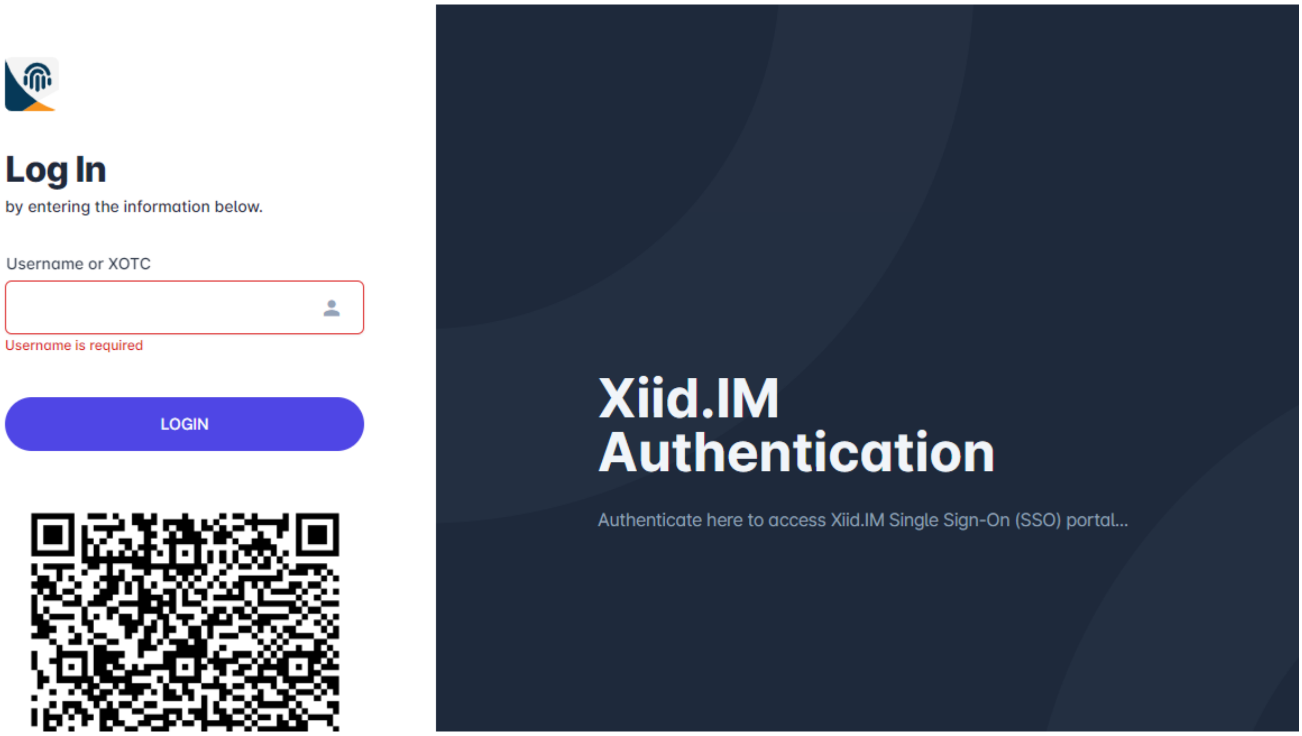
Single Sign-On (SSO) Portal

The **Single Sign-On Portal** allows users to securely authenticate against their domain and access their applications from any location.

Users scan a one-time-use QR code with the XOTC Mobile App on the user's smart device and they are logged in and granted access to their applications and resources.

> **TIP**
>
> Other methods of authentication that do not require a mobile device, such as the YubiKey or CAC/PIV cards, are supported.

Applications accessed through the Single Sign-On Portal can be run locally or over the internet based on user preference and application location.



Log In

by entering the information below.

Xiid.IM Authentication

Authenticate here to access Xiid.IM Single Sign-On (SSO) portal...

XOTC Mobile Application

The **XOTC Mobile Application** allows users to securely access their company's secure network by authenticating with the user's mobile device, such as a smartphone, using Xiid's secure One-Time-Code (XOTC) system.

Users scan the QR Code presented at SSO Portal sign-in using the XOTC Mobile Application to access their applications and resources.

Xiid requires a user-established 6-digit pin code to access the XOTC Mobile Application on the user's device for enhanced security. Other secure methods to access the Mobile Application are allowed, such as biometric authentication (device-permitting).

The XOTC Mobile Application only supports the following operating systems:

iOS

- iOS version 15+

Android

- Android 14+

SSO User Setup

TIP

If your organization chooses not to use the XOTC Authenticator and/or and is using YubiKeys or CAC/PIV cards, contact Xiid for further assistance.

For users to self-onboard to Xiid and access their SSO Portal(s), they must:

- Install the XOTC Authenticator
- Connect their Authenticator to an SSO Portal

Install XOTC

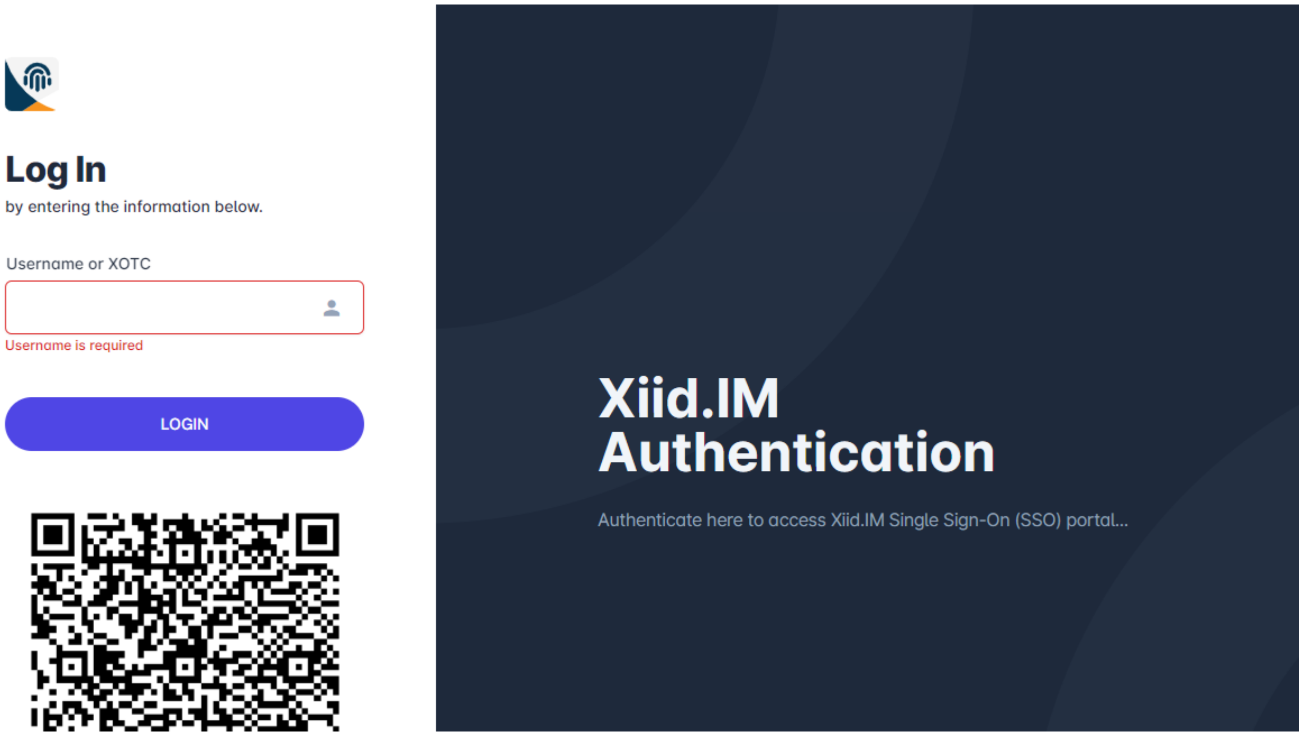
- Install the XOTC Authenticator on your iOS or Android device
- Open the application
- The first time that you open the XOTC Authenticator App, you will be asked to set a 6-digit PIN. This PIN is an added layer of security to ensure that nobody but you can access your Xiid Mobile App.
- You may also enroll in biometric login (recommended, if available on your device)

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

Keep the app open, and we'll return to it soon!

Sign In to the Single Sign-On Portal

- On your computer, navigate 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 may look similar to this: `https://example.us.xiid.im/home/apps/login`



Log In

by entering the information below.

Username or XOTC

Username is required

Xiid.IM Authentication

Authenticate here to access Xiid.IM Single Sign-On (SSO) portal...

- Enter your **company username** in the `Username` 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.

DANGER

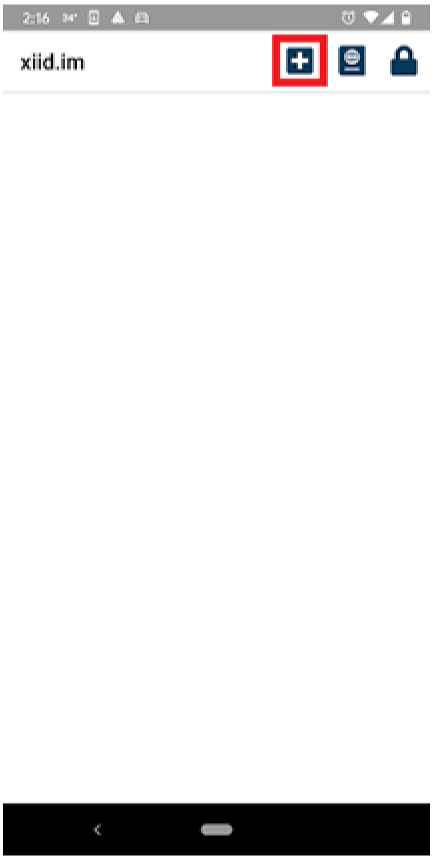
After initial login, Xiid will **never** ask for your password again. If asked for your password in the future, do not provide it. You may be the target of a phishing attack.

- After entering your password, you will be prompted to provide an email address. This email address is used send you a link that can be 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.

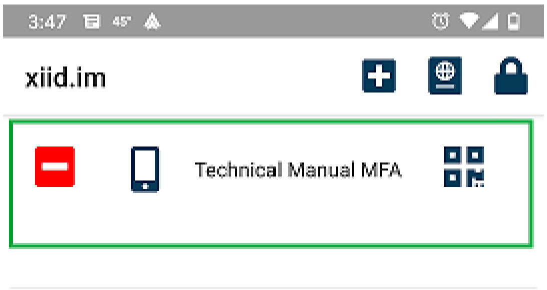
WARNING

You will receive an email from Xiid with a link for you to use to reset your XOTC Authenticator. **Do not lose this email.** If you ever misplace this email, contact your system administrator.

- 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. `HR Resources`) 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 using the link that was emailed to you.

For each new mobile device, you will need to associate the device once with your company network.

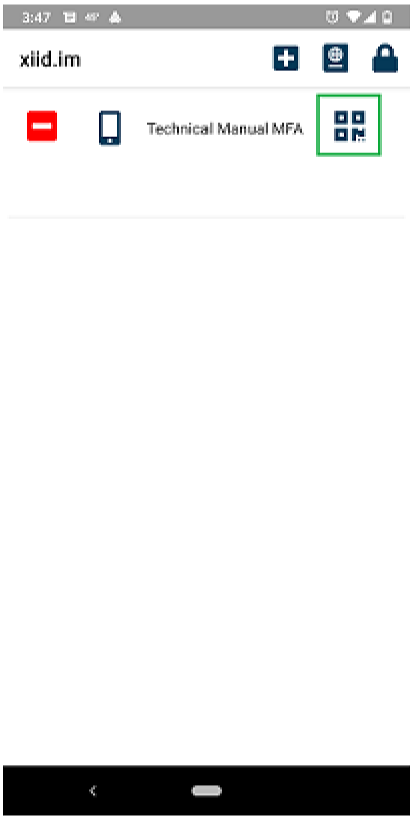
Now you’re all set up to use the Xiid Single Sign-On Portal with the XOTC Authenticator!

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.

Each time you use the Xiid.IM system:

- Navigate your browser to your SSO Portal.
- You will see a QR Code available under the `Username` input box.
- On your mobile device, open the XOTC Authenticator App, find your security profile, and 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 and the XOTC Authenticator will automatically log you in.

That’s it!

SSO Usage

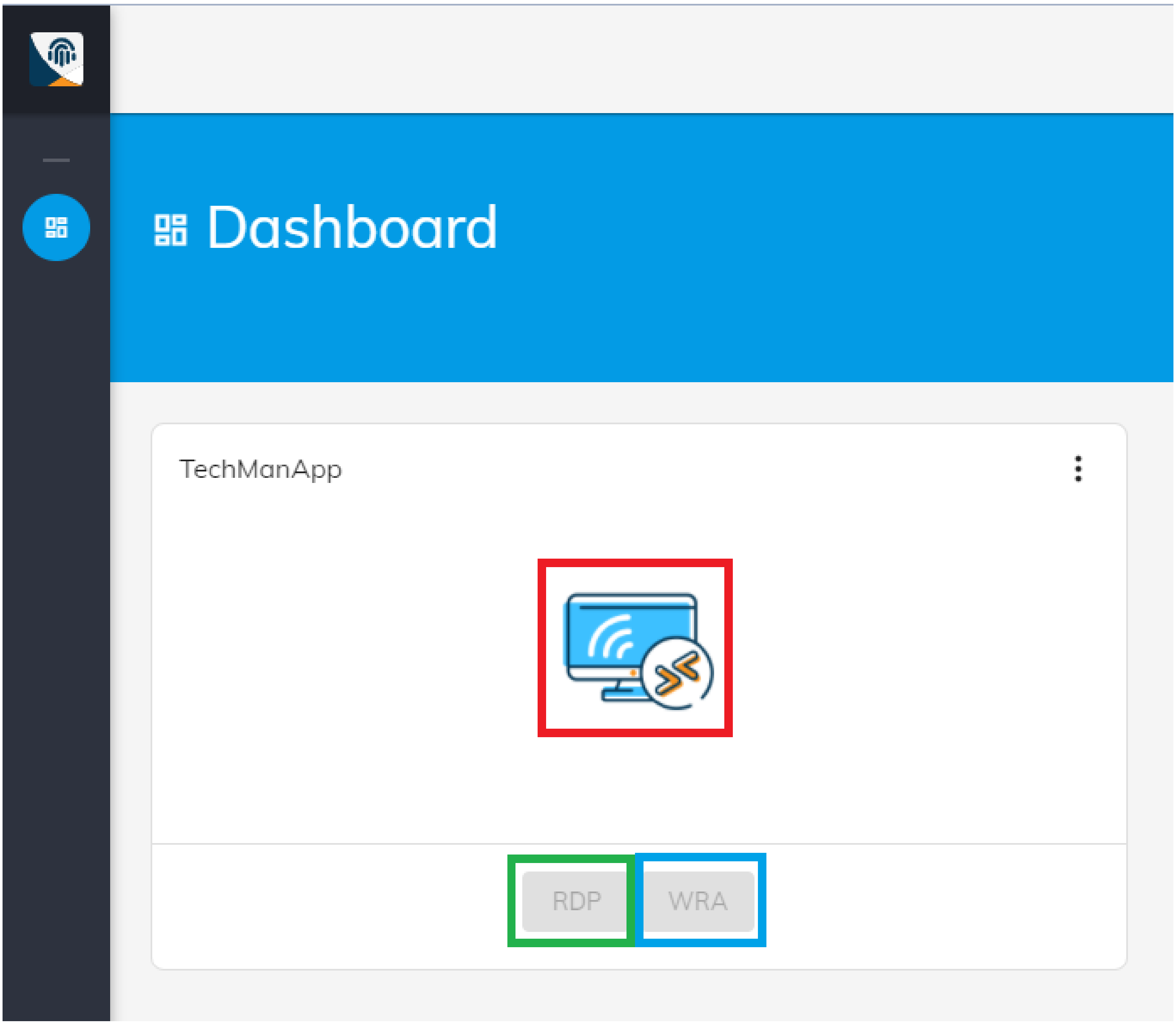
For most applications in the SSO Portal, you will only need to click the card with your desired Application and you will be automatically signed in and directed to the Third Party Application.

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

- RDP/VDI

RDP/VDI

- From the home screen of your SSO Portal, 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 (shown below in blue).



- Open 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.
- A one-time 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**.