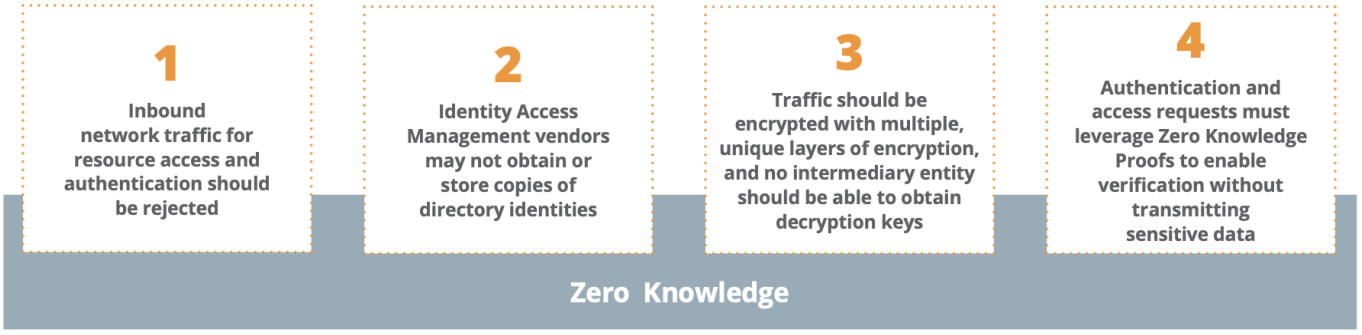
Xiid Zero Knowledge Networking Documentation

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**



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

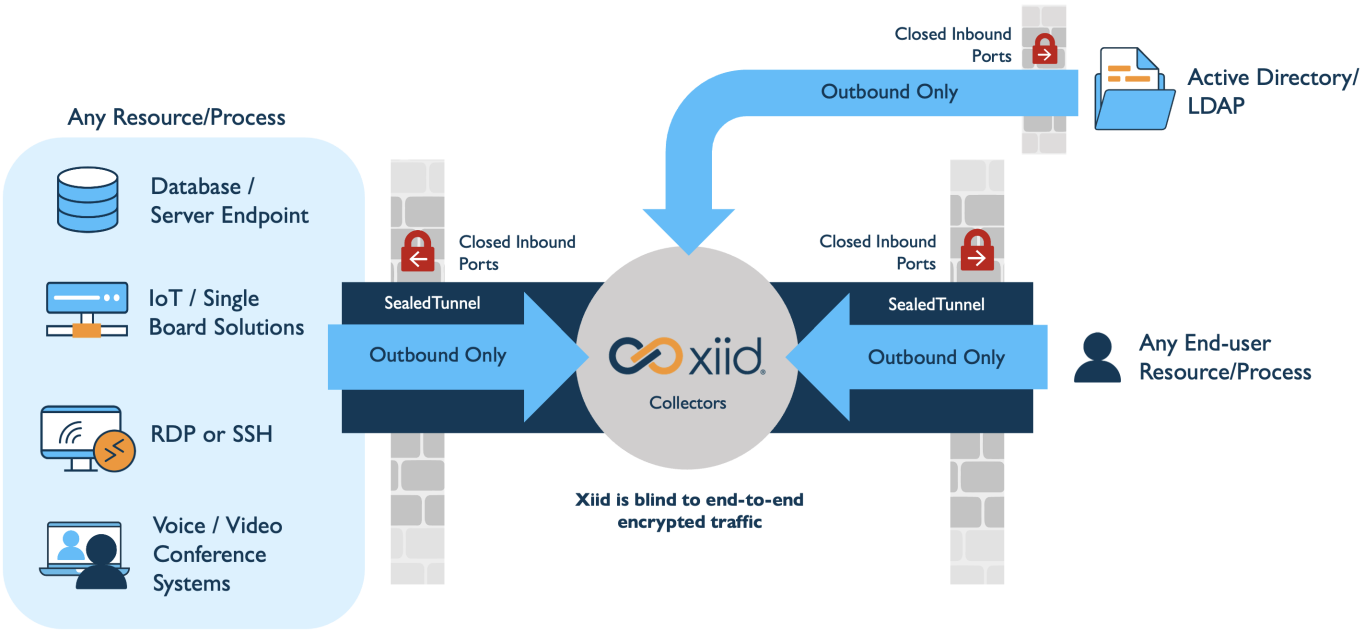
At a high level, the technology underpinning Xiid's products can be split into four major components:

- 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.

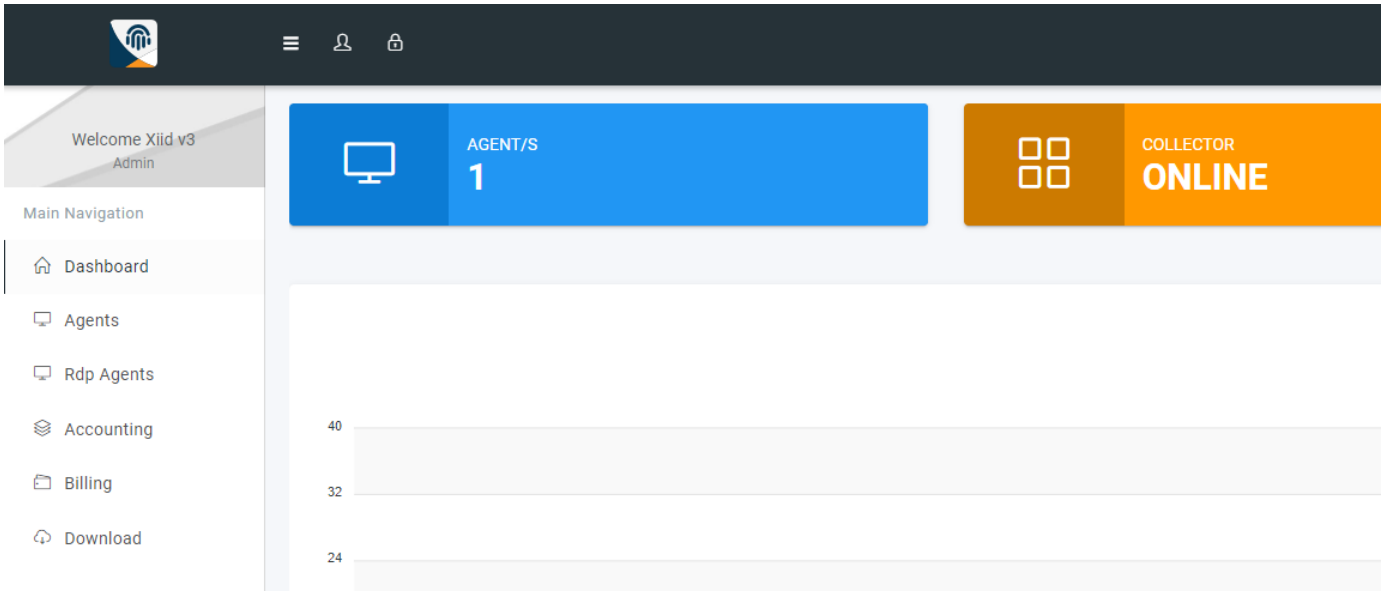
These portals include the Xiid Global Management Portal, the Xiid Agent Configuration Portal, and Single Sign-On (SSO) Portals.

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.

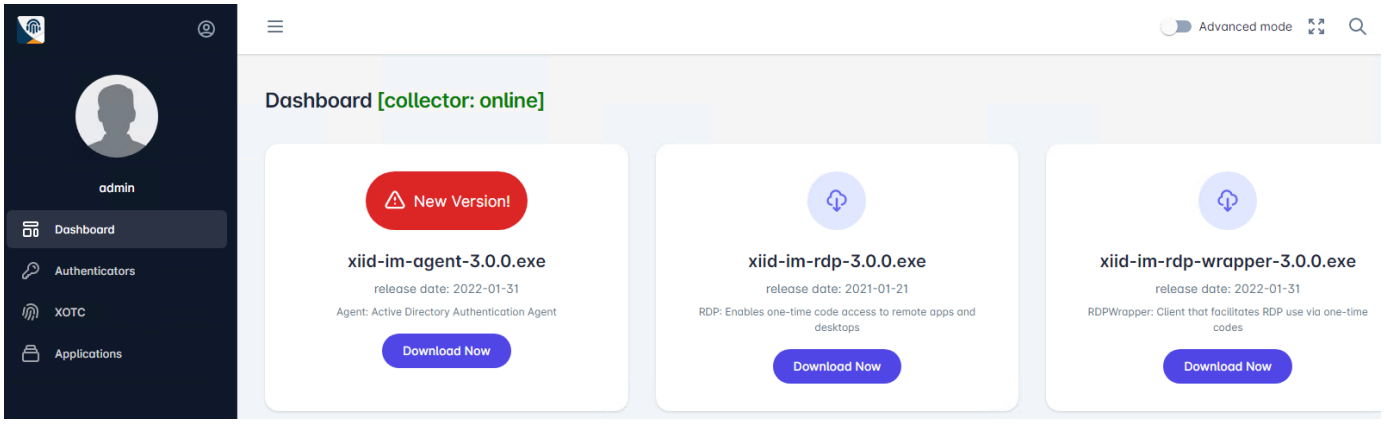
The Global Management Portal also allows administrators to configure Xiid IM Agents to integrate Xiid with their company directory services for authentication.



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.



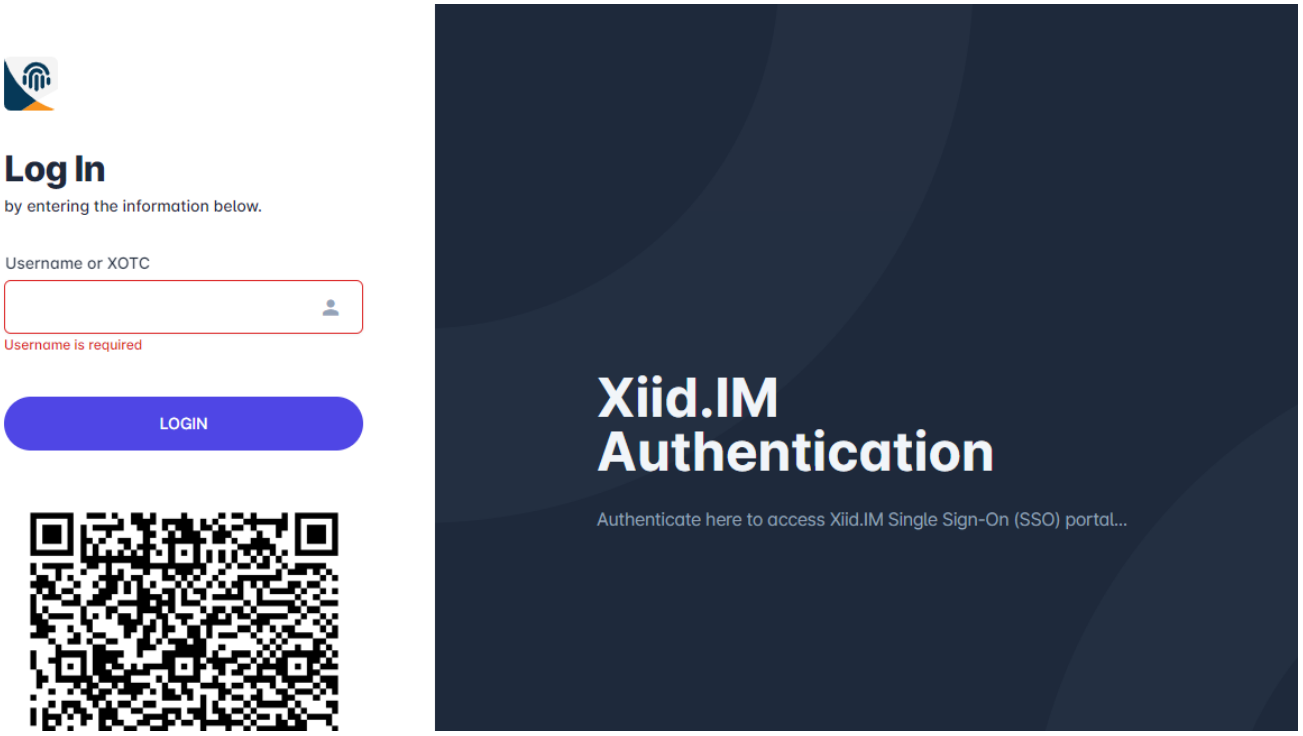
Single Sign-On (SSO) Portal

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.



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+

Xiid Identity Access Management (Xiid IM)

Using Zero Knowledge Proofs and one-time codes for each login session, **Xiid IM** eliminates the risk of credential theft while providing users with a seamless, secure, and hassle-free authentication experience.

Xiid **never** views, syncs, or stores your directory identities and credentials, yet provides efficient worldwide authentication capability.

This guide will walk you through deploying and configuring Xiid IM in your organization.

IM Components

Each component of **Xiid IM** serves a key role in enabling Xiid's comprehensive Zero Knowledge Networking **Identity Access Management (IM) solution**. Understanding the function of each of these components individually will help system administrators better manage and interact with the Xiid ecosystem.

Request Collector

> **DANGER**
>
> Because it is addressable, a Request Collector should **never** be located on the same network as your directory service. We recommend that your directory service be segmented and isolated to its own subnetwork.

Request Collectors are the front lines of Xiid's Zero Knowledge Networking Architecture and are the only component within Xiid's architecture that allows external, inbound communication over inbound Port `443`.

The Request Collector collects authentication requests and puts them into a queue which is then consumed by an Xiid Agent. The response from the Agent is forwarded back through the Request Collector using Perfect Forward Secrecy. Each Collector can support thousands of requests per second.

All code for the Request Collector is compiled to binary and uses no third-party libraries. Data from requests is never stored on disk, and **all data flowing through the Collector is encrypted end-to-end** where the Collector is never one of the "ends".

Xiid-vended Requests Collectors are available as a SaaS service, securely managed on Xiid's infrastructure and distributed across multiple regions and cloud providers.

Although not needed in most cases, a Collector can be self-deployed instead for extremely sensitive use cases.

SealedChannel

The Xiid SealedChannel is a one-way communications channel that is established between an Xiid IM Agent and an Xiid Request Collector.

When an Xiid Agent is set up, a code is provided to the Agent which allows the Agent to reach out to the Request Collector to establish the communications channel.

After the connection has been established, authentication requests will be accepted by the Request Collector. Next, those requests are repackaged into Xiid's patented **Smart Hybrid Protocols (SHyPs)** that only physically allow for the bare minimum, encrypted information necessary to fulfill an authentication request, eliminating the risk of malicious code injection.

Finally, the request, packaged into SHyPs, is put into the Request Collector's queue to be picked up and serviced by the proper Xiid Agent.

XOTC Authenticator

The **Xiid One Time Code (XOTC) Authenticator**, a key piece of Xiid's Zero Knowledge Networking approach, is a highly-secure, one-time-code-based authenticator that uses Zero Knowledge Proofs to authenticate users rather than traditional credentials.

Users scan a QR code with the XOTC Mobile Application to log in to SSO Portals and access their resources.

No sensitive identity information is ever transmitted over the internet and stealable, and the absence of traditional credentials rebuffs phishing attempts.

Requests via XOTC are wrapped in multiple layers of encryption and a patented protocol, **SHyPs**, over the SealedChannel.

Additionally, codes are bound to singular browser sessions, so interception and replay of a code in a Man-in-the-Middle (MITM) Attack would not enable an attacker to authenticate themselves on a victim's behalf.

Agents

An **Xiid Agent** is a light, intermediary piece of software that acts as the liaison between the Request Collector and your internal resources. Through the use of Agents, inbound ports on your network can be closed.

An Agent pulls requests, outbound-only, from the Request Collector queue and takes appropriate action depending on the type of Xiid Agent. Agents reside in the same network segment as the resource with which the Agent interacts.

Xiid highly recommends using proper network segmentation to, at a minimum, separate your resources by subnets, with Xiid Agents handling communication between subnets.

IM Agent

The **IM Agent** resides in the same subnet as your directory and provides the **Agent Configuration Portal** and liaison to your directory for servicing authentication requests.

Importantly, the IM Agent handles all authentication interactions with your directory and moderates access to and vends SSO portals.

Through its Agent Configuration Portal, it allows for configuration of multiple directories, setting up Authenticators, Firewalls, Translators, and Trust Relationships, and configuring your Xiid SSO Portals, including the Applications that should be available through them.

Additionally, this portal is used to configure SealedTunnel.

The Active Directory Agent is part of the core of Xiid's software stack, as almost all interactions with the enterprise network flow through this Agent, either directly or indirectly.

Xiid RDP Agent

The **RDP Agent** runs on machines that you would like to RDP into. The Xiid RDP Agent runs in the background on the machine and manages the credentials used for authentication on the machine through an RDP connection.

When a user attempts to RDP into a machine through an Xiid SSO Portal, the RDP Agent cycles the user's password on the remote machine and pushes this one-time password back out to the client's computer, where it is injected into the user's clipboard.

When the `.rdp` connection file is downloaded from the SSO Portal, the username will already be provided, and the user can paste the password into the prompt to sign in.

As soon as sign in is completed, the user's password is rotated again by the Agent to a new one-time password, reducing the risk of breach if the first password was intercepted.

SSO Portals

Xiid's easy-to-use **SSO Portals** allow users easy access to the resources they need, which include SaaS applications, SAML2.0 applications, RDP/VDI, internal applications, and remote access to any resource over the SealedTunnel.

Xiid allows system administrators to set up an unlimited number of SSO Portals for different groups of users.

When you create a new SSO Portal, you can specify an ID which will be used in the SSO Portal's URL.

It is recommended that, at a minimum, system administrators set up SSO Portals that correspond to directory **Security Groups** that reflect different permission levels, such as an SSO Portal for IT with specific RDP access to remote machines on the network that should not be accessible to other users in the domain.

Applications

Xiid Applications allow System Administrators to integrate various external applications into SSO Portals.

For each application that you would like to provide access to, you can create an Application Component within the Xiid IM Agent defining how to integrate with the external application.

Xiid currently supports 5 types of applications: RDP, RDP Apps (VDI), Microsoft 365, Google Workspace, and any external application that supports SAML2.0 authentication.

When configuring Xiid Applications, you can specify which SSO Portal(s) the application will be available through.

Authenticators

Xiid Authenticators connect IM Agents to LDAP Directories, including Active Directory, and underpin the XOTC Authenticator and other methods of authenticating supported by Xiid.

They are also used to separate SSO Portals and Applications by Security Groups within those directories. For each Security Group, you can create an Authenticator to your LDAP Directory with specified **included** Security Groups (to grant access to specified SSO Portals) as well as **excluded** Security Groups (to deny access to specified SSO Portals).

You may create an unlimited number of Authenticators with any number of connections to any number of LDAP Directory Services within the same subnet as the IM Agent.

Secondary Authentication

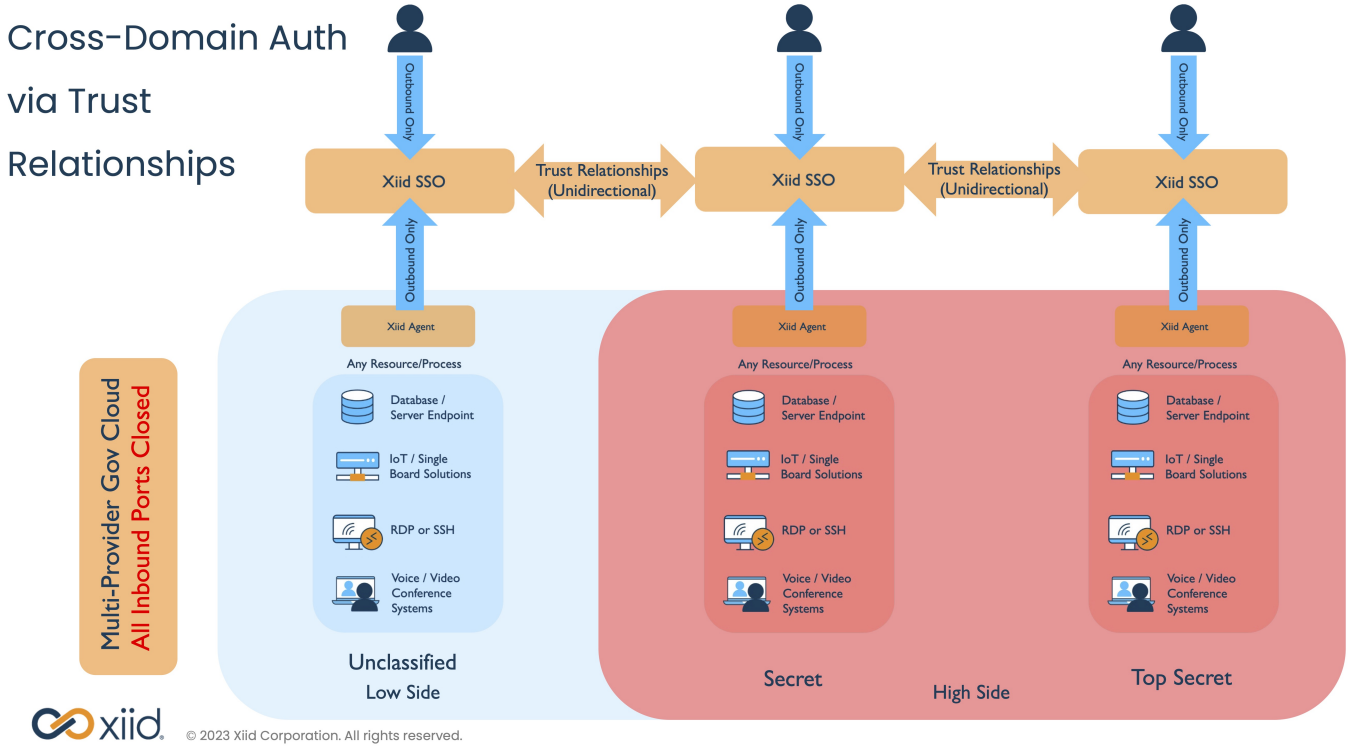
Xiid supports legacy 2-Factor Authentication for accessing Single Sign-On Portals, as well as methods such as YubiKeys and CAC/PIV cards.

Trust Relationships

Virtual Trust Relationships make it easy to share resources between separate domains, unidirectionally, without making modifications to any directories.

Virtual Trust Relationships allow System Adminstrators to create ephemeral "Trust Relationships" between domains and share specific SSO portals and applications between them.

For instance, this could be used in a multi-provider government cloud environment to allow users logged into a "high-side" SSO portal access to specific resources on the "low-side" without having to switch devices or re-authenticate:



Firewalls

> **TIP**
>
> This Firewall component is an additional layer of security and control provided by Xiid, and is not a substitute for an enterprise firewall. When it comes to your enterprise network firewall, Xiid always recommends closing all inbound ports and access.

Xiid's **Firewall** component allows administrators to add IP addresses to **Allow** or **Deny** lists, allowing communications that need to happen while blocking potential risks.

The IM Agent will accept or deny any attempts to authenticate based on the lists configured. If a user attempts to sign in from a denied IP address, the authentication request will be ignored by Xiid.

Users can create and use as many Xiid Firewalls as they see fit to secure their connections in different circumstances.

Translators

Translators are an exceptionally powerful feature that allow administrators to convert incoming authentication requests into particular formats for the local domain.

You can choose to convert domains, usernames, or User Principle Names (UPN) to something that can be understood by the directory service locally.

For instance, if an employee uses their email address for authentication, such as `user@example.com`, but the Active Directory Service uses a local domain name, such as `example.local`, you can configure a domain translator to translate `example.com` to `example.local` when querying the directory.

This could also be leveraged to increase obfuscation of usernames across the network.

IM Agent Setup

Agent Provisioning

Once you have an account with Xiid, the next step is to set up your first **IM Agent**.

- Sign in to the Xiid Management Portal (https://managev3.xiid.com/) and navigate to the **Agents** tab on the left side.
- Click the blue **New Agent** button in the top left of the **Agents** screen to create your first IM Agent.
- The **Agent Info** screen will auto-generate an Xiid Agent ID for you when you start creating a new agent. Fill in the `Friendly Name` section with a display name to contextually associate your IM Agent.
- Ensure that the **Enabled** setting is set to `Enabled` and then click the green **Save** button in the top right of the screen.
- On the **Agents** tab, locate the IM Agent you just created, click **</>** in the **Code and Info** column, and click the green **Copy** button next to the Agent Activation Code. This retrieves your `Code`, which is needed during installation.

Agent Installation

TIP

We highly recommend installing your IM Agent in the same subnet as your LDAP directory or directly on your Domain Controller. For standalone SealedTunnel installations, we recommend installing the IM Agent on its own isolated subnet.

- From the machine you intend to install the IM Agent on, log in to the Xiid Management Portal and via the **Download** tab, download the `Active Directory Authentication Agent (xiid-im-agent)` (blue icon).
  - If the machine does not have internet access, download the installer on another device and transfer it to the desired machine.
- Run the installer as an administrator and move through the prompts.

- After the installation completes, a browser window will appear and will prompt you for your `Code`
- You will be prompted for an Administrator `Username`. This will be your username for the Xiid Agent Configuration Portal.
- Next, you'll be prompted for an Administrator `Password`. This will be your password for the Xiid Agent Configuration Portal.

Your IM Agent is now installed and registered with your Xiid Account!

Agent Uninstallation

To uninstall the Xiid Agent from a machine, you can run the uninstaller from either the Windows **Add or Remove Programs** menu or directly from the installation folder, located by default under `C:\Program Files\Xiid.IM Agent\unins000.exe`.

If they exist, manually delete the Xiid Registry Editor entries under `HKEY_LOCAL_MACHINE\SOFTWARE\Xiid Corporation`, as well as any leftover files/folders in `C:\Program Files\Xiid.IM Agent` and in `C:\ProgramData\xiid`.

It is also recommended that you delete the IM Agent object in the Global Management Portal after uninstalling completely from a machine.

Xiid IM Configuration

With the Xiid Agent securely running on our domain controller, we can now use its **Agent Configuration Portal** to configure Xiid IM! 🚀

You can access the Agent Configuration Portal via the shortcut added to your desktop during installation or at `https://127.0.0.1:10458/`.

> **TIP**
>
> If your browser indicates that your connection is not secure when accessing the Portal on `127.0.0.1:10458`, this is expected behavior. This warning may be ignored safely.

Authenticator Setup

Creating an Authenticator

The first step is to set up an **Authenticator**, which will allow the Agent to communicate with your LDAP director(ies).

- Start by opening the **Xiid Agent Management Portal** by clicking the Browser Icon labeled **Manage Xiid.IM Agent** on your desktop.
- Log in using the administrator credentials you set during setup.
- In the Xiid Agent Management Portal, navigate to the **Authenticators** tab.
- Click the purple **Add Authenticator** button in the top right.
- Enter a description of the Authenticator that will help you associate the authenticator to your LDAP Service and its corresponding user groups, domain mapping, and IM Agent.
- In the **Connector** section, provide a description of the `Connector`. The `Connector` is what defines the communication parameters to your LDAP service.
- In the **Type** dropdown window, select `ldap`.
- For the **Server URL** field, enter the IP Address of the LDAP service. You may use the loopback address (`127.x.x.x`) if the LDAP Directory Service is running on the same machine as the Active Directory Agent.

- For the **Username** and **Password** fields, enter the credentials of an LDAP user that has access **only** to query the LDAP directory. No other permissions are needed nor recommended for this service user.

> **TIP**
>
> The service account that the Xiid Authenticator will use needs sufficient permissions to query the LDAP directory. The minimum level of permissions that is part of the default permissions set in AD and is sufficient is the `Domain Users` group.

The `Username` you provide *must* be the fully qualified User Principle Name.
Incorrect: `user`
Correct: `user@example.com`

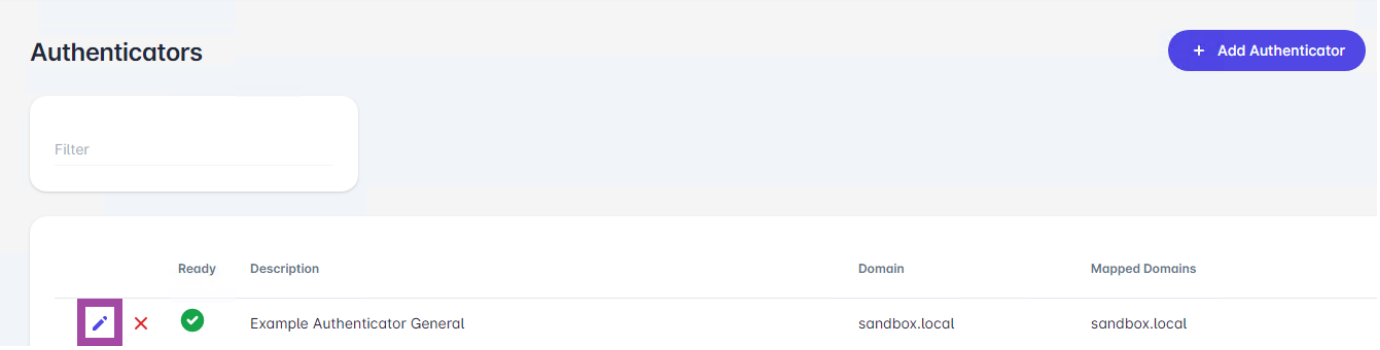
- Click the purple **Save** button and a window will pop up asking for the **external** domain name that you would like to map to the internal domain name. You can choose the same name as the internal if no domain name mappings are necessary.
- In the Authenticators table, you should now see a row for your newly created Authenticator.

Configurating Security Groups for an Authenticator

Next, you can configure the **Security Groups** that will be queried with this Authenticator.

> **TIP**
>
> Only **user-defined** Security Groups can be used. The Windows-defined Security Groups created by default in Active Directory cannot be used.

- Enable **Advanced Mode** by clicking the switch next to **Advanced Mode** in the top right corner.
- Click the **Pencil Button** on the left side of row with the Authenticator you wish to edit (shown below in **purple**).



- With **Advanced Mode** enabled, you will now see two additional fields labeled `Group Include` and `Group Exclude`.
- You can populate either of those fields with as many Security Groups as you would like **included** for the Authenticator (using the `Group Include` field) or specify any number of Security Groups you would like to **exclude** from this Authenticator using the `Group Exclude` field.
  - Separate multiple Security Groups using a comma (`,`).

Firewalls

Firewalls offer an additional, optional layer of application security to filter unwanted IP addresses or restrict subnet access to your SSO portals.

- Enable **Advanced Mode** by clicking the switch next to **Advanced Mode** in the top right corner.
- Navigate to the Firewalls tab and click the purple **Add Firewall** button in the top right.
- On the **Add Firewall** screen, provide a `Description` for the Firewall that reminds you of the firewall rule this policy enacts.
- For the `Block Type` dropdown, select whether you wish to block all requests or approve all requests from a given IP address.
- In the `IP Address` field, enter the IP addresses you wish to allow or block.
- Enter any comma-separated `Tags` you would like to use to differentiate this Firewall.
  - `Tags` can be used to create groups of Firewalls, so if you have a corporate firewall rule that encompasses multiple IP allow/deny lists, you can group them all under a single tag to include in your SSO Portals.
- Click the purple **Save** button to apply your Firewall.

Translator Setup

You can choose to *translate* domains, usernames, or User Principle Names (UPN) to something that can be understood by the directory locally with **Xiid Translators**.

This could be useful, for instance, if an Application requires an email address for sign in as opposed to domain credentials.

- Sign in to the Xiid Agent Management Portal and navigate to the **Translators** tab.
- On the **Translators** screen, click the purple **Add Translator** button in the top right.
- Enter a `Description` for the translator that helps you understand what data is being translated to and from the local domain context.
- In the `Translator Type` dropdown, select one of the following:
  - `Domain`: to translate an external domain name, such as `example.com` for an email address, to an internal domain name, such as `example.local`
  - `Name`: to translate a username, such as `BillNye` to another username, such as `NeildeGrasseTyson`
  - `UPN`: to translate a fully qualified username, such as `BillNye@example.com` to `NeildeGrasseTyson@example.local`
- In the `Translate From` field, enter the `Name`, `UPN`, or `Domain Name` to translate authentication requests from.
- In the `Translate To` field, enter the `Name` or `UPN` to translate to when sending the authentication request to the LDAP service.
  - *Note: The `Domain` type does not have a `Translate To` field because the domain name is implied from the `Connector` in the Authenticator.*
- Enter any `Tags` you would like to use to group this Translator with other Translators.
- Click the purple **Save** button to apply your Translator.

XOTC Setup

TIP

While Xiid IM supports other types of authentication mechanisms, XOTC is the most secure and should be the first choice for most deployments.

The **Xiid One Time Code (XOTC) Authenticator** is a highly-secure, one-time-code-based authenticator that uses Zero Knowledge Proofs to authenticate users rather than traditional credentials.

- Sign in to the Xiid Agent Management Portal and navigate to the **XOTC** tab.
- Click the purple **Add XOTC** button in the top right.
- Provide a `Description` for the XOTC Authenticator that helps you associate which user groups and rules it covers.
- Choose a duration of time with which the One-Time-Code will be valid for.
  - Xiid generally recommends a one-minute interval to give users a bit of breathing room while signing in.
- Click the purple **Save** button to finish.

Now that XOTC Authentication is provisioned, we need to enforce XOTC Authentication on SSO Portals.

- Navigate to the **SSO Portals** tab and click the purple pencil icon to edit the SSO Portal.
- Click **Next** until you arrive at the **XOTC / MFA** section.
- On the **XOTC / MFA** screen you should now see the new XOTC Authenticator you just created listed in the table.
- Select it and click **Next** until you reach the end and save the changes.

Now, your SSO Portal will enforce XOTC Authentication for your users!

SSO Portal Setup

Xiid provides the ability to set up multiple **SSO Portals** for different user groups.

If you have an IT organization or an Engineering organization, for example, that may need access to special applications or resources, you can separate access using distinct SSO Portals.

- Sign in to the Xiid Agent Management Portal and navigate to the **SSO Portals** tab.

  - Xiid creates a default `home` portal when your first Authenticator is created. You can edit that SSO Portal (although you cannot change the id) by clicking the purple pencil button next to the SSO Portal row in the SSO Portals Table.
- To create a new SSO Portal, start by clicking the purple **Add SSO Portal** button in the top right corner.
- On the **Add SSO Portal** screen, start by providing an `ID` for the Portal which defines the full URL path of the SSO Portal.
  - The default SSO Portal created by Xiid has the `ID` of `home`, so its url would resemble `https://exampleportal.us.xiid.im/home`. If you had used `engineering` as the `ID`, the url would resemble `https://exampleportal.us.xiid.im/engineering`.
- After providing an `ID` for the Portal, enter a `Description` to help you remember the purpose of this SSO Portal and whom it serves.
- Click the **Next** button and select the Authenticator you would like to associate with the portal. Keep in mind, the Authenticator defines the Security Group access policies, so the Authenticator must have properly configured `Include` and `Exclude` Groups to control user access.
- Click the **Next** button and select any Firewalls you have created for use in this SSO Portal.
- Click the **Next** button again and select any Translators you would like to translate requests for this SSO Portal.
- Click **Next** again and select an XOTC Authenticator to enforce XOTC Authentication on the SSO Portal. You are not required to select a secondary authentication method.
- Click the purple **Save Portal** button in the bottom right to save your SSO Portal configuration.

On the **SSO Portals** page you will now see a row for your SSO Portal in the table. Verify that the **Ready** column contains a green check mark.

Application Setup

Now that Xiid IM is fully integrated with your directory, it's time to make it possible to securely access your applications and resources through Xiid!

An **Xiid Application** is a third-party application or resource that you want to be accessible via cards in Xiid's SSO Portals.

Follow these guides for examples on how to integrate different types of external applications into your SSO Portals:

- Remote Desktop and/or VDI
- Microsoft 365
- Google Workspace
- SAML2.0 Applications

Remote Desktop (RDP) and VDI Setup

WARNING

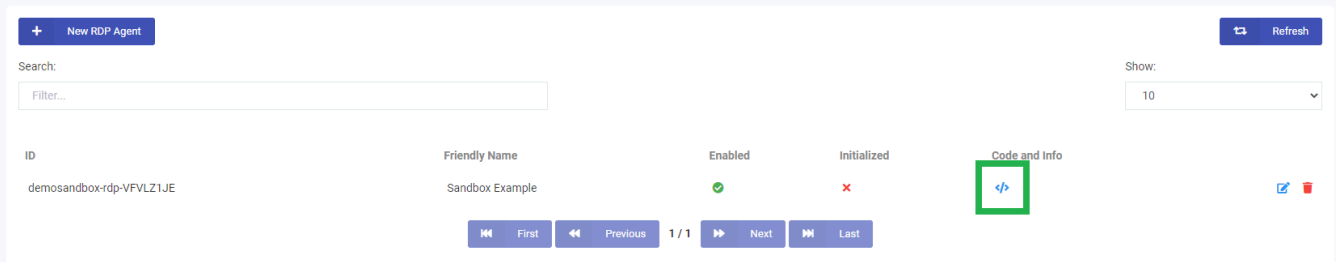
RDP Agents must be able to register themselves with an Xiid IM Agent. If you set up an RDP Agent *prior* to setting up and configuring an Xiid IM Agent, the RDP Agent will not be able to be configured.

This section will walk through setting up RDP/VDI and making access available through your SSO Portal(s).

RDP Agent Creation

First, we need to create an RDP Agent Component in the **Xiid Global Management Portal**.

- Sign in to the Xiid Global Management Portal and navigate to the **RDP Agents** tab.
- On the RDP Agents tab, click the purple **New RDP Agent** button in the top left.
- On the RDP Agent Info screen, provide a name that helps you remember what RDP machine this is.
- Then click the green **Save** button in the top right corner.
- Notice in the RDP Agents table there is a new row for your new RDP Agent. Also take note that the **initialized** column has a red X, which indicates that the RDP Agent Component has not been bound to a running RDP Agent on a machine.
- On the **RDP Agents** tab, locate your newly-created RDP Agent and click the blue **</>** icon in the **Code and Info** column (shown below in green).



- A window will pop up with your `Activation Code` for this RDP Agent. Click the green **Copy** button to copy the code to your clipboard. Please note that sometimes the clipboard does not persist over an RDP connection and you may need to record this code manually.

RDP Agent Setup

With our new RDP Agent provisioned, we're ready to install it on the machine we wish to be able to RDP into.

- Sign in to the Xiid Global Management Portal and navigate to the **Download** tab.
- Click the **Download** button on the RDP Agent Installer icon shown in light green.
- Log into the RDP instance and FTP the RDP Agent Installer to the RDP instance. Alternatively, if your RDP instance has external internet access, you can download the RDP Agent Installer directly on your RDP instance.
- Run the RDP Agent Installer executable on your RDP instance and move through the prompts.
- After the installation completes, a browser will open and ask for your Code, which is the `Activation Code` you obtained in the prior step.

Your RDP Instance is now running the Xiid RDP Agent for secure RDP connection!

RDP Application Setup

DANGER

Never allow the sole administrator account for the machine to be the RDP Agent's `User`.
Since the RDP Agent automatically rotates user passwords, subsequent use of the RDP Agent could cause the administrator to become permanently locked out of the machine.

TIP

The following instructions pertain to setting up an RDP Application *without* the use of SealedTunnel. If you'd like to use RDP over SealedTunnel, follow these instructions instead.

Now that an RDP Agent is configured and bound in the **Global Managament Portal**, adding an RDP Application to your SSO Portal(s) makes it possible to RDP into that machine.

- Sign in to the Xiid Agent Management Portal on your domain controller (or Active Directory Network-adjacent server) and navigate to the **RDP Agents** tab.

    - You should see a row populated in the RDP Agents table for your new RDP Agent. The status column should now show a **green checkmark**.
- After confirming that your IM Agent is aware of your RDP Agent and ready to use it, you can navigate to the **Applications** tab.
- On the Applications tab, click the purple **Choose** button at the bottom of the **RDP** card.
- On the Applications List for RDP Page, click the purple **Add Application** button in the top right.
- Choose the SSO Portal through which you would like be able to access the RDP Connection in the `Portal` dropdown.
- In the `RDP Agent` dropdown, select the RDP Agent you created.
- For `User`, you can provide a username that will always be used for sign-in. This is optional, and if you leave the field blank the **username of the user that is signed in to the SSO Portal** will be used. **Never set `User` to the sole administrator account.**
- In the `IP Address` field, you can provide a static IP address for the RDP instance. If you leave this field blank, the IP address will be dynamically linked to the machine running the RDP Agent. That way, if the RDP machine is assigned a new IP Address, the new address will be automatically used in the SSO portal.
- Check the `Legacy` checkbox to enable `.rdp` file availability in the SSO Portal in addition to the `.wra` file.
- Finally, provide a description for the RDP Application that helps you remember its purpose.
- Click the purple **Save** button and your RDP Connection will be ready for use!

Xiid RDP/VDI App Setup

Instead of granting access to a whole machine, you can grant access to just a single application running on that machine with an **RDP/VDI App**.

- Sign in to the Xiid Agent Management Portal on your domain controller (or Active Directory Network-adjacent server) and navigate to the **RDP Agents** tab.
    - You should see a row populated in the RDP Agents table for your new RDP Agent. The status column should now show a **green checkmark**.
- After confirming that your IM Agent is aware of your RDP Agent and ready to use it, you can navigate to the **Applications** tab.
- Click the purple **Choose** button in the **RDP App** card.

- On the **Application List for RDPAPP** screen, click the purple **Add Application** button in the top right.
- On the next screen, select the SSO Portal to assign the **RDP App Application** to in the `Portal` dropdown.
- Next, in the `RDP Agent` dropdown, select your RDP Agent.
- For `User`, you can provide a username that will always be used for sign-in. This is optional, and if you leave the field blank the **username of the user that is signed in to the SSO Portal** will be used. **Never set `User` to the sole administrator account.**
- In the `IP Address` field, you can provide a static IP address for the RDP instance. If you leave this field blank, the IP address will be dynamically linked to the machine running the RDP Agent. That way, if the RDP machine is assigned a new IP Address, the new address will be automatically used in the SSO portal.
- Check the `Legacy` checkbox to enable `.rdp` file availability in the SSO Portal in addition to the `.wra` file.
- Provide a description that helps you remember what application this is and who it is for.
- In the `Application Path` field, provide the full file path to the application you would like to access over remote connection. The application must be available on the RDP machine. Do not worry about the formatting of the path (e.g. backslashes and whitespace). Example: `C:\Windows\notepad.exe`
- Click the purple **Save** button and your RDP Connection will be ready for use!

RDP Wrapper Setup

> **TIP**
>
> The RDP Wrapper is purely optional and is not required to access any resource through Xiid. Currently, the RDP Wrapper software is only available for Windows.

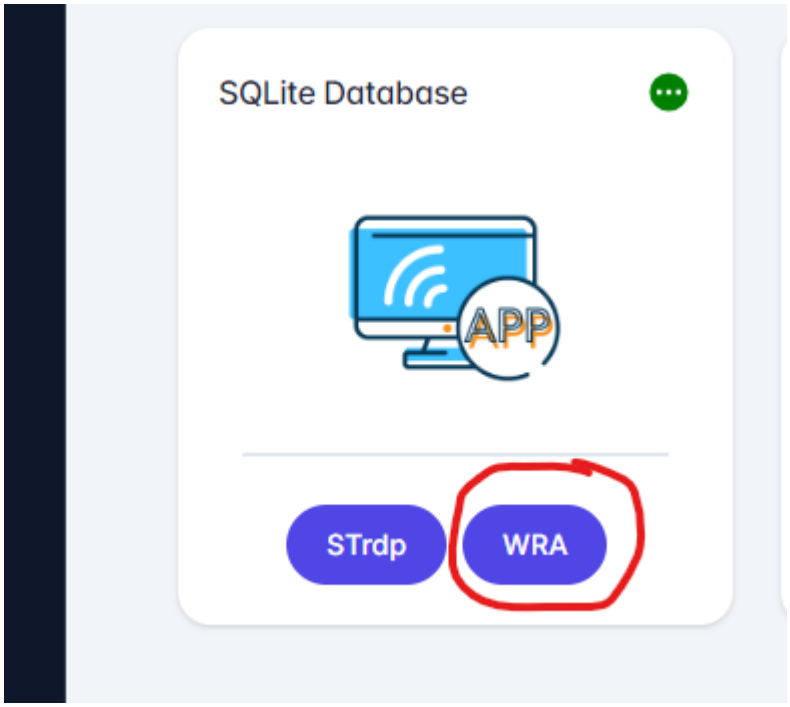
In lieu of pasting a clipboard-injected one-time-password into your RDP application to access a machine through the SSO Portal, Xiid provides **RDP Wrapper** software that includes the one-time-use credential preconfigured.

- From the **Download** tab in the Xiid Global Management Portal, download the RDP Wrapper installer (green icon).
- Run the RDP Wrapper Installer on every machine that you wish to *RDP from*.

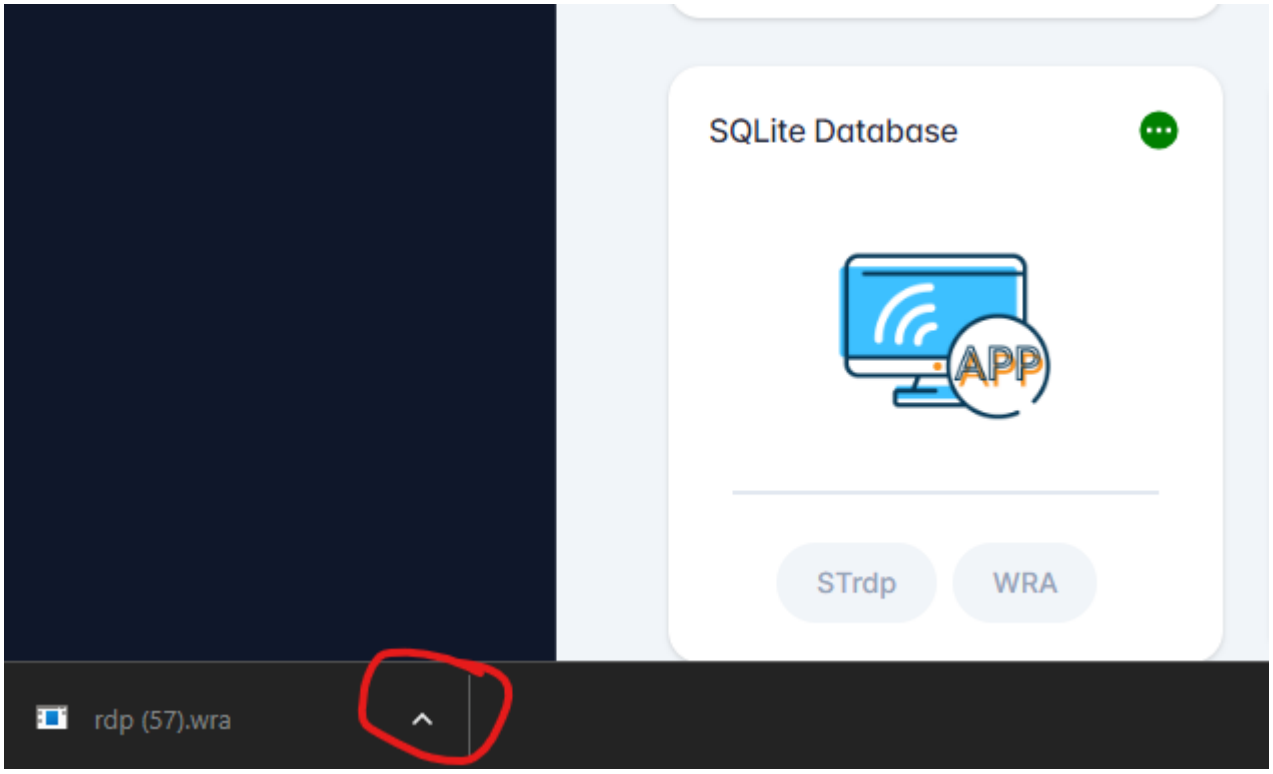
Users can sign in to the Xiid Single Sign-On portal, find the RDP Application, click the **WRA** button and access the machine or application without having to paste a one-time-use password.

RDP Wrapper Auto-Open Setup

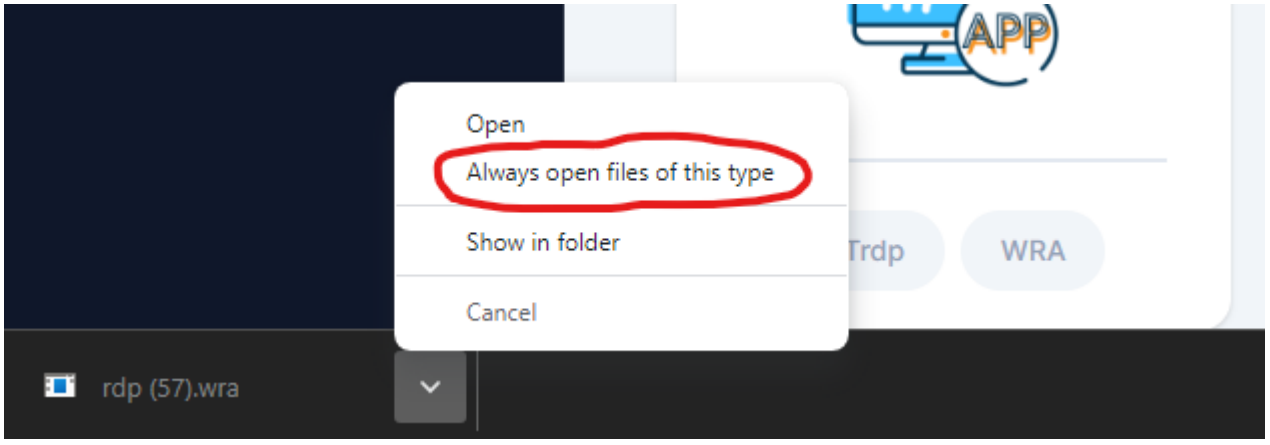
- To enable **WRA** files to open automatically when they are downloaded in Chrome, start by downloading a WRA file through the SSO portal.



- After the **WRA** file is downloaded, near the bottom of Chrome, there will be a pop-up with the file download shown. Click the "Up Arrow" next to the file as shown below:



- Select `Always open files of this type`



- And that's it! Moving forward, your **WRA** files will automatically open after being downloaded in Chrome and prompt you to connect to the instance or application.

Advanced Configuration

When using RDP or RDP App Applications (with or without the SealedTunnel), you may need to leverage dynamic users or reference an internal domain.

For instance, you may want to use a specific structure of local users and grant them all RDP access to the machine (i.e. `username-rdp`).

Dynamic Username Reference

> **TIP**
>
> Using `%username%` in the `Username` field is equivalent to leaving it blank.

You can use `%username%` in the `Username` field of an RDP and RDP App application to reference the user currently logged into the SSO Portal.

For instance, if you would like local users to be created dynamically for each user signing in to the machine, you can enter `%username%-rdp` as the `Username`.

This will tell the RDP Agent on the machine to create a new user based on the current logged-in user's `username` with `-rdp` appended. If the user is named `xiiduser`, for example, the user created locally on the machine will be `xiiduser-rdp` and a one-time-password will be generated for that user.

Domain Reference

You can reference the domain of the Active Directory by using the `%domain%` variable.

For instance, if you would like to cycle the password for a domain user in the Active Directory, you can enter `%domain%\exampleuser` in the `Username` field, and every end-user accessing the machine through the SSO Portal would sign in as `exampleuser` on the domain.

You can also combine variables: `%domain%\%username%` would rotate the `Username` of the domain user that is signed in to the SSO portal.

If you sign in to the SSO Portal as `xiiduser` and click an RDP or RDP App card's blue monitor icon, it will generate a new password on your domain user.

Agent Uninstallation

To uninstall an RDP Agent from a machine, you can run the uninstaller either from the Windows **Add or Remove Programs** menu or directly from the installation folder, located by default under: `C:\Program Files\Xiid.IM RDP Agent\unins000.exe`.

It is also recommended that you delete the RDP Agent object in the Global Management Portal after uninstalling completely from a machine.

Microsoft (Office) 365 Setup

TIP

At a minimum, Microsoft 365 Enterprise E3 Edition is required. Editions below Microsoft 365 Enterprise E3 do not support the authentication mechanisms required by Xiid.

If your company uses **Microsoft 365**, you can enable access via Xiid's SSO Portals.

Xiid IM Configuration

WARNING

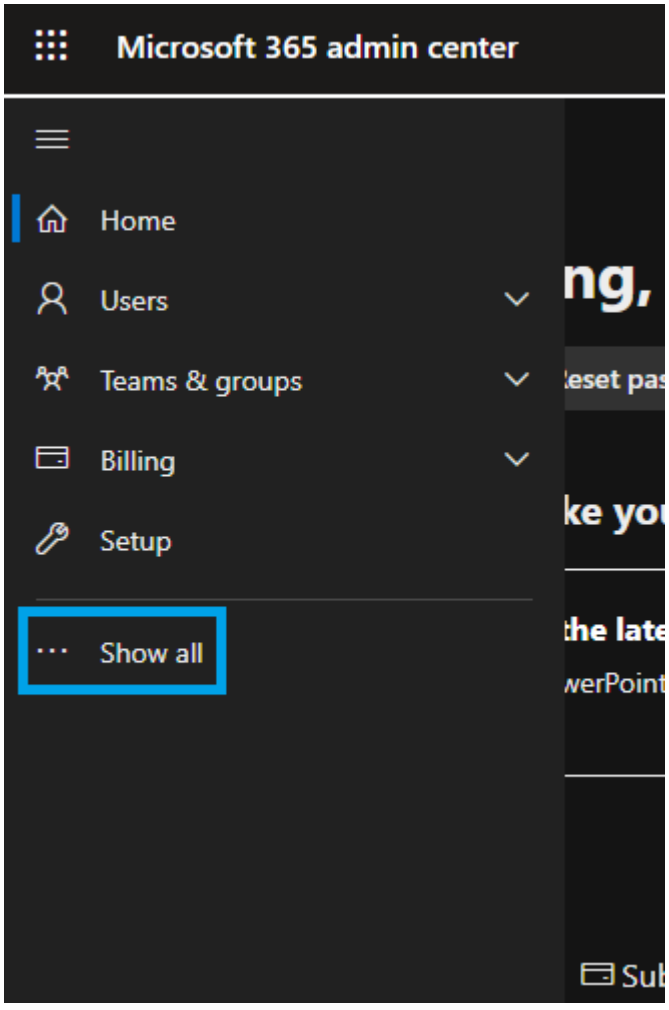
The user account required below must have `Office 365 Global Adminstrator` permissions.

- Sign in to the **Agent Management Portal** and navigate to the **Applications** tab.
- Click the purple **Choose** button in the **Office 365** card on the Applications page.
- On the Applications List for Office365 page, click the purple **Add Application** button in the top right corner.
- In the **Information** section, select the `SSO Portals` you would like to add Microsoft 365 integration to, then enter a human-readable `Description` for your reference.
- Click the **Next** button to advance to the `Parameters` section.
- In the `Username` field, enter **just the username** (do not include the UPN, such as `@domain_name`) for your administrative account for `office.com`.
- Below the `Username`, enter the `Password` associated with your Microsoft 365 administrative account.
- Last, enter the name of the `Domain` associated with your Microsoft 365 account and click the **Next** button.

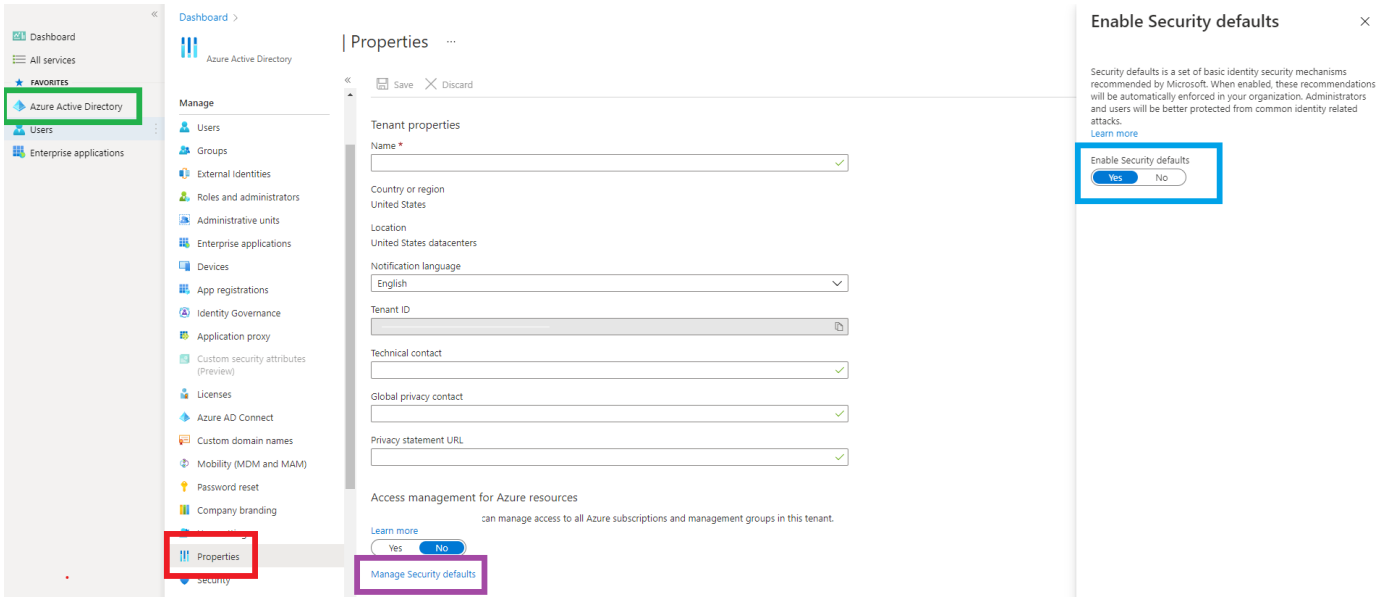
Don't close out of the Agent Management Portal yet – keep it open, and we'll return to it after some configuration on Microsoft's end.

Office 365 Admin Configuration

- Sign in to your Administrative Account on office.com.
- Once signed in, click the Applications button (the 9 dots, 3 per row, on the left side of the page) and click the **Admin** app.
- Once you are in the Microsoft 365 Admin Center, open the navigation bar on the left side and click **Show All** (shown below in blue):



- On the navigation bar, find the **Admin Centers** section and click **Azure Active Directory**.
- In the Azure Active Directory Admin Center, click **Azure Active Directory** on the left side (shown below in green).
- In the second navigation bar from the left, select **Properties** (Shown below in red).
- Locate the blue **Manage Security defaults** text at the bottom of the properties window (shown below in purple).
- Click that text and a window will expand on the right side of the screen.
- Click the **No** button under **Enable Security defaults** (shown below in blue).



Xiid IM Configuration Part 2: Electric Boogaloo

- Return to the Agent Management Portal and click the purple **Save** button after having completed the Office 365 Admin Configuration.

The Xiid Application will take a few moments to save the configurations and finish integrating your Microsoft 365 Account with Xiid's system. After it completes, you will be redirected to the Application List for Office365 and you should see a new row for your Microsoft (Office) 365 Application.

TIP

Microsoft still requires initial sign-in to *their* identity service when you first click the Office365 card in the SSO portal. After entering your credentials once for Microsoft 365, Xiid will ensure that you do not need to input credentials in subsequent use.

Google Workspace Setup

If your company uses **Google Workspace**, you can enable access via Xiid's SSO Portals.

Xiid IM Configuration

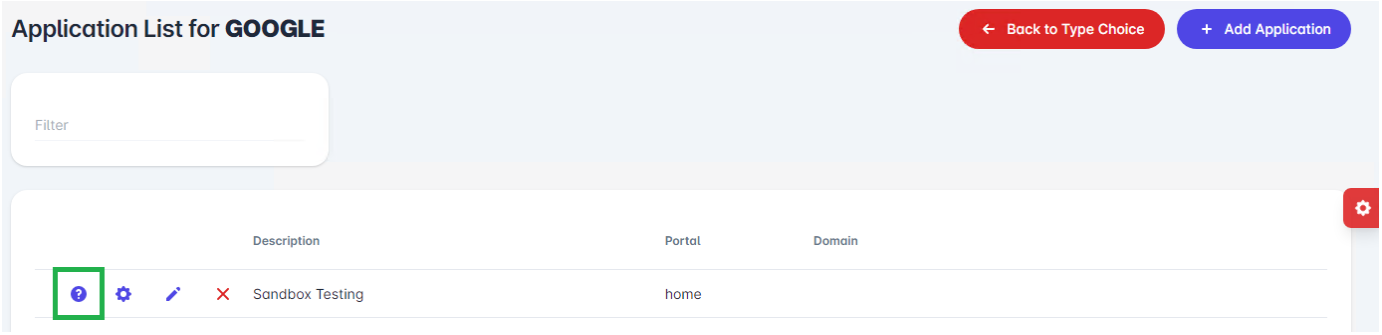
- Start by signing in to the **Xiid Agent Management Portal** and navigating to the **Applications** tab.
- On the Applications screen, click the purple **Choose** button under **GSuite**.
- On the **Application List for Google** screen, click the purple **+ Add Application** button.
- From the **Add Google Application** Information screen, select the `SSO Portal(s)` you would like to assign Google Workspace access to.
- Provide a description of the application for your personal reference, then click the **Next** button.
- For the `Parameters` section, enter the full name of your domain tied to your Google Workspace account.
- Review the information provided and click the purple **Save** button.

Don't close out of the Agent Management Portal yet – keep it open, as you'll need some of this information during configuration on Google's end.

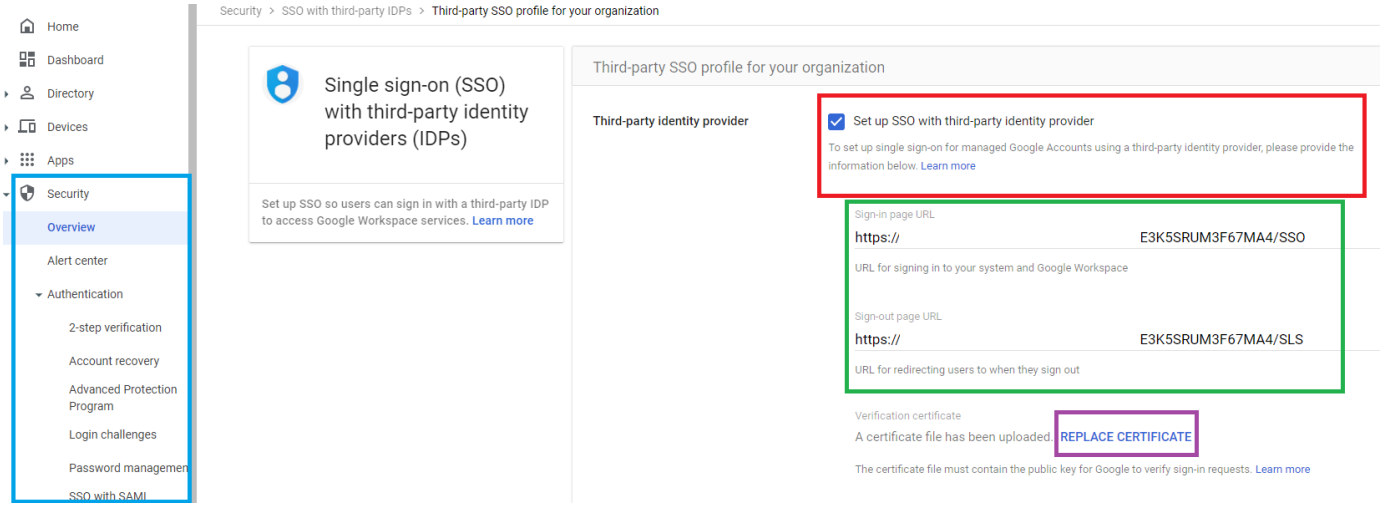
Google Workspace Configuration

The Google Workspace Configuration screen should automatically pop up after clicking the Save button.

However, to view the Configuration screen again, click the **purple question mark "?" button** next to the new Google Workspace entry in the table. (Shown in Green)



- Follow the steps on the screen by signing in to your Google Workspace account and clicking on the **Admin App** in your list of Applications.
- From the Admin App Screen, click the **Security** dropdown and select **Overview**.
- Find the setting dropdown on the right side of the Security Overview screen that is called "**Set Up Single Sign-On (SSO) With a Third Party IdP**" and click the setting.
- Click the section entitled "**SSO profile for your organization**" to edit your SSO settings.
  - You can also find the SSO configurations by selecting **Security→Authentication->SSO with Third Party IdP** (shown below in blue).
- Check the box for `Set up SSO with third-party identity provider` (shown below in red) and then click the `Copy SSO/Copy SLS` from the Xiid Agent Google Workspace Integration screen (on the **Set SSO and SLS** step) and paste them in their respective fields in the Google Workspace Admin settings (shown below in green).
- Next, download the certificate from the Xiid Agent Google Workspace Integration screen on the **Load Certificate** step, and on the Google Workspace Admin page, click the **Replace Certificate** text in blue, and upload your certificate (shown below in purple).



- Finally, click the **Save** button at the bottom of the Google Workspace Admin app to persist the changes.

Xiid IM Configuration Part 2: Electric Boogaloo

After the settings are saved in Google Workspace, go back to the Xiid Agent Integration screen, and click purple **Done** button.

Now your Google Workspace is set up and you can sign in to your Workspace using the Xiid Single Sign-On Portal(s) selected above during setup!

SAML2.0 Application Setup

Many applications support the use of SAML2.0 Authentication with an SSO Portal. For these external applications, you can use the **SAML2.0 Xiid Application** to enable access through the SSO Portals you have created.

SAML2.0 Application Configuration

- Sign to the **Xiid Agent Management Portal** and navigate to the **Applications** tab.
- On the Applications screen, click the purple **Choose** button in the **SAML2.0** card.
- On the Applications List for SAML2 screen, click the purple **+ Add Application** button in the top right.
- In the `Portal` dropdown, select the SSO Portal(s) you would like this external application to be available through.
- Provide a human `Description` for the application and then click the purple **Next** button.
- In the `Parameters` section, provide the `Domain` associated with the external application. If you do not have a domain associated with the external application, use the domain name associated with your user login.
- In the `Access Point` field, enter the initial entry point for the `Identity Provider` Initiated SAML request. The Access Point will be defined by the `Service Provider` and will vary by SPs, however it is often described as the **Service Provider Login URL**.
  - Note: The Access Point is **not** the `Assertion Consumer Service` (or ACS). The ACS is used later in the SAML authentication flow and must be provided in the SAML payloads by the Service Provider.
- After reviewing the information for accuracy, click the purple **Save** button.

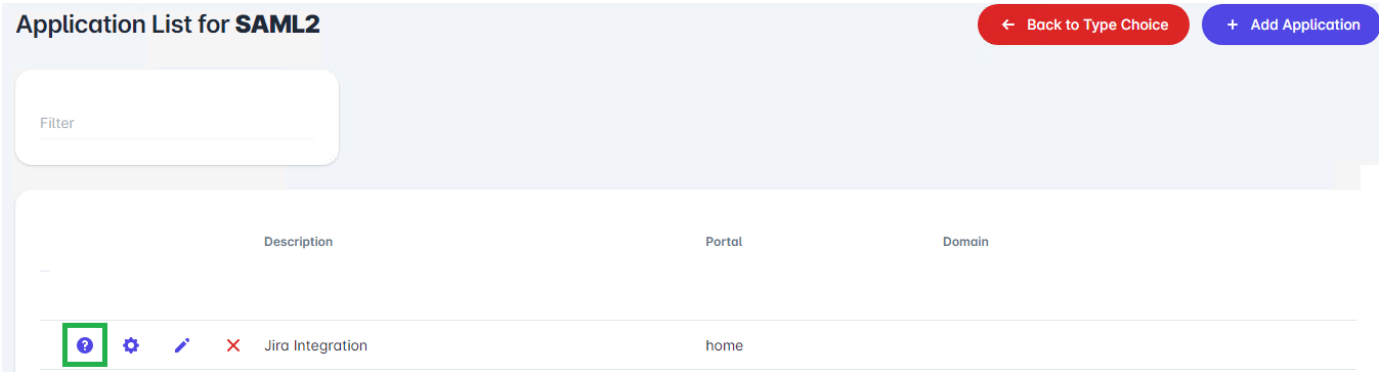
Service Provider (SP) Setup

TIP

Service Provider setup will vary by SP. Generally, you will need to enable SSO Authentication from the Administrator portal for your third-party Application. If you encounter difficulties, contact your SP for assistance.

After finishing has been enabled, you will need to provide the `SSO` and `SLS` URLs to the Service Provider so that the SP knows where to route login requests and how to handle sign in and logout requests from the application.

- To acquire the `SSO` and `SLS` URLs, navigate to the **Applications List for SAML2** screen in the Xiid Agent Management Portal, find your SAML2 Application in the table, and click the purple **Question Mark (?)** button on the left side of the row (shown below in green).



- You will next be taken to the **Help for SAML2 Application** screen, which will display your `SSO` and `SLS` URLs.
- Use the purple **Copy** buttons to copy the `SSO` and `SLS` URLs into their respective fields into your Service Provider's SSO Configurations.

TIP

Each SAML2 Application generates its own `SSO`, `SLS`, and `Public Certificate`. Do not attempt to re-use the same URLs or certificates across different Xiid Applications.

- After copying the `SSO` and `SLS` URLs into the SAML Metadata Configuration for the Service Provider, copy the `Public Certificate` from the Xiid IM Agent over to the Service Provider.
- To obtain the `Public Certificate`, click the purple **Next** button from the SSO/SLS screen, and then click the purple **Download Certificate** button.
- A `.pem` file will be downloaded to your machine. Depending on the Service Provider, you will either need to upload the whole `.pem` file or copy the contents of it into a field in your Service Provider's configuration portal.

After this SAML Trust Relationship has been established between the Service Provider and Xiid, your SAML Application will be available in the designated SSO Portal(s) for use.

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

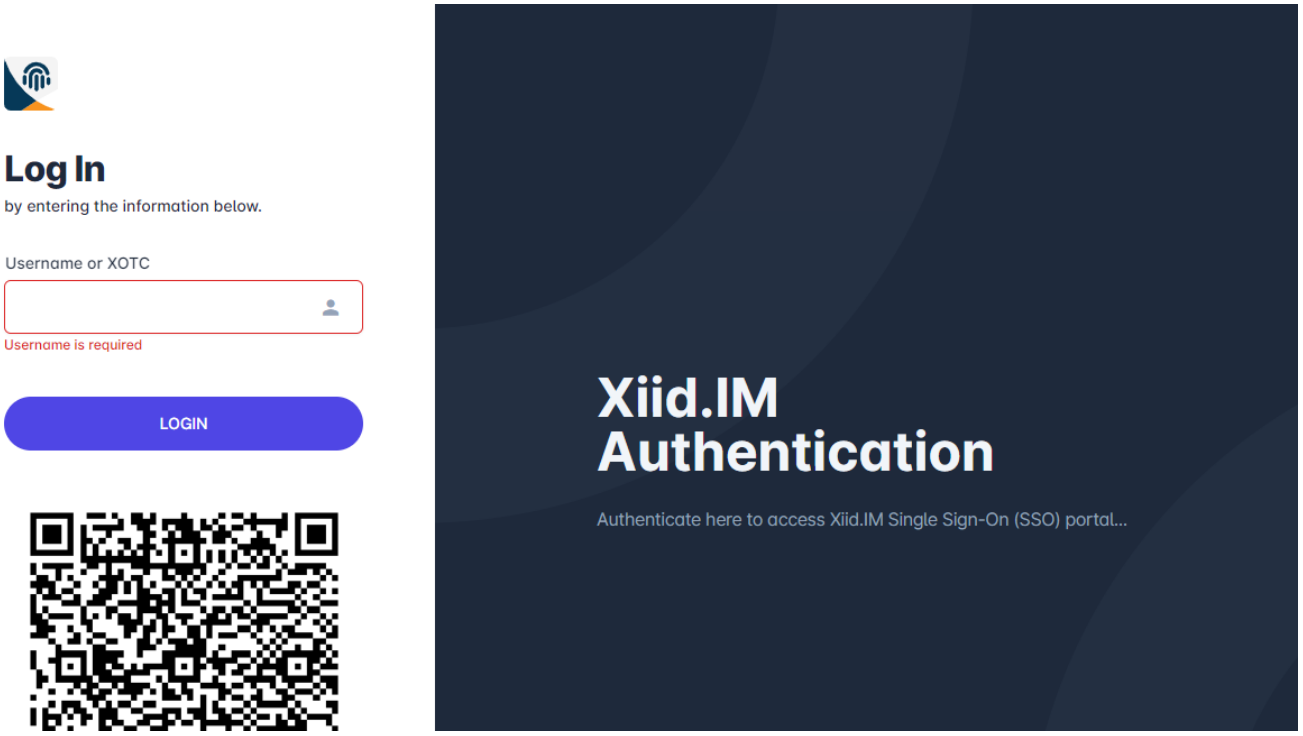
- Install the XOTC Authenticator on your iOS or Android device
- Open the application
- The first time that you open the XOTC Authenticator App, you will be asked to set a 6-digit PIN. This PIN is an added layer of security to ensure that nobody but you can access your Xiid Mobile App.
- You may also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



- 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.

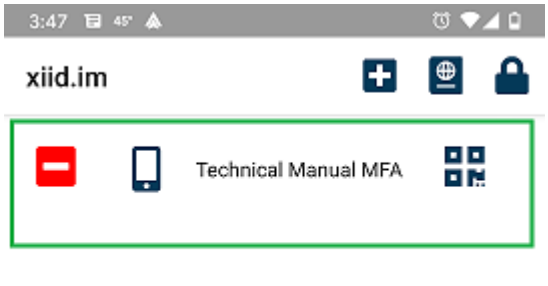
- After entering your password, you will be prompted to provide an email address. This email address is used send you a link that can be used to recover your Xiid credentials if your phone is lost, stolen, or broken.
- After entering your email address, you will receive an One-Time-Password to the email 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.

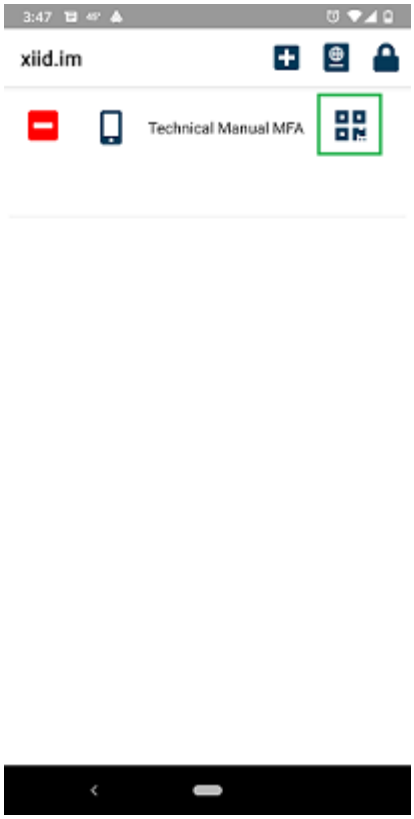
Now you're all set up to use the Xiid Single Sign-On Portal with the XOTC Authenticator!

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

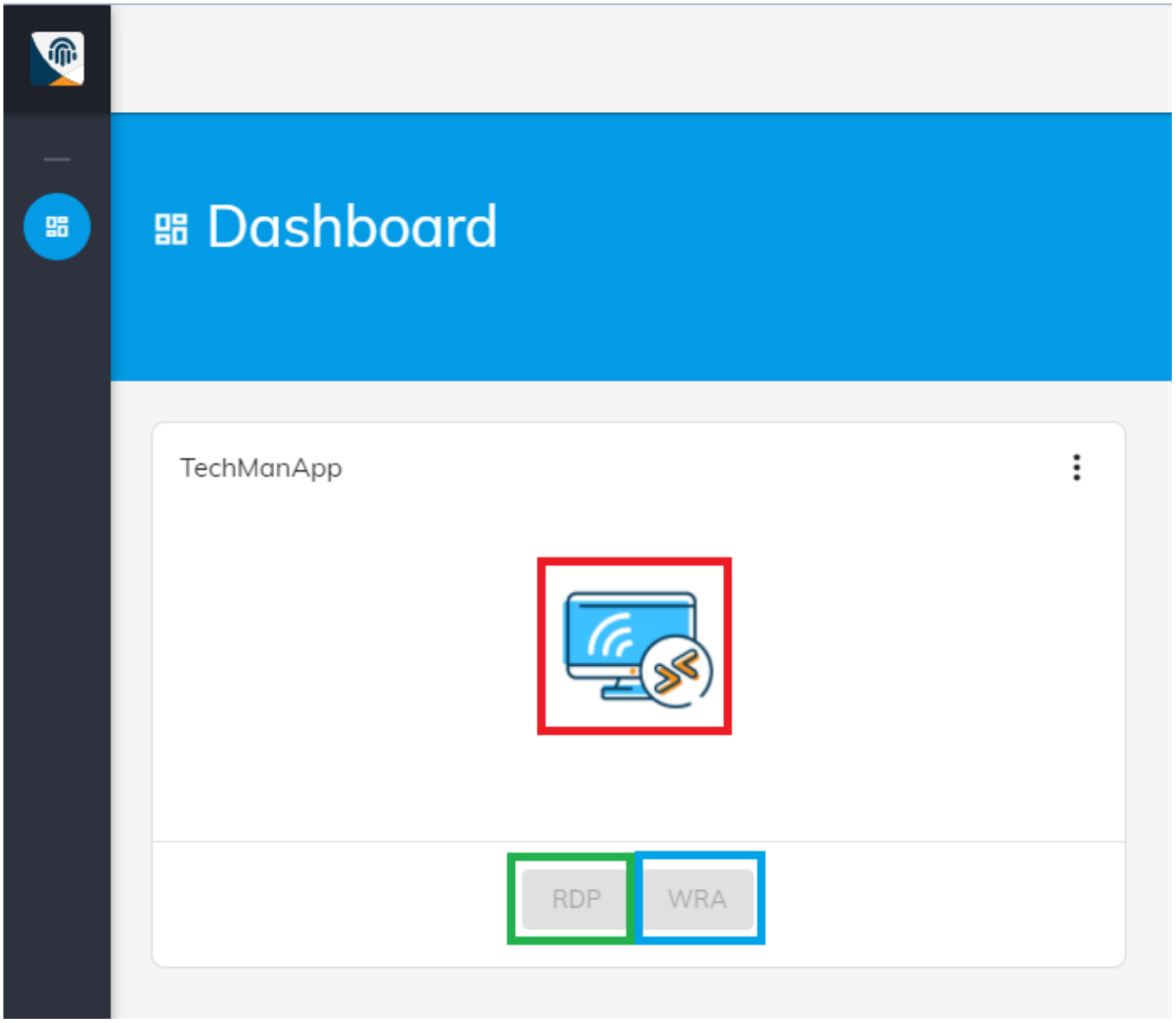
For most applications in the SSO Portal, you will only need to click the card with your desired Application and you will be automatically signed in and directed to the Third Party Application.

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**.

Virtual Trust Relationships

Overview

Xiid **Virtual Trust Relationships** provide a way to securely share resources between distinct domains.

Traditional Trust Relationships in Windows domains are lengthy, complicated, and require opening inbound ports and additional communication between the separate domains.

Virtual Trust Relationships eliminate complexity and risk by allowing a system administrator to share an SSO Portal (and specific resources within) with another domain **without making any modifications to either domain**.

Prerequisites

To set up a Virtual Trust Relationship, you must have:

- Two separate domains
- Two Xiid Management accounts
- An IM Agent deployed within each respective domain with each connected to a separate Xiid Management account (the two referenced above)

In addition, The IM Agents on both domains must use the same Request Collector.

Throughout this guide, we will use the following terminology:

Term	Definition
Owner Domain	The **source** domain that is sharing resources to another domain
Trust Domain	The **recipient** domain that resources should be shared with

Configuring Virtual Trust

Adding a Trust Relationship

- Sign in to the Agent Configuration Portal for the **Owner Domain.**
- Switch "Advanced Mode" on and click the **Trusts** tab on the left side.
- On the **Trusts** page, a list of all current Trust Relationships are shown. These indicate Trusts that the **Owner Domain** has established with other **Trust Domains**.
- Click the purple **+ Add Trust** button in the top right corner.
- On the **Add Trust** screen, provide a `Description` for the Trust Relationship. We recommend that you include what domain or group of users you are trusting and what access you are granting.
- Provide the `Trusted Email` for the **Trust Domain's** account, which is the email address used as the username during sign-in to the Management Portal for the **Trust Domain's**'s account.
- The `Trusted URL` requested is must be filled out in two sections:
  - On the left side, enter the `nickname` tied to the **Trust Domain's** account. This nickname is set during onboarding. The account nickname can also be found in the SSO URL of the **Trust Domain**. It is the first part of the URL before the Zone (see image below).
  - On the right side, enter the `Zone` tied to the **Trust Domain**. Similar to an Availability Zone in many cloud solutions, the `Zone` indicates what region the service is tied to. For most US customers, this will be `us.xiid.im`.

Here is a diagram outlining the construction of the SSO Portal URL. You can find your default SSO Portal URL on the Dashboard tab in the Management Portal.

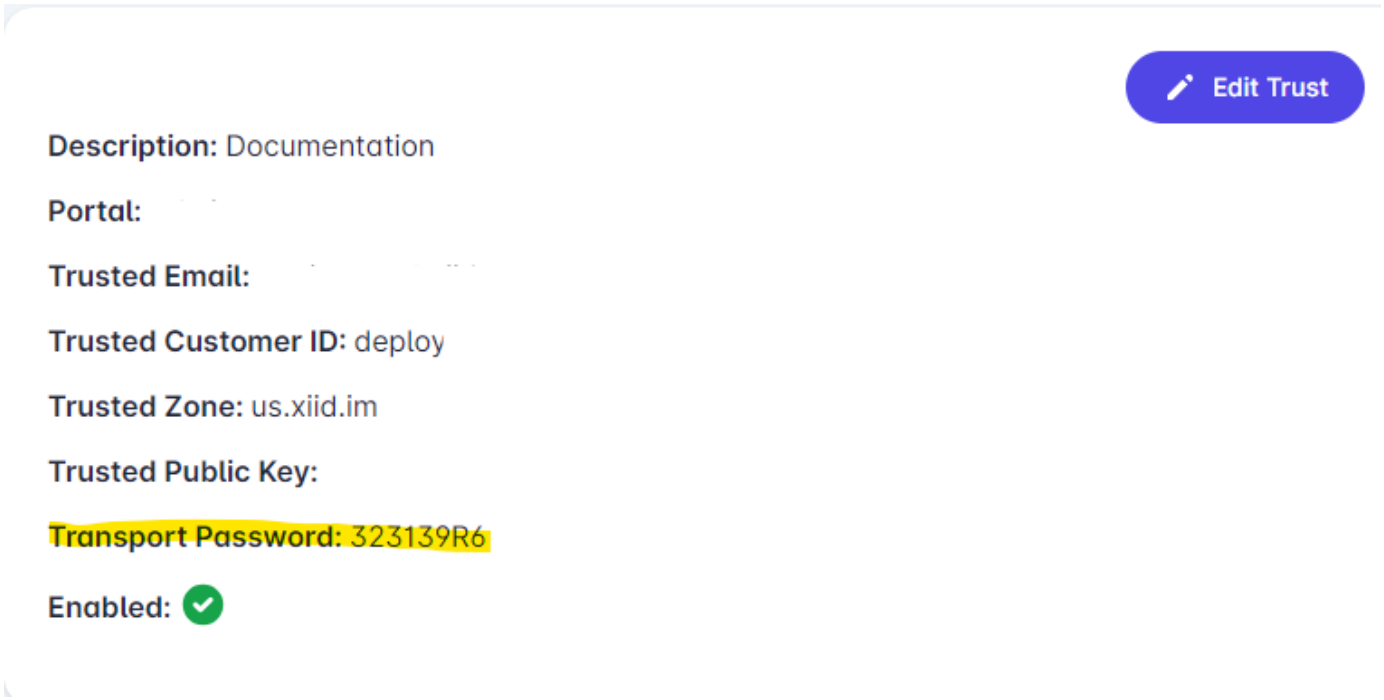
- Click the `Portal` dropdown and select the **Owner Domain** SSO Portal that you would like to share with the **Trust Domain**.
- Review the information above and click the purple **SAVE** button. You will then be taken back to the **Trusts** screen and see your new Virtual Trust shown in the table.

- To enable the Trust Relationship from the **Owner Domain** side, click the purple **+ (plus)** sign to the left of the new Trust Relationship, click the purple **Edit Trust** button, and change the `Enabled` dropdown to `Enabled` and then click the purple **Save** button.

Authorizing the Relationship

In order to allow the Trust Relationship, the System Administrator from the **Trust Domain** must also authorize the relationship in their environment.

- Click on the **Trusts** tab in the Agent Configuration Portal of the **Owner Domain**.
- Find the Trust Relationship you set up on the **Trust Domain** and click the purple **+ (plus)** sign button on the left side.
- On the **Trust Data** screen, there are two purple buttons in the top right, **Send Email** and **Copy to Clipboard**.
  - If you click the **Send Email** button, an email will be sent to the **Trusted Email** provided in the previous step while setting up the Virtual Trust Relationship. The email will contain a `Virtual Trust Code` which will be used later.
  - If you click the **Copy to Clipboard** button, the `Virtual Trust Code` will be copied directly into your clipboard.
- Back on the **Trust Domain**, sign in to the Agent Configuration Portal and click the **Applications** tab on the left side.
- Find the **Trust** application card and click the purple **Choose** button.
- From the **Trust Application List** screen, click the purple **+ Add Application** button in the top right.
- Provide a `Description` for the **Trust Application**.
  - The **Trust Application** will be usable as a card in a **Trust Domain** SSO portal that opens up the shared SSO Portal with authorized applications from the **Owner Domain** SSO Portal.
- In the `Portal` dropdown, select the SSO Portal that you would like to include the **Trust Application** card in.
- In the `Import` text field, paste the `Virtual Trust Code` provided by the **Owner Domain** in the above step.
- To fill the `Password` field, go back to the **Owner Domain**'s Agent Configuration Portal, and obtain the `Transport Password` on the **Trust Data** screen above the **Enabled** property as shown below.



- Click the **Save** button at the bottom after reviewing the information.
- From the **Trust Application List** screen, you will now see your new Virtual Trust application and its associated SSO Portal in the table.
- Click the purple **Edit** button to the left of the new Virtual Trust application.
- On the **Edit Trust Application** screen, there is a black **Confirm** button available near the bottom.
- Click the **Confirm** button and a new browser tab will open to a very long Virtual Trust URL.
  - You should the following json message: `{"msgInfo": "OK"}`. This means your Virtual Trust relationship is verified and working.

Granting Access to Virtual Trust Applications

At this point, end-users in the **Trust Domain** with relevant access may use a Virtual Trust card in their SSO portal that points to an SSO Portal of the **Owner Domain**.

If the user clicks that card, a new tab will be opened to the shared SSO Portal allowed by the **Owner Domain**.

Resources can be added for shared access by following these steps:

- Sign in to the Agent Configuration Portal in the **Owner Domain** and click the **Trusts** tab on the left side.

- Find the **Virtual Trust Relationship** you set up to the **Trust Domain** in the previous steps and click the purple **+ (plus)** button on the left.
- From the **Trust Data** screen, click the purple **+ Add Application** button in the top right.
- On the **Add Application** screen, you will see a list of the available applications from that SSO Portal.
- Check the boxes next to the Applications you would like to share with the **Trust Domain** and click the purple **Save** button on the left side.

You will be taken back to the **Trust Data** screen where you will see the Applications you selected on the right side under **Applications Enabled**.

You can click the red **X** to the left of any application to remove access to it.

Reset Secondary Authenticator

If your phone was lost, stolen, or you got a new phone for any reason and need to reset your XOTC Authenticator, follow the instructions below.

XOTC Reset Link

> **WARNING**
>
> If you've misplaced your reset email, contact your system administrator.

Find the reset email sent to your email when you first set up XOTC. The email has the subject line **"Your reset link"** and contains the following text:

```
"This is your safe Second Factor Authentication (mobile) reset link."
```

You should be able to search through any email client with either of those two pieces of information to locate your reset email.

Xiid highly recommends saving the reset link to a password vault or other secure storage mechanism for easier reference.

Click the orange button labeled **Reset your Second Factor Authentication** or follow the link listed below the button.

Reset Web Page

After following the link, you will be taken to the `reset-otp` URL associated with your secondary authentication.

The page will ask if you would like to reset your secondary authentication. Confirm that the 2FA reset is for your account specifically before proceeding.

Click the **Yes** button to initiate the reset of your secondary authentication. After receiving the thumbs up from Xiid, your secondary factor will be reset.

Re-setup Secondary Authentication

Now that your secondary authentication is reset within Xiid's system, you will need to bind a new security profile to your new phone or app.

Follow the instructions here to bind the security profile.