Technical Manual

Xiid Corporation

Contents

Introduction

Protecting the enterprise network perimeter and cloud-connected users is proving to be more difficult than ever despite the rise of Zero Trust. With its **AbsoluteZero™ Trust (AZT™)** architecture that requires **no open inbound ports** to function, Xiid eliminates all exposed attack surface at the enterprise network perimeter using its **SealedChannel™** and **Smart Hybrid Protocols (SHyPs™)** technologies. The **Xiid One-Time Code (XOTC™) Authenticator** eliminates theft of cloud-based users' credentials by delivering the Xiid SSO portal using zero-knowledge proof methods that never put usernames or password in the open. Ever. These technologies that underpin the AZT™ architecture makes malicious code and ransomware payload injection impossible.

Securing an LDAP Directory is not an easy task. To lockdown your LDAP directory service, Xiid adheres to three (3) cardinal rules:

1. No replication of the LDAP Directory - Keep complete control of your directory in your secure network.
2. Completely close off inbound external access to resources using Xiid's patented SealedChannel™. Your firewall does not need to open any inbound ports for authentication.
3. Every authentication response is digitally signed behind the SealedChannel™. No changes can be made to the response after it leaves your secure firewall.

Plus, as you'll soon see, it's easy to install and use *side-by-side with your current security solutions*!

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.

Technical Overview

This overview walks through the major components of Xiid's technology, how they interact with one another, and where they are generally located. Xiid's products consist of a variety of components that are spread throughout different areas within and outside the private network perimeter. It is helpful to understand what these components are and where they reside.

Birds-eye Overview

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

- Xiid Collectors
- Xiid SealedChannels™ and SealedTunnels™
- Xiid Agents
- XOTC Authenticators

These four components work together under the global paradigm of AbsoluteZero Trust™ (AZT™).

As the name AZT implies, each component operates in its own "silo" and communication between these components is based on the premise of no trust between them. This means that regardless of wherever any component resides (inside or outside the private network), communication is heavily encrypted, heavily vetted, and completely rejected if at all suspicious.

To explain how Xiid's technology works from a birds-eye view, let's use the analogy of a city with multiple canals meandering in and out of the city limits.

You are a person currently outside the city (with the city representing a private network), wishing to access a resource within the city.

Installing Xiid's software is like building a giant, thick stone wall around the city and sealing every gate. The only remaining ways in and out of the city are the canals, but Xiid has modified the canals, too.

To protect the city from outside threats via the canals, inbound traffic into the city is eliminated (all inbound ports are closed). No one is allowed to directly travel the canal to the city boundary and request to enter.

To secure the canals into the city, newly-installed metal gates in the canals (the **Xiid SealedChannel** and **Xiid SealedTunnel** products) make it impossible for barges or packages to directly enter the city. These gates also have specifically-shaped gaps in them, so packages with arbitrary sizes and contents (malware, etc.) physically cannot cross into the city.

Guards are stationed outside the canals' gates, and they unload and inspect the contents of the barges. These external guards are called **Xiid Collectors**.

In addition, the identity of every barge and package must be known and approved by the city before they will even be considered by the **Xiid Collector** guards. This approval process is our credential-less **XOTC Authenticator**. Furthermore, the identity includes the location (IP address) of who is making the request, so the city knows where to ultimately send the honored request.

If the **Xiid Collectors** find anything that looks extraneous, suspicious, or otherwise, that object is destroyed by tossing it into the water below.

In this case, a package containing your resource request is sent by you on a barge to the **Xiid Collectors**. After it's been inspected and approved, only the bare minimum contents of your package needed to fulfill your request are repackaged into a new shape that will fit through the specifically-shaped gaps in the metal gates at the city boundary.

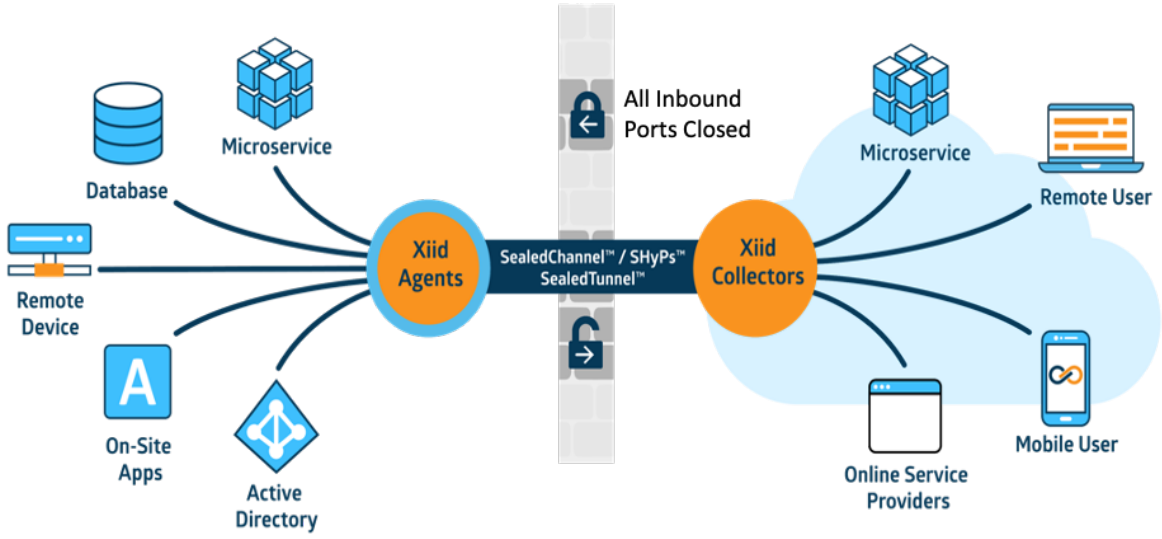
Once the (many-times encrypted) repackaging of your request reaches the city border, a group of **Xiid Agents** on the *inside* of the canal gates then use the small openings in the metal gate to grab supplies from the **Xiid Collectors** (guards), with only the specifically-shaped packages able to pass through.

If, despite all of these processes and restrictions, a supply package still looks suspicious to an **Xiid Agent**, they will reject the package and it will be dumped safely outside the city walls.

Finally, once your package makes it into the city and is approved and honored, a carrier pigeon (carrying a many-times encrypted response) flies outbound from the city and directly to you with your requested resource.

With this strategy, traffic is securely locked down and limited, so that only safe, secure supplies ever enter the city, and malicious actors and items and barred from entry. At no time is any direct inbound communication to the city permitted or possible if all ports are locked down.

Below is a high-level diagram describing this process from a more technical - and less metaphoric - perspective.



Xiid AbsoluteZero Trust™ Model

The Xiid AbsoluteZero Trust (AZT™) Model is a new cybersecurity strategy aimed at bolstering network perimeter security. At the core of the AZT paradigm is the premise that no technical component establishes any trust relationship which grants any level of access to the component's owned resources. To fit the mold of the AZT Model, Xiid utilizes the SealedChannel™ in tandem with the Smart Hybrid Protocols (SHyPs) or the SealedTunnel™ to handle all communication and authentication between network segmented resources. The SealedChannel, SealedTunnel, and SHyPs technologies are 100% proprietary and use no external, third-party library libraries.

The AZT architecture is designed to be non-invasive and seamlessly overlay with existing domain structures. You don't need to change anything about your current network and domain architecture to start using Xiid.

In fact, after installing Xiid, we provide the flexibility to further enhance your network security without causing issues for Xiid's software!

Xiid Collectors (Request Collectors)

The Xiid Request and SealedTunnel Collectors are the front-lines of Xiid's technology. Collectors are one of two components (the XOTC Authenticator being the other) that reside outside the network perimeter. Request Collectors have only one purpose: to collect requests that come in from various identity providers, convert them to SHyPs, and put them into a Queue. The Request Collectors are managed by Xiid, with built-in redundancy across regions and cloud providers, top-of-the-line security, and protections at every level from networking down to reduce the attack surface. SealedTunnel Collectors perform the same job for SealedTunnels without using SHyPs.

Xiid Collectors have no inbound network access to private domains and all the authentication data that they receive is completely anonymized for security and privacy, ensuring that even if a Collector were to be comprised, the attacker still would be unable to access private resources.

XOTC Authenticator

The Xiid One-Time-Code Authenticator, commonly referred to as 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. As of now, the XOTC Authenticator is available for Android and Apple smartphones through their respective application stores. (See Portals and Applications for more information.)

The XOTC Authenticator allows users to access their favorite external applications, files, services, and data without worrying about credential theft. The best way to secure credentials and authentication is to remove credentials from the equation altogether. The XOTC Authenticator offers the strongest security available to ensure that proper access is granted to individual's resources and **not** to malicious actors.

No usernames, no passwords, (far fewer) problems!

Xiid SealedChannel, SHyPs, and SealedTunnel

With Xiid you can (and should) close down all of your inbound ports on your network. Inbound ports aren't needed with Xiid's software and they vastly increase the attack surface of your domain for malicious actors. However, outside communication with your network resources is critical to business operations. The Xiid SealedChannel solves this problem by creating a highly encrypted and secured communication channel that does not rely on inbound communication but instead utilizes the internal network's outbound ports with efficient, consistent polling. The messages polled from within the network are stored in the Xiid Request Collector and are layered with multiple layers of strong encryption, ending with Xiid's own patented technology called Smart Hybrid Protocols.

SHyPs are Xiid's collection of communication protocols which rely on an AbsoluteZero Trust paradigm in which only a portion of the actual protocol is known by either side (hence the word "hybrid"). The Request Collector side only understand a portion of how to encrypt the incoming requests before putting them into a queue. The Xiid Agents (see below) 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 at all suspicious, the request will be immediately discarded.

Layering these two technologies together 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 uses polling a SealedTunnel Collector to function.

Xiid Agents - General

Xiid Agents handle communication via the SealedChannel or SealedTunnel. There are different types of Xiid Agents which poll for different requests from the Xiid Collectors. For example, Xiid LDAP Agents poll for authentication requests whereas RDP Agents poll for RDP session requests. Each type of Xiid Agent knows exactly what information to grab from the request collectors using Xiid's Smart Hybrid Protocols (SHyPs). The Agents than act as the liason to the underlying resource and handle the request "personally". For example, an LDAP Agent would grab an authentication request for a user, and query the Active Directory itself with credential information to determine authentication status and access. In short, Agents are the outbound-polling interop handlers for various requests to your internal network.

Below are the current Xiid Agents available for use:

LDAP Agent

LDAP Agents are deployed on your directory (or Active Directory) server or on any network-adjacent server. The LDAP Agent handles all authentication requests to your directory service, allowing you to close down all of your inbound authentication firewall ports. You can deploy multiple LDAP Agents within a single domain with Trust Relationships, and the Agents will work in tandem to handle authentication requests. An LDAP Agent can also connect to multiple directories and set up application restrictions based on your Active Directory Security Groups, for example. The LDAP Agent is the core of the Xiid.IM Product Solution.

RDP Agent

Xiid 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 have access to anywhere. You can provision RDP Agents in the Xiid Global Management Portal, and then bind the RDP Agents to your account, where they can be accessed by the LDAP Agent to configure RDP (or VDI) applications and RDP connections on the Xiid SSO Portal.

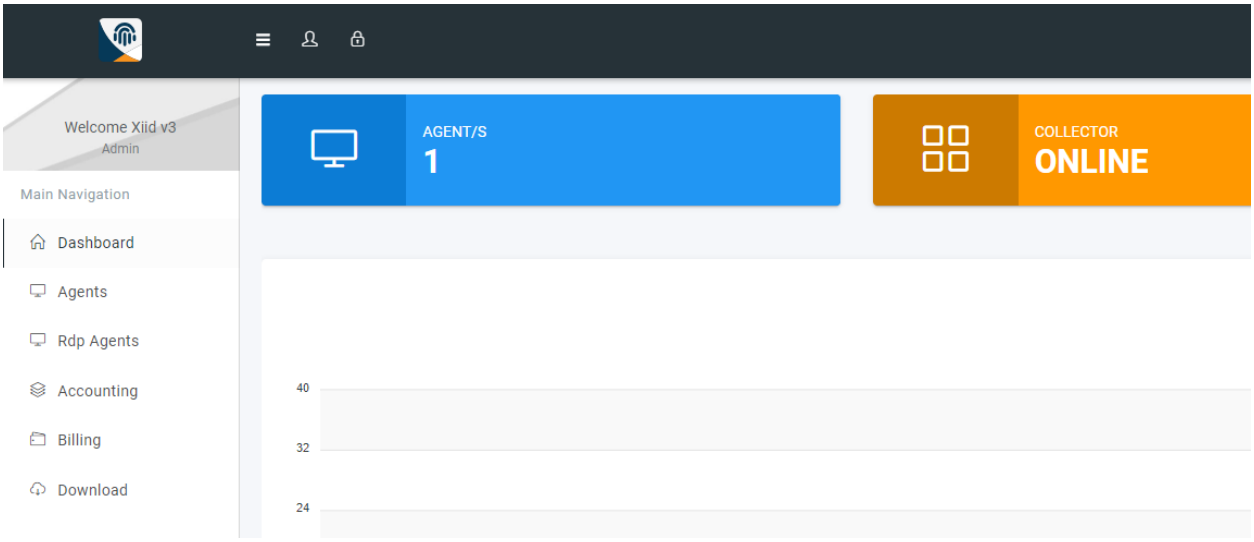
SealedTunnel (ST) Agent

Xiid's ST Agent 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 127.0.0.1 and is dramatically more secure than (and shares little relation with) traditional RDP or VPNs. Only outbound port 443 is required for it to function. # Xiid Portals and Applications #

Xiid offers multiple web portals to assist both users and system administrators. These portals include the Xiid Global Management Portal, the Xiid Agent Management Portal, and the Single Sign-On (SSO) Portal. Xiid also provides the XOTC Mobile Application for secure access to your SSO Portals. The web portals and apps are described below.

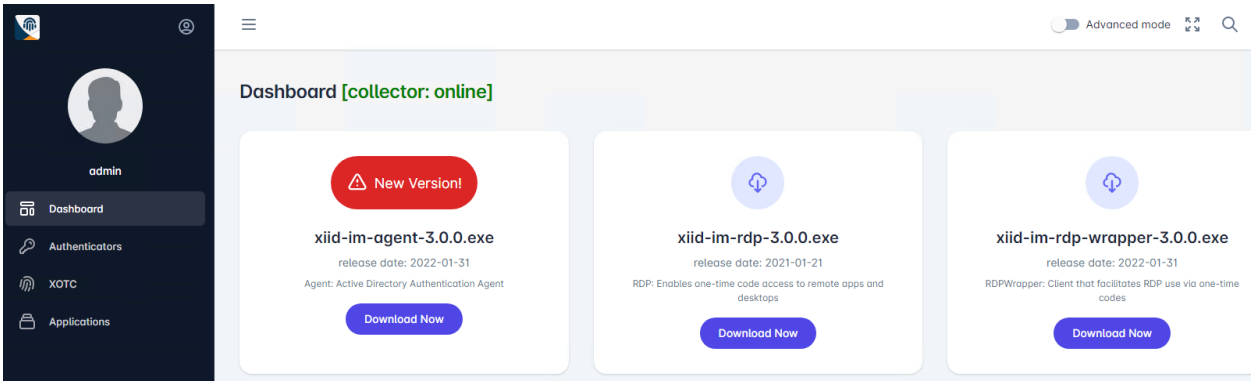
Xiid Global Management Portal

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 generally track, audit, and manage their corporate Xiid account. The Global Management Portal allows administrators to configure Xiid.IM Agents and LDAP Agents to integrate Xiid with their company directory services for authentication. The Accounts tab also lets administrators keep track of their current users and API usage.



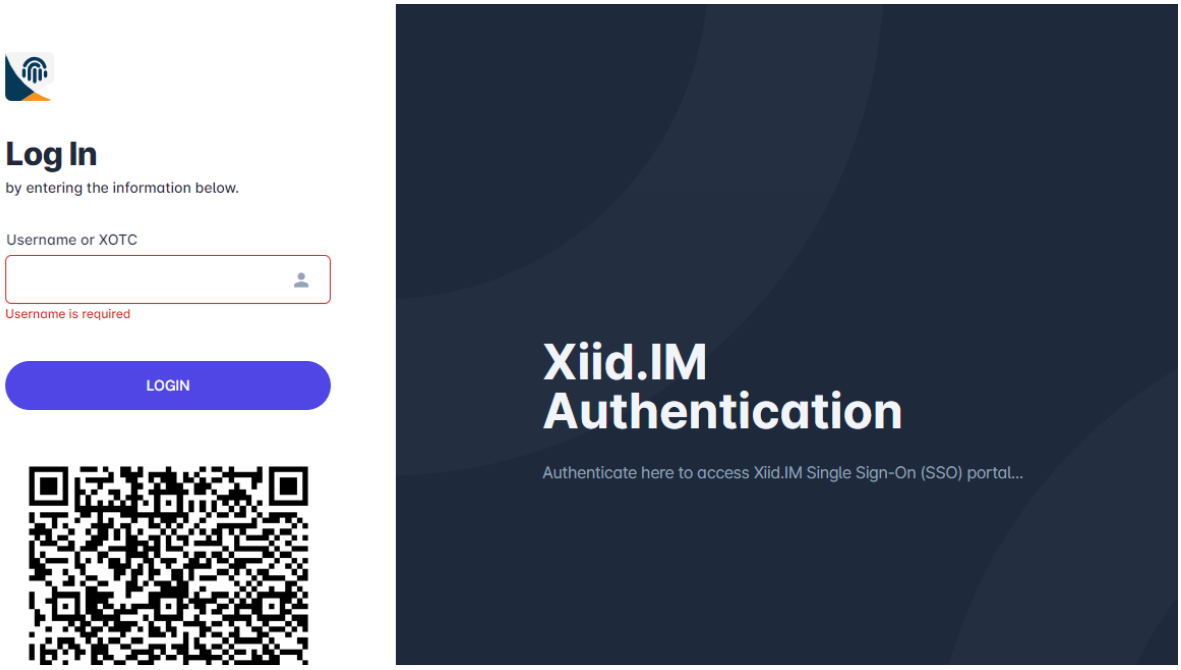
Xiid.IM Agent Management Portal

The Xiid.IM Agent Management Portal allows company system administrators to configure their applications, users, connections, authentication mechanisms, and more. The Agent Management Portal is typically used in tandem by System Administrators and Security Administrators to configure which applications are available to their users, how they can access their applications, and how Xiid should handle authentication and integration with the company's LDAP service. The Agent Management Portal is the main interface used in installing and configuring Xiid software on corporate domains.



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 need only to scan, using the Xiid Mobile App on the user's mobile smart device, the QR code from the Single Sign-On Portal, and they will be automatically logged in with access to all of their applications. Applications through the Single Sign-On Portal can be run locally or over the internet based on user preference and application location.



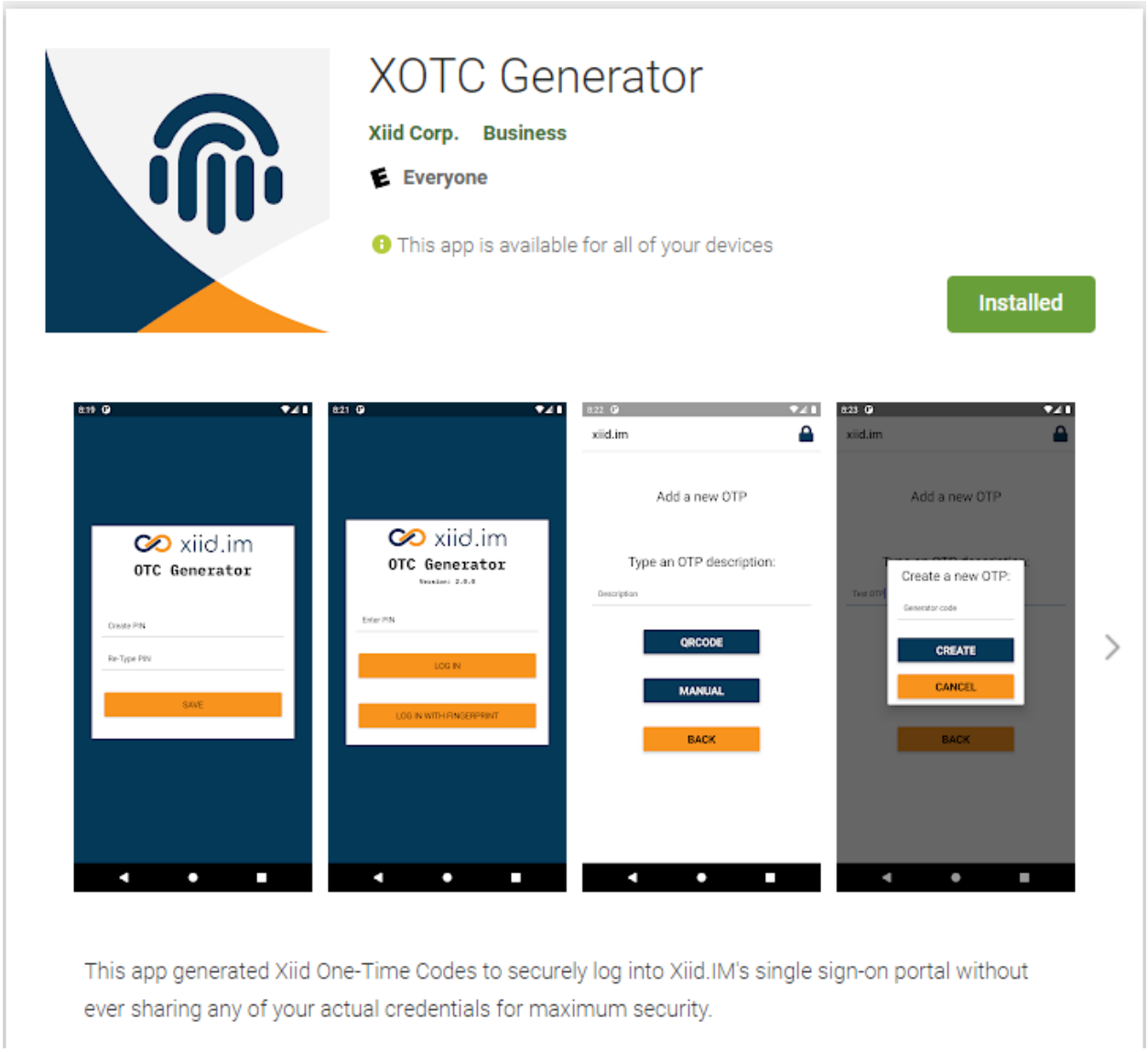
XOTC Mobile Application

The Xiid Mobile Application allows users to securely access their company's secure network through the user's mobile device, such as a smartphone, using Xiid's secure One-Time-Code (XOTC) system. Users may scan the QR Code presented at sign-in using the Xiid Mobile Application to automatically log in to the Xiid Single Sign-On Portal to access their applications. Xiid requires a user-established 6-digit pin code to access the Xiid Mobile Application on the user's device for enhanced security. Other secure methods to access the Mobile Application are allowed, such as biometrics (device-permitting).

For increased security, the Xiid Mobile Applications only support the following operating systems:

Apple Operating Systems: - iOS version 13.3 to current version

Android Operating Systems: - Android 11 - Android 12


XOTC Generator
Xiid Corp. Business
Everyone
This app is available for all of your devices
Installed
xiid.im
OTC Generator
Create PIN
Re-Type PIN
SAVE
xiid.im
OTC Generator
Enter PIN
LOG IN
LOG IN WITH FINGERPRINT
xiid.im
Add a new OTP
Type an OTP description:
Description
QRCODE
MANUAL
BACK
xiid.im
Add a new OTP
Create a new OTP:
Generator code
CREATE
CANCEL
BACK
This app generated Xiid One-Time Codes to securely log into Xiid.IM's single sign-on portal without ever sharing any of your actual credentials for maximum security.

Xiid.IM Agent Components

Xiid has created a variety of technical components for ensuring maximum security as well as creating a fluid integrated system. Each component has its own relative purpose but works in tandem with other components to build a secure user experience. Understanding these components individually will help system administrators manage and interact with the Xiid ecosystem.

Authenticators

Xiid Authenticator components *connect* Active Directory Agents to LDAP Directories. They are also used to separate SSO Portals and Applications for various 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 the SSO Portals) as well as **excluded** Security Groups (to deny access to the 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 LDAP Agent.

Firewalls

Xiid offers an additional layer of application security to ensure that unauthorized access will not be granted, and that integrated services and systems can communicate while restricting outside actors from gaining access. This added layer of security comes with Xiid Firewalls. Using Xiid's Firewall component, users can whitelist or blacklist IP addresses, allowing communications that need to happen while blocking potential risks. Users can create and use as many Xiid Firewalls as they see fit to secure their connections. Xiid Firewalls operate across the Secured Channel, meaning that authentication requests from IP addresses that are whitelisted or blacklisted will be accepted or rejected from the Agent when polling against the Request Collector. Users may still attempt to sign in from a blacklisted IP address, but the authentication request will be ignored by Xiid.

Translators

Translators are a component within the Xiid Active Directory Agent which allows 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 Active 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.

Secondary Authentication

Xiid supports 2-Factor Authentication for accessing the Single Sign-On Portal. You can choose from Legacy Multi-Factor Authentication (a one-time-password system), which is not recommended as it provides less security, but is still supported. You can also create XOTC Authenticators to bind to your SSO Portals. When the XOTC Authenticator is bound to an SSO Portal, a code will generate and rotate on the SSO Portal for use by the XOTC Mobile App users on your domain.

SSO Portals

Xiid allows system administrators to set up different SSO Portals for different groups of users. When you create a new SSO Portal, you will provide an ID which will be used in the SSO Portal's URL. It is recommended that system administrators set up multiple SSO Portals for 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 are configurable components that allow System Administrators to integrate various external applications into your SSO Portals. For each application that you would like to provide access to, you would create an Application Component within the Xiid.IM Agent defining how to integrate with the external application. Xiid currently supports 5 types of applications in the Xiid.IM Agent: RDP, RDP Apps (VDI), Office 365, Google Workspace, and any external application that supports SAML2.0 authentication. When you configure Xiid Applications, you can choose which SSO Portal the application will be assigned to, as well as some additional parameters to make your apps work exactly how you would like.

Quickstart Guide Introduction

This section will walk users through setting up and configuring Xiid's technology. By the end of this guide, you will have:

- Set up a Sandbox Domain for testing Xiid's Software. (Optional)
- Installed and configured the Xiid.IM Agent over LDAP
- Created an Xiid SSO-Vended RDP Application (Optional)
- Set up a remote machine for RDP access through Xiid's secure technology (Optional)
- Set up a Google Workspace Application in your SSO Portal (Optional)
- Set up an Office 365 Application in your SSO Portal (Optional)
- Set up a SAML2.0 Application in your SSO Portal (Optional)
- Enabled XOTC Authentication for Single Sign-On Users

Below is a flowchart detailing the *minimum* configuration steps necessary to install Xiid's software on your domain.

Note: You can click any of the squares to jump to the corresponding step in the documentation.

Xiid Account Onboarding

To start integrating your Identity and Access Management system with Xiid, you must first create an account with Xiid through the onboarding portal here: https://onboardv3.xiid.com/.

Follow the steps and fill out the information to create an Xiid Account. After clicking the **Sign Up** button, you will receive an email with additional instructions to verify your account, including a verification email for your email address and an OTP verification for your provided phone number. Please keep in mind that the SMS code has a 3600 second timeout, so it is recommended to finish account onboarding all at once.

After your account has been verified, you will need to provide a short name for your Xiid Account. This name is used in the DNS Record created for your Single Sign-On (SSO) Portal.

For example, if your short name is "xiidtechnology", the DNS record for your Single Sign-On Portal would be https://xiidtechnology.us.xiid.im/ After finishing these steps, you will receive an additional email from Xiid with a link to the management portal (https://managev3.xiid.com/), as well as your login instructions.

Xiid.IM Agent Setup

Xiid Agent Management

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

Start by signing into the Xiid Management Portal (https://managev3.xiid.com/) and navigating to the **Agents** tab on the left side.

The purpose of this Agent is to integrate with your LDAP service and add a layer of security to your authentication.

Click the blue **New Agent** button in the top left of the **Agents** screen to start creating your first 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 Xiid Agent with the corresponding LDAP Service the Agent will secure.

After setting the friendly name, ensure that the "Enabled" setting is set to "Enabled" and then click the green **Save** button in the top right of the screen.

You now have an Xiid Agent ready to integrate with your LDAP Service!

Active Directory Agent Setup

Now that we have an Xiid Agent set up in the Xiid Management Portal, we are ready to install the Agent on our domain controller that is running Active Directory.

Let's start by logging into the Xiid Management Portal and navigating to the **Download** tab and then download the Active Directory Authentication Agent (Blue Icon).

Transfer the Active Directory Authentication Agent to your domain controller using FTP. Alternatively, if your domain controller has external internet access, you can sign in to the Management Portal directly on your domain controller and download the executable there.

Now that the Active Directory Authentication Agent installer is available on your domain controller, run the installer as an administrator and move through the prompts.

After the installation completes, a command prompt will appear and will prompt you for your Agent ID (referred to as the Agent Config in the prompt).

To retrieve your Agent ID, navigate to the Xiid Management Portal and select the **Agents** tab. Locate the Xiid Agent created in the last section, and copy the value listed in the **ID** column.

Paste the Xiid Agent ID into the command prompt and hit Enter.

After entering the Xiid Agent ID, you will be prompted for an Administrator Username in the command prompt.

Enter the name for your Admin Username (i.e. admin) and then hit Enter again.

Last, you will be prompted for a password for the Administrator account. Enter the password and the command prompt will close.

Now your Active Directory Agent is set up and registered with your Xiid Account's Agent!

Xiid.IM Agent Configuration

Now that we have the Xiid Agent securely running on our domain controller, we're ready to configure the details of the Agent.

Authenticator Setup

The first step is to set up an Authenticator, which will instruct the Agent on how to communicate with your LDAP directory.

Start by opening the Xiid Agent Management Portal by clicking the Browser Icon labeled **Manage Xiid.IM Agent** on your desktop.

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 it's corresponding user groups, domain mapping and Active Directory Authentication 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* 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 on this service user.

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

Hit 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.

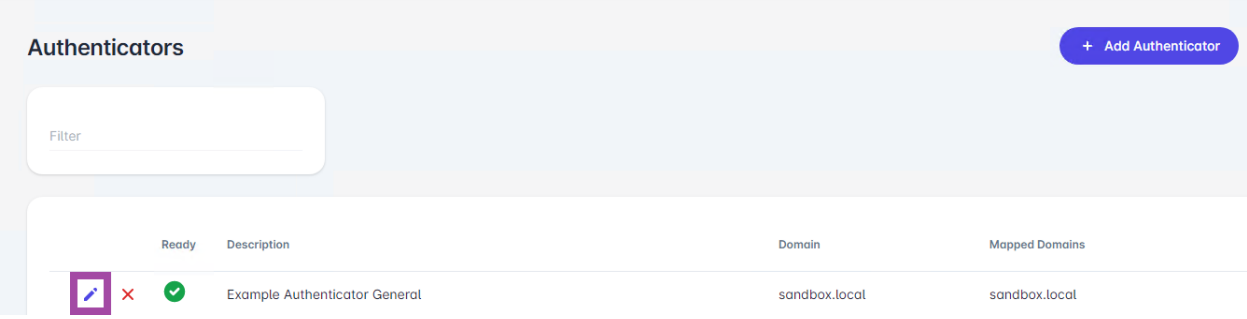
In the Authenticators table, you should now see a row for your newly created Authenticator.

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

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

The first thing you will need to do is enable **Advanced Mode** by click the switch next to **Advanced Mode** in the top right corner.

Click the **Pencil Button** on the left side of the new row of your Authenticator to edit the settings for your Authenticator. (shown below in **purple**)



With **Advanced Mode** enabled, you will see two additional fields in the Authenticator section 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 with using a **comma (“,”)**.

Note: Windows default Security Groups are NOT considered in the Group Include/Exclude filters. It must be a *user-defined* Security Group.

Firewalls

[OPTIONAL]

Firewalls offer an additional layer of Application Security to filter unwanted IP addresses or restrict subnet access to your SSO portals.

If your Agent Management Portal does not show a Firewall tab in the left hand navigation menu, follow this faq for help on enabling advanced mode.

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 Address you wish to allow or block.

Last, 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 White/Blacklists, you can group them all under a single tag to include in your SSO Portals.

Click the purple **Save** button to wrap up creating your Firewall.

Translator Setup

[OPTIONAL]

We’ve now defined how to communicate with our LDAP service, however there may be a problem with our external applications. Some of them may ask for an email address to sign in as opposed to your domain credentials.

We can solve this problem seamlessly using Xiid Translators.

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: - **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 (inbound requests, generally from the SSO Portal).

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.

Last, you can enter any Tags you would like to use to group this Translator with other Translators.

Click the purple **Save** button to finish creating your Translator.

XOTC Component Setup

[OPTIONAL]

Start by signing into 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 that helps you associate which user groups and rules this authentication standard will enforce.

Last, choose a duration of time with which the One-Time-Code will be valid for. Xiid generally recommends a 1-minute interval to give users a bit of breathing room while signing in.

Click the purple **Save** button to finish.

Now that we have our XOTC Authentication mechanism set up, we need to enforce the 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 authentication mechanism listed in the table.

Select the XOTC component and click **Next** until you reach the end and save the changes.

Now your SSO Portal will enforce XOTC Authentication for all of your users!

SSO Portal Setup

[OPTIONAL]

Xiid provides the ability to set up multiple SSO Portals for different user groups. If you have an IT organization or an Engineering organization that may need access to special applications or resources, you can separate access using different SSO Portals.

To start, sign into 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 (though 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. The **ID** will define the full URL path of the SSO Portal. For instance, the default SSO Portal created by Xiid for you has the ID of **home**, so when you navigate to the SSO Portal, you will see a URL path similar to: https://exampleportal.us.xiid.im/home which has the word **home** in the URL. If you used **engineering** as the ID, your new SSO Portal URL would be: https://exampleportal.us.xiid.im/engineering

After providing an ID for the Portal, enter a **Description** that helps you understand the purpose of this SSO Portal in conjunction with the users it will serve.

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/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 do not need to select a secondary authentication method, however it is strongly recommended.

Last, click the purple **Save Portal** button in the bottom right.

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 is fully integrated with LDAP, we can create an Xiid Application. The Xiid Application will act as an umbrella for all third-party applications that we want to integrate with Xiid's Single Sign-On Portal.

Integrating various external applications is more in-depth and the applications to integrate will depend on your needs.

Follow these setup guide sections to integrate different external applications into your SSO Portals:

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

Remote Desktop and VDI Setup

Once your Single-Sign On Portals are set up, you can add External Applications for use within the SSO Portal for specific users.

This section will walk through setting up a Remote Desktop Application to use through the Single Sign-On Portal.

RDP Agent Component Creation

To start out, 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.

RDP Agent Setup

With our new RDP Agent Component created, we're ready to configure the RDP instance (the computer we are Remoting into) with Xiid's technology.

Sign into 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.

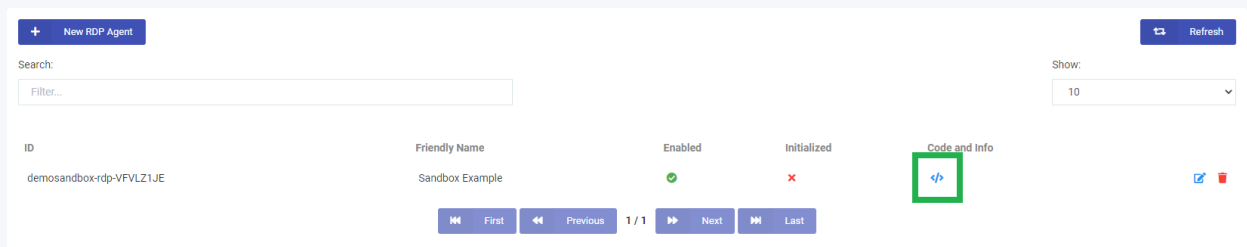
Log into the RDP instance and FTP the RDP Agent Installer to the RDP instance. Alternatively, if your RDP instance has external internet access, you can download the RDP Agent Installer directly on your RDP instance.

Run the RDP Agent Installer executable on your RDP instance and move through the prompts.

After the installation completes, a command prompt will open and ask for your RDP Agent Code.

To get the RDP Agent Code, sign in to the Xiid Global Management Portal and navigate to the **RDP Agents** tab.

Locate the RDP Agent row in the RDP Agents table and click the blue </> icon in the **Code and Info** column. (Shown below in green)



A window will pop up with your Activation Code shown. 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 copy the code elsewhere to propagate over to your RDP instance.

Now go back to your RDP Instance and paste the Activation Code in the command prompt and hit Enter.

You should see the command prompt indicate the installation was successful and close.

Your RDP Instance is now running the Xiid RDP Agent for secure RDP connections.

Note: The RDP Agent *must* register itself with the Xiid.IM Active Directory Agent. If you set up an RDP Agent *prior* to setting up and configuring your Xiid.IM Active Directory Agent, the RDP Agent will not be available in the RDP Agents Tab in the Agent Management Portal. You will need to restart the RDP Agent Service on the RDP instance *after* the Xiid.IM Active Directory Agent is set up and configured to finish the registration.

Xiid RDP Application Setup

Now that the RDP Agent is configured and bound in the Global Managament Portal, we can add an RDP Application to directly RDP into the machine.

Start by signing into 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 entry in the "Status" column should say **ready**.

After confirming that your Active Directory 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 which SSO portal you would like to assign the RDP Connection to in the **Portal** dropdown.

In the RDP Agent dropdown, select the RDP Agent we previously created.

For the **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 into** the SSO Portal will be the used.

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. So if the RDP machine is assigned a new IP Address it will be automatically used in the SSO portal.

Last, 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 App (VDI) Application Setup

Start by confirming that the RDP Agent is available to your Active Directory Agent by signing into the Xiid Agent Management Portal.

Navigate to the **RDP Agents** tab and confirm that your RDP Agent is listed in the RDP Agents table.

Next, navigate to the Applications tab and 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 an SSO Portal to assign the RDP App Application in the **Portal** dropdown.

Next, in the **RDP Agent** dropdown, select the RDP Agent that was confirmed in the RDP Agents tab.

For the **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 into** the SSO Portal will be the used.

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. So if the RDP machine is assigned a new IP Address it will be automatically used in the SSO portal.

Provide a description that helps you remember what application this is and who it is for.

In the **Application Path** field, provide the full program 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`

RDP Wrapper Setup

Now that the RDP Agent is running on the computer we would like to remote to, we need to set up the client computer to integrate the RDP connection with Xiid.

Start by signing into the Xiid Global Management Portal and navigating to the **Download** tab.

Click the Download button on the dark green icon for the RDP Wrapper installation executable.

Run the RDP Wrapper Installer on every machine that you wish to *RDP from*.

No other installation is necessary for the RDP Wrapper.

At this point, users can sign in to the Xiid Single Sign-On portal, find the RDP Application, click the **WRA** button and remote into the machine safely and securely.

Office 365 Setup

If your company is using Office 365, you can configure the Xiid SSO Portal to integrate with Office 365, providing secure access to emails and applications from anywhere, anytime.

Please consult the Office 365 Edition FAQ to ensure that you have an edition of **Microsoft 365** that supports SSO Portal integration.

Xiid.IM Active Directory Agent Configuration

To start out, you will need to configure the Active Directory Agent with your Office 365 information.

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.

On the **Information** section, select the **SSO Portal** you would like to add Office 365 integration to, then enter a **Description** for the Office 365 Application that helps you associate the Office 365 applications to the portal and users that will use it.

Click the **Next** button to advance to the **Parameters** section.

In the **Username** field, enter *just the username* (not the UPN, no @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.

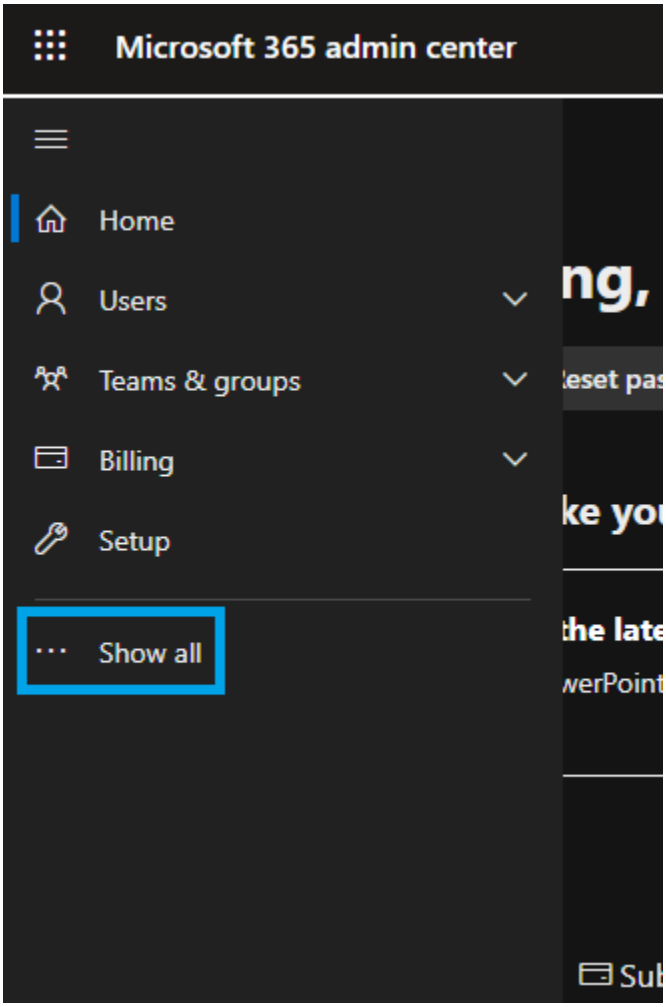
The last 4 sections of the Office Application setup will require access to your Office 365 Administrator Account.

Office 365 Admin Configuration

Start by signing 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)



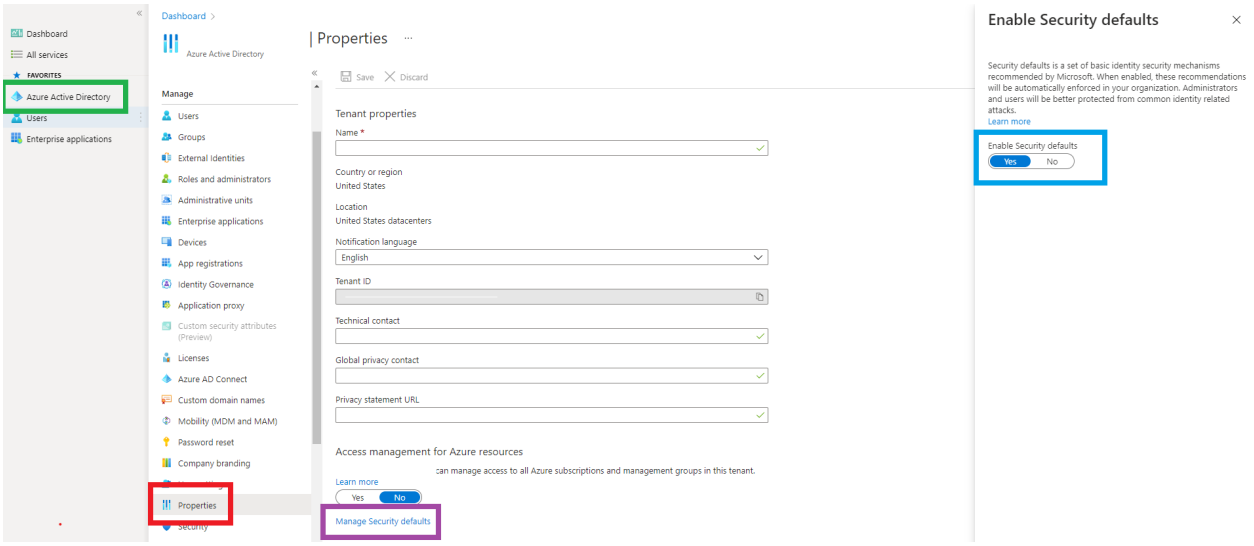
On the navigation bar, find the **Admin Centers** section and click **Azure Active Directory**.

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)



Back in the Agent Management Portal, remember to click the purple **Save** button after disabling Microsoft Security Defaults.

The Xiid Application will take a few moments to save the configurations and finish integrating your Microsoft 365 Account with Xiid's system.

Last, you will be moved back to the Application List for Office365 and you will see a new row for your Office 365 Application.

Google Workspace Setup

As an optional step, you may set up integration with Google Workspaces for your Single Sign-On Portals. This will allow your employees to log in to their Workspace using Xiid's secure authentication mechanisms. If your company is using Google Workspace, follow these steps below to configure your Google Workspace Integration with Xiid.

Xiid.IM GSuite Application Setup

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 you would like to assign Google Workspace access to.

Provide a description of the application for your personal reference, then click the **Next** button.

On the Parameters section, enter the full name of your domain tied to your Google Workspace account.

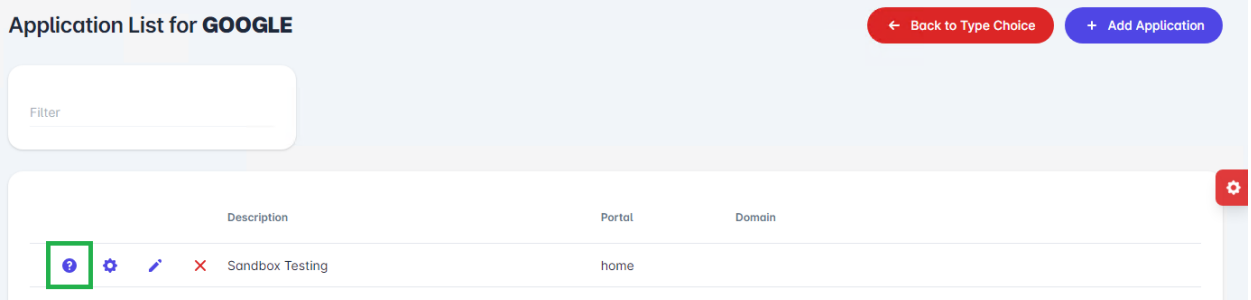
Review the information provided and click the purple **Save** button.

Workspace Integration Configuration

After your Google Application is set up, you need to finish configuring your Google Workspace integration with Xiid.

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 into 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** (the **Settings** option shown on the Xiid Agent Integration window is not available on newer versions of Google Workspace).

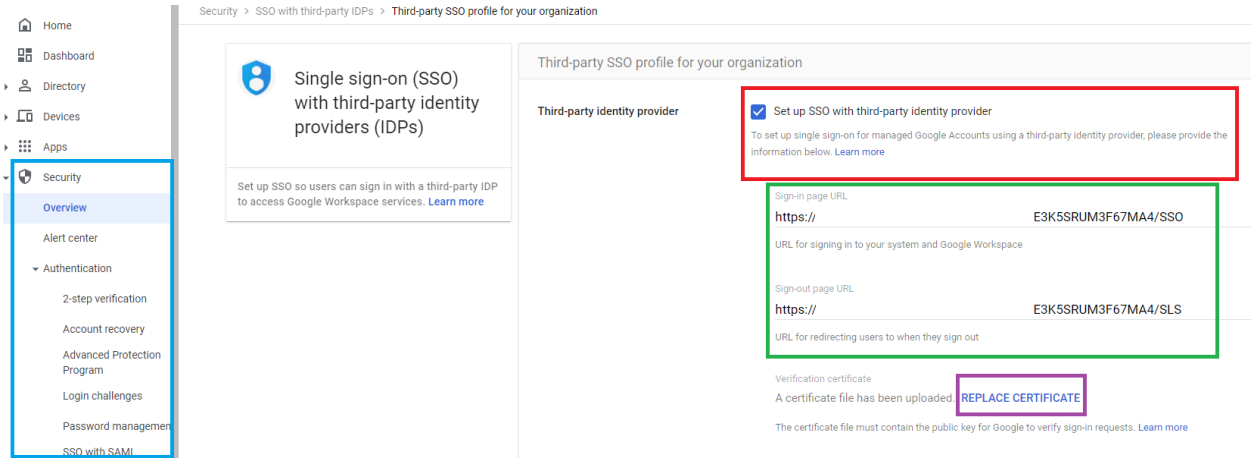
Find the setting dropdown on the right side of the Security Overview screen that is called **"Set Up Single Sign-On (SSO) With a Third Party IdP"** and click the setting.

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 Integration screen on the **Load Certificate** step, and then go to the Google Workspace Admin app, click the **Replace Certificate** text in blue, and then upload your certificate (shown below in purple).



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

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 directly into your workspace using the Xiid Single Sign-On Portal 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 integrate into any of the SSO Portals you have created on your Xiid.IM Agent. Follow the steps below to integrate any pure SAML2.0 supported applications into your SSO Portals.

Xiid.IM SAML2.0 Application 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 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 you would like enable access to this external application.

Provide a **Description** for the application and then click the purple **Next** button.

In the Parameters section, provide the **Domain** associated to the external application. If you do not have a domain associated with the external application, use the domain name associated with your user login.

For 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.

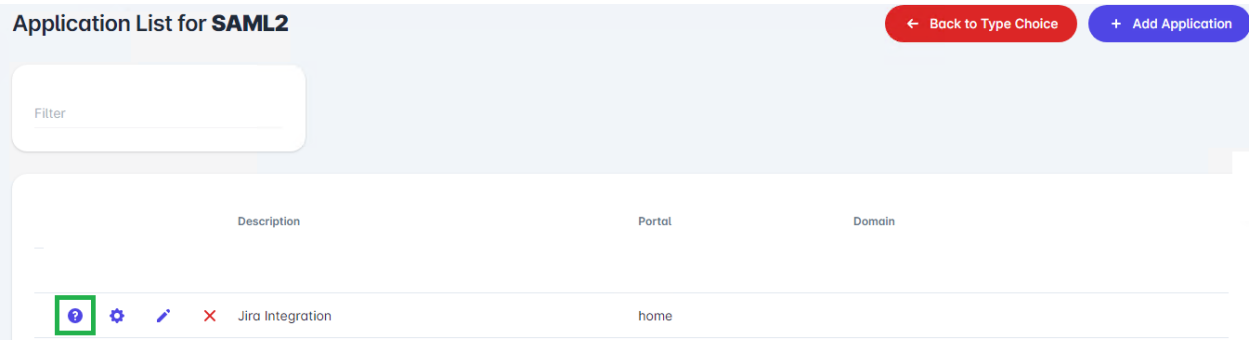
After reviewing the information, click the purple **Save** button to finish setting up the SAML2 Application Configurations for the Xiid.IM Agent.

Service Provider Setup

The Service Provider Setup will vary by each SP. In a general sense, you need to enable SSO Authentication from the Administrator portal for your third-party Application.

After SSO Sign-In 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, handle the sign-in redirects, and handle logout 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)



After clicking the Question Mark button, you will 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* SSO Configurations.

Note: Each SAML2 Application generates its own SSO, SLS and public certificate. Do not attempt to re-use the same URLs or certificates across Xiid Applications or they will not work.

After copying the SSO and SLS URLs into the SAML Metadata Configuration for the *Service Provider*, the last step is to copy the public certificate from the Xiid.IM Agent over to the Service Provider.

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 the certificate and paste it into the field in your Service Provider's configuration portal.

After the *SAML Trust Relationship* has been established between the Service Provider and the Identity Provider, your SAML Application will be available in the designated SSO Portal for use. # Support #

For more information on Xiid Corporation, Xiid's Technology, or additional support, please visit https://www.xiid.com

If you require additional technical support from Xiid, please reach out to technicalsupport@xiid.com.