Operations Manual

Xiid Corporation

Contents

Introduction to Xiid

Who is Xiid?

Xiid Corporation is a company dedicated to security. Our vision is to redesign technology with a focus on security. Cybersecurity threats are more and more ubiquitous and the complexity and maturity of cyber-attacks continues to grow.

Rather than continuing the cat-and-mouse chase between bad actors and technological security, Xiid intends to break the cycle by rethinking how software and technology works, how it interacts within its broader domain and ecosystem, and how each user identifies themselves and uses technology.

By redesigning security along these different facets, Xiid has created a robust and highly secure environment such that people at every level of business can access and use software and systems with the peace of mind and confidence that they are safe and secure.

What does Xiid do?

Xiid has developed world-class security technology to lock down and secure your private networks, giving you the peace of mind that your resources are secured behind closed firewalls, with access only through Xiid's patented SealedChannel™. Xiid offers a rich ecosystem of software solutions to accomplish these goals while providing the customization necessary to cater to different company's security needs.

Below are a few prominent features of Xiid's security technology:

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

How To Use This Manual

This manual is broken up into two major sections – System Overview and Standard Operating Procedures.

The System Overview section provides in-depth descriptions of Xiid's software components and how they relate and operate within Xiid's ecosystem. If you are looking to strengthen your understanding of Xiid's software to enhance your security configurations, the System Overview section is a good place to start.

The System Overview section is split based on both the high-level software and the low-level configurable components.

The Standard Operating Procedures section defines common scenarios while working with Xiid's Software and steps on how to best approach those scenarios utilizing Xiid's Best Security Practices. The Standard Operating Procedures section is split into subsections based on the Xiid Components that they apply to.

If you intend to make a change to your Xiid Configurations, it may be helpful to review the Standard Operating Procedures related to that component to understand the proper steps to take and the "pit-falls" to look out for when modifying these configurations.

Not Included In This Manual

The Operations Manual does not include installation instructions or Single Sign-On onboarding steps. If you need additional resources or information, including installation instructions and guides, please visit the Xiid Documentation website at https://docs.xiid.com.

Operations System Overview

Request Collectors

What is a Request Collector?

Xiid Request Collectors are the frontlines of the Xiid Security System. The Request Collector **collects** all of the authentication requests that come in from various external applications, such as Office 365, (or internal authentication requests such as XOTC codes) and put 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**.

Where does a Collector reside?

There are Xiid-vended Collectors which are securely managed on **Xiid's infrastructure**, distributed across multiple regions and cloud providers. You can also deploy your own Collector as well within your own private network, however this only permissible for highly specialized use-cases. The Request Collector should **never** be in the same network as your directory service. In fact, we recommend that your directory service be **segmented** and **isolated** to its own subnetwork (see Agents below).

Why use a Request Collector?

The Xiid Request Collector is the **frontline defense** against threat actors. The Xiid Request Collector is the only component within Xiid's software that allows external communication for authentication requests. Request Collectors are purpose-built to be **highly-optimized** (handling hundreds of thousands of requests per second) and **highly secure** across multiple levels. The Request Collector only has inbound port 443 open for HTTPS communication, the code that runs the Request Collector Service is compiled to byte-code and uses no third-party libraries (eliminating buffer overflow and injection attacks), and the data from requests is not stored on disk, while all data flowing through the Request Collector is encrypted (elminating MITM attacks and reconnaissance).

How does a Collector work?

The Xiid Collector is effectively a **queue** that listens for inbound authentication requests, packages the requests into Xiid's patented **Smart-Hybrid Protocols (SHyPs)**, and then puts the requests into the queue. Xiid Agents then **pull requests** from the collector based on the Agent's purpose, unpacks the data using the second half of the Smart-*Hybrid* Protocol, and forwards the safe request on to the respective resource. The results are then digitally signed behind the closed Firewall and sent back to the Request Collector which then forwards the results to the respective destination.

Xiid SealedChannel

What is the SealedChannel?

The Xiid SealedChannel™ is a **one-way** communications channel that is established between an Xiid Agent and an Xiid Request Collector. The SealedChannel works the same way across all Xiid Agents: One-way **outbound** communication established from the private network, only allows **SHyPs** to be pulled from the

Request Collector's queue, only pulls **Agent-Specific Information** from the queue and **digitally signs** responses safely behind the firewall.

Where does the SealedChannel reside?

Since the SealedChannel is a communications channel, it does not *physically* reside anywhere. *Abstractly*, it resides **between** the **Request Collector** and the **Xiid Agents**.

Why use the SealedChannel?

Xiid's SealedChannel has been meticulously thought-out to **eliminate** all **attack surfaces** to private networks. Between the three layers of encryption used to handle the consumption of data by the agents behind the closed network, getting any malicious data or execution through the SealedChannel is effectively impossible, providing an air-tight mechanism to safely allow communication between your network and the internet.

How does the SealedChannel work?

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, requests will be accepted by the Request Collector, **packaged** with Xiid's SHyPs, and put into the Request Collector **queue**. The Xiid Agent will begin polling for requests from the Request Collector's queue, and will **extrapolate** any information needed from the request, **route** it to the proper resource, **digitally sign** the response, and send it back to the Request Collector, which will then **forward** the response to the appropriate destination.

XOTC Authenticator

What is the XOTC Authenticator?

The **Xiid One-Time-Code** (XOTC) Authenticator is a mobile application developed by Xiid for use in the Xiid Single Sign-On Portal. In a more abstract sense, XOTC Authentication is Xiid's patented technology that allows authentication without **any** usernames or passwords.

Where does the XOTC Authenticator reside?

The XOTC Authenticator resides on every **user's phone** within the organization via the XOTC Authenticator Mobile Application available in the Google Play Store and Apple App Store. All users that are required to sign into an SSO Portal are required to download the mobile application.

Why use the XOTC Authenticator?

The XOTC Authenticator is the **most secure** form of Multi-Factor authentication. XOTC takes authentication to the next level by removing user credentials from the authentication process. This has a plethora of benefits:

- No **Man in the Middle Attacks** - XOTC codes do not contain **any** user credential information, rendering them useless in reconnaissance.
- No need to write down or **remember passwords**
- In the event that a user's domain credentials are compromised, Xiid's SSO Portal and the applications within are still protected (authentication must occur from the XOTC Authenticator App, **manual entry is not permitted** after the credentials are bound).
- Streamlined **ease-of-use** - it's fast and easy to sign in!

How does XOTC Authentication work?

The XOTC Authenticator starts by **binding** your credentials to your XOTC Security Profile. When you register your XOTC App with your company's domain, you create a **link** between the Agent and the XOTC App for your known Group Numbers. From that point, whenever a user **scans** the QR code on the SSO Portal Screen, the XOTC Mobile App will generate an XOTC Code using one of those Group Numbers and

the screen information, and then will send that code to the Request Collector, where the request will be put into a queue and picked up by the Authentication (see Sealed Channel).

Xiid Agents

What is an Agent?

An Xiid Agent is an intermediary thin-wrapper software that acts as the **liaison** between the Request Collector and your **internal resources**. An Agent pulls requests from the Request Collector queue and will **action** based on the incoming request, depending on the *type* of Xiid Agent. For instance, Xiid.IM Active Directory Agents will pull authentication requests from the Request Collector Queue and authenticate users against the Active Directory Service. An RDP Agent would pull RDP Access Requests from the Request Collector and generate a one-time-password for the user on the local machine.

Where does an Agent reside?

The Xiid Agent resides in the **same network segment as the resource** to which the agent interacts. Xiid highly recommends using proper network segmentation to **separate your resources** by subnets, with Xiid Agents handling the authentication and access to the resources across your enterprise network.

Why use an Agent?

Xiid Agents are paramount to the **SealedChannel** paradigm, and only by use of Xiid Agents can you reduce (or eliminate) inbound ports on your network. Each Xiid Agent that goes online and becomes operational translates to **inbound ports** that can be **closed**, and subsequently **less attack surface** for malicious actors. Xiid Agents also manage overhead, **abstract** and **obfuscate** pertinent enterprise data (such as user credentials), and extend configurations and customization for the particularities of your enterprise network.

How does an Agent work?

Xiid Agents **operate differently** depending on what **resources** they govern. In general, all Xiid Agents adhere to the paradigms of the SealedChannel (**outbound communication** channels only, and only **communicating directly** with the **Request Collector**). The specifics of how interactions with different resources are managed will vary depending on the *type* of Agent deployed. See below for more information.

Xiid RDP Agent

What is an RDP Agent?

An RDP Agent is a **thin-wrapper software** that runs on machines which 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.

Where does an RDP Agent reside?

The RDP Agent runs on the **remote machine** that you would like to **RDP into**. There is also an RDP wrapper which you can download and install on any client machines wishing to access the RDP agent.

Why use an RDP Agent?

RDP Agents **manage credentials** on the machine, making it safer to RDP into the instance without the fear of having your **credentials hijacked**. The integration of RDP Agents into the SSO Portal also makes it much easier for employees who manage or use multiple remote machines to **easily manage** the **connections** and credentials for all of them.

How does an RDP Agent work?

The RDP Agent is first installed on the remote machine and bound to your Xiid account using the RDP Agent Configuration Code. Next, you can configure the remote machine to be available in your SSO Portals as either an RDP Application or RDP App (VDI) Application. When a user clicks the blue monitor icon

in the SSO Portal, a **session** is started and a request is put in the Request Collector Queue, and pulled in from the RDP Agent. The Agent would then generate a new one-time-password for RDP login and push the **password** back out to the client's computer, where it is **injected** into the user's **clipboard**. When the .rdp file is downloaded, the username will already be provided, and the user just pastes the password into the prompt to sign in.

Xiid.IM Active Directory Agent

What is the Active Directory Agent?

The Active Directory Agent is the **configuration portal** and **liason** to your **Active Directory** services. The AD Agent will handle all authentication interactions with Active Directory and check for access to SSO portals. It also provides the configuration portal for configuring access to various Active Directories (if there are multiple), setting up Firewalls and Translations for credentials, and configuring your Xiid SSO Portals. The Active Directory Agent is the **heart** of the Xiid Software stack, as almost all interactions with the enterprise network flow through this Agent, either directly or indirectly.

Where does an Active Directory Agent reside?

The Active Directory Agent resides in the **same network segmentation** as your **Active Directory Service**. The AD Agent just needs to be able to communicate directly with Active Directory. If you have multiple domains or Active Directories, you can deploy an Agent in each of those network segments.

Why use an Active Directory Agent?

Active Directory Agents handle all of the **authentication** requests for your SSO Portal as well as handling **access** validation for portals and applications. The AD Agent is the heart of the your enterprise security, because your **directory** is the **life blood** of your organization. As such, the AD Agent is critical to providing support for any other Agents. Without being able to verify who an individual is, applications cannot be provided securely to them.

How does an Active Directory Agent work?

Active Directory Agents are deployed in the same network as your Active Directory Service. Once installed, the AD Agent is **bound** to your Xiid Account using the **Agent Configuration Code**. A browser application will be available on your desktop which you can open to go directly to the Xiid **Agent Management Portal**. The Agent Management Portal allows you to **configure** Active Directory Agent as well as the Single Sign-On Portals associated with your Xiid account. See the below information on the Xiid Active Directory Agent sub-components for more information.

The following **sub-components** are all part of the Xiid **Active Directory Agent**. All of these sub-components reside on the AD Agent and thus the "Where does it reside?" section has been removed.

Authenticators

What is an Authenticator?

Authenticators define how the AD Agent **communicates** with the **directory service**. The authenticator is comprised of the information regarding your directory service such as where it is physically located (**IP Address**) and how to interact with (query) the service, and who has **access** to what resources (Group Include/Exclude). Xiid recommends that the service account used to communicate with the Active Directory be limited to purely querying the LDAP directory; no other permissions, such as write permissions, are needed nor recommended.

Why use an Authenticator?

An Authenticator serves two main purposes. The first is to aggregate information about how to **communicate** with your **LDAP directory**. This is necessary to handle to authentication to your SSO Portals and

to protect your Active Directory from outside threats. The second purpose is to **limit access** via Group Include and Group Exclude filters.

How does an Authenticator Work?

Authenticators are a sub-component of the AD Agent. An **Authenticator** is comprised of **metadata** regarding the communication with the directory service, such as Group Include/Exclude, as well as **Connector**, which houses the information for the Active Directory Agent to **connect** to the **LDAP** service. This information is then used by Active Directory Agent when authentication requests come into the Request Collector and pulled in by the Agent to validate authentication. Without an Authenticator sub-component, the Agent would not be able to communicate with your Active Directory.

2-Factor Authentication

What is 2-Factor Authentication?

2-Factor Authentication is a framework that utilizes an **"out-of-band"** device to provide additional validation for an individual's identity. An "out-of-band" device refers to a device that is not directly tied to the network you are trying to authenticate against. Typically, the out-of-band device is a person's **smartphone**. Xiid offers two 2-Factor Authentication mechanisms: **Legacy MFA**, which uses the outdated "One-Time-Password" as a secondary authentication mechanism (not recommended), and **XOTC Authentication**, which uses Xiid One-Time-Codes to safely log in users without usernames or passwords (recommended).

Why use 2-Factor Authentication?

2-Factor Authentication is an effective method of adding a **layer** of **security** to the authentication process. Xiid goes a step further than legacy MFA by using our highly **secure XOTC** codes, which helps unify the authentication experience and retain rigid security, and keep usernames and passwords out of the broader internet ether.

How does 2-Factor Authentication work?

Legacy MFA uses a **synchronized one-time-password** on the user's out-of-band device, which cycles based on a specific algorithm for unique passwords.

XOTC Authentication **abstracts usernames** and **passwords** behind ambiguous Group Numbers, which are only known by the AD Agent safely behind your enterprise network. For more information on XOTC, see XOTC Authenticator.

Regardless of which 2-Factor Authentication method you use, you need to create the sub-component (either an XOTC or Legacy MFA) in the Agent Management Portal, and then **add** it to an **SSO Portal** to **enforce** the 2FA mechanism.

Translators

What is a Translator?

Xiid Translators tell the Xiid Agent how to **convert external authentication** credentials to the **internal** format that your LDAP service expects. A single Translator will define the round-trip conversion process from external credentials for authentication requests to the local Active Directory credentials and then inversely converting the authentication response back to the external credentials.

Why use a Translator?

Translators are necessary to convert **external** authentication data to **internal** representations. If you have any **other** username or **credential formats** that are not understood by your LDAP service, then you will need a translator to convert the data.

How do Translators work?

Translators are tied into the operations of the Active Directory Agent. Think of the individual translators as **instruction sets** provided to the Agent. When the Agent sees a username come in with a certain format,

the translator provides the ability to identify that format and then convert from that format to your LDAP format and back. Translators are – in technical terms – **regular expressions** that parse and replace string characters during the intermediary authentication steps done by your AD Agent. An External to Internal translator may look for the characters "example.com" in the username, and replace it with "example.local" for your LDAP service. The translator would then look for the characters "example.local" coming from your Active Directory and replace it with "example.com" for the Service Provider, such as Office 365.

Firewalls

What are Firewalls?

Xiid Firewalls are **Application Firewalls** that provide users the ability to **restrict** and **allow** specific IP addresses to authenticate at the SSO Portal. Xiid Firewalls operate between the collector and agent levels, meaning the restrictions and allowances defined in your Xiid Firewalls apply to authentication requests at the initial stage of authentication. The Collector will accept any authentication requests but the Xiid **Agent** may **accept** or **reject** those requests based on the Firewall settings.

Why use a Firewall?

Xiid Firewalls are not required to set up Xiid's technology, but they can **enhance security** to the systems by further restricting what authentication requests are allowed from what IP Addresses. Xiid Firewalls are particularly useful for **blacklisting** known bad-acting **IP Addresses** (or compromised systems and services) as well as **allowing** authentication requests from known **"safe" IP addresses**. You can also use Xiid Firewalls to restrict access to your SSO Portal within your enterprise network as well.

How do Firewalls work?

Xiid Firewalls are split into two categories: **Blacklist** and **Whitelist**. Blacklist firewalls can be employed to block specific IP Addresses, such as compromised servers or known **bad actor** addresses. Whitelist firewalls can be used to indicate that a specific IP address is a known **"trusted"** address, such as a third-party service or your own enterprise network. Be cognizant of the application firewalls that you create and block malicious addresses while allowing access to intended users.

SSO Portals

What are SSO Portals?

Xiid SSO Portals provide **access** to users for their applications. Xiid supports creating as many SSO Portals as you feel are needed for your organization. From the user perspective, the SSO Portals provide all-in-one access to their applications with secure **SAML2 Authentication** to protect their credentials. From a System Administrator perspective, an SSO Portal is an aggregated **collection** of **sub-components** that are synthesized together to create a cohesive **Single Sign-On** experience for users.

Why use an SSO Portals?

SSO Portals allow your users to **access** their **applications** over the internet safely and **securely**. SSO Portals also provide the flexibility and extensibility to separate access, restrict users, define translations for groups or sub-groups, enforce 2-Factor Authentication, and enforce application firewall rules.

How do SSO Portals work?

When you configure your Active Directory Agent through the Agent Management Portal, by default a **home** SSO Portal will be created and use your first Authenticator (once you have created your first Authenticator sub-component). You can **create** additional SSO Portals or **edit** any existing SSO Portal and change the configurations. The configuration changes happen **immediately** and may require users to sign back into the SSO Portal to observe the changed configurations. The SSO Portals are then vended by the Active Directory Agent to users based on the configurations you have set up for the portal.

Applications

What are Applications?

Xiid Applications are integration **sub-components** used to help configure and **connect** your Xiid **SSO Portals** to your third-party web applications (Also known as **Service Providers**). Xiid offers different types of Applications for different purposes, some very specific (such as the Office 365 and GSuite Applications) and some that are more generalized and support various different external applications (such as the SAML2 Application).

Why use an Application?

Xiid Applications define all of the **configurations** and metadata necessary to configure an external **service provider** to integrate into your SSO Portals. For each Service Provider you would like to **integrate** with, you would create an Xiid Application with the metadata to contact and verify authentication for users into that application. Each of those Xiid Applications will be added to a specified SSO Portal for access by those users.

How do Applications work?

Xiid Applications will vary based on the *type* of Application you are configuring. Some applications, such as GSuite and Office 365, are more streamlined and include additional instructions to configure the Service Provider and the Xiid Application to integrate with each other. Applications like the SAML2 Application are more ambigious and integration instructions will vary. From a general perspective, all applications require minimum configuration with Xiid for information like the **domain name** and the initial SAML2 **entry point**, and all Service Providers generally require **configuring** SSO settings through the **Service Provider** to allow authentication from an **Identity Provider**. For more information regarding Application Setup, see GSuite, Office 365, RDP, or the generic SAML2 setup guides.

Logs

What are Log Components?

The Xiid Log Component is available for system administrators to aggregate logs from their system for **debugging** or for **technical support** from Xiid.

Why use a Log Component?

The Xiid Log Component should be used when you need to **debug** or **diagnose** issues with **Service Provider** integration or SSO Portals. Xiid does **not** recommend leaving the Log sub-component **running** at all times due to computational constraints and security.

How do Log Components work?

Log sub-components are managed by the Active Directory Agent via the Agent Management Portal. You can **enable** logging from the **Logs** tab, which will then **log interactions** with the Active Directory Agent. The logs are stored in `C:\ProgramData\Xiid\XIID-Agent\logs` by default.

Standard Operating Procedures

The following are standard operating procedures for working with Xiid's software stack. Please note that some of the Processes are shortened and abridged. For more complete installation instructions, please view Xiid's Documentation Website.

Xiid RDP Agents

Adding a new RDP Agent

Process: To add a new RDP Agent, start by an Xiid RDP Agent in the Xiid Global Management Portal. After creating the new agent, download and install the RDP Agent executable on the remote machine. After the installation completes, copy the RDP Agent Code from the Xiid Global Management Portal and pasting it in the command prompt when it asks for the **Config Code**.

Gotchas: If the Active Directory Agent is not installed and running within your enterprise network, the RDP Agent will not show up in the Global Management Portal or the RDP Agents Tab of the Agent Management Portal (if the Active Directory Agent was installed after the RDP Agent). To fix this issue, restart the RDP Agent service on the remote machine, and the RDP Agent will be populated in both places.

Removing an RDP Agent

Process: To uninstall an Xiid RDP Agent from a machine, you can run the executable 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`.

Gotchas: It is also recommended that you delete the RDP Agent object in the Global Management Portal when you uninstall completely from a machine.

Xiid Active Directory Agents

Adding a new AD Agent

Process: To add a new Active Directory Agent, start by creating an Agent object in the Xiid Global Management Portal. After creating the new agent there, download and install the Xiid Active Directory Agent executable on the server you wish to run the Agent on (see System Overview: Agents for more information and best practices), after the installation completes a command prompt will appear and ask for the Agent Config Code. Copy the Agent Code from the Xiid Global Management Portal and paste it in the command prompt. Last, the command prompt will ask for an SA (Super User/Administrator) username and a password for the Administrative account.

Gotchas: Check the Supported Browsers and ensure one is installed in order to access the Agent Management Portal, otherwise UI components in the browser may not properly render.

Uninstalling the AD Agent

Process: To uninstall the Xiid Agent from a machine, you can run the uninstall executable 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`.

Gotchas: There may be a couple of artifacts left over after install that are recommended to clean up (particularly if you intend to re-install on the same machine). Delete the Xiid Registry Editor entries under `HKEY_LOCAL_MACHINE\SOFTWARE\Xiid Corporation`. Also delete any leftover files/folders in `C:\Program Files\Xiid.IM Agent` and in `C:\ProgramData\xiid`.

Xiid Authenticators

Adding a new Authenticator

Process: Open the Xiid Agent Management Portal, click Add Authenticator on the Authenticators tab, fill in the information provided, including the IP Address of the LDAP service (which can be 127.0.0.1 if the Agent is running on the same server) and a set of credentials to query the LDAP Service (See System Overview: Authenticators for best practices).

Gotchas: Creating the Authenticator itself does not fully integrate LDAP communication into your Xiid Software environment. You must also add the Authenticators to your SSO Portal for use.

Removing an Authenticator

Process: Open the Xiid Agent Management Portal and navigate to the Authenticators tab. On the Authenticators page, locate the authenticator you want to remove, click the red X button and then confirm.

Gotchas: Authenticators are tied to SSO Portals. When you remove an Authenticator that is bound to a Portal, the Portal may no longer be able to communicate with the LDAP service and disallow authentication. When removing Authenticators, it is recommended that you first remove the Authenticator configuration from any SSO Portals and replace them with the new authenticator to persist SSO uptime.

Xiid Firewalls

Add a new Firewall

Process: Open the Xiid Agent Management Portal and navigate to the Firewalls tab. Click Add Firewall, select the type of Firewall rule to create, enter the IP address to allow/block, then enter any tags to associate or group the Firewall rule.

Gotchas: None

Remove a Firewall

Process: Open the Xiid Agent Management Portal, navigate to the Firewalls tab, find the firewall rule you would like to delete, and click the red X on the Firewall row.

Gotchas: None

XOTC Authenticator

Add XOTC Authentication

Process: Open the Xiid Agent Management Portal, navigate to the XOTC tab, and click the Add XOTC button.

Gotchas: XOTC Authenticators must be added to an SSO Portal in order to actually enforce the authentication mechanism.

Remove XOTC Authentication

Process: Open the Xiid Agent Management Portal, navigate to the XOTC tab, find the XOTC Authenticator row you would like to delete, and then click the red X next to it. It is recommended that you also first remove the XOTC Authenticator from any SSO Portals (see Gotchas below).

Gotchas: XOTC objects in the Agent Management Portal essentially store all of the information regarding registered XOTC Mobile Applications, so if you delete an XOTC object in the XOTC tab, it will also wipe all registered XOTC Mobile Application Security Profiles from all users associated with the XOTC object.

SSO Portals

Add a new SSO Portal

Process: Open the Xiid Agent Management Portal, navigate to the SSO Portals tab, and click Add SSO Portal button. Select any authenticators, firewalls, translators, and secondary authentication mechanisms you would like for the portal.

Gotchas: The **id** that you provide is built into the SSO Portal URL (i.e. https://exampleportal.us.xiid.im/{id}).

Remove an SSO Portal

Process: Open the Xiid Agent Management Portal, navigate to the SSO Portals tab, find the SSO Portal you would like to delete, and click the red X on the row associated with the SSO Portal.

Gotchas: None

Xiid Translators

Adding a new Translator

Process: From the Xiid Agent Management Portal, navigate to the Translators page. Then use the Add Translator button to create a new translator. Provide any tags you would like to group and associate the translator.

Gotchas: Translators are organized by **Tags**. Do not forget to add relevant tags to your Translators and to add those Translator Tags in any SSO Portals you would like the translators to apply to.

Removing a Translator

Process: In the Xiid Agent Management Portal, select the Translators tab, find the Translator you wish to delete, and click the red X button on the left of the Translator.

Gotchas: Check for any SSO Portals that use the Translator rule before deleting and ensure that the rule is no longer needed.

Xiid Applications

Adding an RDP Application

Process: Open the Xiid Agent Management Portal, navigate to the Applications tab, click the Choose button inside the RDP card, and click the Add Application button. Select the SSO Portal to add the RDP access to, select the RDP Agent (see RDP Agents), and fill out the remaining information.

Gotchas: If you leave the User field blank, the User who is signed into the SSO Portal is the username that will be used for RDP access. If you leave the IP Address field blank, the IP Address will be automatically provided (useful for dynamically allocated IP address remote machines).

Adding an RDP App (VDI) Application

Process: Open the Xiid Agent Management Portal, navigate to the Applications tab, click the Choose button inside the RDP App card, and click the Add Application button. Select hte SSO Portal to add the VDI access to, select the RDP Agent (see RDP Agents), and fill in the remaining fields. Provide the full path to the application on the remote machine that you would like to access and any command line arguments to provide to the application.

Gotchas: If you leave the User field blank, the User who is signed into the SSO Portal is the username that will be used for RDP access. If you leave the IP Address field blank, the IP Address will be automatically provided (useful for dynamically allocated IP address remote machines). For multiple command line parameters, enter them as they would be entered via commandline (typically with a space (' ') delineation).

Adding a Google Workspace Application

Process: In the Xiid Agent Management Portal, go to the Applications tab, click the Choose button inside the GSuite card, and click the Add Application button. Fill in the information and select Google for the type. On the Parameters screen, enter the domain tied to your Google Workspace account and click the Create IdP Consumer button. After creating the consumer, the GSuite Configuration screen will pop up with the last steps to configure the Google Workspace integration. Follow the prompts to configure your Google Workspace Administrator settings and add the sign-in/sign-out hooks. On the last step, download the certificate and upload it to your Google Workspace account.

Gotchas: If you lose track of the GSuite Configuration screen, you can click the purple Question Mark (?) button to open the screen again.

Adding an Office 365 Application

Process: Open the Xiid Agent Management Portal, navigate to the Applications tab, click the Choose button inside the Office 365 card, and then click the Add Application button. Select the SSO Portal and fill in the rest of the fields. The Username and Password fields must be an administrator for Microsoft 365 account. Follow the remaining screens to adjust your Microsoft settings.

Gotchas: If you are having issues with the Microsoft administrator account, you may need to temporarily disable MFA on the account while going through the initial setup of the Application. Also, ensure that you have an appropriate Microsoft Subscription.

Adding a SAML2 Application

Process: Open the Xiid Agent Management Portal, navigate to the Applications tab, click the Choose button inside the SAML2.0 card, and click the Add Application button. Select an SSO Portal and fill out the rest of the fields. For the domain, enter the external domain name associated with the SAML Service Provider and for the Entry Point enter the URL of the entry point that initiates the SAML authentication flow.

Gotchas: The Entry Point field is not the Assert Consumer Service (/acs), the ACS should be provided within the SAML XML, as per pure SAML implementation. If you need help finding the Entry Point URL, most Service Providers that support Single Sign-On will specify this URL in their SAML or SSO documentation. It can sometimes be referred to as the Service Provider Login URL. The domain field may be Service-Provider-Specific, so check the SP documentation, particularly if the SP does not know your domain name.