Xiid Zero Knowledge Networking Documentation

Quick Reference Guide

WARNING

The following are abridged, "quick reference" instructions for working with Xiid's software stack, and may be missing key information provided in the main body of the documentation.

Xiid RDP Agents

Adding a new Agent

- Add 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 `Activation Code` from the Xiid Global Management Portal and paste it in the window that appears when it asks for the `Activation Code`.

If the IM Agent is not installed and running within your enterprise network before the RDP Agent, the RDP Agent will not show up in the Global Management Portal or the RDP Agents Tab of the Agent Management Portal. To fix this issue after installing the IM Agent, restart the RDP Agent service on the remote machine and the RDP Agent will be populated in both places.

Agent Uninstallation

- To uninstall an RDP Agent from a machine, you can run the uninstaller either from the Windows **Add or Remove Programs** menu or directly from the installation folder, located by default under: `C:\Program Files\Xiid.IM RDP Agent\unins000.exe`.
- It is also recommended that you delete the RDP Agent object in the Global Management Portal when you uninstall completely from a machine.

Xiid IM Agents

Adding a new Agent

- Provision an IM Agent in the Xiid Global Management Portal.
- Download and install the Xiid Active Directory Agent executable on the server you wish to run the Agent.
- Copy the `Activation Code` from the Xiid Global Management Portal and paste it in the window that appears.
- Last, the window will also ask for you to set an Xiid Administrator username and a password for the Agent Management Portal.

Agent Uninstallation

- To uninstall the Xiid Agent from a machine, you can run the uninstaller from either the Windows **Add or Remove Programs** menu or directly from the installation folder, located by default under `C:\Program Files\Xiid.IM Agent\unins000.exe`.
- If they exist, manually delete the Xiid Registry Editor entries under `HKEY_LOCAL_MACHINE\SOFTWARE\Xiid Corporation`, as well as any leftover files/folders in `C:\Program Files\Xiid.IM Agent` and in `C:\ProgramData\xiid`.
- It is also recommended that you delete the IM Agent object in the Global Management Portal after uninstalling completely from a machine.

Xiid Authenticators

Adding a new Authenticator

- In the Xiid Agent Management Portal, click Add Authenticator on the Authenticators tab and fill in the required information, such as 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
  - 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(s) for use.

Removing an Authenticator

- 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.
  - 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 maximise SSO uptime.

Xiid Firewalls

Add a new Firewall

- 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.

Remove a Firewall

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

XOTC Authenticator

Add XOTC Authentication

- Open the Xiid Agent Management Portal, navigate to the XOTC tab, click the Add XOTC button, and follow the instructions.
  - XOTC Authenticators must be added to an SSO Portal in order to actually enforce the authentication mechanism.

Remove XOTC Authentication

- 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
  - XOTC objects in the Agent Management Portal store 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

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

Remove an SSO Portal

- 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.

Xiid Translators

Adding a new Translator

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

- 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.
  - 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

- 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, and fill out the remaining information.

- If you leave the User field blank, the User who is signed in to 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

- 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 the SSO Portal to add the VDI access to, select the RDP Agent, 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.
  - If you leave the User field blank, the User who is signed in to 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 command line (typically with a space (`' '`) delimiter).

Adding a Google Workspace Application

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

Adding an Office 365 Application

- 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.
  - 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 365 subscription.

Adding a SAML2 Application

- 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
- For the Entry Point, enter the URL of the Entry Point that initiates the SAML authentication flow.
  - 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.