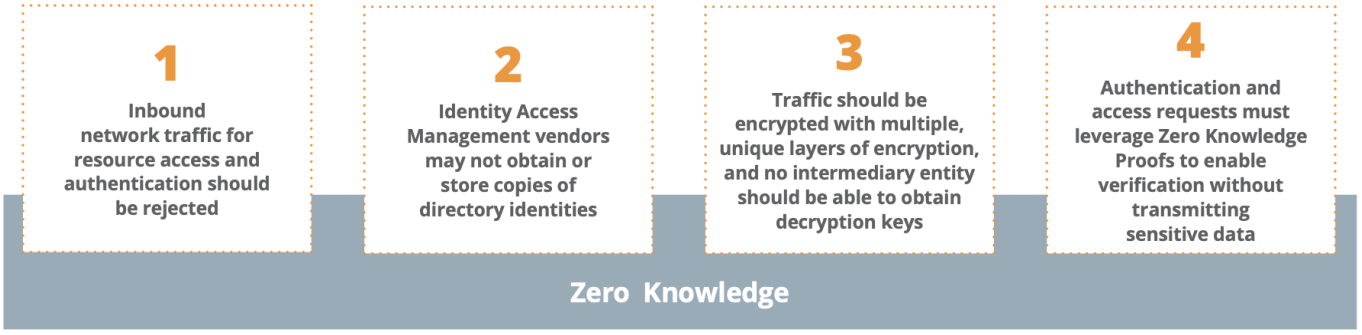
Xiid Zero Knowledge Networking Documentation

Zero Knowledge Networking Introduction

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

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

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



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

Xiid Products

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

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

More Information

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

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

Technical Overview

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

Birds-Eye View

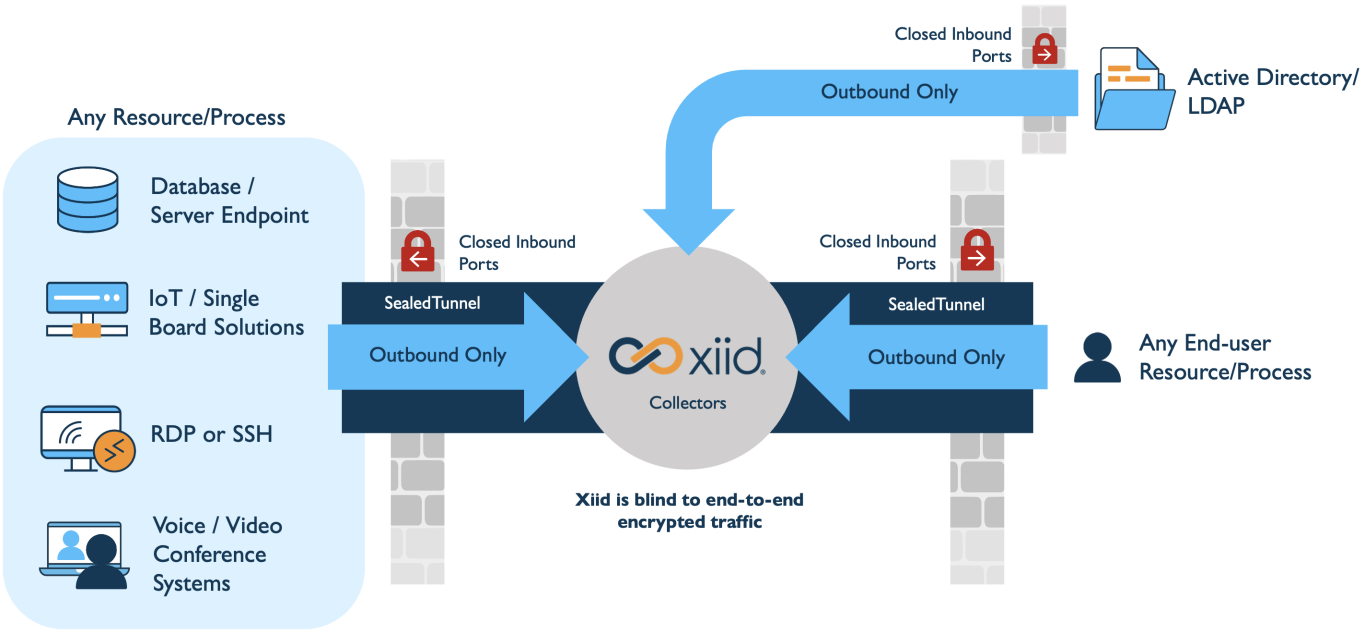
At a high level, the technology underpinning Xiid's products can be split into four major components:

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

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

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

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



Xiid One Time Code Authenticator (XOTC™)

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

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

The XOTC Authenticator is available for Android and iOS devices.

Xiid Collectors

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

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

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

Request Collector

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

SealedTunnel Collector

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

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

SealedChannels and SealedTunnels™

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

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

SealedChannel solves this problem by creating an encrypted and secured communication channel that utilizes outbound ports and efficient, consistent polling. The messages polled from within the network are stored in memory on the Xiid Request Collector with multiple

layers of strong encryption, including with Xiid's own patented technology, **Smart Hybrid Protocols (SHyPs)**.

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

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

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

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

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

Xiid Agents

Xiid Agents handle communication via SealedChannels and SealedTunnels.

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

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

Agent	Function
IM	Authentication requests
RDP	RDP/VDI connections

Agent	Function
STLink	SealedTunnel connections

IM Agent

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

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

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

RDP Agent

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

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

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

STLink

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

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

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

Xiid Portals and Applications

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

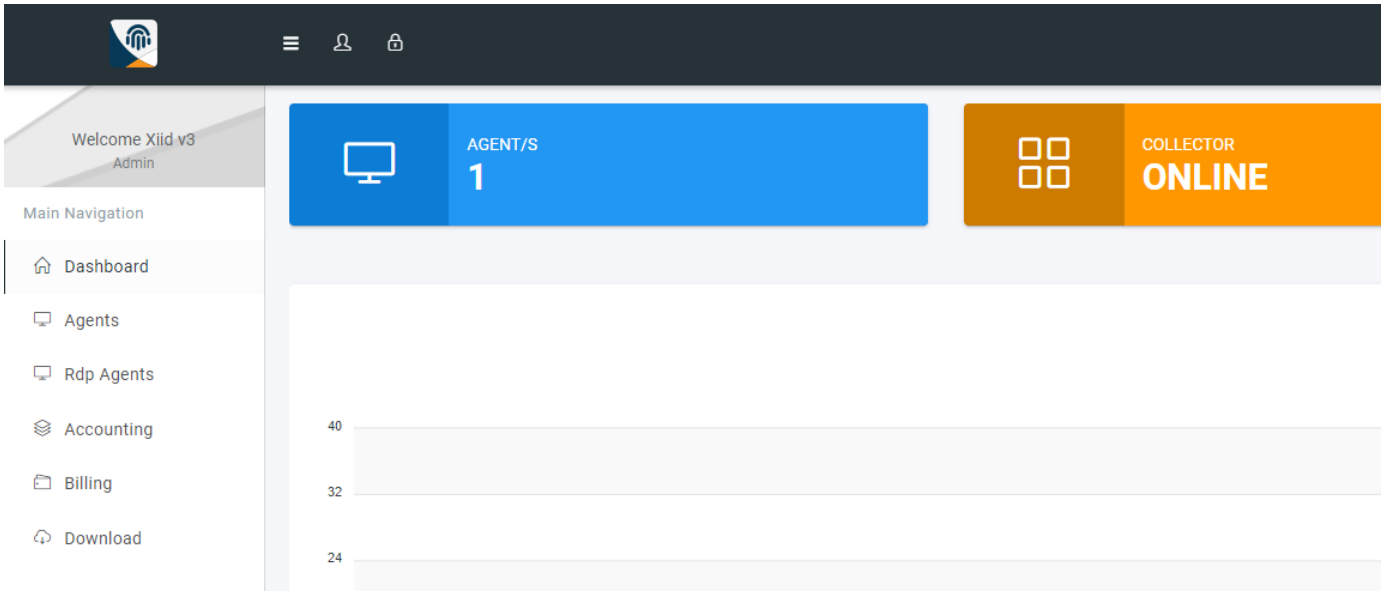
These portals include the Xiid Global Management Portal, the Xiid Agent Configuration Portal, and Single Sign-On (SSO) Portals.

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

Xiid Global Management Portal

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

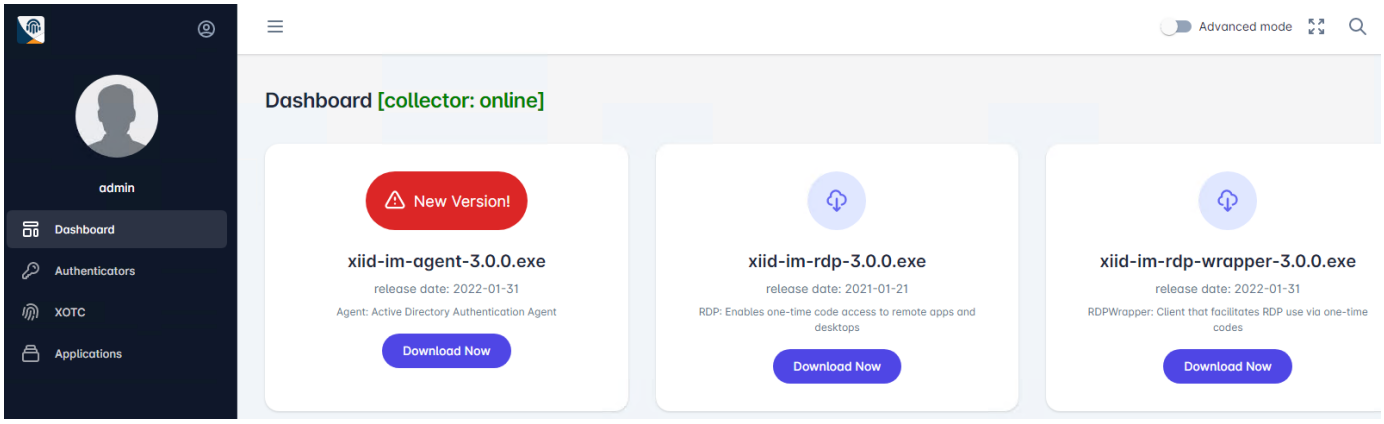
The Global Management Portal also allows administrators to configure Xiid IM Agents to integrate Xiid with their company directory services for authentication.



Xiid Agent Configuration Portal

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

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



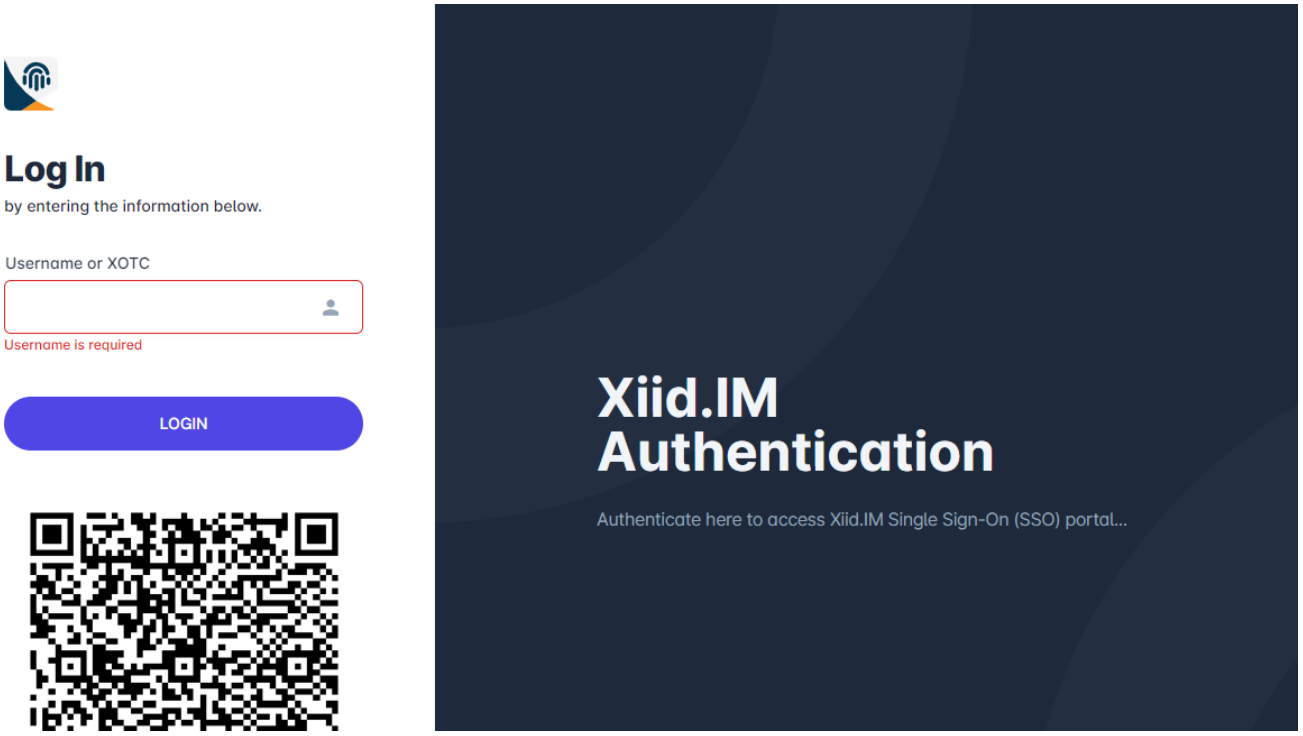
Single Sign-On (SSO) Portal

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

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

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

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



XOTC Mobile Application

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

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

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

The XOTC Mobile Application only supports the following operating systems:

iOS

- iOS version 15+

Android

- Android 14+

SealedTunnel™ (ST)

SealedTunnel™ is a comprehensive solution for network security and access that never requires open inbound firewall ports or public IP addresses, making your enterprise network nearly invisible to threat actors.

SealedTunnel offers on-demand, triple-encrypted, process-to-process secure tunneling, supporting any TCP/IP communication (such as `SSH`, `RDP`, and normal web traffic) between remote resources.

With some easy configuration, this makes accessing an internal web application over SealedTunnel as simple as using a browser normally, requiring no behavioral changes from your users!

There are two different options for SealedTunnel deployments:

- **Standalone SealedTunnel**: works by itself, and does not require licenses for other Xiid products
- **SSO SealedTunnel**: our most powerful SealedTunnel experience backed by the security and access capability of Xiid IM

This guide will walk you through deploying and configuring Standalone and/or SSO SealedTunnel in your organization.

SealedTunnel Components

Each component of **SealedTunnel** serves a key role in enabling Xiid's Zero Knowledge Networking **tunnelling solution**. Understanding the function of each of these components individually will help system administrators better manage and interact with the Xiid ecosystem.

STCollector

> **TIP**
>
> STCollectors are available as either a SaaS offering from Xiid or licensable for on-prem or private cloud deployments.

STCollectors are a type of specialized Request Collector for SealedTunnel.

The STCollector collects packets of triple-encrypted SealedTunnel data and bridges virtual connections between STLinks.

STCollectors do not include the SHyPs that the Request Collector uses due to the unstructured nature of SealedTunnel data.

Agent Configuration Portal

TIP

Xiid IM licenses are not required to run the Agent Configuration Portal, which is necessary to manage SealedTunnel deployments. IM functionality is not available without an IM license.

The Agent Configuration Portal is a web portal used to configure various aspects of your Xiid IM and **SealedTunnel** deployments, including configuring **Virtual Users**.

STLink

WARNING

You cannot reuse the same `Entrypoint Activation Codes` or `Exitpoint Activation Codes` across multiple machines.

The **STLink** is analogous to an Agent in Xiid IM and enables communication via the SealedTunnel.

An STLink is installed on (or near) both machines that wish to communicate over the tunnel.

Generally speaking, the client connecting to a resource is considered an Entrypoint and is configured using an `Entrypoint Activation Code`. The server hosting the resource is considered an Exitpoint and is configured using an `Exitpoint Activation Code`.

The STLink receives Mapping Configurations that contain the loopback address and Port Bindings.

Entrypoints

In the most simplistic terms, an **Entrypoint** is a client-side list of connections to different remote resources.

An Entrypoint defines the loopback addresses and ports associated with a client machine.

Entrypoint Mapping Configurations are configured in the Agent Configuration Portal and map to an Exitpoint's loopback address and port in the form of a Binding.

One Entrypoint can map to any number of Exitpoints.

Exitpoints

Generally, **Exitpoints** are the server-side remote resources clients would wish to access.

Exitpoint Mapping Configurations are configured in the Agent Configuration Portal.

For instance, you can map RDP access to `127.0.0.1:3389` (loopback address `127.0.0.1` on port `3389`).

If you are hosting a web server, such as a Wiki Server, on a remote machine, you can configure `127.0.0.1:443` (loopback address `127.0.0.1` on port `443`, the standard HTTPS port) on the Exitpoint and traffic will be routed over the loopback address to the Wiki Server.

Mapping Configuration

A **Mapping Configuration** is a mapping of a loopback address and port on an Entrypoint or an Exitpoint.

For instance, for an RDP connection, you could configure the address `127.0.0.1` and port `39` (`127.0.0.1:39`) on the client-side and a mapping to `127.0.0.1` on port `3389` (`127.0.0.1:3389`) on the server side.

These Entrypoints and Exitpoints are then linked through a Binding.

The client would connect to `127.0.0.1:39` locally to access port `3389` (`127.0.0.1:3389`) on the remote machine.

Bindings

Bindings link an Entrypoint's Mapping Configuration(s) to a specific Exitpoint's Mapping Configuration(s).

A Binding defines what Mapping Configuration a client would connect to on their device and which Exitpoint Mapping Configuration the traffic would be routed to on the endpoint.

SealedTunnel Setup

IM Agent Required by SealedTunnel

Even if you do not have an Xiid IM License, installation of the IM Agent is still required to manage SealedTunnel.

Whether you're using **Standalone SealedTunnel** or **SSO SealedTunnel** with Xiid IM, these instructions will help you activate, provision, and perform basic configuration of your SealedTunnel deployment.

SealedTunnel Activation

TIP

Activation is only required once, at the enterprise level, to enable SealedTunnel functionality across your organization.

- Access the Agent Configuration Portal via the shortcut added to your desktop during installation or at `https://127.0.0.1:10458/` and navigate to the **Tunnels** tab on the left side.
- When prompted for an `Activation Code`, enter the one provided to you by Xiid.

Exitpoint Provisioning

Exitpoints are, generally, the server-side end of a SealedTunnel connection.

- Navigate to the **Exitpoints** tab under **Tunnels** in the Agent Configuration Portal.
- On the Exitpoints screen, click the **+ Add Exitpoint** button in the top right.
- Provide a `Description` for the Exitpoint.
- Select any Units from the **Units** dropdown.
- Click the **SAVE** button.

- Find the Exitpoint you just created, click the **Green Clipboard** icon and record the `Exitpoint Activation Code` that was just copied to your clipboard. You'll need this during STLink installation for the Exitpoint!

Exitpoint Configuration

> **WARNING**
>
> You must install the STLink using the `Exitpoint Activation Code` before proceeding to configuration.

After creating the Exitpoint, we need to add Mappings to enable clients to access to applications via the Exit Point.

- From the **Exitpoints** screen, click the purple **Pencil** button on the row of your new Exitpoint to edit the Exitpoint.
- In the **Edit Exitpoint** screen, click the **Add Mapping** button located under the red "Back" button.
- In the **Add Mapping** screen, enter a `Description` for the mapping that describes what the mapping will be used for (e.g., RDP Access, SSH Access, Web Portal Access).
- In the **Map To** field, provide a loopback address and port in the format `127.X.X.X:X`, such as `127.0.0.1:3389`.
  - The **Map To** field determines the loopback address that SealedTunnel traffic will be sent to. For instance, if the **Map To** field is set to `127.0.0.1:3389`, then the traffic on the Exitpoint will loop through port `3389` on the machine.
  - If you are integrating a web portal through the SealedTunnel, you can use `127.0.0.1:443` to pick up on the web server's existing listening port without needing to change any configurations on the web server.
- In the **Application** dropdown, leave the `None` option unless this Exitpoint mapping will be used for RDP specifically, in which case choose the `RDP` option.
- After reviewing the configurations, click **SAVE**.

- Back in the **Edit** screen for the Exitpoint, check the `Unattended` mode checkbox and then click **SAVE**.

Entrypoint Provisioning

> **TIP**
>
> Whether accessed in conjunction with Xiid IM or Standalone, all clients (Entrypoints) using SealedTunnel must install the STLink software.

Entrypoints are, generally, the client-side end of a SealedTunnel connection.

Unlike with Exitpoint provisioning, Entrypoints have different configuration procedures depending on whether you are using SSO SealedTunnel (i.e., in conjunction with Xiid IM) or Standalone SealedTunnel without Xiid IM.

- Navigating to the **Entrypoints** tab under **Tunnels** in the Agent Configuration Portal.
- On the **Entrypoints** screen, start by clicking the **+ Add Entrypoint** button in the top right.
- Provide a `Description` for the Entrypoint with a description identifying the device or user's machine and click **Save**.
- Select any Units from the `Units` dropdown.
- Find the Entrypoint you just created, click the **Green Clipboard** icon and record the `Entrypoint Activation Code` that was just copied to your clipboard. You'll need this during STLink installation for the Entrypoint!

Entrypoint Configuration

> **WARNING**
>
> You cannot configure access to the Entrypoint until you have finished STLink installation.

To configure access through your Entrypoint to Exitpoint resources, refer to the access guides under Application Setup.

Installing and Updating the STLink

TIP

The STLink runs as a background service that automatically starts on system boot.

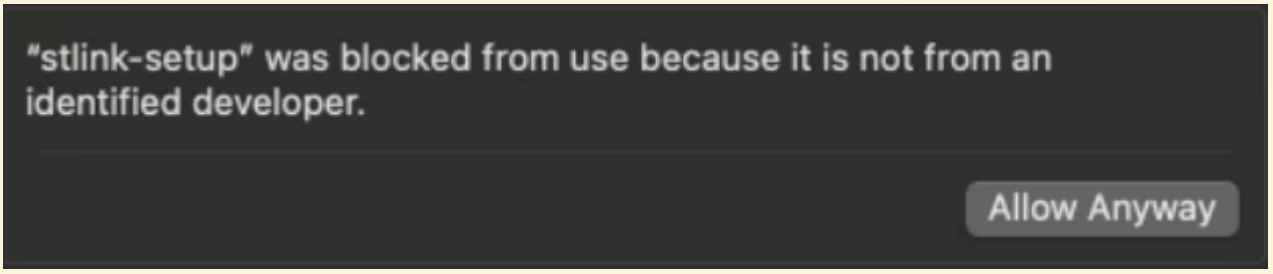
The STLink software must be installed on both Entrypoints and Exitpoints in order to use the SealedTunnel.

macOS and Linux

WARNING

For fresh macOS installations, it is likely that Apple's Gatekeeper feature may block execution of the STLink installer.

To use the installer normally, open **System Settings**, navigate to the **Privacy and Security** tab, scroll to the bottom, and click **Allow Anyway** next to the prompt for `stlink-setup` **only** as shown:



Start by untarring the SealedTunnel installer archive obtained from the Xiid Management Portal under the **Downloads** tab.

For fresh STLink installations, run the following command, substituting `ACTIVATION_CODE` with your `Entrypoint Activation Code` or `Exitpoint Activation Code`:

macOS Linux

bash

```
sudo ./stlink-setup install -i ACTIVATION_CODE
```

For updates, no `ACTIVATION_CODE` is necessary:

macOS Linux

```bash
sudo ./stlink-setup install
```

Windows

- Sign in to the machine you'd like to install the STLink on and download or transfer the STLink software.
- After downloading the STLink installer executable from the Xiid Management Portal under the **Downloads** tab, double-click the executable to start the installer.
- Navigate through the license agreement and the prompts until you get to the Finish button.
- After clicking **Finish**, on fresh installs, a command prompt will pop up and ask for an `Activation Code`, which is your `Entrypoint Activation Code` or `Exitpoint Activation Code`.

STLink Logs

For troubleshooting, log aggregation, or analysis, you can locate STLink logs here:

Operating System	Path
Windows	`C:\ProgramData\Xiid\XIID-stlinkagent\logs`
macOS	`/var/log/Xiid/XIID-stlinkagent/logs`
Linux	`/var/logs/Xiid/`

Application Setup

Now that Xiid ST is set up, it's time to make it possible to securely access your applications and resources through Xiid ST!

Follow these example deployment guides for SealedTunnel:

- SSO SealedTunnel

- Standalone SealedTunnel
- RDP/VDI

SSO SealedTunnel Setup

The **SealedTunnel SSO Application** allows you to make SealedTunnels accessible via the SSO portal for end-users.

SSO SealedTunnel cards in the SSO Portal allows users to switch tunnels on and off, enabling an additional layer of authentication to access resources.

SealedTunnel SSO Application Setup

- Navigate to the **Applications** tab on the left-side navigation.
- Find the card labeled **SealedTunnel** and click the purple **Choose** button inside the card.
- Click the purple **+ Add Application** button in the top right.
- On the **Add SealedTunnel** screen, select the `SSO Portal` you would like to add the SealedTunnel card to.
- Provide a description of the tunnel's intended use in the `Description` field.
- After reviewing the information, click the purple **Save** button in the bottom.
- Back in the SealedTunnel application list, click the **purple pencil** button next to your newly created tunnel.
- On the **Edit SealedTunnel** screen, scroll down and click the **+ Add Mapping** button.
- Provide a `Description` of the purpose of this specific Binding.
- In the `Bind` field, provide a Mapping for the SealedTunnel to connect on.
- Next, select an Exitpoint you would like to associate the Mapping with in the `Exitpoint` dropdown.
- After selecting an Exitpoint, you will see a list of available Mappings populated in the table below.
- Click the checkbox next to the Mapping you would like to associate to this Entrypoint mapping.
- After selecting your Mapping and reviewing the information, click the **SAVE** button.
- You will now see your Binding listed in the table within the Entrypoint.
- Click the **SAVE** button to save the Entrypoint with its new binding.

SealedTunnel Application Custom Variables

When configuring the SSO SealedTunnel Application in the Agent Configuration Portal, there is a `Helper` field that can be customized to provide users with the pre-filled commands to make accessing endpoints more convenient.

Users can click a button and have the `Helper` commands be copied to their clipboard.

Various **Custom Variables** are available for use to make these commands more intelligent.

In the guide below, we will use the following sample information:

Field	Value
Domain	`example.com`
Username	`exampleuser`
Map Address	`127.0.0.1`
Map Port	`22`

UPN Reference

If you would like to reference the UPN of a user within the directory service, use the `$userad` variable. For example:

`$userad` ⇒ `exampleuser@example.com`

Username Reference

To reference the username by itself (not the full UPN with the domain), use the `$user` variable. For example:

`$user` ⇒ `exampleuser`

SealedTunnel Loopback Address Reference

To reference the loopback address that the SealedTunnel is bound to for this Entrypoint/Exitpoint, use the `$addr` variable. For example:

`$addr` ⇒ `127.0.0.1`

SealedTunnel Port Reference

To reference the port of the SealedTunnel binding, use the `$port` variable. For example:

`$port` ⇒ `22`

SealedTunnel Bind Address Reference

To reference the full bind address of the SealedTunnel Entrypoint/Exitpoint (loopback address + port), use the `$bind` variable. For example:

`$bind` ⇒ `127.0.0.1:22`

Standalone SealedTunnel Setup

Standalone SealedTunnels are always listening on the client machine for incoming connections.

These tunnels do not require Xiid IM, though you can still use Standalone SealedTunnels even if you have both products.

Standalone SealedTunnels are configured directly through the **Entrypoint** in the **Tunnels** tab of the Agent Configuration Portal.

The Standalone SealedTunnel secures the connection to and from the resource but will leave aspects like authentication up to the endpoint.

Installing Standalone SealedTunnels

Standalone Exitpoints

Refer to Exitpoint Provisioning and STLink Installation for steps on deploying Standalone SealedTunnel Exitpoints.

Standalone Entrypoints

Refer to Entrypoint Provisioning and STLink Installation for steps on deploying Standalone SealedTunnel Entrypoints.

Configuring Standalone SealedTunnels

Standalone Exitpoint Configuration

Standalone SealedTunnel Exitpoints are configured in the same way regardless of the access method (Standalone or SSO). Refer to Exitpoint Configuration for more information.

Standalone Entrypoint Configuration

Standalone SealedTunnel access on Entrypoints is configured via the Agent Configuration Portal.

Once the Binding is set for the Entrypoint, the STLink will start listening for connections on the loopback address and port.

- Sign in to the **Agent Configuration Portal**.
- Navigate to **Entrypoint** under the **Tunnels** tab.
- On the **Entrypoints** screen, click the purple **Pencil** button on the row of your Entrypoint to edit the Entrypoint.
- In the **Edit Entrypoint** screen, click the **Add Mapping** button located under the red "Back" button.
- In the **Add Mapping** screen, enter a `Description` for the Mapping that describes what the Mapping will be used for (e.g. RDP Access to Domain Controller, SSH Access to RHEL Server, Web Portal Access).
- In the `Bind` field, provide a loopback address and port in the format `127.X.X.X:X` (i.e. `127.0.0.1:39`).
  - The `Bind` field determines the loopback address that the client will use to access the corresponding Exitpoint mapping defined below. You can set up any number of Entrypoint mappings, however, you cannot duplicate mappings.
- Click the `Exitpoint` dropdown and select the Exitpoint you wish to connect this Entrypoint to.
- After selecting an Exitpoint from the dropdown, the table below will populate with the mappings from that Exitpoint that are available.
- Check the box next to the mapping you would like to Bind the Entrypoint mapping to.
- After reviewing the configurations, click the **SAVE** button.
- Back in the Edit screen for the Exit Point, check the `Unattended` mode checkbox and click the **SAVE** button.

Remote Desktop (RDP) and VDI Over SealedTunnel Setup

Exitpoint Setup

TIP

STLink includes RDP Agent functionality, so installing the RDP Agent is not required.

- Provision an Exitpoint for the machine that you'd like to have remote access to and return to these instructions **before** adding a Mapping.
- Ensure that STLink is installed on the Exitpoint.
- On the **Edit Exitpoint** screen for the Exitpoint you just provisioned, click the **Add RDP Mapping** button located under the red "Back" button.
- Near the top of the **Edit** screen for the Exitpoint, check the `Unattended` mode checkbox and then click the **SAVE** button.

RDP over Standalone SealedTunnel Entrypoint Setup

Provisioning and Configuration

- Follow the SSO SealedTunnel Entrypoint Provisioning instructions, and return here **before** enabling SSO access, as we'll need to modify a few things to use the Xiid RDP Agent.
- Ensure that STLink is installed on the Entrypoint.

Application Setup

DANGER

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

could cause the administrator to become permanently locked out of the machine.

- Navigate to the **Applications** tab in the Agent Configuration Portal.
- Find the **SealedTunnel RDP** or **SealedTunnel RDP App** cards listed under the available applications and click the purple **Choose** button.
- On the **Applications List** screen, click the **+ Add Application** button in the top right corner.
- On the **Add ST RDP Application** screen, select the `SSO Portal` that you would like to add this RDP Application to.
- For the **STRDP Agent** dropdown, select the Exitpoint you just set up.
- In the `User` input, you can enter a static user that everyone will sign in as, or you can leave it blank to use individual usernames.
- You may check the `Legacy` checkbox to enable standard `.rdp` file downloads from the Single Sign-On Portal.
  - Without the `Legacy` checkbox selected, end-users will need the Xiid RDP Wrapper installed on the client machine.
- Enter a `Description` for the RDP Application that will be visible to end-users in the Single Sign-On Portal.
- **If you're only granting access to a single RDP App rather than the full machine:**
  - In the `Application Path` field, enter the full path on the local drive to the application you wish to allow end-user access to.
  - You can also specify any application command-line parameters you would like to include in the `Application Params` field.
- Specify any `Security Groups` from your directory that you would like to include or exclude from access.
- Check `Custom Configurations` to edit specific configurations of the `.rdp` file if you wish.
- Click the purple **Save** button at the bottom.

RDP over SSO SealedTunnel Entrypoint Setup

TIP

This section is coming soon – stay tuned for updates!

Advanced Configuration

See here for advanced configuration options, including a list of special variables that can be used to customize your RDP application.

SealedTunnel Usage

> **TIP**
>
> Using the SealedTunnel usually requires little-to-no modification from how users previously accessed their resources! 💪

SealedTunnel is easy to use for end-users, whether you are using the Standalone SealedTunnel or SSO SealedTunnel with IM.

After you have configured your SealedTunnel and Installed the STLink on your Entrypoints and Exitpoints, you can start using tunnels.

Standalone SealedTunnel

RDP Access

If you set up **Remote Desktop access** for the Entry Point, you can create a `.rdp` file, point it to the same loopback address and port you configured for the Entrypoint, and then sign in directly to the RDP machine.

You can also add your SealedTunnel loopback addresses and ports to your favorite remote machine management software, such as **Windows Remote Desktop** or **Royal TS**.

Afterward, users can simply use the `.rdp` file or their management software to access their machines.

SSH Access

If you set up **SSH Access** for the Entrypoint, simply run the SSH command with the loopback address configured for your Entrypoint.

If you are using a non-standard port for SSH in your Entrypoint Binding, don't forget to provide the `-p [port_num]` flag to your SSH command.

Web Application Access

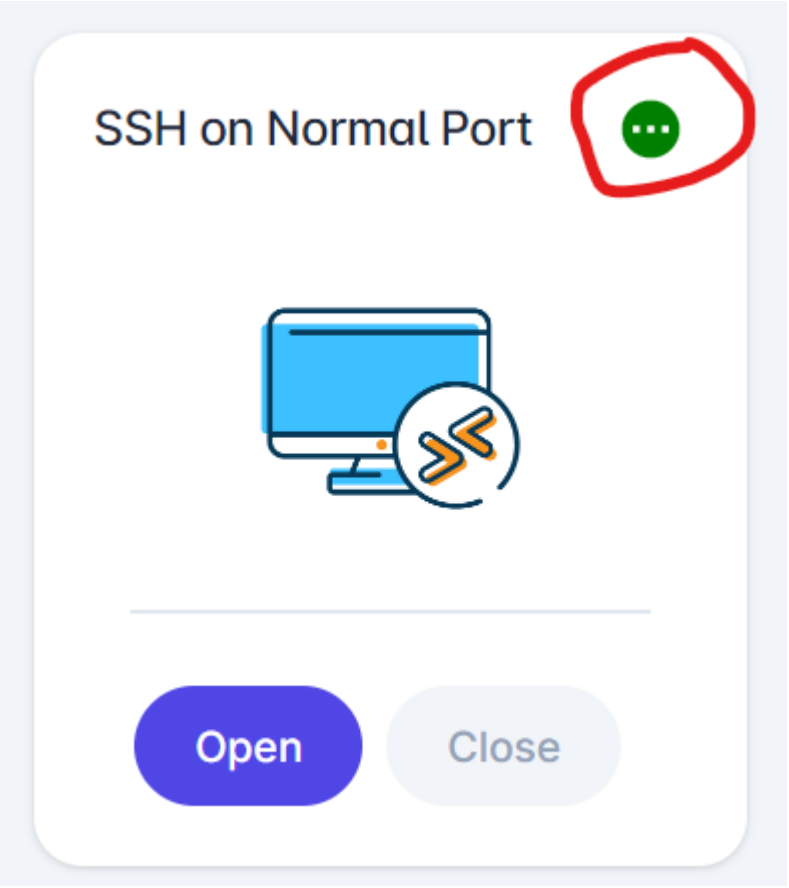
If you set up access to a Web Portal or other web application from an Entrypoint, you can enter the loopback address and port into a web browser to access the portal. Don't forget to add `https://` if required by your application.

If the loopback mapping is standard across Entrypoints and specified at the DNS level, users could simply visit to a URL you specify (e.g., `crm.yourcompany.com`) and use the tunnel seamlessly.

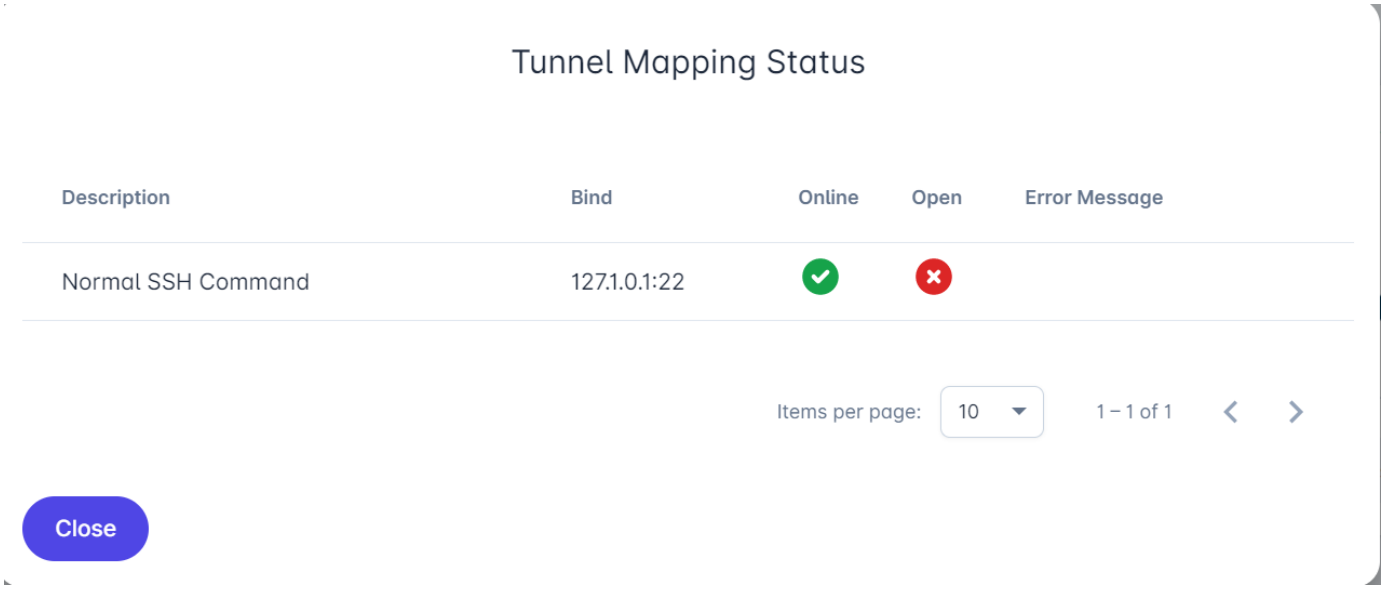
SSO SealedTunnel with Xiid IM

The **SSO Portal usage for the SealedTunnel** works the same way as the Standalone SealedTunnel except that not all SealedTunnel connections are automatically open on the **Entry Point** by default, since that is configurable by administrators.

- Sign in to your SSO Portal and locate your SealedTunnel cards.
  - SealedTunnel cards can be easily identified by the circle in the top right of the card with the three ellipses (`...`) as shown below (circled in red).
  - If the STLink is offline for a given Exitpoint, the card will be grayed out and the circle will be gray as well.



- If needed, clicking `...` will display the mappings for that specific SealedTunnel connection.



- Click the purple **Open** button to open the SealedTunnel connection from your machine to the resource you've selected.
- After the tunnel is open, you're free to access your resource as you need.
- When you're finished accessing the resource, click the **Close** button to shut down your tunnel.

WARNING

Closing the SealedTunnel in the SSO Portal does not end current sessions and only prevents blocks new sessions from being opened.

High-Availability Gateway Setup

DANGER

The traffic routing out of Exitpoints is **decrypted** as it has already traversed the full SealedTunnel.

Throughout this documentation, we have presumed that Mapping Configurations are loopback addresses. However, this is not actually a requirement of SealedTunnel.

In fact, SealedTunnel traffic can be routed from just about anywhere, so long as it's accessible from the Exitpoint.

If you would like to configure access to multiple machines using a single STLink, as a `Sealed Network Gateway` follow the instructions below.

Configure the Sealed Network Gateway

- Create an Exitpoint for the machine that will serve as the gateway.
  - When adding Mappings, rather than using a loopback address, use the **private IP address** of the machine you would like to access within the same subnet as well as the port that you wish to access the machine on.
- Install the STLink on the gateway machine.
  - There are no constraints on the machine other than that it must be accessible by all other machines you would like to access on the network.

This will work for accessing any resource on a separate machine, provided that the machine-level firewalls are configured appropriately.

If you have a web server running on a separate machine, for instance, and would only like to install the STLink on a single machine, you can route the traffic to port `443` (or `80`) and responses will route back through the gateway's STLink.

High-Availability and Smart Load-Balancing

TIP

High Availability and Smart Load Balancing requires additional servers in the same subnet.

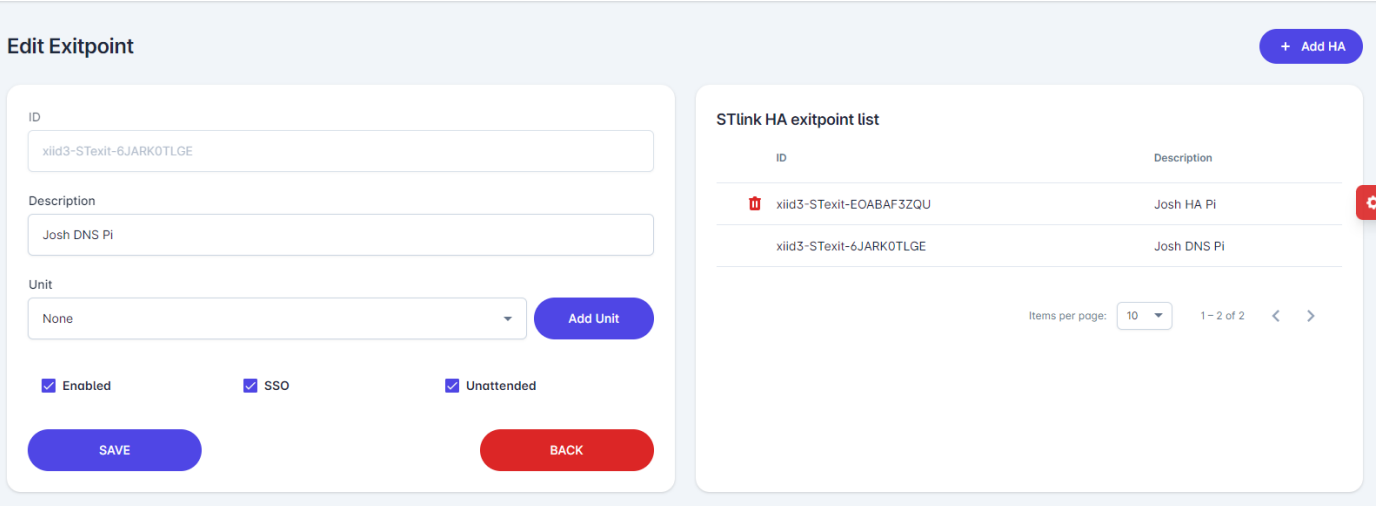
You can install multiple STLinks in the same subnet and configure them to distribute loads and failover in the event that a single Gateway Server goes offline.

- Complete the above gateway setup instructions before starting.
- Create a second Exitpoint for the machine that will serve as an additional gateway.
  - **Do not add any mappings to this Exitpoint**
- Install the STLink software the additional gateway machine.
  - There are no constraints on the machine other than that it must be accessible by all other machines you would like to access on the network.
- After installing and configuring the additional gateway Exitpoint, click the purple **Pencil** button next to the original Exitpoint set up in the gateway setup instructions that includes the mappings to resources within the subnet.
- Click the purple **+ Add HA** button in the top right of the **Edit Exitpoint** screen. In the popup window, select the additional gateway Exitpoint from the dropdown list.

TIP

Only Exitpoints that do not contain mappings will appear in the HA dropdown list. If you do not see your Exitpoint listed, ensure that there are no mappings within that Exitpoint.

After you have added the additional gateway Exitpoint to the High Availability table of the original gateway Exitpoint, you will see it listed in the table on the right.



You can verify that High Availability is configured on the second Exitpoint by clicking the purple **Pencil** button next to the second Exitpoint. You will see all of the mappings from the main gateway Exitpoint listed under the mappings.

WARNING

You can use the High Availability functionality to migrate mappings from one Exitpoint to another. Be aware that when you click the red **Trash Can** button next to a High Availability Exitpoint in the HA Table, mappings will be removed from that Exitpoint.

SealedTunnel Advanced Features

Local Domain Name Routing

TIP

Routes such as those described below can be set globally at the DNS level, making local changes to `hosts` files unnecessary and simplifying configuration across your organization.
Follow these instructions to map addresses to domain names at the **local** level only.

WARNING

Users may see a warning in their browsers that their connection may be insecure if the local domain name does not match the configured certificate.

Connecting to a loopback address in a browser (or through other GUI-based applications) to access a web portal (or service) through the SealedTunnel is not an intuitive or effective user experience.

To make SealedTunnel use easier, you can configure your `hosts` file to locally map addresses to domain names (URLs).

There are two ways to configure local domain name routing for client machines:

- Loopback Address Variation
- Local Port Listening

TIP

`hosts` files can easily be configured via group policies on Windows domains.

Loopback Address Variation

Loopback Address Variation is the simplest way to configure local domain name routing.

When configuring Entrypoints for your end users, map web portals to **unique** loopback addresses and specify port `443` as the port on all of them.

For example, if you have three web portals (i.e., an HR Portal, a Sales Portal, and a Code Repository Portal) all wrapped in the SealedTunnel, use a different address for each under the `127.*.*.* range` with HTTPS port `443` so that browsers (by default) will execute an HTTPS request.

For example:

Portal	Mapping
HR	`127.0.0.1:443`
Sales	`127.0.0.2:443`
Code Repository	`127.1.0.1:443`

Next, edit your `hosts` file and add the mappings for each portal to a domain name.

The `hosts` file can be found at the following locations:

Windows macOS Linux

console

```
C:\Windows\System32\drivers\etc\hosts
```

For example:

```
...
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
+ 127.0.0.1 hr.example.com
+ 127.0.0.2 sales.example.com
+ 127.1.0.1 gitlab.example.com
```

From now on, end users can simply use these URLs in their browser and their connections will be secured through the SealedTunnel behind the scenes.

Local Port Listening

Local Port Listening is an alternative method for configuring local domain name routing.

If you need to use a static loopback address for all of your Entrypoints, then use this paradigm.

First, it helps to construct a table of `ports`, `hostnames`, and `listen addresses`. The `listen address` is any unique address in the `127.*.*.*` range.

For example:

Portal	Mapping	Hostname	Listen Address
HR	`127.0.0.1:45`	`hr.example.com`	`127.65.43.21:443`
Sales	`127.0.0.1:886`	`sales.example.com`	`127.64.43.21:443`
Code Repository	`127.0.0.1:1329`	`gitlab.example.com`	`127.63.43.21:443`

Next, edit your `hosts` file, mapping the `listen address` to the host name (domain name). The `hosts` file can be found at the following locations:

Windows | macOS | Linux

console

```
C:\Windows\System32\drivers\etc\hosts
```

For example:

```
...
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
+ 127.65.43.21 hr.example.com
+ 127.64.43.21 sales.example.com
+ 127.63.43.21 gitlab.example.com
```

Finally, route the traffic listened to on the `listen address` to the ST Mapping.

Below are examples for different operating systems.

> **TIP**
>
> macOS and Linux instructions are coming soon – stay tuned!

For the HR Portal:

Windows

```batch
netsh interface portproxy add v4tov4 listenport=443 listenaddress=127.65.43.21
```

For the Sales Portal:

Windows

```batch
netsh interface portproxy add v4tov4 listenport=443 listenaddress=127.64.43.21
```

For the Code Repository:

Windows

```batch
netsh interface portproxy add v4tov4 listenport=443 listenaddress=127.63.43.21
```

This will route the HTTPS traffic sent to the domain name (e.g., `sales.example.com`) to port `443` on the `listen address` which routes the traffic to SealedTunnel mapping (e.g., `127.0.0.1:45`).

DNS A Record Routing

Rather than configuring host files individually for Entrypoint users, it's usually much easier to update your organization's DNS records to enable hassle-free use of the SealedTunnel.

Pointing DNS A Records to mapped loopback addresses for resource access, such as web services, will allow all users with appropriate SealedTunnel access to use those resources directly without requiring changes to local host files on each Entrypoint.

WARNING

All Entrypoints wishing to access resources via a DNS A Record must have the **same** loopback address and port configured on their individual Entrypoint configurations.

Simply add A Records to your DNS configuration that correspond to the loopback address configured on all Entrypoints that wish to leverage the domain name.

DNS A Records also work well for SealedTunnel Application Cards in the SSO Portal.

At Xiid, we use this ourselves to access our internal resources: here is a real example!

Units

Units are tags that can be used to organize your SealedTunnel Entrypoints and Exitpoints to easily locate them.

Click the **purple pencil** icon to edit the description of the Unit.

Click the **lock** icon to display only the Entrypoints and Exitpoints with the selected Unit assigned. For instance, if you had a Gitlab SealedTunnel Server, you could assign the server Exitpoint and all Entrypoints connecting to that server to a `Gitlab` Unit, making it easy to find them later. Use the red **Unlock Unit** button to remove the Unit filter.

SealedTunnel Troubleshooting

Restarting the STLink Service

Occasionally, the STLink service may need to be restarted.

Windows

After the STLink is installed, you will have a service listed for `xiid-stlink` (the exact service name may vary depending on your STLink version).

You can open Task Manager (`CTRL+SHIFT+ESC`) and click the `Services` tab to view the STLink service.

You can right-click the STLink service to start, stop, or restart it.

macOS and Linux

To start the STLink service, run the following command:

macOS Linux

```bash
sudo launchctl load /Library/LaunchDaemons/com.xiid.xiid-stlink.plist
```

To stop the STLink service, run the following command:

macOS Linux

```bash
sudo launchctl unload /Library/LaunchDaemons/com.xiid.xiid-stlink.plist
```

To view the status of the STLink service, run the following command:

macOS Linux

```bash
sudo launchctl print system/com.xiid.xiid-stlink
```