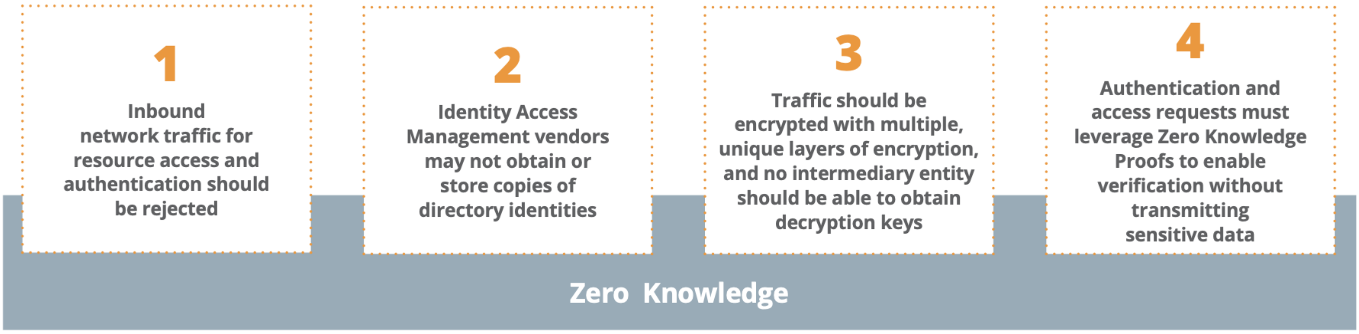
Xiid Zero Knowledge Networking Documentation

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**


1
Inbound network traffic for resource access and authentication should be rejected
2
Identity Access Management vendors may not obtain or store copies of directory identities
3
Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys
4
Authentication and access requests must leverage Zero Knowledge Proofs to enable verification without transmitting sensitive data
Zero Knowledge

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

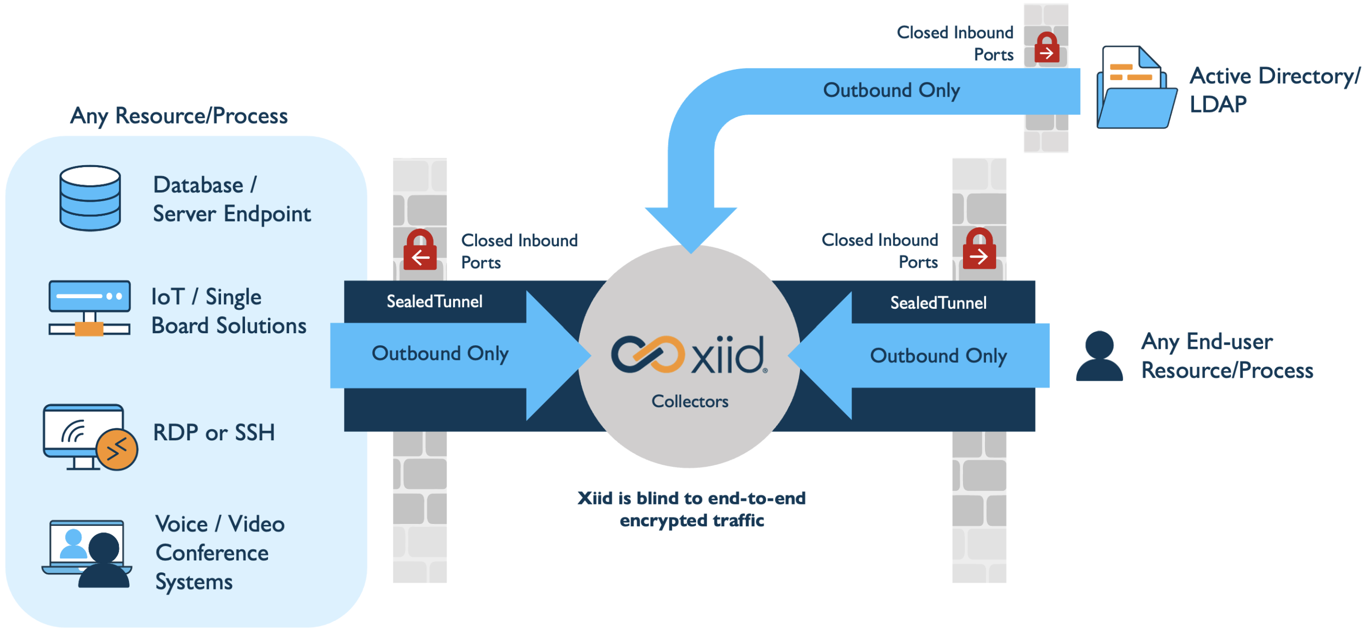
At a high level, the technology underpinning Xiid's products can be split into four major components:

- 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.

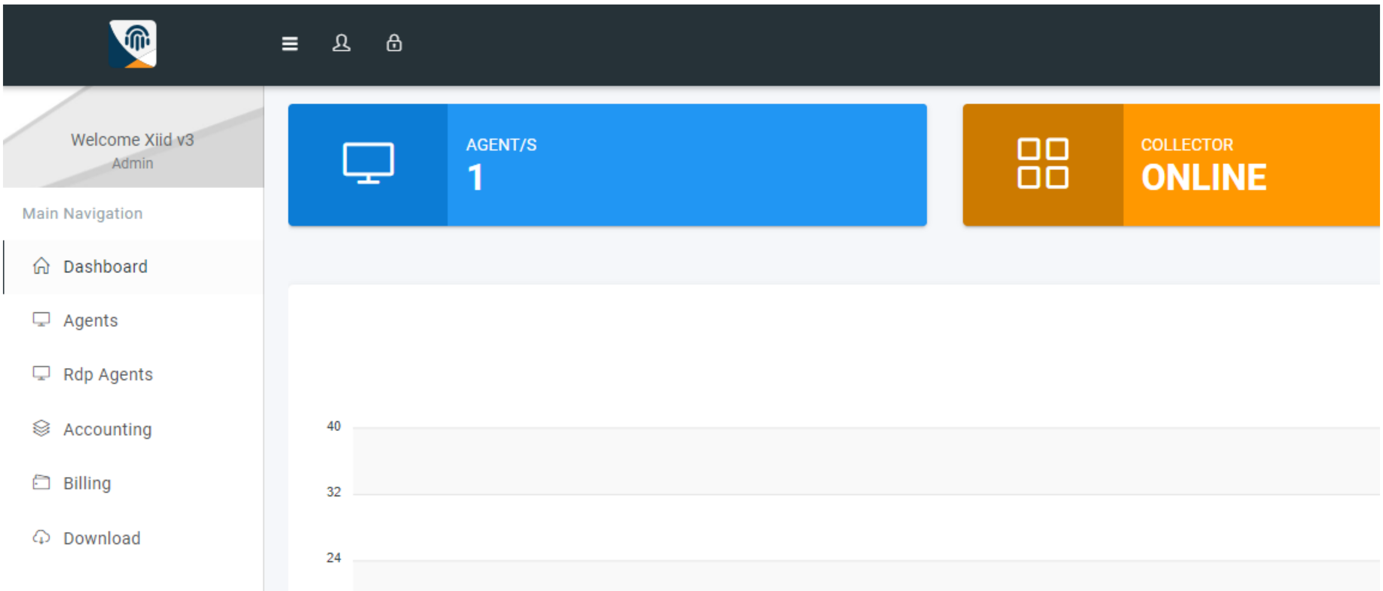
These portals include the Xiid Global Management Portal, the Xiid Agent Configuration Portal, and Single Sign-On (SSO) Portals.

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.

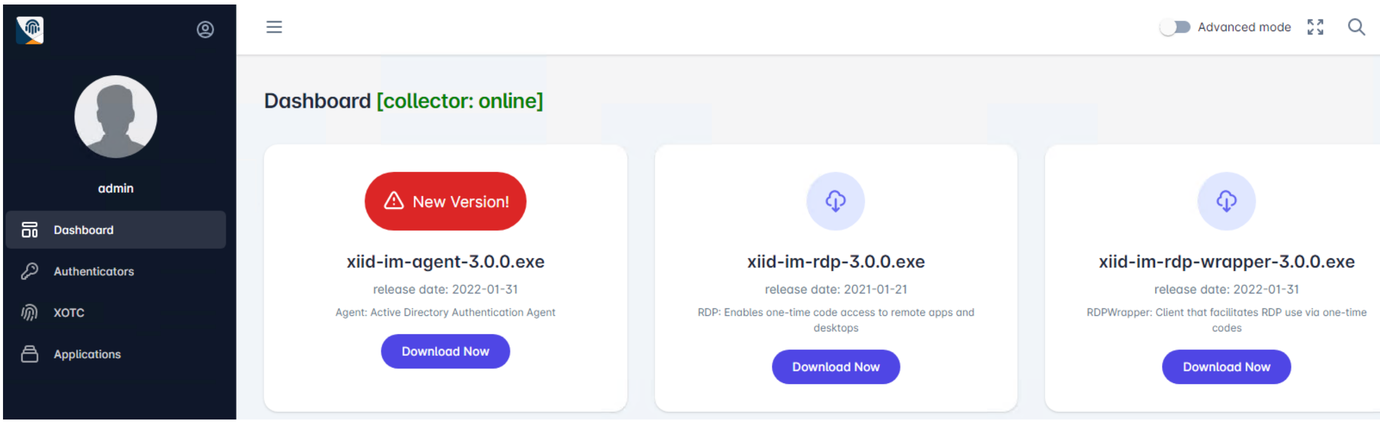
The Global Management Portal also allows administrators to configure Xiid IM Agents to integrate Xiid with their company directory services for authentication.



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.



Dashboard [collector: online]

xiid-im-agent-3.0.0.exe
release date: 2022-01-31
Agent: Active Directory Authentication Agent

xiid-im-rdp-3.0.0.exe
release date: 2021-01-21
RDP: Enables one-time code access to remote apps and desktops

xiid-im-rdp-wrapper-3.0.0.exe
release date: 2022-01-31
RDPWrapper: Client that facilitates RDP use via one-time codes

Single Sign-On (SSO) Portal

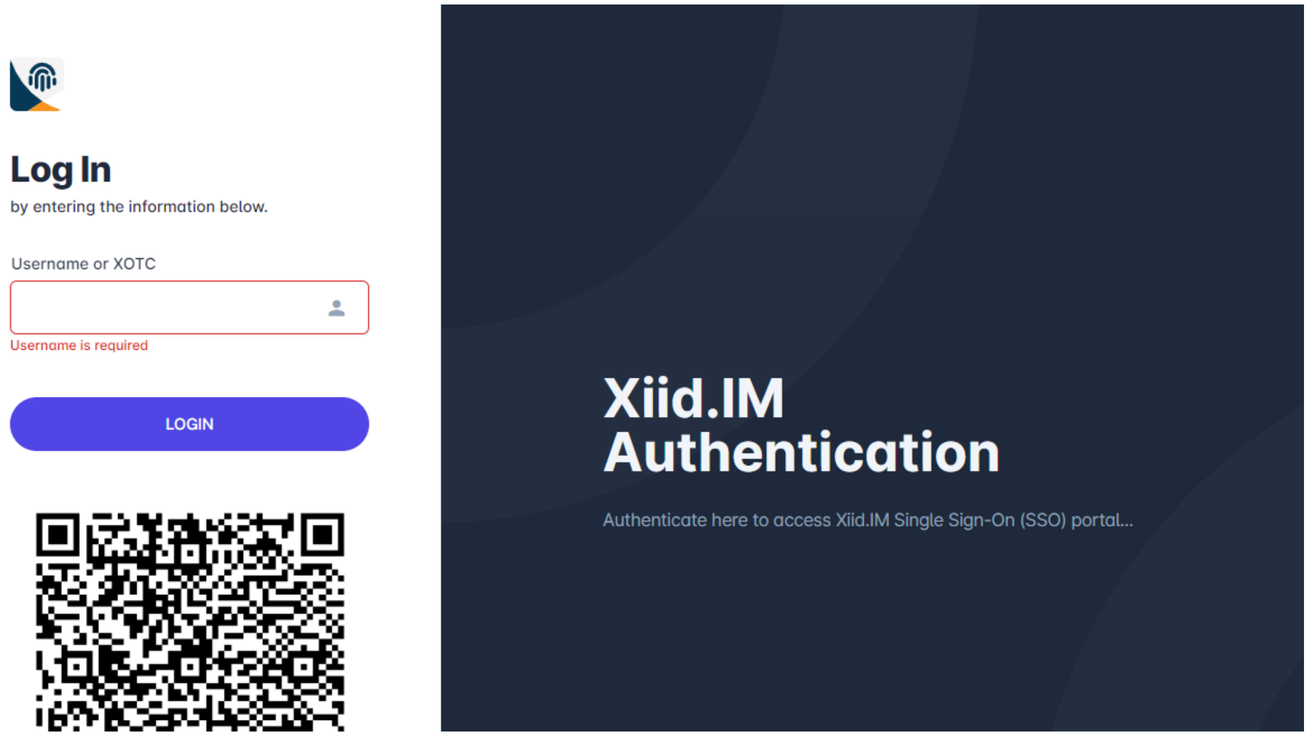
The **Single Sign-On Portal** allows users to securely authenticate against their domain and access their applications from any location.

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.



Log In

by entering the information below.

Username or XOTC

Username is required

Xiid.IM Authentication

Authenticate here to access Xiid.IM Single Sign-On (SSO) portal...

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+

Quickstart Guide Introduction

It's easy to get started with Xiid 🎉

No matter who you are, your first step is to create an administrator Xiid account that can be used by systems adminstrators to manage an organization-wide Xiid deployment.

Production Deployments

If you're ready to deploy in your organization, head directly to the Identity Management or SealedTunnel sections of the documentation.

Sandbox Deployments

Contact Xiid Before Continuing

We'd love to help you get started with a sandbox! Unless we've already been in touch, please talk to us before continuing to get the required Xiid software and automated deployment scripts.

If you'd like to test out Xiid in an isolated environment, we can help you stand up a sandbox and try out the following:

- Set up a Sandbox Domain for testing Xiid's Software (optional)
- Install and configure an Xiid IM Agent with LDAP
- Enable XOTC Authentication for Single Sign-On Users
- Set up SealedTunnel Access to a Remote Machine
- Create an Xiid SSO-Vended RDP Application
- Set up a Google Workspace Application in your SSO Portal
- Set up an Office 365 Application in your SSO Portal

- Set up a SAML2.0 Application in your SSO Portal

Xiid Account Onboarding

To start using Xiid's products, you must first create an Xiid account, for use by systems administrators, to manage your deployment here: https://onboardv3.xiid.com.

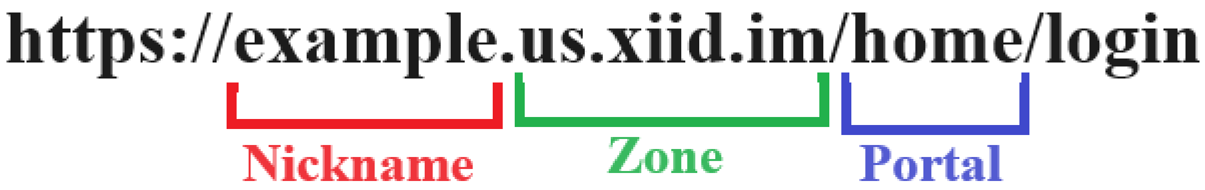
During account creation, you may be asked for email and/or SMS-based validation.

You will also be asked to provide a `nickname` for your Xiid Account. This name is used in the DNS Record created for your Single Sign-On (SSO) Portal.

DANGER

Choose your account nickname wisely as it cannot be changed.

For example, if the nickname you provide is `xiidtechnology`, the DNS record for your Single Sign-On Portal would be `xiidtechnology.us.xiid.im`.



After finishing these steps, you will receive an additional email from Xiid with a link to the management portal (https://managev3.xiid.com), as well as your login instructions.

Sandbox Information

Introduction

Xiid’s **Zero Knowledge Networking** works on top of a domain and a directory.

Domains are critical infrastructure and system administrators are rightfully leery to tamper with them using software that they are unfamiliar with. Domain modifications – particularly for security – require concise and well-understood changes.

For this reason, **Xiid provides domain administrators with the ability to test Xiid’s software in a sandboxed cloud environment that will not affect production domains.**

Automated **Xiid Domain Sandbox Tools** provide customers with the ability to quickly and inexpensively deploy (and destroy) this “sandbox” domain.

What is the Sandbox Domain?

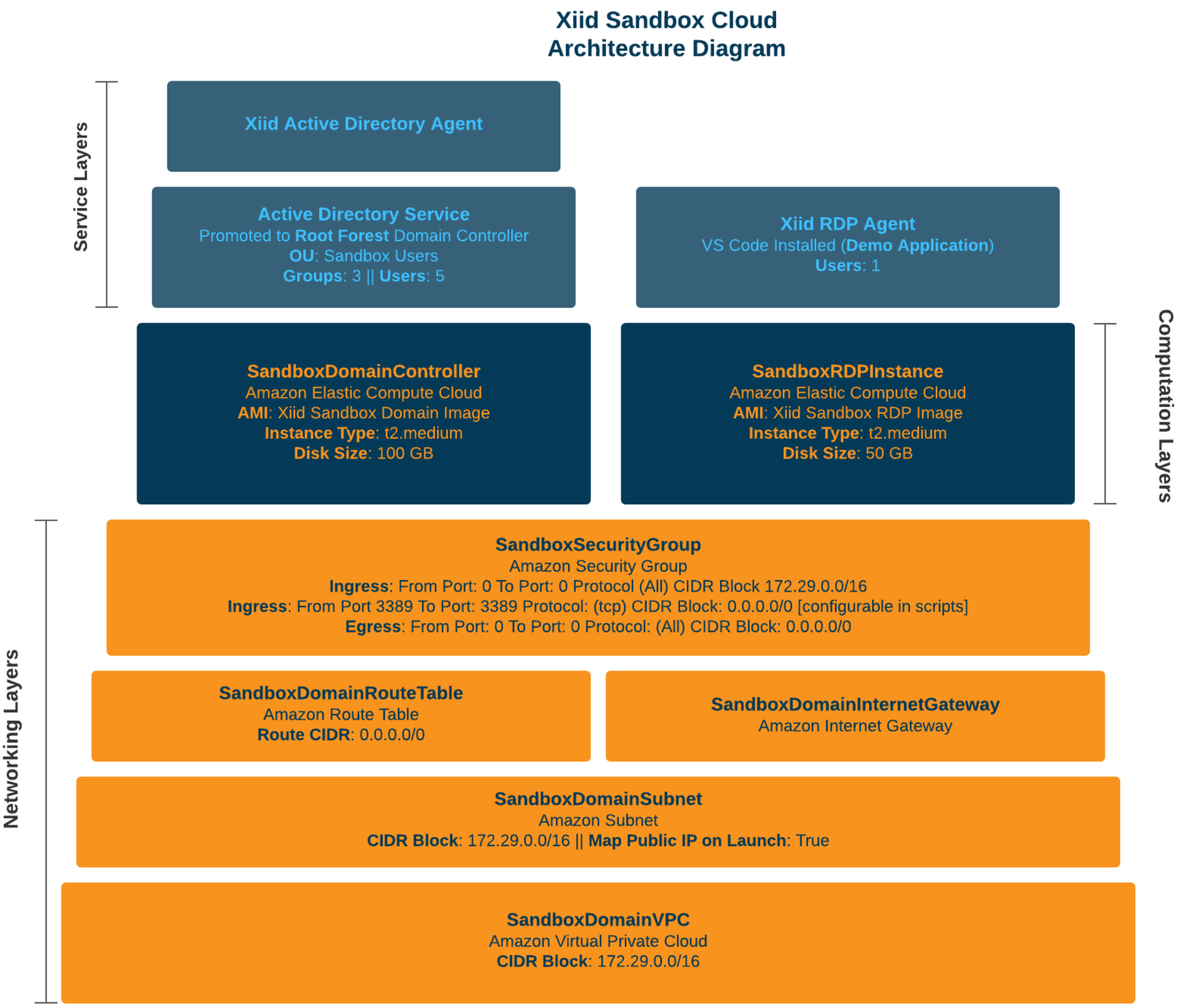
DANGER

Sandbox deployment scripts should not be used in production or for scaffolding infrastructure to be used in production.

The **Sandbox Domain** is a basic domain setup that can be easily deployed within a cloud provider (e.g., AWS, Azure) for testing purposes.

The Sandbox Domain includes the cloud networking layers necessary for creating and managing a domain controller. A basic **Virtual Private Cloud (VPC)** is provided and pre-configured with security groups wrapping the provided domain controller and RDP instance(s) with additional inbound/outbound network security to lock down access to the servers as much as possible.

The architectural diagram below shows the infrastructure components deployed within your cloud computing account when you run the Xiid Domain Sandbox Tools' scripts:


Xiid Sandbox Cloud Architecture Diagram
Service Layers
Xiid Active Directory Agent
Active Directory Service
Promoted to Root Forest Domain Controller
OU: Sandbox Users
Groups: 3 || Users: 5
Xiid RDP Agent
VS Code Installed (Demo Application)
Users: 1
Computation Layers
SandboxDomainController
Amazon Elastic Compute Cloud
AMI: Xiid Sandbox Domain Image
Instance Type: t2.medium
Disk Size: 100 GB
SandboxRDPInstance
Amazon Elastic Compute Cloud
AMI: Xiid Sandbox RDP Image
Instance Type: t2.medium
Disk Size: 50 GB
Networking Layers
SandboxSecurityGroup
Amazon Security Group
Ingress: From Port: 0 To Port: 0 Protocol (All) CIDR Block 172.29.0.0/16
Ingress: From Port 3389 To Port: 3389 Protocol: (tcp) CIDR Block: 0.0.0.0/0 [configurable in scripts]
Egress: From Port: 0 To Port: 0 Protocol: (All) CIDR Block: 0.0.0.0/0
SandboxDomainRouteTable
Amazon Route Table
Route CIDR: 0.0.0.0/0
SandboxDomainInternetGateway
Amazon Internet Gateway
SandboxDomainSubnet
Amazon Subnet
CIDR Block: 172.29.0.0/16 || Map Public IP on Launch: True
SandboxDomainVPC
Amazon Virtual Private Cloud
CIDR Block: 172.29.0.0/16

What the Sandbox Setup Guide Includes

This guide will walk you through setting up a Sandbox Domain for you to use for testing Xiid's software.

For those wanting to use AWS for the sandbox, this guide also includes simple AWS and Terraform instructions. If you are not familiar with AWS, it is recommended that you familiarize yourself with the AWS Console and AWS CLI.

That being said, there are no complex actions required within AWS as all infrastructure and networking will be configured and built automatically by Xiid-provided scripts.

What the Sandbox Setup Guide Does Not Include

This guide will not provide background on managing domains, domain controllers, Active Directory, or other typical system administrator tasks.

Typical use of Xiid’s software does not require in-depth knowledge of domain management. It is, however, advised that you understand how to manage (create/remove/update) users in Active Directory for additional testing.

This guide will not provide background on Terraform, any cloud providers (besides AWS), or any other infrastructure setup. The Terraform scripts and infrastructure setup outlined in this guide are purely for Xiid Sandbox testing purposes.

Do not use these scripts to build a production domain.

What You Will Need

Contact Xiid Before Continuing

We'd love to help you get started with a sandbox! Unless we've already been in touch, please talk to us before continuing to get the required Xiid software and automated deployment scripts.

The following are required for using the Xiid Domain Sandbox Tools for an AWS deployment:

1. An AWS Account
2. An Xiid Domain Sandbox Tools package

If you wish to use a different cloud provider (Azure, GCP, XetaOne, etc.), Xiid will help you provision the sandbox for that environment.

Infrastructure Costs

Sandbox Infrastructure Is Not Free

Xiid is not responsible for any costs incurred by following this guide and using the Sandbox Domain.

Please be aware of the costs associated with standing up infrastructure in AWS. You can refer to the AWS Pricing Guide for more information regarding costs.

Please consider that the region you deploy your infrastructure in will also affect the cost. Also, the length of time that you leave your infrastructure running may affect costs.

To reduce costs of running your infrastructure in AWS, you can use "free-tier" infrastructure, which the automated sandbox deployment scripts attempt to choose by default. You may also stop the sandbox instances and resources when you are not using them to save money.

Sandbox Deployment

Environment Setup

DANGER

Sandbox deployment scripts should not be used in production or for scaffolding infrastructure to be used in production.

To create and use an Xiid Sandbox Domain, you will need to set up your computer and AWS account with the appropriate tools and configurations necessary for the Sandbox deployment.

AWS CLI Setup

TIP

If using macOS, this step is not required. The macOS version of the Xiid Domain Sandbox Tools installs required dependencies automatically.

The **Amazon Web Services Command Line Interface (AWS CLI)** allows users to interact with AWS resources using the command prompt or terminal. The AWS CLI operates as the "engine" behind Terraform, driving the deployment commands to your AWS account.

Download the AWS CLI here, open the installer, and follow the prompts.

After the installation is complete, you can open a command prompt or Terminal window and run `aws`. If a list of available AWS commands is displayed, you have successfully installed the AWS CLI.

AWS IAM User Setup

For the **Xiid Domain Sandbox Tools** to be able to stand up and destroy Xiid Sandbox infrastructure in your AWS account on your behalf, you must generate an **IAM User** with the `AdministratorAccess` policy and have its associated `Access Key` and `Secret Key`, which will be used in future steps.

▶ **View Step-by-Step Instructions**

Later, after Xiid's scripts have finished deploying your infrastructure, you may (but are not required to) delete this IAM user. If you delete the IAM user, you must re-create it before tearing down the infrastructure.

If you choose to re-create the user, you will need to open a command prompt or Terminal window, run `aws configure`, and enter your new `Access Key` and `Secret Key` **before** running any infrastructure teardown commands or scripts.

Script-Based Sandbox Deployment

The following steps will help you get your workspace and infrastructure set up and deployed correctly.

Start by obtaining the **Xiid Domain Sandbox Tools** zip file from Xiid and unzipping it in a safe location.

Infastructure Deployment

WARNING

Make sure to follow these steps on the computer you're going to deploy the sandbox from.

Windows Point-and-Click:

Double-click the `deploy_sandbox.bat` file to deploy your sandbox environment to AWS.

Please note that if you choose this option, you are accepting the default values for `ip_address` and `deploy_region` which are `0.0.0.0/0` and `us-west-1` respectively.

Command-Line Deployments:

TIP

On macOS, the script will automatically prompt you to install required dependencies. On Windows and Linux, Terraform must be installed along with the AWS CLI.

From a command prompt or Terminal window, navigate to the installer directory and run the following command:

Windows macOS Linux

batch

```
deploy_sandbox.bat
```

By default, the values for `ip_address` and `deploy_region` are `0.0.0.0/0` and `us-west-1` respectively.

If you wish to customize these, you can specify one or more of several flags to the Sandbox deployment scripts, but these **must be provided in order and none may be skipped**:

- `ip_address`: The IPv4 IP Address to restrict RDP access to only your computer.
- `deploy_region`: The region to deploy your infrastructure in.
- `rdp_count`: The number of RDP Instances to deploy in your infrastructure.

As an example, a custom deploy command with arguments would look like:

Windows macOS Linux

console

```
deploy_sandbox.bat 0.0.0.0/0 us-west-2 3
```

While Running the Sandbox Tools:

While running the sandbox deployment script for your operating system, you will be prompted for your `Access Key` and `Secret Key`. Enter those values obtained during AWS IAM User Setup. You can hit enter to skip the prompts for region and output format.

Several Terraform commands will be run under the hood, and some will require your confirmation.

When prompted that there are **Plans to Add**, enter `yes` to execute the infrastructure deployment.

After your infrastructure has been provisioned, you will see an **Apply complete!** or **press any key to continue...** message.

DANGER

Do not delete, modify, or move the `terraform.tfstate` or `terraform.tfstate.backup` files generated during deployment. These files are used by Terraform to keep track of the infrastructure you just deployed and are necessary to tear it down when you are finished using it.

Infrastructure Validation

After provisioning, it will usually take a few minutes for the resources to be fully booted-up and available.

Although the deployment scripts are reliable, you can manually verify that the infrastructure is fully stood up and ready to go.

▶ **View Step-by-Step Instructions**

If you encounter any issues with deployment, let us know.

Manual Sandbox Deployment

If you do not wish to use the automated scripts, you can use Terraform directly to deploy your sandbox environment.

▶ **View Step-by-Step Instructions**

Infrastructure Tear Down

WARNING

If you lost the `terraform.tfstate` or `terraform.tfstate.backup` files, you will not be able to automatically tear down your infrastructure and must manually delete the infrastructure from the AWS Console.

Windows

When you are done using your Sandbox and would like to tear it down, double-click the `destroy_sandbox.bat` file that was generated when running the `deploy_sandbox.bat` script.

Terraform will print a destruction plan for your resources. Enter `yes` to execute the tear down.

macOS and Linux

On macOS and Linux, instructions for infrastructure teardown are outputted to a file named `cleanup_instructions.txt`.

Following the simple instructions in the text file should successfully de-provision resources used for the Xiid Sandbox.

Using the Sandbox

What You Can Do

At a minimum, your Sandbox contains a Domain Controller and an RDP Instance.

With these, you should be able to try out the following:

- Install and configure an Xiid IM Agent with LDAP
- Enable XOTC Authentication for Single Sign-On Users
- Set up Traditional RDP Access to a Remote Machine
- Set up SealedTunnel Access to a Remote Machine
- Set up a Google Workspace Application in your SSO Portal
- Set up an Office 365 Application in your SSO Portal
- Set up a SAML2.0 Application in your SSO Portal

While configuring these various pieces of the Sandbox, you'll likely need the following key information on the Sandbox infrastructure, including basic usage instructions and the **default user account names and passwords**.

Domain Controller

Information

The **Sandbox Domain Controller** comes pre-installed with a number of users and groups in **Active Directory**. We encourage you to create any users and groups that you wish, as Xiid has only provided basic defaults.

TIP

Although the Sandbox infrastructure should never be used in production, Xiid highly recommends that you change the passwords associated with all users on the Domain Controller for maximum security.

What Is the Domain Controller?

The Domain Controller is an out-of-the-box Windows 2019 Server.

The Domain Controller has had Active Directory Services installed and has been promoted to a Domain Controller as a new domain forest.

The domain name is `sandbox.local`.

The Domain Controller is **not** a DNS Server. If you would like to promote your Domain Controller to a DNS server, you can do so after deploying the Sandbox Domain. Be aware that you will need to reconfigure your DHCP Options Set in AWS and you will need a domain name from a trusted Certificate Authority.

Users

There are a number of users created by default in the Sandbox Domain.

User	Description
`sandboxadmin`	The administrator account for the Sandbox Domain
`xiid-svc`	Standard service account for use by the Authenticator component in your Xiid Agent with a default password of `Cyb3r$3cur!ty`
`sandbit`	Short for SandboxIT, this is an example IT User on your domain, who may need access to an RDP instance not available to the broader company
`sandboxengineer`	Example engineer User on your domain, who may need access to a shared VS Code repository on an RDP instance
`sandboxuser`	Example of a general user on your domain, only in the `SandboxAll` Security Group.

The `sandbit`, `sandboxengineer`, and `sandboxuser` accounts are disabled by default and passwords are not provided. To use these users, open **Active Directory Users and Computers**, re-enable each account, and set a password for them.

Groups

A few basic Security Groups are created for you and the users listed above are organized into these basic groups to facilitate access management examples.

Group	Description	Members

`SandboxAll`	Security Group for all users in the `sandbox` OU	`sandbit`
		`sandboxengineer`
		`sandboxuser`

`SandboxEngineering`	Example Security Group for an Engineering Organization, recommended to use with the VS Code application utilizing the `RDP App` Application in the Xiid Agent Management Portal	`sandboxengineer`
`SandboxIT`	Example Security Group for an IT Organization and a useful group for demonstrating restricted RDP access to IT	`sandbit`

Usage

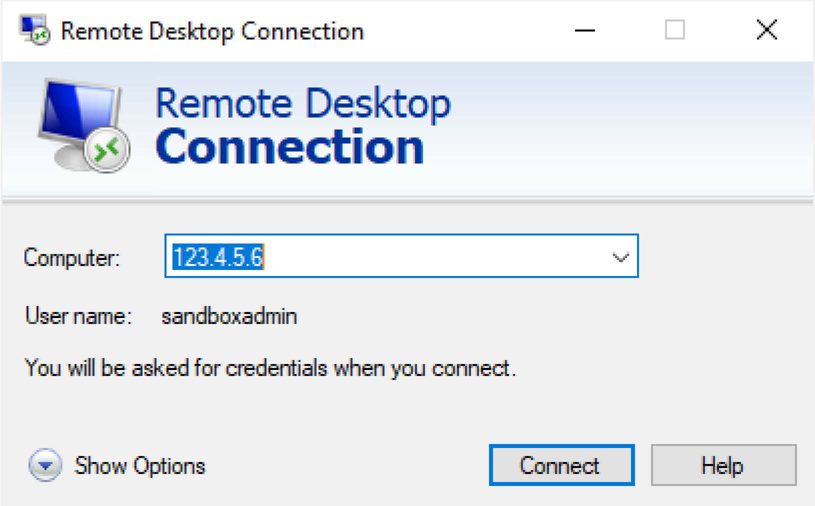
Here is how to access your newly-deployed Domain Controller:

Windows

Navigate to the AWS EC2 Console, find your Domain Controller, and copy the `Public IPv4 Address`.

Paste the IP Address into an RDP connection file (`.rdp`) or into the RDP application of your choosing.

There is also a `domain_controller.rdp` file available to use in the Sandbox Tools. Right-click the file in Windows File Explorer, click `Edit`, enter the Public IPv4 Address copied above into the `Computer` section, and click **Save** (under **Show Options**).



Computer: 123.4.5.6

User name: sandboxadmin

You will be asked for credentials when you connect.

macOS and Linux

The `domain_controller.rdp` file was automatically updated to use your new domain controller's IP address during deployment, so you may use the file without further modification.

Connecting to the Domain Controller via RDP

Double-click the `domain_controller.rdp` file and use the following credentials to connect.

Domain Controller Admin Credentials:

- **Username:** `sandboxadmin`
- **Password:** `4CcXL!#X%JeU9@`

We recommend that you change the `sandboxadmin` User's password after logging in for maximum security.

After you log in to the instance, you can check **Active Directory Users and Computers** to view the default users and groups.

The Xiid Active Directory Agent installer is already available on the desktop, just double click to start the installation process.

RDP Instance

Information

The RDP Instance is a Windows 2019 Server and comes with a default Administrator user (`rdpuser`) and VS Code pre-installed.

Usage

Here is how to access your newly-deployed RDP Instance:

Windows

To access your Sandbox RDP instance, start by navigating to the EC2 Console in AWS, select the **Instances** tab on the left, find the `SandboxRDP` Instance, and copy the **Public IPv4 Address**.

In your `sandbox` folder, right-click the `rdp_instance.rdp` file and click **Edit**.

Enter the IPv4 Address that you just copied in the `Computer` section and click **Save** (under **Show Options**).

macOS and Linux

The `rdp_instance.rdp` file was automatically updated to use your RDP instance's IP address during deployment, so you may use the file without further modification.

Connecting to the RDP Instance via RDP

> **TIP**
>
> As part of testing Xiid in a Sandbox, you'll likely want to close all inbound ports to this RDP Instance and make it only accessible via the SealedTunnel. For now, you'll need to use these credentials and traditional RDP to initially access the machine and, later, to configure the SealedTunnel.

Double-click the *rdp_instance.rdp* file and enter the password below to connect.

RDP Instance Admin Credentials:

- **Username**: `rdpuser`
- **Password**: `Cyb3r$3cur!ty`

Advanced Features

Below are some advanced configuration and usage information. If you are familiar with AWS and Terraform, you can use the following information to make custom changes to the scripts to cater to your specific use case(s).

Script Configuration

You can customize the following aspects of the `main.tf` Terraform script to cater your infrastructure to your preferences. Below are some common modifications to the script:

- **Instance Type:**
  - You can configure the instance types for your Domain Controller and RDP instance, if you would like faster hardware to run your sandbox domain.
  - Modify the instance type on Line `97` (for the Domain Controller) and Line `111` (for the RDP instance) to any of the Amazon Standard Instance Types.
  - **Note:** Changing the instance type may incur additional charges from AWS. Please consult the AWS Pricing Guide for more information.
- **Disk Space:**
  - You can configure the amount of disk space provisioned for your instances.
  - To change the disk space on the Domain Controller, modify the value on line `101`. To modify the RDP instance disk space, modify the value on line `115`.
  - **Note:** Changing the amount of partitioned disk space may incur additional AWS charges.