ZSCALER AND IGEL DEPLOYMENT GUIDE

NOVEMBER 2024, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PRA	Privileged Remote Access
RDP	Remote Desktop Protocol
PSK	Pre-Shared Key
SaaS	Software as a Service
SSH	Secure Shell
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VNC	Virtual Network Computing
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

IGEL Overview

In the age of remote and hybrid work, organizations are increasingly relying on virtual desktop infrastructure (VDI) and cloud workspaces to ensure flexible, secure, and cost-effective digital environments. However, effectively managing many endpoint devices across dispersed locations introduces significant operational and security challenges. Addressing these challenges requires solutions that simplify IT management, strengthen endpoint security, and streamline access to digital workspaces.

IGEL Technology has developed robust solutions for endpoint management and secure access to cloud workspaces. Through its innovative IGEL OS, endpoint management suite, and strategic alliances, IGEL has redefined how organizations approach digital workspaces.

Today, IGEL's primary offerings enable secure and simplified management of endpoint devices for organizations adopting VDI and cloud workspace solutions. Headquartered in Bremen, Germany, with offices in Europe, North America, and APAC, IGEL serves thousands of customers in industries such as healthcare, finance, government, and education. To learn more, refer to IGEL's website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- IGEL Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the following versions of the Zscaler and IGEL software.

ZIA 6.2

- Isolation
- Privileged Remote Access

IGEL OS 12.5.0

- Chromium Browser 127.0.6533.99 BUILD 1.0
- Edge Browser 128.0.2739.79 BUILD1.0
- Firefox Browser 115.12.0 BUILD 2.0

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and IGEL Introduction

Overviews of the Zscaler and IGEL applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Isolation Solution Overview

Isolation is a key component of Zscaler's Zero Trust Exchange that is designed to protect users from web-based threats by isolating their browsing activity in a remote, cloud-based environment. Instead of loading web content directly on the user's device, Isolation renders the content in a secure virtual browser within the Zscaler cloud and streams a safe version back to the user. This helps prevent malware, ransomware, and other malicious content from reaching the endpoint, and can address key data protection use cases faced by organizations today. Isolation does not require the Zscaler Client Connector so can be used by anyone with a modern browser.

Key features of Zscaler's Isolation include:

- Cloud-Based Isolation: The entire browsing process happens in the cloud, reducing the endpoint's exposure to threats.
- Protection Against Advanced Threats: By isolating sessions, it mitigates risks from phishing, malicious downloads, and zero-day vulnerabilities.
- Seamless User Experience: Provides interactive, near-native web experiences without the lag or limited functionality sometimes associated with traditional browser isolation.
- Granular Policy Controls: IT teams can set detailed policies to control browsing permissions, download capabilities, and more, depending on user roles or threat levels.
- Easy Integration: Works seamlessly with Zscaler's cloud security platform, allowing centralized management and consistent policy enforcement across the organization using any modern browser.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Privileged Remote Access Solution Overview

Zscaler's Privileged Remote Access (PRA) is a clientless remote desktop gateway component of ZPA that enables end users to securely connect to servers, jump hosts and bastion hosts, or desktops using Remote Desktop Protocol (RDP), Secure Shell (SSH), or Virtual Network Computing (VNC) from an end user's modern browser without installing Zscaler Client Connector or any browser plugins. PRA allows you to provide third parties (vendors, contractors, suppliers), IT administrators, and remote employees, controlled access to your privileged servers and applications.

PRA allows an admin to set up specific end users for certain privileged consoles with policies for a fixed time frame. You can also choose to provide configured credentials for short-term end users, or prompt end users to enter their credentials when using a privileged console. These PRA features provide secure, user-friendly access while also limiting the end user's access only to what is needed, when, and for a duration of time.

The PRA service includes the following key components:

- Privileged Portals
- Privileged Consoles
- Privileged Approvals
- Privileged Credentials
- Privileged Policies
- Privileged Application Segments
- Diagnostics

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Isolation Help Portal	Help articles for Isolation.
Understanding Privileged Remote Access	Help articles for PRA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Isolation Help Portal	Help articles for Isolation.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

IGEL OS Overview

IGEL OS is a Linux-based operating system designed specifically for secure, efficient, and manageable access to virtual desktops and cloud workspaces. It's lightweight, highly secure, and optimized for endpoint devices such as thin clients, desktops, and laptops. IGEL OS is particularly popular in environments where organizations rely on virtual desktop infrastructure (VDI), desktop-as-a-service (DaaS), and cloud-based applications.

Key features:

- Lightweight and Secure: IGEL OS minimizes the attack surface with a read-only file system, making it less vulnerable to malware.
- Centralized Management: It includes IGEL Universal Management Suite (UMS) for easy remote management of thousands of endpoints, enabling simplified updates, policy enforcement, and troubleshooting.
- Broad Compatibility: It supports major VDI and DaaS providers, such as VMware, Citrix, Microsoft, and Amazon WorkSpaces.
- Fast Boot Time: Because it's resource-efficient, devices boot quickly, ensuring minimal downtime and optimal user experience.

IGEL Resources

The following table contains links to IGEL support resources.

Name	Definition
IGEL Knowledge Base	Help articles for IGEL OS.
IGEL OS Product Page	Information about IGEL OS.

Solution Overview

IGEL OS and Zscaler work together to provide a streamlined approach to empowering browser-based productivity from secure employee and contractor endpoints. The IGEL OS, a lightweight and secure operating system, offers a robust platform upon which to access Zscaler's Isolation and PRA solutions. This interoperability delivers a secure, Zero Trust-oriented endpoint enabling streamlined access to SaaS or private apps, and remote desktops, servers, or devices. This all happens from the user's browser of choice without the need for traditional VDI infrastructures or expensive local OSs.

The IGEL OS rethinks the need for a heavy, vulnerable OS running on a pricey laptop. The secure endpoint OS is tailored to work in modern, cloud-centric environments, for full productivity that maximizes use of a local, thin client compute model. IGEL OS natively offers its Preventative Security Model to stop attacks and malware on the endpoint while preventing data from reaching the local machine.

You can access Zscaler Isolation and PRA using the user's browser of choice on endpoints with the IGEL OS. It directly connects users to the SaaS and private apps, and private consoles, needed for productivity. Not only does Zscaler connect users to apps but does so protecting data with browser-based data controls to stop actions like uploads and downloads, or printing. Zscaler data protection also ensures sensitive data is never accidentally shared or compromised via the browser.

Zscaler Isolation and PRA with IGEL OS Interoperability

The following sections describe how to use Zscaler Isolation and PRA with IGEL OS.

PRA Use Case

An IGEL OS user must securely access a Linux system for troubleshooting. The system is only accessible through Zscaler's Zero Trust Exchange (ZTE), which provides a Privileged Console allowing SSH access. The user does not need to have the Zscaler Client Connector but can use a standard web browser.

1. Log in to the IGEL OS 12 desktop.
2. Install browsers, if needed, via the IGEL App Portal.

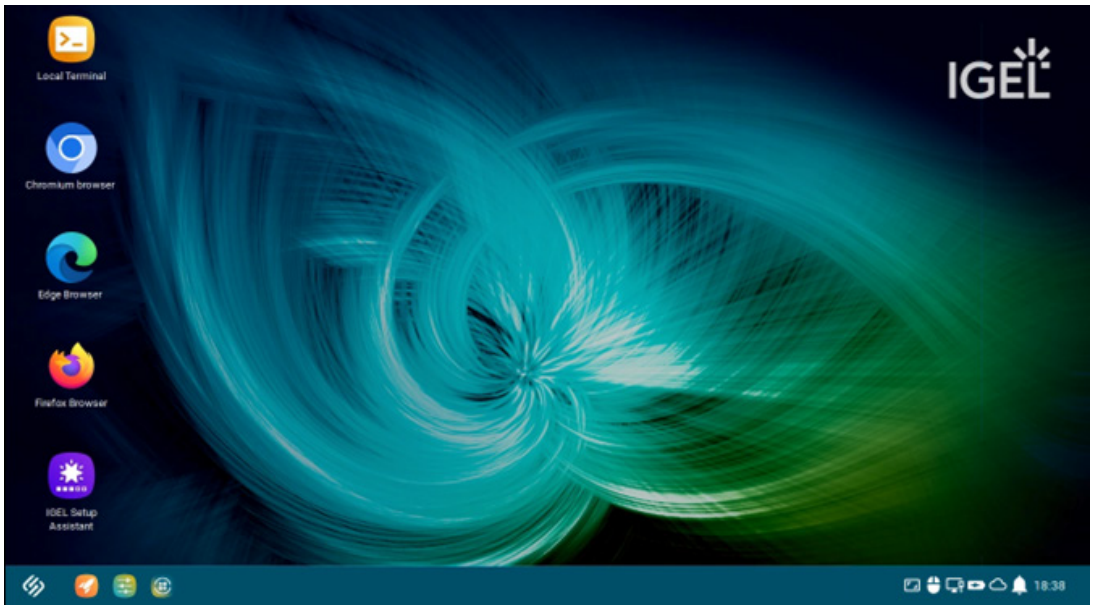

Figure 1. IGEL OS Desktop (PRA)

3. Open a browser and enter the **URL** of your PRA user portal. You are immediately redirected to authenticate to the PRA user portal.

4. Enter your **Username** and click **Sign in**.

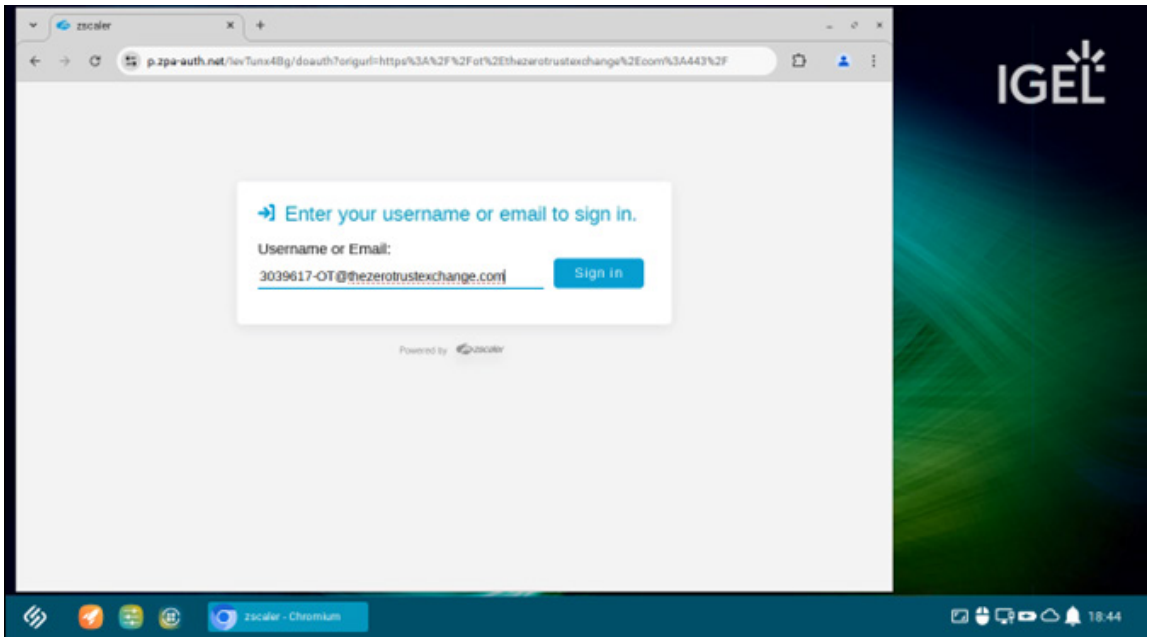

Figure 2. PRA Portal sign in

5. Enter your **Password** and click **Sign In**. You might need to re-enter your username.

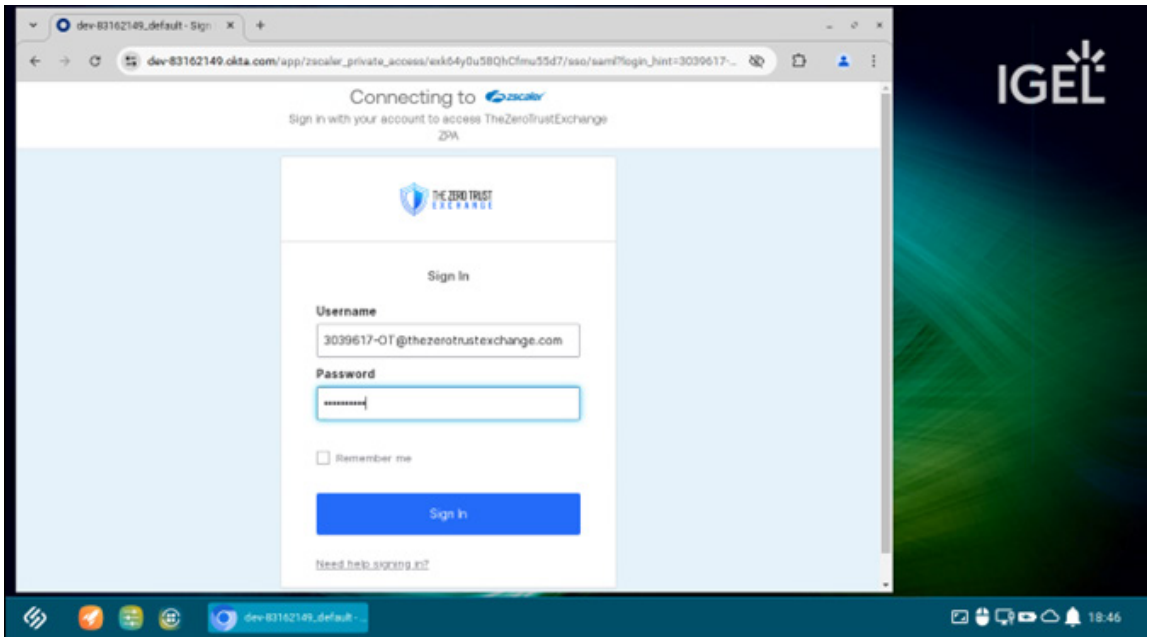

Figure 3. PRA Portal password

After successfully authenticating, you are presented with the consoles to which your user has access. By clicking a console tile, you can make an SSH, RDP, or VNC connection to that system's login window to enter credentials for access.

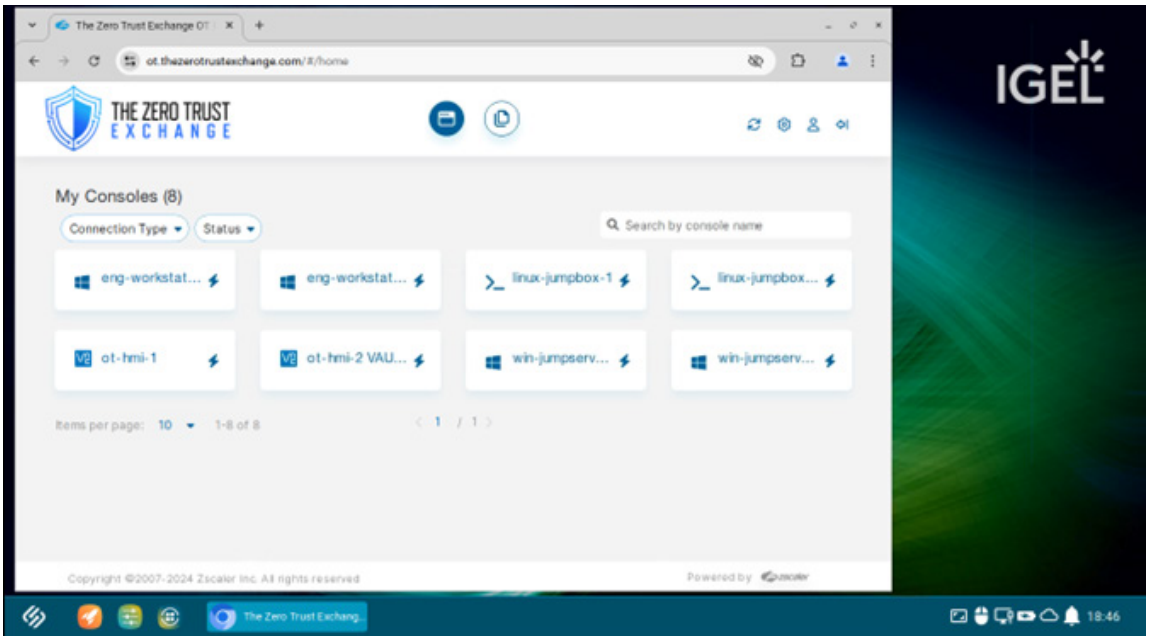

Figure 4. PRA Portal Consoles

In the following example, the user makes a connection to a Linux jumpbox via SSH. When the user no longer requires access, they can either exit the Linux shell or click the **Disconnect** icon in the upper right-hand corner to disconnect from the session.

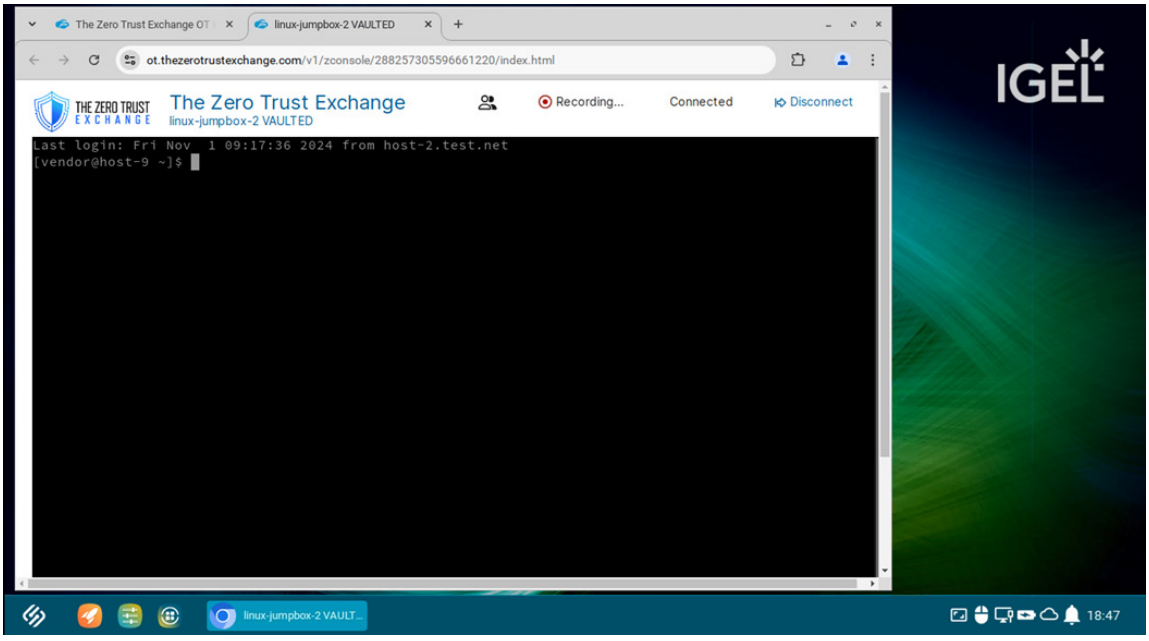

Figure 5. Privileged SSH Console

Isolation Use Case

Users of IGEL OS must access their email on M365. Their company's email is only accessible when going through Zscaler's ZTE. They typically access their email from their laptop which has Zscaler Client Connector installed but now have a need to access it from an IGEL OS thin client. Their company provides access via Isolation for cases like this where they can access their email via Isolation using a standard web browser.

1. Log in to the IGEL OS 12 desktop.
2. Install browsers, as needed, via the IGEL App Portal.

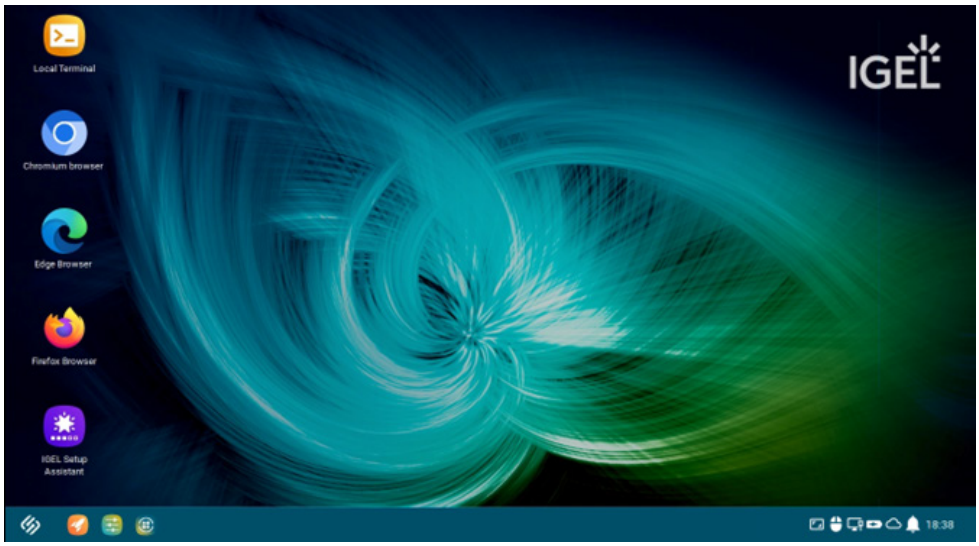

Figure 6. IGEL OS Desktop (Isolation)

3. Open a browser and enter the **URL** of the Isolation user portal. You are immediately redirected to authenticate to the Isolation user portal.
4. Enter your **Username** and click **Sign in**.

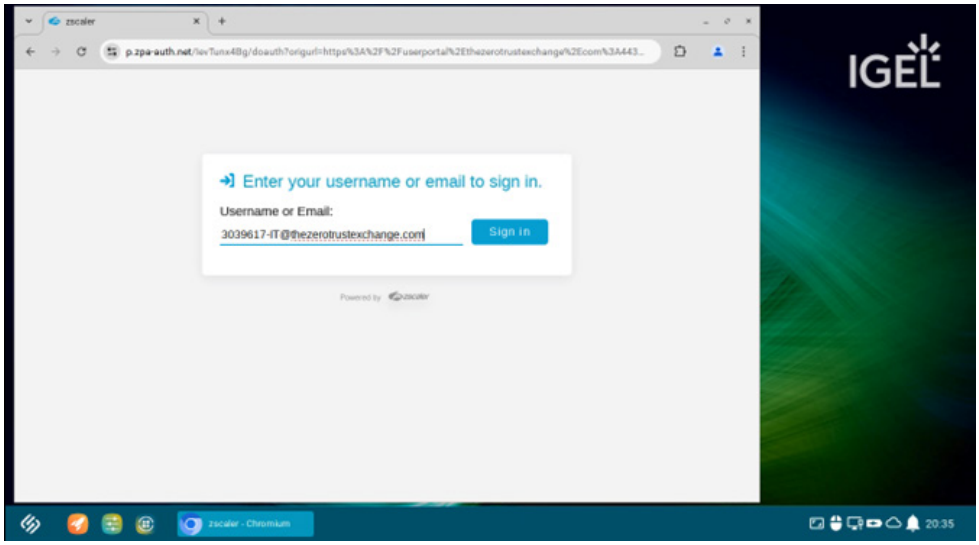

Figure 7. Isolation Portal sign in

5. Enter your **Password** and click **Sign In**. You might need to re-enter your username.

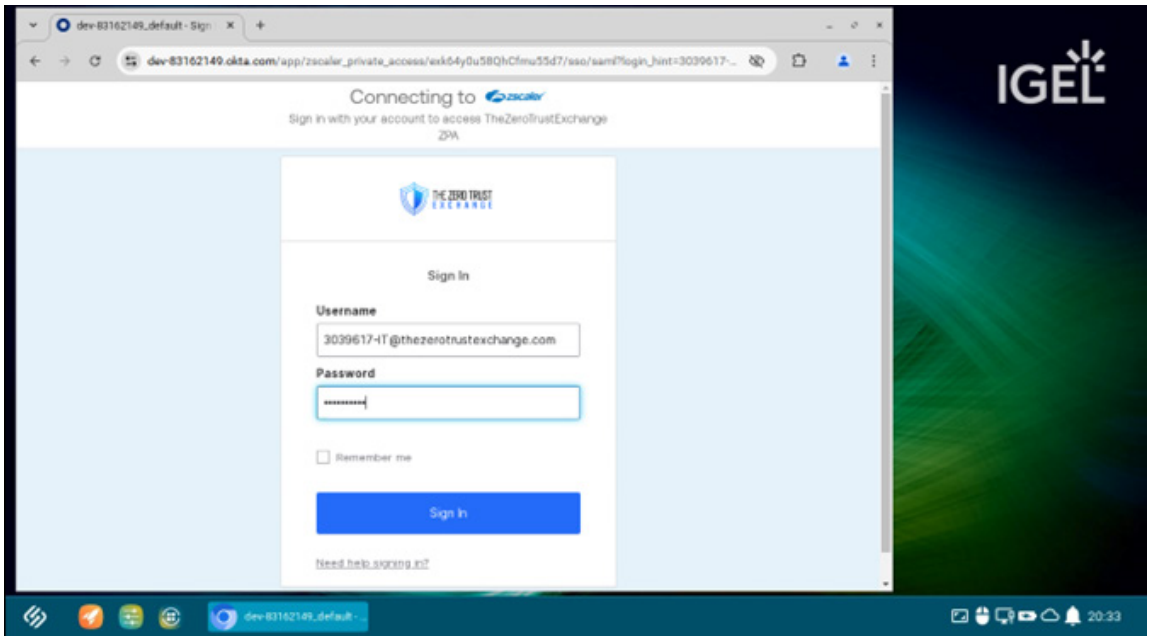

Figure 8. Isolation Portal password

After successfully authenticating, you are presented with the applications to which your user has access. By clicking an application tile, you make a connection to that application's login window through Isolation to enter credentials for access. In this example, the user clicked the M365 application tile.

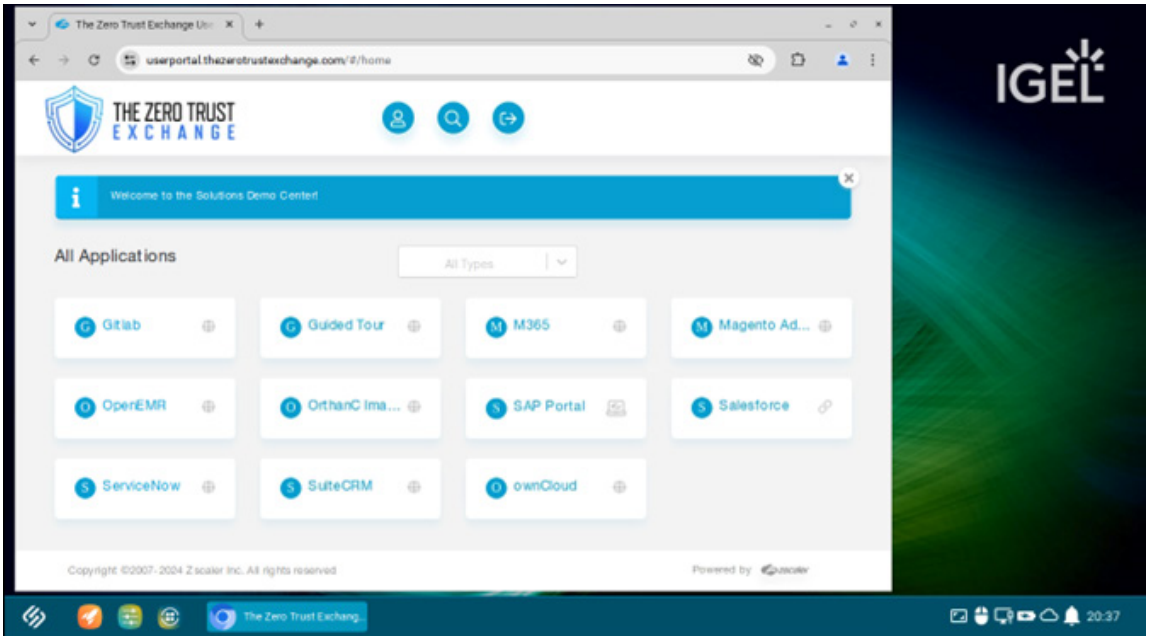

Figure 9. Isolation Applications

For this M365 application, Isolation has been configured to display a banner alerting the users that they are being redirected to Isolation.

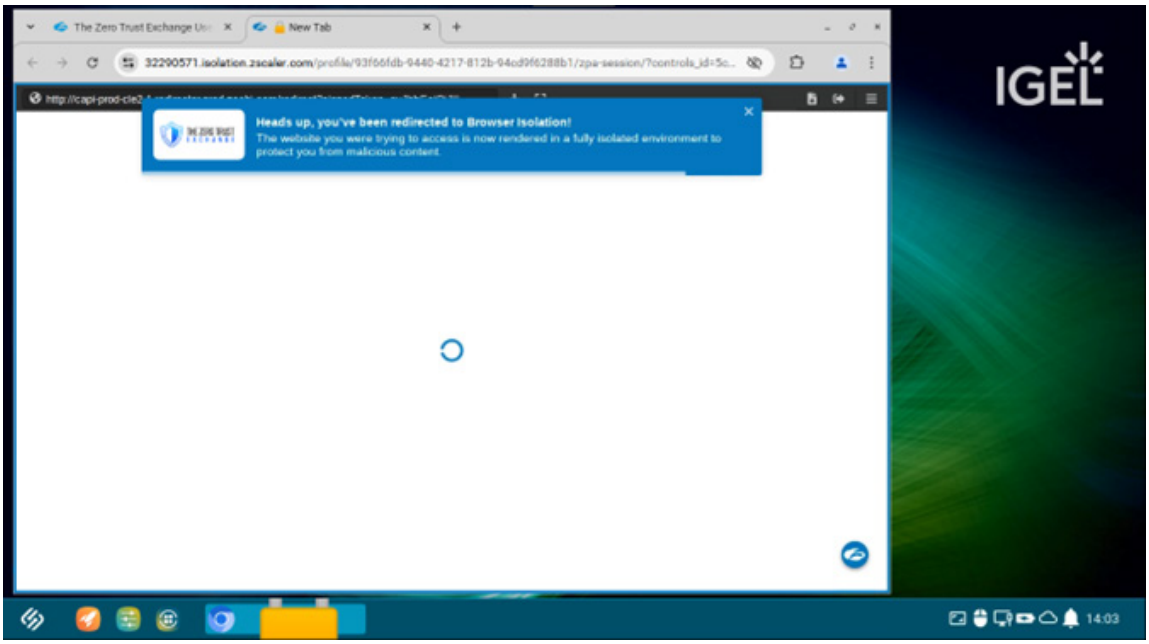

Figure 10. Isolation banner

In addition to the blue border there is also a watermark identifying this as an Isolation session. The user still must sign in to the application, as shown next.

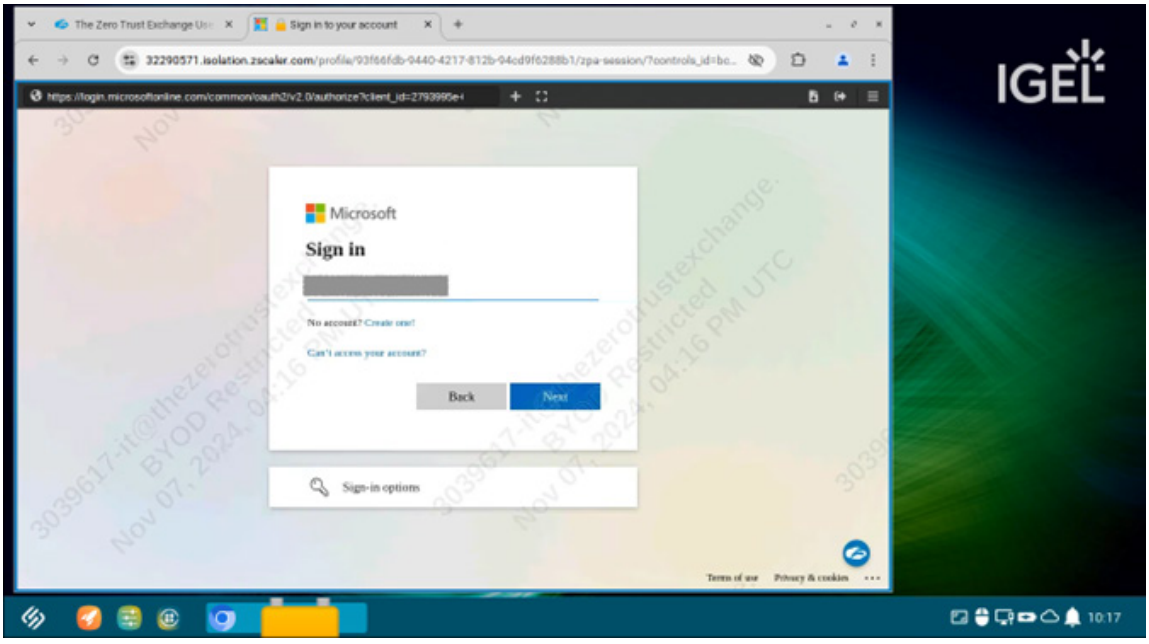

Figure 11. Isolation application login

The user must also enter their password.

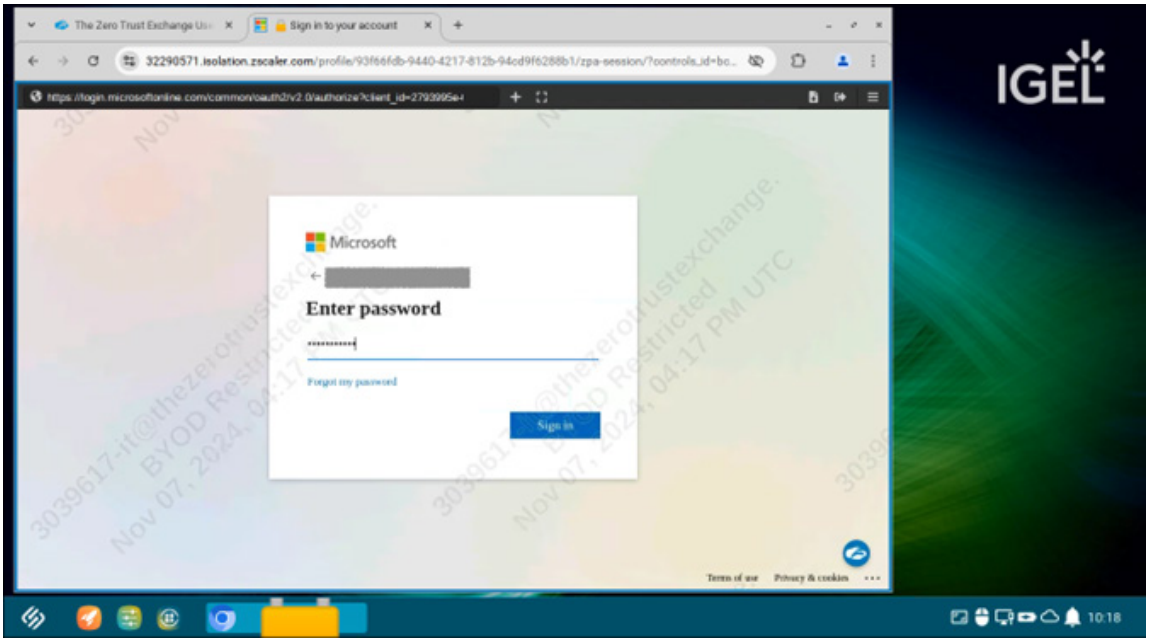

Figure 12. Isolation application password

When the user is done, they can either exit the application or click the **Disconnect** icon in the upper right-hand corner to disconnect from the session.

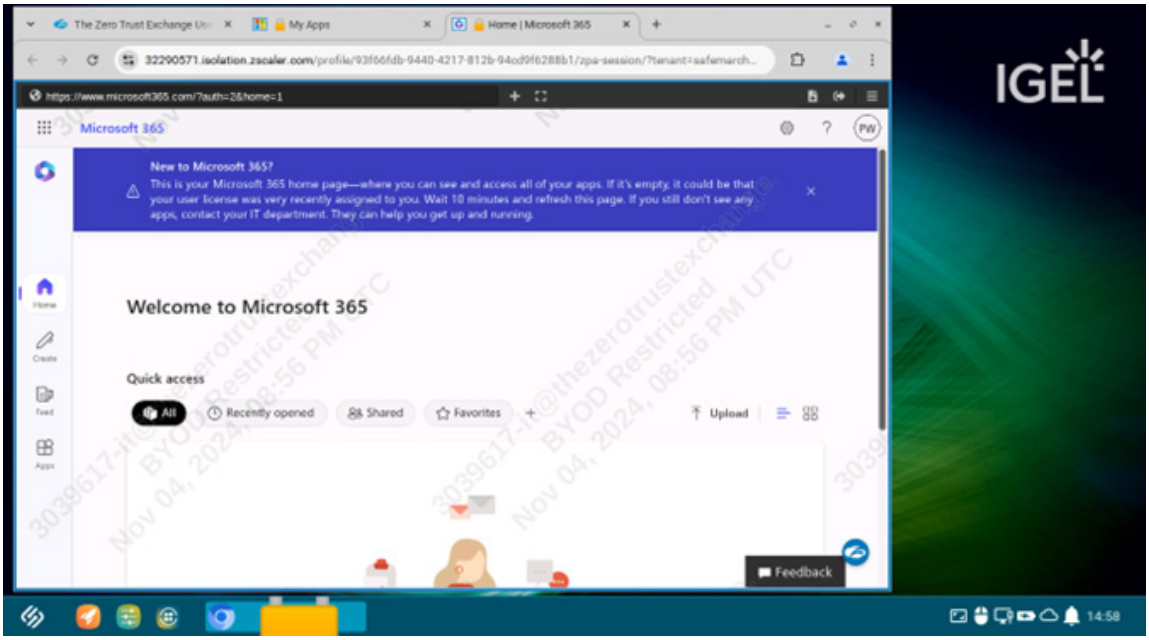

Figure 13. Isolation session

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

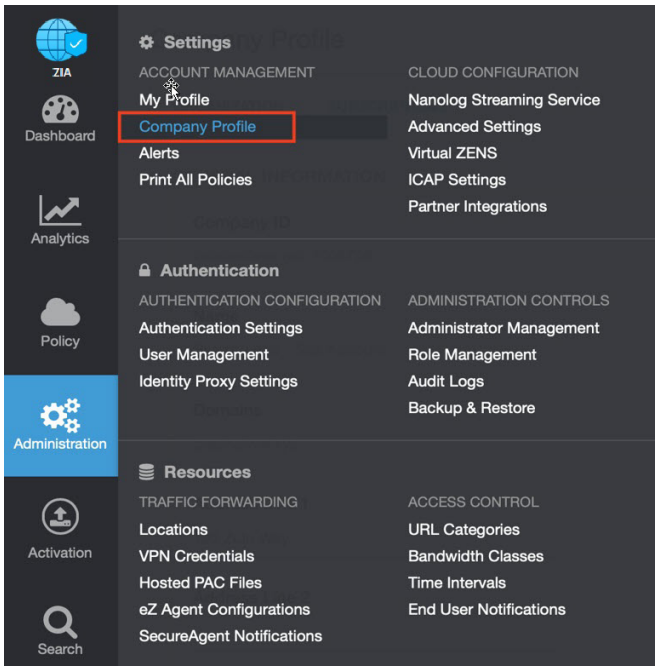

Figure 14. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

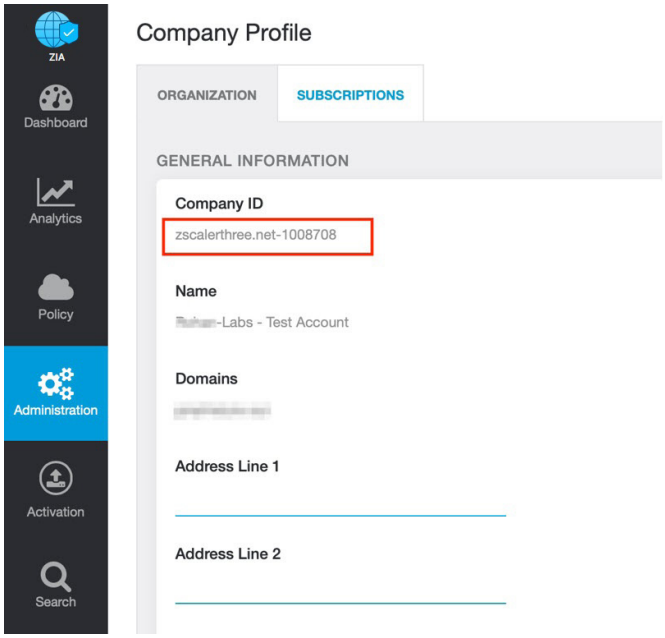

Figure 15. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

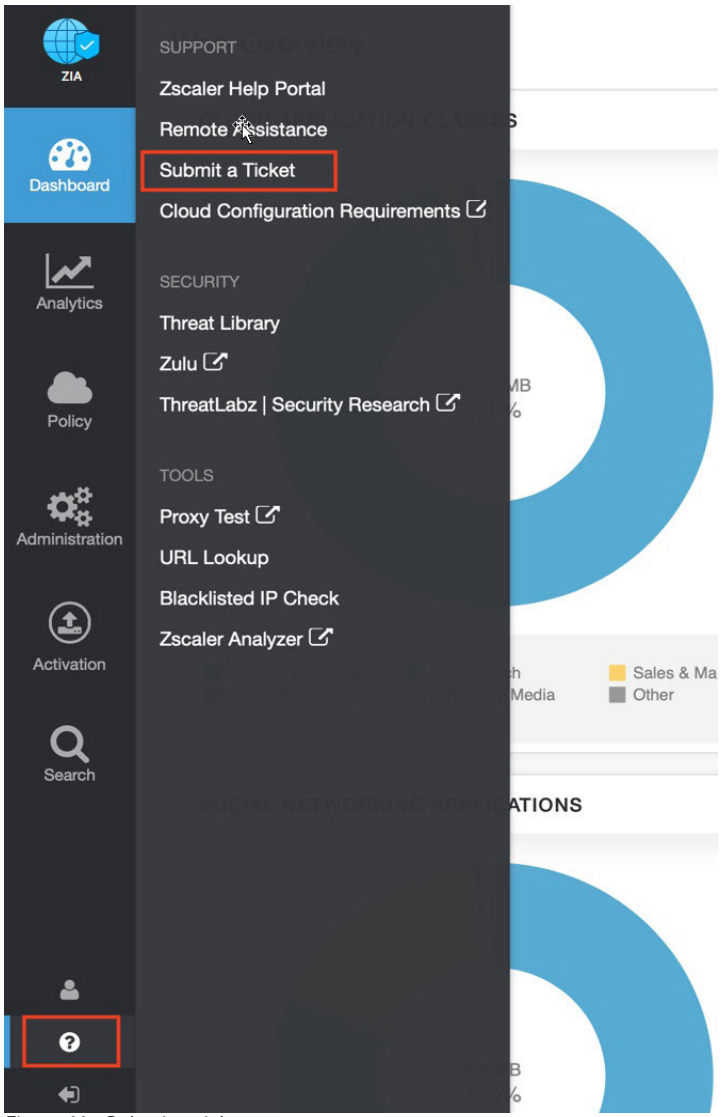

Figure 16. Submit a ticket

