ZSCALER AND IMPRIVATA DEPLOYMENT GUIDE

MARCH 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
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
IWA	Integrated Windows Authentication
MFA	Multi-Factor Authentication
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
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.

Imprivata Overview

Imprivata is a leading healthcare-focused technology company that specializes in providing innovative solutions for identity and access management in the digital healthcare landscape. Imprivata, who's first product came to market in 2004, has emerged as a key player in addressing the unique challenges of the healthcare industry, offering products and services designed to enhance security, efficiency, and workflow optimization. The company is renowned for its expertise in developing authentication and access management solutions, including single sign-on (SSO), multi-factor authentication (MFA), and identity governance. Imprivata's cutting-edge technologies aim to streamline healthcare professionals' access to critical patient information while maintaining rigorous security protocols, ultimately contributing to improved patient care and overall operational efficiency within healthcare organizations. To learn more, refer to Imprivata'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
- Imprivata Resources
- Appendix A: Integrated Windows Authentication
- Appendix B: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

Prerequisites

This guide does not explain how to install or configure the Zscaler or Imprivata solutions. It is expected that both Imprivata Enterprise Access Management (formerly OneSign) and Zscaler (ZIA and/or ZPA) are configured and deployed, and that Zscaler Client Connector is enabled and can perform SSO authentication on Windows.

This guide focuses on installing the Zscaler Client Connector that supports Imprivata (4.4 for Windows at the time of writing) for successful interoperability.

Requirements

Zscaler

- You must have Zscaler Client Connector 4.4 (at a minimum) for Windows to support the integration. (At the time of this writing it is in Limited Availability.)
- You must enable Integrated Windows Authentication (IWA) and configure it to provide SSO authentication for Windows users with Client Connector.
- The Zscaler Client Connector installation on the Imprivata Enterprise Access Management (formerly OneSign) shared workstation, with either the **EXE** or **MSI** packages, requires install options to enable the Imprivata integration.

Imprivata

- This integration is for Imprivata Enterprise Access Management (formerly OneSign) shared workstation environments only.
- You must enable the Single Sign-On feature for users in Enterprise Access Management (formerly OneSign) under User Policy.

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 Imprivata Introduction

Overviews of the Zscaler and Imprivata 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.

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.

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.
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.
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.

Imprivata Enterprise Access Management Overview

Imprivata Enterprise Access Management is a platform that makes authentication and access management simple. The Imprivata Enterprise Access Management platform is an affordable appliance-based solution that easily integrates strong authentication, application single-sign on, physical access control, and event reporting. Imprivata Enterprise Access Management delivers automated access management capabilities within a single easy-to-use administrative framework. The appliance-based approach dramatically decreases implementation time, infrastructure needs, and installation costs because there is no additional hardware or software to purchase, install, or maintain. Imprivata's scalable web service-based architecture gets you up and running easily, and distributed management and failover architecture ensure that your information follows you anywhere in the enterprise and is always available.

Imprivata Resources

The following table contains links to Imprivata support resources.

Name	Definition
• Imprivata Customer Experience Center	Imprivata online support and community support.

Zscaler Client Connector Install

The following sections describe how to install the Zscaler Client Connector in both EXE and MSI formats on the Imprivata Enterprise Access Management (formerly OneSign) shared workstation. While there are specific options required, the installation is otherwise standard. You can also use additional CLI options as needed. Currently the Zscaler icon does not display in the system tray, but you can access the Zscaler Client Connector through the Start menu.

EXE Installation Options

Per the Customizing Zscaler Client Connector with Install Options for EXE help page (government agencies, see Customizing Zscaler Client Connector with Install Options), the format of the command line options required to enable the Imprivata integration are:

```
--userDomain <your authentication domain>

--enableImprivataIntegration 1
```

Optional, but recommended, is:

```
--cloudName <your cloud name>
```

Government agencies can access the command information at:

```
--userDomain <your authentication domain>

--enableImprivataIntegration 1

--cloudName <your cloud name>
```


The following is an example for a tenant with the authentication domain of zs-bd.com, on the zscalertwo.net cloud:

```
Zscaler-windows-4.4.0.265-installer-x64.exe --cloudName zscalertwo
--userDomain zs-bd.com -- enableImprivataIntegration 1
```

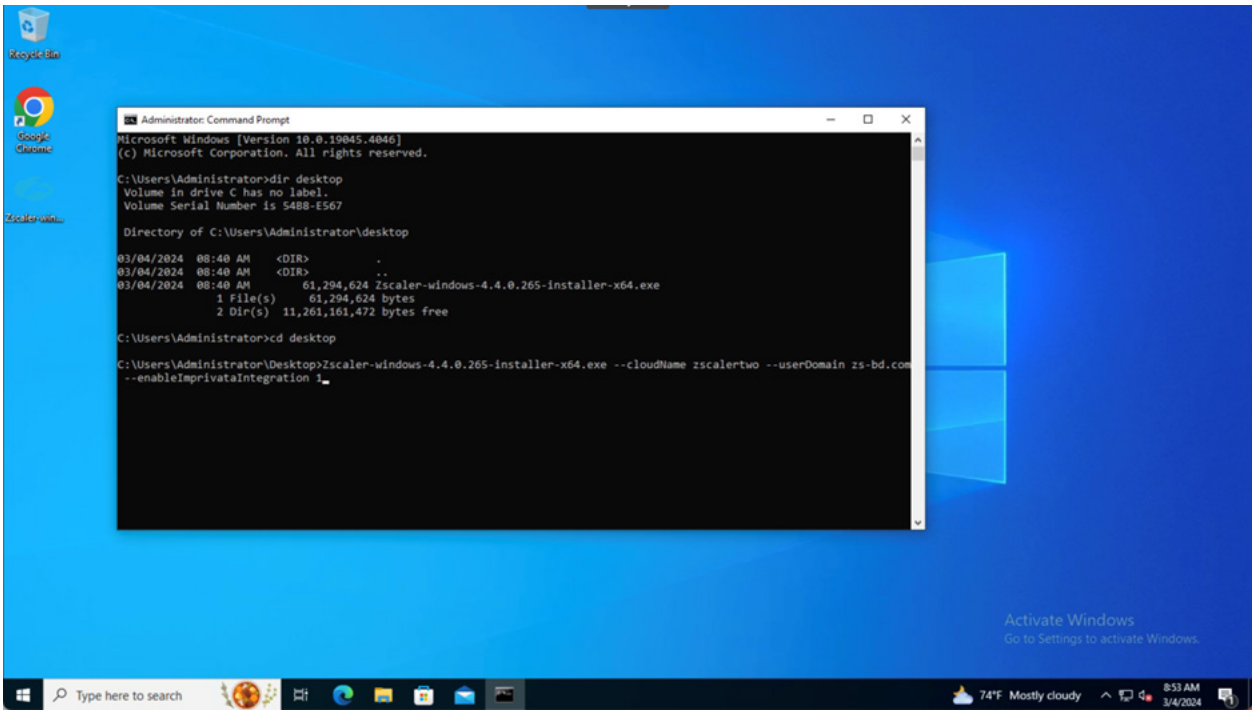

Figure 1. Zscaler Client Connector EXE package installation with options

MSI Installation Options

Per the Customizing Zscaler Client Connector with Install Options for MSI help page (government agencies, see Customizing Zscaler Client Connector with Install Options for MSI help), the format of the command line options required to enable the Imprivata integration are:

```
USERDOMAIN=<your authentication domain>

ENABLEIMPRIVATAINTEGRATION=1
```

Optional, but recommended, is:

```
CLOUDNAME=<your cloud name>
```

Government agencies can access the command information at:

```
USERDOMAIN=<your authentication domain>

ENABLEIMPRIVATAINTEGRATION=1

CLOUDNAME=<your cloud name>
```

The following is an example for a tenant with the authentication domain of zs-bd.com, on the zscalertwo.net cloud:

```
Zscaler-windows-4.4.0.265-installer-x64.msi CLOUDNAME=zscalertwo USERDOMAIN=zs-bd.com
ENABLEIMPRIVATAINTEGRATION=1
```

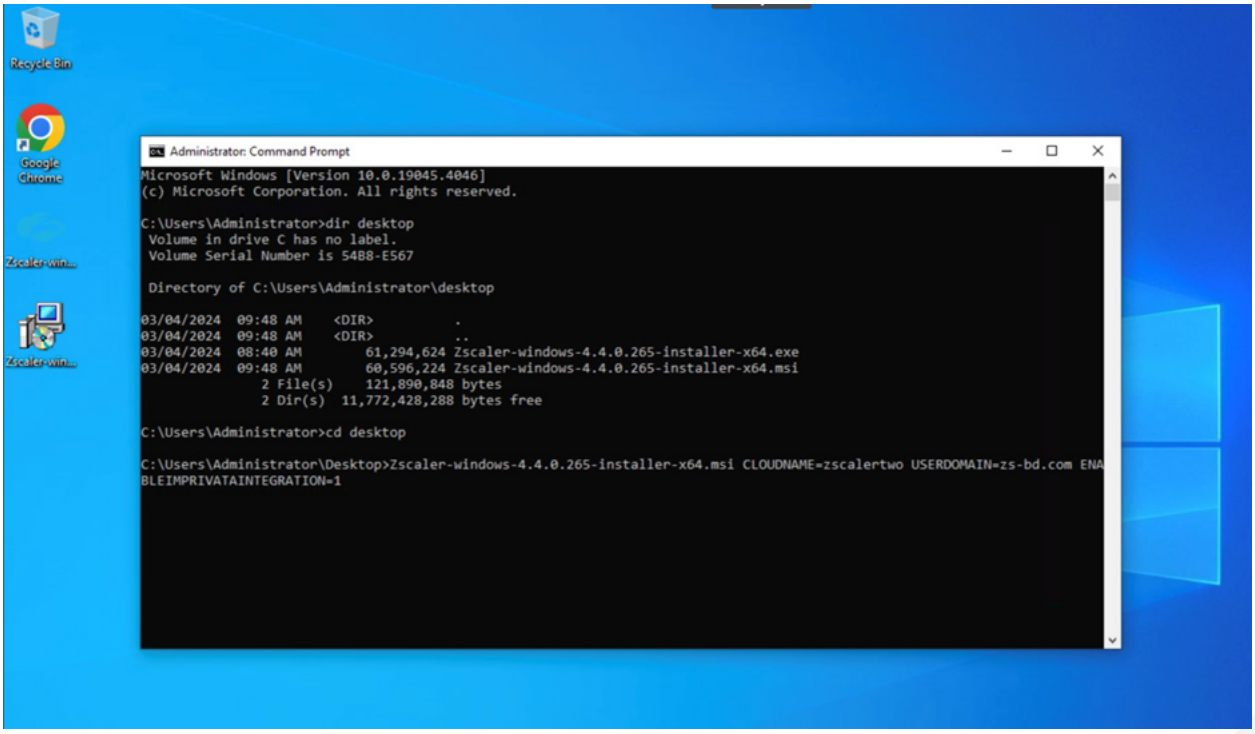

Figure 2. *Zscaler Client Connector MSI package installation with options*

Integration Example

When a user logs into the Imprivata Enterprise Access Management (formerly OneSign) shared workstation, the Zscaler Client Connector identifies the newly logged in user and transparently logs them in to the Zscaler service. This is independent of the service account user logged in to the underlying Windows operating system.

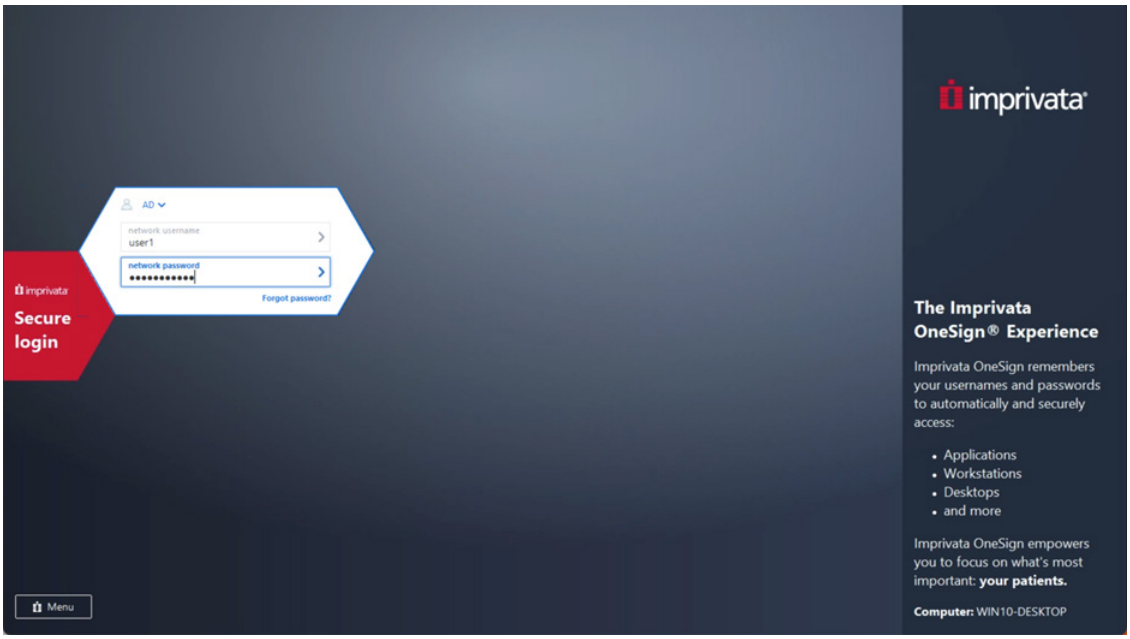

Figure 3. User 'user1' logging in to the Imprivata shared workstation

Looking at the connected user in Zscaler Client Connector, it is identical to the Imprivata user.

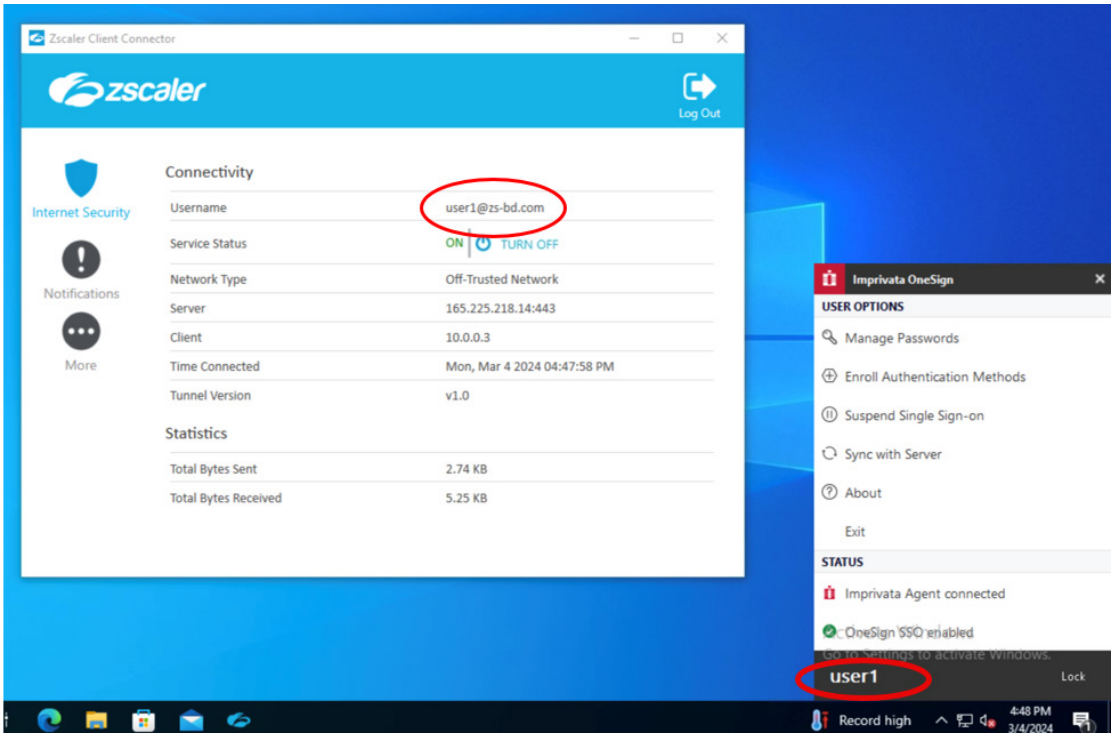

Figure 4. User 'user1' logged in to both Zscaler Client Connector and Imprivata

Logging in as another user, from a locked or exited session, also logs them in to the Zscaler service.

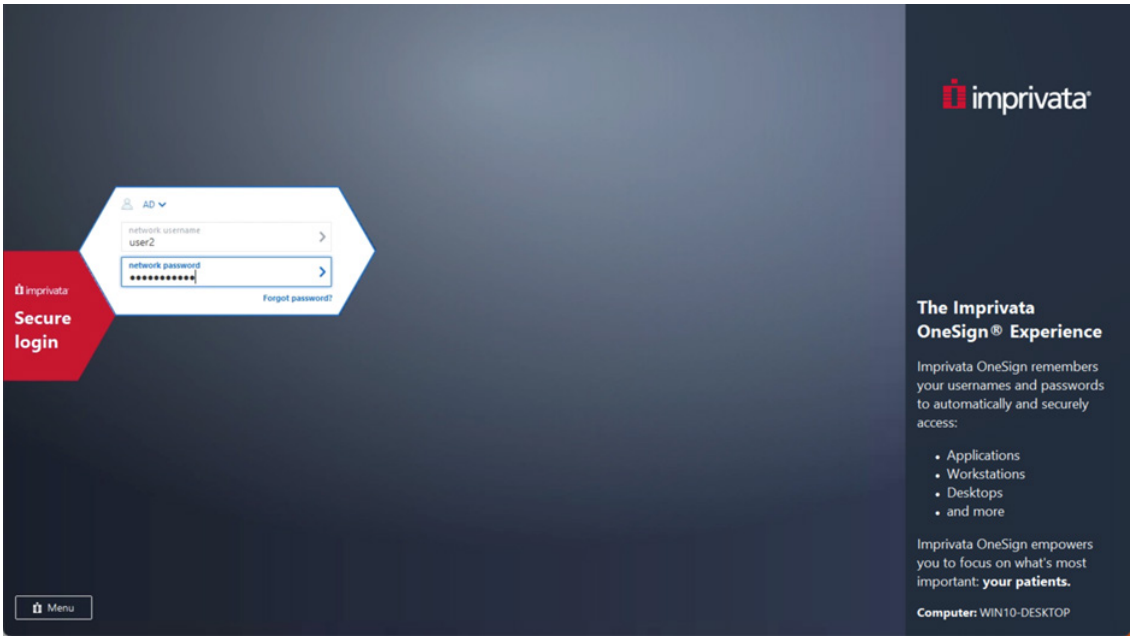

Figure 5. User 'user2' logging in to the Imprivata shared workstation

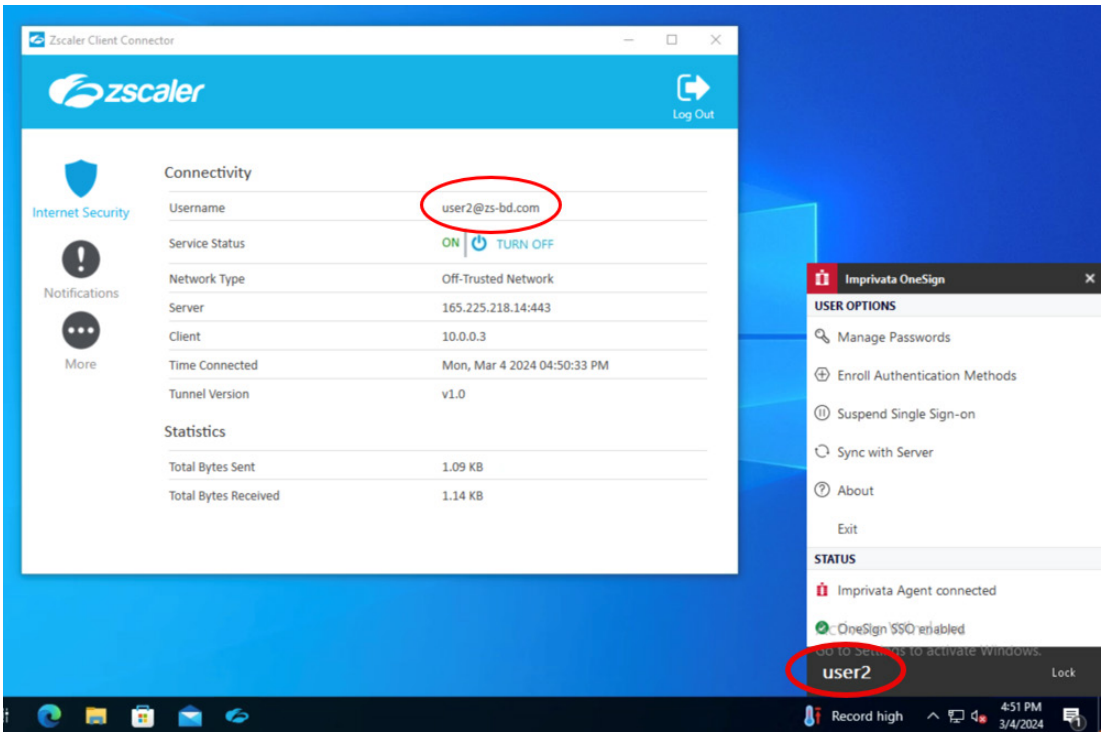

Figure 6. *User 'user2' logged in to both Zscaler Client Connector and Imprivata*

Appendix A: Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a Microsoft technology that allows you to automatically authenticate resources with SSO using Windows Active Directory authentication credentials.

Identity providers such as Entra ID (Azure AD) and Okta can use IWA to allow users to SSO into the Zscaler service. SSO provides a better user experience by automatically authenticating users with their Windows domain credentials without requiring the user to enter their password for a better user experience. Zscaler can take advantage of IWA if it is configured, but it is not a Zscaler feature or Zscaler configuration. IWA is configured between the Windows environment and the IdP.

To enable the Zscaler Client Connector to use IWA, two command line installation parameters are typically used:

```
--userDomain

--cloudName
```

Since IWA was originally designed to work in an intranet environment, you must add URLs as trusted sites in your intranet zone on your browser.

The **Microsoft Azure online documentation** provides detailed configuration options, including GPO options to push the browser settings.

It is important to add trusted domains because, by default, the browser automatically calculates the correct zone (either internet or intranet) from a specific URL. For example, `http://example/` maps to the intranet zone, whereas `http://intranet.example.com/` maps to the internet zone (because the URL contains a period).

Browsers don't send Kerberos tickets to a cloud endpoint, like the Azure AD URL, unless you explicitly add the URL to the browser's intranet zone. For example:

- Add `*.yourlogindomain.com` and `autologon.microsoftazuread-sso.com` to your browser's trusted intranet sites.

Okta provides an **IWA Troubleshooting Guide** that details how IWA works.

Appendix B: 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**.

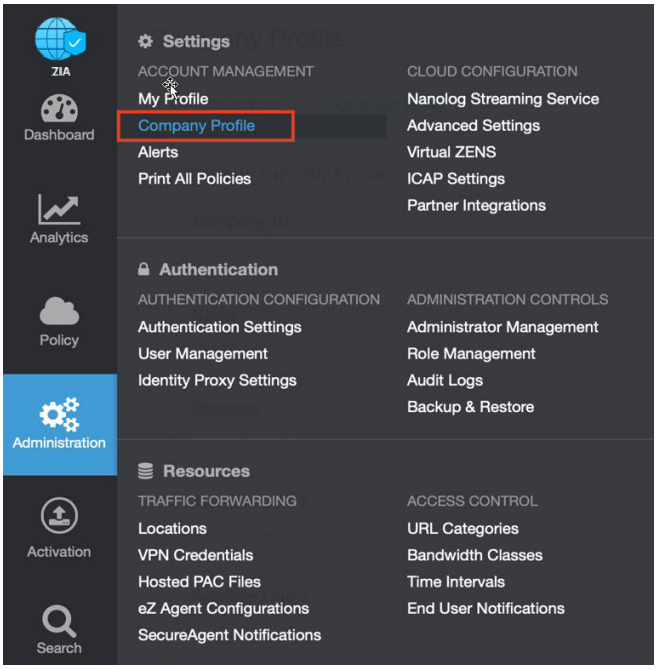

Figure 7. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

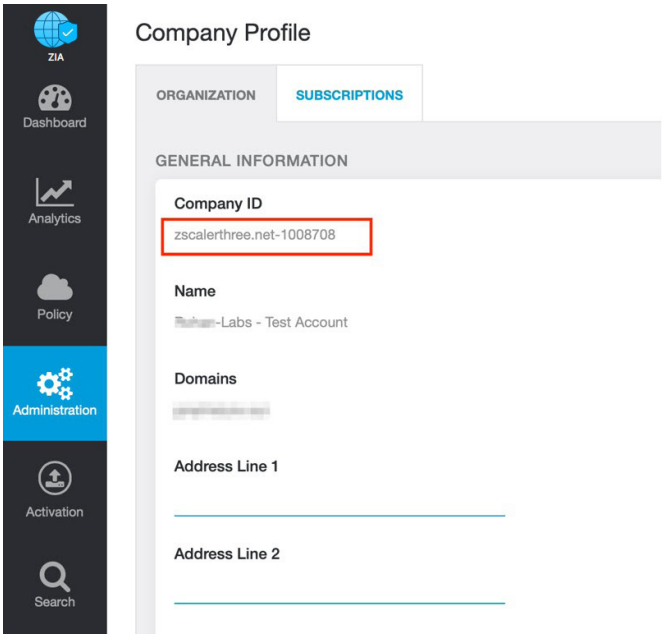

Figure 8. Company ID

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

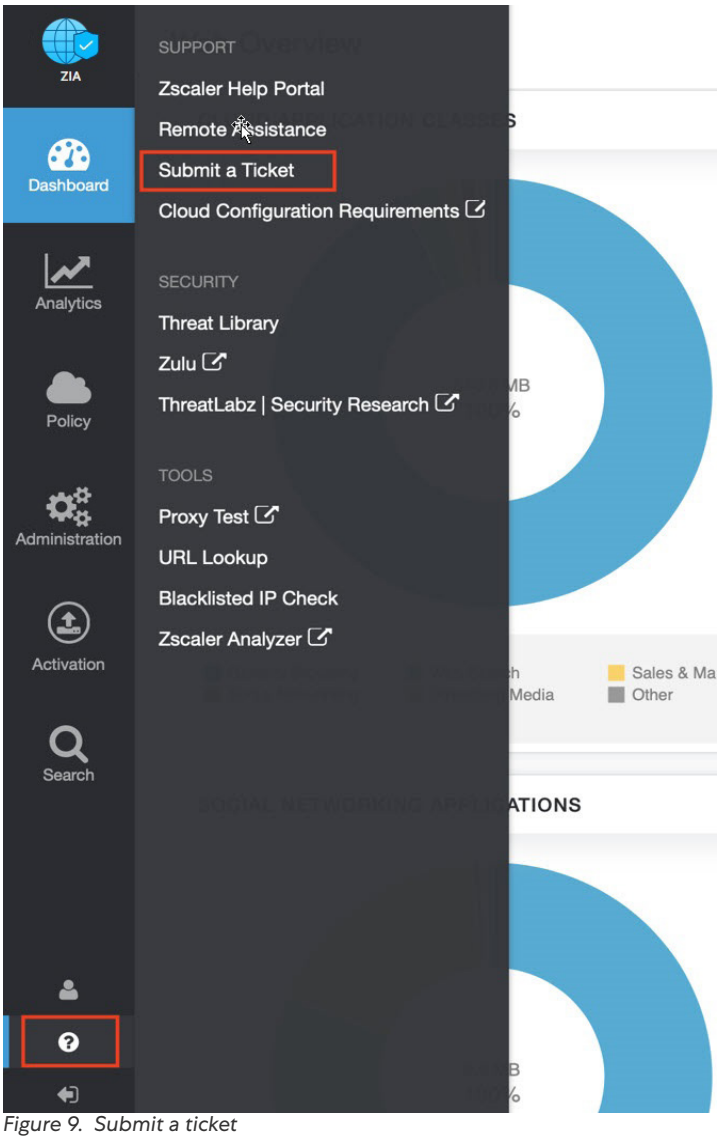

Figure 9. Submit a ticket

