ZSCALER AND SALESFORCE DEPLOYMENT GUIDE

JULY 2024, VERSION 1.3

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
ACS	Advanced Cloud Solutions (Salesforce)
CA	Central Authority (Zscaler)
CASB	Cloud Access Security Broker
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
FFIEC	Federal Financial Institutions Examination Council
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
PSK	Pre-Shared Key
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following are overviews of the Zscaler and Salesforce applications described in this section.

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. Flagship services Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) 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.

Salesforce Overview

Salesforce, Inc. (NASDAQ: CRM) is an American cloud-based software company headquartered in San Francisco, California. It provides customer relationship management (CRM) service and also sells a complementary suite of enterprise applications focused on customer service, marketing automation, analytics, and application development.

Salesforce was founded in 1999. To learn more, refer to Salesforce's website.

Audience

This guide is written for Zscaler administrators, IT administrators, and IT analysts responsible for deploying, monitoring, and managing SaaS services in an enterprise envonment. For additional product and company resources, refer to:

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

Software Versions

This document was authored using Zscaler Internet Access v6.2 and the latest Salesforce Production Release. A Salesforce developer account was used to created and verify the features enabled and used as examples.

To learn more, refer to the Salesforce developer account portal.

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 Salesforce Introduction

Overviews of the Zscaler and Salesforce 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 it as a secure internet on-ramp—all you do is 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 the 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 start with the services you need now and activate others as your needs grow.

ZDX Overview

ZDX is a digital experience monitoring solution delivered as a service from the Zscaler cloud. ZDX provides end-to-end visibility and troubleshooting of end user performance issues for any user or application, regardless of location. In addition, it enables continuous monitoring for network, security, desktop, and helpdesk teams with insight into the end user device, network, and application performance issues. With ZDX, IT teams can proactively analyze and troubleshoot user experience issues, improving business productivity, and IT agility.

Business benefits of ZDX include:

- Increased agility and collaboration among desktop, security, network, and helpdesk operations teams while triaging user experience issues and resolving them.
- Improved productivity due to better user experience and fast, secure, and reliable connectivity through the Zscaler cloud.
- Reduced complexity and cost through elimination of point monitoring solutions.
- Operational simplicity of using the same lightweight agent used for all Zscaler services and the scale of Zscaler cloud to gain insights into digital experiences.

Zscaler Resources

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

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZDX Help Portal	Help articles on ZDX.

Name and Link	Description
ZDX Predefined Applications	Help articles on which predefined applications are available in the ZDX Admin Portal when you log in.
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 and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZDX Help Portal	Help articles on ZDX.
ZDX Predefined Applications	Help articles on which predefined applications are available in the ZDX Admin Portal when you log in.
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.

Salesforce CRM Overview

Salesforce's customer relationship management (CRM) solution helps you find new customers, win their business, and keep them happy by organizing customer and prospect information in a way that helps you build stronger relationships with them and grow your business faster. CRM systems start by collecting a customer's website, email, telephone, social media data, and more, across multiple sources and channels. Salesforce's CRM tool organizes this information to give you a complete record of individuals and companies overall, so you can better understand your relationship over time.

Salesforce's CRM system is then used to manage day-to-day customer activities and interactions, as well as connect to other business apps that help you to develop customer relationships.

Salesforce Resources

The following table contains links to Salesforce support resources.

Name and Link	Description
Salesforce Developer Account	Sign up for a Salesforce Developer Edition.
Salesforce Help	Salesforce help portal. Log in to create a case, view open cases, check your success plan details, view help documentation, etc.
Salesforce Experience	Connect with fellow Trailblazers. Ask and answer questions to build your skills and network.

Zscaler Data Protection and Digital Experience for Salesforce

Salesforce is an industry leader that defined the cloud and the advantages SaaS applications provide to an enterprise. SaaS services are popular because of the collaboration, ease of use, and ease of sharing the services globally. But the downside of this ease of access and sharing is security risk based on the client's environment. It is impossible to train every employee to use SaaS application security best practices at all times, which leads to costly mistakes for the organization. Risk associated with accidental data exposure, malicious intent, and compliance violations can force companies to restrict or prevent use of these incredible business tools.

Another challenge organizations migrating to cloud services in today's environment face is monitoring user experience for SaaS applications—especially in today's work-from-anywhere corporate infrastructures. Zscaler provides a complete Salesforce solution using ZIA for Salesforce security and ZDX for visibility into the user experience.

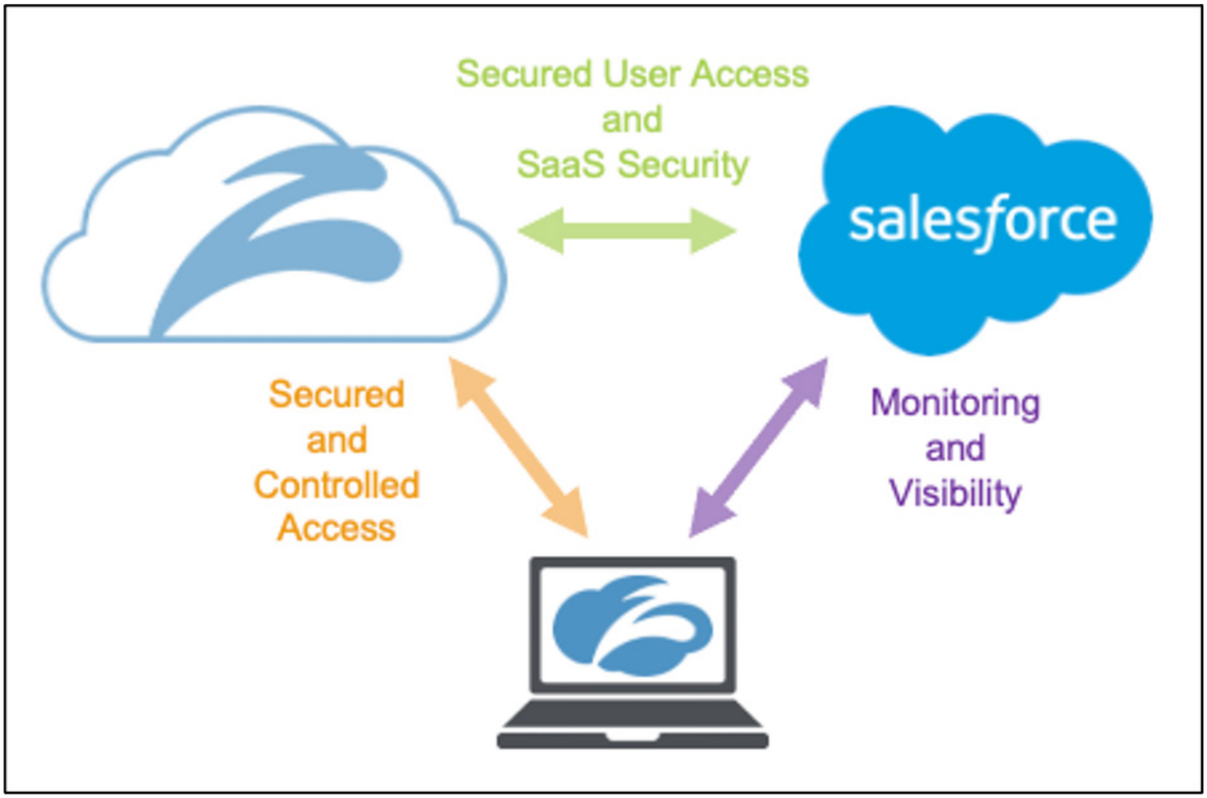


Figure 1. Zscaler solution for Salesforce

ZIA secures Salesforce SaaS through cloud-based access control, identity control, SaaS security posture management, and the SaaS API to scan the Salesforce attachments for malicious content and data loss protection (DLP). ZIA also provides complete security for clients whether they are in the corporate office or their home office.

The ZDX service provides user-specific experience monitoring and visibility to the Salesforce service to help organizations address any user experience concerns or challenges. ZDX has preconfigured monitors for Salesforce that monitor and measure performance of the users' device running Zscaler Client Connector. These monitors provide detailed information on the user device, network path to Salesforce, and the Salesforce SaaS performance itself. This information is invaluable to operations when a user is experiencing issues with Salesforce and provides visibility to every corner of the internet.

Both ZIA SaaS security and ZDX SaaS monitoring operate as separate standalone services and are not dependent on one or the other. However, the two services working together provide a comprehensive solution for both security and operations of Zscaler's partner SaaS CRM service.

This guide covers the following ZIA features for Salesforce security, and the ZDX for Salesforce performance visibility:

- ZIA SaaS Identity Proxy
- Zscaler SaaS Security API Data and Malware Protection for Salesforce
- ZIA SaaS Security Posture Report
- ZIA Cloud Application Control
- ZDX for the Salesforce User Experience

ZIA SaaS Identity Proxy

You can configure the Zscaler service as an identity proxy for Salesforce. This Zscaler feature forces users to authenticate and access Salesforce only through the ZIA security cloud. This provides security, inspection of traffic, and controlled access of anyone using your organization's Salesforce tenant.

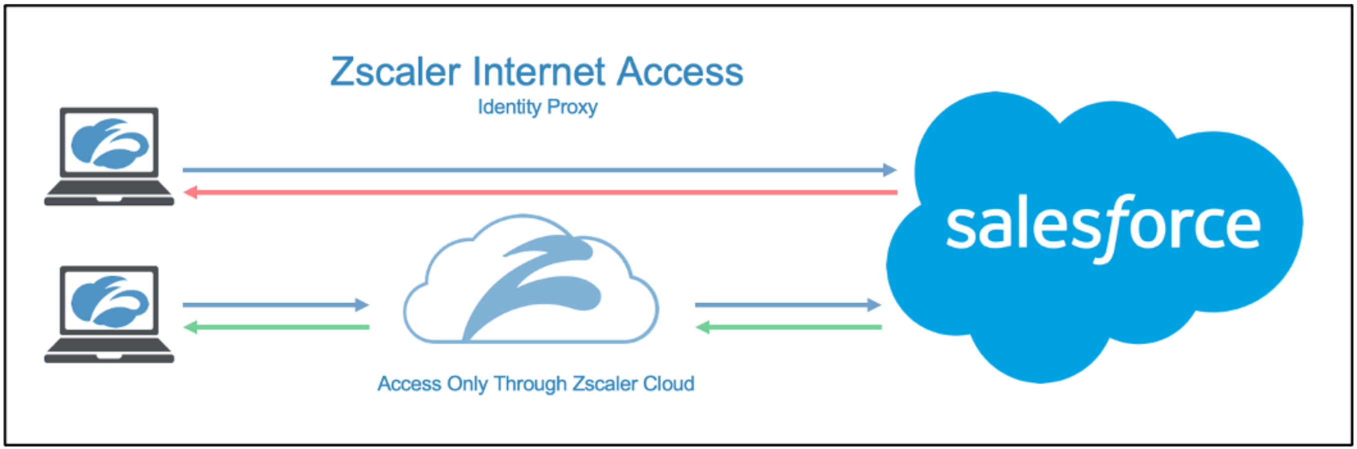


Figure 2. Identity proxy

When users try to access Salesforce with their corporate accounts without using the Zscaler service, a dialog appears, requesting the users log in via Zscaler. The process is controlled using SAML, the IdP that is defined on Zscaler for the ZIA service, and the Salesforce SSO configuration to forward authorization requests to Zscaler.

Zscaler SaaS Security API Data and Malware Protection for Salesforce

The Zscaler SaaS Security API is a feature set that is part of the ZIA security cloud and creates rules to discover and prevent threats to data at rest in sanctioned SaaS applications.

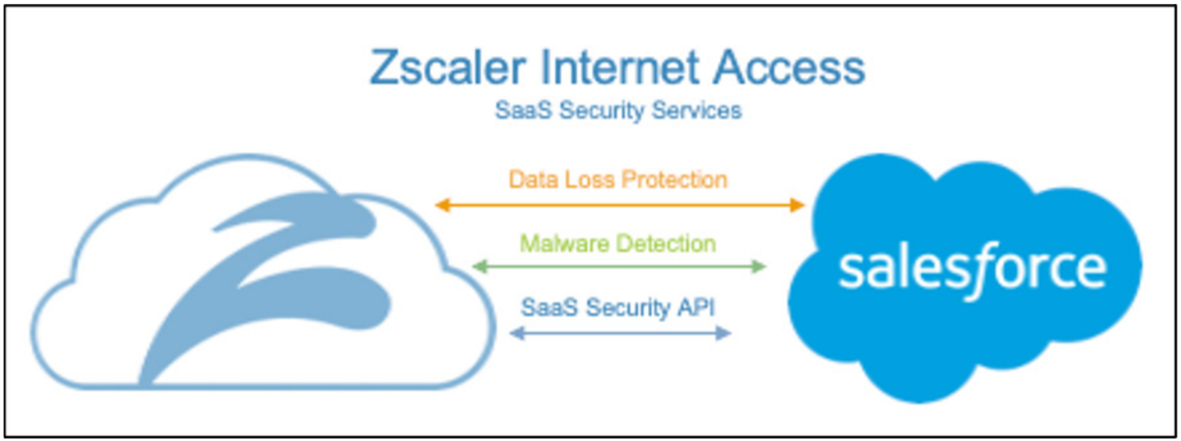


Figure 3. Zscaler SaaS Security API in use with Salesforce

Zscaler SaaS Security enables organizations to securely adopt and govern the use of multiple SaaS applications. It provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.

What makes Zscaler's SaaS Security API unique?

- Data exposure reporting and remediation: Zscaler SaaS Security checks SaaS applications and cloud provider configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.
- Threat identification and remediation: Zscaler SaaS Security checks SaaS applications for hidden threats being exchanged and prevents their propagation.
- Compliance assurance: Zscaler SaaS Security provides compliance visibility across SaaS and cloud providers and can mitigate violations automatically.
- Part of a larger data protection platform: The Zscaler Cloud Security Platform provides unified data protection with DLP, and malware scanning capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance. Zscaler also offers ZPA for Zero Trust access to internal applications, ZDX for active user SaaS application experience monitoring, and Zscaler Cloud Protection. Zscaler provides end-to-end connectivity, security, and visibility from any location on-premises or remote.

For more information, see Zscaler Resources.

ZIA SaaS Security Posture Report

After the Salesforce tenant is configured, Zscaler scans the Salesforce tenant for the organization's security posture for recommended security settings and displays any recommendations to secure the tenant in the SaaS Security Posture report. The results of the scan and the tenant security checks are determined by the SaaS security posture policies. Although all settings are enabled by default, you can disable individual checks on the SaaS Security Posture Policy page, allowing organizations to customize the report to their individual needs. Posture policy check results are displayed on the SaaS Policy Report page, and you can filter the results by best practice recommendations, PCI compliance, or FFIEC compliance.

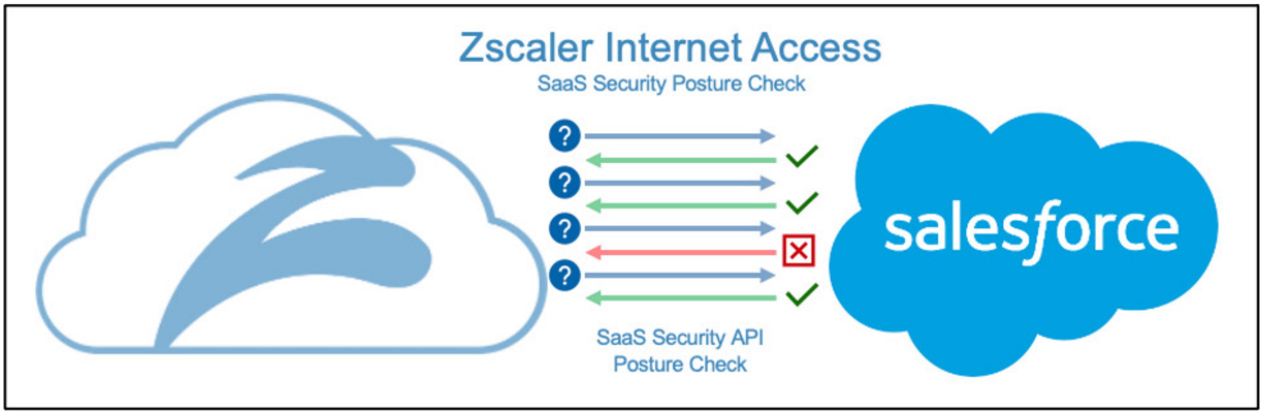


Figure 4. SaaS security posture report

Individual policies checked:

- Enable multi-factor authentication for Salesforce users
- Enable multi-factor authentication for Salesforce API access
- Set IP restrictions for Salesforce users
- Set login hour restrictions for Salesforce users
- Set strong passwords for Salesforce users
- Set passwords to expire for Salesforce users
- Set email domain restrictions for Salesforce users
- Review the health check score in Salesforce
- Set up Salesforce audit trail
- Set up real-time event monitoring in Salesforce
- Set up Salesforce shield encryption for data at rest
- Rotate encryption keys for Salesforce
- Enable multi-factor authentication for Salesforce encryption key management

ZIA Cloud Application Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits inline between users and the internet. It inspects all traffic, including SSL, flowing between them. As part of the platform, Zscaler Cloud Application Control delivers full visibility into application usage, and granular policies ensure the proper use of both sanctioned and unsanctioned applications. While SaaS tenant security is for data that is out of band, SaaS Security API is for data at rest. Zscaler Cloud Application Control is referred to as inline CASB.

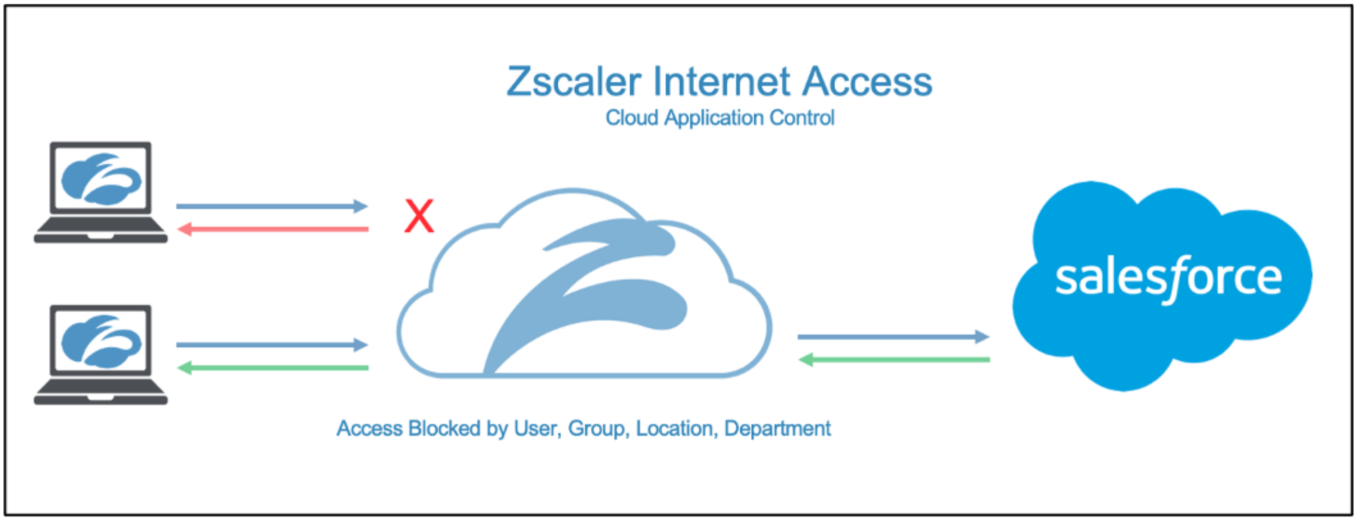

Zscaler Internet Access
Cloud Application Control
X
salesforce
Access Blocked by User, Group, Location, Department

Figure 5. Cloud App Control

Cloud Application Control provides SaaS application intelligence to consolidate all associated URLs and functions of the application in a single security setting. This allows you to control specific user, groups, locations, or departments, and only allow the required users access to the application.

ZDX for the Salesforce User Experience

With ZDX, you can monitor your users' digital experiences. ZDX provides visibility across the complete user-to-cloud app experience and quickly isolates issues. By combining the Zscaler Client Connector endpoint agent with Zscaler's global cloud footprint, ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

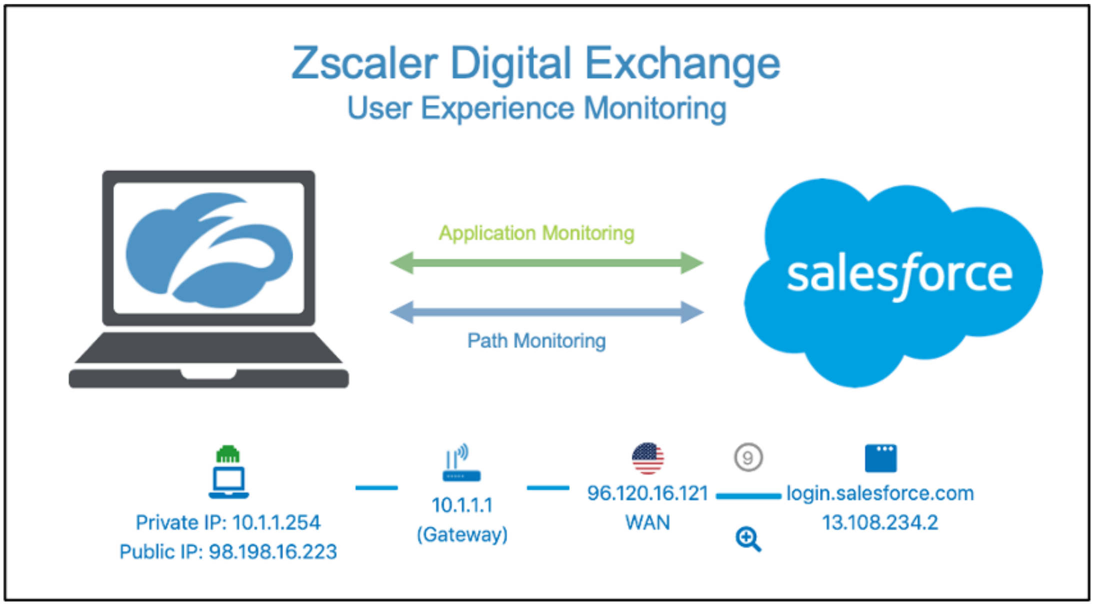


Figure 6. ZDX user experience monitoring

What makes ZDX unique?

- End-user device performance: Continuously gathers and analyzes data on end-user devices that could impact end-user experiences.
- Cloud path performance: Measures and analyzes end-to-end and hop-by-hop network path metrics from every user device to the cloud application.
- Application performance: Continuously monitors and measures application metrics, such as response time, DNS resolution, and broader availability metrics of the application.
- ZDX scoring: Monitors aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

For more information, see Zscaler Resources.

SaaS Identity Proxy

You can configure the Zscaler service as an Identity Proxy for Salesforce. This Zscaler feature forces users to authenticate and access Salesforce only through the Zscaler ZIA security cloud. This provides security, inspection of traffic, and controlled access of all users of your Salesforce tenant.

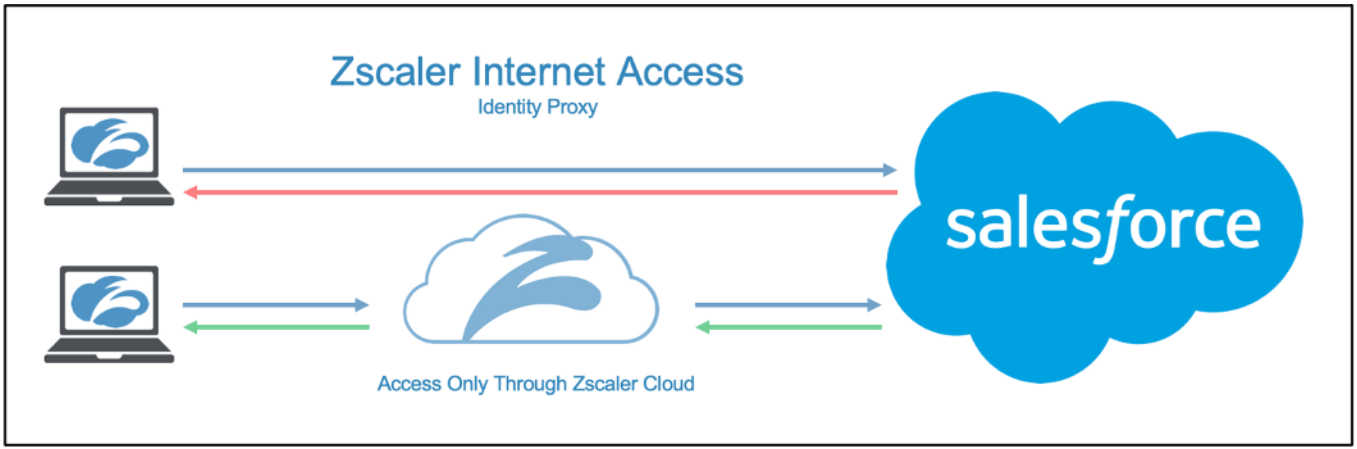


Figure 7. Identity proxy

When users try to access Salesforce with their corporate accounts without going through the Zscaler service, a screen asking them to log in via Zscaler is displayed. The process is controlled using SAML, the IdP that is defined on Zscaler for the ZIA service, and Salesforce SSO configuration to forward authentication requests to Zscaler.

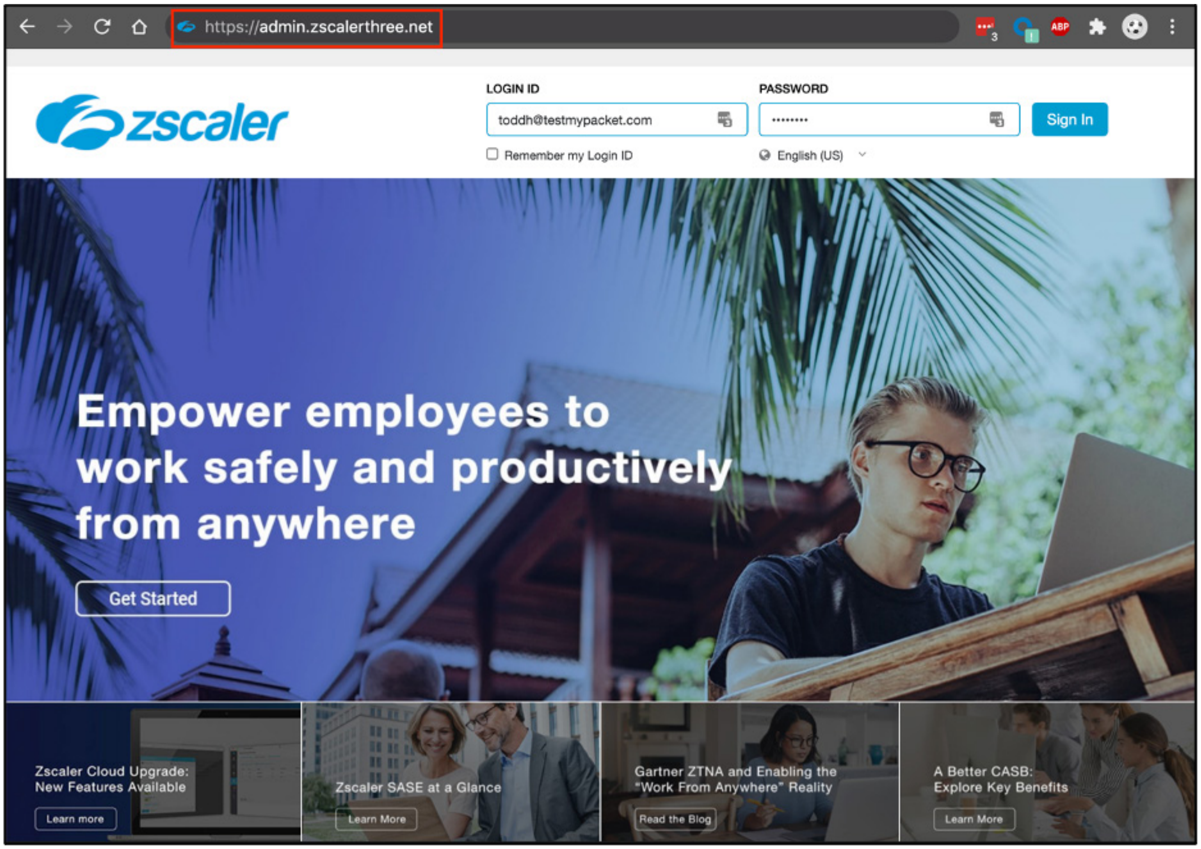
The traffic flow configured in the next steps is:

- The user authenticates with Zscaler using SAML.
- Zscaler syncs the ID from the customer's ZIA IdP.
- Zscaler sets an authentication cookie on the user's system.
- The user goes to the Salesforce.com customized URL and clicks the SSO button (with authentication cookie).
- Salesforce redirects to the ZIA Public Service Edge to confirm identity.
- The ZIA Public Service Edge transforms the cookie and authenticates the user with Salesforce.

Configure the SaaS Identity Proxy

The configuration to enable the SaaS Identity Proxy service builds on itself and configuration is performed on both the Zscaler tenant and the Salesforce tenant. The steps are listed for both tenants. Zscaler recommends configuring the solution by opening two browsers or browser tabs and switching back and forth between the two tenants as required.

To begin the configuration, log in to the ZIA Admin Portal with admin credentials.



https://admin.zscalerthree.net

LOGIN ID: toddh@testmypacket.com

PASSWORD: ••••••••

zscaler
Sign In
□ Remember my Login ID
English (US)
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More

Figure 8. Creating the Salesforce tenant

Configure the SaaS Identity Proxy

To start configuring Zscaler to act as an Identity Proxy for Salesforce:

1. Go to **Administration** > **Identity Proxy Settings** > **Add Cloud Application**. This launches the **Add Cloud Application** window.

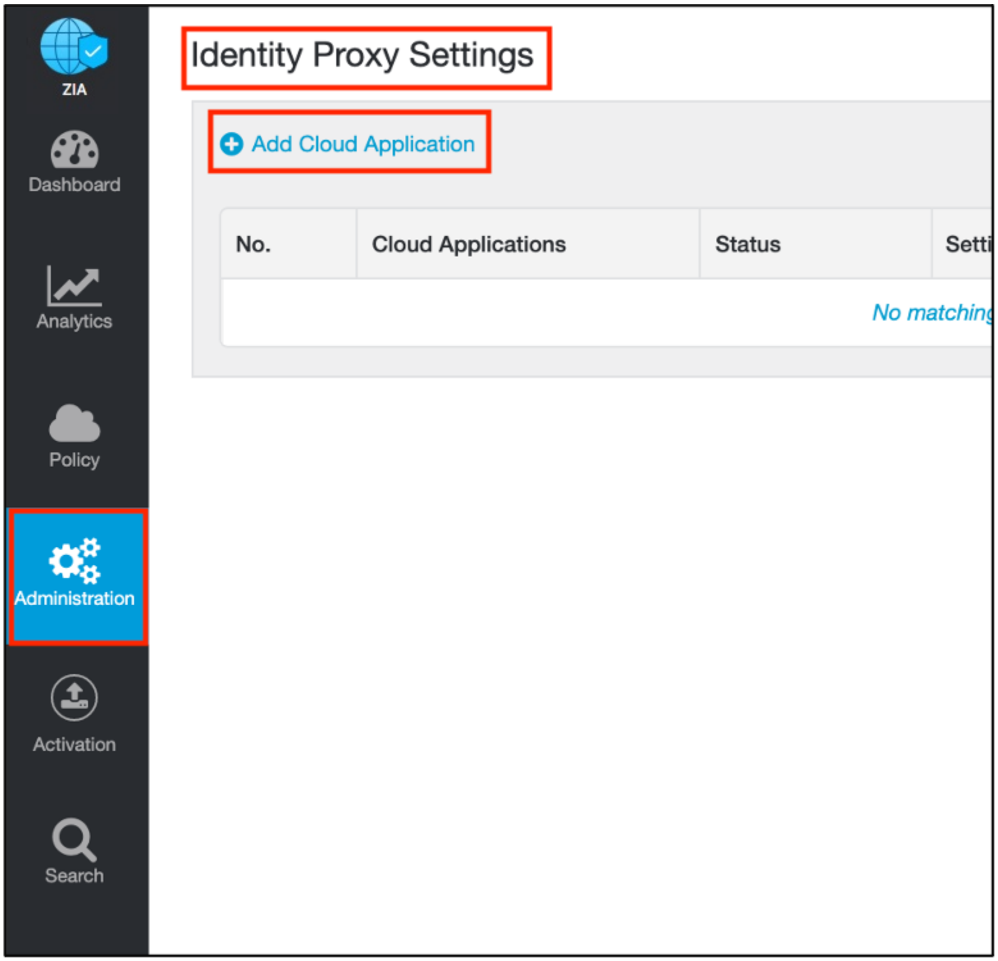
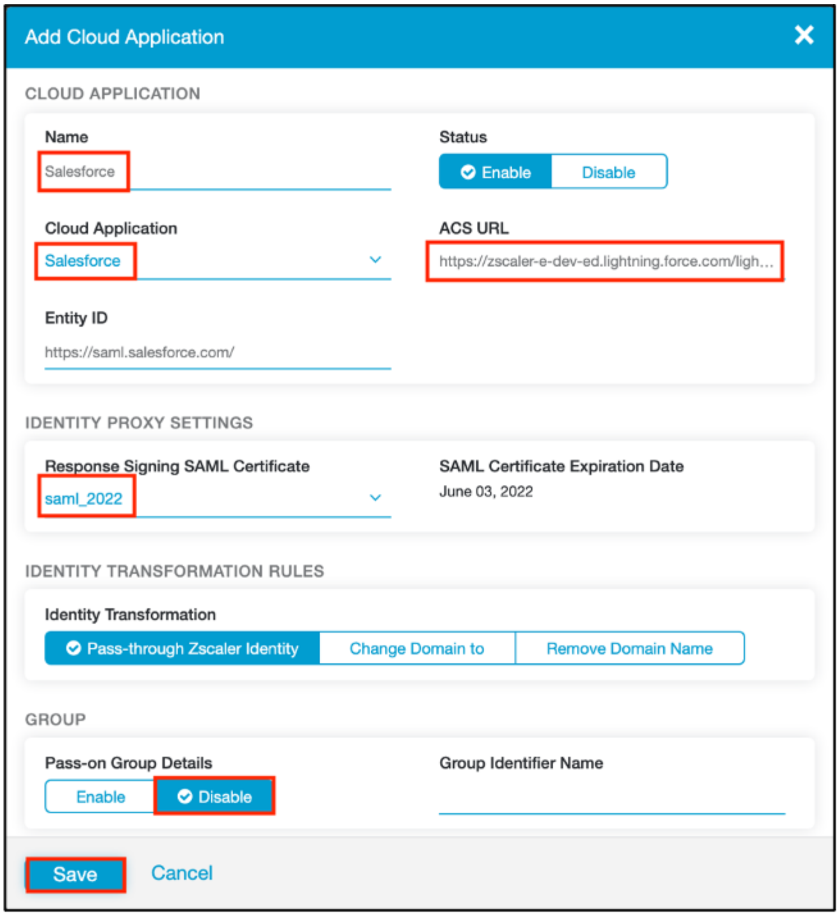


Figure 9. Configure the identity proxy

2. To start configuring Zscaler to act as an Identity Proxy, enter an intuitive name for the cloud application (like `Salesforce`).
3. Select **Salesforce** from the **Cloud Application** drop-down menu.
4. The **ACS URL** isn't created yet, but a URL must be provided to save the configuration. Put the Salesforce Login URL in the ACS field as a holding place.
5. Select **saml_2022** or the latest certificate for the **Response Signing SAML Certificate**.
6. Select **Disable** for the **Pass-on Group Details**.
7. Click **Save**.



Add Cloud Application

CLOUD APPLICATION

Name: Salesforce

Status: [✓ Enable] Disable

Cloud Application: Salesforce

ACS URL: https://zscaler-e-dev-ed.lightning.force.com/ligh...

Entity ID: https://saml.salesforce.com/

IDENTITY PROXY SETTINGS

Response Signing SAML Certificate: saml_2022

SAML Certificate Expiration Date: June 03, 2022

IDENTITY TRANSFORMATION RULES

Identity Transformation: [✓ Pass-through Zscaler Identity] Change Domain to Remove Domain Name

GROUP

Pass-on Group Details: Enable [✓ Disable]

Group Identifier Name:

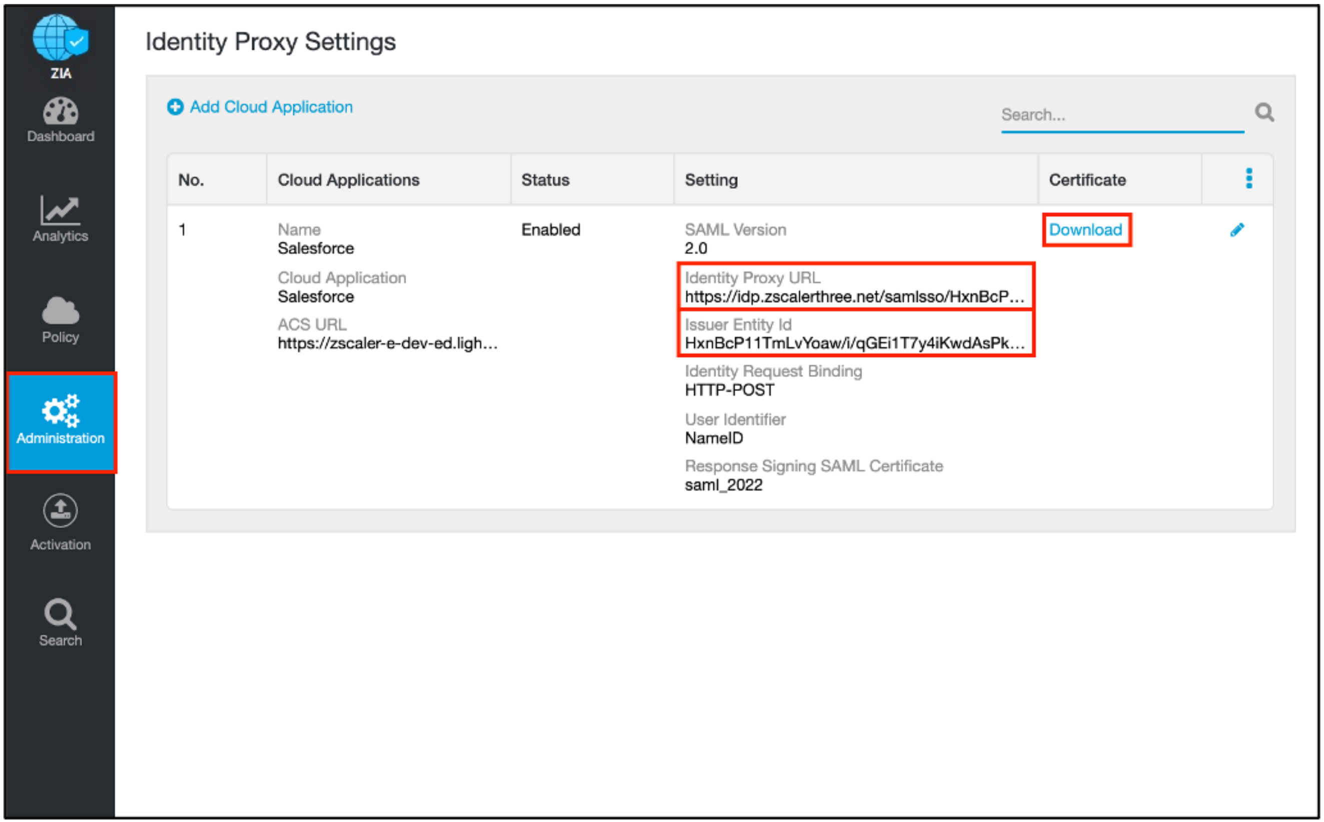
Figure 10. The Identity Proxy wizard

The Completed ZIA Salesforce Identity Proxy

To complete the identity proxy for Salesforce, add the ACS URL that is created on the Salesforce tenant. Copy and save the highlighted URLs for the Salesforce configuration. Also download and save the certificate.

Open a new tab in your browser to access and configure Salesforce, leaving the page open to make the final change:

1. Copy and save the **Identity Proxy URL**.
2. Copy and save the **Issuer Entity Id** URL.
3. Click **Download** and save the **Certificate**.
4. Open the Salesforce tenant.



Identity Proxy Settings

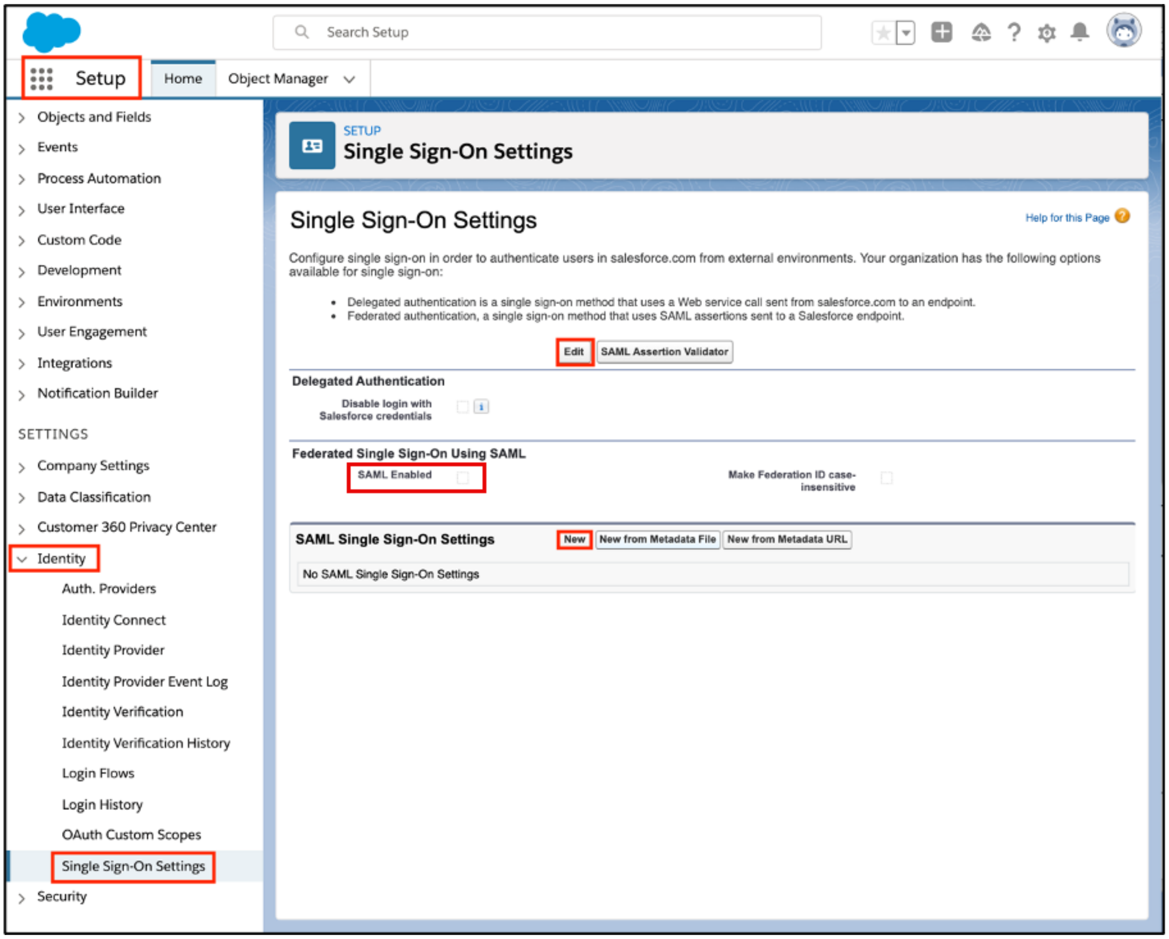
No.	Cloud Applications	Status	Setting	Certificate
1	Name Salesforce Cloud Application Salesforce ACS URL https://zscaler-e-dev-ed.ligh…	Enabled	SAML Version 2.0 Identity Proxy URL https://idp.zscalerthree.net/samlsso/HxnBcP… Issuer Entity Id HxnBcP11TmLvYoaw/i/qGEi1T7y4iKwdAsPk… Identity Request Binding HTTP-POST User Identifier NameID Response Signing SAML Certificate saml_2022	Download

Figure 11. The completed ZIA Salesforce identity proxy

Configure the Salesforce Tenant

To configure the Salesforce tenant for identity proxy in the Salesforce Admin Console:

1. Go to **Setup > Identity** > **Single Sign-On Settings**.
2. Click **Edit**.
3. In the **Single Sign-On Settings** window, select the **SAML Enabled** checkbox.
4. Click **New** next to **SAML Single Sign-On Settings**.



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Delegated Authentication

Disable login with Salesforce credentials □

Federated Single Sign-On Using SAML

SAML Enabled □

Make Federation ID case-insensitive □

SAML Single Sign-On Settings

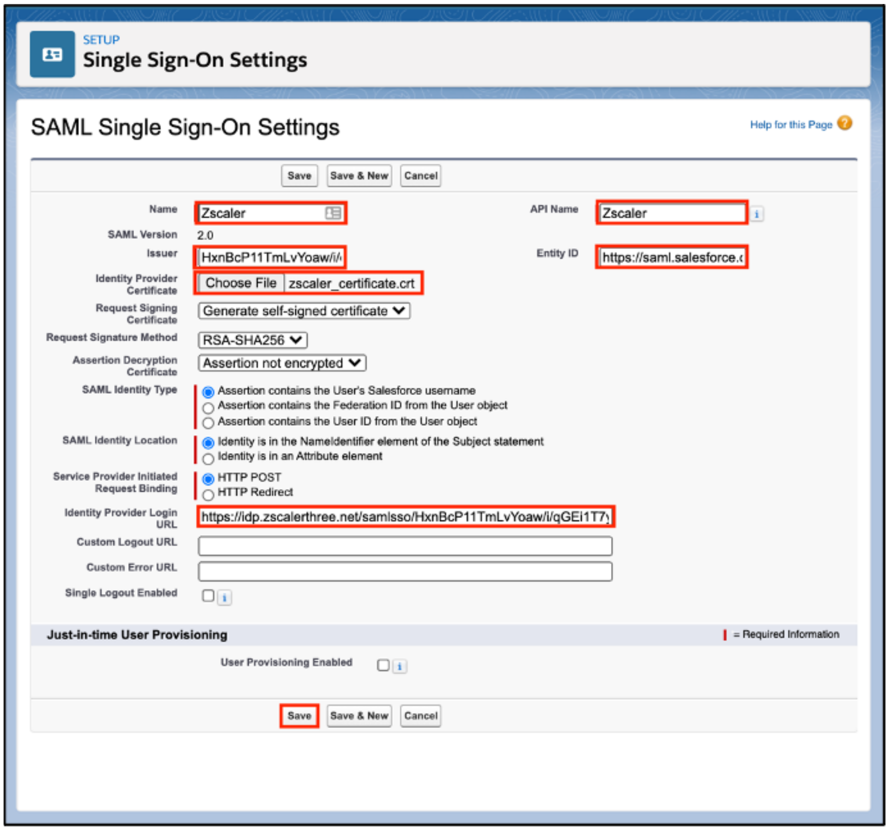
No SAML Single Sign-On Settings

Figure 12. Configure the Salesforce tenant

Salesforce Tenant SAML Settings

To configure the Salesforce tenant for identity proxy:

1. **Name** the profile `Zscaler` (this becomes the default API name).
2. Paste the **Issuer Entity ID URL** that you copied from ZIA into the **Issuer** field.
3. Enter `https://saml.salesforce.com/` for the **Entity ID**.
4. Choose and upload the Zscaler Certificate that you previously downloaded for the **Identity Provider Certificate**.
5. Select **Assertion contains the User's Salesforce username** for the **SAML Identity Type**.
6. Select **Identity is in the Nameidentifier element of the Subject statement** for **SAML Identity Location**.
7. Select **HTTP POST** for **Service Provider Initiated Request Binding**.
8. Paste the ZIA Identity Proxy URL you copied into the **Identity Provider Login URL**.
9. Click **Save**.



SAML Single Sign-On Settings

Name: Zscaler
API Name: Zscaler
SAML Version: 2.0
Issuer: HxnBcP11TmLvYoaw/i/
Entity ID: https://saml.salesforce.
Identity Provider Certificate: Choose File zscaler_certificate.crt
Request Signing Certificate: Generate self-signed certificate
Request Signature Method: RSA-SHA256
Assertion Decryption Certificate: Assertion not encrypted

SAML Identity Type:
● Assertion contains the User's Salesforce username
○ Assertion contains the Federation ID from the User object
○ Assertion contains the User ID from the User object

SAML Identity Location:
● Identity is in the NameIdentifier element of the Subject statement
○ Identity is in an Attribute element

Service Provider Initiated Request Binding:
● HTTP POST
○ HTTP Redirect

Identity Provider Login URL: https://idp.zscalerthree.net/samlsso/HxnBcP11TmLvYoaw/i/qGEi1T7

Custom Logout URL:
Custom Error URL:
Single Logout Enabled: □

Just-in-time User Provisioning
= Required Information

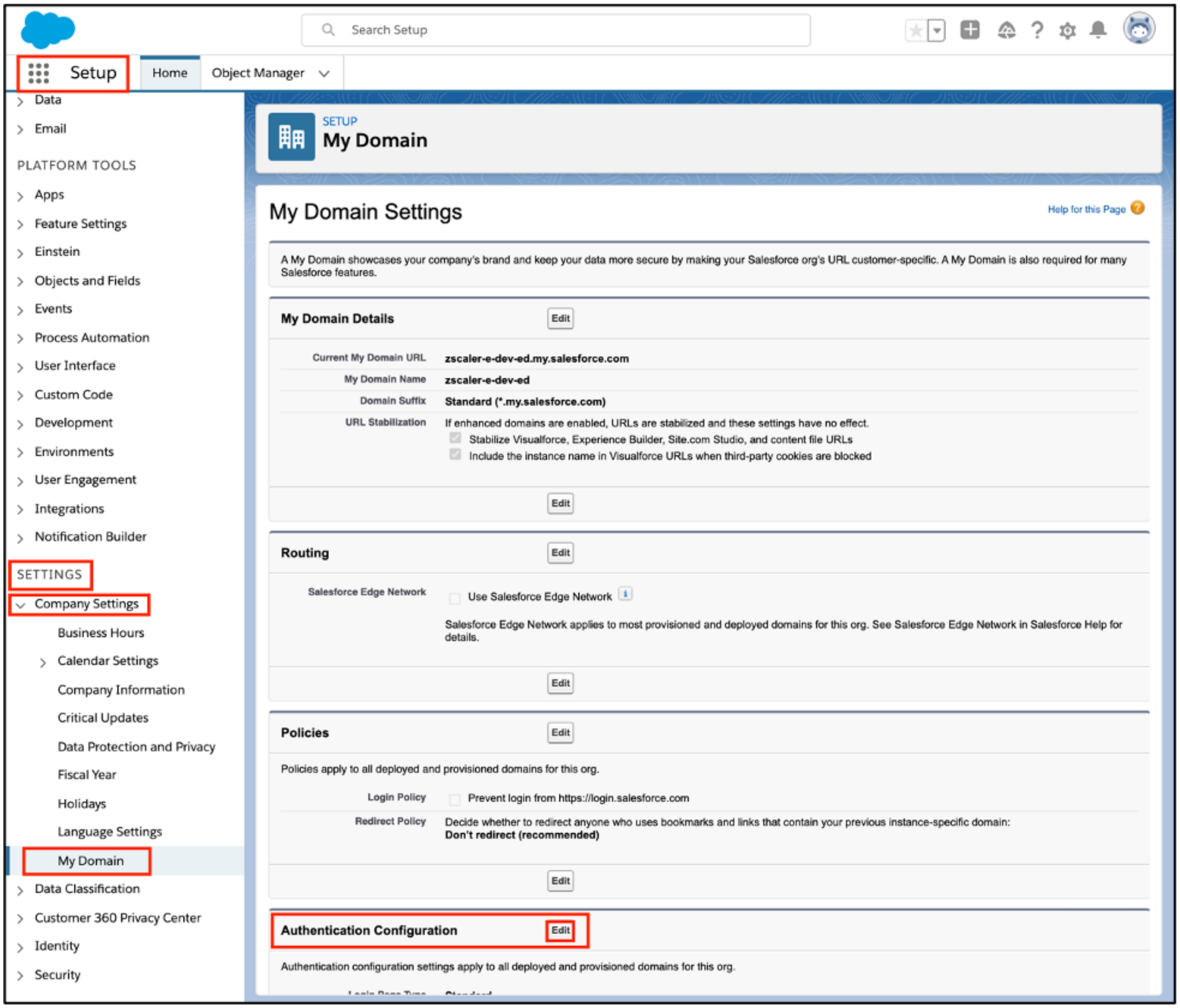
User Provisioning Enabled: □

Figure 13. Configure the Salesforce tenant SAML settings

Salesforce Tenant Authentication Configuration

To configure the Salesforce authentication settings in the Saleforce Admin Console:

1. Go to **Setup** > **Settings** > **Company Settings**.
2. Select **My Domain**.
3. Click **Edit** next to **Authentication Configuration**.



My Domain Settings

A My Domain showcases your company's brand and keep your data more secure by making your Salesforce org's URL customer-specific. A My Domain is also required for many Salesforce features.

My Domain Details

Current My Domain URL	zscaler-e-dev-ed.my.salesforce.com
My Domain Name	zscaler-e-dev-ed
Domain Suffix	Standard (*.my.salesforce.com)
URL Stabilization	If enhanced domains are enabled, URLs are stabilized and these settings have no effect. ☑ Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs ☑ Include the instance name in Visualforce URLs when third-party cookies are blocked

Routing

Salesforce Edge Network: □ Use Salesforce Edge Network

Salesforce Edge Network applies to most provisioned and deployed domains for this org. See Salesforce Edge Network in Salesforce Help for details.

Policies

Policies apply to all deployed and provisioned domains for this org.

Login Policy	□ Prevent login from https://login.salesforce.com
Redirect Policy	Decide whether to redirect anyone who uses bookmarks and links that contain your previous instance-specific domain: **Don't redirect (recommended)**

Authentication Configuration

Authentication configuration settings apply to all deployed and provisioned domains for this org.

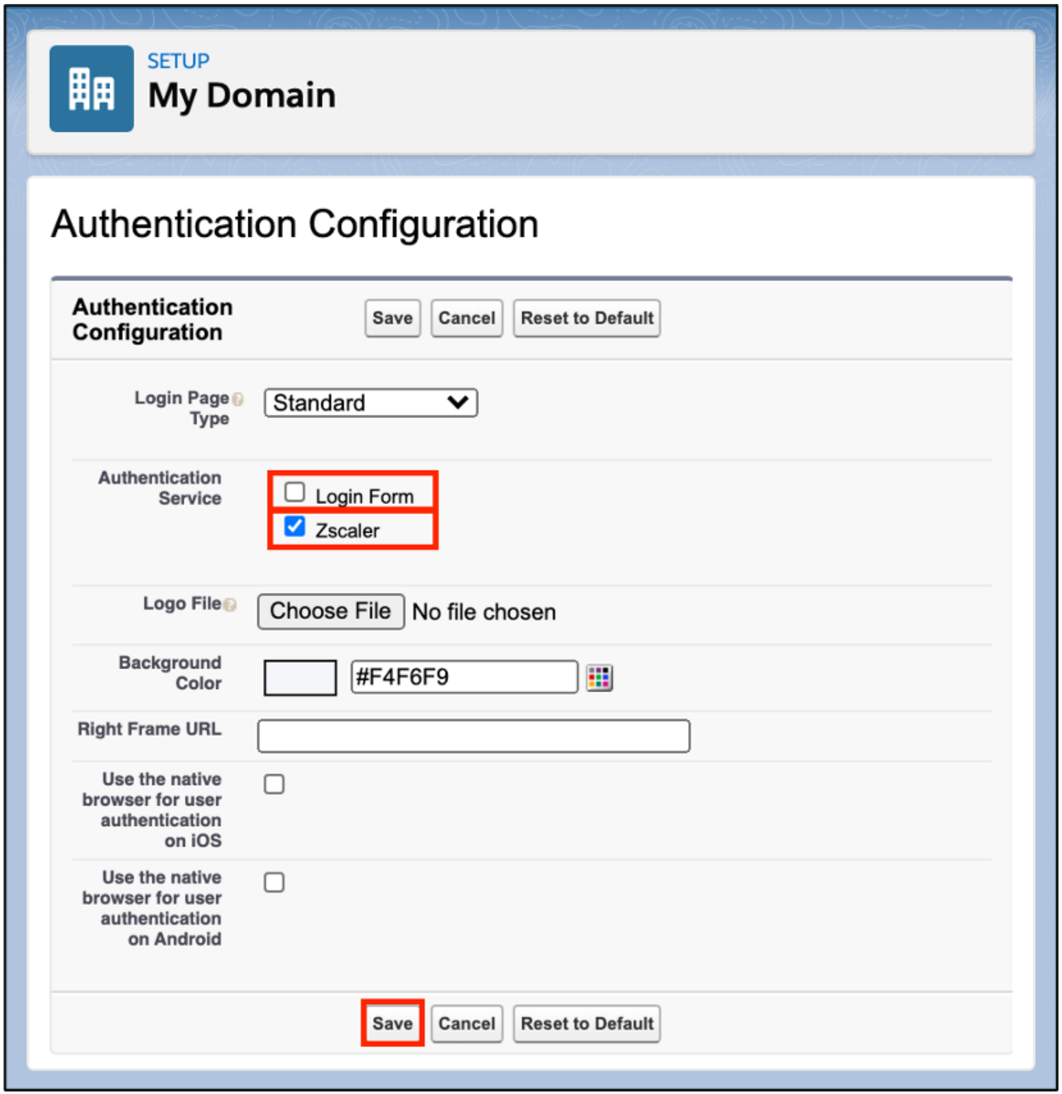
Figure 14. Configure the Salesforce tenant authentication configuration

This opens the **Authentication Configuration** dialog.

Salesforce Tenant Authentication Settings

To configure the Salesforce authentications settings:

1. Deselect the **Login Form** checkbox.
2. Select the **Zscaler** checkbox.
3. Click **Save**.



SETUP

My Domain

Authentication Configuration

Authentication Configuration

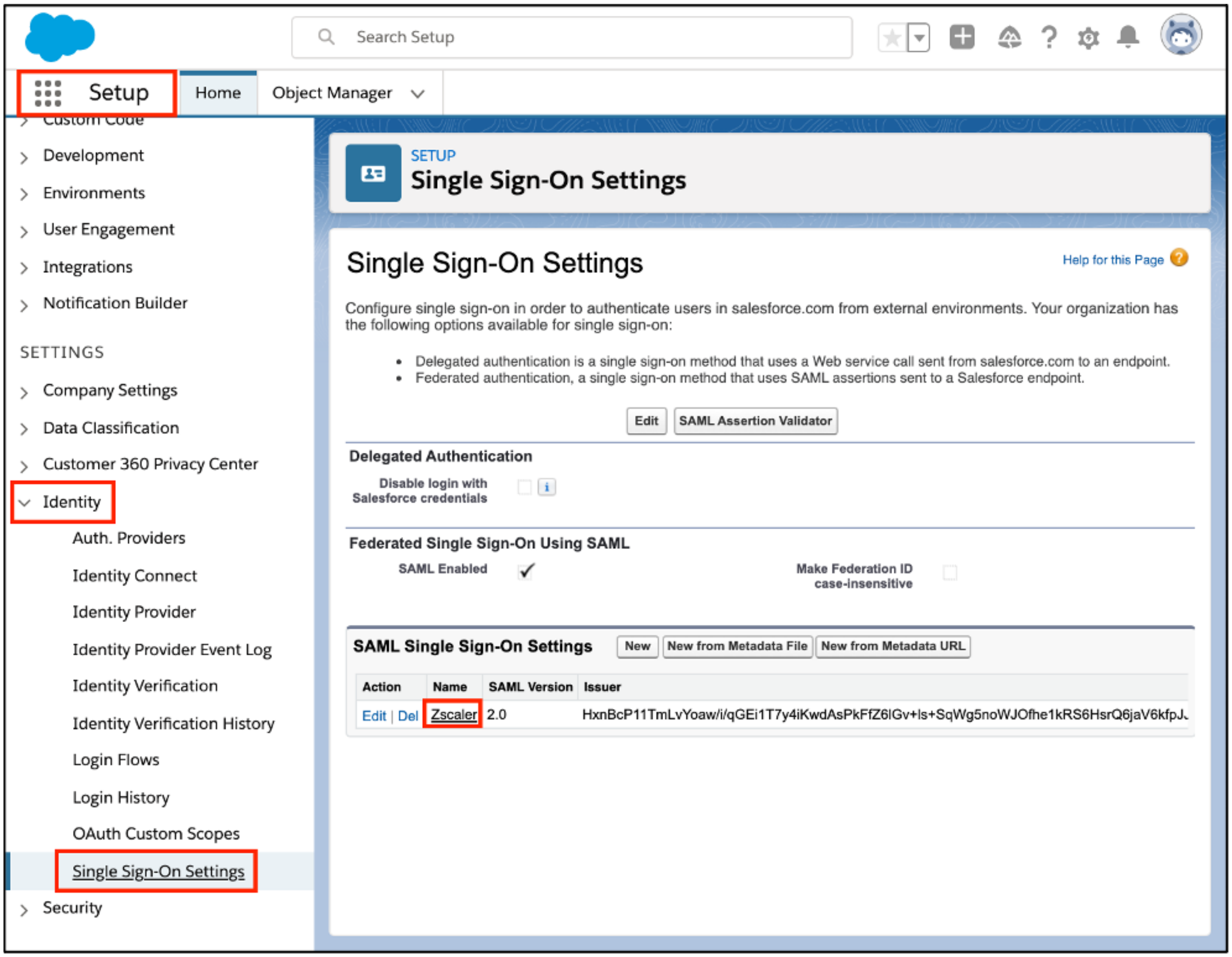
Login Page Type	Standard
Authentication Service	□ Login Form ☑ Zscaler
Logo File	Choose File No file chosen
Background Color	#F4F6F9
Right Frame URL	
Use the native browser for user authentication on iOS	□
Use the native browser for user authentication on Android	□

Figure 15. Configure the Salesforce tenant authentication configuration

Locate and Copy the ACS URL

Although the configuration is complete, you must copy the ACS URL that was missing in the Zscaler setup. To find and copy the URL:

1. Go to **Setup** > **Identity** > **Single Sign-On Settings**.
2. Select the Zscaler settings by clicking the name **Zscaler**.



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Delegated Authentication

Disable login with Salesforce credentials □

Federated Single Sign-On Using SAML

SAML Enabled ✓ Make Federation ID case-insensitive □

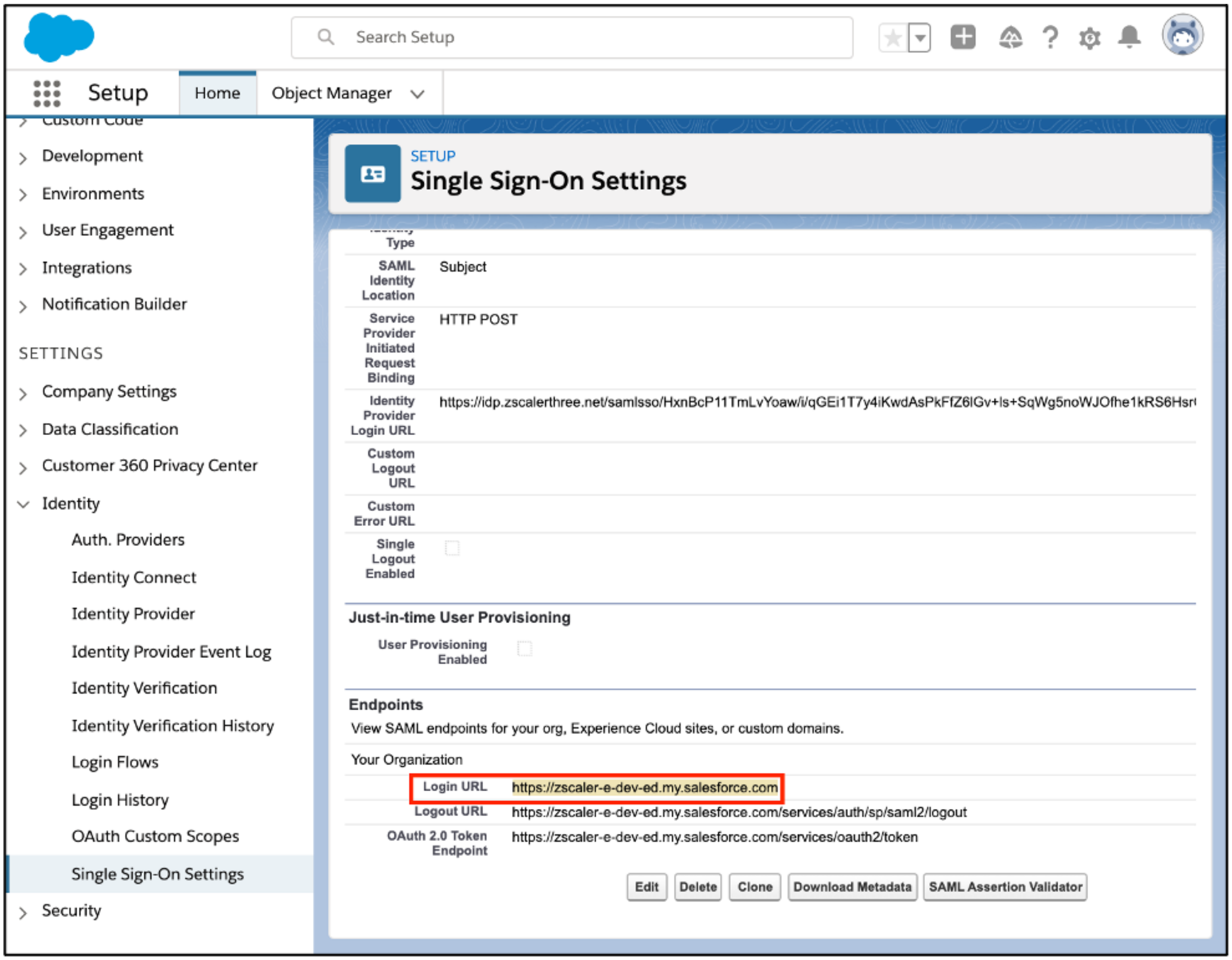
SAML Single Sign-On Settings

Action	Name	SAML Version	Issuer
Edit | Del	Zscaler	2.0	HxnBcP11TmLvYoaw/i/qGEi1T7y4iKwdAsPkFfZ6lGv+ls+SqWg5noWJOfhe1kRS6HsrQ6jaV6kfpJ

Figure 16. Copy the ACS URL from the single sign-on settings

Salesforce Tenant Single Sign-On Settings

Copy the Login URL and save it. Then paste this URL into the SaaS configuration on Zscaler.



Identity Type	
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP POST
Identity Provider Login URL	https://idp.zscalerthree.net/samlsso/HxnBcP11TmLvYoaw/i/qGEi1T7y4iKwdAsPkFfZ6lGv+ls+SqWg5noWJOfhe1kRS6Hsr
Custom Logout URL	
Custom Error URL	
Single Logout Enabled	□

Just-in-time User Provisioning

User Provisioning Enabled	□

Endpoints

View SAML endpoints for your org, Experience Cloud sites, or custom domains.

Your Organization

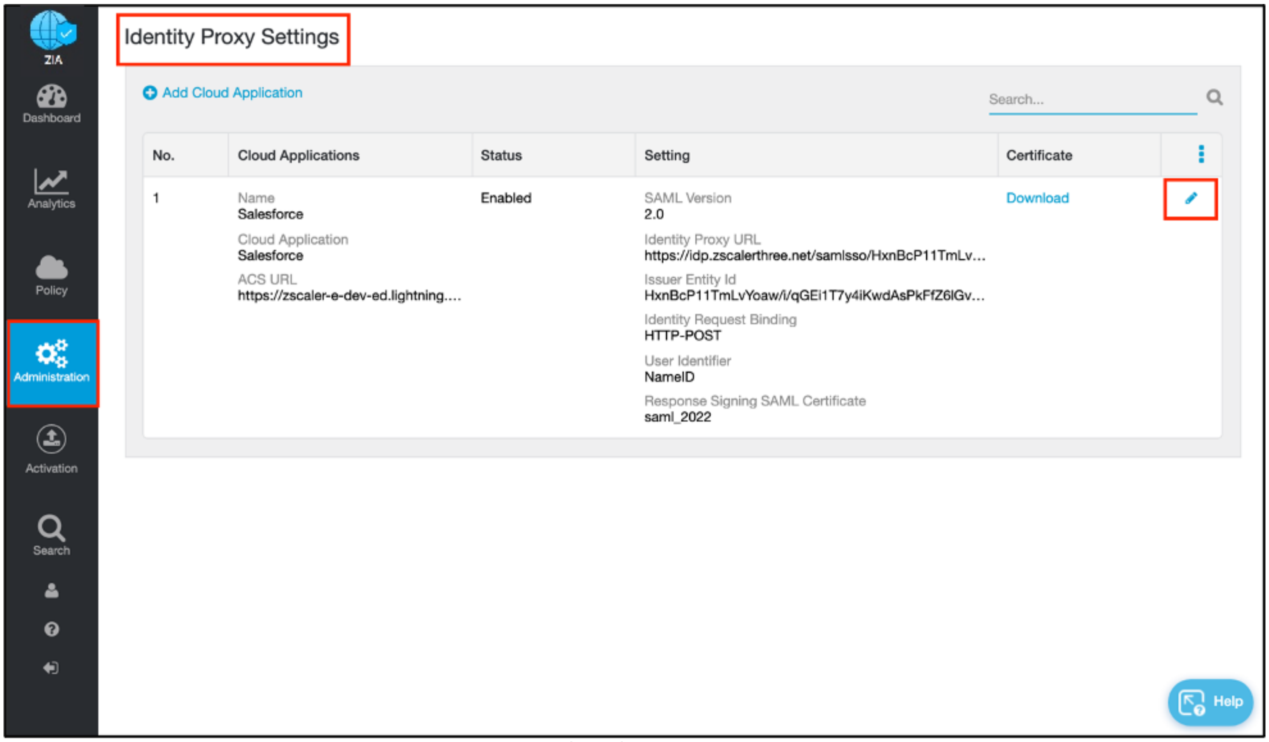
Login URL	https://zscaler-e-dev-ed.my.salesforce.com
Logout URL	https://zscaler-e-dev-ed.my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https://zscaler-e-dev-ed.my.salesforce.com/services/oauth2/token

Figure 17. Copy the Login URL

Completing the Zscaler SaaS Identity Proxy Settings

Return to the Zscaler configuration to complete the SaaS identity proxy.

1. Log in to your ZIA Admin Portal with admin credentials.
2. Go to **Administration > Identity Proxy Settings**.
3. Click the **Edit** icon. This opens the **Edit Cloud Application** window.

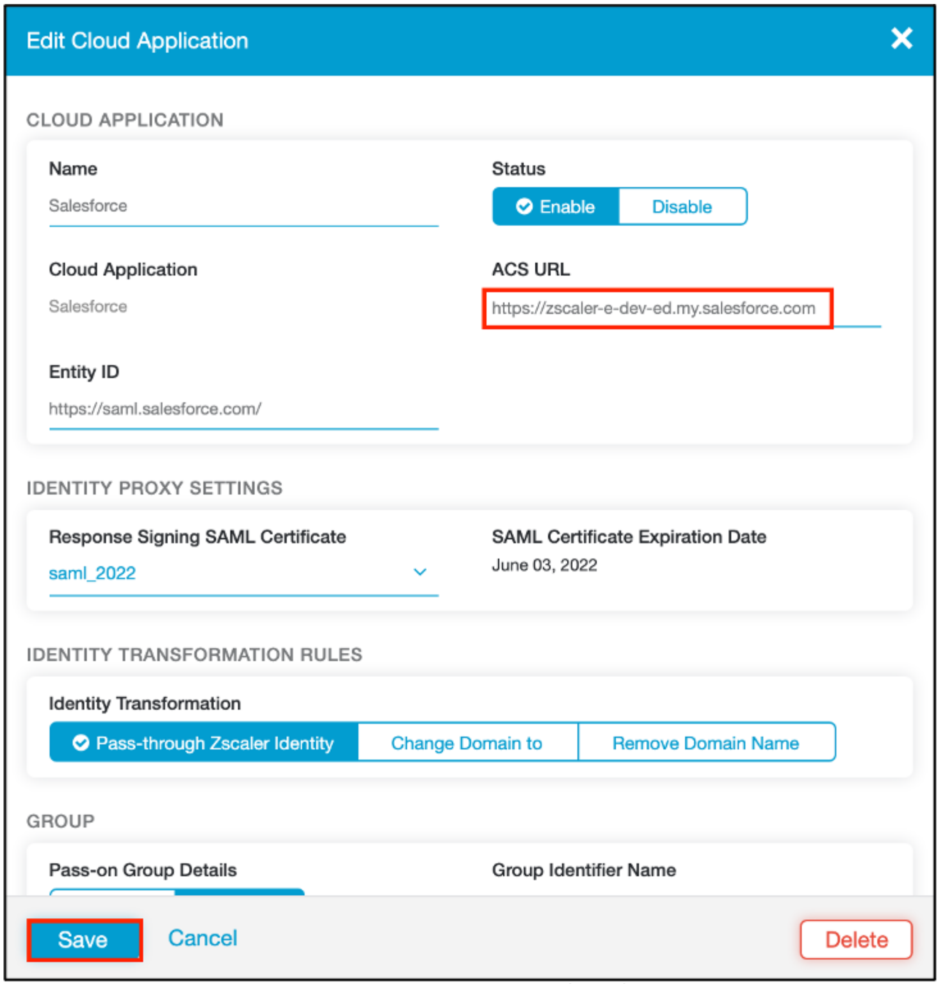


Identity Proxy Settings

No.	Cloud Applications	Status	Setting	Certificate	
1	Name Salesforce Cloud Application Salesforce ACS URL https://zscaler-e-dev-ed.lightning....	Enabled	SAML Version 2.0 Identity Proxy URL https://idp.zscalerthree.net/samlsso/HxnBcP11TmLv... Issuer Entity Id HxnBcP11TmLvYoaw/i/qGEi1T7y4iKwdAsPkFfZ6lGv... Identity Request Binding HTTP-POST User Identifier NameID Response Signing SAML Certificate saml_2022	Download	

Figure 18. Finish the ZIA SaaS identity proxy configuration (1 of 2)

4. Paste the Login URL copied from Salesforce into the **ACS URL** field.
5. Click **Save**.



Edit Cloud Application

CLOUD APPLICATION

Name: Salesforce

Status: Enable | Disable

Cloud Application: Salesforce

ACS URL: https://zscaler-e-dev-ed.my.salesforce.com

Entity ID: https://saml.salesforce.com/

IDENTITY PROXY SETTINGS

Response Signing SAML Certificate: saml_2022

SAML Certificate Expiration Date: June 03, 2022

IDENTITY TRANSFORMATION RULES

Identity Transformation: Pass-through Zscaler Identity | Change Domain to | Remove Domain Name

GROUP

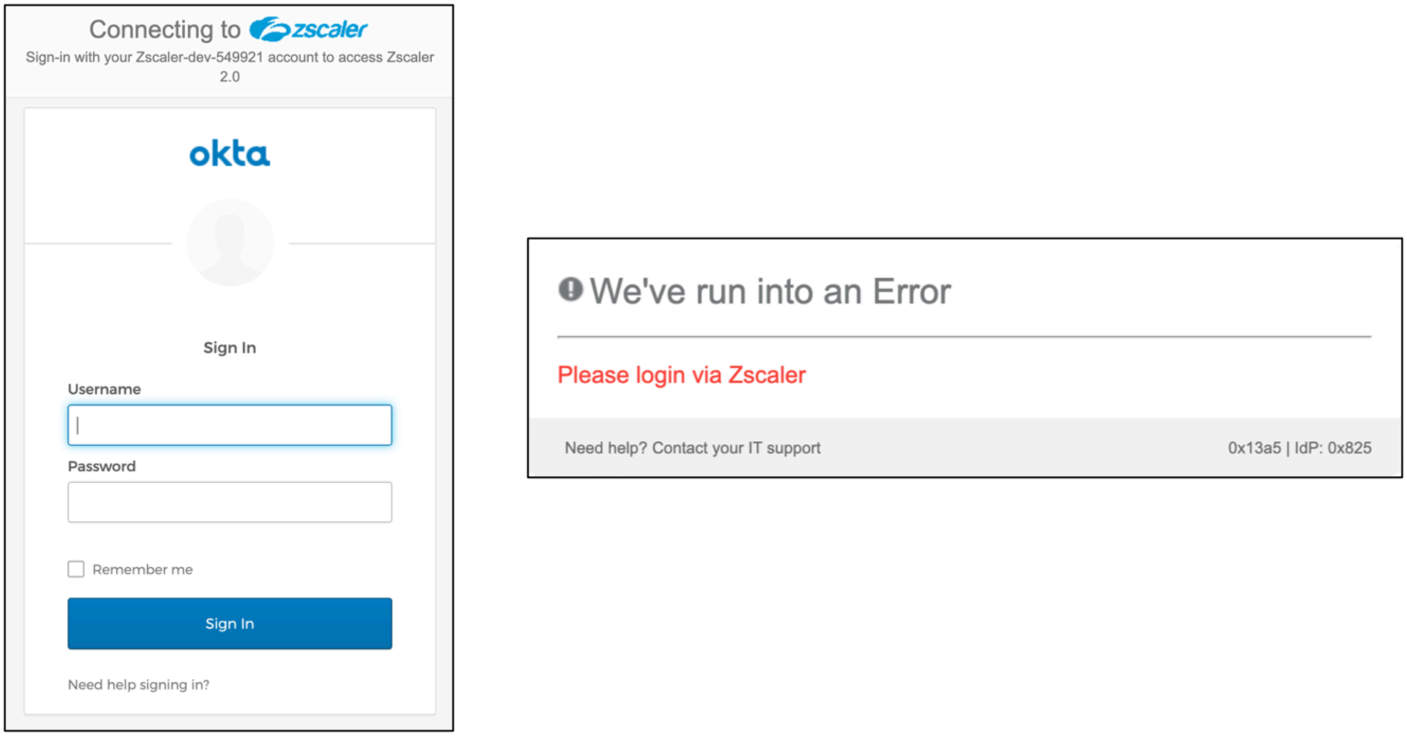
Pass-on Group Details

Group Identifier Name

Figure 19. Finish the ZIA SaaS identity proxy configuration (2 of 2)

The New Identity and Notification Screens

When logging into Salesforce, the ZIA IdP is displayed and asks for user credentials on the IdP user store. If the user attempts to log in to Salesforce without first logging into Zscaler, a dialog is displayed, requesting the user to log in via Zscaler.



Connecting to zscaler

Sign-in with your Zscaler-dev-549921 account to access Zscaler 2.0

We've run into an Error

Please login via Zscaler

Need help? Contact your IT support

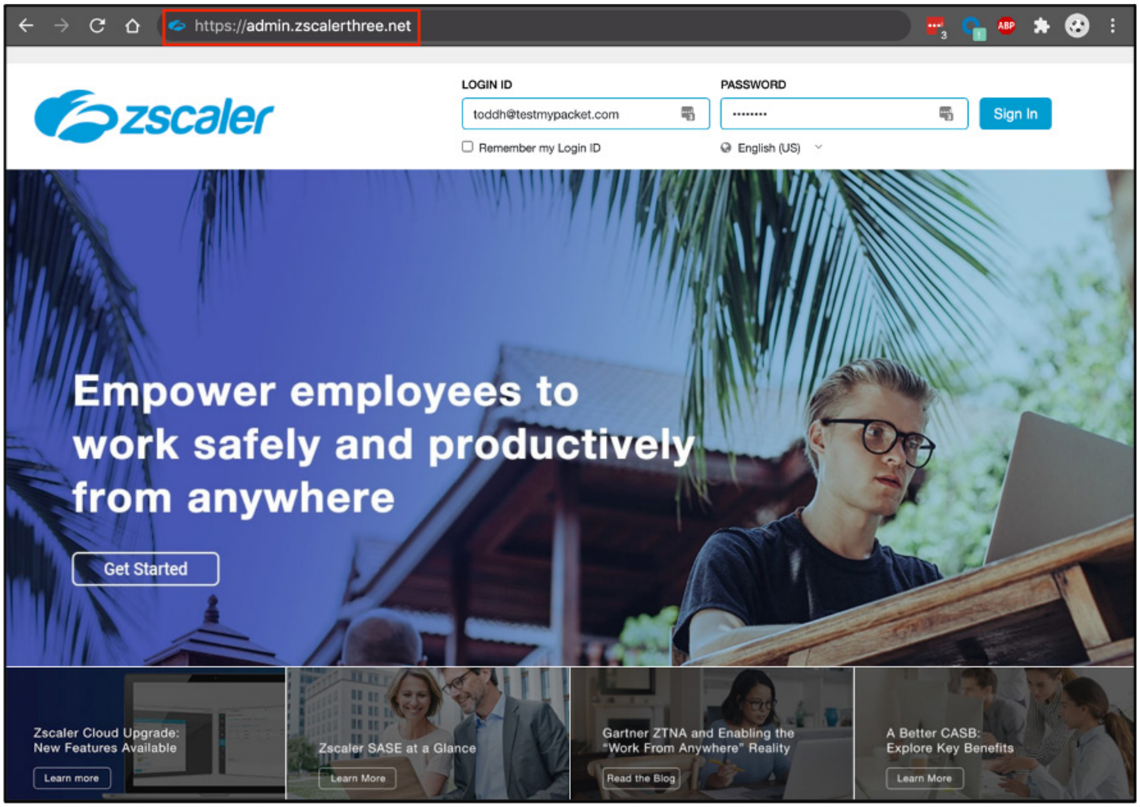
0x13a5 | IdP: 0x825

Figure 20. The new IdP and notification screens

Configuring Zscaler SaaS Security for Salesforce

SaaS Security service configuration builds on itself and is performed on both the Zscaler tenant and the Salesforce tenant. The following steps are for both tenants. Log in to the ZIA Admin Portal tenant to start the configuration process:

- Configuring the Zscaler and the Salesforce Tenant.
- Configuring the Zscaler Tenant on Salesforce.
    - Install the Zscaler package.
    - Create a permission set.
    - Assign the permission set.
- Configuring the Zscaler Salesforce Connector.
- Configuring a SaaS DLP Policy.
- SaaS Malware Policy.
- Configuring the Scan Schedule.



https://admin.zscalerthree.net

LOGIN ID: toddh@testmypacket.com

PASSWORD: ••••••••

□ Remember my Login ID

English (US)

zscaler
Sign In
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More

Figure 21. Creating the Salesforce tenant

Configuring the Zscaler and the Salesforce Tenant

Configure the Salesforce SaaS tenant under Administration in the ZIA Admin Portal.

1. Go to **Administration** > **SaaS Application Tenants**.

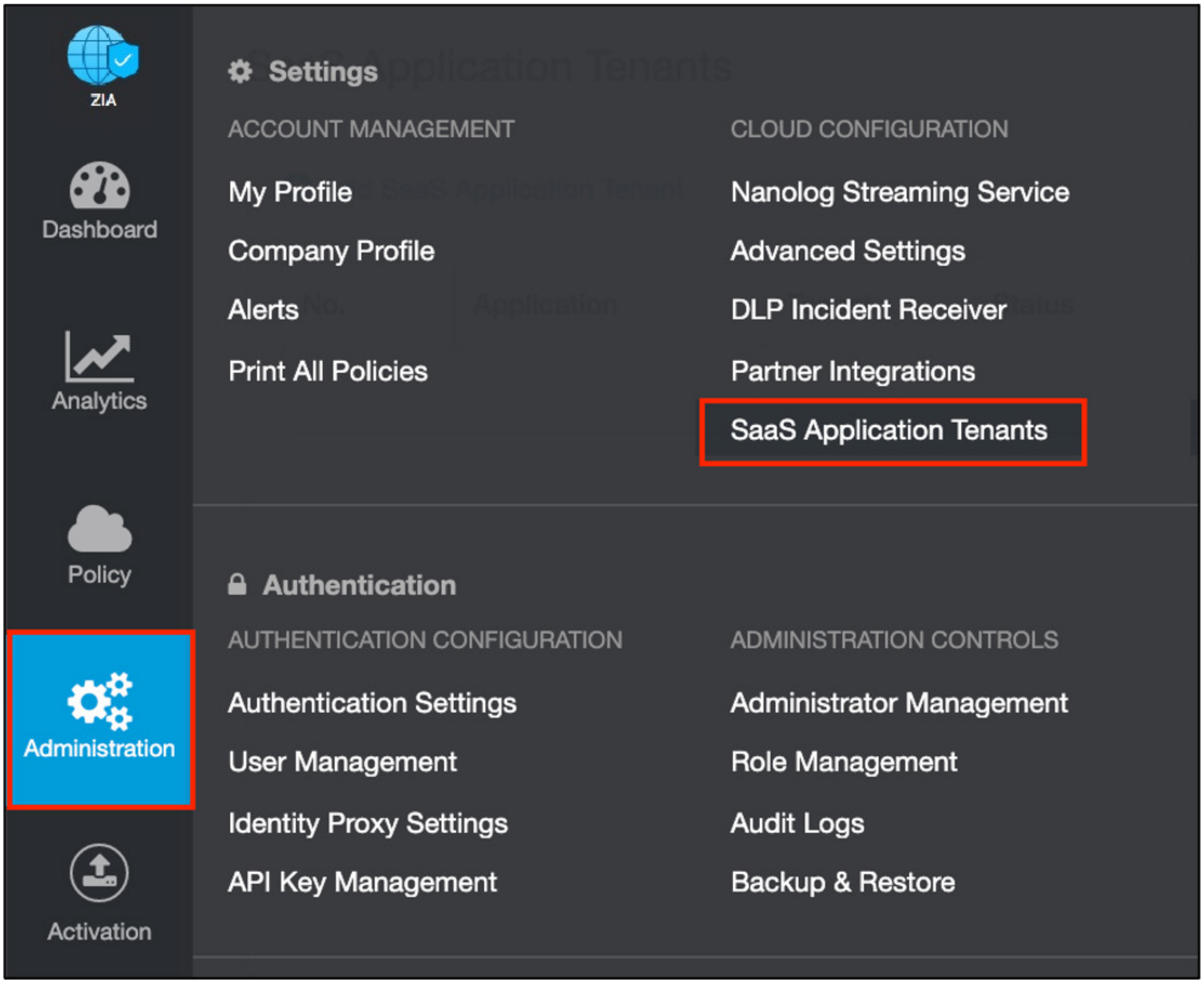
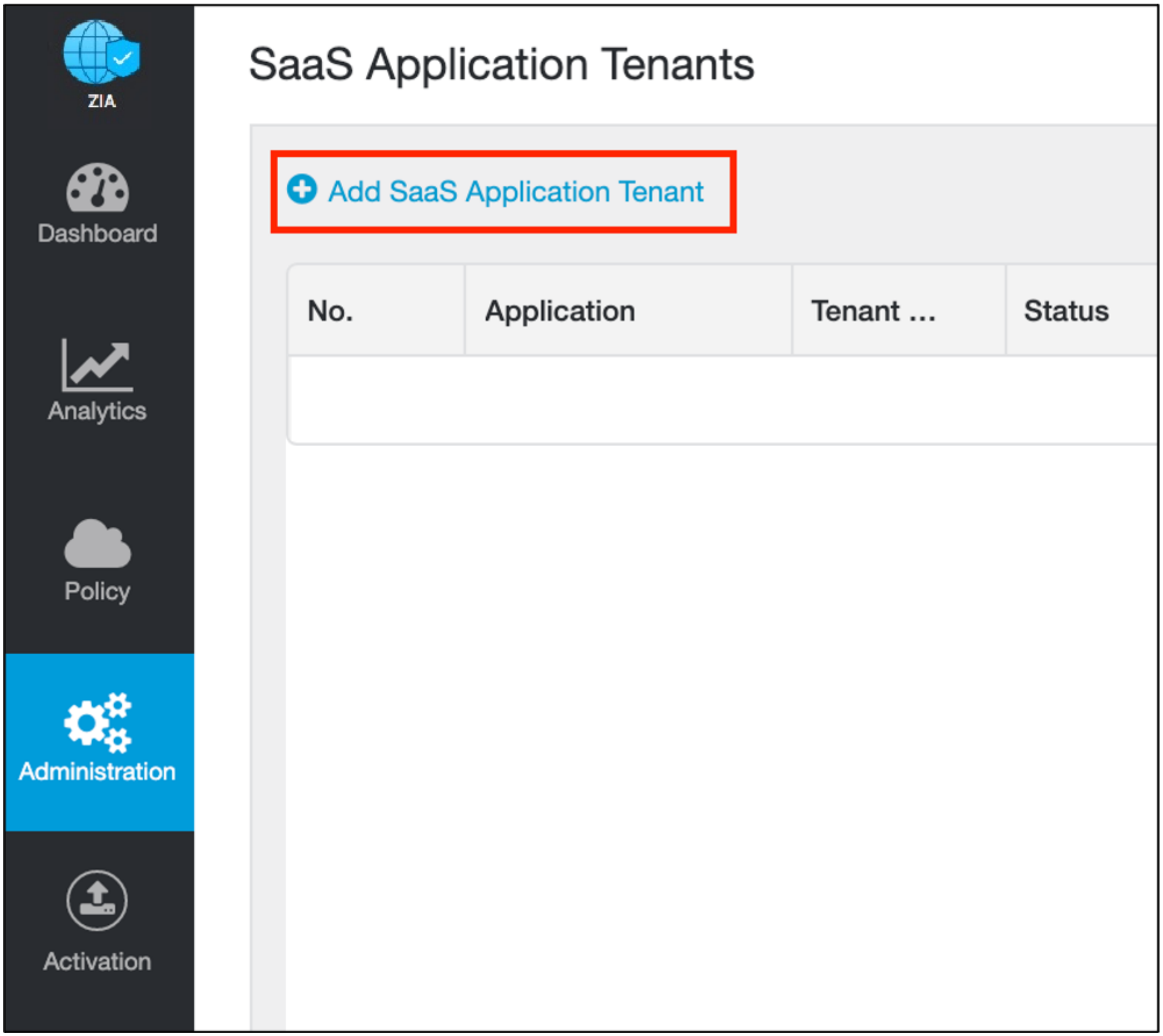


Figure 22. Adding a Salesforce tenant

2. Click **Add SaaS Application Tenant**.



No.	Application	Tenant ...	Status

Figure 23. Adding an application tenant

3. Select the **Salesforce** tile under **Popular Applications**.

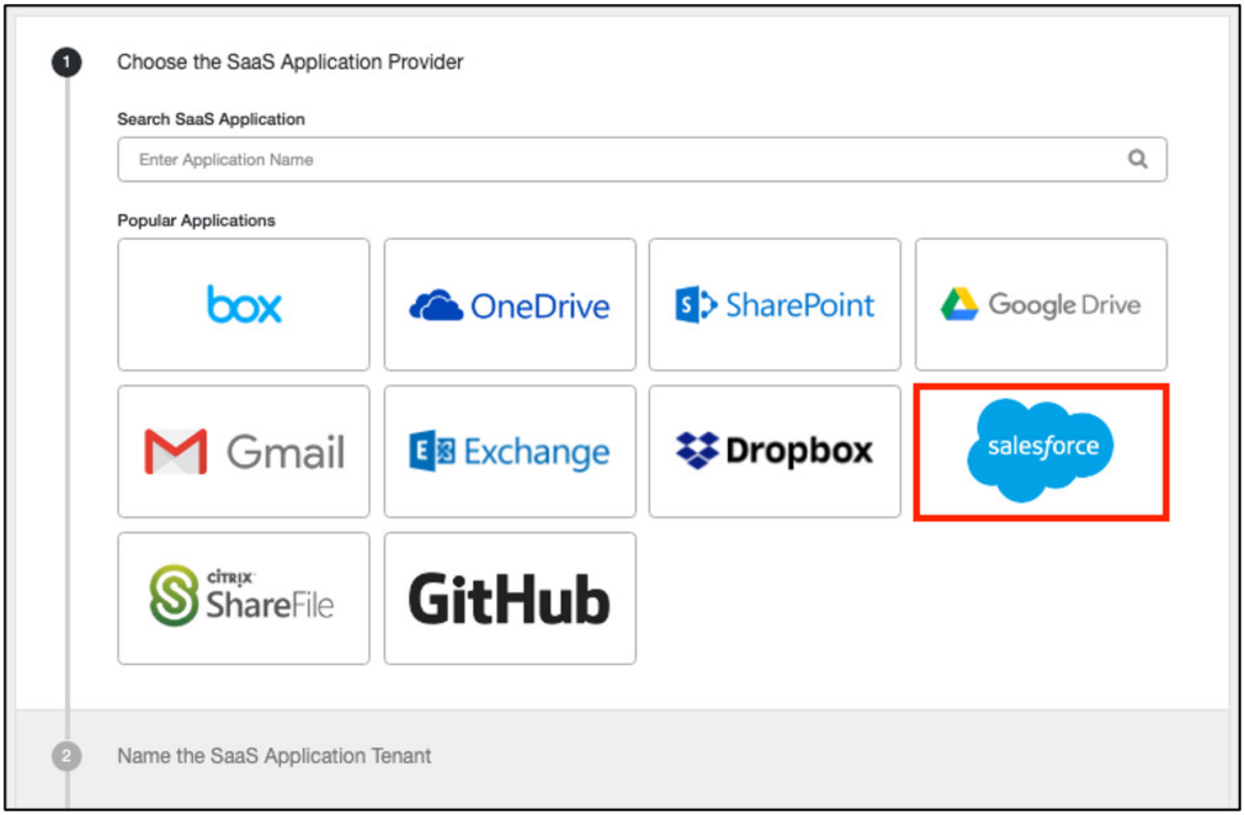


Figure 24. The SaaS Tenant Configuration wizard

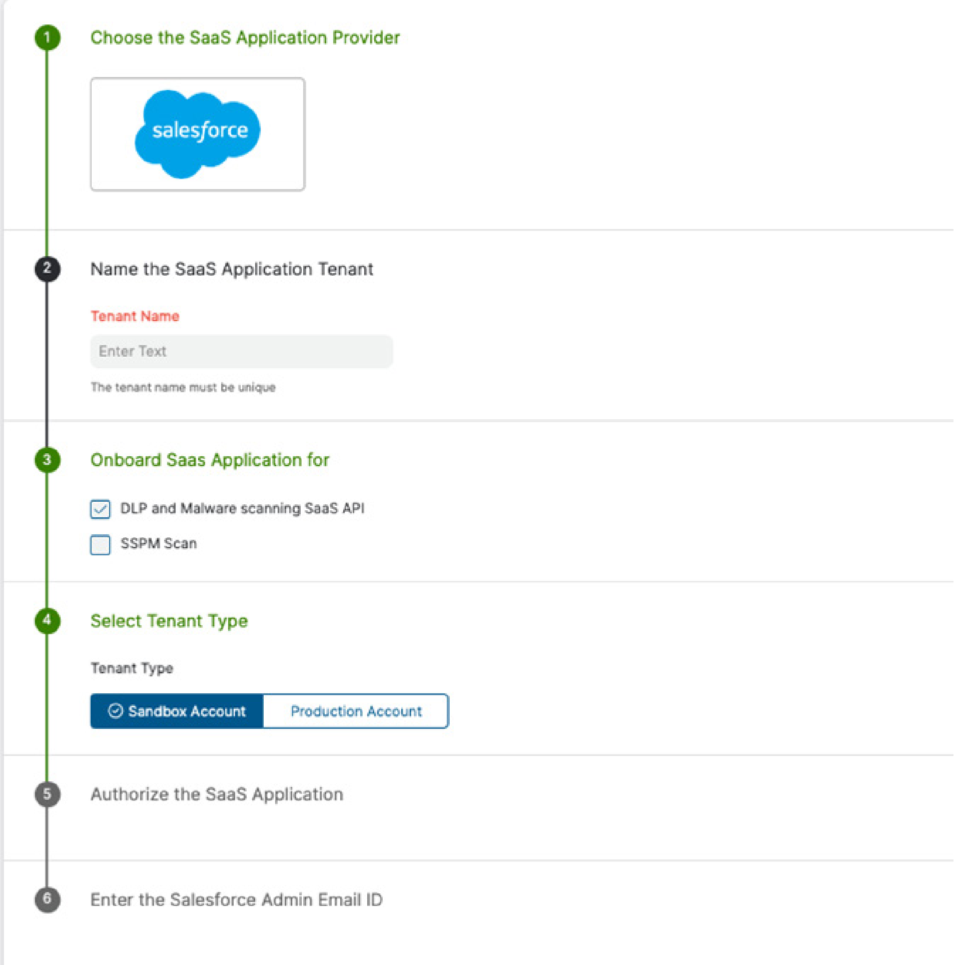
4. Enter a name for the **Tenant Name**. This is the tenant name that is selected when assigning a policy for the Zscaler security features.
5. Select **DLP and Malware scanning SaaS API** for **Onboard SaaS Application for**.
6. For **Select Tenant type**, select either **Sandbox Account** or **Production Account**.

For the **Tenant Type** options:

- **Sandbox Account**: Allows you to access Salesforce from the test.salesforce.com URL where you can test changes without affecting your customers until you move it to your production environment.
- **Production Account**: Allows you to access Salesforce from the login.salesforce.com URL where changes are applied to your production environment and immediately affect customers.

You can add both tenant types separately, but you can't change from a Sandbox Account to a Production Account, or vice versa.

7. Click **Go to Salesforce** to access your Salesforce Admin Console.



1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name

Enter Text

The tenant name must be unique

3 Onboard Saas Application for

☑ DLP and Malware scanning SaaS API

□ SSPM Scan

4 Select Tenant Type

Tenant Type

Sandbox Account | Production Account

5 Authorize the SaaS Application

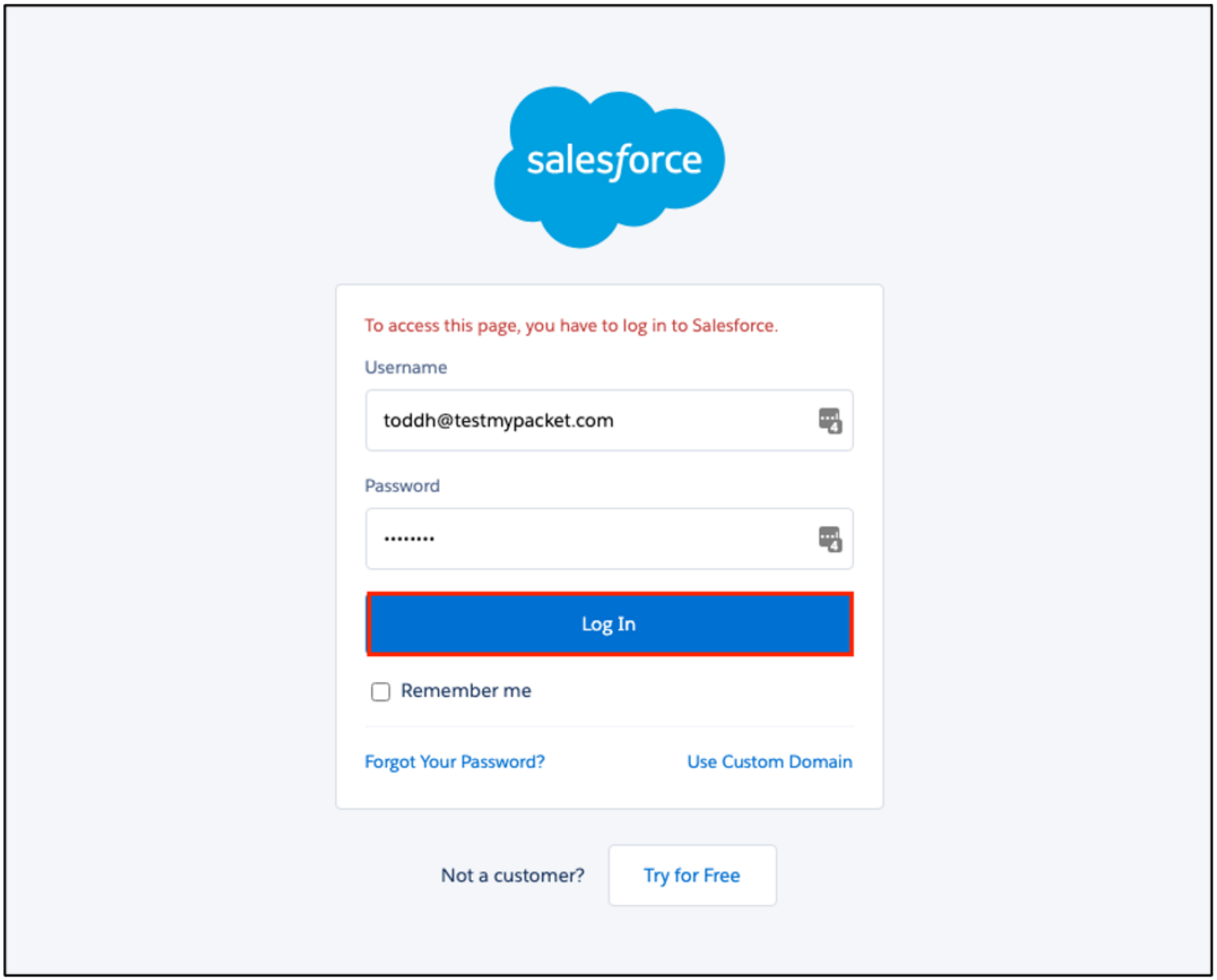
6 Enter the Salesforce Admin Email ID

Figure 25. Open the Salesforce tenant

Configuring the Zscaler Tenant on Salesforce

To configure the Zscaler Tenant from your Salesforce admin account:

1. Log in to Salesforce with admin credentials.



To access this page, you have to log in to Salesforce.

Username

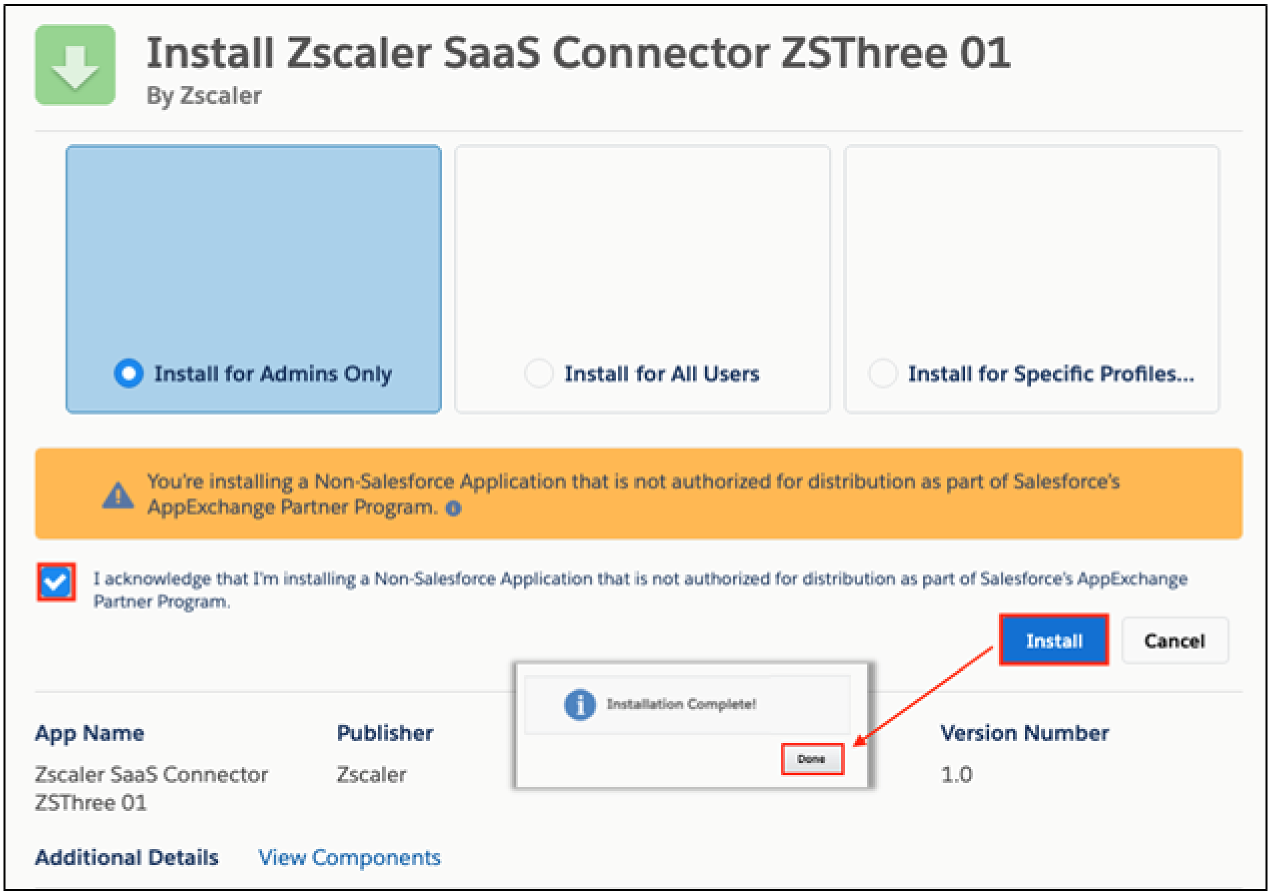
toddh@testmypacket.com

Password

••••••••

Figure 26. Log in to the Salesforce tenant

2. To authorize the custom app that is the Zscaler tenant, select **Install for Admins Only**.
3. Select the checkbox to acknowledge the AppExchange message.
4. Click **Install**.
5. Click **Done** when the installation is complete. You are redirected to the **Installed Packages** page.



Install Zscaler SaaS Connector ZSThree 01

By Zscaler

● Install for Admins Only ○ Install for All Users ○ Install for Specific Profiles...

You're installing a Non-Salesforce Application that is not authorized for distribution as part of Salesforce's AppExchange Partner Program.

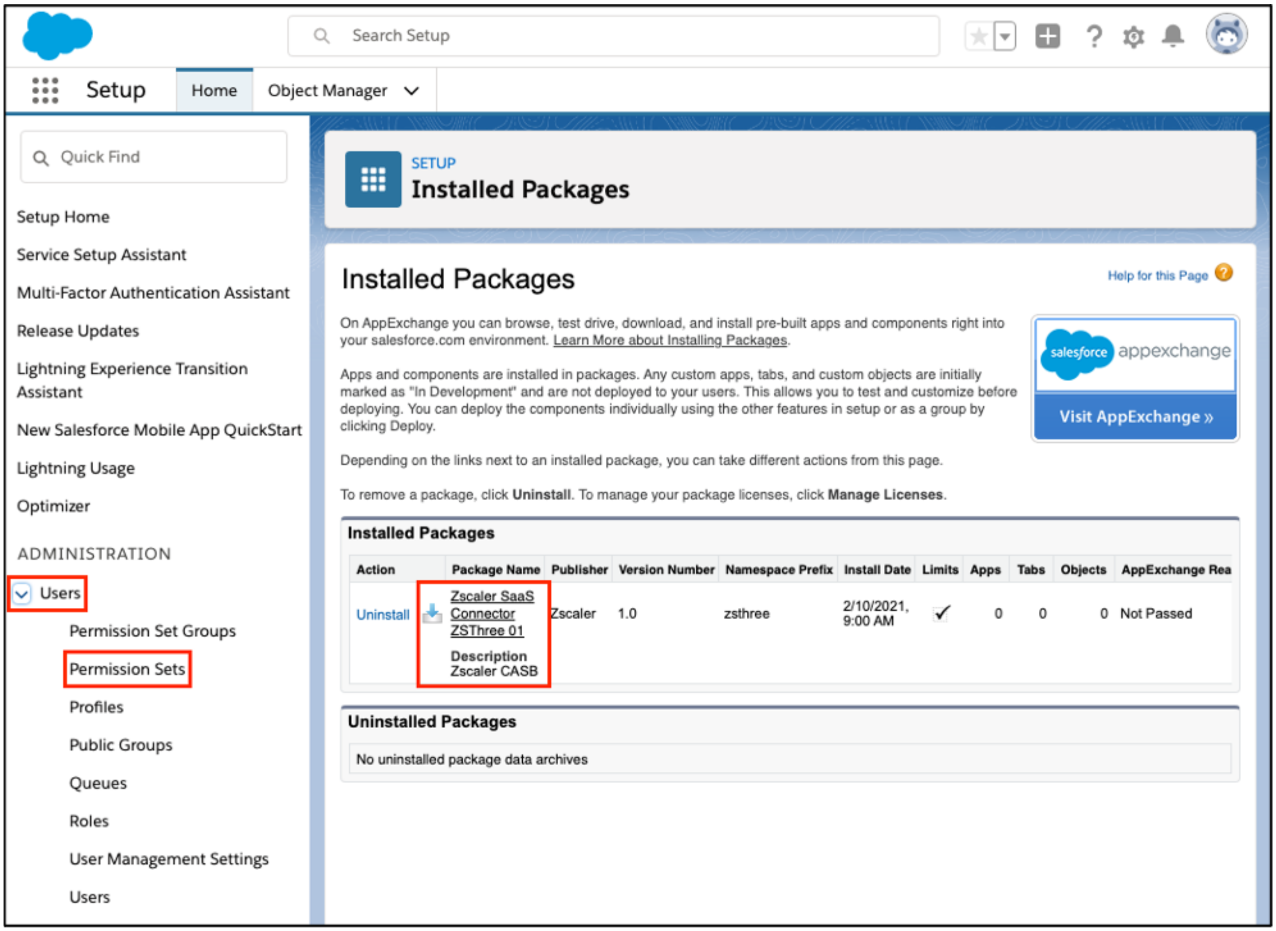
☑ I acknowledge that I'm installing a Non-Salesforce Application that is not authorized for distribution as part of Salesforce's AppExchange Partner Program.

Installation Complete!

App Name	Publisher	Version Number
Zscaler SaaS Connector ZSThree 01	Zscaler	1.0

Figure 27. Install the SaaS Connector

6. Create and assign permission to the user (admin) of the Zscaler application. From the left-side navigation, go to **Users** > **Permission Sets**.



Installed Packages

On AppExchange you can browse, test drive, download, and install pre-built apps and components right into your salesforce.com environment. Learn More about Installing Packages.

Apps and components are installed in packages. Any custom apps, tabs, and custom objects are initially marked as "In Development" and are not deployed to your users. This allows you to test and customize before deploying. You can deploy the components individually using the other features in setup or as a group by clicking Deploy.

Depending on the links next to an installed package, you can take different actions from this page.

To remove a package, click **Uninstall**. To manage your package licenses, click **Manage Licenses**.

Installed Packages

Action	Package Name	Publisher	Version Number	Namespace Prefix	Install Date	Limits	Apps	Tabs	Objects	AppExchange Rea
Uninstall	Zscaler SaaS Connector ZSThree 01 **Description** Zscaler CASB	Zscaler	1.0	zsthree	2/10/2021, 9:00 AM	✓	0	0	0	Not Passed

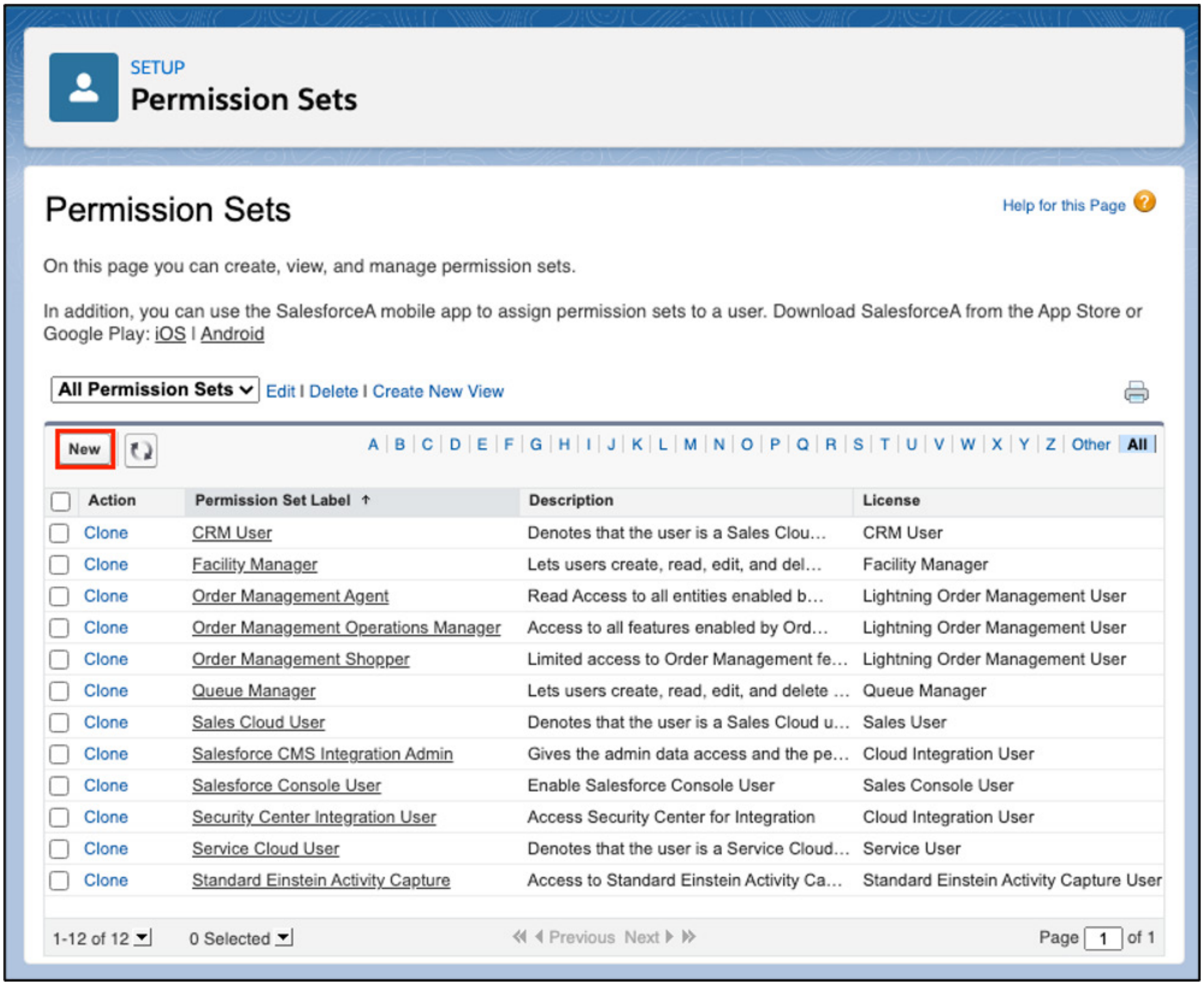
Uninstalled Packages

No uninstalled package data archives

Figure 28. The installed Zscaler SaaS connector

Set Up Permission Sets

Next, you must set up the permission sets. In the **Permission Sets** window, click **New**.



Permission Sets

On this page you can create, view, and manage permission sets.

In addition, you can use the SalesforceA mobile app to assign permission sets to a user. Download SalesforceA from the App Store or Google Play: iOS | Android

All Permission Sets
Edit | Delete | Create New View
New
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All

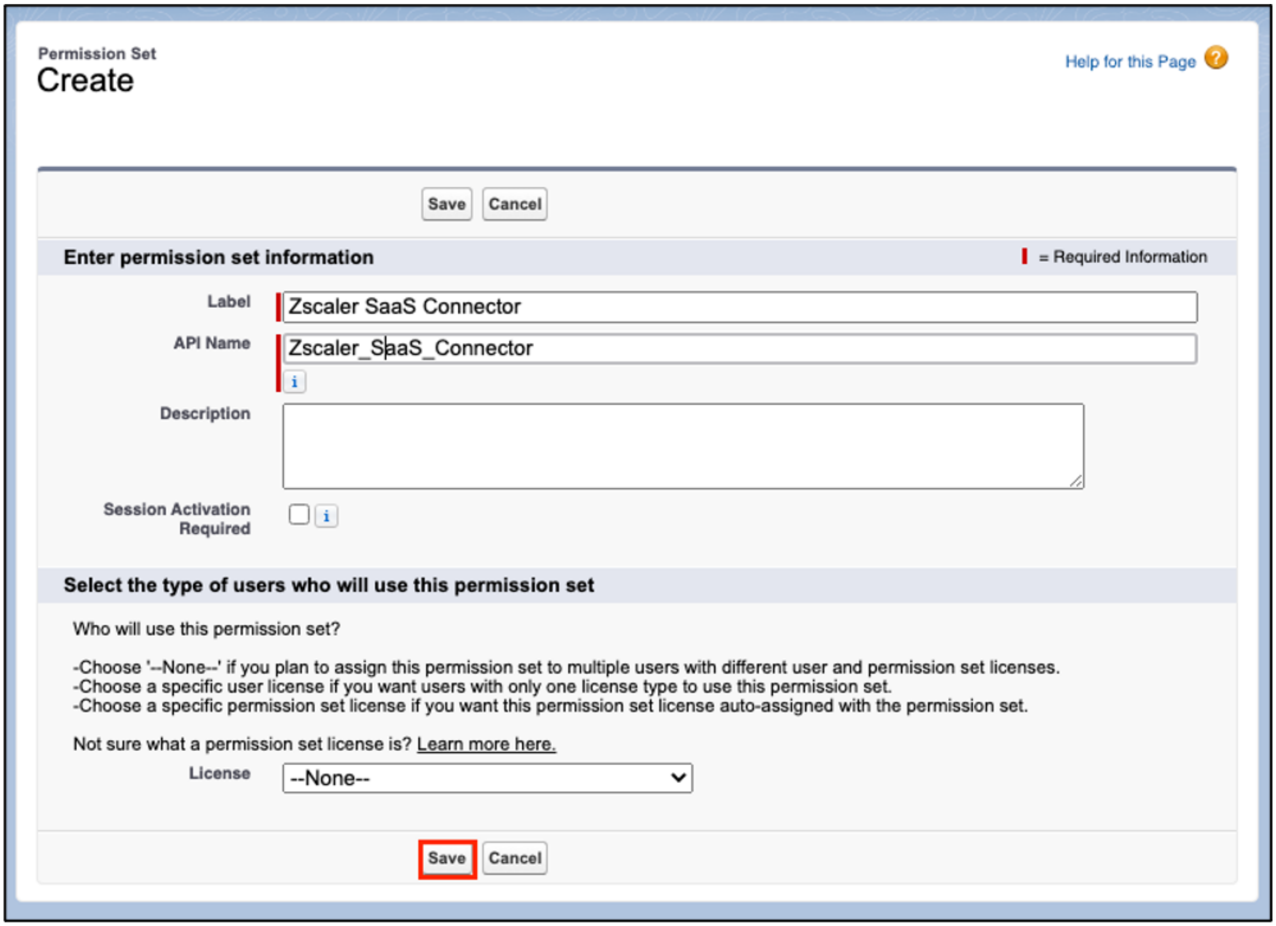
□	Action	Permission Set Label ↑	Description	License
□	Clone	CRM User	Denotes that the user is a Sales Clou…	CRM User
□	Clone	Facility Manager	Lets users create, read, edit, and del…	Facility Manager
□	Clone	Order Management Agent	Read Access to all entities enabled b…	Lightning Order Management User
□	Clone	Order Management Operations Manager	Access to all features enabled by Ord…	Lightning Order Management User
□	Clone	Order Management Shopper	Limited access to Order Management fe…	Lightning Order Management User
□	Clone	Queue Manager	Lets users create, read, edit, and delete …	Queue Manager
□	Clone	Sales Cloud User	Denotes that the user is a Sales Cloud u…	Sales User
□	Clone	Salesforce CMS Integration Admin	Gives the admin data access and the pe…	Cloud Integration User
□	Clone	Salesforce Console User	Enable Salesforce Console User	Sales Console User
□	Clone	Security Center Integration User	Access Security Center for Integration	Cloud Integration User
□	Clone	Service Cloud User	Denotes that the user is a Service Cloud…	Service User
□	Clone	Standard Einstein Activity Capture	Access to Standard Einstein Activity Ca…	Standard Einstein Activity Capture User

Figure 29. Creating permission sets

Create Permission Sets for the Admin Account

In the **Create Permission Set** window:

1. Enter a **Label** for the permission set.
2. Enter an **API Name**.
3. Click **Save**.



Permission Set

Create

Enter permission set information

= Required Information

Label	Zscaler SaaS Connector
API Name	Zscaler_SaaS_Connector
Description	
Session Activation Required	□

Select the type of users who will use this permission set

Who will use this permission set?

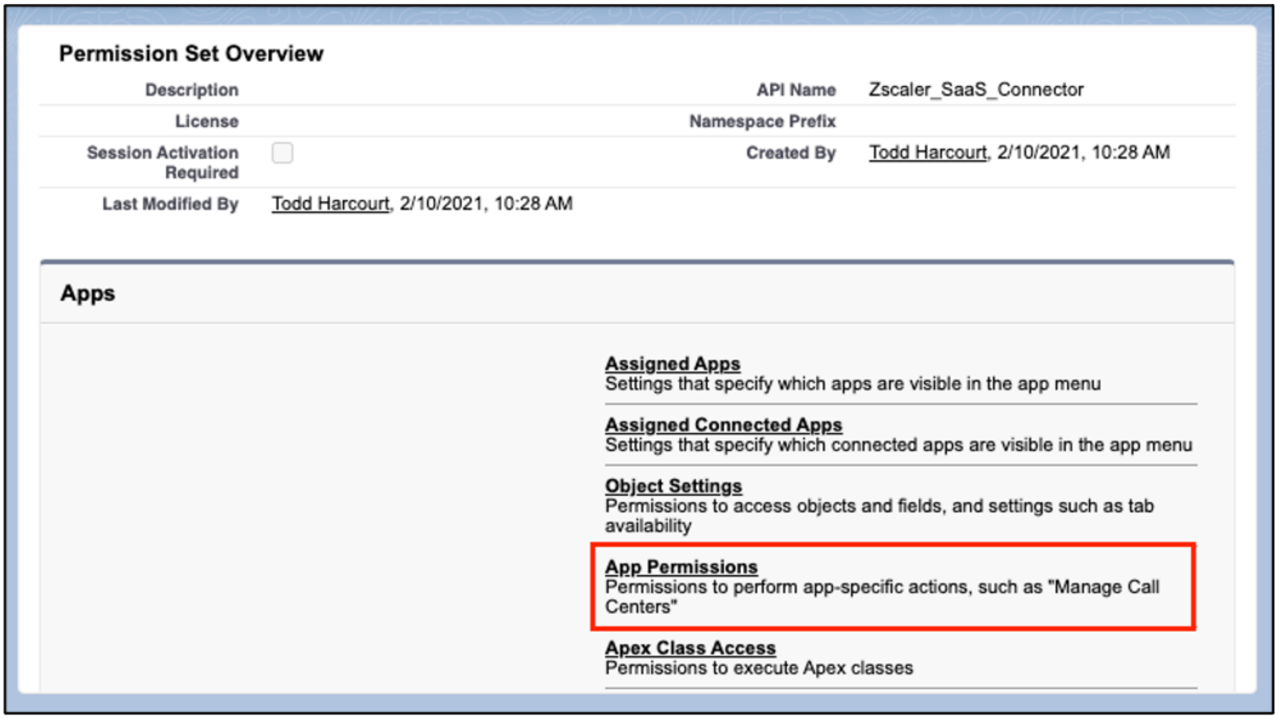
-Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission set licenses.
-Choose a specific user license if you want users with only one license type to use this permission set.
-Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? Learn more here.

License: --None--

Figure 30. Creating permission sets

4. In the **Apps** section, select **App Permissions**.



Permission Set Overview

Description		API Name	Zscaler_SaaS_Connector
License		Namespace Prefix	
Session Activation Required	□	Created By	Todd Harcourt, 2/10/2021, 10:28 AM
Last Modified By	Todd Harcourt, 2/10/2021, 10:28 AM		

Apps

Assigned Apps
Settings that specify which apps are visible in the app menu

Assigned Connected Apps
Settings that specify which connected apps are visible in the app menu

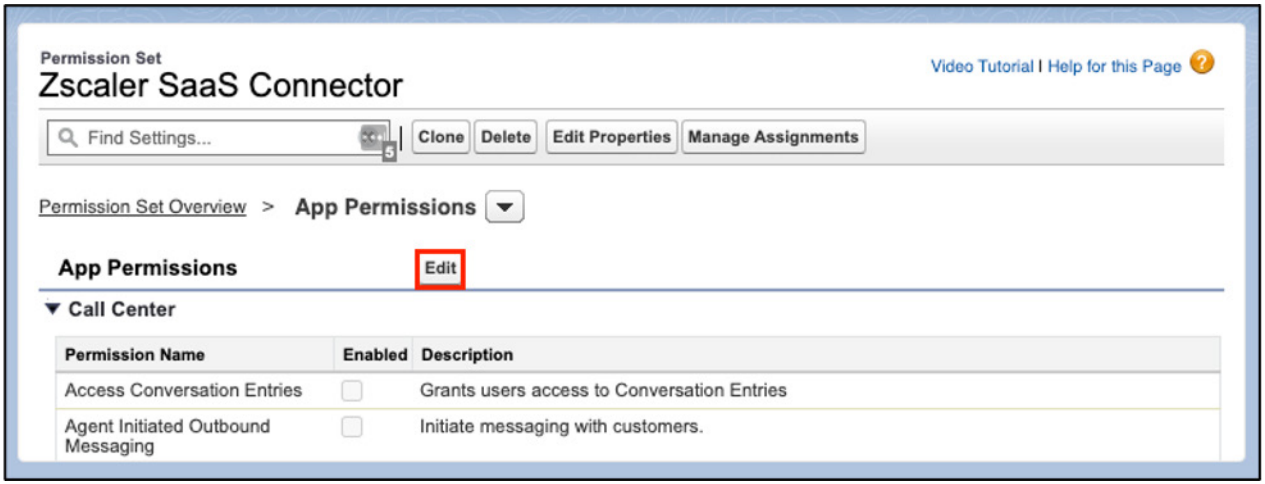
Object Settings
Permissions to access objects and fields, and settings such as tab availability

App Permissions
Permissions to perform app-specific actions, such as "Manage Call Centers"

Apex Class Access
Permissions to execute Apex classes

Figure 31. App permissions

5. Click **Edit**.



Permission Set
Zscaler SaaS Connector

Video Tutorial | Help for this Page
Find Settings...
Clone
Delete
Edit Properties
Manage Assignments
Permission Set Overview > App Permissions
Edit

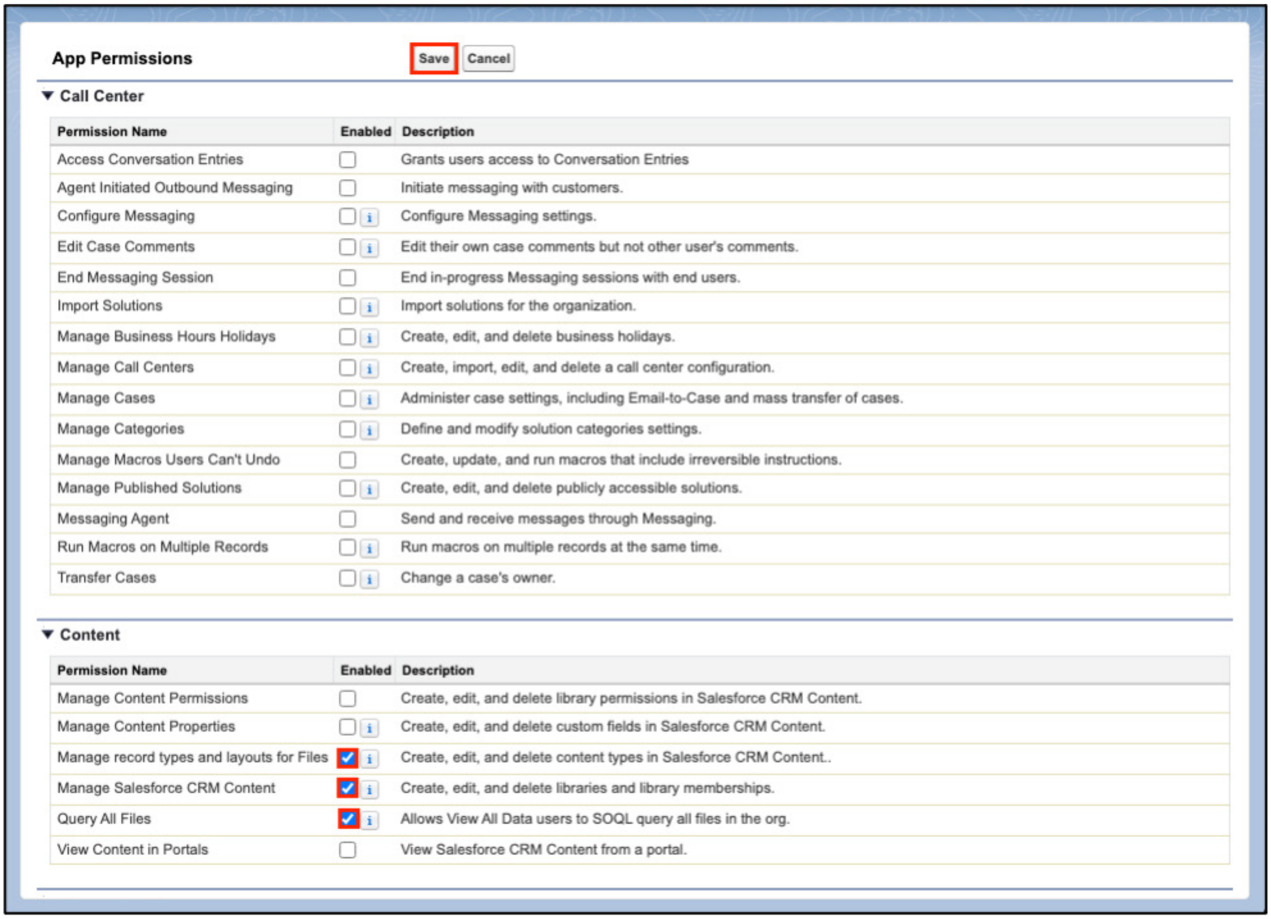
App Permissions

▼ Call Center

Permission Name	Enabled	Description
Access Conversation Entries	□	Grants users access to Conversation Entries
Agent Initiated Outbound Messaging	□	Initiate messaging with customers.

Figure 32. Editing app permissions

6. Under the **Content** section, select the **Manage record types and layouts for Files** checkbox.
7. Select the **Manage Salesforce CRM Content** checkbox.
8. Select the **Query All Files** checkbox.
9. Click **Save**.



App Permissions Save Cancel

▼ **Call Center**

Permission Name	Enabled	Description
Access Conversation Entries	□	Grants users access to Conversation Entries
Agent Initiated Outbound Messaging	□	Initiate messaging with customers.
Configure Messaging	□ i	Configure Messaging settings.
Edit Case Comments	□ i	Edit their own case comments but not other user's comments.
End Messaging Session	□	End in-progress Messaging sessions with end users.
Import Solutions	□ i	Import solutions for the organization.
Manage Business Hours Holidays	□ i	Create, edit, and delete business holidays.
Manage Call Centers	□ i	Create, import, edit, and delete a call center configuration.
Manage Cases	□ i	Administer case settings, including Email-to-Case and mass transfer of cases.
Manage Categories	□ i	Define and modify solution categories settings.
Manage Macros Users Can't Undo	□	Create, update, and run macros that include irreversible instructions.
Manage Published Solutions	□ i	Create, edit, and delete publicly accessible solutions.
Messaging Agent	□	Send and receive messages through Messaging.
Run Macros on Multiple Records	□ i	Run macros on multiple records at the same time.
Transfer Cases	□ i	Change a case's owner.

▼ **Content**

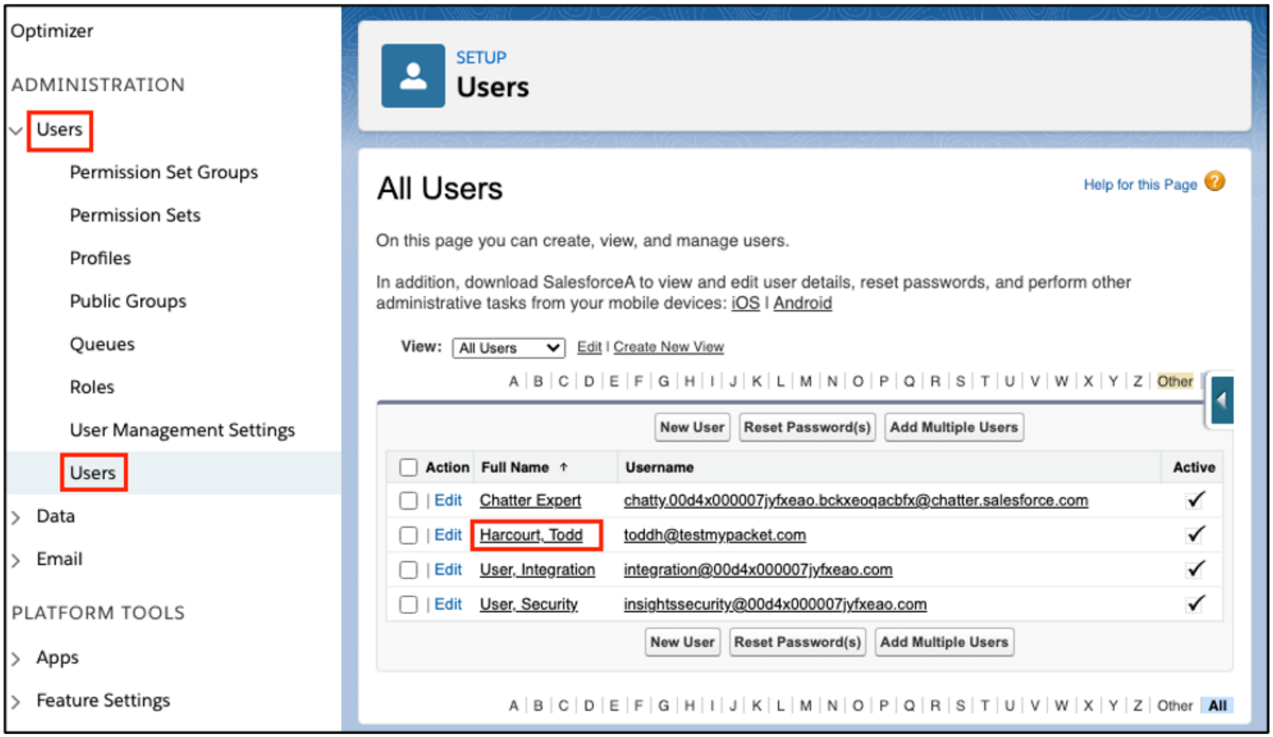
Permission Name	Enabled	Description
Manage Content Permissions	□	Create, edit, and delete library permissions in Salesforce CRM Content.
Manage Content Properties	□ i	Create, edit, and delete custom fields in Salesforce CRM Content.
Manage record types and layouts for Files	☑ i	Create, edit, and delete content types in Salesforce CRM Content..
Manage Salesforce CRM Content	☑ i	Create, edit, and delete libraries and library memberships.
Query All Files	☑ i	Allows View All Data users to SOQL query all files in the org.
View Content in Portals	□	View Salesforce CRM Content from a portal.

Figure 33. Enable and save app permissions

Assign the Permission Set

Under **Account & Billing** of the Salesforce admin account, select and save the enterprise ID. This ID is pasted into the Zscaler wizard and identifies the Salesforce SaaS ID. It allows the Zscaler API to provide security services to this Salesforce tenant. In the **Optimizer** pane, under **Administration**:

1. Select **Users** > **Users**.
2. Select the name to assign permissions (do not select **Edit**).
3. On the next screen, click **Permission Set Assignments**.
4. Click **Edit** for the assignments.



All Users

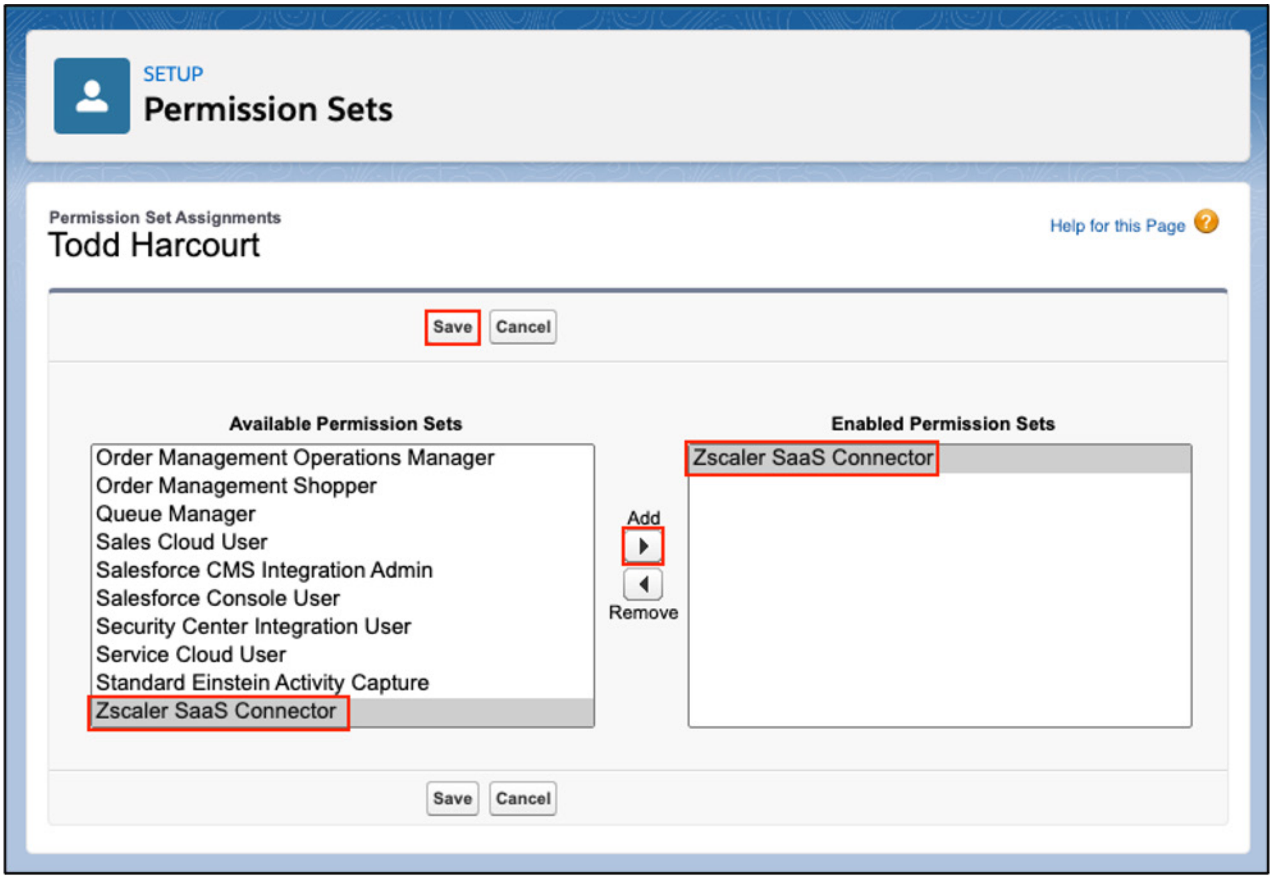
On this page you can create, view, and manage users.

In addition, download SalesforceA to view and edit user details, reset passwords, and perform other administrative tasks from your mobile devices: iOS | Android

☐ Action	Full Name ↑	Username	Active
☐ | Edit	Chatter Expert	chatty.00d4x000007jyfxeao.bckxeoqacbfx@chatter.salesforce.com	✓
☐ | Edit	Harcourt, Todd	toddh@testmypacket.com	✓
☐ | Edit	User, Integration	integration@00d4x000007jyfxeao.com	✓
☐ | Edit	User, Security	insightssecurity@00d4x000007jyfxeao.com	✓

Figure 34. Assign the permission sets to the administrator

5. On the **Setup** screen for permission sets, select the permission set that you created.
6. Click **Add** to add it to the **Enabled Permission Sets**.
7. Click **Save** (located above the permission set panes).


SETUP

Permission Sets

Permission Set Assignments

Todd Harcourt

Available Permission Sets

- Order Management Operations Manager
- Order Management Shopper
- Queue Manager
- Sales Cloud User
- Salesforce CMS Integration Admin
- Salesforce Console User
- Security Center Integration User
- Service Cloud User
- Standard Einstein Activity Capture
- Zscaler SaaS Connector

Enabled Permission Sets

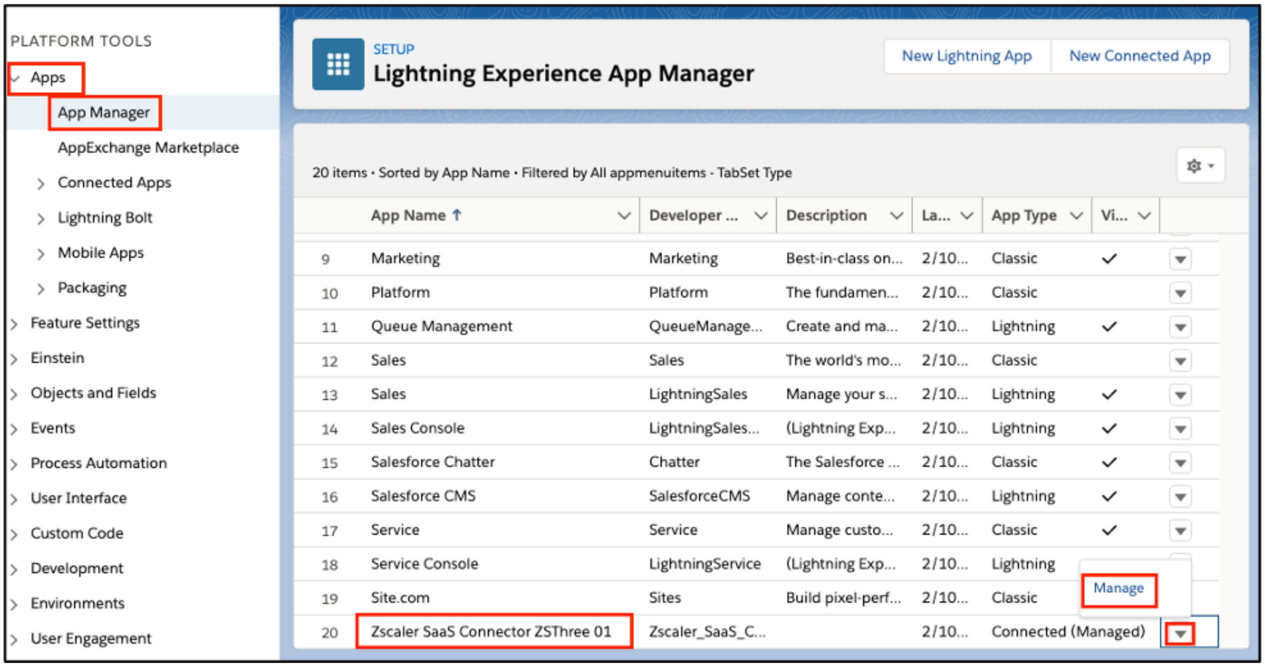
- Zscaler SaaS Connector

Figure 35. Adding the permission set to the admin

Configuring the Zscaler Salesforce Connector

Configure the application connector. In **Setup** under **Platform Tools**:

1. Go to **Apps** > **App Manager**.
2. Find the Zscaler SaaS connector you created and click the **Expand** icon on the right.
3. Select **Manage** from the drop-down menu.



20 items • Sorted by App Name • Filtered by All appmenuitems - TabSet Type

	App Name ↑	Developer ...	Description	La...	App Type	Vi...	
9	Marketing	Marketing	Best-in-class on...	2/10...	Classic	✓	▾
10	Platform	Platform	The fundamen...	2/10...	Classic		▾
11	Queue Management	QueueManage...	Create and ma...	2/10...	Lightning	✓	▾
12	Sales	Sales	The world's mo...	2/10...	Classic		▾
13	Sales	LightningSales	Manage your s...	2/10...	Lightning	✓	▾
14	Sales Console	LightningSales...	(Lightning Exp...	2/10...	Lightning	✓	▾
15	Salesforce Chatter	Chatter	The Salesforce ...	2/10...	Classic	✓	▾
16	Salesforce CMS	SalesforceCMS	Manage conte...	2/10...	Lightning	✓	▾
17	Service	Service	Manage custo...	2/10...	Classic	✓	▾
18	Service Console	LightningService	(Lightning Exp...	2/10...	Lightning		
19	Site.com	Sites	Build pixel-perf...	2/10...	Classic		
20	Zscaler SaaS Connector ZSThree 01	Zscaler_SaaS_C...		2/10...	Connected (Managed)		▾

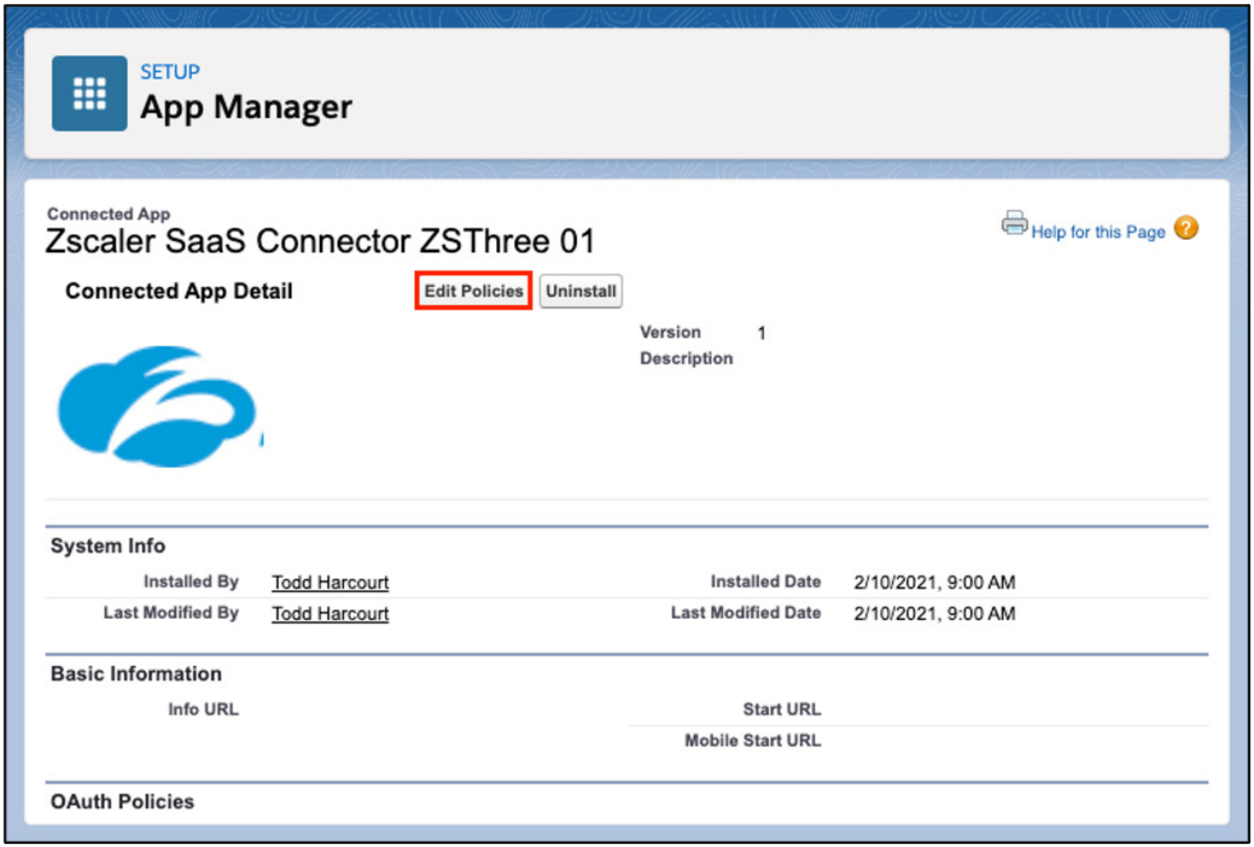
Figure 36. Manage the Zscaler connector

The suffix on the application connector changes based on your Zscaler cloud name. In the example, the SaaS connector you created was for a ZIA tenant hosted by Zscaler Three Cloud.

Configuring the Zscaler Tenant on Salesforce

In the **App Manager** wizard:

1. Click **Edit Policies**.



SETUP

App Manager

Connected App

Zscaler SaaS Connector ZSThree 01

Connected App Detail

Version 1

Description

System Info

Installed By Todd Harcourt

Installed Date 2/10/2021, 9:00 AM

Last Modified By Todd Harcourt

Last Modified Date 2/10/2021, 9:00 AM

Basic Information

Info URL

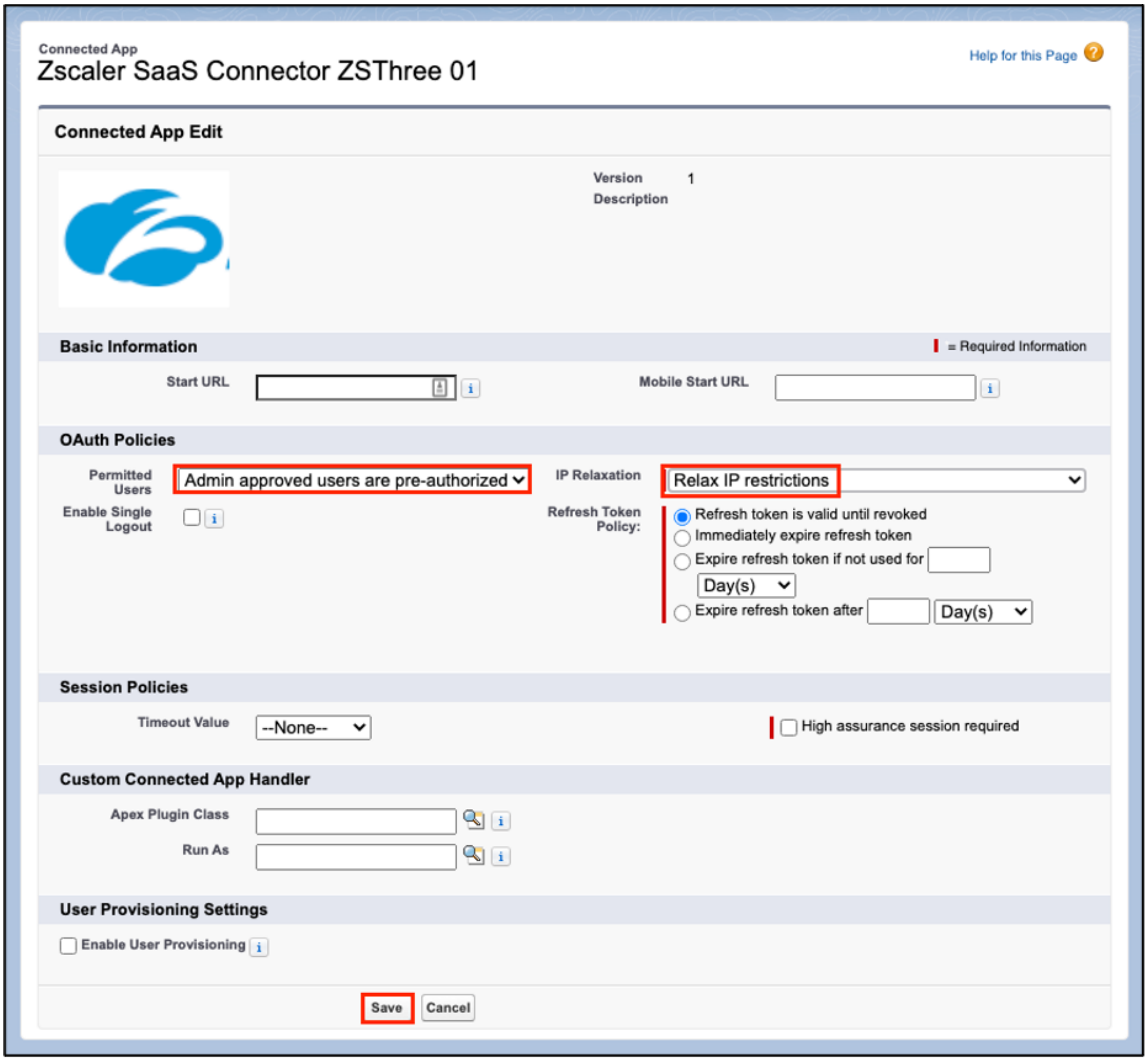
Start URL

Mobile Start URL

OAuth Policies

Figure 37. Editing policies

2. On the **Connected App** window under **OAuth Policies**, select **Admin approved users are pre-authorized** from the **Permitted Users** drop-down menu.
3. Select **Relax IP restrictions** from the **IP Relaxation** drop-down menu.
4. Click **Save**.



Connected App

Zscaler SaaS Connector ZSThree 01

Help for this Page

Connected App Edit

Version 1

Description

Basic Information | = Required Information

Start URL

Mobile Start URL

OAuth Policies

Permitted Users: Admin approved users are pre-authorized

IP Relaxation: Relax IP restrictions

Enable Single Logout □

Refresh Token Policy:
● Refresh token is valid until revoked
○ Immediately expire refresh token
○ Expire refresh token if not used for Day(s)
○ Expire refresh token after Day(s)

Session Policies

Timeout Value: --None--

□ High assurance session required

Custom Connected App Handler

Apex Plugin Class

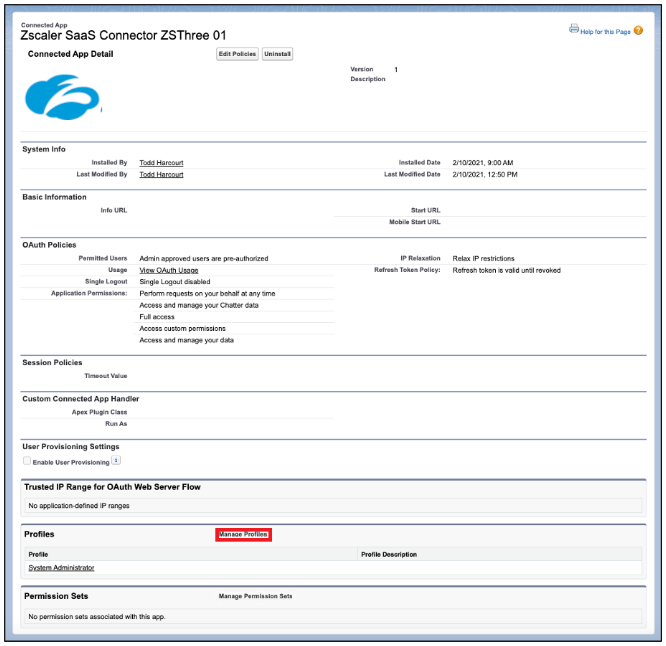
Run As

User Provisioning Settings

□ Enable User Provisioning

Figure 38. Relax IP restrictions

5. Further down the page of the **Connected App** window, edit the **Profiles** by selecting **Manage Profiles**.



Connected App
Zscaler SaaS Connector ZSThree 01

Connected App Detail

Version 1
Description

System Info

Installed By Todd Harcourt
Last Modified By Todd Harcourt
Installed Date 2/10/2021, 9:00 AM
Last Modified Date 2/10/2021, 12:50 PM

Basic Information

Info URL
Start URL
Mobile Start URL

OAuth Policies

Permitted Users Admin approved users are pre-authorized
Usage View OAuth Usage
Single Logout Single Logout disabled
Application Permissions: Perform requests on your behalf at any time
Access and manage your Chatter data
Full access
Access custom permissions
Access and manage your data
IP Relaxation Relax IP restrictions
Refresh Token Policy: Refresh token is valid until revoked

Session Policies

Timeout Value

Custom Connected App Handler

Apex Plugin Class
Run As

User Provisioning Settings

□ Enable User Provisioning

Trusted IP Range for OAuth Web Server Flow

No application-defined IP ranges

Profiles

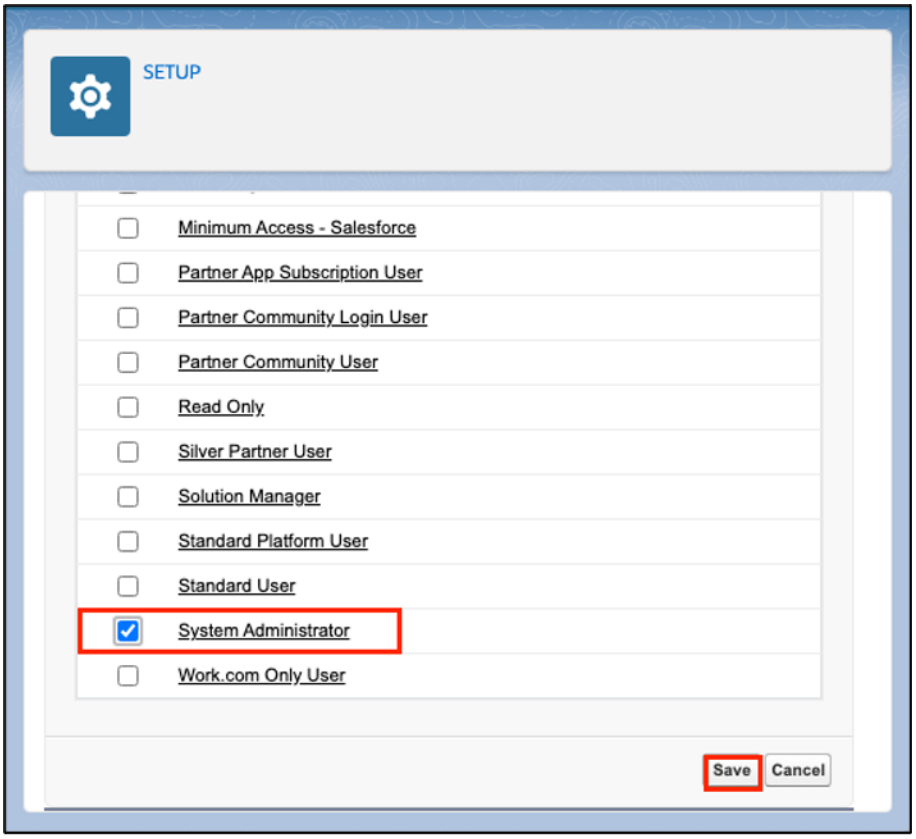
Profile	Profile Description
System Administrator	

Permission Sets

No permission sets associated with this app.

Figure 39. Adding admin privileges to a user

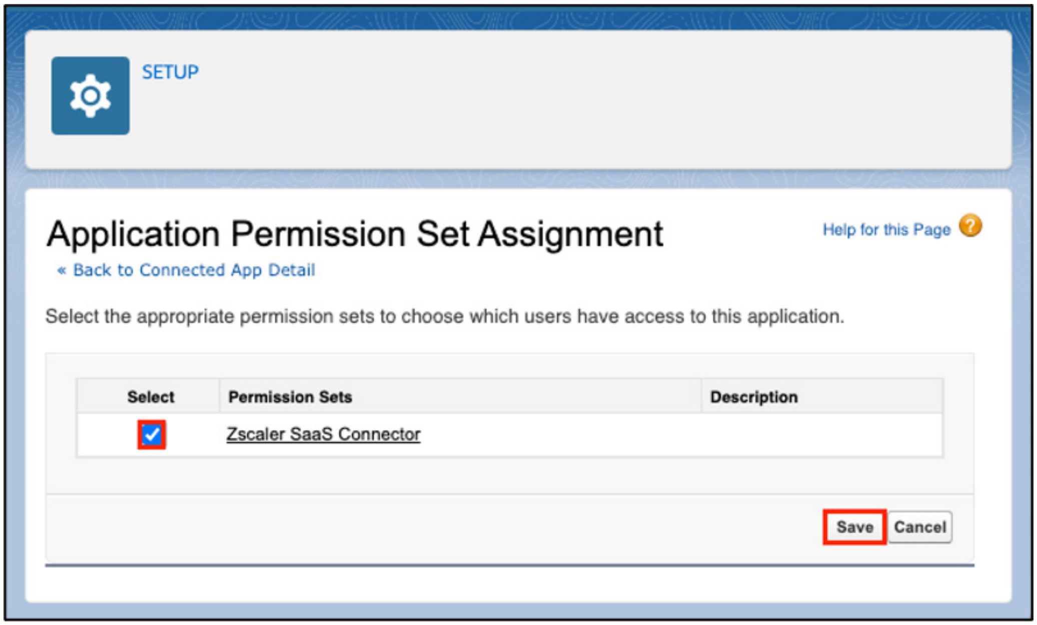
6. Select the **System Administrator** checkbox.



□ Minimum Access - Salesforce
□ Partner App Subscription User
□ Partner Community Login User
□ Partner Community User
□ Read Only
□ Silver Partner User
□ Solution Manager
□ Standard Platform User
□ Standard User
☑ System Administrator
□ Work.com Only User

Figure 40. Assign administrator privileges

7. Click **Save**.
8. Click **Manage Permission Sets**.
9. Under **Application Permission Set Assignment**, select the **Zscaler SaaS Connector** checkbox.
10. Click **Save**.



Application Permission Set Assignment

« Back to Connected App Detail

Select the appropriate permission sets to choose which users have access to this application.

Select	Permission Sets	Description
☑	Zscaler SaaS Connector	

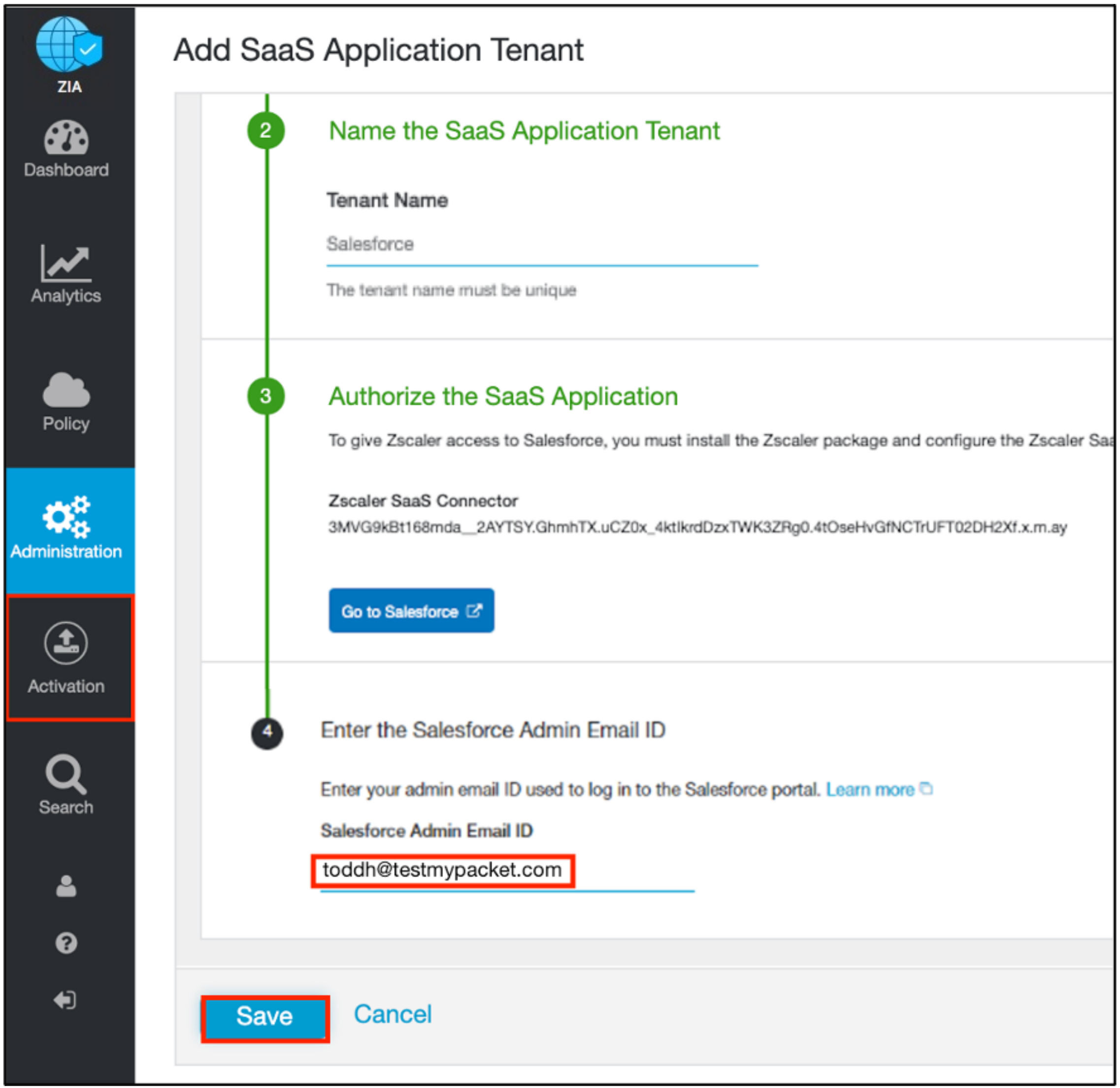
Figure 41. Save the permission and privilege changes

11. Return to the Zscaler setup to finish the configuration.

Finish the Zscaler Side Tenant

On Step 4 of the **Add SaaS Application Tenant** wizard:

1. Enter the **Salesforce Admin Email ID** used to create the Zscaler SaaS connector.
2. Click **Save** to finish the configuration.
3. Click **Activation** to activate changes.



Add SaaS Application Tenant

2 Name the SaaS Application Tenant

Tenant Name: Salesforce

The tenant name must be unique

3 Authorize the SaaS Application

To give Zscaler access to Salesforce, you must install the Zscaler package and configure the Zscaler Saa

Zscaler SaaS Connector: 3MVG9kBt168mda__2AYTSY.GhmhTX.uCZ0x_4ktlkrdDzxTWK3ZRg0.4tOseHvGfNCTrUFT02DH2Xf.x.m.ay

4 Enter the Salesforce Admin Email ID

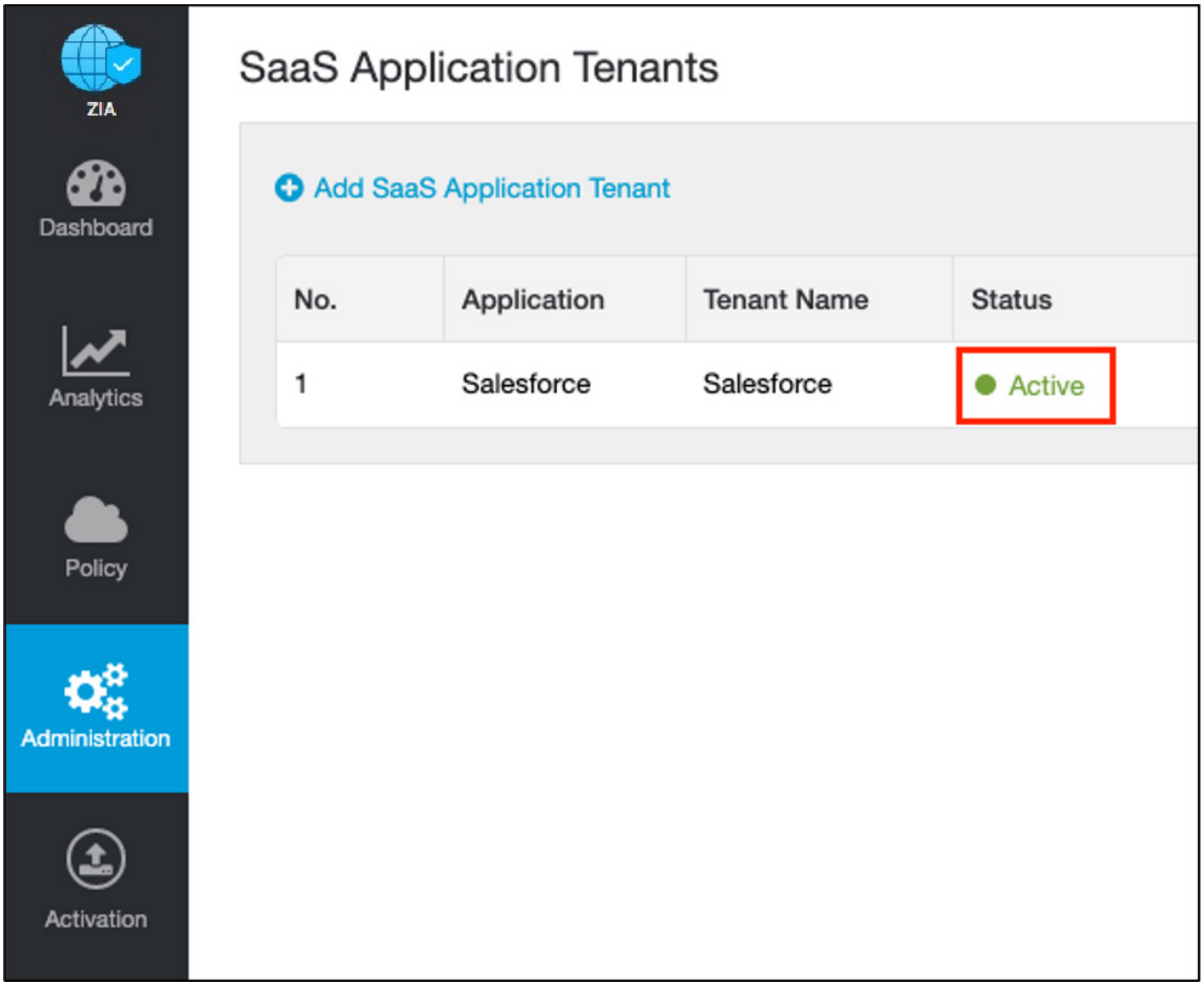
Enter your admin email ID used to log in to the Salesforce portal. Learn more

Salesforce Admin Email ID: toddh@testmypacket.com

Figure 42. Add the Salesforce admin to the ZIA SaaS tenant

The Active Salesforce SaaS API Tenant

The API credentials and connectivity are validated. Refresh your browser to verify the Salesforce tenant is **Active**.



SaaS Application Tenants

No.	Application	Tenant Name	Status
1	Salesforce	Salesforce	● Active

Figure 43. The active tenant

Configuring Salesforce Policies and Scan Configuration

After adding and configuring the Salesforce tenant, you can configure the SaaS security DLP policy, malware detection policy, the scan configuration for the policies, and the options for the SaaS security posture policy. You can also view reports and data for the tenants in the SaaS security report, SaaS security insights, and logs.

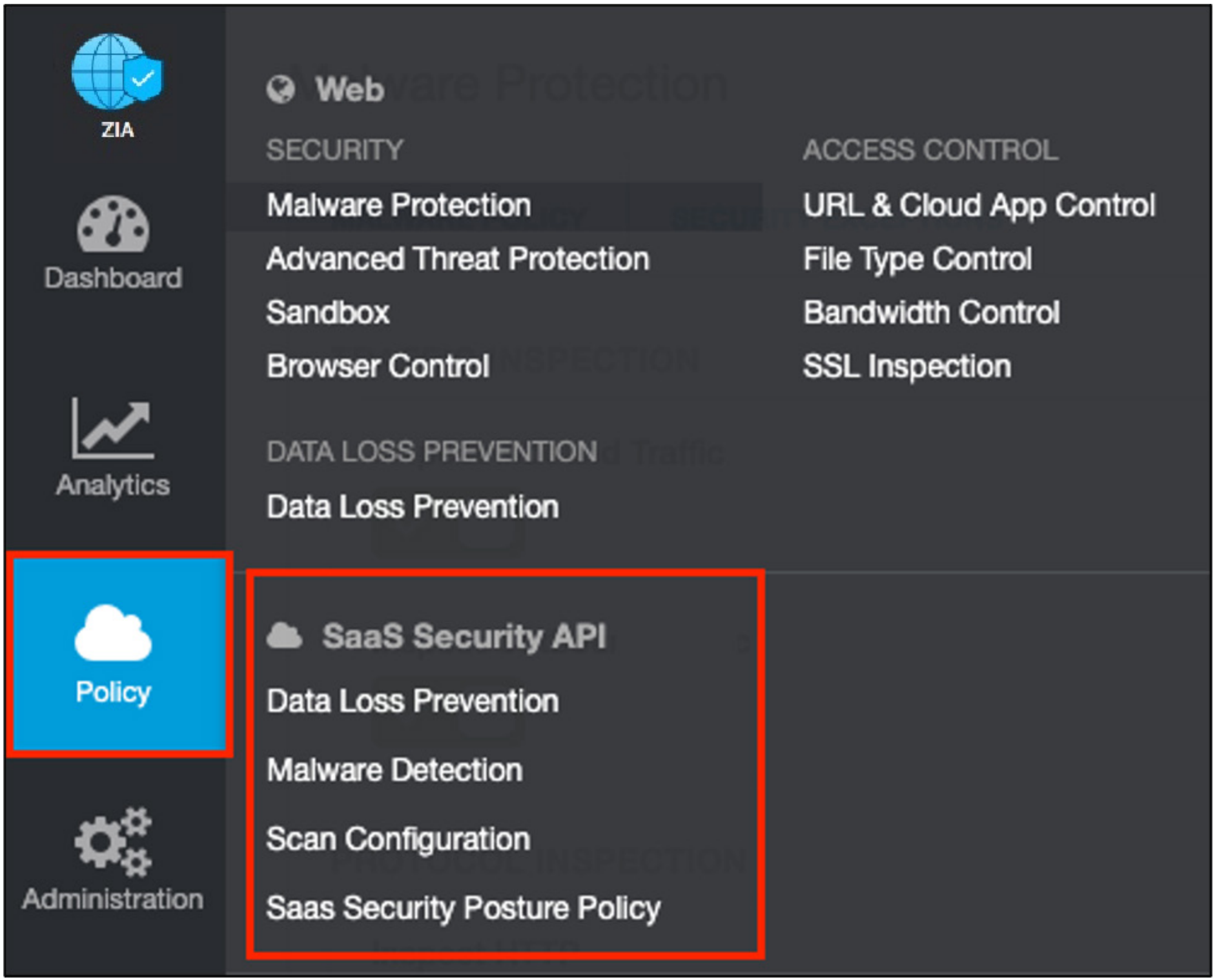
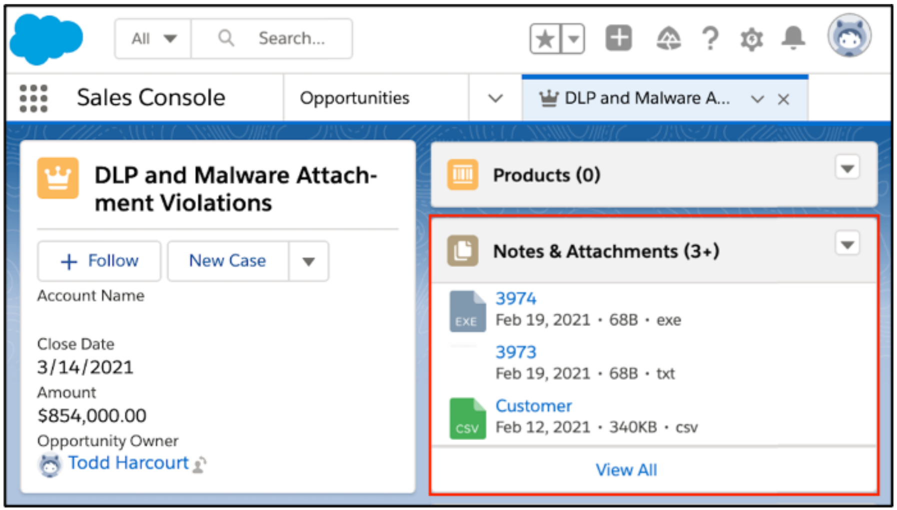


Figure 44. Zscaler policy configuration

Scoping the Policies and Remediation

Zscaler SaaS security scans file attachments and chatter messages. This deployment guide configures a basic DLP policy and a malware policy, and then scans the Salesforce account attachment files for matching DLP content and malware.



DLP and Malware Attachment Violations

Account Name

Close Date
3/14/2021

Amount
$854,000.00

Opportunity Owner
Todd Harcourt

3974
Feb 19, 2021 • 68B • exe

3973
Feb 19, 2021 • 68B • txt

Customer
Feb 12, 2021 • 340KB • csv

Figure 45. Salesforce user account with malicious attachments

Zscaler SaaS security out-of-band data protection capabilities look inside the SaaS applications themselves through API integrations to identify accidental or intentional data exposure and compliance violations that would otherwise go unnoticed.

The DLP policy creates a very broad criteria to identify a spreadsheet with a list of US Social Security numbers. DLP is a subject of its own, and this policy is only used only for demonstration purposes. You must conduct a true DLP policy review to minimize false positives and false negatives.

It is also important to note that the SaaS DLP protection is only part of the Zscaler DLP solution, and is used to scan data at rest like the Salesforce files. This deployment doesn't cover inline data protection or exact data match, although they are integral pieces of a data protection solution.

The next steps are testing the DLP SaaS functionality. Create a basic policy and apply it to the Salesforce tenant. If you already have DLP policies created, see Configure a SaaS Malware Policy.

Creating a DLP Policy

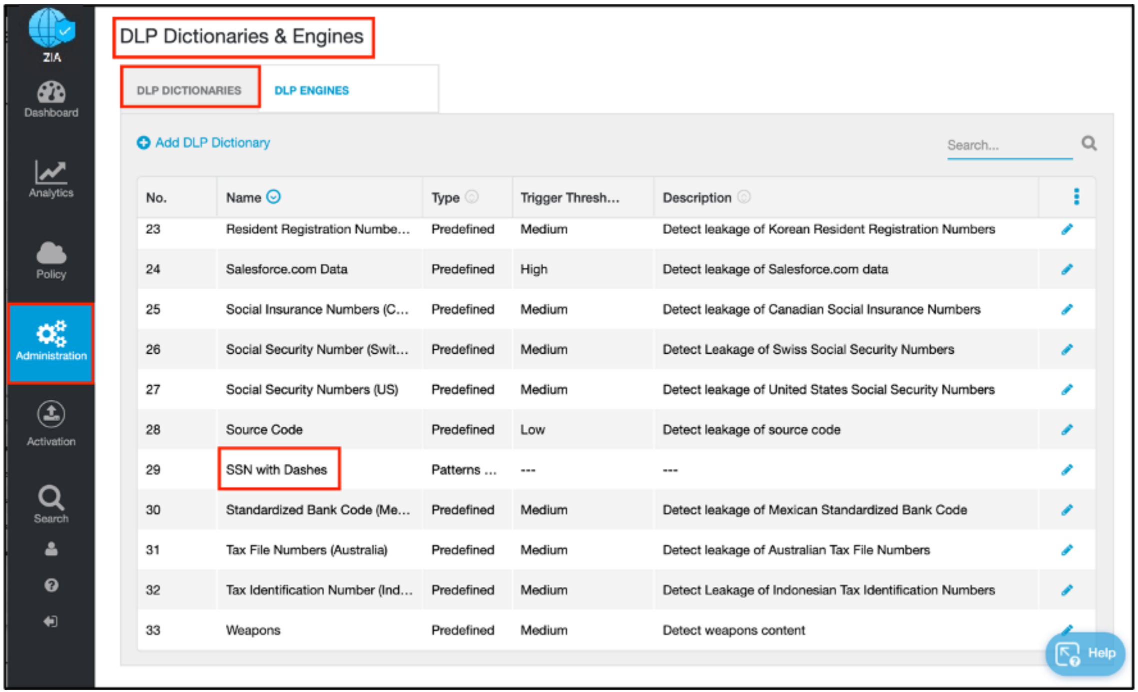
The procedures for creating a DLP policy are straightforward. Create a custom dictionary (or use the available dictionaries) to identify the data the scan captures.

Next, create an engine that is the logical template for adding expressions and additional data. This is where you would specify Social Security numbers and any other criteria for the policy. The engine provides the means to precisely add or remove data to match the violation and eliminate false positives.

Then create a SaaS security DLP policy that allows you to specify the detail about where and when action is taken, and whom to inform about violations. Finally, apply the DLP policy to the Salesforce tenant. Verify the DLP dictionary as next steps.

In the ZIA Admin Portal:

1. Go to **Administration** > **DLP Dictionaries & Engines** > **DLP Dictionaries**.
2. Identify and select the dictionary to use (in this case **SSN with Dashes**).



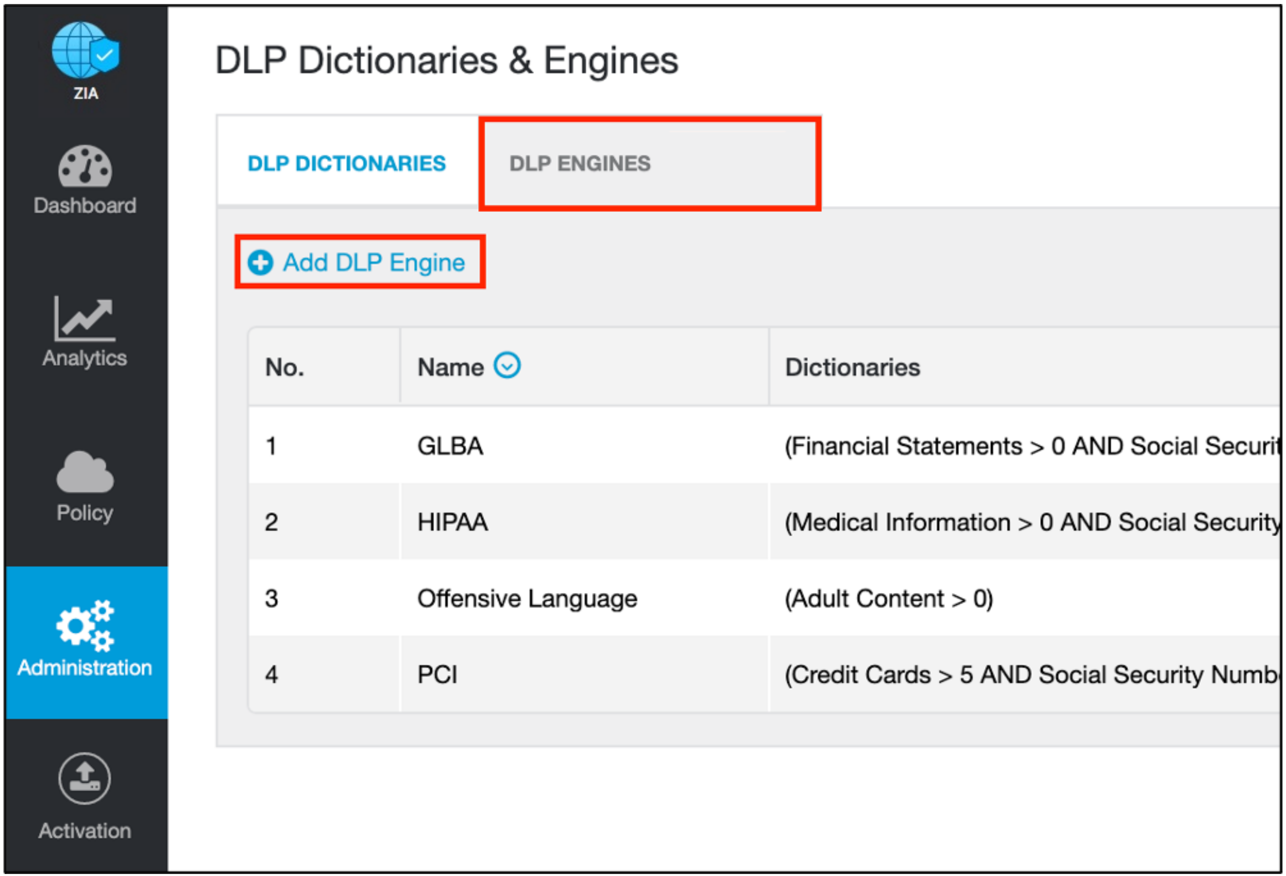
No.	Name	Type	Trigger Thresh...	Description
23	Resident Registration Numbe...	Predefined	Medium	Detect leakage of Korean Resident Registration Numbers
24	Salesforce.com Data	Predefined	High	Detect leakage of Salesforce.com data
25	Social Insurance Numbers (C...	Predefined	Medium	Detect leakage of Canadian Social Insurance Numbers
26	Social Security Number (Swit...	Predefined	Medium	Detect Leakage of Swiss Social Security Numbers
27	Social Security Numbers (US)	Predefined	Medium	Detect leakage of United States Social Security Numbers
28	Source Code	Predefined	Low	Detect leakage of source code
29	SSN with Dashes	Patterns ...	---	---
30	Standardized Bank Code (Me...	Predefined	Medium	Detect leakage of Mexican Standardized Bank Code
31	Tax File Numbers (Australia)	Predefined	Medium	Detect leakage of Australian Tax File Numbers
32	Tax Identification Number (Ind...	Predefined	Medium	Detect Leakage of Indonesian Tax Identification Numbers
33	Weapons	Predefined	Medium	Detect weapons content

Figure 46. Creating a DLP dictionary

Creating a DLP Engine

To create the DLP engine:

1. Select the **DLP Engines** tab.
2. Click **Add DLP Engine**.

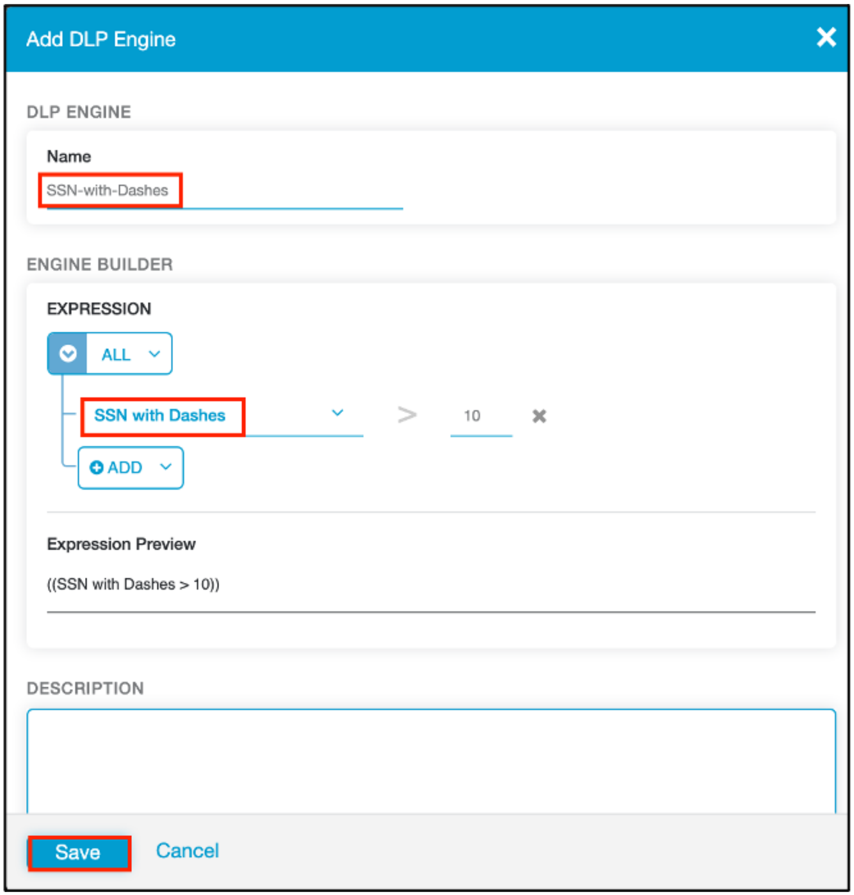


DLP Dictionaries & Engines

No.	Name	Dictionaries
1	GLBA	(Financial Statements > 0 AND Social Securit
2	HIPAA	(Medical Information > 0 AND Social Security
3	Offensive Language	(Adult Content > 0)
4	PCI	(Credit Cards > 5 AND Social Security Numb

Figure 47. Creating a DLP engine

3. Enter a **Name** for the DLP Engine.
4. Select the first dictionary in the **Engine Builder** under **Expression**.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. Select **ADD** to add the next dictionary and repeat the process, if needed.
7. Click **Save**.
8. Activate the configuration.



Name: SSN-with-Dashes

SSN with Dashes > 10

Expression Preview

((SSN with Dashes > 10))

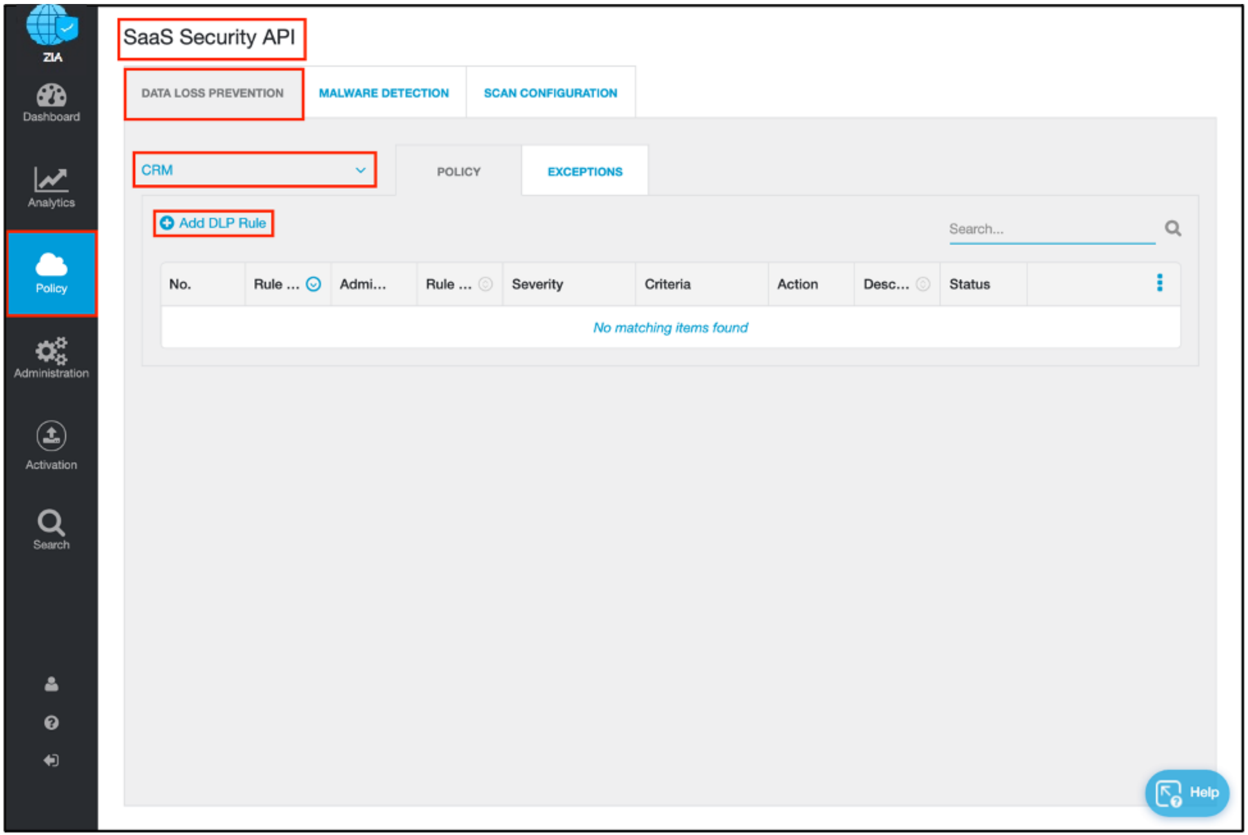
Figure 48. The DLP engine wizard

This policy triggers on the eleventh Social Security number. Again, this is a demonstration and the criteria is too general to be a production DLP rule.

Configuring a SaaS DLP Policy

To launch the DLP Rule wizard:

1. Go to **Policy** > **SaaS Security API** > **Data Loss Prevention**.
2. Select **CRM**.
3. Click **Add DLP Rule**.



No.	Rule ...	Admi...	Rule ...	Severity	Criteria	Action	Desc...	Status
				No matching items found				

Figure 49. The SaaS DLP Policy Configuration wizard

SaaS DLP Policy Details

The SaaS DLP policy is like all Zscaler polices in that you specify the detail on whom and what this policy applies to. You specify the rule order if you have multiple DLP policies that are processed in an ascending manner. The first rule that matches is the applied rule.

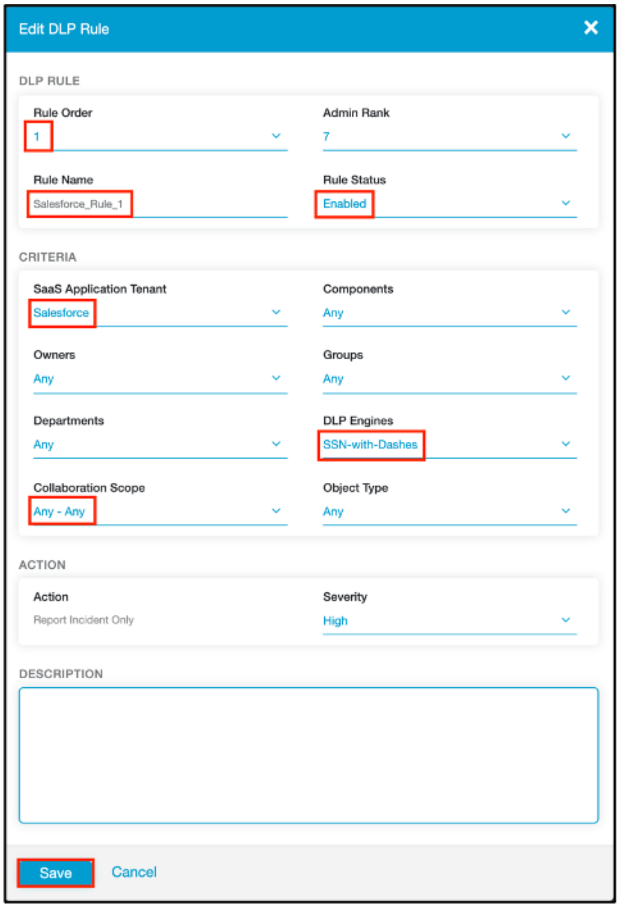
The rule specifies the DLP engine defined; any particular file owners, groups, or departments; and the file types to inspect. The **Collaboration Scope** and the **Action** are unique to SaaS DLP policies and are explained for clarification. For this policy example, select **Any-Any**, and an **Action** of **Report Incident Only**.

- **Collaboration Scope**: The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select **Any-Any** to apply the rule to files with all collaboration levels, or select any number of the following collaboration scopes and specify the permissions for each scope:
  - **External Collaborators**: Files that are shared with specific collaborators outside of your organization.
  - **External Link**: Files with shareable links that allow anyone outside your organization to find the files and have access.
  - **Internal Collaborators**: Files that are shared with specific collaborators or are discoverable within your organization.
  - **Internal Link**: Files with shareable links that allow anyone within your organization to find the files and have access.
  - **Private**: Files that are only accessible to the owner.
- **The Action**: The rule takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For Salesforce, the action is Report Incident Only. This means that any violations are reported in the Zscaler SaaS Analytics and alerts are sent to auditors if defined.
  - **Report Incident Only**: The rule reports the incident only and makes no changes to the file's collaboration scope.

Configure SaaS DLP Policy Details

To finish the DLP policy:

1. Specify the **Rule Order** for processing (the first rule matched is executed).
2. Enter a **Rule Name**.
3. Select **Enabled** for the **Rule Status**.
4. Select **Salesforce** from the **Saas Application Tenant** drop-down menu.
5. Select the DLP engine created in [Creating a DLP Engine](#).
6. Select **Any-Any** from the **Collaboration Scope** drop-down menu.
7. Select **High** as the **Severity** to allow for identification for searches and tracking.
8. Click **Save a**nd activate your configuration.



Edit DLP Rule

DLP RULE

Rule Order: 1
Admin Rank: 7
Rule Name: Salesforce_Rule_1
Rule Status: Enabled

CRITERIA

SaaS Application Tenant: Salesforce
Components: Any
Owners: Any
Groups: Any
Departments: Any
DLP Engines: SSN-with-Dashes
Collaboration Scope: Any - Any
Object Type: Any

ACTION

Action: Report Incident Only
Severity: High

DESCRIPTION

Figure 50. The SaaS DLP Policy Configuration wizard

Configure a SaaS Malware Policy

To launch the DLP Rule wizard.

1. Go to **Policy** > **SaaS Security API** > **Malware Detection**.
2. Select **CRM**.
3. Click **Add Malware Detection Rule**.

   The SaaS malware detection policy is an all-encompassing policy and all files in the tenant are scanned unless removed from the scope. You can remove files by specifying exemptions on the **Exceptions** tab under **Malware Detection**.

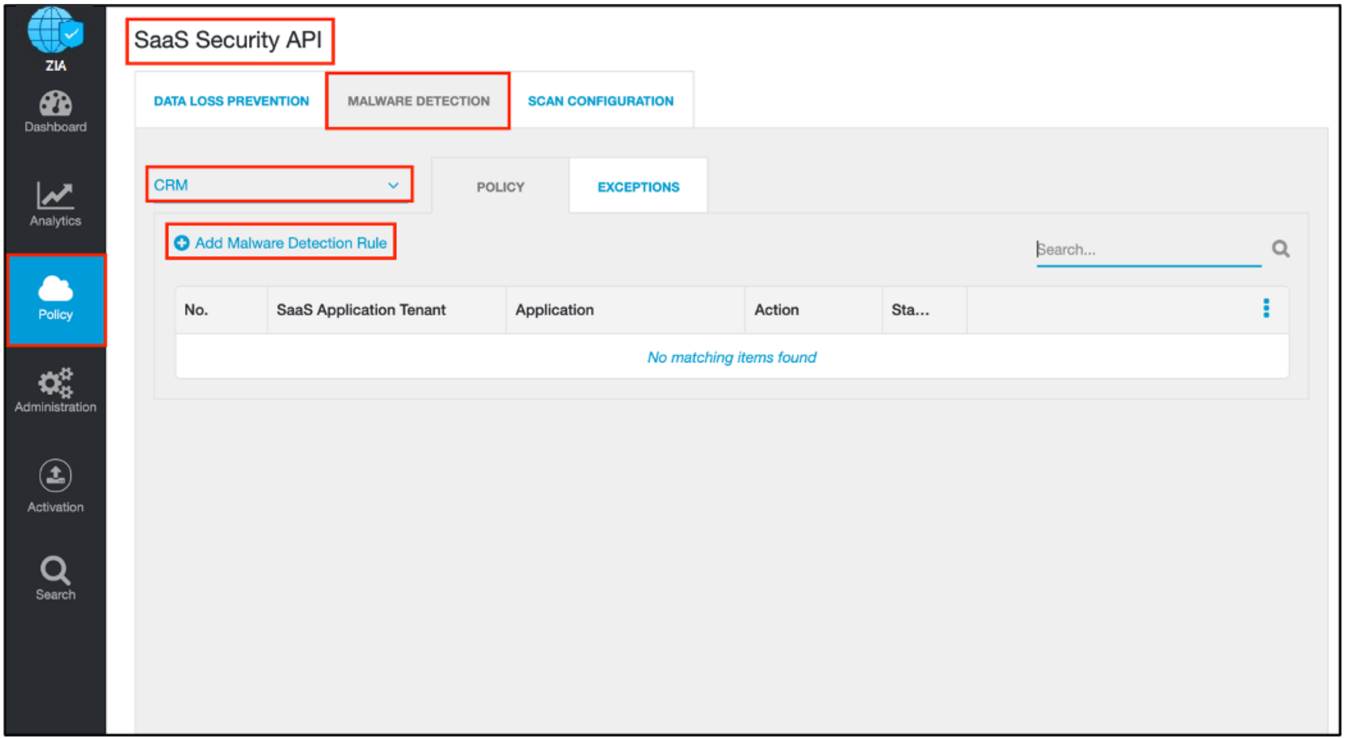
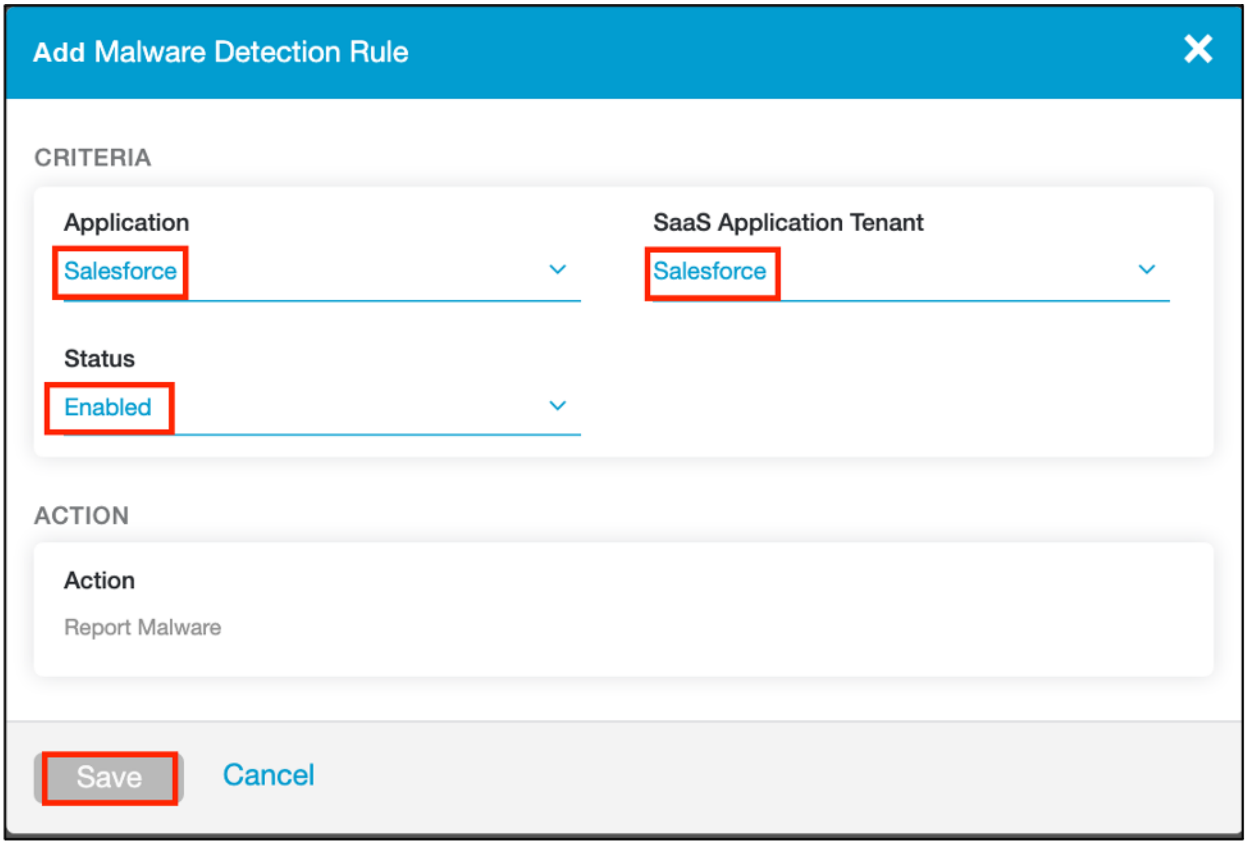


Figure 51. The Malware Policy Configuration wizard

4. Under **Criteria**, select **Salesforce** from the **Application** drop-down menu.
5. Select **Salesforce** from the **SaaS Application Tenant** drop-down menu to apply the policy.
6. Select **Enabled** for **Status**. The **Action** for Salesforce is limited to Report Malware only.
7. Click **Save**.


Add Malware Detection Rule

CRITERIA

Application: Salesforce

SaaS Application Tenant: Salesforce

Status: Enabled

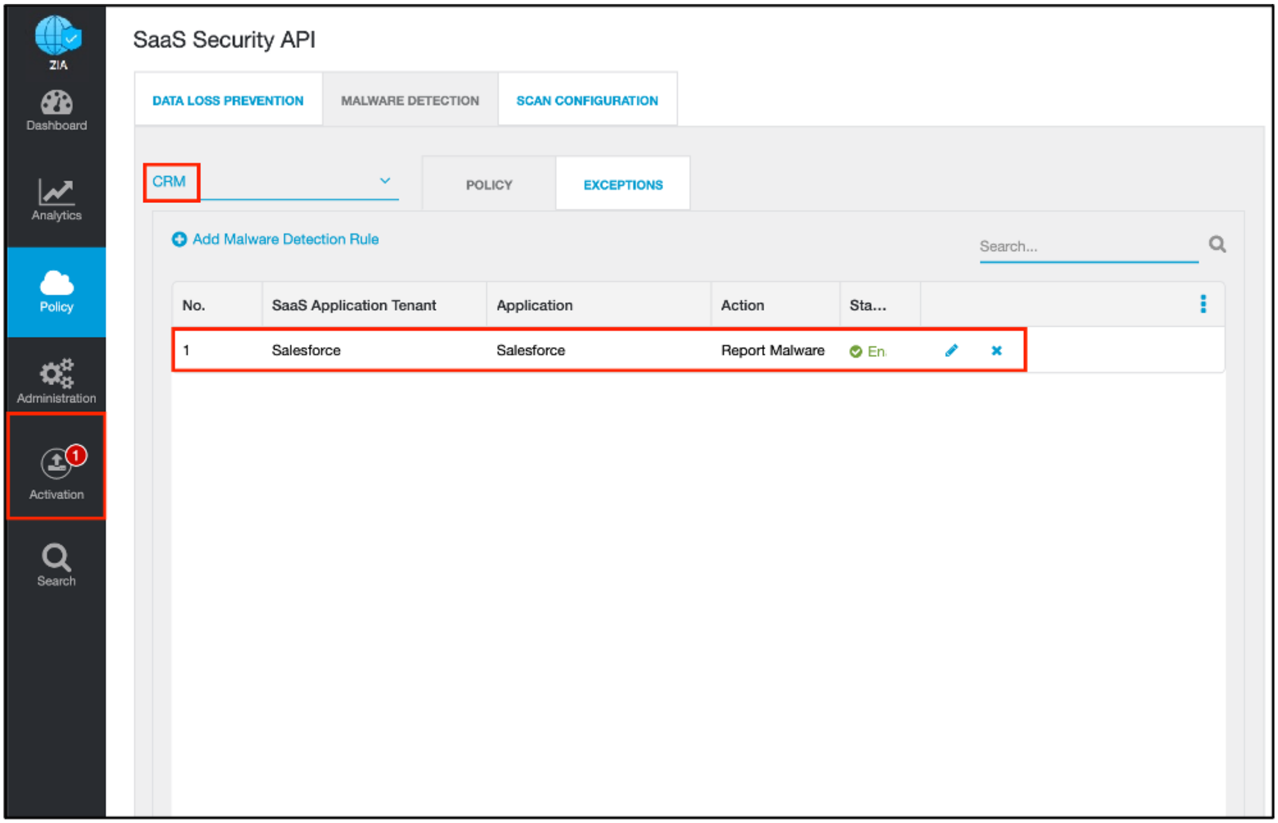
ACTION

Action: Report Malware

Figure 52. The Malware Policy Configuration wizard

SaaS Malware Policy

The completed SaaS security malware policy for the Salesforce SaaS tenant. Click **Activation** to activate your configuration.



No.	SaaS Application Tenant	Application	Action	Sta...
1	Salesforce	Salesforce	Report Malware	En.

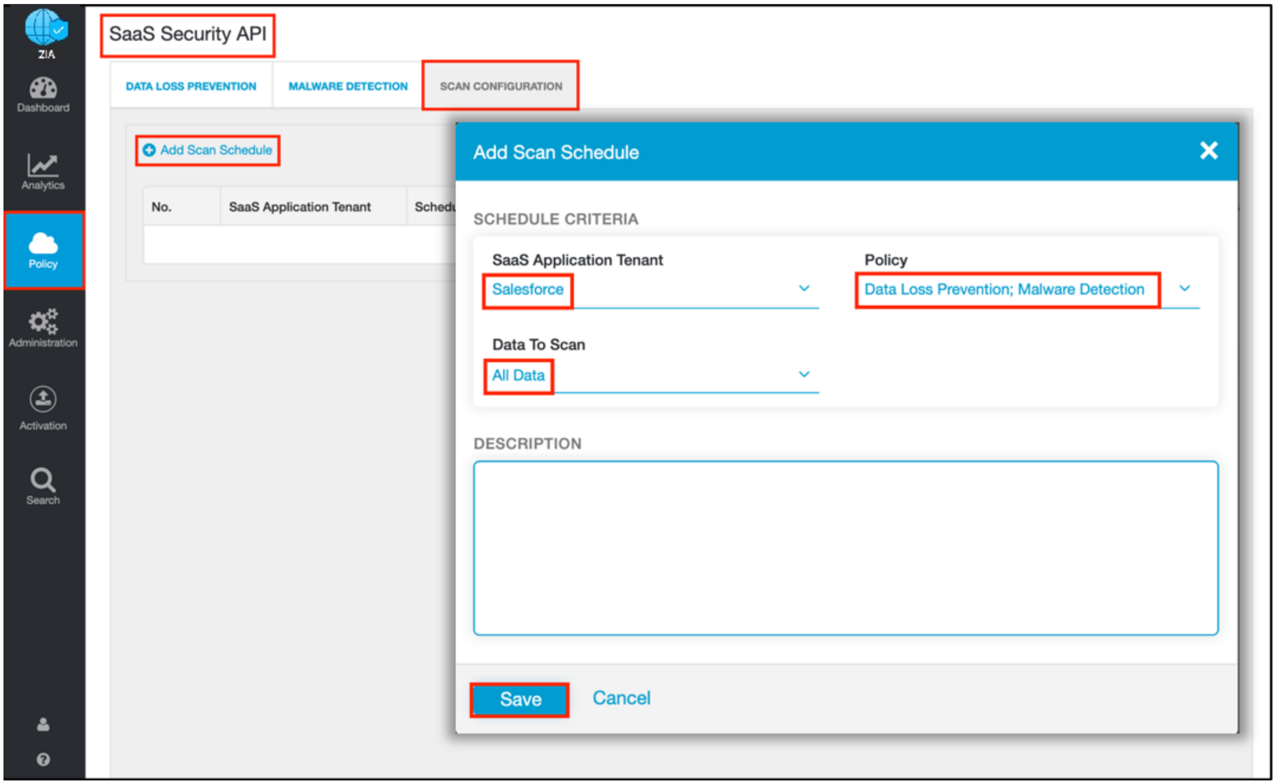
Figure 53. The completed Malware Policy Configuration wizard

Configuring the Scan Schedule

The final configuration step is to create a scan configuration. Specify the tenant the scan configuration applies to, any policies that are to be included in the scan, and what data to scan relative to a date. The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. In this example, select **All Data**. However, if this is a POV or a trial, the only option available is **New Data Only**.

To add a scan schedule:

1. Go to **Policy** > **SaaS Security API** > **Scan Configuration** > **Add Scan Schedule**.
2. Select **Salesforce** for the **SaaS Application Tenant**.
3. Select the malware policy created in prior steps as the data loss **Policy**.
4. Select **All Data** (or **New Data Only** if this is a POV) for **Data to Scan**.
5. Click **Save**.



SaaS Application Tenant: Salesforce

Policy: Data Loss Prevention; Malware Detection

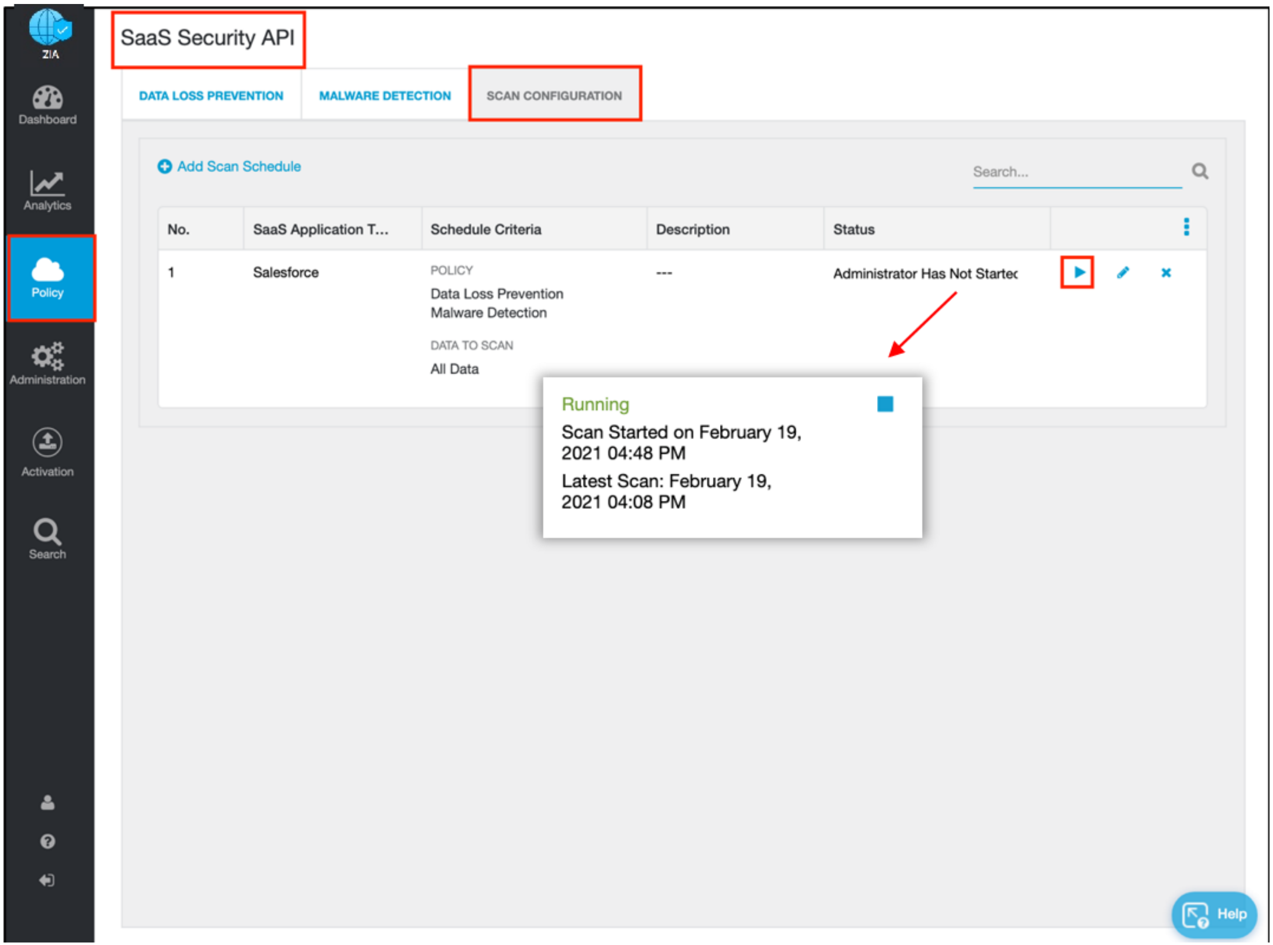
Data To Scan: All Data

Figure 54. Create and enable a scan for the SaaS tenant

Start the Scan Schedule

After the schedule has been configured and saved, start the scan for the DLP and malware policies to be applied:

1. Click **Activation** to activate the configuration changes.
2. Click the **Run** icon on the **Scan Configuration** tab to start SaaS API security on the Salesforce tenant. When finished running, the **Status** displays **Active** with a **Start Date** and a **Latest Scan Date**.



No.	SaaS Application T...	Schedule Criteria	Description	Status
1	Salesforce	POLICY Data Loss Prevention Malware Detection DATA TO SCAN All Data	---	Administrator Has Not Startec

Running

Scan Started on February 19, 2021 04:48 PM

Latest Scan: February 19, 2021 04:08 PM

Figure 55. Starting the scan

Reporting and Visibility

Zscaler Analytics provide detailed reporting of all user activity down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at rest associated with the user. For SaaS partners, Zscaler provides reports and SaaS security insights. These provide visibility from a high-level overview to management of the individual logs and violations.

Take a brief look at the tools, but for detailed information of the SaaS Security Analytics tools, see the SaaS Security Activities Report.

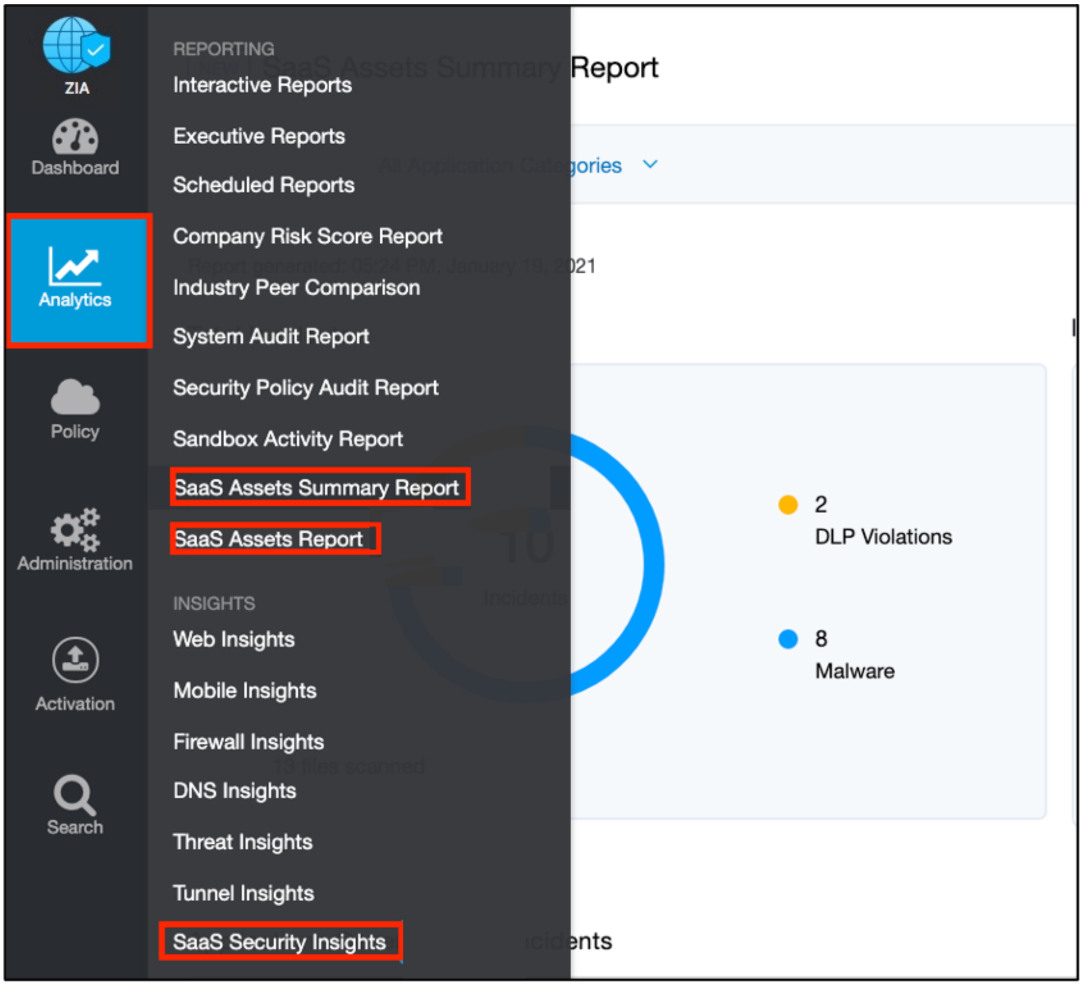


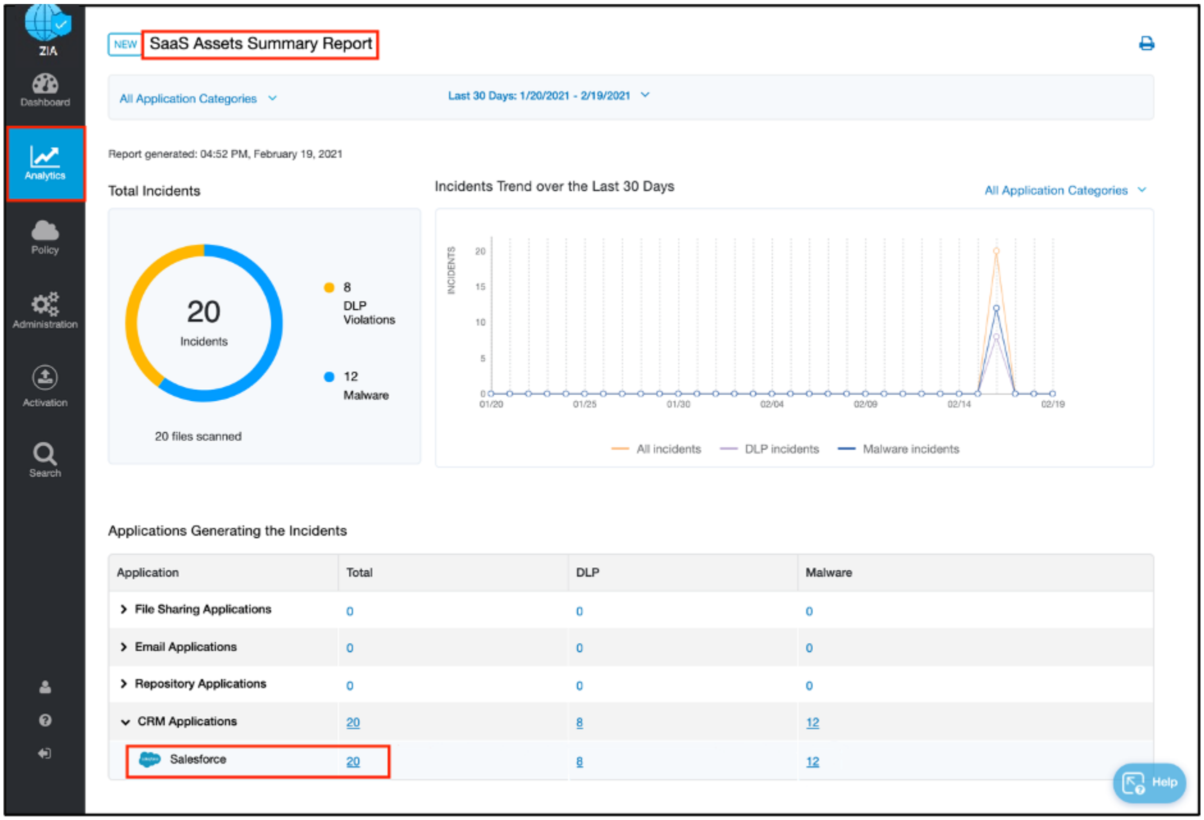
Figure 56. SaaS security visibility

SaaS Assets and SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reports with a quick view of your files and emails. The following is the SaaS Assets Summary Report, which provides all activity and violations at a quick glance. The report identifies all SaaS tenant information from a single screen. The Salesforce activity over the creation of this deployment guide is shown earlier, but any configured tenant is also displayed on this summary screen. The data is hyperlinked, and you can pivot from a summary to individual logs and activities provided by SaaS security insights.

Select the **Total** number of incidents next to the Salesforce application to pivot to **SaaS Security Insights**.

This opens **SaaS Security Insights** and the log data for each violation containing over 30 metadata points of information.



SaaS Assets Summary Report

Report generated: 04:52 PM, February 19, 2021

Total Incidents

20 files scanned

Incidents Trend over the Last 30 Days

Applications Generating the Incidents

Application	Total	DLP	Malware
› File Sharing Applications	0	0	0
› Email Applications	0	0	0
› Repository Applications	0	0	0
⌄ CRM Applications	20	8	12
Salesforce	20	8	12

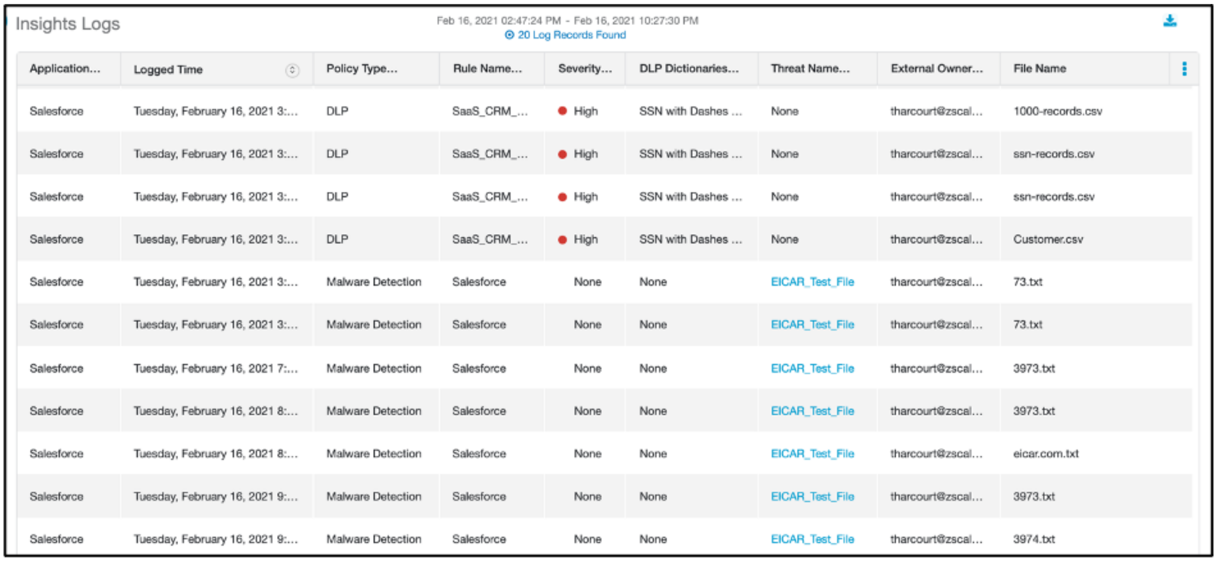
Figure 57. Summary reports

SaaS Security Insights

The SaaS Security Insights page is where you can view and select information fields that you want to see when analyzing files scanned through charts. These logs provide the detail of the policy that found the violation, the threat name, the owner, and over 30 metadata points for identification and threat hunting.

The following are the SaaS Security data types and their associated filters:

- Application
- Application Category
- Department
- DLP Dictionary
- DLP Engine
- Incident Type
- Owner Name
- Severity
- Tenant
- Threat Category
- Threat Super Category
- User



Insights Logs

Feb 16, 2021 02:47:24 PM - Feb 16, 2021 10:27:30 PM
20 Log Records Found

Application...	Logged Time	Policy Type...	Rule Name...	Severity...	DLP Dictionaries...	Threat Name...	External Owner...	File Name
Salesforce	Tuesday, February 16, 2021 3:...	DLP	SaaS_CRM_...	● High	SSN with Dashes ...	None	tharcourt@zscal...	1000-records.csv
Salesforce	Tuesday, February 16, 2021 3:...	DLP	SaaS_CRM_...	● High	SSN with Dashes ...	None	tharcourt@zscal...	ssn-records.csv
Salesforce	Tuesday, February 16, 2021 3:...	DLP	SaaS_CRM_...	● High	SSN with Dashes ...	None	tharcourt@zscal...	ssn-records.csv
Salesforce	Tuesday, February 16, 2021 3:...	DLP	SaaS_CRM_...	● High	SSN with Dashes ...	None	tharcourt@zscal...	Customer.csv
Salesforce	Tuesday, February 16, 2021 3:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	73.txt
Salesforce	Tuesday, February 16, 2021 3:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	73.txt
Salesforce	Tuesday, February 16, 2021 7:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	3973.txt
Salesforce	Tuesday, February 16, 2021 8:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	3973.txt
Salesforce	Tuesday, February 16, 2021 8:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	eicar.com.txt
Salesforce	Tuesday, February 16, 2021 9:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	3973.txt
Salesforce	Tuesday, February 16, 2021 9:...	Malware Detection	Salesforce	None	None	EICAR_Test_File	tharcourt@zscal...	3974.txt

Figure 58. SaaS security insight

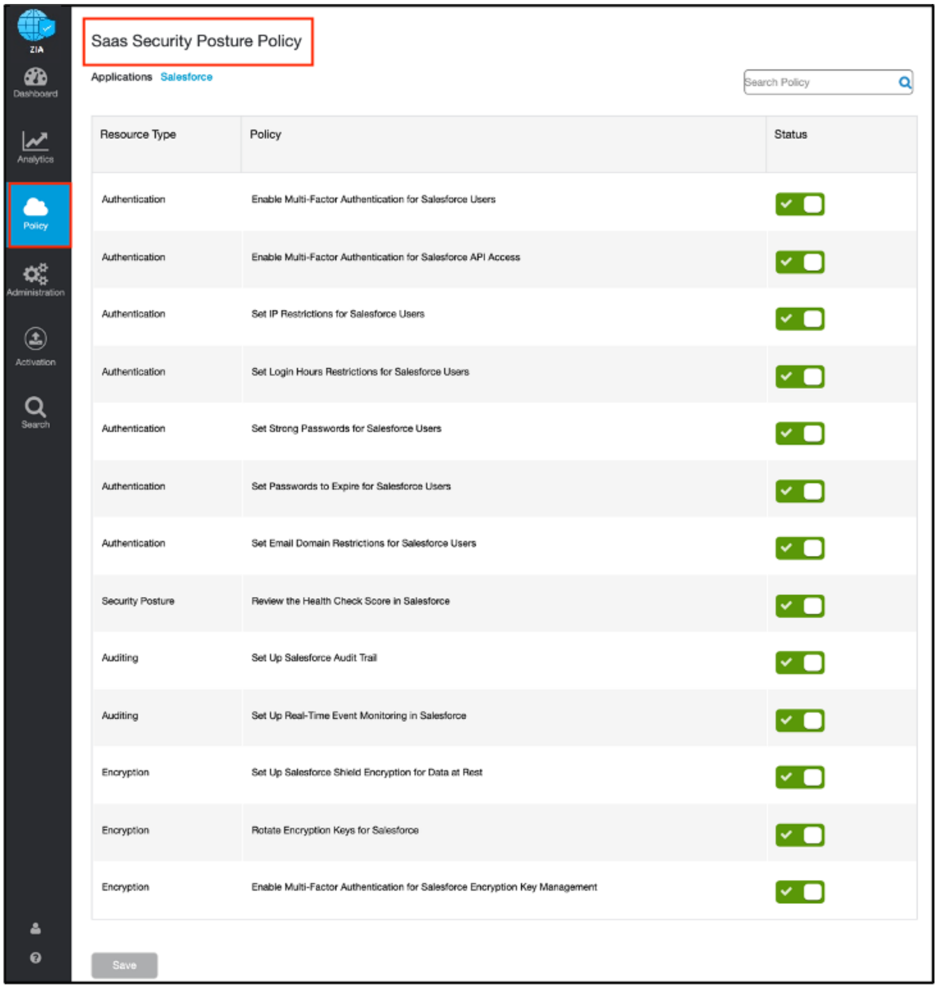
SaaS Security Posture

The following sections describe how to configure SaaS security posture.

SaaS Security Posture Policies

The following are the default SaaS posture policies. You can check what policies are enabled, or disable a policy in the ZIA Admin Portal.

1. Log in to your organization's ZIA Admin Portal with admin credentials.
2. Go to **Policy** > **SaaS Security Posture Policy**.
3. Enable or disable individual policies.
4. Click **Save** and click **Activation** to activate the policy changes.



Saas Security Posture Policy

Applications Salesforce

Search Policy

Resource Type	Policy	Status
Authentication	Enable Multi-Factor Authentication for Salesforce Users	✓
Authentication	Enable Multi-Factor Authentication for Salesforce API Access	✓
Authentication	Set IP Restrictions for Salesforce Users	✓
Authentication	Set Login Hours Restrictions for Salesforce Users	✓
Authentication	Set Strong Passwords for Salesforce Users	✓
Authentication	Set Passwords to Expire for Salesforce Users	✓
Authentication	Set Email Domain Restrictions for Salesforce Users	✓
Security Posture	Review the Health Check Score in Salesforce	✓
Auditing	Set Up Salesforce Audit Trail	✓
Auditing	Set Up Real-Time Event Monitoring in Salesforce	✓
Encryption	Set Up Salesforce Shield Encryption for Data at Rest	✓
Encryption	Rotate Encryption Keys for Salesforce	✓
Encryption	Enable Multi-Factor Authentication for Salesforce Encryption Key Management	✓

Save

Figure 59. SaaS security posture policies

SaaS Security Posture Report

To check the result of the configured SaaS posture policies against the Salesforce tenant, check the SaaS Posture Report in Analytics.

1. Log in to your organization's ZIA Admin Portal with admin credentials.
2. Select **Analytics**.
3. Select **SaaS Security Report**.
4. Select **Security Configuration**.
5. For **Tenant**, select **Salesforce**.
6. For **Compliance Check**, select **Best Practices**, **PCI**, or **FFIEC**.

The results for each check display a pass or fail for the policy check. If you click the name of the policy, a window displays that describes the feature and how to remediate the failure.

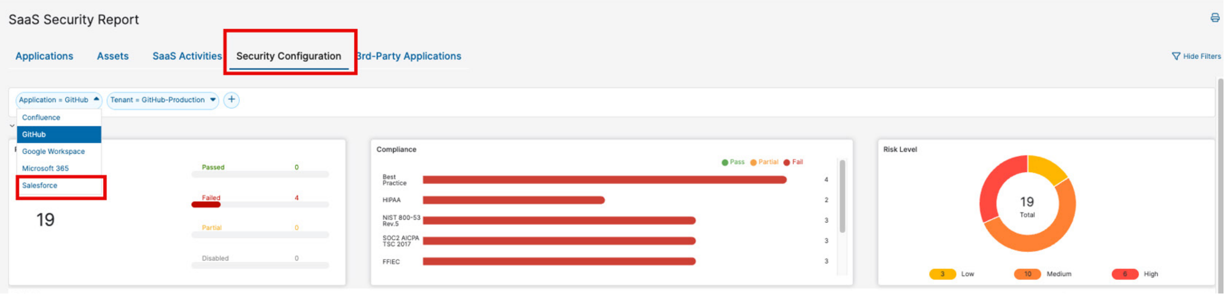
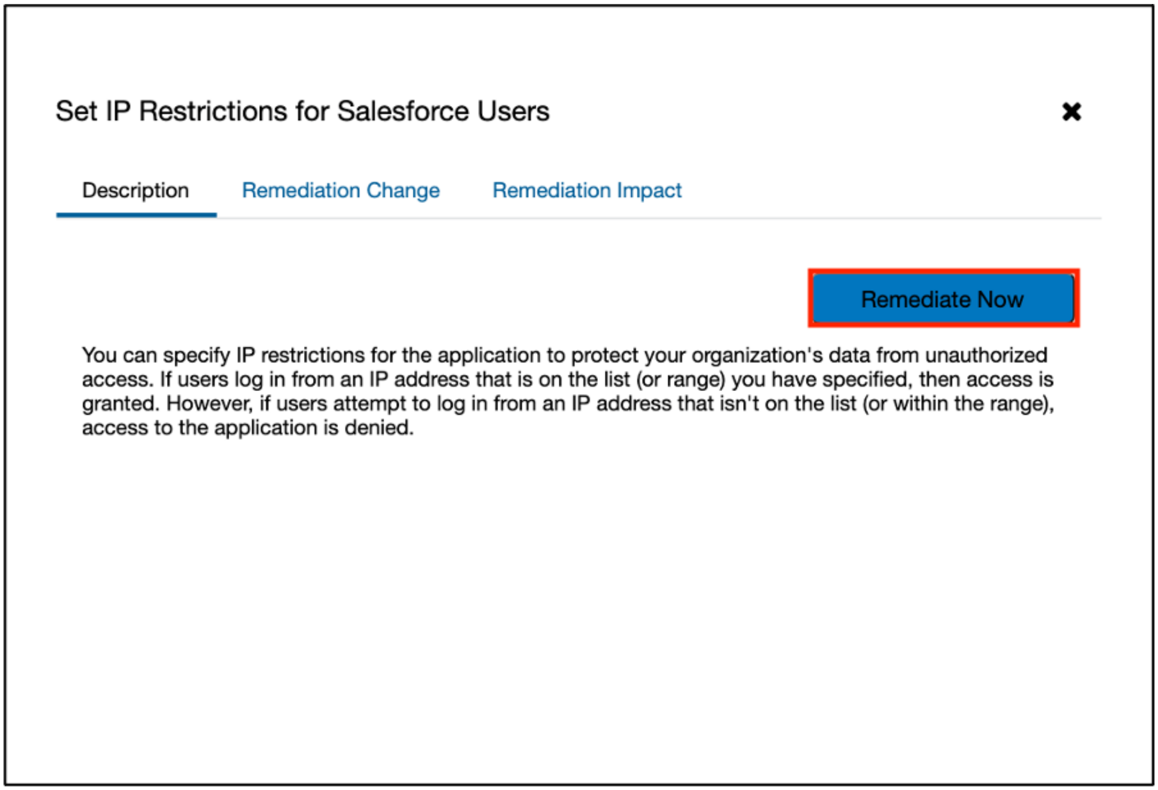


Figure 60. SaaS security posture report

SaaS Security Posture Policies Remediation

The **Set IP Restrictions for Salesforce Users** window provides a description of the failure and the impact of making the recommended changes. Click **Remediate Now** to open the Salesforce documentation that provides the steps to make the change.



You can specify IP restrictions for the application to protect your organization's data from unauthorized access. If users log in from an IP address that is on the list (or range) you have specified, then access is granted. However, if users attempt to log in from an IP address that isn't on the list (or within the range), access to the application is denied.

Figure 61. SaaS security posture remediation steps

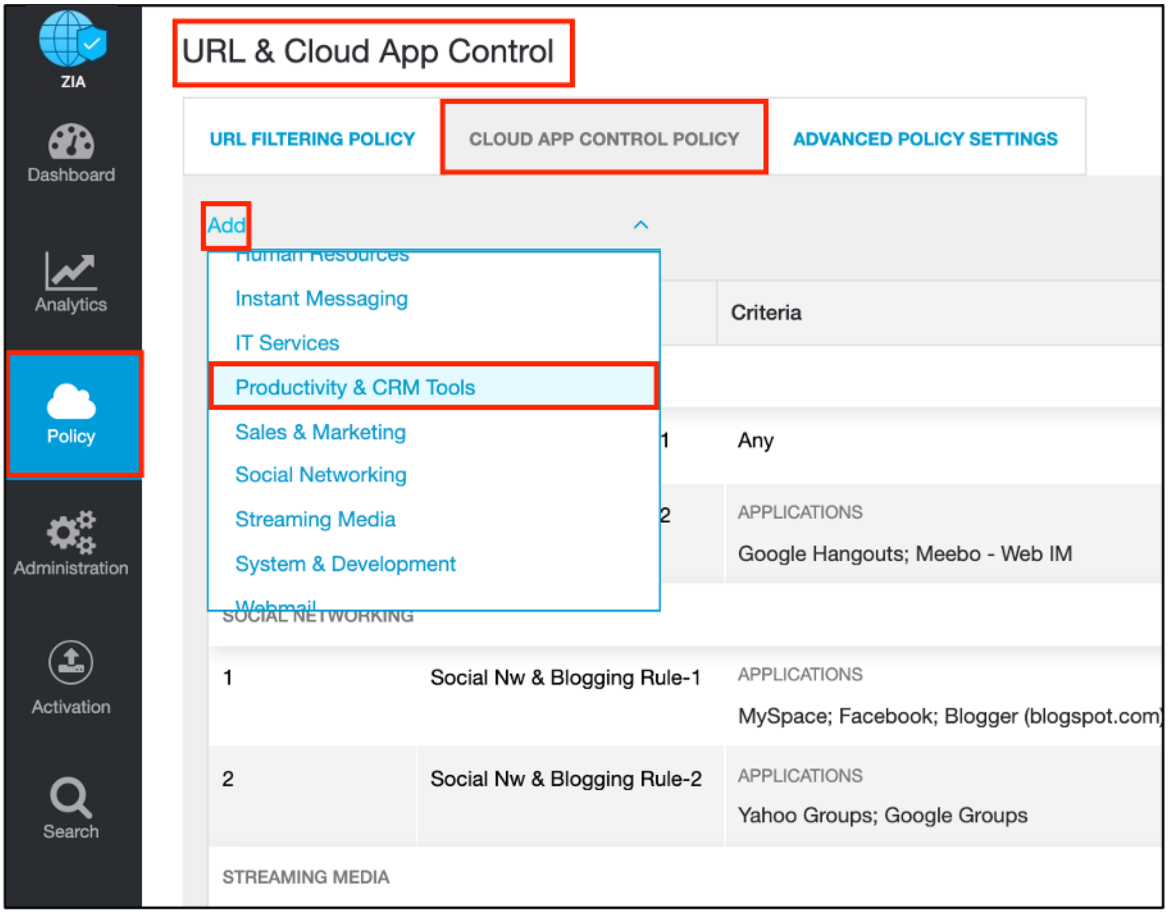
Cloud App Control

The following sections describe how to configure Cloud App Control.

Cloud Application Access Control Policy

To create the policy to allow specific users:

1. Log in to your organization’s ZIA Admin Portal with admin credentials.
2. Go to **Policy** > **URL & Cloud App Control**.
3. Select the **Cloud App Control Policy** tab.
4. From the **Add** drop-down menu, select **Productivity & CRM Tools**.



		Criteria
1		Any
2		APPLICATIONS Google Hangouts; Meebo - Web IM
1	Social Nw & Blogging Rule-1	APPLICATIONS MySpace; Facebook; Blogger (blogspot.com)
2	Social Nw & Blogging Rule-2	APPLICATIONS Yahoo Groups; Google Groups

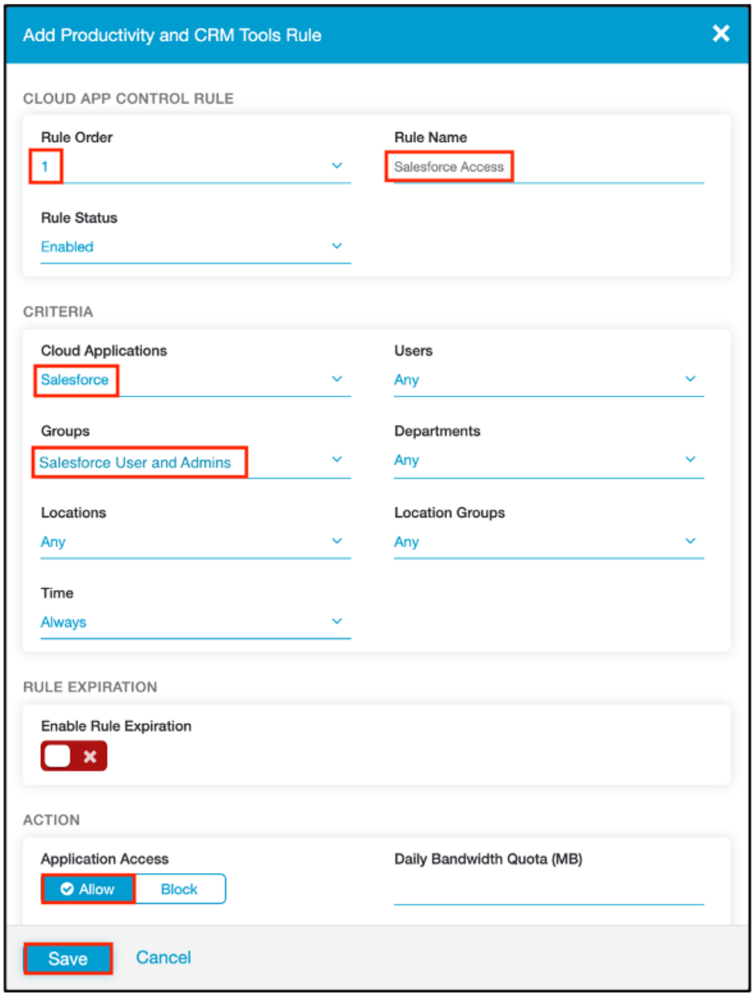
Figure 62. Cloud App Control

This launches the **Policy** wizard.

Cloud Application Access Control Policy Window

To create the policy to allow specific users:

1. Set the **Rule Order** to **1**.
2. Enter an intuitive name for **Rule Name**.
3. Select **Salesforce** from the **Cloud Applications** drop-down menu.
4. Select the group that contains Salesforce users and admins from the **Groups** drop-down menu.
5. Select **Allow** for **Application Access**.
6. Click **Save**.



Rule Order: 1

Rule Name: Salesforce Access

Rule Status: Enabled

Cloud Applications: Salesforce

Users: Any

Groups: Salesforce User and Admins

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Enable Rule Expiration: ☒

Application Access: Allow

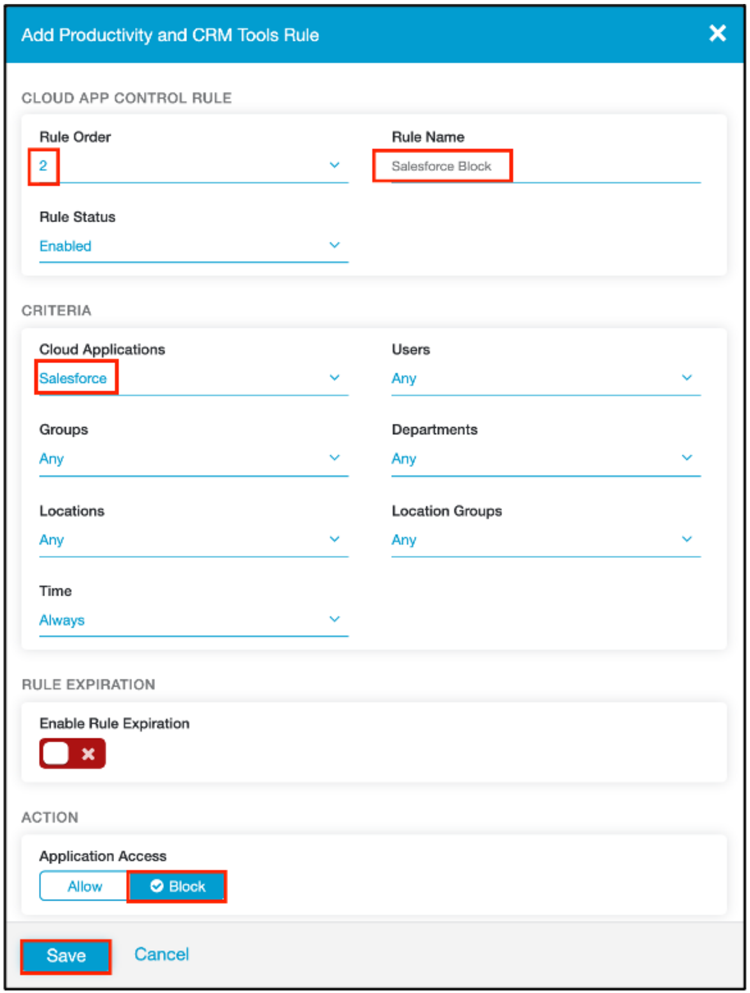
Daily Bandwidth Quota (MB):

Figure 63. Create a Cloud App Control allow policy

Cloud Application Access Control: Deny Policy

To create the policy to deny all other users:

1. Set the **Rule Order** to **2** (must be after the Allow policy).
2. Enter an intuitive name for **Rule Name**.
3. Select **Salesforce** from the **Cloud Applications** drop-down menu.
4. Leave all other settings as **Any**.
5. Select **Block** for **Application Access**.
6. Click **Save**.



Add Productivity and CRM Tools Rule

CLOUD APP CONTROL RULE

Rule Order: 2

Rule Name: Salesforce Block

Rule Status: Enabled

CRITERIA

Cloud Applications: Salesforce

Users: Any

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

RULE EXPIRATION

Enable Rule Expiration: ☒

ACTION

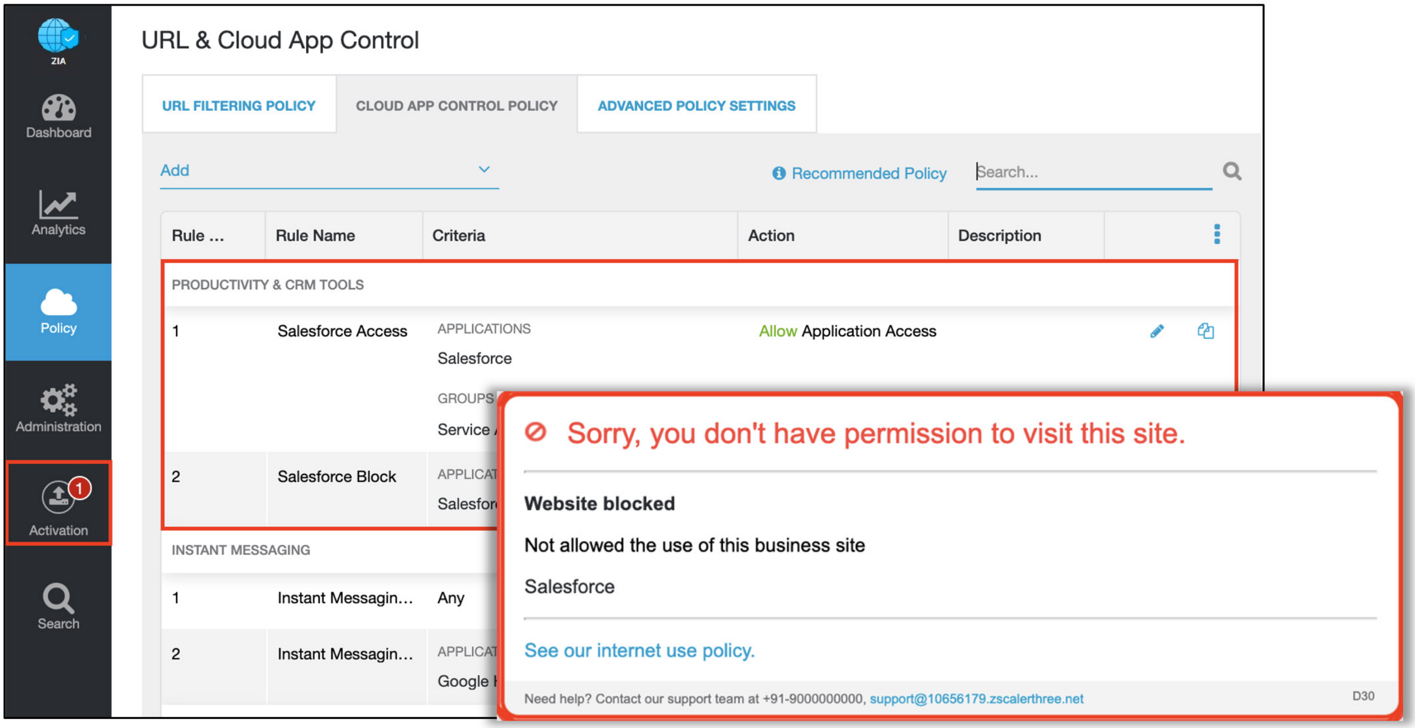
Application Access: Allow [✓ Block]

Figure 64. Create a Cloud App Control deny policy

Cloud Application Access Control

To finish the completed access policies, click **Activation** to activate the policy additions.

Users who try to access the Salesforce application through Zscaler and do not have permission see the **Website blocked** message. Zscaler administrators will receive alerts and logs to the event.



Rule ...	Rule Name	Criteria	Action	Description
PRODUCTIVITY & CRM TOOLS				
1	Salesforce Access	APPLICATIONS Salesforce GROUPS Service /	Allow Application Access	
2	Salesforce Block	APPLICAT Salesfor		
INSTANT MESSAGING				
1	Instant Messagin...	Any		
2	Instant Messagin...	APPLICAT Google I		

⊘ Sorry, you don't have permission to visit this site.

Website blocked

Not allowed the use of this business site

Salesforce

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@10656179.zscalerthree.net D30

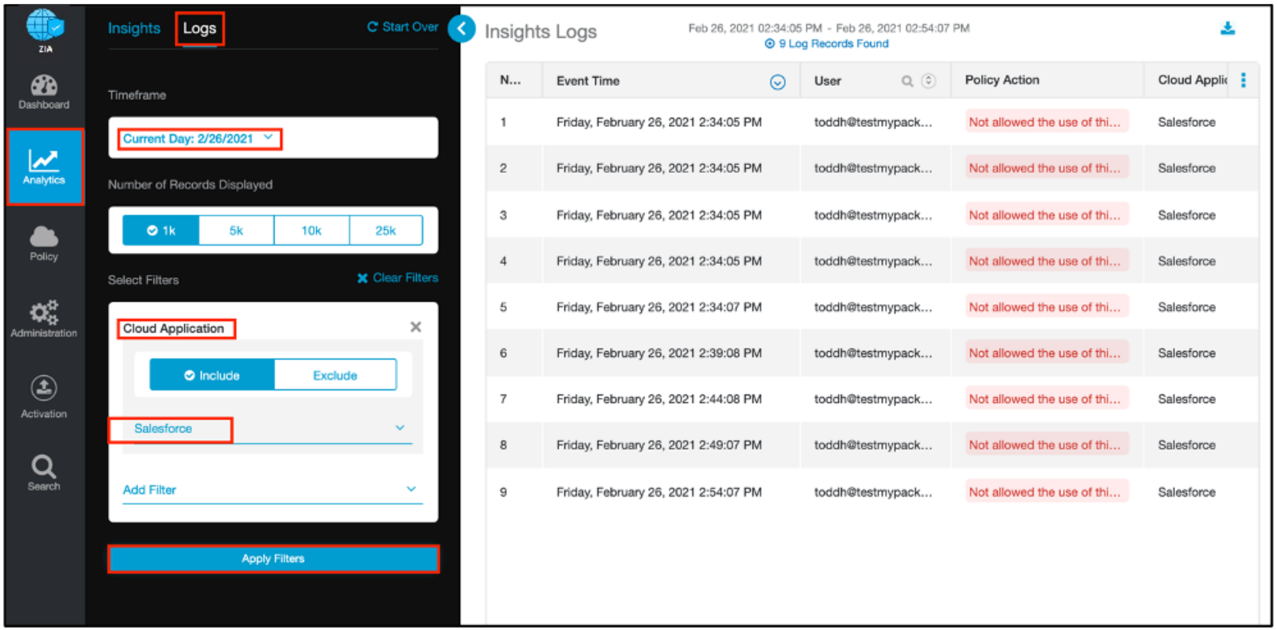
Figure 65. Create a Cloud App Control deny policy

Cloud Application Access Control Logs

Zscaler Analytics provide visibility to see any activity for Salesforce access, or to get usage reports.

To view the Salesforce logs for a certain time frame:

1. Log in to your organization's ZIA Admin Portal with admin credentials.
2. Go to **Analytics** > **Web Insights**.
3. Select the **Logs** tab.
4. Select the desired time frame, or a custom time frame.
5. Select **Include** under **Cloud Application**.
6. Select **Salesforce** from the drop-down menu.
7. Click **Apply Filters**.



Timeframe: Current Day: 2/26/2021

Number of Records Displayed: 1k

Select Filters

Cloud Application: Include

Salesforce

Insights Logs

Feb 26, 2021 02:34:05 PM - Feb 26, 2021 02:54:07 PM

9 Log Records Found

N...	Event Time	User	Policy Action	Cloud Applic
1	Friday, February 26, 2021 2:34:05 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
2	Friday, February 26, 2021 2:34:05 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
3	Friday, February 26, 2021 2:34:05 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
4	Friday, February 26, 2021 2:34:05 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
5	Friday, February 26, 2021 2:34:07 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
6	Friday, February 26, 2021 2:39:08 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
7	Friday, February 26, 2021 2:44:08 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
8	Friday, February 26, 2021 2:49:07 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce
9	Friday, February 26, 2021 2:54:07 PM	toddh@testmypack...	Not allowed the use of thi...	Salesforce

Figure 66. Create a Cloud App Control logs

ZDX for Salesforce

ZDX is the missing link needed for customers and their SaaS applications. As applications move to the cloud, the internet becomes your new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. Salesforce is no exception to this and Zscaler ZDX provides visibility into the client's experience using Salesforce. ZDX uses Zscaler Client Connector to generate application and network probes and gather device health. ZDX is a separate service from ZIA SaaS Security and can run with or without SaaS Security.

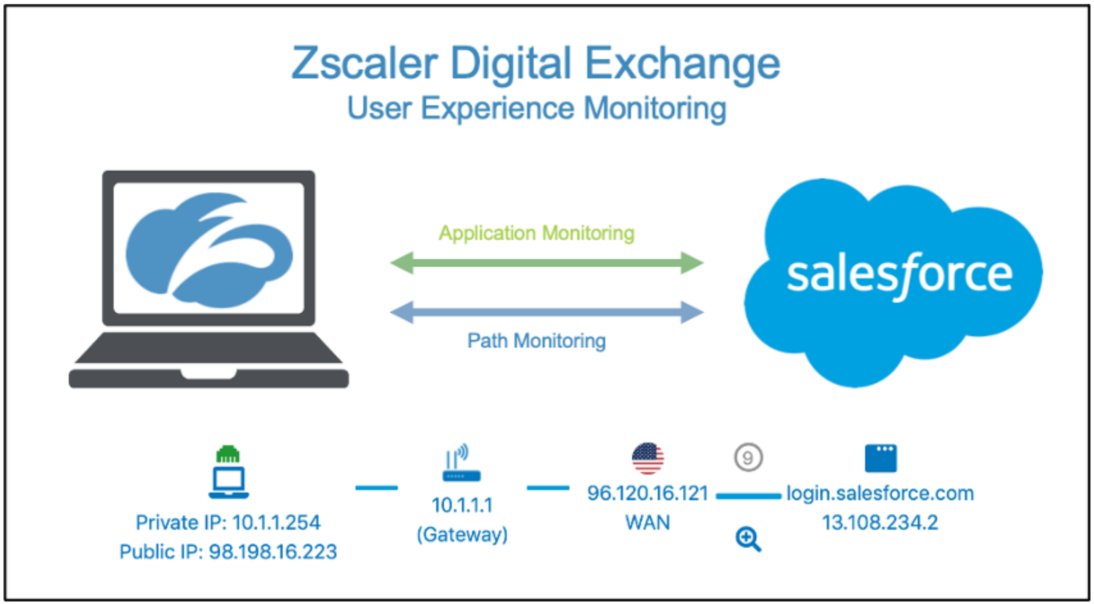


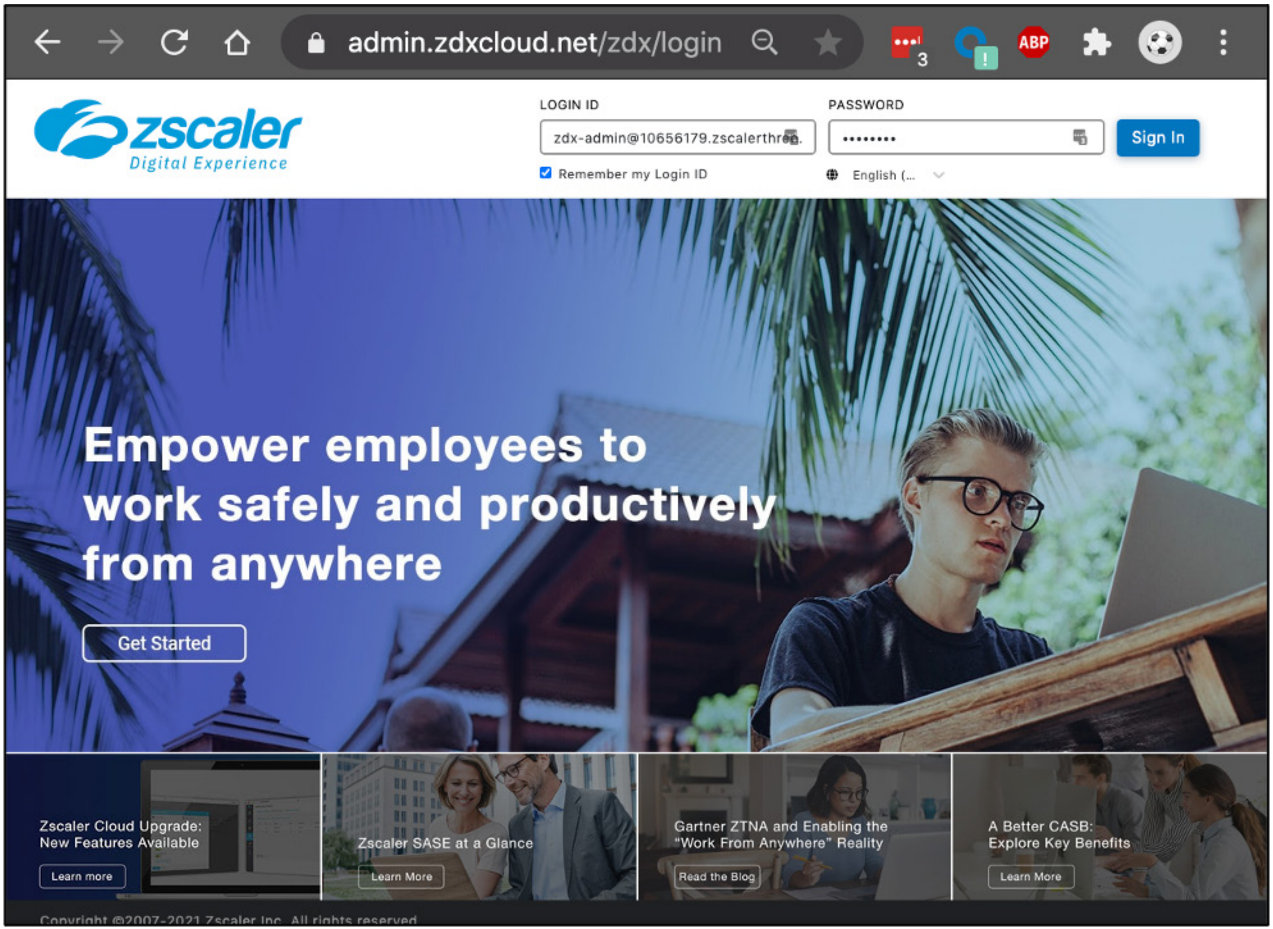
Figure 67. ZDX for user experience monitoring for Salesforce

ZDX allows organizations to continuously gather and analyze data on end user device resources and events, such as CPU, memory usage, and Wi-Fi connectivity that impact end user experiences. You can measure and analyze end-to-end and hop-by-hop network path metrics from every user device to the cloud application. With cloud path visibility, you can proactively detect and resolve end user connectivity issues to cloud applications.

- Continuously monitor and measure application metrics, such as response time, DNS resolution, and broader availability metrics of the application.
- Monitor aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

Configure ZDX for Salesforce

Log in to the ZDX Admin Portal with admin credentials to begin the configuration process.



admin.zdxcloud.net/zdx/login

LOGIN ID: zdx-admin@10656179.zscalerthree.

PASSWORD: ••••••••

Sign In

☑ Remember my Login ID

English (...

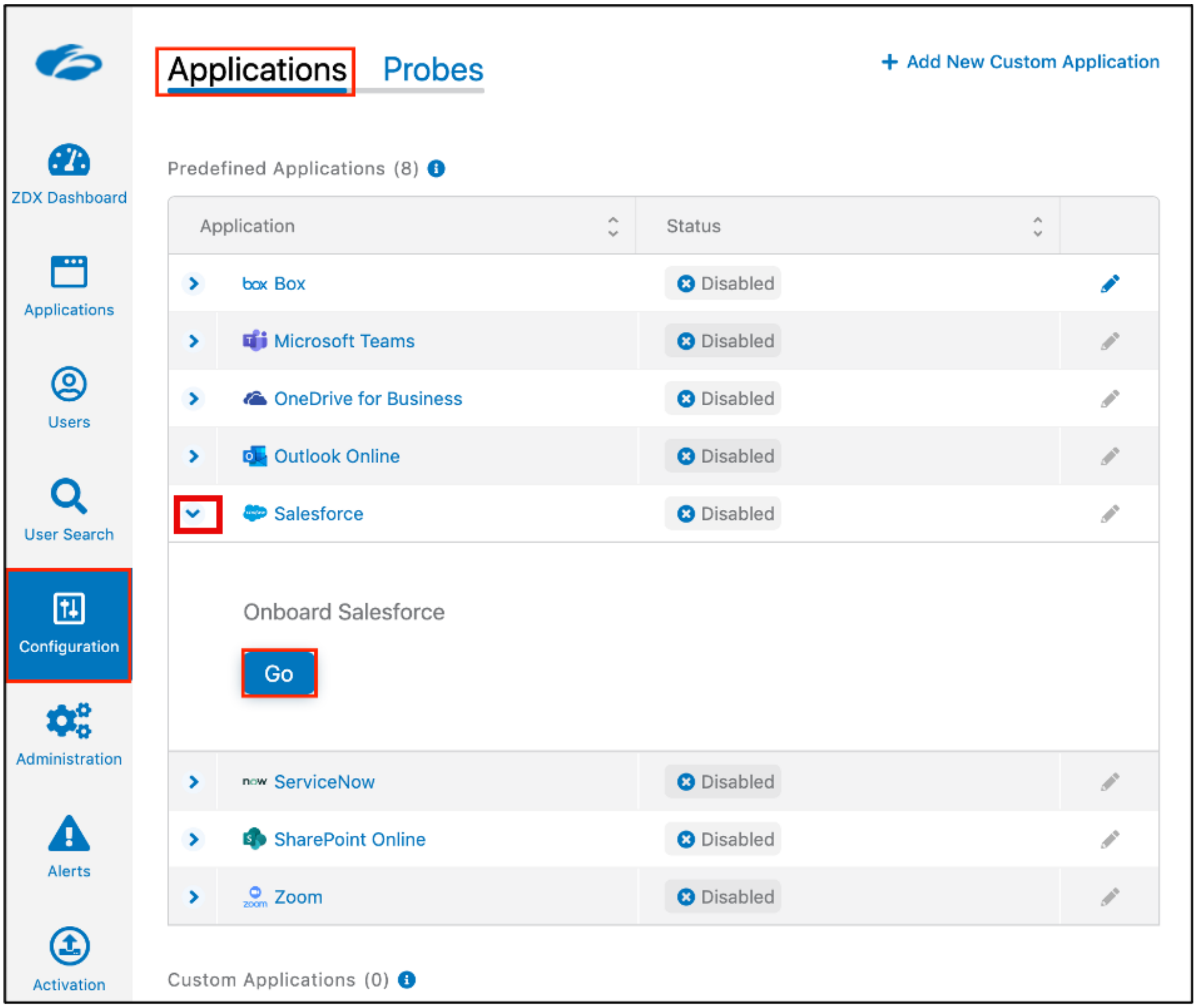
zscaler
Digital Experience
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2021 Zscaler Inc. All rights reserved.

Figure 68. ZDX for user experience monitoring for Salesforce

Salesforce is a predefined application in ZDX.

To configure the Salesforce application for monitoring:

1. Go to **Configuration** > **Applications**.
2. Click the **Expand** icon next to the Salesforce app.
3. Click **Go** to onboard Salesforce.



Predefined Applications (8)

Application	Status
Box	Disabled
Microsoft Teams	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Disabled
ServiceNow	Disabled
SharePoint Online	Disabled
Zoom	Disabled

Custom Applications (0)

Figure 69. Onboard the Salesforce app

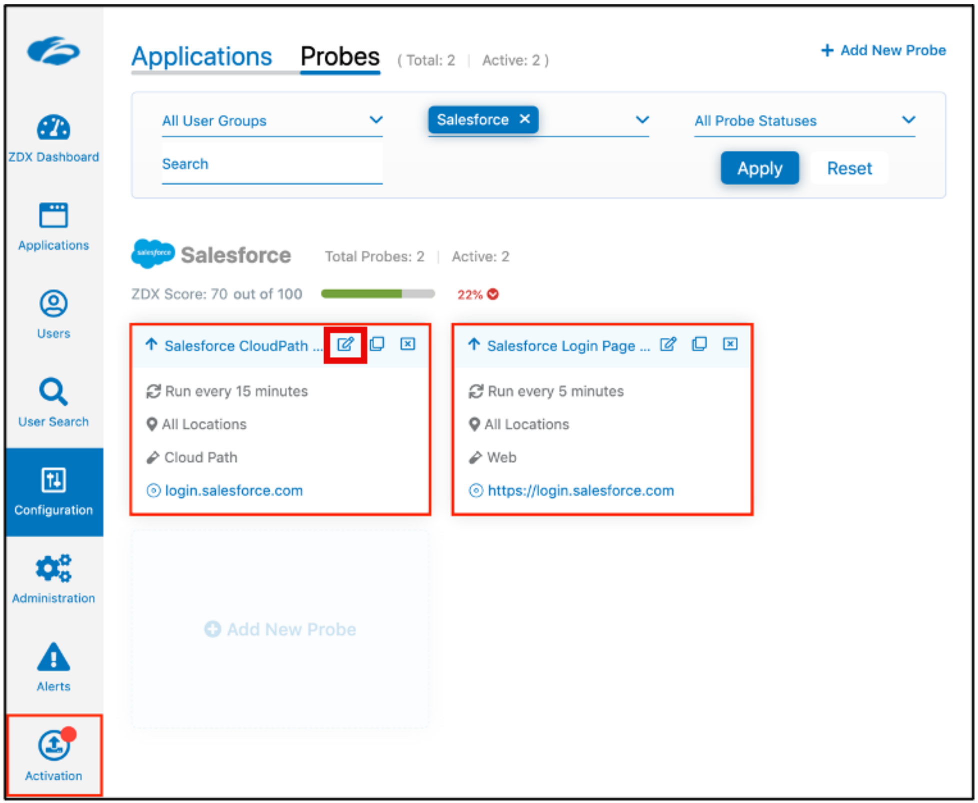
Configure Probes for Salesforce Monitoring

Clicking the **Go** button enables monitoring for the Salesforce app. The preconfigured probes are displayed. The probes consist of a network probe that uses an ICMP Trace Route, and a web probe to the <account>.Salesforce.com location that monitors page load times.

Make one change to the network probe to have it follow the path of the web probe so there is no confusion of the results since this is entirely for Salesforce monitoring.

To edit the rule:

1. Click **Activation** to activate the changes.
2. Click the **Edit** icon to edit the probe.



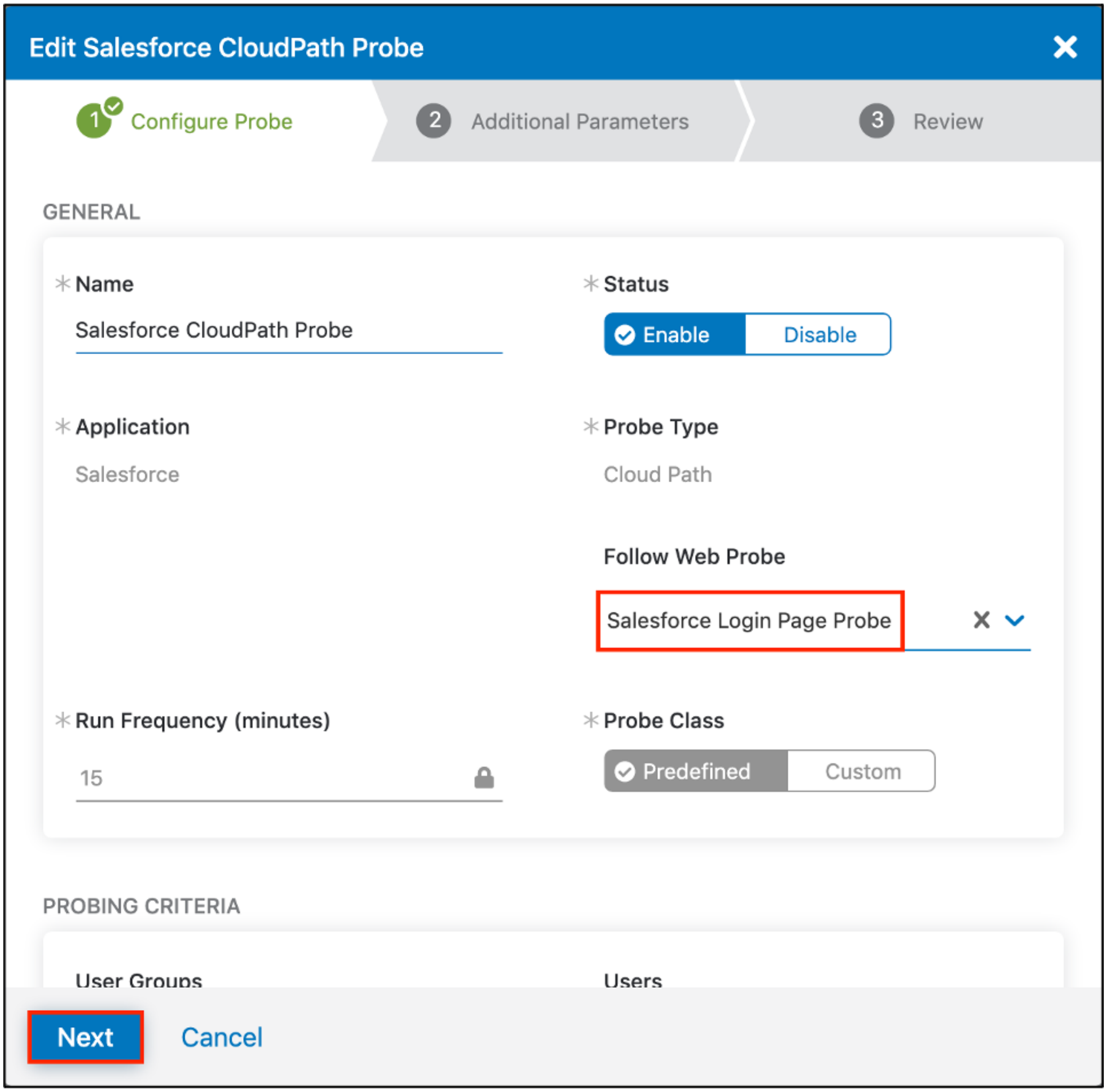
Salesforce CloudPath ...
Run every 15 minutes
All Locations
Cloud Path
login.salesforce.com

Salesforce Login Page ...
Run every 5 minutes
All Locations
Web
https://login.salesforce.com

Figure 70. ZDX for user experience monitoring for Salesforce

To configure the probe to monitor Salesforce:

1. Select **Salesforce Login Page Probe** from the **Follow Web Probe** drop-down menu.
2. Click **Next**.



Edit Salesforce CloudPath Probe

GENERAL

* Name: Salesforce CloudPath Probe

* Status: Enable | Disable

* Application: Salesforce

* Probe Type: Cloud Path

Follow Web Probe: Salesforce Login Page Probe

* Run Frequency (minutes): 15

* Probe Class: Predefined | Custom

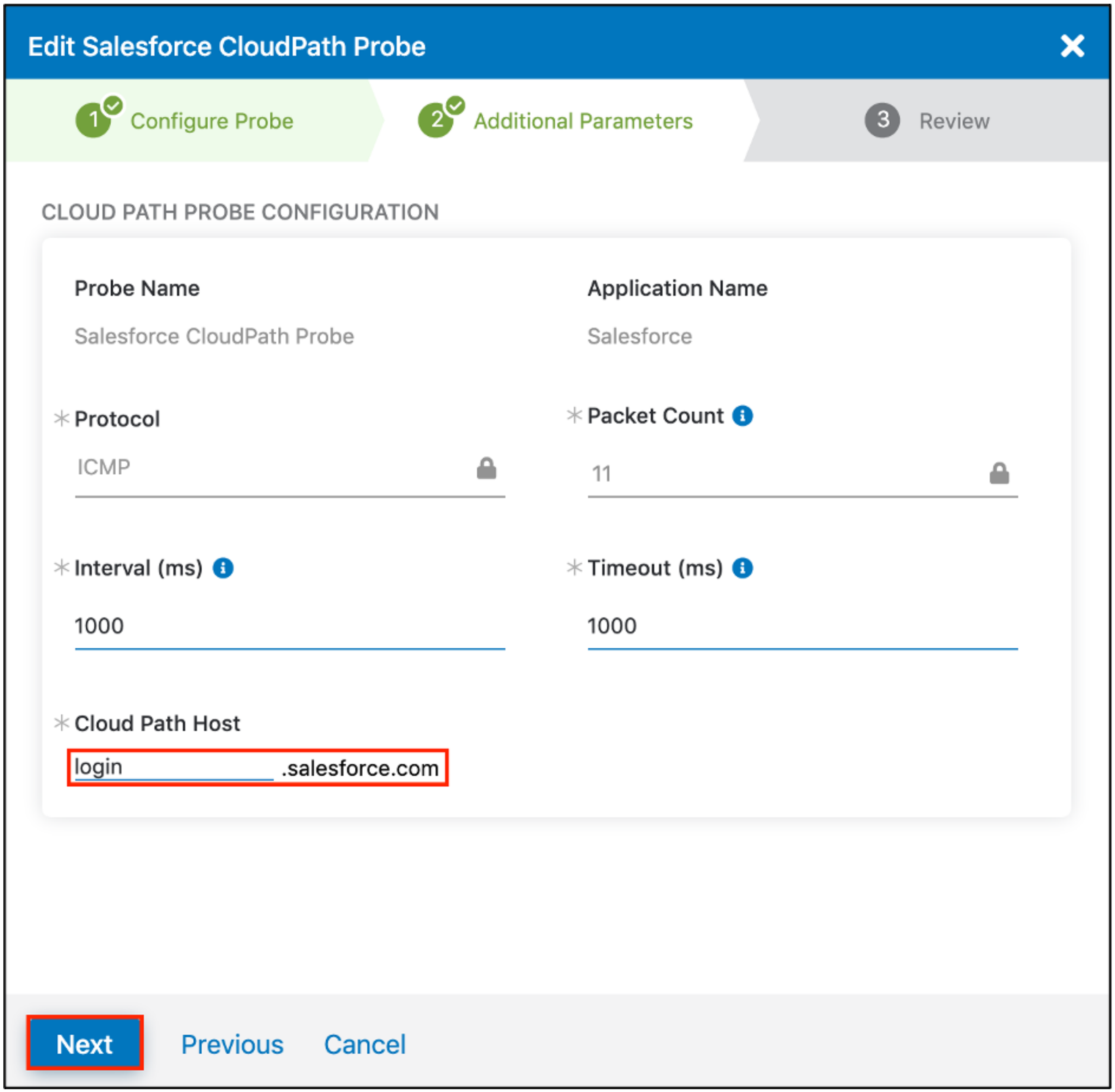
PROBING CRITERIA

User Groups

Users

Figure 71. Edit the network probe

3. Validate the **Cloud Path Host** destination is <account>.Salesforce.com.
4. Click **Next**.



Edit Salesforce CloudPath Probe

CLOUD PATH PROBE CONFIGURATION

Probe Name: Salesforce CloudPath Probe

Application Name: Salesforce

* Protocol: ICMP

* Packet Count: 11

* Interval (ms): 1000

* Timeout (ms): 1000

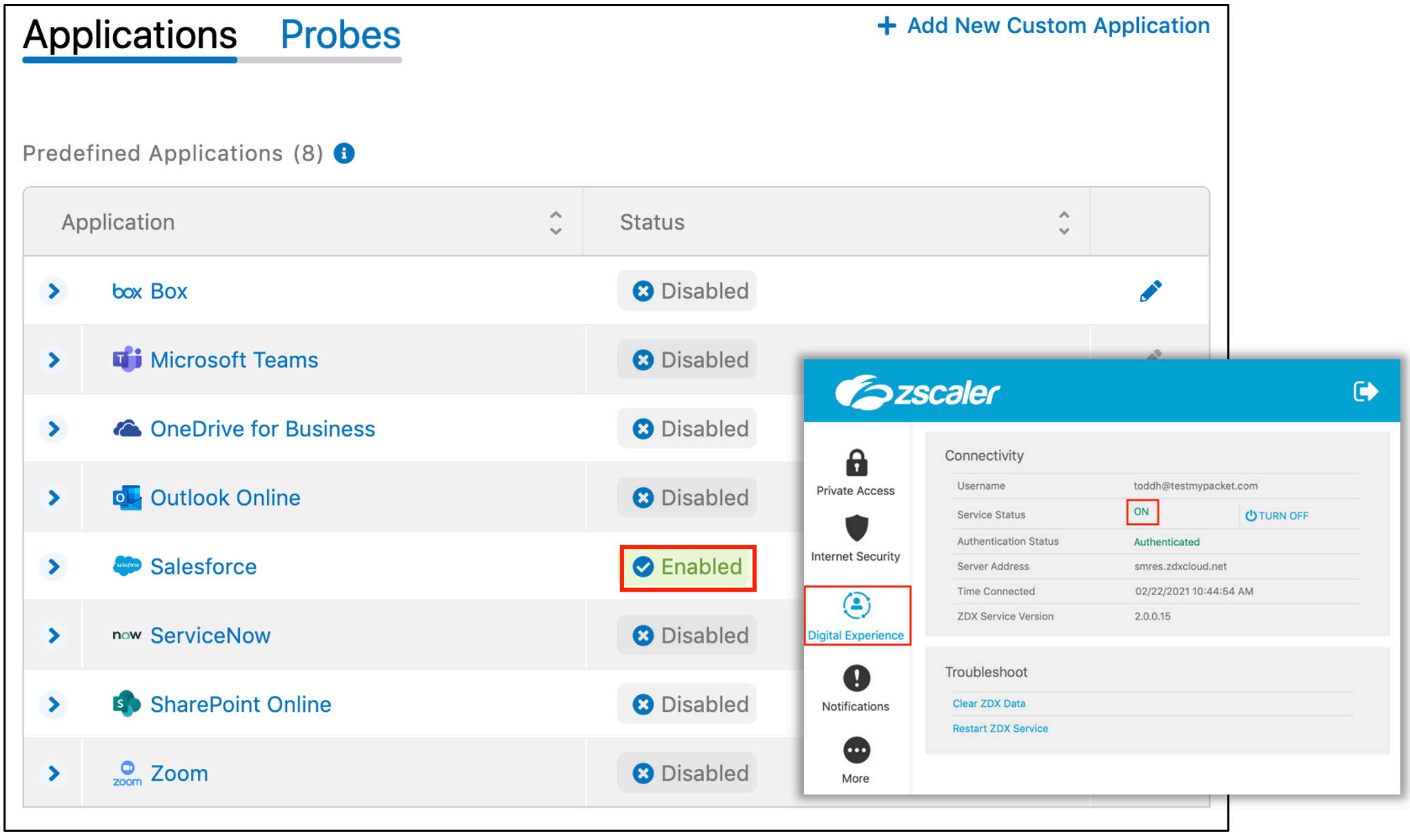
* Cloud Path Host: login .salesforce.com

Figure 72. Edit the network probe

5. Review and activate the changes to the probe.

The Enabled Salesforce Application

The Salesforce application monitoring is now activated and probes start from all of the users using Zscaler Client Connector. The following image shows Zscaler Client Connector running the digital experience with the service **On**.



Predefined Applications (8)

Application	Status
Box	Disabled
Microsoft Teams	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Enabled
ServiceNow	Disabled
SharePoint Online	Disabled
Zoom	Disabled

Connectivity

Username	toddh@testmypacket.com
Service Status	ON ⏻ TURN OFF
Authentication Status	Authenticated
Server Address	smres.zdxcloud.net
Time Connected	02/22/2021 10:44:54 AM
ZDX Service Version	2.0.0.15

Troubleshoot

Figure 73. Active Salesforce monitoring

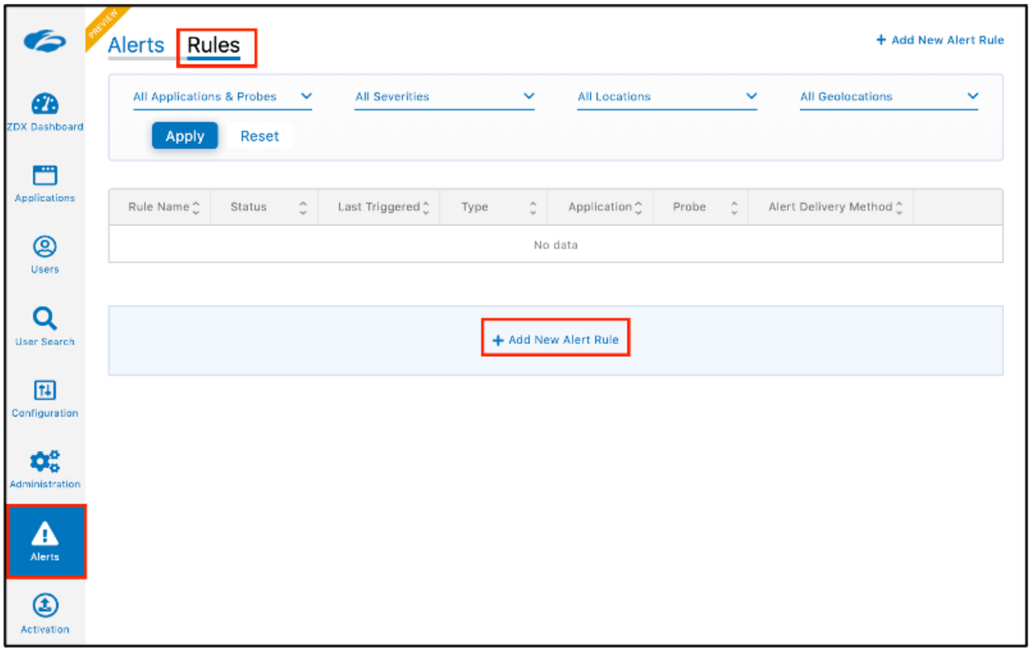
Create an Alert for the Salesforce Service

As a final configuration step, create an email alert in the event of service degradation of the Salesforce application. You can configure an alert for network, application, or device thresholds:

- Network Probe: Latency, MTR, Packet Loss, Number of Hops
- Application Probe: DNS Response Time, Page Fetch Time, Server Response Time, Web Request Availability
- Device Monitor: CPU Usage, Bandwidth, Battery, CPU, Disk, Wi-Fi Signal Strength, Memory, Sent and Received Mbps

To create an alert on Page Fetch Times:

1. Go to **Alerts** > **Rules**.
2. Click **Add New Alert Rule**.

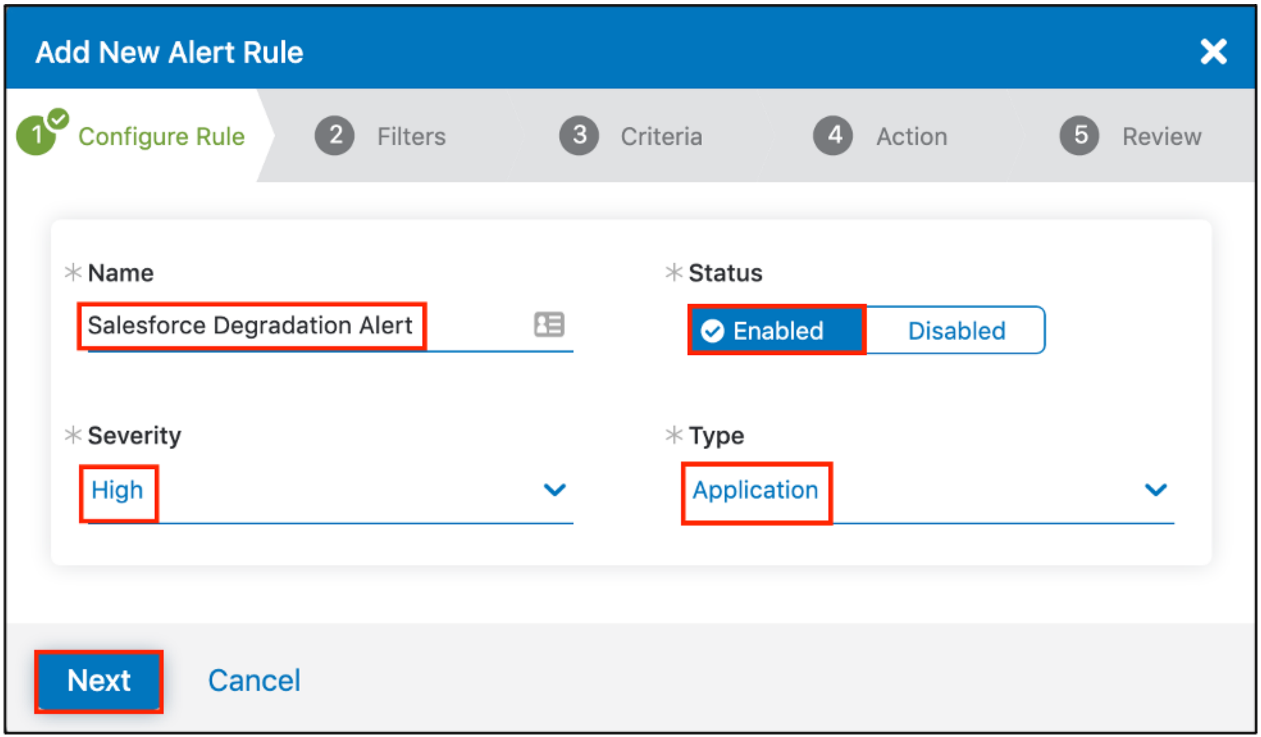


Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
No data						

Figure 74. Creating an alert

Step 1 of the rule wizard:

1. Enter a **Name** for the rule.
2. Select **Enabled** under **Status**.
3. Give the alert an appropriate **Severity**.
4. Select **Application** from the **Type** drop-down menu.
5. Click **Next**.



Add New Alert Rule

*Name: Salesforce Degradation Alert

*Status: Enabled

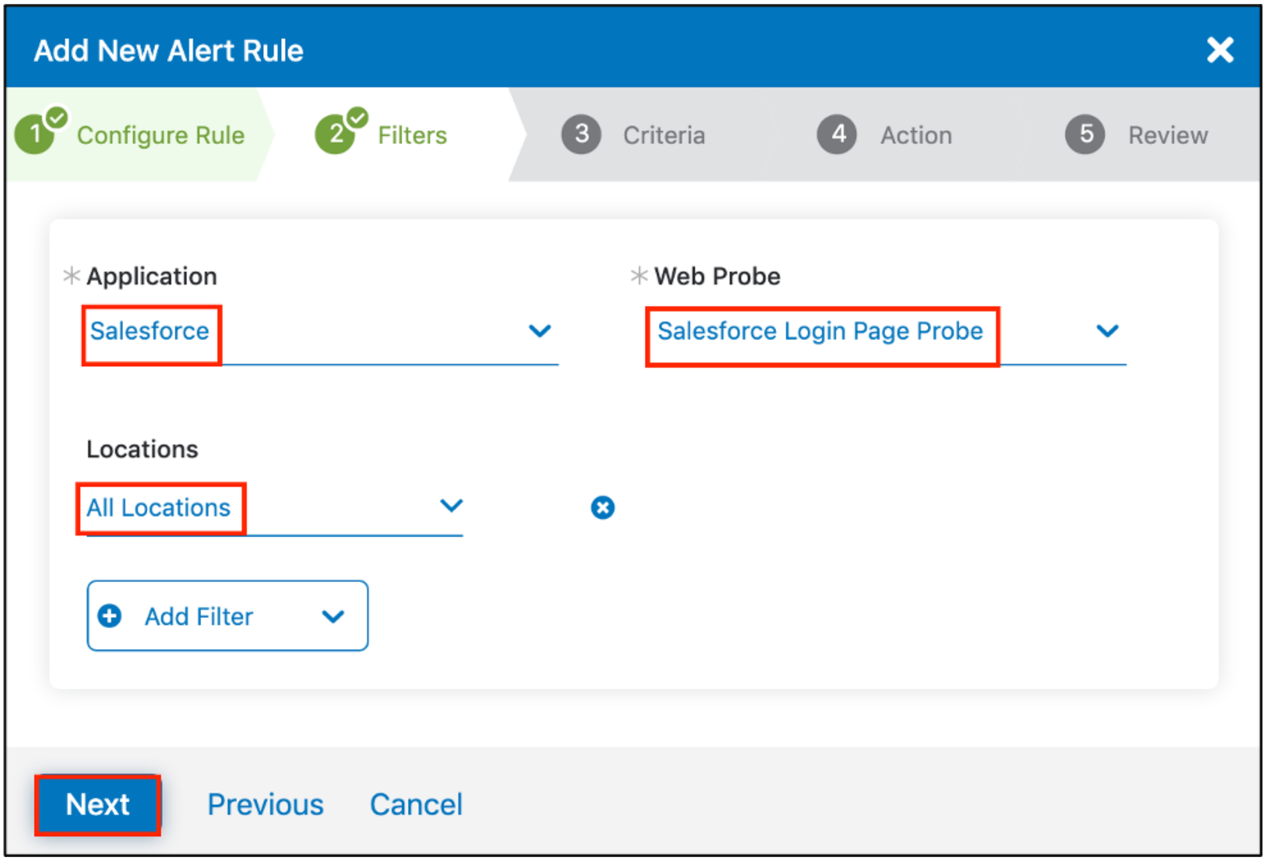
*Severity: High

*Type: Application

Figure 75. The Alert Creation wizard

Step 2 of the rule wizard:

1. Select **Salesforce** as the **Application**.
2. Select **Salesforce Login Page Probe** from the **Web Probe** drop-down menu.
3. Select **All Locations** from the **Locations** drop-down menu.
4. Click **Next**.



Add New Alert Rule

* Application: Salesforce

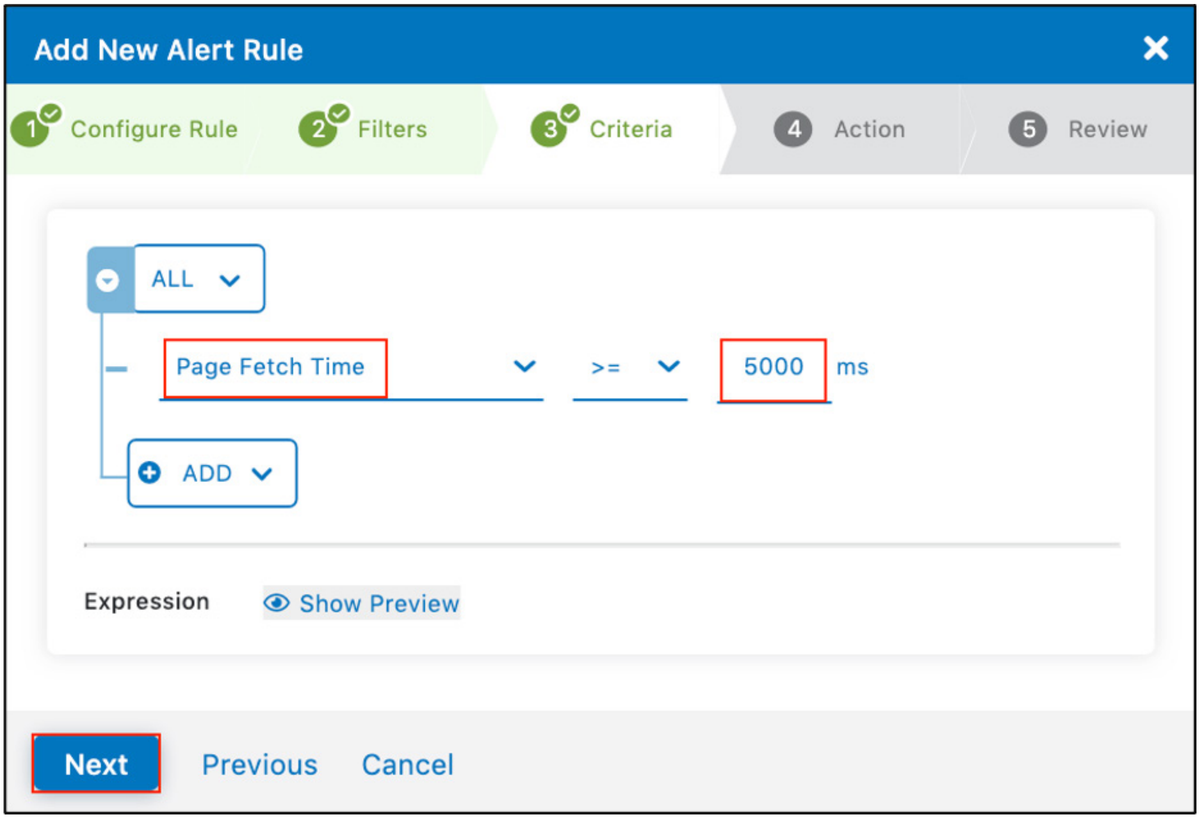
* Web Probe: Salesforce Login Page Probe

Locations: All Locations

Figure 76. The Alert Creation wizard

Step 3 of the rule wizard creates the criteria and threshold that triggers the alert. Use multiple variables here to eliminate false positives.

1. Select **Page Fetch Time**.
2. Enter the time to exceed **5000** ms (5 seconds).
3. Click **Next**.



Add New Alert Rule

1 Configure Rule ✓ | 2 Filters ✓ | 3 Criteria ✓ | 4 Action | 5 Review

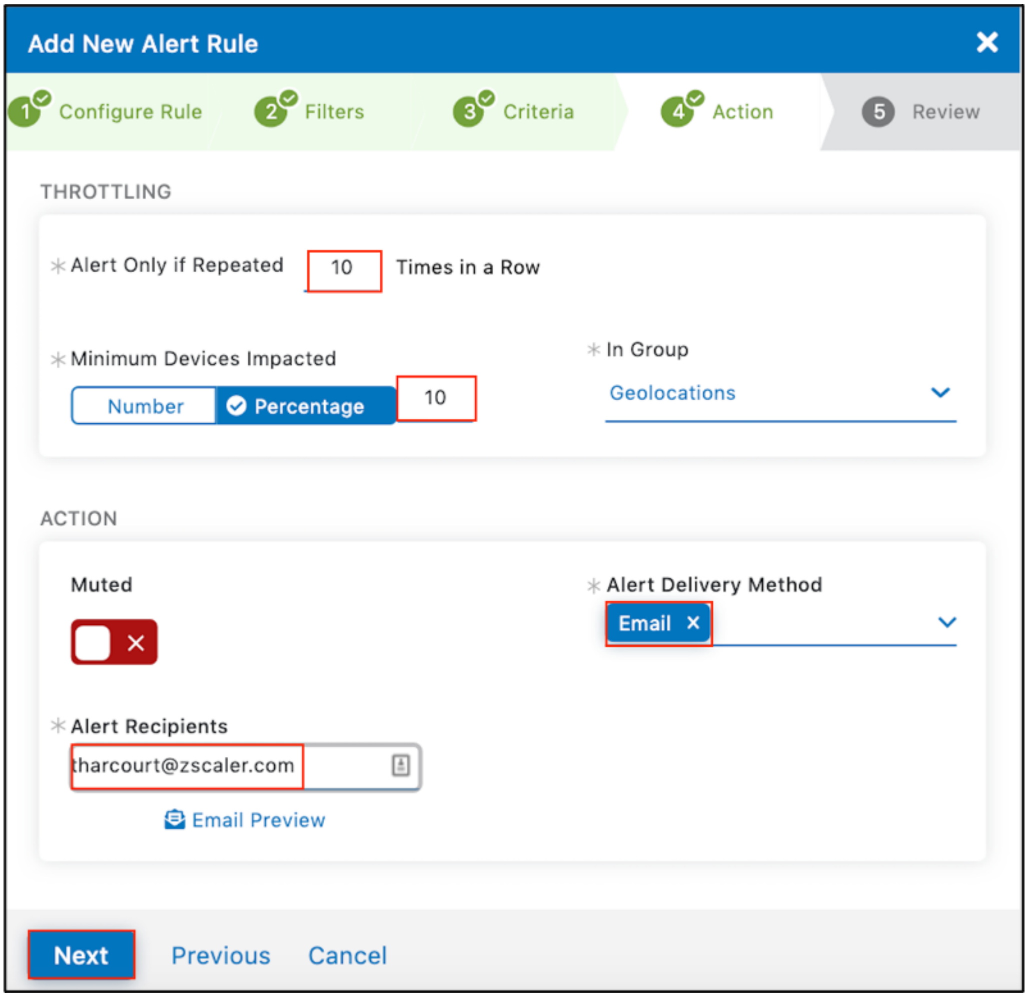
ALL

Page Fetch Time >= 5000 ms

Figure 77. The Alert Creation wizard

Step 4 of the rule wizard adds throttling to control the scope of the alert. Define the action as sending an email. The action can also be defined as an authenticated webhook, which could be used to send the alert to a Slack channel:

1. Enter **10** for the number of times the probe time must exceed the threshold.
2. Select **Percentage** and enter `10` for the **Minimum Devices Impacted**.
3. Select **Email** from the **Alert Delivery Method** drop-down menu.
4. Enter the **Alert Recipients** email addresses separated by commas.
5. Click **Next**.



Add New Alert Rule

THROTTLING

* Alert Only if Repeated 10 Times in a Row

* Minimum Devices Impacted: Number / Percentage (selected) 10

* In Group: Geolocations

ACTION

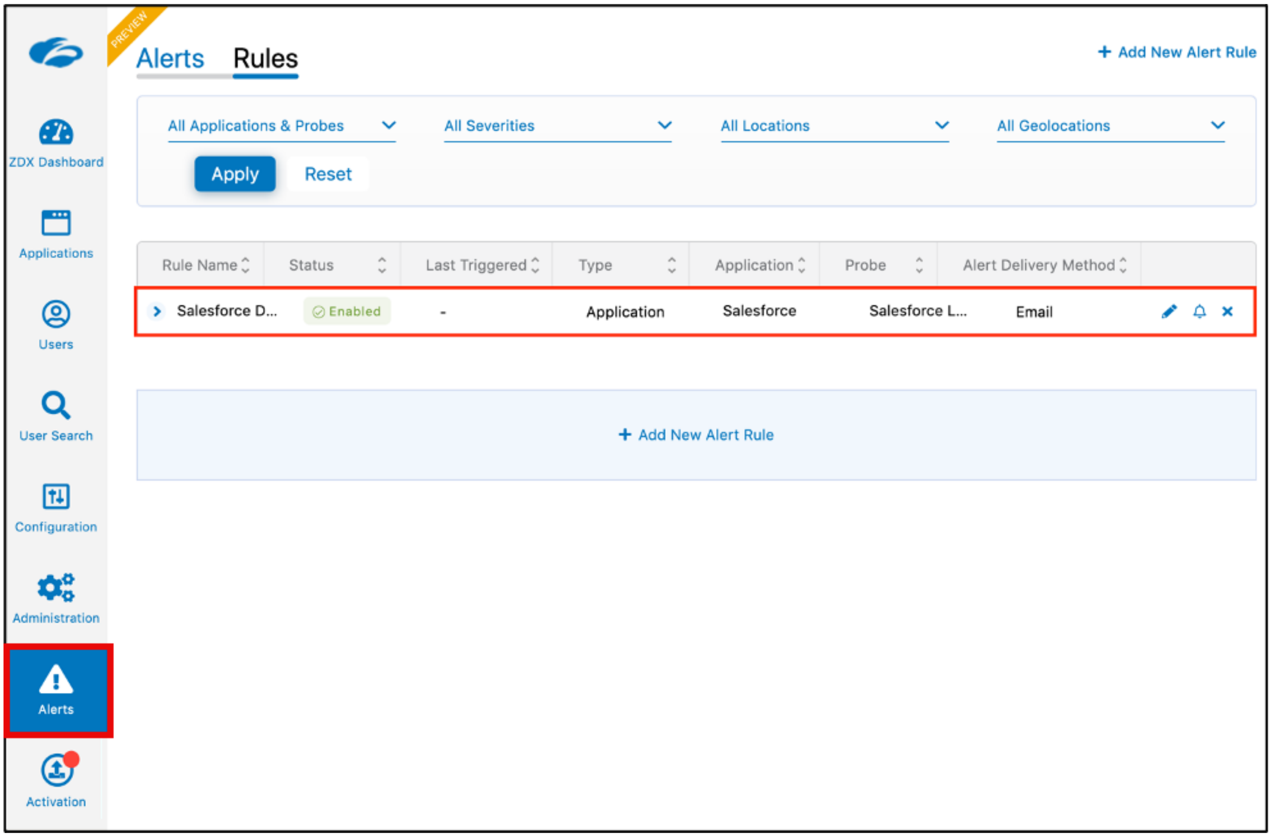
Muted: ☒

* Alert Delivery Method: Email ×

* Alert Recipients: tharcourt@zscaler.com

Figure 78. The Alert Creation wizard

The **Alerts** > **Rules** tab shows the completed rule set for the alert.

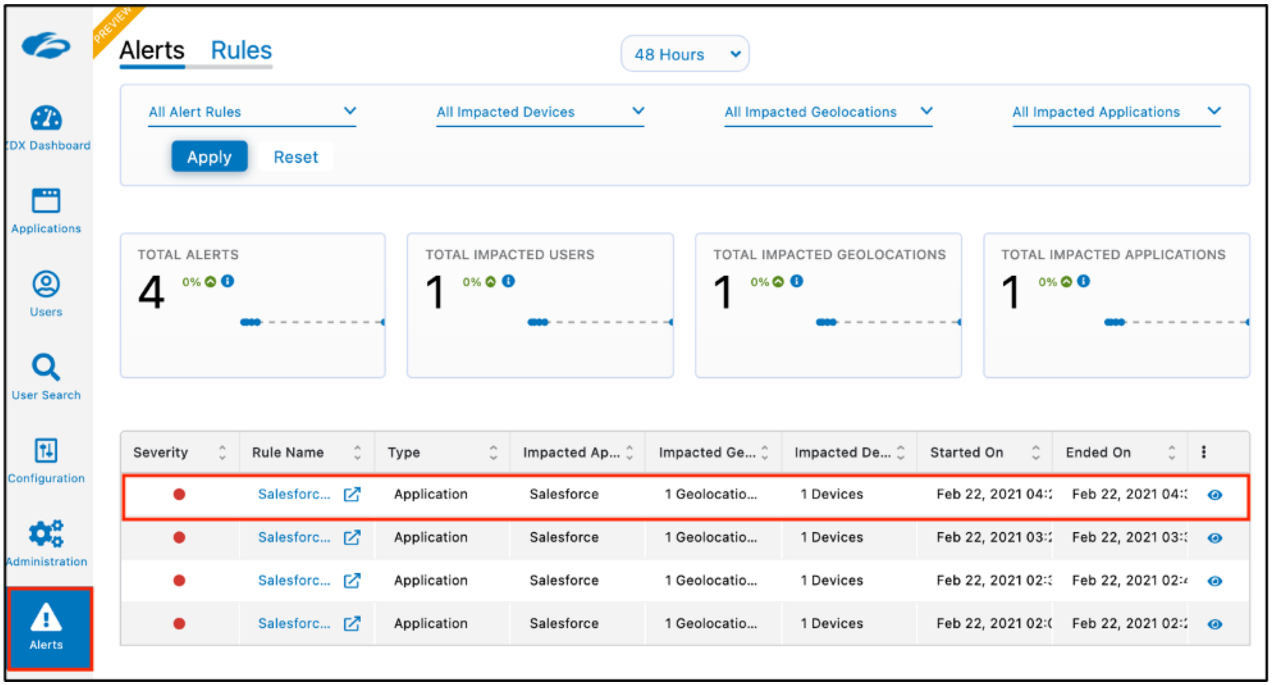


Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
Salesforce D...	Enabled	-	Application	Salesforce	Salesforce L...	Email

Figure 79. The completed rule set

The Triggered Alert for the Salesforce Service

A triggered alert generated by the rule set threshold settings is shown on the **Alerts** > **Rules** tab. You can click the **Rule Name** or click the **View** icon to view more detail about the alert.



TOTAL ALERTS 4 0%

TOTAL IMPACTED USERS 1 0%

TOTAL IMPACTED GEOLOCATIONS 1 0%

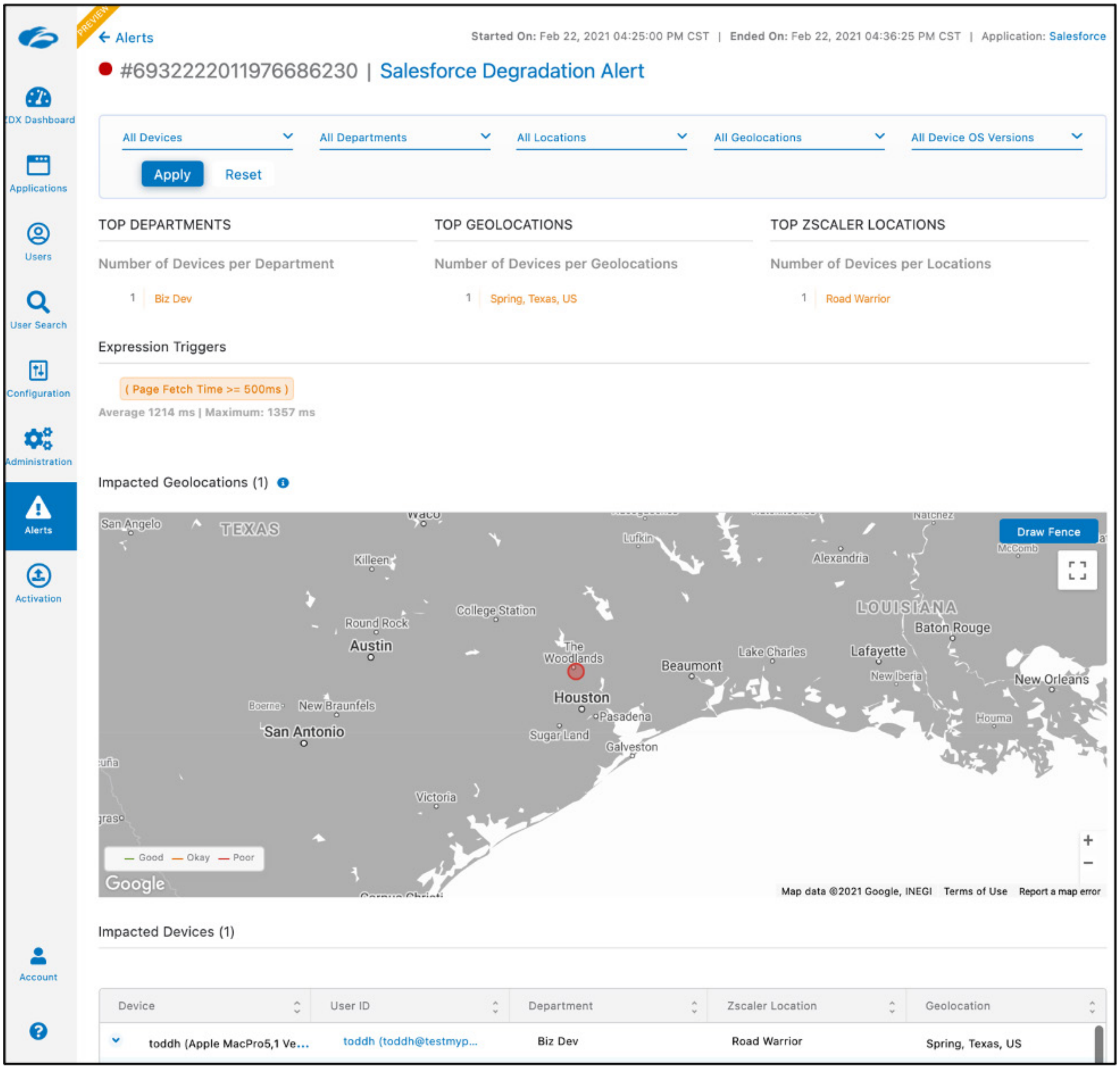
TOTAL IMPACTED APPLICATIONS 1 0%

Severity	Rule Name	Type	Impacted Ap...	Impacted Ge...	Impacted De...	Started On	Ended On
●	Salesforc...	Application	Salesforce	1 Geolocatio...	1 Devices	Feb 22, 2021 04:	Feb 22, 2021 04:
●	Salesforc...	Application	Salesforce	1 Geolocatio...	1 Devices	Feb 22, 2021 03:	Feb 22, 2021 03:
●	Salesforc...	Application	Salesforce	1 Geolocatio...	1 Devices	Feb 22, 2021 02:	Feb 22, 2021 02:
●	Salesforc...	Application	Salesforce	1 Geolocatio...	1 Devices	Feb 22, 2021 02:	Feb 22, 2021 02:

Figure 80. The alert

Alert Detail for the Salesforce Service

The alert detail for the triggered alert shows impacted user and devices, impact location, and threshold details.



Started On: Feb 22, 2021 04:25:00 PM CST | Ended On: Feb 22, 2021 04:36:25 PM CST | Application: Salesforce

● #6932222011976686230 | Salesforce Degradation Alert

TOP DEPARTMENTS

Number of Devices per Department

1 | Biz Dev

TOP GEOLOCATIONS

Number of Devices per Geolocations

1 | Spring, Texas, US

TOP ZSCALER LOCATIONS

Number of Devices per Locations

1 | Road Warrior

Expression Triggers

(Page Fetch Time >= 500ms)

Average 1214 ms | Maximum: 1357 ms

Impacted Geolocations (1)

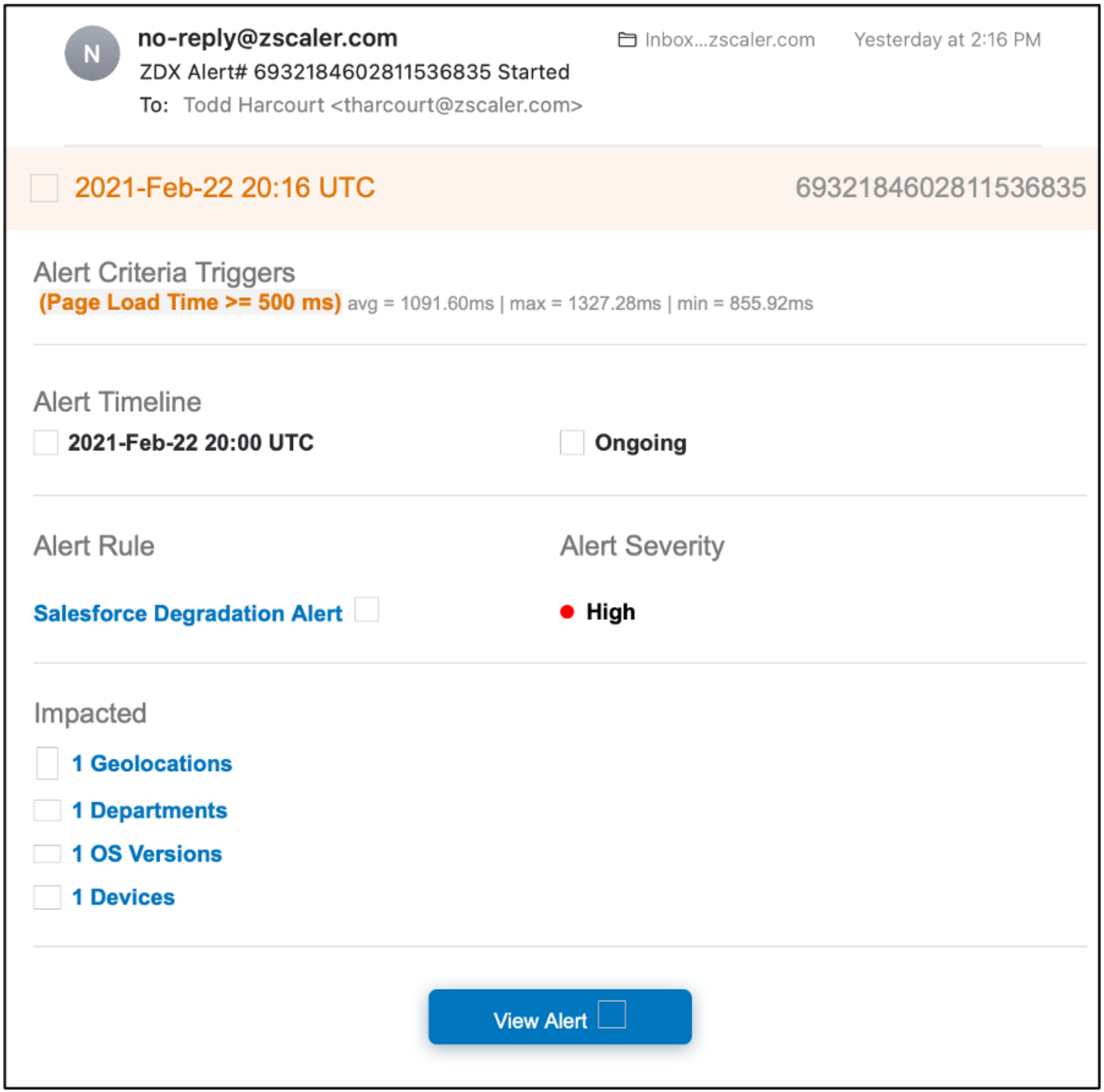
Impacted Devices (1)

Device	User ID	Department	Zscaler Location	Geolocation
toddh (Apple MacPro5,1 Ve...	toddh (toddh@testmyp...	Biz Dev	Road Warrior	Spring, Texas, US

Figure 81. Alert details

The Sent Alert Email for the Salesforce Service

The following is the email alert sent to the recipients after the alert threshold was exceeded. Another email is sent when the threshold returns to normal values if the alert is an ongoing or continuous alert.



no-reply@zscaler.com
Inbox...zscaler.com
Yesterday at 2:16 PM

ZDX Alert# 6932184602811536835 Started

To: Todd Harcourt <tharcourt@zscaler.com>

2021-Feb-22 20:16 UTC 6932184602811536835

Alert Criteria Triggers

(Page Load Time >= 500 ms) avg = 1091.60ms | max = 1327.28ms | min = 855.92ms

Alert Timeline

2021-Feb-22 20:00 UTC Ongoing

Alert Rule

Salesforce Degradation Alert

Alert Severity

● High

Impacted

1 Geolocations

1 Departments

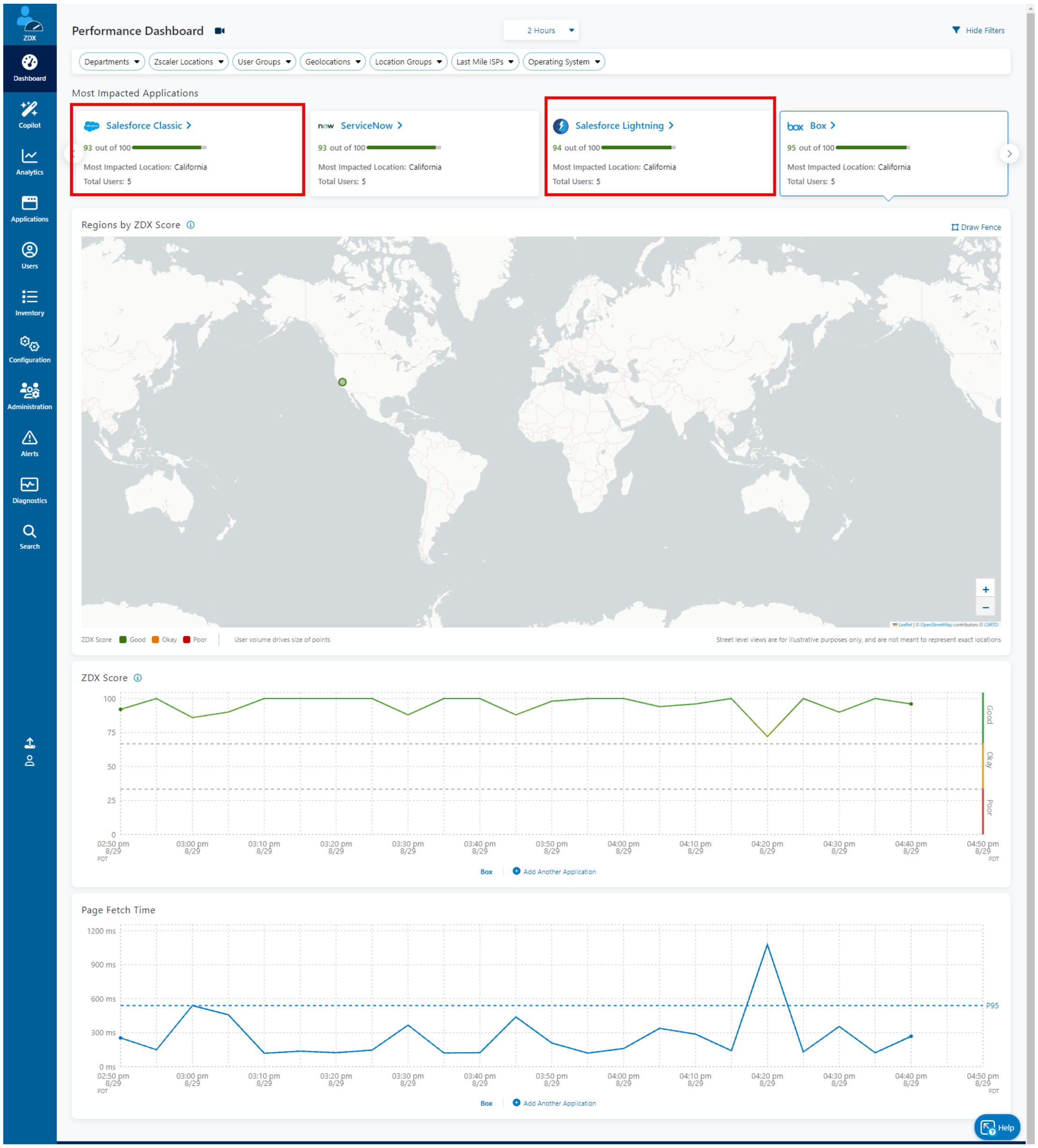
1 OS Versions

1 Devices

Figure 82. The alert email

Using ZDX: The Dashboard

The ZDX dashboard provides a single page to monitor the user experience (ZDX Score) of all users and all applications. An active heat map also shows you any locations globally that might have issues.



Most Impacted Applications

Salesforce Classic
93 out of 100
Most Impacted Location: California
Total Users: 5

ServiceNow
93 out of 100
Most Impacted Location: California
Total Users: 5

Salesforce Lightning
94 out of 100
Most Impacted Location: California
Total Users: 5

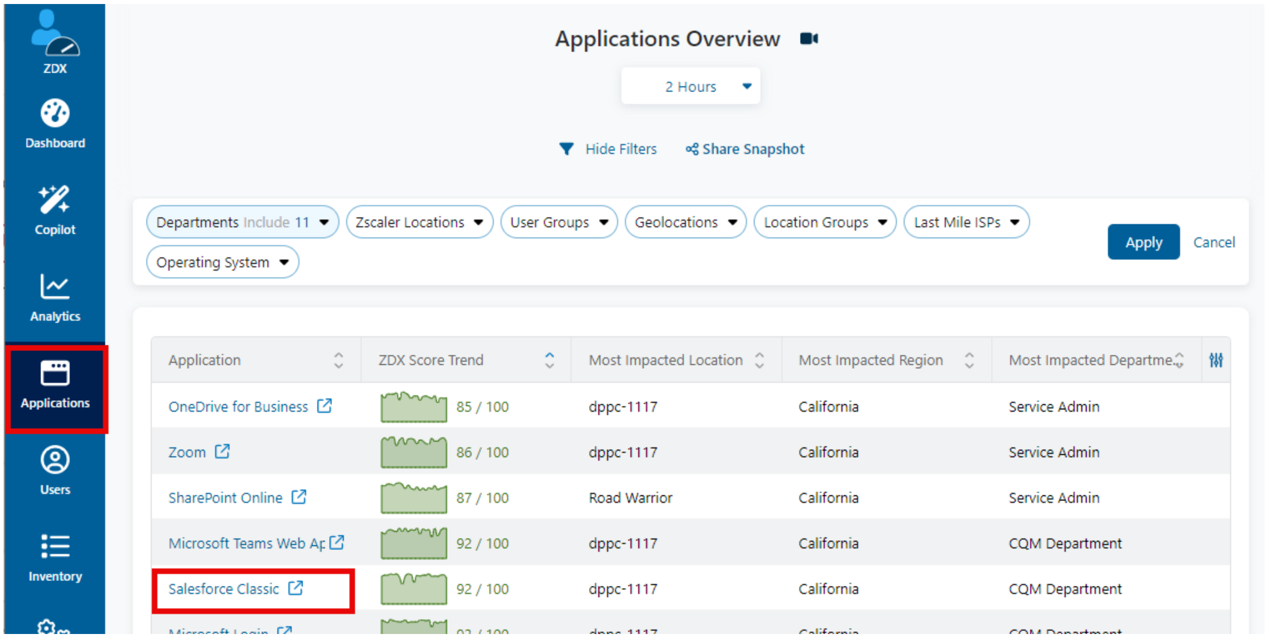
Box
95 out of 100
Most Impacted Location: California
Total Users: 5

Figure 83. The dashboard

Application Overview

Selecting **Applications** on the left-side navigation of the ZDX Admin Portal displays the **Applications Overview** and shows all the configured applications as individual ZDX Scores. Take a look at the detail of the Salesforce application.

1. Go to **Applications**.
2. Select the **Salesforce** application.



Application	ZDX Score Trend	Most Impacted Location	Most Impacted Region	Most Impacted Departme
OneDrive for Business	85 / 100	dppc-1117	California	Service Admin
Zoom	86 / 100	dppc-1117	California	Service Admin
SharePoint Online	87 / 100	Road Warrior	California	Service Admin
Microsoft Teams Web Ap	92 / 100	dppc-1117	California	CQM Department
Salesforce Classic	92 / 100	dppc-1117	California	CQM Department
Microsoft Login	93 / 100	dppc-1117	California	CQM Department

Figure 84. Application overview

Application Detail

The top portion of the application details shows a historical view of the ZDX Score and the page fetch time. Any spike of the page fetch time indicates a possible slowdown of the Salesforce service itself.

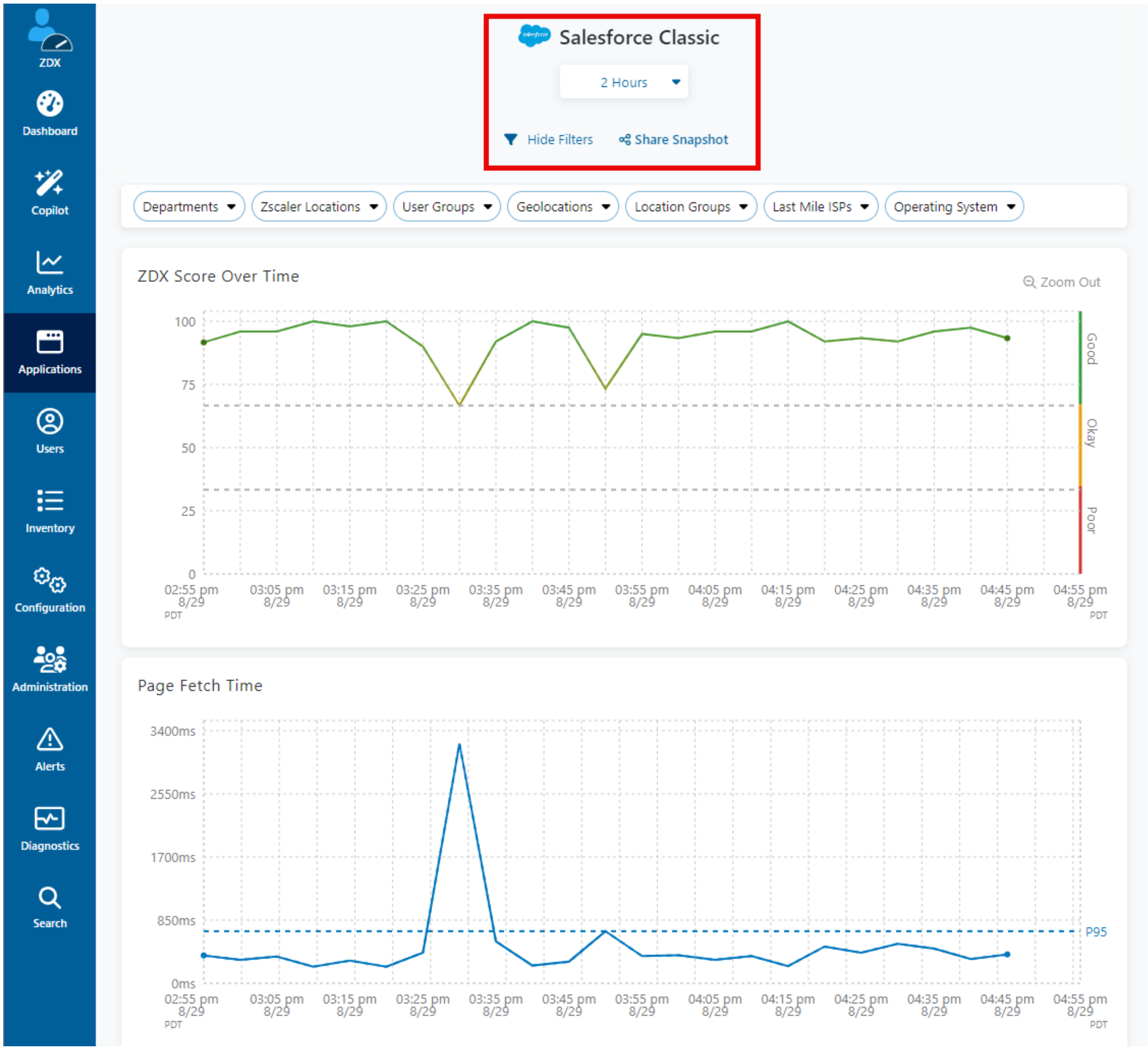
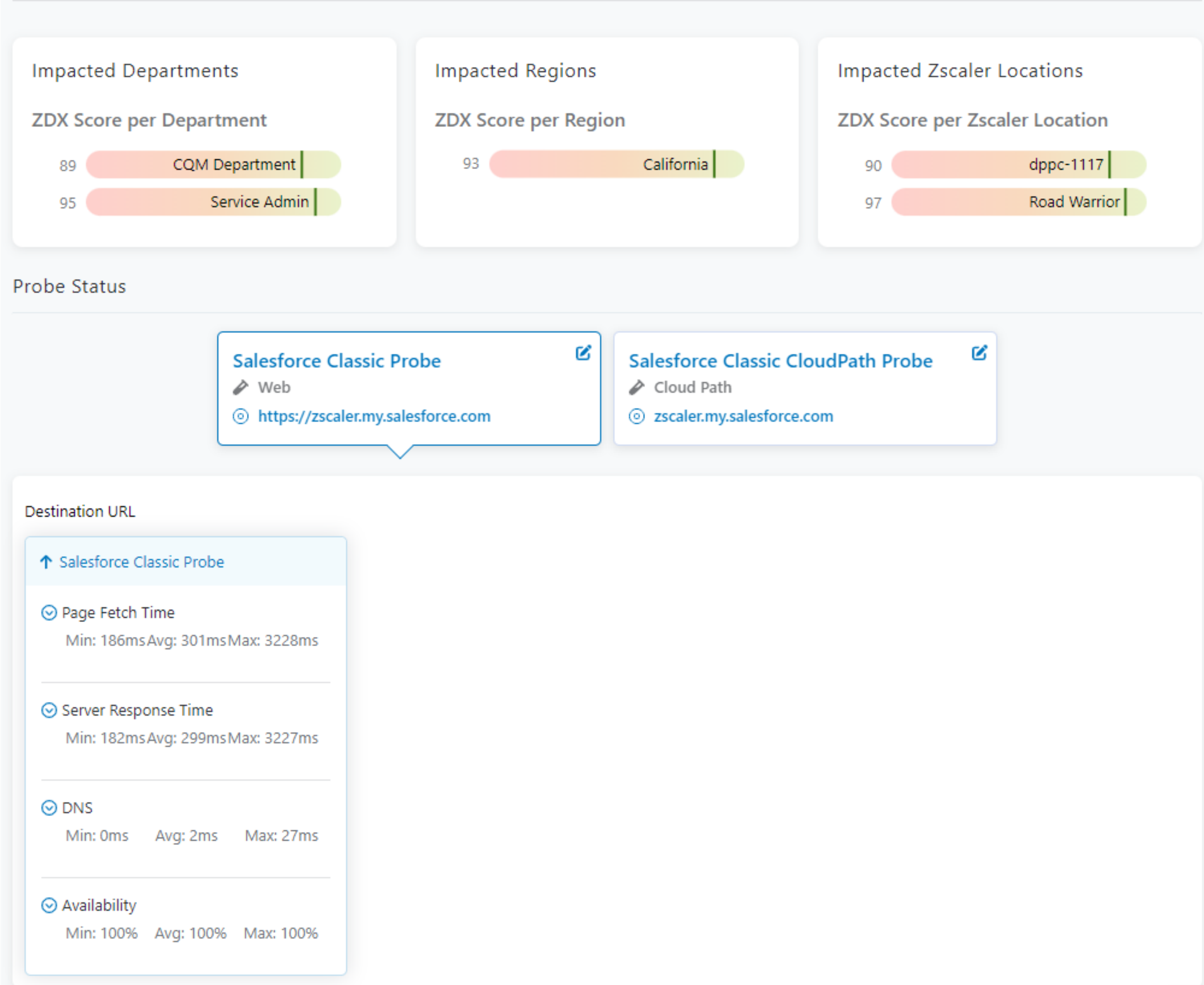


Figure 85. Application detail

The bottom portion of the application details shows the **Top Departments**, **Top Cities**, and **Top Zscaler Locations** using the application and the ZDX Scores at a glance. You can view probe data, with minimum, maximum, and average response times.



Impacted Departments

ZDX Score per Department

89	CQM Department
95	Service Admin

Impacted Regions

ZDX Score per Region

93	California

Impacted Zscaler Locations

ZDX Score per Zscaler Location

90	dppc-1117
97	Road Warrior

Probe Status

Salesforce Classic Probe
Web
https://zscaler.my.salesforce.com

Salesforce Classic CloudPath Probe
Cloud Path
zscaler.my.salesforce.com

Destination URL

Salesforce Classic Probe

Page Fetch Time
Min: 186ms Avg: 301ms Max: 3228ms

Server Response Time
Min: 182ms Avg: 299ms Max: 3227ms

DNS
Min: 0ms Avg: 2ms Max: 27ms

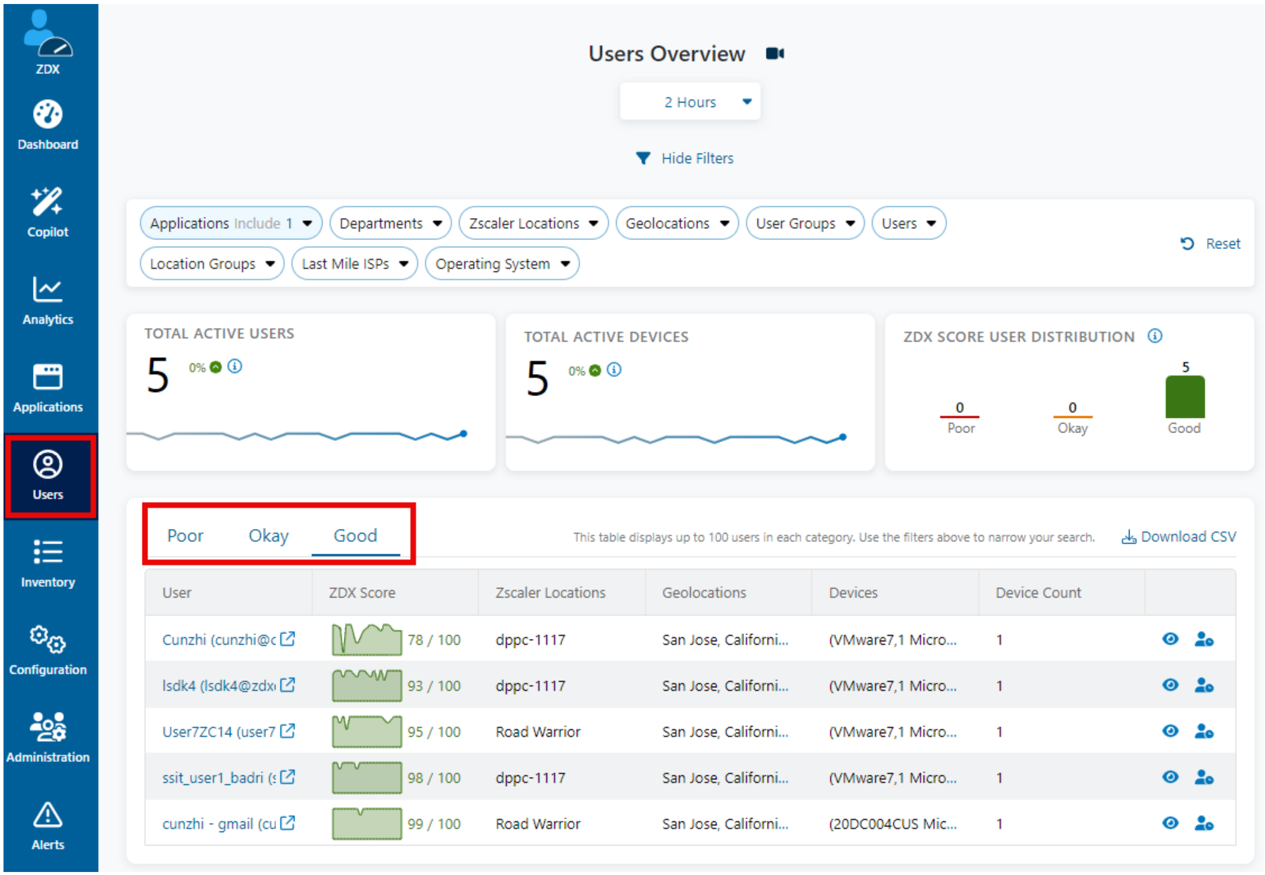
Availability
Min: 100% Avg: 100% Max: 100%

Figure 86. Application detail

User Overview

The **User Overview** provides all the users of an application. Select **Salesforce** and then click **Apply** to see all the Salesforce users. The ZDX Score is provided, and you can select users by **Poor**, **Okay**, or **Good** ZDX Scores. You can get more details about the user by clicking the name or the **View** icon on the right.

Select a **User** to display more detail.



This table displays up to 100 users in each category. Use the filters above to narrow your search.

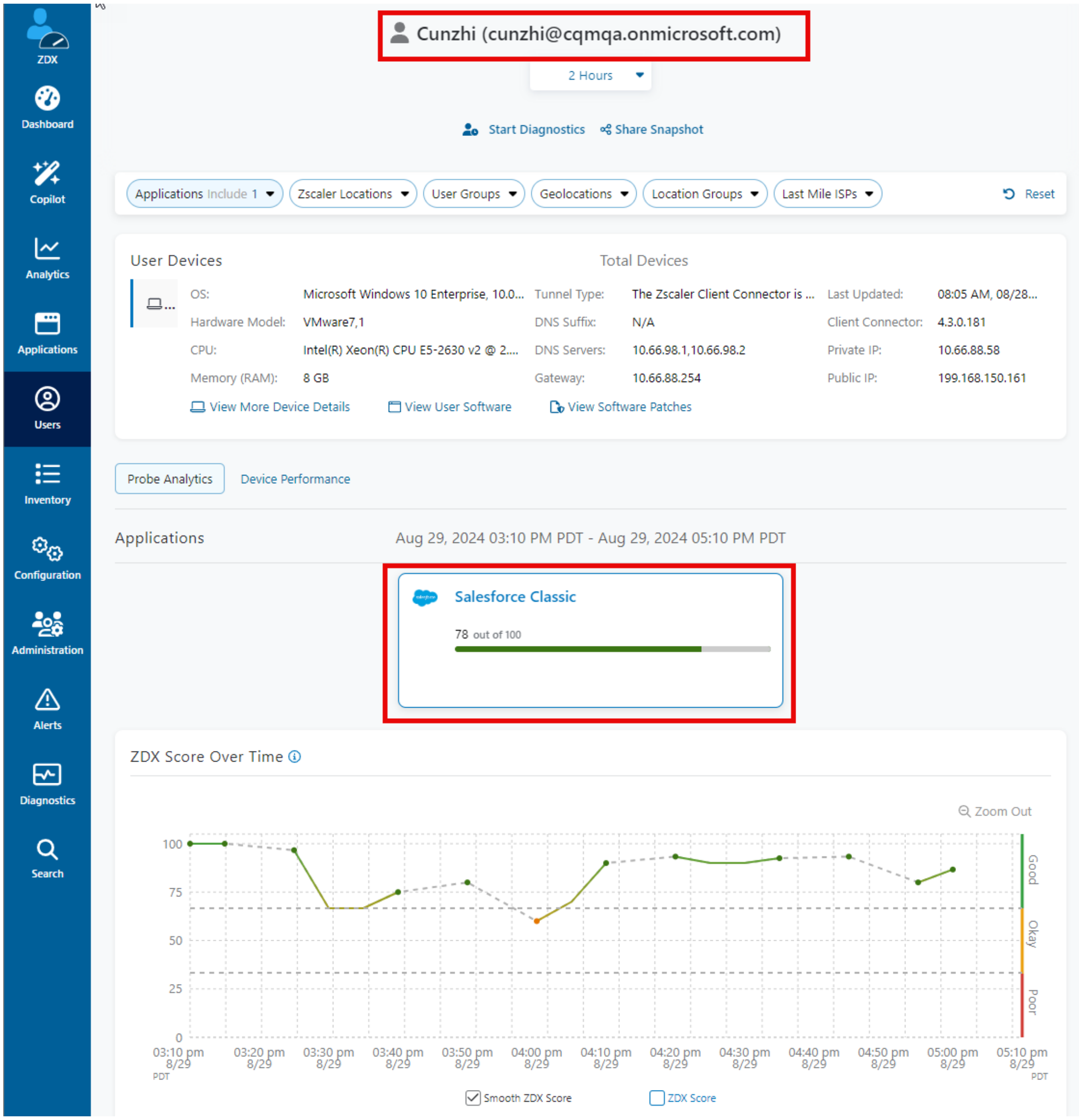
User	ZDX Score	Zscaler Locations	Geolocations	Devices	Device Count
Cunzhi (cunzhi@c	78 / 100	dppc-1117	San Jose, Californi...	(VMware7,1 Micro...	1
lsdk4 (lsdk4@zdx	93 / 100	dppc-1117	San Jose, Californi...	(VMware7,1 Micro...	1
User7ZC14 (user7	95 / 100	Road Warrior	San Jose, Californi...	(VMware7,1 Micro...	1
ssit_user1_badri (s	98 / 100	dppc-1117	San Jose, Californi...	(VMware7,1 Micro...	1
cunzhi - gmail (cu	99 / 100	Road Warrior	San Jose, Californi...	(20DC004CUS Mic...	1

Figure 87. User overview

User Detail

The user detail shows useful data to help isolate any user experience issues.

Select and apply the Salesforce application to see the details of the user experience for the Salesforce app. This report provides the user's devices and the device-specific detail (**OS**, **Device type**, **Network Information**, etc.) by clicking the device. The ZDX Score is also displayed in a time line, and you can see the details of **Page Fetch Times**, **Server Response**, **DNS Response**, **Probe Detail**, and **Device Health** from this page.



Cunzhi (cunzhi@cqmqa.onmicrosoft.com)

2 Hours

Applications Include 1

User Devices

Total Devices

OS:	Microsoft Windows 10 Enterprise, 10.0...	Tunnel Type:	The Zscaler Client Connector is ...	Last Updated:	08:05 AM, 08/28...
Hardware Model:	VMware7,1	DNS Suffix:	N/A	Client Connector:	4.3.0.181
CPU:	Intel(R) Xeon(R) CPU E5-2630 v2 @ 2....	DNS Servers:	10.66.98.1,10.66.98.2	Private IP:	10.66.88.58
Memory (RAM):	8 GB	Gateway:	10.66.88.254	Public IP:	199.168.150.161

Applications

Aug 29, 2024 03:10 PM PDT - Aug 29, 2024 05:10 PM PDT

Salesforce Classic

78 out of 100

ZDX Score Over Time

☑ Smooth ZDX Score

□ ZDX Score

Figure 88. User detail

The following shows the data path end-to-end visibility the user takes to get to the Salesforce SaaS service. If there is any issue from the users' device health, the network at the home office, any service provider in the path, or with Zscaler or Salesforce, ZDX provides cloud visibility to the Zscaler administrators from any of their users' individual environments.

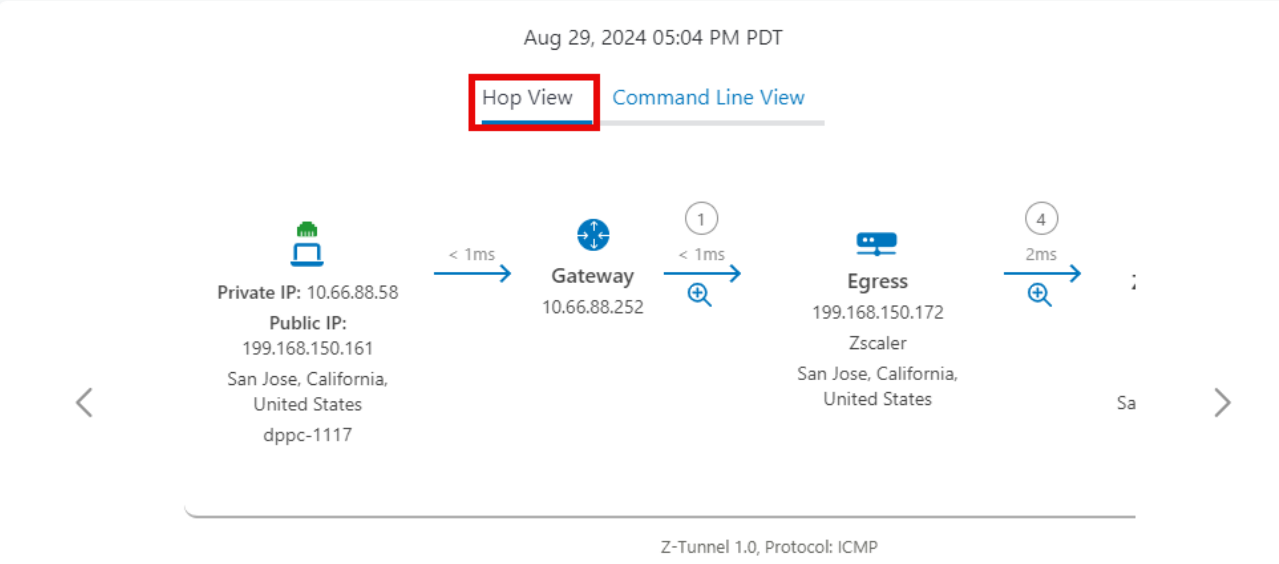
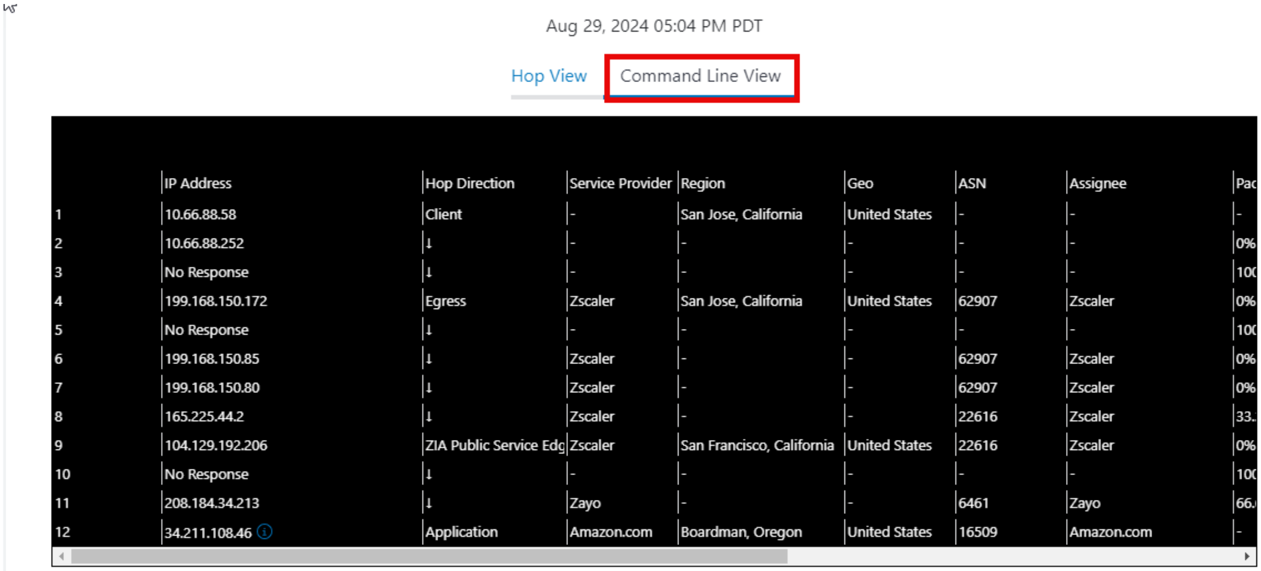


Figure 89. Hop view

You can also see a command line view.



	IP Address	Hop Direction	Service Provider	Region	Geo	ASN	Assignee	Pac
1	10.66.88.58	Client	-	San Jose, California	United States	-	-	-
2	10.66.88.252	↓	-	-	-	-	-	0%
3	No Response	↓	-	-	-	-	-	10(
4	199.168.150.172	Egress	Zscaler	San Jose, California	United States	62907	Zscaler	0%
5	No Response	↓	-	-	-	-	-	10(
6	199.168.150.85	↓	Zscaler	-	-	62907	Zscaler	0%
7	199.168.150.80	↓	Zscaler	-	-	62907	Zscaler	0%
8	165.225.44.2	↓	Zscaler	-	-	22616	Zscaler	33.
9	104.129.192.206	ZIA Public Service Edg	Zscaler	San Francisco, California	United States	22616	Zscaler	0%
10	No Response	↓	-	-	-	-	-	10(
11	208.184.34.213	↓	Zayo	-	-	6461	Zayo	66.
12	34.211.108.46 ⓘ	Application	Amazon.com	Boardman, Oregon	United States	16509	Amazon.com	-

Figure 90. User detail: end-to-end connection detail

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

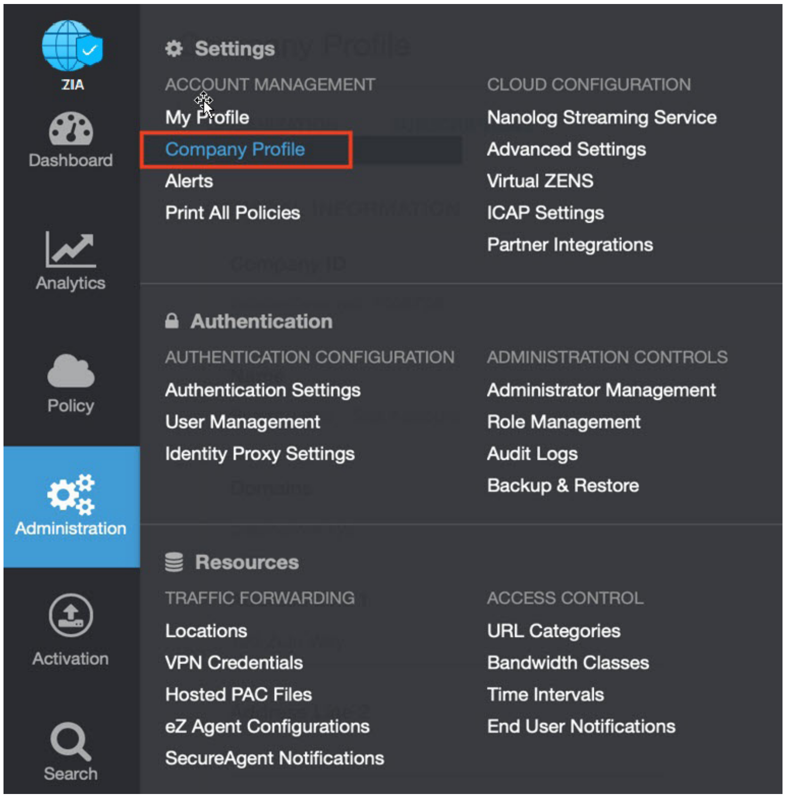
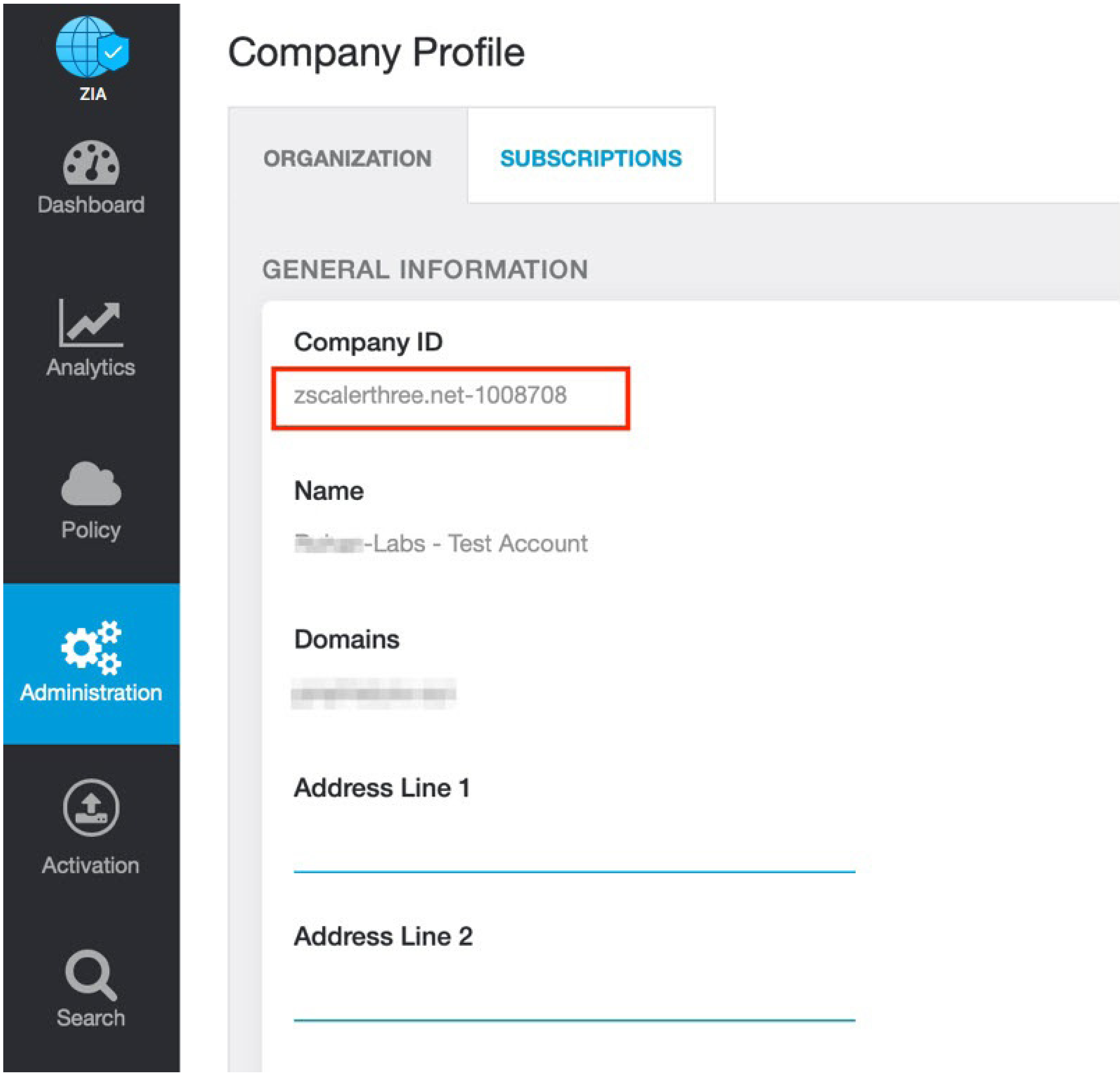


Figure 91. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 92. Company ID

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

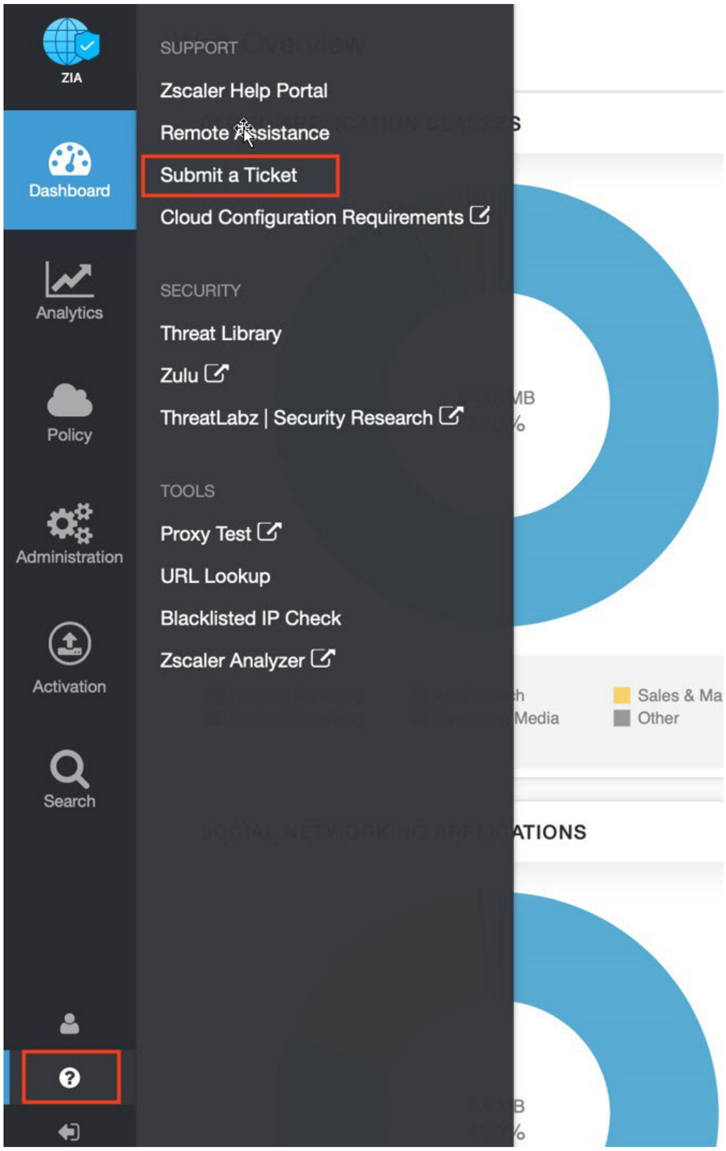


Figure 93. Submit a ticket