Contents

Terms and Acronyms 5

About This Document 6
   Zscaler Overview 6
      Zscaler Internet Access (ZIA) Overview 6
      Zscaler Digital Experience (ZDX) 6
      Zscaler Resources 7
   Salesforce Overview 8
      Salesforce CRM Overview 8
      Salesforce Resources 8
   Audience 8
   Software Versions 9

Zscaler Data Protection and Digital Experience for Salesforce.com 10
   ZIA SaaS Identity Proxy 11
   ZIA CASB Data and Malware Protection for Salesforce 12
   ZIA SaaS Security Posture Report 13
   ZIA Cloud Application Control 14
   ZDX for the Salesforce User Experience 15

SaaS Identity Proxy 16
   Configure the SaaS Identity Proxy 17
      Configure the SaaS Identity Proxy 18
   The Completed ZIA Salesforce Identity Proxy 20
   Configure the Salesforce Tenant 21
   Salesforce Tenant SAML Settings 22
   Salesforce Tenant Authentication Configuration 23
   Salesforce Tenant Authentication Settings 24
   Locate and Copy the ACS URL 25
      Salesforce Tenant Single Sign-On Settings 26
Completing the Zscaler SaaS Identity Proxy Settings 27
The New Identity and Notification Screens 29

Configuring Zscaler SaaS Security for Salesforce 30
Configuring the Zscaler and the Salesforce Tenant 31
Configuring the Zscaler Tenant on Salesforce 35
  Setup Permission Sets 38
  Create Permission Sets for the Admin Account 39
  Assign the Permission Set 42
Configuring the Zscaler Salesforce Connector 44
Configuring the Zscaler Tenant on Salesforce 45
Finish the Zscaler Side Tenant 49

The Active Salesforce SaaS API Tenant 50

Configuring Salesforce Policies and Scan Configuration 51
  Scoping the Policies and Remediation 52
Creating a DLP Policy 53
Creating a DLP Engine 54
Configure a SaaS DLP Policy 56
SaaS DLP Policy Details 57
  Configure SaaS DLP Policy Details 58
Configure a SaaS Malware Policy 59
SaaS Malware Policy Wizard 60
  SaaS Malware Policy 61

Configure the Scan Schedule Configuration 62
  Start the Scan Schedule 63

Reporting and Visibility 64
  SaaS Assets and SaaS Assets Summary Report 65
  SaaS Security Insights 66

SaaS Security Posture 67
  SaaS Security Posture Policies 68
SaaS Security Posture Report 69
SaaS Security Posture Policies Remediation 70

Cloud App Control 71
Cloud Application Access Control Policy 72
Cloud Application Access Control Policy Wizard 73
Cloud Application Access Control: Deny Policy 74
Cloud Application Access Control 75
Cloud Application Access Control Logs 76

Zscaler Digital Exchange (ZDX) for Salesforce 77
Configure ZDX for Salesforce 78
Configure ZDX for Salesforce 79
Configure Probes for Salesforce Monitoring 80
Configure Probes for Salesforce Monitoring 81
The Enabled Salesforce Application 83
Create an Alert for the Salesforce Service 84
The Triggered Alert for the Salesforce Service 90
Alert Detail for the Salesforce Service 91
The Sent Alert Email for the Salesforce Service 92

Using ZDX: The Dashboard 93
Application Overview 94
Application Detail 95
User Overview 97
User Detail 98

Appendix A: Requesting Zscaler Support 100
Gather Support Information 100
Save Company ID 101
Enter Support Section 102
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
</tr>
<tr>
<td>SaaS Security API</td>
<td>Zscaler CASB Service called SaaS Security API</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>ZDX</td>
<td>Zscaler Digital Exchange (Zscaler)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
</tbody>
</table>
About This Document

Below 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. For more information on Zscaler, visit www.zscaler.com or follow Zscaler on Twitter @zscaler.

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—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 our lightweight Zscaler Client Connector or PAC file (for mobile employees)

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

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

Zscaler Digital Experience (ZDX)

Zscaler Digital Experience (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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>About SaaS Application Tenant</td>
<td>Help article on Zscaler SaaS Security API, which provides visibility and security for sanctioned SaaS applications used in your organization.</td>
</tr>
<tr>
<td>Adding SaaS Application Tenant</td>
<td>Help article on adding a SaaS application tenant.</td>
</tr>
<tr>
<td>About Data Loss Prevention</td>
<td>Help article on Data Loss Prevention.</td>
</tr>
<tr>
<td>SaaS Security API DLP Policy</td>
<td>Help article on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications</td>
</tr>
<tr>
<td>About DLP Dictionaries</td>
<td>Help article on DLP dictionaries, which contain a set of patented algorithms that are designed to detect specific kinds of information in your users' traffic.</td>
</tr>
<tr>
<td>About DLP Engines</td>
<td>Help article on adding a custom DLP engine when configuring DLP policy rules.</td>
</tr>
<tr>
<td>SaaS Security Insights</td>
<td>Help article on viewing and defining information that you want to view when analyzing files scanned through charts.</td>
</tr>
<tr>
<td>SaaS Posture Security</td>
<td>Help article on configuring the number of recommended security policies that the report includes in its analysis of your organization's security posture.</td>
</tr>
<tr>
<td>Cloud Application Access Control</td>
<td>Help article on creating rules to control how your users access specific cloud applications.</td>
</tr>
<tr>
<td>SaaS Identity Proxy</td>
<td>Help article on configure Zscaler as an Identity Provider (IdP) for the cloud apps.</td>
</tr>
<tr>
<td>ZDX</td>
<td>Help articles on Zscaler Digital Experience (ZDX).</td>
</tr>
<tr>
<td>ZDX Predefined Applications</td>
<td>Help articles on which predefined applications are available in the ZDX Admin Portal when you log in.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
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. For more information on Salesforce, Inc., visit http://www.Salesforce.com or follow them on Twitter @Salesforce.

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, and social media data—and more—across multiple sources and channels. Their 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.

Their 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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salesforce Developer Account</td>
<td>Sign up for a Salesforce Developer Edition.</td>
</tr>
<tr>
<td>Salesforce Help</td>
<td>Salesforce help portal. Log in to create a case, view open cases, check your success plan details, view help documentation, etc.</td>
</tr>
<tr>
<td>Salesforce Community</td>
<td>Connect with fellow Trailblazers. Ask and answer questions to build your skills and network.</td>
</tr>
</tbody>
</table>

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

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

This document was authored using Zscaler Internet Access v6.0 and Salesforce Production Release dated Feb 11, 2021. A Salesforce developer account was used to created and verify the features enabled and used as examples.

Go to the following link to create a Salesforce developer account:

https://developer.salesforce.com/signup?d=70130000000td6N

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Contact us at 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 Data Protection and Digital Experience for Salesforce.com

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 they enable 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 our Zscaler Internet Services (ZIA) for Salesforce security and Zscaler Digital Experience (ZDX) for visibility into the user experience.

ZIA secures Salesforce SaaS through cloud-based access control, identity control, SaaS security posture management, and our 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 the 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.

Figure 1. Zscaler solution for Salesforce
Both ZIA SaaS security and ZDX SaaS monitoring operate as separate stand-alone 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 our 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
- ZIA CASB 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 Salesforce tenant.

![Identity proxy](image)

When users try to access Salesforce with their corporate accounts without using the Zscaler service, a dialog asking them to login via Zscaler displays. The process is controlled using SAML, the IDP that is defined on Zscaler for the ZIA service, and the Salesforce SSO configuration to forward auth requests to Zscaler.
ZIA CASB Data and Malware Protection for Salesforce

The Zscaler CASB (SaaS Security API) is a feature set that is part of the ZIA security cloud and is designed specifically to help manage the risks of our file collaboration SaaS partners, preventing data exposure and ensure compliance across the SaaS application.

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 our SaaS Security 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 to, and Zscaler Cloud Protection. Zscaler provides end to end connectivity, security, and visibility from any location on-prem or remote.

For more information, see the resources in Zscaler Resources.
ZIA SaaS Security Posture Report

Once the Salesforce tenant has been 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. All settings are enabled by default, but individual checks can be disabled 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 can be filtered by best practice recommendations, PCI compliance, or FFIEC compliance.

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 hours 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 in-line between users and the Internet. It inspects all traffic, including SSL, flowing between them. As part of the platform, Zscaler Cloud Application Visibility & 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 referred to as out-of-band CASB for data-at-rest, Zscaler Cloud Application Control is referred to as inline CASB.

Cloud App Control provides SaaS application intelligence to consolidate all associated URL’s 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 now easily 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.

![Zscaler Digital Exchange User Experience Monitoring](image)

**Figure 6. ZIA cloud SaaS security API in use with Salesforce**

What makes ZDX unique?

- **End-user device performance.** Continuously gathers and analyzes data on end-user device 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 the resources in 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.

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

The traffic flow that we will configure in the next steps is documented below:

- 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 auth cookie)
- Salesforce redirects to the Zscaler Service Edge to confirm identity
- The Zscaler 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 below for both tenants. The easiest way to configure the solution is to open two browsers or browser tabs and switch back and forth between the two tenants as required.

To begin the configuration log into the Zscaler tenant with admin credentials.
Configure the SaaS Identity Proxy

To start configuring Zscaler to act as an Identity Proxy for Salesforce execute the following procedure.

1. Select Administration > Identity Proxy Settings > Add Cloud Application

![Identity Proxy Settings]

Figure 9. Configure the identity proxy
2. This launches the Add Cloud Application wizard. To start configuring Zscaler to act as an Identity Proxy, Name the cloud application an intuitive name (like “Salesforce”).

3. Select Salesforce in the Cloud Application field.

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. Select Save to finish the configuration for now.

Figure 10. The Identity Proxy wizard
The Completed ZIA Salesforce Identity Proxy

To complete the identity proxy for Salesforce, we need to add the ACS URL that is created on the Salesforce tenant. The highlighted URLs need to be copied and saved for the Salesforce configuration. The certificate also needs to be downloaded and saved.

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. Download and save the **Certificate**.
4. Open the Salesforce tenant.

![Identity Proxy Settings](image)

Figure 11. The completed ZIA Salesforce identity proxy
Configure the Salesforce Tenant

To configure the Salesforce tenant for identity proxy, follow the below procedures:

1. Select **Setup**.
2. Select **Identity**.
3. Select **Single Sign-On Settings**.
4. Select **Edit**.
5. In the **Single Sign-On Settings** window, select **SAML Enable**.
6. In the **Single Sign-On Settings** window, select **Save**.
7. Select the **New** button next to the **SAML Sign-On Settings**.

![Configure the Salesforce tenant](image)
Salesforce Tenant SAML Settings

To configure the Salesforce tenant for identity proxy, follow the below procedures:

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 downloaded in the previous step.
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**.

![Figure 13. Configure the Salesforce tenant SAML settings](image-url)
Salesforce Tenant Authentication Configuration

To configure the Salesforce authentications settings, follow the below procedures in the Salesforce Admin Portal:

1. Select Setup.
2. Select Settings.
4. Select Edit next to Authentication Configuration.

This opens the Authentication Configuration dialog.
Salesforce Tenant Authentication Settings

To configure the Salesforce authentications settings, follow the below procedures in the Authentication Configuration dialog:

1. Unselect Login Form.
2. Select Zscaler.
3. Click Save.

![Authentication Configuration](image)

Figure 15. Configure the Salesforce tenant authentication configuration
Locate and Copy the ACS URL

The Configuration has now been completed but we need to copy the ACS URL that was missing in the Zscaler setup. Follow the below to find and copy the URL:

1. Select Setup.
2. Select Identity.
4. Select the Zscaler settings we created by clicking the name Zscaler.

![Figure 16. Copy the ACS URL from the single sign-on settings](image-url)
Salesforce Tenant Single Sign-On Settings

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

Figure 17. Copy the login URL
Completing the Zscaler SaaS Identity Proxy Settings

Navigate back into our Zscaler configuration to complete the SaaS identity proxy.

1. Sign into your ZIA Admin Portal with admin credentials.
2. Select **Administration > Identity Proxy Settings**.
3. Select the **Blue Pencil**.

![Identity Proxy Settings](image)

Figure 18. Finish the ZIA SaaS identity proxy configuration (1 of 2)
4. This opens the **Edit Cloud Application** window. Paste the **Login URL** copied from Salesforce into the **ACS URL Field**.
5. Click **Save**.

![Edit Cloud Application window](image)

*Figure 19. Finish the ZIA SaaS identity proxy configuration (1 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 login to Salesforce without first logging into Zscaler, a dialog displays and asks them to login via Zscaler.

![Figure 20. The new IdP and notification screens](image-url)

©2022 Zscaler, Inc. All rights reserved.
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 steps are listed below for both tenants. Log into the Zscaler tenant to start the configuration process:

1. Configure the Salesforce SaaS tenant in Zscaler.
2. Configure the Zscaler tenant in Salesforce.
   a. Install the Zscaler package.
   b. Create a permission set.
   c. Assign the permission set.
3. Configure the Zscaler SaaS connector application.
4. Configure a SaaS DLP policy in Zscaler.
5. Configure a SaaS malware policy in Zscaler.
6. Configure and start the scan policy for the SaaS service in Zscaler.

Figure 21. Creating the Salesforce tenant
Configure the Salesforce SaaS tenant under Administration in the ZIA Admin Portal.

1. Select **Administration > SaaS Application Tenant**.

---

**Figure 22. Adding a Salesforce tenant**
2. Select **Add SaaS Application Tenant**.

Figure 23. Adding an application tenant
3. Select the **Salesforce** tile under popular applications to move to the next step in the wizard.

![Figure 24. The SaaS Tenant Configuration wizard](image-url)
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. Copy the **Zscaler SaaS Connector** number for next steps.

6. Select the **Go to Salesforce Settings** to bring up your Salesforce portal.

![Figure 25. Open the Salesforce tenant](image)
Configuring the Zscaler Tenant on Salesforce

To configure the Zscaler Tenant from your Salesforce admin account:

1. Log in to Salesforce with admin credentials.

   ![Login to the Salesforce tenant](image)

2. To authorize the custom App that is the Zscaler tenant, select **Install for Admins Only**.
3. Acknowledge the AppExchange Warning (This should be temporary).
4. Select **Install**.
5. Select Done when the installation is complete. You are redirected to the Installed Packages page.

![Install Zscaler SaaS Connector ZSThree 01](image)

**Figure 27. Install the SaaS Connector**
6. We must now create and assign permission to the user (admin) of the Zscaler application. Select **Users** from the left pane.

7. Select **Permission Sets**.

![Users page in Salesforce](image)

Figure 28. The installed Zscaler SaaS connector
Setup Permission Sets

Next, you need to set up the permission sets. On the Permission Sets window, click New.

Figure 29. Creating permission sets
Create Permission Sets for the Admin Account

In the Create Permission Set wizard:

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

![Permission Set Create](image)

Figure 30. Creating permission sets
4. In the Apps section, select App Permissions.

![Figure 31. App permissions](image1)

5. Click Edit.

![Figure 32. Editing app permissions](image2)
6. Under the **Content** section, select **Manage record types and layouts for Files**.
7. Select **Manage Salesforce CRM Content**.
8. Select **Query All Files**.
9. **Save** the additional permissions.
10. Click **Save**.
11. Click **Save** again on the pop-up.

![Figure 33. Enable and save app permissions](image-url)
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**.
2. Select **Users**.
3. Select the **Name** to assign permissions (do not select **Edit**).
4. On the next screen click **Permission Set Assignments**.
5. Edit **Assignments**.

Figure 34. Assign the permission sets to the administrator
6. On the **Setup** screen for permission sets, select the permission set that you created.
7. Select **Add** to add it to the **Enabled Permission Sets**.
8. Click **Save**.

![Figure 35. Adding the permission set to the admin](image)
Configuring the Zscaler Salesforce Connector

We now need to configure the application connector. In Setup under Platform Tools:

1. Select Apps.
2. Select App Manager.
3. Find the Zscaler SaaS connector you created and select the down arrow on the right.
4. Select Manage.

The suffix on the application connector changes based on your Zscaler cloud name. In the above 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. Select Edit Policies.

![Figure 37. Editing policies](image-url)
2. On the **App Connector** screen under **OAuth Policies** select **Admin approved users are pre-authorized** for the **Permitted Users** field.

3. Select **Relax IP restrictions** for the **IP Relaxation** setting.

4. Click **Save**.

![Figure 38. Relax IP restrictions](image-url)
5. Further down the page of the App Connector screen we need to edit the Profiles and Permission Sets select Manage Profiles.


7. Click Save.

8. Click Manage Permission Sets.

Figure 39. Adding admin privileges to a user
9. Under **Application Permission Set Assignments** select **Zscaler SaaS Connector**.

10. Click **Save**.

11. We are now finished with the Salesforce tenant setup. We need to 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 Administrator Account used to create the Zscaler SaaS connector.
2. Click Save to finish the configuration.
3. Select Activate to activate our changes.
The Active Salesforce SaaS API Tenant

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

We are now ready to set up our scan schedule, our DLP policies, and our malware policies.

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.

![Zscaler policy configuration](image)

*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 scan the Salesforce account attachment files for matching DLP content and malware. We will touch more on malware in a later section.

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.

Our DLP policy will create 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. A true DLP policy review would need to be conducted 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. We will create a basic policy and apply it to our Salesforce tenant. If you already have DLP policies created skip ahead to Configure a SaaS Malware Policy.
Creating a DLP Policy

The procedures for creating a DLP policy are pretty 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 our violation and eliminate false positives.

Then create a SaaS security DLP policy that allows us to specify the detail about where and when action is taken, and whom to inform about violations. Finally, apply the DLP policy to our Salesforce tenant. Let’s verify our DLP dictionary as next steps. In the ZIA Admin Portal:

1. Select Administration > DLP Dictionaries and Engines > DLP Dictionaries.
2. Identify and select the dictionary to use (In this case SSN with Dashes).

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Trigger Threshold</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Resident Registration Numbers</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect leakage of Korean Resident Registration Numbers</td>
</tr>
<tr>
<td>24</td>
<td>Salesforce.com Data</td>
<td>Predefined</td>
<td>High</td>
<td>Detect leakage of Salesforce.com data</td>
</tr>
<tr>
<td>25</td>
<td>Social Insurance Numbers (CAN)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect leakage of Canadian Social Insurance Numbers</td>
</tr>
<tr>
<td>26</td>
<td>Social Security Number (Swiss)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect Leakage of Swiss Social Security Numbers</td>
</tr>
<tr>
<td>27</td>
<td>Social Security Numbers (US)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect leakage of United States Social Security Numbers</td>
</tr>
<tr>
<td>28</td>
<td>Source Code</td>
<td>Predefined</td>
<td>Low</td>
<td>Detect leakage of source code</td>
</tr>
<tr>
<td>29</td>
<td>SSN with Dashes</td>
<td>Patterns</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>30</td>
<td>Standardized Bank Code (Mex)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect leakage of Mexican Standardized Bank Code</td>
</tr>
<tr>
<td>31</td>
<td>Tax File Numbers (Australian)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect leakage of Australian Tax File Numbers</td>
</tr>
<tr>
<td>32</td>
<td>Tax Identification Number (Indonesian)</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect Leakage of Indonesian Tax Identification Numbers</td>
</tr>
<tr>
<td>33</td>
<td>Weapons</td>
<td>Predefined</td>
<td>Medium</td>
<td>Detect weapons content</td>
</tr>
</tbody>
</table>

Figure 46. Creating a DLP dictionary
Creating a DLP Engine

To create the DLP engine:

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

![DLP Dictionaries & Engines]

Figure 47. Creating a DLP engine
3. Give the DLP Engine a Name.

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 our next dictionary and repeat the process.

7. Click Save.

8. Activate the configuration.

This policy triggers when we see the 11th Social Security Number. Again, this in a demonstration and the criteria is too general to be a production DLP rule.
**Configure a SaaS DLP Policy**

To Launch the DLP Rule wizard:

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

![Figure 49. The SaaS DLP Policy Configuration wizard](image-url)
SaaS DLP Policy Details

The SaaS DLP policy is like all Zscaler policies 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 we have 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 below for clarification. For our policy example, we will select Any Collaboration, and an Action of Remove Sharing.

- **Collaboration Scope**: The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select 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 Only. This means that any violations will be reported in the Zcaler SaaS Analytics and alerts will be 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 our DLP policy:

1. Specify the Rule Order for processing (the first rule matched is executed).
2. Name the Rule.
3. Enable the Rule.
4. Select the Salesforce SaaS tenant.
5. Select the DLP engine created in the last step.
7. Select High as a Severity to allow for identification for searches and tracking.
8. Save and Activate your configuration.

Figure 50. The SaaS DLP Policy Configuration wizard
Configure a SaaS Malware Policy

To launch the DLP Rule wizard.

1. Select **Policy > SaaS Security API > Malware Detection.**
2. Select **CRM.**
3. Select **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 in the **Exemption** tab under **Malware Detection.**

To add a malware policy:

4. Specify the **Application.**
5. Specify the **SaaS Application Tenant.**
6. Enable the **Status.**
7. The **Action** for Salesforce is limited to Report Malware only.

![Figure 51. The Malware Policy Configuration wizard](image-url)
SaaS Malware Policy Wizard

Configure the Malware Rule wizard.

2. Select CRM.
3. Select Add Malware Detection Rule.
4. Under Criteria select Salesforce as the Application.
5. Select the Salesforce as the SaaS Application Tenant to apply the policy.
7. Click Save.

![Edit Malware Detection Rule](image)

Figure 52. The Malware Policy Configuration wizard
**SaaS Malware Policy**

The completed SaaS security malware policy for the Salesforce SaaS tenant. **Activate** your configuration.

---

**Figure 53. The completed Malware Policy Configuration wizard**
Configure the Scan Schedule Configuration

The final configuration step is to create a scan configuration. We will 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. For this deployment Guide we will 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. Select 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.

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

Once the schedule has been configured and saved, we need to start the scan for our DLP and malware policies to be applied:

1. Activate the configuration changes.
2. Select the Blue Arrow on the Scan configuration to start SaaS API security on the Salesforce tenant.
3. The Status should say Active with a Start Date and a Latest Scan Date.

![Figure 55. Starting the scan](image-url)
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 our 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.

We will take a brief look at the tools, but for detailed information of the SaaS Security Analytics tools visit the Zscaler online documentation.

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 below is the SaaS assets summary report, which provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen. Our Salesforce activity over the creation of this deployment guide is shown above, but any configured tenant is also be displayed on this summary screen. The data is hyperlinked, and you can easily pivot from a summary to individual logs and activities provided by SaaS security insights.

Select the 20 Total Incidents next to Salesforce to pivot to SaaS Security Insights.

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

![Summary reports](image-url)
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 datapoints 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

Figure 58. SaaS security insight
SaaS Security Posture

Once the Salesforce Tenant has been 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. All settings are enabled by default, but individual checks can be disabled on the SaaS Security Posture Policy page, allowing organizations to customize the report to their individual needs. The results of the posture policy checks are then displayed on the SaaS Policy Report page, and can be filtered by Best Practice Recommendations, PCI Compliance, or FFIEC Compliance.

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 Hours 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
**SaaS Security Posture Policies**

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

1. Sign into your organizations ZIA Admin Portal with admin credentials.
2. Select **Policy > SaaS Security Posture Policy**.
3. Enable or Disable individual policies.
4. Save and Activate policy changes.

![SaaS Security Posture Policy](image)

*Figure 60. SaaS security posture policies*
SaaS Security Posture Report

To check the result of the configured SaaS Posture Policies against our Salesforce Tenant we need to check the SaaS Posture Report in Analytics.

1. Sign into your organizations ZIA Admin Portal with admin credentials.
2. Select Analytics.
3. For the Tenant select Salesforce.
4. For the 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.

![SaaS Security Posture Report](image)

**Figure 61. 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. Select **Remediate Now** to be open the Salesforce documentation that walks through the steps to make the change.

<table>
<thead>
<tr>
<th>Description</th>
<th>Remediation Change</th>
<th>Remediation Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Remediate Now</td>
</tr>
</tbody>
</table>

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 62. SaaS security posture remediation steps*
Cloud App Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits in line between users and the internet, inspecting all traffic (including SSL) flowing between them. As part of the platform, Zscaler Cloud Application Visibility & 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 referred to as out-of-band CASB for data-at-rest, Zscaler cloud application security is referred to as inline CASB.

Cloud App Control has SaaS application intelligence that consolidates all associated URL's and application functions in a single security setting. This allows you to control specific user, groups, locations, or departments, and only allow the required users to the application.

Let's define a Cloud Application Control policy to allow only users in a Salesforce security group to access Salesforce and block access for all other users. This requires two policies: one policy to allow our specific users and one to block all other users.
Cloud Application Access Control Policy

To create our policy to allow our specific users please follow the below steps.

1. Sign into your organizations ZIA Admin Portal with admin credentials.
2. Select Policy > URL & Cloud App Control.
3. Select the Cloud App Control Policy tab.
4. Select Add.
5. Select Productivity & CRM Tools.

This launches the Policy wizard.
Cloud Application Access Control Policy Wizard

To create our policy to allow our specific users:

1. Set the **Rule Order** to 1.
2. Set the **Rule Name** to an intuitive name.
3. Select **Salesforce** for the **Cloud Application**.
4. Select the **Security Group** that contains our Salesforce admins and users.
5. Select **Allow** for **Application Access**.
6. Click **Save** to save our changes.

![Cloud Application Access Control Policy Wizard](image)

**Figure 65. Create a Cloud App Control allow policy**
Cloud Application Access Control: Deny Policy

To create our policy to deny all other users:

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

![Add Productivity and CRM Tools Rule](image)

Figure 66. Create a Cloud App Control deny policy
Cloud Application Access Control

To finish the completed access policies, **Activate** the policy additions.

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

![Figure 67. Create a Cloud App Control deny policy](image)
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 timeframe, follow the below steps:

1. Sign into your organizations ZIA Admin Portal with admin credentials.
2. Select Analytics > Web Insights.
3. Select the Logs tab.
4. Select the desired time frame, or a custom time frame.
5. Select Add Filter.
7. Select Salesforce.
8. Apply filters.

Figure 68. Create a Cloud App Control logs
Zscaler Digital Exchange (ZDX) for Salesforce

ZDX is the missing link needed for our 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 the 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.

![Zscaler Digital Exchange](image)

Figure 69. 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 into the ZDX Admin Portal with admin credentials to begin the configuration process.

*Figure 70. ZDX for user experience monitoring for Salesforce*
Configure ZDX for Salesforce

Salesforce is a predefined application in ZDX, and configuration is very simple. To configure the Salesforce application for monitoring:

1. Select Configuration > Applications.
2. Select the blue arrow next to the Salesforce app.
3. Click Go to onboard Salesforce.

![Onboard Salesforce](image)

Figure 71. Onboard the Salesforce app
Configure Probes for Salesforce Monitoring

Clicking the Go button enables monitoring for the Salesforce app. The pre-configured probes are displayed. The probes consist of a network probe that uses an ICMP Trace Route, and a web page probe to the account.Salesforce.com location that monitor page load times.

We are going to make one change to the network probe to have it follow the path of the webpage probe so there is no confusion of the results since this is entirely for Salesforce monitoring.

To edit the rule:

1. **Activate** the changes.
2. Select the blue pencil to edit the probe.

![Figure 72: ZDX for user experience monitoring for Salesforce](image-url)
Configure Probes for Salesforce Monitoring

To configure the probe to monitor Salesforce:

1. Select Salesforce Account Login Page Probe under Follow Web Probe.
2. Click Next.
3. Validate the **Cloud Path Host** destination is account.Salesforce.com.
4. Click **Next**.

![Edit Salesforce CloudPath Probe](image)

**Probes**

- **Probes**
- **Application Name**
- **Protocol**
- **Packet Count**
- **Interval (ms)**
- **Timeout (ms)**
- **SHA256**

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 our users using the Zscaler Client Connector. The figure shows the Zscaler Client Connector running the digital experience with the service On.

![Figure 75. Active Salesforce monitoring](image)

<table>
<thead>
<tr>
<th>Application</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box</td>
<td>Disabled</td>
</tr>
<tr>
<td>Microsoft Teams</td>
<td>Disabled</td>
</tr>
<tr>
<td>OneDrive for Business</td>
<td>Disabled</td>
</tr>
<tr>
<td>Outlook Online</td>
<td>Disabled</td>
</tr>
<tr>
<td>Salesforce</td>
<td>Enabled</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Disabled</td>
</tr>
<tr>
<td>SharePoint Online</td>
<td>Disabled</td>
</tr>
<tr>
<td>Zoom</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Create an Alert for the Salesforce Service

As a final configuration step let’s create an email alert when there is service degradation of the Salesforce application. An alert can be configured for network, application, or device thresholds. Alerts can be created with any of the below information:

- **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, WIFI Signal Strength, Memory, Sent and Received Mbps

To create our alert on Page Fetch Times:

1. Select **Alerts > Rules**.
2. Select **Add New Alert Rule**.

![Figure 76. Creating an alert](image)
Step one of the rule wizard:

1. **Name** the rule.
2. Select **Enable** under **Status**.
3. Give the alert an appropriate **Severity**.
4. Select a **Type** of application.
5. Click **Next**.

![Add New Alert Rule](image)

*Figure 77. The Alert Creation wizard*
Step two of the rule wizard:

1. Select **Salesforce** as the **Application**.
2. Select **Salesforce Account Login Page Probe** for the **Web Probe**.
3. Click **Next**.

![Add New Alert Rule](image)

*Figure 78. The Alert Creation wizard*
Step three of the rule wizard creates the criteria and threshold that triggers the alert. We can use multiple variables here to eliminate false positive:

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

![Figure 79. The Alert Creation wizard](image-url)
Step four of the rule wizard adds throttling to control the scope of the alert. We 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 our threshold.
2. Select **10 Percent** for the **Minimum Number of Devices** that must be impacted.
3. Select **Email** as the **Delivery Method**.
4. Enter the **Alert Recipients** email address separated by commas.

![Figure 80. The Alert Creation wizard](image)
The Alerts > Rules tab shows the completed rule set for the alert.

Figure 81: The completed rule set
The Triggered Alert for the Salesforce Service

A triggered alert generated by our rule set threshold settings is shown in the Alerts > Rules tab. You can click on the Rule Name or click the eye to see more detail about the alert.

Figure 82. The alert
Alert Detail for the Salesforce Service

The above is the triggered alert detail for our triggered alert showing impacted user and devices, impact location, and threshold details.

Figure 83. Alert details
The Sent Alert Email for the Salesforce Service

Below is the email sent to the recipients once 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.

![Email Alert](image)

**Figure 84. 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 may be having issues.

Figure 85. The dashboard
Application Overview

Selecting the Applications tile on the left of the ZDX Admin Portal displays the Applications Overview and shows all the configured applications in individual ZDX scores. Let’s take a look at the detail of our Salesforce application.

1. Select Applications.
2. Select the Salesforce App.

Figure 86. Application overview
Application Detail

The top portion of the application detail shows a historical view of the ZDX score and the Page Fetch Time. The spike of the page fetch time indicates a possible slowdown of the Salesforce service itself.

Figure 87. Application detail
The bottom portion of the app detail show the **Top Locations**, **Top Cities**, and **Top Departments** using the application and the ZDX scores at a glance. We also see our probe data, with minimum, maximum, and average response times.

![Application detail](image)

**TOP DEPARTMENTS**

<table>
<thead>
<tr>
<th>ZDX Score per Department</th>
<th>Top Departments</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Biz Dev</td>
</tr>
</tbody>
</table>

**TOP CITIES**

<table>
<thead>
<tr>
<th>ZDX Score per City</th>
<th>Top Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Spring, TX, US</td>
</tr>
</tbody>
</table>

**TOP ZSCALER LOCATIONS**

<table>
<thead>
<tr>
<th>ZDX Score per Zscaler Location</th>
<th>Top Zscaler Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Road Warrior</td>
</tr>
</tbody>
</table>

**Probe Status**

- **Salesforce CloudPath Probe**: Cloud Path
  - Total Number of Hops: Min: 12 Avg: 12 Max: 13
  - Total Latency: Min: 41 Avg: 43 Max: 45
  - Packet Loss: Min: 0 Avg: 0 Max: 0
  - Packet Count: Min: 11 Avg: 11 Max: 11

- **Salesforce Login Page Probe**: Web
  - Page Fetch Time: Min: 221 Avg: 557 Max: 1652 ms
  - Server Response Time: Min: 200 Avg: 536 Max: 1520 ms
  - DNS: Min: 3 Avg: 21 Max: 28
  - Availability: Min: 10 Avg: 10 Max: 10
User Overview

The User Overview provides all of the users of an application. Select Salesforce and then Apply to see all of our Salesforce users. The ZDX score is provided, and users can be selected by Poor, Okay, or a Good ZDX scores. You can get more detail on the user by clicking the name or the eye on the right.

Select a User to bring up more detail.

Figure 89. User overview
User Detail

The user detail shows an incredible amount of useful data to help isolate any user experience issues.

Select and apply the Salesforce application to see the detail of the user experience for the Salesforce app. This report provides the users devices and the device specific detail (OS, Device type, Network Information, etc.) by clicking on the device. The ZDX score is also displayed in a timeline, and detail of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health can all be seen from this page.

![User Detail](image)

Figure 90. User detail
Below 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, with Zscaler or Salesforce, the ZDX provides cloud visibility to the Zscaler administrators from any of their users’ individual environments.

![Diagram](image)

**Figure 91.** Hop view

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hop Direction</th>
<th>Service Provider</th>
<th>Region</th>
<th>Geo</th>
<th>ASN</th>
<th>Assignee</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.254</td>
<td>Client</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10.1.1.1</td>
<td>Down</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>96.120.16.121</td>
<td>Egress</td>
<td>Comcast Cable</td>
<td>-</td>
<td>United States</td>
<td>922</td>
<td>Comcast Cable</td>
</tr>
<tr>
<td>96.110.157.49</td>
<td>Down</td>
<td>Comcast Cable</td>
<td>-</td>
<td>United States</td>
<td>922</td>
<td>Comcast Cable</td>
</tr>
<tr>
<td>68.86.87.197</td>
<td>Down</td>
<td>Comcast Cable</td>
<td>-</td>
<td>United States</td>
<td>922</td>
<td>Comcast Cable</td>
</tr>
<tr>
<td>96.110.34.82</td>
<td>Down</td>
<td>Comcast Cable</td>
<td>-</td>
<td>United States</td>
<td>922</td>
<td>Comcast Cable</td>
</tr>
<tr>
<td>96.87.11.66</td>
<td>Down</td>
<td>Comcast Business</td>
<td>Huntsville, Alabama</td>
<td>United States</td>
<td>922</td>
<td>Comcast Business</td>
</tr>
<tr>
<td>13.108.7.81</td>
<td>Down</td>
<td>Salesforce.com</td>
<td>-</td>
<td>United States</td>
<td>4340</td>
<td>Salesforce.com, Inc.</td>
</tr>
<tr>
<td>13.108.252.7</td>
<td>Down</td>
<td>Salesforce.com</td>
<td>-</td>
<td>United States</td>
<td>4340</td>
<td>Salesforce.com, Inc.</td>
</tr>
<tr>
<td>13.108.252.56</td>
<td>Down</td>
<td>Salesforce.com</td>
<td>-</td>
<td>United States</td>
<td>4340</td>
<td>Salesforce.com, Inc.</td>
</tr>
<tr>
<td>13.108.250.2</td>
<td>Down</td>
<td>Salesforce.com</td>
<td>-</td>
<td>United States</td>
<td>4340</td>
<td>Salesforce.com, Inc.</td>
</tr>
</tbody>
</table>

**Figure 92.** User detail: end-to-end connection detail
Appendix A: Requesting Zscaler Support

Gather Support Information
You might sometimes need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

To contact Zscaler support, select **Administration > Settings** and then click **Company profile**.

![Collecting details to open support case with Zscaler TAC](image-url)
Save Company ID

Copy the Company ID, as shown below.

Figure 94. Company ID
Enter Support Section

Now that you have our company ID, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

Figure 95. Submit ticket