ZSCALER AND SERVICENOW DEPLOYMENT GUIDE

DECEMBER 2022, VERSION 1.4

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

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

Acronym	Definition
CA	Central Authority (Zscaler)
CPU	Central Processing Unit
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
MTR	My Traceroute
PaaS	Platform as a Service
PFS	Perfect Forward Secrecy
POV	Proof of Value
PSK	Pre-Share 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)
ZCSPM	Zscaler Cloud Secure Posture Management (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the Zscaler and partner companies and software covered in this deployment guide.

Zscaler Overview

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

ServiceNow Overview

ServiceNow, Inc. (NYSE: NOW) is an American software company based in Santa Clara, California that develops a cloud computing platform to help companies manage digital workflows for enterprise operations. ServiceNow is a Platform as a Service (PaaS) provider, providing technical management support, such as IT service management, to the IT operations of large corporations, including providing help desk functionality. The company's core business revolves around management of "incident, problem, and change" IT operational events. ServiceNow was founded in 2004.

To learn more, refer to ServiceNow's website or follow them on Twitter @servicenow.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems.

Software Versions

This document was authored using ZIA ServiceNow production releases. A ServiceNow developer account was created to verify the features were enabled and used as examples.

Create a ServiceNow Developer Account.

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 ServiceNow Introduction

The following are overviews of the Zscaler and ServiceNow applications described in this deployment guide.

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, please 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 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 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 Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

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

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

Zscaler Resources

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

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

Name and Link	Description
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.
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.

ServiceNow Platform

ServiceNow bridges the gap between IT, business objectives, employees, customers, and data—automating complex workflows, enhancing experiences, and driving operational excellence throughout entire processes.

With a comprehensive set of products and solutions tailored to meet the needs of organizations across a wide range of industries, ServiceNow is the ideal choice for any company interested in improving its operations to drive growth and reduce costs. Because after all, IT is central to modern business; give it the support, direction, and power it needs to take your business further, with ServiceNow.

ServiceNow Resources

The following table contains links to ServiceNow support resources.

Name and Link	Description
About ServiceNow	ServiceNow company description.
ServiceNow Developer Program	Website for creating a ServiceNow developer account.
ServiceNow Product Documentation	Online documentation for the ServiceNow platform.
ServiceNow Community	ServiceNow online community portal.
ServiceNow Support	Online support for the ServiceNow platform.

Zscaler Data Protection and Digital Experience for ServiceNow.com

ServiceNow is one of the industry leaders that defined the utility of the cloud, including the advantages a SaaS application and the cloud itself can provide to an enterprise. SaaS services are popular because of the collaboration, ease of use, and ease of sharing they enable globally. ServiceNow.com is still one of the industry leaders. The downside of this ease of access and sharing is that they can present risk based on the client's environment. It is impossible to train every employee to always use safety best practices with SaaS applications, and that can lead 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 business tools.

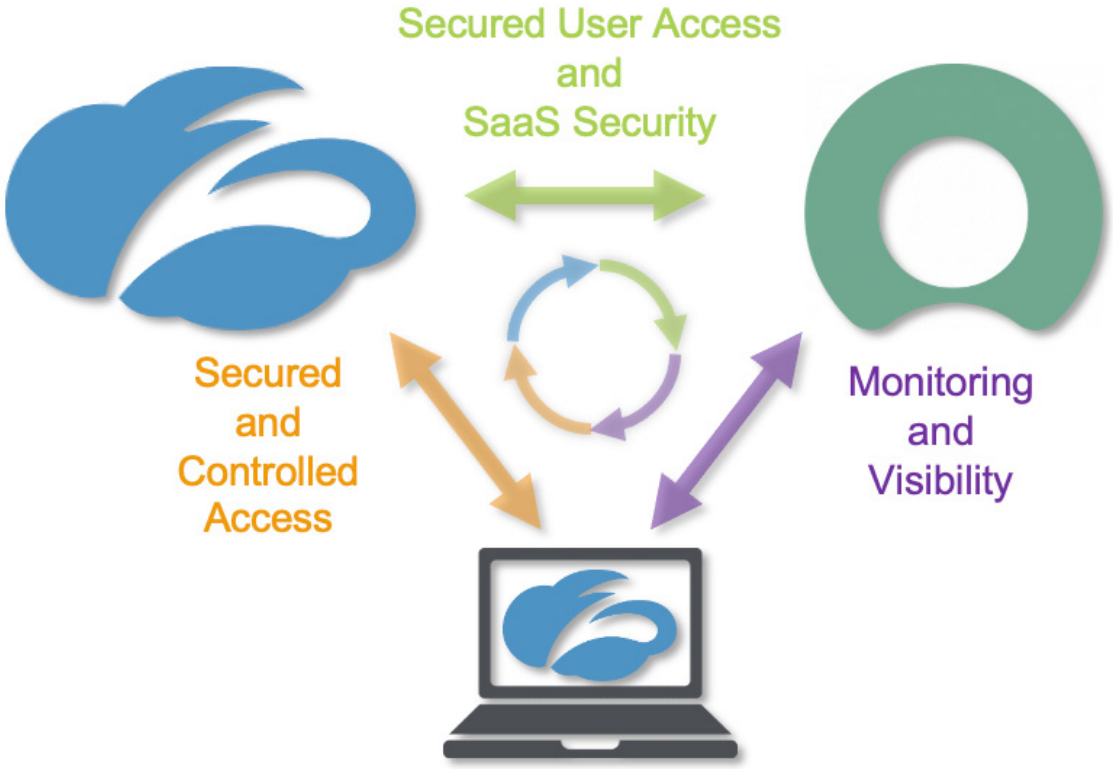


Figure 1. Zscaler solutions for ServiceNow

Another challenge faced by organizations migrating to cloud services in today's environment has been monitoring the user experience for the SaaS application. Especially in today's work from anywhere corporate infrastructures. Zscaler provides a complete ServiceNow solution using ZIA for security of ServiceNow and Zscaler Digital Experience (ZDX) for user experience.

ZIA provides ServiceNow SaaS security by using access control, identity control, Zscaler Cloud Secure Posture Management (ZCSPM), and SaaS Security API to scan the ServiceNow attachments for malicious content and 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 ServiceNow service to help organizations address any user experience concerns or challenges. ZDX has preconfigured monitors for ServiceNow that provide performance monitoring and measurements from the users' device running the Zscaler Client Connector. These monitors provide detailed information on the user's device, the network path to ServiceNow, and the ServiceNow SaaS performance itself. This information is invaluable to operations when a user is experiencing issues with ServiceNow and provides visibility to every corner of the internet.

Both ZIA SaaS Security and ZDX 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 ServiceNow's SaaS CRM service.

This guide covers the following ZIA features for ServiceNow security, and the ZDX for ServiceNow performance visibility.

- SaaS Identity Proxy
- Cloud Browser Isolation
- SaaS Security Data Loss Protection and Malware Detection
- Cloud Application Access Control
- ZDX for ServiceNow
- ZCSPM ServiceNow Incident Creation

ZIA SaaS Identity Proxy

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

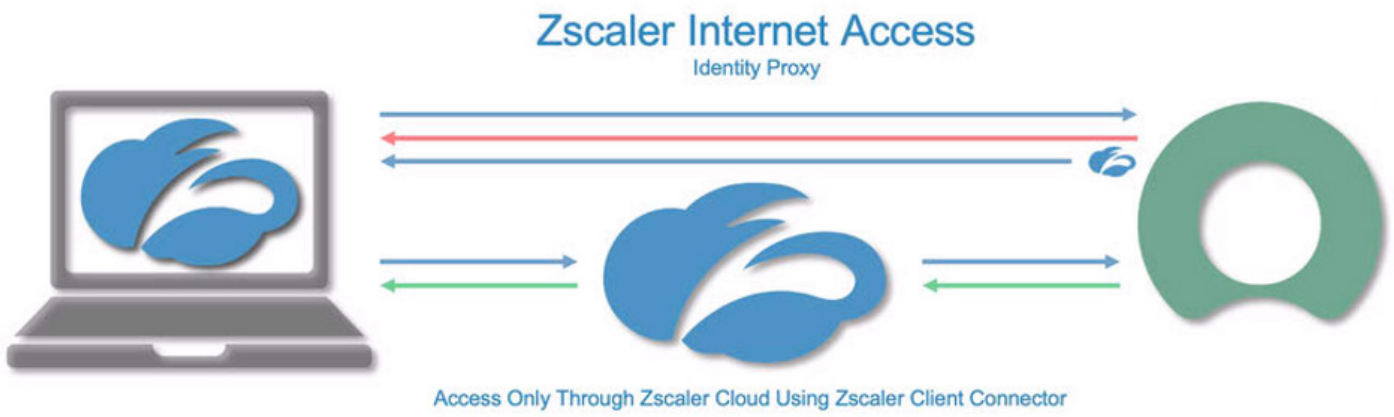


Figure 2. ZIA identity proxy

When users try to access ServiceNow with their corporate accounts without going through the Zscaler service, they receive a pop-up screen asking them to log in via Zscaler. Security Assertions Markup Language (SAML), the identity provider (IdP) that is defined on Zscaler for the ZIA service, and the ServiceNow single sign-on (SSO) configuration control the process and forward authorization requests to Zscaler. After the user's identity is verified, their traffic to and from ServiceNow is secured and the user and the ServiceNow data is inspected using ZIA.

ZIA sits between your users and ServiceNow, inspecting every byte of traffic inline across multiple security techniques, even within Secure Sockets Layer (SSL). You get full protection from web and internet threats. With a cloud platform that supports Cloud Firewall, Cloud intrusion prevention system (IPS), Cloud Sandbox, Cloud DLP, and Cloud Browser Isolation, you can start with the services you need today and activate others as your needs grow.

ZIA Browser Isolation

Most new threats that target organizations are now browser-based. As a result, organizations are left struggling to keep these threats from reaching endpoint devices and preventing sensitive data from leaking out, while providing unobstructed internet access for users.

Figure 3. ZIA Cloud Browser Isolation in use with ServiceNow

Zscaler Cloud Browser Isolation provides safe access to active web content for your users by rendering browser content in an isolated environment, and by minimizing the browser attack surface. Sensitive information is protected from web-based malware and data exfiltration.

By defining granular policies based on user group or department, you can effectively protect endpoint devices and prevent confidential data exposure from business-critical applications by managing user activity within the isolation environment enabling viewing in ServiceNow while preventing the downloading and cutting-and-pasting of confidential business data.

Cloud Browser Isolation can be combined with Identity Proxy to provide extra security to ServiceNow users by assuring the identity of the user, guaranteeing the users traffic is scanned and secured with the ZIA security features.

ZIA Data Loss Protection and Malware Detection for ServiceNow

The Zscaler 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 the file collaboration SaaS partners, preventing data exposure and ensuring compliance across the SaaS application.

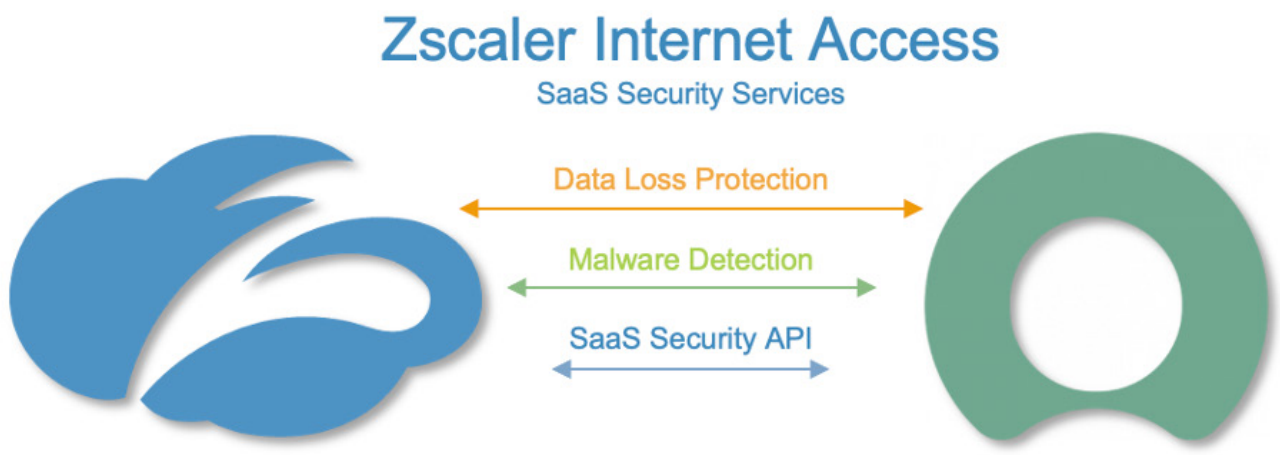


Figure 4. ZIA SaaS security in use with ServiceNow

The 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 Unique?

- **Data exposure reporting and remediation.** Zscaler SaaS Security checks SaaS applications and cloud providers' 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 ZCSPM 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 monitoring of users' experience to SaaS applications, and Zscaler Cloud Protection (ZCP). Zscaler provides end-to-end connectivity, security, and visibility from any location on-premises or remote.

For more information, see the resources in Zscaler Resources.

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, inspecting 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.

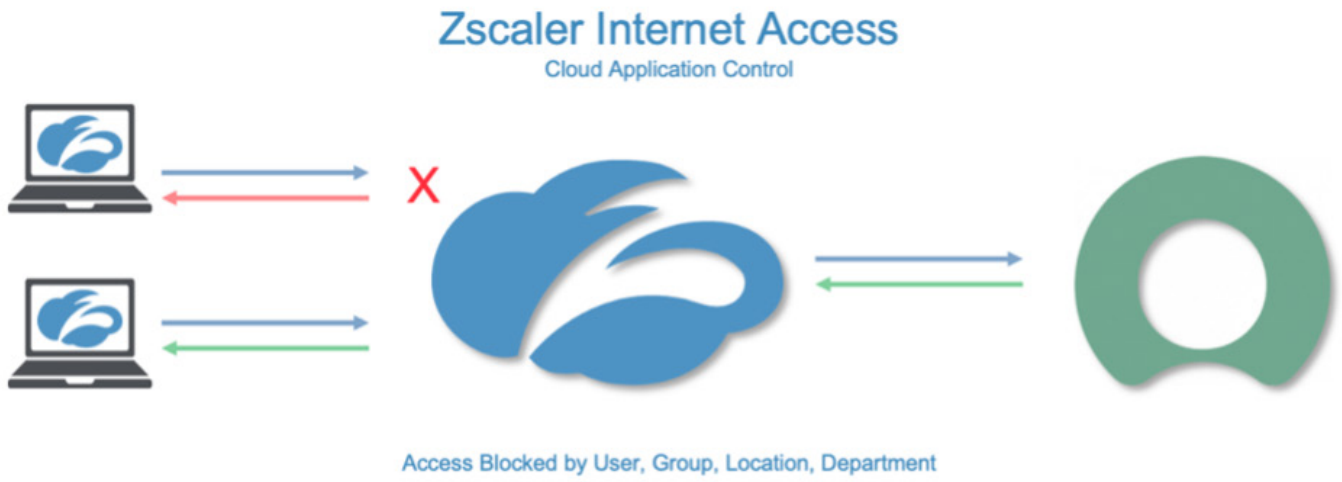


Figure 5. Cloud App Control

Cloud App Control provides SaaS application intelligence to consolidate all associated URLs and provides functions of an 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 ServiceNow User Experience

With ZDX, you can easily monitor your users' digital experiences. ZDX provides visibility across the complete user-to-cloud app experience and quickly isolates issues. ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

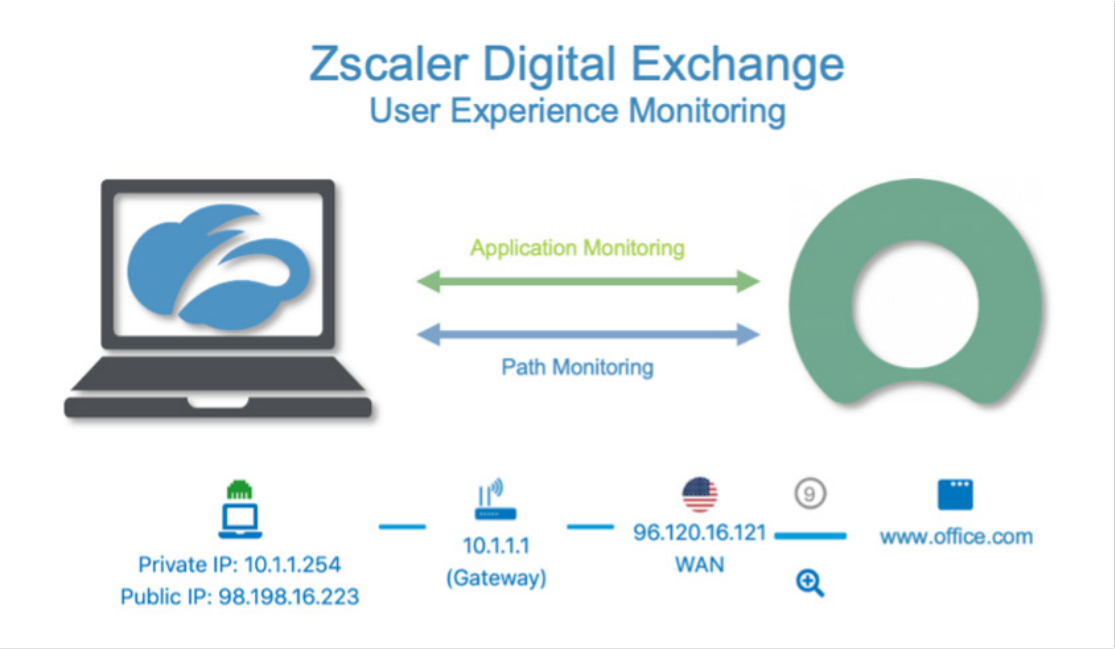


Figure 6. ZDX in use with ServiceNow

What makes the ZDX unique?

- **End-user device performance**. Gather and analyze data on end-user device resources that impact the end-user experience.
- **Cloud path performance**. Measure and analyze end-to-end and hop-by-hop network path metrics from every user device to the cloud application.
- **Application performance**. Continuously monitor and measure application metrics, such as response time, DNS resolution, and broader availability metrics of the application.
- **ZDX scoring**. Monitor 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.

ZPC and ServiceNow Incident Creation

Zscaler Posture Control (ZPC) integrates with ticketing systems to automatically log incidents when misconfigurations or compliance violations are discovered. These violations and misconfigurations can be related to cloud environments such as AWS, Azure, GCP, and Infrastructure as Code (IaC) events. ZPC integrates with incident management (ticketing) tools such as ServiceNow to automate the incident creation and expedite resolution.

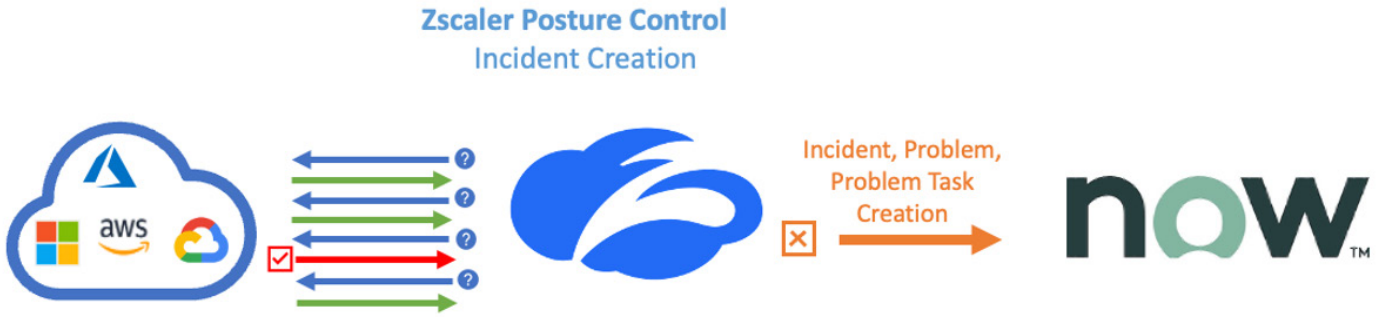


Figure 7. Zscaler Posture Control

The process to configure the integration includes:

- Create a ServiceNow user account with “Web Service Only” capability to open incidents in the SNOW platform.
- Configure ZPC Incident Management for ServiceNow integration.
- Create a ZPC Notification Rule.
- Verify ServiceNow Incidents tickets for ServiceNow admins.

Configure the SaaS Identity Proxy

Log into the Zscaler tenant with administrator credentials.

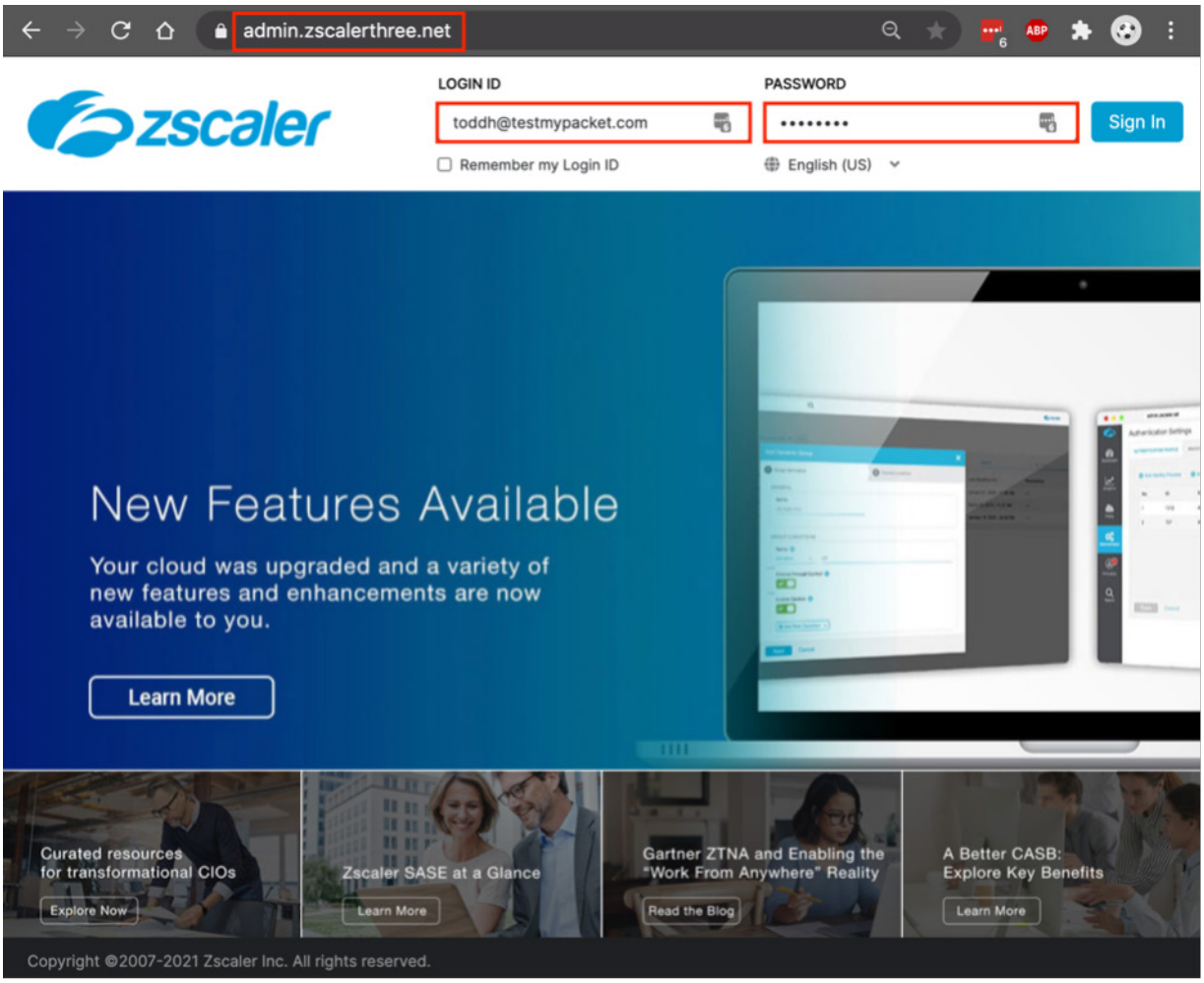


Figure 8. Configure the SaaS identity proxy

Configure the ZIA Admin Portal for the SaaS Identity Proxy

To configure Zscaler for the SaaS Identity Proxy:

1. Go to **Administration** > **Identity Proxy Settings**.
2. Select **Add Cloud Application**.
3. In the configuration wizard that displays, give the cloud application a **Name**.
4. Click **Enable**.
5. Select **ServiceNow** for **Cloud Application**.
6. Set the **ACS URL** to **https://your-servicenow-instance.service-now.com/navpage.do**.
7. Set the **Entity ID** to **https://your-servicenow-instance.service-now.com**.
8. Select the **SAML_2022 or Later** signing certificate.
9. Select **Pass-through Zscaler Identity** for the **Identity Transformation**.
10. Click **Save**.

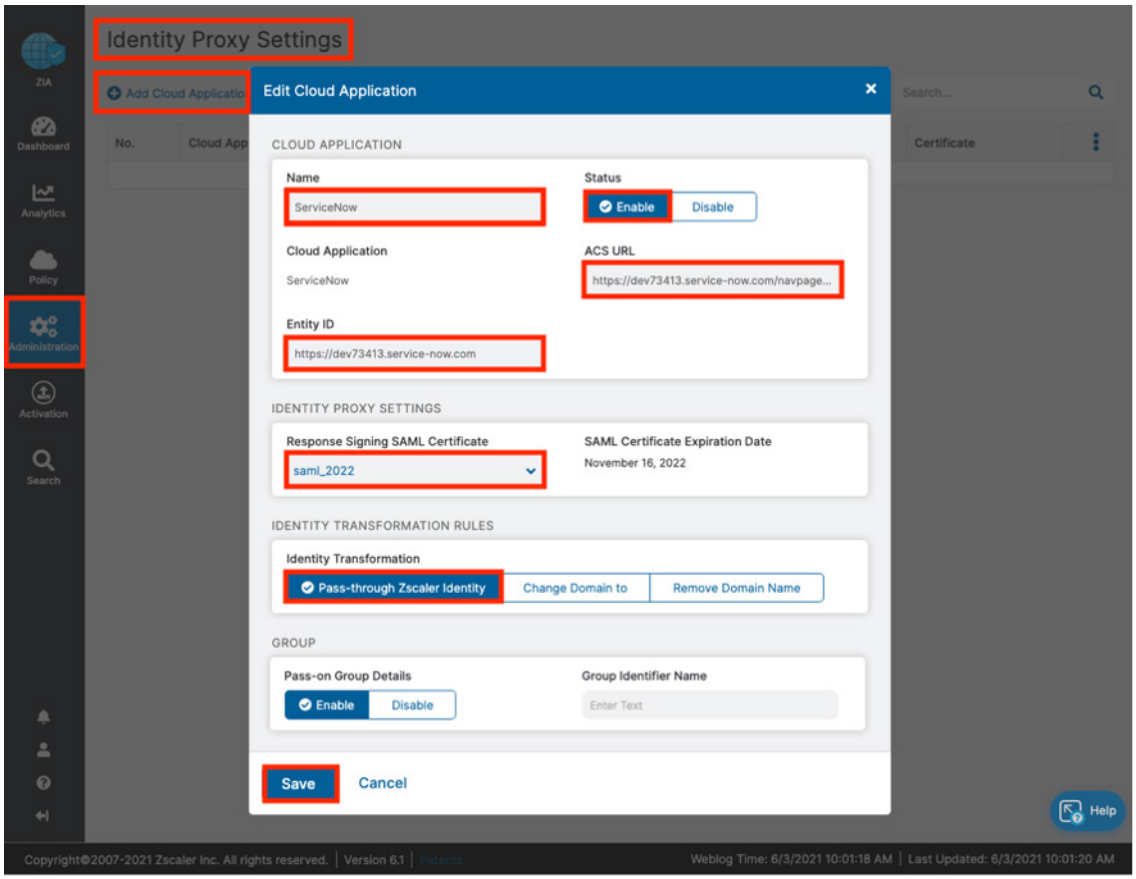


Figure 9. Configure the SaaS identity proxy settings

Complete SaaS Identity Proxy

This is the completed identity proxy configuration on the Zscaler tenant. Copy and save the Identity Proxy URL and the Issuer Entity ID for later in the ServiceNow configuration. Download and save the Signing Certificate:

1. Copy and save the **Identity Proxy URL**.
2. Copy and save the **Issuer Entity ID**.
3. Download and save the **Signing Certificate**.

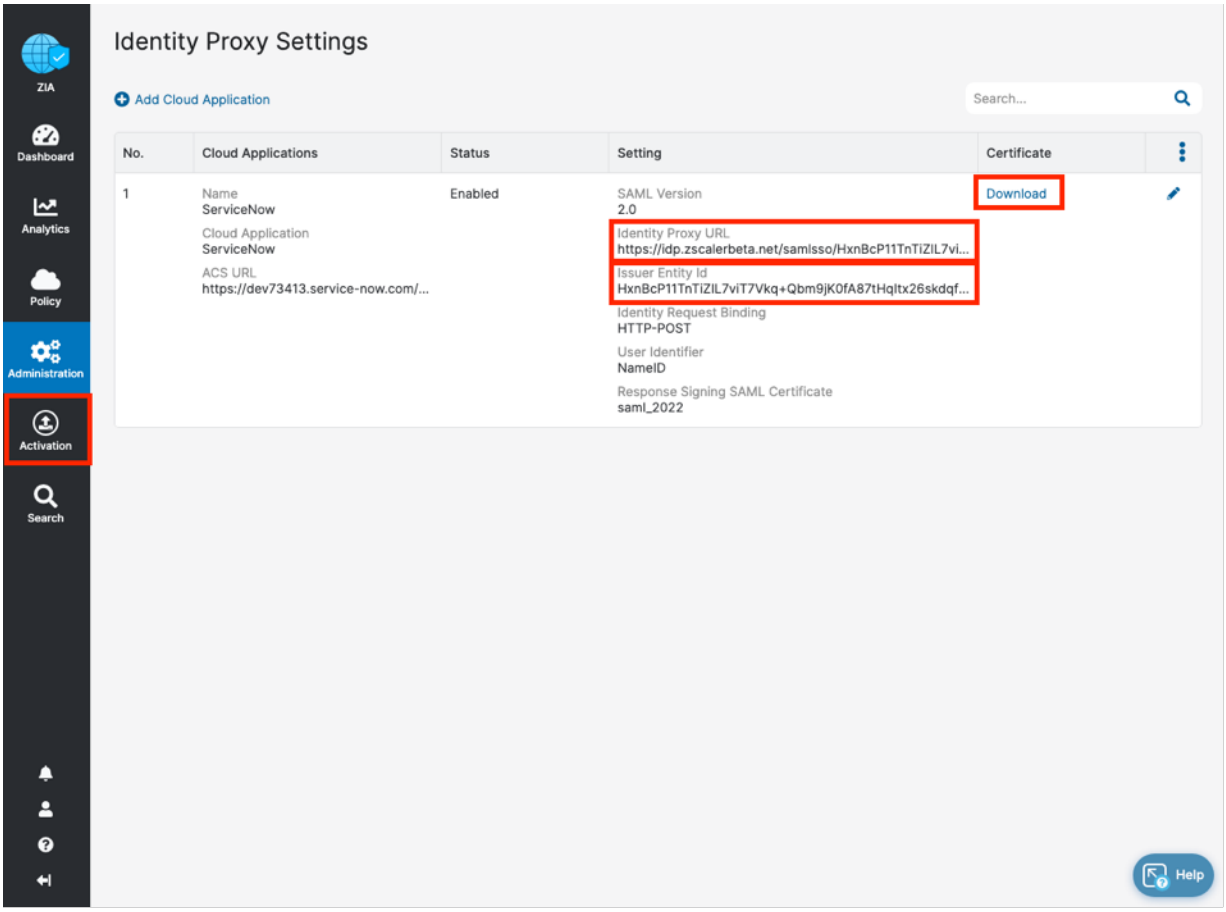


Figure 10. The completed identity proxy

Configure ServiceNow to Use the Identity Proxy

The following steps are based on procedures documented on the ServiceNow website. Log into the ServiceNow tenant with administrator credentials.

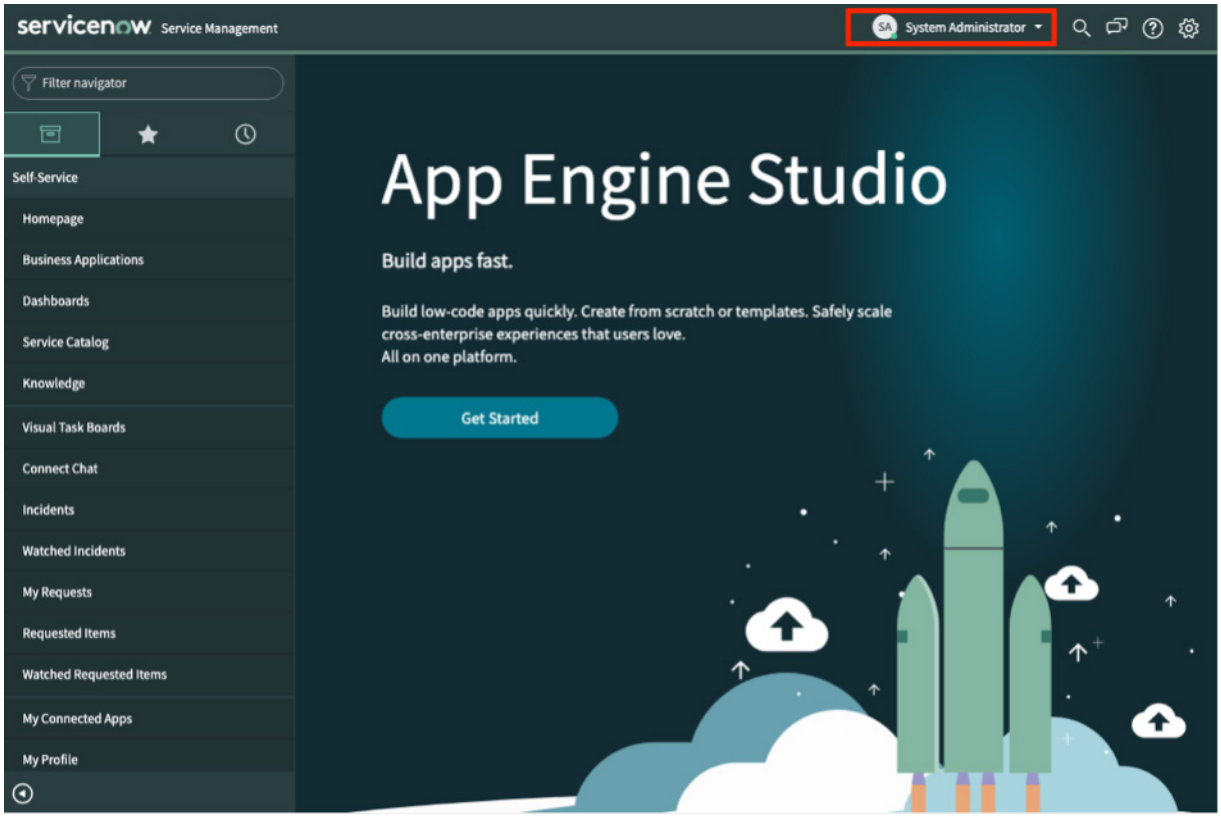


Figure 11. Configure ServiceNow to use the identity proxy

Install the ServiceNow Plugins

In the ServiceNow plugins page:

1. In the **Filter Navigator** search for `system app` .
2. Select **All Available Applications**.
3. Select **All** to display all available plugins.
4. Filter for `multiple provider`.
5. Click **Install** for the **Integration – Multiple Provider Single Sign-On Enhanced UI**.
6. Click **Activate**.

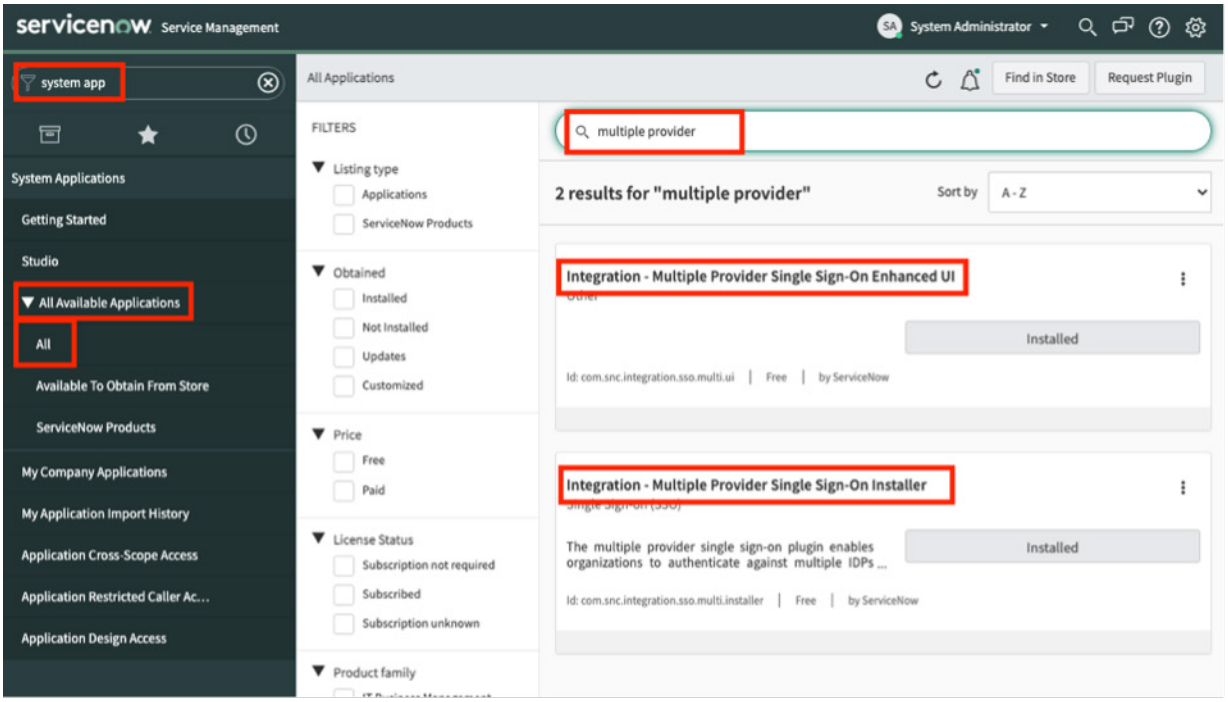


Figure 12. Configure the ServiceNow plugins

Both the Multiple Provider Single Sign-On Enhanced UI and the Multiple Provider Single Sign-On Enhanced plugins are installed, which you must configure for the Zscaler identity proxy.

Configure the SaaS Identity Proxy

Next, configure the SaaS identity proxy:

1. Search for `multi` in the Filter Navigator.
2. Select **Administration** under **Multi-Provider SSO**.
3. Select **Properties** to display the **Customization Properties for Multiple Provider SSO** page.
4. Select **Yes** to enable multiple provider SSO.
5. Select **Yes** to enable **Auto Importing** of users from all identity providers into the user table.
6. Select **Yes** to enable debug logging for the multiple provider SSO integration.
7. Click **Save**.

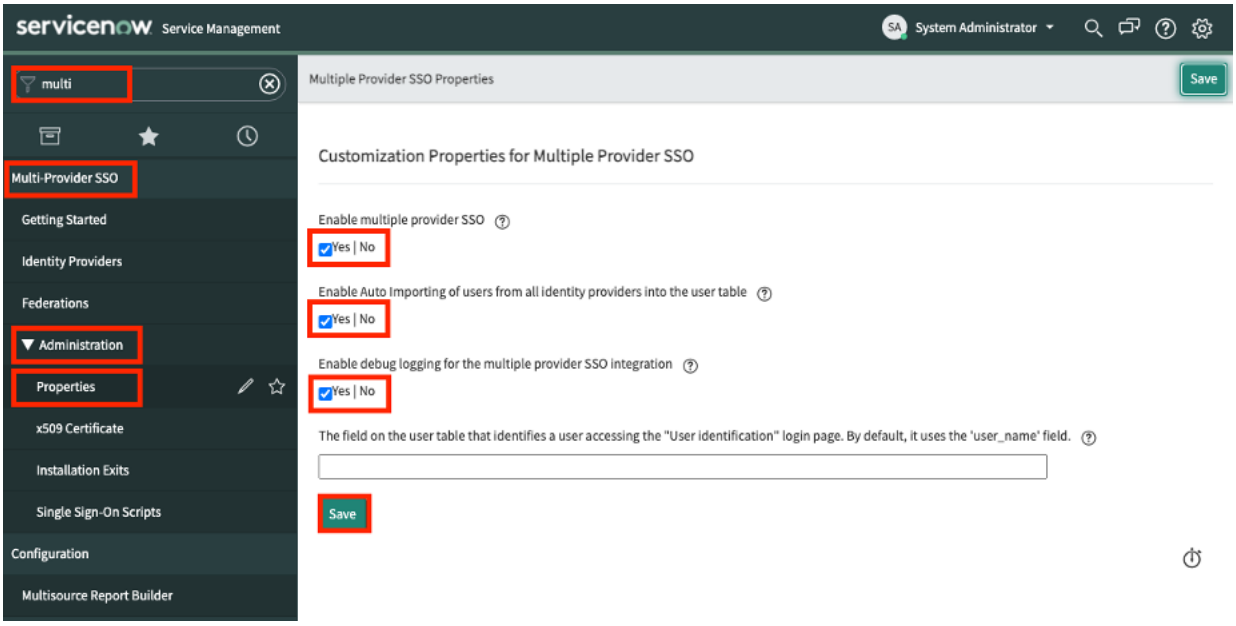


Figure 13. Enable multiple provider SSO

Add Zscaler as an Identity Provider

The next step is to add the Zscaler identity proxy as an identity provider:

1. Select **Identity Providers** in the configuration pane.
2. Select **New**.

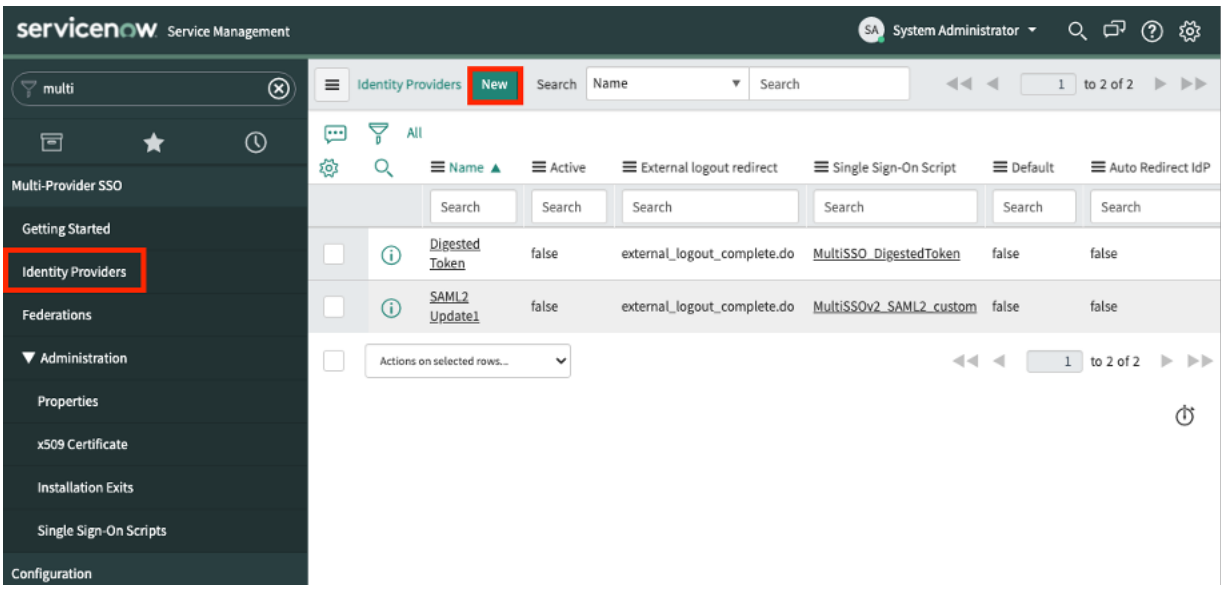


Figure 14. Create the Zscaler Identity Provider

3. In the ServiceNow Identity Providers section, select **SAML**.

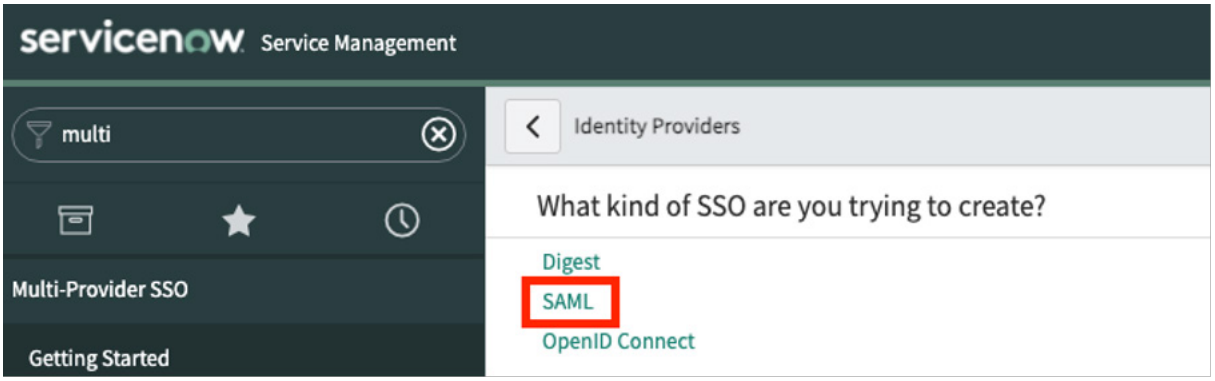


Figure 15. Select SAML SSO

Configure the Identity Provider

Use values that you created in the Zscaler tenant to configure the identity provider in ServiceNow:

1. In the **Identity Provider New Record** window, give the template a **Name**.
2. In the **Identity Provider URL** field, paste in the **Issuer Entity Id** from the Zscaler config.
3. In the **Identity Provider's AuthnRequest URL** field, paste in the **Identity Proxy URL**.
4. For the **ServiceNow Homepage URL**, enter your **ServiceNow Instance/navpage.do**.
5. For the **Entity ID / Issuer**, and for the **Audience URI**, enter your **ServiceNow Instance**.
6. For the **NameID Policy**, enter **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**.
7. Select the **Advanced Tab**.
8. For the **Single Sign-On Script**, search and select the **MultiSSOv2_SAML2_custom Script**.
9. Select **Force AuthnRequest**.
10. Click **Submit**.

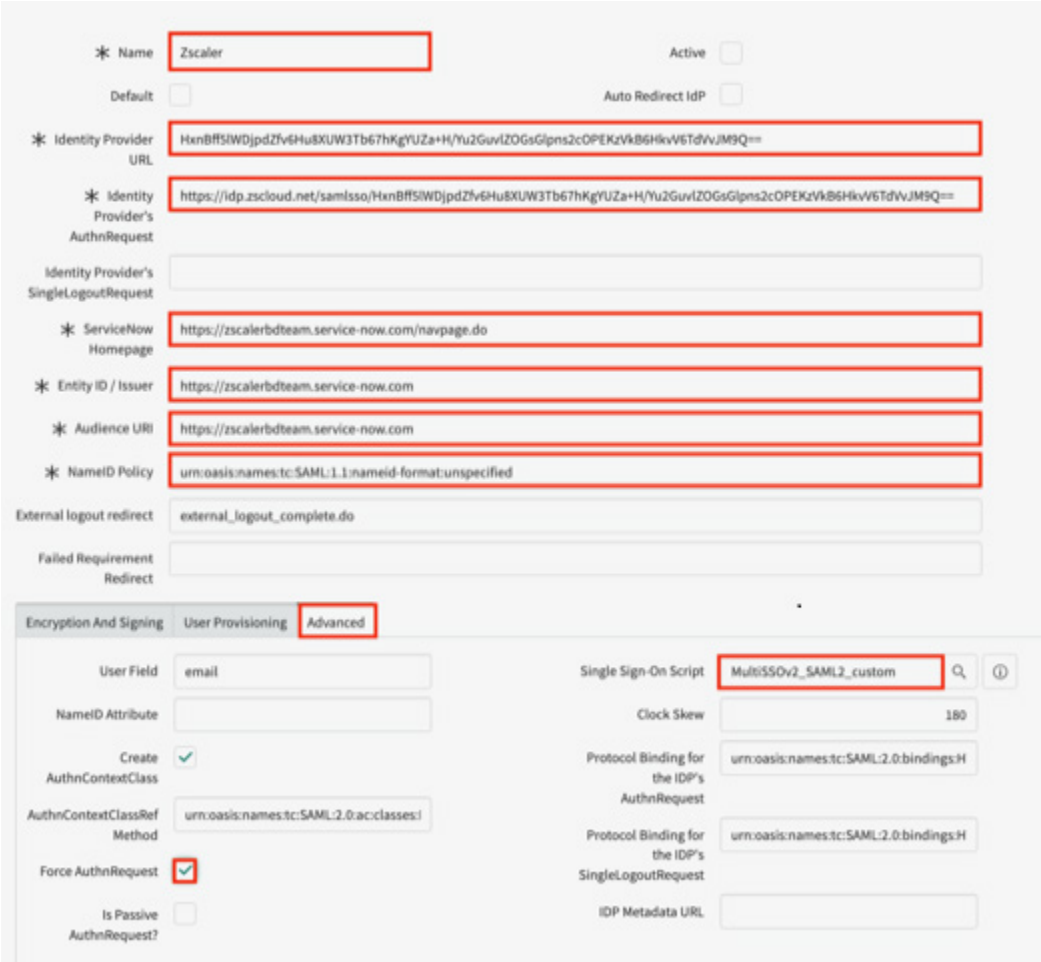


Figure 16. Configure the identity provider

Add the Identity Provider Certificate and Additional Settings

Return to the Identity Provider to finish the configuration, test the IdP, and to activate it:

1. Select the Zscaler Identity Provider.

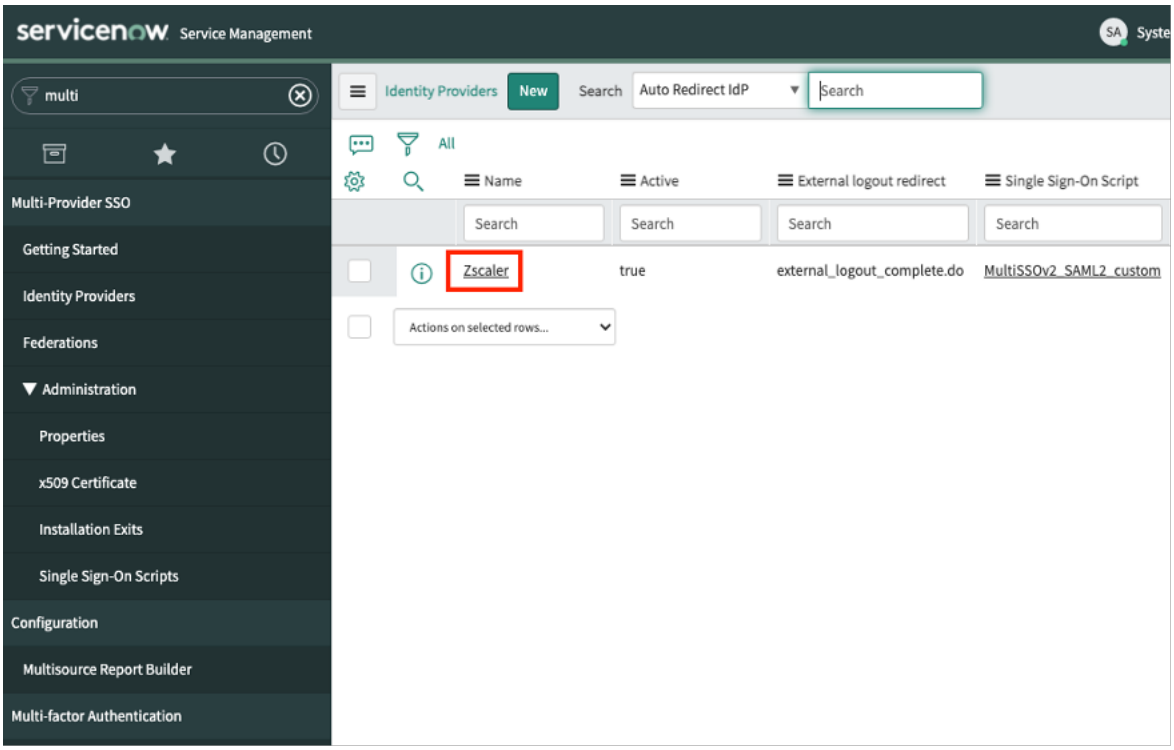


Figure 17. Select the Zscaler identity provider

2. The option to add the Zscaler certificate becomes available at the bottom of the configuration screen. To configure and add the certificate, select **New**.

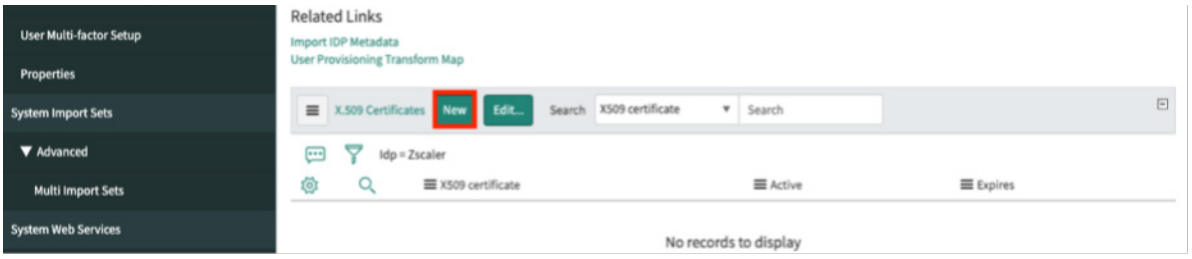


Figure 18. Add the signing certificate

3. To add the certificate is a manual process:
   a. **Name** the certificate.
   b. Open the certificate file from Zscaler and copy the entire contents.
   c. Paste the contents into the **PEM Certificate** field.
   d. Click **Submit.**

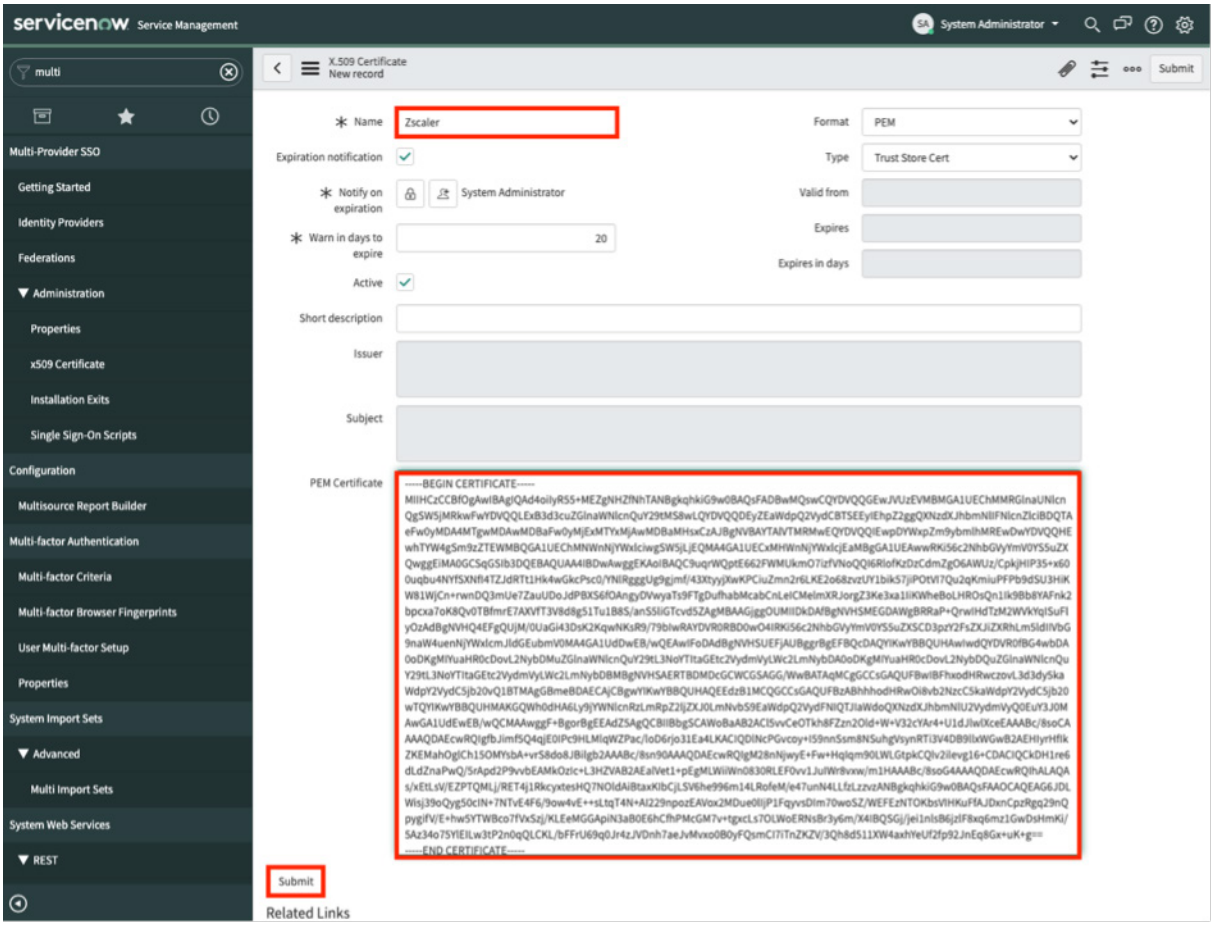


Figure 19. Configure the identity provider certificate

The certificate is one continuous line. Remove any carriage returns.

4. To configure additional identity provider certificate settings:
   a. Select **Default**.
   b. Select **Set** as **Auto Redirect IdP**.
   c. Select **Test**.

This opens a test window and displays the **Authentication** screen from the IdP that is configured on Zscaler. If Okta or Azure AD are set as the IdP, you get an **authentication** prompt. If successful, you can activate the identity provider. You might be able to activate the identity proxy without seeing the following screen, or you might need to activate it on the test screen.

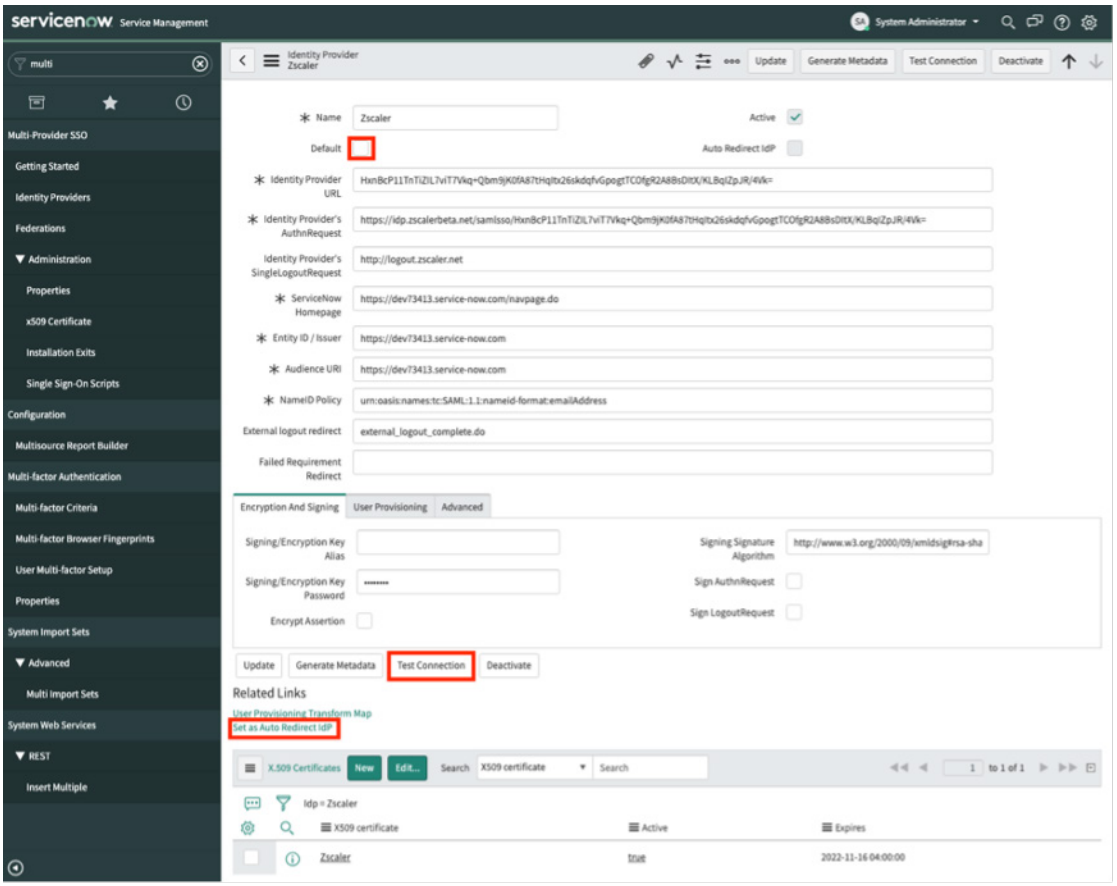


Figure 20. Configure and test the identity proxy

You might need to run the test more than once to enable the identity provider. If auto redirect fails to enable, use an identity provider redirect as shown in Configure Redirect on the Identity Provider.

Testing the Identity Provider

If everything is configured correctly, the following screen is displayed when testing, and any time a change is made to the identity proxy, you need to re-test the identity proxy. The SSO Login Test Results display successful test results. (The SSO Logout Test Results are expected to fail.)

Select **Activate**.

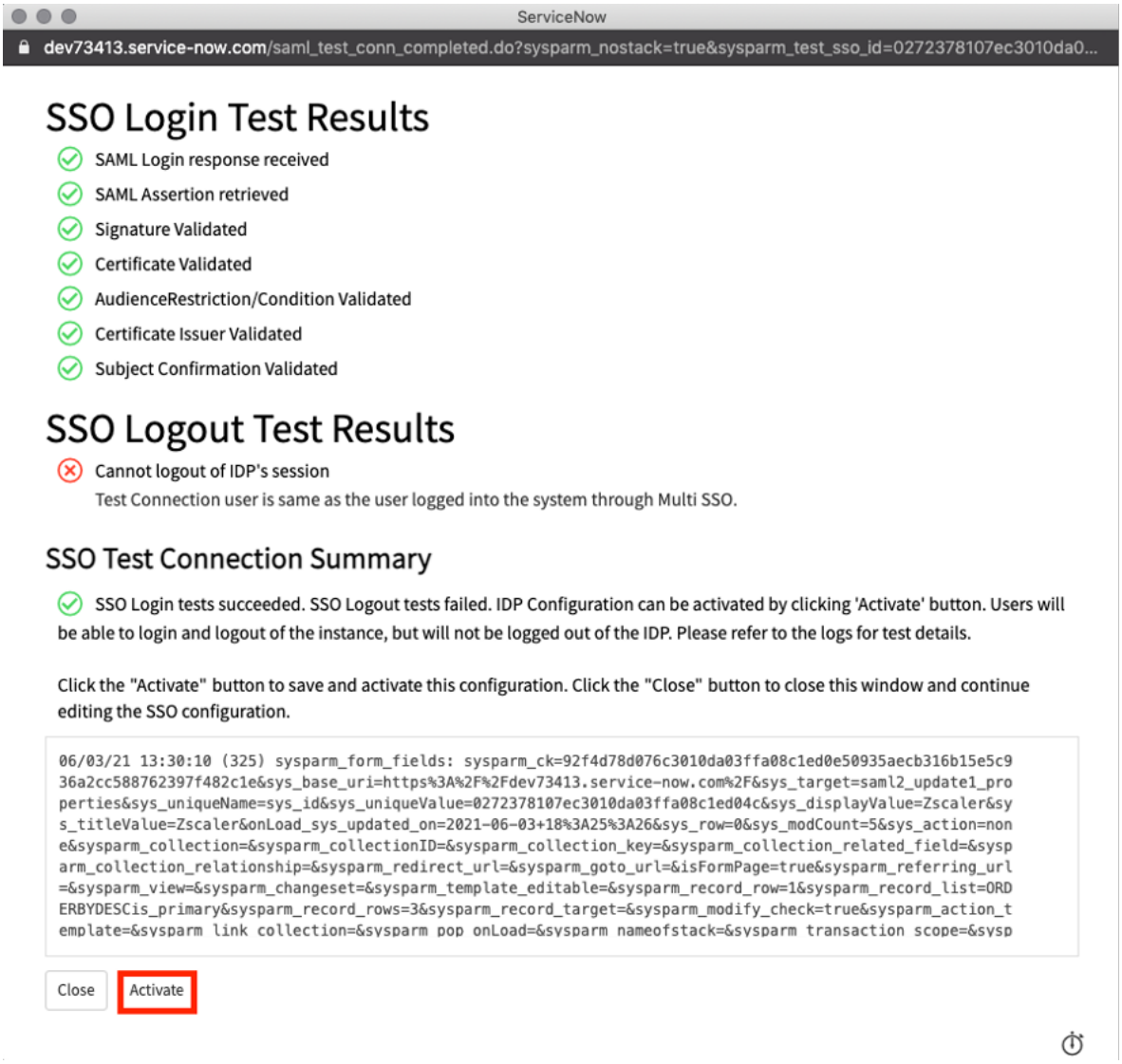


Figure 21. Testing the identity provider

The Active Identity Proxy Notification

This is the notification a ServiceNow user receives if they are trying to log into ServiceNow without going through Zscaler. When your user traffic is going through Zscaler, the users can access ServiceNow as usual.

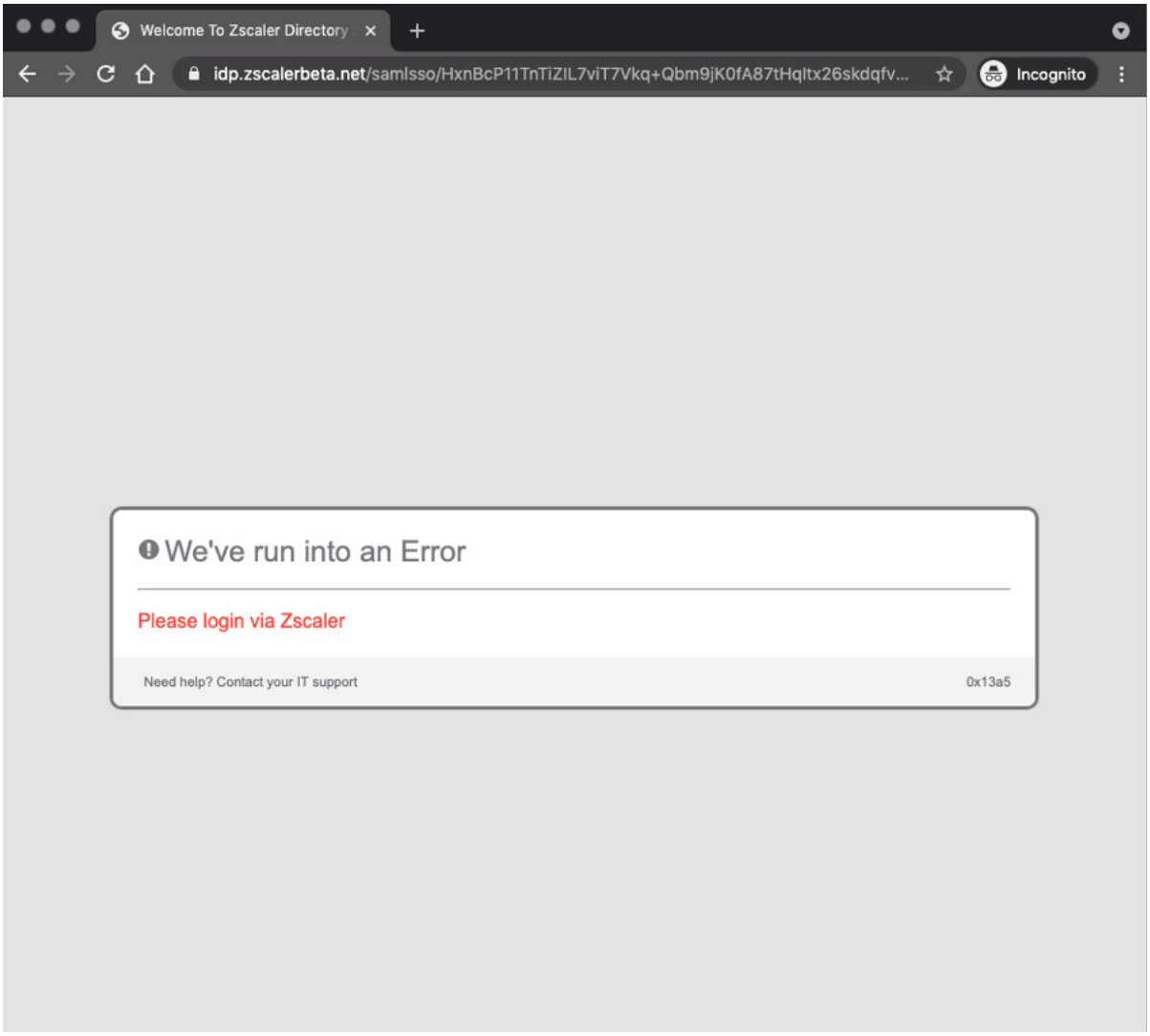


Figure 22. The active authentication proxy

Configure Redirect on the Identity Provider

Use this procedure when the auto redirect IdP doesn't enable from the Configuration screen. Set a system property to enable redirect by default to the Zscaler IdP:

1. Go to the **Identity Providers** page.
2. Click **Zscaler Identity Provider** and copy the sys_id.

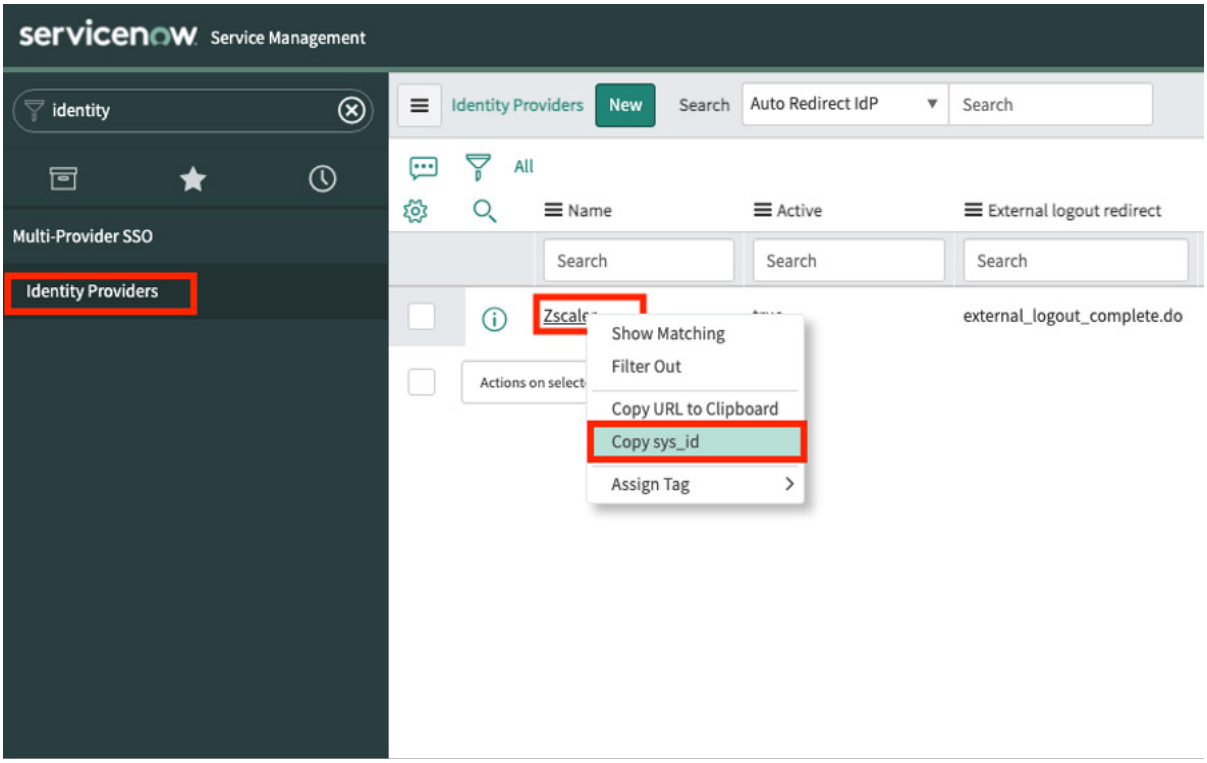


Figure 23. Configure the identity provider

3. Configure the redirect system properties:
    a. Search for `sys_properties.LIST` in the **Filter Navigator**.
    b. Press **Return**.

This launches a new window or tab with all available system properties.

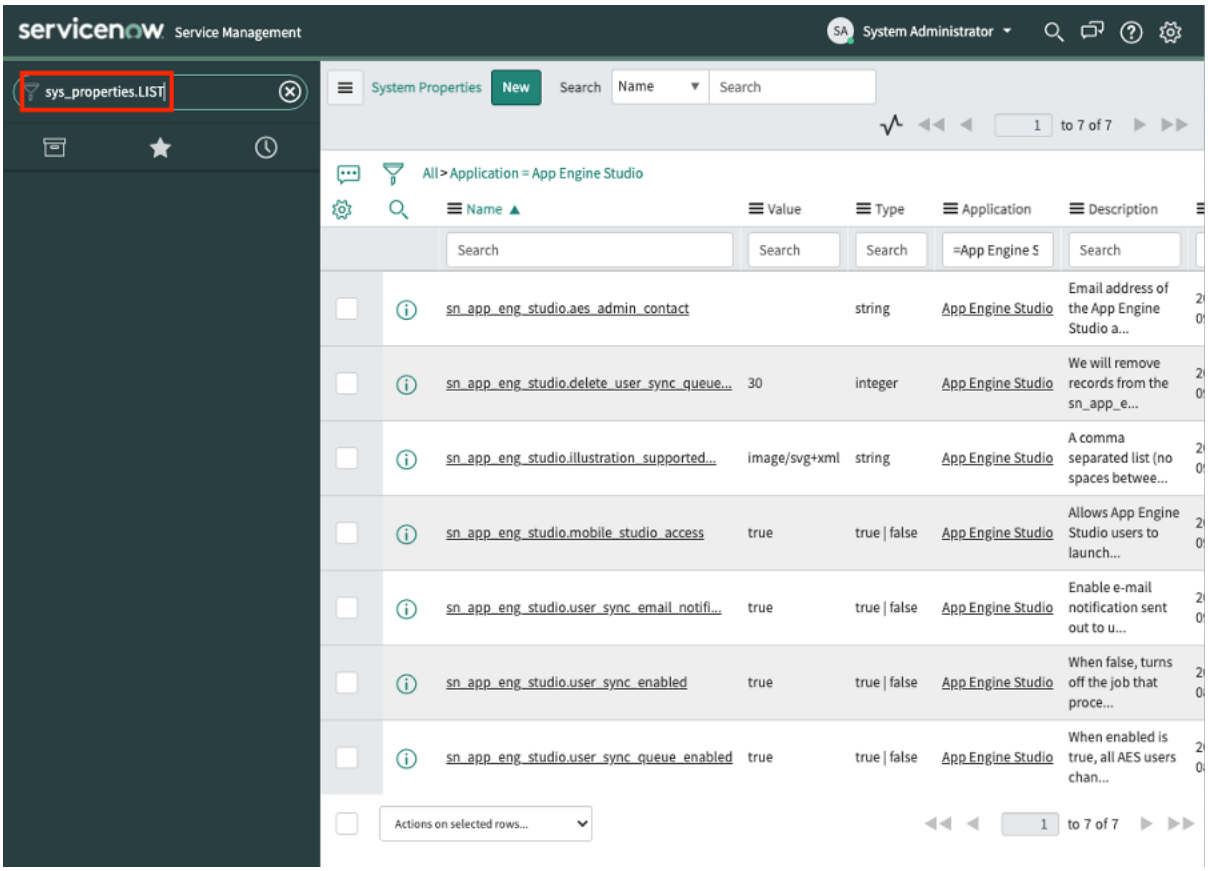


Figure 24. System properties

4. In the Systems Properties screen, search for and edit the system property glide.authentication.sso.redirect.idp. This launches the edit screen for the property:

   a. Search for `glide.authenticate.sso.redirect.idp`.

   b. Select `glide.authenticate.sso.redirect.idp`.

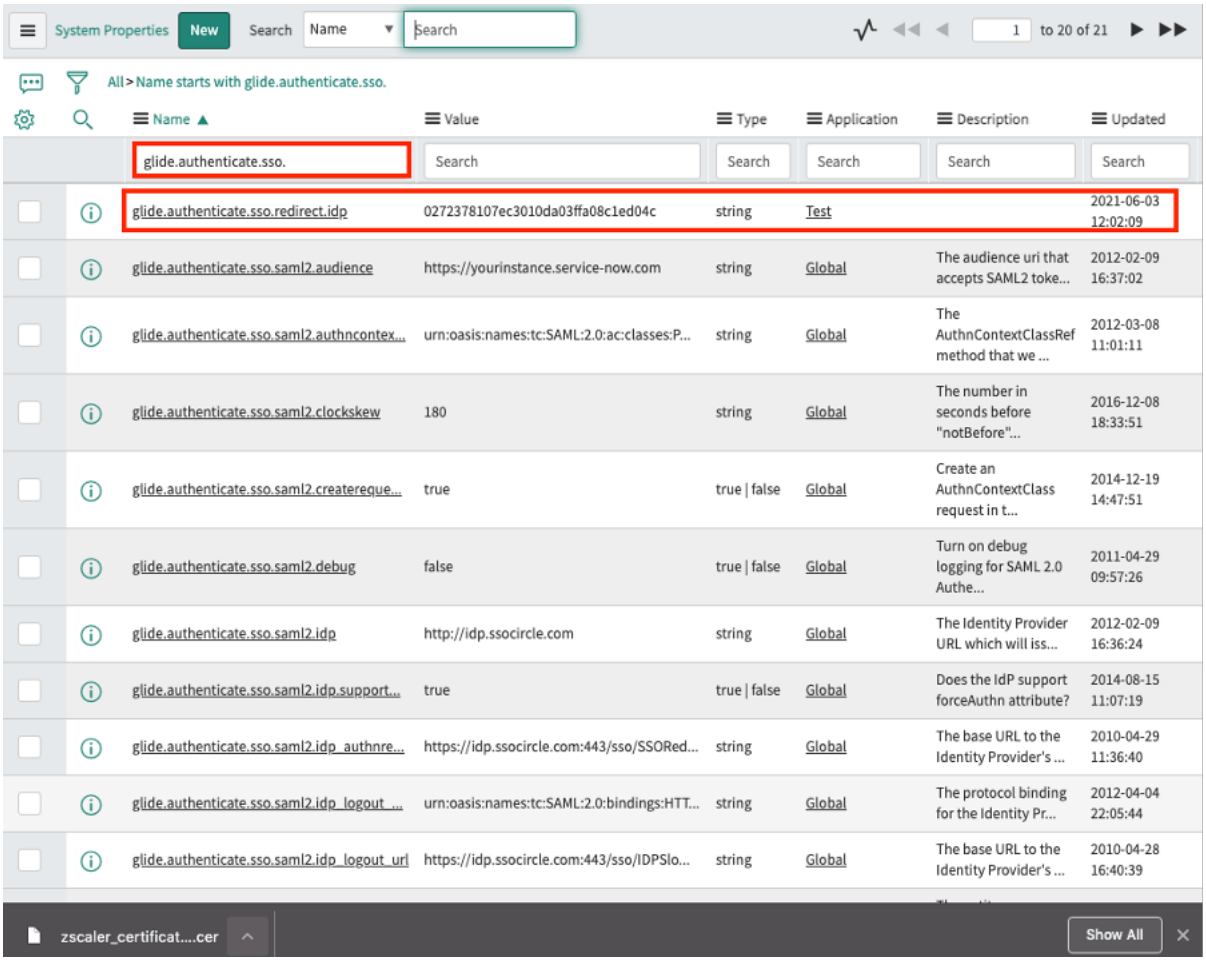


Figure 25. System Property glide.authenticate.sso.redirect.idp

Configure the Property

In the System Property screen, search for and edit the systems property glide.authentication.sso.redirect.idp:

1. In the **Value** field, paste the sys_id from the Zscaler IdP.
2. Click **Update**.

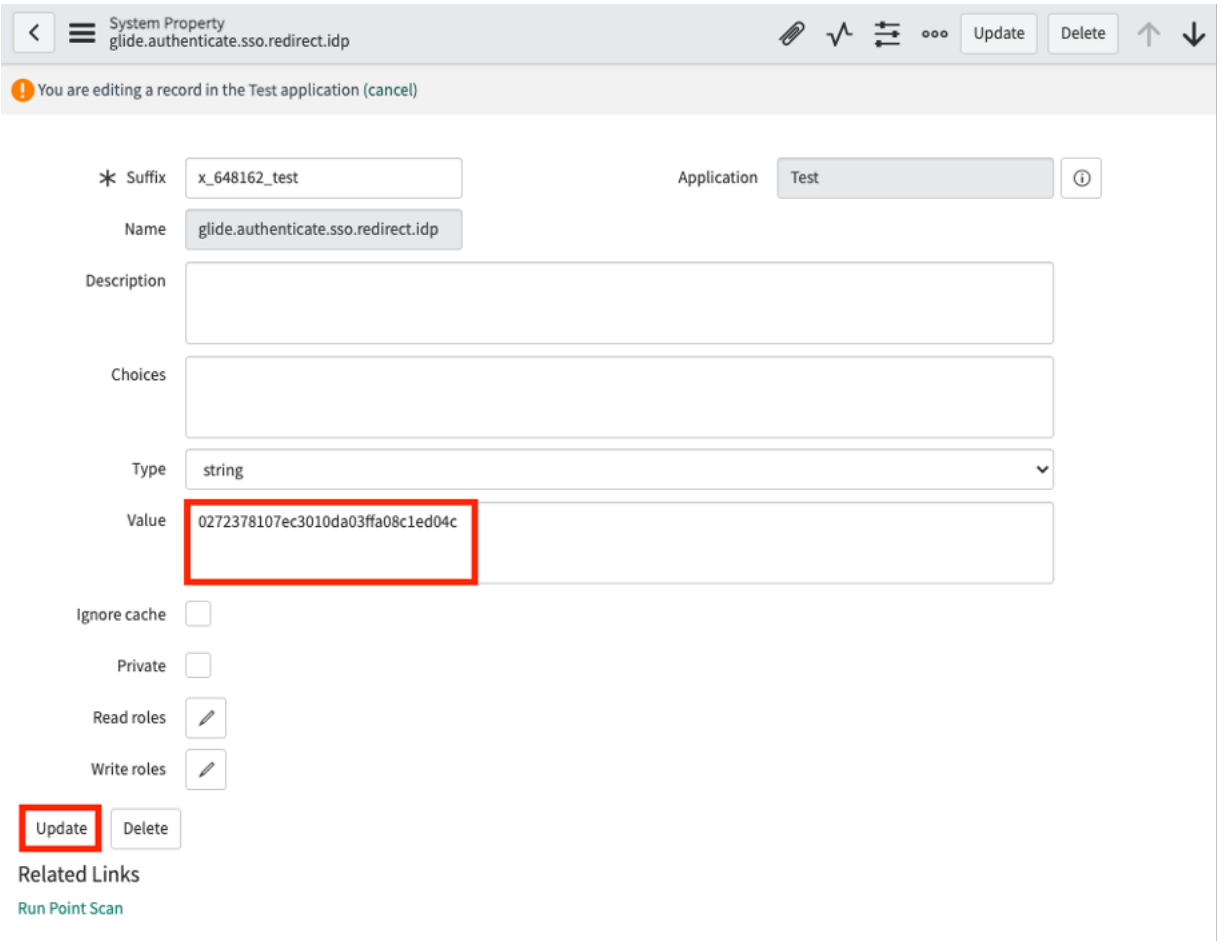


Figure 26. System Property glide.authentication.sso.redirect.idp

Configure Cloud Browser Isolation

Most new threats that target organizations are now browser-based. As a result, organizations are left struggling to keep these threats from reaching endpoint devices and preventing sensitive data from leaking out, while providing unobstructed internet access for users.

Zscaler Cloud Browser Isolation provides safe access to active web content for your users by rendering browser content in an isolated environment, and by minimizing the browser attack surface. Sensitive information is protected from web-based malware and data exfiltration.

Figure 27. ZIA Cloud Browser Isolation in use with ServiceNow

By defining granular policies based on user group or department, you can effectively protect endpoint devices and prevent confidential data exposure from business-critical applications by managing user activity within the isolation environment enabling viewing in ServiceNow while preventing the downloading and cut-and-pasting of confidential business data.

Cloud Browser Isolation can be combined with identity proxy to provide extra security to ServiceNow users by assuring the identity of the user, guaranteeing the user's traffic is scanned and secured with the ZIA security features, and for identified potentially risky users direct to Cloud Browser Isolation for even greater security measures.

Configure the Cloud Browser Isolation Profile

To begin the Cloud Browser Isolation configuration, log into your Cloud Browser Isolation Portal with administrator credentials. This is a different portal than your ZIA or ZPA Admin Portal and the link and administrator credentials are supplied to you by Zscaler Support after your organization has subscribed to the feature:

Log into the Cloud Browser Isolation tenant with administrator credentials.

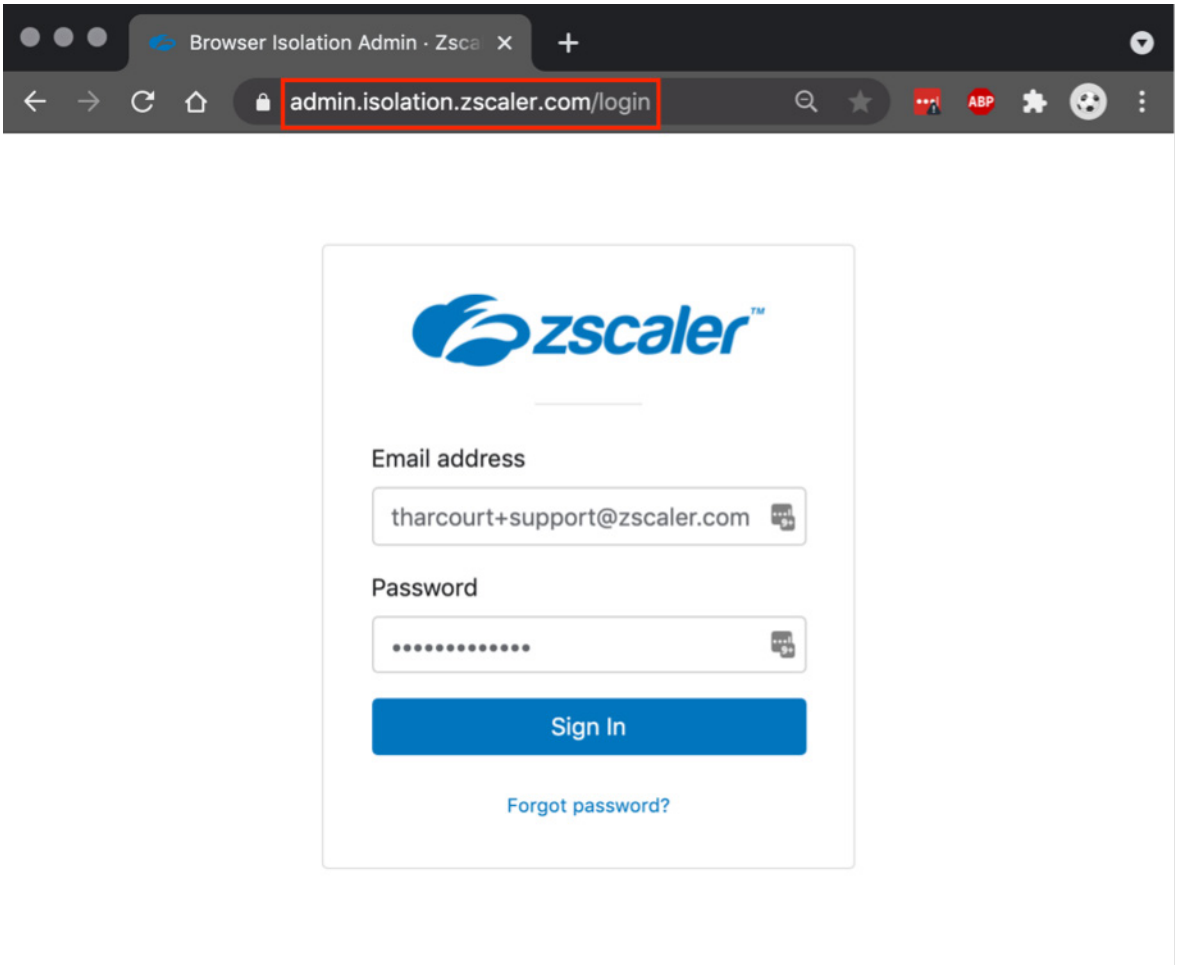


Figure 28. Configure Cloud Browser Isolation

Configure a Cloud Browser Isolation profile or multiple profiles to enable the features that are applied specifically for ServiceNow. Also configure the individual user implementing Cloud Browser Isolation. This is a generic profile for all SaaS applications, or multiple policies for ServiceNow depending on your needs and level of isolation. For example, you could have a policy to control file uploads for one client and copy-paste for another.

To start the **Policy Wizard**:

1. Select **Isolation profiles**.
2. Select the **ZIA** tab.
3. Select **Add New**.

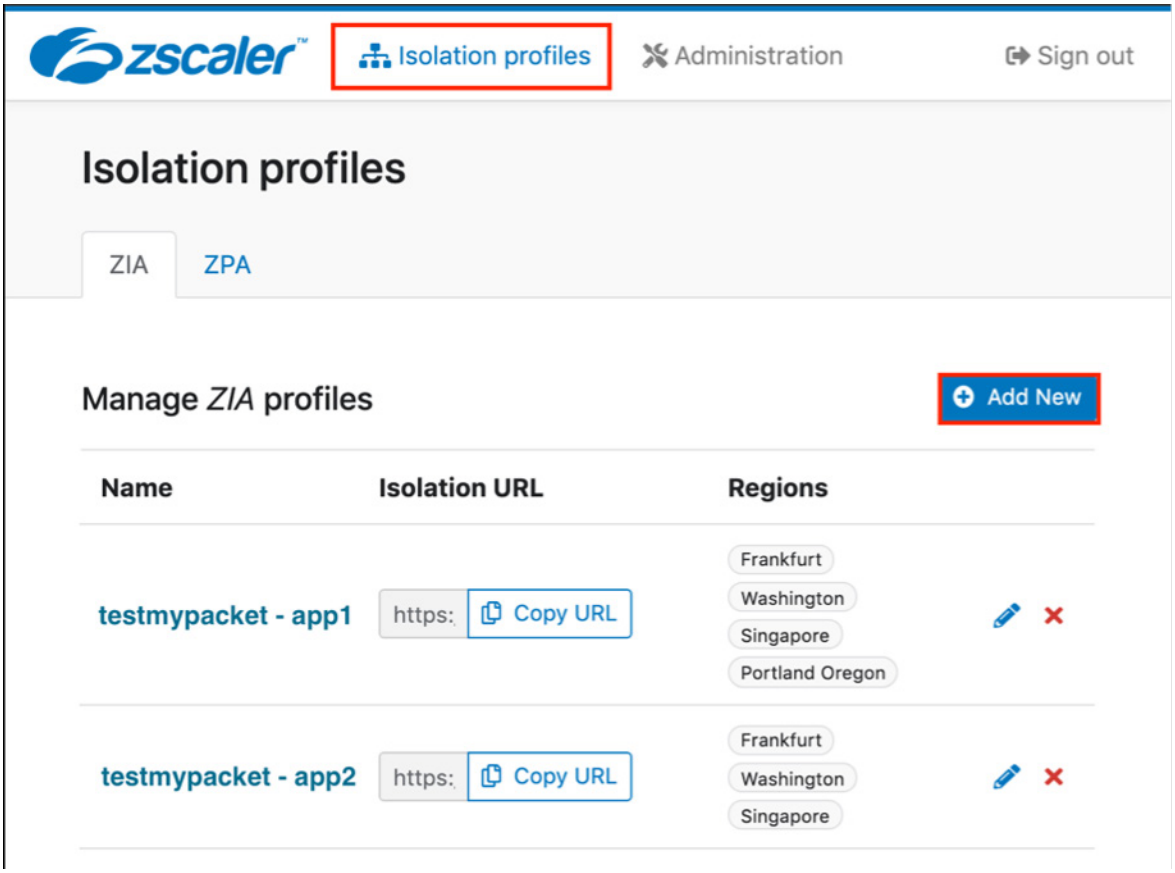


Figure 29. Configure Cloud Browser Isolation profile

This starts the **Browser Isolation** wizard and steps you through enabling **General Information**, **Company Settings**, **Security Controls**, **Regional Connectivity**, and the **End User Notification**.

4. For **General Information**, give the profile an intuitive name and description. Select it in the Isolation Policy on the ZIA Admin Portal and describe the use case:

   a. **Name** the profile.

   b. Give the profile a detailed **Description**.

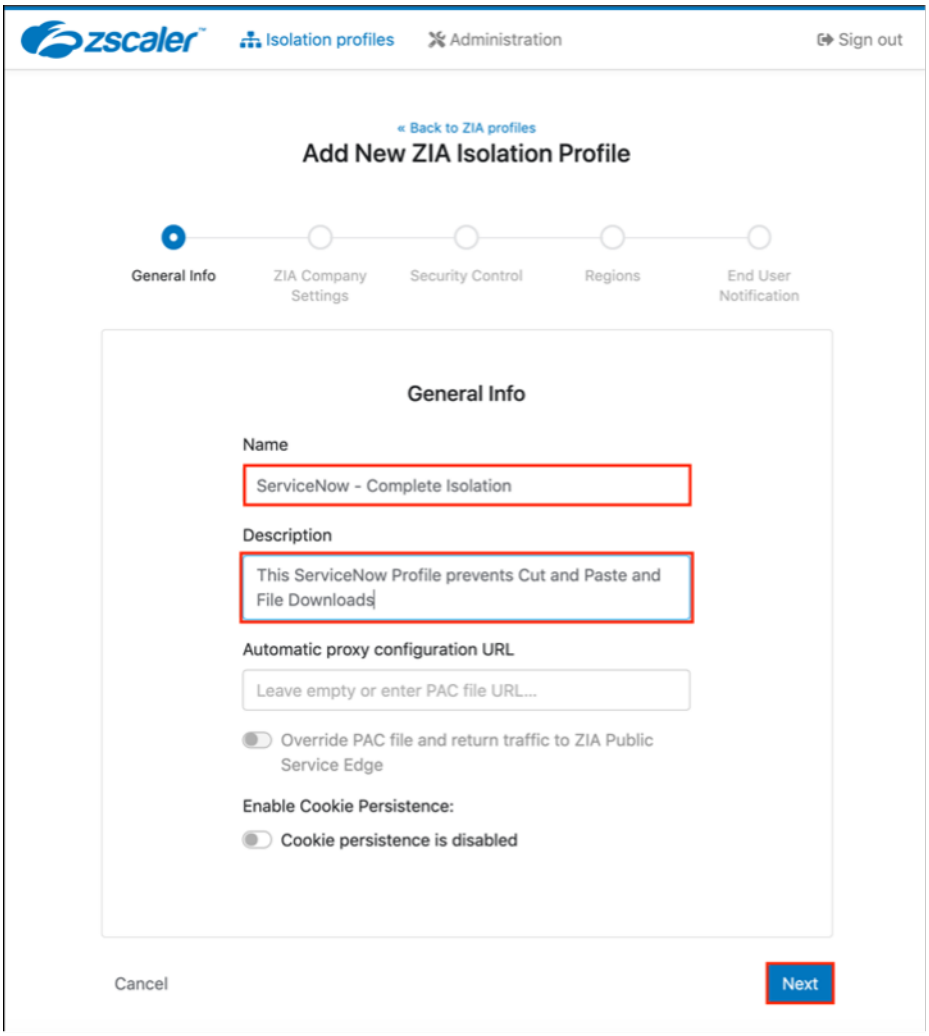


Figure 30. Cloud Browser Isolation general information

5. For the **ZIA Company Settings**, you must select your Company ID and Cloud if your information is not populated automatically. Obtain this information from your ZIA Admin Portal under **Administration** > **Company**:
   a. Select your **Company ID** and **Zscaler Cloud**.
   b. Leave the **Zscaler Root Certificate** as the **Default Certificate**.
   c. Select **Next** to proceed in the wizard.

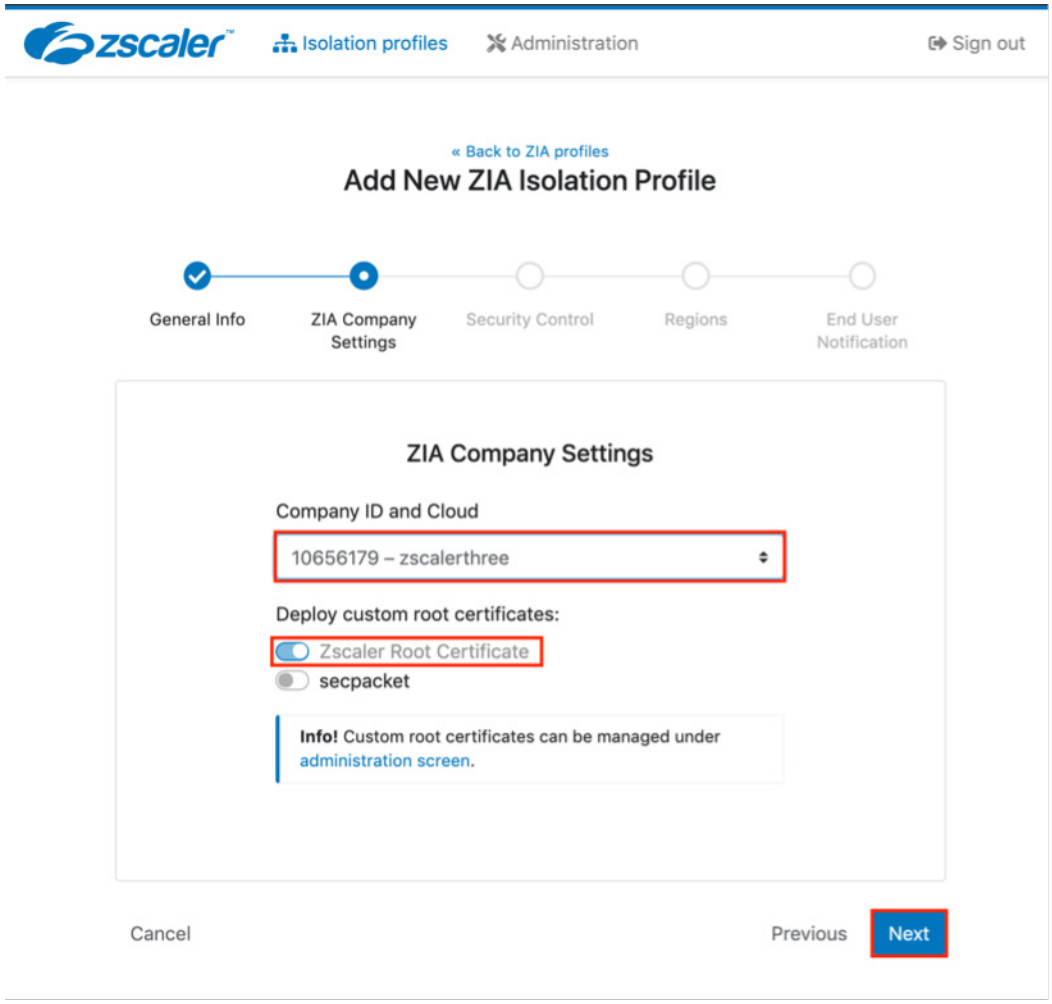


Figure 31. Cloud Browser Isolation ZIA company settings

6. The Security Control allows administrators to maintain a complete air gap between the user and ServiceNow, or allow some level of control of the ServiceNow application in the Isolation Session. Settings include allowing copy-paste up to or down from ServiceNow from or to the local computer. You can also control File Transfers up to or down from ServiceNow from or to the local computer.

   Allowing Local Browser Rendering allows the user to visit pages outside of the ServiceNow domain while in the Isolation Session. For this profile, maintain the strictest security settings and do not enable any controls.

   Select **Next**.

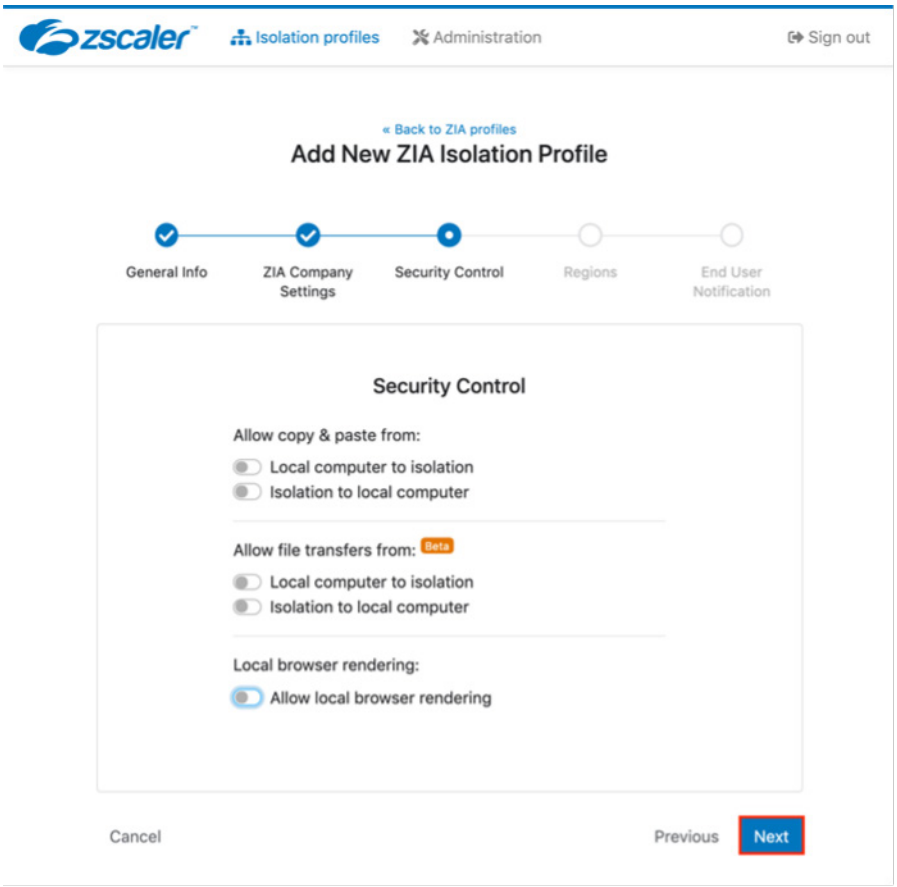


Figure 32. Cloud Browser Isolation security control

7. Select two **Regions** or redundancy. Select the two closet regions to your organization:
   a. Select two **Regions** for redundancy.
   b. Select **Next**.

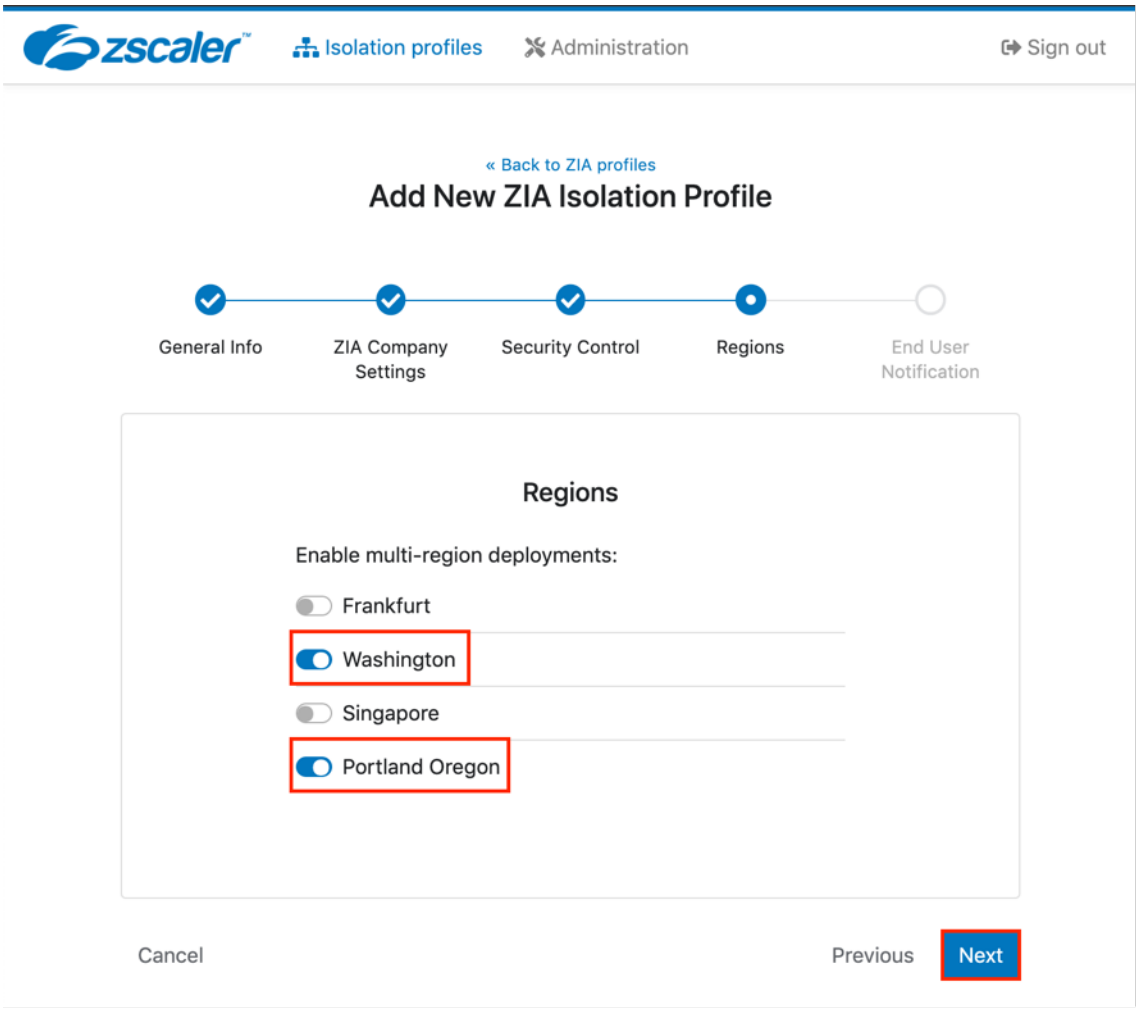


Figure 33. Cloud Browser Isolation regions

8. Use the default **End User Notification (EUN)**. However, you can create a customized EUN in the **Administration** section of the Cloud Browser Isolation Portal and add it to the profile. To complete the profile:

   a. Select **Create Profile**.

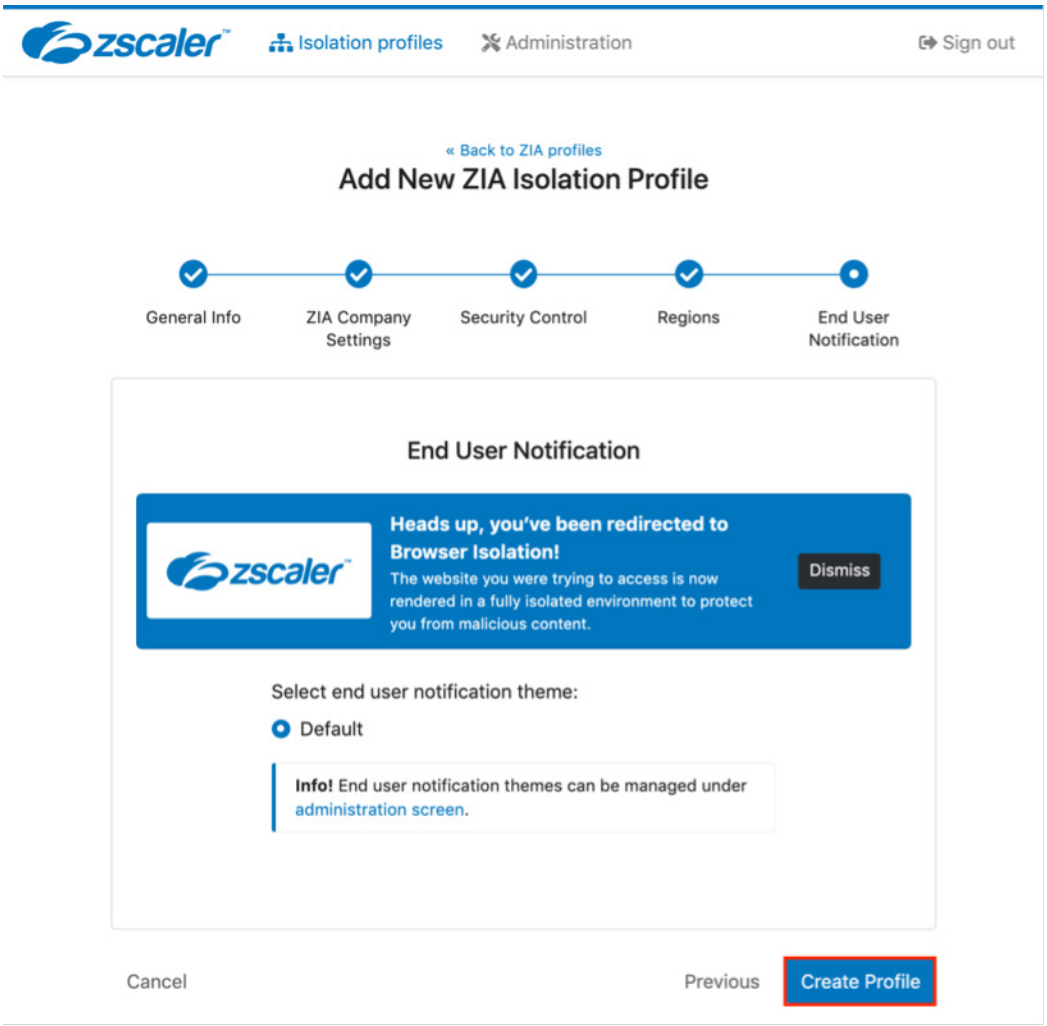


Figure 34. Cloud Browser Isolation EUN

The completed Zscaler Cloud Browser Isolation profile appears as a profile option when setting up isolation policies in ZIA.

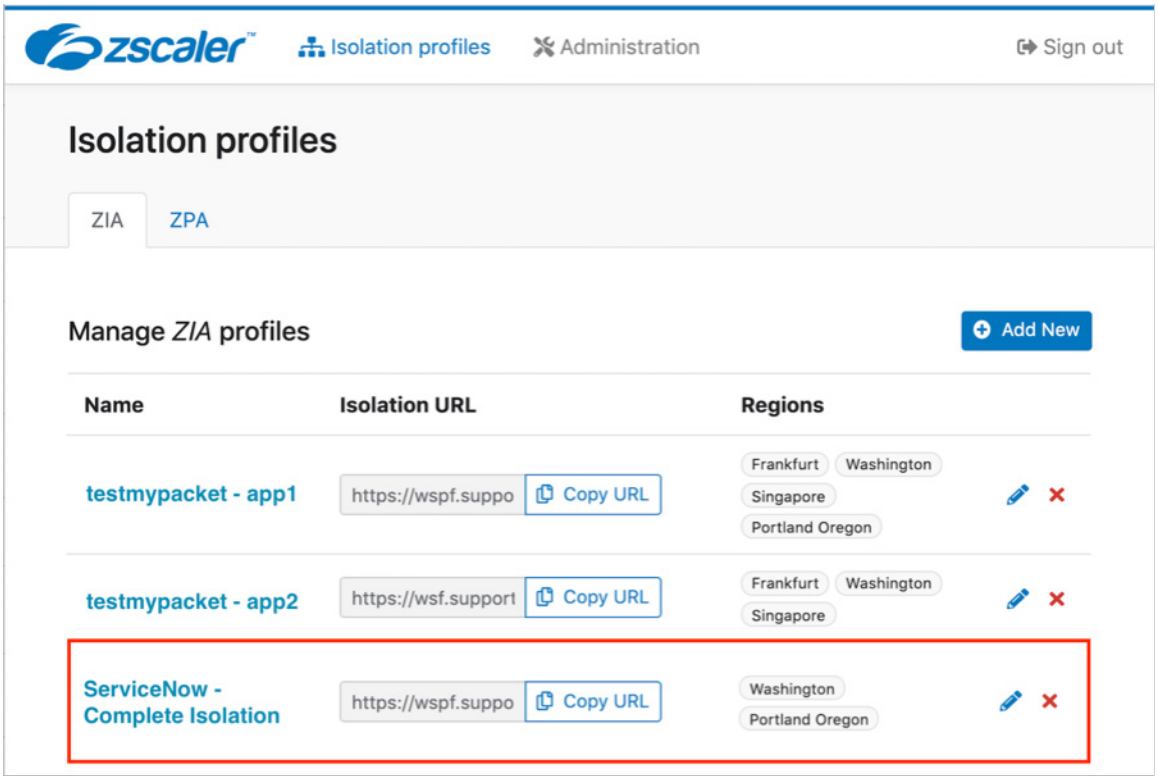


Figure 35. The completed Cloud Browser Isolation profile

Configure the Cloud Browser Isolation Policies

To move to next steps, launch your ZIA Admin Portal and sign in with administrator credentials:

1. Launch your ZIA Admin Portal.
2. Log into the Zscaler tenant with administrator credentials.

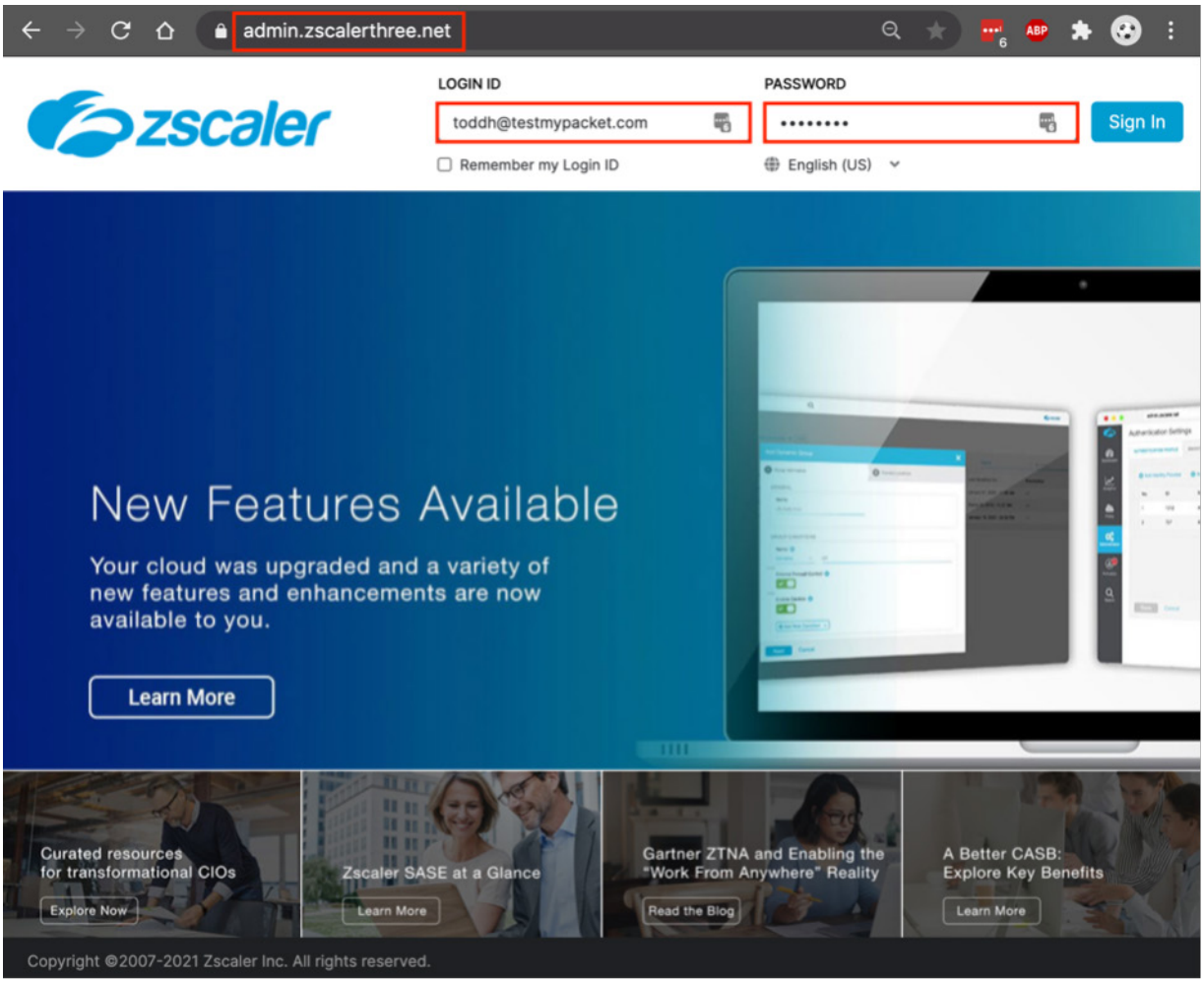


Figure 36. Configure Cloud Browser Isolation policies

3. To configure policies that redirect ServiceNow traffic to Cloud Browser Isolation, launch the **URL Filtering** wizard:
   a. Select **Policy**.
   b. Select **URL & Cloud App Control**.
   c. Select **Add URL Filtering Rule**.

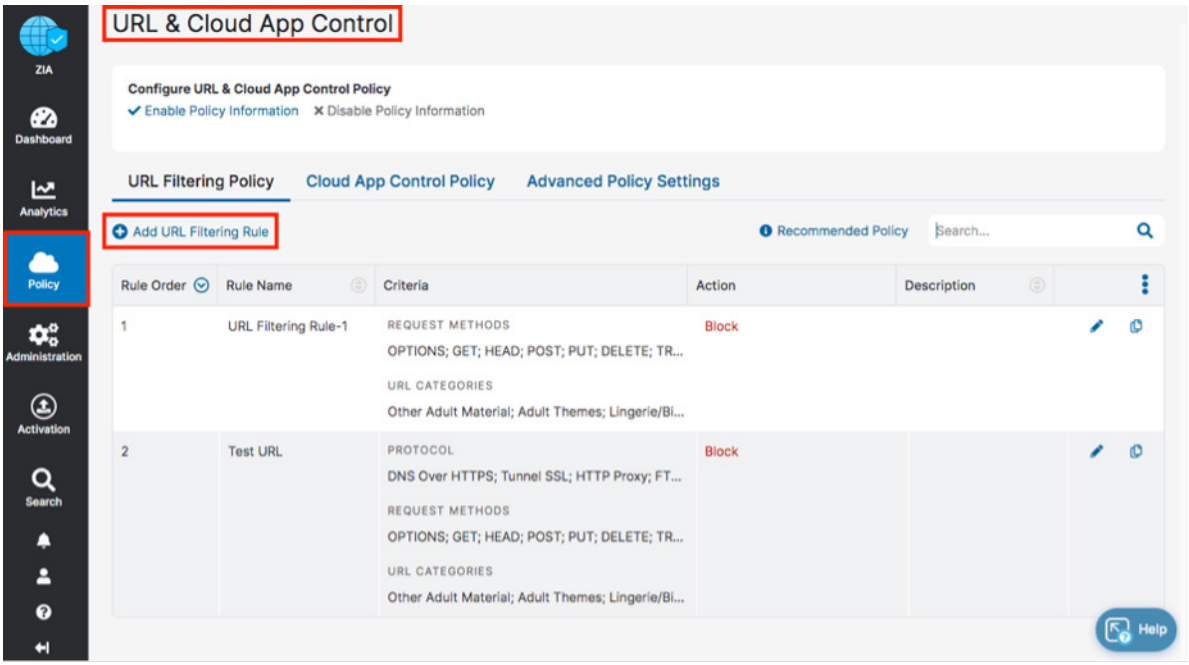


Figure 37. Configure Cloud Browser Isolation policies

4. In the **URL Rule** wizard:
   a. Select the **Rule Order**.
   b. **Name** the rule in the **Rule Name Field**.
   c. **Enable** the rule.
   d. Select the drop-down arrow in the **URL Categories** field.
   e. Select the **Add** icon next to the **Search** field on the **URL Selection** screen (new dialog).
   f. Select **Done**.
   g. Select **Save**.

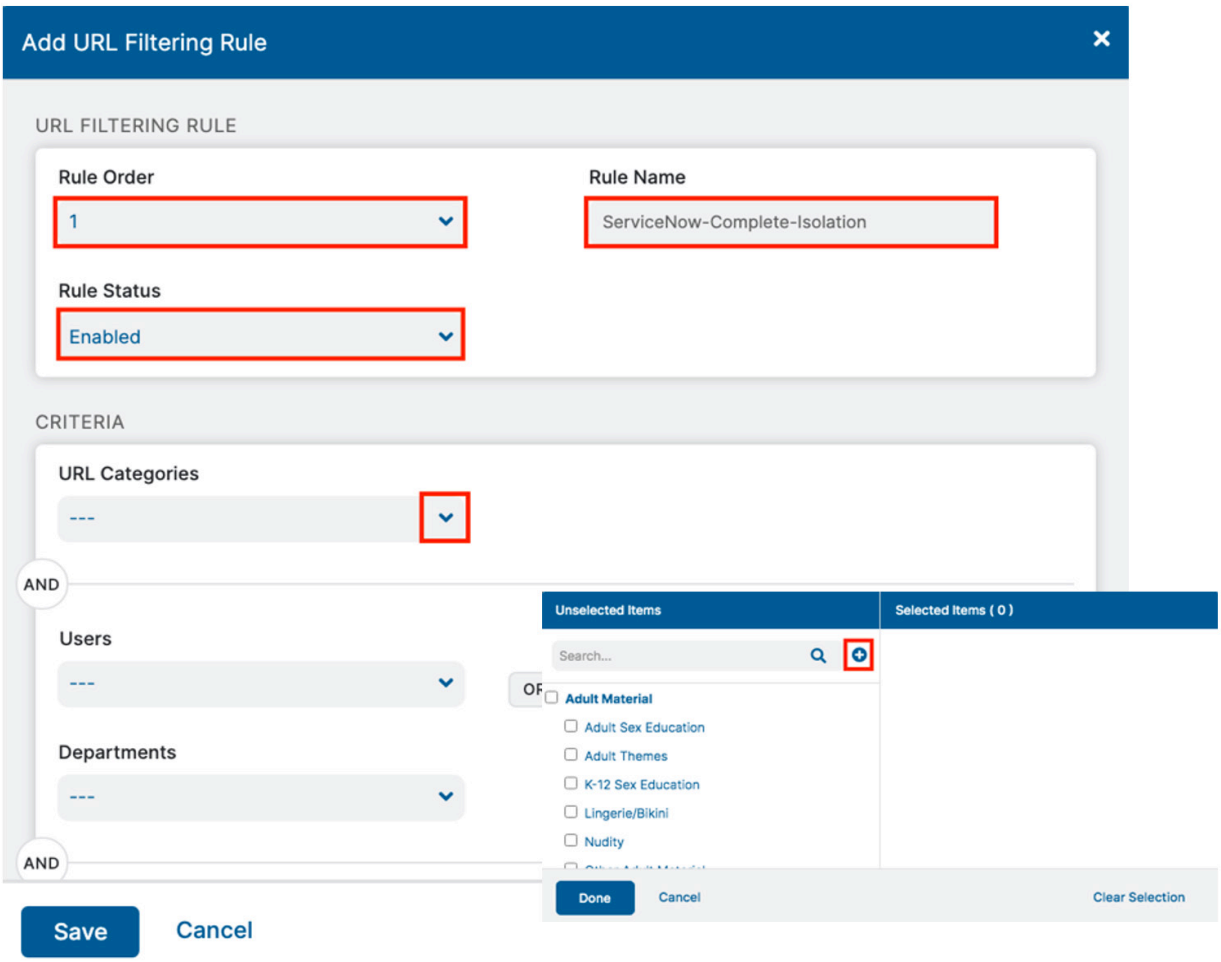


Figure 38. Configure Cloud Browser Isolation policy

5. The **Add URL Category** wizard is displayed. Add the two ServiceNow URLs as Custom URLs:
   a. Name the **URL Category.**
   b. Add `.servicenow.com` and `.service-now.com` by typing the domain in the **Add Items** field and selecting Add Items, one at a time. Leave the period preceding the URL to act as a wildcard for the domain.
   c. Click **Save.**

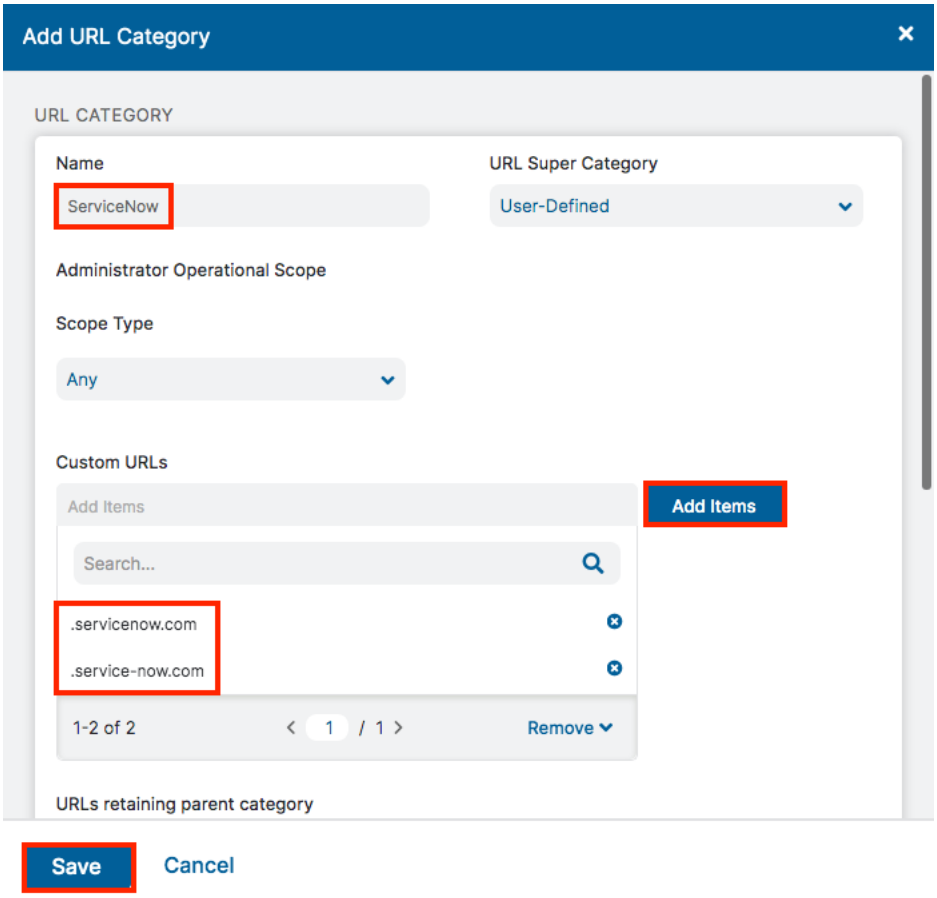


Figure 39. Configure Cloud Browser Isolation

6. Scroll down the wizard to fill in the remaining fields:
    a. For **Request Methods**, select **CONNECT**, **GET**, **HEAD**, and **TRACE.**
    b. For **Protocols**, select **HTTP** and **HTTPS.**
    c. For **User Agent**, select your organization's specific browsers for use with browser isolation.
    d. Click **Save**.

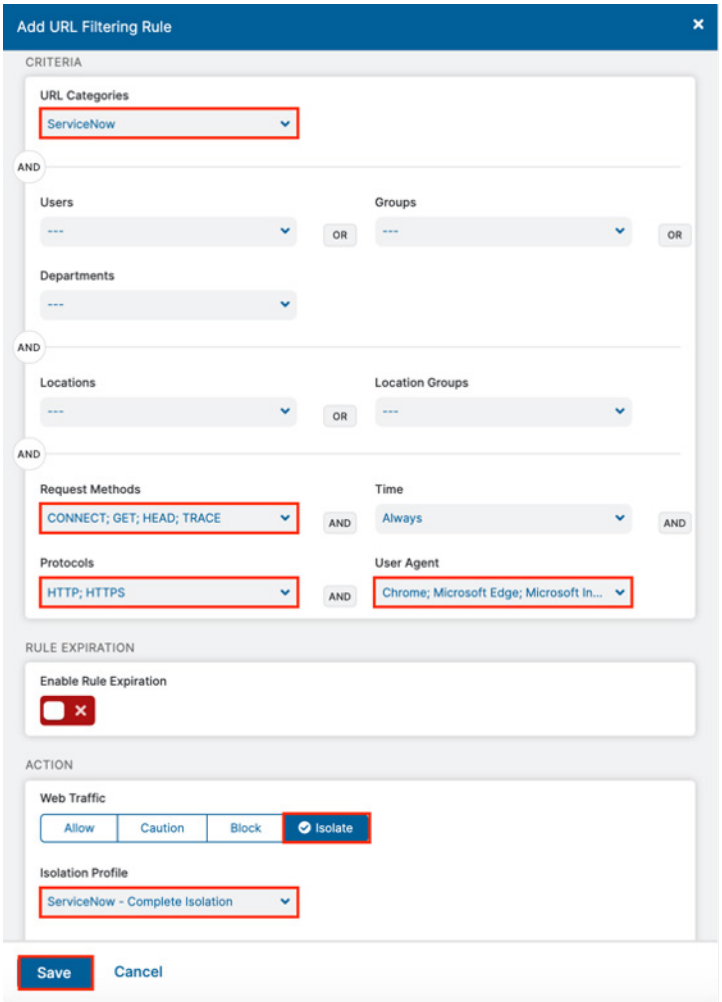


Figure 40. Configure Cloud Browser Isolation

The completed browser isolation profile is displayed.

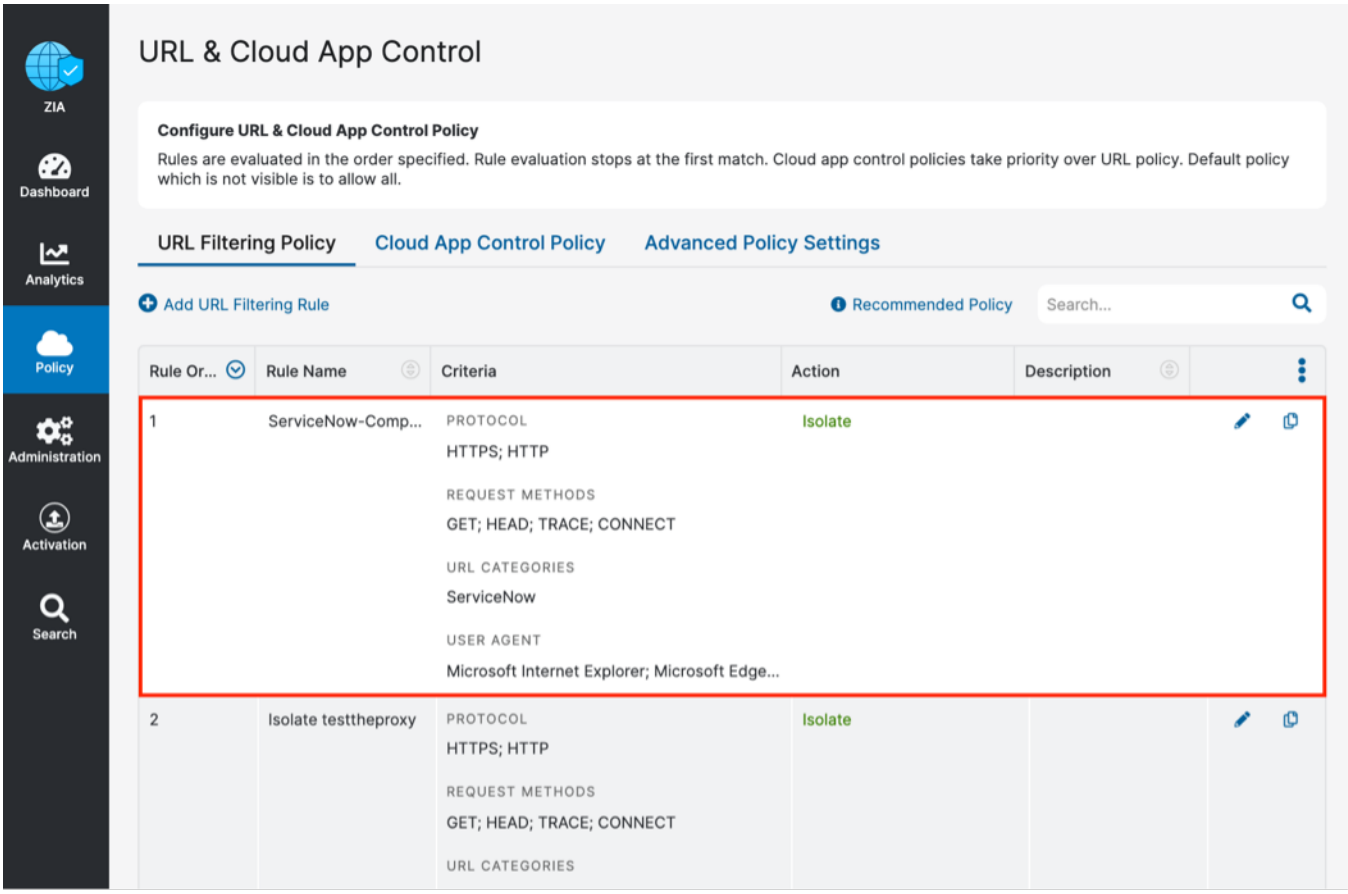


Figure 41. Completed Cloud Browser Isolation profile

Configuring the ServiceNow Tenant

Log into your ZIA tenant with admin credentials to start the installation process. Your Zscaler cloud instance might be different from the example.

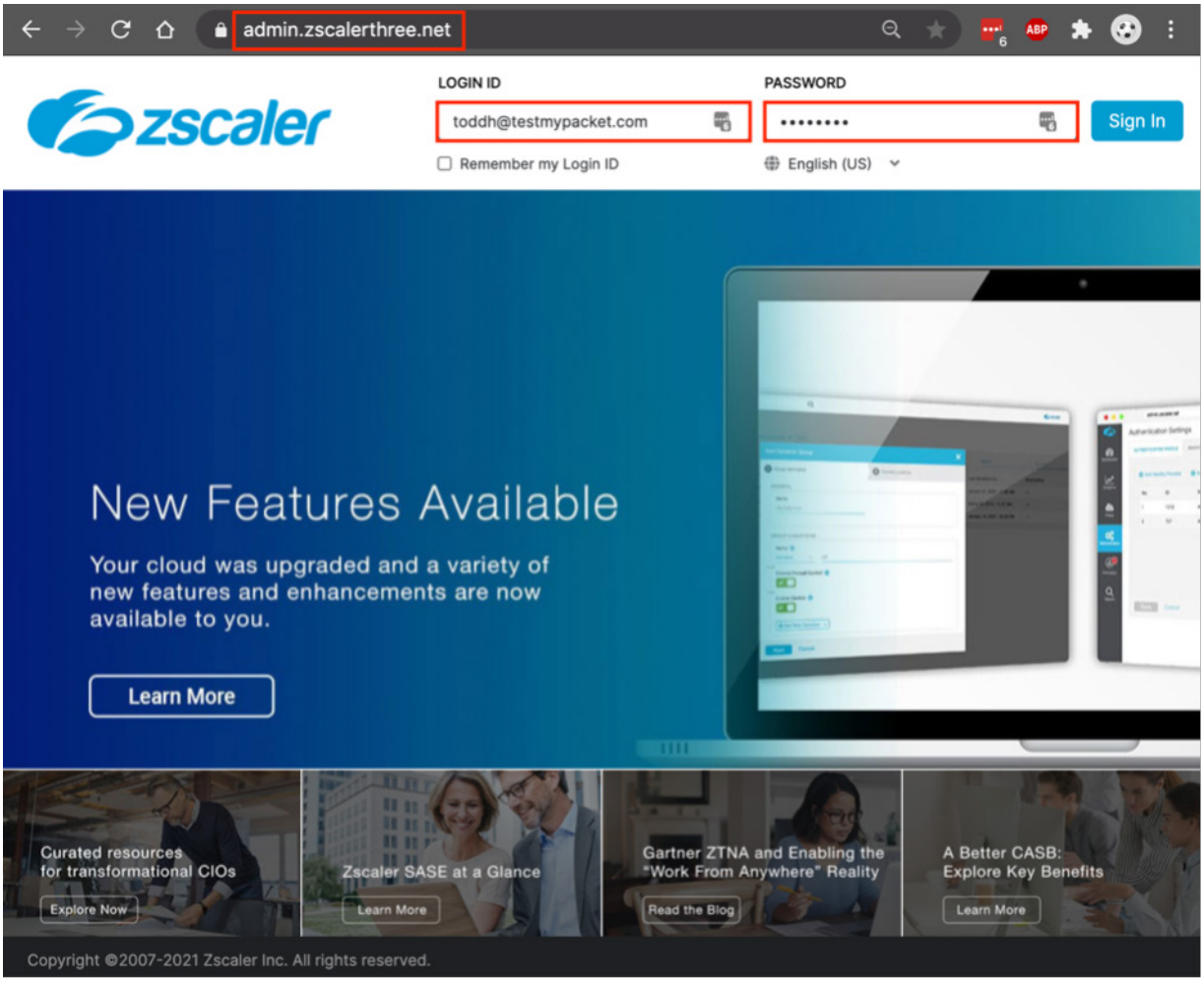


Figure 42. ZIA Admin Portal

Adding the ServiceNow Tenant

To launch the SaaS Application Tenants wizard for the ZIA Admin Portal:

1. Go to **Administration** > **SaaS Application Tenants**.
2. In the **SaaS Application Tenants** dialog, select **Add SaaS Application Tenant**.

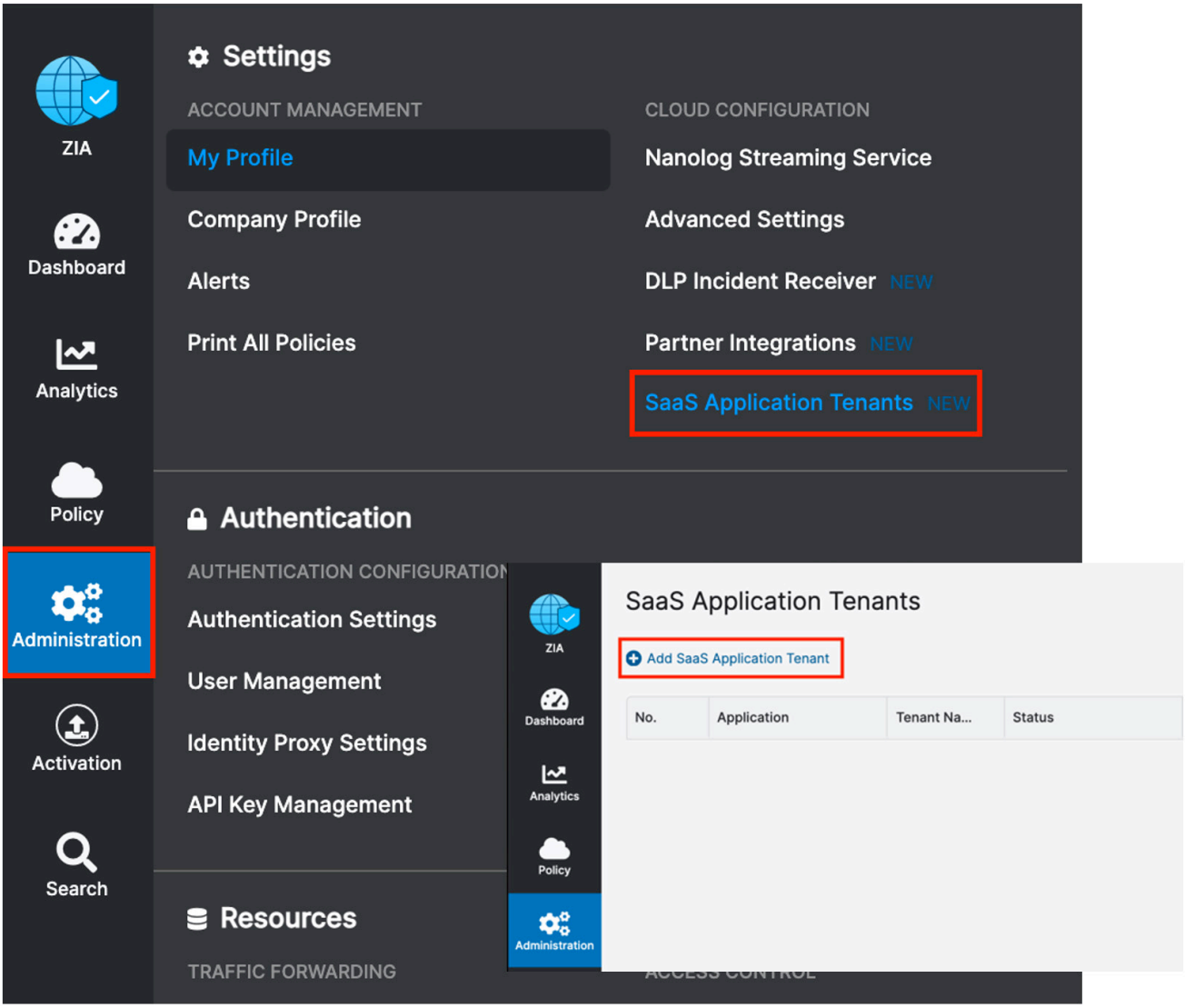


Figure 43. ZIA SaaS application tenant

SaaS Tenant Configuration Wizard

To start the wizard:

1. Select **Add SaaS Application Tenant** on the tenant page.
2. Select the **ServiceNow** tile on the wizard.

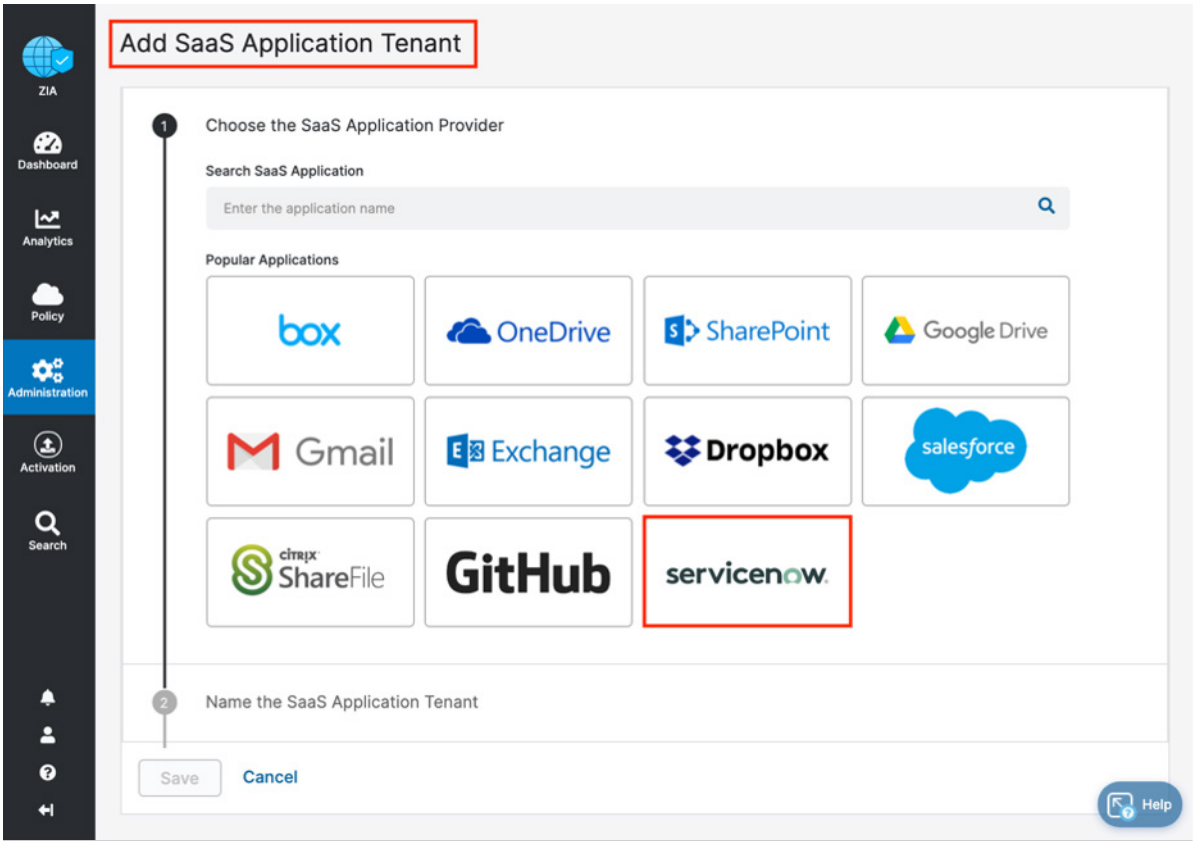


Figure 44. The SaaS tenant configuration wizard

3. Give the ServiceNow tenant a name. This is the name that is selected when assigning a policy for the Zscaler security features:

   a. Enter a name for the **Tenant Name**.

   b. Open a new browser tab and login to your ServiceNow tenant with admin role credentials.

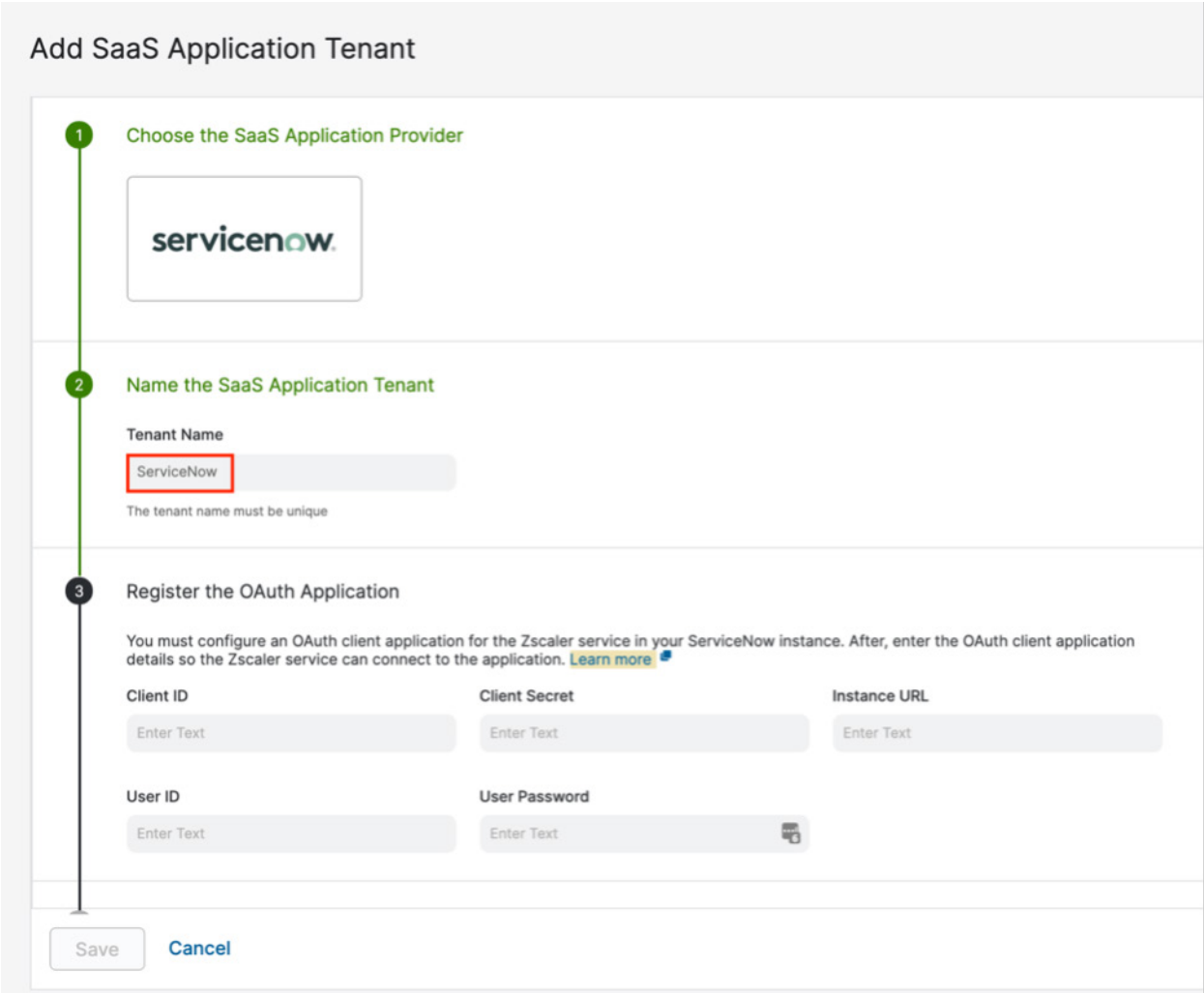


Figure 45. Open the ServiceNow tenant

Configuring the Zscaler Tenant on ServiceNow

The following steps are based on procedures documented on the ServiceNow website. To configure the Zscaler tenant from your ServiceNow admin account:

1. Log in to ServiceNow with administrator credentials.

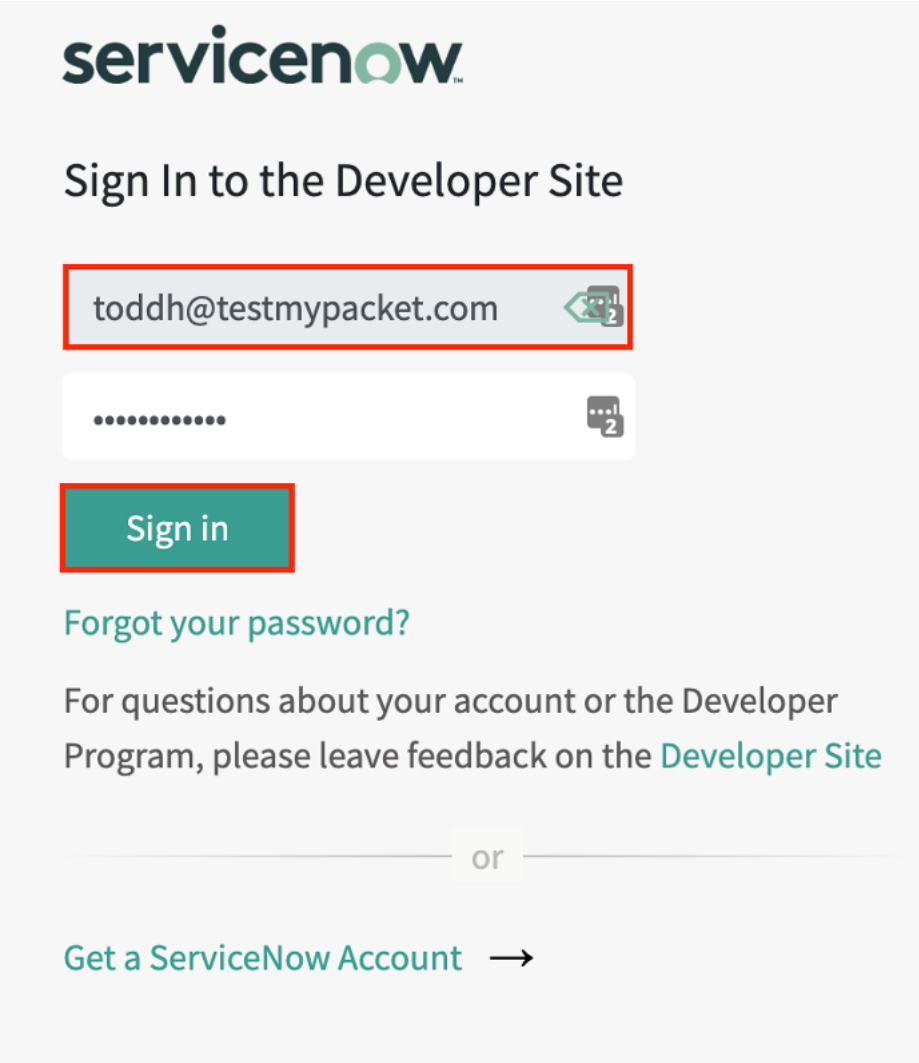


Figure 46. Log in to the ServiceNow tenant

2. Verify OAuth is running, and start it if it is not **Active**:
   a. On the left-side navigation, select the **File Box** at the top of the browser, under the **Filter Navigator**.
   b. Scroll down and select the arrow next to **All Available Applications**.
   c. Select **All**.
3. This displays the **All Applications** page:
   a. In the search box, type `Oath 2.0`.
   b. Verify OAuth is installed.
4. If OAuth is not installed:
   a. Select **Install**.
   b. Select **Activate**.

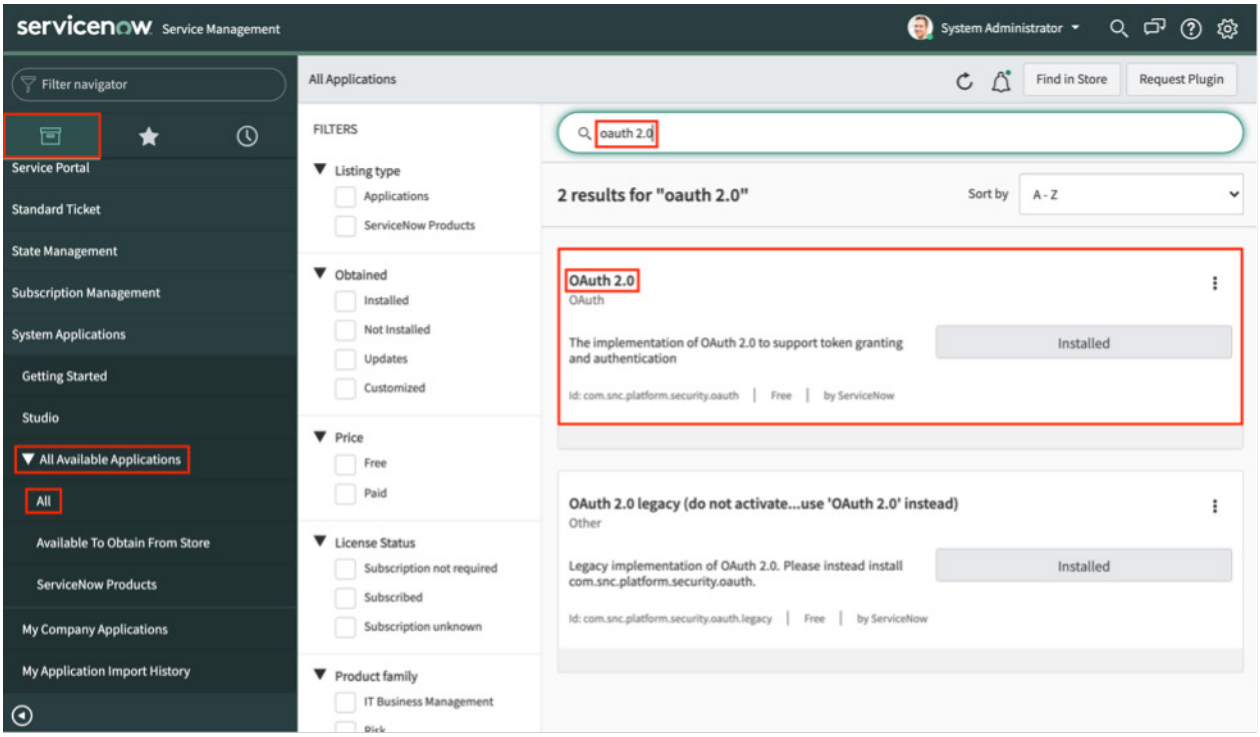


Figure 47. Verify OAuth is installed

Check that OAuth is Installed and Active

Check to see if OAuth 2.0 is installed. Click the name OAuth 2.0 on the OAuth application. This displays the Status page of the OAuth 2.0 application.

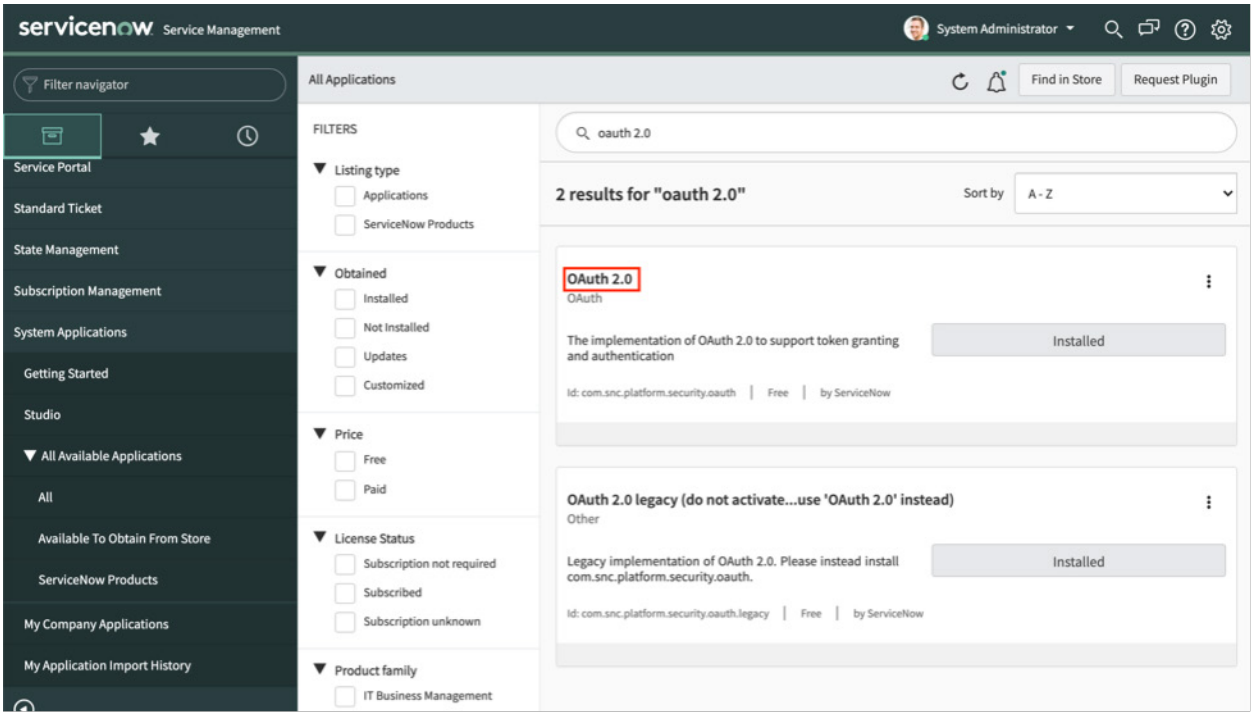


Figure 48. The installed Zscaler SaaS connector

Check that the OAuth Plugin is Active

Check that the status of OAuth 2.0 is Active.

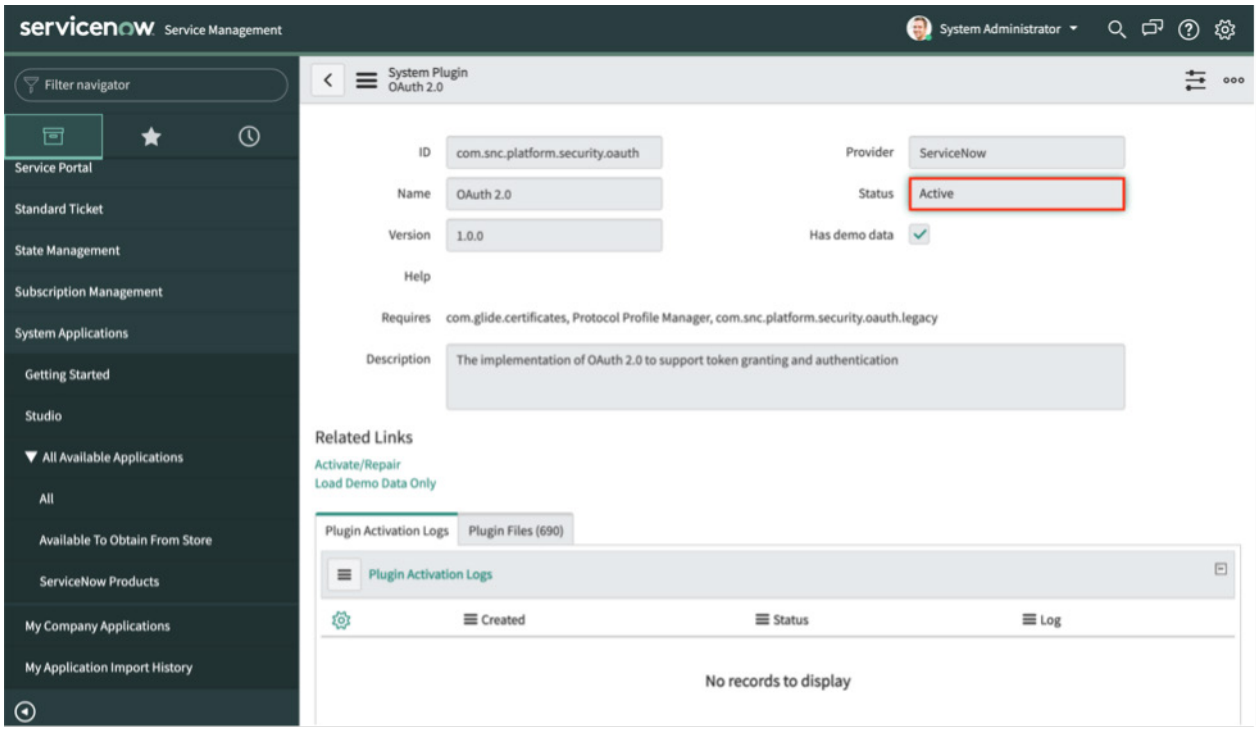


Figure 49. OAuth plugin status

Create an OAuth Application Registry

Create an OAuth application registry for the Zscaler tenant:

1. On the left-side navigation, select the file box at the top of the browser, under the **Filter Navigator**.
2. Scroll down and select **System OAuth**.
3. Select **Application Registry**.
4. Click **New**.

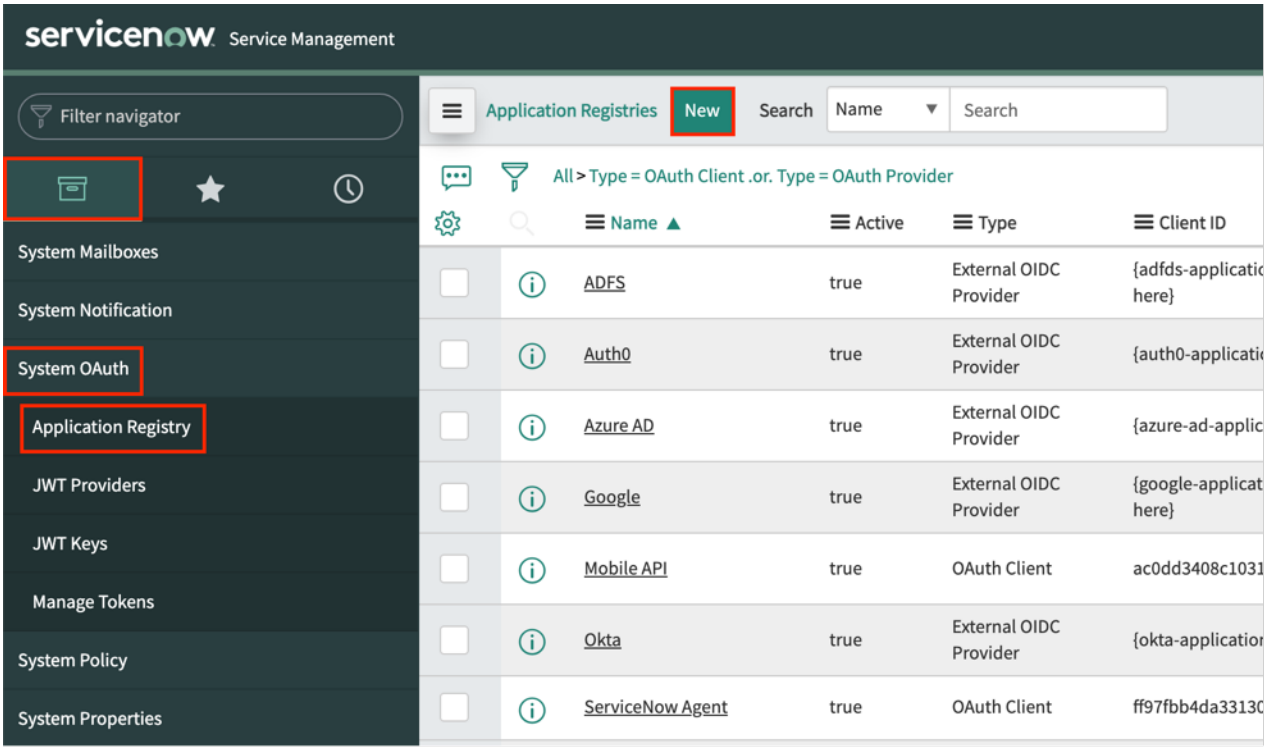


Figure 50. Creating an Application Registry

Create an OAuth Application Registry

In the **What kind of OAuth Application?** window, select **Create an OAuth API endpoint for external clients**.

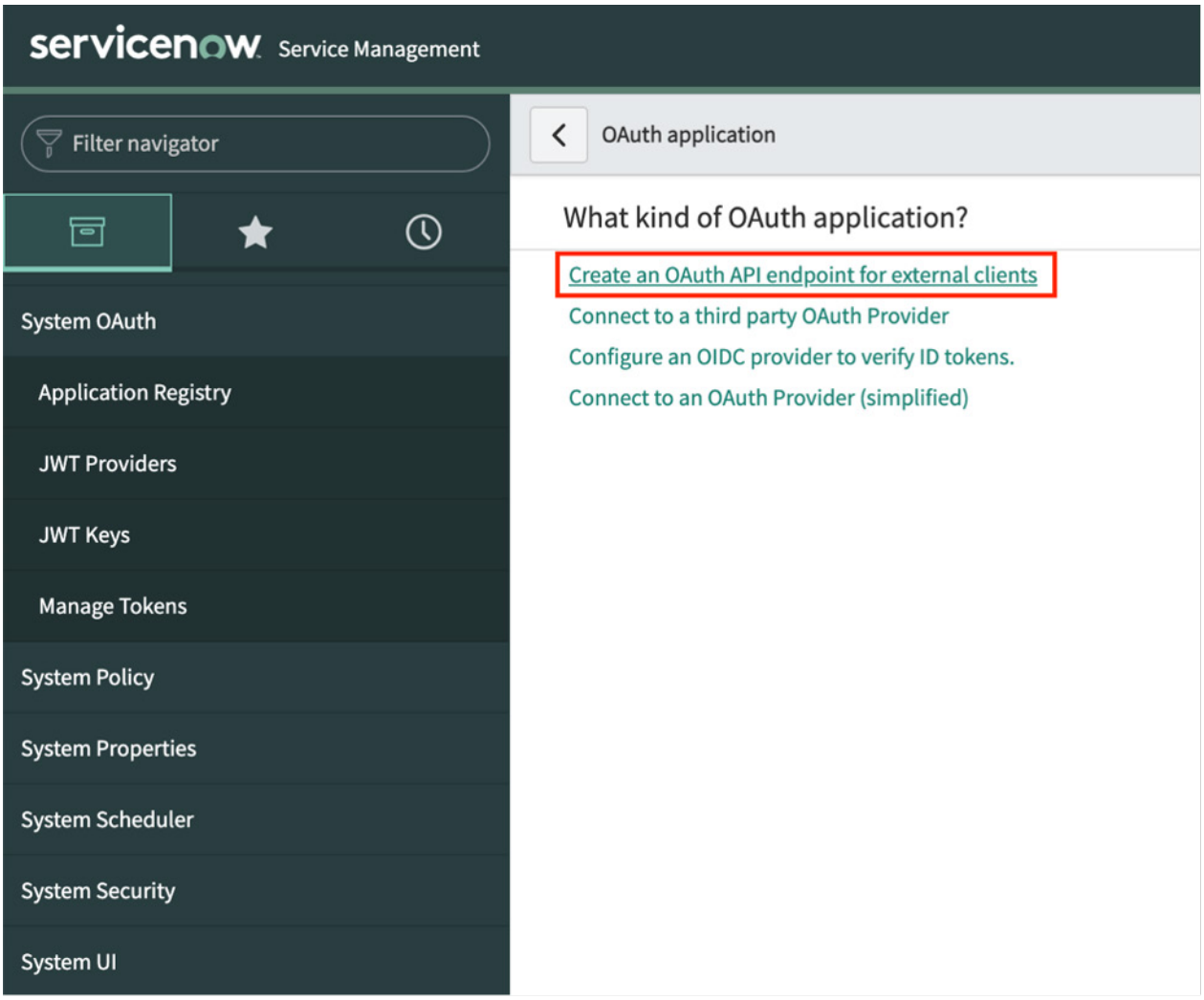


Figure 51. Create an OAuth API endpoint

Configuring the Zscaler Tenant on ServiceNow

Complete the OAuth API endpoint details:

1. Type `Zscaler` (or another name) for the name of the endpoint.
2. Enter the **Refresh Token Lifespan** in seconds. 157,700,000 is five years, at which point the tenant has to be reinstalled.
3. Enter the **Access Token Lifespan** in seconds. Zscaler recommends 86,400 (24 hours).
4. Click **Submit** to save the settings.

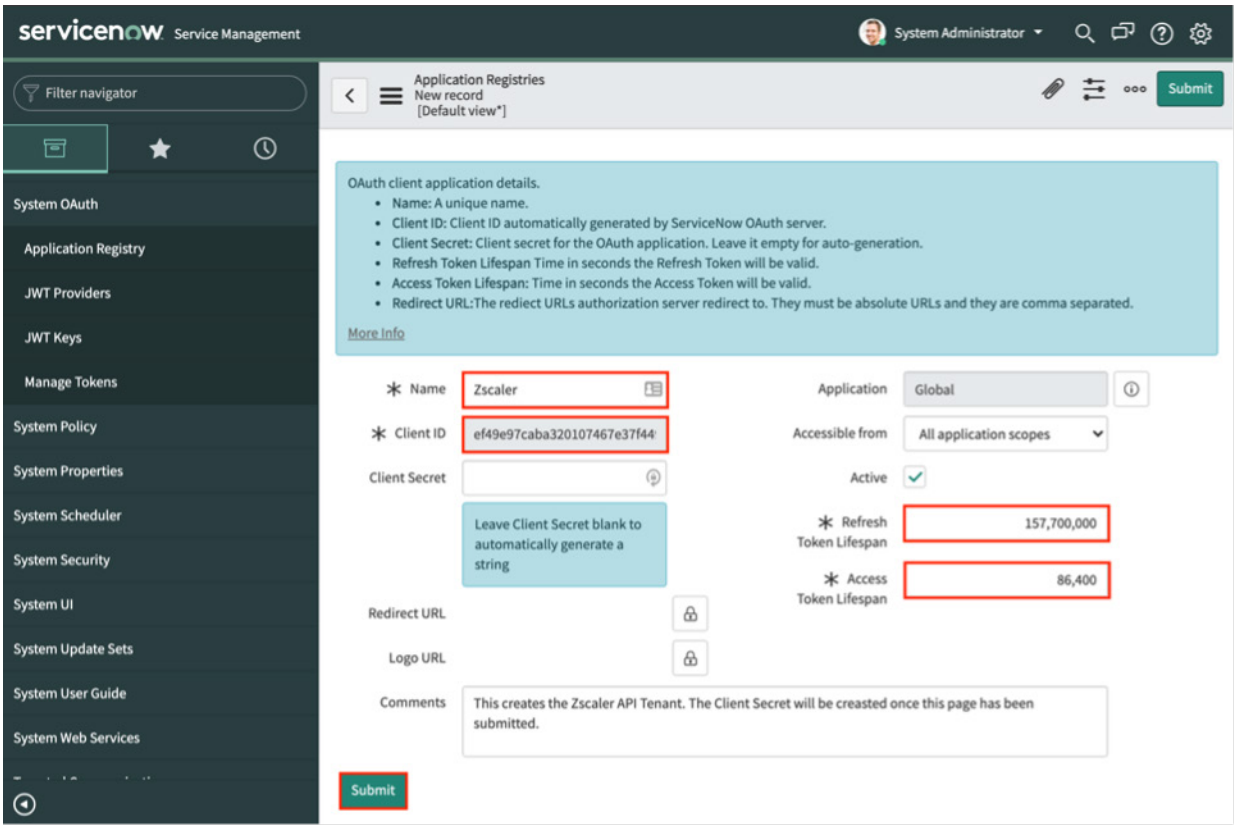


Figure 52. Creating the OAuth endpoint

The **Client Secret** is created after the detail is submitted. Then return to the endpoint to copy it for the Zscaler configuration.

5. Once the Zscaler endpoint is created, select the Zscaler endpoint to open the settings to copy the **Client Secret**.

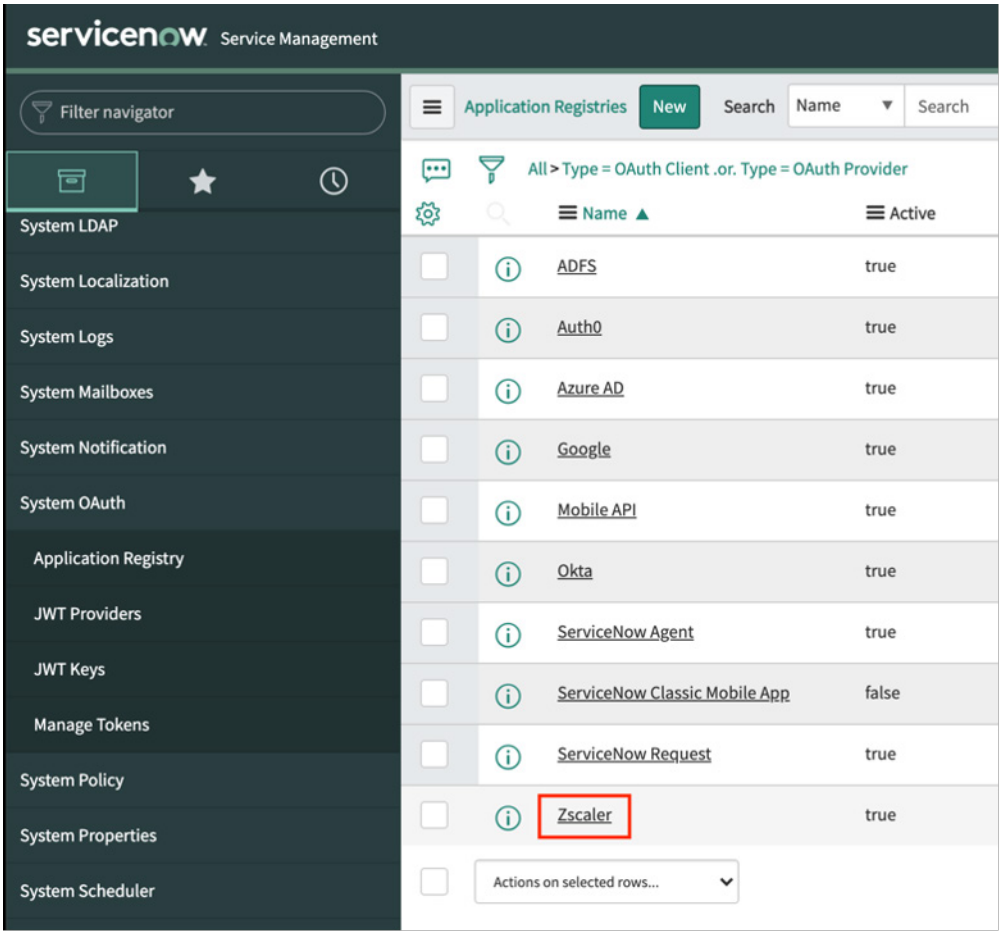


Figure 53. The Zscaler endpoint

Copy the needed OAuth Credentials

Copy the OAuth credentials required to finish the Zscaler side of the installation:

1. Copy the **Client ID**.
2. Select the lock next to the **Client Secret** to reveal the secret.
3. Copy the **Client Secret**.

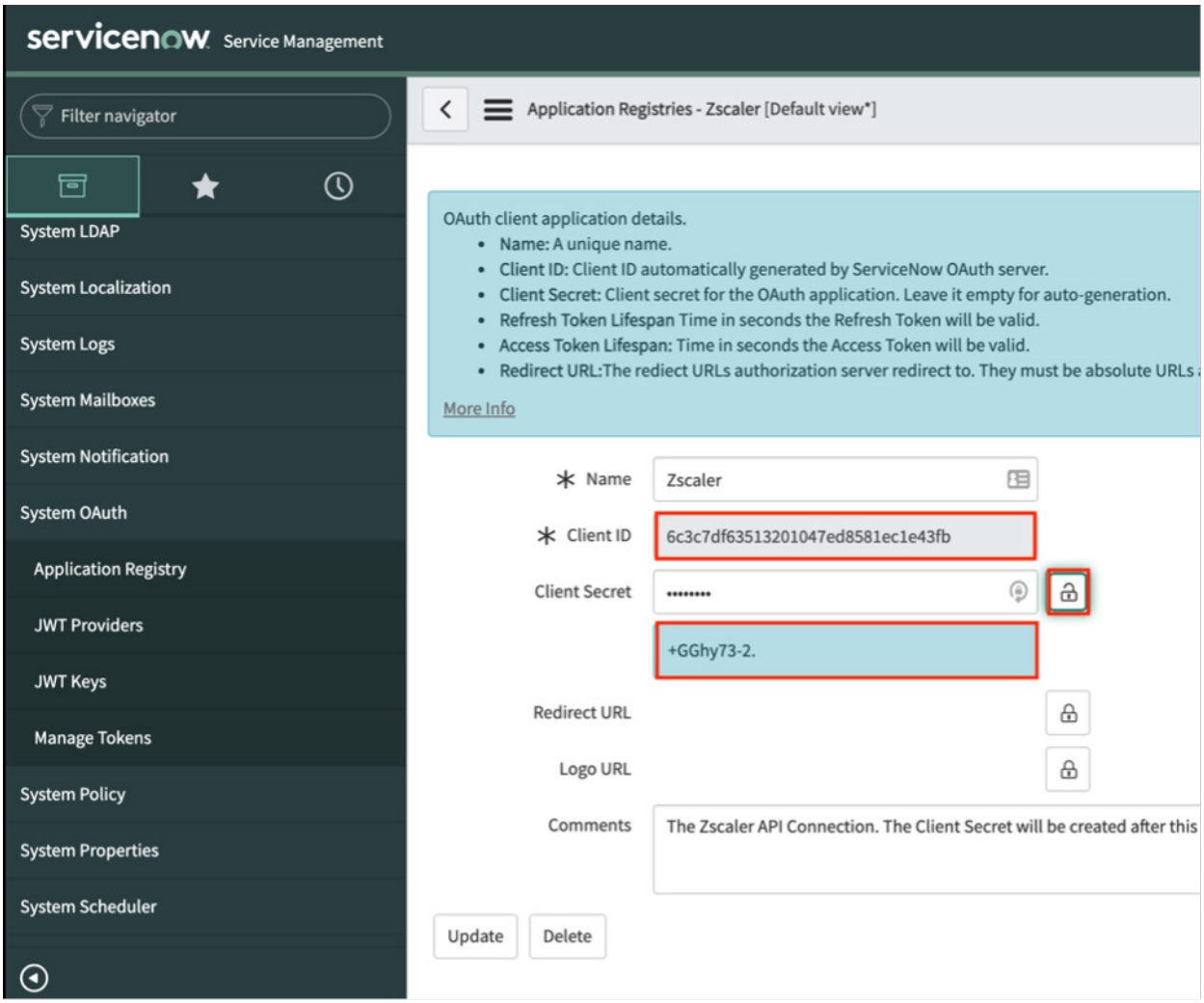


Figure 54. Client ID and Client Secret

Finishing the Zscaler Tenant on the ZIA Admin Portal

Enter the information copied from the ServiceNow Tenant:

1. Enter the ServiceNow **Client ID**.
2. Enter the ServiceNow **Client Secret**.
3. Enter the ServiceNow **Instance URL**.
4. Enter the ServiceNow **User ID** and **Password**.
5. Enter the **ServiceNow Admin Email ID**.
6. Click **Authorize** to verify the credentials.
7. Click **Save**.

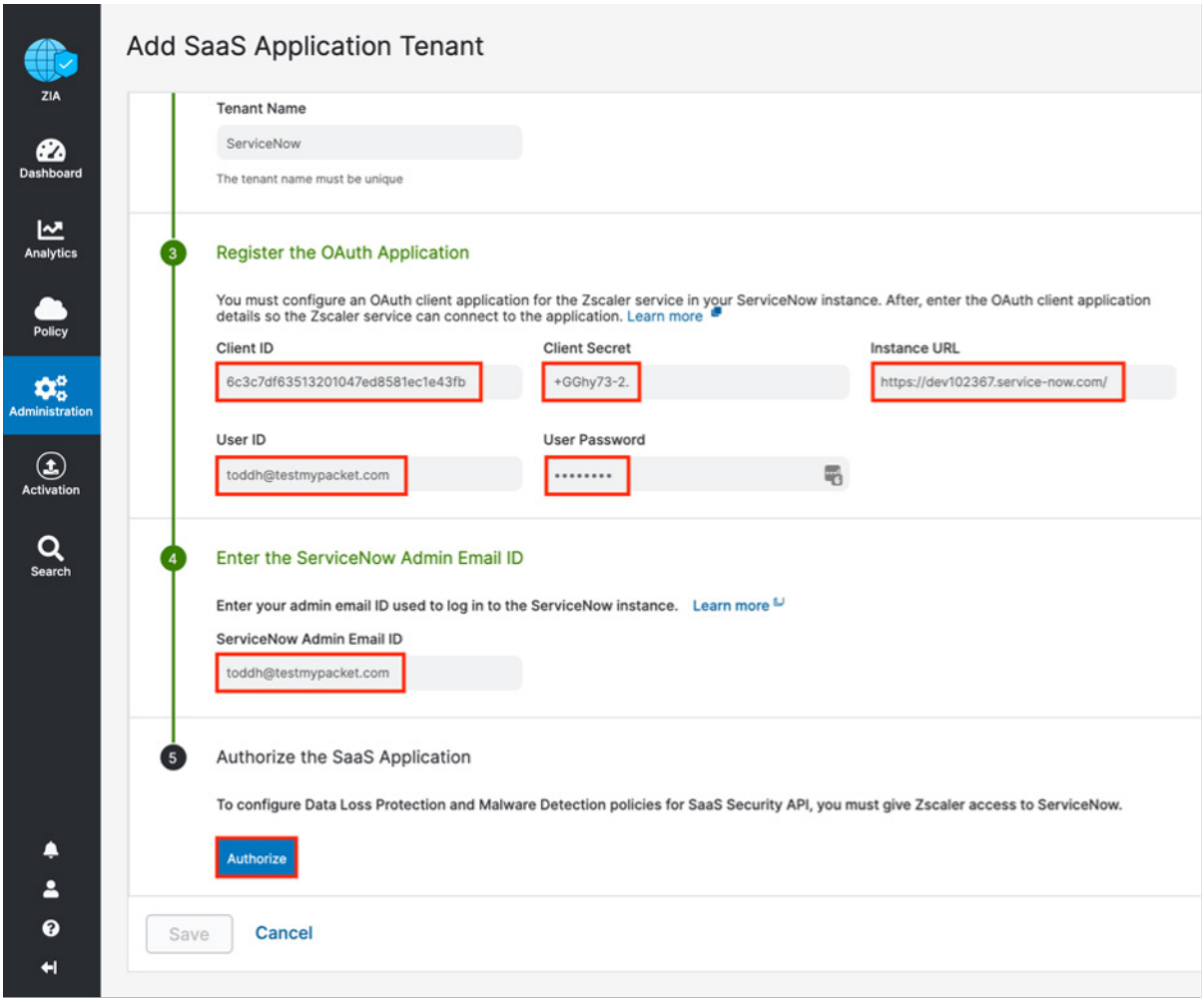


Figure 55. Finish the Zscaler tenant

Configuring the Zscaler ServiceNow Connector

The completed and active ServiceNow API connector is displayed.

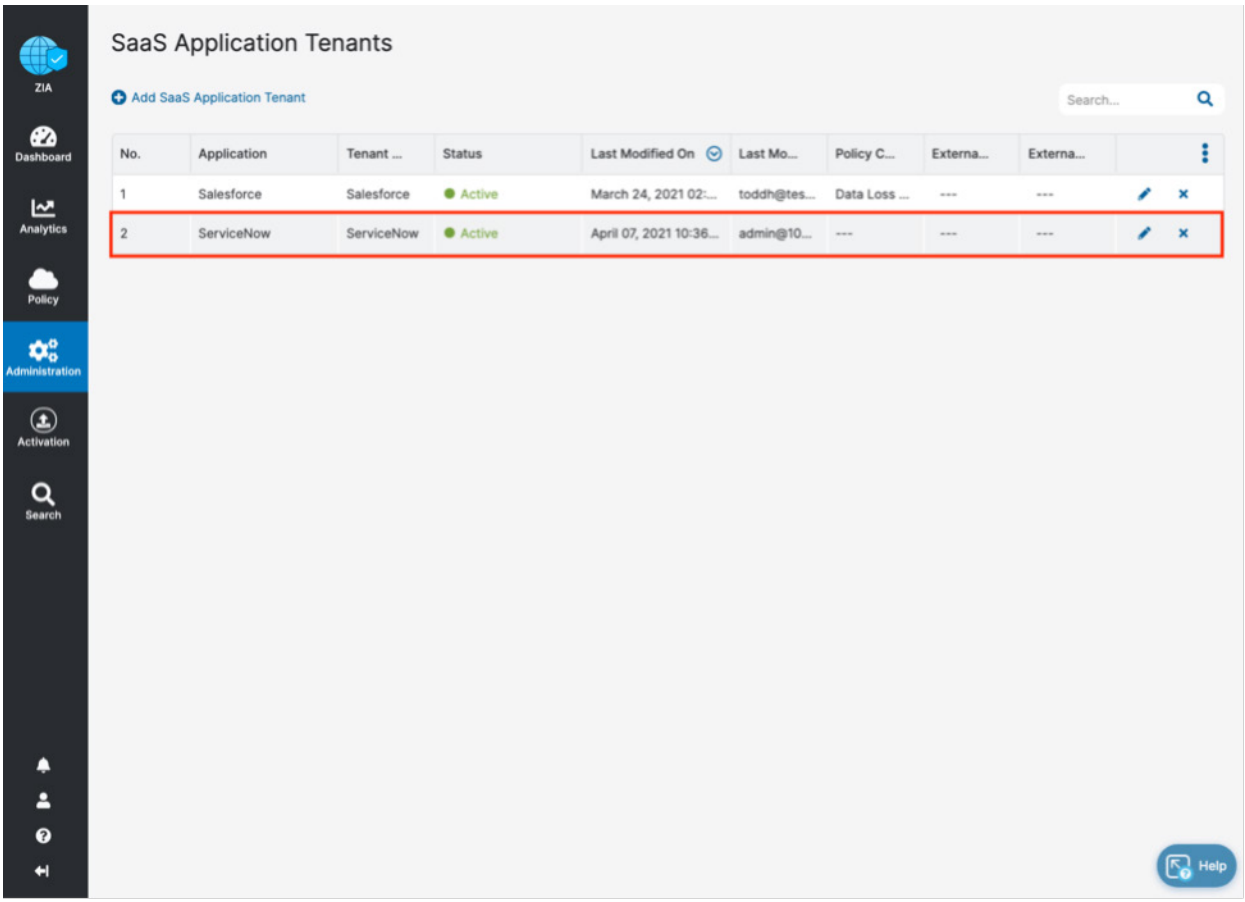


Figure 56. The completed and active ServiceNow tenant

Configuring ServiceNow Policies and Scan Configuration

After adding and configuring the ServiceNow tenant, you can configure the SaaS Security API control DLP and malware policies, and then scan the configuration for the policies. You can also view reports and data for ServiceNow in analytics, SaaS security insights, and logs.

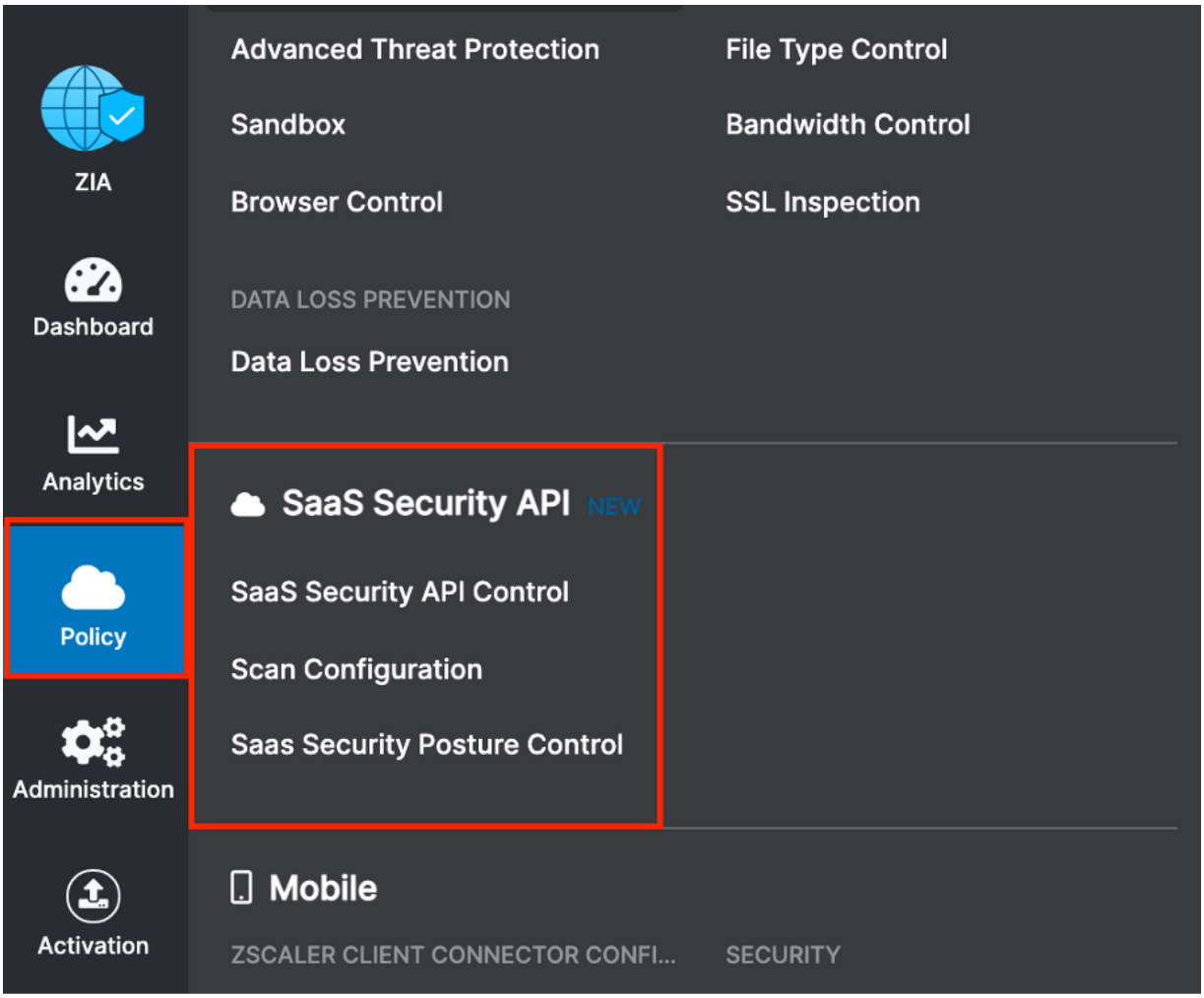


Figure 57. Zscaler policy configuration

Scoping the Policies and Remediation

Zscaler SaaS security scans file attachments. This deployment guide configures a basic DLP policy and a malware policy. The policies scan the ServiceNow account attachment files for matching content of the DLP policy and known malware for the malware policy. A ServiceNow incident was created with malicious attachments and DLP violations to test the policies.

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.

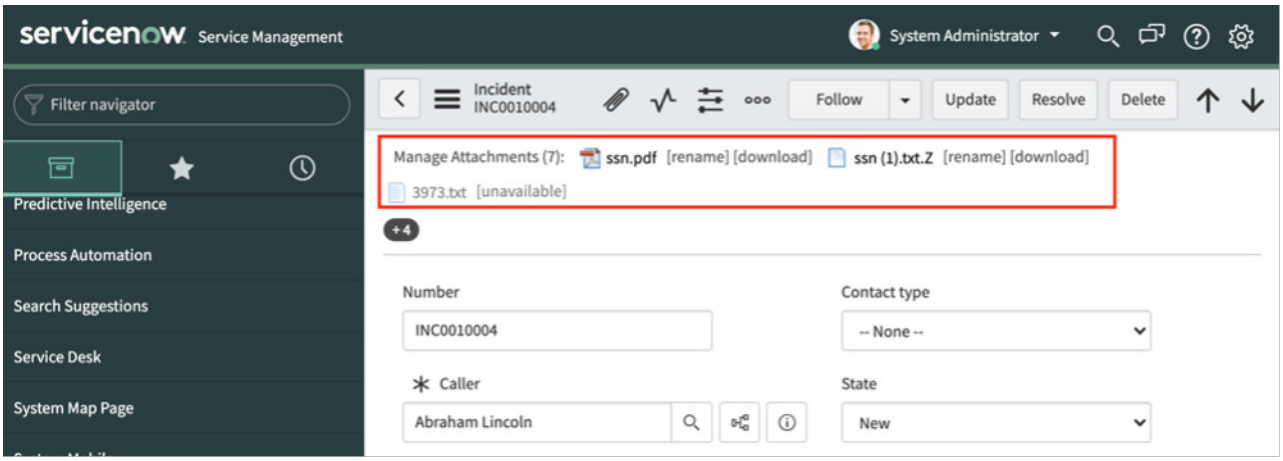


Figure 58. ServiceNow incident with malicious attachments

The DLP policy creates a very broad DLP policy 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 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 SaaS DLP protection is only part of the Zscaler DLP solution and is used to scan data-at-rest (like the ServiceNow files). This deployment doesn't cover inline data protection, exact data match, or indexed document matching (document template fingerprinting), although they are integral pieces of a complete data protection solution.

For next steps to test the DLP SaaS functionality, create a basic policy and apply it to the ServiceNow tenant. If you already have DLP policies created, skip ahead to Configure a SaaS Malware Policy.

Creating a DLP Policy

Create a custom dictionary (or use the available dictionaries) to identify the data the scan is going to look for.

Then 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 violations and eliminate false positives.

A SaaS security DLP policy is created that allows you to specify the detail about where, when, the action taken, and whom to inform about violations:

1. In the ZIA Admin Portal, go to **Administration** > **DLP Dictionaries** > **Engines**.
2. Identify and select the dictionary to use (in this case, **SSN with Dashes**).

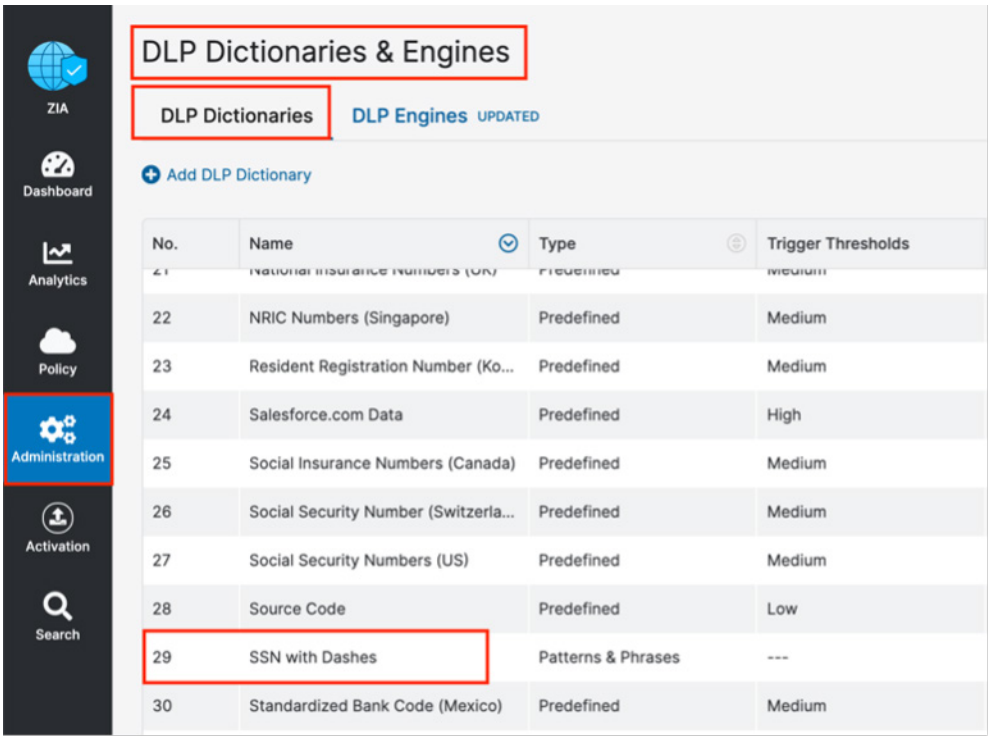


Figure 59. Creating a DLP dictionary

Creating a DLP Engine

To create the DLP engine:

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

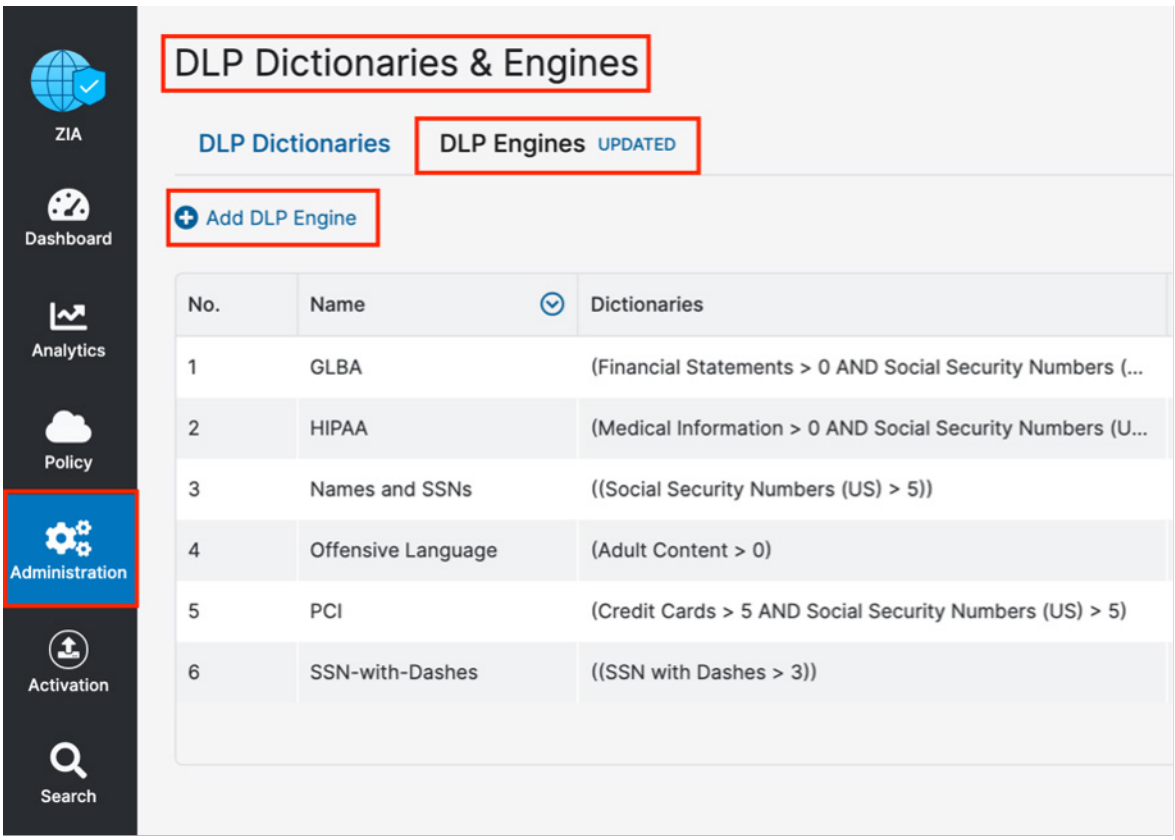


Figure 60. Creating a DLP engine

Creating a DLP Engine

In the Add DLP Engine window:

1. Give the DLP engine a **Name**.
2. In the **Engine Builder** under **Expression**, select the first dictionary.
3. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
4. Click **ADD** to add the next dictionary and repeat the process.
5. Click **Save**, then **Activate** the configuration.

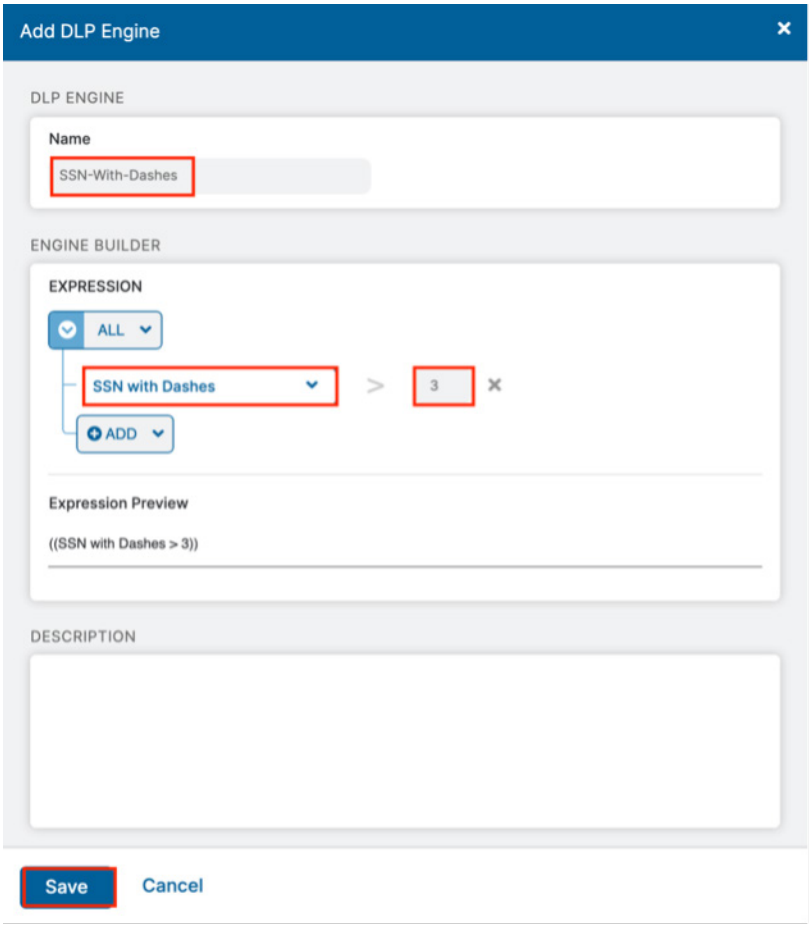


Figure 61. The DLP engine wizard

This policy triggers when you see the fourth Social Security number. Again, this is a demonstration and the criteria is too general to be a production DLP rule.

Configure a SaaS DLP Policy

Apply the engine to a DLP policy used for the ServiceNow instance. Launch the Add DLP Rule wizard to start the process:

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

See the details of the policy on the following pages.

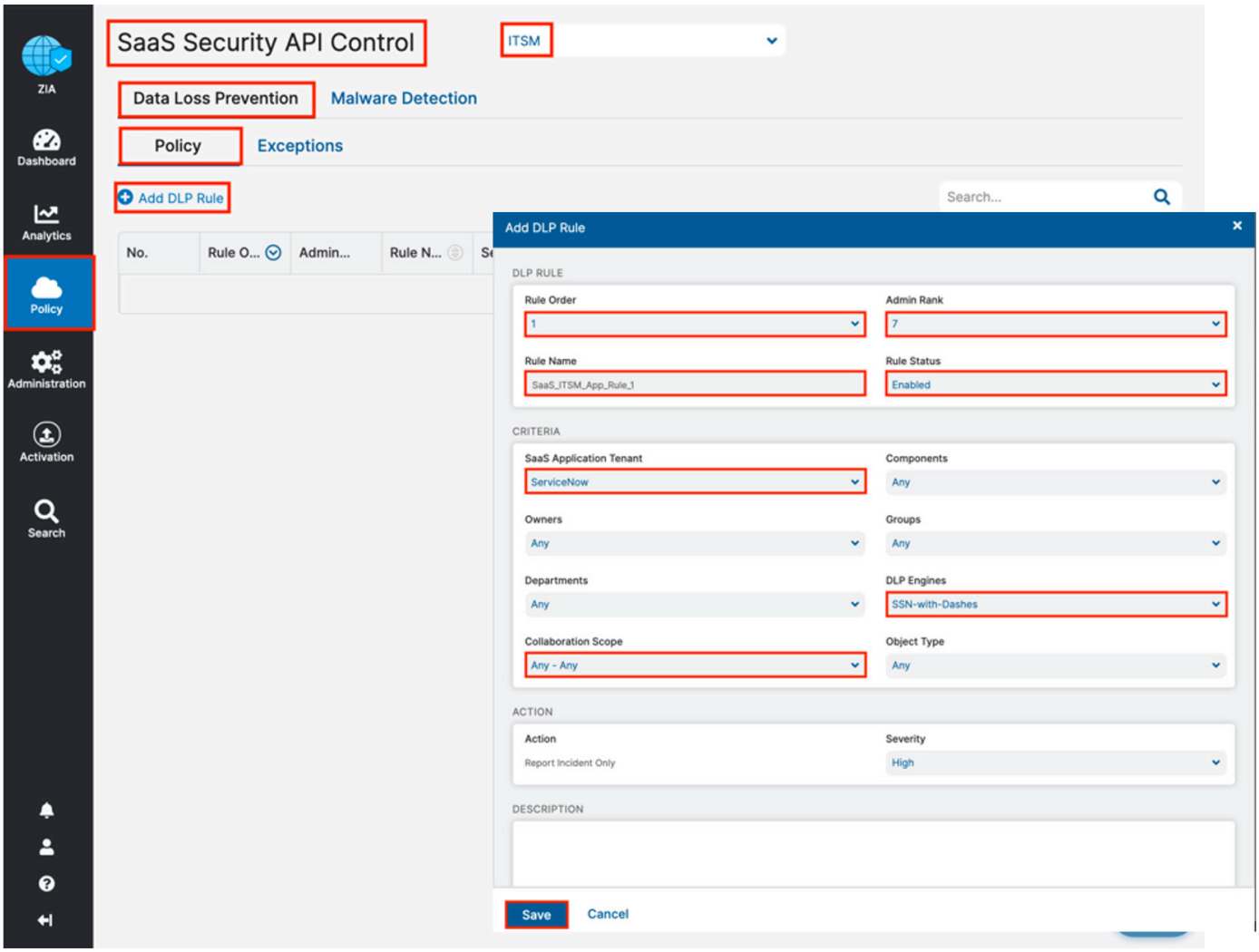


Figure 62. Launch the SaaS DLP Policy Configuration Wizard

SaaS DLP Policy Details

The SaaS DLP policy is like all Zscaler policies where you specify the detail on whom this policy, and to what data this policy, applies. You specify the rule order if you have multiple DLP policies, which are processed in an ascending manner. The first rule that matches is the applied rule. Specify the DLP engine you defined, any file owners, groups or departments, and the file types to inspect. The collaboration scope and the action are unique to the SaaS DLP. Select Any Collaboration, and an Action of Remove Sharing.

The Collaboration Scope includes 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 ServiceNow, the action is Report 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 a SaaS DLP Policy

To finish the 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 **ServiceNow SaaS Tenant**.
5. Select the **DLP Engine** created in [SaaS DLP Policy Details](#).
6. Select **Any-Any** for the **Collaboration Scope**.
7. Select **High** as a **Severity** to allow for identification for searches and tracking.
8. Click **Save** and then **Activate** your configuration.

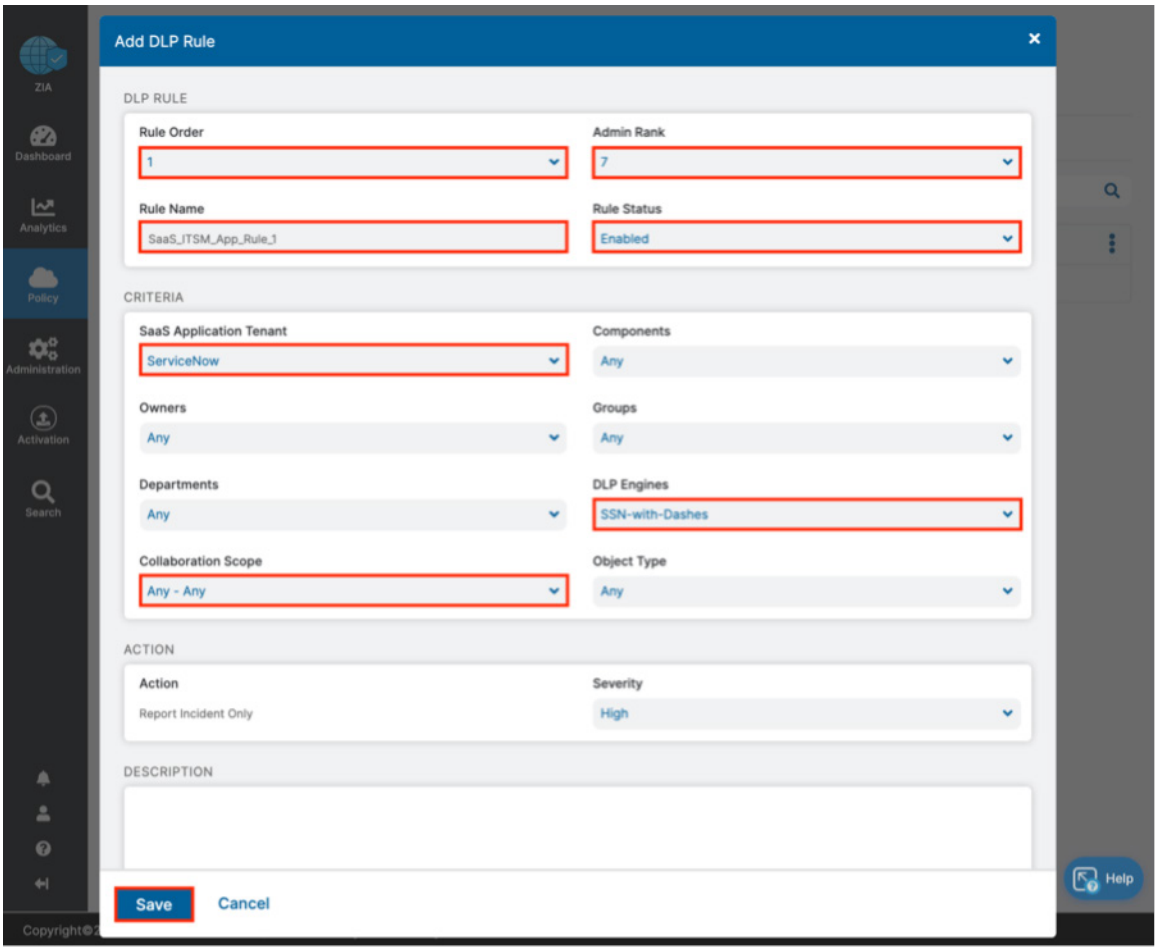


Figure 63. The SaaS DLP Policy Configuration wizard

The completed DLP rule is ready to be applied with a scanning schedule.

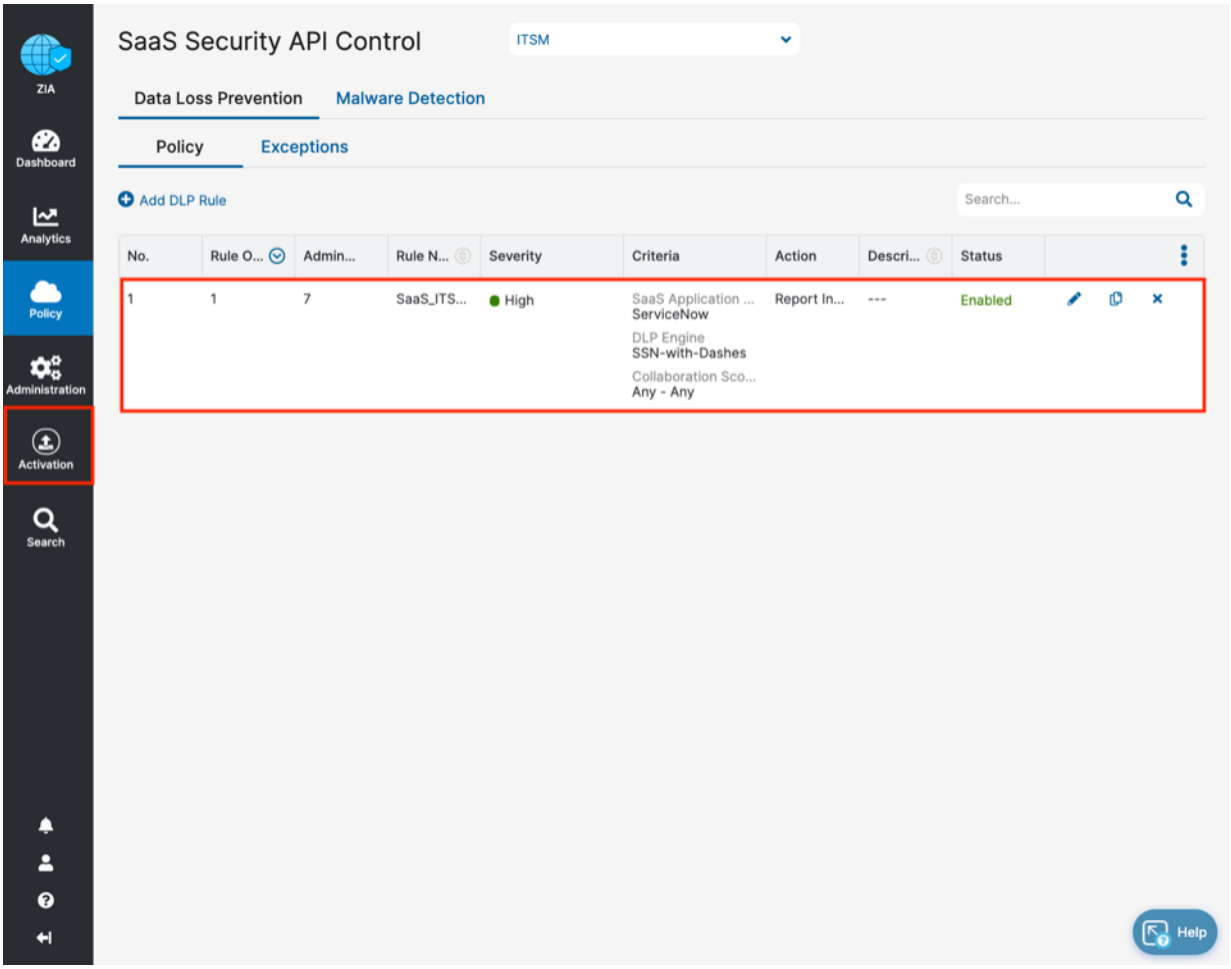


Figure 64. The configured DLP policy

Configure a SaaS Malware Policy

To launch the Malware Rule wizard:

1. Go to **Policy** > **SaaS Security API** > **Malware Detection**.
2. Select **ITSM**.
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 specifying any exemptions by selecting the Exemption tab under Malware Detection. To add a malware policy, specify the application, the SaaS tenant, and the status.

The action for ServiceNow is limited to report malware only.

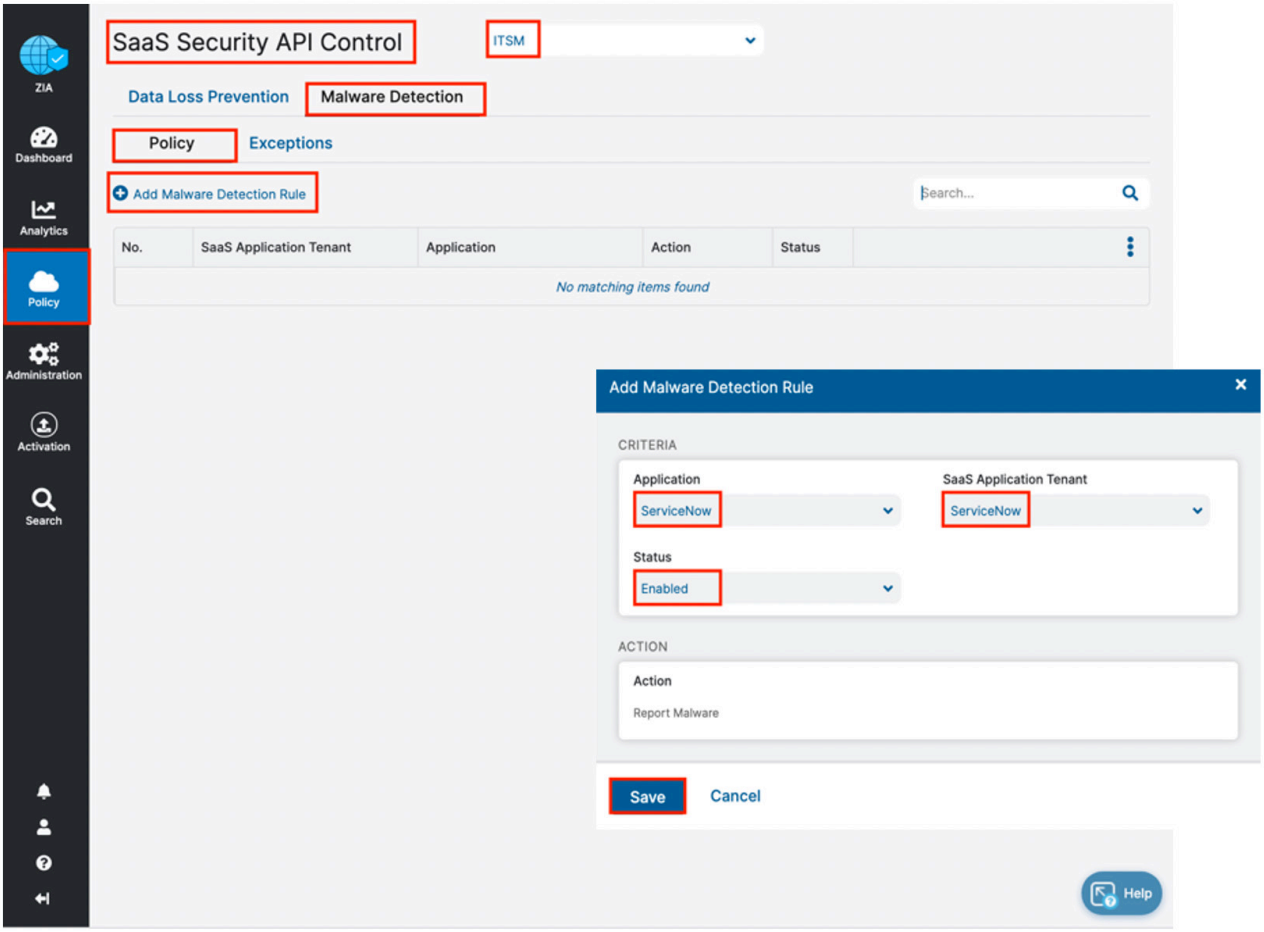


Figure 65. Launch the Malware Policy Configuration Wizard

SaaS Malware Policy Wizard

Configure the Malware Rule wizard:

1. Go to **Policy** > **SaaS Security API** > **Malware Detection**.
2. Select **ITSM**.
3. Select **Add Malware Detection Rule**.
4. Under **Criteria**, select **ServiceNow** as the application.
5. Select the ServiceNow SaaS tenant to apply the policy.
6. Select **Enabled** for **Status**.
7. Click **Save**.

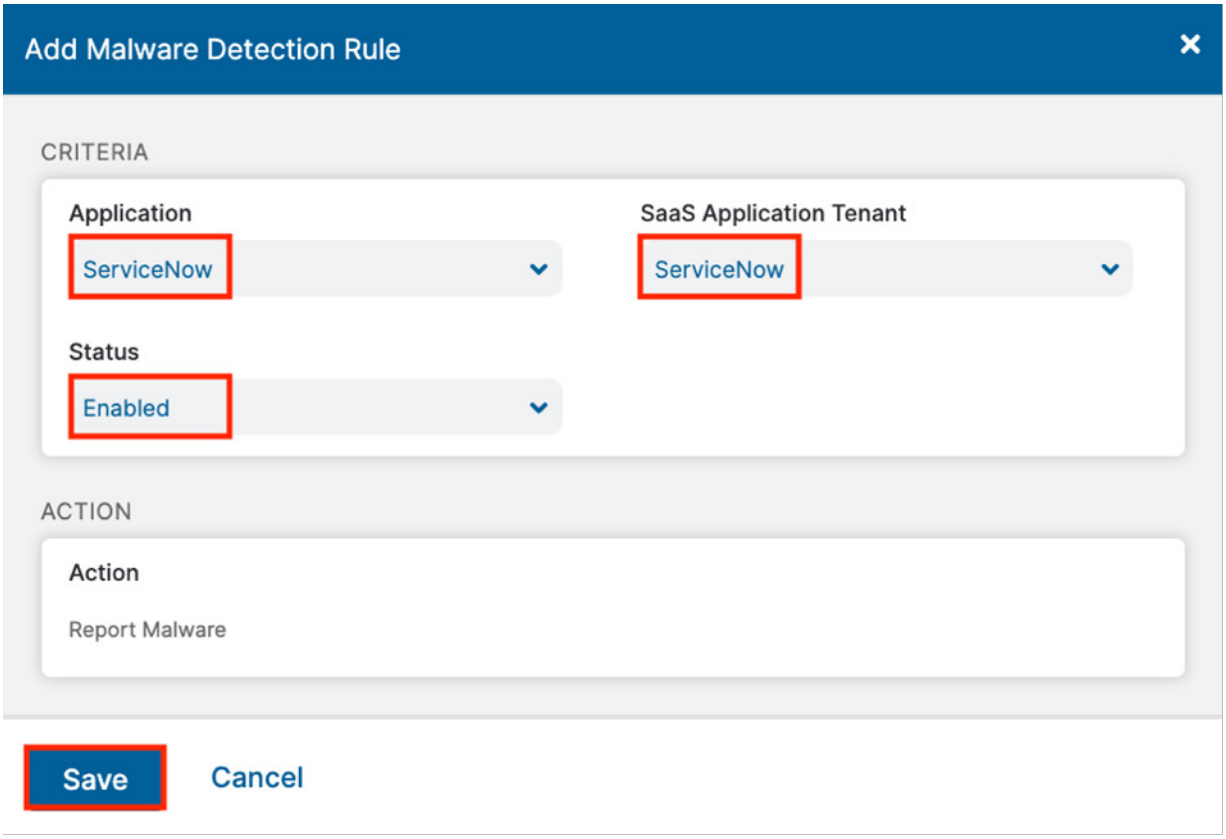


Figure 66. The Malware Policy Configuration wizard

SaaS Malware Policy

Apply the completed SaaS security malware policy for the ServiceNow SaaS tenant to the ServiceNow instance with a scanning schedule. Activate your configuration.

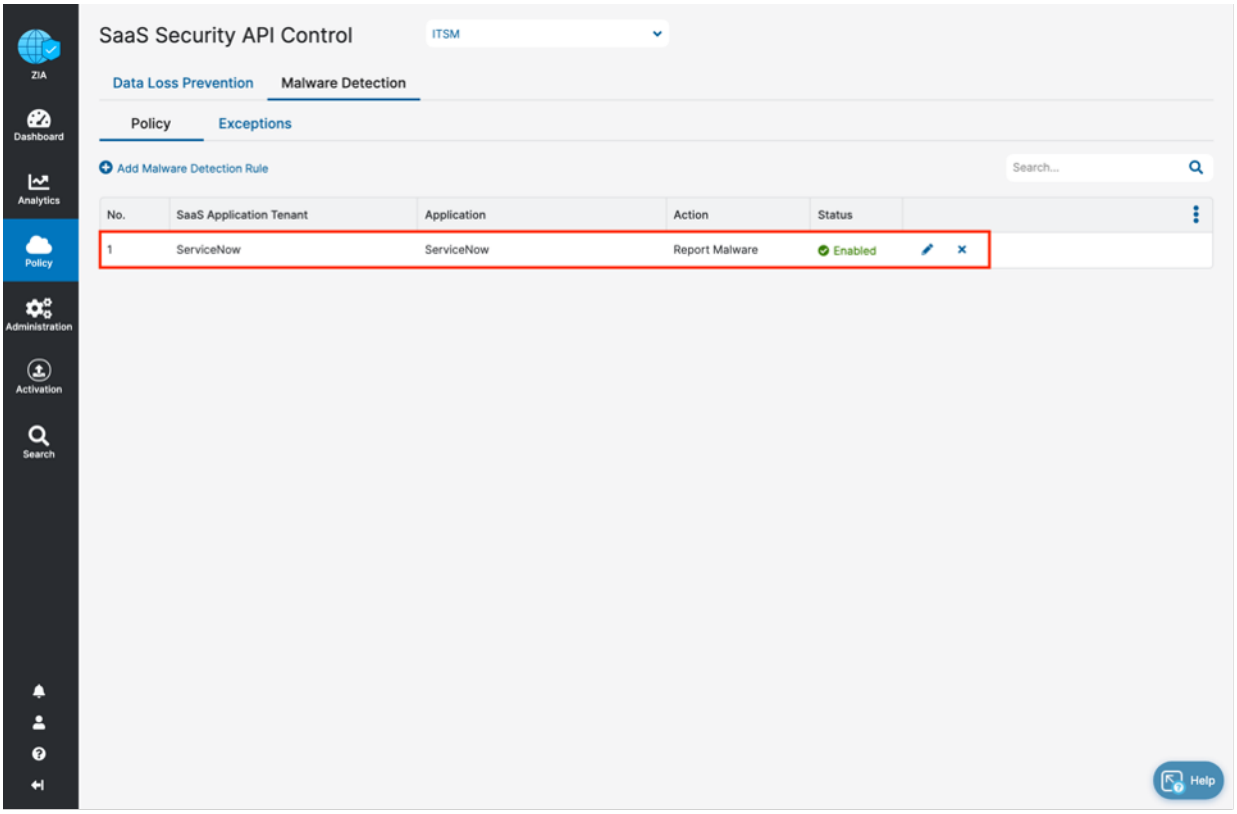


Figure 67. The completed Malware Policy Configuration wizard

Configure the Scan Schedule Configuration

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. For this deployment guide, select All Data.

However, if this is a Proof of Value (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 the ServiceNow SaaS tenant for the **SaaS Application Tenant**.
3. Select the data loss **Policy** and the malware policy created in prior procedures.
4. Select **All Data**, or for a POV select **New Data Only**.
5. Click **Save**, and then **Activate** the configuration.

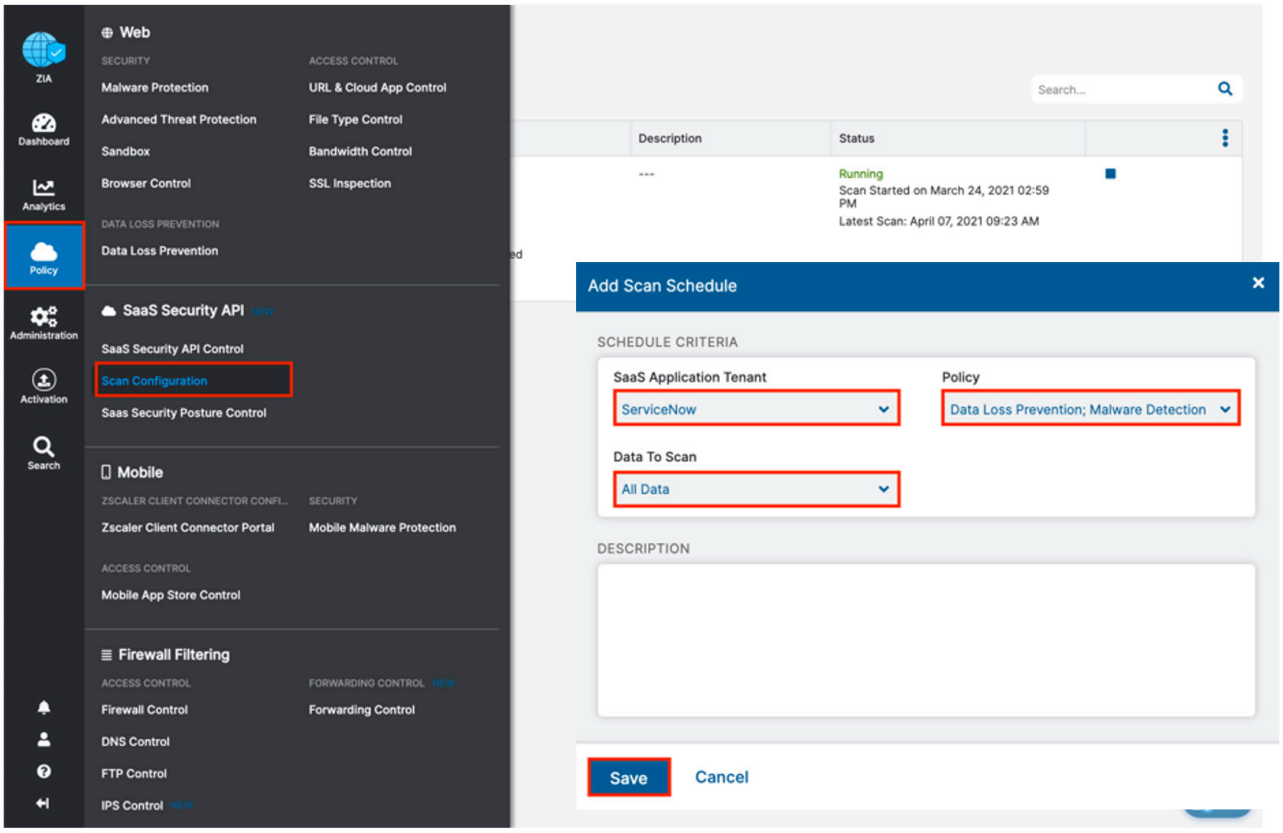


Figure 68. Create and enable a scan for the SaaS tenant

Start the Scan Schedule

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

1. Select the **Start** icon on the scan configuration to start SaaS API security on the ServiceNow tenant.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.

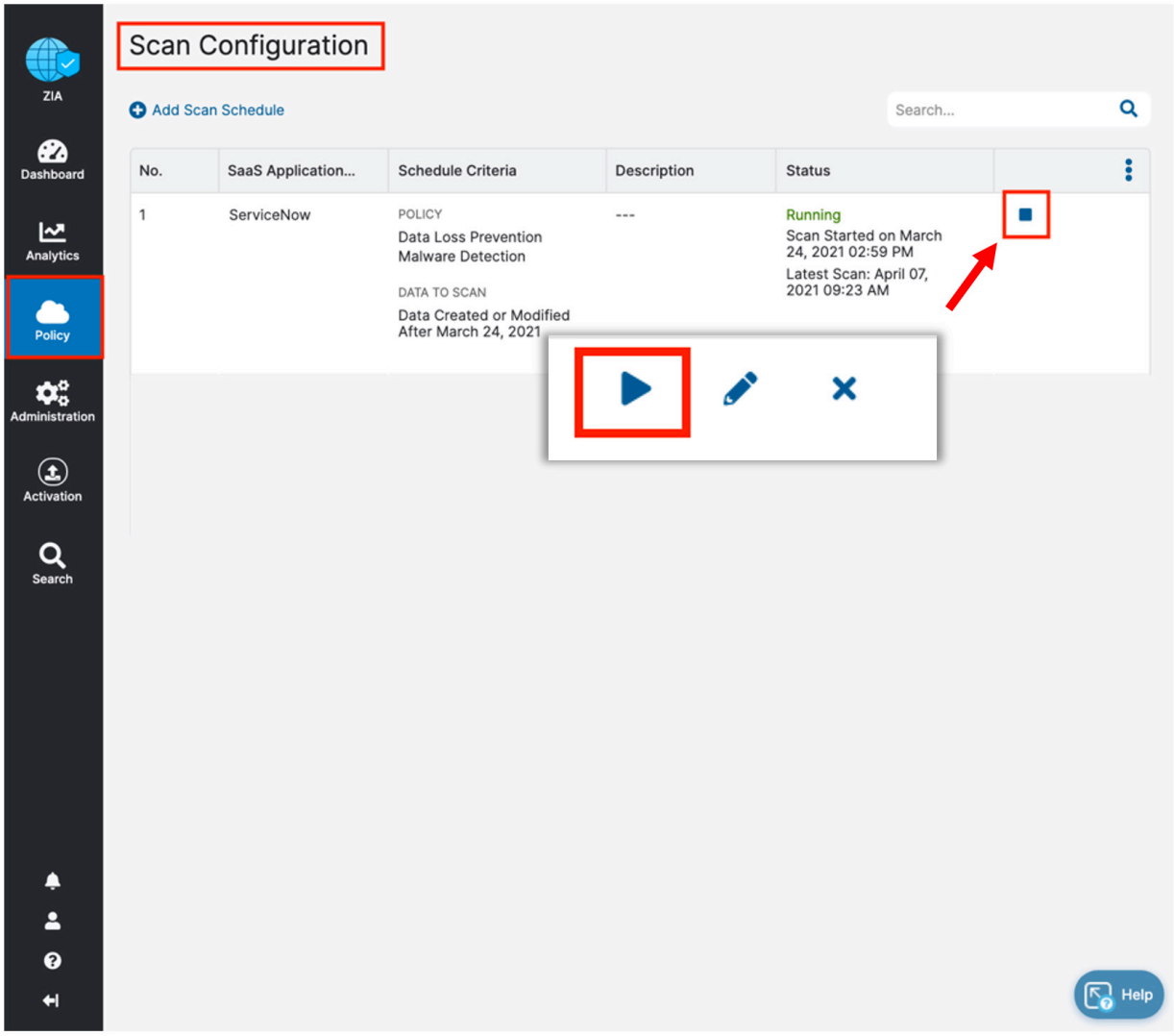


Figure 69. Starting the scan

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. Zscaler has reports and SaaS security insights, which provide visibility from a high-level overview to management of the individual logs and violations.

For more information, see SaaS Security Insights (government agencies, see SaaS Security Insights).

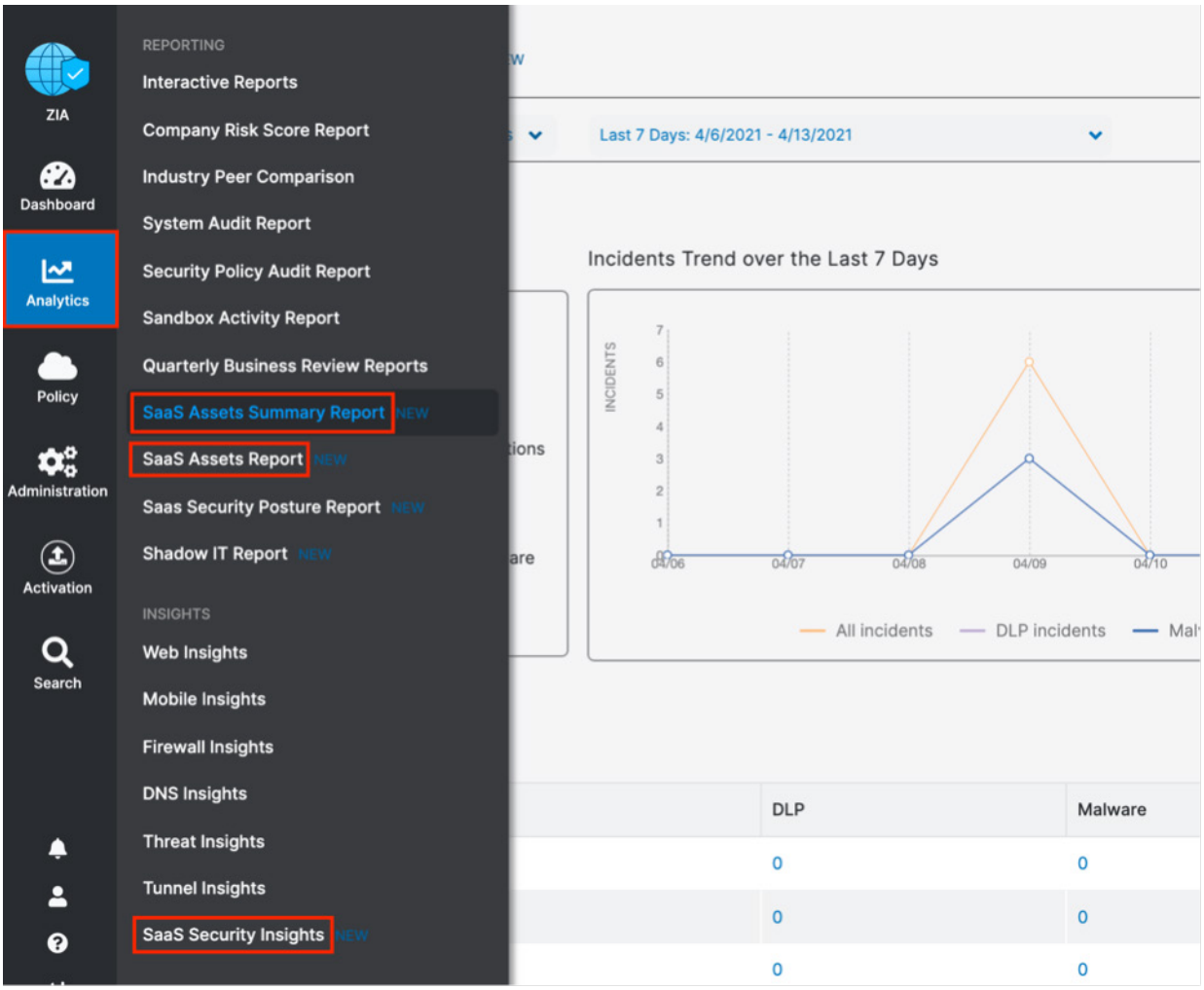


Figure 70. SaaS security visibility

SaaS Assets and SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reporting to have a quick view of your files and emails. A SaaS Assets Summary Report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen. Although your ServiceNow activity over the creation of this deployment guide is shown, any tenant configured is 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.

1. Select the **Total** violations number next to the ServiceNow icon to pivot to SaaS security insights.
2. On the **Security Logs** window, review the log data for each violation containing over 30 metadata points of information.

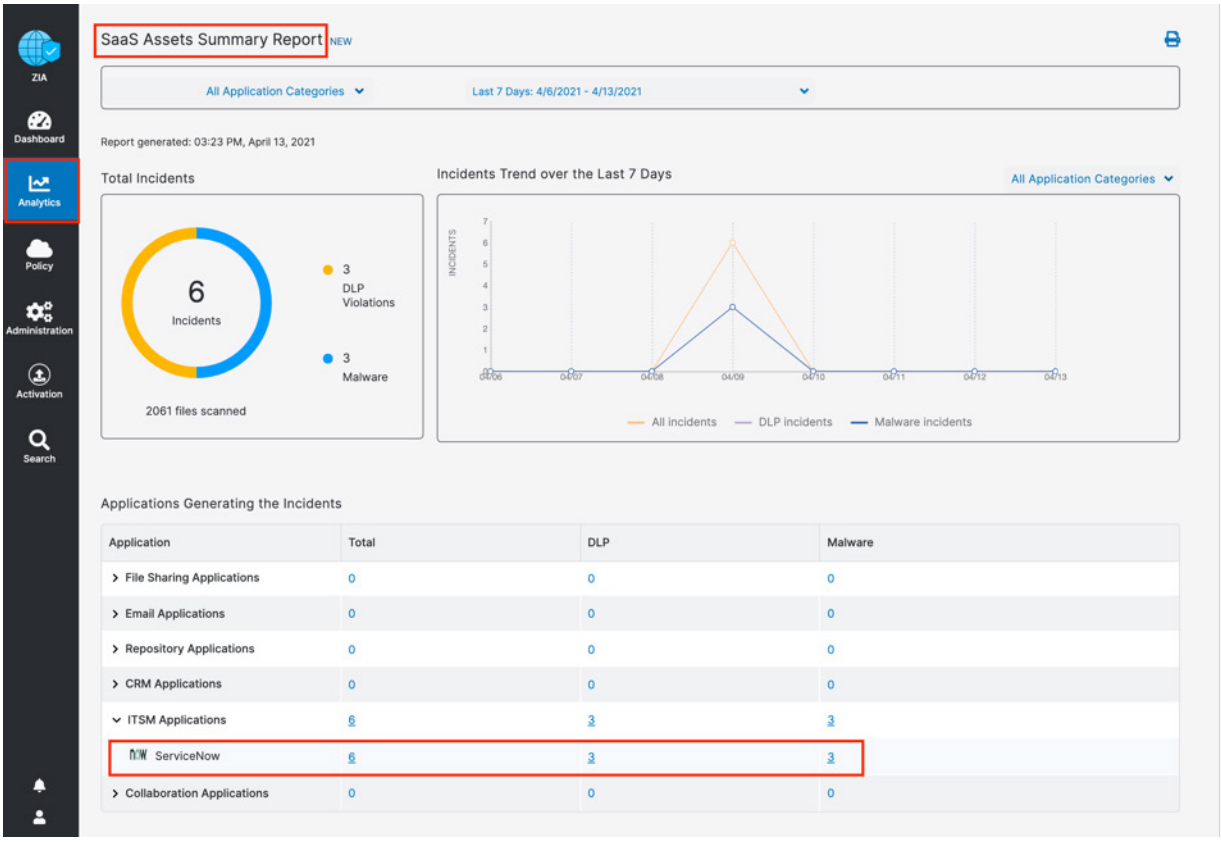


Figure 71. Summary reports

SaaS Security Insights

The SaaS Security Insights Log window allows you to select information fields for closer viewing 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.

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

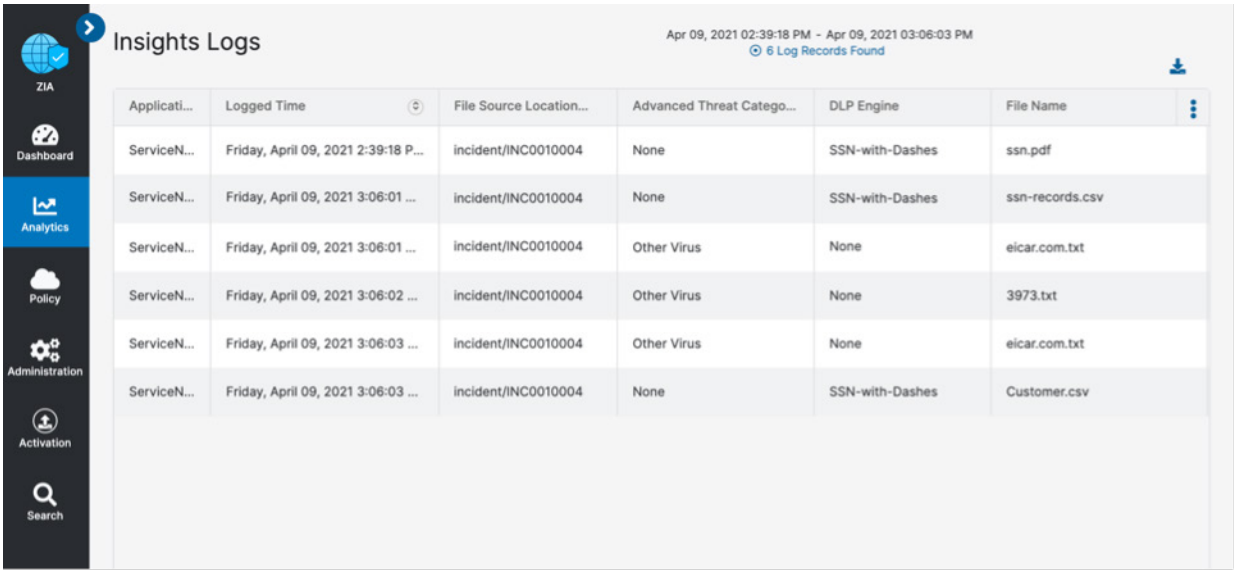


Figure 72. SaaS security insight

Cloud App Control

The following sections describe how to configure Cloud App Control for use with ServiceNow.

Cloud App Control Policy

Create the policy to allow specific users in a ServiceNow security group to access ServiceNow:

1. Sign into your organization's ZIA Admin Portal with administrator credentials.
2. Select **Policy**.
3. Select **URL & Cloud App Control**.
4. Select the **Cloud App Control Policy** tab.
5. Select **Add**.
6. Select **Productivity & CRM Tools**.

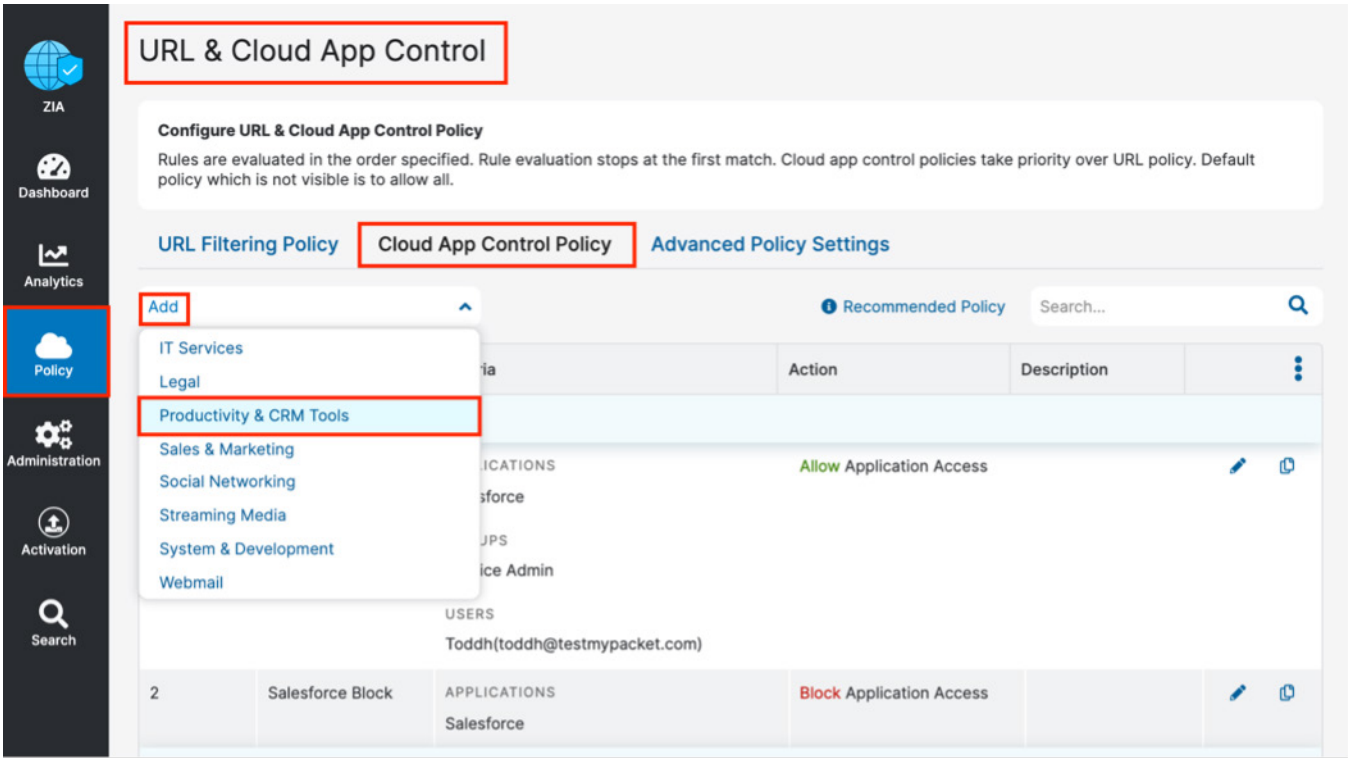


Figure 73. URL & Cloud App Control

This launches the **Policy Wizard**.

Cloud App Control Policy Wizard

To create an Allow policy:

1. Set the **Rule Order** to **1**.
2. Enter an intuitive **Rule Name**.
3. Select **ServiceNow** for the **Cloud Application**.
4. Select the security **Group** that contains the ServiceNow admins and users.
5. Select **Allow** for **Application Access**.
6. Click **Save**.

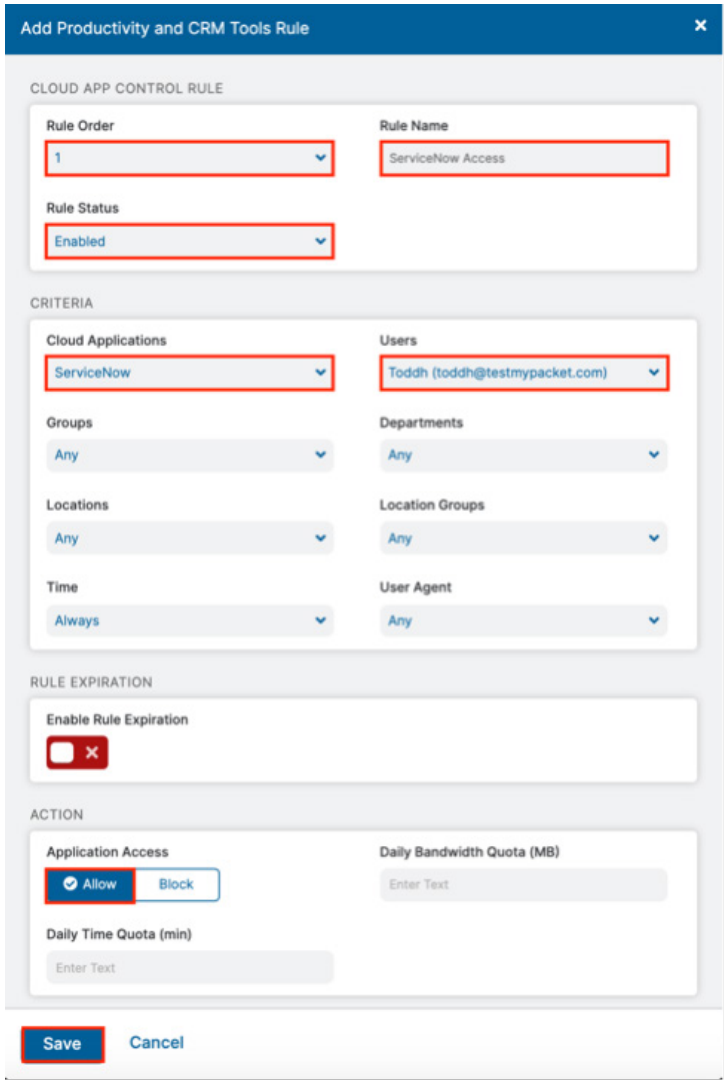


Figure 74. Create a Cloud App Control Allow policy

Cloud App Control Deny Policy

To create the policy to deny all other users:

1. Select **URL & Cloud App Control**.
2. Select the **Cloud App Control Policy** tab.
3. Select **Add**.
4. Select **Productivity & CRM Tools**.
5. Set the **Rule Order** to **2** (must be after the **Allow** policy).
6. Enter an intuitive **Rule Name**.
7. Select **ServiceNow** for the **Cloud Application**.
8. Leave all other settings as **Any**.
9. Select **Block** for **Application Access**.
10. Click **Save**, then **Activate** the changes.

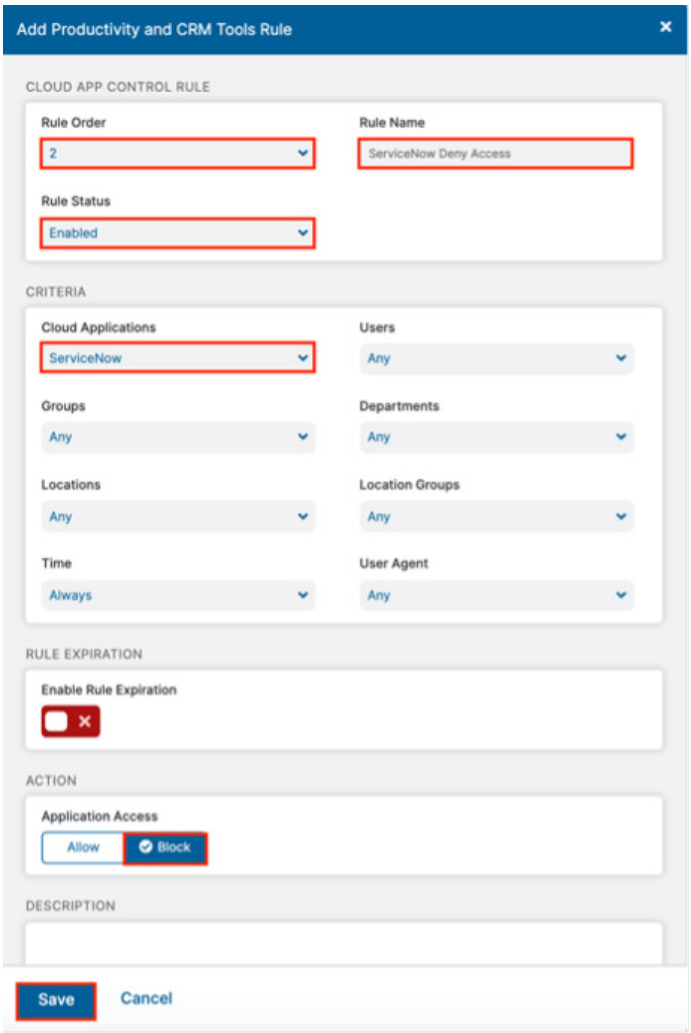


Figure 75. Create a Cloud App Control Deny policy

Users who try to access the ServiceNow application through Zscaler and do not have permission get the following Website blocked window. Zscaler administrators receive alerts and logs about the event.

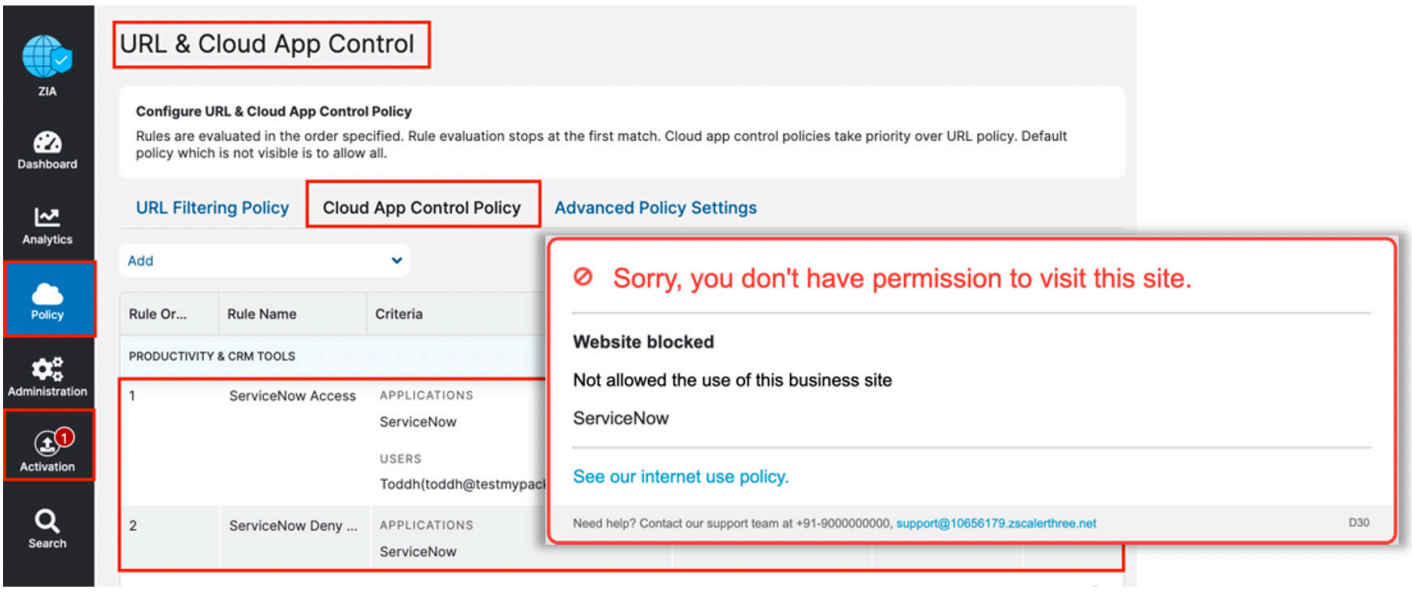


Figure 76. Cloud App Control Deny policy

Cloud App Control Logs

Zscaler analytics provide visibility to see any activity for ServiceNow access, or to get usage reports. To view the ServiceNow logs for a certain time frame:

1. Sign into your organization's ZIA Admin Portal with administrator credentials.
2. Select **Analytics**.
3. Select **Web Insights**.
4. Select the **Logs** tab.
5. Select the desired time frame, or custom time frame.
6. Select **Add Filter**.
7. Select **Cloud Application**.
8. Select **ServiceNow**.
9. **Apply** filters.

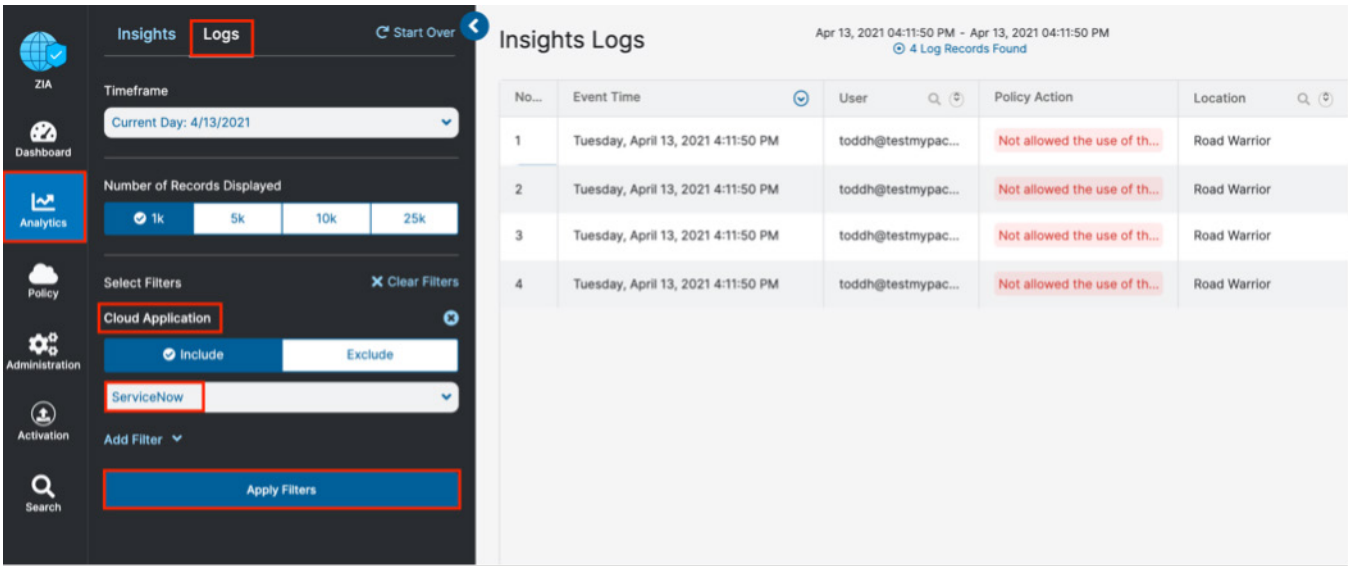


Figure 77. Create a Cloud App Control log

ZDX for ServiceNow

The following sections describe how to configure ZDX for use with ServiceNow.

Configure ZDX for ServiceNow

Log into the ZDX Admin Portal with administrator credentials to begin the configuration process.

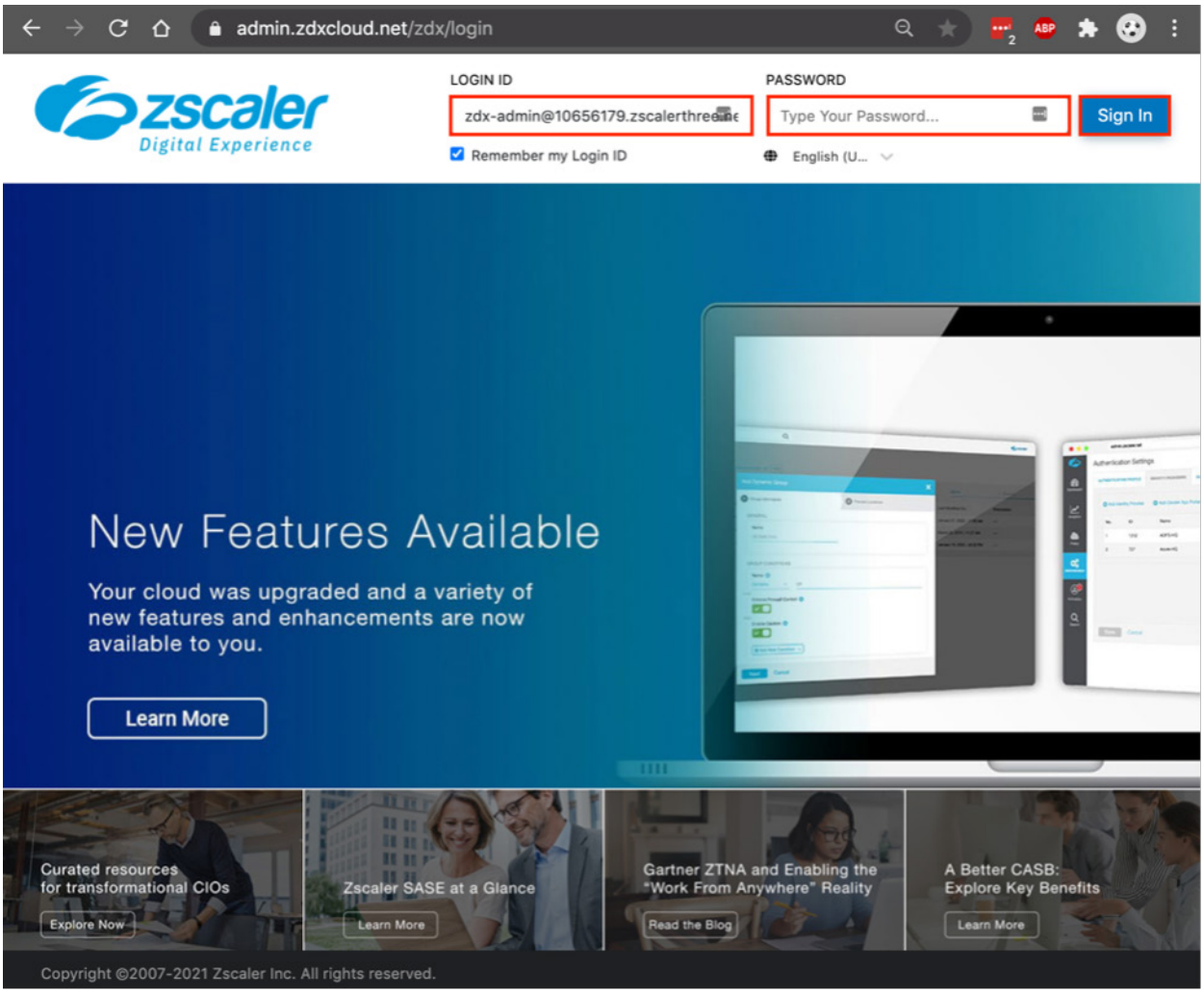


Figure 78. ZDX user experience monitoring for ServiceNow

Configure ZDX for ServiceNow

ServiceNow is a predefined application in ZDX. To configure the ServiceNow application for ZDX monitoring:

1. Select **Configuration**.
2. Select **Applications**.
3. Select the **Expand** icon next to the ServiceNow app.
4. Enter the **URL** for your ServiceNow tenant login.
5. Click **Submit** to onboard ServiceNow.

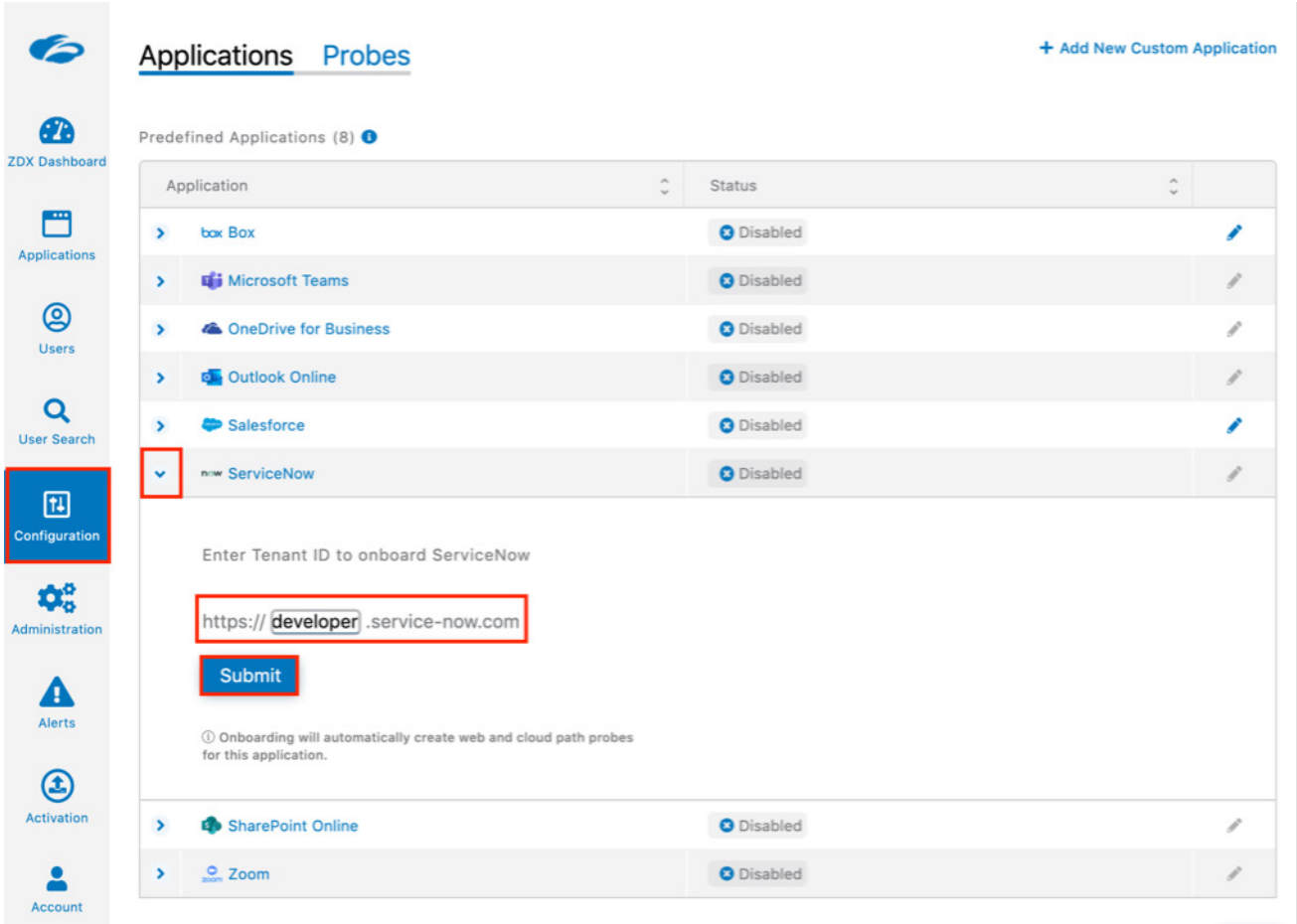


Figure 79. Onboard the ServiceNow app

Configure Probes for ServiceNow Monitoring

After clicking the Submit button, the ServiceNow app is enabled for monitoring and the pre-configured probes are displayed. The probes consist of a CloudPath probe uses Internet Control Message Protocol (ICMP) Trace Route, and a landing page probe to the dev1023676.service-now.com location to monitor page load times.

Modify the CloudPath probe so that it follows the path of the landing page probe so there is no confusion about the results since this is entirely for ServiceNow monitoring.

To edit the rule:

1. **Activate** the changes.
2. Select the **Edit** icon to edit the probe.

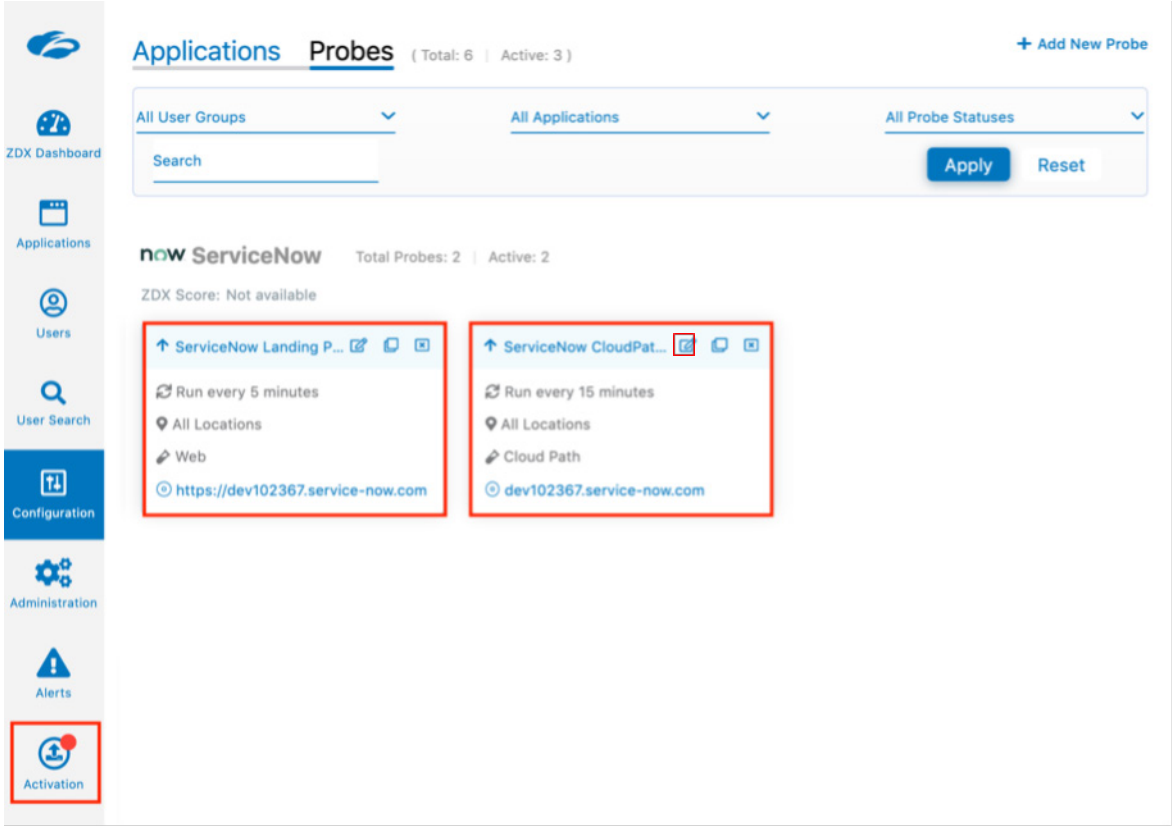


Figure 80. ZDX user experience monitoring for ServiceNow

Configure Probes for ServiceNow Monitoring

To configure probes for ServiceNow monitoring:

1. Select **ServiceNow Account Login Page Probe** under **Follow Web Probe**.
2. Select **Next**.

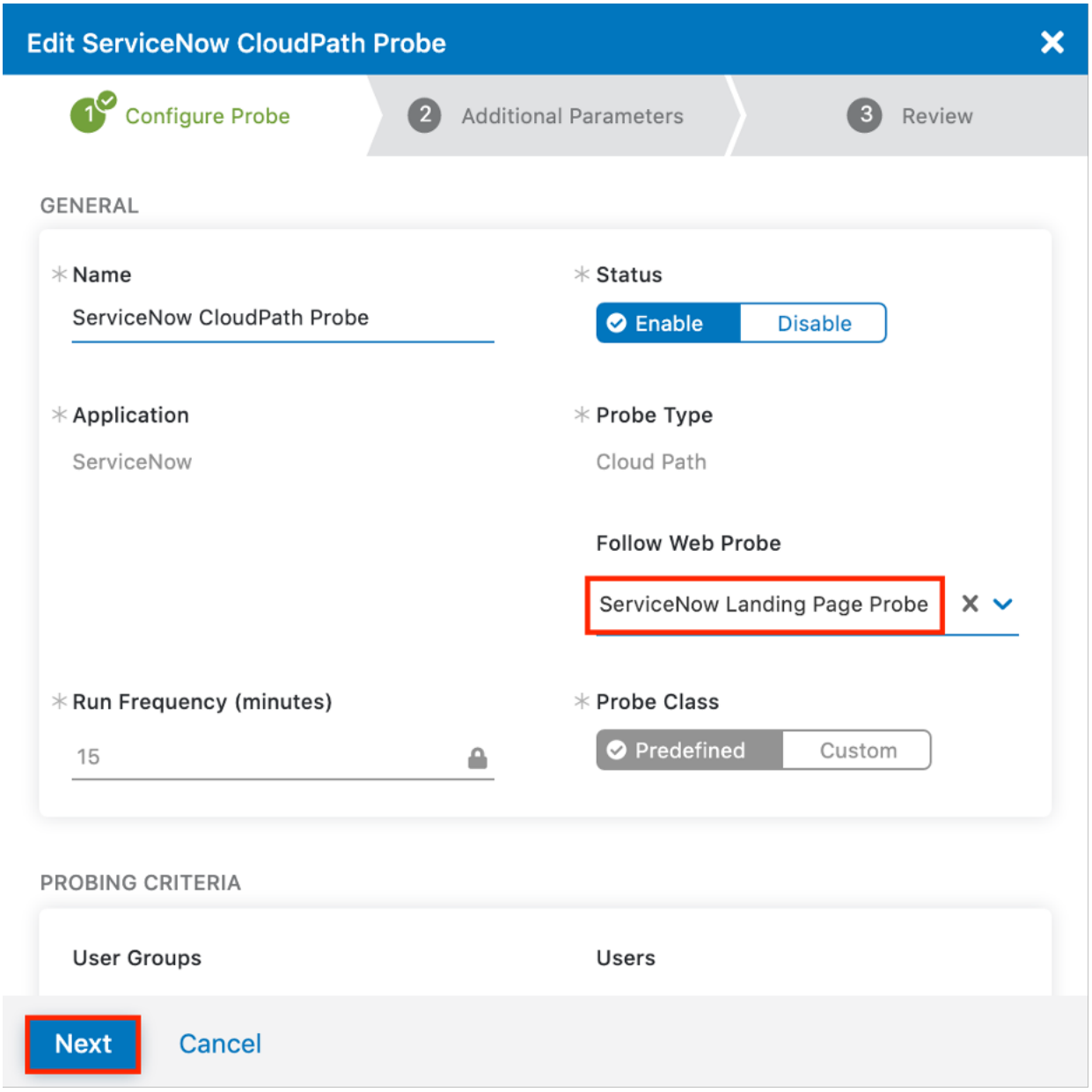


Figure 81. Edit the network probe

3. Validate the destination host to monitor. Ensure it is your ServiceNow Login URL.
4. Select **Next**.
5. Review and **Activate** the changes to the probe.

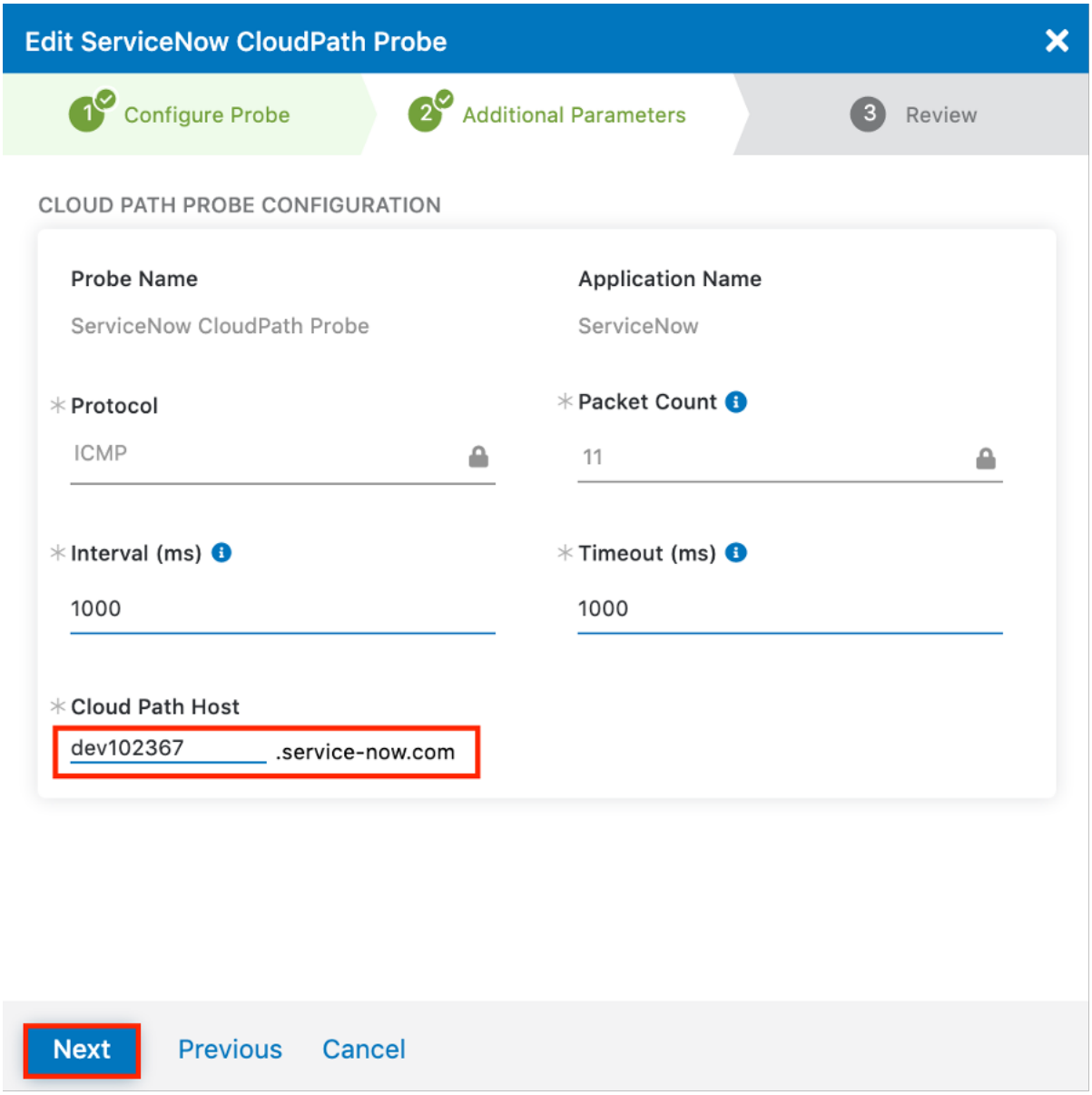


Figure 82. Edit the CloudPath probe

The ZDX-Enabled ServiceNow Application

The ServiceNow application monitoring is activated, and the probes begin for everyone using the Zscaler Client Connector. The figure shows the Zscaler Client Connector running the digital experience and the service is on.

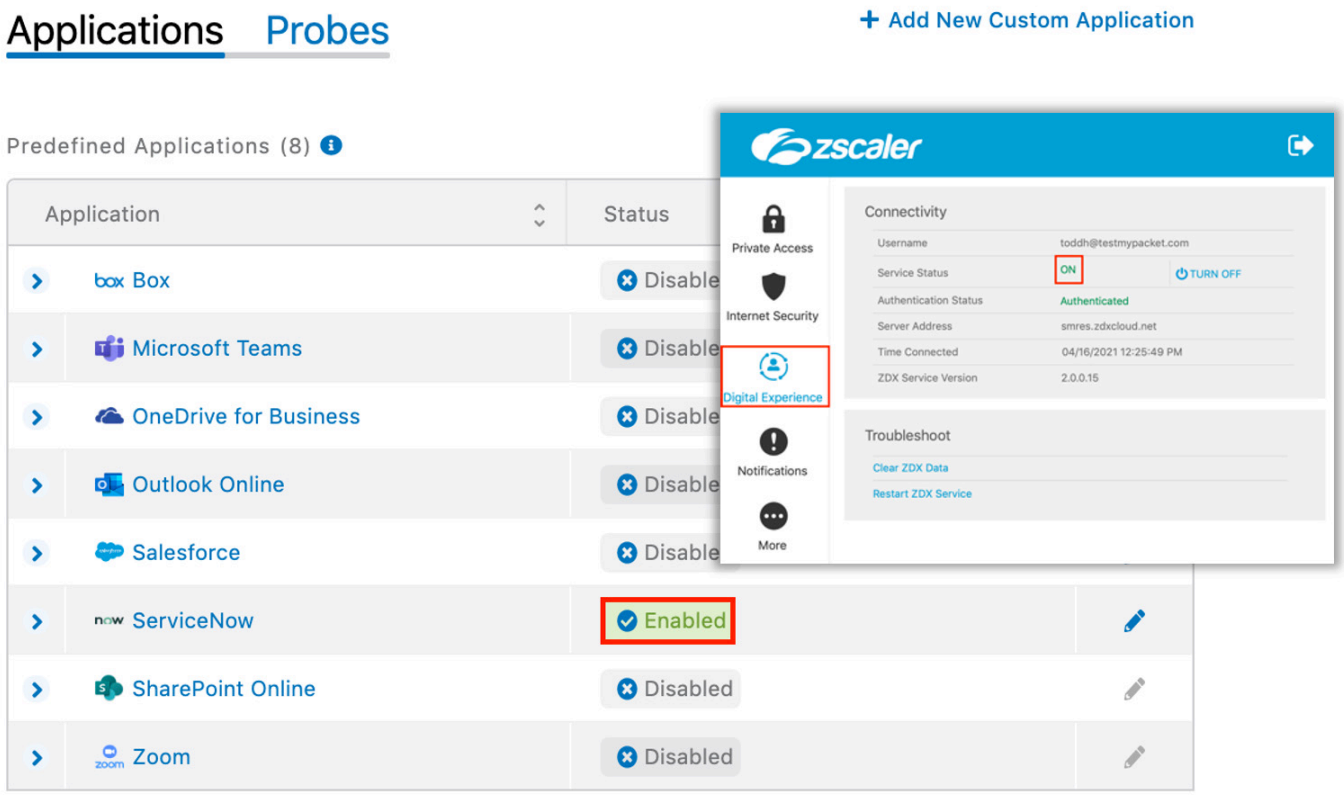


Figure 83. Active ServiceNow monitoring

Create an Alert for the ServiceNow Service

As a final configuration step, create an alert to email when there is service degradation of the ServiceNow application. You can configure an alert for network, application, or device thresholds. You can create an alert rule with any of the following:

- Network Probe: Latency, My Traceroute (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. Select **Alerts**.
2. Select **Rules**.
3. Select **Add New Alert Rule**.

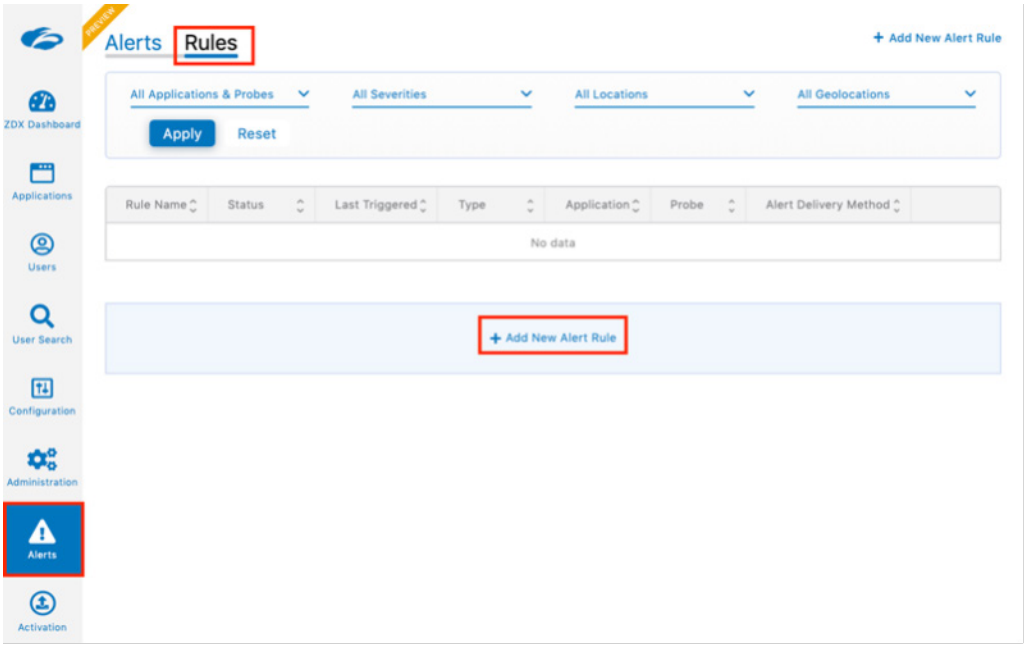


Figure 84. Creating an alert

4. Configure Rule:
    a. **Name** the Rule.
    b. Select **Enable** under **Status**.
    c. Give the alert an appropriate severity.
    d. Select an application **Type**.
    e. Click **Next**.

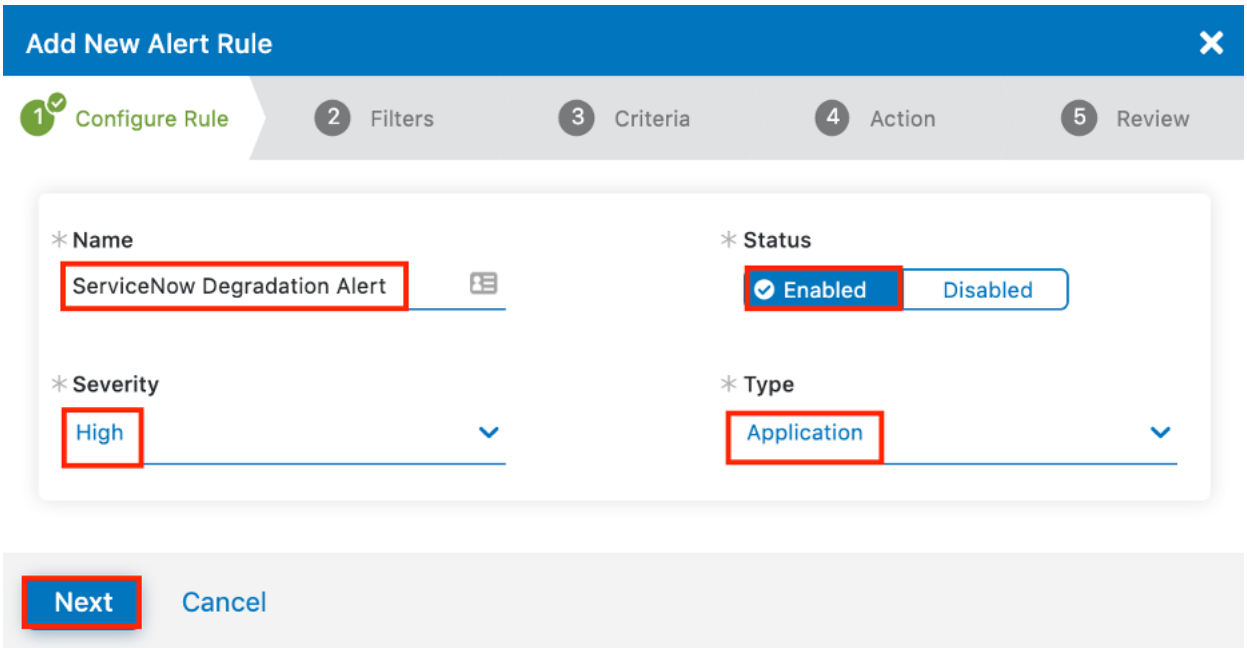


Figure 85. The Alert Creation wizard step 1

5. Filters:
    a. Select **ServiceNow** as the **Application**.
    b. Select **ServiceNow Landing Page Probe** for the **Web Probe**.
    c. Click **Next**.

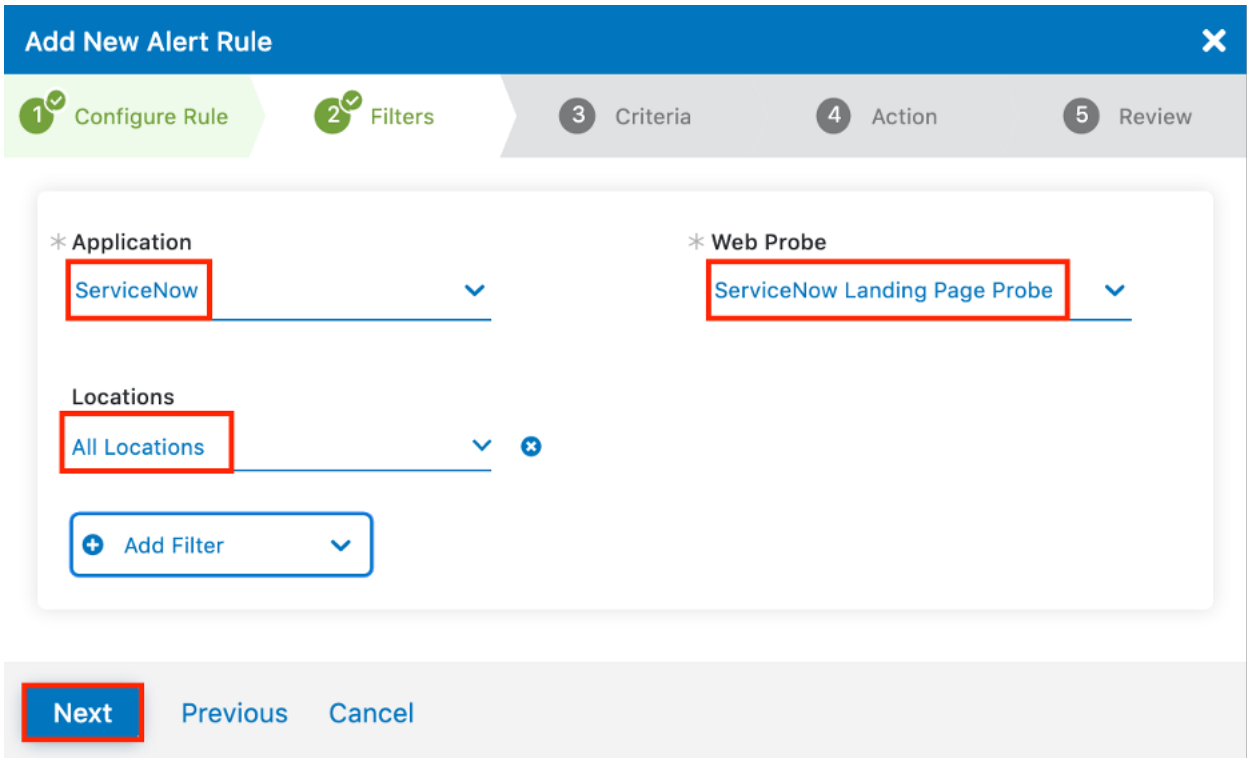


Figure 86. The Alert Creation wizard step 2

6. Criteria creates the threshold that triggers the alert. Use multiple variables to eliminate false positive.
   a. Select **Page Fetch Time**.
   b. Select the time to exceed **5000ms** (five seconds).
   c. Click **Next**.

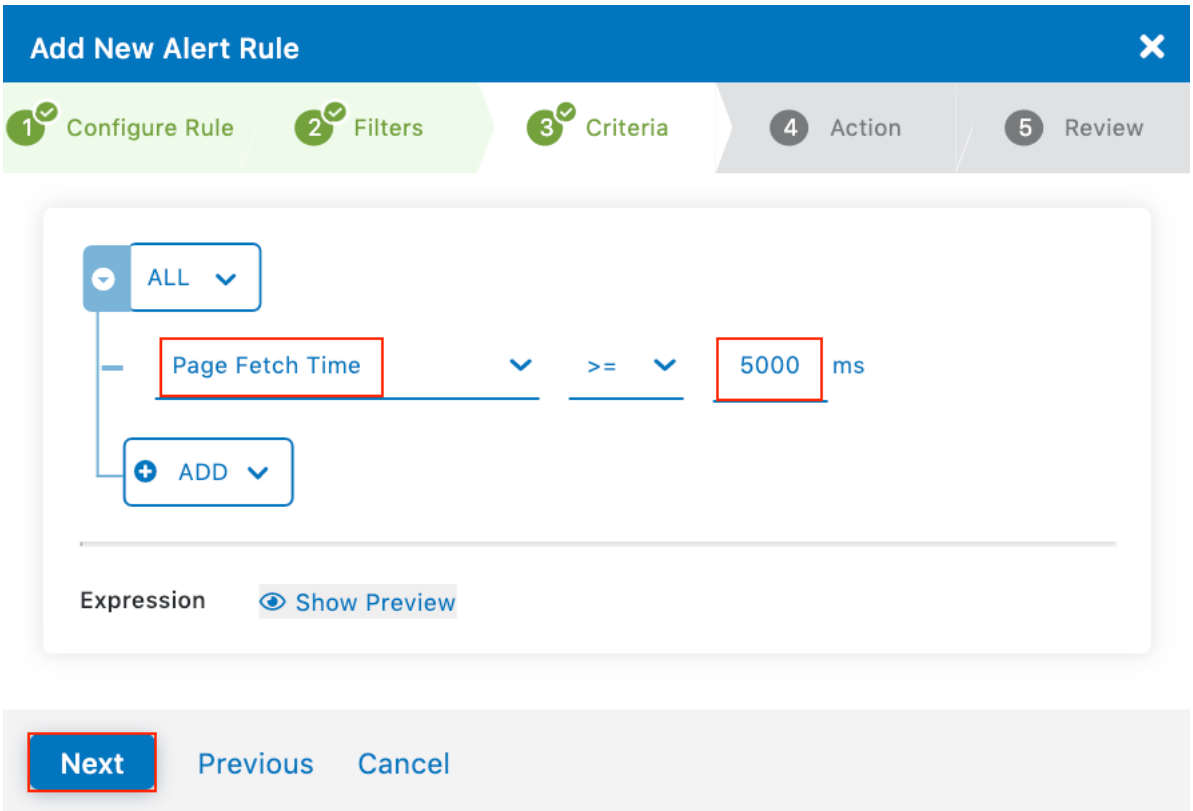


Figure 87. The Alert Creation wizard step 3

7. Add throttling to control the scope of the alert. Then define the action as email. The action can also be defined as an authenticated webhook to send the alert to a Slack channel:

   a. Enter **10** for the number of times the probe time must exceed the threshold.
   b. Select **10 Percent** for the **Minimum Devices Impacted**.
   c. Select **Email** as the **Delivery Method**.
   d. Enter the **Alert Recipients** email addresses separated by commas.
   e. Click **Next**.

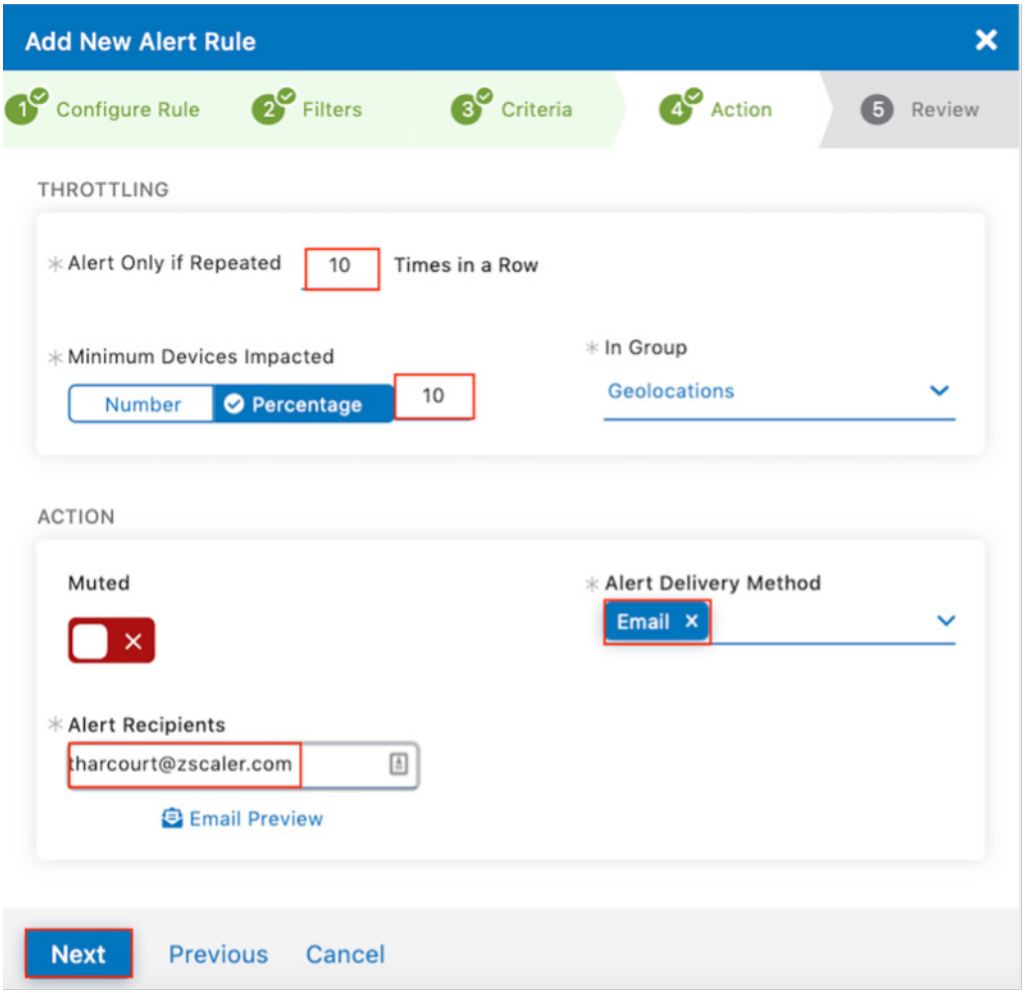


Figure 88. The Alert Creation wizard step 4

The completed rule set for the alert:

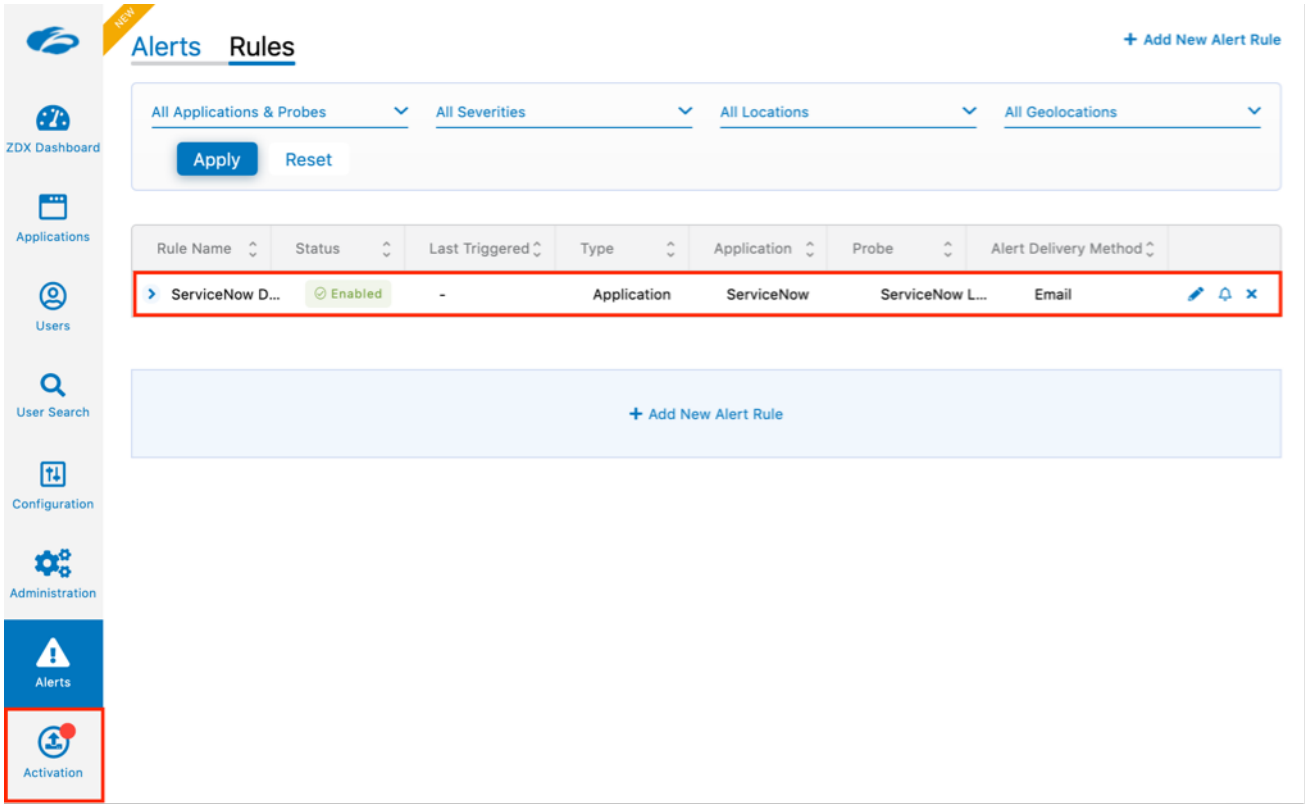


Figure 89. The completed rule set

The Triggered Alert for the ServiceNow Service

You can see the triggered alert generated by the threshold settings in the rule set. Click the rule name or the View icon to see more detail about the alert.

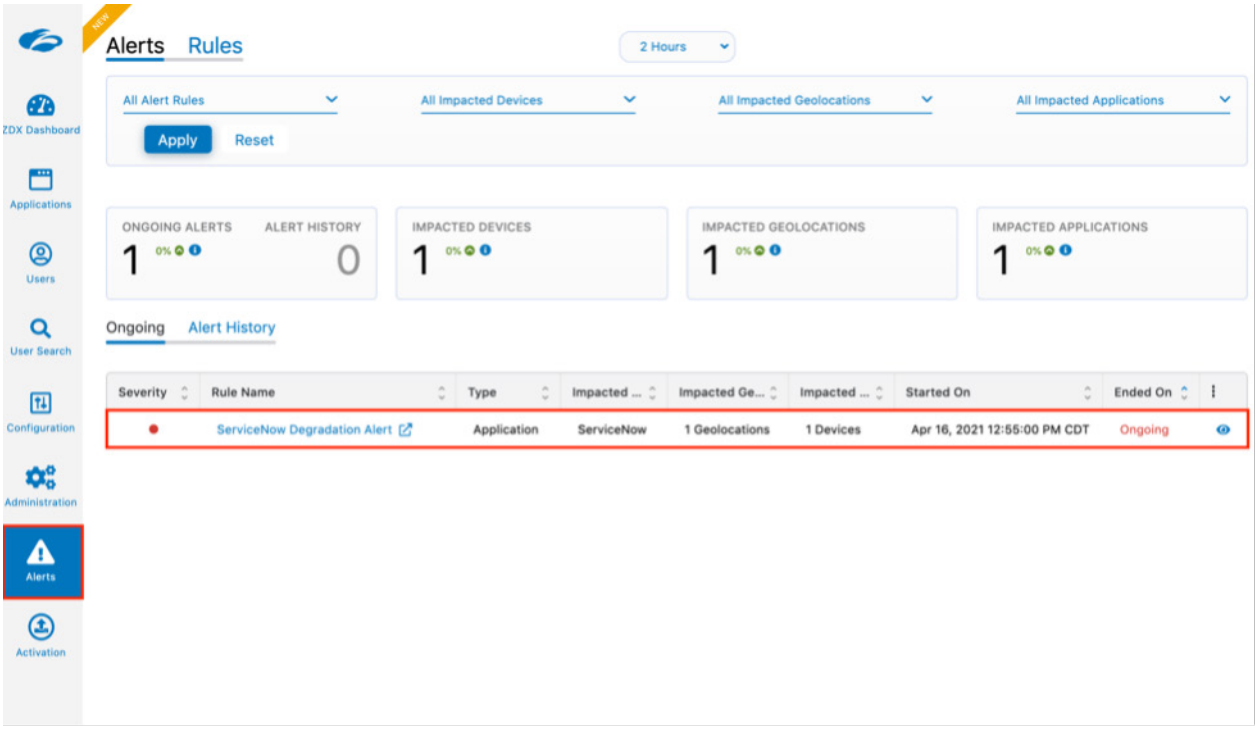


Figure 90. The alert

Alert Detail for the ServiceNow Service

The following details the triggered alert showing impacted user and devices, impact location, and threshold details.

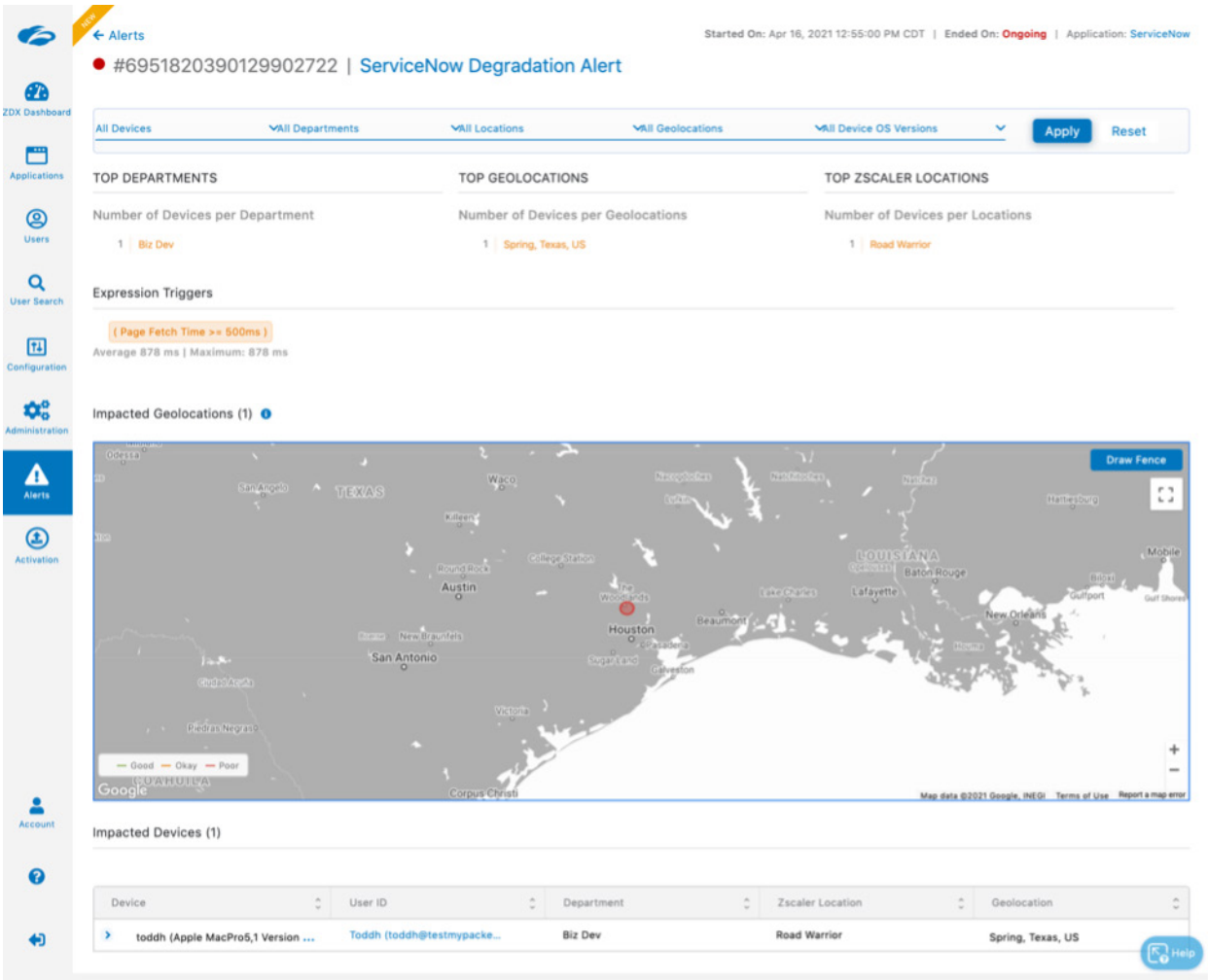


Figure 91. Alert details

The Sent Alert Email for the ServiceNow Service

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

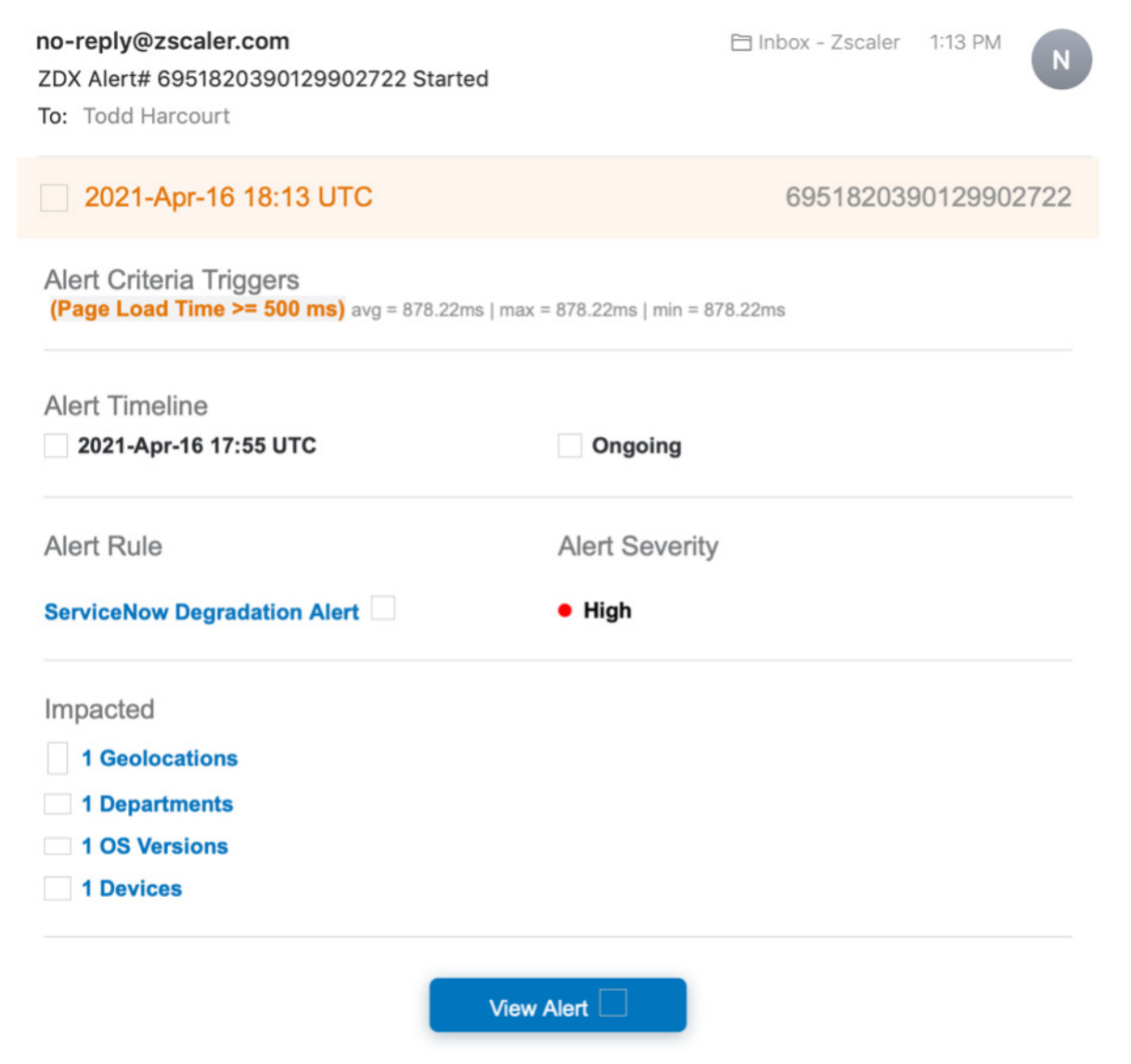


Figure 92. The alert email

Using the ZDX 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 shows any locations globally with issues.

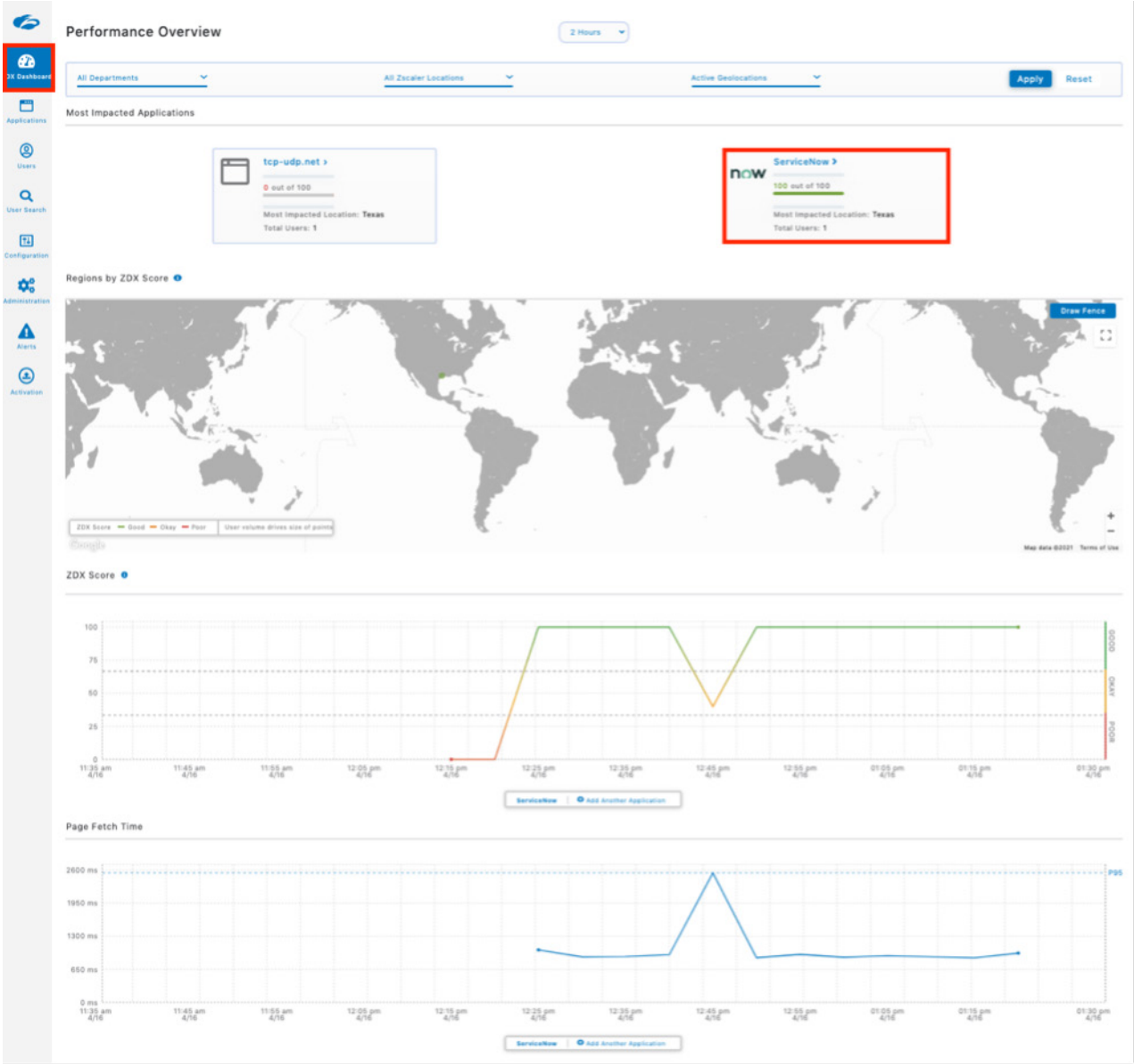


Figure 93. The ZDX Dashboard

Application Overview

Select Applications in the left-side navigation. This displays the Applications Overview and shows all the configured applications and the individual ZDX Score:

1. Select **Applications**.
2. Select the **ServiceNow** app.

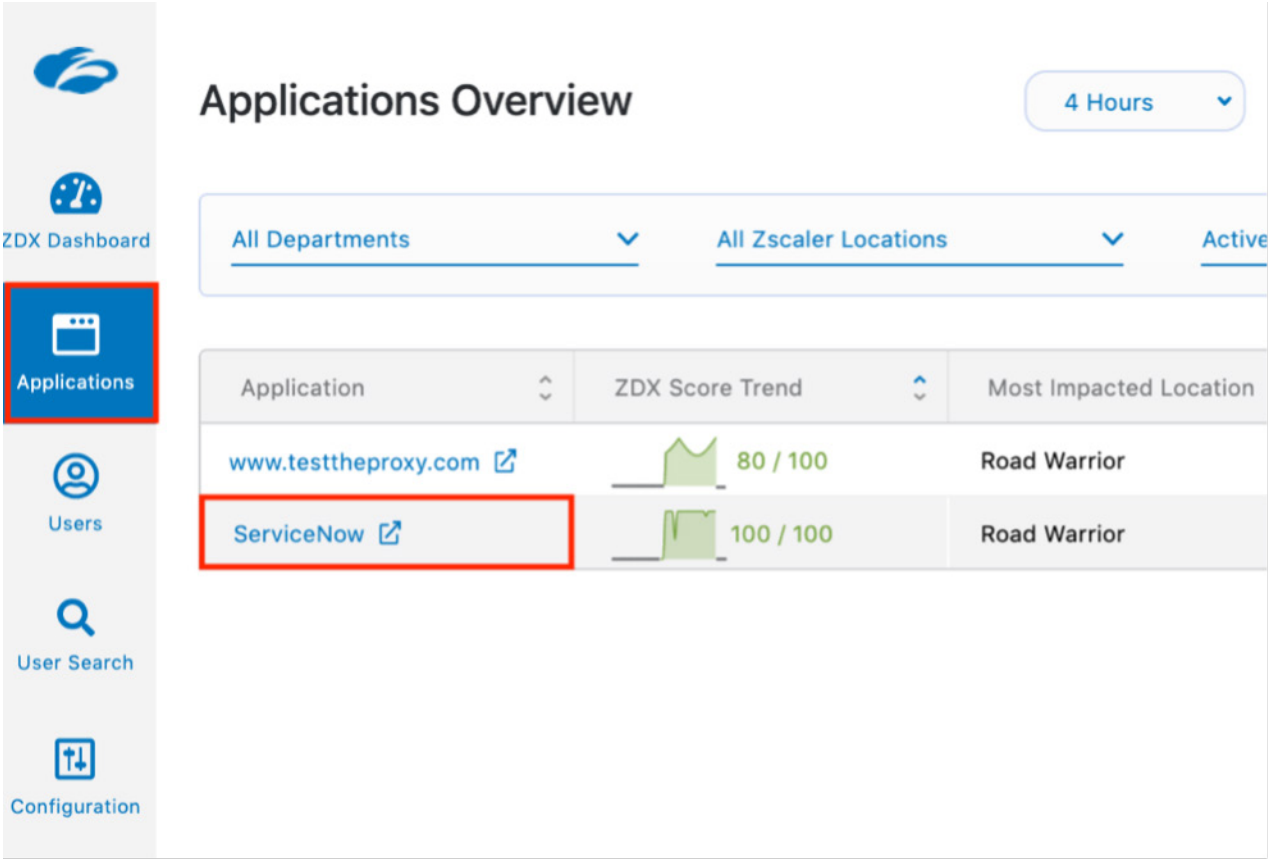


Figure 94. Applications overview

ServiceNow Application Performance Detail

The top portion of the application details show 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 ServiceNow service itself.

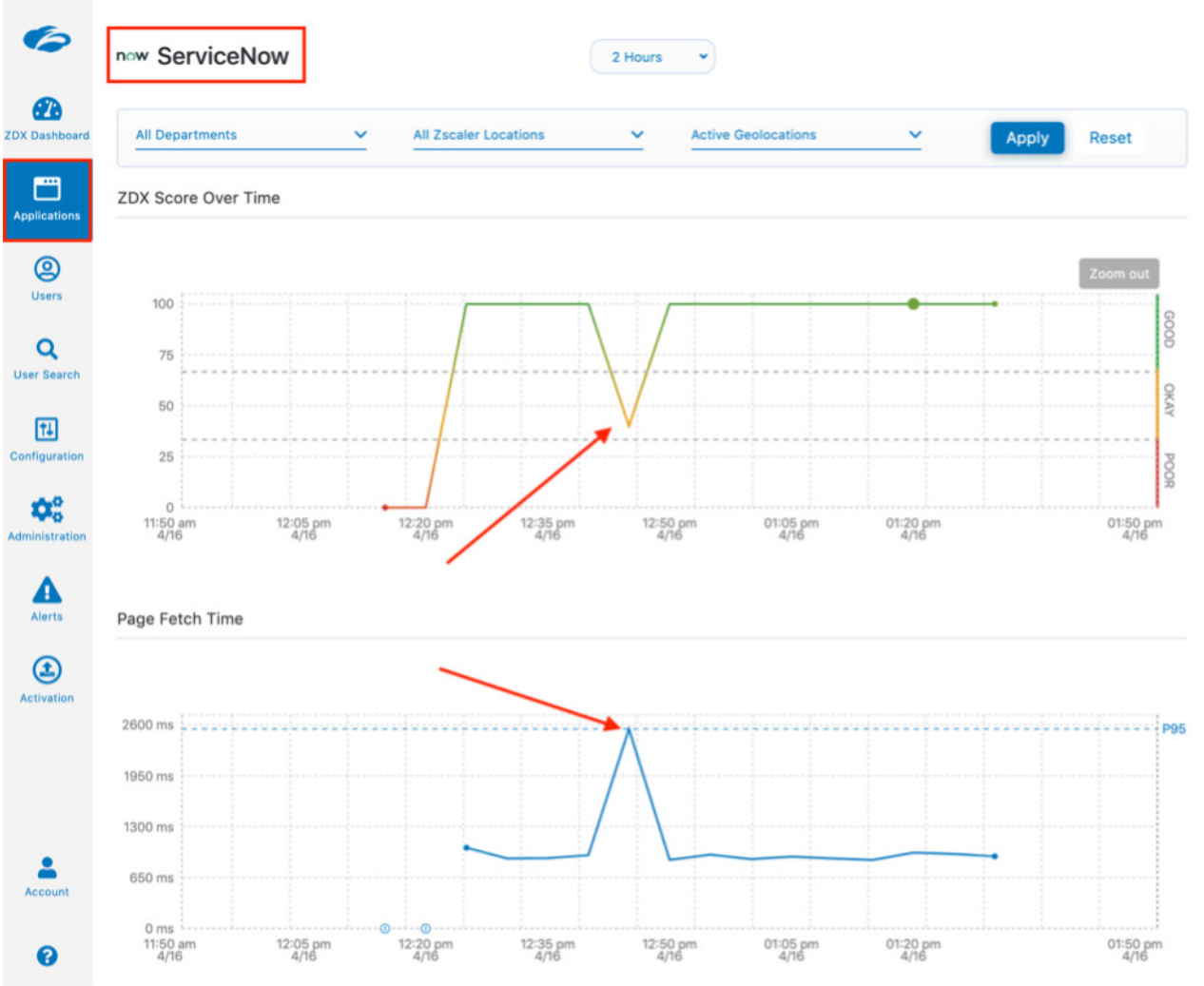


Figure 95. Application details

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

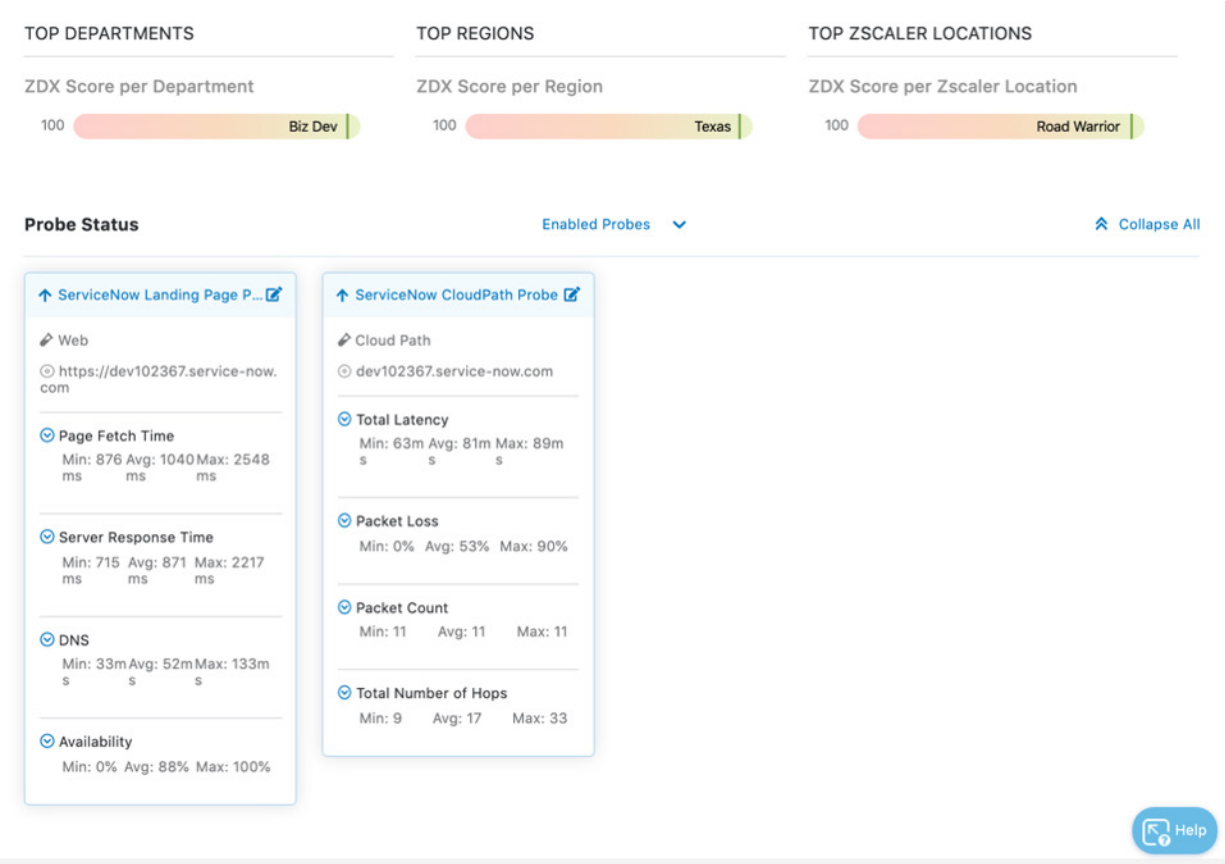


Figure 96. Application details

User Overview

The User Overview provides information about all the users of an application. Select ServiceNow and then Apply to see all the ServiceNow users. You can select users by Poor, Okay, or a Good ZDX Score. You can get more detail on the user by clicking the user name or the View icon on the right. Select a user to display more detail.

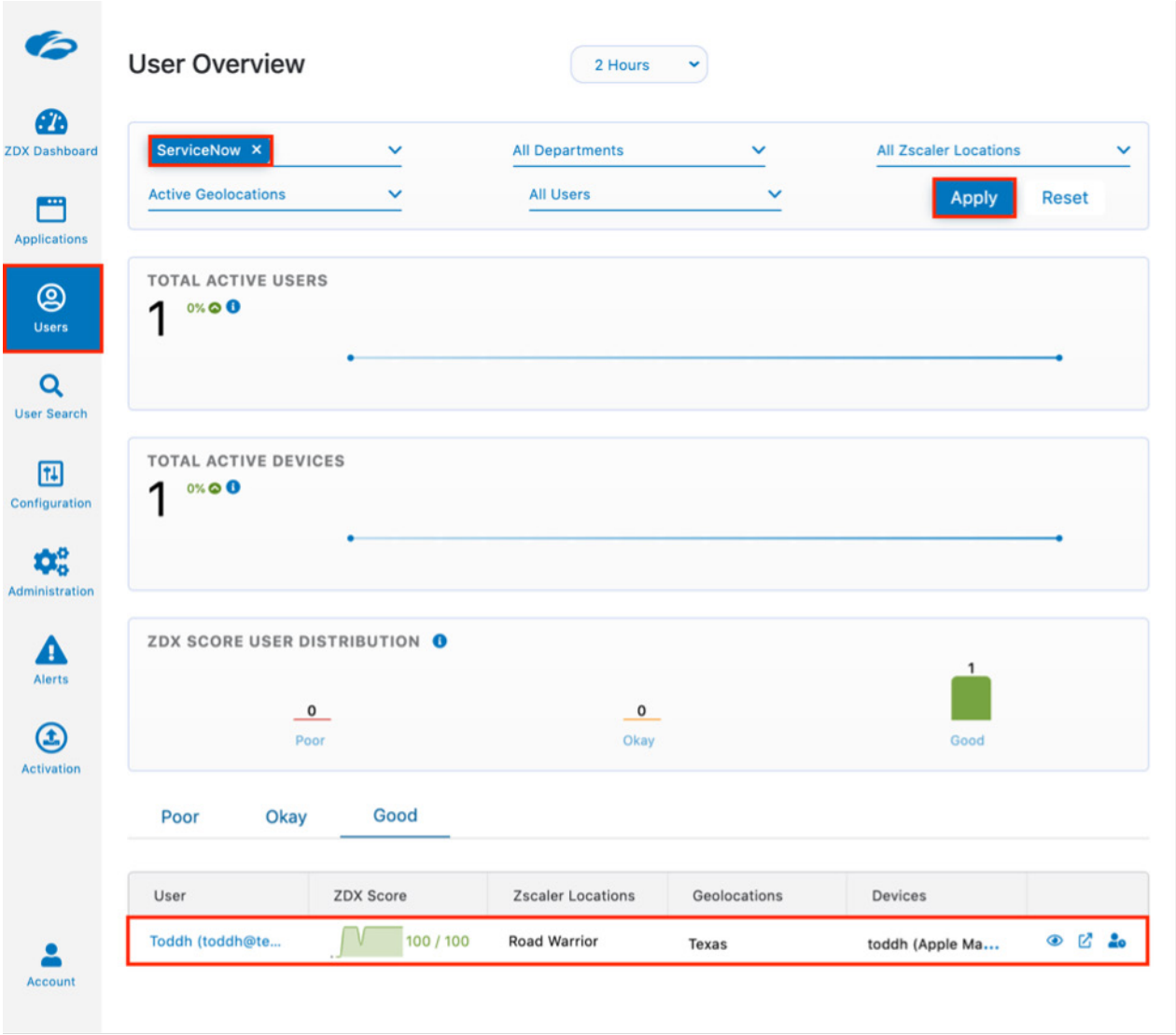


Figure 97. User overview

ServiceNow User Detail

The user detail shows data to help isolate any user experience issues. Select and apply the ServiceNow application to see the detail of the user experience for the ServiceNow app. This report provides the Users Devices and device-specific detail (OS, Device type, Network Information, etc.) by clicking the device. The ZDX Score is also displayed in a timeline, along with details of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health.

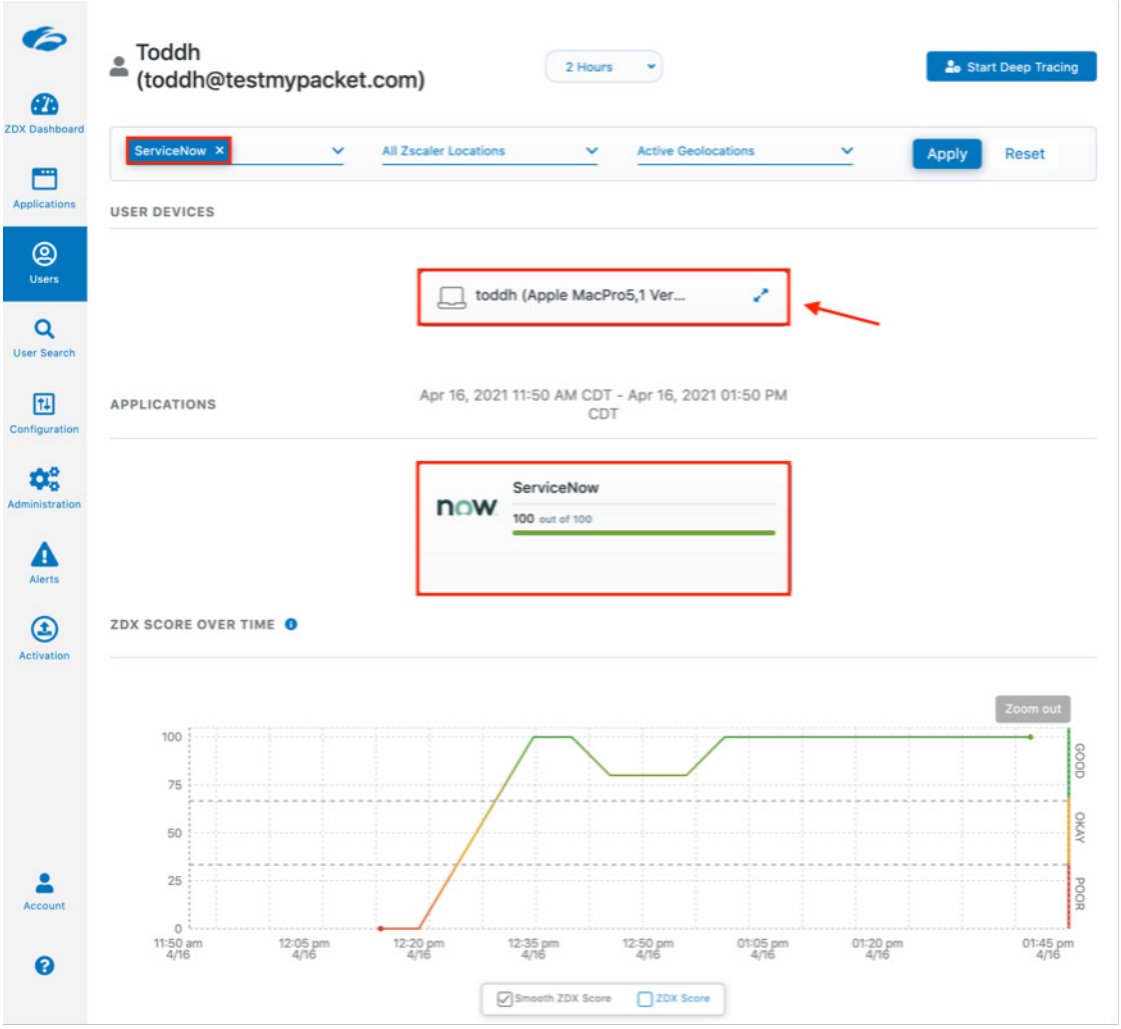


Figure 98. User detail

This is the end-to-end visibility of the data path the user is taking to get to the ServiceNow 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 an issue with Zscaler, or ServiceNow itself, ZDX provides the visibility of the cloud to the Zscaler administrators from any of their users' individual environments.

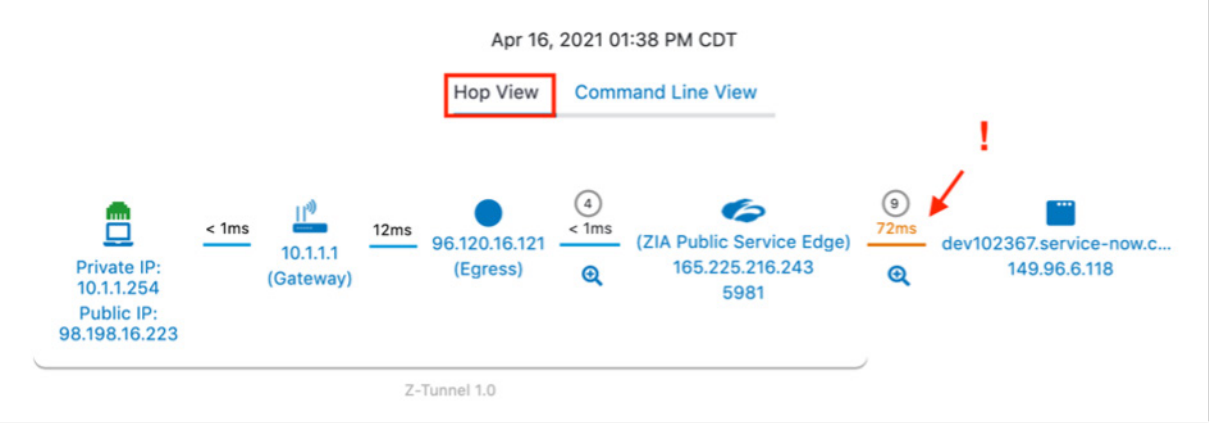
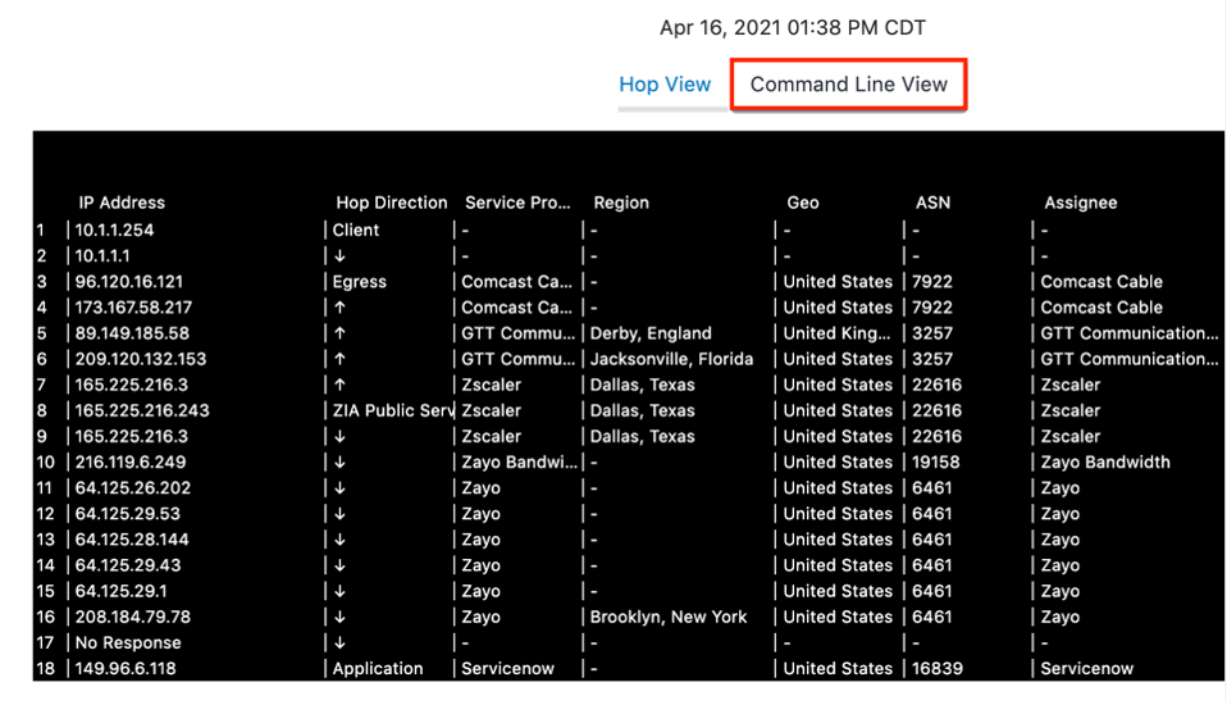


Figure 99. User detail: end-to-end connection detail (1 of 2)



	IP Address	Hop Direction	Service Pro...	Region	Geo	ASN	Assignee
1	10.1.1.254	Client	-	-	-	-	-
2	10.1.1.1	↓	-	-	-	-	-
3	96.120.16.121	Egress	Comcast Ca...	-	United States	7922	Comcast Cable
4	173.167.58.217	↑	Comcast Ca...	-	United States	7922	Comcast Cable
5	89.149.185.58	↑	GTT Commu...	Derby, England	United King...	3257	GTT Communication...
6	209.120.132.153	↑	GTT Commu...	Jacksonville, Florida	United States	3257	GTT Communication...
7	165.225.216.3	↑	Zscaler	Dallas, Texas	United States	22616	Zscaler
8	165.225.216.243	ZIA Public Serv	Zscaler	Dallas, Texas	United States	22616	Zscaler
9	165.225.216.3	↓	Zscaler	Dallas, Texas	United States	22616	Zscaler
10	216.119.6.249	↓	Zayo Bandwi...	-	United States	19158	Zayo Bandwidth
11	64.125.26.202	↓	Zayo	-	United States	6461	Zayo
12	64.125.29.53	↓	Zayo	-	United States	6461	Zayo
13	64.125.28.144	↓	Zayo	-	United States	6461	Zayo
14	64.125.29.43	↓	Zayo	-	United States	6461	Zayo
15	64.125.29.1	↓	Zayo	-	United States	6461	Zayo
16	208.184.79.78	↓	Zayo	Brooklyn, New York	United States	6461	Zayo
17	No Response	↓	-	-	-	-	-
18	149.96.6.118	Application	Servicenow	-	United States	16839	Servicenow

Figure 100. User detail: end-to-end connection detail (2 of 2)

ZDX ServiceNow Application

The ServiceNow solution integrates with ZDX Alerting to set up near real-time alerts that are pushed through webhook to the ServicenNow Incident Management system and the ability to create Deep Tracing sessions right from the ServiceNow instance.

The Zscaler Digital Experience Incident Management integration application provides the following features:

- Automatically create Incidents in a customer's ServiceNow instance whenever a rule configured in the Zscaler Digital Experience (ZDX) Admin Portal has been triggered.
- Zscaler Digital Experience's Deep Tracing feature has been enabled in the application: it is designed for creating Deep Tracing Sessions in ZDX Admin Portal from ServiceNow, thus reducing the number of actions needed to resolve Incident.

Requirements:

- Internet Technology Service Management (ITSM) software, which integrates with ZDX and must be configured on the ZDX side (alerting, webhook, system users, etc.). Instructions are included the following sections.

  For more information about ZDX alerts, see About Alerts (government agencies, see About Alerts). For more information about ZDX users and roles, see Adding ZDX Roles (government agencies, see Adding ZDX Roles).
- A web service user who is used to authenticate against target ServiceNow instances.
- A System user on the ZDX side who is used to authenticate against ZDX API to create Deep Tracing sessions.

Install the ZDX ServiceNow Application

To install the ZDX ServiceNow application:

1. Log in to the ServiceNow Instance as administrator.
2. In the **Filter Navigator** type Applications.
3. Click **All**.
4. In the search bar, type `Zscaler Digital Experience`.
5. Click **Install**.

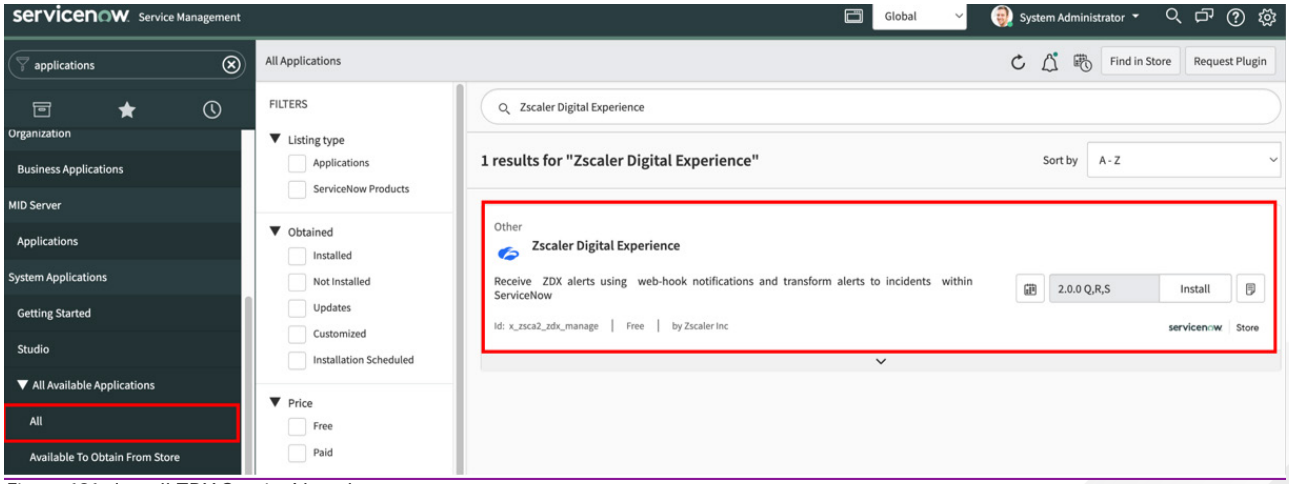


Figure 101. Install ZDX ServiceNow App

6. Once the installation is complete the browser window automatically reload

Configure ServiceNow Service Account in ZDX

Before configuring the integration, Zscaler recommends creating a dedicated service account with Web Service Access Only rights.

To configure the service account in ServiceNow:

1. Login as administrator to the ServiceNow instance.
2. In the **Filter Navigator**, type `sys_user.list`.

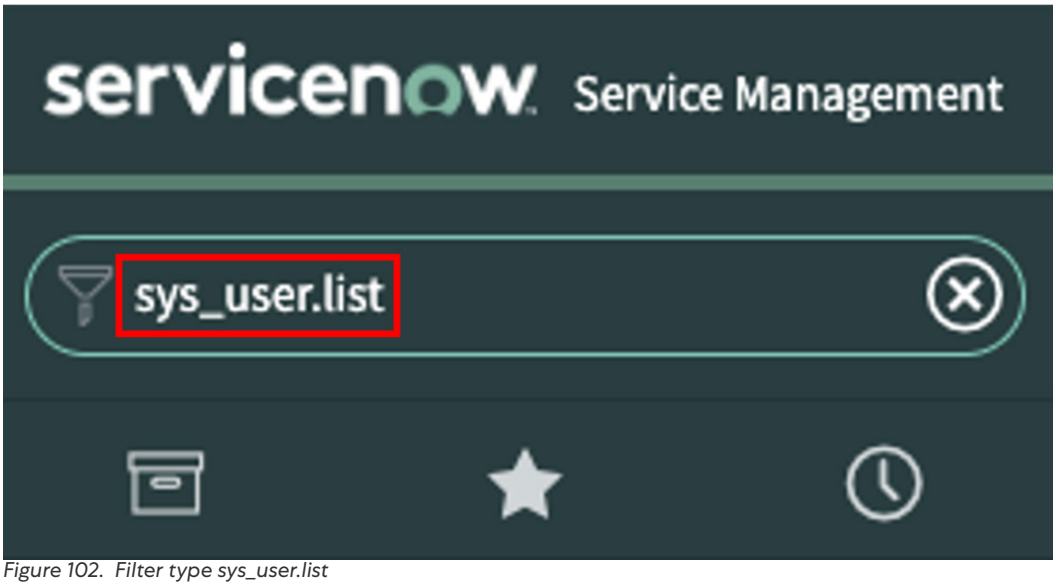


Figure 102. Filter type sys_user.list

3. In the list of users, select **New**.
4. Provide a **User ID** for the new user. This is used by ZDX for authentication.
5. Provide a **First Name**, **Last Name**, and **Password**.
6. Provide an **Email** address for the service account.
7. Select **Web Service Access Only**.
8. Click **Submit**.

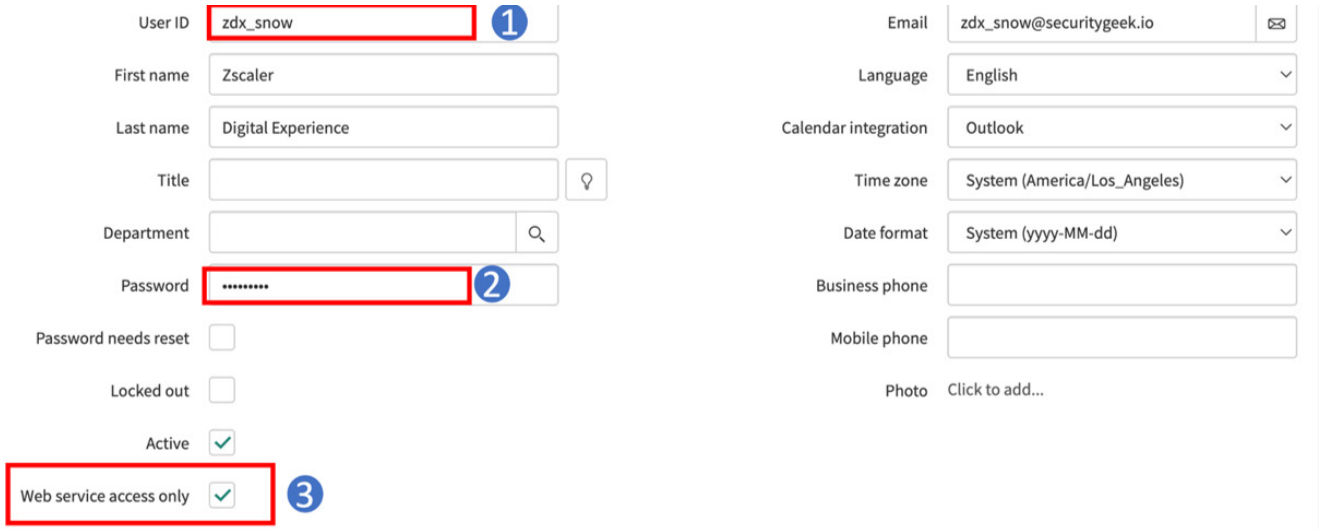


Figure 103. Configure service account

9. Edit the user's roles and add the **x_zsca2_zdx_manage.zdx_management** role so that it can access the application and its contents.

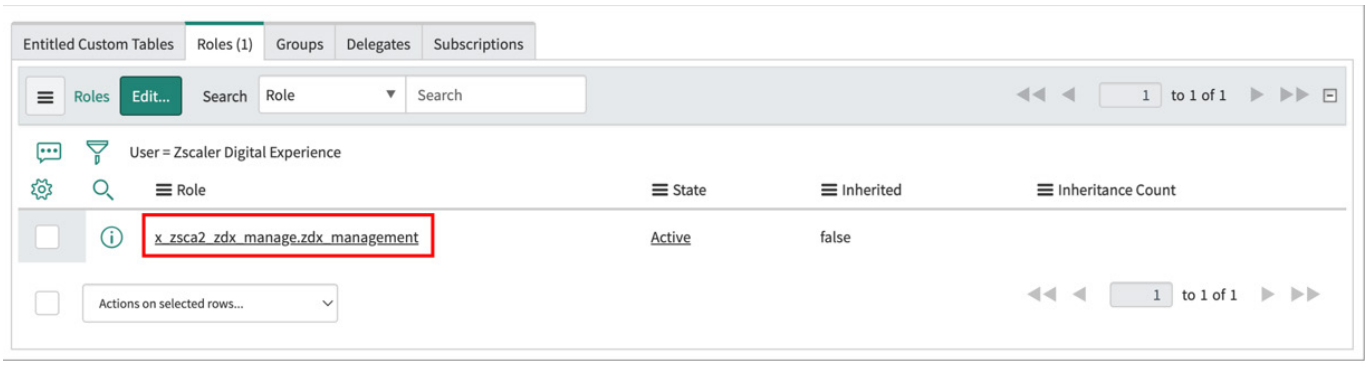


Figure 104. ServiceNow User Role

Configure the ZDX ServiceNow Application

To configure the ZDX ServiceNow application, type Zscaler Digital Experience in the filter navigation

1. Select **Setup**.

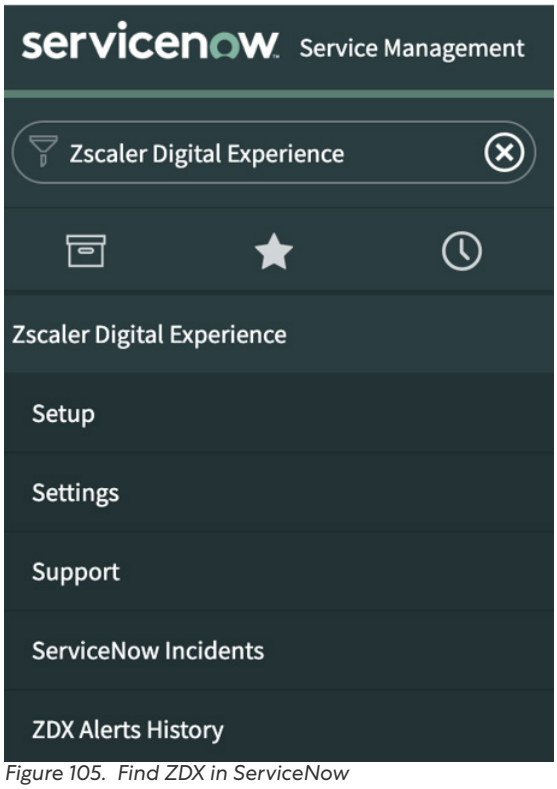


Figure 105. Find ZDX in ServiceNow

2. Click **Get Started** in **Configure the connection and settings**.

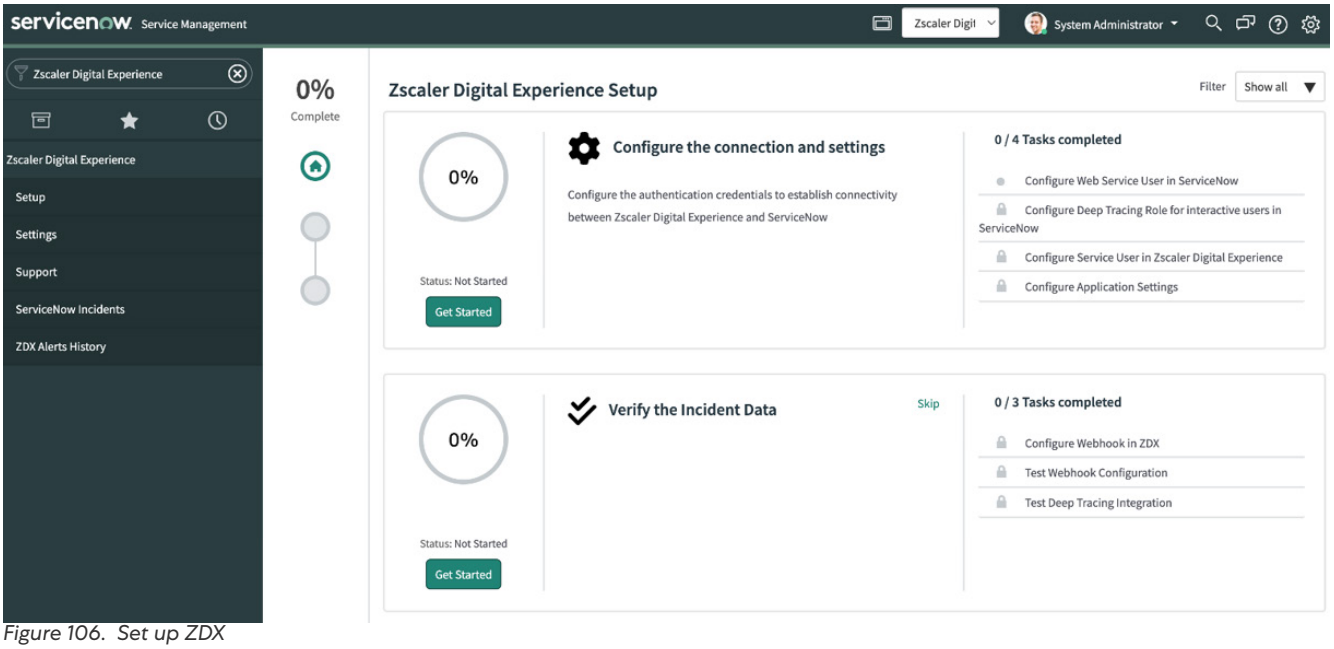


Figure 106. Set up ZDX

Configure Deep Tracing Role for Interactive Uses in ServiceNow

For those interactive users who will be working with the Deep Tracing feature, the zdx_dt_management role should be assigned as follows:

1. Go to **All** > **User Administration** > **Users** and then open a user record.
2. In the **Roles** related list, click **Edit**.
3. In the **Collection** list, select the **x_zsca2_zdx_manage.zdx_dt_management** role and assign it to the targeted user.
4. Click **Save**.

A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user. Whenever a user is assigned a new role, it only takes effect after logging in with a new session.

Configure Service User in Zscaler Digital Experience

In order to authenticate against the ZDX API it is mandatory to create a service user in ZDX. Below steps describe the process of creating such user in ZDX:

1. Go to **Administration** > **Role Management** > **Add ZDX Role**.
2. Enter a **Name** (e.g., ServiceNow Role).
3. Configure permissions as shown in the following table.

Permission Name	Required Value
Deep Tracing	Full
Webhooks	Full
User and Device Names	Visible
Configuration Access	Full
Alerts	Full
UCaaS Monitoring	View Only

4. Click **Save**.
5. Go to **Administration** > **Administrator Management** > **Add ZDX Admin**.
6. Enter a **Login ID** (e.g., servicenow_user)
7. Select the role you created previously.
8. Enter an **Email** and **Name**, and select a scope.
9. Enable **Password Based Login** option and enter secure password.
10. Click **Save**.

Configure Application Settings

Configure applications settings such as caller name, alert category, logging level and other properties.

1. Click **Configure**.

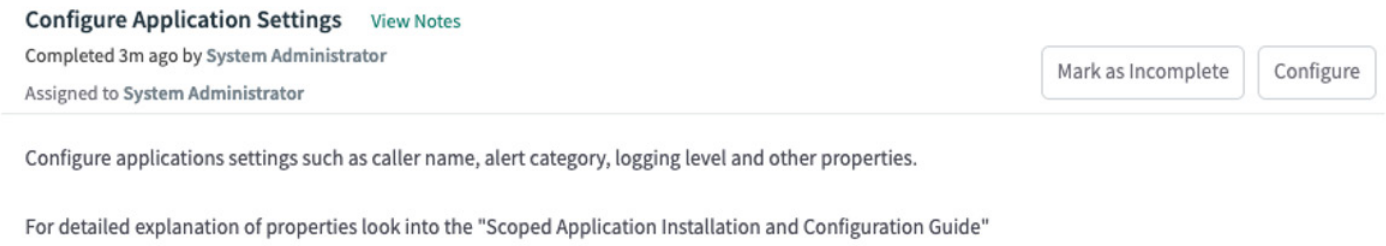


Figure 107. Configure Application Settings

2. In the **Zscaler Digital Experience Properties** page, enter the required information.
3. Click **Save**.

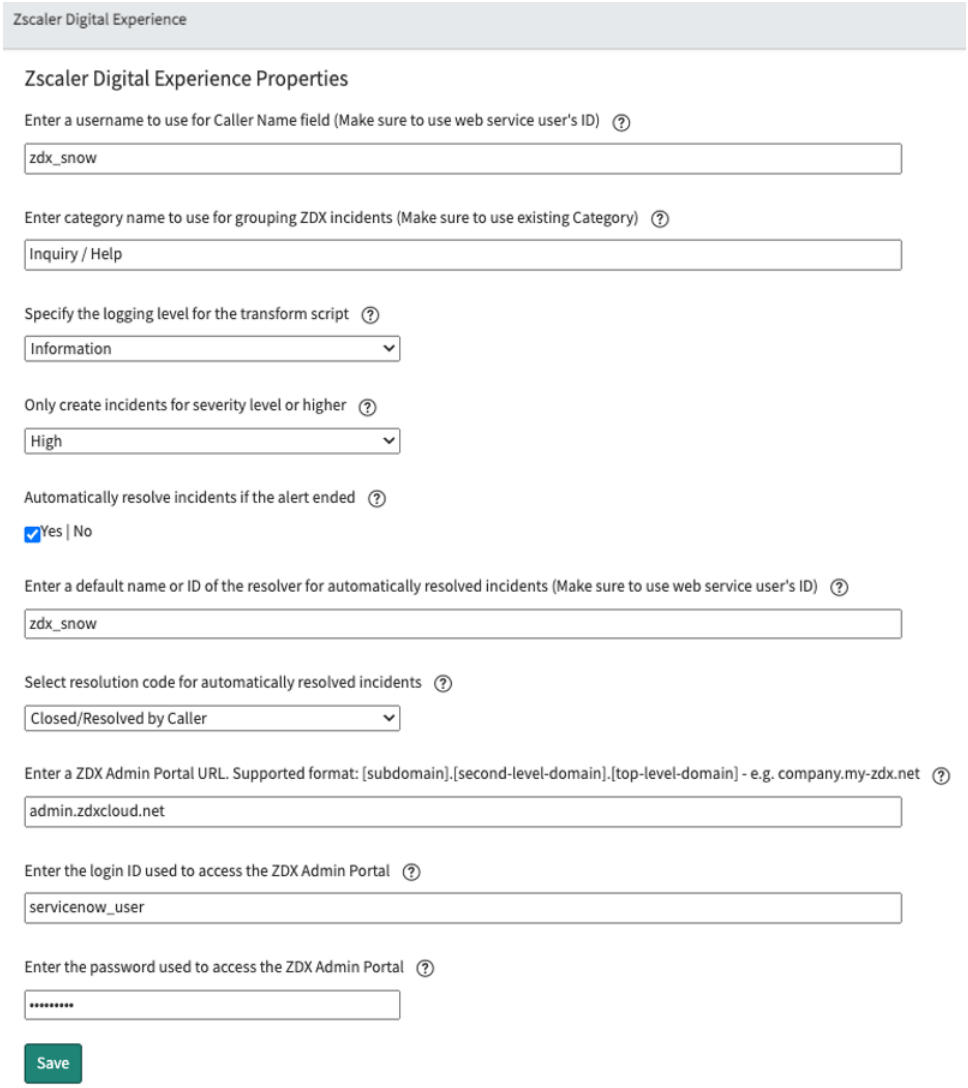


Figure 108. Configure ZDX properties

Configure ZDX Webhook in ZDX

To configure ZDX to perform Webhook calls into ServiceNow:

1. Login as administrator to the ZDX portal.
2. From the sidebar select **Administration** and from the opened menu select **Webhooks**.
3. You are redirected to the **Webhooks** windows. Click **Create new webhook**.
4. Use the following URL for the **Incident Management endpoint**:

   ```
   https://[your-instance-id].service-now.com/api/x_zsca2_zdx_manage/
   incident_management_api
   ```

5. Use the credentials for the user you created in the previous step.
6. In order to test the integration go to the webhook configuration page in ZDX, open your webhook and click **Test Webhook**.
7. Click **Save**.

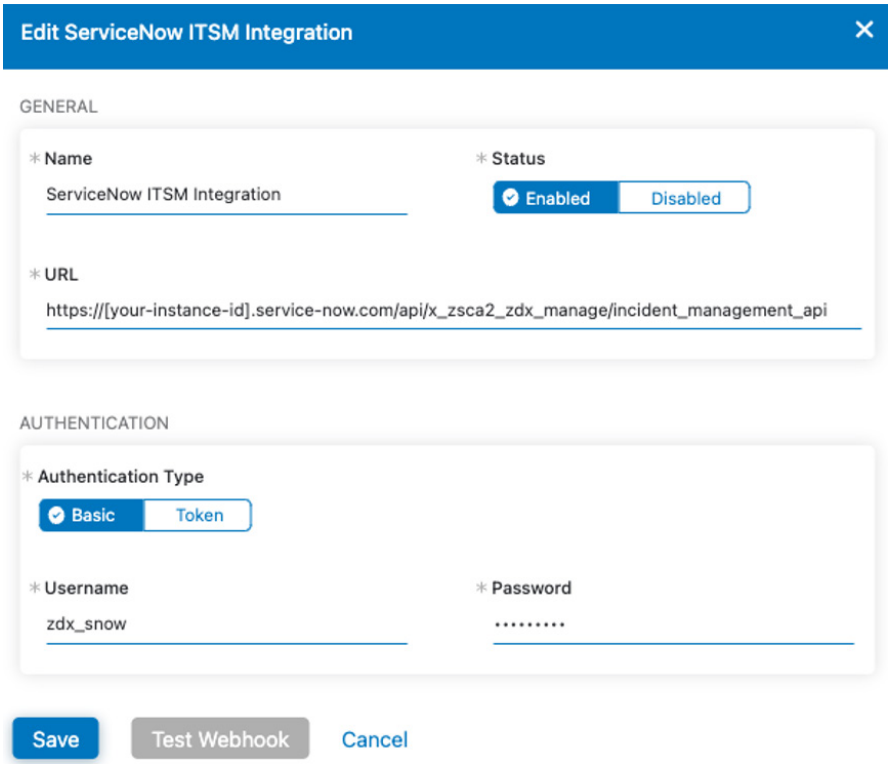
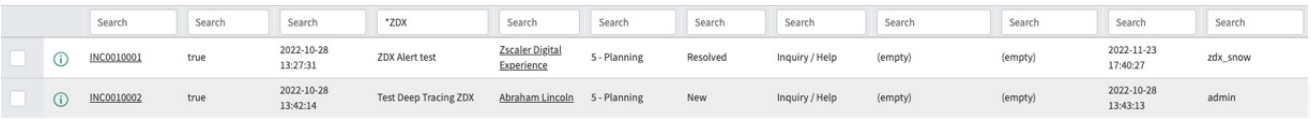


Figure 109. Edit ServiceNow ITSM Integration

8. Go to the ServiceNow instance and from the ZDX application and select the **ServiceNow Incidents** menu to verify that a test alert created an incident.



	Search	Search	Search	*ZDX	Search	Search	Search	Search	Search	Search	Search	Search	
	INC0010001	true	2022-10-28 13:27:31	ZDX Alert test	Zscaler Digital Experience	5 - Planning	Resolved	Inquiry / Help	(empty)	(empty)	2022-11-23 17:40:27	zdx_snow	
	INC0010002	true	2022-10-28 13:42:14	Test Deep Tracing ZDX	Abraham Lincoln	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2022-10-28 13:43:13	admin	

Figure 110. ServiceNow Incidents Menu

Test ZDX Deep Tracing Integration with ServiceNow

To ensure that the Deep Tracing connection is also working correctly:

1. In the **Filter Navigator** search for `Zscaler Digital Experience`.
2. From the menu select `ServiceNow Incidents`.
3. Open target Incident record.
4. Go to the **Deep Tracing** section.

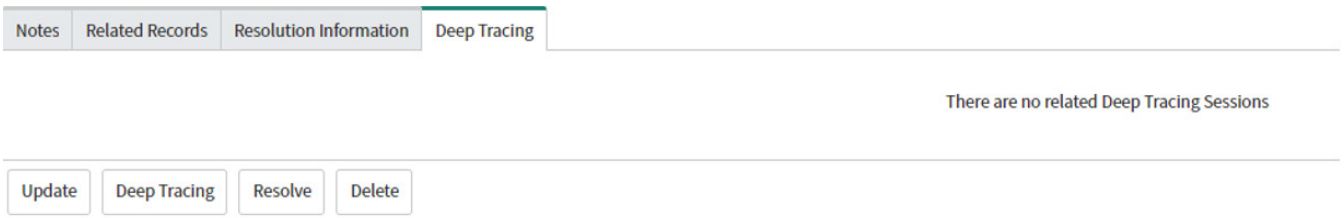


Figure 111. Deep Tracing Sessions

You might see the information message **There are no related Deep Tracing Sessions**. This means that no deep tracing sessions related to the current incident exist in ZDX.

ZPC: ServiceNow Integration for Ticket Creation

Zscaler Posture Control (ZPC) integrates with ticketing systems to automatically log incidents when misconfigurations or compliance violations are discovered. These violations and misconfigurations can be related to cloud environments such as AWS, Azure, GCP, and IaC events. ZPC integrates with incident management (ticketing) tools such as ServiceNow to automate the incident creation and expedite resolution.

The process to configure the integration includes the steps below:

- Create a ServiceNow user account with Web Service Only capability to open incidents in the SNOW platform.
- Configure ZPC Incident Management for ServiceNow integration.
- Create a ZPC Notification Rule.
- Verify ServiceNow Incidents tickets for ServiceNow admins.

ServiceNow: Configure Service Account

Before configuring the integration, Zscaler recommends creating a dedicated service account with "Web Service Access Only" rights.

To configure the service account in ServiceNow:

1. Login as administrator to the ServiceNow instance.
2. In the **Filter Navigator** type `sys_user.list`.

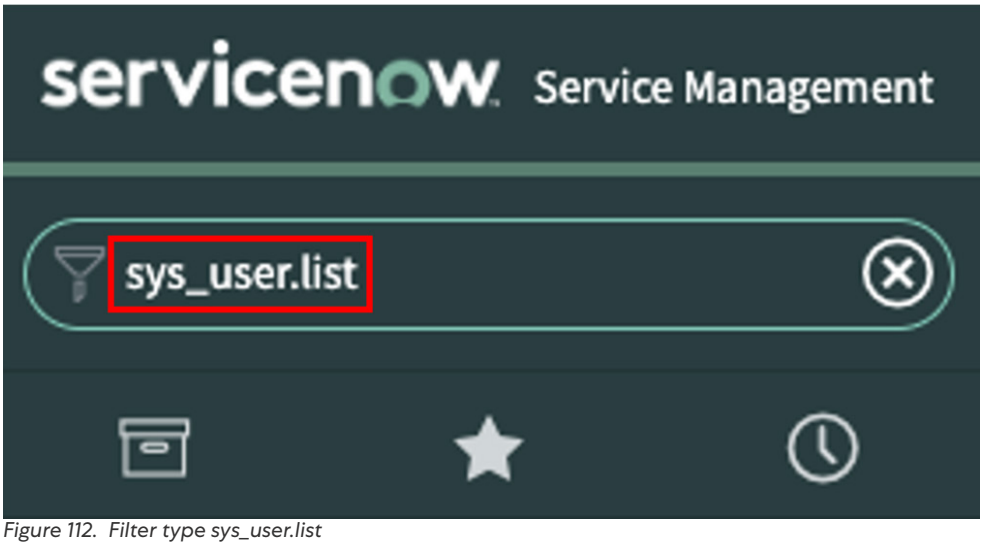


Figure 112. Filter type sys_user.list

3. In the list of users, select **New**.
4. Provide the **User ID** for the new user. This is used by ZPC for authentication.
5. Provide a **First Name**, **Last Name**, and **Password**.
6. Provide an **Email** address for the service account.
7. Select the **Web Service Access Only** option.
8. Click **Submit**.

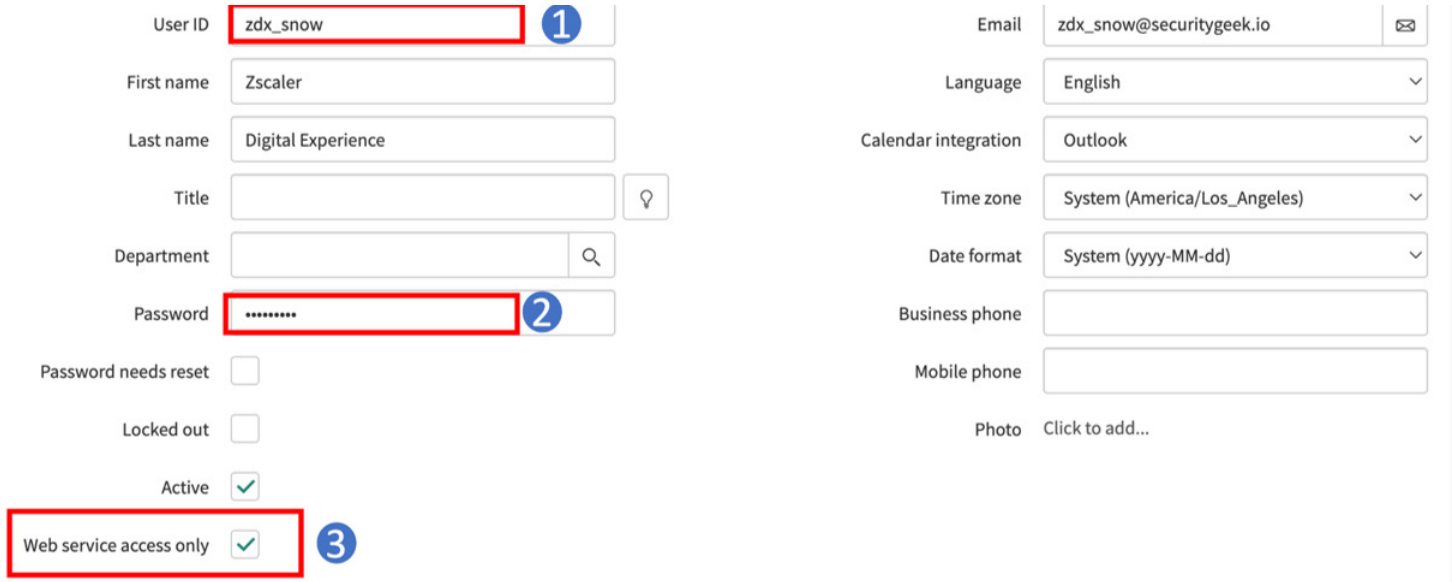


Figure 113. Configure service account

Configure ZPC and ServiceNow Integration

To configure the ServiceNow ticketing system integration:

1. Log in to the ZPC portal as an administrator.
2. Go to **Administration**, then select **Integrations**.
3. On the **Integrations** windows, click **Add** under the **ITSM** section.

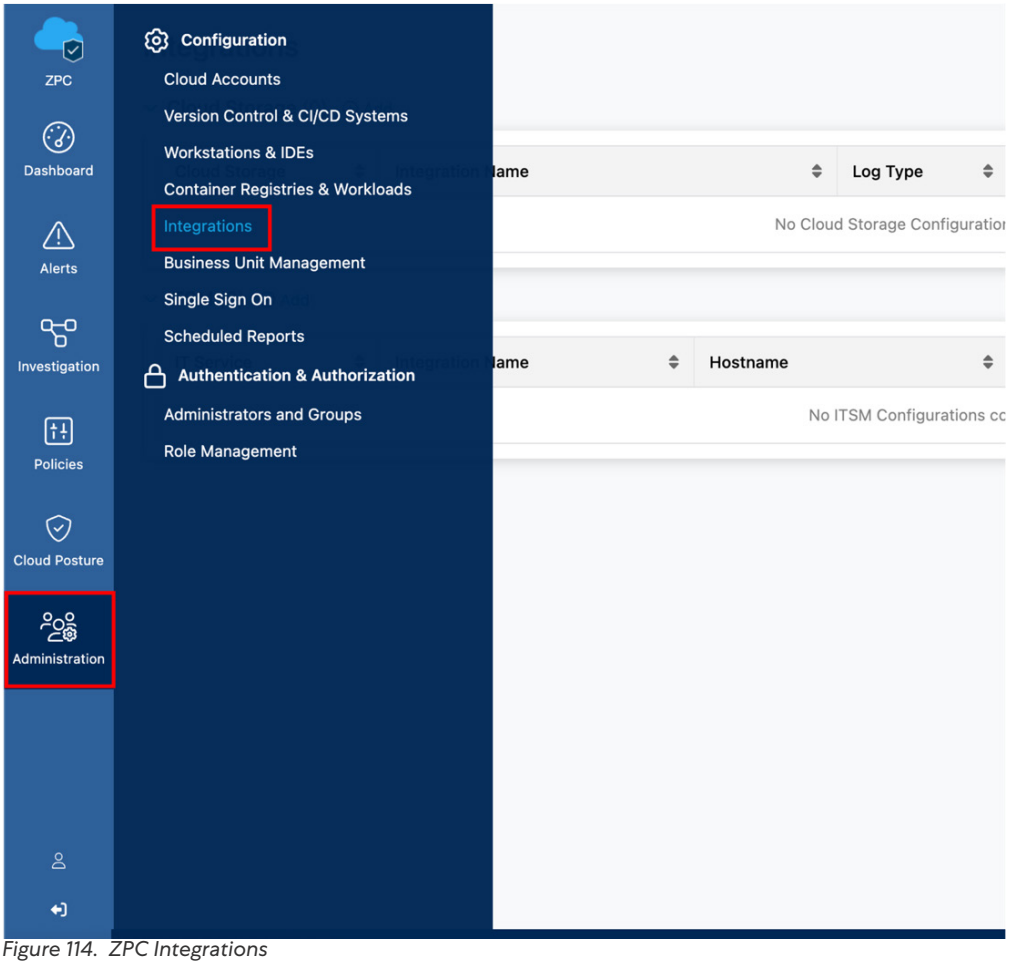


Figure 114. ZPC Integrations

ZPC ServiceNow ITSM Configuration

On the Integrations page:

1. Go to ITSM and select **Add**. The **Add ITSM Integration** window displays.

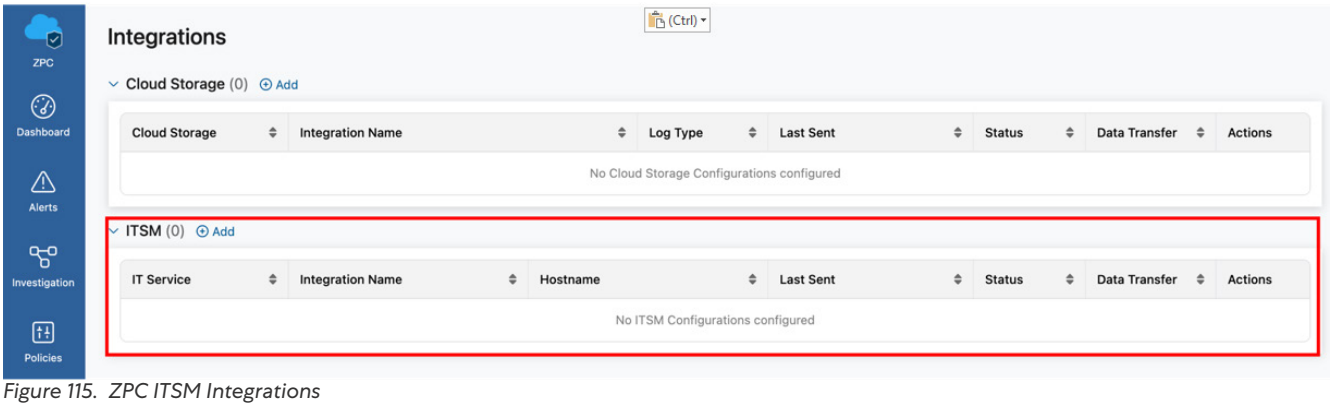


Figure 115. ZPC ITSM Integrations

2. Give the integration a name.
3. Select **ServiceNow**.
4. Click **Next**. The **Add ITSM Details** window displays.

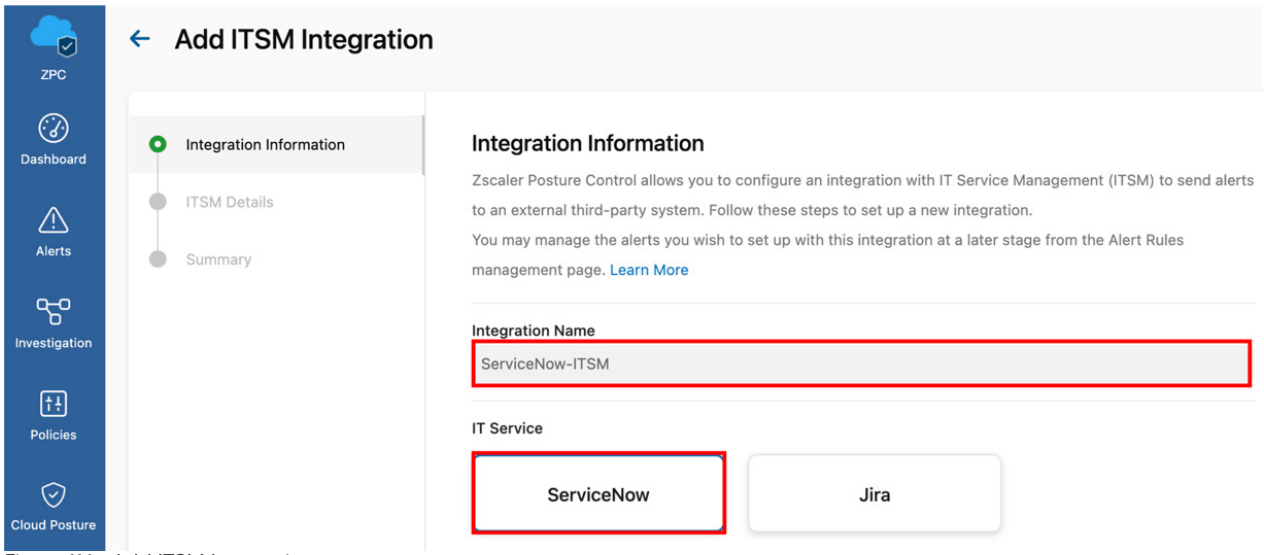


Figure 116. Add ITSM Integration

5. Enter the ServiceNow instance ID into the **ServiceNow Hostname**.
6. Enter the ServiceNow account with rights to create incidents into the **ServiceNow Username**.
7. Enter the **ServiceNow Password**.
8. Click **Test Connection**. If the validation was successful, the message **ServiceNow credentials have been validated** displays.
9. Click **Next**.

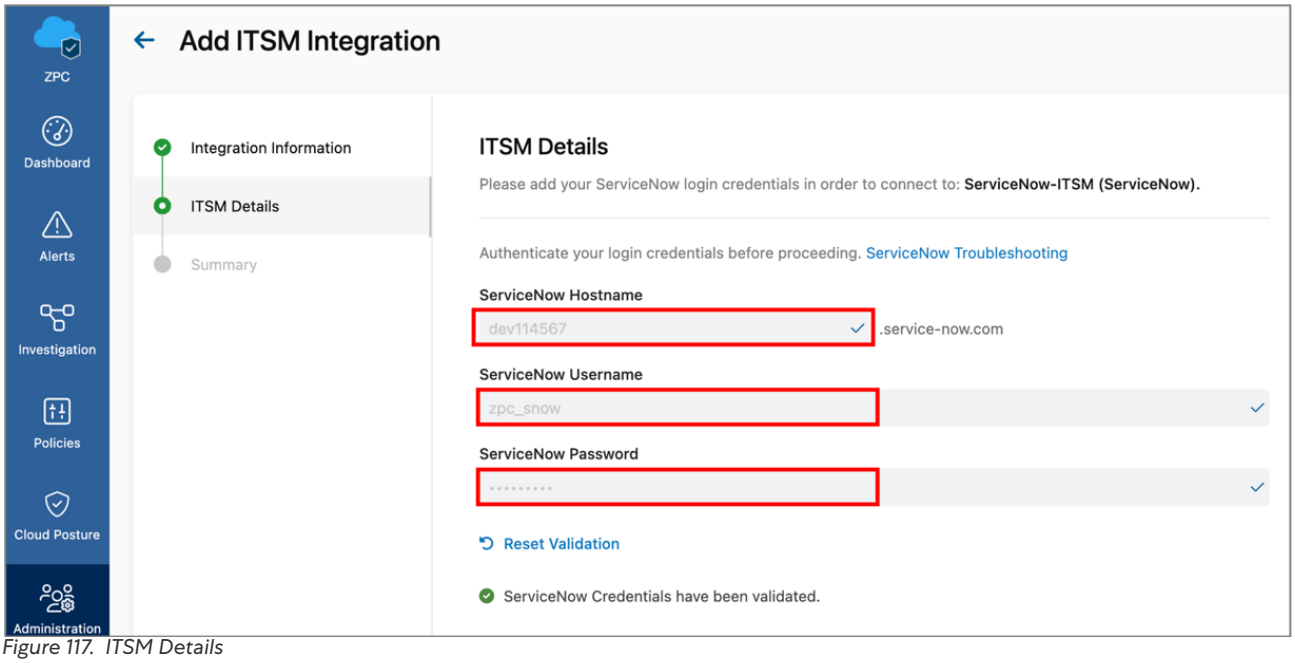


Figure 117. ITSM Details

10. Review the summary.
11. Click **Finish**.

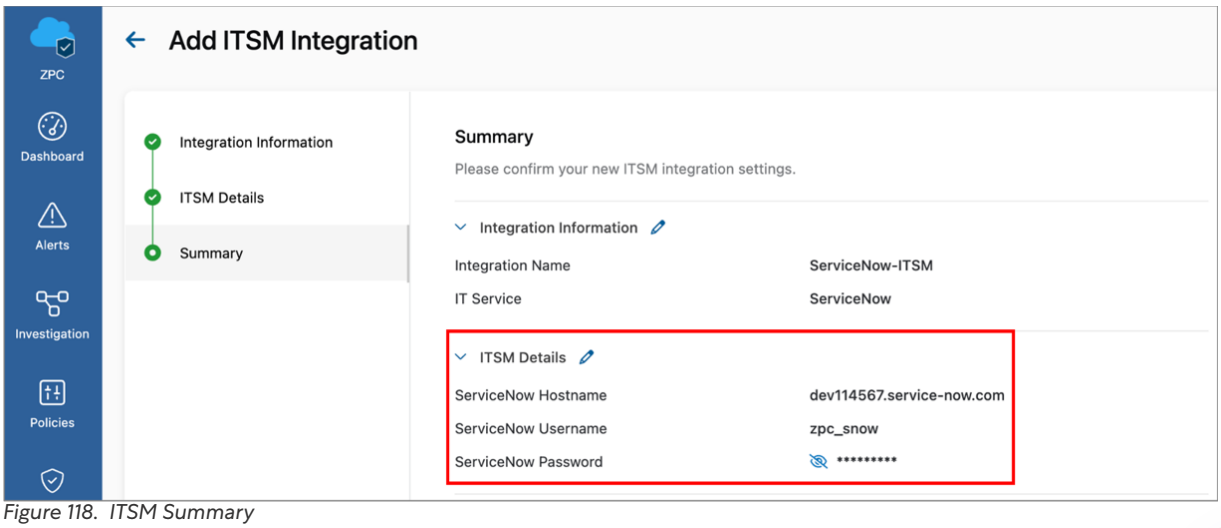


Figure 118. ITSM Summary

Once the configuration is complete, the integration Status is Pending, until a Notification Rule is created and new notifications are sent to ServiceNow.

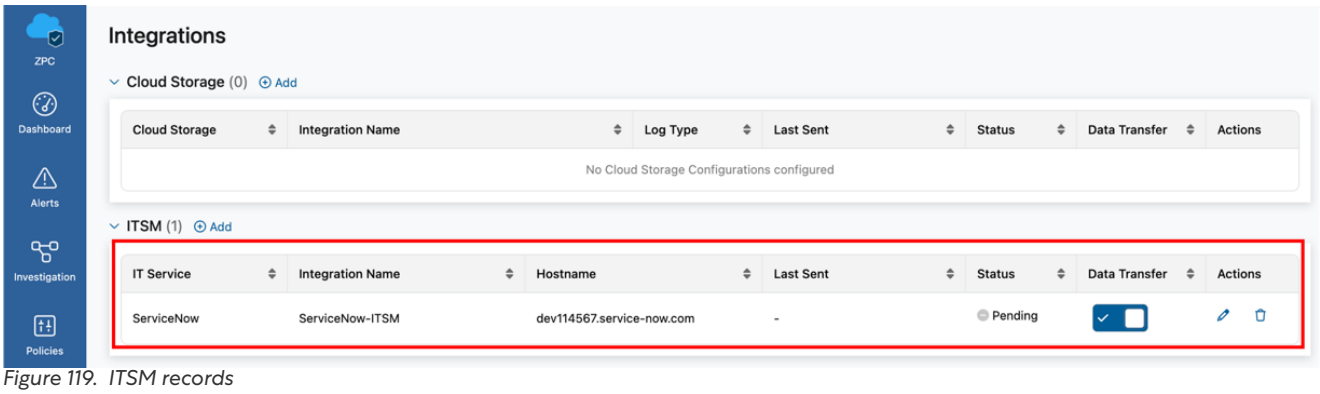


Figure 119. ITSM records

ZPC: Create Notification Rules

ZPC sends notifications to ServiceNow ITSM based on alerts generated due to security and compliance violations in cloud workloads and IAC.

On the Administration Page page:

1. Click **Alerts**.
2. Select **Notifications**.
3. Click **Create Rule**.

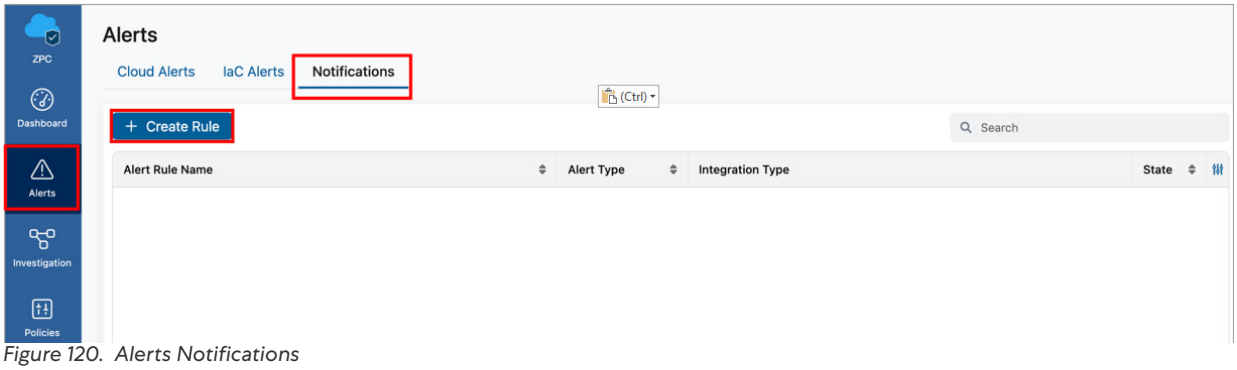


Figure 120. Alerts Notifications

ZPC: Create A Cloud Notification Rule

To create a cloud notification rule:

1. Provide an **Alert Rule Name** to the notification rule.
2. Select **Cloud** in **Alert Type**.
3. Select **Alert Rule Status**.
4. Click **Next**.

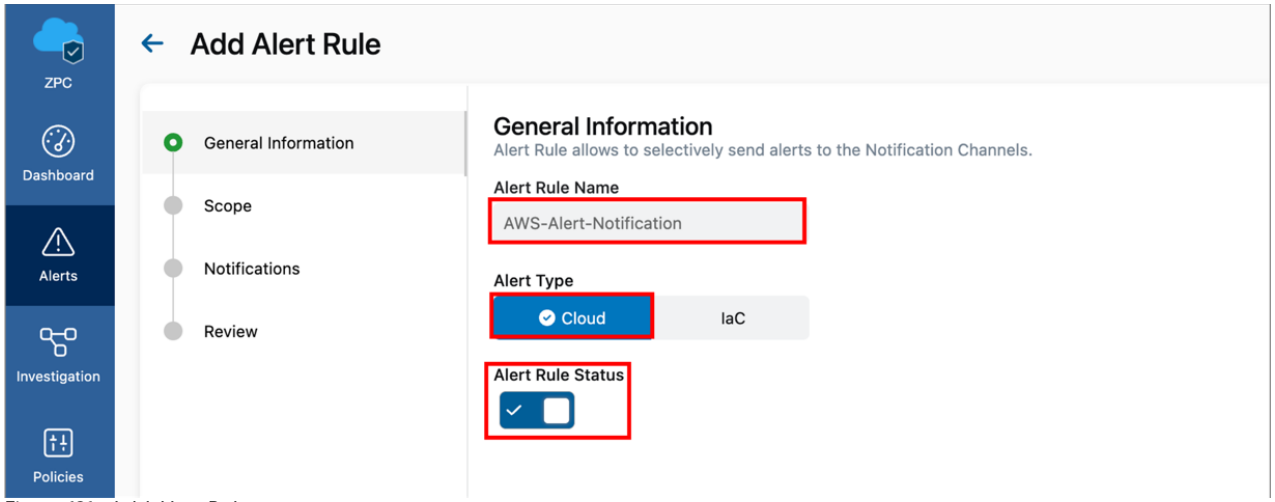


Figure 121. Add Alert Rule

5. In the **Scope** window, select the scope for which you wish to receive notifications.
6. In the **Select Policy** section, select the policies which you want alerts to be sent to ServiceNow.
7. Click **Next**.

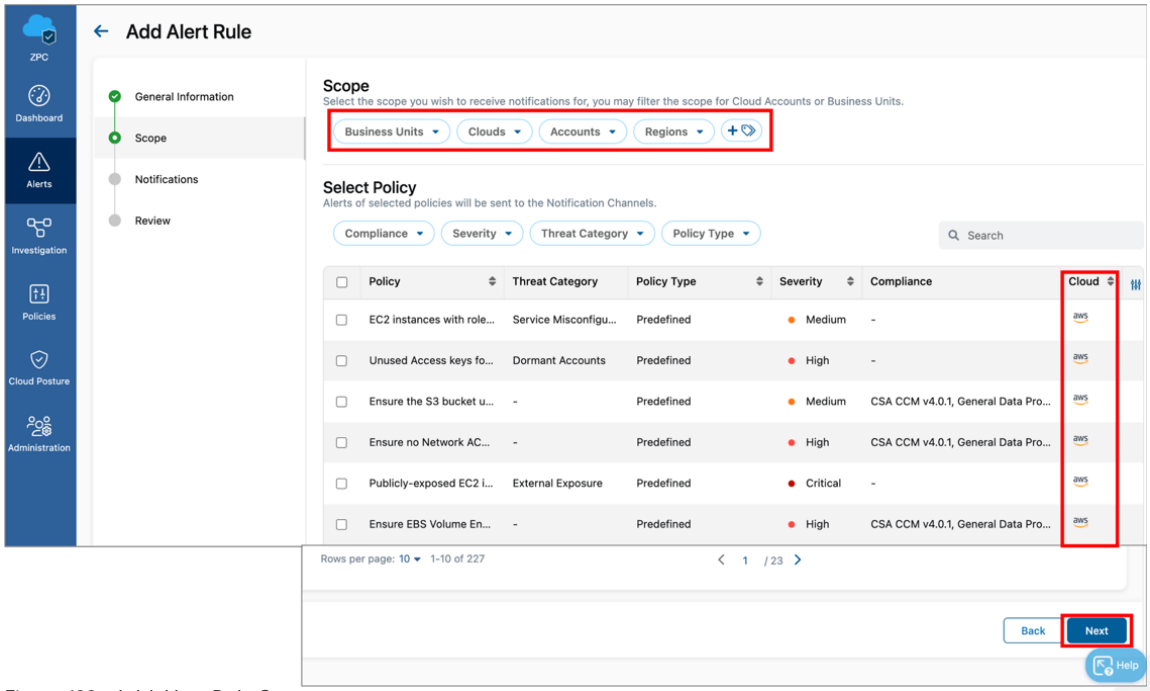


Figure 122. Add Alert Rule Scope

8. In the **Notifications** window, select **ServiceNow** in the **ITSM/Ticketing** section.
9. Select the integration configured in the drop-down menu.
10. In **Assignee**, provide the email address you'd like notifications to be sent when an incident is closed or resolved in ServiceNow. The following options are available:
    a. **Send Notifications for closed Alerts**.
    b. **Send Notifications for resolved Alerts**.
11. Click **Next**.

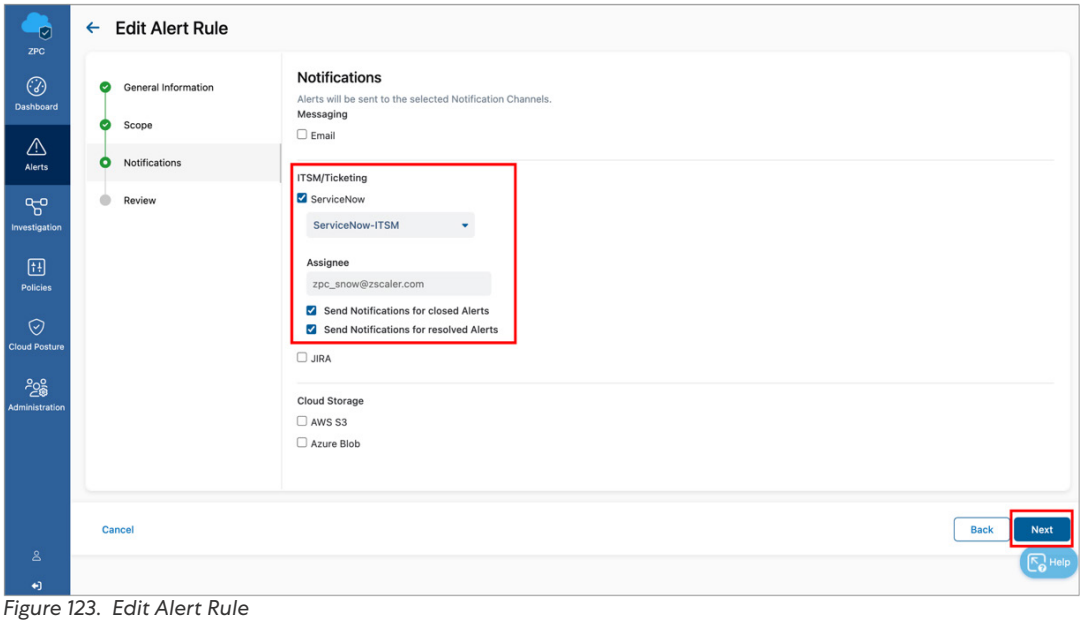


Figure 123. Edit Alert Rule

12. In the **Review** window, review the information to ensure everything is correct.
13. Click **Finish**.

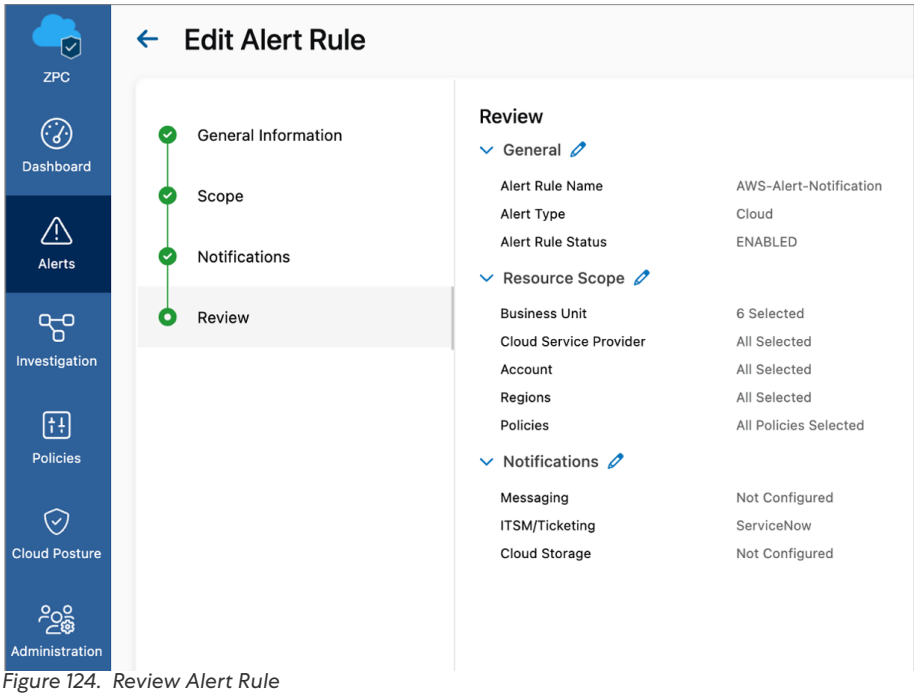


Figure 124. Review Alert Rule

The alert is displayed in the **Notifications** window.

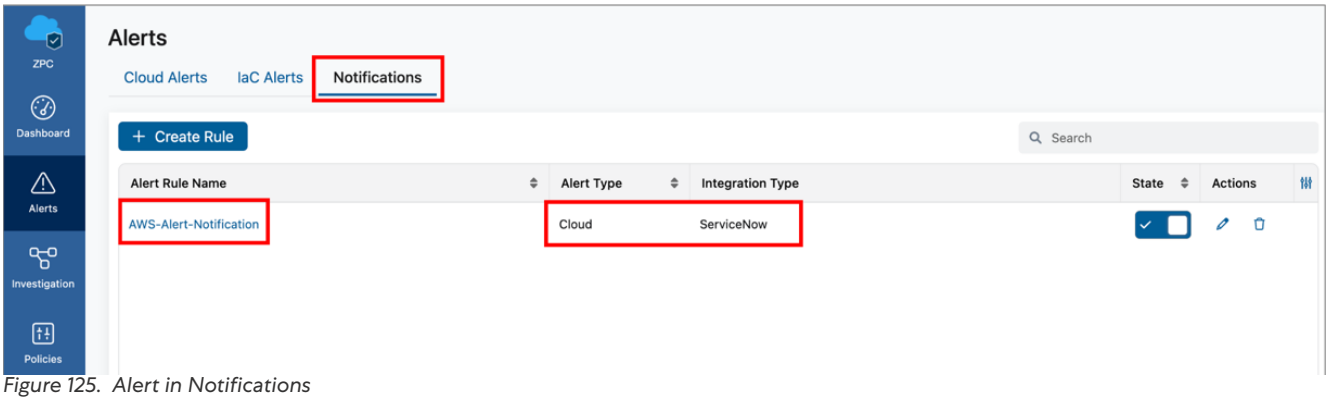


Figure 125. Alert in Notifications

ZPC: Create IaC Notification Rule

To create an IaC notification rule:

1. Provide an **Alert Rule Name** for the notification rule.
2. Select **IaC** in **Alert Type**.
3. Select **Alert Rule Status**.
4. Click **Next**.

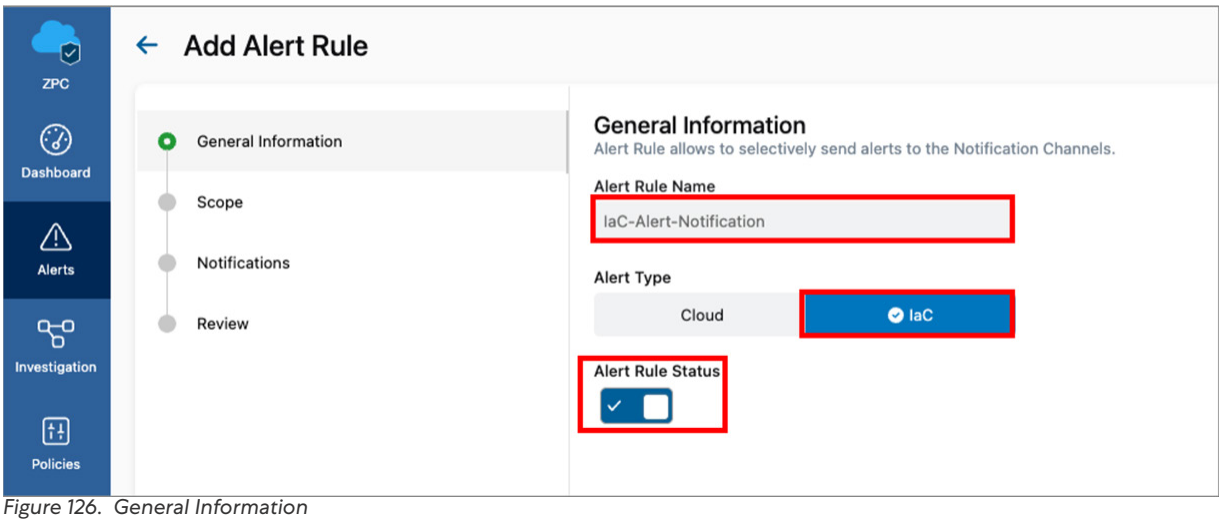


Figure 126. General Information

5. In the **Scope** window, select the **Scan Plugin or Repository.** Alerts associated with Scan Plugins and Repositories are sent to the ServiceNow Notification Channel.
6. Configure the **Scan Plugin** options:
   a. **GitHub Actions**
   b. **Jenkins**
   c. **GitLab**
   d. **Azure Pipelines**
   e. **Azure Repos**
7. Select the repositories for which you want notifications to be sent to ServiceNow via the notification rule.

8. In **Select Policy**, ZPC allows several different compliance policy values:
    a. **CIS (Center for Internet Security)**
    b. **CSA CCM (CSA Cloud Controls Matrix)**
    c. **HIPAA**
    d. **ISO-IEC 27001**
    e. **NIST SP 8000**
    f. **PCI DSS 3.2.1**
    g. **SOC 22**
    h. **Zscaler Best Practices**

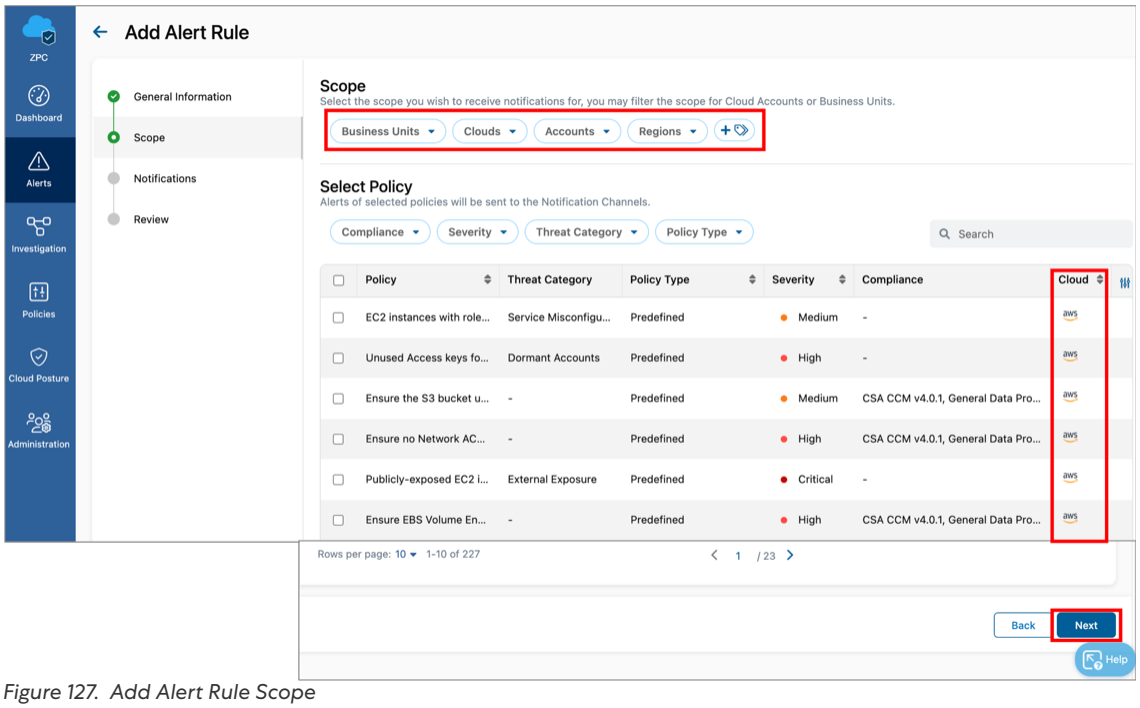


Figure 127. Add Alert Rule Scope

9. In the **Notifications** window, select ServiceNow in the **ITSM/Ticketing** section.
10. Select the integration configured in the drop-down menu.
11. In the **Assignee** field, provide the email address you'd like notifications to be sent when an incident is closed or resolved in ServiceNow. The following options are available:
    a. **Send Notifications for closed Alerts**.
    b. **Send Notifications for resolved Alerts**.
12. Click **Next**.
13. Click **Finish**.

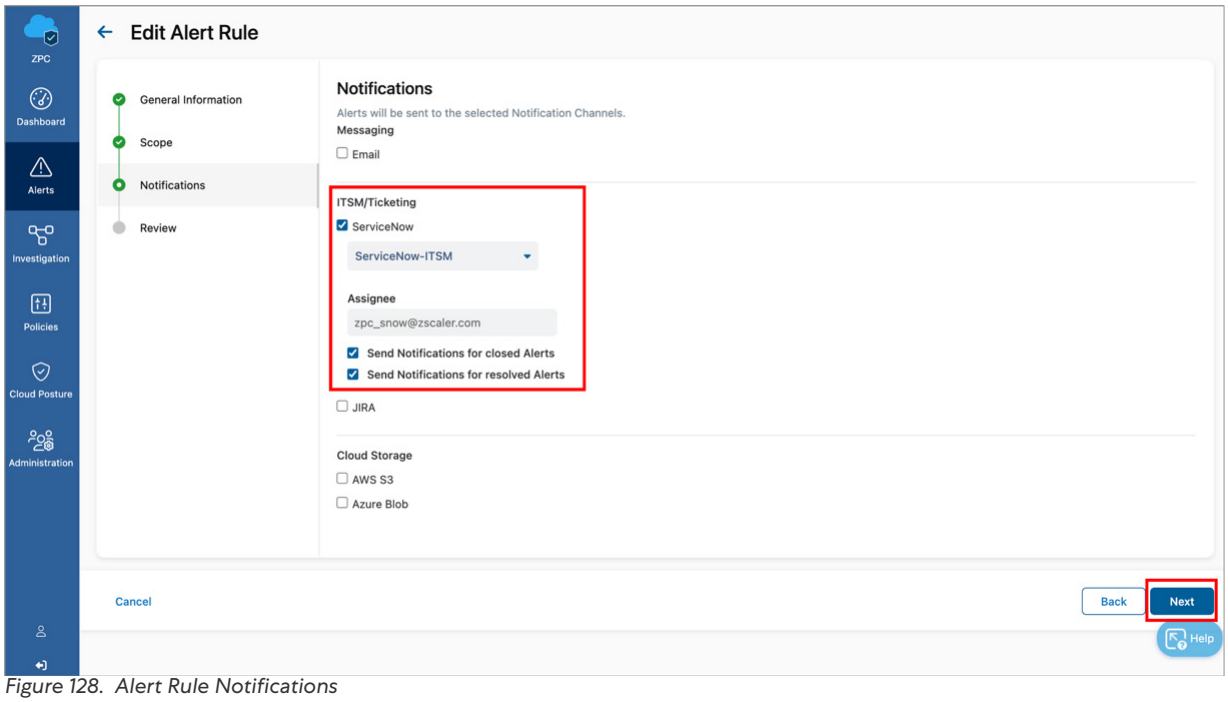


Figure 128. Alert Rule Notifications

Alerts are displayed in the Notifications window.

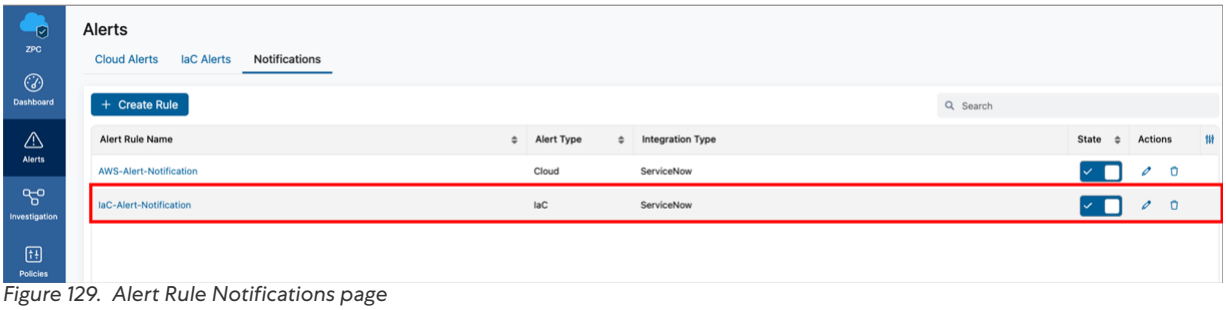


Figure 129. Alert Rule Notifications page

ZPC ServiceNow Incidents

ZPC creates incident, problems, or problem tasks for security workflow management and compliance violations found in your monitored cloud services and IAC. The ServiceNow entries contain the following fields by default (additional customization can be applied):

- Incident: Includes a Short Description, a more Detailed Description, Problem ID, State, Priority, Urgency, Impact, Assigned To, and a Caller ID.
- Problem task: Includes a Short Description, a more Detailed Description, Problem, Workaround, Problem Task Type.
    - Problem task includes a Short Description and a more Detailed Description.

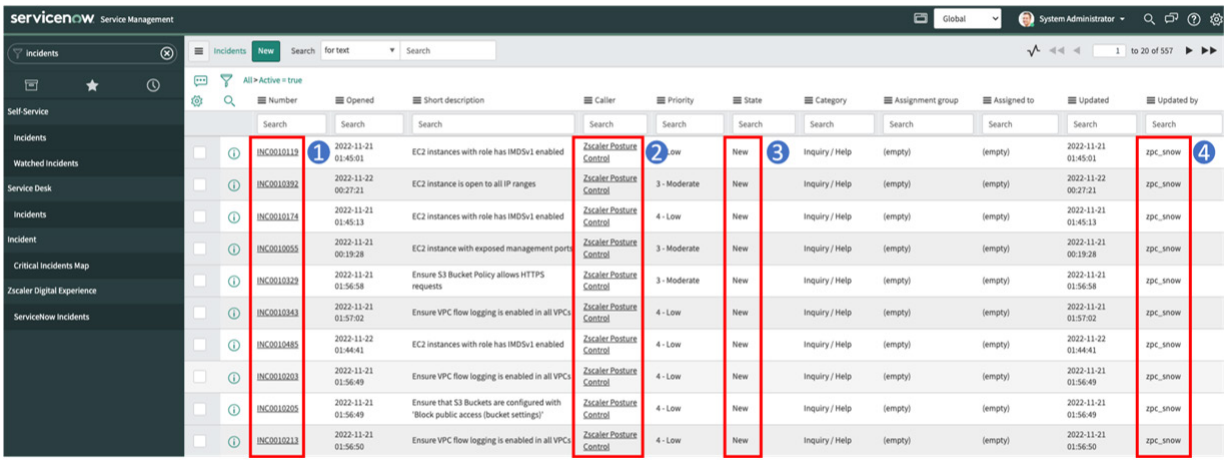


Figure 130. ServiceNow Incidents page

Appendix A: Requesting Zscaler Support

You might 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:

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

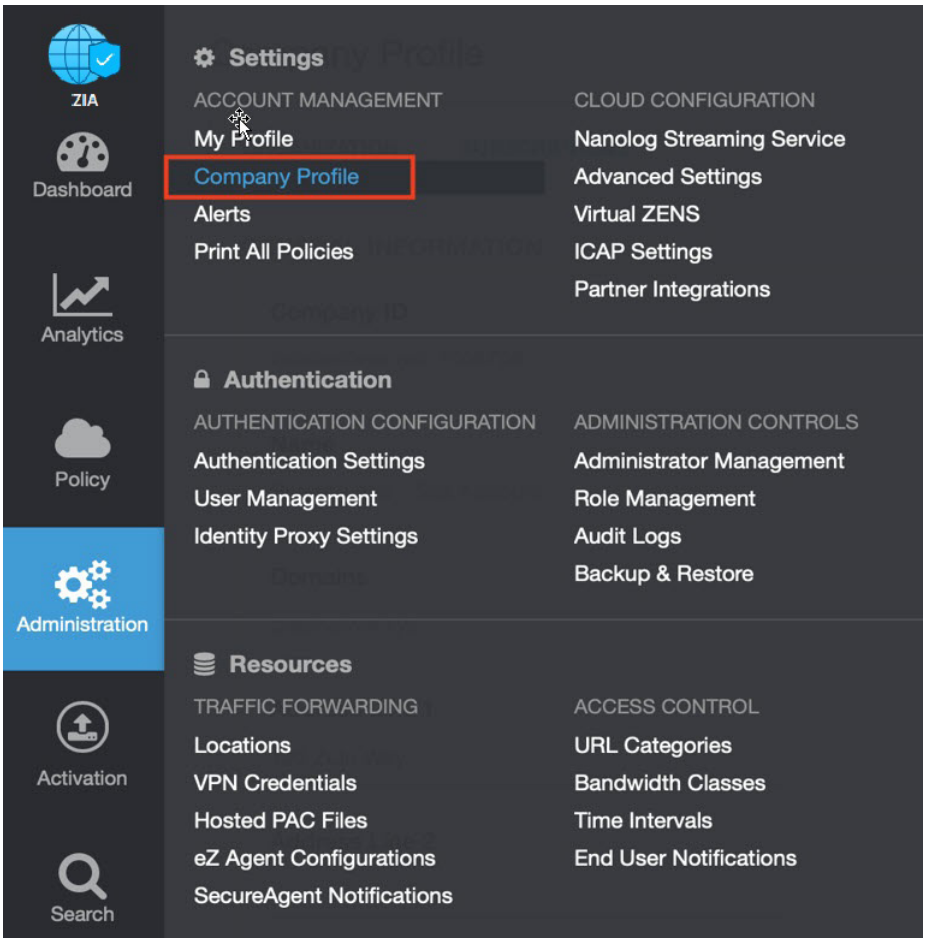


Figure 131. Collecting details to open a support case with Zscaler TAC

2. Copy the Company ID.

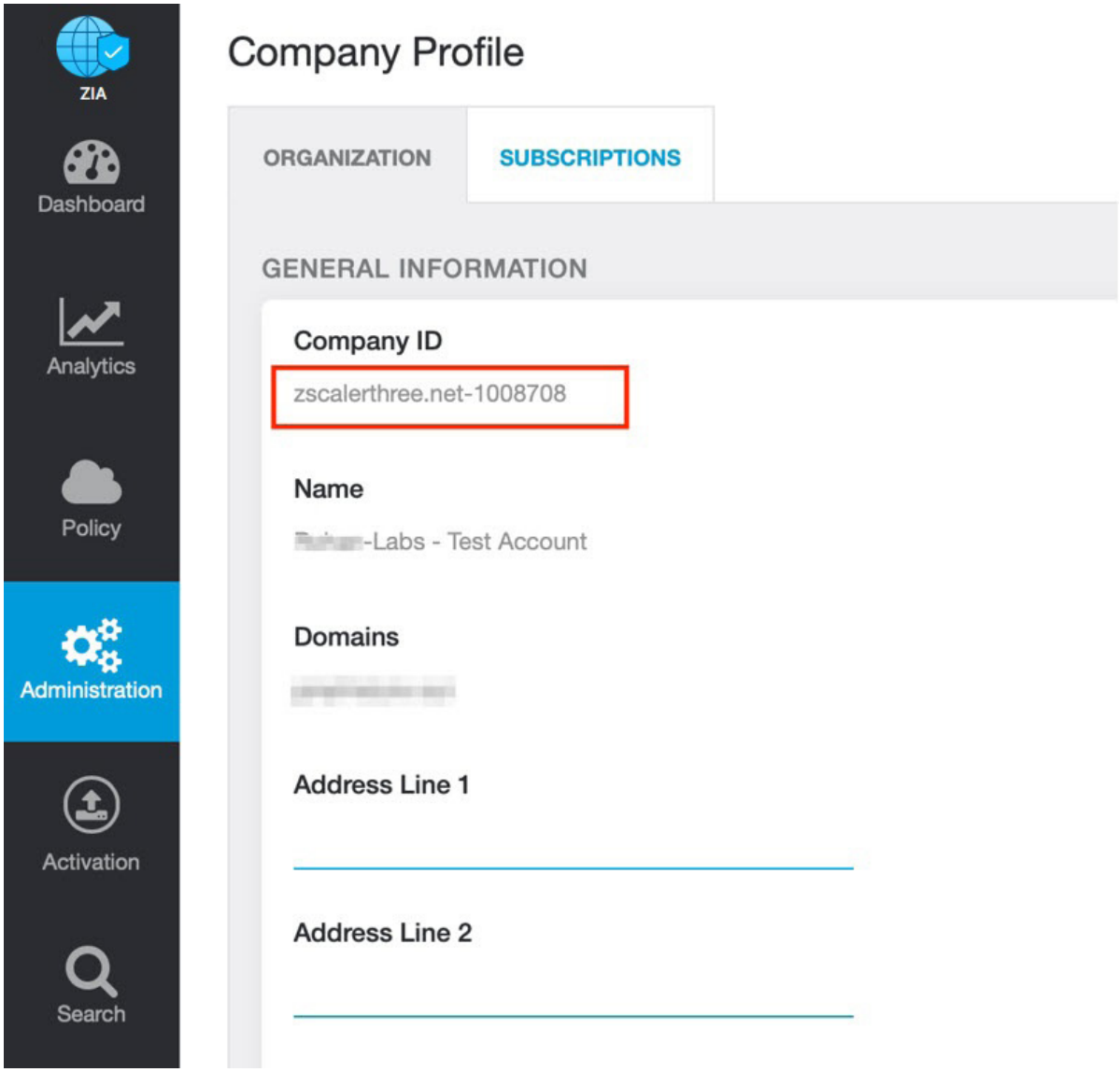


Figure 132. Company ID

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

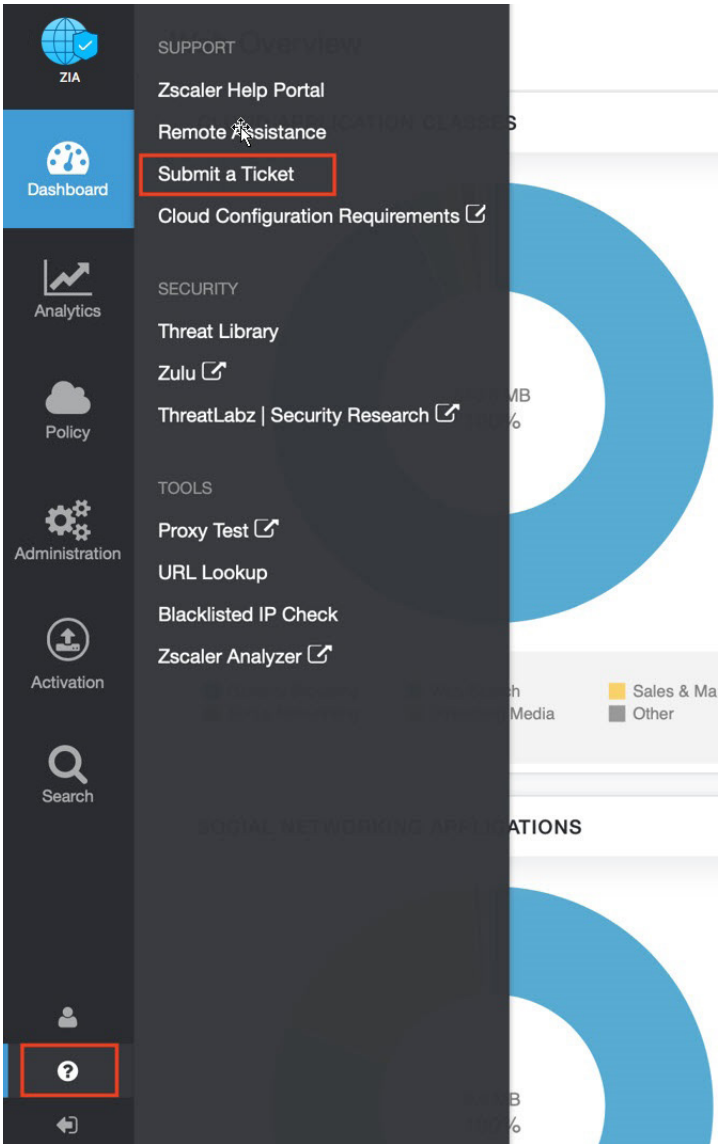


Figure 133. Submit a Ticket

