

# ZSCALER AND SERVICENOW DEPLOYMENT GUIDE

# Contents

<b>Terms and Acronyms</b>	<b>7</b>
<b>About This Document</b>	<b>8</b>
Zscaler Overview	8
ServiceNow Overview	8
Audience	8
Software Versions	8
Request for Comments	8
<b>Zscaler and ServiceNow Introduction</b>	<b>9</b>
ZIA Overview	9
ZPA Overview	9
Zscaler Resources	9
ServiceNow Platform	10
ServiceNow Resources	10
<b>Zscaler Data Protection and Digital Experience for ServiceNow.com</b>	<b>11</b>
ZIA SaaS Identity Proxy	12
ZIA Isolation	13
ZIA Data Loss Protection and Malware Detection for ServiceNow	14
What Makes Zscaler's SaaS Security Unique?	14
ZIA Cloud Application Control	15
ZDX for the ServiceNow User Experience	16
What Makes ZDX Unique?	16
ZPC and ServiceNow Incident Creation	17
<b>Configure the SaaS Identity Proxy</b>	<b>18</b>
Configure the ZIA Admin Portal for the SaaS Identity Proxy	19
Complete SaaS Identity Proxy	20
Configure ServiceNow to Use the Identity Proxy	21

Install the ServiceNow Plugins	22
Configure the SaaS Identity Proxy	23
Add Zscaler as an Identity Provider	24
Configure the Identity Provider	25
Add the Identity Provider Certificate and Additional Settings	26
Testing the Identity Provider	29
The Active Identity Proxy Notification	30
Configure Redirect on the Identity Provider	31
Configure the Property	34
<b>Configure Isolation</b>	<b>35</b>
Configure the Isolation Profile	36
Configure the Isolation Policies	44
<b>Configuring the ServiceNow Tenant</b>	<b>50</b>
Adding the ServiceNow Tenant	51
SaaS Tenant Configuration Wizard	52
Configuring the Zscaler Tenant on ServiceNow	54
Check that OAuth is Installed and Active	56
Check that the OAuth Plugin is Active	57
Create an OAuth Application Registry	58
Create an OAuth Application Registry	59
Configuring the Zscaler Tenant on ServiceNow	60
Copy the needed OAuth Credentials	62
Finishing the Zscaler Tenant on the ZIA Admin Portal	63
Configuring the Zscaler ServiceNow Connector	64
<b>Configuring ServiceNow Policies and Scan Configuration</b>	<b>65</b>
Scoping the Policies and Remediation	66
Creating a DLP Policy	67

Creating a DLP Engine	68
Creating a DLP Engine	69
Configure a SaaS DLP Policy	70
SaaS DLP Policy Details	71
Configure a SaaS DLP Policy	72
<b>Configure a SaaS Malware Policy</b>	<b>74</b>
SaaS Malware Policy	75
SaaS Malware Policy	76
<b>Configure the Scan Schedule Configuration</b>	<b>77</b>
Start the Scan Schedule	78
<b>Reporting and Visibility</b>	<b>79</b>
SaaS Assets and SaaS Assets Summary Report	80
SaaS Security Insights	81
<b>Cloud App Control</b>	<b>82</b>
Cloud App Control Policy	83
Cloud App Control Deny Policy	84
Cloud App Control Logs	86
<b>ZDX for ServiceNow</b>	<b>87</b>
Configure ZDX for ServiceNow	87
Configure ZDX for ServiceNow	88
Configure Probes for ServiceNow Monitoring	89
Configure Probes for ServiceNow Monitoring	90
The ZDX-Enabled ServiceNow Application	92
Create an Alert for the ServiceNow Service	93
The Triggered Alert for the ServiceNow Service	99
Alert Detail for the ServiceNow Service	100
The Sent Alert Email for the ServiceNow Service	101



<b>Using the ZDX Dashboard</b>	<b>102</b>
Applications Overview	103
ServiceNow Application Performance Detail	104
User Overview	106
ServiceNow User Detail	107
<b>ZDX ServiceNow Application</b>	<b>109</b>
Install the ZDX ServiceNow Application	109
Configure ServiceNow Service Account in ZDX	110
Configure the ZDX ServiceNow Application	111
Configure Deep Tracing Role for Interactive Uses in ServiceNow	112
Configure Service User in Zscaler Digital Experience	113
Configure Application Settings	114
Configure ZDX Webhook in ZDX	115
Test ZDX Deep Tracing Integration with ServiceNow	116
<b>ZPC: ServiceNow Integration for Ticket Creation</b>	<b>117</b>
ServiceNow: Configure Service Account	117
Configure ZPC and ServiceNow Integration	119
ZPC ServiceNow ITSM Configuration	120
ZPC: Create Notification Rules	122
ZPC: Create A Cloud Notification Rule	123
ZPC: Create IaC Notification Rule	125
ZPC ServiceNow Incidents	128
<b>Contextualizing Risk Using ServiceNow and Avalor UVM</b>	<b>129</b>
Configuring the ServiceNow Tenant for OAuth 2.0	129
Create a Client ID and Client Secret	130
Retrieve the Refresh Token	132
Configure the ServiceNow UVM Data Connectors	133
Configure the ServiceNow Assets Data Source	133
Configure the Service Now Users Data Source	136

Configure the ServiceNow Generic Data Source	139
Configure the ServiceNow Outegrations	142
Review and Adjust Data Model Mapping	145
Mark a ServiceNow Asset Internet Facing	145
Map the Internet Facing Field to Your Avalor Data Model	146
Review and Adjust Risk Scoring	149
<b>Appendix A: Requesting Zscaler Support</b>	<b>151</b>

## 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)
DSPM	Data Security Posture Management
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-Shared Key
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

## About This Document

The following 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](#).

### 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](#).

### Audience

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

For additional product and company resources, see:

- [Zscaler Resources](#)
- [ServiceNow Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

### 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](mailto:partner-doc-support@zscaler.com) to offer feedback or corrections for this guide.
- **For Zscaler employees:** Contact [z-bd-sa@zscaler.com](mailto: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, 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 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
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZDX Help Portal</a>	Help articles on ZDX.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

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

Name and Link	Description
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZDX Help Portal</a>	Help articles on ZDX.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	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
<a href="#">About ServiceNow</a>	ServiceNow company description.
<a href="#">ServiceNow Developer Program</a>	Website for creating a ServiceNow developer account.
<a href="#">ServiceNow Product Documentation</a>	Online documentation for the ServiceNow platform.
<a href="#">ServiceNow Community</a>	ServiceNow online community portal.
<a href="#">ServiceNow Support</a>	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.

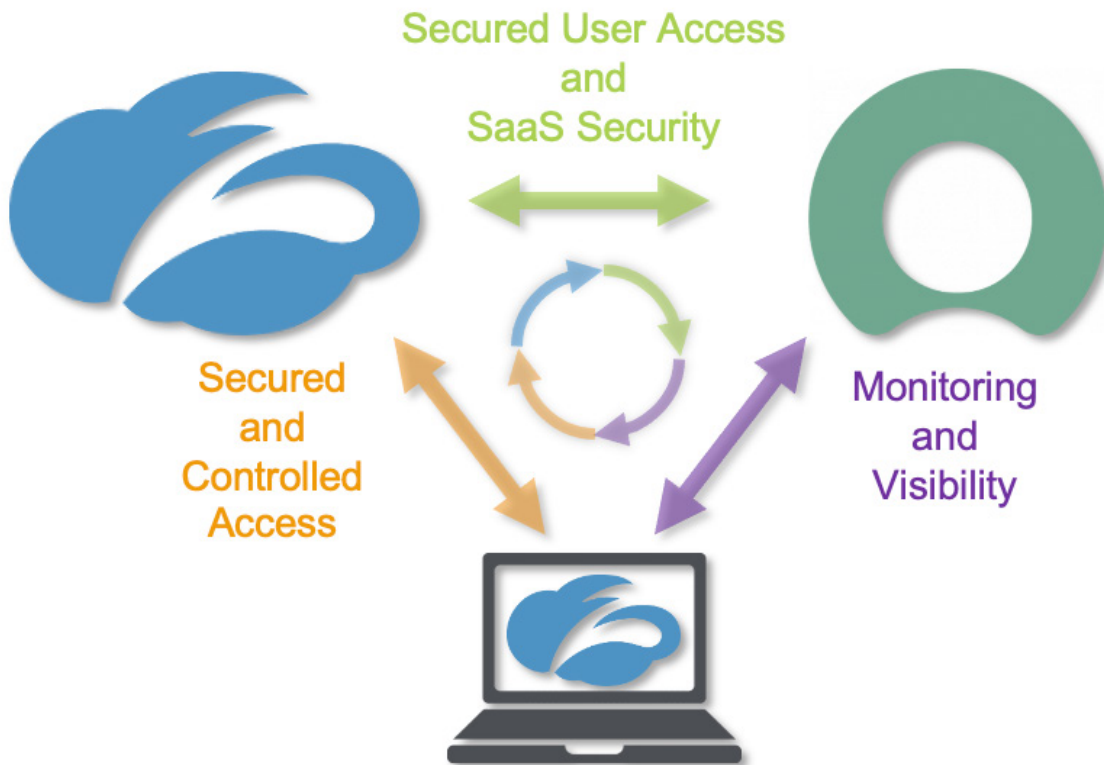


Figure 1. Zscaler solutions for ServiceNow

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, Data Security Posture Management (DSPM), and SaaS Security 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
- Isolation
- SaaS Security Data Loss Protection and Malware Detection
- Cloud Application Access Control
- ZDX for ServiceNow
- DSPM 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.

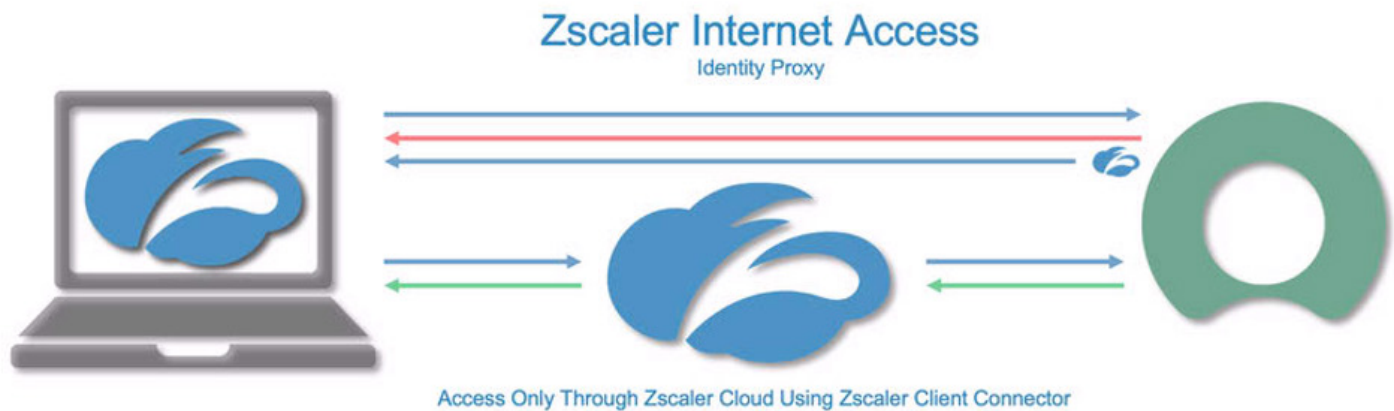


Figure 2. ZIA identity proxy

When users try to access ServiceNow with their corporate accounts without going through the Zscaler service, they receive a pop-up window 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 Isolation, you can start with the services you need today and activate others as your needs grow.



## ZIA 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 Isolation in use with ServiceNow

Zscaler 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.

You can combine Isolation 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 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.

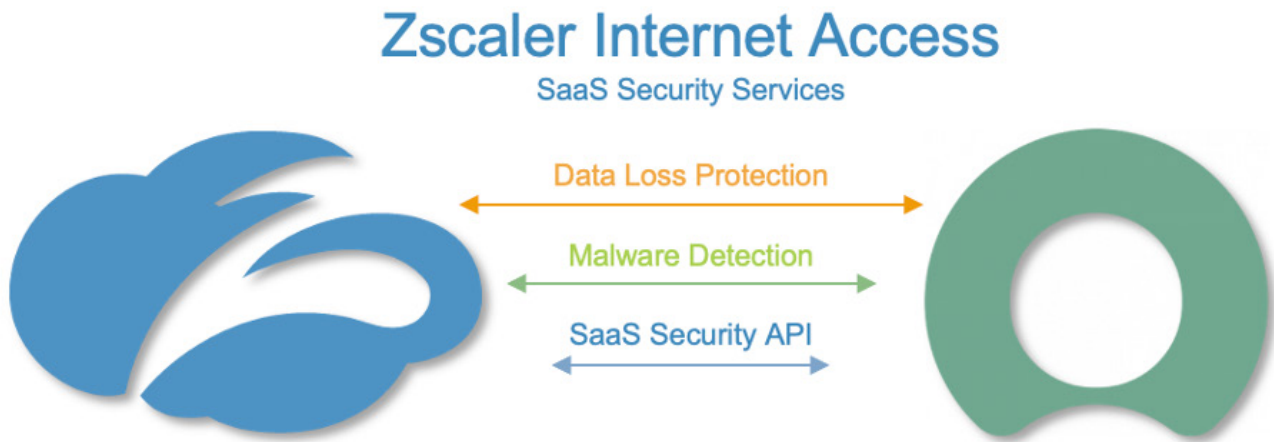


Figure 4. ZIA SaaS Security in use with ServiceNow

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 DSPM 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 and 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, ZIA Cloud Application Control delivers full visibility into application usage, and granular policies ensure the proper use of both sanctioned and unsanctioned applications.

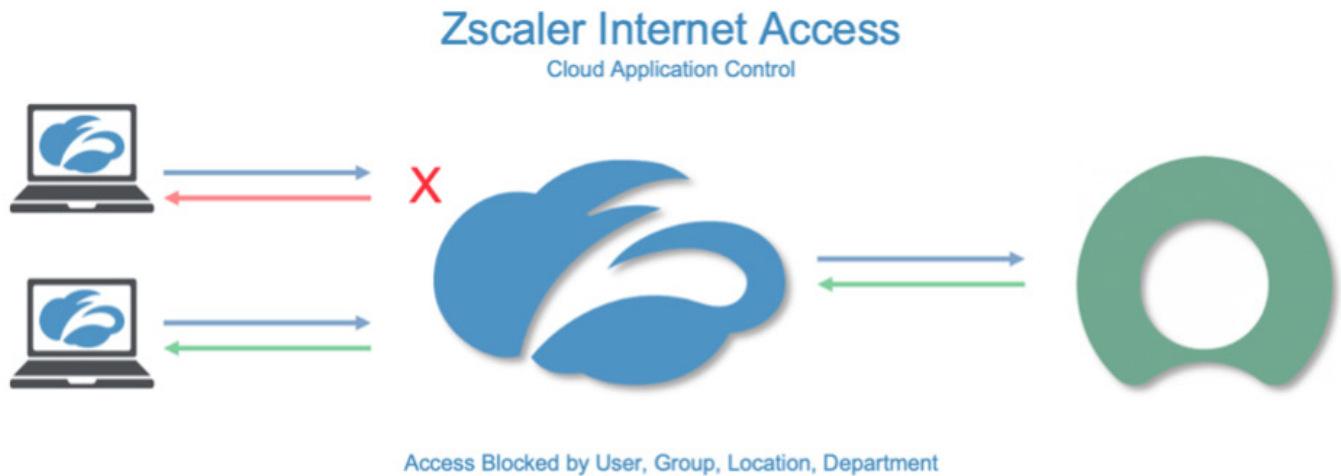


Figure 5. Cloud App Control

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.

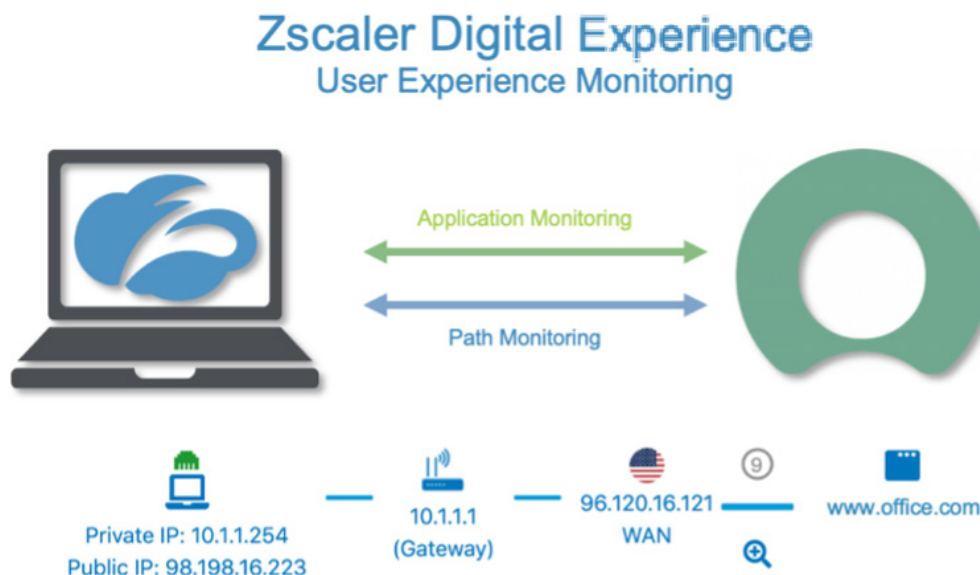


Figure 6. ZDX in use with ServiceNow

### What Makes 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 in to the Zscaler tenant with administrator credentials.

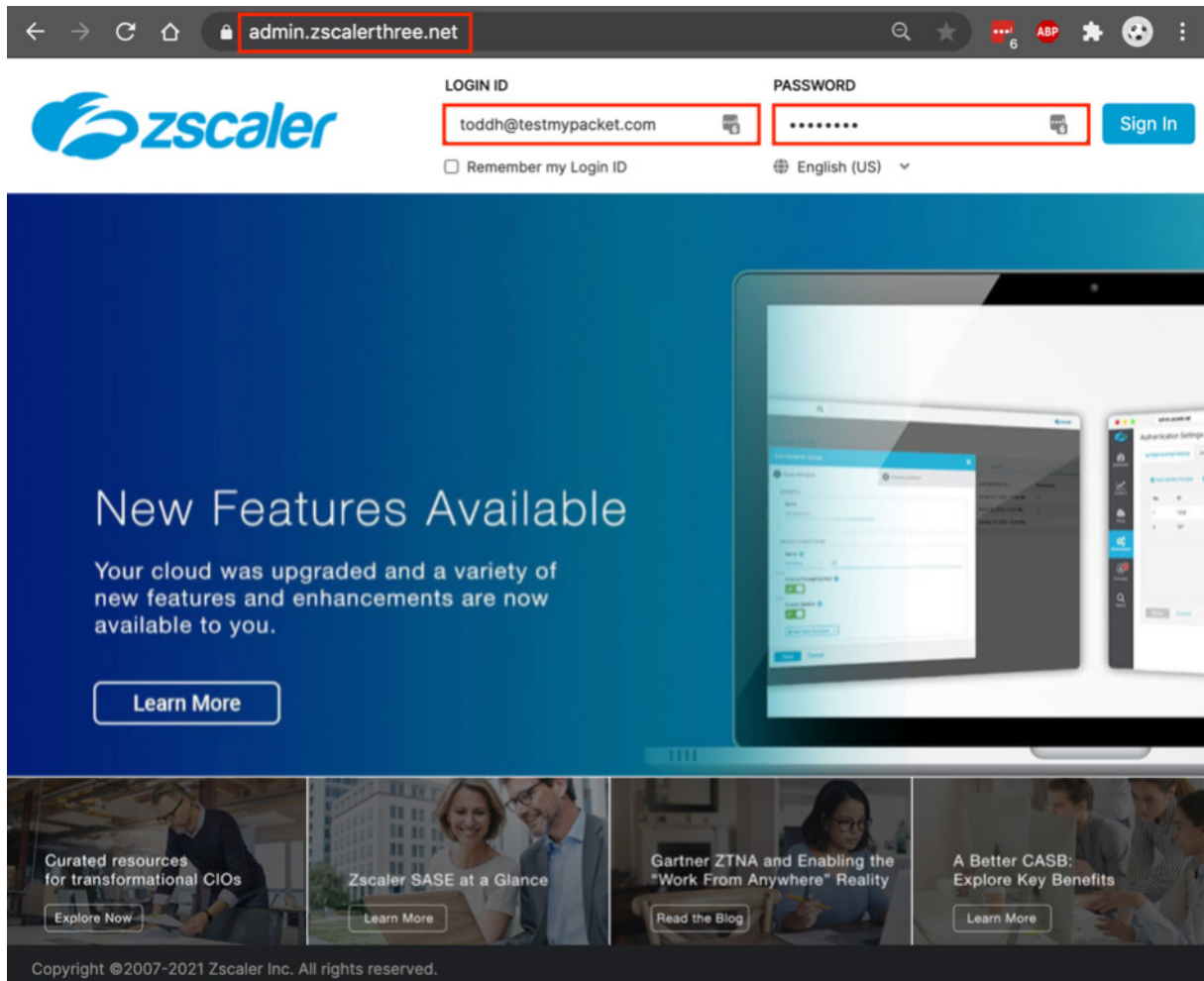


Figure 8. Configure the SaaS identity proxy

## 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, enter a **Name** for the cloud application.
4. **Enable** the **Status**.
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) from the drop-down menu for **Response Signing SAML Certificate**.
9. Select **Pass-through Zscaler Identity** for **Identity Transformation**.
10. Click **Save**.

The screenshot displays the 'Edit Cloud Application' configuration window in the ZIA Admin Portal. The window is titled 'Edit Cloud Application' and contains several sections:

- CLOUD APPLICATION**: Includes fields for Name (ServiceNow), Status (Enabled), Cloud Application (ServiceNow), ACS URL (https://dev73413.service-now.com/navpage...), and Entity ID (https://dev73413.service-now.com).
- IDENTITY PROXY SETTINGS**: Includes Response Signing SAML Certificate (saml\_2022) and SAML Certificate Expiration Date (November 16, 2022).
- IDENTITY TRANSFORMATION RULES**: Includes Identity Transformation (Pass-through Zscaler Identity) and buttons for Change Domain to and Remove Domain Name.
- GROUP**: Includes Pass-on Group Details (Enabled) and Group Identifier Name (Enter Text).

The 'Save' button is located at the bottom left of the configuration window.

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**.

**Identity Proxy Settings**

+ Add Cloud Application

Search...

No.	Cloud Applications	Status	Setting	Certificate	
1	Name ServiceNow Cloud Application ServiceNow ACS URL https://dev73413.service-now.com/...	Enabled	SAML Version 2.0 Identity Proxy URL https://idp.zscalerbeta.net/samlso/HxnBcP11TnTIZIL7vi... Issuer Entity Id HxnBcP11TnTIZIL7viT7Vkq+Qbm9jK0fA87tHqItx26skdqf... Identity Request Binding HTTP-POST User Identifier NameID Response Signing SAML Certificate saml_2022	Download	

Administration

Activation

Search

Help

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 in to the ServiceNow tenant with administrator credentials.

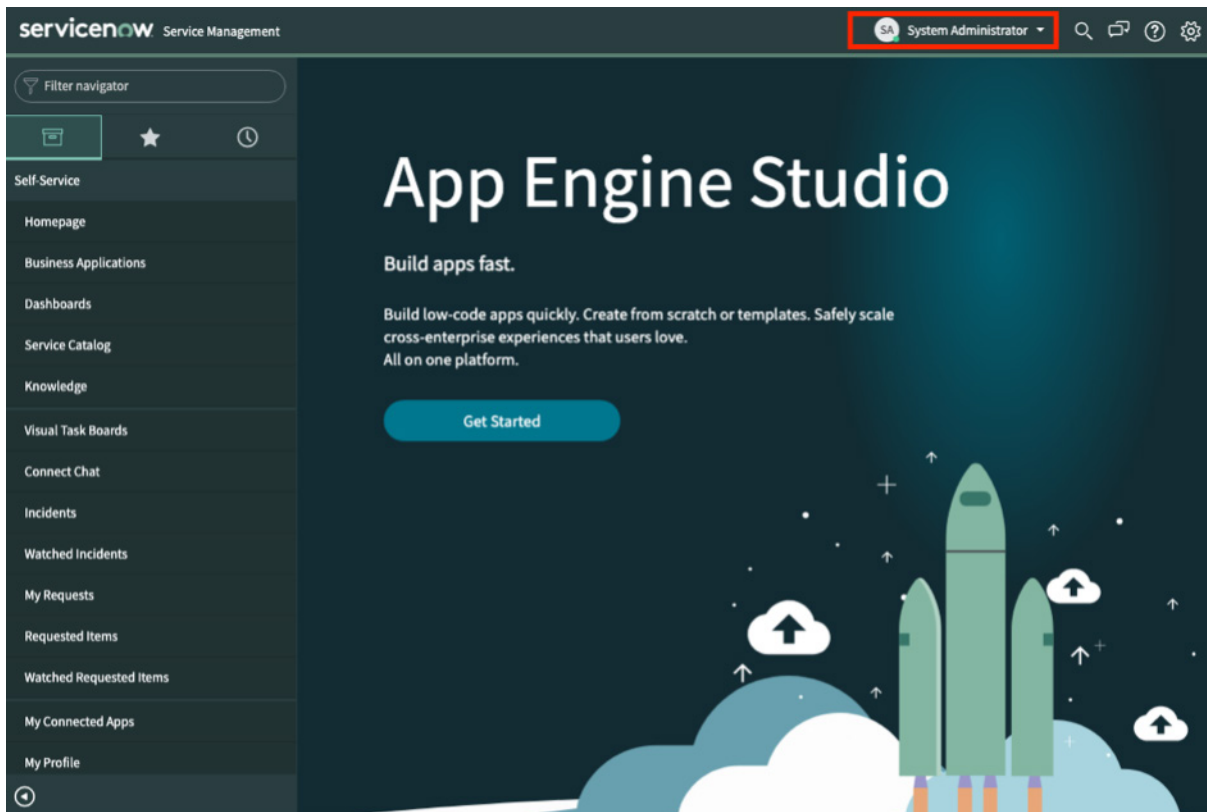


Figure 11. Configure ServiceNow to use the identity proxy

## Install the ServiceNow Plugins

In the ServiceNow plugins page:

1. In the **Filter Navigator** search bar, enter `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**.

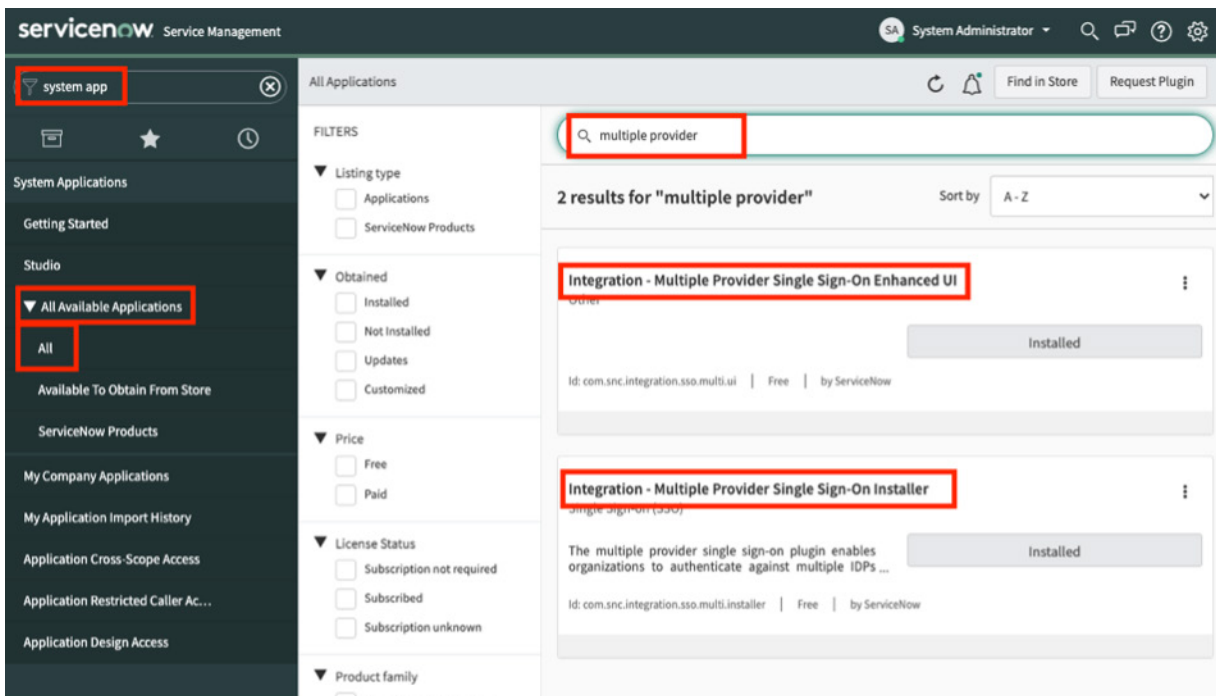


Figure 12. Configure the ServiceNow plugins

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. In the **Filter Navigation** search bar, enter `multi`.
2. Select **Administration** under **Multi-Provider SSO**.
3. Select **Properties** to display the **Customization Properties for Multiple Provider SSO** window.
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**.

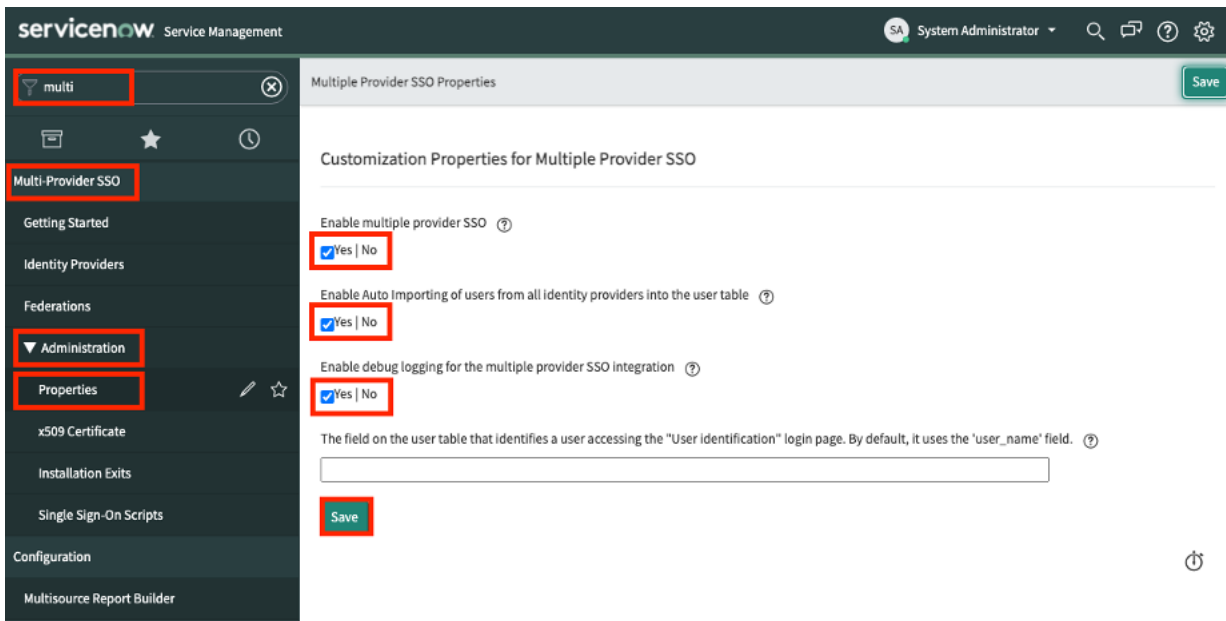


Figure 13. Enable multiple provider SSO

## 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**.

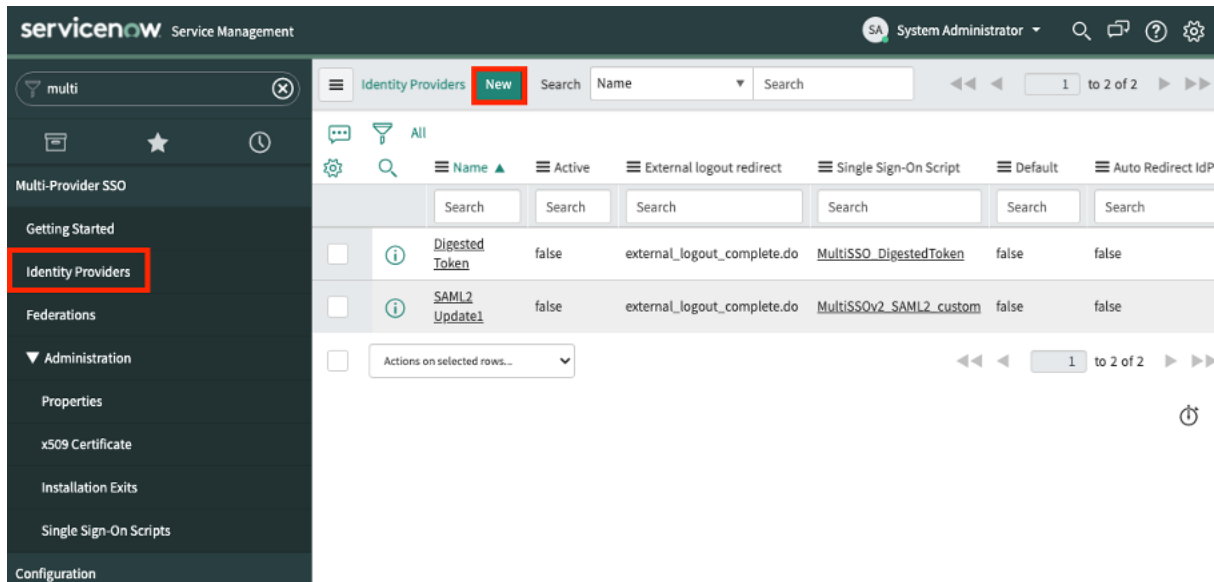


Figure 14. Create the Zscaler Identity Provider

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

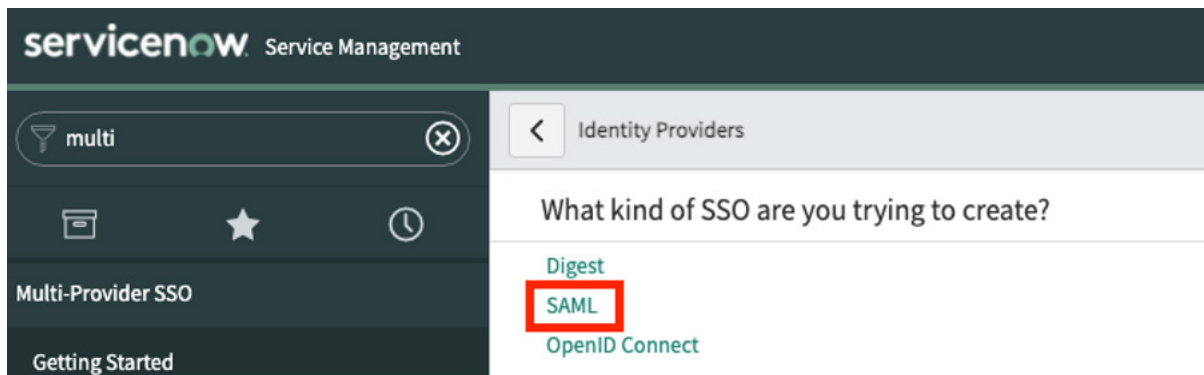


Figure 15. Select SAML SSO

## 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, enter a **Name** for the template.
2. In the **Identity Provider URL** field, paste in the **Issuer Entity Id** from the Zscaler config.
3. In the **Identity Provider's AuthnRequest** field, paste in the Identity Proxy URL.
4. For the **ServiceNow Homepage**, enter your ServiceNow Instance/namespace.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**.

The screenshot shows the 'Identity Provider New Record' form in ServiceNow. The 'Name' field is 'Zscaler'. The 'Identity Provider URL' and 'Identity Provider's AuthnRequest' fields contain long alphanumeric strings. The 'ServiceNow Homepage' is 'https://zscalerbdtteam.service-now.com/namespace.do'. The 'Entity ID / Issuer' and 'Audience URI' are 'https://zscalerbdtteam.service-now.com'. The 'NameID Policy' is 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'. The 'Advanced' tab is selected, showing 'User Field' as 'email', 'Create AuthnContextClass' checked, 'AuthnContextClassRef Method' as 'urn:oasis:names:tc:SAML:2.0:ac:classes!', 'Force AuthnRequest' checked, and 'Single Sign-On Script' as 'MultiSSOv2\_SAML2\_custom'.

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. The option to add the Zscaler certificate becomes available at the bottom of the configuration window.

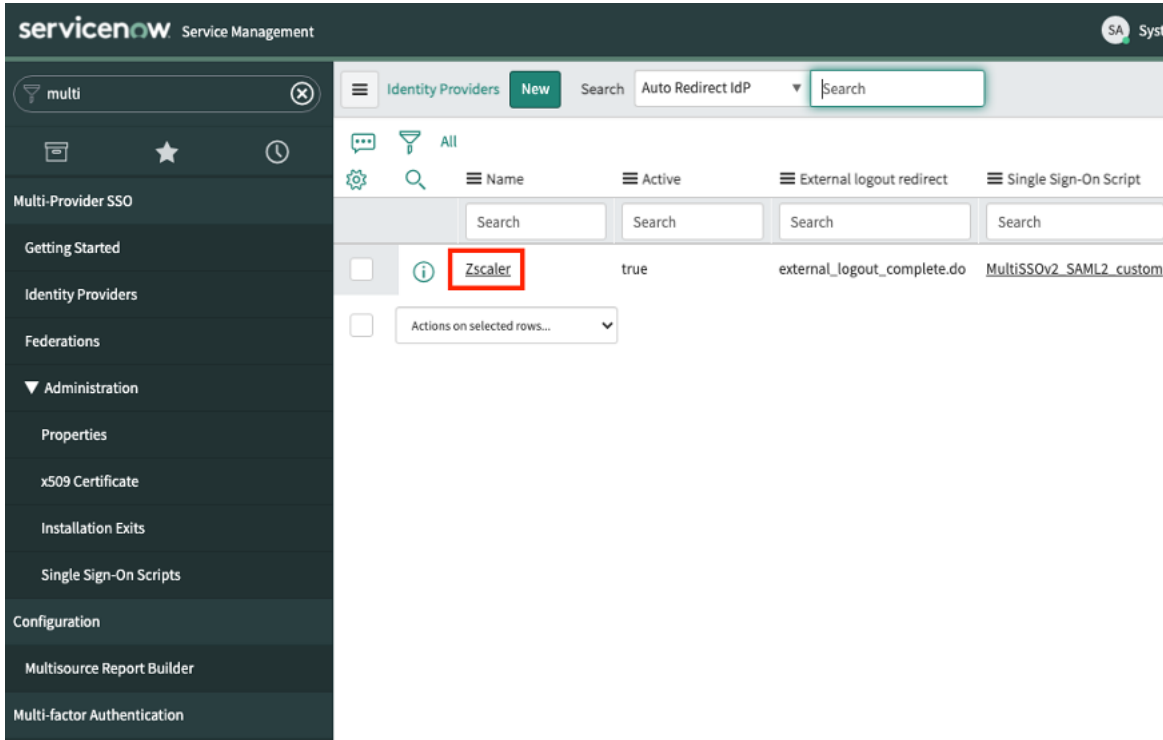


Figure 17. Select the Zscaler identity provider

2. Select **New** to configure and add the certificate.

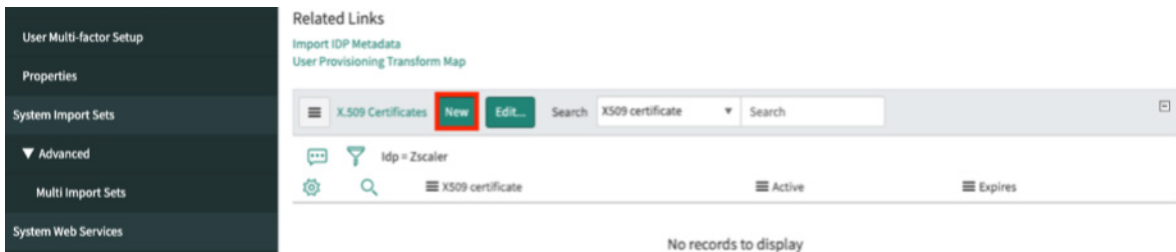


Figure 18. Add the signing certificate

## 3. Manually add the certificate:

- Name** the certificate.
- Open the certificate file from Zscaler and copy the entire contents.
- Paste the contents into the **PEM Certificate** field.
- Click **Submit**.

The screenshot shows the 'X.509 Certificate' configuration page in ServiceNow. The 'Name' field is set to 'Zscaler'. The 'Format' is 'PEM' and 'Type' is 'Trust Store Cert'. The 'Warn in days to expire' is set to 20. The 'PEM Certificate' field contains a long, single-line certificate string. The 'Submit' button is highlighted with a red box.

Figure 19. Configure the identity provider certificate



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

#### 4. Configure additional identity provider certificate settings:

- Select **Default**.
- Select **Set** as **Auto Redirect IdP**.
- Select **Test**.

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

The screenshot shows the ServiceNow Identity Provider configuration page for Zscaler. The page is titled "Identity Provider Zscaler" and includes a sidebar with navigation options like "Multi-Provider SSO", "Getting Started", "Identity Providers", "Federations", "Administration", "Properties", "x509 Certificate", "Installation Exits", "Single Sign-On Scripts", "Configuration", "Multisource Report Builder", "Multi-factor Authentication", "Multi-factor Criteria", "Multi-factor Browser Fingerprints", "User Multi-factor Setup", "Properties", "System Import Sets", "Advanced", "Multi Import Sets", "System Web Services", "REST", and "Insert Multiple". The main configuration area includes fields for Name (Zscaler), Identity Provider URL, Identity Provider's AuthnRequest, Identity Provider's SingleLogoutRequest, ServiceNow Homepage, Entity ID / Issuer, Audience URI, NameID Policy, External logout redirect, and Failed Requirement Redirect. The "Default" dropdown is highlighted with a red box. Below these fields are tabs for "Encryption And Signing", "User Provisioning", and "Advanced". The "User Provisioning" tab is selected, showing fields for Signing/Encryption Key, Password, and Encrypted Assertion. The "Test Connection" button is highlighted with a red box. Below the configuration fields, there are tabs for "Encryption And Signing", "User Provisioning", and "Advanced". The "User Provisioning" tab is selected, showing fields for Signing/Encryption Key, Password, and Encrypted Assertion. The "Test Connection" button is highlighted with a red box. Below the configuration fields, there are tabs for "Encryption And Signing", "User Provisioning", and "Advanced". The "User Provisioning" tab is selected, showing fields for Signing/Encryption Key, Password, and Encrypted Assertion. The "Test Connection" button is highlighted with a red box.

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 window is displayed when testing, and any time a change is made to the identity proxy, you must 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**.

ServiceNow

dev73413.service-now.com/saml\_test\_conn\_completed.do?sysparm\_nostack=true&sysparm\_test\_sso\_id=0272378107ec3010da0...

### SSO Login Test Results

- ✓ SAML Login response received
- ✓ SAML Assertion retrieved
- ✓ Signature Validated
- ✓ Certificate Validated
- ✓ AudienceRestriction/Condition Validated
- ✓ Certificate Issuer Validated
- ✓ Subject Confirmation Validated

### SSO Logout Test Results

✗ Cannot logout of IDP's session  
Test Connection user is same as the user logged into the system through Multi SSO.

### SSO Test Connection Summary

✓ SSO Login tests succeeded. SSO Logout tests failed. IDP Configuration can be activated by clicking 'Activate' button. Users will be able to login and logout of the instance, but will not be logged out of the IDP. Please refer to the logs for test details.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

```
06/03/21 13:30:10 (325) sysparm_form_fields: sysparm_ck=92f4d78d076c3010da03ffa08c1ed0e50935aecb316b15e5c936a2cc588762397f482c1e&sys_base_uri=https%3A%2F%2Fdev73413.service-now.com%2F&sys_target=saml2_update1_properties&sys_uniqueName=sys_id&sys_uniqueValue=0272378107ec3010da03ffa08c1ed04c&sys_displayValue=Zscaler&sys_titleValue=Zscaler&onLoad_sys_updated_on=2021-06-03+18%3A25%3A26&sys_row=0&sys_modCount=5&sys_action=none&sysparm_collection=&sysparm_collectionID=&sysparm_collection_key=&sysparm_collection_related_field=&sysparm_collection_relationship=&sysparm_redirect_url=&sysparm_goto_url=&isFormPage=true&sysparm_referring_url=&sysparm_view=&sysparm_changeset=&sysparm_template_editable=&sysparm_record_row=1&sysparm_record_list=ORD ERBYDESCis_primary&sysparm_record_rows=3&sysparm_record_target=&sysparm_modify_check=true&sysparm_action_template=&sysparm link collection=&sysparm pop onLoad=&sysparm nameofstack=&sysparm transaction scope=&sysp
```

Close **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 in to ServiceNow without going through Zscaler. When your user traffic is going through Zscaler, the users can access ServiceNow as usual.

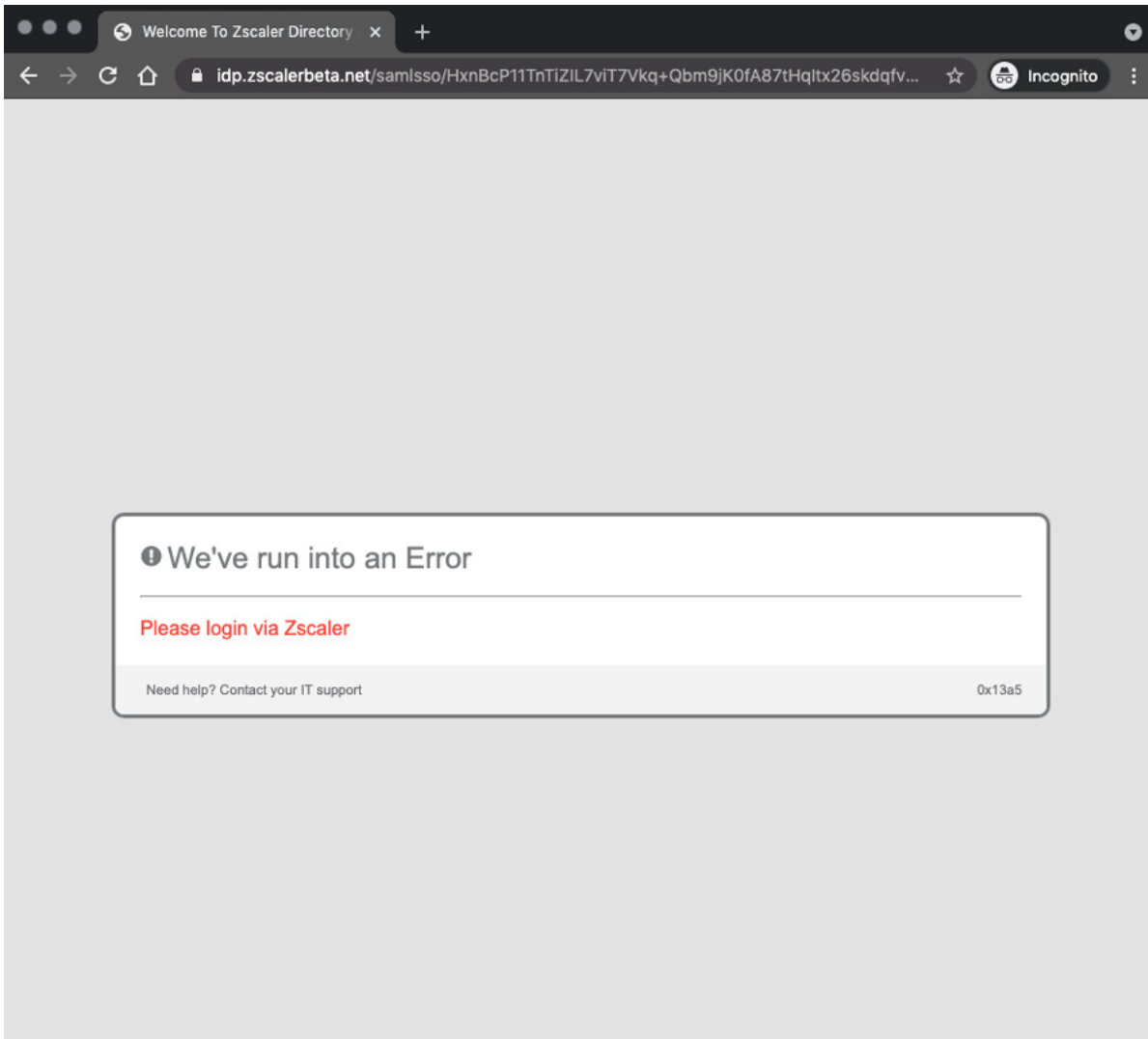


Figure 22. The active authentication proxy

## Configure Redirect on the Identity Provider

Use this procedure when the auto redirect IdP doesn't enable from the Configuration window. 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**.
3. Select **Copy sys\_id**.

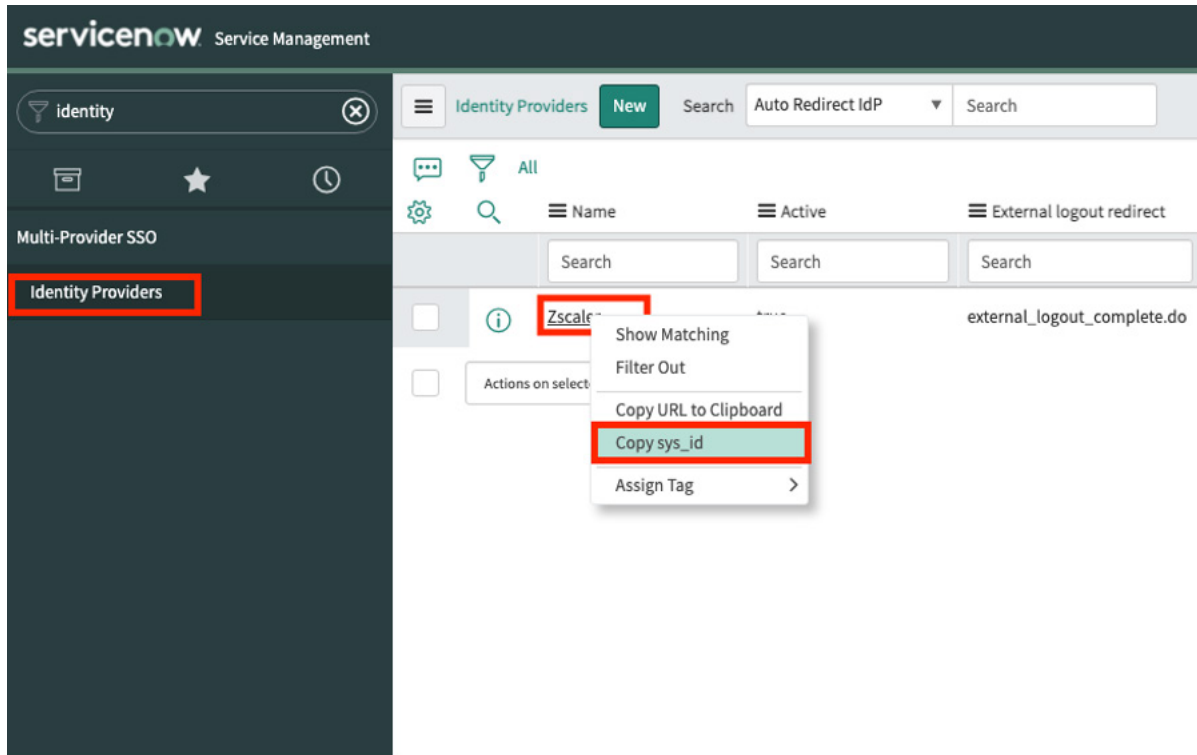


Figure 23. Configure the identity provider

4. Configure the redirect system properties:

- In the **Filter Navigator** search bar, enter `sys_properties.LIST`.
- Press Enter.

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

The screenshot shows the ServiceNow interface with the 'System Properties' list. The Filter Navigator on the left has 'sys\_properties.LIST' entered in the search bar. The main panel shows a table of system properties for 'App Engine Studio'.

Name	Value	Type	Application	Description
<a href="#">sn_app_eng_studio.aes_admin_contact</a>		string	App Engine Studio	Email address of the App Engine Studio a...
<a href="#">sn_app_eng_studio.delete_user_sync_queue...</a>	30	integer	App Engine Studio	We will remove records from the sn_app_e...
<a href="#">sn_app_eng_studio.illustration_supported...</a>	image/svg+xml	string	App Engine Studio	A comma separated list (no spaces between...
<a href="#">sn_app_eng_studio.mobile_studio_access</a>	true	true   false	App Engine Studio	Allows App Engine Studio users to launch...
<a href="#">sn_app_eng_studio.user_sync_email_notifi...</a>	true	true   false	App Engine Studio	Enable e-mail notification sent out to u...
<a href="#">sn_app_eng_studio.user_sync_enabled</a>	true	true   false	App Engine Studio	When false, turns off the job that proce...
<a href="#">sn_app_eng_studio.user_sync_queue_enabled</a>	true	true   false	App Engine Studio	When enabled is true, all AES users chan...

Figure 24. System properties



## Configure the Property

In the System Property window, 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**.

The screenshot shows the 'System Property' configuration window for the property `glide.authentication.sso.redirect.idp`. The window has a header bar with a back arrow, a menu icon, the title 'System Property glide.authentication.sso.redirect.idp', and action buttons: 'Update', 'Delete', and up/down arrows. Below the header is a warning message: 'You are editing a record in the Test application (cancel)'. The main form contains the following fields and controls:

- Suffix**: `x_648162_test`
- Application**: `Test` (with an information icon)
- Name**: `glide.authentication.sso.redirect.idp`
- Description**: (empty text area)
- Choices**: (empty text area)
- Type**: `string` (dropdown menu)
- Value**: `0272378107ec3010da03ffa08c1ed04c` (highlighted with a red box)
- Ignore cache**: ☐
- Private**: ☐
- Read roles**:
- Write roles**:
- Update** and **Delete** buttons (the **Update** button is highlighted with a red box)
- Related Links**: [Run Point Scan](#)

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

## Configure 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.

ZIA 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 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.

You can combine Isolation 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. For identified potentially risky users, go directly to Isolation for even greater security measures.

## Configure the Isolation Profile

To begin the Isolation configuration:

1. Log in to your ZIA Admin Portal with administrator credentials.

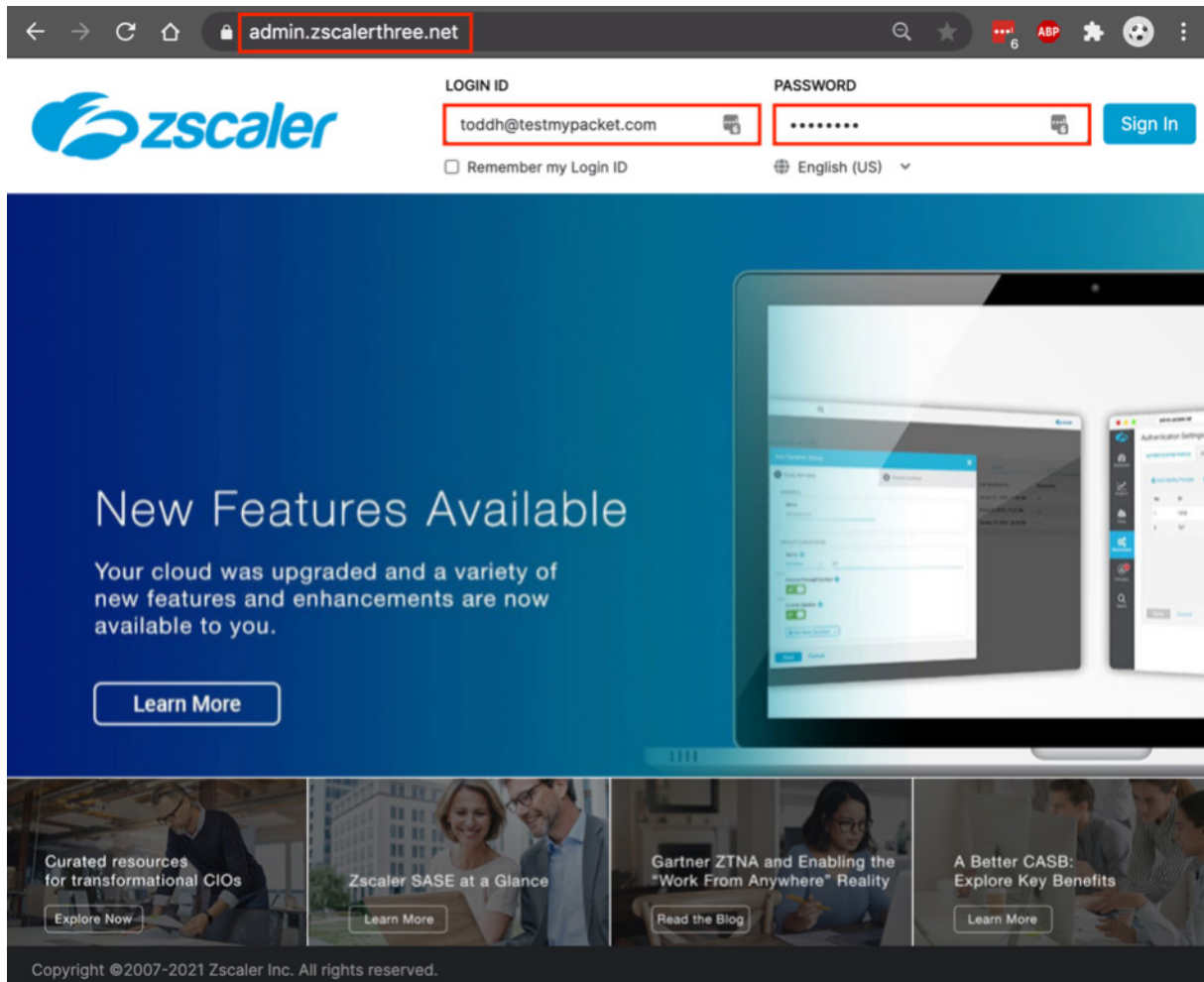


Figure 28. Configure Isolation



Configure an Isolation profile or multiple profiles to enable the features that are applied specifically for ServiceNow. Also configure the individual user implementing 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**:

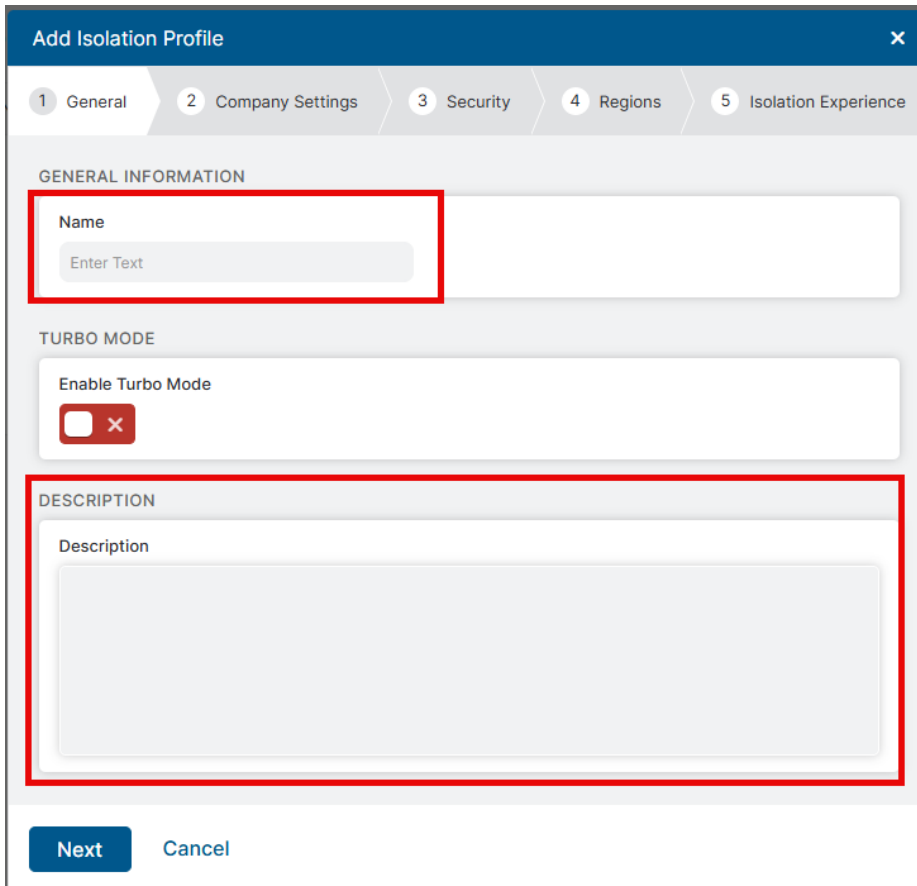
1. From the left-side navigation, select **Administration > Browser Isolation**.
2. Select **Add Profile**.

No.	Name	Regions	Security Controls
1	Default Isolation Profile	Frankfurt, London, Mumbai, Portl...	<div>ALLOW PRINTING Disabled</div> <div>RESTRICT TEXT INPUT Disabled</div> <div>VIEWING OFFICE FILES View office files in isolation</div> <div>LOCAL BROWSER RENDERING Disabled</div>

Figure 29. Configure Isolation profile

This starts the **Isolation** wizard and steps you through enabling **General Information**, **Company Settings**, **Security**, **Regions**, and the **Isolation Experience**.

3. 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. Enable or disable **Turbo Mode**.
  - c. Enter a detailed **Description**.
  - d. Click **Next**.



The screenshot shows the 'Add Isolation Profile' dialog box with a dark blue header and a close button (X) in the top right corner. Below the header is a horizontal navigation bar with five tabs: '1 General', '2 Company Settings', '3 Security', '4 Regions', and '5 Isolation Experience'. The 'General' tab is selected and highlighted. The main content area is divided into three sections: 'GENERAL INFORMATION', 'TURBO MODE', and 'DESCRIPTION'. The 'GENERAL INFORMATION' section contains a 'Name' label and a text input field with a placeholder 'Enter Text'. The 'TURBO MODE' section contains an 'Enable Turbo Mode' label and a toggle switch that is currently turned off. The 'DESCRIPTION' section contains a 'Description' label and a large text area. The 'Name' field and the 'DESCRIPTION' section are highlighted with red rectangular boxes. At the bottom of the dialog, there are two buttons: 'Next' (dark blue) and 'Cancel' (light blue).

Figure 30. Isolation general information

4. For the **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. Choose to use either the recommended PAC file URL or your own manually configured PAC file URL:
    - If you select **Use recommended PAC file URL**, the **Automatic proxy configuration URL** field is populated by default with the recommended PAC file from your Hosted PAC Files list in ZIA. The isolation browser configures the PAC file within the endpoint experience containers, and any traffic to the internet from the isolated browser is also forwarded through the ZIA cloud.
    - Enable or disable **Override PAC file and return traffic to ZIA Public Service Edge**. The ZIA Public Service Edges use auto-geoproximity, meaning that the traffic is returned to the service edge closest to the location of the user, not the location of the isolation browser. To see the full list of ZIA Public Service Edges, see the Zscaler Configuration Portal.
  - b. Enable or disable **Debug Mode**. If you enable it, you must set a password for the ZIP file that is created at the end of a debug troubleshoot. Make sure to share the password with the user associated with the isolation profile. To learn more, see [Using Debug Mode for Isolation](#).
  - c. Select at least one file from the **File (.pem)** drop-down menu in the **Root Certificates** section. The **Zscaler Root Certificate** that ZIA uses for SSL inspection appears by default in the drop-down menu. If your organization uses custom root certificates for SSL inspection, you can add them before creating isolation profiles. You can add up to 10 root certificates for your organization. To learn more, see [About Root Certificates for Isolation in ZIA](#) (government agencies, see [About Root Certificates for Isolation in ZIA](#)).
5. Click **Next**.

**Add Isolation Profile**

1 General 2 **Company Settings** 3 Security 4 Regions 5 Isolation Experience

**PROXY AUTO-CONFIGURATION (PAC)**

**PAC File URL**

☒ Use recommended PAC file URL ☐ I want to use my own PAC file URL

**Automatic proxy configuration URL**

https://pac.zscalerbeta.net/zscalerbeta.net/proxy.pac

**Override PAC file and return traffic to ZIA Public Service Edge**

☐

**DEBUGGING**

**Enable Debug Mode**

☐

**ROOT CERTIFICATES**

**File (.pem)**

Zscaler Root Certificate

Previous Next Cancel

Figure 31. Isolation company settings

- The Security 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.
- Click **Next**.

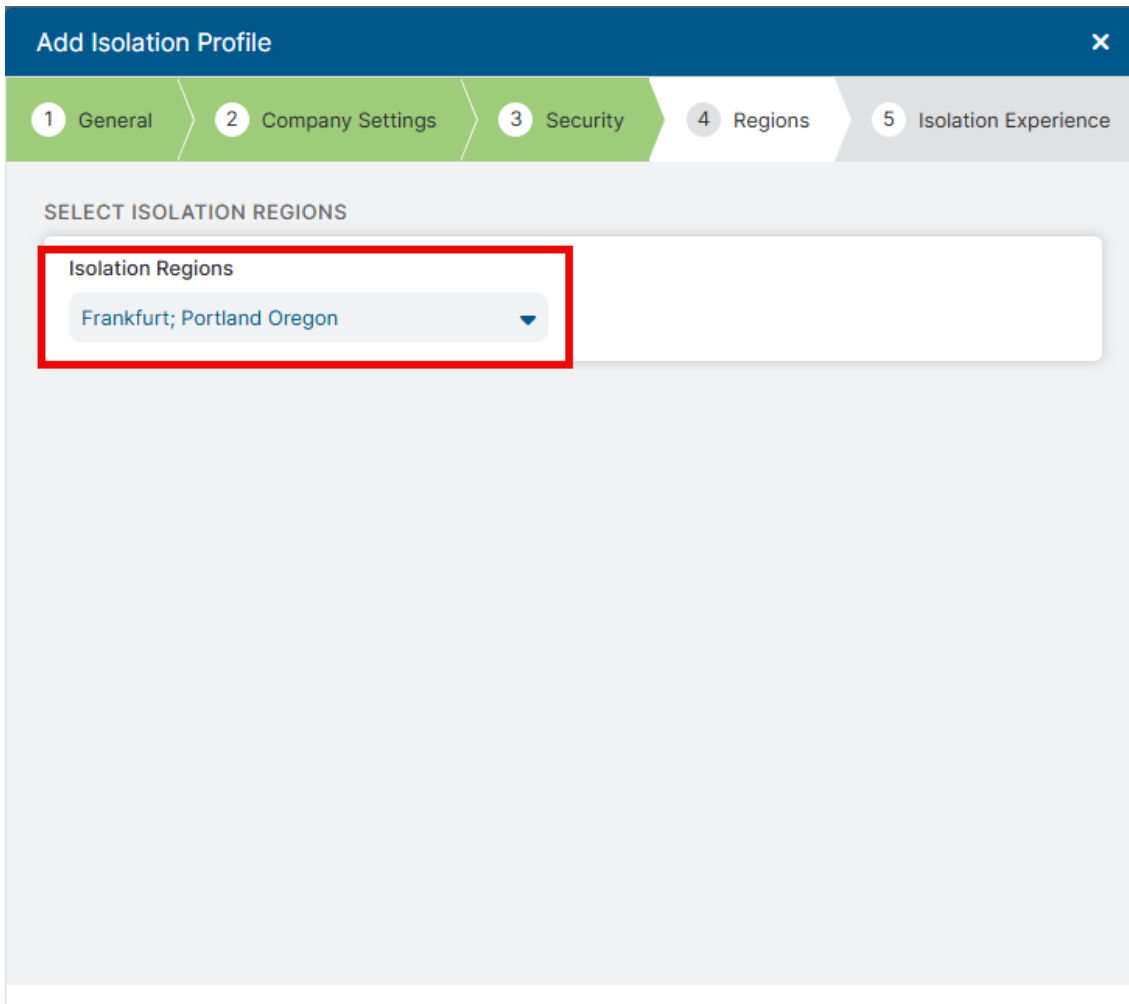
The screenshot shows the 'Add Isolation Profile' dialog with the 'Security' tab selected. The dialog has five tabs: General, Company Settings, Security, Regions, and Isolation Experience. The Security tab contains four sections, each with a toggle switch and a red 'X' icon:

- ALLOW COPY & PASTE FROM**
  - Local computer to isolation: ☐
  - Isolation to local computer: ☐
- ALLOW FILE TRANSFERS FROM**
  - Local computer to isolation: ☐
  - Isolation to local computer: ☐
- ALLOW PRINTING**
  - Allow printing from isolation: ☐
- RESTRICT TEXT INPUT**
  - Read-Only Isolation: ☐

At the bottom, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Figure 32. Isolation security

9. Select two **Regions** for redundancy. Select the two closet regions to your organization:
  - a. Select two **Regions** for redundancy.
  - b. Click **Done**.
  - c. Select **Next**.



The screenshot shows a multi-step configuration window titled "Add Isolation Profile". The steps are: 1 General, 2 Company Settings, 3 Security, 4 Regions, and 5 Isolation Experience. Step 4, "Regions", is the active step. Below the step indicators, the text "SELECT ISOLATION REGIONS" is displayed. A dropdown menu labeled "Isolation Regions" is shown, with a red rectangular box highlighting it. The dropdown menu is open, displaying the selected region "Frankfurt; Portland Oregon" with a downward arrow icon to its right.

Figure 33. Isolation regions

10. Use the defaults from the **Isolation Experience** tab, then click **Save**.

Add Isolation Profile

1 General


2 Company Settings

3 Security

4 Regions

5 Isolation Experience

ISOLATION BANNER PREVIEW



**Heads up, you've been redirected to Browser Isolation!**  
The website you were trying to access is now rendered in a fully isolated environment to protect you from malicious content.

Isolation Banner

Default

Persist Browser Isolation URL bar

☐

Isolation Experience

☒ Native browser experience

☐ Browser-in-browser experience

WATERMARKING

Enable Watermarking

☐

COOKIE PERSISTENCE

Cookie Persistence

☐

LANGUAGE TRANSLATION

Enable Language Translation

☐

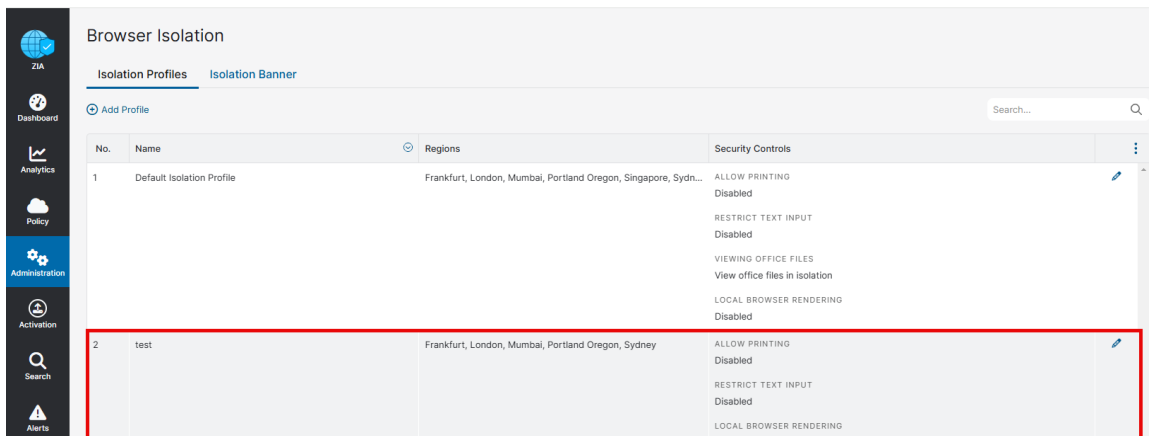
Previous

Save

Cancel

Figure 34. Isolation Experience

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



No.	Name	Regions	Security Controls
1	Default Isolation Profile	Frankfurt, London, Mumbai, Portland Oregon, Singapore, Sydne...	ALLOW PRINTING Disabled RESTRICT TEXT INPUT Disabled VIEWING OFFICE FILES View office files in isolation LOCAL BROWSER RENDERING Disabled
2	test	Frankfurt, London, Mumbai, Portland Oregon, Sydney	ALLOW PRINTING Disabled RESTRICT TEXT INPUT Disabled LOCAL BROWSER RENDERING

Figure 35. The completed isolation profile

## Configure the 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 in to the Zscaler tenant with administrator credentials.

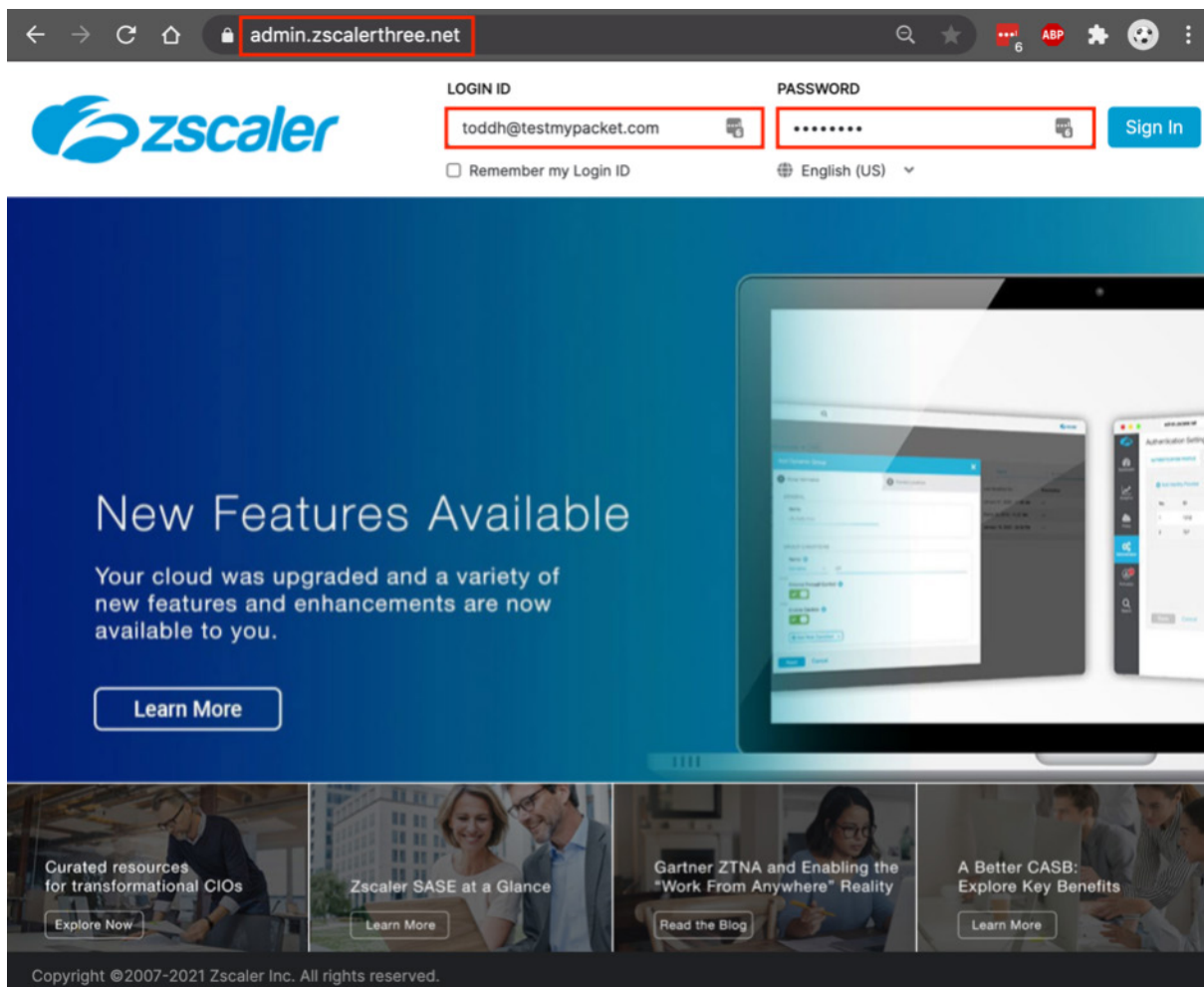


Figure 36. Configure Isolation policies



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

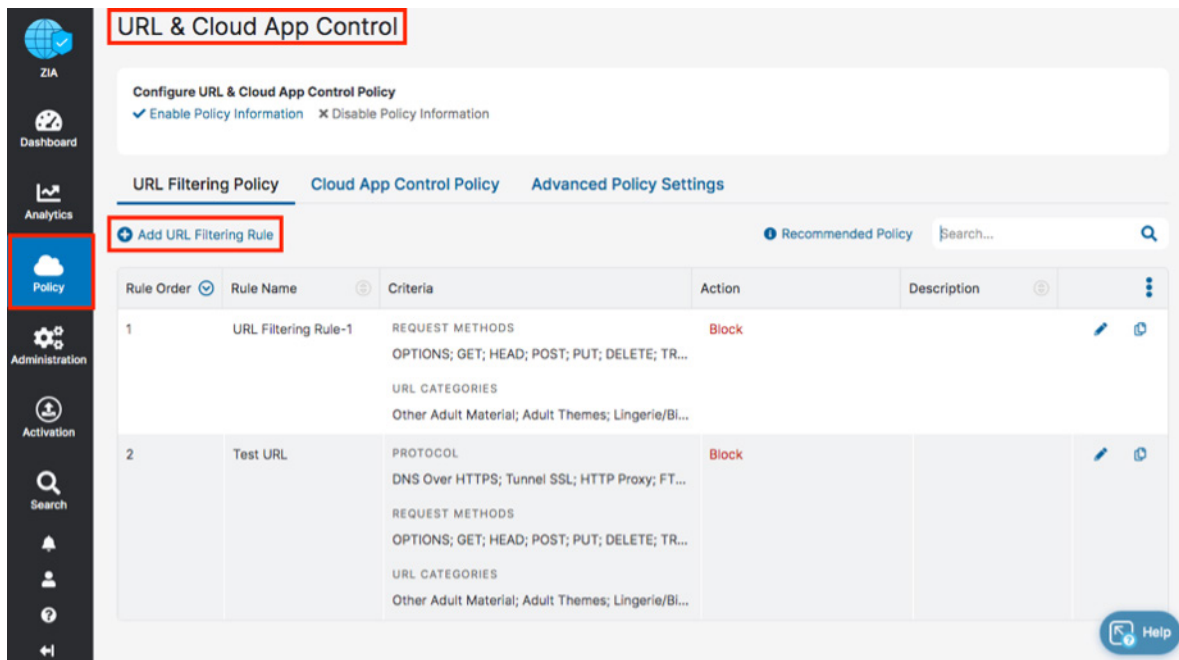


Figure 37. Configure Isolation policies

4. In the **Add URL Filtering Rule** dialog:
  - a. Select the **Rule Order**.
  - b. Enter a **Name** for the rule in the **Rule Name** field.
  - c. Select **Enabled** from the **Rule Status** drop-down menu.
  - 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** window (new dialog).
  - f. Select **Done**.
  - g. Select **Save**.

**Add URL Filtering Rule** [X]

**URL FILTERING RULE**

**Rule Order**  
1

**Rule Name**  
ServiceNow-Complete-Isolation

**Rule Status**  
Enabled

**CRITERIA**

**URL Categories**  
---

**AND**

**Users**  
---

**Departments**  
---

**OR**

Search...

- ☐ Adult Material
- ☐ Adult Sex Education
- ☐ Adult Themes
- ☐ K-12 Sex Education
- ☐ Lingerie/Bikini
- ☐ Nudity

**Unselected Items** | **Selected Items ( 0 )**

**Done** **Cancel** **Clear Selection**

Figure 38. Configure Isolation policy

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

**Add URL Category**

URL CATEGORY

Name: **ServiceNow**

URL Super Category: **User-Defined**

Administrator Operational Scope

Scope Type: **Any**

Custom URLs

Add Items

Search...

**.servicenow.com**

**.service-now.com**

1-2 of 2 < 1 / 1 > Remove

URLs retaining parent category

**Save** Cancel

Figure 39. Configure Isolation

6. Scroll down to fill in the remaining fields:
  - a. For **Request Methods**, select **Connect, Get, Head, and Trace**.
  - b. For **Time**, select **Always**.
  - c. For **Protocols**, select **HTTP** and **HTTPS**.
  - d. For **User Agent**, select your organization's specific browsers for use with Isolation.
  - e. Click **Save**.

**Add URL Filtering Rule**

**CRITERIA**

URL Categories  
ServiceNow

AND

Users  
---

Groups  
---

OR

Departments  
---

AND

Locations  
---

Location Groups  
---

OR

AND

Request Methods  
CONNECT; GET; HEAD; TRACE

Time  
Always

AND

Protocols  
HTTP; HTTPS

User Agent  
Chrome; Microsoft Edge; Microsoft In...

**RULE EXPIRATION**

Enable Rule Expiration  
☐

**ACTION**

Web Traffic  
Allow Caution Block **Isolate**

Isolation Profile  
ServiceNow - Complete Isolation

**Save** **Cancel**

Figure 40. Configure Isolation

The completed isolation profile is displayed.

ZIA

Dashboard

Analytics

Policy

Administration

Activation

Search

## URL & Cloud App Control

Configure URL & Cloud App Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

URL Filtering Policy

Cloud App Control Policy

Advanced Policy Settings

+ Add URL Filtering Rule

Recommended Policy

Search...

Rule Or...	Rule Name	Criteria	Action	Description
1	ServiceNow-Comp...	PROTOCOL HTTPS; HTTP  REQUEST METHODS GET; HEAD; TRACE; CONNECT  URL CATEGORIES ServiceNow  USER AGENT Microsoft Internet Explorer; Microsoft Edge...	Isolate	
2	Isolate testtheproxy	PROTOCOL HTTPS; HTTP  REQUEST METHODS GET; HEAD; TRACE; CONNECT  URL CATEGORIES	Isolate	

Figure 41. Completed isolation profile

## Configuring the ServiceNow Tenant

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

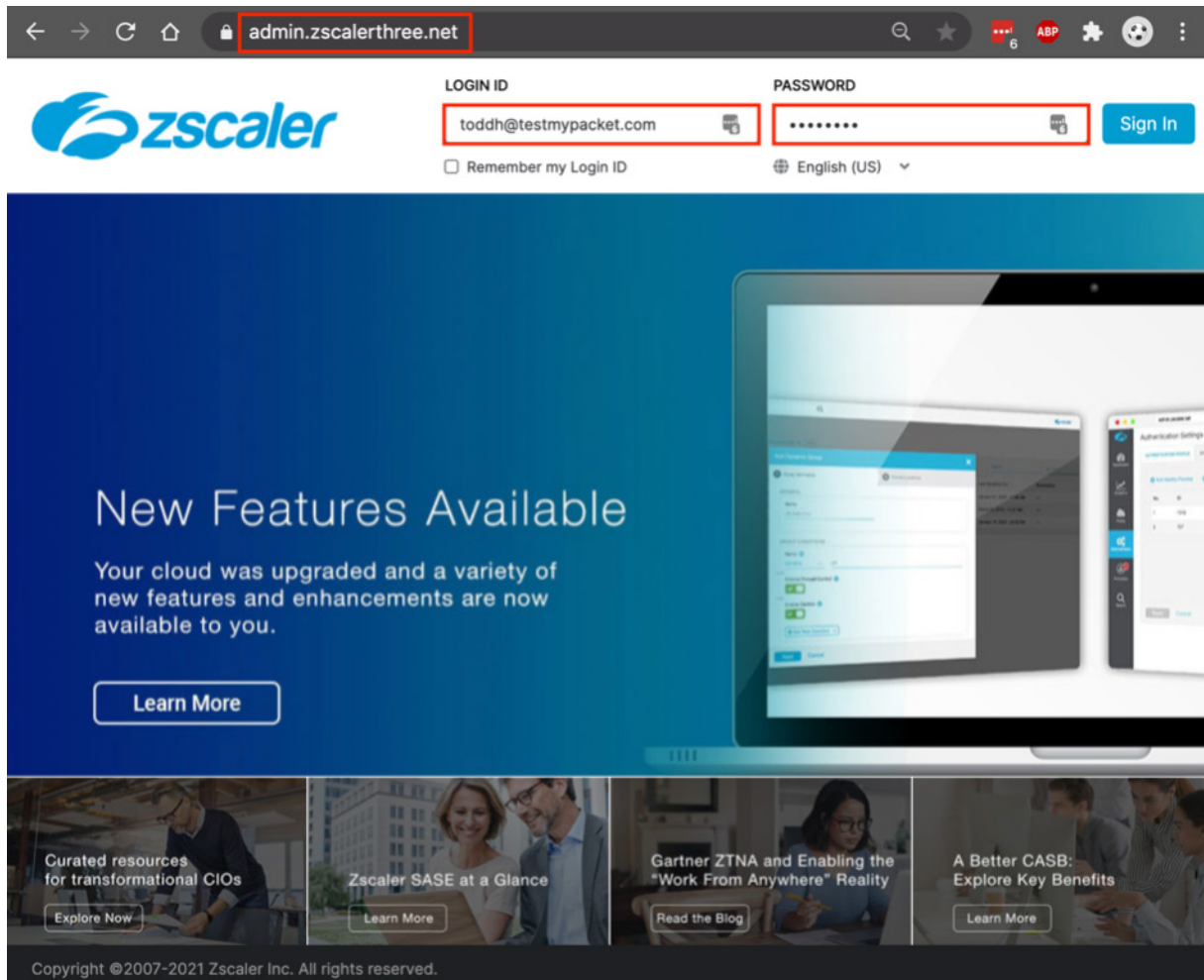


Figure 42. ZIA Admin Portal

## 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**.

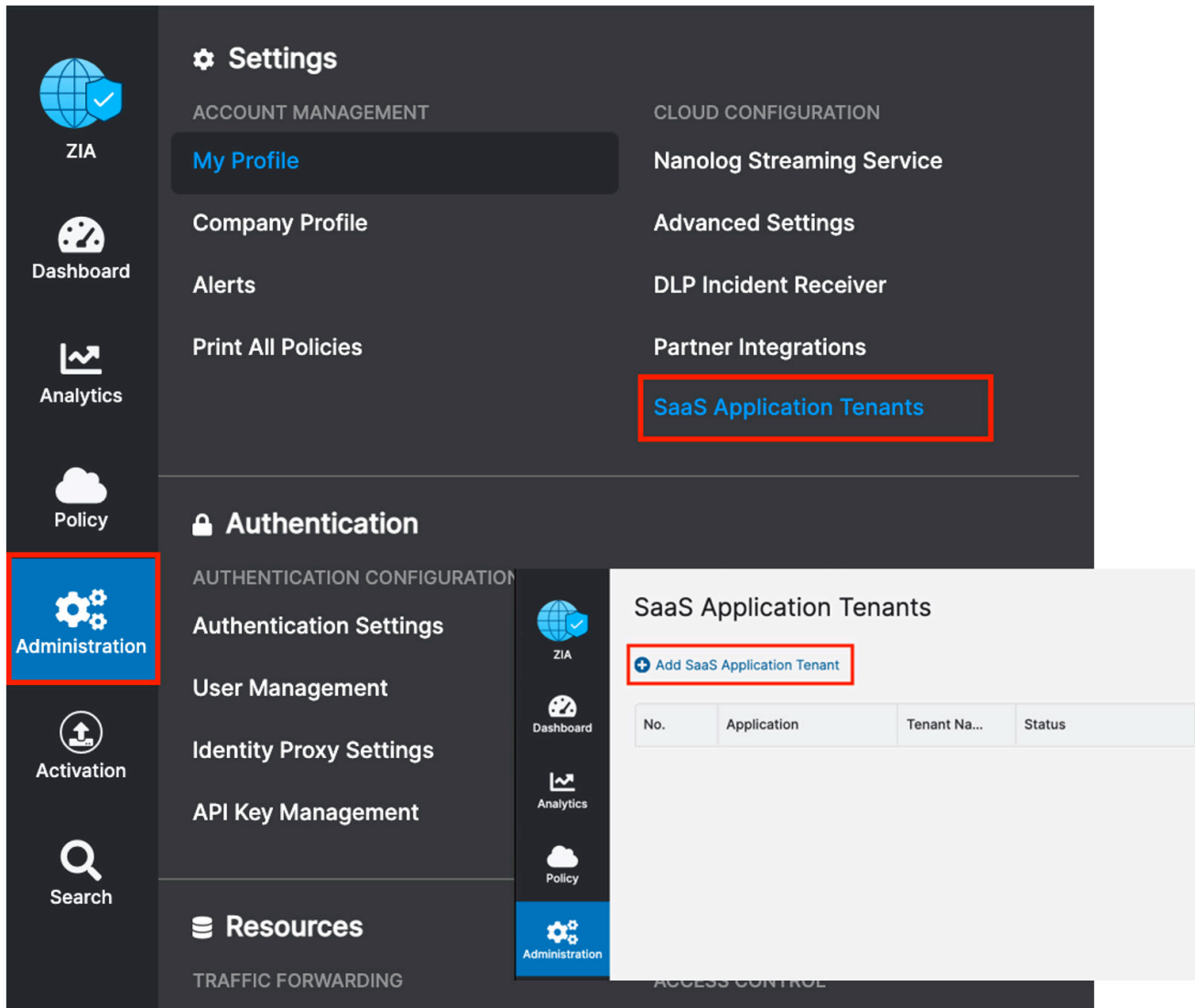


Figure 43. ZIA SaaS application tenant

## SaaS Tenant Configuration Wizard

To start the wizard:

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

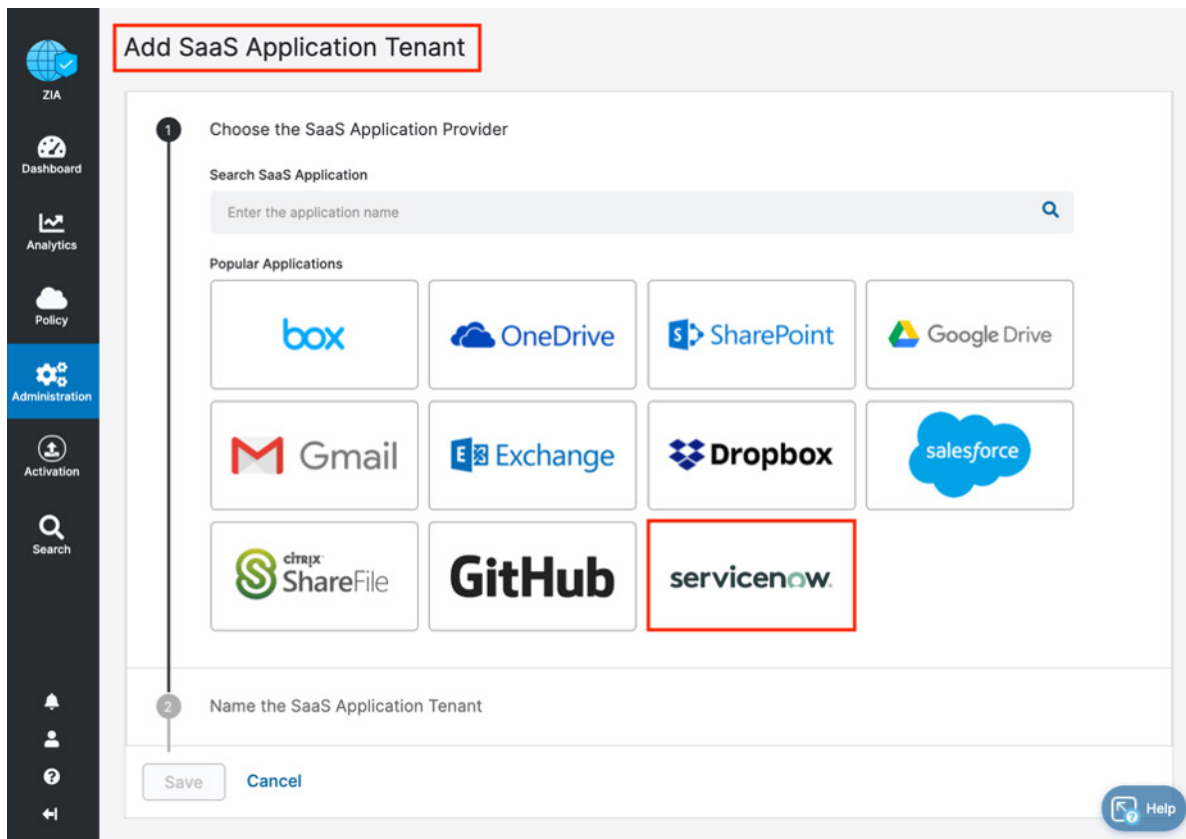


Figure 44. The SaaS tenant configuration



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 log in to your ServiceNow tenant with admin role credentials.

**Add SaaS Application Tenant**

1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name

ServiceNow

The tenant name must be unique

3 Register the OAuth Application

You must configure an OAuth client application for the Zscaler service in your ServiceNow instance. After, enter the OAuth client application details so the Zscaler service can connect to the application. [Learn more](#)

Client ID

Client Secret

Instance URL

User ID

User Password

Save Cancel

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.

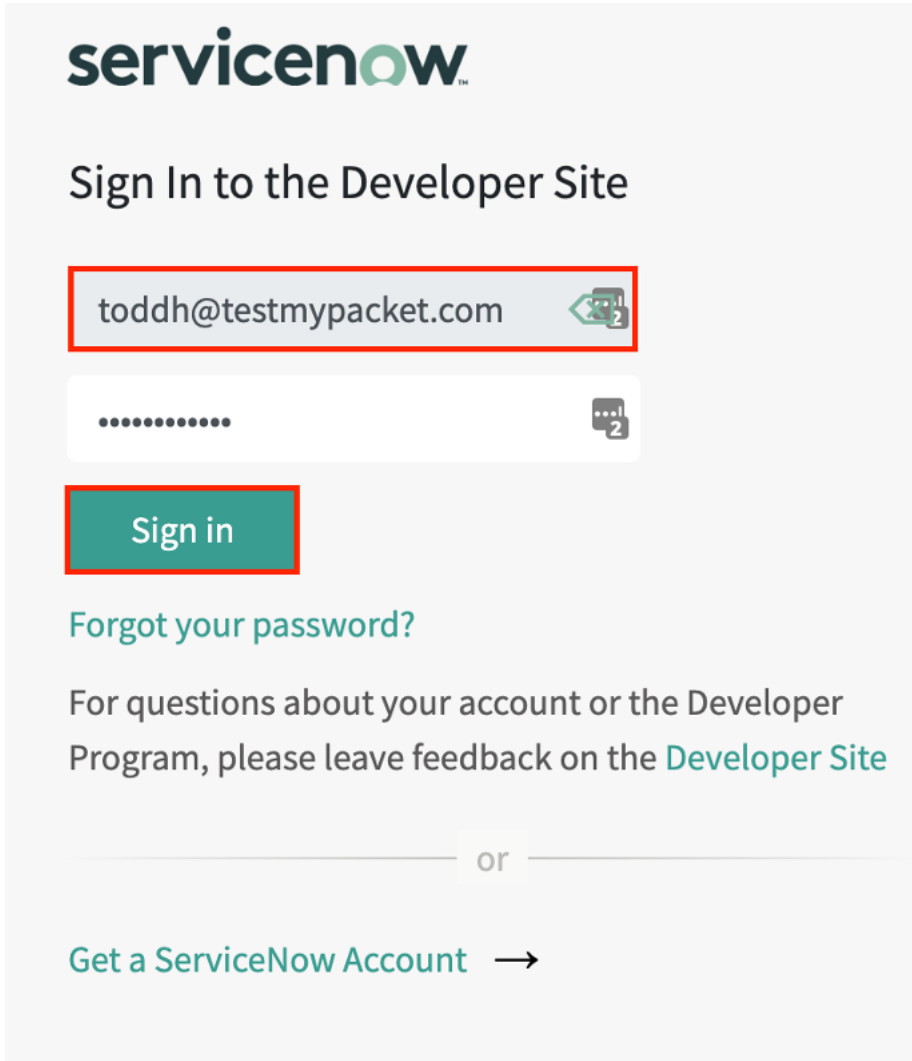
The image shows the ServiceNow login page for the Developer Site. At the top is the ServiceNow logo. Below it is the heading "Sign In to the Developer Site". There are two input fields: the first for the email address, which contains "toddh@testmypacket.com" and is highlighted with a red rectangle; the second for the password, which is masked with dots and also highlighted with a red rectangle. Below the password field is a green "Sign in" button, also highlighted with a red rectangle. Under the button is a link "Forgot your password?". Below that is a paragraph of text: "For questions about your account or the Developer Program, please leave feedback on the Developer Site". At the bottom, there is a horizontal line with the word "or" in the center, and below that is a link "Get a ServiceNow Account" followed by a right-pointing arrow.

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, enter `OAuth 2.0`.
  - b. Verify OAuth is installed.
4. If OAuth is not installed:
  - a. Select **Install**.
  - b. Select **Activate**.

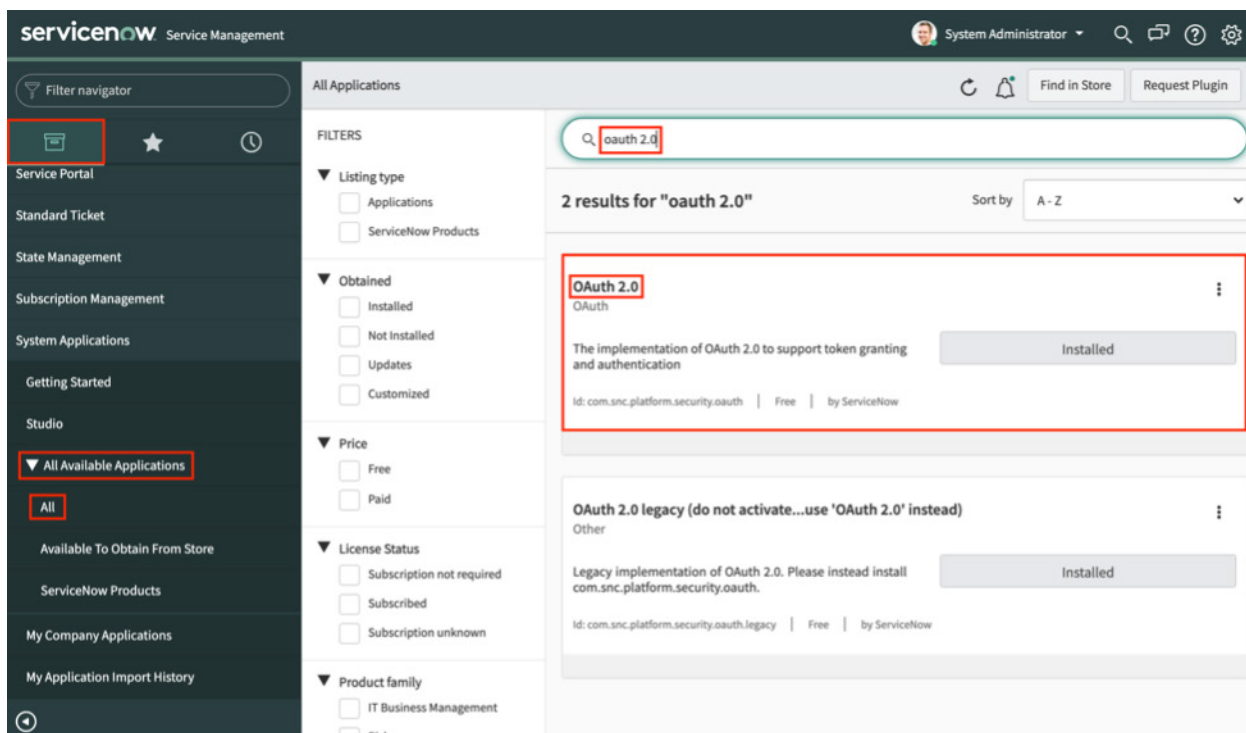


Figure 47. Verify OAuth is installed

## 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.

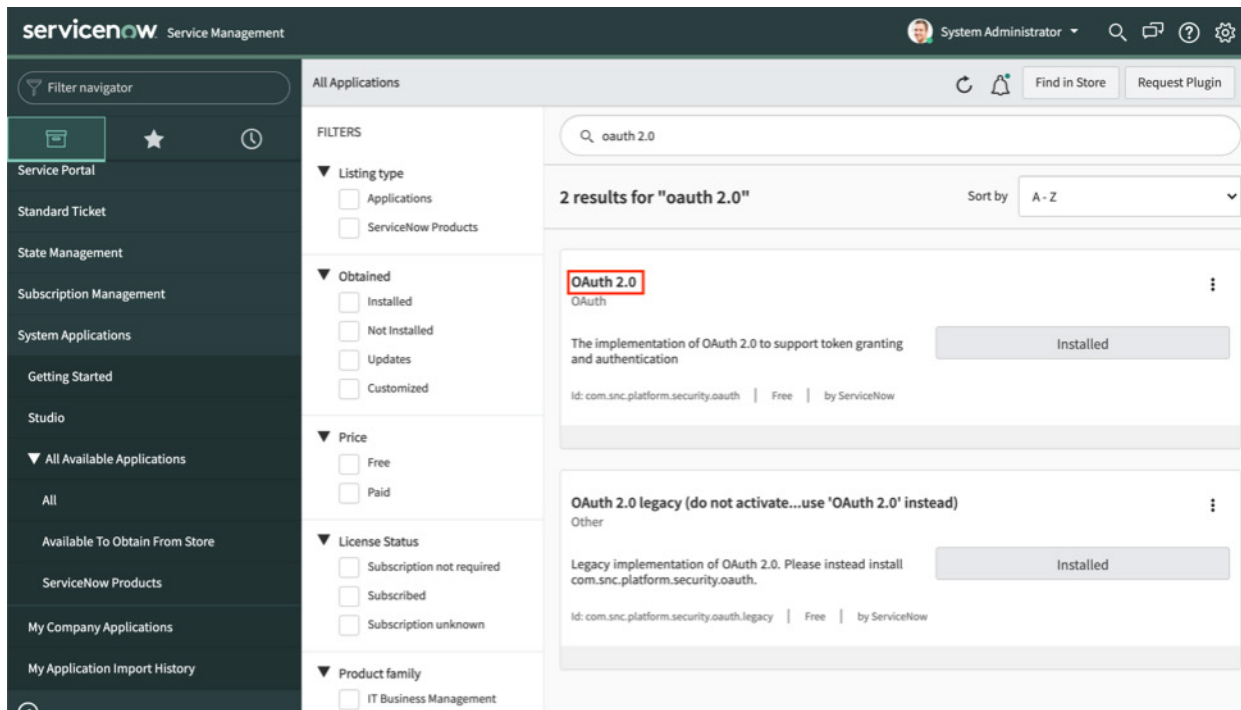
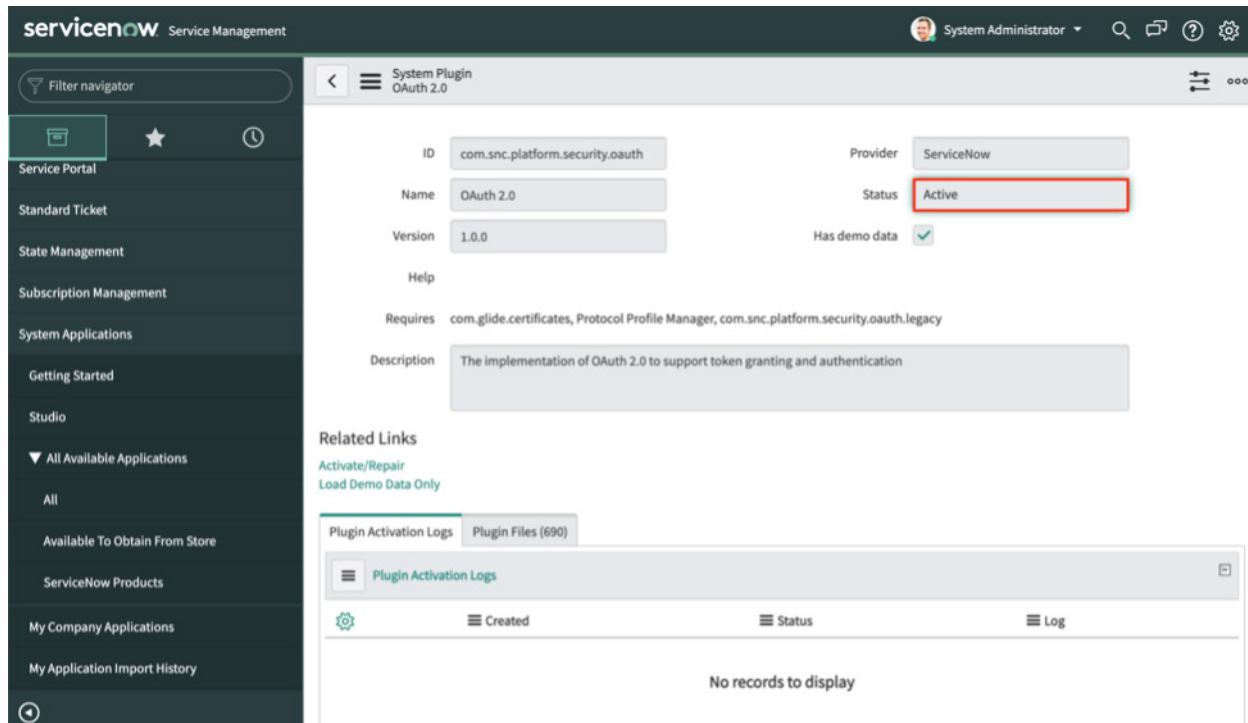


Figure 48. The installed Zscaler SaaS connector

## Check that the OAuth Plugin is Active

Check that the status of OAuth 2.0 is **Active**.



The screenshot shows the ServiceNow Service Management console. The left sidebar contains navigation links: Service Portal, Standard Ticket, State Management, Subscription Management, System Applications, Getting Started, Studio, All Available Applications, All, Available To Obtain From Store, ServiceNow Products, My Company Applications, and My Application Import History. The main content area displays the configuration for the 'System Plugin OAuth 2.0'. The 'Status' field is highlighted with a red box and shows 'Active'. Other fields include ID (com.snc.platform.security.oauth), Name (OAuth 2.0), Version (1.0.0), Provider (ServiceNow), and Has demo data (checked). The 'Requires' field lists dependencies: com.glide.certificates, Protocol Profile Manager, and com.snc.platform.security.oauth.legacy. The 'Description' field states: 'The implementation of OAuth 2.0 to support token granting and authentication'. Below the configuration, there are 'Related Links' (Activate/Repair, Load Demo Data Only) and a 'Plugin Activation Logs' section. The 'Plugin Activation Logs' section shows a table with columns 'Created', 'Status', and 'Log', but it is currently empty, displaying 'No records to display'.

ID	Provider	Name	Status	Version	Has demo data
com.snc.platform.security.oauth	ServiceNow	OAuth 2.0	Active	1.0.0	<input checked="" type="checkbox"/>

Requires: com.glide.certificates, Protocol Profile Manager, com.snc.platform.security.oauth.legacy

Description: The implementation of OAuth 2.0 to support token granting and authentication

Related Links: [Activate/Repair](#), [Load Demo Data Only](#)

Plugin Activation Logs

Created	Status	Log
No records to display		

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**.

The screenshot shows the ServiceNow Service Management interface. On the left, the 'Filter navigator' is visible with a file box icon highlighted. Below it, the 'System OAuth' menu is expanded, and 'Application Registry' is selected. At the top of the main content area, the 'Application Registries' tab is active, and the 'New' button is highlighted. A search bar is present with the text 'Name' and a search icon. Below the search bar, a filter bar shows 'All > Type = OAuth Client .or. Type = OAuth Provider'. The main table displays a list of application registries with columns for Name, Active, Type, and Client ID.

	Name	Active	Type	Client ID
<input type="checkbox"/>	<a href="#">ADFS</a>	true	External OIDC Provider	{adfds-applicatio here}
<input type="checkbox"/>	<a href="#">Auth0</a>	true	External OIDC Provider	{auth0-applicatio here}
<input type="checkbox"/>	<a href="#">Azure AD</a>	true	External OIDC Provider	{azure-ad-applic here}
<input type="checkbox"/>	<a href="#">Google</a>	true	External OIDC Provider	{google-applicat here}
<input type="checkbox"/>	<a href="#">Mobile API</a>	true	OAuth Client	ac0dd3408c1031
<input type="checkbox"/>	<a href="#">Okta</a>	true	External OIDC Provider	{okta-applicatio here}
<input type="checkbox"/>	<a href="#">ServiceNow Agent</a>	true	OAuth Client	ff97fbb4da33130

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**.

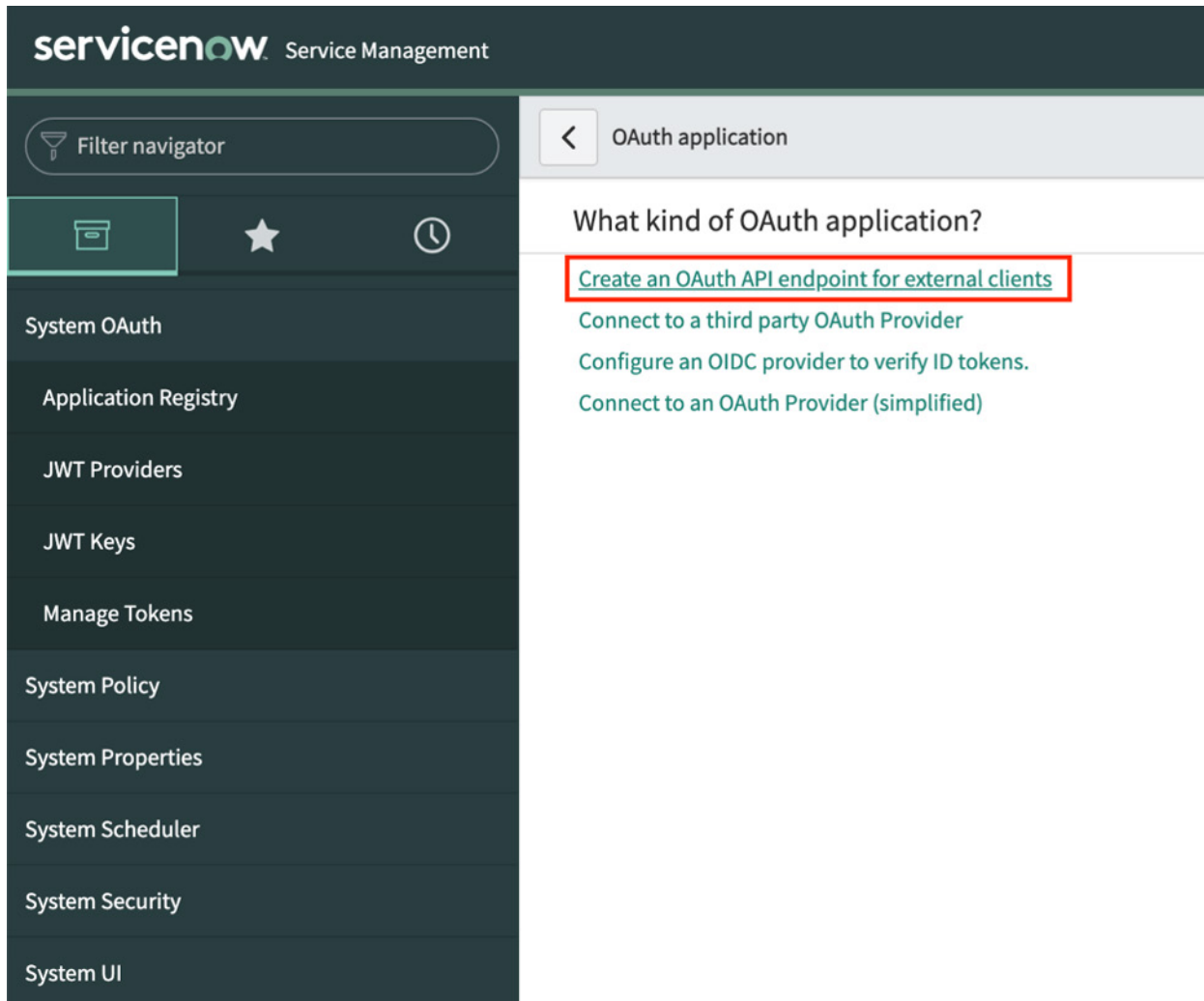


Figure 51. Create an OAuth API endpoint

## Configuring the Zscaler Tenant on ServiceNow

Complete the OAuth API endpoint details:

1. Enter `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 must be reinstalled.
3. Enter the **Access Token Lifespan** in seconds. Zscaler recommends 86,400 (24 hours).
4. Click **Submit** to save the settings.

The screenshot shows the ServiceNow 'Application Registries' form. The left sidebar contains navigation links: Filter navigator, System OAuth, Application Registry, JWT Providers, JWT Keys, Manage Tokens, System Policy, System Properties, System Scheduler, System Security, System UI, System Update Sets, System User Guide, and System Web Services. The main form area is titled 'Application Registries' and shows a 'New record' button. Below this is a 'More Info' section with details about OAuth client application details. The form fields are as follows:

- Name:** Zscaler (highlighted with a red box)
- Client ID:** ef49e97caba320107467e37f44 (highlighted with a red box)
- Client Secret:** (empty field with a note: 'Leave Client Secret blank to automatically generate a string')
- Application:** Global
- Accessible from:** All application scopes
- Active:** ☒
- Refresh Token Lifespan:** 157,700,000 (highlighted with a red box)
- Access Token Lifespan:** 86,400 (highlighted with a red box)
- Redirect URL:** (empty field)
- Logo URL:** (empty field)
- Comments:** This creates the Zscaler API Tenant. The Client Secret will be created once this page has been submitted.

A red 'Submit' button is located at the bottom left of the form.

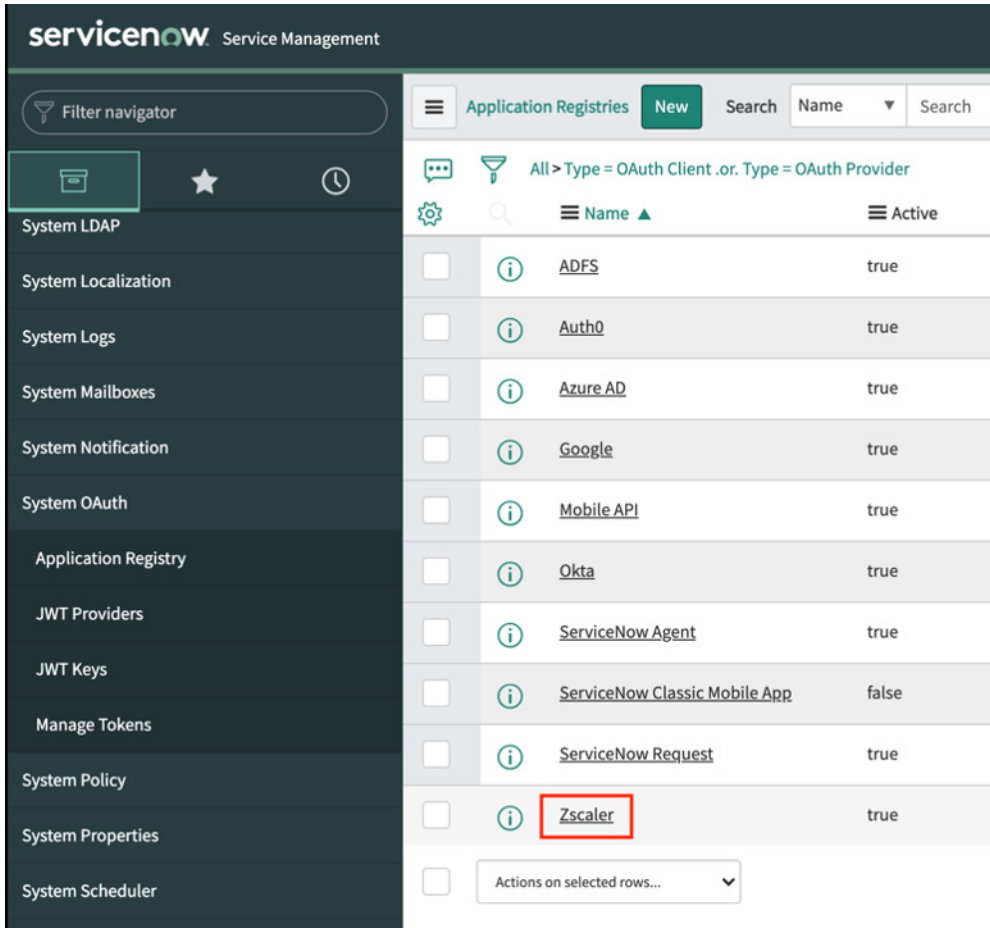
Figure 52. Creating the OAuth endpoint



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



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



The screenshot shows the ServiceNow Service Management interface. On the left is a dark sidebar with a 'Filter navigator' and a list of system settings including 'System LDAP', 'System Localization', 'System Logs', 'System Mailboxes', 'System Notification', 'System OAuth', 'Application Registry', 'JWT Providers', 'JWT Keys', 'Manage Tokens', 'System Policy', 'System Properties', and 'System Scheduler'. The 'Application Registry' item is highlighted. The main content area is titled 'Application Registries' and includes a 'New' button, a search bar, and a filter 'All > Type = OAuth Client .or. Type = OAuth Provider'. Below this is a table with columns 'Name' and 'Active'. The table lists several OAuth providers, with 'Zscaler' highlighted by a red box. At the bottom of the table is an 'Actions on selected rows...' dropdown.

	Name	Active
<input type="checkbox"/>	<a href="#">ADFS</a>	true
<input type="checkbox"/>	<a href="#">Auth0</a>	true
<input type="checkbox"/>	<a href="#">Azure AD</a>	true
<input type="checkbox"/>	<a href="#">Google</a>	true
<input type="checkbox"/>	<a href="#">Mobile API</a>	true
<input type="checkbox"/>	<a href="#">Okta</a>	true
<input type="checkbox"/>	<a href="#">ServiceNow Agent</a>	true
<input type="checkbox"/>	<a href="#">ServiceNow Classic Mobile App</a>	false
<input type="checkbox"/>	<a href="#">ServiceNow Request</a>	true
<input type="checkbox"/>	<a href="#">Zscaler</a>	true
<input type="checkbox"/>	Actions on selected rows...	

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** icon next to the **Client Secret** to reveal the secret.
3. Copy the **Client Secret**.

The screenshot shows the ServiceNow interface for managing OAuth client applications. The left sidebar contains a 'Filter navigator' and a list of system settings including System LDAP, System Localization, System Logs, System Mailboxes, System Notification, System OAuth, Application Registry, JWT Providers, JWT Keys, Manage Tokens, System Policy, System Properties, and System Scheduler. The main content area is titled 'Application Registries - Zscaler [Default view\*]'. It features a light blue informational box with OAuth client application details, including Name, Client ID, Client Secret, Refresh Token Lifespan, Access Token Lifespan, and Redirect URL. Below this, the 'Zscaler' application is configured with a Client ID of '6c3c7df63513201047ed8581ec1e43fb' and a Client Secret of '+GGhy73-2.'. The Client Secret field is locked, indicated by a lock icon. The Redirect URL and Logo URL fields are also locked. The Comments field contains the text 'The Zscaler API Connection. The Client Secret will be created after this'. At the bottom, there are 'Update' and 'Delete' buttons.

ServiceNow Service Management

Filter navigator

Application Registries - Zscaler [Default view\*]

OAuth client application details.

- Name: A unique name.
- Client ID: Client ID automatically generated by ServiceNow OAuth server.
- Client Secret: Client secret for the OAuth application. Leave it empty for auto-generation.
- Refresh Token Lifespan: Time in seconds the Refresh Token will be valid.
- Access Token Lifespan: Time in seconds the Access Token will be valid.
- Redirect URL: The redirect URLs authorization server redirect to. They must be absolute URLs.

[More Info](#)

\* Name Zscaler

\* Client ID 6c3c7df63513201047ed8581ec1e43fb

Client Secret \*\*\*\*\*

+GGhy73-2.

Redirect URL

Logo URL

Comments The Zscaler API Connection. The Client Secret will be created after this

Update Delete

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 **User Password**.
5. Enter the **ServiceNow Admin Email ID**.
6. Click **Authorize** to verify the credentials.
7. Click **Save**.

**Add SaaS Application Tenant**

**Tenant Name**  
ServiceNow  
The tenant name must be unique

**3 Register the OAuth Application**  
You must configure an OAuth client application for the Zscaler service in your ServiceNow instance. After, enter the OAuth client application details so the Zscaler service can connect to the application. [Learn more](#)

**Client ID**  
6c3c7df63513201047ed8581ec1e43fb

**Client Secret**  
+GGhy73-2.

**Instance URL**  
https://dev102367.service-now.com/

**User ID**  
toddh@testmypacket.com

**User Password**  
\*\*\*\*\*

**4 Enter the ServiceNow Admin Email ID**  
Enter your admin email ID used to log in to the ServiceNow instance. [Learn more](#)

**ServiceNow Admin Email ID**  
toddh@testmypacket.com

**5 Authorize the SaaS Application**  
To configure Data Loss Protection and Malware Detection policies for SaaS Security API, you must give Zscaler access to ServiceNow.

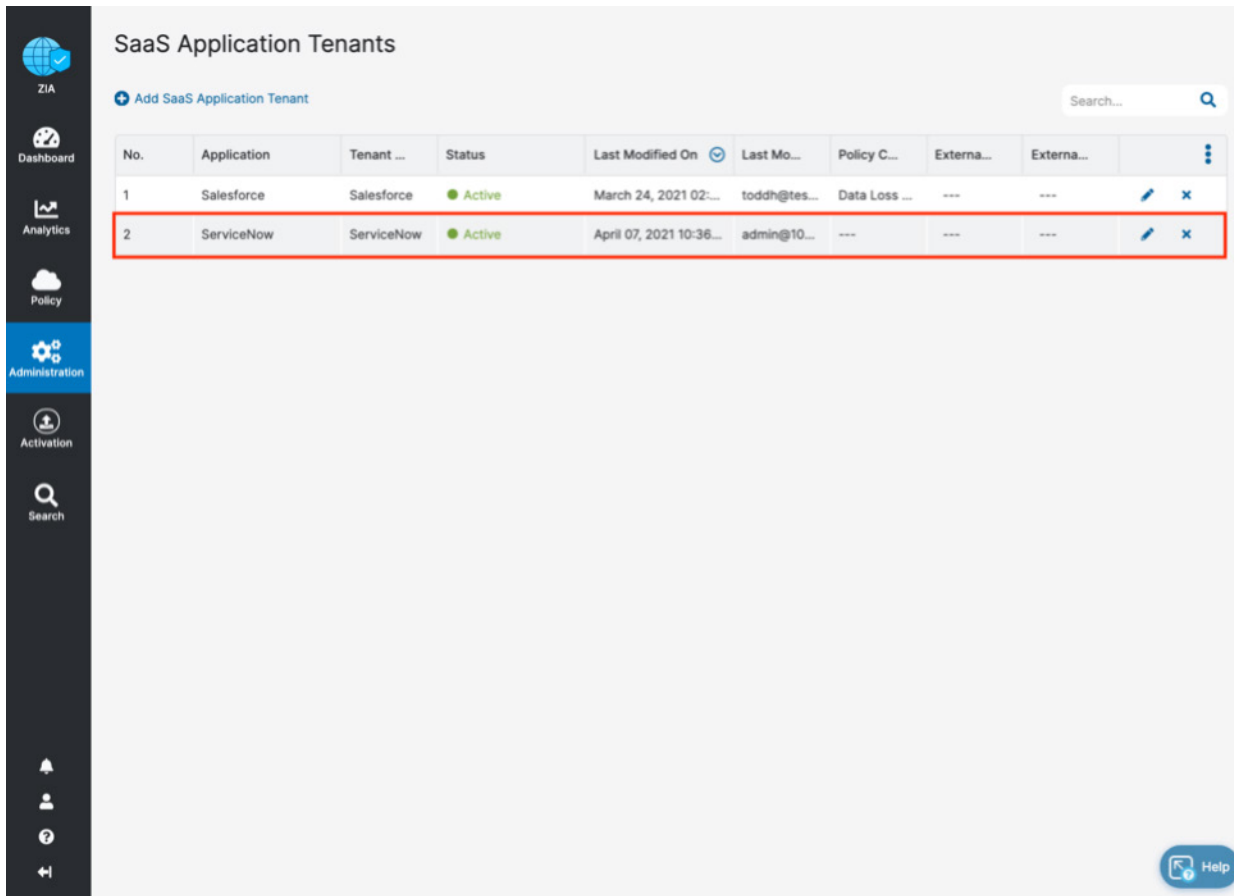
**Authorize**

**Save Cancel**

Figure 55. Finish the Zscaler tenant

## Configuring the Zscaler ServiceNow Connector

The completed and active ServiceNow API connector is displayed.



**SaaS Application Tenants**

[+ Add SaaS Application Tenant](#)

No.	Application	Tenant ...	Status	Last Modified On	Last Mo...	Policy C...	Externa...	Externa...	
1	Salesforce	Salesforce	Active	March 24, 2021 02:...	toddh@tes...	Data Loss ...	---	---	<a href="#">Edit</a> <a href="#">Delete</a>
2	ServiceNow	ServiceNow	Active	April 07, 2021 10:36...	admin@10...	---	---	---	<a href="#">Edit</a> <a href="#">Delete</a>

[Help](#)

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 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.

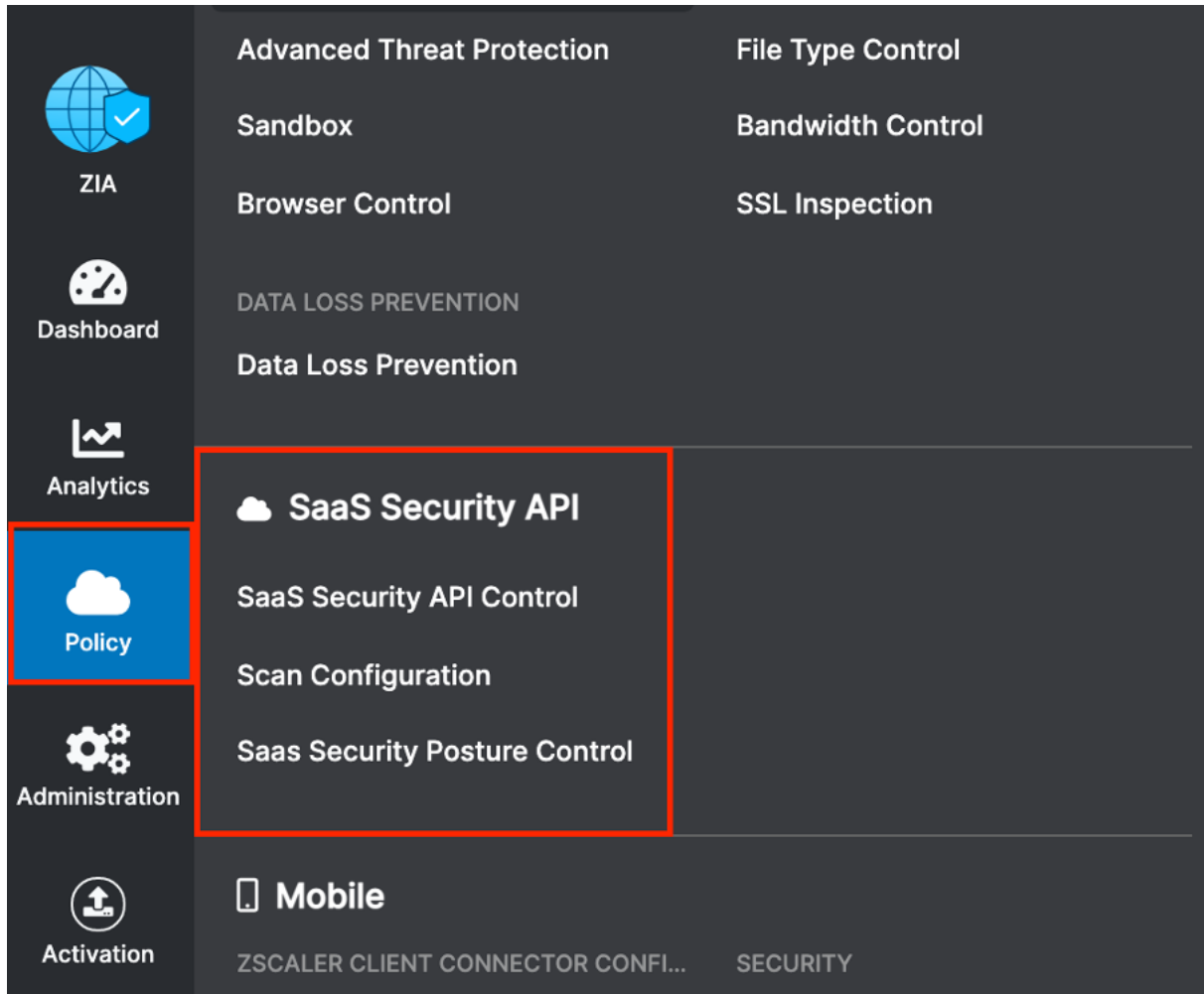


Figure 57. Zscaler policy configuration

## 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.

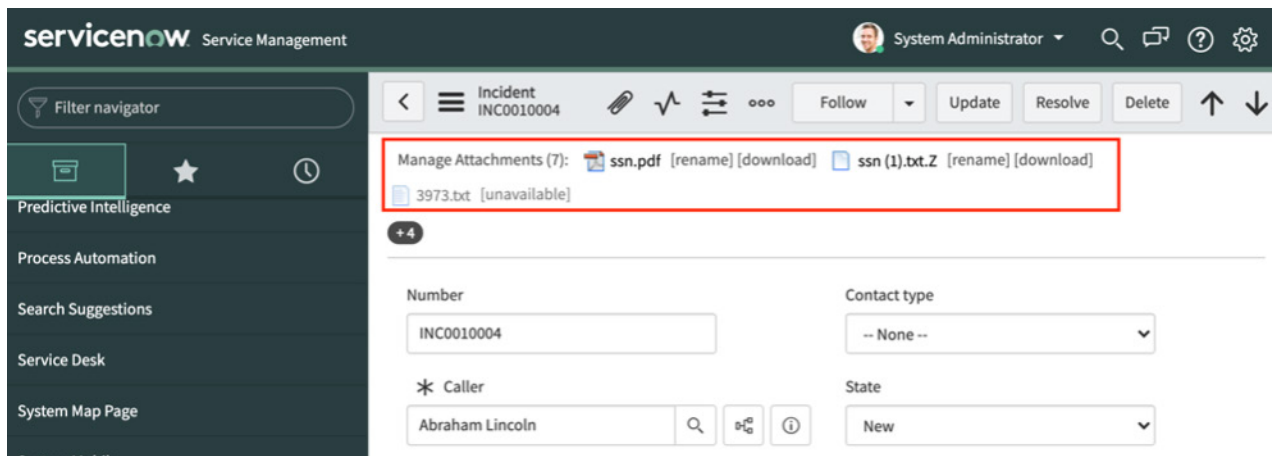


Figure 58. ServiceNow incident with malicious attachments

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 must 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](#).

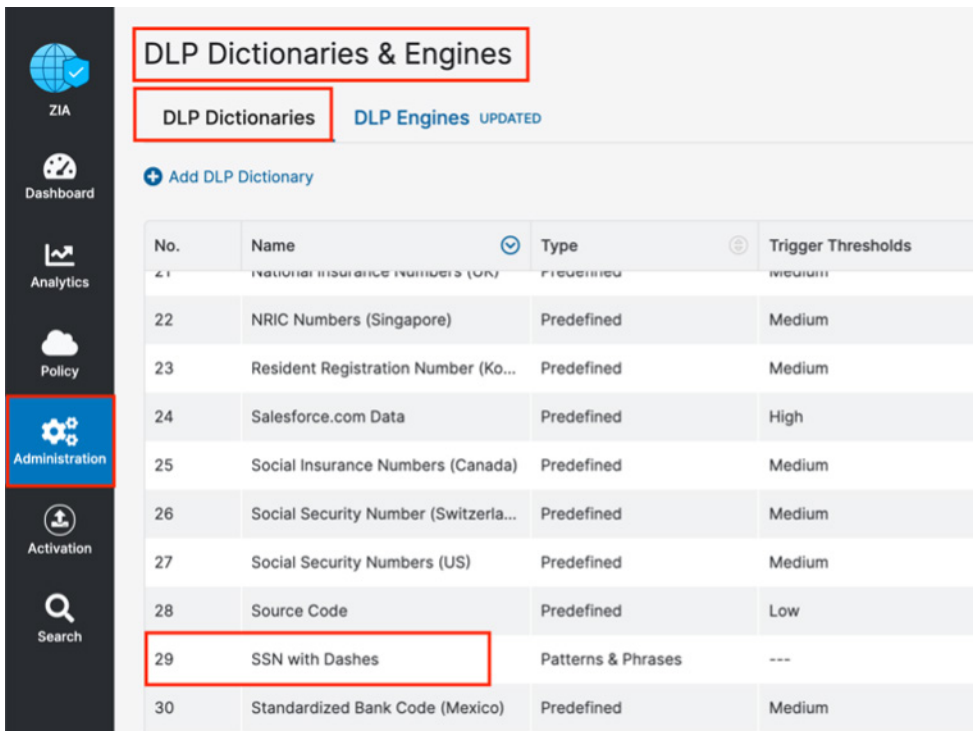
## Creating a DLP Policy

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**).



The screenshot shows the ZIA Admin Portal interface. On the left sidebar, the 'Administration' menu item is highlighted. The main content area is titled 'DLP Dictionaries & Engines'. Below this title, there are two tabs: 'DLP Dictionaries' (selected) and 'DLP Engines' (marked as 'UPDATED'). A '+ Add DLP Dictionary' button is visible. Below the tabs is a table listing various dictionaries. The table has columns for 'No.', 'Name', 'Type', and 'Trigger Thresholds'. The dictionary 'SSN with Dashes' (No. 29) is highlighted with a red box. It is of type 'Patterns & Phrases' and has a trigger threshold of '---'.

No.	Name	Type	Trigger Thresholds
21	National Insurance Numbers (UK)	Predefined	Medium
22	NRIC Numbers (Singapore)	Predefined	Medium
23	Resident Registration Number (Ko...	Predefined	Medium
24	Salesforce.com Data	Predefined	High
25	Social Insurance Numbers (Canada)	Predefined	Medium
26	Social Security Number (Switzerla...	Predefined	Medium
27	Social Security Numbers (US)	Predefined	Medium
28	Source Code	Predefined	Low
29	SSN with Dashes	Patterns & Phrases	---
30	Standardized Bank Code (Mexico)	Predefined	Medium

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**.

No.	Name	Dictionaries
1	GLBA	(Financial Statements > 0 AND Social Security Numbers (...)
2	HIPAA	(Medical Information > 0 AND Social Security Numbers (U...
3	Names and SSNs	((Social Security Numbers (US) > 5))
4	Offensive Language	(Adult Content > 0)
5	PCI	(Credit Cards > 5 AND Social Security Numbers (US) > 5)
6	SSN-with-Dashes	((SSN with Dashes > 3))

Figure 60. Creating a DLP engine



## Creating a DLP Engine

In the Add DLP Engine window:

1. Enter a **Name** for the DLP engine.
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.

The screenshot shows the 'Add DLP Engine' wizard. The 'Name' field is 'SSN-With-Dashes'. The 'EXPRESSION' section shows a dropdown menu set to 'ALL', followed by a dropdown menu set to 'SSN with Dashes', a greater-than sign '>', and a text input field containing '3'. Below this is an 'ADD' button. The 'Expression Preview' section shows the preview text '((SSN with Dashes > 3))'. The 'DESCRIPTION' section is empty. At the bottom, there are 'Save' and 'Cancel' buttons.

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 > Data at Rest Scanning**.
2. Select **Add DLP Rule**.

See the details of the policy on the following pages.

The screenshot shows the 'Add DLP Rule' wizard in the Zscaler console. The wizard is titled 'Add DLP Rule' and is part of the 'Data At Rest Scanning' section. It contains several fields for configuring a new DLP rule. The 'Rule Order' is set to 1, 'Admin Rank' is 7, 'Rule Name' is 'SaaS\_File\_Sharing\_App\_Rule\_1', and 'Rule Status' is 'Enabled'. The 'Rule Label' is currently empty. Under the 'CRITERIA' section, 'SaaS Application Tenant' is set to 'Select SaaS Application Tenant', 'Owners' is 'Any', 'Groups' is 'Any', 'Departments' is 'Any', 'DLP Engines' is 'Any', and 'File Type' is 'Any'. The 'Collaboration Scope' is also visible. At the bottom, there are 'Save' and 'Cancel' buttons.

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 action 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 **ServiceNow** as the **SaaS Application 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.

**Add DLP Rule**

**DLP RULE**

Rule Order: 1 | Admin Rank: 7

Rule Name: SaaS\_ITSM\_App\_Rule\_1 | Rule Status: Enabled

**CRITERIA**

SaaS Application Tenant: ServiceNow | Components: Any

Owners: Any | Groups: Any

Departments: Any | DLP Engines: SSN-with-Dashes

Collaboration Scope: Any - Any | Object Type: Any

**ACTION**

Action: Report Incident Only | Severity: High

**DESCRIPTION**

**Save** **Cancel**

Figure 63. The SaaS DLP Policy Configuration wizard

Apply the completed DLP rule with a scanning schedule.

The screenshot displays the Zscaler SaaS Security API Control interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy, Administration, and Activation (highlighted with a red box). The main content area is titled 'SaaS Security API Control' with a dropdown menu set to 'ITSM'. Below this, there are tabs for 'Data Loss Prevention' and 'Malware Detection'. Under 'Data Loss Prevention', there are sub-tabs for 'Policy' and 'Exceptions'. A '+ Add DLP Rule' button and a search bar are visible. A table lists the configured DLP rules, with the first rule highlighted by a red border:

No.	Rule O...	Admin...	Rule N...	Severity	Criteria	Action	Descri...	Status	
1	1	7	SaaS_JTS...	High	SaaS Application ... ServiceNow DLP Engine SSN-with-Dashes Collaboration Sco... Any - Any	Report In...	---	Enabled	

A 'Help' button is located in the bottom right corner of the interface.

Figure 64. The configured DLP policy

## Configure a SaaS Malware Policy

To launch the Malware Rule:

1. Go to **Policy > SaaS Security > Data at Rest Scanning**.
2. Select **Malware Detection**.
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.

The screenshot displays the Zscaler console interface. On the left is a navigation sidebar with icons for ZIA, Dashboard, Analytics, Policy, Administration, Activation, Search, and Alerts. The main content area is titled 'Data At Rest Scanning' and includes sub-tabs for 'Data Loss Prevention', 'Malware Detection', and 'Scanning Exceptions'. The 'Malware Detection' sub-tab is selected, and within it, the 'Policy' sub-tab is active. A modal window titled 'Add Malware Detection Rule' is open in the foreground. This modal is divided into two main sections: 'CRITERIA' and 'ACTION'. Under 'CRITERIA', there are four fields: 'Rule Name' (a text input field with a red border), 'Status' (a dropdown menu with 'Enabled' selected and a red border), 'Application' (a dropdown menu with 'Select Application' selected and a red border), and 'SaaS Application Tenant' (a dropdown menu with 'Select Tenant' selected). Below these is a 'Rule Label' field with a red border. Under the 'ACTION' section, there is an 'Action' dropdown menu with 'Select Action' selected. At the bottom of the modal are 'Save' and 'Cancel' buttons. The background page shows a table with columns 'No.' and 'Rule Name'.

Figure 65. Launch the Malware Policy Configuration

## SaaS Malware Policy

Configure the Malware Rule:

1. Go to **Policy > SaaS Security > Data at Rest Scanning**.
2. Select **Malware Detection**.
3. Select **Add Malware Detection Rule**.
4. Under **Criteria**, select **ServiceNow** as the **Application**.
5. Select **ServiceNow** as the **SaaS Application Tenant** to apply the policy.
6. Select **Enabled** for **Status**.
7. Click **Save**.

**Add Malware Detection Rule** [X]

**CRITERIA**

**Application**  
ServiceNow

**SaaS Application Tenant**  
ServiceNow

**Status**  
Enabled

**ACTION**

**Action**  
Report Malware



**Save** Cancel

Figure 66. The Malware Policy configuration

## SaaS Malware Policy

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

The screenshot displays the Zscaler Data At Rest Scanning configuration page. The left sidebar contains navigation links: ZIA, Dashboard, Analytics, Policy (highlighted), Administration, Activation, and Search. The main content area is titled 'Data At Rest Scanning' and has three tabs: Data Loss Prevention, Malware Detection (selected), and Scanning Exceptions. Under the 'Malware Detection' tab, there are two sub-tabs: Policy and Exceptions. The 'Policy' sub-tab is active, showing a table with one rule. The table has columns: No., SaaS Application Tenant, Application, Action, Status, and a menu icon. The first row is highlighted with a red border and contains the following data:

No.	SaaS Application Tenant	Application	Action	Status	
1	ServiceNow	ServiceNow	Report Malware	Enabled	 

Below the table, there is a '+ Add Malware Detection Rule' button and a search bar. A 'Help' button is located in the bottom right corner of the main content area.

Figure 67. The completed Malware Policy configuration



## Configure the Scan Schedule Configuration

The final configuration step is to create a Scan Configuration. Specify the tenant to which the Scan Configuration applies, 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 > Scan Configuration > Add Scan Schedule**.
2. Select the ServiceNow SaaS tenant for the **SaaS Application Tenant**.
3. For **Policy**, select the Data Loss Prevention policy and the Malware Detection policy created in prior procedures.
4. For **Data To Scan**, select **All Data** (or for a POV, select **New Data Only**).
5. Click **Save**, and then **Activate** the configuration.

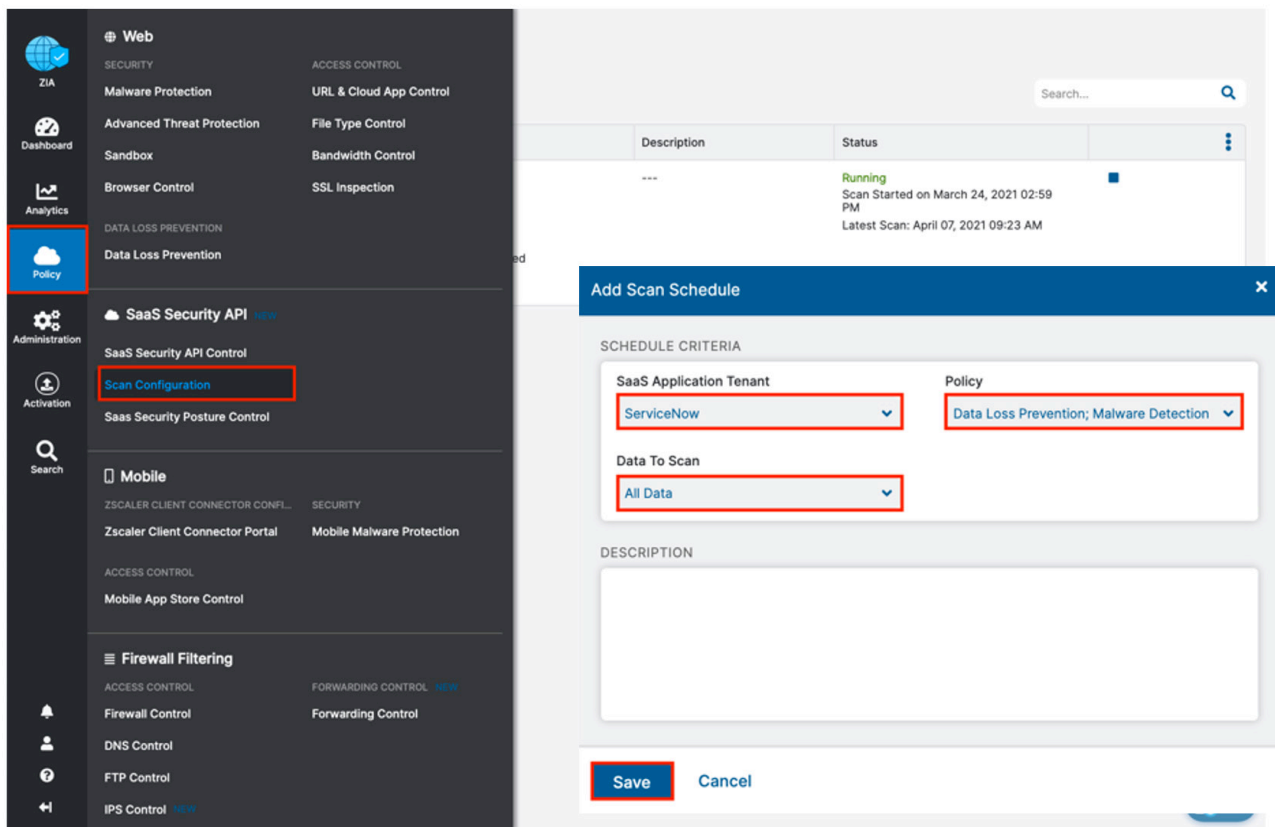


Figure 68. Create and enable a scan for the SaaS tenant

## 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 Security on the ServiceNow tenant.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.

The screenshot shows the ZIA Scan Configuration interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy (highlighted with a red box), Administration, Activation, and Search. The main content area is titled 'Scan Configuration' (also highlighted with a red box) and includes an 'Add Scan Schedule' button and a search bar. A table lists scan configurations, with the first entry for 'ServiceNow' having a status of 'Running'. The status column for this entry contains a blue square icon, which is highlighted with a red box and pointed to by a red arrow. Below the table, a toolbar contains three icons: a blue play button (highlighted with a red box), a blue pencil, and a blue 'X'.

No.	SaaS Application...	Schedule Criteria	Description	Status
1	ServiceNow	POLICY Data Loss Prevention Malware Detection  DATA TO SCAN Data Created or Modified After March 24, 2021	---	Running Scan Started on March 24, 2021 02:59 PM Latest Scan: April 07, 2021 09:23 AM

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](#)).

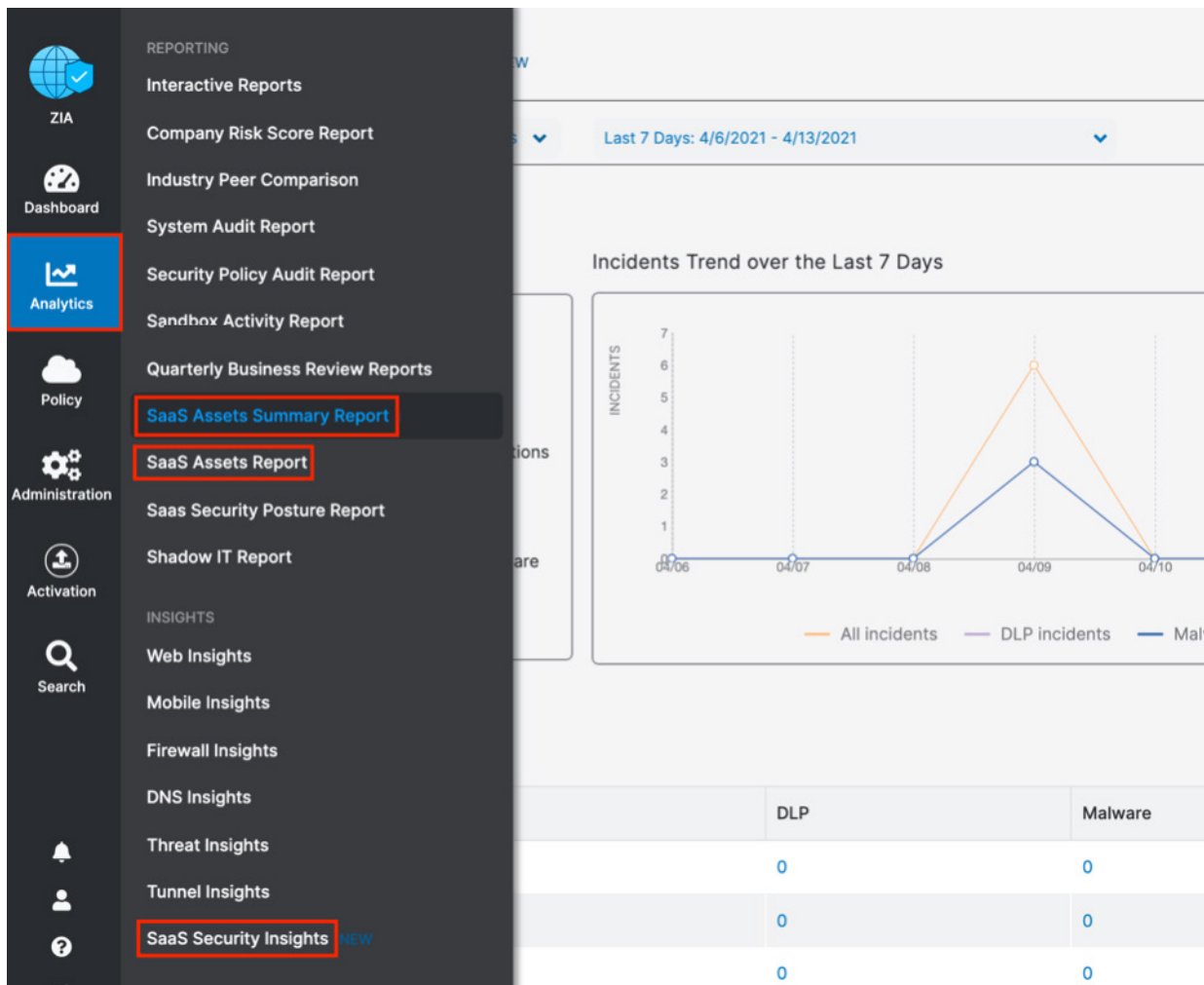


Figure 70. SaaS Security visibility

## SaaS Assets and SaaS Assets Summary Report

The SaaS Assets 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 at a quick glance. The report identifies all SaaS tenant information from a single window. Although your ServiceNow activity over the creation of this deployment guide is shown, any tenant configured is displayed on this summary report.

The data is hyperlinked, and you can 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.

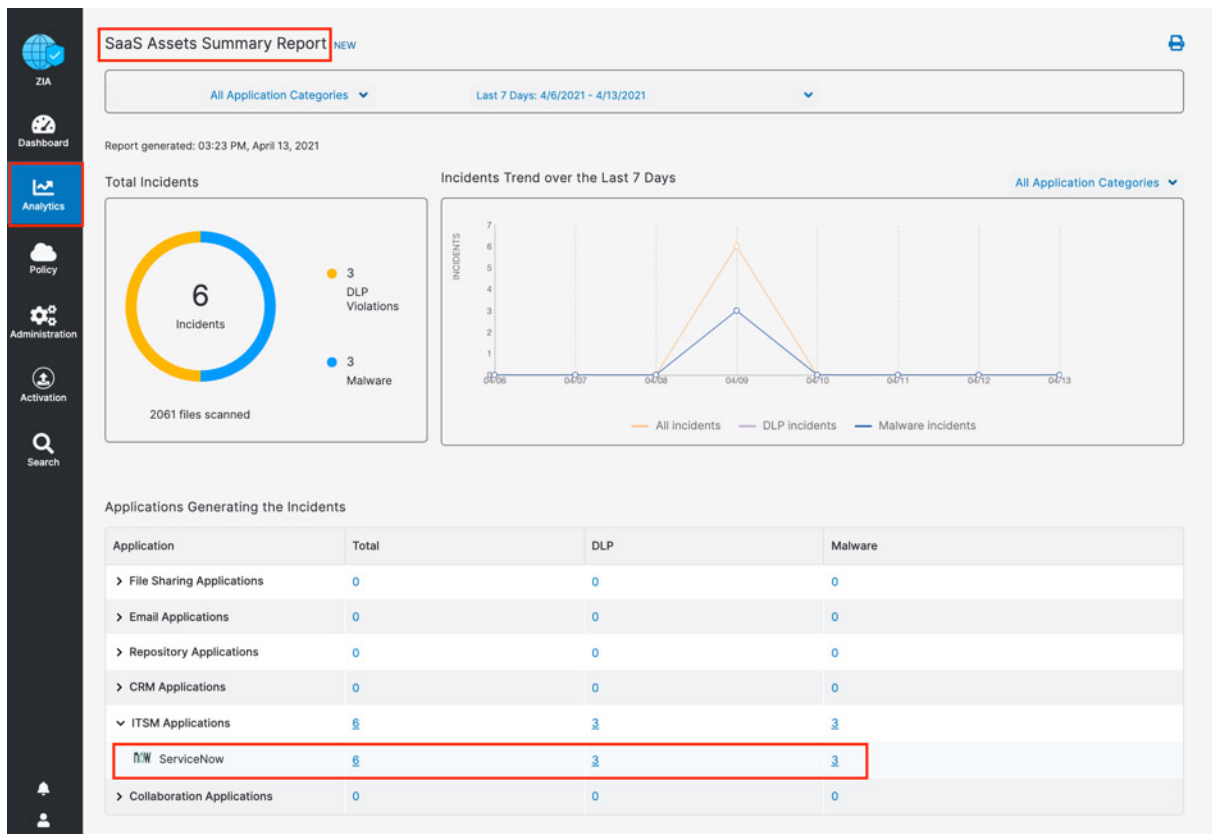


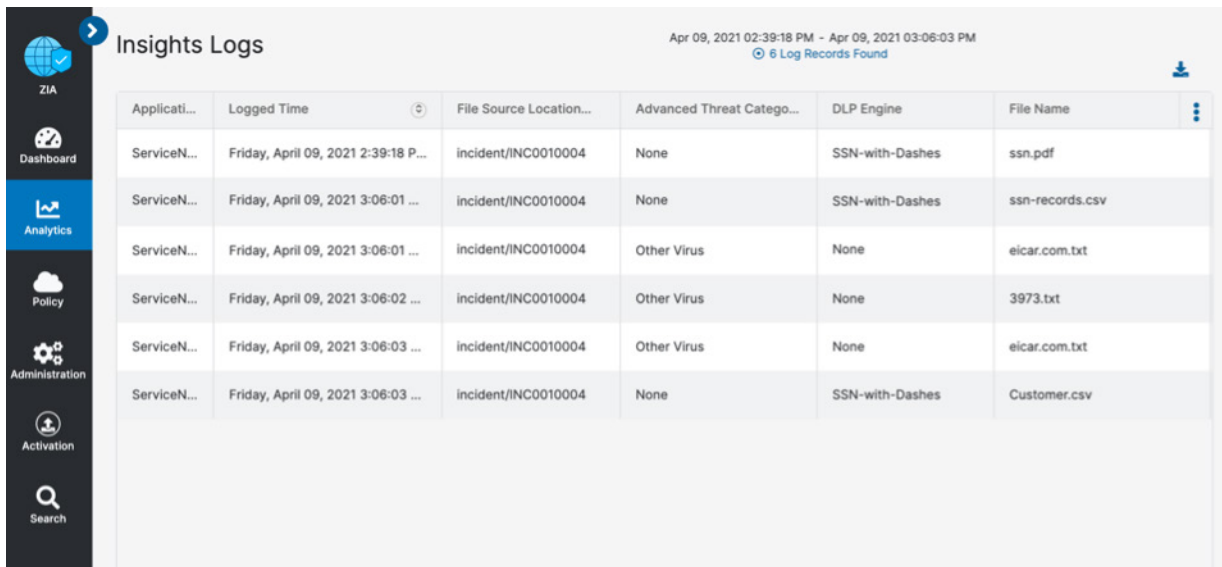
Figure 71. Summary reports

## 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



The screenshot shows the ZIA Insights Logs interface. On the left is a sidebar with navigation icons for ZIA, Dashboard, Analytics (highlighted), Policy, Administration, Activation, and Search. The main header area displays the title 'Insights Logs', a time range 'Apr 09, 2021 02:39:18 PM - Apr 09, 2021 03:06:03 PM', and a status '6 Log Records Found'. Below the header is a table with the following columns: Application, Logged Time, File Source Location, Advanced Threat Category, DLP Engine, and File Name. The table contains six rows of log records.

Applicati...	Logged Time	File Source Location...	Advanced Threat Catego...	DLP Engine	File Name
ServiceN...	Friday, April 09, 2021 2:39:18 P...	incident/INC0010004	None	SSN-with-Dashes	ssn.pdf
ServiceN...	Friday, April 09, 2021 3:06:01 ...	incident/INC0010004	None	SSN-with-Dashes	ssn-records.csv
ServiceN...	Friday, April 09, 2021 3:06:01 ...	incident/INC0010004	Other Virus	None	eicar.com.txt
ServiceN...	Friday, April 09, 2021 3:06:02 ...	incident/INC0010004	Other Virus	None	3973.txt
ServiceN...	Friday, April 09, 2021 3:06:03 ...	incident/INC0010004	Other Virus	None	eicar.com.txt
ServiceN...	Friday, April 09, 2021 3:06:03 ...	incident/INC0010004	None	SSN-with-Dashes	Customer.csv

Figure 72. SaaS Security Insights

# 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. Log in to your 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**.

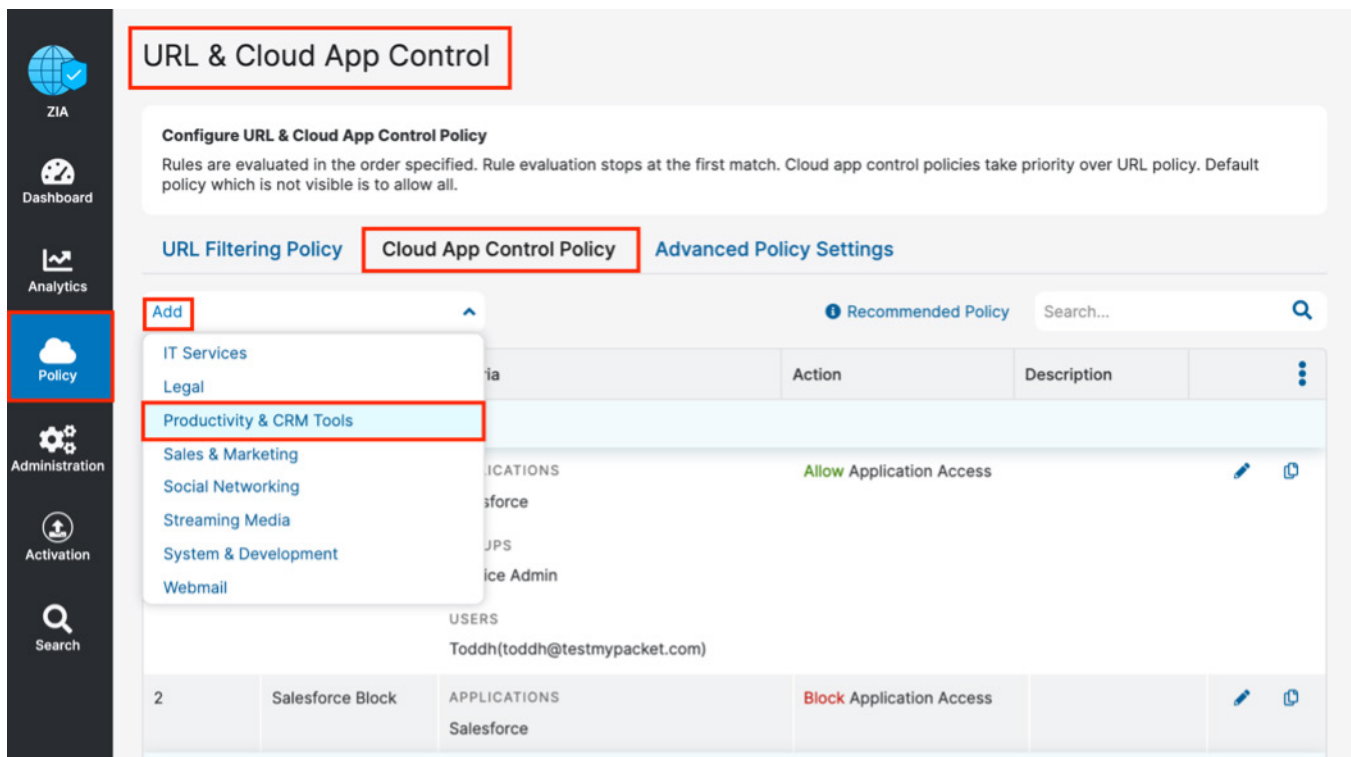


Figure 73. URL & Cloud App Control

This launches the **Add Productivity and CRM Tools Rule** dialog.

## Cloud App Control Policy

To create an Allow policy:

1. Set the **Rule Order** to 1.
2. Enter an intuitive **Rule Name**.
3. For **Cloud Applications**, select **ServiceNow**.
4. For **Users**, select the user that is the ServiceNow admins.
5. Select **Allow** for **Application Access**.
6. Click **Save**.

**Add Productivity and CRM Tools Rule**

**CLOUD APP CONTROL RULE**

Rule Order: 1

Rule Name: ServiceNow Access

Rule Status: Enabled

**CRITERIA**

Cloud Applications: ServiceNow

Users: Toddh (toddh@testmypacket.com)

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

User Agent: Any

**RULE EXPIRATION**

Enable Rule Expiration: ☐

**ACTION**

Application Access: ☒ Allow ☐ Block

Daily Bandwidth Quota (MB): Enter Text

Daily Time Quota (min): Enter Text

**Save** **Cancel**

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. For **Cloud Applications**, select **ServiceNow**.
8. Leave all other settings as **Any**.
9. Select **Block** for **Application Access**.
10. Click **Save**, then **Activate** the changes.

**Add Productivity and CRM Tools Rule**

CLOUD APP CONTROL RULE

Rule Order: 2

Rule Name: ServiceNow Deny Access

Rule Status: Enabled

CRITERIA

Cloud Applications: ServiceNow

Users: Any

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

User Agent: Any

RULE EXPIRATION

Enable Rule Expiration: ☐

ACTION

Application Access:

DESCRIPTION

Figure 75. Create a Cloud App Control Deny policy



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

The screenshot displays the Zscaler management console. On the left is a navigation sidebar with icons for ZIA, Dashboard, Analytics, Policy, Administration, and Search. The main content area is titled "URL & Cloud App Control" and contains a "Configure URL & Cloud App Control Policy" section. Below this, there are three tabs: "URL Filtering Policy", "Cloud App Control Policy" (which is selected and highlighted with a red box), and "Advanced Policy Settings".

Under the "Cloud App Control Policy" tab, there is a table of rules. The table has columns for "Rule Or...", "Rule Name", and "Criteria". A red box highlights the first rule, which is a deny policy for ServiceNow.

Rule Or...	Rule Name	Criteria
PRODUCTIVITY & CRM TOOLS		
1	ServiceNow Access	APPLICATIONS ServiceNow
		USERS Toddh{toddh@testmypac
2	ServiceNow Deny ...	APPLICATIONS ServiceNow

Overlaid on the right side of the screenshot is a red-bordered error message box. It contains the following text:

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

---

**Website blocked**

Not allowed the use of this business site

ServiceNow

---

[See our internet use policy.](#)

Need help? Contact our support team at +91-9000000000, [support@10656179.zscalerthree.net](mailto:support@10656179.zscalerthree.net) D30

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. Log in to your 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. Click **Apply Filters**.

The screenshot displays the Zscaler ZIA Admin Portal interface. On the left sidebar, the 'Analytics' and 'Logs' tabs are visible, with 'Logs' selected. The main panel shows the 'Insights Logs' view for the time frame 'Apr 13, 2021 04:11:50 PM - Apr 13, 2021 04:11:50 PM'. The table below shows 4 log records found.

No...	Event Time	User	Policy Action	Location
1	Tuesday, April 13, 2021 4:11:50 PM	toddh@testmypac...	Not allowed the use of th...	Road Warrior
2	Tuesday, April 13, 2021 4:11:50 PM	toddh@testmypac...	Not allowed the use of th...	Road Warrior
3	Tuesday, April 13, 2021 4:11:50 PM	toddh@testmypac...	Not allowed the use of th...	Road Warrior
4	Tuesday, April 13, 2021 4:11:50 PM	toddh@testmypac...	Not allowed the use of th...	Road Warrior

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

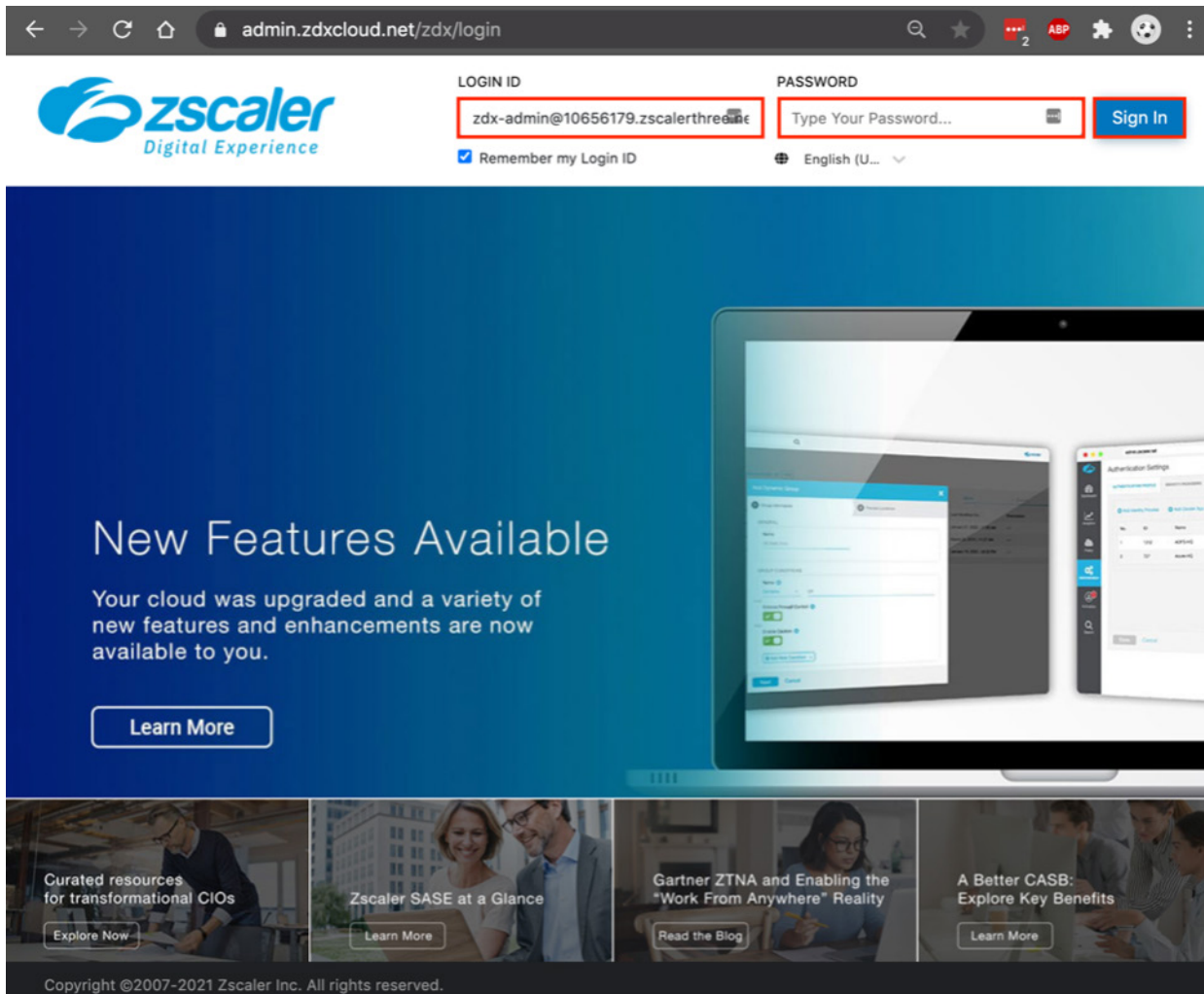


Figure 78. ZDX user experience monitoring for ServiceNow

## 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. For **Enter Tenant ID to onboard ServiceNow**, enter the URL for your ServiceNow tenant login.
5. Click **Submit**.

The screenshot shows the ZDX Applications configuration interface. On the left is a sidebar with navigation icons: ZDX Dashboard, Applications, Users, User Search, Configuration (highlighted with a red box), Administration, Alerts, Activation, and Account. The main content area has tabs for 'Applications' and 'Probes'. Below the tabs, it says 'Predefined Applications (8)'. A table lists applications: Box, Microsoft Teams, OneDrive for Business, Outlook Online, Salesforce, ServiceNow (expanded with a red box), SharePoint Online, and Zoom. The 'ServiceNow' row is expanded, showing a form to 'Enter Tenant ID to onboard ServiceNow'. The form contains a text input field with the URL 'https://developer.service-now.com' (highlighted with a red box) and a 'Submit' button (also highlighted with a red box). Below the form, a note states: 'Onboarding will automatically create web and cloud path probes for this application.'

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

Enter Tenant ID to onboard ServiceNow

Onboarding will automatically create web and cloud path probes for this application.

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 preconfigured probes are displayed. The probes consist of a Cloud Path 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 Cloud Path probe to follow 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.

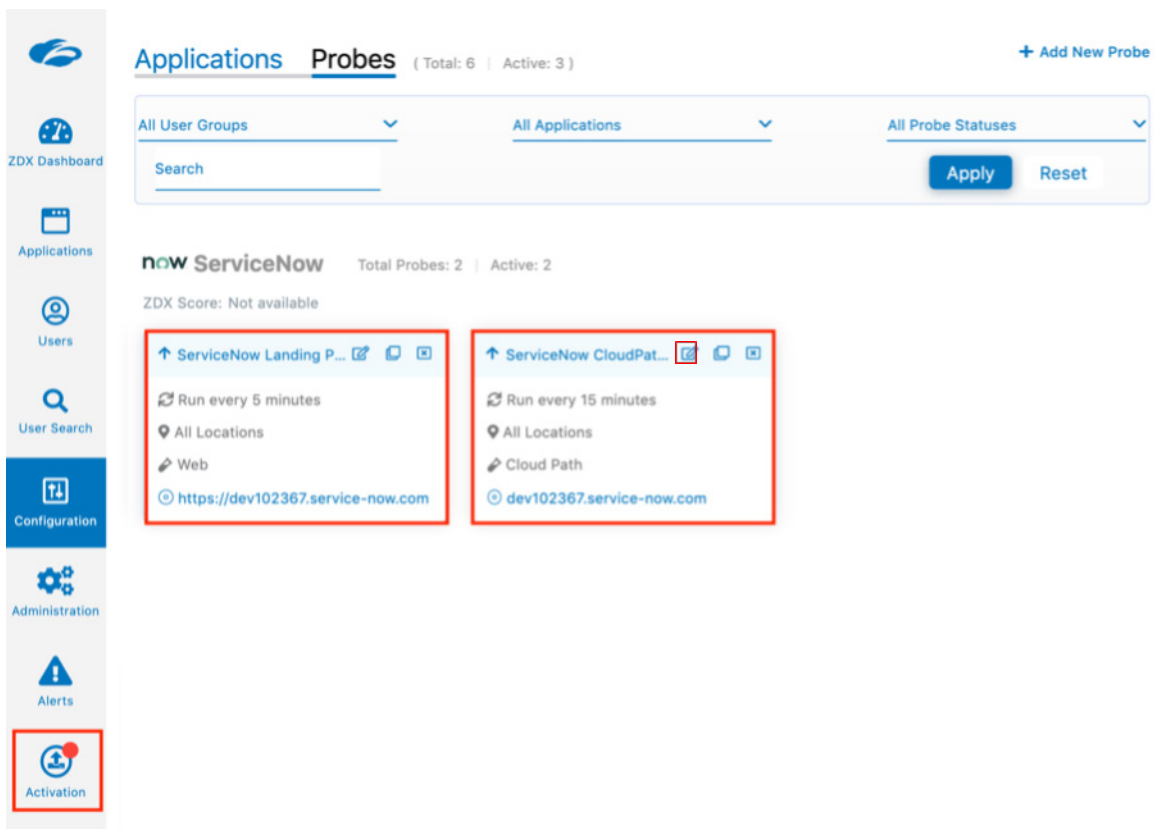


Figure 80. ZDX user experience monitoring for ServiceNow

## Configure Probes for ServiceNow Monitoring

To configure probes for ServiceNow monitoring:

1. For **Follow Web Probe**, select **ServiceNow Landing Page Probe**.
2. Select **Next**.

### Edit ServiceNow CloudPath Probe

1 Configure Probe

2 Additional Parameters

3 Review

#### GENERAL

\* Name

ServiceNow Cloud Path Probe

\* Status

☒ Enable

Disable

\* Application

ServiceNow

\* Probe Type

Cloud Path

Follow Web Probe

ServiceNow Landing Page Probe

\* Run Frequency (minutes)

15

\* Probe Class

☒ Predefined

Custom

#### PROBING CRITERIA

User Groups

Users

Next

Cancel

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.

### Edit ServiceNow CloudPath Probe ✕

1 ✓ Configure Probe

2 ✓ Additional Parameters

3 Review

#### CLOUD PATH PROBE CONFIGURATION

<b>Probe Name</b> ServiceNow Cloud Path Probe	<b>Application Name</b> ServiceNow
<b>* Protocol</b> ICMP <span>🔒</span>	<b>* Packet Count</b> <span>ℹ</span> 11 <span>🔒</span>
<b>* Interval (ms)</b> <span>ℹ</span> 1000	<b>* Timeout (ms)</b> <span>ℹ</span> 1000
<b>* Cloud Path Host</b> <div>dev102367 .service-now.com</div>	

Next

Previous

Cancel

Figure 82. Edit the Cloud Path 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.

### Applications Probes

[+ Add New Custom Application](#)

Predefined Applications (8) ⓘ

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

Private Access

Internet Security

Digital Experience

Notifications

More

Connectivity

Username: toddh@testmypacket.com

Service Status: **ON** [TURN OFF](#)

Authentication Status: **Authenticated**

Server Address: smres.zdxcloud.net

Time Connected: 04/16/2021 12:25:49 PM

ZDX Service Version: 2.0.0.15

Troubleshoot

[Clear ZDX Data](#)

[Restart ZDX Service](#)

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**.

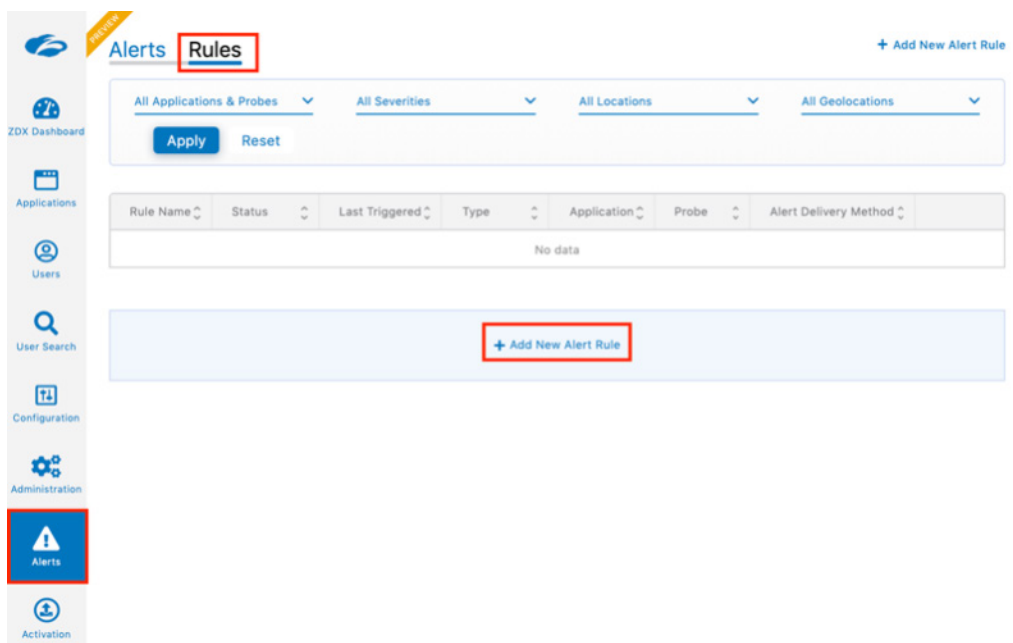


Figure 84. Creating an alert

## 4. Configure Rule:

- a. **Name** the Rule.
- b. Select **Enable** under **Status**.
- c. Give the alert an appropriate severity.
- d. For **Type**, select **Application**.
- e. Click **Next**.

**Add New Alert Rule** [X]

1 **Configure Rule** 2 Filters 3 Criteria 4 Action 5 Review

\* **Name**  
ServiceNow Degradation Alert

\* **Status**  
☒ Enabled ☐ Disabled

\* **Severity**  
High

\* **Type**  
Application

**Next** Cancel

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. For **Locations**, select **All Locations**.
- d. Click **Next**.

**Add New Alert Rule** [X]

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

\* Application  
ServiceNow

\* Web Probe  
ServiceNow Landing Page Probe

Locations  
All Locations

+ Add Filter

**Next** Previous Cancel

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. Enter the time to exceed **5000 ms** (five seconds).
  - c. Click **Next**.

Add New Alert Rule

1 Configure Rule

2 Filters

3 Criteria

4 Action

5 Review

ALL

—

Page Fetch Time

≥

5000

ms

+ ADD

Expression

Show Preview

Next

Previous

Cancel

Figure 87. The Alert Creation wizard step 3

7. Add throttling to control the scope of the alert. Then define the action as email. You can also define the action 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. Enter 10 for the **Percentage** for the **Minimum Devices Impacted**.
  - c. Select **Email** as the **Alert Delivery Method**.
  - d. Enter the **Alert Recipients** email addresses separated by commas.
  - e. Click **Next**.

**Add New Alert Rule** [X]

1 Configure Rule 2 Filters 3 Criteria 4 Action 5 Review

**THROTTLING**

\* Alert Only if Repeated  Times in a Row

\* Minimum Devices Impacted

☒ **Percentage**

\* In Group

[v]

**ACTION**

Muted

☐ [X]

\* Alert Delivery Method

[X] [v]

\* Alert Recipients

[Add]

Figure 88. The Alert Creation wizard step 4

The completed rule set for the alert:

**Alerts Rules** [+ Add New Alert Rule](#)

All Applications & Probes All Severities All Locations All Geolocations

[Apply](#) [Reset](#)

Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method	
> ServiceNow D...	Enabled	-	Application	ServiceNow	ServiceNow L...	Email	<a href="#">Edit</a> <a href="#">Alerts</a> <a href="#">Delete</a>

[+ Add New Alert Rule](#)

**Activation**

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.

The screenshot displays the Zscaler Alerts management interface. On the left is a sidebar with navigation options: ZDX Dashboard, Applications, Users, User Search, Configuration, Administration, Alerts (highlighted with a red box), and Activation. The main content area is titled 'Alerts' with a 'Rules' tab. A '2 Hours' filter is applied. Below the filter are four summary cards: 'ONGOING ALERTS' (1), 'ALERT HISTORY' (0), 'IMPACTED DEVICES' (1), 'IMPACTED GEOLOCATIONS' (1), and 'IMPACTED APPLICATIONS' (1). The 'Ongoing' tab is selected, showing a table with one alert. The alert is highlighted with a red border.

Severity	Rule Name	Type	Impacted ...	Impacted Ge...	Impacted ...	Started On	Ended On	
●	<a href="#">ServiceNow Degradation Alert</a>	Application	ServiceNow	1 Geolocations	1 Devices	Apr 16, 2021 12:55:00 PM CDT	Ongoing	<a href="#">View</a>

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.

**Alerts** | Started On: Apr 16, 2021 12:55:00 PM CDT | Ended On: **Ongoing** | Application: **ServiceNow**

**#6951820390129902722 | ServiceNow Degradation Alert**

All Devices | All Departments | All Locations | All Geolocations | All Device OS Versions | **Apply** | **Reset**

TOP DEPARTMENTS	TOP GEOLOCATIONS	TOP ZSCALER LOCATIONS
Number of Devices per Department	Number of Devices per Geolocations	Number of Devices per Locations
1   <b>Biz Dev</b>	1   <b>Spring, Texas, US</b>	1   <b>Road Warrior</b>

**Expression Triggers**

( Page Fetch Time >> 500ms )

Average 878 ms | Maximum: 878 ms

**Impacted Geolocations (1)**

Map showing impacted geolocations in Texas and Louisiana. A red dot indicates the location of the impacted device in Spring, Texas, US.

**Impacted Devices (1)**

Device	User ID	Department	Zscaler Location	Geolocation
toddh (Apple MacPro5,1 Version ...)	Toddh (toddh@testmypacke...)	Biz Dev	Road Warrior	Spring, Texas, US

Figure 91. Alert details



## The Sent Alert Email for the ServiceNow Service

The following email alert is 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.

no-reply@zscaler.com

ZDX Alert# 6951820390129902722 Started

To: Todd Harcourt

Inbox - Zscaler

1:13 PM

N

☐ 2021-Apr-16 18:13 UTC

6951820390129902722

Alert Criteria Triggers

(Page Load Time >= 500 ms) avg = 878.22ms | max = 878.22ms | min = 878.22ms

Alert Timeline

☐ 2021-Apr-16 17:55 UTC

☐ Ongoing

Alert Rule

ServiceNow Degradation Alert ☐

Alert Severity

☒ High

Impacted

☐ 1 Geolocations

☐ 1 Departments

☐ 1 OS Versions

☐ 1 Devices

View 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.

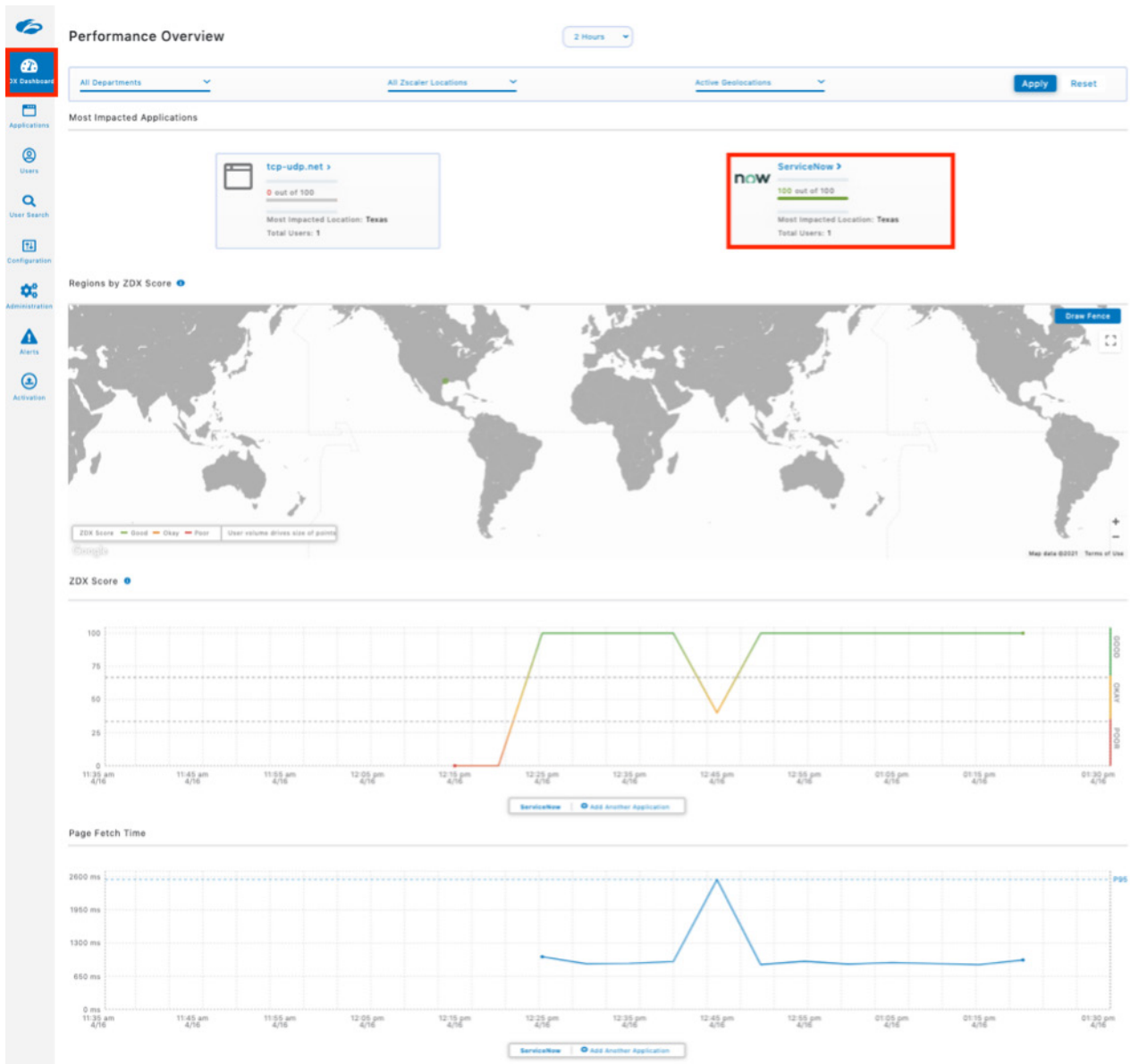


Figure 93. The ZDX Dashboard

## Applications 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.

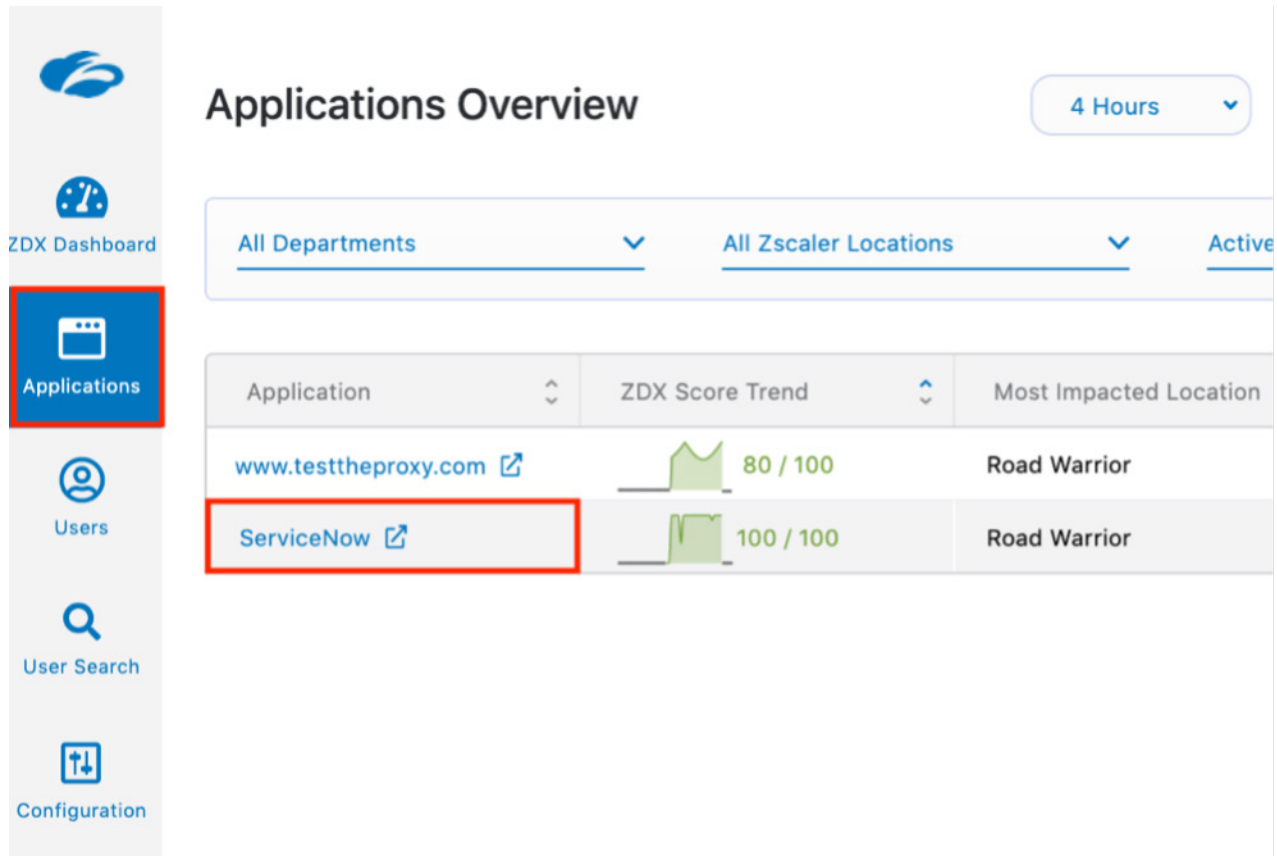


Figure 94. Applications overview

## 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.

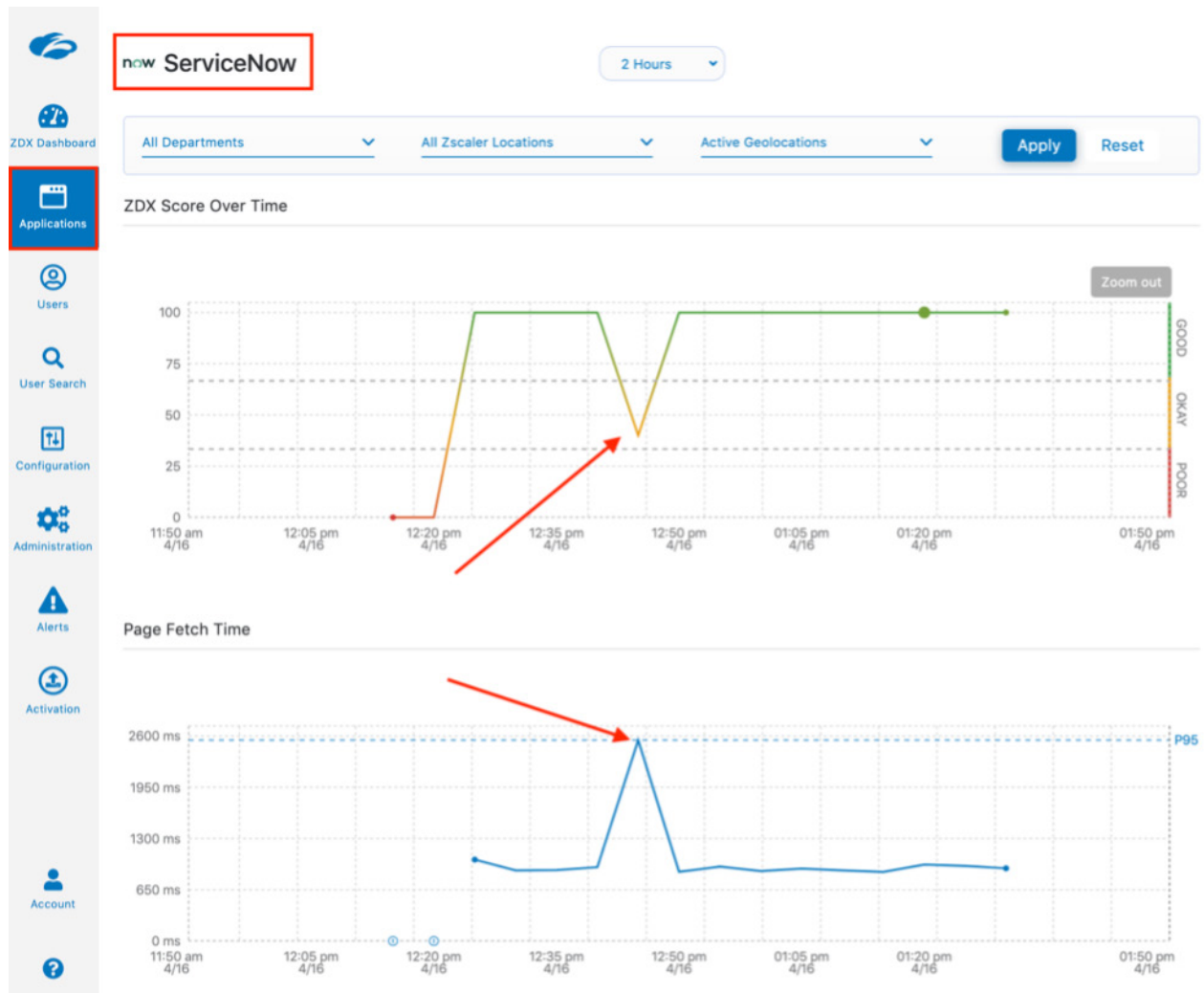


Figure 95. Application details

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

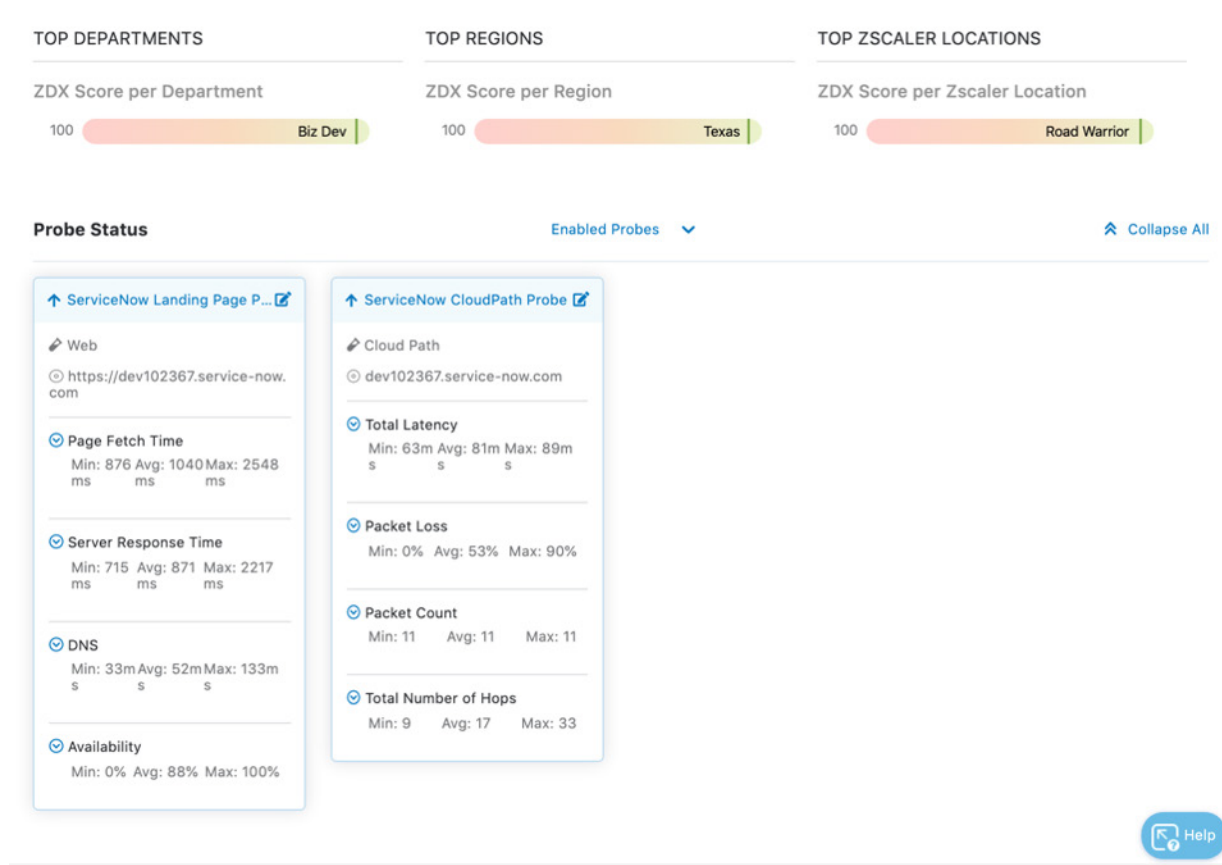


Figure 96. Application details

## 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 a Poor, Okay, or Good ZDX Score. You can see more detail on the user by clicking the user name or the View icon on the right. Select a user to display more detail.

**User Overview** 2 Hours

ServiceNow X ▼ All Departments ▼ All Zscaler Locations ▼

Active Geolocations ▼ All Users ▼ Apply Reset

**TOTAL ACTIVE USERS**  
1 0% 📊 ℹ️

**TOTAL ACTIVE DEVICES**  
1 0% 📊 ℹ️

**ZDX SCORE USER DISTRIBUTION** ℹ️

0 Poor 0 Okay 1 Good

Poor Okay Good

User	ZDX Score	Zscaler Locations	Geolocations	Devices	
Toddh (toddh@te...)	<span>100 / 100</span>	Road Warrior	Texas	toddh (Apple Ma...)	<span>👁️</span> <span>✎️</span> <span>👤</span>

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 User 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.

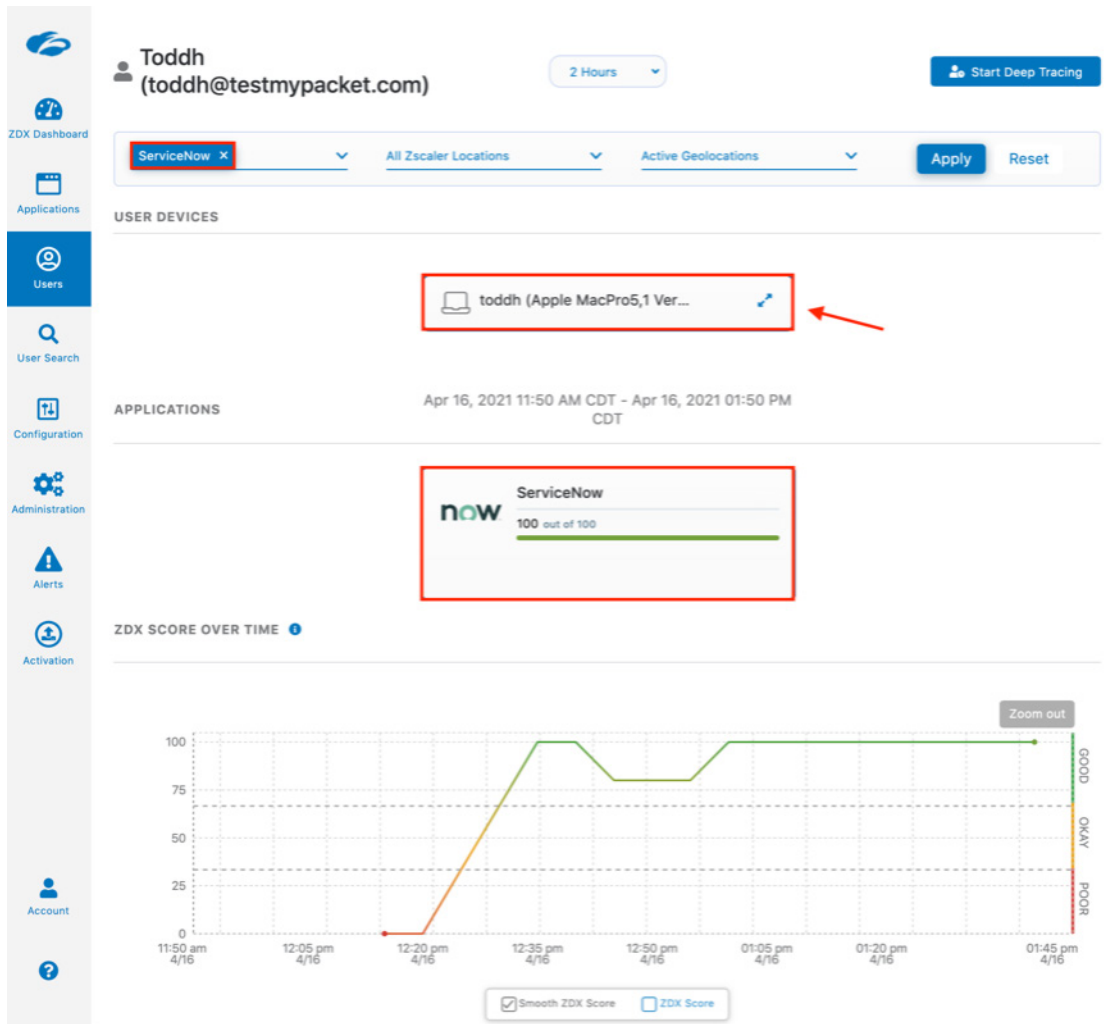


Figure 98. User detail

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)

The following image shows the Command Line View.

	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 ServiceNow 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 an 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**, enter Applications.
3. Click **All**.
4. In the search bar, enter Zscaler Digital Experience.
5. Click **Install**. After the installation is complete, the browser window automatically reloads.

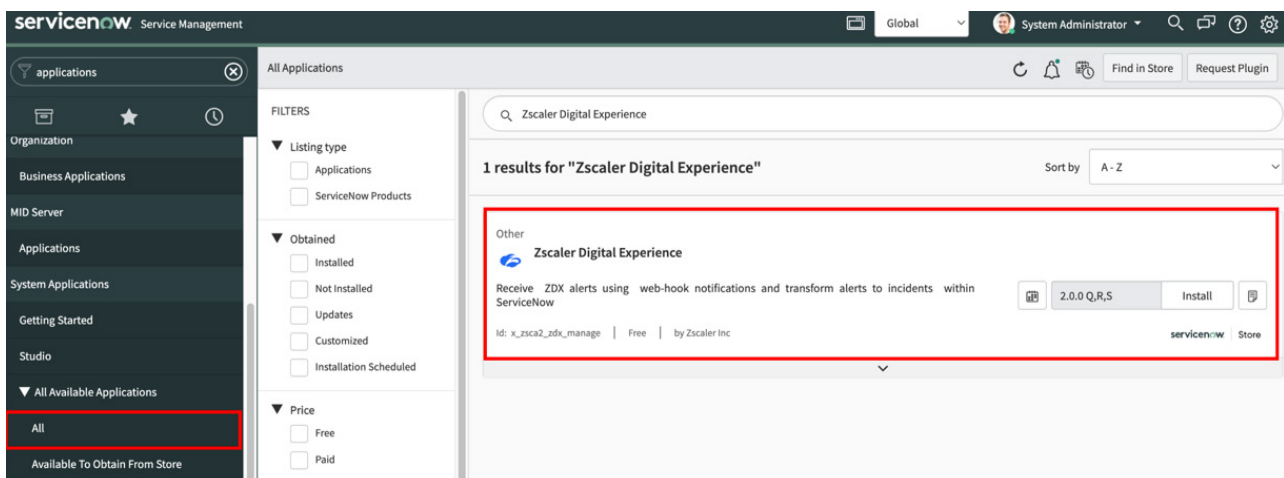


Figure 101. Install ZDX ServiceNow App

## 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. Log in as administrator to the ServiceNow instance.
2. In the **Filter Navigator**, enter `sys_user.list`.

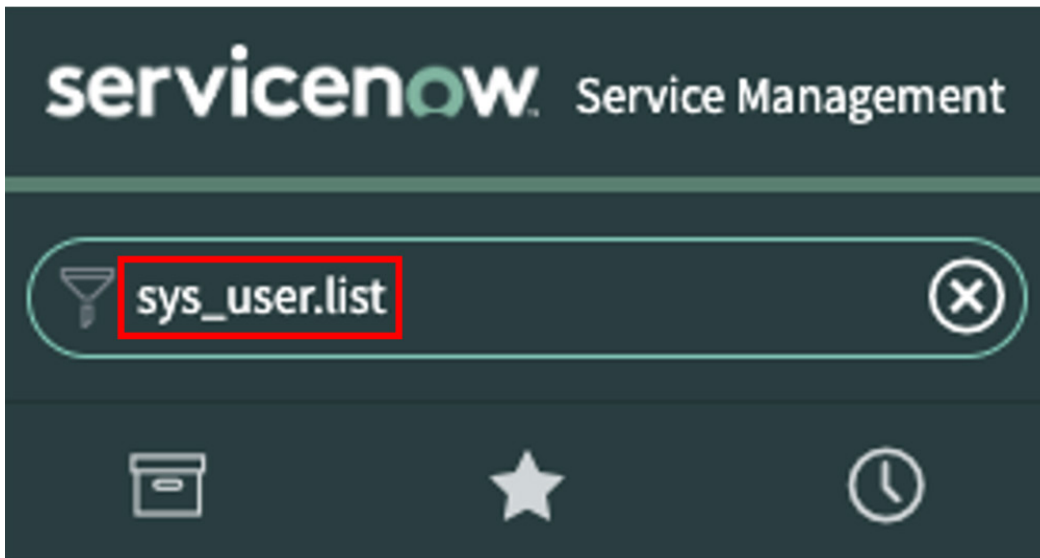


Figure 102. Filter type `sys_user.list`

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

 A screenshot of the ServiceNow 'New User' form. The form is divided into two columns. The left column contains fields for 'User ID' (filled with 'zdx\_snow' and circled with a red box and a blue '1'), 'First name' (filled with 'Zscaler'), 'Last name' (filled with 'Digital Experience'), 'Title' (empty), 'Department' (empty with a search icon), 'Password' (filled with '\*\*\*\*\*' and circled with a red box and a blue '2'), 'Password needs reset' (checkbox), 'Locked out' (checkbox), 'Active' (checkbox with a checkmark), and 'Web service access only' (checkbox with a checkmark, circled with a red box and a blue '3'). The right column contains fields for 'Email' (filled with 'zdx\_snow@securitygeek.io'), 'Language' (dropdown set to 'English'), 'Calendar integration' (dropdown set to 'Outlook'), 'Time zone' (dropdown set to 'System (America/Los\_Angeles)'), 'Date format' (dropdown set to 'System (yyyy-MM-dd)'), 'Business phone' (empty), 'Mobile phone' (empty), and 'Photo' (text 'Click to add...').

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.

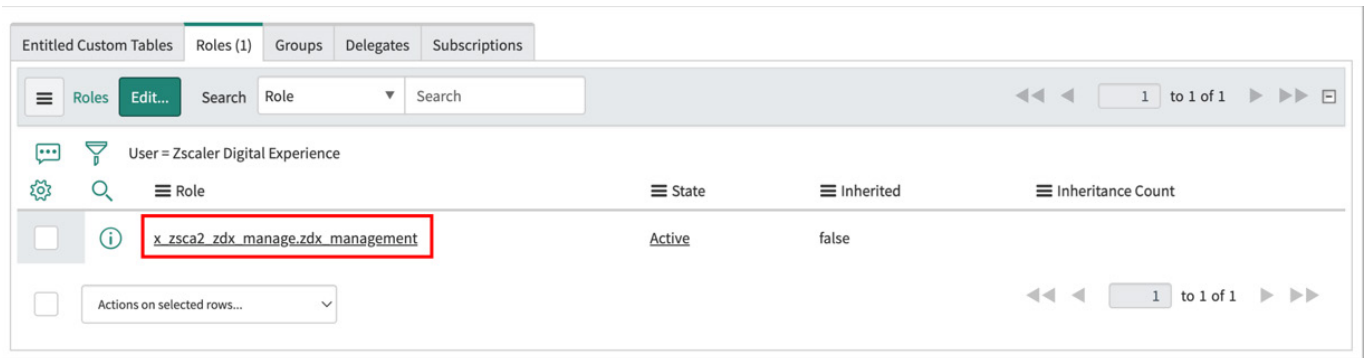


Figure 104. ServiceNow User Role

## Configure the ZDX ServiceNow Application

To configure the ZDX ServiceNow application:

1. Enter Zscaler Digital Experience in the **Filter Navigator**.
2. Select **Setup**.

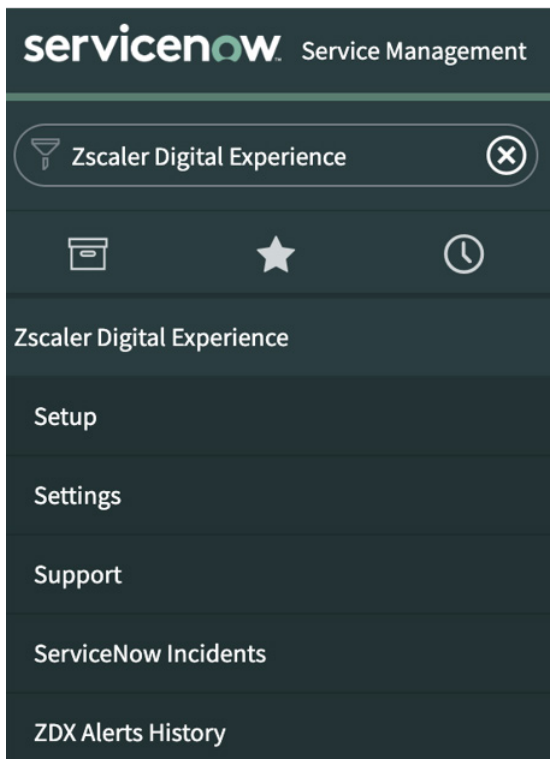


Figure 105. Find ZDX in ServiceNow

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

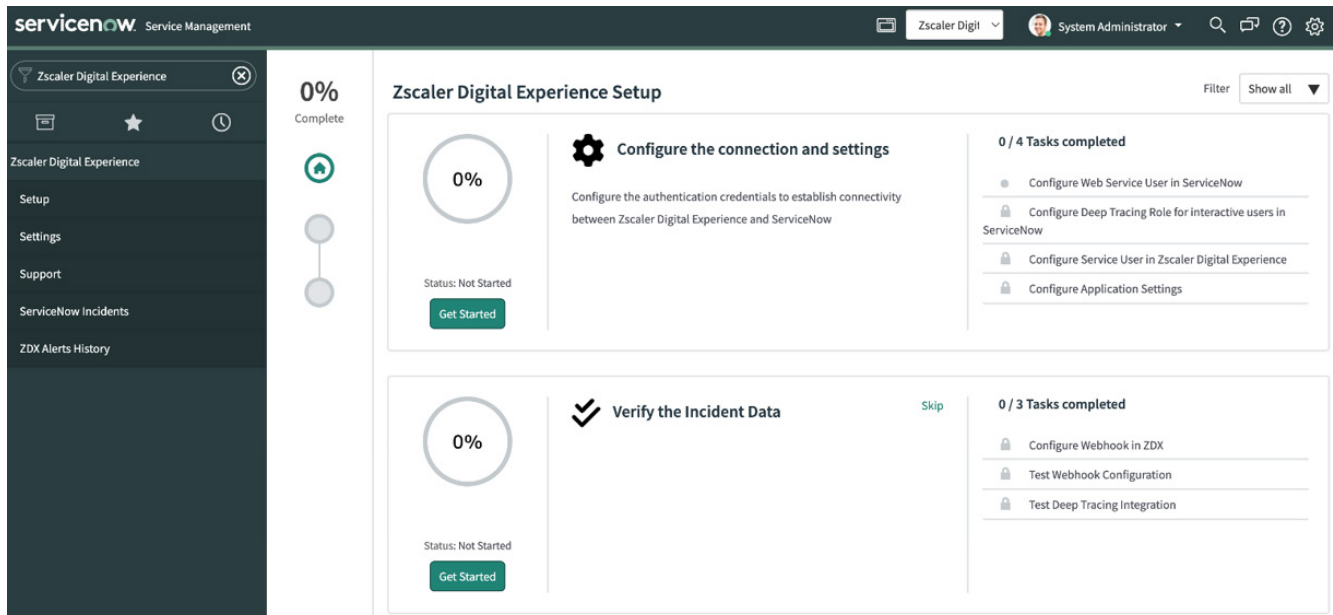


Figure 106. Set up ZDX

## Configure Deep Tracing Role for Interactive Uses in ServiceNow

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

- Go to **All > User Administration > Users** and then open a user record.
- In the **Roles** related list, click **Edit**.
- In the **Collection** list, select the `x_zsca2_zdx_manage.zdx_dt_management` role and assign it to the targeted user.
- 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. The following 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.

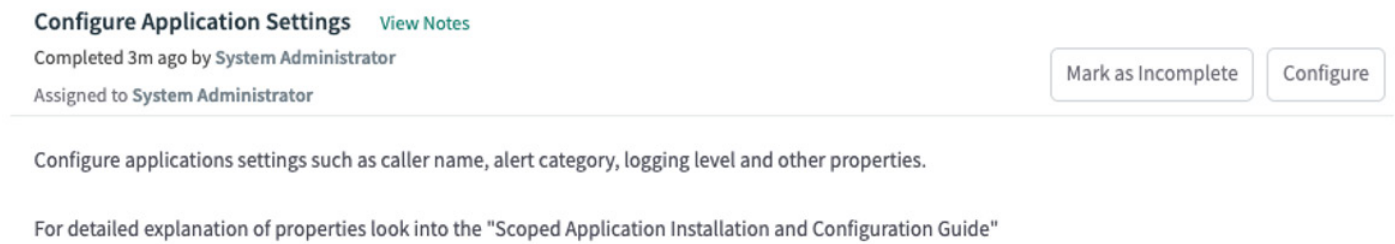
Permission Name	Required Value
Deep Tracing	Full
Webhooks	Full
User and Device Names	Visible
Configuration Access	Full
Alerts	Full
UCaaS Monitoring	View Only

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 the **Password Based Login** option and enter a 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**.



**Configure Application Settings** [View Notes](#)

Completed 3m ago by System Administrator

Assigned to System Administrator

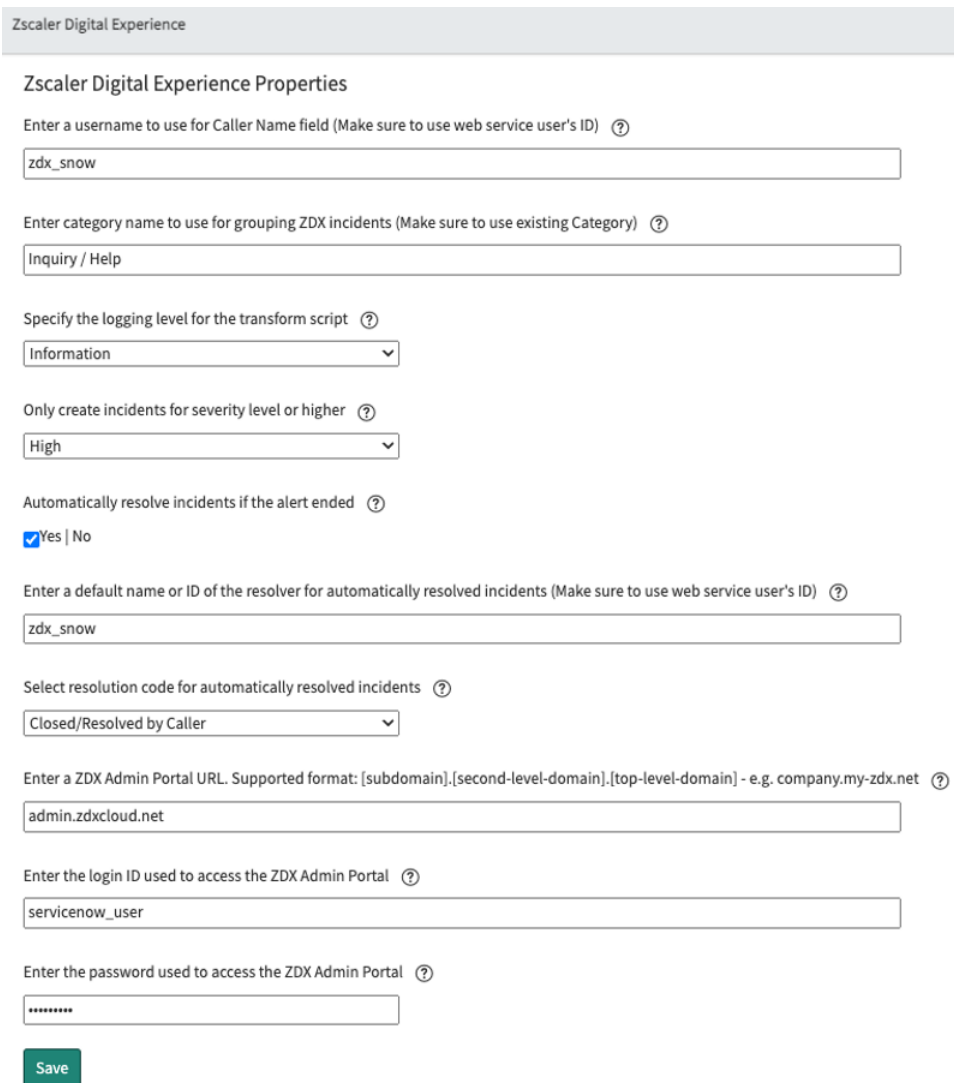
Mark as Incomplete Configure

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

For detailed explanation of properties look into the "Scoped Application Installation and Configuration Guide"

Figure 107. Configure Application Settings

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



Zscaler Digital Experience

### Zscaler Digital Experience Properties

Enter a username to use for Caller Name field (Make sure to use web service user's ID) ?

zdx\_snow

Enter category name to use for grouping ZDX incidents (Make sure to use existing Category) ?

Inquiry / Help

Specify the logging level for the transform script ?

Information

Only create incidents for severity level or higher ?

High

Automatically resolve incidents if the alert ended ?

☒ Yes | No

Enter a default name or ID of the resolver for automatically resolved incidents (Make sure to use web service user's ID) ?

zdx\_snow

Select resolution code for automatically resolved incidents ?

Closed/Resolved by Caller

Enter a ZDX Admin Portal URL. Supported format: [subdomain].[second-level-domain].[top-level-domain] - e.g. company.my-zdx.net ?

admin.zdxcloud.net

Enter the login ID used to access the ZDX Admin Portal ?

servicenow\_user

Enter the password used to access the ZDX Admin Portal ?

\*\*\*\*\*

Save

Figure 108. Configure ZDX properties

## Configure ZDX Webhook in ZDX

To configure ZDX to perform Webhook calls into ServiceNow:

1. Log in as administrator to the ZDX Admin Portal.
2. From the left-side navigation, select **Administration** > **Webhooks**. You are redirected to the **Webhooks** windows.
3. 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. Enter the user credentials.
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, 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
<input type="checkbox"/>	<a href="#">INC0010001</a>	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
<input type="checkbox"/>	<a href="#">INC0010002</a>	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 the target Incident record.
4. Select the **Deep Tracing** tab.

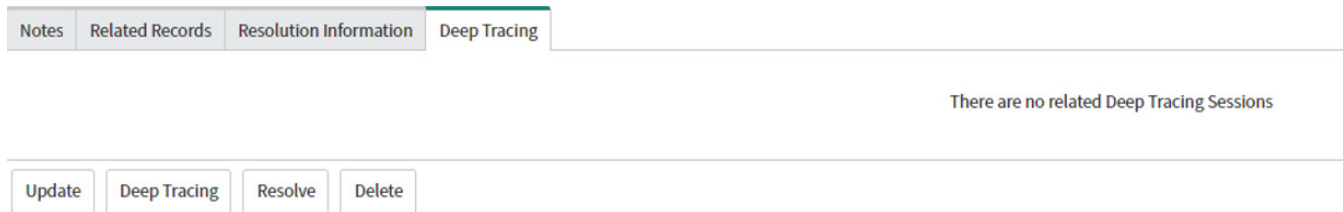


Figure 111. Deep Tracing Sessions

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

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 following steps:

- 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. Log in as administrator to the ServiceNow instance.
2. In the **Filter Navigator**, enter `sys_user.list`.

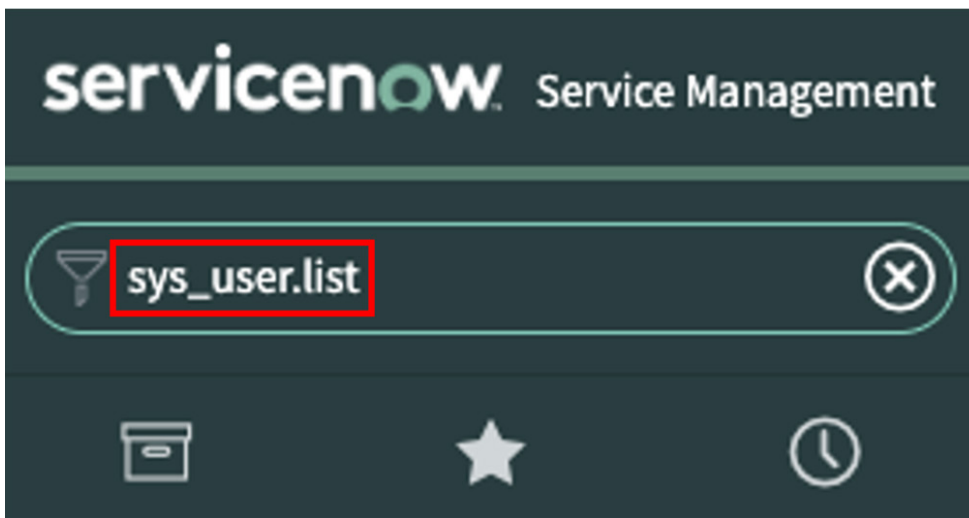
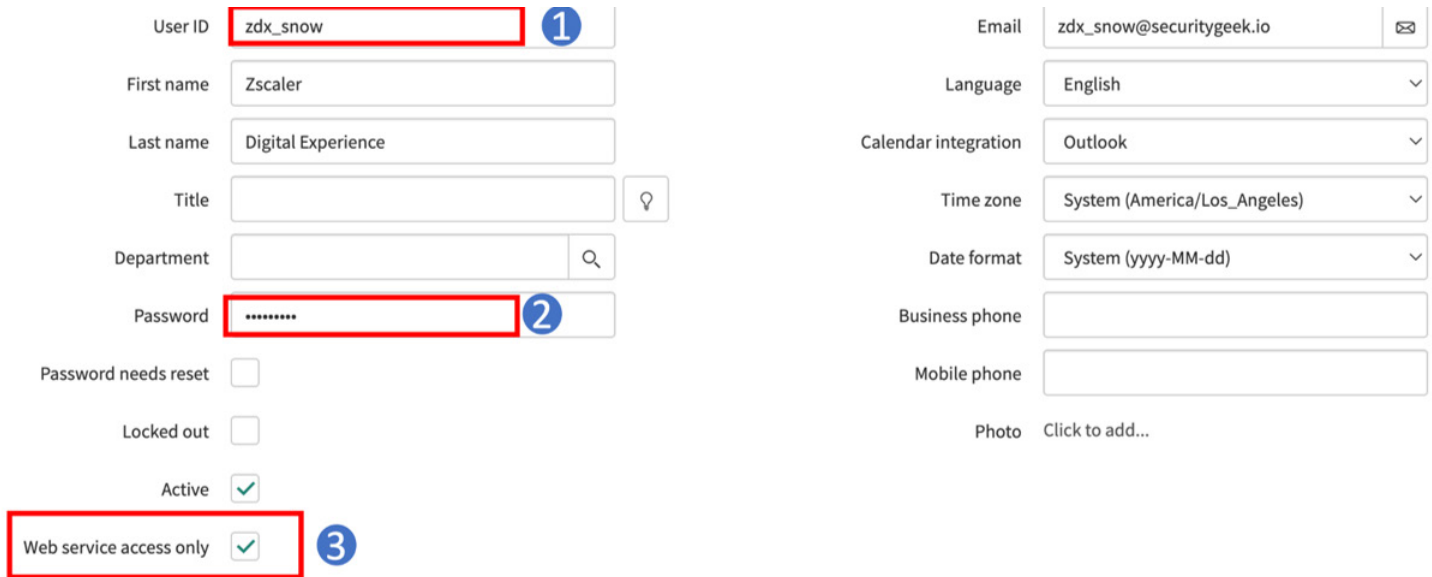


Figure 112. Filter type `sys_user.list`

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



User ID	<input type="text" value="zdx_snow"/>	1
First name	<input type="text" value="Zscaler"/>	
Last name	<input type="text" value="Digital Experience"/>	
Title	<input type="text"/>	
Department	<input type="text"/>	
Password	<input type="password" value="*****"/>	2
Password needs reset	<input type="checkbox"/>	
Locked out	<input type="checkbox"/>	
Active	<input checked="" type="checkbox"/>	
Web service access only	<input checked="" type="checkbox"/>	3

Email	<input type="text" value="zdx_snow@securitygeek.io"/>	
Language	<input type="text" value="English"/>	
Calendar integration	<input type="text" value="Outlook"/>	
Time zone	<input type="text" value="System (America/Los_Angeles)"/>	
Date format	<input type="text" value="System (yyyy-MM-dd)"/>	
Business phone	<input type="text"/>	
Mobile phone	<input type="text"/>	
Photo	<input type="text" value="Click to add..."/>	

Figure 113. Configure service account

## Configure ZPC and ServiceNow Integration

To configure the ServiceNow ticketing system integration:

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

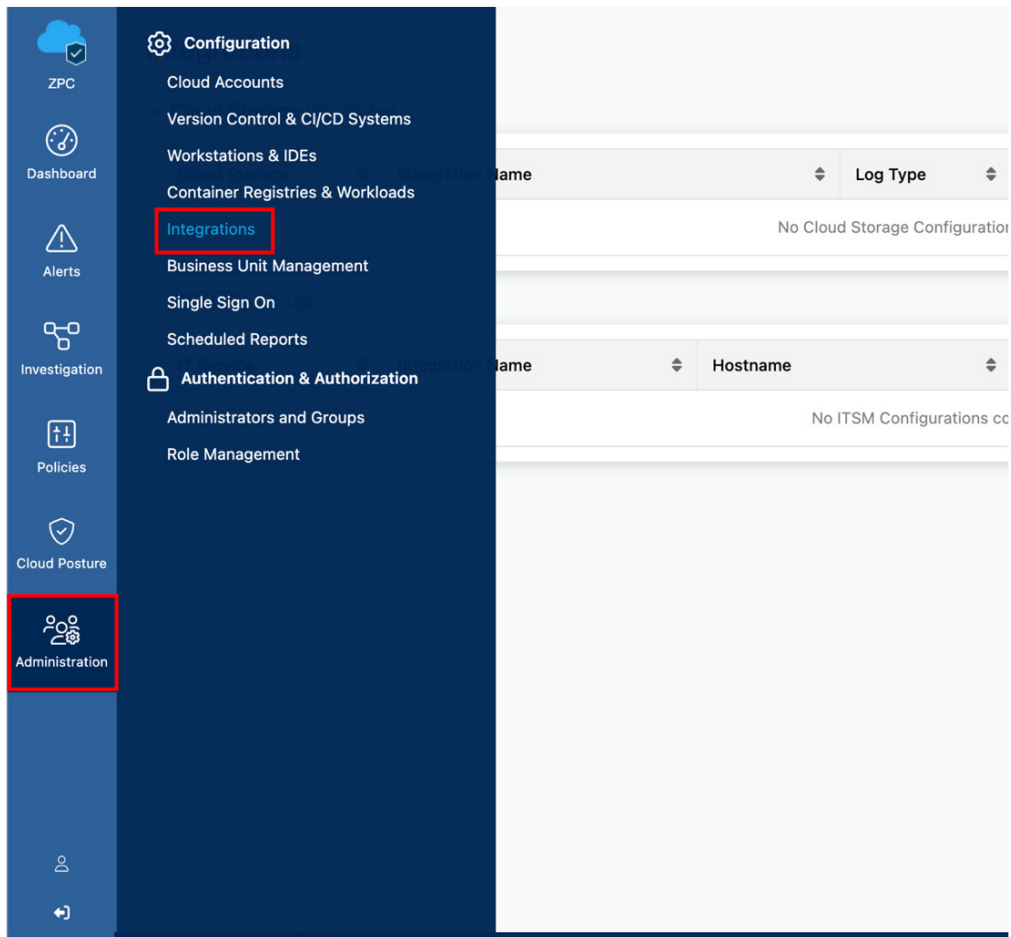


Figure 114. ZPC Integrations

## ZPC ServiceNow ITSM Configuration

On the Integrations page:

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

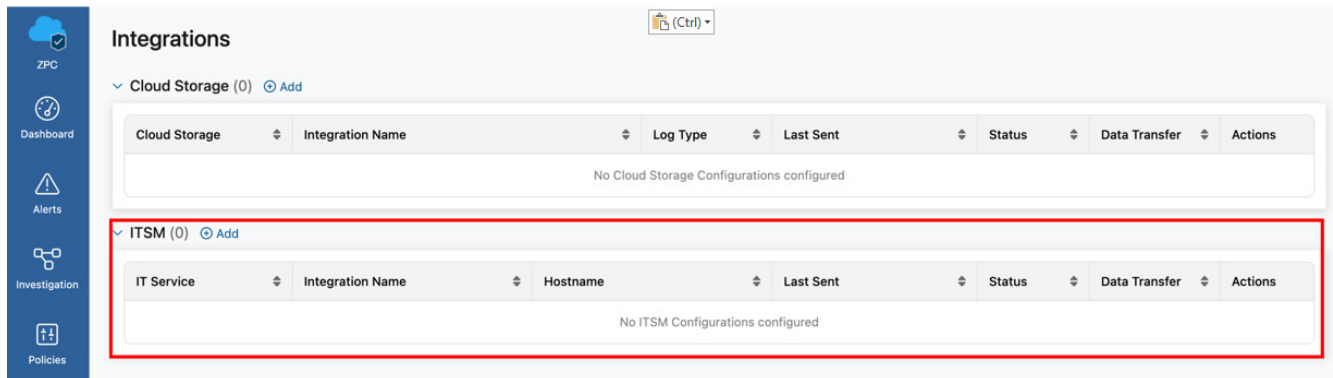


Figure 115. ZPC ITSM Integrations

2. For **Integration Name**, enter a name. After the installation is complete, the browser window automatically reloads.
3. Select **ServiceNow**.
4. Click **Next**. The **Add ITSM Details** window displays.

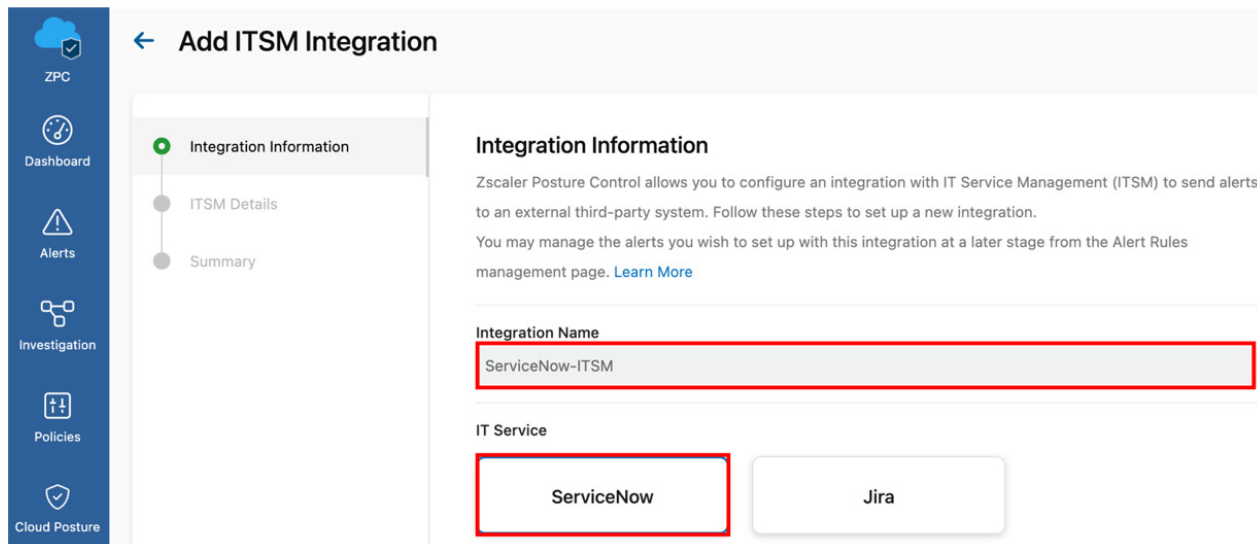


Figure 116. Add ITSM Integration

5. For the **ServiceNow Hostname**, enter the ServiceNow instance ID.
6. For the **ServiceNow Username**, enter the ServiceNow account with rights to create incidents.
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**.

**Add ITSM Integration**

Integration Information

ITSM Details

Summary

**ITSM Details**

Please add your ServiceNow login credentials in order to connect to: **ServiceNow-ITSM (ServiceNow)**.

Authenticate your login credentials before proceeding. [ServiceNow Troubleshooting](#)

**ServiceNow Hostname**

dev114567 .service-now.com

**ServiceNow Username**

zpc\_snow

**ServiceNow Password**

.....

[Reset Validation](#)

ServiceNow Credentials have been validated.

Figure 117. ITSM Details

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

**Add ITSM Integration**

Integration Information

ITSM Details

Summary

**Summary**

Please confirm your new ITSM integration settings.

Integration Information

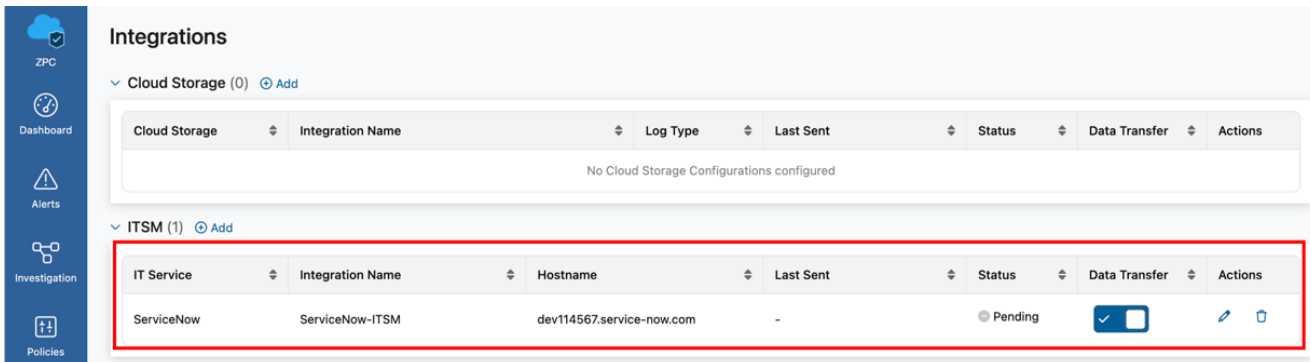
Integration Name	ServiceNow-ITSM
IT Service	ServiceNow

ITSM Details

ServiceNow Hostname	dev114567.service-now.com
ServiceNow Username	zpc_snow
ServiceNow Password	.....

Figure 118. ITSM Summary

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



**Integrations**

Cloud Storage (0) [Add](#)

Cloud Storage	Integration Name	Log Type	Last Sent	Status	Data Transfer	Actions
No Cloud Storage Configurations configured						

ITSM (1) [Add](#)

IT Service	Integration Name	Hostname	Last Sent	Status	Data Transfer	Actions
ServiceNow	ServiceNow-ITSM	dev114567.service-now.com	-	Pending	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

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:

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

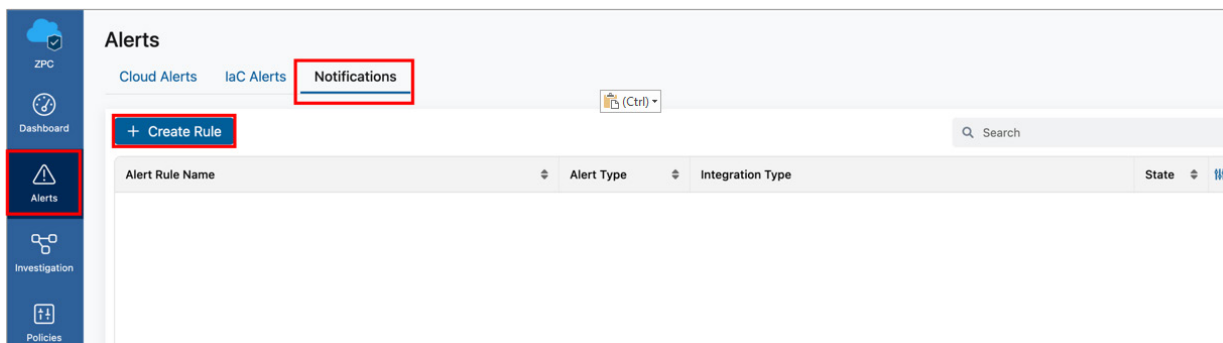


Figure 120. Alerts Notifications

## ZPC: Create A Cloud Notification Rule

To create a cloud notification rule:

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

**Add Alert Rule**

**General Information**  
Alert Rule allows to selectively send alerts to the Notification Channels.

**Alert Rule Name**  
AWS-Alert-Notification

**Alert Type**  
☒ Cloud ☐ IaC

**Alert Rule Status**  
☒ ☐

Figure 121. Add Alert Rule

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

**Add Alert Rule**

**Scope**  
Select the scope you wish to receive notifications for, you may filter the scope for Cloud Accounts or Business Units.

Business Units Clouds Accounts Regions +

**Select Policy**  
Alerts of selected policies will be sent to the Notification Channels.

Compliance Severity Threat Category Policy Type Search

Policy	Threat Category	Policy Type	Severity	Compliance	Cloud
<input type="checkbox"/> EC2 instances with role...	Service Misconfigu...	Predefined	Medium	-	<input checked="" type="checkbox"/>
<input type="checkbox"/> Unused Access keys fo...	Dormant Accounts	Predefined	High	-	<input checked="" type="checkbox"/>
<input type="checkbox"/> Ensure the S3 bucket u...	-	Predefined	Medium	CSA CCM v4.0.1, General Data Pro...	<input checked="" type="checkbox"/>
<input type="checkbox"/> Ensure no Network AC...	-	Predefined	High	CSA CCM v4.0.1, General Data Pro...	<input checked="" type="checkbox"/>
<input type="checkbox"/> Publicly-exposed EC2 I...	External Exposure	Predefined	Critical	-	<input checked="" type="checkbox"/>
<input type="checkbox"/> Ensure EBS Volume En...	-	Predefined	High	CSA CCM v4.0.1, General Data Pro...	<input checked="" type="checkbox"/>

Rows per page: 10 1-10 of 227

Back 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 where you'd like notifications to be sent when an incident is closed or resolved in ServiceNow. The following options are available:
  - **Send Notifications for closed Alerts**
  - **Send Notifications for resolved Alerts**
11. Click **Next**.

**Edit Alert Rule**

**Notifications**  
Alerts will be sent to the selected Notification Channels.

**Messaging**

☐ Email

**ITSM/Ticketing**

☒ ServiceNow

ServiceNow-ITSM

**Assignee**

zpc\_snow@zscaler.com

☒ Send Notifications for closed Alerts

☒ Send Notifications for resolved Alerts

☐ JIRA

**Cloud Storage**

☐ AWS S3

☐ Azure Blob

Cancel Back **Next** Help

Figure 123. Edit Alert Rule

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

**Edit Alert Rule**

**Review**

General Information

Alert Rule Name: AWS-Alert-Notification

Alert Type: Cloud

Alert Rule Status: ENABLED

Resource Scope

Business Unit: 6 Selected

Cloud Service Provider: All Selected

Account: All Selected

Regions: All Selected

Policies: All Policies Selected

Notifications

Messaging: Not Configured

ITSM/Ticketing: ServiceNow

Cloud Storage: Not Configured

Figure 124. Review Alert Rule



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

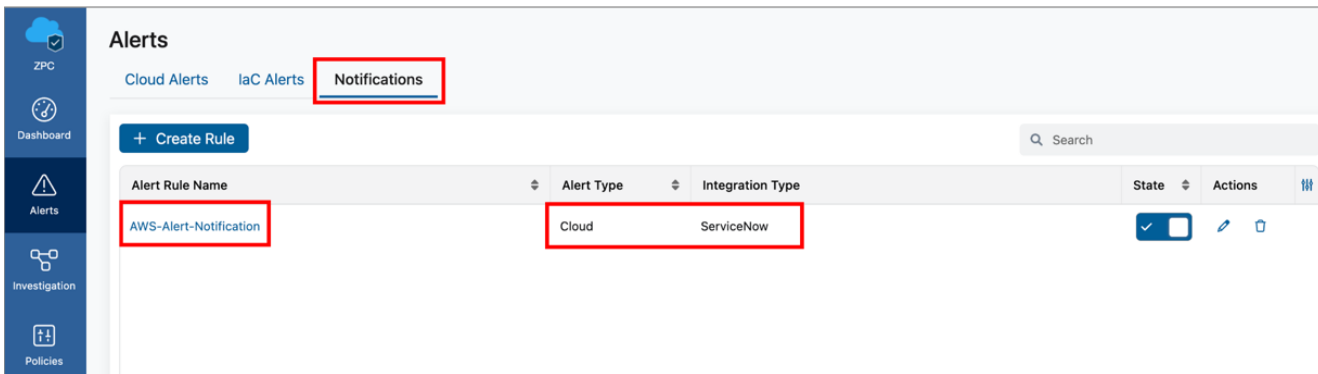


Figure 125. Alert in Notifications

## ZPC: Create IaC Notification Rule

To create an IaC notification rule:

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

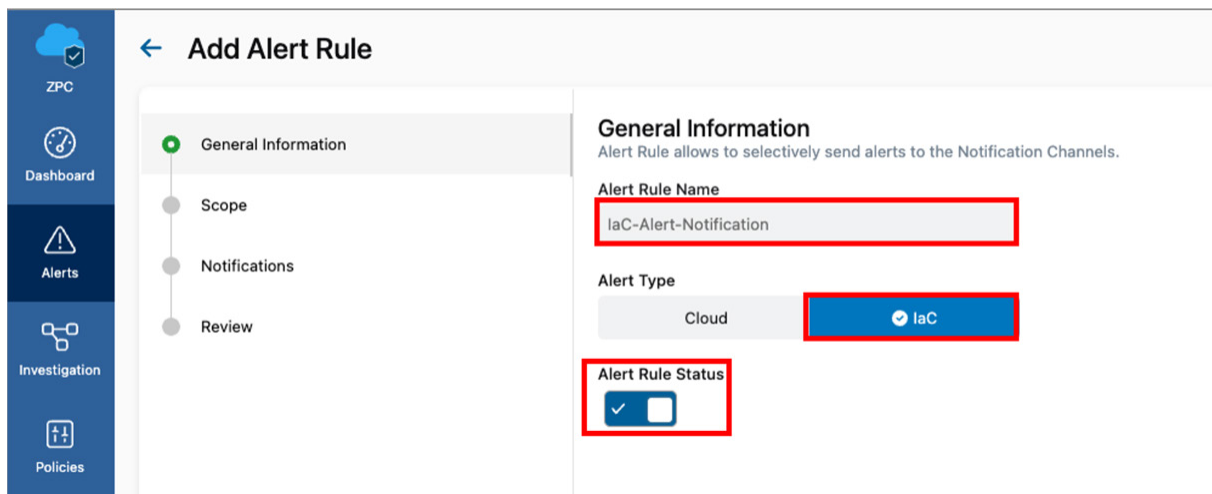


Figure 126. General Information

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:
  - **GitHub Actions**
  - **Jenkins**
  - **GitLab**
  - **Azure Pipelines**
  - **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:

- CIS (Center for Internet Security)
- CSA CCM (CSA Cloud Controls Matrix)
- HIPAA
- ISO-IEC 27001
- NIST SP 8000
- PCI DSS 3.2.1
- SOC 22
- Zscaler Best Practices

**Add Alert Rule**

**Scope**  
Select the scope you wish to receive notifications for, you may filter the scope for Cloud Accounts or Business Units.

Business Units Clouds Accounts Regions +

**Select Policy**  
Alerts of selected policies will be sent to the Notification Channels.

Compliance Severity Threat Category Policy Type Search

Policy	Threat Category	Policy Type	Severity	Compliance	Cloud
EC2 instances with role...	Service Misconfigu...	Predefined	Medium	-	AWS
Unused Access keys fo...	Dormant Accounts	Predefined	High	-	AWS
Ensure the S3 bucket u...	-	Predefined	Medium	CSA CCM v4.0.1, General Data Pro...	AWS
Ensure no Network AC...	-	Predefined	High	CSA CCM v4.0.1, General Data Pro...	AWS
Publicly-exposed EC2 i...	External Exposure	Predefined	Critical	-	AWS
Ensure EBS Volume En...	-	Predefined	High	CSA CCM v4.0.1, General Data Pro...	AWS

Rows per page: 10 1-10 of 227

Back Next

Help

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 where you'd like notifications to be sent when an incident is closed or resolved in ServiceNow. The following options are available:
  - **Send Notifications for closed Alerts**
  - **Send Notifications for resolved Alerts**
12. Click **Next**.
13. Click **Finish**.

**Edit Alert Rule**

General Information

Scope

Notifications

Review

**Notifications**

Alerts will be sent to the selected Notification Channels.

**Messaging**

☐ Email

**ITSM/Ticketing**

☒ ServiceNow

ServiceNow-ITSM

**Assignee**

zpc\_snow@zscaler.com

☒ Send Notifications for closed Alerts

☒ Send Notifications for resolved Alerts

☐ JIRA

**Cloud Storage**

☐ AWS S3

☐ Azure Blob

Cancel

Back

Next

Help

Figure 128. Alert Rule Notifications

Alerts are displayed in the Notifications window.

**Alerts**

Cloud Alerts   IaC Alerts   Notifications

+ Create Rule

Search

Alert Rule Name	Alert Type	Integration Type	State	Actions
AWS-Alert-Notification	Cloud	ServiceNow	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
IaC-Alert-Notification	IaC	ServiceNow	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

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 (you can apply additional customization):

- 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.

Incident Number	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
INC0010119	EC2 instances with role has IMDSv1 enabled	Zscaler Posture Control	Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:45:01	zpc_snow
INC0010392	EC2 instance is open to all IP ranges	Zscaler Posture Control	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2022-11-22 00:27:21	zpc_snow
INC0010174	EC2 instances with role has IMDSv1 enabled	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:45:13	zpc_snow
INC0010095	EC2 instance with exposed management ports	Zscaler Posture Control	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2022-11-21 00:19:28	zpc_snow
INC0010349	Ensure S3 Bucket Policy allows HTTPS requests	Zscaler Posture Control	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:56:58	zpc_snow
INC0010343	Ensure VPC flow logging is enabled in all VPCs	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:57:02	zpc_snow
INC0010485	EC2 instances with role has IMDSv1 enabled	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-22 01:44:41	zpc_snow
INC0010203	Ensure VPC flow logging is enabled in all VPCs	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:56:49	zpc_snow
INC0010205	Ensure that S3 Buckets are configured with 'Block public access (bucket settings)'	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:56:49	zpc_snow
INC0010213	Ensure VPC flow logging is enabled in all VPCs	Zscaler Posture Control	4 - Low	New	Inquiry / Help	(empty)	(empty)	2022-11-21 01:56:50	zpc_snow

Figure 130. ServiceNow Incidents page

## Contextualizing Risk Using ServiceNow and Avalor UVM

Avalor's Data Fabric and Unified Vulnerability Management (UVM) solution integrates, normalizes, and unifies data from various enterprise security and business systems to provide actionable insights, analytics, and operational efficiencies.

Avalor offers preconfigured integrations for the following ServiceNow services, which can be added as:

- Connectors:
  - ServiceNow Generic: Allows you to retrieve any table from ServiceNow.
  - ServiceNow Assets: Retrieves computer assets from ServiceNow. The assets are retrieved from the following tables: cmdb\_ci\_computer, cmdb\_ci\_server, cmdb\_ci\_vm\_instance.
  - ServiceNow Users: Retrieves user data from the sys\_user tables and enrich every row with data from cmn\_department.
- Outegrations:
  - ServiceNow: Allows you to create a ServiceNow Incident, Request, Remediation Task or Task from an Avalor Ticket, Asset, Incident, Alert, or Finding.

The following steps outline how to start ingesting data from these sources, while also (optionally) combining ServiceNow Asset data with Avalor vulnerability information to provide a more contextualized and personalized risk assessment for your organization.

### Configuring the ServiceNow Tenant for OAuth 2.0

Check if the OAuth 2.0 Application is installed and active:

1. Log in to ServiceNow with Administrator credentials.
2. Verify OAuth 2.0 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. In the **All Applications** page:
  - a. In the search box, enter `OAuth 2.0`.
  - b. Verify OAuth is installed.

4. If OAuth 2.0 is not installed:
  - a. Select **Install**.
  - b. Select **Activate**.

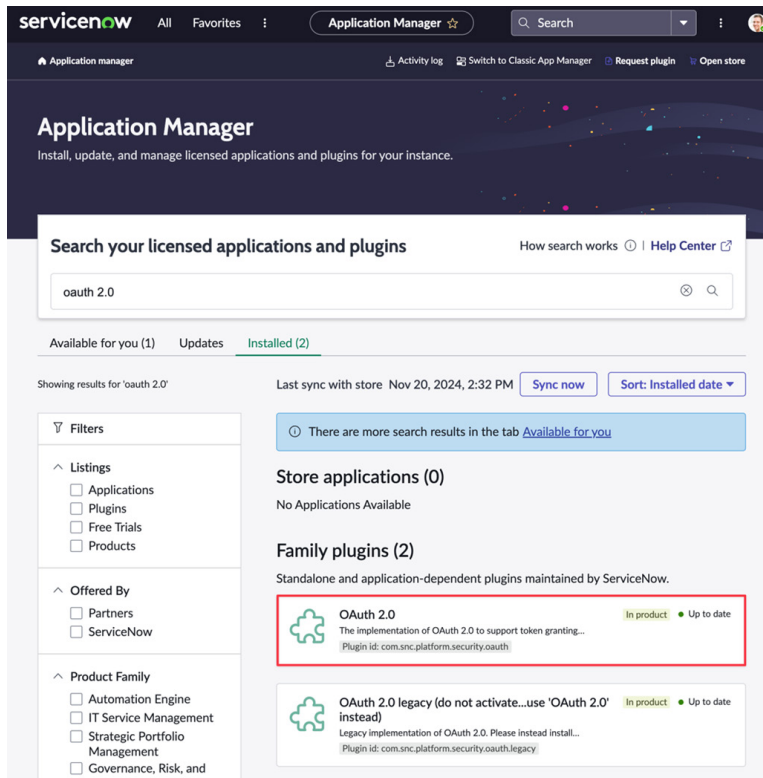


Figure 131. Application Manager

## Create a Client ID and Client Secret

To create a Client ID and Client Secret:

1. Click **All Results**, then search for OAuth.
2. Click **Application Registry**.

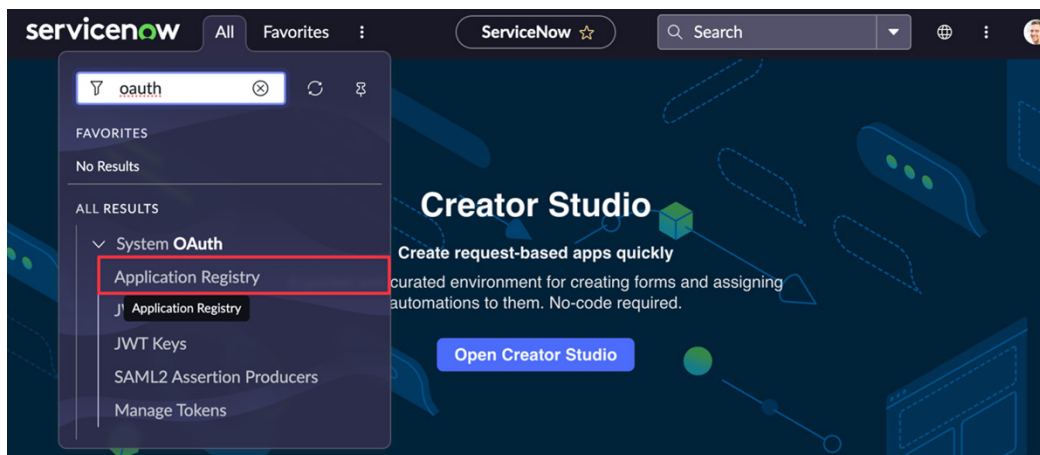


Figure 132. Creator Studio

3. Select **New > Create an OAuth API endpoint for external clients** and configure the following:
  - a. **Name:** Enter a unique name that identifies the platform.
  - b. **Client ID:** This is automatically generated by the instance.
  - c. **Client Secret:** This is automatically generated by the instance after you submit the form.
  - d. **Refresh Token Lifespan:** 8,640,000 seconds (100 days) and it can be increased.
  - e. **Access Token Lifespan:** 1800 seconds (30 Minutes) and it can be increased.
  - f. Click **Submit**.

OAuth client application details.

- Name:** A unique name.
- Client ID:** Client ID automatically generated by ServiceNow OAuth server.
- Client Secret:** Client secret for the OAuth application. Leave it empty for auto-generation.
- Refresh Token Lifespan:** Time in seconds the Refresh Token will be valid.
- Access Token Lifespan:** Time in seconds the Access Token will be valid.
- Redirect URL:** The redirect URL's authorization server redirect to. They must be absolute URLs and they are comma separated.
- Enforce Token Restriction:** Restricts the access token usage to the API's defined in the [REST API Access Policies](#). Unselecting this option would allow access token usage across other REST API's. [Learn more.](#)

[More Info](#)

\* Name:  Application: Global

\* Client ID:  Accessible from: All application scopes

Client Secret:

Active: ☒

\* Refresh Token Lifespan:

\* Access Token Lifespan:

Redirect URL:

Logo URL:

Public Client: ☐

Client Type: -- None --

Comments:

Auth Scopes

Auth Scope

Insert a new row...

**Submit**

Figure 133. Create an OAuth API endpoint for external clients

4. Click the newly created **Application Registry**, then copy the **Client ID** and **Client Secret**.

OAuth client application details.

- Name:** A unique name.
- Client ID:** Client ID automatically generated by ServiceNow OAuth server.
- Client Secret:** Client secret for the OAuth application. Leave it empty for auto-generation.
- Refresh Token Lifespan:** Time in seconds the Refresh Token will be valid.
- Access Token Lifespan:** Time in seconds the Access Token will be valid.
- Redirect URL:** The redirect URL's authorization server redirect to. They must be absolute URLs and they are comma separated.
- Enforce Token Restriction:** Restricts the access token usage to the API's defined in the [REST API Access Policies](#). Unselecting this option would allow access token usage across other REST API's. [Learn more.](#)

[More Info](#)

\* Name:  Application: Global

\* Client ID:  Accessible from: All application scopes

Client Secret:

Active: ☒

\* Refresh Token Lifespan:

\* Access Token Lifespan:

Redirect URL:

Logo URL:

Public Client: ☐

Client Type: -- None --

Comments:

Auth Scopes

Auth Scope

Insert a new row...

**Update** **Delete**

Figure 134. Application Registry

## Retrieve the Refresh Token

(Optional) To generate the refresh token for your ServiceNow source, you must make an HTTP POST request to the ServiceNow OAuth token endpoint. To do this, prepare the OAuth 2.0 credentials retrieved previously, including the Instance Name, Username, Password for the Administrator account, Client ID, and Client Secret.

1. To generate the **Refresh Token**, launch your terminal and run the following command (optionally, you can use an API platform such as Postman):

```
curl --location 'https://<instance-name>.service-now.com/oauth_token.do' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'client_id=<client_ID>' \
--data-urlencode 'client_secret=<client_secret>' \
--data-urlencode 'username=<username>' \
--data-urlencode 'password=<user_password>'
```

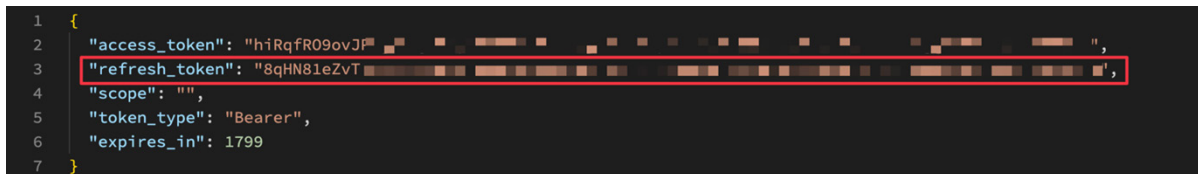
Where:

- instance\_name is set to your instance name (e.g., for dev255652.service-now.com, it would be dev255652).
- grant\_type is set to password.
- client\_id the Client ID of your OAuth application generated earlier.
- client\_secret is the Client Secret of your OAuth application generated earlier.
- Username is your ServiceNow Administrator account name that authorizes the access token request.
- Password is the password for the ServiceNow Administrator account that authorizes the access token request.

The request returns two tokens:

- An access token
- A refresh token

Make sure to enter the Refresh Token (and not the Access Token) in to the Authentication section in the Data Source Configuration page.



```
1 {
2   "access_token": "hiRqfR09ovJf...",
3   "refresh_token": "8qHN81eZvT...",
4   "scope": "",
5   "token_type": "Bearer",
6   "expires_in": 1799
7 }
```

Figure 135. Refresh token



## Configure the ServiceNow UVM Data Connectors

The following sections describe how to configure the ServiceNow UVM data connectors.

### Configure the ServiceNow Assets Data Source

To configure the ServiceNow assets data source:

1. Ensure your Administrator has access to the following tables:
  - cmdb\_ci\_computer
  - cmdb\_ci\_server
  - cmdb\_ci\_vm\_instance

If you choose to retrieve application data, add the relevant tables listed below:

- Include Related Application Services IDs: cmdb\_ci\_service\_discovered
- Include Related Applications IDs: cmdb\_ci\_appl
- Include Related Business Applications IDs: cmdb\_ci\_business\_app

2. Log in to your Avalor tenant and click **Configure**.

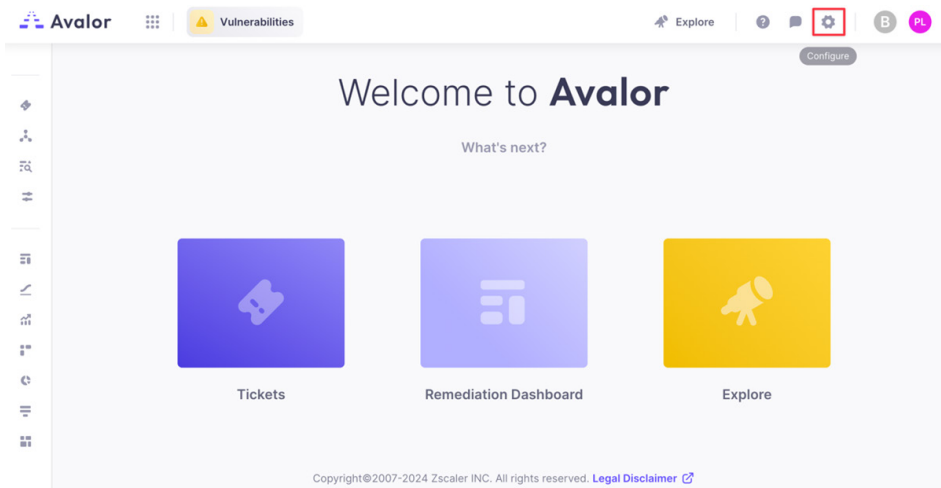


Figure 136. Configure

3. Search for Service Now Assets.

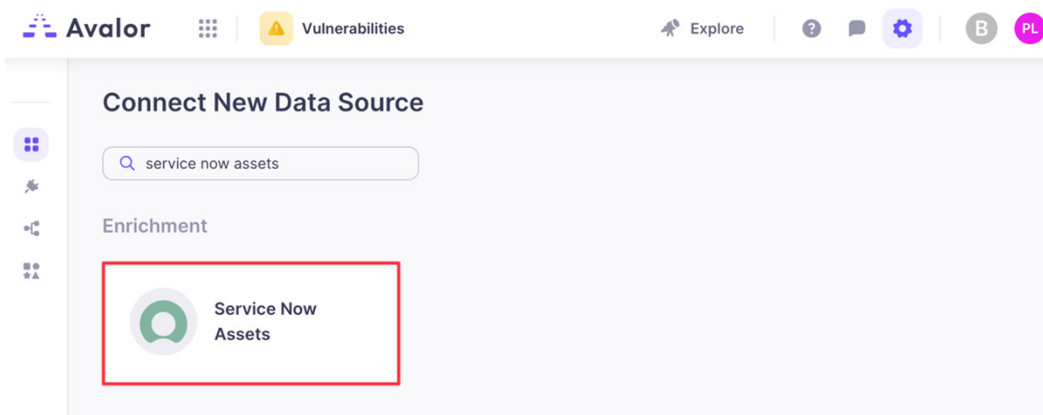


Figure 137. ServiceNow Assets

4. Click the **Service Now Assets** application.
5. On the **Create Service Now Assets Source** page, complete the following:
  - a. **Name:** Enter a name for the Data Connector.
  - b. **Active:** Toggle to enable the Data Connector.
  - c. **Instance Name:** Enter your instance name (e.g., for dev255652.service-now.com, it would be dev255652).
  - d. **Authentication:** Select **OAuth2**.
  - e. **Grant Type:** Password. If you would prefer to use a refresh token, select refresh token.
  - f. **Username:** Enter your Administrator Username.
  - g. **Password:** Enter your Administrator Password.
  - h. **Client ID:** Enter your Client ID.
  - i. **Client Secret:** Enter your Client Secret.
  - j. **Include Related Applications Data:** Select if required.
  - k. **Include Related Application Services Data:** Select if required.
  - l. **Include Related Business Applications Data:** Select if required.
  - m. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
  - n. **Remediation Detection Settings:** Select your desired option to determine when findings will automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
  - o. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials have been entered in correctly, the system responds with Test Passed.

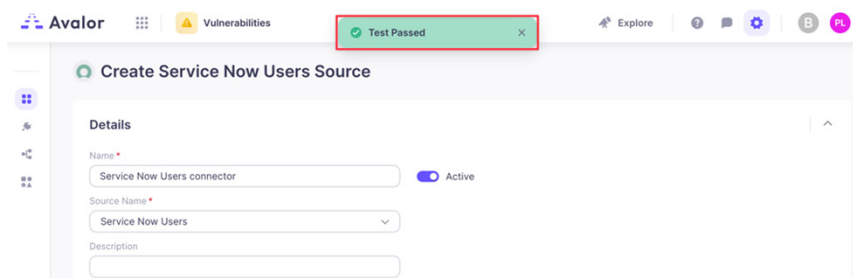


Figure 138. Test Passed

7. Click **Save**.

**Create Service Now Assets Source**

**Details**

Name\*  
Service Now Assets connector ☒ Active

Source Name\*  
Service Now Assets

Description

**Retrieval**

Instance Name\*  
dev255833

Authentication\*  
☒ OAuth2 ☐ Basic Auth

Grant Type\*  
Password

Username\*  
admin

Password\*

Client ID\*  
alef9eb805c463dbce50cd572918d4

Client Secret\*

☐ Include Related Applications Data  
☐ Include Related Application Services Data  
☐ Include Related Business Applications Data

**Scheduling**

Full Refresh Frequency\*  
Weekly

Repeat On\*  
S M T W T F S

Time (UTC)\*  
07:00 PM

Incremental Refresh Frequency\*  
Daily

Time (UTC)\*  
07:00 PM

**Remediation Detection Settings**

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

**Aging criteria** [+ Add Rule](#)

☐ Age Immediately if Finding was not seen, while Asset was seen in the latest full data refresh

**Fallback**

☐ Age Immediately if Finding was not seen for  day(s)

**Advanced Settings**

**Suppression Rules**

Select Field  Contains  Type Value

☒ Prevent NULL from overriding existing values

Figure 139. Create ServiceNow Assets Source

## Configure the Service Now Users Data Source

To configure the ServiceNow users data source:

1. Ensure your Administrator has access to the following tables:
  - sys\_user
  - cmn\_department
2. Log in to the Avalor UVM Platform.
3. Click **Configure**.

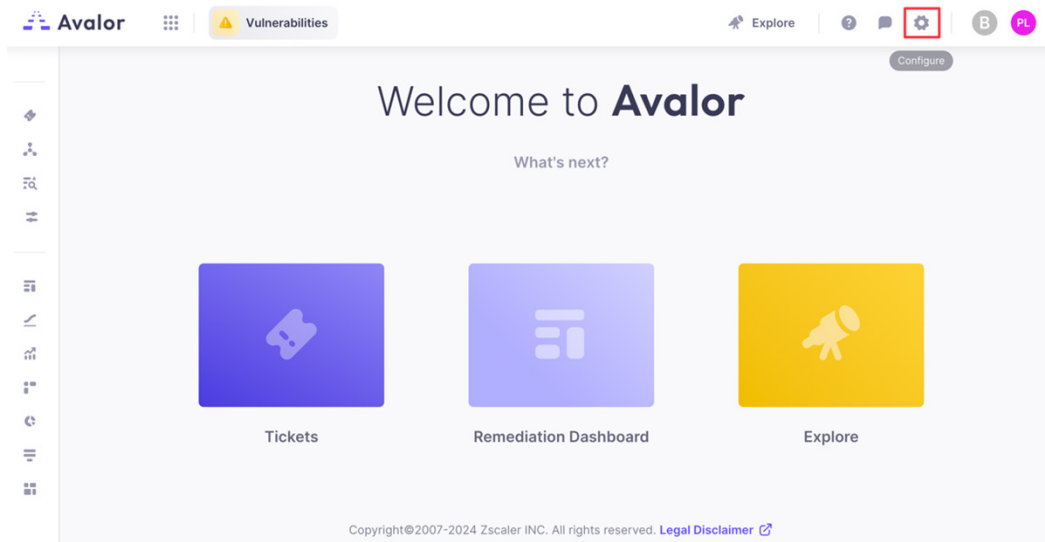


Figure 140. Configure

4. Click **Create**, then search for Service Now Users.

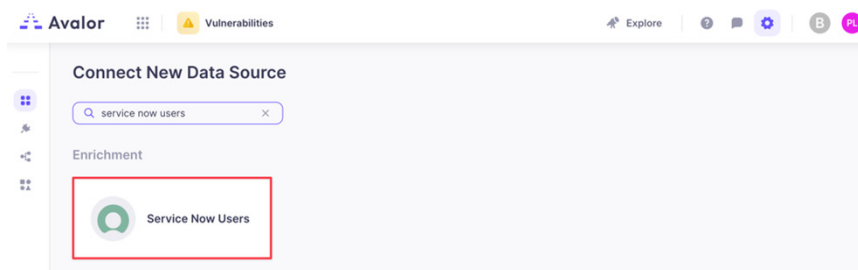


Figure 141. ServiceNow Users

5. Click the **ServiceNow Users** application.

6. On the **Create ServiceNow Users Source** page, complete the following:
  - a. **Name:** Enter a name for the Data Connector.
  - b. **Active:** Toggle to enable the Data Connector.
  - c. **Instance Name:** Enter your instance name (e.g., for dev255652.service-now.com, it would be dev255652).
  - d. **Authentication:** Select **OAuth2**.
  - e. **Grant Type:** Password. If you would prefer to use a refresh token, select refresh token.
  - f. **Username:** Enter your Administrator Username.
  - g. **Password:** Enter your Administrator Password.
  - h. **Client ID:** Enter your Client ID.
  - i. **Client Secret:** Enter your Client Secret.
  - j. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
  - k. **Remediation Detection Settings:** Select your desired option to determine when findings will automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
  - l. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
7. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

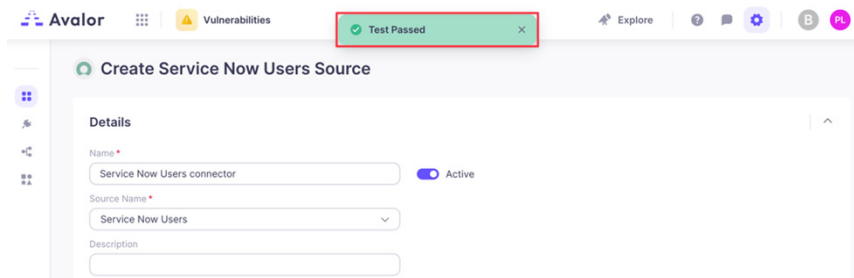


Figure 142. Test Passed

8. Click **Save**.

**Create Service Now Users Source**

**Details**

Name \*  
Service Now Users connector ☒ Active

Source Name \*  
Service Now Users

Description

**Retrieval**

Instance Name \*  
dev255633

Authentication  
☒ OAuth2 ☐ Basic Auth

Grant Type \*  
Password

Username \*  
admin

Password \*  
[Masked]

Client id \*  
a9ef8e9d805c463d9ce50cd572911dc4

Client Secret \*  
[Masked]

**Scheduling**

Full Refresh Frequency \*  
Weekly

Repeat On \*  
S M T W T F S

Time (UTC) \*  
08:00 PM

Incremental Refresh Frequency \*  
Daily

Time (UTC) \*  
08:00 PM

**Remediation Detection Settings**

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria + Add Rule  
☐ Age immediately if Finding was not seen, while Asset was seen in the latest full data refresh

Fallback  
☐ Age immediately if Finding was not seen for  day(s)

**Advanced Settings**

Suppression Rules

Select Field  Contains  Type Value

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 143. Create ServiceNow Users Source

## Configure the ServiceNow Generic Data Source

Ensure your Administrator has access to the tables this data source is configured to access.

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

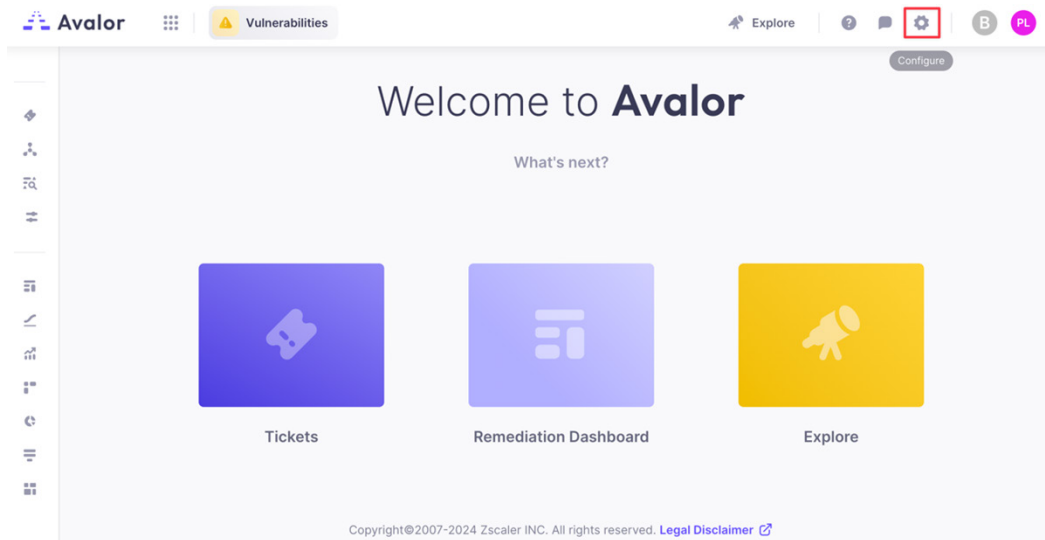


Figure 144. Configure

3. Click **Create**, then search for Service Now Generic.

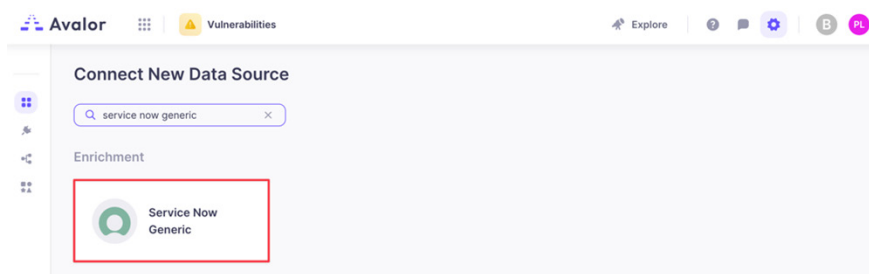


Figure 145. Connect New Data Source

4. Click the **ServiceNow Generic** application.

5. On the **Create ServiceNow Generic Source** page, complete the following:
  - a. **Name:** Enter a name for the Data Connector.
  - b. **Active:** Toggle to enable the Data Connector.
  - c. **Instance Name:** Enter your instance name (e.g., for dev255652.service-now.com, it would be dev255652).
  - d. **Authentication:** Select **OAuth2**.
  - e. **Grant Type:** Password. If you would prefer to use a refresh token, select refresh token.
  - f. **Username:** Enter your Administrator Username.
  - g. **Password:** Enter your Administrator Password.
  - h. **Client ID:** Enter your Client ID.
  - i. **Client Secret:** Enter your Client Secret.
  - j. **Include Related Applications Data:** Select if required.
  - k. **Include Related Application Services Data:** Select if required.
  - l. **Include Related Business Applications Data:** Select if required.
  - m. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
  - n. **Remediation Detection Settings:** Select your desired option to determine when findings will automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
  - o. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials have been entered in correctly, the system responds with Test Passed.

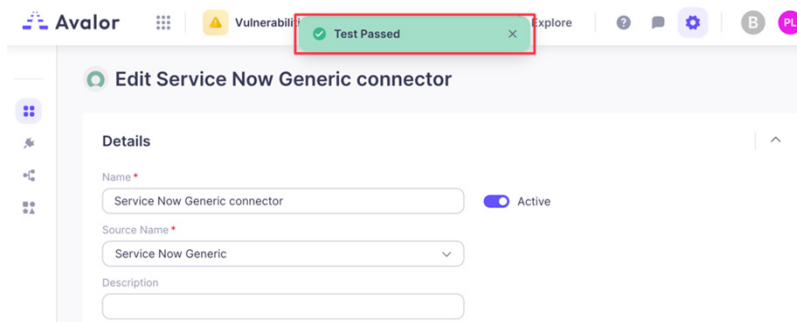


Figure 146. Create ServiceNow Generic connector



7. Click **Save**.

**Create Service Now Generic Source**

**Details**

Name:  ☒ Active

Source Name:

Description:

**Retrieval**

Instance Name:

Authentication: ☒ OAuth2 ☐ Basic Auth

Grant Type:

Username:

Password:

Client ID:

Client Secret:

Table Name:

Field Name:

Fields Params:

**Scheduling**

Full Refresh Frequency:

Repeat On:

Time UTC:

Incremental Refresh Frequency:

Time UTC:

**Remediation Detection Settings**

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria: ☐ Age immediately if Finding was not seen, while Asset was seen in the latest full data refresh

Fallback: ☐ Age immediately if Finding was not seen for

**Advanced Settings**

Suppression Rules

Select Field:  Contains:

AND OR

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 147. Create ServiceNow Generic Source

## Configure the ServiceNow Outegrations

An Avalor Outegration allows you to create a ServiceNow Incident, Request, Remediation Task or Task based on an Avalor Ticket, Asset, Incident, Alert or Finding. The following configuration creates a ServiceNow Incident based on an Avalor Ticket.

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

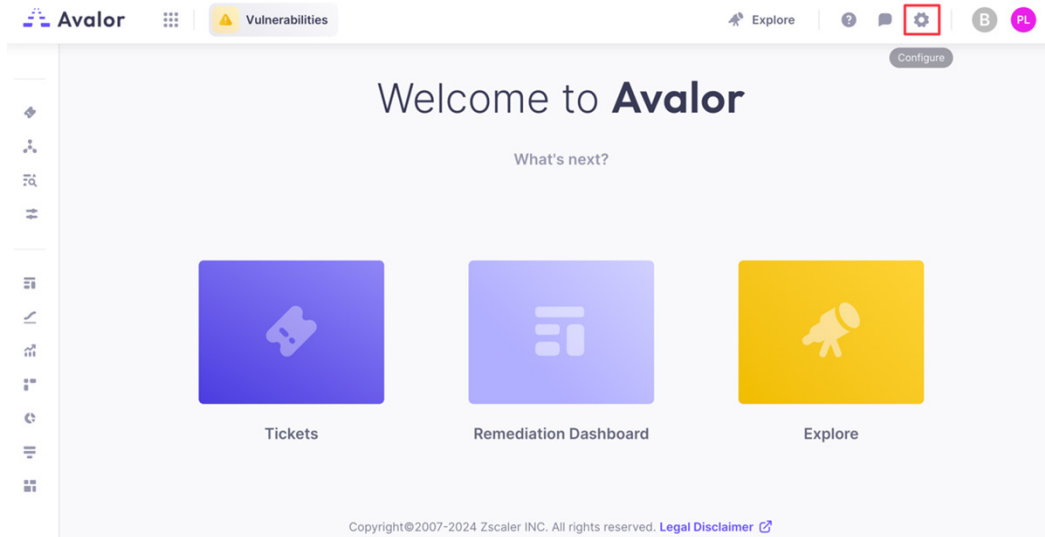


Figure 148. Configure

3. Click **Outegrations**.

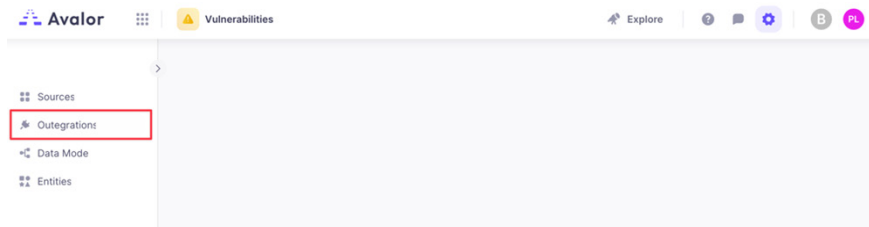


Figure 149. Outegrations

4. Click **Create New Integrations**, then search for ServiceNow.

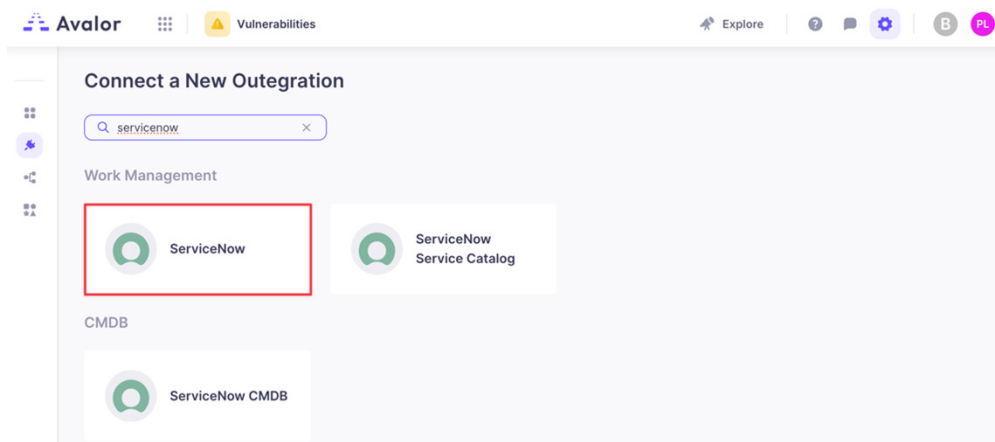


Figure 150. Connect a new outegration

5. Click the **ServiceNow** application.
6. On the **Create ServiceNow Outegration** page, complete the following:
  - a. **Display Name:** Enter a name for the Outegration.
  - b. **Active:** Toggle to enable the Outegration.
  - c. **Create ServiceNow from:** Select which attribute to create a ServiceNow event from. For this example, select **Ticket**.
  - d. **Instance Name:** Enter your instance name (e.g., for dev255652.service-now.com, it would be dev255652).
  - e. **Table:** Select the ServiceNow table to create the ticket in. For this example, select **Incident**.
  - f. **Authentication:** Select **OAuth2**.
  - g. **Grant Type:** Password. If you would prefer to use a refresh token, select refresh token.
  - h. **Username:** Enter your Administrator Username.
  - i. **Password:** Enter your Administrator Password.
  - j. **Client ID:** Enter your Client ID.
  - k. **Client Secret:** Enter your Client Secret.
  - l. **Tickets View:** Select whether to show this integration in the **Create Ticket** menu. For this example, select **Always**.
  - m. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
7. Click **Test**. If the credentials were entered correctly, the system responds with **Test Passed**.

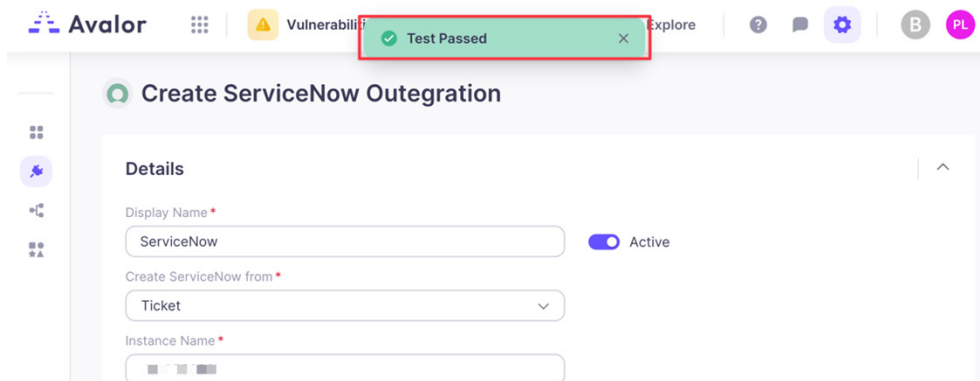


Figure 151. Test Passed

8. Click **Save**.

## Creating an Incident

1. Click **Tickets** in the Avalor Portal.

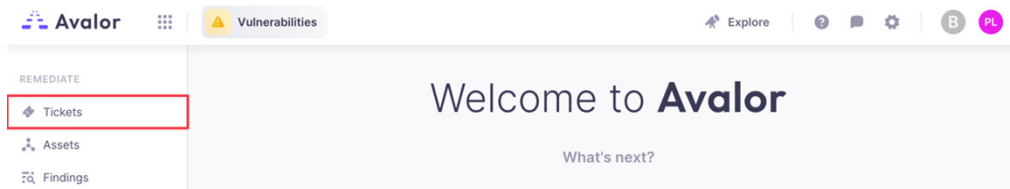


Figure 152. Tickets

2. Select one of your tickets and click **Create ServiceNow Ticket**.

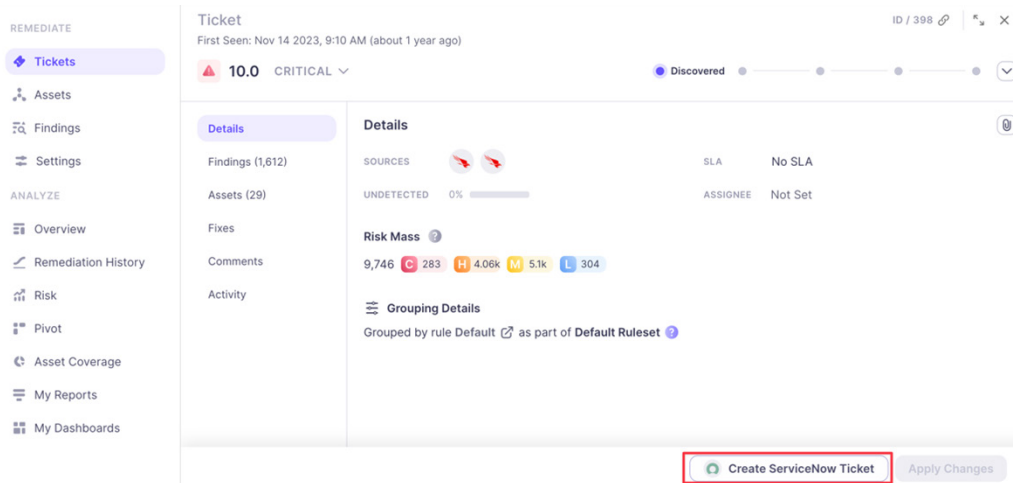


Figure 153. Create ServiceNow Ticket

Avalor now displays the Incident ID.

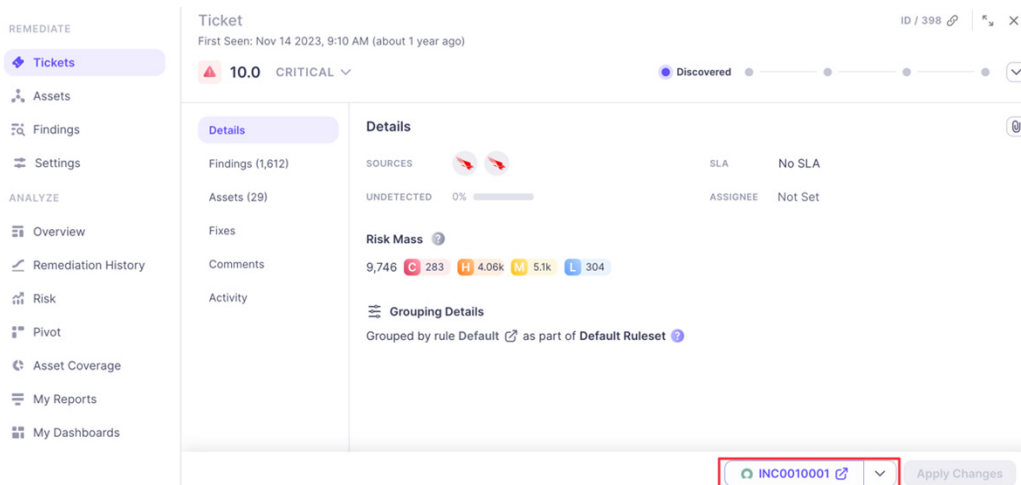


Figure 154. Incident ID

## Review and Adjust Data Model Mapping

(Optional) Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin right away. However, many data sources also provide additional data points that might provide additional context to risk prioritization.

The following example shows how to leverage ServiceNow's *Is Internet Facing* attribute for a hardware asset so that that attribute can be used as a Risk Factor when calculating risk for an Asset in Avalor.

### Mark a ServiceNow Asset Internet Facing

To mark a ServiceNow asset internet facing:

1. Log in to your ServiceNow tenant.
2. Go to [https://<your-instance>.service-now.com/cmdb\\_ci\\_computer\\_list.do](https://<your-instance>.service-now.com/cmdb_ci_computer_list.do)
3. Click one of your **Assets**, then select **Configure** > **Form Layout** from the drop-down menu.

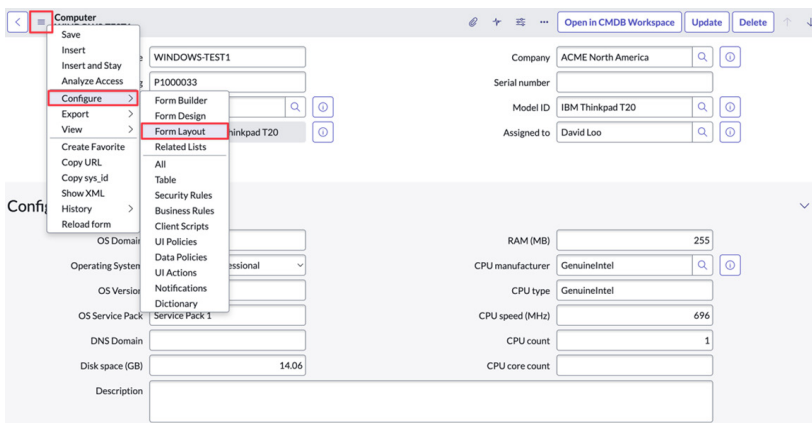


Figure 155. Form Layout

4. Select **Internet Facing** from the list of **Available** field and add it to the **Selected** field list.
5. Click **Save**.

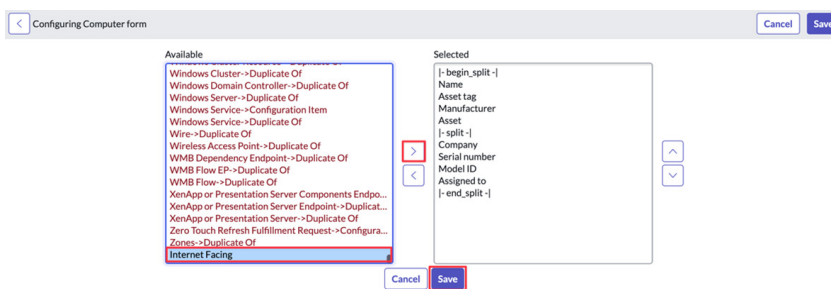


Figure 156. Configuring Computer form

6. For an Asset that is Internet Facing, select **Internet Facing** and click **Update**.

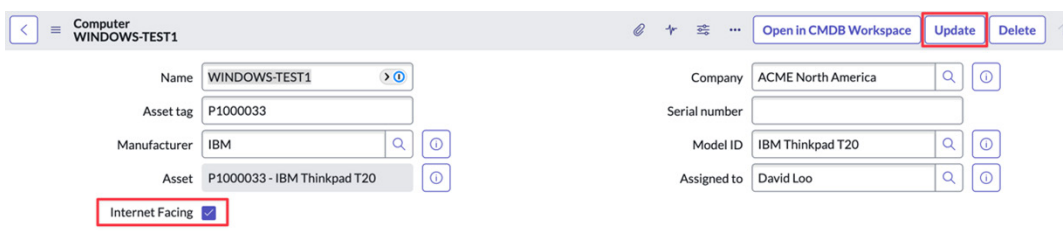


Figure 157. Internet Facing

## Map the Internet Facing Field to Your Avalor Data Model

To map the Internet Facing field to your Avalor data model:

1. Go to **Configure > ServiceNow Assets Connector**.
2. Click **Process Now**, then **Process Now** again to ensure **Data Retrieval Type** is set to **Full Processing**.

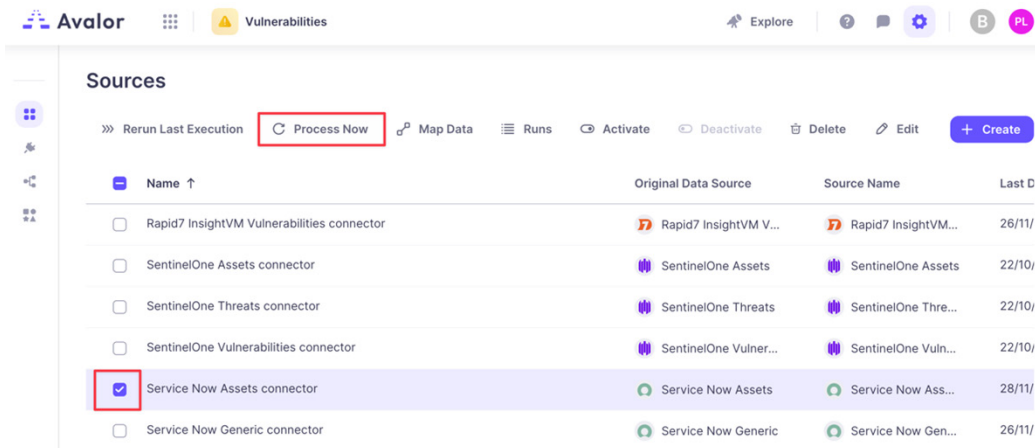


Figure 158. Process Now

3. Select your **ServiceNow Assets Connector**, and click **Map Data**.
4. Drag the **name** field from the **Ingested Data** to the **Create New Connection** box, and drag **Key** from the **Asset Data Entity** to the **Create New Connection** box. This maps the **Assets Name** as its Key value in Avalor.
5. Click **Map**.

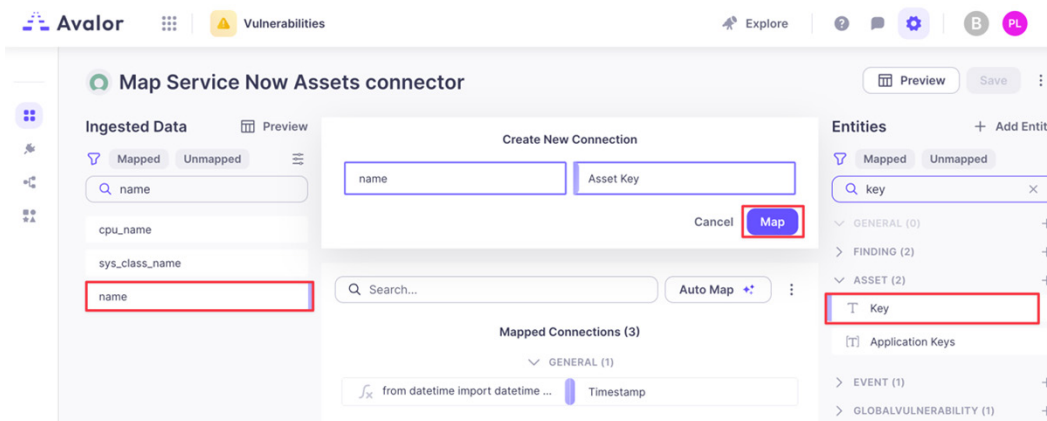


Figure 159. Map ServiceNow Assets connector

6. Click the **Set as** icon.

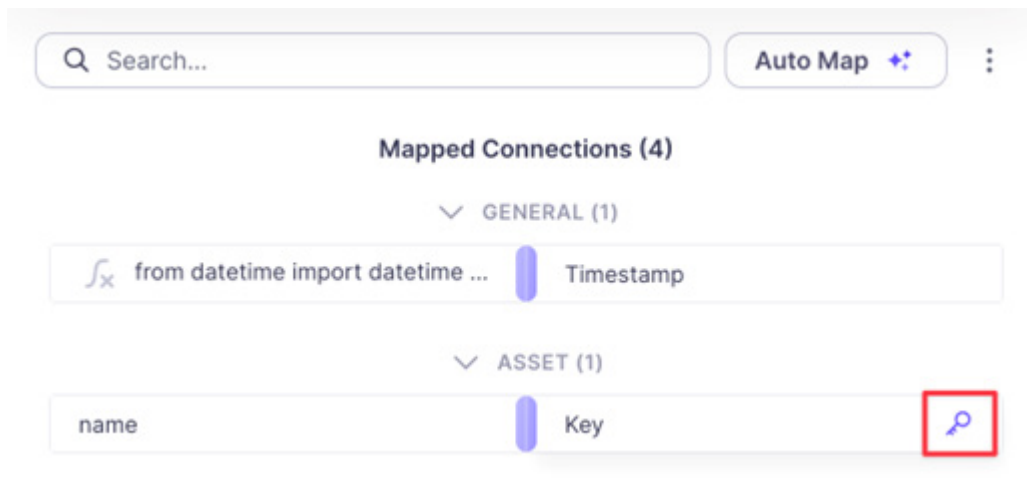


Figure 160. Set as Key

7. Create a new field called **Internet\_Facing** under **Asset**, with **Field Type** as **Boolean**.  
8. Click **Update**.

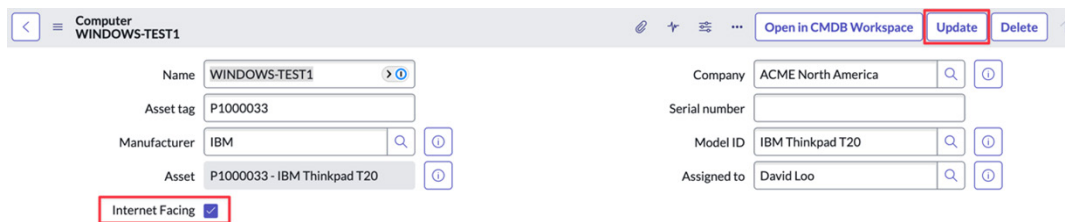


Figure 161. Internet Facing

9. Drag the **Internet\_Facing** field from the **Ingested Data** to the **Create New Connection** box, and drag **Is Internet Facing** from the **Asset Data Entity** to the **Create New Connection** box.  
10. Click **Map**.

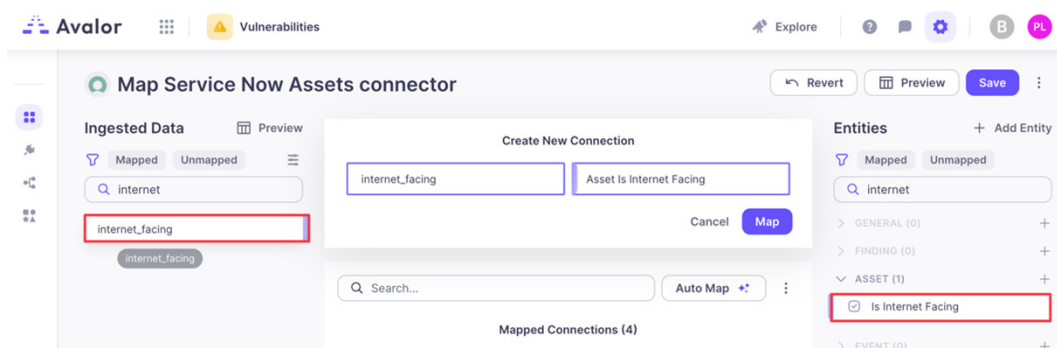
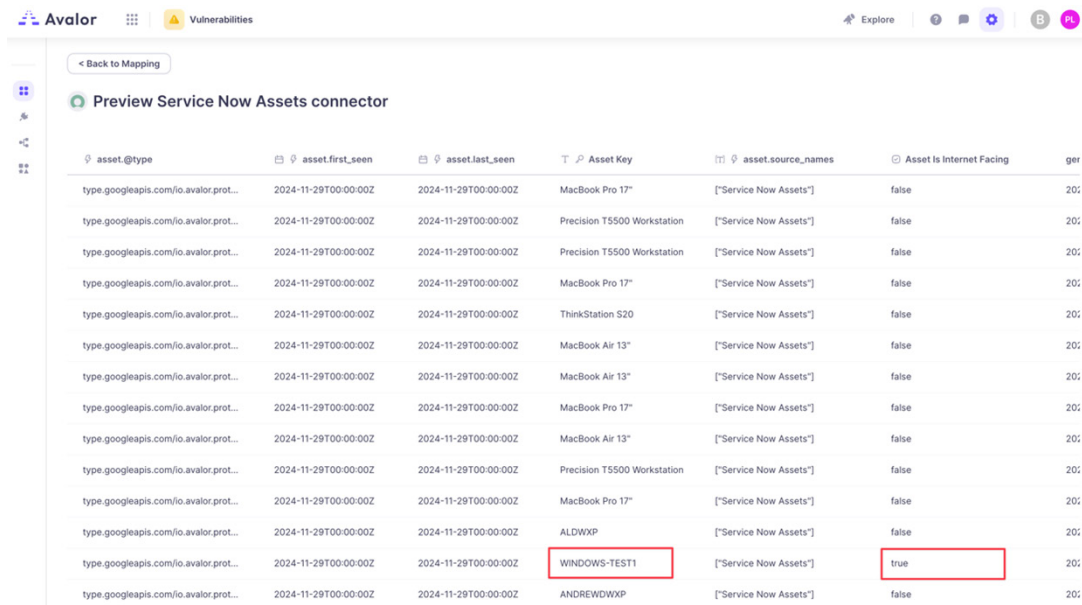


Figure 162. Create New Connection

11. Click **Save**.
12. Click **Preview** to show how Assets have their **ServiceNow Name** mapped to the **Avalor Asset Key**, and the **Service Now Internet Facing** attribute mapped to the **Avalor Is Internet Facing** field.



< Back to Mapping

Preview Service Now Assets connector

asset.@type	asset.first_seen	asset.last_seen	Asset Key	asset.source_names	Asset Is Internet Facing	ger
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Pro 17"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	Precision T5500 Workstation	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	Precision T5500 Workstation	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Pro 17"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	ThinkStation S20	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Air 13"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Air 13"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Pro 17"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Air 13"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	Precision T5500 Workstation	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	MacBook Pro 17"	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	ALDWXP	["Service Now Assets"]	false	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	WINDOWS-TEST1	["Service Now Assets"]	true	20;
type.googleapis.com/io.avalor.prot...	2024-11-29T00:00:00Z	2024-11-29T00:00:00Z	ANDREWDXP	["Service Now Assets"]	false	20;

Figure 163. Preview Service Now Assets connector



## Review and Adjust Risk Scoring

After the ingested data has been normalized and mapped to the Data Model, Avalor UVM can evaluate the risk.

The following example shows how the Is Internet Facing field is added as a Risk Factor for risk scoring. A value of True increases the risk calculation (since the asset is Internet Facing).

1. From the Vulnerabilities tab in the Avalor dashboard (Remediation Hub):
  - a. In the left-side pane, select **Settings > Score**.
  - b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
2. In the **Add new factor** modal:
  - a. Select **Risk Factors** for **Factor Type** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
  - b. Enter a **Name**.
  - c. Select **Is Internet Facing** for **Field**.
  - d. In the **Boolean** log in section, under **True**, enter a percentage by which the risk is increased.
  - e. Click **Apply**, then **Save & Run**.

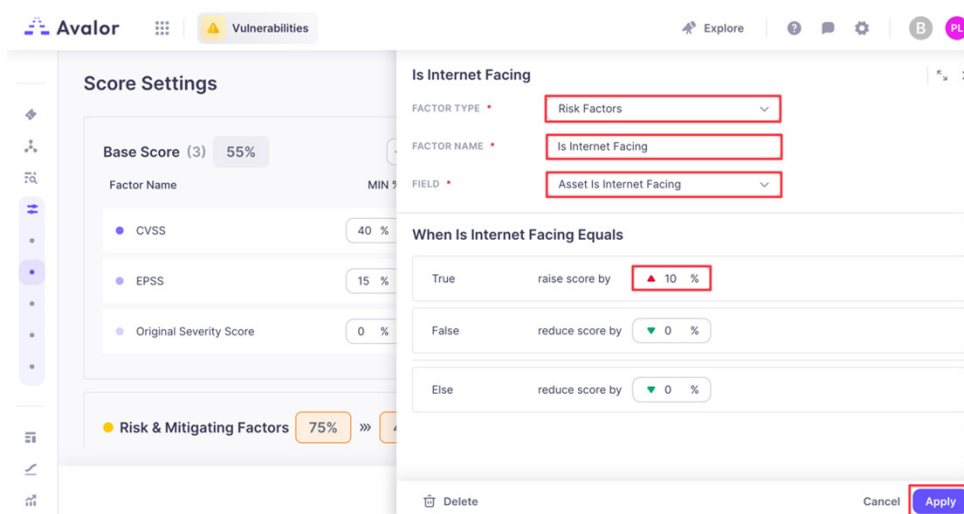


Figure 164. Score settings

3. In the left-side pane, select the **Assets** dashboard. From the **Assets** dashboard:
  - a. Set a filter by selecting **True** from the **Is Internet Facing** drop-down menu.

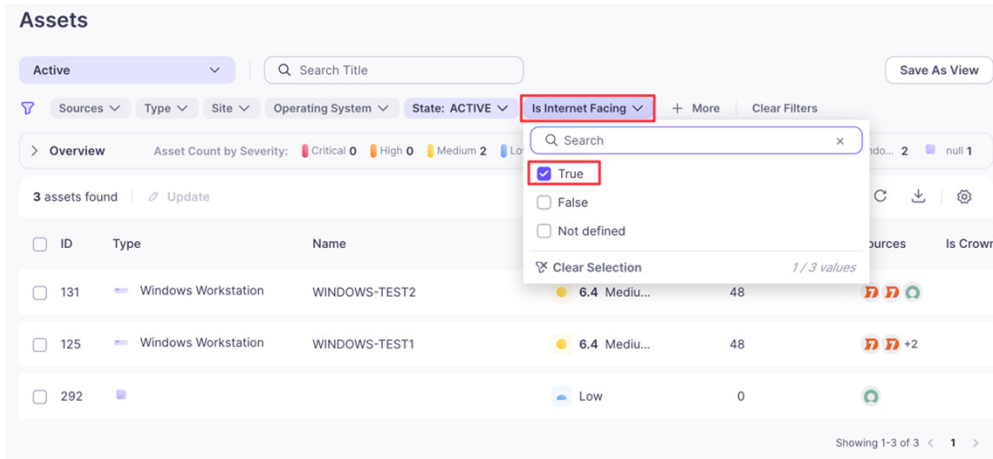


Figure 165. Assets

- b. Click one of your **Assets** in the filtered list.
- c. In the **Asset** modal that appears, click the **Findings** tab.
- d. Click one of the **Findings**.
- e. Review the output (notice the **Score Adjustment** section and whether **Is Internet Facing** has modified the risk scoring).

## 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**.

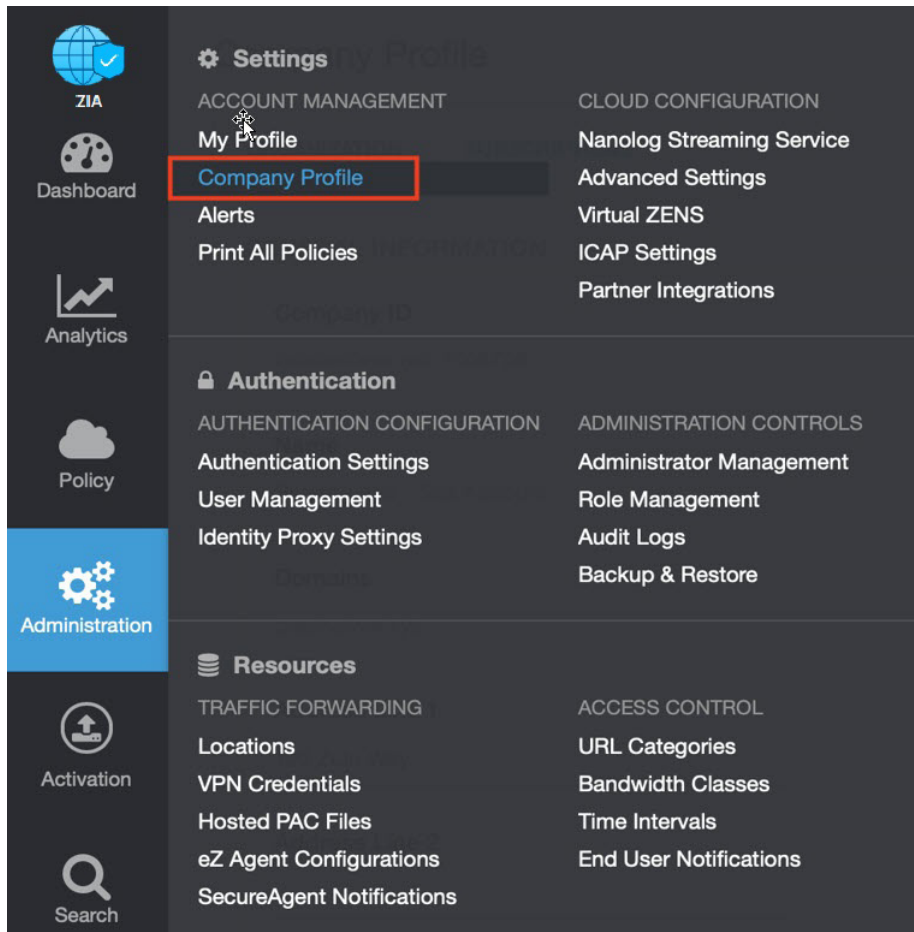
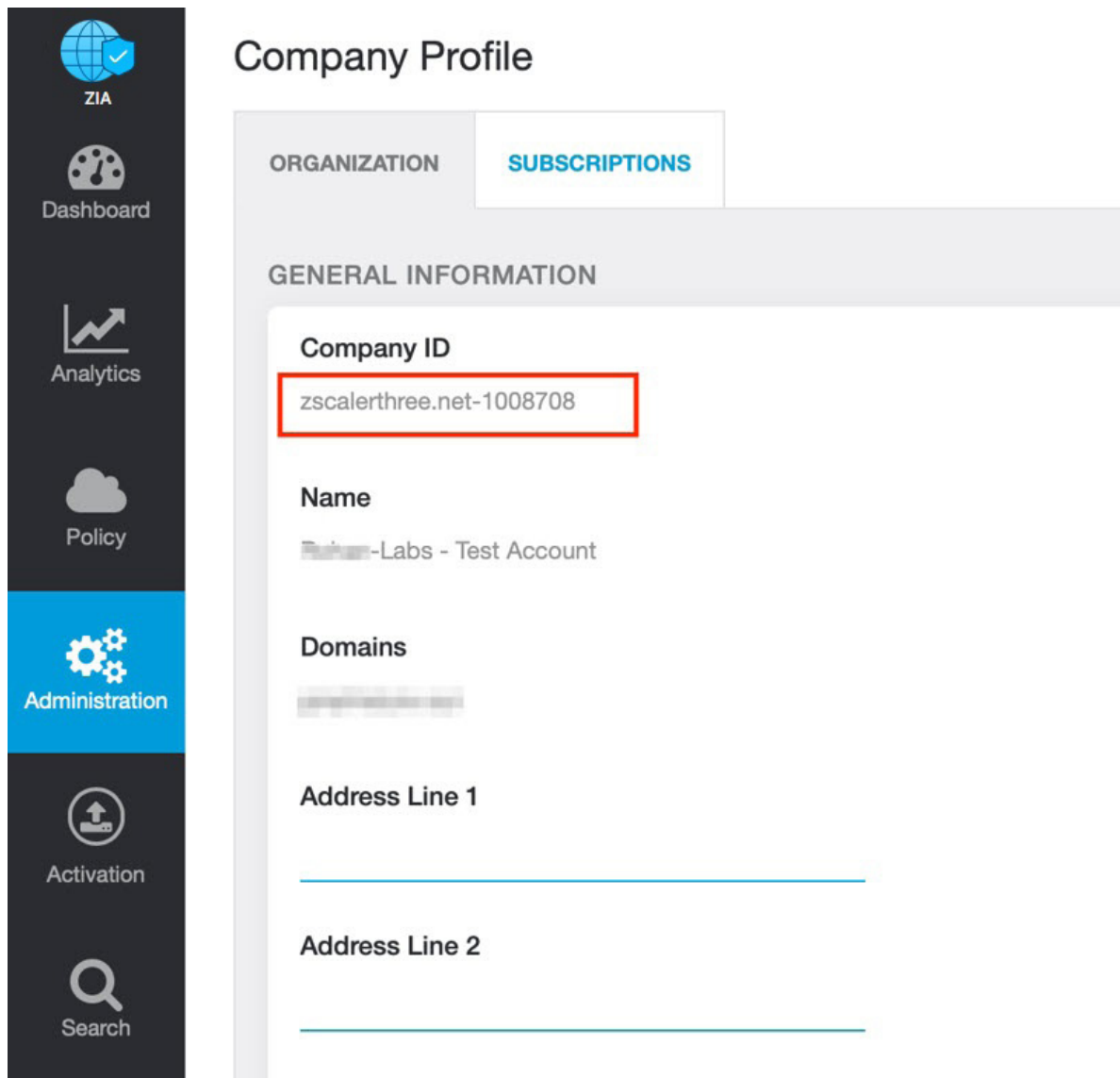


Figure 166. Collecting details to open a support case with Zscaler TAC

2. Copy the Company ID.



The screenshot displays the Zscaler user interface. On the left is a dark sidebar with navigation icons and labels: ZIA (globe icon), Dashboard (circular nodes icon), Analytics (line graph icon), Policy (cloud icon), Administration (gears icon, highlighted in blue), Activation (upload icon), and Search (magnifying glass icon). The main content area is titled "Company Profile" and has two tabs: "ORGANIZATION" and "SUBSCRIPTIONS" (which is active). Under the "SUBSCRIPTIONS" tab, there is a section titled "GENERAL INFORMATION". Within this section, the "Company ID" field is highlighted with a red rectangular border and contains the text "zscalerthree.net-1008708". Below the Company ID are fields for "Name" (containing "Zscaler-Labs - Test Account"), "Domains" (containing a blurred domain), "Address Line 1" (an empty input field), and "Address Line 2" (an empty input field).

Figure 167. Company ID

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

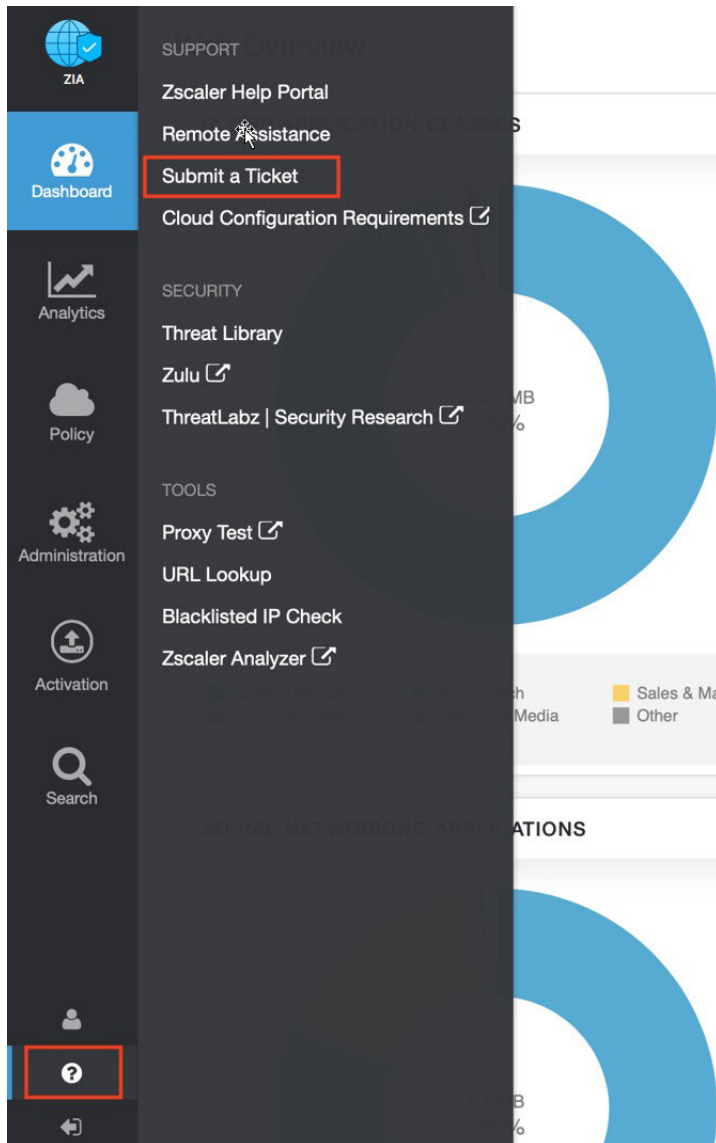


Figure 168. Submit a ticket