Table of Contents

1 Zscaler Data Protection and Digital Experience for ServiceNow.com ........................................7
  1.1 Overview ........................................................................................................................................ 7
  1.2 Zscaler SaaS Identity Proxy............................................................................................................... 9
  1.3 Zscaler Internet Access Browser Isolation ....................................................................................... 10
  1.4 Zscaler Internet Access CASB Data and Malware Protection for ServiceNow .............................. 11
  1.5 Zscaler Internet Access Cloud Application Control ......................................................................... 13
  1.6 Zscaler Digital Experience for the ServiceNow User Experience .................................................. 14

2 Configure the SaaS Identity Proxy.................................................................................................... 15
  2.1 Configure the SaaS Identity Proxy ................................................................................................... 16
  2.2 Configure the Zscaler Portal for the SaaS Identity Proxy ................................................................. 17
  2.3 Configure ServiceNow to use the Identity Proxy ........................................................................... 19
  2.4 Install the ServiceNow Plugins ...................................................................................................... 20
  2.5 Configure the SaaS Identity Proxy ................................................................................................... 21
  2.6 Add Zscaler as an Identity Provider ............................................................................................... 22
  2.7 Configure the Identity Provider ....................................................................................................... 24
  2.8 Add the Identity Provider Certificate and Additional Settings ...................................................... 25
  2.9 Testing the Identity Provider ........................................................................................................... 29
  2.10 The Active Identity Proxy Notification .......................................................................................... 30
  2.11 Configure Redirect on the Identity Provider .................................................................................. 31

3 Configure Cloud Browser Isolation .................................................................................................. 35
  3.1 Configure the Cloud Browser Isolation Profile ............................................................................... 36
  3.2 Configure the Cloud Browser Isolation Policies ............................................................................ 44

4 Configuring the ServiceNow Tenant ................................................................................................ 50
  4.1 Adding the ServiceNow Tenant ....................................................................................................... 51
  4.2 SaaS Tenant Configuration Wizard ............................................................................................... 52
  4.3 Configuring the Zscaler Tenant on ServiceNow ............................................................................ 54
  4.4 Check that OAuth is Installed and Active ....................................................................................... 56
  4.5 Create an OAuth Application Registry ............................................................................................ 58

5 Configuring ServiceNow Policies and Scan Configuration ................................................................. 65
  5.1 Scoping the Policies and Remediation ............................................................................................. 66
  5.2 Creating a DLP Policy ...................................................................................................................... 67
  5.3 Creating a DLP Engine ..................................................................................................................... 68
  5.4 Configure a SaaS DLP Policy ......................................................................................................... 70
  5.5 SaaS DLP Policy Details ............................................................................................................... 71

6 Configure a SaaS Malware Policy ...................................................................................................... 74
  6.1 SaaS Malware Policy Wizard ......................................................................................................... 75

7 Configure the Scan Schedule Configuration ..................................................................................... 77
  7.1 Start the Scan Schedule .................................................................................................................... 78

8 Reporting and Visibility ..................................................................................................................... 79
  8.1 SaaS Assets and SaaS Assets Summary Report ............................................................................... 80
  8.2 SaaS Security Insights .................................................................................................................... 81
Zscaler / ServiceNow Deployment Guide

9 Cloud App Control
  9.1 Cloud Application Access Control Policy
  9.2 Cloud Application Access Control Policy Wizard
  9.3 Cloud Application Access Control Logs

10 Zscaler Digital Exchange (ZDX) for ServiceNow
  10.1 Configure ZDX for ServiceNow
  10.2 Configure Probes for ServiceNow Monitoring
  10.3 The ZDX Enabled ServiceNow Application
  10.4 Create an Alert for the ServiceNow Service
  10.5 The Triggered Alert for the ServiceNow Service
  10.6 Alert Detail for the ServiceNow Service
  10.7 The Sent Alert Email for the ServiceNow Service

11 Using ZDX – The Dashboard
  11.1 Application Overview
  11.2 ServiceNow Application Performance Detail
  11.3 User Overview
  11.4 ServiceNow User Detail

12 ZCSPM – ServiceNow Integration for Ticket Creation
  12.1 Configure ServiceNow Ticketing Integration

13 Appendix A:
  13.1 Zscaler Resources
  13.2 ServiceNow.com Resources
## Terms and Acronyms

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

Zscaler Overview

Zscaler (Nasdaq: ZS), Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss.

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

ServiceNow Overview

ServiceNow, Inc. (NYSE; NOW), ServiceNow, Inc. 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 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.

For more information on ServiceNow, Inc., please visit www.servicenow.com or follow them on Twitter@servicenow.
Audience

This guide is written for Zscaler Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring, and managing SaaS services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka “BD SA”). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and ServiceNow Production Release dated Apr 14, 2021. A ServiceNow developer account was used to created and verify the features enabled and used as examples.

Create a ServiceNow Developer Account:
https://developer.servicenow.com/dev.do#!/

Request for Comments

- **For Prospects / Customers:** We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at:
  - partner-doc-support@zscaler.com

- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
  - z-bd-sa@zscaler.com
1 Zscaler Data Protection and Digital Experience for ServiceNow.com

1.1 Overview

ServiceNow is one of the industry leaders that defined the utility of the Cloud, 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, and our partner ServiceNow.com defined the cloud and is still one of the industry leaders. But 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 incredible business tools.
Another challenge faced by organizations migrating to Cloud Services in today’s environment has been the ability to monitor the Users’ experience for the SaaS application. Especially in today’s Work from Anywhere corporate infrastructures. Zscaler provides a complete ServiceNow solution using our Zscaler Internet Services (ZIA) for Security of ServiceNow and our Zscaler Digital Access Exchange Service (ZDX), for visibility of the Users’ experience.

ZIA provides ServiceNow SaaS Security by using Access Control, Identity Control, SaaS Security Posture Management, and our SaaS API to scan the ServiceNow attachments for Malicious Content, and Data Loss Protection. 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 Users 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 SaaS Monitoring operate as separate stand-alone services and are not dependent on one or the other. However, the two services working together provide a comprehensive solution for both security and operations of our Partners SaaS CRM service.

This guide will cover the following Zscaler Internet Access features for ServiceNow Security, and the Zscaler Digital Experience for ServiceNow performance visibility.

- SaaS Identity Proxy
- Cloud Browser Isolation
- SaaS Security Data Loss Protection (CASB)
- SaaS Security Malware Detection (CASB)
- Cloud Application Access Control
- Zscaler Digital Experience for ServiceNow
- Zscaler Cloud Security Posture Management ServiceNow Incident Creation
1.2 Zscaler Internet Access 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.

When users try to access ServiceNow with their corporate accounts without going through the Zscaler service, they will receive a Pop-up screen asking them to login via Zscaler. The process is controlled using SAML, the IDP that is defined on Zscaler for the ZIA service, and the ServiceNow SSO configuration to forward auth requests to Zscaler. Once the user’s identity has been verified their traffic to and from ServiceNow is secured and the user and the ServiceNow data is inspected using Zscaler Internet Access.

Zscaler Internet Access sits between your users and ServiceNow, inspecting every byte of traffic inline across multiple security techniques, even within SSL. You get full protection from web and internet threats. And with a cloud platform that supports Cloud Firewall, Cloud IPS, Cloud Sandbox, Cloud DLP, CASB and Cloud Browser Isolation, you can start with the services you need today and activate others as your needs grow.
1.3 Zscaler Internet Access Browser Isolation

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

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

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

Cloud Browser Isolation can be combined with Identity Proxy to provide extra security to ServiceNow users by assuring the Identity of the user, guaranteeing the users traffic is scanned and secured with the ZIA security features.
1.4 Zscaler Internet Access CASB Data and Malware Protection for ServiceNow

The Zscaler CASB (SaaS Security API) is a feature set that is part of the Zscaler Internet Access security cloud and is designed specifically to help manage the risks of our File Collaboration SaaS Partners, preventing data exposure and ensure compliance across the SaaS application.

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 our 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 Zscaler Cloud Security Platform provides unified data protection with DLP, and Malware Scanning capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance. Zscaler also offers Zscaler Private Access for Zero-Trust access to internal applications, Zscaler Digital Experience for active monitoring of a Users’ experience to SaaS applications, and Zscaler Cloud Protection. Zscaler provides end to end connectivity, security, and visibility from any location on-prem or remote.

For more information, please see the resources in Appendix A: Zscaler Resources.
1.5 Zscaler Internet Access Cloud Application Control

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

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

Let's define a Cloud Application Control Policy to allow only users in a ServiceNow security group to access ServiceNow and block access for all other users. This will require two policies, one policy to allow our specific users and one to block all other users.
1.6 Zscaler Digital Experience for the ServiceNow User Experience

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

What makes the Zscaler Digital Experience 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, please see the resources in Appendix A: Zscaler Resources.
2 Configure the SaaS Identity Proxy

![Zscaler Internet Access Identity Proxy](image)

**Figure 7: Zscaler Internet Access 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.

When users try to access ServiceNow with their corporate accounts without going through the Zscaler service, they will receive a Pop-up screen asking them to login via Zscaler. The process is controlled using SAML, the IDP that is defined on Zscaler for the ZIA service, and the ServiceNow SSO configuration to forward auth requests to Zscaler. Once the user’s identity has been verified their traffic to and from ServiceNow is secured and the user and the ServiceNow data is inspected using Zscaler Internet Access.

Zscaler Internet Access sits between your users and ServiceNow, inspecting every byte of traffic inline across multiple security techniques, even within SSL. You get full protection from web and internet threats. And with a cloud platform that supports Cloud Firewall, Cloud IPS, Cloud Sandbox, Cloud DLP, CASB and Cloud Browser Isolation, you can start with the services you need today and activate others as your needs grow.
2.1 Configure the SaaS Identity Proxy

Figure 8: Configure The SaaS Identity Proxy

- Log into the Zscaler Tenant with Administrator Credentials
2.2 Configure the Zscaler Portal for the SaaS Identity Proxy

To configure Zscaler for the SaaS Identity Proxy:

- Select Administration / Identity Proxy Settings
- Then Select Add Cloud Application (This will open the configuration Wizard)
- Give the Cloud Application a Name
- Select Enable
- For Cloud Application Select ServiceNow
- Set the ACS URL to https://your-servicenow-instance.service-now.com/navpage.do
- Set the Entity ID to https://your-servicenow-instance.service-now.com
- Select the SAML_2022 or Later Signing Certificate
- Select Pass-through Zscaler Identity for the Identity Transformation
- Select Save
2.2.1 Configure the SaaS Identity Proxy

This is the completed Identity Proxy configuration on the Zscaler Tenant. We need to copy and save the Identity Proxy URL and the Issuer Entity ID for later in the ServiceNow configuration. We also need to download and save the Signing Certificate.

- Copy and Save the **Identity Proxy URL**
- Copy and Save Issuer **Entity ID**
- Download and Save the **Signing Certificate**
2.3 Configure ServiceNow to use the Identity Proxy

Figure 11: Configure ServiceNow for the Identity Proxy

- Log into the ServiceNow Tenant with Administrator Credentials
2.4 Install the ServiceNow Plugins

Figure 12: Configure the ServiceNow Plugins

- In the Filter Navigator search for “system app”
- Select All Available Applications
- Then Select All to display all available plugins
- Filter for “multiple provider”
- Click Install for the “Integration – Multiple Provider Single Sign-On Enhanced UI”
- Then Click Activate

This will install both the Multiple Provider Single Sign-On Enhanced UI and the Multiple Provider Single Sign-On Enhanced plugins, which we will configure for the Zscaler Identity Proxy.
2.5 Configure the SaaS Identity Proxy

Figure 13: Enable Multiple Provider SSO

- In the Filter Navigator search for “multi”
- Under Multi-Provider SSO Select Administration
- Then Select Properties

This will bring up the Customization Properties for Multiple Provider SSO page.

- Select Yes to Enable multiple provider SSO
- Select Yes to Enable Auto Importing of users from all identity providers into the user table
- Select Yes to Enable debug logging for the multiple provider SSO integration
- Then Select Save
2.6 Add Zscaler as an Identity Provider

The next step is to add the Zscaler Identity Proxy as an Identity Provider.

- In the configuration pane select **Identity Providers**
- Then Select **New**

**Figure 14: Configure the Identity Provider**
2.6.1 Add Zscaler as an Identity Provider

Figure 15: Configure The SaaS Identity Proxy

- Select SAML
2.7 Configure the Identity Provider

![Image of Identity Provider configuration screen]

**Figure 16: Configure the Identity Provider**

- In the Identity Provider New Record Window give the Template a **Name**
- In the Identity Provider URL Field paste in the **Issuer Entity Id** from the Zscaler Config
- In the Identity Provider’s AuthnRequest URL Field paste in the **Identity Proxy URL**
- For the Identity Provider’s SingleLogoutRequest Enter `http://logout.zscaler.net`
- For the ServiceNow Homepage URL Enter your **ServiceNow Instance/navpage.do**
- For the Entity ID / Issuer, and the Audience URI, Enter your **ServiceNow Instance**
- For the NameID Policy Enter `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
- Then Select the **Advanced Tab**
- For the Single Sign-On Script Search and Select the **MultiSSOv2_SAML2_custom Script**
- Select **Force AuthnRequest**
- The Select **Submit**
2.8 Add the Identity Provider Certificate and Additional Settings

Not all features are available in the first configuration screen until it has been submitted. We need to go back into the Identity Provider to finish the configuration, test the IdP and to activate it.

- Select the Zscaler Identity Provider
2.8.1 Add the Identity Provider Certificate

Figure 18: Add the Signing Certificate

The option to add the Zscaler Certificate is now available at the bottom of the configuration screen. To configure and add the Certificate:

- Select New
2.8.2 Add the Identity Provider Certificate

The process to add the Certificate is very manual.

- Name the Certificate
- Open the Certificate file from Zscaler and Copy the entire contents
- Paste the contents into the PEM Certificate Field
- Select Submit

NOTE: The certificate is one continuous line. Remove any carriage returns.
2.8.3 Additional Configuration Settings

- Select Default
- Select Set as Auto Redirect IdP
- The final step is to Select Test before we can Activate the IdP

This will open a test window and will bring up the Authentication Screen from the IdP that is configured on Zscaler. If Okta or AZURE AD are set as the IdP, you will get that Authentication Prompt. If successful you will be able to Activate the Identity Provider. You may be able to Activate the Identity Proxy without seeing the following screen, or you may need to Activate it on the Test screen.

NOTE: You may need to run the Test more than once to enable the Identity Provider. If Auto Redirect fails to enable, use the following Configure Redirect on the IdP procedures.
2.9 Testing the Identity Provider

Figure 21: Testing the Identity Provider

If everything is configured correctly this should be the screen we see when testing the Identity Provider, and anytime a change is made to the Identity Proxy you will need to re-test the Identity Proxy. This screen has good test results. The Logout Test Results are expected to fail.

- Select Activate
2.10 The Active Identity Proxy Notification

This is the Notification a ServiceNow user will receive if they are trying to log into ServiceNow without going through Zscaler. When your user traffic is going through Zscaler they will be able to access ServiceNow as usual.

Figure 22: The Active Authentication Proxy
2.11 Configure Redirect on the Identity Provider

This procedure is only for the case that the Auto Redirect IdP will not enable from the Configuration Screen. We need to set a System Property to enable redirect by default to our IdP.

- Go to the Identity Provider Page
- Left Click on the Zscaler Identity Provider and copy the sys_id
2.11.1 Configure the System Property for a Redirect

Figure 24: Systems Properties

- Search for sys_properties.LIST in the Filter Navigator
- Hit Return

This will launch a new window or tab with all available Systems Properties.
2.11.2 Configure the Identity Provider Redirect

In the Systems Property Screen, Search for and Edit the Systems Property glide.authentication.sso.redirect.idp. This will launch the edit screen for the Property.

- Search for glide.authenticate.sso.redirect.idp
- Select glide.authenticate.sso.redirect.idp
2.11.3 Configure the Property

Figure 26: Configure the Identity Provider

In the Systems Property Screen, Search for and Edit the Systems Property glide.authenticate.sso.redirect.idp.

- In the Value Field paste in the sys_id from our IdP
- Select Update
3 Configure Cloud Browser Isolation

**Figure 27: Zscaler Internet Access Cloud Browser Isolation in Use with ServiceNow**

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

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

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

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

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

- Log into the Zscaler Browser Isolation Tenant with Administrator Credentials
3.1.1 Configure the Cloud Browser Isolation Profile

A Browser Isolation Profile or multiple profiles need to be configured to enable the Zscaler Cloud Browser Isolation Features that will be applied specifically for ServiceNow and the individual user using Browser Isolation. This could be a generic profile for all SaaS applications, or it could be 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 and paste for another. To start the Policy Wizard, follow the below procedures.

- Select Isolation profiles
- Select the ZIA Tab
- Select Add New
3.1.2 Configure the Cloud Browser Isolation Profile

![Cloud Browser Isolation General Information](image)

**Figure 30: Cloud Browser Isolation General Information**

This will start the Browser Isolation Wizard and will step you through enabling General Information, Company Settings, Security Controls, Regional Connectivity, and the End User Notification. For General Information give the profile an intuitive name and description. It will be selected in the Isolation Policy on the ZIA portal and should be clear to the use case.

- Name the Profile
- Give the Profile a detailed Description
3.1.3 Configure the Cloud Browser Isolation Profile

For the ZIA Company Settings, you must select your Company ID and Cloud if your information is not populated automatically. This information can be obtained from your ZIA Portal under Administration / Company.

- Select your Company ID and Zscaler Cloud
- Leave the Zscaler Root Certificate as the Default Certificate
- Select Next to proceed in the Wizard
3.1.4 Configure the Cloud Browser Isolation Profile

The Security Control of Browser Isolation 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 and Paste up to or down from ServiceNow from/to the local computer. You can also control File Transfers up to or down from ServiceNow from/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 we are going to maintain the strictest security settings and not enable any controls.

- Select Next
3.1.5 Configure the Cloud Browser Isolation Profile

Figure 33: Cloud Browser Isolation Regions

Two Regions must be selected for redundancy. Select the two closest regions to your organization.

- Select Two Regions for Redundancy
- Select Next
3.1.6 Configure the Cloud Browser Isolation Profile

We will use the default End User Notification. However, a customized EUN can be created in the Administration section of the Browser Isolation Portal and added to our Profile. To complete our Profile, select the Create Profile button.

- Select Create Profile
3.1.7 Configure the Cloud Browser Isolation Profile

![Figure 35: The Completed Cloud Browser Isolation Profile](image)

Our completed Zscaler Cloud Browser Isolation Profile. This will appear as a profile option when setting up isolation policies in Zscaler Internet Access. Let’s setup our Zscaler Isolation Policies in the Zscaler Internet Access portal. To move to next steps, launch your Zscaler Internet Access Portal and sign in with Administrator Credentials.

- Launch your Zscaler Portal
3.2 Configure the Cloud Browser Isolation Policies

Figure 36: Configure Cloud Browser Isolation

- Log into the Zscaler Tenant with Administrator Credentials
3.2.1 Configure the Cloud Browser Isolation Policies

To begin the policy configuration to redirect ServiceNow traffic to Cloud Browser Isolation. Launch the URL Filtering Wizard by following the below steps.

- Select Policy
- Select URL & Cloud App Control
- Select Add URL Filtering Rule

![Figure 37: Configure Cloud Browser Isolation Policies](image)
3.2.2 Configure the Cloud Browser Isolation Policies

In the URL Rule Wizard Select the Rule Order based on your current policy processing and enable the rule under Rule Status. Select the arrow in URL Categories and then select the plus sign on the URL Selection Screen to add the ServiceNow URLs.

- Select the Rule Order
- Name the Rule in the Rule Name Field
- Enable the Rule
- Select the Dropdown Arrow in the URL Categories Field
- Select the Plus Sign next to the Search Field on the URL Selection Screen (New Page)
3.2.3 Configure the Cloud Browser Isolation Policies

This will bring up the Add URL Category Wizard. We need to add the two ServiceNow URLs as Custom URLs.

- Name the URL Category
- Add ".servicenow.com” and “.service-now.com” by typing the domain in the Add Items Field and selecting Add Items, one at a time. Leave the period in front of the URL to act as a Wildcard for the domain
- Select Save
3.2.4 Configure the Cloud Browser Isolation Policies

Scroll down the Wizard to fill in the remaining fields.

- For Request Methods Select CONNECT, GET, HEAD, and TRACE
- For Protocols Select HTTP, and HTTPS
- For User Agent Select your Organizations Specific Browsers for use with Browser Isolation
- Select Save to Complete our Configuration
3.2.5 Configure the Cloud Browser Isolation Policies

**Figure 41: Configure Cloud Browser Isolation**

The Completed Browser Isolation Profile.
4 Configuring the Service Now Tenant

Log into your ZIA tenant with Admin credentials to start the installation process. Your Zscaler Cloud Instance may be different from the example. The current Zscaler Internet Access clouds include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.
4.1 Adding the Service Now Tenant

To launch the SaaS Application Tenants Wizard for the ZIA Admin Interface:

- Select Administration
- Select SaaS Application Tenants
- On the SaaS Applications Tenants page Select “Add SaaS Application Tenant”
4.2 SaaS Tenant Configuration Wizard

To start the Wizard select Add SaaS Application Tenant. The above Wizard will then appear. Select the ServiceNow Tile under popular applications to move to the next step in the Wizard.

- Select Add SaaS Application Tenant on the Tenant page
- Select the ServiceNow tile on the Wizard
4.2.1 SaaS Tenant Configuration Wizard

![Add SaaS Application Tenant](image)

**Figure 45: Open the ServiceNow Tenant**

Give the ServiceNow tenant a name. This will be the name that will be selected when assigning a policy for the Zscaler security features.

- Enter a name for the Tenant Name
- Open a new browser tab and login to your ServiceNow Tenant with Admin role credentials
4.3 Configuring the Zscaler Tenant on ServiceNow

Figure 46: Login to the ServiceNow Tenant

To configure the Zscaler Tenant from your ServiceNow Admin account.

- Log in to ServiceNow with Administrator Credentials
4.3.1 Configuring the Zscaler Tenant on ServiceNow

We need to verify OAuth is running and start it if it is not Active.

- On the left-hand pane Select the File Box at the top of the browser, under the Filter Navigator
- Scroll down and Select the Arrow next to All Available Applications
- Select All

This will show the All Applications Page

- In the Search Box type “Oath 2.0”
- Verify OAuth is Installed

If OAuth is not installed

- Select Install
- Select Activate
4.4 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 will bring up the Status Page of the OAuth 2.0 Application
4.4.1 Check that the OAuth Plugin is Active

Figure 49: OAuth Plugin Status

- Check that the Status of OAuth 2.0 is Active
4.5 Create an OAuth Application Registry

We need to create an Oath application registry for the Zscaler Tenant.

- On the left-hand pane Select the File Box at the top of the Browser, under the Filter Navigator
- Scroll down and Select System OAuth
- Select Application Registry
- Then Select New
4.5.1 Create an OAuth Application Registry

In the dialog box asking, “What kind of OAuth Application?”

- Select “Create an OAuth API endpoint for external clients”
4.5.2 Configuring the Zscaler Tenant on ServiceNow

Complete the OAuth API endpoint details

- Enter Zscaler (Can be a different name) for the name of the endpoint
- Enter the Token Lifespan in seconds. 157,700,000 is 5 years at which point the Tenant will have to be reinstalled
- Enter the Access Token Lifespan in seconds. 86,400 is 24 hours and the recommended duration by Zscaler
- Enter Submit to save the settings

Note: The Client Secret will be created after the detail is Submitted. We will need to go back into the endpoint to copy it for the Zscaler configuration.
4.5.3 Configuring the Zscaler Tenant on ServiceNow

The Zscaler Endpoint is created.

- Select the Zscaler endpoint to open the settings to copy the Client Secret
4.5.4 Copy the needed Oath Credentials

Copy the OAuth credentials required to finish the Zscaler side installation.

- Copy the Client ID
- Select the lock next to the Client Secret to reveal the secret
- Copy the Client Secret

We are now finished with the ServiceNow side tenant configuration!
4.5.5 Finishing the Zscaler Tenant on the Zscaler

Figure 55: Finish the Zscaler Tenant

Let's finish the Zscaler API Tenant by entering the information copied from the ServiceNow Tenant

- Enter the ServiceNow Client ID
- Enter the ServiceNow Client Secret
- Enter the ServiceNow Instance URL
- Enter the ServiceNow User ID and Password
- And finally Enter the Admin ID, for me this is the same Admin User
- Select Authorize to verify the credentials and if successful, Select Save
4.5.6 Configuring the Zscaler ServiceNow Connector

Figure 56: The Completed and Active ServiceNow Tenant

The Completed and Active ServiceNow API connector.
5 Configuring ServiceNow Policies and Scan Configuration

![Zscaler Policy Configuration Diagram]

*Figure 57: Zscaler Policy Configuration*

After adding and configuring the ServiceNow tenant, you can configure the SaaS Security API Control DLP and Malware policies and the Scan Configuration for the policies. You can also view reports and data for ServiceNow in Analytics, SaaS Security Insights, and Logs.
5.1 Scoping the Policies and Remediation

Zscaler SaaS Security scans file attachments. For this Deployment Guide, we will configure a basic DLP policy and a Malware policy to scan the ServiceNow account attachment files for matching content of the DLP policy, and to scan the files for known malware for the malware policy. A ServiceNow Incident has been created with malicious attachments and DLP violations to test our 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.

For our DLP policy we are going create a very broad DLP policy to identify a spreadsheet with a list of US Social Security Numbers. Data Loss Protection is a subject of its own, and this policy is only used only for demonstration purposes. A true DLP policy review would need to be conducted to minimize false positives and false negatives.

It is also important to note, the 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 will not cover Inline Data Protection, Exact Data Match, or Indexed Document Matching (Document Template Finger Printing), although they are integral pieces of a complete Data Protection solution.

For next steps to test the DLP SaaS functionality we will create a basic policy and apply it to our ServiceNow tenant. If you already have DLP policies created skip ahead to Section 4.
5.2 Creating a DLP Policy

The procedures for creating a DLP policy are straight forward. Create a custom dictionary, or use the available dictionaries, to identify the data the scan is going to look for.

Then an engine is created which is the logical template for adding expressions and additional data. This is where you would specify Social Security Numbers AND any other criteria for the policy. The Engine provides the means to precisely add or remove data to match our violation and eliminate false positives.

A SaaS Security DLP policy is then created which allows us to specify the detail about where, when, the action taken, and whom to inform about Violations. Finally, the DLP policy is then applied to our ServiceNow tenant. Let’s verify our DLP dictionary as next steps. In the ZIA UI.

- Select Administration
- Select DLP Dictionaries and Engines
- Select DLP Dictionaries
- Identify and Select the Dictionary to be used (In this case SSN with Dashes)
5.3 Creating a DLP Engine

To create the DLP engine.

- Select the DLP Engines Tab
- Select Add DLP Engine
5.3.1 Creating a DLP Engine

Figure 61: The DLP Engine Wizard

- Give the DLP Engine a Name
- In the Engine Builder under Expression select the first dictionary
- Specify the Match Count, which is the minimum number of instances the data must occur in the file
- Select ADD to add our next dictionary and repeat the process.
- Select Save to save the configuration
- Activate the Configuration

Note: This policy will trigger when we see the 4th Social Security Number. Again, this in a demonstration and the criteria is too general to be a production DLP rule.
5.4 Configure a SaaS DLP Policy

Figure 62: Launch the SaaS DLP Policy Configuration Wizard

Now let’s apply the engine to a DLP policy that will be used for our ServiceNow instance. Launch the DLP Rule Wizard to start the process.

- Select Policy / SaaS Security API / Data Loss Prevention
- Select ITSM
- Select Add DLP Rule

See detail of the policy on the following pages.
5.5 SaaS DLP Policy Details

The SaaS DLP Policy is like all Zscaler Policies where you will specify the detail on whom this policy, and to what data this policy will apply to. You will specify the rule order if you have multiple DLP policies which are processed in an ascending manner. The first rule that matches will be the applied rule. We will specify the DLP Engine we have 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 and are explained below for clarification. For our Policy we will select Any Collaboration, and an Action of Remove Sharing.

**Collaboration Scope:** The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select *Any* to apply the rule to files with all collaboration levels, or select any number of the following collaboration scopes and specify the permissions for each scope:

- **External Collaborators:** Files that are shared with specific collaborators outside of your organization.
- **External Link:** Files with shareable links that allow anyone outside your organization to find the files and have access.
- **Internal Collaborators:** Files that are shared with specific collaborators or are discoverable within your organization.
- **Internal Link:** Files with shareable links that allow anyone within your organization to find the files and have access.
- **Private:** Files that are only accessible to the owner.

**The Action** the rule takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For ServiceNow the action is Report Only. This means that any violations will be reported in the Zscaler SaaS Analytics and Alerts will be sent to Auditors if defined.

- **Report Incident Only:** The rule reports the incident only and makes no changes to the file’s collaboration scope.
5.5.1 Configure a SaaS DLP Policy

Figure 63: The SaaS DLP Policy Configuration Wizard

To Finish our DLP Policy

- Specify the Rule order for Processing (The first rule matched will be executed)
- Name the Rule
- Enable the Rule
- Select the ServiceNow SaaS Tenant
- Select the DLP Engine created in the last step
- Select Any-Any for the Collaboration Scope
- Select High as a Severity to allow for identification for searches and tracking
- Save and Activate your configuration
5.5.2 Configure a SaaS DLP Policy

![Image of Configure DLP Policy](image)

**Figure 64: The Configure DLP Policy**

The completed DLP rule ready to be applied with a scanning schedule.
6 Configure a SaaS Malware Policy

To Launch the Malware Rule Wizard:

- Select Policy / SaaS Security API / Malware Detection
- Select ITSM
- Select Add Malware Detection Rule

The SaaS Malware Detection Policy is an all-encompassing policy and all files in the Tenant will be scanned unless removed from the scope by specifying any exemptions by selecting the Exemption Tab under Malware Detection. To add a malware policy, we will specify the Application, the SaaS Tenant, and the Status.

The Action for ServiceNow is limited to Report Malware only.
6.1 SaaS Malware Policy Wizard

Configure the Malware Rule Wizard.

- Select Policy / SaaS Security API / Malware Detection
- Select ITSM

- Select Add Malware Detection Rule
- Under Criteria Select ServiceNow as the Application
- Select the ServiceNow SaaS Tenant to apply the policy
- Select Enabled for Status
- Select Save
6.1.1 SaaS Malware Policy

![Image of SaaS Security API Control with policy settings]

**Figure 67: The Completed Malware Policy Configuration Wizard**

The completed SaaS Security Malware policy for the ServiceNow SaaS Tenant ready to be applied to our ServiceNow instance with a Scanning Schedule.

- Activate your configuration
Configure the Scan Schedule Configuration

Figure 68: Create and Enable a Scan for the SaaS Tenant

The final configuration step is to create a Scan Configuration. We will specify the Tenant the Scan Configuration applies to, any policies that are to be included in the scan, and what data to scan relative to a date. The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. For this deployment Guide we will select All Data. However, if this is a POV or a Trial, the only option available will be New Data Only.

To add a Scan Schedule.

- Select Policy / SaaS Security API / Scan Configuration / Add Scan Schedule
- Select the ServiceNow SaaS Tenant for the SaaS Application Tenant
- Select the Data Loss Policy and the Malware Policy Created in Prior Steps
- Select All Data or for a POV Select New Data Only
- Select Save to save the Scan Schedule and Activate the configuration
7.1 Start the Scan Schedule

Once the Schedule has been configured and saved, we need to start the Scan for our DLP Policy and Malware policy to be applied.

- Select the Blue Arrow on the Scan configuration to start SaaS API Security on the ServiceNow Tenant

The Status should say Running with a Start Date and a Latest Scan Date.
8 Reporting and Visibility

Zscaler Analytics provide detailed reporting of all user activity down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of Data-at-Rest associated with the user. For our SaaS partners Zscaler provides Reports and SaaS Security Insights. This provides visibility from a high-level overview to management of the individual logs and violations.

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

Figure 70: SaaS Security Visibility
8.1 SaaS Assets and SaaS Assets Summary Report

The SaaS Asset Reports provide a summary or customizable reporting to have a quick view of your files and emails. The above is the SaaS Assets Summary Report, which provides all activity and violations in a quick glance. The report identifies all SaaS Tenant information from a single screen. Our ServiceNow activity over the creation of this Deployment Guide is shown above, but any Tenant configured will also be displayed on this summary screen. The data is hyperlinked, and you can easily pivot from a Summary to individual logs and activities provided by SaaS Security Insights.

- Select the 20 Total Violations next to ServiceNow to pivot to SaaS Security Insights

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

![Image of SaaS Security Insights]

Figure 72: SaaS Security Insight

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

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

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

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

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

Let’s define a Cloud Application Control Policy to allow only users in a ServiceNow security group to access ServiceNow and block access for all other users. This will require two policies, one policy to allow our specific users and one to block all other users.
9.1 Cloud Application Access Control Policy

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

- Sign into your organizations ZIA UI with Administrator Credentials
- Select Policy
- Select URL & Cloud App Control
- Select the Cloud App Control Policy Tab
- Select Add
- Select Productivity & CRM Tools

This will launch the Policy Wizard to create the policy.
9.2 Cloud Application Access Control Policy Wizard

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

- Set the Rule Order to 1
- Set the Rule Name to an intuitive name
- Select ServiceNow for the Cloud Application
- Select the Security Group that contains our ServiceNow Admins and Users
- For Application Access select Allow
- Select Save to save our changes
9.2.1 Cloud Application Access Control – Deny Policy

To create our policy to deny all other users please follow the below steps.

- Select URL & Cloud App Control
- Select the Cloud App Control Policy Tab
- Select Add
- Select Productivity & CRM Tools
- Set the Rule Order to 2 (Must be after our Allow Policy)
- Set the Rule Name to an intuitive name
- Select ServiceNow for the Cloud Application
- Leave all other Settings as “Any”
- For Application Access select Block
- Select Save to save our changes

Figure 76: Create a Cloud App Control Deny Policy
9.2.2 Cloud Application Access Control

![Image of Cloud Application Access Control](image)

**Figure 77: Create a Cloud App Control Deny Policy**

Our completed Access Policies.

- Activate the Policy additions

Users who try to access the ServiceNow application through Zscaler who do not have permission will have the Website blocked Pop-up screen above displayed on their browser. The Zscaler administrators will receive alerts and logs to the event.
9.3 Cloud Application Access 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 timeframe, follow the below steps.

- Sign into your organizations ZIA UI with Administrator Credentials
- Select Analytics
- Select Web Insights
- Select the Logs Tab
- Select the desired time frame, or custom time frame
- Select Add Filter
- Select Cloud Application
- Select ServiceNow
- Apply Filters
ZDX has become the missing link needed for our customers and their SaaS applications. As applications move to the cloud, the Internet becomes your new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. ServiceNow is no exception to this and Zscaler ZDX provides visibility into the client’s experience using ServiceNow. ZDX utilizes the Zscaler Endpoint Client Connector to generate application and network probes and gather device health. ZDX is a separate service from ZIA SaaS Security and can run with or without SaaS Security being enabled.

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

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

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

- Log Into your organizations ZDX portal

Figure 80: ZDX for User Experience Monitoring for ServiceNow

Log into the ZDX Portal with Administrator credentials to begin the configuration process.
10.1.1 Configure ZDX for ServiceNow

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

- Select Configuration
- Select Applications
- Select the blue arrow next to the ServiceNow App
- Enter the URL for your ServiceNow Tenant Login
- Select Submit to Onboard ServiceNow
10.2 Configure Probes for ServiceNow Monitoring

Once the Submit button is clicked, the ServiceNow app is enabled for monitoring and the pre-configured probes are displayed. The probes consist of a CloudPath Probe which utilizes ICMP Trace Route, and a Landing Page Probe to the dev1023676.service-now.com location to monitor page load times.

We are going to make one change to the CloudPath Probe to have it follow the path of the Landing Page Probe so there is no confusion of the results since this is entirely for ServiceNow monitoring.

To edit the rule:

- Activate the Changes first and then
- Select the blue pencil to edit the probe
10.2.1 Configure Probes for ServiceNow Monitoring

Figure 83: Edit the Network Probe

- Select ServiceNow Account Login Page Probe under Follow Web Probe
- Select Next
10.2.2 Configure Probes for ServiceNow Monitoring

- Validate the destination host to Monitor it should be to your ServiceNow Login URL
- Select Next
- Review and Activate the changes to the Probe
10.3 The ZDX Enabled ServiceNow Application

![Figure 85: Active ServiceNow Monitoring](image)

The ServiceNow application monitoring has now been activated and our Probes will begin from all of our users that are using the Zscaler Client Connector (ZCC). The above figure shows ZCC running the Digital Experience and the Service is On.
10.4 Create an Alert for the ServiceNow Service

As a final configuration step let’s create an alert to email us when there is service degradation of the ServiceNow application. An alert can be configured for Network, Application, or Device thresholds. An Alert Rule can be created with any of the below information.

**Network Probe:** Latency, MTR, Packet Loss, Number of Hops

**Application Probe:** DNS Response Time, Page Fetch Time, Server Response Time, Web Request Availability

**Device Monitor:** CPU Usage, Bandwidth, Battery, CPU, Disk, WIFI Signal Strength, Memory, Sent and Received Mbps

To Create our alert on Page Fetch Times.

- Select Alerts
- Select Rules
- Select Add New Alert Rule
10.4.1 Create an Alert for the ServiceNow Service

**Figure 87: The Alert Creation Wizard**

Step One of the rule Wizard.

- Name the Rule
- Select Enable Under Status
- Give the Alert an appropriate Severity
- Select a Type of Application
- Select Next
10.4.2 Create an Alert for the ServiceNow Service

Figure 88: The Alert Creation Wizard

Step Two of the rule Wizard.

- Select ServiceNow as the application
- Select ServiceNow Landing Page Probe
- Select Next
10.4.3 Create an Alert for the ServiceNow Service

Step Three of the rule Wizard we will create the criteria for which the Alert will trigger if the threshold is exceeded. We can use multiple variables here to eliminate false positive.

- Select Page Fetch Time
- Select the time to exceed 5000ms (5 Seconds)
- Select Next

Figure 89: The Alert Creation Wizard
10.4.4 Create an Alert for the ServiceNow Service

Figure 90: The Alert Creation Wizard

Step Four of the rule Wizard we will add Throttling to control the scope of the Alert. We will then define the Action as Email. The action can also be defined as an authenticated Webhook, which could be used to send the Alert to a Slack Channel.

- Enter “10” for the number of times the Probe time must exceed our threshold
- Select 10 Percent for the Minimum Number of Devices that must be impacted
- Select Email as the Delivery Method
- Enter the Recipients email address separated by commas
10.4.5 Create an Alert for the ServiceNow Service

![Alerts Rules](image)

**Figure 91: The Completed Rule Set**

Our Completed Rule Set for the Alert.
10.5 The Triggered Alert for the ServiceNow Service

The above is the triggered alert generated by our Threshold Settings in our Rule Set being exceeded. You can click on the Rule Name or click the eye to see more detail about the Alert.

Figure 92: The Alert
10.6 Alert Detail for the ServiceNow Service

The above is the triggered alert detail for our triggered alert showing impacted user and devices, impact location, and threshold details.
10.7 The Sent Alert Email for the ServiceNow Service

The above is the Email Alert that was sent to the recipients once our threshold was exceeded. Another email will be sent when the threshold returns to normal values if the alert was an ongoing or continuous alert.

Figure 94: The Alert Email
11 Using ZDX – The Dashboard

The Dashboard provides single page to monitor the user experience (ZDX Score) of all users and all applications. An active heat map will also show you any locations globally that may be having issues.

Figure 95: The Dashboard
11.1 Application Overview

Selecting the Applications Tile on the left of the UI will bring up the Applications Overview and will show all the configured applications and the individual ZDX score. Let’s look at the detail of our ServiceNow application.

- Select Applications
- Select the ServiceNow App
11.2 ServiceNow Application Performance Detail

Figure 97: Application Detail

The top portion of the application detail shows a historical view of the ZDX score and the Page Fetch Time. The Spike of the page fetch time indicates a possible slowdown of the ServiceNow service itself.
11.2.1 ServiceNow Application Performance Detail

Figure 98: Application Detail

The bottom portion of the App detail show the Top Zcaler Locations, Top Cities, and the Top Departments using the Application and the ZDX Scores at a glance. We also see our probe data, with minimum, maximum, and average response times.
11.3 User Overview

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

Figure 99: User Overview
11.4 ServiceNow User Detail

The User Detail will show an incredible amount of useful 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 will provide the Users Devices and will provide the device specific detail (OS, Device type, Network Information, etc...) by clicking on the device. The ZDX score is also displayed in a timeline, and detail of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health can all be seen from this page.

Figure 100: User Detail
11.4.1 User Detail

The above 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.
12 ZCSPM – ServiceNow Integration for Ticket Creation

ZCSPM supports integration with ticketing systems to automatically log incidents when a misconfiguration or compliance violation is discovered by ZSCPM in the monitored production environment. Incident Management (Ticketing) allows integrations with ServiceNow.

The process to configure the integration will include the steps below.

- Configure Ticketing System Integration for ServiceNow ZCSPM License Admin
- Configure Incident Management ZCSPM Subscription Owner
- Verify Ticket Creation ServiceNow Admin
12.1 Configure ServiceNow Ticketing Integration

To configure the ServiceNow ticketing system integration:

- Log in to the ZCSPM portal as a License Admin
- Navigate to Configurations, then select Integrations
- On the Incident Management (Ticketing) card, click Edit

Figure 103: Configure the Ticketing System Integration for ServiceNow
12.1.1 ZCSPM Incident Management

![Configure Incident Management](image)

**Figure 104: Select and Configure ServiceNow**

On the Configure Incident Management Page.

- For Ticketing System select ServiceNow
- Select Ticket Creation Frequency of Incident Creation
- Click Configure

A Configure Service Now window appears.
12.1.2 ZCSPM ServiceNow Account and Credentials

Figure 105: User Detail – End to End Connection Detail

- For Instance Name, type in the ServiceNow instance name
- For Instance Username, type in the admin's username for the ServiceNow instance
- For Instance Password, type in the admin's password for the ServiceNow instance
- For Assign Ticket To, Enter an email address. Tickets from the ServiceNow instance will be assigned to this Email
- Click Save
12.1.3 ZCSPM – Configuration Validated

![Figure 106: Successful Integration](image)

If ZCSPM connects to the ServiceNow Tenant using the supplied Credentials, the ZCSPM configuration will show a checkmark verifying connectivity.

- Click Save

This Integration Configuration between ZCSPM and ServiceNow is now complete, and Violations will be reported daily. Additional configuration can be made to prioritize created Incidents on a per Cloud Service basis.

Next Let’s verify Incidents are being created as expected.
12.1.4 ServiceNow Incidents

Figure 107: ZCSPM Created ServiceNow Incident

ZCSPM will create incident, Problems, or Problem Tasks for workflow management of Security and Compliance Violations ZCSPM finds in your monitored cloud services. The ServiceNow entries will contain the below fields by default and additional customization can be applied if desired.

Incident will include a Short Description, a more Detailed Description, Problem ID, State, Priority, Urgency, Impact, Assigned To, and a Caller ID.

Problem Task will include a Short Description, more Detailed Description, Problem, Workaround, Problem Task Type.

Problem will include a Short Description, more Detailed Description.
13 Appendix A:

13.1 Zscaler Resources

Zscaler Internet Access (ZIA)
https://www.zscaler.com/products/zscaler-internet-access

Adding SaaS Application Tenant
https://help.zscaler.com/zia/adding-saas-application-tenants

About SaaS Application Tenant
https://help.zscaler.com/zia/about-saas-application-tenants

SaaS Security API DLP Policy

About Data Loss Prevention

About DLP Dictionaries

About DLP Engines

SaaS Security Insights

SaaS Posture Security

Cloud Application Access Control
https://help.zscaler.com/zia/about-cloud-app-control

SaaS Identity Proxy

ZDX
https://help.zscaler.com/zdx

ZDX Predefined Applications
https://help.zscaler.com/zdx/predefined-applications-zdx
13.2 ServiceNow.com Resources

About ServiceNow
https://www.servicenow.com/company.html

ServiceNow Developer Account

ServiceNow Product Documentation
https://docs.servicenow.com/

ServiceNow Community
https://community.servicenow.com/community

ServiceNow Support
https://support.servicenow.com/hisp