# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terms and Acronyms</td>
<td>6</td>
</tr>
<tr>
<td>About This Document</td>
<td>7</td>
</tr>
<tr>
<td>Zscaler Overview</td>
<td>7</td>
</tr>
<tr>
<td>Zscaler Internet Access (ZIA) Overview</td>
<td>7</td>
</tr>
<tr>
<td>Zscaler Private Access (ZPA) Overview</td>
<td>7</td>
</tr>
<tr>
<td>Zscaler Resources</td>
<td>8</td>
</tr>
<tr>
<td>ServiceNow Overview</td>
<td>8</td>
</tr>
<tr>
<td>ServiceNow Resources</td>
<td>9</td>
</tr>
<tr>
<td>Audience</td>
<td>9</td>
</tr>
<tr>
<td>Software Versions</td>
<td>9</td>
</tr>
<tr>
<td>Request for Comments</td>
<td>9</td>
</tr>
<tr>
<td>Zscaler Data Protection and Digital Experience for ServiceNow.com</td>
<td>10</td>
</tr>
<tr>
<td>ZIA SaaS Identity Proxy</td>
<td>11</td>
</tr>
<tr>
<td>ZIA Browser Isolation</td>
<td>12</td>
</tr>
<tr>
<td>ZIA CASB Data Loss Protection and Malware Detection for ServiceNow</td>
<td>13</td>
</tr>
<tr>
<td>What makes our SaaS Security unique?</td>
<td>13</td>
</tr>
<tr>
<td>ZIA Cloud Application Control</td>
<td>14</td>
</tr>
<tr>
<td>Zscaler Digital Experience for the ServiceNow User Experience</td>
<td>15</td>
</tr>
<tr>
<td>What makes the Zscaler Digital Experience unique?</td>
<td>15</td>
</tr>
<tr>
<td>Zscaler Cloud Security Posture Management ServiceNow Incident Creation</td>
<td>16</td>
</tr>
<tr>
<td>Configure the SaaS Identity Proxy</td>
<td>17</td>
</tr>
<tr>
<td>Configure the SaaS Identity Proxy</td>
<td>18</td>
</tr>
<tr>
<td>Configure the Zscaler Portal for the SaaS Identity Proxy</td>
<td>19</td>
</tr>
<tr>
<td>Configure the SaaS Identity Proxy</td>
<td>20</td>
</tr>
<tr>
<td>Configure ServiceNow to use the Identity Proxy</td>
<td>21</td>
</tr>
<tr>
<td>Install the ServiceNow Plugins</td>
<td>22</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configure the SaaS Identity Proxy</td>
<td>23</td>
</tr>
<tr>
<td>Add Zscaler as an Identity Provider</td>
<td>24</td>
</tr>
<tr>
<td>Configure the Identity Provider</td>
<td>25</td>
</tr>
<tr>
<td>Add the Identity Provider Certificate and Additional Settings</td>
<td>26</td>
</tr>
<tr>
<td>Testing the Identity Provider</td>
<td>29</td>
</tr>
<tr>
<td>The Active Identity Proxy Notification</td>
<td>30</td>
</tr>
<tr>
<td>Configure Redirect on the Identity Provider</td>
<td>31</td>
</tr>
<tr>
<td>Configure the Property</td>
<td>34</td>
</tr>
<tr>
<td>Configure Cloud Browser Isolation</td>
<td>35</td>
</tr>
<tr>
<td>Configure the Cloud Browser Isolation Profile</td>
<td>36</td>
</tr>
<tr>
<td>Configure the Cloud Browser Isolation Policies</td>
<td>44</td>
</tr>
<tr>
<td>Configuring the Service Now Tenant</td>
<td>50</td>
</tr>
<tr>
<td>Adding the Service Now Tenant</td>
<td>51</td>
</tr>
<tr>
<td>SaaS Tenant Configuration Wizard</td>
<td>52</td>
</tr>
<tr>
<td>Configuring the Zscaler Tenant on ServiceNow</td>
<td>54</td>
</tr>
<tr>
<td>Check that OAuth is Installed and Active</td>
<td>56</td>
</tr>
<tr>
<td>Check that the OAuth Plugin is Active</td>
<td>57</td>
</tr>
<tr>
<td>Create an OAuth Application Registry</td>
<td>58</td>
</tr>
<tr>
<td>Create an OAuth Application Registry</td>
<td>59</td>
</tr>
<tr>
<td>Configuring the Zscaler Tenant on ServiceNow</td>
<td>60</td>
</tr>
<tr>
<td>Copy the needed Oath Credentials</td>
<td>62</td>
</tr>
<tr>
<td>Finishing the Zscaler Tenant on the Zscaler</td>
<td>63</td>
</tr>
<tr>
<td>Configuring the Zscaler ServiceNow Connector</td>
<td>64</td>
</tr>
<tr>
<td>Configuring ServiceNow Policies and Scan Configuration</td>
<td>65</td>
</tr>
<tr>
<td>Scoping the Policies and Remediation</td>
<td>66</td>
</tr>
<tr>
<td>Creating a DLP Policy</td>
<td>67</td>
</tr>
<tr>
<td>Creating a DLP Engine</td>
<td>68</td>
</tr>
<tr>
<td>Creating a DLP Engine</td>
<td>69</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configure a SaaS DLP Policy</td>
<td>70</td>
</tr>
<tr>
<td>SaaS DLP Policy Details</td>
<td>71</td>
</tr>
<tr>
<td>Configure a SaaS DLP Policy</td>
<td>72</td>
</tr>
<tr>
<td><strong>Configure a SaaS Malware Policy</strong></td>
<td>74</td>
</tr>
<tr>
<td>SaaS Malware Policy Wizard</td>
<td>75</td>
</tr>
<tr>
<td>SaaS Malware Policy</td>
<td>76</td>
</tr>
<tr>
<td><strong>Configure the Scan Schedule Configuration</strong></td>
<td>77</td>
</tr>
<tr>
<td>Start the Scan Schedule</td>
<td>78</td>
</tr>
<tr>
<td><strong>Reporting and Visibility</strong></td>
<td>79</td>
</tr>
<tr>
<td>SaaS Assets and SaaS Assets Summary Report</td>
<td>80</td>
</tr>
<tr>
<td>SaaS Security Insights</td>
<td>81</td>
</tr>
<tr>
<td><strong>Cloud App Control</strong></td>
<td>82</td>
</tr>
<tr>
<td>Cloud Application Access Control Policy</td>
<td>83</td>
</tr>
<tr>
<td>Cloud Application Access Control Policy Wizard</td>
<td>84</td>
</tr>
<tr>
<td>Cloud Application Access Control: Deny Policy</td>
<td>85</td>
</tr>
<tr>
<td>Cloud Application Access Control</td>
<td>86</td>
</tr>
<tr>
<td>Cloud Application Access Control Logs</td>
<td>87</td>
</tr>
<tr>
<td><strong>Zscaler Digital Exchange (ZDX) for ServiceNow</strong></td>
<td>88</td>
</tr>
<tr>
<td>Configure ZDX for ServiceNow</td>
<td>89</td>
</tr>
<tr>
<td>Configure ZDX for ServiceNow</td>
<td>90</td>
</tr>
<tr>
<td>Configure Probes for ServiceNow Monitoring</td>
<td>91</td>
</tr>
<tr>
<td>Configure Probes for ServiceNow Monitoring</td>
<td>92</td>
</tr>
<tr>
<td>The ZDX Enabled ServiceNow Application</td>
<td>94</td>
</tr>
<tr>
<td>Create an Alert for the ServiceNow Service</td>
<td>95</td>
</tr>
<tr>
<td>The Triggered Alert for the ServiceNow Service</td>
<td>101</td>
</tr>
<tr>
<td>Alert Detail for the ServiceNow Service</td>
<td>102</td>
</tr>
<tr>
<td>The Sent Alert Email for the ServiceNow Service</td>
<td>103</td>
</tr>
</tbody>
</table>
Using ZDX: The Dashboard 104
   Application Overview 105
   ServiceNow Application Performance Detail 106
   User Overview 108
   ServiceNow User Detail 109

ZCSPM: ServiceNow Integration for Ticket Creation 111
   Configure ServiceNow Ticketing Integration 112
      ZCSPM Incident Management 113
      ZCSPM ServiceNow Account and Credentials 114
      ZCSPM Configuration Validated 115
      ServiceNow Incidents 116

Appendix A: Requesting Zscaler Support 117
   Gather Support Information 117
      Save Company ID 118
      Enter Support Section 119
## 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

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

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—all you do is make Zscaler your next hop to the Internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices)
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees)

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

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

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on 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, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel 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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>Adding SaaS Application Tenant</td>
<td>Help articles on using Zscaler API for visibility and security for sanctioned SaaS applications used in your organization.</td>
</tr>
<tr>
<td>About SaaS Application Tenant</td>
<td>Help articles on adding SaaS applications to Zscaler.</td>
</tr>
<tr>
<td>SaaS Security API DLP Policy</td>
<td>Help articles on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.</td>
</tr>
<tr>
<td>About Data Loss Prevention</td>
<td>Help article on DLP.</td>
</tr>
<tr>
<td>About DLP Dictionaries</td>
<td>Help article on DLP dictionaries.</td>
</tr>
<tr>
<td>About DLP Engines</td>
<td>Help article on DLP engines.</td>
</tr>
<tr>
<td>SaaS Security Insights</td>
<td>Help article providing SaaS security information.</td>
</tr>
<tr>
<td>SaaS Posture Security</td>
<td>Help article on configuring the SaaS security posture control policy.</td>
</tr>
<tr>
<td>Cloud Application Access Control</td>
<td>Help article on Zscaler cloud app control.</td>
</tr>
<tr>
<td>SaaS Identity Proxy</td>
<td>Help article on configuring the Zscaler identity proxy for cloud apps.</td>
</tr>
<tr>
<td>ZDX Help Portal</td>
<td>Help articles on ZDX.</td>
</tr>
<tr>
<td>ZDX Predefined Applications</td>
<td>Help articles on predefined applications for ZDX.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>

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 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](http://www.servicenow.com) or follow them on Twitter @servicenow.
ServiceNow Resources

The following table contains links to ServiceNow support resources.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About ServiceNow</td>
<td>ServiceNow company description.</td>
</tr>
<tr>
<td>ServiceNow Developer Account</td>
<td>Website for creating a ServiceNow developer account.</td>
</tr>
<tr>
<td>ServiceNow Product Documentation</td>
<td>Online documentation for the ServiceNow platform.</td>
</tr>
<tr>
<td>ServiceNow Community</td>
<td>ServiceNow online community portal.</td>
</tr>
<tr>
<td>ServiceNow Support</td>
<td>Online support for the ServiceNow platform.</td>
</tr>
</tbody>
</table>

Audience

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

Software Versions

This document was authored using ZIA 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.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler Employees: contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.
Zscaler Data Protection and Digital Experience for ServiceNow.com

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.

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 our Zscaler Internet Services (ZIA) for security of ServiceNow and our Zscaler Digital Experience (ZDX).

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 (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 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 covers the following ZIA features for ServiceNow Security, and the ZDX for ServiceNow performance visibility.

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

![ZIA identity proxy diagram](image)

*Figure 2. ZIA identity proxy*

When users try to access ServiceNow with their corporate accounts without going through the Zscaler service, they receive a pop-up screen asking them to login via Zscaler. SAML, the IDP that is defined on Zscaler for the ZIA service, and the ServiceNow SSO configuration control the process and forward authorization requests to Zscaler. Once 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 SSL. You get full protection from web and internet threats. 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.
ZIA Browser Isolation

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

Figure 3. ZIA Cloud Browser Isolation in use with ServiceNow

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

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

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

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

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 (ZPA) for zero-trust access to internal applications, ZDX for active monitoring of users’ experience to SaaS applications, and Zscaler Cloud Protection (ZCP). Zscaler provides end to end connectivity, security, and visibility from any location on-prem or remote.

For more information, please see the resources in [Zscaler Resources](#).
ZIA Cloud Application Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits in line between users and the internet, inspecting all traffic, including SSL, flowing between them. As part of the platform, Zscaler Cloud Application Visibility and 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 an 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.

Figure 5. Cloud App Control
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 Zscaler Resources.
Zscaler Cloud Security Posture Management ServiceNow Incident 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 includes the steps below:

- Configure ServiceNow Ticketing Integration for ServiceNow ZCSPM License Admin
- Configure ZCSPM Incident Management for the subscription owner
- Verify ServiceNow Incidents tickets for ServiceNow admins
Configure the 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 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 receive a pop-up screen asking them to login via Zscaler. SAML, the IDP that is defined on Zscaler for the ZIA service, and the ServiceNow SSO configuration control forwarding authorization requests to Zscaler. Once the user’s identity has been verified, ZIA secures traffic to and from ServiceNow and inspects user and the ServiceNow data.

ZIA 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.
Configure the SaaS Identity Proxy

Log into the Zscaler tenant with administrator credentials.

Figure 9. Configure the SaaS identity proxy
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 opens the configuration wizard:

1. Give the cloud application a **Name**.
2. Select **Enable**.
3. Select **ServiceNow** for **Cloud Application**.
4. Set the **ACS URL** to `https://your-servicenow-instance.service-now.com/navpage.do`.
5. Set the **Entity ID** to `https://your-servicenow-instance.service-now.com`.
6. Select the **SAML_2022 or Later** signing certificate.
7. Select **Pass-through Zscaler Identity** for the **Identity Transformation**.
8. Select **Save**.

![Configuration Wizard](image)

**Figure 10. Configure the SaaS identity proxy settings**
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:

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

Figure 11. The completed identity proxy
Configure ServiceNow to use the Identity Proxy

Log into the ServiceNow tenant with administrator credentials.

Figure 12. Configure ServiceNow for the identity proxy
Install the ServiceNow Plugins

In the ServiceNow plugins page:

1. In the Filter Navigator search for “system app”.
2. Select All Available Applications.
3. Then 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. Then click Activate.

![Configure the ServiceNow plugins](image)

This installs both the Multiple Provider Single Sign-On Enhanced UI and the Multiple Provider Single Sign-On Enhanced plugins, which we must configure for the Zscaler identity proxy.
Configure the SaaS Identity Proxy

Next, configure the SaaS identity proxy:

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

![Figure 14. Enable multiple provider SSO](image)
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. Then select **New**.
3. In the ServiceNow Identity Providers section, select **SAML**.

---

**Figure 15. Create the Identity Provider**

**Figure 16. Select SAML SSO**
Configure the Identity Provider

Configure the identity provider:

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

Figure 17. Configure the identity provider
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:

1. Select the Zscaler Identity Provider.

![Figure 18. Select the Zscaler identity provider](image)

2. 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**.

![Figure 19. Add the signing certificate](image)
3. 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**

![Figure 20. Configure the identity provider certificate](image)

The certificate is one continuous line. Remove any carriage returns.
4. To configure additional identity provider certificate settings:

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

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

![Configure and test the identity proxy](image)

You may 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 this should be the screen we see when testing the identity provider, and anytime a change is made to the identity proxy you need to re-test the identity proxy. This screen has good test results. The Logout Test results are expected to fail.

- Select **Activate**

![Testing the identity provider](image)

**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**
- **X** 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.

![Figure 22. Testing the identity provider](image)
The Active Identity Proxy Notification

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

![Image of Zscaler login error message]

Figure 23. The active authentication proxy
Configure Redirect on the Identity Provider

This procedure is only for the case that the auto redirect IdP doesn’t enable from the Configuration screen. We need to set a system property to enable redirect by default to our IdP:

1. Go to the Identity Provider page.
2. Left click on the Zscaler Identity Provider and copy the sys_id.

![Figure 24. Configure the identity provider](image-url)
3. The next step is to configure the redirect system properties:
   
   - Search for `sys_properties.LIST` in the Filter Navigator
   - Hit `Return`

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

![System properties](image-url)

*Figure 25. System properties*
5. In the **Systems Property** screen, search for and edit the systems property `glide.authentication.sso.redirect.idp`. This launches the edit screen for the property:

- Search for `glide.authenticate.sso.redirect.idp`
- Select `glide.authenticate.sso.redirect.idp`

![Figure 26. System Property glide.authenticate.sso.redirect.idp](image-url)
Configure the Property

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

1. In the **Value** field paste in the sys_id from our IdP.
2. Select **Update**.

![Configure the identity provider](image)

*Figure 27. Configure the identity provider*
Configure Cloud Browser Isolation

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

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

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.
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 Admin Portal and the link and administrator credentials are supplied to you by Zscaler Support after your organization has subscribed to the feature:

- Log into the Zscaler Browser Isolation Tenant with administrator credentials

![Configure Cloud Browser Isolation](image)

*Figure 29. Configure Cloud Browser Isolation*
A Browser Isolation Profile or multiple profiles need to be configured to enable the Zscaler Cloud Browser Isolation Features that are 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:

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

![Isolation profiles](image)

*Figure 30. Configure Cloud Browser Isolation profile*

This starts the **Browser Isolation Wizard** and steps you through enabling **General Information**, **Company Settings**, **Security Controls**, **Regional Connectivity**, and the **End User Notification**.
4. For **General Information** give the profile an intuitive name and description. It is 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**

Figure 31. Cloud Browser Isolation general information
5. For the ZIA Company Settings, you must select your Company ID and Cloud if your information is not populated automatically. This information can be obtained from your ZIA Admin 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

![Cloud Browser Isolation ZIA company information](image)

*Figure 32. Cloud Browser Isolation ZIA company information*
6. 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 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 we are going to maintain the strictest security settings and not enable any controls:

- Select **Next**

---

**Figure 33. Cloud Browser Isolation security settings**
7. Two **Regions** must be selected for redundancy. Select the two closest regions to your organization:

- Select two regions for redundancy
- Select **Next**

*Figure 34. Cloud Browser Isolation regions*
8. 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**

![Cloud Browser Isolation EUN](image-url)

*Figure 35. Cloud Browser Isolation EUN*
9. Our completed Zscaler Cloud Browser Isolation Profile. This appears as a profile option when setting up isolation policies in ZIA.

Let’s setup our Zscaler Isolation Policies in the ZIA Admin Portal.
Configure the Cloud Browser Isolation Policies

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

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

Figure 37. Configure Cloud Browser Isolation
3. To configure policies that redirect ServiceNow traffic to Cloud Browser Isolation, launch the URL Filtering wizard:

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

![Configure Cloud Browser Isolation policies](image-url)
4. In the **URL Rule** wizard:

- 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 dialog)

![Add URL Filtering Rule](image)

*Figure 39. Configure Cloud Browser Isolation policy*
5. This displays 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**

   ![Add URL Category](image-url)

   *Figure 40. Configure Cloud Browser Isolation*
6. 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 organization’s specific browsers for use with browser isolation
   - Select **Save** to complete the configuration

*Figure 41. Configure Cloud Browser Isolation*
7. The completed browser isolation profile.

**Figure 42. Configure Cloud Browser Isolation**
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 ZIA clouds include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.

Figure 43. ZIA Admin Portal
Adding the Service Now Tenant

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

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

![Figure 44. ZIA SaaS application tenant](image-url)
SaaS Tenant Configuration Wizard

To start the wizard:

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

![Add SaaS Application Tenant](image)

*Figure 45. The SaaS tenant configuration wizard*
3. Give the ServiceNow tenant a name. This is the name that is selected when assigning a policy for the Zscaler security features:

- Enter a name for the **Tenant Name**
- Open a new browser tab and login to your ServiceNow tenant with admin role credentials

![Add SaaS Application Tenant](image)

*Figure 46. Open the ServiceNow tenant*
Configuring the Zscaler Tenant on ServiceNow

To configure the Zscaler tenant from your ServiceNow admin account:

1. Log in to ServiceNow with administrator credentials.

   ![Login to the ServiceNow tenant](image)

   **Sign In to the Developer Site**

   Input:
   - toddh@testmypacket.com
   - Password

   Sign in

   **Forgot your password?**

   For questions about your account or the Developer Program, please leave feedback on the **Developer Site**.

   Get a ServiceNow Account
2. 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**

3. This displays the **All Applications** page:
   - In the search box type “Oath 2.0”
   - Verify OAuth is installed

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

   ![Figure 48. Verify OAuth is installed](image-url)
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 49. The installed Zscaler SaaS connector
Check that the OAuth Plugin is Active

Check that the status of OAuth 2.0 is Active.

Figure 50. OAuth plugin status
Create an OAuth Application Registry

We need to create an OAuth application registry for the Zscaler tenant:

1. On the left-hand pane 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. Then select New.

Figure 51. Creating an Application Registry
Create an OAuth Application Registry

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

- Select Create an OAuth API endpoint for external clients

![Create an OAuth Application Registry](image)

*Figure 52. 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 **Token Lifespan** in seconds. 157,700,000 is five years, at which point the tenant has to be reinstalled.
3. Enter the **Access Token Lifespan** in seconds. 86,400 is 24 hours and the recommended duration by Zscaler.
4. Enter **Submit** to save the settings.

![Image of ServiceNow interface showing OAuth endpoint configuration](figure-53.png)

Figure 53. Creating the OAuth endpoint

The **Client Secret** is created after the detail is submitted. Then go back into the endpoint to copy it for the Zscaler configuration.
5. Once the Zscaler endpoint is created, select the Zscaler endpoint to open the settings to copy the **Client Secret**.

![Figure 54. The Zscaler endpoint](image-url)
Copy the needed OAuth Credentials

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

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

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

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

1. Enter the ServiceNow Client ID.
2. Enter the ServiceNow Client Secret.
3. Enter the ServiceNow Instance URL.
4. Enter the ServiceNow User ID and Password.
5. And finally enter the Admin ID (in this case, it’s the same Admin User).
6. Select Authorize to verify the credentials.
7. Select Save.

![Add SaaS Application Tenant](image-url)

Figure 56. Finish the Zscaler tenant
Configuring the Zscaler ServiceNow Connector

The completed and active ServiceNow API connector.

Figure 57. The completed and active ServiceNow tenant
Configuring ServiceNow Policies and Scan Configuration

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

Figure 58. 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 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.

The DLP policy creates 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 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 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 Configure a SaaS Malware Policy.
Creating a DLP Policy

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

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

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

![Figure 60. Creating a DLP dictionary](image-url)
Creating a DLP Engine
To create the DLP engine:

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

![Creating a DLP engine](image)

*Figure 61. Creating a DLP engine*
Creating a DLP Engine

In the Add DLP Engine dialog:

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

![Image of the DLP engine wizard]

*Figure 62. The DLP engine wizard*

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

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

2. Select ITSM.
3. Select Add DLP Rule.

See detail of the policy on the following pages.

![SaaS Security API Control](image)

*Figure 63. Launch the SaaS DLP Policy Configuration Wizard*
SaaS DLP Policy Details

The SaaS DLP Policy is like all Zscaler Polices where you specify the detail on whom this policy applies, 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. We 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 select **Any Collaboration**, and an **Action** of **Remove Sharing**.

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

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

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

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

To finish our DLP Policy:

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

Figure 64. The SaaS DLP Policy Configuration wizard
9. The completed DLP rule ready to be applied with a scanning schedule.

Figure 65. The configured DLP policy
Configure a SaaS Malware Policy

To launch the Malware Rule Wizard:

2. Select ITSM.
3. Select Add Malware Detection Rule.

The SaaS Malware Detection policy is an all-encompassing policy and all files in the Tenant are scanned unless removed from the scope by specifying any exemptions by selecting the Exemption tab under Malware Detection. To add a malware policy, specify the application, the SaaS tenant, and the status.

The action for ServiceNow is limited to report malware only.

Figure 66. Launch the Malware Policy Configuration Wizard
SaaS Malware Policy Wizard

Configure the **Malware Rule Wizard**:

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

*Figure 67. The malware policy configuration wizard*
**SaaS Malware Policy**

The completed SaaS security malware policy for the ServiceNow SaaS tenant can be applied to our ServiceNow instance with a scanning schedule:

- Activate your configuration

![Image of SaaS Security API Control](image)

*Figure 68. The completed malware policy configuration wizard*
Configure the Scan Schedule Configuration

The final configuration step is to create a Scan Configuration. We 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 select All Data.

However, if this is a POV or a Trial, the only option available is New Data Only.

To add a Scan Schedule:

1. Select Policy > SaaS Security API > Scan Configuration > Add Scan Schedule.
2. Select the ServiceNow SaaS tenant for the SaaS Application Tenant.
3. Select the data loss Policy and the malware policy created in prior steps.
4. Select All Data, or for a POV select New Data Only.
5. Select Save to save the scan schedule and Activate the configuration.

![Add Scan Schedule](image)

Figure 69. Create and enable a scan for the SaaS tenant
Start the Scan Schedule

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

1. Select the blue arrow on the scan configuration to start SaaS API security on the ServiceNow tenant.
2. The Status should say Running with a start date and a latest scan date.
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.

Visit the Zscaler online documentation for detailed information of the SaaS Security Analytics tools.

Figure 71. SaaS security visibility
SaaS Assets and SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reporting to have a quick view of your files and emails. A SaaS assets summary report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen. Our ServiceNow activity over the creation of this deployment guide is shown, but any tenant configured is displayed on this summary screen. The data is hyperlinked, and you can easily pivot from a summary to individual logs and activities provided by SaaS security insights.

1. Select the **20 Total Violations** next to ServiceNow to pivot to SaaS security insights.
2. This opens the **Security Logs** dialog and the log data for each violation containing over 30 meta-data points of information.

Figure 72. Summary reports
SaaS Security Insights

The SaaS Security Insights Log page shows and 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 and their associated filters.

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

Figure 73. SaaS security insight
Cloud App Control

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

Cloud App Control 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 requires two policies: one policy to allow our specific users and one to block all other users.
Cloud Application Access Control Policy

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

1. Sign into your organizations ZIA Admin Portal with administrator credentials.
2. Select Policy.
4. Select the Cloud App Control Policy tab.
5. Select Add.

Figure 75. URL & Cloud App Control

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

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

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

Figure 76. Create a Cloud App Control Allow policy
Cloud Application Access Control: Deny Policy

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

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. Set the **Rule Name** to an intuitive name.
7. Select **ServiceNow** for the **Cloud Application**.
8. Leave all other settings as **Any**.
9. Select **Block** for **Application Access**.
10. Select **Save** to save changes.

![Cloud App Control Deny policy](image)

*Figure 77. Create a Cloud App Control Deny policy*
Cloud Application Access Control

Our completed access policies:

- **Activate** the policy additions

Users who try to access the ServiceNow application through Zscaler and do not have permission get the **Website Blocked** pop-up screen below displayed on their browser. Zscaler administrators receive alerts and logs about the event.

![Figure 78. Create a Cloud App Control Deny policy](image-url)

©2022 Zscaler, Inc. All rights reserved.
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:

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

Figure 79. Create a Cloud App Control log
Zscaler Digital Exchange (ZDX) for ServiceNow

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.

Figure 80. ZDX user experience monitoring for ServiceNow

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.
Configure ZDX for ServiceNow

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

Figure 81. ZDX user experience monitoring for ServiceNow
Configure ZDX for ServiceNow

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

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

![Onboard the ServiceNow app](image)

*Figure 82. Onboard the ServiceNow app*
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 uses 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:

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

![Figure 83. ZDX user experience monitoring for ServiceNow](image)
Configure Probes for ServiceNow Monitoring

To configure probes for ServiceNow monitoring:

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

---

**Edit ServiceNow CloudPath Probe**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>ServiceNow CloudPath Probe</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Enable</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>ServiceNow</td>
</tr>
<tr>
<td><strong>Probe Type</strong></td>
<td>Cloud Path</td>
</tr>
<tr>
<td><strong>Follow Web Probe</strong></td>
<td>ServiceNow Landing Page Probe</td>
</tr>
<tr>
<td><strong>Run Frequency (minutes)</strong></td>
<td>15</td>
</tr>
<tr>
<td><strong>Probe Class</strong></td>
<td>Predefined</td>
</tr>
</tbody>
</table>

**PROBING CRITERIA**

<table>
<thead>
<tr>
<th>User Groups</th>
<th>Users</th>
</tr>
</thead>
</table>

**Figure 84. Edit the network probe**
3. Validate the destination host to monitor it should be to your ServiceNow Login URL.
4. Select **Next**.
5. Review and **Activate** the changes to the probe.

![Figure 85. Edit the CloudPath probe](image-url)
The ZDX Enabled ServiceNow Application

The ServiceNow application monitoring is activated, and our 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**.

![Predefined Applications](image)

Figure 86. Active ServiceNow monitoring
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, Wi-Fi signal strength, memory, sent and received Mbps

To create our alert on page fetch times:

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

Figure 87. Creating an alert
4. Step One of the rule wizard:
   - **Name** the Rule
   - Select **Enable** under **Status**
   - Give the alert an appropriate severity
   - Select an application **Type**
   - Select **Next**

![Add New Alert Rule](image)

* Name: ServiceNow Degradation Alert
* Status: Enabled
* Severity: High
* Type: Application

**Figure 88. The Alert Creation wizard step 1**
5. Step two of the rule wizard:

- Select ServiceNow as the Application
- Select ServiceNow Landing Page Probe for the Web Probe
- Select Next

Figure 89. The Alert Creation wizard step 2
6. Step three of the rule wizard creates the threshold that triggers the alert. We can use multiple variables here to eliminate false positive.

- Select **Page Fetch Time**
- Select the time to exceed **5000ms** (five seconds)
- Select **Next**

*Figure 90. The Alert Creation wizard step 3*
7. Step four of the rule wizard adds throttling to control the scope of the alert. We 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 Devices Impacted
- Select Email as the Delivery Method
- Enter the Alert Recipients email address separated by commas

Figure 91. The Alert Creation wizard step 4
8. Our completed rule set for the alert:

*Figure 92. The completed rule set*
The Triggered Alert for the ServiceNow Service

You can see the triggered alert generated by our threshold settings in our rule set. You can click on the rule name or click the eye to see more detail about the alert.

![Alerts](image)

*Figure 93. The alert*
Alert Detail for the ServiceNow Service

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

![Alert detail for the ServiceNow Service](image)

Figure 94. Alert details
The Sent Alert Email for the ServiceNow Service

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

---

**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

---

**Figure 95. The alert email**
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 shows you any locations globally with issues.

Figure 96. The Dashboard
Application Overview

Select the Applications tile on the left of the UI. This displays the Applications Overview and shows all the configured applications and the individual ZDX score:

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

![Application overview](image)

*Figure 97. Application overview*
ServiceNow Application Performance 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.

Figure 98. Application detail
The bottom portion of the app details show the **Top Zscaler Locations**, **Top Cities**, and the **Top Departments** using the application and the ZDX scores at a glance. We also see our probe data, with minimum, maximum, and average response times.

![Application detail](image)

**Figure 99. Application detail**
User Overview

The User Overview provides 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 100. User overview
ServiceNow User Detail

The user detail shows 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 provides the Users, Devices and device specific detail (OS, Device type, Network Information, etc.) by clicking on 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.

![ServiceNow User Detail](image)

Figure 101. 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.
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 ZCSPM in the monitored production environment. Incident Management (Ticketing) allows integrations with ServiceNow.

The process to configure the integration includes the steps below:

- Configure ServiceNow Ticketing Integration for ServiceNow ZCSPM License Admin
- Configure ZCSPM Incident Management for the subscription owner
- Verify ServiceNow Incidents tickets for ServiceNow admins

Figure 104. Zscaler Cloud Security Posture Management
Configure ServiceNow Ticketing Integration

To configure the ServiceNow ticketing system integration:

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

![Figure 105. Configure the ticketing system integration for ServiceNow](image-url)
ZCSPM Incident Management

On the Configure Incident Management page:

1. For Ticketing System select ServiceNow.
2. Select Ticket Creation Frequency of incident creation.
3. Click Configure. A Configure ServiceNow window displays.

![Configure Incident Management](image)

Figure 106. Select and configure ServiceNow
**ZCSPM ServiceNow Account and Credentials**

To create a ZCSPM account instance:

1. For **Instance Name**, type in the ServiceNow instance name.
2. For **Instance Username**, type in the admin's username for the ServiceNow instance.
3. For **Instance Password**, type in the admin's password for the ServiceNow instance.
4. For **Assign Ticket To**, enter an email address. Tickets from the ServiceNow instance are assigned to this email.
5. Click **Save**.

*Figure 107. User detail: end-to-end connection detail*
**ZCSPM Configuration Validated**

If ZCSPM connects to the ServiceNow tenant using the supplied credentials, the ZCSPM configuration shows a checkmark verifying connectivity:

- Click **Save**

This integration configuration between ZCSPM and ServiceNow is now complete, and violations are reported daily. Additional configuration can be made to prioritize created incidents on a per-cloud-service basis.

![Figure 108. Successful integration](image)

Next let's verify incidents are created as expected.
ServiceNow Incidents

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

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

Figure 109. ZCSPM created ServiceNow incident
Appendix A: Requesting Zscaler Support

Gather Support Information

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

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

![Figure 110. Collecting details to open support case with Zscaler TAC](image)
Save Company ID

Copy the Company ID, as shown below.

**Company Profile**

![Company Profile](image)

**Company ID**

zscalerthree.net-1008708

**Name**

Labs - Test Account

**Domains**

domains.domains.domains.domains

**Address Line 1**


**Address Line 2**


*Figure 111. Company ID*
Enter Support Section

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

Figure 112. Submit ticket