Deployment Guide

ZIA SaaS Security API
&
ZDX Monitoring

Jan2021
Version 1.0

Business Development and Technical Alliances

Copyright ©, Zscaler, Inc.
Table of Contents

1 Zscaler SaaS Security API for Box ................................................................. 6
  1.1 Overview.................................................................................................. 6
  1.2 Zscaler Internet Access SaaS Security API for Box .................................. 8
  1.3 Zscaler Digital Exchange for the Box user experience .............................. 9

2 Configuring Zscaler SaaS Security for Box ................................................. 11
  2.1 Configuring the Zscaler and the Box Tenant ......................................... 12
  2.2 Configuring the Box Tenant on Zscaler ............................................... 13
  2.3 SaaS Tenant Configuration Wizard ....................................................... 14
  2.4 Configuring the Zscaler Tenant on Box ................................................ 16
  2.5 Finish the Zscaler Configuration ............................................................ 21
  2.6 The Active SaaS API Tenant ................................................................. 22

3 Configuring Box Policies and Scan Configuration ..................................... 23
  3.1 Scoping the Policies and Remediation ................................................. 24
  3.2 Creating a DLP Policy ........................................................................... 25
  3.3 Creating a DLP Engine ......................................................................... 26
  3.4 Configure a SaaS DLP Policy ................................................................. 28
  3.5 SaaS DLP Policy Details ....................................................................... 29

4 Configure a SaaS Malware Policy ............................................................... 32

5 Configure the Scan Schedule Configuration ............................................. 36

6 The Box Tenant Post Scan ........................................................................... 38

7 Reporting and Visibility ............................................................................. 39
  7.1 SaaS Assets and SaaS Assets Summary Report ..................................... 40
  7.2 SaaS Security Insights ......................................................................... 41

8 Zscaler Digital Exchange (ZDX) for Box ................................................. 42
  8.1 Configure ZDX for Box ........................................................................ 43
  8.2 Configure Probes for Box Monitoring ................................................. 45
  8.3 The Enabled Box Application ............................................................... 46
  8.4 Create an Alert for the Box Service ....................................................... 49
  8.5 The Triggered Alert for the Box Service .............................................. 55
  8.6 The Sent Alert Email for the Box Service ............................................ 56

9 Using ZDX – The Dashboard .................................................................... 57
  9.1 Using ZDX – Application Overview .................................................... 58
  9.2 Using ZDX – Application Detail ........................................................... 59
  9.3 Using ZDX – User Overview ................................................................. 61
  9.4 Using ZDX – User Detail ..................................................................... 62

10 Appendix A: ............................................................................................... 64
  10.1 Zscaler Resources ................................................................................ 65

Copyright ©, Zscaler, Inc.
Zscaler Business Development and Technical Alliances
## 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>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), 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.

Box Overview

Box, Inc. (NYSE: BOX), Box, Inc., is a Leader in SaaS Cloud Content Platforms based in Redwood City, California. The company focuses on cloud content management and file sharing service for businesses. Official clients and apps are available for Windows, macOS, and several mobile platforms. Box was founded in 2005. For more information on Box, Inc., please visit www.box.com or follow them on Twitter @box.
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.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and Box Production Release dated Jan 11, 2021.

Request for Comments

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.
1 Zscaler SaaS Security API for Box

1.1 Overview

SaaS applications that provide Content Management and File Sharing services are popular precisely because of the collaboration, ease of use and sharing they enable, and our partner Box.com is one of the industry leaders. But the downside of this ease of access is that they can present risk based on the client’s environment. It is impossible to train every employee to use safety best practices with SaaS applications at all times, 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 User’s experience for the SaaS application. Especially in today's Work from Anywhere corporate infrastructures. Zscaler provides a complete Box
solution using our Zscaler Internet Services (ZIA) and our Zscaler Digital Access Exchange Service (ZDX).

ZIA provides SaaS Security using our SaaS API to scan the Box Datastores for Malicious Content, and Data 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 Box service to help organizations address any experience concerns or challenges. ZDX has preconfigured monitors that provide performance monitoring and measurements from the user’s device running the Zscaler Client Connector. These monitors provide detailed information on the Users Device, The Network Path to Box, and the Box SaaS performance itself.

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 a service.
1.2 Zscaler Internet Access SaaS Security API for Box

The Zscaler 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.

Zscaler SaaS Security API 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 API unique?

Data exposure reporting and remediation
Zscaler SaaS Security API 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 API checks SaaS applications for hidden threats being exchanged and prevents their propagation.

Compliance assurance
Zscaler SaaS Security API 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 User's 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.

1.3 Zscaler Digital Exchange for the Box 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. By combining the Zscaler Client Connector endpoint agent with Zscaler’s global cloud footprint, ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

What makes the Zscaler Digital Experience unique?

**End-user device performance**  
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.

**Cloud path performance**
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.

**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*.
The configuration to enable the SaaS Security service builds on itself, and the steps are listed below. Log into the Zscaler Tenant to Start the configuration process.

Configure the Box SaaS Tenant in Zscaler
Configure the Zscaler Tenant in Box
Configure a SaaS DLP Policy
Configure a SaaS Malware Policy
Configure and Start the Scan Policy for the SaaS service

- Log into your Zscaler Tenant with Administrator credentials

2.1 Configuring the Zscaler and the Box Tenant
Configure the Box SaaS Tenant under Administration in the ZIA UI.

- Select Administration
- Select SaaS Application Tenant

### 2.2 Configuring the Box Tenant on Zscaler
Add the SaaS Application Tenant.

- Select Add SaaS Application Tenant

### 2.3 SaaS Tenant Configuration Wizard
Figure 7: The SaaS Tenant Configuration Wizard

Select the box Tile under popular applications to move to the next step in the Wizard.

- Select the box tile

2.3.1 SaaS Tenant Configuration Wizard
Give the Box tenant a name. This will be the tenant name that will be selected when assigning a policy for the Zscaler security features.

- Enter a name for the Tenant Name
- Copy the Zscaler SaaS Connector number for next steps
- Select the Go to Box Settings to bring up your Box portal

2.4 Configuring the Zscaler Tenant on Box
To configure the Zscaler Tenant from your Box Admin account.

- Select Apps
- Select Custom Apps
- Select Authorize New App

**2.4.1 Configuring the Zscaler Tenant on Box**
Figure 10: Authorize the Zscaler App on the Box Tenant

To authorize the Custom App that will be the Zscaler Tenant.

- Paste the Zscaler SaaS Connector that was copied from the Zscaler Wizard two steps back
- Select Next

2.4.2 Configuring the Zscaler Tenant on Box
Figure 11: Authorize the Zscaler App on the Box Tenant

- Select Authorize

2.4.3 Configuring the Zscaler Tenant on Box
The new Zscaler tenant has been created and we must now complete the Zscaler configuration by selecting the Enterprise ID which will be pasted into Step 4 of the Zscaler configuration wizard.

- Select Account & Billing

### 2.4.4 Configuring the Zscaler Tenant on Box
Figure 13: The Enterprise ID

Under Account & Billing of the Box Admin account select and save the Enterprise ID. This ID will be pasted into the Zscaler wizard identifying the Box SaaS ID and will allow the Zscaler API to provide security services to this Box tenant.

- Copy and Save the Enterprise ID
- Go back to the Zscaler window to finish the configuration

2.5 Finish the Zscaler Configuration
Figure 14: Zscaler Configuration Wizard

- Paste the Box Enterprise ID copied from the last step into step 4
- Save the Zscaler / Box configuration
- Activate your changes

2.6 The Active SaaS API Tenant
The API credentials and connectivity will now be validated.

- Refresh your browser to verify the Box tenant is Active

We are now ready to set up our Scan Schedule, our DLP policies and our Malware polices.

3  Configuring Box Policies and Scan Configuration
Figure 16: Zscaler Configuration Wizard

After adding the tenants, you can configure the SaaS Security API DLP policy, Malware Detection policy, and Scan Configuration. You can also view reports and data for the tenants in the SaaS Security Report, Insights, and Logs.

3.1 Scoping the Policies and Remediation
For this Deployment Guide, we will configure a basic DLP policy and a Malware policy to scan the Box account files for matching content of the DLP policy, and also to scan the files for known malware for the malware policy. We will touch more on Malware in a later section.

Zscaler SaaS Security out-of-band data protection capabilities look inside the SaaS applications themselves through API integrations to identify accidental or intentional data exposure and compliance violations that would otherwise go unnoticed.

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 and remove the Shared link to prevent further sharing of the file. 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 Box files. This deployment will not cover Inline Data Protection or Exact Data Match, although they are integral pieces of a Data Protection solution.

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

### 3.2 Creating a DLP Policy
The procedures for creating a DLP policy are pretty 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 US Social Security Numbers AND US Names. 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 Box 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 the Dictionary to be used. In this case Names and Social Security Numbers.

### 3.3 Creating a DLP Engine
To create the DLP engine:

- Select the DLP Engines Tab
- Select Add DLP Engine

3.3.1 Creating a DLP Engine
Figure 20: 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

3.4 Configure a SaaS DLP Policy
To Launch the DLP Rule Wizard:

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

### 3.5 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 particular 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.

**Action:** Choose the **Action** the rule takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant.

- **Change to Read Only for All Collaborators:** The rule reports the incident and changes the file’s collaboration scope for all collaborators to read only.
- **Change to Read Only for External Collaborators:** The rule reports the incident and changes the file’s collaboration scope for external collaborators to read only.
- **Change to Read Only for Internal Collaborators:** The rule reports the incident and changes the file’s collaboration scope for internal collaborators to read only.
- **Remove All Collaborators:** The rule reports the incident and removes all of the file’s external and internal collaborators.
• **Remove External Collaborators and Shareable Link**: The rule reports the incident and removes all of the file’s external collaborators and any shareable links.

• **Remove Internal Collaborators and Shareable Link**: The rule reports the incident and removes all internal collaborators and any shareable links.

• **Remove Internal Shareable Link**: The rule reports the incident and removes the file’s internal shareable link. Existing collaborators are unaffected.

• **Remove Public Shareable Link**: The rule reports the incident and removes the file’s public shareable link. Existing collaborators are unaffected.

• **Remove Sharing**: The rule reports the incident and removes all of the file’s collaborators and any shareable links.

• **Report Incident Only**: The rule reports the incident only and makes no changes to the file’s collaboration scope.

• **Update to Not Discoverable Externally**: The rule reports the incident and changes the file’s collaboration scope to prevent it from being discoverable through public search engines.

• **Update to Not Discoverable for All**: The rule reports the incident and changes the file’s collaboration scope to prevent it from being discoverable through public search engines or within your organization.

• **Update to Not Discoverable Internally**: The rule reports the incident and changes the file’s collaboration scope to prevent it from being discoverable within your organization.

---

### 3.5.1 Configure a SaaS DLP Policy
Figure 22: The SaaS DLP Policy Configuration Wizard

To Finish our DLP Policy

- Specify the Rule order for Processing
- Name the Rule
- Enable the Rule
- Select the Box SaaS Tenant
- Select the DLP Engine created in the last step
- Select Any-Any for the Collaboration Scope
- Select Medium as a Severity to allow for identification for searches and tracking
- Save and Activate your configuration

4 Configure a SaaS Malware Policy
Figure 23: The Malware Policy Configuration Wizard

To Launch the DLP Rule Wizard:

- Select Policy / SaaS Security API / Malware Detection
- Select File Sharing
- 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, the Status, the Action and the Quarantine Location.

The Action and the Quarantine Location are unique to the SaaS Tenants. For the Action you can Quarantine, Remove, or report a violation. If you Select Quarantine you will need to
specify the Box ID for the user where the files will be quarantined. This would typically be the Security Operations Group.

**Action**: Select the action for the rule to take when it detects malware.

- **Quarantine Malware**: The Zscaler service quarantines the suspicious file.
- **Remove Malware**: The service deletes the suspicious file.
- **Report Malware**: The Zscaler service reports the incident but doesn't quarantine or remove the malware.

**Quarantine Location**: This field appears only if you select the **Quarantine Malware** action.

- This is the location where malicious files are moved for quarantine. The Zscaler service creates a folder or library called "Zscaler_Quarantine" for the location.
- To specify the quarantine location, enter the Box ID for the user who will own the folder. The service will create the folder on the user’s account.

### 4.1.1 Configure a SaaS Malware Policy
Configure the Malware Rule Wizard.

- Select Policy / SaaS Security API / Malware Detection
- Select File Sharing
- Select Add Malware Detection Rule
- Under Criteria Select Box as the Application
- Select the Box SaaS Tenant to apply the policy
- Select Enabled for Status
- Select Quarantine Malware as the Action
- Select the User ID where the Quarantine folder will be created, and the infected files stored
- Select Save

### 4.1.2 Configure a SaaS Malware Policy
Figure 25: The Completed Malware Policy Configuration Wizard

The completed SaaS Security Malware policy for the Box SaaS Tenant.

- Activate your configuration

5 Configure the Scan Schedule Configuration
Figure 26: 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 any 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 Box SaaS Tenant for the SaaS Application Tenant
- Select the Data Loss Policy and the Malware Policy Created in Prior Steps
- Select All Data or New Data Only if this is a POV
- Select Save to save the Scan Schedule

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

- Activate the Configuration Changes
- Select the Blue Arrow on the Scan configuration to start SaaS API Security on the Box Tenant.

The Status should say Active with a Start Date and a Latest Scan Date.

### Figure 27: Starting the Scan

6  The Box Tenant Post Scan
Figure 28: Our SaaS Security Results

The above is our Box Tenant after the Scan Schedule has completed. The Malware Policy has detected Malware in the two infected files and the SaaS Security API created the Quarantine Folder and moved the files into the folder. A file with the same name was also created to replace the infected file with a note telling the user the file has been quarantined.

The DLP Policy also found the configured violation and once the file containing the sensitive data was identified, the shared link was removed, preventing the file from being distributed.

7 Reporting and Visibility
Zscaler Analytics provide detailed reporting of all user activity down to each session created by the user when attaching to 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.

7.1 SaaS Assets and SaaS Assets Summary Report

Figure 29: SaaS Security Visibility
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 Box activity over the creation of this Deployment Guide is shown above, but any Tenant configured will be 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 10 Total Violations 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.

7.2 SaaS Security Insights
The SaaS Security Insights page is where you can view and define information 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.

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

8 Zscaler Digital Exchange (ZDX) for Box
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. And with users working from home and anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. Box is no exception to this and Zscaler ZDX provides visibility into the client’s experience using Box. ZDX utilizes the Zscaler Client Connector to generate application and network probes and gather device health. ZDX is a separate service from ZIA SaaS Security and can run with or without SaaS Security 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.

8.1 Configure ZDX for Box

Figure 32: ZDX for User Experience Monitoring for Box
Log into the ZDX Portal with Administrator credentials to begin the configuration process.

Log into your organizations ZDX portal

8.1.1 Configure ZDX for Box
Box is a predefined application in ZDX, and configuration is very simple. To configure the Box application for monitoring.

- Select Configuration
- Select Applications
- Select the blue arrow next to the Box App
- Select Go to Onboard Box

8.2 Configure Probes for Box Monitoring
Once the Go button was clicked, the Box app is enabled for monitoring and the pre-configured probes are displayed. The probes consist of a Network Probe which utilizes an ICMP Trace Route, and a Web Page Probe to the account.box.com location to monitor page load times.

We are going to make one change to the Network Probe to have it follow the path of the Webpage Probe so there is no confusion of the results since this is entirely for Box monitoring.

To edit the rule:

- Activate the Changes
- Select the blue pencil to edit the probe

### 8.2.1 Configure Probes for Box Monitoring
8.2.2 Configure Probes for Box Monitoring

- Select Box Account Login Page Probe under Follow Web Probe
- Select Next

**Figure 36 Edit the Network Probe**

- Select Box Account Login Page Probe under Follow Web Probe
- Select Next
8.3 The Enabled Box Application

- Validate the destination host to Monitor it should be account.box.com
- Select Next
- Review and Activate the changes to the Probe
Figure 38: Active Box Monitoring

The Box 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.

8.4 Create an Alert for the Box Service
As a final configuration step let’s create an alert to email us when there is service degradation of the Box application. An alert can be configured for Network, Application, or Device thresholds. Alert 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

### 8.4.1 Create an Alert for the Box Service
8.4.2 Create an Alert for the Box Service

Figure 40: 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
Figure 41: The Alert Creation Wizard

Step Two of the rule Wizard.

- Select Box as the application
- Select Box Account Login Page Probe for the Web Probe
- Select Next

8.4.3 Create an Alert for the Box 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

8.4.4 Create an Alert for the Box Service
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

8.4.5 Create an Alert for the Box Service
Figure 44: The Completed Rule Set

The Completed Rule Set for the Alert.

8.5 The Triggered Alert for the Box Service
Figure 45: The Alert

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

8.6 The Sent Alert Email for the Box 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.

9 Using ZDX – The Dashboard
Figure 47: 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.

9.1 Using ZDX – 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 take a look at the detail of our Box application.

- Select Applications
- Select the Box App

### 9.2 Using ZDX – 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 slow down of the Box service itself.

9.2.1 Using ZDX – Application Detail
The bottom portion of the App detail 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.

**Figure 50: Application Detail**

9.3 Using ZDX – User Overview
The User Overview will provide all of the users of an application. Select Box and then Apply to see all of our Box 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.

9.4 Using ZDX – User Detail

Figure 51: User Overview
Figure 52: User Detail

The Top portion of the User Detail will show an incredible amount of useful data to help isolate any user experience issues. Select and apply the Box application to see the detail of the user experience for the Box 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.

9.4.1 Using ZDX – User Detail
The above is the End to End visibility of the Data Path the user is taking to get to the Box 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 the Box SaaS itself, ZDX provides the visibility of the cloud to the Zscaler administrators from any of their users individual environments.

10 Appendix A:
10.1 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

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

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

Zscaler – Box Intro Video
https://drive.google.com/file/d/1592y8vu3B6dnlHFZEnbZ3bLKle9_kYTP/view?usp=sharing

Zscaler – Box Configuration Video
https://drive.google.com/file/d/1WrSy131pZS_7ccHeO9VKspVZ4Qd8dRQJ/view?usp=sharing