# Table of Contents

1. Introduction 3

2. Environment Overview 3
   2.1 Applications 4
   2.2 Users 4
   2.3 Access Policy 4

3. Test Plan 5
   3.1 Test Access with B2B Supplier User 6
   3.2 Test Access with B2B Vendor User 9
   3.3 Test Access and Navigation with the IT Admin User 16
   3.3.1 Applications Dashboard Overview 17
   3.3.2 Users Dashboard Overview 18
   3.3.2 Health Dashboard Overview 19
   3.3.3 App Connectors Dashboard Overview 21
   3.3.4 Application Segment Configuration 22
   3.3.5 Access Policy 23
   3.3.6 Diagnostics Interface 24
   3.3.7 Live Logs 27

4. Conclusion 29
1. Introduction

Zscaler B2B is a cloud service that provides B2B partners and customers with fast, seamless, and secure access to your web apps over the internet, regardless of where the apps are hosted. The service takes a zero trust network access approach that ensures the right people connect to the right resources with the right level of access, based on context and policy. It delivers the consumer app-like experience users expect without the repetitive logins and authentications required by remote access VPN.

This guide walks you through the foundational components that power Zscaler B2B. It will show the typical end-user experience for different B2B partners who only have access to the specific web apps they need for collaboration as per the policy configured. It will also show the typical end-user experience for an IT admin who needs to see B2B users and the apps they access and monitor the health of servers and resources.

2. Environment Overview

Zscaler B2B builds end-to-end, encrypted microtunnels between the user and each of the applications the user accesses, no matter where the applications are located. This ensures the best possible performance for each application and optimal end-user experience, as the traffic does not need to be backhauled through a central choke point and provides direct-to-cloud connectivity instead.
2.1 Applications

For this guide, we will be using the two applications listed in the table to the right:

<table>
<thead>
<tr>
<th>Application</th>
<th>DNS Name</th>
<th>Int IP</th>
<th>Ext IP</th>
<th>Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magento</td>
<td>magento.b2b.acmemodern.com</td>
<td>10.3.0.8</td>
<td>None</td>
<td>Microsoft Azure East US 2</td>
</tr>
<tr>
<td>CRM</td>
<td>crm.b2b.acmemodern.com</td>
<td>192.168.1.11</td>
<td>None</td>
<td>Amazon AWS US-West-2b</td>
</tr>
</tbody>
</table>

Table 1: Applications used in guide.

2.2 Users

When you signed up for Zscaler B2B Interactive, you received an email containing one read-only admin account for the admin interface, as well as two business customer accounts. Zscaler B2B supports multiple Identity Providers (IdP). This allows you to utilize your business customers’ own IdP instead of having to manage their users in your own user directory.

The table below lists the users created for you and the IdP used.

<table>
<thead>
<tr>
<th>User</th>
<th>Company</th>
<th>Username</th>
<th>Password</th>
<th>IdP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier</td>
<td>Apex Systems</td>
<td>PDR-#@apexsysstems.tech</td>
<td>Admin@123</td>
<td>Microsoft Azure AD</td>
</tr>
<tr>
<td>Vendor</td>
<td>Apogee One</td>
<td>PDR-#@apogeeone.net</td>
<td>Admin@123</td>
<td>Okta</td>
</tr>
<tr>
<td>IT</td>
<td>Acme Modern</td>
<td>PDR-#@b2b.acmemodern.com</td>
<td>Admin@123</td>
<td>Internal DB</td>
</tr>
</tbody>
</table>

Table 2: Lists end user and admin accounts.

2.3 Access Policy

Zscaler B2B uses a zero trust model, making sure users only have access to the applications they need and nothing more. With Zscaler B2B it’s possible to configure access policies based on any SAML attribute, which are generally derived from your or your business customer’s user directory such as Active Directory or Google G Suite User Directory.

For this guide, we will only use the IdP used as the policy criterion. Though it is possible to combine this with, for example, group membership or department as well. The table below shows the access policy:

<table>
<thead>
<tr>
<th>External User</th>
<th>Application</th>
<th>Supplier (Apex Systems)</th>
<th>Vendor (Apogee One)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Supplier</td>
<td>Block</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>Vendor</td>
<td>Block</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Table 3: Access policy
3. Test Plan

This test plan is created to explore and learn about the following items:

- With Zscaler B2B and the correct access rights, the CRM application is reachable seamlessly by the supplier end user.

- With Zscaler B2B and the correct access rights, the Magento application is reachable seamlessly by the vendor end user.

- Using Zscaler B2B, the IT end user can quickly navigate the admin portal and configure policy settings for secure B2B application access.

We will log in with users from different companies, each trying to access different applications. Zscaler B2B will determine for each user-application the best performing path. The traffic will never have to be backhauled to a central location before going to an application. The end-user will always have the best possible performance without having to choose a gateway, even when mobile and accessing the applications from different locations.

This guide is designed to highlight points of interest, but there is nothing stopping you from exploring the rest of the admin portal. In fact, it’s encouraged!

Note that in this test plan, anywhere a user is shown (such as user@apexsystems.tech), it needs to be replaced with the corresponding user that was emailed to you (such as PDR-#####@apexsystems.tech)
3.1 Test Access with B2B Supplier User

This test will show that when logged in as a user from Apex Systems, the CRM application is accessible. However, the Magento application isn’t. This will also show the user portal for this user.

Note that since we will login as a different user in the next test, it’s easier to use “Incognito Mode”, “In Private Window” or “Private Browsing” functionality of your browser so it’s not needed afterward to logout but only close the windows.

Part 1

In a new Incognito Window, browse to https://crm.b2b.acmemodern.com

You will be prompted to enter your username. This prompt is to determine which IdP to use. When only using a single IdP, this prompt does not appear and the page will go straight to the IdP’s login page.

Enter your Apex Systems’ user and click “Sign in”.

Since Apex Systems is using Microsoft Azure AD, you will get the Microsoft login prompt. Login with your Apex Systems’ user and password.

After logging in, you will be forwarded to the CRM application as expected since the access policy allows it.
3.1 Test Access with B2B Supplier User (Cont.)

Part 2

It is likely that a business customer’s user would already be logged into their IdP. In that case, they would not get the Microsoft login prompt. Since we are now logged in, let’s try the other application.

Browse to https://magento.b2b.acmemodern.com

Since we are already logged into Zscaler B2B, we don't have to authenticate again. However, we don't get access to the application because there is no policy defined that allows us access. So, access is blocked.
3.1 Test Access with B2B Supplier User (Cont.)

**Part 3**

Zscaler B2B also has User Portals. As we have shown in the previous part, we can access applications by going to their URL. However, if you have many applications that need to be accessed by business customers, it is easier to setup a User Portal. A User Portal can contain the applications someone has access to as well as publicly available links.

Zscaler B2B User Portal only shows the applications someone has access to. So, it’s possible to have a single User Portal serving users with different access rights.

Browse to [https://portal.b2b.acmemodern.com](https://portal.b2b.acmemodern.com)

This user’s portal shows the CRM application as well as a public link for Zscaler. Clicking on either will directly forward you to the selected destination, as you are already logged into Zscaler B2B.
3.2 Test Access with B2B Vendor User

This test will show that when logged in as a user from Apogee One, the Magento application is accessible. However, the CRM application isn’t. This will also show the user portal for this user. Finally, the test will show an isolated browser session for this user. Make sure you close all the Incognito Mode browser windows so that the Apex Systems user isn’t logged in anymore.

Part 1

Open a new Incognito Mode window and navigate to https://magento.b2b.acmemodern.com

As before you will get prompted to provide your username so Zscaler B2B can determine which IdP to use. Enter your Apogee One username and click “Sign in”.

Since Apogee One uses Okta as their IdP, you are presented with the Okta login screen. Sign in with your Apogee One credentials.

After logging in, you will be forwarded to the Magento Web Store application.
3.2 Test Access with B2B Vendor User

Part 2

As you remember from the Access Policy that is defined, Apogee One users have access to the Magento application, but not the CRM application.

Browse to https://crm.b2b.acmemodern.com

Access is denied, as is expected.

Part 3

Apogee One users use the same User Portal as Apex Systems users. However, since their access is not the same, let’s verify that the User Portal shows the correct applications.

Navigate to https://portal.b2b.acmemodern.com

And indeed, the User Portal now shows Magento, but not CRM.
3.2 Test Access with B2B Vendor User (Cont.)

Part 4

Next, open a new Incognito window and navigate to https://magento.b2b.acmemodern.com/admin_ovhk2

Because you will now be visiting the Administrative portion of the web application, please log in with the following credentials:

**Username:** vendoruser  
**Password:** Admin@123

Upon successful authentication with the above-listed credentials, you will now be presented with the Magento administrative portal.
3.2 Test Access with B2B Vendor User (Cont.)

Notice the “Heads Up!” alert bar at the top of your browser, which is informing you that this session is running within Zscaler Browser Isolation. With Browser Isolation, a user can view sensitive content, but only within a ‘virtualized’ browser running within their local browser, and only with whatever actions the organization deems appropriate for the user.

In a Browser Isolation session, rather than rendering the page as normal in the user’s browser, the user can interact with the page just as they typically would, but in reality what they are seeing is essentially an interactive image of the website, not the website itself. Because of this level of separation between user and content, it is easy to set up limitations around user behavior — in this case, the “vendor user” user can view the Magento Admin application, but cannot upload or download anything to or from the app.
3.2 Test Access with B2B Vendor User (Cont.)

To verify this, click on “Sales” in the menu bar on the left, and select Invoices.

From the Invoices panel, click on the “View” option for the top-most entry.
3.2 Test Access with B2B Vendor User (Cont.)

From the resulting Invoice detail screen, click Print.

Upon clicking the Print option, a PDF entry appears in the bar along the bottom of the window, as shown below.
3.2 Test Access with B2B Vendor User (Cont.)

Click this PDF entry, and in the PDF Preview screen that appears, try to download the summary document by clicking here:

![PDF Preview Screen](image)

As you can see, the PDF is visible to the user, but cannot be saved to their local machine — it remains within the Browser Isolation window.

As another example of how Zscaler Browser Isolation can help limit the spread of sensitive data or content, try selecting some text within the Browser Isolation window (for instance, the mailing address seen in an existing Order), and right-click on that text to Copy it to the clipboard.
3.3 Test Access and Navigation with the IT Admin User

The Zscaler B2B Admin UI is always available from any location with an internet connection. Admin logins support 2-factor authentication, as well as authenticating against an IdP using SAML. However, in this environment, the admin login names and passwords are stored in the Zscaler B2B Admin Database.

To access the Admin UI, navigate to https://admin.private.zscaler.com

You will be prompted with a login screen. Use your b2b.acemodern.com credentials to login.
3.3.1 Applications Dashboard Overview

When logging in, the first screen is the Applications Dashboard.

This dashboard allows a quick overview of your apps, including top applications by bandwidth, top applications by users, and any errors/policy blocks. An example error would be when a connector cannot reach an application because the application is down. Policy blocks are attempts made by users to access an application that they do not have access to according to the configured access policy. For each dashboard, at the top, you can change the timeframe for which to show the widgets.
3.3.2 Users Dashboard Overview

Navigate to the “Users” tab at the top.

The second dashboard is the Users Dashboard. This dashboard has similar information, though from the users’ perspective instead of the applications’ perspective. It’s a great way to find users who are trying to access applications they shouldn’t or users who use the most bandwidth.
3.3.2 **Health Dashboard Overview**

Navigate to the "Health" tab at the top.

The last dashboard is the Health Dashboard. This dashboard differs a lot from the previous two and is a graphical representation of the health status of your apps, servers, and connectors.

At the top right of each section, there are filters on what to show based on the status of the applications, servers, or connectors. Each application/app connector/service edge has an icon on it depicting the health status. There are multiple possible health statuses as listed in the table below.

<table>
<thead>
<tr>
<th>Status</th>
<th>Applications</th>
<th>App Connectors</th>
<th>Service Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Functioning as expected</td>
<td>Functioning as expected</td>
<td>Functioning as expected</td>
</tr>
<tr>
<td>Down</td>
<td>Application is down or no app connector can reach the application</td>
<td>App connector is down</td>
<td>App connector is down</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>Application is still accessible but one or most servers hosting it is unhealthy or down</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Unknown</td>
<td>Application is configured for &quot;On Access&quot; health reporting and no user has accessed the application in the last 30 minutes</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
3.3.2 Health Dashboard Overview (Cont.)

It’s possible to see more data for each of the items in the dashboard by hovering your mouse over them.

When hovering your mouse over an application, an icon in the top right appears.

Clicking this icon will show you a diagram of how the application is accessed by which servers and which App Connectors.
### 3.3.3 App Connectors Dashboard Overview

Navigate to the "App Connectors" tab at the top.

This dashboard will give you an overview of all your App Connectors. It is possible to view graphs here as well.
3.3.4 Application Segment Configuration

Navigate to Administration → Application Segments.

This page is to define the applications you want accessible through Zscaler B2B. To view an application, click the pencil edit icon next to the CRM application.

In this screen you can configure how the application will be accessed. Even if the application itself only supports port 80 (HTTP), traffic will never go unencrypted over the internet. The App Connector, which is hosted on the same network as the application will use HTTP, but all other traffic (App Connector to Zscaler Cloud, User to Zscaler Cloud) is all in TLS tunnels with strong encryption.
3.3.5 Access Policy

The Access Policy defines who is allowed access to which applications and application group. The rules are evaluated top to bottom and stops when a match is found. In our environment, we have two rules. One for allowing Apex Systems access to CRM and one rule for allowing Apogee One access to Magento. Any access attempt that isn’t explicitly allowed will be denied. Click on the pencil edit button next to “Magento Access for Apogee One”.

It is possible to select a single application segment, multiple application segments or, more commonly used, application segment group(s) that group together multiple applications. Decisions can be based on any SAML attribute that the SAML IdP returns, but most commonly used are group membership or departments. Generally, these attributes are derived from your user directory, such as Microsoft Active Directory or Google G Suite User Directory. It is possible to enter multiple SAML attributes. For example, it’s not required to make multiple rules to give multiple departments access to an application (group). Zscaler B2B supports having multiple IdPs per tenant. In our environment, we allow access based on the IdP used to authenticate the user.
3.3.6 Diagnostics Interface

Navigate to Diagnostics on the left hand panel.

This page contains the logs for all activity and status changes and allows for drilling into sessions revealing lots of important details. There are four different log types that can be viewed: User Activity, User Status, Private Service Edge Status and Connector Status. By default, the page is on User Activity. For this guide, we will examine events that were generated in the previous steps by filtering the events. As noted, by default the Diagnostics Page is set for the “User Activity” Log Type. Verify it is set to “User Activity” at the top of the page. By default, no filters are applied to the logs, showing all log entries for the time period selected. Click on the “Add Filters” link and select “Username” from the dropdown box. Start typing the username for your users (PDR-#####) and select both when presented. Click “Apply”. If no entries show up, make sure that the correct time period is selected at the top of the page. By default, it is set for the last 24 hours.
3.3.6 Diagnostics Interface (Cont.)

Select “Successful” at the top.

Expand one of the entries. Information is grouped together in columns based on:

- Connection
- Policy
- User
- Service Edge
- App Connector
- Application

Some of the interesting details include start-stop time, the policy used, and locations of the user and Service Edge.

This session was a success, showing that the user, user@apogeeone.net, accessed magento.b2b.acmemodern.com on port TCP/443, which was allowed by the policy “Magento Access for Apogee One”.
3.3.6 Diagnostics Interface (Cont.)

Now select the "Access Policy Blocks" at the top.

Expand one of the entries and notice that access was denied because there was no policy configured allowing access.
3.3.7 Live Logs

The Diagnostics page has lots of valuable information on events that already happened. However, Zscaler B2B also provides Live Logs, which will show you log entries as events happen, making it a valuable tool for troubleshooting.

Navigate to “Live Logs” in the left pane.

It is possible here to add filters like specific users or specific applications to only show events that you are interested in. Enter your Apogee One user under “User”. Leave this window open and open a new window.

Navigate to https://crm.b2b.acmemodern.com

If you are still logged in as your Apogee User, you will get the blocked message. Otherwise, you will have to login again.
3.3.7 Live Logs (Cont.)

Right after trying to access the CRM application, Zscaler B2B informs us that there are new logs. Click on "New Logs" and expand one of the entries.

This will show you the same information as the diagnostics page but in a real-time fashion.
4. Conclusion

This guide demonstrated how Zscaler B2B operates with a zero trust model, allowing business customers and partners to securely access your applications while keeping them off your network.

This guide also demonstrated that it does not matter where an application is hosted—corporate data center, private or public cloud—including geographic location. An end-user will always automatically get the best possible performance.

Lastly, this guide demonstrated how the Zscaler B2B Admin UI makes it easy for administrators to configure remote access to internal business customer applications. It showed the detailed information that gets logged for each session, including how easy it is to find that information using filters.

In this guide, we showed you the highlights of ZB2B, but there's even more to see and it is encouraged to look around!