User Provisioning and Authentication to Zscaler Services

Reference Architecture — Zscaler for Users

Contents

About Zscaler Reference Architectures Guides 1

Who Is This Guide For? 1

A Note for Federal Cloud Customers 1

Conventions Used in This Guide 1

Finding Out More 1

Terms and Acronyms Used in This Guide 2

Introduction 3

New to ZIA or Zero Trust? 5

User Provisioning and Authentication 6

Provisioning Users' Accounts 7

Authenticating Users 7

Recommendations 8

Resources 8

User Provisioning to ZIA 9

Selecting a Provisioning Protocol 9

SAML and SCIM (Recommended) 11

SAML Auto-Provisioning 12

Zscaler Authentication Bridge 13

LDAP Directory Server Synchronization 14

User Authentication to ZIA 15

Understanding Authentication Cookies 15

Authenticating Users Using SAML 16

Authenticating Users Using the Zscaler Authentication Bridge 18

Authenticating Users Using LDAP Directory Server Authentication 19

Authentication from Known and Unknown Locations 21

User Authentication Frequency 22

Handling Traffic from Applications that Cannot Authenticate 22

Summary 23

About Zscaler 23

About Zscaler Reference Architectures Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the **Zscaler website** (**https://www.zscaler.com/resources/reference-architectures**).

You can join our user and partner community and get answers to your questions in the **Zenith Community** (**https://community.zscaler.com**).

Terms and Acronyms Used in This Guide

Acronym	Definition
AD	Active Directory
API	Application Programming Interface
DC	Data Center
DMZ	Demilitarized Zone
IdP	Identity Provider
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SP	Service Provider
SSE	Security Service Edge
SSL	Secure Socket Layer (superseded by TLS)
SSO	Single Sign-On
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
ZAB	Zscaler Authentication Bridge
ZCA	Zscaler Central Authority
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

Introduction

Zscaler Internet Access (ZIA) is a cloud native Security Service Edge (SSE) solution that builds on a decade of secure web gateway leadership. ZIA is a part of Zscaler's cloud platform, the Zero Trust Exchange (ZTE), the world's largest security cloud.

ZIA replaces legacy network security appliance solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach. Inspection covers your organization's users and devices, including mobile users and IoT devices. With data centers located around the world, your users avoid latency associated with traditional VPN backhaul strategies. The same policies and protections follow your users no matter where they connect.

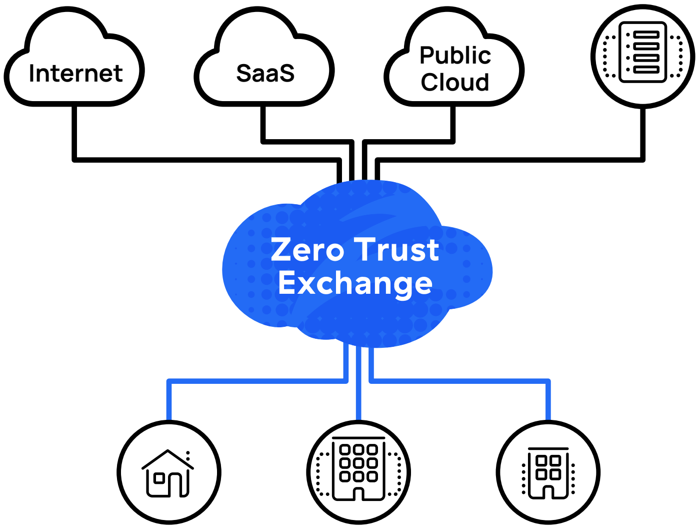

Figure 1. ZIA protects your users, devices, and data everywhere they connect

With ZIA, you can enable zero trust access to internet sites and web applications. This least-privilege access model gives you the controls to enforce your acceptable use policy (AUP). Unlike traditional firewalls and other controls, Zscaler builds policy based on more than just user credentials.

Instead of building and fitting a user into roles, you can design policies with conditions that must be true for your users to be granted access to resources. The user's authentication credentials are the first step in determining which policies are applied to a user based on the response from your identity provider (IdP). Zscaler partners with industry leading IdPs, such as Azure Active Directory (AD), Okta, or PingFederate. Responses from the IdP can include:

- The user's identity
- The user's department
- The user's group membership

Policy assignment with ZIA considers the entire user context, which you can then use to refine and tighten policy. By evaluating the user, the machine, and the location, you can allow or deny the same user access to applications and websites. A positive authentication can be combined with other aspects of the user's context such as:

- The user's current location
- The device a user is connecting with and its posture
- Time of day

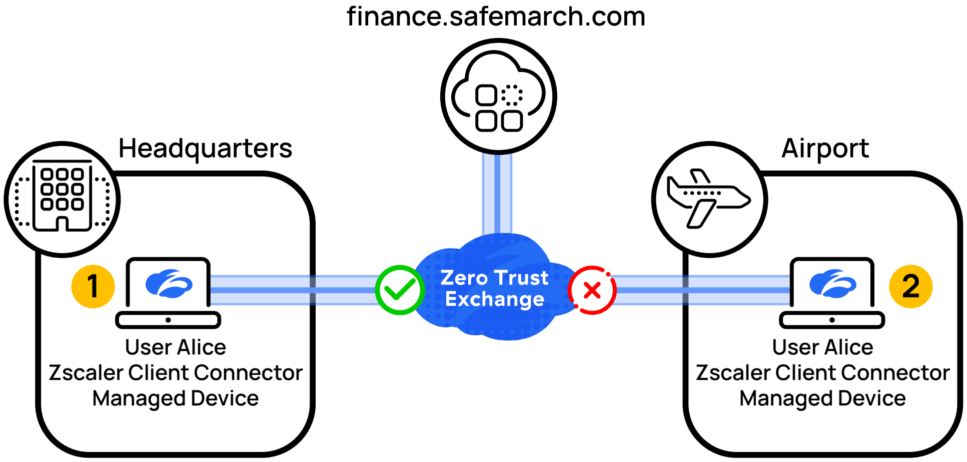

Figure 2. Authentication is more than user identity and context can be used to determine access

As an example, you might only allow your users to connect to your financial application if they are a member of the finance team, located at your organization's headquarters location, and using an organization-issued laptop with Zscaler Client Connector installed and connected. When a user matches these conditions, as in number 1 in the image, they are granted access to the application. If the same user is traveling and attempts to access the application from the same laptop using the same credentials, but is in an airport as in number 2, they are denied access.

Depending on the user's authentication and posture information, you assign policy rules to allow or deny access to destinations. This differs from role-based access policies that force you to create different static roles. With ZIA, you instead evaluate the user, device, location, group, and more to determine which policies to apply. This granular control allows you to build a security policy that matches your organizational goals and work styles.

In this guide, we discuss provisioning and authentication methods for your users, and supported options and recommend best practices to get your users up and running. Other guides in this series explore policy development. Here, we build the foundation of policy enforcement by making sure your authorized users can authenticate to the ZIA service.

New to ZIA or Zero Trust?

If this is your first time reading about Zscaler Internet Access or zero trust architectures, the following resources are available to get you started:

- For an introduction to ZIA, see the Zscaler website (https://www.zscaler.com/products/zscaler-internet-access).
- For an overview of the wider Zscaler Secure Service Edge, see the Zscaler website (https://www.zscaler.com/capabilities/zscaler-security-service-edge).
- For a complete list of available provisioning and authentication options, see Choosing Provisioning and Authentication Methods (https://help.zscaler.com/zia/choosing-provisioning-authentication-methods).
- For a list of Zscaler's identity technology partners, see the Zscaler website (https://www.zscaler.com/partners/technology/identity).
- To learn more about zero trust access, see What Is Zero Trust? (https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust).

User Provisioning and Authentication

This guide discusses the different authentication methods available in ZIA and the tradeoffs in each. The purpose of authentication is to give you the ability to create tailored policies that align with a user's role within your organization. While it is possible to apply policies based on a known location or dedicated proxy port, the policies applied treat all users from that location equally. By provisioning and authenticating your users, you can tailor access policy to the resources they require to fulfill their roles.

Authentication is the way we access resources on the internet where identification is important, and ZIA is no different. Many organizations have migrated to single sign-on (SSO) technologies from various vendors that allow your users to authenticate to many, if not all, the services they access with a single set or credentials. This is a benefit to your users, as they only have a single set of credentials to remember. By leveraging the same SSO with ZIA, the user's transition to ZIA from your legacy solutions can be much smoother.

While ZIA supports a broad number of authentication techniques, we focus on authentication options that are scalable, maintainable, and widely applicable to most organizations. This enables you to build a robust system for keeping ZIA synchronized with your existing IdP. By enabling authentication, your organization can move beyond traditional location- and role-based access, and instead define policy that meets the needs of your users and organization.

You should consult your IdP vendor's documentation to understand the specific capabilities of your authentication platform. You want to understand which methods are available to you for both provisioning and authentication of your users.

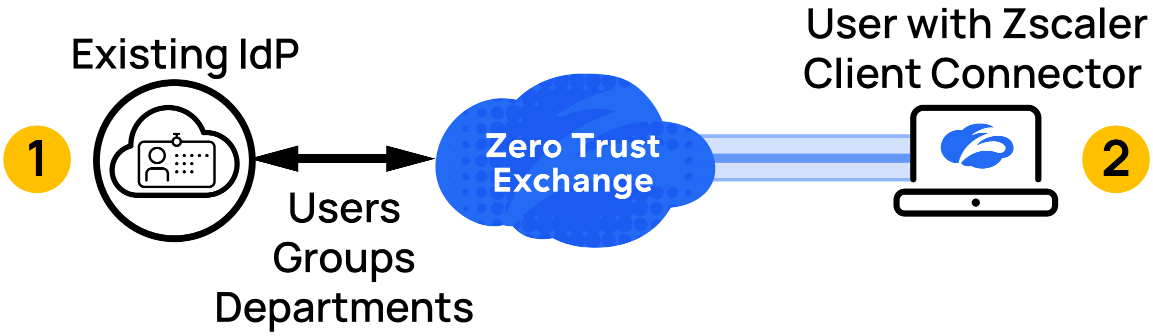

Figure 3. Users are first provisioned to use ZIA, and then can authenticate to the platform

When you configure ZIA to authenticate your users, there are two distinct sets of decisions to make:

1. Initial account provisioning and synchronization – In the provisioning phase, you determine how to get ZIA access to your user identity information. This includes user credentials, group membership, and department information. You must also determine how to synchronize changes to Zscaler when your organization updates user information.
2. User authentication method – In the authentication phase, you determine what protocol is used for your users to authenticate to the system. This is the mechanism used when your users are authenticating to confirm they are a part of your organization. This evaluation, along with the user's context, is used when determining policy.

While ZIA supports several provisioning and authentication methods, not all available on ZIA are necessarily the right choice for production environments. Some methods, such as Kerberos, have poor mobile support. Others, such as one-time links and one-time passwords, make sense for small demonstration environments or guest access, but don't provide the user information or scale you want when developing policy.

Provisioning Users' Accounts

The first step in authenticating your users to ZIA is making sure their accounts are accessible by the system. Your user's information is provisioned to ZIA by synchronizing it with your existing IdP. By leveraging your existing data store, you do not need to manually manage your user's credentials in multiple locations. Because of Zscaler's holistic approach to policy assignment, the provisioning process does not require you to create and assign roles within ZIA.

In **User Provisioning to ZIA**, we discuss the following provisioning options:

- SAML and SCIM (recommended)
- SAML Auto-Provisioning
- LDAP Directory Server Synchronization
- Zscaler Authentication Bridge

Provisioning pulls over usernames, groups, and department information for your users. Your passwords are not pulled over, making sure your complete user credentials are only available at your IdP.

Authenticating Users

After your users are provisioned to the cloud, we can now authenticate the users to the ZIA service. Like many systems, this involves your users providing their credentials to the system. These credentials are checked against your IdP to ensure your users are valid members of your organization and should be provided access. This includes authentication help for applications that cannot authenticate to ZIA.

In **User Authentication to ZIA**, we discuss the following options for user authentication to ZIA:

- SAML
- Zscaler Authentication Bridge
- LDAP Directory Server Synchronization

In addition to the authentication method, this guide covers other aspects of user authentication. These include your reauthentication interval and how to handle traffic from applications that cannot authenticate.

Recommendations

For both provisioning and authentication, Zscaler recommends using Security Assertion Markup Language (SAML). The ease of use, wide adoption, and strong industry support make SAML the right choice for most organizations. You might already have a SAML provider such as Azure Active Directory (AD), Okta, or PingFederate.

If you choose to use SAML, Zscaler also recommends the use of System for Cross-Domain Identity Management (SCIM) to keep changes synchronized in near-real time. While SAML itself can provide an update mechanism, SCIM is recommended to keep users in sync ahead of their next session authentication.

If your users connect from known locations, it is possible to set up policy based on that location without authentication. However, this approach lacks the ability to build policy based on the user's groups and departments and limits reporting. Zscaler instead recommends that you authenticate all user devices where possible.

Zscaler recommends a reauthentication interval of only once. This means your users are not forced to reauthenticate to use the service. Because Zscaler is not providing privileged access to applications, there is no security concern for users staying logged in.

For devices and applications that cannot authenticate, Zscaler also recommends the use of surrogate IP. The surrogate IP feature maps a user's private IP address to other traffic seen by the service that does not have the capability of authenticating. This can include applications such as Google Earth or Skydrive that do not support cookies, unknown user agents, and undecrypted HTTPS sessions. Zscaler recommends using surrogate IP as a best practice to enable consistent access for users with proper reporting.

Resources

For a full list of authentication options, see **Choosing Provisioning and Authentication Methods** (**https://help.zscaler.com/zia/choosing-provisioning-authentication-methods**).

For a complete list of Zscaler's identity technology partners, see the **Zscaler website** (**https://www.zscaler.com/partners/technology/identity**).

User Provisioning to ZIA

Provisioning users to ZIA is the first step in developing and deploying granular access policies. When you provision your users to ZIA, you upload your user ID, group, and department information to ZIA. This information is used to authenticate users to the system as they send traffic. You also use the information contained in the response to make policy-based forwarding decisions. User and department information is also used for reporting and analytics, either at the user or group level. Finally, you want to keep your identity data synchronized with your existing identity store.

First let's examine the data about the user, and how this data is used in ZIA.

- User IDs – A user ID can be included as a decision criterion in policies, as well as in reports and analytics. The user ID must be in the form of an email address. The email address does not have to be a valid address, but it must be unique, and its domain must belong to the organization. User data is often useful in finding out who is accessing a particular application or site, or who is using the majority of the bandwidth at a site.
- Groups – Groups can be included as criteria in policies to control access. You can use groups to define access to applications, such as applications specific to a user's role. For example, you might give your social media managers unlimited access to social media sites while restricting other users' access. A user can be a member of up to 128 groups.
- Departments – A department is like a group in that it can be used as both a policy criterion and a reporting and analytics input. Unlike groups, a user can belong to only one department at a time. Departments are useful for limiting access to applications or aggregate reporting on members of a group.

Later guides in this series focus on leveraging this information for policy and reporting purposes.

Selecting a Provisioning Protocol

Determining which protocol to use when provisioning your users to ZIA is primarily driven by your existing IdP vendor. In the following image, we present a decision tree that can help you understand your options for deployment. The two most common identity provisioning systems are Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP).

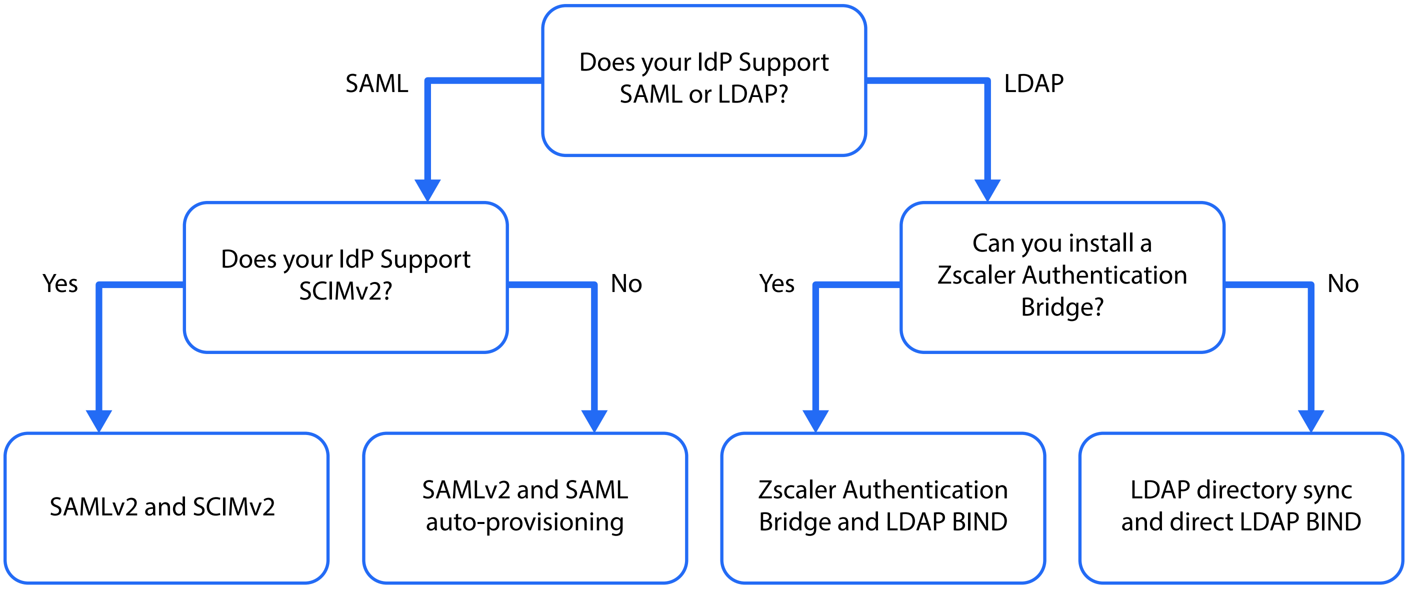
Does your IdP Support SAML or LDAP?
SAML
LDAP
Does your IdP Support SCIMv2?
Yes
No
Can you install a Zscaler Authentication Bridge?
Yes
No
SAMLv2 and SCIMv2
SAMLv2 and SAML auto-provisioning
Zscaler Authentication Bridge and LDAP BIND
LDAP directory sync and direct LDAP BIND

Figure 4. The provisioning list should be used in conjunction with your IdP vendor's documentation to select your provisioning method

You might have already encountered SAML if your organization uses a single sign-on (SSO) service to enable access to tools, especially for web-based applications. SAML was designed to standardize security authentication across security domains. SAML consists of three primary entities: the user, the identity provider (IdP), and the service provider (SP), which in this case is ZIA. When a user attempts to authenticate, the SP requests an authentication assertion from the IdP. After that assertion has been provided, the SP can use that information to decide what access to resources it will allow for the user.

NOTE
Zscaler supports SAML version 2.0 and above.

Many organizations rely on LDAP for their user account management. This might be through a commercial product, such as Microsoft Active Directory, or via an open-source project such as OpenLDAP. The LDAP system was designed to be accessed by multiple applications over a TCP/IP connection to provide authentication for users. LDAP servers are queried by LDAP clients, in this case ZIA.

If SAML is not an option for your organization, LDAP synchronization is your next best option. Zscaler supports two methods for synchronization: the **Zscaler Authentication Bridge** and direct **LDAP Directory Server Synchronization**.

After your users are provisioned, you must also update them as your organization evolves over time. Your organization will have changes in people, roles, and organizations, and you must ensure that these changes are also updated on ZIA. The goal is to have these changes automatically synchronized to ZIA. Manual synchronization risks users having different states on the IdP versus ZIA, and is more likely to encounter human error when a change needs to be made twice. The following protocols and tools can help you manage synchronization:

- About SAML (https://help.zscaler.com/zia/about-saml)
- OASIS Security Services (SAML) (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
- LDAP website (https://ldap.com/)

SAML and SCIM (Recommended)

The use of SAML in enterprise deployments and tools has grown quickly in recent years. By filling the gap in authentication across security domains, SAML is often the tool of choice for SSO authentication. While SAML can handle provisioning on its own (see SAML Auto-Provisioning), SCIM updates are much faster than auto-provisioning.

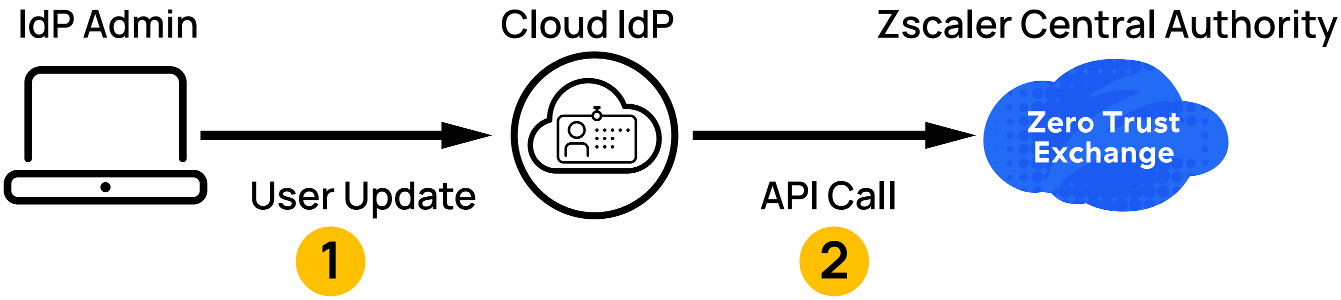

Figure 5. SCIM pushes updates via API calls to ZIA

When you enable SCIM updates, ZIA is updated in near-real time. SCIM leverages web API calls to ZIA to update identity information as it is updated in the data store.

1. An administrator makes a change to the user store at your IdP, in this example a cloud IdP vendor (recommended).
2. The Cloud IdP in turn makes an API call to the Zscaler Central Authority (ZCA), updating the user identity information.

This includes provisioning of new users, updating as changes occur, and deprovisioning users. SCIM also has the advantage of not needing an inbound connection to your IdP, as the API call is outbound only.

To leverage SCIM, you must have a SCIM client connected to your IdP to push changes to ZIA over the API. Most major providers have SCIM clients integrated into their products, including Microsoft Azure AD, Okta, and PingFederate.

Zscaler recommends combining SAML and SCIM to be used together to provision and maintain your identity information in ZIA.

NOTE
Zscaler supports only SCIM version 2.0, and it must be used with SAML for authentication. No other authentication types are supported.

SAML Auto-Provisioning

If your organization is using SAML, but your IdP does not support SCIM updates, SAML auto-provisioning is the next best alternative. With SAML auto-provisioning, identity information is retrieved from the IdP when a user attempts authentication.

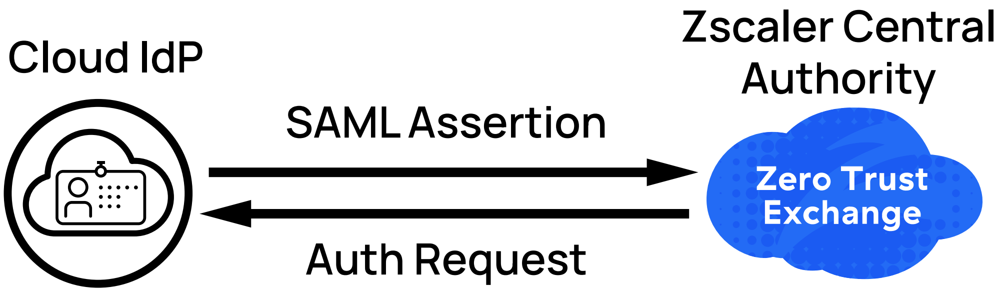

Figure 6. SAML auto-provisioning updates user information based on the information returned in the user's assertion

If successful, the user identity information is added to the database, including username, groups, and department information. The following actions are taken by auto-provisioning:

- New users who previously did not exist are added to the ZIA database with their identity information from the SAML response.
- If a user exists, but the SAML response has updated identity information, that information is updated in the ZIA database. This change can include removing information, including the user if they are no longer active in the IdP database.

While SAML auto-provisioning and SCIM result in effectively the same action, SCIM is a proactive change when the IdP is updated. Auto-provisioning is a reactive update, only changing database information when a user attempts to authenticate.

NOTE
Zscaler supports SAML responses up to 4 MB in size.

To learn more, see [About SAML](https://help.zscaler.com/zia/about-saml) (https://help.zscaler.com/zia/about-saml).

Zscaler Authentication Bridge

Synchronizing LDAP with the Zscaler Authentication Bridge (ZAB) eliminates the need to directly connect ZIA to your LDAP server. In this model, a virtual machine exists between your LDAP server and the ZIA service, typically in your DMZ. The ZAB is used to import your user identity information into ZIA without requiring an inbound connection. The ZAB can also be used for authentication if you are using client TLS certificates.

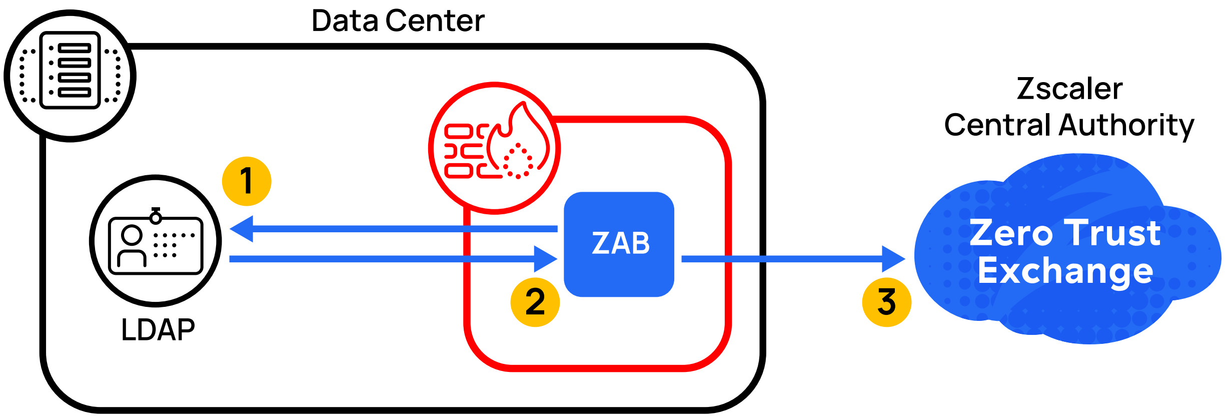

Figure 7. The ZAB connects your IdP to the ZCA to authenticate and synchronize user identity information

1. LDAP queries originate from the ZAB to your LDAP server.
2. The LDAP server responds with the requested user identity information.
3. This information is forwarded on to the ZCA.

When you configure the ZAB, you can choose a synchronization interval: on demand, daily, weekly, or monthly. This information includes user identity, groups, and departments. The ZAB does not synchronize passwords, as those remain stored on your LDAP system.

During the authentication process, the ZCA forwards the authentication request to the ZAB. The ZAB challenges the user on behalf of your LDAP server, proxying the request to the LDAP server for final determination. It then signals the result back to the ZCA.

When synchronizing identity data with ZIA, the ZAB can:

- Add users, groups, and departments that exist on the LDAP server but not on the ZIA service.
- Remove users, groups, and departments that exist on the ZIA service but not on the LDAP server.

NOTE
When using the ZAB, the LDAP server is considered the single source of truth, and the ZIA database is modified to match the LDAP server.

To learn more, see **About the Zscaler Authentication Bridge** (**https://help.zscaler.com/zia/about-zscaler-authentication-bridge**).

LDAP Directory Server Synchronization

If both SAML and the ZAB are unavailable to your organization, you need to connect ZIA directly to your LDAP server. In this model, you need to open firewall ports to support a direct connection to the server from the ZCA over a TLS link using secure LDAP.

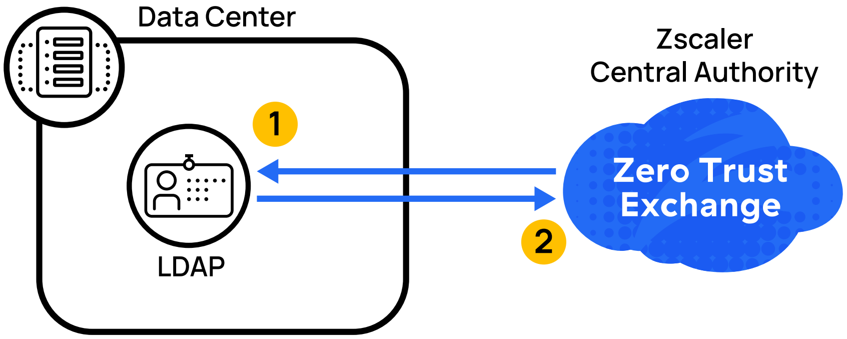

Figure 8. Direct LDAP synchronization is possible between your LDAP server and the ZCA

1. The ZCA binds directly to your LDAP instance. This requires that ports be opened on your firewall from Zscaler IP addresses.
2. Your LDAP server responds with the user's identity information, but not passwords, directly from the ZCA.

When the ZCA imports user information, it can:

- Add users, groups, and departments that exist on the LDAP server but not on the ZIA service.
- Remove users, groups, and departments that exist on the ZIA service but not on the LDAP server.

NOTE
The LDAP server is considered the single source of truth, and the ZIA database is modified to match the LDAP server.

When a synchronized user logs in, the ZCA presents the password request form. It then performs an LDAP BIND request with the user's username and password. ZCA never stores the user's password in its database.

User Authentication to ZIA

After users are provisioned, they must authenticate to the ZIA service. The authentication method you choose is driven by your IdP's supported protocols. In this section, we look at options for user authentication:

- Identity federation using SAML
- Directory server synchronization
- The Zscaler Authentication Bridge (ZAB)

These options are the most scalable solutions for user authentication. Zscaler supports additional authentication methods that are beyond the scope of this guide, primarily because they lack the scalability and flexibility of the other three authentication methods. Zscaler uses cookies to record a user's authentication state.

In addition to specifying which authentication method your users will use, you can also set the reauthentication interval. This determines how often a user is prompted to reauthenticate to ZIA.

The final piece of authentication is handling traffic that cannot authenticate, such as legitimate applications that do not accept cookies. We discuss how you can map that traffic back to your users.

For a complete list of authentication methods, see **Choosing and Provisioning Authentication Methods** (**https://help.zscaler.com/zia/choosing-provisioning-authentication-methods**).

Understanding Authentication Cookies

When a user authenticates to the ZIA service, several cookies are set. These cookies are used to determine the user's authentication status to the service. When a user authenticates, they receive the following cookies:

- Gateway cookie – This cookie contains the user's login information, including current login state and number of logins.
- Acceptable use policy cookie – When a user accepts the AUP, the ZIA Service Edge sets this cookie.
- Domain cookies – For each site that a user browses, the ZIA Service Edge sets a cookie for that domain. This prevents having to reauthenticate the user for domains they have already visited. Domain cookies have a life span of 12 hours.

Some applications do not support cookies, and therefore cannot be authenticated. For these types of applications, see **Handling Traffic from Applications that Cannot Authenticate** in this guide.

For more information, see **About Zscaler Cookies** (**https://help.zscaler.com/zia/about-zscaler-cookies**).

Authenticating Users Using SAML

When you use SAML for authentication, there are two ways a user can authenticate to the service: service provider-initiated SAML and IdP-initiated SAML. In both cases, the user is authenticated to ZIA, but the difference is where the user starts. Both authentication methods can be used at the same time to allow maximum flexibility for the end user.

Service Provider-Initiated SAML

In this use case, the user attempts to go to any URL or web application, and the ZIA Service Edge first checks to see if the user is authenticated. Because the user in this case is not authenticated, the service begins the authentication process with your IdP. This is a very common model for users because it requires no additional step to trigger authentication.

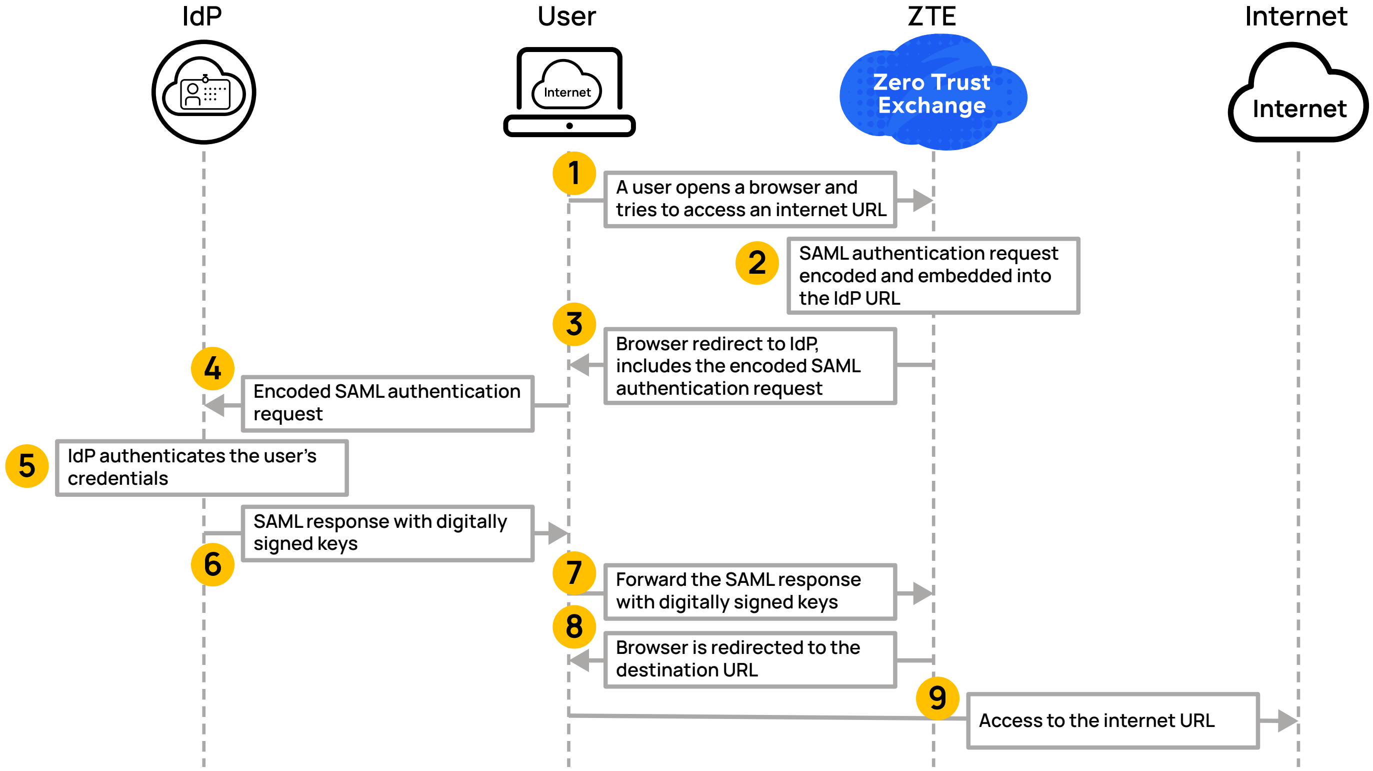
IdP
User
ZTE
Internet
Internet
Zero Trust Exchange
Internet
1 A user opens a browser and tries to access an internet URL
2 SAML authentication request encoded and embedded into the IdP URL
3 Browser redirect to IdP, includes the encoded SAML authentication request
4 Encoded SAML authentication request
5 IdP authenticates the user's credentials
6 SAML response with digitally signed keys
7 Forward the SAML response with digitally signed keys
8 Browser is redirected to the destination URL
9 Access to the internet URL

Figure 9. Service provider-initiated SAML authentication

1. A user opens a browser and tries to reach a website.
2. The Zscaler service generates a SAML authentication request, which is encoded and embedded into the URL for the IdP.
3. The service sends a redirect to the user's browser that includes the encoded SAML authentication request to be submitted to the IdP.
4. The user's browser submits the authentication request to the IdP.
5. The IdP does the following:
    a. Decodes the SAML request.
    b. Extracts the URL for the Customer Assertion Service (CAS) of Zscaler.
    c. Authenticates the user by login credentials or by checking for a valid Active Directory session.
6. The IdP generates a SAML response with digitally signed public/private DSA/RSA keys, encodes it, and sends it to the browser.

7. The browser forwards the SAML response to the service, and the CAS of Zscaler uses the IdP's public key to verify the response.
8. After the service successfully verifies the response, it logs in the user and redirects the user's browser to the destination URL.
9. The user can now access the destination URL based on your organization's policy.

IdP-Initiated SAML

In this use case, the user first logs into their IdP via their SSO portal. These portals have tiles for applications that the user is authorized to access. Zscaler appears as an application tile that can be clicked on to launch the application. When the user clicks the tile, they are authenticated to ZIA in the background.

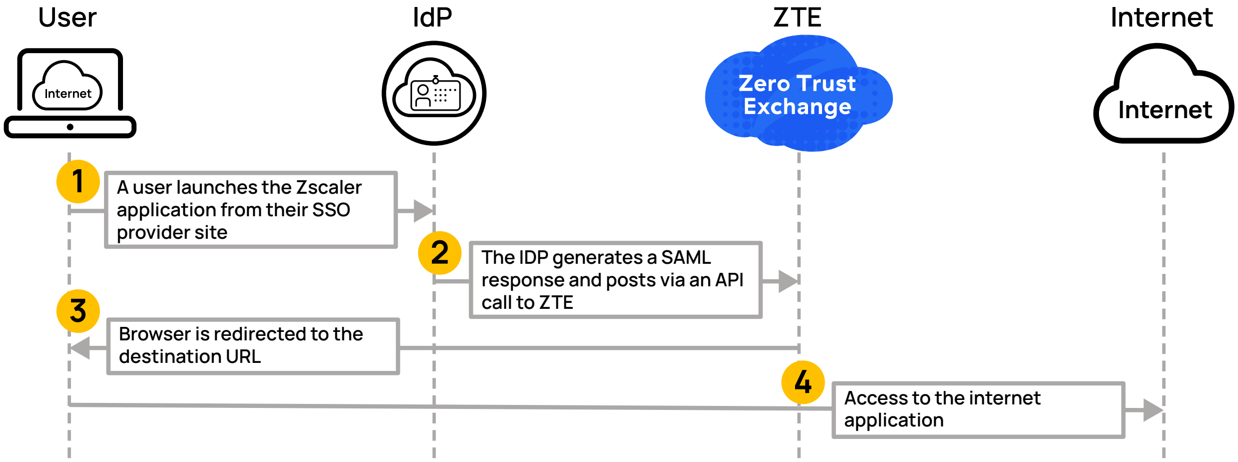
User
IdP
ZTE
Internet
Internet
Zero Trust Exchange
Internet
1
A user launches the Zscaler application from their SSO provider site
2
The IDP generates a SAML response and posts via an API call to ZTE
3
Browser is redirected to the destination URL
4
Access to the internet application

Figure 10. Identity provider-initiated SAML login

1. The user logs into their IdP. From the IdP's portal, they select the an application icon.
2. The IdP posts a SAML response to the API for the Zscaler Central Authority (ZCA).
3. The user's browser is redirected through the ZIA Service Edge, as the user was previously authorized by signing into the IdP.
4. The user can now access the destination URL based on your organization's policy.

In this use case, the SSO portal acts as a bookmark and authentication service. To learn more about SAML configuration, see **Configuring SAML** (**https://help.zscaler.com/zia/configuring-saml**).

Authenticating Users Using the Zscaler Authentication Bridge

The Zscaler Authentication Bridge (ZAB) can be used for both provisioning of user identity information as well as authenticating your users. The ZAB runs as a virtual machine and acts as a proxy for the ZCA. The ZAB is typically deployed in the DMZ with secure access to your directory server on the inside connection.

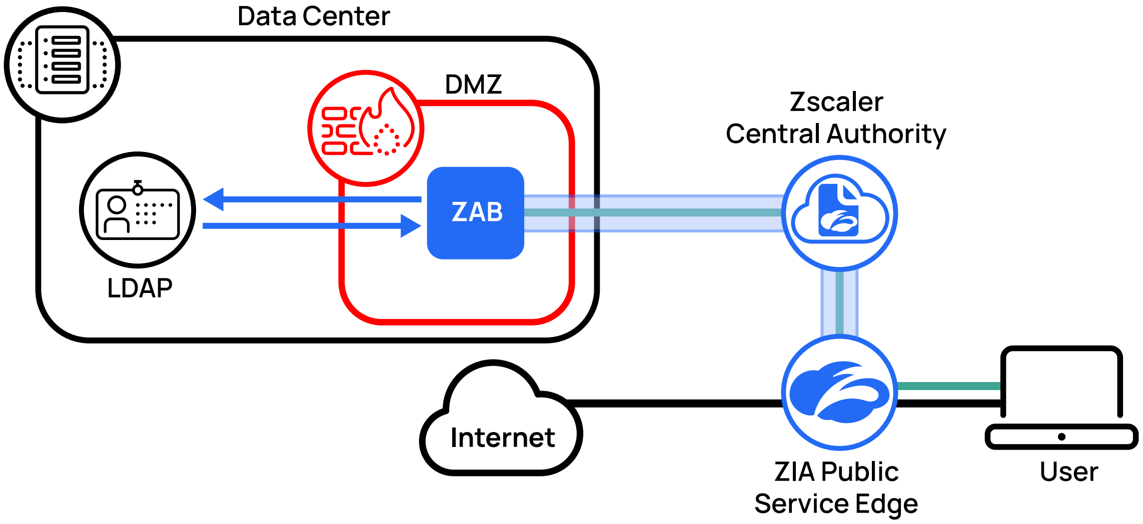

Figure 11. The ZAB works with the ZCA and the ZIA Service Edge to authenticate users

In the previous image, the green line represents the authentication path that occurs as the user is authenticated. In this case, the user is presented with a login form by the ZIA Service Edge requesting the username. The ZIA Service Edge takes the response and forwards it to the ZCA, which in turn forwards it to the ZAB. The ZAB requests the user's password. Remember, ZIA does not store your user's passwords.

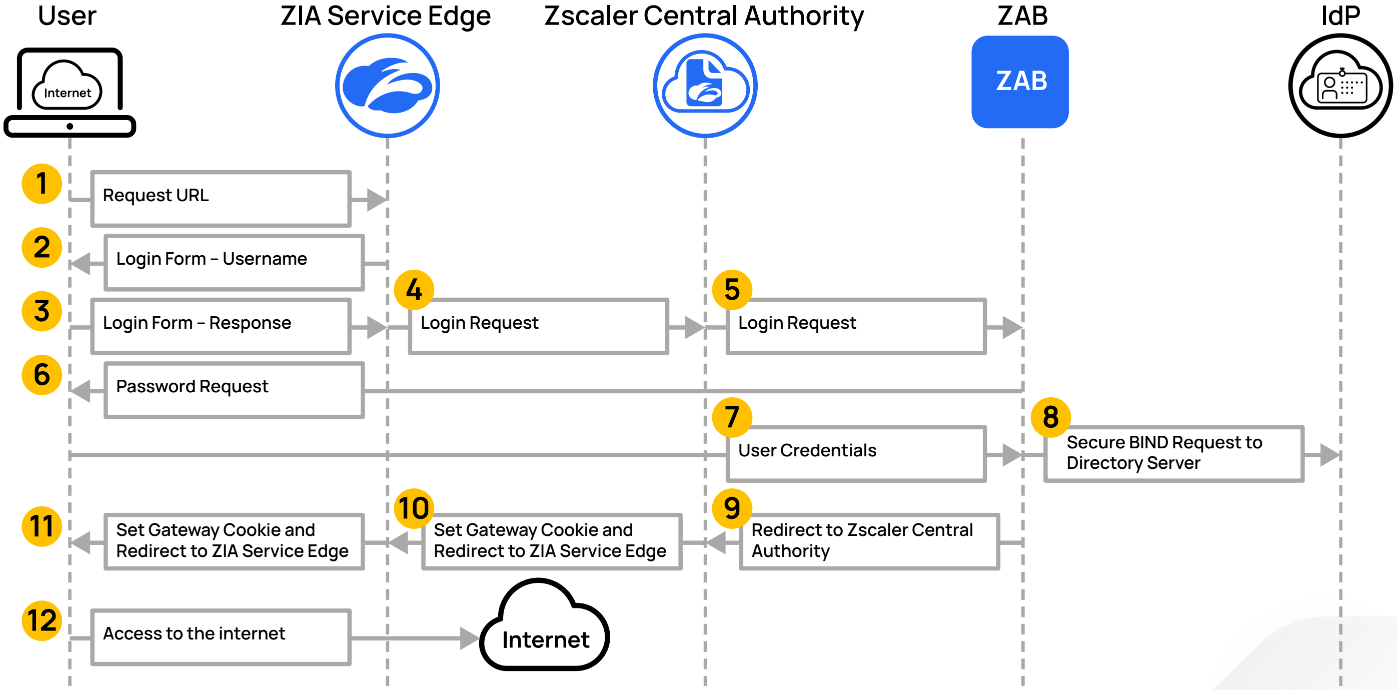
User
ZIA Service Edge
Zscaler Central Authority
ZAB
IdP
Internet
ZAB
1
Request URL
2
Login Form – Username
3
Login Form – Response
4
Login Request
5
Login Request
6
Password Request
7
User Credentials
8
Secure BIND Request to Directory Server
9
Redirect to Zscaler Central Authority
10
Set Gateway Cookie and Redirect to ZIA Service Edge
11
Set Gateway Cookie and Redirect to ZIA Service Edge
12
Access to the internet
Internet

Figure 12. Authentication using the ZAB

1. A user opens a browser and sends an HTTP request.
2. When the ZIA Public Service Edge receives an unauthenticated request, it displays the login form.
3. The user enters a login name.
4. The ZIA Public Service Edge sends the request to the Central Authority (CA).
5. The CA directs the request to the ZAB.
6. The ZAB requests the user's password.
7. The user enters the username and password.
8. The ZAB creates a TLS connection to the directory server and sends an LDAP BIND request with the username and password.
9. After the user is authenticated, the ZAB redirects the browser to the CA.
10. The CA sets the Zscaler gateway cookie and redirects the browser to the ZIA Public Service Edge.
11. The ZIA Public Service Edge sets the domain cookie on the browser and sends the HTTP request to the requested site.
12. The user can successfully browse the internet.

By using the ZAB, you eliminate the need to give the ZCA direct access to your directory server. To learn more, see About the Zscaler Authentication Bridge (https://help.zscaler.com/zia/about-zscaler-authentication-bridge).

Authenticating Users Using LDAP Directory Server Authentication

Direct authentication to your LDAP server is also available. This requires modification of your firewall to allow the ZCA to bind directly to your directory server.

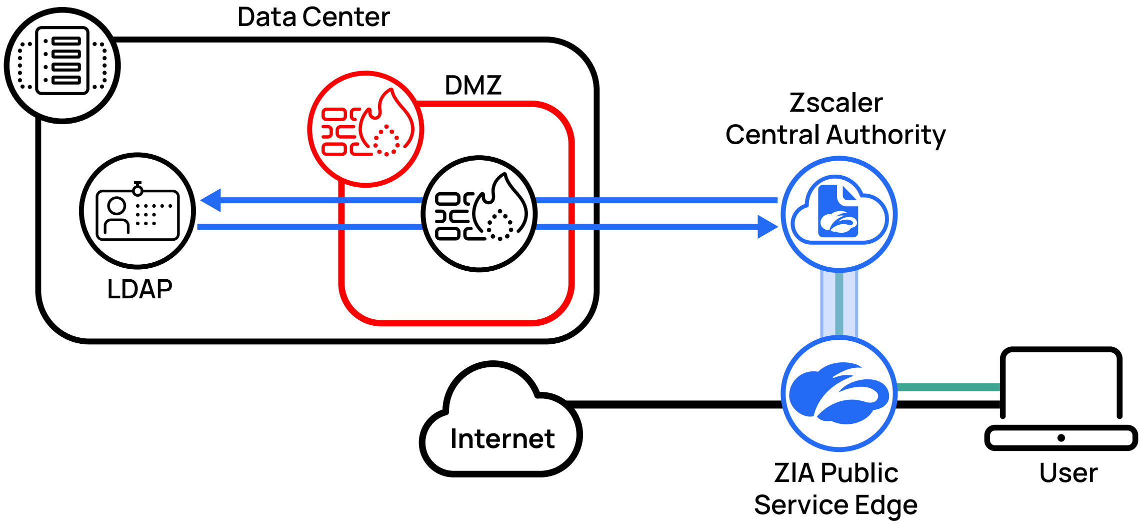

Figure 13. ZCA communicates directly with your LDAP server to authenticate users

In this use case, the ZCA first prompts the user for their username. When a matching synchronized user is found, a password request form appears. With both valid credentials, the ZCA sends an LDAP BIND request to authenticate the user. Unlike ZAB, there is no proxy between the ZCA and your directory server.

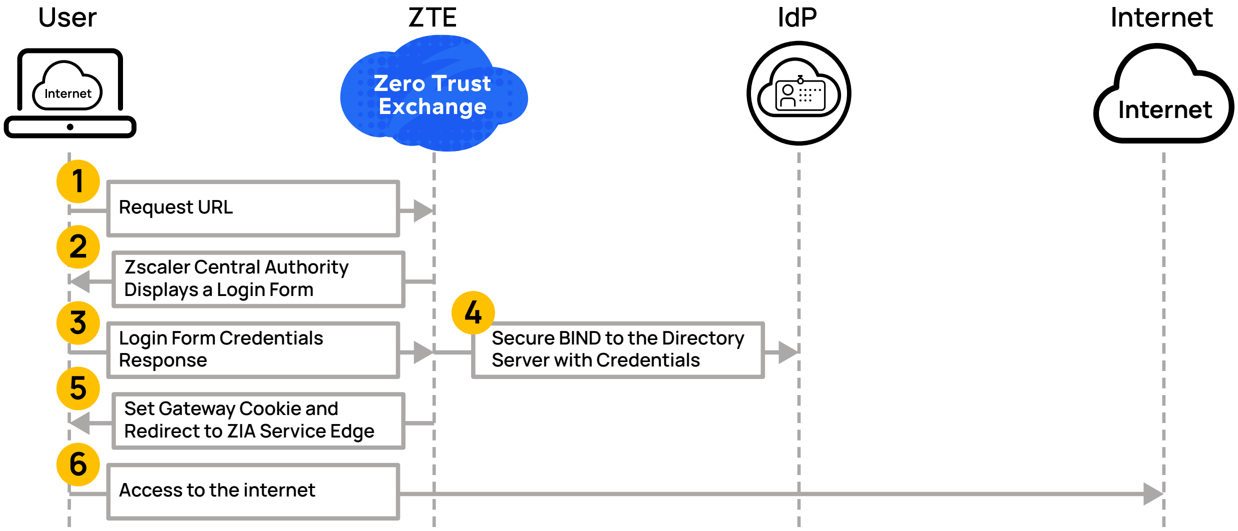
User
ZTE
IdP
Internet
Internet
Zero Trust Exchange
Internet
1
Request URL
2
Zscaler Central Authority Displays a Login Form
3
Login Form Credentials Response
4
Secure BIND to the Directory Server with Credentials
5
Set Gateway Cookie and Redirect to ZIA Service Edge
6
Access to the internet

Figure 14. Authentication with ZCA accessing the directory server

1. The user attempts to browse the internet without first being authenticated.
2. The ZCA prompts the user for their username and password.
3. The user provides their username and password.
4. The ZCA makes a secure LDAP bind request to your directory server using the provided username and password.
5. The user is authenticated, and cookies are set.
6. The user can browse the internet.

For more information, see About LDAP User Synchronization (https://help.zscaler.com/zia/about-ldap-user-synchronization).

Authentication from Known and Unknown Locations

With ZIA, you can specify your known locations. These are networks where traffic originates and is then forwarded via GRE or IPSec to ZIA. When the ZIA Service Edge receives traffic, it first checks to see if the traffic originated in a known location.

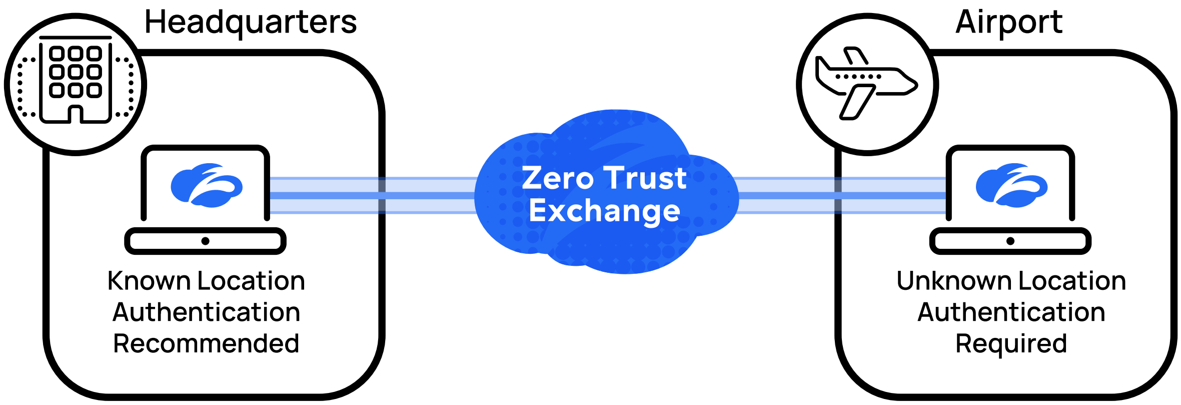
Headquarters
Known Location Authentication Recommended
Zero Trust Exchange
Airport
Unknown Location Authentication Required

Figure 15. Known locations can use location polices or user policies; unknown locations require authentication

When traffic reaches the ZIA Service Edge from a known location, you can force authentication for users, or allow them to use policies tied to the location. The decision to force authentication depends on your need for granular policy enforcement.

Zscaler recommends using surrogate IP for known locations. All traffic from your known locations will reach a ZIA Service Edge, even traffic from applications that cannot authenticate. Surrogate IP helps tie this traffic to the originating users. See Handling Traffic from Applications that Cannot Authenticate later in this guide.

Traffic from an unknown location, such as mobile users connecting via Zscaler Client Connector, must be authenticated. This allows Zscaler to identify that user as a member of your organization and apply the correct policy.

To learn more about ZIA locations, see About Locations (https://help.zscaler.com/zia/about-locations).

To learn more about surrogate IP, see About Surrogate IP (https://help.zscaler.com/zia/about-surrogate-ip).

To learn more about forwarding traffic to ZIA, see the Zscaler website (https://www.zscaler.com/resources/reference-architectures).

User Authentication Frequency

Most organizations require that users reauthenticate to the system on a regular basis. The frequency that they must authenticate is configurable. The default authentication interval is only once on the first connection, but the following authentication frequencies are available:

- Only Once – Default, users remain authenticated while their cookie is valid (typically 2 years).
- Daily – Users reauthenticate every 12–24 hours, depending on their time of login.
- Once per session – The user remains logged in until the browser is closed. When a new session begins, the user needs to reauthenticate again.
- Custom – You can choose a time from 1–180 days (inclusive) when the cookie expires, forcing reauthentication.

Choosing an authentication frequency should be driven by your organization's policy. If a laptop is stolen or a member of your organization is removed, they might still be authenticated. This is generally not a concern, as Zscaler does not grant privileged access to applications. Zscaler recommends setting the reauthentication interval to only once.

To learn more, see **About User Authentication Frequency** (**https://help.zscaler.com/zia/about-user-authentication-frequency**).

Handling Traffic from Applications that Cannot Authenticate

Some traffic and applications are not capable of authenticating to the Zscaler service. In these instances, there are a few options you can consider.

If your organization leverages Zscaler Private Access (ZPA) or Zscaler Digital Experience (ZDX) in addition to ZIA, your users can use Zscaler Client Connector for connectivity to these services. Zscaler Client Connector does not use cookies for authentication, and the applications can be tunneled across Zscaler Client Connector. Zscaler Client Connector is included as a part of your Zscaler subscription.

In the case where a user is at a trusted location, Zscaler recommends using the surrogate IP feature. Surrogate IP maps a user to their private IP address so that the user's policy can be applied to these traffic types. Zscaler recommends using surrogate IP whenever possible from your known locations.

NOTE
The use of surrogate IP requires that ZIA is able to see the private IP of the user. Your forwarding solution must not NAT the user's IP address.

Finally, when users are at a known location, you can choose to exempt URLs or cloud-based applications from authentication altogether. This should only be used when a user is at a known location and cannot use surrogate IP.

To learn more, see the following resources:

- **What Is Zscaler Client Connector?** (**https://help.zscaler.com/z-app/what-zscaler-app**)
- **About Surrogate IP** (**https://help.zscaler.com/zia/about-surrogate-ip**)
- **Exempting URLs and Cloud Apps from Authentication** (**https://help.zscaler.com/zia/exempting-urls-cloud-apps-authentication**)
- **Reference Architectures** (**https://www.zscaler.com/resources/reference-architectures**)

Summary

Authentication to Zscaler services provides you with the flexibility to differentiate access for users based on who they are, the device they are using, and their current location. Zscaler encourages you to authenticate all of your users to provide the best results in reporting and consistent access to resources.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.