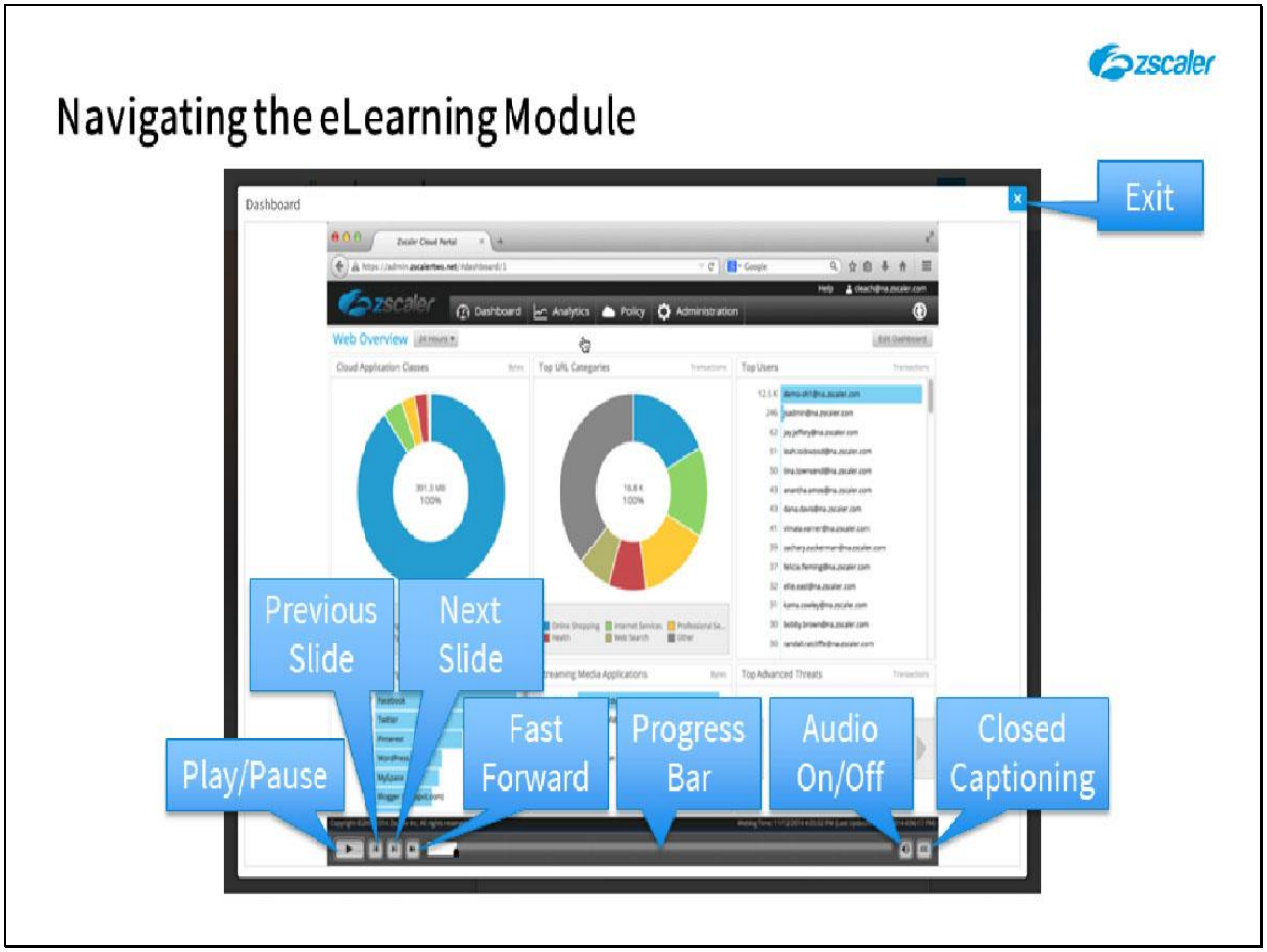
Slide 1 - Zscaler Policies

Slide notes

Welcome to the this Zscaler training module on integrating with Microsoft Office 365, and other Cloud application suites.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, next slide and fast forward. You can also mute the audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda

Slide notes

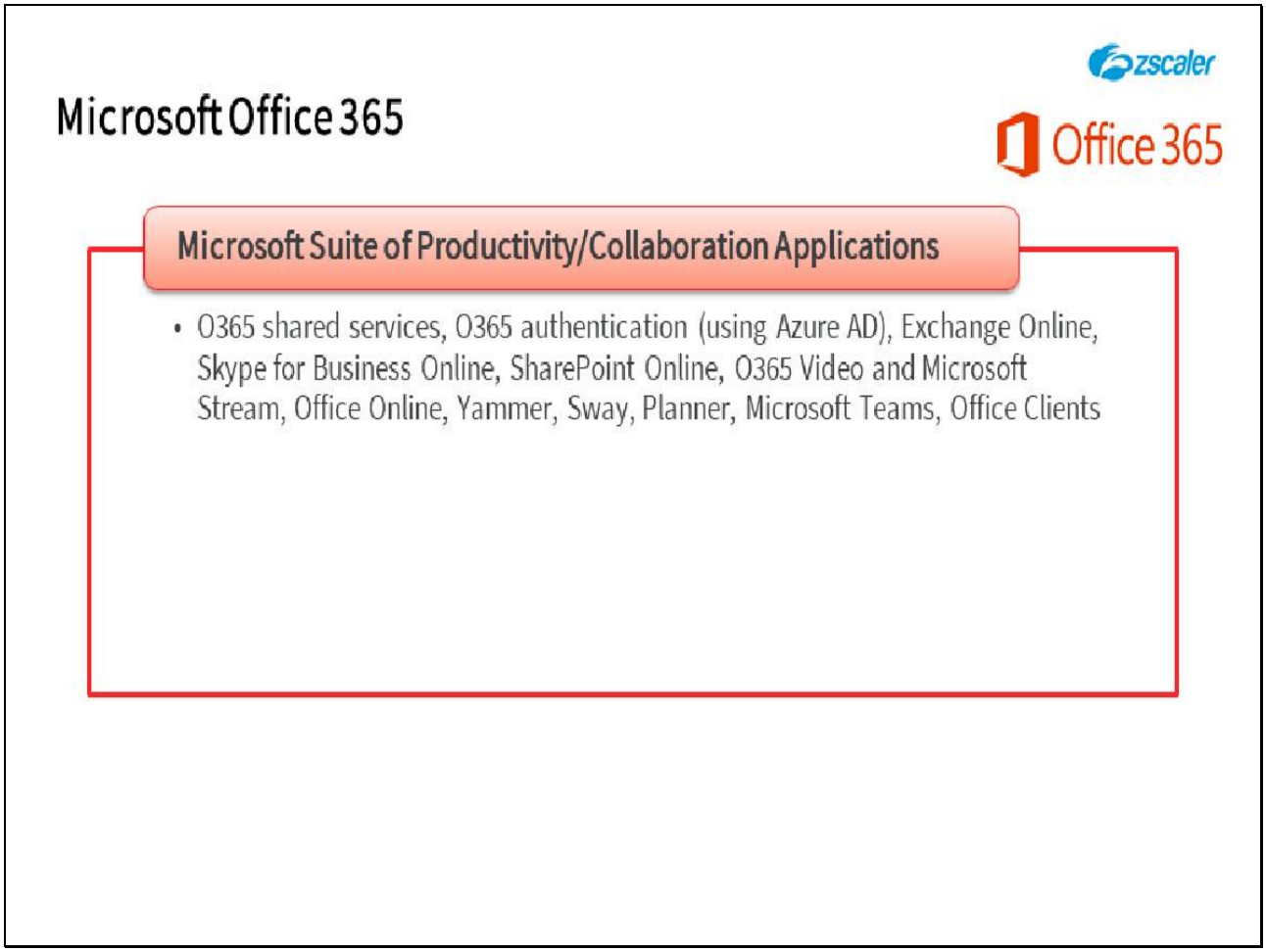
In this module, we will cover the Office 365 One Click integration capability, and the option to control access to certain Corporate application suites (Box, Google Apps, and Salesforce).

Slide 4 - Microsoft Office 365 One Click Policy

Slide notes

The first topic that we'll cover is the ability to create **One Click** policy for Microsoft Office 365 applications.

Slide 5 - Microsoft Office 365

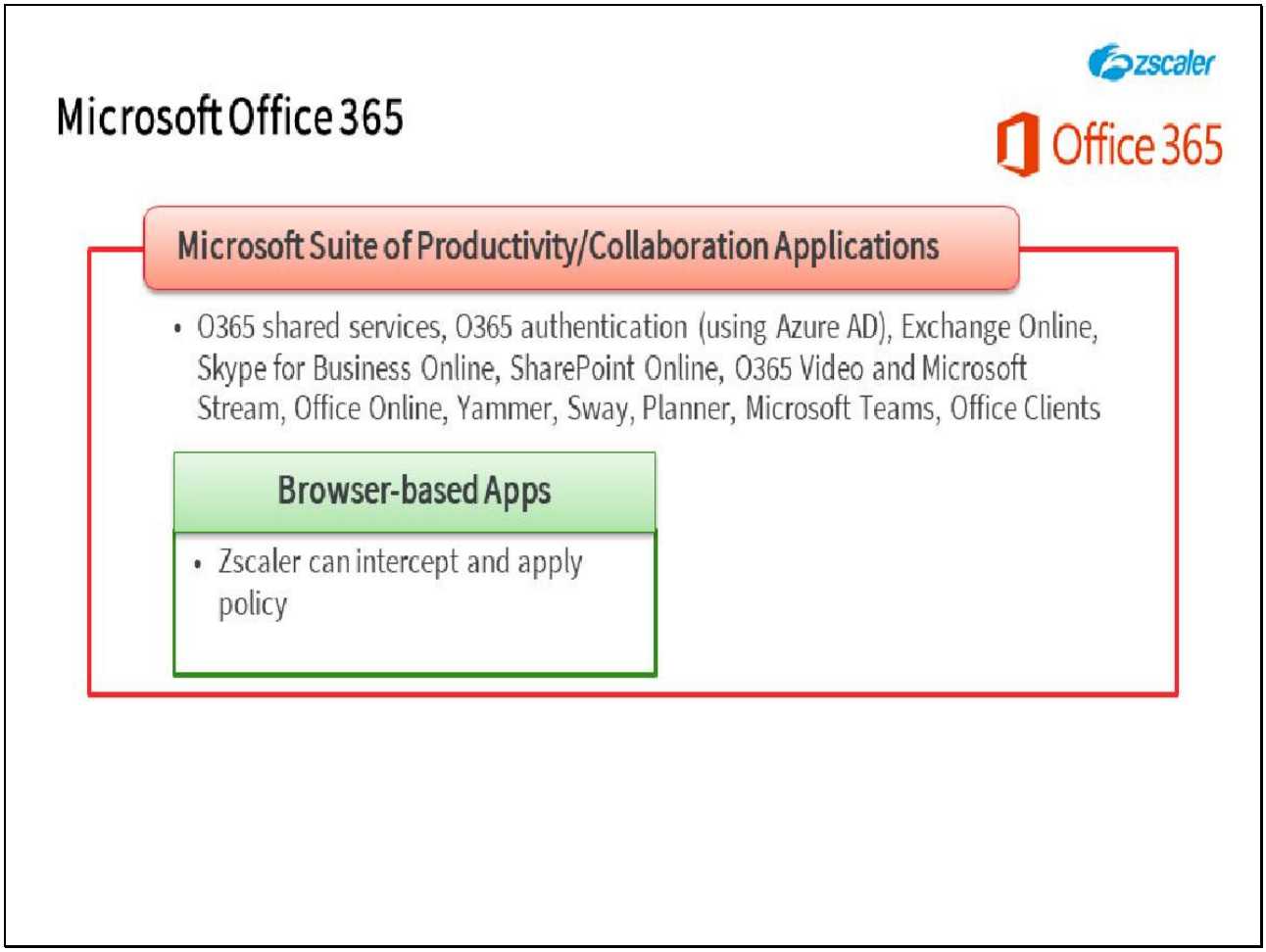


Slide notes

Office 365 is a suite of popular cloud-based productivity and collaboration applications from Microsoft, that you can purchase in various bundles. It includes:

- Optional directory services with Azure AD for authenticating Office 365 users.
- Email access to Exchange Online, either using Outlook, or Outlook Web Access.
- Collaboration applications such; as Skype for Business, Skype for Business Online Meeting, and Yammer.
- File sharing and workspace applications such as; SharePoint Online, OneDrive, and the Office Productivity Application.

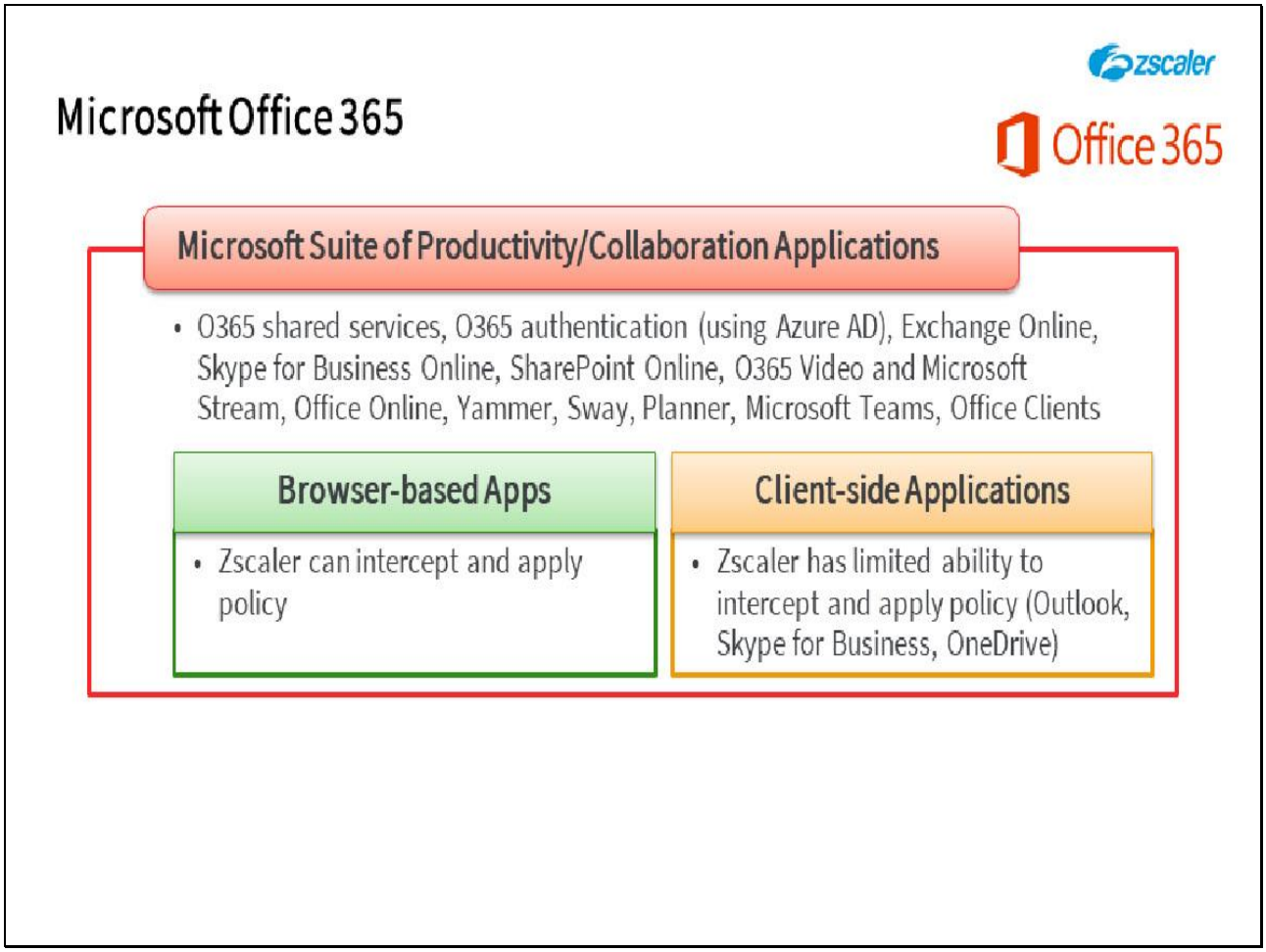
Slide 6 - Microsoft Office 365



Slide notes

When Office 365 applications are used within a Web Browser, most of the traffic can be handled by the Zscaler service, as long as authentication and SSL interception are enabled. This allows Zscaler to enforce corporate compliance policies for Office 365 traffic, such as; Security, DLP and Bandwidth Control policies.

Slide 7 - Microsoft Office 365

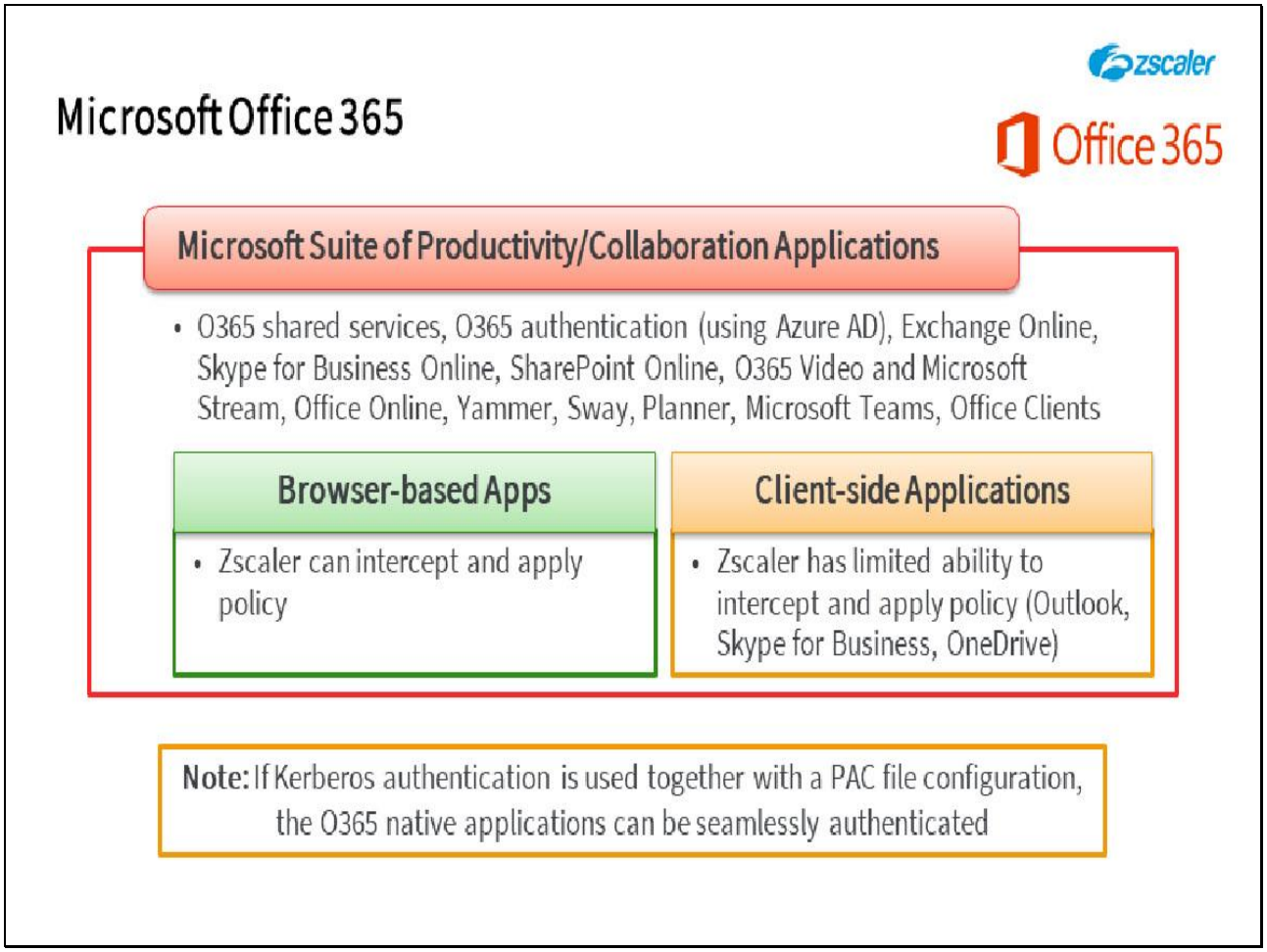


Slide notes

However, enterprises prefer to deploy native Office 365 applications such as Outlook, Skype for Business, and OneDrive, instead of using these applications within a Web browser. While these native applications provide a better user experience, they also present additional challenges from a security solutions viewpoint.

When the Zscaler outbound Firewall is also enabled, the Zscaler service can also handle non-Web ports and protocols to provide granular access control and visibility for all Office365 traffic.

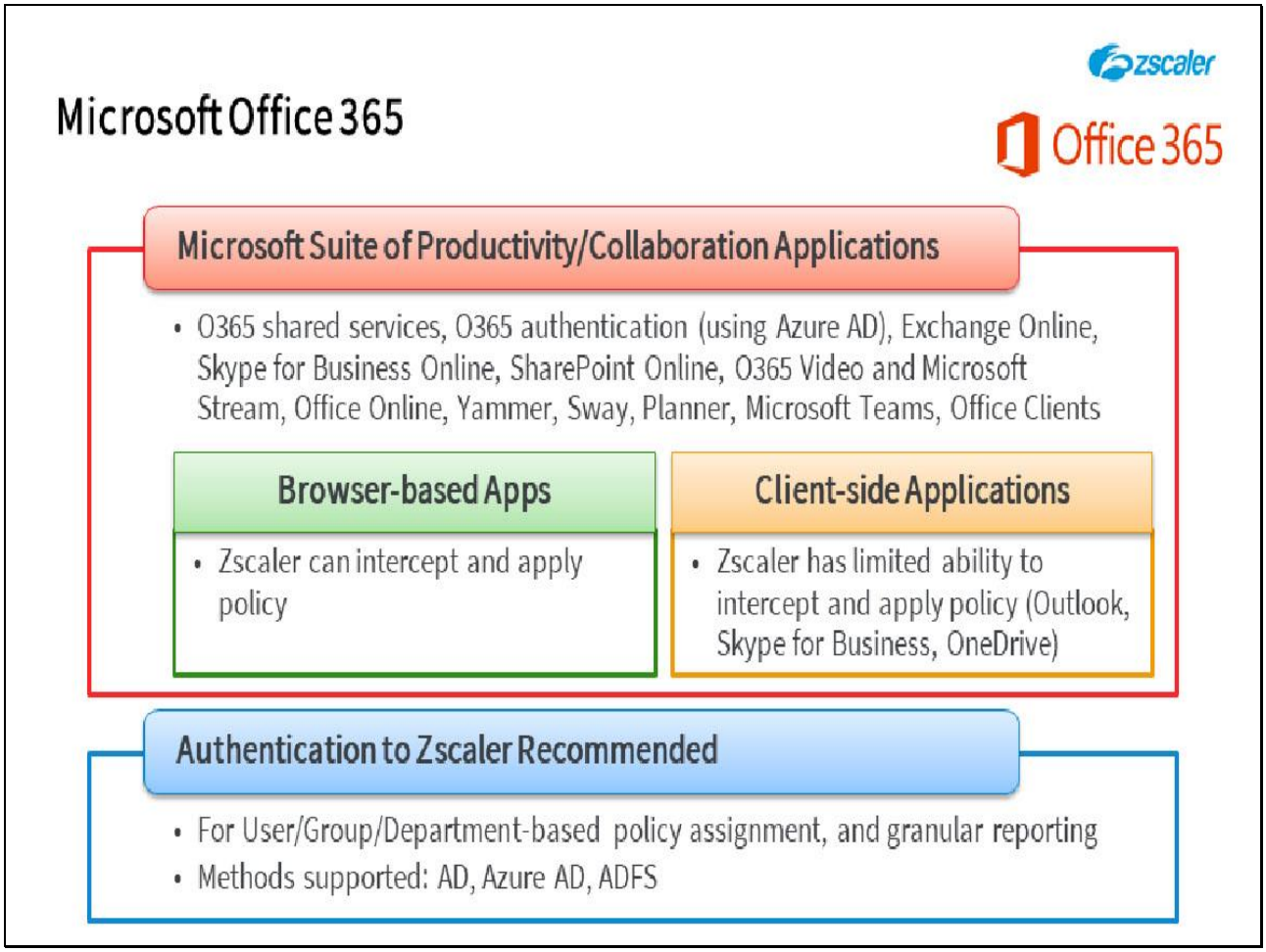
Slide 8 - Microsoft Office 365



Slide notes

Note that if you use Kerberos authentication, this allows the service to authenticate all Office 365 client-based traffic that is otherwise not compliant with Zscaler's default cookie-based authentication. But note that because Kerberos authentication cannot be used in transparent proxy mode, you must deploy PAC files as well.

Slide 9 - Microsoft Office 365



Slide notes

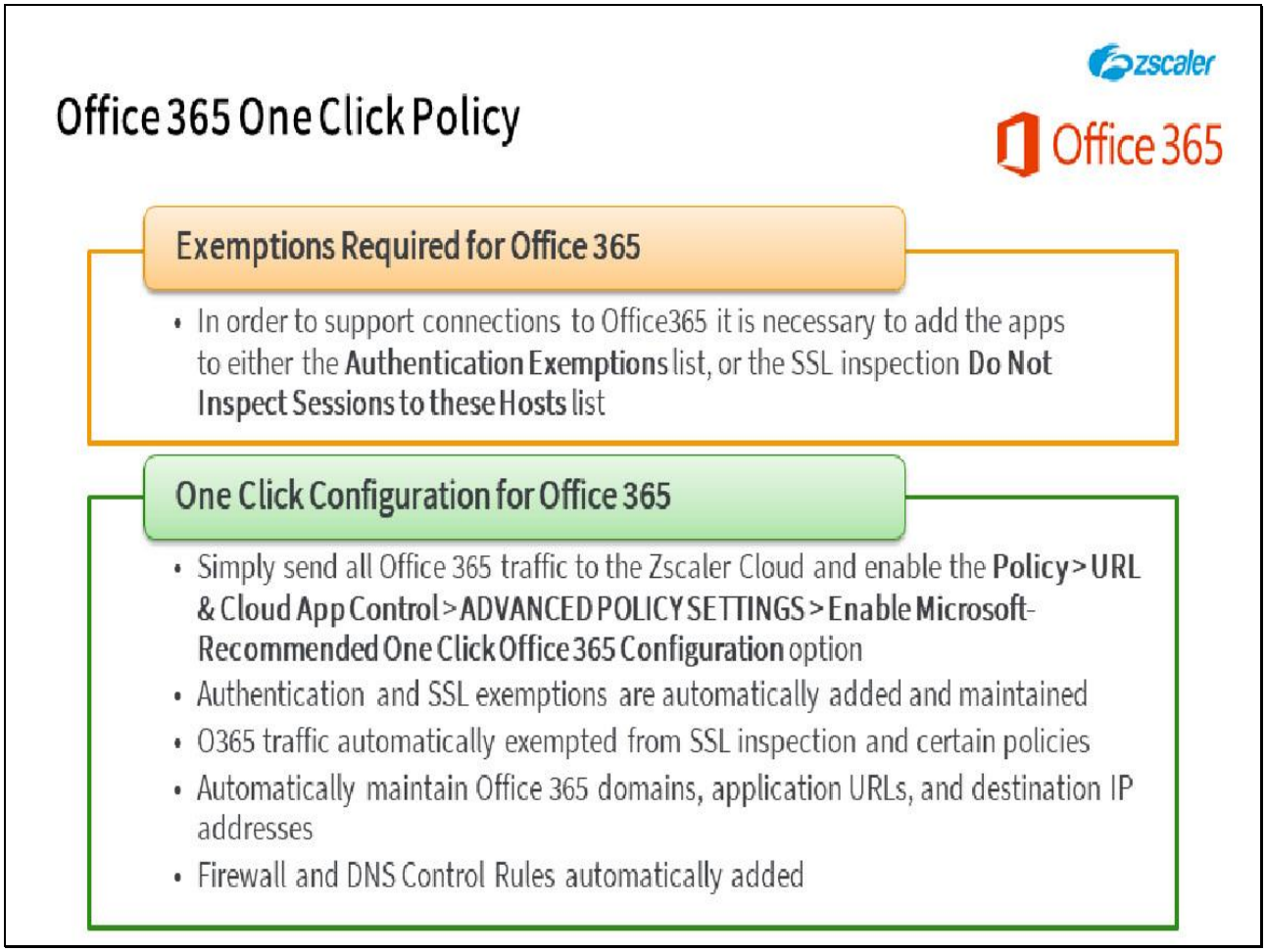
If you want to implement **Group** and **User** policies, and leverage the **User** and **Department** reporting capabilities of the Zscaler service, user authentication is required. For Office 365 users, Zscaler supports authentication using; Microsoft Active Directory, Azure Active Directory, and ADFS for SAML-based Single Sign-On.

Slide 10 - Office 365 One Click Policy

Slide notes

Zscaler does not support content inspection for non-HTTP/HTTPS traffic, so although we can intercept tunneled traffic, we cannot inspect the content (for example for the Outlook connections to Online Exchange server). As a result, we must add many Office 365 application URLs to the **Do Not Inspect Sessions to these Hosts** list, to disable SSL Inspection for them. In the past, these exceptions had to be configured manually.

Slide 11 - Office 365 One Click Policy



Slide notes

The Office 365 **One Click** option greatly simplifies the configuration of Zscaler to effectively support Office 365. It is enabled on the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab.

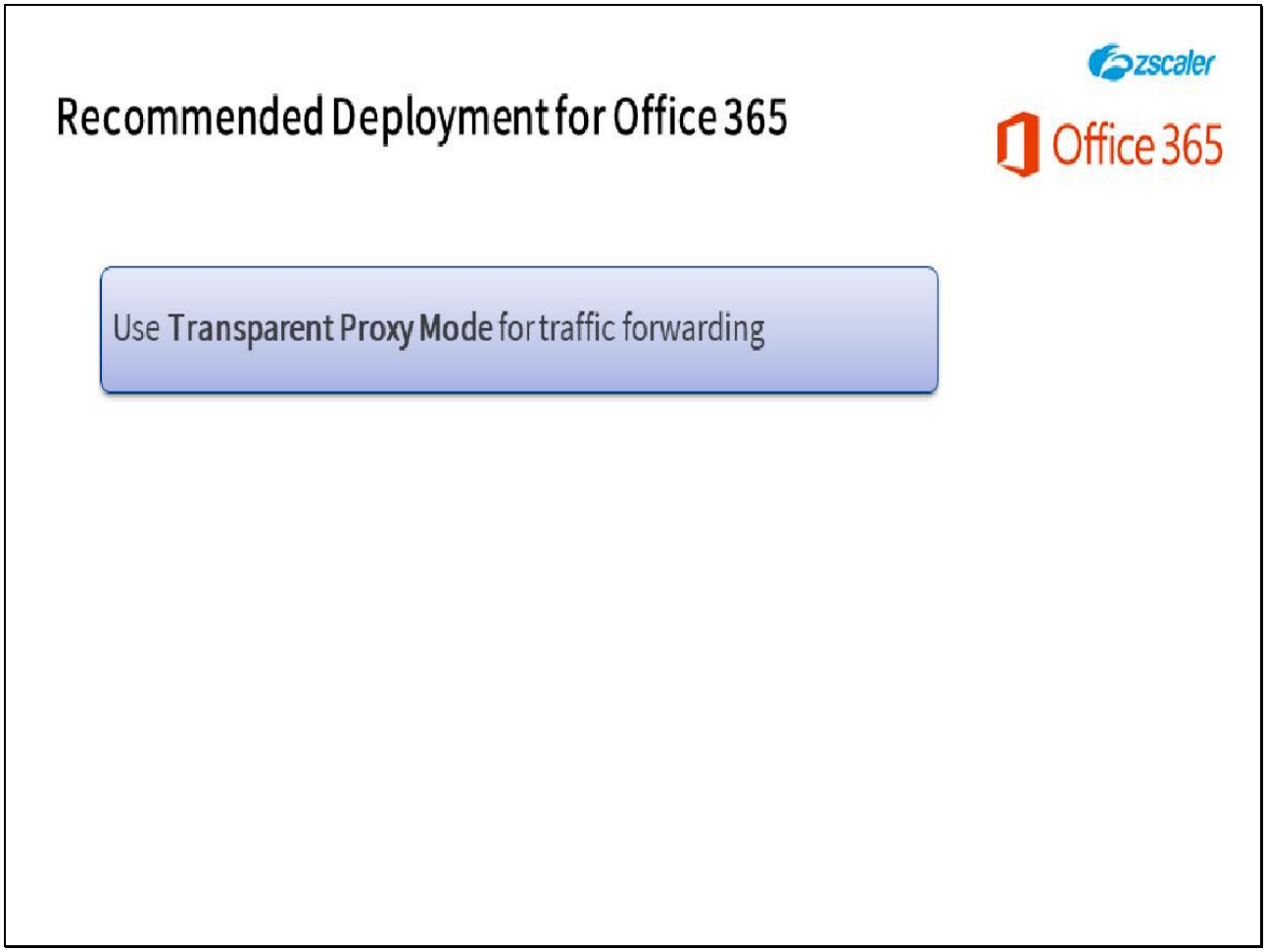
With the Office 365 One Click Configuration enabled, Zscaler automatically configures the **Do Not Inspect Sessions to these Hosts** list, and the **Authentication Exemptions** rules required for the service to seamlessly support and secure your Office 365 traffic. In addition:

- We automatically exempt the necessary URLs from SSL inspection, as well as exempting URLs from cookie-based authentication when necessary.
- We also exempt Office 365 traffic from certain policies, such as; **URL & Cloud App Control**, **Cloud Sandbox**, **Advanced Threat Protection**, and **Malware Protection**.
- Zscaler monitors the Office 365 destination IP addresses and URLs, fingerprints the apps, and adjusts the configurations accordingly, so you won't have to worry about any URL changes in the Office 365 applications.

- We also automatically add and manage a Firewall rule and a DNS Control rule for the Office 365 applications. We automatically apply a DNS override for O365 traffic received on transparent proxy connections (tunnels), to ensure that the user is re-directed to the closest Microsoft instance.

Using the One Click capability ensures the best possible user experience for your Office 365 users, as their connections will always be optimized no matter where they connect from.

Slide 12 - Recommended Deployment for Office 365

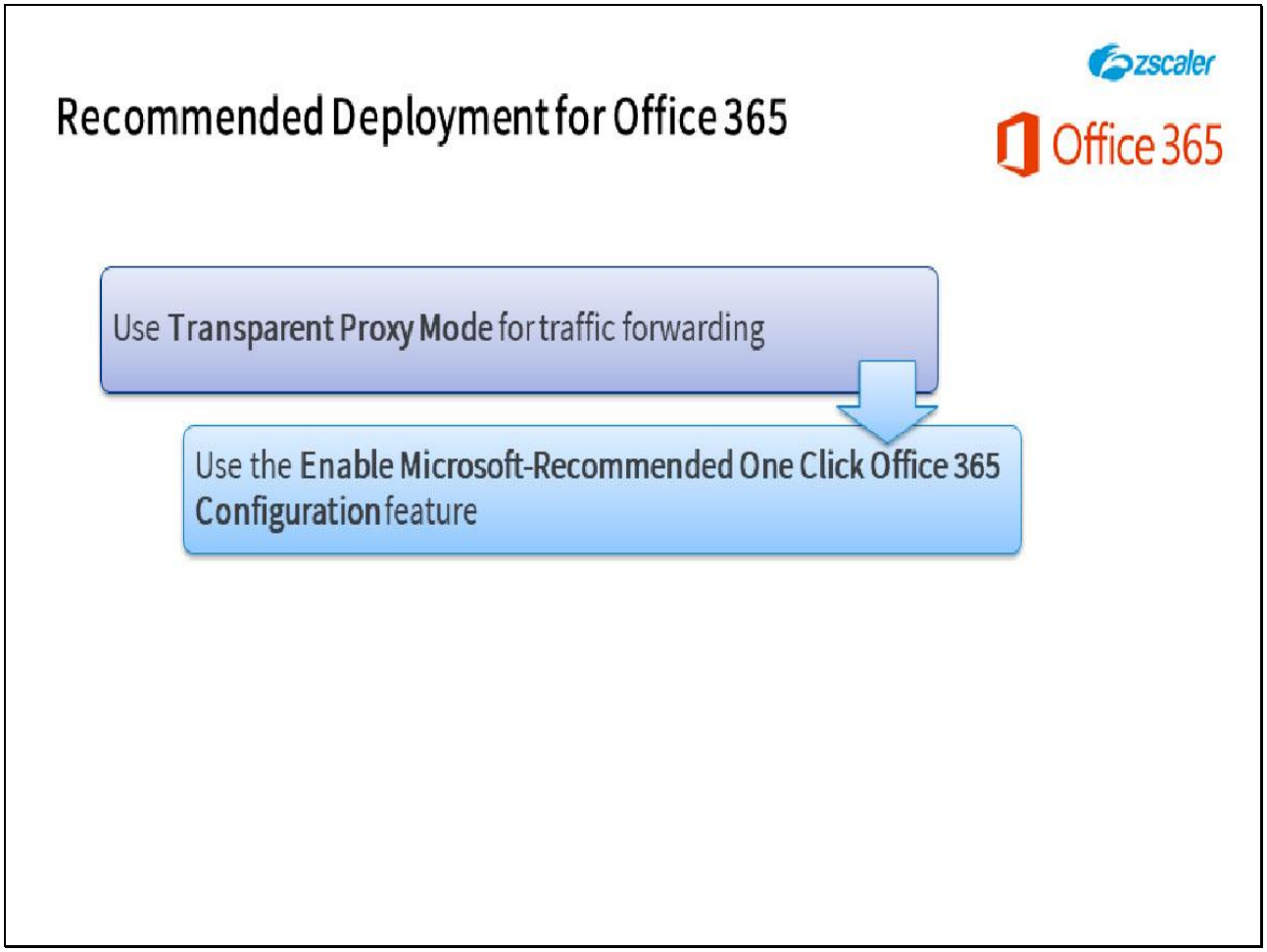


Slide notes

If you use any of the Office 365 applications, Zscaler recommends that you deploy the service as follows:

Firstly, use transparent proxy mode by forwarding traffic to the service through GRE or IPsec tunnels to ensure that all Office 365 traffic, including non-port 80/443 traffic, is sent to the Zscaler service.

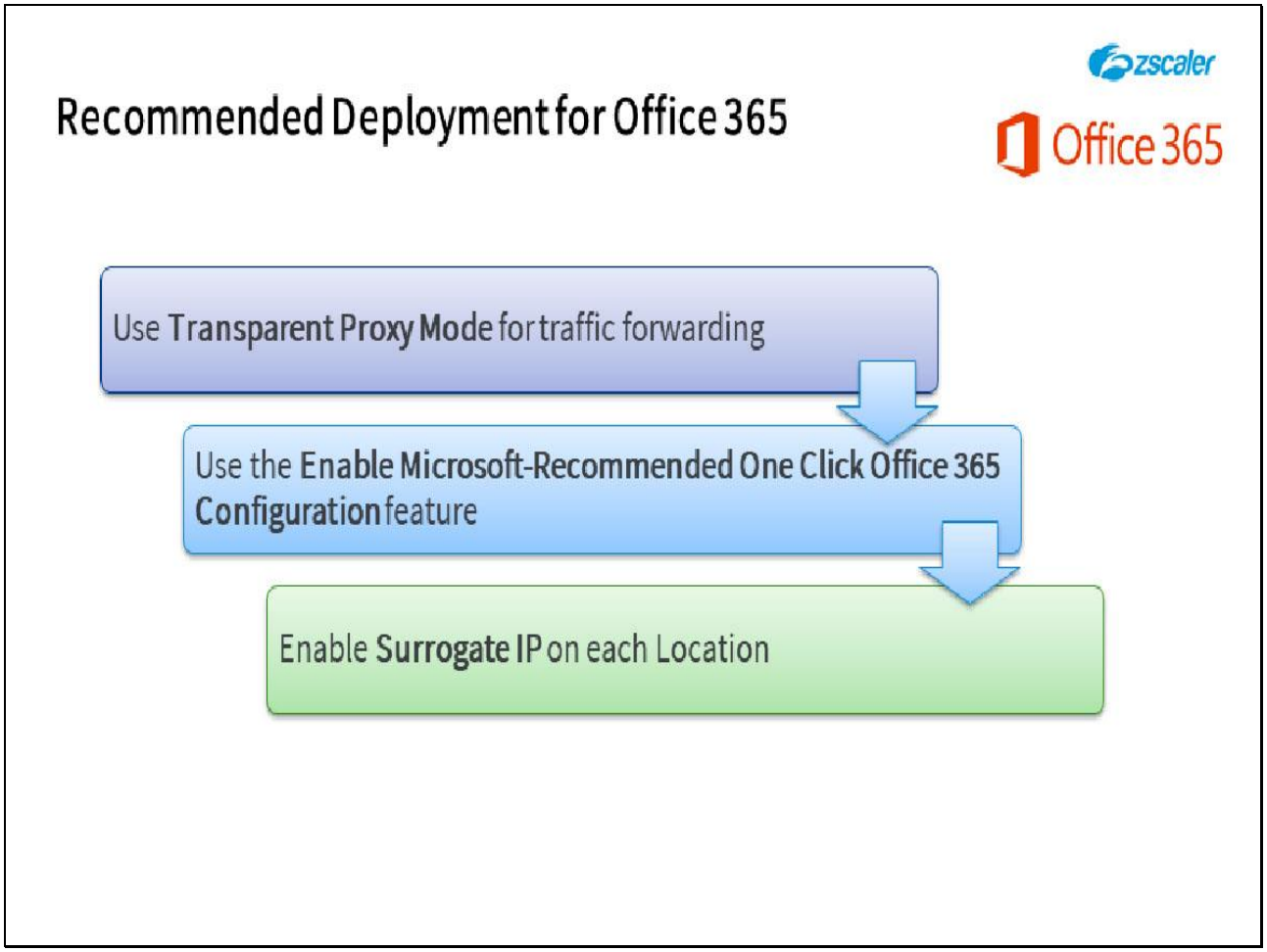
Slide 13 - Recommended Deployment for Office 365



Slide notes

Be sure to use the **Enable Microsoft-Recommended One Click Office 365 Configuration** feature, which allows Zscaler to automatically configure additional SSL and authentication bypass rules. We also fingerprint more than 300 applications, including Office 365 applications, so you do not have to worry about any URL changes within the Office 365 suite.

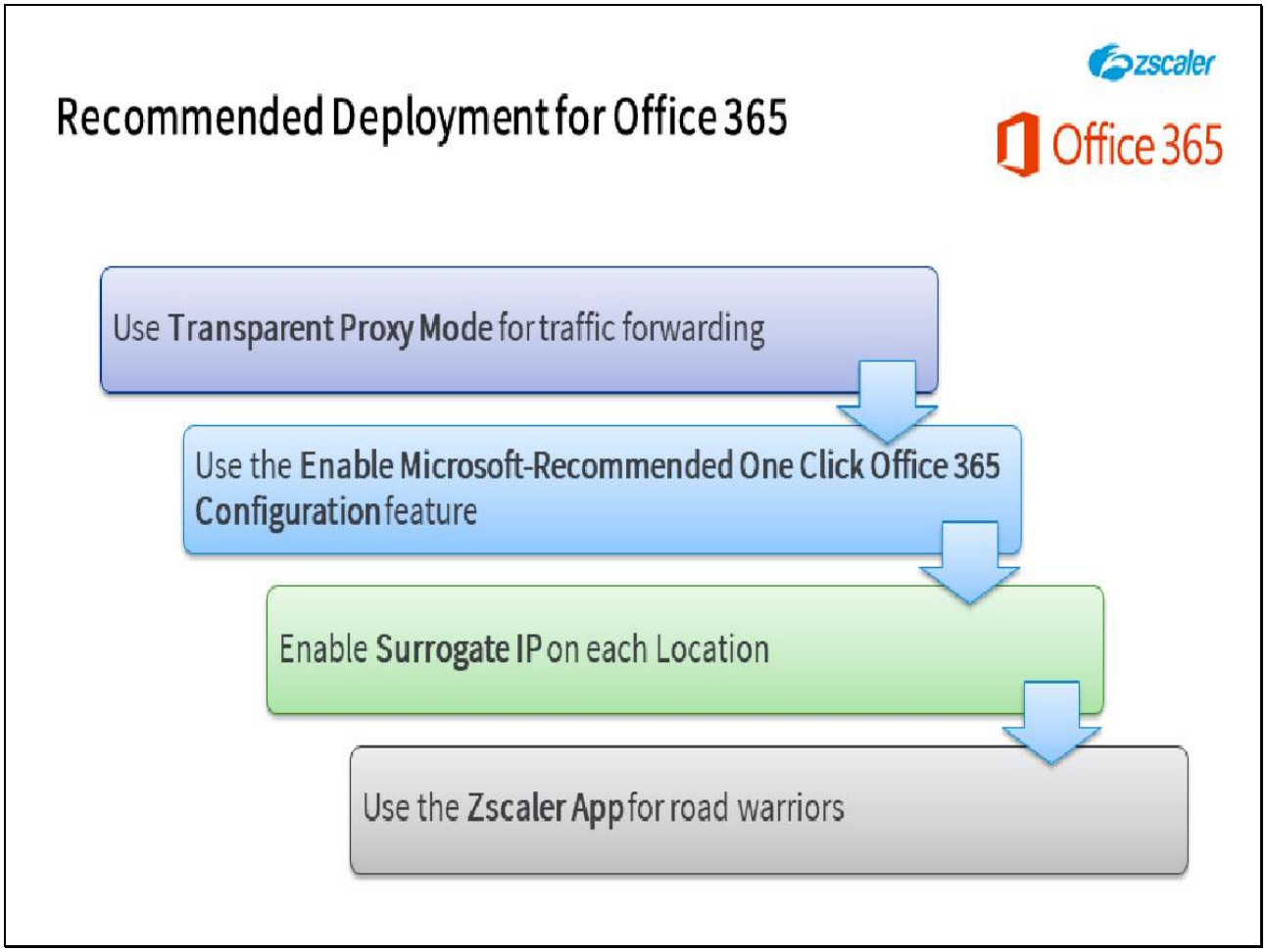
Slide 14 - Recommended Deployment for Office 365



Slide notes

Next, also enable **Surrogate IP**, which allows us to map unauthenticated Office 365 traffic to a user's internal IP address within the organization. Using the **Surrogate IP** feature also enables authentication for the Zscaler outbound firewall, so that non-HTTP/HTTPS traffic is authenticated and mapped to users, as well as the Office 365 client-based Web traffic.

Slide 15 - Recommended Deployment for Office 365

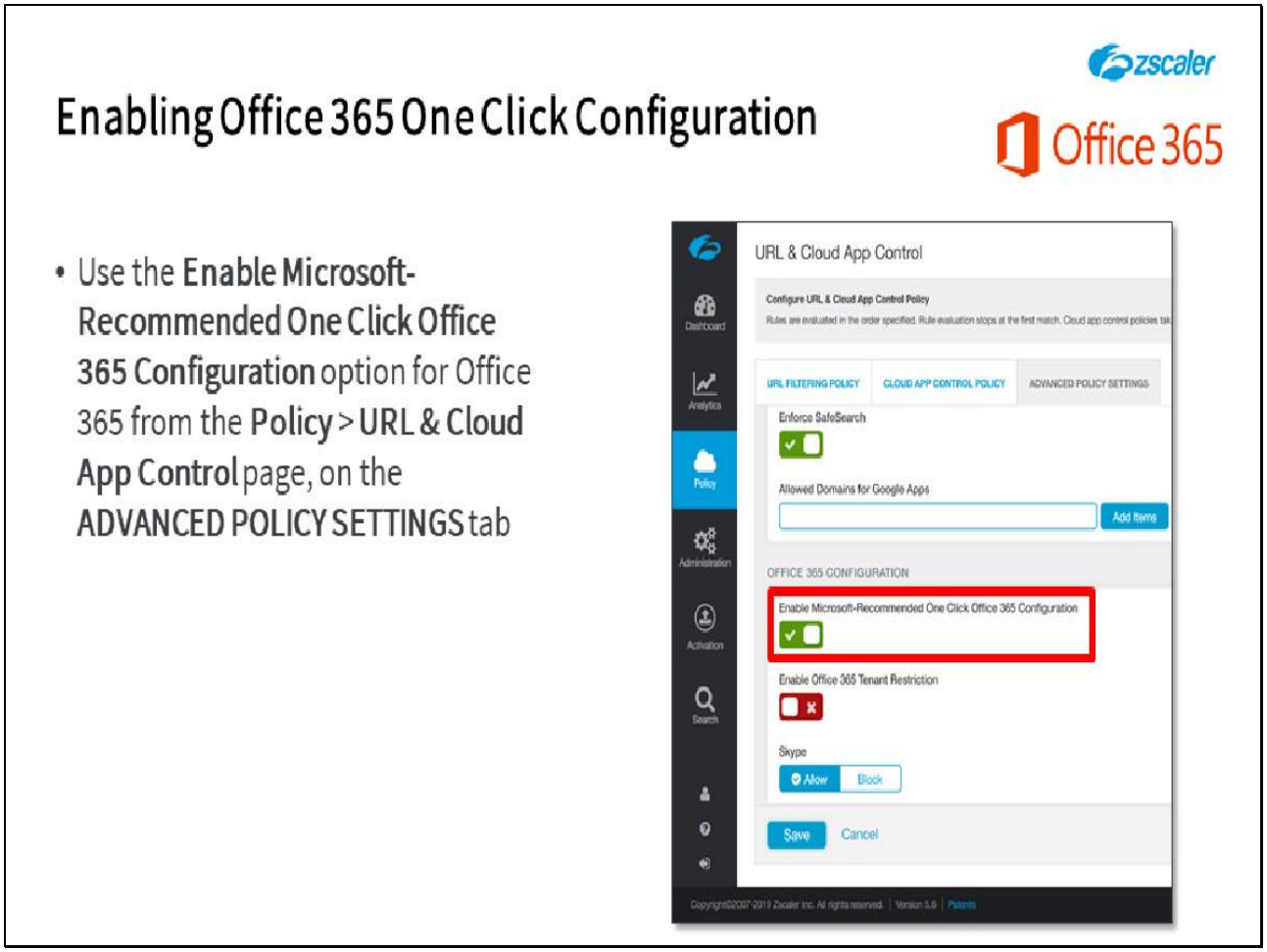


Slide notes

Finally, use the Zscaler App for your road warriors. The Zscaler App does not use cookies for user authentication, so there is no need to bypass security controls for roaming users. The App also provides proxy enforcement even when users have admin privileges for their computers.

It simplifies configuration because if the App is installed, then the use of a dedicated port, Kerberos authentication, or Surrogate IP are no longer requirements for your road warriors. In addition, because the Zscaler App supports both Browser and non-Browser traffic, it solves proxy-interoperability issues with Outlook and Skype for Business.

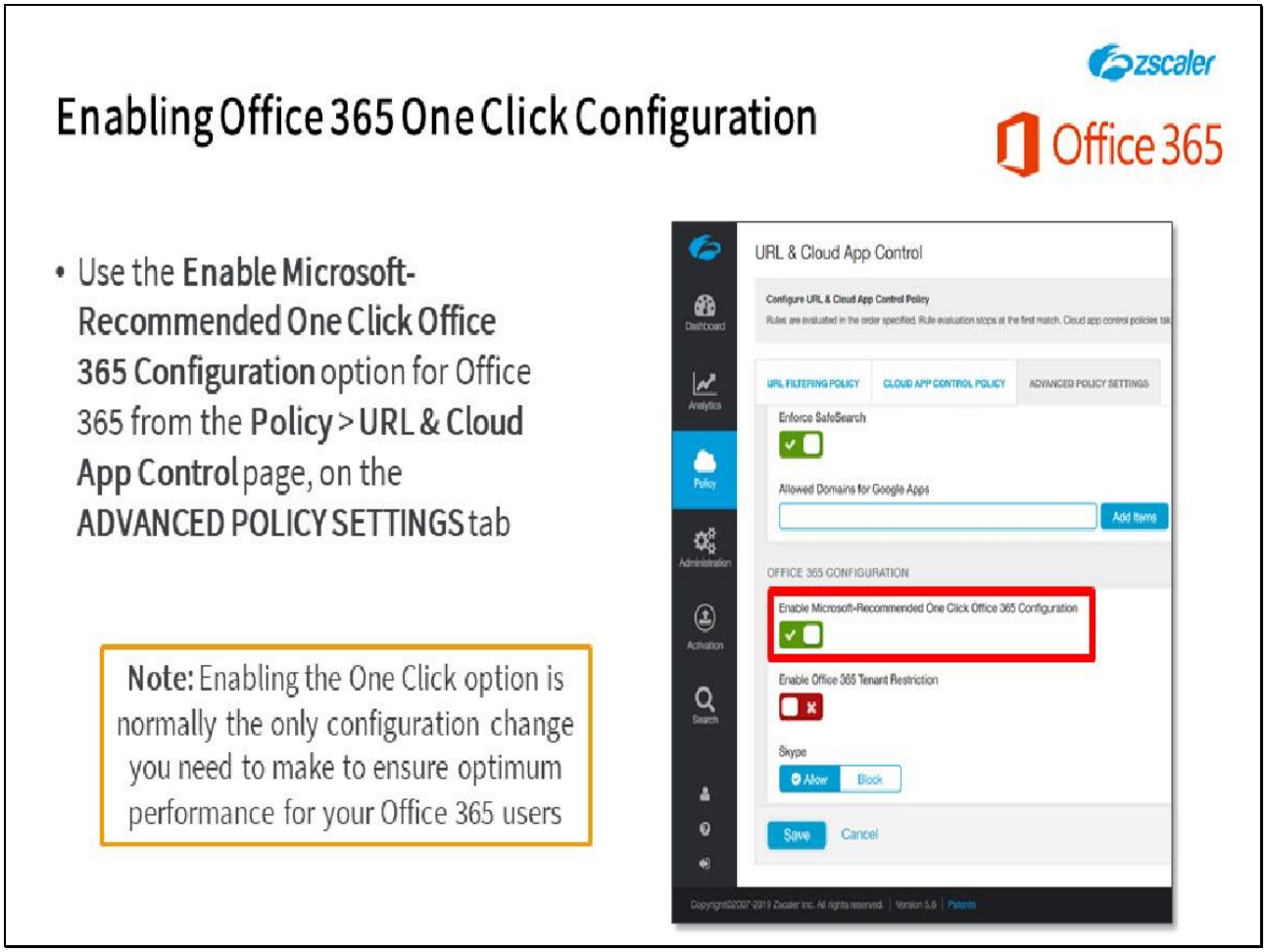
Slide 16 - Enabling Office 365 One Click Configuration



Slide notes

To enable the Office 365 One Click configuration, navigate to the **Policy > URL & Cloud App Control** page, then go to the **ADVANCED POLICY SETTINGS** tab. Select the **Enable Microsoft-Recommended One Click Office 365 Configuration** option, then save and activate your changes.

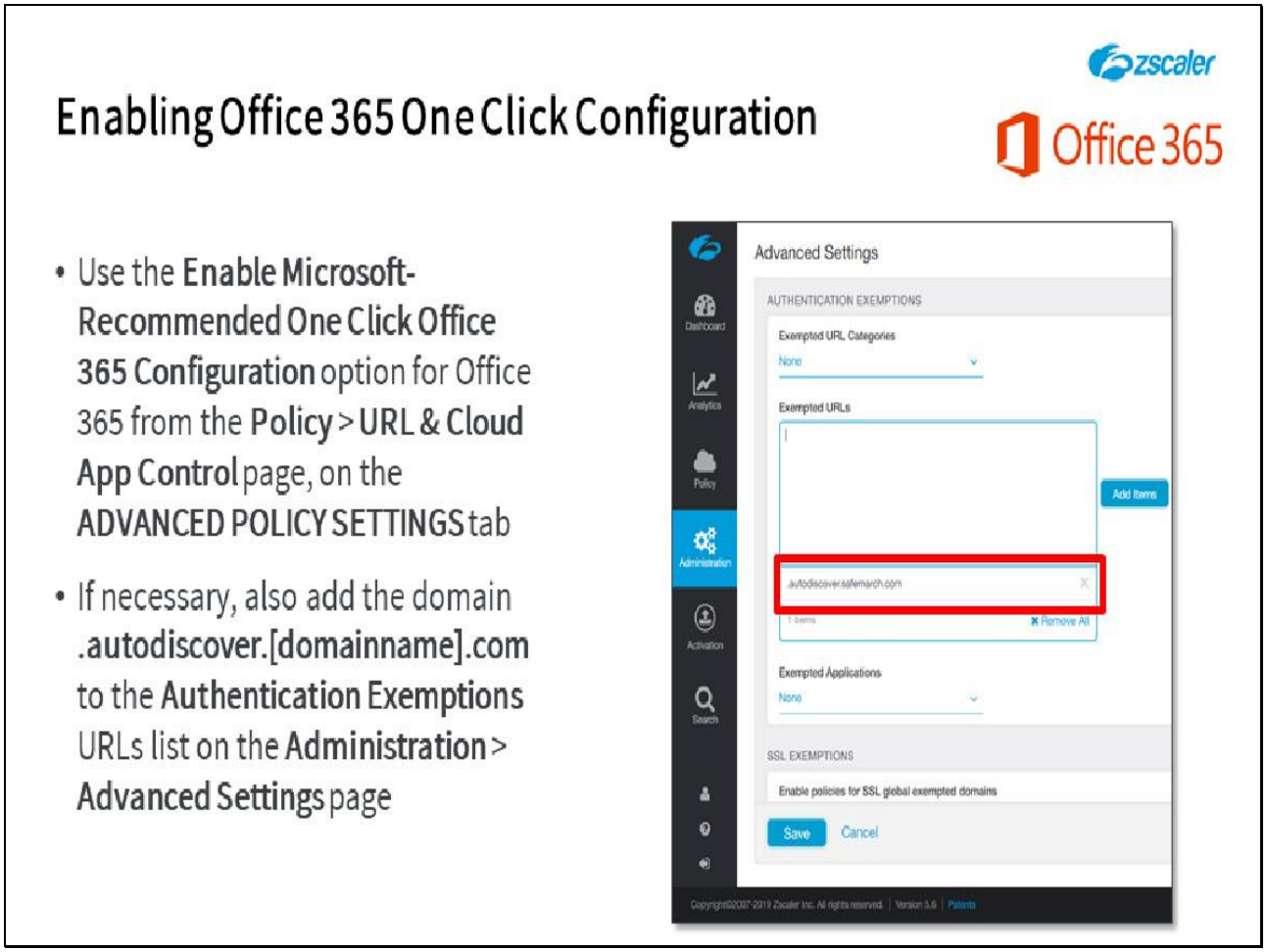
Slide 17 - Enabling Office 365 One Click Configuration



Slide notes

Note that enabling the **One Click** option is normally the only configuration change you need to make to ensure optimum performance for your Office 365 users!

Slide 18 - Enabling Office 365 One Click Configuration

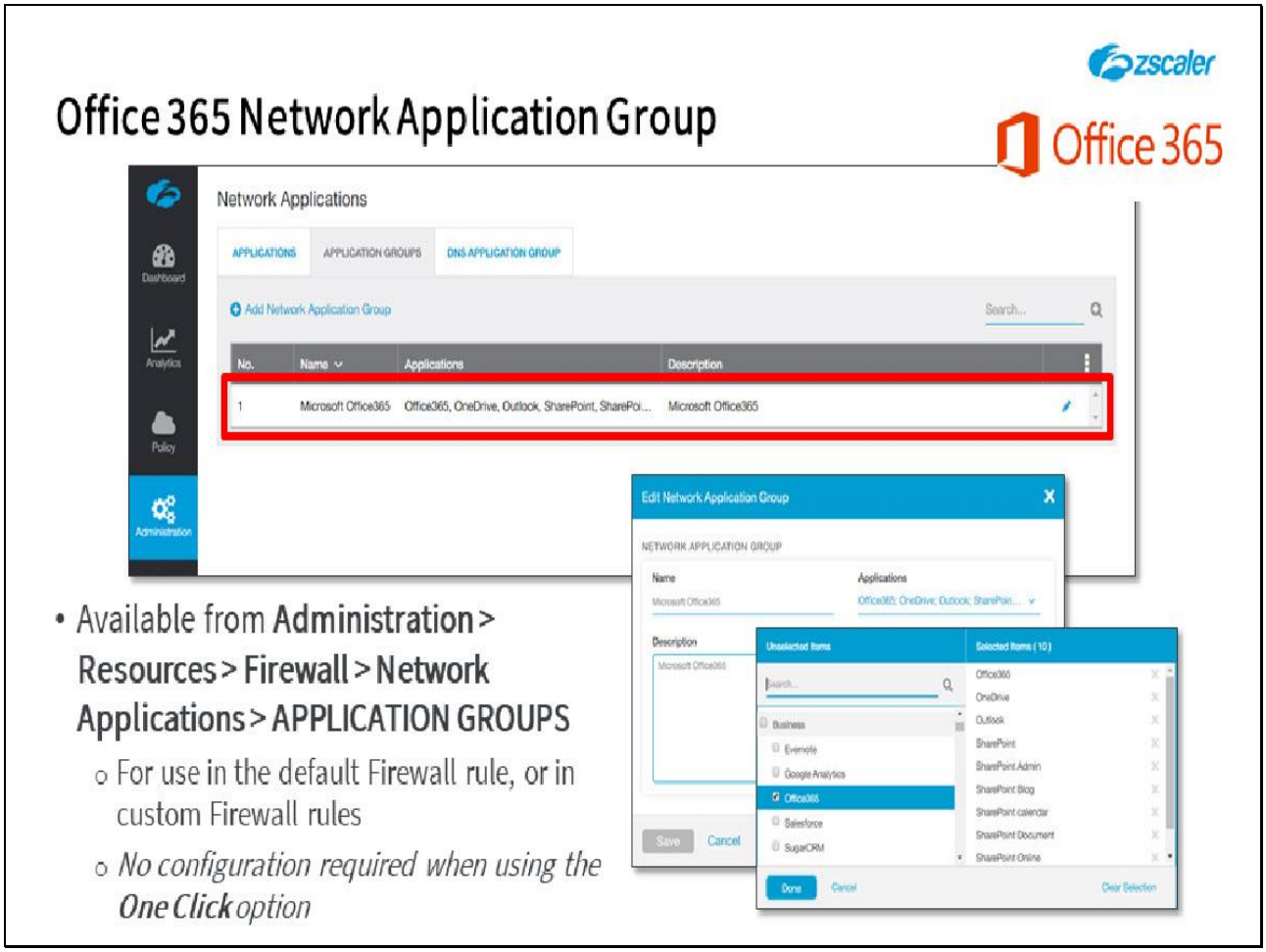


Slide notes

One item that Zscaler cannot configure automatically when the Office 365 **One Click** feature is enabled, is your custom Domain auto-discovery URL in the authentication exemption list. Depending on your business requirements, you may need to manually add the URL: **.autodiscover.[domainname].com** to the **Exempted URLs** list on the **Administration > Advanced Settings** page.

This URL is used by clients for discovering an EWS node associated with the company domain, the **domainname** parameter will of course vary from company to company. This exemption is not required if you use the EWS managed API to do auto-discovery.

Slide 19 - Office 365 Network Application Group

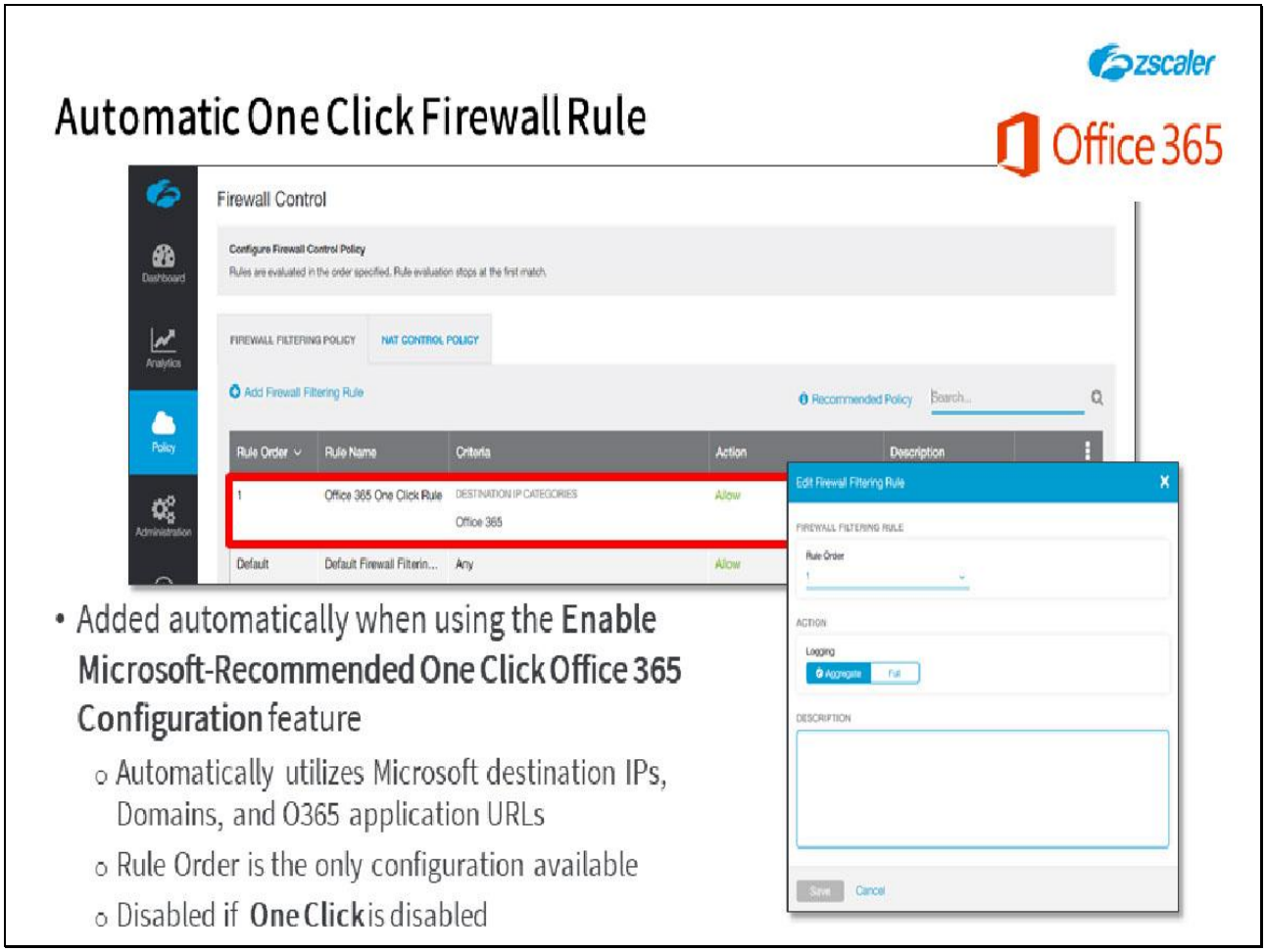


Slide notes

We also maintain a list of Office 365 applications in an **Application Group** that is used in the default Firewall rule when the **One Click** setting is enabled. Again, there is nothing here that you normally need to configure, although this group is available for you to use in any custom Firewall rules that you choose to add.

This group is maintained by us to ensure that the Microsoft destination IPs, Domains, and O365 application URLs are always up-to-date.

Slide 20 - Automatic One Click Firewall Rule

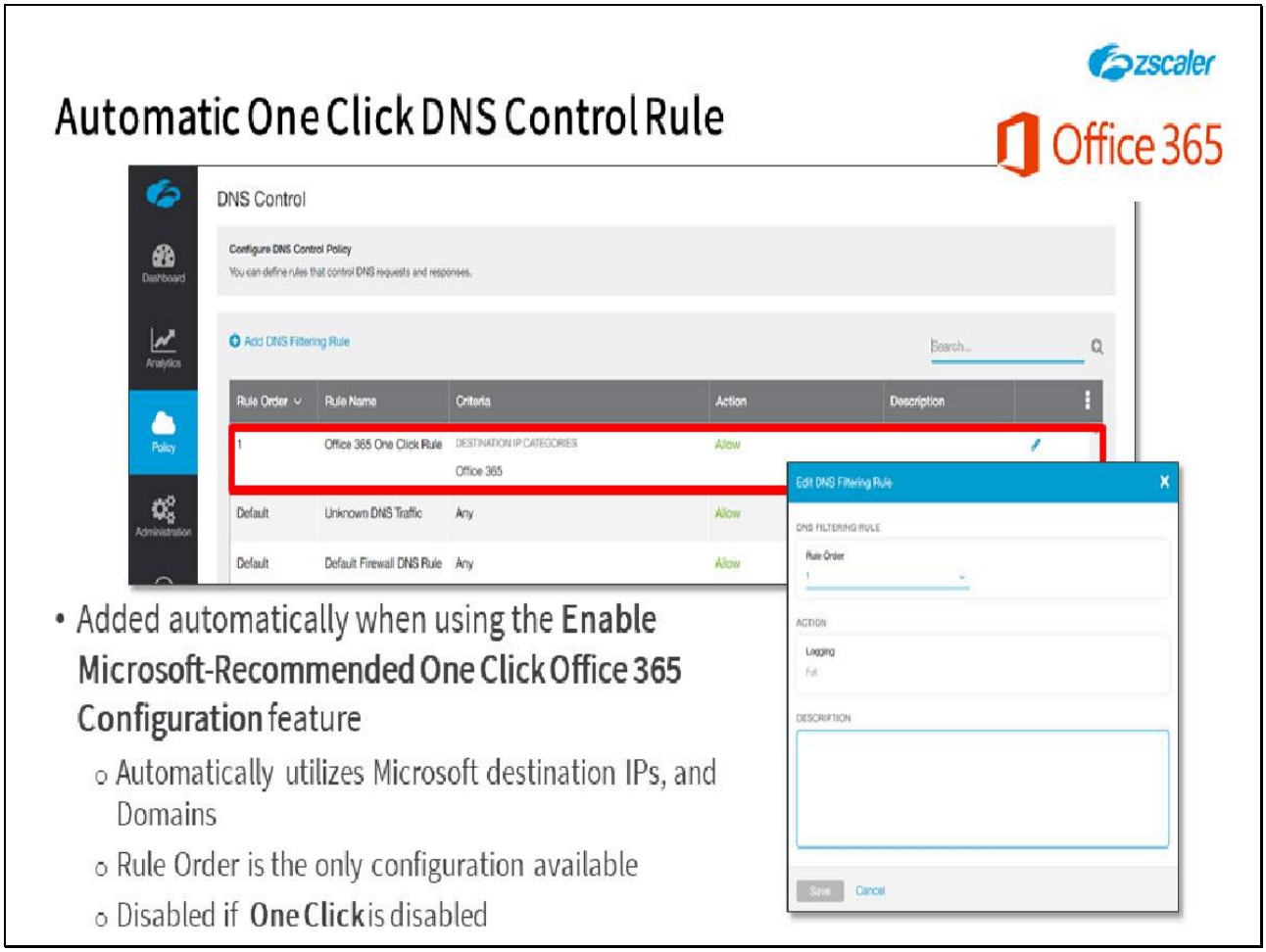


Slide notes

When the Microsoft Office **One Click** setting is enabled, we automatically add a Firewall rule that targets and allows the **Application Group** mentioned in the previous slide. It is added at rule 1 and is not configurable, nor can you delete it, although the rule order can be changed if necessary. As we are responsible for maintaining that **Application Group** up-to-date, this should always ensure that the Office 365 application set is always allowed at the Firewall.

Note that if the Office 365 **One Click** setting is subsequently disabled, this rule will be set to the **Disabled** state, but will still appear in the Firewall rules list.

Slide 21 - Automatic One Click DNS Control Rule

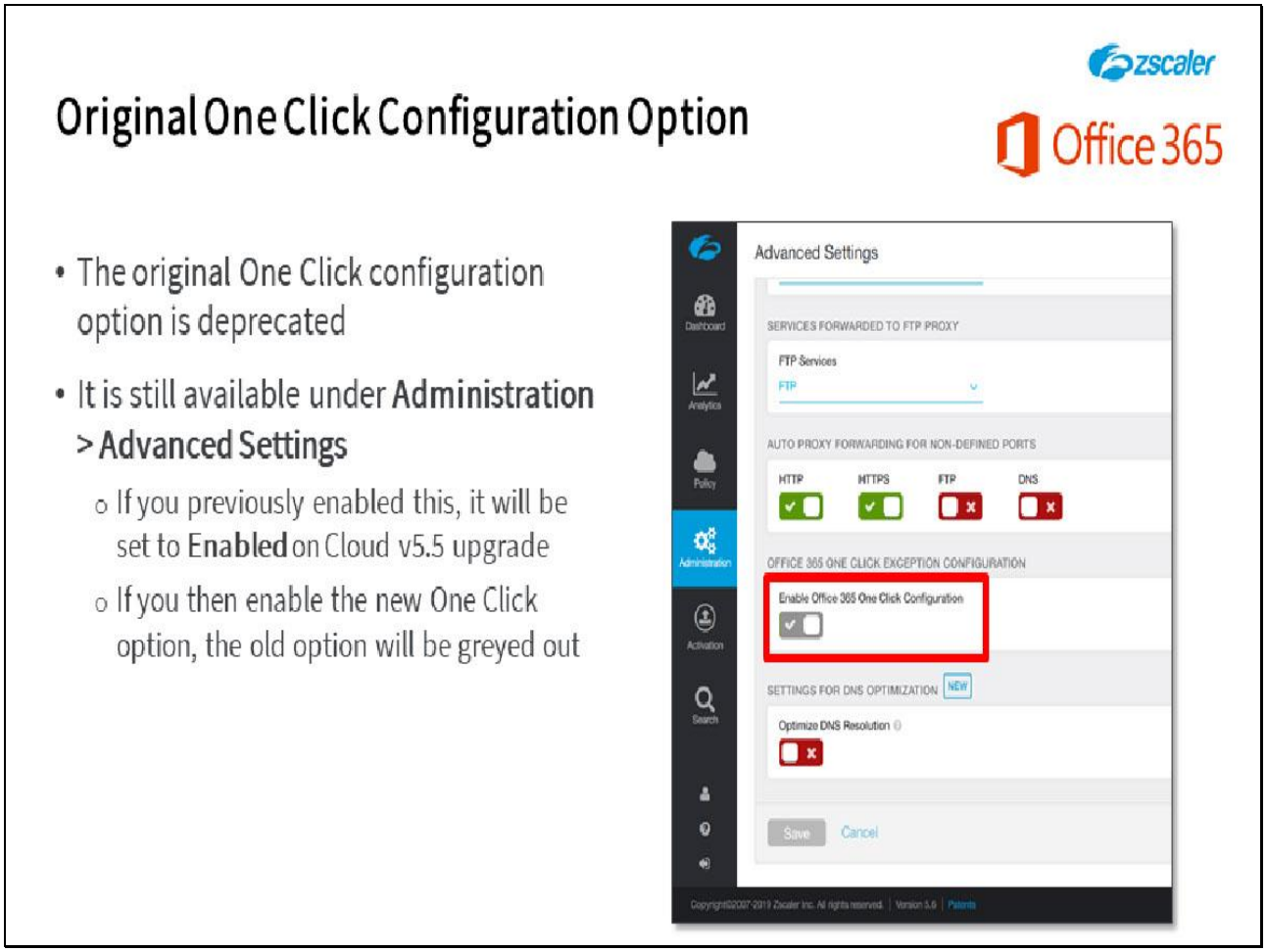


Slide notes

In addition, we also automatically add a DNS Control rule for Office 365 that automatically uses the Microsoft destination IP addresses and Domains that we maintain. As with the Firewall rule, this rule is added at position 1, it is not configurable and cannot be deleted, although the rule order can be changed. We automatically apply a DNS override for O365 traffic received on transparent proxy connections (tunnels), to optimize the data path for users and ensure that they connect to the closest Microsoft application instance.

Also, as with the Firewall rule, if the Office 365 **One Click** setting is subsequently disabled, this rule will be set to the **Disabled** state, but will still appear in the DNS Control rules list.

Slide 22 - Original One Click Configuration Option

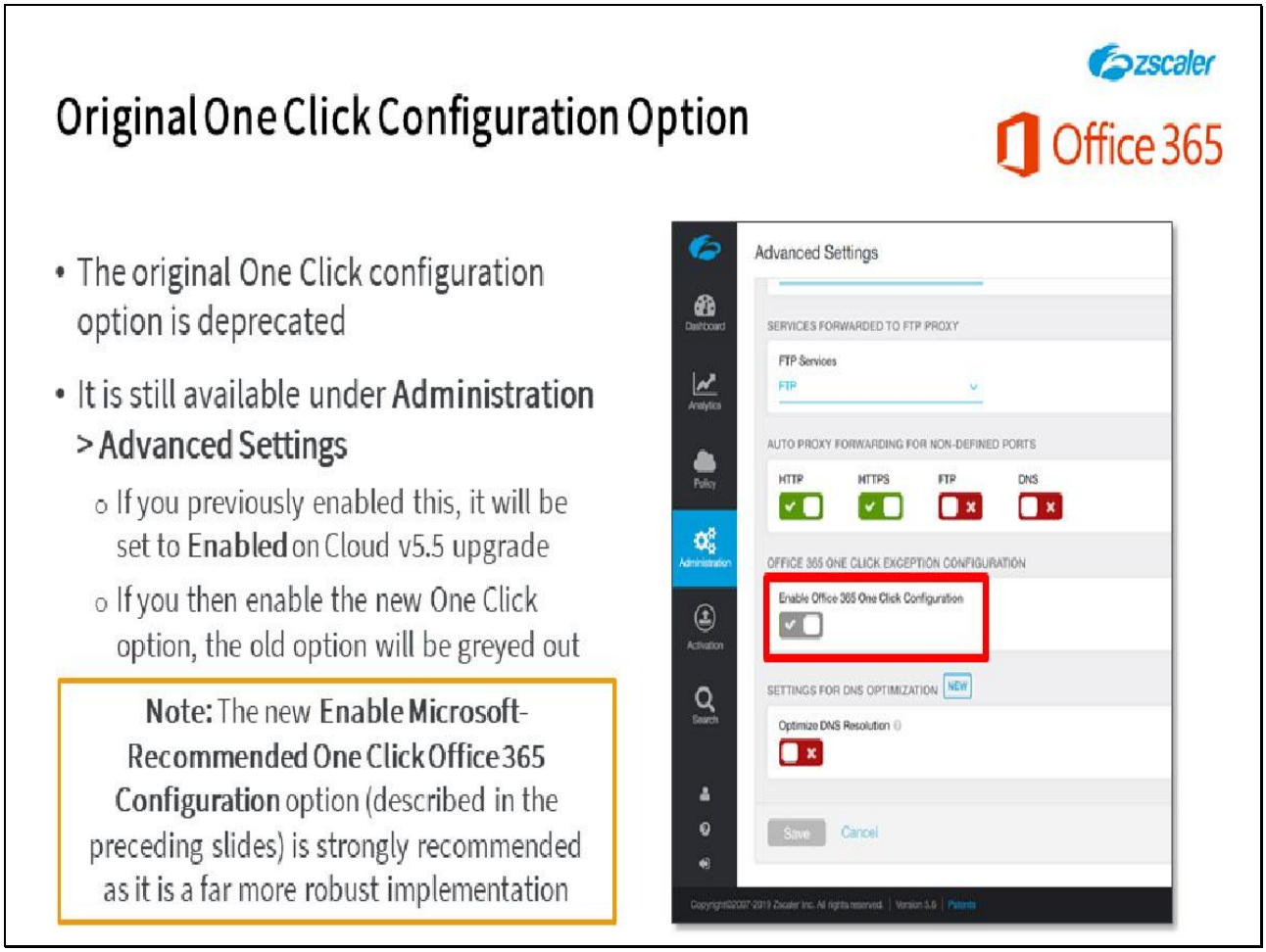


Slide notes

The original **One Click** option for Office 365, that was introduced in an earlier release, has been deprecated with the introduction of the enhanced capabilities in Cloud software v5.5. It is still available for backward compatibility purposes however, on the **Administration > Advanced Settings** page.

If you had previously enabled the original One Click capability, you will find that it is still enabled. If you had not previously enabled this setting, you still have the option to do so from the **Advanced Settings** page, although the new **One Click** configuration is much more capable and is strongly recommended. If you subsequently enable the **new One Click** capability (as described in the preceding slides), you will find that the **old** option is greyed out and can no longer be managed.

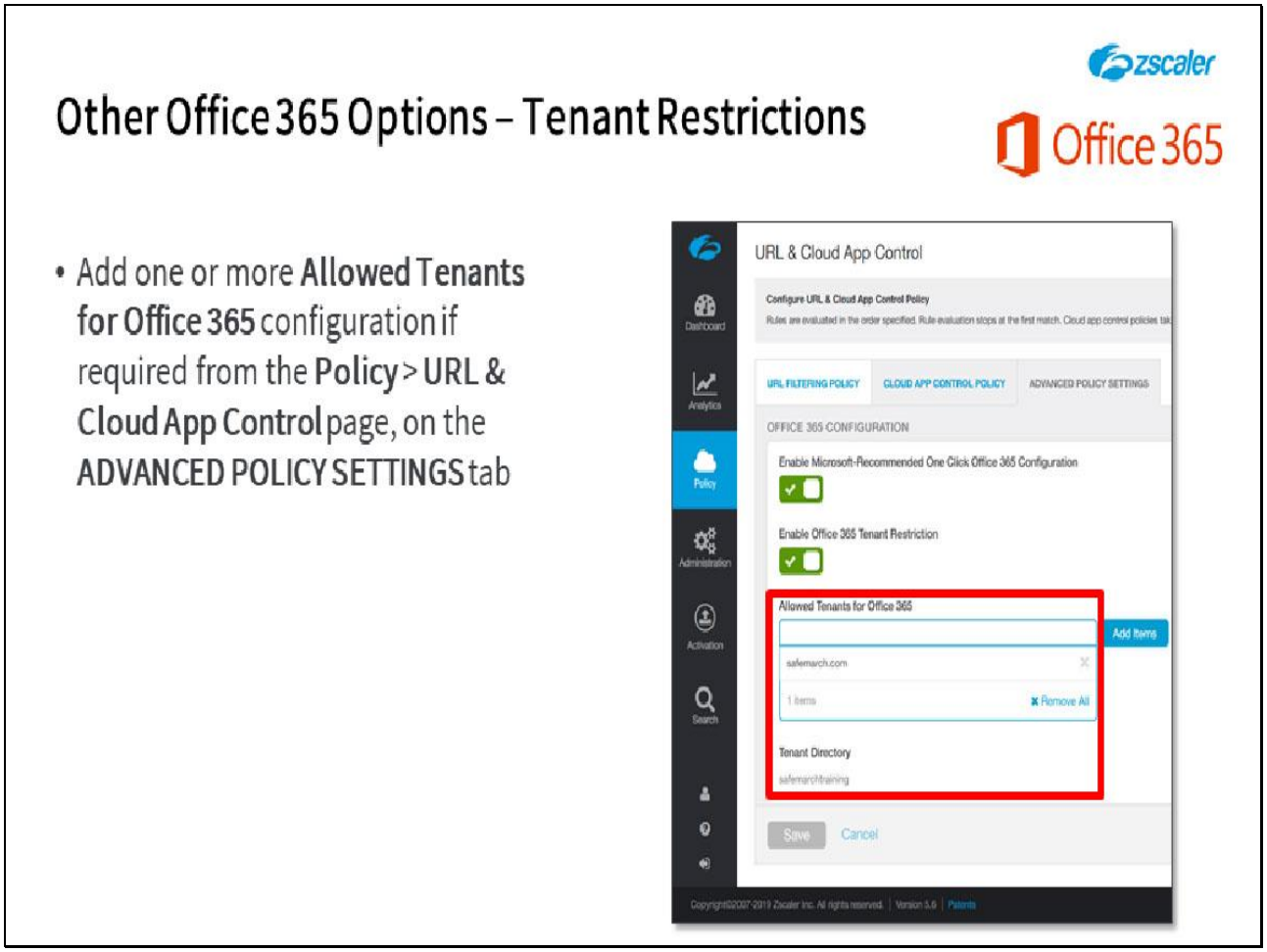
Slide 23 - Original One Click Configuration Option



Slide notes

Note that, if you have previously enabled the **One Click** setting for Office 365, we strongly recommend that you transition to use the **new** implementation of it, as it is a far more capable and robust solution.

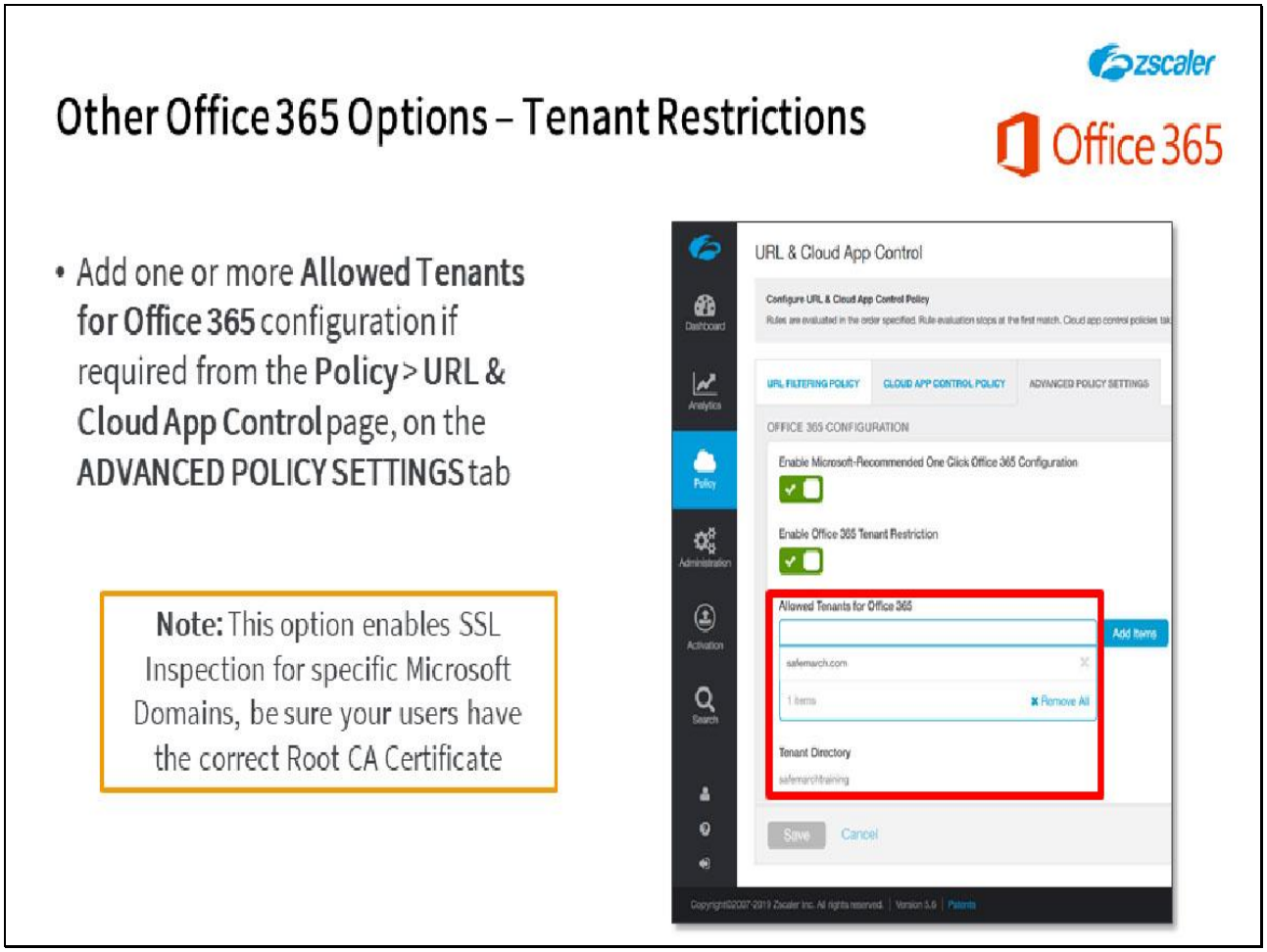
Slide 24 - Other Office 365 Options – Tenant Restrictions



Slide notes

An additional Office 365 setting available, is the option to specify the specific Office 365 tenants that are to be permitted access through the Zscaler service. Enabling and configuring this would prevent end users from accessing any other Office 365 tenant (for example their personal accounts) when connecting through Zscaler. You can add up to 30 domains, plus you must also add the appropriate **Tenant Directory**.

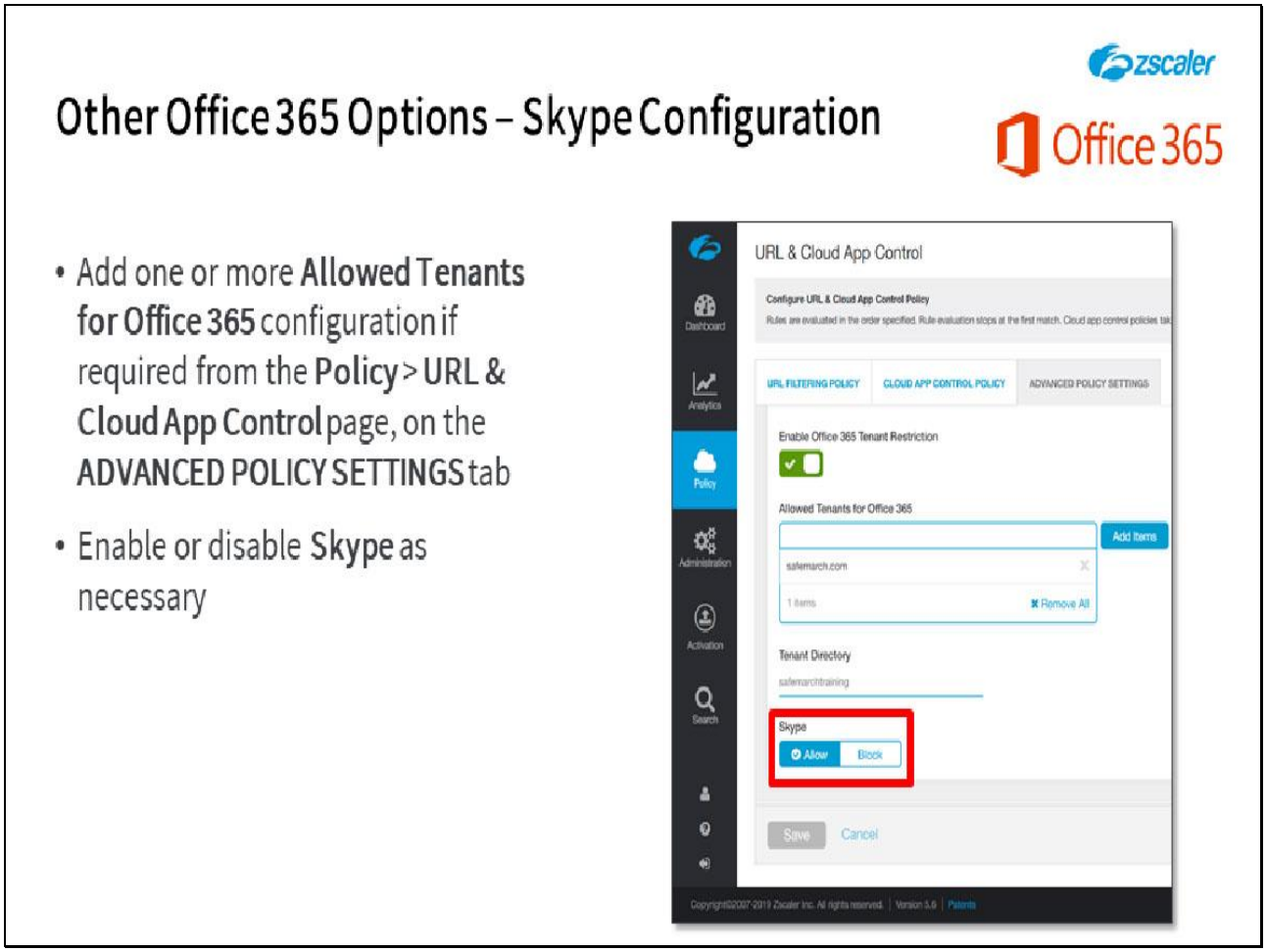
Slide 25 - Other Office 365 Options – Tenant Restrictions



Slide notes

Note that this configuration enables SSL interception for the **login.microsoftonline.com**, **login.microsoft.com**, and **login.windows.net** domains, so be sure that the appropriate root CA certificate for SSL Inspection is installed on your client PCs before enabling this option.

Slide 26 - Other Office 365 Options – Skype Configuration



Slide notes

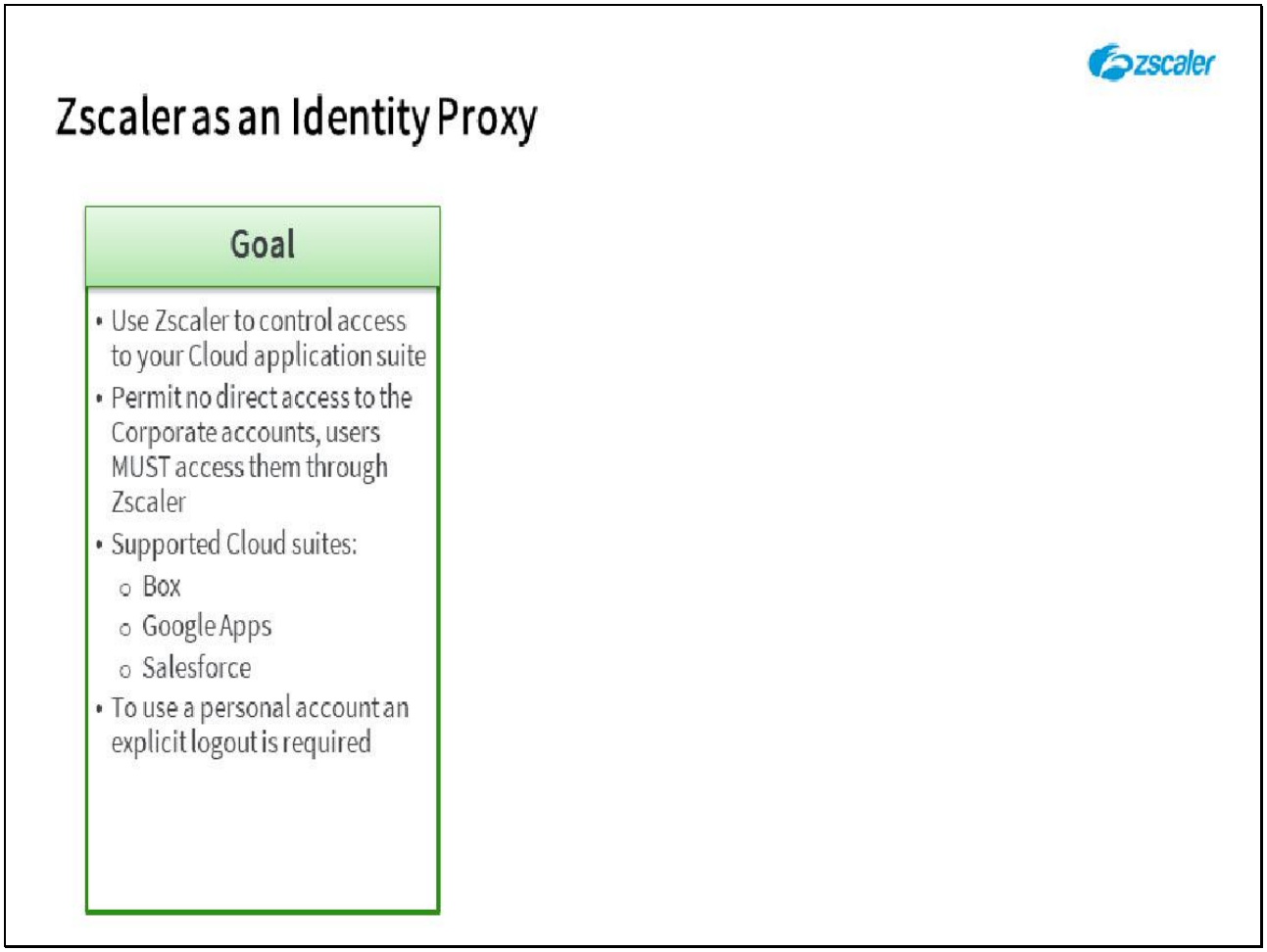
Finally, this is also where you have the option to enable or disable **Skype**.

Slide 27 - Controlling Access to Box, Google Apps, and Salesforce

Slide notes

The final topic that we'll cover, is the option to use Zscaler as the SAML IdP for certain Corporate application suites, to ensure that access to them is only possible through Zscaler.

Slide 28 - Zscaler as an Identity Proxy

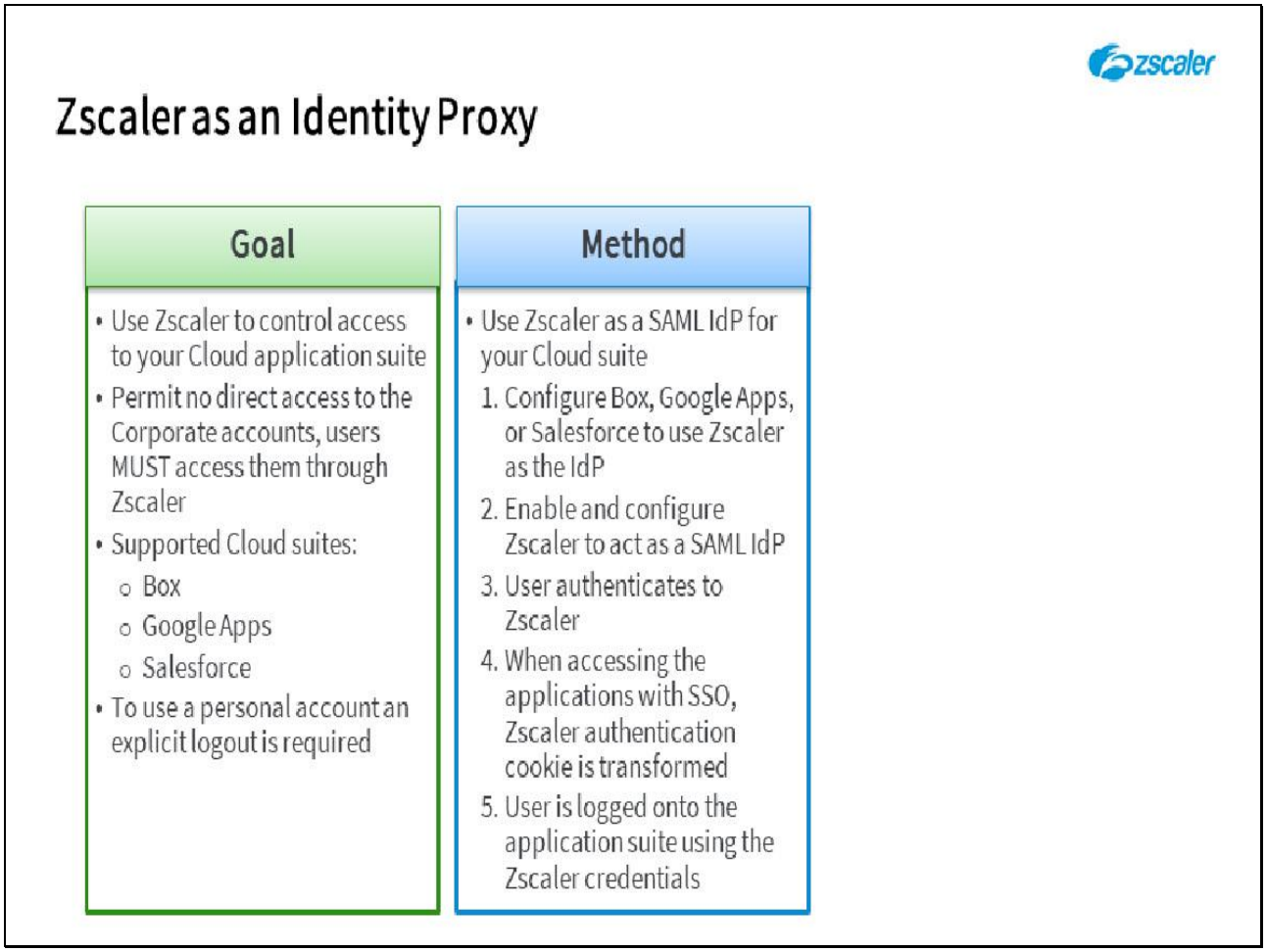


Slide notes

For certain application suites (namely; Box, Google Apps, and Salesforce), Zscaler can be specified as the SAML Identity Provider. The object here is to ensure that the Corporate instances of these applications can only be reached if the user is accessing them through Zscaler, to ensure the full protection of the Zscaler platform, and to log all access attempts.

If the user wants to access the Corporate instance of these application suites, they must go through Zscaler and authenticate using SAML single sign on (SSO). Personal access can be direct, although an explicit logout from the Corporate instance would be needed first.

Slide 29 - Zscaler as an Identity Proxy

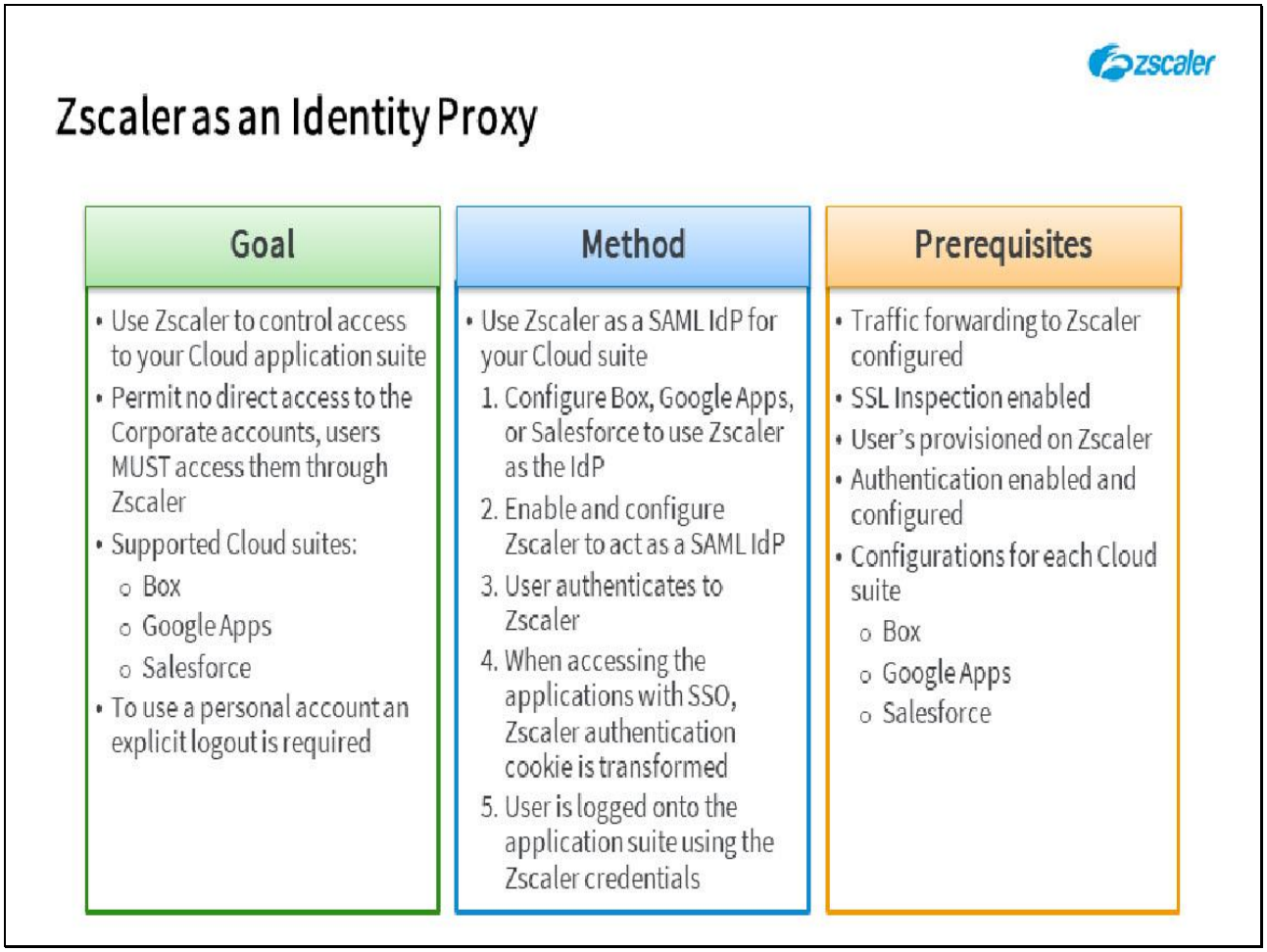


Slide notes

The method used to ensure that Zscaler is in the path, is to require authentication into these application suites using Zscaler as the SAML IdP. Users MUST be authenticated into Zscaler, and be in possession of a Zscaler authentication cookie, to be able to use the Corporate instance of these applications. The applications themselves must be configured to integrate with Zscaler as the IdP, and Zscaler must of course be configured to act in that capacity for each of these application suites.

Users must first authenticate to Zscaler and receive a Zscaler authentication cookie. Then, when they try to sign into any their Corporate applications with this feature enabled, they will be seamlessly logged in based on their Zscaler credentials.

Slide 30 - Zscaler as an Identity Proxy

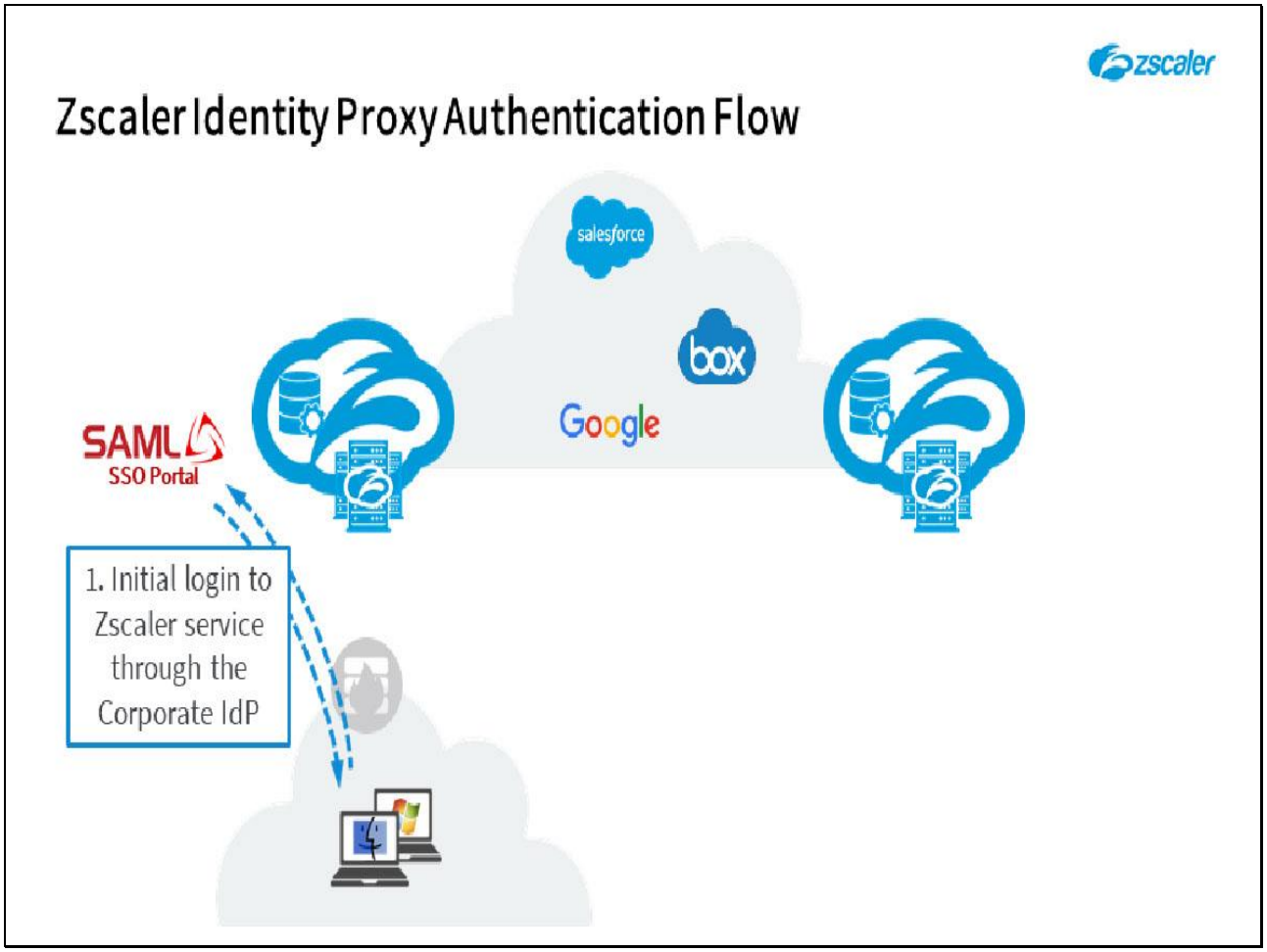


Slide notes

There are some prerequisites in order to enable this functionality, namely:

- Traffic forwarding to Zscaler must be configured.
- The **SSL Inspection** feature must be enabled.
- The user's must be provisioned on the Zscaler database.
- Zscaler authentication must be enabled and configured.
- Plus, the configurations for each Cloud application suite must be completed; Box, Google Apps, and Salesforce.

Slide 31 - Zscaler Identity Proxy Authentication Flow

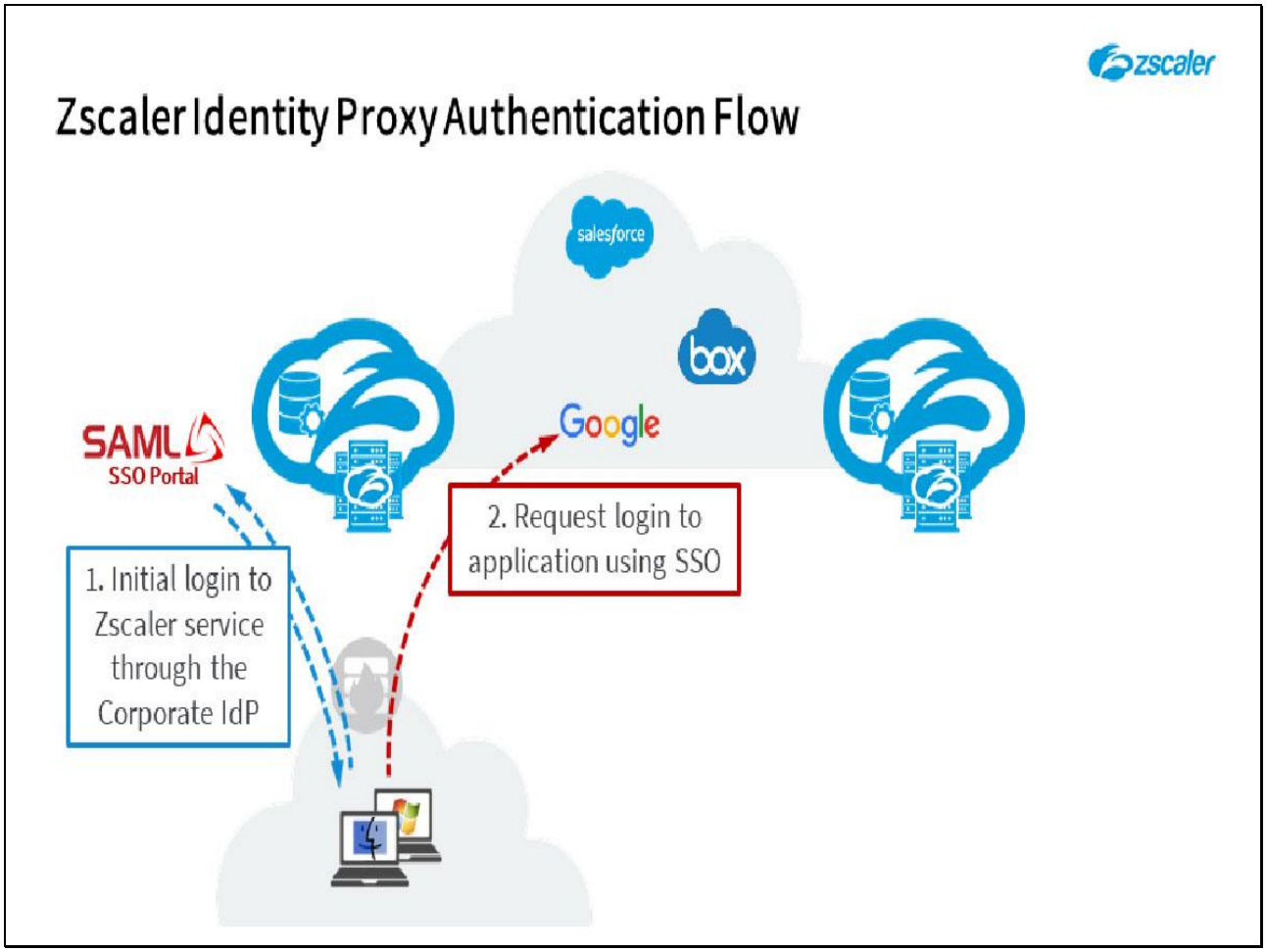


Slide notes

Once this feature is enabled and configured, both on Zscaler and on the relevant application suite, the authentication flow for users is as follows:

1. Users must first authenticate to the Zscaler service, to gain access to the Internet in the first place.

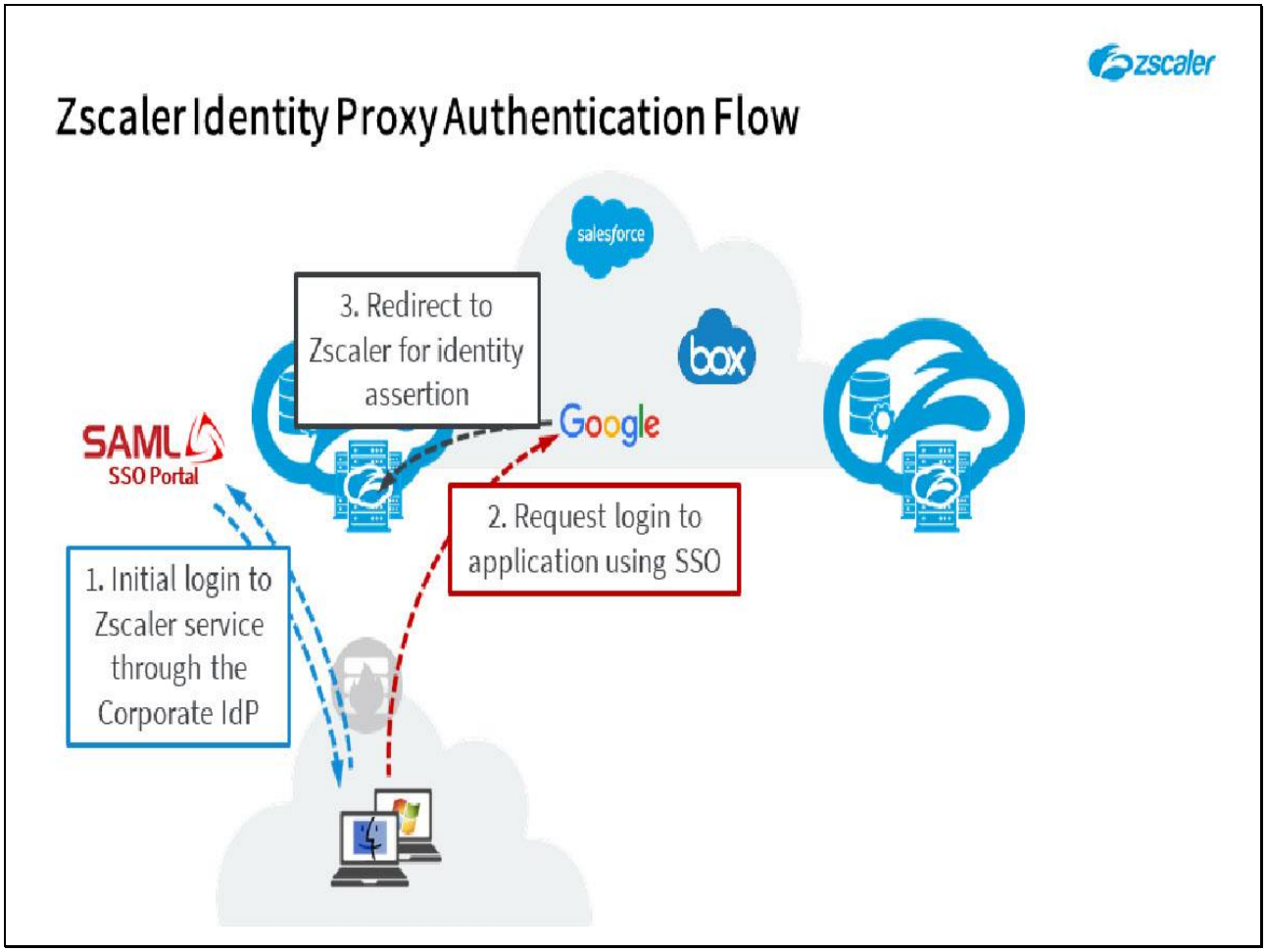
Slide 32 - Zscaler Identity Proxy Authentication Flow



Slide notes

2. The user goes to login to the Corporate instance of a configured application suite, using SSO.

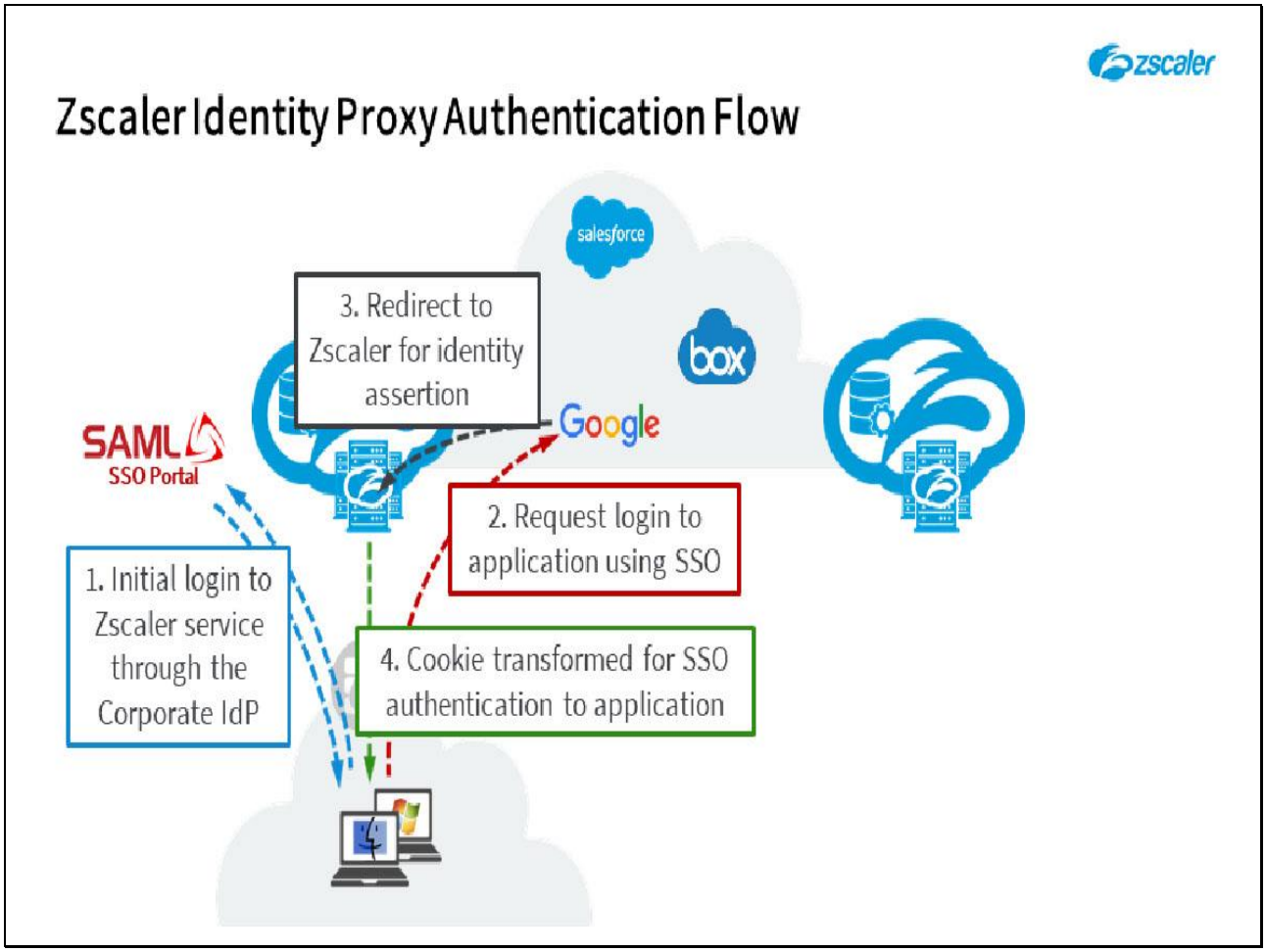
Slide 33 - Zscaler Identity Proxy Authentication Flow



Slide notes

3. The user is transparently re-directed to Zscaler, which is acting as a SAML IdP.

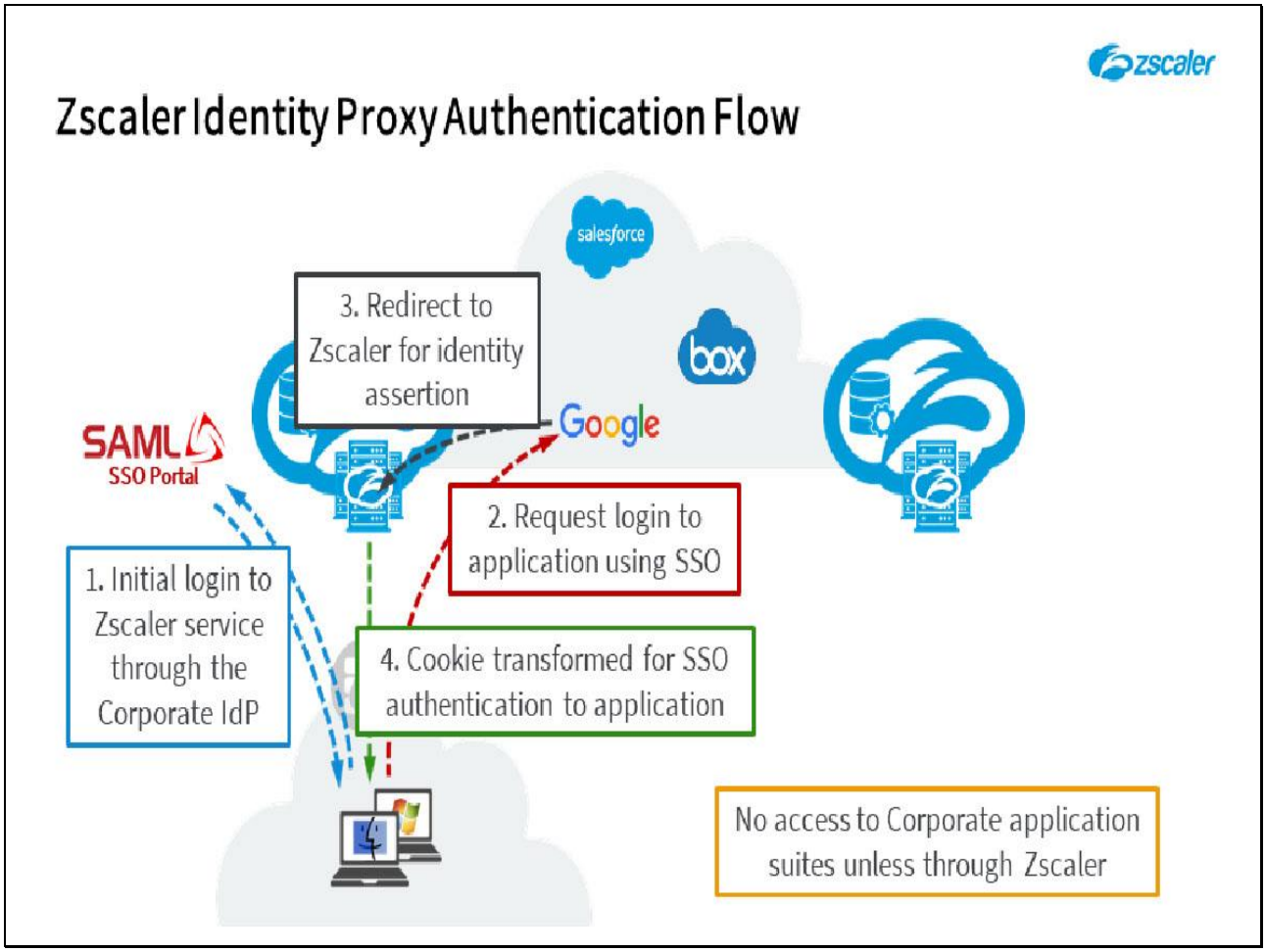
Slide 34 - Zscaler Identity Proxy Authentication Flow



Slide notes

4. Zscaler transforms the existing authentication cookie on the user's machine, for use with the application suite requested, and the user is seamlessly authenticated to it. All that the users sees, is that they request access to the application using SSO, and they are signed in almost immediately.

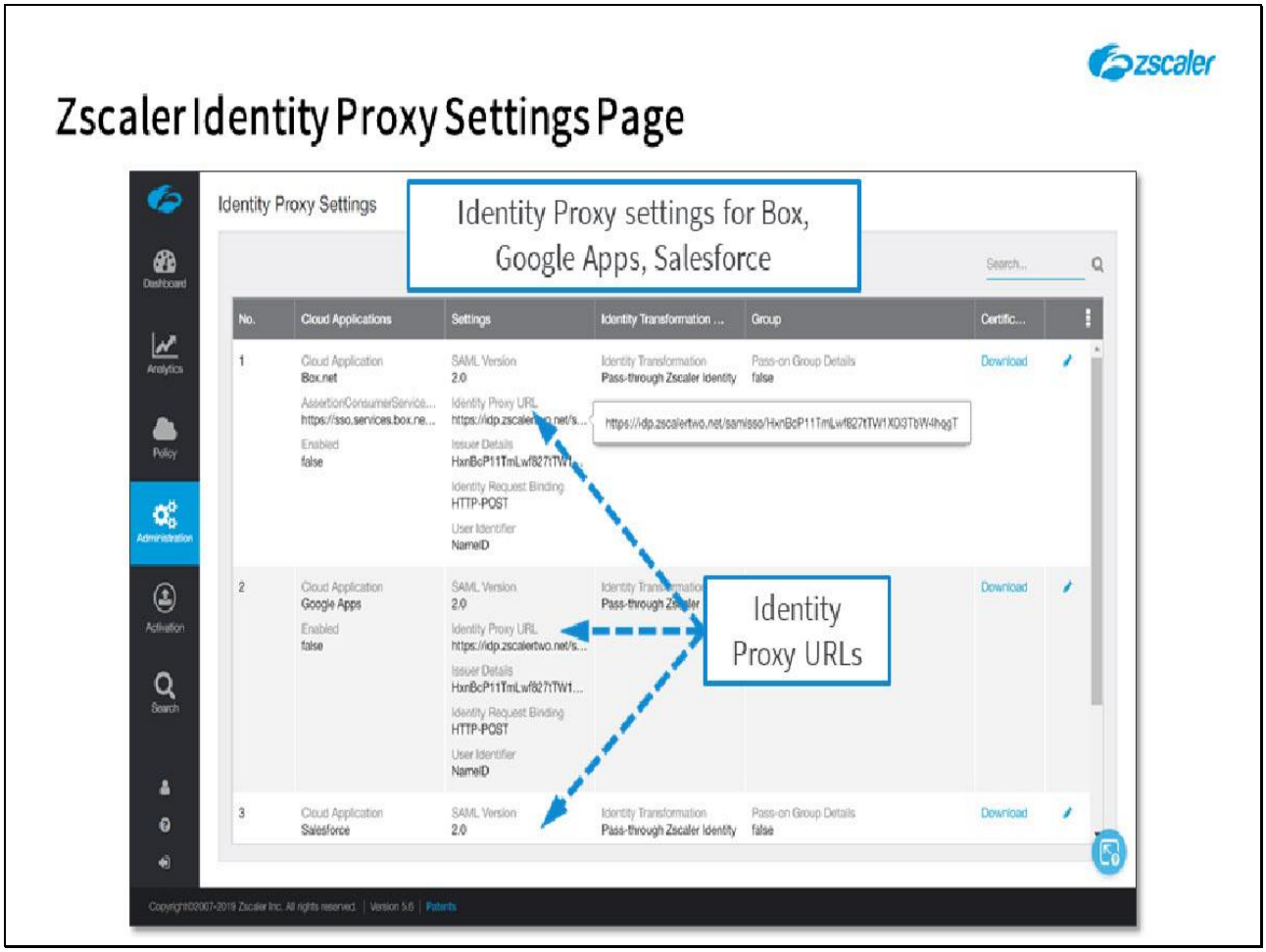
Slide 35 - Zscaler Identity Proxy Authentication Flow



Slide notes

When this feature is enabled and configured, access to the Corporate instance of the Box, Google Apps, or Salesforce application suites is only possible when connecting through Zscaler. Access to these application suites using some other account is possible whether or not the user is connecting through Zscaler.

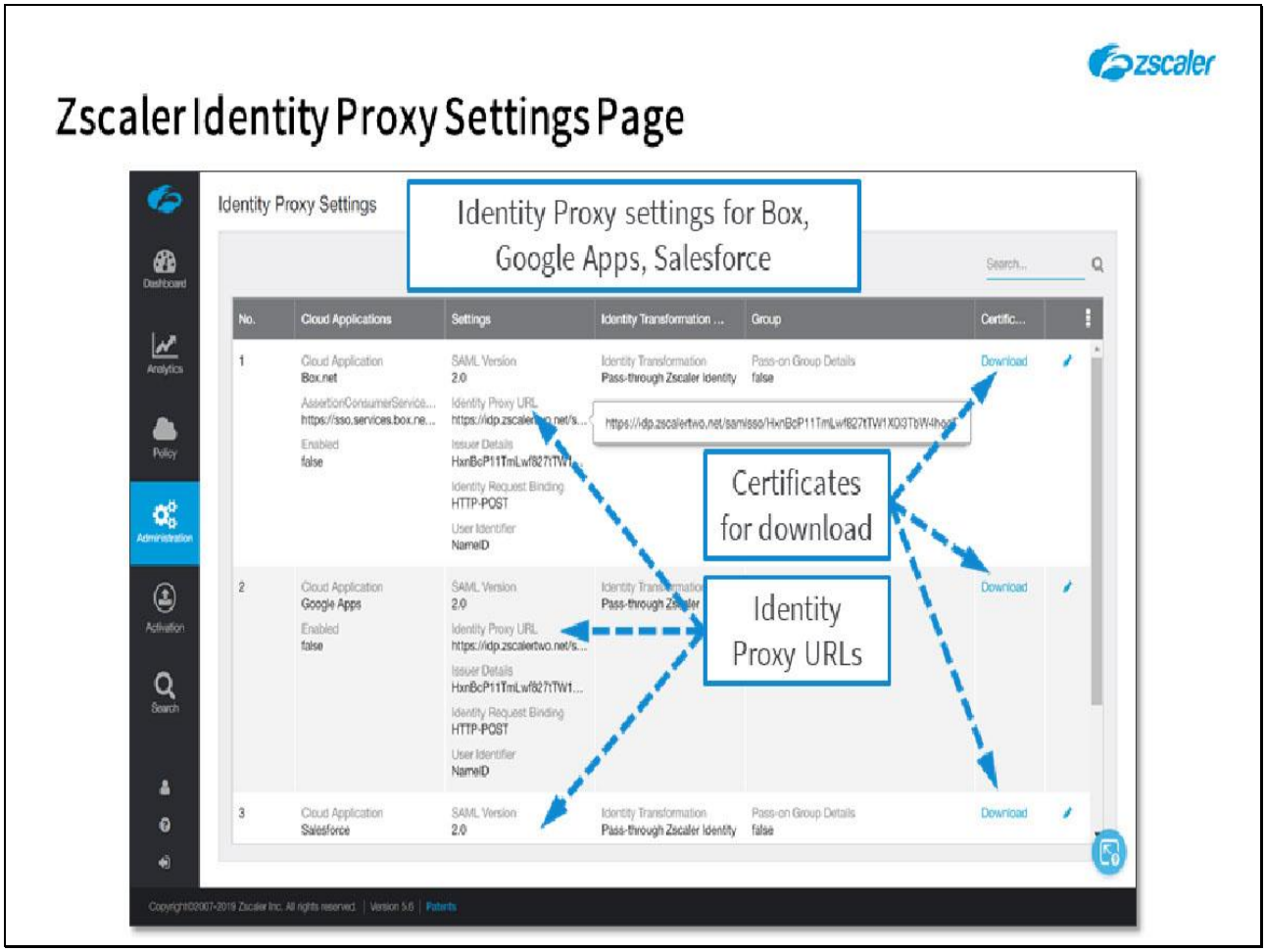
Slide 36 - Zscaler Identity Proxy Settings Page



Slide notes

To configure Identity Proxy settings for Box, Google Apps, and Salesforce, navigate to the **Administration > Identity Proxy Settings** page in the Zscaler Admin Portal. Here you will find separate settings for Box, Google Apps, and Salesforce, with the data necessary to configure those application suites to use Zscaler as the IdP, including the **Identity Proxy URLs**.

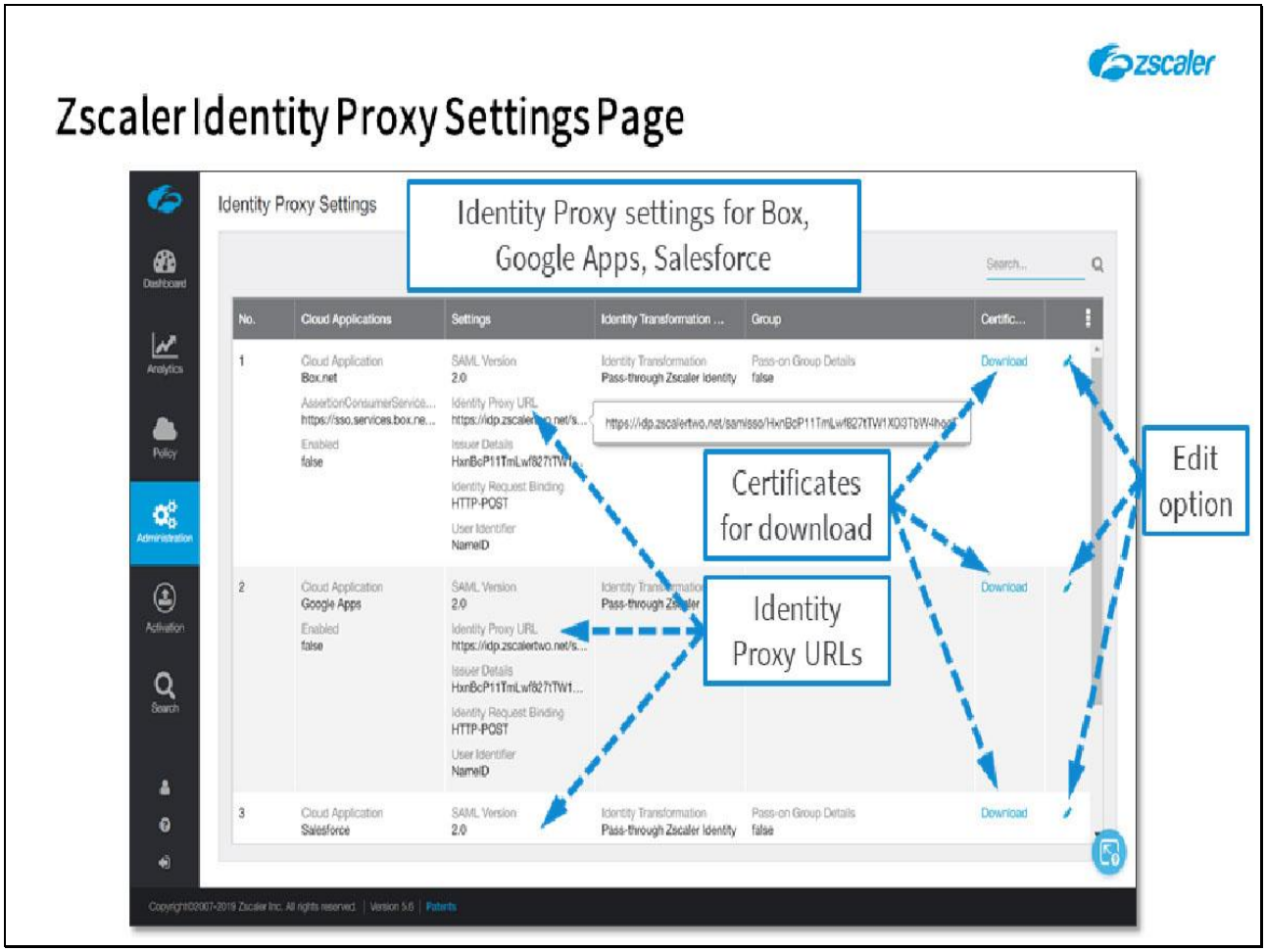
Slide 37 - Zscaler Identity Proxy Settings Page



Slide notes

The certificates that must be uploaded to the Corporate instances of these application suites can be downloaded from this page...

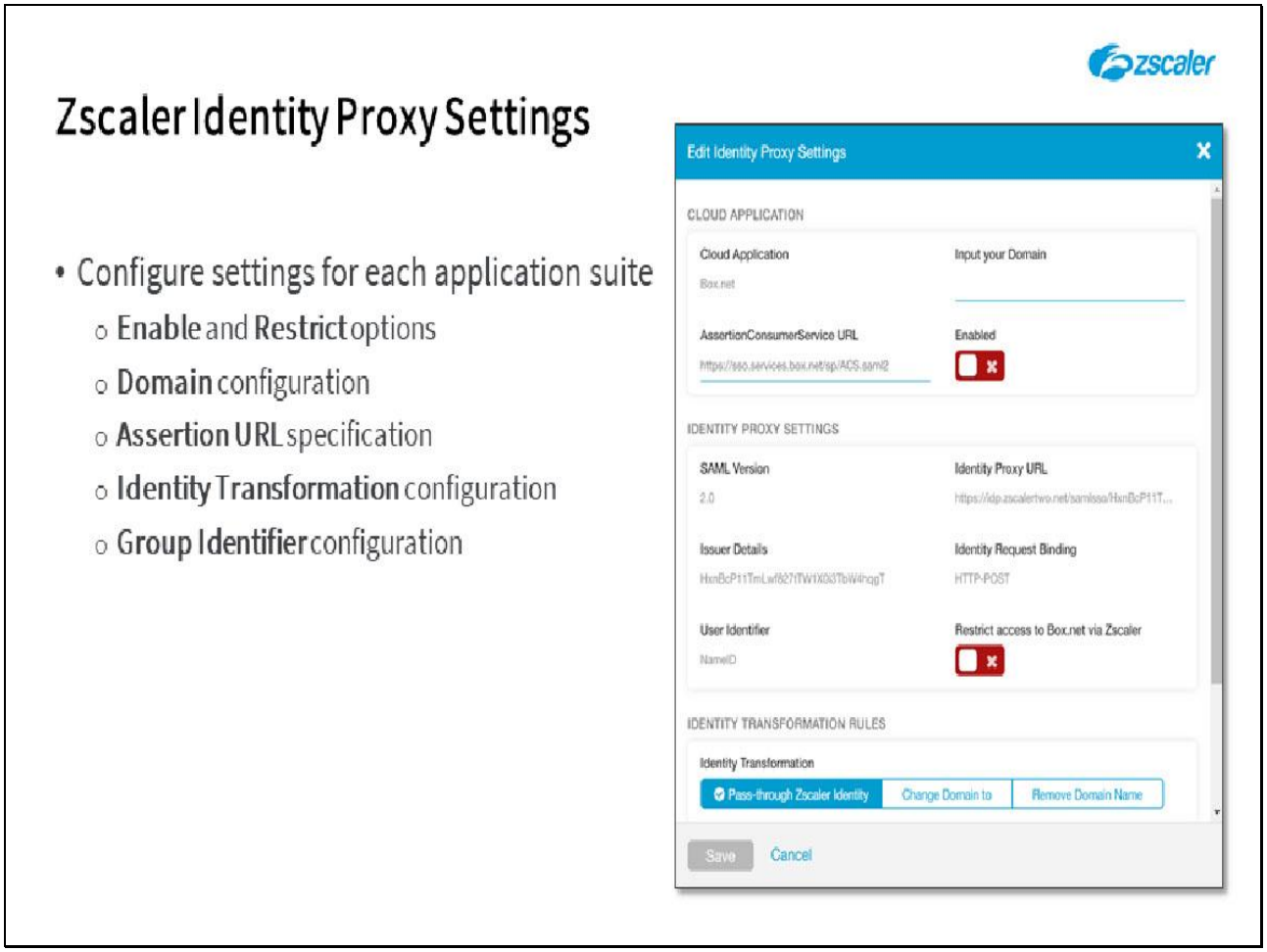
Slide 38 - Zscaler Identity Proxy Settings Page



Slide notes

...and you have the option to edit each of these settings.

Slide 39 - Zscaler Identity Proxy Settings

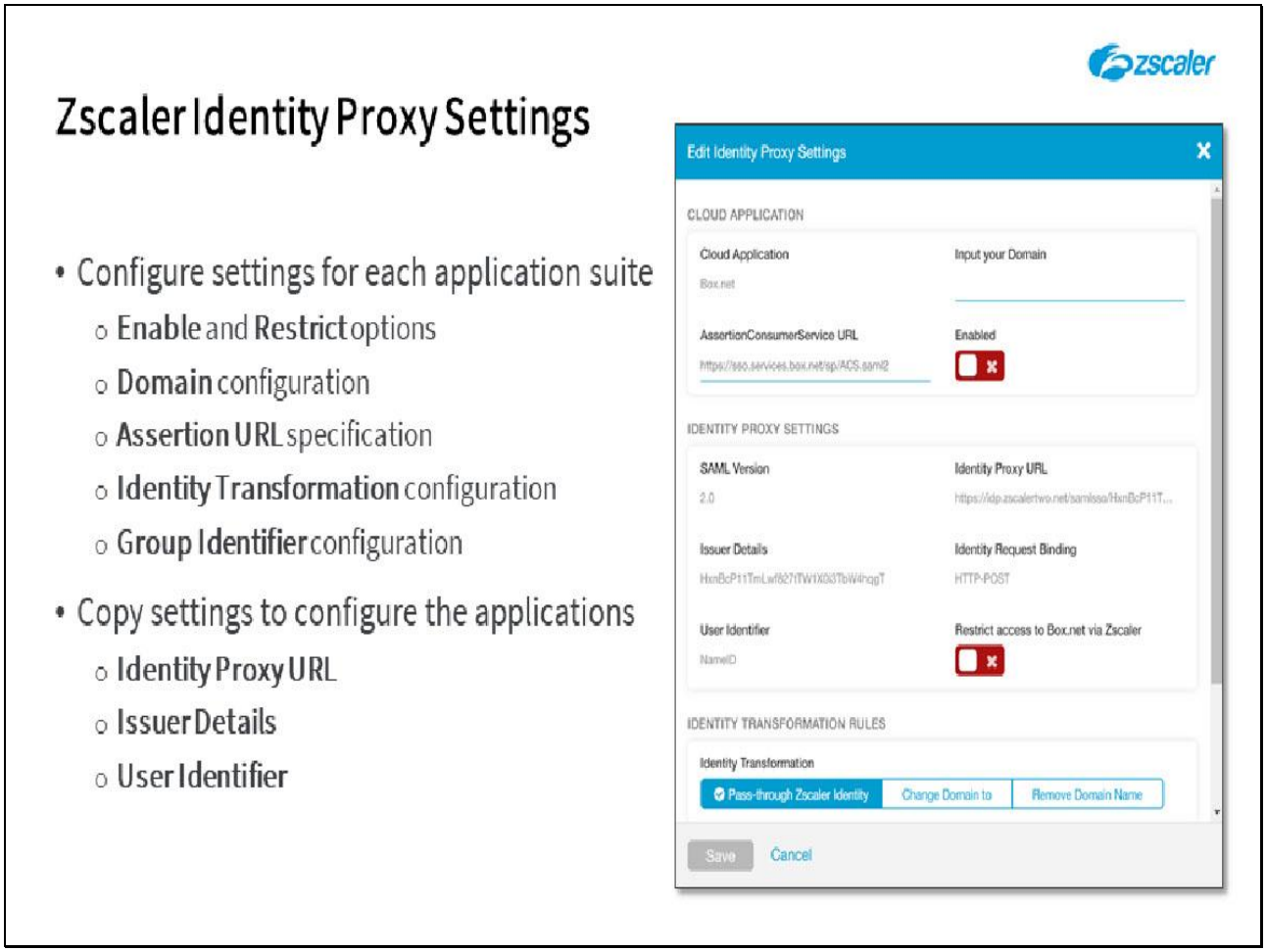


Slide notes

You must configure settings for each application suite individually, the settings available are:

- To use Zscaler as an Identity Proxy you must **Enable** the configuration and turn on the **Restrict access to [the relevant application suite] via Zscaler** option.
- You must provide your Domain information.
- You must provide the **AssertionConsumerService URL**, which for Box is displayed automatically, for Google Apps the URL is completed as you type in your domain, and for Salesforce you must enter the Salesforce Login URL.
- There is an **Identity Transformation** configuration, where you choose whether to pass-through the Zscaler login as is, replace the Domain part of the user name with a different Domain name (from the pick-list), or delete the Domain part of the user name entirely and pass only the user ID.
- For Box and Salesforce, you have the option to **Pass-on Group Details**, to send all group identifiers, or specify the **Group Identifier Name** to send.

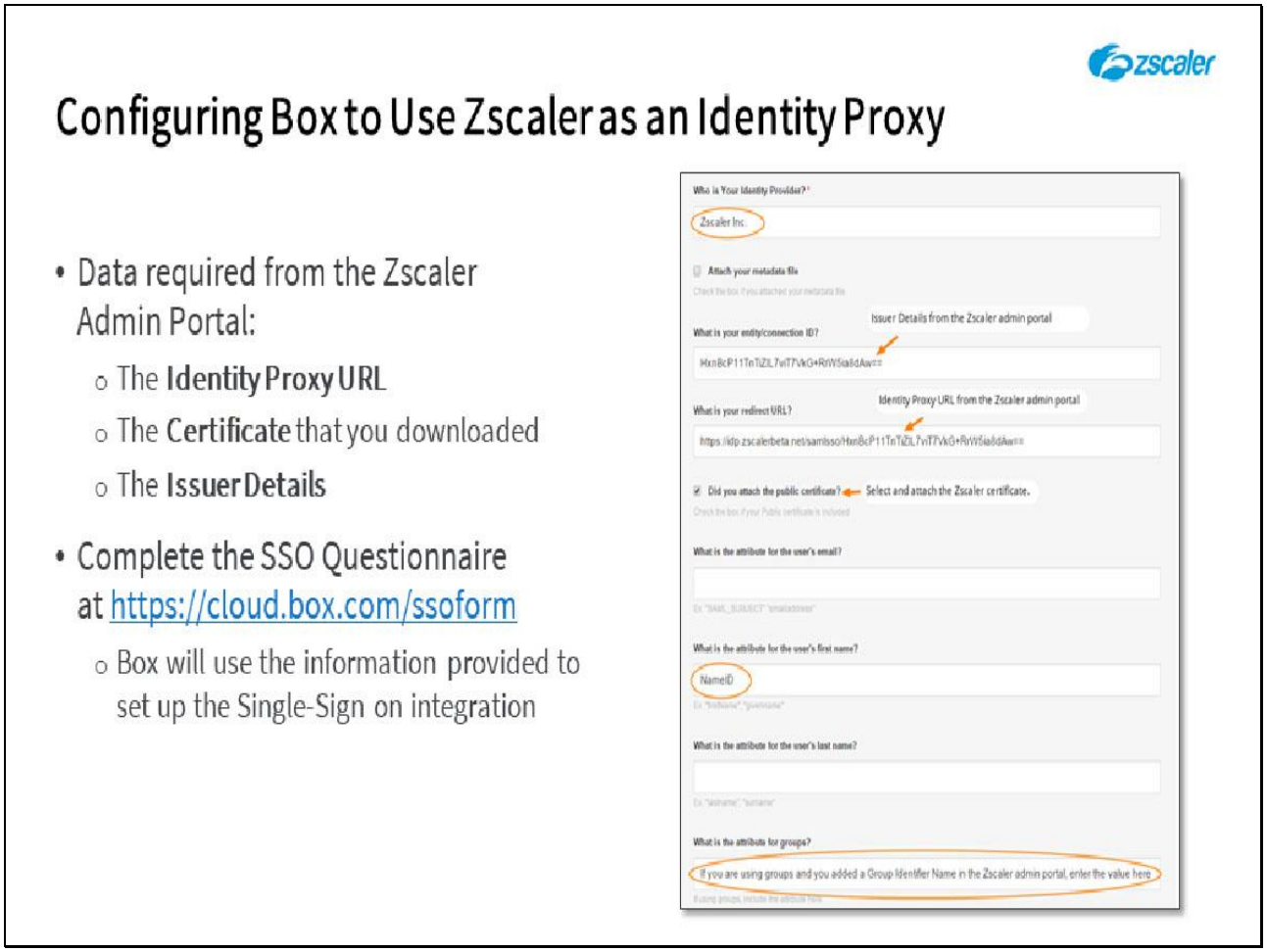
Slide 40 - Zscaler Identity Proxy Settings



Slide notes

These settings also contain data that you will need to copy and paste across to the application suite in question. The data required depends on the suite, but you will certainly need the **Identity Proxy URL**, and you may also need the **Issuer Details** and **User Identifier**.

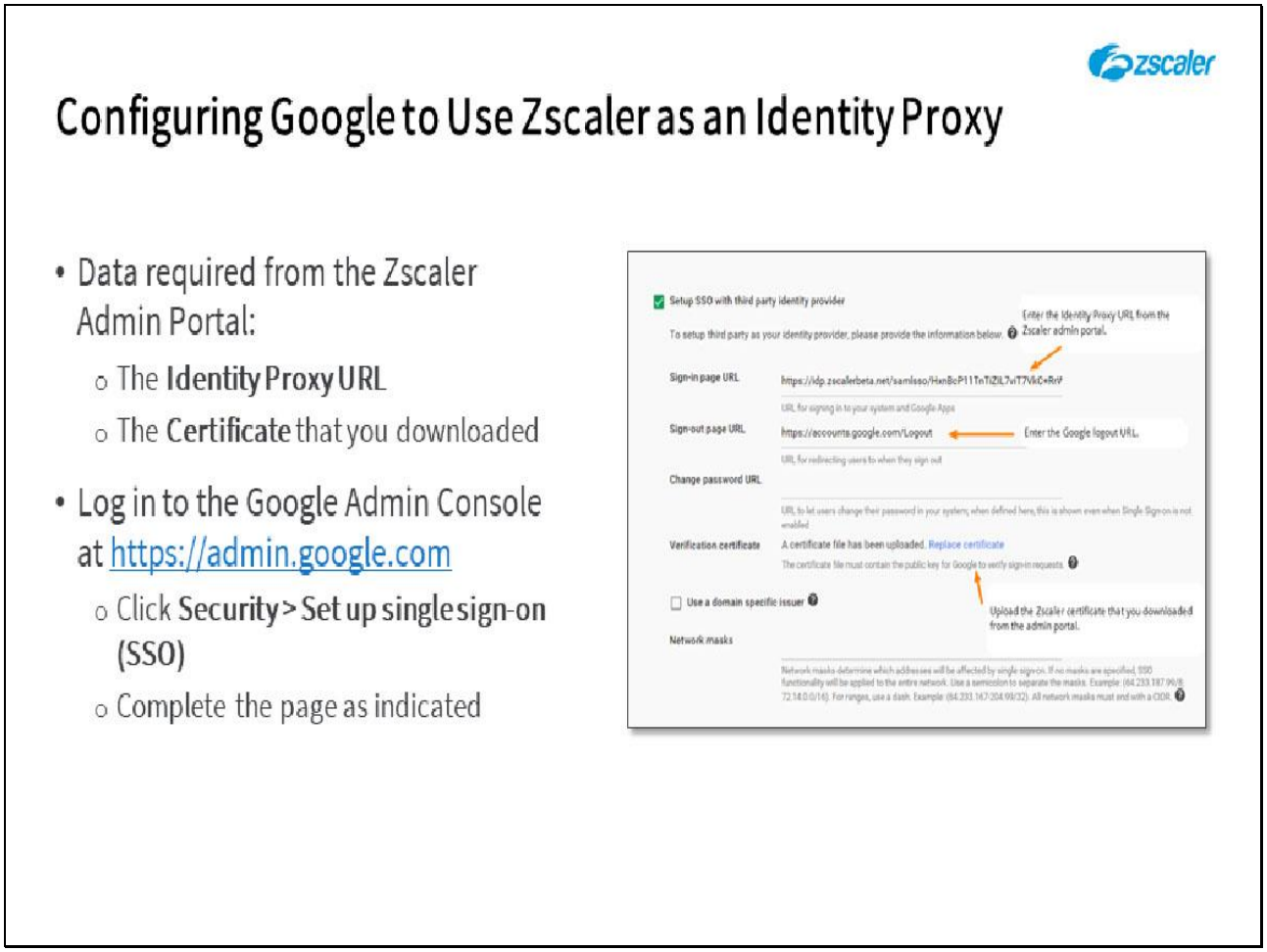
Slide 41 - Configuring Box to Use Zscaler as an Identity Proxy



Slide notes

You must of course configure the application suite to use Zscaler as the IdP. For Box, the data you will need is the **Identity Proxy URL**, the Certificate that you downloaded from Zscaler, and the **Issuer Details**. To integrate with Box, simply complete the for at **https://cloud.box.com/ssoform** and provide all the required data. Box will then set up the SSO functionality for you.

Slide 42 - Configuring Google to Use Zscaler as an Identity Proxy



Slide notes

For Google Apps, the data you will need is the **Identity Proxy URL**, and the Certificate that you downloaded from Zscaler. Log in to the Google Admin Console at **https://admin.google.com**, go to the **Security > Set up single sign-on (SSO)** page, and provide the required information as indicated in this image.

Slide 43 - Configuring Google to Use Zscaler as an Identity Proxy

Configuring Google to Use Zscaler as an Identity Proxy

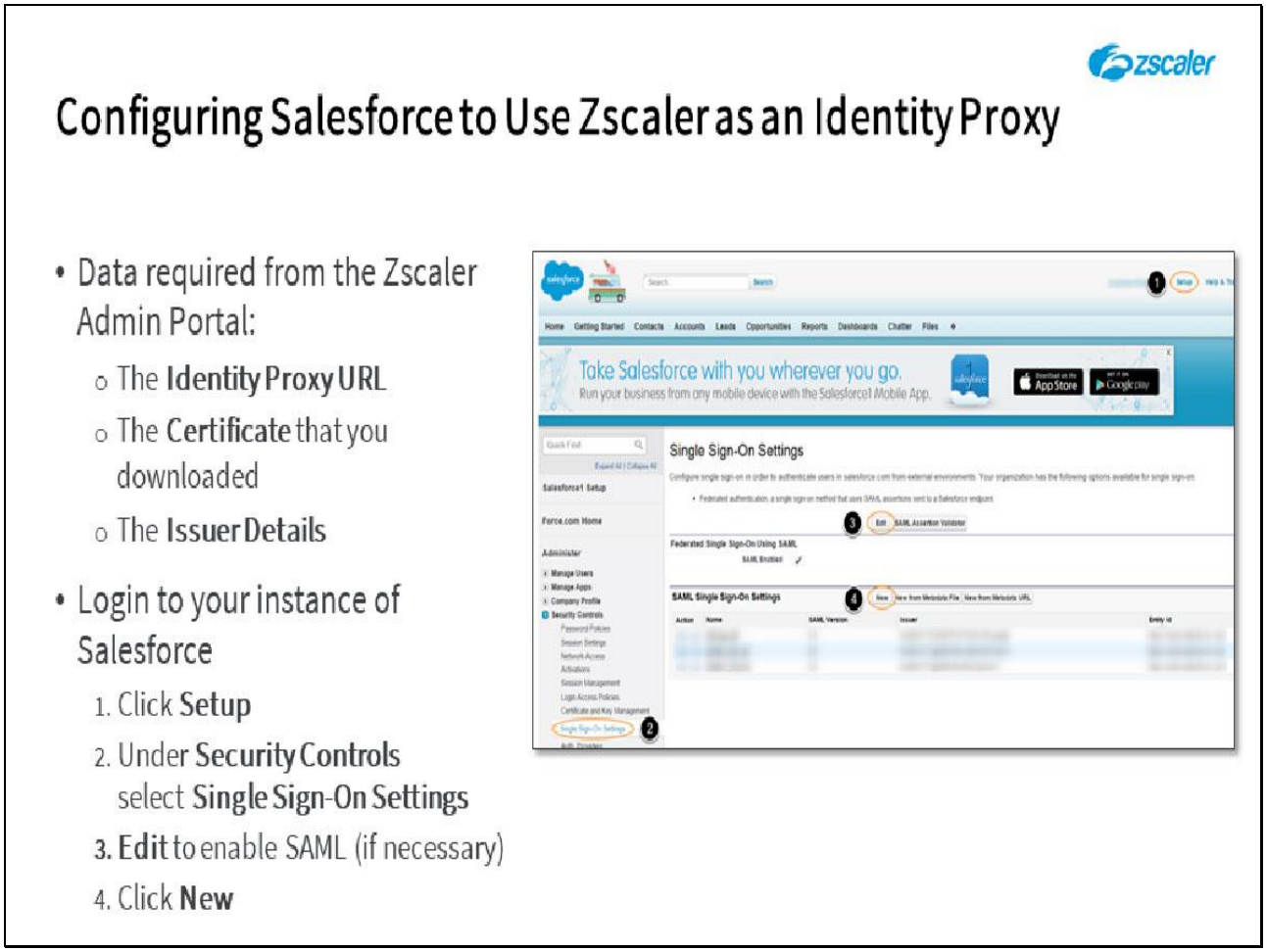
- Data required from the Zscaler Admin Portal:
  - The **Identity Proxy URL**
  - The **Certificate** that you downloaded
- Log in to the Google Admin Console at https://admin.google.com
  - Click **Security > Set up single sign-on (SSO)**
  - Complete the page as indicated

Note: the single-sign on feature cannot be used by users who are assigned administrator roles in Google

Slide notes

One thing to note with Google Apps, users who are assigned administrator roles in Google cannot use the SSO functionality.

Slide 44 - Configuring Salesforce to Use Zscaler as an Identity Proxy

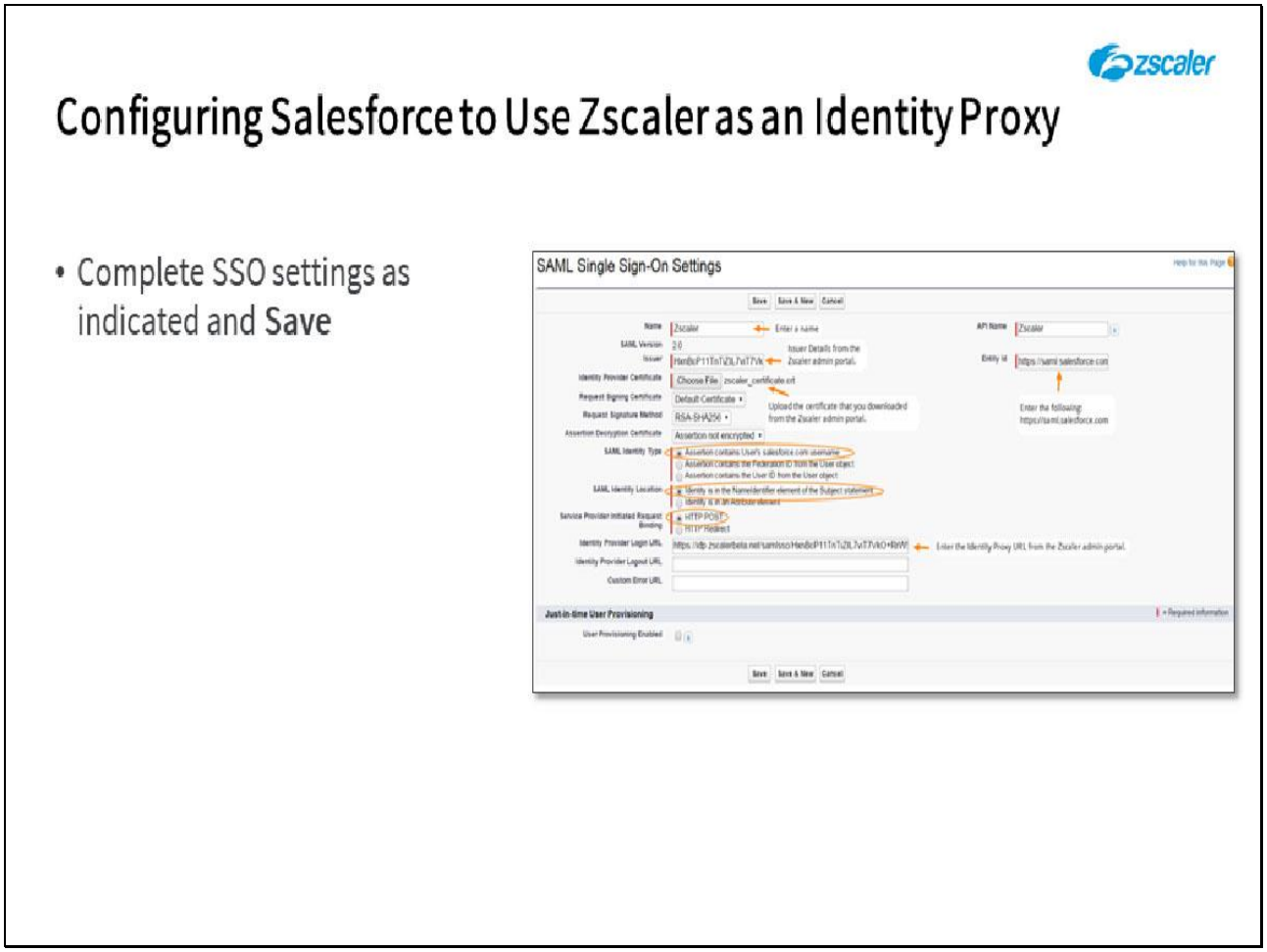


Slide notes

The Salesforce integration is the most complex, and the data you will need is the **Identity Proxy URL**, the Certificate that you downloaded from Zscaler, and the **Issuer Details**.

There are several steps to the Salesforce configuration, and the first is to login to your instance of Salesforce and click **Setup** at the top right. In the side bar navigation menu at the left, under **Security Controls** select **Single Sign-On Settings**. If necessary click **Edit** and enable SAML, then under **SAML Single Sign-on Settings** click **New**.

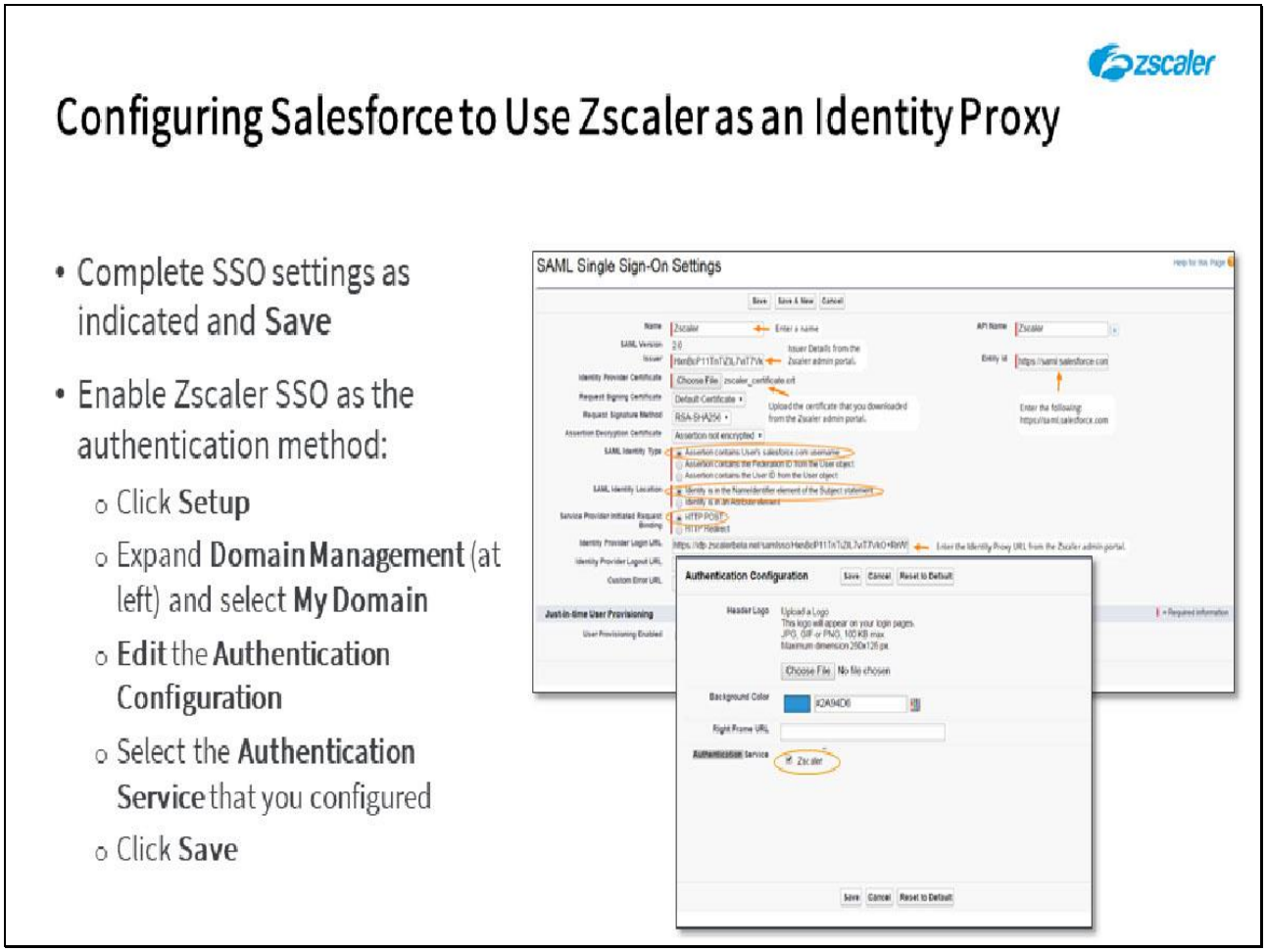
Slide 45 - Configuring Salesforce to Use Zscaler as an Identity Proxy



Slide notes

Complete the SSO settings as indicated in this image and click **Save**.

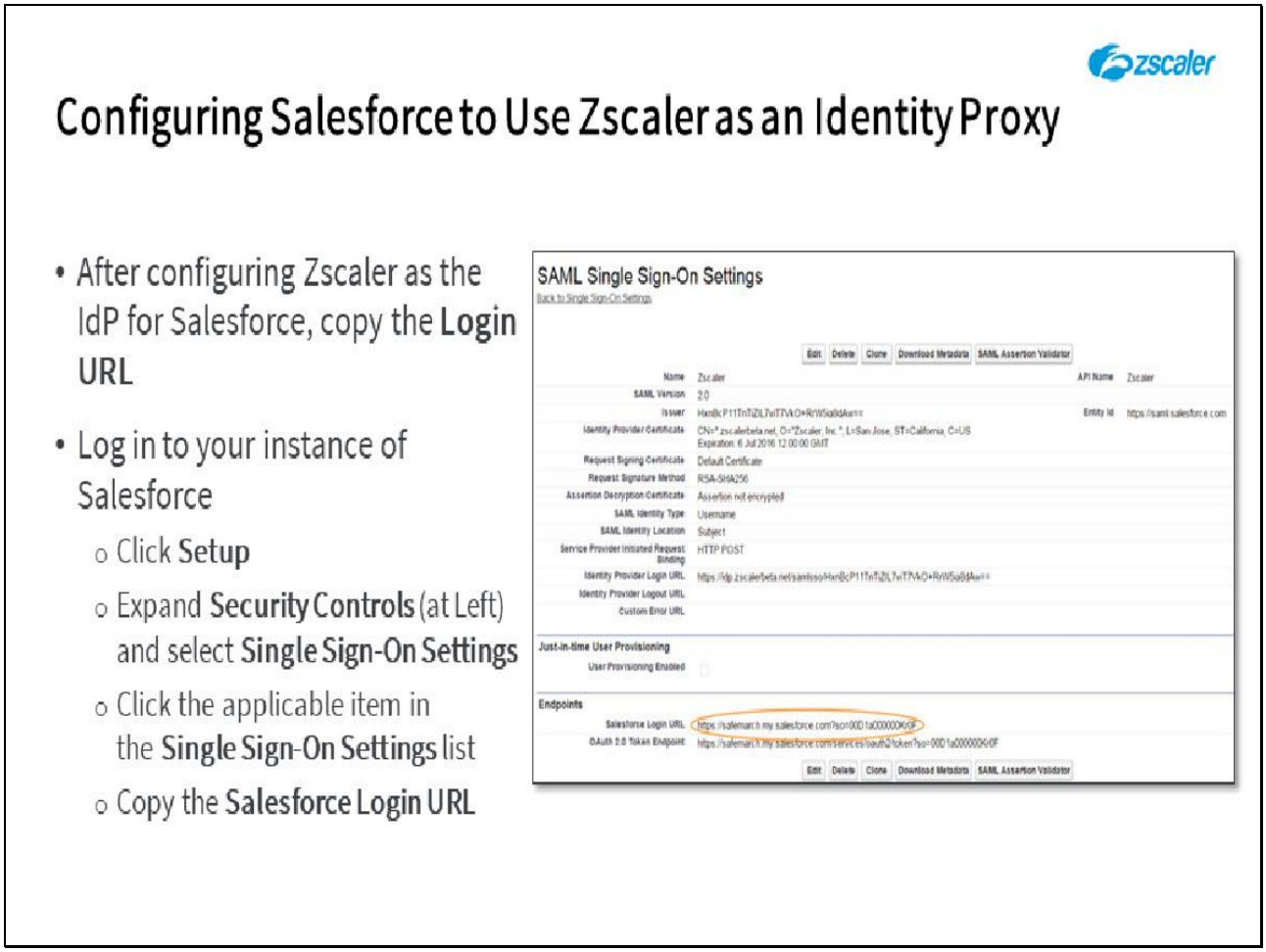
Slide 46 - Configuring Salesforce to Use Zscaler as an Identity Proxy



Slide notes

Next you must enable Zscaler SSO as the authentication method, to do this click **Setup** again, expand the **Domain Management** option in the side bar menu at left and select **My Domain**. Select to **Edit** the **Authentication Configuration**, select the **Authentication Service** that you configured (**Zscaler** or the name that you set), and click **Save**.

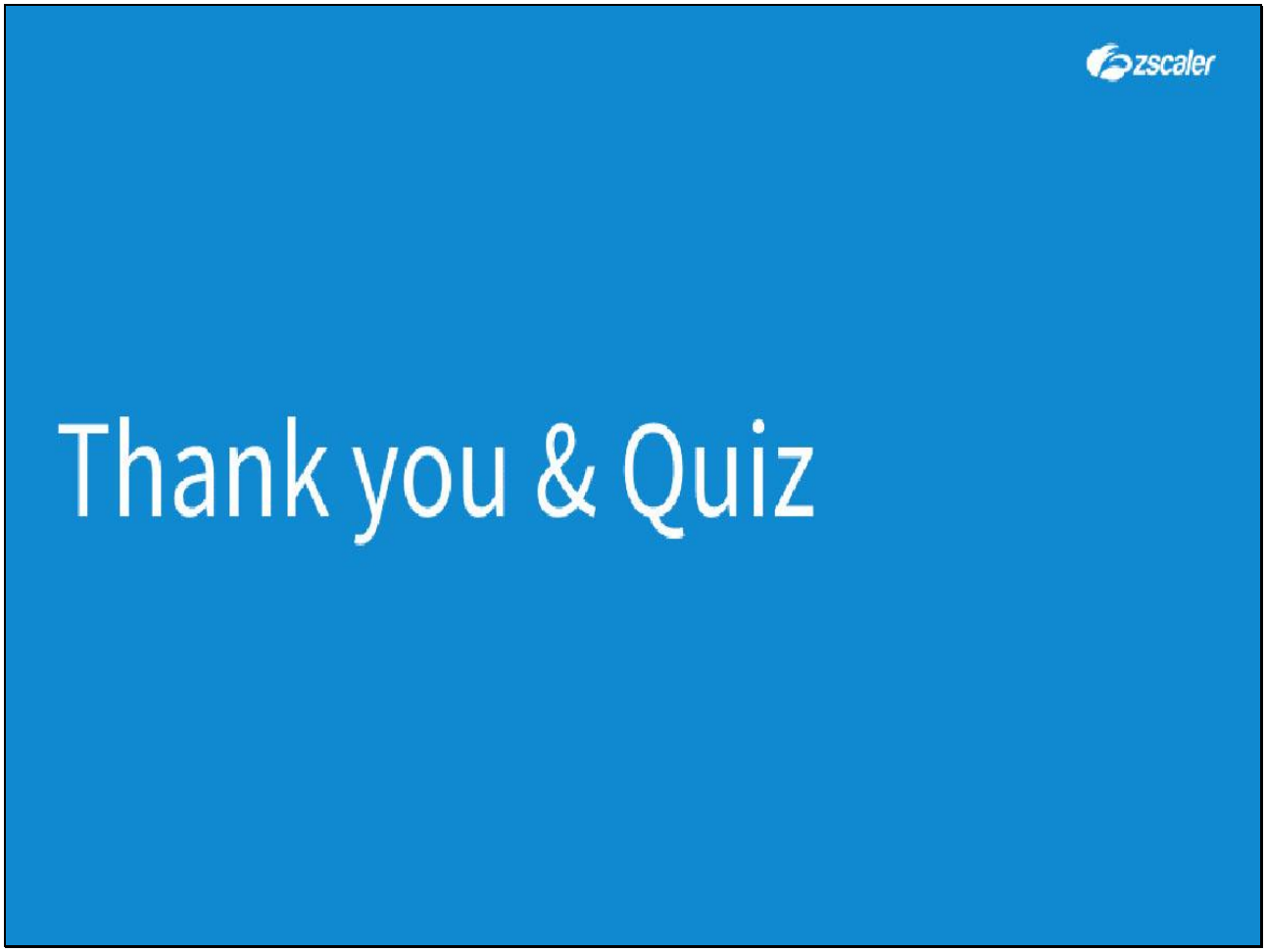
Slide 47 - Configuring Salesforce to Use Zscaler as an Identity Proxy



Slide notes

Lastly, you need to copy the **Login URL**, which you need for the **AssertionConsumerService URL** in the Zscaler settings. Log in to your instance of Salesforce and click **Setup**, expand the **Security Controls** option in the side bar menu at left and select **Single Sign-On Settings**, click on the applicable item in the **Single Sign-On Settings** list and copy the **Salesforce Login URL**. Paste this value into the Salesforce settings in the Zscaler Admin Portal.

Slide 48 - Thank you & Quiz



Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

Click the **X** at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.