


Slide 1 - Zscaler Policies



# Zscaler Policies

## Office 365 and Cloud Application Suites

©2019 Zscaler, Inc. All rights reserved.

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

## Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. The dashboard includes a navigation bar with links for Dashboard, Analytics, Policy, and Administration. The main content area displays several charts and tables, including 'Cloud Application Classes', 'Top URLs Categories', 'Top Users', and 'Streaming Media Applications'. Overlaid on the screenshot are several blue callout boxes with white text, each pointing to a specific control:

- Exit**: Points to the 'X' button in the top right corner of the dashboard window.
- Previous Slide**: Points to the left arrow button in the bottom left corner of the video player.
- Next Slide**: Points to the right arrow button in the bottom left corner of the video player.
- Play/Pause**: Points to the play/pause button in the bottom left corner of the video player.
- Fast Forward**: Points to the fast forward button in the bottom left corner of the video player.
- Progress Bar**: Points to the progress bar in the bottom left corner of the video player.
- Audio On/Off**: Points to the audio on/off button in the bottom right corner of the video player.
- Closed Captioning**: Points to the closed captioning button in the bottom right corner of the video player.

## 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



# Agenda

- Microsoft Office 365 One Click Policy
- Controlling Access to Box, Google Apps, and Salesforce

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

The slide features a white background with a black border. In the top right corner, there is a blue 'zscaler' logo and the 'Office 365' logo, which consists of a red square icon followed by the text 'Office 365' in red. The main title 'Microsoft Office 365' is positioned in the upper left in a large, black, sans-serif font. Below the title, a red-bordered box contains a red header 'Microsoft Suite of Productivity/Collaboration Applications' and a bulleted list of services. The list includes: 'O365 shared services, O365 authentication (using Azure AD), Exchange Online, Skype for Business Online, SharePoint Online, O365 Video and Microsoft Stream, Office Online, Yammer, Sway, Planner, Microsoft Teams, Office Clients'.

Microsoft Office 365

zscaler

Office 365

**Microsoft Suite of Productivity/Collaboration Applications**

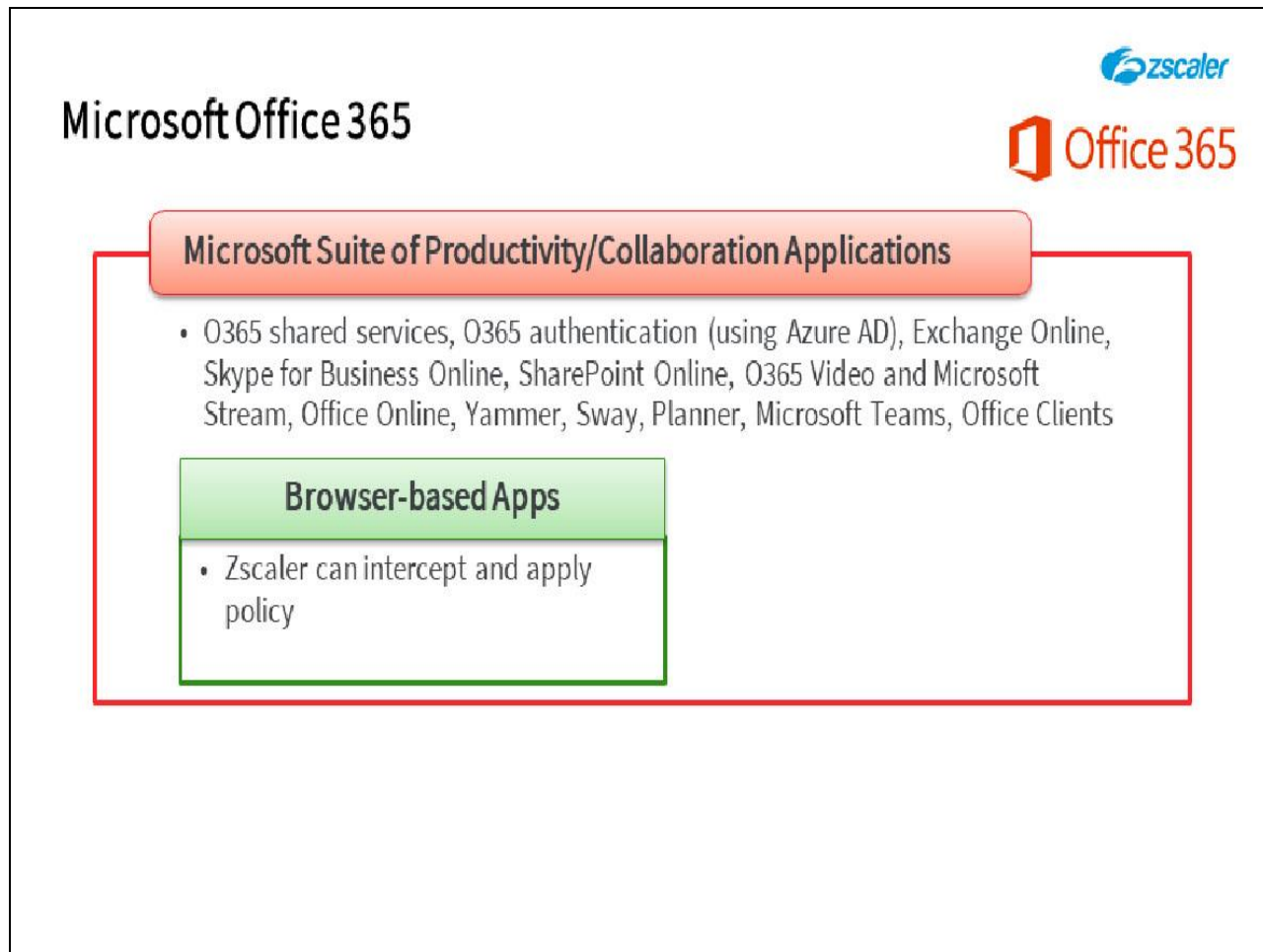
- O365 shared services, O365 authentication (using Azure AD), Exchange Online, Skype for Business Online, SharePoint Online, O365 Video and Microsoft Stream, Office Online, Yammer, Sway, Planner, Microsoft Teams, Office Clients

**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.

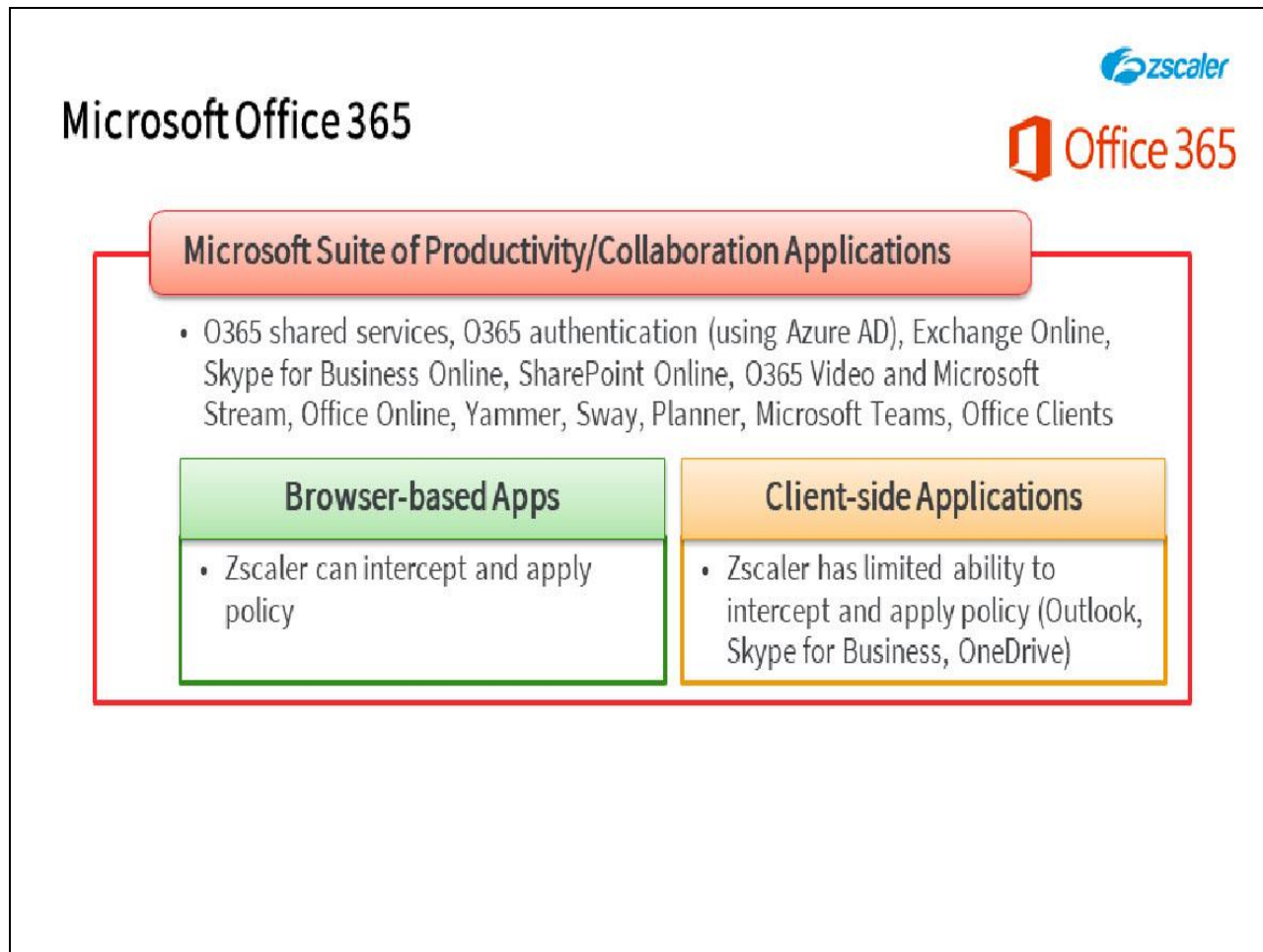
## Slide 6 - Microsoft Office 365



## 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

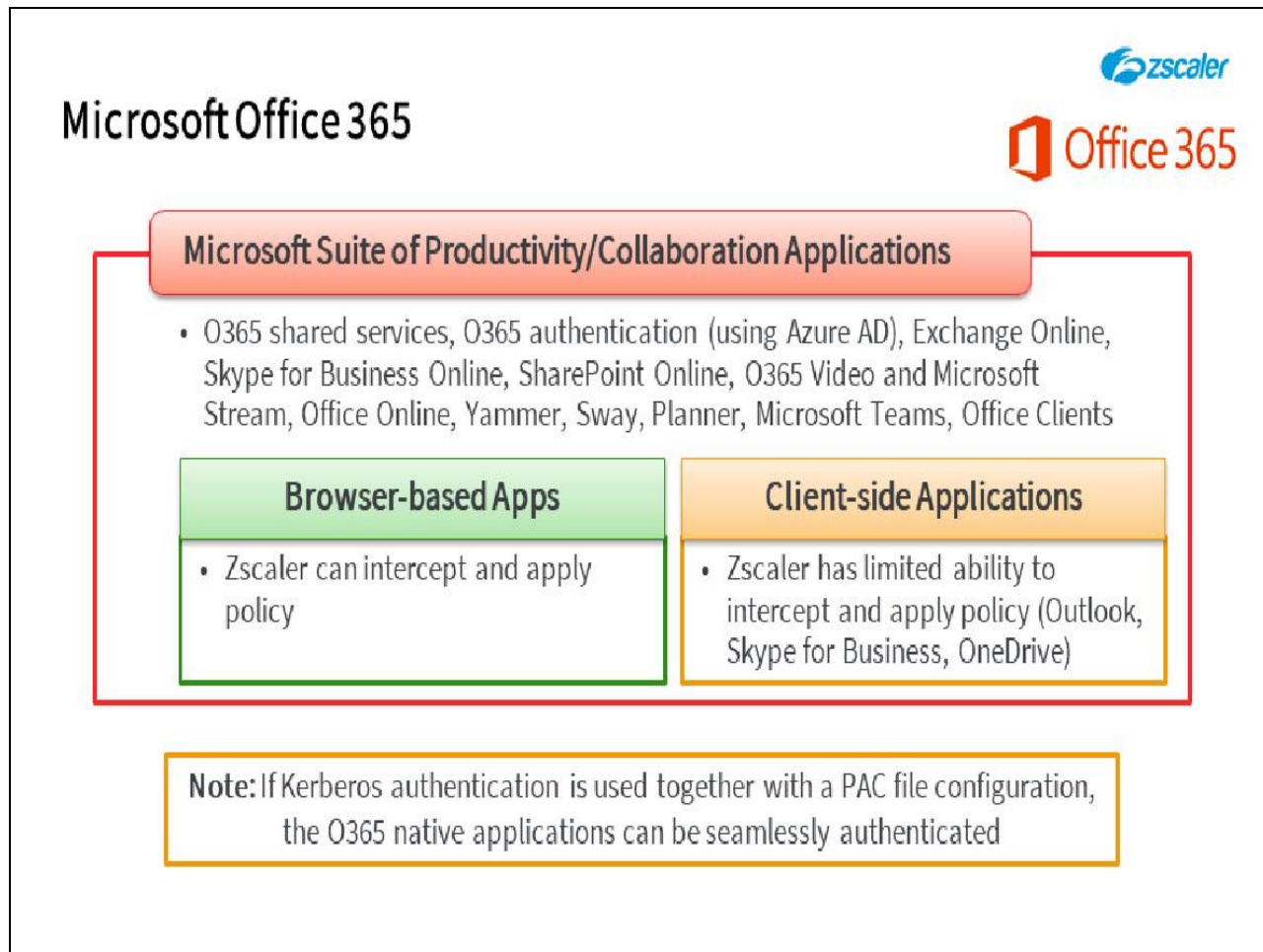


## Slide notes

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

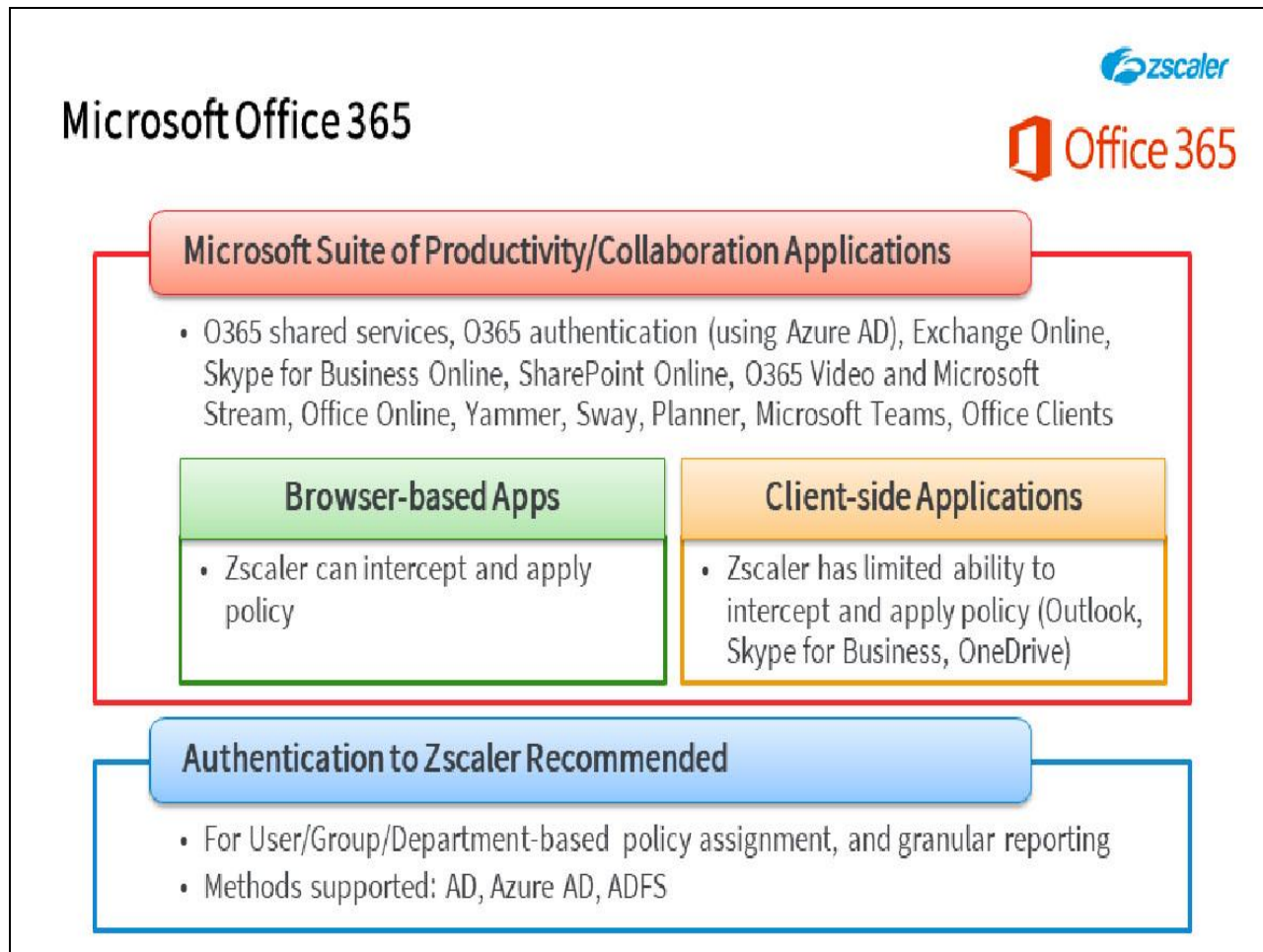


## Slide notes

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.



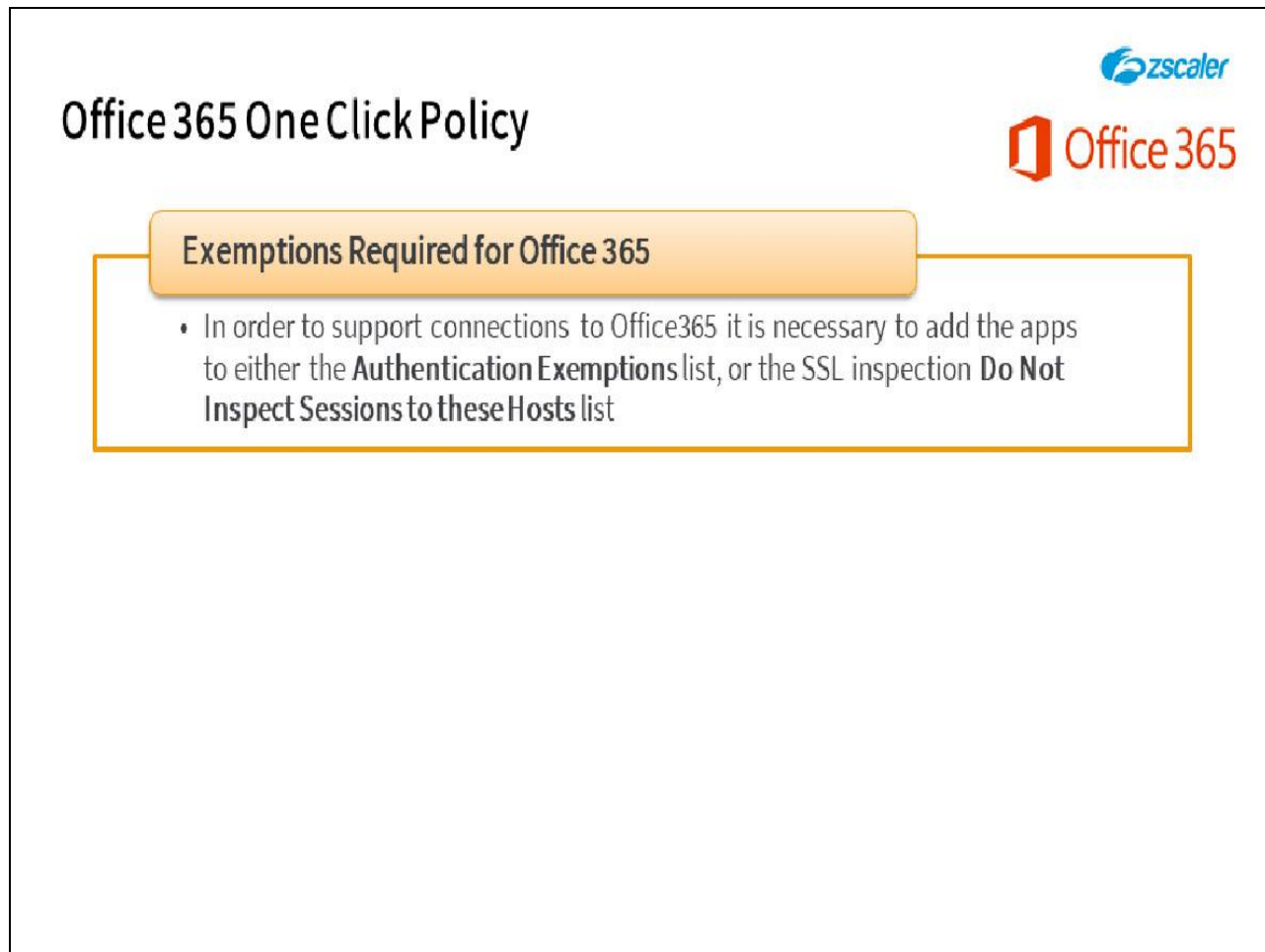
## Slide 9 - Microsoft Office 365



## 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



The slide features a white background with a black border. In the top right corner, there are two logos: the Zscaler logo (a blue circle with a white 'Z' and the word 'zscaler' in blue) and the Office 365 logo (a red square with a white 'O' and the text 'Office 365' in red). The main title 'Office 365 One Click Policy' is positioned in the upper left in a large, bold, black font. Below the title, there is a yellow rectangular box with a black border. Inside this box, the text 'Exemptions Required for Office 365' is written in a bold, black font. Below this text, there is a bulleted list with one item: 'In order to support connections to Office365 it is necessary to add the apps to either the **Authentication Exemptions** list, or the SSL inspection **Do Not Inspect Sessions to these Hosts** list'. The text in the list is in a standard black font.

## Office 365 One Click Policy

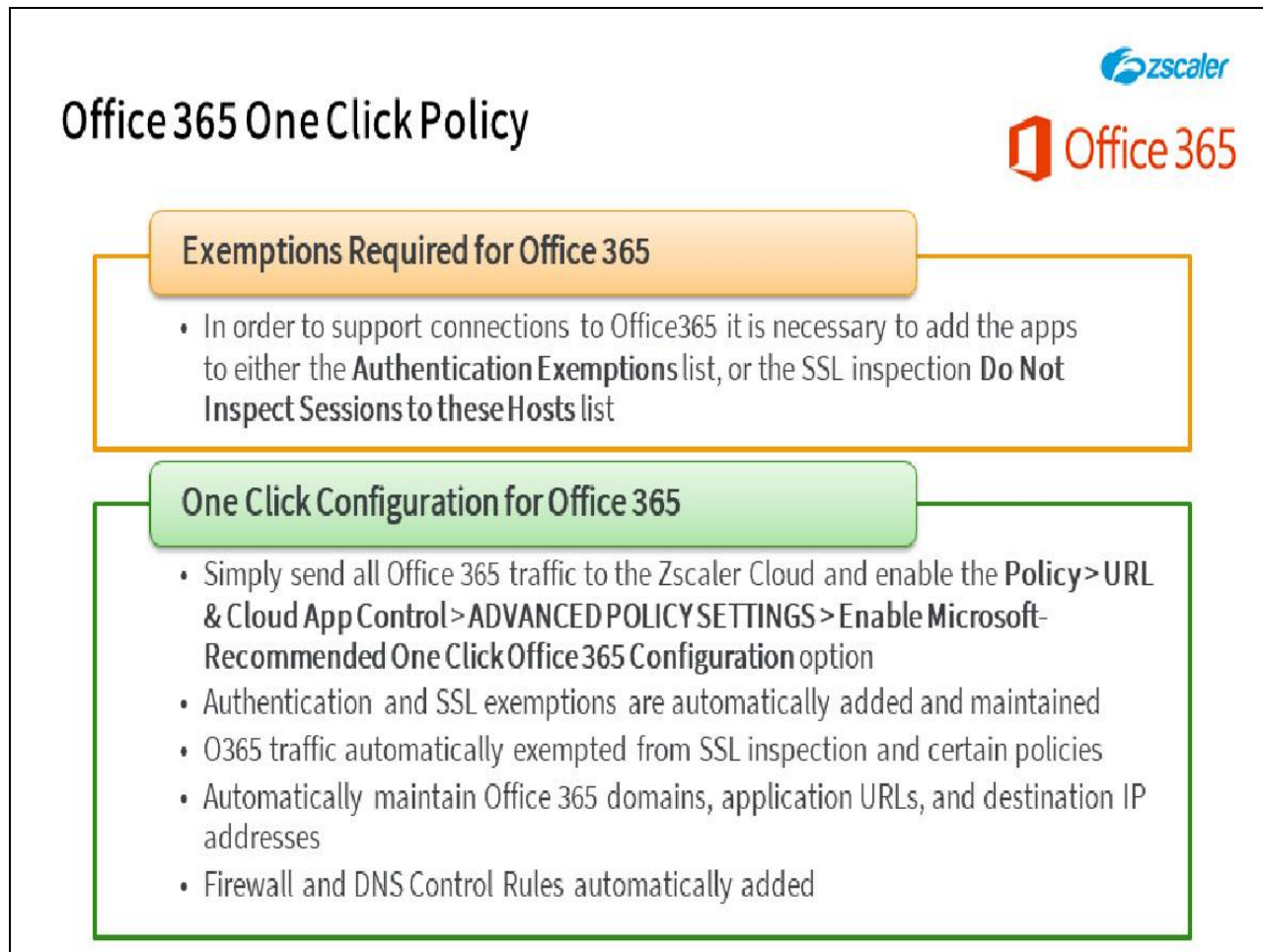
**Exemptions Required for Office 365**

- In order to support connections to Office365 it is necessary to add the apps to either the **Authentication Exemptions** list, or the SSL inspection **Do Not Inspect Sessions to these Hosts** list

## 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



The slide is titled "Office 365 One Click Policy" and features the Zscaler and Office 365 logos in the top right corner. It contains two main sections: "Exemptions Required for Office 365" and "One Click Configuration for Office 365".

### Office 365 One Click Policy

**Exemptions Required for Office 365**

- In order to support connections to Office365 it is necessary to add the apps to either the **Authentication Exemptions** list, or the SSL inspection **Do Not Inspect Sessions to these Hosts** list

**One Click Configuration for Office 365**

- Simply send all Office 365 traffic to the Zscaler Cloud and enable the **Policy > URL & Cloud App Control > ADVANCED POLICY SETTINGS > Enable Microsoft-Recommended One Click Office 365 Configuration** option
- Authentication and SSL exemptions are automatically added and maintained
- O365 traffic automatically exempted from SSL inspection and certain policies
- Automatically maintain Office 365 domains, application URLs, and destination IP addresses
- Firewall and DNS Control Rules automatically added

## 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.

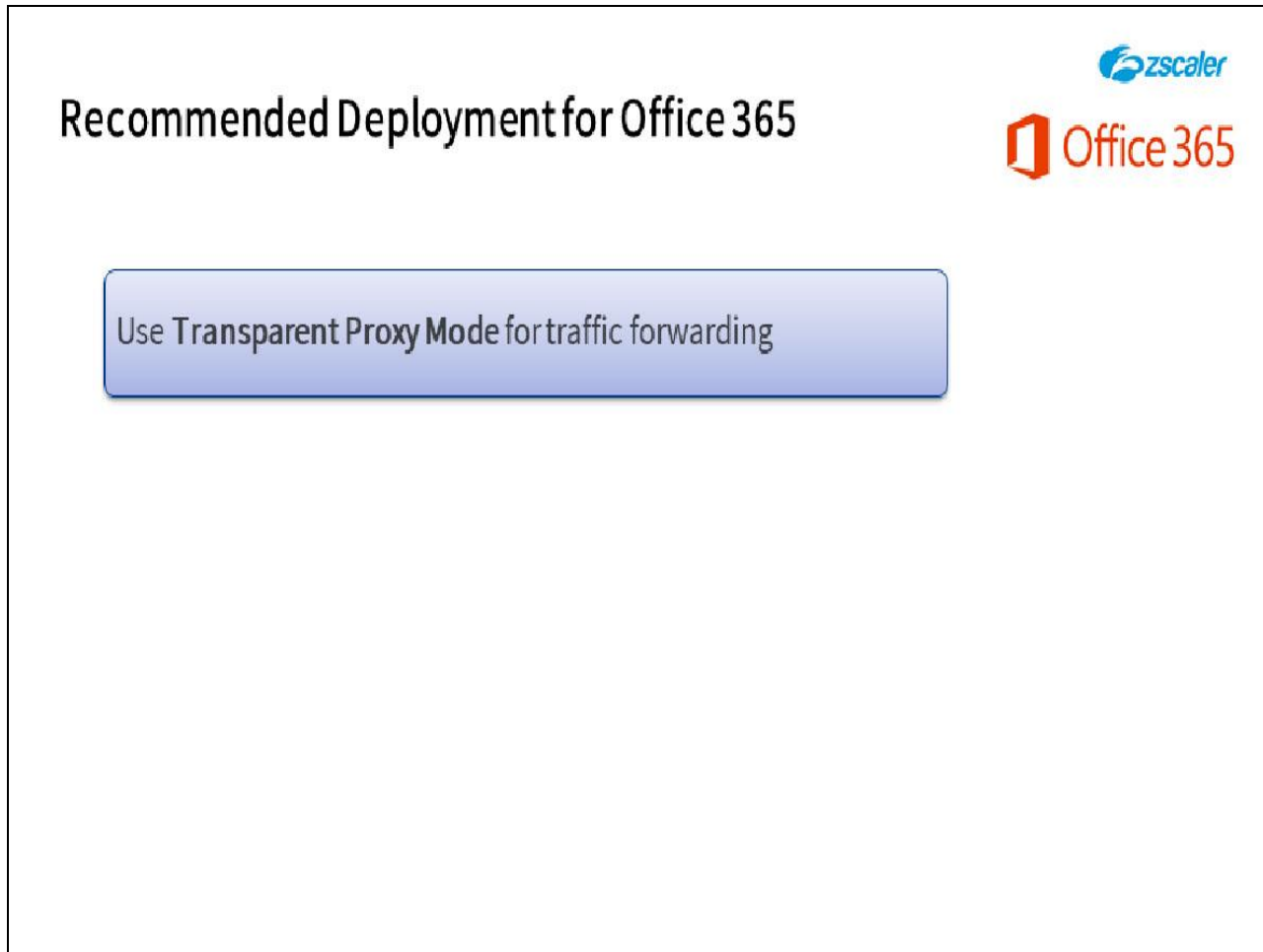
With the Office 365 One Click Configuration enabled, Zscaler automatically configures the **Do Not Inspect Sessions to these Hosts** list, and the **Authentication Exemptions** rules required for the service to seamlessly support and secure your Office 365 traffic. In addition:

- 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



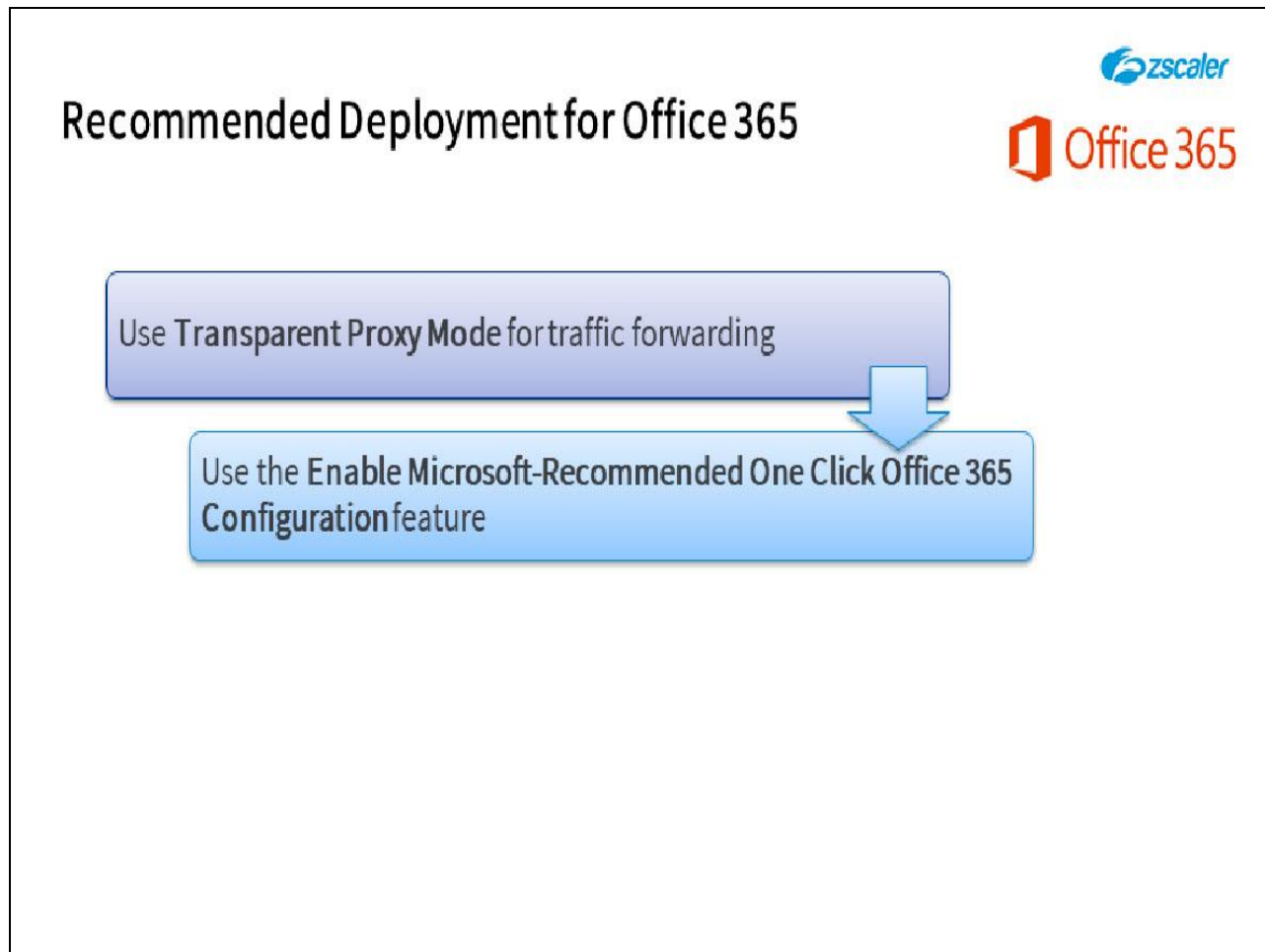
The slide content is enclosed in a black rectangular border. At the top left, the text "Recommended Deployment for Office 365" is displayed in a large, black, sans-serif font. To the right of this text, the Zscaler logo (a blue circle with a white 'Z' and the word "zscaler" in blue) is positioned above the Office 365 logo (an orange square with a white 'O' and the text "Office 365" in orange). Below the title and logos, a light blue rounded rectangular button with a subtle gradient and a thin black border contains the text "Use Transparent Proxy Mode for traffic forwarding" in a black, sans-serif font.

**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.

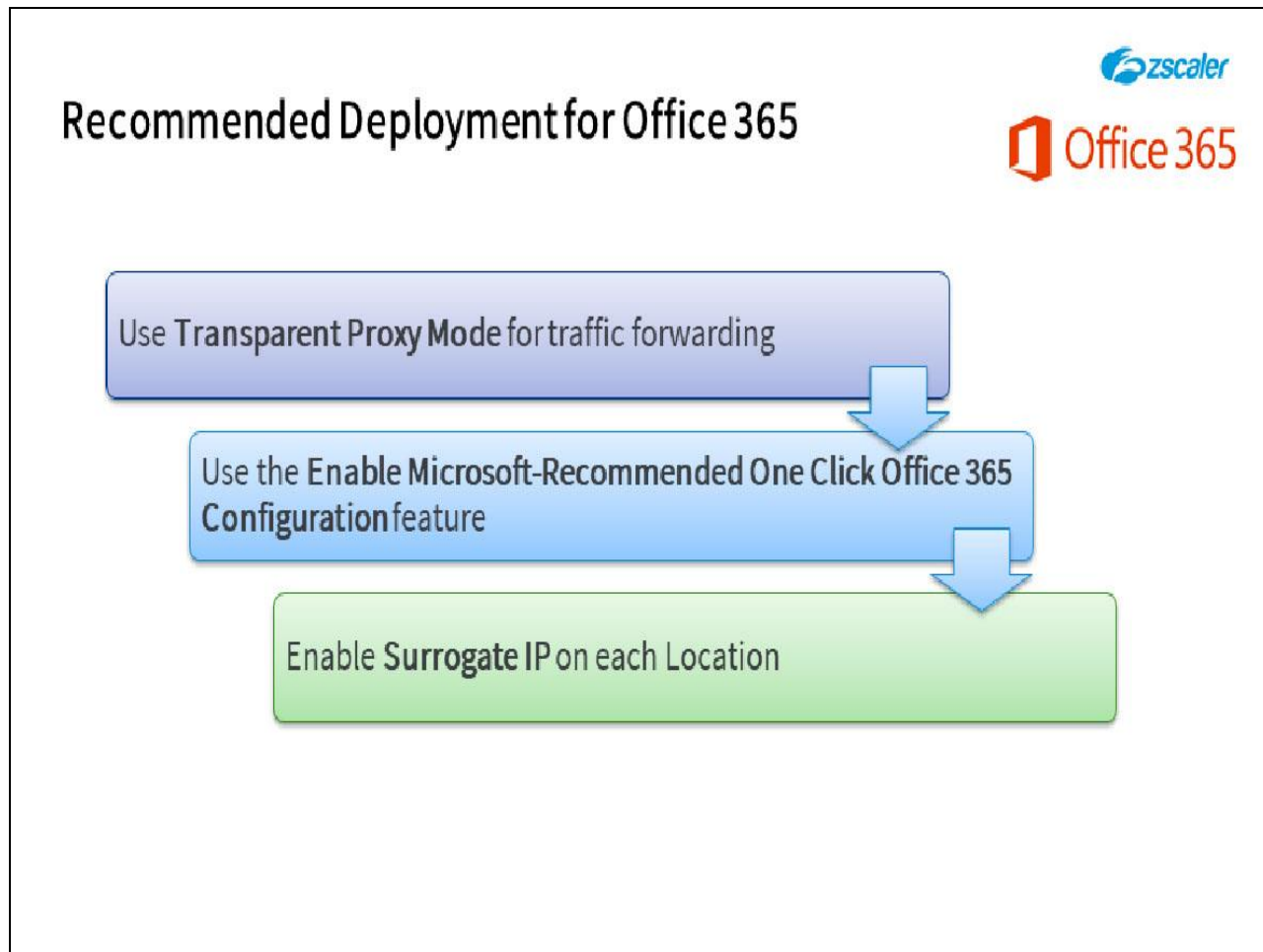
## Slide 13 - Recommended Deployment for Office 365



## 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.

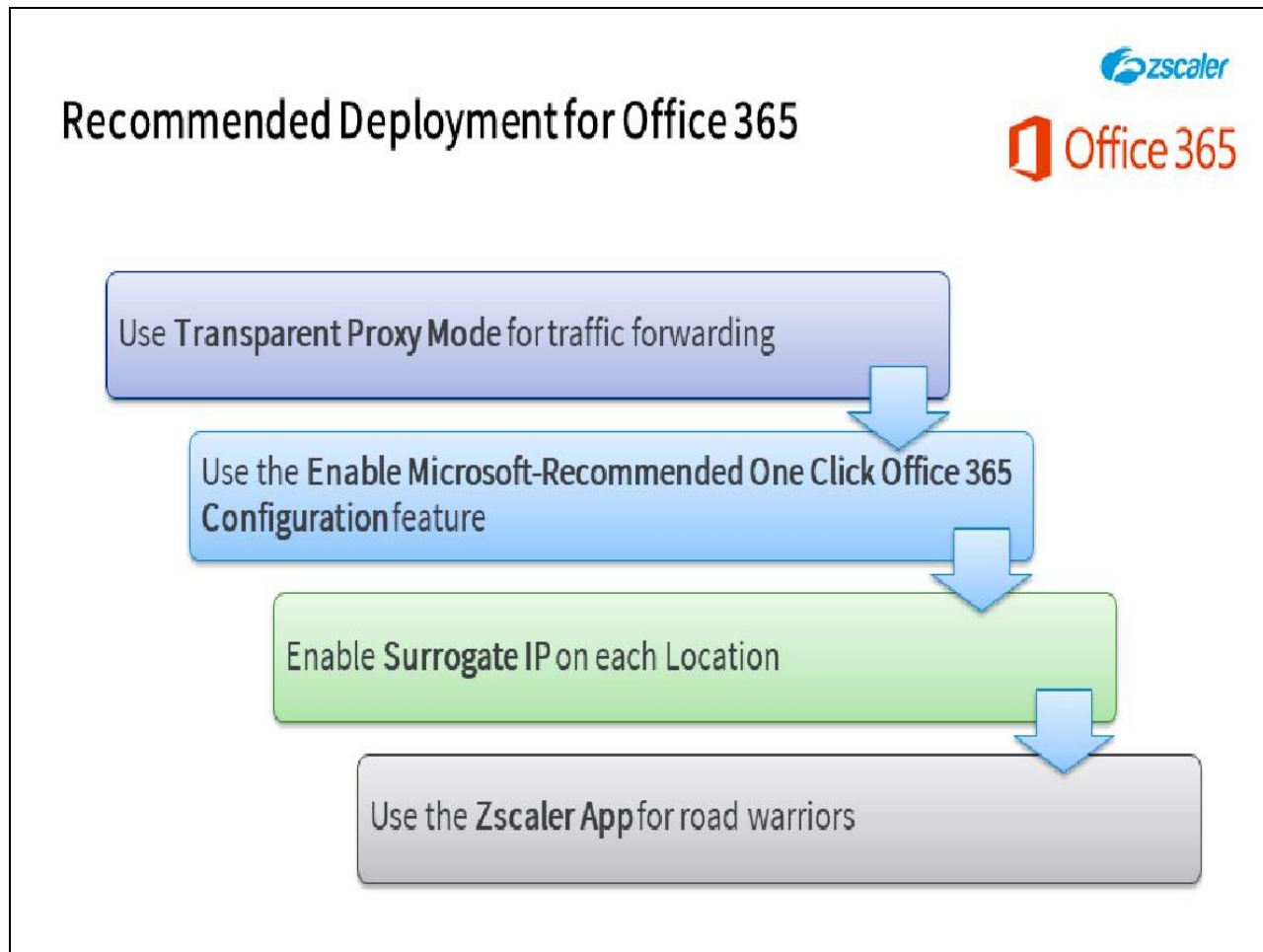
## Slide 14 - Recommended Deployment for Office 365



## 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.

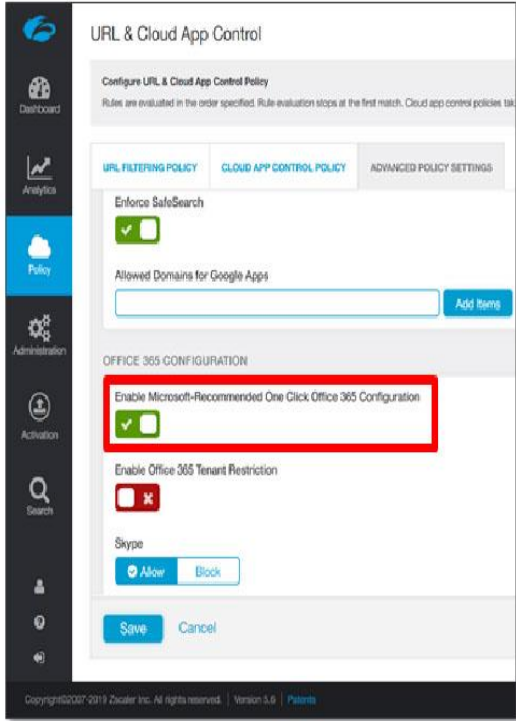
It simplifies configuration because if the App is installed, then the use of a dedicated port, Kerberos authentication, or Surrogate IP are no longer requirements for your road warriors. In addition, because the Zscaler App supports both Browser and non-Browser traffic, it solves proxy-interoperability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



## Slide 16 - Enabling Office 365 One Click Configuration

## Enabling Office 365 One Click Configuration

- Use the **Enable Microsoft-Recommended One Click Office 365 Configuration** option for Office 365 from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab



## 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

## Enabling Office 365 One Click Configuration

- Use the **Enable Microsoft-Recommended One Click Office 365 Configuration** option for Office 365 from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab

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

The screenshot shows the Zscaler management console interface for 'URL & Cloud App Control'. The left sidebar contains navigation links for Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main content area is titled 'URL & Cloud App Control' and includes a sub-header 'Configure URL & Cloud App Control Policy'. Below this, there are three tabs: 'URL FILTERING POLICY', 'CLOUD APP CONTROL POLICY', and 'ADVANCED POLICY SETTINGS'. The 'ADVANCED POLICY SETTINGS' tab is active. Under the 'OFFICE 365 CONFIGURATION' section, the 'Enable Microsoft-Recommended One Click Office 365 Configuration' option is checked with a green checkmark and is highlighted by a red rectangular box. Other settings include 'Enforce SafeSearch' (checked), 'Allowed Domains for Google Apps' (with an 'Add Items' button), 'Enable Office 365 Tenant Restriction' (unchecked), and 'Skype' (set to 'Allow'). At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The footer of the console displays 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Privacy'.



## Slide notes

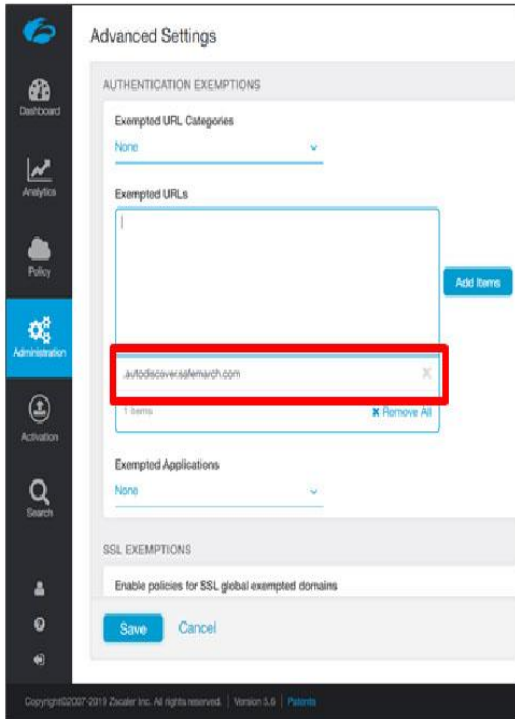
Note that enabling the **One Click** option is normally the only configuration change you need to make to ensure optimum performance for your Office 365 users!

## Slide 18 - Enabling Office 365 One Click Configuration

## Enabling Office 365 One Click Configuration

- Use the **Enable Microsoft-Recommended One Click Office 365 Configuration** option for Office 365 from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab
- If necessary, also add the domain **.autodiscover.[domainname].com** to the **Authentication Exemptions URLs** list on the **Administration > Advanced Settings** page





## Slide notes

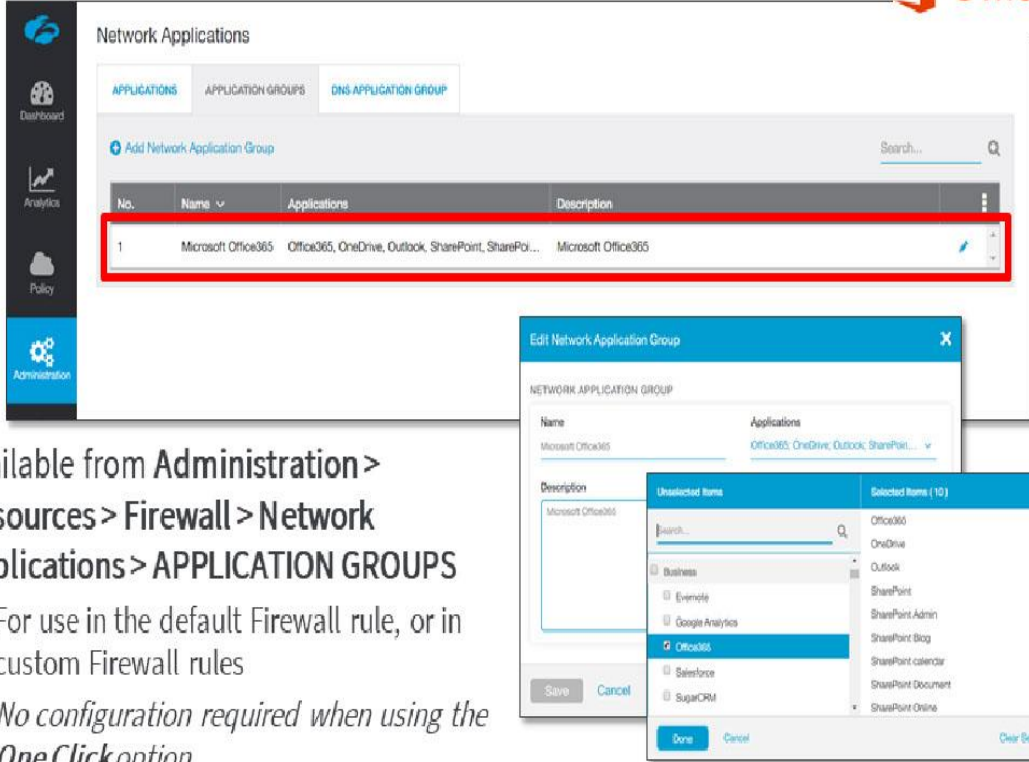
One item that Zscaler cannot configure automatically when the Office 365 **One Click** feature is enabled, is your custom Domain auto-discovery URL in the authentication exemption list. Depending on your business requirements, you may need to manually add the URL: **.autodiscover.[domainname].com** to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

## Office 365 Network Application Group



**Network Applications**

APPLICATIONS APPLICATION GROUPS DNS APPLICATION GROUP

Add Network Application Group

No.	Name	Applications	Description
1	Microsoft Office365	Office365, OneDrive, Outlook, SharePoint, SharePoi...	Microsoft Office365

**Edit Network Application Group**

NAME APPLICATION GROUP

Name: Microsoft Office365 Applications: Office365, OneDrive, Outlook, SharePoi...

Description: Microsoft Office365

**Unselected Items**

- Business
- Evernote
- Google Analytics
- Office365**
- Salesforce
- SugarCRM

**Selected Items (10)**

- Office365
- OneDrive
- Outlook
- SharePoint
- SharePoint Admin
- SharePoint Blog
- SharePoint calendar
- SharePoint Document
- SharePoint Online

- Available from Administration > Resources > Firewall > Network Applications > APPLICATION GROUPS
  - For use in the default Firewall rule, or in custom Firewall rules
  - *No configuration required when using the One Click option*



## Slide notes

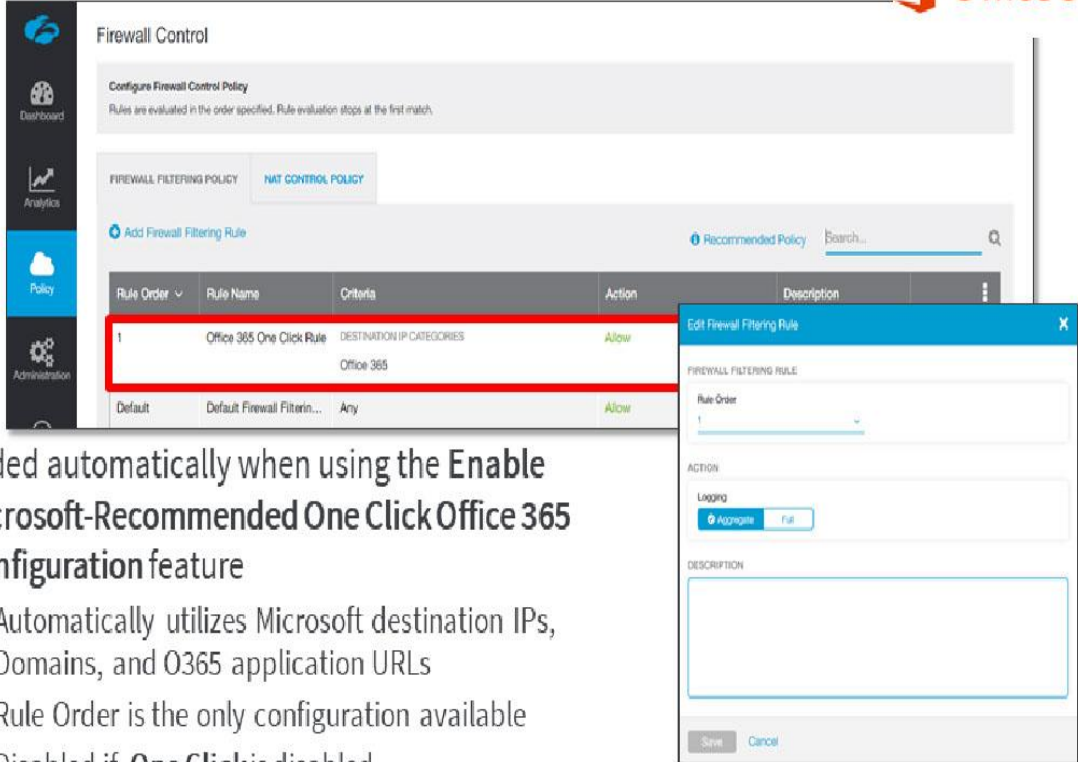
We also maintain a list of Office 365 applications in an **Application Group** that is used in the default Firewall rule when the **One Click** setting is enabled. Again, there is nothing here that you normally need to configure, although this group is available for you to use in any custom Firewall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

## Automatic One Click Firewall Rule



**Firewall Control**

Configure Firewall Control Policy  
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

FIREWALL FILTERING POLICY NAT CONTROL POLICY

+ Add Firewall Filtering Rule Recommended Policy Search...

Rule Order	Rule Name	Criteria	Action	Description
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow	
Default	Default Firewall Filterin...	Any	Allow	

**Edit Firewall Filtering Rule**

FIREWALL FILTERING RULE

Rule Order: 1

ACTION

Logging: ☒ Aggregate ☐ Full

DESCRIPTION

Save Cancel



- Added automatically when using the **Enable Microsoft-Recommended One Click Office 365 Configuration** feature
  - Automatically utilizes Microsoft destination IPs, Domains, and O365 application URLs
  - Rule Order is the only configuration available
  - Disabled if **One Click** is disabled

## Slide notes

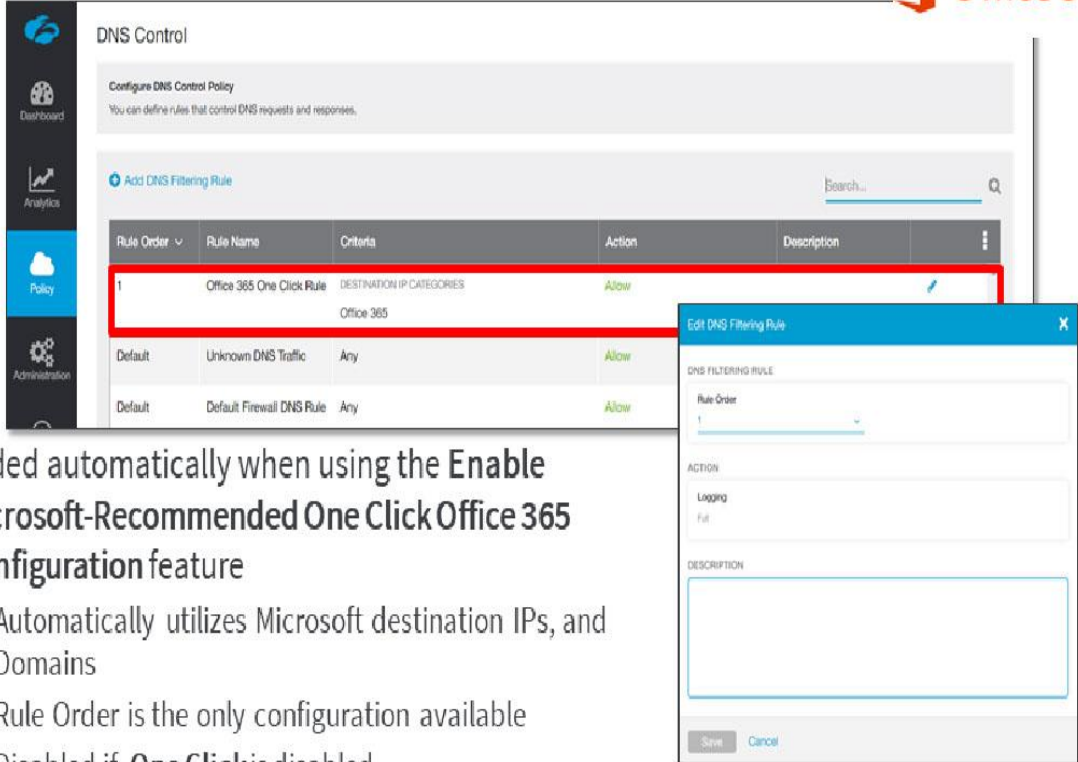
When the Microsoft Office **One Click** setting is enabled, we automatically add a Firewall rule that targets and allows the **Application Group** mentioned in the previous slide. It is added at rule 1 and is not configurable, nor can you delete it, although the rule order can be changed if necessary. 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

## Automatic One Click DNS Control Rule



**DNS Control**

Configure DNS Control Policy  
You can define rules that control DNS requests and responses.

[Add DNS Filtering Rule](#)

Rule Order	Rule Name	Criteria	Action	Description
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow	
Default	Unknown DNS Traffic	Any	Allow	
Default	Default Firewall DNS Rule	Any	Allow	

**Edit DNS Filtering Rule**

DNS FILTERING RULE

Rule Order: 1

ACTION: Logging: Full

DESCRIPTION:

Save Cancel

- Added automatically when using the **Enable Microsoft-Recommended One Click Office 365 Configuration** feature
  - Automatically utilizes Microsoft destination IPs, and Domains
  - Rule Order is the only configuration available
  - Disabled if **One Click** is disabled

## 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.

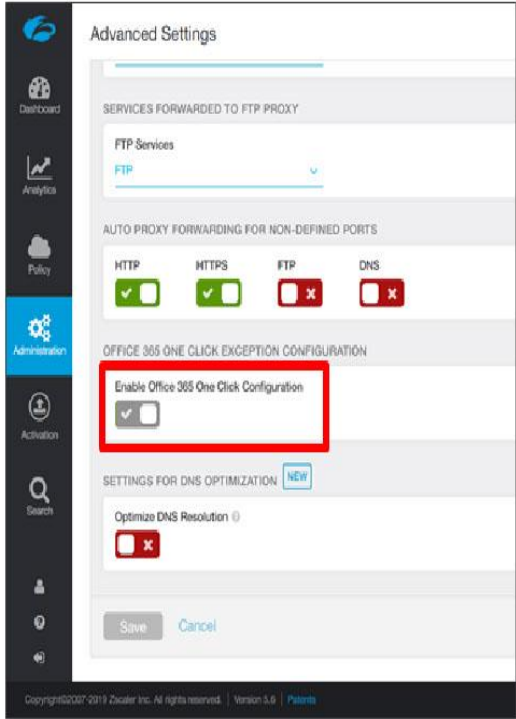
Also, as with the Firewall rule, if the Office 365 **One Click** setting is subsequently disabled, this rule will be set to the **Disabled** state, but will still appear in the DNS Control rules list.



## Slide 22 - Original One Click Configuration Option

## Original One Click Configuration Option

- The original One Click configuration option is deprecated
- It is still available under **Administration > Advanced Settings**
  - If you previously enabled this, it will be set to **Enabled** on Cloud v5.5 upgrade
  - If you then enable the new One Click option, the old option will be greyed out



## 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.

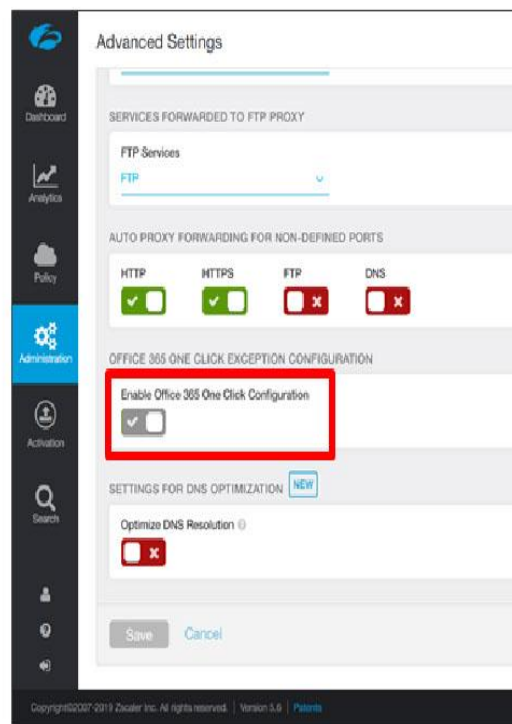
## Slide 23 - Original One Click Configuration Option

## Original One Click Configuration Option



- The original One Click configuration option is deprecated
- It is still available under **Administration** > **Advanced Settings**
  - If you previously enabled this, it will be set to **Enabled** on Cloud v5.5 upgrade
  - If you then enable the new One Click option, the old option will be greyed out

**Note:** The new **Enable Microsoft-Recommended One Click Office 365 Configuration** option (described in the preceding slides) is strongly recommended as it is a far more robust implementation



### Slide notes

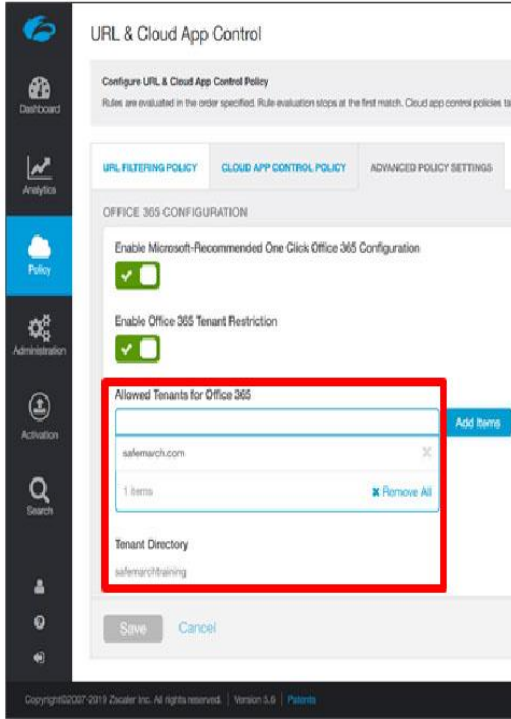
Note that, if you have previously enabled the **One Click** setting for Office 365, we strongly recommend that you transition to use the **new** implementation of it, as it is a far more capable and robust solution.



## Slide 24 - Other Office 365 Options – Tenant Restrictions

## Other Office 365 Options – Tenant Restrictions

- Add one or more **Allowed Tenants** for Office 365 configuration if required from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab



## 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

## Other Office 365 Options – Tenant Restrictions

- Add one or more **Allowed Tenants** for Office 365 configuration if required from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab

**Note:** This option enables SSL Inspection for specific Microsoft Domains, be sure your users have the correct Root CA Certificate

The screenshot shows the Zscaler management console interface for 'URL & Cloud App Control'. The 'ADVANCED POLICY SETTINGS' tab is selected. Under 'OFFICE 365 CONFIGURATION', two options are checked: 'Enable Microsoft-Recommended One Click Office 365 Configuration' and 'Enable Office 365 Tenant Restriction'. Below these, the 'Allowed Tenants for Office 365' section shows a list with 'safemarch.com'. To the right of this list is a red-bordered box containing the 'Add Items' button. Below the list, there is a 'Remove All' link. The 'Tenant Directory' section shows 'safemarchtraining'. At the bottom, there are 'Save' and 'Cancel' buttons. The footer indicates 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Privacy'.

## Slide notes

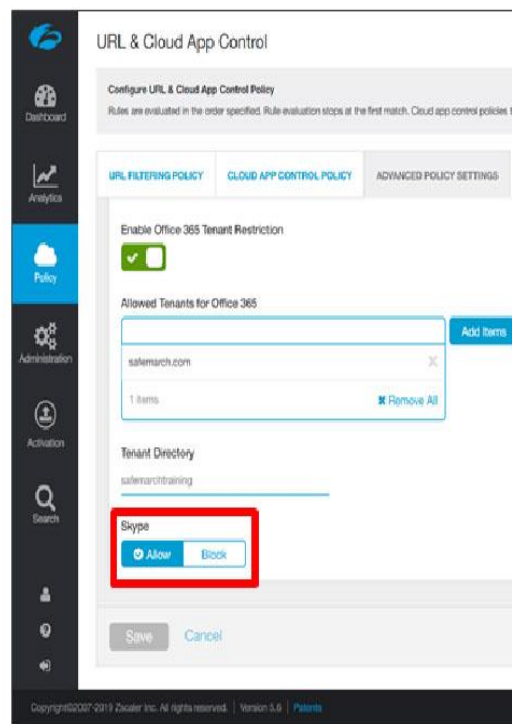
Note that this configuration enables SSL interception for the **login.microsoftonline.com**, **login.microsoft.com**, and **login.windows.net** domains, so be sure that the appropriate root CA certificate for SSL Inspection is installed on your client PCs before enabling this option.

## Slide 26 - Other Office 365 Options – Skype Configuration

## Other Office 365 Options – Skype Configuration



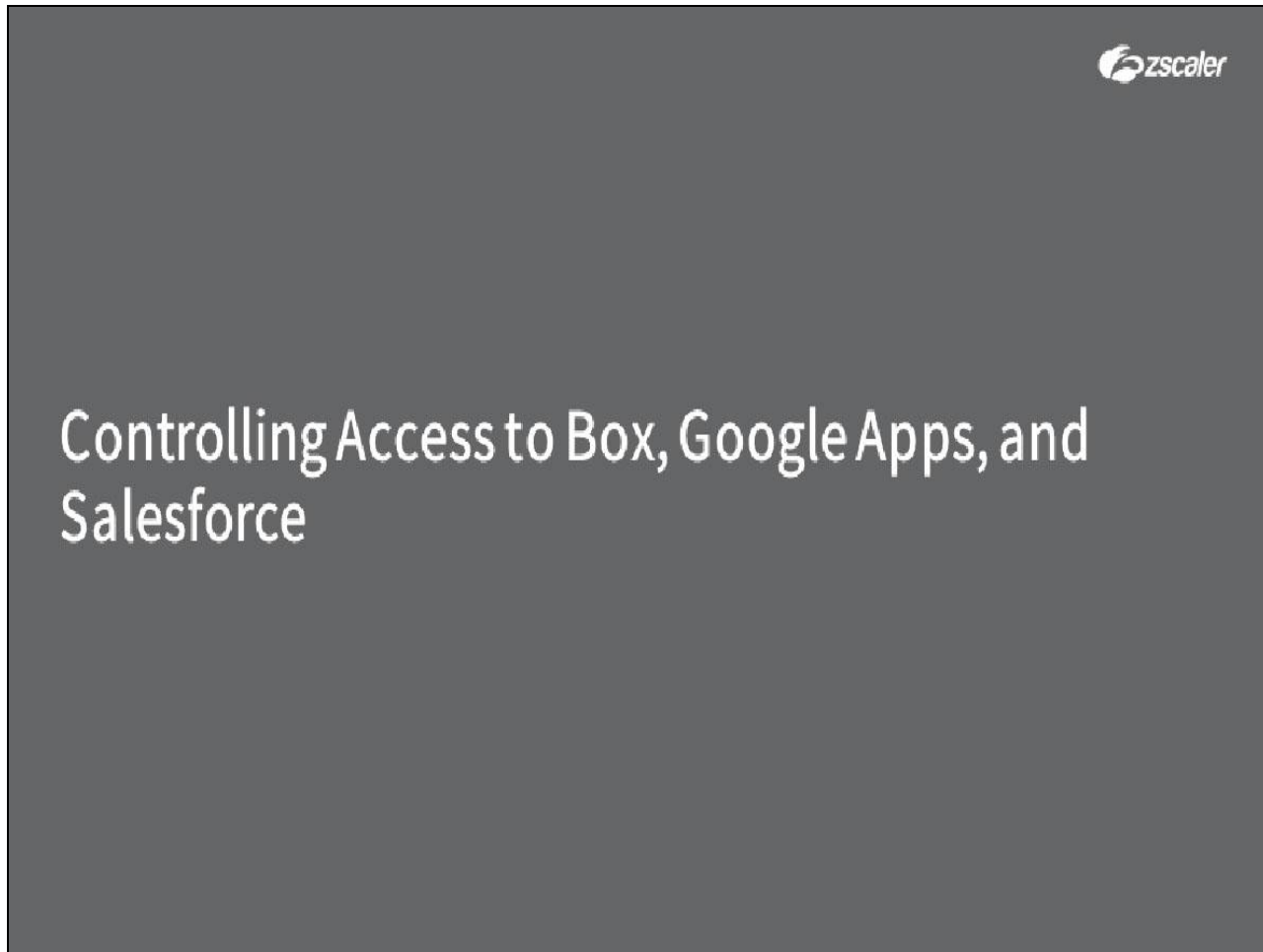
- Add one or more **Allowed Tenants** for Office 365 configuration if required from the **Policy > URL & Cloud App Control** page, on the **ADVANCED POLICY SETTINGS** tab
- Enable or disable **Skype** as necessary



## 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



## Zscaler as an Identity Proxy


Goal
------

## 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



## Zscaler as an Identity Proxy


Goal	Method
<ul style="list-style-type: none"><li>• Use Zscaler to control access to your Cloud application suite</li><li>• Permit no direct access to the Corporate accounts, users MUST access them through Zscaler</li><li>• Supported Cloud suites:<ul style="list-style-type: none"><li>◦ Box</li><li>◦ Google Apps</li><li>◦ Salesforce</li></ul></li><li>• To use a personal account an explicit logout is required</li></ul>	<ul style="list-style-type: none"><li>• Use Zscaler as a SAML IdP for your Cloud suite</li></ul> <ol style="list-style-type: none"><li>1. Configure Box, Google Apps, or Salesforce to use Zscaler as the IdP</li><li>2. Enable and configure Zscaler to act as a SAML IdP</li><li>3. User authenticates to Zscaler</li><li>4. When accessing the applications with SSO, Zscaler authentication cookie is transformed</li><li>5. User is logged onto the application suite using the Zscaler credentials</li></ol>

## 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



## Zscaler as an Identity Proxy

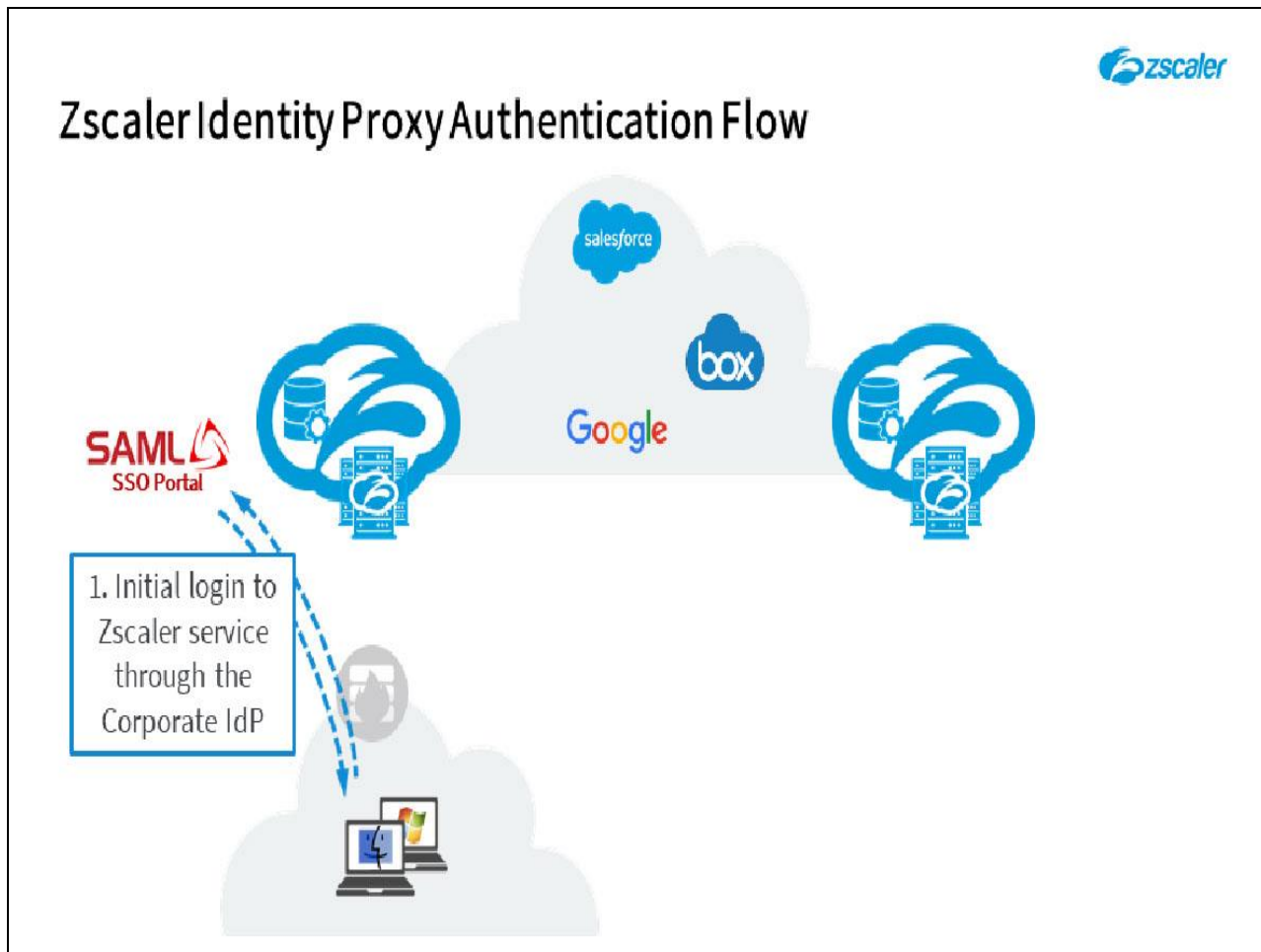
Goal	Method	Prerequisites
<ul style="list-style-type: none"> <li>• Use Zscaler to control access to your Cloud application suite</li> <li>• Permit no direct access to the Corporate accounts, users MUST access them through Zscaler</li> <li>• Supported Cloud suites: <ul style="list-style-type: none"> <li>◦ Box</li> <li>◦ Google Apps</li> <li>◦ Salesforce</li> </ul> </li> <li>• To use a personal account an explicit logout is required</li> </ul>	<ul style="list-style-type: none"> <li>• Use Zscaler as a SAML IdP for your Cloud suite</li> </ul> <ol style="list-style-type: none"> <li>1. Configure Box, Google Apps, or Salesforce to use Zscaler as the IdP</li> <li>2. Enable and configure Zscaler to act as a SAML IdP</li> <li>3. User authenticates to Zscaler</li> <li>4. When accessing the applications with SSO, Zscaler authentication cookie is transformed</li> <li>5. User is logged onto the application suite using the Zscaler credentials</li> </ol>	<ul style="list-style-type: none"> <li>• Traffic forwarding to Zscaler configured</li> <li>• SSL Inspection enabled</li> <li>• User's provisioned on Zscaler</li> <li>• Authentication enabled and configured</li> <li>• Configurations for each Cloud suite <ul style="list-style-type: none"> <li>◦ Box</li> <li>◦ Google Apps</li> <li>◦ Salesforce</li> </ul> </li> </ul>

## 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



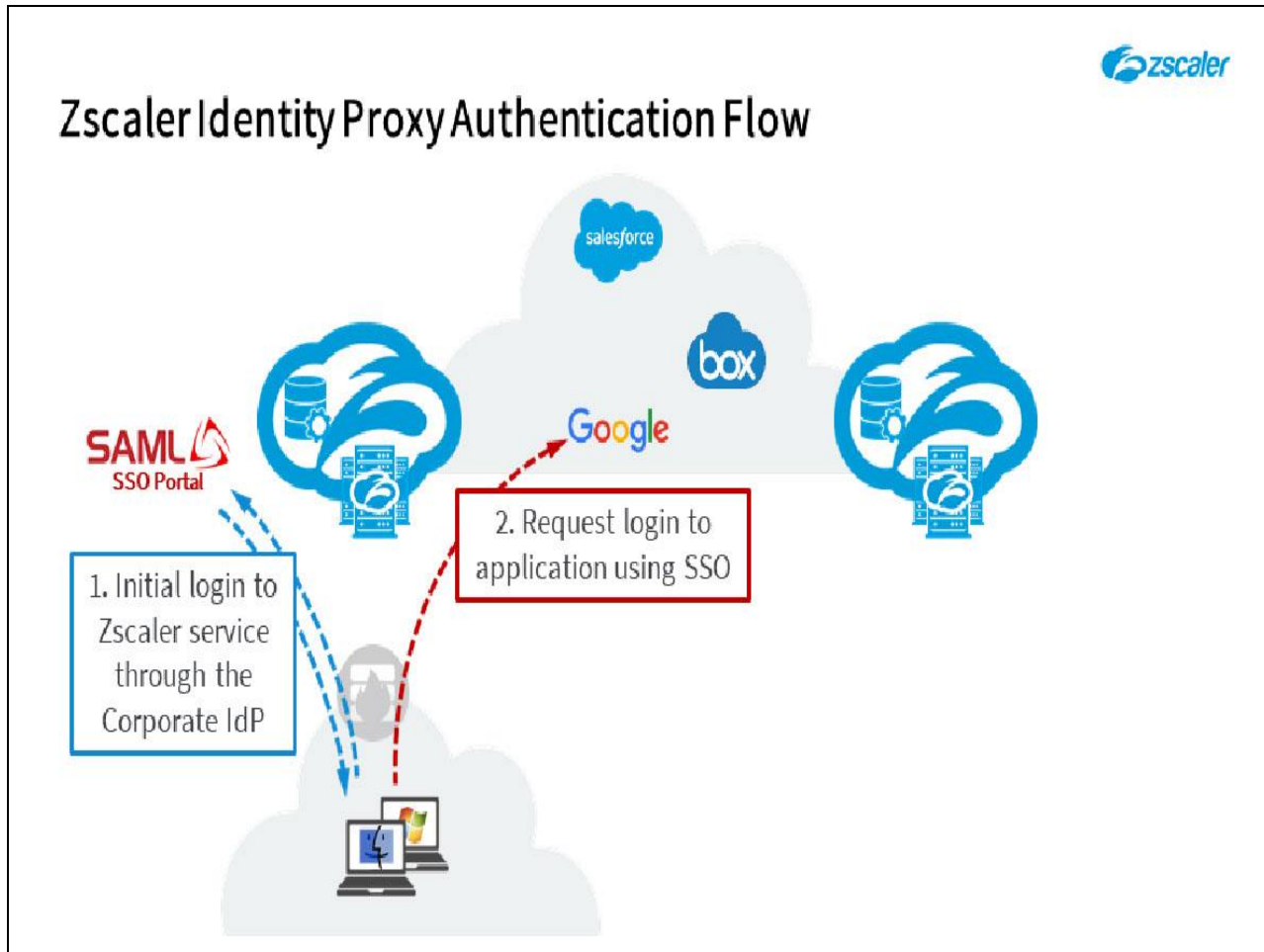
## Slide notes

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.



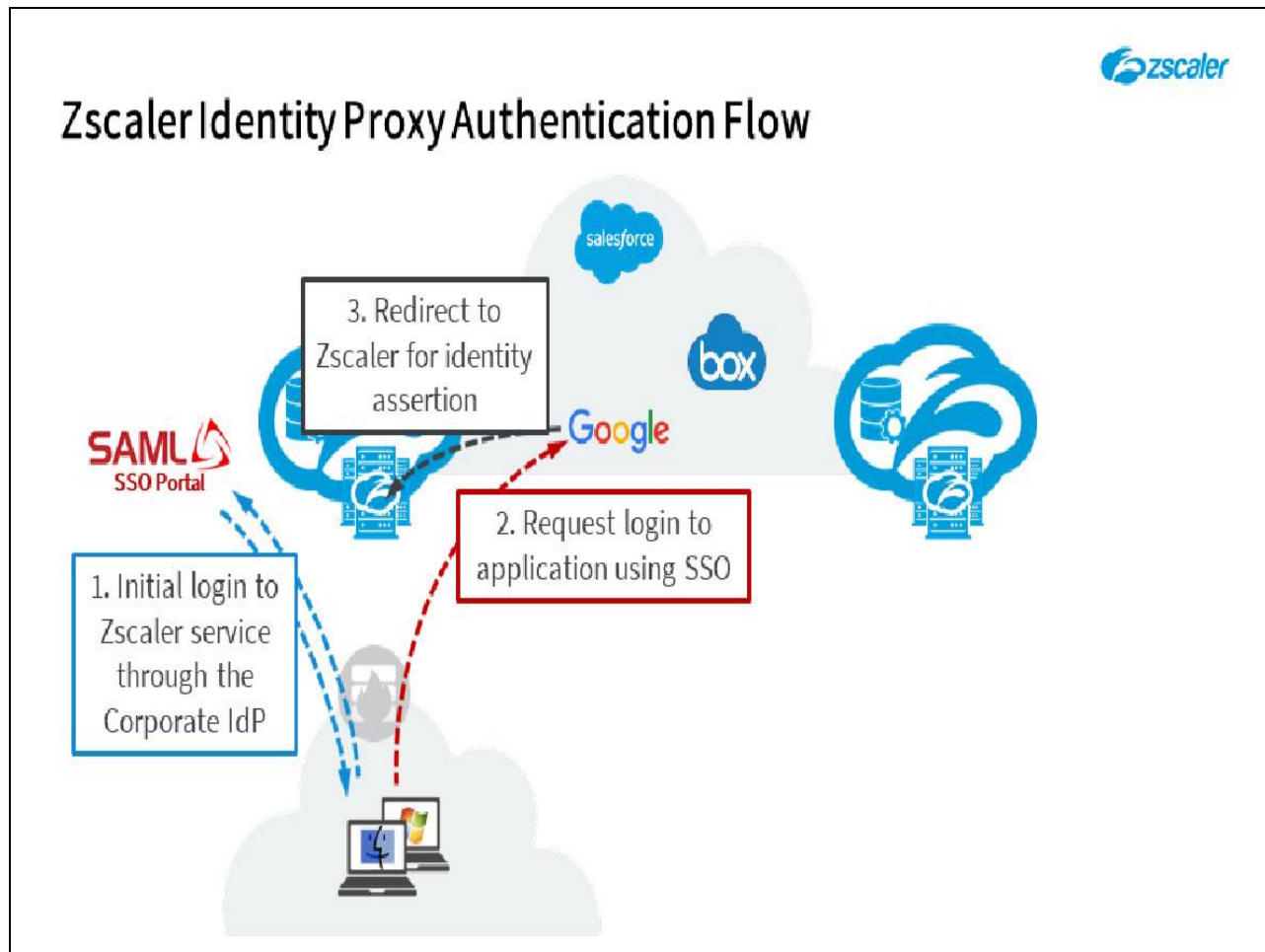
## Slide 32 - Zscaler Identity Proxy Authentication Flow



## Slide notes

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

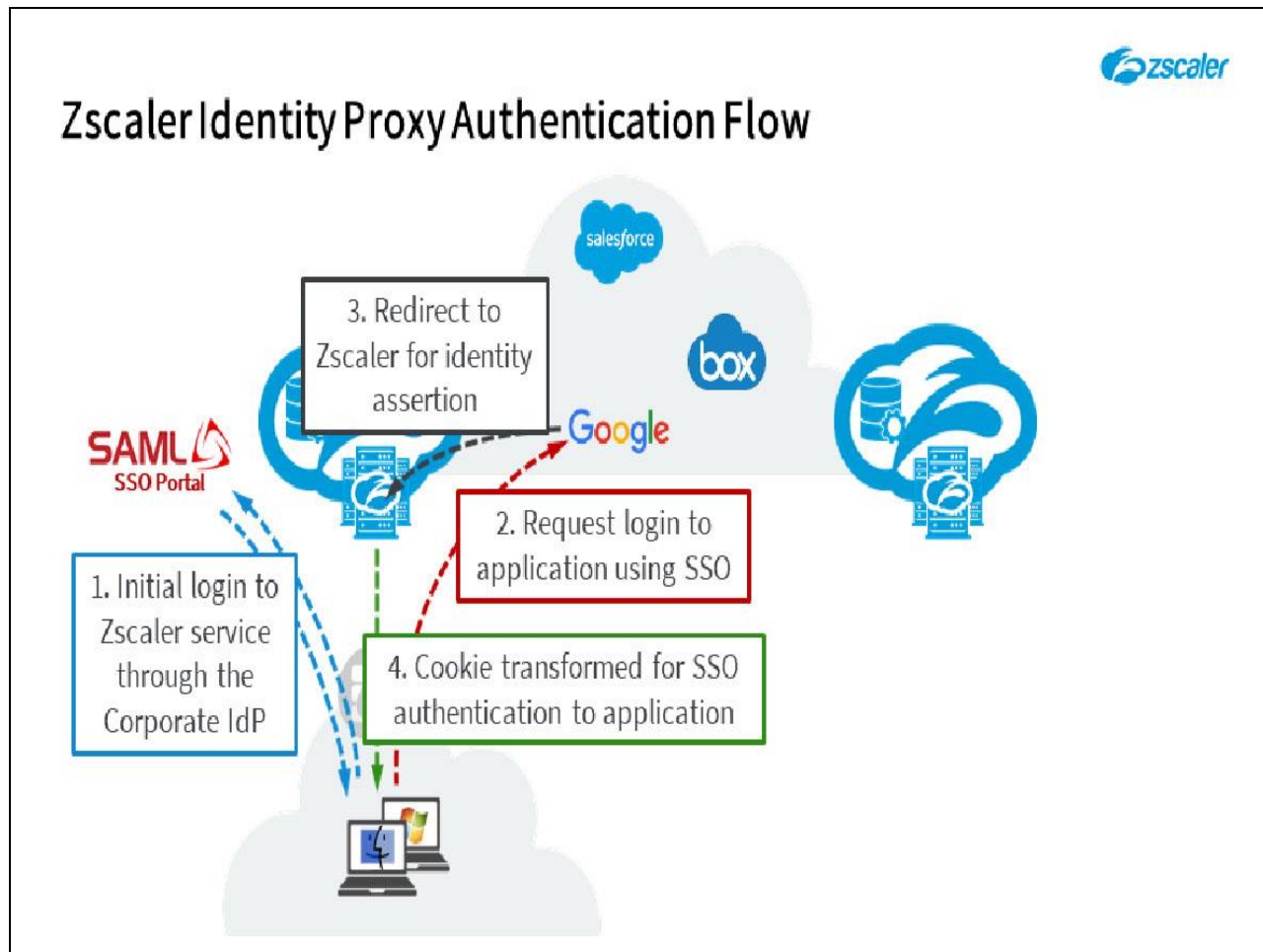
## Slide 33 - Zscaler Identity Proxy Authentication Flow



## Slide notes

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

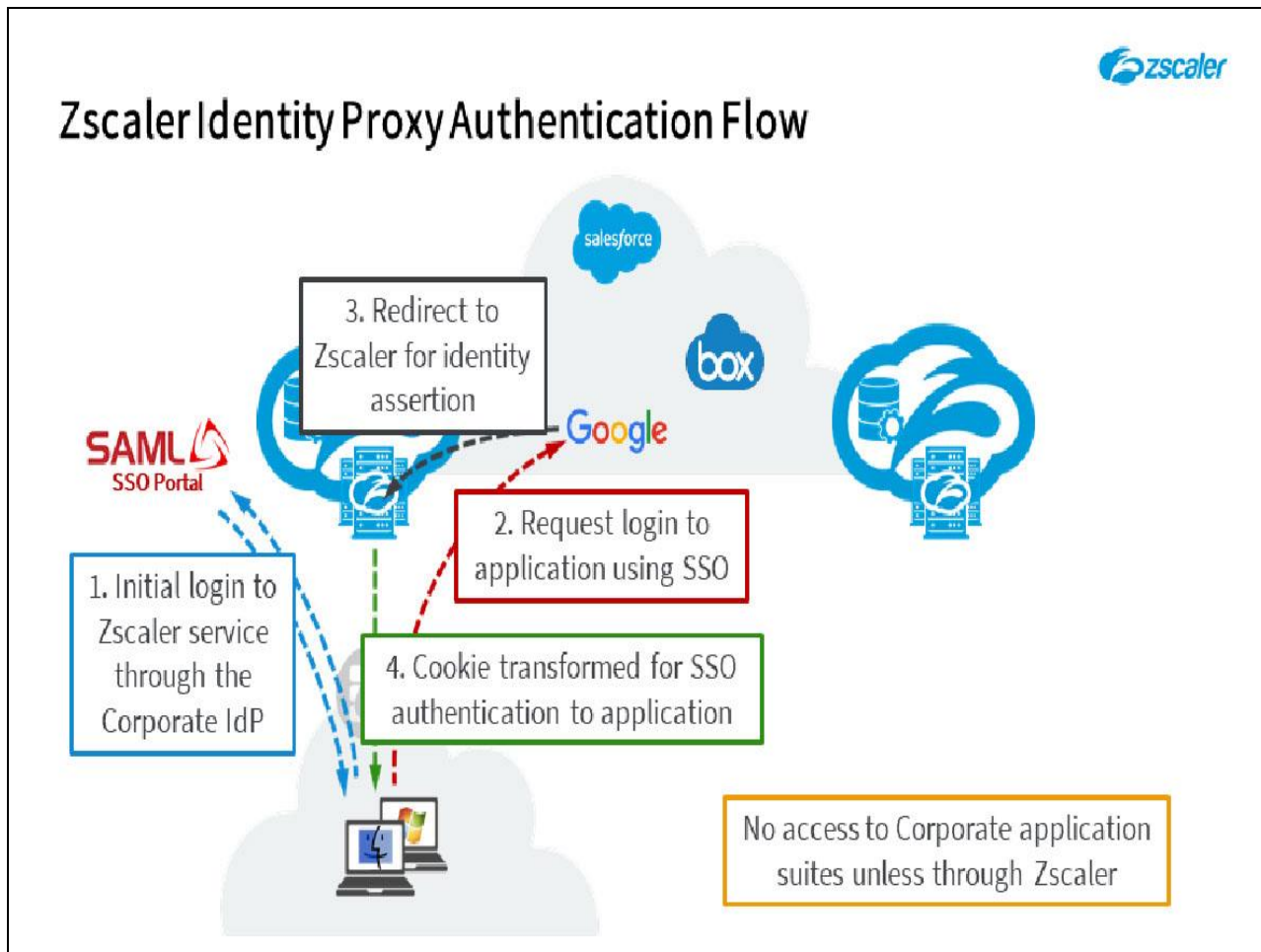
## Slide 34 - Zscaler Identity Proxy Authentication Flow



## 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

**Zscaler Identity Proxy Settings Page**

Identity Proxy settings for Box, Google Apps, Salesforce

No.	Cloud Applications	Settings	Identity Transformation ...	Group	Certific...	
1	Cloud Application Box.net AssertionConsumerService... https://sso.services.box.ne... Enabled false	SAML Version 2.0 Identity Proxy URL https://idp.zscaler.net/s... Issuer Details HxbBcP11TmLw8271TW1... Identity Request Binding HTTP-POST User Identifier NameID	Identity Transformation Pass-through Zscaler Identity	Pass-on Group Details false	Download	
2	Cloud Application Google Apps Enabled false	SAML Version 2.0 Identity Proxy URL https://idp.zscaler.net/s... Issuer Details HxbBcP11TmLw8271TW1... Identity Request Binding HTTP-POST User Identifier NameID	Identity Transformation Pass-through Zscaler		Download	
3	Cloud Application Salesforce	SAML Version 2.0	Identity Transformation Pass-through Zscaler Identity	Pass-on Group Details false	Download	

Identity Proxy URLs

## 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**.

## Zscaler Identity Proxy Settings Page



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

**Zscaler Identity Proxy Settings Page**

The screenshot displays the Zscaler Identity Proxy Settings page. The page title is "Identity Proxy Settings". The main content is a table with columns: No., Cloud Applications, Settings, Identity Transformation ..., Group, and Certificate... (partially visible). The table lists three cloud applications: Box.net, Google Apps, and Salesforce. Each application has a "Download" link in the "Certificate..." column. Annotations include:

- A box labeled "Identity Proxy settings for Box, Google Apps, Salesforce" pointing to the "Settings" column.
- A box labeled "Certificates for download" pointing to the "Download" links in the "Certificate..." column.
- A box labeled "Identity Proxy URLs" pointing to the "Identity Proxy URL" field in the "Settings" column.
- A box labeled "Edit option" pointing to the "Download" link in the "Certificate..." column.

No.	Cloud Applications	Settings	Identity Transformation ...	Group	Certificate...
1	Cloud Application Box.net	SAML Version 2.0 Identity Proxy URL https://idp.zscaler.net/s... Issuer Details HxbBcP11TmLw8271TW1... Identity Request Binding HTTP-POST User Identifier NameID	Identity Transformation Pass-through Zscaler Identity	Pass-on Group Details false	Download
2	Cloud Application Google Apps	SAML Version 2.0 Identity Proxy URL https://idp.zscaler.net/s... Issuer Details HxbBcP11TmLw8271TW1... Identity Request Binding HTTP-POST User Identifier NameID	Identity Transformation Pass-through Zscaler Identity		Download
3	Cloud Application Salesforce	SAML Version 2.0	Identity Transformation Pass-through Zscaler Identity	Pass-on Group Details false	Download

## Slide notes

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



## Slide 39 - Zscaler Identity Proxy Settings

## Zscaler Identity Proxy Settings

- Configure settings for each application suite
  - Enable and Restrict options
  - Domain configuration
  - Assertion URL specification
  - Identity Transformation configuration
  - Group Identifier configuration

**Edit Identity Proxy Settings**

**CLOUD APPLICATION**

Cloud Application	Input your Domain
Box.net	
AssertionConsumerService URL	Enabled
https://sso.services.box.net/sp/ACS.saml2	<input checked="" type="checkbox"/>

**IDENTITY PROXY SETTINGS**

SAML Version	Identity Proxy URL
2.0	https://idp.zscaler-two.net/samlsoa/1amDcP11T...
Issuer Details	Identity Request Binding
HmDcP11TmLwF627TW1XG3TbW4ngT	HTTP-POST
User Identifier	Restrict access to Box.net via Zscaler
NameID	<input checked="" type="checkbox"/>

**IDENTITY TRANSFORMATION RULES**

Identity Transformation

☒ Pass-through Zscaler Identity ☐ Change Domain to ☐ Remove Domain Name

Save Cancel

### Slide notes

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

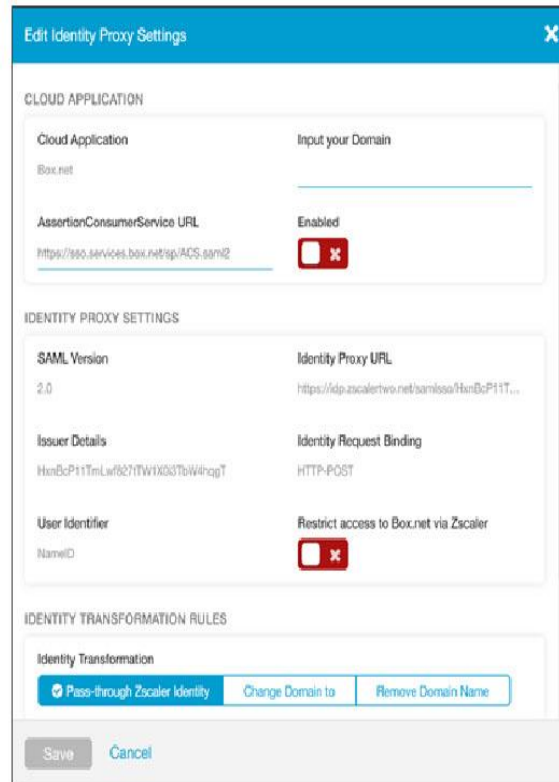
- To use Zscaler as an Identity Proxy you must **Enable** the configuration and turn on the **Restrict access to [the relevant application suite] via Zscaler** option.
- You must provide your Domain information.
- You must provide the **AssertionConsumerService URL**, which for Box is displayed automatically, 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

## Zscaler Identity Proxy Settings

- Configure settings for each application suite
  - Enable and Restrict options
  - Domain configuration
  - Assertion URL specification
  - Identity Transformation configuration
  - Group Identifier configuration
- Copy settings to configure the applications
  - Identity Proxy URL
  - Issuer Details
  - User Identifier



The screenshot shows the 'Edit Identity Proxy Settings' dialog box in the Zscaler interface. The dialog is divided into three main sections: CLOUD APPLICATION, IDENTITY PROXY SETTINGS, and IDENTITY TRANSFORMATION RULES.

**CLOUD APPLICATION**

Cloud Application	Input your Domain
Box.net	
AssertionConsumerService URL	Enabled
<a href="https://sso.services.box.net/sps/ACS.saml2">https://sso.services.box.net/sps/ACS.saml2</a>	<input type="checkbox"/> <input type="checkbox"/>

**IDENTITY PROXY SETTINGS**

SAML Version	Identity Proxy URL
2.0	<a href="https://idp.zscaler-two.net/samlsoa/1anDcP11T...">https://idp.zscaler-two.net/samlsoa/1anDcP11T...</a>
Issuer Details	Identity Request Binding
<a href="#">HmDcP11TmLw627ITW1XG3TbW4ngT</a>	HTTP-POST
User Identifier	Restrict access to Box.net via Zscaler
NameID	<input type="checkbox"/> <input type="checkbox"/>

**IDENTITY TRANSFORMATION RULES**


Identity Transformation

☒ Pass-through Zscaler Identity

### Slide notes

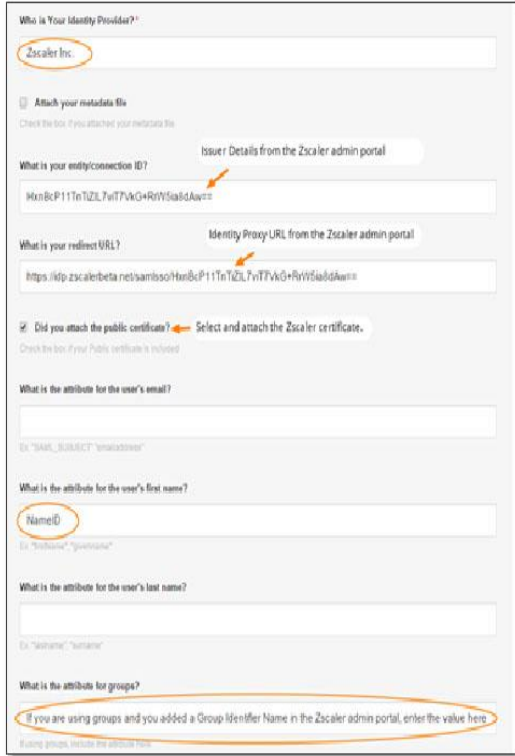
These settings also contain data that you will need to copy and paste across to the application suite in question. The data required depends on the suite, but you will certainly need the **Identity Proxy URL**, and you may also need the **Issuer Details** and **User Identifier**.

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



## Configuring Box to Use Zscaler as an Identity Proxy

- Data required from the Zscaler Admin Portal:
  - The **Identity Proxy URL**
  - The **Certificate** that you downloaded
  - The **Issuer Details**
- Complete the SSO Questionnaire at <https://cloud.box.com/ssoform>
  - Box will use the information provided to set up the Single-Sign on integration



## 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

## 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

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below.

Sign-in page URL: <https://idp.zscalerbeta.net/samlso/HanBcP11TnTiZIL7vT7NMc+RvP> Enter the Identity Proxy URL from the Zscaler admin portal.

Sign-out page URL: <https://accounts.google.com/Logout> Enter the Google logout URL.

Change password URL: URL to let users change their password in your system, when defined here, this is shown even when Single Sign-on is not enabled.

Verification certificate: A certificate file has been uploaded. Replace certificate. The certificate file must contain the public key for Google to verify sign-in requests.

☐ Use a domain specific issuer

Network masks: Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (84.233.187.90/8 72.14.0.0/16). For ranges, use a dash. Example: (84.233.167.204/99/32). All network masks must end with a CIDR.

## 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


The screenshot shows the 'Setup SSO with third party identity provider' page in the Google Admin Console. It includes fields for 'Sign-in page URL', 'Sign-out page URL', 'Change password URL', 'Verification certificate', and 'Network masks'. Annotations with orange arrows point to specific fields: 'Enter the Identity Proxy URL from the Zscaler admin portal.' points to the 'Sign-in page URL' field, which contains 'https://idp.zscalerbeta.net/samlso/HanBcP11TnTiZIL7vT7NMc8rP'. 'Enter the Google logout URL.' points to the 'Sign-out page URL' field, which contains 'https://accounts.google.com/Logout'. 'Upload the Zscaler certificate that you downloaded from the admin portal.' points to the 'Verification certificate' section, which states 'A certificate file has been uploaded. Replace certificate'. A note at the bottom explains that network masks determine which addresses will be affected by single sign-on.

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

## Slide notes

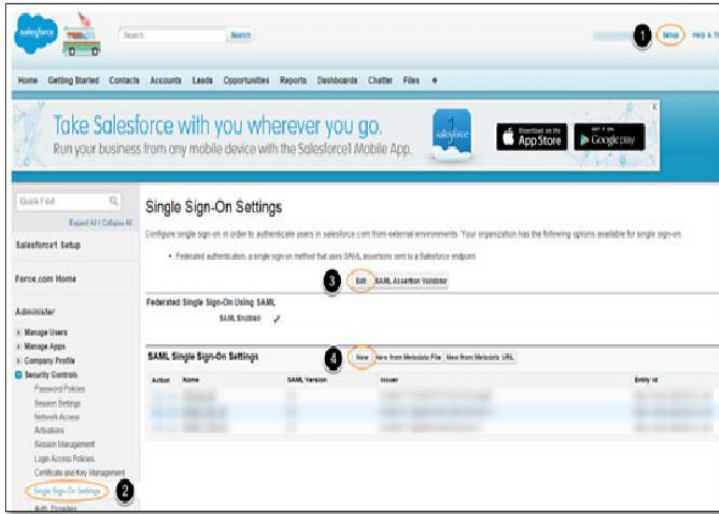
One thing to note with Google Apps, users who are assigned administrator roles in Google cannot use the SSO functionality.

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



## Configuring Salesforce to Use Zscaler as an Identity Proxy

- Data required from the Zscaler Admin Portal:
  - The **Identity Proxy URL**
  - The **Certificate** that you downloaded
  - The **Issuer Details**
- Login to your instance of Salesforce
  1. Click **Setup**
  2. Under **Security Controls** select **Single Sign-On Settings**
  3. **Edit** to enable SAML (if necessary)
  4. Click **New**



## 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

## Configuring Salesforce to Use Zscaler as an Identity Proxy

- Complete SSO settings as indicated and **Save**

**SAML Single Sign-On Settings**

Back Save & More Cancel

Name  Enter a name

SAML Version  Issuer Details from the Zscaler admin portal

Issuer  Enter the issuer details from the Zscaler admin portal

Identity Provider Certificate  zscaler\_certificate.cer

Request Signing Certificate  Upload the certificate that you downloaded from the Zscaler admin portal

Request Signature Method  Enter the following: https://www.safeservice.com

Assertion Encryption Certificate  Enter the following: https://www.safeservice.com

SAML Identity Type  Assertion contains User's SAMLServiceName attribute  
 Assertion contains the Federation ID from the User object  
 Assertion contains the User ID from the User object

SAML Identity Location  Identity is in the NameIdentifier element of the Subject statement  
 Identity is in an Assertion element

Service Provider Initiated Request Binding  Enter POST

Identity Provider Login URL  Enter the Identity Proxy URL from the Zscaler admin portal

Identity Provider Logout URL

Custom Error URL

**Just-In-Time User Provisioning**

User Provisioning Enabled ☐

Save Save & More Cancel

## 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

## Configuring Salesforce to Use Zscaler as an Identity Proxy

- Complete SSO settings as indicated and **Save**
- Enable Zscaler SSO as the authentication method:
  - Click **Setup**
  - Expand **Domain Management** (at left) and select **My Domain**
  - **Edit** the **Authentication Configuration**
  - Select the **Authentication Service** that you configured
  - Click **Save**

The screenshot shows the "SAML Single Sign-On Settings" configuration page. The interface includes tabs for "Save", "Save & New", and "Cancel". The settings are organized into several sections:

- Name:** Set to "Zscaler". Annotation: "Enter a Name".
- SAML Version:** Set to "2.0".
- Issuer:** Set to "https://zscaler.com/zscaler-admin-portal". Annotation: "Issuer Details from the Zscaler admin portal".
- Identity Provider Certificate:** Set to "Choose File | zscaler\_certificate.crt". Annotation: "Upload the certificate that you downloaded from the Zscaler admin portal".
- Request Signing Method:** Set to "RSA-SHA256".
- Assertion Encryption Certificate:** Set to "Assertion not encrypted".
- SAML Identity Type:** Two options are selected: "Assertion contains User's samlforce.com username" and "Assertion contains the Permission to host the User object".
- SAML Identity Location:** Two options are selected: "Identify as the NameIdentifier element of the Subject statement" and "Identify as the AssertionID element".
- Service Provider Initiated Request Binding:** Two options are selected: "HTTP POST" and "HTTP Redirect".
- Identity Provider Login URL:** Set to "https://zscaler.net/samlso/Handler?IdP=Zscaler%2F7XKD-HWVt". Annotation: "Enter the Identity Proxy URL from the Zscaler admin portal".
- Custom Error URL:** Left blank.

A separate section titled "Just-in-time User Provisioning" has "User Provisioning Enabled" checked.

An inset window titled "Authentication Configuration" shows additional settings:

- Header Logo:** Includes a field to "Upload a Logo" (with instructions: "This logo will appear on your login pages. JPG, GIF or PNG, 100 KB max. Maximum dimensions 256x128 px") and a "Choose File" button labeled "No file chosen".
- Background Color:** A color picker set to "#C9A0D6".
- Right Frame URL:** An empty text field.
- Authentication Service:** A dropdown menu with "Zscaler" selected.

At the bottom of the main form are "Save", "Cancel", and "Reset to Default" buttons. The inset window also has similar buttons at its bottom.

## Slide notes

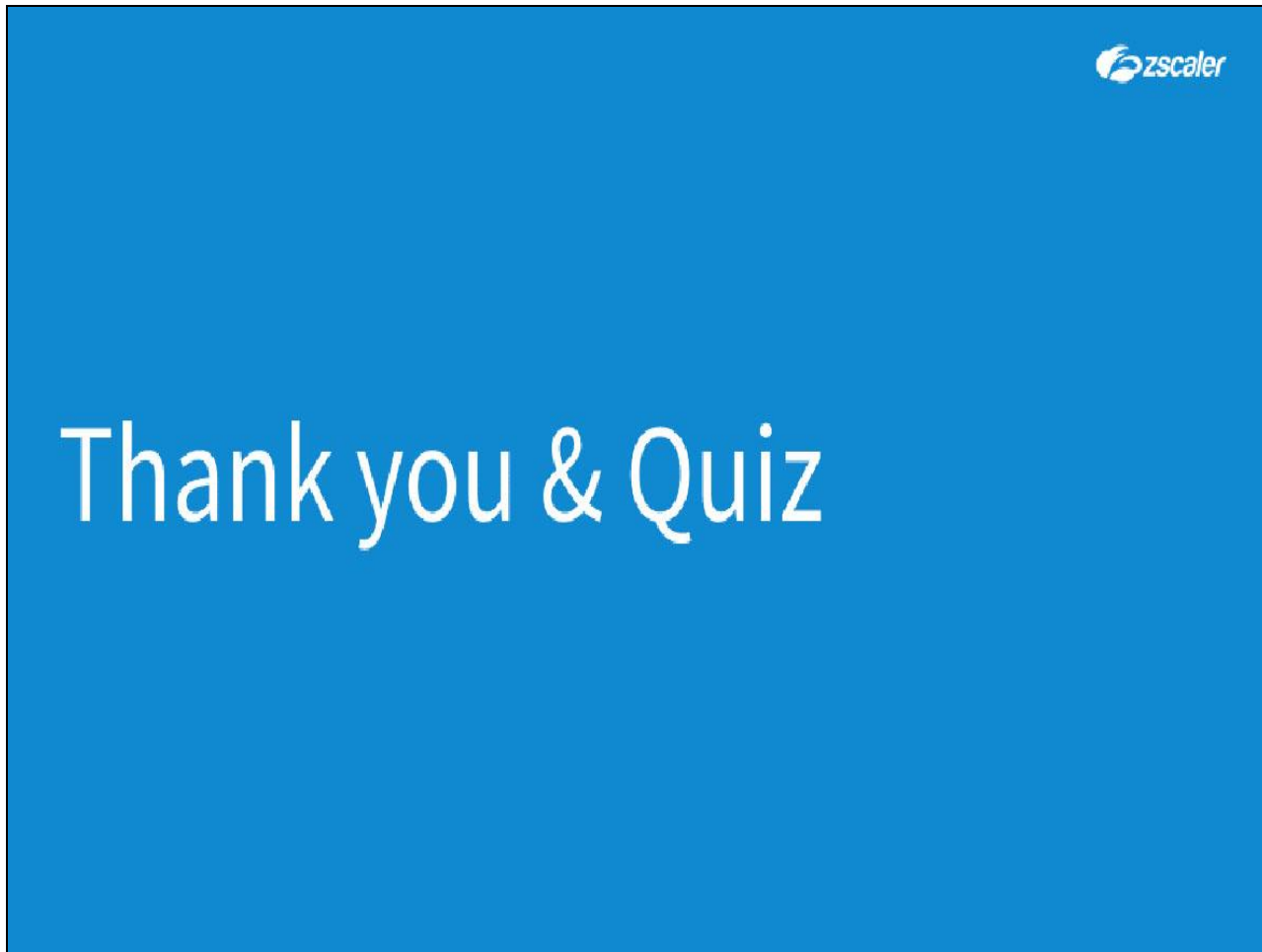
Next you must enable Zscaler SSO as the authentication method, to do this click **Setup** again, expand the **Domain Management** option in the side bar menu at left and select **My Domain**. Select to **Edit** the **Authentication Configuration**, select the **Authentication Service** that you configured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







## Slide 48 - Thank you &amp; 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.