# Table of Contents

Terms and Acronyms ........................................................................................................ 4

About This Document ....................................................................................................... 5

  Zscaler Overview ............................................................................................................. 5
  Zscaler Resources ............................................................................................................. 5
  Microsoft Azure (Azure) ................................................................................................. 6
  Microsoft Resources ......................................................................................................... 6
  Audience ......................................................................................................................... 6
  Software Revisions .......................................................................................................... 6
  Request for Comments ..................................................................................................... 6

Understanding Zscaler and Azure WVD .......................................................................... 7

  Product Overview ............................................................................................................ 7
  Zscaler Internet Access (ZIA) Overview ........................................................................... 8
  Zscaler Private Access (ZPA) Overview ........................................................................... 9
  Azure Windows Virtual Desktop (WVD) Overview .......................................................... 10

Azure WVD Installation .................................................................................................... 10

  Windows Virtual Desktop Installation Video ................................................................... 10
  Creating a WVD Host Pool ............................................................................................... 11
    Installing Windows Virtual Desktop ................................................................................ 12
  Creating a Personal (Dedicated) Host Pool ....................................................................... 13
  Creating a Pooled (Shared) Host Pool ............................................................................ 18

Zscaler Traffic Forwarding Options .................................................................................... 19

  Setting up Zscaler Client Connector .............................................................................. 19
  PAC Files ......................................................................................................................... 24
  Site-to-Site VPN – IPsec Tunnels .................................................................................... 26
    Overview ......................................................................................................................... 26
    Creating an Azure VPN Gateway ................................................................................... 27
  Configuring the Virtual Network Gateway Application .................................................. 29
    Gateway Deployment ...................................................................................................... 30
    Configuring Zscaler ........................................................................................................ 37
    Create a Redundant VPN Connection for Manual Fail-over .......................................... 43
Create a Route Table ........................................................................................................ 49

Appendix A: Troubleshooting ............................................................................................. 54
  VPN Troubleshooting ........................................................................................................ 54
  Troubleshooting from the VNET ...................................................................................... 56
  Verify Traffic is going through the Tunnel to Zscaler .................................................. 57

Appendix B: PAC Examples ............................................................................................... 58
  APP PAC Example: ........................................................................................................ 58
  Forward PAC: ................................................................................................................ 61
  Browser PAC: ................................................................................................................ 64

Appendix C: Requesting Zscaler Support .......................................................................... 68
  Gather Support Information ......................................................................................... 68
  Save Company ID .......................................................................................................... 68
  Enter Support Section ................................................................................................. 69
### Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>WVD</td>
<td>Windows Virtual Desktop</td>
</tr>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection <em>(RFC 3706)</em></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC2890)</em></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange <em>(RFC2409)</em></td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security <em>(RFC2411)</em></td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>PAC</td>
<td>Proxy Auto-Configuration</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Share Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC6101)</em></td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC7239)</em></td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>ZCC</td>
<td>Zscaler Client Connector (Zscaler)</td>
</tr>
</tbody>
</table>
About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can’t match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, visit www.zscaler.com or follow Zscaler on Twitter @zscaler.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>ZIA Best Practices for Traffic Forwarding</td>
<td>Help article on traffic forwarding best practices.</td>
</tr>
<tr>
<td>ZIA – PAC Files</td>
<td>Help articles for PAC, Forwarding PAC, Application Profile PAC.</td>
</tr>
<tr>
<td>ZIA – Installing SSL Certificate on IE-11</td>
<td>Help articles for installing SSL Certificate.</td>
</tr>
<tr>
<td>ZIA – Configuring VPN Credentials</td>
<td>Help articles for configuring VPN.</td>
</tr>
<tr>
<td>ZIA – Configuring a Location</td>
<td>Help articles configuring a location.</td>
</tr>
<tr>
<td>ZIA – Configuring an IPsec Tunnel</td>
<td>Help articles for configuring IPsec tunnels.</td>
</tr>
<tr>
<td>ZCC - Help</td>
<td>Help articles for Zscaler Client Connector.</td>
</tr>
<tr>
<td>ZCC - Bypasses for Tunnel-2 App PAC and Forward PAC</td>
<td>Help articles for ZCC tunnel and PAC bypasses.</td>
</tr>
<tr>
<td>ZCC - Configuring Zscaler App Profiles</td>
<td>Help articles for ZCC profiles.</td>
</tr>
<tr>
<td>ZCC- Configuring Zscaler Forwarding Profiles</td>
<td>Help articles for forwarding profiles.</td>
</tr>
<tr>
<td>ZCC - Customizing Zscaler App with Install Options (MSI)</td>
<td>Help articles for ZCC installs.</td>
</tr>
<tr>
<td>ZCC - Customizing Zscaler App with Install Options (EXE)</td>
<td>Help articles for ZCC installs.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
Microsoft Azure (Azure)

Microsoft Azure, part of Microsoft.com (Nasdaq: MSFT), Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. For more information on Azure, visit azure.microsoft.com or follow them on Twitter@microsoft.

Microsoft Resources

The following table contains links to Microsoft Azure resources based on general topic areas.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Trial License</td>
<td>Link to obtain Azure trial license.</td>
</tr>
<tr>
<td>Azure Documentation</td>
<td>Azure help documentation.</td>
</tr>
<tr>
<td>Windows Virtual Desktop Environment</td>
<td>Setup procedures for Windows Virtual Desktop Environment.</td>
</tr>
<tr>
<td>Azure Virtual Network</td>
<td>Help articles for Azure Virtual Network.</td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td>Help articles for Azure Active Directory.</td>
</tr>
<tr>
<td>Azure Virtual Network Gateway</td>
<td>Tutorial: Create a Site-to-Site connection in the Azure portal.</td>
</tr>
<tr>
<td>Azure VPN High Availability</td>
<td>Highly Available cross-premises and VNet-to-VNet connectivity.</td>
</tr>
<tr>
<td>Azure Route Tables</td>
<td>Virtual network traffic routing.</td>
</tr>
<tr>
<td>Getting Started with WVD</td>
<td>Help article on getting started with Windows Virtual Desktop.</td>
</tr>
</tbody>
</table>

Audience

This guide is for network administrators, endpoint / IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to About This Document.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and Zscaler Client Connector version 2.1.2.105 for the Windows 10 Dedicated Desktop, and PAC file Windows 10 Shared desktop.

Request for Comments

- **For Prospects / Customers**: We value reader opinions and experiences. Contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.

  **For Zscaler Employees**: contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.
Understanding Zscaler and Azure WVD

The following sections detail how Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) operate and interact with Microsoft Azure WVD.

Product Overview

Figure 1 shows a high-level overview of Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) in a Microsoft WVD environment.

Figure 1. Zscaler Internet Access, Zscaler Private Access in a Microsoft WVD Environment

You can integrate Azure and Zscaler in multiple ways. You can forward Internet traffic from Azure to Zscaler Internet Access (ZIA) by using the Zscaler Client Connector (ZCC) on a dedicated private WVD Instance, by using a Browser PAC File, or by forwarding traffic over an IPsec Tunnel (as shown in Figure 1). The IPsec tunnel can be created using various industry standard network and/or native Microsoft components.

You can connect customer traffic destined for internal private resources seamlessly and securely over ZPA by placing a ZPA Application Connector inside the Azure environment. Zscaler Private Access initiated from inside Azure destined to External private resources is currently limited to using the Zscaler Client Connector on a Dedicated Private WVD Instance.

This Deployment Guide covers all of the available traffic forwarding methods. IPsec Tunnels are created using the Azure Virtual Network Gateway, and the Zscaler Client Connector is deployed on a WVD private instance to both Zscaler Internet Access and Zscaler Private Access.
Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—all you do is make Zscaler your next hop to the Internet through one of the following methods:

- Use a tunnel from a network device like an Azure Virtual Gateway or a Cisco CSR for general forwarding from Azure to Zscaler Internet Access (ZIA).

![Figure 2. IPsec Tunnel to Zscaler Internet Access](image)

- Use Zscaler Client Connector, PAC File, or Tunnel for Microsoft Azure WVD Personal (Dedicated Workstation) Instance.

![Figure 3. Zscaler Client Connector on a WVD Private Instance](image)

- Use a PAC file or Tunnel from a network device for Microsoft Azure WVD Pooled (Shared) Instance.

![Figure 4. Browser PAC File](image)

- Forward traffic via our lightweight Zscaler Client Connector or PAC file for mobile or remote employees.
No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a WVD instance in Azure in South Korea—they get identical protection. ZIA sits between your users and the Internet, inspecting every byte of traffic inline across multiple security techniques (even SSL-encrypted traffic).

You get full protection from web and Internet threats. With a cloud platform that supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Browser Isolation you can start with the services you need today and activate others as your needs grow. For more information, see the resources in Zscaler Resources.

Zscaler Private Access (ZPA) Overview

The Zscaler Private Access (ZPA) service enables organizations to provide access to internal applications and services while ensuring the security of their networks. ZPA is an easier to deploy, more cost-effective, and more secure alternative to VPNs. Unlike VPNs, which require users to connect to your network to access your enterprise applications, ZPA allows you to give users policy-based secure access only to the internal apps they need to get their work done. With ZPA, application access does not require network access.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. The Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

ZPA is a separate cloud service from Zscaler Internet Access but is applicable for Dedicated Instance WVD environments for connectivity back to client’s internal applications. It is also applicable for external or remote clients, connecting into applications hosted in Azure eliminating the need for a jump box. For this guide, ZPA access is used to RDP to the WVD instance for administrative purposes, and the Internet bound traffic is sent through an IPsec tunnel to Zscaler Internet Access providing a Dark Internet, Zero-Trust secured Internet experience.

- To access Internal Azure Applications, install a ZPA Application Connector in your Azure environment. ZPA provides Dark Internet, Zero-Trust access using controlled Natural Access for the best possible user experience.

![Figure 5. ZPA Access to Internal Azure Applications](image)
• For access from the Azure WVD environment to the customers external private resources using ZPA, run the Zscaler Client Connector on a Private WVD instance.

ZPA provides the clients environment Zero Trust, Always-on, VPN-like connectivity over a dark Internet. This creates a user experience with secure, simple, low latency connectivity via the same ZIA client for secure internet browsing. For more information, see the resources in Zscaler Resources.

Azure Windows Virtual Desktop (WVD) Overview

Microsoft WVD is a desktop and app virtualization service that run on Azure. You can use Azure WVD to provision Windows 10 pools of resources in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. You can pay either monthly or hourly, just for the WVD instances you launch, which helps you save money when compared to traditional desktops and on-premises VDI solutions. WVD helps you eliminate the complexity in managing hardware inventory, OS versions and patches, and Virtual Desktop Infrastructure (VDI), which helps simplify your desktop delivery strategy. With Microsoft WVD, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device. For more information, see the resources listed under Zscaler Resources.

Azure WVD Installation

The scope of this document is not to walk through the step-by-step procedures to install WVD in Azure, but to provide the Zscaler installation procedures for a WVD Personal, or Pooled environment and the options and requirements for each. Microsoft videos were followed to build and create the WVD pools for testing. The tested installation required a working Hybrid Azure AD instance to domain join the WVD VMs, a Resource Group, Storage Account, Virtual Network, Network Security Group. The installation requires some basic Power Shell Scripting to create the WVD Tenant and bind the Azure subscription to the Tenant. Creation of the Tenant requires Global Admin Privileges for Azure and Local Administrator privileges on the workstation used to create the WVD Tenant.

Windows Virtual Desktop Installation Video

https://www.youtube.com/watch?v=DrkQFSVD9Ik
Creating a WVD Host Pool

A WVD Host Pool in Azure is a resource Pool of VM’s that can be configured as personal stand-alone VM’s with their own operating system that can be assigned to an individual user, or a Pool of Shared VM resources sharing an operating system. The Zscaler Client Connector runs on a Personal Windows 10 Enterprise and all Client Connector forwarding using TLS or DTLS to ZIA, ZPA, and ZDX is supported.

There are several technical and security benefits provided by using a Personal Windows-10 Workstation and the Zscaler Client Connector. The Zscaler Client Connector allows for Zscaler Private Access (ZPA) Connectivity allowing access to all private applications. The Client Connector also enhances connectivity for Zscaler Internet Access (ZIA), and provides all TCP and UDP ports to be forwarded to the Zscaler Enforcement Node which can provide Traditional and Application Firewall protection using the Zscaler Cloud Firewall.

The addition of the Zscaler Digital Experience (ZDX) on the Client Connector also gives you complete end-to-end traffic visibility, from the Zscaler Client to any SaaS Application in the Cloud using application monitors sent by the Client Connector to your most critical applications.

After creating a Personal Pool, you need to define the criteria for the pool which includes the location where the VM’s exist. This selected location should be as geographically central to your organization’s population as possible for a single pool, or as close as possible if you create multiple pools for your different locations. You also need to select Windows-10 Enterprise for Zscaler Client Connector support. Today only single session is supported for the Zscaler Client Connector. Multisession is not supported.

The administrator account is a global administrator account or a service principle that domain joins the VM to the Azure AD Domain. This is a requirement for Reverse Connect to work for the WVD environment.

Reverse Connect is one of the core differences between a typical Remote Desktop Service and Microsoft WVD. It allows an Azure authenticated user to connect to an Azure domain joined VM through a Remote Desktop Gateway in Azure using a Browser or the RD Client which uses HTML5 over TCP port 443. For more information, see Getting Started with WVD.

The VM’s were configured without a Public IP Address and you must use Reverse Connect to use the VM as a WVD Resource. However, ZPA can be used to connect to internal Azure resources that do not have an external IP address, which eliminates the need to have a jump box for support or configuration. This provides a zero-trust dark internet solution for administrators to attach to resources or applications.
Installing Windows Virtual Desktop

After the WVD Tenant has been created and assigned to the Azure license, the first step is to create a host pool. Select **Create a host pool** to start the installation wizard. There are two types of host pools for a WVD environment. They are Pooled or Personal.

**Figure 7. Create a Windows Virtual Desktop Host pool**
Creating a Personal (Dedicated) Host Pool

To select and create the Pool type for the host pool, select either **Pooled** (which for Zscaler connectivity requires a PAC file for traffic forwarding, or **Personal** (which creates a stand-alone workstation that can load the Zscaler Client Connector).

This example uses a Personal host pool. Use **Select a Host type of Personal**.

![Image of Microsoft Azure portal with selected host pool type](image)

**Figure 8. Select Host Pool Type**

To configure the Virtual Machine, Enter the **VM** and **Network** specifics for the **Pool** and then enter the credentials of an Azure administrator that can attach the VM to a domain.

**NOTE**

The installation fails if the VM cannot attach to the domain.

Select **Next Virtual Machines** to continue.
Select Yes to register the Desktop App Group and Create a new Workspace name. This is the workspace the client sees when attaching from the RD client or a browser. Then select Review + create to create the host pool. The installation can take around 30 minutes.

**Figure 9. Configuration of the host pool**
Create a host pool

Figure 10. Configuration of the host pool

Here are the configured host pool and all the created resources from the installation processes. The highlighted devices are the Host Pool, the Desktop Application Group (DAG), and the Dedicated Personal Virtual Machines. We need to assign the users to the Virtual Machine. This is done in two steps:

1. Assigning the user in the Desktop Application Group
2. Assigning the machine to the user is the Session Host Pool under the Host Pool.

Figure 11. The Created WVD Host Pool
To start, Select the **Application Group** to bring up the configuration parameters. Select **Assignments** and then **Add** to bring up the Azure AD User selection menu. Select the user/s to assign to the dedicated VMs and then click **Select** to give the user access to the WVD VM resources.

**Figure 12. The Created Virtual Machine**

Select **All Resource**, and then select the **WVD Host Pool, Session hosts** and **Assign** to bring up the VMs and then select **(Assign)**. Select the user that is assigned to the VM and click **Select**.

We are finished with the VM configuration and if everything completed successfully our users should be able to connect to the VM through the remote desktop application or a browser by using reverse connect.

**Figure 13. The Created Virtual Machine**
Let’s test our VM using Reverse Connect. Bring up a browser and go to the following URL.

https://rdweb.wvd.microsoft.com/webclient

**Figure 14. Browser Access to the Workspace**

This brings up the workspace we created. Double-click on the Default Desktop icon and enter the Azure domain user credentials. This opens Windows-10 VM in our browser.

**Figure 15. The Windows-10 Workstation ready to Install the Zscaler Client Connector or PA**
Our VM is ready to install traffic forwarding to Zscaler for network and endpoint security. We will walk through the methods of configuring forwarding depending on the type of VM. If the VM is a pooled device using multi-threaded Windows-10 OS, we will install a PAC file using the example in the appendix with the appropriate bypasses.

If the VM is a Private VM, the Zscaler Client Connector will be used, although PAC file is an option for every browser if the Zscaler Client Connector is not an option for some reason.

We will also configure a tunnel to ZIA for Internet bound traffic using a virtual network gateway.

**Creating a Pooled (Shared) Host Pool**

A pooled device is a shared virtual machine where each device will have multiple users that use the same resources, but to the user it feels like a personal dedicated Windows workstation. This has financial advantages by pooling resources and provide some operational simplification of management.

![Create a host pool](image)

**Figure 16. Selecting an Image for Pooled (Shared) VM Pool Type**

A pooled host environment also has ramifications for Zscaler. The **Zscaler Client Connector is not supported on pooled machines**. Connectivity to Zscaler is then provided by other means, such as a PAC file for browsers on the pooled system, a Virtual Zscaler Edge Connector, or a tunnel from a firewall or network device running in the Azure environment. VM’s of this type run a Windows-10 Multi-Session OS, which is not supported by the Zscaler Client Connector today.
Zscaler Traffic Forwarding Options

The following processes install the Zscaler Client Connector for the Private WVD VM, or a PAC file using a Dedicated Proxy Port for the Pooled VM. For either the Zscaler Client Connector or a PAC file, bypasses need to be added to direct traffic away from being sent to Zscaler with the goal to keep control traffic local to the Azure environment. This could also include the clients own internal domain.

Setting up Zscaler Client Connector

![Traffic Flow with Zscaler Client Connector using ZIA and ZPA](image)

Figure 17. Traffic Flow with Zscaler Client Connector using ZIA and ZPA

The Zscaler Client Connector is a common endpoint agent for both ZIA and ZPA services. Users can get all of the benefits of the Zscaler Internet security using ZIA, as well as granular, policy-based access to internal resources from a single end-point client using ZPA.

The Zscaler Client Connector has two different modes of operation for forwarding traffic to Zscaler Internet Access. These modes are referred to as Tunnel-1 and Tunnel-2. Tunnel-1 mode only forwards HTTP and HTTPS traffic to ZIA and all other traffic is sent direct to the destination. Whereas, Tunnel-2 mode forwards all TCP, UDP, and ICMP traffic. Using Tunnel-2 and Zscaler Cloud Firewall enables complete traffic coverage and security for Zscaler cloud services, but requires a bit more setup detail compared to Tunnel-1. Selection of Tunnel-1 or Tunnel-2 depends on where you enable Firewall services. If you have Zscaler Cloud Firewall, or want to use the Standard L4 Firewall, configure Tunnel-2 mode.

Zscaler Client Connector traffic forwarded to ZIA is evaluated and inspected according to your organization's security and access policies. By using the Client Connector and Tunnel-2 mode, all user traffic is secured and enforced from the Azure WVD instance out to Internet destinations.
ZPA is a Zscaler cloud service that enables your users to securely access internal enterprise applications in traditional private data centers, or IaaS cloud providers. ZPA establishes a secure transport for accessing your enterprise apps by forwarding all TCP and UDP traffic destined for the application over a TLS connection regardless of the tunnel mode of ZIA. Using ZPA requires the Zscaler Client Connector, and is an advantage to using a Private WVD instance. ZPA provides authenticated, zero trust Access over unadvertized Internet connectivity.

![Figure 18. Comparison of Tunnel-1 and Tunnel-2 modes](image)

After you’ve selected a tunnel mode, configure the Zscaler Client Connector to bypass the appropriate local traffic. This is done with configuration PAC files. For Tunnel-1, add an App Profile PAC to bypass traffic. For Tunnel-2, configure and add a Forwarding Profile PAC. Configure the PAC files in the ZIA Admin Portal, under Hosted PAC Files using the examples and then create forwarding profile for WVD. For more information, see the PAC file examples in Appendix B: PAC Examples.

Use the default forwarding profile for Tunnel-1. To create a Forwarding Profile for Tunnel-2 mode, open the Zscaler Client Connector and select Administration / Forwarding Profile and Add Forwarding Profile. This brings up the Edit Forwarding Profile window.

![Figure 19. Create a Forwarding Profile](image)
To create a Tunnel-2 Forwarding Profile, Enter the **Profile Name** and select the settings shown above. Under the **Z-Tunnel 2.0 > Configure System Proxy Settings > Enforce > Use Automatic Configuration Script**, and you will need to add the location of the Forward Profile PAC file location we just created on the ZIA Admin Portal. Save the profile.

![Edit Forwarding Profile](image)

*Figure 20. Create a Forwarding Profile for Tunnel 2.0*
Next create the Application Profile for the Zscaler Client Connector to assign to the WVD devices. To add the Application profile, select **App Profile > Windows > Add Windows Policy**.

This brings up the **Windows Policy Screen**.

![Windows Policy Screen](image)

**Figure 21. Create an Application Profile**

To create the App Profile for a Tunnel-1 configuration give the profile a **Name**, enable the profile, select the Groups it applies to (typically an AD Group), enter the **Custom PAC URL** (This is the App PAC we created), and enable **Install Zscaler SSL Certificate**.
For Tunnel-2 there are two additional steps. Select the **Forwarding Profile** we just created, and under **Destination Exclusions** enter the public IP address of the Thin Client or remote device that connects to the VM.

![Add Windows Policy](image)

**Figure 22. Create an Application Profile**

**NOTE**

This step is not required if you are deploying Zscaler Client Connector version 3.0 or later.

We should be ready to launch Zscaler Client Connect on the VM after it has been deployed with the appropriate installation switching specifying the Zscaler Cloud, and the Customer Domain, and any other installation switches preferred. See the Client Connector installation instructions link in Zscaler Resources.
PAC Files

Proxy Auto-Configuration (PAC) files are used to support explicit proxy deployments in which client browsers are explicitly configured to send traffic to Zscaler. PAC files can be used for HTTP and HTTP traffic.

A PAC file is a text file that instructs a browser to forward traffic to a proxy server, instead of directly to the destination server. It contains JavaScript that specifies the proxy server and, optionally, additional parameters that specify when and under what circumstances a browser forwards traffic to the proxy server.

For example, a PAC file can specify on what days of the week or what hours of the day traffic is sent to a proxy, or for which domains and URLs traffic is not sent to a proxy. Zscaler uses Macros for proxy selection. The macros used in these examples are `PROXY ${COUNTRY_GATEWAY_FX}` in the APP and Browser PAC, and `PROXY ${ZAPP_TUNNEL2_BYPASS}`; for the Forwarding PAC.

![Traffic Flow using Proxy Auto-Config (PAC File)](image)

*Figure 23. Traffic Flow using Proxy Auto-Config (PAC File)*

All major browsers support PAC files. Browsers simply require the address of the PAC file so they can fetch the file from the specified address and execute the JavaScript in the file. PAC files can be hosted on VDI, an internal web server, or a server outside the corporate network. For the Zscaler macros to work the PAC must be hosted on Zcaler.

The Zscaler service hosts a default PAC file that uses geo-location technology to forward traffic to the nearest Zcaler Enforcement Node (ZEN). You can also upload custom PAC files to the Zscaler service.

There are three PAC files used in the various deployments referenced in this document and each have differences in the configuration. For the Zscaler Client Connector think of the PAC file as a configuration file. It is not ever changing and unmanageable as the reputation of normal browser PAC file use. The primary use case for using the PAC file is to define what IP addresses, URLs, and domains should “Bypass” the Zscaler proxy. Bypasses allow for traffic to stay local or go direct to the defined resources. In the case of WVD, all control traffic and anything that is a local trusted resource should stay local to Azure and not forwarded to ZIA and back. However, any resource that is publicly resolvable can be forwarded to ZIA for security.
For the Pool or Shared VM, you should install a traditional browser PAC file in the browser settings. Depending on the Zscaler connectivity, you may need to use a dedicated proxy port provided by Zscaler and assigned to a specific customer. A dedicated proxy port allows Zscaler to identify any traffic that is received on that unique port and eliminates the initial authentication pop-up and along with Integrated Windows Authentication allows for transparent authentication and a better user experience. If traffic is received over a tunnel, a dedicated proxy port is not needed.

For Tunnel-1 mode on the Zscaler Client Connector, install an Application PAC file in the App Profile under the Custom PAC URL.

For Tunnel-2 mode on the Zscaler Client Connector, install the application PAC file in the App Profile under the Custom PAC URL and a Forwarding Profile PAC containing the same bypasses in the APP PAC. See the example below for the required syntax for each file.

**Tunnel-2 Requires bypasses in both forwarding profile and app profile PAC:**

1. Create a forwarding profile pac that redirects example.com to return "PROXY $(ZAPP_TUNNEL2_BYPASS)"; rest of the traffic should be routed as return "DIRECT";

2. Create app profile that returns SME1 for example.com and SME 2 for rest of traffic.

```
function FindProxyForURL(url, host) {
    /* Updates are directly accessible */
    if(localhostOrDomainIs(host, "example.com"))
        return "PROXY $(ZAPP_TUNNEL2_BYPASS)";
    Return DIRECT to tunnel using Tunnel2 */
    return "DIRECT";
}
```

```
function FindProxyForURL(url, host) {
    /* Updates are directly accessible */
    if(localhostOrDomainIs(host, "example.com"))
        return "DIRECT";
    /* Default Traffic Forwarding. */
    return "PROXY SME2";
}
```

*Figure 24. Tunnel-2 PAC File Symbiosis*

For more information and example PAC files including the Browser PAC, the App PAC, and the Forwarding PAC, the resources in Zscaler Resources.
Site-to-Site VPN – IPsec Tunnels

Overview

This section shows you how to use the Azure and the ZIA Admin Portals to create site-to-site VPN gateway connections from Azure to Zscaler that route and secure your Internet bound traffic using Zscaler Internet Security.

A site-to-site VPN gateway connection is used to connect your Azure virtual network over an IPsec/IKEv2 VPN tunnel to the Zscaler cloud. All Internet bound traffic is then directed through the tunnel using a default route. This configuration uses the Microsoft Virtual Network Gateway, a Local Network Gateway and VPN connection per Zscaler location. A route table is used to direct traffic down the tunnel and to bypass local and unique traffic that must bypass the Zscaler cloud. The native Microsoft features also provide redundancy in case of a failure of one of the components.

Figure 25. Active-Standby Gateway Redundancy Active-Active Tunnels
Azure VPN Gateway Redundancy

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically and resume the site-to-site VPN connections. The switch over causes a brief interruption. For planned maintenance, the connectivity should be restored within 10 to 15 seconds. For unplanned issues, the connection recovery is be longer: about one to one and a half minutes in the worst case.

![Diagram of Azure Virtual Network Gateway with active and standby instances]

**Figure 26. Active-Standby Gateway Redundancy Active-Active Tunnels**

Both the Azure and Zscaler clouds are highly redundant, and the secondary Tunnel is only provided as an example for manual redundancy in case of compliance requirements. The routes would be switched on the Local Gateways to use the secondary Tunnel. Currently there is no state or health check to remove the routes in case of a tunnel failure event.

**Creating an Azure VPN Gateway**

To create a VPN Gateway to attach to Zscaler locations, you must add it as a resource. Select all resources and then select **Add** to start the process of adding a new resource.

![Microsoft Azure interface for adding resources]

**Figure 27. Create a VPN Gateway**
Installing the Virtual Network Gateway Application

After selecting **dd**, type **Virtual Network Gateway** in the search field and hit return. This displays the VPN application.

![Image of Microsoft Azure dashboard with search bar for virtual network gateway]

*Figure 28. Search for the Resource*

![Image of Microsoft Azure Marketplace with virtual network gateway search results]

*Figure 29. Virtual Network Gateway*
Select the **Virtual network gateway** to get started with the configuration and then select **Create** to start the Installation Wizard for the Gateway.

**Figure 30. Create the Virtual network gateway**

**Configuring the Virtual Network Gateway Application**

To create the Virtual Network Gateway, fill in the required information. Give the gateway a name that is easily identified as the VPN Gateway. For this configuration, a Prefix of “A-“ was used for all resources associated with this installation. That keeps everything together when you look at the resources created. Select the **Region** for the gateway creation. The region selected should be the location of the Virtual Network (Vnet). Select:

- A **Gateway type** of VPN
- A **VPN type** of Route-based
- The **Virtual Network** where the gateway is created, and traffic served
- Name the **External Public IP** associated with this gateway

**Figure 31. Create an Application Profile**

This IP address is used as part of the VPN credentials and defined as a location in the ZIA Admin Portal. **Review and Create** the gateway.
Gateway Deployment

Deployment of the gateway can take up to 45 minutes to complete. When the gateway is created, a message saying the deployment is complete appears. You can then select the Go to resource button or select the gateway from the All resources page. The procedures below always start from All resources to use it as a constant.

Figure 32. Deployment of the VPN Gateway

Configuring the Virtual Network Gateway

From the All resources page select the newly created Virtual network gateway. This brings up the gateway details and allows you to create the additional components.

Figure 33. All Resources
Adding Connections to the Gateway

To create a VPN connection to Zscaler, you need to create one for each location you are going to connect to. In our example we created a connection to Dallas and to Denver for redundancy (See Figure 35). Select Connection and then Add. This brings up the Connection Wizard.

Figure 34. Creating Connections
Configuring the Virtual Network Gateway

In the **Add Connection** wizard enter a **Name** that identifies the connection, then select a **Connection type** of **Site-to-site (IPsec)**. The virtual network gateway should be pre-populated with the gateway we just created. Enter the **Shared key (PSK)** that is used by the Zscaler setup as part of the VPN credentials. Then select **IKEv2**. Next select the **arrow (>)** next to the **Local network gateway** to start the wizard to create the local gateway that represents the Zscaler VPN.

![Image of the Add Connection wizard]

**Figure 35. Create a VPN Connection**

![Image of the Choose local network gateway]

**Figure 36. Add a Local network gateway**
After the wizard has launched select **Create new** to create a new local gateway. Give the gateway an intuitive **Name** that identifies it as a VPN to a Zscaler location, then select an **Endpoint of FQDN**. The fully qualified domain name (FQDN) is selected from the Zscaler list of VPN hostnames for your cloud. (Zscaler Three Cloud is used for this example, but your cloud could be any of the Zscaler clouds.)

![Create local network gateway](image)

*Figure 37. Create a Local network gateway*

See the following page to identify your Zscaler cloud and the VPN Host to populate as the FQDN.

**Identify the FQDN for the VPN**

To identify your Zscaler cloud, select **Administration**, and then **Company profile** from the Zscaler UI. Your cloud is identified as the prefix of your company ID.

![Company Profile](image)

*Figure 38. Your Zscaler Cloud*
Go to URL [https://ips.(yourzscalercloud).net/cenr](https://ips.(yourzscalercloud).net/cenr) and select the **VPN Host Name** for the **Location** you want the VPN tunnel to terminate at. In our example, we use dfw1-2-vpn.zscalerthree.net, which is the Zscaler Dallas location. Enter the name as the FQDN in the Azure Gateway setup.

**Figure 39. Identify the FQDN**

**Finish the Local Gateway Setup**

After identifying the name of the VPN host, enter it in the **FQDN field**. Enter the **Address space** for which the local gateway provides access. Address space entries are the destination IP addresses. In this case it is the Internet or all IP addresses in CIDR block format.

**Figure 40. Create a Local network gateway**

You can’t enter 0.0.0.0/0, but you can break it up into two entries of **0.0.0.0/1** and **128.0.0.0/1** as the address space. Then select **OK** to finish the local gateway configuration.
Finish the Virtual Network Gateway Setup

After the creation of the local gateway, we are placed back into the Virtual network gateway wizard, which is now finished. Select OK to finish the configuration.

![Figure 41. Create a Connection]

Configure the IPsec Parameters

Next, set the IPsec configuration parameters on the connection. Select All resources, and then select the Connection that was just created.

![Figure 42. Select the Connection]
This opens the **Connection** screen. Select **Configuration** to bring up the configuration screen.

Under **IPsec / IKE policy** select **Custom**. This opens the IPsec parameters. For **IKE Phase 1** set:

- Encryption to AES256
- Integrity/PRF to SHA256
- DH Group to DHGroup14

For **IKE Phase2 (IPsec)** set:

- IPsec Encryption to none (Null Encryption)
- Integrity to SHA256
- PFS Group to none

Then select **Save**.

![A-VPN-for-Dallas | Configuration](image)

**Figure 43. Customizing IPsec**
Identify the Public IP Address

You must identify the public IP address used to connect to Zscaler to create the VPN credentials and the location identifying the inbound traffic. Select All resources and then select the Public IP Address object created on Page 38. The IP address is located on the right side of the parameter screen. Copy the address and move to the next section to open a support ticket with Zscaler to have the address added as an identified IP address.

![Figure 44. Identify the External IP Address](image)

Configuring Zscaler

Submit a Zscaler Ticket to Add the IP Address to your Zscaler Account

Zscaler support must provision the IP address saved from the last step needs as an identified IP address bound to the Zscaler account. From the ZIA Admin Portal select the question mark (?) at the bottom left of the portal screen. Then select Submit a Ticket. This opens the Submit a Case page.

![Figure 45. Submit a Provisioning Ticket](image)
Fill in the fields to have the IP address added to the Zscaler tenant and select Submit.

**Figure 46. Submit a Case**
Create VPN Credentials

After you get confirmation that the IP has been added successfully, create the VPN Credentials and the Location. Select Administration and then select VPN Credentials.

![VPN Credentials](image)

**Figure 47. Create VPN Credentials**

Select Administration and Add VPN Credentials, which opens the Add VPN Credentials screen.

![Add VPN Credentials](image)

**Figure 48. Add VPN Credentials**

Select IP and then select the IP address just added from the pull-down menu. To complete the configuration, enter the Shared Key (PSK) created in
Configuring the Virtual Network Gateway, then select **Save**.

![Add VPN Credential](image)

*Figure 49. Create VPN Credentials*

**Adding a Zscaler Location**

You must create a location needs to terminate the IPsec VPN connection. To create a location, select **Administration** and then select **Location Management**.

![Select Location Management](image)

*Figure 50. Select Location Management*
Then select **Add Location**. This opens the **Add Location** screen.

![Location Management](image)

**Figure 51. Add a Location**

**Location Parameters**

In the **Add Location** screen enter an intuitive **Name** for the VPN tunnel, then enter the **Country**, **City/State/Province**, and **Time-Zone** information.

Select the **Azure Public IP address** from the **Static IP Address** pull down menu and the **VPN Credentials** created in the previous step.

Finally select the **Gateway Options** to enforce on the VPN connections and **Save** the configuration.

![Add Location](image)

**Figure 52. Create a Location**
Check the Status of the VPN Connection

To check the status of the VPN connection with tunnel insights select **Analytics** and **Tunnel Insights** from the ZIA Admin Portal user interface. This brings up the Insights selection screen.

![Analytics and Tunnel Insights](image)

*Figure 53. Tunnel Insights*

Identify the Public IP Address

To check the VPN tunnel status, filter the logs to find the **Tunnel Status**. Depending on your installation you may need to provide additional filters to narrow down the logs. For this example, this is the first tunnel, so we just need to select **Logs** at the top of the filter selections and then select a **Timeframe** to display. In this example, you can see our IPsec Tunnel is now up. If no logs are displayed, or the logs show an error, revisit all of the configuration steps (or open a support ticket with Zscaler).

![Tunnel Insights](image)

*Figure 54. Tunnel Insights*
Create a Redundant VPN Connection for Manual Fail-over

To create a redundant connection, repeat the steps to create a connection bound to the Virtual Network Gateway. From All resources, select the Virtual network gateway.

![Microsoft Azure](image)

Figure 55. The Virtual Network Gateway
Select **Connections** and then **Add**. This brings up the **Add Connection** screen.

![Figure 56. Add a Connection](image)
In the **Add Connection** wizard give the connection a **Name** that identifies the connection, then select a **Connection type** of **Site-to-site (IPsec)**. The virtual network gateway should be pre-populated with the gateway we just created.

Enter your **Shared key (PSK)** that is used as part of the VPN credentials configured on the Zscaler setup. Then select IKEv2.

Next, select the **arrow (>)** next to the **Local network gateway** to start the wizard to create the Local Gateway that represents the Zscaler VPN.

*Figure 57. Configure the Connection*
In the wizard, select **Create new** to create a new local gateway. Give the gateway an intuitive **Name** identifying it as a VPN to a Zscaler location, then select an **Endpoint of FQDN**. The fully qualified domain name (FQDN) is selected from the Zscaler list of VPN hostnames for your cloud. Repeat the steps in Identify the FQDN for the VPN to identify the FQDN from https://ips.(yourzscalercloud).net/cenr.

Figure 58. *Create a Local Gateway*

![Create a Local Gateway](image)

After you are back into the **Virtual Network Gateway** wizard, select **OK** to finish the configuration.

**NOTE**

Routes are manually added to the Address space and removed from the other local network gateway to force redundancy in case of a catastrophic failure.
Set the IPsec VPN Parameters

You do not need to set the IPsec configuration parameters on the connection. Select All resources and then select the Connection you just created.

![Diagram showing Microsoft Azure portal with All resources selected.](image)

**Figure 60. Select the Connection**
This opens the **Connection** screen. Select **Configuration** to bring up the configuration screen. Under **IPsec / IKE** policy select **Custom** to reveal the IPsec parameters.

For **IKE Phase 1** set:

- Encryption to AES256
- Integrity/PRF to SHA256
- DH Group to DHGroup14.

For **IKE Phase2 (IPsec)** set:

- IPsec Encryption to none (Null Encryption)
- IPsec Integrity to SHA256
- PFS Group to none

Then select **Save**.

---

**Figure 61. Configure IPsec Parameters**

We have finished the configuration of the redundant VPN connection. The final step is to create a Route Table. Move to the next section to complete our installation.
**Create a Route Table**

You need to create a route table and assign it to our subnets sending traffic to Zscaler to control the flow of traffic in Azure. Since the default action is to forward traffic to Zscaler, the route table is used to send local traffic locally and control any Internet traffic that needs to bypass Zscaler.

To create a route table from all resources select **Add**.

![Figure 62. Add a Resource](image)

**Figure 63. Create an Application Profile**
You must configure the route table’s basic features. Select:

- The **Resource group** containing the subnets that need to have traffic directed away from Zscaler
- The **Region** for the route table and give the resource an **Intuitive name**
- Select **No** to **Propagate gateway routes** because we want to control the routes that are applied to the subnet

---

**Figure 64. Create an Application Profile**
Configure the Route Table

To configure the details of the route table, from All resources select the Route Table that was just created. This brings up the Route Table configuration Screen.

![Microsoft Azure interface](image)

**Figure 65. Select the Route Table to Edit**

To create the needed bypass routes, select Routes on the left and then select Add to bring up the Add route screen.

Adding Routes

![Add route screen](image)

**Figure 66. Add Routes**
NOTE

Any local traffic that needs to stay local or bypass Zscaler out to the Internet needs a route with a next hop type of Virtual Network or Internet.

In the above example, the 192.168.0.0/16 network would be kept local. We also need to add the default route of 0.0.0.0/0 with a next hop of Virtual Network Gateway (Zscaler).

In the above example, 3.130.30.39 goes directly to the Internet site and bypass Zscaler. Microsoft is releasing a new feature for bypassing routes based on a tag. This simulates FQDN bypasses. Currently route bypasses are destination-IP-based. To perform FQDN bypasses you need to install a component like the Microsoft firewall. That need is currently out of the scope of this document.
Applying the Route Table

The route table needs to be applied to the subnet that contains our devices that talk to the Internet. From All resources select the Vnet that contains our resources and select Subnets. Then select the Subnet/s that contain the devices that talk to Internet resources, and then apply the route table that was just created.

Figure 68. Apply the Route Table to a Subnet

Our configuration is now completed.
Appendix A: Troubleshooting

VPN Troubleshooting

There are a couple of tools to help troubleshoot the VPN connections. From Zscaler you can use Tunnel Insights (described in Check the Status of the VPN Connection) to check if our tunnel was initiated. You can also use the native VPN troubleshooting tool in Azure (located in the Virtual Network Gateway resource). To use this tool, you must create both Storage and a Container resources. You are prompted to **Select** the resource or **Create** the resource as you initiate troubleshooting.

![Figure 69. VPN Troubleshooting](image)
To start troubleshooting, select the storage and container, then select the **Gateway** and the **Connection** to test. Then select **Start troubleshooting**.

![Troubleshooting a VPN](image)

**Figure 70. Troubleshooting a VPN**

To get successful results, the test may need to be run twice. The connection has to be healthy before the gateway shows healthy, but the gateway test has to be run first. Essentially you need to run the test twice for everything to show healthy.
Troubleshooting from the VNET

From the Vnet you can issue an ICMP or TCP query to see if destinations are reachable. By issuing an ICMP probe to a Zscaler global IP, you can validate destinations are reachable from the Vnet.

Figure 71. Sending an ICMP Echo from a VM
Verify Traffic is going through the Tunnel to Zscaler

The simplest test to see if traffic is flowing through Zscaler is to open a browser and go to ip.zscaler.com. If traffic is flowing through the tunnel through Zscaler, this page tells you traffic is received from a Zscaler location. It also tells you the traffic source public IP address. In this case, traffic is flowing from our public IP Azure in Azure to the Zscaler Dallas facility.

![ip.zscaler.com](image)

*Figure 72. ip.zscaler.com*
Appendix B: PAC Examples

APP PAC Example:

```javascript
function FindProxyForURL(url, host) {

  var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9]+$/;
  var resolved_ip = dnsResolve(host);

  // Don't send non-FQDN or private IP auths to us
  if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") || privateIP.test(resolved_ip))
    return "DIRECT";

  // FTP goes directly
  if (url.substring(0,4) == "ftp")
    return "DIRECT";

  // Updates are directly accessible
  if ((localHostOrDomainIs(host, "trust.zscaler.com")) &&
      (url.substring(0,5) == "http:" || url.substring(0,6) == "https:"))
    return "DIRECT";
}
```
// Example Don't send to Zscaler Internal Domains
//if (dnsDomainIs(host, ".name.of.customer.domain.to.bypass1.com") ||
//dnsDomainIs(host, ".name.of.customer.domain.to.bypass2.com"))
//return "DIRECT";

// Example Don't send to Zscaler Customer Internal IP Addresses
//if (shExpMatch(host, "8.8.8.*") ||
//shExpMatch(host, "4.4.4.*"))
//return "DIRECT";

// Azure Bypass for Authentication
if (dnsDomainIs(url, ".microsoftonline.com") ||
dnsDomainIs(url, ".microsoftonline-p.net") ||
dnsDomainIs(url, ".azure.com"))
return "DIRECT";

// Azure and Microsoft Application Bypasses
if (shExpMatch(url, "microsoft.com") ||
shExpMatch(url, "windows.net") ||
shExpMatch(url, "sharepointonline.com") ||
shExpMatch(url, "office.com") ||
shExpMatch(url, "office.net") ||
shExpMatch(url, "onmicrosoft.com") ||
shExpMatch(url, "lync.com") ||
shExpMatch(url, "sbassets.com") ||
shExpMatch(url, "trafficmanager.net") ||
shExpMatch(url, "msecnd.net") ||
shExpMatch(url, "asnetcdn.com") ||
shExpMatch(url, "azure.net") ||
shExpMatch(url, "secure.skypeassets.com") ||
shExpMatch(url, "tenor.com") ||
shExpMatch(url, "microsoftstream.com") ||
shExpMatch(url, "skype.com") ||
shExpMatch(url, "live.com") ||
shExpMatch(url, "skypeforbusiness.com") ||
shExpMatch(url, "office365.com"))
return "DIRECT";

// Specific to WVD
if (  
  shExpMatch(url, "wvd.microsoft.com") ||
  shExpMatch(url, "core.windows.net") ||
  shExpMatch(url, "login.windows.net") ||
  shExpMatch(url, "servicebus.windows.net") ||
  shExpMatch(url, "warmpath.msftcloudees.com") ||
  shExpMatch(url, "azureedge.net") ||
  shExpMatch(url, "events.data.microsoft.com") ||
  shExpMatch(url, "msftconnecttest.com") ||
  shExpMatch(url, "microsoftonline.com") ||
  shExpMatch(url, "prod.do.dsp.mp.microsoft.com") ||
  shExpMatch(url, "sfx.ms") ||
  shExpMatch(url, "digicert.com") ||
  shExpMatch(url, "aka.ms") ||
  shExpMatch(url, "aka.ms") ||
  shExpMatch(url, "prod.cms.rt.microsoft.com"))
return "DIRECT";
function FindProxyForURL(url, host) {

var resolved_ip = dnsResolve(host);

// Don't send non-FQDN or private IP auths to us
if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0","255.255.255.0") || privateIP.test(resolved_ip))
return "PROXY ${ZAPP_TUNNEL2_BYPASS}";

// FTP goes directly
if (url.substring(0,4) == "ftp:")
return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Updates are directly accessible
if ((localHostOrDomainIs(host, "trust.zscaler.com") &&
(url.substring(0,5) == "http:" || url.substring(0,6) == "https:"))
return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Example Don't send to Zscaler Internal Domains
//if (    
//dnsDomainIs(host, ".name.of.customer.domain.to.bypass1.com") ||
//dnsDomainIs(host, ".name.of.customer.domain.to.bypass2.com")   
//return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Example Don't send to Zscaler Customer Internal IP Addresses
//if (    
//shExpMatch(host, "8.8.8.*") ||
//shExpMatch(host, "4.4.4.*")
// return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Azure Bypass for Authentication
if (    
dnsDomainIs(url, ".microsoftonline.com") ||
dnsDomainIs(url, ".microsoftonline-p.net") ||
dnsDomainIs(url, ".azure.com")
return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Azure and Microsoft Application Bypasses
shExpMatch(url, ".microsoft.com") ||
shExpMatch(url, ".windows.net") ||
shExpMatch(url, ".sharepointonline.com") ||
shExpMatch(url, "office.com") ||
shExpMatch(url, "office.net") ||
shExpMatch(url, "onmicrosoft.com") ||
shExpMatch(url, "lync.com") ||
shExpMatch(url, "sfbassets.com") ||
shExpMatch(url, "trafficmanager.net") ||
shExpMatch(url, "msecnd.net") ||
shExpMatch(url, "asynetcdn.com") ||
shExpMatch(url, "azure.net") ||
shExpMatch(url, "secure.skypeassets.com") ||
shExpMatch(url, "tenor.com") ||
shExpMatch(url, "microsoftstream.com") ||
shExpMatch(url, "skype.com") ||
shExpMatch(url, "live.com") ||
shExpMatch(url, "skypeforbusiness.com") ||
shExpMatch(url, "office365.com")
return "PROXY ${ZAPP_TUNNEL2_BYPASS}"

// Specific to WVD
if (  
shExpMatch(url, "wvd.microsoft.com") ||
shExpMatch(url, "core.windows.net") ||
shExpMatch(url, "login.windows.net") ||
shExpMatch(url, "servicebus.windows.net") ||
shExpMatch(url, "warmpath.msftcloudes.com") ||
shExpMatch(url, "azureedge.net") ||
shExpMatch(url, "events.data.microsoft.com") ||
shExpMatch(url, "msftconnecttest.com") ||
shExpMatch(url, "microsoftonline.com") ||
shExpMatch(url, "prod.do.dsp.mp.microsoft.com") ||
shExpMatch(url, ".sfx.ms") ||
shExpMatch(url, ".digicert.com") ||
shExpMatch(url, "aka.ms") ||
shExpMatch(url, ".aka.ms") ||
shExpMatch(url, ".prod.cms.rt.microsoft.com")
return "PROXY ${ZAPP_TUNNEL2_BYPASS}";

// Send to Zscaler Cloud
//
return "DIRECT";
}

Browser PAC:

/////////////////////////////////////////
/////////////////////////////////////////
/////////////////////
//
// Filename: AzureWVD
// Description: PAC file for use in Azure Windows Virtual Desktop with
// Dedicated Proxy Port 10000. The Dedicated Proxy Port
// requires a Zscaler License and will be a unique port number.
//
////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////

function FindProxyForURL(url, host) {

var privateIP = /^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$/;
var resolved_ip = dnsResolve(host);

if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0","255.255.255.0") || privateIP.test(resolved_ip))
return "DIRECT";

// FTP goes directly
if (url.substring(0,4) == "ftp:"
return "DIRECT";

// Updates are directly accessible
if ((localhostOrDomainIs(host, "trust.zscaler.com")) &&
(url.substring(0,5) == "http:" || url.substring(0,6) == "https:"))
return "DIRECT";

// Example Don't send to Zscaler Internal Domains
//if (
//dnsDomainIs(host, ".name.of.customer.domain.to.bypass1.com") ||
//dnsDomainIs(host, ".name.of.customer.domain.to.bypass2.com")
//return "DIRECT";

// Example Don't send to Zscaler Customer Internal IP Addresses
//if (
//shExpMatch(host, "8.8.8.*") ||
//shExpMatch(host, "4.4.4.*")
//return "DIRECT";

// Azure Bypass for Authentication
if (
domainIs(url, ".microsoftonline.com") ||
domainIs(url, ".microsoftonline-p.net") ||
domainIs(url, ".azure.com")
return "DIRECT";

// Azure and Microsoft Application Bypasses
if (  
    shExpMatch(url, ".microsoft.com") ||  
    shExpMatch(url, ".windows.net") ||  
    shExpMatch(url, ".sharepointonline.com") ||  
    shExpMatch(url, ".office.com") ||  
    shExpMatch(url, ".office.net") ||  
    shExpMatch(url, ".onmicrosoft.com") ||  
    shExpMatch(url, ".lync.com") ||  
    shExpMatch(url, ".sfassets.com") ||  
    shExpMatch(url, ".trafficmanager.net") ||  
    shExpMatch(url, ".msecnd.net") ||  
    shExpMatch(url, ".asnetcdn.com") ||  
    shExpMatch(url, ".azure.net") ||  
    shExpMatch(url, ".secure.skypeassets.com") ||  
    shExpMatch(url, ".tenor.com") ||  
    shExpMatch(url, ".microsoftstream.com") ||  
    shExpMatch(url, ".skype.com") ||  
    shExpMatch(url, ".live.com") ||  
    shExpMatch(url, ".skypeforbusiness.com") ||  
    shExpMatch(url, ".office365.com"))  
  return "DIRECT";

// Specific to WVD  
if (  
    shExpMatch(url, ".wvd.microsoft.com") ||  
    shExpMatch(url, ".core.windows.net") ||  
    shExpMatch(url, ".login.windows.net") ||  
    shExpMatch(url, ".servicebus.windows.net") ||  
    shExpMatch(url, ".warmpath.msftcloudes.com") ||  
    shExpMatch(url, ".azureedge.net") ||
shExpMatch(url, ".events.data.microsoft.com") ||
shExpMatch(url, ".msftconnecttest.com") ||
shExpMatch(url, ".microsoftonline.com") ||
shExpMatch(url, ".prod.do.dsp.mp.microsoft.com") ||
shExpMatch(url, ".sfx.ms") ||
shExpMatch(url, ".digicert.com") ||
shExpMatch(url, "aka.ms") ||
shExpMatch(url, ".aka.ms") ||
shExpMatch(url, ".prod.cms.rt.microsoft.com")
return "DIRECT";

//
// Send to Zscaler Proxy
//
return "PROXY ${COUNTRY_GATEWAY_FX}:10000; PROXY
${COUNTRY_SECONDARY_GATEWAY_FX}:10000; DIRECT";
Appendix C: Requesting Zscaler Support

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

To contact Zscaler support, select Administration > Settings > and then click Company profile.

Figure 73. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

Figure 74. Company ID
Enter Support Section

With your company ID information, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

Figure 75. Submit a ticket