

Slide 1 - Troubleshooting ZIA



# Troubleshooting ZIA

Troubleshooting Tools

©2020 Zscaler, Inc. All rights reserved.

**Slide notes**

Welcome to this training module on some of the tools available for ZIA troubleshooting.

**Slide 2 - Navigating the eLearning Module**

## Navigating the eLearning Module

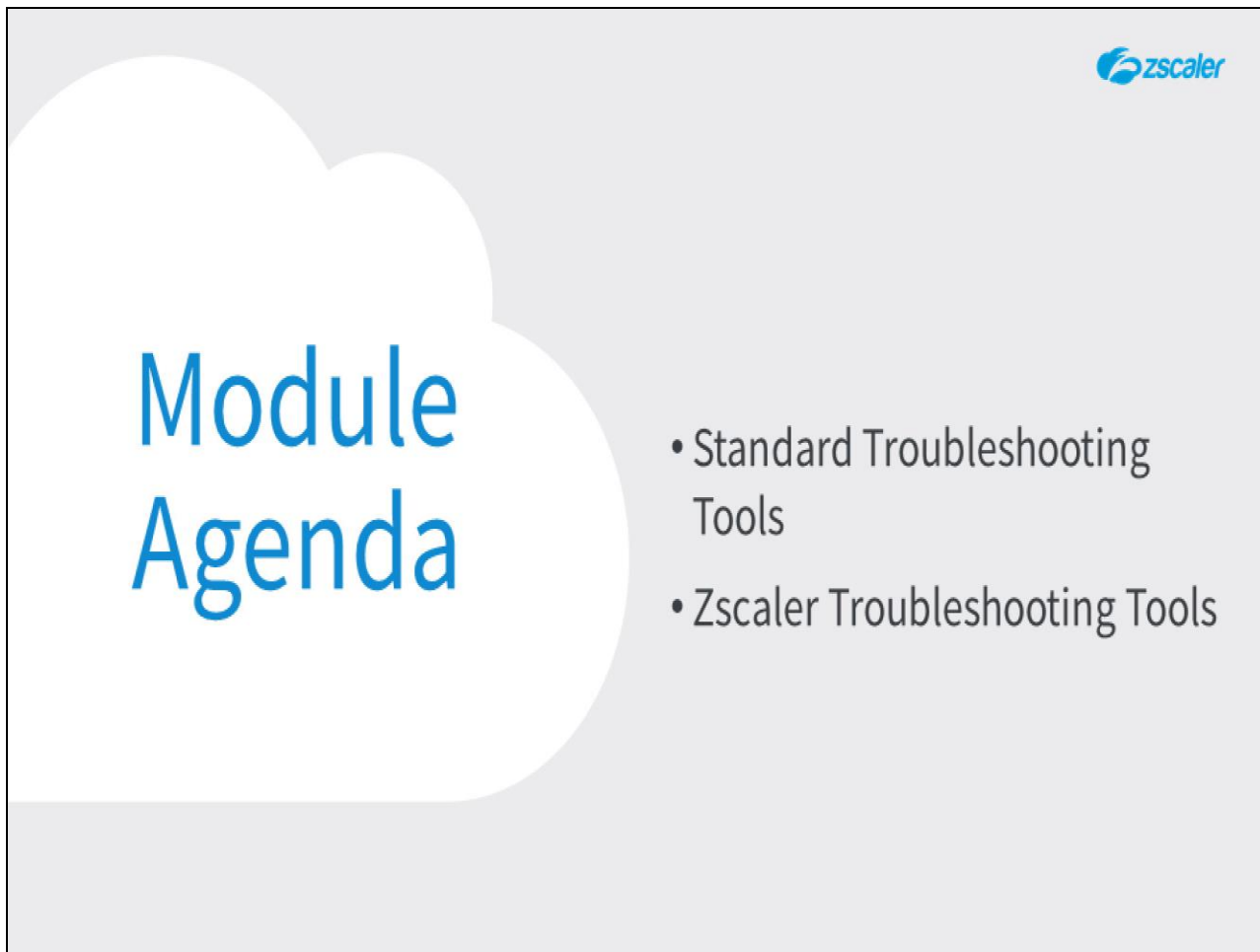
The screenshot displays the Zscaler eLearning module interface. At the top right is the Zscaler logo. The main content area shows a dashboard with four summary cards: 'APPLICATIONS ACCESSED' (15), 'DISCOVERED APPLICATIONS' (3), 'ACCESS POLICY BLOCKS' (0), and 'SUCCESSFUL TRANSACTIONS' (884). Below these are two charts: 'APPLICATIONS ACCESSED' and 'TOP APPLICATIONS BY BANDWIDTH'. The interface includes a sidebar with navigation links like 'Dashboard', 'Diagnostics', 'Live Logs', 'Administration', and 'Search'. At the bottom, there is a video player with a progress bar and playback controls. Several blue callout boxes highlight specific controls: 'Exit' (top right), 'Previous Slide' (bottom left), 'Next Slide' (bottom left), 'Play/Pause' (bottom left), 'Progress Bar' (bottom center), 'Audio On/Off' (bottom right), and 'Closed Captioning' (bottom right).

**Slide notes**

Here is a quick guide to navigating this module. There are various controls for playback including **play** and **pause**, **previous**, and **next** slide.

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 - Module Agenda**



The slide features a light gray background with a large white cloud shape on the left. Inside the cloud, the text "Module Agenda" is written in a large, blue, sans-serif font. To the right of the cloud, there is a bulleted list of two items. In the top right corner of the slide, the Zscaler logo is displayed in blue.

- Standard Troubleshooting Tools
- Zscaler Troubleshooting Tools

**Slide notes**

In this module, we will first review some standard network connectivity troubleshooting tools, then move on to look at some Zscaler-specific tools.

**Slide 4 - Standard Troubleshooting Tools**




**Slide notes**

In the first section, we will review some commonly used network troubleshooting tools.

Slide 5 - Troubleshooting Tools – General

## Troubleshooting Tools – General



Windows **ipconfig**,  
or MAC **ifconfig**

- Use the **/all** or **-a** options for full details


Slide notes

The first tool that we look at is the **ipconfig** (Windows) or **ifconfig** (MAC) utility. This tool allows you to review the interface configuration for the network adapters installed on a Windows or MAC PC. For full details use the options **/all** (Windows), or **-a** (MAC).

Verify that the device has a valid IP configuration, that it has a valid gateway set, and that there is a valid DNS server configuration.

Slide 6 - Troubleshooting Tools – General

## Troubleshooting Tools – General



```
ipconfig /all

configuration
. . . . . : petrelaptop
no suffix . . . . . :
. . . . . : Hybrid
Enabled. . . . . : No
Enabled. . . . . : No
Search list. . . . . : 1m

eter Ethernet 2:
-specific DNS Suffix . :
IP . . . . . : Zscaler Network Adapter 1.0.2.0
Address. . . . . : 00-FF-9F-C2-1A-80
nd. . . . . : Yes
uration Enabled . . . : Yes
IPv6 Address . . . . : fe80::907:9d3a:4098:e40720(Prefere
IPv6 . . . . . : 100-64-0-5(Prefere
IPv6 . . . . . : 255-255-0-0
nday . . . . . :
ID . . . . . : 117509951
mtt GUID. . . . . : 00-01-00-01-1D-07-54-73-1C-39-47-2C-2
P . . . . . : 100-64-0-5
100-64-0-5
```

```
ping csc.com [151.101.45.47] with 32 bytes of data:
P: from 151.101.45.47: icmp=32 time=30ms TTL=64
P: from 151.101.45.47: icmp=32 time=30ms TTL=64
P: from 151.101.45.47: icmp=32 time=30ms TTL=64
P: from 151.101.45.47: icmp=32 time=30ms TTL=64
P: from 151.101.45.47: icmp=32 time=30ms TTL=64

Ping statistics for 151.101.45.47:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
round-trip time in milliseconds:
Minimum = 30ms, Maximum = 30ms, Average = 30ms

harping 8.8.8.8

ping 8.8.8.8 with 32 bytes of data:
P: from 8.8.8.8: icmp=32 time=30ms TTL=64
P: from 8.8.8.8: icmp=32 time=30ms TTL=64
P: from 8.8.8.8: icmp=32 time=30ms TTL=64
P: from 8.8.8.8: icmp=32 time=30ms TTL=64
P: from 8.8.8.8: icmp=32 time=30ms TTL=64

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
round-trip time in milliseconds:
Minimum = 30ms, Maximum = 30ms, Average = 30ms
```

Windows **ipconfig**,  
or MAC **ifconfig**

- Use the **/all** or **-a** options for full details

**Ping** from an affected PC

- Local and Internet destinations
- By FQDN and by IP


Slide notes

The next tool we will talk about is the **ping** utility, available at the command line on both Windows and MAC OS X machines. This tool can be used to evaluate the extent of a network outage. You can ping local addresses to confirm the device has connectivity, then ping Internet addresses to confirm that the gateway does actually go somewhere.

Also ping by FQDN, to verify that DNS resolution is working, and if not ping by IP address, for example to the **8.8.8.8** address of the public Google DNS service. Check the round trip time for the pings, to get a feel for the end-to-end latency on the connection.

Slide 7 - Troubleshooting Tools – General

## Troubleshooting Tools – General



```
ipconfig /all

configuration
. . . . . : petrelaptop
ma Suffix . . . . . :
. . . . . : Hybrid
y Enabled. . . . . : No
y Enabled. . . . . : No
* Search list. . . . . : lan

eter Ethernet 2:
-specific DNS Suffix . :
IP . . . . . : Zscaler Network Adapter 1.0.2.0
Address. . . . . : 00-FF-9F-C2-1A-80
nd. . . . . : Yes
uration Enabled . . . : Yes
IPv6 Address . . . . : fe80::907:9d3a:4098:e40720(Prefere
ma . . . . . : 100-64-0-2(Prefere
h . . . . . : 255-255-0-0
tweety . . . . . :
ID . . . . . : 117509951
ant GUID. . . . . : 00-01-00-01-1D-07-54-73-1C-39-47-2C-2
9 . . . . . : 100-64-0-3
. . . . . : 100-64-0-4
. . . . . : 100-64-0-5
```

```
Microsoft Corporation. All rights reserved.

C:\Users\petrel>ping csc.com

ping csc.com [151.101.45.47] with 32 bytes of data:
y from 151.101.45.47: bytes=32 time=20ms TTL=64
y from 151.101.45.47: bytes=32 time=20ms TTL=64
y from 151.101.45.47: bytes=32 time=20ms TTL=64
y from 151.101.45.47: bytes=32 time=20ms TTL=64

y statistics for 151.101.45.47:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
routetime round trip times in milliseconds:
Minimum = 10ms, Maximum = 20ms, Average = 10ms

C:\Users\petrel>ping 8.8.8.8

ping 8.8.8.8 with 32 bytes of data:
y from 8.8.8.8: bytes=32 time=10ms TTL=64
y from 8.8.8.8: bytes=32 time=10ms TTL=64
y from 8.8.8.8: bytes=32 time=10ms TTL=64
y from 8.8.8.8: bytes=32 time=10ms TTL=64

y statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
routetime round trip times in milliseconds:
Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

```
(version 10.0.14303)
Microsoft Corporation. All rights reserved.

C:\Users\petrel>tracert csc.com

tracert to csc.com [151.101.193.47]
over hops:
0 ms 2 ms dsldevice.lan [192.168.1.1]
1 ms 11 ms 129.196-4-62-afFi-dyn.lip.proxad.net [42.4.1
14 ms 14 ms aa-43-100.larvtr.lip.halgcom.be [51.183.16
14 ms 14 ms aa-13-100.larvtr.lip.halgcom.be [51.183.16
13 ms 13 ms brv-61-link.telix.net [42.115-68-99]
18 ms 18 ms wsh-9b3-link.telix.net [42.115-140-66]
19 ms 19 ms wsh-62-link.telix.net [42.115-141-51]
* * Request timed out.
* * Request timed out.
19 ms 19 ms 151.101.193.47
```

Windows **ipconfig**,  
or MAC **ifconfig**

- Use the **/all** or **-a** options for full details

**Ping** from an affected PC

- Local and Internet destinations
- By FQDN and by IP

**Traceroute** from an affected PC


- Local and Internet destinations


Slide notes

Next is the **tracert** utility (MAC), **tracert** on Windows. This tool will tell you the full path of the traffic to the destination address, and the round-trip times for each hop. It can be used to identify where in the route a problem is occurring. Trace the route to local destinations (such as the default gateway) to confirm local connectivity, and to Internet destinations to confirm end-to-end connectivity.

Slide 8 - Troubleshooting Tools – General


## Troubleshooting Tools – General





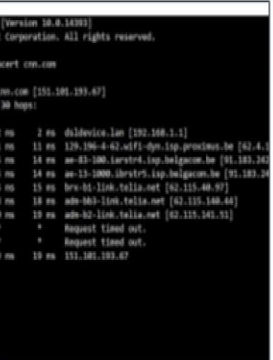
**Windows ipconfig, or MAC ifconfig**

- Use the **/all** or **-a** options for full details



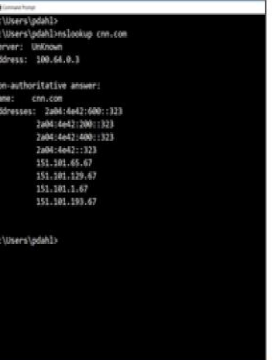
**Ping from an affected PC**

- Local and Internet destinations
- By FQDN and by IP



**Traceroute from an affected PC**

- Local and Internet destinations



**Use nslookup on Windows or Mac**

- Forward resolution of FQDN
- Reverse resolution of IP address

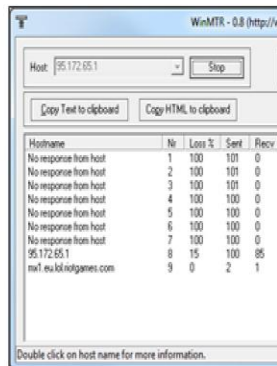
Slide notes

You can also use the **nslookup** network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any specific DNS record. You can use this utility to forward resolve a FQDN to an IP address, or reverse resolve a public IP address to the matching FQDN.



Slide 9 - Troubleshooting Tools – General

## Troubleshooting Tools – General



### WinMTR diagnostic tool

- Combined **ping** and **traceroute** in a GUI-based app
- Exportable results

### Slide notes

The **WinMTR** utility combines the functions of the command line 'ping' and 'traceroute' commands in a GUI-based application for Windows. It also allows for the export of data to a file, which could subsequently be uploaded to a support ticket if necessary.

Slide 10 - Troubleshooting Tools – General

## Troubleshooting Tools – General



WinMTR - 0.8 (http://w...)

Host: 95.172.65.1 [Stop]

[Copy Text to clipboard] [Copy HTML to clipboard]

Hostname	No.	Loss %	Sent	Recv
No response from host	1	100	101	0
No response from host	2	100	101	0
No response from host	3	100	101	0
No response from host	4	100	100	0
No response from host	5	100	100	0
No response from host	6	100	100	0
No response from host	7	100	100	0
95.172.65.1	8	15	100	85
m1.eu.kilodgames.com	9	0	2	1

Double click on host name for more information.

### WinMTR diagnostic tool

- Combined **ping** and **traceroute** in a GUI-based app
- Exportable results

Live HTTP Headers

Headers Generator Config About

HTTP Headers

X-Robots-Tag: noindex, nofollow, noarchive  
Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
Pragma: no-cache  
Expires: Mon, 01 Jan 1990 00:00:00 GMT  
Date: Tue, 27 Jun 2017 15:57:02 GMT  
Access-Control-Allow-Origin: https://docs.google.com  
Access-Control-Allow-Credentials: true  
Access-Control-Expose-Headers: Cache-Control, Content-Length, Content-Type, Date, Expires  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Server: GSE  
Alt-Svc: quic="443"; ma=2592000 v="39,38,37,36,35"  
X-Firefox-Spdy: h2

[Save All] [Printing] [Capture]

### HTTP Header Trace

Capture from browser


- Plug-ins for popular Browsers
- View real-time HTTP Headers
- Exportable results

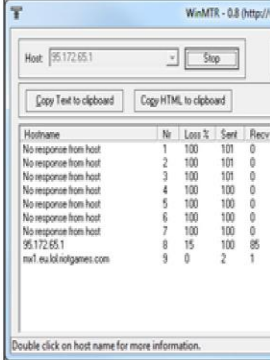
### Slide notes

HTTP Header trace plug-ins are available for most popular Browsers, that give real-time visibility into the HTTP headers as pages load. The results can be saved into a file that can be provided to Zscaler Technical Support.

Slide 11 - Troubleshooting Tools – General


# Troubleshooting Tools – General





**WinMTR diagnostic tool**

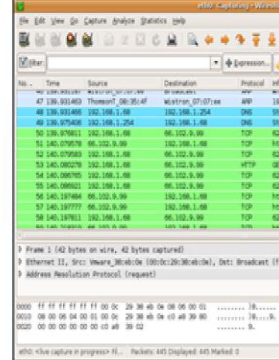
- Combined **ping** and **traceroute** in a GUI-based app
- Exportable results



**HTTP Header Trace**

Capture from browser

- Plug-ins for popular Browsers
- View real-time HTTP Headers
- Exportable results



**Protocol Analyzer**

such as **Wireshark**

- Capture packets during transactions
- Analyze connection and debug protocol flows

Slide notes

If necessary, you can also use a Protocol Analyzer such as Wireshark, to capture packets on the wire as transactions take place. The packet captures can be saved to file for analysis of the protocol flows, or to be uploaded to a support ticket.

Note that a Protocol Analyzer should be a tool of last resort, as it can be quite a labor-intensive process to actually capture the traces. You must first identify where the captures are required and get an Analyzer in place, and you may need to do simultaneous captures at multiple places on the network path.

**Slide 12 - Zscaler Troubleshooting Tools**





**Slide notes**

In the final section, we will look at some of the Zscaler-specific troubleshooting tools available.

Slide 13 - Troubleshooting Tools – Zscaler

## Troubleshooting Tools – Zscaler





### Zscaler **Proxy Test**

from an affected PC


- Check there is a connection to Zscaler
- Check the status of the connection to Zscaler



Slide notes

The first Zscaler tool you should try, is the Zscaler **Proxy Test** Website. Accessed from an affected device, this tool is discussed in detail in the ‘Problem Localization’ module. The output from the Proxy test page can show you if there is a connection through Zscaler or not, and if so what the status of that connection is.

**Slide 14 - Troubleshooting Tools – Zscaler**

## Troubleshooting Tools – Zscaler





### Zscaler Proxy Test

from an affected PC

- Check there is a connection to Zscaler
- Check the status of the connection to Zscaler

### Check the Zscaler Trust site

- Check the status of the Zscaler Cloud
- Check for on-going incidents


<https://trust.zscaler.com>


**Slide notes**

Next, you should check the Zscaler Trust page for the appropriate Cloud, accessed through the page at **<https://trust.zscaler.com>**, to check for known outages or issues.

Slide 15 - Troubleshooting Tools – Zscaler


## Troubleshooting Tools – Zscaler





**Zscaler Proxy Test**  
from an affected PC

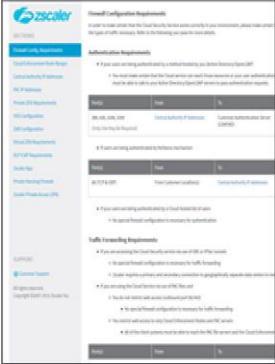
- Check there is a connection to Zscaler
- Check the status of the connection to Zscaler



**Check the Zscaler Trust site**

- Check the status of the Zscaler Cloud
- Check for on-going incidents

<https://trust.zscaler.com>



**Review Zscaler configuration requirements**

- Local and Internet destinations
- By FQDN and by IP



[https://ips.\[Your Cloud Name\].net](https://ips.[Your Cloud Name].net)

Slide notes

If necessary, you can use the Cloud-specific configuration pages at **[https://ips.\[Your Cloud Name\].net](https://ips.[Your Cloud Name].net)** (where [Your Cloud Name] is the Cloud that you are provisioned on), to review what your settings should be, and check for misconfigurations.

Slide 16 - Troubleshooting Tools – Zscaler

# Troubleshooting Tools – Zscaler



Zscaler **Cloud Performance Test** page

- Test performance to the proxy
- Save results to file for upload to a support ticket


Slide notes


The **Cloud Performance Test** page, accessible from the **Connection Quality** link on the Proxy Test page, can be used to test performance to the Zscaler Proxy. The results can be saved to a file for upload to a support ticket if necessary.



**Slide 17 - Troubleshooting Tools – Zscaler**

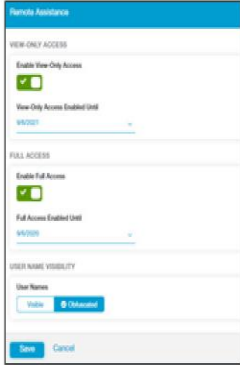
## Troubleshooting Tools – Zscaler





**Zscaler Cloud Performance Test**

- Test performance to the proxy
- Save results to file for upload to a support ticket



**Zscaler Remote Assistance**


- Enable Zscaler Support to access the Admin Portal for your tenant


**Slide notes**

Remote Assistance can be enabled by an administrator at your Zscaler Admin Portal, to allow Zscaler Support to review your settings and Policy configurations and assignments.

Slide 18 - Troubleshooting Tools – Zscaler

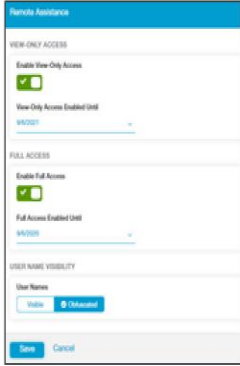
## Troubleshooting Tools – Zscaler





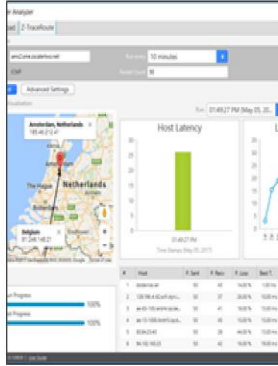
**Zscaler Cloud Performance Test**

- Test performance to the proxy
- Save results to file for upload to a support ticket



**Zscaler Remote Assistance**

- Enable Zscaler Support to access the Admin Portal for your tenant



**Zscaler Analyzer**

- Test performance to Internet destinations
- Export results for upload to Support


Slide notes

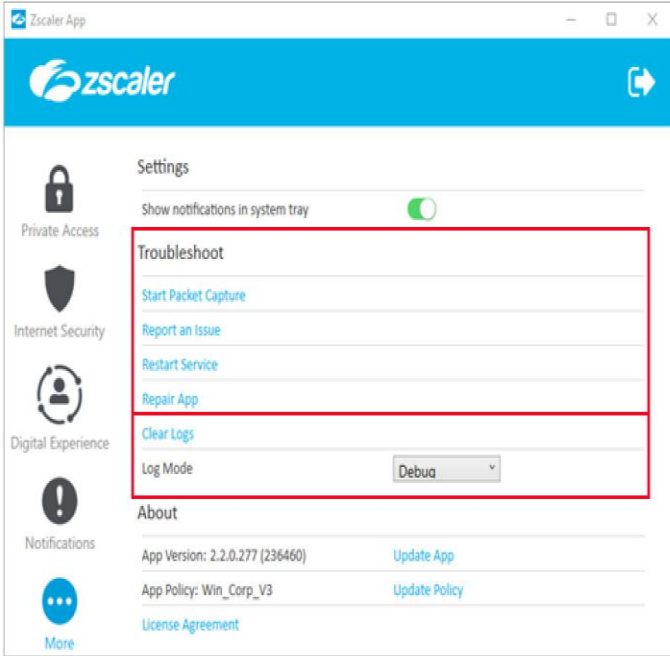
The Zscaler **Network Analyzer** can be downloaded from the Help Portal **Tools** page, or from the Proxy Test page.

It can be used to analyze the path between your location and the ZIA Public Service Edge that you are connecting through, or analyze the time it takes for your Browser to load a Web page. The results can be saved to file for upload to a support ticket.

**Slide 19 - Troubleshooting Tools – Client Connector Logs**

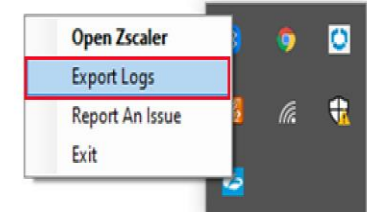
## Troubleshooting Tools – Client Connector Logs





Log Locations

- Windows
  - C:\ProgramData\Zscaler
- OSX
  - ~/Library/Application Support/com.zscaler.Zscaler/
  - /var/log/zscaler/ZSATunnel\_\*.log



**Slide notes**

The troubleshooting tools available on the **More** tab of the Client Connector can be enabled in the Client Connector portal, under **Administration> Zscaler App Support**. Besides being able to clear log files, you can also set different log modes that determine what type of information is stored in the various logs. For example, the **Debug** Mode logs all client connector activity that could assist Zscaler Support with troubleshooting issues.

To manually collect the log files, navigate to the directories listed here. The recommended way to collect the log files is by using the **Export Logs** function. Log files are then exported as a zip file which can be attached to a support ticket.

**Slide 20 - Troubleshooting Tools – Client Connector Logs**

## Troubleshooting Tools – Client Connector Logs




Log File Name	Content
AppInfo	<ul style="list-style-type: none"><li>• System and App info</li></ul>
Setupapi.dev	<ul style="list-style-type: none"><li>• If error in driver installation</li></ul>
ZSAAuth	<ul style="list-style-type: none"><li>• Authentication/Login issues</li></ul>
ZSAService	<ul style="list-style-type: none"><li>• Service/Registry or session related issues</li></ul>
ZSATray	<ul style="list-style-type: none"><li>• UI/Interaction or Windows proxy settings</li></ul>
ZSATunnel	<ul style="list-style-type: none"><li>• Traffic/Network issues</li></ul>
ZSAUpdate	<ul style="list-style-type: none"><li>• App update/Auto update issues</li></ul>

**Slide notes**

This table lists the log filenames and what type of information is contained in each of the files.

## Slide 21 - Troubleshooting Tools – Client Connector Error Codes

## Troubleshooting Tools – Client Connector Error Codes

 Zscaler Client Connector

### Zscaler Client Connector Errors

The tables below provide lists of error messages your user might see on the Zscaler Client Connector (formerly Zscaler App or Z App) while the app is in use:

- Cloud Authentication Error Codes
- Cloud Error Codes

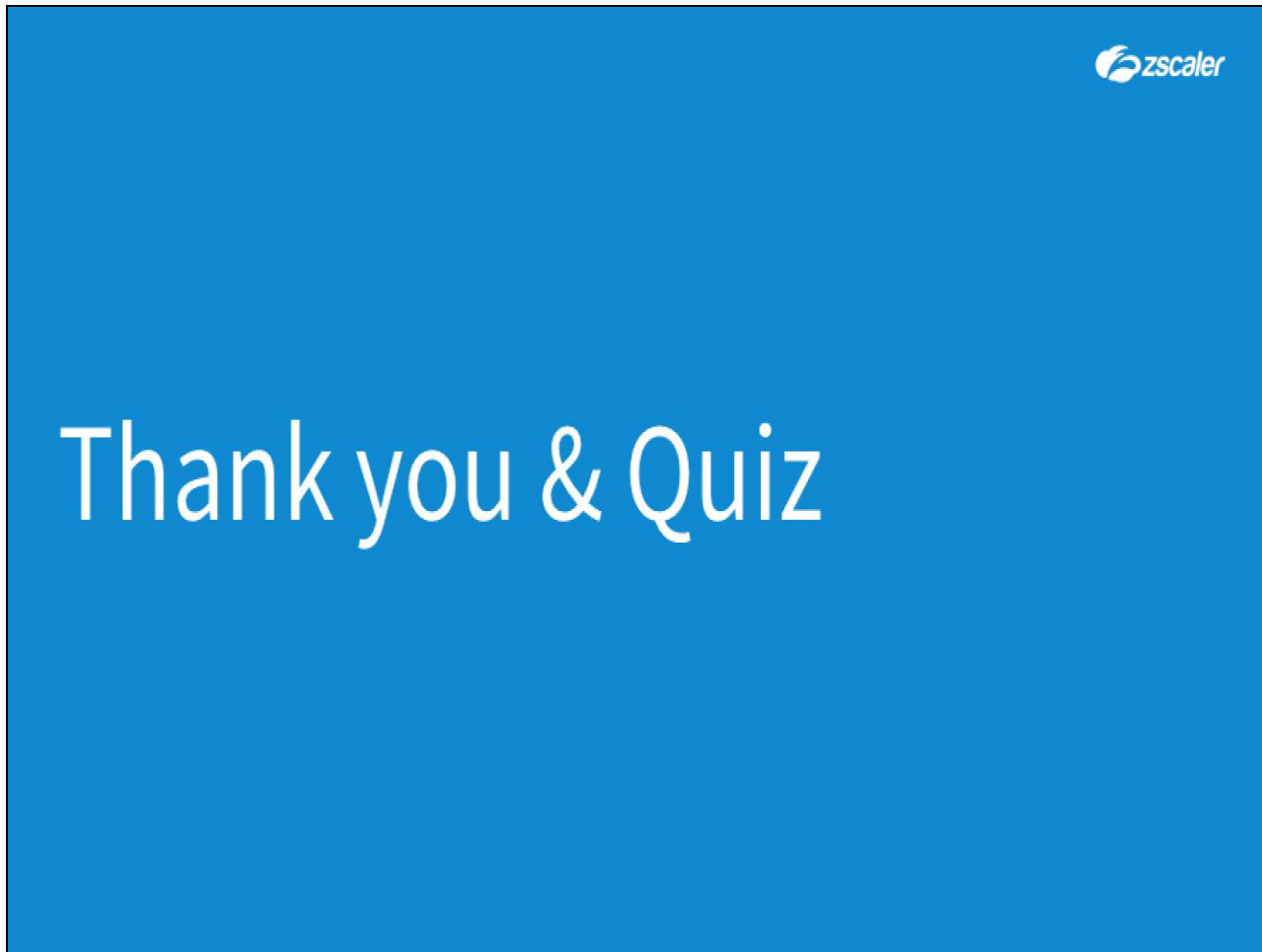
Error Code	Error Message	Error Description	Resolution
1	Zscaler Client Connector Internal Error, Please Contact Administrator.	This is a generic error.	Export logs and contact Zscaler Support.
2	Zscaler Internet Security Authentication Error.	This authentication error occurs when the user's cookie is expired or is no longer valid.	Have the user reauthenticate to Zscaler Client Connector. If the issue persists, export logs and contact Zscaler Support.
3	Zscaler Internet Security Enrollment Version Error.	This error occurs when the device runs a version that is not supported by the cloud.	Upgrade to the latest version of Zscaler Client Connector.
4	Enrollment System Bad Timestamp Error, Please	This error occurs when there is a time mismatch between the device and the	Check the system time and ensure that it is accurate.

<https://help.zscaler.com/z-app/zscaler-app-errors>

## Slide notes

The Help portal URL listed here provides more detailed information about any Client Connector error codes that you may see in the log files.

**Slide 22 - Thank you & Quiz**



**Slide notes**

Thank you for following this training module on ZIA troubleshooting tools. We hope this module has been useful to you and thank you for your time.

What follows is a short 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.