



Zscaler Deployment

Troubleshooting Guide - Training Aid

ZCDS Troubleshooting Guide
Feb 2022

ZIA/ZPA: Authentication	1
Zscaler Client Connector Authentication - Troubleshoot Client Connector Authentication Error	1
Scenario/ Expected Result: User is prompted to Authenticate.	1
Problem: Authentication error is returned. Restarting the service and trying to reauthenticate fails.	1
Check Client Connector Authentication Error Log Entry	1
ZIA/ZPA: Authentication	2
Zscaler Client Connector Authentication - Troubleshoot User Credential Inconsistency Error (42000)	2
Scenario/ Expected Result: User fills in valid authentication credentials and expects to be enrolled into Zscaler.	2
Problem: [42000] error message is displayed: Inconsistency in user credentials is detected.	2
Diagnose Credential Usage Change	2
Test Client Connector Re-enroll	2
ZIA: Authentication	3
Zscaler Client Connector Authentication - Troubleshoot Authentication Internal Error	3
Scenario/ Expected Result: User attempts to authenticate with Client Connector using valid credentials.	3
Problem: Authentication fails and displays a message saying "An internal error occurred".	3
Diagnose Incorrect User Auth Domain Issue	3
Prepare Zscaler Tenant Auth Domain Provisioning Request	3
ZIA: Authentication	4
Zscaler Client Connector Authentication - Troubleshoot Authentication Server Connection Error	4
Scenario/ Expected Result: User fills in valid authentication credentials and expects to be enrolled into Zscaler.	4
Problem: Secure Connection Failed message is displayed	4
Adjust Auth Server URL SSL Exemption	4
Verify Authentication Server Exemptions	5
Adjust Auth Server URL PAC File Direct Entry	5
ZIA: Authentication	6
Zscaler Client Connector Authentication - Troubleshoot No Authentication Policy Enforcement Error	6
Scenario/ Expected Result: User browses to a website from a location where Enforce Authentication is enabled. Logs should show them as the user on the transaction.	6
Problem: Authentication is not being enforced. Transaction logs show a generic looking username for an unauthenticated user.	6
Check SSL Inspection For Authentication Required Destination	6
Check IP Surrogate Setting	6
ZIA: Traffic Forwarding	7
Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Endpoint Firewall/ Antivirus Error	7
Scenario/ Expected Result: Service Status ON in Zscaler Client Connector Connectivity	7
Problem: Zscaler Client Connector shows Endpoint FW/AV Error.	7
Verify Health Check Traffic Routing	7
Check Windows Firewall Connection Block	7
ZIA: Traffic Forwarding	8
Zscaler Client Connector Traffic Forwarding - Diagnose Client Connector Connection Failure	8

Scenario/ Expected Result: Zscaler Client Connector processes permitted to run on the user's device.	8
Problem: Endpoint protection solutions or other permission controls prevent Zscaler Client Connector from running.	8
Check Client Connector End User Device Connectivity - Process Permissions	8
ZIA: Traffic Forwarding	9
Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Captive Portal Detection Issue	9
Scenario/ Expected Result: User connects their device to a new network and enrolls the device into Zscaler.	9
Problem: Zscaler Client Connector shows Captive Portal Detected error.	9
Check Captive Portal Detection Log Entry	9
Check Captive Portal HTTP Response Code	9
Check reachability of Captive Portal Detection URL	9
Check reachability to download default PAC file	10
ZIA: Traffic Forwarding	11
Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Network Error	11
Scenario/ Expected Result: User authenticates and device is enrolled in Zscaler.	11
Problem: Zscaler Client Connector shows Network Error	11
Retry the network connection	11
Check outbound connectivity to mobile.<cloudname>.net:443	11
Check Host Name Resolution for mobile.<cloudname>.net	11
Diagnose Host Not Found DNS Failure	11
Diagnose Connection Reset by Peer Failure	11
Check connectivity to Zscaler cloud	12
Diagnose No Route To Host Failure	12
Diagnose Network is Unreachable Failure	12
Diagnose Certificate Validation Error	12
ZIA: Traffic Forwarding	13
Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Driver Error	13
Scenario/ Expected Result: Zscaler User sees “Driver error” on Zscaler Client Connector, repair option does not help.	13
Problem: Driver Error issue occurs when the files are corrupted.	13
Repair Client Connector Driver Error	13
Re-install Client Connector	13
Re-install Client Connector (Manual)	13
ZIA: Traffic Forwarding	14
Troubleshoot Internet Traffic Forwarding - Check ZIA Public Service Edge Routing	14
Scenario/ Expected Result: Internet traffic should be routed to the closest Zscaler data center.	14
Problem: Traffic is routed to a node that is geographically distant from the user's location. User asks "Why do I get sent to LAX1 when I'm in Atlanta?".	14
Check GeoIP Coordinates	14
Check Zscaler Data Center Health	14
Check Service Edge Connection Timeout	14
Check Service Edge Subcloud	14



ZIA: Traffic Forwarding	14
Troubleshoot Internet Traffic Forwarding - Troubleshoot ZIA Network Infrastructure Issues	15
Scenario/ Expected Result: Traffic is being forwarded to a Zscaler Public Service Edge	15
Problem: Traffic is blocked by an intermediate device or some other failure.	15
Troubleshoot ZIA Network Outage	15
Troubleshoot Zscaler Public Service Edge Issue	15
ZIA: Policy	15
Troubleshoot Internet Application Access - Check Inspection Policy Bypass/ Failure	16
Scenario/ Expected Result: Access to a specific URL is expected to be controlled by a policy that defines what the user may or may not access.	16
Problem: A user is either allowed to access a website they should not be able to access, or they are restricted from accessing a site they should be able to access.	16
Check CDN URLs in HTTP Header Trace	16
Check SSL Inspection Bypass	16
Check URL Inspection Bypass	16
Check Cloud App Inspection Bypass	17
Check SSL Bypass List	17
Check SSL Wildcard Domains Bypass	17
Check Inspection Bypass List	17
ZIA: Policy	17
Troubleshoot Internet Application Access - Troubleshoot Website Loading Issue	18
Scenario/ Expected Result: User should be able to connect to a website according to the policies in place.	18
Problem: Website is unreachable through Zscaler.	18
Check Network Access Control List (ACL) Blocks	18
Check Destination Webmaster Denylist	18
Analyze Internet Access Issue HTTP Headers File Capture	19
Analyze Internet Access Issue Packet Capture	19
ZPA: Authentication	19
Zscaler Client Connector Authentication - Check ZPA Authentication	20
Scenario/ Expected Result: SAML attributes for enrolled users are received in ZPA and available as criteria of use in policies.	20
Problem: SAML attributes are not received or have incorrect details.	20
Check ZPA Enablement on Mobile Portal	20
Verify User SAML Setup	20
ZPA: Traffic Forwarding	20
Troubleshoot Private Application Traffic Forwarding - Troubleshoot ZPA Application Traffic Failure	21
Scenario/ Expected Result: Access policies are configured for a user to be able to access a private application.	21
Problem: User is unable to access a private application. ZPA Diagnostics Data shows status code such as CA: Application not reachable .	21
Test Application Host Reachability From App Connector	21
Test App Connection From App Connector	21

ZPA: Traffic Forwarding	21
Troubleshoot Private Application Traffic Forwarding - Troubleshoot App Connector	22
Scenario/ Expected Result: App Connector starts and is enrolled for use within ZPA.	22
Problem: zpa-connector status shows enrollment error. Messages such as cannot decrypt data indicated issues with the provisioning key.	22
Check App Connector Enrollment	22
ZPA: Policy	22
Troubleshoot Private Application Access - Diagnose Private Application Access Error	23
Scenario/ Expected Result: User is granted access to a private application.	23
Problem: User is unable to access the application, and ZPA diagnostics indicate that a policy is not configured.	23
Diagnose SE: Policy Not Configured For Access Error	23
ZPA: Policy	23
Troubleshoot Private Application Access - Check Private Application Reachability	24
Scenario/ Expected Result: User is granted access to a private application.	24
Problem: Unable to access application and ZPA diagnostic logs show error “SE: Policy not configured for access”	24
Verify Application Domain Seen By Client Connector is ZPA Domain	24
Check App Segment Configuration	24
ZIA: User Experience	24
Troubleshoot Zscaler User Experience	25
Scenario/ Expected Result: Applications should be usable through Zscaler without any noticeable extra delays or rendering issues.	25
Problem: User complains that access to a private application is "slow".	25
Test ISP to Zscaler Data Center Latency	25
Capture Web Page Load Time Records	25
Check Packet Retransmission Rates / Fragmentation	26
ZIA: Logging & Reporting	26
Troubleshoot Zscaler Log Streaming Issue	27
Scenario/ Expected Result: Log streams feeds are received at the destination such as a SIEM	27
Problem: Log entries are missing at the SIEM. They may not be arriving at all or are missing for a period of time.	27
Check NSS Connectivity	27
Check NSS SIEM reachability	27



ZIA/ZPA: Authentication

Zscaler Client Connector Authentication - Troubleshoot Client Connector Authentication Error

Scenario/ Expected Result: User is prompted to Authenticate.

Problem: Authentication error is returned. Restarting the service and trying to reauthenticate fails.

Tips for avoiding this issue: Educate users to be aware that this can occur if something changes the device fingerprint, and is part of the security. Logging out and re-enrolling should validate a changed device fingerprint that might prompt this error.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check Client Connector Authentication Error Log Entry	Examine log file: C:\ProgramData\Zscaler\ZSATunnel_ <date>.log for ERROR entries.</date>	ERR zpn_client_authenticate error: BRK_MT_AUTH_SAML_FINGER_PRINT_FAIL	Zscaler Client Connector collects device information and sends it to Zscaler which enables fingerprinting of the device for security and reporting purposes. The fingerprint contains key unique data from the device, to prevent any possibility of cloning the machine for unauthorized access. Any update in the user's device attributes triggers Zscaler to re-enforce authentication for that user.

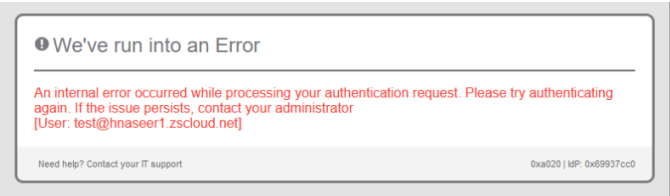
ZIA/ZPA: Authentication

Zscaler Client Connector Authentication - Troubleshoot User Credential Inconsistency Error (42000)

Scenario/ Expected Result: User fills in valid authentication credentials and expects to be enrolled into Zscaler.

Problem: [42000] error message is displayed: *Inconsistency in user credentials is detected.*

Tips for avoiding this issue: Ensure that all of the needed user domains are provisioned on the Zscaler tenant.



Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause								
Diagnose Credential Usage Change	Help article: Zscaler Client Connector: ZPA Authentication Errors	<div><div>Zscaler Client Connector Help > Troubleshooting > Zscaler Client Connector: ZPA Authentication Errors</div><div><div>Client Connector</div><div>Zscaler Client Connector: ZPA Authentication Errors</div><div>The table below provides a list of error messages your users might see for Zscaler Client Connector (formerly Zscaler App or Z App) during the enrollment process.</div><table><thead><tr><th>Error Code</th><th>Error Message</th><th>Error Description</th><th>Resolution</th></tr></thead><tbody><tr><td>42000</td><td>Inconsistency in user credentials is detected. Log out of the client and retry.</td><td><div>When the user attempts to reauthenticate to ZPA, this error occurs if:</div><ul style="list-style-type: none">The user enters a different username instead of the one provided during initial enrollment.The IdP SAML response has a different NameID instead of the one sent during initial enrollment.</td><td><div>Verify that the user has entered the username provided during initial enrollment, and have the user retry authentication.</div><div>If the error persists, verify that the IdP SAML response has the NameID that ZPA received during initial enrollment.</div><div>You can also have the user log out from Zscaler Client Connector and attempt to re-enroll into ZPA.</div></td></tr></tbody></table></div></div>	Error Code	Error Message	Error Description	Resolution	42000	Inconsistency in user credentials is detected. Log out of the client and retry.	<div>When the user attempts to reauthenticate to ZPA, this error occurs if:</div> <ul style="list-style-type: none">The user enters a different username instead of the one provided during initial enrollment.The IdP SAML response has a different NameID instead of the one sent during initial enrollment.	<div>Verify that the user has entered the username provided during initial enrollment, and have the user retry authentication.</div> <div>If the error persists, verify that the IdP SAML response has the NameID that ZPA received during initial enrollment.</div> <div>You can also have the user log out from Zscaler Client Connector and attempt to re-enroll into ZPA.</div>	Authentication error codes and error messages are documented on the help portal. In this example the possible resolutions are: <ul style="list-style-type: none">check the username initially used and verify that the same is being used for re-enrollment.verify the IdP SAML response.have the user logout and retry.
Error Code	Error Message	Error Description	Resolution								
42000	Inconsistency in user credentials is detected. Log out of the client and retry.	<div>When the user attempts to reauthenticate to ZPA, this error occurs if:</div> <ul style="list-style-type: none">The user enters a different username instead of the one provided during initial enrollment.The IdP SAML response has a different NameID instead of the one sent during initial enrollment.	<div>Verify that the user has entered the username provided during initial enrollment, and have the user retry authentication.</div> <div>If the error persists, verify that the IdP SAML response has the NameID that ZPA received during initial enrollment.</div> <div>You can also have the user log out from Zscaler Client Connector and attempt to re-enroll into ZPA.</div>								
Test Client Connector Re-enroll	User logs out with the Log Out button on the Client Connector.	<div><div>Zscaler Client Connector</div><div><div><div></div><div>Log Out</div></div><div><div><div>Private Access</div><div>Notifications</div></div><div><div>Connectivity</div><div>Username</div><div>Service Status</div><div>Network Type</div><div>Authentication Status</div><div>Broker</div></div><div><div>student@patraining50.safemarch.com</div><div>ON</div><div>Off-Trusted Network</div><div>Authenticated</div><div>165.225.211.253</div></div></div></div></div>	Since authentication is a sequence of multiple steps be sure to start from a fully logged out device when troubleshooting. Carefully check the credentials entered at each step of the enrollment to make sure they are for an authorized user on a valid domain.								



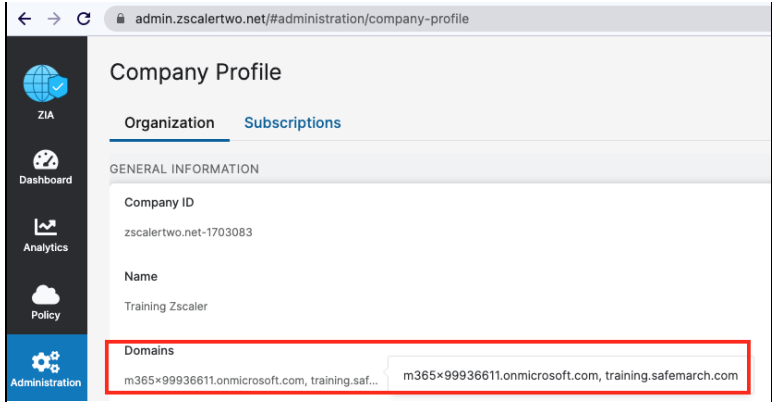
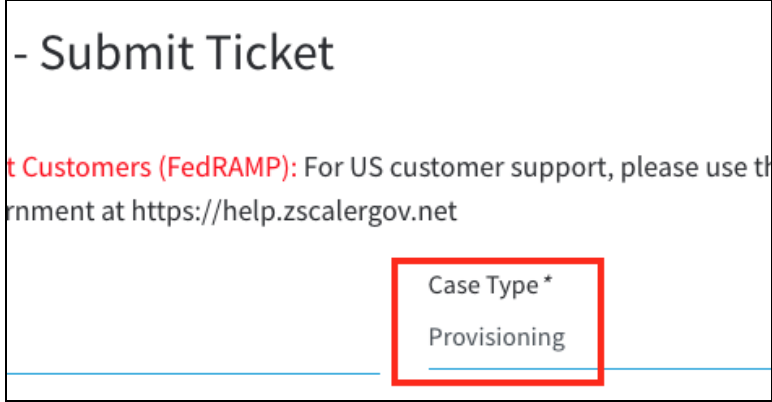
ZIA: Authentication

Zscaler Client Connector Authentication - Troubleshoot Authentication Internal Error

Scenario/ Expected Result: User attempts to authenticate with Client Connector using valid credentials.

Problem: Authentication fails and displays a message saying "An internal error occurred".

Tips for avoiding this issue: Verify that the domains provisioned on the ZIA tenant cover all of the domains of the credentials that the users have been instructed to use to enroll into Zscaler services.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Diagnose Incorrect User Auth Domain Issue	Check the provisioned domain on the ZIA Tenant. https://admin.<cloud_name>.net/#administration/company-profile		Some possible scenarios: <ul style="list-style-type: none">some users in the organization may be on a different domain that has not yet been provisioned; orthis user is confused about which credentials to use.
Prepare Zscaler Tenant Auth Domain Provisioning Request	Zscaler Help - Submit a ticket https://help.zscaler.com/submit-ticket Case Type: Provisioning		Opening a Provisioning support case with the Zscaler Global Support team is the most direct method to get a needed domain provisioned.

ZIA: Authentication

Zscaler Client Connector Authentication - Troubleshoot Authentication Server Connection Error

Scenario/ Expected Result: User fills in valid authentication credentials and expects to be enrolled into Zscaler.

Problem: *Secure Connection Failed* message is displayed

Tips for avoiding this issue: Ensure that all authentication traffic goes direct to the Identity Provider destination URL. This should not be an issue for users who are off the trusted network and will have traffic forwarded with the Client Connector, but check for any other forwarding that may send the authentication traffic to Zscaler (e.g. PAC file or GRE/IPSec tunnel) instead of directly to the IdP. Make sure that the authentication traffic is not being intercepted for inspection by Zscaler.

Secure Connection Failed

An error occurred during a connection to ██████████.okta.com.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

[Learn more...](#)

Try Again

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Adjust Auth Server URL SSL Exemption	Create a custom URL category and add the IdP host domain: https://admin.<cloud>.net/#administration/url-categories Create an SSL rule to bypass inspection on the custom URL category: https://admin.<cloud>.net/#policy/web/ssl-inspection		Traffic for IdP URLs in the custom URL category (SSL Bypass in this example) will bypass inspection, allowing the traffic to go direct and unchanged to the IdP.

Add URL Category

URL CATEGORY

Name

SSL Bypass

URL Super Category

User-Defined

Administrator Operational Scope

Scope Type

Any

Custom URLs

Add Items

Search...

safemarch.okta.com

1-1 of 1

Add Items

Remove

Add SSL Inspection Rule

SSL INSPECTION RULE

Rule Order

3

Rule Name

SSL_1

Rule Status

Enabled

Rule Label

CRITERIA

URL Categories

SSL Bypass

OR

Cloud Applications

Unselected Items

Selected Items (1)

SSL

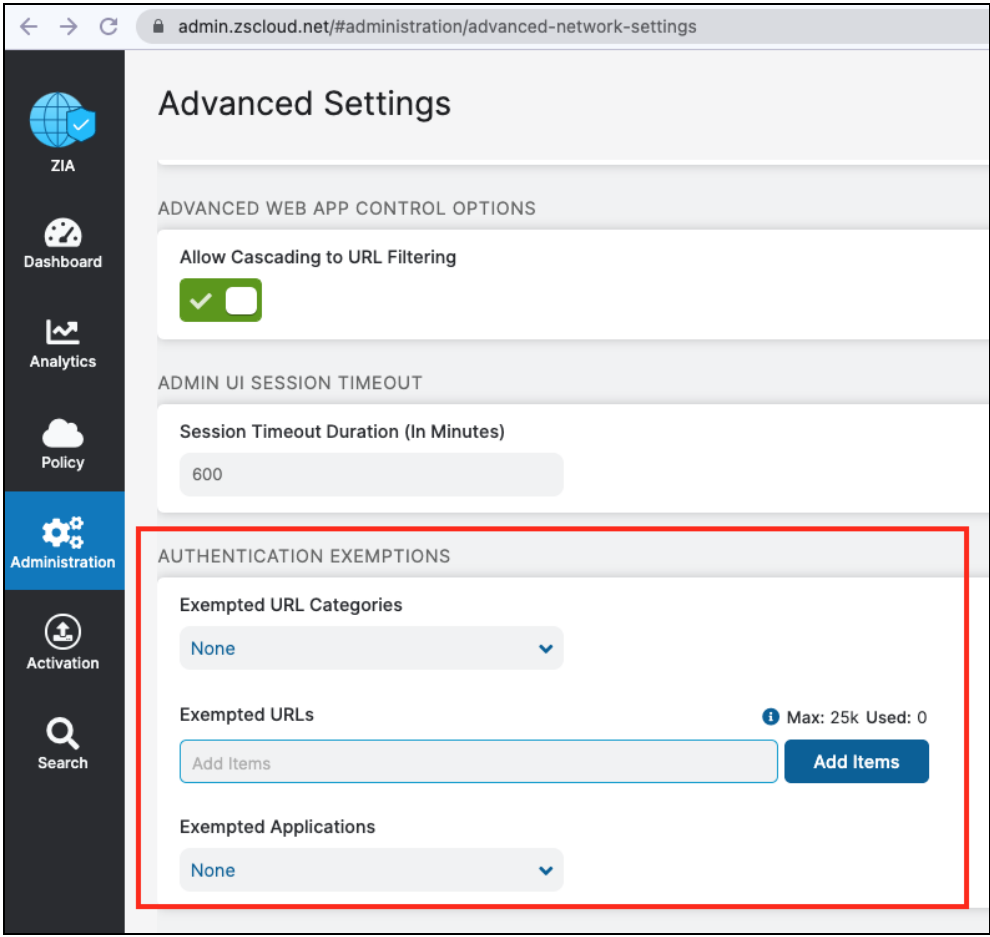
SSL Bypass

AND

User-Defined

SSL Bypass



Verify Authentication Server Exemptions	https://admin.zscloud.net/#administration/advanced-network-settings		Authentication traffic exemptions are needed to prevent authentication loops. In this example with no exempted URL Categories, URLs, or Applications it is very likely that authentication will be interfered with and fail.
Adjust Auth Server URL PAC File Direct Entry	<a href="https://admin.<cloud>.net/#administration/hosted-pac">https://admin.<cloud>.net/#administration/hosted-pac	<pre>if(shExpMatch(host, ██████████.okta.com") shExpMatch(host, ██████████oktacdn.com")) return "DIRECT";</pre>	In this example Okta is being used as the IdP. Rules in the PAC file are directing all web traffic to Zscaler, so this bypass is needed for the Okta IdP hosts.

ZIA: Authentication

Zscaler Client Connector Authentication - Troubleshoot No Authentication Policy Enforcement Error

Scenario/ Expected Result: User browses to a website from a location where Enforce Authentication is enabled. Logs should show them as the user on the transaction.

Problem: Authentication is not being enforced. Transaction logs show a generic looking username for an unauthenticated user.

Tips for avoiding this issue: Ensure that ZIA is configured to require authentication for all traffic. Get all users to use Client Connector (users must authenticate before forwarding traffic). Also ensure that an SSL inspection policy is in place that covers the URL.

No...	Event Time	User	
9	Sunday, May 16, 2021 1:33:53 AM	noauth-protocol\$@	zsccloud.net

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause								
Check SSL Inspection For Authentication Required Destination	https://admin.<cloud>.net/#insights/web	<table><tr><th>User</th><th>Location</th><th>URL</th><th>SSL Policy Reason</th></tr><tr><td>tara.tone@ziatrain.safemarch....</td><td>trgen</td><td>pbs.twimg.com/profile_images/147808198528...</td><td>Inspected</td></tr></table>	User	Location	URL	SSL Policy Reason	tara.tone@ziatrain.safemarch....	trgen	pbs.twimg.com/profile_images/147808198528...	Inspected	Web Insights log entries in this example show a real user name indicating that they were authenticated. SSL Policy Reason shows that the traffic is being SSL inspected. For an entry showing an unauthenticated user check the SSL Inspected and SSL Policy Reason fields for indications of it not being inspected because of SSL policies.
User	Location	URL	SSL Policy Reason								
tara.tone@ziatrain.safemarch....	trgen	pbs.twimg.com/profile_images/147808198528...	Inspected								
Check IP Surrogate Setting	https://admin.<cloud>.net/#administration/locations	<div>GATEWAY OPTIONS</div> <div>Use XFF from Client Request <input type="checkbox"/></div> <div>Enable IP Surrogate <input type="checkbox"/></div> <div>Enforce Authentication <input checked="" type="checkbox"/></div>	For tunneled traffic from a location there may be traffic that could be identified for the user that is being missed. Enable IP Surrogate to help add some context that may be helpful to identify the user.								



ZIA: Traffic Forwarding

Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Endpoint Firewall/ Antivirus Error

Scenario/ Expected Result: Service Status ON in Zscaler Client Connector Connectivity

Problem: Zscaler Client Connector shows *Endpoint FW/AV Error*.

Zscaler sends TCP/UDP probes on the default NIC on IP addresses 100.64.0.6 and 100.64.0.8 on TCP and UDP port 80 to check for Firewall(FW) or Antivirus(AV) blocks.

If the probe fails, Client Connector concludes this as an interruption from FW/AV application in the host machine and notifies it as **Endpoint FW/AV error** on Client Connector.

Service Status

ON |  TURN OFF

Service Status

Endpoint FW/AV Error
Off-Trusted Network

Tips for avoiding this issue:

- Check with the Desktop management team on the expected profile for the target devices in terms of VPN, firewall, antivirus, and endpoint protection agent configurations. See [Zscaler Client Connector Help - Interoperability](#)

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis
Verify Health Check Traffic Routing	Find-NetRoute -RemoteIPAddress 100.64.0.6 (Powershell)	PS C:\WINDOWS\system32> Find-NetRoute -RemoteIPAddress 100.64.0.6 IPAddress : 192.168.15.180 InterfaceIndex : 6 InterfaceAlias : Ethernet0	Client Connector health check traffic is routed to 100.64.0.6. In this case the result is good in that the InterfaceAlias shows that it is going out through the Ethernet0 interface. Wi-Fi would be another valid interface. A bad result would be If this health traffic is seen to be routed to a VPN adapter - that would need to be corrected.
Check Windows Firewall Connection Block	netsh advfirewall firewall show rule name = "Zscaler App Rule" verbose (Powershell)	PS C:\WINDOWS\system32> netsh advfirewall firewall show rule name = "Zscaler App Rule" verbose Rule Name: Zscaler App Rule ----- - Description: Allow incoming network traffic to ZSATunnel Enabled: Yes Direction: In Profiles: Domain,Private,Public Grouping: ZSATunnel Rule Group LocalIP: Any RemoteIP: Any Protocol: Any Edge traversal: No Program: C:\Program Files (x86)\Zscaler\ZSATunnel\ZSATunnel.exe InterfaceTypes: Any Security: NotRequired Rule source: Local Setting Action: Allow Ok.	Windows Firewall rule Zscaler App Rule is configured, enabled, and set to allow traffic to the ZSATunnel.exe process. Other resources: Zscaler Client Connector Processes to Allowlist

ZIA: Traffic Forwarding

Zscaler Client Connector Traffic Forwarding - Diagnose Client Connector Connection Failure

Scenario/ Expected Result: Zscaler Client Connector processes permitted to run on the user's device.

Problem: Endpoint protection solutions or other permission controls prevent Zscaler Client Connector from running.

Tips for avoiding this issue:

- Check with the Desktop management team on the expected profile for the target devices in terms of allowlists for Zscaler Client Connector operation. See <https://help.zscaler.com/z-app/zscaler-app-processes-allowlist>

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check Client Connector End User Device Connectivity - Process Permissions	Examine log file: C:\ProgramData\Zscaler\ZSAServ ice_<date>.log for signs of the ZSATray process being started and failing on each try to connect.	2020-09-25 15:06:29.709844(+0100)[10652:8028] DBG Created tray process 30496 for session 1 2020-09-25 15:06:30.711047(+0100)[10652:8028] INF send ZSATray Notification called 2020-09-25 15:06:30.711047(+0100)[10652:8028] DBG Failed to RPC connecting tray process 30496 for session 1. 30 2020-09-25 15:06:31.711480(+0100)[10652:8028] INF send ZSATray Notification called 2020-09-25 15:06:31.711480(+0100)[10652:8028] DBG Failed to RPC connecting tray process 30496 for session 1. 29 2020-09-25 15:06:32.711812(+0100)[10652:8028] INF send ZSATray Notification called 2020-09-25 15:06:32.711812(+0100)[10652:8028] DBG Failed to RPC connecting tray process 30496 for session 1. 28 2020-09-25 15:06:33.711853(+0100)[10652:8028] INF send ZSATray Notification called 2020-09-25 15:06:33.711853(+0100)[10652:8028] DBG Failed to RPC connecting tray process 30496 for session 1. 27 2020-09-25 15:06:34.712467(+0100)[10652:8028] INF send ZSATray Notification called 2020-09-25 15:06:34.712467(+0100)[10652:8028] DBG Failed to RPC connecting tray process 30496 for session 1. 26	ZSATray is being continuously killed and initiated. Endpoint protection solutions may not have been configured to allow the process to run.



ZIA: Traffic Forwarding

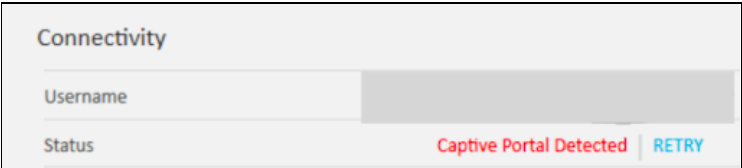
Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Captive Portal Detection Issue

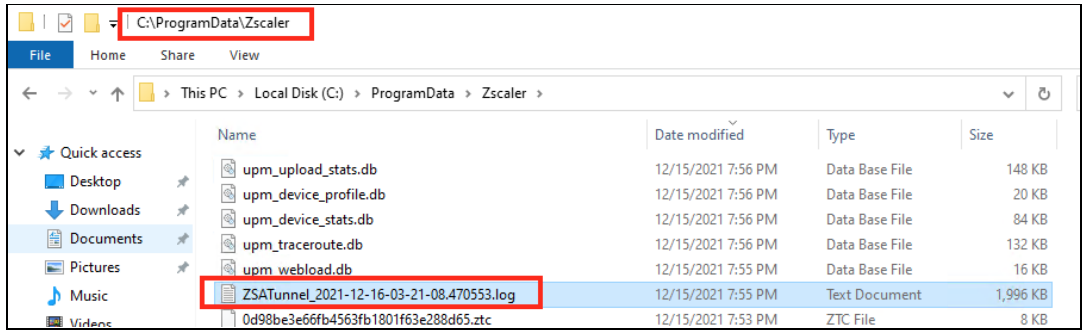
Scenario/ Expected Result: User connects their device to a new network and enrolls the device into Zscaler.

Problem: Zscaler Client Connector shows *Captive Portal Detected* error.

Device is connected to a network where users are redirected to a captive portal to manage their connection. Client Connector Connectivity Status displays **Captive Portal Detected** error. They may be on a public Wi-Fi point, or

Tips for avoiding this issue: Rollout plans should include steps for user awareness of captive portals on public Wi-Fi and the need to get connected before enrolling Client Connector into ZIA.



Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis
Check Captive Portal Detection Log Entry	Navigate to C:\Program Data\Zscaler and find the latest ZSATunnel.log		Sort by Date Modified to see the latest ZSATunnel log.
Check Captive Portal HTTP Response Code	Search for keyword “ detectCaptive ” in ZSATunnel log files.	DBG ZCPM detectCaptive: Response Status 204 Length: 0 DBG ZCPM detectCaptive: Captive not detected. INF ZCPM Captive portal not detected.	Client Connector reaches out to http://gateway.zscloud.net/generate_204 and expects an HTTP Connection Response Status 204. Response Status 302 indicates captive portal connection was detected instead.
Check reachability of Captive Portal Detection URL	curl <a href="http://gateway.<zscloud>.net/generate_204">http://gateway.<zscloud>.net/generate_204	PS C:\WINDOWS\system32> curl http://gateway.zscalertwo.net/generate_204 StatusCode : 204 StatusDescription : No Content Content : {} RawContent : HTTP/1.1 204 No Content Connection: close Content-Length: 0 Date: Mon Feb 14 21:33:37 2022 GMT	204 Response Status code indicates that the captive portal detection URL is reachable.

Check reachability to download default PAC file	curl http://pac.<zsccloud>.net/proxy.pac	PS C:\WINDOWS\system32> curl http://pac.zscalertwo.net/proxy.pac StatusCode : 200 StatusDescription : OK Content : {10, 9, 102, 117...} RawContent : HTTP/1.1 200 OK Connection: close Content-Type: application/x-ns-proxy-autoconfig function FindProxyForURL(url, host) { var privateIP = /^(0 10 127 192\.168 172\.1[6789] 172\.2[0-9] 172\.3... Headers : {[Connection, close], [Content-Type, application/x-ns-proxy-autoconfig]} RawContentLength : 2611	200 Response Status code indicates that the default PAC file download URL is reachable.
---	--	--	---

ZIA: Traffic Forwarding

Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Network Error

Scenario/ Expected Result: User authenticates and device is enrolled in Zscaler.


Problem: Zscaler Client Connector shows Network Error

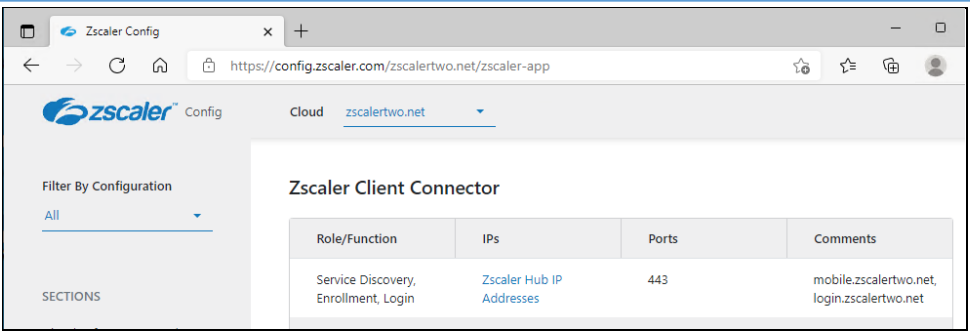
Zscaler Client Connector is unable to connect to the Zscaler cloud. Connectivity issues between the user's device and the Zscaler mobile server **mobile.<cloudname>.net** .



Tips for avoiding this issue:

- 1. Check that Zscaler Client Connector has **unrestricted outbound access to the Internet on port 443**. This is needed to ensure access to all Zscaler nodes as the infrastructure evolves and expands.
- 2. Click **Retry** to see if the issue was temporary. if retry doesn't fix the issue use the tools shown below to diagnose and further isolate the issue.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis
Retry the network connection	Client Connector: Internet Security / Private Access -> Connectivity -> Service Status -> Retry		Users see the Retry button displayed in Zscaler Client Connector when a connection cannot be established to the Zscaler cloud.
Check outbound connectivity to mobile.<cloudname>.net:443	Test-NetConnection -ComputerName mobile.<cloudname>.net -Port 443 (Powershell)	PS C:\> Test-NetConnection -ComputerName mobile.zscalertwo.net -Port 443 ComputerName : mobile.zscalertwo.net RemoteAddress : 104.129.202.233 RemotePort : 443 InterfaceAlias : Ethernet0 SourceAddress : 192.168.15.180 TcpTestSucceeded : True	Run from the user's device, this example shows that the needed access to the Zscaler cloud (Zscalertwo in this case) is available on port 443 .
Check Host Name Resolution for mobile.<cloudname>.net	nslookup mobile.<cloudname>.net (Command Prompt or Powershell)	PS C:\WINDOWS\system32> nslookup mobile.zscalertwo.net ... Non-authoritative answer: Name: mobile.zscalertwo.net Addresses: 104.129.202.233 104.129.202.231	Run from the user's device, this example shows that the mobile server host name is being properly resolved.
Diagnose Host Not Found DNS Failure	Examine log file: C:\ProgramData\Zscaler\ZSATray_<date>.log for ERROR entries.	Sample Log Entry: #NORMAL #ERROR : Error checking updates: { "error":-8, "errorMessage": " Host not found. mobile.zscalertwo.net ", "response": "", "success": "false" }	Retry failed. Log file shows DNS resolution to mobile.<cloudname>.net is failing.
Diagnose Connection Reset by Peer Failure	Examine log file: C:\ProgramData\Zscaler\ZSATray_<date>.log for ERROR entries.	Sample Log Entry: #NORMAL #ERROR : Error checking updates: { "error":-8, "errorMessage": " Connection reset by peer. ", "response": "1.4.3.1", "success": "false" }	Retry failed. Log file shows connectivity from user's device and Mobile Server has been intercepted

Check connectivity to Zscaler cloud	Find service discovery and login hosts for each cloud at: https://config.zscaler.com/zscaler.net/zscaler-app	 <table><thead><tr><th>Role/Function</th><th>IPs</th><th>Ports</th><th>Comments</th></tr></thead><tbody><tr><td>Service Discovery, Enrollment, Login</td><td>Zscaler Hub IP Addresses</td><td>443</td><td>mobile.zscalertwo.net, login.zscalertwo.net</td></tr></tbody></table>	Role/Function	IPs	Ports	Comments	Service Discovery, Enrollment, Login	Zscaler Hub IP Addresses	443	mobile.zscalertwo.net, login.zscalertwo.net	Cloud selected in this example is zscalertwo.net Hosts that must be reachable are: mobile.zscalertwo.net login.zscalertwo.net They will respond to ping if they are reachable from the user's device.
Role/Function	IPs	Ports	Comments								
Service Discovery, Enrollment, Login	Zscaler Hub IP Addresses	443	mobile.zscalertwo.net, login.zscalertwo.net								
Diagnose No Route To Host Failure	Examine log file: C:\ProgramData\Zscaler\ZSATray_<date>.log for ERROR entries.	Sample Log Entry: #NORMAL #ERROR : Error checking updates: {"error":-8,"errorMessage":" Net Exception. No route to host ","response":"","success":"false"}	Retry failed. Log file shows Zscaler Couldn't find a route to mobile.<cloudname>.net in the routing table.								
Diagnose Network is Unreachable Failure	Examine log file: C:\ProgramData\Zscaler\ZSATray_<date>.log for ERROR entries.	Sample Log Entry: #NORMAL #INFO : Keep Alive Response: {"error":-8,"errorMessage":" Net Exception. Network is unreachable ","success":"false"}	Retry failed. Log file show that Zscaler Client Connector is unable to reach mobile.<cloudname>.net								
Diagnose Certificate Validation Error	Examine log file: C:\ProgramData\Zscaler\ZSATray_<date>.log for ERROR entries.	Sample Log Entry: #NORMAL #INFO : Keep Alive Response: {"error":-8,"errorMessage":" Net Exception. Network is unreachable ","success":"false"}	Traffic to mobile.<cloudname>.net , should not be intercepted. This error may be caused by an intermediate device performing SSL Decryption.								

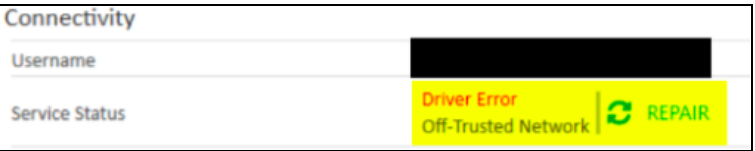


ZIA: Traffic Forwarding

Zscaler Client Connector Traffic Forwarding - Troubleshoot Client Connector Driver Error

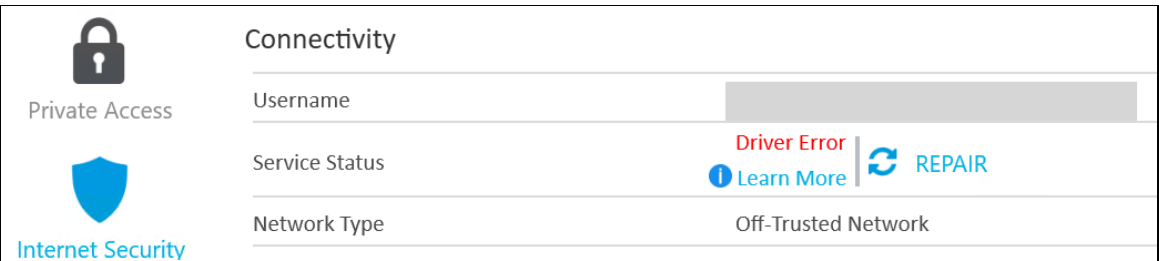
Scenario/ Expected Result: Zscaler User sees “Driver error” on Zscaler Client Connector, repair option does not help.

Problem: Driver Error issue occurs when the files are corrupted.



Uninstalling and reinstalling the Zscaler Client Connector, without rebooting the machine after uninstallation may result in Driver Error on the Zscaler Client Connector.

Tips for avoiding this issue:

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis
Repair Client Connector Driver Error	In the More window, click Repair. This option is available under the Troubleshoot menu.		When an error is detected the REPAIR option is offered to enable the application to try and recover. If the repair option continues to report a driver error the application may need to be reinstalled.
Re-install Client Connector	MSI package - Reinstall Zscaler Client Connector and force the driver re-installation using the command line option REINSTALLDRIVER=1 . See help.zscaler.com topic on Customizing Zscaler Client Connector with Install Options for EXE		
Re-install Client Connector (Manual)	Perform a fresh install manually Uninstall the Zscaler Client Connector from the user device. See help.zscaler.com topic on Manually uninstall Zscaler Client Connector on Windows Delete the mentioned folders at the following location: C:\Windows\System32\DriverStore\FileRepository zapprd.inf_xxxxxxx ztap.inf_xxxxxxx		

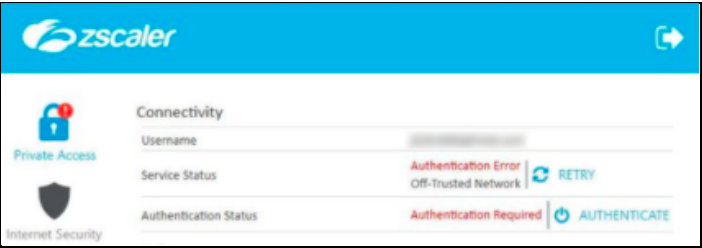
ZIA: Traffic Forwarding

Troubleshoot Internet Traffic Forwarding - Check ZIA Public Service Edge Routing

Scenario/ Expected Result: Internet traffic should be routed to the closest Zscaler data center.

Problem: Traffic is routed to a node that is geographically distant from the user's location. User asks "Why do I get sent to LAX1 when I'm in Atlanta?"

Tips for avoiding this issue: Recognize that traffic routing can be very dynamic and is influenced potentially by many factors. Stay aware of outages or issues that are prompting temporary changes to keep services working. Be able to quantify if the routing has any measurable impact on the user's experience. Check the user's DNS settings as well since users may configure something like 8.8.8.8 which is based in California and could incorrectly influence traffic routing.



Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check GeoIP Coordinates	<code>https://ip.zscaler.com/</code> <code>http://www.maxmind.com</code>	A screenshot of the ip.zscaler.com website. It shows a message: "You are accessing the Internet via Zscaler Cloud: Vancouver I in the zscalertwo.net cloud." Below this, it lists IP address, proxy virtual IP, Zscaler proxy virtual IP, Zscaler hostname, and gateway IP address. At the bottom, there is a table titled "GeoIP2 Precision: City Results" with columns: IP Address, Country Code, Location, Network, Postal Code, and Approximate Coordinates*. The row shows IP 207.102.188.167, Country Code CA, Location Kelowna, British Columbia, Network 207.102.188.160/28, Postal Code V1P, and Approximate Coordinates 49.8959, -119.1724.	Cross-reference the maxmind coordinates of egress IP against the MaxMind Database. If MaxMind has incorrect coordinates, you can submit a GeoIP data correction request with MaxMind. Alternatively, You can open a case with Zscaler Support to override MaxMind coordinates to route to the closest Zscaler Primary DC.
Check Zscaler Data Center Health	<code>https://trust.zscaler.com/cloud-status</code>	A screenshot of a "Datacenter Issue" status page. It shows "Status: Resolved" and a message: "We are investigating an issue with our datacenter. If you're currently experiencing any traffic impacting issues, please reach out to Zscaler Support." Below this, it shows an "Update - Wed, 15 Dec 2021 17:53:57 UTC" and a message: "This incident has been resolved. Please contact Zscaler Support if you have additional questions." At the bottom, it shows "Started at: Wed, 15 Dec 2021 16:10:09 UTC" and "Ended at: Wed, 15 Dec 2021 17:53:57 UTC".	This example was for a two hour period in a Montreal DC. If users noticed issues it might have already failed over to the secondary, so by the time they checked they might have seen their traffic going to a distant data center. They might conclude (incorrectly) that this was the cause of any issues they were seeing. History from the Trust site helps to fill in the context for what they may have experienced.
Check Service Edge Connection Timeout	<code>https://admin.<cloud>.net/#administration/hosted-pac</code>	<code>return "PROXY \${GATEWAY}:9490; PROXY \${SECONDARY_GATEWAY}:9400; DIRECT";</code>	In this example there is a typo in the primary gateway port (9490 instead of 9400). This would cause a poor user experience while the connection times out and then fails over to the secondary.
Check Service Edge Subcloud	<code>https://help.zscaler.com/zia/what-subcloud</code> <code>https://admin.<cloud>.net/#administration/hosted-pac</code>	<code>\${GATEWAY.Europe.zscaler.net}</code> and <code>\${SECONDARY.GATEWAY.Europe.zscaler.net}</code>	In this example users are restricted by the PAC file to Service Edges in a specific set of nodes in a subcloud called Europe. If the subcloud does not include nodes close to the user's location it may cause issues.



ZIA: Traffic Forwarding

Troubleshoot Internet Traffic Forwarding - Troubleshoot ZIA Network Infrastructure Issues

Scenario/ Expected Result: Traffic is being forwarded to a Zscaler Public Service Edge

Problem: Traffic is blocked by an intermediate device or some other failure.

Tips for avoiding this issue: Review and be familiar with the resources available on trust.zscaler.com and config.zscaler.com that provide updates and status of all Zscaler infrastructure.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause																																																																																																
Troubleshoot ZIA Network Outage	<div>https://trust.zscaler.com/cloud-status</div>	<div><div><div><div><div><div>zscaler</div><div>TRUST</div></div><div><div>ZscalerTwo.net</div><div>SupportRSSSign InSubscribe</div></div></div></div><div><div>Cloud Overview</div><div>Cloud Status</div><div>Maintenance</div><div>Incidents</div><div>Advisories</div><div>URL Category Notifications</div><div>Data Center Map</div></div><div>CLOUD STATUS</div><div><div>CORE CLOUD SERVICES</div><div><div>< Previous 7 Days</div><div>Next 7 Days ></div></div><table><thead><tr><th>Service</th><th>Feb 8</th><th>Feb 9</th><th>Feb 10</th><th>Feb 11</th><th>Feb 12</th><th>Feb 13</th><th>Feb 14</th></tr></thead><tbody><tr><td>Remote Browser Isolation</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Traffic Forwarding</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Zscaler Cloud Connector Portal</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Authentication</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>DNS</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>PAC</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Nanolog</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Admin UI</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Partner Admin UI</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Zscaler Client Connector Admin</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Security</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table></div></div></div>	Service	Feb 8	Feb 9	Feb 10	Feb 11	Feb 12	Feb 13	Feb 14	Remote Browser Isolation								Traffic Forwarding								Zscaler Cloud Connector Portal								Authentication								DNS								PAC								Nanolog								Admin UI								Partner Admin UI								Zscaler Client Connector Admin								Security								<div>Status the current week on Zscalertwo.net (selected in the list at the top).</div> <div>In this example we see everything has been available except for a noted outage related to the Admin UI on Feb 8.</div>
Service	Feb 8	Feb 9	Feb 10	Feb 11	Feb 12	Feb 13	Feb 14																																																																																												
Remote Browser Isolation																																																																																																			
Traffic Forwarding																																																																																																			
Zscaler Cloud Connector Portal																																																																																																			
Authentication																																																																																																			
DNS																																																																																																			
PAC																																																																																																			
Nanolog																																																																																																			
Admin UI																																																																																																			
Partner Admin UI																																																																																																			
Zscaler Client Connector Admin																																																																																																			
Security																																																																																																			
Troubleshoot Zscaler Public Service Edge Issue	<div>https://config.zscaler.com/cloud/cenr</div> <div>https://config.zscaler.com/cloud/zia-sedge</div>	<div><div>ZIA Service Edge Access Requirements</div><div>In order to make certain that the ZIA Service Edge works correctly in your environment, please ensure that your ACL configuration allow the types of traffic necessary. Refer to the following tables for more details.</div><table><thead><tr><th>Rule Name</th><th>Rule</th><th>Protocol, Port</th><th>From</th><th>Source</th></tr></thead><tbody><tr><td colspan="5">Inbound Requirements</td></tr><tr><td rowspan="2">Inbound Active Service Monitor</td><td>Allow</td><td>TCP ANY, ICMP</td><td>from</td><td>Zscaler HUB IP Address</td></tr><tr><td>Allow</td><td>UDP 500, 4500</td><td>from</td><td>Zscaler HUB IP Address</td></tr><tr><td rowspan="2">Inbound Traffic Forwarding</td><td>Allow</td><td>TCP 80, 443, 8080, 8800, 9400, 9443, 9480, Custom Customer Ports</td><td>from</td><td>ANY</td></tr><tr><td>Allow</td><td>UDP 500, 4500</td><td>from</td><td>ANY</td></tr></tbody></table></div>	Rule Name	Rule	Protocol, Port	From	Source	Inbound Requirements					Inbound Active Service Monitor	Allow	TCP ANY, ICMP	from	Zscaler HUB IP Address	Allow	UDP 500, 4500	from	Zscaler HUB IP Address	Inbound Traffic Forwarding	Allow	TCP 80, 443, 8080, 8800, 9400, 9443, 9480, Custom Customer Ports	from	ANY	Allow	UDP 500, 4500	from	ANY	<div>Public IPs and all of the access needed for communications with service edges are listed on these pages.</div>																																																																				
Rule Name	Rule	Protocol, Port	From	Source																																																																																															
Inbound Requirements																																																																																																			
Inbound Active Service Monitor	Allow	TCP ANY, ICMP	from	Zscaler HUB IP Address																																																																																															
	Allow	UDP 500, 4500	from	Zscaler HUB IP Address																																																																																															
Inbound Traffic Forwarding	Allow	TCP 80, 443, 8080, 8800, 9400, 9443, 9480, Custom Customer Ports	from	ANY																																																																																															
	Allow	UDP 500, 4500	from	ANY																																																																																															

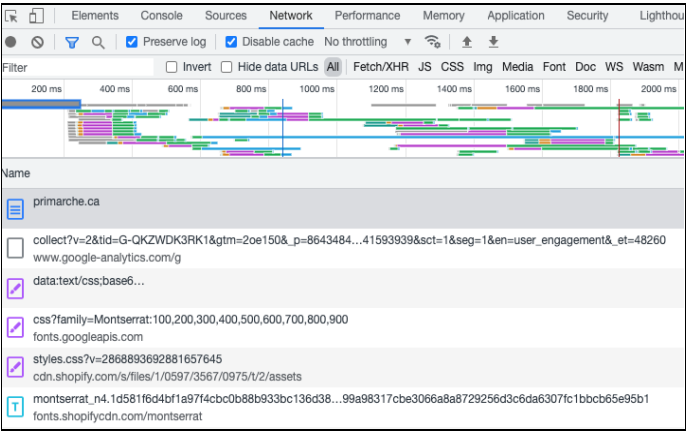
ZIA: Policy

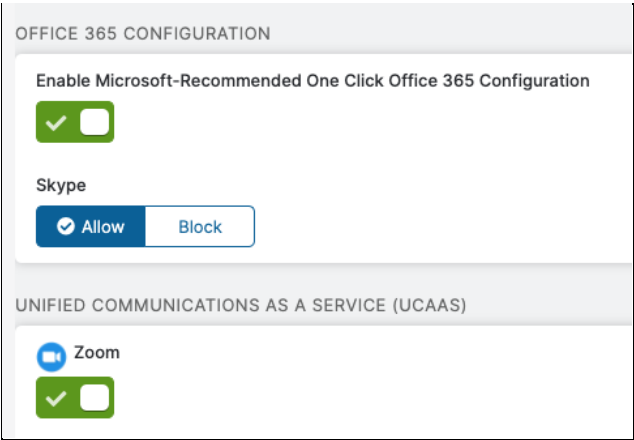
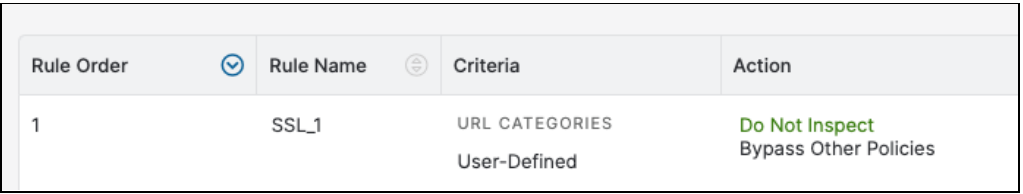
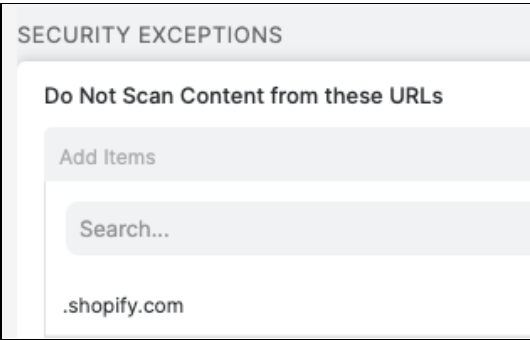
Troubleshoot Internet Application Access - Check Inspection Policy Bypass/ Failure

Scenario/ Expected Result: Access to a specific URL is expected to be controlled by a policy that defines what the user may or may not access.

Problem: A user is either allowed to access a website they should not be able to access, or they are restricted from accessing a site they should be able to access.

Tips for avoiding this issue: Configure the SSL inspection policies to inspect as much of the traffic as possible, since any traffic that bypasses SSL inspection could also potentially be missed by other types of rules that need the context about the user or the transaction that are encrypted. Keep policies as simple and as specific as possible, and try to minimize the use of bypasses and exceptions. Always check the Web Insights log entry for a transaction to get insight into all of the factors that may be affecting access.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check CDN URLs in HTTP Header Trace	In Chrome: View > Developer > Developers Tools - Network Tools		<p>In this example the network view of the HTTP transactions shown in the developer tools view shows that the shopping site (<i>primarche.ca</i>) uses cdn.shopify.com to deliver site content.</p> <p>There could be issues with access controls for <i>primarche.ca</i> if they are bypassed or overridden by other rules that govern the delivery of <i>cdn.shopify.com</i>.</p>
Check SSL Inspection Bypass	https://admin.<cloud>.net/#policy/web/ssl-inspection	<div><div>Default SSL Inspection Rule</div><div>Any</div><div>Do Not Inspect Evaluate Other Policies Show End User Notifications Enabled Untrusted Server Certificates Allow OCSP Revocation Check Disabled Minimum TLS Version TLS 1.0</div></div>	<p>Any traffic hitting this rule will not be SSL inspected. Ensure that there are other rules higher in the list that will ensure that inspection is done for all traffic that should not be explicitly excluded from inspection.</p> <p>If an expected policy is not being enforced on some traffic it could be that URL categorization or Cloud App identification end up being too general to match the criteria in a URL Filtering or Cloud App control rule. Always check the Web Insights log entries for the traffic to see if it is being SSL inspected or not.</p>
Check URL Inspection Bypass	https://admin.<cloud>.net/#administration/url-categories	<div>Custom URLs</div> <div>Add Items</div> <div>Search...</div> <div>.safemarch.com</div>	<p>Traffic for any <i>safemarch.com</i> URL would match this URL category. Typically this might be done to include this category in a URL Filtering <i>Allowlist</i> type rule that permits traffic to these destinations. All traffic to <i>safemarch.com</i> would match this URL category and any corresponding URL Filtering rule using the category in its criteria.</p>

			Always check for custom URL categories and the URLs and wildcards defined to be aware of traffic that may be included in a rule that bypasses the required policy.
Check Cloud App Inspection Bypass	<a href="https://admin.<cloud>.net/#policy/web/url-and-cloud-app-control">https://admin.<cloud>.net/#policy/web/url-and-cloud-app-control (Advanced Policy Settings tab)		Policy exceptions configured here for Office 365, Skype, and UCAAS such as Zoom will bypass all inspections. If there was a more granular Cloud App Control Policy rule in place to block something specific like OneDrive for a group of users, this would override that rule and OneDrive access would be allowed.
Check SSL Bypass List	<a href="https://admin.<cloud>.net/#policy/web/ssl-inspection">https://admin.<cloud>.net/#policy/web/ssl-inspection		This SSL inspection rule would bypass inspection for any URLs in the User-Defined URL categories. Be sure to check what is in the user-defined categories to know what will be bypassed.
Check SSL Wildcard Domains Bypass	https://help.zscaler.com/zia/url-format-guidelines	.safemarch.com	This would match almost anything in safemarch.com. For example: <ul style="list-style-type: none">atlanta.safemarch.comserv1.atlanta.safemarch.com/webinarsapp.safemarch.com:10443 A leading period (".") functions as a wildcard to the left of the named URL. Note that the asterisk ("*") character is not used as a wildcard.
Check Inspection Bypass List	Policy > Malware Protection and Policy > Advanced Threat Protection (Security Exceptions tabs)		.shopify.com could have been added to a category that is being used in an inspection bypass to work around an access issue for a page on the shopify.com domain. Unfortunately this matches something like cdn.shopify.com , which could be the content distribution network for content for many other sites that use the Shopify platform for delivering their web apps.

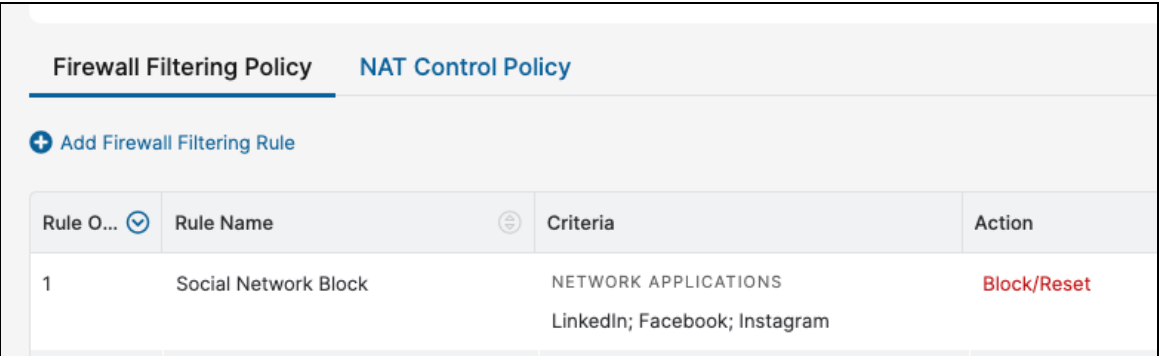
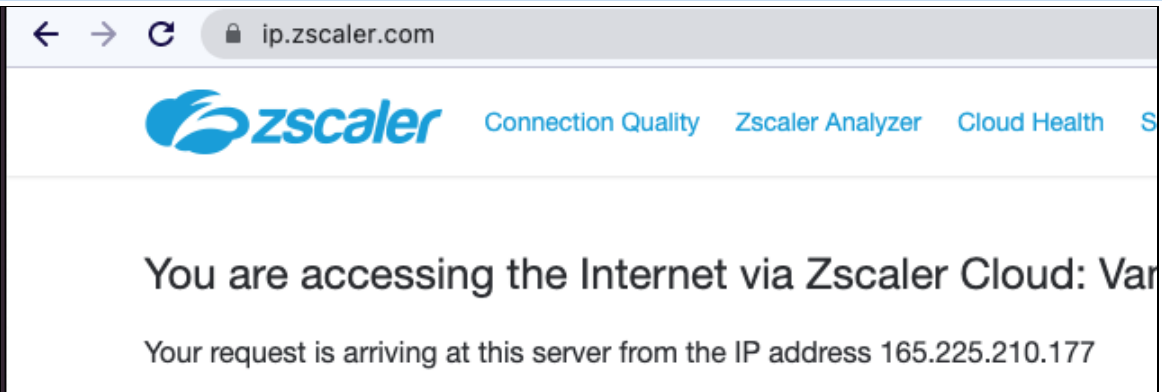
ZIA: Policy

Troubleshoot Internet Application Access - Troubleshoot Website Loading Issue

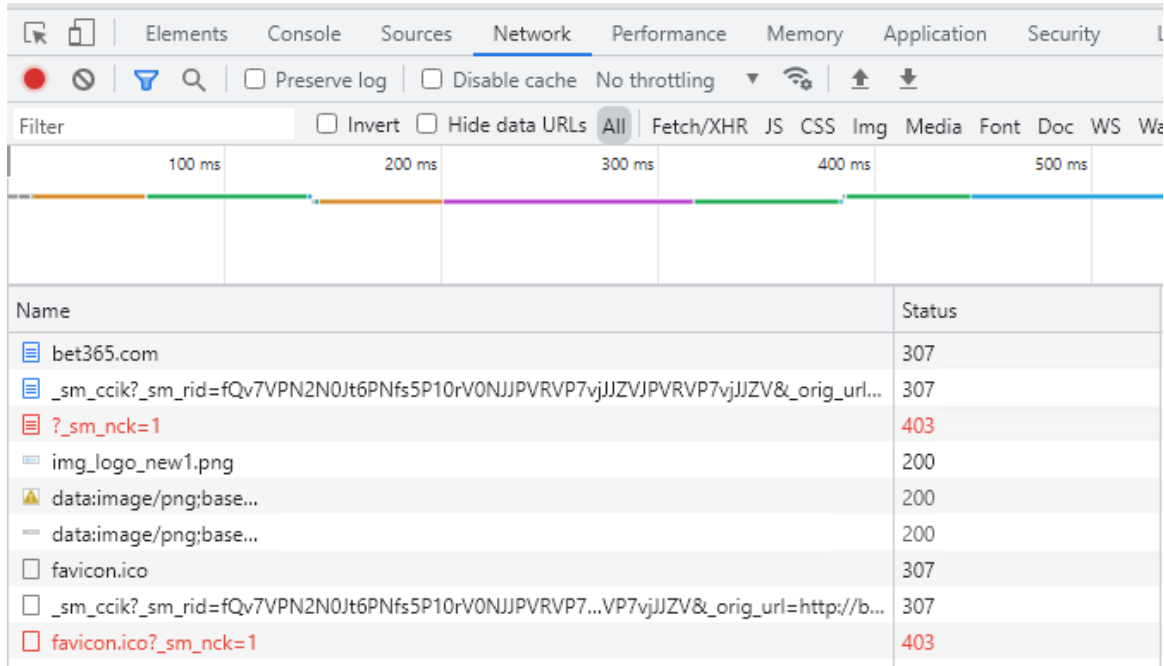
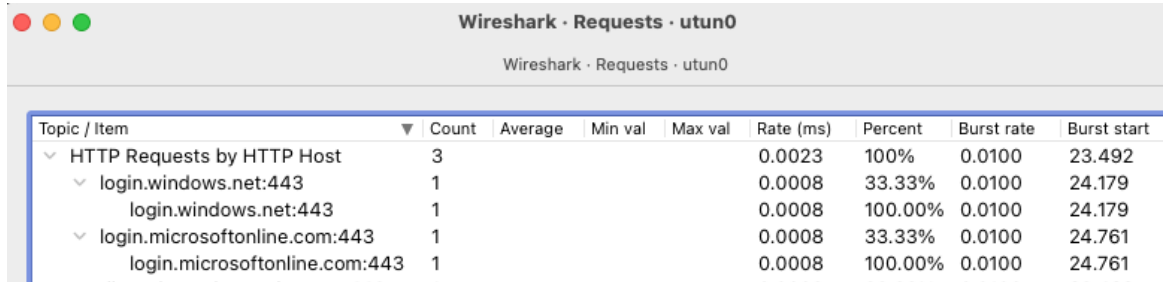
Scenario/ Expected Result: User should be able to connect to a website according to the policies in place.

Problem: Website is unreachable through Zscaler.

Tips for avoiding this issue: Check for overlaps between firewall and URL and Cloud App rules for conflicting blocks. Best practices of keeping the rule sets small and as specific as possible will help to avoid hidden conflicts.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check Network Access Control List (ACL) Blocks	https://admin.<cloud>.net/#policy/firewall/firewall-control		<p>Even if LinkedIn was permitted by the URL & Cloud App control policies, the traffic would be blocked by this firewall rule.</p> <p>Firewall rules are evaluated and applied before further inspection of web content and application of other rules.</p>
Check Destination Webmaster Denylist	https://ip.zscaler.com/		<p>Content is being proxied by Zscaler via 165.225.210.177. Check with the host or public checking sites that access is not being denied based on traffic originating from that IP.</p>



Analyze Internet Access Issue HTTP Headers File Capture	In Chrome: View > Developer > Developers Tools - Network Tools		<p>There is a lot of useful information in the Network view that is helpful for tracking down web access issues. In this example HTTP 307 - Temporary Redirect and 403 - Forbidden responses indicate access controls are being applied.</p> <p>Timing data also will show where there may be timeouts or long delays.</p> <p>Download and save this data in an HTTP Archive (HAR) file to have a record for further analysis if needed.</p>
Analyze Internet Access Issue Packet Capture	In Wireshark: Statistics > HTTP > Requests		<p>Wireshark has some tools in the Statistics and Analysis menus that can help to isolate transactions of interest and see related details. In this example the HTTP Requests summary shows hosts that are being requested and related details for each host.</p>

ZPA: Authentication

Zscaler Client Connector Authentication - Check ZPA Authentication

Scenario/ Expected Result: SAML attributes for enrolled users are received in ZPA and available as criteria of use in policies.

Problem: SAML attributes are not received or have incorrect details.

Tips for avoiding this issue: Test the receipt of SAML attributes when initially configuring the Identity Provider relationship with ZPA.

Connection

START TIME

Feb 15th, 10:27:51.048 PST

END TIME

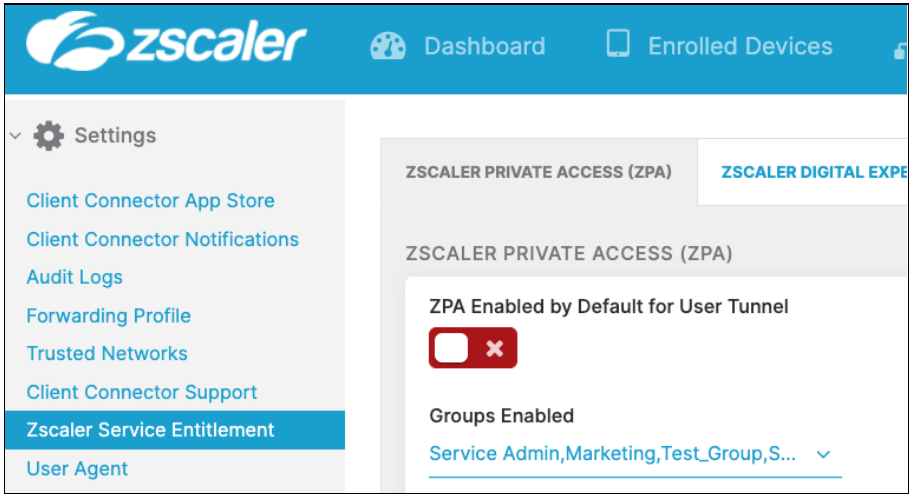
Feb 15th, 10:27:51.068 PST

STATUS CODE

CA: Application is not reach...

INTERNAL STATUS CODE

APP_NOT_REACHABLE

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check ZPA Enablement on Mobile Portal	Client Connector Portal -> Administration -> Zscaler Service Entitlement		In this example ZPA is set up for user in the groups selected (Service Admin, Marketing, Test_Group, etc.)
Verify User SAML Setup	<p>Access this link from the user's device while enrolled into ZPA. Substitute the real value for CUSTOMERDOMAIN</p> <p><code>https://samlsp.private.zscaler.com/auth/v2/login?domain=CUSTOMERDOMAIN.TLD&ssotype=test</code></p> <p>For Admin users authenticated via SAML the link is different:</p> <p><code>https://adminsamlsp.private.zscaler.com/auth/v2/login?domain=CUSTOMERDOMAIN&ssotype=test</code></p>	<p><code>https://samlsp.private.zscaler.com/auth/v2/login?domain=training.safemarch.com&ssotype=test</code></p> <pre>{ "nameid": "katsu.kay@training.safemarch.com", "orgId": null, "idpEntityID": null, "idpId": null, "saml_attributes": { "http://schemas.microsoft.com/identity/claims/tenantid": "5a934f03-f005-4f48-95b5-f304bf2353ef", "http://schemas.microsoft.com/identity/claims/objectidentifier": "21b63e09-cadd-46b5-bf35-b7085bae9962", "http://schemas.microsoft.com/identity/claims/displayname": "Katsu Kay", "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/5a934f03-f005-4f48-95b5-f304bf2353ef/", "http://schemas.microsoft.com/claims/authnmethodsreferences": "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "Katsu", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Kay", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "katsu.kay@training.safemarch.com", "Department": "Building & Grounds" }, "samlassertion": null }</pre>	<p>This response shows details returned for the user shown (katsu.kay@training.safemarch.com) on the training.safemarch.com domain. It shows:</p> <p>givenname: Katsu surname: Kay name: katsu.kay@training.safemarch.com Department: Buildings & Grounds</p>



ZPA: Traffic Forwarding

Troubleshoot Private Application Traffic Forwarding - Troubleshoot ZPA Application Traffic Failure

Scenario/ Expected Result: Access policies are configured for a user to be able to access a private application.

Problem: User is unable to access a private application. ZPA Diagnostics Data shows status code such as *CA: Application not reachable* .

Tips for avoiding this issue: App connector VM should be installed on the same network segment as the application server and be set to use the DNS server that will resolve the application host names.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Test Application Host Reachability From App Connector	From the App Connector: ping <app fully qualified domain name>	[admin@zpa-connector ~]\$ ping intranet.patrainig.safemarch.com PING intranet.patrainig.safemarch.com (10.0.0.9) 56(84) bytes of data. 64 bytes from host-1.patrainig.safemarch.com (10.0.0.9): icmp_seq=1 ttl=128 time=2.68 ms	Ping response shows that the DNS lookup of the app server host name (intranet.patrainig.safemarch.com) resolved to 10.0.0.9. Also the ping response indicates that the connector can reach the app server.
Test App Connection From App Connector	From the App Connector: telnet <app fully qualified domain name> <port>	[admin@zpa-connector ~]\$ telnet 10.0.0.9 443 Trying 10.0.0.9... Connected to 10.0.0.9. Escape character is '^]'. 	App connector is able to reach the server at 10.0.0.9 and connect on port 443.

ZPA: Traffic Forwarding

Troubleshoot Private Application Traffic Forwarding - Troubleshoot App Connector

Scenario/ Expected Result: App Connector starts and is enrolled for use within ZPA.

Problem: zpa-connector status shows enrollment error. Messages such as cannot decrypt data indicated issues with the provisioning key.

Tips for avoiding this issue: Check zpa-connector status after initial provisioning. Issues with incorrect or corrupted keys will usually result from issues in copying the provisioning key.

```
[root@zpa-connector var]# systemctl status zpa-connector
● zpa-connector.service - Zscaler Private Access Connector
   Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2018-01-31 16:14:54 UTC; 26min ago
     Main PID: 11955 (zpa-connector)
    CGroup: /system.slice/zpa-connector.service
            └─11955 /opt/zscaler/bin/zpa-connector

Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: zpa-connector-child: starting, version 17.62.1
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: SSL version: OpenSSL 1.0.2k  26 Jan 2017
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: Libevent version: 2.0.22-stable
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: Connector version: 17.62.1
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: Checking Enrollment
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: Cannot decrypt data from instance_id.crypt
Jan 31 16:15:06 zpa-connector zpa-connector-child[12018]: Cannot get instance id
Jan 31 16:15:08 zpa-connector zpa-connector[11955]: zscaler-update: zpa-connector-child exited too fast, was running for 3 seconds
Jan 31 16:15:08 zpa-connector zpa-connector[11955]: zscaler-update: zpa-connector-child failed too many times in a row- reverting to default software
Jan 31 16:15:08 zpa-connector zpa-connector[11955]: zscaler-update: zpa-connector-child Default software failing; waiting 12 hours for smoke to clear
```

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check App Connector Enrollment	<div>1) Create a new provisioning key in the ZPA Admin portal</div> <div>2) Stop zpa-connector: \$ sudo systemctl stop zpa-connector</div> <div>3) Remove old key data: \$ sudo find "/opt/zscaler/var" -mindepth 1 -delete</div> <div>4) Add in the new provisioning at: sudo cp provision_key /opt/zscaler/var/</div> <div>5) Restart zpa-connector \$ sudo systemctl stop zpa-connector</div>	<div>[admin@zpa-connector ~]\$ sudo systemctl stop zpa-connector</div> <div>[admin@zpa-connector ~]\$ sudo find "/opt/zscaler/var" -mindepth 1 -delete</div> <div>[admin@zpa-connector ~]\$ sudo cp provision_key /opt/zscaler/var/</div> <div>[admin@zpa-connector ~]\$ sudo systemctl start zpa-connector</div> <div>[admin@zpa-connector ~]\$ sudo systemctl status zpa-connector</div> <div>● zpa-connector.service - Zscaler Private Access Connector</div> <div> Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: enabled)</div> <div> Active: active (running) since Tue 2022-02-15 10:57:58 PST; 11s ago</div> <div> Main PID: 3982 (zpa-connector)</div> <div> CGroup: /system.slice/zpa-connector.service</div> <div> └─3982 /opt/zscaler/bin/zpa-connector</div> <div> └─3990 zpa-connector-child</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Initializing assista...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Assistant capability...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Adding name resoluti...</div> <div>Feb 15 10:58:09 zpa-connector zpa-connector-child[3990]: Waiting for connecto...</div>	Clearing out the files in the /opt/zscaler/var directory removes files that were generated using the old provisioning key. After the new key was copied in the zpa-connector process restarted and was able to enroll in ZPA.



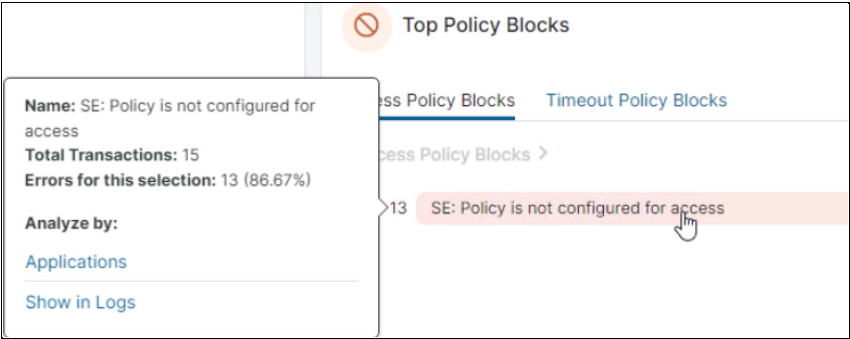
ZPA: Policy

Troubleshoot Private Application Access - Diagnose Private Application Access Error

Scenario/ Expected Result: User is granted access to a private application.

Problem: User is unable to access the application, and ZPA diagnostics indicate that a policy is not configured.

Tips for avoiding this issue: Check the configured access policies to be aware of what has been configured as criteria. Check that users and devices will meet any criteria related to device posture, trusted networks, or SCIM attributes configured in the access rules.



Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Diagnose SE: Policy Not Configured For Access Error	Expand to log entry in the Diagnostics view of the ZPA Admin Portal. Check for indications of underlying errors or unresolved references. For example the User Metadata will show information on criteria such as SCIM attributes, posture profiles, and trusted networks.	<div>User ⓘ</div> <div>Client Connector ⚙</div> <div>▼ USER METADATA ⓘ</div> <div>IDP NAME</div> <div>Azure ⚙</div> <div>IDP ID</div> <div>144133929165651981 ⓘ</div> <div>SAML ATTRIBUTES</div> <div>👁 ⬇️ ⓘ</div> <div>SCIM USERS</div> <div>Unavailable</div> <div>SCIM GROUPS</div> <div>Unavailable</div> <div>HOSTNAME</div> <div>Disabled</div> <div>PLATFORM</div> <div>windows</div> <div>CLIENT CONNECTOR TRUSTED NETWORKS ⓘ</div> <div>Unavailable</div> <div>POSTURE PROFILES VERIFIED ⓘ</div> <div>Unavailable</div> <div>POSTURE PROFILES UNVERIFIED ⓘ</div> <div>Windows Domain Joined (zscloud.net)</div> <div>144133929165652165 ⓘ</div>	Posture profile evaluation result in this example shows that the device posture was evaluated against the criteria of needing to be a domain joined device, and this was not verified. This provides context for examining the configured access policy to see what criteria are configured for access. In this case since the device was not domain joined it did not match the criteria for access and the unsuccessful attempt was logged.

ZPA: Policy

Troubleshoot Private Application Access - Check Private Application Reachability

Scenario/ Expected Result: User is granted access to a private application.

Problem: Unable to access application and ZPA diagnostic logs show error “SE: Policy not configured for access”

Tips for avoiding this issue: Ensure that testing exercises all of the access rules to all of the configured apps. Check Client Connector logs and diagnostic results to see what criteria are checked and the results for each test.

Connection

START TIME

Feb 15th, 10:27:10.660 PST

END TIME

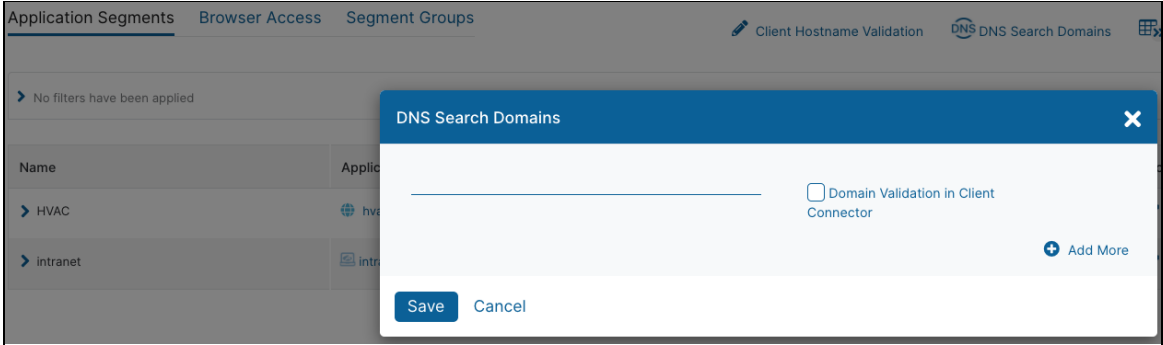
Feb 15th, 10:27:10.660 PST

STATUS CODE

SE: Policy is not configured for access

INTERNAL STATUS CODE

BRK_MT_SETUP_FAIL_NO_POLICY_FOUND

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Verify Application Domain Seen By Client Connector is ZPA Domain	Check Client Connector ZSATunnel.log for results of any DNS and application domain lookups.	Forwarding Profile: DnsHostname: [] Condition Match Type: [Any] Predefined Networks: [0] Trusted DNS Servers: [] DNS Resolved IPs: [] DNS Search Domain: []	These log entries show that the Client Connector is not seeing any specific configurations related to configuration such as DNS for domain matches or use in trusted network criteria. This can be checked against the configuration in the portal for items like configured DNS Search Domains for the App Segments.
Check App Segment Configuration	ZPA Admin Portal > Administration > Application Segments > DNS Search Domains		In this example DNS Search Domains are not configured and the Client Connector is not set to validate the domain. If these were configured there will be entries in the Client Connector logs for the results of any validation.

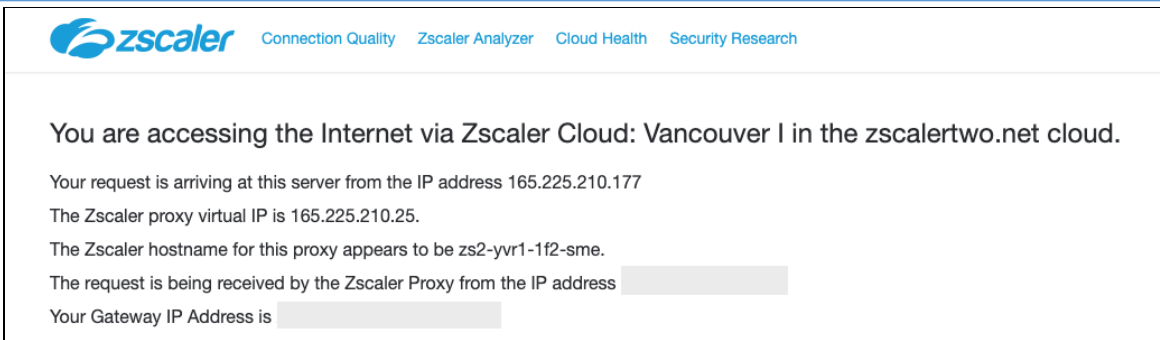
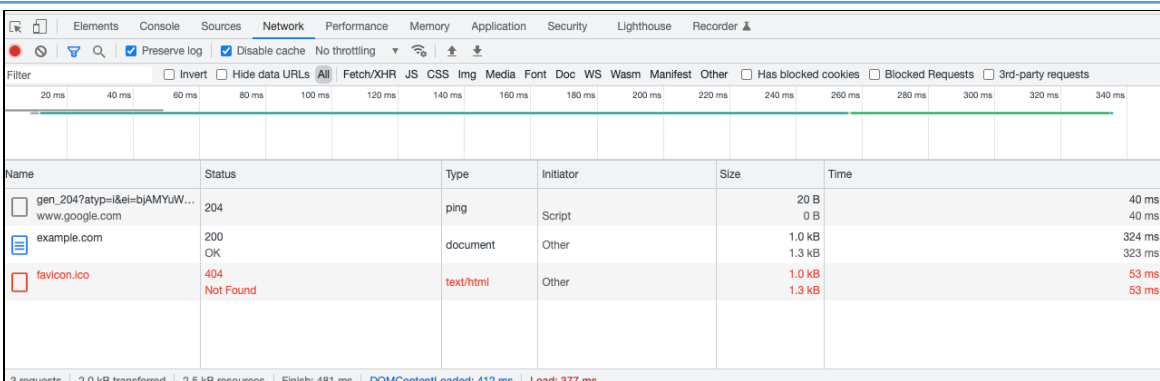
ZIA: User Experience

Troubleshoot Zscaler User Experience

Scenario/ Expected Result: Applications should be usable through Zscaler without any noticeable extra delays or rendering issues.

Problem: User complains that access to a private application is "slow".

Tips for avoiding this issue: Be aware of any need to optimize MTU settings to avoid packet fragmentation that may result from tunnel overheads. For example see: [Determining Optimal MTU for GRE or IPSec Tunnels](#).

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause																																										
Test ISP to Zscaler Data Center Latency	<p>ip.zscaler.com to check which data center a user is currently forwarding through.</p> <p>Ping to test for any current network issues.</p>	<div><p>You are accessing the Internet via Zscaler Cloud: Vancouver I in the zscalertwo.net cloud.</p><p>Your request is arriving at this server from the IP address 165.225.210.177</p><p>The Zscaler proxy virtual IP is 165.225.210.25.</p><p>The Zscaler hostname for this proxy appears to be zs2-yvr1-1f2-sme.</p><p>The request is being received by the Zscaler Proxy from the IP address [redacted]</p><p>Your Gateway IP Address is [redacted]</p></div> <pre>\$ ping 165.225.210.25 PING 165.225.210.25 (165.225.210.25): 56 data bytes 64 bytes from 165.225.210.25: icmp_seq=0 ttl=64 time=25.134 ms</pre>	Connectivity from the user's device looks good in this example. Ping times look ok. Network conditions between the user and the ISP do not appear to be an issue.																																										
Capture Web Page Load Time Records	<p>Browser Development Tools: Chrome for example: Customize > More Tools > Developer Tools</p> <p>Export results to an HTTP Archive (HAR) file for a record and follow up investigation.</p>	<div><table><tr><th>Name</th><th>Status</th><th>Type</th><th>Initiator</th><th>Size</th><th>Time</th></tr><tr><td>gen_204?atyp=i&ei=bjAMYUW...</td><td>204</td><td>ping</td><td>Script</td><td>20 B</td><td>40 ms</td></tr><tr><td>www.google.com</td><td></td><td></td><td></td><td>0 B</td><td>40 ms</td></tr><tr><td>example.com</td><td>200 OK</td><td>document</td><td>Other</td><td>1.0 kB</td><td>324 ms</td></tr><tr><td></td><td></td><td></td><td></td><td>1.3 kB</td><td>323 ms</td></tr><tr><td>favicon.ico</td><td>404 Not Found</td><td>text/html</td><td>Other</td><td>1.0 kB</td><td>53 ms</td></tr><tr><td></td><td></td><td></td><td></td><td>1.3 kB</td><td>53 ms</td></tr></table></div>	Name	Status	Type	Initiator	Size	Time	gen_204?atyp=i&ei=bjAMYUW...	204	ping	Script	20 B	40 ms	www.google.com				0 B	40 ms	example.com	200 OK	document	Other	1.0 kB	324 ms					1.3 kB	323 ms	favicon.ico	404 Not Found	text/html	Other	1.0 kB	53 ms					1.3 kB	53 ms	<p>Network tab shows all of the objects loaded for a page along with timing details.</p> <p>See for example: https://help.zscaler.com/zia/capturing-http-headers-google-chrome</p> <p>HTTP archive files are the records that will be needed to submit from a test showing user experience issues.</p>
Name	Status	Type	Initiator	Size	Time																																								
gen_204?atyp=i&ei=bjAMYUW...	204	ping	Script	20 B	40 ms																																								
www.google.com				0 B	40 ms																																								
example.com	200 OK	document	Other	1.0 kB	324 ms																																								
				1.3 kB	323 ms																																								
favicon.ico	404 Not Found	text/html	Other	1.0 kB	53 ms																																								
				1.3 kB	53 ms																																								

Check Packet Retransmission Rates / Fragmentation	Packet Capture from Client Connector: More > Start Packet Capture		Packet capture files get stored with the Client Connector log files. For example in C:\ProgramData\Zscaler See Enabling Packet Capture for Zscaler Client Connector Packet captures and HTTP archive files are the records that will be needed to submit from a test showing user experience issues.
---	--	---	--

ZIA: Logging & Reporting

Troubleshoot Zscaler Log Streaming Issue

Scenario/ Expected Result: Log streams feeds are received at the destination such as a SIEM

Problem: Log entries are missing at the SIEM. They may not be arriving at all or are missing for a period of time.

Tips for avoiding this issue: Check server host names, IP addresses and ports provided by the SIEM team. Ensure that the NSS server is placed in the network where it is able to reach the SIEM server and that there are no intermediate firewalls or proxies that will interfere.

Troubleshooting Activity/ Symptom	Tools	Sample Output	Analysis/ Cause
Check NSS Connectivity	Troubleshooting Deployed NSS Servers sudo nss test-firewall sudo nss troubleshoot netstat sudo nss troubleshoot connection sudo nss troubleshoot feeds	<pre>[zsroot@ ~]\$ sudo nss troubleshoot feeds Password: Feed name: ZCDS: Connection Status: [?:? -> 10.0.0.3:514] : Not Found</pre>	Tested from the NSS server VM. This example shows that the NSS server is not able to establish a connection to the configured SIEM server. We would want to check with the SIEM administrators on the server address and that it is up and able to receive the streams.
Check NSS SIEM reachability	telnet <SIEM Host> <port>	<pre>[zsroot@ ~]\$ telnet 10.0.0.3 514 Trying 10.0.0.3... telnet: connect to address 10.0.0.3: Connection refused telnet: Unable to connect to remote host [zsroot@ ~]\$</pre>	Tested from the NSS server. The host (10.0.0.3) is reachable, but does not have anything listening that may be connected to on port 514. We would want to check with the SIEM administrator for the correct port to configure for the log streaming.

