Client Connector

Client Connector App Release Summary (2025)

This article provides a summary of all new features and enhancements released per operating system (OS) for the Zscaler Client Connector app. To successfully update to the latest version of Zscaler Client Connector, see Best Practices for Updating Latest Versions of Zscaler Client Connector Application.

Select an OS:

Windows

Select an app version:

All

Select a deployment date:

All

The Client Connector app versions for Windows listed below were deployed on the following dates.

December 23, 2025

Release Available: Client Connector 4.8.0.88 for Windows

Zscaler Client Connector 4.8.0.88 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response. You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.8.0.115.

- Adds support for Zscaler Deception service entitlement for ZIdentity tenants.
- Adds support to download the forwarding PAC file through the tunnel when in Tunnel mode instead of directly. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector.
- Fixes an issue where, when notifying users to reauthenticate Zscaler Private Access (ZPA), the app displayed both the custom message configured in the ZPA timeout policy and the default English Zscaler Client Connector message.

- Updates the VPN Gateway Bypass to optionally not bypass subdomains for FQDNs. To learn more, see Bypassing FQDN Subdomains for VPN Gateway Bypass.
- Fixes a DNS resolution timing issue that resulted in users being unable to access internal sites after connecting to OpenVPN.
- Improves the retrial logic of the VPN (for Legacy Apps) client in cases where the VPN gateway port is unreachable.
- Fixes an issue where, if the Automatically use previously selected certificate for reauthentication option is enabled, Zscaler Client Connector didn't clear the stored certificate if reauthentication timed out.
- Fixes an issue where Zscaler Client Connector sent a config request immediately upon receiving a response from the ZPA Public Service Edge, which could result in service degradation.
- Fixes an issue where Zscaler Internet Access (ZIA) Disaster Recovery was not activated after querying the DNS TXT record using a VPN connection.
- Fixes a captive portal login failure that occurred if the Send All DNS During Fail-Close to Trusted-DNS Server option was enabled.
- Fixes an issue where Zscaler Client Connector continued to use DNS suffixes from ZPA even after switching to a network type with a forwarding mode of None.
- Fixes an issue where Zscaler Client Connector incorrectly allowed fail-close settings on the app profile to control network

lockdown even if the Install WFP Driver option was disabled.

- Updates Zscaler Client Connector to monitor changes to the system-level proxy configuration and to enforce the Zscaler proxy settings based on the forwarding profile.
- Fixes a connection issue for ZPA apps that attempt multiple connections over the machine tunnel.
- Fixes an issue where the network detection process temporarily switched to Off-Trusted instead of keeping the current network type when the detection was not due to a network change.
- Fixes an issue where, even if the device posture for posture-based service entitlement passed, ZIA was not enabled after enrollment if the user's app profile had Business Continuity enabled.
- Adds support for using registry keys with the REG_BINARY type with the Registry Key device posture profile.
- Updates the version check for Zscaler Deception to prevent downgrades during slow or phased rollouts.
- Fixes an issue where Zscaler Client Connector couldn't retrieve the PAC file when the source was the HKEY_CURRENT_USER Registry location provided in the forwarding profile.
- Fixes an issue where Zscaler Client Connector bypassed non-DNS requests on port 53.
- Fixes an issue where the `Access to certain applications requires you to`

`reauthenticate into Zscaler Client Connector` message didn't appear as a pop-up notification or on the Notifications window in the app for ZIdentity users. message didn't appear as a pop-up notification or on the Notifications window in the app for ZIdentity users.

- Fixes an issue where the app didn't display a device posture failure notification from ZPA if the Enable ZIA Notifications option was disabled.
- Fixes a tunnel crash that occurred after upgrading which resulted in Zscaler Client Connector remaining in a `Connecting` state.
- Fixes a timing issue that caused a delay in Zscaler Client Connector bypassing a URL after it was added to the app profile PAC file.

December 22, 2025

Release Available: Client Connector 4.7.0.168 for Windows

Zscaler Client Connector 4.7.0.168 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response. You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.7.0.202.

- Updates Npcap to version 1.84.
- Fixes an issue where, when notifying users to reauthenticate Zscaler Private Access (ZPA), the app displayed both the custom message configured in the ZPA timeout policy and the default English Zscaler Client Connector message.
- Fixes a DNS resolution timing issue that resulted in users being unable to access internal sites after connecting to OpenVPN.
- Improves the retrial logic of the VPN (for Legacy Apps) client in cases where the VPN gateway port is unreachable.
- Fixes an issue where Zscaler Internet Access (ZIA) Disaster Recovery was not activated after querying the DNS TXT record using a VPN connection.
- Fixes a captive portal login failure that occurred if the Send All DNS During Fail-Close to Trusted-DNS Server option was enabled.
- Fixes an issue where Zscaler Client Connector continued to use DNS suffixes from ZPA even after switching to a network type with a forwarding mode of None.
- Fixes an issue where Zscaler Client Connector incorrectly allowed fail-close settings on the app profile to control network lockdown even if the Install WFP Driver option was disabled.
- Updates Zscaler Client Connector to monitor changes to the system-level proxy configuration and to enforce the Zscaler proxy settings based on the forwarding profile.

- Fixes a connection issue for ZPA apps that attempt multiple connections over the machine tunnel.
- Fixes an issue where, even if the device posture for posture-based service entitlement passed, ZIA was not enabled after enrollment if the user's app profile had Business Continuity enabled.
- Adds support for using registry keys with the REG_BINARY type with the Registry Key device posture profile.
- Fixes an issue where Zscaler Client Connector couldn't retrieve the PAC file when the source was the HKEY_CURRENT_USER Registry location provided in the forwarding profile.
- Fixes an issue where Zscaler Client Connector bypassed non-DNS requests on port 53.
- Fixes an issue where the `Access to certain applications requires you to reauthenticate into Zscaler Client Connector` message didn't appear as a pop-up notification or on the Notifications window in the app for ZIdentity users. message didn't appear as a pop-up notification or on the Notifications window in the app for ZIdentity users.
- Fixes a timing issue that caused a delay in Zscaler Client Connector bypassing a URL after it was added to the app profile PAC file.

Release Available: Client Connector 4.6.0.351 for Windows

Zscaler Client Connector 4.6.0.351 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response. You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.6.0.371.

- Updates Npcap to version 1.84.
- Fixes an issue where, when notifying users to reauthenticate Zscaler Private Access (ZPA), the app displayed both the custom message configured in the ZPA timeout policy and the default English Zscaler Client Connector message.
- Fixes a DNS resolution timing issue that resulted in users being unable to access internal sites after connecting to OpenVPN.
- Improves the retrial logic of the VPN (for Legacy Apps) client in cases where the VPN gateway port is unreachable.
- Fixes an issue where Zscaler Internet Access (ZIA) Disaster Recovery was not activated after querying the DNS TXT record using a VPN connection.
- Fixes an issue where Zscaler Client Connector incorrectly allowed fail-close settings on the app profile to control network lockdown even if the Install WFP Driver option was disabled.

- Updates Zscaler Client Connector to monitor changes to the system-level proxy configuration and to enforce the Zscaler proxy settings based on the forwarding profile.
- Fixes a connection issue for ZPA apps that attempt multiple connections over the machine tunnel.
- Adds support for using registry keys with the REG_BINARY type with the Registry Key device posture profile.
- Fixes an issue where Zscaler Client Connector bypassed non-DNS requests on port 53.
- Fixes a timing issue that caused a delay in Zscaler Client Connector bypassing a URL after it was added to the app profile PAC file.

December 09, 2025

Release Available: Client Connector 4.5.0.508 for Windows

Zscaler Client Connector 4.5.0.508 Enhancements and Fixes

- Adds support to download the forwarding PAC file through the tunnel when in Tunnel mode instead of directly. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector.
- Updates the VPN Gateway Bypass to optionally not bypass subdomains for FQDNs. To learn more, see Bypassing FQDN Subdomains for VPN Gateway Bypass.
- Fixes a delay in tunnel establishment and traffic forwarding caused by Full Disk Encryption (FDE) posture evaluation failures.

- Fixes an issue where Zscaler Internet Access (ZIA) Disaster Recovery was not activated after querying the DNS TXT record using a VPN connection.
- Fixes a connection issue for Zscaler Private Access (ZPA) apps that attempt multiple connections over the machine tunnel.
- Fixes an issue where, if a device was in a device group enabled or disabled for ZIA service entitlement, Zscaler Client Connector didn't enable or disable ZIA correctly after exiting and relaunching the app.
- Fixes an issue where ZPA did not turn off when users clicked Turn Off in the Zscaler Client Connector app.
- Updates the version check for Zscaler Deception to prevent downgrades during slow or phased rollouts.

December 05, 2025

Release Available: Client Connector 4.4.0.472 for Windows

Zscaler Client Connector 4.4.0.472 Enhancements and Fixes

Updates the version check for Zscaler Deception to prevent downgrades during slow or phased rollouts.

November 26, 2025

Release Available: Client Connector 4.7.0.141 for Windows

Zscaler Client Connector 4.7.0.141 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response. You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.7.0.202.

- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate is enabled and also to remove the existing certificate for SSL Inspection.
- Supports using one-time passwords (OTPs) for customers with ZIdentity tenants.
- Removes deprecated Windows command usage from the Zscaler Client Connector uninstallation process.
- Fixes an issue where the system proxy was cleared and not updated with the forwarding profile PAC after a network change, especially when Apply on Any Network Change was configured.
- Adds support to download the forwarding PAC file through the tunnel when in Tunnel mode instead of directly. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector.
- Fixes an issue where the MAC Address in the Zscaler Client Connector Registered Device Details window was blank for ZIdentity users.

- Fixes an issue where Zscaler Client Connector didn't send updated trusted network information to Zscaler Private Access (ZPA) while ZPA was connecting.
- Fixes a delay in tunnel establishment caused when Zscaler Client Connector checked for a captive portal on a device that wasn't configured for captive portal detection, resulting in VPN Gateway Bypass traffic temporarily going to the Zscaler service.
- Fixes an issue where Zscaler Client Connector incorrectly detected a Split VPN-Trusted Network if the VPN Trusted Network Adapter Criteria included, but was not connected to, the F5 VPN.
- Fixes an issue where Zscaler Client Connector didn't handle an exception caused by an invalid source port bypass configuration correctly, resulting in a tunnel crash.
- Fixes an issue where, if Pre-Populate Client Connector Username (Using Javascript) was enabled, cursor focus was on the last input box with a type of password instead of the first input box when users authenticated in the app, which could skip focus on a field.
- Fixes an issue where a driver error during installation was displayed as an `FW/AV` error instead of as a `Driver Error` that also displays the Repair Driver option.
- Fixes an issue where Zscaler Client Connector frequently switched between the primary and secondary service edges for Z-Tunnel 1.0 traffic, even though there were no latency changes.

- Fixes an issue where the Policy Name on the Device Management page was not updated correctly for ZIdentity users with an app profile applied by device group.
- Fixes an issue where, after an upgrade, Zscaler Client Connector sent an old certificate to ZPA for authentication.
- Updates the VPN Gateway Bypass to optionally not bypass subdomains for FQDNs. To learn more, see Bypassing FQDN Subdomains for VPN Gateway Bypass.
- Updates Zscaler Client Connector to accept the hash (#) character in the partner tenant username.
- Fixes an issue where DNS resolution could fail for a ZPA application.
- Fixes an issue where, if Zscaler Client Connector was installed with the VDI installation parameter, the Zscaler Client Connector configuration file was not restored when a VDI was launched because the file was not saved correctly in the directory.
- Fixes delays in forwarding application traffic that occurred when switching network types (e.g., from an VPN-Trusted Network to an Off-Trusted Network).
- Fixes an issue where Zscaler Client Connector didn't connect to Zscaler Tunnel (Z-Tunnel) 2.0 after switching from a strict enforcement app profile configured with the route-based filter and Z-Tunnel 1.0 to an app profile that used the packet-based filter and Z-Tunnel 2.0.
- Fixes an issue where, if Egress IP was a Trusted Network condition, Zscaler Client Connector switched to an Off-Trusted

Network after network detection even though the device was still on a trusted IP address.

- Fixes an issue where users received frequent notifications to reauthenticate ZPA if auto-reauthentication failed, even though the Enable Notifications for ZPA reauthentication option was disabled.
- Fixes an issue where ZPA remained in a `Connecting` state due to a failed DNS resolution.
- Fixes an issue where, if Automatically use previously selected certificate for reauthentication is enabled, Zscaler Client Connector didn't clear the stored certificate if reauthentication timed out.
- Fixes a policy update delay that occurred when ZIdentity users clicked Update Policy on the More window of the app.
- Fixes an issue where the `Internet Security is Connected` user notification displayed even when the Zscaler Internet Access (ZIA) service was disabled through a forwarding mode of None.
- Fixes an issue where Zscaler Client Connector detected a VPN-Trusted Network instead of an Off-Trusted Network if `Wireguard` was entered in the VPN Trusted Network Adapter Criteria field.
- Fixes an issue where Zscaler Client Connector applied the DNS request handling logic (tunnel or bypass) of the first request to the following requests from the same source port, even if they were set up to be forwarded differently.
- Fixes an `Adapter_down_error` that occurred when connecting to a VPN using a cellular

network instead of Ethernet or Wi-Fi.

- Fixes an issue where, after a network switch on a device on a dual-stack network, Zscaler Client Connector temporarily bypassed traffic even though the Intercept ZIA traffic option was enabled.
- Fixes an issue where Zscaler Client Connector incorrectly displayed an `FW/AV` error instead of a network error if the network went down while a device was in Modern Standby mode.
- Fixes a delay in tunnel establishment and traffic forwarding caused by Full Disk Encryption (FDE) posture evaluation failures.
- Fixes an issue where ZIA traffic was not forwarded if the Intercept ZIA traffic option was enabled in the app profile.
- Fixes an issue where, when using a forwarding profile in Tunnel with Local Proxy mode, users couldn't connect through a captive portal because the captive portal URL was the same as a ZPA app segment.
- Fixes an issue where, if Automatic ZPA Reauthentication and Browser-Based Authentication were enabled, ZIdentity users received an `Internal Error. Please Contact Administrator` message even after authenticating when a ZPA application timed out.
- Fixes an issue where the network detection process temporarily switched to Off-Trusted instead of keeping the current network type when the detection was not due to a network change.
- Fixes an issue where, if a device was in a device group enabled or disabled for ZIA

service entitlement, Zscaler Client Connector didn't enable or disable ZIA correctly after exiting and relaunching the app.

- Fixes an issue where custom IP-based bypasses were not downloaded or applied when Zscaler Client Connector was in strict enforcement and machine tunnel mode.
- Fixes a tunnel crash that occurred after upgrading which resulted in Zscaler Client Connector remaining in a `Connecting` state.
- Fixes an issue where DNS requests for domains added in the Domain Inclusions field in App Profiles were bypassed instead of being routed through Z-Tunnel 2.0 on IPv4-only (non-dual stack) networks.
- Fixes an issue where the Zscaler Digital Experience (ZDX) domain `pac.zdxcloud.net` was spelled incorrectly when added to the internal bypass proxy list, resulting in unnecessary DNS requests, and which could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569)

Release Available: Client Connector 4.6.0.334 for Windows

Zscaler Client Connector 4.6.0.334 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response.

You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.6.0.371.

- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate is enabled and also to remove the existing certificate for SSL Inspection.
- Supports using one-time passwords (OTPs) for customers with ZIdentity tenants.
- Removes deprecated Windows command usage from the Zscaler Client Connector uninstallation process.
- Adds support to download the forwarding PAC file through the tunnel when in Tunnel mode instead of directly. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector.
- Fixes an issue where the MAC Address in the Zscaler Client Connector Registered Device Details window was blank for ZIdentity users.
- Fixes an issue where Zscaler Client Connector didn't send updated trusted network information to Zscaler Private Access (ZPA) while ZPA was connecting.
- Fixes a delay in tunnel establishment caused when Zscaler Client Connector checked for a captive portal on a device that wasn't configured for captive portal detection, resulting in VPN Gateway Bypass traffic temporarily going to the Zscaler service.
- Fixes an issue where Zscaler Client Connector incorrectly detected a Split VPN-Trusted Network if the VPN Trusted Network

Adapter Criteria included, but was not connected to, the F5 VPN.

- Fixes an issue where Zscaler Client Connector didn't handle an exception caused by an invalid source port bypass configuration correctly, resulting in a tunnel crash.
- Fixes an issue where, if Pre-Populate Client Connector Username (Using Javascript) was enabled, cursor focus was on the last input box with a type of password instead of the first input box when users authenticated in the app, which could skip focus on a field.
- Fixes an issue where a driver error during installation was displayed as an `FW/AV` error instead of as a `Driver Error` that also displays the Repair Driver option.
- Fixes an issue where Zscaler Client Connector frequently switched between the primary and secondary service edges for Z-Tunnel 1.0 traffic, even though there were no latency changes.
- Fixes an issue where the Policy Name on the Device Management page was not updated correctly for ZIdentity users with an app profile applied by device group.
- Fixes an issue where, after an upgrade, Zscaler Client Connector sent an old certificate to ZPA for authentication.
- Updates the VPN Gateway Bypass to optionally not bypass subdomains for FQDNs. To learn more, see Bypassing FQDN Subdomains for VPN Gateway Bypass.
- Updates Zscaler Client Connector to accept the hash (#) character in the partner tenant username.

- Fixes an issue where, if Zscaler Client Connector was installed with the VDI installation parameter, the Zscaler Client Connector configuration file was not restored when a VDI was launched because the file was not saved correctly in the directory.
- Fixes delays in forwarding application traffic that occurred when switching network types (e.g., from an VPN-Trusted Network to an Off-Trusted Network).
- Fixes an issue where Zscaler Client Connector didn't connect to Zscaler Tunnel (Z-Tunnel) 2.0 after switching from a strict enforcement app profile configured with the route-based filter and Z-Tunnel 1.0 to an app profile that used the packet-based filter and Z-Tunnel 2.0.
- Fixes an issue where, if Egress IP was a Trusted Network condition, Zscaler Client Connector switched to an Off-Trusted Network after network detection even though the device was still on a trusted IP address.
- Fixes an issue where users received frequent notifications to reauthenticate ZPA if auto-reauthentication failed, even though the Enable Notifications for ZPA reauthentication option was disabled.
- Fixes a policy update delay that occurred when ZIdentity users clicked Update Policy on the More window of the app.
- Fixes an issue where the `Internet Security is Connected` user notification displayed even when the Zscaler Internet Access (ZIA) service was disabled through a forwarding mode of None.

- Fixes an issue where Zscaler Client Connector applied the DNS request handling logic (tunnel or bypass) of the first request to the following requests from the same source port, even if they were set up to be forwarded differently.
- Fixes an `Adapter_down_error` that occurred when connecting to a VPN using a cellular network instead of Ethernet or Wi-Fi.
- Fixes an issue where, after a network switch on a device on a dual-stack network, Zscaler Client Connector temporarily bypassed traffic even though the Intercept ZIA traffic option was enabled.
- Fixes an issue where Zscaler Client Connector incorrectly displayed an `FW/AV` error instead of a network error if the network went down while a device was in Modern Standby mode.
- Fixes a delay in tunnel establishment and traffic forwarding caused by Full Disk Encryption (FDE) posture evaluation failures.
- Fixes an issue where ZIA traffic was not forwarded if the Intercept ZIA traffic option was enabled in the app profile.
- Fixes an issue where, when using a forwarding profile in Tunnel with Local Proxy mode, users couldn't connect through a captive portal because the captive portal URL was the same as a ZPA app segment.
- Fixes an issue where, if Automatic ZPA Reauthentication and Browser-Based Authentication were enabled, ZIdentity users received an `Internal Error. Please Contact Administrator` message even

after authenticating when a ZPA application timed out.

- Fixes an issue where the network detection process temporarily switched to Off-Trusted instead of keeping the current network type when the detection was not due to a network change.
- Fixes an issue where, if a device was in a device group enabled or disabled for ZIA service entitlement, Zscaler Client Connector didn't enable or disable ZIA correctly after exiting and relaunching the app.
- Fixes an issue where custom IP-based bypasses were not downloaded or applied when Zscaler Client Connector was in strict enforcement and machine tunnel mode.
- Fixes a tunnel crash that occurred after upgrading which resulted in Zscaler Client Connector remaining in a `Connecting` state.

Release in Limited Availability: Client Connector 4.8.0.63 for Windows

Zscaler Client Connector 4.8.0.63 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response. You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been

corrected on Zscaler Client Connector version 4.8.0.115.

- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate is enabled and remove the existing certificate for SSL Inspection.
- Fixes the clear log process to include cleanup of `wfpdiag` logs created for packet captures and auto-cleanup for `wfpdiag` logs generated due to system error (e.g., archive failure).
- Fixes an issue where the Policy Name on the Device Management page was not updated correctly for ZIdentity users with an app profile applied by device group.
- Fixes an issue where, after an upgrade, Zscaler Client Connector sent an old certificate to Zscaler Private Access (ZPA) for authentication.
- Fixes delays in forwarding of application traffic that occurred when switching network types (e.g., from a VPN-Trusted Network to an Off-Trusted Network).
- Fixes an issue where, if Egress IP was a Trusted Network condition, Zscaler Client Connector switched to an Off-Trusted Network after network detection even though the device was still on a trusted IP address.
- Fixes an issue where ZPA remained in a `Connecting` state due to a failed DNS resolution.
- Fixes a policy update delay that occurred when ZIdentity users clicked Update Policy on the More window of the app.
- Fixes an `Internet Security is Connected` user notification that displayed

even when the Zscaler Internet Access (ZIA) service was disabled through a forwarding mode of None.

- Fixes an issue where Zscaler Client Connector detected a VPN-Trusted Network instead of an Off-Trusted Network if `Wireguard` was entered in the VPN Trusted Network Adapter Criteria field.
- Fixes an `Adapter_down_error` that occurred when connecting to a VPN using a cellular network instead of Ethernet or Wi-Fi.
- Fixes an issue where, after a network switch on a device on a dual-stack network, Zscaler Client Connector temporarily bypassed traffic even though the Intercept ZIA traffic option was enabled in the app profile.
- Fixes an issue where Zscaler Client Connector incorrectly displayed an `FW/AV` error instead of a network error if the network went down while a device was in Modern Standby mode.
- Fixes a delay in tunnel establishment and traffic forwarding caused by Full Disk Encryption (FDE) posture evaluation failures.
- Fixes an issue where ZIA traffic was not forwarded if the Intercept ZIA traffic option was enabled in the app profile.
- Fixes an issue where, when using a forwarding profile in Tunnel with Local Proxy mode, users couldn't connect through a captive portal because the captive portal URL was the same as a ZPA app segment.
- Fixes an issue where, if Automatic ZPA Reauthentication and Browser-Based Authentication were enabled, ZIdentity users received an `Internal Error. Please`

`Contact Administrator` message when a ZPA application timed out.

- Fixes an issue where, if a device was in a device group enabled or disabled for ZIA service entitlement, Zscaler Client Connector didn't enable or disable ZIA correctly after exiting and relaunching the app.
- Fixes an issue where DNS requests for domains added to the Domain Inclusion field in App Profiles were bypassed instead of being routed through Zscaler Tunnel (Z-Tunnel) 2.0 on IPv4-only (non-dual stack) networks.
- Fixes an issue where the Zscaler Digital Experience (ZDX) domain `pac.zdxcloud.net` was spelled incorrectly when added to the internal bypass proxy list, resulting in unnecessary DNS requests, and which could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569)

October 30, 2025

Release in Limited Availability: Client Connector 4.8 for Windows

Zscaler Client Connector 4.8 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where a trusted network defined by the Hostname and IP condition isn't detected when the DNS response of the hostname used includes both the `CName` and the `ipaddress` in the response.

You can temporarily resolve the issue by removing this criteria from the trusted network conditions. The issue has been corrected on Zscaler Client Connector version 4.8.0.115.

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.8.0.63.

- Supports IPv6 traffic forwarding from IPv6-only Windows devices to Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). To learn more, see Enabling IPv6 Resolution for Zscaler Domains.
- Supports using one-time passwords (OTPs) for customers with ZIdentity tenants.
- Enhances the Packet Capture on the More window in the app to provide separate filter options for adapter packets and Lightweight Filter (LWF) driver packets. To learn more, see Enabling Packet Capture for Zscaler Client Connector.
- Supports automatically starting packet captures for specific scenarios such as tunnel failures and health checks. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Supports controlling how End User Notifications (EUNs) from ZIA are displayed for users. To learn more, see Configuring

Notification Templates for Zscaler Client Connector.

- Expands support for adding additional user login domains in the Additional IdP Domains field, making it available to all customers, not just those using Imprivata. To learn more, see Using WebView2 Authentication.
- Supports using OAuth 2.0 to authenticate for ZIdentity users before the machine tunnel starts, requiring end users to use an external device. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Updates Zscaler Client Connector to always use the packet-based filter driver when in Tunnel mode regardless of the Tunnel Driver Type setting in a user's forwarding profile.

  If your organization has multiple versions of Zscaler Client Connector installed across devices, devices with versions 4.7 and earlier installed continue to use the driver selected in the forwarding profile. Devices with Zscaler Client Connector version 4.8 and later installed use the packet-based filter driver even if the forwarding profile has Route-Based Driver selected.

- Supports identifying the system proxy manually instead of using the default Microsoft Windows APIs. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Enforces the use of the secure https:// prefix for the Default PAC URL and prevents fallback to HTTP if the HTTPS download of the default

PAC file fails. To learn more, see Enforcing Secure PAC URLs.

- Expands HTTP_CONNECT_TIMING metrics for Web probes, improving visibility into TCP handshake and HTTP connection times between Z-Tunnel 1.0 and the Service Edge.
- Supports a new traffic forwarding action for ZIA Disaster Recovery so you can forward traffic using Zscaler Tunnel (Z-Tunnel) 2.0. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Supports testing Business Continuity mode with a group of users. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Adds the ability to download, validate, and cache the CRL used when performing the CRL check for the Client Certificate device posture check in certain fallback scenarios. To learn more, see Configuring Device Posture Profiles.
- Supports the Adaptive Access Engine used to receive user-related context signals from Microsoft Defender. To learn more, see Integrating Microsoft Defender with Adaptive Access Engine.
- Supports automatically switching to a TLS connection if the Z-Tunnel 2.0 DTLS connection becomes unstable. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector.
- Updates captive portal detection to make asynchronous requests to reduce latency.
- Enables Zscaler Client Connector to steer traffic and manage endpoint firewall rules based on the user's network type (e.g., On-

Trusted or Off-Trusted). You can use this feature to fix the security concern where DNS requests might be resolved using local system resolvers or external DNS servers rather than being forced through the Zscaler tunnel (CVE-2025-54984). To learn more, see About Location-Based Policies.

- Supports automatic ZPA reauthentication settings on the app profile that can override the global setting and can be applied based on a user's network environment (e.g, On-Trusted or Off-Trusted). To learn more, see Configuring Zscaler Client Connector App Profiles.
- Adds an app profile option to define the default language for the Zscaler Client Connector app and an in-app option that allows users to change the language as needed. To learn more, see Configuring Zscaler Client Connector App Profiles and Changing the Display Language for Zscaler Client Connector.
- Supports using location services on the user's device to find the nearest data center. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Adds an install option that can be used to prevent Zscaler Client Connector from starting automatically after installation. To learn more, see Customizing Zscaler Client Connector with Install Options for EXE and Customizing Zscaler Client Connectorwith Install Options for MSI.
- Supports enabling and disabling ZIA and Zscaler Digital Experience (ZDX) remotely via

CLI. To learn more, see Interacting with Zscaler Client Connector Remotely.

- Supports enabling local packet capture on an app profile in addition to the existing global packet capture enablement. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Supports preventing automatic reauthentication to ZPA while a user's device is locked. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Supports a device posture check for specific Zscaler Client Connector versions. To learn more, see Configuring Device Posture Profiles.
- Supports monitoring system proxy settings and re-caching them if Zscaler Client Connector detects changes. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Updates Zscaler Client Connector to run Npcap in non-promiscuous mode (instead of promiscuous mode) when performing packet captures.
- Supports creating and assigning notification templates per app profile to allow more granularity in which users see different notifications. To learn more, see Configuring Notification Templates for Zscaler Client Connector.
- Removes deprecated Windows command usage from the Zscaler Client Connector uninstallation process.
- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate

is enabled and remove the existing certificate for SSL Inspection.

- Fixes an issue where Zscaler Client Connector installed expired code signing certificates during installation.
- Fixes an issue where, if Zscaler Client Connector was installed using a 32-bit installer, Zscaler Diagnostics did not launch if users clicked Launch Zscaler Diagnostics.
- Updates Zscaler Client Connector to retrieve the system PAC file settings and pass them to WebView2 for authentication during enrollment to ensure that the correct proxy setting is used.
- Fixes an issue with ZSAService certificate validation that caused Zscaler Client Connector to not appear in the system tray and not launch from the Start menu after a user rebooted.
- Fixes an issue where users still received an `Authentication required on Lock screen` message to onboard the machine tunnel even after the ZPA Machine Authentication option was disabled in the policy.
- Fixes an issue where Zscaler Client Connector did not allow remote access via NinjaOne if the app profile included a process-based application bypass.
- Fixes an issue where Zscaler Client Connector did not clear added DNS search domains from ZPA after moving from a machine tunnel to a user tunnel.
- Fixes an issue where, if load balancing was used by the ISP, sites could fail to load when using Z-Tunnel 1.0 on an Off-Trusted network.

- Fixes a delay during the tunnel exit process which resulted in Zscaler Client Connector forcing the exit, which could be reported as a tunnel crash in the logs.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Updates ZSATrayManager to streamline the config file check to reduce ongoing disk I/O consumption.
- Fixes a delay when connecting to the ZDX service on an IPv6-only network when Zscaler Client Connector is configured with a system proxy PAC file.
- Fixes an issue where Zscaler Client Connector didn't end the connection to the ZPA Private Service Edge and exit Business Continuity, even though the Zero Trust Exchange (ZTE) was reachable.
- Updates a Zscaler Client Connector firewall rule to remain active from starting to stopping the app to minimize the number of Windows Filtering Platform (WFP) log events.
- Fixes an issue where users could not log in to Zscaler Client Connector again after their device was soft-removed if the Automatically Attempt ZPA Reauthentication option was enabled.
- Fixes an issue where uninstalling Zscaler Client Connector failed if anti-tampering was enabled and the logged-on Windows user name was in Japanese.
- Fixes an issue where users could frequently experience a FW/AV error state due to

incorrectly parsed string parameters during logging.

- Fixes an issue where the system proxy was cleared and not updated with the forwarding profile PAC after a network change, especially when Apply on Any Network Change was configured.
- Updates the LWF driver so it can be accessed only by a local admin Windows user.
- Updates the network interface retrieval process for the LWF driver to clear temporary kernel buffer data to prevent data leakage.
- Fixes an issue where ZPA remained in a `Registration Required` or `Connecting` state after ZIdentity users upgraded from Windows 10 to Windows 11, even though users tried to reauthenticate.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the ZIA Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where direct flow logs for bypassed applications recorded an incorrect public IP address after a network change.
- Fixes an issue where, if strict enforcement was enabled, the Zscaler Client Connectortray became unresponsive when the tray was terminated and restarted (e.g., after clicking the back arrow on the IdP authentication window).
- Fixes an issue where the Data Protection window did not appear on the Zscaler Client Connector app after enabling Endpoint Data

Loss Prevention (DLP) in the app profile for a user without ZIA enabled.

- Fixes an issue where the MAC Address in the Zscaler Client Connector Registered Device Details window was blank for ZIdentity users.
- Fixes an issue where Zscaler Client Connector could experience an `FW/AV` error after upgrading.
- Fixes an issue where Zscaler Client Connector could incorrectly bypass traffic after recovering from an authentication error by ensuring the post-recovery proxy state is updated to ON.
- Updates a previous change to keep a Zscaler Client Connector firewall rule active from starting to stopping the app to also delete the rule when exiting the app and add the rule when restarting the app.
- Improved localized strings for French translations, i.e., replacing Private Access with Accès Privé where applicable.
- Fixes an issue where Zscaler Client Connector repeatedly switched between primary and secondary Service Edges when Dynamic ZIA Service Edge Assignment is enabled.
- Fixes an issue where the captive portal login page could fail to load with a `403` error with both the embedded captive portal or the external browser.
- Removes the character limit for a partner tenant username.
- Fixes an issue where users received an `Endpoint FW/AV Error` due to Zscaler Client Connector not handling unsupported paths in application bypass correctly.

- Fixes an issue where the WFP driver didn't stop running when a user transitioned from a strict enforcement app profile with WFP enabled to an app profile with WFP disabled
- Fixes a delay in sending device posture check results to ZPA, which could result in blocked ZPA application access, even though the posture evaluation completed in a timely manner.
- Fixes a delay caused when Zscaler Client Connector checked for a captive portal on a device that wasn't configured for captive portal detection, resulting in VPN Gateway Bypass traffic temporarily going to the Zscaler service.
- Fixes an issue where Zscaler Client Connector incorrectly detected a Split VPN-Trusted Network if the VPN Trusted Network Adapter Criteria included, but was not connected to, the F5 VPN.
- Fixes an issue where Zscaler Client Connector bypassed non-DNS UDP 53 traffic when in a fail-close state and the Send All DNS During Fail-Close to Trusted-DNS Server option was enabled, even though the Z-Tunnel 2.0 Setup Failure Behavior option was set to Block All Traffic.
- Updates the process check for the Full Disk Encryption device posture to use a more reliable check, preventing incorrect encryption status results.
- Fixes an issue where Zscaler Client Connector didn't handle an exception caused by an invalid source port bypass configuration correctly, resulting in a tunnel crash.

- Fixes an issue where, if Pre-Populate Client Connector Username (Using Javascript) was enabled, cursor focus was on the last input box with a type of password instead of the first input box when users authenticated in the app, which could skip focus on a field.
- Fixes an issue in the exit routine of the Zscaler Client Connector app that could result in the app becoming unresponsive and failing to relaunch until after restarting the device.
- Fixes an issue where Zscaler Client Connector mistakenly treated the logged-in user as absent after the device woke up from sleep mode due to an unexpected session logoff event from another user on the machine.
- Fixes an issue where users with Japanese characters in their Windows username could not export logs using the Export Logs feature.
- Fixes a DNS registry error that occurred when a ZPA app segment was bypassed on a network that was configured as a trusted network based on the DNS server.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Fixes an issue where, when in Business Continuity mode in a no-default route environment, Zscaler Client Connector could not switch to the public cloud even after the cloud became available.
- Fixes an issue where Zscaler Client Connector continued bypassing processes from a strict enforcement policy if they were running during the transition to a new app

profile with different process-based bypasses.

- Fixes an issue where the Crowdstrike ZTA Score posture check failed even if the evaluation passed.
- Fixes an issue where a driver error during installation was displayed as an FW/AV error instead of as a `Driver Error` that also displays the Repair Driver option.
- Fixes an issue where Zscaler Client Connector frequently switched between the primary and secondary service edges for Z-Tunnel 1.0 traffic, even though there were no latency changes.
- Fixes a network connectivity issue during tunnel startup for non-persistent VDIs even though the forwarding mode was None.
- Fixes an issue where the tunnel could crash for users without flow logging enabled.
- Fixes an issue with the IPv6 address assigned by Zscaler Client Connector when connecting to a VPN using a cellular network adapter which could result in an `Adapter_down_error` error.
- Fixes an issue where Zscaler Client Connector didn't add all the ZPA application DNS suffixes to the device, even though the DNS Suffix limit of 50 had not been reached.
- Fixes an issue where Zscaler Client Connector failed to intercept DNS traffic after the ZIA service was turned back on following a network change or reconnection.
- Updates Zscaler Client Connector to accept the hash (#) character in the partner tenant username.

- Fixes an issue where DNS resolution could fail for a ZPA application.
- Fixes an issue where, if Zscaler Client Connector was installed with the VDI installation parameter, the Zscaler Client Connector configuration file was not restored when a VDI was launched because the file was not saved correctly in the directory.
- Fixes an issue where users received frequent notifications to reauthenticate ZPA if auto-reauthentication failed, even though the Enable Notifications for ZPA reauthentication option was disabled.
- Fixes an issue where, if Automatically use previously selected certificate for reauthentication is enabled, Zscaler Client Connector didn't clear the stored certificate if reauthentication timed out.
- Fixes a tray manager crash that could occur after upgrading to Zscaler Client Connector version 4.7.0.61.
- Fixes a tunnel crash that could occur when using the unsupported legacy PAC parser (and not the V8 PAC Parser option).
- Fixes an issue where Zscaler Client Connector applied the DNS request handling (tunnel or bypass) of the first request to all requests from the same source port, even if they were set up to be handled differently.

October 24, 2025

Release Available: Client Connector 4.5.0.498 for Windows

Zscaler Client Connector 4.5.0.498 Enhancements and Fixes

- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate is enabled and to remove the existing certificate for SSL Inspection.
- Removes deprecated Windows command usage from the Zscaler Client Connector uninstallation process.
- Fixes an issue where the MAC Address in the Zscaler Client Connector Registered Device Details window was blank for ZIdentity users.
- Fixes an issue where a driver error during installation was displayed as an `FW/AV` error instead of as a `Driver Error` that also displays the Repair Driver option.
- Fixes a network connectivity issue during tunnel startup for non-persistent VDIs even though the forwarding mode was None.
- Fixes an issue where the tunnel could crash for users without flow logging enabled.
- Fixes an issue where Zscaler Client Connector didn't add all the Zscaler Private Access (ZPA) application DNS suffixes to the device, even though the DNS Suffix limit of 50 had not been reached.
- Fixes an issue where, if Zscaler Client Connector was installed with the VDI installation parameter, the Zscaler Client Connector configuration file was not restored when a VDI was launched because the file was not saved correctly in the directory.
- Fixes an issue where users received frequent notifications to reauthenticate ZPA if auto-reauthentication failed, even though the Enable Notifications for ZPA reauthentication option was disabled.

- Fixes a policy update delay that occurred when ZIdentity users clicked Update Policy on the More window of the app.
- Fixes a tunnel crash that could occur when using the unsupported legacy PAC parser (and not the V8 PAC Parser option).
- Fixes an issue where, after a network switch on a device on a dual-stack network, Zscaler Client Connector temporarily bypassed traffic even though the Intercept ZIA traffic option was enabled.

Release Available: Client Connector 4.4.0.468 for Windows

Zscaler Client Connector 4.4.0.468 Enhancements and Fixes

- Adds support to install the latest Zscaler Root CA Certificate if Install Zscaler SSL Certificate is enabled and to remove the existing certificate for SSL Inspection.
- Removes deprecated Windows command usage from the Zscaler Client Connector uninstallation process.
- Fixes an issue where the MAC Address in the Zscaler Client Connector Registered Device Details window was blank for ZIdentity users.
- Fixes an issue where Zscaler Client Connector incorrectly detected a Split VPN-Trusted Network if the VPN Trusted Network Adapter Criteria included, but was not connected to, the F5 VPN.
- Fixes an issue where Zscaler Client Connector mistakenly treated the logged-in user as absent after the device woke up from sleep mode due to an unexpected session

logoff event from another user on the machine.
- Fixes an issue where the tunnel could crash for users without flow logging enabled.
- Fixes an issue where Zscaler Client Connector didn't add all the Zscaler Private Access (ZPA) application DNS suffixes to the device, even though the DNS Suffix limit of 50 had not been reached.
- Fixes an issue where users received frequent notifications to reauthenticate Zscaler Private Access (ZPA) if auto-reauthentication failed, even though the Enable Notifications for ZPA reauthentication option was disabled.
- Fixes a tunnel crash that could occur when using the unsupported legacy PAC parser (and not the V8 PAC Parser option).
- Fixes an issue where, after a network switch on a device on a dual-stack network, Zscaler Client Connector temporarily bypassed traffic even though the Intercept ZIA traffic option was enabled.

October 17, 2025

Release Available: Client Connector 4.6.0.310 for Windows

Zscaler Client Connector 4.6.0.310 Enhancements and Fixes

- Adds an option to allow Zscaler to retrieve and analyze Zscaler Client Connector log bundles to expedite resolution of customer-reported issues and to proactively resolve internal issues. Zscaler recommends enabling this feature. To learn more, see Enabling Auto System Info and Log Fetch.

- Updates Zscaler Client Connector to run Npcap in non-promiscuous mode (instead of promiscuous mode) when performing packet captures.
- Fixes an issue where the system proxy was cleared and not updated with the forwarding profile PAC after a network change, especially when Apply on Any Network Change was configured.
- Fixes an issue where Zscaler Private Access (ZPA) remained in a `Registration Required` or `Connecting` state after ZIdentity users upgraded from Windows 10 to Windows 11, even though users tried to reauthenticate.
- Fixes an issue where, if strict enforcement was enabled, the Zscaler Client Connector tray became unresponsive when the tray was terminated and restarted (e.g., after clicking the back arrow on the IdP authentication window).
- Fixes an issue where Zscaler Client Connector could experience an `FW/AV` error after upgrading.
- Updates a previous change to keep a Zscaler Client Connector firewall rule active from starting to stopping the app to also delete the rule when exiting the app and add the rule when restarting the app.
- Improved localized strings for French translations, i.e., replacing `Private Access` with `Accès Privé` where applicable.
- Fixes a delay in sending device posture check results to ZPA, which could result in blocked ZPA application access, even though the

posture evaluation completed in a timely manner.

- Fixes the clear log process to include cleanup of `wfpdiag` logs created for packet captures and auto-cleanup for `wfpdiag` logs generated due to system error (e.g., archive failure).
- Fixes an issue in the exit routine of the Zscaler Client Connector app that could result in the app becoming unresponsive and failing to relaunch until after restarting the device.
- Fixes an issue where Zscaler Client Connector mistakenly treated the logged-in user as absent after the device woke up from sleep mode due to an unexpected session logoff event from another user on the machine.
- Fixes an issue where users with Japanese characters in their Windows username could not export logs using the Export Logs feature.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Fixes an issue where, when in Business Continuity mode in a no-default route environment, Zscaler Client Connector could not switch to the public cloud even after the cloud became available.
- Fixes an issue where the Crowdstrike ZTA Score posture check failed even if the evaluation passed.
- Fixes a network connectivity issue during tunnel startup for non-persistent VDIs even though the forwarding mode was None.
- Fixes an issue where the tunnel could crash for users without flow logging enabled.

- Fixes an issue with the IPv6 address assigned by Zscaler Client Connector when connecting to a VPN using a cellular network adapter which could result in an `Adapter_down_error` error.
- Fixes an issue where Zscaler Client Connector didn't add all the ZPA application DNS suffixes to the device, even though the DNS Suffix limit of 50 had not been reached.
- Fixes an issue where Zscaler Client Connector failed to intercept DNS traffic after the Zscaler Internet Access (ZIA) service was turned back on after a network change or reconnection.
- Fixes a tunnel crash that could occur when using the unsupported legacy PAC parser (and not the V8 PAC Parser option).
- Fixes an issue where DNS resolution could fail for a ZPA application.

October 15, 2025

Release Available: Client Connector 4.7.0.113 for Windows

Zscaler Client Connector 4.7.0.113 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.7.0.141.

- Updates Zscaler Client Connector to run Npcap in non-promiscuous mode (instead of promiscuous mode) when performing packet captures.
- Fixes an issue where Zscaler Private Access (ZPA) remained in a `Registration Required` or `Connecting` state after ZIdentity users upgraded from Windows 10 to Windows 11, even though users tried to reauthenticate.
- Fixes an issue where, if strict enforcement was enabled, the Zscaler Client Connector tray became unresponsive when the tray was terminated and restarted (e.g., after clicking the back arrow on the IdP authentication window).
- Fixes an issue where Zscaler Client Connector could experience an `FW/AV` error after upgrading.
- Updates a previous change to keep a Zscaler Client Connector firewall rule active from starting to stopping the app to also delete the rule when exiting the app and add the rule when restarting the app.
- Improved localized strings for French translations, i.e. replacing `Private Access` with `Accès Privé` where applicable.
- Fixes a delay in sending device posture check results to ZPA, which could result in blocked ZPA application access, even though the posture evaluation completed in a timely manner.
- Fixes an issue where Zscaler Client Connector bypassed non-DNS UDP 53 traffic when in a fail-close state and the Send All DNS During Fail-Close to Trusted-DNS Server

option was enabled, even though the Z-Tunnel 2.0 Setup Failure Behavior option was set to Block All Traffic.

- Fixes the clear log process to include cleanup of `wfpdiag` logs created for packet captures and auto-cleanup for `wfpdiag` logs generated due to system error (e.g., archive failure).
- Fixes an issue in the exit routine of the Zscaler Client Connector app that could result in the app becoming unresponsive and failing to relaunch until after restarting the device.
- Fixes an issue where Zscaler Client Connector mistakenly treated the logged-in user as absent after the device woke up from sleep mode due to an unexpected session logoff event from another user on the machine.
- Fixes an issue where users with Japanese characters in their Windows username could not export logs using the Export Logs feature.
- Fixes a DNS registry error that occurred when a ZPA app segment was bypassed on a network that was configured as a trusted network based on the DNS server.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Fixes an issue where, when in Business Continuity mode in a no-default route environment, Zscaler Client Connector could not switch to the public cloud even after the cloud became available.
- Fixes an issue where the Crowdstrike ZTA Score posture check failed even if the evaluation passed.

- Fixes a network connectivity issue during tunnel startup for non-persistent VDIs even though the forwarding mode was None.
- Fixes an issue where the tunnel could crash for users without flow logging enabled.
- Fixes an issue with the IPv6 address assigned by Zscaler Client Connector when connecting to a VPN using a cellular network adapter which could result in an `Adapter_down_error` error.
- Fixes an issue where Zscaler Client Connector didn't add all the ZPA application DNS suffixes to the device, even though the DNS Suffix limit of 50 had not been reached.
- Fixes an issue where Zscaler Client Connector failed to intercept DNS traffic after the Zscaler Internet Access (ZIA) service was turned back on after a network change or reconnection.
- Fixes a tray manager crash that could occur after upgrading to Zscaler Client Connector version 4.7.0.61 for Windows.
- Fixes a tunnel crash that could occur when using the unsupported legacy PAC parser (and not the V8 PAC Parser option).

September 22, 2025

Release Available: Client Connector 4.5.0.495 for Windows

Zscaler Client Connector 4.5.0.495 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the

unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.5.0.498 for Windows.

- Updates Zscaler Client Connector to run Npcap in non-promiscuous mode (instead of promiscuous mode) when performing packet captures.
- Fixes an issue where Zscaler Private Access (ZPA) remained in a `Registration Required` or `Connecting` state after ZIdentity users upgraded from Windows 10 to Windows 11, even though users tried to re-authenticate.
- Fixes an issue where Zscaler Client Connector incorrectly detected a Split VPN-Trusted Network if the VPN Trusted Network Adapter Criteria included the F5 VPN, but Zscaler Client Connector was not connected to it.
- Fixes an issue where Zscaler Client Connector incorrectly displayed an `FW/AV` error after switching to an On-Trusted Network with a forwarding profile action of None, where both Zscaler Internet Access (ZIA) and ZPA are disabled.

September 19, 2025

Release Available: Client Connector 4.4.0.465 for Windows

Zscaler Client Connector 4.4.0.465 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.4.0.468 for Windows.

- Updates Zscaler Client Connector to run Npcap in non-promiscuous mode (instead of promiscuous mode) when performing packet captures.
- Fixes an issue where Zscaler Client Connector incorrectly displayed an `FW/AV` error after switching to an On-Trusted Network with a forwarding profile action of None, where both Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) are disabled.

September 02, 2025

Release Available: Client Connector 4.7.0.88 for Windows

Zscaler Client Connector 4.7.0.88 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on

Zscaler Client Connector version 4.7.0.113 for Windows.

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.7.0.141.

- Fixes an issue with ZSAService certificate validation that caused Zscaler Client Connector to not appear in the system tray and not launch from the Start Menu after a user rebooted.
- Fixes a delay when connecting to the Zscaler Digital Experience (ZDX) service on an IPv6-only network when Zscaler Client Connector is configured with a system proxy PAC file.
- Updates a Zscaler Client Connector firewall rule to remain active from starting to stopping the app to minimize the number of Windows Filtering Platform (WFP) log events.
- Fixes an issue where, if IPv6 was enabled, Zscaler Client Connector could have intermittent connection issues with a Zscaler Private Access (ZPA) application due to multiple unanswered DNS queries.
- Fixes an issue where uninstalling Zscaler Client Connector failed if anti-tampering was enabled and the logged-on Windows user name was in Japanese.
- Fixes an issue where the AzureAD Domain Joined device posture check was not evaluated and applied to the machine tunnel.

- Adds a check to return an error message if a customer tries to add a partner tenant using the same domain as the main tenant.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the Zscaler Internet Access (ZIA) Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where direct flow logs for bypassed applications recorded an incorrect public IP address after a network change.
- Fixes an issue where the Data Protection window did not appear on the Zscaler Client Connector app after enabling Endpoint Data Loss Prevention (DLP) in the app profile for a user without ZIA enabled.
- Fixes an issue where Zscaler Client Connector could incorrectly bypass traffic after recovering from an authentication error by ensuring the post-recovery proxy state is updated to ON.
- Fixes an issue where TCP connections made with only a handshake (without a client hello) were logged as bypass traffic, even though the traffic was inspected and sent through the Zscaler service.
- Fixes an issue where, after switching from the machine tunnel to the user tunnel, traffic forwarded to ZIA using Source IP Anchoring (SIPA) was instead sent to ZPA due to Zscaler Client Connector reusing the machine tunnel's synthetic IP address.
- Fixes an issue where Zscaler Client Connector repeatedly switched between primary and secondary Service Edges when

Dynamic ZIA Service Edge Assignment is enabled.

- Fixes an issue where the captive portal login page sometimes failed to load with a `403` error using either the embedded captive portal or the external browser.
- Removes the character limit for a partner tenant username.
- Fixes an issue where users received an `Endpoint FW/AV Error` due to Zscaler Client Connector not handling unsupported paths in application bypass correctly.
- Addresses a security vulnerability in earlier versions of SQLite used by Zscaler Client Connector by upgrading to SQLite version 3.50.4.
- Fixes an issue where Zscaler Client Connector tunneled DNS traffic to ZIA (instead of resolving it locally) when using Zscaler Tunnel (Z-Tunnel) 2.0, resulting in the ZPA connection stalling.
- Fixes an issue where Microsoft applications (e.g., the Microsoft Store version of Slack) did not launch if anti-tampering was enabled.

Release Available: Client Connector 4.5.0.484 for Windows

Zscaler Client Connector 4.5.0.484 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app

profile. The issue has been corrected on Zscaler Client Connector version 4.5.0.498 for Windows.

- Addresses a security vulnerability in earlier versions of SQLite used by Zscaler Client Connector by upgrading to SQLite version 3.50.4.
- Fixes an issue where Microsoft applications (e.g., the Microsoft Store version of Slack) did not launch if anti-tampering was enabled.

August 29, 2025

Release Available: Client Connector 4.6.0.284 for Windows

Zscaler Client Connector 4.6.0.284 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.6.0.304 for Windows.

- Addresses a security vulnerability in earlier versions of SQLite used by Zscaler Client Connector by upgrading to SQLite version 3.50.4.
- Fixes an issue where Microsoft applications (e.g., the Microsoft Store version of Slack) did not launch if anti-tampering was enabled.

Release Available: Client Connector 4.4.0.464 for Windows

Zscaler Client Connector 4.4.0.464 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.4.0.468 for Windows.

- Addresses a security vulnerability in earlier versions of SQLite used by Zscaler Client Connector by upgrading to SQLite version 3.50.4.
- Fixes an issue where Microsoft applications (e.g., the Microsoft Store version of Slack) did not launch if anti-tampering was enabled.

August 15, 2025

Release Available: Client Connector 4.6.0.282 for Windows

Zscaler Client Connector 4.6.0.282 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app

profile. The issue has been corrected on Zscaler Client Connector version 4.6.0.304 for Windows.

- Fixes an issue with ZSAService certificate validation that caused Zscaler Client Connector to not appear in the system tray and not launch from the Start Menu after a user rebooted.
- Updates a Zscaler Client Connector firewall rule to remain active from starting to stopping the app to minimize the number of Windows Filtering Platform (WFP) log events.
- Fixes an issue where, if IPv6 was enabled, Zscaler Client Connector could have intermittent connection issues with a Zscaler Private Access (ZPA) application due to multiple unanswered DNS queries.
- Fixes an issue where uninstalling Zscaler Client Connector failed if anti-tampering was enabled and the logged-on Windows user name was in Japanese.
- Fixes an issue where the AzureAD Domain Joined device posture check was not evaluated and applied to the machine tunnel.
- Adds a check to return an error message if a customer tries to add a partner tenant using the same domain as the main tenant.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the Zscaler Internet Access (ZIA) Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where direct flow logs for bypassed applications recorded an incorrect

public IP address after a network change.

- Fixes an issue where the Data Protection window did not appear on the Zscaler Client Connector app after enabling Endpoint Data Loss Prevention (DLP) in the app profile for a user without ZIA enabled.
- Fixes an issue where Zscaler Client Connector could incorrectly bypass traffic after recovering from an authentication error by ensuring the post-recovery proxy state is updated to ON.
- Fixes an issue where TCP connections made with only a handshake (without a client hello) were logged as bypass traffic, even though the traffic was inspected and sent through the Zscaler service.
- Fixes an issue where, after switching from the machine tunnel to the user tunnel, traffic forwarded to ZIA using Source IP Anchoring (SIPA) was instead sent to Zscaler Private Access (ZPA) due to Zscaler Client Connector reusing the machine tunnel's synthetic IP address.
- Fixes an issue where Zscaler Client Connector repeatedly switched between primary and secondary Service Edges when Dynamic ZIA Service Edge Assignment is enabled.
- Fixes an issue where the captive portal login page sometimes failed to load with a `403` error using either the embedded captive portal or the external browser.
- Fixes an issue where users received an `Endpoint FW/AV Error` due to Zscaler Client Connector not handling unsupported paths in application bypass correctly.

July 28, 2025

Release Available: Client Connector 4.5.0.478 for Windows

Zscaler Client Connector 4.5.0.478 Enhancements and Fixes

Zscaler Client Connector version 4.5.0.478 for Windows has a known issue where some users experience intermittent failures with command-line applications such as Slack, Microsoft Teams, and other apps that use Command Prompt (CMD). This issue only happens on devices with anti-tampering enabled.

To resolve this issue, temporarily disable anti-tampering until you can upgrade to a newer version of Zscaler Client Connector. This issue has been corrected in Zscaler Client Connector version 4.6.0.282 for Windows and is not seen in Zscaler Client Connector version 4.7 for Windows. A fix for this issue is expected in upcoming releases.

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.5.0.498 for Windows.

- Fixes an issue with ZSAService certificate validation that caused Zscaler Client Connector to not appear in the system tray and not launch from the Start Menu after a user rebooted.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the Zscaler Internet Access (ZIA) Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where uninstalling Zscaler Client Connector failed if anti-tampering was enabled and the logged-on Windows user name was in Japanese.
- Fixes an issue where users could frequently experience a FW/AV error state due to incorrectly parsed string parameters during logging.
- Fixes an issue where the AzureAD Domain Joined device posture check was not evaluated and applied to the machine tunnel.
- Adds a check to return an error message if a customer tries to add a partner tenant using the same domain as the main tenant.
- Fixes an issue where the Data Protection window did not appear on the Zscaler Client Connector app after enabling Endpoint Data Loss Prevention (DLP) in the app profile for a user without ZIA enabled.
- Fixes an issue where Zscaler Client Connector could incorrectly bypass traffic after recovering from an authentication error by ensuring the post-recovery proxy state is updated to ON.

- Fixes an issue where, after switching from the machine tunnel to the user tunnel, traffic forwarded to ZIA using Source IP Anchoring (SIPA) was instead sent to Zscaler Private Access (ZPA) due to Zscaler Client Connector reusing the machine tunnel's synthetic IP address.

July 25, 2025

Release Available: Client Connector 4.4.0.460 for Windows

Zscaler Client Connector 4.4.0.460 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the ZSATunnel can crash intermittently if you use the unsupported legacy PAC Parser. You can resolve the issue by enabling V8 JavaScript based PAC Parser in the app profile. The issue has been corrected on Zscaler Client Connector version 4.4.0.468 for Windows.

- Fixes an issue with ZSAService certificate validation that caused Zscaler Client Connector to not appear in the system tray and not launch from the Start Menu after a user rebooted.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the Zscaler Internet Access (ZIA) Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.

- Fixes an issue where the AzureAD Domain Joined device posture check was not evaluated and applied to the machine tunnel.
- Adds a check to return an error message if a customer tries to add a partner tenant using the same domain as the main tenant.
- Fixes an issue where the Data Protection window did not appear on the Zscaler Client Connector app after enabling Endpoint Data Loss Prevention (DLP) in the app profile for a user without ZIA enabled.
- Fixes an issue where Zscaler Client Connector could incorrectly bypass traffic after recovering from an authentication error by ensuring the post-recovery proxy state is updated to ON.

July 07, 2025

Release Available: Client Connector 4.7.0.61 for Windows

Zscaler Client Connector 4.7.0.61 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.7.0.141.

- Updates Zscaler Client Connector to retrieve the system PAC file settings and pass them to WebView2 for authentication during

enrollment to ensure that the correct proxy setting is used.

- Fixes an issue where users still received an `Authentication required on Lock screen` message to onboard the machine tunnel even after the ZPA Machine Authentication option was disabled in the policy.
- Fixes an issue where Zscaler Client Connector did not allow remote access via NinjaOne if the app profile included a process-based application bypass.
- Fixes an exception handling issue that caused Zscaler Client Connector to not run in a virtual desktop infrastructure (VDI) when the Zscaler Client Connector processes did not have access permission to the user's roaming application data directory.
- Fixes an issue where a user's device couldn't connect to the domain controller through the machine tunnel before the user logged in if Strict Enforcement mode and App Scaling were enabled.
- Fixes an issue where Zscaler Private Access (ZPA) incoming traffic processing could be delayed when the Send Location Hint to Client Connector feature was enabled.
- Fixes an issue where Zscaler Client Connector sent incorrect logs to the server for flow logging when multiple connections were opened on the same local port.
- Fixes an issue where Zscaler Client Connector did not connect to a domain set to bypass Zscaler Tunnel (Z-Tunnel) 2.0 in the forwarding profile if the proxy to which the app profile PAC file sent all non-Z-Tunnel 2.0

traffic was unavailable, even though the app profile included another specific proxy for the domain.

- Fixes an issue where users could not access a URL bypassed by the app profile PAC file if the URL was also in the Zscaler Internet Access (ZIA) disaster recovery global database allowlist and the ZIA Cloud Not Reachable app fail-open setting was configured to fallback to ZIA DR, even though ZIA was not in disaster recovery mode.
- Fixes an issue where Zscaler Client Connector could repeatedly enter a `Registration required state for ZPA` if it was deployed in Strict Enforcement mode.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the ZIA Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where users could not log in to Zscaler Client Connector again after their device was soft-removed if the Automatically Attempt ZPA Reauthentication option was enabled.
- Fixes an issue where Zscaler Client Connector did not send DNS requests to the DNS server for the VPN Service Edge, even though the Network Connector was connected.
- Fixes an issue where Zscaler Client Connector did not reconnect to the VPN Service Edge after a ZPA reconnection using VPN (for Legacy Apps).

- Fixes an issue where users on an IPv6-only network experienced ZPA disconnections if Hyper-V was enabled on their device.

July 03, 2025

Release Available: Client Connector 4.5.0.471 for Windows

Zscaler Client Connector 4.5.0.471 Enhancements and Fixes

- Updates Zscaler Client Connector to retrieve the system PAC file settings and pass them to WebView2 for authentication during enrollment to ensure that the correct proxy setting is used.
- Fixes an issue where users still received an `Authentication required on Lock screen` message to onboard the machine tunnel even after the ZPA Machine Authentication option was disabled in the policy.
- Fixes an issue where Zscaler Client Connector did not allow remote access via NinjaOne if the app profile included a process-based application bypass.
- Fixes an issue where Zscaler Private Access (ZPA) incoming traffic processing could be delayed when the Send Location Hint to Client Connector feature was enabled.
- Fixes an issue where Zscaler Client Connector sent incorrect logs to the server for flow logging when multiple connections were opened on the same local port.
- Fixes an issue where users could not log in to Zscaler Client Connector again after their device was soft-removed if the Automatically

Attempt ZPA Reauthentication option was enabled.

June 30, 2025

Release Available: Client Connector 4.4.0.456 for Windows

Zscaler Client Connector 4.4.0.456 Enhancements and Fixes

- Updates Zscaler Client Connector to retrieve the system PAC file settings and pass them to WebView2 for authentication during enrollment to ensure that the correct proxy setting is used.
- Fixes an issue where users still received an `Authentication required on Lock screen` message to onboard the machine tunnel even after the ZPA Machine Authentication option was disabled in the policy.
- Fixes an issue where the machine tunnel didn't start after upgrading Zscaler Client Connector.
- Fixes an issue where a user's device couldn't connect to the domain controller through the machine tunnel before the user logged in if Strict Enforcement mode and App Scaling were enabled.
- Fixes an issue where Zscaler Private Access (ZPA) applications could not be accessed after a user who was already connected to Zscaler Client Connector clicked Update Policy on Zscaler Diagnostics.
- Fixes an issue where Zscaler Client Connector sent incorrect logs to the server

for flow logging when multiple connections were opened on the same local port.

- Fixes an issue where Zscaler Client Connector experienced a connection error when a cellular device was placed in isolation through the Intune Microsoft Defender portal, and the device could not be removed from isolation through the portal.
- Fixes an issue where users could not log in to Zscaler Client Connector again after their device was soft-removed if the Automatically Attempt ZPA Reauthentication option was enabled.

June 27, 2025

Release Available: Client Connector 4.6.0.240 for Windows

Zscaler Client Connector 4.6.0.240 Enhancements and Fixes

- Updates Zscaler Client Connector to retrieve the system PAC file settings and pass them to WebView2 for authentication during enrollment to ensure that the correct proxy setting is used.
- Fixes an issue where users still received an `Authentication required on Lock screen` message to onboard the machine tunnel even after the ZPA Machine Authentication option was disabled in the policy.
- Fixes an issue where Zscaler Client Connector did not allow remote access via NinjaOne if the app profile included a process-based application bypass.

- Fixes an exception handling issue that caused Zscaler Client Connector to not run in a virtual desktop infrastructure (VDI) when the Zscaler Client Connector processes did not have access permission to the user's roaming application data directory.
- Fixes an issue where a user's device couldn't connect to the domain controller through the machine tunnel before the user logged in if Strict Enforcement mode and App Scaling were enabled.
- Fixes an issue where Zscaler Private Access (ZPA) incoming traffic processing could be delayed when the Send Location Hint to Client Connector feature was enabled.
- Fixes an issue where Zscaler Client Connector sent incorrect logs to the server for flow logging when multiple connections were opened on the same local port.
- Fixes an issue where Zscaler Client Connector experienced a connection error when a cellular device was placed in isolation through the Intune Microsoft Defender portal, and the device could not be removed from isolation through the portal.
- Fixes an issue where Zscaler Client Connector did not connect to a domain set to bypass Zscaler Tunnel (Z-Tunnel) 2.0 in the forwarding profile if the proxy to which the app profile PAC file sent all non-Z-Tunnel 2.0 traffic was unavailable, even though the app profile included another specific proxy for the domain.
- Fixes an issue where users could not access a URL bypassed by the app profile PAC file if the URL was also in the Zscaler Internet

Access (ZIA) disaster recovery global database allowlist and the ZIA Cloud Not Reachable app fail-open setting was configured to fallback to ZIA DR, even though ZIA was not in disaster recovery mode.

- Fixes an issue where Zscaler Client Connector could repeatedly enter a `Registration required state for ZPA` if it was deployed in Strict Enforcement mode.
- Fixes an issue where Zscaler Client Connector did not update the correct device trust level to the ZIA Public Service Edge during initial enrollment if the tunnel was in a connecting state and took longer to transition to a connected state.
- Fixes an issue where users could not log in to Zscaler Client Connector again after their device was soft-removed if the Automatically Attempt ZPA Reauthentication option was enabled.
- Fixes an issue where Zscaler Client Connector did not send DNS requests to the DNS server for the VPN Service Edge, even though the Network Connector was connected.
- Fixes an issue where Zscaler Client Connector did not reconnect to the VPN Service Edge after a ZPA reconnection using VPN (for Legacy Apps).
- Fixes an issue where users on an IPv6-only network experienced ZPA disconnections if Hyper-V was enabled on their device.

June 04, 2025

Release Available: Client Connector 4.5.0.459 for Windows

Zscaler Client Connector 4.5.0.459 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector started the enrollment process in the background before the Autopilot setup was complete when deploying Zscaler Client Connector using Microsoft Autopilot.
- Fixes an issue with Zscaler Digital Experience (ZDX) probes that occurred after Zscaler Tunnel (Z-Tunnel) 1.0 failures, even though the Z-Tunnel 2.0 connection was healthy and both the Use Tunnel 2.0 for Proxied Traffic option and the Redirect Web Traffic to Local Proxy option were enabled.
- Fixes an issue where a Detect Antivirus device posture check passed for an outdated AV signature, even though the Check if AV definitions are up to date option was enabled.
- Fixes an issue where Zscaler Client Connector did not clear added DNS search domains from Zscaler Private Access (ZPA) after moving from a machine tunnel to a user tunnel.
- Fixes an issue where crash events were observed in the logs after shutdown of a device with machine tunnels enabled.
- Fixes an issue where the machine tunnel didn't start after upgrading Zscaler Client Connector.
- Fixes an issue where a blank screen displayed when authenticating using the embedded browser to access a ZPA

application and the Automatically Attempt ZPA Reauthentication feature was enabled.

- Fixes an issue where Zscaler Client Connector did not open a Microtunnel (M-Tunnel) for an ICMP request for a ZPA application that came in during the Cooldown period (the one-second period after receiving 100 requests with less than a one-second gap between them).
- Fixes a machine tunnel authentication failure that occurred due to Zscaler Client Connector not handling the config file correctly if an error was encountered after a system proxy change.
- Fixes an issue where a user's device couldn't connect to the domain controller through the machine tunnel before the user logged in if Strict Enforcement mode and App Scaling were enabled.
- Fixes an issue where ZPA applications could not be accessed after a user who was already connected to Zscaler Client Connector clicked Update Policy on Zscaler Diagnostics.
- Fixes an issue where Zscaler Client Connector experienced a connection error when a cellular device was placed in isolation through the Intune Microsoft Defender portal, and the device could not be removed from isolation through the portal.
- Fixes disconnections to the ZPA service caused by parallel ICMP and TCP M-Tunnel requests.

Release in Limited Availability: Client Connector 4.7.0.47 for Windows

Zscaler Client Connector 4.7.0.47 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.7.0.141.

- Fixes an issue where Zscaler Client Connector started the enrollment process in the background before the Autopilot setup was complete when deploying Zscaler Client Connector using Microsoft Autopilot.
- Fixes an issue where a Detect Antivirus device posture check passed for an outdated AV signature, even though the Check if AV definitions are up to date option was enabled.
- Fixes an issue where Zscaler Client Connector did not clear added DNS search domains from Zscaler Private Access (ZPA) after moving from a machine tunnel to a user tunnel.
- Fixes an issue where crash events were observed in the logs after shutdown of a device with machine tunnels enabled.
- Fixes an issue where a blank screen displayed when authenticating using the embedded browser to access a ZPA application and the Automatically Attempt ZPA Reauthentication feature was enabled.
- Fixes performance issues due to logging, particularly for ICMP request packets.

- Fixes a machine tunnel authentication failure that occurred due to Zscaler Client Connector not handling the config file correctly if an error was encountered after a system proxy change.
- Fixes an issue where Zscaler Client Connector authentication could fail with an internal error when a manually configured external proxy was not correctly identified on the system.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Fixes an issue where ZPA applications could not be accessed after a user who was already connected to Zscaler Client Connector clicked Update Policy on Zscaler Diagnostics.
- Fixes an issue where Zscaler Client Connector sent traffic from devices via the built-in cellular adapter instead of the Wi-Fi network, which caused connectivity issues for IPv6-only Wi-Fi networks.
- Fixes an issue where Zscaler Client Connector experienced a connection error when a cellular device was placed in isolation through the Intune Microsoft Defender portal, and the device could not be removed from isolation through the portal.
- Fixes traffic forwarding issues that could occur while accessing ZPA and Zscaler Internet Access (ZIA) apps due to Zscaler Client Connector indefinitely retaining the source port-based bypass used during proxy health checks (CVE-2025-54983).

- Fixes an issue where Zscaler Client Connector didn't end the connection to the ZPA Private Service Edge and exit Business Continuity, even though the Zero Trust Exchange (ZTE) was reachable.
- Fixes an issue where external proxy detection failed due to third-party process interference, preventing the system from correctly determining proxy settings from the PAC file.
- Fixes disconnections to the ZPA service caused by parallel ICMP and TCP Microtunnel (M-Tunnel) requests.

May 28, 2025

Release Available: Client Connector 4.6.0.216 for Windows

Zscaler Client Connector 4.6.0.216 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector started the enrollment process in the background before the Autopilot setup was complete when deploying Zscaler Client Connector using Microsoft Autopilot.
- Fixes an issue where Zscaler Client Connector sent traffic from devices via the built-in cellular adapter instead of the Wi-Fi network, which caused connectivity issues for IPv6-only Wi-Fi networks.
- Fixes an issue where a Detect Antivirus device posture check passed for an outdated AV signature, even though the Check if AV definitions are up to date option was enabled.
- Fixes an issue where Zscaler Client Connector did not clear added DNS search

domains from Zscaler Private Access (ZPA) after moving from a machine tunnel to a user tunnel.

- Fixes an issue where crash events were observed in the logs after shutdown of a device with machine tunnels enabled.
- Fixes an issue where a blank screen displayed when authenticating using the embedded browser to access a ZPA application and the Automatically Attempt ZPA Reauthentication feature was enabled.
- Fixes an issue where Zscaler Client Connector did not open a Microtunnel (M-Tunnel) for an ICMP request for a ZPA application that came in during the Cooldown period (the one-second period after receiving 100 requests with less than a one-second gap between them).
- Fixes performance issues due to logging, particularly for ICMP request packets.
- Fixes a machine tunnel authentication failure that occurred due to Zscaler Client Connector not handling the config file correctly if an error was encountered after a system proxy change.
- Fixes an issue where Zscaler Client Connector authentication could fail with an internal error when a manually-configured external proxy was not correctly identified on the system.
- Fixes an issue where Zscaler Client Connector entered Business Continuity mode in a no-default route environment, even though the cloud was available.
- Fixes an issue where ZPA applications could not be accessed after a user who was already

connected to Zscaler Client Connector clicked Update Policy on Zscaler Diagnostics.

- Fixes traffic forwarding issues that could occur while accessing ZPA and Zscaler Internet Access (ZIA) apps due to Zscaler Client Connector indefinitely retaining the source port-based bypass used during proxy health checks (CVE-2025-54983).
- Fixes an issue where Zscaler Client Connector didn't end the connection to the ZPA Private Service Edge and exit Business Continuity, even though the Zero Trust Exchange (ZTE) was reachable.
- Fixes an issue where external proxy detection failed due to a third-party process interference, preventing the system from correctly determining proxy settings from the PAC file.
- Fixes disconnections to the ZPA service caused by parallel ICMP and TCP M-Tunnel requests.

May 16, 2025

Release Available: Client Connector 4.4.0.432 for Windows

Zscaler Client Connector 4.4.0.432 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector started the enrollment process in the background before the Autopilot setup was complete when deploying Zscaler Client Connector using Microsoft Autopilot.
- Fixes an issue where Zscaler Client Connector could not access an IP-based Zscaler Private Access (ZPA) application due

to LWF filters created based on an incomplete application list.

- Fixes an issue where WFP filters were not deleted correctly after a tunnel crash, resulting in an FW/AV error when trying to reconnect.
- Fixes an issue with Zscaler Digital Experience (ZDX) probes that occurred after Zscaler Tunnel (Z-Tunnel) 1.0 failures, even though the Z-Tunnel 2.0 connection was healthy and both the Use Tunnel 2.0 for Proxied Traffic option and the Redirect Web Traffic to Local Proxy option were enabled.
- Fixes an issue where Zscaler Client Connector did not download the PAC file after switching to a Split VPN-Trusted network with Zscaler Internet Access (ZIA) enabled, which could cause unexpected traffic handling.
- Fixes an issue where crash events were observed in the logs after shutdown of a device with machine tunnels enabled.
- Fixes an issue where a blank screen displayed when authenticating using the embedded browser to access a ZPA application and the Automatically Attempt ZPA Reauthentication feature was enabled.
- Fixes issues where the ZSATunnel service could crash when restarting due to conflicts in background processes.
- Fixes an issue where Zscaler Client Connector stopped working after users clicked Revert App if they had previously opened the app from the tray icon during an upgrade.
- Fixes an issue where Zscaler Client Connector did not open a Microtunnel (M-

Tunnel) for an ICMP request for a ZPA application that came in during the Cooldown period (the one-second period after receiving 100 requests with less than a one-second gap between them).

- Fixes an issue where Zscaler Client Connector didn't connect to the ZPA Service Edge after switching from a machine tunnel to a user tunnel, causing some users to experience authentication errors.
- Fixes a machine tunnel authentication failure that occurred due to Zscaler Client Connector not handling the config file correctly if an error was encountered after a system proxy change.

April 29, 2025

Release in Limited Availability: Client Connector 4.7 for Windows

Zscaler Client Connector 4.7 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.7.0.47.

This version of Zscaler Client Connector has a known issue that could potentially prevent a limited amount of traffic from being inspected under specific and limited

circumstances. (CVE-2026-22569) The issue has been corrected on Zscaler Client Connector version 4.7.0.141.

- Enables the ability to base alternative cloud name detection on the Zscaler Internet Access (ZIA) Public Service Edge location instead of the Zscaler Client Connector location and to have an alternative cloud name per ZIA Public Service Edge.
- Adds an option to allow Zscaler to retrieve and analyze Zscaler Client Connector log bundles to expedite resolution of customer-reported issues and to proactively resolve internal issues. Zscaler recommends enabling this feature. To learn more, see Enabling Auto System Info and Log Fetch.
- Supports step-up authentication for conditional access to ZIA based on dynamic requests for stronger authentication for ZIdentity-enabled tenants. To learn more, see Verifying Access to Applications.
- Supports downloading a Zscaler Digital Experience (ZDX) package to deploy with the Mobile Device Management (MDM) used by your organization. To learn more, see Viewing and Configuring ZDX Module Upgrades.
- Displays the Windows devices' serial numbers in the Device Details section of the Zscaler Client Connector Portal.
- Updates the French localization support to include translated notification messages from Windows and Zscaler Client Connector, including pop-up notifications.
- Supports suppressing the message from Zscaler Private Access (ZPA) that displays to

users when a ZPA policy blocks access to an app. To learn more, see Configuring Access Policies.

- Supports having Zscaler Client Connector fail close when users experience a driver error, an FW/AV error, or a tunnel crash, or when they click Repair App. To learn more, see Configuring Zscaler Client Connector App Profiles.
- Improves certificate prompt handling in Zscaler Client Connector to enhance user experience and reduce prompt frequency.
- Adds granularity to restrict ZPA partner logins to specify which partners can access your organization's tenant.
- Supports sending DNS traffic to a specific IPv4 or IPv6 DNS server when Zscaler Client Connector is in a fail-close state.
- Supports authentication to the ZPA VPN (for Legacy Apps) for ZIdentity users.
- Adds pop-up notifications to indicate when a device enters or exits Business Continuity.
- Updates the Business Continuity configuration file properties to include device posture information.
- Supports an option to control screen focus on the notifications pop-up window from the Zscaler Notification Framework.
- Fixes an issue where the Firewall device posture check could fail, even though the firewall was enabled on the user device.
- Fixes an issue where Zscaler Client Connector did not auto-upgrade due to an error in the installer URL received from the Zscaler Client Connector Portal.

- Limits the total size of all Zscaler log files for all Windows user profiles to 500 MB on a machine with Zscaler Client Connector integrated with Imprivata by deleting the oldest files when the maximum is reached.
- Fixes an issue with anti-tampering that could cause a driver error when upgrading Zscaler Client Connector.
- Fixes a delay in detecting the captive portal when Zscaler Client Connector encountered network issues while establishing a connection.
- Fixes an issue where the ZSATunnel process could crash and sometimes create dump files in the export logs after a fragmented packet was received.
- Fixes an issue where ZSAHelper log files were created frequently for forwarding profiles when the Route-Based tunnel driver type was selected and Enable Split VPN-Trusted Network was disabled.
- Fixes an issue where Zscaler Client Connector did not prevent the Windows Defender firewall domain profile from being applied to the device, even though the device network type (e.g., Off-Trusted Network) was selected in Block Domain Profile Detection.
- Fixes an issue where the Zscaler Client Connector tray icon disappeared after logging in due to receiving two authentication responses via browser-based authentication.
- Fixes an issue where the Service Status on the Private Access window continued to display as `Connecting` after a change in network type, even though the traffic was forwarded correctly to the Zscaler service.

- Fixes an issue where Zscaler Client Connector wasn't redirected to the correct ZPA Private Service Edge after switching from a machine tunnel to a user tunnel.
- Fixes an issue where some apps couldn't connect to the internet if Zscaler Client Connector was installed using strict enforcement and the Remove Existing Exempted Containers feature was enabled.
- Fixes an issue where Zscaler Client Connector showed an incorrect connectivity status after a device switched from an Off-Trusted Network to a VPN-Trusted Network.
- Fixes an issue where Zscaler Client Connector removed loopback exemptions, even though the Remove Existing Exempted Containers feature was disabled.
- Fixes an issue where Zscaler Client Connector displayed an `Internal Error` message during device startup due to the Network Driver Interface Specification (NDIS) not binding the Zscaler Client Connector's Windows Filter Driver to the network adapter.
- Fixes an issue where users on a dual-stack network or an IPv6-only network were intermittently unable to access ZPA applications after the device awakened from sleep mode.
- Fixes an issue where user traffic bypassed the Zscaler cloud (e.g., users could access restricted websites) for a short interval of time while the Zscaler Tunnel (Z-Tunnel) 2.0 was reconnecting due to a network type switch.
- Fixes an issue where a partner tenant did not reconnect after a machine reboot.

- Fixes an issue where Zscaler Client Connector did not register with ZPA client-to-client capability and could not be connected to via RDP over ZPA.
- Fixes an issue where Zscaler Client Connector continually displayed `Registering Device` after a ZIdentity user reauthenticated, even though the device was successfully registered.
- Improves Zscaler Client Connector's handling of unattended installs when anti-tampering is enabled.
- Fixes an issue where Zscaler Client Connector displayed a `Server Down` error after connecting to the default gateway if the primary and secondary proxy addresses in the PAC file were unavailable when using Tunnel with Local Proxy.
- Fixes an issue where the ZPA reauthentication required notification didn't display as a pop-up or in the Notifications window for enrolled users after Automatically Attempt ZPA Reauthentication was disabled.
- Fixes an issue where the ZIA trust level was incorrectly calculated using device posture results from the cache after a reboot.
- Fixes an issue that prevented Zscaler Client Connector from establishing a ZIA Z-Tunnel 2.0 connection when the ZIA Service Edge was configured as a ZPA application.
- Fixes an issue where an echo test request was sent to ZPA from a device on a dual-stack network if the synthetic IP range was beyond the 100.64.0.0/16 default range.
- Fixes an issue where the Microsoft System Center Configuration Manager (SCCM)

ClientAlwaysOnInternet registry key was not updated based on the SCCM Client configuration after switching from a Trusted Network to an Off-Trusted Network or vice versa.

- Fixes an issue where the connection from Zscaler Client Connector to the ZPA Public Service Edge was not closed correctly, which occasionally resulted in a slow response from the server.
- Fixes an issue where ZIdentity users saw an incorrect Zscaler Client Connector Version on the Device Management page and in the Registered Device Details window.
- Fixes an issue where tunnel crashes were observed from pacparser failures due to a Windows API failing to download the proxy PAC file.
- Fixes an issue where ZIdentity users were unable to complete the ZPA reauthentication process.
- Fixes an issue where Windows displayed a blue screen for some users when flow logging was enabled.
- Fixes an issue where Zscaler Client Connector could not access an IP-based ZPA application due to LWF filters created based on an incomplete application list.
- Fixes an issue where uploads to a network drive were slow when using the Server Message Block (SMB) protocol using ZPA.
- Fixes an issue with tunnel disconnects caused by pacparser crashes.
- Fixes an issue where users couldn't access a ZPA application at times due to Zscaler Client

Connector not removing a stale entry from the dynamic bypass table.

- Updates Zscaler Client Connector to ignore blank serial numbers when generating UDIDs, preventing multiple devices for a single user from having the same UDID.
- Fixes an issue where ZPA reauthentication could fail after upgrading Zscaler Client Connector from a much earlier version (e.g., Zscaler Client Connector version 3.7).
- Fixes an issue where Zscaler Client Connector remained on the Loading page when reauthenticating ZPA due to a posture evaluation delay.
- Fixes an internal error (`302`) that occurred during a ZPA automatic reauthentication attempt after a user restarted the system.
- Fixes an issue with posture updates that caused Zscaler Client Connector to be in a `Connecting` state for a prolonged time, resulting in a delayed connection to ZPA applications via an external proxy.
- Updates the way Zscaler Client Connector retrieves the MAC Address from the device during registration to prioritize the active adapter connected to the internet.
- Fixes an issue where WFP filters were not deleted correctly after a tunnel crash, resulting in an FW/AV error when trying to reconnect.
- Fixes an issue with Zscaler Digital Experience (ZDX) probes after Zscaler Tunnel (Z-Tunnel) 1.0 failures, even though the Z-Tunnel 2.0 connection was healthy and both the Use Tunnel 2.0 for Proxied Traffic option and the

Redirect Web Traffic to Local Proxy option were enabled.

- Fixes a delay in ZPA reauthentication after users authenticated with an IdP.
- Fixes an issue where Zscaler Client Connector used the incorrect app profile while using the Registry Key device posture profile with an HKEY_CURRENT_USER registry key.
- Updates Zscaler Client Connector to not launch if a user starts the device in Safe mode.
- Fixes an issue where process-based application bypasses sometimes did not work if the policy update of the app identity list failed.
- Fixes an issue where Zscaler Client Connector did not download the PAC file after switching to a Split VPN-Trusted Network with ZIA enabled.
- Fixes an issue where the machine tunnel didn't start after upgrading Zscaler Client Connector.
- Fixes issues where the ZSATunnel service could crash when restarting due to conflicts in background processes.
- Fixes an issue where Zscaler Client Connector stopped working after users clicked Revert App if they had previously opened the app from the tray icon during an upgrade.
- Fixes an issue where Zscaler Client Connector did not open a Microtunnel (M-Tunnel) for an ICMP request for a ZPA application that came in during the Cooldown period (the one-second period after receiving

100 requests with less than a one-second gap between them).
- Fixes connectivity issues with SQL Server for customers using ZPA without ZIA or ZDX sending traffic through Z-Tunnel 1.0 to port 1433.
- Fixes an issue where some applications could not be accessed due to Zscaler Client Connector incorrectly proxying HTTP payloads containing binary data.

April 24, 2025

Release Available: Client Connector 4.6.0.200 for Windows

Zscaler Client Connector 4.6.0.200 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.6.0.216.

- Fixes a delay in detecting the captive portal when Zscaler Client Connector encountered network issues while establishing a connection.
- Fixes an issue where Zscaler Client Connector displayed incorrect connectivity information in the app after a user's device switched from an off-trusted network to a VPN network.

- Fixes an issue where the Zscaler Internet Access (ZIA) trust level was incorrectly calculated using device posture results from the cache after a reboot.
- Fixes an issue for ZIdentity users where the number in the Zscaler Client Connector Version field displayed incorrectly on the Device Management page and in the Registered Device Details window of the Zscaler Client Connector Portal.
- Fixes an issue where ZIdentity users were unable to complete the ZPA reauthentication process.
- Fixes an issue where Windows could display a blue screen for some users when flow logging was enabled.
- Fixes an issue where Zscaler Client Connector could not access an IP-based Zscaler Private Access (ZPA) application due to LWF filters created based on an incomplete application list.
- Fixes an issue where uploads to a network drive were slow when using the Server Message Block (SMB) protocol using ZPA.
- Fixes an issue with tunnel disconnects caused by pacparser crashes due to running out of memory.
- Fixes an issue where users couldn't access a ZPA application at times due to Zscaler Client Connector not removing a stale entry from the dynamic bypass table.
- Updates Zscaler Client Connector to ignore blank serial numbers when generating UDIDs, preventing multiple devices for a single user from having the same UDID.

- Fixes an issue where Zscaler Client Connector remained on the Loading page when reauthenticating ZPA due to a posture evaluation delay.
- Fixes an internal error (`302`) that occurred during a ZPA automatic reauthentication attempt after a user restarted the system.
- Fixes an issue with posture updates that caused Zscaler Client Connector to be in a `Connecting` state for a prolonged time, resulting in a delayed connection to ZPA applications via an external proxy.
- Updates the way Zscaler Client Connector retrieves the MAC Address from the device during registration to prioritize the active adapter connected to the internet.
- Fixes an issue where WFP filters were not deleted correctly after a tunnel crash, resulting in an FW/AV error when trying to reconnect.
- Fixes an issue with Zscaler Digital Experience (ZDX) probes after Zscaler Tunnel (Z-Tunnel) 1.0 failures, even though the Z-Tunnel 2.0 connection was healthy and both the Use Tunnel 2.0 for Proxied Traffic option and the Redirect Web Traffic to Local Proxy option were enabled.
- Fixes a delay in ZPA reauthentication that could occur when loading the page after a user authenticated with an IdP.
- Fixes an issue where Zscaler Client Connector used the incorrect app profile after login for a user who was assigned an app profile configured for a device group using the Registry Key device posture profile with an HKEY_CURRENT_USER registry key.

- Updates Zscaler Client Connector to not launch if a user starts the device in Safe mode.
- Fixes an issue where process-based application bypasses sometimes did not work if the policy update of the app identity list failed.
- Fixes an issue where Zscaler Client Connector did not download the PAC file after switching to a Split VPN-Trusted network with ZIA enabled, which could cause unexpected traffic handling.
- Fixes an issue where the machine tunnel didn’t start after upgrading Zscaler Client Connector.
- Fixes an issue where Zscaler Client Connector stopped working after users clicked Revert App if they had previously opened the app from the tray icon during an upgrade.
- Fixes issues where the ZSATunnel service could crash when restarting due to conflicts in background processes.
- Fixes connectivity issues with SQL Server for customers using ZPA without ZIA or Zscaler Digital Experience (ZDX) sending traffic through Z-Tunnel 1.0 to port 1433.
- Fixes an issue where Zscaler Client Connector didn't connect to the ZPA Service Edge after switching from a machine tunnel to a user tunnel, causing some users to experience authentication errors.
- Fixes an issue where some applications could not be accessed due to Zscaler Client Connector incorrectly proxying HTTP payloads containing binary data.

April 22, 2025

Release Available: Client Connector 4.5.0.434 for Windows

Zscaler Client Connector 4.5.0.434 Enhancements and Fixes

- Fixes a delay in detecting the captive portal when Zscaler Client Connector encountered network issues while establishing a connection.
- Fixes an issue where Zscaler Client Connector displayed incorrect connectivity information in the app after a user's device switched from an off-trusted network to a VPN network.
- Fixes an issue where the Zscaler Internet Access (ZIA) trust level was incorrectly calculated using device posture results from the cache after a reboot.
- Fixes an issue where Windows could display a blue screen for some users when flow logging was enabled.
- Fixes an issue where Zscaler Client Connector could not access an IP-based Zscaler Private Access (ZPA) application due to LWF filters created based on an incomplete application list.
- Fixes an issue where uploads to a network drive were slow when using the SMB (Server Message Block) protocol using ZPA.
- Fixes an issue where users couldn't access a ZPA application at times due to Zscaler Client Connector not removing a stale entry from the dynamic bypass table.
- Updates Zscaler Client Connector to ignore blank serial numbers when generating UDIDs,

preventing multiple devices for a single user from having the same UDID.

- Fixes an issue where Zscaler Client Connector remained on the Loading page when reauthenticating ZPA due to a posture evaluation delay.
- Fixes an internal error (302) that occurred during a ZPA automatic reauthentication attempt after a user restarted the system.
- Updates the way Zscaler Client Connector retrieves the MAC Address from the device during registration to prioritize the active adapter connected to the internet.
- Fixes an issue where WFP filters were not deleted correctly after a tunnel crash, resulting in an FW/AV error when trying to reconnect.
- Fixes a delay in ZPA reauthentication that could occur when loading the page after a user authenticated with an IdP.
- Fixes an issue where Zscaler Client Connector used the incorrect app profile after login for a user who was assigned an app profile configured for a device group using the Registry Key device posture profile with an HKEY_CURRENT_USER registry key.
- Updates Zscaler Client Connector to not launch if a user starts the device in Safe mode.
- Fixes an issue where process-based application bypasses sometimes did not work if the policy update of the app identity list failed.
- Fixes an issue where Zscaler Client Connector did not download the PAC file after switching to a Split VPN-Trusted network with

ZIA enabled, which could cause unexpected traffic handling.

- Fixes an issue where Zscaler Client Connector stopped working after users clicked Revert App if they had previously opened the app from the system tray icon during an upgrade.
- Fixes issues where the ZSATunnel service could crash when restarting due to conflicts in background processes.
- Fixes an issue where Zscaler Client Connector didn't connect to the ZPA Service Edge after switching from a machine tunnel to a user tunnel.

April 16, 2025

Release Available: Client Connector 4.4.0.428 for Windows

Zscaler Client Connector 4.4.0.428 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector displayed incorrect connectivity information in the app after a user's device switched from an off-trusted network to a VPN network.
- Fixes an issue where the Zscaler Internet Access (ZIA) trust level was incorrectly calculated using device posture results from the cache after a reboot.
- Updates Zscaler Client Connector to ignore blank serial numbers when generating unique device identifiers (UDIDs), preventing multiple devices for a single user having the same UDID.

- Updates the way Zscaler Client Connector retrieves the MAC Address from the device during registration to prioritize the active adapter connected to the internet.
- Fixes a delay in Zscaler Private Access (ZPA) reauthentication that could occur when loading the page after a user authenticated with an IdP.
- Fixes an issue where Zscaler Client Connector used the incorrect app profile after login for a user who was assigned an app profile configured for a device group using the Registry Key device posture profile with an HKEY_CURRENT_USER registry key.
- Fixes an issue where process-based application bypasses sometimes did not work if the policy update of the app identity list failed.

March 07, 2025

Release Available: Client Connector 4.6.0.168 for Windows

Zscaler Client Connector 4.6.0.168 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.6.0.216.

- Fixes an issue where the ZSATunnel process could crash and sometimes create dump files in the export logs after a fragmented packet was received.
- Fixes an issue where some apps couldn't connect to the internet if Zscaler Client Connector was installed using strict enforcement and Remove Existing Exempted Containers was enabled.
- Fixes an issue where Zscaler Client Connector displayed an `Internal Error` message during device startup due to the Network Driver Interface Specification (NDIS) not binding the Zscaler Client Connector Windows Filter Driver to the network adapter.
- Fixes an issue where users with Zscaler Private Access (ZPA) and either Zscaler Digital Experience (ZDX) or Zscaler Active Defense (ZAD) could receive an `Internal Error, Please Contact Admin [10112]` message and be unable to log in to Zscaler Client Connector.
- Fixes an issue where a ZIdentity user could not log in to Zscaler Client Connector if their login name included a special character (e.g., # or @).
- Improves Zscaler Client Connector's handling of unattended installs when anti-tampering is enabled.
- Fixes an issue where the ZPA reauthentication required notification didn’t display as a pop-up or in the Notifications window for enrolled users after Automatically Attempt ZPA Reauthentication was disabled.
- Fixes an issue where ZDX probes sent via Zscaler Tunnel (Z-Tunnel) 1.0 were not

forwarded to the specific proxy address configured in the app profile.

- Fixes an issue that prevented Zscaler Client Connector from establishing a Zscaler Internet Access (ZIA) Z-Tunnel 2.0 connection when the ZIA Service Edge was configured as a ZPA application.
- Fixes an issue where an echo test request was sent to ZPA from a device on a dual-stack network if the synthetic IP range was beyond the 100.64.0.0/16 default range.
- Fixes an issue where the Microsoft System Center Configuration Manager (SCCM) ClientAlwaysOnInternet registry key was not updated based on the SCCM Client configuration after switching from a Trusted network to an Off-Trusted network or vice versa.
- Fixes an issue where the connection from Zscaler Client Connector to the ZPA Public Service Edge was not closed correctly, which could result in a slow response from the server.
- Fixes an issue where an `Internal Error` message displayed when authenticating ZPA if ZPA was enabled after the user logged in to Zscaler Client Connector.
- Fixes an issue where tunnel crashes were observed from pacparser failures due to a Windows API failing to fetch the proxy PAC file after Zscaler Client Connector was connected using ZPA, ZDX, and ZIA with a forwarding profile of None.
- Fixes an issue where ZPA reauthentication could fail after upgrading Zscaler Client

Connector from a much earlier version (e.g., Zscaler Client Connector version 3.7).

March 06, 2025

Release Available: Client Connector 4.5.0.381 for Windows

Zscaler Client Connector 4.5.0.381 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.5.0.434.

- Updates Npcap to version 1.80.
- Fixes an issue with anti-tampering that could cause a driver error when upgrading Zscaler Client Connector.
- Fixes an issue where the ZSATunnel process could crash and sometimes create dump files in the export logs after a fragmented packet was received.
- Fixes an issue where some apps couldn't connect to the internet if Zscaler Client Connector was installed using strict enforcement and Remove Existing Exempted Containers was enabled.
- Fixes an issue where Zscaler Client Connector displayed an `Internal Error` message during device startup due to the Network Driver Interface Specification (NDIS)

not binding the Zscaler Client Connector Windows Filter Driver to the network adapter.

- Fixes an issue where Zscaler Client Connector did not register with Zscaler Private Access (ZPA) client-to-client capability and could not be connected to via RDP over ZPA.
- Fixes an issue where a ZIdentity user could not log in to Zscaler Client Connector if their login name included a special character (e.g., # or @).
- Improves Zscaler Client Connector's handling of unattended installs when anti-tampering is enabled.
- Fixes an issue where Zscaler Client Connector displayed a `Server Down` error after connecting to the default gateway if the primary and secondary proxy addresses in the PAC file were unavailable when using Tunnel with Local Proxy.
- Fixes an issue where the ZPA reauthentication required notification didn't display as a pop-up or in the Notifications window for enrolled users after Automatically Attempt ZPA Reauthentication was disabled.
- Fixes an issue where Zscaler Digital Experience (ZDX) probes sent via Zscaler Tunnel (Z-Tunnel) 1.0 were not forwarded to the specific proxy address configured in the app profile.
- Fixes an issue that prevented Zscaler Client Connector from establishing a Zscaler Internet Access (ZIA) Z-Tunnel 2.0 connection when the ZIA Service Edge was configured as a ZPA application.

- Fixes an issue where an echo test request was sent to ZPA from a device on a dual-stack network if the synthetic IP range was beyond the 100.64.0.0/16 default range.
- Fixes an issue where the Microsoft System Center Configuration Manager (SCCM) ClientAlwaysOnInternet registry key was not updated based on the SCCM Client configuration after switching from a Trusted network to an Off-Trusted network or vice versa.
- Fixes an issue where the connection from Zscaler Client Connector to the ZPA Public Service Edge was not closed correctly, which could result in a slow response from the server.
- Fixes an issue where tunnel crashes were observed from pacparser failures due to a Windows API failing to fetch the proxy PAC file after Zscaler Client Connector was connected using ZPA, ZDX, and ZIA with a forwarding profile of None.
- Fixes an issue where ZPA reauthentication could fail after upgrading Zscaler Client Connector from a much earlier version (e.g., Zscaler Client Connector version 3.7).

March 05, 2025

Release Available: Client Connector 4.4.0.406 for Windows

Zscaler Client Connector 4.4.0.406 Enhancements and Fixes

- Updates Npcap to version 1.80.
- Fixes an issue with anti-tampering that could cause a driver error when upgrading Zscaler

Client Connector.

- Fixes an issue where the ZSATunnel process could crash and sometimes create dump files in the export logs after a fragmented packet was received.
- Fixes an issue where some apps couldn't connect to the internet if Zscaler Client Connector was installed using strict enforcement and Remove Existing Exempted Containers was enabled.
- Fixes an issue where Zscaler Client Connector did not register with Zscaler Private Access (ZPA) client-to-client capability and could not be connected to via RDP over ZPA.
- Improves Zscaler Client Connector's handling of unattended installs when anti-tampering is enabled.
- Fixes an issue where the ZPA reauthentication required notification didn’t display as a pop-up or in the Notifications window for enrolled users after Automatically Attempt ZPA Reauthentication was disabled.
- Fixes an issue where Zscaler Digital Experience (ZDX) probes sent via Zscaler Tunnel (Z-Tunnel) 1.0 were not forwarded to the specific proxy address configured in the app profile.
- Fixes an issue that prevented Zscaler Client Connector from establishing a Zscaler Internet Access (ZIA) Z-Tunnel 2.0 connection when the ZIA Service Edge was configured as a ZPA application.
- Fixes an issue where an echo test request was sent to ZPA from a device on a dual-

stack network if the synthetic IP range was beyond the 100.64.0.0/16 default range.

March 04, 2025

Release Available: Client Connector 4.3.0.277 for Windows

Zscaler Client Connector 4.3.0.277 Enhancements and Fixes

- Fixes an issue with anti-tampering that could cause a driver error when upgrading Zscaler Client Connector.
- Fixes an issue where the ZSATunnel process could crash.
- Improves Zscaler Client Connector's handling of unattended installs when anti-tampering is enabled.
- Fixes an issue where the Zscaler Private Access (ZPA) reauthentication required notification didn’t display as a pop-up or in the Notifications window for enrolled users after Automatically Attempt ZPA Reauthentication was disabled.
- Fixes an issue that prevented Zscaler Client Connector from establishing a Zscaler Internet Access (ZIA) Z-Tunnel 2.0 connection when the ZIA Service Edge was configured as a ZPA application.

February 07, 2025

Release in Limited Availability: Client Connector 4.6.0.146 for Windows

Zscaler Client Connector 4.6.0.146 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.6.0.216.

- Fixes an issue where the Firewall device posture check could fail even though the firewall was enabled on the user device.
- Limits the total size of all Zscaler log files for all Windows user profiles to 500 MB on a machine with Zscaler Client Connector integrated with Imprivata by deleting the oldest files when the maximum is reached.
- Fixes an issue with anti-tampering that could cause a driver error when upgrading Zscaler Client Connector.
- Fixes an issue where packet capture failed to start but a notification displayed that packet capture was started and quickly finished.
- Fixes an issue where ZSAHelper log files were created frequently for forwarding profiles with the Route-Based tunnel driver type and Enable Split VPN Trusted Network disabled.
- Fixes an issue where Zscaler Client Connector did not prevent the Windows Defender firewall domain profile from being applied to the device even though the device network type (e.g., Off Trusted Network) was selected in Block Domain Profile Detection.

- Fixes an issue where the Zscaler Client Connector tray icon disappeared after logging in due to receiving two authentication responses via browser-based authentication.
- Fixes an issue where the Service Status on the Private Access window continued to display as `Connecting` after a change in network type, even though the traffic was forwarded correctly to the Zscaler service.
- Fixes an issue where Zscaler Client Connector did not correctly close an existing Zscaler Private Access (ZPA) app session when in the ZPA forced reauthentication state.
- Fixes an issue where the incorrect forwarding action (tunnel or bypass) could be applied because the network detection process wasn't re-run after reconnecting to a network that was interrupted initially.
- Fixes an issue where Zscaler Client Connector removed loopback exemptions even though the Remove Existing Exempted Containers feature was disabled.
- Fixes an issue where users on a dual stack network or an IPv6-only network intermittently were unable to access ZPA applications after the device woke up from sleep mode.
- Fixes an issue where user traffic bypassed the Zscaler cloud (e.g., users could access restricted websites) for a short interval of time while the Zscaler Tunnel (Z-Tunnel) 2.0 was connecting due to a network type switch.
- Fixes an issue where a partner tenant did not reconnect after a machine reboot.

- Fixes an issue where the Private Access tab did not automatically display for a user who was assigned service entitlement to ZPA in ZIdentity after upgrading Zscaler Client Connector.
- Fixes an issue where Zscaler Client Connector took a long time to connect after rebooting because of a trusted network evaluation delay with IPv6 DNS servers using a forwarding profile with Drop IPv6 Packets enabled.
- Fixes an issue where DNS traffic in Domain Inclusion was not forwarded because Zscaler Client Connector's internal DNS proxy state was stuck in an initialized state after network disconnect and reconnect events.
- Fixes an issue where Zscaler Client Connector did not register with ZPA client-to-client capability and could not be connected via RDP over ZPA.
- Fixes an issue where Zscaler Client Connector continually displayed `Registering Device` after a ZIdentity user reauthenticated even though the device was successfully registered.

January 24, 2025

Release Available: Client Connector 4.5.0.366 for Windows

Zscaler Client Connector 4.5.0.366 Enhancements and Fixes

This version of Zscaler Client Connector has a known issue where the cached ports for source port-based bypasses were not

being cleared, leading to high memory consumption and new connections being blocked or unintentionally bypassed. The issue has been corrected on Zscaler Client Connector version 4.5.0.434.

- Fixes an issue where Zscaler Client Connector intermittently did not follow IP-based Zscaler Tunnel (Z-Tunnel) 2.0 inclusion and exclusion rules.
- Limits the total size of all Zscaler log files for all Windows user profiles to 500 MB on a machine with Zscaler Client Connector integrated with Imprivata by deleting the oldest files when the maximum is reached.
- Fixes an issue where packet capture failed to start but a notification displayed that packet capture was started and quickly finished.
- Fixes an issue where ZSAHelper log files were created frequently for forwarding profiles with the Route-Based tunnel driver type and Enable Split VPN Trusted Network disabled.
- Fixes an issue where Zscaler Client Connector did not prevent the Windows Defender firewall domain profile from being applied to the device even though the device network type (e.g., Off Trusted Network) was selected in Block Domain Profile Detection.
- Fixes an issue where the Zscaler Client Connector tray icon disappeared after logging in due to receiving two authentication responses via browser-based authentication.
- Fixes an issue where the Service Status on the Private Access window continued to display as `Connecting` after a change in

network type, even though the traffic was forwarded correctly to the Zscaler service.

- Fixes an issue where the incorrect forwarding action (tunnel or bypass) could be applied because the network detection process wasn't re-run after reconnecting to a network that was interrupted initially.
- Fixes an issue where Zscaler Client Connector removed loopback exemptions even though the Remove Existing Exempted Containers feature was disabled.
- Fixes an issue where user traffic bypassed the Zscaler cloud (e.g., users could access restricted websites) for a short interval of time while the Z-Tunnel 2.0 was connecting due to a network type switch.
- Fixes an issue where a partner tenant did not reconnect after a machine reboot.
- Fixes an issue where the Private Access tab did not automatically display for a user who was assigned service entitlement to Zscaler Private Access (ZPA) in ZIdentity after upgrading Zscaler Client Connector.
- Fixes an issue where Zscaler Client Connector took a long time to connect after rebooting because of a trusted network evaluation delay with IPv6 DNS servers using a forwarding profile with Drop IPv6 Packets enabled.
- Fixes an issue where DNS traffic in Domain Inclusion was not forwarded because Zscaler Client Connector's internal DNS proxy state was stuck in an initialized state after network disconnect and reconnect events.
- Fixes an issue where Zscaler Client Connector continually displayed Registering

Device after a ZIdentity user reauthenticated even though the device was successfully registered.

January 23, 2025

Release Available: Client Connector 4.4.0.395 for Windows

Zscaler Client Connector 4.4.0.395 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector intermittently did not follow IP-based Zscaler Tunnel (Z-Tunnel) 2.0 inclusion and exclusion rules.
- Limits the total size of all Zscaler log files for all Windows user profiles to 500 MB on a machine with Zscaler Client Connector integrated with Imprivata by deleting the oldest files when the maximum is reached.
- Fixes an issue where packet capture failed to start but a notification displayed that packet capture was started and quickly finished.
- Fixes an issue where ZSAHelper log files were created frequently for forwarding profiles with the Route-Based tunnel driver type and Enable Split VPN Trusted Network disabled.
- Fixes an issue where the Zscaler Client Connector tray icon disappeared after logging in due to receiving two authentication responses via browser-based authentication.
- Fixes an issue where a partner tenant did not reconnect after a machine reboot.
- Fixes an issue where Zscaler Client Connector took a long time to connect after rebooting because of a trusted network

evaluation delay with IPv6 DNS servers using a forwarding profile with Drop IPv6 Packets enabled.

January 21, 2025

Release Available: Client Connector 4.3.0.272 for Windows

Zscaler Client Connector 4.3.0.272 Enhancements and Fixes

- Fixes an issue where Zscaler Client Connector intermittently did not follow IP-based Zscaler Tunnel (Z-Tunnel) 2.0 inclusion and exclusion rules.
- Fixes an issue where ZSAHelper log files were created frequently for forwarding profiles with the Route-Based tunnel driver type and Enable Split VPN Trusted Network disabled.
- Fixes an issue where the Zscaler Client Connector tray icon disappeared after logging in due to receiving two authentication responses via browser-based authentication.

Was this article helpful? Click an icon below to submit feedback.