



Zscaler is an alternative to VPN that utilizes a different method of allowing users access to resources within an internal network. It operates on the application layer whereas traditional VPNs operate on the network layer. It uses tunneling to transmit data between the client and desired resource. Zscaler's zero trust remote

access service securely connects trusted users to trusted internal applications, without placing remote users on the network as is done with VPN.

The Zscaler solution is made up of two primary modules; **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)**.

Zscaler Internet Access
<p>Zscaler Internet Access (ZIA) is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet onramp when connected with the Zscaler Client Connector. No matter where users connect—from home, a coffee shop, a hotel, or the office—they get identical protection.</p> <p>ZIA sits between the users and the internet, inspecting every byte of traffic inline across multiple security techniques, even within SSL providing full protection from web and internet threats.</p> <p>ZIA is managed and supported by the ESS- Security Team. Any questions, concerns, or tickets for ZIA should be directed to the ESS- Security Team by contacting the Service Center, ServiceCenterSOS@cms.hhs.gov.</p>
Zscaler Private Access
<p>Zscaler Private Access (ZPA) is a cloud service from Zscaler that provides seamless, zero trust access to private applications running on public cloud or within the data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them. Users are never placed on the network. This zero trust network access (ZTNA) approach supports both managed and unmanaged devices and any private application.</p> <p>ZPA is managed and supported by the ESS- Access Management Team. Any questions, concerns, or tickets for ZPA should be directed to the ESS- Access Management Team by contacting the Service Center, ServiceCenterSOS@cms.hhs.gov.</p>

Zscaler Updates

4/17/2024 - Please ensure that you are using the most up to date version of Zscaler, [Zscaler Installer - User Instructions](#).

Need Help ?

Please contact one of the following:

- CCSQ Support Central:** Provides you with multi-program support to submit a new ticket, and track the status of an existing case, incident, or request. No login required. https://cmsqualitysupport.servicenowservices.com/ccsq_support_central
- Service Center:** Feel free to contact the CCSQ Service Center at:

Phone: (866) 288-8914 (TRS:711)

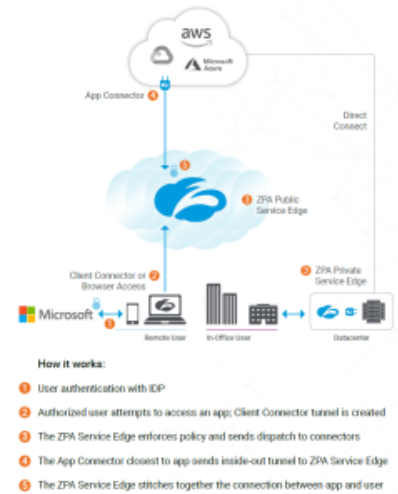
Slack: #help-service-center-sos

Email: ServiceCenterSOS@cms.hhs.gov

Hours of Operation: 24/7

How ZPA Works

When a user attempts to access an application, the user's identity and device posture are verified using Zscaler™ Client Connector software installed on the user device. Policy is checked, and a ZPA Service Edge determines where the closest application instance exists. Next, two outbound tunnels, one from the Client Connector on the device and the other from the App Connector, are stitched together by a ZPA Service Edge. All of this takes place automatically and in real time. Below is a look at the ZPA architecture:



Who Will Get Zscaler?

The users that require access to the Zscaler solution consist of contractors approved for services connecting to the QualityNet network included but not limited listed below.

- AWS Environment
- Splunk
- CloudBees Jenkins
- Ansible Tower
- Tenable Nessus
- Nexus RM
- Nexus IQ
- CMSNet resources
- CyberArk
- CASPER
- Cloudbees Jenkins Enterprise (CJE)

For requests outside of the initial onboarding process please refer to the [Getting Started](#) tab.

Quick Start Notes

- Zscaler utilizes a client which **must** be installed on any Contractor Furnished Equipment (CFE)/Government Furnished Equipment (GFE) computer that will use it.
- Zscaler **must** be configured for an organization before it can be used on CFE/GFE computers.
- End users **must** be approved by their SO within HARP prior to obtaining access. Follow steps in Requesting the Zscaler User Access Role within HARP below.
- Contractors installing Zscaler will need administrator rights to successfully install the client.

The Zscaler Adoption Process

Organizations Seeking Zscaler

If you are a new organization and need access to the QualityNet environment you will require Zscaler. These organizations will be granted access during the ISG contract onboarding process. For more information please contact the Contract Engagement team ISGContractorOnboardingServices@cms.hhs.gov.

For new organizations, Contract Onboarding can assist you through these processes.

ORGANIZATIONS REQUESTING ZSCALER

Listed below are the steps for an organization to request Zscaler. Expand the steps below to view the process.

All Zscaler users will require a valid HARP ID. For instructions on the process, refer to the HARP page.

Organizations are required to install the Zscaler client on their corporate machines. Please refer to the [Zscaler Installation Instructions](#) page to download copies of installation guides as well as the client installation packages.

Additionally, the client installation packages can be obtained by contacting the Service Center @ 866-288-8914 (TRS: 711), slack channel [help-service-center-sos](#) or via email at ServiceCenterSOS@cms.hhs.gov.

If you have issues, please submit a Service Request within ServiceNow requesting support for Zscaler Installation. The ticket will be routed to the ESS Access Management Team.

Once your organization is added to the vetted list, your end users can utilize HARP to request Zscaler as a service. The SO will be able to automatically approve requests from end users.

Once your organization has been added to the vetted list, Zscaler has been installed and the end user has been approved via HARP, you are ready to access and use Zscaler. For information on how to get started, please refer to the [Zscaler User Guide](#).

Note: Feel free to contact the Service Center-SOS for assistance with instructions if needed.

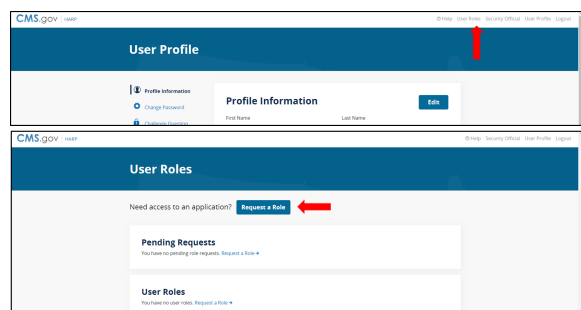
Service Center @ 866-288-8914 (TRS: 711), slack channel [help-service-center-sos](#) or via email at ServiceCenterSOS@cms.hhs.gov

If Your Organization Already Has Zscaler and You Are a New User - How to Request?

REQUESTING THE ZSCALER USER ACCESS ROLE WITHIN HARP

Once you have created your HARP account (For instructions on the process, refer to the [HARP page](#)), the next step is to request the Zscaler User Access User role. Expand the steps below to view the process.

Go to <https://harp.qualitynet.org> and log into your HARP account.



Select a Program

Select a CMS program to begin the role request process.

- ☐ Data Element Library-DEL
- ☐ ESS-DEVTEAM-SBX
- ☐ ESS-QATEAM-SBX
- ☐ ESS-SECTEAM-SBX
- ☐ Headless Content Management (Hi-CMS)
- ☐ Managed File Transfer
- ☐ Managed File Transfer Admin
- ☐ QMARS
- ☐ QTSO
- ☐ QualityNet Atlassian
- ☐ QualityNet IT Services
- ☐ QualityNet-New Relic
- ☒ QualityNet-Zscaler
- ☐ ServiceNow Quality System

User Roles

1 2 3

Select an Organization

Select your organization for the **QualityNet-Zscaler** program.

- ☐ ADO-ASPEN-Alpine Technology Group
- ☐ ADO-DARRT-SemanticBits
- ☐ ADO-DEL-Nguyen Information Consulting
- ☐ ADO-EQRS-Mantech
- ☐ ADO-ESS-Ventura
- ☐ ADO-FIVS-Customer Value Partners
- ☐ ADO-HCQAR-Customer Value Partners
- ☐ ADO-HCQIS-FC-Flexion
- ☐ ADO-HEIST-Titania Solutions Group
- ☐ ADO-HIDS-Ventech Solutions
- ☐ ADO-HQR-Bellese Technology

User Roles

1 2 3

Select Roles

Select one or many roles for the level of access you need for **ADO-HIDS-Ventech Solutions**.

- ☐ Zscaler-Security Official
- ☒ Zscaler-User Access

< 1 >

Cancel

Once your role has been approved by your SO, you will then have access to Zscaler

Zscaler User Guide



use, tight security and cost feasibility. Zscaler will be the preferred method to access tools and applications residing on the QualityNet network as we retire our legacy VPN connectivity technology.

Zscaler is a cloud hosted, Enterprise Shared Services (ESS) supported service that is currently available to end users within QualityNet organizations. Zscaler was chosen, piloted and deployed due to its ease of

- For IT Administrators - [Zscaler Installation Instructions](#) (Includes: Instructions, Client, Certs and Scripts)
- For Security Officers (SOs) or Account Administrators (AAs) - Please review [Getting Started](#) page.
- Complete [Zscaler User Guide](#) - From the Vendor

Security Guidelines

- [HCQIS CFE Data Management Policy](#)
- [Rules of Behavior](#)

Frequently Asked Questions

Zscaler is an alternative to VPN that utilizes a different method of allowing users access to resources within an internal network. It uses tunneling to transmit data between the client and desired resource. This approach eliminates the need to have clients enter into the network directly as is done with VPN.

The Zscaler solution is made up of two primary modules; Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA).

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Before reaching the user, ZIA inspects every byte of traffic inline across multiple security techniques, even within SSL providing full protection from web and Internet threats.

Zscaler Private Access (ZPA) provides secure remote access and works by abstracting a private, internal application from the network on which it resides and provides specific applications access to authorized users via encrypted, per session micro tunnels that are created upon demand.

When logged into Zscaler (utilizing both ZIA and ZPA) you will be able to reach tools residing on the QualityNet network such as AWS or QualityNet applications. It will also allow access Internet facing sites that your organization's firewall and anti-virus policies allow access to.

When logged into Zscaler (utilizing both ZIA and ZPA), you will not be able to access anything that your organizations Firewall or Anti-virus policies prohibit. Please reach out to your IT Administrator for information regarding policies for your organizations firewall and anti-virus configurations.

Please refer to the [How to Request Zscaler Confluence Page](#). This page provides information for New and Existing QualityNet contractors.

SOs should be submitting requests for Zscaler via a ServiceNow request or inquiry with the QualityNet Service Desk. The "How to Request Zscaler" Confluence page lays out all these details.

Yes. You can use the Outlook Desktop Application or Outlook on the Web or what is formerly known as OWA.

No. The reason for this configuration is to enforce protection of the computer while connected to QualityNet using Zscaler. ZIA provides threat protection for Internet traffic reducing overall risk that the computer will become infected by an external threat while connected to QualityNet. Only a Zscaler Private Access Administrator (not local IT Admin) can turn off ZIA and still remain active with their ZPA account.

Yes. However, you will not be able to access information or tools residing upon the QualityNet network such as AWS or QualityNet applications such as those residing on [QualityNet.org](#).

Yes. If your organization is using Split-Tunneling or Full-Tunneling settings within your VPN, please be prepared to share your VPN HostName (or IP) with ESS Access Management. Additional configurations may be required within your settings to properly route traffic, and allow users to access both corporate systems as well as QualityNet systems simultaneously.

If you or an end user within your organization is receiving the following error when logging into Zscaler "Endpoint FW/AV Error", then your organizations Firewall (FW) or Antivirus (AV) is blocking Zscaler, causing it to be non-operational. To remedy this, your organization's IT Administrator will have to white-list a specific subnet within your FW or AV.

If you run into this issue during configuration or thereafter, please submit a ticket within ServiceNow referencing the error you received. ESS Access Management will provide the proper subnet to white-list.

If you cannot access a tool, drive, host or server that you normally could prior to Zscaler, first bring this up with your organization's IT Administrator or colleagues to ensure that naming conventions are using Fully Qualified Domain Names (FQDN). A FQDN is the complete domain name for a specific computer, or host, on the internet. The FQDN consists of two parts: the hostname and the domain name.

- For example: Use "<http://hostname.domain/test/>" or "<http://hostname.qnet.qualnet.org/test/>"
 - Only using <http://hostname/test/> will not work on Zscaler, but would work on the current VPN setup

If FQDN names are being used or were added and access is still not available, then submit a ServiceNow ticket and assign to ESS Access Management Team. Please include detailed information such as the tool, host and server name. The ESS Access Management team may have to add this tool, drive, host or server to your network segment group to ensure all at your organization with access can get to it in the future.

No, not at this time. The mobile (Android and iOS) policies have been disabled at this time. If the use of Zscaler via mobile becomes a necessity for a number of users, this feature could be addressed at a later time.

If you are experiencing any issues with Zscaler such as installation, errors, loss of service or any other problems, please contact the Service Center @ 866-288-8914 (TRS: 711) or via email at ServiceCenterSOS@cms.hhs.gov.

Please provide as much information, error codes or screenshots if possible to allow for quick troubleshooting.

If you are experiencing this error when attempting to log into Zscaler, your Security Point of Contact needs to open a Service Now Request for your HARP ID to be configured for Zscaler. The ticket should be assigned to ESS-HARP team.

If you are experiencing this error when attempting to log into Zscaler, first you should verify you are able to log in and that your token method set up for your HARP ID is working by going to <https://harp.cms.gov>. If you are able to log in there and the problem with logging into Zscaler continues, then try rebooting your workstation.

According to Zscaler support, the only Windows Disk Encryption supported by Zscaler is BitLocker. All 3rd party encryption is not recognized. An Enhancement Request has been submitted "To provide 3rd party support for encryption products". However, there is no planned/expected release date at this time.

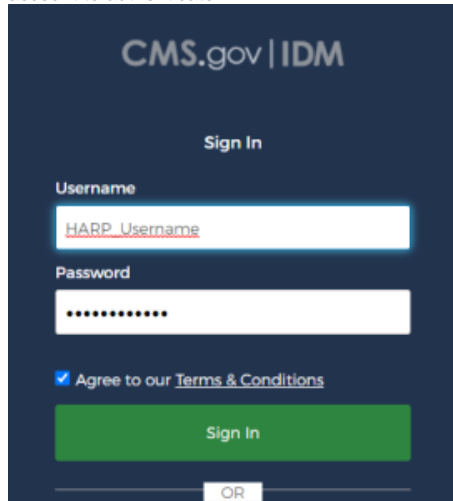
Issue: All RHEL AMIs have routing settings that force the Zscaler networks over the Management interface on the host. Due to this static routing configuration, Zscaler connections will not be allowed to the Functional interface on the host. This will prevent users being able to reach application web pages while logged into Zscaler.

To resolve this issue please contact the Service Center @ 866-288-8914 (TRS: 711), slack channel [help-service-center-sos](#) or via email at ServiceCenterSOS@cms.hhs.gov.

The ADO or Customer Success Manager will submit a ServiceNow Ticket assigned to the ESS-HARP team.

The concept of zero trust has been around for more than a decade, yet there's been a lot of confusion about what the term actually means. It is not simply a single technology. Zero trust is a holistic approach to securing modern organizations, based on least-privileged access and the principle that no user or application should be inherently trusted. It begins with the assumption that everything is hostile, and only establishes trust based upon the user identity and context, with policy serving as the gatekeeper every step of the way.

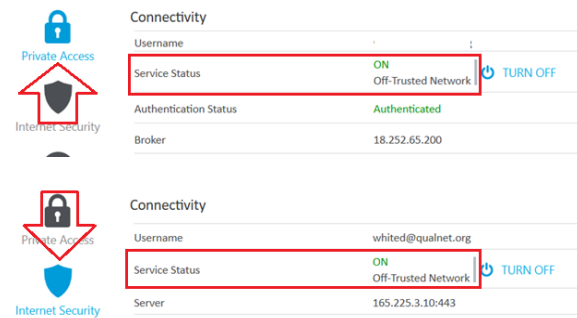
Zscaler uses your HARP ID for its login credentials. You will also use the same MFA for your HARP account to authenticate.



The image shows a sign-in page for CMS.gov | IDM. It has a dark blue background. At the top, it says "CMS.gov | IDM". Below that is "Sign In". There are two input fields: "Username" with "HARP Username" entered, and "Password" with masked characters. Below the password field is a checkbox labeled "Agree to our Terms & Conditions". At the bottom is a green "Sign In" button. Below the button is a small "OR" button.

No. Zscaler works on the application layer and not the network layer the way traditional VPN clients work. Unlike VPNs, Zscaler uses Zero Trust Network Access (ZTNA) technologies to deliver a means of application access without network access, and the ability to mask applications from the open internet.

Zscaler has 2 types of connections, Private Access and Internet Security. You can confirm connectivity for both by opening Zscaler and clicking the Private Access or Internet Security icons and then checking the Service Status.

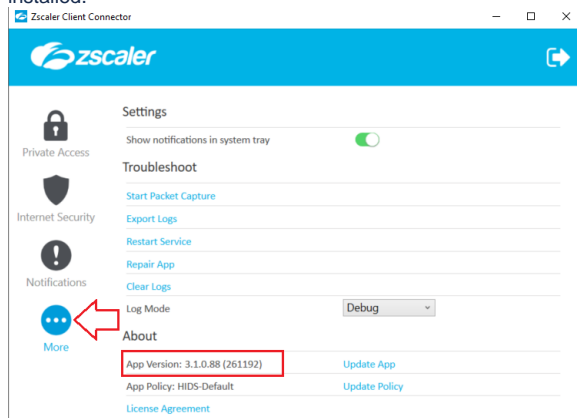


The image shows two screenshots of the Zscaler interface. The top screenshot is for "Private Access" and the bottom is for "Internet Security". Both show a "Connectivity" table with columns for Username, Service Status, Authentication Status, and Broker. In both, the Service Status is "ON" and "Off-Trusted Network" is highlighted with a red box. A red arrow points to the "TURN OFF" button in the top screenshot. In the bottom screenshot, a red arrow points to the "More" icon in the left sidebar.

Connectivity			
Username			
Service Status	ON	Off-Trusted Network	TURN OFF
Authentication Status	Authenticated		
Broker	18.252.65.200		

Connectivity			
Username	whited@qualnet.org		
Service Status	ON	Off-Trusted Network	TURN OFF
Server	165.225.3.10:443		

Open Zscaler and click the More icon. Under the About section you should see the version of Zscaler installed.



The image shows the Zscaler Client Connector application window. The title bar says "Zscaler Client Connector". The main window has a blue header with the Zscaler logo. On the left is a sidebar with icons for Private Access, Internet Security, Notifications, and More. The "More" icon is highlighted with a red arrow. The main content area shows the "About" section, which includes "App Version: 3.1.0.88 (261192)" highlighted with a red box, and links for "Update App", "Update Policy", and "License Agreement".

Yes. Click the More icon and there is a Troubleshoot section that has multiple utilities to both address issues you may be having with the client like Restart Service or Repair App. In addition, it has options to help in providing troubleshooting details to support teams like Export Logs and Start Packet Capture which can assist in identifying and resolving issues more quickly.

blocked URL

- **Start Packet Capture:** If your organization's admin enabled packet captures, you can use this feature when reproducing an issue. To learn more, see [Using the Start Packet Capture Option](#).
- **Report an Issue:** If your organization's admin enabled in-app support access, you can use this feature to report an issue. When you submit the form, depending on your organization's set up, Zscaler Client Connector can send an email to your organization's support admin or submit a ticket directly to Zscaler Support (your support admin will receive a copy of this ticket as well). After you submit the form, you will receive an email acknowledging the support request. For instructions on completing the form, see [Reporting an Issue with Zscaler Client Connector for Windows](#).
- **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
- **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
- **Clear Logs:** You can clear stored logs.
- **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. Below is a description of each log mode.
 - **Error:** Logs only when the app encounters an error and functionality is affected.
 - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
 - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.
 - **Debug:** Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

Reference the links below for a full list of the various errors, their meaning, and steps to resolve them.

- Cloud Authentication Error Codes - <https://help.zscaler.com/z-app/zscaler-app-errors#cloud-authentication>
- ZPA Authentication Errors - <https://help.zscaler.com/z-app/zscaler-app-zpa-authentication-errors>
- Cloud Error Codes - <https://help.zscaler.com/z-app/zscaler-app-errors#cloud>
- Zscaler Client Connector Portal Error Codes - <https://help.zscaler.com/z-app/zscaler-app-errors#mobile-admin-portal>
- Zscaler Connection Status Errors - <https://help.zscaler.com/z-app/zscaler-app-connection-status-errors>
- Report an Issue Error Codes - <https://help.zscaler.com/z-app/zscaler-app-errors#report-an-issue>

You can log out of Zscaler at any time by clicking the arrow icon in the top right corner of the Zscaler screen.



No. Zscaler handles no network segmentation of any kind. Network isolation is handled via Security Groups and VPC configurations which are managed by the CCOM Team. When SSL inspection is enabled, the Zscaler service establishes a separate SSL tunnel with the user's browser and with the destination server. The diagram below shows the Zscaler SSL inspection process:

1. A user opens a browser and sends an HTTPS request.
2. The Zscaler service intercepts the HTTPS request. Through a separate SSL tunnel, the service sends its own HTTPS request to the destination server and conducts SSL negotiations.
3. The destination server sends the Zscaler service its certificate with its public key.
4. The Zscaler service and destination server complete the SSL handshake. The application data and subsequent messages are sent through the SSL tunnel.
5. The Zscaler service conducts SSL negotiations with the user's browser. It sends the browser the Zscaler intermediate certificate or your organization's custom intermediate root as well as a server certificate signed by the Zscaler intermediate CA. The browser validates the certificate chain in the browser's certificate store.
6. The Zscaler service and the browser complete the SSL handshake. The application data and subsequent messages are sent through the SSL tunnel.

blocked URL

<https://help.zscaler.com/zia/about-ssl-inspection>

Contractors are responsible for installing the Zscaler client as well as certificates on Go-Co or Customer Furnished Equipment (CFE). ESS will support Contractors with Zscaler installations, but will not conduct the actual installations for organizations.

Key Things to Keep in Mind:

1. It is highly recommended that ADO IT Administrators proceed with the Zscaler installation for their organizations. Admin access is required for the install.
2. Installation Instructions and the Zscaler Installation package can be found in Confluence at: [Z Scaler Installation Instructions](#)
3. Zscaler installation package contains:
 - a. Zscaler client
 - b. Necessary Certificates
 - c. Scripts to install

Need help?

Feel free to submit Service Request for Zscaler Client Installation Support within ServiceNow or contact the service desk @ 866-288-8914 or via email at ServiceCenterSOS@cms.hhs.gov if you need assistance.