Zscaler Recommended Baseline Policy

Goal of Recommended Baseline Policies

- The entire Zscaler Ecosystem including Professional Services, Support, Customer Success, and even Sales should be recommending the same Baseline Policies to our customers.
- The intention of Baseline Policies is to give customers a good **starting point** to build their policies.
- The Recommended Baseline Policies are common sense policies that provide customers with a **strong security foundation** that they can (and should) build on.

Expectations of Recommended Baseline Policies

- Recommended Baseline Policies are built to address the **most common scenarios** (e.g. 80% of our customers). Customers with unique edge cases or complex environments may need to tweak the policies.
- These recommendations and leading practices are based on the Zscaler suite "as is", meaning they are subject to change as the product and external factors evolve.

These documents may be shared with customers. It contains extra context, descriptions about the product, and links to Help Articles that customers should find useful.

Table of Contents

File Type Control

About File Type Control Policies

Purpose of File Type Controls

1. Regulate and monitor data flow.
2. Block unscannable content and prevent inappropriate transfers.
3. Mitigate the risk of sensitive information leakage.
4. Enhance compliance with data protection regulations.
5. Protect against unauthorized access and cyber threats.

File Type Control policies provide the following benefits:

- Restrict the upload and download of various types of files, including unknown file types.
- Define rules to restrict the transmission of various files and apply them to individuals, groups, departments, and locations.
- Allow, caution, or block uploads and downloads. You can configure end-user notifications to explain the action for blocked uploads and downloads.
- Define rules according to corporate policy and follow the recommended baseline policies described.

File Type Control Constraints:

- We recommend adding File Type Control rules for files that can't use Sandbox or Zero Trust browser (Browser Isolation), such as Database, Movies, Executables, and Source Code. Archives are advised not to be included in Filetype Control if "Advanced Sandbox SKU" is available.
- There is a 400MB file size limitation for file scanning.

For more information, please refer to the following knowledge-based articles:

- About File Type Control
- Configuring the File Type Control Policy | Zscaler

Rule Order	Rule Name	Criteria	Action	Description
1	Allow_Trusted_Unscannable	ACTIVE CONTENT **Disabled** FILE TYPES **Any** URL Categories **Operating System and Software Updates; Custom_Allow_Unscannable_Files (custom category, add placeholder for example_unscannable.abc);** UNSCANNABLE FILE **Enabled**	**Allow**	Rule to set unscannable file exceptions based upon destination category. Use the "Custom_Allow_Unscannable_Files" category; any other URL categories; or Cloud Application(s) when need for exceptions are discovered.
2	Block_MS_ActiveContent_Global	ACTIVE CONTENT **Enabled** FILE TYPES **Microsoft Office (Microsoft Word, Microsoft Excel,**	**Block Download**	Enable the toggle button to apply the rule to files with active content. This criterion is applicable only

Rule Order	Rule Name	Criteria	Action	Description
		Microsoft PowerPoint) and PDF UNSCANNABLE FILE **Disabled**		to Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and PDF file formats. The File Types field must be set to one of the supported file formats in order to configure this criterion
3	Block_Database_ Global	ACTIVE CONTENT **Disabled** FILE TYPES <Entire Database Class> **Virtual Hard Disk Files (vhd, vhdx, vmdk);** **ACCDB (accdb);** **DBF (dbf)** **DB2SQL (sql, sqlproj, eql);** **KeePass Password Manager files (kdbx);** **EDMX Files (edmx);** **FRM (frm);** **DB file (db);** **MS Access Project (ade);** **SDB files (sdb)** UNSCANNABLE FILE **Disabled**	**Block**	Block all "Database" File Types (SuperCategory "DB") from ANY URL Category.
4	Block_Unscannabl e_Global	ACTIVE CONTENT **Disabled** FILE TYPES **Any** UNSCANNABLE FILE	**Block Download/ Upload**	Enable the toggle button to apply the rule only to files that the Zscaler service is unable to scan. This

Rule Order	Rule Name	Criteria	Action	Description
		Enabled		might occur if the file is in an unrecognized file format, excessive size, corrupted, or recursively compressed.

Notes regarding User Groups and File Types:
User Groups: Groups such as IT_Helpdesk and Super_Admin are customizable at each customer. Their usage is recommended and encouraged in order to have enough granularity for individual policies attached to individual user groups.

File Types: (Required) Select file types to which you want to apply the rule. You can also select Undetectable File under Other to apply the rule to unknown file types. For unknown file types, the service checks for the file type in the file header using true file type detection. If the file is still unknown, the service performs MIME type checks and tags as an unknown file type for any that fall outside of well-defined MIME types for common apps. You can select any number of file types and also search for file types.

Why File Type Controls?

File Type Controls regulate data flow, block unscannable content, and prevent sensitive file transfers to risky destinations like gambling sites. This strategy mitigates information leakage, enforces data protection compliance, and enhances security. Implementing File Type Controls protects critical data from unauthorized access and cyber threats, fostering trust and reliability. The following table highlights common use cases for implementing File Type Control:

Use Case	Action	Partially Implemented
Prohibit Office documents from uploading to any website category.	Prohibit any Office Document from being uploaded to any category (Group or Individual exceptions might apply).	No
Prohibit Office Document Transfers to Unsanctioned Sites.	Prohibit Office documents from uploading/downloading to "Entertainment", "Gambling", and "Productivity Loss" sites.	No
Permit Trusted Downloads for Auto-Updates.	Permit exe/cab/dll downloads from trusted vendors whose applications automatically update end-user machines.	Yes
Block Executable File Downloads.	Block download of Executable files from all sites except those sanctioned (Exceptions possibly for IT).	No
Block Unauthorized File Uploads by Design Teams.	Block the upload of ZIP, CAD/DWG/STL, or Undetectable files from teams to unsanctioned destinations.	No

Use Case	Action	Partially Implemented
Block Large File Uploads.	Block the upload of files over x megabytes, helping to identify large file uploads and possibly data exfiltration. (Block all uploads of any size to uncategorized sites).	Yes (Unscannable rule)
Block unscannable files.	Global Block of unscannable Files. i.e., Files that use proprietary encryption algorithms are compressed more than seven times (i.e., Winzip or 7zip to compress a file over 7 times, a common malware trick) or a file type that is not recognized or a MIME type that is not recognized.	Yes

Example File Type Control for Unscannable Content

Blocking of unscannable content, i.e., content that cannot be inspected due to proprietary encryption algorithms, multi-layer compression (greater than seven), or a file type or MIME type that is not recognized. It is recommended that any DLP Deployment always blocks these Unscannable Files.

Common Customer Questions for File Type Controls

- **Is there a list of File Types supported by File Type Control?**
  The list is available in the portal when configuring a File Type Control Policy.

- **Can we limit file sizes, i.e., limit the sending, uploading, or downloading of files of a certain size?** We can do this via a File Type Control Policy or a DLP Policy without content inspection.

- **Can File Type Control detect password-protected and encrypted files?**
  Yes, using DLP Policies without content inspection.

- **Can Zscaler block file upload/download by filename, by MIME type and manually listed file extension types?**
  File Type Control is looking for the first few bytes of the file, also known as the “magic bytes? to determine the file type. This is much more reliable than merely looking at the extension or MIME type which can be easily changed. If you are looking to block based on filename, MIME type or manually listed extension, you may need to look into DLP policy to achieve it.

Summary

File Type Controls are essential to data security strategies, helping organizations manage and mitigate risks associated with file-based threats. By regulating and monitoring data flow, these controls prevent the inappropriate transfer of sensitive files to unauthorized destinations, thereby protecting business-critical information from unauthorized access and cyber threats. Implementing robust File Type Controls enhances an organization's security posture and ensures compliance with Data Protection regulations, fostering trust and operational reliability.

URL Filtering

About URL Filtering

The URL Filtering policies consist of rules that customers define. When you add a rule, you specify criteria, such as URL categories, users, groups, departments, locations, and time intervals. The most specific rules should be at the top. By default, the Cloud App Control policies take precedence over the URL Filtering policies, and all group exceptions should be done there. Blocking Single URL rules should leverage Firewall rules for speed and efficiency.

Avoid the creation of complex URL Filtering Policies and leverage Cloud App Control Policies as much as possible. When adding URLs to categories use the option "URLs Retaining Parent Category" to keep the URLs in other Zscaler defined categories.

Zscaler organizes URLs into a hierarchy of categories for granular filtering and policy creation. There are six(6) predefined "Classes", each divided into predefined "Super-Categories", and then further divided into predefined "Categories".

The six predefined classes are:

1. Bandwidth Loss
2. Business Use
3. General Surfing
4. Legal Liability
5. Productivity Loss
6. Privacy Risk

You can download the preceding list from here. Please refer to About URL Categories for more details related to Zscaler URL categories.

Finally, if necessary use the recommended baseline on this document, and build your custom denylist approach on the URL filter.

For more information, please refer to the following resources:

- Landing page | Knowledge Based articles for URL Filtering
- About URL Filtering
- URL Format Guidelines
- Configuring the URL Filtering Policy
- Configuring Custom URL Categories
- About TLD Categories
- Configuring Advanced URL Policy Settings
- Adding URLs to the Allowlist
- Looking Up URLs in the ZIA Admin Portal
- Looking Up URLs in Site Review

Recommended Baseline Policies

Rule Order	Rule Name	Criteria	Action	Description
1	Block Legal Liability Class	PROTOCOL WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER; PROPFIND; PROPPATCH; MOVE; MKCOL; LOCK; COPY; UNLOCK; PATCH URL CATEGORIES Other Adult Material; Adult Themes Lingerie/Bikini; Nudity; Pornography;Body Art;Adult; Sex Education; K-12 Sex Education;Other Drugs; Gambling;Other Illegal or Questionable; Copyright Infringement; Computer Hacking; Questionable; Profanity; Mature	Block	The majority of Zscaler customers opt to block all SuperCategories under the class "Legal Liability" (About URL Categories & Classes). An override to this rule can be achieved by leveraging the action "Block With Override". If you enable this option, the EUN provides the users with a link to access the blocked page. The users are then prompted to enter their single sign-on credentials or hosted database credentials based on the Enable Identity-based Block Override settings. The authenticated users are allowed to access the blocked page only during their current browser session. They must re-authenticate if they try to access it through another browser session.

Rule Order	Rule Name	Criteria	Action	Description
		Humor; Anonymizer; Militancy/Hate and Extremism; Tasteless; Violence; Weapons/Bombs; Social Networking Adult; Marijuana		
2	Block Privacy Risk Class	PROTOCOL WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER; PROPFIND; PROPPATCH; MOVE; MKCOL; LOCK; COPY; UNLOCK; PATCH URL CATEGORIES OtherSecurity; Spyware/Adware; Custom Encrypted Content; Dynamic DNS Host; Newly Revived Domains	Block	It is highly recommended to block all SuperCategories under the class "Privacy Risk" (About URL Categories & Classes).

Rule Order	Rule Name	Criteria	Action	Description
4	Block Custom Category Globally	PROTOCOL WebSocket SSL; WebSocket; DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FTP; HTTPS; HTTP; SSLTunnel REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER; PROPFIND; PROPPATCH; MOVE; MKCOL; LOCK; COPY; UNLOCK; PATCH URL CATEGORIES "URL_Custom_Block_Category"	Block	The rule blocks destinations manually added to a custom URL category called: "URL_Custom_Block_Category". For demonstration purposes "www.example.com" will be the only destination added to the URL Category "URL_Custom_Block_Category".

Firewall Filtering

About Firewall Filtering

Firewall Control allows you to configure policies that define which types of your network traffic are allowed from specific sources and to reach specific destinations. Firewall Control policies provide the following benefits and enable Zscaler customers to:

- Protect your organisation's internal network from unauthorised access or connections to the internet by monitoring and applying policies to all non-HTTP/HTTPS network traffic.

- Define granular firewall filtering rules using several conditions, such as users, groups, or departments, client locations, network services, network applications, source IP addresses, destination IP addresses/FQDNs. User/Group based criteria and Network Applications field are only available with Advanced Firewall SKU. For more information regarding firewall capabilities refer to Understanding Firewall Capabilities.

- Enforce condition-based actions on your traffic, such as allowing, silently blocking, or blocking traffic by informing clients about the firewall action.

When working with Zscaler Firewall can be configured in the criteria of each rule. But Network services are identified in the first packet leading to immediate policy action. In contrast, multiple packets are required by deep packet inspection to identify network applications before a policy action can take place. Therefore, Zscaler recommends that you rank firewall filtering rules for network services higher than rules for network applications to prevent packets from being allowed unnecessarily from traffic that would have been otherwise blocked by rules using first-packet identification. To learn more, see About Network Services and About Network Applications.

First 4 rules including the default should not be modified. Any additional rule that needs to be added should always be after the rule "Recommended Firewall Rule". And for additional security, any custom rules should have at least 3 criteria elements. For more information, please refer to the following knowledge-based articles:

- About Firewall Control
- Configuring the Firewall Filtering Policy
- Understanding Predefined Firewall Filtering Rules
- Editing the Default Firewall Filtering Rules

Recommended Baseline Policies - Firewall Filtering

Rule Order	Rule Name	Criteria	Action	Description
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs NETWORK SERVICES Zscaler Proxy Network Services	Allow	Zscaler Proxy Traffic (created by default).
2	UCaaS One Click Rule	APPLICATION SERVICE GROUPS Zoom; Webex; Ring Central; GoTo	Allow	Unified Communication (UCaaS) One Click Rule.
3	Block QUIC Protocol	NETWORK SERVICES QUIC	Block/ICMP	If this rule is disabled it should be enabled. The selection of the ICMP block not only drops the UDP packet but also sends the client an error message of Type 3 (Destination Unreachable) and Code 13 (Communication Administratively Prohibited) via ICMP, which allows the client a potentially faster switchover to another web transport method. This results in a better user experience with reduced lag from QUIC to TCP. QUIC is not bound to only use the default destination port for HTTPS (dest:443), it is further recommended to block UDP over HTTP:80. Additionally modify the existing network service definition for QUIC to include UDP over destination port 80.

Rule Order	Rule Name	Criteria	Action	Description
4	Office 365 One Click Rule	APPLICATION SERVICE GROUPS Microsoft 365	Allow	Office 365 One Click Rule.
5	Block malicious IPs and domains	DESTINATION IP CATEGORIES Malicious Content	Block/Drop	Block malicious IPs and domains (created by default).
6	Recommended Firewall Rule	NETWORK SERVICES DNS; HTTP; HTTPS	Allow	This is the Default rule, any custom rules should be inserted after this rule. Note that Network Application is not used here as the proxy engines will serve that function.
…	…	…	…	Any other required Firewall Filtering rule goes after rule 6 and should always use at least 3 criteria.
7	Allow NTP	NETWORK APPLICATIONS NTP NETWORK SERVICES NTP	Allow	Take advantage of the Next-Generation Firewall (NGFW) capabilities of the Advanced Cloud Firewall (If Advanced is not available then Network Application is unavailable as a criteria) to limit applications to their assigned ports & protocols. Creating an Allow rule that defines a match of both Network Application and Network Service will only allow flows that match both. This is a recommended firewall policy related to Network Time Protocol (NTP).
Default	Default	Default Firewall Filtering Rule	Block/Drop	Make sure it's always set to Block/Drop.

Cloud Configuration (Advanced Settings)

About Advanced Settings

You can configure settings for various Zscaler service features on the Advanced Settings page. To adjust the advanced settings, navigate to **Administration > Advanced Settings**. The table below provides a comparison between the "Default Values" and best practices.

Configuration	Default Value	Best Practice	Description
Admin Ranking	Disabled	**Optional**	Turn on this feature if you want to rank administrators, and use the ranks when you manage policies. To learn more, refer to Admin ranking.
Allow Cascading to URL Filtering	Disabled	**Disabled**	Allow Cascading to URL Filtering: Enable this if you want the service to apply the URL Filtering policy even if it has already applied a Cloud App Control policy that explicitly allows a transaction. If you enable this option, the system globally allows cascading to URL filtering for all the Cloud App Control policies, irrespective of the cascading settings at the policy level. To learn more, refer to Allow Cascading to URL Filtering
Admin Portal Session Timeout	30	**30**	Session Timeout Duration: Specify how long admins can be inactive on the ZIA Admin Portal before they must log in again. By default, sessions restart after 30 minutes. You can enter a different time interval, from 5 to 600 minutes (10 hours).

			To learn more, refer to Session Timeout Duration
Authentication Exemptions	None	**Optional** **Cloud App matching customer's Identity provider (IdP)**	You can have the service exempt specific URL categories, URLs, cloud app categories, or specific cloud apps from **cookie authentication**: • Exempted URL Categories • Exempted URLs • Exempted Applications To learn more, refer to Authentication Exemptions
Kerberos Authentication Exemptions	None	**Optional**	You can have the service exempt specific URL categories, URLs, cloud app categories, or specific cloud apps from **Kerberos authentication**: • Exempted URL Categories • Exempted URLs • Exempted Applications To learn more, refer to Kerberos Authentication Exemptions
Basic Authentication Exemptions	None	**Optional**	You can have the service exempt specific URL categories, URLs, cloud app categories, or specific cloud apps from **basic authentication**: • Exempted URL Categories • Exempted URLs • Exempted Applications To learn more, refer to Basic Authentication Exemptions This feature is not enabled by default. To have this feature enabled for your organization, contact your Zscaler Account team.

			Note: This feature is not enabled by default. To have this feature enabled for your organization, contact your Zscaler Account team
Digest Authentication Exemptions	None	**Optional**	You can have the service exempt specific URL categories, URLs, cloud app categories, or specific cloud apps from **digest authentication**: ● Exempted URL Categories ● Exempted URLs ● Exempted Applications To learn more, refer to Digest Authentication Exemptions
Remove Range Headers	None	**Optional**	URL Categories: Select the URL categories for which you want to remove range headers.
Log Internal IPs from XFF Headers	Disabled	**Optional**	Log Internal IPs from XFF Headers: When the Zscaler service logs a transaction, it includes the source IP address, which is always the public IP address of the firewall or edge router that sends the traffic to the service. But if you use proxy chaining to forward traffic to the Zscaler service, a proxy server can insert an X-Forwarded-For (XFF) header in outbound HTTP requests. The XFF header identifies the IP address of the original client that sent the HTTP request through the proxy server. **Zscaler Client Connector also sends IP addresses as part of the XFF headers.** To learn more, refer to Internal IP Logging

Enforce Surrogate IP Authentication	Disabled	**Optional**	**Enforce Surrogate IP Authentication:** Some Windows 8 Metro apps use Internet Explorer as their user agent but do not support cookies or redirects, so the service does not allow traffic to these sites. Enable this option to allow the service to use the user-to-device mappings to apply the appropriate use policies to the traffic of the top Windows 8 Metro apps. The feature About Surrogate IP must be enabled. To learn more, refer to Windows App Traffic Authentication
Enable Policy For Unauthenticated Traffic	Disabled	**Enabled**	**Enable Policy For Unauthenticated Traffic:** For policies where you can specify users and departments in the criteria, the Zscaler service allows you to specify whether you want a rule to apply if the user traffic is unauthenticated. You must turn on this feature here if you want this option to appear when configuring your policy rules. Any rule that applies to unauthenticated traffic must apply to all locations; you cannot apply a rule to unauthenticated traffic and select particular locations. To learn more, see How do I configure the policy for unauthenticated traffic? **Note**: This applies only if "Authentication" is enabled on the location. To learn more, refer to Policy for Unauthenticated Traffic
HTTP Tunnel Control			
Inspect Tunneled HTTP Traffic	Enabled	**Enabled**	**This option is enabled by default**, and allows the Zscaler service to enforce configured policies on tunneled HTTP traffic that is sent via a CONNECT method request. For example, with this feature enabled, if the service receives a CONNECT request to www.cnn.com:80, the

			service will apply the configured web policies to HTTP traffic that it forwards to www.cnn.com. If this option is disabled, then the service will not apply the policies to the traffic to www.cnn.com.
Block Tunneling to Non-HTTP/HTTPS Ports	Enabled	**Enabled**	**This feature is enabled by default**. The service restricts HTTP CONNECT method requests to the standard HTTP/HTTPS ports (80 and 443). You can disable this option to allow all HTTP CONNECT requests to non-standard HTTP/HTTPS ports, in addition to ports 80 and 443. For example, a CONNECT request for SSH to port 22 will be allowed if this feature is disabled.
Block Non-RFC Compliant HTTP Traffic on HTTP/HTTPS Ports	Disabled	**Enabled**	**This feature is disabled by default**. Enable this option to allow the service to block traffic that isn't compliant with Request for Comments (RFC) HTTP protocol standards. For example, binary traffic or other non-RFC compliant traffic, such as HTTP/0.9, is blocked through standard HTTP/HTTPS ports 80 and 443. You can disable this option to allow non-RFC-compliant traffic over HTTP/HTTPS ports. To learn more, refer to HTTP Tunnel Control.
Block Domain Fronting	**Disabled**	**Enabled**	**By default, this option is disabled**. Enabling this option blocks domain fronting for HTTP/S transactions with an FQDN mismatch between: • The requested URL and the request's host header. There is no mismatch if either of the fields, host header or FQDN URL is empty. • The SNI (Server Name Indication) and the inner request's host header. The service doesn't consider it a mismatch if either of the fields, host header or SNI is empty.

			To learn more, refer to HTTP Tunnel Control.
Block CONNECT Host and SNI Mismatch	Disabled	**Enabled**	Enable to block forward proxy connections where the CONNECT host doesn't match the SSL/TLS client hello SNI. When there is a mismatch, SNI is logged into the URL weblog field and the CONNECT host is logged into the existing weblog field **Domain fronted host header**.
URL Category Exemptions for Block CONNECT Host and SNI Mismatch	Zscaler Proxy IPs	**Optional**	Enter URL categories you want to exempt from the Block CONNECT Host and SNI Mismatch setting.
Exempted Cloud Applications for Block CONNECT Host and SNI Mismatch	Empty	**Optional**	Select cloud app categories or cloud apps you want to exempt from the Block CONNECT Host and SNI Mismatch setting.
Services Forwarded to HTTP Web Proxy	By default, the Zscaler service "listens to": • Port 80 for HTTP traffic • Port 443 for HTTPS traffic • Port 53 for DNS traffic • Port 21 for FTP traffic • Port 554 for RTSP traffic • Port 1723 for PPTP traffic If your organisation uses other or additional ports for the above types of traffic, you can enable the service to use custom ports for them. To do this, create a custom network service with the appropriate ports and select it from the options below: • Services Forwarded to HTTP Web Proxy • Services Applicable to DNS Transaction Policies		

	• Services Forwarded to FTP Proxy • Services Forwarded to RTSP • Services Forwarded to PPTP		
HTTP Services	HTTP	**HTTP**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 80 for HTTP traffic, you can use your custom ports by creating a network service and selecting it here.
HTTPS Services	HTTPS	**HTTPS**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 443 for HTTPS traffic, you can use your custom ports by creating a network service and selecting it here.
Services Applicable to DNS Transaction Policies	DNS	**DNS**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 53 for DNS traffic, you can use your custom ports by creating a network service and selecting it here.
Services Forwarded to FTP Proxy	FTP	**FTP**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 21 for FTP traffic, you can use your custom ports by creating a network service and selecting it here.
Services forwarded to RTSP	RTSP	**RTSP**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 554 for RTSP traffic, you can use your custom ports by creating a network service and selecting it here.
Services forwarded to PPTP	PPTP	**PPTP**	Only complete this if you have enabled the firewall service. If your organization uses ports other than 1723 for PPTP traffic, you can use your custom ports by creating a network service and selecting it here.

Auto Proxy Forwarding for Non-defined Ports	**Enabled**	**Enabled**	Enable to redirect outbound HTTP, HTTPS, FTP, DNS, RTSP, and PPTP traffic to the web engine for inspection. Use this if the traffic is destined to a **non-standard port and doesn't match any predefined network services**. RTSP and PPTP are applicable only with transparent mode connectivity to the ZIA Public Service Edge (i.e., GRE or IPSec tunnels with no PAC file). The firewall identifies destinations of web traffic when an Allow rule exists, identifying HTTP or HTTPS at a network application. The next time a session is directed to a non-standard web location, the CFW will ensure that the traffic is inspected by the SWG. **Note: Auto Proxy Forwarding for Non-Defined Ports requires the Advanced Firewall license.**
Office 365 One Click Configuration	Disabled	**Disabled**	This is a **legacy one-click** setting with fewer SSL/auth bypasses for O365 traffic. To learn more, refer to About Microsoft One Click Options.
Traffic Forwarded to ZPA from ZIA Insert XFF Header for ZPA traffic	Disabled	**Enabled**	Enable or disable this option to insert XFF header to all traffic (Source IP Anchored and ZIA-inspected ZPA application traffic) forwarded from ZIA to ZPA. This option is enabled by default. **Note: This field is only available if you have a subscription to either Source IP Anchoring or ZPA App Inspection.**
Settings for DNS Optimization			

Optimize DNS Resolution	Disabled	**Optional**	Enable this option to configure DNS optimization settings. The Zscaler service performs a DNS lookup and may override the externally-resolved IP addresses in the outbound HTTP/S connections to establish a connection to the destination server that is geographically closer to the ZIA Service Edge. This setting applies only to transparent mode traffic. **Note:** After enabling this option, you need to configure the DNS optimization settings individually for URL categories, cloud applications, and FQDNs.
Prefer SNI Over CONNECT Host for DNS Resolution	Disabled	**Optional**	Enable the SSL/TLS client hello SNI for DNS resolution instead of the CONNECT host for forward proxy connections. This works only if the CONNECT host is not part of an SSL policy. This handles exceptions such as a malformed but valid SNI server name that isn't parsable to the actual resolvable domain.
Enable Firewall for Z-Tunnel 1.0 and PAC Road Warriors	Disabled	**Enabled**	Enable Firewall for Z-Tunnel 1.0 and PAC Road Warriors: Enabling the option applies the following firewall rules to the remote user traffic forwarded via Z-Tunnel 1.0 or PAC: ● All the default firewall rules. ● All the user-defined rules are configured without any location criteria. ● All the user-defined rules configured for the Road Warrior location because Road Warrior applies only to Z-Tunnel 2.0 when this option is disabled.

			Hence, before enabling, ensure that the above firewall rules are relevant for the traffic forwarded via Z-Tunnel 1.0 and PAC.
Enable ECS Option for Locations and Remote Users	Disabled	**Optional**	Enable this option to support the EDNS Client Subnet (ECS) option at the organization level. This is applicable to all DNS queries, originating from locations or remote users.
Enable Real Time Risk Score Updates	Disabled	**Optional**	Enable Real-Time Risk Score Updates: Enable this option to allow ZIA Public Service Edges to track risky user activities that might increase user risk in real time. When enabled: • Displays the risk score in the User Risk Profile column on the User Management page. • The policies that include user risk as a criterion can only receive real-time risk increase updates. This might result in limited user access. • You can view the recent risk score increases in the User Risk Report.

For more information please refer to [Configuring Advanced Settings | Zscaler]

Malware & Advanced Threat Protection

Malware Protection

Configuration Settings		Default Value	Best Practice
Traffic Inspection	Inbound	Enable	**Enable**
	Outbound	Enable	**Enable**
Protocol Inspection	Inspect HTTP	Enable	**Enable**
	Inspect FTP over HTTP	Enable	**Enable**
	Inspect FTP	Disable	**Enable**
Malware Protection	Unwanted Applications	Block	**Block**
	Trojans	Block	**Block**
	Worms	Block	**Block**
	Ransomware	Block	**Block**
	Remote Access	Block	**Block**
	Other Viruses	Block	**Block**
Adware/Spyware Protection	Adware	Block	**Block**
	Spyware	Block	**Block**
Security Exceptions	Password Protected Files	Allow	**Block**
	Unscannable Files	Allow	**Allow**
	Do Not Scan Content from these URLs	Blank	**Blank**

Note: For Security Exceptions (Do Not Scan Content from these URLs) there may be trusted websites for which the content might be blocked due to anti-virus, anti-spyware, or anti-malware policies. Enter the URLs of sites that you do not want the service to scan.

This allowlist also applies to the Advanced Threat Protection and Sandbox policies. If you want to allowlist URLs and files completely, you must also configure the URL Filtering and

File Type Control policies. To learn more, see Adding URLs to the Allowlist. For more information please refer to Malware Protection.

Configuration Settings		Default Value	Best Practice
SUSPICIOUS CONTENT PROTECTION (RISK PAGE™)	Low Risk: Allow users to access safe web pages. **There is no risk tolerance. (0-35)** Moderate Risk: Allow users to access slightly suspicious web pages. **There is a moderate risk tolerance. (36-65)** High Risk: Allow users to access very risky web pages. **There is a high risk tolerance. (66-99)**	35	**35**
BOTNET PROTECTION	Command & Control Servers	Block	**Block**
	Command & Control Traffic	Block	**Block**
	Domain Generated Algorithm (DGA) domains	Block	**Block**
MALICIOUS ACTIVE CONTENT PROTECTION	Malicious Content & Sites	Block	**Block**
	Vulnerable ActiveX Controls	Block	**Block**
	Browser Exploits	Block	**Block**
	File Format Vulnerabilities	Block	**Block**

	Block Malicious URLs	Blank	-
FRAUD PROTECTION	Known Phishing Sites	Block	**Block**
	Suspected Phishing Sites	Block	**Block**
	Spyware Callback	Block	**Block**
	Web Spam	Block	**Block**
	Crypto Mining	Block	**Block**
	Known Adware & Spyware Sites	Block	**Block**
UNAUTHORIZED COMMUNICATION PROTECTION	IRC Tunneling	Block	**Block**
	SSH Tunneling	Allow	**Block**
	Anonymizers	Block	**Block**
CROSS-SITE SCRIPTING (XSS) PROTECTION	Cookie Stealing	Block	**Block**
	Potentially Malicious Requests	Block	**Block**
SUSPICIOUS DESTINATIONS PROTECTION	Blocked Countries	Blank	**Per customer's security policy**
P2P FILE SHARING PROTECTION	BitTorrent	Block	**Block**
P2P ANONYMIZER PROTECTION	Tor	Block	**Block**
P2P VOIP PROTECTION	Google Hangouts	Block	**Block**
Security Exceptions	Do Not Scan Content from these URLs	Blank	**Blank**

Note: For Security Exceptions (Do Not Scan Content from these URLs) there may be trusted websites for which the content might be blocked due to anti-virus, anti-spyware, or anti-malware policies. Enter the URLs of sites that you do not want the service to scan.
This allowlist also applies to the Advanced Threat Protection and Sandbox policies. If you want to allowlist URLs and files completely, you must also configure the URL Filtering and File Type Control policies. To learn more, see Adding URLs to the Allowlist. For more information please refer to Advanced Threat Protection.

Sandbox

About Sandbox

If the customer is entitled to Advanced Sandbox additional rules can be configured. Due to the wide range of risk tolerance and performance expectations, configuring Sandbox policies may vary significantly for different customers. It is recommended to start with the Baseline Sandbox Rules Security Approach. This highlights the possible configurations that can be achieved.

For more information, please refer to the following resources:

- Sandbox | Landing Page
- About Sandbox
- Configuring the Default Sandbox Rule
- Configuring the Sandbox Policy
- Viewing Sandbox Reports and Data
- Configuring the Patient 0 Alert
- Add Custom File Hashes
- About Sandbox End User Notifications
- Using the Sandbox Scanning Port

Recommended Baseline Sandbox Rules

Rule Order	Rule Name	Criteria	Action	AI Instant Verdict	Description
1	MS Office and PDF Quarantine	**FILE TYPES** Microsoft Excel (xls, xlsx, xlsm, xlam, xlsb, slk, xltm); Microsoft Word (doc, docx, docm, dotx, dotm); Microsoft Rich Text Format (rtf); Microsoft PowerPoint (ppt, pptx, pptm, potx, ppsx, ppam, potm, ppsm) Portable Document Format (pdf) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools Sandbox Suspicious **URL CATEGORIES** Entertainment; Music and Audio Streaming; Other Entertainment/Recreation; Radio	**Quarantine** First Time **Block** Subsequent Downloads **70** Minimum Threat Score State: **Disabled**	Enabled	**Example Rule** This example rule is disabled by default and will act to quarantine files being downloaded from categories where productivity needs are unlikely - prioritizing safety for these categories. Removing any categories which are likely to relate with the organization's services. The rule matches MS Office and PDF files. It sets the first action to "Quarantine" based upon matching the URL category of the destination.

		Stations; Video Streaming; Television/Movies; Advertising; File Converters; Image Host; Shareware Download; Translators; Blogs; Discussion Forums; Internet Services; Online Chat; Other Internet Communication; Peer-to-Peer Site; Remote Access Tools; Games; Shopping and Auctions; Society and Lifestyle; Travel; Vehicles; Adult Sex Education; Adult Themes; Body Art; K-12 Sex Education; Lingerie/Bikini; Nudity; Other Adult Material; Pornography; Social Networking Adult; Miscellaneous or Unknown; Newly Registered and Observed Domains; Non Categorizable; Other Miscellaneous; Custom Encrypted Content; Dynamic DNS Host; Newly Revived Domain; Other Security Spyware/Adware;			

2	Allow Scan Executables	**FILE TYPES** Batch (.cmd, .bat); Microsoft Installer (msi); Python Files (py, p, pkl, pickle, pyd, pyw; Visual Basic Script (vbs); Windows Executable (exe, exe64, scr); Windows Library (dll64, dll, ocx, sys); Windows PowerShell Script (ps1) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **URL CATEGORIES** **Any URL Category** **GROUPS** **Service_Admin**	**Allow & Scan First Time** **Block Subsequent Downloads** **70** Minimum Threat Score	Enabled	This rule allows a user group like Service Administrators to download (with scanning) of files.
3	Quarantine Executables	**FILE TYPES** Batch (.cmd, .bat); Microsoft Installer (msi); Python Files (py, p, pkl, pickle, pyd, pyw;	**Quarantine** First Time **Block** Subsequent Downloads **70** Minimum Threat Score	Enabled	The rule matches the file types included in the SuperCategory "Executables". It sets the first action to

		Visual Basic Script (vbs); Windows Executable (exe, exe64, scr); Windows Library (dll64, dll, ocx, sys); Windows PowerShell Script (ps1) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **URL CATEGORIES** **Any URL Category**			"Quarantine" only if the destination URL matches the SuperCategory "Miscellaneous" or the category "Shareware Download".
4	Catch All BA Rule	**FILE TYPES** **All file types** **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious	**Allow and scan** First Time **Block** Subsequent Downloads **70** Minimum Threat Score	Enabled	Overwrites the Default Behaviour Analysis (BA) Rule. For all file types and any URL Category, the first action is set to "Allow and scan First Time".

		URL CATEGORIES **Any URL Category**			
Default	Default_BA_Rule	**FILE TYPES** ZIP (zip); Windows Library (dll64, dll, ocx, sys); Windows Executable (exe, exe64, scr) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **URL CATEGORIES** Suspicious Destinations **PROTOCOLS** Any	**Allow and scan** First Time **Block** Subsequent Downloads	Disabled	The Default Behaviour Analysis (BA) Rule.

Microsoft Defender for Endpoint Integration:

- Zscaler and Microsoft Defender Deployment Guide
- Microsoft Defender and ZIA Demo

CrowdStrike Integration:Integrating with CrowdStrike

Cloud App Control

The Cloud App Control policies provide granular control over popular websites and applications. They are organised by function into categories for easy reference and to facilitate defining rules for similar applications. You can create rules to control how your users access specific cloud applications. For example, you can specify a rule for Instant Messaging applications that allows chatting but blocks file transfers. Additionally, you can define a daily quota by bandwidth or time. When users browse these sites after their quota has been reached, the Zscaler service displays a message that explains that the content cannot be viewed because they exceeded their daily quota. Cloud App categories are a crucial part of Cloud App Control. By default, the Cloud App Control policy precedes the URL Filtering policy. **If a user requests a Cloud App which is explicitly allowed (without the "Cascading to URL Filtering" option enabled) or blocked based on a Cloud App Control policy, the service only applies the Cloud App Control policy and not the URL Filtering policy**. For example, if you have a Cloud App Control policy rule that allows viewing Facebook but a URL Filtering policy rule that blocks www.facebook.com, a user is still allowed to view Facebook. This is because, by default, the service does not apply the URL Filtering policy if a Cloud App Control policy rule allows the transaction. The service organises cloud applications into eighteen (18) categories. For thirteen (13) categories, you can create rules with allow or block options. For the other five(5) categories, you can create rules to control the specific actions a user can take within the application.

Cloud App Categories with Allow or Block Options

The following are the cloud application categories with the allow or block options.

1. AI & ML Applications
2. Collaboration & Online Meetings
3. Consumer
4. DNS Over HTTPS Services
5. Finance
6. Health Care
7. Hosting Providers
8. Human Resources
9. IT Services
10. Legal

11. Productivity & CRM Tools
12. Sales & Marketing
13. System & Development

Cloud App Categories with Action-Specific Allow or Block Options

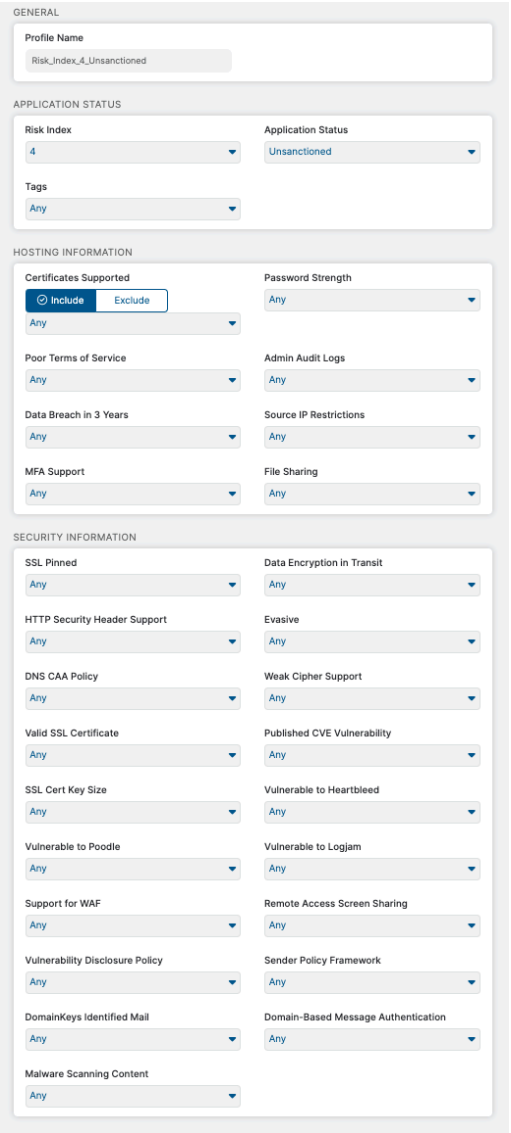
The following are the cloud application categories with action-specific allow or block options.

1. File Sharing
2. Instant Messaging
3. Social Networking
4. Streaming Media
5. Webmail

For more information, please refer to the following resources:

- Landing page | Knowledge Based articles for Cloud Apps
- About Cloud App Control
- About Cloud App Categories
- Adding Rules to the Cloud App Control Policy
- About Cloud Applications
- Adding a Custom Cloud Application
- About Cloud Application Instances
- Adding a Cloud Application Instance
- About Office 365
- About Microsoft One Click Options - Office 365
- About Cloud Application Risk Profile
- Adding a Cloud Application Risk Profile
- About Tenant Profiles
- Adding Tenant Profiles

About Cloud App Risk Profiles



The cloud application risk profile feature allows you to control how cloud applications are used in your organisation. The feature consists of two (2) parts: creating a cloud application risk profile and associating the profile with the Cloud App Control policy. The feature enables you to create the Cloud App Control policy based on the cloud application attributes. The policy applies to cloud applications with attributes that match the risk profile criteria.

For example, if a risk profile is created with its criteria set as follows: Risk Index to 5 (AND) Application Status to Unsanctioned (AND) Poor Terms of Service to Yes, and the profile is associated with the File Sharing cloud app control policy with the Upload action set to Blocked. The upload action for all file-sharing apps that match the risk profile criteria is blocked. **The Cloud App Control policy applies to all specified cloud applications if the cloud application risk profile criterion is selected.**

How to create Cloud App Risk Profiles?

Navigate to "**Administration > Risk Profile**" and create the following two(2) Risk Profiles. When creating a Risk Profile, choose "Any" for all options under "Hosting Information" & "Security Information". The Cloud App Risk Profile should look as per the below configuration snippet:

Cloud App Risk Profiles - Overview

Rule Order	Profile Name	Applications Status	Risk Index	Certification Supported	Details
1	Unsanctioned_Risk_Index_4	Unsanctioned	4	—	SECURITY INFORMATION Data Encryption in Transit-Any
2	Unsanctioned_Risk_Index_5	Unsanctioned	5	—	SECURITY INFORMATION Data Encryption in Transit-Any

Recommended Baseline Policies Per Cloud App Category

The Zscaler Risk Index is useful for governing access to more risky destinations. Risk Index 4 & 5 Cloud Applications that are unsanctioned can either be blocked or isolated. A custom browser notification can inform the user as a precaution instead of blocking. Blocking of Risk Index 4 & 5 Cloud Applications that are unsanctioned is highly recommended. However, this should typically be done after discovering the applications in use to avoid interruption of any legitimate usage of a more risky application. Allowing access to a cloud application does not mean that Zscaler will forgo inspection. As long as there are no SSL or security exemptions for a destination, Zscaler will still inspect the content of the session. It is not uncommon for "Risk Index 4" & sometimes "Risk Index 5" applications to be used as underlying services for legitimate web properties. If they are set to "Block" or "Caution" there can be unintended consequences. For example, a user may be able to browse to a website and select an item for purchase, but when attempting to purchase the item from their "cart" a Risk Index 4 CDN is used and they experience a failure without any notification because it is only a portion of the page rather than the main destination. It may be beneficial to allow even "Risk Index 4" & sometimes "Risk Index 5" applications; use the "SaaS Security Report (Shadow IT Report)" to understand what applications are being used before implementing any blocking, and sanction applications that should not match the block rules.

(1) AI & ML Applications				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(2) CONSUMER				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.

2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(3) DNS OVER HTTPS SERVICES				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Any_DNS_Over_HTTPS	APPLICATIONS Any	**Block Application Access**	Block all Cloud Apps under the category "DNS Over HTTPS Service". The recommendation is to block to ensure ZPA sees all DNS requests. If ZPA is not in use, the decision regarding blocking or allowing "DNS Over HTTPS (DoH)" is based on the customer's policy. **Note:** DOH can be addressed in DNS Controls as well.
(4) COLLABORATION & ONLINE MEETINGS				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS	**Allow Application Access**	Office 365 One Click Rule.

		Viva Engage; SharePoint Online; Microsoft Teams; Microsoft Sway		
2	UCaaS One Click Rule	APPLICATIONS Zoom; RingCentral; LogMeIn	**Allow Application Access**	UCaaS One Click Rule.
3	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are “Unsanctioned” and classified by Zscaler as “Risk Index 4”. It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
4	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are “Unsanctioned” and classified by Zscaler as “Risk Index 5”.

(5) PRODUCTIVITY & CRM TOOLS				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS Common Office 365 Applications; Microsoft Dynamics 365; Microsoft Delve; Microsoft Power BI; Microsoft Planner	**Allow Application Access**	Office 365 One Click Rule.
2	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are “Unsanctioned” and classified by Zscaler as “Risk Index 4”. It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
3	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are “Unsanctioned” and classified by Zscaler as “Risk Index 5”.

(6) FILE SHARING				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS OneDrive	**Allow** **Viewing, Uploading**	Office 365 One Click Rule.
2	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
3	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(7) FINANCE				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess

				whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(8) HEALTH CARE				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

(9) HOSTING PROVIDERS				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS Microsoft Azure	**Allow Application Access**	Office 365 One Click Rule.
2	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
3	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(10) HUMAN RESOURCES				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess

				whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(11) INSTANT MESSAGING				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

(12) IT SERVICES				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS Microsoft Azure AD; Microsoft Intune	**Allow IT Services**	Office 365 One Click Rule.
2	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
3	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(13) LEGAL				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess

		Unsanctioned_Risk_Index_4		whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(14) SALES & MARKETING				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

(15) SOCIAL NETWORKING				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(16) STREAMING MEDIA				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.

2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".
(17) SYSTEM & DEVELOPMENT				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
2	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

(18) WEBMAIL				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS Outlook	**Allow Viewing Mail, Sending Attachments, Sending Mail**	Office 365 One Click Rule.
2	Block_Unsanctioned_Risk_Index_4	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_4**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
3	Block_Unsanctioned_Risk_Index_5	CLOUD APPLICATION RISK PROFILE **Unsanctioned_Risk_Index_5**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

URL & Cloud App Control (Advanced Policies)

About URL & Cloud App Control (Advanced Policy Settings)

To configure the advanced policy settings navigate to “Policy > URL & Cloud App Control” and click the “Advanced Policy Settings” tab. The table below provides a comparison between the "Default Values" and best practices.

Configuration	Default Value	Best Practice	Description
Enable CIPA Compliance	Disabled	**Optional**	Enable to enforce Children's Internet Protection Act (CIPA) Compliance. About CIPA Compliance | Zscaler
Enable Suspicious New Domains Lookup	Disabled	**Enabled**	Enable this feature to provide advanced protection to users against the newly registered and observed domains that are identified within hours of going live. This feature also identifies newly revived domains. These domains are often considered potentially malicious until they are well known or categorized. Identifying them improves the overall security posture.

Configuration	Default Value	Best Practice	Description
Enable AI/ML based Content Categorization	Disabled	**Enabled**	Enable if you want the service to analyze the content of uncategorized websites using AI/ML tools to check if they belong to one of these URL super categories: Adult Material, Drugs, Gambling, Violence, Online Shopping, Sports, Health, Games or Religion. If the service determines the site belongs in one of those categories, it will categorize those sites and apply policy accordingly.
Enable Embedded Sites Categorization	Disabled	**Enabled**	Enable to allow the service to enforce URL Filtering policy for sites that are translated using translation service websites. For example, when this feature is enabled, if you have a policy that blocks www.gambling.com, and a user translates the page to another language using Google Translate, the service will block the translated page.
Enforce SafeSearch	Disabled	**Enabled**	Enable if you want the service to return only safe content from searches on certain websites. Learn more. SSL inspection must be enabled for this option.
Enable Identity-based Block Override	Disabled	**Optional**	Enable to allow authorized users to provide access to blocked pages by using company provided credentials such as single sign-on credentials.
Microsoft Recommended Office One-Click	Enabled	**Enabled**	Enabling this option allows Zscaler to enable local breakout for Office 365 traffic automatically without any manual configuration needed by customers. Please note that enabling this option would turn off SSL Interception for all Office 365 destinations

Configuration	Default Value	Best Practice	Description
			as per Microsoft's recommendation. If using existing granular controls for Office365, disable this option and enable pre-existing configuration here.
Skype	Allow	**Block**	While VoIP may be encouraged for its telephone cost savings, it may also be discouraged because of the high bandwidth utilisation associated with it. The Zscaler service can block access to Skype, a popular P2P VoIP application.
Unified Communications As a Service (UCaaS)	UCaaS is a cloud delivery model that offers communications and audio/video-based collaboration services. It's rapidly being adopted by enterprises of all sizes. Zscaler enables direct-to-cloud access for UCaaS applications like Zoom, GoTo, RingCentral, and Webex by enabling organizations to send traffic directly to application servers over the internet, instead of backhauling traffic over costly MPLS circuits.		
Zoom	Disabled	**Optional**	Enabling this allows Zscaler to permit secure local breakout for "Zoom / GoTo / RingCentral / Webex" traffic automatically, without any manual configuration needed. When enabled, this option turns off SSL interception for all "Zoom / GoTo / RingCentral / Webex" destinations. To continue using existing granular controls for those services, disable this option and enable cloud application and firewall network application policies accordingly.
GoTo	Disabled	**Optional**	
RingCentral	Disabled	**Optional**	
Webex	Disabled	**Optional**	

Configuration	Default Value	Best Practice	Description
GenAI Prompt Configuration	Generative AI prompts are a series of instructions that are provided as input to generative AI applications to get the desired response from them. The Zscaler service categorizes and stores prompts for generative AI applications. Enabling the following options allows Zscaler to categorize and store the prompts for the respective applications.		
ChatGPT	Disabled	**Optional**	Enabling this feature allows Zscaler to store end-user prompts, up to 2 KB in size, in logs for up to six months, or for the period defined by your organization. Authorized users with access to Zscaler logs will be able to view the prompts entered by end users in the Gen AI application.
Microsoft Copilot	Disabled	**Optional**	
Gemini	Disabled	**Optional**	
Perplexity	Disabled	**Optional**	
Poe	Disabled	**Optional**	
Meta AI	Disabled	**Optional**	

For more information please refer to [Configuring Advanced Policy Settings | Zscaler]

Isolation & Secure Browsing

Cloud Browser Isolation (CBI)

Cloud Browser Isolation (CBI) provides an organization the capability to isolate users from potentially harmful content on the Internet. This is done by loading the accessed web page on a remote browser in any one of the many Zscaler data centers across the globe, and streaming the rendered content as a stream of pixels to the user's native browser.

Isolating web pages on an ephemeral, remote browser ensures that the HTML files, CSS files, JavaScript files, and any other active content served by the accessed web page never reach the end user's machine or the corporate network, thus ensuring an "air gap" between the end user and the web page accessed.

Isolation not only provides the capability to isolate web pages, but also allows the user to view file types in isolation without requiring a download of the files to their local machine.

This feature is fully integrated with Zscaler Internet Access (ZIA), allowing the admins of an organization to granularly define what web traffic should be isolated and what policies need to be applied to the isolated traffic. The traffic egressing the isolation browser is also passed through the ZIA Public Service Edges before reaching the internet web page being accessed.

In addition to the security policies enforced by ZIA, Isolation provides additional data exfiltration security controls, which enables an organization to granularly control the level of interaction the user can have with the isolated web page.

For more information, please refer to the following resources:

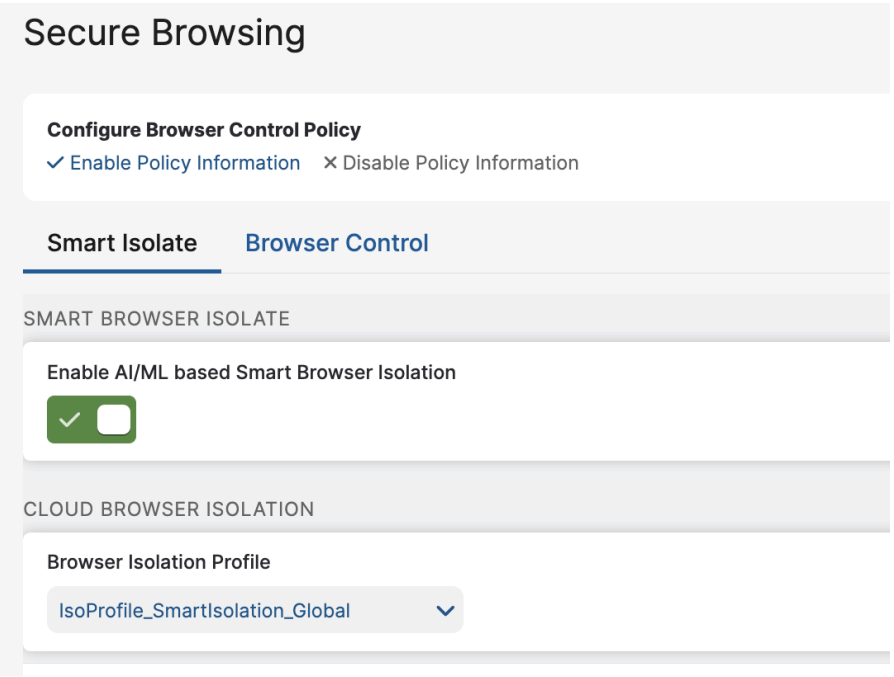
- Isolation (CBI) | Landing Page
- What Is Isolation?
- Limits in Isolation
- Configuring ZIA for Isolation
- Default Isolation Profiles for Isolation
- Creating Isolation Profiles for ZIA
- About Sandbox Integration with Isolation
- Using Sandbox Integration with Isolation

Smart Browser Isolation (SBI)

You can configure a Smart Browser Isolation (SBI) policy that automatically isolates potentially malicious web content using the AI/ML models. This policy identifies suspicious websites and decrypts them using SSL inspection. It presents the users with a rendition of the actual websites in a remote browser using the cloud browser isolation. To configure the Smart Browser Isolation (SBI) policy:

1. **Go to Policy > Secure Browsing.**
2. On the Smart Isolate tab:
    - Enable AI/ML-based Smart Browser Isolation: Enable this option to protect the users from suspicious websites hosting malicious active content using AI/ML models, which continually identify suspicious domains. Enabling this option automatically creates an editable SSL inspection rule to decrypt suspicious websites. Once this feature is enabled, the following option appears:
        - Browser Isolation Profile: You can choose the isolation profile the policy applies to.
        - Ensure to create isolation profiles for your organisation on the Cloud Browser Isolation Portal for them to be available in this field.

Note: Smart Browser Isolation(SBI) requires a Cloud Browser Isolation(CBI) licence.



Isolation Profiles

The "Default Isolation profiles" are automatically created for any organization licensed for CBI. This allows a quick setup for your organization without manually creating the first Isolation profile needed for configuring Isolation. It is not required to use the default Isolation profiles for any configuration. They are only used if your organization does not manually create any Isolation profiles. When creating a Zscaler Internet Access (ZIA) policy with the action as Isolate, you must reference an isolation profile in the policy you're creating. These profiles determine certain attributes and specifications about how the user interacts with the isolated web page, where the isolation containers are spun up, and what the isolation experience looks like to the user. You can use ZPA Isolation profiles to create policies in Zscaler Private Access (ZPA) to isolate specific web applications. To learn more, see About Isolation Policy. For any organization that is using Isolation, ZIA and ZPA automatically create default isolation profiles. You can use the default isolation profiles or manually create isolation profiles to use in ZIA and ZPA policies. To learn more, see Default Isolation Profiles in Isolation.

Prerequisites

Before creating an isolation profile for ZIA, ensure the following:

- For isolation policies to be applied, the Zscaler service must authenticate the web traffic. Unauthenticated traffic or traffic from locations with authentication disabled is not subjected to isolation policies.
- For HTTPS web pages to be isolated, the Zscaler service must SSL inspect the traffic.

The isolation browser trusts all the well-known certificate authorities trusted by Chromium. In addition, Zscaler also provides administrators with the capability to upload root certificates of their choice that they want the isolated browser to trust for successful SSL communication. These uploaded certificates can be associated with the isolation profiles that are created on the Secure Internet and SaaS Access (ZIA) Admin Portal.

Understanding Turbo Mode for Isolation

Turbo Mode is an alternative to pixel streaming. It allows the transfer of rendered information from an isolated browser to a local browser as an instruction set. This method of rendering is much faster and much less bandwidth-intensive than pixel streaming. It also promises a higher frame rate, ensuring a smooth isolated browsing experience. The capability provides a near-native experience.

Turbo Mode functions by taking browser instructions from the Zscaler Isolation platform and rendering the output natively to an end user's browser. This arrangement eliminates the requirement to stream the isolated content to a browser and is far more efficient with limited internet bandwidth. Turbo Mode is fully functional on most modern desktops and mobile devices. There is no compromise to security if Turbo Mode is enabled on an isolation profile. Web content is processed on Isolation containers, and only the rendered content is represented in the end user's browser. As a result, no code is executed locally on the device.

Note: Zscaler Admins must enable this feature for the user's isolation profile. To learn more, see Creating Isolation Profiles for ZIA and Creating Isolation Profiles for ZPA. **Turbo Mode is not supported for Internet Explorer 11.**

For more information regarding Isolation profiles, please refer to the following knowledge-based articles:

- Default Isolation Profiles for Isolation
- Creating Isolation Profiles for ZIA
- About Root Certificates for Isolation in ZIA
- Accessing Multiple Sessions In Isolation
- User Experience Modes in Isolation
- Understanding Turbo Mode for Isolation

To summarise, Isolation Profiles are required for the the following services:

1. Smart Browser Isolation (SBI)

2. Cloud Browser Isolation (CBI) actions for:
    a. Cloud App Control Policies
    b. URL Filtering Polices
    c. Sandbox Policies

Smart Browser Isolation (SBI) Profile

This profile is to be used for Smart Browser Isolation (SBI) configuration:

Isolation Profile Configuration	
General	
Name	**Smart_Isolation_ReadOnly**
Turbo Mode	**Enabled**
Description	**CAUTION: Please only amend this Isolation Profile with approval.** **Isolation Regions set to any for global redundancy and better user experience**
Company Settings	
Proxy configuration URL	Use recommended PAC file URL
Override PAC file and return traffic to ZIA Public Service Edge	Enabled

Isolation Profile Configuration	
Root Certificates	Zscaler Root Certificate
Debug Mode	Disabled
Security	
ALLOW COPY & PASTE FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW FILE TRANSFERS FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW PRINTING	
Allow printing from isolation	Disabled
RESTRICT TEXT INPUT	
Read-Only Isolation	**Enabled**
ALLOW VIEWING OFFICE FILES	
View office files in isolation	Disabled
LOCAL BROWSER RENDERING	
Allow local browser rendering	Disabled
APPLICATION DEEP LINKING	
Allow Application Deep Linking	Disabled
VOTIRO CDR INTEGRATION	
Enable Votiro CDR	Disabled
Isolation Regions	
Any	
Isolation Experience	
ISOLATION BANNER PREVIEW	

Isolation Profile Configuration	
Isolation Banner	Default
Persist Browser Isolation URL bar	Disabled
Isolation Experience	Native browser experience
WATERMARKING	
Enable Watermarking	Disabled
COOKIE PERSISTENCE	
Cookie Persistence	**Enabled**

Low Risk Isolation Profile for Cloud Browser Isolation (CBI)

This isolation profile should be used in places where productivity is a priority, with features like:

- Zscaler Client Connector Posture Control
- User specific URL Filtering Policies

Isolation Profile Configuration	
General	
Name	**Low_Risk**
Turbo Mode	**Enabled**
Description	Read Only Isolation Profile Isolation Regions are set to all for global redundancy and better user experience
Company Settings	
Proxy configuration URL	Use recommended PAC file URL
Override PAC file and return traffic to ZIA Public Service Edge	Enabled
Root Certificates	Zscaler Root Certificate
Security	
ALLOW COPY & PASTE FROM	
Local computer to isolation	**Enabled**
Isolation to local computer	Disabled
ALLOW FILE TRANSFERS FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW PRINTING	
Allow printing from isolation	Disabled

Isolation Profile Configuration	
RESTRICT TEXT INPUT	
Read-Only Isolation	False
ALLOW VIEWING OFFICE FILES	
View office files in isolation	**Enabled**
LOCAL BROWSER RENDERING	
Allow local browser rendering	Disabled
APPLICATION DEEP LINKING	
Allow Application Deep Linking	Disabled
VOTIRO CDR INTEGRATION	
Enable Votiro CDR	Disabled
Isolation Regions	
Any	
Isolation Experience	
ISOLATION BANNER PREVIEW	
Isolation Banner	Default
Persist Browser Isolation URL bar	Disabled
Isolation Experience	Native browser experience
WATERMARKING	
Enable Watermarking	Disabled
COOKIE PERSISTENCE	
Cookie Persistence	Disabled

High Risk Isolation Profile for Cloud Browser Isolation (CBI)

This isolation profile should be used in places where security is a priority, with features like:

- User Risk Criteria (Critical Risk score 80-100) for URL Filtering and Cloud App Control Policies
- URL Filtering Policies associated with the following URL categories under the Miscellaneous SuperCategory:
    - Miscellaneous or Unknown
    - Other Miscellaneous
    - Newly Registered and Observed Domains

Isolation Profile Configuration	
General	
Name	**Hish_Risk_ReadOnly**
Turbo Mode	Enabled
Description	Read Only Isolation Profile Isolation Regions are set to all for global redundancy and better user experience
Company Settings	
Proxy configuration URL	Use recommended PAC file URL
Override PAC file and return traffic to ZIA Public Service Edge	Enabled
Root Certificates	Zscaler Root Certificate
Security	
ALLOW COPY & PASTE FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW FILE TRANSFERS FROM	

Isolation Profile Configuration	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW PRINTING	
Allow printing from isolation	Disabled
RESTRICT TEXT INPUT	
Read-Only Isolation	**Enabled**
ALLOW VIEWING OFFICE FILES	
View office files in isolation	**Enabled**
LOCAL BROWSER RENDERING	
Allow local browser rendering	Disabled
APPLICATION DEEP LINKING	
Allow Application Deep Linking	Disabled
VOTIRO CDR INTEGRATION	
Enable Votiro CDR	Disabled
Isolation Regions	
Any	
Isolation Experience	
ISOLATION BANNER PREVIEW	
Isolation Banner	Default
Persist Browser Isolation URL bar	Disabled
Isolation Experience	Native browser experience

Isolation Profile Configuration	
WATERMARKING	
Enable Watermarking	Disabled
COOKIE PERSISTENCE	
Cookie Persistence	**Enabled**

Sandbox Isolation Profile (Sandbox Isolation Integration with Advanced Cloud Sandbox)

Isolation Profile Configuration	
General	
Name	**Sandbox_Isolation**
Turbo Mode	**Enabled**
Description	The Isolation Profile is used for Sandbox Integration. Isolation Regions set to all for global redundancy and better user experience
Company Settings	
Proxy configuration URL	Use recommended PAC file URL
Override PAC file and return traffic to ZIA Public Service Edge	Enabled
Root Certificates	Zscaler Root Certificate
Security	
ALLOW COPY & PASTE FROM	
Local computer to isolation	Disabled
Isolation to local computer	Disabled
ALLOW FILE TRANSFERS FROM	
Local computer to isolation	Disabled
Isolation to local computer	**Enabled**
Isolation to local computer controls	**Sandbox Scanned**
ALLOW PRINTING	
Allow printing from isolation	**Enabled**
RESTRICT TEXT INPUT	
Read-Only Isolation	Disabled
ALLOW VIEWING OFFICE FILES	

Isolation Profile Configuration	
View office files in isolation	**Enabled**
LOCAL BROWSER RENDERING	
Allow local browser rendering	Disabled
APPLICATION DEEP LINKING	
Allow Application Deep Linking	Disabled
VOTIRO CDR INTEGRATION	
Enable Votiro CDR	Disabled
Isolation Regions	
Any	
Isolation Experience	
ISOLATION BANNER PREVIEW	
Isolation Banner	Default
Persist Browser Isolation URL bar	Disabled
Isolation Experience	Native browser experience
WATERMARKING	
Enable Watermarking	Disabled
COOKIE PERSISTENCE	
Cookie Persistence	Disabled

For more information, please refer to the following resources:

- Sandbox Integration with Isolation
- Configuring the Sandbox Policy

Cloud App Control Policies and Isolation

FILE SHARING				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS OneDrive	**Allow Viewing, Uploading**	Office 365 One Click Rule
2	Isolate_GDrive_Globally	APPLICATIONS GDrive USER AGENT Opera;Firefox;MicrosoftInternetExplorer; Microsoft Edge;Chrome;Safari;MS Chromium Edge	**Isolate Viewing Mail** **Isolation Profile Low_Risk**	Isolate GDrive, see Secure Browsing LEading Practices document for more information on Isolation
3	Block_Risk_Index_4_Unsanctioned	CLOUD APPLICATION RISK PROFILE **Risk_Index_4_Unsanctioned**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
4	Block_Risk_Index_5_Unsanctioned	CLOUD APPLICATION RISK PROFILE **Risk_Index_5_Unsanctioned**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

In this section we present some examples as to how we can leverage Cloud Browser Isolation (CBI) with Cloud App Control Policies. We provide example for the Cloud App Category "File Sharing" and "Webmail":

WEBMAIL				
Rule Order	**Rule Name**	**Criteria**	**Action**	**Description**
1	Office 365 One Click Rule	APPLICATIONS Outlook	**Allow Viewing Mail, Sending Attachments, Sending Mail**	Office 365 One Click Rule
2	Isolate_Gmail_Globally	APPLICATIONS Gmail USER AGENT Opera;Firefox;MicrosoftInternetExplorer; Microsoft Edge;Chrome;Safari;MS Chromium Edge	**Isolate Viewing Mail** **Isolation Profile Low_Risk**	Isolate GDrive, see Secure Browsing LEading Practices document for more information on Isolation
3	Block_Risk_Index_4_Unsanctioned	CLOUD APPLICATION RISK PROFILE **Risk_Index_4_Unsanctioned**	**Disabled**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 4". It is recommended to use the SaaS Security Report (Shadow IT Report) to assess whether changing the status from "Disabled" to "Block Application Access" could have any business impact.
4	Block_Risk_Index_5_Unsanctioned	CLOUD APPLICATION RISK PROFILE **Risk_Index_5_Unsanctioned**	**Block Application Access**	Block Cloud Applications which are "Unsanctioned" and classified by Zscaler as "Risk Index 5".

URL Filter Policies and Isolation

In this section we present some examples as to how we can leverage Cloud Browser Isolation (CBI) with URL Filter Policies. We provide an example that would isolate based on a specific URL categories and browser user agents:

Rule Order	Rule Name	Criteria	Action	Description
1	Isolate_Miscellaneous_Globally	**PROTOCOL** HTTPS;HTTP **REQUEST METHODS** OPTIONS;GET;HEAD;POST;PUT;DELETE;TRACE;CONNECT;OTHER **URL CATEGORIES** Other Miscellaneous; Newly Registered and Observed Domains; Non-Categorizable; **USER AGENT** Opera; Firefox; Microsoft Internet Explorer; Microsoft Edge; Chrome; Safari	**Isolate** **Isolation Profile "Hish_Risk_ReadOnly"**	Isolate the most critical Zscaler URL Categories. In case a customer requires more strict isolate criteria, Zscaler recommends to isolate the URL Category "Miscellaneous or Unknown" as well (About URL Categories & Classes).

Rule Order	Rule Name	Criteria	Action	Description
2	Isolate_User_Risk_Profile	**PROTOCOL** HTTPS;HTTP **REQUEST METHODS** OPTIONS;GET;HEAD;POST;PUT;DELETE;TRACE;CONNECT;OTHER **USER AGENT** Opera;Firefox;Microsoft Internet Explorer;Microsoft Edge;Chrome;Safari;MS Chromium Edge **USER RISK PROFILE** High (60 - 79); Critical (80 - 100)	**Isolate** **Isolation Profile** **"Hish_Risk_ReadOnly"**	Isolate based on User Risk Profiles (High & Critical). Users are assigned a risk score based on their browsing activities. A range of risk scores is grouped as a risk score level. By default, the following user risk score levels are available: • Low: Level with user risk scores ranging from 0 to 29 • Medium: Level with user risk scores ranging from 30 to 59 • High: Level with user risk scores ranging from 60 to 79 • Critical: Level with user risk scores ranging from 80 to 100 In case the customer is not enrolled for CBI. Zscaler recommends setting the action to "Caution" or "Block" for User Risk Profiles (High & Critical). NOTE: User Risk Profiles must be enabled for the tenant for this.

Sandbox and Isolation

Rule Order	Rule Name	Criteria	Action	AI Instant Verdict	Description
1	MS_Office_PDF_Sandbox_Isolate	**FILE TYPES** Microsoft Excel (xls, xlsx, xlsm, xlam, xlsb, slk, xltm); Microsoft Word (doc, docx, docm, dotx, dotm); Microsoft Rich Text Format (rtf); Microsoft PowerPoint (ppt, pptx, pptm, potx, ppsx, ppam, potm, ppsm) Portable Document Format (pdf); **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; **PROTOCOLS** HTTPS; HTTP	**Quarantine and Isolate First Time** **Block Subsequent Downloads** **Isolation Profile "Sandbox_Isolation"**	Enabled	The user does not have to wait for the Sandbox analysis to complete (5-15 minutes). While sandbox analysis is in progress, a safer file version can be viewed within the isolation browser. The action "Quarantine and Isolate" is only visible when you select file types such as " Microsoft Office Files" or "PDF". Subscriptions required to enable Sandbox integration with Isolation: 1. Advanced Sandbox 2. Cloud Browser Isolation (CBI)

Rule Order	Rule Name	Criteria	Action	AI Instant Verdict	Description
2	Catch_All_BA_Rule	**FILE TYPES** **All file types** **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; Sandbox Suspicious **URL CATEGORIES** **Any URL Category**	**Quarantine** First Time **Block** Subsequent Downloads **70 Minimum Threat Score**	Enabled	Overwrites the Default Behaviour Analysis (BA) Rule. The first action is set to Quarantine for all file types and any URL Category.

Rule Order	Rule Name	Criteria	Action	AI Instant Verdict	Description
Default	Default_BA_Rule	**FILE TYPES** ZIP (zip); Windows Library (dll64, dll, ocx, sys); Windows Executable (exe, exe64, scr) **SANDBOX CATEGORIES** Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anonymizer; Sandbox Ransomware; Sandbox Offsec Tools; **URL CATEGORIES** Suspicious Destinations **PROTOCOLS** Any	**Allow and scan** First Time **Block** Subsequent Downloads	Disabled	The Default Behaviour Analysis (BA) Rule

Note: This approach is suggested for financial and healthcare institutions.

Browser Control

You can define a Browser Control policy to warn users from going out to the Internet when they are using outdated or vulnerable browsers, plugins, and applications. The service examines browser versions and patches (including beta browsers), internet applications (for example, Adobe Flash, Sun Java, Apple QuickTime), and media download applications (for example, Windows Media Player). You can also reduce your organisation's security risk by blocking older browsers or specific browser versions with known vulnerabilities. The ZIA Admin Portal displays the latest 12 versions for most browsers. To learn more, refer to Browser Control.

Secure Browsing	
BROWSER VULNERABILITY PROTECTION	
Enable Checks & User Notification	Enabled
How Often to Check	Monthly
Disable Notification for Browsers	Disable
Disable Notification for Plugins	None
Disable Notification for Applications	None
BROWSER BLOCKING	
Allow All Browsers	Enabled

Note: Zscaler recommends that browser software versions be maintained by other enterprise tooling such as Mobile Device Management (MDM). Browser Control will operate based on the User Agent header present in an HTTP or SSL Inspected HTTPS session. Since this is a tenant wide setting there can be unintended consequences when using this feature. For example, Slack and Postman present a Chrome version that is significantly older than the current version released by Google.

SSL Inspection

About SSL Inspection

The HTTPS (Hypertext Transfer Protocol Secure) protocol is an aggregate of HTTP (Hypertext Transfer Protocol) and the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol, wherein the authentication and encryption capabilities of SSL/TLS protect HTTP communications. This protection is vital as the information you send online is passed from one device to another before it reaches the destination server. Sensitive information, such as credit card numbers, usernames, and passwords, could be seen by intermediate devices if the information is sent in clear text over HTTP. When the information is encrypted and protected by the SSL protocol, only the intended recipient can read the information. For more general information about SSL, see About Secure Sockets Layer (SSL).

Unfortunately, the security that SSL/TLS provides can be misused in several ways:

- SSL/TLS hides dangerous content such as viruses, spyware, and other malware.
- Attackers build their own websites with SSL/TLS encryption.
- Attackers inject their malicious content into well-known and trusted SSL-enabled sites.
- SSL/TLS can hide data leakage, for example, the transmission of sensitive financial documents from an organization.
- SSL/TLS can hide the browsing of websites that belong to legal-liability classes.

As more and more websites utilize HTTPS, including social media such as Meta/Facebook and X/Twitter, the ability to control and inspect traffic to and from these sites has become an essential piece of an organization's security posture.

The Zscaler service can inspect HTTPS traffic from your organization. It can also scan data transactions and apply policies to them. The Zscaler service functions as a full SSL proxy or SSL man-in-the-middle (MITM) proxy.

Refer to the following knowledge-based articles for more information:

- About SSL Inspection
- About Secure Sockets Layer (SSL)
- Supported Cipher Suites in SSL Inspection
- Safeguarding SSL Keys and Data Collected during SSL Inspection
- Adding Custom Certificate to an Application Specific Trust Store
- About SSL Inspection Policy
- Configuring SSL Inspection Policy
- Deploying SSL Inspection
- Deployment Scenarios for SSL Inspection

- Certificate Pinning and SSL Inspection
- Best Practices for Testing and Rolling Out SSL Inspection

What cannot be inspected?

Transport Layer Security (TLS) inspection requires that the endpoints trust the certificate presented by the inspecting service. Customers must install a certificate onto each endpoint to build this trust. Inspection is not possible on devices that cannot reasonably install the certificate (e.g., IoT/OT, BYOD, guest networks, etc.).

Some vendors have implemented an SSL verification commonly referred to as certificate pinning (see Certificate Pinning or Hard-Coded Certificates). Certificate pinning is designed to prevent MITM inspection. As such, Zscaler cannot inspect TLS traffic from sites or applications that use certificate pinning (e.g., Apple, many Microsoft 365 apps, Adobe, Cisco WebEx, Dropbox app, etc.). Applications that have end-to-end encryption privacy support, such as iMessage, Signal, Zoom, and WhatsApp, can be inspected for inline policy controls.

Zscaler cannot inspect sites and applications that use client-certificate authentication or that use unsupported ciphers.

Additionally, TLS inspection is often configured to exempt URL categories that have personally identifiable information (PII) concerns. The most common are health and finance sites. The exemption might be based on local compliance guidelines per country or recommended Acceptable User Policy (AUP) from legal or regulatory concerns with HR, councils, or legal experts for local privacy laws.

References

- ZIA SSL Inspection Leading Practices Guide | Zscaler
- Best Practices for Testing and Rolling Out SSL Inspection | Zscaler
- Software Developer Solution Guide | TLS and Certificate Integration (Software Developer Solution Guide)

Recommended Baseline Policies

Rule Order	Rule Name	Criteria	Action	Description
1	Smart Isolation One Click Rule	URL CATEGORIES **Suspicious Domains**	**Inspect** **Evaluate Other Policies** • Untrusted Server Certificates: **Block** • OCSP Revocation Check: **Enabled** • Block No Server Name Indication (SNI): **Enabled** • Block Undecryptable Traffic: **Enabled** • Minimum Client TLS VersionTLS: **1.0** • Minimum Server TLS VersionTLS: **1.0**	Auto-generated rule. Smart Isolate Single Click Rule is automatically created when you enable Smart Isolation from Browser Control. This feature requires a Cloud Browser Isolation (CBI) license. Consider rule order. You must create exceptions to not have Smart Isolation for specific URL categories or custom URLs listed above this policy.
2	Zscaler Recommended Exemptions	URL CATEGORIES **Recommended SSL Exemption**	**Do not inspect** **Bypass Other Policies** Block No Server Name Indication (SNI): **Disabled**	Auto-generated rule. The percentage of traffic that matches this rule is usually small and less than 1%.

Rule Order	Rule Name	Criteria	Action	Description
				The "Zscaler Recommended Exemptions" URL Category contains destinations that cannot be SSL inspected for various reasons, such as certificate pinning from well-known vendors. This list also includes Zscaler-owned domains. While it is recommended not to inspect these domains, you can always disable this rule. Alternatively, you can leave the rule enabled, but create higher-order Inspect rules if you want to inspect only specific domains outside the list. To discover the traffic that is not getting SSL inspected due to this rule, you can search the weblogs. Look for the reason "Not inspected because of Zscaler best practices" in the SSL Policy Reason field.
3	UCaaS One Click	CLOUD APPLICATIONS **RingCentral; Zoom; LogMeIn**	**Do not inspect** **Bypass Other Policies** Block No Server Name Indication (SNI): **Disabled**	An auto-generated rule. The UCaaS One Click Rule is created when the UCaaS option is enabled. Enabling the Zoom, GoTo, RingCentral, and/or the Webex option allows Zscaler to permit secure local breakout for their traffic automatically, without any manual configuration needed. When any of those options are enabled, it turns off SSL interception for all Zoom, GoTo, RingCentral, or for Webex destinations. To continue using existing granular controls for Zoom, GoTo, RingCentral traffic, or for Webex, disable the

Rule Order	Rule Name	Criteria	Action	Description
				respective option, and enable cloud application and firewall network application policies accordingly.
4	Exclude Endpoint Protection	CLOUD APPLICATIONS **Microsoft Defender Advanced Threat Protection; Crowdstrike**	**Do not inspect** **Bypass Other Policies** Block No Server Name Indication (SNI): **Disabled**	Bypass Microsoft Defender Advanced Threat Protection and/or CrowdStrike Cloud Application because of certificate pinning requirements.
5	Inspected MS Services	CLOUD APPLICATIONS **Microsoft Login; OneDrive; SharePoint Online**	**Inspect** ● Untrusted Server Certificates: **Block** ● OCSP Revocation Check: **Enabled** ● Block No Server Name Indication (SNI): **Enabled** ● OCSP Revocation Check: **Enabled** ● Block Undecryptable Traffic: **Enabled** ● Minimum Client TLS Version: **TLS 1.1**	SSL Inspection of OneDrive & SharePoint Online Cloud Applications is required for applying Data Loss Prevention policies. This rule should always be placed above (higher rank) the rule "Office 365 One Click."

Rule Order	Rule Name	Criteria	Action	Description
			• Minimum Server TLS Version: **TLS 1.1**	
6	Office 365 One Click	URL CATEGORIES **Office 365; Zscaler Recommended Exemptions Office 365**	**Do not inspect** **Bypass Other Policies** Block No Server Name Indication (SNI): **Disabled**	An auto-generated rule. Office 365 One Click Rule was created during the company creation.
7	Exclude FinanceHealthGovernment	URL CATEGORIES **Finance; Government; Health; Other Government and Politics**	**Do not inspect** **Evaluate Other Policies** • Untrusted Server Certificates: **Block** • Block No Server Name Indication (SNI): **Enabled** • Show End User Notifications: **Enabled** • Show Notifications for ATP Blocks: **Enabled** • OCSP Revocation Check: **Enabled** • Minimum TLS Version: **TLS 1.1**	Destination-based exemptions example. Exclude categories "Finance, Health, Government, & Other Government and Politics" from SSL Inspection. Consult with stakeholders to understand whether additional or different categories are needed. Evaluate URL Filtering Policy and/or Cloud App Control Policy.

Rule Order	Rule Name	Criteria	Action	Description
8	Exclusions due to Certificate Pinning	Certificate Pinning and SSL Inspection	**Do not inspect** **Evaluate Other Policies** ● Untrusted Server Certificates: **Allow** ● Block No Server Name Indication (SNI): **Disabled** ● Show End User Notifications: **Disabled** ● OCSP Revocation Check: **Enabled** ● Minimum TLS Version: **TLS 1.1**	Exclude cloud applications that require SSL certificate pinning only when exclusion is observed to be impacting services and when the exclusion is approved by the organization as a necessary and acceptable risk.
9	Exclude Source Locations	Device Groups **No Client Connector** Location Groups **Guest Wifi Group; Server Traffic Group; IoT Traffic Group**	**Do not inspect** **Evaluate Other Policies** ● Untrusted Server Certificates: **Allow** ● Block No Server Name Indication (SNI): **Disabled** ● Show End User Notifications: **Disabled** ● OCSP Revocation Check: **Enabled**	Excludes inspection from source locations that are traditionally not inspectable when Client Connector is not running. This keeps user machines with Client Connector from being exempted from inspection based upon their network selection.

Rule Order	Rule Name	Criteria	Action	Description
			• Minimum TLS Version: **TLS 1.1**	
…	**Add any additional rules between rules 9-10**	…	…	…
10	Crypto Downgrade Rule	URL CATEGORIES **Cryptography_Approved_Downgrades**	**Inspect** **Evaluate Other Policies** • Untrusted Server Certificates: **Block** • OCSP Revocation CheckE: **Enabled** • Block No Server Name Indication (SNI): **Enabled** • Block Undecryptable Traffic: **Enabled** • Minimum Client TLS Version: **TLS 1.1** • Minimum Server TLS Version: **TLS 1.1**	Allow and Inspect destinations within the URL category "Cryptography_Approved_Downgrades" that require TLS 1.1.

Rule Order	Rule Name	Criteria	Action	Description
11	SSL Inspect Catch All	**Any**	**Inspect** **Evaluate Other Policies** ● Untrusted Server Certificates: **Pass Through** ● OCSP Revocation Check: **Enabled** ● Block No Server Name Indication (SNI): **Enabled** ● Block Undecryptable Traffic: **Enabled** ● Minimum Client TLS Version: **TLS 1.2** ● Minimum Server TLS Version: **TLS 1.2**	This rule overwrites the default SSL Inspection rule. The rule blocks TLS 1.0 & TLS 1.1 globally. For enhanced security, consider changing "Untrusted Server Certificates" to "Block."
Default	Default SSL Inspection Rule	**Any**	**Do Not Inspect** **Evaluate Other Policies** ● Block No Server Name Indication (SNI): **Disabled** ● Show End User Notifications: **Disabled** ● Untrusted Server Certificates: **Block**	Default SSL Inspection Rule created during the company creation.

Rule Order	Rule Name	Criteria	Action	Description
			• OCSP Revocation Check: **Disabled** • Minimum TLS Version: **TLS 1.0**	

Untrusted Server Certificates: Select how the service handles untrusted certificates (e.g., path validation failure, unknown issuer, certificate expired, common name does not match):

- **Allow**: The service allows access to sites with untrusted certificates. Certificate warnings are displayed only when users access sites with expired certificates.
- **Pass Through**: Certificate warnings are displayed to users, and users can then decide to proceed to the site.
- **Block**: The service blocks access to sites with untrusted certificates.

DNS Control

About DNS Control

DNS Control provides the following benefits and enables Zscaler customers to:

- Monitor and apply policies to all DNS requests and responses, irrespective of the protocol and encryption. This includes UDP, TCP, and DNS over HTTPS (DoH).
- Define granular DNS filtering rules using several DNS conditions, such as users, groups, or departments, client locations, categorisation of domains and IP addresses, DNS record types, the location of resolved IPs, etc.
- Enforce condition-based actions on DNS traffic, such as allowing or blocking traffic, redirecting requests to specific DNS servers, redirecting users by overwriting DNS responses, etc.
- Detects and prevents DNS-based attacks and data exfiltration through DNS tunnels.
- Enhance your security posture by using Zscaler Trusted DNS Resolver for domain resolution.

For more information, please refer to the following knowledge-based articles:

- About DNS Control
- Configuring the DNS Control Policy
- Modifying the Default DNS Control Rule
- Detecting and Controlling DNS Tunnels
- DNS Control rules essential best practices
- Reference Architecture - Zscaler DNS Security and Control

Based on the default rules the following configuration should work for the vast majority of customers:

Recommended Baseline Policies - The “Zscaler’s Default Policies” approach

Rule Order	Rule Name	Criteria	Action	Description
1	ZPA Resolver for Road Warrior	LOCATIONS **Road Warrior**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Road Warrior traffic	Redirect Road Warrior Traffic to ZPA.
2	ZPA Resolver for Locations	**Any**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Location traffic	Redirect Location Traffic to ZPA.
4	Office 365 One Click Rule	REQUEST CATEGORIES **Office 365** RESPONSE CATEGORIES **Office 365**	**Allow**	Predefined allows DNS Categories by "Office 365 One-Click Rule".
5	Critical risk DNS categories	REQUEST CATEGORIES **Phishing;** **Botnet Callback;** **Malicious Content;** **Spyware/Adware;** **Domain Generation Algorithm (DGA) Domains** RESPONSE CATEGORIES **Phishing;** **Botnet Callback;**	**Block**	Predefined rule which blocks “Critical risk DNS categories”.

Rule Order	Rule Name	Criteria	Action	Description
		Malicious Content; **Spyware/Adware;** **Domain Generation Algorithm (DGA) Domains**		
6	Critical risk DNS tunnels	DNS TUNNELS & NETWORK APPS **BaiduYunDns; DnsTunMaliciousRsvd; GenesisMissionaryBaptistChurch; Hoff; Kr0; LearnZolaSuite; MailShell; SongMountainFineArt; TGIN; ThreeMinuteWebsite; ToadTexture; Truckinsurance; WeaverPublishing**	**Block**	Predefined rule which blocks "Critical risk DNS tunnels".
7	High risk DNS categories	REQUEST CATEGORIES **Other Security;** **Newly Registered and Observed Domains;** **Newly Revived Domains** RESPONSE CATEGORIES **Other Security;** **Newly Registered and Observed Domains;** **Newly Revived Domains**	**Block**	Predefined rule which blocks "High risk DNS categories".
8	High risk DNS tunnels	DNS TUNNELS & NETWORK APPS **DnsTunUnknownRsvd; DnsTunCatSocial;**	**Block**	Predefined rule which blocks "High risk DNS tunnels".

Rule Order	Rule Name	Criteria	Action	Description
		DnsTunCatIM; DnsTunCatP2P; DnsTunCatStreaming; DnsTunCatWebSearch; DnsTunCatMalware; DnsTunCatImgHost; DnsTunCatEnterprise; DnsTunCatBusiness; DnsTunCatMappStore; DnsTunCatGaming; DnsTunCatNetMgmt; DnsTunCatAuth; DnsTunCatTunneling; DnsTunCatFileTransfer; DnsTunCatDatabase; DnsTunCatConf; DnsTunCatRemote; DnsTunCatMobile; DnsTunCatAds		
9	Block DoH	Protocol **DNS Over HTTPS**	**Block**	The decision regarding blocking or allowing "DNS Over HTTPS (DoH)" is based on the customer's policy.
Default	Fallback ZPA Resolver for Road Warrior	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Road Warrior Traffic.
Default	Fallback ZPA Resolver for Locations	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Location Traffic.
Default	Unknown DNS Traffic	PROTOCOL **Any**	**Block**	Applies "Block" action on suspected malformed traffic, non-standard DNS traffic, or even

Rule Order	Rule Name	Criteria	Action	Description
				non-DNS traffic attempting to conceal itself as DNS traffic.
Default	Default Firewall DNS Rule	PROTOCOL **Any**	**Allow**	This rule is preconfigured to manage all the DNS traffic not explicitly defined and actioned in the higher-ranked, user-defined rules.

Appendix: Alternative DNS Control Examples

The following examples are alternative baseline policies structure for DNS Control Policies:

1. The "Default Allow" approach.
2. The "Default Block" approach for highly secured environments.

Note: In the context of the "Default Allow" and "Default Block" approaches, it is assumed that the "Zscaler's Default Policies" are disabled and not implemented. Therefore, for illustrative purposes, we have omitted them from the relevant tables provided.

Recommended Baseline Policies - The “Default Allow” approach

Rule Order	Rule Name	Criteria	Action	Description
1	ZPA Resolver for Road Warrior	LOCATIONS **Road Warrior**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Road Warrior traffic	Redirect Road Warrior Traffic to ZPA
2	ZPA Resolver for Locations	**Any**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Location traffic	Redirect Location Traffic to ZPA
3	Office 365 One Click Rule	REQUEST CATEGORIES **Office 365** RESPONSE CATEGORIES **Office 365**	**Allow**	DNS Category permitted by "Office 365 One-Click Rule".

Rule Order	Rule Name	Criteria	Action	Description
4	BlockCategory -Advanced-Security	REQUEST CATEGORIES **Phishing; Botnet Callback; Malicious Content; Domain Generated Algorithm Domains** RESPONSE CATEGORIES **Phishing; Botnet Callback; Malicious Content; Domain Generated Algorithm Domains**	**Block**	Block DNS requests matching the SuperCategory "Advanced Security".
5	BlockCategory -Security	REQUEST CATEGORIES **Other Security; Spyware/Adware; Custom Encrypted Content; Dynamic DNS Host; Newly Revived Domains** RESPONSE CATEGORIES **Other Security; Spyware/Adware; Custom Encrypted Content; Dynamic DNS Host; Newly Revived Domains**	**Block**	Block DNS requests matching the SuperCategory "Security"
6	Block DoH	DNS TUNNELS & NETWORK APPS **AdGuard; Blah DNS; CleanBrowsing; Cloudflare; DNSComcast; DNSGoogle; DNSNextdns; Open DNS; PowerDNS; Quad9; Rubyfish; DoHUnknown; Secure DNS**	**Block**	The decision regarding blocking or allowing "DNS Over HTTPS (DoH)" is based on the customer's policy.
7	Commonly Blocked DNS Tunnels	DNS TUNNELS & NETWORK APPS **Truckinsurance; TGIN; IMRWORLDWIDE; GenesisMissionaryBaptistChurch; SongMountainFineArt; BaiduYunDns; Hoff;**	**Block**	Block Commonly Blocked DNS Tunnels

Rule Order	Rule Name	Criteria	Action	Description
		LearnZolaSuite; WeaverPublishing; DnsTunMaliciousRsvd; MailShell; ToadTexture; Kr0; ThreeMinuteWebsite		
8	Block Unknown DNS Tunnels	DNS TUNNELS & NETWORK APPS **DnsTunCatAds; DnsTunCatAuth; DnsTunCatBusiness; DnsTunCatConf; DnsTunCatDatabase; DnsTunCatEnterprise; DnsTunCatFileTransfer; DnsTunCatGaming; DnsTunCatIM; DnsTunCatImgHost; DnsTunCatMalware; DnsTunCatNetMgmt; DnsTunUnknownRsvd; DnsTunCatP2P; DnsTunCatRemote; DnsTunCatSocial; DnsTunCatStreaming; DnsTunCatTunneling; DnsTunCatWebSearch; DnsTunCatMappStore; DnsTunCatMobile**	**Block**	Block Unknown DNS Tunnels
Default	Fallback ZPA Resolver for Road Warrior	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Road Warrior Traffic
Default	Fallback ZPA Resolver for Locations	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Location Traffic
Default	Unknown DNS Traffic	PROTOCOL **Any**	**Block**	Applies “Block” action on suspected malformed traffic, non-standard DNS traffic, or even non-DNS traffic

Rule Order	Rule Name	Criteria	Action	Description
				attempting to conceal itself as DNS traffic.
Default	Default Firewall DNS Rule	PROTOCOL **Any**	**Allow**	This rule is preconfigured to manage all the DNS traffic not explicitly defined and actioned in the higher-ranked, user-defined rules.

Recommended Baseline Policies - The "Default Block" approach for highly secured environments

Rule Order	Rule Name	Criteria	Action	Description
1	ZPA Resolver for Road Warrior	LOCATIONS **Road Warrior**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Road Warrior traffic	Redirect Road Warrior Traffic to ZPA
2	ZPA Resolver for Locations	**Any**	**Resolve by ZPA** IP Pool: ZPA IP Pool for Location traffic	Redirect Location Traffic to ZPA

Rule Order	Rule Name	Criteria	Action	Description
3	Office 365 One Click Rule	REQUEST CATEGORIES **Office 365** RESPONSE CATEGORIES **Office 365**	**Allow**	DNS Category permitted by "Office 365 One-Click Rule"
4	Allow Cloudflare DoH	DNS TUNNELS & NETWORK APPS **Cloudflare**	**Allow**	Example Rule : Allows Cloudflare "DNS Over HTTPS(DoH)" based on company policy.
5	Allowed DNS Categories	REQUEST CATEGORIES **"To be determined by the customer, based on company policy"**	**Allow**	**Define the DNS Categories that should be allowed. This rule is mandatory to be able to change the action of the rule "Default Firewall DNS Rule" to "Block".**
Default	Fallback ZPA Resolver for Road Warrior	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Road Warrior Traffic
Default	Fallback ZPA Resolver for Locations	PROTOCOL **Any**	**Disabled**	Fallback ZPA Resolver for Location Traffic
Default	Unknown DNS Traffic	PROTOCOL **Any**	**Block**	Applies "Block" action on suspected malformed traffic, non-standard DNS traffic, or even non-DNS traffic attempting to conceal itself as DNS traffic.

Rule Order	Rule Name	Criteria	Action	Description
Default	Default Firewall DNS Rule	PROTOCOL **Any**	**Block**	This rule is preconfigured to manage all the DNS traffic not explicitly defined and actioned in the higher-ranked, user-defined rules.