



SonicOS 7.1

DPI-SSL

Administration Guide

SONICWALL®

# Contents

<b>About SonicOS</b> .....	<b>3</b>
Working with SonicOS .....	3
SonicOS Workflow .....	5
How to Use the SonicOS Administration Guides .....	6
Guide Conventions .....	7
<b>About DPI-SSL</b> .....	<b>8</b>
Using DPI-SSL .....	8
Supported Features .....	9
Security Services .....	11
Deployment Scenarios .....	11
Proxy Deployment .....	11
Customizing DPI-SSL .....	12
Connections per Appliance Model .....	13
<b>DPI-SSL/TLS Client</b> .....	<b>14</b>
Deploying the DPI-SSL/TLS Client .....	14
Configuring General DPI-SSL/TLS Client Settings .....	15
Selecting the Re-Signing Certificate Authority .....	18
Configuring Exclusions and Inclusions .....	19
Applying DPI-SSL/TLS Client .....	30
Performing Content Filtering using DPI-SSL .....	30
Filtering Content by App Rules using DPI-SSL .....	31
Viewing DPI-SSL Status .....	32
<b>DPI-SSL/TLS Server</b> .....	<b>33</b>
Deploying the DPI-SSL/TLS Server .....	33
Configuring General DPI-SSL/TLS Server Settings .....	34
Configuring Exclusions and Inclusions .....	35
Configuring Server-to-Certificate Pairings .....	35
<b>SonicWall Support</b> .....	<b>37</b>
About This Document .....	38

# About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on deploying and applying DPI-SSL/TLS Client and Server.

## Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

## Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

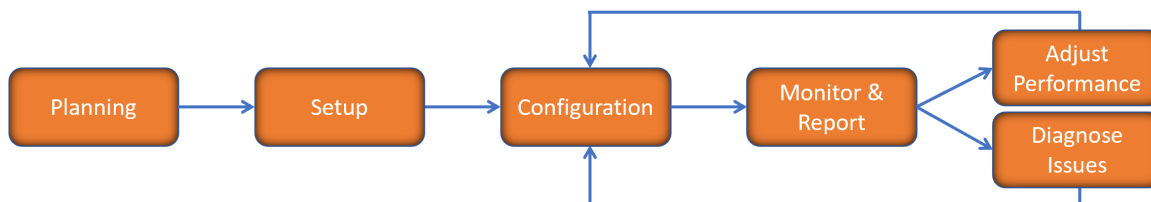
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS 7.1 API Reference Guide](#)

# SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

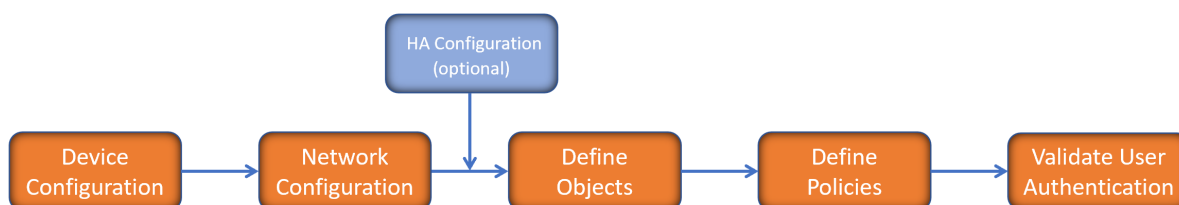


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

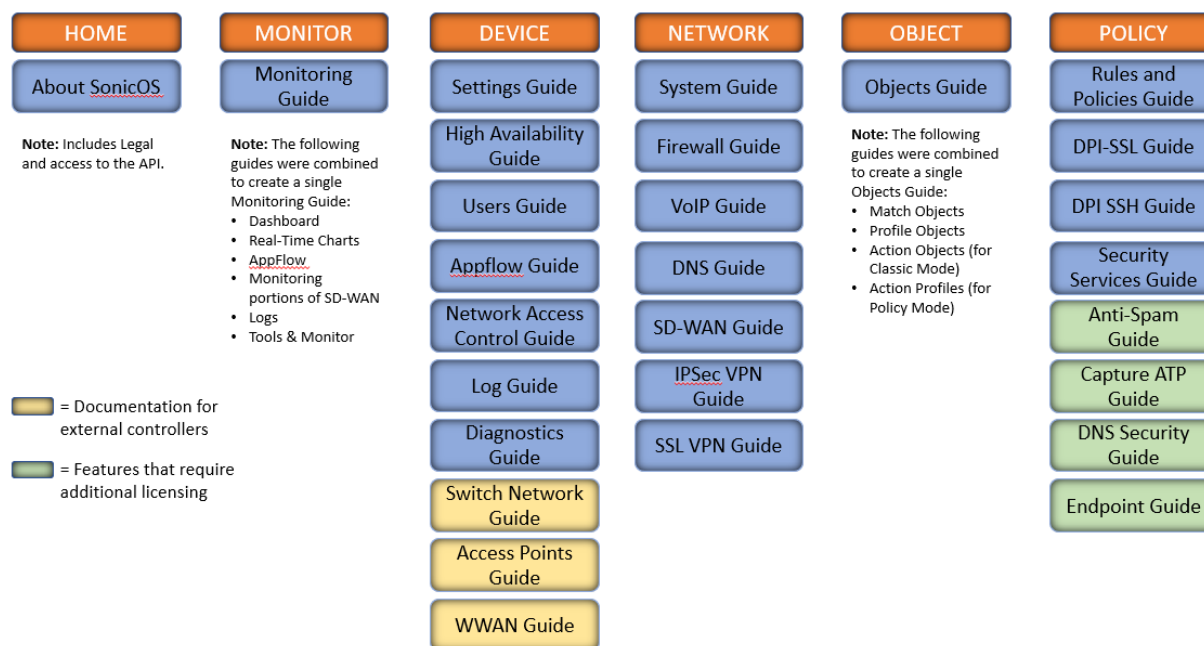


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

## How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the [SonicOS 7.1 Monitor Guide](#) and the [SonicOS 7.1 Objects Guide](#) which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

# Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
<b>Bold text</b>	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
<b>Function   Menu group &gt; Menu item</b>	Indicates a multiple step menu choice on the user interface. For example, <b>NETWORK   System &gt; Interfaces</b> means to select the <b>NETWORK</b> functions at the top of the window, then click on <b>System</b> in the left navigation menu to open the menu group (if needed) and select <b>Interfaces</b> to display the page.
<b>Code</b>	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<b>&lt;Variable&gt;</b>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment <b>serialnumber=&lt;your serial number&gt;</b> , replace the variable and brackets with the serial number from your device, such as <b>serialnumber=2CB8ED000004</b> .
<b>Italics</b>	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

# About DPI-SSL

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWall's Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL based traffic. The SSL traffic is decrypted (intercepted) transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic. DPI-SSL deployed in two main scenarios, Client DPI-SSL and Server DPI-SSL.

① **NOTE:** DPI-SSL is a separate, licensed feature that provides inspection of encrypted HTTPS traffic and other SSL-based IPv4 and IPv6 traffic.

## Topics:

- [Using DPI-SSL](#)
- [Deployment Scenarios](#)
- [Proxy Deployment](#)
- [Customizing DPI-SSL](#)
- [Connections per Appliance Model](#)

# Using DPI-SSL

## Topics:

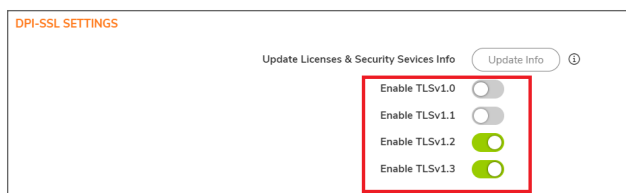
- [Supported Features](#)
- [Security Services](#)



# Supported Features

DPI-SSL supports:

- By the default, DPI-SSL supports only TLS 1.3 and TLS 1.2. If any customer wants to add TLS 1.0 and/or TLS 1.1, they can enable them on diag page. To support TLS 1.1 or TLS 1.0, customer can enable the necessary option and reboot firewall. Make sure that the firewall is rebooted to apply the changes.



- SHA-256 – All re-signed server certificates are signed with the SHA-256 hash algorithm.
- Perfect Forward Secrecy (PFS) – Perfect Forward Secrecy-based ciphers and other stronger ciphers are prioritized over weak ciphers in the advertised cipher suite. As a result, the client or server is not expected to negotiate a weak cipher unless the client or server does not support a strong cipher.

ⓘ | **NOTE:** DPI-SSL does not support SSL 3.0 which is forbidden, no option to restore it.

DPI-SSL also supports application-level Bandwidth Management over SSL tunnels. App Rules HTTP bandwidth management policies also applies to content that is accessed over HTTPS when DPI-SSL is enabled for App Rules.

DPI-SSL for both client and server can be controlled by Access Rules.

## Topics:

- [Support for Local CRL](#)
- [TLS Certificate Status Request Extension](#)
- [Support for Ciphers](#)
- [DPI-SSL and CFS HTTPS Content Filtering Work Independently](#)
- [Original Port Numbers Retained in Decrypted Packets](#)

## Support for Local CRL

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. A problem with contacting the CA for this list is that the browser cannot confirm whether it has reached the CA's servers or if an attacker has intercepted the connection to bypass the revocation check.

Local CRL is relative to typical CRL (or online CRL). For typical CRL, the client needs to download the CLR from a CRL distribution point. If the client is unable to download the CRL, then by default, the client trusts the certificate. Contrary to typical CRL, Local CRL maintains a list of revoked certificates locally in import memory for DPI-SSL to verify whether the certificate has been revoked.

For further information about this feature, contact [Technical Support](#).

## TLS Certificate Status Request Extension

DPI-SSL supports the TLS Certificate Status Request extension (formally known as OCSP stapling). By supporting this extension, the certificate status information is delivered to the DPI-SSL client through an already established channel, thereby reducing overhead and improving performance.

## Support for Ciphers

DPI-SSL Client supports ECC (Elliptic Curve Cryptography) ciphers:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256

DPI-SSL Client supports three TLS 1.3 ciphers:

- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256

## DPI-SSL and CFS HTTPS Content Filtering Work Independently

DPI-SSL and CFS HTTPS content filtering can be enabled at the same time and function as follows:

- If DPI-SSL Client Inspection is disabled, Content Filter Service filters HTTPS connections.
- If DPI-SSL Client Inspection is enabled, but the Content Filter option is not selected, Content Filter Service filters HTTPS connections.
- If DPI-SSL Client Inspection is enabled and the Content Filter option is selected, CFS does not filter HTTPS connections.

## Original Port Numbers Retained in Decrypted Packets

For encrypted connections DPI-SSL/DPI-SSH connections, the decrypted packet shows the destination port as 80 (in the case of HTTPS). When the decrypted packets are observed in packet capture/Wireshark, they now retain the original port numbers. The port number change applies only to the packet capture and not to the actual packet or connection cache.

## Security Services

The following security services and features can use DPI-SSL:

Gateway Anti-Virus	Content Filtering
Gateway Anti-Spyware	Application Firewall
Intrusion Prevention	

## Deployment Scenarios

DPI-SSL has two main deployment scenarios:

- **Client DPI-SSL:** Used to inspect HTTPS traffic when clients on the appliance's LAN access content located on the WAN. Exclusions to DPI-SSL can be made on a common-name or category basis.
- **Server DPI-SSL:** Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the appliance's LAN.

## Proxy Deployment

DPI-SSL supports proxy deployment, where all client browsers are configured to redirect to a proxy server, but an appliance sits between the client browsers and the proxy server. All DPI-SSL features are supported in this scenario, including supporting domain exclusions when the domain is part of a virtual hosting server, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

Additionally, typical data center server farms are fronted with a load balancer and/or reverse SSL Proxy to offload SSL processing on the servers. For a load balancer fronting the servers and doing decryption, the appliance usually only sees the IP of the load balancer, and the load balancer decrypts the content and determines the specific server to assign this connection to. DPI-SSL now has a global policy option to disable an IP-based exclusion cache. The exclusions continues to work even if the IP-based exclusion cache is off.

# Customizing DPI-SSL

① **IMPORTANT:** Add the NetExtender SSL VPN gateway to the DPI SSL IP-address exclusion list. As NetExtender traffic is PPP-encapsulated, having SSL VPN decrypt such traffic does not produce meaningful results.

In general, the policy of DPI-SSL is to secure any and all traffic that flows through the appliance. This may or may not meet your security needs, so DPI-SSL allows you to customize what is processed.

DPI-SSL comes with a list (database) of built-in (default) domains excluded from DPI processing. You can add to this list at any time, remove any entries you have added, and/or toggle built-in entries between exclusion from and inclusion in DPI processing. DPI-SSL also allows you to exclude or include domains by common name or category (for example, banking or health care).

Excluded sites, whether by common name or category, however, can become a security risk that can be exploited in the future by exploit kits that circumvent the appliance and are downloaded to client machines or by a man-in-the-middle hijacker presenting a fake server site/certificate to an unsuspecting client. To prevent such risks, DPI-SSL allows excluded sites to be authenticated before exclusion.

As the percentage of HTTPS connections increase in your network and new https sites appear, it is improbable for even the latest SonicOS version to contain a complete list of built-in/default exclusions. Some HTTPS connections fail when DPI-SSL interception occurs due to the inherent implementation of a new client app or the server implementation, and these sites might need to be excluded on the appliance to provide a seamless user experience. SonicOS keeps a log of these failed connections that you can troubleshoot and use to add any trusted entries to the exclusion list.

In addition to excluding/including sites, DPI-SSL provides both global authentication policy and a granular exception policy to the global one. For example, with a global policy to authenticate connection, some connections may be blocked that are in essence safe, such as new trusted CA certificates or a self-signed server certificate of a private (or local-to-enterprise deployment) secure cloud solution. The granular option allows you to exclude individual domains from the global authentication policy.

You can configure exclusions for a domain that is part of a list of domains supported by the same server (certificate). That is, some server certificates contain multiple domain names, but you want to exclude just one of these domains without having to exclude all of the domains served by a single server certificate. For example, you can exclude `youtube.com` without having to exclude any other domain, such as `google.com`, even though `*.google.com` is the common name of the server certificate that has `youtube.com` listed as an alternate domain under Subject Alternate-Name extension.

# Connections per Appliance Model

To learn about the hardware model and its maximum concurrent connections to perform the Client DPI-SSL inspections, refer to the following platform datasheets: SonicWall TZ Series.

Refer to the SonicWall resources page for more information about our Product Series. Search for high-end, mid-range, entry level, and virtual firewall details, such as Maximum connections (DPI SSL), from the **By Product Series** drop-down menu.

# DPI-SSL/TLS Client

The DPI-SSL/TLS Client deployment scenario typically is used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In this scenario, the firewall typically does not own the certificates and private keys for the content it is inspecting. After performing DPI-SSL inspection, the appliance re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By the default, this is the firewall certificate authority (CA) certificate, but a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

## Topics:

- [Deploying the DPI-SSL/TLS Client](#)
- [Applying DPI-SSL/TLS Client](#)
- [Viewing DPI-SSL Status](#)

## Deploying the DPI-SSL/TLS Client

Deploying the DPI-SSL/TLS Client includes:

- [Configuring General DPI-SSL/TLS Client Settings](#)
- [Selecting the Re-Signing Certificate Authority](#)
- [Configuring Exclusions and Inclusions](#)

# Configuring General DPI-SSL/TLS Client Settings

From the General Settings, you can set the services to be included with which to perform inspection, authenticate decrypted or intercepted connections, and allow or deny expired CA.

① **NOTE:** Make sure that DPI-SSL Client is enabled on a zone or zones according to [Enabling DPI-SSL Client on a Zone](#) to apply the DPI-SSL settings.

## To enable SSL Client inspection:

1. Navigate to **POLICY | DPI-SSL > Client SSL**.

By the default, Client SSL page displays the **General** tab.

The screenshot shows the 'Client SSL' configuration page with the 'General' tab active. The 'DPI-SSL STATUS' section indicates 0 current connections out of a 35000 limit. Under 'GENERAL SETTINGS', the 'Enable SSL Client Inspection' toggle is turned off. Other security services like Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Application Firewall, and Content Filter are also disabled. Several other settings are enabled, including 'Always authenticate server for decrypted connections', 'Allow Expired CA', 'Allow SSL without decryption (bypass) when connection limit exceeded', and 'Always authenticate server before applying exclusion policy'. The 'Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup' and 'Audit new default exclusion domain names prior to being added for exclusion' are disabled. 'Cancel' and 'Accept' buttons are at the bottom right.

2. **Enable SSL Client Inspection** to enable inspection of the encrypted HTTPS traffic.

3. Enable one or more services with which to perform inspection:

- **Intrusion Prevention**
- **Gateway Anti-Virus**
- **Gateway Anti-Spyware**
- **Application Firewall**
- **Content Filter**

4. Set the remaining General Settings.

---

<b>Always authenticate server for decrypted connections</b>	<p>To authenticate servers for decrypted or intercepted connections.</p> <p>When enabled this option, DPI-SSL blocks connections:</p> <ul style="list-style-type: none"><li>• To sites with untrusted certificates.</li><li>• If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.</li></ul> <p><b>i</b> <b>IMPORTANT:</b> Only enable this option if you need a high level of security. Blocked connections show up in the connection failures list, as described in <a href="#">Showing Connection Failures</a>.</p> <p><b>i</b> <b>TIP:</b> Use the <b>Skip CFS Category-based Exclusion</b> option (refer to <a href="#">Adding Custom Common Names</a>) along with this option to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.</p>
<b>Allow Expired CA</b>	<p>To allow expired or intermediate CAs.</p> <p><b>Allow Expired CA</b> becomes available only when <b>Always authenticate server for decrypted connections</b> is enabled.</p> <p>If it is not selected, connections are blocked if the domain name in the Client Hello cannot be validated against the server certificate for the connections.</p>
<b>Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup</b>	<p>To disable use of the server IP address-based dynamic cache for exclusion.</p> <p>This option is useful for proxy deployments, where all client browsers redirect to a proxy server, including if appliance is between the client browsers and the proxy server. All DPI-SSL features are supported, including domain exclusions when the domain is part of a virtual hosting server, as part of a server farm fronted with a load balancer, or in some cloud deployments, wherein the same server IP can be used by multiple domains.</p> <p>In such deployments, all server IPs as seen by the appliance are the proxy server's IP. It is, therefore, imperative that in proxy deployments, IP-based exclusion cache is disabled. Enabling this option does not affect SonicOS's capability to perform exclusions.</p>
<b>Allow SSL without decryption (bypass) when connection limit exceeded</b>	<p>To allow new connections to bypass decryption instead of being dropped when the connection limit is exceeded.</p> <p>By the default, this option is enabled and new connections over the DPI-SSL connection limit are bypassed.</p> <p>Disable <b>Allow SSL without decryption (bypass) when connection limit exceeded</b> to ensure new connections over the DPI-SSL connection limit are dropped.</p>

---



<b>Audit new built-in exclusion domain names prior to being added for exclusion</b>	<p>To audit new, built-in exclusion domain names before they are added for exclusion.</p> <p>When this option is enabled, whenever changes to the built-in exclusion list occur, for example, an upgrade to a new firmware image or other system-related actions, a notification pop-up dialog displays over the <b>Decryption Services &gt; DPI-SSL/TLS Client</b> page with the changes. You can inspect or audit the new changes and accept or reject any, some, or all of the new changes to the built-in exclusion list. At this point, the run-time exclusion list is updated to reflect the new changes.</p> <p>If this option is disabled, SonicOS accepts all new changes to the built-in exclusion list and adds them automatically.</p>
<b>Always authenticate server before applying exclusion policy</b>	<p>To always authenticate a server before applying a common-name or category exclusion policy.</p> <p>When enabled, DPI-SSL blocks excluded connections:</p> <ul style="list-style-type: none"> <li>• To sites with untrusted certificates.</li> <li>• If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.</li> </ul> <p>This is a useful feature to authenticate the server connection before applying exclusion policies. Enabling this option ensures that the appliance does not blindly apply exclusion on connections and thereby create a security hole for exclusion sites or sites belonging to excluded categories. This is especially relevant when banking sites, as a category, are excluded.</p> <p>By validating both the server certificate and the domain name in the Client Hello before applying an exclusion policy, SonicOS can reject untrusted sites and potentially block a type of zero-day attack from taking place. The SonicOS implementation takes the <i>trust-but-verify</i> approach to ensure that a domain name that matches the exclusion policy criteria is validated first, thus preventing an unsuspecting client from phishing or URL-redirect-related attacks.</p> <p><b>i</b>   <b>IMPORTANT:</b> If you are excluding alternate domains in the Subject-Alternate-Name extension, it is recommended that you enable this option.</p> <p><b>i</b>   <b>TIP:</b> Use the <b>Skip CFS Category-based Exclusion</b> option (refer to <a href="#">Adding Custom Common Names</a>) along with this option to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.</p>

5. Click **Accept**.

## Enabling DPI-SSL Client on a Zone

### To enable DPI-SSL Client on a zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone to be edited and click the **Edit** icon.
3. Select **Enable SSL Client Inspection**.
4. Finish configuring the zone.

5. Click **OK**.
6. Repeat Step 2 through Step 5 for each zone on which to enable DPI-SSL client inspection.

## Selecting the Re-Signing Certificate Authority

The re-signing certificate replaces the original certificate signing authority only if that authority certificate is trusted by the firewall. If the authority is not trusted, then the certificate is self-signed. To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

- ① **NOTE:** For information about requesting or creating a DPI SSL Certificate Authority (CA) certificate, refer to the Knowledge Base article, [Gen 7: How can I create a DPI-SSL certificate for the purpose of DPI-SSL certificate resigning?](#)

### To select a re-signing certificate:

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Certificate**.

The screenshot shows the 'Certificate' tab of the 'DPI-SSL STATUS' configuration page. At the top, there are tabs for 'General', 'Certificate', 'Objects', 'Common Name', and 'CFS Category-based Exclusion/Inclusion'. Below the tabs, the 'DPI-SSL STATUS' section displays 'Current DPI-SSL connections (cur/peak/max)' as '0 / 0 / 35000'. The 'CERTIFICATE RE-SIGNING AUTHORITY' section contains a blue information icon and text explaining that the certificate will replace the original authority only if trusted by the firewall. Below this text is a 'Certificate' dropdown menu with 'Default SonicWall DPI-SSL 2048 bit CA ce...' selected. There are 'Download', 'Cancel', and 'Accept' buttons at the bottom of the form.

3. Select the **Certificate** from the drop-down menu.  
By the default, DPI-SSL uses the Default SonicWall DPI-SSL CA certificate to re-sign traffic that has been inspected.  
① **NOTE:** If the certificate you want is not listed, you can import it from the **DEVICE | Settings > Certificates**. For more information, refer to [Importing a Certificate Authority Certificate](#).
4. Click the **Download** link to download the selected certificate to the firewall.  
① **TIP:** To view available certificates, click **System > Certificates** link which displays the **DEVICE | Settings > Certificates**.
5. Click **Accept**.
6. Add trust to the browser according to [Adding Trust to the Browser](#).

## Adding Trust to the Browser

For a re-signing certificate authority to successfully re-sign certificates, browsers have to trust the certificate authority. Such trust can be established by having the re-signing certificate imported into the browser's trusted CA list. Follow your browser's instructions for importing re-signing certificates. For more information, refer to [KB article](#).

## Configuring Exclusions and Inclusions

By the default, when DPI-SSL is enabled, it applies to all traffic on the appliance. You can customize to which traffic DPI-SSL inspection applies:

- **Exclusion/Inclusion** lists exclude or include specified objects and groups
- **Common Name** exclusions excludes specified host names
- **CFS Category-based Exclusion/Inclusion** excludes or includes specified categories based on CFS categories

This customization allows individual exclusion or inclusion of alternate names for a domain that is part of a list of domains supported by the same server (certificate). In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

① **NOTE:** If DPI-SSL is enabled on the firewall when using Google Drive, Apple iTunes, or any other application with pinned certificates, the application may fail to connect to the server. To allow the application to connect, exclude the associated domains from DPI-SSL. For example, to allow Google Drive to work, exclude:

```
.google.com  
.googleapis.com  
.gstatic.com
```

As Google uses one certificate for all its applications, excluding these domains allows Google applications to bypass DPI-SSL.

Alternatively, exclude the client machines from DPI-SSL.

### Topics:

- [Configuring Exclusions and Inclusions by Objects and Groups](#)
- [Configuring Exclusions and Inclusions by Common Name](#)
- [Configuring Exclusions and Inclusions by CFS Category](#)

# Configuring Exclusions and Inclusions by Objects and Groups

To customize DPI-SSL client inspection:

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Objects**.

General Certificate **Objects** Common Name CFS Category-based Exclusion/Inclusion

**DPI-SSL STATUS**

Current DPI-SSL connections (cur/peak/max) 0 / 0 / 35000

**EXCLUSION/INCLUSION**

ADDRESS OBJECT/GROUP

Exclude None

Include All

SERVICE OBJECT/GROUP

Exclude None

Include All

USER OBJECT/GROUP

Exclude None

Include All

Cancel Accept

3. Select an object or group to exclude or include the Objects or Groups from DPI-SSL inspection.  
**TIP:** The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

Object	Default Exclude	Default Include
ADDRESS OBJECT/GROUP	None	All
SERVICE OBJECT/GROUP		
USER OBJECT/GROUP		

4. Click **Accept**.

# Configuring Exclusions and Inclusions by Common Name

You can add trusted domain names to the exclusion list. Adding trusted domains to the Built-in exclusion database reduces the CPU effect of DPI-SSL and prevents the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

From **Common Name** section, you can:

- View the list of default common names excluded from DPI-SSL inspection.
- Reject or Approve the default common names.
- Add custom trusted domain names to:
  - Exclusion list.
  - Skip CFS Category-based Exclusion list.
  - Skip authenticating the server list.  
Opt-out of authenticating the server for this domain if authenticating the server results in the connection being blocked. Enable this setting only if the server is a trusted domain.
- Delete the custom common names.
- Import exclusions manually If you work in a closed environment or prefer to update default exclusions manually.
- Refresh the COMMON NAME EXCLUSIONS/INCLUSIONS table to get the latest data.

The screenshot shows the 'Common Name' configuration page in the SonicOS 7.1 DPI-SSL Administration Guide. The page is divided into several sections:

- DPI-SSL STATUS:** Shows current DPI-SSL connections (0/0/35000), default exclusions timestamp (UTC 01/00/1900 00:00:00.000), and last checked time (09/18/2023 02:08:25.640).
- COMMON NAME EXCLUSIONS/INCLUSIONS:** A table with columns for #, COMMON NAME, ACTION, and BUILT-IN. The table lists 10 entries, all with 'Exclude' as the action and 'Approved' as the built-in status.
- UPDATE DEFAULT EXCLUSIONS MANUALLY:** A section with a blue icon and text: 'If you work in a closed environment or prefer to update default exclusions manually, please download exclusions file from [www.mysonicwall.com](http://www.mysonicwall.com) to your disk, then import the file.' Below this is an 'Import Exclusions' button.

## Topics:

- [Viewing Status of DPI-SSL Default Exclusions](#)
- [Rejecting or Accepting Default Common Names](#)
- [Adding Custom Common Names](#)
- [Editing Custom Common Names](#)
- [Deleting Custom Common Names](#)
- [Showing Connection Failures](#)
- [Updating Default Exclusions Manually](#)

## Viewing Status of DPI-SSL Default Exclusions

The firewall periodically checks for updates to the DPI-SSL default exclusions database on MySonicWall and displays the latest status of the database in the **DPI-SSL Status** section. You can update the database on the firewall manually as described in [Updating Default Exclusions Manually](#).

### To view the status of default exclusions:

1. Navigate to **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.

You can find the status under **DPI-SSL STATUS** group.

DPI-SSL STATUS	
Current DPI-SSL connections (cur/peak/max)	0 / 0 / 35000
Default Exclusions Timestamp	UTC 01/00/1900 00:00:00.000
Last Checked	09/18/2023 02:08:25.640

<b>Default Exclusions Timestamp</b>	Date and time the default exclusions database was updated.
<b>Last Checked</b>	Date and time the firewall checked the default exclusions database.

## Rejecting or Accepting Default Common Names

❗ | **NOTE:** Default common names cannot be modified or deleted, but you can reject or accept them.

### To reject or accept common names:

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.
3. Scroll to **Common Name: Exclusions/Inclusions**.

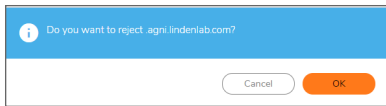
COMMON NAME EXCLUSIONS/INCLUSIONS			
#	COMMON NAME	ACTION	BUILT-IN
1	agni.lindenlab.com	Exclude	Approved
2	ati.ctrixonline.com	Exclude	Approved
3	ctrixonlinecdn.com	Exclude	Approved
4	gotomeeting.com	Exclude	Approved
5	jad.ctrixonline.com	Exclude	Approved
6	icloud.com	Exclude	Approved
7	itunes.apple.com	Exclude	Approved
8	itwin.com	Exclude	Approved
9	jas.ctrixonline.com	Exclude	Approved
10	live.ctrixonline.com	Exclude	Approved

You can control the display of the common names from the **View** drop-down menu:

<b>All</b>	Displays all common names.
<b>Default</b>	Displays the default common names (excludes <b>Custom</b> ).
<b>Custom</b>	Displays only common names you have added.

4. Hover over the approved common name to be rejected and click the **Reject this built-in name (-)** icon displayed at end of the row.

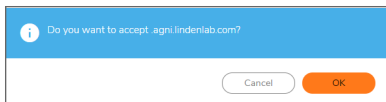
By the default, all Built-in common names are approved. You can reject the approval of a Built-in common name.



5. Click **OK**.

The **Reject (-)** icon becomes an **Accept (+)** icon, and **Approved** in the **Built-in** column becomes **Rejected**.

6. Hover over the rejected common name to be accepted and click the **Accept this built-in name (+)** icon displayed at end of the row.



7. Click **OK**.

The **Accept (+)** icon becomes an **Reject (-)** icon, and **Rejected** in the **Built-in** column becomes **Approved**.

## Adding Custom Common Names

**To add a custom common name:**

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.
3. Scroll to **Common Name: Exclusions/Inclusions**.

#	COMMON NAME	ACTION	BUILT-IN
1	agri.lindentab.com	Exclude	Approved
2	ati.ctrixonline.com	Exclude	Approved
3	ctrixonlinecdn.com	Exclude	Approved
4	gotomeeting.com	Exclude	Approved
5	jad.ctrixonline.com	Exclude	Approved
6	icloud.com	Exclude	Approved
7	itunes.apple.com	Exclude	Approved
8	itwin.com	Exclude	Approved
9	jas.ctrixonline.com	Exclude	Approved
10	live.ctrixonline.com	Exclude	Approved

You can control the display of the common names from the **View** drop-down menu:

<b>All</b>	Displays all common names.
<b>Default</b>	Displays the default common names (excludes <b>Custom</b> ).
<b>Custom</b>	Displays only common names you have added.

- Click **+Add** icon to add a custom common name.

## Add Common Names

---

Please add new common name entries separated by comma or newline characters.

**Action**

Exclude

Skip CFS Category-based Exclusion

Skip authenticating the server (i)

**Always authenticate server before applying exclusion policy**

Use Global Setting (i)

Close
Accept

- Add one or more common names in the field.  
Separate multiple entries with comma or newline characters.
- Specify the type of **Action**:
  - Exclude** (default)
  - Skip CFS Category-based Exclusion**
  - Skip authenticating the server** to opt out of authenticating the server for this domain if doing so results in the connection being blocked. Enable this option only if the server is a trusted domain.
- Select an option from the **Always authenticate server before applying exclusion policy** drop-down menu to **Enable** or **Disable** use of dynamic exclusion cache (both server IP and common-name based). **Use Global Setting** is selected by the default.



DPI-SSL dynamically determines if a connection should be intercepted (included) or excluded, based on policy or configuration. When DPI-SSL extracts the domain name for the connection, exclusion information is readily available for subsequent connections to the same server or domain.

8. Click **Accept**.

The **Common Name Exclusions/Inclusions** table is updated, with **Custom** in the **Built-in** column. Hover over the Information icon to see which custom attributes were selected. If a common name was added through the **Connection Failure List**, the Information icon indicates the type of failure:

- Skip CFS category exclusion
- Skip Server authentication
- Failed to authenticate server
- Failed Client handshake
- Failed Server handshake

9. Click **Accept**.

## Editing Custom Common Names

**NOTE:** Default common names cannot be modified or deleted, but you can modify or delete custom common names.

**To edit custom common names:**

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.
3. Scroll to **Common Name: Exclusions/Inclusions**.

#	COMMON NAME	ACTION	BUILT-IN
1	agni.lindentab.com	Exclude	Approved
2	atl.ctrixonline.com	Exclude	Approved
3	ctrixonlinecdn.com	Exclude	Approved
4	gotomeeting.com	Exclude	Approved
5	jad.ctrixonline.com	Exclude	Approved
6	icloud.com	Exclude	Approved
7	itunes.apple.com	Exclude	Approved
8	itwin.com	Exclude	Approved
9	las.ctrixonline.com	Exclude	Approved
10	live.ctrixonline.com	Exclude	Approved

You can control the display of the common names from the **View** drop-down menu:

<b>All</b>	Displays all common names.
<b>Default</b>	Displays the default common names (excludes <b>Custom</b> ).
<b>Custom</b>	Displays only common names you have added.

4. Hover over the custom common name to be edited and click the **Edit** icon.
5. Make the necessary changes.
6. Click **Accept**.

## Deleting Custom Common Names

① **NOTE:** Default common names cannot be modified or deleted, but you can modify or delete custom common names.

### To delete custom common names:

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.
3. Scroll to **Common Name: Exclusions/Inclusions**.

#	COMMON NAME	ACTION	BUILT-IN
1	agri.lindenlab.com	Exclude	Approved
2	att.ctrixonline.com	Exclude	Approved
3	ctrixonlinecdn.com	Exclude	Approved
4	gotomeeting.com	Exclude	Approved
5	lad.ctrixonline.com	Exclude	Approved
6	icloud.com	Exclude	Approved
7	itunes.apple.com	Exclude	Approved
8	itwin.com	Exclude	Approved
9	las.ctrixonline.com	Exclude	Approved
10	live.ctrixonline.com	Exclude	Approved

You can control the display of the common names from the **View** drop-down menu:

<b>All</b>	Displays all common names.
<b>Default</b>	Displays the default common names (excludes <b>Custom</b> ).
<b>Custom</b>	Displays only common names you have added.

4. Do one of the following:
  - Hover over the custom common name to be deleted and click the **Delete** icon.
  - Select check boxes of the custom common names in the **Common Name Exclusions/Inclusions** table and click the **Delete** icon on top of the table.
  - Select the check box in the table header to select all custom common names and click the **Delete** icon on top of the table.
5. Click **Accept**.

## Showing Connection Failures

SonicOS keeps a list of recent DPI-SSL client-related connection failures. This is a powerful feature that:

- Lists DPI-SSL failed connections.
- Allows you to audit the failed connections.
- Provide a mechanism to automatically exclude some failing domains.

The dialog box displays the run-time connection failures. The connection failures could be any of the following reasons:

- Failure to handshake with the Client
- Failure to handshake with the Server
- Failed to validate the domain name in the Client Hello
- Failure to authenticate the server (the server certificate issuer is not trusted)

The failure list is only available at run-time. The number logged for each failure is limited to ensure a single failure type does not overrun the entire buffer.

**To use the connection failure list:**

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **Common Name**.
3. Scroll to **Common Name: Exclusions/Inclusions**.

#	COMMON NAME	ACTION	BUILT-IN
1	agri.lindentab.com	Exclude	Approved
2	atl.ctrixonline.com	Exclude	Approved
3	ctrixonlinecdn.com	Exclude	Approved
4	gotomeeting.com	Exclude	Approved
5	jad.ctrixonline.com	Exclude	Approved
6	icloud.com	Exclude	Approved
7	itunes.apple.com	Exclude	Approved
8	itwin.com	Exclude	Approved
9	ias.ctrixonline.com	Exclude	Approved
10	live.ctrixonline.com	Exclude	Approved

4. Click **Show Connection Failures**.

Connection Failure List

Browse through the list of connection failures. You can add an entry or entries as custom exclusion names, clear some or clear all entries

#	CLIENT ADDRESS	SERVER ADDRESS	COMMON NAME	ERROR MESSAGE
No Data				

Each entry in this lists displays:

- **Client Address**
- **Server Address**
- **Common Name** – The common name of the failed connection’s domain. You can edit this entry inline before adding it to the automatic exclusion list.
- **Error Message** – Provides contextual information associated with the connection that enables you to make appropriate choices about excluding this connection.

5. Perform the actions as necessary on the list:

<b>Add an entry to the exclusion list</b>	<ol style="list-style-type: none"><li>a. Select the entry.</li><li>b. Make any edits to the entry.</li><li>c. Click <b>Exclude</b>.</li></ol>
<b>Delete an entry</b>	Select the entry to be deleted and click the <b>Clear</b> icon.
<b>Delete all entries</b>	Click the <b>Clear All</b> icon.

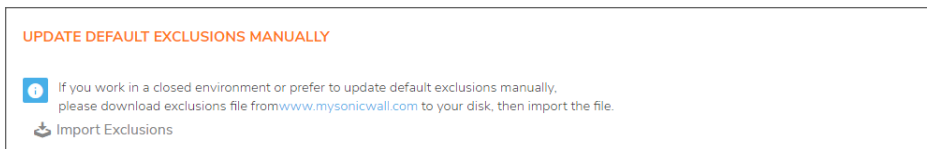
6. Click **Close** when finished.

## Updating Default Exclusions Manually

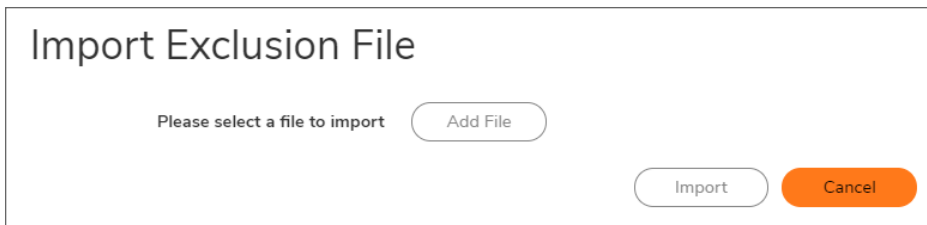
If your environment is closed or you prefer to update default exclusions manually, you can download the default exclusions database from [www.MySonicWall.com](http://www.MySonicWall.com) and then import them.

### *To update default exclusions manually:*

1. Import the default exclusions database from [www.MySonicWall.com](http://www.MySonicWall.com).
2. Navigate to the **POLICY | DPI-SSL > Client SSL**.
3. Scroll to the **Update Default Exclusions Manually** section.



4. Click **IMPORT EXCLUSIONS**.



5. Click **Add File**.
6. Browse and select the downloaded default exclusions database file.
7. Click **Import**.

The **Common Name Exclusions/Inclusions** table and the status of the default database used by the firewall in the DPI-SSL Default Exclusions Status section are updated.

# Configuring Exclusions and Inclusions by CFS Category

You can exclude or include entities by content filter categories.

## To specify CFS category-based exclusions/inclusions:

1. Navigate to the **POLICY | DPI-SSL > Client SSL**.
2. Click **CFS Category-based Exclusions/Inclusions**.

General Certificate Objects Common Name CFS Category-based Exclusion/Inclusion

**DPI-SSL STATUS**

Current DPI-SSL connections (cur/peak/max) 0/0/50000

**CONTENT FILTER CATEGORY INCLUSIONS/EXCLUSIONS**

Content Filtering is not licensed.

Please select an action for following categories:  Exclude  Include

Select all Categories

1. Violence	<input type="checkbox"/>	2. Intimate Apparel/Swimsuit	<input type="checkbox"/>	3. Nudism	<input type="checkbox"/>
4. Pornography	<input type="checkbox"/>	5. Weapons	<input type="checkbox"/>	6. Adult/Mature Content	<input type="checkbox"/>
7. Cult/Occult	<input type="checkbox"/>	8. Drugs/Illegal Drugs	<input type="checkbox"/>	9. Illegal Skills/Questionable Skills	<input type="checkbox"/>
10. Sex Education	<input type="checkbox"/>	11. Gambling	<input type="checkbox"/>	12. Alcohol/Tobacco	<input type="checkbox"/>
13. Chat/Instant Messaging (IM)	<input type="checkbox"/>	14. Arts/Entertainment	<input type="checkbox"/>	15. Business and Economy	<input type="checkbox"/>
16. Abortion/Advocacy Groups	<input type="checkbox"/>	17. Education	<input type="checkbox"/>	18. Training and Tools	<input type="checkbox"/>
19. Cultural Institutions	<input type="checkbox"/>	20. Online Banking	<input type="checkbox"/>	21. Online Brokerage and Trading	<input type="checkbox"/>
22. Games	<input type="checkbox"/>	23. Government	<input type="checkbox"/>	24. Military	<input type="checkbox"/>
25. Political/Advocacy Groups	<input type="checkbox"/>	26. Health	<input type="checkbox"/>	27. Information Technology/Computers	<input type="checkbox"/>
28. Hacking	<input type="checkbox"/>	29. Search Engines and Portals	<input type="checkbox"/>	30. E-Mail	<input type="checkbox"/>
31. Web Communications	<input type="checkbox"/>	32. Job Search	<input type="checkbox"/>	33. News and Media	<input type="checkbox"/>
34. Personals and Dating	<input type="checkbox"/>	35. Usenet News Groups	<input type="checkbox"/>	36. Reference	<input type="checkbox"/>
37. Religion	<input type="checkbox"/>				

Exclude connection if Content Filter Category is not available

Cancel Accept

**NOTE:** The status of the list is shown by an icon at the top of the view. A green icon indicates Content Filtering is licensed, a red icon that it is not.

3. Select the **Action** to be set for the categories:
  - **Exclude** (default)
  - **Include**
4. Do one of the following:
  - Select the categories to be included or excluded.  
By the default, all categories are unselected.
  - Click **Select all Categories** to select all categories.
5. Repeat the steps 3 and 4 to create the opposite list if required.  
For example, if categories are set for Exclude action in previous steps, you can set the categories for Include action in this step. This step is not applicable if **Select all Categories** option is set in previous step.
6. Select the **Exclude connection if Content Filter Category is not available** to exclude a connection if the content filter category information for a domain is not available to DPI-SSL.

In most cases, category information for a HTTPS domain is available locally in the firewall cache. When the category information is not locally available, DPI-SSL obtains the category information from the cloud without blocking the client or server communication. In rare cases, the category information is not available for DPI-SSL to make a decision. By the default, such sites are inspected in DPI-SSL.

7. Click **Accept**.

## Applying DPI-SSL/TLS Client

After you finish configuring your DPI-SSL Client, you can apply in:

- [Performing Content Filtering using DPI-SSL](#)
- [Filtering Content by App Rules using DPI-SSL](#)

## Performing Content Filtering using DPI-SSL

*To perform SonicWall Content Filtering on HTTPS and SSL-based traffic using DPI-SSL:*

- ① **IMPORTANT:** Make sure that **Enable SSL Inspection** and **Content Filter** options are enabled on **General** tab of **POLICY | DPI-SSL > Client SSL**. For more information, refer to [Configuring General DPI-SSL/TLS Client Settings](#).

*To perform SonicWall Content Filtering on HTTPS and SSL-based traffic using DPI-SSL:*

1. Create a content filter profile object on **OBJECT | Profile Objects > Content Filter**.
2. Configure a content filter rule on **POLICY | Rules and Policies > Content Filter Rules**.  
Make sure to select:
  - Content filter **Profile** object created on **OBJECT | Profile Objects > Content Filter**.
  - Default content filter **Action** object from the drop-down menu as the default action object is configured to Block, Confirm, or Passphrase the page or create a content filter action object for Block, Confirm, or Passphrase page on **OBJECT | Action Objects > Content Filter Actions**.
3. Navigate to **POLICY | Security Services > Content Filter**.  
Make sure that **SonicWall CFS** is selected for the Content Filter Type from the drop-down menu.
4. Scroll to the **Global Settings** section.  
Make sure that **Enable Content Filtering Service** is selected.  
By the default, **Enable Content Filtering Service** is selected.



GLOBAL SETTINGS	
Max URL Caches (entries)	15360
Enable Content Filtering Service	<input checked="" type="checkbox"/>
Block if CFS Server is Unavailable	<input type="checkbox"/>
Server Timeout	5 second(s)
Enable Local CFS Server	<input type="checkbox"/>
Primary Local CFS Server	<input type="text"/> ⓘ
Secondary Local CFS Server	<input type="text"/> ⓘ

5. Click **Accept**.

6. Navigate to a blocked, confirmed, or passphrased site using the HTTPS protocol to verify that it is properly blocked, confirmed, or passphrased.  
① **NOTE:** For content filtering over DPI-SSL, the first time HTTPS access is blocked results in a blank page being displayed. If the page is refreshed, the user sees the firewall block page.

## Filtering Content by App Rules using DPI-SSL

- ① **IMPORTANT:** Make sure that **Enable SSL Inspection** and **Application Firewall** options are enabled on **General** tab of **POLICY | DPI-SSL > Client SSL**. For more information, refer to [Configuring General DPI-SSL/TLS Client Settings](#).

### *To filter HTTPS and SSL-based traffic by app rules using DPI-SSL:*

1. Navigate to **POLICY | Rules and Policies > App Rules**.
2. Click the **Global Settings** icon and select **Enable App Rules**.
3. Configure an HTTP Client policy to block Microsoft Internet Explorer browser with block page as an action for the policy.

Here is an example to configure a match object and set the action for the app rule policy. But you can configure and set the action in other ways to allow or block the content.

- a. Create a match object with **Web Browser** as **Match Object Type** on **OBJECT | Match Objects > Match Objects** page and add **MSIE** Browser to the match object.
  - b. Add an app rule with **HTTP Client** as **Policy Type** on **POLICY | Rule and Policies > App Rules** page. Set match object created in previous step in **Match Object Included** and/or **Match Object Excluded** options.
4. Access any website using the HTTPS protocol with Internet Explorer to verify it is blocked.

### Topics:

[Enabling App Control Service on a Zone](#)

## Enabling App Control Service on a Zone

### *To enable DPI-SSL Client on a zone:*

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone to be edited and click the **Edit** icon.
3. Select **Enable App Control Service**.
4. Finish configuring the zone.
5. Click **OK**.
6. Repeat Step 2 through Step 5 for each zone on which to enable App Control Service.

# Viewing DPI-SSL Status

The **DPI-SSL Status** section displays the current DPI-SSL connections, peak connections, and maximum connections.

## ***To view DPI-SSL Status:***

Navigate to **POLICY | DPI-SSL > Client SSL**.

Under **General**, you can view the DPI-SSL Status.

**DPI-SSL STATUS**

Current DPI-SSL connections (cur/peak/max)    0 / 0 / 30000



## DPI-SSL/TLS Server

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall's LAN. Server DPI-SSL allows you to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

Afterward, if the pairing defines the server to be cleartext, then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

**NOTE:** In this deployment scenario, the owner of the firewall owns the certificates and private keys of the origin content servers. You would have to import the server's original certificate onto the appliance and create an appropriate server IP address to server certificate mappings in the Server DPI-SSL UI. For information about DPI-SSL, refer to [About DPI-SSL](#).

### Topics:

[Deploying the DPI-SSL/TLS Server](#)

## Deploying the DPI-SSL/TLS Server

Deploying the DPI-SSL/TLS server include:

- [Configuring General DPI-SSL/TLS Server Settings](#)
- [Configuring Exclusions and Inclusions](#)
- [Configuring Server-to-Certificate Pairings](#)

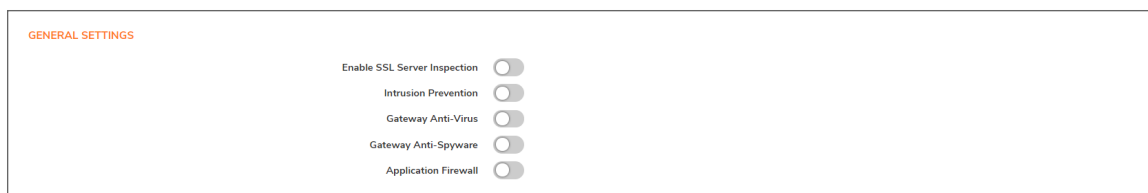
# Configuring General DPI-SSL/TLS Server Settings

From the General Settings, you can set the services to be included with which to perform inspection.

① **NOTE:** Make sure that DPI-SSL Server is enabled on a zone or zones according to [Enabling DPI-SSL Server on a Zone](#) to apply the DPI-SSL General settings.

**To enable Server DPI-SSL inspection:**

1. Navigate to the **POLICY | DPI-SSL > Server SSL**.



2. Scroll to the **General Settings** section.
3. Select **Enable SSL Server Inspection**.
4. Select one or more of the services with which to perform inspection:
  - **Intrusion Prevention**
  - **Gateway Anti-Virus**
  - **Gateway Anti-Spyware**
  - **Application Firewall**
5. Click **Accept**.
6. Scroll down to the **SSL Servers** section and configure the server or servers to which DPI-SSL inspection is applied. For more information, refer to [Configuring Server-to-Certificate Pairings](#).

## Enabling DPI-SSL Server on a Zone

**To enable DPI-SSL Server on a zone:**

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone to be edited and click the **Edit** icon.
3. Select **Enable SSL Server Inspection**.
4. Finish configuring the zone.
5. Click **OK**.
6. Repeat Step 2 through Step 5 for each zone on which to enable DPI-SSL server inspection.

# Configuring Exclusions and Inclusions

By the default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure inclusion or exclusion lists to customize to which traffic DPI-SSL inspection applies. The **Inclusion/Exclusion** lists provide the ability to specify certain objects or groups. In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

## To customize DPI-SSL server inspection:

1. Navigate to the **POLICY | DPI-SSL > Server SSL**.
2. Scroll to the **Inclusion/Exclusion** section.

3. Select an object or group to exclude or include the Objects or Groups from DPI-SSL inspection.
  - TIP:** The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

Object	Default Exclude	Default Include
ADDRESS OBJECT/GROUP	None	All
USER OBJECT/GROUP		

4. Click **Accept**.

# Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate is used to sign traffic for each server that has DPI-SSL inspection performed on its traffic.

## To configure a server-to-certificate pairing:

1. Navigate to the **POLICY | DPI-SSL > Server SSL**.
2. Scroll to the **SSL Servers** section.


3. Click **+Add**.


## Server DPI-SSL - SSL Server Setting


To view and manage certificates, go to [System > Certificates](#).


---

### SSL SERVER SETTING

 Server DPI-SSL allows you to configure pairings of an address object and certificate to typically offload/protect an internal Server from inbound WAN access.

Address Object/Group  

SSL Certificate  

Cleartext  

4. Select the **Address Object/Group** for the server or servers to which you want to apply DPI-SSL inspection.
5. Select the **SSL Certificate** to be used to sign the traffic for the server.  
This certificate is used to sign traffic for each server that has DPI-SSL Server inspection performed on its traffic. For more information on:
  - Importing a new certificate to the appliance, refer to [Selecting the Re-Signing Certificate Authority](#).
  - **Creating a Linux certificate.**
    - ① **TIP:** Clicking the [\(Manage Certificates\)](#) link displays the **DEVICE | Settings > Certificates** page. For more information, refer to [Creating a PKCS-12 Formatted Certificate File \(Linux Systems Only\)](#).
6. Select **Cleartext** to enable SSL offloading. When adding server-to-certificate pairs, the **Cleartext** option provides a method of sending unencrypted data onto a server.
  - ① **IMPORTANT:** For such a configuration to work properly, a NAT policy needs to be created for this server on the **POLICY | Rules and Policies > NAT Rules** page to map traffic destined for the offload server from an SSL port to a non-SSL port. Traffic must be sent over a port other than 443. For example, for HTTPS traffic used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to port 80 needs to be created for things to work properly.
7. Click **Add**.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

SonicOS DPI-SSL Administration Guide

Updated - December 2023

Software Version - 7.1

232-005879-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035