

## SonicWall® SonicOS 6.5.1.0

### Beta Release Notes

February 2018

These release notes provide information about the SonicWall® SonicOS 6.5.1.0 release.

Topics:

- [About SonicOS 6.5.1.0](#)
- [Supported Platforms](#)
- [New Features](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

## About SonicOS 6.5.1.0

SonicOS 6.5.1.0 introduces a number of new features. See the [New Features](#) section for more information.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.5. For more information, see the previous release notes, available on MySonicWall.

## Supported Platforms

SonicOS 6.5.1.0 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2650
- NSA 2600
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

+New platforms.

# New Features

This section describes the new features introduced in SonicOS 6.5.1.0.

Topics:

- [SonicOS API](#)
- [AWS Integration with SonicOS](#)
- [CFS Blocking of Individual Videos](#)
- [Capture ATP Friendly Filename Display](#)
- [DHCPv6 Relay](#)
- [DPI-SSH Blocking of SSH Port Forwarding](#)
- [FQDN Address Objects for NAT](#)
- [FQDN Over TCP DNS](#)
- [Access Rule Enhancements](#)
- [CFS Custom Header Insertion for HTTP Requests](#)
- [Enhanced HTTP/HTTPS Redirection with DP Offload](#)
- [LLDP Support](#)
- [Per User Client Side UI Preferences Storage](#)
- [Refactored SonicOS Web Interface Layout](#)
- [Capture Threat Assessment Client Enhancements](#)
- [Increased SPI/DPI Connection Capacity](#)
- [DPI vs DPI-SSL Dynamic Connection Sizing](#)
- [DPI-SSL Scalability Through Extended Memory](#)
- [DPI-SSL Support for Extra Ciphers](#)
- [Active/Active Clustering on NSA Platforms](#)
- [SonicOS Global Search](#)
- [Source MAC Overwrite for NAT](#)
- [UUID for Rules and Objects](#)
- [UX/UI Improvements for Content Pages](#)
- [WAN DDOS Protection Performance Enhancement](#)

## SonicOS API

SonicOS APIs provide an alternative method to the SonicOS Command Line Interface (CLI) for configuring selected functions.

Topics:

- [Supported Methods and MIME Types](#)
- [HTTP Status Codes](#)
- [Status & Error Representation](#)
- [Enabling SonicOS API](#)

- [Client Authentication](#)
- [Example - Commit Pending Configuration](#)
- [Example - Address Object API Calls](#)

## Supported Methods and MIME Types

SonicOS API utilizes four of the methods defined in the HTTP protocol (RFC 7231 & 5789) to create, read, update and delete resources. The table below describes the HTTP methods currently supported by SonicOS API.

### Supported HTTP Request Methods

HTTP Method	Description
GET	Retrieves the specified resource or collection of resources. GET is a read-only operation that does not alter appliance state or configuration. A GET operation should not contain a request-body.
POST	Submits data to be processed by the specified resource or collection of resources. In most cases, the POST verb is used by SonicOS APIs to create and add a resource to a collection of resources (e.g. add a new MAC address-object to collection of objects).
PUT	Updates the specified resource. The data included in the PUT request-body replaces the previous configuration.
DELETE	Deletes the specified resource or collection of resources.

SonicOS API uses standard HTTP status codes to report success or failure when servicing a request.

SonicOS APIs currently supports the following MIME types:

- Text/plain

Example:

```
GET /api/sonicos/address-objects/mac
Accept: text/plain
```

- Application/JSON

Example:

```
POST /api/sonicos/address-objects/mac
Content-type: application/json
Accept: application/json
{
  "address_object": {
    "mac": {
      "name": "001122334455"
    },
    "address": "001122334455"
    , "multi_homed": true
    , "zone": "LAN"
  }
}
```

The **Content-type** HTTP header is used to specify the format (MIME type) of the request body (input). The **Accept** HTTP header is used to specify the format of the response body (output).

## HTTP Status Codes

SonicOS API uses standard HTTP status codes to report success or failure when servicing a request.

## HTTP Status Codes

Code	Status Text	Description
200	OK	The request succeeded.
400	Bad Request	An invalid request was submitted. Verify that the request URI is correct and that the request body is as expected.
401	Not Authorized	The user is unauthenticated or lacks the required privileges for the operation requested.
403	Forbidden	The request was understood by the server but denied. The response body will note the reason why the request was denied.
404	Not Found	The resource specified was not found.
405	Method Not Allowed	The HTTP verb specified is not allowed or supported by the resource specified.
406	Not Acceptable	The MIME type specified in the HTTP 'Content-type' and/or 'Accept' header is not supported.
413	Request body too large	Maximum size of the request body was exceeded.
414	Request URL too long	The request URL exceeded the maximum size allowed or contains extra/unknown parameters (directories).
500	Internal Server Error	The request failed due to an internal server error. The response body should note the reason why the request failed.

## Status & Error Representation

All plain text output from the last CLI command executed is captured and returned back to the client. If the command executed was not a **show** command, and the requested operation succeeded, then the response body is empty. This is consistent with the CLI when executing a command via SSH or the serial console in that status is only rendered to the console upon error.

A JSON status object is guaranteed to be returned in the response body when performing a POST, PUT, DELETE operation or upon error(s) encountered when processing a request.

## Schema Structure

```
{
  "status": {
    "success": {boolean}
    , "cli": {
      "depth": {number}
      , "mode": "{string}"
      , "command": "{string}"
      , "configuring": {boolean}
      , "pending_config": {boolean}
      , "restart_required": "{string}"
    }
    , "info": [
      { "level": "{string}", "code": "{string}", "message": "{string}" }
      ...
    ]
  }
}
```

## Schema Attributes

### Schema Attributes

Attribute	Type	Description
status	object	Status object.
status.success	boolean (true   false)	Boolean success flag. Refer to the status.info array for more detailed info as to what caused the error if the success flag is false.
status.cli	object	CLI status. Note, this attribute will only be included when an API sent one or more commands to the CLI backend.
status.cli.depth	number (uint8)	Current mode depth of the CLI. 0 = top-level mode, >= 1 config mode.
status.cli.mode	string	Name of the current mode.
status.cli.command	string	Command last executed. Note, this attribute will only be included upon command error(s).
status.cli.configuring	boolean (true   false)	Boolean configuring flag. Should always be true upon one or more consecutive POST, PUT or DELETE API calls that modify configuration.
status.cli.pending_config	boolean (true   false)	Boolean pending-config flag. Should always be true upon one or more consecutive POST, PUT or DELETE API calls that modify configuration. This flag should be cleared once any/all pending changes are committed (saved).
status.cli.restart_required	string	Appliance restart status. Some configuration changes require an appliance restart in order to take effect. The following values indicate the type of restart needed: <ul style="list-style-type: none"><li>• NONE</li><li>• APPLIANCE</li><li>• CHASSIS</li><li>• CHASSIS_SHUTDOWN</li><li>• ALL_BLADES</li></ul>
status.info	array	Informational message(s).
status.info.level	string	Status level. One of the following types: info, warning, error.
status.info.code	string	Status code. If success, E_OK will be returned, else E_{XXX} where XXX = error code.
status.info.message	string	Status message.

## Enabling SonicOS API

SonicOS API is disabled by default in SonicOS. Any attempts to access SonicOS API while disabled will result in an HTTP 403 *Forbidden* error.

SonicOS API can be enabled by one of the following methods:

- In the SonicOS web management interface, navigate to **MANAGE | System Setup | Appliance > Base Settings** and select the **Enable SonicOS API** checkbox.
- In the CLI, starting at the `config#` prompt:

```
config(<serial number>)# administration
(config-administration)# sonicos-api
(config-administration)# commit
```

## Client Authentication

SonicOS API currently offers two mechanisms for client authentication:

- HTTP Basic Authentication (RFC 2617)
- Challenge-Handshake Authentication (CHAP)

Regardless of the authentication mechanism used:

- Only a single administrator can manage (modify configuration) at any given time. This remains true regardless of where an admin is logged in from (web management UI, CLI, GMS or SonicOS API).
- Only users with full admin privileges are allowed to access SonicOS API.
- Only a single SonicOS API session is currently allowed.

HTTP Basic Authentication is the simplest method for client authentication as it does not require cookies, session identifiers, etc. HTTP Basic Authentication uses the standard **Authentication** HTTP header to pass user credentials between the client and server. Because HTTP Basic Authentication provides no means for protecting the confidentiality of a user's credentials, SonicOS API requires user credentials to be transmitted over HTTPS.

For SonicOS API HTTP Basic Authentication, use the Linux command-line **curl** command with the **-u** option:

- Login:

```
curl -k -i -u admin:password -X POST https://a.b.c.d/api/sonicos/auth
```

- Logout:

```
curl -k -i -X DELETE https://a.b.c.d/api/sonicos/auth
```

## Example - Commit Pending Configuration

All SonicOS APIs that modify configuration (POST, PUT, DELETE) do not take effect immediately. Rather, configuration is staged and is not pushed to run-time config and saved to flash/permanent storage until API clients explicitly execute a POST request to `/api/sonicos/config/pending`. This is the same behavior as in the SonicOS CLI and equivalent to invoking the **commit** command from the top-level config mode.

Pending configuration can be canceled (deleted) at any time by executing a DELETE request to `/api/sonicos/config/pending`. Any/all pending configuration is canceled upon client session termination, whether due to idle-timeout or explicit logout. In this case, all unsaved changes are lost. It is the client's responsibility to either commit pending configuration after each POST/PUT/DELETE API call or maintain pending changes on the client side to be restored in a later session.

### Endpoint

Endpoint	HTTP Method & Body			
URI: <code>/api/sonicos/config/pending</code>	GET	POST	PUT	DELETE
Schema: <i>N/A</i>	Empty	Empty	-	Empty

### Schema Structure

A schema is not really applicable here as POST, PUT and DELETE HTTP body is expected to be empty. However, GET will return any/all pending (unsaved) configuration.

### Schema Attributes

Not applicable.

### Examples:

# GET Pending Changes (unchanged)

Request:

```
GET /api/sonicos/config/pending
Accept: application/json
```

**Response:**

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
}
```

**# GET Pending Changes**

**Request:**

```
GET /api/sonicos/config/pending
Accept: application/json
```

**Response:**

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
  "address_objects": [
    {
      "pending": "ADD"
      , "ipv4": {
        "name": "B"
        , "host": {
          "ip": "2.2.2.2"
        }
        , "zone": "WAN"
      }
    }
  ]
}
```

**# POST Pending Changes**

**Request:**

```
POST /api/sonicos/config/pending
Accept: application/json
```

**Response:**

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
  "status": {
    "success": true
    , "cli": {
      "depth": 1
      , "mode": "config_mode"
      , "configuring": true
      , "pending_config": false
      , "restart_required": "NONE"
    }
  }
  , "info": [
    { "level": "info", "code": "E_OK", "message": "Success." }
  ]
}
```

## Example - Address Object API Calls

# Create a new IPv4 Address Object named **Web Server**

```
POST /api/sonicos/address-objects/ipv4
```

```
Content-type: application/json
```

```
{
  "address_object": {
    "ipv4": {
      "name": "Web Server",
      "zone": "DMZ",
      "host": {
        "ip": "192.168.168.168"
      }
    }
  }
}
```

# Modify the **Web Server** Address Object host IP

```
PUT /api/sonicos/address-objects/ipv4/name/Web%20Server
```

```
Content-type: application/json
```

```
{
  "address_object": {
    "ipv4": {
      "host": {
        "ip": "192.168.168.1"
      }
    }
  }
}
```

# Delete the **Web Server** Address Object

```
DELETE /api/sonicos/address-objects/ipv4/name/Web%20Server
```

## AWS Integration with SonicOS

The SonicOS integration with Amazon Web Services (AWS) enables logs to be sent to AWS CloudWatch Logs, Address Objects and Groups to be mapped to EC2 Instances, and creation of VPNs to allow connections to Virtual Private Clouds (VPCs). SonicOS communicates with the various Application Programming Interfaces (APIs) of AWS.

### Topics:

- [Creating an AWS Identity](#)
- [AWS Access Configuration in SonicOS](#)
- [AWS Logs Configuration](#)
- [AWS Objects Configuration](#)
- [AWS VPN Configuration](#)

## Creating an AWS Identity

IAM Identities, including Users and Groups, can be created and managed from the IAM page in the AWS Management Console.



Assuming that the AWS Account is already created and that an Administrator with either Root access or widespread privileges is logged into that account, it is then necessary to create an *IAM User*, if one does not already exist, that will be used by the firewall to access the various AWS APIs for the services supported by the firewall.

The user needs certain permissions to access the different services. These permissions can either be granted directly to the user or included in a security access policy assigned to an IAM Group and then the user added to that group.

The security policy used, either for a group to which the user belongs or attached to the user directly, must include the following permissions:

- AmazonEC2FullAccess – For **AWS Objects** and **AWS VPN**
- CloudWatchLogsFullAccess – For **AWS Logs**

The IAM user can be created specifically for use by the firewall alone. However, if the same user is going to access the AWS Management Console, the **Programmatic access** checkbox must be selected.

The second step of the Add User wizard determines which permissions the user will have assigned, either through adding the user to a group or attaching the permission policies directly.

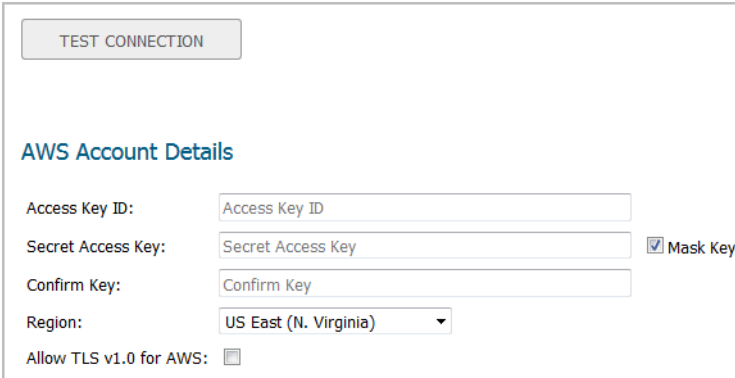
After reviewing the details of the user to be created and pressing the **Create User** button, there is a final and critical stage.

–DO NOT LEAVE THE ADD USER WIZARD–

You must retrieve the **Secret Access Key** that has been created for the user. The Secret Access Key together with the Access Key will be used in the configuration of the firewall. It will be needed for all API access to AWS. You should either copy it to a safe location or download the CSV file and keep that in a safe, secure location.

## AWS Access Configuration in SonicOS

You can configure SonicOS with the AWS Security Credentials on the **MANAGE | System Setup | Network > AWS Configuration** page.



TEST CONNECTION

### AWS Account Details

Access Key ID:

Secret Access Key:   Mask Key

Confirm Key:

Region:

Allow TLS v1.0 for AWS:

The settings include an AWS Identity and Access Management (IAM) User's Access Key (**Access Key ID**), the corresponding **Secret Access Key** and a default region. The default region is used by the **AWS Logs** page, and for initialization of the **AWS Objects** and **AWS VPN** pages (though different regions can be selected on those two pages).

## AWS Logs Configuration

Logged events generated on the firewall can be sent to the AWS CloudWatch Logs service. From there, the data can be used by AWS hosted analysis tools such as ElasticSearch and Kibana.

The SonicOS **AWS Logs** page allows configuration of the AWS endpoint to which the logs are sent along with settings affecting the frequency with which the data is posted.

In order to send the logs from SonicOS to Amazon CloudWatch Logs, you must first create a Log Group and a Log Stream in AWS. Assuming that you have an Identity Access Management (IAM) user account with the appropriate permissions to access CloudWatch Logs from the AWS Console, navigate to the CloudWatch section and select the Logs item in the left hand navigation menu. Ensure that you have selected the appropriate AWS Region for the logs to be stored. As with many AWS services, CloudWatch Logs is region specific. First create the Log Group and then the Log Stream.

#### **To enable AWS logs in SonicOS:**

- 1 Navigate to the **MANAGE | Logs & Reporting | Log Settings > AWS Logs** page.
- 2 Select the **Enable Logging** checkbox.
- 3 Ensure that the selected AWS **Region** is the one in which the Log Group and Log Stream were created. You can change the region used by the firewall either on this page or on the AWS Configuration page.
- 4 Enter the names of the **Log Group** and **Log Stream** that you created earlier and which will hold the logs sent to AWS CloudWatch Logs.
- 5 The logs will be sent at the specified **Synchronization Interval**. Change the Interval to suit your needs.
- 6 Click **ACCEPT**.

## **AWS Objects Configuration**

The **AWS Objects** page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with Address Objects (AOs) and Groups (AGs) configured on the firewall.

New AOs are created for Instance IP addresses, AGs for all addresses of an Instance and those Instance AGs can be added to existing Address Groups. Those objects, as with any other AOs and AGs, can then be used in firewall policies for networking, access control and to shape the interaction with EC2 Instances running on AWS.

In AWS, tag the EC2 Instance to then be able to use that tag when defining Address Object Mappings in SonicOS. With the Instance selected, click on the **Actions** button to launch the popup menu and then choose **Instance Settings > Add/Edit Tags**.

#### **To create a new Address Object Mapping:**

- 1 Navigate to the **MANAGE | Policies | Objects > AWS Objects** page in SonicOS.
- 2 Click the **New Mapping** button.
- 3 Click the **New Condition** button to choose from the whole range of allowable properties.
- 4 For example, select *Custom Tag* for **Property**, then enter the key and value used in your EC2 Instance tag and click **OK**.
- 5 Optionally add a second mapping condition by clicking **New Condition** again.
- 6 When ready, click **OK** and then click **ACCEPT** to save the mapping.  
Address Objects are then created for the IP addresses of each EC2 Instance that matches the mapping.
- 7 Select the **Enable Mapping** checkbox and then click **ACCEPT** to make the Address Object Mappings take effect.

With mappings in place, a **Synchronization Interval** set, **Regions to Monitor** specified, and **Enable Mapping** selected, you will see Address Objects and Groups representing the matched EC2 Instances and their IP addresses start to appear.

On the **AWS Objects** page, the Address Group and the Mapped Address Groups are shown in the AWS EC2 Instances table. Expanding the relevant row reveals the Address Objects corresponding to an Instance's public and private IP addresses. You can see those same host Address Objects on the **Objects > Address Objects** page in SonicOS.

# AWS VPN Configuration

Establishing and managing the connections between the computers on the local area network (LAN) and those in the Virtual Private Clouds (VPCs) on AWS is achieved by using the **MANAGE | Connectivity | VPN > AWS VPN** page in SonicOS.

The screenshot shows the SonicOS interface for configuring AWS VPN connections. The main content area is titled "AWS Virtual Private Clouds" and displays a table of VPCs. The table has the following columns: #, VPC/Subnets, CIDR, VPC Status, Manage VPN Connection, VPN Status, and Details. The data is filtered by "Region: US West (Oregon) (us-west-2)".

#	VPC/Subnets	CIDR	VPC Status	Manage VPN Connection	VPN Status	Details
▼ Region: US West (Oregon) (us-west-2)						
1	VPC: vpc-34217153	10.13.0.0/24	available	CREATE VPN CONNECTION		i
▼ 2	VPC: vpc-4e316e2a	172.31.0.0/16	available	CREATE VPN CONNECTION		i
	Route Table: rtb-a2cbc1c6			<input checked="" type="checkbox"/> Propagate Connection		
	Subnet: subnet-b4fab7d0	172.31.16.0/20	available			
	Subnet: subnet-058d2d5d	172.31.0.0/20	available			
	Subnet: subnet-52c2a724	172.31.32.0/20	available			
▶ 3	VPC: vpc-1616e571	10.0.0.0/16	available	CREATE VPN CONNECTION		i
4	VPC: vpc-ba89dddd	10.30.0.0/24	available	CREATE VPN CONNECTION		i
5	VPC: vpc-eeb56388	192.168.12.0/24	available	CREATE VPN CONNECTION		i

The VPC table on the SonicOS **AWS VPN** page reflects the VPC information that is available on the AWS Console under the VPC Dashboard.

The administrator can browse VPCs from one or more AWS Regions and create VPNs between the firewall and the subnets on each of those VPCs. The creation of firewall VPN and Route Policies, VPN Tunnels and associated Address Objects along with the necessary gateways and propagating the connections on AWS are all done automatically when the administrator clicks the button to establish a connection.

## To create a new VPN connection:

- 1 Navigate to the **MANAGE | Connectivity | VPN > AWS VPN** page in SonicOS.
- 2 Click the **Create VPN Connection** button in the row for the VPC you wish to connect to the firewall.
- 3 In the **New VPN Connection** dialog, verify that the **IP Address** field contains the public IP address of the firewall, or change it as needed.

If the firewall is behind a router or some other proxy, NAT rules should be put in place to ensure VPN traffic initiated from the AWS side is able to be routed back to the firewall.

- 4 If the firewall detects that route propagation is disabled for one or more route tables within a VPC, the dialog will include the **Propagate connection to all existing subnets in the VPC** checkbox. Select it unless you prefer to propagate the connection only to specific subnets (see [Step 6](#)).
- 5 Click **OK**.

A series of processes on both the firewall and AWS configure the VPN connection between them. You can click the *Information* 'i' button in the table row for details about the VPN connection. Use the *Refresh* button on the **AWS VPN** page to reload the data in the table and on the associated dialogs.

- 6 After the VPN Connection is established, expand the row on the **AWS VPN** page to display all of the subnets in that VPC, organized by route table. Select the **Propagate Connection** checkbox for each route table (unless you chose to enable propagation for all route tables in [Step 4](#)) and the associated subnets.

### To delete a VPN connection:

- 1 On the **MANAGE | Connectivity | VPN > AWS VPN** page, click the **Delete VPN Connection** button in the related table row.
- 2 Click **YES** in the confirmation dialog.

Deletion removes the associated VPN and Route Policies, and the Tunnel interfaces on the firewall. On AWS, it removes the Customer Gateway only if it is not being used elsewhere (perhaps on other VPN Connections from the same firewall, but to other VPCs). It does not delete the VPN Gateway or change the Route Propagation settings.

## CFS Blocking of Individual Videos

Starting in SonicOS 6.5.1.0, SonicWall Content Filtering Service (CFS) can filter and block individual YouTube videos. Previously, CFS could only allow or block *all* YouTube videos.

CFS inspects the site domain for each HTTP connection, and if the domain matches *youtube.com*, it extracts the video information from the query string, then reconstructs a new URI and sends a rating request for it to the CFS server. The reconstructed URI looks like this: **www.youtube.com/watch/v=-uWymC73jOY**

This feature is supported when using the SonicWall public CFS server, but not when using a local CFS server. This is due to a conflict with the blacklist/whitelist feature in the local CFS server.

This feature only works if the SonicWall CFS server already has a rating for the specific video identified in the “v=” parameter of the URI.

No SonicOS configuration is required.

## Capture ATP Friendly Filename Display

In SonicOS 6.5.1.0, SonicWall Capture Advanced Threat Protection logs the friendly filename of scanned files for the following non-HTTP protocols:

- SMTP
- IMAP
- POP3
- NetBIOS
- FTP

With this feature, system administrators can easily identify the files being scanned by Capture ATP and their status. Previously, (*unknown*) was displayed for filenames of these protocol types in the Capture > Status table, and log messages referred to *a file*.

Limitations:

- Friendly filenames up to a maximum of 256 characters are supported.
- This feature cannot parse filename information for TCP protocol streams.
- This feature cannot parse a filename if it is not part of single network packet.

No SonicOS configuration is required.

## DHCPv6 Relay

SonicOS 6.5.1.0 supports DHCPv6 Relay. A DHCP relay agent is a node that acts as an intermediary to deliver DHCP messages between clients and servers, and is on the same link as the client. A *DHCPv6* relay agent is used to relay messages between the client and the server when they are not on the same IPv6 link.

In SonicOS 6.5.1.0, supported destination addresses can be global addresses or link-local addresses, but not multicast addresses. DHCPv6 relay can be enabled on both physical and virtual interfaces. You can configure it from the **MANAGE | System Setup | Network > IP Helper** page.

**To configure DHCPv6 relay:**

- 1 Navigate to the **MANAGE | System Setup | Network > IP Helper** page.
- 2 In the **Relay Protocols** section, click **ADD**.
- 3 In the **Add IP Helper Application** dialog, configure the protocol **Name**, **Port 1**, **Port 2**, and **Timeout** fields.

- 4 For **Mode**, select **Broadcast**.
- 5 Select the **Enable Application** checkbox and **Allow Source IP translation** checkbox.
- 6 Click **OK**.
- 7 In the **Policies** section, click **ADD**.
- 8 In the **Add IP Helper Policy** dialog, select **DHCPv6** from the **Protocol** drop-down list.
- 9 Select the desired interface from the **From** drop-down list.
- 10 In the **To** field, type in the destination IPv6 address.
- 11 In the **Egress Interface** drop-down, do one of the following:
  - If the destination in the **To** field is a global address, there is no need to select an egress interface.
  - If the destination in the **To** field is a link-local address, select an egress interface.

- 12 Click **OK**.

A new DHCP lease will appear in the **DHCPv6 Relay Leases** section of the page when the client gets a new IP address from the server.

## DPI-SSH Blocking of SSH Port Forwarding

SSH makes it possible to tunnel other applications through SSH by using port forwarding. Port forwarding allows local or remote computers (for example, computers on the internet) to connect to a specific computer or service within a private local-area network (LAN). Port forwarding translates the address and/or port number of a packet to a new destination address and forwards it to that destination according to the routing rules. Since these packets have new destination and port numbers, they can bypass the firewall security policies.

To prevent circumvention of the application-based security policies on the SonicWall firewall, SonicOS 6.5.1.0 supports blocking of the port forwarding feature for Local and Remote port forwarding.

- Local port forwarding allows a computer on the local network to connect to another server, which might be an external server.

*Dynamic* port forwarding allows you to configure one local port for tunneling data to all remote destinations. This can be considered as a special case of Local port forwarding.

- Remote port forwarding allows a remote host to connect to an internal server.

You can enable this feature by selecting the **Block Port Forwarding** checkbox and enabling either or both Local Port Forwarding and Remote Port Forwarding from the **MANAGE | Security Configuration | Decryption Services > DPI-SSH** page in SonicOS.

DPI-SSH must be enabled for blocking of SSH port forwarding to work. DPI-SSH decrypts incoming SSH packets and inspects the commands. If any local or remote port forwarding requests are made when the blocking feature is enabled, SonicOS will block those requests and reset the connection.

SSH is a secure channel that supports shell, file transfer, port forwarding, and other services. Specific clients and servers are supported.

DPI-SSH port forwarding supports the following clients:

- SSH client for Cygwin
- Putty
- SecureCRT
- SSH on Ubuntu
- SSH on CentOS

DPI-SSH port forwarding supports the following servers:

- SSH server on Fedora
- SSH server on Ubuntu

SSH port forwarding supports both:

- Route mode
- Wire mode – only supported in Secure Mode

SSH port forwarding supports a maximum of 1000 connections, matching the maximum supported by DPI-SSH.

# FQDN Address Objects for NAT

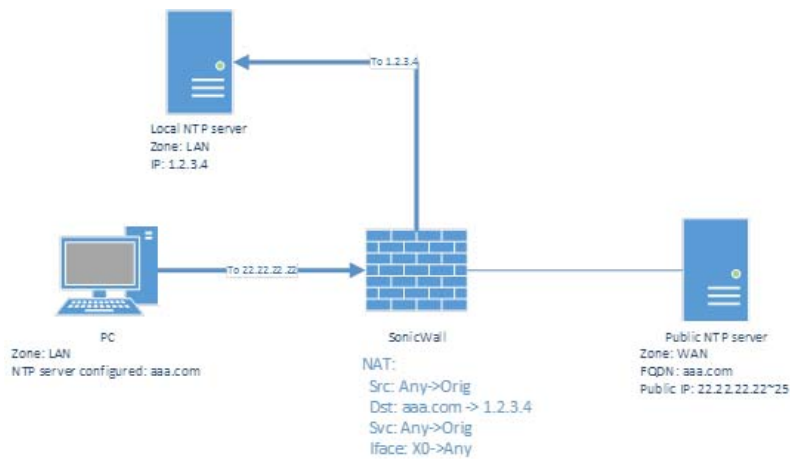
SonicOS 6.5.1.0 supports NAT policies using FQDN Address Objects for the original source/destination.

Use cases include:

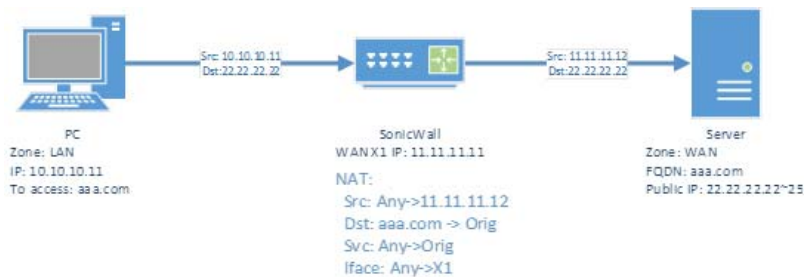
- Specifying public IP addresses with FQDN to a local server



- Specifying a public server with FQDN for consistency across replacement with a server that has a known IP address



- Routing traffic from/to a FQDN to have a source IP address other than the outbound interface IP.



The following functionality is supported:

- The original source/destination can be a pure FQDN or an address group with FQDN(s) and other IPv4 or IPv6 addresses, depending on the IP version of the NAT policy. A new FQDN address object can be directly created from the **MANAGE | Policies | Rules > NAT Policies** page.  
FQDN is not supported for the translated source/destination.
- IP Version options are provided for a NAT policy only if the version is ambiguous based on settings for original/translated source/destination fields. Either IPv4 or IPv6 must be selected.
- Mousing over an FQDN object of a NAT policy displays the IP addresses in the same IP version as the NAT policy.
- When NAT translation is performed, only the IP addresses in the NAT's IP version are considered.

- The Advanced page is disabled if FQDN is used in either or both the original source/destination fields. If probing is enabled and/or the NAT method is configured to a non-default value such as Sticky IP, neither of original source/destination address objects can be modified to contain an FQDN.
- FQDN based NAT policies are supported in High Availability configurations.

## FQDN Over TCP DNS

SonicOS 6.5.1.0 provides a new **Enable DNS host name lookup over TCP for FQDN** option on the **MANAGE | System Setup | Network > DNS** page.

By default, DNS queries are sent over UDP. The DNS response can include a Truncated flag if the response length exceeds the maximum allowed by UDP.

When the **Enable DNS host name lookup over TCP for FQDN** option is enabled and the Truncated flag is set in the DNS response, SonicOS sends an additional DNS query over TCP to determine the full DNS response for multiple IP addresses. When the option is disabled, DNS queries are sent over UDP and SonicOS only processes the IP addresses in the DNS response packet, although the Truncated flag is set in the response.

The DNS query times out after 1 second if no DNS response over TCP is received from the DNS server.

## Access Rule Enhancements

SonicOS 6.5.1.0 provides several feature enhancements to Access Rules:

- [Rules with Any zone](#)
- [Priority Options](#)
- [Rule Hit Counters](#)
- [Timestamps](#)

### Rules with Any zone

- Allows using *Any* for source and destination zones of an access rule during configurations.
- Maintains a single flat list for the configuration table.
- Adds source and destination zones as key dimensions to search in the lookup table.
- Prioritizes rules based on zones in the auto prioritize feature.
- No changes to how manual priority works.
- A single set of counters per unit for *save count*, *connection count* and similar counters.

### Priority Options

- New rules have the option of setting a priority for the rule in the table. The following three options are provided:
  - Auto Prioritize - SonicOS chooses the index according to an algorithm in which the most specific rules are given the highest priority.
  - Insert at the end - New policies are inserted at the end of the rule table.
  - Manual Priority - New policies are inserted at the index provided by the administrator.
- The SonicOS web management interface and CLI provide an option to choose the priority of the new rule.



## Rule Hit Counters

- Support per rule counters to keep track of rule hits.
- Counters are saved in the exported configuration settings to maintain persistence.
- Counters are displayed in the SonicOS web management interface and in the TSR.
- An option to clear counters is available in the SonicOS web management interface and CLI.

## Timestamps

- Support for the following timestamps per rule:
  - Creation Time – Time that the rule was created.
  - Last Updated – Time when the last edit was done.
  - Last Hit – Time when the most recent connection was classified by this rule.
- Timestamps are saved in the exported configuration settings to maintain persistence.
- Timestamps are displayed in the SonicOS web management interface and in the TSR.

## CFS Custom Header Insertion for HTTP Requests

In SonicOS 6.5.1.0, administrators can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

This feature requires the following:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.

*To configure a CFS custom header and enable custom header insertion:*

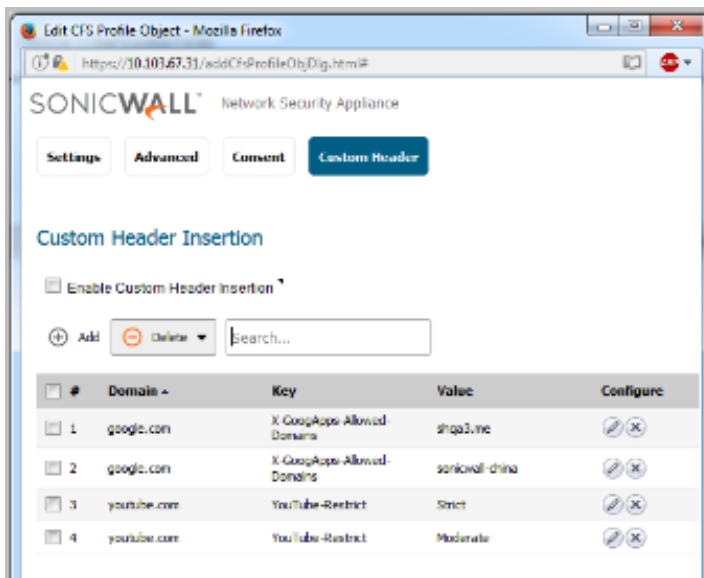
- 1 In the SonicOS web management interface, navigate to the **MANAGE | Policies | Objects > Content Filter Objects** page.
- 2 On the **CFS Profile Objects** screen, click **Add**.
- 3 In the **Add/Edit CFS Profile Object** dialog, click **Custom Header** to display the Custom Header Insertion options.
- 4 Select the **Enable Custom Header Insertion** checkbox.
- 5 Click **Add** to configure the **Domain**, **Key**, and **Value** for the custom header entry.

**Domain** is used to check whether the host in an HTTP request is matched to an entry during packet handling. **Key** and **Value** are used to generate the right header for the entry when building runtime data for custom header insertion.

The **Domain** can contain:

- Each domain name can contain up to 16 tokens separated by periods (.).
- The domain name cannot start or end with separators.
- Each token can contain up to 128 printable ASCII characters.
- Tokens in a domain name can only contain the characters: **0-9a-zA-z\$-\_'(),,**

- IPv4/IPv6 addresses can be defined as a domain name, e.g. “[2001:2002:2003::2005:2006]”.



- 6 Click **OK**.

## Enhanced HTTP/HTTPS Redirection with DP Offload

In SonicOS 6.5.1.0, this feature improves handling of HTTP/HTTPS redirection requests that occur when user authentication is required for users to get access through the firewall. HTTP/HTTPS requests received from sources that are not authenticated users are redirected to the firewall’s login page, which is served up by its built-in web server. This redirection happens if Single Sign-On (SSO) cannot identify the user, or if SSO is not in use.

If HTTP/HTTPS requests are received from sources from which users do not log in, and one or more such sources repeatedly try to open new connections, it can flood the firewall with connections that all need to be redirected. These could be non-user devices that are validly trying to get access, or it could be malicious code attempting a DOS attack. The effect that it has on the firewall is to cause high CPU load in the Control Plane (CP), which can impact web management access if it gets too high.

This feature improves efficiencies in both the web server and the HTTP/HTTPS redirection processes, and offloads most of the redirection processes to the Data Plane (DP) where the processing can be spread across multiple cores.

### **To enable the HTTP/HTTPS redirection feature:**

- 1 In the SonicOS web management interface, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox.

This checkbox is found in the **Edit Interface** dialog when editing a physical interface from the **Network > Interfaces** page, depending on the **Mode/IP Assignment** setting. You can also set this option in the **Add Interface** dialog when adding a **Virtual Interface** or a **WLAN Tunnel Interface**.

Enabling redirect from HTTP to HTTPS creates an access rule that also enables certain intermediate redirect pages to be fetched via HTTP even when the final page is served via HTTPS. This effectively allows redirection from HTTPS to HTTP for those intermediate tasks, but does not incur any security issues.

- 2 Click **OK**.

Elements of this feature can be controlled by *internal* User Authentication Settings options. This includes an option to globally enable/disable redirection processing in the DP, a flush option to clear the redirect files cache, and an option to specify the internal NAT port number used for the web server. Contact SonicWall Technical Support for information about internal settings.

# LLDP Support

SonicOS 6.5.1.0 support Link Layer Discovery Protocol (LLDP) on the following platforms:

- NSA 3600 / 4600 / 5600 / 6600
- SuperMassive 9200 / 9400 / 9600

LLDP is also supported when High Availability is enabled.

LLDP is used to discover neighboring devices and their capabilities. LLDP operates at Layer 2 and exchanges LLDP Protocol Data Units (LLDPDUs) between the neighbors containing a sequence of variable length information elements that include type-length-values (TLV). The information is stored in the SNMP MIBs. LLDP makes troubleshooting easier, especially in cases where the peers are not detected by ping or traceroute.

Three LLDP modes are supported in SonicOS 6.5.1.0:

- LLDP-receive (already supported in previous versions of SonicOS 6.5)
- LLDP-transmit
- LLDP-transmit-receive

LLDP profiles can be created on individual interfaces to choose the modes.

LLDP is supported with the following interface types and modes:

- L2 Interface – if the physical port is configured in L2 Mode
- L3 Interface – if the physical port is configured in L3 Mode
- Wire-Mode Interface – supported only for the physical interface, but not for VLAN interfaces
- L2 Bridge Interface – supported for the physical interface, but not for VLAN interfaces
- VLAN Sub-Interface – not supported
- LAG/LACP – supported on the primary port of the LAG

Each LLDP frame starts with three mandatory TLVs: Chassis ID, Port ID and TTL. The mandatory TLVs are followed by any number of optional TLVs. The LLDP frame ends with a mandatory End-of-frame TLV.

The **Mandatory TLVs** table describes the mandatory LLDP TLVs supported for both transmit and receive.

## Mandatory TLVs

TLV Name	TLV Type	Description	SonicOS Usage
Chassis ID TLV	1	Identifies the firewall chassis. Each firewall must have exactly one unique Chassis ID.	SonicOS sends the MAC address of the firewall in the Chassis ID field. The MAC address is same as the firewall serial number.
Port ID TLV	2	Identifies the port from which the LLDPDU is sent. The firewall uses the interface's ifname as the Port ID. For example, Port ID can be X1, X2, X3, ...	The Port ID subtype 5 (interface name) is used to identify the transmitting port.

### Mandatory TLVs

TLV Name	TLV Type	Description	SonicOS Usage
Time-to-live (TTL) TLV	3	Specifies how long (in seconds) LLDPDU information received from the peer is retained as valid in the local firewall (range is 0-65535). The value is a multiple of the LLDP Hold Time Multiplier. When the TTL value is 0, the information associated with the device is no longer valid and SonicOS removes that entry from the database.	Calculated internally
End of LLDPDU frame TLV	0	Indicates the end of the TLVs in the LLDP Ethernet frame.	

The **Optional TLVs** table describes the optional LLDP TLVs supported for both transmit and receive.

### Optional TLVs

TLV Name	TLV Type	Description	SonicOS Usage
Port Description	4	The port description in alpha-numeric format.	Advertises the values/string added in the comment section of network interface field.
System Name	5	The firewall name in alpha-numeric format.	Advertises the Firewall Name configured on the System Administration page.
System Description	6	The full name and version identification of the system's hardware type, software operating system, and networking software in alpha-numeric format.	Advertised as "Firewall" in this field.

## Optional TLVs

TLV Name	TLV Type	Description	SonicOS Usage
System Capabilities	7	<p>This field contains a bit-map of the capabilities that define primary functions of the system. Describes the deployment mode of the interface, as follows:</p> <ul style="list-style-type: none"><li>• An L3 interface is advertised with router (bit 6) capability and the “other” bit (bit 1).</li><li>• An L2 interface is advertised with MAC Bridge (bit 3) capability and the “other” bit (bit 1).</li><li>• A virtual wire interface is advertised with Repeater (bit 2) capability and the “other” bit (bit 1).</li></ul>	Advertises the features supported by the firewall and the enabled features.
Management Address	8	<p>One or more IP addresses used for the management of the device, as follows:</p> <ul style="list-style-type: none"><li>• IP address of the management (MGT) interface</li><li>• IPv4 and/or IPv6 address of the interfaceLoopback address</li><li>• User-defined address entered in the management address field; If no management IP address is provided, the default is the MAC address of the transmitting interface. The interface number of the specified management address is included. Also included is the OID of the hardware interface with the specified management address (if applicable). If more than one management address is specified, they are sent in the order they are specified, starting at the top of the list. A maximum of four Management Addresses are supported.</li></ul> <p>This is an optional parameter and can be left disabled.</p>	Advertises the management IP address of an interface if it is configured.

The LLDP options are configured on the **MANAGE | System Setup | Switching > L2 Discovery** page.

By default LLDP is globally enabled. You can toggle the **LLDP** switch to enable or disable LLDP transmit and receive globally.

LLDP profiles are created on the **LLDP Profile** screen of this page. SonicOS 6.5.1.0 supports a maximum of 20 LLDP Profiles.

#	Name	Admin Status	Msg Tx Hold	Msg Tx Interval	Reinit Delay	Tx Credit Max	Tx Fast Init	Class	Comments	Configure
1	Default LLDP Disabled	Disabled	4	30	2	5	4	Default		
2	Default LLDP RX	Rx Only	4	30	2	5	4	Default		
3	Default LLDP RX_TX	Tx & Rx	4	30	2	5	4	Default		
4	Default LLDP TX	Tx Only	4	30	2	5	4	Default		
5	LLDP RX Only - Max ReinitDelay	Rx Only	4	30	10	5	4	Custom		

You can add an LLDP Profile by clicking **Add**, or edit one by clicking the **Configure** button in its row.

**SONICWALL** Network Security Appliance  
 Name:   
 Admin Status:   
 Message Tx Hold:   
 Message Tx Interval (seconds):   
 Reinitializing Delay (seconds):   
 Maximum Tx Credit:   
 Tx Fast Init:   
 Comment:   
 Enable Port Description TLV  
 Enable System Name TLV  
 Enable System Description TLV  
 Enable System Capabilities TLV  
 Enable Management Address TLV  
 Ready

The fields of the LLDP Profile are described as follows:

- **Name** – Any string value given to the LLDP profile
- **Modes** – Disable, Receive-Only, Transmit-Only, Transmit-and-Receive
- **LLDP Protocol Parameters** – The following parameters are used for the LLDP transmit state-machine. Changing the values will affect the duration and the number of frames transmitted during each cycle.
  - **msgFastTx** – This variable defines the time interval in timer ticks between transmissions during fast transmission periods (i.e., txFast is non-zero). The default value of msgFastTx is 1; this value can be changed by to a value in the range 1 through 3600.
  - **msgTxHold** – This variable is used, as a multiplier of msgTxInterval, to determine the value of txTTL that is carried in LLDP frames transmitted by the LLDP agent. The default value of msgTxHold is 4; this value can be changed any value in the range 1 through 100.
  - **msgTxInterval** – This variable defines the time interval in timer ticks between transmissions during normal transmission periods (i.e., txFast is zero). The default value for msgTxInterval is 30 seconds; this value can be changed to any value in the range 1 through 3600.
  - **txFastInit** – This variable is used as the initial value for the txFast variable. This value determines the number of LLDPDUs that are transmitted during a fast transmission period. The default value of txFastInit is 4; this value can be changed to any value in the range 1 through 8.

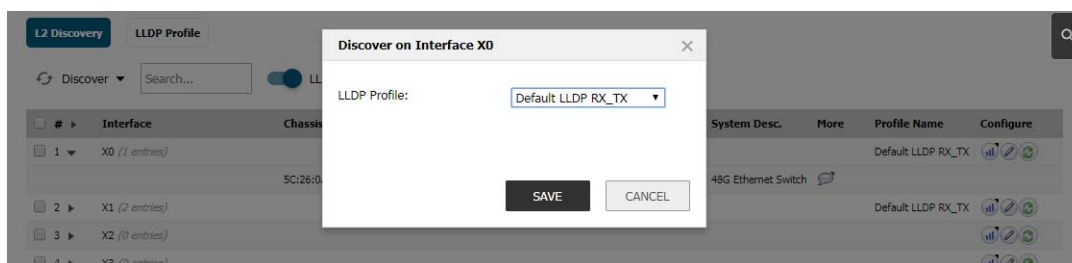
Parameter	Min Value	Max Value	Default Value
msgFastTx	1	3600	1
msgTxHold	1	100	4
msgTxInterval	1	3600	30
txFastInit	1	8	4

SonicOS provides four Default LLDP Profiles:

- **Mode Disabled** with all the default values of LLDP protocol parameters.
- **Mode Receive-Only** with all the default values of LLDP protocol parameters.
- **Mode Transmit-Only** with all the default values of LLDP protocol parameters.
- **Mode Transmit-and-Receive** with all the default values of LLDP protocol parameters.

**To associate an LLDP Profile with an L2 Discovery interface:**

- 1 Navigate to the **MANAGE | System Setup | Switching > L2 Discovery** page.
- 2 Click the **Configure** button in the row with the desired interface.
- 3 In the popup dialog, select the **LLDP Profile**.
- 4 Click **SAVE**.



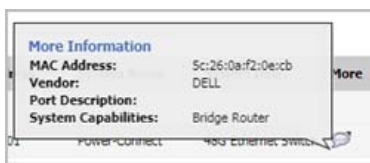
The following neighbor information is displayed per interface:

- **Interface** - Existing interface name
- **Chassis ID** - A string value mostly representing MAC address of the peer

- **Port ID** - A string value mostly port name or number
- **Management Address** - Either IP or MAC address
- **System Name** - A string value representing the name of the peer device
- **System Description** - A string value representing description of peer device

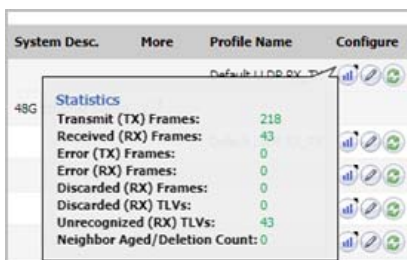
Additional peer information is displayed in a popup by hovering your mouse pointer over the **More** icon for the interface:

- **MAC Address** - A string value
- **Vendor** - The vendor name from the main menu
- **Port Description** - A string value from the Comments field for the interface on SonicWall firewalls
- **System Capabilities** - A string value representing the list of capabilities supported by the peer device
- **Enabled Capabilities** - A string value representing the list of capabilities enabled by the peer device



LLDP interface statistics are displayed in a popup by hovering your mouse pointer over the *statistics* icon under **Configure** for the interface:

- Transmit (TX) Frames
- Received (RX) Frames
- Error (RX) Frames
- Error (TX) Frames
- Discard (RX) Frames
- Unrecognized (RX) Frames
- Neighbor Aged/Deletion Count



LLDP only functions when the interface link is up. When link goes down or the mode is changed to Receive-Only or Disabled, a final LLDP shutdown LLDPDU is sent with:

- Chassis ID TLV
- Port ID TLV
- TTL TLV
- End of LLDPDU TLV

The statistics counters are reset after the link goes down.



## Per User Client Side UI Preferences Storage

SonicOS 6.5.1.0 provides the ability to separate the client-side UI preferences for each admin user, so each admin user can have their own UI settings consistent through every login. It maintains the settings for each admin even when other admin users log in through the same browser. This feature also offers options to store/retrieve client-side data shared across users or pages.

One common use case of this feature is restoring the last visited page for different logged-in admins.

Another common user case is restoring display options of certain table pages. For instance, display options such as IP version, view type and From/To zone in the Access Rules page can be restored for different admin users respectively. Only certain table pages can benefit from this feature, including all Object list pages, Access Rules page, and Connection Log page.

No configuration is required for this feature.

## Refactored SonicOS Web Interface Layout

The main page of the SonicOS web management interface is updated to use a flexbox with embedded iframes, and other features of modern browsers. This provides the foundation for new features such as Global Search in the UI. APIs relying on window.frames are not impacted and will continue to work as in previous releases.


This feature is supported in modern browsers:

- Chrome: 45+
- Firefox: 38+
- IE: 10+
- Edge: All
- Safari: 9+
- Opera: 32+

## Capture Threat Assessment Client Enhancements

SonicOS 6.5.1.0 adds new functionality to the existing Capture Threat Assessment feature:

- [Auto-Email the SFR File](#)
- [On-Demand SFR File Push to Capture Threat Assessment Server](#)
- [SFR File Data Content Additions](#)
- [New Capture Threat Assessment Page Location](#)

 **NOTE:** On the SOHO-W, bandwidth data information might not be available in the SFR file due to certain limitations in Flow Reporting on that platform.

This feature is only available when the device is registered and has an App Visualization license.

### Auto-Email the SFR File

This allows scheduled emailing of the SonicFlow Report File (SFR file) to an email user account. The SFR file is attached to the email. You can then use this to upload to MySonicWall and use the offline Capture Threat Assessment tool to generate a report. This option is configured on the **SFR Mailing** screen on the **MANAGE | AppFlow Settings** page.

The following email server settings are configured on this screen:

- **Send Report by E-mail** - checkbox to enable/disable sending of SFR email

- **SMTP Server Host Name** - host name or IP address of SMTP server to use
- **E-mail To** - email account to receive the SFR file
- **From E-mail** - email name to denote the sender
- **SMTP Port** - TCP port use by the SMTP server
- **Connection Security Method** - specifies whether to use secure (select protocol) or non-secure email
- **Enable SMTP Authentication** - specifies whether SMTP server requires authentication
- **SMTP User Name** - user name to use for SMTP authentication
- **SMTP User Password** - password to use for SMTP authentication
- **Enable POP Before SMTP** - specifies if POP authorization is needed for sending email
- **POP Server Address** - IP address of POP server
- **POP User Name** - user name to use for POP authorization
- **POP User Password** - password to use for POP authorization

At any point even if the above parameters are not yet saved, you can test the email by clicking on the **Test Email** button. An alert message pops up for either a successful or failed email transaction.

To schedule the email to be sent, click the **Edit Schedule** button. A dialog is displayed to edit the App Visualization Report Hours schedule object. Like any other schedule object, you can edit this to be one-time, recurring or mixed scheduling. However, this is a system created object so you cannot delete it.

## On-Demand SFR File Push to Capture Threat Assessment Server

This provides a one click operation to send the SFR file to the Capture Threat Assessment backend site for report generation. There is a report table that lists all the generated reports stored in the backend. You can click to download or to delete the report file.

## SFR File Data Content Additions

Two new sections are added to the SFR file report format:

- **Real-Time Monitor History Data** for applications, bandwidth, packets, connections, core usage that is useful to generate graphs and charts in the Capture Threat Assessment report
- **DPI-SSL Visibility Monitor Statistics** monitors mode statistics.

There are no configuration options for this.

## New Capture Threat Assessment Page Location

The **Capture Threat Assessment** page is moved from **AppFlow Settings > Flow Reporting** to a new page of its own under **Investigate | Reports | Capture Threat Assessment**.

## Increased SPI/DPI Connection Capacity

SonicOS 6.5.1.0 increases the maximum number of Stateful Packet Inspection (SPI) and Deep Packet Inspection (DPI) connections supported on NSA 2600-6600 and SuperMassive 9200-9600 platforms. You can enable SPI or DPI connections on the **Firewall Settings > Advanced** page in SonicOS.

The [SPI Previous vs New Maximum Connections](#) table shows the previous maximums and new target maximums for the number of connections supported on each platform with SPI enabled.

#### SPI Previous vs New Maximum Connections

Platform	Previous Maximum Connections	New Maximum Connections
NSA 2600	225,000	500,000
NSA 3600	325,000	750,000
NSA 4600	400,000	1,000,000
NSA 5600	750,000	1,500,000
NSA 6600	750,000	1,500,000
SM 9200	1,250,000	5,000,000
SM 9400	1,250,000	7,500,000
SM 9600	1,500,000	10,000,000

For appliances with DPI enabled, the [DPI Previous vs New Maximum Connections](#) table shows the previous maximums and new target maximums for the number of connections supported on each platform.

#### DPI Previous vs New Maximum Connections

Platform	Previous Maximum Connections	New Maximum Connections
NSA 2600	125,000	250,000
NSA 3600	175,000	375,000
NSA 4600	200,000	500,000
NSA 5600	500,000	1,000,000
NSA 6600	500,000	1,000,000
SM 9200	1,000,000	1,500,000
SM 9400	1,000,000	1,500,000
SM 9600	1,250,000	2,000,000

The maximum connection counts for the new hardware platforms (including NSA 2650) in the SonicOS 6.5.1.0 release are shown in the [New Hardware Connection Counts](#) table.

#### New Hardware Connection Counts

Platform	Max SPI Connections	Max DPI Connections
NSA 2650	1,000,000	500,000

*To select the connection mode (SPI or DPI) for the firewall:*

- 1 Navigate to the **MANAGE | Security Configuration | Firewall Settings > Advanced Settings** page.
- 2 In the **Connections** section, select one of the following radio buttons:
  - **Maximum SPI Connections (DPI services disabled)** — Enables Stateful Packet Inspection. This option allows the most simultaneous connections, but does not provide as much security as Deep Packet Inspection.
  - **Maximum DPI Connections (DPI services enabled)** — Enables Deep Packet Inspection. This is the default and recommended setting for most SonicWall network security appliance deployments.
  - **DPI Connections (DPI services enabled with additional performance optimizations)** — Enables Deep Packet Inspection with increased firewall DPI inspection throughput and fewer overall DPI connections. This option is intended for performance critical deployments.
- 3 Click **Accept**.

- 4 Restart the firewall. Any change to the Connection settings requires a restart for the changes to take effect.

## DPI vs DPI-SSL Dynamic Connection Sizing

For the products that support more than 250,000 DPI connections (NSA 2650 and higher), there is an option to adjust the number of desired DPI vs DPI-SSL connections. For every 125,000 DPI connections reduced, the number of available DPI-SSL connections increases by 750. For example:

- A reduction of 250,000 DPI connections results in an increase of 1,500 additional DPI-SSL connections.
- A reduction of 500,000 DPI connections results in an increase of 3,000 additional DPI-SSL connections.

### To configure a reduction in DPI connections:

- 1 Navigate to the **MANAGE | Security Configuration | Firewall Settings > Advanced** page.
- 2 On NSA and SuperMassive platforms, the **Dynamic Connection Sizing** section is displayed below **Connections**.

**i** **NOTE:** This setting is only available when one of the following options is selected under **Connections**:

- **Maximum DPI Connections (DPI services enabled)**
- **DPI Connections (DPI services enabled with additional performance optimizations)**

- 3 Using the **DPI Connections** drop-down list, adjust the desired number of DPI connections.  
For every 125,000 DPI connections reduced, the maximum number of DPI-SSL connections increases by 750.
- 4 Alternatively, adjust the desired number of DPI-SSL connections with the **DPI-SSL Connections** drop-down list.
- 5 Click **Accept**.

## DPI-SSL Scalability Through Extended Memory

An extended memory architecture in recent releases of SonicOS makes it possible for SonicOS to use memory beyond 4GB. In SonicOS 6.5.1.0, DPI-SSL data, including OpenSSL data, can reside in extended memory. This allows the number of DPI-SSL connections to scale significantly.

No configuration is required for this feature.

## DPI-SSL Support for Extra Ciphers

SonicOS 6.5.1.0 adds support for ECDSA related ciphers. This only affects the DPI-SSL client related function. For SSL web sites with ECDSA certificates, DPI-SSL will resign the ECDSA certificate.

No configuration is required for this feature.

## Active/Active Clustering on NSA Platforms

SonicOS 6.5.1.0 extends support for Active/Active Clustering to the following platforms:

- NSA 3600
- NSA 4600

In this mode, multiple firewalls are grouped together as cluster nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI and sharing the network load.

Each cluster node consists of two units acting as a Stateful HA pair. Active/Active Clustering provides Stateful Failover support in addition to load-sharing. Optionally, each cluster node can also consist of a single unit, in which case Stateful Failover and Active/Active DPI are not available.

**i** | **NOTE:** As with NSA 5600 and 6600, Active/Active Clustering is supported on the newly added platforms only with the purchase of a SonicOS Expanded License.

## SonicOS Global Search

SonicOS 6.5.1.0 provides a new global search button. Global search makes it easy for administrators to navigate to a desired feature. Results contain links to main pages which are part of menu items in the left-hand navigation pane.

Only static data can be searched. Dynamic data (like object names, policy details, etc.) are out of scope for this revision.

The SonicOS management interface displays the search icon in the upper right corner of the page. When the search icon is clicked, a slider text box opens. You can enter your search queries in the textbox. The slider can be closed by pressing the **ESC** key or by clicking the > button or by clicking in the area outside the slider.

The search results are shown by pressing the up-arrow key or by clicking in the area below the search textbox. The results are sorted by relevance. By default, only the top 10 results are displayed. If there are more results you can click **Show more results** to view them.

The following types of queries are supported:

- Single word queries, e.g. **ARP**
- Multiword queries, e.g. **Network Interface**
- Queries with wildcards, e.g. **Network Inter\***

A maximum of 50 characters are allowed in the search query string. Alphanumeric (A-Z a-z 0-9) and special character set (. \_ / \*) are allowed.

The search feature is not available on the classic/legacy management interface.

## Source MAC Overwrite for NAT

In SonicOS 6.5.1.0, this feature provides a way to replace the source MAC address of the packet with the MAC address specified in a NAT policy.

This feature is disabled by default, and can be enabled using an internal setting. Contact SonicWall Technical Support for information about internal settings.

## UUID for Rules and Objects

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is widely used by many network devices providers for multiple purposes.

In SonicOS 6.5.1.0, UUID is implemented to uniquely identify some entities on SonicWall Network Security Appliances. In this release, SonicOS UUIDs are automatically generated and bound to the following SonicOS entities:

- Address Object
- Service Object
- User Object
- Zone Object
- Schedule Object

- Access Rule
- NAT Policy
- Routing Policy

The SonicOS UUID is a system-generated, read-only internal value that cannot be modified by the administrator. It is automatically generated when an entity is created. UUID takes more memory than an ID and might not be available in all SonicWall firewall products. The availability of SonicOS UUID feature depends on the product matrix.

The UUID relies upon a combination of components to ensure uniqueness. SonicOS UUID contains:

- Global ID (aka, GID) per object type
- Network MAC address of the Network Security Appliances
- Object Type
- Version

UUID is bound to an entity and allows you to identify and track the history of an entity, for example, to see the referenced entities based on UUID.

- You can search for a partial or entire UUID from the SonicOS web management interface.
- If an object with UUID is referenced by another entity with a UUID, a clickable link allows you to jump to the referring entity.

For example, when an address object is referenced by another entity, hovering your mouse pointer over the **Comment** icon displays a popup with details and a link to the referenced entity.

- You can add a configuration option on the SonicOS web management interface to show UUID column and policy name. For user-friendly notation, a user-friendly **Name** field is added for access rule and NAT policies configured by an administrator. This name is optional, but must be unique if configured.

When importing configuration settings from one appliance to another, GID remains the same as in the imported preference file to retain the same configuration state. However, when viewing the UUID, the MAC address from the imported settings is replaced with the MAC address of the current running network appliance.

## UX/UI Improvements for Content Pages

Two pages in the SonicOS 6.5.1.0 web management interface are updated for an improved user experience.

- The **CFS Policies** screen on the **MANAGE | Security Services | Content Filter** page in SonicOS 6.5.0.x is moved to its own page in SonicOS 6.5.1.0, located at **MANAGE | Policies | Rules > Content Filter Policies**.
- The **MANAGE | Logs & Reporting | RF Monitor** page in SonicOS 6.5.0.x is moved in SonicOS 6.5.1.0 to **MONITOR | Appliance Health | RF Monitor**.

## WAN DDOS Protection Performance Enhancement

SonicOS 6.5.1.0 improves WAN DDOS Protection performance and makes more efficient use of the Allow List. The Allow List was previously populated with the destination IP of any packet ingressing a LAN/DMZ interface, but is now populated only when a packet from a non-WAN source zone egresses a WAN interface.

A new **Always allow VPN Negotiation traffic** checkbox is added, which is disabled by default. When enabled, a VPN can be negotiated even when the appliance is under a non-TCP DDOS attack.

WAN DDOS Protection provides protection against non-TCP DDOS attacks and so should be used in combination with SYN-Flood Protection if TCP SYN-flood attacks are a concern. This feature is not intended to protect a well-known server of non-TCP services on the internet (such as a central DNS server), but is intended to protect LAN and DMZ networks for which the majority of non-TCP traffic is initiated from LAN/DMZ side, possibly in combination with limited WAN initiated traffic.

WAN DDOS Protection is configured on the **MANAGE | Security Configuration | Firewall Settings > Flood Protection** page.

## Resolved Issues

This section provides a list of resolved issues in this release.

### Networking

Resolved issue	Issue ID
Traffic cannot pass through a VLAN trunking interface because all incoming ARP requests are dropped. Occurs after removing the VLAN trunking interface from an LACP LAG.	191702

### Switching

Resolved issue	Issue ID
Traffic fails through L2 LAG. Occurs after upgrading from SonicOS 6.2.7 or 6.2.9 to 6.5.0.0 and then shutting down the aggregator port from the SonicOS management interface.	193305

### User Interface

Resolved issue	Issue ID
SonicOS does not save after editing a URL, and the edit pop up cannot be closed. Occurs when adding the URL in user Authentication Bypass, then selecting the URL to edit and then clicking OK or Cancel.	194611

## Known Issues

This section provides a list of known issues in this release.

### 3G/4G

Known issue	Issue ID
Editing a 4G profile displays a secondary profile pop-up and additional errors. Occurs when editing a 4G profile (changing connect type, enabling data limit) and a pop-up is displayed that a secondary profile is being created. When accepted, another error is displayed "Error:Ordered list of profiles to use: Preferred profile already exists." <b>Workaround:</b> Click the <b>Cancel</b> button to save the edits to the profile.	196813

### Access Points

Known issue	Issue ID
SonicPoint dynamic VLAN ID assignment does not work. Occurs when configuring a SonicPoint object, selecting the <b>Enable Dynamic Vlan ID Assignment for Radio 0</b> checkbox and including a VLAN ID higher than 256 in the <b>Edit Dynamic Vlan ID</b> dialog, then trying to connect from a wireless client.	198457

## CLI

Known issue	Issue ID
<p>CLI help does not show how to create a new address object although command parsing remains intact.</p> <p>Occurs when typing <code>address-object ipv4 ?</code>, which previously came back with something like <code>config(C0EAE4ACxxxx)# address-object ipv4 &lt;NAME&gt;</code>, where <code>&lt;NAME&gt;</code> was expanded to show the host/network/range address object name, but now returns nothing. Tab completion would return the names of custom address objects to select, but now returns only the uuid if no custom address objects exist and returns names of existing objects if they exist, but provides no indicator of how to add a new address object.</p>	196421

## DPI-SSH

Known issue	Issue ID
<p>A dialog with the message "User Object/Group Included &amp; Excluded can not be the same" is displayed on the DPI-SSH page.</p> <p>Occurs when navigating to the DPI-SSH page.</p>	196702

## DPI-SSL

Known issue	Issue ID
<p>Block of attachment and append message actions do not work with SMTP over SSL.</p> <p>Occurs when <b>SSL Client Inspection</b> is enabled and the <b>Application Firewall</b> checkbox is selected on the <b>DPI-SSL/TLS Client</b> page and an App Rule policy exists to block attachments and add text, and then an email message matching the policy is sent.</p>	198590
<p>The behavior for an HTTPS server is that the certificate is re-signed by authority cert selected in certificate drop-down list (Default is SonicWall DPISSL Certificate), which is not right.</p> <p>Occurs when <b>SSL Client Inspection</b> is enabled and you access an HTTPS website with a self-signed certificate from the LAN.</p>	198367
<p>Caches are not deleted when making configuration changes (reject or accept) to built-in common names.</p> <p>Occurs when <b>SSL Client Inspection</b> is enabled and you access a website from the LAN whose common-name is in the built-in list, like <code>https://www.sonicwall.com</code>. This creates the cache. Then click the reject icon to reject <code>.sonicwall.com</code>. The cache is not deleted and <code>sonicwall.com</code> is still excluded even though it has been rejected.</p>	198252
<p><b>Skip CFS Category-based Exclusion</b> does not work correctly.</p> <p>Occurs when a common name like <code>bankofamerica.com</code> is added on the <b>DPI-SSL/TLS Client</b> page with the <b>Skip CFS Category-based Exclusion</b> option selected, category "20. Online Banking" is excluded, and then a LAN side PC attempts to access <code>bankofamerica.com</code> and it is excluded from inspection.</p>	198185
<p>HTTPS servers which use certificate with V1 version cannot be opened, and the browser displays the error message "The site can't provide a secure connection. 10.8.158.200 doesn't adhere to security standards. ERR_SSL_SERVER_CERT_BAD_FORMAT".</p> <p>Occurs when <b>SSL Client Inspection</b> is enabled and Chrome is used from the LAN side to access an HTTPS server with a V1 version certificate.</p>	198118
<p>CFS Category-based Inclusions/Exclusions does not exclude correctly.</p> <p>Occurs when <b>Enable SSL Client Inspection</b> is selected on the <b>DPI-SSL/TLS Client</b> page and category <i>29 Search Engines and Portals</i> is excluded on the <b>CFS Category-based Exclusions/Inclusions</b> screen, and then a LAN side PC accesses <code>https://www.baidu.com</code> and DPI-SSL still occurs.</p>	196892



## Networking

Known issue	Issue ID
The name query response is dropped after adding a NetBIOS policy. Occurs when adding a NetBIOS policy from the Network > IP Helper page.	198565
Traffic fails after disabling an L3 LAG; it is received at x0, but does not forward out from x1. Occurs when configure x1 with static ip address and set x3 as aggregate port, configure connected switch with portchannel, enable Stateful HA and virtual, send ping traffic from LAN side (x0) to internet through the LAG (traffic is reachable), and then disable link aggregation on interface x1 and do the same to the switch.	197952
HTTP/HTTPS Redirection with DataPlane offloading still uses ControlPlane for most processing. Occurs when a Firewall Access Rule exists, such as allow LAN-WAN HTTP trusted users, and then HTTP LAN to WAN traffic is passed.	197852
OSPF neighbor is stuck at <i>ExStart</i> state and cannot reach <i>Full</i> state. Occurs after Stateful HA failover with some traffic running.	197425
A VLAN cannot be deleted from a logical LAG interface (all members of a LAG) without dismantling the LAG. Occurs when the VLAN is deleted, but results in only being deleted from one member of the LAG.	197244
In a High Availability pair, the custom NAT policy name in the auto-added NAT policy does not match between primary and backup units. Occurs when configuring the X2 interfaces as WAN with static IP address.	196474
The WAN interface cannot get an IP address in PPTP mode. Occurs when changing the WAN interface from L2TP mode with static IP assignment to PPTP mode.	196020

## Security Services

Known issue	Issue ID
For CFS, the <b>OK</b> and <b>Cancel</b> buttons are not visible in the frame. Occurs when Adding/Editing CFS Profile Objects.	198339
Cannot activate GAV/IPS/CFS security service licenses on NSA. The <b>Security Service &gt; CFS</b> page displays “upgrade required”. Occurs when a CFS/GAV/IPS security service activation key is applied, then the <b>Manage service online</b> page displays GAV/IPS/CFS as licensed, but the <b>System &gt; Status</b> page shows them as still unlicensed.	198257

## SonicOS API

Known issue	Issue ID
Unable to log into API using CHAP authentication. Occurs when using a Perl script which uses a <i>curl</i> command to get ID and challenge.	194501
Unable to log into API with a non-default admin account. Occurs when using a user that is member of SonicWall Administrators.	194120

## SSL VPN

Known issue	Issue ID
The RDP connection via SSL VPN tunnel is disconnected. Occurs when modifying an Address Object.	197488

## Switching

Known issue	Issue ID
The L2 LAG fails to aggregate. Occurs when importing configuration settings from NSA 3600.	198374
The profile names for all interfaces are missing on the <b>Switching &gt; L2 Discovery</b> page. Occurs after importing configuration settings from NSA 3600.	198355
Modification of a link aggregation member port displays an error message. Occurs when using GMS to make the change, selecting the existing member port and then selecting a new member port.	198327

## System

Known issue	Issue ID
A SuperMassive 9600 cannot load firmware, but fails with not enough memory. Occurs when the appliance was running traffic for three days, then idle for one day before attempting to upgrade the firmware to a new build.	198293
A custom NAT policy has a duplicate name. Occurs when custom NAT policies exist on an NSA 3600 running SonicOS 6.5.0.1, then the settings are exported and then imported to an NSA running 6.5.1.0.	196703

## Users

Known issue	Issue ID
The password of a local user cannot be changed and displays the error message “Error: Incorrect Password” when trying to change it. Occurs when a local user is created with the <b>User must change password at next login</b> option set, the user is added to the SonicWall Administrators group, and then the user logs in and tries to change the password.	198760
The default partition policy changes, causing the partition feature to not work. Occurs when adding a remote-user partition policy from CLI.	197455

## VoIP

Known issue	Issue ID
The SIP-Invite message is not interpreted as an INVITE by Wireshark. Occurs when ALG is configured for SIP/IPv6 in NAT section and SIP-IPv6 is transformed on WAN side.	197490

## VPN

Known issue	Issue ID
SonicOS fails to forward IPv6 Jumbo frames over Site to Site VPN. Occurs when the default X1 interface has MTU 1500 configured.	198407
SSH traffic through IPv6 VPN fails. Occurs when only enabling SSH on the VPN policy, but not enabling it on the interface.	197788

# System Compatibility

This section provides additional information about hardware and software compatibility with this release.

## Wireless 3G/4G Broadband Devices

SonicOS 6.5 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:

<https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240>

## GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.1.0 requires GMS 8.4 SP2 for management of firewalls using the new features in SonicOS 6.5.1.0. SonicWall GMS 8.4 supports management of all features in earlier SonicOS 6.5 releases.

## WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.5. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

## Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 45 and higher
- Firefox 38 and higher
- IE 10 and higher
- Edge (all versions)
- Opera 32 and higher
- Safari 10 and higher running on non-Windows machines

**i** | **NOTE:** On Windows machines, Safari is not supported for SonicOS management.

**i** | **NOTE:** Mobile device browsers are not recommended for SonicWall appliance system administration.

## Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.

# Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.5 Upgrade Guide* available on the Support portal at <https://www.sonicwall.com/support/technical-documentation>.

## SonicWall Support

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

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 video tutorials
- Access MySonicWall
- 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>.

Copyright © 2018 SonicWall Inc. All rights reserved.




This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. 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>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>. Select the language based on your geographic location to see the EUPA that applies to your region.

## Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 2/6/18  
232-00xxxx-00 Rev 01