



High Availability on SonicWALL TZ Series

Document Scope

This document describes how to configure and manage the High Availability feature for SonicWALL TZ Series security appliances.

This document contains the following sections:

- [“High Availability Overview”](#) on page 1
- [“Configuring High Availability”](#) on page 4
- [“Applying Licenses to SonicWALL Security Appliances”](#) on page 15
- [“Verifying High Availability Status”](#) on page 17

High Availability Overview

This section provides an introduction to the High Availability feature. This section contains the following subsections:

- [“What is High Availability?”](#) on page 1
- [“Benefits of High Availability”](#) on page 2
- [“How Does High Availability Work?”](#) on page 2
- [“High Availability Terminology”](#) on page 3
- [“Supported Platforms”](#) on page 3

What is High Availability?

High Availability allows two identical SonicWALL security appliances running SonicOS Enhanced to be configured to provide a reliable, continuous connection to the public Internet. One SonicWALL device is configured as the Primary unit, and an identical SonicWALL device is configured as the Backup unit. In the event of the failure of the Primary SonicWALL, the Backup SonicWALL takes over to secure a reliable connection between the protected network and the Internet. Two appliances configured in this way are also known as a High Availability Pair (HA Pair).

High Availability provides a way to share SonicWALL licenses between two SonicWALL security appliances when one is acting as a high availability system for the other. To use this feature, you must register the SonicWALL appliances on MySonicWALL as Associated Products. Both appliances must be the same SonicWALL model.

Benefits of High Availability

High Availability provides the following benefits:

- **Increased network reliability** – In a High Availability configuration, the Backup appliance assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant SonicWALL security appliances. You do not need to purchase a second set of licenses for the Backup unit in a High Availability Pair.
- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA Pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability. By default, the Virtual MAC address is provided by the SonicWALL firmware and is different from the physical MAC address of either the Primary or Backup appliances.

How Does High Availability Work?

High Availability requires one SonicWALL device configured as the Primary SonicWALL, and an identical SonicWALL device configured as the Backup SonicWALL. During normal operation, the Primary SonicWALL is in an Active state and the Backup SonicWALL in an Idle state. If the Primary device loses connectivity, the Backup SonicWALL transitions to Active mode and assumes the role and configuration of Primary, including the interface IP addresses of the configured interfaces. After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWALL. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary SonicWALL loses power. The Primary and Backup SonicWALL devices are currently only capable of performing Active/Idle High Availability – Active/Active failover is not supported at present.

High Availability requires that PortShield is disabled on all interfaces of both the Primary and Backup appliances prior to configuring the HA Pair. Besides disabling PortShield, SonicWALL security appliance configuration is performed on only the Primary SonicWALL, with no need to perform any configuration on the Backup SonicWALL. The Backup SonicWALL maintains a real-time mirrored configuration of the Primary SonicWALL via an Ethernet link between the designated HA ports of the appliances. If the firmware configuration becomes corrupted on the Primary SonicWALL, the Backup SonicWALL automatically refreshes the Primary SonicWALL with the last-known-good copy of the configuration preferences.

High availability license synchronization allows sharing of the SonicOS Enhanced license, the Support subscription, and the security services licenses present on the Primary SonicWALL appliance with the associated Backup appliance. All security services you see on the **Security Services > Summary** screen are shareable, including Free Trial services. The only licenses that are not shareable are for consulting services, such as the SonicWALL GMS Preventive Maintenance Service. When a hardware failover occurs, the Backup appliance is licensed and ready to take over network security operations.

There are two types of synchronization for all configuration settings: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete synchronization is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

High Availability Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - Describes the actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

Supported Platforms

In SonicOS Enhanced 5.3, High Availability is currently available on the following SonicWALL TZ Series security appliances:

- SonicWALL TZ 210 / 210 Wireless
- SonicWALL TZ 200 / 200 Wireless

Use the interface shown in the following table when connecting the two SonicWALL security appliances in the HA Pair to each other.

Platform	Interface for High Availability
SonicWALL TZ 210 / 210 Wireless-N	X6
SonicWALL TZ 200 / 200 Wireless-N	X4

Configuring High Availability

This section describes how to associate two SonicWALL appliances as a High Availability Pair on MySonicWALL, and describes procedures for High Availability configuration on SonicOS Enhanced.

- “[Configuration Overview](#)” on page 4
- “[Configuring a High Availability Pair on MySonicWALL](#)” on page 4
- “[Configuring High Availability on SonicOS](#)” on page 8

Configuration Overview

You can associate two SonicWALL security appliances as HA Primary and HA Secondary on MySonicWALL. Note that the Backup appliance of your High Availability Pair is referred to as the HA Secondary unit on MySonicWALL. After the appliances are associated as an HA Pair, they can share licenses.

You need only purchase a single set of licenses for the HA Primary appliance. The licenses are shared with the Backup unit. This includes the SonicOS Enhanced license, the Support subscription, and the security services licenses. The only licenses that are not shareable are for consulting services, such as the SonicWALL GMS Preventive Maintenance Service.

It is not required that the Primary and Backup appliances have the same security services enabled. The security services settings will be automatically updated as part of the initial synchronization of settings. License synchronization is used so that the Backup appliance can maintain the same level of network protection provided before the failover.

In addition to associating the appliances on MySonicWALL, you must use the SonicOS management interface to configure your two appliances as a High Availability Pair in Active/Idle mode.

**Note**

Even if you first register your appliances on MySonicWALL, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances. See “[Applying Licenses to SonicWALL Security Appliances](#)” on page 15 for both procedures.

See the following sections to perform each task in the High Availability configuration:

- “[Configuring a High Availability Pair on MySonicWALL](#)” on page 4
- “[Configuring High Availability on SonicOS](#)” on page 8

Configuring a High Availability Pair on MySonicWALL

You can associate a SonicWALL security appliance with another appliance of the same model when you first register it, or at any time after both appliances are already registered on MySonicWALL. The procedure for associating two registered appliances is provided in this document. See the *SonicOS Enhanced 5.3 Administrator's Guide* for complete information, available online at:

<<http://www.sonicwall.com/us/Support.html>>

**Note**

You can remove an appliance from an association at any time.

See the following sections:

- “Associating Two Appliances on MySonicWALL” on page 5
- “Removing an HA Association in MySonicWALL” on page 5
- “Replacing One Appliance in a High Availability Pair” on page 6

Associating Two Appliances on MySonicWALL

This section describes how to associate two SonicWALL security appliances on MySonicWALL. This association is required when using a High Availability deployment.



Note This procedure is for appliances that are already registered.

To associate two appliances as a High Availability Pair on MySonicWALL, perform the following steps:

- Step 1** Login to your MySonicWALL account at <<https://www.mysonicwall.com/>>.
- Step 2** In the left navigation pane, click **My Products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance that you want to use as the Parent, or Primary, unit. Click the product **name** or **serial number**.
- Step 4** On the **Service Management** page, scroll down to the **Associated Products** section.
- Step 5** Under **Associated Products**, click **HF Secondary**.
- Step 6** On the **My Product - Associated Products** page, in the **Serial Number** field, type the **serial number** of the Secondary (Backup) appliance.
- Step 7** In the **Friendly Name** field, type a descriptive name of up to 30 characters for the Secondary appliance.
- Step 8** From the **Product Group** drop-down list, select the Product Group for the Secondary appliance. The Product Group is a group of appliances that can be managed by users belonging to the assigned User Group. Product Groups and User Groups can be configured on MySonicWALL.
- Step 9** Click **Register**.

Removing an HA Association in MySonicWALL

You can remove the association between two SonicWALL security appliances on MySonicWALL at any time. You might need to remove an existing HA association if you replace an appliance or reconfigure your network. For example, if one of your SonicWALL security appliances fails, you will need to replace it. Or, you might need to switch the HA Primary appliance with the Backup, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association and then create a new association that uses a new appliance or changes the parent-child relationship of the two units.

See also “Replacing One Appliance in a High Availability Pair” on page 6.

To remove the association between two registered SonicWALL security appliances, perform the following steps:

- Step 1** Login to your MySonicWALL account at <<https://www.mysonicwall.com/>>.
- Step 2** In the left navigation pane, click **My Products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the Secondary appliance from which you want to remove associations. Click the product **name** or **serial number**.

Step 4 On the **Service Management** page, scroll down to the **Parent Product** section, just above the **Associated Products** section.

Step 5 In the **HF Primary** row, click **Remove** to remove the association.

Figure 1 Removing an Association (1)

PARENT PRODUCT			
Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

Step 6 Wait for the page to reload, scroll down, and then click **Remove** again.

Figure 2 Removing an Association (2)

Are you sure you want to remove this Parent product Association? If yes then click 'Remove' again.

PARENT PRODUCT			
Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

Replacing One Appliance in a High Availability Pair

If your SonicWALL security appliance has a hardware failure while still under warranty, SonicWALL will replace it. In this case, you need to remove the HA association containing the failed appliance in MySonicWALL, and add a new HA association that includes the replacement. If you contact SonicWALL Technical Support to arrange the replacement (known as an RMA), Support will often take care of this for you.

After replacing the failed appliance in your equipment rack with the new unit, you can update MySonicWALL and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing a failed HA Secondary unit. Both procedures are provided in the following sections:

- [Replacing an HA Primary Unit](#)
- [Replacing an HA Secondary Unit](#)

Replacing an HA Primary Unit

In the case where your HA Primary unit fails, the most efficient replacement procedure is to promote the original Backup unit to Primary, and add the new replacement unit as the new Backup. This allows you to maintain the configuration settings that are already in place on the original Backup unit.

To replace an HA Primary unit, perform the following steps:

-
- Step 1** Connect the replacement SonicWALL appliance to your network and perform basic system setup and registration.
 - Step 2** In the SonicOS management interface of the remaining SonicWALL security appliance (the original Backup unit), on the **High Availability > Settings** page, clear the **Enable High Availability** checkbox to disable HA.
 - Step 3** Clear the **Backup SonicWALL Serial Number** text box.
 - Step 4** Select the **Enable High Availability** checkbox.

The old Backup unit now becomes the Primary unit. Its serial number is automatically displayed in the **Primary SonicWALL Serial Number** text box.

- Step 5** Type the serial number for the replacement unit into the **Backup SonicWALL Serial Number** text box.
- Step 6** Click **Synchronize Settings**.
- Step 7** On MySonicWALL, remove the old HA association.
See [“Removing an HA Association in MySonicWALL” on page 5](#).
- Step 8** On MySonicWALL, create an HA association with the new Primary (original Backup) unit as the HA Primary, and the replacement unit as the HA Secondary.
See [“Associating Two Appliances on MySonicWALL” on page 5](#).
- Step 9** Contact SonicWALL Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.

This step is required when the HA Primary unit has failed, because the licenses are linked to the Primary unit in an HA Pair.

Replacing an HA Secondary Unit

To replace an HA Secondary unit, perform the following steps:

-
- Step 1** Connect the replacement SonicWALL appliance to your network and perform basic system setup and registration.
 - Step 2** In the SonicOS management interface of the remaining SonicWALL security appliance (the Primary unit), on the **High Availability > Settings** page, clear the **Enable High Availability** checkbox to disable HA.
 - Step 3** Clear the **Backup SonicWALL Serial Number** text box.
 - Step 4** Select the **Enable High Availability** checkbox.
 - Step 5** Type the serial number for the replacement unit into the **Backup SonicWALL Serial Number** text box.
 - Step 6** Click **Synchronize Settings**.
 - Step 7** On MySonicWALL, remove the old HA association.
See [“Removing an HA Association in MySonicWALL” on page 5](#).
 - Step 8** On MySonicWALL, create an HA association with the original HA Primary, using the replacement unit as the HA Secondary.
See [“Associating Two Appliances on MySonicWALL” on page 5](#).

Configuring High Availability on SonicOS

To configure High Availability, you must configure High Availability in the SonicOS management interface using the two SonicWALL appliances associated on MySonicWALL. For information about associating two appliances, see [“Configuring a High Availability Pair on MySonicWALL”](#) on page 4.

The High Availability feature of the SonicWALL TZ Series appliance can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances.

You can disable PortShield either by using the **PortShield Wizard**, or manually from the **Network > PortShield Groups** page.

Refer to the following sections:

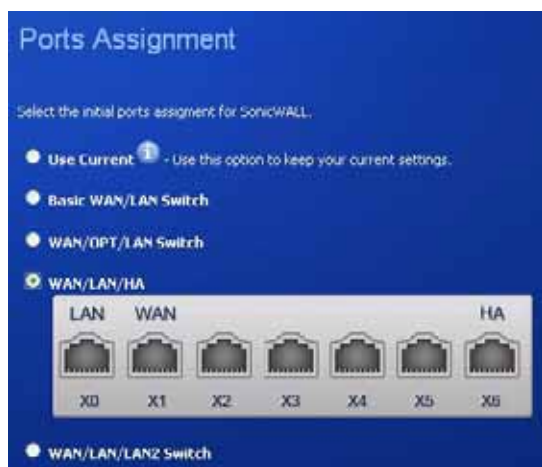
- [“Disabling PortShield with the PortShield Wizard”](#) on page 8
- [“Disabling PortShield Manually”](#) on page 9
- [“Configuring High Availability > Settings”](#) on page 11
- [“Configuring High Availability > Advanced Settings”](#) on page 11
- [“Configuring High Availability > Monitoring”](#) on page 13

Disabling PortShield with the PortShield Wizard

The High Availability feature of the SonicWALL TZ Series appliance can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address.

To use the PortShield Wizard to disable PortShield on each SonicWALL, perform the following steps:

-
- Step 1** On one appliance of the planned HA Pair, click the **Wizards** button at the top right of the management interface.
- Step 2** In the **Welcome** screen, select **PortShield Interface Wizard**, and then click **Next**.
- Step 3** In the **Ports Assignment** screen, select **WAN/LAN/HA**, and then click **Next**.



- Step 4** In the **SonicWALL Configuration Summary** screen, click **Apply**.
- Step 5** In the **PortShield Wizard Complete** screen, click **Close**.
- Step 6** Log into the management interface of the other appliance in the HA Pair and repeat this procedure.

Disabling PortShield Manually

The High Availability feature of the SonicWALL TZ Series appliance can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address.

To manually disable PortShield on each SonicWALL, perform the following steps:

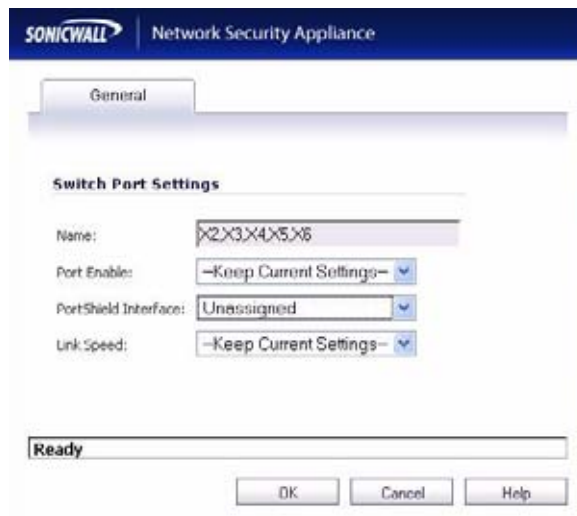
- Step 1** On one appliance of the planned HA Pair, navigate to the **Network > PortShield Groups** page.

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	LAN	Auto Negotiate	100 Mbps - Half duplex	Default LAN	
X1	WAN	Auto Negotiate	No link	Default WAN	
X2	X0	Auto Negotiate	No link		
X3	X0	Auto Negotiate	No link		
X4	X0	Auto Negotiate	No link		
X5	X0	Auto Negotiate	No link		
X6	X0	Auto Negotiate	100 Mbps - Full duplex		

- Step 2** Click the **Select All** link at the top of the page.

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	LAN	Auto Negotiate	100 Mbps - Full duplex	Default LAN	
X1	WAN	Auto Negotiate	No link	Default WAN	
X2	X0	Auto Negotiate	No link		
X3	X0	Auto Negotiate	No link		
X4	X0	Auto Negotiate	No link		
X5	X0	Auto Negotiate	No link		
X6	X0	Auto Negotiate	100 Mbps - Full duplex		

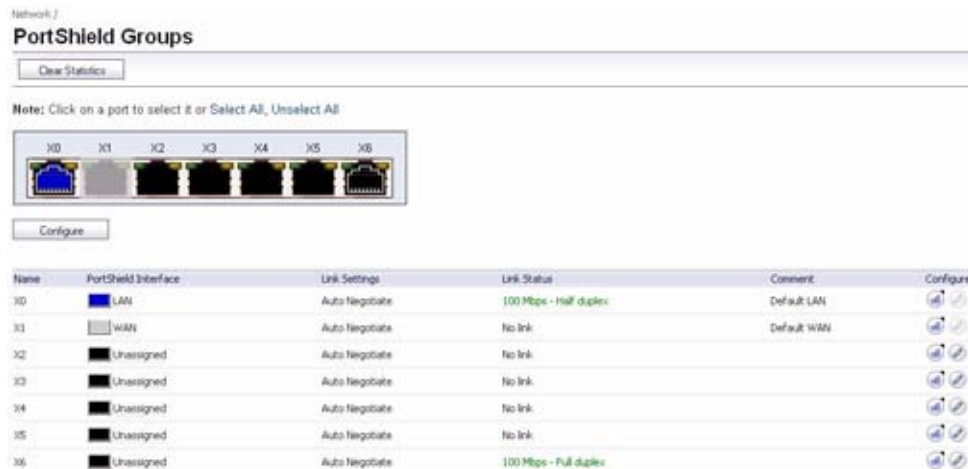
Step 3 Click the **Configure** button.



Step 4 In the **Switch Port Settings** dialog box, select **Unassigned** in the **PortShield Interface** drop-down list.

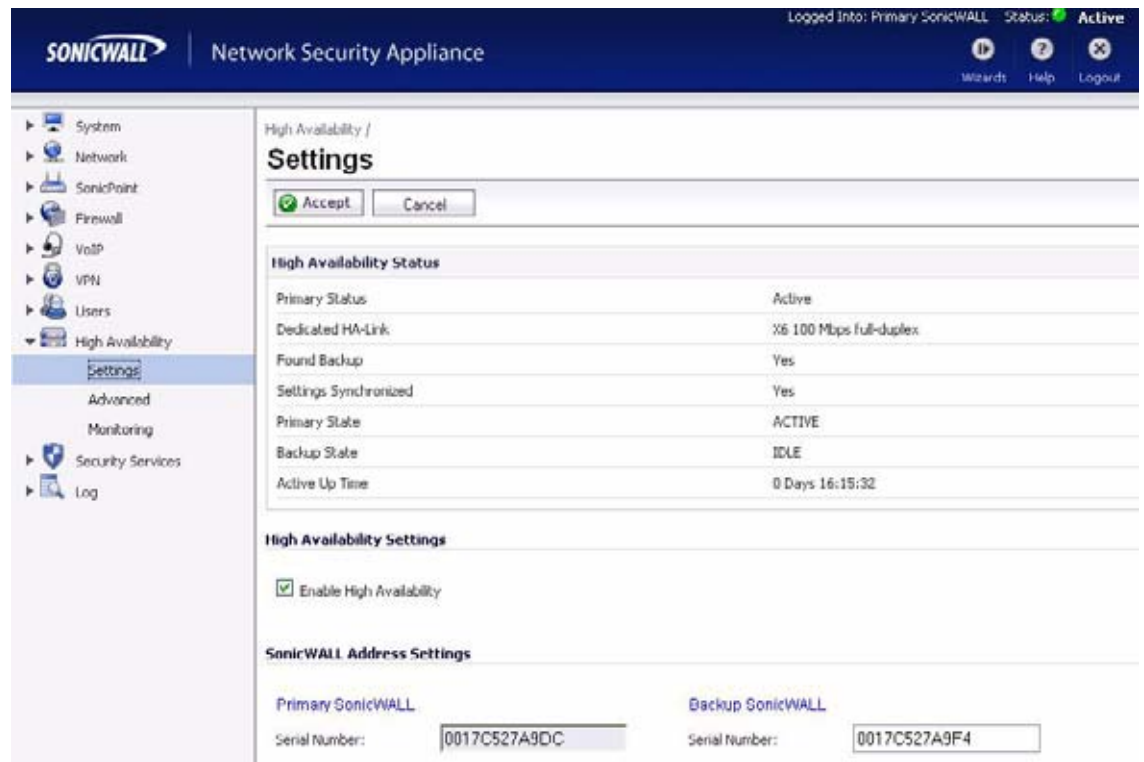
Step 5 Click **OK**.

The **Network > PortShield Groups** page displays the interfaces as unassigned.



Configuring High Availability > Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary unit and then are automatically synchronized to the Backup.



To configure the settings on the **High Availability > Settings** page:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.
- Step 2** In the left navigation pane, navigate to **High Availability > Settings**.
- Step 3** In the **High Availability > Settings** screen, select the **Enable High Availability** checkbox.
- Step 4** Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance.
You can find the serial number on the back of the SonicWALL security appliance, or in the **System > Status** screen of the Backup unit. The serial number for the Primary SonicWALL is automatically populated.
- Step 5** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit, and the Idle unit will reboot.

Configuring High Availability > Advanced Settings

The configuration tasks on the **High Availability > Advanced** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To configure the settings on the **High Availability > Advanced** page, perform the following steps:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.

Step 2 In the left navigation pane, navigate to **High Availability > Advanced**.



Step 3 In the **High Availability > Advanced** screen, to configure the High Availability Pair so that the Primary unit takes back the Primary role once it restarts after a failure, select **Enable Preempt Mode**.

Step 4 To back up the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.

Step 5 Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address.

Step 6 Optionally adjust the **Heartbeat Interval** to control how often the two units communicate. The default is 5000 milliseconds; the minimum supported value is 1000 milliseconds. You can use higher values if your SonicWALL handles a lot of network traffic.

Step 7 Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. The default is 5.

Step 8 Set the **Probe Interval** to the interval in seconds between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This is used in logical monitoring. SonicWALL recommends that you set the interval for at least 5 seconds. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability > Monitoring** screen. See [“Configuring High Availability > Monitoring” on page 13](#).

Step 9 Set the **Probe Count** to the number of consecutive probes before SonicOS Enhanced concludes that the network critical path is unavailable or the probe target is unreachable. This is used in logical monitoring. The default is 3, and the allowed range is 3 to 10.

Step 10 Set the **Election Delay Time** to the number of seconds allowed for internal processing between the two units in the High Availability Pair before one of them takes the Primary role. The default is 3 seconds.

Step 11 Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.

Step 12 You do not need to click **Synchronize Settings** at this time, because all settings will be automatically synchronized to the Idle unit when you click Accept after completing HA configuration. To synchronize all settings on the Active unit to the Idle unit immediately, click **Synchronize Settings**. The Idle unit will reboot.

- Step 13** Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Backup unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Backup appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
- Step 14** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

Configuring High Availability > Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability. Logical monitoring involves configuring the SonicWALL to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Backup IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (only on X0 and X1 interfaces)
- To allow synchronization of licenses between the Idle unit and the SonicWALL licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Backup SonicWALL security appliances' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.



Note

Only the X0 and X1 interfaces can be used for Web-based management using the unique management IP addresses.

The management IP address of the Backup/Idle unit is used to allow license synchronization with the SonicWALL licensing server, which handles licensing on a per-appliance basis (not per-HA Pair). Even if the Backup unit was already registered on MySonicWALL before creating the HA association, you must use the link on the **System > Licenses** page to connect to the SonicWALL server while accessing the Backup appliance through its management IP address.

When using logical monitoring, the HA Pair will ping the specified Logical Probe IP address target from the Primary as well as from the Backup SonicWALL. The IP address set in the Primary IP Address or Backup IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWALLs will assume that the problem is with the target, and not the SonicWALLs. But, if one SonicWALL can ping the target but the other SonicWALL cannot, the HA Pair will failover to the SonicWALL that can ping the target.

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Backup.

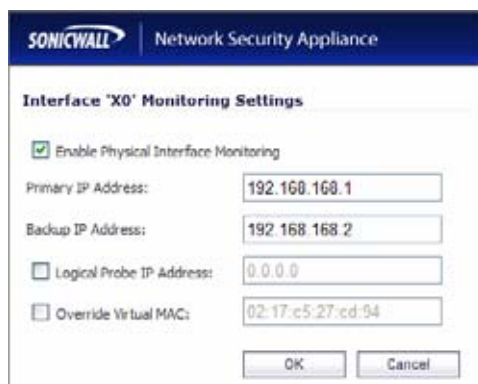
To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring, perform the following steps:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.

Step 2 In the left navigation pane, navigate to **High Availability > Monitoring**.



Step 3 Click the **Configure** icon for the **X0** interface



Step 4 To enable link detection between the designated HA interfaces on the Primary and Backup units, leave the **Enable Physical Interface Monitoring** checkbox selected.

Step 5 In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.

Step 6 In the **Backup IP Address** field, enter the unique LAN management IP address of the Backup unit.

Step 7 In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) The Primary and Backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the SonicWALL appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.

The **Primary IP Address** and **Backup IP Address** fields must be configured with independent IP addresses on the X0 interface (X1 for probing on the WAN) to allow logical probing to function correctly.

Step 8 Optionally, to manually specify the virtual MAC address for the interface, select **Override Virtual MAC** and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as A1:B2:C3:d4:e5:f6. Care must be taken when choosing the Virtual MAC address to prevent configuration errors.

When the **Enable Virtual MAC** checkbox is selected on the **High Availability > Advanced** page, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.

Step 9 Click **OK**.

Step 10 To configure monitoring on any of the other interfaces, repeat the above steps.

- Step 11** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

Applying Licenses to SonicWALL Security Appliances

When your SonicWALL security appliances have Internet access, each appliance in a High Availability Pair must be individually registered from the SonicOS management interface while the administrator is logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL licensing server and share licenses with the associated Primary appliance. There is also a way to synchronize licenses for an HA Pair whose appliances do not have Internet access.

When live communication with SonicWALL's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your appliances. When you register a SonicWALL security appliance on MySonicWALL, a license keyset is generated for the appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the appliance, it cannot perform the licensed services.



Note

In a High Availability deployment without Internet connectivity, you must apply the license keyset to **both** of the appliances in the HA Pair.

You can use one of the following procedures to apply licenses to an appliance:

- [“Activating Licenses from the SonicOS User Interface”](#)
- [“Copying the License Keyset from MySonicWALL”](#)

Activating Licenses from the SonicOS User Interface

Follow the procedure in this section to activate licenses from within the SonicOS user interface. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See [“Configuring High Availability > Monitoring”](#) on page 13 to configure the individual IP addresses.

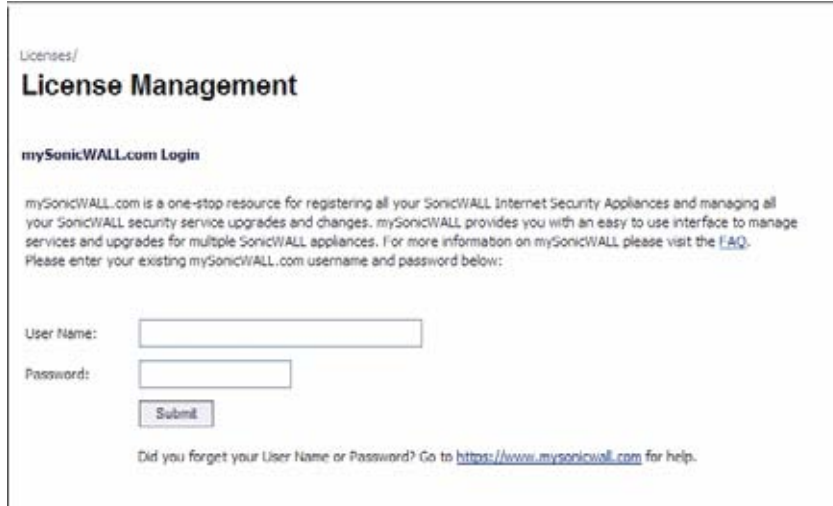
- Step 1** Log in to the SonicOS user interface using the individual LAN management IP address for the appliance.
- Step 2** On the **System > Licenses** page, under **Manage Security Services Online**, click the link for **To Activate, Upgrade or Renew services, click here**.

Manage Security Services Online

To Activate, Upgrade, or Renew services, [click here](#).

For Free Trials, [click here](#).

- Step 3** In the **Licenses > License Management** page, type your MySonicWALL user name and password into the text boxes.



- Step 4** Click **Submit**.
- Step 5** On the **Systems > Licenses** page under **Manage Security Services Online**, verify the services listed in the **Security Services Summary** table.
- Step 6** Repeat this procedure for the other appliance in the HA Pair.

Copying the License Keyset from MySonicWALL

You can follow the procedure in this section to view the license keyset on MySonicWALL and copy it to the SonicWALL security appliance. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See [“Configuring High Availability > Monitoring” on page 13](#) to configure the individual IP addresses.

- Step 1** Login to your MySonicWALL account at <https://www.mysonicwall.com/>.
- Step 2** In the left navigation pane, click **My Products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance to which you want to copy the license keyset. Click the product **name** or **serial number**.
- Step 4** On the **Service Management** page, click **View License keyset**.
- Step 5** On the **License Keyset** page, use your mouse to highlight all the characters in the text box.

This is the license keyset for the SonicWALL security appliance that you selected in [Step 3](#).

Step 6 To copy the license keyset to the clipboard, press **Ctrl+C**.

Step 7 Log in to the SonicOS user interface by using the individual LAN management IP address.

Step 8 On the **Systems > Licenses** page under **Manual Upgrade**, press **Ctrl+V** to paste the license keyset into the **Or enter keyset** text box.

Step 9 Click **Submit**.

Step 10 Repeat this procedure for the other appliance in the HA Pair.

Verifying High Availability Status

There are several ways to view High Availability status in the SonicOS Enhanced management interface. See the following sections:

- “[Viewing the High Availability Status Table](#)” on page 18
- “[Receiving Email Alerts About High Availability Status](#)” on page 19
- “[Viewing High Availability Events in the Log](#)” on page 20

Viewing the High Availability Status Table

The **High Availability Status** table on the **High Availability > Settings** page displays the current status of the HA Pair. If the Primary SonicWALL is Active, the first line in the table indicates that the Primary SonicWALL is currently Active.

It is also possible to check the status of the Backup SonicWALL by logging into the unique LAN IP address of the Backup SonicWALL. If the Primary SonicWALL is operating normally, the status indicates that the Backup SonicWALL is currently Idle. If the Backup has taken over for the Primary, the status table indicates that the Backup is currently Active.

In the event of a failure in the Primary SonicWALL, you can access the management interface of the Backup SonicWALL at the Primary SonicWALL virtual LAN IP address or at the Backup SonicWALL LAN IP address. When the Primary SonicWALL restarts after a failure, it is accessible using the unique IP address created on the High Availability > Monitoring page. If preempt mode is enabled, the Primary SonicWALL becomes the Active firewall and the Backup firewall returns to Idle status.

High Availability Status	
Primary Status	Active
Dedicated HA-Link	X6 100 Mbps full-duplex
Found Backup	Yes
Settings Synchronized	Yes
Primary State	ACTIVE
Backup State	IDLE
Active Up Time	0 Days 16:15:32

The table displays the following information:

- **Primary Status** – This field is labeled **Backup Status** when viewed on the Backup appliance. The possible values are:
 - **Active** – Indicates that this appliance is in the ACTIVE state.
 - **Idle** – Indicates that this appliance is in the IDLE state.
 - **Disabled** – Indicates that High Availability has not been enabled in the management interface of this appliance.
 - **Not in a steady state** – Indicates that HA is enabled and the appliance is neither in the ACTIVE nor the IDLE state.
- **Dedicated HA-Link** – Indicates the port, speed, and duplex settings of the HA link, such as **X6 100 Mbps full-duplex**, when two SonicWALL TZ 210 appliances are connected over their designated HA interfaces. When the HA interfaces are not connected or the link is down, the field displays **X6 No Link**. When High Availability is not enabled, the field displays **Disabled**.



Note The designated HA port is port **X6** on the SonicWALL TZ 210 Series and port **X4** on the SonicWALL TZ 200 Series.

- **Found Backup** - Indicates **Yes** if the Primary appliance has detected the Backup appliance, and **No** if there is no HA link or if the Backup is rebooting. This field is labeled **Found Primary** when viewed on the Backup appliance, and indicates **Yes** if the Backup appliance has detected the Primary appliance, and **No** if there is no HA link or if the Primary is rebooting.
- **Settings Synchronized** - Indicates if the settings are synchronized between the two appliances. This includes all settings that are part of the system preferences, for example, NAT policies, routes, user accounts. Possible values are **Yes** or **No**.

- **Primary State** - Indicates the current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Backup appliances. The possible values are:
 - **ACTIVE** – Indicates that the Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
 - **IDLE** – Indicates that the Primary unit is passive and is ready to take over on a failover.
 - **ELECTION** – Indicates that the Primary and Backup units are negotiating which should be the ACTIVE unit.
 - **SYNC** – Indicates that the Primary unit is synchronizing settings or firmware to the Backup.
 - **ERROR** – Indicates that the Primary unit has reached an error condition.
 - **REBOOT** – Indicates that the Primary unit is rebooting.
 - **NONE** – When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Backup unit, **NONE** indicates that the Backup unit is not receiving heartbeats from the Primary unit.
- **Backup State** - Indicates the current state of the Backup appliance as a member of an HA Pair. The Backup State field is displayed on both the Primary and the Backup appliances. The possible values are:
 - **ACTIVE** – Indicates that the Backup unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
 - **IDLE** – Indicates that the Backup unit is passive and is ready to take over on a failover.
 - **ELECTION** – Indicates that the Backup and Primary units are negotiating which should be the ACTIVE unit.
 - **SYNC** – Indicates that the Backup unit is synchronizing settings or firmware to the Primary.
 - **ERROR** – Indicates that the Backup unit has reached an error condition.
 - **REBOOT** – Indicates that the Backup unit is rebooting.
 - **NONE** – When viewed on the Backup unit, **NONE** indicates that HA is not enabled on the Backup. When viewed on the Primary unit, **NONE** indicates that the Primary unit is not receiving heartbeats from the Backup unit.
- **Active Up Time** - Indicates how long the current Active firewall has been Active, since it last became Active. This line only displays when High Availability is enabled. If failure of the Primary SonicWALL occurs, the Backup SonicWALL assumes the Primary SonicWALL LAN and WAN IP addresses. There are three main methods to check the status of the High Availability Pair: the High Availability Status window, Email Alerts and View Log. These methods are described in the following sections.

Receiving Email Alerts About High Availability Status

If you have configured the Primary SonicWALL to send email alerts, you receive alert emails when there is a change in the status of the High Availability Pair. For example, when the Backup SonicWALL takes over for the Primary after a failure, an email alert is sent indicating that the Backup has transitioned from Idle to Active. If the Primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the Primary SonicWALL takes over and another email alert is sent to the administrator indicating that the Primary has preempted the Backup.

Viewing High Availability Events in the Log

The SonicWALL also maintains an event log that displays the High Availability events in addition to other status messages and possible security threats. This log may be viewed in the SonicOS management interface or it may be automatically sent to the administrator's email address. To view the SonicWALL log, click **Log** on the left navigation pane of the management interface.