

SonicWall® Global Management System 3G/4G/Modem

Administration

SONICWALL®

Contents

3G/4G/LTE Modem Overview	3
Device Detection and Selecting the Interface	3
Understanding 3G/4G/LTE	3
3G/4G/LTE Connection Types	4
SonicWave MiFi Extender	4
3G/4G/LTE Failover	5
3G/4G/LTE Prerequisites	7
Enabling the U0/U1 Interface	7
Configuring 3G/4G/Modem Settings	8
Auto-detect	8
3G/4G/LTE/Mobile	8
Analog Modem	10
Configuring 3G/4G/Modem Advanced Settings	12
Configuring 3G/4G/Modem Advanced Settings	12
Configuring Bandwidth Management	13
Setting the Connection Limit for Dialup Connections	14
Configuring the 3G/4G/Modem Connection Profiles	15
General View Settings	15
Parameters View Settings	16
IP Address View Settings	16
Schedule View Settings	17
Data Limiting View Settings	17
Advanced View Settings	18
SonicWall Support	19
About This Document	20

3G/4G/LTE Modem Overview

SonicWall network security appliances with a USB extension port can support either an external 3G/4G/LTE interface or analog modem interface.

Topics:

- [Device Detection and Selecting the Interface](#)
- [Understanding 3G/4G/LTE](#)
- [3G/4G/LTE Prerequisites](#)
- [Enabling the U0/U1 Interface](#)

Device Detection and Selecting the Interface

By default, the appliance tries to detect the type of external interface that is connected. If it can successfully identify what kind it is, the left side navigation changes to show what was detected.

You can manually specify which type of interface you want to configure on the **3G/4G/Modem > Settings** page.

The **3G/4G/LTE/Modem Device Type** drop-down menu provides these options:

- **Auto-detect** - Select this option and the appliance attempts to determine what kind of device is attached.
- **3G/4G/LTE/Mobile** - Select this option to manually configure a 3G/4G/LTE/Mobile interface.
- **Analog Modem** - Select this option to manually configure an analog modem interface.

When a device is connected after being detected or identified, the **3G/4G/Modem > Settings** page displays configuration settings for it.

NOTE: A 3G/4G/LTE device can be connected/disconnected from the **Network > Interfaces** page after clicking **MANAGE** for the U0 interface. See [Enabling the U0/U1 Interface](#) on page 7.

Understanding 3G/4G/LTE

SonicWall security appliances support 3G/4G/LTE Wireless WAN connections that utilize data connections over cellular networks. The 3G/4G/LTE connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a preconfigured connection might not be available, such as at trade-shows and kiosks.
- Mobile networks, where the SonicWall appliance is based in a vehicle.

- Primary WAN connection where wire-based connections are not available and 3G/4G Cellular is.

To use the 3G/4G interface you must have a 3G/4G/LTE PC card or USB device and a contract with a wireless service provider. A 3G/4G/LTE service provider should be selected based primarily on the availability of supported hardware. GMS supports the devices listed online at:

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

Topics:

- [3G/4G/LTE Connection Types](#)
- [SonicWave MiFi Extender](#)
- [3G/4G/LTE Failover](#)

3G/4G/LTE Connection Types

When the 3G/4G/LTE device is installed prior to starting the appliance, the device is listed in the Interface Settings table at **Network > Interfaces**. The interface name is listed as **U0** or **U1** in the name column.

The 3G/4G/LTE Connection Types setting provides flexible control over WAN connectivity on SonicWall appliances with 3G/4G/LTE interfaces. The Connection Type is configured when you edit the profile on **3G/4G > Connection Profiles**. The following connection types are offered on the **Parameters** tab of the 3G/4G Profile Configuration window:

- **Persistent Connection** – After the 3G/4G interface is connected to the 3G/4G service provider, it remains connected until the administrator disconnects it or a network event (such as the WAN becoming available) causes it to disconnect.
- **Connect on Data** – The 3G/4G interface connects automatically when the SonicWall appliance detects specific types of network traffic.
- **Manual Connection** – The 3G/4G interface is connected only when the administrator manually initiates the connection.



CAUTION: Although the 3G/4G connection can be manually enabled on the **Network > Interfaces** page (by clicking **MANAGE** for the U0/U1 interface), this is not recommended; it can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described previously.

SonicWave MiFi Extender

The SonicWave 3G/4G/LTE MiFi Extender feature allows SonicWall wireless access points to connect to 3G or 4G cellular networks to create a wireless hot spot that can be shared among mobile devices such as smart phones, laptops, and tablets. This WWAN solution allows multiple end users and mobile devices to share a 3G or 4G mobile broadband Internet connection.

To use this feature, plug a USB device into the SonicWave access point and it connects to the Internet over 3G/4G. In GMS, you bind a VLAN Interface to the USB modem.

This feature is supported on all SonicWall firewalls running GMS and all SonicWave and access points with USB interfaces. A USB device that supports 3G, 4G, or the QMI protocol is required.

Use the following settings for the VLAN configuration:

- Set the Zone to WAN.
- Set the parent interface to the physical interface to which access points are connected.

- For a 3G USB modem, the IP Assignment should be Static, and assign a private IP address to it. Leave the gateway and DNS servers fields blank; they are filled automatically after the provisioning for the access point is completed.
- For 4G and QMI Modem, the IP Assignment should be DHCP. It gets the DHCP lease from the USB modem server after the modem is connected.

This feature uses 3G/4G connection profile settings configured on the MiFi Extender configuration page.

3G/4G/LTE Failover

i **IMPORTANT:** You can manage the failover behavior of the 3G/4G/LTE device when the primary WAN interface goes down. For the 3G/4G/LTE interface to function as a backup interface, it can be configured as the Final Backup interface in the default load balancing group. Go to the **Network > Failover & LB** page, and edit the group that contains the 3G/4G/LTE device.

The following sections describe the three different methods of WAN-to-3G/4G/LTE failover. All of these sections assume that the U0/U1 interface is configured as the Final Backup interface in the load balancing group.

- [3G/4G/LTE Failover with Persistent Connection](#)
- [3G/4G/LTE Failover with Connect on Data](#)
- [Manual Dial 3G/4G/LTE Failover](#)

3G/4G/LTE Failover with Persistent Connection

The following depicts the sequence of events when the WAN Ethernet connection fails and the 3G/4G/LTE Connection Profile is configured for **Persistent Connection**.

- 1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. The U0/U1 interface is never connected while the Ethernet WAN interface is available.
- 2 **Primary Ethernet connection fails** – The U0/U1 interface is initiated and remains in an *always-on* state while the Ethernet WAN connection is down.

If another Ethernet WAN interface is configured as part of the load balancing group, the appliance first fails over to the secondary Ethernet WAN before failing over to the U0/U1 interface. In this situation, failover to the U0/U1 interface only occurs when both the primary and secondary WAN paths are unavailable.

- 3 **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the primary WAN port or the secondary WAN port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The U0/U1 interface connection is closed.


i **NOTE:** If the 3G/4G/LTE is configured as an Alternate WAN, even if **Preempt and failback to preferred interfaces when possible** is unchecked (**System Setup | Network > Edit Default LB Group**), the U0 connection disconnects when the Ethernet WAN becomes available.


⚠ CAUTION: Do not configure a policy-based route that uses the U0/U1 interface when the U0/U1 interface is configured and up as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1 interface, the connection remains up until the Maximum Connection Time (if configured) is reached.

3G/4G/LTE Failover with Connect on Data


The following depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G/LTE Connection Profile is configured for **Connect on Data**.

- 1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G/4G/LTE is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies the U0/U1 interface as the destination interface).
- 2 **Primary Ethernet Connection Fails** – The U0/U1 interface connection is not established until outbound data attempts to pass through the SonicWall appliance.
- 3 **3G/4G Connection Established** – The U0/U1 interface connection is established when the device or a network node attempts to transfer data to the Internet. The U0/U1 interface stays connected until the Maximum Connection Time (if configured) is reached.
- 4 **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again or the inactivity timer (if configured) is reached, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The U0/U1 interface connection is terminated.

 **NOTE:** If the 3G/4G/LTE is configured as an Alternate WAN, even if **Preempt and failback to preferred interfaces when possible** is unchecked (**Network > Failover & LB | Edit**), the U0 connection disconnects when the Ethernet WAN becomes available.

 **CAUTION:** Do not configure a policy-based route that uses the U0/U1 interface when the U0/U1 interface is configured and up as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1 interface, the connection remains up until the Maximum Connection Time (if configured) is reached.

Manual Dial 3G/4G/LTE Failover


 **CAUTION:** SonicWall does not recommend using a Manual Dial 3G/4G Connection Profile when the U0/U1 interface is intended to be used as a failover backup for the primary WAN interface. During a WAN failure the appliance loses WAN connectivity until the U0/U1 interface connection is manually initiated by the administrator. The following depicts the sequence of events that occur when the WAN Ethernet connection fails, and the 3G/4G Connection Profile is configured for Manual Dial.

- 1 **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G/4G/LTE is never connected while the Ethernet WAN connection is available.
- 2 **Primary Ethernet Connection Fails** - The U0/U1 interface connection is not established until the administrator manually enables the connection.
- 3 **3G/4G Connection Established** – A U0/U1 interface connection is established when the administrator manually enables the connection on the SonicWall appliance. The U0/U1 interface stays connected until you manually disable the connection.
- 4 **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G/4G connection** until the connection is manually disabled by you. After a manual disconnect, the available Ethernet connection is used.

3G/4G/LTE Prerequisites

Before configuring the 3G/4G/LTE interface, you must complete the following prerequisites:

- Purchase a 3G/4G/LTE service plan from a supported third-party wireless provider.
- Configure and activate your 3G/4G/LTE device.
- Insert the 3G/4G/LTE device into the SonicWall appliance **before** powering on the SonicWall security appliance.


 **IMPORTANT:** The 3G/4G/LTE device should only be inserted or removed when the SonicWall security appliance is powered off.

Enabling the U0/U1 Interface

When a 3G/4G/LTE USB modem is connected to a SonicWall security appliance, GMS detects the model and displays a U0 interface in the **Network > Interfaces** page. This interface belongs to the WAN zone by default and can be used for Failover and Load Balancing. The U0 configuration settings include the device type, Connect on Data categories, and management/user login options. The U0 interface also provides a **MANAGE** button for accessing the **Connection Manager**.

To use the modem, one needs to connect the USB device to the network by clicking **Connect** in the Connection Manager. Before the connection is established, U0's Connection Manager status is *Disconnected*.


 **NOTE:** For all 3G/4G/LTE USB devices, a 3G/4G profile must be created before clicking **Connect**.

 **CAUTION:** Repeatedly manually enabling the 3G/4G/LTE connection on the **Network > Interfaces** page (by clicking **MANAGE** for the U0/U1 interface) is not recommended. This can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G/LTE interface using the connection types described in **3G/4G/LTE Connection Types**.

To manually initiate a connection on the U0/U1 external 3G/4G/LTE interface:

- 1 On the **Network > Interfaces** page, click **Connect** for the U0/U1 interface. The **U0/U1 Connection Status** dialog displays.
- 2 Click **Connect**. The WAN interface address and DNS address are assigned by the ISP's DHCP server. GMS uses this DHCP IP address for the U0 interface IP address.

When the connection is active, the **U0/U1 Connection Status** (Connection Manager) displays statistics on the session. Images for a 4G/LTE device and a 3G (PPP) device are shown as follows.

 **NOTE:** The DNS server address 192.168.1.1 is a temporary IP address. This address is the default internal DNS server address. Because this address might cause an IP address conflict, it cannot be used in GMS as a DNS server address. In the case of ATT Velocity/Huawei E3372 LTE devices, the device does not provide an AT command interface for fetching the real DNS server information. However, the LTE modem's internal web server has a valid DNS server. An HTTP communication channel is initiated by GMS to retrieve this valid DNS server address.

- 3 To end the connection, click **Disconnect**.

Configuring 3G/4G/Modem Settings

SonicWall network security appliances with a USB extension ports can support either external 3G/4G/LTE interfaces or analog modem interfaces.

Topics:

- [Auto-detect](#)
- [3G/4G/LTE/Mobile](#)
- [Analog Modem](#)

Select SonicWall appliances are equipped to use analog modem, and/or wireless WAN (WWAN) devices for alternative or primary Internet connectivity.

 **NOTE:** For information on configuring WWAN settings, see [Configuring 3G/4G/Modem Advanced Settings](#).

To configure the modem settings for one or more SonicWall access points:

- 1 Select the SonicWall appliance to manage.
- 2 Navigate to the **3G/4G/Modem > Settings** page.
- 3 Select the **3G/4G/LTE/Modem Device Type** depending on your environment. Options include:
 - **Auto-detect** - Select this option and the appliance attempts to determine what type of device is attached.
 - **3G/4G/LTE/Mobile** - Select this option to manually configure a 3G/4G/LTE/Mobile interface.
 - **Analog Modem** - Select this option to manually configure an analog modem interface.

When a device is connected after being detected or identified, the **3G/4G/Modem > Settings** page displays specific configuration settings for it.

Auto-detect

By default, GMS attempts to detect the type of connected external interfaces. You can use this option when you would like GMS to determine your modem device type, or when you are not sure of your modem device type. If you have changed from a previous configuration, click **Update**.

3G/4G/LTE/Mobile

To manually configure a 3G/4G/LTE/Mobile interface, select from the following options:

- 1 Select the check boxes for any combination of the following Connect on Data Categories:
 - NTP Packets

- AV Profile Updates
 - Firmware Update Requests
 - GMS Heartbeats
 - SNMP Traps
 - Syslog Traffic
 - System Log Emails
 - Licensed Updates
- 2 For the **Management/User Login**, select the check boxes for any combination of the following **Management** methods:
- HTTPS
 - HTTP
 - Ping
 - SNMP
 - SSH
- 3 Select the check boxes for any combination of the following **User Login** methods:
- HTTP
 - HTTPS
 - For HTTPS, check the box next to **Add rule to enable redirect from HTTP to HTTPS** to redirect an HTTP address to HTTPS.
- 4 Click **Update** to save your settings.

Analog Modem

To configure an analog modem, select from the following options:

MODEM SETTINGS

Modem Device Type: Analog Modem

MODEM SETTINGS

Speaker volume: On

Modem Initialization

Initialize Modem for use in: United States

Initialize Modem using AT Commands:

CONNECT ON DATA CATEGORIES

NTP packets

AV Profile Updates

Firmware Update requests

GMS Heartbeats

SNMP Traps

Syslog traffic

System log emails

Licensed Updates

MANAGEMENT / USER LOGIN

Management

HTTPS

HTTP

Ping

SNMP

SSH

User Login

HTTP

HTTPS

Add rule to enable redirect from HTTP to HTTPS

Update Reset

- 1 Select the **Speaker volume** drop-down menu to configure the speaker volume **On** or **Off**.
- 2 Modem initialization has two options:
 - To initialize the modem for use in a specific country, select the radio button next to **Initialize Modem for use in** and select the country in the drop-down menu.
 - To initialize the modem using AT commands, select the radio button next to **Initialize Modem using AT Command** and enter the AT command(s) the modem needs to establish a connection in the text box.
- 3 Select the check boxes for any combination of the following Connect on Data Categories:
 - NTP Packets
 - AV Profile Updates
 - Firmware Update Requests
 - GMS Heartbeats
 - SNMP Traps
 - Syslog Traffic

- System Log Emails
 - Licensed Updates
- 4 For the **Management/User Login**, select the check boxes for any combination of the following **Management** methods:
- HTTPS
 - HTTP
 - Ping
 - SNMP
 - SSH
- 5 Select the check boxes for any combination of the following **User Login** methods:
- HTTP
 - HTTPS
 - For HTTPS, check the box next to **Add rule to enable redirect from HTTP to HTTPS** to redirect an HTTP address to HTTPS.
- 6 Click **Update** to save your settings.

Configuring 3G/4G/Modem Advanced Settings

The **Remotely Triggered Dial-out** section enables you to remotely initiate a WAN modem connection. The following process describes how a Remotely Triggered Dial-out call functions:

- 1 The network administrator initiates a modem connection to the SonicWall security appliance located at the remote location.
- 2 If the appliance is configured to authenticate the incoming call and prompts the network administrator to enter a password. After the call is authenticated, the appliance terminates the call.
- 3 The appliance then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
- 4 Access the appliance's web management interface to perform the required tasks.

Before configuring the **Remotely Triggered Dial-out Settings** feature, ensure that your configuration meets the following prerequisites:

- The 3G/4G connection profile is configured for dial-on-data.
- The SonicWall Security Appliance is configured to be managed using HTTPS, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Inactivity Disconnect** field. This field is located in **3G/4G/Modem > Connection Profiles | Add** page on the **Parameters** tab. See [Configuring the 3G/4G/Modem Connection Profiles](#) for more information. If you do not enter a value in this field, dial-out calls remain connected indefinitely.

Topics:

- [Configuring 3G/4G/Modem Advanced Settings](#)
- [Configuring Bandwidth Management](#)
- [Setting the Connection Limit for Dialup Connections](#)

Configuring 3G/4G/Modem Advanced Settings

To configure advanced modem settings:

- 1 Select the SonicWall appliance to manage.

- 2 Navigate to the **3G/4G/Modem > Advanced** page.

REMOTELY TRIGGERED DIAL-OUT SETTINGS

Enable Remotely Triggered Dial-out

Requires Authentication

Password

Confirm Password

BANDWIDTH MANAGEMENT

Enable Egress Bandwidth Management

Enable Ingress Bandwidth Management

Compression Multiplier

Note: BWM Type: None; To change go to [Firewall Settings > BWM](#) screen.

DIALUP CONNECTION LIMIT

Max Hosts (0 = unlimited)

Update Reset

- 3 To enable remotely triggered dial-out, check **Enable Remotely Triggered Dial-out**.
- 4 If your remotely triggered dial-out requires authentication, check **Requires Authentication** and enter your password in the **Password** and **Confirm Password** fields.
- 5 Click **Update**.

i **NOTE:** For information on configuring WWAN settings, see [Configuring 3G/4G/Modem Advanced Settings](#).

Configuring Bandwidth Management

The **Bandwidth Management** section allows you to enable egress or ingress bandwidth management services on the 3G/4G interface.

To configure bandwidth management:

- 1 Select the SonicWall appliance to manage.
- 2 Navigate to the **3G/4G/Modem > Advanced** page.
- 3 Scroll down to the **Bandwidth Management** section.
- 4 Check the box to **Enable Egress Bandwidth Management**.
- 5 Check the box to **Enable Ingress Bandwidth Management**.
- 6 Select the **Compression Multiplier** from the drop-down menu:
1.0x (default), **1.5x**, **2.0x**, **2.5x**, **3.0x**, **3.5x**, or **4.0x**.
The Compression Multiplier applies to both egress and ingress bandwidths.
- 7 Click **Update** to save your settings.

The note under Bandwidth Management also tells you what bandwidth management type was selected and provides a link to change it if you would like.


Setting the Connection Limit for Dialup Connections

The **Dial-up Connection Limit** section allows you to set a host/node limit on the 3G/4G connection. This feature is especially useful for deployments where the 3G/4G connection is used as an overflow or in load-balanced situations to avoid overtaxing the connection.

To set the connection limit for dial-up connections:

- 1 Select the SonicWall appliance to manage.
- 2 Navigate to the **3G/4G/Modem > Advanced** page.
- 3 In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.
- 4 Click **Update**.

Configuring the 3G/4G/Modem Connection Profiles

 **NOTE:** For information on configuring WWAN connection profiles, see [Configuring 3G/4G/Modem Settings](#).

A profile is a list of dial-up connection settings that can be used by a SonicWall SonicWave/SonicPoint appliance.

Topics:

- [General View Settings](#)
- [Parameters View Settings](#)
- [IP Address View Settings](#)
- [Schedule View Settings](#)
- [Data Limiting View Settings](#)
- [Advanced View Settings](#)

General View Settings

To configure a profile:

- 1 Select the SonicWall appliance to manage.
- 2 Navigate to the **3G/4G/Modem > Connection Profiles** page.
- 3 Select a primary profile from the **Primary Profile** drop-down menu. Optionally, select alternate profiles from **Alternate Profile 1** and **Alternate Profile 2**.

 **NOTE:** To configure modem profiles, navigate to **3G/4G/Modem > Connection Profiles**.

- 4 Scroll down to the **Connection Profiles** section.
- 5 Click **Add**.
- 6 On the **General** view, select the country where your modem is located.
- 7 Select a **Service Provider** from the drop-down list, or select **Other** if yours is not available.
- 8 Select your **Plan Type**. Choices depend on the **Service Provider**.
- 9 The Plan Type **Name** auto-populates depending on your selections.
- 10 The **Connection Type** auto-populates depending on your selection.
- 11 Enter the primary ISP phone number in the **Primary Dial Number** field (if it has not auto-populated).
- 12 Enter the backup ISP phone number in the **Secondary Dial Number** field.

- 13 Enter the user name associated with the account in the **User Name** field.
- 14 Enter the password associated with the account in the **User Password** and **Confirm User Password** fields.
- 15 The **APN** is your ISP Access Point Name.
- 16 Click **Update** to save your settings.

Parameters View Settings

The **Parameters** settings allows you to define conditions under which the service connects. The three connection types are **Persistent Connection**, **Connect on Data**, and **Manual Connection**. The mechanics of these connection types are described in [Understanding 3G/4G/LTE](#).

To configure the Parameter settings:

- 1 Click **Parameters**.
- 2 Select from the following **Connect Type** connection options:
 - If the SonicWall appliance(s) remains connected to the Internet until the broadband connection is restored, select **Persistent Connection**.
 - If the SonicWall appliance(s) only connects to the Internet when data is being sent, select **Connect On Data**.
 - If the SonicWall appliance(s) connects to the Internet manually, select **Manual Connection**.
- 3 To enable the modem to disconnect after a period of inactivity, check **Enable Inactivity Disconnect** and specify how long (in minutes) the modem waits before disconnecting from the Internet in the **minutes** field.
- 4 To specify the maximum connection time, select **Enable Max Connection Time** and enter the maximum connection time (in minutes) in the **minutes** field. To configure the SonicWall device to allow indefinite connections, enter **0**.
- 5 To specify a time (in minutes) before the connection reconnects, enter the number of **minutes** in the **Delay Before Reconnect** fields.
- 6 To allow the modem to attempt a connection multiple times, check the **Dial Retries per Phone Number** box and specify the number of retries.
- 7 To specify how long the modem waits between retries, check **Delay between Retries** and specify the delay (in minutes).
- 8 To disable VPN when dialed, check **Disable VPN when dialed**.
- 9 Force the Password Authentication Protocol (PAP) by checking **Force PAP Authentication**.
- 10 Click **Update** to save your settings.

IP Address View Settings

Use **IP Address Settings** to configure dynamic or static IP addressing for a 3G/4G/LTE interface. In most cases, you want to **Obtain an IP Address Automatically**; however, you can configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.


Under IP Address Settings, select from the following:

- 1 Select one of the following **IP Address** options:

- If the account obtains an IP address dynamically, select **Obtain an IP Address Automatically**.
 - If the account uses a fixed IP address, select **Use the following IP Address** and type the IP address in the field.
- 2 Select from the following **DNS Servers** options:
 - If the account obtains DNS server information from the ISP, select **Obtain an IP Address Automatically**.
 - If the account uses a specific DNS servers, select **Use the following IP Address** and type the IP address in the field.

Schedule View Settings

Use **Schedule** to limit connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.

 **NOTE:** When this feature is enabled, if the checkbox for a day is **not** selected, 3G/4G/LTE access is denied for that entire day.


To specify the time periods when the modem can connect:

- 1 Click **Schedule**.
- 2 Check **Limit Times for Connection Profile** and click **Configure**. The **Edit Schedule String** pop-up displays.
- 3 In the **Edit Schedule String** pop-up, check the box next to the day(s) you want to allow dial-up connections. Next to the day(s) you select, enter the **Start** and **End** times between which dial-up connections are allowed. Enter the hour and minute in the 24-hour format.
- 4 Click **Apply**.
- 5 On the **Schedule | Limited 3G/4G Access Times** view, click **Update** to save your settings.

Data Limiting View Settings

Data Limiting is only available for 3G/4G/LTE devices. Use it to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G/4G/LTE provider's billing cycle and disconnect when a given limit is reached.

To limit data usage:

- 1 Click **Data Limiting**.
 -  **TIP:** If your 3G/4G/LTE account has a monthly data or time limit, enabling Data Usage Limiting is strongly recommended.
- 2 Check **Enable Data Usage Limiting** and have the 3G/4G/LTE interface become automatically disabled when the specified data or time limit has been reached for the month.
- 3 Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** drop-down menu.
- 4 Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.

Advanced View Settings

Use **Advanced** to manually configure a chat script used during the 3G/4G connection process.

i | **TIP:** Configuring a chat script is only necessary when you need to add commands or special instructions to the standard dial-up connection script.

To configure a chat script:

- 1 Click the **Advanced** view.
- 2 Enter the connection chat script in the **Chat Script** field (optional).
- 3 Click **Update**.

SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access **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>.

About This Document

Legend



NOTE: A NOTE icon indicates supporting information.



IMPORTANT: An IMPORTANT icon indicates supporting information that may need a little extra attention.



TIP: A TIP indicates helpful information.



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



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

SonicWall GMS 3G/4G/Modem Administration
Updated - October 2020
Software Version - 9.3
232-005122-00 Rev B

Copyright © 2020 SonicWall Inc. All rights reserved.

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

Open Source Code

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

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