SonicWall® Global Management System MANAGE Virtual Assist

Administration

SONICWALL®

Contents

Configuring Virtual Assist

ⓘ **IMPORTANT:** This page displays only when Virtual Assist is enabled.

Virtual Assist allows users to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. Users can allow or invite customers to join a "queue" to receive support, then virtually assist each customer by remotely taking control of a customer's computer to diagnose and remedy technical issues.

To maximize the flexibility of the Virtual Assist feature, take time to properly adjust all of the available settings. To configure settings within the GMS management interface, go to the **Virtual Assist > Settings** page.

Topics:

- General Settings
- Notification Settings
- Request Settings
- Updating the Settings
- Restriction Settings

General Settings

The first decision you need to make is how to provide access for customers to gain support through Virtual Assist. There are two options:

- Provide an "Assistance Code" for customers to enter when accessing the portal after receiving an invitation.
- Enable virtual assist support without the need for an invitation.

By setting a global assistance code for customers, you can restrict who enters the system to request help. The code can be a maximum of eight (8) characters, and can be entered in the Assistance Code field. Customers receive the code through an email provided by the technician or administrator. To allow customers to request

Virtual Assist support without needing to provide a code, leave the **Assistance Code** field blank, and select **Enable Support without Invitation**.

The **Disclaimer** field allows administrators to set a written message that customers must read and agree to prior to receiving support. If a disclaimer is set, it must be accepted by each customer before they can enter the Virtual Assist queue.

The **Customer Access Link** field allows users to set a URL for customer access to your SSL-VPN appliance, from outside your network. If no URL is entered, the support invitation to customers uses the same URL the technician uses to access the appliance.

ⓘ **NOTE:** You should configure this URL if the SSL-VPN appliance is accessed through a different URL from outside your network.

If customers navigate to the technician login page, you have the option to display a link there to redirect them to the support login page. To do this, select **Display Virtual Assist link from Portal Login**. Support without invitation should be enabled, if you want customers to be able to request help from the login page.

Notification Settings

Under the **Notification Settings** section, you can customize various aspects of the invitation and technician notification settings. All email address entries in the **Technician E-mail List** field receives a notification email

when a customer enters the support queue (uninvited). A maximum of 10 emails can be added to this list, with each separated by a semicolon.

You can customize the subject line of support invitation emails by entering your desired text in the **Subject of Invitation** field. The following variables can be used within the **Subject of Invitation** field:

- Technician Name: `%EXPERTNAME%`

  The default is **`%EXPERTNAME%` has sent you a support invitation**.

- Customer Message in the Invitation: `%CUSTOMERMSG%`

- Link for Support: `%SUPPORTLINK%`

- Link to SSL-VPN: `%ACCESSLINK%`

These variables can also be used in the **Invitation Message** field, where you can further customize the body of the invitation email, by entering your desired text. The message can be a maximum length of 800 characters. The default is:

```
An assistance invitation has been generated for you by:
%EXPERTNAME%<br>%CUSTOMERMSG%<br>%SUPPORTLINK%<br>If you cannot access the link,
request assistance by copying and pasting this link: <br>%ACCESSLINK%<br>Please do
not reply.This message was automatically generated
```

To utilize the email invitation capabilities of Virtual Assist, you must configure the appropriate Mail Server and Mail from Address settings on the **Log > Settings** page.

Request Settings

In the **Request Settings** section of the **Virtual Assist > Settings** page, you configure various settings related to support request limits.

- The **Maximum Requests** field allows you to limit the number of customers that can be awaiting assistance in the queue at one time by specifying the maximum number of customer requests allowed before new requests are blocked. The default is **10**.

- The **Limit Message** field allows you to enter text to be displayed as a message to customers when there are currently no available spots in the queue because the maximum requests limit has been reached. The maximum length of the message is 256 characters. The default message is **Maximum queue size reached, please try again later**.

- You can also limit the number of requests coming from a single IP. This prevents the same customer from repeatedly requesting Virtual Assist support. Enter the desired amount limit in the **Maximum Requests from One IP** field. Enter 0 (default) for no limitation.

- To avoid customers waiting indefinitely for Virtual Assist support during high-volume periods, you can set a time limit (in minutes) for how long a customer can remain in the queue without receiving support. Set this limit by entering the desired number of minutes in the **Pending Request Expired** field. Enter 0 (default) if you do not wish to set a limit.

Updating the Settings

When you have finished configuring the settings, click **Update**. The **Modify Task Description and Schedule** dialog displays.
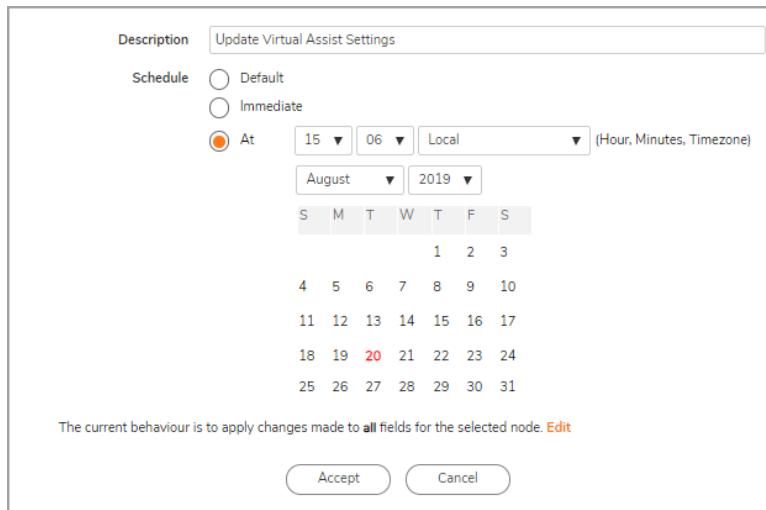

To schedule the update:

1. Navigate to the **Virtual Assist > Settings** page.

2. Scroll down to the **Restriction Settings** section.

3. Enter the name of the schedule in the **Description** field. This field is populated with the name of the setting to which the schedule applies.

4. Select the type of schedule for the task:

   - **Default**

   - **Immediate**

   - **At:** (specify when the task is to take place)

5   Click **Accept**.

Restriction Settings

If you encounter requests from unwanted or illegitimate sources, you can block requests from defined IP addresses. You can do this in the **Restriction Settings** section.
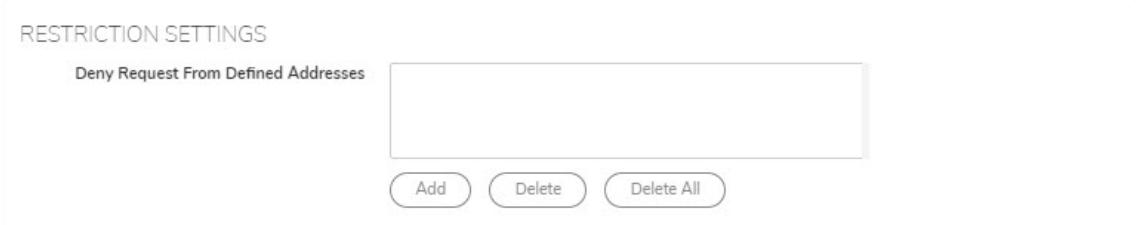

Topics:

- Adding Denied Addresses
- Deleting Denied Addresses

Adding Denied Addresses

To add a denied address:

1   Navigate to the **Virtual Assist > Settings** page.

2   Scroll down to the **Restriction Settings** section.

3   Click **Add** to add a source IP address to block. The **Admin Address** dialog displays.
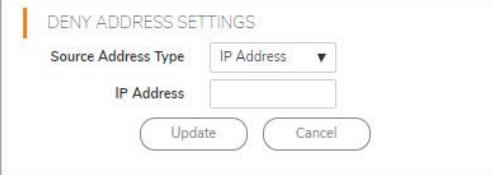
4   Specify the **Source Address Type**:

- **IP Address** (default)
- **IP Network**

5   Enter the address from which you wish to deny support requests in the **IP Address** field.

6   Click **Update** to submit the information. The **Modify Task Description and Schedule** dialog displays.

| Description | Add New Virtual Assist Deny Address: 120.34.56.78/255.255.255.255 |

Schedule ○ Default
          ○ Immediate
          ● At   15 ▼   16 ▼   Local   ▼   (Hour, Minutes, Timezone)

          August ▼   2019 ▼

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

          (Accept)   (Cancel)

7   Enter the name of the schedule in the **Description** field. This field is autopopulated with the name of the setting to which the schedule applies.

8   Select the type of schedule for the task:

- **Default**

- **Immediate**

- **At:** (specify when the task is to take place)

9   Click **Accept**. The newly blocked address now appears in the **Deny Request From Defined Address** table.

Deleting Denied Addresses

To delete an address:

1   Navigate to the **Virtual Assist > Settings** page.

2   Scroll down to the **Restriction Settings** section.

3   Select the address in the **Deny Request From Defined Addresses** table.

4   Click **Delete**.

To delete all denied addresses:

1   Navigate to the **Virtual Assist > Settings** page.

2   Scroll down to the **Restriction Settings** section.

3   Click **Delete All**.

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.

About This Document

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, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

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