Getting Started

https://campus.barracuda.com/doc/84968123/

When deploying Barracuda Firewall Insights, you must configure basic settings before the system can be used in production. Complete the steps below to make your Firewall Insights ready for production and to connect your first CloudGen Firewall devices.

Before You Begin

- Verify that you have completed all steps from Deployment.
- To get familiar with log retention periods, see Understanding Data Retention and Storage Capacity.
- Connect your network interface card again, or connect it to the correct network if it is a KVM Hypervisor.
- Verify that the following ports are not blocked by your CloudGen Firewall:

Port	Function
2400	Authentication of devices
8001	Data streaming
443	Web UI – https

For general information on required outbound connections, see Required Outbound Connections for Barracuda Networks Appliances.

Step 1. Licensing

For Barracuda Firewall Insights you need:

- A license for Barracuda Firewall Insights
- A subscription for Barracuda Firewall Insights on every CloudGen Firewall you want to connect to your Firewall Insights

There is no restriction by license on your Firewall Insights. The only restriction is the system performance of the virtual machine itself. Your virtual machine can be sized to fit your needs and is not limited by the license.

Enter a License Token for Barracuda Firewall Insights

1. For Barracuda Firewall Insights you need a valid license token before you can continue.
2. To enter the license token for Barracuda Firewall Insights, follow the instructions in How to Configure Network Settings and Licensing on First Boot.
3. Open your web browser and enter `https://<ip address of Firewall Insights>`
4. The license agreement is shown. Please read it.
5. Scroll down. Type in your name, email address and company, and click **Accept** to finish.
6. It may take some time until the process is finished. Afterwards, you can log into your Barracuda Firewall Insights again.

Step 2. Change Your Password

1. Open your web browser and enter `https://<ip address of Firewall Insights>`
2. Log in:
   - **Username**: `admin`
   - **Password**: The numeric part of the Barracuda Firewall Insights serial. E.g., for BNG-1234567, enter 1234567.

     The default password is intended for initial access only. You must change it once you are logged in.
     - Under **New password**, enter a password of your choice. The password must consist of at least 8 characters.
     - Re-enter the new password in the field below.
   - Click **Sign in**.
3. The **Basic > General** tab is displayed.

(Optional) To re-change your password in Firewall Insights later, go to **Basic > Administration**.

You must provide a **System Alerts Email Address** in the **Email Notification** section and a **Shared Secret** in the **Connected Devices** section, which are both located on **Basic > Administration** page, before you can save the new password. Otherwise, follow the steps below.

Step 3. Configure Email Notifications

1. Go to **Basic > Administration**.
2. Scroll down to the **Email Notification** section.
3. Enter the configuration for the email address you want Firewall Insights to use to send email notifications from:
   - **SMTP Host** – Enter the SMTP host of the email address.

- **SMTP Port** – Enter the SMTP port.
- **Connection Security** – Select your connection security from the drop-down menu.
- **Username** and **Password** – Provide username and password of the email account you want to use.
- **System Alerts Email Address** – Enter the email address that will receive Firewall Insights system alerts next to. If you enter more than one email address, separate them with a comma.
- **From Email** – Enter the email address that Firewall Insights sends its emails from.
- **Test SMTP Configurations** – To test your email configuration, enter an email address where you would like to send a test mail to next to and click **Send Test Email**.

Step 4. Provide Time and NTP Server Settings

1. Go to **Basic > Administration**.
2. In the **Time** section, select your time zone from the drop-down menu next to **Time Zone**.
3. In the **NTP Server** section, you can choose to enable a sync with an NTP server you specify.
   - To enable, click **Yes** next to **Enable NTP Sync**.
     - Provide an NTP server IP address or hostname of an NTP server in the field next to **NTP Servers**.
   - To disable, click **No** next to **Enable NTP Sync**.

Step 5. Configure the Web Interface Settings

1. Go to **Basic > Administration**.
2. Specify the web interface settings for the web interface of your Barracuda Firewall Insights in the **Web Interface Settings** section.
3. **Web Interface Certificate** – Select either **Default certificate** or **User-defined certificate.** If you select **User-defined certificate**, you can choose between:
   - **Single Certificate in PEM FILE** – Upload the certificate file using the **Browse** button. Click the **Upload** button after you select your certificate file.
   - **All other PEM Certificates** – Upload the certificate file and the certificate key file using the **Browse** button. Provide the certificate password and click **Upload**.
   - **PKCS12 Token** – Upload the signed certificate file using the **Browse** button. Provide the certificate password and click **Upload**.
4. **Session Expiration Length** – Time of inactivity, in minutes, before users are required to log on again to access the web interface.
   Minimum value: 1 minute. Default setting: 20 minutes.
5. **Update Dashboard Every 30 Minutes** – Select **Yes** to automatically refresh the dashboard so you can see the most recent information.
   - If you select **Yes**, as long as you leave the dashboard up as the active screen, you will not be logged out of the dashboard, and it will continue to display updated information every 30 minutes. When you switch to a different tab, if the **Session Expiration Length** is

exceeded, you will be logged out.
- If you select **No**, the **Session Expiration Length** will apply to the **Dashboard** along with the rest of the tabs.

Step 6. Configure a Log Retention Period and a Shared Secret

1. Go to **Basic > Administration**.
2. In the **Connected Devices** section, you can define a shared secret and a log retention period.
3. Next to **Log Retention Period**, choose the log retention period from the drop-down menu. You can choose between 1, 2, 3, 6, 9, and 12 months. The default log retention period is 6 months.
4. Next to **Shared secret**, enter the shared secret.

Step 7. Save the Configuration

1. To save the configuration, click **Save Changes** in the upper-right corner.
2. Some settings are mandatory before you can save the configuration. If one of these settings is not configured, you will receive a notification. Provide the missing settings and click **Save Changes** again to save the configuration.

Step 8. Connect CloudGen Firewall Devices

Barracuda Firewall Insights is the Shared Secret authority. Specify the Shared Secret for Barracuda Firewall Insights (in Step 6), then use that Shared Secret in devices you want to connect. You must specify these settings in Barracuda Firewall Insights first. If they are not specified in Barracuda Firewall Insights, you will receive an error when you click **Connect**.

1. Verify that the firmware of your CloudGen Firewall supports Firewall Insights. See Supported CloudGen Firewall Firmware.
2. Connect your CloudGen Firewall with Barracuda Firewall Insights following the steps in Barracuda Firewall Insights Integration.
3. (optional) If your CloudGen Firewall is in a remote network, follow these steps: How to Stream Data to Firewall Insights via a Remote Management Tunnel.
4. Open your web browser and enter `https://<ip address of Firewall Insights>`
5. Navigate to the **BASIC > Administration** page, then scroll down to the **Connected Devices** section to confirm that the connection was successful. The devices connect automatically.

Further Information

- To create a snapshot, see Backing Up Your Virtual Machine System State.
- To create a configuration backup, see Backups.