NovoZil AlertMe

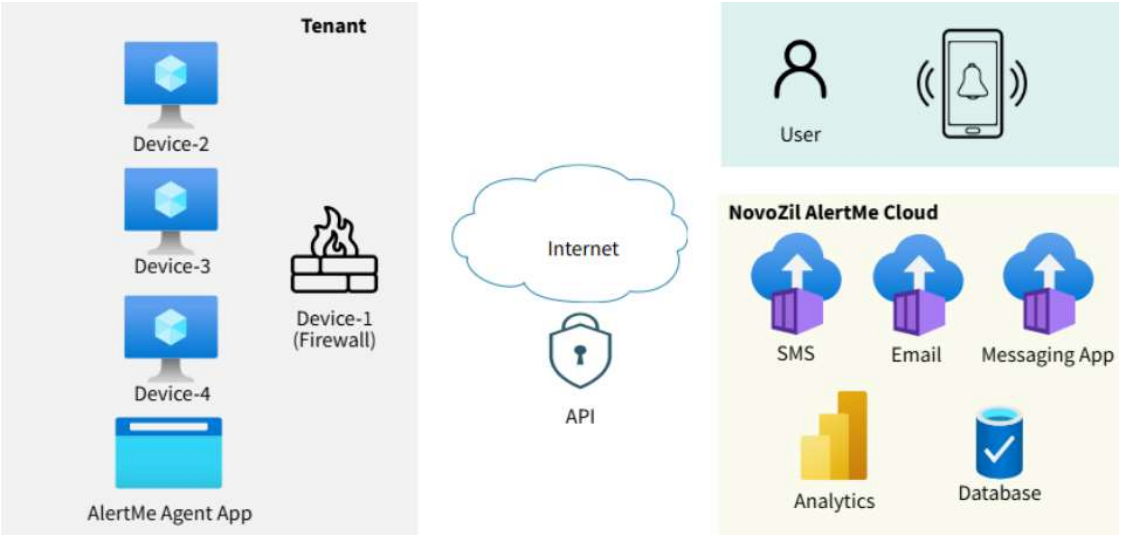
USER MANUAL

NovoZil AlertMe Portal

Introduction

NovoZil AlertMe is a cloud-based service designed to provide real-time security and system health monitoring through seamless Syslog message processing. This solution consists of two key components: the NovoZil AlertMe Agent and the Cloud Portal.

The NovoZil AlertMe Agent runs on the client's network, receiving Syslog messages from various devices and filtering relevant security and operational events. These filtered messages are then securely transmitted to the NovoZil Cloud Portal. The portal not only provides an intuitive interface for monitoring Syslog alerts but also enables instant notifications via SMS, email, or Telegram, ensuring that IT staff members stay informed of critical events in real time.



What are the key benefits?

Enhanced Security Awareness: Stay informed with real-time alerts and SMS/Text, email, or Telegram notifications, ensuring immediate awareness of security incidents and device health.

Efficient Management: Simplify administrative tasks with a multi-tenant architecture, making it an ideal solution for Managed Service Providers (MSPs) or Managed Security Service Providers (MSSPs) overseeing multiple client environments.

Hassle-Free Setup: Experience zero-touch deployment with the NovoZil AlertMe Agent, which automatically configures itself, reducing setup time and effort.

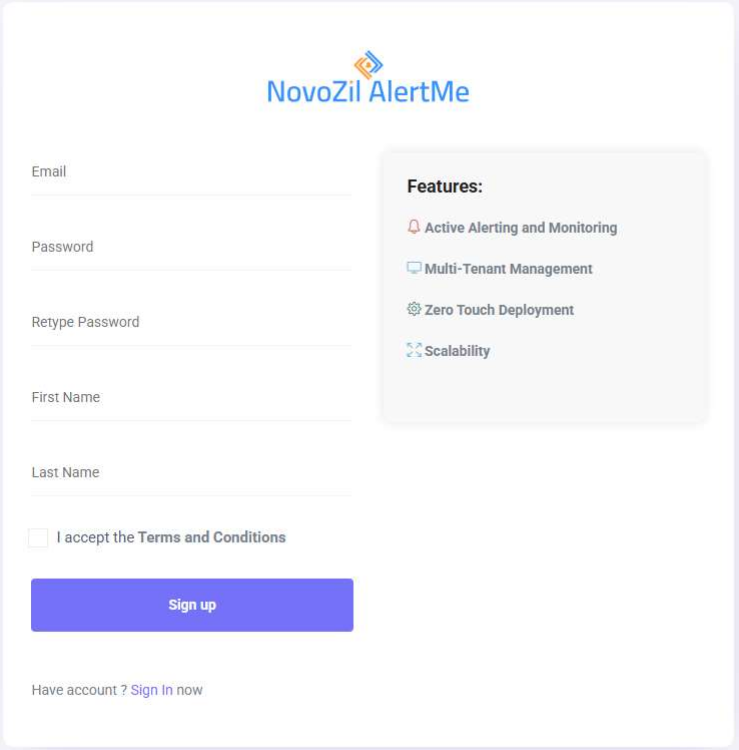
Seamless Scalability: Grow your business effortlessly with NovoZil's scalable multi-tenant architecture, supporting expansion for both end customers and MSPs.

Pre-Requesits

- ✔ NovoZil AlertMe Agent application installed on a host computer
- ✔ Access to the NovoZil AlertMe portal https://alertme.novozil.com

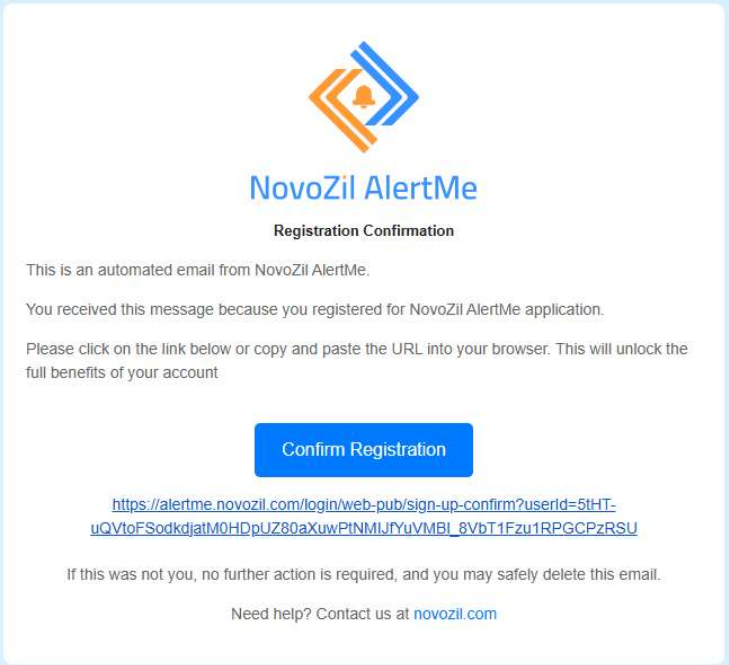
Signing Up

Open your browser and navigate to `https://alertme.novozil.com`. Click on the `Sign Up` option and complete the required fields. After submitting the form, you will receive an email to verify your account.



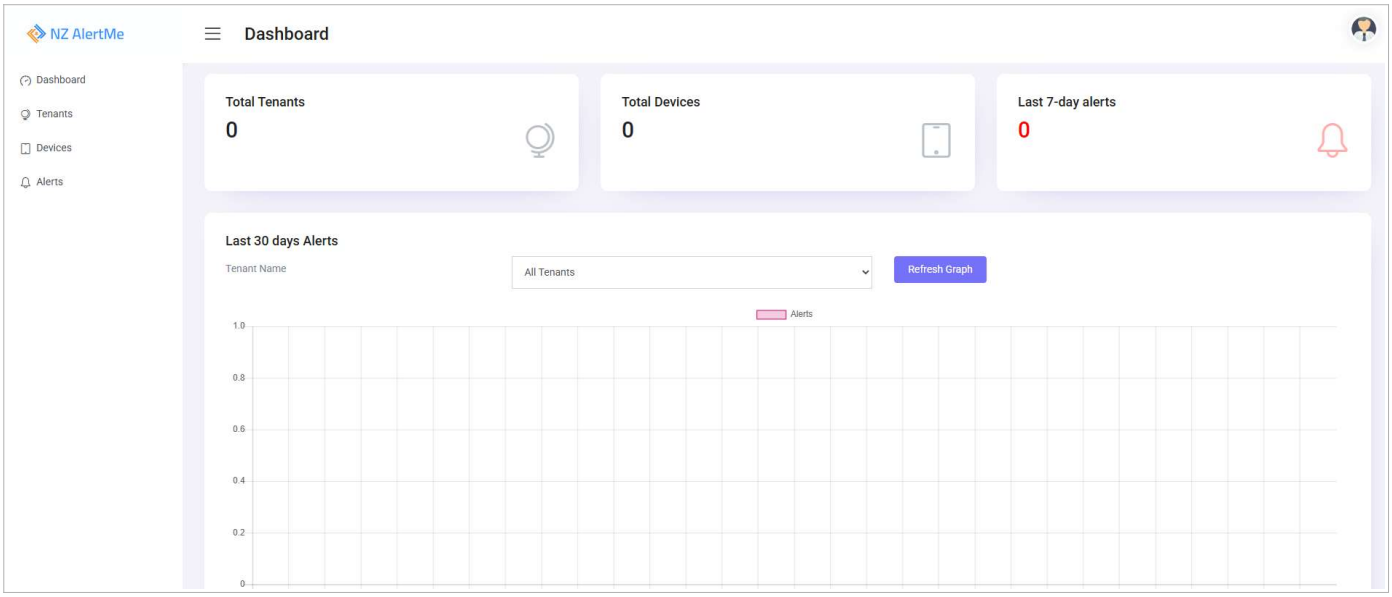
Registration Confirmation

After signing up, you will receive an email to complete your registration.



Signing-in

Signing in to the portal will direct you to the `Dashboard` landing page. The dashboard provides an overview of the number of tenants, devices, and alerts from the past seven days, along with a chart displaying alert trends over the last 30 days.



Overview of Features

The NovoZil AlertMe portal can receive Syslog messages from SonicWall, FortiGate, and Sophos firewalls. Additionally, to monitor device availability, it also supports ICMP ping. Users will receive notifications when a device becomes unreachable and when it becomes available again.

The left-side menu provides access to the following sections:

Dashboard: Displays an overview of the number of tenants, devices, and alerts from the past seven days, along with a 30-day alert trend chart.

Tenants: Supports multiple tenants, making it ideal for MSPs/MSSPs managing multiple clients or businesses with multiple office locations. Each client or location can have its own tenant.

Devices: Allows users to register devices. A tenant must be created first before adding any devices, as each device must be associated with a tenant.

Alerts: Displays Syslog messages received from the NovoZil AlertMe Agent.

The right-side menu provides access to the following sections:

Profile: Displays user information such as email, name, company name, and phone number.

Licenses: The NovoZil AlertMe service operates on a subscription or license-based model. Each registered device requires an active subscription or license to send notifications to registered channels such as SMS, email, or the Telegram app.

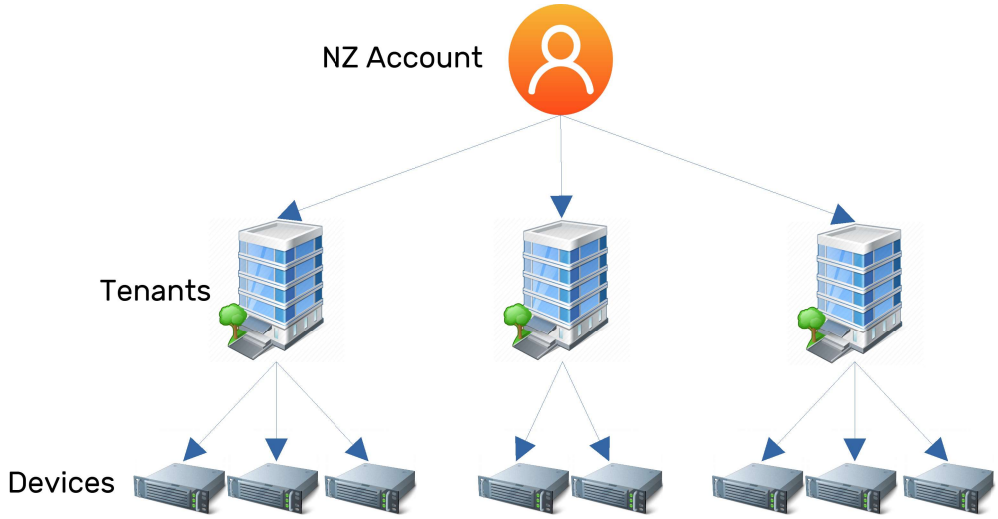
Invoices: This section displays processed invoices, which can be viewed or downloaded.

Change Password: Users can update their account credentials on this page.

Logout: Logs the user out of the portal.

Account-Tenant-Device Hierarchy

Within your account, you can manage multiple tenants, each of which can host multiple devices. A tenant serves as a logical container for devices, ensuring organized management. Each tenant can be associated with only one agent application, which reports all devices under that tenant to the cloud portal.

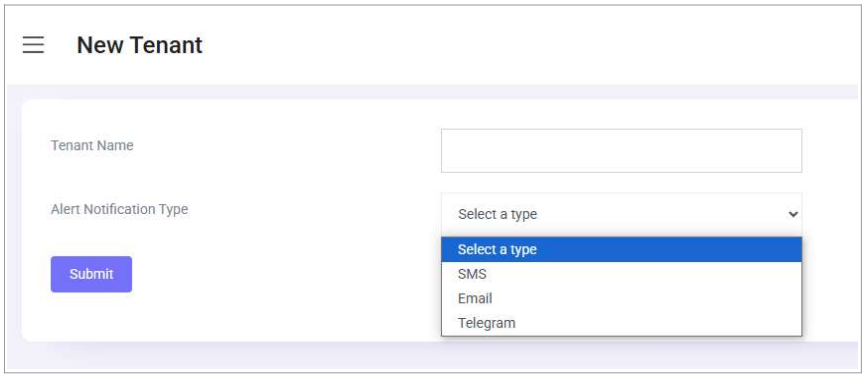


Creating a Tenant

Before adding any devices, a tenant must be created. To do this, navigate to the `Tenants` section in the main menu and select `Add Tenant`.

When creating a tenant:

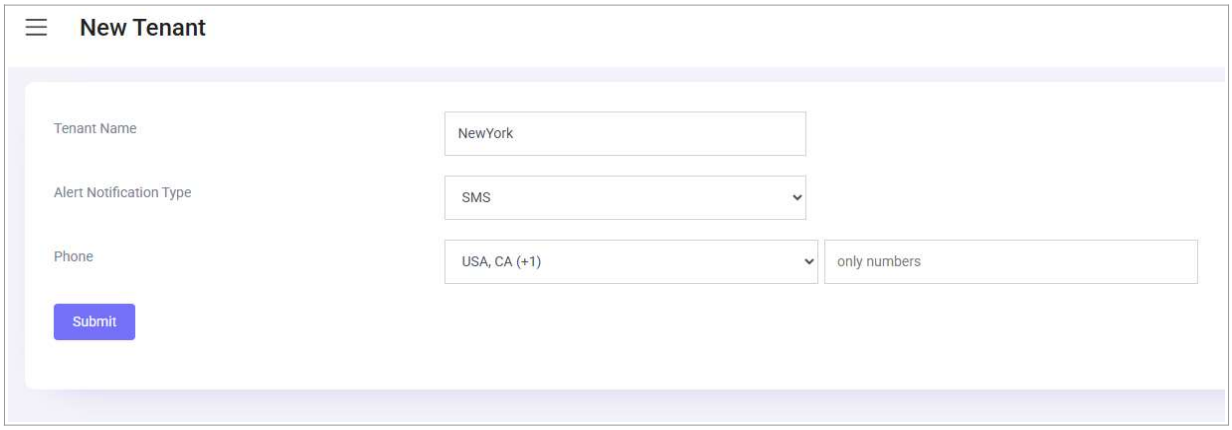
- Assign a unique name within the account scope.
- Choose an `Alert Notification Type`.



If `SMS` is selected as the notification type:

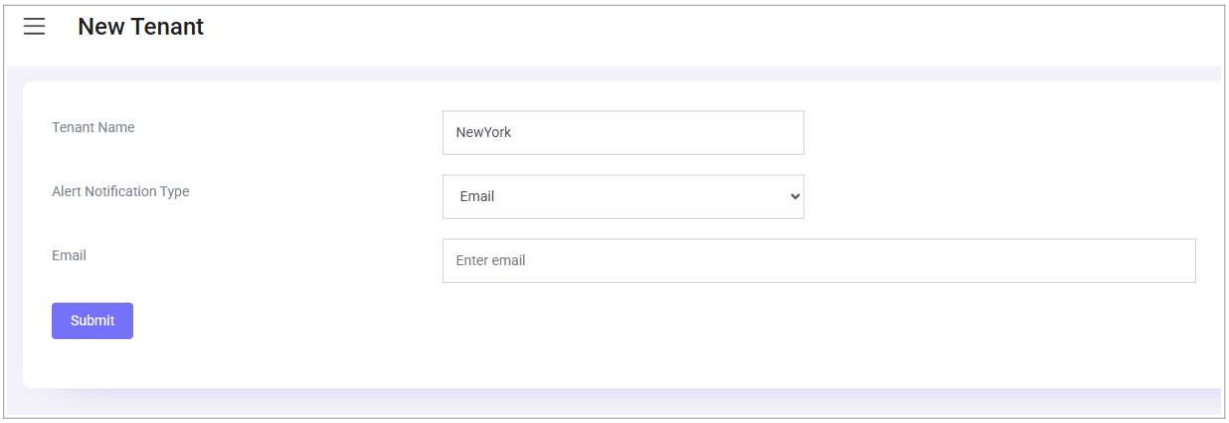
- You will be prompted to enter a phone number.
- After submission, a verification code will be sent to the registered phone number for confirmation.

Please note that, SMS notifications are currently available only in US and Canada.



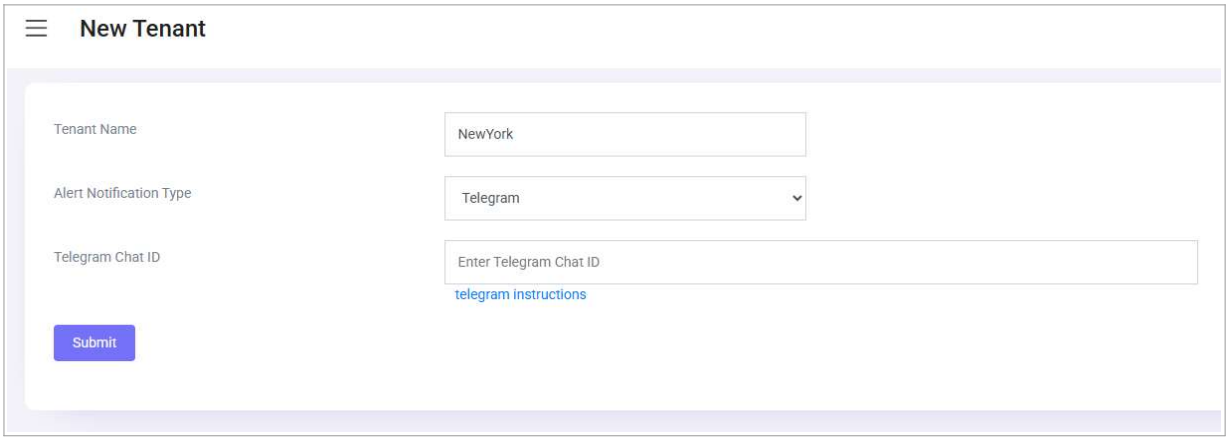
If `Email` is selected as the notification type:

- You will be prompted to enter an email address.
- After submission, a verification code will be sent to the registered email address for confirmation.



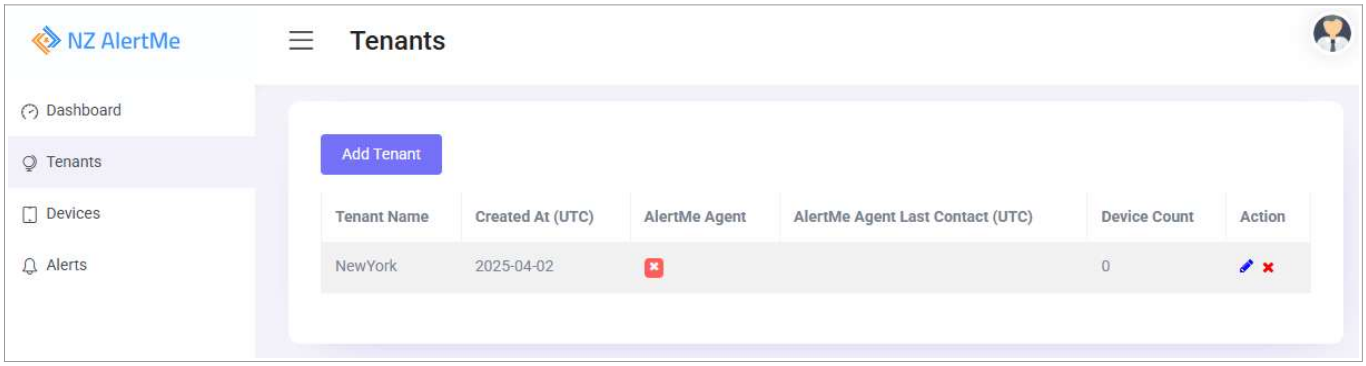
If `Telegram` is selected as the notification type:

- You will be prompted to enter the `Telegram Chat ID`.
- For an individual user, send a `/start` message to `@AlertMeAppBot https://t.me/AlertMeAppBot`. Then, copy the chat ID provided in the reply.
- For a group, first add `@AlertMeAppBot https://t.me/AlertMeAppBot` to your telegram group. Next, send a `/start` message within the group, and copy the group chat ID including `'-'` from the reply.



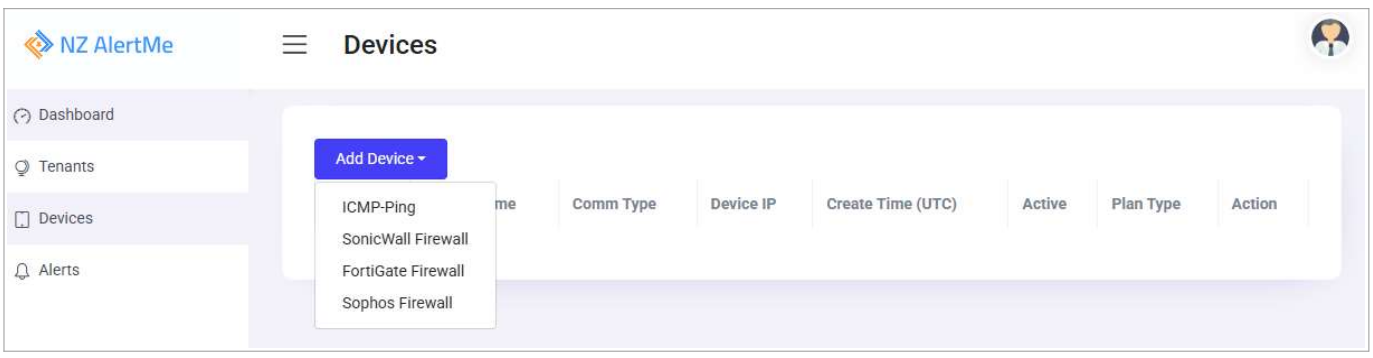
Editing/Deleting a Tenant

A tenant can be edited or deleted by using the icons under the `Action` column. If the tenant contains a device, then the device needs to be deleted first.



Adding a Device

NovoZil AlertMe processes Syslog messages from SonicWall, FortiGate, and Sophos firewalls. Additionally, it supports ICMP Ping monitoring to track device health and availability.



Add Device – ICMP/Ping Monitoring

When selecting `ICMP Ping` as the monitoring method for a device, the following details must be provided:

Device Name: A unique identifier for the device within the tenant.

Tenant Name: The tenant to which the device will be assigned.

IP Address: The target device's IP address for monitoring.

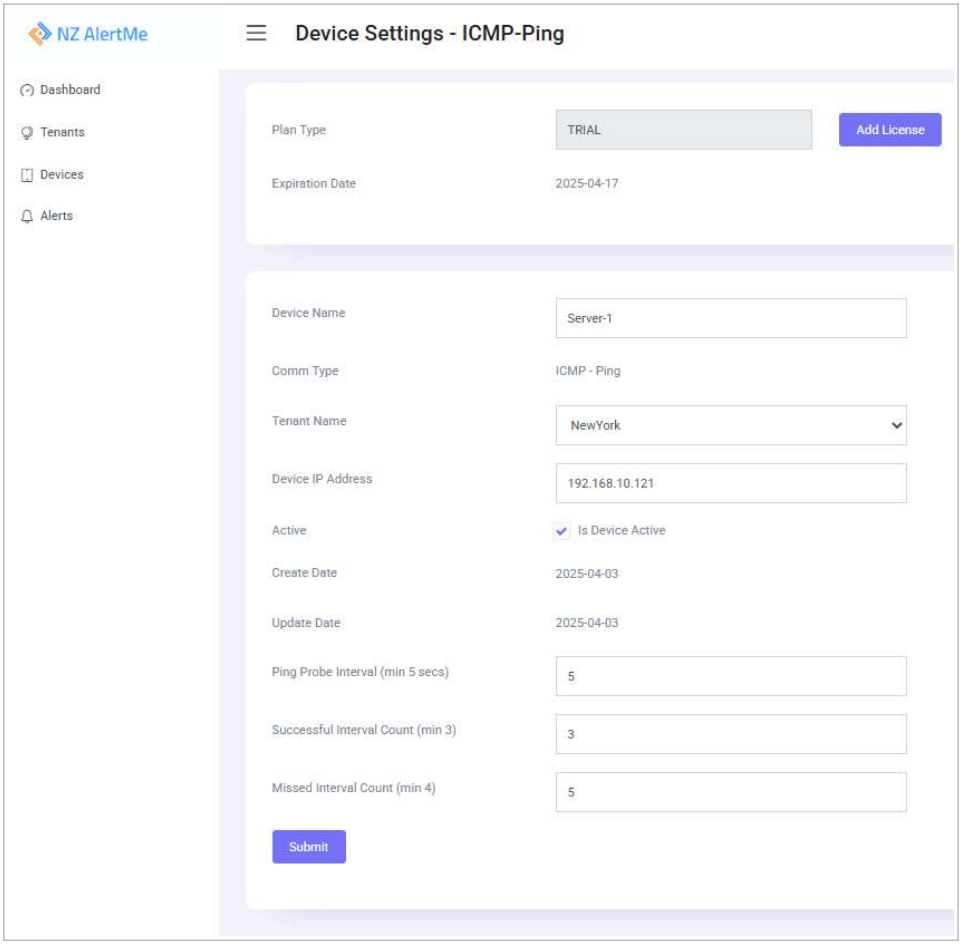
Active: Enables or disables monitoring for the device.

Ping Probe Interval: The frequency at which the system will send ICMP Ping requests to check the device's availability.

Successful Interval Count: The number of consecutive successful ping responses required to consider the device available.

Missed Interval Count: The number of consecutive missed ping responses before the device is considered unavailable.

Once configured, the system will continuously monitor the device's availability. If the device fails to respond within the defined threshold, the NovoZil AlertMe Agent will send a status update to the NovoZil AlertMe Portal, which will then trigger a notification through the selected channels (SMS, Email, or Telegram).



Add Device – SonicWall Firewalls

Device Name: A unique identifier for the device within the tenant.

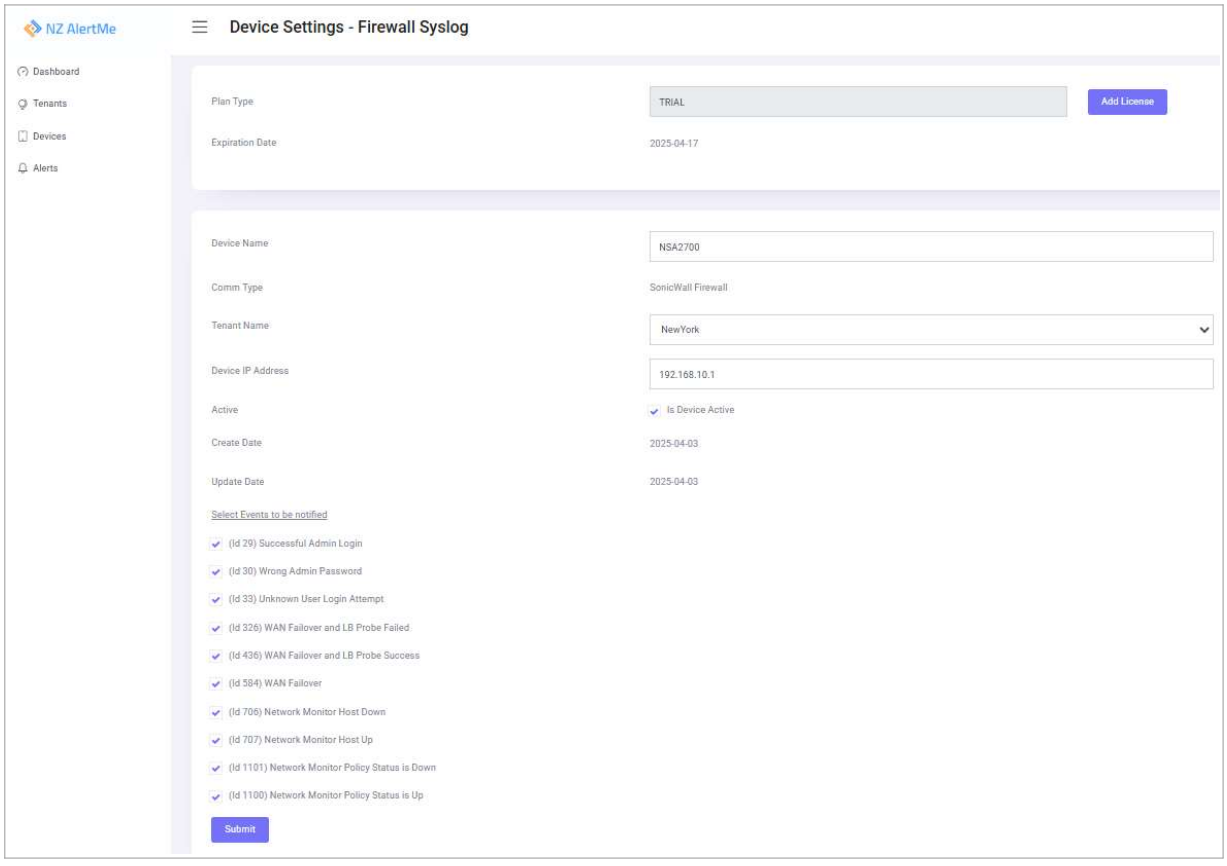
Tenant Name: The tenant to which the firewall device will be assigned.

IP Address: The IP address of the SonicWall firewall.

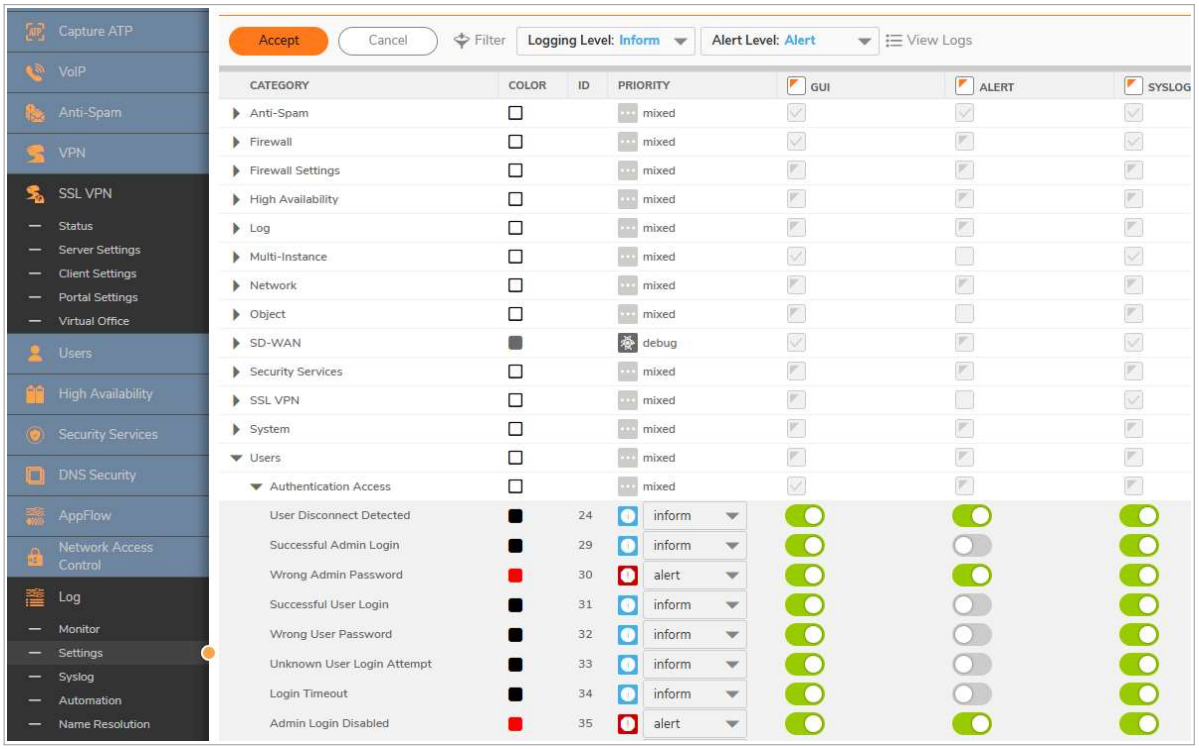
Active: Enables or disables monitoring for the device.

Syslog Events: The following events can be chosen to receive notifications.

- (Id 29) Successful Admin Login
- (Id 30) Wrong Admin Password
- (Id 33) Unknown User Login Attempt
- (Id 326) WAN Failover and LB Probe Failed
- (Id 436) WAN Failover and LB Probe Success
- (Id 584) WAN Failover
- (Id 706) Network Monitor Host Down
- (Id 707) Network Monitor Host Up
- (Id 1101) Network Monitor Policy Status is Down
- (Id 1100) Network Monitor Policy Status is Up



Pease note that the ID represents the unique identifier for each event, which can be found on the SonicWall firewall or in the Syslog Reference Document. Below are examples of events from a SonicWall firewall.



Add Device – FortiGate Firewalls

Device Name: A unique identifier for the device within the tenant.

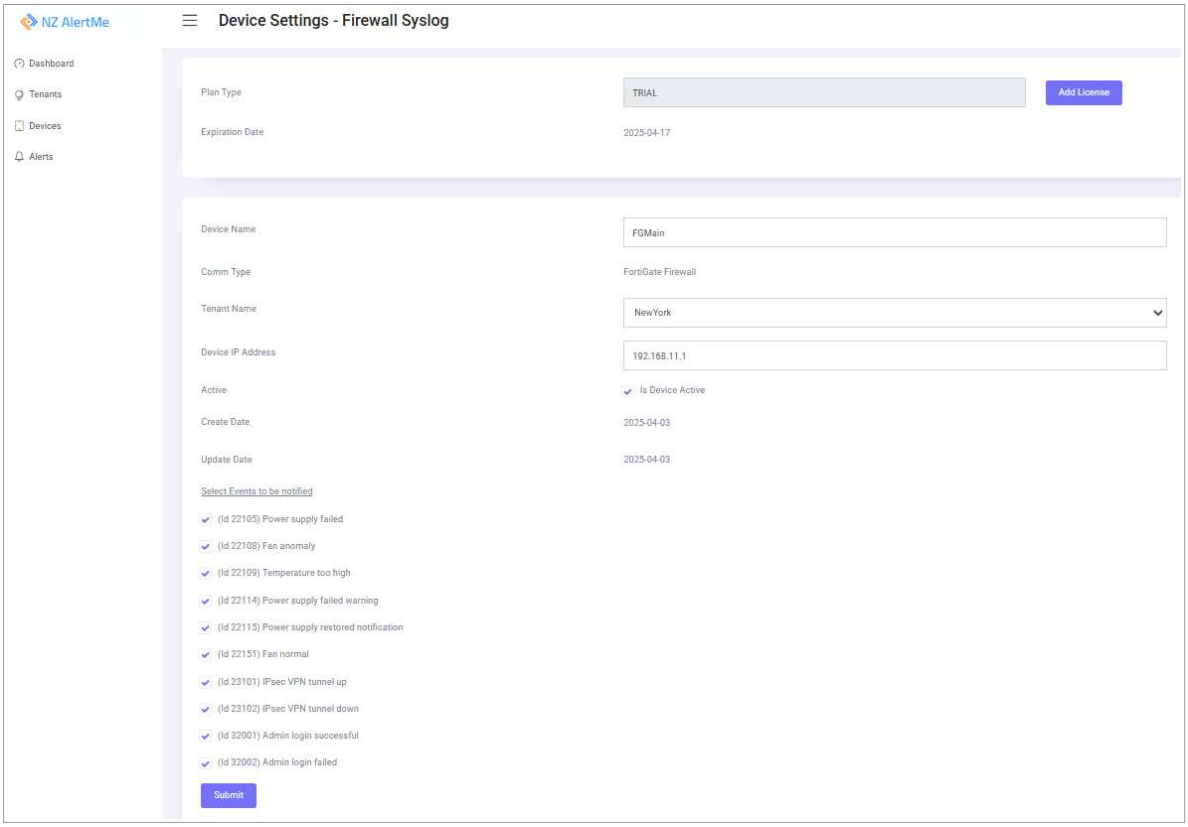
Tenant Name: The tenant to which the firewall device will be assigned.

IP Address: The IP address of the SonicWall firewall.

Active: Enables or disables monitoring for the device.

Syslog Events: The following events can be chosen to receive notifications.

- (Id 22105) Power supply failed
- (Id 22108) Fan anomaly
- (Id 22109) Temperature too high
- (Id 22114) Power supply failed warning
- (Id 22115) Power supply restored notification
- (Id 22151) Fan normal
- (Id 23101) IPsec VPN tunnel up
- (Id 23102) IPsec VPN tunnel down
- (Id 32001) Admin login successful
- (Id 32002) Admin login failed



Add Device – Sophos Firewalls

Device Name: A unique identifier for the device within the tenant.

Tenant Name: The tenant to which the firewall device will be assigned.

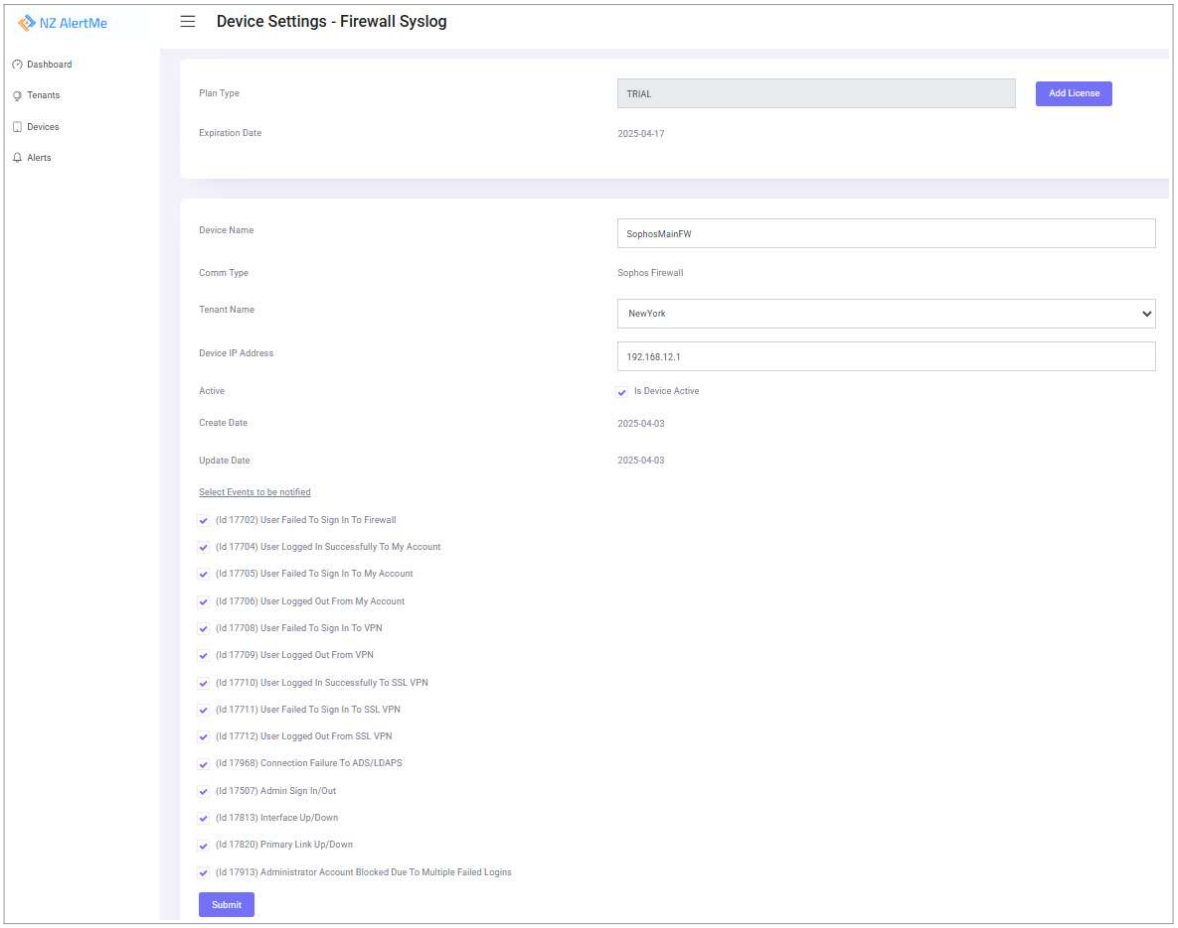
IP Address: The IP address of the SonicWall firewall.

Active: Enables or disables monitoring for the device.

Syslog Events: The following events can be chosen to receive notifications.

- (Id 17702) User Failed To Sign In To Firewall
- (Id 17704) User Logged In Successfully To My Account
- (Id 17705) User Failed To Sign In To My Account
- (Id 17706) User Logged Out From My Account
- (Id 17708) User Failed To Sign In To VPN
- (Id 17709) User Logged Out From VPN
- (Id 17710) User Logged In Successfully To SSL VPN
- (Id 17711) User Failed To Sign In To SSL VPN
- (Id 17712) User Logged Out From SSL VPN
- (Id 17968) Connection Failure To ADS/LDAPS
- (Id 17507) Admin Sign In/Out

- (Id 17813) Interface Up/Down
- (Id 17820) Primary Link Up/Down
- (Id 17913) Administrator Account Blocked Due To Multiple Failed Logins

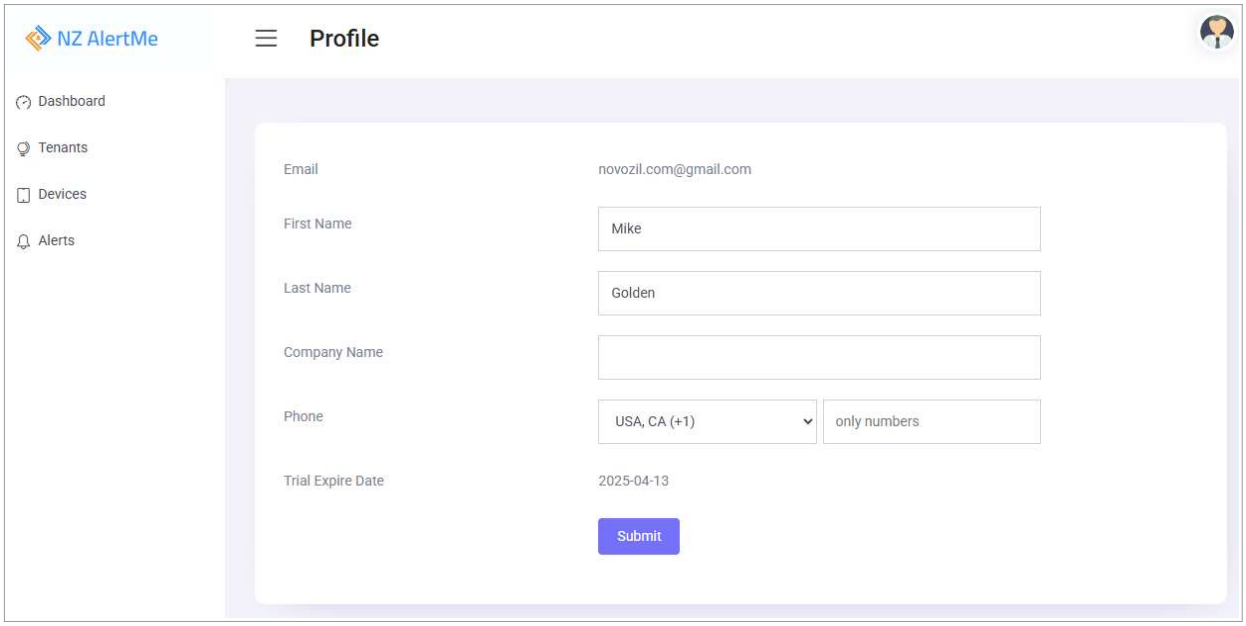


Alerts

The NovoZil AlertMe Agent monitors firewalls (SonicWall, FortiGate, Sophos) and device availability using the ICMP/Ping protocol. When events are detected, the agent reports them to the NovoZil AlertMe Cloud Server, where they are displayed on the Alerts page for review. Simultaneously, notifications are sent through the subscribed channels, SMS, Email, or the Telegram application.

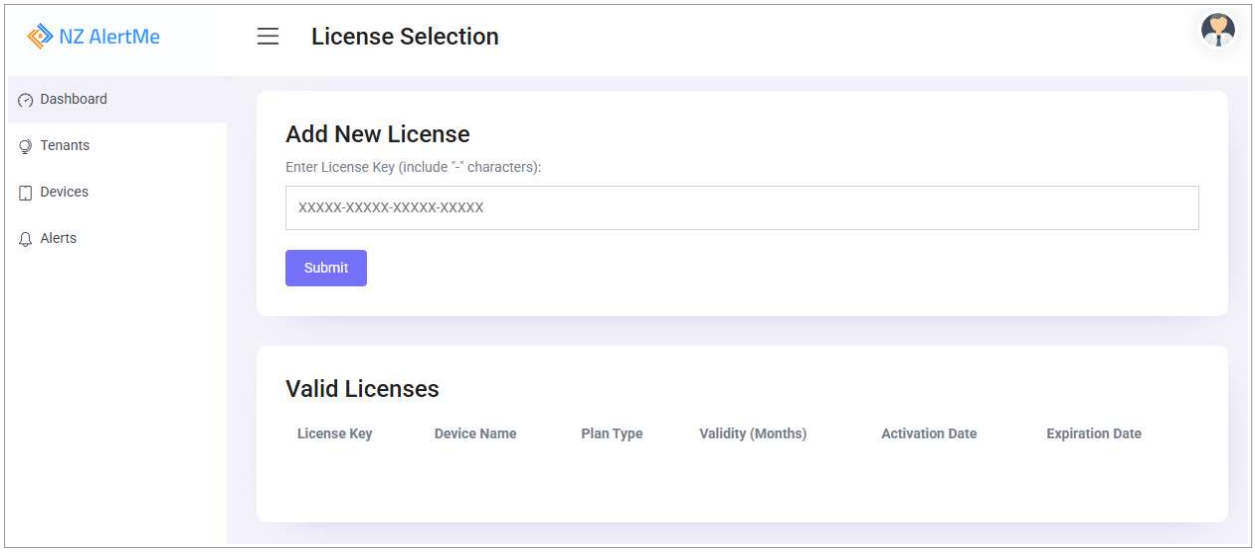
Profile

Under the Profile menu, the following data fields can be updated.



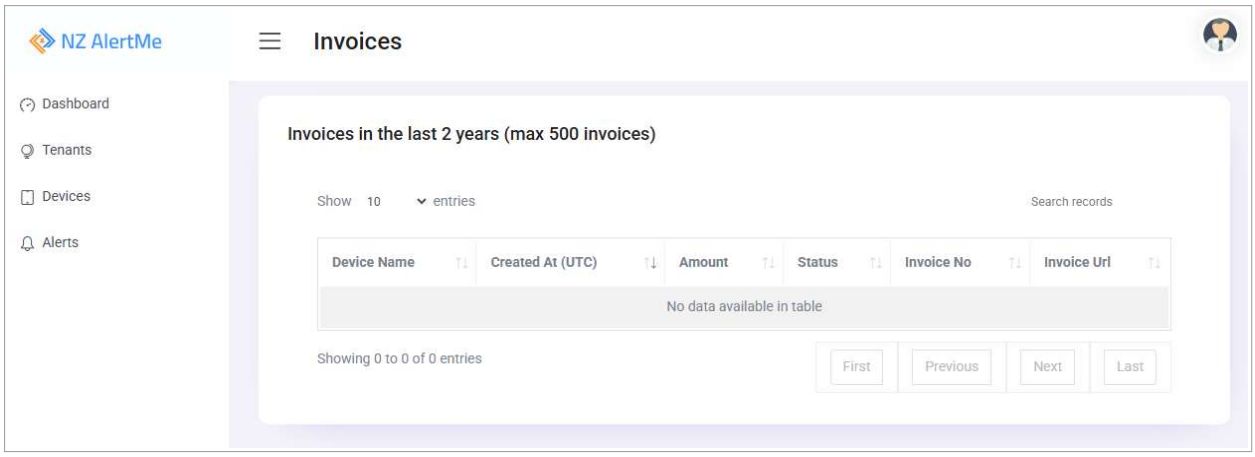
Licenses

NovoZil AlertMe service is provided based on subscription or licensing. Once the license is purchased, it can be entered from this page. Once a valid license is submitted, it can be associated to a device to function properly.



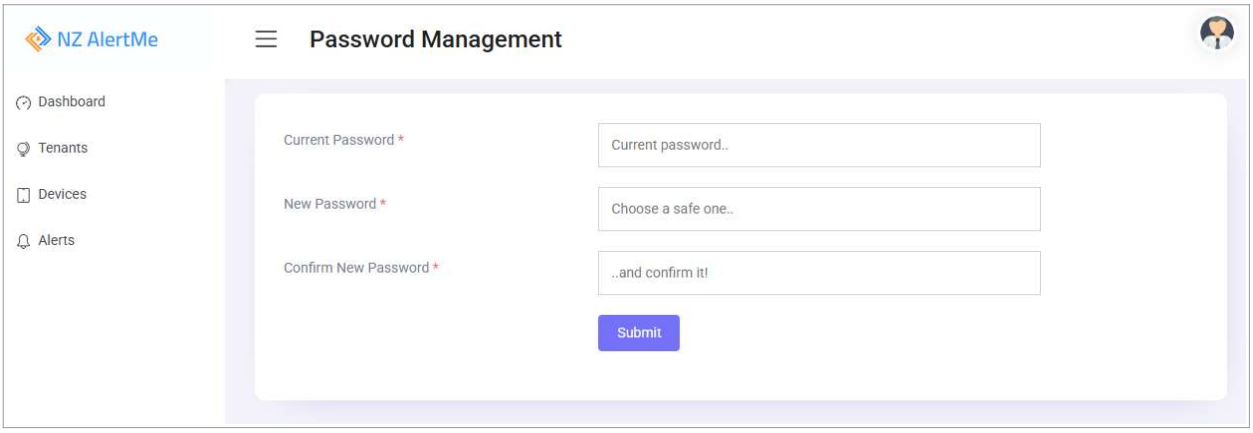
Invoices

Invoices for the account are accessible on this page.



Change Password

The account password can be changed on this page.



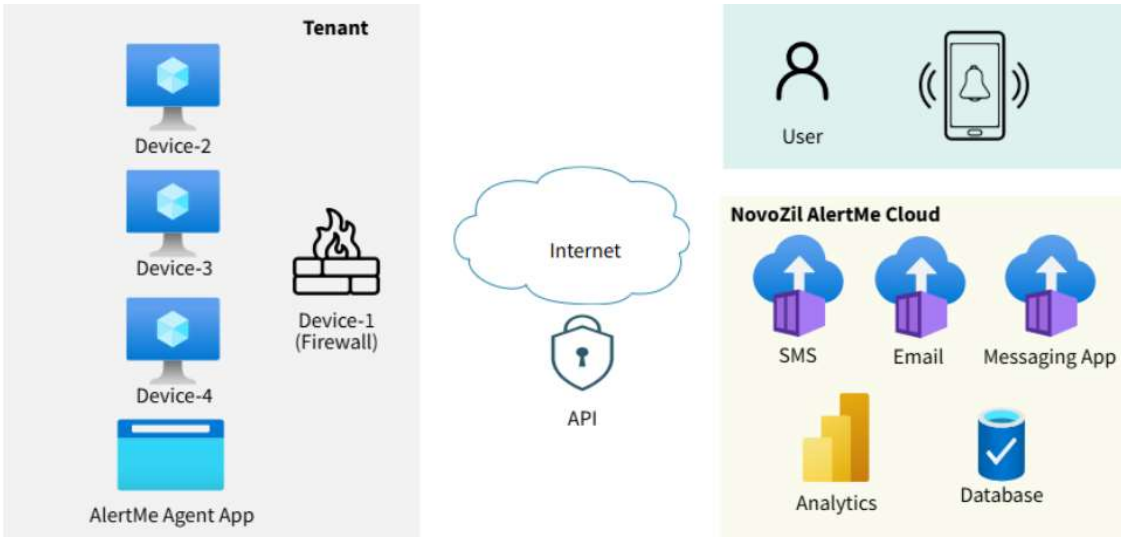
Logout

This will logout the user from the NovoZil AlertMe portal.

NovoZil AlertMe Agent

Introduction

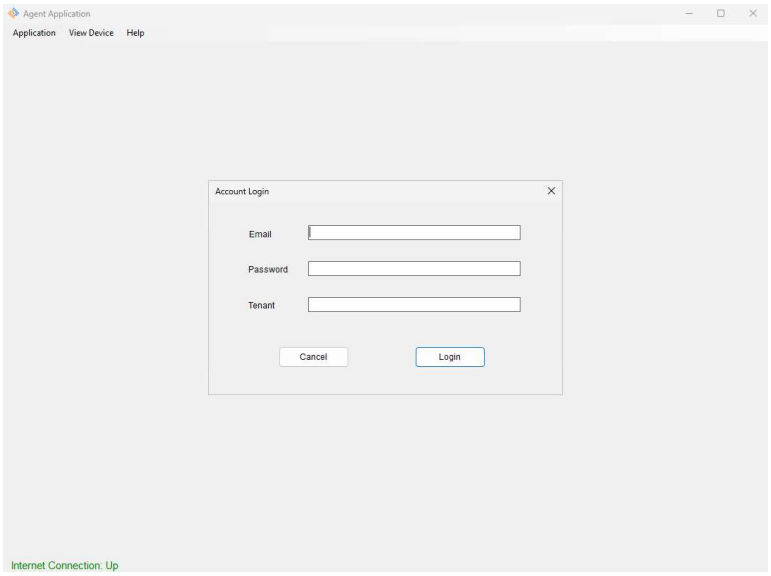
The NovoZil AlertMe Agent runs on the client's network on Windows 11 host, receiving UDP Syslog messages from various devices (SonicWall, FortiGate, Sophos firewalls) and filtering relevant security and operational events. These filtered messages are then securely transmitted to the NovoZil Cloud Portal. The portal not only provides an intuitive interface for monitoring Syslog alerts but also enables instant notifications via SMS, email, or Telegram, ensuring that IT staff members stay informed of critical events in real time.



Running The Application

For detailed installation instructions, please refer to the NovoZil AlertMe Agent Installation Guide.

After successful installation, a shortcut to the application will appear on the Windows desktop. Double-clicking this shortcut will launch the application and prompt the user to enter their account login credentials.



The main menu bar includes the following options: Application, View Device, and Help.

Under the Application menu, you will find:

- Login
- Registered Devices
- Settings
- Exit

The View Device menu displays the list of devices registered under the currently logged-in tenant.

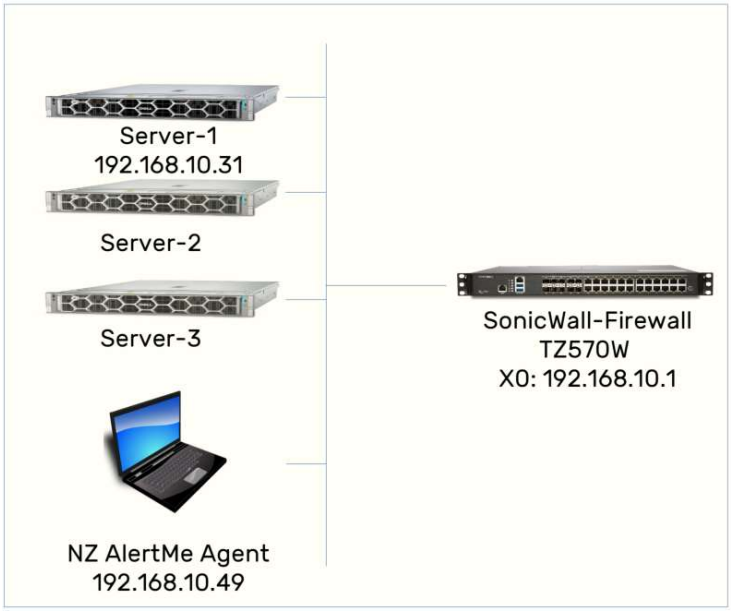
Before running the NovoZil AlertMe Agent application, ensure that the tenant and associated devices have been created on the NovoZil AlertMe Portal. Upon logging into the Agent application, all device configuration data for the selected tenant will be automatically retrieved from the portal.

Sample Configuration

To better understand the configuration process, this section walks through a sample use case.

In this scenario, our New York network environment includes a SonicWall firewall, three server instances, and a computer running the NovoZil AlertMe Agent. The objective is to process Syslog messages from the firewall and monitor the availability of Server-1 using the ICMP Ping protocol.

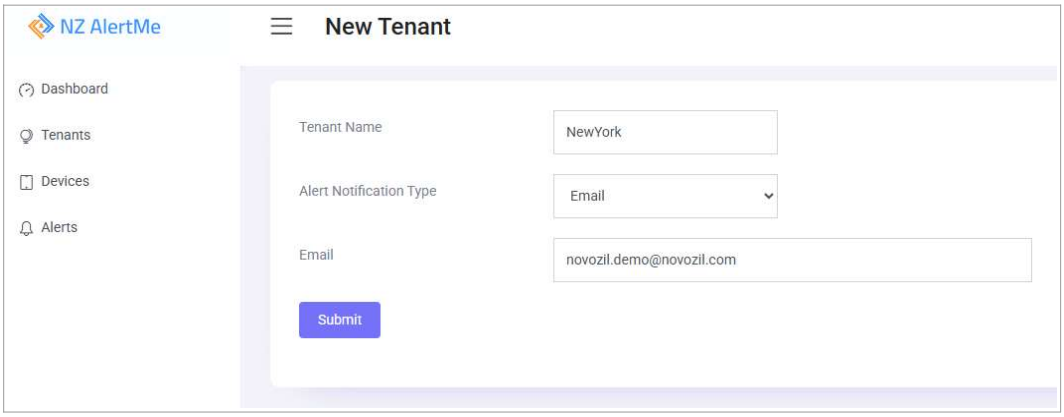
	Firewall	Server
Device Name	SW-TZ570W	Server-1
IP Address	192.168.10.1 (X0)	192.168.10.31
Communication Type	SonicWall Syslog	ICMP Ping
Syslog Port	UDP 514	Not Applicable



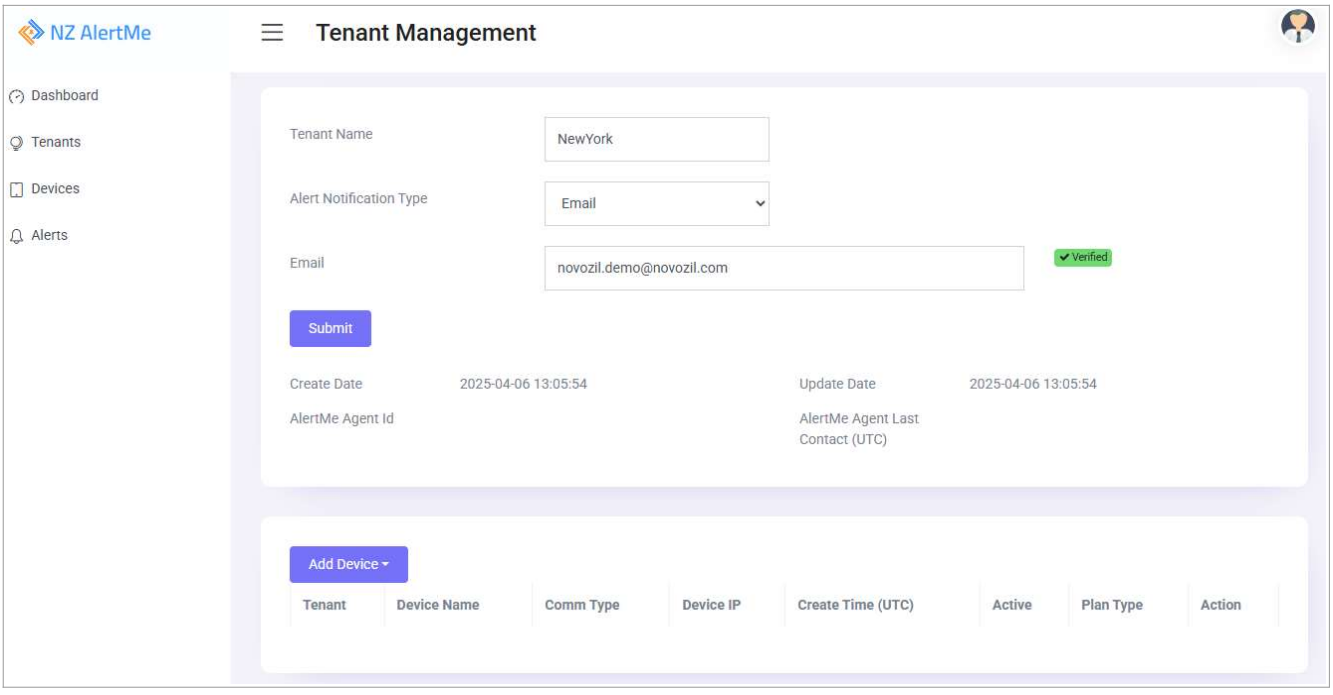
1. Creating New Tenant

Log in to the NovoZil AlertMe Portal at `https://alertme.novozil.com` and navigate to the `Tenants` menu to create a new tenant.

- Tenant Name: NewYork
- Alert Notification Type: Email
- Email: [The desired email address to receive notifications]



After submitting the form a verification code will be sent to your email. Enter the code to activate the tenant. Once verified, you should be redirected to the confirmation page showing a `Verified` status.



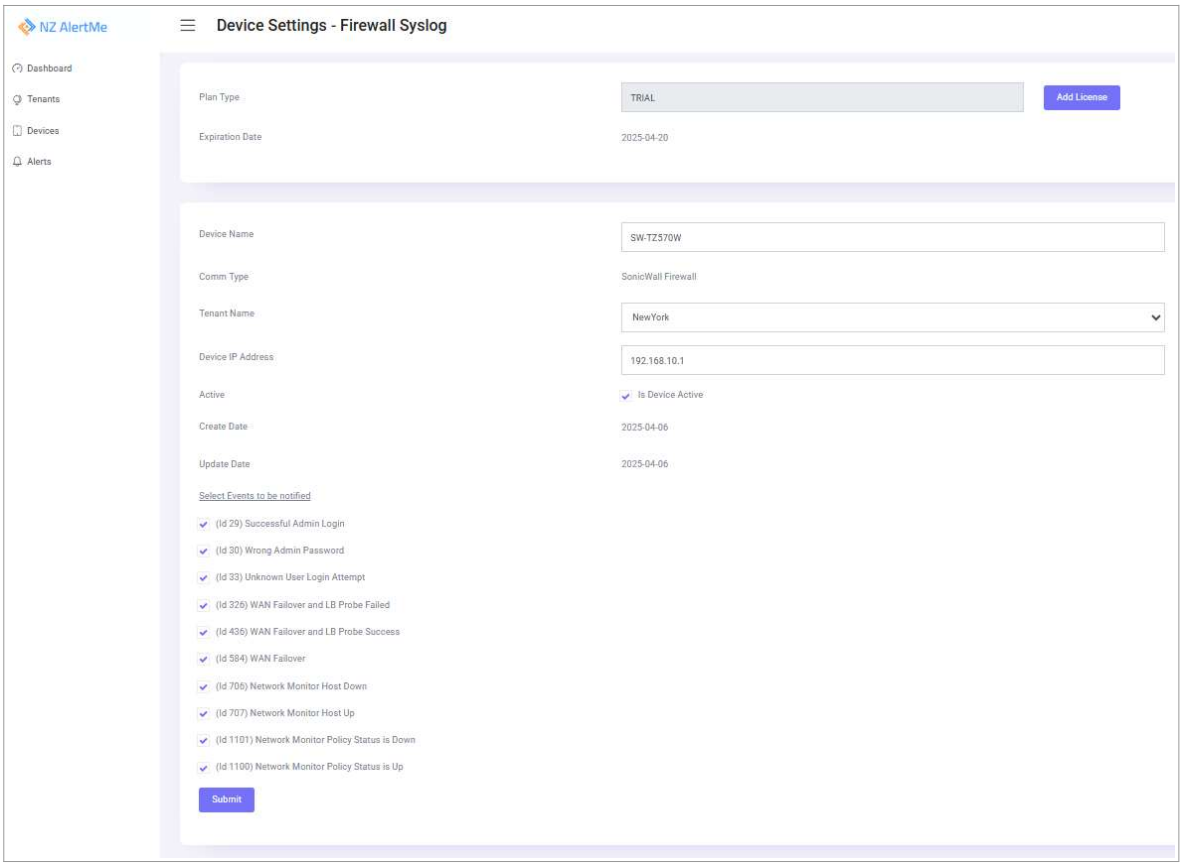
Now, we can add devices.

2. Adding Devices

In this scenario, we will add two devices. The order of addition does not matter.

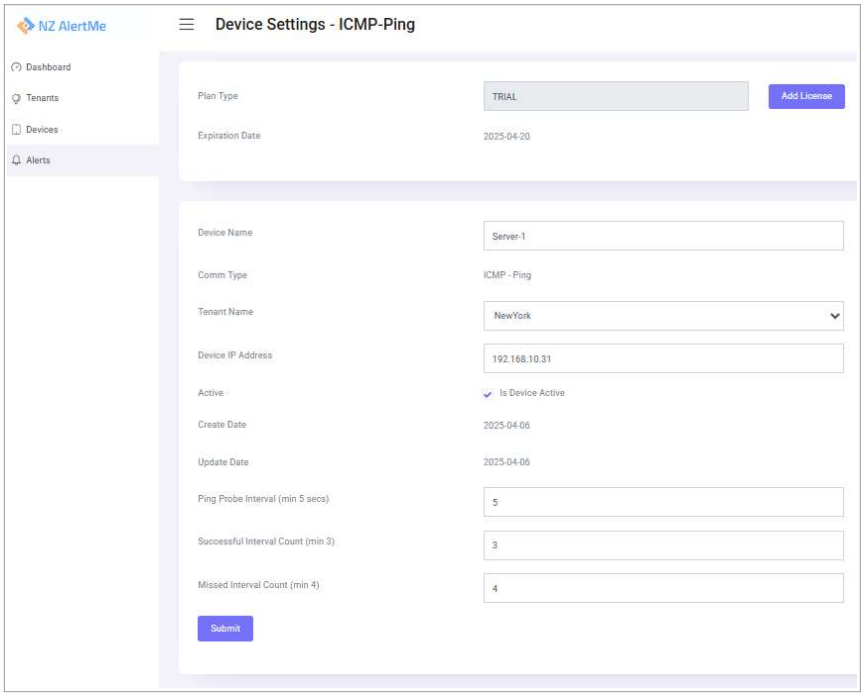
- First, we add the SW-TZ570W to monitor Syslog messages.
- Then, we add Server-1 to be monitored via ICMP Ping.

From the `Add Device` dropdown menu, select `SonicWall Firewall` and enter the required information based on your environment.



Please note that he NovoZil AlertMe Agent must be able to communicate with the specified Device IP. While the agent does not need to be on the same subnet as the target device, there must be a valid communication path between them.

Next, add `Server-1` by selecting `ICMP Ping` from the `Add Device` dropdown menu.

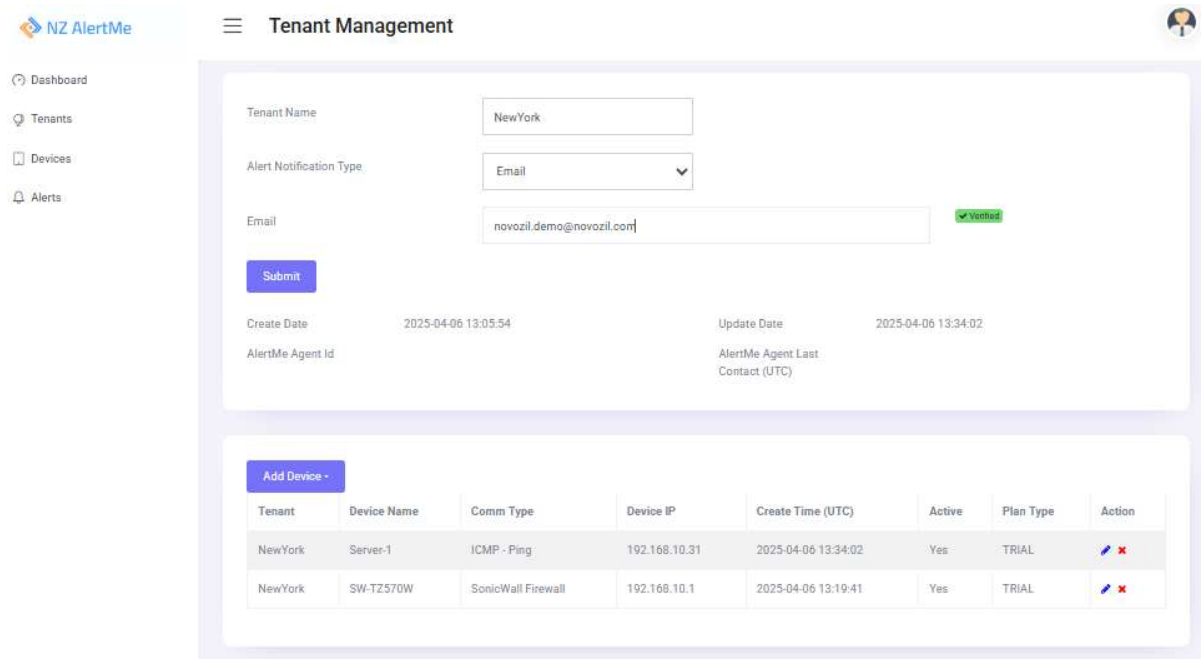


You may use the default values or adjust the following settings based on your monitoring requirements:

Ping Probe Interval: The frequency at which the system will send ICMP Ping requests to check the device's availability.

Successful Interval Count: The number of consecutive successful ping responses required to consider the device available.

Missed Interval Count: The number of consecutive missed ping responses before the device is considered unavailable.



To ensure successful monitoring and event reporting, the following configuration steps must be ensured:

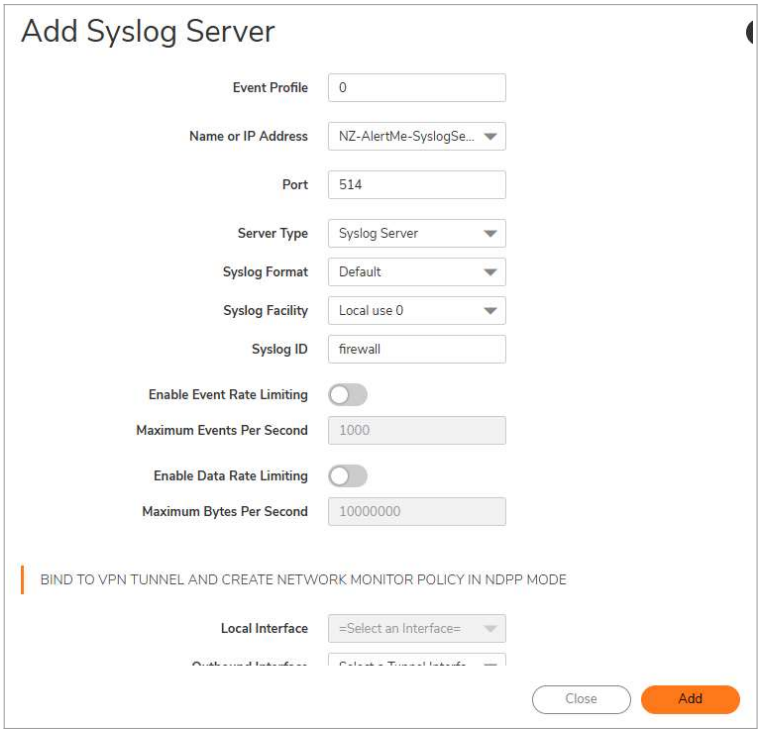
3. Network and Firewall Configuration Considerations

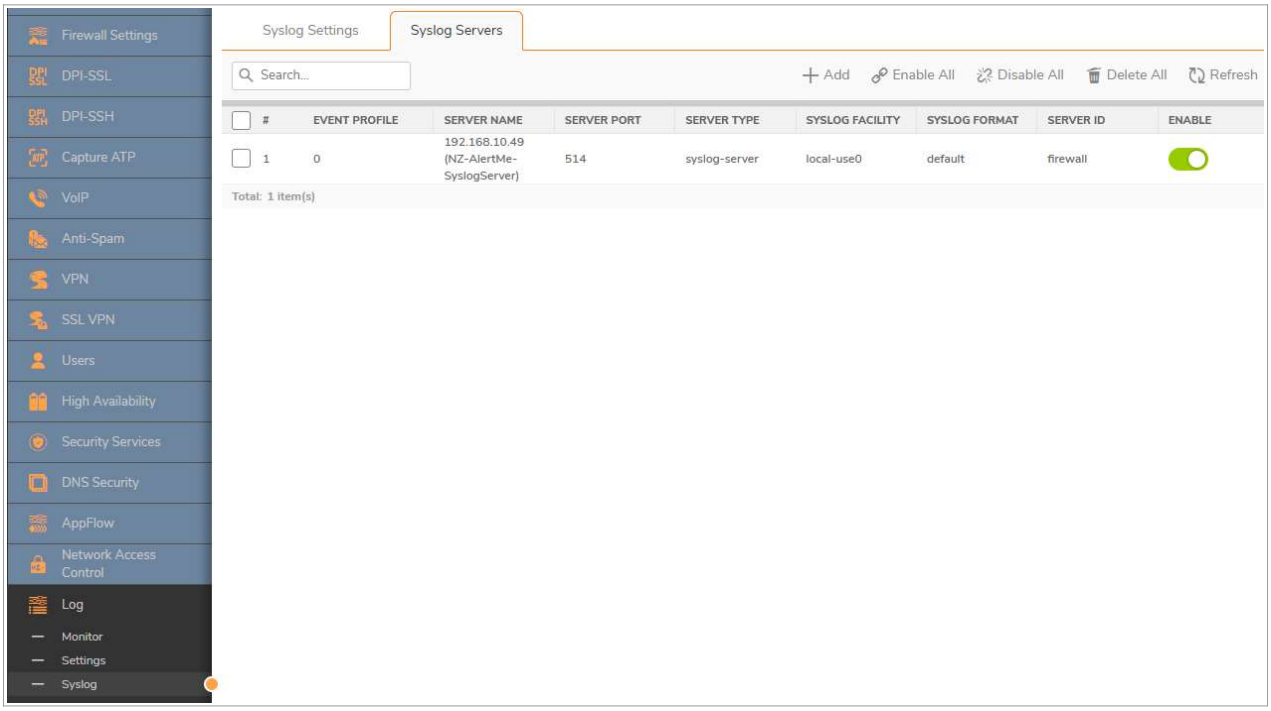
Confirm that ICMP Ping requests are not blocked by any antivirus software, Endpoint Detection and Response (EDR) tools, or the Windows Firewall on Server-1. ICMP must be allowed for the NovoZil AlertMe Agent to accurately monitor the device's availability.

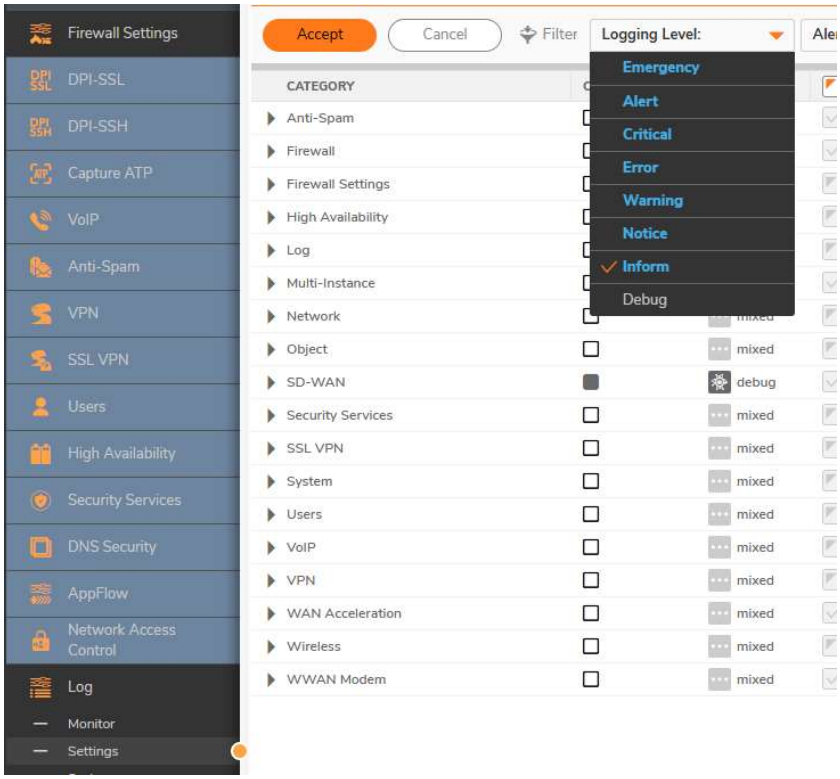
The NovoZil AlertMe Agent functions as a Syslog server, receiving and processing Syslog messages from supported firewalls. To configure the SonicWall firewall:

- Log in to the SonicWall firewall interface.
- Navigate to `Log > Syslog > Syslog Servers`.
- Click the `+` icon to add a new Syslog server.
- Create an Address Object that contains the IP address of the host machine running the NovoZil AlertMe Agent.
- Ensure the logging level is set to `Inform` to capture sufficient event detail.

These steps are essential to establish communication between the firewall and the agent, allowing for accurate event logging and real-time alerting.

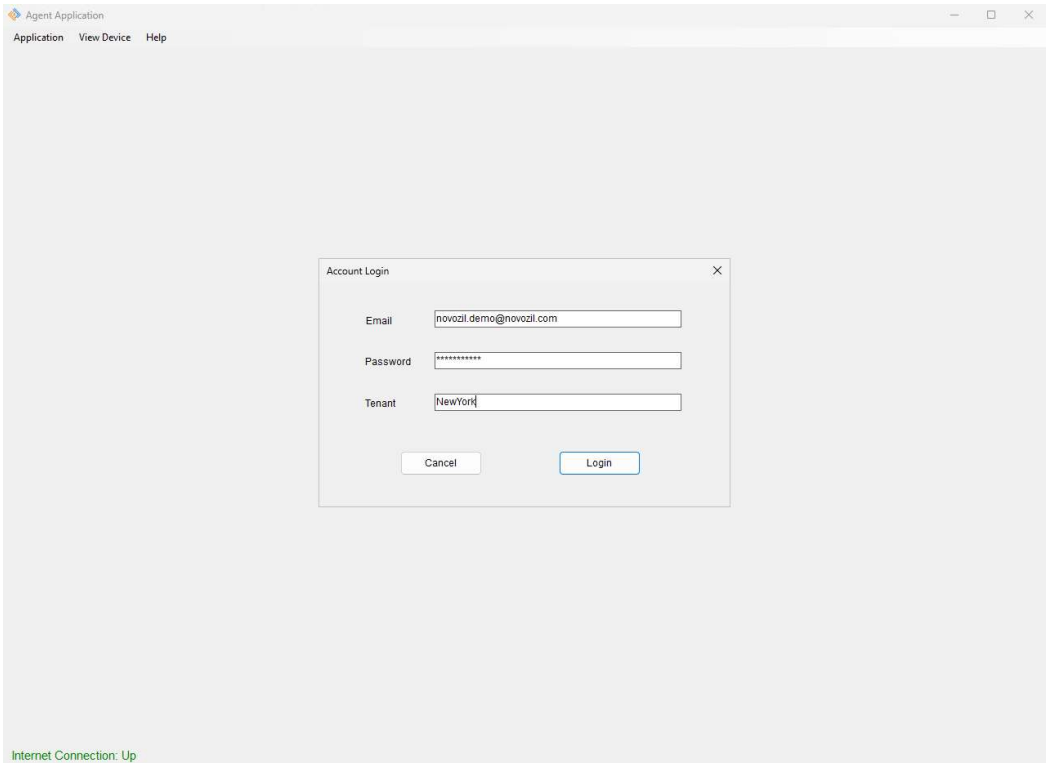




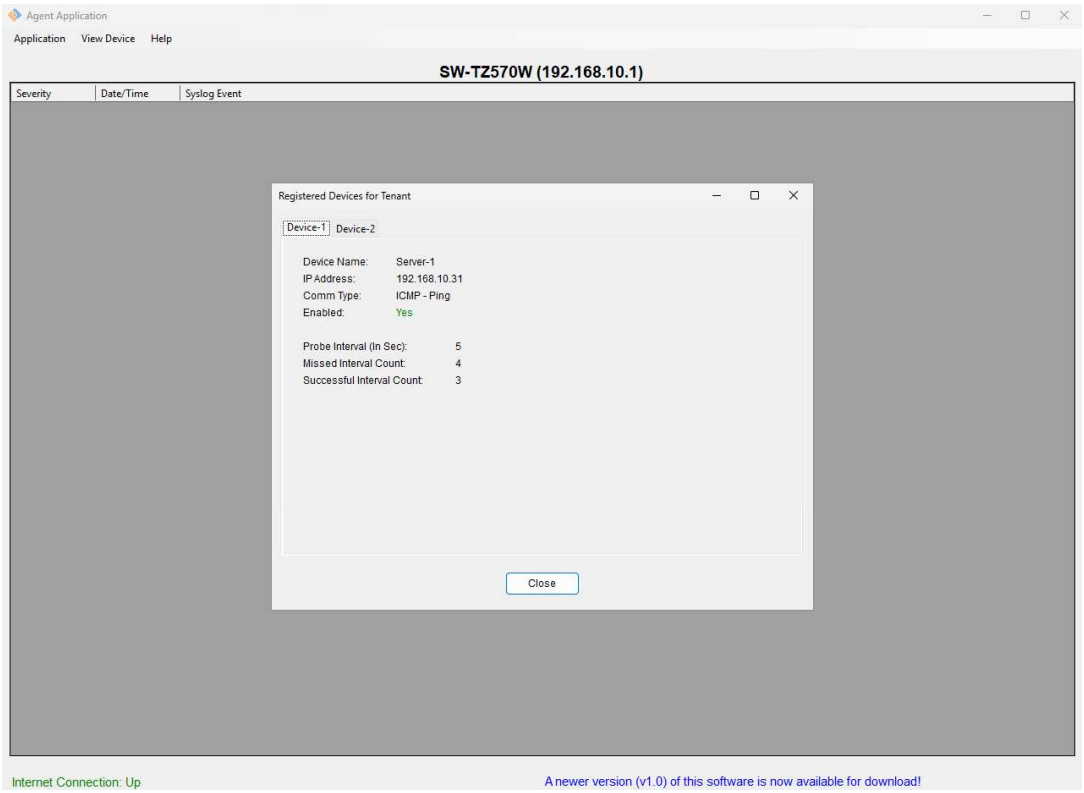


4. NovoZil AlertMe Agent Application

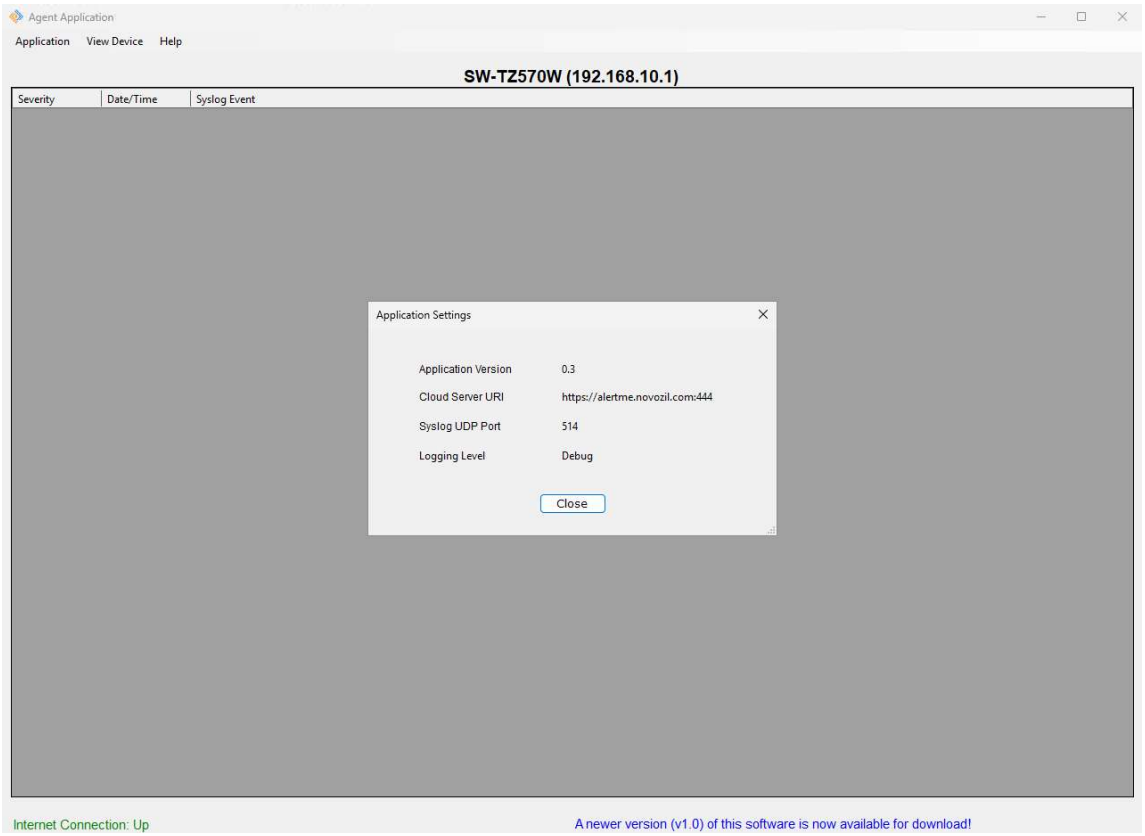
Run the NovoZil AlertMe Agent and enter the credentials, including the tenant name.



Go to `Application > Registered Devices`, which will display the registered devices under the tenant `NewYork`.



Go to `Application > Settings`, which will display the general settings of the application.



The `View Device` menu will have sub-menus for each defined device. If the device communication type is Syslog, it will display the messages that are captured. If the device communicate type is ICMP-Ping then it will display the ping responses in a bar-graph.