



NovoZil AlertMe

USER MANUAL

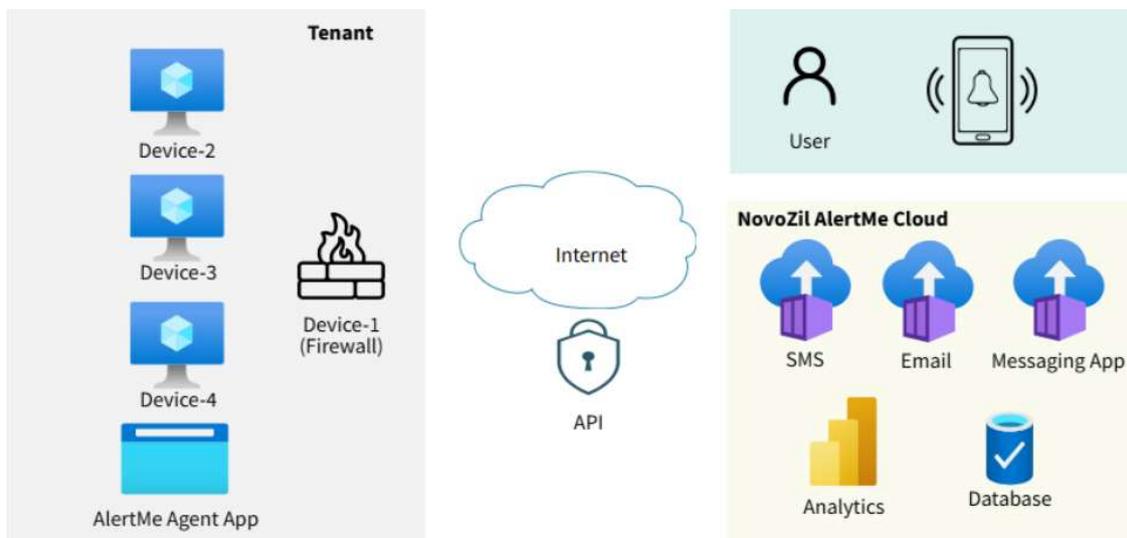


NovoZil AlertMe Portal

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.

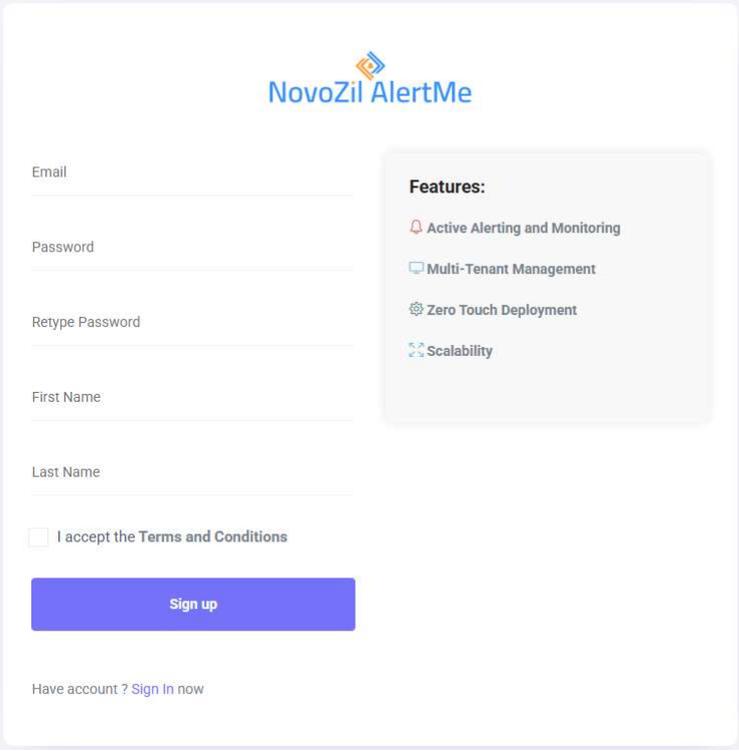
Seamless Scalability: Grow your business effortlessly with NovoZil's scalable multi-tenant architecture, supporting expansion for both end customers and MSPs.

Pre-Requisites

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

Signing Up

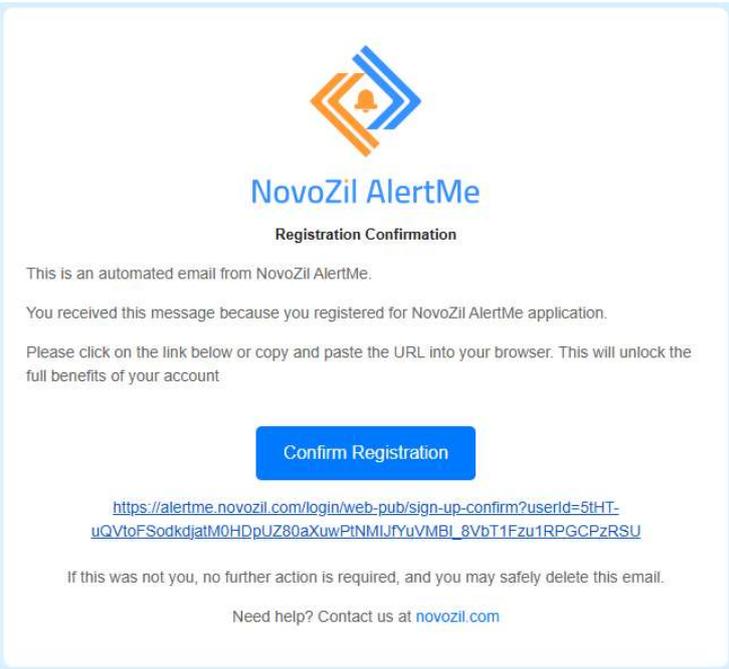
Open your browser and navigate to <https://alertme.novozil.com>. Click on the Sign Up option and complete the required fields. After submitting the form, you will receive an email to verify your account.



The image shows the NovoZil AlertMe sign-up form. It features a logo at the top center. Below the logo are input fields for Email, Password, Retype Password, First Name, and Last Name. To the right of these fields is a 'Features' box listing: Active Alerting and Monitoring, Multi-Tenant Management, Zero Touch Deployment, and Scalability. Below the input fields is a checkbox for 'I accept the Terms and Conditions' and a blue 'Sign up' button. At the bottom left, there is a link: 'Have account? Sign In now'.

Registration Confirmation

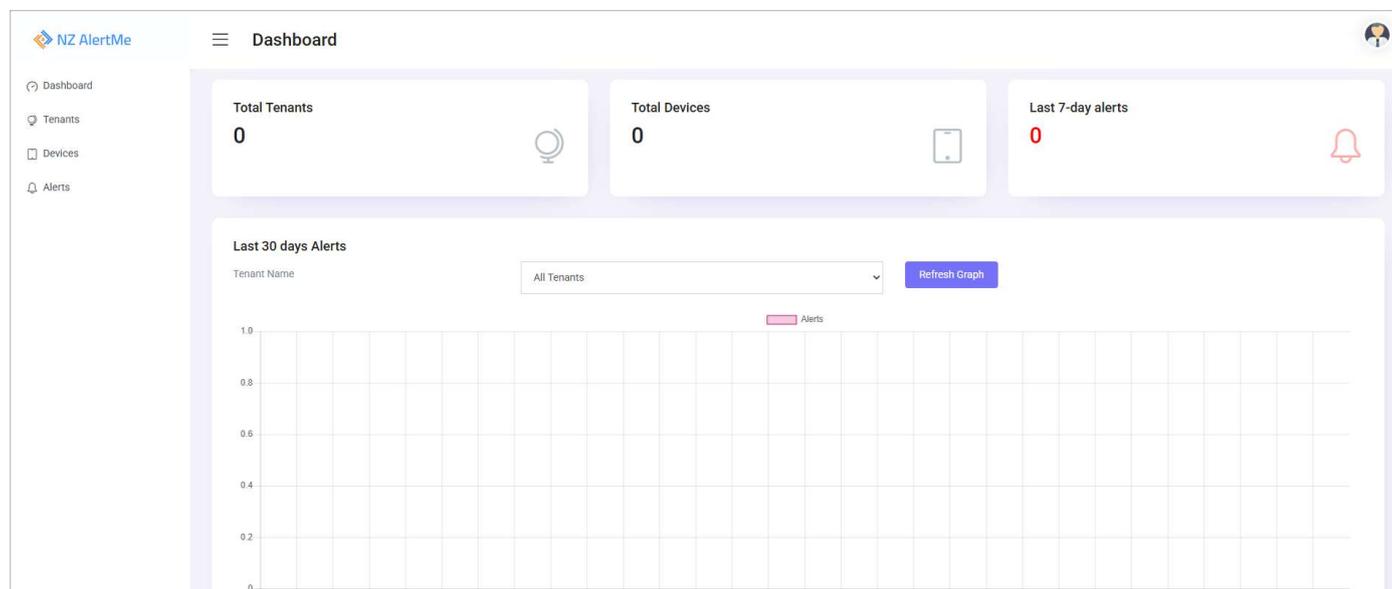
After signing up, you will receive an email to complete your registration.



The image shows a registration confirmation email from NovoZil AlertMe. It features the NovoZil AlertMe logo at the top center. Below the logo is the text 'Registration Confirmation'. The email body contains the following text: 'This is an automated email from NovoZil AlertMe.', 'You received this message because you registered for NovoZil AlertMe application.', and 'Please click on the link below or copy and paste the URL into your browser. This will unlock the full benefits of your account'. Below this text is a blue button labeled 'Confirm Registration'. Underneath the button is a long URL: https://alertme.novozil.com/login/web-pub/sign-up-confirm?userId=5tHT-uQVtoFSodkdjatM0HDpUJZ80aXuwPtNMIJFYuVMBI_8VbT1Fzu1RPGCPzRSU. At the bottom, there is a note: 'If this was not you, no further action is required, and you may safely delete this email.' and a link: 'Need help? Contact us at novozil.com'.

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.

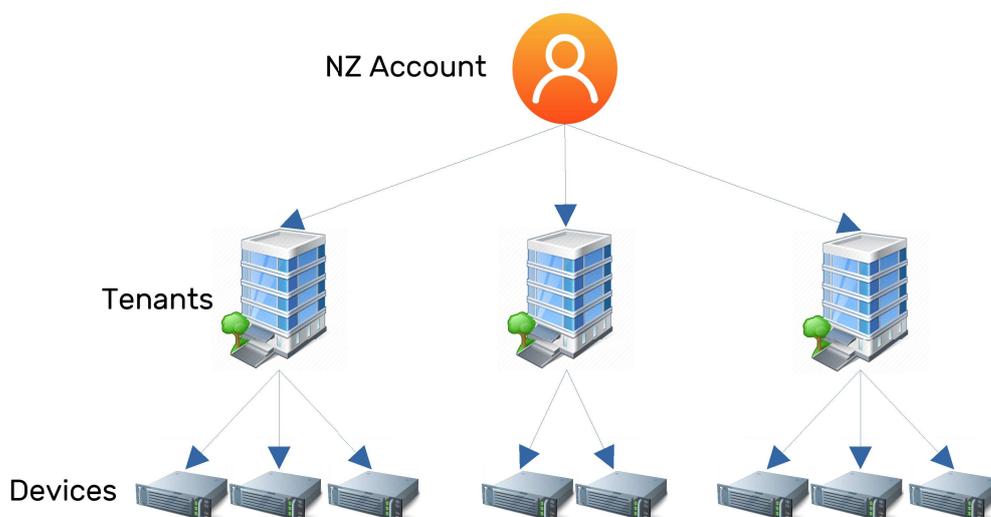
Invoices: This section displays processed invoices, which can be viewed or downloaded.

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.

The screenshot shows a web form titled "New Tenant". It contains the following fields and options:

- Tenant Name:** A text input field containing "NewYork".
- Alert Notification Type:** A dropdown menu with "SMS" selected.
- Phone:** A dropdown menu with "USA, CA (+1)" selected, and an adjacent text input field containing "only numbers".
- Submit:** A blue button.

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.

The screenshot shows a web form titled "New Tenant". It contains the following fields and options:

- Tenant Name:** A text input field containing "NewYork".
- Alert Notification Type:** A dropdown menu with "Email" selected.
- Email:** A text input field containing "Enter email".
- Submit:** A blue button.

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.

New Tenant

Tenant Name:

Alert Notification Type:

Telegram Chat ID:
[telegram instructions](#)

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.

Tenants

Tenant Name	Created At (UTC)	AlertMe Agent	AlertMe Agent Last Contact (UTC)	Device Count	Action
NewYork	2025-04-02	x		0	

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.

Devices

- ICMP-Ping
- SonicWall Firewall
- FortiGate Firewall
- Sophos Firewall

Name	Comm Type	Device IP	Create Time (UTC)	Active	Plan Type	Action
------	-----------	-----------	-------------------	--------	-----------	--------

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).

The screenshot shows the 'Device Settings - ICMP-Ping' configuration page in the NovoZil AlertMe interface. The page is divided into a sidebar and a main content area. The sidebar contains navigation links for Dashboard, Tenants, Devices, and Alerts. The main content area displays the following configuration fields:

- Plan Type:** TRIAL (with an 'Add License' button)
- Expiration Date:** 2025-04-17
- Device Name:** Server-1
- Comm Type:** ICMP - Ping
- Tenant Name:** NewYork (dropdown menu)
- Device IP Address:** 192.168.10.121
- Active:** Is Device Active
- Create Date:** 2025-04-03
- Update Date:** 2025-04-03
- Ping Probe Interval (min 5 secs):** 5
- Successful Interval Count (min 3):** 3
- Missed Interval Count (min 4):** 5

A 'Submit' button is located at the bottom left of the form.

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

Device Settings - Firewall Syslog

Plan Type: TRIAL Add License

Expiration Date: 2025-04-17

Device Name: NSA2700

Comm Type: SonicWall Firewall

Tenant Name: New York

Device IP Address: 192.168.10.1

Active: Is Device Active

Create Date: 2025-04-03

Update Date: 2025-04-03

Select Events to be notified

- (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

Submit

Please 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.

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG
Anti-Spam			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall Settings			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
High Availability			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Log			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Multi-Instance			mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Network			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Object			mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SD-WAN		debug		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security Services			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SSL VPN			mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
System			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Users			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Access			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Disconnect Detected	Black	24	inform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Successful Admin Login	Black	29	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Wrong Admin Password	Red	30	alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Successful User Login	Black	31	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Wrong User Password	Black	32	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Unknown User Login Attempt	Black	33	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Login Timeout	Black	34	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Admin Login Disabled	Red	35	alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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



NZ AlertMe Device Settings - Firewall Syslog

Dashboard
Tenants
Devices
Alerts

Plan Type: TRIAL [Add License](#)

Expiration Date: 2025-04-17

Device Name: FGMain

Comm Type: FortiGate Firewall

Tenant Name: NewYork

Device IP Address: 192.168.11.1

Active: Is Device Active

Create Date: 2025-04-03

Update Date: 2025-04-03

Select Events to be notified

- (Id 22105) Power supply failed
- (Id 22106) 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

[Submit](#)

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

NZ AlertMe Device Settings - Firewall Syslog

Plan Type: TRIAL [Add License](#)

Expiration Date: 2025-04-17

Device Name: SophosMainFW

Comm Type: Sophos Firewall

Tenant Name: NewYork

Device IP Address: 192.168.12.1

Active: Is Device Active

Create Date: 2025-04-03

Update Date: 2025-04-03

Select Events to be notified

- (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

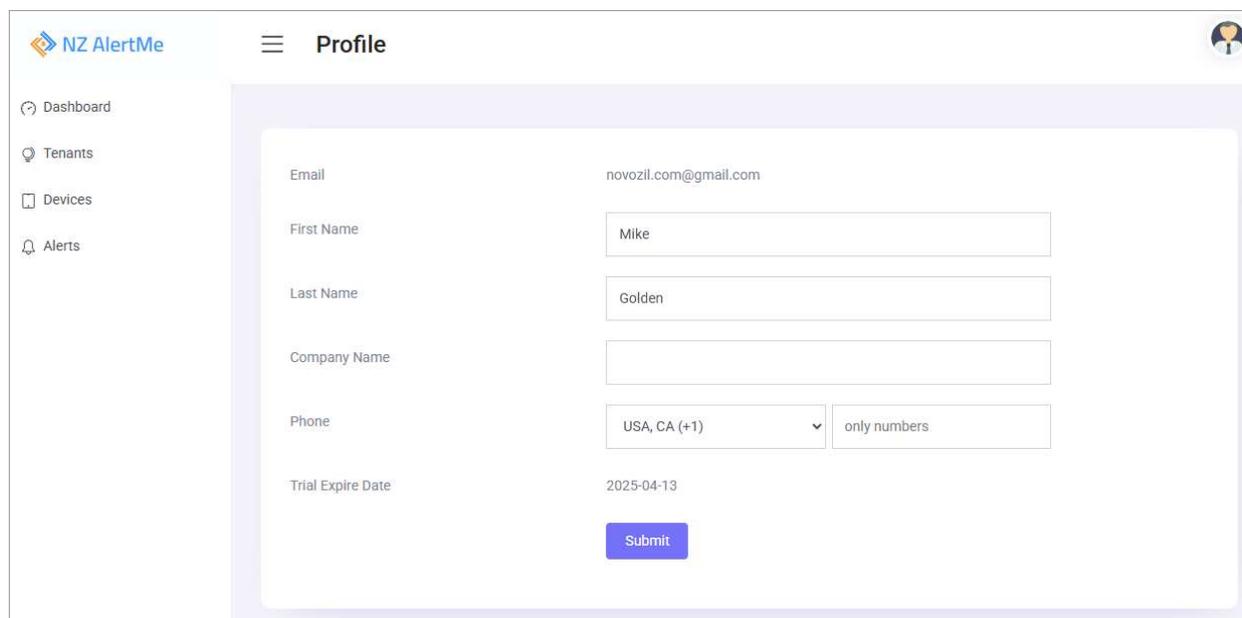
[Submit](#)

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.



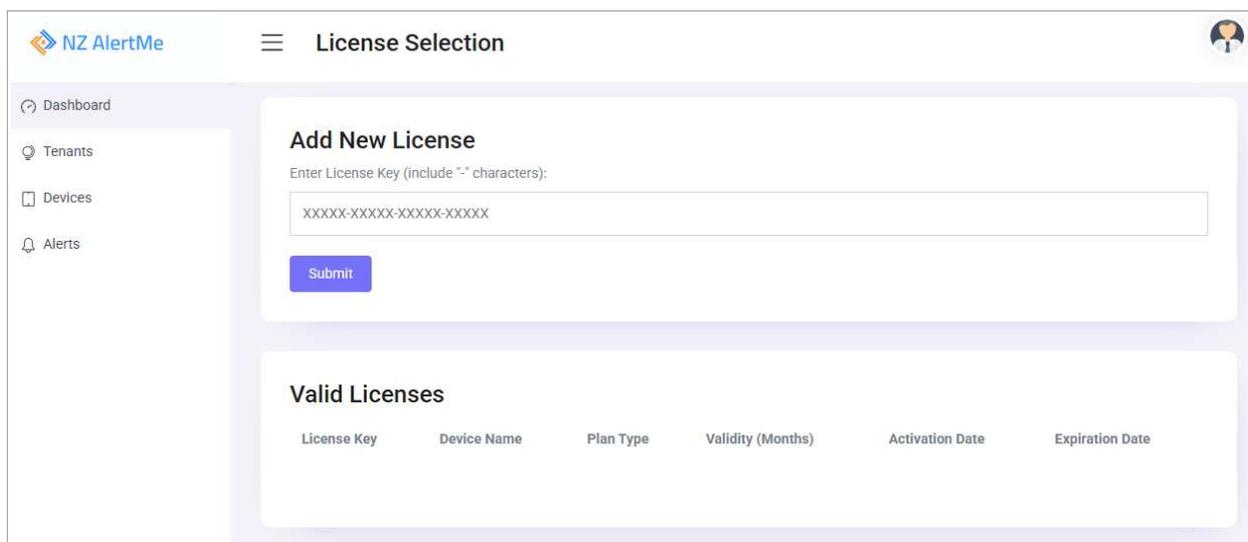
The screenshot shows the 'Profile' page in the NZ AlertMe application. The page has a sidebar with navigation links: Dashboard, Tenants, Devices, and Alerts. The main content area contains a form with the following fields:

- Email:** novozil.com@gmail.com
- First Name:** Mike
- Last Name:** Golden
- Company Name:** (empty field)
- Phone:** USA, CA (+1) (dropdown menu) and only numbers (input field)
- Trial Expire Date:** 2025-04-13

A blue 'Submit' button is located at the bottom of the form.

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.

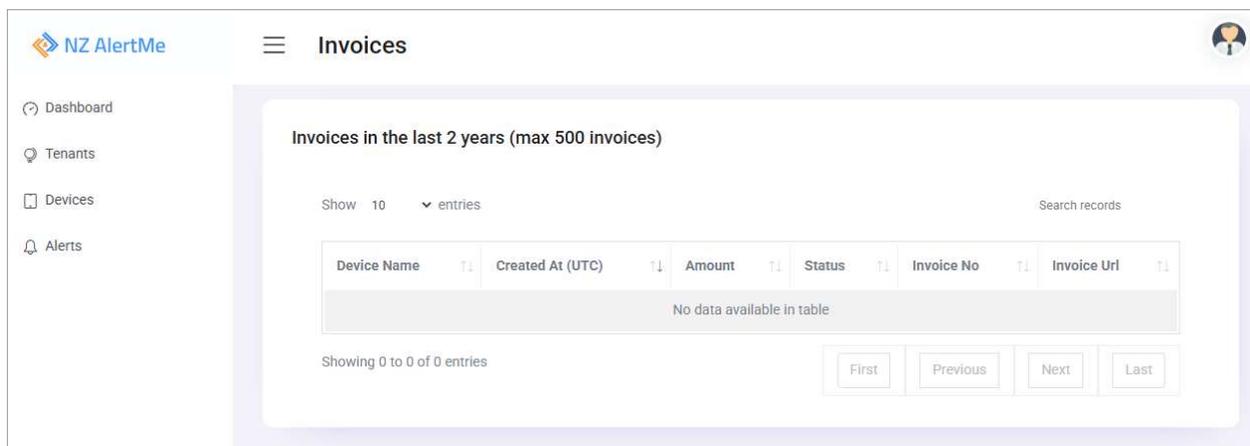


The screenshot shows the 'License Selection' page in the NZ AlertMe application. The page has a sidebar with navigation links: Dashboard, Tenants, Devices, and Alerts. The main content area contains two sections:

- Add New License:** A form with a text input field for the license key (placeholder: XXXXX-XXXXX-XXXXX-XXXXX) and a blue 'Submit' button.
- Valid Licenses:** A table with the following columns: License Key, Device Name, Plan Type, Validity (Months), Activation Date, and Expiration Date.

Invoices

Invoices for the account are accessible on this page.



NZ AlertMe Invoices

Invoices in the last 2 years (max 500 invoices)

Show 10 entries Search records

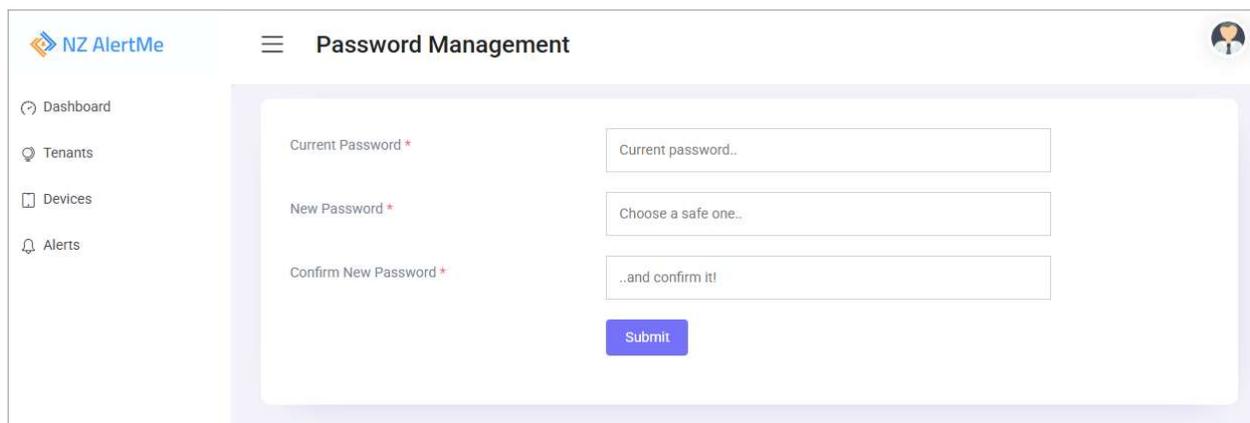
Device Name	Created At (UTC)	Amount	Status	Invoice No	Invoice Url
No data available in table					

Showing 0 to 0 of 0 entries

First Previous Next Last

Change Password

The account password can be changed on this page.



NZ AlertMe Password Management

Current Password *

New Password *

Confirm New Password *

Submit

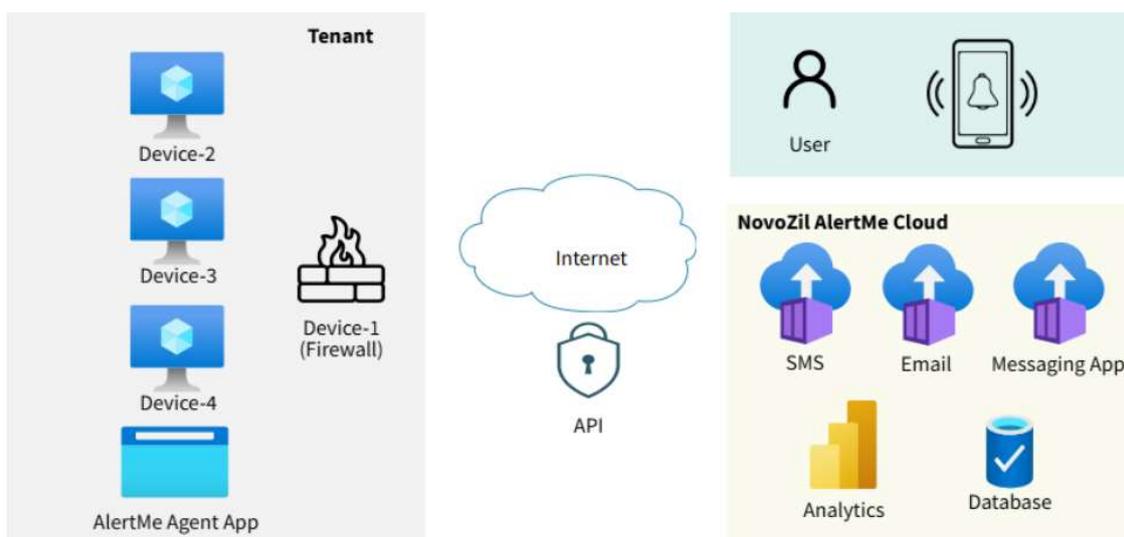
Logout

This will logout the user from the NovoZil AlertMe portal.

NovoZil AlertMe Agent

Introduction

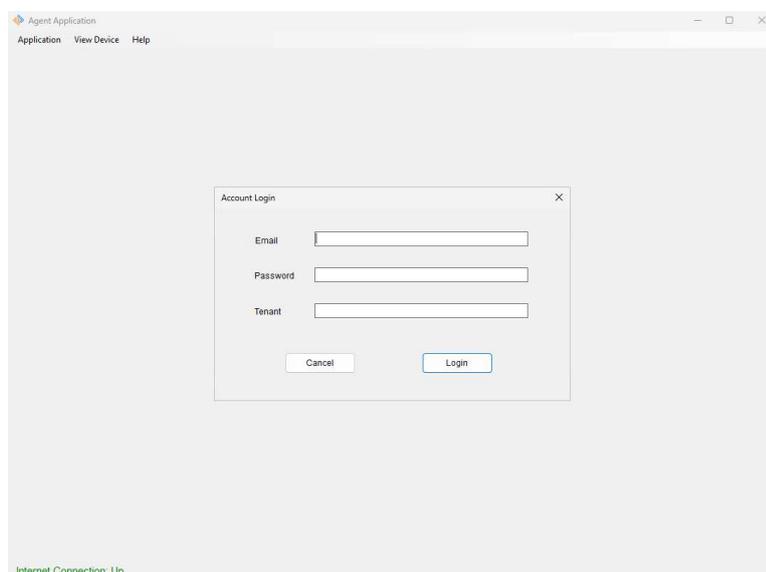
The NovoZil AlertMe Agent runs on the client's network on Windows 11 host, receiving UDP Syslog messages from various devices (SonicWall, FortiGate, Sophos firewalls) and filtering relevant security and operational events. These filtered messages are then securely transmitted to the NovoZil Cloud Portal. 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.

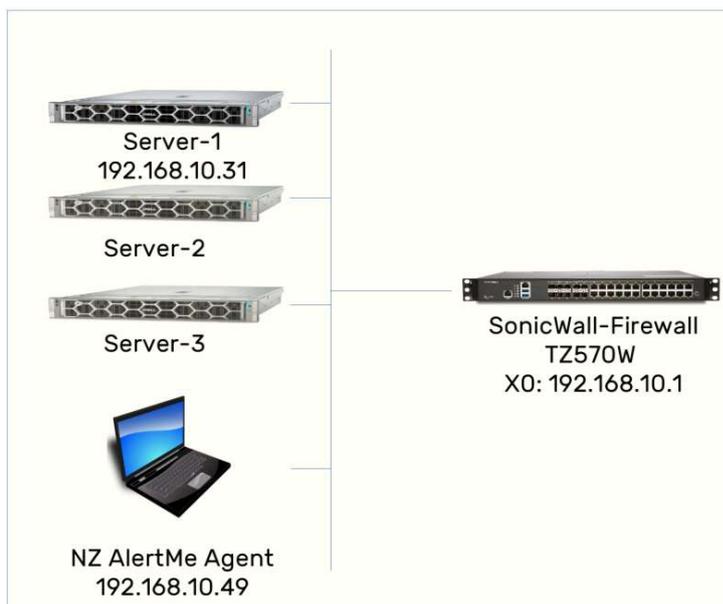
Before running the NovoZil AlertMe Agent application, ensure that the tenant and associated devices have been created on the NovoZil AlertMe Portal. Upon logging into the Agent application, all device configuration data for the selected tenant will be automatically retrieved from the portal.

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]

The screenshot shows the 'New Tenant' form in the NZ AlertMe portal. The form is titled 'New Tenant' and has a sidebar with navigation options: Dashboard, Tenants, Devices, and Alerts. The form fields are:

- Tenant Name: NewYork
- Alert Notification Type: Email
- Email: novozil.demo@novozil.com

A blue 'Submit' button is located below the form fields.

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.

The screenshot shows the 'Tenant Management' page in the NZ AlertMe portal. The page is titled 'Tenant Management' and has a sidebar with navigation options: Dashboard, Tenants, Devices, and Alerts. The page displays the details of the newly created tenant 'NewYork'.

The tenant details are:

- Tenant Name: NewYork
- Alert Notification Type: Email
- Email: novozil.demo@novozil.com (Verified)
- Create Date: 2025-04-06 13:05:54
- Update Date: 2025-04-06 13:05:54
- AlertMe Agent Id
- AlertMe Agent Last Contact (UTC)

An 'Add Device' button is located below the tenant details. Below the button is a table with the following columns:

Tenant	Device Name	Comm Type	Device IP	Create Time (UTC)	Active	Plan Type	Action
--------	-------------	-----------	-----------	-------------------	--------	-----------	--------

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.

The screenshot shows the 'Device Settings - Firewall Syslog' page in the NZ AlertMe interface. The page has a sidebar with navigation options: Dashboard, Tenants, Devices, and Alerts. The main content area contains the following fields and options:

- Plan Type:** TRIAL (with an 'Add License' button)
- Expiration Date:** 2025-04-20
- Device Name:** SW-TZ570W
- Connm Type:** SonicWall Firewall
- Tenant Name:** New York (dropdown menu)
- Device IP Address:** 192.168.10.1
- Active:** Is Device Active
- Create Date:** 2025-04-06
- Update Date:** 2025-04-06
- Select Events to be notified:** A list of events with checkboxes, all of which are checked:
 - (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
- Submit** button

Please note that the 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.

Device Settings - ICMP-Ping

Plan Type: TRIAL Add License

Expiration Date: 2025-04-20

Device Name: Server-1

Comm Type: ICMP - Ping

Tenant Name: New York

Device IP Address: 192.168.10.31

Active: Is Device Active

Create Date: 2025-04-06

Update Date: 2025-04-06

Ping Probe Interval (min 5 secs): 5

Successful Interval Count (min 3): 3

Missed Interval Count (min 4): 4

Submit

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.

Tenant Management

Tenant Name: New York

Alert Notification Type: Email

Email: novozil.demo@novozil.com ✓ Verified

Submit

Create Date: 2025-04-06 13:05:54 Update Date: 2025-04-06 13:34:02

AlertMe Agent Id: AlertMe Agent Last Contact (UTC)

Add Device -

Tenant	Device Name	Comm Type	Device IP	Create Time (UTC)	Active	Plan Type	Action
New York	Server-1	ICMP - Ping	192.168.10.31	2025-04-06 13:34:02	Yes	TRIAL	✎ ✖
New York	SW-TZ570W	SonicWall Firewall	192.168.10.1	2025-04-06 13:19:41	Yes	TRIAL	✎ ✖

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.

Add Syslog Server

Event Profile: 0

Name or IP Address: NZ-AlertMe-SyslogSe...

Port: 514

Server Type: Syslog Server

Syslog Format: Default

Syslog Facility: Local use 0

Syslog ID: firewall

Enable Event Rate Limiting:

Maximum Events Per Second: 1000

Enable Data Rate Limiting:

Maximum Bytes Per Second: 10000000

BIND TO VPN TUNNEL AND CREATE NETWORK MONITOR POLICY IN NDPP MODE

Local Interface: =Select an Interface=

Close Add

Syslog Settings Syslog Servers

Search...

+ Add Enable All Disable All Delete All Refresh

#	EVENT PROFILE	SERVER NAME	SERVER PORT	SERVER TYPE	SYSLOG FACILITY	SYSLOG FORMAT	SERVER ID	ENABLE
1	0	192.168.10.49 (NZ-AlertMe-SyslogServer)	514	syslog-server	local-use0	default	firewall	<input checked="" type="checkbox"/>

Total: 1 item(s)

- Firewall Settings
- DPI-SSL
- DPI-SSH
- Capture ATP
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Users
- High Availability
- Security Services
- DNS Security
- AppFlow
- Network Access Control
- Log
 - Monitor
 - Settings
 - Syslog

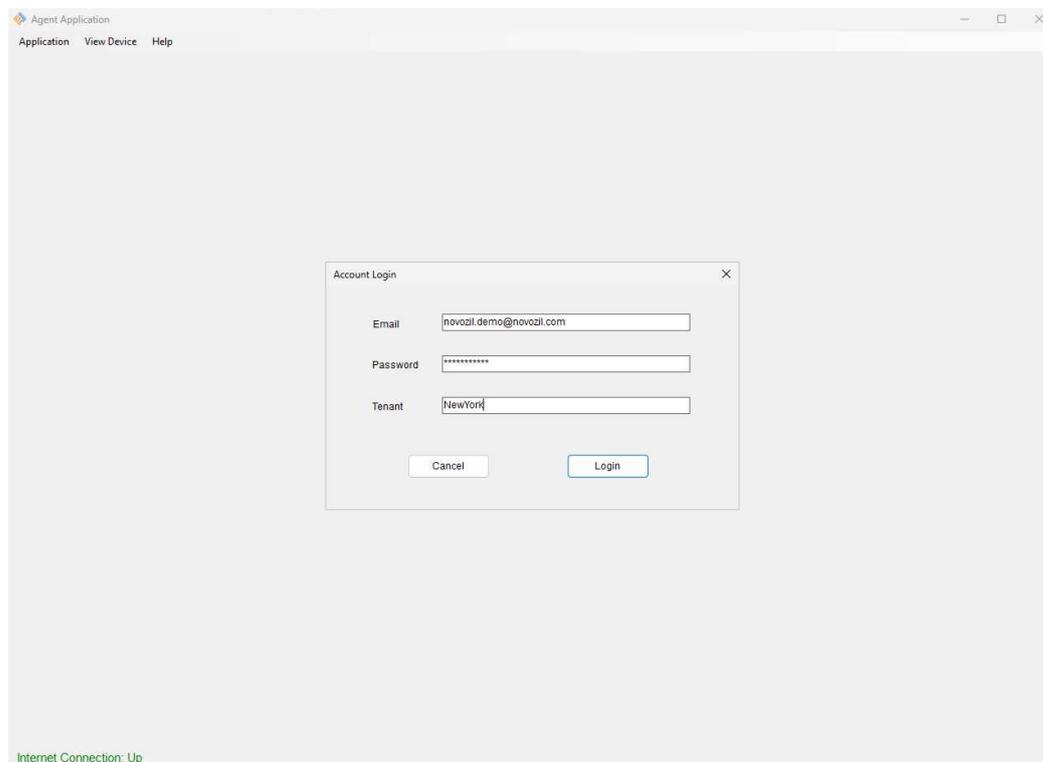
Accept Cancel Filter Logging Level: Alert

CATEGORY	Logging Level	Alert
▶ Anti-Spam		
▶ Firewall		
▶ Firewall Settings		
▶ High Availability		
▶ Log		
▶ Multi-Instance		
▶ Network		
▶ Object	mixed	
▶ SD-WAN	debug	
▶ Security Services	mixed	
▶ SSL VPN	mixed	
▶ System	mixed	
▶ Users	mixed	
▶ VoIP	mixed	
▶ VPN	mixed	
▶ WAN Acceleration	mixed	
▶ Wireless	mixed	
▶ WWAN Modem	mixed	

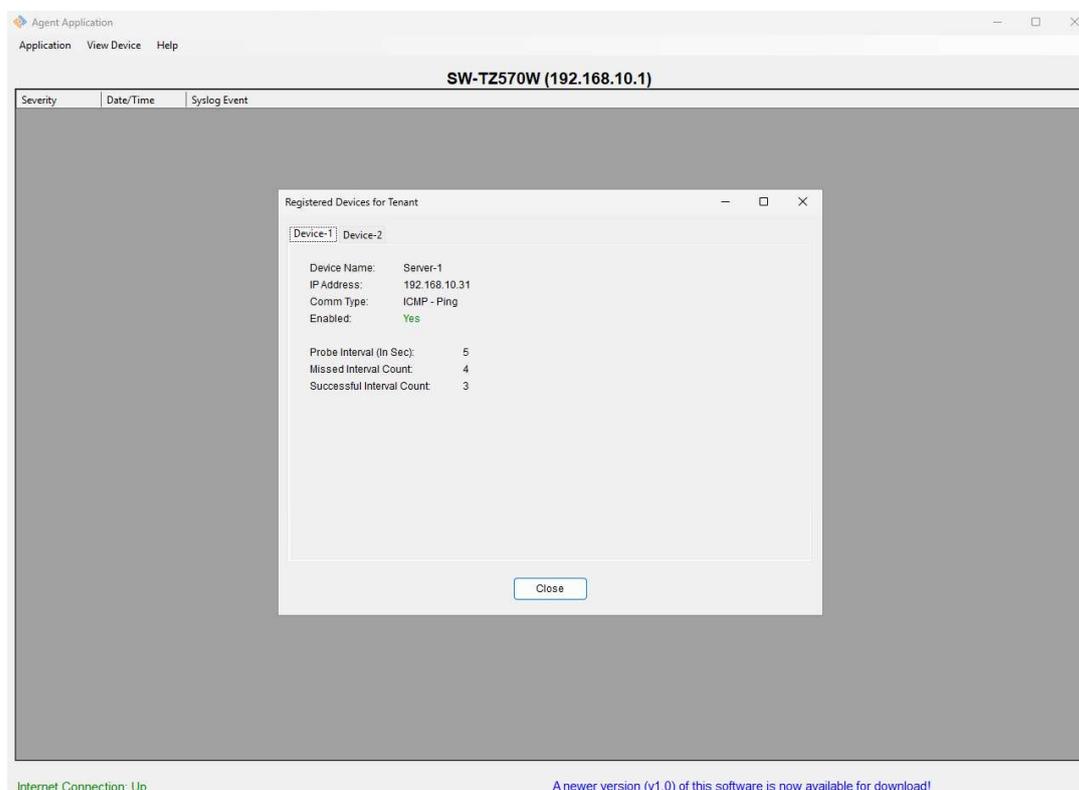
- Firewall Settings
- DPI-SSL
- DPI-SSH
- Capture ATP
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Users
- High Availability
- Security Services
- DNS Security
- AppFlow
- Network Access Control
- Log
 - Monitor
 - Settings

4. NovoZil AlertMe Agent Application

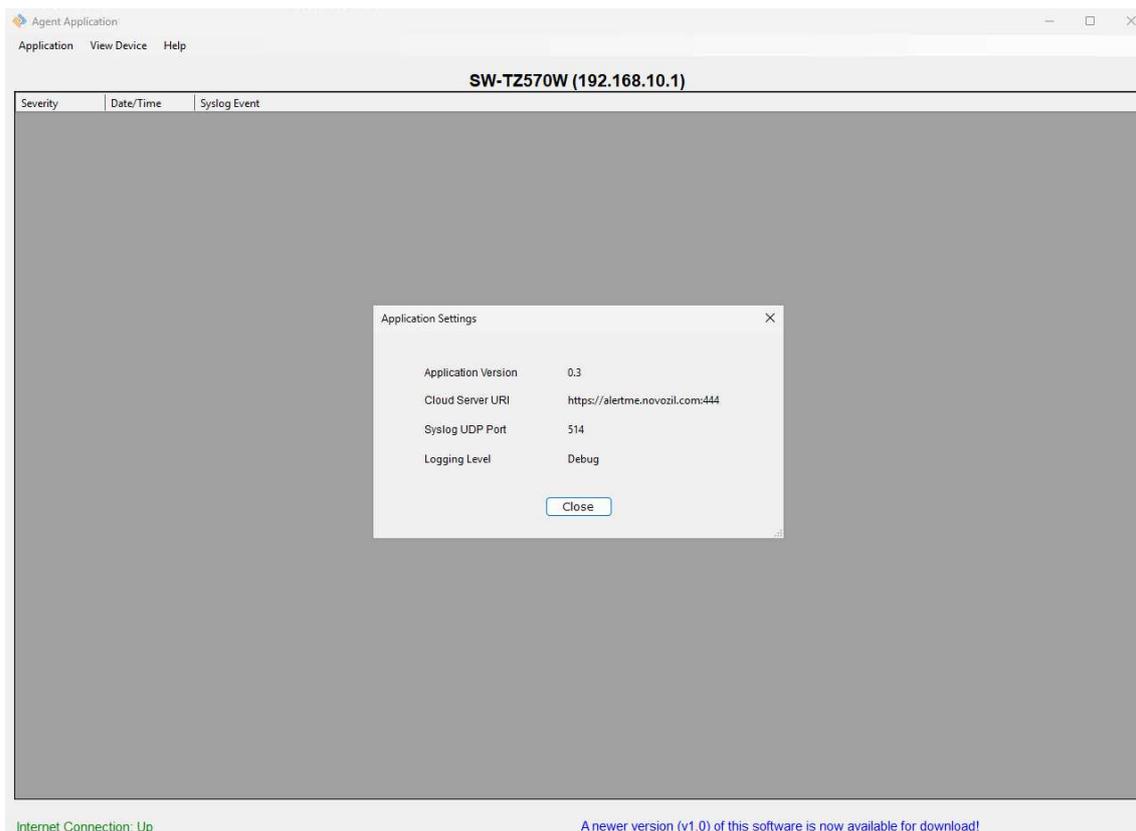
Run the NovoZil AlertMe Agent and enter the credentials, including the tenant name.



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.

