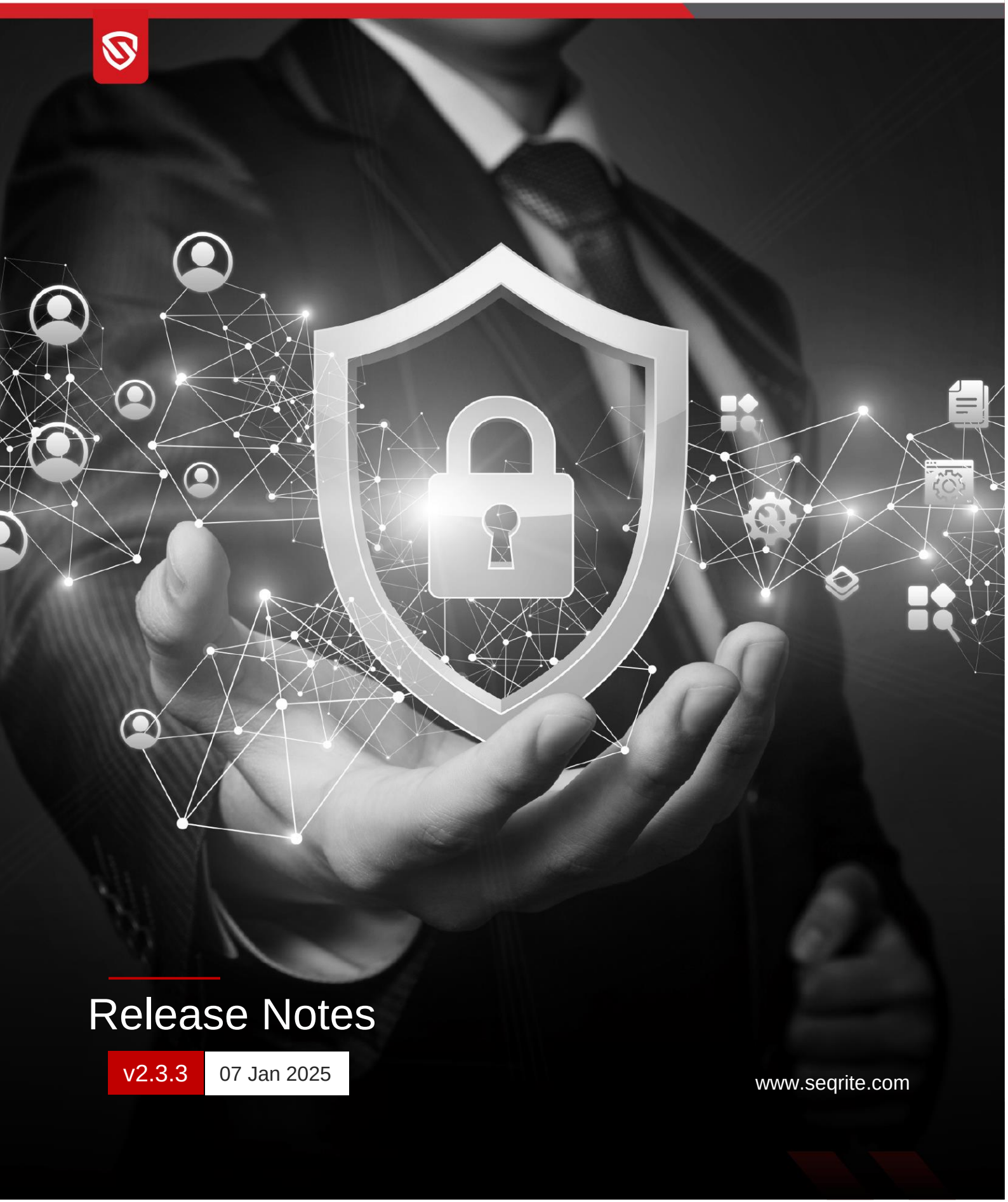
Seqrite ZTNA

SEQRITE



Release Notes

v2.3.3 | 07 Jan 2025

www.seqrite.com

Copyright Information

Trademarks

License Terms

Contents

Introducing Seqrite ZTNA

Seqrite ZTNA from Seqrite helps organizations enforce the zero-trust user access paradigm, where an organization by default does not trust any employee, contractor, or vendor staff with access to its systems and applications whether from within or outside the corporate network. It also replaces the complexity of VPN management.

Starting your zero-trust journey with Seqrite ZTNA:

- Create a zero-trust ecosystem with controlled set of users and applications.
- Deploy an agent-less solution and expand as per security appetite.
- Plug in your security requirements and deploy Seqrite ZTNA within minutes.
- Integrate Seqrite ZTNA with your existing IT infrastructure for identity management.

What's New

Seqrite ZTNA 2.3.3 includes the following new features.

A Loader for User Actions

Introducing a loader for user actions such as policy addition/edit/delete and so on to enhance the user experience of the system.

Enhancing Device Posture list with Notes and Descriptions

When adding a hostname to the device posture list, users can now include a note or description. The Descriptions & Notes will applicable for all the list types (IPV4, IPV6, Hostname, Serial number, MAC Address & Domain Joined)
This feature helps maintain clarity, especially as the list of devices grows, making it easier to identify devices. The notes also provide valuable context, simplifying device management and removal.

Email Alerts for Configuration Changes

Administrators can now receive email notifications for all significant configuration changes, ensuring improved visibility and streamlined auditing.
These notifications include critical details to enhance context and traceability.

Key Features:

- **Comprehensive Notifications**: Email alerts are triggered for specific configuration events across various categories.
- **Detailed Email Content**: Each notification includes:
    - Entity Name
    - Entity Type
    - Action Type
    - Admin Name
    - Timestamp
    - Configuration Details

Covered Events:

1. **Certificate Configuration**
    - Certificate added, edited/updated, or deleted.
2. **Site Configuration**
    - Site deleted.
    - IdP associated with a site changed.
    - Timeout settings modified.
3. **Application Configuration**
    - New application added.
    - Application tags or parameters (e.g., URLs, ports) edited.
    - Application enabled, disabled, or deleted.

4. **Policy Configuration**
    - New Zero Trust (ZT), Firewall, or DDoS policy added.
    - Policy configuration edited, deleted, enabled, or disabled.
5. **App Connector Configuration**

- App connector added, removed from a group, upgraded, or uninstalled.
- App Connector is in Active or Passive status
- App Connector UDP tunnel status Connected / Disconnected

This feature enhances accountability and helps administrators stay informed of key system changes.

Application Visibility on Mobile Screens

In upcoming versions, Guacamole-based and Agent-based applications will no longer be displayed in the User Portal when accessed on mobile devices with a screen width of 767 pixels or less.
This change is aimed at enhancing the user experience on smaller screens by focusing on optimized content and functionality.

Additional fields in the App Connector Sidebar

The App Connector Sidebar has been updated to include the following changes for improved usability and consistency:

- **Modified Fields**:
    - **Device Name (Hostname)**: Displays the generic hostname, aligned with the format used in the current device's sidebar.
    - **IP Address**: Clearly presented for easy reference.
    - **OS**: Displays the operating system of the App Connector.
- **Sidebar Heading**: Now shows a generic hostname to provide a consistent experience across device-related views.