ZTA Release Notes 16th June 2024

This document serves as the release notes for the Instasafe Zero Trust Access (ZTA) platform slated for a rollout on 16th June 2024. The document contains information about improvements and upgrades to the Web Portal, ZTNA Agent, and ZTA Gateways, including feature enhancements, bug resolutions, etc. In case of discrepancies between the information provided in the Release Notes and the Product Documentation, the information in the Release Notes is to be assumed to be correct.

- ZTNA Client version: 3.6.1.0
- ZTNA Service version: 7.7.24.0
- mZTNA Android app version: 1.27
- mZTNA iOS app version: 1.8.5
- Unified Gateway version: 7.3.4

General Notes

1. Minor modifications and Bug Fixes not significantly affecting the User experience are not a part of the release notes
2. Multiple bug fixes or enhancements relating to a particular feature may not be separately featured in release notes
3. New Features have been made available in the ZTA Admin Console for Early Access. Detailed information on these Features and Admin Guides shall be provided once they are ready for General Availability. Please email us at support@instasafe.com if you are interested in enabling these features or have any questions

Major Enhancements

Component	Description
Console	**Authentication** ● Radius authentication has been enhanced to support push notification authentication from the InstaSafe Authenticator app. Admins can now also select to allow users to perform Radius authentication with OTP, TOTP, or Push notification by enabling the ‘Enable auto select MFA’ toggle in the RADIUS Identity Provider profile. ● Azure-synced AD users can reset their password from the ZTA portal **Device Posture checks** ● Device Compliance profiles have been introduced under Perimeter Management -> Devices

  - This feature allows admins to set a “Device Compliance profile” based on certain device posture elements and restricts users from connecting to the ZTNA Client if they try to log in from non-compliant devices.
  - Admins can configure the “Device Compliance Profiles” to either block users from logging in from non-compliant devices or allow users to log in and have an automatic email triggered to notify Admins.
  - The supported elements with which a “Device Compliance Profile can be set:
    - Serial Number
    - Antivirus Name
    - OS Family
    - Domain Name
    - Antivirus Enabled
    - OS Main Version
    - Genuine Windows
    - OS Name
    - Antivirus Updated
- Enhancement to allow web and SAML application access from a selected list of system serial numbers.

Audits

- A new Audit Report named ‘Max Concurrency Graph’ has been introduced which fetches the count of concurrent VPN users for a select time duration.
  - if the time duration is a date range then the maximum number of concurrent VPN users per day data is plotted in the graph.
  - if the time duration is a single day then the maximum number of concurrent VPN users per hour data is plotted in the graph.
- A new Audit Report named ‘Network Packet Logs’ has been introduced which captures the details of the network applications accessed by the users
- Multiple new events have been added to capture the activities performed by Tenant admins.

  A new system event “MFA Push Notification Status” has been introduced which captures the details of the user and the location from where they are approving the push notification in the InstaSafe Authenticator app.

Configurations

- Enhancement to the process of VPN IP allocation to end users.
- Enhancement to configure SMS template for Custom SMS provider.

	Endpoint controls ● Configured “Device Compliance Profile” can be selected to be applied over the required OS. ● Admins can configure an Inactivity Timeout to disconnect users’ VPN sessions or log them out of the agent
Gateway	Unified Gateway version 7.3.4 contains performance improvements and minor fixes.
ZTNA Client	● ZTNA agent version 3.6.1.0: o This version of the ZTNA agent supports web application access from the Chrome browser. o All the network and web applications a user has been granted access to are displayed in the agent. o Network applications defined with an FQDN can be opened from the ZTNA agent body. o Ability to grant/restrict application access to users based on location. o Uninstallation of the agent msi in Windows is now password protected. Tenant admins can generate the password for agent uninstallation o Force close browsers when the ZTNA agent is disconnected o Log out the user from the ZTNA agent if they log out of the web portal.
ZTNA Service	● ZTNA version 7.7.24.0: - Inactivity timeout: Enhancement to either disconnect the user from the VPN or log the user from the agent due to inactivity. - Support to force closing browsers on disconnecting the ZTNA Client.
mZTNA App	mZTNA Android app version 1.27 and mZTNA iOS app version 1.8.5 have the following enhancements: - users can open applications in their default browser by clicking on the application clips available under “More Info”. - support for the device compliance feature.

Feedback

For any feature/enhancement request or feedback on the InstaSafe ZTA Solution, please email us at: support@instasafe.com