ZTA Release Notes 18th August, 2022

This document serves as the release notes for the Instasafe Zero Trust Access (ZTA) platform slated for a rollout on 18th August, 2022. The document contains information about improvements and upgrades made to the Web Portal, which include Feature Enhancements, Bugs resolved, 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.

- ZTAA Agent version: 4.23.2
- ZTNA service: 4.8.0.0
- VPN Gateway version: 4.3.2
- TCP Gateway version: 4.3.2
- RDP Gateway version: 4.1.6
- Web Gateway version: 1.5.9

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

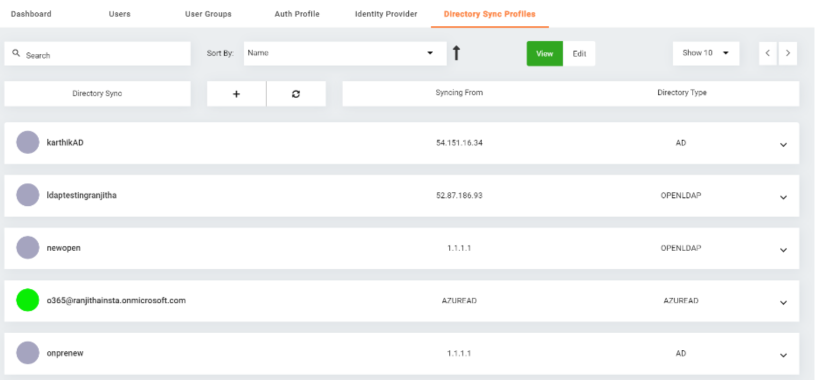
Noteworthy New Features

1. Automatically enable 2FA for users that have integrated the InstaSafe Authenticator App on their mobile devices. This feature automates the process of enabling 2FA, and reduces overhead for Admins.
   As soon as a user registers their profile in Instasafe Authenticator, 2FA would get automatically enforced during subsequent login attempts. On Uninstalling the Authenticator App, 2FA will remain active with Email/SMS based OTP becoming the default medium for 2FA.

   Please reach out to support@instasafe.com to enable this feature. To learn more, click here.

Major Enhancements

1 In Directory Sync Profiles (in Identity Management), the column ‘Distinguished Name’ has been changed to ‘Directory type’. The Directory Type will represent the integration with directory services like Active Directory (AD), Azure AD, Open LDAP or anything similar. This change can be seen by Administrator in InstaSafe ZTAA Console.



Directory Sync	Syncing From	Directory Type
karthikAD	54.151.16.34	AD
ldaptestingranjitha	52.87.186.93	OPENLDAP
newopen	1.1.1.1	OPENLDAP
o365@ranjithainsta.onmicrosoft.com	AZUREAD	AZUREAD
onprenew	1.1.1.1	AD

Major Bug Fixes

1. The "Quick look" icon does not show Azure AD user details added to the User Group

All details of Azure AD users are not showing under ‘Quick Look’ in user groups. Now, Administrators can see Azure AD User details by clicking the Quick Look icon
Severity: Low

2. Username lookup failure due to authCredential missing

The Username lookup would fail in certain situations, when the authCredential parameter is missing in the backend. This has been addressed, so Username lookups should no longer fail
Severity: Low

3. 'Primary Password Authentication Failed' Event for AD Users

In ZTA Console, inconsistency in messages noticed for User Fail Logins in Authentication Logs Report. If AD User Login fails, message should be ‘Primary AD authentication check failed for user’. If Local User Login fails, message should be: ‘Primary password authentication check failed for user.’
The inconsistency in message was observed in two scenarios

- Auth profile for an AD user has primary authentication as AD but the gateway toggle is off/disabled in auth profile
- Auth profile for an AD user has primary authentication as AD but the Domain name field is set with invalid data in auth profile

The issue has been addressed and now the report will show correct messages in the Authentication Logs Report.
Severity: Medium

Feedback

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