BeyondInsight and Password Safe 22.2.2 Release Notes

July 26, 2022

Issues Resolved:

- Resolved permission issue in TeamPasswords.
- Resolved authentication issue in which the RADIUS fallback server was not respected.
- Resolved database upgrade failure for some customers who have mapped Azure AD users.
- Resolved issue in which the user interface allowed Azure AD users to attempt to change their password.
- Resolved Azure AD authentication issue related to PRA / Password Safe integration.
- Resolved SCIM connector issue in which the /GET containers endpoint was returning a 500 error.

Known Issues:

- When using the **ps_automate** session utility and configured to use the Firefox browser to a website using a self-signed certificate and the **IgnoreCerts** flag, the login is successful but the webpage does not respond. Workarounds: use a different browser, use a valid (not self-signed) certificate, after login click shift-refresh and manually accept the browser security warning for the session, or add the necessary steps to the automate configuration file to accept the warning prompt.
- When creating a new password policy or DSS key policy, an unnecessary success toast message displays: *Changes have been discarded*. This notification can be ignored.
- When modifying a **Set attributes on account** Smart Rule action, if you change the attribute type from one, which is a numeric name (i.e. **1**) to a different attribute type, an error will occur: *Key type must be int for this method of adding items*. Workaround: delete the **Set Attributes** action and recreate.
- In a FIPS-enabled environment, attempting an RDP Admin Session will be unsuccessful and an error message shown. Workaround: use a standard managed RDP session if possible.
- In rare cases, if the time zone of the scanner has changed, a scheduled scan may not start at the scheduled time. Workaround: The scan will run at the next scheduled time.
- If forms login is disabled for a user when another login method is not setup, that user cannot login. Workaround: ensure that another login method is setup before setting **Disable Forms Login** to **yes** globally or for any user.
- Upgrading after installing BeyondInsight to a location other than the default displays an error message. Workaround: if you manually upgrade, select the alternate install folder during the upgrade.
- **Scan Data Users** grid may incorrectly display *Password Expired* for some accounts. Workaround: log in with the affected user, or force them to change/set the password.
- Analytics and Reporting: The **Retina Product Usage Details by Organization** report may not show any results in environments that do not have Retina scanners. Workaround: none, this report is no longer valid and will be removed in an upcoming release.
- **Scan Data User Details** shows the user **Description** in the **Full Name** field, and may show a blank description. Workaround: none, this is informational and does not have any impact on the onboarding of the user.
- In rare cases, installing BeyondInsight 22.2 on a U-Series Appliance may crash due to BIAdmin service not starting. Workaround: delete all JSON files from the BIAdmin directory, then repair the BeyondInsight installation from **Programs and Features**.
- Configure HSM Credentials utility may crash when testing a new HSM Credential if you don't fill in the **Key Name** field. Workaround: be sure to fill in all the fields before testing the credential.
- Deleting a user that has an active Password Safe Request or related SSH Session will not succeed, and the error message is vague. Workaround: none, this is expected behavior. The error message may be improved in an upcoming release.
- The first attempt to edit a BeyondInsight user from the **User Details Edit** form results in a form validation error on fields that were not changed. Workaround: discard the changes and try again, or edit the user from the grid row action.

- Analytics and Reporting: changes to saved views or snapshots do not reflect right away in the list. Workaround: refresh the page to see the changes.
- In the Configure HSM Credentials utility, selecting the **Hardware Security Module User Guide** from the **Help** menu displays an error. Workaround: this documentation is now avaiable online on the BeyondTrust documentation site.
- The **No Enumerations Selected** banner may not display in the Scan Wizard if the **Unlimited Users** box is unchecked. Workaround: ensure you select the enumeration options needed for the scan.
- The **Scan Data Ports** grid shows a limited number of ports, with fewer details. Workaround: none; this is informational. The new BeyondTrust Discovery Agent does not perform protocol detection and returns only the standard database and remote access ports here.
- Naming a scan with a name belonging to a previously deleted scan appends a counter to the end of the scan name. Workaround: the deleted scan still exists behind the scenes and the name cannot be reused. Give your scan a new name.
- Using a low/least privilege user as proxy during Analytics and Reporting configuration may lead to this user not being able to download the Analytics and Reporting log files. Workaround: add this user to the **msdb.dbo** table so they can download the logs.
- It is possible to create multiple SAML providers with the same name. Workaround: none; this is not an issue because name is not the unique identifier. If the user finds it confusing, they can edit the names to be unique.
- If a credential description begins with text matching the name of the scan it is used in, the scan is displayed as though an ad-hoc credential was used. Workaround: edit the credential description to be something other than the scan name.
- Analytics and Reporting: pivot grid chart may display blank if the data was recently pivoted. Workaround: expand the data after pivoting, or remove/re-add the chart.
- System Event Viewer may display errors with sources of *SideBySide* or *AppBus*. Workaround: none; this is informational. The errors do not cause any system issues and will be cleaned up in a future release.
- If the Endpoint Privilege Management plugin is configured but the corresponding MSI is not installed, the Event Service log may contain error messages such as *System.Net.Http.HttpRequestException*. Workaround: be sure that the MSI is installed and complete the plugin configuration to use this feature.
- IIS App Pool users may be displayed in the **Scan Data Users** grid if those accounts have logged into the scanned asset. Workaround: none; this is expected behavior.
- Some long field names from BeyondInsight password policy changes or directory credential changes might be truncated in the **User Audit Details** view. Workaround: none; this is informational. Some field names can be inferred from the parts that are visible before they are truncated.

Notes:

- Direct upgrades to 22.2.2 are supported from BeyondInsight versions 7.0 or later.
- This release is available by download for BeyondTrust customers (https://beyondtrustcorp.service-now.com/csm) and by using the BeyondTrust BT Updater.
- The MD5 signature is: 74c9483c907d1f8487c44702af521b52
- The SHA-1 signature is: 547a4b9907f4b6b1540dac4edbf97374b4826bef
- The SHA-256 signature is: 2b2b150ec262d3682ba2edf1d5cacf081c710f4fe8c2dc155f32bba6e53f0b94