BeyondInsight and Password Safe 6.10 Release Notes

February 11, 2020

Release Availability:

This release is available by download from BeyondTrust customers (https://beyondtrustcorp.service-now.com/csm) and using the BeyondTrust BT Updater.

For downloads prior to February 28, 2020, use the following:

- The MD5 signature is: 3dc8569a33cccc9e7a5b04da2432f948
- The SHA-1 signature is: 13ed1b38dbcb755c440ecc730b6b49ed4d9cc57e
- The SHA-256 signature is: 603158e2b36f751da7660349c2361975c936e5d6ae769a2b0a0f2eb9483ffc62

For downloads after February 28, 2020, use the following:

- The MD5 signature is: f00867eb64fb3c2b14e2ef33af269649
- The SHA-1 signature is: 0c40a6a1c821cd49831b570674ee6d4e64bec3b2
- The SHA-256 signature is: 3cb4c2a507d81b86cbd37b8126e202ab1212650d5074872d3251b78969775208

New Features and Enhancements:

- **General:**
  - Moved **Smart Rules** management under **Configuration**.
  - Replaced Flash **Smart Rules** management UI with HTML5 UI.
  - Added **Process Smart Rule** action to **Smart Rule** management grid.
  - Changed the default **Asset Grid** from the Flash UI to the HTML5 UI.
  - Replaced Flash **Asset Advanced Details** UI with HTML5 UI.
  - Replaced Flash **Directory Queries** UI with HTML5 UI.
  - Replaced Flash **Users and Groups** UI with HTML5 UI.
  - Added new UI to manage Directory Credentials (for use with Users and Groups and Directory Queries).
  - Replaced Flash Organizations and Flash Workgroups configuration areas with HTML5 area to manage both.
  - Added a **Smart Group** filter to select assets by **Last Retina Scan Time**.
  - Migrated BeyondInsight Omniworker and RemManager services from 32-bit to 64-bit.
  - Added the ability to remove PowerBroker for Windows User Based Policy via Smart Rule.
  - Enhanced field mapping for ServiceNow Ticket System.
  - Added support for normalizing Event Source of forwarded events to database Event tables.
  - Added support for updating MS Azure connector **ClientID** and **Client Secret** values programmatically.
  - Added **Configuration** and **Dashboard** screens for Privileged Remote Access Integration.
  - Updated internal licensing functionality.
  - Added support for SQL Server 2017.
  - Added support for Windows Server 2019.
  - Removed support for installation of BeyondInsight on Windows Server 2008.
  - No longer supporting configuration of BeyondInsight with SQL Server 2008 or SQL Server 2008 R2.

  - Enhanced support for extra LightWriteBack data.
  - Replaced embedded documentation with links to online documentation.
  - Enhanced password policy.
  - Removed the greyscale color palette from the UI.
  - Updated EULA, branding, product icons, and colors in BeyondInsight Console and Analytics & Reporting.
  - Updated name of PowerBroker Server Management Console menu link to BeyondInsight Unix & Linux.
  - Added TCP/53 to default discovery port list.
  - Added client credential authentication to SCIM.
  - Added Generate Rule XML and Exclude Application/Publisher row actions to Endpoint Privilege Management Events grid.
  - Added the **Rule Name** field to the default set of columns for the **Endpoint Privilege Management Events** grid.
  - Added preview of dynamic dashboards for administrators.
  - Added preview of HTML5 UI for Active and Completed Scans.
  - Improved reliability and performance of Asset meta-data purging.
- **Analytics & Reporting:**
  - Added **Cube Last Sync time** to 19 Password Safe and Endpoint Privilege Management Cube-based reports.
- **Password Safe:**
  - Promote Managed System to be a first-class citizen in the product.
  - Added ability to use TNS stored in Active Directory and OID for accessing Oracle databases.
  - Added ability to onboard disabled accounts via a Smart Rule.
  - Added new Smart Rule type: Managed Systems.
  - Renamed **Agent Assignment** to **Worker Nodes**.
  - Renamed **Password Rule** to **Password Policies**.
  - Renamed **DSS Key Rules** to **DSS Key Policies**.
  - Replaced Flash UI with HTML5 UI in the following configuration areas: **Agent Assignment**, **Multi-Factor Authentication**, **DSS Key Rules**, **Functional Accounts**, **Applications**, **Password Policies**.
  - Replaced Flash UI with HTML5 UI for **Managed Account** and **Managed System Management**.
  - Updated database client libraries (Oracle, Sybase, MySql, MongoDB, PostgreSQL, Teradata).
  - Added support for auditing SCP and SFTP sessions.
  - Control codes are now translated into displayable characters in keystroke logging.
  - Created standalone installer for ESA components (pbpsmon and pbpslaunch).
  - PBMSD is now 64-bit.
  - RDP performance settings are now configurable via registry keys.
  - Iolog buffer size is now configurable, reducing likelihood of lost or incomplete session recordings.
  - RDP audio and performance settings are now copied from user's RDP client.
  - SSH host key algorithms are now configurable via registry keys.
- **BeyondInsight and Password API:**
  - Added PUT ManagedSystems/{id}.
  - Added Managed Directory support - GET/POST/DELETE Managed Directories and associated Managed Systems.

- Added GET Configuration/Version.
- Added GET UserGroups/{id}/Permissions.
- Added GET Databases/{databaseID}/ManagedSystems.
- Added POST Databases/{databaseID}/ManagedSystems.
- Added DELETE ManagedSystems/{id}.
- Added GET ManagedSystems.
- Added GET ManagedSystems/{id}.
- Added GET Assets/{assetID}/ManagedSystems.
- Added POST Assets/{assetID}/ManagedSystems.
- Added PUT ManagedAccounts.
- Added GET ManagedSystems/{id}/ManagedAccounts.
- GET ManagedAccounts now supports paging.
- Updated GET Sessions to allow filtering on status and userId.
- GET ManagedAccounts now supports filtering by type, i.e., ?type=system.

Issues Resolved:

- Resolved an issue in which PBW application launch events configuration setting was being ignored.
- Resolved an issue in which clicking on Clarity Analytics link returns a blank page.
- Resolved an issue in which creating a new Address Group goes under the **AddressGroup** category and not **Address Groups**.
- Resolved an issue with SSO if there is an expired token in the local date store.
- Resolved an issue in which enumerating Active Directory groups auditing shows the logged in user making the refresh changes.
- Resolved an issue in which scheduled scan jobs do not reflect the modified template settings when modifying a Scan template.
- Resolved an issue with BeyondSaaS import in which **FirstDiscoveredDate** and **LastDiscoveredDate** month and day are swapped for regions that are not using en-US short date format.
- Resolved an issue with how the SMTP password is stored in the BeyondInsight database.
- Resolved an issue with Smart rule attributes for smart rules created prior to BeyondInsight version 6.9.
- Resolved an issue with logging in using UPN for user in a child domain when a Universal Active Directory Group is in parent domain and user is in child domain.
- Resolved an issue with Password Safe user licensing not returning all login data.
- Resolved an issue with Password Safe Activity Report timing out when executed by an Auditor.
- Resolved an issue with Password and Session Activity Report showing no records when administrator group is unchecked.
- Resolved an issue with saving SMTP settings in BeyondInsight configuration utility on a UVM appliance.
- Resolved an issue with SMTP settings in the BeyondInsight Configuration Tool not applying on a UVM Appliance with Windows 2016 and SQL 2016.
- Resolved an issue with managing vulnerability scanners in BeyondInsight without having the correct permissions set.
- Resolved an issue with PCI report sometimes showing the wrong number of assets.
- Resolved an issue with SCIM connector Active Directory authentication failing.
- Resolved an issue with Event Forwarding log time fields being dropped.
- Resolved an issue with Omniworker failing to complete a transaction in rare cases.

- Resolved an issue with smart rules assigning duplicate attributes after XML import.
- Resolved an issue with importing Benchmark scans when filename and file path together are greater than 259 characters.
- Resolved an issue with debug logging for Benchmark Scans showing password in PolicyService log file.
- Resolved an issue with smart rules that have multiple filters causing issues with SQL TempDB space usage.
- Resolved an issue in which purging assets IPs isn't respecting the batch purge option in larger environments.
- Resolved an issue with Overnight purge in which it does not loop correctly if the initial purge takes between 31 and 59 minutes.
- Resolved an issue with 169.254.x.x and 127.0.0.1 IP addresses in which assets are not purged from BeyondInsight during nightly purge window.
- Resolved an issue with Asset IP purge not respecting the BatchPurge configuration item setting.
- Resolved an issue with PBW session monitoring data failing to purge on schedule.
- Resolved an issue with PBW Application Launch configuration options being ignored for some PBW client versions.
- Resolved an issue with Password and Session Activity report misrepresenting Remote Application Requests as SSH Requests.
- Resolved an issue with custom audit settings being overwritten on audit updates.
- Resolved an issue with Database users not being associated with correct DB instance with BTNSS version 6.6.0+.
- Resolved an issue with unassigned user policies in a BeyondInsght smart rule user assignment table not updating to remove user policy assignment.
- Resolved an issue with ServiceNow returning two tasks instead of one when requesting ticket validation on a request.
- Resolved an issue with BeyondInsight configuration page link to Endpoint Privilege Management Exclusions missing for some license types.
- Resolved an issue with custom reports from **Analytics and Reporting Pivot Grid** outputting duplicate sets of records when exporting to CSV or XML.
- Resolved an issue with updating user account names to proper upper and lower case following a scan of a Linux/Unix asset.
- Resolved an issue in which adding an active directory user to a local BeyondInsight group requires a first name.
- Resolved an issue in which users in BeyondInsight with read access to credentials are unable to use credentials for scanning.
- Resolved an issue in which smart rule assigning Host Scan Group rule runs slow in larger environments.
- Resolved an issue in which scans against cloud asset smart rules can fail to start with the error *Could not start scan*.
- Resolved an issue with Configuration Compliance reports showing duplicate benchmark profiles for the Benchmark parameter.
- Resolved an issue during login in which some users' attributes isLocked and isDisabled are not correctly updated from the Active Directory.
- Resolved an issue with Active Directory in which a user's expiry date and status do not get updated on login.
- Resolved an issue in which Detailed Discovery Scans configured to enumerate unlimited users do not actually enumerate unlimited users.
- Resolved an issue in which logging into A&R Configuration Wizard on a UVM fails when using just username.
- Resolved an issue in which BeyondInsight configuration tool does not allow changing the SAML access URL to a relative URL.
- Resolved an issue with events not being forwarded to event collector in a multiple Omniworker environment.
- Resolved an issue with Flex asset grid vulnerabilities area in which chart time frame buttons do not work if user does not have Patch Management read access.
- Resolved an issue with AWS targets being ignored when scanning using the public IP address option.
- Resolved an issue with Splunk in which scan events are missing the values for the **OS**, **EventSeverity**, and **EventType** fields.

- Resolved an issue in which **Operating System** filter can return unexpected results when using **Limit to most recent OS detected** and **Include assets where value is unassigned**.
- Resolved an issue with BeyondInsight not always respecting a user's preferred domain controller.
- Resolved an issue in which A&R Password Safe Synchronized Accounts report grouping by account name hides rows with the same account name.
- Resolved an issue in which Engine ID used by BeyondInsight for SNMPv3 packets does not conform to RFC1910.
- Resolved an issue with Asset attributes manual selection missing (Flex to HTML5 port).
- Resolved an issue in which CSV import (Qualys, Nexpose, Tripwire) fails unexpectedly with *NullReferenceException in 'Logger.txt' file*.
- Resolved an issue in which ServiceNow executor is unable to connect with TLS 1.2.
- Resolved an issue in which software versions sometimes do not get updated after scanning an asset.
- Resolved an issue in which Clarity Cluster Analysis report for Password Safe fails to load and displays an error.
- Resolved an issue in which stored procedure Util_CleanupPBWVulnerabilityScans fails with error: *statement conflicted with the REFERENCE constraint 'FK_Scan_ScanExtensions'*.
- Resolved an issue with Asset purge failing when an asset IP has over 90k process instances.
- Resolved an issue in which UserSSHKeys Normalization failure causes Active scan job to never complete.
- Resolved an issue in which SSO Logins fail for AD users if their domain has any capital letters in it.
- Resolved an issue in which credentials for a scheduled scan get replaced when a managed scan credential has its password changed.
- Resolved an issue in which JIRA ticket connector in Password Safe does not allow TLS 1.2 connection.
- Resolved an issue with ServiceNow data exports not working when using TLS 1.2.
- Fixed multiple issues in which **Domain Controller** drop-down fails to load, Database Accounts fail to on-board via smart rule, and ServiceNow Connector fails test connection.
- Resolved an issue in which Omniworker service stops unexpectedly when attempting to access a socket connection that is already closed.
- Resolved an issue in which an Auditor user attempts to launch an RDP session and receives an on-screen error.
- Resolved an issue in which requestors sometimes do not see their DomainLinked Mapped accounts on the **Applications** or **Database** tabs in Password Safe.
- Resolved an issue with auto-managed functional accounts not getting passwords rotated in multi-organization environments.
- Resolved an issue with scheduled tasks not resolving when account name is using UPN prefix and UPN prefix and account do not match samAccountName.
- Resolved an issue in which Connection Profile Alerts from PBSMD have an invalid time-stamp.
- Resolved an issue with PBSDeploy encountering an error on non-English environments.
- Resolved an issue with smart rules for Dedicated account with UPN suffix matching.
- Resolved an issue in which **Domain Linked** tab does not reflect the asset group filter that is contained in a smart rule.
- Resolved an issue with being unable to use the **Assign Workgroup** smart rule action.
- Resolved an issue with ClaimsAware attempting auto login after user logs out.
- Resolved an issue in which Managed Accounts do not reflect the proper case when imported via XML.
- Resolved an issue in which Password Safe database platform lists items which have no policy.
- Resolved an issue in which Password Safe onboarding smart rules time out due to inefficient sub query.
- Resolved an issue in PBSMD in which Diffie–Hellman key exchange results in SSH sessions are dropping randomly.
- Resolved an issue in which Password Safe Quick Rules are being flagged to re-execute repeatedly.

- Resolved an issue with Password Safe not being able to test or change a password for Oracle database users if the username is numeric.
- Resolved an issue with Event Forwarding for Password Safe events in which remote sessions created by a *requestor* are missing the asset name.
- Resolved an issue wherein trying to perform an ISA release the following error is received: *unable to find the specified column in the result set*.
- Resolved an issue in which Oracle connection pooling is enabled for password testing and is changed, causing .NET to hold onto the connections.
- Resolved an issue with SAML **web.config** where TextWriter is both enabled and disabled.
- Resolved an issue with High CPU usage when navigating to the Approvers table in Password Safe.
- Resolved an issue in which Password Safe password rotation fails when using LDAP functional accounts.
- Resolved an issue with Password Safe platforms with elevation enabled sending *None* as part of the command if it is saved.
- Resolved an issue in which users can edit managed accounts that they do not have correct permissions to via a smart rule.
- Resolved an issue in which scheduled password changes do not take the time of the retry into consideration when attempting to change the password.
- Resolved an issue in which retrieved passwords are stored in local disk caches of some browsers.
- Resolved an issue with **Login Account for SSH Session** not being able to be set for automatic password management.
- Resolved an issue with failure to connect to OpenLDAP server when using posixGroup type.
- Resolved an issue with LDAP filter not working for IBM LDAP servers.
- Resolved an issue with Password Safe in which dependent parent services are causing the process to hang when trying to update services.
- Resolved an issue in which after a failed login attempt AD users can be locked out for 5 minutes when using a managed bind account.
- Resolved an issue with SAML Logout URL not redirecting correctly.
- Resolved an issue with Password Safe Session Monitoring Keystrokes data not appearing or delayed.
- Resolved an issue in which Password Safe users cannot select release start date for next month on last day of the month.
- Resolved an issue in which editing a smart rule causes lastprocesseddate to be set to 100 years in the future and prevents the smart rule from reprocessing.
- Resolved an issue in which LDAP users cannot authenticate via API unless their LDAP server allows binding without password.
- Resolved an issue in which users in API created user groups are unable to login.
- Resolved an issue with API only supporting static bind accounts when adding an Active Directory group; managed bind accounts would not work.
- Resolved an issue in which API AppSignIn generates a 500 Internal Error when there is a UserGroup with no associated Group Permission entries.
- Resolved an issue with API call causing crash of service if a large number of Active Directory users are added.
- Resolved an issue with Benchmark Compliance reports when multiple profiles are selected.
- Resolved a performance issue with Password Safe Activity report.
- Resolved a performance issue with Password Safe Release Activity report.
- Addressed a data discrepancy involving Zero Day vulnerabilities between the Vulnerabilities Delta by Month and Vulnerabilities Delta by Day reports.
- Resolved an issue with storing passwords with specific characters in the BeyondInsight Configuration Utility SQL account password field.
- Resolved an issue with administrator username updates in BeyondInsight Configuration Utility.

- Resolved an issue in which LDAP User Groups fail to enumerate when using SSL and memberUID as the Membership attribute.
- Resolved an issue with high CPU usage by pbpsdeploy when cleaning up after session ends.
- Resolved an issue with RDP disconnect caused by screen resolution not divisible by 4.
- Addressed incompatibility with old versions of Putty.
- Resolved issue with X11 Forwarding.
- Resolved issue with connection profile blocking and locking.
- Resolved issue with unlocking of a session locked by IP/hostname match.
- Resolved issue with ssh session locking by IP/hostname match in connection profile.
- Resolved issue with direct connect with Putty 0.71.
- Resolved RDP connection issues related to per-device licensing.
- Resolved issue with SSH key re-exchange.
- Resolved RDP disconnection related to beep sounds.
- Corrected missing SSH keystroke audits.
- Resolved double logging by pbsmd watchdog process.
- Resolved Diffie Hellman group exchange rekeying.
- RDP session replay now responds to desktop resolution changes.
- Resolved issue that enabled SSH connection sharing even with multiplexing disabled.
- Resolved handling of keystroke audit messages for SCP sessions.
- Corrected UI slowdown that can occur in RDP sessions when ESA is enabled.

Known Issues:

- LDAP users with language specific special characters (including but not necessarily limited to äÄéöÖüÜßÇéâêîôûàèùëïü) in their names may not be displayed in BeyondInsight.
- When two smart card users have the same name but a different domain or UPN, the smart card throws an error and the user cannot log in.
- Registry may contain a key showing an incorrect BeyondInsight version after an upgrade.
- Cannot set smart rule with action **Assign EPP Policy**.
- When adding optional columns to a grid, they are added to the right of the action menu icon. This can result in the action menu icon not being the rightmost item in a grid.
- The limit on the user/password field for BI/AD/LDAP users is 117 characters. An account with a username or password greater than 117 characters cannot be added.
- Removing automanagement setting from Functional Account configuration after manually resetting the password causes future password resets to fail.
- When an asset that was previously a PowerBroker for Windows asset is migrated to Defendpoint and checks into BeyondInsight as a Defendpoint Privilege Manager for Windows asset, all previous PowerBroker for Windows events may show Defendpoint as the Product Type. This is because the product type is set/stored at the asset level, not with each event.
- Launching the Organization Related Items report on a newly created organization may result in a **MISSING KEY** string in the breadcrumbs.
- A user in a child domain that is brought into BeyondInsight via the parent domain using LDAP to connect to AD may not be able to log into BeyondInsight.
- Cannot run Web Application scan report from **Scan** area in BeyondInsight.

- Upon switching from Password to DSS and manually entering password credentials with automanagement set (Password and DSS) after save and edit, auth type still shows as Password.
- Subscribing to Organization Related Items report fails if report is accessed from the **Configuration/Organizations** area.
- A Manual Smart Group created from the **Managed Accounts** grid does not show up in the **Smart Group** filter even after refreshing the grid.
- In the Endpoint Privilege Management event details, a Defendpoint Privilege Management for Windows event will show the Workstyle name in the **Policy Name** field.
- Deleting an attribute that is in use in a smart rule will cause the smart rule to quietly choose the next attribute in the dropdown upon next smart rule edit and save.
- Under a **Managed System Advanced Details** list of Managed Accounts, the non-managed cloud platforms show a **Test** button that is not applicable and does not do anything.
- DSS Keygen using newer OPENSSH client results in a key generated with OPENSSH header that we don't support.
- Newly created custom asset attributes do not appear in the smart rule editor attribute dropdown.
- Database compatibility level still at SQL Server 2008 (100) on upgrades, even though SQL Server 2008 is not supported in 6.10.
- Selecting and deselecting items in the column chooser on a grid may change the order of the items in the column chooser.
- When attempting to configure a previously configured smart card to a second account, there should be a warning to prevent this, but there is not.
- Subscribing to Asset Details report fails if report is accessed from the **Asset** Grid.
- The **Password Policy** dropdown on the **Create New Managed System** form is not long enough.
- Migration from PowerBroker for Mac to Defendpoint Privilege Management for Mac may see a delay in policy delivery to the asset.
- When onboarding LDAP users, you cannot create an Account Naming attribute with fewer than 3 characters.
- Using the third party template to import an RTD file can cause errors before completing.
- In Windows SSO, if there are identical usernames with different domains, the second user may have trouble logging in.
- Managed Systems Smart Rules name and description filters use the **Starts With** operator rather than the **Contains** operator.
- When adding long-named columns to a grid, the column titles may not be fully visible.
- Under a **Managed System Advanced Details** list of Managed Accounts, the Amazon platforms show a **Use Own Credentials** switch that is not applicable.
- When configuring a Managed System Smart Rule to match on **Assigned Custom Attributes**, changing the operator after selecting the attribute type changes the list of attributes to the default, **Business Unit**, instead of keeping them related to the attribute type selected.
- It is not possible to import an active directory group if a local group of the same name already exists. This only affects importing new groups. Groups that existed before the upgrade to 6.10 are not affected.
- Limited user with full access to Managed Systems cannot see Functional Accounts related to a Managed System.
- Downloading Flash grid contents using the FireFox browser may be prevented by the browser.
- In the **Server Keys** grid in the Advanced Details of a Managed System, the **Denied Dates** filters do not function.
- The Test Functional Account of an LDAP Directory Managed System improperly uses the **Use SSL** setting from the Managed System instead of the Functional Account. This can result in the testing of the LDAP functional account to fail if SSL is enabled.
- The Snapshot selection dropdown on the Asset Advanced Details view does not update the details. The details will always show the data from the latest scan.
- Within the **Configuration > Password Policies** user interface, if you have scrolled to view the bottom section of a password policy, and then click **Create New**, the form to create a new password policy will be opened, but the UI will not automatically take the user to the first field on the form.

- The PostgreSQL client library is not FIPS certified. If FIPS mode is enabled, then operations against a PostgreSQL database (onboarding, functional account test, etc) will fail. Workaround: Disable FIPS mode.
- Pulling users into an LDAP group within user management may fail if using LDAP + SSL on any port other than 636. Log files contain an error message stating *The directory service is unavailable.* As a workaround, use SSL standard port (636) or contact support to obtain a hotfix.
- Pulling users into an LDAP group within user management via LDAP + SSL may fail if there is any inconsistency in the environment's certificates. As a workaround, ensure that the environment's certificates are configured correctly.
- When using LDAP, searching the directory for groups or users using an asterisk (*) as the filter may fail if there are more than 100 search results. As a workaround, narrow your search criteria to return fewer than 100 results.

Notes:

- Direct upgrades to 6.10.0 are supported from BeyondInsight versions 6.6.x or higher.
- The following areas of BeyondInsight require Adobe Flash Player 32.0.0.255 or higher:
    - Configuration – General – Attributes
    - Configuration – General – Connectors
    - Configuration – Patching – SCCM
    - Configuration – Patching – WSUS
    - Configuration – Discovery and Vulnerability Management – Audit Manager
    - Configuration – Discovery and Vulnerability Management – Benchmarks
    - Configuration – Discovery and Vulnerability Management – Scan Options
    - Configuration – Privileged Access Management – Password Safe
    - Access Policies
    - Access Policies - Connection Profiles
    - Change Agent
    - Custom Platforms
    - Global Settings
    - Mail Agent
    - Mail Templates
    - Managed Account Aliases
    - Managed Acccount Caching
    - Old PBPS Import
    - Session Monitoring
    - Test Agent
    - Ticket Systems
    - Configuration – Privileged Desktop Management – Endpoint Privilege Management Exclusions
    - Configuration – Privileged Desktop Management – Protection Policies
    - Legacy Assets view - PBUL Events
    - Legacy Assets view - PBUL Solar Search
    - Legacy Assets view - PBUL Session Reply
    - Legacy Assets view - PBW Session Reply
    - Legacy Assets view - PBW FIM Events
    - Legacy Assets view - PBW Windows Events

- Legacy Assets view - BeyondInsight Ticketing Views
- Legacy Assets view - Retina Agents View
- Legacy Assets view - Asset Attacks Grid
- Legacy Assets view - Asset Vulnerabilities Grid
- Legacy Assets view - Asset Malware Grid
- Scan - Report Templates
- Scan - Report Template Options
- Scan - Scan Initiation
- Jobs - Advanced Scan Jobs view (Host Scans, Benchmark Scans, Scan Details)