RED IM Revision History

May 2018

Contents

Version 0.40 (March 2, 2002)

- Initial release of the RED IM product.

Version 0.51 (December 21, 2003)

- Updated the account usage discovery mechanism.
- Updated the database usage code as well as stored procedures.

Version 1.01 (February 20, 2004)

- Added Accounts View.
- Updated the account usage discovery mechanism.
- Updated database usage code as well as stored procedures.
- Updated the grid display in order to decrease memory usage when displaying large system sets.

Version 1.10 (July 21, 2004)

- Added a database creation wizard.
- Added the ability to see the password age of accounts in the Accounts View.
- Added an In Use count for accounts in the Accounts View.
- Added Basic Account Management to the Accounts View.
- Resolved an issue with the system creating missing database tables.

Version 1.11 (February 15, 2005)

- Added the ability to discover and propagate IIS accounts.
- Added filtering options to the Accounts View.
- More logging is now available during propagation events.
- Update the code dedicated to storing information in the database.
- Changed the location in which the system would attempt to propagate.

Version 1.13 (September 18, 2005)

- Added more filtering options in the Accounts View.
- Added color coding for password age in the Accounts View.
- Resolved an issue with dynamic group updates.

Version 1.25 (December 5, 2005)

- Added more encryption options.
- Modified menu items.

Version 2.32 (February 4, 2006)

- Added a refresh option to Context > Jobs Monitor.
- Added a refresh button to the Jobs Monitor.
- Added the option to shorten the splash screen display and to dismiss the splash screen with a left-click to the Preferences dialog.
- Added the option to push web application registry settings to the Install Web Application Custom section.
- Updated the product documentation.
- Modified the Install Service button in the Deferred Processor Status and Configuration dialog. The action attempts to automatically remove the service before attempting to install.
- Resolved an issue with the system status failing to update in the Main dialog after operations have completed.

- Resolved an issue with setting status passwords.
- Resolved an issue with the Password Settings tab in the Job Details dialog showing blank passwords for jobs with encrypted static passwords.
- Resolved an issue with failures occurring when creating a new database using the database creation wizard.

Version 2.52 (June 8, 2006)

- Added the ability to create and email password report jobs, which check stored passwords for validity.
- Added more detailed status information for fail password checks in the Password Status Report.
- Added a password recovery email alert to the web interface.
- Added a Recovery Comment to the bottom of the recovery alert email.
- Added an interactive Password Test option to the Stored Passwords dialog.
- Added logging and user interface updates to the Password Status Report jobs.
- Added the ability to update the system automatic login cache when changing passwords.
- Added the ability to clear the automatic logon cache when changing passwords.
- Added the ability to edit all properties of a dynamic group from the Managed Groups dialog.
- Added the ability to store all passwords in a Password History section, which is accessible via the Recovery dialog
-
- Added a password vault to store external passwords.
- Added IP Address and Password Comment fields to stored passwords.
- Added logging for adding and updating external passwords to the data store.
- Added filtering options to the Stored Password dialog.
- Added IP Address and Comments fields to the Account display in the web interface.
- Added the ability to search for stored passwords by IP address in the web interface.
- Implemented extra security to encrypt database connection passwords.
- Updated the Password Status Test to be multi-threaded as well as single-threaded on a per system-basis, increasing overall performance.
- Modified the behavior of the web application to not auto-spin statically-set passwords.
- Modified the default path for reporting resources, allowing to reside in its own sub-folder under the main program directory.
- Updated email settings.
- Updated user interface for consistency.
- Resolved an issue with required service rights not always being added to the deferred processor account.
- Resolved an issue with domain password checks by adding a local account namespace to the password status check.
- Resolved an issue preventing report template files from being properly installed.
- Resolved an issue with status report jobs continuing to run even after the operation had already failed.
- Resolved an issue with web installation failing if the COM+ application was not already found on the target system.
- Resolved an issue with the web component not updating its settings upon install.
- Resolved an issue with the web interface displaying an error if a user belonged to more than 100 groups.

Version 2.63 (September 21, 2006)

- Added the check to deferred jobs are deleted when the corresponding group is deleted.
- Added a warning message stating “The web application will not support this mode” when Integrated Authentication is selected.
- Added the ability to use integrated SQL authentication for the password recovery website.
- Optimized the loading time of group data.
- Optimized the display code for the Deferred Jobs display.
- Optimized the deferred processor job logic to determine the order in which jobs are run.
- Resolved an issue with the buffer overflow improperly formatting system names.

- Resolved an issue with symmetric password changes causing a blank password to be saved.
- Resolved an issue with retried jobs running immediately rather than at the scheduled time.
- Resolved an issue with configuring a job to set a status password after setting a random password would cause the settings to not save.
- Resolved an issue with the deferred process not properly initialize the database settings.
- Resolved an issue with Password Status Report no always mailing out when the job was run via the deferred processor.
- Resolved an issue with the deferred processor not connecting to the database.

Version 3.02 (March 23, 2007)

- Added functionality to where the built-in admin account was renamed during password change jobs.
- Added the ability for users to perform self-service recovery for explicit systems.
- Added the ability to manage Linux accounts.
- Added the ability to manage SQL accounts.
- Added a new management console.
- Added filtering options for the System and Accounts views.
- Added New Jobs dialog.
- Added filtering options for the Jobs dialog.
- Added the Display Option column to the filtering options.
- Added more logging via the event viewer for password randomization jobs.
- Added a new web interface.
- Added the ability to control delegation via the web console application.
- Added the ability to delegate actions to users.
- Added the ability to delegate to Random Password Manager explicit accounts.
- Added the ability to view the rights of any user or group and how the rights were derived.
- Added support for multiple websites.
- Added cross domain authentication.
- Added support for web service website authentication.
- Added password checkout time extension option.
- Added the ability to check passwords in.
- Added the ability to limit the number of simultaneous passwords checkouts.
- Added a view which can see who has checked out a password.
- Added the ability for an admin to force a password check-in.
- Added more logging and log filters.
- Added the ability for a user to be notified that a password is not checked in before automatically randomizing the password.
- Added functionality to where checked-in passwords are set to randomize immediately.
- Added functionality to where checked-in passwords are randomized immediately.
- Added functionality to where password check-ins are blocked if the password is in use.
- Optimized database connectivity.
- Resolved memory usage issues for large queries.
- Resolved an issue with thread throttling not operating appropriately.
- Resolved an issue with alternate admins were not using stored passwords for necessary systems.
- Resolved an issue with password jobs not allowing you to reset the password length to 14 or more characters.
- Resolved an issue with the Export Systems List to Text File option resulting in a blank file.
- Resolved an issue with certain webpages not handling certain special symbols.

Version 3.03 (June 19, 2007)

- Added controls to the password propagation mechanism.

- Added console delegation, which allows administrators to select who can launch the Win32 Console.
- Added character constraints for password randomization.
- Added the ability to create custom LDAP queries which populate systems lists in the Dynamic Group settings.
- Added the ability to log password checkouts to a certain system's application log.
- Added a password check-in comment field.
- Added the ability for users to store their own passwords in the web interface.
- Added the ability to search and to filter results by system in the web interface.
- Resolved an issue where options would always resort back to System Name during a refresh operation no matter what options were selected.

Version 3.06 (February 5, 2008)

- Added the ability to manage Cisco IOS passwords.
- Added the ability to manage OSX passwords.
- Added the ability to use SUDO to change Linux/Unix passwords.
- Added the ability for RPM to provide formal / strict FIPS 140-2 certified encryption of passwords in the
- central database using an external certified software module.
- Added comments for external passwords in the password vault.
- Added comments for user passwords in the personal vault.
- Added an account selection dialog for creating password change jobs.
- Added the ability to manage remote connections via VNC, which requires VNC Pass.
- Added the ability to manage remote connections via terminal services such as RDP.
- Added the ability to manage remote connections via SSH, which requires a separate SSH install.
- Added the ability to manage remote connections via Telnet. The telnet client must be enabled on the target system.
- Added the ability to test remote connections via SSH.
- Added the ability to test remote connections via Telnet.
- Updated the website to no longer use sessions.
- Increased support for password changes on various flavors of Linux/Unix.
- Resolved a website issue resulting in incorrectly indexed links.
- Resolved an issue with RPM not using stored passwords for alternate connection credentials.
- Resolved an issue with RPM requiring administrative credentials to perform directory lookups for users and computers.
- Resolved an issue with deferred processors not always installing correctly during initial configuration of the tools.
- Resolved an issue with RPM not using SMTP Express for its mail server.
- Resolved an issue with RPM not adding missing users during a password change operation.
- Resolved an issue with IP scans failing to export systems to a specified systems list.
- Resolved an issue with the system ignoring the retry policy and trying to connect to failed systems.

Version 4.01 (March 16, 2008)

- Added custom propagations to call additional programs during propagation operations.
- Added custom propagations that can perform ASCII, Unicode, or binary file direct manipulation.
- Added RSA SecurID authentication for the win32 app.
- Added RSA SecurID authentication for the website.
- Added hardware encryption capabilities to work for any PKCS#11 Hardware provider, which enables FIPS140-2 Level 2 and Level 3 encryption.
- Added a password request workflow, allowing users to request access to passwords.
- Added a SDK for managing passwords in autonomous applications such as scripts, batch files, etc. using a scripting call to the secured password.
- Added support for Oracle databases.

- Added support for MySQL databases.
- Added support for named instances of MS SQL.
- Added support for mainframes such as OS390 and AS400.
- Added the ability to copy and move systems between systems lists.
- Added automatic re-randomization for all support account types.
- Added additional information in the website for easier system identification when dealing with multiple
- domains or IP resolutions.
- Added an option to display all operations logged in the web application.
- Added a Machine filter option for web logs.
- Added an item count for the Jobs monitor.
- Updated scheduled jobs update the scheduling information as soon as the job is changed rather than after the next run interval.
- Updated RPM to no longer hide disabled accounts.
- Updated the Comment field for explicit accounts to display in the web interface.
- Improved the load time for displaying passwords in the Win32. The win32 application no longer loads all passwords when performing a password recovery operation.
- Improved the default sorting to show the most recent jobs first.
- Changed the order of operations during an account rename and randomization job to allow the name to be updated prior to the randomization.
- Modified the interface to display a message notifying the user that a job must be selected before viewing any job details.
- Updated the system identification process to better detect when a system is listed multiple times with different system names.
- Resolved an issue with MS SQL password change jobs failing when the new password included a single or double quote mark.
- Resolved an issue with password verification jobs not sending emails.
- Resolved an issue with scheduled jobs not moving out of Retry status.
- Resolved an issue with scheduled jobs not stopping at the maximum retry interval limit.
- Resolved an issue with a display error appearing on the thread count.

Version 4.02 (June 12, 2008)

- Added time-based access controls for all website functions.
- Added the ability to refresh website permissions automatically without having to re-login.
- Added Remote Desktop (RDP/TS) functionality for the password recovery website.
- Added the ability to display passwords phonetically.
- Added an Accounts Store view.
- Added support for clustered services.
- Optimized the database I/O in the website.
- Optimized the database I/O in the win32 application.
- Resolved an issue with the system not being able to manage passwords consisting of 60 or more characters.
- Resolved an issue with SQL password change jobs not functioning properly when managing SQL 2000 and SQL 2005 passwords in the same job.
- Resolved issues with COM+ in IIS 7 (Server 2008).
- Resolved an issue with not being able to schedule system refresh job as desired.

Version 4.50 (September 3, 2008)

- Added a user Interface for zone processing operations.
- Added a dynamic group OU (LDAP) exclusion list.
- Added a web input for shared external accounts and passwords.

- Added a win32 bulk import operation for external accounts and passwords.
- Added the ability to display Linux/Unix accounts in the Account Store view.
- Added the ability to display database accounts in the Account Store view.
- Added the ability to display accounts for Cisco devices in the Account Store view.
- Added the ability to use Active Directory delegations to perform password changes for domain accounts. This action no longer requires administrative rights to manage domain account passwords on a domain controller.
- Added a website option to require users to enter a ticket number during a password checkout.
- Added a website option to require users to specify the exact system for password recovery.
- Added a website option to allow System Account Info columns to be disabled.
- Added a website option to redirect the password display page back to the main page after a set number of seconds to avoid displaying a password for too long.
- Updated and separated propagation steps for scheduled tasks and AT accounts.
- Updated and separated propagation steps for scheduled COM and D/COM tasks.
- Updated the Linux support library to enable better handling of various distros, such as SSH and keys.
- Resolved an issue with machines on the global exclusion list still being licensed.
- Resolved an issue with the explicit SQL connection limit not properly functioning.
- Resolved an issue with display options reverting to default settings.
- Resolved an issue with the export list to text file action.
- Resolved an issue with the display cache when switching from the Accounts Store view to the Accounts view.
- Resolved an issue with the animation timer.
- Resolved an issue with the Accounts view displaying incorrect last logon and password age information.
- Resolved an issue with custom propagations not properly functioning when using an explicit account or managed account fails

Version 4.70 (December 31, 2008)

- Added Event Sink Modeling.
- Added File Vaulting.
- Added more compliance reports.
- Added ability to schedule and capture compliance report data.
- Updated the system to have Password history enabled by default.
- Updated the website navigation.
- Updated the Linux Support Library in order to better handle various distros, etc.
- Resolved an issue with paging on personal not able to go beyond the first page.
- Resolved and issue with being able to access View Delegation rights without full access.
- Resolved an issue with zone processor editing.
- Resolved an issue with password history for external accounts.
- Resolved and issue with the Global System Exclusion list causing errors on a job with excluded systems.
- Resolved an issue with a password request not generating an email notification when SMTP Express was used as the email server.
- Resolved an issue with settings displaying incorrectly on the website when SMTP Express was used as the mail server.
- Resolved a Date/time issue for the non-US standard format.

Version 4.72 (March 16, 2009)

- Added the ability to email the new password to a specific email address when Windows accounts are changed.
- Added the ability to provide notifications of password recoveries for certain system lists to certain managers.
- Added status dialog for running threads and thread ID.
- Added the ability to search for accounts based on account comment field (website).
- Added the ability to edit accounts via the website, namely, to update passwords, comments, and delete account.

- Added “Number of systems to display” filter when editing a job.
- Resolved an issue to allow all dropdown lists in management app and website to be alphabetized.
- Resolved an issue so that account comments will wrap based on screen size.
- Resolved an issue so that custom propagation no longer defaults to turning on file copy causing errors if not explicitly turned off when no files are being copied.
- Updated the SSH/Telnet Library for better multi-threading support and handling for non-standard configurations.
- Resolved an issue where Import external account for single entry and System field is not correctly parsing selected system names when [all highlighted systems] is selected.
- Resolved an issue with AS/400 support.
- Resolved an issue where logging errors during password propagation job that showed AT account failed to be managed (display issue only).
- Resolved an issue so that enumeration of accounts in an Oracle database instance can now be properly enumerated for account store view.
- Resolved an issue so that enumeration of accounts in an MS SQL database instance can now be properly enumerated for account store view.

Version 4.80 (May 26, 2009)

- Added DB2 Account Discovery.
- Added management of SCOM Run As Accounts.
- Added SCOM 2007 Run As Account account discovery.
- Added management of IIS 7 Application Pools.
- Added IIS 7 Application Pool Account Discovery.
- Added SCOM 2007 and SCCM 2007 Management Pack Extras.
- Added Accounts Store view - list of all services, tasks, COM/DCOM, IIS, Application Pools, SCOM Run As account lists.
- Added new website option to [dis-]allow editing of random passwords via website.
- Added more filtering options in jobs dialog to account for different job states and status.
- Added Account Elevation, enabling a user's group membership on a target system to grant elevated privileges.
- Added auto-index tuning support to SQL 2008.
- Update makes is possible to manage non-root accounts on Linux/Unix/OSX targets on a scheduled basis.
- Update makes is possible to manage Login accounts used for "SU to Root" password management.
- Update added more options for SDK, as well as support for SCOM/SCCM Management Pack.
- Linux Support Library updated with better multi-threading abilities and troubleshooting.
- Update makes is possible to manage SSH and Telnet port usage for system refresh, account discovery, and password change jobs.
- Non-Windows systems are no longer displayed in the Windows systems view.
- Change made so that user is prompted to update next run time display when deleting jobs or modifying jobs (has no effect on next run time).
- Resolved an issue with some event sink notifications not working as expected.
- Resolved an issue with Oracle password change jobs not always working.
- Resolved an issue with "Anonymous" account for virtual directories and "non-default websites" not being discovered.
- Resolved an issue with RDP via web not working on Vista/2008 ActiveX.
- Resolved an issue with self-recovery rules returning invalid number of arguments error.
- Resolved an issue with the system not discovering scheduled tasks with Run As information on Windows Vista/ 2008.

Version 4.81 (October 9, 2009)

- Added the option to use Oracle database (11g) as a backend data store.

- Added the option to use any LDAP compliant directory for user authentication (e.g. Oracle Internet Directory, Open LDAP, Tivoli Directory, etc.).
- Added the option to manage accounts in any LDAP compliant directory.
- Added account discovery for any LDAP compliant directory.
- Added verification for stored Linux and UNIX passwords.
- Added SSH connection for Cisco and IOS type devices.
- Added retry DB connection if DB is not available on first connection.
- Added feature so that SDK can generate a random password when importing external accounts.
- Added feature so that jobs can be disabled and copied - Job Templates.
- Added job run-time window (specified amount of time Job can run).
- Added management of Sybase Database accounts.
- Added discovery of Sybase Database accounts.
- Added App Pool Management for IIS 6.
- Added account propagation for MS SQL jobs.
- Added account discovery for MS SQL jobs.
- Added account propagation for SharePoint farms.
- Added account discovery for SharePoint farm.
- Added file propagation for non-Windows systems and devices.
- Added feature so that file propagation now creates a backup copy of the file being modified.
- Added feature to launch arbitrary program for non-Windows systems and devices.
- Added more event sinks.
- Added feature so that multiple propagation steps can be tied together and ordered (Aggregation of multiple base types).
- Added feature so that propagation and discovery can be targeted by operating system as well as by system set.
- Added role based authentication for website.
- Added response file generator to help resolve connection and management issues for non-Windows systems.
- Update allows for Alternate Administrative credentials to now be stored in the database.
- Update allows for website settings to now be stored in the database.
- Update allows for explicit accounts to now leverage a personal password vault.
- Update allows for heartbeat monitor to reset a job status if the job gets killed so job is not left locked.
- Update added additional options to allow Linux/UNIX to handle slow responding systems (step timeout).
- Update added database improvements so that dynamic group updates that took 45 minutes+ may now take only a few minutes.
- Update allows for integrated or explicit authentication to be used for discovery and management of MS SQL databases.
- Updated the handling of OS/390 and AS400.
- Index optimizer is now allowed to work with MS SQL 2008.
- Account map (self-recovery) now requires an account name, in addition to a system name.
- "Linux Support Library" is now called "Cross Platform Support Library".
- Resolved an issue to allow accounts used in non-default (secondary) websites in IIS to be properly discovered.
- Resolved an issue were the event sink heartbeat monitor would cause deferred processor to hang or stop processing job all together, leaving the job in an indeterminate state.
- Resolved an issue where, when creating a password change job from account store view for a Linux or UNIX system, the account name would auto-populate as "Root" and not "root".
- Resolved an issue to that a fully decorated account name is now displayed for SCOM RunAs accounts.
- Resolved an issue with testing SSH and Telnet connections.
- Resolved an issue where multiple event sink events could not be used in a single event sink.
- Resolved an issue where a job would run against all systems instead of just new systems when added through dynamic group updates.
- Resolved an issue where SDK could fail to enroll systems.

Version 4.82 (April 21, 2010)

- Added per system-set delegations.
- Added new propagation - update system logon cache.
- Added new propagation - auto-login account.
- Added new propagation - user defined propagation target (arbitrary process).
- Added verification for stored MS SQL passwords.
- Added verification for stored Linux/UNIX passwords.
- Added the option to name and save custom propagation steps.
- Added new options to view, run, delete jobs options to web interface.
- Added the capability to enable jobs for delegations via website.
- Added full password history, which includes all passwords ever attempted to be set.
- Added SDK configuration settings manager and tester.
- Added option to website configuration to set website address (used for auto-launch of website).
- Added recursive membership lookups for website authentication.
- Added website option to disable COPY button.
- Added website option during password request to define incident or change.
- Added incident or change option to determine alert status from website.
- Added a number of answer files for various platforms included in the "AnswerFiles" directory in the installation directory.
- Added support for DRAC IPMI remote management cards.
- Added DRAC node in the accounts store view.
- Added more event sink options for alerts - MSMQ and ArcSight.
- Added ability to set system set comments.
- Added more password change options for AS400.
- Added more password change options for OS390.
- Updated the cross platform support library code error handling.
- Updated the cross platform support library logging.
- Updated the cross platform support library threading.
- Updated support for all platform types when adding systems from website.
- Update ensures that code for how long password requests will be displayed in the website.
- Updated internal query and insert routines to improve database performance when using SQL.
- Updated memory usage for large queries and inserts.
- Updated the response file timeout options.
- Resolved an issue with Sybase accounts not being properly discovered.
- Resolved an issue with Sybase database where, if an account used to change other accounts was also managed, subsequent password change jobs would fail.
- Resolved an issue with Oracle database where, if an account used to change other accounts was also managed, subsequent password change jobs would fail.
- Resolved an issue with MS SQL where, if an account used to change other accounts was also managed, subsequent password change jobs would fail.
- Resolved an issue with MySQL where, if an account used to change other accounts was also managed, subsequent password change jobs would fail.
- Resolved an issue with task names not being discovered/displayed when determining local account usage.
- Resolved an issue where, when running arbitrary processes, created processes would not always run.
- Resolved an issue where account names with a % in their name could cause personal vault to not work.
- Resolved an issue where SDK could not work without integrated authentication because of an error in ASP processing page.
- Resolved an issue where System tester would report encryption was enabled when it wasn't.

- Resolved an issue where copy function would copy incorrect characters.
- Resolved an issue where when selecting a Linux account rather than system for password change, a job would not get created correctly.
- Resolved an issue with AS400 not auto-rolling passwords following recovery.
- Resolved an issue with OS390 not auto-rolling passwords following recovery.
- Resolved an issue with OS390 not auto-rolling passwords following a schedule.
- Resolved an issue where OS390 was tagged as wrong system type in website.
- Resolved an issue where private password vault could generate an error following recovery.
- Resolved an issue with RSA compatibility with 64bit systems.
- Resolved an issue where adding and external password to the store from the management console was not working properly for single system import.
- Resolved an issue where email reports for password verification or other mail enabled items were not being formatted correctly.
- Resolved an issue where some compliance reports collected incorrect information.

Version 4.82a (April 28, 2010)

- Resolved an issue where some propagation steps would not work in allowable configurations.

Version 4.83 (July 8, 2010)

- Added out of the box support for more SSH / Telnet devices.
- Added standard configuration dialog for BMC Remedy integration.
- Added more Event Sinks.
- Added extended SDK support to non-Windows clients via Java SDK.
- Added support for non-standard port configuration for all database types.
- Added Per Account Delegations.
- Added future checkout of passwords.
- Added feature so that all delegations support semi-colon delimited email lists (instead of singular email addresses).
- Added feature so that event sinks now support semi-colon delimited email lists (instead of singular email addresses).
- Added new event sinks output type - Run arbitrary program.
- Added non-standard port support for password recovery website configuration.
- Added non-standard port support for password recovery website configuration when using SDK.
- Added feature so it is possible to target a domain controller for account elevation to a domain level group.
- Added feature so that a non-local admin can launch ERPM by pre-specifying a run-as account within the program.
- Resolved issue with account comment behavior when updating accounts via the web console.
- Updated where certain operations are performed from DB to main memory to contend with MS SQL limitations.
- Updated the management of MS SQL performance statistics for auto-index creation.
- Resolved an issue where propagation for IIS 7 application pools would improperly re-write domain name.
- Resolved an issue with the custom connection string for Oracle databases not always working as expected.
- Resolved an issue where the Auto-logon propagation was examining the incorrect registry key.
- Resolved an issue with the auto-logon propagation not properly recording fail-to-update events.
- Resolved an issue with the remote web-site deployment not copying all required files, causing Syslog write events to not occur.
- Resolved an issue with websites where, if the compliance DB had been setup but had not previously gathered a data capture from the console, the webpage could error.
- Resolved an issue where a missing session cookie information from some web pages could cause sessions to be terminated when using Internet Explorer.
- Resolved an issue where web terminal services sessions would not always properly initiate a web terminal session.

- Resolved an issue with OS Type on system set properties not working for any system type property other than 'Explicit Inclusions'.
- Resolved an issue with Move/Copy function not adding selected systems to destination system set's 'Explicit Inclusions' list.
- Resolved an issue with the IP Scanner not working.
- Resolved an issue with the system set properties IP Scanner not working.
- Resolved an issue where, when using an Oracle database, a user with "View Systems" global delegations could not view any systems.
- Resolved an issue where sorting by account name in the website could cause a system to incorrectly appear twice.

Version 4.83.1 (December 3, 2010)

- Added integration for Microsoft System Center Service Manager.
- Added integration for Q1 Labs QRadar.
- Added integration for Privileged User Management (PUM) Systems.
- Added account properties for Linux accounts.
- Added account properties for Microsoft SQL database accounts.
- Added account properties for Sybase database accounts.
- Added account properties for Oracle database accounts.
- Added more event sinks for new integrations and various product actions.
- Added multi-instance/multi-system password change jobs for Microsoft SQL databases.
- Added multi-instance/multi-system password change jobs for Oracle databases.
- Added multi-instance/multi-system password change jobs for Sybase databases.
- Added multi-instance/multi-system password change jobs for MySQL databases.
- Added dynamic port connectivity for Microsoft SQL.
- Added IPMI Device management using IPMI protocol for password management.
- Added IPMI Device auto-discovery.
- Added IPMI Device account discovery.
- Added Web app color option – green bar – alternating rows can have a color defined for easy line identification.
- Added Web app ticket number verification for BMC Remedy & Microsoft SCSM.
- Added Open web application log via context menu from 'Manage Web App' dialog.
- Added Additional ‘Account Elevation’ settings for local systems or domains.
- Added Web application security options – disable multiple concurrent logins from single user.
- Added Web application security options – embed unique identifier with each page.
- Added Web application security options – use a unique identifier for each request.
- Added Web application security options – disable explicit web application accounts.
- Added Web application security options – store only authentication token in the cookie.
- Added Web application security options – force logout on any page error.
- Added feature so the Web application log can be opened from the management console “Manage Web App” dialog.
- Added option to validate the generation of all event sinks to the target output.
- Added additional configuration options for BMC Remedy integration.
- Added feature to make it possible to select Telnet or SSH for connection with Linux/UNIX node.
- Added feature to make it possible to collect system information for Linux/UNIX systems.
- Added MS SQL Database index defragment utility and statistics regeneration for database optimization.
- Added Web application error logging in the website.

- Added feature so when a request for a password is made, the request comment is now visible in the web interface from the requestor for the password approver.
- Added support for CTR negotiation to SSH protocol.
- Added more options for SDK such as randomizing a password.
- Updated databases so that they are no longer explicitly tied to systems; adding a database no longer auto-adds the host system to the list.
- Update the custom account stores to provide for admin configuration of target settings and default login accounts.
- Updated authentication server settings to now examine 'default naming context' for base LDAP path.
- Updated authentication server search filter to now use paging to better handle large searches.
- Updated Website options so they can be edited per instance without affecting the default configuration.
- Updated Website page layouts to move all 'actions' closer to the system and account name columns.
- Optimized the zone processor job handling on large system sets.
- Updated the namespace categorization for databases.
- Updated session timeouts to cause the website to force logoff and clear session cookie.
- Updated the order of global delegation rules.
- Resolved an issue with web application crashes due to improper application unloading.
- Deferred processor and zone processor lag for large system set job processing.
- Resolved issue with explicit password input via the website causing an error and/or logging out the user.
- Resolved issue with compliance reports being unable to run if the dataset was too large.
- Resolved issue with compliance reports not running if using an Oracle database.
- Resolved issue with indexes not getting created on certain Oracle tables.
- Resolved issue with IIS 7 Propagation.
- Resolved issue with re-logging a checkout when re-viewing an already checked out password.
- Resolved issue with Linux/UNIX auto-roll jobs getting created with Telnet rather than SSH selected.
- Resolved issue with Leading and trailing spaces in system names so that they are no longer treated as real characters.
- Resolved issue with password change job not succeding when constraint option to 'Prevent username from appearing in password' was enabled.
- Updated zone processor state status so it works correctly.
- Resolved issue with password requests being immediately expired.
- Resolved issue with semi-colon delimited email list issues for client agent.

Version 4.83.2 (July 19, 2011)

- Added OATH Token support for console startup - HOTP/TOTP/Yubico via SMS/Email/Device.
- Added OATH Token support for client access to password recovery website -HOTP/TOTP/Yubico via SMS/Email/Device.
- Added OATH Token Auto Enrollment.
- Added Pass-thru SSH session for non-Windows systems.
- Added pass-thru Telnet session for non-Windows systems.
- Added IBM WebSphere Account Propagation.
- Added Oracle WebLogic Account Propagation.
- Added SQL Reporting Services Account Propagation.
- Added ViewDS LDAP Directory as a default LDAP directory type.
- Added HP Service Manager direct integration for ticket creation and verification.
- Added auto-enumeration of MS SQL Database instances.
- Added support for TN3270 Terminal Types.
- Added arbitrary account elevation - helpdesk feature.

- Added customization of email templates for emails sent from website.
- Added IPMI power operations via website.
- Added SDK options - support for IPMI power operations.
- Added RADIUS authentication.
- Added support for UPN names.
- Added SQL server custom schema support.
- Added text file mapping import for all management types.
- Added more event sinks.
- Added filter for Management Set dialog.
- Added default protocol/answer file configuration for non-Windows systems using answer files: Custom Communication Types.
- Added standalone installer for integration components to ease remote website and zone processor deployment.
- Added standalone installer for event server COM wrapper to supplement event sink integration for remote website and zone processor deployment as needed.
- Added favorites icon to website (URL link).
- Added more functionality to JAVA SDK operations.
- Added more functionality to Windows only SDK operations.
- Added more functionality to Web Service operations.
- Added new website display mode to reduce number of queries performed to database.
- Added ability for website auditing to log permission changes made from management console.
- Changed Oracle database account enumeration to better work with versions prior to 11g.
- Changed account bulk import to support all name spaces.
- Changed website options so that logging password actions to event log with blank field will default to local system's application log.
- Changed how pressing F5 works when in the jobs display, so that it no longer initiates whatever job is highlighted.
- Changed the description and comment field so it is now available to private password store.
- Removed SSH/Telnet/RDP icons from web UI for a more consistent feel.
- Updated the format of the data being sent to Remedy/HPSM/SCSM to be more descriptive.
- Changed the confirmation on password delete from website.
- Changes made to the account stores (databases, IPMI, LDAP directories) so they are now counted as systems.
- Updated IPMI devices to support v1.5 and v2.0.
- Updated the LDAP authentication servers so they can now choose to page for accounts list result – some LDAP systems require and some don't.
- Updated the password settings dialog for better identification of options being set.
- Updated the event sink data elements sent to include more information across all event sinks.
- Updated Java SDK propagation with support for all name space attributes.
- Updated the query code for website user logon.
- Updated the query code for website user permissions verification.
- Updated the query code for next job run.
- Updated the Move/Copy system to support databases.
- Updated the Syslog to support an alternate port.
- Updated the authentication servers list so it can be ordered (affects website logon).
- Updated many event sink's message data to include more useful information.
- Updated the console display options to remove unused display filters.
- Moved "Delegations" to be a top-level menu item.
- Updated the error reporting for some web operations.
- Resolved an issue with LDAP users not being able to properly authenticate to the website, which resulted in failed logins.
- Resolved an issue with some LDAP directories not paging query results correctly.
- Resolved an issue with Microsoft System Center Service Manager ticket verification not working.

- Resolved an issue with Microsoft System Center Service Manager ticket creation not working.
- Resolved an issue where a testing event sink output for certain output types could cause the management console to crash.
- Resolved an issue with all access web account being able to view all personal passwords.
- Resolved an issue with per account delegations not working for Databases.
- Resolved an issue with per account delegations not working for LDAP directories.
- Resolved an issue with delegation changes made in the console getting logged with the responsible user account in the website.
- Resolved an issue with zone processors not retrying failed jobs.
- Resolved an issue with the workflow icon not showing up for users with outstanding password requests.
- Resolved an issue with many cases that could cause function block errors in the website.
- Resolved an issue where searching for '[' in any table would never return results.
- Resolved an issue where spin jobs created for various account store types would be generated with incorrect settings.
- Resolved an issue with alternate port support for SSH/Telnet connections not working properly for account discovery.
- Resolved an issue with website COM object sometimes crashing on exit.
- Resolved an issue where the deferred processor could sometimes crash on exit.
- Resolved an issue to make IIS 6 Web Services properly enumerated.
- Resolved an issue with failure to move database account stores.
- Resolved an issue with failure to move LDAP account stored.

Version 4.83.3 (December 15, 2011)

- Added SAP NetWeaver as a management target (Custom account store type library).
- Added McAfee EPO as a management target (Custom account store type library).
- Added Oracle WebLogic as a management target (Custom account store type library).
- Added IBM WebSphere as a management target (Custom account store type library).
- Added DSRM (Directory Service Restore Mode) password management.
- Added Password Spreadsheet Manager to allow users to import and maintain their password spreadsheets.
- Added Password spreadsheet import utility.
- Added Delegation and workflow system for Password Spreadsheet Manager.
- Added ability for personal password store to support website links.
- Added ability for personal password store to support description fields.
- Added personal password store disclaimer field.
- Added configurable themes to the web interface.
- System metadata now visible in website.
- Added links from systems/devices to accounts and account information/metadata.
- User account metadata now available in website.
- Added password history popup to the web application.
- Added system type categorization menu in website navigation menu - can select all systems/devices by system or device type.
- Added account type column and filter to the password store page of the web interface.
- Added web application configuration option to the security tab to prevent a user from granting their own password request.
- Added website delegation permission to allow users to add/edit/delete stored passwords on account stores that they already have access to.
- Added import/report to the permissions on accounts delegation dialog.
- Added import/report to the global delegations dialog.

- Added import permissions menu to the main dialog and added several global permission import operations.
- Added import/export feature for permissions on groups.
- Added auto-population of IPMI account store with IPMI credentials if they were successfully used to connect after a scan.
- Added Select-All button on the IPMI scan dialog.
- Added automatic population of the password store with credentials after any successful connection.
- Password change job can now set comments for managed accounts.
- Password change job will now allow selecting to run a job against only selected targets or all systems/devices in the management set.
- Added menu and option in the orphaned systems dialog to clean up some account store information in group database references for groups that are deleted.
- Added progress indicators for jobs while running to the status message in the deferred job display.
- Added progress indicators for jobs that have failed to the deferred job display.
- Added context menu on Jobs in the Jobs dialog to open the verbose text log.
- Added filter for Per Management Set delegations dialog to show only management sets with permissions assigned.
- Added filter for Per Account delegations dialog to show only Accounts with permissions assigned.
- Added filter for Per System delegations dialog to show only systems with permissions assigned.
- Added job affinity to the zone processor config to allow password change, refresh, and group update jobs.
- Added ability to deploy zone processors that are not group locked.
- Added password activity report in the web application.
- Added report generation utility to interactive job completion status dialog.
- Added report generation utility to job properties dialog.
- Added job completion statistics to Jobs management console dialog.
- Added job completion statistics to Jobs web dialog.
- Added network path credentials to IIS6 and IIS7 account usage discovery.
- Added network path credentials to IIS6 and IIS7 account usage.
- Added SSH support to IBM WebSphere account usage propagation.
- Added SSH support to Oracle WebLogic account usage propagation.
- Added ping utility from context menu of management console.
- Added ability to view system details from context menu of management console.
- Added more default answer files.
- Added SSH and Telnet support for custom types that are telnet and SSH.
- Added progress dialog popups for long-running database operations and display draw operations.
- Added multiple [subsystem] logging options to log settings dialog.
- Added Linux system info caching to the job dispatch loop to minimize database deadlock frequency on frequent data lookup for system/stored password info during SSH operations.
- Updated default behavior to the web application instance dialog editor to edit the configuration of selected instances.
- Updated website filters to mandate selection of a system type.
- SSH/Telnet Library is now a native code implementation rather than a managed code implementation - resolves memory and handle leaks from previous versions.
- SSH/Telnet Library now supports all five variables for all sections (Login Account, Login Account Password, Change Account, Change Account Password, New Password).
- SSH/Telnet Library is now using a new set of variables that are consistent across all portions of the answer files.
- New installation mini-setup wizard now prompts for encryption settings.
- New installation mini-setup wizard now prompts website installation.
- Updated UPN caching algorithm in management console Accounts Store view that would cause excessively long load times when hundreds of domain controllers for the same domain were in the same management set.
- Updated the web application auto-installation procedure so it configures settings for File Vault when file vault is enabled.

- Updated IBM WebSphere web integration so it no longer requires a static account.
- Updated Oracle WebLogic web integration so it no longer requires a static account.
- Truncated the web activity log export to top 1000 rows to prevent the render from taking too long and timing out the dialog.
- Updated the DB query code for auto-created views.
- Updated the Oracle query code for large scale operations.
- Resolved an issue with function Block Error if telnet/SSH was not enabled globally.
- Resolved an issue with Required DLLs for SSH/Telnet functionality that were not being copied to target ZP systems when doing a zone processor install/remove.
- Resolved an issue with improper logging of the authenticator name in the audit log if OATH token login was being used.
- Resolved an issue with Username format not being persisted in the OATH token config dialog after selecting a domain user from browse.
- Resolved an issue where Check to see if RDP access is granted would cause an assert and fail.
- Resolved an issue where IPMI systems would show up in the list in the web interface once per group they were in.
- Resolved an issue where after removing a custom account store from the list the count would not update until next refresh.
- Resolved an issue with change and remove options would not displaying when viewing passwords in the web interface for randomized accounts with dynamic website display options enabled.
- Resolved an issue with cropping problem on the systems page for the job wizard.
- Resolved issue with spelling errors.
- Resolved resizing issues in the web application on certain context menu options mouse-over events.
- Resolved an issue with permissions on accounts dialog having an extra column.
- Resolved an issue with assertion errors when expanding a SharePoint node in the Accounts Store view.
- Resolved an issue with Error on attempted deletion of a locked job.
- Resolved an issue where Jobs could immediately show failed status after stopping a job in progress.
- Resolved an issue with Uninitialized variable for the Linux password change page that would sometimes cause the login username and password field to not show up.
- Resolved an issue where Dynamic group updates involving large explicit exclusion lists could take an excessive amount of time to update.
- Resolved an issue with authentication failures during IPMI operations to report as successful completions.
- Resolved an issue where editing the schedule of a failed job would not reschedule the job.
- Resolved an issue where blank files could cause errors when checking out the file from the file vault.
- Resolved an issue where stored jobs dialog would provide additional filters that could not be used when filtering for an account name.
- Resolved an issue with Email alerts for recovered passwords not occurring for email addresses configured in the global delegations.
- Resolved an issue with File vault being inaccessible to users if the website security option to only store authentication information in the cookie was enabled.
- Resolved an issue where Active Directory account password change would fail when delegated rights were only set for "reset password".

Version 4.83.4 (July 2, 2012)

- Added Per user definable dashboards.
- Added Dashboard configuration control.
- Added Dashboard data audit drill down and visualization.
- Added pure certificate based authentication and authorization.
- Added CAC/PIV card support.

- Added Website support for automatic login after user-certificate identification.
- Added ability for RDP account pass-thru accounts to be used for any system.
- Added ability for SSH account pass-thru accounts to be used for any system.
- Added Multi-RDP Gateway support.
- Added configuration to enable/disable multiple per-user simultaneous RDP sessions.
- Added configuration to enable/disable multiple per-user simultaneous SSH sessions.
- Added configuration to enable/disable multiple per-user simultaneous telnet sessions.
- Added additional telnet support for Linux/UNIX node.
- Added additional telnet support for custom account store node.
- Added SSH/Telnet support sixth new replacement variable for target system.
- Added multi-language support for web interface including Chinese (traditional and simplified), Arabic, German, French, Italian, Hungarian, and more.
- Added multi-language support configurations per user profile.
- Added scheduled refresh operations for system enumeration.
- Added scheduled refresh operations for account enumeration.
- Added scheduled refresh operations for account usage discovery.
- Added ability for self-service account elevation jobs to provide for an elevation comment.
- Added pre-populated list of common groups to the arbitrary account elevation page so a user can choose a group instead of typing one in.
- Added password confirmation field for static passwords in password change jobs.
- Added progress indicators for jobs in progress in the web application.
- Added automatic Oracle database detection for Windows systems.
- Added account usage display in the web interface.
- Added test connection option for MS SQL databases.
- Added test connection option for Oracle databases.
- Added job Queue dialog for determining which job is running, which job is next, and other job information.
- Added ability for zone processors to handle parts of password propagation jobs for propagation targets that are within their zone.
- Added ability for zone processors to perform account elevation jobs.
- Added ability for zone processors to perform system refresh operations.
- Added ability for zone processors to perform password verification reports.
- Added orphaned job unlock code to the scheduling service to unlock and reschedule jobs that are found locked by the current system when the owning process no longer exists.
- Added compliance snapshot jobs as a supported type of job that can be run by a zone processor.
- Added unique event sink message for adding/changing managed passwords through the web app.
- Added password verification for accounts on non-Windows systems managed by SU or SUDO.
- Added SSH/Telnet target types configuration option to always load stored password.
- Added security option on website configuration to block session if more than N number of requests per second is received from session.
- Added Oracle database password verification.
- Added compliance report for all stored shared credentials.
- Added password history accessible via website.
- Added support for asset tag in the management console.
- Added visible and searchable asset tags to the web interface.
- Added ability to import custom account store systems via text file import.
- Added on-demand token code support for RSA SecurID token checks.
- Added support for system-generated RSA SecurID PIN codes for the web application.
- Added option to disable LDAP servers for use as authentication servers.
- Added account elevation jobs filters available in the jobs page filter list in the web interface.
- Added various interstitial dialogs in web application to indicate work being done.

- Added various interstitial dialogs in management console to indicate work being done and actual progress.
- Updated the way deferred processors will examine jobs left in a partially complete state to determine if they need to be completed.
- Updated management set database query string length to support 1024 characters (up from 255).
- Updated web application schedule permission restriction code to allow daily restrictions to carry over from PM to the next day's AM times.
- Updated schedule restricting users attempting to login when their login permission was restricted to a schedule restriction message.
- Updated way in which LDAP password change jobs would always use the managed account to change its own password.
- Updated the input method for SSH/Telnet connections so now it passes a single character at a time.
- Updated the tab order for various dialogs.
- Updated the mnemonic controls in various places in the management console (Section 508 compliance).
- Resolved an issue with password cache population problems for Cisco password changes.
- Resolved an issue with password cache population problems for LDAP password changes.
- Resolved an issue with password cache population problems for Oracle password changes.
- Resolved an issue with password cache population problems for Sybase password changes.
- Resolved an issue with password cache population problems for MySQL password changes.
- Resolved an issue with password cache population problems for MS SQL password changes using explicit accounts.
- Resolved an issue with password cache population problems for IPMI password changes.
- Resolved an issue with known passwords discovered as valid for IPMI devices not being associated with IPMI device.
- Resolved an issue with date time pickers in website filters for account elevation.
- Resolved an issue with service propagation not propagating to services configured with UPNs if service and account had not already been previously enumerated.
- Resolved an issue with text file discovery on non-Windows systems.
- Resolved an issue with text file propagation on non-Windows systems.
- Resolved an issue with process initiation on non-Windows systems.
- Resolved an issue where adding a personal password was not associated with the correct menu sections in the web interface.
- Resolved password cache concurrency issues during multi-threaded SSH operations.
- Resolved an issue with bug in the web interface that was causing false positive errors to be logged on some page loads.
- Resolved an issue with RDP sessions liable to create duplicate log entries per connection.
- Resolved an issue with HTML markup characters in password list entries causing the password list pages to fail on various operations.
- Resolved an issue with DCOM application name not being properly populated in memory during a propagation, causing confusing log messages.
- Resolved an issue where the program log would show internal warnings when attempting to expand JavaSDK entries for account usage.
- Resolved an issue with Password check-in comments not being required even when enabled.
- Resolved an issue where event sink logging was not always including the web logins responsible for the event.
- Resolved an issue where .\AccountName was being ignored for service account name matching when using local accounts on 2008 and later systems.
- Resolved an issue with the system page of the job sheet showing incorrect next retry times for jobs that were partially complete.
- Resolved an issue where Generate full stats on all tables would fail if a custom tablespace name was used.
- Resolved an issue with LDAP connection throwing an error if integrated authentication was used and a user login name was not provided.
- Resolved an issue with permissions on password list check failing if one of the identities that had permissions assigned has been deleted.

- Resolved an issue where Windows integrated authentication could bypass Oath token checks.
- Resolved an issue with DB2 custom connection strings not working.
- Resolved an issue with Errors on SQL server refreshing if the name-case (upper-case) was incorrect in the program data store.
- Resolved an issue with not being able to add new credentials to an existing password list for Password Spread Sheet Manager feature.
- Resolved an issue where certain delegation import features opened the export dialog.
- Resolved an issue where certain delegation export features opened the import dialog.
- Resolved an issue where removing item with account info from database option in management console did not work.

Version 4.83.5 (October 21, 2012)

- Removed support for Windows Server 2003 as a hosting platform.
- Added additional user interface languages: Danish, Dutch, Finnish, Hebrew, Hindi, Japanese, Korean, Norwegian, Russian, Swedish, Tagalog.
- Added SAP Certified password management via SAP NetWeaver Gateway (We are now an SAP Partner).
- Added more event sinks.
- Added additional permissions for viewing password history.
- Added additional permissions for viewing account activity.
- Added SDK options for file vault management.
- Added SDK options for shared password lists.
- Added automatic Index Creation deadlock resolution via index deletion.
- Added Add account lockout for web access (website options).
- Added dialog to monitor user lockout status and reset logouts selectively.
- Added control for number of rows to export when exporting audit logs from website (website options).
- Added Active Directory domain account restrictions to target OUs for user discovery or exclusion from discover.
- Added OLEDB timer override (Datastore Config) to aid in slow databases and long running queries.
- Added RPC Kill timer to help deal with hung RPC calls to unhealthy Windows systems.
- Added password change that provides the option to unlock an account (Windows).
- Added SOAP web service interface.
- Added explicit impersonation in the SOAP web service.
- Added OData web service interface.
- Added support for international characters in email messages.
- Added the ability for password jobs to load any stored credential for non-Windows systems.
- Added password history for shared password lists.
- Added the ability to specify SSH port on auto-SSH connection per system.
- Added ability to auto-SSH for custom account store types that use SSH.
- Added wild card search in website for account names when mandatory account search requirement is enabled.
- Added SDK option to retrieve stored passwords and ignore password checkout flags.
- Added email field cache for password requests in the web interface when users do not have a pre-defined email address.
- Updated the way a job removes the restricted system on subsequent run when a system is added to the restricted systems list after being added to a job.
- Updated the way a cloned job inheriting the statuses of its parent job.
- Updated certain logging functions and heuristics to try and avoid confusing log messages.
- Updated startup algorithm to improve console launch time when management set objects have overlapping ranges (duplicated systems).

- Updated installation routines for Dashboard visualization installations.
- Updated the SDK password set command so it will add passwords to shared list if not found.
- Updated several file vault logging messages to include the symbolic name of the file affected as well as the fileID.
- Updated the way setting auto-logins works, so that the system will check for target computer's bit level (32 v 64) to write to the correct registry location.
- Updated the process for selecting multiple accounts to create a password change job and choosing the run immediately option, so that jobs get scheduled to run now, rather than actually attempting to run immediately.
- Updated the IntegrationComponents supplemental installer so it can choose the proper installation path for zone processor installations.
- Updated Microsoft RDP ActiveX component to version 5.2.3790.4252.
- Updated EasyMail SMTP & SSL components to version 6.5.
- Updated ArcSight CEF output and parsing.
- Resolved an issue with Windows 2008 R2 systems OS TYPE incorrectly reporting as Windows 7 systems in web interface.
- Resolved an issue where systems added to restricted systems list after being added to a job would cause job to fail.
- Resolved an issue with cross-site scripting exploits.
- Resolved an issue with service accounts defined via UPN so that they are properly handled on first password change without requiring pre-discovery.
- Resolved an issue where performing an IP scan for systems when OS type is set for Linux and the system responds could cause a crash.
- Resolved an issue with the default button on website login page not working.
- Resolved an issue with integrated authentication in website not working if automatic login was also not enabled.
- Resolved an issue with syslog CEF output of heartbeat monitor event sink causing an error rather than log.
- Resolved an issue where certain scenarios could cause the job thread dispatcher to prematurely delete state, resulting in memory leaks.
- Resolved an issue where, when management set type was set to Linux, objects under the Linux/UNIX node would be added or removed simply because the management set was updated.
- Resolved an issue with upgrade code when dealing with custom schemas.
- Resolved an issue where database migration steps not present in v4.83.4 could cause basic password change jobs to fail.
- Resolved an issue with database migration steps not present in v4.83.4 could cause propagation steps to fail from previously existing jobs.
- Resolved an issue with file store problems when using custom schemas.
- Resolved an issue with compliance Database problems when using custom schemas.
- Resolved an issue with custom LDAP filters for Active Directory domains not working.
- Resolved an issue with Oracle password changes not propagating.
- Resolved an issue where Oracle instances page would not show all correct oracle instances unless account had all access.
- Resolved an issue where deleting a password from password history would delete all entries from the history for that computer/system.
- Resolved an issue with not being able to enter the same system name into multiple custom account stores.
- Resolved an issue with RSA Login page in the web interface preventing set pin mode to work correctly.
- Resolved an issue with RSA SecurID not working in next PIN mode.
- Resolved an issue with the displayed number of targets in a management set not including custom account stores.
- Resolved an issue where saving new passwords to the password store with encryption disabled would log asserts.
- Resolved an issue with Web interface account filters not working if the user also had account masks defined in their delegations.
- Resolved an issue with alternate administrator accounts access and stored credential access not working in certain scenarios.
- Resolved an issue with Web application not showing account filter if a non-All access user was logged in.

- Resolved an issue with password recovery email alert using incorrect email template for notification.
- Resolved an issue where the main dialog would exit when admin reporting job could not be verified.
- Resolved an issue with importing delegation identities and permissions failing because it expected the import file to contain extra columns.
- Resolved an issue with the scenario where users could not create new delegation permissions on files in the file store.
- Resolved an issue with text for requesting a password list password showing deny request.
- Resolved an issue with SDK (COM version) GetStatusSettings failing.
- Resolved an issue with users without grant all access not being able to see accounts other than Windows.
- Resolved an issue with "Run job on new systems" being erroneously set.

Version 4.83.6 (May 17, 2013)

- Added Web Service Interface which exposes hundreds of functions via SOAP & WSDL.
- Added PowerShell CMDLets to make use of new web service interface and functions.
- Added Password Compartmentalization - 4-Eyes password retrieval (FR 379, 380).
- Added Standalone zone processor installer (FR 309).
- Added Certified McAfee EPO integration - EPO can consume information from ERPM.
- Added Certified Qualys Integration.
- Added Service Now help desk system integration - event sinks and ticket verification.
- Added Support for customized SAP database - database information not at default/expected location.
- Added Cisco node to handle VTY and alternative login credentials (FR 465).
- Added password check-out to a group (FR 354).
- Added support for SQL native client - adds support for OLEDB and high availability database mirroring (FR 441).
- Added ObserveIT integration point within password retrieval website.
- Added additional heartbeat monitoring to handle more RPC timeout cases for unhealthy systems.
- Added auto-Index support for MS SQL 2012.
- Added log archiving.
- Added own default password checkout limits to each platform.
- Updated TN3270 node types to use Linux logic; old answer files and process will not work.
- Updated cached database connection handling to account for intermittent database unavailability.
- Updated Oracle password change so it no longer automatically attempts an account unlock; option is selected on password settings tab at job creation.
- Updated Audit logs so they are exported as a zip file rather than a potentially large CSV file.
- Updated Cisco node and response files to reflect new password change options.
- Updated handling of propagation subsystem code to better handle memory leaks found in O/S stack.
- Updated Oracle connection code for better scaling.
- Updated Oracle connection pool handling.
- Updated Oracle DB algorithms to improve performance when using an Oracle backend.
- Updated Dashboards to use .NET framework 4 (do not use .NET 3.5 SP1).
- Updated license checks algorithm to improve program start time.
- Updated the handling of string replacement propagation when field became too large.
- Resolved an issue with TN3270 broken.
- Resolved an issue with SAP broken.
- Resolved an issue where Account Elevation jobs could immediately de-elevate when multiple deferred processors were active (Case 629).
- Resolved an issue with Sybase ASE not using a custom defined (non-default) port (Case 628).

- Resolved an issue with Auto-SSH functionality not working when passwords contained custom characters (Case 609).
- Resolved an issue with Microsoft System Center Service Manager integration not working for SCSM 2010.
- Resolved an issue with HP Service Manager integration not working.
- Resolved an issue with File Store accessibility via SDK not working as expected.
- Resolved an issue with IPMI scan not properly associating credentials used during an IPMI scan when devices were found.
- Resolved an issue with IPMI not committing IP address changes when IP was changed on an existing device.
- Resolved an issue with system memory leak which led to system instability.
- Resolved an issue with system handle leak which led to system instability.
- Resolved an issue with sorting the job queue which could cause asserts.
- Resolved an issue with function block error when checking in a non-Windows password and "Check if password in use option" enabled.
- Resolved an issue with function block error when checking in a non-Windows password and "Log to application log if password in use option" enabled
- Resolved an issue with Heartbeat monitor not killing outstanding threads when enabled to do so.
- Resolved an issue with missing SharePoint 2010 icons causing asserts in program log.
- Resolved an issue with missing SharePoint 2010 icons orphaned elements under the "All discovered uses node" of an account.
- Resolved an issue with account elevation comment causing URL string to become too long and cause an operation to fail.
- Resolved an issue with Generate Stats Fullscan not running against all DB tables.
- Resolved an issue with user supplied names for custom propagations not persisting when propagation was created.

Version 4.83.7 (October 4, 2013)

- Added support for SQL Native Client (SQLNCLI) using ODBC. Allows use of SQL Mirroring in HA mode.
- Added Phone Factor two factor authentication via local agent
- Added Phone Factor two factor authentication via cloud service
- Added SafeNet two factor authentication
- Added generic RADIUS support for two factor authentication
- Added support for SafeNet hardware security module (HSM)
- Added additional compliance reports to the web interface, now in parity with the console.
- Added additional compliance reports to the console, now in parity with the web interface.
- Added new explicit option to define which attribute should be pulled from Active Directory when querying for systems (FR-261).
- Added new default page option for new users logging into the website. This is configured through the web application settings.
- Added option for the secure file store to pre-define what permissions to define for a file when uploaded (FR-508).
- Added option to hide password is the password recovery page until shown (FR-476).
- Added new response file for Palo Alto devices.
- Added new response file for Tandem systems.
- Added new response file for Fortigate systems.
- Added new response file for CiscoPriv15 login accounts.
- Updated behavior of auto-RDP sessions via the website, with the target system going full screen to the entire desktop resolution when the full screen option is selected.
- Updated website behavior to deselect the integrated authentication automatically if a different user account name is provided in the username field, when logging into the website and integrated authentication is enabled

- Updated behavior when configuring the web application global delegation rules, so that the permissions will be auto-applied when the highlighted identity loses focus or the user clicks OK.
- Updated management set to automatically ignore NULL values when using a DB query to discover systems.
- Updated default response file to use all types of encryption (BlowFish still not supported).
- Updated default response file with new settings for changing non-enable accounts.
- Updated various UI elements for date/time reporting.
- Updated RSA enVision Package to include the 6000 series event sink IDs.
- Resolved an issue with memory leak in data access layer that could cause the deferred processing service to stop or produce “out of resources” messages.
- Resolved an issue with memory leak in data access layer that could cause the website COM object to stop or produce “out of resources” messages.
- Resolved an issue with memory leak in data access layer that could cause the management console to produce “out of resources” messages.
- Resolved an issue with per account delegations not working for anything other than Windows or Linux systems (B-640).
- Resolved an issue where the website would generate function block errors if ‘Block password check-in if password is in use’ was selected and user checked in a Linux system.
- Resolved an issue where the website would generate ‘500’ errors if ‘Block password check-in if password is in use’ was selected and ‘Log all password check-outs to system’s event log’ were selected and user checked in a Windows system (B-651).
- Resolved an issue with SCSM ticket integration not always properly verifying ticket status.
- Resolved an issue with HPSM ticket integration not always properly verifying ticket status.
- Resolved an issue with BMC ticket integration not always properly verifying ticket status.
- Resolved an issue with ServiceNow ticket integration not always properly verifying ticket status.
- Resolved an issue with website deployment bug that could cause the website deployment to fail when the .net framework was not properly registered on the target web server.
- Resolved an issue with website verification that could fail when website was installed to a virtual directory that was not the default name.
- Resolved an issue with various typos in the website.
- Resolved an issue with various typos in the management console.
- Resolved an issue with improper username case comparison - If user logged in as userX and checked out password, then checked logged back in as Userx, he could not re-view the same password.
- Resolved an issue with audit Logs exported with a .asp extension instead of .zip.
- Resolved an issue with scheduled refresh job comments not persisting in the jobs queue dialog.
- Resolved an issue with Checkout to Group disallowing checkout extension for subsequent users.
- Resolved an issue with the possibility for account lockout when a connection uses a cached credential for Windows authentication (different than alt-admins or integrated authentication).
- Resolved an issue with Checkout to Group disallowing checkout extension for subsequent users.
- Resolved an issue with SDK Login Procedure Fails When Using Integrated Authentication. See article:
- http://forum.liebsoft.com/enterprise-random-password-manager-knowledgebase/650-sdk-login-procedure-fails-when-using-integrated-authentication.html.
- Resolved an issue with password compartments that cannot be edited from the dialog.
- Resolved an issue where, for compartmentalized passwords, the Show/Check in Password option for a password that is already checked out always re-prompts the user to reenter their password recovery reason.
- Resolved an issue when using compartmentalization with check out to group, after the user recovers their segment of the compartmentalized password and checks it out to a group, no user can use the Extend Checkout or Check In buttons.
- Resolved an issue with account elevation - automatic de-elevation occurs immediately when multiple zone processors are present.
- Resolved an issue with a Bug causing disabled jobs the possibility of getting re-enabled.

- Resolved an issue with errors and asserts listed when ERM configured with a bad AD / LDAP path.
- Resolved an issue with manual installation of web service having incorrect web service DLL.
- Resolved an issue with Web.config files for web service having incorrect parameter when using SSL.
- Resolved an issue with numerous PowerShell CMDlets not working.
- Resolved an issue with numerous web service calls not returning data as expected.
- Resolved an issue with web service calls to add various databases not properly applying encryption to the password.
- Resolved an issue with ERPM task discovery failing when target task was set to run as SYSTEM (B-658).
- Resolved an issue with incorrect permissions applied when using per account permissions for multiple accounts on the same system (B-660).
- Resolved an issue with IPMI node not displaying more than 100 devices (B-657).
- Resolved an issue with built-in administrator password change job not renaming the administrator account - when elected to do so – until after the password was changed, resulting in bad information in the website (B-654).
- Resolved an issue with discovery of SQL Server instances overwriting system information, which resulted in alt-admin information being incorrect (B-653).
- Resolved an issue where if retry policy is set to 'STOP', jobs that fail will never retry (expected) and never get rescheduled for next run time (unexpected) (B-650).
- Resolved an issue with shared credentials list not sending email notification on password recovery (B-649).
- Resolved an issue with last login column in Windows Accounts view not being sorted out in chronological order (B-647).
- Resolved an issue with app crash that could occur when using alternate administrators to manage an untrusting domain (B-642).
- Resolved an issue with console delegation that could allow users to bypass delegation rules (B-641).
- Resolved an issue with IIS reset happening when managing SharePoint even if no account usage was found (B-639).
- Resolved an issue with the personal password store not allowing empty entries to be added to the list (B-638).
- Resolved an issue with RADIUS authentication not working all the time (B-636, B-637).
- Resolved an issue with system rename producing asserts (B-635).

Version 4.83.8 (July 31, 2014)

- Added application launcher to launch any application on a local system.
- Added application launcher to launch any application on a bastion host / jump server.
- Added application security for launched applications (hash, digital signing, etc.).
- Added application launcher automatic application push.
- Added session recording for applications via bastion host / jump server.
- Added SSH Key support for Linux/UNIX password management.
- Added SSH Key support for Linux/UNIX application launch.
- Added SSH proxy capability for launched applications to Linux/UNIX hosts.
- Added support for RDP 6.x+ fat client (support for NLA and app launching).
- Added tools to build and develop web login connectors.
- Added tools to build and develop fat client login connectors.
- Added CLR connector capability for web only based management.
- Added dynamic list creation for custom account stores; website system type filters.
- Added support for SHA2 SSH algorithms.
- Added console delegation for most functions in the administrative console (FR-345).
- Added database tuning options for SQL 2014.
- Added user controllable (persistent) settings for SSH console access when using MindTerm SSH component.
- Added Website will recall last system type filter when logging in or navigating back to previously viewed pages.

- Added password change job constraint option to not allow repeated characters (FR-422).
- Added comment for auto-RDP and auto-SSH launch (FR-457).
- Added more mapping options for remotely connected systems (RDP, SSH) (FR-503).
- Added ability to rename shared credential lists (FR-517).
- Added Exposed Account masks management in web service (FR-522).
- Added pre-run notifications for scheduled jobs (FR-523).
- Added file size limiting for File Vault in website configuration (FR-529).
- Updated the verbiage in website delegations to match that of the selected permissions (FR-586).
- Updated the arbitrary elevation in PowerShell to use its own settings rather than global settings (FR-553).
- Removed the automatic refresh of dialog for many dialogs which did not require it (FR-559).
- Updated the Web Activity and account activity to use a consistent time zone for activity time stamps as displayed in the website.
- Updated the restricted systems list so it is no longer case sensitive.
- Upgraded to IPWorks v9
- Removed the tempura.org from WCF service (FR-530).
- Resolved an issue with Directory Services Restore Mode (DSRM) causing asserts during password change
- Resolved an issue with DSRM password change not working.
- Resolved an issue with account rename during password change on 2008 and newer generating errors.
- Resolved an issue with ServiceNow! Ticket integration not working.
- Resolved an issue where WebSphere password changes could hang indefinitely if login password was out of synch.
- Resolved an issue where Web Logic password changes could hang indefinitely if login password was out of synch.
- Resolved an issue where SAP password changes could hang indefinitely if login password was out of synch.
- Resolved an issue with MySQL accounts not appearing in the website.
- Resolved an issue where if the website option to "Display available options" was not enabled, low powered login accounts would receive the extra permission to view password history.
- Resolved an issue where if the website option to "Display available options" was not enabled, low powered login accounts would receive the extra permission to view account activity.
- Resolved an issue where the global "Recover Password" permission combined with per account delegations to
- "Recover Password" would grant the low powered user access to "Change" and "Remove" password options (B-673).
- Resolved an issue where the global "Recover Password" permission combined with per management set delegations to "Recover Password" would grant the low powered user access to "Change" and "Remove" password options (B-687).
- Resolved an issue where opening the self-recovery permissions dialog and attempting to close the identity selection dialog without selecting an identity would cause an application crash (B-674).
- Resolved an issue where attempting a Cisco password change job using Telnet (rather than SSH) could cause ERPM to crash (B-676).
- Resolved an issue with password extension for non-Windows accounts extending beyond platform specific extension settings (B-677).
- Resolved an issue with ERPM console incorrectly displaying job type affinity for zone processors (B-678).
- Resolved an issue with various typos and formatting problems.
- Resolved an issue with component errors when both a system name and NetBIOS name filter are filled out on the systems page (B-684).
- Resolved an issue where a job set to run every N days did not retain set schedule following an interactive run (B-689).
- Resolved an issue with permission restriction by schedule not working as expected (B-690).
- Resolved an issue where low powered users without proper permission could create a shared credential list (B-692).
- Resolved an issue where jobs set to run after the 28th day of the month would repeatedly run in February (B-693).
- Resolved an issue with management of MS SQL databases using SQL Authentication, where the login account included a semi-colon in the password could cause password change job operations to fail (B-695).

- Resolved an issue where bad Active Directory paths on management set properties would stop subsequent enumeration of Active Directory paths for the same management set (B-703).
- Resolved an issue with custom account store jobs breaking if the login account information is changed for a job (B-706).
- Resolved an issue where deleting self-recovery rules caused asserts.
- Resolved an issue where exporting of encryption key via Windows REG function did not maintain proper formatting.
- Resolved an issue where the option to use a custom schema was not remembered when using the SQL Native client (B-711).
- Resolved an issue with SQL Server database instances not displaying properly when using the system name filter (B-714).
- Resolved an issue where Windows service propagation could fail if service dependency buffer size grew too large (B-716).
- Resolved an issue where SQL Reporting Services discovery would fail when more than one instance of SSRS was present on a target systems (B-717).
- Resolved an issue where SQL Reporting Services management would fail when more than one instance of SSRS was present on target systems (B-717).
- Resolved an issue with password checkout duration would use Windows platform extension setting rather than platform specific settings (B-719).
- Resolved an issue where using console launch impersonation when UAC was enabled could cause application crash (B-720).

Version 4.83.8 SR1 (October 1, 2014)

- Added licensing support for integration and migration of RPM systems to ERPM systems.
- Added CA Service Desk Integration.
- Added ticket status verification for JIRA.
- Added ticket status verification for OTRS.
- Added SSH key support for password changes.
- Added custom port support for MySQL databases.
- Resolved an issue with shared credential list grid padding when viewed in IE with compatibility mode enabled.
- Resolved an issue with support for Cyrillic characters in password lists.
- Resolved an issue with support for umlaut characters in password lists.
- Resolved an issue with Date Picker date selection for dashboards on international date/time formats.
- Resolved an issue where application launcher would not work when login names included Cyrillic characters.
- Resolved an issue PowerShell Cmdlet Get-LSWebAuditLogs not returning data data (B-733).
- Resolved an issue with SSH key for one to many system mapping for application launching (B-732).
- Resolved an issue where Web delegation changes via website would fail when user came from alternate domain (B-731).
- Resolved an issue Oracle text file import did not importing username and password when a custom connection string was used (B-730).
- Resolved an issue where, after performing a password check-in via the website, the filters would set the system type to TN3270 (B-729).
- Resolved an issue with Heartbeat monitor dialog not reading correct values regarding its settings and would therefore write back wrong settings if dialog was OKd (B-725).
- Resolved an issue with account elevation time discrepancy (B-702).
- Resolved an issue where the Ignore password checkout permission did not apply when recovering shared credentials (B-701).

- Resolved an issue with ERPM not loading the stored credential to continue managing the device once an IPMI connection account was managed (B-699).
- Resolved an issue with self-recovery permissions not being properly imported (B-686)
- Resolved an issue with users granted self-recovery permissions not being able to page through multiple pages of accounts for recovery (B-686).
- Resolved an issue where installing ERM website to an IIS host already hosting multiple existing root level websites could cause application pool corruption.
- Resolved an issue with special 2012 and 2012 R2 tasks that did not fully qualify the name (always using domain accounts) being improperly attributed in the account store view.

Version 4.83.8 SR2 (October 1, 2014)

- V1 Feature: A<>B Service Account Pooling. Contact your account manager for more information.
- V1 Feature: Enumeration of groups on target system. Contact your account manager for more information.
- V1 Feature: SSH Key discovery and association. Contact your account manager for more information.
- Added sSupport for Shadow Accounts when launching applications.
- Added ability to launch application as connecting RDP user (windows local or domain accounts only).
- Added SSH tunneling with username and password.
- Added SSH tunneling with public key authentication.
- Added interstitial dialog for editing jobs to prompt if the job will run now when closing the dialog.
- Added ObserveIT integration point for application launcher host to improve metadata collection.
- Added performance and timing metrics collection.
- Updated application launcher so it no longer needs recover password permission to function.
- Updated the heuristics checking for DB queries which was disabled by default, resolving compatibility problems with Oracle.
- Resolved an issue with compliance report "All Job Activity" able to cause ERPM to crash when using an Oracle database (B-715).
- Resolved an issue web service installer not configuring IIS SSL setting (B-726).
- Resolved an issue with zone processors not running scheduled jobs despite assigned affinity (B-746).
- Resolved an issue with zone processor job affinity reported incorrectly (B-747).
- Resolved an issue with job queue "check status" causing ERPM to crash (B-748).
- Resolved an issue with job queue "show query" causing ERPM to crash (B-749).
- Resolved an issue where ERPM deferred processing service may not start.
- Resolved an issue with password checkout status not properly determined when display options are not enabled (B-757).
- Resolved an issue with re-randomization jobs against Linux targets not re-using certificates properly.
- Resolved an issue where toggling SSH keys for use on ALL SYSTEMS after being mapped to a single system (when the single system had already been managed) could cause job to log errors.
- Resolved an issue where users without permissions could see (though not recover) all shared credentials when setting list filter to 'All Lists'.

Version 4.83.9 (March 10, 2015)

- Added logging messages to indicate enabled option override settings.
- Added SSH key change/rotation (same concept as password rotation but for SSH keys).
- Added support for update in place for key usage on target during SSH key update job.

- Added ability for Linux password change job to attempt to populate SSH keys associated with Linux targets with password change jobs against the targeted systems.
- Added warning if the user removes an SSH key that is used as part of password change jobs.
- Added SSH key refresh to account refresh on Linux.
- Added SSH key details page to Linux system details sheet.
- Added SSH daemon refresh to account refresh on Linux.
- Added SSH daemon configuration details to Linux system details sheet.
- Added SSH daemon configuration dialog to show filtered list view of SSHd config for selected machines.
- Added SSH key display to indicate if the private key data for an SSH key was stored but not associated with a known user key.
- Added ability for ERPM to automatically save the private key data for discovered keys to the key store if the private key data can be parsed.
- Added ability to define and edit key labels once specified.
- Added ability to re-label existing key from the user key to account store mapping dialog.
- Added ability for ERPM to save the private key data for user keys on discovery if the private key data is known, the label is the key signature by default.
- Added SSH key details dialog to the SSH key view context menu.
- Added SSH key export option to the managed key mapping dialog to export both the public and private parts of stored keys.
- Added option to delete SSH key files from systems where the keys are found during SSH key update.
- Added ability to set a standard SSHD config that all discovered configs should be compared against.
- Added differential analysis to the SSHD configuration display to show differences between discovered configs and the standard config.
- Added code to save the certificate info after windows system refresh.
- Added a certificate display property page to the Windows system details.
- Added option to allow ICMP ping test to a target before any Linux operation is performed.
- Added Edit button for web application instances in the web app settings dialog.
- Added an option to the web application configuration dialog to allow updating the default settings to match an existing installation's settings.
- Added removal option to web application configurations in the web app instance dialog.
- Added account cache option for web application to maintain a server side cache of all accounts visible for each current user session.
- Added username parsing for domain\user and UPN name formats to the login page logic (FR-648).
- Added option to the web application configuration to hide the list of available authenticators.
- Added a filter option to the launch application page to support filtering application lists.
- Added a details view option to the remote application launch page.
- Added an icon view option to the remote application launch page.
- Added ability for shared credential list to display the password list name while selecting all lists.
- Added list specific options for permissions to the shared credential list when viewing all password lists.
- Added paging controls for password history in the web interface for managed passwords and shared credential lists.
- Added paging controls for password activity in the web interface for managed passwords and shared credential lists.
- Added direct password request grant links to the email notifications sent by the web application (FR-197).
- Added direct password request deny links to the email notifications sent by the web application (FR-197).
- Added web application configuration pages to support direct password request approval and deny links.
- Added an option to the compliance report to automatically generate all basic reports after capturing a new snapshot.
- Added code to the web interface to force the file extension of user uploaded files to match the file extension of the uploaded file (FR-673).

- Added an option to the compliance report generation settings to automatically copy the basic generated reports to the web application reports paths.
- Added an option to delete compliance report data snapshots to the compliance report dialog.
- Added a feature to the web application for compliance reporting to download pre-generating compliance reports if they are found on the server instead of generating them.
- Added automatic installation and registration of the RSA support library as part of the web application install.
- Added page load effects to the web interface to indicate when the web application is processing user requests (to avoid double submits).
- Added dynamic page panel fade effects to the web interface at page load times.
- Added application metrics (FR-551).
- Added web service supports app metrics.
- Added web service parameter validation.
- Added support for create/delete/list role based permissions to the web service.
- Added PowerShell cmdlets to support add/remove/list role based permissions.
- Added support for web service job limits based on total jobs and based on user created jobs (FR-625, FR-626).
- Added support for PostgresSQL management through the web service.
- Added PowerShell commandlets to manage PostgreSQL instances and stored passwords.
- Added an update option to the web app config dialog to allow updating the files for existing web instances without overwriting the settings.
- Added an automatic restart of the website COM+ application for a web instance when changes are made to the instance's configuration that could require a restart.
- Added password last set time to the shared credential class returned by web service calls.
- Added password last set time to the stored credential class returned by web service calls.
- Added a version commandlet to the PowerShell commandlet code.
- Added web service and PowerShell commandlet for displaying the list of checked out accounts to support all account types instead of just windows and Linux.
- Added GetVersion call to the web service support library and returned it as part of the web service call.
- Added PeopleSoft integration library for account store.
- Added Discovery of PeopleSoft user accounts and user attributes
- Added PeopleSoft password management.
- Added support for management of PostgreSQL accounts.
- Added support for discovery of PostgreSQL accounts.
- Added support for discovery of PostgreSQL server attributes.
- Added, for launched applications, shadow account mapping support for non-windows account types (ignores login and create process as for non-windows accounts).
- Added, for launched applications, $(ProcessID) to the list of replacement arguments available to the multi-tab command line.
- Added, for launched applications, Lieberman-specific custom path to the list of paths checked for the existence of the OIT agent when loading the agent to update the login user for remote sessions.
- Added, for launched applications, the run as account and run as password to the set of information available for multi-tab jobs.
- Added, for launched applications, ability to load user profile and use working directory options to the remote application configuration.
- Added, for launched applications, a time out update mechanism so that remote app sessions that crash or are abandoned will no longer cause tab jobs to target their abandoned sessions.
- Added, for launched applications, an output hook for processes called by the launcher to return data to persist in the application session record.
- Added, for launched applications, a replacement variable to the list of arguments for multi-tab command line operations called $(ProcessOutput) which is the result of the launched process.

- Added, for launched applications, a load user profile flag and working directory string to the multi-tab automation instructions for launching tabbed operations.
- Added, for launched applications, code to the remote app config dialog to ensure that default file paths and working directories always include a trailing backslash.
- Added, for launched applications, the span monitors option to the configuration for all terminal service configs launched through the web interface.
- Added logging to the application launcher to indicate the status of the run as user, the state of load profile and working directory and whether run as credentials were used.
- Added, for launched applications, the option to sign RDP files used for remote app to the remote application launcher.
- Added support for application session and multi-tab operations for RDP, script and web launch types.
- Added $(SessionID) and $(AppSessionID) arguments to the multi-tab launch command line replacement list of arguments.
- Added support for multi-tab automation operations to applications that launched with fixed credentials.
- Added support for multi-tab automation for script launch type remote applications.
- Added support for creating application groups and assigning configured remote applications to the application sets.
- Added the ability to automatically update references in remote application sets if the label of a remote application is edited.
- Added remote app set filter option to the application launch page.
- Added permission sets for remote application sets.
- Added custom connection fields for RDP remote app configuration.
- Added custom connection replacement arguments for RDP remote app configuration.
- Added a reset button to the custom RDP settings configuration dialog to remove any custom RDP settings used for a remote app launch.
- Added a flag to the remote app configuration settings dialog to prevent the application from using any configured run as settings.
- Added white-list capability for icons output with remote app configurations to the security tab of the web application configuration dialog.
- Added Delete file to the SSH library helper module for SFTP.
- Added a check to ensure that if the background and foreground color of the mindterm console are set to the same value, the settings revert to white on black.
- Added logging feedback to object queries performed through LDAP.
- Added cleanup code for abandoned role based mapping for authentication servers that have been deleted (FR-281).
- Added database pruning processes (FR-556, FR-456)
- Added a database cleanup maintenance step to the database maintenance dialog to cleanup references to role based permission mappings where the auth server or identity is deleted.
- Added a program icon to property sheet and pages for custom propagation types for file search and replace.
- Added a local file browse to the text file search and replace custom propagation settings configuration dialog.
- Added code to update authentication servers referenced in role based permissions when authentication server names are edited.
- Added support for importing single accounts for custom account store types.
- Added code to detect and log if the certificate specified to sign RDP files could not be found in the user's certificate store, or if the load of the certificate fails.
- Added code to the web application settings lookup to match all domain suffixes for web application installation systems.
- Added additional filter settings to the job configuration dialog.
- Added menu options to the deferred job configuration dialog to control select (all/none/invert).
- Added a batch delete operation to the deferred job dialog if all visible jobs are selected.

- Added support for SSO to the remote application jump server configuration.
- Added a handler to reset the JobID range filter in the job display if the value is set to 0 to set the value back to the defaults (1 and INT_MAX).
- Added a handler to reset the job dialog system filter to all if the filter was manually erased by the user.
- Added a pre-populated filter of available namespaces to the stored passwords dialog to ease the use of looking for non-Windows passwords.
- Added item counts and namespace filter to the password history dialog.
- Added password history configuration to control the saving of the last n historical passwords and/or saving historical passwords for n days (FR-260).
- Added a log message to indicate when a unique session string reuse is causing a forced logout if unique session string and force logout on error are both enabled.
- Added password restrictions for repeated characters (FR-558).
- Added database maintenance code to remove all old file data references for file store files that have been removed.
- Added clean up processes for the file data binary in the database when files in the file store are removed.
- Added log information for the logged on username and system name when encryption/decryption takes place in the console (FR-646).
- Added support for changing PIN for RSA SecurID to the console.
- Added %%JobID%% to the list of arguments that get replaced for a pre-run job alert.
- Added deny character filter for special characters when configuring password change jobs (FR-636).
- Added console delegation for the Jobs dialog button in the console.
- Added console delegation to View Management Sets in the console.
- Updated the cleanup code for job data to leave job data if it is referenced by stored random passwords for future spin jobs.
- Updated the App supplied credential call back method to put accounts with the name root or administrator at the beginning of the list of credentials to try.
- Updated the passcode field in the 2FA dialog in the console to a password type field.
- Updated the shadow account password selection dialog to only show windows accounts.
- Updated the Safenet token code field to a password field in the web interface.
- Updated the multi-tab launch code to run new tabs using the run as account information if it is provided.
- Updated the multi-tab creation logic so that a new tab will be launched if a different run as (shadow account) is used to launch another instance of the target application.
- Updated the code to create multi-tab instructions will now ignore shadow accounts that are not Windows accounts for run as.
- Updated the Run-as in the launcher to use the ProcessInfo method instead of the P-invoke method so that output redirection is possible using managed code objects.
- Updated the run as logic for multi-tab launches so it may use any existing session if the multi-tab run as account is not a windows account.
- Updated the remote app multi-tab creation logic so it can use any existing application session regardless of run as settings when the new launch does not target a Windows account (integrated authentication).
- Updated the Cert signature for signing generated RDP files to a global setting so that types of launches that are no applications can be signed as well (i.e. RDP sessions).
- Standardized the view creation statements to use table-derived names for columns (Better support for Oracle DB backend data store).
- Updated the remote application dialog to only allow configuring multi-tab options for applications running on remote jump servers.
- Updated the code when importing passwords from the web application to ignore illegal system names for non-system object cases (DBs, custom, etc.).
- Updated timeout values for rdpsign.exe to try to address failure in some cases.
- Updated the order of columns in the details view for launch app.

- Updated the file check behavior to log and continue if rdpsign could not be found using File.Exists to ignore some false positives with the check.
- Updated the title of automatically generated .rdp files and their title windows to systemTarget_GUID instead of LiebsoftLauncher_GUID.
- Updated the location of all web application configuration settings to the database, instead of the local web server's registry.
- Updated the pre-run job alert settings so they are now copied when a job is cloned.
- Updated the web application pages to support compatibility with IE 11.
- Verified that the latest versions of Java no longer overwrite session cookie data (B-723).
- Updated the text in the registration dialog to indicate that clicking exit will close the application (B-797).
- Updated the code to support change/edit password permissions on account level based on group memberships in addition to global level.
- Updated a few logging instances that would record the simple login name instead of the fully qualified login name for the user performing the operation in the console.
- Updated the password activity report to only return web activity for the account, removing password change activities, this was required to implement paging.
- Updated the shared credential list page to show the permissions and add options even if the shared credential list is empty.
- Updated the password history attempt recording logic to delete password change attempts if the password is saved to the password store.
- Updated the permission cleanup code to remove permissions on accounts where the password is no longer stored.
- Updated the default settings for OATH token config to use GUIDs instead of blank IDs to support auto-generation for users with default settings enabled.
- Updated the default port settings for SIEM event sink to 514.
- Updated the help dialog for delegation permission import to indicate the decimal encodings for each permission bit.
- Updated the option to store password history from the stored passwords dialog to the password history settings dialog.
- Updated the RDP configuration to be available regardless of whether or not the application is configured to run on a remote jump server.
- Updated the display code to always show load user profile options.
- Updated the log message associated with password encryption to include a timestamp.
- Updated chart pages to use posts instead of gets to prevent the auth token from being passed as a query string argument.
- Updated the code in the job display to use the application configured job paths when opening text log files associated with the deferred processor or jobs.
- Updated the scheduling page code to allow jobs that are scheduled per N days to specify hour and minute of day to run (FR-662).
- Updated the dimensions of several dialogs (Job details/delegate console access/delegation permissions/Stored Jobs) to fit on 1024x768 resolution.
- Resized and fixed tab order on password change settings property page.
- Updated the compliance reporting page to show all available reports instead of a drop list of reports.
- Updated the console to use support code for RSA that calls the COM object - Console code still does not implement set PIN or on demand token code.
- Updated the Cisco password change job property page to include a single option to load all stored passwords, when running the job in a similar manner to Linux change jobs.
- Updated the Cisco password change job property page to default to SSH instead of telnet as the connection type.
- Updated the default behavior of a windows password change job created through PowerShell to default to w2k password complexity.

- Updated the behavior of the check-in operation in the web application to take you back to the accounts page without setting the filter type to the type of account that was checked in.
- Updated the alignment of several input fields on the compliance report page in the web application.
- Updated the compliance database key migration code to move the key under the datastoreconfig key, aligning it with the new paradigm for storing data store config settings.
- Updated the localization files in the web interface.
- Updated the Twitter App Launcher Profile to map to new Twitter login page.
- Updated, RSA re-factored to support dynamic loading of RSA components to minimize the amount of admin configuration.
- Updated RSA integration to only support v7 and v8 of RSA client.
- Updated the RSA component integration location to a COM+ application to simplify integration and deployment of website when RSA is used.
- Updated the ERPM demo license to enable ALL possible features.
- Resolved an issue where multiple ERPM consoles tied to the same database would cause secondary consoles to not load correct licensing data resulting in a console demo mode timeout scenario (FR-183).
- Resolved an issue where app metrics database failure could critically disable ERPM.
- Resolved an issue where app metrics database failure would cause website and zone processor logs to be spammed with messages of inaccessible database.
- Resolved an issue where ERPM would hang when deleting multiple keys from the user key to system mapping dialog if multiple entries had the same key label.
- Resolved an issue where system states for jobs, once set to special case "interrupted" would retain that state even after subsequent successes or failures.
- Resolved an issue where the path to the application would be displayed incorrectly in the error message dialog if console delegation run as fails.
- Resolved an issue where ERPM would log an incorrect error message when failing to authenticate using Phonefactor's agent, the new message indicates the operation failed, not that the library failed to load.
- Resolved an issue where data integrity database table creation would fail if the tamper key was not found.
- Resolved an issue where permission checks for external account would not be returned correctly in the web interface.
- Resolved an issue where remote apps could appear incorrectly when shadow accounts or per account permissions were used.
- Resolved an issue with multi-tab command line arguments not being replaced correctly.
- Resolved an issue where deleting a shadow account mapping would delete all delegated application permissions that used shadow accounts.
- Resolved an issue where remote applications were being shown in the web interface if any user had the ability to launch the application on the targeted account, not just the logged in user.
- Resolved an issue with multi-tab application launch logic that caused tabbed execution steps to fail if run-as accounts or shadow accounts were specified.
- Resolved an issue with Cisco web application page for launching remote apps with shadow accounts where the system name attribute was incorrectly store identifier.
- Resolved an issue with Run as user module not loading profile and working directory correctly.
- Resolved an issue where, assigning application permissions with no group restrictions to applications for a user that already had permissions on that application would fail.
- Resolved an issue various typos in the web and UI interfaces.
- Resolved an issue where, in IPMI systems, the database view creation would fail against databases that were operating in case-sensitive modes.
- Resolved an issue where shadow accounts for systems based launched would not be shown by default because of a change made to support remote app filters.
- Resolved an issue with session expiration not triggering all the logout logic correctly.
- Resolved an issue with remote app signing causing the file signing to fail (transposed arguments).

- Resolved an issue where user search settings in the web interface would not be cached correctly for DRAC, IPMI, or custom account store types.
- Resolved an issue where application sets could not be deleted from the application set dialog (failure to delete after confirmation).
- Resolved an issue where default web application configuration settings were not populated correctly when the configuration dialog opened.
- Resolved an issue where interpretation of private key data would fail if a passphrase was used to protect the key data.
- Resolved an issue where web-service created account elevation jobs would use incorrect de-elevation settings, which could cause the alert emails to fail.
- Resolved an issue with system path redirection that caused RDP signing to fail on 64 bit systems in release versions of the launcher.
- Resolved an issue with the creation of pre-run alert settings for each job that is created if multiple accounts are targeted when creating password change jobs (FR-645).
- Resolved an issue with the configuration of the compliance reporting database once it has been previously configured (B-760).
- Resolved an issue with the compliance database configuration not pushed to new website instances or when updating existing websites (B-761).
- Resolved an issue where RDP password lookup could fail if the namespace didn't match the account name.
- Resolved an issue with web service request for removal of permissions on accounts that were non-windows accounts to fail.
- Resolved an issue with website not displaying the edit/delete options when delay loading permissions for accounts in the web interface.
- Resolved an issue with website not properly adding the target system from to the terminal services configuration file for terminal service remote app.
- Resolved an issue so custom resolution of a custom RDP session is not to be used.
- Resolved an issue with an erroneous check that would report an error when using SSO with remote application launch on the jump server.
- Resolved an issue where changing passwords for MySQL accounts would fail if custom ports were used.
- Resolved an issue where MySQL refresh operations would fail if using stored passwords for connection credentials.
- Resolved an issue where editing a MySQL server registration would cause the account store type to change to Sybase.
- Resolved an issue where subsequent Cisco password change jobs targeting enable would fail after the first successful run (B-788).
- Resolved an issue where Cisco password change jobs would fail without a target account name explicitly defined (B-786).
- Resolved an issue with the removal of permissions on accounts using the web service/PowerShell components.
- Resolved an issue where a deferred processor would record job update queue information for all jobs run even though the job update queue is no longer used.
- Resolved an issue where password length settings would be set to 1 every time the spin control was clicked.
- Resolved an issue where the web application could prompt for ticket number on password segment view even if the segment was checked out to the user.
- Resolved an issue where the tbl_certificatesfoundonsystem table was not being auto-created as part of the data store check.
- Resolved an issue where editing a shared credential list entry could fail if the password had been added with a very old version of the web interface.
- Resolved an issue where it was not possible to add a shared credential if the shared credential was entered with the wrong case for the list name.
- Resolved an issue where the web interface could display account information for non-all-access users without proper delegations.

- Resolved an issue where attempting to change a root password while logging in as root would cause ERPM to crash.
- Resolved an issue where the zip file output of web audit logs did not show the correct operation description for remote app launch link generation events.
- Resolved an issue where password re-encryption could fail after a successful decryption due to a lingering key stored with file vault encryption settings.
- Resolved an issue where users that owned files in the file store could gain all access to all files in the file store (B-828).
- Resolved an issue where permission check code could allow remote application access if the system was in a managed group the user could access.
- Resolved an issue with a character encoding bug in the delay load permission call to get the available operations for password entries in the web application.
- Resolved an issue where the launch app could show up in the web interface when delay loading permissions for an account, even if there were no remote apps available for launch.
- Resolved an issue where the file upload procedure would not correctly display error messages if files failed to upload based on access permission checks if no other files are visible to the user.
- Resolved an issue where the session recorders would always post-pend an extra file extension to recordings that had the correct extension, and not add it, if it was missing.
- Resolved an issue where the Console would not show refresh jobs in the jobs dialog if the refresh filter was selected.
- Resolved an issue where IPMI account rows would not to show up in the web interface for all access users if no account type was specified but a group filter was set.
- Resolved an issue with the personal password store, where an escaped password was not being added to the response and the copied value was always empty.
- Resolved an issue where forcing password list check-ins was failing because it was calling the wrong function on the back-end.
- Resolved an issue where the web application would display an error page if a user attempted to check-in a password that was not checked to them.
- Resolved an issue with the delegation checking for deleting jobs to check the delete job permission, instead of the edit job.
- Resolved an issue with the session recording not working properly when PSR options was selected.
- Resolved an issue with the session recording not working properly when VLC recorder was selected.
- Resolved an issue where custom propagations could leave behind stale task information (B-830).
- Resolved an issue with the %OldPassword% replacement value not getting populated for arbitrary propagations when managing an LDAP based account (as opposed to Active Directory) (B-831).
- Resolved an issue where disabling and re-enabling a job that had not run would cause the job to run immediately and continuously loop (B-832).
- Resolved an issue where external accounts may not display recovery password options (B-758).
- Resolved an issue where password recovery could fail with a function block error when a password was randomized and set for re-randomization, and the customer was using an Oracle DB as the back end data store (B-762).
- Resolved an issue where the use of per-management set delegations could cause errors in website (B-820).
- Resolved an issue where ERPM could crash after changing system type of a Linux system (B-823).
- Resolved an issue where ERPM would crash if the user tried to edit system delegations and user delegations at the same time (B-833).
- Resolved an issue with hard coded path to job log files when selecting option to view job log files (B-829).
- Resolved an issue where when performing a password change job with propagation and using zone processors, job hand off did not properly occur (B-822).

Version 4.83.9 SR1 (May 9, 2015)

- Added logging and a web service update if the recorder state fails to transition to
- stopped/complete.
- Added redirection to the login page that will redirect to HTTPS if secure cookies are required by the web application settings to prevent failed logins back to the login page.
- Added logging to indicate "no ticket" for web operations that did not log a ticket.
- Added compatibility tag to all page headers to indicate IE optimizations for edge version.
- Added code to the SSH console settings to default to black on white if the background and foreground colors are the same.
- Added page loading effects to the user session pages for RDP and SSH.
- Added the ability to automatically output the seed for a user's oath token to the oath login page.
- Added the ability to automatically generate a QR code for the seed file of an OATH token.
- Added the ability to automatically generate a Google Authenticator QR code for OATH token seeds and show them on OATH login page until successful login.
- Added request/grant work flow to remote applications/SSH/telnet/RDP.
- Added the ability for job creators to be granted full control of jobs.
- Added new delegation to request remote access on groups/systems/accounts dialogs.
- Added new "request access" PowerShell commandlet to create remote access requests.
- Added remote access request specific log messages for remote access requests to differentiate between password requests and access requests.
- Added new warning pop-up for remote application sessions and local application launch sessions.
- Added new event for the event sink system for changing encryption settings (FR-647).
- Added new work flow pages that are SSH specific to indicate that passwords are being accessed, not recovered.
- Added sort and group behaviors to the global delegation dialog.
- Added option to push encryption settings to a remote machine's registry.
- Added time out values to the LDAP authentication server configurations.
- Added sorting to all queries that return delegation managers.
- Added double password change (double tap) as an option to the password change settings configuration dialog.
- Added the ability to schedule a reboot as part of the completion of a job (FR-277).
- Added encryption migration code so that stored SSH keys will be re-encrypted with new encryption settings if the encryption settings are changed.
- Added 2 factor web configuration to use most restrictive settings instead of least restrictive.
- Added per-system delegation checks to launching applications using shadow accounts.
- Added service start and stop time configuration to the program options.
- Moved program options to the database to facilitate having the same settings among all consoles and deferred processors.
- Added comment for shared credentials to the list of fields returned in SharedCredential to the web service/PowerShell when running get-lslistsharedcredentialsforlist.
- Added SSH key discovery code to flag unknown key types.
- Added support for index defragmentation when using SQL native client (FR-575).
- Updated code for file store encryption.
- Updated code for SSH key re-cryption so that failures to decrypt stored keys will not crash the application with unhandled exceptions.
- Moved 2 factor authentication settings to a separate page for web installation.
- Updated the accounts page so it will no longer link back to the top of the page if the options link was expanded.
- Updated permissions for adding and removing systems from groups to require add/edit/delete passwords and management set assignment instead of all access.
- Updated the delegation dialog to save the current user settings before creating a new user.

- Updated the web application for remote app/RDP/SSH so it will not leave the pages open if the launcher is blocked by the browser.
- Moved the options to use the thick terminal services client to the web application settings instead of the application launcher settings.
- Updated the web application to hide SSH for the windows platform type.
- Resized various dialogs.
- Updated the enrolled identities delegation dialog sort order.
- Updated the account mask delegation dialog sort order.
- Updated the account mask delegation dialog to show the display names for identities.
- Updated the account mask delegation dialog to show the correct type name strings for certificates.
- Updated the log message for not attempting Windows RPCs against a non-windows system from trace to normal.
- Updated the key export code to create explicit ASCII files to work with putty.
- Updated the custom account store password change jobs to display the option to "use stored passwords for all accounts" when creating a new job.
- Removed the SSH proxy pass phrase from the set of data being drawn into the SSH user settings page.
- Updated the color html string output code to support 3 digit RGB values (the default format of the color picker).
- Resolved an issue by swapping the rows and columns for the Mindterm client to get the corrected dimensions.
- Resolved an issue with new website installations to use the hard-coded defaults instead of the configured defaults.
- Resolved an issue where the ticket number and target system were not logged correctly when doing an RDP password checkout.
- Resolved an issue where a page error could occur if there are no password lists and the user shows password lists (B-836).
- Resolved an issue where "Page loading" screen could show indefinitely if the user edits an existing password list (B-836).
- Resolved an issue where the "cleared checkout" log message would be logged twice if a password change job ran when the password was checked out.
- Resolved an issue with various typos.
- Resolved an issue with the request approval logging that would log password request grant when a password request had been denied through the email link.
- Resolved an issue with launching applications with custom connection settings when shadow accounts were configured did not work as expected.
- Resolved an issue where the loading screen would display indefinitely if attempting to update a stored file with a new version.
- Resolved an issue where using the built-in SSH launcher may cause ERPM to create telnet sessions.
- Resolved an issue where the web application could create a bad settings entry when updating web application settings.
- Resolved an issue where editing application settings in the web application would fail because the attributes were not enumerated correctly in the COM object.
- Resolved an issue with the broken remote warning on the applications static credential launch page.
- Resolved an issue where the ActiveXRDP page could cause script errors on load due to the comment style for VB script being wrong.
- Resolved an issue where password requests would not be listed as actionable for non all access accounts for some account store types.
- Resolved an issue with the export of permissions on systems failing to write any output in most cases.
- Resolved an issue with legacy SDK (clientagentrequests.asp page) to correct the display of accounts in shared credential lists.
- Resolved an issue where an error could occur when opening up a Cisco password change job.
- Resolved an issue with a concurrency bug when scheduling new jobs and setting the jobs to run against a dynamic group and run when new systems are added.
- Resolved an issue where sorting on store identifiers in the web application could cause the pages to fail to load.

- Resolved an issue where the asset tag could be removed from a system if the system was moved or copied to a different management set (B-846).
- Resolved an issue with the normalized permissions for systems to be removed, if the permission on system was edited.
- Resolved an issue where immediate account elevation jobs could be scheduled to occur a year later.
- Resolved an issue where the user name was not be returned through the web service when returning web audit logs messages.
- Resolved an issue with Hebrew translations not working.
- Resolved an issue where the web application would hang on a loading screen if you edited a shared credential list and saved settings without changing any settings.
- Resolved an issue where the web application installer could crash occasionally.
- Resolved an issue where some SSH keys might not be discovered.
- Resolved an issue with web application workflow logging that would cause request password to show up twice if a user had permission to request password and access.
- Resolved an issue where deleting stored password through the web service could fail.
- Resolved an issue where iInteractive password verification checks did not produce any results in the output report.
- Resolved an issue where the log message that is generated when creating an RDP link using a store password through the launcher did not indicate the correct system being connected to.
- Resolved an issue where a deferred Processor would reset/re-enable the enablement of alternate administrator (B-845).
- Resolved an issue where interstitial dialog would pend when attempting to update and check in a file to the file store (B-843).
- Resolved an issue where arbitrary Elevation would attempt to put user into the target local group as well as a domain group (B-844).
- Resolved an issue where all delegated identities with an email would receive notifications when a password was requested (B-847).

Version 5.0.1 (August 3, 2015)

- Added a completely new web interface based on bootstrap and JSON.
- Added content management system for website.
- Added delegations in website for management sets, systems, accounts.
- Added admin defined notifications in website (global).
- Added control of browser local DB cache.
- Added sudoers settings discovery and comparison.
- Added SSH key update jobs to the types of jobs that will be run when password change is selected in the zone processor job affinity settings.
- Added automated DB index defragmenting option.
- Added web page for remote app launch logging.
- Added end times to remote app launch web operations to track when the session is ended and published that information to the remote app logging page.
- Added a column in the web operations display to show request entries associated with a password recovery or remote session.
- Added request id to the generated zip output file for web activity logs.
- Added request information to the checkout and check in operation logs related to password recoveries.
- Added the target system field to the list of filters available in the remote app launch audit page.
- Added a field to the web application settings for the server certificate used by the recording server.

- Added a download link to the user settings page of the web application to download the certificate used by the recording server if specified.
- Added endpoint entries to the web application settings to provide the endpoints to the web interface in the session info page.
- Added test connection buttons to the web application configuration to test the connection to the web service endpoints.
- Added web service endpoint links to the user session page in the web interface and links to the JSON help page.
- Added option to prevent any default creation of authentication servers (Options.AppSepcific.Roulette.WebAppOptions.DontCheckAuthServerList).
- Added logging for any operation that updates an authentication server using the console dialog.
- Added missing permissions to the schedule restrictions console dialog under global delegations.
- Added event sink message logging to the remove system from group calls made by the main dialog.
- Added controls on logging functions that use request IDs to ensure the value of the request ID is valid even on failures.
- Updated ServiceNow! Interface updated to account for ServiceNow! Web service API changes (B-859)
- Updated language translations.
- Updated the code to force refresh the display after a system name change is performed to ensure the display shows the updated system name.
- Updated the code that handles merging system information when renaming systems, to set the system type if the existing system type is external.
- Updated the web application to display chart controls using the local time zone of the session.
- Resolved an issue where remote app sets would not show up in the selection list for all access identities in the web interface.
- Resolved an issue where the Console could crash if the key view was shown and known_host files had been discovered under non-root users on remote systems.
- Resolved an issue with various typos.
- Resolved an issue where verification reports would fail when specifying a mailing list instead of a specific individual address.
- Resolved a display issue when showing SSH keys and correlating stored key info with the display to show correct discovered instances for keys.
- Resolved a timing issue with the launcher checking for multi-tab job instructions that could cause the link to appear to be used.
- Resolved an issue where the session recorder (expression) could fail when UAC is enabled on the bastion host.
- Resolved an issue with job prioritization settings code that would cause asserts on some job creations.

Version 5.4.0 (February 12, 2016)

- Added the ability to edit aggregate propagation steps and settings on jobs via console (B608).
- Added Ticket verification to the default SSH console launch process (not using app launcher).
- Added option to use multiple monitors to the Default RDP option (not using app launcher).
- Added elevation expiration email alerting flags to the account elevation job (controlled in the job settings via console or web service/PowerShell).
- Added email options for account elevation jobs to web service and PowerShell structures.
- Moved account elevation email alert templates to EPRM data store as configurable email templates.
- Added new email system with new authentication and security options.
- Added email send verification with server feedback dialog.
- Added validation checking code to the secure email operations.
- Added new secure email settings to the web application configuration pages.

- Added ability for all web services to send an email message using the default email configuration.
- Added ability for PowerShell cmdlet to send an email using the default email configuration.
- Added ability for Password verification reports to support multiple target email addresses separated by a semi-colon (;) (FR705).
- Added ability to remove Website Favorites references when the user loses access to the system/account or original password is deleted.
- Added error handling indicating passwords are not stored when attempting to spin or checkout a password that is not stored.
- Added a message template editor to the console for stored message templates.
- Added an editor for message templates to the web interface under settings.
- Added the ability for compartmentalized passwords settings to apply to password change jobs setting static passwords (B899).
- Added the ability for the Validation for the web app's auto login page to check for required components installed before attempting to process logins.
- Added filters to the event list for configuring event sinks.
- Added pre and post run operation steps for management set updates.
- Added pre and post run operation steps for account elevation jobs.
- Added pre and post run operation steps for password change jobs.
- Added pre and post run operation steps for SSH key change jobs.
- Added pre and post operation job configuration to the web service.
- Added pre and post operation job configuration to the PowerShell commandlets.
- Added a program option (to the program options property sheet) to control whether or not the "item in use" cache is reloaded only on demand.
- Added the ability to clone multiple jobs at once.
- Added the ability to store answer files in the ERPM database.
- Added code to auto-migrate the use of response files for SSH/telnet jobs to the database.
- Added an editor in the ERPM GUI to allow editing of answer files that are stored in the database.
- Added the option to re-create/reset response files to program default.
- Added the ability for the Website "Favorites" panel to edit entries.
- Added the ability for Event Sinks to support TCP and SSL connectivity.
- Added an Event sinks syslog forwarder application.
- Added the ability for the Syslog output to support transform of output message structure.
- Added the ability for the Website to dynamically display all instances of custom configured account store types.
- Added the ability for the Website to dynamically hide account store types and account lists for types that have no configured instances.
- Added the ability for user defined discovery & propagation elements to be displayed in the account store view when actually discovered.
- Added the ability to discover accounts in Azure/O365 cloud instances.
- Added the ability to manage passwords of accounts in Azure/O365 cloud instances.
- Added the ability to auto-discover systems and auto-categorize system from Azure/O365 cloud instances.
- Added the ability to discover accounts in Amazon EC2 cloud instances.
- Added the ability to manage passwords of accounts in Amazon EC2 cloud instances.
- Added the ability to auto-discover systems and auto-categorize system from Amazon EC2 cloud instances.
- Added the ability to discover accounts in RackSpace Public Cloud instances.
- Added the ability to manage passwords of accounts in RackSpace Public Cloud Instances.
- Added the ability to discover accounts in Salesforce (Force.com) cloud instances.
- Added the ability to manage passwords of accounts in Salesforce (Force.com) cloud instances.
- Added the ability to discover accounts in IBM Softlayer cloud instances.
- Added the ability to manage passwords of accounts in IBM Softlayer cloud instances.
- Added the ability for Node for Vmware ESXi Vsphere server management via ESXi web service.

- Added the ability to discover accounts in VMware ESXi vSphere server instances.
- Added the ability to manage passwords of accounts in VMware ESXi vSphere server instances.
- Added the ability to auto-discover systems and auto-categorize system from VMware ESXi vSphere server instances.
- Added stored account browser to the Linux password change configuration page.
- Added Teradata database management.
- Added Teradata account and account attribute discovery.
- Added Teradata account password management.
- Added sorting and grouping to the account store display in the console to ensure like-type account stores are next to each other.
- Added the ability for custom account stores to be hidden from account store view (custom account store settings).
- Added error handling for jobs if the custom account store type is changed or deleted.
- Added a context menu for ERPM console to hide each account store type in the account store view.
- Added the ability for IPMI scan to include the default SuperMicro admin credentials.
- Added the ability to specify N number of additional utility accounts to be used within an SSH Linux password change jobs.
- Added the ability to specify N number of additional utility accounts to be used within an SSH Cisco password change jobs.
- Added web service support for utility accounts for password change jobs.
- Added new variable for Cisco based SSH password change jobs that will always try to load a stored enable password (EableAccount)and make that argument accessible in jobs: $(EnablePassword).
- Added the ability for entries to be double-clicked to add them to the Add Identity dialog when adding identities via the console.
- Added web service function to support scheduling existing jobs to run immediately.
- Added extension of PowerShell cmdlets to support "run job now" for existing jobs.
- Added web Service method to clone jobs (JobOps_CloneJob).
- Added PowerShell cmdlet to clone jobs (New-LSJobClone).
- Added ability for web service to create remote app launch links (AccountStoreOps_CreateRemoteAppLaunchLink).
- Added the ability for PowerShell cmdlets to create remote app launch links (New-LSRemoteAPplicationLaunchID).
- Added the ability for web service method to create SSH key jobs (JobOps_CreateKeyChangeJob).
- Added the ability for web service method to get SSH key job settings (JobOps_GetKeyChangeJob).
- Added the ability for web service method to edit SSH key jobs (JobOps_SetKeyChangeSettings).
- Added the ability for PowerShell to create SSH key jobs (New-LSJobSSHKeyChange).
- Added the ability for PowerShell to get SSH key job settings (Get-LSJobSSHKeyChangeSettings).
- Added the ability for PowerShell to edit SSH key jobs (Set-LSJobSSHKeyChangeSettings).
- Added the ability for Web Service to generate new spin jobs for non-Windows accounts based on previous password change settings.
- Added the ability for Web Service method to set job comments (JobOps_SetJobComment).
- Added the ability for PowerShell cmdlet to set job comments (Set-LSJobComment).
- Added the ability for Web service definitions for IPMI account store objects to set flag to "Use Stored Passwords" to facilitate adding new devices with the option set.
- Added Web service method to facilitate creating IPMI system refresh jobs (JobOps_CreateRefreshIPMISystemJob).
- Added PowerShell cmdlet to facilitate creating IPMI device refresh jobs (New-LSJobRefreshAndDiscoveryIPMI).
- Added Web service method to retrieve known system names for discovered systems (QueryTargetInfo_SystemName).
- Added the ability for PowerShell cmdlet to retrieve known system names for discovered systems (Get-LSSystemName).
- Added the ability for Web service installation configuration files to include service endpoints for the code signing service.
- Added Web service installation tester support for integrated authentication.

- Added the ability for PowerShell job creation cmdlets to have a "delay window" setting (B930).
- Added the ability for Web service definition for job scheduling types to include every N hours
- Added zone processor support for operation against multiple management sets.
- Added zone processor support for multiple zone processors on a zone processor host.
- Added more discovery, cataloging and views to Linux/UNIX sudoers discovery and reporting dialog.
- Added the ability for Event Sink JSON format output transform to support FireEye's TAP collection parser.
- Added the ability for Cisco password change jobs to have two different default answer files reflecting management paradigm shift (CiscoEnablePassword and CiscoTTYPassword).
- Added a log message to ERPM text logs when a system is removed from a mangement set.
- Added a dialog popup to skip the check for existing passwords on password import to secure passwords store from text file.
- Added Event Sink filter to event sink selection pick list.
- Added "Confirm" message box when removing systems from the current management set by hitting the delete button on the keyboard.
- Added /? Help context to the deferred processor executable to show additional [zone processor] required arguments.
- Added the ability for the "Edit Shared Credential Lists website" to display an "Add" button if no lists are found.
- Added validation logic to service account push to ensure the account being pushed is different from the current configured credential.
- Added new program option to disable the warning to prompt for system removal from current management set.
- Added view propagation element details (context menu of discovered item).
- Changed the time window calculation again for the chart controls (legacy website) to fix residual issues with the display window times.
- Updated the website to allow both request password and request access when delay load option is disabled.
- Updated the location of all email templates, now located in the database; physical files are now a failsafe if required template not found in the database.
- Updated the the Linux/UNIX sudo permission data to be exposed on a system by system basis.
- Updated the chart code for legacy website to show current local date times instead of UTC times.
- Updated the the multifactor authentication configuration page to clarify verbiage for most and least privileged settings.
- Updated the web service and PowerShell calls to ignore page size for stored password list calls, returns all stored passwords for system now (B724).
- Updated the RSA next token dialog in the console by resizing to display the system generated PIN.
- Updated the used RSA token code display in the RSA login page to obfuscate any previous used passcode.
- Updated the PUM page for the new interface.
- Updated the management set configuration dialogs to a new look.
- Updated the location of the Event sink configurations to the ERPM data store to make it globally available
- (FR695).
- Updated the Event sink list so it no longer accepts events outside of acceptable ranges.
- Updated the Cisco password change job processing paradigm - Caution! There is no migration path for old jobs to new format, but old jobs will still work post upgrade.
- Updated the default propagation scope to disabled for all account types.
- Updated all instances of JobID used by the web service to use strings instead of integers.
- Updated all return types from the web service to be structured data.
- Updated the PeopleSoft extension to return data in XML format.
- Updated the way the reconfig of the ApplicationHost.config file is handled, from error to warning in case IIS is holding the file open and it can't be written.
- Updated the account selection dialog for account credential to push to use the generic stored password select dialog for scalability.

- Updated the "Item in use" display to use fully qualified account names for lookup to avoid false positive matches for accounts from other namespaces.
- Updated the reboot options to disabled when the job type is for management set updates.
- Updated the behavior of the SSHD configuration dialog to show a value of "Default" instead of implicit values to better handle the case where no explicit option is set.
- Updated the password input fields for personal password storage to be obfuscated password input fields.
- Updated the importing of stored passwords with no namspace argument so it is no longer allowed.
- Updated the ticket verification logic so it no longer performs ticket verification if the web application's "Require Ticket Number" option is not enabled.
- Updated the "Request Access" icon in the web interface to differentiate from "Request Password" icon.
- Updated the job scheduling option "Every N Days" to accept a maximum entry of 1 million days.
- Resolved an issue with an Event sink COM server unload timing issue that could cause the deferred processor to improperly/prematurely terminate.
- Resolved an issue with Event sink logging settings not being retained (B914).
- Resolved an issue with logic error where span monitors and fixed resolution could be specified in the same config (span monitors forces full screen).
- Resolved an issue with various typos in the website and console.
- Resolved an issue with the web application installation configuring ipworks9 files instead of the ipworks8 files.
- Resolved an issue where the deferred processor configuration dialog did not update paths for components when their paths were reconfigured.
- Resolved an issue where the MFA settings would disable the most restrictive options when OATH was enabled in the multifactor settings.
- Resolved an issue where the job locking mechanism could cause an abandoned transaction instance.
- Resolved an issue where the multi-stage launcher verification code paths would incorrectly mark the launch GUID as used.
- Resolved an issue where the application launcher would cause an error if any of the abort operation cases occurred (observed if the hashing verification failed for exes).
- Resolved an issue with the website timing that would cause the terminal.asp page to not show the SSH applet automatically under some circumstances.
- Resolved an issue where changing permissions on files that included the underscore character in their name would not work in the website.
- Resolved an issue where the user SSH keys writing function could cause failures to save SSH keys for any database that was not migrated from a previous version.
- Resolved an issue where changing the settings of the Compliance Database would not update the website settings properly while the application was running.
- Resolved an issue where the compartmentalized password display in the website could indicate the wrong password slice.
- Resolved a cosmetic issue in the website that would cause some password options to appear (access denied if clicked) that were not allowed when dynamically loading permissions.
- Resolved an issue with several missing configuration options in the web application site config page.
- Resolved an issue where the website would show an error when navigating to shared credential lists list page if the last list the user viewed was removed (B911).
- Resolved an issue where the SSH password change jobs may not correctly set the login username when using an SSH key for authentication.
- Resolved an issue where the application launcher hash verification might not work properly (B906).
- Resolved an issue where the web service could strip the login user from logout messages.
- Resolved an issue where the RSA logins to the management console could report errors in some success cases for next token checks and PIN assignments.
- Resolved a display issue with the Job Activity compliance reports, which was causing some job types being incorrectly identified as "unknown".

- Resolved an issue where the web service relied on users owning at least one job in order to fulfill the permission check.
- Resolved an issue with the Password Lists failing to draw.
- Resolved a display issue with Oracle password change defaults for the password change settings.
- Resolved an issue where the shared credential page could display errors if permissions were removed from the active list.
- Resolved an issue with the website system page for postgreSQL that would prevent the database instances from being shown for non all-access users.
- Resolved an issue with an ASP bug affecting the file checkout page.
- Resolved an issue where retrieving passwords for custom types would cause passwords of multiple types to be returned if the stores had the same system name.
- Resolved an issue where password change jobs for custom account store types could appear successful even when they failed.
- Resolved an issue with certain table name collisions when using oracle as the backend datastore.
- Resolved an issue with web interface session panels bugs when using the Oracle provider.
- Resolved an issue with a logic bug that caused RSA challenge to be issued if Force 2FA was enabled in the web and the user was configured to use OATH.
- Resolved an issue where requesting access to shared credential lists did not always work as expected (B908).
- Resolved an issue where editing the personal password store would cause the account name field to be submitted twice resulting in entries with duplicate account names.
- Resolved an issue where explicitly provided credentials used for SSH connections would not be used if there were stored credentials for the same target.
- Resolved an issue where the client agent requests page would not display lists of accounts for a shared credential list.
- Resolved an issue with the loading icon appearing when files were recovered from the file request page.
- Resolved an issue where the account filter was not showing account type "None" in the account type filter page.
- Resolved an issue where the password history, activity, and edit/remove were not correctly displayed when the website delay loading option was enabled (B901).
- Resolved an issue with the password history not being properly kept for passwords that were 126 characters or longer.
- Resolved an issue with the website compliance reporting page not showing a page error if no compliance reports were stored.
- Resolved an issue where the website display issue recorded sessions logged on user field incorrectly identified the target user. Actual data was intact.
- Resolved an issue with custom communication types not working (B851).
- Resolved an issue where the window of opportunity setting for job run was not being saved when job type was set to run every N hours (B850).
- Resolved an issue with the Account Elevation job priority not being set (B849).
- Resolved an issue where access requests for shared credentials were not showing on favorites panel (B896).
- Resolved an issue where the website/service may not trigger event sinks all the time due to premature COM application unloading (B872).
- Removed the Lieberman logo from the generic report output template.
- Removed the Advanced service configuration from the default install mini wizard for new installations.
- Removed the display for "User can't change password" account setting for Windows domain accounts in the account details page.
- Removed the old EasyMail email system.
- Disabled the option to configure OATH QR codes if the setting is disabled globally.
- Updated the grouping of the QR code settings for the user tokens for OATH.
- Updated the Mindterm component for SSH session to version 4.1.9 to support more security options.
- Updated international language translations.

- Updated the compliance reports paging to deal with result set size problems while rendering the reports.

Version 5.5.0 (June 29, 2016)

- Changed the Namespace dropdown list to sort alphabetically for all namespaces.
- Added support for adding Azure Active Directory users to delegation roles.
- Added support for logging into the web interface using Azure AD identities using OAuth.
- Added the ability to pre-load a scan configuration when launching the scanner GUID.
- Added the current web client session authentication token to the current session information page.
- Resolved an issue with a bug that removed the password column from the Stored Passwords dialog.
- Resolved an issue with a bug that allowed a user to move a system, effectively removing it from the current group.
- Changed the password verification report to include Oracle accounts in the result data.
- Resolved an issue with a Schedule Settings bug that allowed you to schedule a job on a day that doesn't exist for the configured month.
- Resolved an issue with a bug that would cause password verifications for SQL Server accounts to always use integrated authentication instead of the stored password.
- Resolved an issue with a bug that would cause the local and global account elevation times to both always display the global elevation times in the web interface.
- Resolved an issue with a console bug that would occur if invalid database connection credentials were provided on startup.
- Updated the language utility to import and export CSV text formats for the language files.
- Added custom error handler code to route all standard IIS error codes to the normal error page with the standard IIS message.
- Resolved an issue with a bug in the applicationhost config update code that would cause the custom error code setting to fail if httpErrors was not the first element of the block.
- Resolved an issue with a typo in the name of the GetSystemName PowerShell cmdlet.
- Added proxy web configuration support for connections to Amazon EC2 (AWS).
- Added an “export all” function to the language template support utility.
- Resolved an issue with a bug in the language utility that assumed data coming from CSV import contained headers.
- Resolved an issue with a bug that would cause zone processor errors when determining if pre-run alert email messages should be sent.
- Added the ability to schedule a refresh of custom account stores and custom account store accounts.
- Added a web service and PowerShell call to retrieve private SSH keys from the database.
- Updated the language utility to support tabbed CSV input files.
- Added the ability to use Salesforce (Force.com) instances as authentication sources.
- Added the ability to do OAuth authentication against Salesforce for web user logins.
- Resolved an issue with a bug with the PhoneFactor 2 factor authentication of users where failure cases would be treated as success.
- Resolved an issue with a few bugs that would cause zone processors installed on stand-alone machines to use default encryption settings instead of the settings specified during the push.
- Added code to the Azure AD OAuth code path to support authenticating with Windows Live users that are federated in Azure AD.
- Added custom connection replacement argument explanations to the custom RDP config dialog for application launch.
- Added the ability to specify an RDS connection broker as part of the application launch's RDP config on a remote jump server.

- Changed the Login page to hide the user name and password fields if the user is using OAuth sources for authentication.
- Resolved an issue with a bug in the AWS system discovery code that would throw an exception if a specific region could not be enumerated.
- Added support for classification of virtual compute resources in AWS that don't have platform tags. (Most images built off AMI are of this type.)
- Resolved an issue with a bug related to being able to see accounts (not passwords) on MySQL, PostgreSQL, Teradata, Oracle types in the web interface for non all access accounts.
- Added support for Xerox Phaser printer account stores.
- Fixed a bug in the zone processor system set calculation for account stores in groups. The fix accommodates for account store types when the account store ID matched.
- Resolved an issue with a bug with radio control enabling in the add delegation dialog.
- Resolved an issue with a bug with the remote app jump server config dialog that was not enabling disabling the fields correctly for the new RDS connection broker config.
- Added an SNMP scanner for discovering Xerox Phaser printers.
- Added web service and PowerShell calls to manage Xerox Phaser printer instances.
- Resolved an issue with a bug with the ServiceNow ticketing integration that would attempt to retrieve all tickets to verify a login.
- Resolved an issue with a bug with the processuniquecommand page.
- Added pre and post operation settings to the list of settings that are copied when a job is cloned.
- Resolved an issue with a bug in the Set-lsjobpreandpostrunsettings cmdlet that would cause PowerShell to crash.
- Resolved an issue with a bug in the launcher that would cause a failure if the remote server name was blank even when using the RDP connection broker to create the session.
- Added an extra log message when testing connections using PhoneFactor auth to check the SSL/TLS security certificate if you get a failed check.
- Updated the PhoneFactor support integration library to be compiled for .NET 4.0.
- Added an OAuth login authentication indicator badge to web application header menu.
- Resolved an issue with a web service login bug that would cause client certificate authentication to fail if the certificate did not have permission to log in.
- Resolved an issue with a bug with zone processor scheduling queries that would cause bad queries to be displayed in the query dialog.
- Resolved an issue with an issue related to account elevation jobs and scheduling queries.
- Updated the custom account store details dialog to display formatted XML.
- Updated the jump server configuration to always allow entering a jump server name.
- Resolved an issue with a bug related to the addition of OAuth authentication servers handled in the legacy web application.
- Resolved an issue with a bug in the legacy web application related to changing getPasswordSettings new reliance on passing an authentication token.
- Added a custom context popup menu for external Azure AD accounts to prevent password change operations.
- Updated the additional data format reported back from AWS account discovery to be compliance XML.
- Resolved an issue with a performance issue with the delegation dialog related to redundant sort calls while adding new items.
- Updated the TestConnection cmdlet to return success when authentication is not allowed between client and server.
- Updated the delegation dialog and delegation permission dialog to streamline the load and view processes by adding paged queries.
- Updated the default web.config file for the web interface to use custom error settings with custom pages.
- Added a result cap to the delegation permission display dialog to help with long loading times when there are logs of delegation permissions.

- Implemented delay load callbacks for permission on account dialog tree expanding to accommodate for hundreds of identities with permissions on accounts.
- Removed some references to removed JavaScript files from the web interface.
- Added paging controls and queries to the remote applications launch page to increase performance of page loads.
- Resolved an issue with a bug in the web service serialization code that prevented the change twice password change setting from being updated when password settings were set through the service.
- Resolved an issue with a bug where that default sort column was not defined for the stored passwords dialog on initial load.
- Updated parity for the TestConnection cmdlet to return success instead of failure on security errors while connecting.
- Resolved an issue with a bug with default result maximum filters when loading delegated permission identities.
- Resolved an issue with a bug that was incorrectly assigning the Radius 2-factor permission bit to OATH requirements for delegation permissions on identities.
- Resolved an issue with a bug that was causing the request remote access global permission to not be deserialized correctly in the web service when set or read from XML.
- Added extra trace code to the login PowerShell cmdlet to indicate the subject name of the certificate being used to auth with IIS and the exception trace if auth with IIS fails.
- Resolved an issue with a bug in the web interface related to launching applications using shadow accounts on several non-windows type systems.
- Added code to ensure the default email profile template exists if the database changes while ERPM is running.
- Added code to the message template dialog to be able to default all the templates.
- Added code to show which message templates are not set to the defaults.
- Added code to revert each selected message template to the defaults.
- Updated the default password status report template to include the management set name and the generation date.
- Resolved an issue with a bug related to creating the missing shell association registry key for opening interactive reports.
- Resolved an issue with a bug that was causing account filters for Xerox, PostgreSQL and Teradata not to cache correctly in the web interface.
- Re-added save and load group info from XML with new serialization code.
- Resolved an issue with a bug with the unique command processing page related to password request
- approval/deny.
- Added an index to the login name field of the web interface sessions table.
- Resolved an issue with a bug with the default encrypted value for OAuth email settings that would cause the default email settings to fail to be read if there were no legacy settings on the system.
- Updated the default page size controls for users to use the default global values unless overridden explicitly.
- Resolved an issue with a bug in the email configuration pages that was dropping settings when browsing for certificates.
- Updated the ability to save an explicit account used for a custom account store and update the config to use that stored password.
- Resolved an issue with a bug in the web application that was causing some selectors to cause JavaScript failures if the selector ID had a period in it.
- Added a timeout redirection to web pages that logs users out when the session expires.
- Added a visual alert to the web application to indicate impending session timeout.
- Improved error logging for VMWare when the password being set doesn't meet the complexity requirements.
- Resolved an issue with a display bug that would cause the custom account store type name in the console to revert to "Custom Account Store" after operations.
- Resolved an issue with a bug in the CLR account store load code that would cause a failure if two threads tried to set the CLR configuration at the same time.

- Resolved an issue with a bug in the custom account store refresh code that could generate error messages when the jobs were first created because internal data for the job was out of sync.
- Removed the custom error page for authorization failure because the browser depends on getting back a 401 error to handle the integrated authentication case.
- Resolved an issue with a bug in the Windows integrated login case for the PowerShell cmdlets that would cause failures on login.
- Updated the web service impersonation feature to allow impersonating Windows group identities, Radius users, roles, and certificates, as well as Windows users and explicit identities.
- Resolved an issue with a bug that could cause activity lifecycle relationships to be wrong for password checkouts in the web application log.
- Updated the password set function in the web service to preserve any existing password generation and constraint settings.
- Boldly localized where no one had localized before.
- Made another change to the default web.config file to support other cases in IIS with custom errors and authentication providers not working with integrated authentication.
- Added the checkout user name to the displayed list of users in the web interface along with the checked out icon.
- Added code to detect and default if the user sets their default login page to a page that doesn't exist on the web server.
- Changed the default sort order for the management set dialogs.
- Updated bootstrap versions for the web interface.
- Updated JQuery versions for the web interface.
- Updated TinyMCE version for the web interface.
- Rewrote the management set serialization code for the web service to support get and set operations for the new management set code.
- Added resize controls to the Linux system details pages.
- Added code to track which web users have viewed which web messages and added display code to show callouts when there are unread messages.
- Added an account name filter to the Windows accounts page in the web interface.
- Resolved an issue with a bug where the job comment was not added to the event sink output message for account elevation jobs.
- Resolved an issue with a bug with password checkout through the PowerShell cmdlets that was not passing the checkout comment correctly.
- Updated URI and descriptions for the JSON web service.
- Updated the deferred processor to launch child processes as create process with logon in order to get a new user login token.
- Added code to the deferred processor to restart the deferred processing service every 5 hours by default, AppSpecific.Roulette.SchedulerService.SchedulerRestartMinutes.
- Added UI code to control the service reset settings.
- Resolved an issue with OAuth logins by adding the required ipworksssl9.dll to the list of files that are copied with a web installation.
- Added the ipworksssl.dll to the list of files that the web application checks for when it starts to ensure that everything required is present.
- Resolved an issue with a bug related to Cisco device filter settings in the console.
- Resolved an issue with a bug where the Azure and Salesforce instances were not correctly using the selected defaults when you edit the authentication server entry in the console.
- Added resize code to the zone processor configuration dialog.
- Refactored the resource names of the web application management property pages to match with the property page naming convention.
- Updated the multi-factor authentication options around to support internal and external MFA being enabled at the same time.

- Removed the cached service credentials for zone processors because it is not necessary to store them when installing or editing zone processors.
- Resolved an issue with a bug in the deferred processor scheduling logic having to do with job affinity filters.
- Resolved an issue with a bug with Serilog assembly version breaking some of the CLR interop types when attempting operations.
- Resolved an issue with a bug with the web service where settings the password change settings in a job would revert all password constraint settings to the default.
- Removed scan results from the web application.
- Updated the favicon.ico path in the web application so that it resolves now according to the current conventions.
- Resolved an issue with a problem with Bootstrap's default CSS map linking to files that aren't present in the default install.
- Added code to the authenticator retrieval call to ensure that the explicit login type exists.
- Added explicit proxy settings configuration for all supported cloud types.
- Added a few missing translation strings to the localization files.
- Added a GetSSHKeyList command to list all available ssh keys in the store with their type.
- Added a getOperationsForPassword command to get the permissions for a specific target account that are available to the calling user.
- Resolved an issue with a serialization bug for times that affected many of the time related fields in the web service.
- Added a key data class to return private key data in a structure through the web service to include key type, key length, passphrase, and so on.
- Resolved an issue with a bug with the proxy settings check in the CLR extensions for the cloud.
- Resolved an issue with a bug with the 2factor login pages that would cause the loading div not to show up while logging in.
- Resolved an issue with a bug in the web service verb capitalization scheme that changed POST to Post.
- Resolved an issue with a problem with styles involving the default message templates from reports generated from the database.
- Resolved an issue with a typo on the password recovery page comment prompt that included the wrong text.
- Updated the verbiage on the scheduler service restart frequency option.
- Resolved an issue with some typos in the new web service function description strings.
- Added filter settings for unknown and ignored target types.
- Added caching and lookup as well as replace-in-place for ignored and unknown target types.
- Updated icons and verbiage for unknown and ignored targets to un-categorized and explicitly categorized.
- Resolved an issue with a bug that caused adding or editing Radius authentication server configurations to fail.
- Updated the default behavior of users with delegation permissions on shared credential lists to prevent them from having other implicit permissions.
- Resolved an issue with a bug that prevented users with shared credential list delegation permissions from being able to see and edit the delegation settings of the list.
- Added context menu handlers to popup the context menu for un-categorized and explicitly categorized filters.
- Updated the name of the dialog for un-categorized and explicitly categorized targets to be generic.
- Restructured the web application installation dialog to support UI caching.
- Adjusted the web application installation dialog to conform with maximum size requirements.
- Added sanity checks and warnings to the web application installation dialog to check for system root paths and website root installs.
- Resolved an issue with a bug with hiding the un-categorized and categorized types from the main display.
- Resolved an issue with a bug related to editing proxy settings for SoftLayer account stores.
- Resolved an issue with a bug related to PowerShell/web services overwriting password generation settings on set.
- Added caching for OATH token user email and phone number data so it is not looked up each time the OATH token needs to be sent.
- Resolved an issue with a bug where a few web permissions reported to the cookie for caching improperly spelled DENY as DENTY. This did not affect anything functionally but has been fixed.

- Updated the LDAP connection code to do an IP lookup before attempting a connection because apparently the Windows LDAP code is very slow for name lookup.
- Resolved an issue with a few typos in the message template defaults for styles on some of the HTML reports.
- Updated the default styles for some of the message templates.
- Removed the warning about explicit exclusion when removing account store types from the group because account stores cannot be explicitly excluded.
- Resolved an issue with a bug that would cause a recursive loop crash if the display was redrawn while a windows group membership node was expanded in the main display.
- Updated the login group enumeration to use LDAP instead of ADSI.
- Updated the text on the account store options property page to reflect the updated language.
- Updated the return code from the remove panel call in the web interface to return success if the panel has already been removed.
- Made a UI change to check for and replace a specific value in a previous version's email verification defaults.
- Updated the default text encoding of generate response file temp files to UTF8 so that the XML parsing engine wouldn't get confused and fail if it accidently created a UTF16 file instead.
- Resolved an issue with a bug in the accounts page caused by the new account name filter which caused delay-loaded page data to fail with internal errors.
- Resolved an issue with a bug in the legacy web application that caused password retrieval pages to fail to load.
- Updated the wording and layout of the categorization node selection in the account store display page.
- Resolved an issue with a bug with LDAP group enumeration for web application logins.
- Updated the launcher to not delete the generated temp RDP files in debug builds.
- Resolved an issue with a bug that would cause a crash if the cloud instance specific settings got desynchronized with the expected XML format.
- Resolved an issue with a bug that would assert if you try to edit VMWare instance specific proxy settings.
- Updated the certificate parsing code for parsing CAC FASC-N fields to ignore extra data encoded into the end of the FASC-N field.
- Added a configuration option for the loadbalancerinfo field to the remote application server's configuration information.
- Resolved an issue with a bug in the zone processor and service startup code that would cause the display to show the wrong job affinity in the config dialog.
- Changed the layout of the licensing dialog to conform with the current sizing layout guidelines.
- Changed the data store maintenance to log an error message and continue instead of assert and fail if the ranges for maintenance are not valid.
- Resolved an issue with a UTC time conversion bug in the checkout password logic.
- Updated the stored account view code in the web interface to check the view accounts permission instead of the recover accounts permission.
- Resolved an issue with a typo in a log message that would occur if you had removed the default shell association from the browser.
- Resolved an issue with an error in the BMC Remedy module that caused ticket verification lookups to look in the wrong schema for tickets.
- Resolved an issue with a bug in the error handling for loading MFA libraries that would cause unhandled exceptions if the libraries aren't configured on the system.
- Resolved an issue with a bug in the RSA passcode test dialog in the console.
- Resolved an issue with a bug in the RSA next token code login code for the web application.
- Resolved an issue with a bug related to calling the Safenet agent when the BSAPI component is not installed.
- Resolved an issue with a bug that was causing external accounts to show up as a menu item in the accounts list in the web application (web client).
- Added JavaScript minimization for the web interface JavaScript files.
- Consolidated the JSON and WSDL endpoints into the AuthService service.
- Added descriptions to the web service functions of the AuthService service (AuthService_Json is unchanged).

- Resolved an issue with a bug that could cause a race condition on session timeout between the timeout in the database and the timeout in the JavaScript code on the web page.
- Updated the known default credentials to be encrypted with the internal encryption method.
- Checked in a change that will cause the web application (web client) to ignore the ForwardingAddress cookie value when logging in.
- Resolved an issue with a bug with encoding query string arguments used in the search filter items in the web pages when AJAX page loads are configured.
- Resolved an issue with a URI encoding problem when passing arguments from the Favorites panel.
- Resolved an issue with a bug that caused the launcher to try to start the debugger.
- Resolved an issue with a bug in the authentication server dialog that would assert if you attempted to move an auth server up in priority when it was already the first in the list.
- Resolved an issue with a bug that would prevent the Favorites panel from displaying.
- Resolved an issue with a bug related to the web application display of LDAP and DRAC system types.
- Resolved an issue with a bug related to querying for available applications using the paged view code.
- Resolved an issue with a bug that would cause the application launcher link to not show up when using shadow accounts for several account store types.
- Resolved an issue with some discrepancies between several translation files and the reference content for the status panel where the number of spaces did not match.
- Resolved an issue with another issue related to the application launcher and shadow accounts that would not show the correct available shadow accounts for account store types.
- Updated some verbiage on the delegation identities pages to make it more consistent.
- Updated the delegation identity dialog to disable the role assignment button if no valid role identities are selected.
- Updated the shared code email settings to support registry-based usage when the database is not the program data-store.
- Resolved an issue with an application launcher bug that would cause the query that gets the launched app's settings to fail on launch attempt.
- Resolved an issue with more language issues with \ \ in the translation files.
- Started a UMP reporting web service to trigger the creation of reporting jobs in UMP.
- Resolved an issue with a typo in the AS400 systems page of the web application.
- Added support for multi-factor authentication token codes to the web service login.
- Updated the LDAP login code to remove the assumption of doing a DN search to bind simple user names for Windows directories (Kerberos issue).
- Resolved an issue with a bug that would cause LDAP connection failures not to log the error on the connection in some cases.
- Added an override case when using integrated authentication and LDAP to not replace the system name with the system's IP address because that would break Kerberos over LDAP.
- Added a few error strings to the translation template that can be returned through COM calls.
- Resolved an issue with the zone processor and deferred processor installation code so it correctly uses the application's configured relative log paths instead of the defaults.
- Updated the Hebrew and Arabic translation files.
- Updated the deferred processor config GUI to show the current default log file path for the deferred processor.Error! Not a valid link.Fixed: the pop-up menu for Linux host is different on Account Store View and Linux/Unix System View.
- Resolved an issue with SSH Daemon Settings tab so it should appear regardless of presence of data.
- Resolved an issue with SSH Key fingerprint decoding data, which was sometimes incorrect.
- Resolved an issue with the Manage User Keys screen—Account Store Type always empty.
- Updated the ERPM reporting system keys in the Manage User Keys dialog.
- Resolved an issue with the system refresh throwing the following message: "Note: No access rule information available from remote target in currently supported format”.
- Resolved an issue with the SSH Key not finding RSA v1 public key files.

- Resolved an issue with the RSA1 keys not showing up in SSH Key View after system scan.
- Resolved an issue with the SSH Key discovery partially failing if more than one key of a type exists for a user.
- Updated the low power user Linux system to require default value requiretty in sudoers file.
- Resolved an issue with so that the paths to authorized_keys and known_hosts are hard-coded to /root and /home.
- Updated the Manage User Keys screen by applying proper "Key Type" field values.
- Resolved an issue with the Store Password "Mask Passwords" checkbox/text object not tracking window size changes.
- Resolved an issue with Known_hosts not being understood if not in /home on Linux host.
- Resolved an issue with the Manage user keys screen so "Public Key?" field needs to be populated for discovered keys.
- Updated the stored passwords dialog to be resizable again.
- Resolved an issue with some Linux operating system distributions not being properly recognized.
- Resolved an issue with Low-power discovery by fixing a bug that did not properly deal with empty directories.
- Resolved an issue with SSH Key rotation (Update) so it uses proper EOL characters in the authorized_keys file.
- Resolved an issue with ECDSA and ED25519 HOST keys so they are properly identified as such.
- Added low-power discovery—discovery of key types by content, not by name.
- Resolved an issue with Partial completion. Sort functionality in COXTreeCtrlEx was broken.
- Added DSA, EC key support for SSH.
- Resolved an issue with ECDSA keys bit length being incorrectly identified.
- Resolved an issue with ECDSA type being inconsistently identified in SSH Key View.
- Resolved an issue with low-power discovery not working correctly.
- Resolved an issue with the warnings in console about password length.
- Resolved an issue with the user name displaying incorrectly if the home directory was not in /home.
- Updated the persistent column widths and sort column/order for SSH Keys dialog.
- Resolved an issue with the zone processor installer by adding installation support for multiple zone processors.

Version 5.5.1 (September 7, 2016)

- Added Web service function to create reporting jobs. These job types are currently not available in the console or web client, only in the web services.
- Added Web service functions for "global group membership" reports.
- Added Web service function for "local group membership" reports.
- Added Web service functions for "global groups" reports.
- Added Web service function for "local groups" reports.
- Added Web service function for "trust/computer accounts" reports.
- Added Web service function for "local users" reports.
- Added Web service function for "logged on users" reports.
- Added Web service function for "Rights" reports.
- Added Web service function for "Policies" reports.
- Added Web service function for "NTFS file permissions" reports.
- Added Web service function for "File and folder" reports.
- Added Web service function for "Network Shares" reports.
- Added Web service function for "Audit settings" reports.
- Added Web service function for "Event Log Information" reports.
- Added Web service function for "Event Log Settings" reports.
- Added Web service function for "IE Updates" reports.
- Added Web service function for "Installed Software" reports.
- Added Web service function for "Windows Updates" reports.

- Added Web service function for "VNC Instances" reports.
- Added Web service function for "UNIX users" reports.
- Added Web service function for "System Information" reports.
- Added Web service function for "Network Sessions" reports.
- Added Web Service function for deleting stored reports.
- Added Web Service functions for listing of stored reports.
- Added Web service function to remove user imported SSH keys.
- Added Web service support for custom account stores (user defined, CLR, other nodes) in management sets.
- Added verification of settings capabilities to the Session Recording configuration utility.
- Added session recording config utility can check for the presence of an ObserveIT agent.
- Added Web client ability to hide and never show passwords upon retrieval (clipboard access only).
- Added automatic CSV generation to the compliance report generation snapshots.
- Added automatic PDF generation to the compliance report generation snapshots.
- Added LDAP users as a delegation identity type (rather than only through roles).
- Added SAML-based authentication for Okta.
- Added SAML-based authentication for PingOne.
- Added SAML-based authentication for OneLogin.
- Added SAML-based authentication for Microsoft ADFS.
- Added SAML attribute mapping filtering.
- Added known default credential password store for mapping default credentials to specific platforms when performing a system scan to update the management sets.
- Updated password change job logic to check for checked-out passwords for all built-in types before running change jobs, instead of just Windows change job types.
- Updated the compliance reports so they now store and render stored reports from the database.
- Updated the password check-in error logic to show a popup error and redirect if a user tries to check-in a password that is not checked out to them.
- Updated the code so that password checkout expiration events are sent even when pending checkout expiration notifications are disabled.
- Removed the read only nature of the authentication server information related to Salesforce as an OAuth authentication source.
- Updated the password wizard so that it will only allow "system reboot" when editing/creating windows password change jobs.
- Resolved an issue where application launcher recorded sessions longer than 5 minutes would not transcode.
- Resolved an issue where the application launcher login name parameters might not be replaced correctly when launching apps.
- Resolved an issue where delegations to domain users would always change domain name to default domain instead of selected domain.
- Resolved an issue with various typos.
- Resolved an issue with proxy usage for endpoints being case-sensitive.
- Resolved an issue where compliance report generation code might generate UTF-16 formatted files instead of configured UTF-8 formatted files.
- Resolved an issue with tree control for account delegations where the tree would fail to expand.
- Resolved an issue where the Web client would list an expired password checkout to appear to still be checked out.
- Resolved an issue where if the base log path was left as the default, bad log paths for subsequent log would be generated.
- Resolved an issue with database maintenance jobs not running as scheduled.
- Resolved an issue where Web service Teradata functions would not properly read/report Teradata account information.
- Resolved an issue where Web client filters for retrieving systems available operations would not always return available systems.

- Resolved an issue where password request grant/deny page for one time email links would return scripting errors when viewed or used (though it functioned correctly).
- Resolved an issue so application launch links not show up in the systems pages for use with shadow accounts.
- Resolved an issue where jobs page in web client would cause system propagation states not to display correctly.
- Resolved an issue with the Web client Windows account page account filter not working.
- Resolved an issue where the Web client Windows account page logic for evaluating and displaying account usage for accounts was used across multiple systems.
- Resolved an issue with the Web client Windows account page only displaying usage information based on the first system loaded on the page.
- Resolved an issue with application launch icons not displaying properly on the Linux and Cisco system pages.
- Resolved an issue where the Web client would show application launch links for shadow account mapping in system to all users if any user had shadow accounts configured.
- Resolved an issue where LDAP user delegations would prevent simple username authentication from working for non FQDN LDAP login names.
- Resolved an issue with improperly initialized system name field when adding/editing the system name of a Xerox printer.
- Resolved an issue where the Salesforce client secret would not populate correctly when editing the authentication server entries directly.
- Resolved an issue with zone processors not running management set update jobs when target management sets targeted a specific management set AND job affinity include system based job types (e.g. account elevation or password change jobs).
- Resolved an issue where users with only "request remote access" permissions could make password requests.
- Resolved an issue with password expiration events triggered multiple times.
- Resolved an issue where if Event Sink output format was set to JSON, the output mapped the basic event type ID instead of the “appsepcific” event id.
- Resolved an issue where the Web client would log an error (though the function did work) when uploading files from a user with only group memberships, and no default permissions for secondary group memberships on uploaded files.
- Resolved an issue where ERPM would log errors when trying to change passwords for custom account store types (Web Logic and Web Sphere), even though job did fully succeed.
- Resolved an issue with the Web client controls for use of the RDP thick client not changing the setting.
- Resolved an issue with a page error in the password lists page if there are no password lists configured and visible to the user.
- Resolved an issue with SSH key rotations (when not also removing old key data) could cause a "newline character" to show up in the key string when appending a new key to the authorized keys file.
- Resolved an issue with compliance reports not including all names for all possible report types when generating report output files.
- Resolved an issue where management sets would not remove a system from the management set when a user deleted the system manually.
- Resolved an issue where management sets would not remove systems from the management set when discovery methods no longer included the target system.
- Resolved an issue with a system that was discovered through system scanner as an uncategorized system, which was later categorized and subsequently removed, would be automatically added back to the management set on the next update.
- Resolved an issue where VMware ESX custom account stores could generate errors or fail during back to back password rotations.
- Removed IIS 401 error page redirection because it interferes with IIS integrated authentication when accessing the secure file store.
- Updated the Web service web configuration files to support new endpoint definitions.

Version 5.5.2 (January 25, 2017)

- Added SSH key operations via web service: /Rest/SSHKey, /Rest/SSHKeys, AccountStoreOps_SetSSHKey, AccountStoreOps_RemoveSSHKey, AccountStoreOps_GetSSHKey.
- Added PowerShell cmdlet for SSH key operations: Get-LSListSSHKeys, Remove-LSSSHKey, Set-LSSSHKey.
- Added PowerShell cmdlet to list authentication servers: Get-LSListAuthenticators.
- Added support for account pooling settings to be copied during job clone operations.
- Added PowerShell cmdlets: Get-LSOperationsForAccount, Get-LSAvailableSystems.
- Added PowerShell cmdlets for custom account stores: Get-LSSystemsInManagementSetCustom, New-LSSystemInManagementSetCustom, Remove-LSSystemFromManagementSetCustom.
- Added interactive charts, panels and dashboard elements: password search panel, User Activity, Password Activity, Password Summary, Password Usage Summary, Password Access Times charts, and more!
- Added support for SAML SSO to SecureAuth.
- Added chart and panel configurations to the user settings page.
- Added log messages if historical passwords are removed through the dialog or automatically according to history settings.
- Added the ability for Account Elevation to support multiple systems per elevation job.
- Added password constraints to the password settings object for the web service/PowerShell.
- Added password propagation settings to the settings object for web service/PowerShell.
- Added completion stats to all jobs that have run instead of just failed jobs.
- Added delegation permission for job functions to the web service/PowerShell.
- Added logging messages for adding and removing users from roles.
- Added user session information to web service API.
- Added request remote access permission to the delegated permission on management set object in the web service.
- Added simple username option to the RADIUS external MFA configuration dialog.
- Added context menu option to set delegation settings for jobs in the jobs dialog (console).
- Added Web service function to return all registered web service configurations: /Rest/Config/WebServiceInstallations, Config_GetWebServiceInstallations.
- Added per-system account elevation logic to account elevation jobs to support multi-system account elevation jobs.
- Added user created account/system elevation lists to the account elevation page of the web interface.
- Added CORS support to the web service to enable calling the web service from any origin context (change web.config to enable).
- Added Web service function to delete a stored web service configuration:
- /Rest/Config/WebServiceSettings, Config_DeleteWebServiceConfig.
- Added: Web service function to extend password checkout: /Rest/StoredCredential/Extend, AccountStoreOps_StoredCredential_ExtendCheckout.
- Added PowerShell cmdlet to extend password checkout: Set-LSPasswordExtendCheckout.
- Added displayName field to the list of attributes that are returned during user enumeration from Active Directory.
- Added custom port config for BMC Remedy ticket integration.
- Added new web application setting to prevent users from elevating any account other than the current logged in web user.
- Added system list replacement argument to pre-run alerts for jobs.
- Added new panel in the web interface to enable fast search for managed passwords without opening the managed password page.
- Added log messages for SSH connection retry attempts.
- Added additional logging for SSH connections to help better diagnose.

- Added SSH option to control absolute timeout for SSH operations (Options.SSH.AbsoluteTimeout).
- Added additional method of copying data to the clipboard for Chrome 43+, IE10+ that doesn't require special permissions.
- Added website links and description fields to stored passwords and shared passwords.
- Added links to open website links from the password recovery page.
- Added copy to clipboard functionality for website links.
- Added validation to website login page for ERPM web service version information.
- Added Web service version information shown on website settings page.
- Added ability for ERPM to automatically drop and re-create views on upgrade.
- Added: Permission checking for chart type panels.
- Added ability to generate a random password to shared credential list page when adding/editing a shared credential (note, this does not set the password).
- Added Copy buttons to most input fields for password recovery/edit in website.
- Added page size controls and data gathering controls for AJAX based web service page data (AJAX Settings).
- Added password generation capability to the personal password store.
- Added support for HP Service Manager version 9.5 to the ticket verification integration library.
- Added program option to timeout DCOM discovery if the operation appears like it is going to take more than a specified amount of time (Addresses appearance of hanging jobs).
- Added PDF export to every page in the web application that supports search.
- Added program option to timeout Windows Scheduled Task discovery if the operation appears like it is going to take more than a specified amount of time (Addresses appearance of hanging jobs).
- Added password change job ID to the input arguments to generate new random passwords through the web service.
- Added UpdateLocalPassword commandlet to the Powershell commandlets.
- Added PowerShell module for offline password management: LSClientUpdatePassword.
- Added Web install dialog will change the default values (80 or 443) if the use SSL checkbox is enabled.
- Added Windows system refresh will attempt to capture DNS name information.
- Added account name filter parameter to the web service call to enumerate the stored accounts for a system: /Rest/System/StoredCredentials, QueryTargetInfo_StoredCredentials.
- Added:Web service support for personal password management: /Rest/PersonalCredential,
- /Rest/PersonalCredentials.
- Added new columns to the web application instances dialog to indicate version and port configuration.
- Added automatic registration of web applications to the database when they are run.
- Added Event for password verification report event.
- Added Event for system added to restricted systems dialog.
- Added "Clear Filters" button to "Currently checked out accounts" web page.
- Added Hide/Show filter indicator to "Checked out passwords" web page.
- Added JavaScript check for Google Chrome browsers to disable the Mindterm SSH component on versions of Chrome (42+) as Chrome no longer supports NAPI and Java applets.
- Added audience field to the function that will look up the stored SAML authenticator information to account for scenarios where IDP URI was identical among two or more SAML based authentication servers.
- Added CSRF checks to delegation and settings AJAX calls.
- Added Request access to the list of permissions that are serialized for the web service in the cases for permissions on systems and permissions on accounts.
- Added log message to indicate if compliance reports could not be found in the program database and removed the assert logging for that case.
- Added whitelist input argument detection for multiple input fields in website.
- Added auto-index tuning support for MS SQL 2016.
- Added improved ability for the website operation to website installation dialog to perform a quicker website lookup when it is known the server meets the minimum requirements.

- Added logging and event sink (1022) for database deletion from Console.
- Added controllable website behavior to allow authenticated or non-authenticated access for direct approval/deny links.
- Added ability for job status to display how many machines failed/succeeded in the management console.
- Added ability for Web application to track which users have read which web application messages.
- Added a variable for system names to pre-run job alerts.
- Added the ability for Website access requests to attempt to capture the user's display name (as opposed to account name) for inclusion in request emails.
- Added management set discovery option for AD queries to add systems using CN, dNSName, or another custom attribute.
- Added ability for the individual management set include/exclude elements to be disabled without removing the setting.
- Added PowerShell module for website, web service and zone processor management: LSClientUpdateConfiguration.
- Updated the lookup and data processing routines to keep memory usage lower (in RAM) during discovery operation against domains with several million user objects.
- Updated the location of the Management Set field to the bottom of web page.
- Updated the Windows password change jobs, in the jobs monitor dialog, to indicate the job is for Windows l the same way as all other account types indicated their type.
- Updated the column order of all accounts pages in the web interface to always show the system name or store identifier in the first column.
- Updated the Web app install dialog so it will disable the SSL port settings if an explicit address is used instead.
- Updated the MFA login pages to auto-redirect back to the login page after 5 minutes.
- Updated the account elevation web page to show the job status instead of the job state for elevation jobs.
- Updated the logic for "datetime invalid" check on setting job run schedule.
- Updated the job details and log pages so it will allow users to see the details for jobs that they own.
- Updated the Cancel buttons in the web application to execute a browser "back" action instead of navigating the user to "manage.asp".
- Updated shared credential list pages to show all options immediately on load.
- UPdated SQL Server password update jobs to always use stored passwords for accounts used to connect to the database.
- Updated the Web application installation dialog to use the FQDN system name for local system web application installations.
- Updated the default visibility of the search fields to be shown instead of hidden when web pages are first loaded.
- Updated the maximum elevation duration for arbitrary elevation to 87,600 hours (3,650 days).
- Updated the Add/Edit password in web interface to fail if the management set name specified does not exist.
- Updated the Verbose logging so it is no longer enabled by default for website (browser side).
- Updated the Mindterm SSH Java component to version 4.1.9 (Java compatibility problems verified, resolved through Java 1.8 u111).
- Updated the Mindterm SSH Java component signing certificate.
- Updated disabled jobs to stay disabled instead of being re-enabled when configured to "Run job on new systems added to the management set" and new systems get added to the management set.
- Updated the HP Service Manager integration to use the HPSM 9.2 method for checking login access.
- Updated DNS calculation code to account for short system names.
- Updated ERPM not to log and continue rather than error when stored DNS system names have an improper format.
- Updated ERPM so it no longer records the bad data as the "DNS Name" when a name lookup returns an IP address instead of a DNS name.
- Updated the Managed password page to show which username a password is checked out to.
- Updated the Managed password page to hide all actions to secondary users if the target account is checked out to another user.

- Updated the physical location of the error page and updated internal references to prevent pen test suites from incorrectly calculating root directories.
- Updated additional validation for user defined default logon pages in web application "User Settings" to help prevent against bad page input (on logon).
- Updated HSM integration code for better error handling and multi-threaded access.
- Updated HSM dialog code to prevent the need to restart the application when HSM is forcefully configured with bad non-working settings.
- Updated .Net 3.5 SP1 to only be required for PeopleSoft Integration.
- Updated Web Service to be a requirement for the ERPM website to function (changes security considerations when web service and website are hosted on different systems or accessed with different names).
- Updated the Console initialization routine to avoid situations which could result in a deadlock issues with Microsoft's Winsock.
- Updated the SSH System Key information to be hidden by default in the SSH key view to better highlight user related keys.
- Updated the default SQL Server index defragmentation timeout up to 300 seconds (and added internal option to control timeout as needed).
- Updated all DLL version information to reflect the current build.
- Updated all EXE files with code signing certificate.
- Updated all SSH session information so it is always hidden - even in verbose logging, even when failures occur. Option must be enabled to explicitly turn on session logging (Logging.LogMessagesWhichMayContainSensitiveInformation).
- Updated the behavior for launching applications so it no longer uses implicit permissions; identity must now be granted "view account".
- Updated the organization of the user session configuration page.
- Updated .Net 4.5.2 to be required for all ERPM default components.
- Resolved an issue with Web service response not including SAML data for authentication servers in authenticator type enum, causing serialization problems (/REST/Config/Authenticators, config_GetAuthenticators).
- Resolved an issue with logic in account pooling configuration dialog that would cause enable/disable edits to the account pooling settings to be ignored on job edit.
- Resolved an issue with various internal code improvements.
- Resolved an issue with website login routine related to error handling unexpected cases (explicit user with no stored identity).
- Resolved an issue with LDAP error handling when the LDAP provider doesn't return an error but the target server does.
- Resolved an issue with logging message for account elevation operations in the database.
- Resolved an issue with a Windows account type filter that was not working in website.
- Resolved an issue by adding a missing table into the auto creation statement to support group membership reporting.
- Resolved an issue with the direct approval links page.
- Resolved an issue with Web application installations not using the default system path as the destination would incorrectly use a blank destination root, causing file copies to fail.
- Resolved an issue with the Key label variable to the web service/PowerShell for password Changed: job settings.
- Resolved an issue where the Xerox printer stored password entries would show up in the password list (passwords can't be recovered if not allowed, just row is displayed).
- Resolved an issue where IPMI devices edited through the web service would not correctly save the option to use the stored password.
- Resolved an issue with the password import dialog incorrectly using the Sybase textual hints for importing custom account store passwords.
- Resolved an issue with the password generation settings did not save settings correctly when called via web service/PowerShell.

- Resolved an issue with System types for windows being incorrectly identified and affecting the "abort password if checked out" option.
- Resolved an issue with the exported key data not being properly formatted in all cases.
- Resolved an issue with the job display filter settings not updating correctly when the last result filter was changed.
- Resolved an issue with extra HTML and doctype tags being added to the custom content panels.
- Resolved an issue with the Console collapsing the "un-categorized" and "explicitly categorized" system nodes during an interactive refresh to prevent memory related crashes.
- Resolved an issue with jobs scheduled to run monthly not correctly scheduling or rescheduling, causing ERPM to continuously loop the job run.
- Resolved an issue with the automatic logout redirection logic when integrated windows authentication AND auto-login is enabled, which would redirect to a bad page on auto-login after session timeout.
- Resolved an issue with deleting scheduled restrictions in the console not removing the scheduled restriction references used for reporting.
- Resolved an issue with various spelling errors.
- Resolved an issue with the Passwords page not displaying passwords of unknown types.
- Resolved an issue with various display issues (field sizes, etc.).
- Resolved an issue with default deferred processors ignoring any specified job affinity flags during retry operations.
- Resolved an issue with not all event sinks being triggered during a "test output" operation.
- Resolved an issue with Favorite links possibly not saving correctly.
- Resolved an issue with Website debug logging flags not being honored (browser side).
- Resolved an issue where a refresh of Salesforce users would return only the first 25 user accounts.
- Resolved an issue with delegation changes made through web service also being reflected in the permissions reporting dialog.
- Resolved an issue with errors caused by trying to delete scheduled restrictions associated with a certificate.
- Resolved an issue with an initialization problem with the delegation account filter in the website.
- Resolved an issue with a broken cross site scripting problem in the LaunchApp.asp page.
- Resolved an issue where the automatic website registration recorded COM Identity as a simple name rather than fully-qualified name.
- Resolved an issue with incorrect event sinks triggered during ticket verification success and failure.
- Resolved an issue where the Event sink for password expiration triggered immediately on password checkout (did not affect actual checkout).
- Resolved an issue where low-powered users could not see custom account store accounts in the web application.
- Resolved an issue where a user refresh of Azure AD only captured the first 100 returned users during a directory refresh.
- Resolved an issue where the Web application removal would fail to delete the COM related files if they were installed to a custom location.
- Resolved an issue with potential CSRF and XSS attack vectors.
- Resolved an issue with potential encoding vulnerabilities.
- Resolved an issue with XSS finding regarding password list names and comments.
- Resolved an issue with all instances of DateTime so now they are all nullable in the web service to avoid JSON serialization errors when converting DateTime.MinValue to timezones ahead of UTC.
- Resolved an issue where the Website would stop triggering event sinks after a period of usage, idle time, or number of calls.
- Resolved an issue where the Management set update code would not correctly add un-classified systems to uncategorized systems node.
- Resolved an issue with ERPM DP/ZP logging into DB with every tick of the sleep counter.
- Resolved an issue where the Shadow account dropdown menu was missing from some account types in the website.
- Resolved an issue with SSH key data not being properly decrypted when changing encryption keys when using an HSM.

- Resolved an issue with the last refresh time for Linux/UNIX systems not being captured during system refreshes.
- Resolved an issue where the Web Service test utility could remove SSL binding when certificate due to bad parsing.
- Resolved an issue where the Console would log errors when opening Clustered Services Configuration dialog.
- Resolved an issue with SAML/ADFS certificates that did not work when the size larger than 2048 bits.
- Resolved an issue where a String replacement propagation on a Linux/UNIX host using a low powered user would incorrectly prepend the password of the low power user being used to run the job at the top of the file in addition to performing the configured change.
- Resolved an issue with Network Scanner not scanning for MS SQL Instances when included with other system types.
- Resolved an issue with Network Scanner not saving discovered SQL port or instance settings.
- Resolved an issue with Network scanner attempting an SSH scan of a Windows system even when SSH was not selected.
- Resolved an issue where a job owner who is not an all access user would receive errors when launching a job from the website, although the job did actually run.
- Resolved an issue where a first run of any operation against a CLR based account store (cloud items and ESX) would cause the ERPM MSI installation routine to begin (non-fatal).
- Resolved an issue where renaming an account store did not properly migrate discovered information to the new name.
- Resolved an issue with Management set updates able to cause logging errors and DB timeouts when several million systems were refreshed over time.
- Resolved an issue with Management set updates able to create bad Parent GUID associations resulting in errors in the logging pane and text log.
- Resolved an issue with a potential parsing error during Linux/UNIX refresh of SUDOERS file information.
- Resolved an issue with the SSH Key data being saved to incorrect fields in the database, and in some situations resulting in loss of private key information.
- Resolved an issue where Scanner settings could be lost on configuration dialogs if user hit the back button.
- Resolved an issue with Website text log logging: Image File Execution Options key exists for application file; execution may be modified (no functionality effect).
- Resolved an issue with AppPerf Control Diagnostic log not being created when enabled.
- Resolved an issue where DP/ZP would log line break HTML characters in logging messages.
- Resolved an issue where turning off ticket verification option in website settings page did not actually turn off the setting.
- Resolved an issue where Arbitrary Account Elevation "Schedule Elevation for a Future Time" would remain enabled on account elevation jobs even though explicitly disabled.
- Removed Klingon and Elvish as translatable languages.
- Updated jquery, bootstrap, and other libraries to newer releases.
- Resolved an issue where the first run of any operation against a CLR based account store (cloud items and ESX) would cause the ERPM MSI installation routine to begin (non-fatal).
- Resolved an issue where renaming an account store did not properly migrate discovered information to the new name.
- Resolved an issue with Management set updates able to cause logging errors and DB timeouts when several million systems were refreshed over time.
- Resolved an issue with Management set updates able to create bad Parent GUID associations resulting in errors in the logging pane and text log.
- Resolved an issue with potential parsing error during Linux/UNIX refresh of SUDOERS file information.
- Resolved an issue where SSH Key data was saved to incorrect fields in the database in some situations resulting in loss of private key information.
- Resolved an issue where Scanner settings could be lost on configuration dialogs if the user hit the back button.
- Resolved an issue with the Website text log logging: Image File Execution Options key exists for application file; execution may be modified (no functionality effect).
- Resolved an issue with the AppPerf Control Diagnostic log not being created when enabled.

- Resolved an issue with DP/ZP would log line break HTML characters in logging messages.
- Resolved an issue where turning off ticket verification option in website settings page did not actually turn off the setting.
- Resolved an issue where Arbitrary Account Elevation "Schedule Elevation for a Future Time" would remain enabled on account elevation jobs even though explicitly disabled.
- Removed Klingon and Elvish as translatable languages.
- Updated jquery, bootstrap, and other libraries to newer releases.

Version 5.5.2.1 (June 6, 2017)

- Enterprise Random Password Manager (ERPM) re-branded to Rapid Enterprise Defense Identity Management (RED IM).
- New Feature: Disconnected Account Management for management of disconnected system's privileged accounts.
- New Feature: VeriClouds Identity Verification Integration.
- Added Install Web Service button to the web application installation page that launches the web service installer on the local system.
- Added Server DNS name support for Radius 2 factor settings.
- Added Google OAuth support for logins.
- Added Enabled Facebook OAuth support for logins.
- Added SAML Login support for PowerShell (Get-LSLoginSAMLToken).
- Added SAML Login support for SOAP (DoLoginSAML).
- Added SAML Login support for REST (LoginSAML).
- Added account elevation extension cmdlet for PowerShell (Set-LSJobAccountElevationExtension).
- Added account elevation extension API for SOAP (JobOps_SetJobElevationExtension).
- Added account elevation extension API for REST (Job/WindowsElevation/Extend).
- Added list filter and max count to the shared credential delegation dialog in the management console.
- Added paging and filtering to the shared credential list dialog in the management console.
- Added filtering and max results to the web service call to retrieve shared credential lists.
- Added SQL provider selection and encryption settings to managed SQL Server instance account stores.
- Added SQL provider and encryption settings to the SQL account store settings for operations and for PowerShell/web service.
- Added SQL provider and encryption settings to the textual SQL Server import.
- Added paging and caching for viewing of shared credential lists and list contents in the web application.
- Added reporting for Disconnected Account Management password permissions in the management console.
- Added missing permissions to the export/import dialog and mechanisms for permissions on management sets.
- Added settings for the client agent settings (and PowerShell cmdlet Set-LSClientSettings) to configure the use of the current user or local system certificate store for certificate based authentication.
- Added start and end dates to the job log retrieval REST web service API (Job/Logs).
- Added requested time input argument to the web service API call for future password requests.
- Added favorite support for account elevations in the web application.
- Added external account references now returned when calling Get-LSListOfStoredAccountsForSystems (and related web services).
- Added a variable for email templates to capture the user's display name from Active Directory if available.
- Added quick check for web application deployment to validate IIS components rather than full windows server validation.
- Added SSH connection options for management of SSH targets to control retry, retry delay and timeout.
- Added ability for .Net Config password propagation to support "user", in addition to the previous "Uid" and "User ID".

- Added ability for the zone processor dialog to remember windows size, column width and sort order.
- Updated last password change times appear as local times in the stored passwords page.
- Updated shared credential list edit and view pages to use web service with paging and caching.
- Updated the Windows Integrated Authentication checkbox on web application login page so it will show as disabled instead of hiding if integrated auth is enabled but not possible.
- Updated the Delete/Remove panel behavior in the web application so it will delete by panel ID instead of name.
- Updated the stored credential dialog so it will not to show the namespaces in the drop-list if displaying shared credential lists.
- Updated the website update function so it will allow blank values (to facilitate setting values back to defaults).
- Updated the default chart generation behavior for group size so it will not save data if there are no systems in management sets.
- Updated the default chart generation code so it will replace older saved versions of chart data instances (as opposed to accumulate).
- Updated the Web application default message panel padding.
- Updated the text of the MFA configuration dialog in the management console to indicate that
- "require MFA" applies to "external MFA" types (requiring MFA will require external MFA for all users).
- Renamed "VMWare" to "VMware".
- Updated the service installation code to always quote the service file path.
- Updated the default client cert and CA generation code to generate keys using SHA256 instead of SHA1.
- Updated the format of the elevation lists page in the web application.
- Updated the password change job so it no longer changes a user's UAC attribute to set
- home_dir_required.
- Updated the order of operations for Active Directory logins to web application that could cause some accounts to not be properly evaluated.
- Updated the node names registered for clustered services management needed to exactly match the target names in the job and now must match any of the discovered systems names (i.e. NetBIOS, DNS, or IP).
- Resolved an issue where importing custom account stores programmatically did not properly configure the account store (COM interop problem).
- Resolved an issue where accounts and systems list menus may not always populate on web service driven pages.
- Resolved an issue with a JavaScript problem related to adding and removing favorites.
- Resolved an issue with automatic registration of web application instances that are in the root of a site.
- Resolved an issue where the account filter field in the jobs dialog of the management console would be ignored in some cases.
- Resolved an issue with empty DNS name not updating the correct web application server's settings.
- Resolved an issue where the file delegation page of web applications may not properly grant permissions.
- Resolved an issue with management set PowerShell and web service management serialization errors.
- Resolved an issue where zone processors configured to run both password verification jobs and jobs that require system sets may not operate as expected.
- Resolved an issue where import files with more than 5 import columns may not properly import via the management console.
- Resolved an issue where replacement arguments in email messages would not be replaced when requesting passwords through the web service/PowerShell.
- Resolved an issue where accounts page for custom account stores would not display if there is a stored password for the account.
- Resolved an issue where users that were enabled for MFA would not be required to use MFA unless it was required for all users' logins.
- Resolved an issue so you can no longer create or delete shared credential lists with empty names. Related: deleting shared credential lists with empty names would also delete all managed passwords.
- Resolved an issue with a delegation identity serialization problem that would cause "require MFA" and "allow remote sessions" to be enabled by default for users created through the web service.

- Resolved an issue where exporting permissions on management sets via the management console would export the data with the wrong settings.
- Resolved an issue with various typos.
- Resolved an issue with a Favorites panel error that stopped the editing of favorites.
- Resolved an issue where the unloading of a legacy/deprecated SDK COM object caused crashing.
- Resolved an issue with string replacement for Linux/UNIX propagation not working when authenticating with a low powered account using an SSH key.
- Resolved an issue where account pooling would attempt to always change next account value into a UPN value.
- Resolved an issue where account pooling was not properly defining COM+ account during next account rotation.
- Resolved an issue with Web service tester not working on Windows Server 2016.
- Resolved an issue where the Application Launcher installer would not run successfully on Windows Server 2016.
- Resolved an issue with job priority settings not being honored.
- Resolved an issue where enabling MFA options via web application was not actually configuring the required delegations.
- Resolved an issue where failures on pre-run execution steps that failed were not properly incrementing the job fail counter, causing the jobs to enter a continuous processing loop.
- Resolved an issue where using "Run Now..." for App Data Store Maintenance task would remove all systems.
- Resolved an issue where the App data store maintenance operation did not remove permissions on management sets for identities that no longer exist.
- Resolved an issue where Account Stores based on CLR code could enter a race condition causing 100% CPU utilization. Typically, this was witnessed when managing ESX hosts on the VMware ESX node.
- Resolved an issue with the Jobs dialog not properly applying an account name filter to list control.
- Resolved an issue where a refresh of Linux systems with mapped SSH keys loaded the key and attempted a connection twice.
- Resolved an issue with Host Key connection data being displayed as orphaned keys in SSH Key View.
- Resolved an issue where Postgres database password change jobs could fail due to improper name character casing.
- Resolved an issue with Report output for management sets from management console showing incorrect "Run By".
- Removed the Log message generated by web application for failed MFA settings if MFA has not been initialized.
- Updated the PowerShell cmdlet support for strong crypto using TLS 1.1 and TLS 1.2 secured connections.
- Updated the Default response file tester utility test files with updated files.

Version 5.5.2.2 (August 1, 2017)

- Added a search filter to the settings page in the web application.
- Added a search filter to the user session page in the web application.
- Added a search filter terms to the free-form password search panel.
- Added the ability to click on a shared credential list name to set and apply the password list filter argument.
- Updated the VeriClouds fields so they are now password fields rather than text fields.
- Updated VMware ESX nodes so they can manage accounts other than Administrator level accounts.
- Updated the Web application registration for the management console to avoid duplicate site registrations.
- Updated the web application authorization process to perform SID lookups to improve logon performance in large enterprises.
- Resolved an issue with the schema lookup code for data store configuration that prevented non-sysadmin level users or non-DBO users assigned permissions solely via group memberships from being able to use the management console.
- Resolved an issue editing shared credentials.

- Resolved an issue with inability to edit or display disconnected account information or settings when using Internet Explorer.
- Resolved an issue with inability to set propagation settings via web service/PowerShell.
- Resolved an issue with inability to set propagation scope via web service/PowerShell
- Resolved an issue with inability to configure a job to target a management set when creating/editing a job via web service/PowerShell.
- Resolved an issue with password generation settings not encrypting a statically specified password.
- Resolved an issue with shared credential list edit comment field not being edited in all expected situations.
- Resolved an issue with the MySQL accounts page not properly applying the account name filter for known passwords when clicking the link to show stored passwords.
- Resolved an issue with the add and delegate controls for shared credential lists in the web application not displaying in all expected situations.
- Fixed: Salesforce account password updates failed due to updated APIs requirements from SFDC (unclosed stream).
- Resolved an issue where Azure AD password management could fail could cause password updates to fail.
- Resolved an issue where SalesForce password changes could fail for accounts that were not returned in the first page of results from SalesForce.
- Resolved an issue with form validation in the arbitrary elevation lists page.
- Resolved an issue with diagnostic data serialization for account stores based on the AccountStoreCLR framework (AAD, SFDC, SoftLayer, Rackspace, and ESX).
- Resolved an issue with Application Launcher compiled in wrong format, causing 64bit applications to not launch.
- Updated Jquery to version 3.2.1.
- Updated DevExtreme to version 17.1.4.

Version 5.5.3.0 (December 19, 2017)

- Added "Do not delete" flag for jobs.
- Added caching for filter values to the stored passwords dialog.
- Added DUO MFA for web application.
- Added self-elevation account elevation feature and associates self-elevation delegations.
- Added import/export for self-elevation permissions to the management console.
- Added self-elevation web service APIs (Delegation/SelfElevation, DelegationOps_SetSelfElevationPermission, DelegationOps_DeleteSelfElevationPermission, DelegationOps_GetSelfElevationPermissions, Delegation/SelfElevationCurrentUser, DelegationOps_GetSelfElevationPermissionsCurrentUser).
- Added self-elevation PowerShell cmdlets (Get-LSListDelegationPermissionsForSelfElevation, New-LSDelegationPermissionForSelfElevation, Remove-LSDelegationPermissionForSelfElevation).
- Added custom account store account list to the web service APIs (System/Accounts/Custom, AccountStoreOps_GetAccountListCustom).
- Added custom account store account list PowerShell cmdlets (Get-LSListCustomAccountsForStore).
- Added support for application launcher to use custom account store accounts.
- Added delete button to the message template dialog.
- Added hidden application option to limit the number of custom web panels that can be created, defaulted to enabled and set to 10.
- Added web application option to control if the web content (panels/templates) can be created and edited.
- Added Disconnected Account Management options and settings for machines that will never connect to the system in web application.
- Added Disconnected Account Management added a new column for off-line system status.

- Added explicit notion of off-line always (indicated by magic value for secret renew time of 8760000 hours i.e. 1,000 years).
- Added account comment field to the managed password recovery/view page.
- Added account comment field to the personal password recovery/view page.
- Added string truncation to the personal password store's list view (300px).
- Added support for password history for shared credentials.
- Added unique password client-side encryption/decryption for personal passwords.
- Added unique password client-side encryption/decryption for shared passwords.
- Added system name field to personal passwords store.
- Added popup error message if adding an account of the same name in the Personal Password Store.
- Added session based master password feature for personal password store and web interface.
- Added website link and description added to the list of fields that can be imported when importing shared credentials via textual import.
- Added website link and description to the import dialog fields for shared credentials.
- Added ability to create favorites for specific personal passwords in personal password store.
- Added browser specific functionality to attempt to make password fields more difficult to copy to the clipboard when Copy to Clipboard functionality is disabled.
- Added sort chevrons for last change time, system name, and account name to personal passwords.
- Added several event sinks for remote application operations (session start, session end).
- Added favorites links and favorites support for personal passwords.
- Added ability to export the database settings from the console using the command line switch
- "/GenerateConnectionSettings".
- Added ability to run jobs on management sets for all types of refresh and password change jobs.
- Added comment filter to the deferred job display dialog.
- Added MRU list for comment filter field for job display dialog.
- Added description to the deferred processor when the console installs it.
- Added code to translate content ad-hoc for web service dynamic (asynchronous) content.
- Added log message when an authentication server is automatically added in the default domain into the list of authentication servers.
- Added URL and description for managed passwords.
- Added Date Last Set time for Shared Passwords.
- Added time zone controls (Program Settings) to better handle distributed installations for scheduling job runs with zone processors.
- Added JSON data export utility to support data and data store migration.
- Added support for direct ODBC usage for data access to prepare for OLEDB deprecation in Microsoft SQL Server.
- Added experimental (currently unsupported) support for MySQL database as a back-end data store.
- Added support for Windows Server 2016 scheduled task discovery and propagation.
- Added support for hosting Application Launcher on Windows Server 2016.
- Added support for hosting web application and web service on Windows Server 2016.
- Added Smart Key Labelling to automatically label SSH keys.
- Added individual passwords in password history are now masked until shown.
- Added support for importing additional key types (DSA, EC and ED).
- Added support for SSH key creation of type RSA and EC.
- Added support for SSH key archiving (during delete operation).
- Added support for SSH archive key restoration.
- Added SSH Public key derived automatically from imported or discovered Private Key.
- Added SSH key mapping support post SSH key import.
- Added additional SSH key file metadata information (e.g. SSH key age) to SSH key view.
- Added SSH key filtering options for SSH key view.
- Added SSH key update support for key types other than RSA (DSA, EC and ED).

- Added additional SSH key rotation operations.
- Added SSH Key pass phrase pre-seeding option to auto-import SSH keys with pass phrases during key discovery operations.
- Added additional views to Sudo permissions view dialog to help identify users, groups, and assigned permissions.
- Added support to better visually identify specific Linux/UNIX/OSX distributions.
- Added support to better handle later versions of OSX during password management operations.
- Added Linux/UNIX/OSX account scan rules to help filter out system accounts from the account store view.
- Added Per-Host SSH port configuration.
- Updated Fields on Managed, Shared, and Personal Passwords now reflect similar naming structure.
- Updated account type filters (admin/root/etc.) are now saved with favorites.
- Updated installation path of deferred and zone processors that are pushed via management console will now be double quoted.
- Updated shared credential list behavior so that when a list is selected but empty, it will be clearer to users.
- Updated Web application installation routine will attempt to clear the default document before setting it to login.asp to overwrite any parent level default document settings.
- Updated template editing code to only allow editing of email templates with known types.
- Updated max length to the favorite comment. Default is 32 characters (WebLimits_LimitFavoriteCommentLength).
- Updated max number of favorites per user. Default is 32 characters (WebLimits_LimitFavoriteCount).
- Updated panel delete operations to work on IDs rather than names to avoid potential collision during delete operations.
- Updated deleting a shared credential so it will now return user to the list of shared credential lists.
- Updated User Session Settings verbiage for panels changed from Charts - X to Display Charts - X for session info in web interface.
- Updated when selecting a hyper-link for an account from the personal password store so you will be taken to a new tab.
- Updated the Personal Password Store Filter to filter on account name and system name.
- Updated logic of the shared passwords list navigation menu to show all lists the current user has any permissions for.
- Updated magnifying glass icon to the filter icon in the web interface for web application filters.
- Updated verbiage in Disconnected Account Management feature from "tenant" to "list".
- Updated column order of the accounts page to be consistent with other account pages.
- Updated Disconnected Account Management global config/add/edit to require unique names for systems/configs.
- Updated Disconnected Account Management OS type detection for icon association to be case insensitive.
- Updated Disconnected Account Management input fields to dis-allow lists/tenants with the same name for off-line password management.
- Updated viewing of managed passwords so it no longer requires separate "View Accounts" permission.
- Updated password recovery pages hide the copy button (lower left) when password field is shown and has the copy password button available.
- Updated verbiage for delete account/password to indicate the entire entry will be removed, not just the password
- Updated personal password filters will be reset once the user leaves the personal password area.
- Updated default behavior for "enter" on the Radius login page to submit the form.
- Updated default zone processor installation path to be the local program installation path.
- (required for CLR integration components).
- Updated the dropdown width of the combo boxes in the deferred jobs display dialog.
- Updated PowerShell cmdlet to use the web service to get the current website settings rather than local registry.
- Updated the display of disabled text input fields to help avoid user confusion.
- Updated Vericlouds verification functionality to fail and allow login if Vericlouds service cannot be reached.
- Updated custom web panel names so they no longer contain non-alphanumeric characters.
- Updated Authentication Server connection evaluation to improve login performance.
- Updated AWS integration so that updating root access API keys works in-line.

- Updated filters to no longer be hidden from view in web application.
- Updated Run-as password field in the advanced launch application pages in web application to be a password field.
- Updated personal password store enabled for the built-in administrative account.
- Updated Overwrite Permissions warning displayed when importing permissions in the management console to be hidden in cases where the settings are not actually overwritten.
- Updated the System name, now added to the list of fields cached by the password display dialog in the console.
- Updated the Recovery pages to hide phonetic guide if hide passwords security option is enabled.
- Updated SCL import/error messages to correctly indicate column names and requirements.
- Updated SSH Key (Manage User Keys) dialog menus.
- Updated the Import SSH key dialog to specify key type to be imported.
- Updated the auto-generated name for imported SSH key.
- Updated default SSH module to use Java based MindTerm control.
- Resolved an issue with App Data Store Maintenance job last run time not displaying correctly.
- Resolved an issue with App Data Store Maintenance job did not always correctly saving settings.
- Resolved an issue where the continue options were not available when users explicitly copy/pasted OATH token codes into the OATH token field in the login page,.
- Resolved an issue with free-form text search filter on the password panel when specifying account TYPE not working.
- Resolved an issue with Windows accounts page account type filter being ignored.
- Resolved an issue with Smart card redirection for application launcher when connecting with Terminal Services/RDS.
- Resolved an issue with Account store name improperly set to the type during custom account store job creation.
- Resolved an issue with Error message logged when stored passwords were tested individually via management console.
- Resolved an issue with Import of global delegation with management set to lose the management set info.
- Resolved an issue with SQL server instance text import not retaining provider and encryption settings.
- Resolved an issue where the Add operation would appear available on shared credential lists even if it was not allowed based on user permissions.
- Resolved an issue with Delegated permissions to view permissions on shared credential lists not allowing users to see the permissions.
- Resolved an issue with URL encoding during copy operations from the web application.
- Resolved an issue with retrieval of a static password recovery liable to fail when password spin is enabled (default).
- Resolved an issue with Jobs dialog hanging when viewing Delegation Settings.
- Resolved an issue with low powered web accounts and the Windows account page filter settings for system and account filters not always working.
- Resolved an issue with SCL password import via management console incorrectly parsing text file columns.
- Resolved an issue with password display dialog caching error.
- Resolved an issue with low powered users not able to filter account names in the Accounts view of the web application.
- Resolved an issue where modification of permissions on accounts, permissions on systems, permissions on password lists, and permissions on management groups did not affect the flat permission structure, affecting permissions reporting.
- Resolved an issue with filters for system pages not being saved with favorites if AJAX was enabled.
- Resolved an issue with Disconnected Account Management off-line update service not using the symbols specified.
- Resolved an issue with Disconnected Account Management off-line update service installer sometimes failing on first run.
- Resolved an issue where the Web service URI needed to be case sensitive for Disconnected Account Management to work properly in web application.

- Resolved an issue with Favorites in web application not always being saved correctly.
- Resolved an issue with the Web application permissions page showing hex values instead of actual permissions.
- Resolved an issue where MFA could be disabled for some users when it should be enabled.
- Resolved an issue with Input validation errors on the charts page.
- Resolved an issue with password change job add/edit operations via web service improperly encrypting current and login passwords.
- Resolved an issue with the zone processor system query that caused custom account store types (E.g. ESX) not to be run as part of refresh jobs in zones.
- Resolved an issue with the Index defragmentation dialog.
- Resolved an issue where users could potentially add panels to their user settings that don't exist.
- Resolved a Display issue for IIS discovery when multiple root websites were configured with specific anonymous credentials.
- Resolved an issue with various typos.
- Resolved an issue with Type Mismatch Error on SQL index defragmentation.
- Resolved an issue with SSH Key filters not always working as expected.
- Removed Dependency for IIS6 Metabase Compatibility when scanning/propagating for .net configuration file credentials (ODBC data sources).