What's New in Own Secure

To access the package link for installation please find instructions here:
Own Knowledge Base

Secure 25.1 - December '24

- Security Insights risk management & reporting improvements
    - Scoring of individual insights updated to use a linear algorithm and target scores (new) are now automatically calculated based upon changes to threshold configurations. **NOTE:** Org scores will change after update and the execution of a new Security Insights analysis job. Old scores will continue to be available in the Security Insights Time Machine.
    - The dashboard has been updated to reflect lens risks, targets, actual scores, and trend data. Dashboard reports are also updated and now include the ability to download a detailed risk report, summary risk report, and trend data
    - Alerts are now available for each scored insight on the Settings tab
    - Multi-org reporting has been updated to reflect the new scoring and will accommodate mixed version, multi org environments
- Data Classification now includes a guide that interacts with the filter sets feature introduced earlier this year to guide new users through how to classify an org
- Salesforce in app guidance provides an overview of how to use each tab of the Secure application
- The top of the Settings tab has been updated to make it easier to find new version information, help, how to videos, & open a support case
- Saving changes to the Settings tab should no longer cause metadata deployments
- Data Classification
    - Added "Last Classified By" & "Last Classified Date" as optionally viewed columns. These fields are contained in the download and are filterable.

- Who Sees What
    - System Permission lens shows up to 15 users assigned a permission at a time
    - Users lens Compliance Category filter and download column added
    - Users lens added user's profile to the results from the search drop down
    - Object, Users, & Profile/Perm Sets lenses will all display custom fields which are required
- History Retention Policy Manager
    - Added a high risk fields filter

Secure 25.0 - September '24

- Salesforce Winter 25 Compatibility
- High Risk Permissions are now configurable on the Settings tab and can include system permissions, application permissions, & custom permissions. This updates permission-based security insights, permission-based filtering in Who Sees What, and permission-based alert subscriptions.
- Security Insights - Administrative Activities insight: Filter by date range to better support audit evidence gathering.
- Security Insights - Stale Users Insights: Rename to "Stale Internal Users" and filter out Community/Digital Experience, Chatter users.

Secure 24.7 - July '24

- Who Sees What User Lens: Add a user details button which will display username, email, last login, active or not, profile, roles, permission sets, and permission set group assignments.
- Who Sees What User Lens, Object Lens, Profile / Perm Set Lens, System Permissions Lens: Added a filtered view download
- Who Sees What User Lens: Added a field api name column
- Security Insights - Stale Users insight: Added columns for Created Date, Profile. Added Created Date, Profile, & Profile ID to download.
- Security Insights - Users w/o Roles insight: Will only display Active standard users and Partner Portal users.
- Security Insights - Administrative Activities insight and SSO/MFA insight: Added multi-select type ahead search filter to improve filtering capabilities.

- Security Insights - Administrative Activities insight: Added “All Data” & “Filtered Data” csv download capabilities.
- Security Insights - SSO/MFA Usage, Report Access, High Risk Permission Access, Digital Experience Sharing, Digital Experience Access to High Risk Permissions insights: Add the ability to specify a 100% allocation for score weighting.
- Security Insights-Users with View Setup & Configuration, Users who can Modify All Data, Users who can Export Reports, Users with API Access, Users who can Subscribe to Reports, & Users who can Perform Weekly Data Export Insights: Update text displayed to clarify that these insights are a % of both internal and external users.

Secure 24.6 - May ‘24

- Salesforce Summer ‘24 compatibility
- Who Sees What Users lens refresh including: compare capability, object CRUD, field level security, effective access, enhanced filtering, and enhanced reasons for access screen.
- Introduction of classification filter sets to ease classification efforts. Includes default sets and the ability to create custom filter sets which can be used across orgs.
- NOTE: The following enhancements require a new Security Insights analysis job to be run after the upgrade to Secure 24.6
    - Unencrypted Settings insight will show settings with *id* in their name
    - High Risk Permission Access insight adds a flip when a permission is selected. The flip will show profile or permission set names that are assigned the permission (with deep links to setup), the type (profile or permission set), the internal user count, and the external user estimate.
    - Objects Open to Deletion insight adds a flip when an object is selected. The flip will show profile or permission set names that are assigned the permission (with deep links to setup), the type (profile or permission set), the internal user count, and the external user estimate. Flip information is exportable from the insight.
    - Unstored Event Types insight has been updated with a new method to show which events have not been configured for storage.

Secure 24.5 - April ‘24

- Security Insights Read Only mode for users with Salesforce Standard User or Read Only User profile equivalents.

Secure 24.4 - March ‘24

- Additional updates for Salesforce Spring ‘24 Compatibility
- Security Insights job handling and time machine enhancements

Secure 24.3 - January ‘24

- Improved visibility of Security Insights completed job status, errors, and scoring policy changes.
- Data Classification filtering additions (Fields w/No Records, External Objects)
- Settings Policy Wizard, new tabs added to import summary screen
- Salesforce Spring ‘24 Compatibility

Secure 24.2 - November ‘23

- WsW Object Lens refresh including: display of both data access assignments & net effective access, enhanced searchable filtering, multi-select, and comparison capabilities.
- Various minor updates to the recently released Digital Experience security insights.

Secure 24.1 - October ‘23

- New scored Security Insights: Digital Experience High Risk Permissions, Digital Experience Access to High Risk Fields, & Digital Experience Sharing

Secure 24.0 - September ‘23

- Platform Encryption Exclusion tags
- Salesforce Winter ‘24 Compatibility

Secure 23.9 - August ‘23

- Exclude fields from Platform Encryption Analyzer wish list.
- Security Insights Scoring - Event Bus defaults based on org configuration & score bar guidance updated

Secure 23.8 - July ‘23

- Security Insights Configurable Scoring (*Note: This update will cause your Security Insights scores to change*)
- Data Classification Enhancements: “Fields Modified Since” filter, Add / Remove Data Owner, Field Durable ID added to export, remove classification dependency on sensitivity level.
- WsW Multi Object Download Enhancements: Improve column sorting, improved search
- WsW Profile Compare Enhancements: Column alignment, session-based access display improvements, new Object access filter, new system permission assigned filter

Secure 23.7 - May ‘23

- Salesforce Summer ‘23 Compatibility
- Who Sees What - Profile / Perm Set / Perm Set Group Compare
- Who Sees What Object Lens - Multi Object Download
- Security Insights MFA/SSO Insight add filter for integration users (API access only, interactive access not allowed)
- Security Insights Report Access Insight adds a column for Subscribe to Reports
- Who Sees What System Permission Lens “High Risk” column added to download
- Who Sees What Profile / Perm Set / Perm Set Group lens made iconography more clear
- Who Sees What User Lens, check “Can Read” & “Can Edit” even if access is only derived from a session-based permission set.
- Alerting sort High Risk System Permission alerts alphabetically
- Alerting for email alerts display user first name, last name, & alias

Secure 23.6 - April ‘23

- High Risk Permission Assignment Alerts
- Field Description & Help Text are searchable in Data Classification & Platform Encryption Analyzer
- Security Insights, Unencrypted Settings insight adds explanatory hover text on “Analysis Results” column

- Security Insights, MFA/SSO insight graph shows green only for MFA logins, all other types are red
- WsW User & Profile / Permission Set lenses updated display & handling of muted perm set information & session based perm set information

Secure 23.5 - March ‘23

- New Who Sees What Lens, Profiles & Permission Sets
- Banner notification of Secure update availability
- Outbound Messages Security Insight includes sensitive field information
- Removing field classification (sensitivity, compliance categorization, data owner, or usage) in Secure will remove from Salesforce metadata on sync to Salesforce

Secure 23.4.1 - February ‘23

- Show field description & help text in Data Classification, Platform Encryption Analysis modules. Show field description in WsW field hover text.
- Show current version, released version on Appexchange, enable in app update.
- Update Change Data Capture Security Insight to show objects with sensitive fields
- Add encryption type details to Platform Encryption Analysis download
- Add Sarbanes Oxley as a default compliance category for data classification

Secure 23.3 - January ‘23

- Salesforce Spring ‘23 Support
- Add a flip icon to each Security Insight that is two-sided
- Relax DC Policy Migration file naming validation
- Enhance tooltips on the Settings tab

Secure 23.2 - December ‘22

- Insight Risk Language: Update all Security Insights to provide information regarding what Secure is finding, what’s the risk of the finding, and what we generally see in our Customers through services engagements. This feature is intended to foster improved conversations between Infosec and Salesforce Administrators regarding risk.
- Risk Weighted Scoring: Customer configurable risk ratings for all Security Insights, which ties directly to the scoring seen in Security Insights. This feature is intended to enable Customers to better tailor Security Insights scoring to the actual risk operating context of the org(s) running Secure.
- Add "# of High Risk Fields" to the SI widget "Objects Open to Deletion"
- Include the filled records and total records values in the CSV for DC
- Enhancement to bulk classify: Notify user the job is still running

Secure 23.1 - November ‘22

- New Security Insight: Objects That Should Be Monitored. For those Customers who licensed Salesforce Shield Event Monitoring, or are considering it, one significant implementation challenge will be in determining what to monitor. This new insight combines the following information to enable a focused Shield EM implementation:
    - Fields identified during data classification as sensitive or high risk.
    - Field usage using fill rate analysis
    - % Field accessibility by the user community
- Update the text displayed when there are issues with Users accessing Secure to be more explicit/helpful.
- Free up screen real estate to enable viewing of more app content by removing title divs

Secure 23.0 - September ‘22

- Salesforce Winter ‘23 Support
- Update how LightningLogin is categorized within SSO/MFA insight