

User Manual

Aptean Food and Beverage ERP

eSignature

Product Documentation



Contents

- [Release notes](#)
 - [2603.0.0.0](#)
 - [2602.0.0.0](#)
 - [2601.1.0.0](#)
 - [2601.0.0.0](#)
 - [2502.1.0.0](#)
 - [2502.0.0.0](#)
 - [2501.1.0.0](#)
 - [2501.0.0.0](#)
- [Introduction](#)
- [Setup](#)
 - [Manage permission sets](#)
 - [Set up e-signature configuration](#)
 - [Configure Two-Factor Authentication](#)
 - [Set up delegate groups](#)
 - [Set up e-signature user groups](#)
 - [Configure compliance locations](#)
- [Manage vendor status log](#)
- [Manage e-signature requests](#)
- [View e-signature request entries](#)
- [View completed signatures](#)
- [Set up production scenarios](#)
- [Manage item audit trail](#)
- [View e-signature snapshots](#)
- [View routing snapshot history](#)
- [View production BOM snapshot history](#)
- [View production scenario snapshot history](#)
- [Generate audit report for production order](#)
- [Set up BOM](#)
- [View deviation](#)
- [Use e-signature in a production order](#)
- [Manage batch record](#)



Filter eSignature snapshots	
View snapshots in treeview format	
View eSignature entries from production BOM	
View eSignature entries from routing	
View eSignature entries from production scenarios	
Generate reports from enhanced XML snapshots	
Monitor pending pre-weigh verifications	
Review pending pre-weigh verifications	
Approve pre-weighed ingredients	
Approve multiple pre-weighed ingredients	
View verification audit trail	
Search verification history	
View blocked posting attempts	
Reject a pre-weighed verification line	
Batch reject verification lines	
Integrations	
Aptean Advanced Attributes	
Aptean Approved Supplier	
Aptean Status Management	
Aptean Audit Trail	
Aptean Compliance Documents	
Aptean Filter Group	
Aptean Inspection Status	
Aptean License and Subscription Management	
Aptean Non Conformances	
Aptean Process Manufacturing	
Aptean Production Scenarios	
Aptean Quality Control (BC)	
Aptean Vendor Item Catalog	



Release notes

Article • 7/22/2026 • 1 min read

To view what's new or changed in each release of the Aptean eSignature extension, select the specific release version.

Date	Release version	Description
July 2026	2603.0.0.0	Major release
April 2026	2602.0.0.0	Major release
March 2026	2601.1.0.0	Stability release
January 2026	2601.0.0.0	Feature release
November 2025	2502.1.0.0	Stability release
October 2025	2502.0.0.0	Feature release
September 2025	2501.1.0.0	Platform release
August 2025	2501.0.0.0	Initial release



2603.0.0.0

Release Note • 7/22/2026 • 1 min read

Enhancements/Modifications

With this release of the Aptean eSignature extension, the extension no longer requires the Aptean Formulation Management extension. The **Pending Status Change To** field and the delete protection for status-managed records are now handled through the Aptean Status Management Integration Layer extension, so eSignature can be deployed independently of Formulation Management.



2602.0.0.0

Release Note • 4/22/2026 • 4 min read

Features

With the features added in this release of the Aptean eSignature extension, you can:

- You can monitor pending pre-weigh verifications through a new **Role Center** cue that displays the real-time count of eSignature scan entries awaiting second-person verification, with color-coded visual indicators and direct navigation to the **Component Verification Workbench**. For more information, see [Monitor pending pre-weigh verifications](Monitor-pending-pre-weigh-verifications.md).
- You can review and process pending pre-weigh verifications through the **Component Verification Workbench**, a centralized list page displaying production order components requiring verification with filtering, a **FactBox** showing lot-level eSignature scan entry details, and support for approving or rejecting entries directly from the workbench. For more information, see [Review pending pre-weigh verifications](#).
- You can approve a single pre-weighed ingredient line using electronic signature, with credential validation against the user database, automatic recording of the approver's user ID, full name, and timestamp, and an immutable audit trail entry for compliance. For more information, see [Approve pre-weighed ingredients](#).
- You can select and approve multiple pre-weighed ingredient lines with a single electronic signature using multi-select, with all selected lines receiving the same timestamp and approver information, individual audit trail entries per line with a batch reference, and full atomicity ensuring that if any line update fails the entire batch is rolled back. For more information, see [Approve multiple pre-weighed ingredients](#).
- The system now automatically captures every verification approval and rejection event through the Aptean eSignature framework into an immutable, write-once audit log with sequential record IDs, including verifier identity, timestamps, item details, lot numbers, and weights, with bi-directional drill-down navigation from posted warehouse activity lines and item ledger entries to the corresponding verification records for full traceability. For more information, see [View verification audit trail](#).
- You can search, filter, and export verification history through a centralized read-only **Verification History** inquiry page, with filters by date range, action type, verifier, item, lot, production order, and posted status, support for export to Excel, PDF, or CSV, and a **Batch Release Report** that can be generated and attached to the production order for enhanced batch documentation. For more information, see [Search verification history](#).
- The system logs every blocked posting attempt when a user tries to post or process ingredients that have not been verified, recording the user's identity, document number, item and lot numbers, weights, and timestamp in a tamper-proof write-once audit log, with the blocked attempt visually distinguished by a red icon in the **Verification History** page and a unique log ID included in the error message for traceability. For more information, see [View blocked posting attempts](#).



- You can reject a pre-weighed verification line by selecting a standardized rejection reason code and entering a comment, with the rejection recorded in the eSignature audit trail, the rejection context stored on the related warehouse pick line for traceability, the line's reject count incremented, and escalation to supervisor review triggered when configured rejection thresholds are exceeded. For more information, see [Reject a pre-weighed verification line](#).
- You can batch reject multiple selected verification lines in a single action with one rejection reason and comment applied to all selected entries, with group-aware cleanup that removes eSignature request entries when all lines in a group are rejected while retaining request context for remaining pending lines in partial rejections. For more information, see [Batch reject verification lines](#).

UI/UX changes

The following UI/UX changes have been made in this release.

- The **Component Verification Workbench** page has been added.
- The **Pick Lines** FactBox has been added to the **Component Verification Workbench** page.
- The **Pending Pre-Weigh Verifications** cue has been added to the Quality Manager Role Center.
- The **Verification Record ID** field has been added to the **Registered Warehouse Activity Line** page.
- The **Verification Record ID** field has been added to the **Item Ledger Entries** page.
- The **Pre-Weigh Verification History** page has been added.



2601.1.0.0

Release Note • 3/25/2026 • 1 min read

Resolved issues

The following issue has been resolved in this release.

ID	Description
361164	The system incorrectly skips the user login prompt when capturing eSignatures, allowing signatures to be recorded without proper user verification and compromising compliance requirements.



2601.0.0.0

Release Note • 1/30/2026 • 3 min read

Features

With the features added in this release of the Aptean eSignature extension, you can create immutable snapshots of certified:

- Production BOMs that capture complete formulation data including all header information, weight unit configuration, component lines, lot attribute requirements, scrap percentages, co-products, and production BOM comments. The snapshot links to e-signature records containing user ID, date, time, and reason for certification, ensuring FDA-compliant audit trails for regulatory inspections. For more information, see [View production BOM snapshot history](#).
- Production scenarios that link items to specific certified BOM and routing versions, capturing item number, production BOM number and version, routing number and version, location code, unit of measure, and all configuration settings. The snapshot includes e-signature records for full audit trail compliance. For more information, see [View production scenario snapshot history](#).
- Routings that capture complete process details including all header data, operation lines with times, operation comments, tools, personnel, quality measures, routing comments, and complete details of all referenced work centers and machine centers. The snapshot includes e-signature records to ensure process validation compliance. For more information, see [View routing snapshot history](#).
- You can filter eSignature snapshots by document type, record ID, record name, date range, user, and status to quickly locate specific snapshot records for compliance tracking and audit purposes. For more information, see [Filter eSignature snapshots](#).
- You can view eSignature snapshots in a hierarchical treeview format that presents data in an organized structure, allowing you to expand and collapse nodes to analyze complex data relationships. For more information, see [View snapshots in treeview format](#).
- You can access eSignature entries directly from the **Production BOM** page without navigating away from your current work. For more information, see [View eSignature entries from production BOM](#).
- You can access eSignature entries directly from the **Routing** and **Routing Version** pages to review certification history and approval workflows. For more information, see [View eSignature entries from routing](#).
- You can access eSignature entries directly from the **Production Scenario** pages to review certification and approval information. For more information, see [View eSignature entries from production scenarios](#).
- The system has enhanced XML snapshot data to include field ID, field name, table ID, and table name metadata, enabling report data designer to dynamically generate datasets without hardcoding field structures. For more information, see [Generate reports from enhanced XML snapshots](#).



- This extension has been updated to ensure interoperability with the recent changes in the Aptean Report Data Designer extension. To know more, see [What's new in Report Data Designer, version 2601.0.0.0](#).

UI/UX changes

The following UI/UX changes have been made in this release.

- The **Show Snapshot** action and the **Snapshot History** FactBox have been added to the following pages:
 - Production BOM
 - Production Scenarios
 - Routing
- The **Show Snapshot** action has been added to the **eSignature Entries** page.
- The **Certified Production BOM History**, **View eSignature Entries**, and **Pending Status Change To** actions have been added to the **Production BOM** page.
- The **Certified Production BOM History** action has been added to the **Production BOM List** page.
- The **Pending Status Change To** field, **Certified Routing History**, and **View eSignature Entries** actions have been added to the **Routing** page.
- The **Certified Routing History** action has been added to the **Routing List** page.
- The **Pending Status Change To** field and **View eSignature Entries** action has been added to the **Routing Version** page.
- The **Pending Status Change To** field, **Certified Production Scenario History**, **View eSignature Snapshots**, and **View eSignature Entries** actions have been added to the **Item Production Scenarios** page.



2502.1.0.0

Release Note • 11/26/2025 • 1 min read

Resolved issues

The following issue has been resolved in this release.

ID	Description
337204	The system fails to delete locations that do not have a compliance location on The Location Card page.



2502.0.0.0

Release Note • 10/22/2025 • 1 min read

Enhancements/Modifications

This extension has been updated to ensure interoperability with the recent changes in the Apteian Inspection Status extension. For more information, see [What's new in Inspection Status, version 2504.0.0.0](#).



2501.1.0.0

Release Note • 9/4/2025 • 1 min read

Enhancements/Modifications

With this release of the Aptean eSignature extension, the following updates have been introduced to improve authentication handling and maintainability:

- Updates to *eSignatureMgt173FDW* codeunit
 - Replaced direct authentication logic with calls to the new *eSignatureOAuthMicrosoft173FDW* codeunit.
 - Standardized error messaging with labels: *AuthFailureErr*, *AuthFailureNoHTTPStatusErr*.
 - Delegated token acquisition and validation to a dedicated *OAuth* codeunit for improved maintainability.
- Additions to *eSignatureOAuthMicrosoft173FDW* codeunit
 - Implemented the *GetOAuthToken* procedure to acquire access tokens using the OAuth 2.0 authorization flow.
 - Added *ValidateUserSignIn* to enforce Multi-Factor Authentication (MFA) claims validation during login.
 - Introduced error handling for token request failures using the following error labels:
 - *DidNotUseMfaErr*
 - *AccessTokenNotInResponseErr*
 - *FailedGetAccessTokenErr*
 - *FailedToSendRequestErr*
 - Standardized redirect URL retrieval logic by combining default URL handling with setup configuration.



2501.0.0.0

Release Note • 8/27/2025 • 3 min read

Features

With the features added in this release of the Aptean eSignature extension, you can:

- Set up centralized eSignature configuration to manage digital signature settings and requirements across your organization. For more information, see [Set up e-signature configuration](#).
- Configure Two-Factor Authentication (2FA) settings to enforce additional security measures during the digital signature process. For more information, see [Configure Two-Factor authentication](#).
- Create eSignature user groups to define which users are required to sign documents and assign their roles as primary, secondary, or other signing authorities. For more information, see [Set up e-signature user groups](#).
- Sign documents, review content, reject requests, delegate signatures, and show document responsibilities to maintain efficient workflow. For more information, see [Manage e-signature requests](#).
- Set up delegate groups when the primary signer is unavailable. For more information, see [Set up delegate groups](#).
- Configure status management flows to integrate e-signature requirements into document approval workflows. For more information, see [Integration with Aptean Status Management](#).
- Track the status of vendor related records. For more information, see [Manage vendor status log](#).
- Process signature requests through a centralized interface that displays pending, approved, and rejected signatures. For more information, see [Manage e-signature requests](#).
- Set up and manage production scenarios with status management, e-signature certification workflows, and version control for bills of material (BOMs) and routing instructions. This ensures manufacturing processes use only approved, certified versions and require an e-signature when moving scenarios to certified status. For more information, see [Set up production scenarios](#).
- Generate comprehensive audit trail reports to track items and lot history across all production, sales, purchase, warehouse, and quality documents for regulatory compliance and traceability. For more information, see [Manage item audit trail](#).
- Create snapshot records of certified production BOMs, routings, and production scenarios with embedded e-signature data for historical audit and compliance purposes. For more information, see [View e-signature snapshots](#).
- Generate audit reports for finished production orders, including consumption details, output data, deviations, and linked certified scenarios for regulatory review. For more information, see [Generate audit report for](#)



[production order](#).

- Configure compliance-controlled locations to enforce additional regulatory controls and mandatory certified scenario usage at designated manufacturing sites. For more information, see [Configure compliance locations](#).
- Track and approve production order planning deviations through e-signature workflows when components, quantities, or routing changes occur during manufacturing processes. For more information, see [View deviation](#).
- Generate comprehensive batch record reports that include production order planning data, actual production transactions, related quality control records, and electronic signatures to support regulatory compliance requirements. For more information, see [Manage batch record](#).

Integrations

The Aptean eSignature extension has been integrated with the following extensions:

- Aptean [Status Management](#)
- Aptean [Advanced Attributes](#)
- Aptean [Approved Supplier](#)
- Aptean [Audit Trail](#)
- Aptean [Quality Control \(BC\)](#)
- Aptean [License and Subscription Management](#)
- Aptean [Inspection Status](#)
- Aptean [Production Scenarios](#)
- Aptean [Non Conformances](#)
- Aptean [Filter Group](#)
- Aptean [Compliance Documents](#)
- Aptean [Process Manufacturing](#)
- Aptean [Vendor Item Catalog](#)

For more information, see [Integrations](#).



Introduction

Article • 8/27/2025 • 1 min read

The Aptean eSignature (ESG) extension streamlines your document approval process by enabling secure digital signatures within Business Central. You can define signature requirements, manage user groups with different signing authorities, and ensure compliance with regulatory and organizational policies through automated validations.

This extension integrates seamlessly with existing Business Central workflows by adding signature checkpoints at critical approval stages. When documents require signatures, the system automatically routes them to the appropriate signers based on predefined user groups and authority levels. It enforces signing authority structures, and provides comprehensive audit trails for traceability.

Key benefits include:

- Ensures regulatory and company policy compliance with mandatory e-signature workflows.
- Enhances security through Two-Factor Authentication (2FA) and hierarchical approval levels.
- Automates routing, delegation, and notifications to reduce processing time.
- Provides tamper-proof audit trails for compliance reporting and historical reference.
- Maintains complete traceability across business and production records.

Note

- To use the Aptean eSignature extension, the following extensions must be installed:
- Aptean [Status Management](#)
- Aptean [Advanced Attributes](#)
- Aptean [Approved Supplier](#)
- Aptean [Audit Trail](#)
- Aptean [Quality Control \(BC\)](#)
- Aptean [License and Subscription Management](#)
- Aptean [Inspection Status](#)
- Aptean [Production Scenarios](#)
- Aptean [Non Conformances](#)
- Aptean [Filter Group](#)
- Aptean [Compliance Documents](#)
- Aptean [Process Manufacturing](#)



Setup

Article • 8/27/2025 • 1 min read

The following setups are required.

- [Manage permission sets](#)
- [Set up eSignature configuration](#)
- [Configure Two-Factor Authentication](#)
- [Set up eSignature user groups](#)
- [Set up delegate groups](#)
- [Configure compliance locations](#)



Manage permission sets

Article • 8/27/2025 • 3 min read

Permission sets in Business Central define a user's access level to various features and data within this extension.

We provide the following system permission sets:

- Direct
- Indirect

Direct permission sets

Users with this permission set can perform specific actions directly without requiring additional approvals or workflows. These sets include permissions to read, modify, delete, and create data.

The direct permission set ID for this extension is *ESIGNATURE173FDW*.

Indirect permission sets

Users with this permission set can perform specific actions. This is used in conjunction with other permission sets to allow you to perform certain actions. These permissions typically involve additional conditions or approvals before the action can be completed.

The indirect permission set ID for this extension is *ESIGNATBASIC173FDW*.

User-defined permission sets

In addition to the system permission sets we provide, you can create new permission sets or copy system permission sets and modify or delete access to specific entities according to your requirements. For more information, see [Assign permissions to users and groups](#).

Assign a permission set

1. Select the Search icon , enter **Users**, and then choose the related link.
The **Users** list page opens.
2. Navigate to the username for which you want to assign the permission set and select it.
The **User Card** page opens.
3. On the **User Permission Sets** FastTab, in the **Permission Set** field, enter the valid permission set for this extension.



eSignature

The associated fields are automatically updated based on the entered value.

The user has the necessary permissions to use the features of the Aptean eSignature extension, ensuring secure and role-based access.



Set up e-signature configuration

Article • 8/27/2025 • 2 min read

You can set up the e-signature configuration to manage digital signature settings and notifications across your organization.

To set up e-signature configuration, follow these steps:

1. Select the Search icon , enter **eSignature Setup**, and then choose the related link. The **eSignature Setup** page opens.
2. Turn on the **eSignature Enabled** toggle to activate the e-signature feature for all relevant transactions.
3. Turn on the **Enable Alerts** toggle to configure notification settings.
4. On the **Alerts** FastTab, enter the required information in the following fields:
When *Azure Service Bus* is selected in the **Notification Service** field, the **Azure Service Bus URL**, **Topic**, **Time to Live**, and **Number of Retries** fields are visible.

Field	Description
Notification Service	Select the method of alert notification. The available options are: <i>Azure Service Bus</i> or <i>HTTP Endpoint</i> . When <i>Azure Service Bus</i> is selected, the Azure Service Bus Settings Group fields become available. When <i>HTTP Endpoint</i> is selected, the <i>HTTP Endpoint</i> settings group become available.
Azure Service Bus URL	Specify the endpoint URL for the azure service bus.
Topic	Enter the name of the topic where messages should be sent.
Time to Live	Define the duration (in seconds) that a message remains valid before expiring.
Number of Retries	Specify how many times the system will retry sending a failed message.

These fields are available when **Notification Service** field is set to *HTTP Endpoint*.

Field	Description
HTTP Endpoint URL	Specify the URL where alerts sent.
Authentication Type	Select the type of authentication used for HTTP endpoint. The available options are: <i>Basic</i> or <i>Anonymous</i> .
Username	Enter the username used for basic authentication. This field is available only when the Authentication Type field value is set to <i>Basic</i> .



Password	Enter the password used for basic authentication. This field is available only when the Authentication Type field value is set to <i>Basic</i> .
----------	---

5. On the **Microsoft Entra ID Settings** FastTab, enter the required information in the following fields:

Field	Description
Client ID	Enter the client ID used for Microsoft Entra ID integration.
Client Secret	Enter the client secret used for Microsoft Entra ID authentication.
Redirect URL	Enter the URL to which users are redirected after Entra ID authentication.

The e-signature configuration is set up and ready to use.



Configure Two-Factor Authentication

Article • 8/27/2025 • 1 min read

You can configure Two-Factor Authentication (2FA) settings to enforce additional security measures for user authentication during the digital signature process.

! Note

You can configure Two-Factor Authentication only after the fields on the **Microsoft Entra ID Settings** FastTab are set up on the **eSignature Setup** page.

You can execute the **User Security Info** action on the **eSignature Setup** page, then you can navigated to the **Security info** page. To know more, see [Multifactor authentication \(MFA\) for Business Central](#).



Set up delegate groups

Article • 8/27/2025 • 2 min read

You can set up delegate groups to allow signature responsibilities to be transferred when the primary signer is unavailable, ensuring continuity.

To set up delegate groups, follow these steps:

- 1. Select the Search icon , enter **eSignature Delegate Group**, and then choose the related link. The **eSignature Delegate Group** page opens.
- 2. On the **General** FastTab, enter the required information in the following fields:

Field	Description
Code	Enter a unique identifier for the delegate group.
Description	Enter a description for the delegate group.

- 3. On the **eSignature Delegate Group Lines** FastTab, enter the required information in the following fields:

Field	Description
User ID	Select the user who can sign documents when the primary signing authority is not available.
User Full Name	Enter the full name of the delegate user.

The delegate group is set up and can be assigned to e-signature user groups as needed.



Set up e-signature user groups

Article • 8/27/2025 • 2 min read

You can create user groups that require e-signatures to control which users are required to sign documents. Additionally, you can define users within each group and specify their role as primary, secondary, or other levels of signing authority.

To set up e-signature user groups follow these steps:

- 1. Select the Search icon , enter **eSignature User Group Management**, and then choose the related link. The **eSignature User Group Management** page opens.
- 2. The following fields are available:

Field	Description
Code	Displays a unique identifier for the user group.
User Group Name	Displays a descriptive name for the user group (for example, purchasing, quality assurance).
Enforce Signing Hierarchy	Displays whether the checkbox is selected.

- 3. On the action bar, select **New** to create a user group.
- 4. Enter the required information in the following fields:

Field	Description
Code	Enter a unique identifier for the user group.
User Group Name	Enter a descriptive name for the user group (for example, Purchasing, Quality Assurance).
Enforce Signing Hierarchy	Turn on this toggle to enforce that signatures must be obtained in a specific sequence based on authority.
Delegate Group Code	Select the delegated user group code.

- 5. On the **eSignature Users** FastTab, enter the required information in the following fields:

Field	Description
User ID	Select the identifier of the user to include in the eSignature group.



Signing Authority	Define the level of signing authority assigned to the user. Enter 1 for primary signer, 2 for secondary signer, and so on. The Signing Authority field value cannot have a value higher than the previous value. For example, you cannot assign 2 if there is no user with 1.
Mandatory	Select this checkbox if the user's signature is mandatory for document approval.

If you attempt to delete a user group that is currently in use, the system displays an error message.

If you modify the list of users or change signing authority, the system provides an informational message if there are any open signing requests for this user group.

The eSignature user group is created and ready for use in signature workflows.



Configure compliance locations

Article • 8/27/2025 • 2 min read

You can designate specific manufacturing locations as compliance-controlled locations where additional regulatory controls apply.

To configure compliance locations, follow these steps:

1. Select the Search icon , enter **Compliance Controlled Locations**, and then choose the related link.
The **Compliance Controlled Locations** page opens.
2. On the action bar, select **New** to add a location that requires compliance controls.
3. In the **Location Code** field, select the manufacturing location.

The location is configured for compliance controls. All production activities at this location enforces certified production scenario usage and mandatory deviation approvals.

Note

If the Two-Factor Authentication is not configured, the system throws an error message. If you try to sign a document not assigned to you, the system displays a notification.



Manage vendor status log

Article • 8/28/2025 • 3 min read

You can view all status transitions for the record on the **Status Management Log** page.

To change the status in the vendor follow the steps:

- 1. Select the Search icon , enter **Vendors**, and then choose the related link. The **Vendors** page opens.
- 2. On the **Vendor** page, search **Change Status Mgmt Status** page in the Tell Me and then choose the related link. The **Status Management Lines** page opens.
- 3. Select the status code line.
- 4. Select **OK** to confirm.
The system updates the **Status Mgmt. Description** field value with the selected codes description. If the selected status code does not include the **eSignature User Group** field value, the **Pending Change Status To** field is not displayed. The **Pending Change Status To** field displays the description from the selected status code line.
- 5. Select the **Pending Change Status To** field value.
The **eSignature Request Entries** page opens.
- 6. Sign the documentation to complete the status change.
- 7. On the action bar, select **Status Management Log**.
The **Status Management Log** page opens.
- 8. Enter the required information in the following field:

Field	Description
Previous Status Management Status Code	Displays the status code before the change occurred.
New Status Management Status Code	Displays the status code after the change occurred.
Date and Time	Displays the date and time when the status change occurred.
Time	Displays the time of the status change.
User ID	Displays the ID of the user who made the status change.

- 9. On the **Change Log Entries** FastTab, enter the information in the following field:

Field	Description
Date and Time	Displays the date and time when the change was logged.
Time	Displays the time when the change was logged.



User ID	Displays the ID of the user who made the change.
Field Caption	Displays the name of the field that was changed.
Old Value	Displays the value of the field before the change.
New Value	Displays the value of the field after the change.

10. On the **Approved / Rejected** FastTab, enter the information in the following fields:

Field	Description
Entry No.	Displays the unique entry number for the approval or rejection.
From Status	Displays the original status before the action.
To Status	Displays the new status after the action.
eSignature User Group	Displays the user group authorized to provide an eSignature.
User ID	Displays the ID of the user who performed the action.
Signing Authority	Displays the person authorized to approve or reject.
Status	Displays the current status of the request.
Signed Date and Time	Displays the date and time when the request was signed.
Key	Displays the unique identifier for the signature record.
Comment	Displays the remarks provided during approval or rejection.
Delegated From User ID	Displays the ID of the user who delegated the task.

On the **Vendor Item Catalog** page, filter vendors by the **Status Management Status Code** field value.



Manage e-signature requests

Article • 8/27/2025 • 2 min read

You can sign documents, review content, reject requests, and delegate signature responsibilities to maintain efficient workflow operations.

Sign documents

You can sign documents assigned to you through the **eSignature Request Entries** page.

To sign a document follow these steps:

1. Navigate to the **eSignature Request Entries** page.
2. Select a record associated with your user.
3. Execute the **Sign** action.

If the Two-Factor Authentication is configured on the **Security info** page of the Microsoft, the system sends an a One-Time Password (OTP) to your registered mobile device.

Note

If the Two-Factor Authentication is not configured, the system throws an error message. If you try to sign a document not assigned to you, the system displays a notification.

Once you sign the document successfully, the record moves to the **eSignature Entries** page, and the document status updates according to the workflow configuration.

Show documents

You can open and review the related document where a signature is being requested before proceeding with the signature process.

To view a document follow these steps:

1. Navigate to the **eSignature Request Entries** page.
2. Select the appropriate record.
3. On the action bar, select **Show Document** to view the selected document.

The document opens in a new window or tab for review.

If the document is not available, the system displays an error message.



Reject signature requests

You can reject signature requests when documents do not meet approval criteria or require modifications.

The system performs the following actions on the **eSignature Entries** page:

- Deletes all signature requests associated with the selected record.
- Tracks the rejection entry.
- Records the comment.

Note

If you try to reject a record you are not authorized to, the system displays an error message.

Delegate signature requests

You can delegate signature requests to other authorized users when you are unavailable or when delegation is appropriate.

To delegate a signature request follow these steps:

1. Navigate to the **eSignature Request Entries** page.
2. Select the record you want to delegate.
3. Execute the **Delegate** action.
4. Select the person who should sign the document from the available delegate users.

The signature request is transferred to the selected delegate user.



View e-signature request entries

Article • 8/27/2025 • 2 min read

You can view all signature requests on the **eSignature Request Entries** page. This page displays pending, approved, and rejected signature requests.

To view e-signature request entries, follow these steps:

- 1. Select the Search icon , enter **eSignature Request Entries**, and then choose the related link.

The **eSignature Request Entries** page opens.

- a. The following fields are available:

Field	Description
Entry No.	Displays the unique identifier for the eSignature request entry.
Date and Time	Displays the timestamp when the request entry was created.
User ID	Displays the user who created or is responsible for the request.
Table Caption	Displays the name or type of the record involved in the signature process.
Source Primary Key	Displays the reference key for the source record that triggered the request.
From Status	Displays the current status before the signing action (for example, New, Under Review).
To Status	Displays the target status that the entry moves to after signing action (for example, Approved, Certified).
eSignature User Group	Displays the group responsible for reviewing and signing the request.
Signing Authority	Displays the level or order of authority required to sign the entry.
Version	Displays the version number of the signing record.
Delegated From User ID	Displays the original user who held the request before delegation.



View completed signatures

Article • 8/27/2025 • 2 min read

You can view all completed signature activities through the **eSignature Entries** page, which provides a comprehensive audit trail.

To view completed signatures, follow these steps:

- 1. Select the Search icon , enter **eSignature Entries**, and then choose the related link. The **eSignature Entries** page opens.
- 2. View the required information in the following fields:

Field	Description
Entry No.	Displays the sequential number of the e-signature entry.
Date and Time	Displays the date and time when the e-signature was triggered or logged.
Status	Displays the status of the e-signature entry (for example, signed, pending).
Table Caption	Displays the name of the table related to the signed document (for example, sales header).
From Status	Displays the target status that the entry moves to after signing action (for example, approved, certified).
To Status	Displays the status of the document after the e-signature was recorded.
eSignature User Group	Displays the user group associated with the signer.
User ID	Displays the user who performed the signature.
Signing Authority	Displays the signing level or authority value of the user.
Mandatory	Displays whether the signature was mandatory for the document to proceed.
Signed Date and Time	Displays the actual date and time the document was signed.
Comment	Displays any comment entered by the user during the signing process.
Delegated From User ID	Displays the original user if the signature was delegated from another user.



Set up production scenarios

Article • 8/27/2025 • 3 min read

You can configure production scenarios to define standardized manufacturing processes that can be certified and tracked.

To set up production scenarios, follow these steps:

1. Select the Search icon , enter **Items**, and then choose the related link.
The **Items** list page opens.
2. Select the required **No.** field value to open the relevant **Item Card** page.
The **Item Card** page opens.
3. On the action bar, select **Production Scenarios (Related > Bill of Materials > Production)**.
The **Item Production Scenario** page opens.
4. In the **Status** field, select the status of the production scenario. The available options are:
 - *New*: Default status for newly created scenarios.
 - *Under Development*: Work in progress stage.
 - *Certified*: Scenario approved for use in production. Locked from further edits unless reverted. Requires an eSignature for transition.
 - *Closed*: Scenario is no longer active or valid for production.

When the **Status** field is set to *Certified* for a production scenario, an eSignature request is triggered. If multi-factor authentication is configured on the **eSignature Setup** page, you must complete OTP (One-Time Password) validation before signing the document. After the status is set to **Certified**, you cannot change other field values. When the *Status* field is set to *New** or *Under Development*, you can make changes in the production scenario.

Note

If you try to sign a document not assigned to you, the system displays a notification.

5. In the **Production BOM Version Code** field, select the specific BOM version code. If this field value is left blank on the **Item Production Scenario** page, then the **Active Version** field value can be configured on the **Production BOM** page.
6. In the **Routing Version Code** field, select the specific routing version code. If this field value is left blank on the **Item Production Scenario** page, then the **Active Version** field value can be configured on the **Routing** page.
7. On the action bar, select **Certified Production Scenario History** to view the eSignature history for this production order.



 Note

The system must verify that the entered production BOM version code matches the version available in the system. The system must verify that the entered routing version code matches the version available in the system.

For all existing production scenario documents, the system updates the **Status** field value to *Certified* upon extension installation or upgrade. For any new production scenario document, the system automatically assigns the **Status** field value is set to *New*.

 Note

Only certified scenarios are available for selection in production orders. If BOM or route versions linked to the scenarios are not certified, the **Refresh Production Order** action on the **Planned Production Order** page cannot be executed.



Manage item audit trail

Article • 8/28/2025 • 2 min read

You can use the **Item Audit Trail** page to trace and review all documents and records where a specific item and lot are referenced. This helps auditors, compliance officers, and system administrators track production, sales, purchases, warehouse, and quality-related activities for a given item and lot.

To generate an audit trail, follow these steps:

1. Select the Search icon , enter **Item Audit Trail**, and then choose the related link.
The **Item Audit Trail** page opens.
2. On the **Filters** section, enter the required information in the following fields:

Field	Description
Item No.	Select the item number for which you want to generate the audit trail.
Lot No.	Enter the lot number. This field value is mandatory.

3. On the action bar, execute the following actions:

Action	Description
Trace	Generates the list of related documents where the selected item and lot are referenced.
Item	Opens the Item Card page for the selected item number.
Lot No. Information	Opens the Lot No. Information page with detailed records of the selected lot.

4. In the **Related Entries** field, view the list of all associated documents.
5. In the **No. of Entries** field, view the number of entries.

The audit trail includes the following record types:

- Production Orders (all types, showing whether the item/lot is an output line or component line)
- Sales Documents (posted and open)
- Purchase Documents (posted and open)
- Warehouse Documents (posted and open)
- Inspection Tags
- Non-Conformances (closed and open)
- Compliance Documents



eSignature

- Quality Checks (posted and open)
- Item Ledger Entries
- Warehouse Ledger Entries

You can view all the related documentation of the item in the audit trail.



View e-signature snapshots

Article • 8/27/2025 • 2 min read

The **eSignature Snapshots** page allows you to view tamper-proof snapshot records that are created when a document is certified with an e-signature. These snapshots store historical data, providing compliance officers and auditors with full traceability of who signed a record and when it was certified.

To view e-signature snapshots, follow these steps:

1. Select the Search icon , enter **eSignature Snapshots**, and then choose the corresponding link.
The **eSignature Snapshots** page opens.
2. On the action bar, select **View Snapshot** to open the selected snapshot record in detail, and display all data captured at the time of certification.
The system automatically updates snapshots in the **Entry No.** field.

The snapshot list displays all certified records with signatures. Each entry represents a frozen record of the document as it existed when signed.

Note

- Snapshots are read-only and cannot be modified once created, ensuring audit and compliance integrity.
- Snapshots specifically apply to certified production BOM, routing, and production scenarios.



View routing snapshot history

Article • 8/30/2025 • 2 min read

To view routing snapshot history, follow these steps:

1. Select the Search icon  , enter **Routings**, and then choose the related link. The **Routings** list page opens.
2. Select the required routing to view.
3. Select **Show Snapshot** to view the complete certification history. The **e-Signature Snapshot** page opens showing all certification events.
4. Select a snapshot entry to view the complete process detail captured at that point in time, including all work centers, machine centers, tools, personnel, and quality measures.

Important

The certified routings cannot be modified. To make changes, create a new version with a different version code.



View production BOM snapshot history

Article • 1/30/2026 • 2 min read

To view production BOM snapshot history, follow these steps:

1. Select the Search icon  , enter **Production BOMs**, and then choose the related link. The **Production BOMs** list page opens.
2. Select the required production BOM to view.
3. On the action bar, select **Show Snapshot** to view the complete snapshot history. The **e-Signature Snapshot** page opens showing all certification events with linked e-signatures.
4. Select a snapshot entry to view the complete formulation data captured at that point in time.

Important

The certified production BOMs cannot be modified. The system enforces this by making all fields read-only when the **Status** field value is set to *Certified*. To make changes, create a new version with a different version code.



View production scenario snapshot history

Article • 1/30/2026 • 2 min read

To view production scenario snapshot history, follow these steps:

1. Select the Search icon , enter **Item Production Scenarios**, and then choose the related link. The **Item Production Scenarios** list page opens.
2. Select the production scenario to view.
3. On the action bar, select **Show Snapshot** to view the certification history. The **e-Signature Snapshot** page opens showing all certification events.
4. Select a snapshot entry to view the complete configuration captured at that point in time.

Note

The production scenarios must reference certified BOM and routing versions. The system validates this before allowing certification.



Generate audit report for production order

Article • 8/28/2025 • 1 min read

You can generate an audit details report to review completed production orders and all associated records.

To generate the report, follow these steps:

1. Navigate to the desired **Finished Production Order** page.
2. On the action bar, select **Audit Details Report (Actions > Other)**.
The **Audit Details Report** page opens.
3. Select **Print**.
4. Select the desired file type.
5. Select **OK**.

The system generates a report including:

- Production order header and finish date.
- Related e-signatures.
- Deviations logged with signatures.
- Consumption details (item, lot, quantity, user, timestamp).
- Output details (item, lot, quantity, user, timestamp).
- Certified production scenario, BOM, and routing linked to the Production Order.

Note

If the Two-Factor Authentication is not configured, the system throws an error message. If you try to sign a document not assigned to you, the system displays a notification.



Set up BOM

Article • 8/27/2025 • 3 min read

You can configure BOM to define production bills that can be certified and tracked.

To set up production scenarios, follow these steps:

- 1. Select the Search icon , enter **Production BOMs**, and then choose the related link.
The **Production BOMs** list page opens.
- 2. Select the required **No.** field value to open the relevant **Production BOM** page.
The **Production BOM** page opens.
- 3. On the **General** FastTab, enter the required information in the following fields:

Field	Description
Allow Over and Under Production	Select the handling method for overproduction and underproduction scenarios. The available options are Percentage and Unlimited. The default value is <i>Unlimited</i> .
Allow % Over Production	Enter the percentage of overproduction allowed. This field is displayed only when the Allow Over and Under Production field value is set to <i>Percentage</i> . The value must be between 0-100.
Allow % Under Production	Enter the percentage of underproduction allowed. This field is displayed only when the Allow Over and Under Production field value is set to <i>Percentage</i> . The value must be between 0-100.
Active Version	Enter the version of the production BOM that is currently active. If the BOM Version Code field value is left blank on the Item Production Scenario page, the system uses this active version. The value must be between 0-100.

On the action bar, select **Change Status Mgmt Status** to change the **Status Mgmt. Description** field value on the **General** FastTab. For more information, see [Execute e-signature in production order](#).



View deviation

Article • 8/27/2025 • 1 min read

When you change field values on the **Lines** FastTab of the **Firm Planned Production Order**, **Planned Production Order**, or **Released Production Order** page and with e-signature setup configured, deviations must be logged and approved.

To view the deviation, follow these steps:

- 1. On the action bar, select **Deviations**.
The **eSignature Deviation List** page opens.
- 2. The following fields are available:

Field	Description
Status	Displays the status of the deviation. The available options are: <i>Pending, Approved, Rejected</i> .
Action	Displays the type of action that triggered the deviation. The available options are: <i>Insert, Modify, Delete</i> .
Old Value	Displays the original value before the change.
New Value	Displays the updated value after the change.
Source Document	Displays the document where the deviation originated in the production order, purchase order, or quality control check.
Source Type	Displays the type of source record in the production, sales, or purchase.
Source Subtype	Displays the detailed classification of subtype in the released production order or sales invoice.
Source ID	Displays the identifier of the source record. The available options are: <i>Document No., Order ID</i> .
Source Batch Name	Displays the associated batch name, if any.
Source Prod. Order Line	Displays the production order line number, if applicable.
Source Ref. No.	Displays the reference number.

- 3. On the action bar, select **Request Signature**.
The document is e-signed.



 Note

- Deviations must be signed off with an e-signature. Production orders cannot be finished until deviations are approved.
- You can view the **Prod. Order Line** and **Prod. Order Component** Factboxes on the **eSignature Deviation List** page.



Use e-signature in a production order

Article • 8/28/2025 • 2 min read

You can manage status changes through an enhanced e-signature workflow on the **Released Production Order**, **Planned Production Order**, and **Firm Planned Production Order** pages.

To sign the documentation, follow these steps:

- 1. Navigate to **Production Order List** page.
- 2. Select the related production order.
- 3. On the action bar, select **Change Status Mgmt Status**. The **Status Management Lines** page opens.
- 4. Select a related line.
- 5. Select **OK** to confirm.

The system updates the value in the **Status Mgmt. Description** field with selected codes description. If the selected code does not include an **eSignature User Group** field value on the **Status Management Flow** page, then the **Pending Change Status To** field is not displayed. The **Pending Change Status To** field value displays the description from the selected status line.

- 6. Select the **Pending Change Status To** field value. The **eSignature Request Entries** page opens.
- 7. On the action bar, select **Sign** the documentation. The document is e-signed.
- 8. On the action bar, select (**Related** > **Status Management Log**). The **Status Management Log** page opens. On the **Approved/Rejected** FastTab, view the information in the following fields:

Field Name	Description
Entry No.	Displays the unique entry number for the approval or rejection.
From Status	Displays the original status before the action.
To Status	Displays the new status after the action.
eSignature User Group	Displays the user group authorized to provide an eSignature.
User ID	Displays the ID of the user who performed the action.
Signing Authority	Displays the person authorized to approve or reject.
Status	Displays the current status of the request.
Signed Date and Time	Displays the date and time when the request was signed.
Key	Displays the unique identifier for the signature record.
Comment	Displays the remarks provided during approval or rejection.



Delegated From User ID	Displays the ID of the user who delegated the task.
------------------------	---

 **Note**

If the **Location Code** field value is not selected on the **Planned Production Order** page, the system displays an error message.

When you change any field values on the **Lines** FastTab of production orders after eSignature setup is configured, execute the **Deviations** action and then execute the **Request Signature** action on the **eSignature Deviation List** page to request the e-signature.



Manage batch record

Article • 8/27/2025 • 2 min read

You can use the **Batch Record** page to generate comprehensive manufacturing documentation that includes production order planning data, production order transaction details, related quality control records, and electronic signatures.

This report supports regulatory compliance requirements for regulated manufacturing industries and provides complete batch production reporting for recording and audit purposes.

To generate a batch record, follow these steps:

1. Select the Search icon , enter **Batch Record**, and then choose the related link. The **Batch Record** page opens.

[NOTE!] You must create a report layout to meet your specific requirements.

2. On the **General** FastTab, enter the required information in the following fields:

Field	Description
User ID	Select the ID of the user whose signatures you want to include in the report.
Record Status	Select the eSignature entry status to filter signatures.
Include Quality Check	Turn on this toggle to include quality check data in the batch record. The data includes planned quality checks from the routing and posted quality control results.
Include eSignatures for QC	Turn on this toggle to include electronic signatures related to quality control activities. The Include Quality Check toggle must turned on to use this toggle.

3. Select the required filter options on all related filter FastTabs.

4. Enter the required information in the following FastTabs:

Filter FastTabs	Description
Production Order Component	Includes component consumption and usage data, including lot numbers and quantities.
Item Production Scenario	Includes certified production scenarios with BOM versions, routing versions, and MMR references.
Quality Control Check Line	Includes planned quality measures and specifications from the production routing.



Posted Quality Control Check Line	Includes actual quality control results, measurements, and approval status.
Quality Control Check Header	Includes quality control summary information and batch approvals.
eSignature Entry	Includes production-related electronic signatures with timestamps and user information.
eSignature Deviation	Includes deviation approval signatures and corrective action authorizations.
eSignature Request Entry	Includes pending signature requests and workflow status.
Routing Header	Includes master routing information and operation sequences.
Routing Line	Includes detailed operation information for work centers and machine centers.
Work Center	Includes work center details, capacity information, and equipment data.
Machine Center	Includes machine-specific information, maintenance records, and settings.
Item Ledger Entry	Includes complete item transaction history for material traceability.
Warehouse Entry	Includes warehouse transaction details for material handling activities.
Lot No. Information	Includes lot-specific tracking data, attributes, and certifications.

5. On the **Advanced Settings** FastTab, enter the required information in the following fields:

Field	Description
Maximum row generation time	Select the timeout limit for report generation. The default value is <i>06:00:00</i> .
Maximum rows	Select the maximum number of rows in the report. The default value is <i>500,000</i> .
Maximum documents	Enter the number of documents included. The default value is <i>200</i> .
Format region	Select regional formatting for numbers and dates.
Language	Select the report language for international operations.

6. Select **Print**.

The batch record report is generated.



Filter eSignature snapshots

Article • 1/30/2021 • 2 min read

You can filter eSignature snapshots using key attributes to efficiently identify records required for compliance and audit tracking.

To filter eSignature snapshots, follow these steps:

- 1. Select the Search icon , enter **eSignature Entries**, and then choose the related link.
The **eSignature Entries** page opens.
- 2. On the action bar, select **Filter** to open the filter pane.
- 3. In the filter pane, enter your criteria in the following fields as needed:

Field	Description
Table Caption	Filter by document type (e.g., Production BOM, Routing, Production Scenario)
Primary Key 1 Value	Filter by record ID or number
Date and Time	Filter by date range when the snapshot was created
User ID	Filter by the user who created the snapshot
Status	Filter by eSignature entry status
Snapshot Exists	Filter to show only entries with snapshots

The page refreshes automatically to display entries matching your filter criteria.

- 4. To view additional details about a filtered entry, select the entry from the list.
The entry details display on the **eSignature Entries** page displays complete metadata including table information, primary key values, status changes, and snapshot availability.



View snapshots in treeview format

Article • 1/30/2026 • 2 min read

On the **eSignature Entries** page to view snapshots in treeview format, follow these steps:

- 1. Select the Search icon , enter **eSignature Entries**, and then choose the related link.
The **eSignature Entries** page opens.
- 2. Locate the eSignature entry with a snapshot you want to view. Entries with snapshots have *Yes* in the **Snapshot Exists** field.
- 3. Select the entry with the snapshot.
- 4. On the action bar, select **Show Snapshot**. The **eSignature Snapshot** page opens in treeview format.

The treeview displays snapshot data with the following columns:

Field	Description
Field Caption	The caption of the field or table name.
Snapshot Value	The value from the snapshot at the time it was captured.
Current Value	The current value of the field in the live database.



View eSignature entries from production BOM

Article • 1/30/2026 • 2 min read

To view eSignature entries from a production BOM, follow these steps:

1. Select the Search icon  , enter **Production BOM**, and then choose the related link.
The **Production BOM** page opens.
2. Select the production BOM you want to review. The production BOM card opens showing details including the **Pending Status Change To** field, which displays the required status. The record will be assigned if all required eSignatures are signed.
3. On the action bar, select **View eSignature Entries**. The **eSignature Entries** page opens, filtered to show only entries related to the selected production BOM.
4. Review the eSignature entries to see:
 - Entry numbers and creation dates
 - User IDs and signing authorities
 - Status changes (From Status and To Status)
 - Signed date and time
 - Comments and delegation information
 - Snapshot availability
5. To view the certified snapshot history, return to the **Production BOM** page.
6. On the action bar, select **Certified Production BOM History**. The system displays the certified snapshot history for the production BOM showing all certification events and their associated snapshots.



View eSignature entries from routing

Article • 1/30/2026 • 4 min read

You can access eSignature entries directly from Routing to review certification history and approval workflows by following these steps:

1. Select the Search icon , enter **Routing**, and then choose the related link.
The **Routing** page opens.
2. Select the routing you want to review. The Routing Card opens showing details including the **Pending Status Change To** field, which displays the required status. The record will be assigned if all required eSignatures are signed.
3. On the action bar, select **View eSignature Entries**.
The **eSignature Entries** page opens, filtered to show only entries related to the selected routing.
4. Review the eSignature entries to see certification history, user information, status changes, and snapshot availability.
5. To view the certified snapshot history, return to the **Routing** page.
6. On the action bar, Select **Certified Routing History**. The system displays the certified snapshot history for the routing.

View eSignature entries from routing version

You can access eSignature entries directly from routing version to review certification history and approval workflows by following these steps:

1. Select the Search icon , enter **Routing Version**, and then choose the related link.
The **Routing Version** page opens.
2. Select the routing version you want to review.
3. On the action bar, select **View eSignature Entries**.
The **eSignature Entries** page opens, filtered to show only entries related to the selected routing version.



View eSignature entries from production scenarios

Article • 1/30/2026 • 2 min read

To view eSignature entries from a production scenario, follow these steps:

1. Select the Search icon , enter **Item Production Scenarios**, and then choose the related link. The **Item Production Scenarios** page opens.
2. Select the production scenario you want to review. The production scenario card opens showing details including the **Pending Status Change To** field, which displays the required status. The record will be assigned if all required eSignatures are signed.
3. On the action bar, select **View eSignature Entries**. The **eSignature Entries** page opens, filtered to show only entries related to the selected production scenario.
4. Review the eSignature entries to see certification history, user information, status changes, and snapshot availability.
5. To view the certified snapshot history, return to the **Item Production Scenarios** page.
6. On the action bar, select **Certified Production Scenario History**. The system displays the certified snapshot history for the production scenario.
7. To view eSignature snapshots, on the action bar, select **View eSignature Snapshots**. The **eSignature Snapshots** page opens showing all snapshots associated with the production scenario.



Generate reports from enhanced XML snapshots

Article • 1/30/2026 • 3 min read

The enhanced XML snapshot data includes the following metadata for each field:

Field	Description
Field ID	Unique identifier of the field
Field Name	Name of the field
Field Value	Value of the field at snapshot time
Table ID	Unique identifier of the table
Table Name	Name of the table

This functionality provides the following benefits:

- **Dynamic report dataset generation:** Report data designer can dynamically generate datasets from XML snapshots without hardcoding field structures, allowing reports to adapt to data model changes.
- **Complete audit trail:** Missing or changed data elements are logged separately, providing a complete history of structural changes for regulatory compliance.
- **Flexible reporting:** Reports can reference historical data accurately even when the current data structure has been modified.

To use enhanced XML snapshots in report data designer, follow these steps:

1. Select the Search icon , enter **Report Data Designer List**, and then choose the related link. The **Report Data Designer List** page opens.
2. On the action bar, select **New** to create a report data design. The **Report Data Design Card** page opens.
3. On the **General** FastTab, enter the report code, description, and report name.
4. In the **Data Source** field, select required option.
 - *Database:* Data is generated from database tables.
 - *XML:* Data is generated from XML snapshots.
5. The system dynamically generates the report dataset structure from the XML snapshot metadata. Field IDs, field names, table IDs, and table names are automatically populated from the snapshot XML, eliminating the need to manually define field structures.
6. On the action bar, select **Generate Report Code** to create the AL code for the report. The report uses the enhanced XML metadata to build the dataset, ensuring accurate historical data representation.



7. On the action bar, select **Build and Deploy App Package** to deploy the report. The report is available for use with XML snapshot data.



Monitor pending pre-weigh verifications

Article • 4/22/2026 • 1 min read

The **Pending Pre-Weigh Verifications** cue on the Quality Manager Role Center displays the real-time count of warehouse pick lines awaiting second-person verification. The cue uses color-coded indicators to signal workload levels: normal for 10 or fewer, yellow alert for 11 to 50, and red critical for more than 50 pending verifications.

To monitor pending pre-weigh verifications, follow these steps:

1. Open the Quality Manager Role Center.

The **Pending Pre-Weigh Verifications** cue displays the current count of unverified lines.

2. Review the cue color to assess workload urgency:

- *Normal*: 10 or fewer pending verifications
- *Yellow*: 11 to 50 pending verifications
- *Red*: More than 50 pending verifications

3. Select the cue to navigate directly to the **Component Verification Workbench** filtered to pending approvals.

Note

The cue is visible only to users with verification permissions and is enabled only when the count is greater than zero.



Review pending pre-weigh verifications

Article • 4/22/2026 • 3 min read

The **Component Verification Workbench** provides a centralized view of production order components requiring pre-weigh verification. The page displays component-level summary information with FlowFields for picked quantities, approved quantities, variance, lot counts, and pending line counts, while a FactBox shows the lot-level pick line details for the selected component.

To review pending pre-weigh verifications, follow these steps

1. Select the Search icon , enter **Component Verification Workbench**, and then choose the related link.
The **Component Verification Workbench** page opens.
2. Optionally, in the **Pick No.** filter field, enter the warehouse activity number to focus on a specific pick document.
3. Optionally, use the **Location** and **Status** filters to narrow the list.
4. Select a component line to view its pick line details in the **Pick Lines** FactBox.
The FactBox displays the lot number, actual weight, weighed by, checked by, status, and rejection reason for each pick line.
5. To approve all pick lines for a component, select the component line and select **Approve All**.
6. To approve or reject individual pick lines, select the lines in the FactBox and select **Approve Selected** or **Reject Selected**.
7. Use the drill-down on FlowField columns such as **Picked Total Qty**, **Approved Total Qty**, or **Pending Lines Count** to view the underlying pick lines.

Note

Approval is always performed against warehouse activity lines (pick lines). A single electronic signature can cover multiple pick lines in a batch operation.



Approve pre-weighed ingredients

Article • 4/22/2026 • 2 min read

You can approve a single pre-weighed ingredient line using your electronic signature to record the verification for compliance and traceability. The approval records the approver's user ID, full name, and timestamp, and creates an immutable audit trail entry.

To approve a pre-weighed ingredient, follow these steps:

1. Select the Search icon , enter **Component Verification Workbench**, and then choose the related link.

The **Component Verification Workbench** page opens.

2. Select the verification line to approve.

3. Select **Approve**.

The electronic signature dialog opens.

4. Enter your username and password.

5. Select **OK** to confirm the approval.

The system validates the credentials, records the approval with the approver's user ID, full name, and timestamp, and updates the line status from *Pending* to *Approved*. A confirmation message displays with the approved item details.

Note

Once recorded, an approval cannot be undone. All approval actions are logged in the audit trail.



Approve multiple pre-weighed ingredients

Article • 4/22/2026 • 2 min read

You can approve multiple pre-weighed ingredient lines simultaneously with a single electronic signature for efficient batch processing. All selected lines receive the same timestamp and approver information, and individual audit trail entries are created for each line with a common batch reference. The operation is fully atomic, meaning that if any line update fails, the entire batch is rolled back.

To approve multiple pre-weighed ingredients, follow these steps:

1. Select the Search icon , enter **Component Verification Workbench**, and then choose the related link.

The **Component Verification Workbench** page opens.

2. Select the lines to approve using Ctrl+Click, Shift+Click, or **Select All**.

The selection count displays the number of selected items.

3. Select **Batch Approve**.

The electronic signature dialog opens displaying a summary of the selected items.

4. Enter your credentials and select **OK**.

The system approves all selected lines simultaneously with the same timestamp and approver information. A confirmation message displays the count of approved items.

Note

If any line fails validation during batch approval, the entire batch is rolled back to prevent inconsistent data states. The selection is cleared after successful batch approval.



View verification audit trail

Article • 4/22/2026 • 2 min read

Every pre-weigh verification event, whether an approval or rejection, is automatically logged through the Aptean eSignature framework into an immutable audit trail. Each entry captures the verifier identity, timestamps, item and lot details, weights, and a cryptographic signature token for 21 CFR Part 11 compliance. After posting, the verification record ID is stored on registered warehouse activity lines and item ledger entries for bi-directional traceability.

To view the verification audit trail, follow these steps:

1. Select the Search icon , enter **Item Ledger Entries**, and then choose the related link.
The **Item Ledger Entries** page opens.
2. Locate the consumption entry for the production order.
3. Review the **Verification Record ID** field, which links to the pre-weigh verification log entry.
4. Select the **Verification Record ID** to drill down to the verification audit log and view the full signature details including verifier name, timestamp, action, and signature token.

Note

The audit log is write-once. No user can update or delete audit log entries. Corrections require new compensating entries.



Search verification history

Article • 4/22/2026 • 3 min read

The **Pre-Weigh Verification History** page provides a centralized, read-only view of all pre-weigh verification audit log entries. You can search, filter, and export verification records for compliance review, audit inquiries, and batch release documentation. The page supports filters by date range, action type, verifier, item, lot, production order, and posted status, and includes export to Excel, PDF, or CSV.

To search verification history, follow these steps:

1. Select the Search icon  , enter **Pre-Weigh Verification History**, and then choose the related link.
The **Pre-Weigh Verification History** page opens.
2. Use the filter pane to narrow the results by date range, action type, verifier, item, production order, lot number, or posted status.
3. Review the summary statistics in the FactBox, which display the total records, approved count, rejected count, and date range.
4. To export the filtered results, select **Export to Excel**, **Export to PDF**, or **Export to CSV** from the reporting actions.
5. To generate a batch release report for a specific production order, select **Generate Batch Release Report**, enter the production order number, and select **OK**.
The report is saved as a document attachment on the production order.

 Note

The page is read-only. No insert, modify, or delete actions are available. Access is restricted to Quality, Compliance, and Admin roles.



View blocked posting attempts

Article • 4/22/2026 • 2 min read

When a user attempts to post or process ingredients that have not been verified, the system blocks the operation and logs the attempt in a tamper-proof enforcement audit log. Each blocked attempt records the user's identity, document type and number, unverified item and lot details, weights, and timestamp. The error message includes a unique log ID for traceability.

To view blocked posting attempts, follow these steps:

1. Select the Search icon , enter **Pre-Weigh Verification History**, and then choose the related link.
The **Pre-Weigh Verification History** page opens.
2. Use the filter to select **Show Enforcement Events** to display only blocked posting attempts.
Blocked attempts are visually distinguished with a red icon and a *Blocked* status.
3. Review the enforcement log entries, which include the user ID, document type, document number, blocked reason, count of unverified lines, and the details of each unverified line.
4. Select an entry to view the full details including the item numbers, lot numbers, and weights of each unverified line.

 Note

The enforcement log is write-once and cannot be modified or deleted. Each posting attempt creates a separate log entry. The error message shown to the blocked user includes the log ID for cross-referencing.



Reject a pre-weighed verification line

Article • 4/22/2026 • 3 min read

You can reject a pre-weighed ingredient line when a discrepancy or quality concern is identified during verification. The rejection requires a standardized reason code and an optional comment, is recorded in the eSignature audit trail, and triggers a re-weigh workflow for the rejected line. If the rejection count for a line exceeds the configured threshold, the system escalates to supervisor review.

To reject a pre-weighed verification line, follow these steps:

1. Select the Search icon , enter **Component Verification Workbench**, and then choose the related link.

The **Component Verification Workbench** page opens.

2. Select the verification line to reject.

3. Select **Reject**.

The rejection dialog opens, displaying a summary of the item number, lot number, and actual weight.

4. In the **Rejection Reason** field, select the reason for rejection. The available options are:

- *Weight Discrepancy*
- *Damaged Material*
- *Incorrect Item*
- *Incorrect Lot*
- *Contamination Suspected*
- *Packaging Issue*
- *Other*

5. In the **Comment** field, enter additional details about the rejection.

Note

The comment is mandatory when the rejection reason is *Other*.

6. Select **Reject and Re-Weigh**.

The electronic signature dialog opens.

7. Enter your credentials and select **OK**.

The line status changes to *Rejected* and the weigh status changes to *Pending Re-Weigh*. The rejection is logged in the audit trail and the line's rejection count is incremented.



 Note

If the rejection count exceeds 2, the system triggers an escalation notification to the quality supervisor. The rejected line appears in the *Pending Re-Weigh* view on the warehouse pick for the operator to re-weigh the material.



Batch reject verification lines

Article • 4/22/2026 • 3 min read

You can reject multiple pre-weighed verification lines simultaneously in a single action, applying one rejection reason and comment to all selected entries. The batch rejection processes all lines in a single atomic transaction with a single electronic signature, and individual audit trail entries are created for each line linked to a common batch rejection event.

To batch reject verification lines, follow these steps:

1. Select the Search icon , enter **Component Verification Workbench**, and then choose the related link.
The **Component Verification Workbench** page opens.
2. Select the lines to reject using Ctrl+Click, Shift+Click, or **Select All**.
3. Select **Reject Selected**.
The batch rejection dialog opens, displaying the number of lines selected and total weight affected.
4. In the **Rejection Reason** field, select the reason for rejection. The selected reason applies to all lines.
5. In the **Comment** field, enter additional details. The comment applies to all selected lines.

! Note

The comment is mandatory when the rejection reason is *Other*.

6. Select **Reject and Re-Weigh**.
A confirmation prompt displays: "This will reject [X] lines and trigger re-weigh for all. Continue?"
7. Select **Yes** to confirm, then enter your electronic signature credentials.
All selected lines are rejected in a single transaction. A confirmation message displays the count of rejected lines.

! Note

If any line fails validation during batch rejection, the entire batch is rolled back. Batch rejection supports up to 100 lines. For batches exceeding 100 lines, a performance warning is displayed before processing.



Integrations

Article • 8/27/2025 • 1 min read

The Aptean eSignature extension has been integrated with the following extensions:

- [Aptean Status Management](#)
- [Aptean Advanced Attributes](#)
- [Aptean Approved Supplier](#)
- [Aptean Audit Trail](#)
- [Aptean Quality Control \(BC\)](#)
- [Aptean License and Subscription Management](#)
- [Aptean Inspection Status](#)
- [Aptean Production Scenarios](#)
- [Aptean Non Conformances](#)
- [Aptean Filter Group](#)
- [Aptean Compliance Documents](#)
- [Aptean Process Manufacturing](#)
- [Aptean Vendor Item Catalog](#)



Aptean Advanced Attributes

Article • 8/27/2025 • 1 min read

The Aptean [Advanced Attributes](#) extension must be installed to use the Aptean eSignature extension to ensure digital signature capability for managing critical data changes and attribute modifications.



Aptean Approved Supplier

Article • 8/27/2025 • 1 min read

The Aptean [Approved Supplier](#) extension must be installed to use the Aptean eSignature extension to enhance approved supplier processes with digital signature requirements.



Aptean Status Management

Article • 8/28/2025 • 1 min read

The Aptean [Status Management](#) extension must be installed to use the Aptean eSignature extension, you can configure status management flows to integrate eSignature requirements into document approval workflows. For more information, see [Use e-signature in a production order](#).



Aptean Audit Trail

Article • 8/27/2025 • 1 min read

The Aptean [Audit Trail](#) extension must be installed with the Aptean eSignature extension to ensure comprehensive tracking and logging of signature activities, ensuring audit compliance.



Aptean Compliance Documents

Article • 8/27/2025 • 1 min read

The Aptean [Compliance Documents](#) extension must be installed to use the Aptean eSignature extension to ensures compliance through mandatory digital signatures on critical documentation and approval workflows.



Aptean Filter Group

Article • 8/27/2025 • 1 min read

The Aptean [Filter Group](#) extension must be installed to use the Aptean eSignature extension to support approval workflows for filter group configuration and access control using digital signatures.



Aptean Inspection Status

Article • 8/27/2025 • 1 min read

The Aptean [Inspection Status](#) extension must be installed to use the Aptean eSignature extension to include digital signature requirements within inspection workflows and status updates.



Aptean License and Subscription Management

Article • 8/27/2025 • 1 min read

The Aptean [License and Subscription Management](#) extension must be installed to use the Aptean eSignature extension to manage license and subscription approval processes with digital signature validations.



Aptean Non Conformances

Article • 8/27/2025 • 1 min read

The Aptean [Non Conformances](#) extension must be installed to use the Aptean eSignature extension to include the required digital signatures during non-conformance resolution and corrective action processes.



Aptean Process Manufacturing

Article • 8/27/2025 • 1 min read

The Aptean [Process Manufacturing](#) extension must be installed to use the Aptean eSignature extension to ensure manufacturing documentation go through mandatory digital signatures on critical documentation and approval workflows.



Aptean Production Scenarios

Article • 8/27/2025 • 1 min read

The Aptean [Production Scenarios](#) extension must be installed to use the Aptean eSignature extension to include digital signatures for production scenario approvals and process validations.



Aptean Quality Control (BC)

Article • 8/27/2025 • 1 min read

The Aptean [Quality Control \(BC\)](#) extension must be installed to use the Aptean eSignature extension to enhance quality control processes with digital signature requirements.



Aptean Vendor Item Catalog

Article • 8/27/2025 • 1 min read

When the Aptean [Vendor Item Catalog](#) extension is used in conjunction with the Aptean eSignature extension, you can enable eSignature requirements for vendor approval workflows. This ensures full compliance and audit trails for vendor-related status changes that require authorized approval within the system. For more information, see [Manage vendor status log](#).

