System administration home page

Article • 12/05/2024

This article points to content for system administrators of finance and operations. This content will help you configure the system so that it works smoothly and effectively for your organization.

One Version

In July 2018 we announced a change to the way we deliver Dynamics 365 updates that will help you stay current in a consistent, predictable, and seamless manner. The following topics are intended to provide clarity on the finance and operations service updates, processes, and tools you can use to stay current.

- One Version service updates overview
- One Version service updates FAQ
- Service update availability
- Apply updates to cloud environments
- Configure service updates through Lifecycle Services (LCS)
- Pause service updates through Lifecycle Services (LCS)
- Get notified about service updates through Lifecycle Services (LCS)

Implementation management with Lifecycle Services

Microsoft Dynamics Lifecycle Services (LCS) is a collaboration portal that provides an environment and a set of regularly updated services that can help you manage the lifecycle of your finance and operations implementations.

The lifecycle of an implementation spans many phases from pre-sales through Analysis, Design and Development, Test, and Deployment to Operation, possibly in multiple iterative roll-outs. It can last a few months to multiple years, based on the scope and complexity of the project and the chosen deployment model, for example, in the managed cloud or on-premises.

The management of the implementation involves many different stakeholders from the customer and partner organizations and, especially in the cloud-hosted deployment model, from Microsoft. The implementation is supported through tools provided on LCS and through processes defined within the Microsoft FastTrack and through the partner's implementation approach.

Add links to your organization's legal terms and privacy statement

Article • 12/31/2024

This article explains how administrators can add links to their organization's legal terms and privacy statement in the **About** pane of Microsoft Dynamics 365 Finance, Supply Chain Management, and Commerce.

Organizations often need to ensure that the links to their legal terms and privacy statement are readily available and visible to users in order to meet legal and compliance requirements. Administrators of an organization can follow these steps to have the links to their legal terms and privacy statement be available in the **About** pane (**Settings** > **About**).

Add links

1. Go to the **System parameters** page and click **Legal and Privacy.** On this page:

    a. Enter the link to a page that outlines the legal terms for your organization.

    b. Enter the link to a page that outlines the privacy statement for your organization.

    > ⓘ **Note**
    >
    > Make sure that you enter the full URL, starting with either *https* or *http*.

2. Click **Save**.

3. If you are using Commerce, go to the **Distribution schedules** page. On this page:

    a. Select the **1110 – Global configuration** job.

    b. Click **Run now**.

    > ⓘ **Note**
    >
    > To verify that the job completed, go to the **Download sessions** page.

User security role reporting and technical validation for finance and operations apps FAQ

Article • 04/19/2025

This article answers frequently asked questions about feature user license validation for user security roles. It focuses specifically on questions about licensing assignment and reporting for finance and operations apps.

On March 28, 2025, Microsoft released a blog post to introduce updates that help centralize user license management and provide clarity for administrators.

As of **April 30, 2025**, administrators have access to license usage reporting that shows available and assigned licenses. In addition, users who don't have a license assigned to them start to receive in-product notifications that instruct them to contact their administrator to request license assignment.

As of **August 30, 2025**, only users who have a license assigned to them can access finance and operations apps. Microsoft is announcing this change now, so that customers have time to prepare tools and training to support any action that is required. For users who already have licenses assigned to them, there is no disruption, and no administrator action is required.

> **Important**
>
> Currently, user license validation is applicable only to commercial cloud solutions.

How can I learn more about the licensing model?

To learn more about the licensing model, visit the Dynamics 365 Licensing page. There, you can find comprehensive resources, including the Dynamics 365 Licensing Guide and Dynamics 365 Licensing Deck. You can also contact your Microsoft account team or your implementation partner for support.

What is changing on April 30, 2025?

Two key developments are scheduled for April 30, 2025:

- Users who lack the correct licenses start to receive notifications in finance and operations apps. These notifications instruct the users to request the required licenses from their

License codes and configuration keys report

Article • 07/01/2022

This article points you to a report that lists the license codes and configuration keys available in finance and operations.

When you purchase finance and operations, all functionality is included. By default, some features and functionality that you do not use may be enabled. The administrator should disable the features that are not needed by disabling license codes and configuration keys.

When a license code or configuration key is disabled, the associated module or feature is removed from the user interface. Large sets of functionality, such as modules, are controlled by license codes. Many license codes, in turn, enable configuration keys that allow you to enable and disable functionality at a more detailed level.

To view the report

The **License codes and configuration keys report**, included with the Technical reference reports, lists each configuration key that is available. The report also indicates the license code and menu items associated with each configuration key.

Feedback

Cross-company data sharing overview

Article • 02/19/2025

Cross-company data sharing concept allows you to share company specific master, reference, and setup data across companies within finance and operations deployment.

Two data sharing concepts are available:

> **Note**
>
> Master Company Data Sharing is GA in 10.0.43.

- Duplicate record sharing (DRS) is a concept where creating, updating, or deleting of records in for any company in the policy is copied/replicated across all companies in the policy. Updates of fields replicates if selected for sharing in the policy. DRS was the first sharing type made available.
- Master company sharing, also known as single record sharing (SRS), is a concept where a single physical record belonging to a master company is virtually shared across child companies. Create, update, or delete in any company in the policy updates the single records used across all companies.

Why should you consider cross-company data sharing?

You should consider cross-company data sharing if you need consistent data across more than one company in a deployment. There might be hundreds of companies in a deployment and the business requires that at any time, these companies can rely on a single version of truth for critical data.

Here are some examples of business scenarios for cross-company data sharing:

- All customers should always be available to service and have the same terms across all companies.
- Terms for payment and delivery should always be aligned across all companies per region.
- Configuration for cash and bank management parameters must be aligned to secure consistent processing across all companies.

Using roles and security configuration it's possible to centralize maintenance of shared tables by only providing permissions to selected users in selected companies.

Tables supported for duplicate record data sharing

Article • 09/09/2023

This list describes the tables supported for duplicate record data sharing. Duplicate record data sharing is a mechanism for sharing reference and group data among companies in a deployment. It might be possible to add additional tables to duplicate record data sharing policies, however, any table not listed in the following tables is not officially supported.

Dynamics 365 Finance

Expand table

Table object Name	Table description (Label)
AssetCondition	Fixed asset condition
AssetBookTable	Fixed asset book setup
AssetGroup	Fixed asset groups
AssetLedger	Fixed asset posting profile
AssetLedgerAccounts	Fixed asset posting profile
BankCentralBankPurpose	Payment purpose codes
BankChequeLayout	Check layout
BankGroup	Bank groups
BankParameters	Bank parameters
BankTransType	Bank transaction type
CashDisc	Cash discount
CompanyNAFCode	NAF codes
CredManAccountStatusTable	Account statuses
CredManCollectionsGroupTable	Collection groups
CredManGroup	Credit management groups
CredManReasonTable	Reason table

Cross-company data sharing for developers

Article • 01/10/2024

This article describes cross-company data sharing for developers. Cross-company data sharing is a mechanism for sharing reference and group data among companies in a deployment.

Enable a table for cross-company data sharing

Enabling a table for data sharing is a two-step process that requires updating the metadata property for the table. To enable a custom table for cross-company data sharing, follow these steps.

1. Open the table properties, and set the **Data Sharing Type** property to **Single** or **Duplicate**. **Single** stands for single record sharing (SRS), and **Duplicate** stands for duplicate record sharing (DRS).
2. For each field on the table, you must review the **Single Data Sharing Type** metadata property. **Always** is the default value and implies that the field is always shared. **Never** implies that the field is never shared. Don't select **Optional**, because there isn't currently any related logic.

> **Note**
>
> - When a table is set as **Duplicate**, it can participate in both DRS and SRS policies.
> - When a table is set to **Single**, it can participate only in SRS policies.
> - When a table property is set to **Duplicate**, it can't be changed to **Single**. This change is considered a breaking change, because DRS policies that use the table would no longer be valid.
> - When you use SRS, fields that are set to **Never** get the default value for the field's type in all child companies. You can't update these fields to a different value in a child company. For example, if an integer/real field has a value of **0**, strings will be empty, and enumerations will be nondeterministic, based on whether they're extensible.

Maintenance mode

Article • 01/30/2024

This article provides information about maintenance mode in finance and operations apps. When maintenance mode is turned on, it provides a safe way for system administrators to make system changes that might affect system functionality. For example, configuration keys can be enabled or disabled. While maintenance mode is on, only system administrators and users who have the **Maintenance mode user** role can sign in to the system. By default, maintenance mode is turned off. When maintenance mode is off, you can't edit the **License configuration** page.

> ⓘ **Note**
>
> After enabling maintenance mode on an environment, only one interactive AOS and one non-interactive AOS (batch AOS) is available for use.

Turn maintenance mode on and off on sandbox and production environments through Lifecycle Services

You can now turn maintenance mode on and off directly through Microsoft Dynamics 365 Lifecycle Services on your sandbox and production environments.

To turn maintenance mode on and off directly through Lifecycle Services, follow these steps.

1. Go to the environment details page and on the **Maintain** menu, click **Enable Maintenance Mode**.
2. In the slider, set **Turn maintenance mode on** for the environment and select **Confirm**.
3. A servicing operation begins and your system goes into maintenance mode.
4. On completion, the environment state is **In Maintenance**. At this point, only the system administrator has access to the environment.
5. After you're done making system-wide changes, you can turn off maintenance mode by clicking **Disable Maintenance Mode** under the **Maintain** menu.
6. A servicing operation starts and takes your environment out of maintenance mode. You can see the progress of the operation in the environment details page.

Preconfigured system accounts

Article • 06/27/2024

Preconfigured system accounts are included on deployed environments so that Microsoft can manage and operate the finance and operations service and provide specific features to customers. The following table provides information about each account, including the purpose and use case for the account.

> **Important**
>
> Do not delete these system accounts. Deleting these accounts will cause a disruption in key functionality provided by Microsoft.

Expand table

Account	Purpose/use case
Axrunner	Monitoring the health of the environment, and providing alerts as required. **Note:** This account is deprecated for self-service environments and is no longer used.
DataSyncFrameworkApp	Used by Microsoft Power Platform apps that are provided by Microsoft to synchronize data from finance and operations virtual tables in Dataverse, based on row version change tracking.
DataverseSearchApp	Used for synchronizing data from finance and operations apps to Microsoft Azure Cognitive Services through Dataverse virtual tables that have row version change tracking. This account enables global search functionality for finance and operations data on Microsoft Power Platform apps.
DynamicsMaintAppUser	Performing deployment and service operations in finance and operations apps.
FRServiceUser	The Financial Reporting service user account. The Management Reporter application uses this account for integrations with finance and operations apps.
MonitoringAppUser	Used as part of **Geneva Synthetics Monitoring in FnO** to help identify availability or functionality loss issues in customer environments and contribute to CRI reduction.

Export business-to-business (B2B) users to Microsoft Entra ID

Article • 03/08/2024

You can automatically export business-to-business (B2B) users to Microsoft Entra ID.

In the past, B2B users were exported manually to a .csv file. Then the Microsoft Entra tenant administrator had to use this file to manually add the users to Microsoft Entra using the Azure portal.

To enable the automatic export feature, a one-time setup and configuration process must be completed. When the process is completed, you can use the **Provision Microsoft Entra B2B user** workflow task to automatically export B2B users to Microsoft Entra ID.

The one-time set up and configuration means that you'll need to:

1. Set up a B2B invitation service application in Microsoft Entra ID.
2. Configure the B2B invitation service settings in finance and operations.

Set up a B2B invitation service application in Microsoft Entra ID

The tenant administrator of your Microsoft Entra tenant will need to complete the following steps.

1. Log on to the Azure portal as the tenant administrator.
2. Click **Microsoft Entra ID** > **Properties**.
3. Copy the **Directory ID** (this is the tenant ID) and save it. You will need this later.
4. Click **App registrations** > **New application registration**.
5. Enter the following information, and then click **Create**.
   a. In the **Name** field, enter the name of the application. For example: **B2B admin application**.
   b. In the **Application type** field, select **Web app /API**.
   c. In the **Sign-on URL** field, enter the URL for finance and operations.
6. Click the **App registrations** tab, click the newly created application, copy the **Application ID**, and save it. You will need this later.

Data maintenance

Article • 06/10/2024

Data maintenance enables simple scheduling processes that you can run to find or correct data inconsistencies in your environment.

Incorrect data can adversely affect your day-to-day, monthly, and yearly operations. Inconsistencies and errors that come from incorrect data has the potential to halt major events like year-end activities and can even halt your daily revenue streams and affect your organization's decision-making capabilities.

The *Data Maintenance Portal* is a tool that lets system administrators schedule and run various actions that will have a direct effect on the data or the system. Some actions can be scheduled to continuously look for opportunities to fix issues, and others can be run on demand to enact some change on the system. Currently there are three basic types of actions: direct, scanning, and fixing.

Types of actions

- *Direct actions* can be run on-demand only, and can run tasks directly. Microsoft Support may use direct actions, which could be as simple as clearing a cache without the need for downtime or as complicated as running a reference scanner to aid the support process.
- *Scanning actions* will search your data, a few times a day, looking for problems in the data. The problems found will be reported to Microsoft. There are a number of system actions that may not yet have an automated fix, but will provide valuable data to Microsoft to improve the health of your data. Microsoft may reach out to you regarding problems found through this method.
- *Fixing actions* runs on the same cadence as a scanning action, but when an opportunity is found, it will schedule a fix to the data. Fixing actions are meant to be data idempotent and may not fix all of the data on the first run. We recommend that a fixing action only fixes a subset of data each time it runs. Over time, the data will reach a clean state without exposing a significant load on the system. This type of action may help facilitate an in-place upgrade of your system.

Control of actions

Manage access to network printers across legal entities

Article • 07/01/2022

> **Important**
>
> Access to the System administration utility is managed by the Carbon Flighting Service. The **System network printers management** page is only available for system admins.

Domain admins register network printers with the finance and operations service by using the Document Routing Agent (DRA). After the printers are registered, the organization admin is responsible for making them available to users. The settings are managed on the **Manage network printers** page (**Organization administration** > **Setup** > **Network printers**).

Because the settings on the **Manage network printers** page are intended for organization admins, the data is limited to the active legal entity. Because system admins can't manage network printer settings across legal entities, it can be difficult to update settings across legal entities in some situations, such as when network printer changes occur. For example, a network printer instance is deleted when a network printer path is updated or hardware is replaced, or someone tries to purge all documents in the printer queue.

The System administration utility is a recovery tool for inadvertent print instructions. It also simplifies the task of managing network printer settings, such as access from specific legal entities.

Access the feature

After the feature has been turned on, a **Preview** group will appear on the **Options** tab of the Action Pane on the **Manage network printers** page.

Monitoring and Telemetry using Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management

Learn how to implement a monitoring solution to capture and analyze telemetry for Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management.

About Monitoring and Telemetry

OVERVIEW

Monitoring and Telemetry Feature overview

Getting started

Available telemetry

CONCEPT

Gathering requirements for monitoring

Understanding and controlling cost

For developers

CONCEPT

Adding your custom telemetry signals

REFERENCE

Telemetry data model

Application Insights API for custom events and metrics

Analyzing telemetry

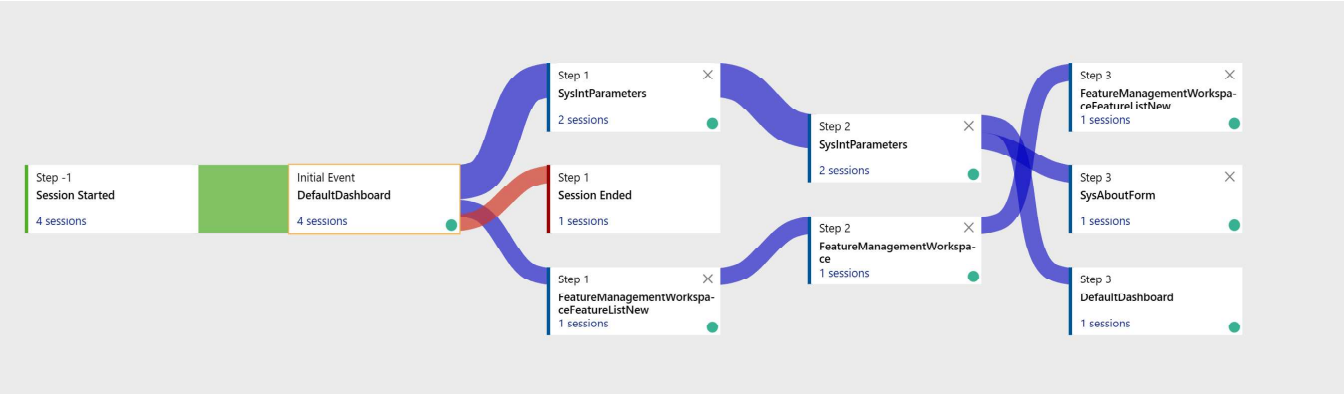
Monitoring and telemetry overview

Article • 01/17/2025

The Monitoring and telemetry feature is a direct, point-to-point integration between an instance of Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management and the target Azure Application Insights destination. Azure Application Insights is a service that is hosted in Azure, and that gathers telemetry data for analysis and presentation.

This feature addresses the following needs:

- Gather telemetry to gain insights into how the application is used.
- Let developers and admins gather additional information in diagnosing scenarios.
- Improve efficiency in issue detection, diagnosis, and troubleshooting, and therefore reduce the overall time to resolution.
- Enable proactive alerting through standard capabilities that Azure Application Insights provides.



> **Note**
>
> Microsoft doesn't collect the emitted telemetry for support or other operational reporting. Instead, the data is customer-owned and customer-driven.

Gather monitoring requirements

It's easy and straightforward to configure and enable telemetry signals so that you can get the signals that are provided out of the box. However, before you can build the right experience for your team, it's important that you define the correct set of requirements that the monitoring solution must meet. Learn more in Gather monitoring requirements.

Get started

Available telemetry

Article • 01/30/2025

Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management include robust, out-of-box telemetry capabilities when Application Insights is enabled. These capabilities provide critical insights into various aspects of the system and help customers monitor performance, diagnose issues, and optimize operations. This article provides an overview of the types of telemetry that are available and corresponding resources.

Form run telemetry

Form run telemetry captures detailed information about forms within the application. It provides insights into the following details:

- The forms that were opened
- The users who accessed the forms
- Load times for the forms

Customers can use this data for the following purposes:

- Analyze average load times, P90s, and other performance metrics to improve the user experience.
- Identify frequently accessed forms, and optimize them for better usability.
- Detect patterns in user behavior to enhance form design and navigation.
- Monitor trends in form usage to prioritize resources and updates effectively.

Resources

- Plug-and-play dashboard: Forms Telemetry Dashboard

X++ exceptions

All exceptions that occur in the X++ layer are captured and logged to Application Insights. Customers can use this telemetry for the following purposes:

- Monitor and diagnose application errors to maintain application stability.
- Track exception trends over time to identify recurring issues.
- Prioritize resolution efforts based on the frequency and severity of exceptions.
- Analyze the impact of exceptions on user operations and workflows.

Gather monitoring requirements

Article • 01/20/2025

To build an effective monitoring and telemetry solution in finance and operations apps, it's crucial that you define the correct set of requirements. This approach also ensures that the solution is aligned with your team's needs and delivers actionable insights that help maintain the health of your applications. Use the information in this article to establish a strong foundation for your monitoring and telemetry strategy.

Understand your business objectives

Begin by identifying the overarching goals (objectives) that your monitoring solution should support. These objectives should be aligned with the strategic priorities of your organization.

Examples of objectives:

- Reduce downtime, and improve system availability.
- Optimize performance to enhance the user experience.
- Monitor compliance with Service Level Agreements (SLAs).
- Gain visibility into key business processes.

Identify key stakeholders

Gather input from all stakeholders who will use or benefit from the monitoring solution.

Common stakeholders:

- IT Operations teams
- Development teams
- Product managers
- Customer support teams
- Executive leadership

Sample questions to ask stakeholders:

- What information is critical for your role?
- What issues or pain points do you face today?
- How do you plan to use telemetry data in your workflows?

Get started with telemetry for finance and operations apps

Article • 01/20/2025

This article explains how to start to send telemetry from Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management environments to Azure Application Insights.

To configure your environments to send telemetry to Azure Application Insights, follow these steps.

1. Set up an Application Insights resource in Azure.
2. Enable the **Monitoring and Telemetry** feature in Finance and Supply Chain Management.
3. Configure environments to link to the correct Azure Application Insights resources.
4. Configure the type of telemetry that must be sent to Azure Application Insights.

Set up an Application Insights resource in Azure

To get started, you must create a Azure Application Insights resource in Azure if you don't already have one. Learn more in Workspace-based Application Insights resources.

Enable the Monitoring and telemetry feature

To enable the Monitoring and telemetry feature, follow these steps.

1. In Finance and Supply Chain Management, open the **Feature management** workspace.
2. Filter the feature list to find the **Monitoring and Telemetry** feature. Select the feature, and then select **Enable**.

Analyze and monitor telemetry with KQL

Article • 01/17/2025

Telemetry from Microsoft Dynamics 365 Finance and Dynamics 365 Supply Chain Management is stored in Application Insights. To query that telemetry, the Kusto Query Language (KQL) is used. This article provides information and links to resources to help you learn about KQL.

Run your first KQL query

To run your first KQL (Kusto) query, follow these steps.

1. In the Azure portal, open your Application Insights resource.
2. On the **Monitoring** menu, select **Logs**.
3. To get the last 100 traces, on the **New Query** tab, enter the following query.

```kql
pageViews
| where timestamp > ago(7d)                                    // look back 7
days
| take 100                                                     // only take
100 rows
| project timestamp, name, duration, customDimensions          // only choose
these columns
| sort by timestamp desc                                       // show the
most recent data first
```

Where can I use Kusto queries?

You can use Kusto queries as the data source in many places. Here are some examples:

- The **logs** part of Application Insights in the Azure portal
- Power BI reports
- Alerts
- Azure dashboards
- Jupyter notebooks (with the Kqlmagic extension)

Use telemetry-based alerts

Article • 01/17/2025

When a Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management environment is emitting telemetry to Azure Application Insights, that telemetry can be used to create proactive alerts. Here are some examples of alerting:

- Notify stakeholders when someone changes a customer bank account.
- Notify system administrators when specific form loads are taking longer than usual.
- Get notifications when specific errors occur in nightly batch jobs.

You can use the following tools to define and set up alerts on telemetry events:

- Azure Application Insights Alerts
- Power BI metrics
- Azure Logic Apps
- Power Automate

No-code alerting with Power BI Metrics

If you use the Power BI app on telemetry data, it's easy to track the metrics that are important to you.

With metrics in Power BI, you can curate your own metrics and track them against key business objectives in a single pane. This feature enhances data culture by promoting accountability, alignment, and visibility for teams and initiatives within organizations.

Follow this four-step process to set up alerting with Power BI Metrics.

1. Create a scorecard in the Power BI service. Learn more in Create scorecards and manual metrics in Power BI.
2. Add the *metrics* that you want to track by connecting to your Power BI report on telemetry. Learn more in Create connected goals in Power BI.
3. Add alerting by defining status rules for your metrics. Statuses are then automatically updated based on the rules that govern each metric. Because the rules trigger changes based on the value, the percentage of the target that was met, date conditions, or a combination of the three, they are very versatile. For connected metrics, the status rules are refreshed every time the data on the scorecard is updated. Learn more in Create automated status rules for metrics.

Add custom telemetry signals

Article • 01/17/2025

When the Monitoring and telemetry feature is activated, telemetry is emitted to Azure Application Insights. Some telemetry is emitted out of the box. However, you can also provide extensions to add your own custom telemetry signals. These signals can provide more insights into your custom processes.

Telemetry logger

The main entry point for logging custom telemetry is through the `SysApplicationInsightsTelemetryLogger` class. This class encapsulates the Azure Application Insights telemetry client and provides access to the operations that are required to track an event, page view, trace, exception, or metric.

The logger uses the static constructor pattern to ensure a singleton instance per user session. The encapsulated Azure Application Insights telemetry client is further cached to ensure that only one telemetry client is created per Application Object Server (AOS) instance.

Telemetry data contract types

Microsoft Dynamics 365 Finance and Microsoft Dynamics 365 Supply Chain Management currently support the following types of data contracts.

Expand table

Type	X++ class	Application Insights data type
Event	SysApplicationInsightsEventTelemetry	Microsoft.ApplicationInsights.DataContracts.EventTelemetry
PageView	SysApplicationInsightsPageViewTelemetry	Microsoft.ApplicationInsights.DataContracts.PageViewTelemetry
Exception	SysApplicationInsightsExceptionTelemetry	Microsoft.ApplicationInsights.DataContracts.ExceptionTelemetry
Trace	SysApplicationInsightsTraceTelemetry	Microsoft.ApplicationInsights.DataContracts.TraceTelemetry

Events

To log a custom event to Azure Application Insights, you can create an instance of the `SysApplicationInsightsEventTelemetry` class and pass in the necessary payload. Then use the `trackEvent` method on the `SysApplicationInsightsTelemetryLogger` class to emit the event.

The following example shows how to emit an event when a record is created in the `SysUserLog` table.

```
X++
```

Understand and control costs

Article • 01/17/2025

Management of telemetry costs in finance and operations apps is crucial, because data that is sent to Azure Application Insights incurs charges based on many factors. By implementing effective strategies, you can help control these expenses and also maintain robust monitoring. The guidelines and resources in this article come from both the Microsoft Dynamics 365 Application Insights team and the Azure Application Insights team.

Understand telemetry costs

Azure Application Insights is an extension on top of Azure Monitor. Although many factors drive the cost of Azure Monitor, the main drivers are the ingestion and retention of data. Azure Application Insights provides the tools that you need to gain insights into the current usage. It also provides ways to automate the retrieval of usage cost information, and ways to set thresholds and alert when those thresholds are exceeded.

Learn more about all the cost factors in Azure Monitor cost and usage.

Strategies for controlling telemetry costs

You can use the following strategies to control telemetry costs.

Selective telemetry collection

- **Production environment focus –** Configure Application Insights to collect only essential telemetry in production environments. This approach reduces data volume and associated costs.
- **Custom telemetry management –** Be careful when you add custom telemetry. Ensure that any other data that is collected provides value that is significant enough to justify the cost.

Data retention policies

- **Archiving practices –** Regularly archive telemetry data that is more than 30 days old to more cost-effective storage solutions. This approach helps you manage storage costs and also lets you retain access to historical data.

Role-based security

Article • 04/02/2024

This article provides an overview of the elements of role-based security in finance and operations.

In role-based security, access isn't granted to individual users, only to security roles. Users are assigned to roles. A user who is assigned to a security role has access to the set of privileges that is associated with that role. A user who isn't assigned to any role has no privileges.

In finance and operations apps, role-based security is aligned with the structure of the business. Users are assigned to security roles based on their responsibilities in the organization and their participation in business processes. The administrator grants access to the duties that users in a role perform, not to the program elements that users must use.

Because rules can be set up for automatic role assignment, the administrator doesn't have to be involved every time that a user's responsibilities change. After security roles and rules have been set up, business managers can control day-to-day user access based on business data.

Overview of role-based security

This section provides an overview of the elements of role-based security. The security model is hierarchical, and each element in the hierarchy represents a different level of detail. Permissions represent access to individual securable objects, such as menu items and tables. Privileges are composed of permissions and represent access to tasks, such as canceling payments and processing deposits. Duties are composed of privileges and represent parts of a business process, such as maintaining bank transactions. Both duties and privileges can be assigned to roles to grant access to finance and operations.

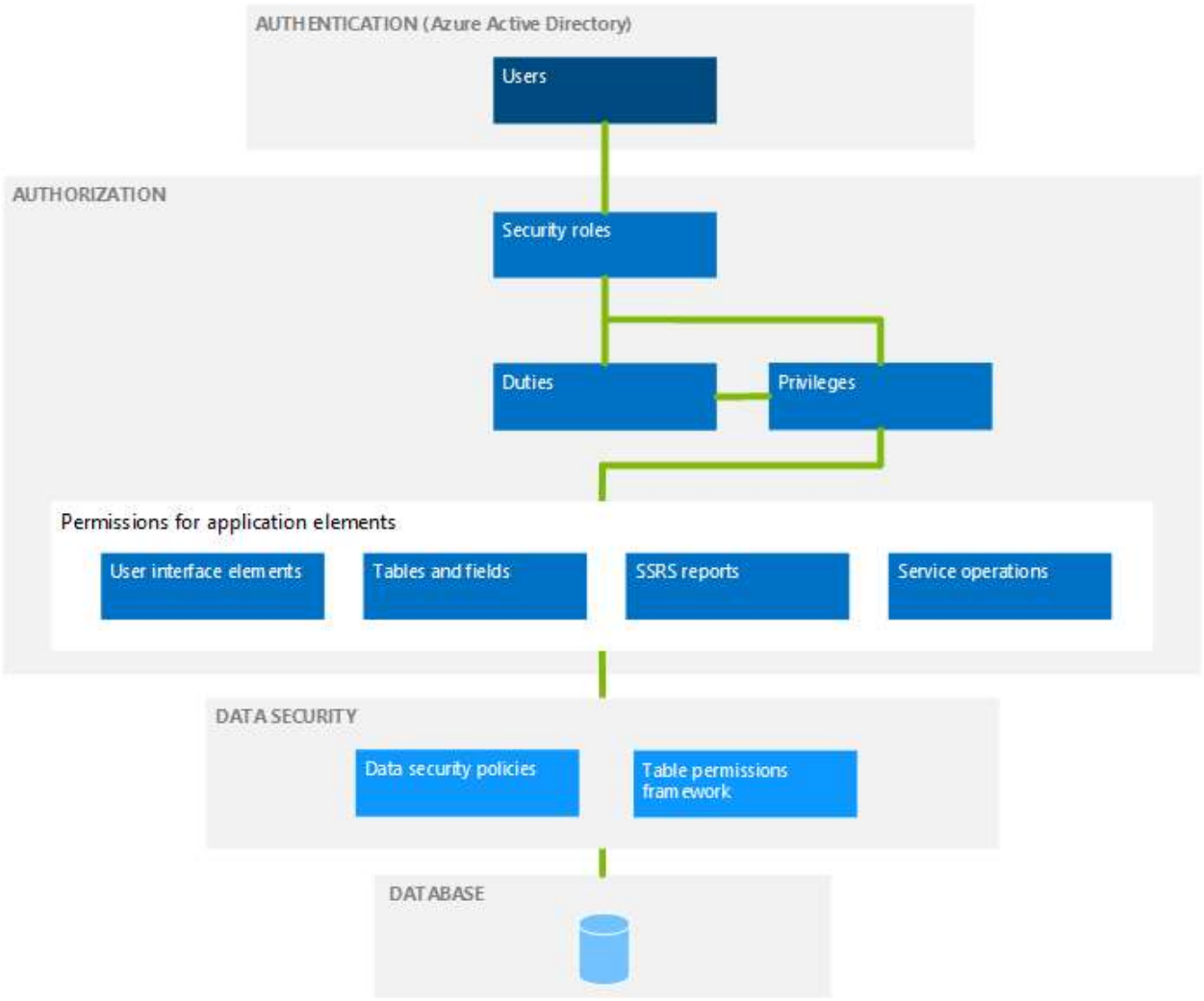
The following illustration shows the elements of role-based security and their relationships.

Security architecture

Article • 03/08/2024

This article provides an overview of the security architecture of finance and operations.

When you understand the security architecture, you can more easily customize security to fit the requirements of your business. The following diagram provides a high-level overview of the security architecture.



Authentication

By default, only authenticated users who have user rights can establish a connection.

Microsoft Entra ID is a primary identity provider. To access the system, users must be provisioned into a finance and operations instance and should have a valid Microsoft Entra account in an authorized tenant.

Authorization

Finance and operations storage account security updates

Article • 01/17/2025

This article describes the latest security enhancements in the finance and operations storage account.

Frequently asked questions

I receive the following error on my developer machine/customer-hosted environment: "Fetching a valid storage connection string is disabled." How can I fix this error?

The **Microsoft.Dynamics.Clx.ServicesWrapper.CloudInfrastructure::GetCsuStorageConnectionString()** public method is being deprecated. Learn more in End of support for sharing storage account connection strings via public API GetCsuStorageConnectionString.

If the flight is set to *false* by default, an issue occurs when changes are deployed in developer environments or customer-hosted environments (CHEs). In this case, you receive the following error on your developer machine:

> EnableSharingOfValidStorageConnectionString is false. Fetching a valid storage connection string has been disabled.

If you receive the error, follow these steps.

1. In Microsoft SQL Server Management Studio (SSMS), run the following query.

```SQL
declare @flightName NVARCHAR(100) =
'EnableSharingOfValidStorageConnectionString';
IF NOT EXISTS (SELECT TOP 1 1 FROM SysFlighting WHERE flightName =
@flightName)
INSERT INTO SYSFLIGHTING(FLIGHTNAME,ENABLED, FLIGHTSERVICEID,PARTITION)
SELECT @flightName, 1, 12719367,RECID FROM DBO.[PARTITIONS];
ELSE
UPDATE SysFlighting SET enabled = 1, flightServiceId = 12719367 WHERE
flightName = @flightName;
```

Encryption in finance and operations apps

Article • 08/12/2022

Encryption at rest

Microsoft uses encryption technology to protect customer data while at rest in an environment's SQL Server database and Azure Storage.

All instances utilize Microsoft SQL Server Transparent Data Encryption (TDE) and Azure Storage encryption to perform real-time encryption of data when written to the disk at rest.

Finance and operations apps use server-side encryption using service-managed keys. All key management aspects such as key issuance, rotation, and backup are handled by Microsoft.

In addition to the default encryption at rest provided above, you can use the encryption API available in the **Global** X++ class. The methods **Global::editEncryptedField()** and **Global::editEncryptedStringField()** use the environment-specific data encryption certificate to perform data encryption and decryption. You can use these methods as an additional layer of protection beyond the default encryption at rest technology used for data storage.

Encryption in transit

Connections established between customers and Microsoft datacenters are encrypted, and all public endpoints are secured using industry-standard Transport Layer Security (TLS) 1.2. TLS effectively establishes a security-enhanced browser-to-server connection to help ensure data confidentiality and integrity between desktops and datacenters.

Supported TLS versions

Finance and operations apps support TLS 1.2 only. Earlier TLS versions, 1.0 and 1.1, are not supported.

Supported cipher suites

Finance and operations apps only support the following cipher suites:

Use customer-managed keys to control encryption keys for data at rest

Article • 12/06/2024

Microsoft services adhere to data privacy and compliance requirements when they secure customer data by encrypting data at rest. This practice secures the data from being exposed if a copy of the database is stolen. When data encryption at rest is used, any stolen database data is protected from being restored to a different server without the encryption key.

By default, data is encrypted by using *Microsoft-managed keys*. However, if you want more control over your encryption keys, you can manage your own keys by using *customer-managed keys* (CMKs) instead. CMKs must be stored in Microsoft Azure Key Vault.

This article explains how to set up CMKs to control encryption keys for data at rest in finance and operations environments.

> **Important**
>
> - The CMK feature is provided through Microsoft Power Platform. It applies to environments that run one or more finance and operations apps that are integrated with Microsoft Power Platform. It also applies to all environment-specific resources, including SQL databases and Azure storage accounts. (For more information, see Enable the Microsoft Power Platform integration.)
> - This feature is being gradually rolled out across regions and might not yet be available in your region.
> - CMK policy enforcement doesn't include cloud-hosted environments because these environments are deployed in customer-managed subscriptions. For more information on best practices for securing cloud-hosted environment, see Secure one-box development environments.
> - Refer to Licensing requirements for customer managed key.

Enable CMKs

You can enable enforcement of the CMK policy for finance and operations environments where Microsoft Power Platform integration is enabled). Finance and operations

Set the session inactivity timeout

Article • 06/03/2022

The session inactivity timeout setting represents the amount of time a user can be inactive before the user's session times out and closes. It only affects user browser sessions.

You can set the values from 5 minutes to 60 minutes.

This function has a default value of 30 minutes. You can set the value up to 60 minutes, however doing so might cause extra load on the system.

> **Note**
>
> This feature is available as of Platform update 29.
>
> If you previously set a session inactivity timeout in the web.config (**WebClientStatefulSessionTimeoutInSeconds** key) through a support request, then that old value will still be honored. The change in default will only affect those who had not explicitly set a new session inactivity timeout in the web config.

To change the value, follow these steps:

1. Select **System administration** > **Setup** > **System parameters** to open the **System parameters** page.
2. On the **General** tab, in the **Session management** section, enter a value in the **Session inactivity timeout in minutes** field.
3. Select **Save**.

   If you set the value to greater than 30, you will be prompted to confirm your selection. The confirmation prompt says "Increasing the inactivity session timeout can cause extra load on your system, which can lead to a decrease in performance. Are you sure you want to continue?" The higher the value, the higher the load will be, which can affect negatively system performance. Select **Yes** to save the changes, or **No** to revert to the existing value.

Alerting users before sessions end due to inactivity

To give users awareness of an impending session suspension due to inactivity and to help prevent users from losing any unsaved changes when this occurs, users will be

Out-of-box security reports

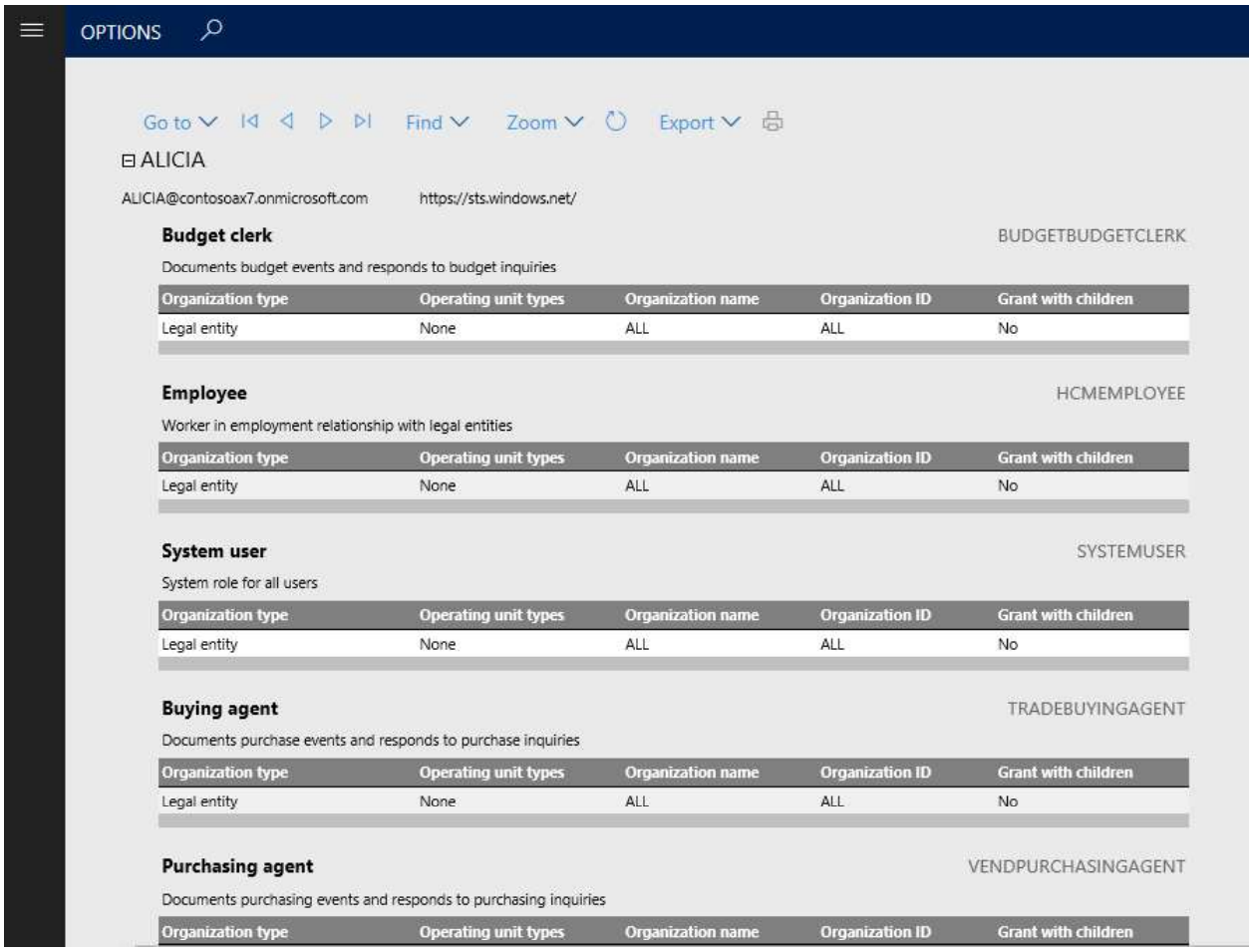
Article • 07/01/2022

Finance and operations provides a set of rich security reports to help you understand the set of security roles running in your environment and the set of users assigned to each role. In addition to the reports noted in this article, developers can generate a workbook containing all user security privileges for all roles using **Visual Studio** > **Dynamics 365** > **Addins** > **View related objects and licenses for all roles**.

Each of the security reports can be found under **System administration** > **Inquiries** > **Security.** A description of each report is provided below.

User role assignments

The **User role assignments** report generates a view of the current user role assignments in your system. By default, the report includes all users with roles assigned. You can optionally limit the report to a specific set of users by entering a list of users when generating the report. On the **User role assignments** parameters pane, go to **Records to include** > **Filter.** From here you can add or remove filters to the list of users the report will be generated for.



Create new users

Article • 03/12/2024

Before you can access finance and operations apps, you must first be added to the **Users** page (**System administration** > **Users** > **Users**). Users include internal employees of your organization, or external customers and vendors. Users can be imported or added manually. All users must be correctly licensed for compliant use.

For information about how to buy and license for finance and operations apps, see Microsoft Dynamics 365 Licensing Guide.

Assign a license to a user

System admins can assign licenses to users in the Microsoft 365 admin center.

Add an external user in Entra ID and assign a license

External users must be represented in your tenant directory (Microsoft Entra ID) so that they can be assigned licenses. Those external users should be added to the tenant in Entra ID as guest users and then assigned the appropriate licenses. A requirement for finance and operations apps is that the guest user's company must use Entra ID. For more information, see Add Entra ID B2B collaboration users in the Azure portal.

Import new users from Microsoft Entra ID

1. Go to **System administration** > **User** > **Users**.
2. On the Action Pane, select **Import users**.
3. Select the users to be imported. The list includes Microsoft Entra users that are currently not users in this environment.
4. Select **Import users**.
5. Select **Close**.

> **Note**
>
> The value for the **Company** field will be set based on the current session company for the admin. After import, you must assign roles and organizations as applicable. For more information, see Assign users to security roles. Conditionally, it might

Block access by location with Microsoft Entra Conditional Access

Article • 03/11/2025

> **Note**
>
> The new and improved Power Platform admin center is now in public preview! We designed the new admin center to be easier to use, with task-oriented navigation that helps you achieve specific outcomes faster. We'll be publishing new and updated documentation as the new Power Platform admin center moves to general availability.

You can limit access to users with block access by location to reduce unauthorized access. By using Conditional Access policies, you can apply the right access controls when needed to help keep your organization secure and stay out of your user's way when not needed. Conditional Access analyses signals such as user, device, and location to automate decisions and enforce organizational access policies for resources. For example, when location restrictions are set in a user's profile and the user tries to sign in from a blocked location, access to customer engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing, Dynamics 365 Project Service Automation), and finance and operations apps are denied. For more information about Conditional Access, see the Conditional Access documentation.

Requirements

- A subscription to Microsoft Entra ID P1 or P3.
- A federated Microsoft Entra ID tenant. See What is Conditional Access?

Additional security considerations

Block access is only enforced during user authentication. This is done by the Microsoft Entra ID Conditional Access capability. Customer engagement and finance and operations apps set a session timeout limit to balance protecting user data and the number of times users are prompted for their sign-in credentials. Block access for devices (including laptops) is not applied until the session timeout expires.

Import users from Microsoft Entra ID

Article • 03/08/2024

Import select users

This procedure can be used by system administrators to import select users from Microsoft Entra ID.

1. User will be imported with the current session company as their default company. Change current company if applicable before importing users.
2. Go to **System administration** > **Users** > **User**s.
3. Click **Import users**.
4. Select the users that should be imported and select **Import users**.

After import is completed it will be required to assign roles to users.

Import users in bulk

This procedure can be used by system administrators to import a large number of users from Microsoft Entra ID. Note that it is not possible to select users when using the Batch import option.

Run the import as a batch job

1. User will be imported with the current session company as their default company. Change current company if applicable before importing users.
2. Go to **System administration** > **Users** > **Users**.
3. Click **Batch import**.
4. Expand the **Run in the background** section.
5. Select **Yes** in the **Batch processing** field.
6. In the **Batch group** field, enter or select a value. This is an optional step.
7. Select **Yes** in the **Private** field. This is an optional step.
8. Select **Yes** in the **Critical job** field. This is an optional step.
9. In the **Monitoring category** field, select an option.
10. Click **OK**.

After import is completed, it will be required to assign roles to users.

Run in a sandbox environment

Set up segregation of duties

Article • 09/29/2023

You can set up rules to separate tasks that must be performed by different users. This concept is named segregation of duties. For example, you might not want the same person to acknowledge the receipt of goods and to process payment to the vendor. Segregation of duties helps you reduce the risk of fraud, and it also helps you detect errors or irregularities. You can also use segregation of duties to enforce internal control policies. Complete the following procedure to create a rule. You must be a system administrator to complete the procedure.

1. Go to **System administration** > **Security** > **Segregation of duties** > **Segregation of duties rules**.
2. Click **New**.
3. In the **Name** field, type a value for the rule.
4. In the **First duty** field, click the drop-down button to open the lookup.
5. In the list, find and select the desired record. Select the first duty that is controlled by the rule.
6. In the **Second duty** field, click the drop-down button to open the lookup.
7. In the list, find and select the desired record. Select the second duty that is controlled by the rule.
8. In the **Severity** field, select an option. Select the severity of the risk that occurs when the same user or role performs both duties.
9. In the **Security risk** field, type a value. Enter a description of the security risk.
10. In the **Security mitigation** field, type a value. Enter a description of the actions that you take to mitigate the security risk. For example, you can mitigate the risk by conducting more detailed reviews of the process, by conducting a monthly managerial review, or by sharing resources with other departments.
11. Click **Save**.

> **ⓘ Important**
>
> Compliance with the rules for segregation of duties is not verified when you create a rule. You can create a rule that creates a conflict for existing roles. Existing user role assignments can also be in conflict with the new rule. You must validate compliance after you create or modify a rule. For more information, see **Identify and resolve conflicts in segregation of duties**

Identify and resolve conflicts in segregation of duties

Article • 09/29/2023

This article explains how to identify and resolve conflicts in segregation of duties. You can set up rules to separate duties that must be performed by different users. This concept is named segregation of duties. When the definition of a security role or the role assignments of a user violate the rules, the conflict is logged. All conflicts must be resolved by the administrator. Complete the following procedure to identify and resolve conflicts.

After a rule has been added, verify that all existing roles are compliant.

Verify that existing roles and duties comply with new rules for segregation of duties

1. Go to **System administration** > **Security** > **Segregation of duties** > **Segregation of duties rules**.
2. Select **Validate duties and roles**. If any roles violate the rules, a message is displayed that contains the name of the rule, the role, and the names of the conflicting duties. Conflicting roles must be modified using **Security configuration** and can't include conflicting duties. If no roles violate the selected rule, a message indicates that all roles comply.

> **Note**
>
> The validation is only performed for the selected rule. It is important to validate compliance for each rule.

When you create or modify a role, the rules for segregation of duties are automatically enforced. You cannot assign conflicting duties to a role.

Next, verify that all existing role assignments are compliant.

Verify that user role assignments comply with new rules for segregation of duties

Manage users and security roles

Article • 09/29/2023

To use anything other than common capabilities in finance and operations apps, users must be assigned to security roles. You can assign users to roles automatically, based on rules and business data, exclude users from automatic role assignment, or add users to roles manually.

Automatically assign users to roles

This procedure explains how system administrators can automatically assign users to roles, based on business data.

1. Go to **Navigation pane** > **Modules** > **System administration** > **Security** > **Assign users to roles**.
2. In the tree, select 'Accounting supervisor'. Select the role that you want to configure the rule for. In this example, select Accounting supervisor.
3. Select **Add rule** to open the dialog menu.
4. In the **Select a query** list, find and select the desired record. Select the query to use for this rule.
5. In the **Membership rule name** list, click the link in the selected row.
6. Select **Edit query**. Edit the query, as needed.
7. Select **OK**.
8. Select **Run automatic role assignment**.
9. Go to **Navigation pane** > **Modules** > **System administration** > **Users** > **Users** (ideally in a separate browser tab).
10. Review the roles assigned to various users to confirm that the role assignment query was correct. Adjust and re-run if needed.

Exclude users from automatic role assignment

This procedure explains how to exclude users from automatic role assignment.

1. Close the page.
2. Go to **Navigation pane** > **Modules** > **System administration** > **Security** > **Assign users to roles**.
3. In the tree, select 'Accounting supervisor'. Select a role. For this example, select Accounting supervisor.
4. In the **Users assigned to role** menu, select **Manually assign/exclude users**.

User security governance overview

Article • 02/18/2025

[This article is prerelease documentation and is subject to change.]

User security governance helps organizations create a security architecture that is closely aligned with their business processes. It empowers organizations to apply precise role management, advanced audit capabilities, and comprehensive license optimization tools.

User security governance provides the following capabilities:

- Detailed reporting about segregation of duties and separation of privileges
- Process-based security roles, duties, and/or privileges
- Creation of new roles/duties from existing objects through import processes
- Temporary role capabilities
- Privileged user management, which enables dedicated accounts to gain time-bound access

User security governance features

User security governance provides the following functionality:

- Design process-based security roles, duties, and/or privileges. Learn more in Set up a process hierarchy, roles, and privileges.
- Design position/responsibility-based user roles.
- Create new roles/duties from existing objects through import processes, and merge duties.
- Automate temporary role assignments. Learn more in Temporary role management.
- Grant time-bound elevated privileges to dedicated accounts through privileged user management. Learn more in Privileged user management.
- Continuously monitor segregation of duties and separation of privileges. Define a threshold, and control the creation of duties/privileges that have overlapping entry points. Learn more in Roles violating segregation of duties.
- Draft and eventually convert defined roles to an Application Object Tree (AOT) project.

Set up security categories

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

Security categories

Categories are used for an aggregation in the **Process roles maintain** module. You can define categories that help you save a new role under a given work stream or department. We strongly recommend that you complete this setup correctly. In this way, you help reduce the development costs when security upgrades are required.

There are two ways to create a category:

- Create a new category from scratch.
- Import an existing category from a different company.

Create a new category

To create a new category from scratch, follow these steps.

1. Go to **System administration** > **Security governance** > **Security category**.
2. Select **New**.
3. Set the **Name** field.
4. Optional: Set the **Company** and **Description** fields.
5. Select **Save**.

Import an existing category

To import an existing category, follow these steps.

1. Go to **System administration** > **Security governance** > **Security category**.
2. Select **Import**.
3. Expand the **Parameters** section.
4. Use the **Browse** button to provide the file path of the attachment.
5. In the **Type** dropdown, select one of the following values:

- **User security governance -** This option impacts the process roles under security governance module and it won't impact the security configuration.
- **Security configuration -** This option impacts the security configuration under core platform and not the process roles under security governance module.

Security category export/import

Article • 02/12/2025

[This article is prerelease documentation and is subject to change.]

Security categories offer options for both backing up as XML and restoring from XML. Learn more about the import process in Import an existing category. This article describes various scenarios that system administrators can handle.

Back up as XML

1. Go to **System administration** > **Security governance** > **Security category**.
2. Before you start the backup, confirm that security categories are set up.
3. Select a security category, and then select **Backup as XML**.

   > **Important**
   >
   > You can back up either a single selected category or all available categories. You can't individually select multiple categories for backup at the same time.

4. In the dialog that appears, on the **Parameters** FastTab, in the **Type** field, select one of the following values:

   - **User security governance –** Generate a complete XML file of the security category and its related configuration from the **Process hierarchy** page. If multiple hierarchies, tasks, duties, privileges, entry points, or roles are defined under the category, the XML includes only objects that were created on the **Process hierarchy** page. It excludes all objects that were created under **Core security configuration**. For example, the XML includes the hierarchy, tasks, and entry points, but it excludes duties, privileges, and roles.
   - **Security configuration –** Generate a complete XML file of the security category and its related configurations from **Core security configuration**. If multiple hierarchies, tasks, duties, privileges, entry points, roles, and so on, are defined under the category, the XML includes only objects that were created under **Core security configuration**. It excludes all objects that are limited to the **Process hierarchy** page. For example, the XML includes duties, privileges, and roles, but it excludes the hierarchy, tasks, and entry points.
   - **Governance + configuration –** Generate a complete XML file of the security category and its related configurations from the **Process hierarchy** page and

Set up security governance parameters

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

This article explains how to set up various parameters that are related to the security governance feature. These parameters are useful for licensing reports and user aging reports.

Basic license cost

1. Go to **System administration** > **Security governance setup** > **Parameters**.
2. Expand the **Basic license cost** section.
3. Select **New**.
4. In the **Basic user license** field, select the user license.
5. In the **Price** field, enter the manual price of the license.
6. Repeat steps 3 through 5 to set up the manual price for other user licenses.
7. To exclude user accounts from the license price calculation on the **Licenses usage summary** report, in the **Exclude** section, select **Group**.
8. To exclude all system administrators from the license price calculation on the **Licenses usage summary** report, set the **System administrator** option to **Yes**.

General

1. Go to **System administration** > **Security governance setup** > **Parameters**.
2. Expand the **General** section.
3. In the **Check similarity** field, select **Yes** to turn on the similarity check for duties in the **Segregation of duties validation** feature. Select **No** to turn off the similarity check.
4. In the **Level for similarity validation** field, enter the level of similarity validation that is done for the **Segregation of duties validation** feature. This field defines the amount of similarity that can exist between duties before a conflict is detected.
5. In the **Allow unpublished objects** field, select **Yes** to allow unpublished objects in **Security configuration** (**System administration** > **Security** > **Security configuration**). Select **No** to disallow unpublished objects.

User aging periods

1. Go to **System administration** > **Security governance setup** > **Parameters**.

Set up a process hierarchy, roles, and privileges

Article • 03/17/2025

[This article is prerelease documentation and is subject to change.]

A *process hierarchy* provides a way to organize and manage the business processes in your company. After you define the process hierarchy for your company, you can assign various tasks, and define roles, entry points, and privileges according to the business requirements.

This feature helps you set up your company's security configuration based on position-based roles and duties/privileges. New roles can be created based on the organization's hierarchy and existing positions. Therefore, the feature helps you create optimal roles that take into account user interface (UI) effectiveness, license levels, and data security.

The feature extracts business processes from positions and converts them into security roles. Therefore, the roles are easy to understand and define. The goal is to implement roles that represent the specific set of tasks and privileges that are required to perform a unique job in finance and operations apps.

The benefits of this feature are optimization of license costs and reduced risk of data fraud.

Set up a process hierarchy

The first and most important step in the process of setting up an accurate security configuration is to define a process hierarchy that closely represents your company's functional hierarchy. Although the process hierarchy that you define can be modified later, modification requires a significant amount of work.

To set up a process hierarchy, follow these steps.

1. Go to **System administration** > **Security** > **Security governance** > **Security process role maintain**.
2. In the **Security category** field, select a category, and then select the desired tree level within that category.
3. On the Action Pane, select **New process**.
4. In the **Process name** field, enter a unique name for the process.
5. Specify other details, such as a description and version information.

Security tasks under the process hierarchy

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

The security tasks under the process hierarchy are the key processes that a given role completes in Dynamics 365 finance and operations apps to perform its specific duties. This feature lets system administrators convert these processes into individual tasks and multiple functionalities that those tasks support.

Segregation of duties

Segregation of duties prevents duties that have overlapping privileges and roles that have overlapping responsibilities. Segregation of duties can be enabled on the **Parameters** page. After you create a new task and assign entry points to it, you can validate the percentage of overlapping duties. You can set up segregation of duties rules to prevent users from saving conflicting duties.

Privilege separation validation

Privilege separation validation is more focused on the privileges that are assigned to roles. After you create a new task and assign entry points to it, you can validate the percentage of overlapping privileges.

Load from task recordings

Create new tasks from existing task recordings that are generated by capturing interactions with the user interface (UI) in the Task recorder tool. Users can record core business actions and share the recordings with system administrators. System administrators can then convert the recordings into security tasks in the security configuration. This approach offers an efficient way to create new tasks.

Load from user or role

Convert the entry points from existing user accounts or roles into security tasks. After you select an existing user account or role, the entry points are extracted and converted into tasks. System administrators can have a starting point to design a new security role

Security entry points under the process hierarchy

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

The security entry points under the process hierarchy are critical for defining and designing the access level and privileges for any given role. Here are some of the key entry point–related functions that are supported in user security governance:

- Explode entry point
- Update permissions

Explode entry point

System administrators can expand the permissions of a given role by including all the other entry points that are related to the menu item. The menu item that is associated with the entry point is retrieved by using its name and type. The system then fetches all the other entry points that are associated with that menu item. If the menu item exists, the access rights and labels are set for the entry point. If the record type is a menu item, other properties are set, such as user licenses and manual permissions.

> **ⓘ Important**
>
> This function adds all neighboring entry points from the selected entry point. We recommend that you use it with workspaces.

Update permissions

System administrators can update the permissions of a given role by changing the permission levels for each entry point.

For each entry point, the **Unselect**, **Grant**, or **Deny** permissions can be reconfigured at the following levels:

- Read
- Create
- Update
- Correct

Roles violating segregation of duties

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

The **Roles violating segregation of duties** view shows all roles that violate segregation of duties rules. It also shows how many violations of this type exist for each role.

View violations for a selected role

To view violations of segregation of duties rules, follow these steps.

1. Activate the **Summary** tab on the **Roles violating segregation of duties** view.
2. Under the **Security roles** grid, select the specific role to see segregation of duties violation.
3. On this grid, you see the role name and total count of segregation of rules set up.
4. After selecting a specific role, data is loaded on the grid **Segregation of duties rules**.
5. Go to the **Segregation of duties rules** grid.
6. If there are multiple rules setup for the selected role, there are multiple rows.
7. Select the name of a specific rule to see the violation.
8. The view shows the specific segregation of duties rule that the selected role violates.
9. Under the **Infolog text** column, you see complete details about the violation.

View all violations

To view a report that lists all violations, go to **System administration** > **Security** > **Security governance** > **Role violating segregation of duties** > **List**.

The report uses the defined segregation of duties rules. All duties are monitored against these rules. If a duty is assigned to a role that violates any of these rules, it appears on this report.

Feedback

Temporary role management

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

Temporary role management lets system administrators assign temporary roles to a specific user account for a specific amount of time (known as a *session*). This feature is useful when a user in a company is away from work for a period, or if a role must temporarily be divided among multiple users. When the session ends, the user account returns to its original roles.

Session approval and processing

Only users who have the **System administrator** role can initiate new temporary role sessions.

The process for temporary role sessions has these steps.

1. On the **Temporary role management** page, select **New** to create a request for a new session. The request has a status of **Draft**. Wait for a system administrator to approve the request. System administrators can approve or edit session requests.
2. To approve the session request, in the **Change status** field, select **Planned**.
3. The background process picks up the session request for processing. Alternatively, a system administrator can manually process it by selecting **Process**.
4. When the session begins, the selected user account obtains temporary roles in finance and operations apps.
5. When the session ends, the user account returns to its original roles.

> ⓘ **Note**
>
> There is no limit on the length of a temporary role session.

Session types

When you create a new temporary role session, set the type to **Merge** or **Replace**.

- **Merge –** Add the temporary roles to the existing roles of the user account. After the temporary roles session is over, users retain their original roles and the added temporary roles are revoked.

Security version management

Article • 01/29/2025

[This article is prerelease documentation and is subject to change.]

The security version feature lets you maintain multiple versions of security configurations in a company. You can also compare and restore versions.

Create a version

To create a version of the security configurations at a point in time, follow these steps.

1. Go to **System administration** > **Security** > **Security governance** > **Security versions**.
2. Select **Create version**.
3. In the **Name** field, enter a name for the version.
4. Select **OK**.

Version creation is an asynchronous process. You can use the **Status** column to monitor the status of the process. A status of **Executing** indicates that version creation is in progress.

Restore a version

To restore the security configurations to a version that was created earlier, follow these steps.

1. Go to **System administration** > **Security** > **Security governance** > **Security versions**.
2. Select the version to restore.
3. Select **Restore version**.
4. In the dialog box that appears, select options as required.
5. Select **OK**.

Compare versions

After security versions are created, users can compare them to gain insights into the differences between them.

To compare versions, follow these steps.

Privileged user management

Article • 01/31/2025

[This article is prerelease documentation and is subject to change.]

Privileged user management lets system administrators schedule a session for selected user accounts. All user interactions are recorded in Dynamics 365 finance and operations apps during that session, if the user decides to continue using Dynamics 365 finance and operations after reading the consent on the landing page. This feature is useful when some elevated privileged accounts are used for auditing purposes. It helps ensure that users aren't performing any unauthorized activities in the system and keeps a recording of it, in case it's later needed for audit or compliance reviews.

System administrators can choose to enable or disable the given user account once the session begins. As soon as the session ends, the account returns to its original state.

Session approval and processing

New privileged user sessions are initiated by a system administrator.

1. On the **Privileged user management** page, select **New** to create a request for a new session. The request has a default status of **Draft**.
2. The system administrator can decide if they want to enable or disable the user account selected for the **Privileged user session**. **Enable** means it changes the user account to enabled state, if it was originally disabled. **Disable** deactivates the user account as soon as the session starts. After the session is over, user accounts return to their original state.
3. Anyone who has the **System administrator** role can approve or edit the session request. To approve the request, in the **Change status** field, select **Approve**.
4. The background process picks up the session request for processing. Alternatively, a system administrator can manually process it. The system administrator can schedule the session for the user account. They can also enable or disable the account after the session begins. As soon as the session ends, the account returns to its original state.

> **Note**
>
> The maximum duration for a privileged user session is 24 hours.

Available reports for security

Article • 03/17/2025

[This article is prerelease documentation and is subject to change.]

The following reports are available to help with security, licenses, roles, and duties:

- **User activity aging –** This report tracks sign-in information.
- **Role audit trail** – This report shows the history of a role that is assigned and unassigned to users.
- **Security analysis –** This report provides information about various roles and their privilege access levels. It shows how many users belong to each role and the change history of duties, roles, and privileges.

User activity aging report

The **User activity aging** report tracks information about sign-in to Dynamics 365 finance and operations apps. Therefore, it helps administrators effectively monitor user activity. Some of the most common monitoring ranges are 10, 30, 60, 90, and 120 days. The day ranges are configurable and can be customized to suit the organization's needs. The data on this report can be used to optimize licensing costs.

To define and customize day ranges for the **User activity aging** report, follow these steps.

1. Go to **System administration** > **Security governance setup** > **Parameters**.
2. On the **User aging periods** tab, configure all five day ranges as you require.
3. Select **Save**.

Role audit trail report

The **Role audit trail** report provides a history of the roles that have been assigned and unassigned to users. Details include the time when a role was assigned and the individual who assigned it. Data is collected from the assignment and deallocation of roles.

To view the **Role audit trail** report, follow one of these steps.

- Go to **System administration** > **Users** > **User's role**.
- Go to **System administration** > **Security** > **Security governance** > **Temporary role management**.

Security governance FAQ

Article • 02/15/2025

[This article is prerelease documentation and is subject to change.]

This article provides answers to the most frequently asked questions about setting up and using the security governance feature.

Can the feature be used to hide specific fields on a page or control the ability of some roles to edit specific fields on a page?

For most fields, you must do a custom implementation of the business logic to control the permissions. However, if there's an entry point behind the selected field, it can be controlled through the user security governance feature.

Is the feature integrated with any version control system to maintain the various XML or AXTR files that are generated during use?

No, security governance isn't integrated directly with any version control. We recommend that you control all files through version control, so that system administrators can maintain copies of files or task recording files. This approach is helpful for compliance audits, because users just have to compare the security versions with the approved security architecture.

Does the process hierarchy work with customized menu items that are mapped to privileges?

Yes, the process hierarchy works with custom menu items.

Is temporary role management captured in the security audit trail?

Microsoft Entra ID security groups

Article • 01/06/2025

Microsoft Entra ID security groups is a legacy feature that enables roles and organizations to be assigned to users, based on their memberships in Microsoft Entra ID security groups. (For more information about Entra ID security groups, see Entra ID security groups.) The feature also enables just-in-time (JIT) provisioning of users when they sign in to the finance and operations environment for the first time.

Group-based role assignments are applied by using manual and automatic rule-based assignments for a user. The union of assigned roles determines the actual data access.

Known limitations when the Entra ID security groups feature is used

Before you enable the **Microsoft Entra ID security groups** feature, it's important that you are aware of the following known limitations. Several of the limitations affect internal control and auditing.

- No database logging can be done for these role assignments.
- Security and licensing reports don't include these role assignments.
- Segregation of duties engine is not compatible with these role assignments.
- Pages that show role assignments, the **Assign users to role** page, and the **Roles for selected user** FactBox don't include these role assignments.
- External users aren't supported. They can't use JIT provisioning, and no roles can be assigned to them based on group memberships.
- Workflows that depend on assigned roles don't consider these role assignments.
- Disabling a group in system administration doesn't stop JIT provisioning or role assignment.
- The **User Id** value of users that are created through JIT provisioning has a leading dollar sign ($) and numbers.
- Publishing views to security roles doesn't consider the role assignments made to Entra ID security groups.
- Legal entity assignments are applied to the entire Entra ID security group.
- Starting with FR version 10.0.42, role and privilege assignments made through imported Entra ID security groups will no longer be supported in Financial Reporting (FR). User roles and privileges must be assigned directly to FnO user accounts for access to FR.

Import or export a customized security configuration by using Data management

Article • 07/12/2024

The article explains how a customized security configuration can be exported and imported across environments by using the Data management framework. This functionality can be used when, for example, a customized security configuration must be moved from a test environment to a production environment.

The following entities hold the customized, role-based security (that is, privileges, duties, and roles) that has been added or modified by using security configuration:

- Security privilege metadata customization entity
- Security duty metadata customization entity
- Security role metadata customization entity

Export customized security configuration

1. Go to **System administration** > **Workspaces** > **Data management**.
2. Select the **Export** tile.
3. In the **Group name** field, enter a name for the group.
4. Set the **Generate data package** option to **Yes**.

Security diagnostics for task recordings

Article • 09/29/2023

Before you begin

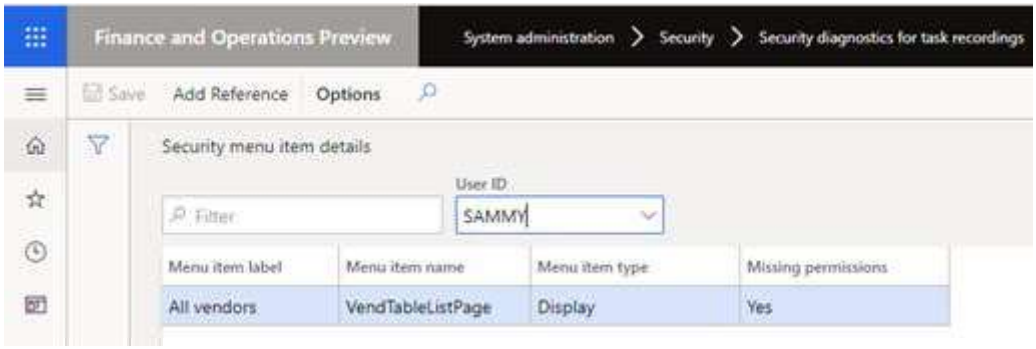
This article provides information about how to analyze and manage security permission requirements based on a task recording. Before you complete the steps in this article, you must have a task recording of the business process that you want to analyze. To record a business process, see Task recorder resources.

Manage security for a task recording

1. Go to **System administration** > **Security** > **Security diagnostic for task recording**.
2. Open the task recording from its location. Select **Open from this PC** or **Open from Lifecycle Services**, and then select **Close**.
3. This will open the **Security menu item details** page that lists the security objects required for the process.

> **Note**
>
> The **Action** and **Output** menu items are not included in the list.

4. In the **User ID** field, select a user. If the user does not have permissions for some menu items, the **Missing permissions** field will update to **Yes**.



5. Select **Add Reference** to see a list of the security objects, including roles, duties, and privileges that grant the missing permission.

6. Select a security object from the list:

   - If **Role** is selected, select **Add role to user**. This will open the **Assign users to roles** page. For more information, see Assign users to security roles page.

Extensible data security policies

Article • 08/09/2023

This article provides an overview of Extensible Data Security (XDS) policies in Finance and operations apps. XDS allows developers to supplement role-based security by restricting access to table records based on security policies. The query in the policy applies a filter and only records that satisfy the conditions of the filter will be accessible from the restricted tables.

Data security policy components

- **Constrained tables**: The table or tables from which data is filtered or secured. For example, in a policy that secures access to transactions based on customer, the **CustTrans** would be an example of a constrained table.
- **Primary table**: Used to secure the content of the related constrained table. In the following example, the **CustTable** table would be the primary table. The primary table must have an explicit relationship to the constrained tables.
- **Policy query**: Used to secure the constrained tables content using a range condition on the primary table contents. Only records that are included in the range are accessible. The range can, for example, be based on a specific value for Customer.
- **Context –** Controls the conditions under which a policy is applicable. Two main types of contexts are available:
    - **Role context**: Based on the roles that the user is assigned. There are two suboptions for role context:
        - **RoleName** – Indicates that the security policy is only applied to the application user assigned to the role equal to the value of RoleName.
        - **RoleProperty –** This value is used in combination with the **ContextString** property to specify multiple user roles context. It's applied when the Context String value defined in the **Role Property** field for the policy is the same as the **ContextString** field value for the assigned user roles.
    - **Application context**: Applied if the context string set by the application using the XDS::SetContext API is the same as the value defined in the **Context String** field for the policy.

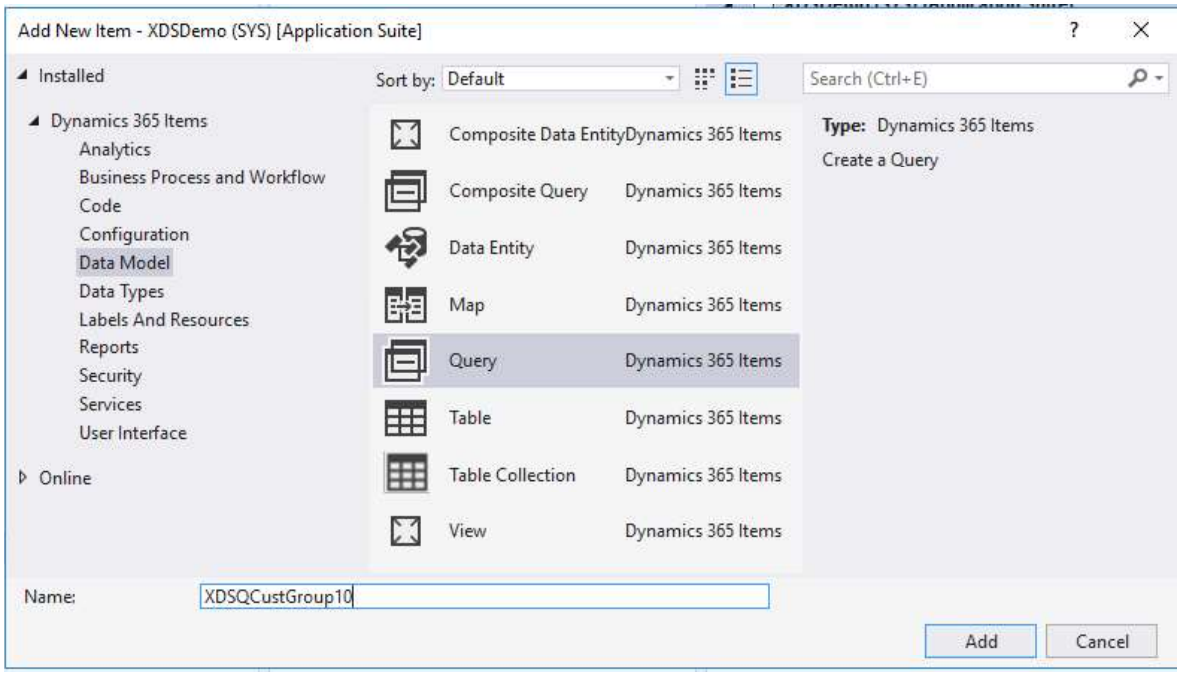
Create a security policy

Article • 06/03/2022

This article explains how to create a simple security policy that secures access to customers and customer groups, based on a range for a customer group.

Add a new query

1. In Visual Studio, add a new query, such as XDSQCustGroup10, to your project/solution. The query will be used to restrict data access from the **Constraint** table.



2. Right-click **Data Sources**, and the select **New Data Source**.

3. In the **Table** field, enter the primary table name **CustGroup**.

4. Right-click **Ranges**, and then select **New Range**.

5. Set the **Enabled** field to **Yes**.

6. In the **Data Source** field, enter the primary table name, in this case, 'CustGroup'.

7. In the **Value field**, enter **10** to restrict access to data where CustGroup has value of 10, by defining the Range for the CustGroup field.

Stay compliant with user licensing requirements

Article • 12/26/2024

This article provides an overview of how customers can stay compliant with the user licensing requirements for finance and operations apps. These apps include Microsoft Dynamics 365 Finance, Dynamics 365 Supply Chain Management, and Dynamics 365 Commerce.

The licensing requirements for users are determined by the security roles that are assigned to enabled users. Security roles are built based on a hierarchy of the following elements:

- Subroles
- Duties
- Privileges
- Directly referenced securable objects

For more information, see Role-based security.

The licensing requirements for users are determined at the organization or tenant level. This article is focused on the requirements for a single environment. If you have multiple environments, the requirements must be analyzed across all of them.

A licensing requirement is assigned to every securable object or resource that's included in a user role.

The rest of this article describes the different tools that you can use to ensure that the actual licensing complies with the expected licensing requirements. The first thing to verify is that the user roles have the expected licensing requirements and are assigned to the appropriate users.

License requirement per role

The **Assign roles to user** dialog box that's opened from the **System Administration** > **Security** > **Users** page can help you understand the impact on user licensing when roles are assigned. You can also use it to get an overview of the licensing requirements for each role. You can use the dialog box itself or export data to Excel for further analysis. Custom roles can require licenses for more than one application.

View independent software vendor license status

Article • 08/12/2022

This article explains how you can view the status of independent software vendor (ISV) licenses for finance and operations apps, such as Dynamics 365 Finance, Dynamics 365 Supply Chain Management, and Dynamics 365 Commerce.

License codes and configuration keys are part of the ISV licensing model for finance and operations apps.

> **Note**
>
> Configuration keys that are provided by Microsoft aren't part of the licensing model for finance and operations apps. The keys are only used to enable and disable functionality.

When an ISV license key and code are installed, the corresponding configuration key will be available and enabled on the **License configuration** page.

View ISV license status

Each ISV solution that is tied to a license runs only when a valid license code exists in the customer's environment. Therefore, if an ISV ties their solution to a license, but the customer doesn't have a valid license code, the solution doesn't run. To prevent the loss of functionality, it's important to track the expiration dates, if applicable, for license codes. To view the expiration dates, go to **System administration** > **Setup** > **License configuration**, and select the **License codes** tab.

To avoid downtime, review the expiration dates of the license keys, and if applicable, obtain and import new license keys before moving to a new version. The **License codes** tab shows the expired license codes. The corresponding configuration key won't appear in the **Configuration keys** tab.

Additional resources

For more information about the ISV licensing feature, see Independent software vendor (ISV) licensing.

Process automation

Article • 06/10/2024

Process automation allows simple scheduling of processes that will be run by the batch server. The updated calendar view of the scheduled work allows end users to view and take action on scheduled and completed work.

Administration

The central administration page for all process automations is found in the System Administration module under the **Setup** menu. This page will list all automated processes (series) that are set up in the system. It will also allow you to add new process automations directly from this page. After a series is set up, you can manage each series from this list. You can choose to edit the entire series, delete it, view all occurrences in a list view, or disable the series if you would like to pause the scheduled work for a while.

Use the **Background processes** tab on this page to administer any background processes that are running in your environment. Select **Edit** to make schedule changes for any background process. These changes can include a sleep time period that will cause the process to "sleep" or pause running for a specified period each day. Select **View most recent results** to view the execution results for each background process.

Any processes that are disabled in feature management won't show when the feature is disabled. Additionally, the process automation scheduling engine won't schedule any occurrences or background processes for a disabled feature. Re-enabling the feature will cause any scheduled occurrences or background processes in the past to run immediately. The process automation scheduling engine relies on the system batch job, **Process automation polling system job** to run. The job shouldn't be altered or tampered with at any time. If this batch job isn't running, or it's in an error state, select **Initialize process automation** to reset the batch job. This reset ensures that any new automations released in a more recent version of the application are initialized.

Calendar view

One of the key benefits of process automation is the ability to see the scheduled work in a simple calendar view. This view allows you to see work for a week at a time. You'll see this view on the right side of the **Process automation** page. It will be populated with the scheduled work for the selected series.

Batch processing overview

Article • 02/09/2024

This article provides an overview of batch processing.

Many tasks in finance and operations can be run as part of batch jobs. For example, batch jobs can include tasks for printing reports, performing maintenance, or sending electronic documents. By using batch jobs, you can avoid slowing down your computer or the server during typical working hours.

The tasks in a batch job can run either sequentially or at the same time. Additionally, you can create dependencies between tasks. In other words, the sequence of tasks can differ, depending on whether an earlier task succeeds or fails.

You can set up recurrence patterns for batch jobs. For example, you can set up a job to process invoices automatically at the end of every month.

To monitor batch jobs, you can set up alerts. Alerts can be sent when the batch job succeeds, fails, or finishes.

After a batch job is processed, you can view the history. The history includes any messages that were encountered while the job was running.

Use batch groups to categorize batch tasks and run them on specific servers. The servers in your environment might have different software installed, or they might be available at different times of the day. Batch groups are used to direct batch tasks to the most appropriate server. Tasks in the same batch job can belong to different batch groups.

For example, server A is set up to print reports, and server B is set up to send electronic documents. You can use batch groups to make sure that reporting tasks are run on server A and electronic documents are processed by server B.

For more information, see:

- Batch processing and batch servers
- Batch capacity

Batch functions

Administrators and Batch managers can perform common tasks including creating and copying batch jobs, changing a batch job user, and specifying a time period in which a job shouldn't run. For more information about these tasks, see the following topics:

Batch processing and batch servers

Article • 11/12/2024

This article describes batch processing and batch servers, and how to plan for their use.

The batch platform provides an asynchronous, server-based batch processing environment that can process tasks across multiple instances of Application Object Server (AOS).

You should become familiar with the following aspects of the batch platform:

- A **batch job** is a process that is used to achieve a specific goal. A batch job consists of one or more batch tasks.
- A **batch task** is an activity that is run by a batch job. You can add batch tasks that have multiple types of dependencies to a batch job. You can also configure AOS instances to run multiple threads, each of which runs a task. All batch tasks that are waiting to be executed can be picked on any available AOS instance that is configured as a batch server. To improve throughput and reduce overall execution time, you can define a batch job as many tasks and then use a batch server to run the tasks against all available AOS instances.
- A **batch group** is an attribute of a batch task. It lets the administrator determine or specify which AOS instance runs the task. When you create a new task, it's put in the default batch group. All batch servers are configured to process the default batch group and the waiting tasks from any job. Additionally, you can create a named batch group and then set an affinity between that batch group and specific AOS instances. After you create this affinity, only the specified AOS instances process tasks from the named batch group, and those AOS instances process tasks from the named batch group only. You can also add the default batch group to the configured servers, if that batch group is required.

> ⓘ **Note**
>
> After you implement batch priority-based scheduling, batch groups no longer control associations with batch servers. Instead, they're used to assign priorities to batch jobs and manage the maximum concurrency of batch tasks within their respective batch jobs. For more information, see Priority-based batch scheduling.

Batch server topology planning

Priority-based batch scheduling

Article • 03/21/2024

In Platform update 31, you can turn on the **Batch priority-based scheduling** feature in Feature management. Priority-based scheduling decouples batch groups from the batch server and lets you define priorities for batch groups. It's no longer necessary to assign batch jobs to batch servers. Instead, relative scheduling priorities based on business requirements are used to determine the order in which tasks are run across available batch servers.

> **Important**
>
> - This feature is available with version 10.0.25.
> - This feature is enabled by default for all new instances with version 10.0.28 (PU 52).
> - This feature is enabled by default for all existing instances with version 10.0.36 (PU 60).
> - This feature is required for all instances starting with version 10.0.38 (PU 62).

A scheduling priority is defined for batch groups, but it can be overridden for specific batch jobs. The scheduling priority classifications are used to declare relative priorities, and to determine the processing order of jobs and business processes. The available values for the scheduling priority are **Low**, **Normal**, **High**, **Critical**, and **Reserved capacity**.

Normal is the default value and is applied to all existing batch groups when the feature is turned on. **Reserved capacity** represents the highest priority. In Platform update 32 and later versions, you can use it to dedicate reserved capacity for jobs. For more information, see the Set the batch reserved capacity level section later in this article.

For example, there are 100 batch tasks for processing. Forty tasks are served from the reserved queue, 30 from the critical queue, 15 from the high queue, 10 from the normal queue, and five from the low queue. It isn't the priority-based order of execution that's selected for processing. Instead, it's the weight of the batch tasks from each priority.

Expand table

Priority	Weight
Low	5%

Batch capacity

Article • 03/21/2024

Batch capacity refers to the maximum number of batch tasks that can be processed at a time. It depends on both the number of batch servers and the number of batch threads available for processing these tasks.

To calculate the batch capacity, multiply the number of batch servers by the number of batch threads per server:

Batch capacity = Number of batch servers × Number of batch threads per server

The total batch capacity for the environment is determined based on user licenses. We establish the minimum and maximum number of batch servers required to serve this batch capacity.

To view batch capacity, use **System Administration** > **Setup** > **Server configuration** and look for available batch servers.

Batch auto scaling

Auto scaling is a new feature that automatically adjusts your batch servers according to resource usage thresholds. It provides elasticity to your environment, allowing it to adapt to varying workloads dynamically. This process is entirely automated and relies on predefined signals based on CPU and memory usage of batch servers.

Auto scaling becomes beneficial when the workload on an environment fluctuates over time. We continuously monitor the reported load and periodically evaluate triggers to determine if scaling is necessary.

The lower load threshold signifies the point at which the service scales in. If the average load falls below this threshold, the service scales in.

Conversely, the upper load threshold indicates when the service scales out. If the average load exceeds this threshold, the service scales out.

> ⓘ **Note**
>
> - For batch auto scaling to work, your environment should have batch priority-based scheduling enabled, and your PU should be 10.0.26 (PU 50) or higher.

Create a batch job

Article • 03/21/2024

A batch job is a group of tasks that are submitted to an Application Object Server (AOS) instance for automatic processing. Batch jobs are run by using the security credentials of the user who created the job. Use the following procedure to create a batch job. The demo data company used to create this procedure is USMF.

Create the batch job

1. Go to **System administration** > **Inquiries** > **Batch jobs**.
2. Select **New**.
3. In the **Job description** field, enter a description of the batch job.
4. In the **Scheduled start date/time** field, enter the date and time when the batch job should run.
5. Select **Save**.

Create a recurrence

1. On the Action Pane, select **Batch job**.
2. Select **Recurrence**. Use these options to enter a range and pattern for the recurrence.
3. Select **OK**.

> **Note**
>
> All recurring batch jobs are automatically returned to the waiting state, regardless of whether they fail or succeed. This behavior ensures that recurring jobs can complete any pending work during the next run if the previous run failed. This functionality can be enabled only if the batch job's recurrence conditions are still valid. For example, the batch job must have a remaining recurrence count or a recurrence end date that hasn't passed.

Add alerts

1. On the Action Pane, select **Batch job**.
2. Select **Alerts**. Indicate if you want alert messages sent when the batch job ends, has an error, or is canceled. Then specify if you want the alerts to be displayed as

Copy a batch job

Article • 06/03/2022

When you want to create the same jobs for different legal entities, you can use the copy batch job functionality to copy an existing batch job and the batch tasks, including recurrences.

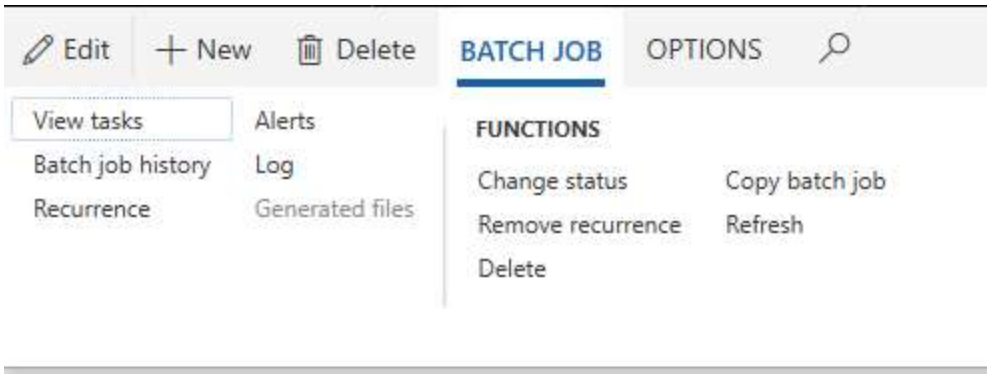
You can set the description, company, schedule start date and time, the recurrence, and the run by account at the same time. When you copy the batch job, any alerts and dependencies from the source job will also be copied.

> **Note**
>
> This feature is available as of Platform update 20.

Copy a batch job

Complete the following steps to copy a batch job.

1. Click **System administration** > **Inquiries** > **Batch jobs**.
2. Select the job that you want to copy, and on the Action Pane, click **Batch Job** > **Copy batch job**.



4. Enter or add any changes. If you set **View tasks** to **Yes**, when you click **OK** you will go directly to the **Batch tasks** page for the copied job.

Create a batch class

Article • 04/02/2024

In Microsoft Dynamics 365 finance and operations apps, batch processing lets you efficiently perform tasks in the background, without affecting system performance. This article explains how to create a batch class by using `RunBaseBatch` as the base class.

Prerequisites

To create a batch class, you must have the following prerequisites:

- Access to a finance and operations apps environment
- A basic understanding of the X++ programming language
- Visual Studio with finance and operations development tools installed

Create a batch class by using RunBaseBatch

1. In Visual Studio, connect to your finance and operations apps development environment.
2. In Solution Explorer, select and hold (or right-click) your project, and then select **Add** > **New Item**.
3. Select **FinNaceOperations** > **Dynamics 365 Items** > **Code** > **Class**.
4. Enter a meaningful name for the class, such as **MyBatchClass**.
5. Inside the new class, define the class by extending the `RunBaseBatch` class. The `RunBaseBatch` class provides the basic functionality that's required for batch processing.

   ```
   X++

   class MyBatchClass extends RunBaseBatch
   {
       // Your code will go here
   }
   ```

6. As required, override the methods that the `RunBaseBatch` class provides. The most commonly overridden methods are `run()` and `main()`.

   ```
   X++
   ```

Enable batch retries

Article • 03/21/2024

Implementation of a retry mechanism in Finance and Operations Batch is vital for maintaining robust data processing. A retry mechanism provides fault tolerance by automatically handling transient errors. Therefore, it ensures uninterrupted operation without requiring manual intervention. In addition, it enhances data integrity by reprocessing incomplete or failed transactions. Therefore, it reduces the risk of data loss. By minimizing downtime and manual intervention, a retry mechanism improves operational efficiency, so that batch processing can proceed smoothly, despite intermittent errors or disruptions.

Retry mechanisms for batch tasks

Two types of retries can be used for batch tasks:

- **Retry for any error or batch server restart –** To configure this type of retry, adjust the retry count on the batch task through the **Batch job** page.
- **Retry for SQL transient connection errors –** You can achieve this type of retry through code, either by implementing the **BatchRetryable** interface on the batch class or by using **BatchInfo** to set the **Idempotent** attribute for the batch class.

Retry for any error or batch server restart

You can configure this functionality through the batch job setup, by adjusting the retry count on the batch task. The **Maximum retries** parameter determines the number of retries that are attempted for a task, regardless of the error type or batch server restart. If a task fails, the batch platform evaluates the number of retries that have been performed. If the count is less than the **Maximum retries** value, the task is reset to a ready state for reprocessing. The highest allowed value for the **Maximum retries** parameter is **5**.

To set the **Maximum retries** value via the Batch user interface, follow these steps.

1. On the **Batch jobs** page, select **Batch task details**.
2. On the **General** tab, adjust the value of the **Maximum retries** field for the batch task.

> ⓘ **Note**

Batch parameter versioning

Article • 03/25/2024

In finance and operations apps, batch processing is used to run tasks asynchronously in the background. Batch jobs can range from simple tasks such as data import to complex calculations or integrations.

There are various situations where it might be necessary to update batch parameters and version them. Here are some examples:

- **Configuration changes –** Changes in the configuration settings or parameters might be required for batch processing. For example, a batch job that previously processed data in a specific way must now accommodate new fields or data sources. In these cases, you might have to update the batch parameters.
- **Performance optimization –** As your system evolves and grows, you might find opportunities to optimize batch processing for better performance. This optimization might involve adjusting batch parameters such as batch size or datasets to make the processing more efficient.
- **Software updates or enhancements** – If bugs are found in batch processing, or if new features affect batch jobs, you might have to change the batch parameters to fix issues or include new functions.
- **Integration changes –** Changes might be made in external systems or interfaces that interact with batch jobs, such as API endpoints or data formats. In these cases, you might have to update the batch parameters to accommodate the changes and ensure seamless integration.

Versioning of batch parameters is essential for maintaining a record of changes and ensuring consistency and reliability in batch processing. It lets you track the history of parameter changes, revert to previous versions if you must, and maintain documentation for auditing purposes. It also helps you manage and deploy changes across different environments, such as development, testing, and production environments.

Why you might receive errors during batch parameter unpack

When you run a batch, you might receive an error message like "An error occurred while unpacking parameters for batch job XXXXX." This error occurs when the batch job can't correctly unpack the parameters because of issues such as the following list:

Active batch periods

Article • 06/03/2022

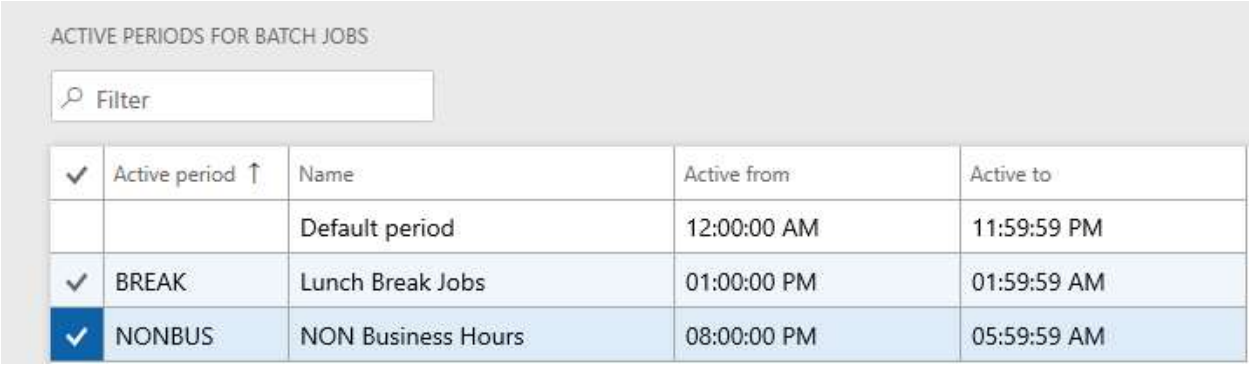
With the release of Platform update 21, an additional level of control over when batch jobs execute is now available. Previously, it was only possible to schedule a batch job to execute every hour for a specified number of hours or until a given date. Administrators can now provide information for an additional active period, such as in the following scenarios:

- Specifying time ranges during which jobs within a batch group can start execution.
- Selecting to run batch jobs outside of office hours only.
- Setting the recurrence for anytime within the active period. For example, you administrator might select to run the batch jobs every hour, but only between the hours of 6:00 PM and 8:00 AM.

> ⓘ **Note**
>
> This feature is available as of Platform update 21.

Set up active periods for batch jobs

1. Go to **System administration** > **Setup** > **Active periods for batch jobs**.
2. Enter the name of the batch job, and specify start and end dates that the batch job is active.
3. Click **Save**.



✓	Active period ↑	Name	Active from	Active to
		Default period	12:00:00 AM	11:59:59 PM
✓	BREAK	Lunch Break Jobs	01:00:00 PM	01:59:59 AM
✓	NONBUS	NON Business Hours	08:00:00 PM	05:59:59 AM

Assign active periods to batch jobs

1. Go to **System administration** > **Inquiries** > **Batch jobs**.
2. Select the batch job that you want to assign a period to, and click **Edit**.

Daylight saving time support for active batch periods

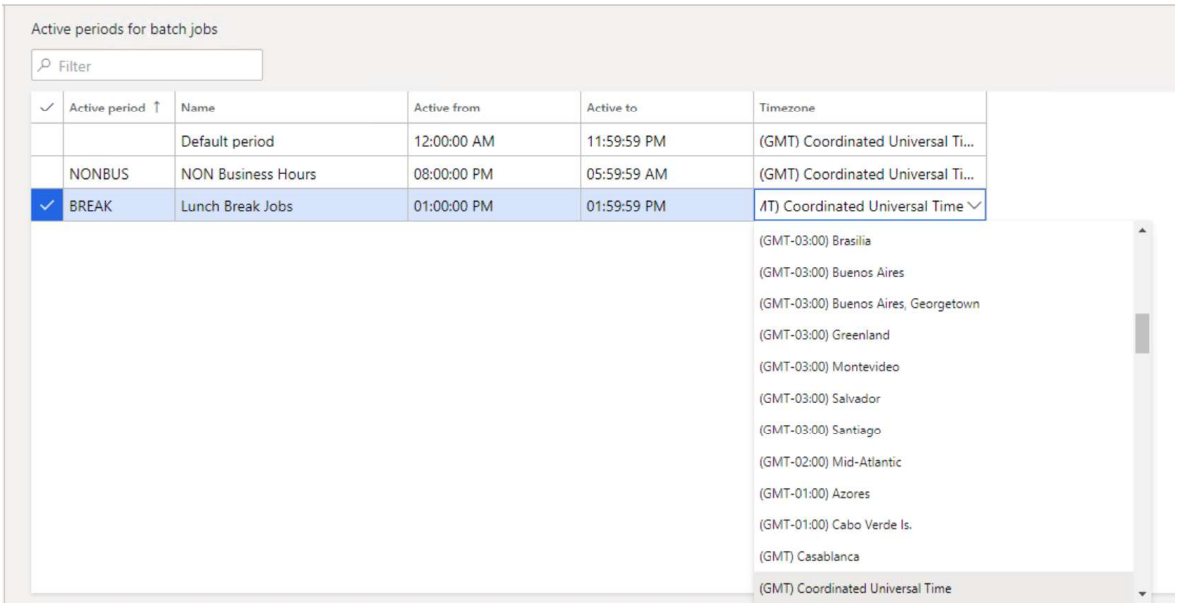
Article • 08/12/2022

Microsoft Dynamics 365 Finance version 10.0.12 includes a **Daylight Saving Time support for batch job active periods** feature that can be turned on in Feature management. This feature introduces daylight saving time (DST) support for the active periods for batch jobs and lets users associate their active periods with different time zones.

> **Note**
>
> This feature is a one-way feature. In other words, it can't be turned off after it's turned on.

When this feature is turned on, the following changes occur:

- On the **Active periods for batch jobs** page, a **Timezone** field is added for each active period. This field specifies the time zone that the active period uses. By default, every active period initially uses the Coordinated Universal Time (UTC) time zone.



- The start and end times of existing active periods are adjusted according to the UTC time zone. 'Although the active periods will continue to start and end at the same times that they previously started and ended, the times that are shown might change if the user's preferred time zone isn't UTC.

Batch manager security role

Article • 06/03/2022

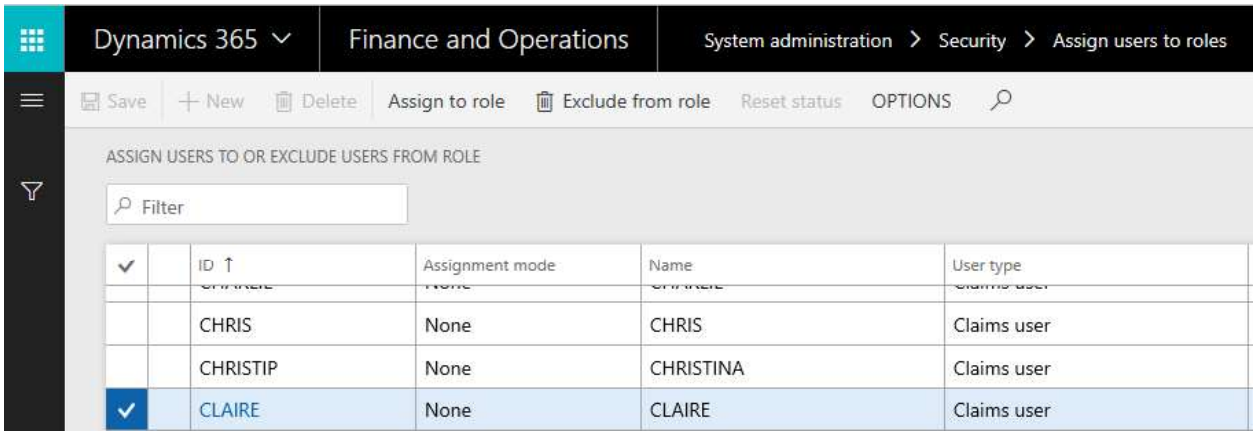
Before Platform update 20, users needed to be assigned to the system admin or IT admin security role to manage batch jobs. With the release of Platform update 20, there is a more targeted role, Batch manager. With this security role, a user now has permissions to copy batch jobs, change who will execute jobs, and specify the time ranges during which jobs can execute. The Batch maintain security privilege is part of the Batch manager security role and it allows a user to create an ad hoc batch job and grant privileges to other users.

> **Note**
>
> This feature is available as of Platform update 20.

Assign the Batch manager role to a user

Complete the following steps to assign the Batch manager security role to a specific user.

1. Select **System administration** > **Security** > **Assign users to roles**.



2. Select **Batch Job Manager**, and on the left pane, select **Manually assign/exclude user**.

Set up alerts

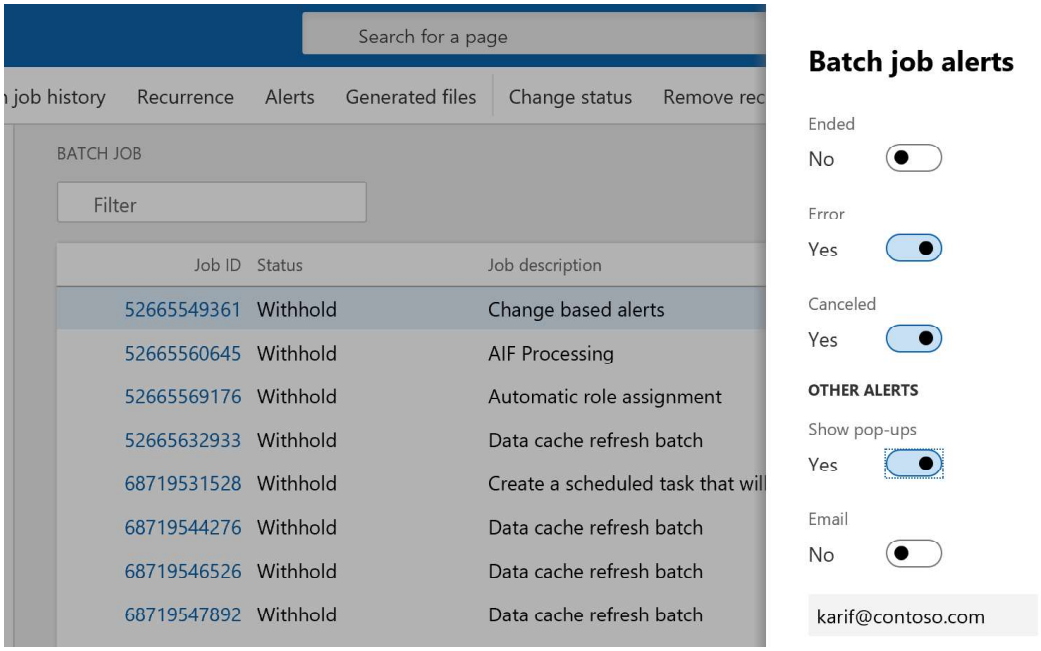
Article • 07/01/2022

Alerts form a notification system for critical events in finance and operations. You can use alerts to stay informed about events that you want to track during the workday. You can set up a set of alert rules so that you're alerted when a batch job ends, ends in error, or is canceled. You can select whether the alerts are emailed to you or appear as notifications in the Action center. Alerts can be set up per batch job and per user.

Set up alerts for batch enhanced forms

Follow these steps to set up alerts for batch enhanced forms.

1. Go to **System administration** > **Inquiries** > **Batch jobs**.
2. Select a batch job in the list, and then, on the Action Pane, select **Alerts**.
3. In the **Batch job alerts** dialog box, configure the alerts, and then select **OK**.



4. Check the Action center for alert notifications.

Enhanced batch forms

Article • 06/03/2022

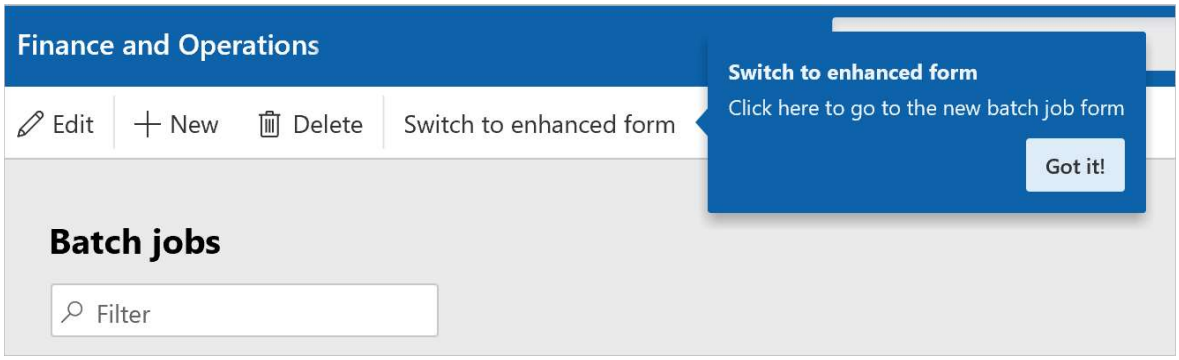
You can open an enhanced detail transaction form by selecting the job ID for a batch job. The enhanced form provides a header and lines that summarize the batch tasks and constraints that are related to the selected batch job.

Switch to the enhanced form

Follow these steps to switch to the enhanced form.

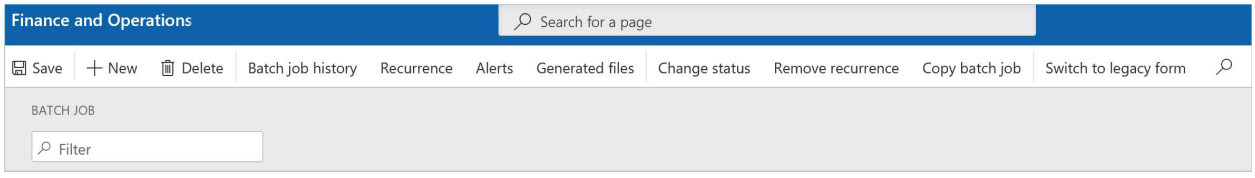
1. Go to **System administration** > **Inquiries** > **Batch jobs**.

   You're notified about the enhanced form. The notification shows the location of the **Switch to enhanced form** button on the Action Pane.



2. Select **Switch to enhanced form**.

To switch back to the unenhanced form, select **Switch to legacy form** on the Action Pane of the enhanced form.



Feedback

Was this page helpful? Yes No

Provide product feedback

Clean up the batch job history

Article • 05/02/2024

When you run a batch job, a history is recorded. This history can be used to monitor the correct execution of jobs. However, when several batch jobs are created, especially batch jobs with high recurrence, many batch job history entries are generated. Too many entries in the history table can negatively affect the performance of future jobs.

Two pages added to the **System administration** module make it easy to clean up the batch job history:

- System administration > Periodic tasks > Batch job history clean-up
- System administration > Periodic tasks > Batch job history clean-up (custom)

Batch job history clean-up

Follow these steps to quickly clean up all history entries that are older than a specified number of days.

1. On the **Periodic tasks in System administration** module, select **Batch job history clean-up**.
2. In the **History limit (days)** field, specify the number of days to keep a history of batch jobs.
3. Select **OK**.

Batch job history clean-up (custom)

The custom batch job lets you apply other filtering, based on criteria such as status, job description, company, or user. You can also add other filter criteria by selecting the **Filter** button.

1. On the **Periodic tasks in System administration** module, select **Batch job history clean-up (custom)**.
2. In the **History limit (days)** field, specify the number of days to keep a history of batch jobs.
3. In the **Records to delete in a transaction** field, input a value ranging from **10** to **100** to indicate the number of records to delete within a single database transaction. The associated job iterates through and removes data in batches of this size until all records are deleted. When the batch job processes a large volume of data, particularly within the parameters and information log fields of related jobs and

Clean up the batch job table

Article • 05/02/2024

Over time, new batch jobs are created for specific user actions, one-time jobs are run, and batch jobs are re-created. As a result, many abandoned or unused batch jobs accumulate in the system. Accumulated batch jobs can eventually lead to the growth of the batch job table and related tables. This growth can negatively affect the performance of other jobs.

In version 10.0.39 (Platform update 63), the **System administration** module includes a **Batch job clean-up** page that simplifies the process of cleaning up the batch job table. To open this page, go to **System administration** > **Periodic tasks** > **Batch job clean-up**.

Run batch job cleanup

To quickly clean up the records in the batch job table, follow these steps.

1. Go to **System administration** > **Periodic tasks** > **Batch job clean-up**.
2. In the **Retain jobs (days)** field, specify the number of days to keep the records of batch jobs.
3. In the **Records to delete in a transaction** field, input a value ranging from **1** to **200** to indicate the number of records to be deleted within a single database transaction. The associated job iterates through and removes data in batches of this size until all records are deleted. When the batch job processes a large volume of data, particularly within the parameters and information log fields of related jobs and tasks, it's advisable to enter a smaller number. This approach facilitates deletion in smaller segments and prevents the obstruction of other jobs.
4. In the **Caption** field, specify the title of the batch job to be deleted. The matching process is case-insensitive and requires an exact match.
5. In the **Class** field, specify the class name of a batch task for the batch job to delete.
6. Enable the **Delete by end date time** field if the cleanup should consider the end date/time of the last execution to determine which batch jobs to delete. By default, the cleanup considers the creation date/time.
7. In the **Created by** field, specify the user ID of the person who created the job.
8. In the **Withhold**, **Error**, **Finished**, and **Canceled** terminal status fields, select at least one option to delete the batch jobs.
9. Select **OK**.

Best Practice

Cancel a running batch job

Article • 11/17/2023

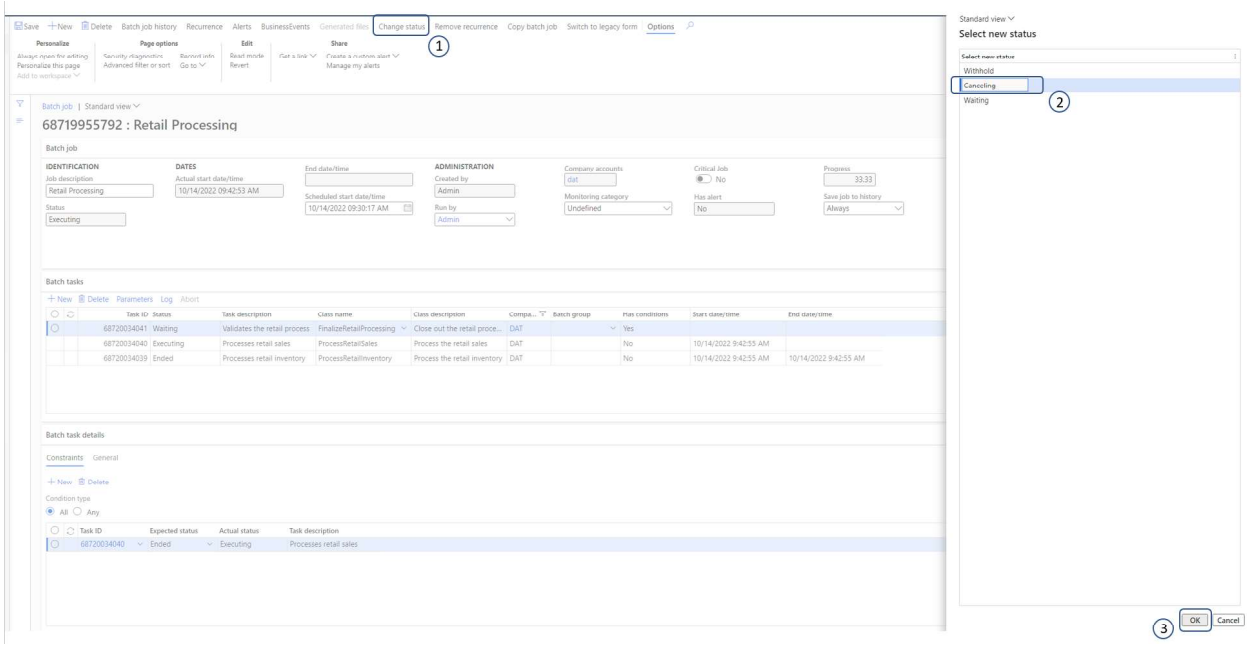
Cancel a batch job

> **Note**
>
> System jobs can't be moved to **Canceling** status.

If you must cancel a batch job that is running, you can change its status to **Canceling**. The batch job is then prevented from picking up new tasks. The status of tasks in the batch job that hasn't started is set to **Didn't run**, and the status of tasks that have started is set to **Canceling**. The status of a task isn't changed until that task can be terminated gracefully (that is, either it completes or it errors out).

To cancel a running batch job, follow these steps.

1. On the **Batch job** page, on the Action Pane, select **Change status**.
2. In the **Select new status** dialog box, under **Select new status**, select **Canceling**.
3. Select **OK**.



The following illustration shows an example of a batch job and its tasks after batch job is canceled.

Batch OData API

Article • 07/01/2022

This article provides information about the batch Open Data Protocol (OData) application programming interface (API) and explains how you can use OData to reschedule a job.

In the existing batch processing functionality, if some types of job failures have to be retried, either with or without any changes, based on the interpretation of the error, they must be manually retried. For jobs that are scheduled to be run during off-peak times to avoid active business hours for customers, monitoring failures and re-triggering the jobs requires either 24/7 support or a wait time until users resume work during normal business hours.

Integration of business events with batch functionality

Business event capabilities enable customers to configure notifications about changes in state (started, failed, finished, or canceled) for batch jobs. Integration with Microsoft Power Automate lets customers capture information about affected jobs without having to sign in to the system. However, manual intervention is required if any action must be taken based on the business events.

For information about how to configure batch events, see Batch business events.

End-to-end automation

In version 10.0.22, the batch functionality now provides an OData API that can be used to requeue batch jobs. Customers can use the OData endpoint to requeue batch jobs that are in a terminal state. This feature can be integrated with any automation by using Power Automate, custom APIs, and so on.

Optimization advisor overview

Article • 09/29/2023

This article describes how you can use Optimization advisor to help ensure optimal configuration of finance and operations.

Overview

Incorrect configuration and setup of a module can adversely affect the availability of application features, system performance, and the smooth operation of business processes. The quality of business data (for example, the correctness, completeness, and cleanliness of the data) also affects system performance, and an organization's decision-making capabilities, productivity, and so on.

The **Optimization advisor** workspace is a tool that lets power users, business analysts, functional consultants, and IT support functions identify issues in module configuration and business data. Optimization advisor suggests best practices for module configuration and identifies business data that is obsolete or incorrect.

Optimization advisor periodically runs a set of best practice rules. A default set of rules is available, however users can also create rules that are specific to their customizations, solutions from independent software vendors (ISVs), and business data. For more information about how to create rules, see Create rules for Optimization advisor.

When a violation of a rule is detected, an optimization opportunity is generated and appears in the **Optimization advisor** workspace. A user can take appropriate corrective action directly from the **Optimization advisor** workspace.

Opportunities can be company-specific or cross-company, depending on the type of setup and data that is being validated. Cross-company opportunities can be viewed from all companies. To view the opportunities for a specific company, you must first select the company.

Standard security policies apply to optimization opportunities. For example, the optimization opportunities that are related to configuration of the **Warehouse management** module are visible only to users who have access to Warehouse management and can change its setup.

When you take action on some optimization opportunities, the system calculates the impact of the opportunity in terms of the reduction in the runtime of business processes. Unfortunately, this feature isn't available for all optimization opportunities.

Create rules for Optimization advisor

Article • 09/29/2023

This article explains how to create new rules for **Optimization advisor**. For example, you can create a new rule that identifies which Request for Quotations (RFQ) cases have an empty title. Using titles on cases makes them easily identifiable and searchable. While quite simple, this example shows what can be achieved with optimization rules.

A *rule* is a check on application data. If the condition that the rule evaluates is met, opportunities to optimize processes or improve data are created. The opportunities can be acted upon and, optionally, the impact of the actions can be measured.

To create a new rule for the **Optimization advisor**, add a new class that extends the **SelfHealingRule** abstract class, implements the **IDiagnosticsRule** interface, and is decorated by the **DiagnosticRule** attribute. The class must also have a method decorated with the **DiagnosticsRuleSubscription** attribute. By convention, that is done on the **opportunityTitle** method, which will be discussed later. This new class can be added to a custom model with a dependency on the **SelfHealingRules** model. In the following example, the rule being implemented is called **RFQTitleSelfHealingRule**.

X++

```
[DiagnosticsRule]
public final class RFQTitleSelfHealingRule extends SelfHealingRule
implements IDiagnosticsRule
{
…
}
```

The **SelfHealingRule** abstract class has abstract methods that must be implemented in inheriting classes. The core is the **evaluate** method, which returns a list of the opportunities identified by the rule. Opportunities can be per legal entity or can apply to the whole system.

X++

```
protected List evaluate()
{
    List results = new List(Types::Record);

    DataArea dataArea;

    while select id from dataArea
        where !dataArea.isVirtual
    {
```

Report a production outage

Article • 07/01/2022

Lifecycle Services (LCS) has a feature called **Report production outage**. This feature is available to all customers who have purchased one or more Dynamics 365 finance and operations apps and have implementation projects with a production environment deployed in LCS. This feature provides a quick and effective channel to escalate issues to Microsoft Support in the event that the services in a production environment are degraded or become unavailable.

Following mutually inclusive conditions, a production outage can be defined as one or more system-wide issues on a live production environment that impact multiple users and prevent your business from performing daily operations.

Reporting flow

The following list shows the order in which an issue should be handled:

1. In a live production environment, a customer experiences an outage or other situation with prevents business from continuing.
2. The customer reports a production outage issue by using the LCS Support portal.
3. The customer selects a production outage issue and provides additional information.
4. A Microsoft support engineer acknowledges the production outage ticket within 30 minutes of submission and begins to immediately collaborate with stakeholders to investigate and resolve the issue.
5. A support engineer contacts the customer to provide a status update.

Access and availability

All users who have been added to a customer's implementation project have access to this feature. This includes project owners, organization admins, team members, and environment managers.

This feature is available for:

- Dynamics 365 Finance
- Dynamics 365 Supply Chain Management
- Environments that are managed by Microsoft
- A production environment in the LCS project

Configure database logging

Article • 06/11/2023

Database logging provides a way to track specific types of changes to the tables and fields in Finance and Operation apps. Changes that can be tracked include insert, update, delete, and rename key operations. When you configure logging for a table or field, a record of every change to that table or field is stored in the database log table, **sysdatabaselog**, in the environment database.

Database logging can be used for these purposes:

- Create an auditable record of changes to specific tables that contain sensitive information.
- Monitor the use of electronic signatures. By default, all transactions that have been signed by using electronic signatures are logged.

Database logging is intended to track individual transactions. It isn't intended to track automated transactions that are run in batch jobs.

Security for database logging

Database logs can contain sensitive data. By default, any user who has database access can query the database log table (**sysdatabaselog**) by using X++ or alerts, or by querying the database directly. To help protect data, you should restrict permissions on the **sysdatabaselog** table for on-premises deployments.

Database logging and performance

Although database logging can be valuable from a business perspective, it can be expensive with regard to resource use and management. Here are some of the performance implications of database logging:

- The database log table can grow quickly and can increase the size of the database. The amount of growth depends on the amount of logged data that you decide to retain.
- When logging is turned on for a transaction type, each instance of that transaction type causes multiple records to be written to the Microsoft SQL Server transaction log file. Specifically, one record is written for the initial transaction, and one record logs the transaction in the database log table. Therefore, the transaction log file will grow more quickly and might require additional maintenance.

Build OData metadata cache when the AOS starts

Article • 08/12/2022

With the release of Platform update 32, we have introduced the ability to build OData metadata cache when the Application Object Server (AOS) starts, instead of when the first OData request is made. This significantly decreases the response time for the first OData call after an AOS process restart.

This option is useful if your business process can't wait for the OData metadata cache to be built each time that the AOS process restarts. Follow these steps to turn on this feature.

1. Go to **System administration** > **Setup** > **System parameters**.
2. On the **General Tab**, select **Build metadata cache when AOS starts**, and then select **Save**.

> **Note**
>
> When you enable this functionality, the AOS should already be running and should have served one OData request. This means that the cache is already built. This new functionality will take effect during the next AOS restart.

Feedback

Understand Interactive Application Object Server (AOS) restarts

Article • 01/09/2025

The interactive Application Object Server (AOS) might be restarted for several reasons. Here's an overview of these reasons:

- **Routine maintenance activities –** During routine maintenance activities, such as patching, there might be temporary interruptions to AOS services. To understand the effect of maintenance activities and access-known maintenance schedules, see the following articles:
  - Operating System Maintenance Schedule – Learn more about planned operating system maintenance schedules.
  - Experience during the nZDT Maintenance Window – Gain insights into system behavior during the nZDT maintenance window.
- **Interactive AOS server failures ("crashes") –** Failures on Interactive servers might occur because of application services that are currently running. Detailed failure information is available in Microsoft Dynamics Lifecycle Services. For more information about how to monitor failure information, see Monitoring and telemetry using Application Insights.
- **Infrastructure failover –** Restarts can occur if infrastructure issues lead to an internal failover. Autoscaling and capacity management are used to ensure optimal environmental performance and availability.

Feedback

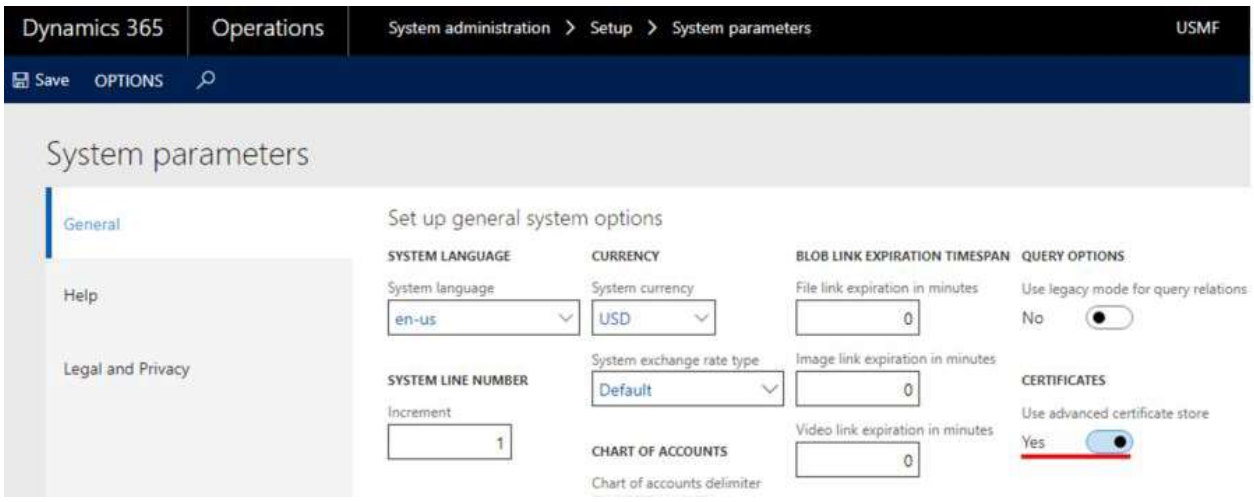
Set up the Azure Key Vault client

Article • 07/11/2024

The functionality for storing advanced certificates lets you define the type of certificate storage that is used in finance and operations apps.

The functionality provides two options for storing certificates: local storage and Microsoft Azure Key Vault storage. You can define the option that is used by setting the new **Use advanced certificate store** option on the **General** tab of the **System parameters** page (**System administration** > **Setup** > **System parameters**).

- **Local storage –** This storage option can be used with on-premises deployments and any kind of on-premises development environment. To use it, set the **Use advanced certificate store** option to **No**. This storage option is recommended for development environments that are used for development and validation purposes, where it's necessary to validate the certificate and work with it.
- **Azure Key Vault storage –** This storage option is required for cloud deployments, but it can also be used with on-premises deployed environments and any kind of on-premises development environment. To use it, set the **Use advanced certificate store** option to **Yes**. This storage option is the only option for a production environment in the Azure cloud.



Some setup is required before you can work with certificates that are stored in Key Vault. For information about the required settings, see the following Microsoft Knowledge Base (KB) article: 4040294 - Maintaining Azure Key Vault storage. After you set up the Key Vault storage, you should link to the certificates in finance and operations apps.

After the certificate is installed in Key Vault, it must be set up in the application.

1. Go to **System administration** > **Setup** > **Key Vault parameters**.
2. Select **New** to create a new instance.

Cleanup routines in Dynamics 365 Finance and Dynamics 365 Supply Chain Management

Article • 03/14/2025

In Microsoft Dynamics 365 Finance and Dynamics 365 Supply Chain Management, cleanup routines are available in various modules. This article provides an overview of the routines that are currently available. The information is organized by module.

> **Important**
>
> These cleanup routines should be run only after the business has done detailed analysis and confirmed that the data is no longer required.
>
> Always test each cleanup routine in a test environment before you run it in a production environment.

System administration

Expand table

Path	Description
System administration > Periodic tasks > Notification clean up	This cleanup routine is used to periodically delete records from the EventInbox and EventInboxData tables. **Recommendation:** If you don't use alert functionality, turn off the alert from the batch job.
System administration > Periodic tasks > Batch job history clean-up	This regular version of the batch job history cleanup routine lets you quickly clean all history entries that are older than a specified number of days. Any entry that was created earlier is deleted from the BatchJobHistory table, and also from linked tables that have related records (BatchHistory and BatchConstraintsHistory). This version has improved performance optimization, because it doesn't have to run any filtering.
System administration > Periodic tasks > Batch job history clean-up (custom)	This custom batch job history cleanup routine should be used only when specific entries must be deleted. You can clean up selected types of batch job history records, based on criteria such as status, job description, company, or user. You can add other criteria by using the **Filter** button.

Invalid users in Dynamics 365 Finance

Article • 11/15/2024

Users in any Microsoft Dynamics 365 finance and operations environment must comply with Microsoft guidelines to avoid sign-in failures. As of Dynamics 365 Finance version 10.0.39, administrators can use the **Invalid users** page to view details about invalid users.

To view invalid users, follow these steps.

1. Go **System administration** > **Invalid users**.
2. Select **Refresh**. This page shows a list of users who require attention from the system administrator. If there are no invalid users, the page is blank.

The following sections describe the five types of invalid users that must be addressed.

Users who aren't found in Microsoft Entra ID

All finance and operations apps users must be present in your Microsoft Entra ID tenant. Administrators can directly add users to your tenant through the Microsoft Entra ID portal. For more information, see Add or delete users.

You can use business-to-business (B2B) functionality to include these users in Microsoft Entra ID. For more information, see Export business-to-business (B2B) users to Microsoft Entra ID.

Users whose telemetry ID doesn't match the object ID from Microsoft Entra ID

For sign-in functionality to work correctly, the telemetry ID of a user in finance and operations apps must be aligned with the object ID of the same user in Microsoft Entra ID. If the IDs don't match, we recommend that you delete and then reimport the user. For more information, see Find the user object ID.

1. Verify that a user who has the corresponding email address exists in your Microsoft Entra ID.
2. Delete the user from finance and operations apps. Note the user roles before deleting so the roles can be added back after reimporting the users.
3. Reimport the user. For more information, see Create new users.