Infor Operating Service Infor Government Solutions (IGS) Enablement Guide

October 2020 release updated for May 2021

Copyright © 2021 Infor

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

Publication Information

Release: Infor Operating Service 2020-x

Publication date: May 20, 2021

Document code: inforosigseg

Contents

About this guide

The objective of this document is to explain the configuration changes that must be made after the installation of Infor Federation Services (IFS), Infor Ming.le™, ION API, Infor Homepages, and Infor Document Management (IDM) in the multi-tenant cloud to enable Infor Government Solutions (IGS).

Note: For Infor ION, no additional configuration steps are required to enable IGS. Configuration is automated for deployment.

Terminology

Term	Description
Infor Federation Services (IFS)	Provides single sign on and user management capabilities for Infor applications
Infor Ming.le	Provides portal, collaboration, and homepages capabilities for Infor applications
ION API	Provides API Gateway capability for Infor applications
Homepages	Provides access to homepage widgets and enables users to create homepages composed of one or more widgets
Infor Document Management (IDM)	Provides document management capability for Infor applications

Supported languages

Currently, only English (**en-US)** is supported for the IGS environment.

Security roles

When the tenant is provisioned, the tenant administrators have all of the required security roles to do the configuration at the tenant level.

Organization

This table shows the chapters of the guide:

Section	Description
Chapter 1, Enabling Infor Ming.le for IGS	Tasks required to enable Infor Ming.le for IGS
Chapter 2, Enabling Infor Homepages for IGS	Tasks required to enable Infor Homepages for IGS

Related documents

You can find documents in the product documentation section of the Infor Support Portal, as described in "Contacting Infor" on page 6.

- *Infor Operating Service Release Notes for 2021 for Infor Government Solutions (IGS) October 2020 release updated for May 2021*

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

If we update this document after the product release, we will post the new version on the Infor Support Portal. To access documentation, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Changes for this release

Service accounts are now available in IGS. Any risk associated to the Service Accounts is deferred to customers as documented in our customer responsibility matrix.

The SCIM services are now available in IGS. Integration with the customer identity provider (IdP) is IGS approved. It is the recommended automated method for user provisioning.

Chapter 1 Enabling Infor Ming.le for IGS

The 12.0.43 version of Infor Ming.le is being implemented for the current release of Infor OS IGS (Infor Government Solutions).

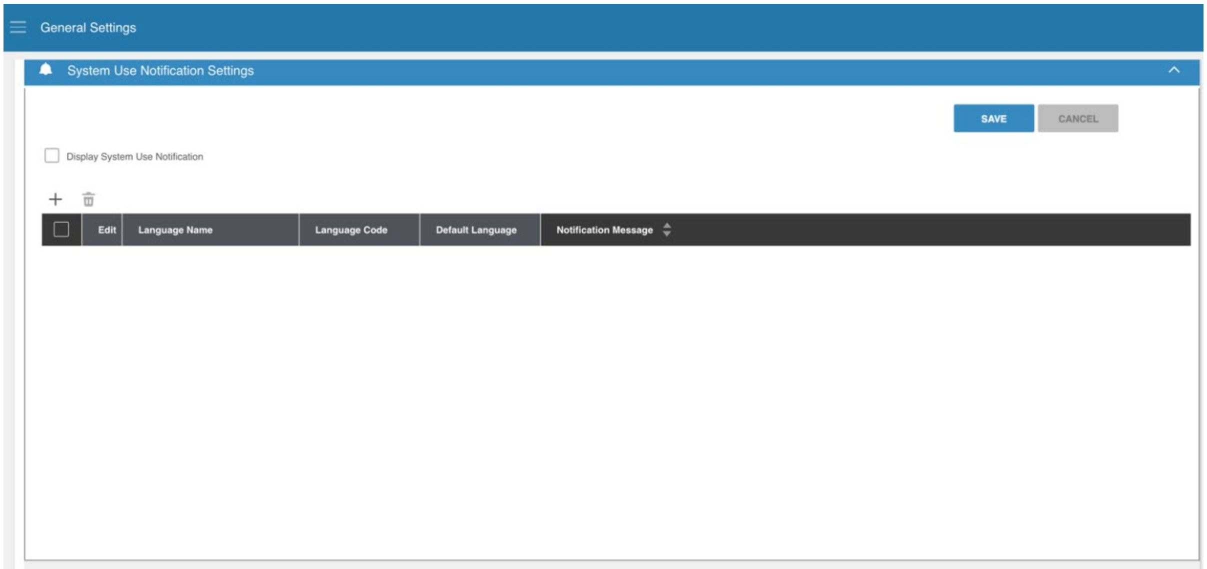
To enable Infor Ming.le for IGS, complete the tasks in this chapter.

Enabling system use notification settings

After the IGS feature flag is enabled, an IFS administrator must ensure that the System Use Notification Settings are configured and enabled at the tenant level.

As an IFS administrator, access the **System Use Notification Settings** page:

1. Log in to the Infor Ming.le portal.
2. Select **User Menu > User Management**.
3. On the left navigation menu, click **Security Administration > Settings > General Settings**.
4. Click **System Use Notification Settings** to display the **System Use Notification Settings** page:



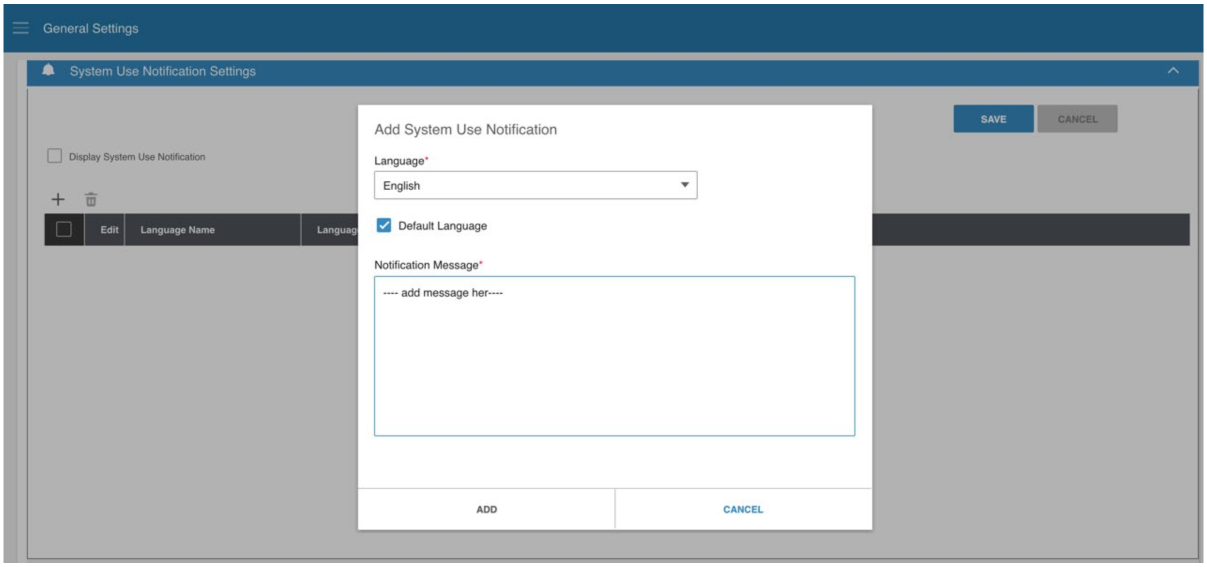
5 Use the plus (+) icon to add the notification message as shown below:

6 Select the language code as `English (en-US)` from the **Language** drop-down box.

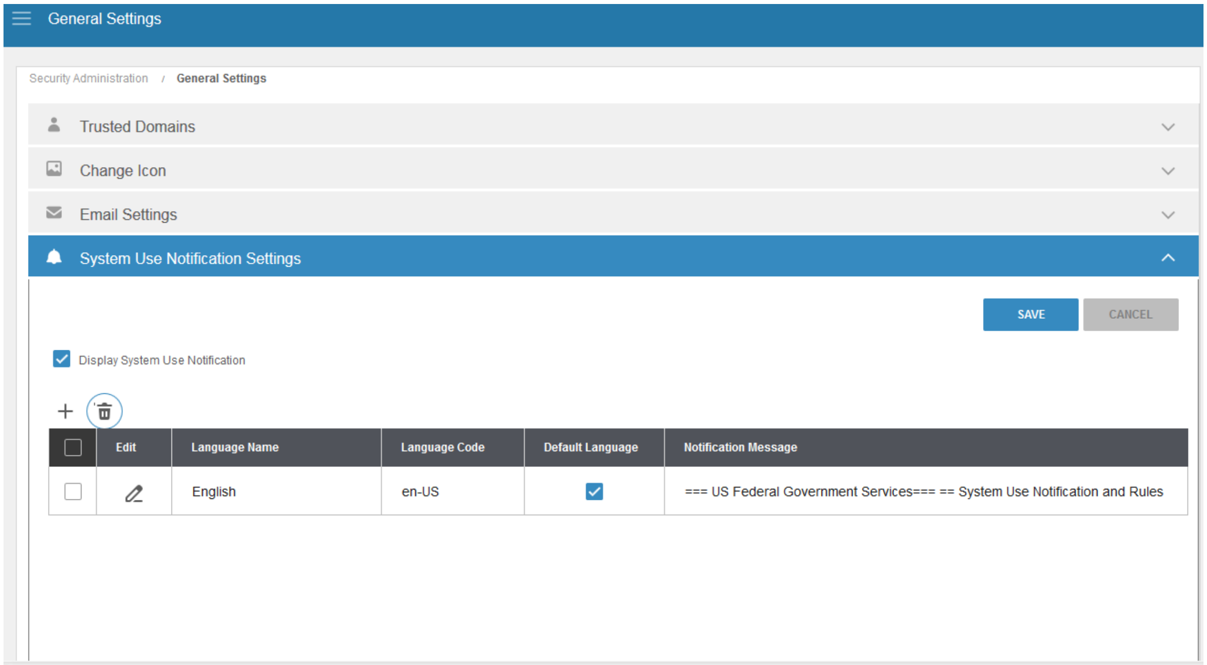
7 Select the **Default Language** check box to set `English` as the default language to display the system notification message.

Note: Currently, English is the only supported language.

8 Specify a valid notification message in the **Notification Message** box.



9 Click **ADD** to save the information to the database.



General Settings
Security Administration / General Settings
Trusted Domains
Change Icon
Email Settings
System Use Notification Settings
SAVE
CANCEL

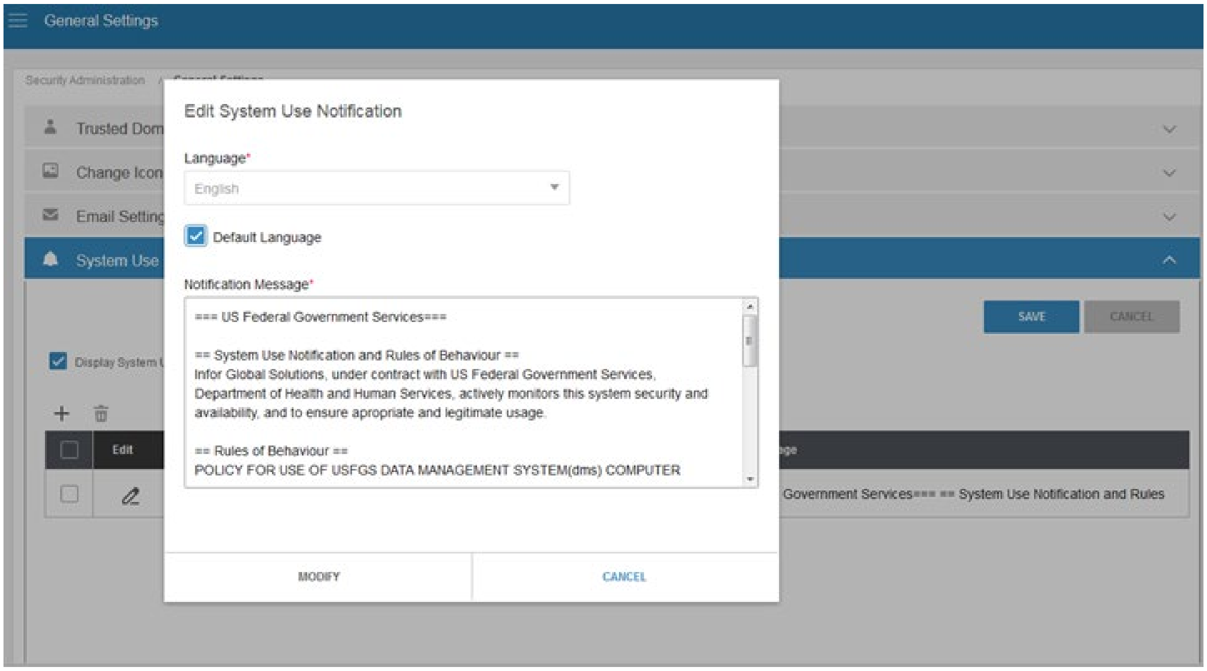
☑ Display System Use Notification

□	Edit	Language Name	Language Code	Default Language	Notification Message
□	✎	English	en-US	☑	=== US Federal Government Services=== == System Use Notification and Rules

10 Click **SAVE** to save the information on the **System Use Notification Settings** page.

Editing the system use notification

1 Click the edit icon to modify the notification message.



Edit System Use Notification

Language*
English

☑ Default Language

Notification Message*

```
=== US Federal Government Services===

== System Use Notification and Rules of Behaviour ==
Infor Global Solutions, under contract with US Federal Government Services,
Department of Health and Human Services, actively monitors this system security and
availability, and to ensure apropriate and legitimate usage.

== Rules of Behaviour ==
POLICY FOR USE OF USFGS DATA MANAGEMENT SYSTEM(dms) COMPUTER
```

2 Edit the message in the **Notification Message** box and click **MODIFY** to save the changes.

3 Click **SAVE** to save the information on the **System Use Notification Settings** page. The information is updated in the database.

Creating and configuring Federated Security, Part 1

As the tenant administrator, set up the Federated security:

1 On left navigation pane, select **Security Administration > Federated Security**.

2 Click the plus (+) icon.

3 In the SAML 2.0 section of the **Federated Security** tab, complete the IDP parameters:

   a Select the **SAML 2.0 Enabled** option.

   b Specify the **Display Name**.

   c In the Import SAML Metadata section, click **From File**, select the metadata file (FederationMetadata.xml) provided by the ADFS server, and confirm that the fields below are populated:

   - The Issuer
   - Identity Provider Certificate
   - Assertion Consumer Service
   - Single Logoff Service

   d In the Assertion Identity Key section, select **Identity is a NameIdentifier element of the Subject statement**.

   e Select **`Email Address`** in the **IFS user lookup**.

   f Click **Save**.

   g Select the **JIT User Provisioning Enabled** check box.

4 Specify the First Name claim:
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`

5 Specify the Last Name claim:
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

6 Specify the Email Address claim -
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

Note: With Just-in-Time provisioning, SAML assertion attributes are used to create users the first time they try to log on to Infor Ming.le.

7 Click **Save** to save the configurations.

8 Click **View** to view the service provider information.

9 Click **EXPORT SAML METADATA (.xml)**. This metadata file is used to configure IDP.

Creating and configuring Federated Security, Part 2

1 Log on to the ADFS machine and launch the ADFS console.

2 Create a relying party trust:

   a Select the Relying Party Trusts folder.

   b Select **Actions > Add Relying Party Trust > Welcome to the Add Relying Party Trust Wizard**.

   c Select `Claims aware` and click **Start**.

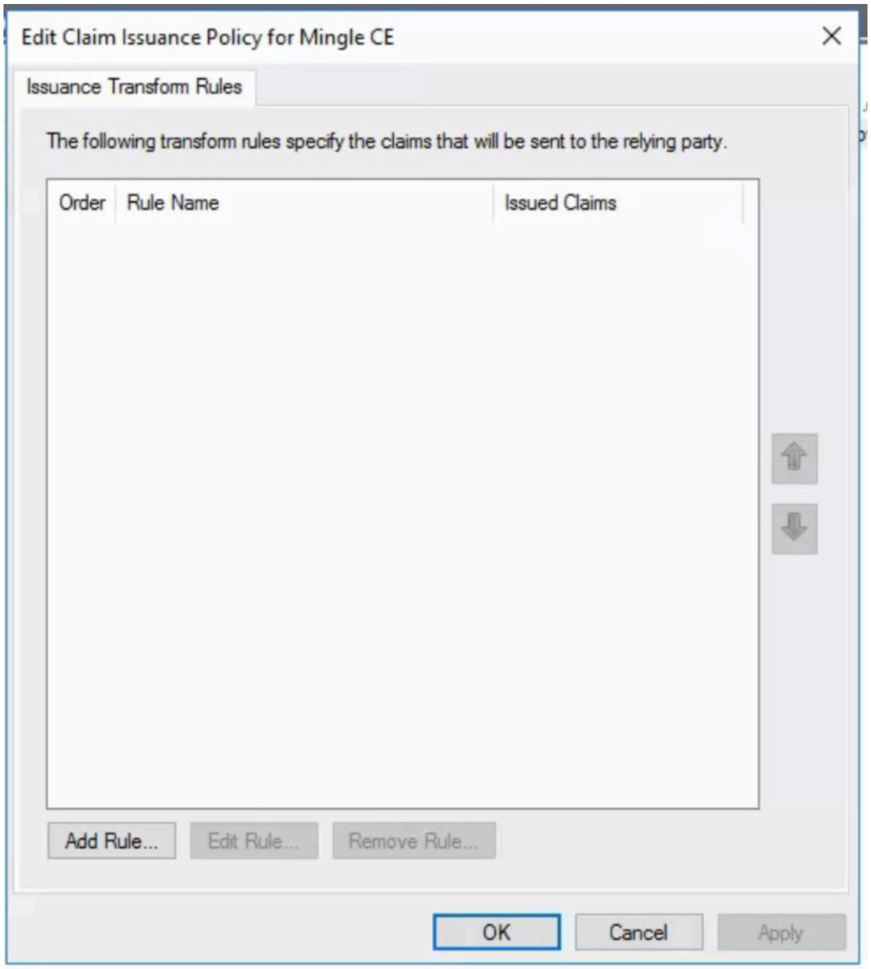
   d Select the **Import data about the relying party from a file** option. Select the sp-metadata.xml file obtained in “Creating and configuring Federated Security, Part 1” and click **Next**.

   e Specify the **Display name** and click **Next**.

   f Select **Permit everyone to access this relying party** and click **Next**.

   g Click **Next** on Ready to Add Trust.

   h Click **Close**. The claim rule dialog box is opened.



Edit Claim Issuance Policy for Mingle CE

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

3 Add these rules for this relying party trust created:

Rule 1

a Choose the rule type:

Claim Rule Template: `Send LDAP attributes as claims` and click **Next**.

b Configure the claim rule:

Claim Rule Name: `Get Ldap Attributes`

Attribute Store: `Active Directory`

Map LDAP attributes to outgoing claim types:

LDAP attribute	Outgoing claim type
E-mail-Addresses	E-mail-Address
Given-Name	Given Name
Surname	Surname

c Click **Finish**.

Rule 2

a Choose the rule type:

Claim Rule Template: `Transform an Incoming Claim`

Click **Next**.

b Configure the claim rule:

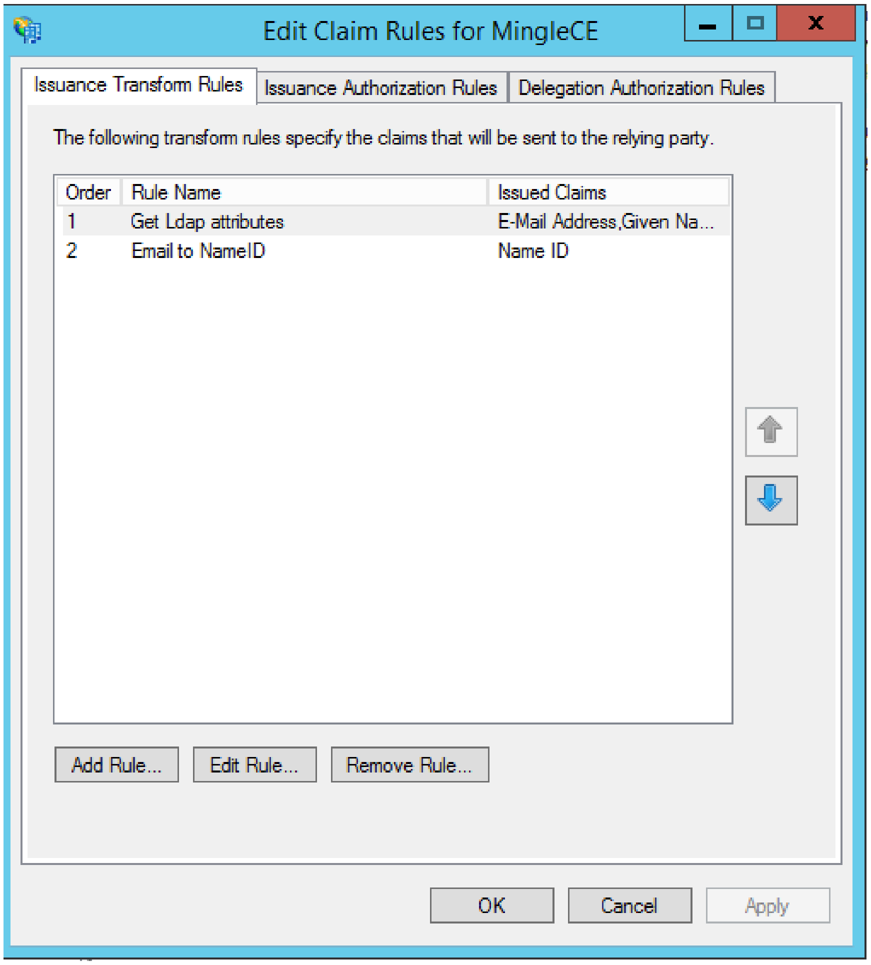
Claim Rule Name: `Email to NameID`

Incoming Claim Type: `E-mail Address`

Outgoing Claim Type: `NameID`

Outgoing name ID Format: `Unspecified`

c Click **Finish**.


Edit Claim Rules for MingleCE
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Get Ldap attributes	E-Mail Address,Given Na...
2	Email to NameID	Name ID

d Click **Apply** and **OK**.

Enabling Federated Identities as the IDP

To ensure that the handshake is complete and to enable the option for Federated Identities:

1. Log in to the Infor OS IGS CloudSuite.
2. Select **User Menu > User Management**.
3. On the left navigation menu, click **Security Administration > Authentication URL Options**.
4. Select the **Allow users to choose the authentication mode** option.
5. Click **Save**.

This option enables users to select ADFS as an IDP during the initial logon.

Adding the capability for multiple federated IdPs to IGS

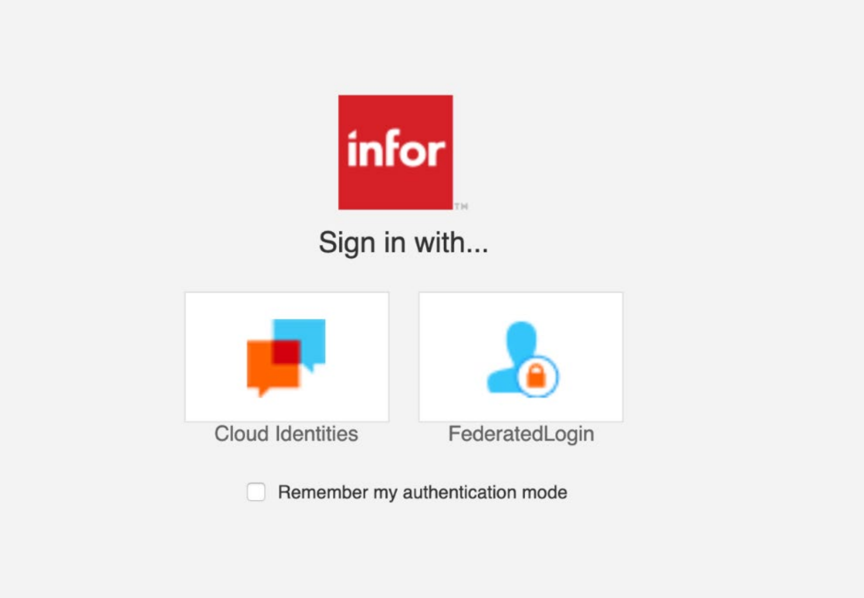
To add multiple federated IdPs to IGS:

1. Set IFSMULTIPLEIDP=1 / trueset
2. MaxAllowedIdp=5

Testing

Note: Ensure you are on the IGS network before testing ADFS connection.

1. After the trust is established, open the Infor Ming.le URL, which displays two IDP options.



2 Select **ADFS**, which is the **Display Name** given while configuring the CloudSuite in Part 1. You are redirected to the ADFS server login page.

3 Provide a user name and password.

When you are successfully authenticated, you are redirected to the Infor Ming.le page.

Enabling Multi-Factor Authentication (MFA)

In the IGS environment, you must configure your own MFA on your identity provider.

Adding Multi-Factor Authentication for Infor Ming.le Identities to IGS

To add MFA for Infor Ming.le Identities to IGS:

1 Set IFSMULTIPLEIDP=1 / true

2 Set MFA =1

Disabling Infor Communities Identities

In the IGS environment, Infor Communities Identities are not supported. You must turn off the feature for external users:

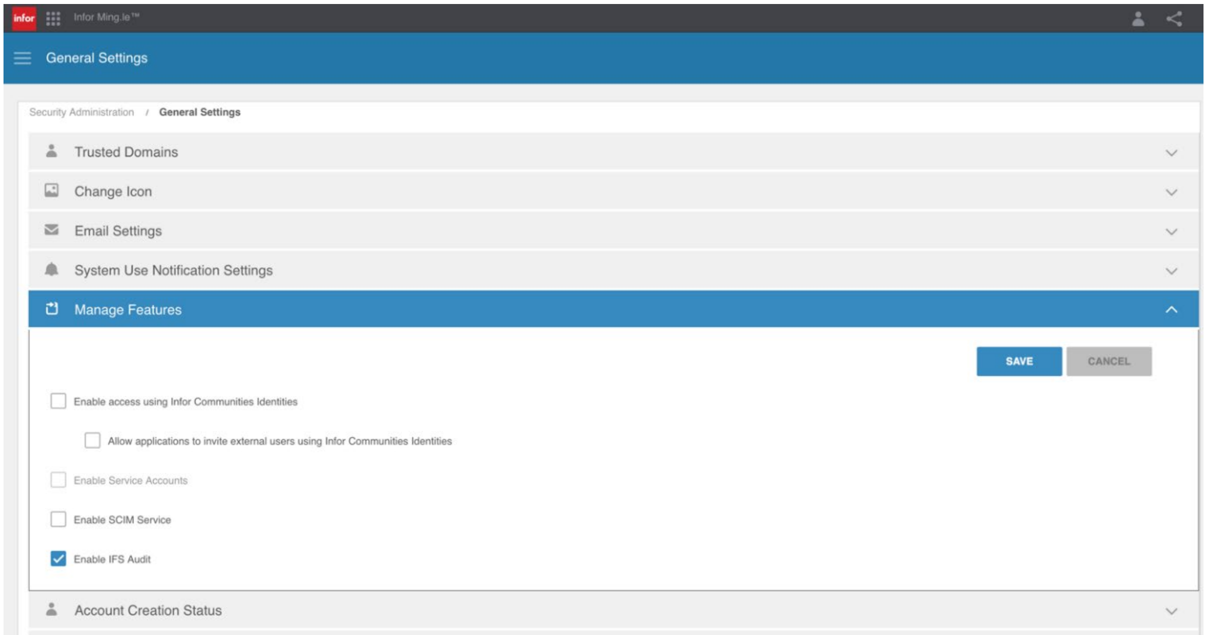
1 On the left navigation menu, select **Security Administration > Settings > General Settings**.

2 Click **Manage Features** and confirm that the check boxes for these settings are cleared:

- **Enable access using Infor Communities Identities**

  This setting controls access to the Infor Ming.le application using Infor Communities Identities. Once disabled, this setting does not allow users to access the Infor Ming.le application using Infor Communities Identities.

- **Allow application to invite external users using Infor Communities Identities**



□ Enable access using Infor Communities Identities

□ Allow applications to invite external users using Infor Communities Identities

□ Enable Service Accounts

□ Enable SCIM Service

☑ Enable IFS Audit

3 Click **SAVE**.

Configuring service accounts

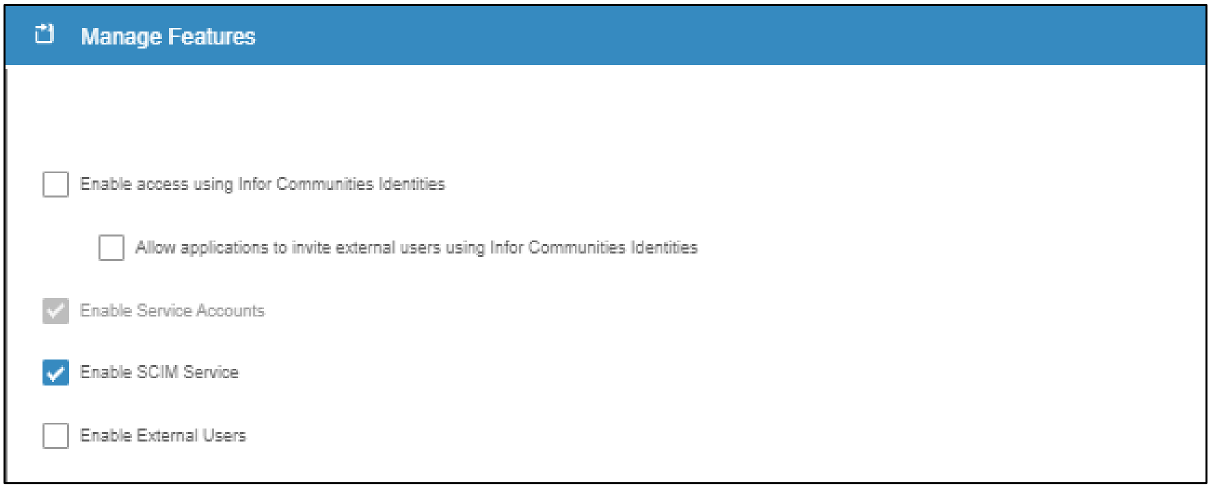
Note: The **Service Accounts** page is not displayed when the **Enable Service Accounts** setting is disabled.

To configure the setting:

1 On the left navigation page, select **Security Administration > Settings > General Settings**.

2 Expand **Manage Features**.

3 Configure the feature by selecting the **Enable Service Accounts** check box.



Manage Features

☐ Enable access using Infor Communities Identities

☐ Allow applications to invite external users using Infor Communities Identities

☑ Enable Service Accounts

☑ Enable SCIM Service

☐ Enable External Users

Configuring the SCIM service

The page where the SCIM service can be configured is enabled by default.

Note: The **SCIM Accounts** page is not displayed when the **Enable SCIM Service** setting is disabled.

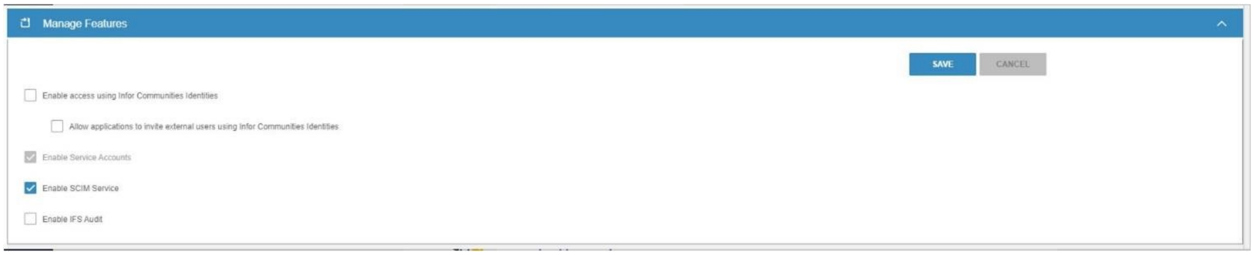
To configure the SCIM service:

1 On the left navigation page, select **Security Administration > Settings > General Settings**.

2 Expand **Manage Features**.

3 Confirm that the **Enable SCIM Service** check box is selected.

The user can use the **Enable SCIM Service** option in the **Manage Features** menu to enable and disable SCIM accounts. Further information on managing SCIM accounts can be found in the *Infor Ming.le Cloud Edition Online Help*.



Manage Features

☐ Enable access using Infor Communities Identities

☐ Allow applications to invite external users using Infor Communities Identities

☑ Enable Service Accounts

☑ Enable SCIM Service

☐ Enable IFS Audit

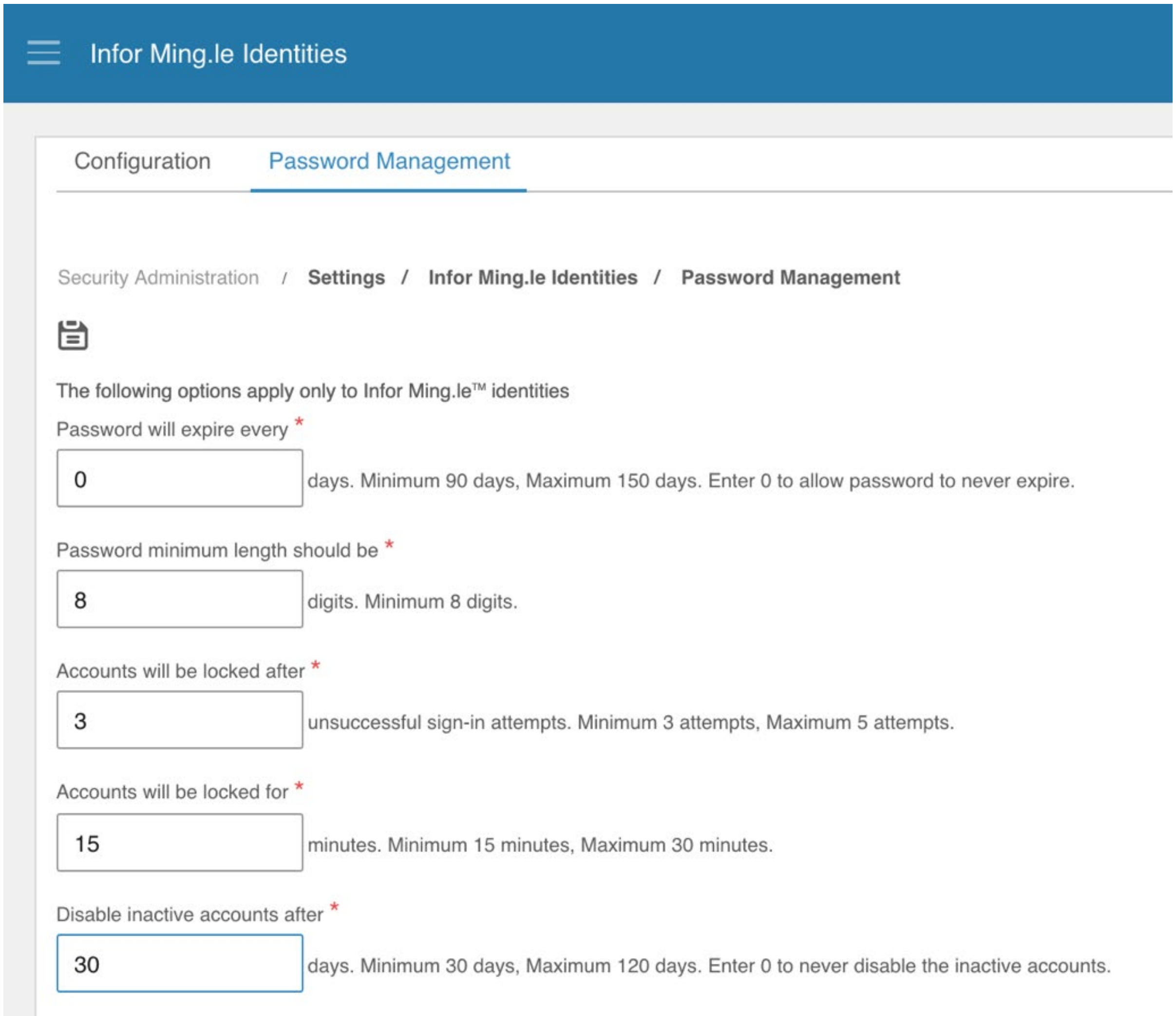
Configuring inactive accounts

The **Disable inactive accounts after** setting determines the number of inactive days before a user account is disabled. The system automatically disables a user account after the specified number of days.

To configure the inactive days value:

1 On left navigation pane, select **Security Administration > Settings > Infor Ming.le Identities > Password Management**.

2 In the **Disable inactive accounts after** field, specify a value from `30` to `120` days.


Infor Ming.le Identities
Configuration
Password Management
Security Administration / Settings / Infor Ming.le Identities / Password Management

The following options apply only to Infor Ming.le™ identities

Password will expire every *
0 days. Minimum 90 days, Maximum 150 days. Enter 0 to allow password to never expire.

Password minimum length should be *
8 digits. Minimum 8 digits.

Accounts will be locked after *
3 unsuccessful sign-in attempts. Minimum 3 attempts, Maximum 5 attempts.

Accounts will be locked for *
15 minutes. Minimum 15 minutes, Maximum 30 minutes.

Disable inactive accounts after *
30 days. Minimum 30 days, Maximum 120 days. Enter 0 to never disable the inactive accounts.

3 Click **SAVE**.

Enabling and configuring concurrent sessions

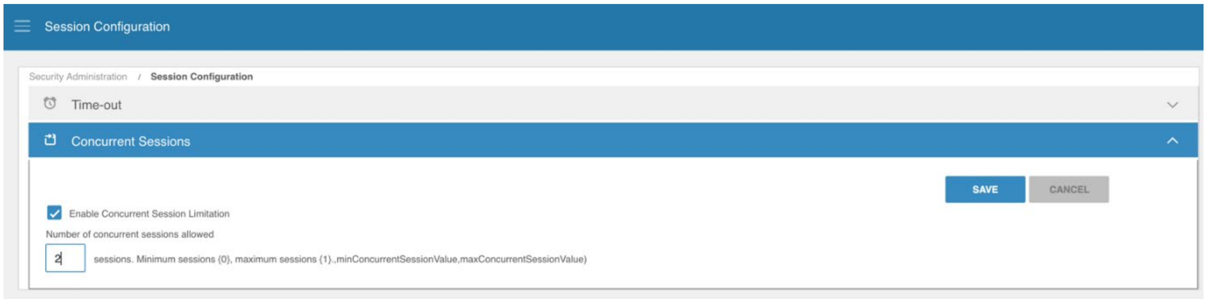
The **Concurrent Sessions** setting determines the number of sessions a user can have at one time within the system. The system can restrict the user to a maximum of 1 to 5 sessions. By default, the concurrent sessions limitations setting is disabled.

To enable and configure the concurrent sessions value:

1 On left navigation pane, select **Security Administration > Session Configuration > Concurrent Sessions** tab.

2 Select the **Enable Concurrent Session Limitation** check box.

3 Set the value for **Number of concurrent sessions allowed**.



☑ Enable Concurrent Session Limitation

Number of concurrent sessions allowed

2 sessions. Minimum sessions {0}, maximum sessions {1}.,minConcurrentSessionValue,maxConcurrentSessionValue)

4 Click **SAVE**.

Adding users

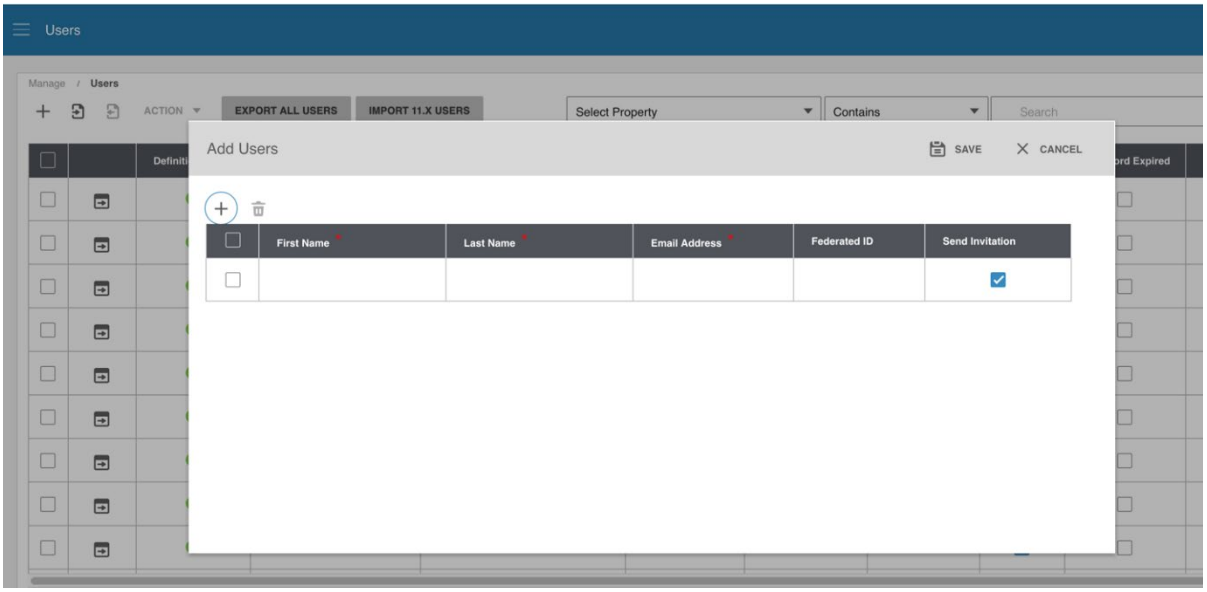
Users (Tenant Administrators) sign into the Infor Ming.le portal site by using Infor Ming.le Identities authentication mode:

- Infor Ming.le Identities are enabled by default to the tenant administrators to configure the environment and set up the Federated Identities for the users.
- Users can be added to the system in these ways:
  - Manually adding each user
  - Importing users from a file

Adding users manually

1 On the left navigation menu, select **Manage > Users**.

2 Click the plus (+) icon to display the **Add Users** page.



3 Complete these fields for the user:

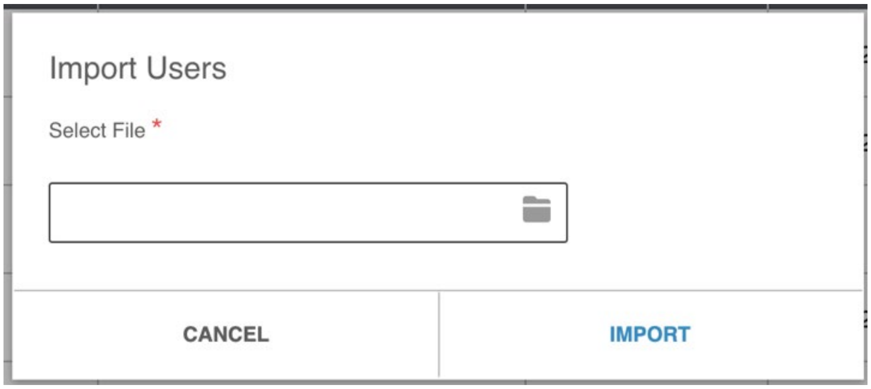
- First Name
- Last Name
- Email Address

4 Click **SAVE**.

Importing users

1 On the left navigation menu, select **Manage > Users**.

2 Click **Import 11.X Users** to display the **Import Users** pop-up.



3 Click the folder icon.

4 Select either an XML or CSV file containing the user information.

5 Verify the users' information and click **IMPORT**.

Disabling Infor Ming.le identities

When the IFS IGS features are enabled, as the IFS administrator, you must disable Infor Ming.le identities at the tenant level.

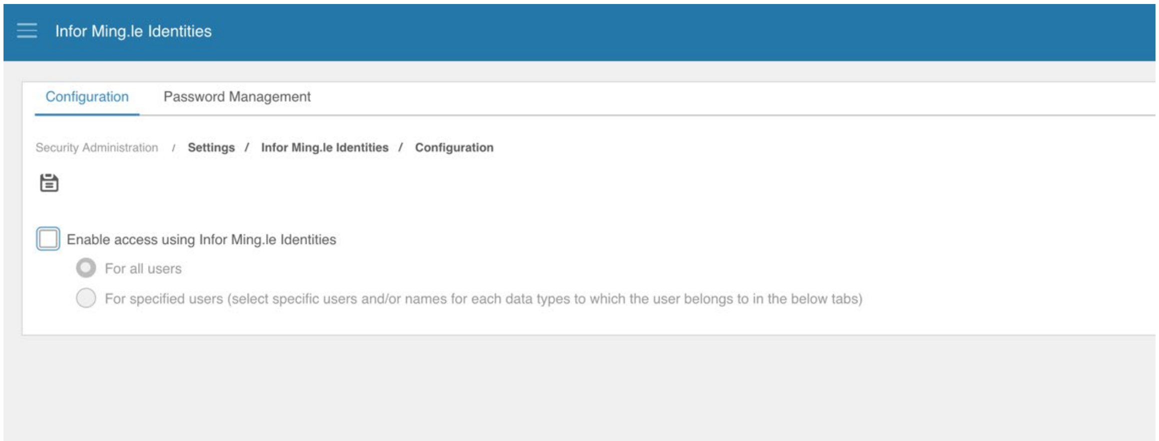
To disable access to the Infor Ming.le application using Infor Ming.le identities, you must disable the settings.

Note: Before you disable Infor Ming.le identities, you must first configure Federated Security.

1. On the left navigation menu, select **Security Administration > Settings > Infor Ming.le Identities**.
2. On the **Configuration** page, confirm that the check box for this setting is cleared:

   Enable access using Infor Ming.le Identities

   This setting controls access to the Infor Ming.le application using Infor Ming.le identities. This setting is enabled by default. Once disabled, users cannot access the Infor Ming.le application using Infor Ming.le identities.



Security Administration / Settings / Infor Ming.le Identities / Configuration

□ Enable access using Infor Ming.le Identities

○ For all users

○ For specified users (select specific users and/or names for each data types to which the user belongs to in the below tabs)

3. Click **SAVE**.

Soft-deleting users

For IGS, IFS must be configured to perform the soft-deletion of users. To soft-delete users:

1. While logged in as a user with a UserAdmin role, click the profile icon in the top right corner of the screen to access the profile panel.
2. Click **User Management** on the profile panel.
3. Click **Soft Deleted Users** under **Manage**.
4. On the **Soft Deleted Users** screen, enter the name of the user to be deleted in the search box on the right and press **Enter**.

5 Click the Soft Deleted Users table and select the check box next to the name of the user to be deleted.

6 Select **Action > Delete**.

Audit

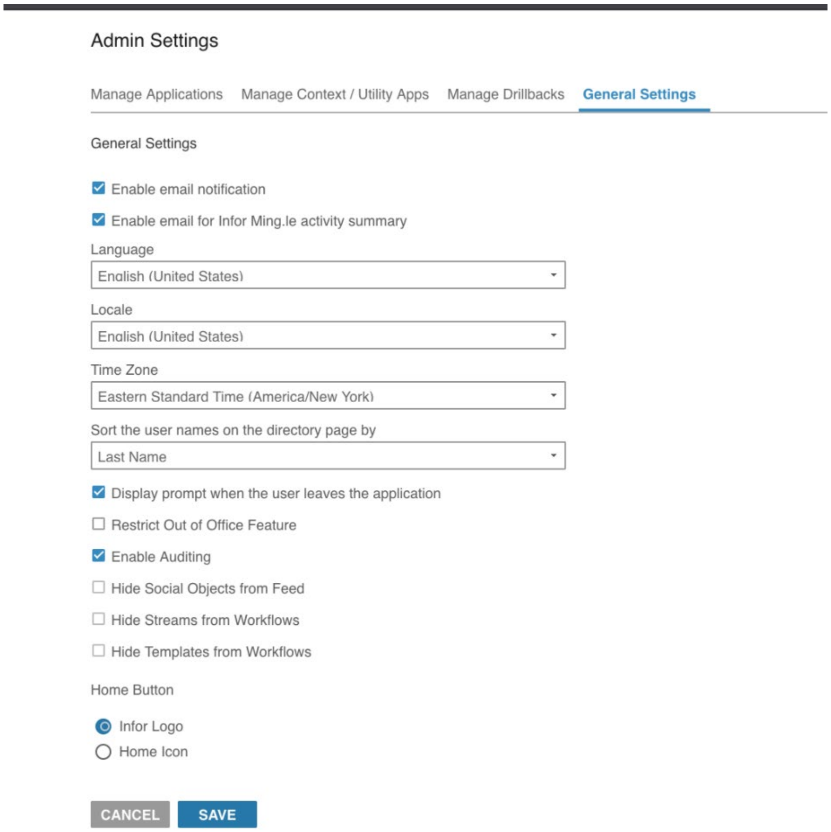
For the tenant to be IGS compliant, the audit setting for all the components should be turned on at the tenant level.

Verifying the audit setting for Infor Ming.le Portal and Collaboration

Confirm that the audit setting for Portal and Collaboration is enabled.

1 Select **User Menu > Admin Settings > General Settings**.

2 Confirm that the check box for the **Enable Auditing** setting is selected.



Admin Settings

General Settings

☑ Enable email notification

☑ Enable email for Infor Ming.le activity summary

Language: English (United States)

Locale: English (United States)

Time Zone: Eastern Standard Time (America/New York)

Sort the user names on the directory page by: Last Name

☑ Display prompt when the user leaves the application

☐ Restrict Out of Office Feature

☑ Enable Auditing

☐ Hide Social Objects from Feed

☐ Hide Streams from Workflows

☐ Hide Templates from Workflows

Home Button

● Infor Logo

○ Home Icon

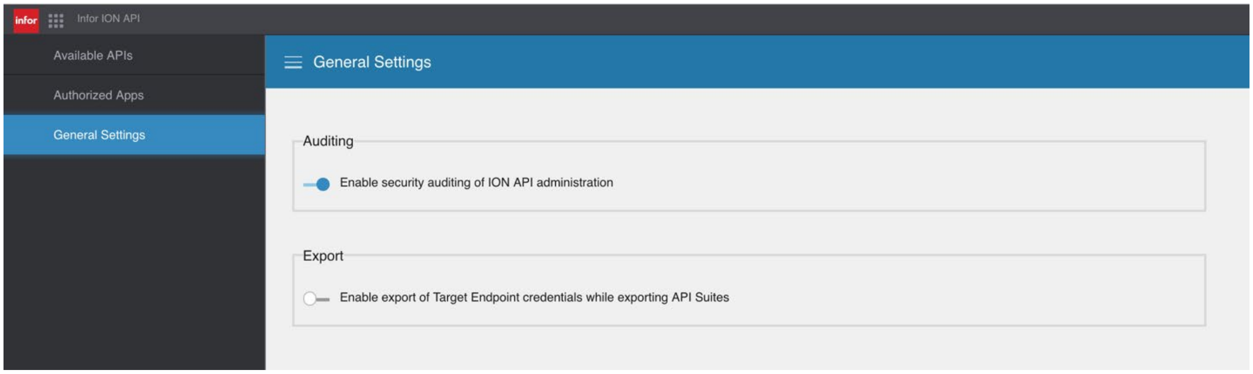
3 Click **SAVE**.

Verifying the audit setting for Infor ION API

Confirm that the audit setting for ION API is enabled.

1 Select **App Switcher Panel > Infor ION API > General Settings**.

2 Confirm that the toggle switch for the **Enable security auditing of ION API administration** setting in the Auditing section is turned on.



Auditing

● Enable security auditing of ION API administration

Export

○ Enable export of Target Endpoint credentials while exporting API Suites

Verifying the audit setting for IFS Audit

Audits related to users and other privileged functions in User Management (IFS) are not enabled by default.

Note: When the **Enable IFS Audit** setting is enabled, the system starts logging events in User Management.

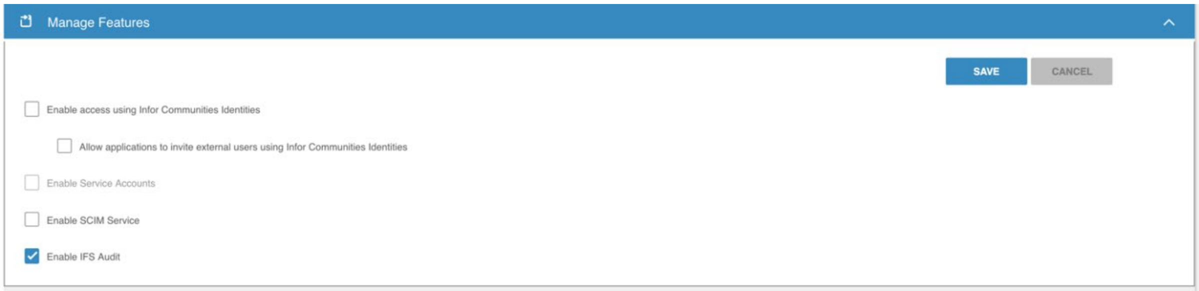
Confirm that the audit setting for IFS is enabled.

1 Select **User Menu > User Management**.

2 On the left navigation page, select **Security Administration > Settings > General Settings**.

3 Expand **Manage Features**.

4 Confirm that the check box for the **Enable IFS Audit** setting is selected.



□ Enable access using Infor Communities Identities

□ Allow applications to invite external users using Infor Communities Identities

□ Enable Service Accounts

□ Enable SCIM Service

☑ Enable IFS Audit

5 Click **SAVE**.

Verifying the Auditing and Monitoring tab is absent

The **Auditing and Monitoring** tab is not available in IGS environments.

Confirm that the **Auditing and Monitoring** menu option is absent.

1 Select **User Menu > User Management**.

2 On the left navigation page, confirm that there is no menu option for Auditing and Monitoring.

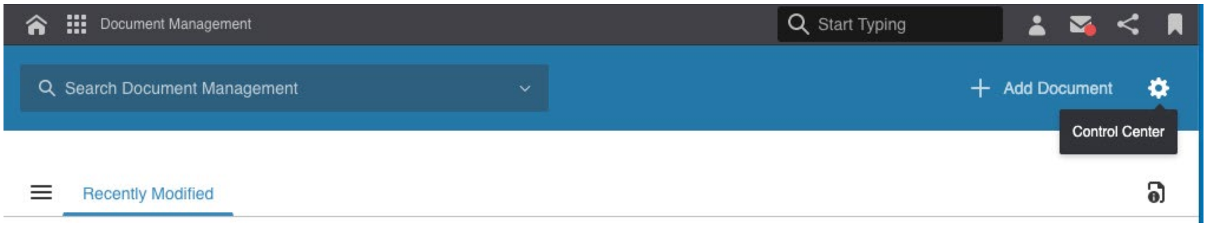
Verifying the audit setting for Infor Document Management (IDM)

The 12.0.43 version of Infor Document Management is being implemented for the current release of Infor OS IGS (Infor Government Solutions).

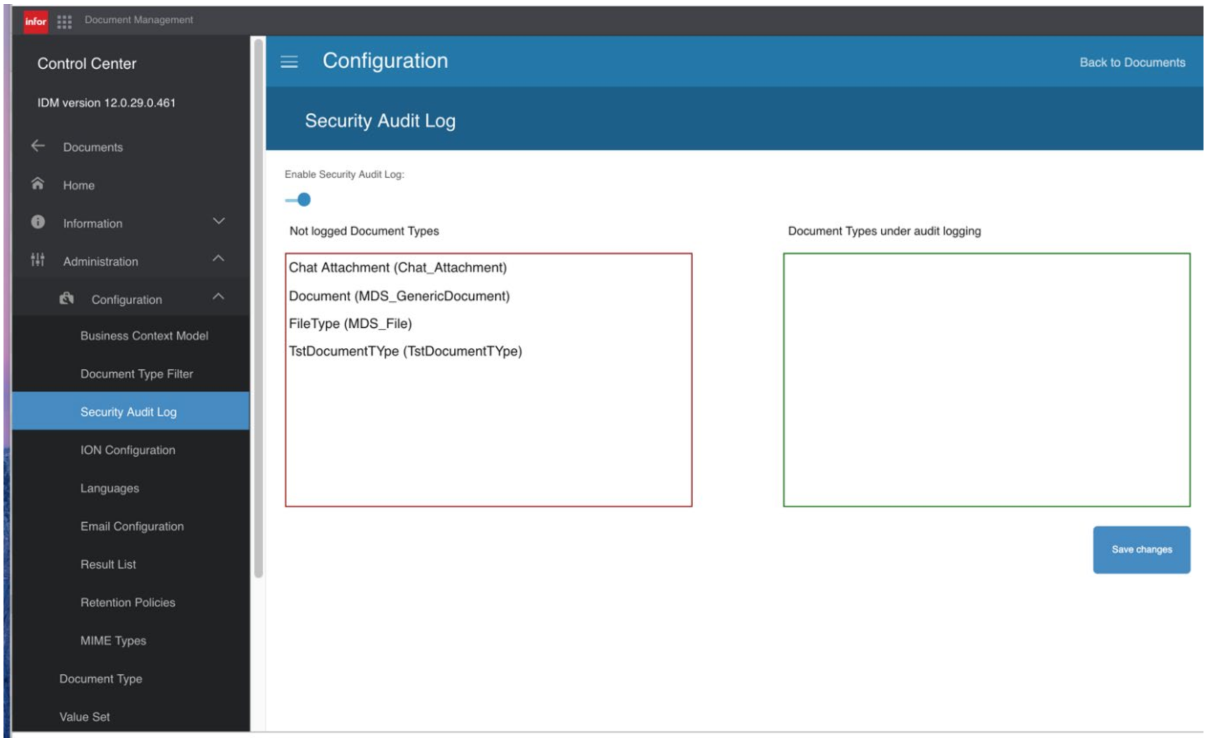
Confirm that the audit setting for IDM is enabled.

1 Select **App Switcher Panel > Document Management**.

2 Click the Control Center icon on the top right.



3 Select **Administration > Configuration > Security Audit Log**.



Enable Security Audit Log:

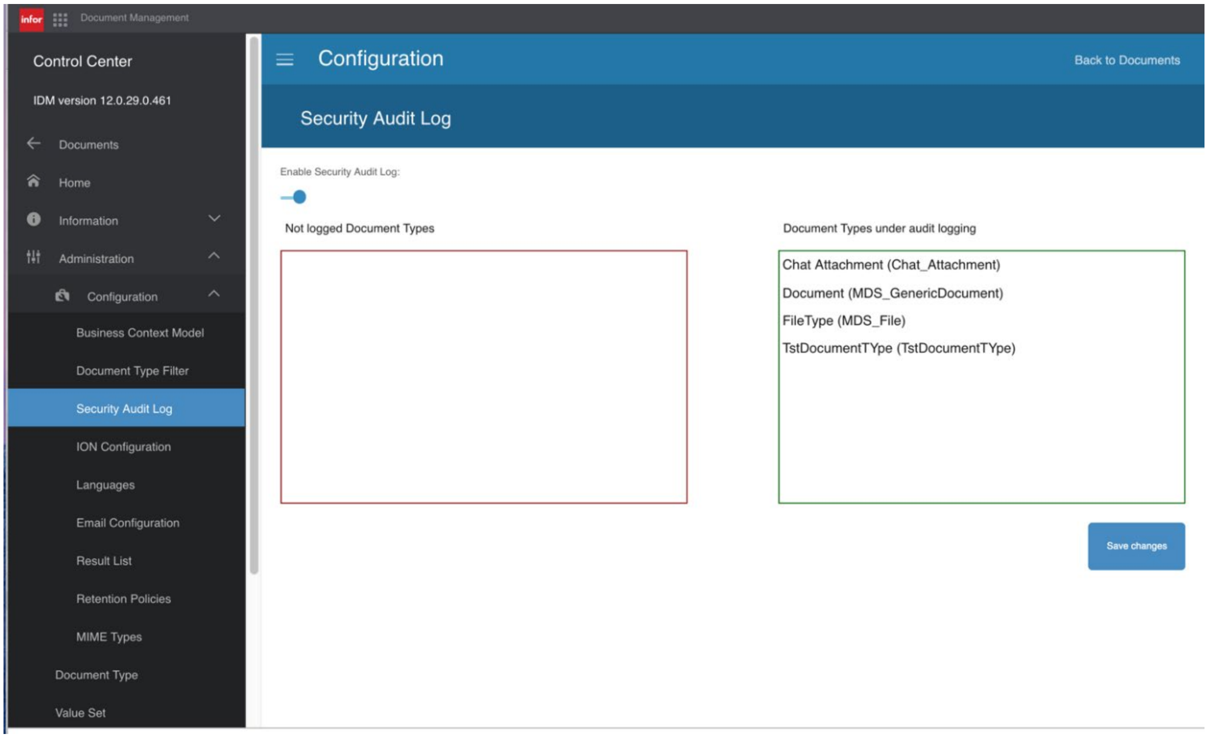
Not logged Document Types

Chat Attachment (Chat_Attachment)
Document (MDS_GenericDocument)
FileType (MDS_File)
TstDocumentTYpe (TstDocumentTYpe)

Document Types under audit logging

4 Confirm that the toggle switch for the **Enable Security Audit Log** setting is turned on.

5 Move all document types from the **Not logged Document Types** section to the **Document Types under audit logging** section.



Security Audit Log

Enable Security Audit Log:

Not logged Document Types

Document Types under audit logging

Chat Attachment (Chat_Attachment)
Document (MDS_GenericDocument)
FileType (MDS_File)
TstDocumentTYpe (TstDocumentTYpe)

6 Click **Save changes**.

Audit setting for Homepages

The audit setting for Homepages is enabled at the infrastructure level; therefore, no additional action is required at the tenant level.

ION Alarms

ION Alarms mobile apps are available, but they are not IGS certified.

Note: This mobile application is available but cannot used in IGS.

ION OneView

An ION OneView Android mobile app is available, but it is not IGS certified.

Note: This mobile application is available but cannot used in IGS.

Infor Document Management

Infor Document Management mobile apps are available, but they are not IGS certified.

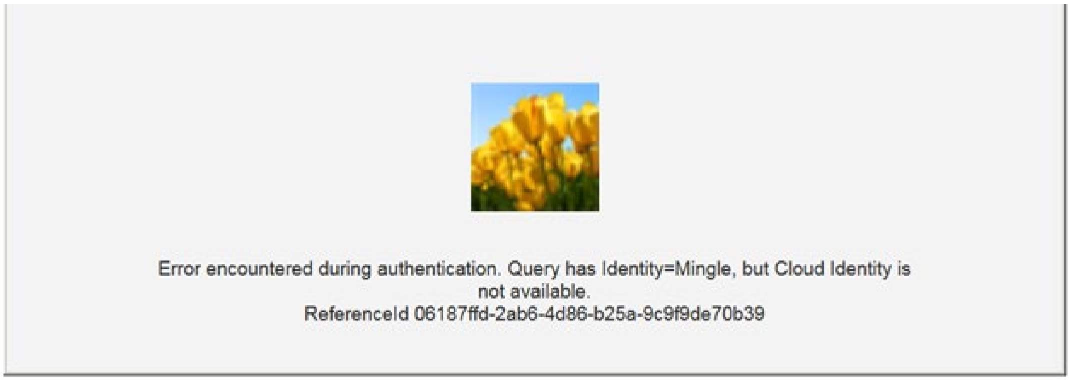
Note: This mobile application is available but cannot used in IGS.

References

When the Infor Ming.le Identities setting is disabled

When the **Infor Ming.le Identities** setting is turned off, the user cannot access the Infor Ming.le application using Infor Ming.le identities. If the user tries to access the Infor Ming.le Identity URL directly, an error results.

For example: URL: https://server/{tenantId}/?Identity=Mingle

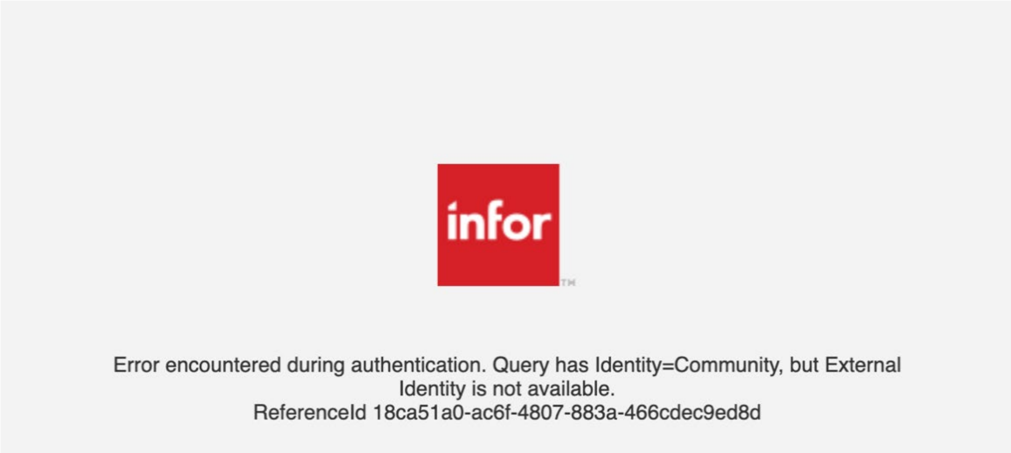


Error encountered during authentication. Query has Identity=Mingle, but Cloud Identity is not available.
ReferenceId 06187ffd-2ab6-4d86-b25a-9c9f9de70b39

When the Infor Communities Identities setting is disabled

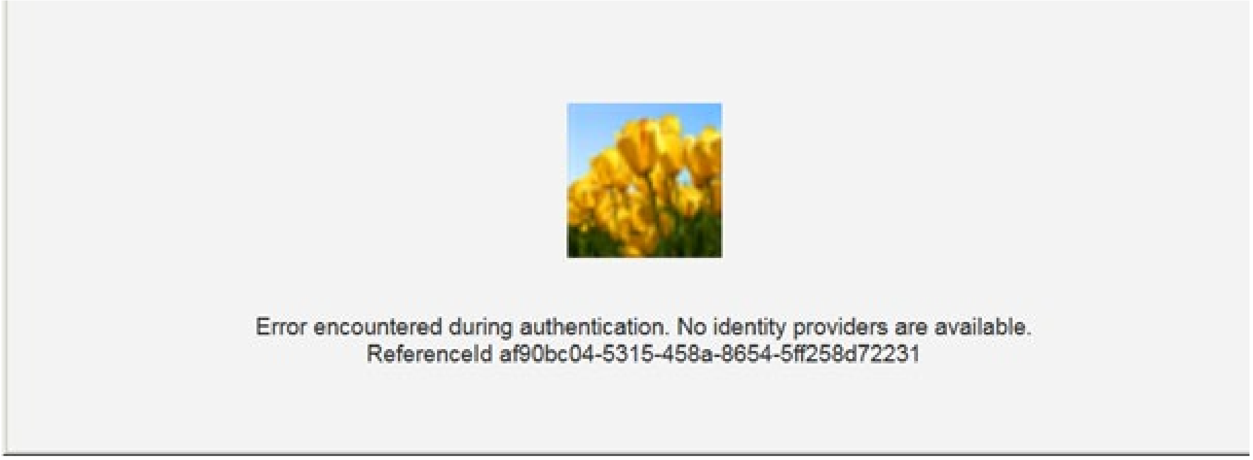
When the **Infor Communities Identities** setting is turned off, the external user cannot access the Infor Ming.le site using Communities Identities. If the user tries to access Infor Communities Identity URL directly, an error results.

For example: URL: https://server/{tenantId}/?Identity=community



Error encountered during authentication. Query has Identity=Community, but External Identity is not available.
ReferenceId 18ca51a0-ac6f-4807-883a-466cdec9ed8d

If no Infor identity provider is available (Federated Identity, Infor Ming.le Identity, or Infor Communities Identity), this error message is displayed:



Error encountered during authentication. No identity providers are available.
ReferenceId af90bc04-5315-458a-8654-5ff258d72231

Different scenarios with Infor identities availability

There are multiple URLs that the user can use to log into Infor Ming.le:

- This URL is the default URL to sign in to Infor Ming.le. This URL enables users to log in with the default authentication mode:

  https:// server/{tenantId}/

- This URL enables an administrator to log in with an Infor Ming.le identity:

  https:// server/{tenantId}/?Identity=Mingle

- This URL enables an administrator to log on with a federated identity:

  https:// server/{tenantId}/?Identity=Federated

- This URL enables external users to log on with an Infor Communities Identity:

  https:// server/{tenantId}/?Identity=community
- This URL enables an administrator to be prompted at the time of login:

  https:// server/{tenantId}/?AuthMode=Prompt

Scenario 1: The federated identity is configured and the Infor Ming.le identity is disabled

These results occur when the user tries to access the Infor Ming.le application with these URLs:

- Default Sign in URL: https://server/{tenantId}/

  The user is directed to the federated login page.
- Infor Ming.le Identity URL: https://server/{tenantId}/?Identity=Mingle

  The user is directed to the federated login page.
- Federated Identity URL: https://server/{tenantId}/?Identity=Federated

  The user is directed to the federated login page.
- Infor Communities Identity URL: https://server/{tenantId}/?Identity=community

  Case 1: When Infor Communities identity is not turned off:

  Displays the Infor Communities Identity login page.

  Case 2: When access using Infor Communities identities is also turned off:

  The user is directed to an error page.
- Prompt URL to select Infor Ming.le, Federated Identity, or Infor Communities Identity: https://server/{tenantId}/?AuthMode=Prompt

  The prompt to sign in using Infor Ming.le identities is not displayed. Other options are displayed, based on configuration. If the **Infor Communities Identities** setting is also disabled, then the user is directed to the federated login page.

Scenario 2: The federated identity is not configured and the Infor Ming.le Identity is disabled

These results occur when the user tries to access the Infor Ming.le application with these URLs:

- Default Sign in URL: https://server/{tenantId}/

  The user is directed to an error page because the federated identity is not configured.
- Infor Ming.le Identity URL: https://server/{tenantId}/?Identity=Mingle

The user is directed to an error page since Infor Ming.le identity is disabled and the federated identity is not configured.

- Federated Identity URL: https://server/{tenantId}/?Identity=Federated

  The user is directed to an error page because federated identity is not configured.

- Infor Communities Identity URL: https://server/{tenantId}/?Identity=community

  Case 1: When Infor Communities identity is not turned off.

  The user is directed to the Infor Communities Identity login page.

  Case 2: When access using Infor Communities identities is also turned off:

  The user is directed to an error page.

- Prompt URL to select Infor Ming.le, Federated Identity, or Infor Communities Identity: https://server/{tenantId}/?AuthMode=Prompt

  The prompt to sign in using Infor Ming.le identities and the federated identity is not displayed. The Infor Communities login page is displayed if access using the Infor Communities identities is enabled. If not, then the user is directed to an error page.

Chapter 2 Enabling Homepages for IGS

The 12.0.42 version of Infor Homepages is being implemented for the current release of Infor OS IGS (Infor Government Solutions).

To enable Infor Homepages for IGS, complete the tasks in this chapter.

Enabling dynamic pages

Dynamic pages are available in IGS. To add these pages to the user interface:

1. Navigate to Homepages.
2. Click the page menu icon (…) in the page title bar.
3. Select **Advanced > Administration > Features**.
4. Set the value of the **Dynamic Pages** feature to `true`.
5. Click **Save**.

Hiding tenant widgets

Tenant widgets are not available in IGS. To remove this page from the user interface:

1. Navigate to Homepages.
2. Click the page menu icon (…) in the page title bar.
3. Select **Advanced > Administration > Features**.
4. Set the value of the **Tenant Widgets** feature to `false`.
5. Click **Save**.

Confirming early access widgets are disabled

Early access widgets are not available in IGS.

To confirm that the early access widgets are disabled:

1. Navigate to Homepages.
2. Click the page menu icon (…) in the page title bar.
3. Select **Advanced > Administration > Widgets > Early Access Widgets**.
4. Confirm that the datagrid is empty. If not, select each widget individually, and click **Delete** from the Actions bar.

Enabling viewing and publishing pages to Infor Go

Infor Go is available in IGS. Homepages and Infor Go enablement is required. To enable viewing and publishing pages for Infor Go:

1. Navigate to Homepages.
2. Click the page menu icon (…) in the page title bar.
3. Select **Advanced > Administration > Settings**.
4. Set the value of **View and Publish Pages for Infor** Go to `true`.
5. Click **Save**.