



**Advanced
Cloud
Security**



F O Q U S

Advanced Cloud Security is the best way to limit what data your users have access to in Microsoft Dynamics 365 Business Central.

You have control over fields and most controls on every single page in the system and you can apply dynamic filters to all tables throughout the system.

Feature Highlights

- **Field Control**
Specify if a field should be visible or not, or enabled or not.
- **Control Control**
Specify if a control (non-field) on a page should be visible or not.
- **Action Control**
Specify if an action (in the action bar) should be enabled or not.
- **Data Filter**
Apply a dynamic filter whenever a specific table is accessed.
The above controls can be bundled together in a **Security Feature**. Security Features can then be assigned to:
 - Users
 - User Groups
 - Permission SetsWhen a user logs on to Business Central, ACS will cache all the setting that applies to that user from all three places.

Advanced Cloud Security supports 99%(*) of the standard application and other 3rd party extensions.

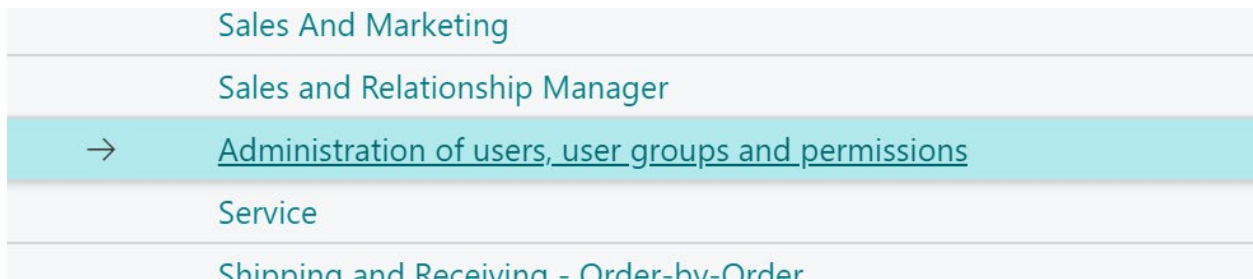
(*) A few pages in Business Central do not allow to be extended. This is typically technical configuration and setup pages and API pages.

Visit www.foqus.ca for more information.

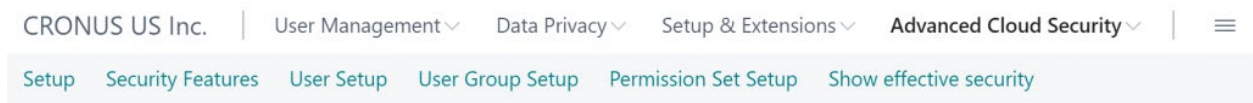
Setup and Configuration

Start by selecting **Advanced Cloud Security** from **AppSource** and install it onto your environment.

Next, change your plan to the **Administration of users, user groups and permissions** role center to access the setup of ACS.



Now you have access to setup ACS:



Click **Setup** to start the configuration of ACS.

The first time you access setup, you'll be redirected to the App registration.

ABOUT ADVANCED CLOUD SECURITY



**Advanced
Cloud
Security**



FOQUS

[Click here to register and to sign up for ACS](#)

Please register this extension to activate the functionality. You'll get a registration code to unlock this extension.

Enter Registration Code

Registered To




The E Foqus App Registration Dialog

Click on **Click here to register and to sign up for ACS** and complete the process at www.foqus.ca. Completing this process will give you a registration code that you can enter into the dialogue to register the app.

Now you can see the setup page:

Setup

[Actions](#) [Navigate](#)

 Create Extension  See problem fields Transfer Setup ▾ 

ACS Integration Wrapper Extension

| | | | |
|-------------------------|-----------|-------------------------|----------------------------------|
| Extension Bloud Meth... | Optimized | End Object Range | 69999 |
| Extension Version No. | 1.0.0.1 | Bad pages (Must be e... | 356,683,896,1754,1800,5555,55... |
| Start Object Range | 60000 | | |

The secret sauce in ACS is that it creates a new extension to your Business Central. The new extension is the connection between ACS and all the pages and data.

There are two ways to generate the Extension **Complete** or **Optimized**.

Complete will generate an extension that covers every single field and action on every page.

Optimized will generate an extension that **only** covers the pages where you have a security setup defined.

So, if your purpose of using ACS is limited to a set of specific areas, then **Optimized** is the right method for you, but if you have security set up throughout the system choose **Complete**. You can switch between the methods without any issues.

The important part to understand, is that if you install **NEW** extensions, from AppSource or by your local developer, the extension has to be re-generated to cover the functionality in the new app.

The **Object Range** is where the new extension will be installed. ACS will search automatically to find an appropriate free range in the 50.000-99.999 range. You can control this yourself. The important part is the ACS will generate 1000s of pageextensions if you have 1000s of pages.

Bad Pages are pages that do not allow to be extended. This is typically technical setup pages. The list provided is pages in standard Business Central that cannot be extended. Right now, there's no way for ACS to figure out if a page can be extended or not. So if you install an App that has a page that breaks the extension, add the page number to this list.

This is the list for BC versions 15 and 16. We'll keep this list updated when we discover new "bad pages":

356,683,896,1754,1800,5555,5557,7200,7201,7202,7207,9169,9190,9511,9551,9620,9621,9622,9630,9631,9632,9634,9813,9814,9992,20043,20044,20045,20046,20047,130407

Problem Fields are fields where visibility and editability are controlled by other apps and ACS cannot override that behaviour. You'll have to generate the extension first to see the problem fields.

PROBLEM FIELDS | WORK DATE: 4/6/2020

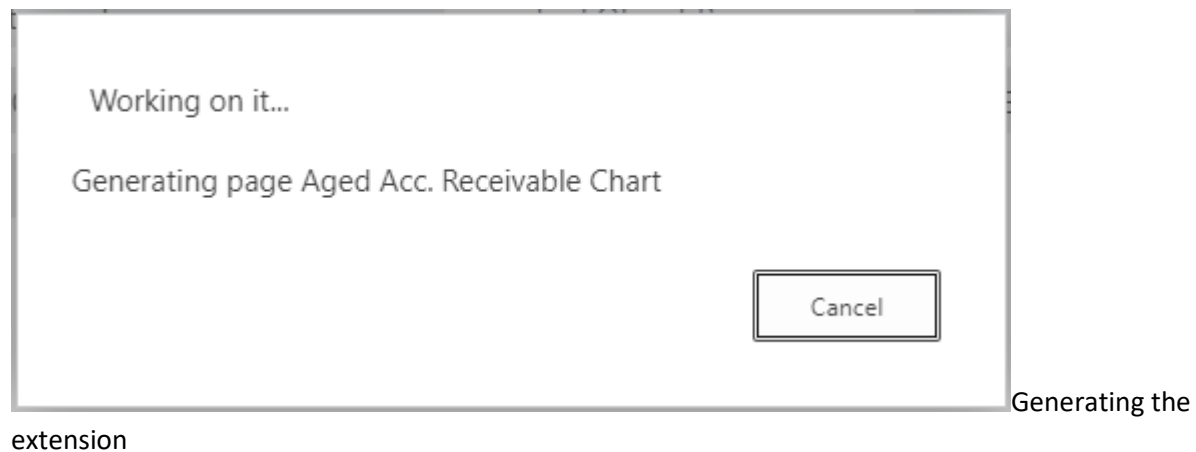
Search Open in Excel

| Table Name | Field Name | Visible Reason | Enabled Reason |
|------------|------------|-------------------|----------------|
| Customer | No. | p21NoFieldVisible | true |


In this case, we can see that visibility on **No.** on the customer card is controlled by something else (**p21NoFieldVisible** is an internal programming reference).

Generate the Extension

Click **Create Extension** to generate the extension, depending on the creation method and amount of security set up, this might take a while:



When you have generated the extension, it should be installed in **Extension Management** and be ready to go:

| Description | Name ↑ | Version |
|------------------|---|---------|
| Installed |  ACS Integration Wrapper | v. 1.0 |
| Installed | Advanced Cloud Security | v. 1.0 |

It's called the **ACS Integration Wrapper**

The extension is also downloaded as an app file, so if you're generating the app in a sandbox environment, it can be installed on production by uploading it in **Extension Management**.

If you're testing this on a docker container the PowerShell script to install the extension is:

```
Publish-BCContainerApp -containerName BCcontainer -appFile 'c:\users\erik\downloads\ACS Integration Wrapper_E Foqus Canada Inc._1.0.0.2.app' -install -sync -skipVerification -scope Tenant
```

Security Features

In ACS all security configuration is bundled in **Security Features**. Security Features are then assigned to **User**, **User Groups** or **Permission Sets**.

Security Features can be prioritized in case you have overlapping features. The highest priority Security Feature wins.

A Security Feature can hold four different types of configuration:

- **Field Access** – Specify the rules for database fields. This is can done on four different levels: (*)
 - For all fields on the table (by not specifying a field)
 - For all fields no the table on a specific page
 - For all places where a specific field is used
 - For a specific field, on a specific page*(*) Field Access can be combined so you can turn off all fields and turn on specific ones you need.*
- **Page Controls** – Specify the rules for controls (fields) on a specific page. This is usually for controls that are not bound to database fields.
- **Action Access** – Specify the rules for actions in the action bar.
- **Data Access Filters** – Apply filters on data. The filters can be based on **User Filters** so filters can be individually per user.



Notifications: 2 *Table Customer Posting Group is not included in t...* | *Table Customer is not included in the curr...* ▼

🔍 Search
➕ New
✎ Edit List
🗑 Delete
📄 Open in Excel
🔍 Filter
☰ Menu

| ID ↑ | Description | Priority |
|-----------|-----------------|----------|
| → ADDRESS | Address Control | 0 |

Field Access | Manage

| Table Name | Field Name | Page Name | Setting |
|------------|------------|-----------|---------|
| → Customer | Address | - | Disable |
| Customer | Address 2 | - | Disable |

Page Controls | Manage

| Page Name | Control ↑ | Setting |
|-----------------|-----------|---------|
| → Customer Card | ShowMap | Hide |

Action Access | Manage

| Page Name | Action ↑ | Setting |
|-----------------|----------|---------|
| → Customer Card | Action76 | Disable |

Data Access Filters | Manage

| Table Name | Field Name | Filter Value | Allow User Filters |
|--------------------------|------------------------|--------------|-------------------------------------|
| Customer | Customer Posting Group | \$UF_31\$ | <input checked="" type="checkbox"/> |
| → Customer Posting Group | Code | \$UF_31\$ | <input checked="" type="checkbox"/> |

The above **Security Feature** example does the following:

- Disable the **Address** and **Address 2** fields on Customers
- Hide the **Map** control on the customer card
- Disables the **Statistics** action on the customer card (called Action76)
- Apply a dynamic filter on **Customer Posting Group** on both the Customer and Customer Posting Group tables.

Notice the notification at the top:

| | |
|---|---|
| Notifications: 2 | ^ |
| × Table Customer Posting Group is not included in the current security extension, please regenerate | v |
| × Table Customer is not included in the current security extension, please regenerate | v |

Warning about security settings not covered in the current generated extension

Here we're using the **Optimized** method but the current generated extension does not include Customer and Customer Posting Tables.

The **Action76** in the above example is the name of the action we want to disable. Some control and actions have very strange names behind the scenes, but when you perform the lookup in ACS, we'll find the caption that hopefully will help you find the right control:

| | |
|------------------|---------------------|
| ShowLog | Synchronization Log |
| Ledger E&ntries | Ledger E&ntries |
| <u>Action76</u> | ⋮ Statistics |
| S&ales | S&ales |
| Entry Statistics | Entry Statistics |

Some controls can be very hard to locate since not all control does have a caption. In that case, you might need to get in contact with a technical Business Central resource or do some trial-and-error testing yourself.

Apply Security to Users

When you have defined a **Security Feature**, you must assign it to your users for it to have any effect.






A user can get security features in three different ways:

- Assigned directly to the user
- Assigned to a user group
- Assigned to a permission set

USER SETUP | WORK DATE: 4/6/2020

✓ SAVED   

 Search  Edit List  Open in Excel

| | User Name | | Full Name | License Type |
|---|-----------|---|------------------------------|---------------|
| → | EH | : | | Full User |
| | MSOLSYNC | | Microsoft Online Sync Daemon | External User |


Security Features | Manage

| | Feature ID ↑ | | Feature Description |
|---|--------------|---|---------------------|
| → | ADDRESS | : | Address Control |

The user EH has the ADDRESS security features assigned.

You can use the **Show effective security** function to show what specific security setting a user will get from the current setup:

CRONUS Canada, Inc. | < Setup & Extensions ▾ **Advanced Cloud Security** ▾ > | ☰

Setup User Setup Permission Set Setup
 Security Features User Group Setup Show effective security 

Show effective security: All ▾ | 🔍 Search + New Manage ▾ 📄 Open in Excel 🗑️ ☰ 📌

Select user to see effective security settings

User EH ⋮

| What | Type | Setting |
|---------------------------------|----------|----------|
| Customer.Address | Field | Disable |
| Customer.Address 2 | Field | Disable |
| Customer Card.ShowMap | Control | Hide |
| Customer Card.Action76 | Action | Disable |
| Customer Posting Group.Code | Filter | DOMESTIC |
| Customer.Customer Posting Group | ⋮ Filter | DOMESTIC |

User Filters

User filters is a way to apply a different filter on the same field depending on the user:

USER SECURITY FILTERS | WORK DATE: 4/6/2020 ✓ SAVED 📌 📄 ↗

🔍 Search + New 📄 Edit List 🗑️ Delete ⚙️ Filter Codes 📄 Open in Excel 🗑️ ☰

| User Name | Purchase Resp. Ctr. Filter | Service Resp. Ctr. Filter | Currency Code | Customer Posting Group | Vendor Posting Group | Invento Posting |
|-----------|----------------------------|---------------------------|---------------|------------------------|----------------------|-----------------|
| → EH | ⋮ | | | DOMESTIC | | |

User EH is assigned to Customer Posting Group DOMESTIC

The user filters are available as **Filter Codes** that can be used in filters:

🔍 Search + New 🗑 Edit List 🗑 Delete 📄 Open in Excel 🔍 ☰

| Code ↑ | Description | Type | Builtin Reference No. |
|---------|----------------------------|---------|-----------------------|
| → UF_11 | Customer No. | Builtin | 11 |
| UF_12 | Vendor No. | Builtin | 12 |
| UF_13 | Item No. | Builtin | 13 |
| UF_14 | G/L Account No. | Builtin | 14 |
| UF_15 | Resource No. | Builtin | 15 |
| UF_16 | Job No. | Builtin | 16 |
| UF_17 | Employee No. | Builtin | 17 |
| UF_18 | FA No. | Builtin | 18 |
| UF_21 | Salespers./Purch. Code | Builtin | 21 |
| UF_22 | Country/Region Code | Builtin | 22 |
| UF_23 | Location Code | Builtin | 23 |
| UF_24 | Global Dimension 1 Code | Builtin | 24 |
| UF_25 | Global Dimension 2 Code | Builtin | 25 |
| UF_26 | Sales Resp. Ctr. Filter | Builtin | 26 |
| UF_27 | Purchase Resp. Ctr. Filter | Builtin | 27 |
| UF_28 | Service Resp. Ctr. Filter | Builtin | 28 |
| UF_29 | Currency Code | Builtin | 29 |
| UF_31 | Customer Posting Group | Builtin | 31 |
| UF_32 | Vendor Posting Group | Builtin | 32 |
| UF_33 | Inventory Posting Group | Builtin | 33 |

Here UF_31 is used on a **Security Feature**:

| Data Access Filters | | Manage | | Allow User Filters |
|--------------------------|------------------------|--------------|--|-------------------------------------|
| Table Name | Field Name | Filter Value | | |
| → Customer Posting Group | Code | \$UF_31\$ | | <input checked="" type="checkbox"/> |
| Customer | Customer Posting Group | \$UF_31\$ " | | <input checked="" type="checkbox"/> |

Filter Codes can be **Builtin** or **Event Supplied**. If you want to create your own filter code, you can create that as an extension and subscribe to a specific event from ACS.