

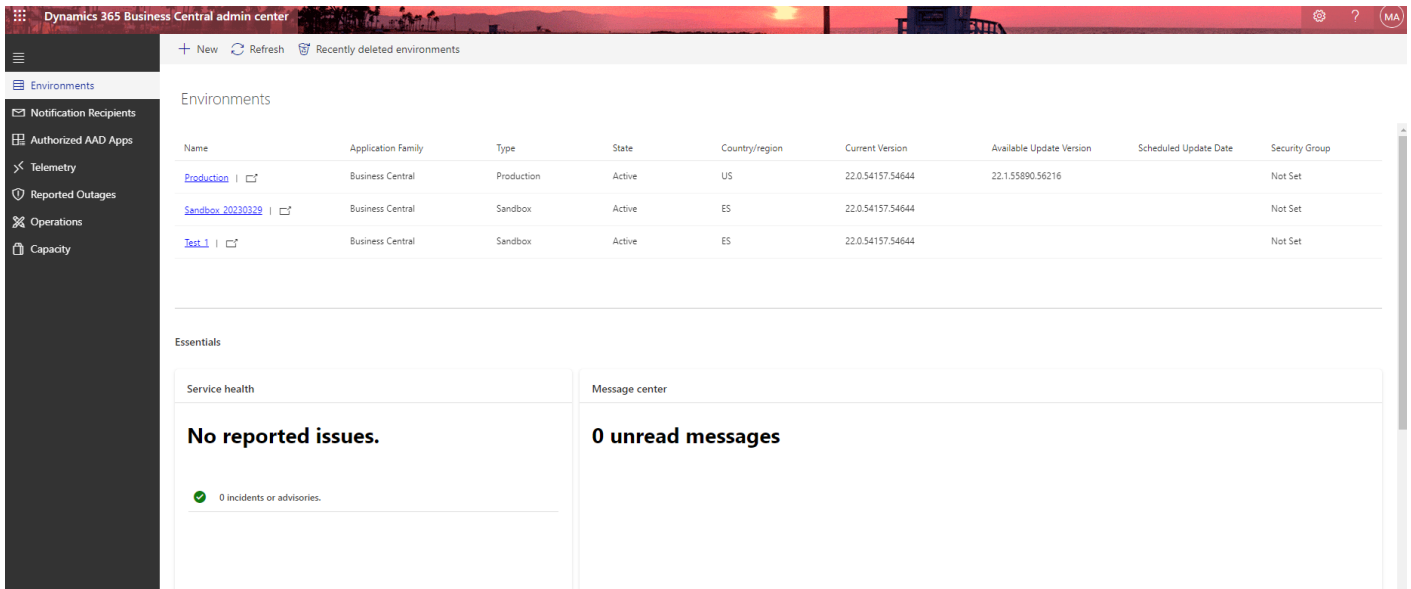
Restringir el uso de un Entorno mediante un Grupo de Seguridad

Artículo original (EN) - Documentación Oficial de Microsoft <https://learn.microsoft.com/es-es/dynamics365/business-central/ui-security-groups>

Es muy importante la selección de los usuarios administradores que deberán pertenecer al grupo para que una vez en uso no quede bloqueado el acceso a los entornos de Business Central.

Aconsejamos la realización de pruebas en entornos Sandbox como paso previo cualquier acción con estos grupos de seguridad.

Para agregar un grupo de seguridad en Business Central, deberemos entrar desde nuestra cuenta al modo administrador y acceder a la página del entorno deseado.



The screenshot shows the Dynamics 365 Business Central admin center interface. The left sidebar contains navigation options: Environments, Notification Recipients, Authorized AAD Apps, Telemetry, Reported Outages, Operations, and Capacity. The main content area displays a table of Environments with columns: Name, Application Family, Type, State, Country/region, Current Version, Available Update Version, Scheduled Update Date, and Security Group. Below the table is the Essentials section, which includes Service health (No reported issues) and Message center (0 unread messages).

Name	Application Family	Type	State	Country/region	Current Version	Available Update Version	Scheduled Update Date	Security Group
Production	Business Central	Production	Active	US	22.0.54157.54644	22.1.55890.56216		Not Set
Sandbox_20230329	Business Central	Sandbox	Active	ES	22.0.54157.54644			Not Set
Test_1	Business Central	Sandbox	Active	ES	22.0.54157.54644			Not Set

Essentials

Service health

No reported issues.

0 Incidents or advisories.

Message center

0 unread messages

Environments

Notification Recipients

Authorized AAD Apps

Telemetry

Reported Outages

Operations

Capacity

An update to version 22.1.55890.56216 is available. Updates will begin on 5/6/2023. You may schedule a date for the update on the Update action list. Go to [Business Central Updates](#) for more information.

Environments > Sandbox_20230329

Details

Active

Name	Application Family	Country/region	Azure Region
Sandbox_20230329	Business Central	ES	North Europe
Type	Application Insights Connection String	Security Group	Access with Microsoft 365 Licenses
Sandbox	Not Set (Define)	Not Set (Define)	Off (Modify)
URL			
https://businesscentral.dynamics.com/62f692fd-0e81-4a40-9f01-0bd63eefbaa8/Sandbox_20230329			

Version Management

Application Version	Platform Version	Available Update Version	Update Scheduling Available
22.0.54157.54644	22.0	22.1.55890.56216	Yes
Update will start on or after	Update Window (UTC+02:00)	Update Rollout State	
05 jun 2023 (Modify)	20:00 - 06:00 (Modify)	Active	

Una vez dentro, en la sección de "Detalles" utilizaremos la opción de "Grupo de seguridad"

Details

Active

Name	Application Family	Country/region	Azure Region
Sandbox_20230329	Business Central	ES	North Europe
Type	Application Insights Connection String	Security Group	Access with Microsoft 365 Licenses
Sandbox	Not Set (Define)	Not Set (Define)	Off (Modify)
URL			
https://businesscentral.dynamics.com/62f692fd-0e81-4a40-9f01-0bd63eefbaa8/Sandbox_20230329			

Por defecto el acceso a cualquier entorno de Business Central esta abierto a todos los usuarios licenciados siempre que no se haya definido un "Grupo de Seguridad" concreto.

Al seleccionar la acción de Definir aparecerá un menú desplegable en la parte izquierda con los grupos definidos en la administración de grupos en Microsoft 365. Una vez seleccionado el grupo de seguridad será necesario reiniciar el entorno para que el cambio tenga efecto.



Edit Security Group

Sandbox_20230329

Restrict environment access to people in this security group. Otherwise, any licensed user can access. Users with administrator role can access all environments, regardless if they are added to the group or not. [Learn more](#)

Current security group:

No group is selected

 Search

SecurityGroup	Id
Ejemplo	1c24a478-44a7-4fca-8b30...
Test1	1bb7484f-964d-44d3-b5a...

Save

Cancel