Security Concepts

Dynamics Human Resources

Microsoft

Today's topics

1

Security Principles

- Imp Standard Roles
- Comparison

2

Implementation Guidelines

- Best Practices
- Role based demo

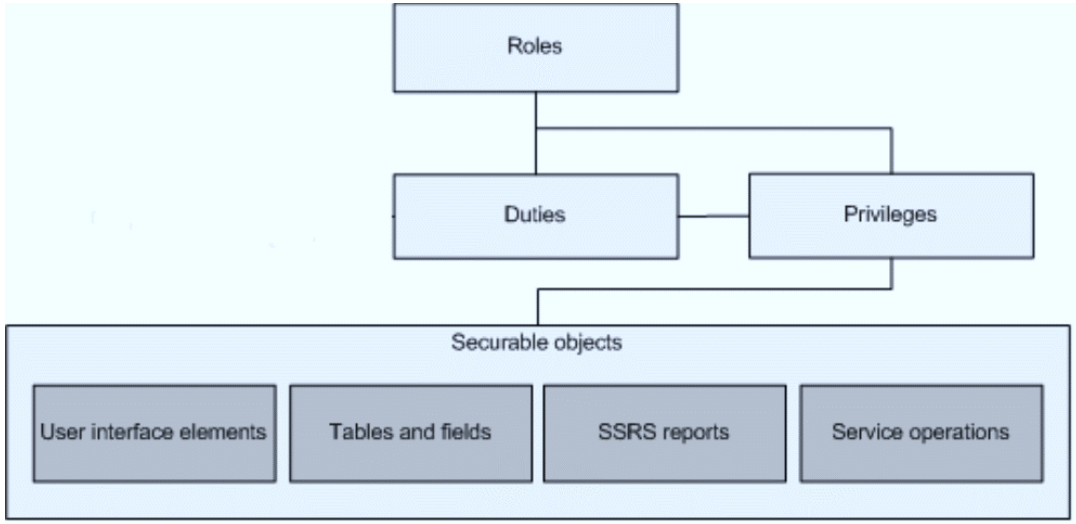
3

CDS Security

- How it interfaces with Talent Security
- PowerApps/Flow Security

Security Principles

- Role based security model using standard Roles/Duties/Privileges/…
- Select XDS policies are in place for Worker, Compensation, Contacts…
- LE security based on roles defined



Talent – Important Roles

	Human Resource Assistant	Human Resource Manager
	❑ Documents and administers human resource events ❑ Responds to human resource inquiries ❑ This role is the "super user" of HR and has the rights to view and update Employee information ❑ Ability to set up most areas of HR ❑ **HR Assistant does not have access to the setup and processing of Compensation and Benefits.**	❑ Periodically reviews human resource process performance and enables the human resource process ❑ This role has view rights into workers and processes ❑ The HR manager roles has additional viewing that may not be available via HR assistant.

We would recommend assigning in both the HR Manager and Assistant roles if Users needs full access to HR

Talent – Important Roles

	Payroll Administrator	Payroll Manager
	❑ Documents payroll events, responds to payroll inquiries and records the financial consequences of payroll events ❑ This role is like the HR Assistants role within the Payroll areas ❑ The PR admin can set up employee data that will be used in integrating to Payroll systems (Benefits Setup) ❑ This role allows you to maintain data across Tax regions, Positions, Calendars, and Compliance	❑ Authorizes activity in the payroll process ❑ The PR Manager role is like the HR Manager ❑ This is an approval roles and can view information across HR and PR areas as they relate to Payroll ❑ View capabilities includes Benefits and Compensation and all Payroll related worker information.

Talent – Important Roles

	Compensation/ Benefits Manager	Manager
	❑ This role Documents compensation and benefit events ❑ Responds to compensation and benefit inquiries and records the financial consequences of compensation and benefit events ❑ This role can see and update compensation and compensation processing ❑ By default, this role can see all compensation plans, both Fixed and Variable and adjust, either for individuals or in mass through compensation processing.	❑ The manager role is a people manager in the organization that view employee information for his/her organization (directs and extended reports) in MSS ❑ This role is also allowed to Update and request changes based on configuration options that have been enabled by the HR Assistant role ❑ This includes work on behalf options as well as personnel actions for specific Hire, Transfer and Termination Actions.

Best Practices

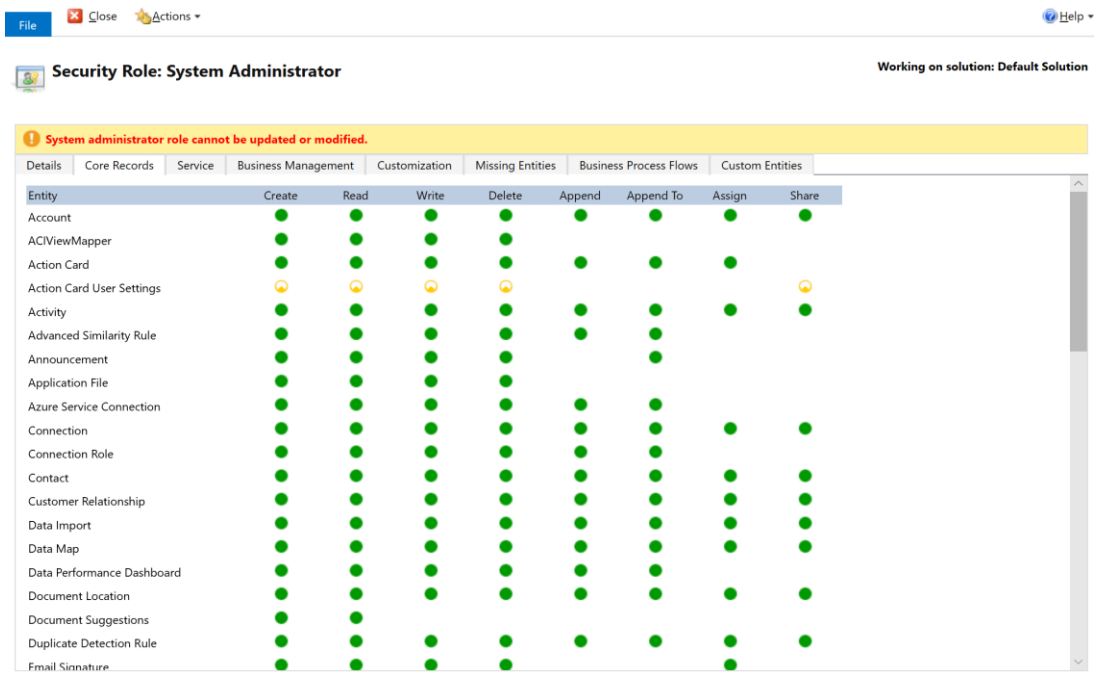
- Change Roles by duplicating role
- Change duties by duplicating to custom duties
- Although Privileges can be added directly, it is better to add it though duties
- Identify and resolve conflicts in segregation of duties

Demo

Change Human Resource Manger role to prevent accessing Shared Parameters configuration

CDS Security

- Common Data Service uses role-based security to group together a collection of privileges.



CDS Security

Common Data Service uses role-based security to group together a collection of privileges.

Predefined Security Roles:

System Administrator: Has full permission to customize or administer the environment, including creating, modifying, and assigning security roles. Can view all data in the environment.

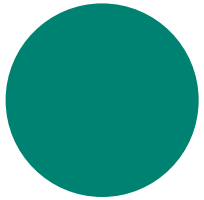
System Customizer: Has full permission to customize the environment. However, can only view records for environment entities that they create

Environment Maker: Can create new resources associated with an environment including apps, connections, custom APIs, gateways, and flows using Microsoft Power Automate. However, does not have any privileges to access data within an environment

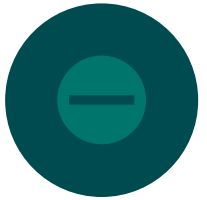
Common Data Service User: Can run an app within the environment and perform common tasks for the records that they own. Note: this only applies to non-custom entities

Delegate: Allows code to run as another user or impersonate. Typically used with another security role to allow access to records

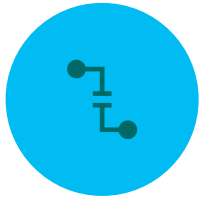
PowerApps/Flow



Users are authenticated by Azure Active Directory (Azure AD).

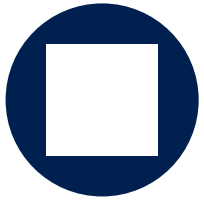


Licensing is the first control-gate to allowing access to PowerApps components.



Ability to create applications and flows is controlled by security roles in the context of environments.

A user's ability to see and use apps is controlled by sharing the application with the user.



Sharing of canvas apps is done directly with the user or Azure AD group. Sharing of model-drive apps is done via Common Data Service security roles.

Flows and Canvas apps use connectors, the specific connections credentials and associated service entitlements determine permissions when apps use the connectors.

Demo

Scenario 1: Sharing Powerapps
Scenario 2: Manually Triggered Flow and Data Extraction
Scenario 3: Calling Flow from Powerapps with out share and edit authorization