Fine-grained access control

IBM® Maximo® Worker Insights features a multi-layered access control system that follows the principle of least privilege access. This access control system allows for fine-grained access control, which uses flexible access control policies.

Terminology

Fine-grained access control in IBM Maximo Worker Insights uses the following entities:

- **Contexts** can be either an organization or a location. Organizations and locations are hierarchical. The following organizations and locations are examples of contexts:
    - ORG.IBM is the root (or the parent) organization, while ORG.IBM.WIOT is a child organization, and ORG.IBM.WIOT.WHI is a grandchild organization.
    - LOC.IBM is root (or the parent) location, while LOC.IBM.IRL is a child location, and LOC.IBM.DEU is another child location. LOC.IBM.IRL and LOC.IBM.DEU are peers (or siblings).
- **Subjects** are users or user groups or a program or an API call that operates on behalf of a user.
- **Objects** are items that subjects interact with, such as devices or hazards.
- **Roles** are assigned to subjects. IBM Maximo Worker Insights has the following default roles:
    - Administrator: This role administers and operates the service at the tenant level, across all organizations.
    - Operator: This role administers and operates the service within an organization.
    - Supervisor: This role supervises workers within an organization.
    - Workers: This role is a worker within an organization.

  Subjects can have multiple roles. Contexts are always mapped to non-administrator roles. The following examples are roles for workers and supervisors in the context of the ORG.IBM.WIOT organization:
    - worker:ORG.IBM.WIOT
    - supervisor:ORG.IBM.WIOT
- **Attributes** are assigned to objects and subjects.
    - Object attributes are limited to contexts. The organization context is inherited from the subject who created the object.
    - Subject attributes combine roles and contexts to form context-based role attributes. An example of a context-based role attribute is `worker:ORG.IBM.WIOT`. Contexts are assigned to subjects by using the dashboard or the API.
- **Access control policies** define which context-based role attributes a subject needs to operate on an object.

Access control policies

Access control policies are pivotal to fine-grained access control. Access control policies serve as the decision point that assesses all of the previously listed entities against each other. In simple terms, access control policies define which context-based role attributes a *subject* needs to operate on an *object*.

When IBM Maximo Worker Insights is provisioned, it comes with many access control policies that address known use-

case scenarios. These access control policies can be customized for specific needs. Tenant administrators can customize existing access control policies and create new access control policies.

Example of an access control policy

The following example is based on an access control policy for a hazard that is named `ha_01`.

Access control policy definition

The following table shows the access control policy for hazard `ha_01`:

Operation type	Required context-based role attributes
Read	• supervisor:ORG.IBM.WIOT • worker:ORG.IBM.WIOT • supervisor:LOC.ISR.HAIFA • worker:LOC.ISR.HAIFA
Create	• supervisor:ORG.IBM • supervisor:LOC.ISR
Delete	• supervisor:ORG.IBM • supervisor:LOC.ISR

Access attempts on hazard 'ha_01' that are successful

The access control policy for hazard `ha_01` determines which operations a subject can perform:

- A subject can *read* the hazard, if they have one of the following context-based role attributes:
  - A supervisor in the organization ORG.IBM.WIOT or the parent organization ORG.IBM.
  - A worker in the organization ORG.IBM.WIOT or the parent organization ORG.IBM.
  - A supervisor in the location LOC.ISR.HAIFA or the parent location LOC.ISR.
  - A worker in the location LOC.ISR.HAIFA or the parent location LOC.ISR.
- A subject can *create* or *delete* the hazard only if they have one of the following context-based role attributes:
  - A supervisor in the organization ORG.IBM.
  - A supervisor in the location LOC.ISR.

Access attempts on hazard 'ha_01' that fail

Examples of context-based role attributes that fail an operation request on hazard `ha_01`:

Subject	Subject's context-based role attributes	Operation attempted	Reason for denied access
Sarah	worker:ORG.IBM.ANALYTICS	Read	This worker's organization, ORG.IBM.ANALYTICS, doesn't match any of the organizations that are defined for the hazard.

Ethan	worker:ORG.IBM.WIOT.WHI	Read	This subject is a worker in the organization ORG.IBM.WIOT.WHI, which is one organization lower in the hierarchy than the required organization, ORG.IBM.WIOT.
Karl	worker:ORG.IBM supervisor:LOC.DEU	Delete	Although Karl is a supervisor, his location context is LOC.DEU. To delete hazard `ha_01`, Karl must be a supervisor with a location context of LOC.ISR or an organization context of ORG.IBM.

Related information

- Access control matrix
- Owner check
- Setting up a newly provisioned IBM Maximo Worker Insights tenant