MO-004c — Unauthorized Resource Prohibition

Go to MO-004 — Connected and Disconnected Operations

Statement

Crucible SHALL NOT access a resource that is not an Authorized Resource for the applicable operational environment.

Derived From

This requirement derives from:

- MO-004 — Connected and Disconnected Operations

The Original Requirement states:

> *The system SHALL support both connected and disconnected operational environments.*[C1]

MO-004c preserves the implied constraint that Crucible operates within the resource-authorization boundary established for the applicable operational environment.

The separate requirements derived from MO-004 address:

- MO-004a — Connected Environment Operation
- MO-004b — Disconnected Environment Operation
- MO-004d — External Resource Independence

Assessment

The Original Requirement does not identify the resource-authorization constraints applicable within connected and disconnected operational environments.

The phrase **support both connected and disconnected operational environments** does not identify:

- The resources Crucible is permitted to access
- The authority that approves a resource for use
- The operational environment to which the authorization applies
- The duration or conditions of the authorization
- The treatment of a resource whose authorization expires or is revoked
- The behavior required when Crucible encounters an unauthorized resource

- The Evidence required to demonstrate compliance with the authorization boundary

MO-004c:

- Identifies Crucible as the responsible actor
- States the prohibited behavior directly through **SHALL NOT**
- Identifies an unauthorized resource as the prohibited object of access
- Ties resource authorization to the applicable operational environment
- Separates authorization from resource availability
- Separates unauthorized-resource prohibition from connected operation, disconnected operation, and external-resource independence

Rationale

A resource can be available within an operational environment without being authorized for use.

Examples include:

- An unapproved repository
- An unapproved package
- An unapproved container registry
- An unapproved network service
- An unapproved external endpoint
- An imported Artifact that has not completed admission checks
- A resource whose authorization has expired
- A resource whose authorization has been revoked
- A resource approved for a different operational environment
- A resource approved for a different Operational Lifecycle activity

An Authorized Resource has an identified authorization that applies to the operational environment and intended use.

Prohibiting access to unauthorized resources supports:

- Enforcement of environment boundaries
- Supply-chain control
- Prevention of unapproved dependency use
- Prevention of unauthorized external communication
- Configuration control
- Security control enforcement
- Compliance evaluation
- Provenance
- Traceability
- Generation of auditable Evidence

This requirement does not require every Authorized Resource to be available.

This requirement does not establish the resources required for execution in a Disconnected Environment. MO-004b addresses disconnected execution, and MO-004d addresses independence from unavailable external resources.

Applies To

This requirement applies to:

- Crucible
- Authorized Resources
- Unauthorized resources
- Connected Environments
- Disconnected Environments
- Air-Gapped Environments
- Operational Lifecycle activities
- Controlled Inputs
- Artifacts
- Artifact repositories
- Package repositories
- Image registries
- Network services
- External endpoints
- Imported dependencies
- Transfer Bundles
- Attached storage
- Runtime services
- Evidence
- Provenance
- Traceability

Verification

Verification confirms that:

1. The applicable operational environment is identified
2. The resources authorized for the operational environment are identified
3. Each resource accessed by Crucible has a valid authorization for the operational environment
4. Each resource authorization applies to the intended use
5. Crucible does not access a resource absent from the authorized resource set
6. Crucible does not access a resource whose authorization has expired or been revoked
7. Crucible does not access a resource authorized only for another operational environment
8. Each attempted access to an unauthorized resource is denied
9. Each attempted unauthorized access is recorded
10. The generated Evidence supports the authorization determination

Verification includes:

- Authorized Resource inventory inspection
- Resource authorization inspection
- Authorization-scope inspection
- Authorization-validity inspection
- Repository-access testing
- Registry-access testing

- Network-service access testing
- External-endpoint access testing
- Imported Artifact admission testing
- Expired-authorization testing
- Revoked-authorization testing
- Cross-environment authorization testing
- Access-denial testing
- Audit-record inspection
- Evidence inspection
- Provenance inspection
- Traceability inspection

The verification record identifies:

1. The applicable operational environment
2. The Authorized Resource set
3. Each resource accessed during execution
4. The authorization applicable to each accessed resource
5. The authorization scope
6. The authorization status
7. Each attempted unauthorized resource access
8. The denial result for each attempted unauthorized access
9. The audit record associated with each attempted unauthorized access
10. Each identified failure or exception
11. The observed result
12. The generated Evidence

Requirements Realized By

This requirement is realized by:

- OR-001 — Operational Roles
- OR-002 — Deployment Environments
- OR-003 — Classified and Unclassified Environments
- OR-005 — Distributed Environment Management
- FR-CFG-001 through FR-CFG-005
- FR-DEP-001 through FR-DEP-007
- FR-AG-001 through FR-AG-005
- FR-COMP-001 through FR-COMP-010
- FR-DSO-001 through FR-DSO-006
- FR-DEPC-001 through FR-DEPC-005
- SEC-001 through SEC-010

Related Architecture Sections

- 7. Infrastructure and Deployment
- 8. Dependencies and Air Gap Operations
- 9. Compliance and Security

- 10. Reproducibility, Provenance, and Traceability

Referenced By

The following pages reference this requirement:

- 3.1 Connectivity Conditions
- 4.3 External Systems
- MO-004a — Connected Environment Operations
- MO-004b — Disconnected Environment Operations
- MO-004d — Disconnected Resource Availability
- Annex D: Requirements Traceability

Delivery Phase

Phase 1 and subsequent phases

Implementation Status

Not Assessed

Implementation status requires verification that the current Crucible implementation denies access to resources that are not authorized for the applicable operational environment.

Requirement Status

Draft

This requirement derives from MO-004 in the Crucible System Requirements Specification, Version 1.1 Draft.

Notes for Editors

This requirement page should retain the stable requirement identifier `MO-004c`.

This page is a leaf requirement page and omits a trailing `:start` from its namespace.

Changes to the Statement SHALL preserve the unauthorized-resource prohibition derived from MO-004.

The authorization record for each Authorized Resource should identify:

- The resource identifier
- The resource type
- The applicable operational environment
- The permitted use
- The authorizing authority
- The authorization date
- The authorization status
- The authorization expiration condition
- Any applicable restrictions
- The supporting Evidence

Material changes should receive review and should update the related verification criteria, requirements realization, related architecture sections, and source records.

To reference this requirement Statement from another wiki page, insert:

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:01-mission-objectives:mo-004:mo-004c#Statement&noheader&nofooter&noeditbtn}}
```

Do not rename this page after an external citation unless a redirect or move plan is in place.
