

3.3 Security Domains and Transfer Boundaries

[Go to 3. Operational Environment](#)

[Crucible](#) operates across environments governed by different security controls, access restrictions, information-handling rules, and transfer constraints.

A [Security Domain](#) establishes the security conditions under which information, software, infrastructure resources, and operational activities are controlled. Different Security Domains can apply different authorization, access, handling, auditing, retention, and transfer requirements.

A [Transfer Boundary](#) separates environments or Security Domains and governs the movement of permitted [Artifacts](#), [Dependencies](#), records, and supporting [Evidence](#) between them.

Security Domains

Crucible can perform applicable [Operational Lifecycle](#) activities within [Classified Environments](#) and [Unclassified Environments](#).

The controls applicable to a Security Domain can affect:

- Which users, systems, and processes can access the environment
- Which Artifacts and Dependencies can enter or leave the environment
- Which repositories, services, and providers can be used
- Which information-handling and retention rules apply
- Which assessment, logging, and auditing activities are required
- Which transfer mechanisms and approvals are permitted
- Which [Baselines](#), configurations, and deployment subjects are authorized

Crucible applies the controls and restrictions established for the environment. Crucible does not establish the Security Classification, authorize access, or approve movement between Security Domains.

Transfer Boundaries

A Transfer Boundary governs movement between environments that do not share unrestricted access to the same resources.

A transfer can occur between:

- Connected and Disconnected Environments
- Connected and Air-Gapped Environments
- Classified and Unclassified Environments
- Security Domains with different access or handling restrictions
- Environments operated by different organizations or authorities

The responsible organization determines whether a transfer is permitted and identifies the applicable [Transfer Authorization](#), review process, handling controls, and transfer mechanism.

Crucible supports the controlled preparation and consumption of content associated with an authorized transfer. Crucible does not independently authorize the transfer.

Transfer Bundles

A [Transfer Bundle](#) provides a controlled package for moving identified Artifacts between environments.

The same Transfer Bundle retains its identity through:

1. Creation in the source environment
2. Review under the applicable Transfer Authorization
3. Movement across the Transfer Boundary
4. Receipt in the destination environment
5. Verification of [Transfer Bundle Integrity](#)
6. Import of identified Artifacts
7. Recording of the resulting Provenance, Traceability, and Evidence

A Transfer Bundle can contain permitted content such as:

- Machine Images
- Container Images
- Infrastructure Configurations
- Baselines
- Software packages
- Dependencies
- Manifests
- Content digests
- Digital Signatures
- Provenance records
- Traceability records
- Assessment results
- Supporting Evidence

The content of a Transfer Bundle depends on the selected lifecycle activity and the applicable transfer controls.

Export and Import

In the source environment, Crucible creates a Transfer Bundle for identified Artifacts selected for transfer.

The export activity identifies:

- The Transfer Bundle

- The included Artifacts
- The Artifact identifiers and revisions
- The source environment
- The intended destination environment
- The applicable transfer information
- The associated Provenance, Traceability, and Evidence

In the destination environment, Crucible imports identified Artifacts from the Transfer Bundle.

The import activity identifies:

- The received Transfer Bundle
- The Artifacts selected for import
- The destination environment and repository
- The import result
- The associated Provenance, Traceability, and Evidence

Import does not independently approve an Artifact for deployment, promotion, or operation. The applicable acceptance, security, compliance, and authorization processes determine whether the imported Artifact can be used.

Traceability Across Boundaries

Crucible preserves [Traceability](#) between the source and destination environments.

The traceability information can identify:

- The source and destination environments
- The applicable Security Domains
- The Transfer Boundary
- The Transfer Bundle identifier and revision
- The included Artifact identifiers and revisions
- The applicable Transfer Authorization
- Transfer Bundle Integrity information
- The export, transfer, receipt, and import activities
- The actors or processes associated with those activities
- The deployment or lifecycle result that consumes the imported content
- The Evidence generated during the transfer lifecycle

Preserving this information allows a reader or auditor to follow an Artifact from its source environment through transfer and import into the receiving environment.

Detailed transfer operations appear in [Section 7: Disconnected and Air-Gapped Operations](#).

Requirements Addressed

Requirement	Statement
OR-003a — Classified Environment Operations	Crucible SHALL execute each selected Operational Lifecycle activity within a Classified Environment .

Requirement	Statement
OR-003b — Unclassified Environment Operations	Crucible SHALL execute each selected Operational Lifecycle activity within an Unclassified Environment .
OR-003c — Security Domain Resource Enforcement	Crucible SHALL prevent an operation from accessing a resource not authorized for the operation's governing Security Domain .
OR-003d — Security Domain Information Enforcement	Crucible SHALL prevent an operation from processing information not authorized within the operation's governing Security Domain .
OR-003e — Information Handling Rule Enforcement	Crucible SHALL prevent an operation from handling information in a manner prohibited by the Information Handling Rules governing that information.
OR-003f — Cross-Domain Transfer Control	Crucible SHALL transfer information between Security Domains only through an authorized Cross-Domain Transfer .
OR-003g — Security Domain Access Control	Crucible SHALL deny an access request that the governing Security Domain does not authorize for the requesting identity.
FR-AG-002 — Artifact Export Packages	Crucible SHALL create Transfer Bundles for export.
FR-AG-003 — Artifact Import Packages	Crucible SHALL import Transfer Bundles .
FR-AG-005 — Deployment Traceability Across Disconnected Environments	Crucible SHALL maintain Deployment Traceability across Disconnected Environments .

The linked leaf requirement pages remain the canonical sources.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:
<https://wiki.didosolutions.com/dido/02-crusible/03-operational-context/03-03-security-domains-and-transfer-boundaries>

Last update: **2026/08/01 05:52**

