Genetec™

Genetec ClearID — Identity Request
Identity requests made easy

To provide access rights for a new contractor, tenant, or employee, an identity needs to be created in your access control system. With Genetec ClearID™, employees with the required permission can use the self-service portal to request an identity for users that are not currently in the system.

Creating identities without a paper trail

Traditionally, most access control systems would typically not track the details of a new identity created. Therefore, an organization assumes a level of risk when adding someone to their ACS. The risk increases when dealing with external parties such as contractors and tenants because they can come and go just like regular employees.

A better approach exists

Rather than submitting a form or picking up the phone to request a new identity, the ClearID web portal simplifies the process. This approach ensures accountability of the requestor and approver while providing complete visibility of the details to the relevant stakeholders. The identity request results in the creation of a cardholder in Security Center Synergis™.

Industry:
Financial institutions, Cannabis, Energy and Utilities, Commercial (office, factories, manufacturing plants), IT and telecommunications (Data Centers)

Applications:
Access Control, ClearID

Category:
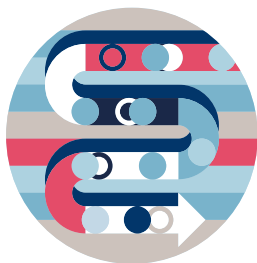Operations

Key benefits

User-friendly self-service portal

Automated workflow process is efficient and seamless

Identity is created as a cardholder with access rights automatically assigned in the Synergis ACS

The entire process is tracked, and audit trails details are available to the relevant stakeholders

How we help

Streamline identity requests

Using the self-service portal with optional approver workflow optimizes contractor and employee management and improves efficiency by interrupting fewer individuals who might not be the correct approvers.

Reduce risk

By automating the process to request a new identity, ClearID reduces the risk of human error. An identity created using the identity request can inherit specific access rights associated with an automatically provisioned role membership.

Increase accountability

The correct stakeholders in the organization gain complete visibility when a new identity is requested and approved. The requester, the approver, and the reason for the request are also tracked.

Key features and specifications

Workflow-based approach
The identity request workflow helps automate identity request tasks, such as approving, modifying, or denying requests.

Notification emails
Emails are sent to the relevant approver(s) when a new request is received, and to the requester after the request is approved or denied.

Approval process
Only a supervisor and/or identity approver can approve or deny identity requests.

Account administrator
Only an account administrator can create an identity template. The template can then be selected to request an identity.

Request multiple identities
Request multiple identities in the portal in one single request. When approved, all identities will be created in ClearID.

How it works

1 Create an identity template:
To begin, an administrator must create identity templates. Each template can have different configurations, such as enforcing an expiry date and maximum duration for the ACS, and an approval workflow.
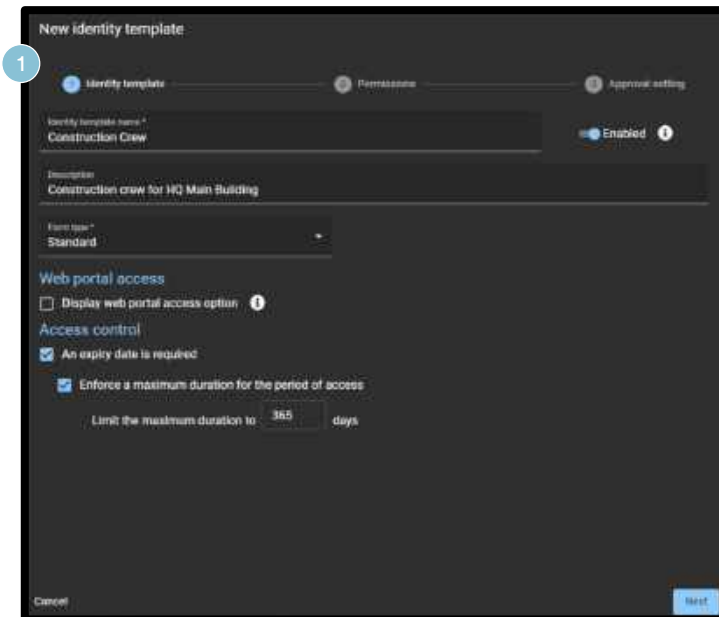
2 Request an identity:
Select an identity template and enter the new identity's information, work details, and access control activation date. When the request is approved, the identity is created in ClearID. The template selected determines the role membership and any role access for the new identity.