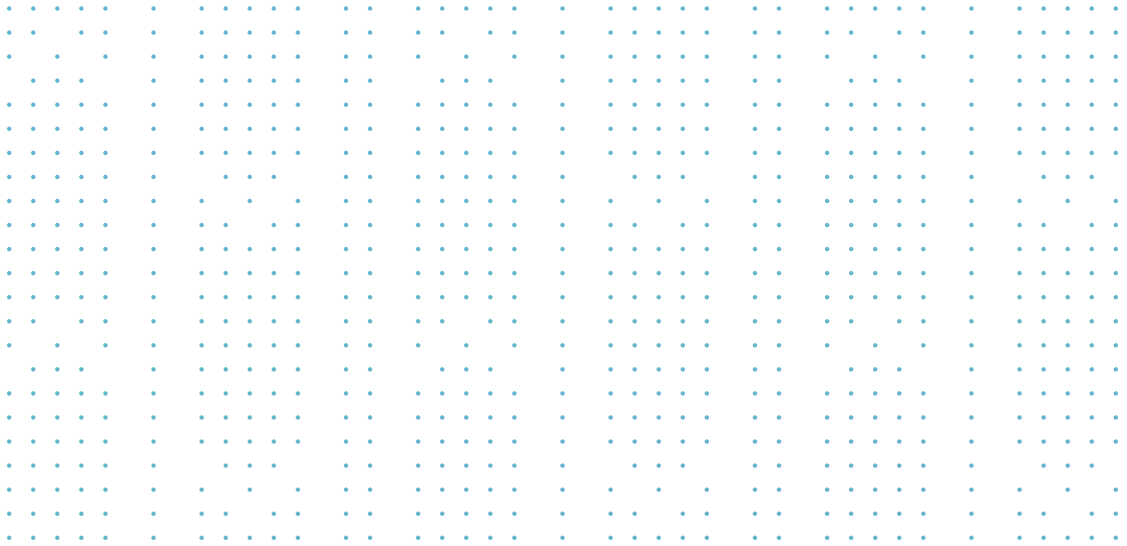




Unified physical identity and access management



Genetec ClearID™ improves the flow of people while being more efficient, compliant, and secure. The solution automates your organization's security policies, while centrally managing the access rights of your employees, contractors, and visitors.

Key benefits



Automate your operational procedures

Manually managing access requests, enrolling new employees, and checking in visitors is an outdated strategy. ClearID automates these activities, freeing up time and eliminating a common source of errors.



Simplify cardholder management

Standardize and streamline your organizations' policies from onboarding to offboarding employees and access requests. ClearID ensures access rights are always up to date.



Prevent unauthorized access

Ensure that only individuals with the right approvals have access to secure areas for the exact time frame required with access requests and reviews. Keep complete control over your organization's areas.



Improve the flow of people

Remove friction from temporary access requests and visitor management with the ClearID self-service portal. Requests are sent to the right individuals directly, eliminating unnecessary interruptions and delays.



Quick to deploy

Enjoy fast deployment with fewer integrations to maintain by unifying ClearID with Security Center Synergis access control system. Take advantage of a unified approach to security where you become more efficient and make better decisions with greater confidence.



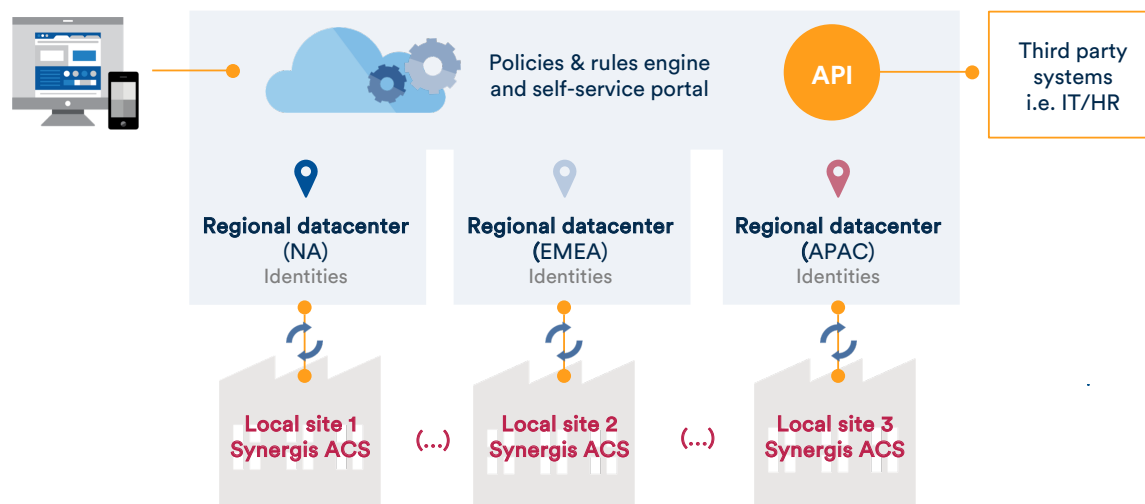
Reduce infrastructure cost

With ClearID, there is no need to deploy new servers, manage upgrades or worry about storing policies and identities outside of local jurisdiction. Its distributed cloud architecture lets you focus on your activities.

A global solution ensuring compliance and security

The integrated approach to traditional physical identity and access management (PIAM) system means that deployments and upgrades are complex and expensive. ClearID is 100% unified with Synergis, the Genetec Access Control System (ACS), offering a solution that will make your organization more efficient and secure. This means that any actions performed in ClearID are automatically synchronized with Synergis. ClearID appeals to global and multi-site organizations that manage thousands of internal and external people. The globally distributed architecture synchronizes data between local sites, regional services, and global services.

ClearID architecture



Private and secure by design

ClearID takes full advantage of its cloud-based architecture. It minimizes risks by storing encrypted data in data centers closest to the country specified by the employee profile. This ensures compliance with local data privacy regulations globally.

High availability

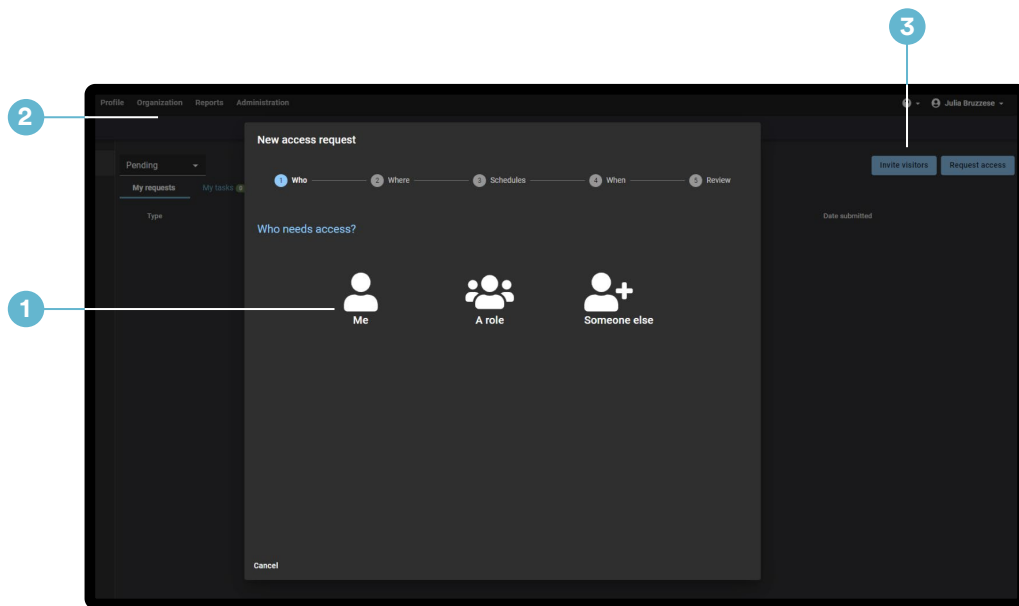
The service architecture is built for high availability and scalability. Critical data in Genetec ClearID™ is stored redundantly to mitigate the impact of any hardware failure.

Information security

All data and files imported in Genetec ClearID™ are encrypted, and all communication with the platform is secure. These encryption and security measures ensure that sensitive data, files, and communications are only seen by users with the appropriate access.

Automate access management

Manually managing access requests and visitors is time consuming, error-prone, and costly. ClearID offers a smarter, more efficient solution. Using the self-service portal, employees can make access requests, provision access rights, schedule and complete access reviews, and invite visitors on site. The automated process increases your organization's overall efficiency and improves the flow of individuals. ClearID also uses a workflow-based approach to request, and then approve or reject access or visit invites.



- 1 Requesting access**
An employee can easily request access for themselves, a role, or someone else within the organization. Access is granted based on employee attributes and policies.

- 2 Managing user tasks**
Under the Organization tab, employees can create new areas, identities, roles, and provisioning policies all from the comfort of a user-friendly portal.

- 3 Inviting visitors**
Through the self-service portal, employees can invite visitors on site for a specific event and duration.

ClearID key features

Unified with Synergis

Rather than piecing together systems that were never designed to work together, ClearID can be deployed faster and more easily because it's intrinsically unified with Synergis access control system.

Self-service portal

Give employees a better way to request new access privileges and invite visitors. With an online portal, they submit requests to area owners and supervisors without any direct interaction with access control system operators.

Automated workflows

Rely on automated workflows to process, and then approve or reject, access and visit requests, so that people involved in the review process can focus on other tasks.

Audit trail

Get tracking and reports for every operation associated with an identity. From temporary or permanent access requests and approvals to movement throughout the premises, ClearID provides the context behind exceptions and one-time requests.

Connectivity to 3rd party systems

Connect your ClearID platform to internal platforms like HR systems and Microsoft Active Directory to manage the entire lifecycle of an employee's identity in one place.

Automated onboarding/offboarding

When employees change role, job title, department, or location, ClearID automatically adjusts their access rights accordingly. This reduces internal risks and centralizes the application of onboarding and offboarding policies.

Auditing made simple

Improve your auditing process with ClearID access reviews. Perform an access review for an area or role to confirm that the access is still required and valid. Access reviews can be scheduled to occur automatically.

Visitor management

Ensure a memorable visit with ClearID. Whether guests are pre-registered or walk-in, all processes are automated, including check-in, temporary access management, and more.

Managing direct reports

Quickly adjust access rights of team members to ensure employees can contribute to your organization. Empower supervisors with the permissions to review, approve and manage direct reports' access, roles, and task delegation.

Visitor screening with internal watchlists

Ensure that your organization can take decisive action about visitors who are invited on site. Based on a list of Watchlist criteria, you can block unwanted visitors or notify personnel of an important visitor coming on site.

Comprehensive features list

ClearID general functions

Scalable for global deployments

“Out-of-the-box” nature of ClearID means it’s ready-to-commission and deploy

Support internal and external identities like employees, contractors, and visitors

Supporting multiple approval workflows

Notifications and approval emails

Integration with Google Maps for enhanced user experience

Customized branding of self-service portal per site

Automatic consolidation of existing cardholders into one identity profile based on various attributes

Delegation of permissions and tasks to another identity during period of absence

Comment box available for identities to capture reason for workflow actions

Platform

Corporate logo for Portal and email notifications

Cloud platform

HTML5 web interface with mobile support

REST API available to automate any functions available in the Web Portal

REST API compliant with OpenAPI specification

REST API documented using Swagger UI for quick experimentation

Synchronize Identity using Microsoft LDAP

Synchronize Identity using Microsoft Azure Active Directory

Synchronize Identity using ClearID REST API

Synchronize Identity using Database (SQL, Oracle, and ODBC)

Synchronize Identity using a CSV file

Customizable fields available with cardholders/Identities

Multi-site management

Global management of cardholders for multiple Synergis systems and across multiple sites

Time zone support (built-in)

Automatic synchronization of permanent credentials when someone travels between sites

Synchronization of cardholders and cardholder groups on the Synergis system

Site owners can configure access review schedules or initiate manual access reviews

Site owners can generate, save, and print an access reviews report

Centralized cardholder management and syncs between independent sites

Security and authentication

Single sign-on via OpenID connect

Support multi-factor authentications for users using OpenID connect

Single sign-on via Microsoft Office365

Single sign-on using Microsoft Azure Active Directory (AD)

ISO 27001:2013 certification

No centralized database contains all information

Personal data is stored in the data center closest to the country specified in the employee profile

Audit trails secured using block chain approach

AES-256 encryption with RSA

Encryptions keys and secret secured using Azure Key Vault

Software as a Service

Multi-tenant architecture leveraging Microsoft Azure

Virtualization support

Distributed cloud architecture

Comprehensive features list (continued)

Area management

- Delegate the management of controlled areas to one or more area owners
- Area owner or area approver can view, add, and remove people or roles from Areas
- Area owner or area approver can grant temporary access to a role
- Permanent cardholder can request temporary access to an area (built-in workflow)
- Actions in workflow are captured and available in workflow history
- Area approvers can approve or deny access requests
- Area approvers can perform area access reviews
- Email notifications when an access request is submitted, approved, or denied

Role management

- Delegate the management roles or cardholder group to one or more owners
- Role managers can add or remove people from their groups
- Automatic provisioning and synchronization of cardholder groups for multiple sites
- Role owners can request access to an area for their entire group
- Role managers can perform role access reviews

Visitor management

- Unified multi-site visitor management with Security Center Synergis Visitor Management task
- Preregister visitors using web portal
- Capture and report on the visit reason
- CSV visitor import supported for large events
- Visitor self-registration using the self-service kiosk
- Visitor check-in using Security Desk & self-service kiosk
- Automatic access right provisioning of visitors with required areas automatically assigned
- Paper badges and temporary credentials
- Email invitation sent to visitor with a meeting invite, site details, and optional file attachments
- SMS notifications sent to visitor host when visitor checks in
- Visitor escort with multiple visitor hosts

