Genetec ClearID™

Unified physical identity and access management

Genetec ClearID™ is a Physical Identity and Access Management (PIAM) platform that allows you to standardize, automate, and enforce security policies across all sites, while centrally managing the access rights of your internal and external identities so that you're more efficient, compliant and secure.

Key benefits

Automate your security policies

Lower your risk by moving away from the manual and error prone method of making access requests and managing access rights.

Improve the flow of people

Remove the friction employees face when requesting and receiving access to secure areas.

Ensure security is always up-to-date

Be certain that workarounds are not applied today or in the future. Standardize and streamline your policies from onboarding and offboarding, to access requests, and issuing new credentials.

Benefit from an "off-the-shelf" approach

Get ease of mind. Enjoy fast deployment with fewer integrations to maintain by unifying ClearID with Security Center Synergis™ access control system.

Reduce your risk of security breaches

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

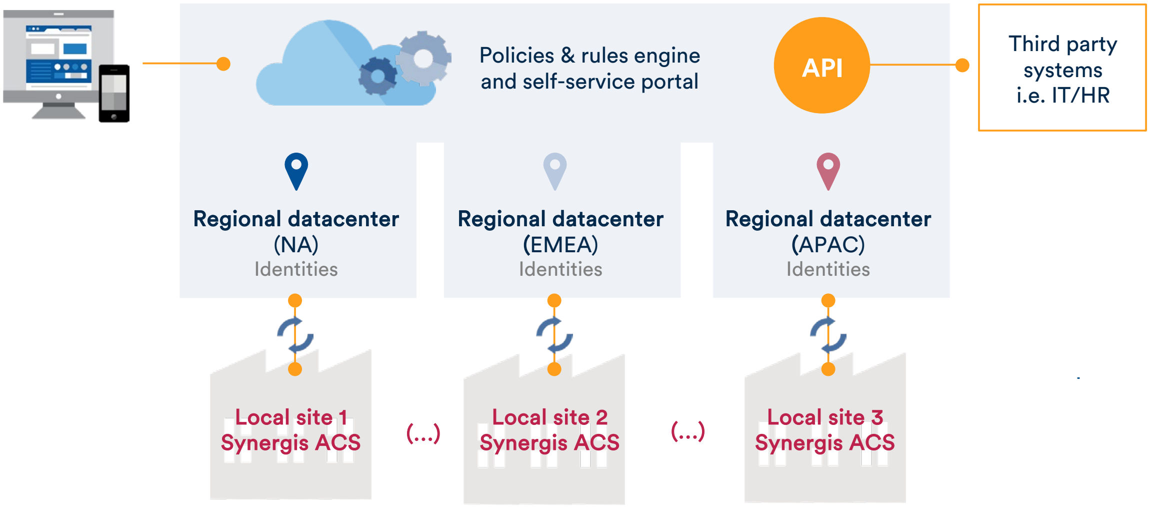
Maintain less infrastructure

Reduce your total cost of ownership. Benefit from a distributed cloud-based approach where identities are stored in their closest region, helping you maintain your people's privacy.

Reach new operational heights

The integrated approach to traditional Physical Identity and Access Management (PIAM) systems means deployments and upgrades are complex and expensive. ClearID is unified with Synergis, Access Control system (ACS), offering a true “out-of-the-box” solution that will make you more efficient. Offered as a truly hosted service, you benefit from a system that’s always up-to-date so that you keep your people moving and contributing to your organizational success.

ClearID architecture


Policies & rules engine and self-service portal
API
Third party systems i.e. IT/HR
Regional datacenter (NA)
Identities
Regional datacenter (EMEA)
Identities
Regional datacenter (APAC)
Identities
Local site 1 Synergis ACS
(...)
Local site 2 Synergis ACS
(...)
Local site 3 Synergis ACS

Private and secure by design

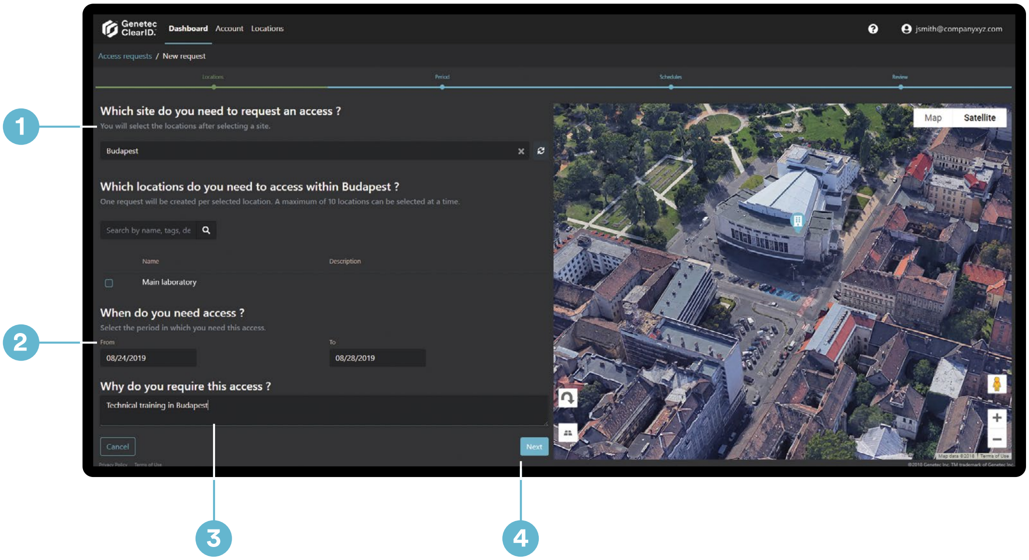
ClearID keeps your identities and policies highly secure in the closest Microsoft Azure datacenter to where your identities reside. This ensures that Personally Identifiable Information (PII) never leaves the region of where identities reside.

Scalable for global deployments

Backed up by the uptime and scalability from Microsoft Azure, ClearID appeals to global and multi-site organizations who manage thousands of internal and external identities.

Improve the flow of people

From smaller campus installations to complex multi-site deployments, ClearID is cleverly engineered to make your organization more efficient. With approval workflows, reduced operating overhead, and risk mitigation, ClearID will help organizations of all sizes improve their flow of people.. The web-based approach also means that employees can make access requests on their own, without having to wait and interact with an operator at the card office.



Access requests / New request

Which site do you need to request an access ?
You will select the locations after selecting a site.

Budapest

Which locations do you need to access within Budapest ?
One request will be created per selected location. A maximum of 10 locations can be selected at a time.

Search by name, tags, de

	Name	Description
□	Main laboratory	

When do you need access ?
Select the period in which you need this access.

From: 08/24/2019
To: 08/28/2019

Why do you require this access ?

Technical training in Budapest

1 Select location

Choose your desired location over a map-based interface or by selecting from a search bar. Select from an entire building or right down to a specific room.

2 Specify a duration

Most individuals don't require indefinite access to your resources. Identities can request access to a location for the exact time they need.

3 Input reasoning behind request

Management should know why identities are making requests to their resources to improve traceability.

4 Workflows behind the scenes

Once an access request is made, your security policies routes the request to the right approver(s) or simply auto approves based on identities, role, and attributes.

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.

Self-service portals

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

Workflow engine

Rely on automated workflows and email notifications to manage the lifecycle of identities so you enable a more fluid and efficient working environment for everyone – from entry to exit.

Traceability

Get tracking and reports of every operation or action tied to an identity throughout their lifecycle. From temporary or permanent access requests and approvals, to movement throughout the premises, ClearID paints the full picture by providing 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.

Pre-registration for visitor management

Improve your visitors' experience by automating all the processes throughout their lifecycle, including visitor pre-registration, check-in and out, badge printing, and more. It provides a central place to enforce visitor policies at all sites.

Automated onboarding/offboarding

Reduce your internal risk by centralizing your onboarding and offboarding policies. ClearID continuously updates access rights based on whether employees are active, on leave, or terminated.

Team management workspace

Empower supervisors to manage access requests on behalf of their team. Quickly swap access rights from one team member to another to ensure employees can contribute seamlessly to your organization.

Safeguarded identities storage

Keep private information about employees and visitors private and stored in the closest datacenter to where identities reside. ClearID distributes the storage of Personally Identifiable Information (PII) to lower your organizational risk.

End-to-end data security and privacy

Ensure servers, communications, and data are secured with the latest cryptographic protocols so that your ClearID and Synergis system are protected against emerging cyber threats.

Comprehensive features list

Core ClearID functions

- “Out-of-the-box” nature of ClearID means it’s ready-to-commission and deploy
- Attribute and role-based self-service portal for easy entitlement
- Support internal and external identities like employees and visitors
- Automatic consolidation of existing cardholders into one identity profile based on various attributes
- Approval workflows supporting multiple levels of authority
- Self-service means to request and manage temporary access requests to secure areas
- Location owners can review, grant, or deny access to people though self-service portal
- Dynamic access provisioning based on evolving attributes
- Comment box for collaboration between identities
- Notifications and approval emails
- Integration with Google maps for easier search queries
- HTML5 web interface with mobile support
- Customized branding of self-service portal

API and platform extensibility

- REST API compliant with OpenAPI specification
- REST API documented via Swagger UI for quick experimentation
- Single sign-on via OpenID connect
- Single sign-on via Microsoft Office365
- Synchronize Identity via Microsoft LDAP
- Synchronize Identity via Microsoft SQL Server upcoming
- Synchronize Identity from custom source via Identity REST API
- Customizable fields available with cardholders/Identities

Visitor management

- Unified multi-site visitor management with Security Center Synergis Visitor Management task
- Visitor pre-registration form supported
- Customized policies per work site
- Invitation email sent to guests with instructions that can be customized
- Reception assisted check-in (iOS app and Security Center web client)
- Host notification including SMS and email
- QR code support for check-in
- Create visitor groups
- Multi-host support
- Issue visitor badges (paper or access card)
- Support for visitor escort
- CSV visitor import supported for large events
- Visitor presence reports

Multi-site management

- Consolidate multiple instances of cardholders to a single identity across multiple sites
- Automatic replications of credentials across sites
- Centralized cardholder management and syncs between independent sites
- Global reporting and monitoring of independent sites through Federation™
- Temporary access request workflow for travelers

Security measures

- Claim based authentication with OAUTH 2 (RFC 6749)
- No centralized database with all the information
- Personal data is distributed in regional datacenters based on user citizenship and or residence
- Audit trails secured via block chain approached
- Personal Data encrypted AES 256 bits and RSA 1024 bits
- Encryptions keys and secret secured via Azure Key Vault

Software as a Service

- Multi-tenant architecture leveraging Microsoft Azure
- ISO 27001:2013 certification upcoming
- Virtualization support
- Distributed architecture

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

© Genetec Inc., 2019. Genetec, Clear ID, Synergis and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. All images are used for illustrative purposes only.