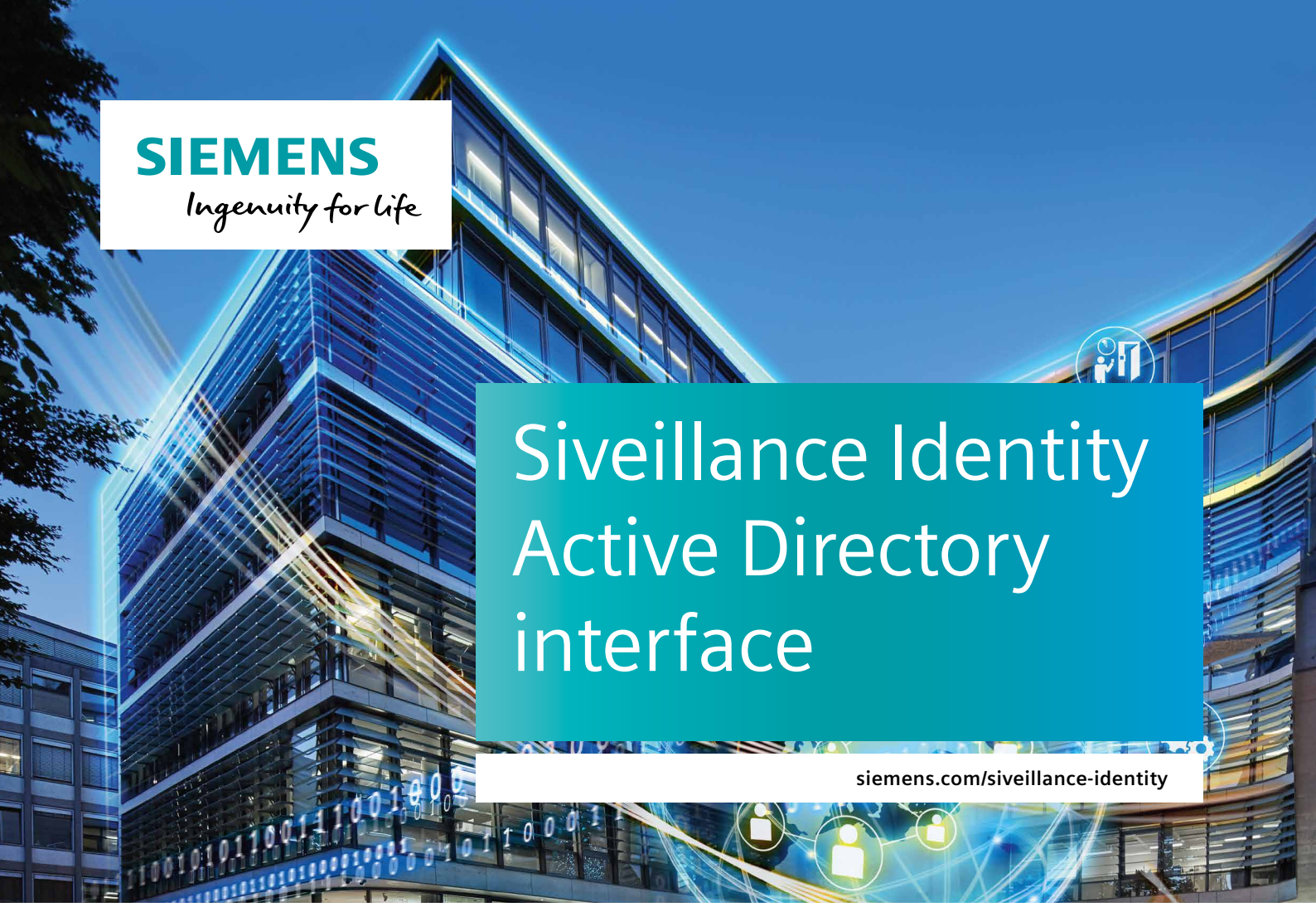


SIEMENS
Ingenuity for life

Siveillance Identity Active Directory interface

siemens.com/siveillance-identity

For the fast and effortless management of huge numbers of employee data. Siveillance Identity™ Active Directory interface enables the connection of Active Directory with SiPass integrated or SIPORT access control from Siemens, thus enabling the automation of on-boarding and off-boarding for employees, resulting in faster operations and an overall increase in security.

Cost reduction and improved performance
It is extremely important in a connected and digitalized world that physical access control seamlessly integrates into the HR and IT environment, so that new employees gain access to their workplaces smoothly and efficiently. It is equally important that access can be revoked instantly and reliably for employees leaving the organization. Siveillance Identity Active Directory offers an efficient and easy approach for managing the entire life-cycle of the employee's physical access using the company's Active Directory and electronic workflows.

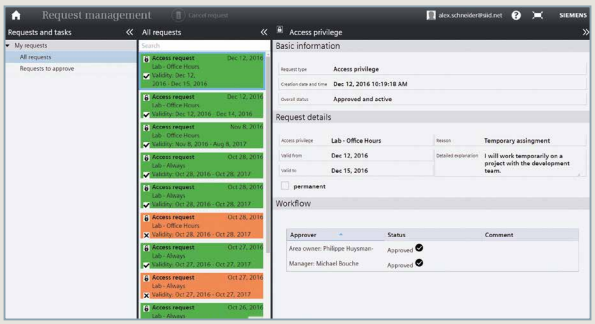
Designed for the needs of small to enterprise-scale companies and adhering to company policies and regulations, Siveillance Identity Active Directory interface is the ideal choice for offices, financial and insurance companies looking for the optimal solution to simplify life-cycle management of physical identities and access management.

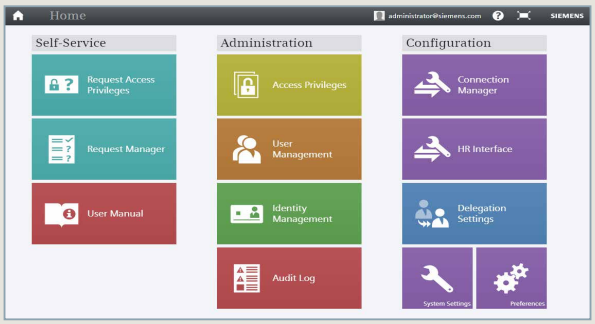
Authentication and authorization of all users
Active Directory is prominently available and an essential part of the IT infrastructure in all businesses. It allows authentication and authorization of all users and computers in a Windows domain type network. Management tasks such as on-boarding and off-boarding of employees are however not synchronized with the physical identities managed in physical access control systems.

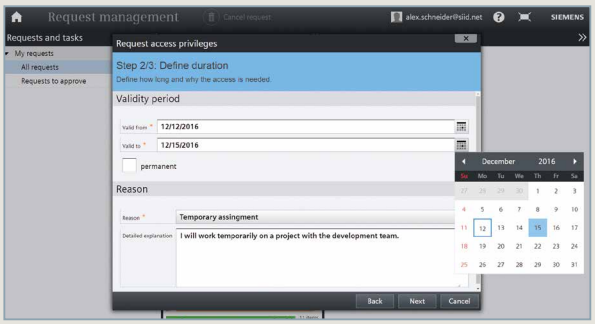
The link between logical and physical identity
The Siveillance Identity Active Directory interface allows the connection of the Active Directory and import of the user data in Siveillance Identity. Consequently, the information is also synchronized with SiPass integrated or SIPORT access control. As well as being added in the onboarding process, the data is also deleted in case a user is removed from the Active Directory.

A user can be either deleted in the Active Directory to remove access, or be temporarily disabled with the possibility of enabling him again, or deleting him permanently. When a user is disabled in the Active Directory, the Siveillance Identity™ interface ensures that the linked physical identity is also blocked in the access control system.

Siveillance Identity acts as the link between the "logical identity" (the Active Directory user) and the "physi-







cal identity" in the connected physical access control system. The convergence of physical and logical identities thus becomes reality.

Faster, more secure and always up-to-date

Automated processes speed up the on-boarding and off-boarding of employees, resulting in an increase in overall security. Identity information, such as organizational data, is always up-to-date, without the need for additional administration effort by access control operators. The use of a standard plug-and-play connector offers advantages compared to developing project specific interfaces that are known to be costly and difficult to maintain over the entire life-cycle.

Meeting regulations

"Cybersecurity by Design" is supported through extensive testing and hardening measures along the entire development process of Siveillance Identity Active Directory. It offers Lightweight Directory Access Protocol (LDAP) for user authentication as well as certificate-based, encrypted communication (HTTPS). In addition to this, the ProductCERT from Siemens provides an additional layer of cybersecurity and peace of mind through continuous global cyber threat monitoring that all the company's solutions benefit from. In case an employee leaves the company or is for various reasons blocked from accessing the company networks, blocked physical access is also ensured. Siemens supports you in complying with data privacy regulations, such as the European General Data Protection Regulation, as personal data is stored and then accurately and automatically erased when the employee leaves the company.

Highlights

- Streamlined and simplified access management
- Flexible and customizable solution
- Intuitive and user-friendly UI
- Increased security through automated on- and off-boarding
- Automated manual processes
- Cost reduction and savings in resources
- Meets enterprise compliance requirements
- Always up-to-date identity information

Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel. +41 41 724 24 24