Next Level Access Management & Security

topicus KEYHUB

TIME TO UPGRADE YOUR CORPORATE **SECURITY**

CREATE A NEW MINDSET

To optimize your business, digital solutions are crucial. Either comfortably in the cloud or on-premises. In order to improve efficiency, employees should be able to access all required applications easily and instantly. This poses an increasing challenge: how can you provide the exact right access for every employee without creating a huge management burden or annoying thresholds.

This is a challenge for every organisation, from SME to multinational. The jungle of accounts, applications, servers and passwords continues to grow. Nowadays, managing digital access is at least as important as physical security. Data of clients, customers or personnel are worth a lot and a data leak could potentially have catastrophic consequences. More and more organisations realize the need for a decent access management solution.

For such solutions to function properly, user adoption is key. Besides the obvious level of corporate security, it should be easy to use, maintain and manage. No unnecessary thresholds but an actual solution that raises awareness and minimizes risk.

“No unnecessary thresholds but an actual solution that raises awareness and minimizes risk.”

Unlimited flexibility

To safeguard your digital environment, employees should really embrace a solution. Flawless integration of cyber security thresholds help to create a positive user experience. While valuable information cannot be accessible to everyone, a flexible access management solution is required. A solution capable of easily integrating existing applications. Users will adopt such a system more quickly which results in more awareness and a more secure organisation.

Effortless management

Complex systems frustrate employees and prevent adoption. The more effort it takes to maintain control, the higher the risk of shadow IT and unmonitored accounts. Unmanaged servers, accounts or systems are an important attack factor and can be easily abused. To prevent this, an access management solution should support effortless management of privileged accounts and shared passwords and ensure ease of access, use and integration.

“Privileged accounts, default passwords and shared accounts pose a great risk for organisations”

Topicus KeyHub

Topicus KeyHub makes access management easier and more secure, increasing awareness among employees and reducing the management burden for system administrators. Every organisation that has shared accounts, self-supporting teams or external systems will become more productive and more transparent. Central authentication and decentral authorisation pave the road to a more secure organisation.

Central authentication

A single point to verify an identity ensures a single truth. Connected to the corporate Active Directory, HR-system or any other Identity Provider, each person has to be part of the organisation in order to log on. The mandatory 2FA reduces the risk of a password breach. An employee is only allowed to access the systems and servers he requires after successful authentication. This way, Topicus KeyHub ensures simplicity, security and authentication control.

Decentralized authorisation

Once a user has been authenticated, their authorisation is determined. Every organisation consists of multiple groups, departments or teams which all require access to specific resources. Topicus KeyHub ensures that each group of people has access to the exact set of applications, shared accounts or servers required to perform the tasks belonging to that specific group of people. Create custom groups for any occasion and let the group manager control the group members. This minimizes overhead of a central IT-department and guarantees awareness, control and compliance.

Next Level Administrator

It is no longer necessary to maintain a central administrative department to control the access rights of every employee. Topicus KeyHub passes the responsibility back to the business. It remains possible to organise access management centrally, but hybrid models or complete decentralisation are possible as well. This way the IT department can focus again on the already challenging tasks of monitoring the corporate infrastructure and its applications.

Security made easy

Topicus KeyHub makes securing your organisation simple. Installation takes less than a day and as Topicus KeyHub can be set up without a big bang introduction, the various applications, servers and teams can be connected gradually, as and when required. Employees instantly have their password manager, which already enables a more secure organisation. No rush or hasty implementations but dedicated steps towards more access control.

“Topicus KeyHub makes access management easier and more secure, increasing awareness among employees and reducing the management burden for system administrators”

SOME OF THE BENEFITS OF TOPICUS KEYHUB

01 BETTER SECURITY

Central authentication with 2FA
Topicus KeyHub authenticates users against an Active Directory, HR-system or any other Identity Provider within an organisation. This ensures that only active employees can log on and 2FA is enforced. Topicus KeyHub offers its own 2FA-app with push notifications, but other 2FA-solutions can be integrated as well.

Real-time provisioning
With Topicus KeyHub it's 'least privileged' on steroids. By default, no active accounts are present on connected systems such as servers or applications. If access to these systems is required, the corresponding group in Topicus KeyHub is activated and a personal account is created and provisioned. By default these accounts are enabled for an hour, after which they are disabled again. Any system that can authenticate against an LDAP of Active Directory can be connected this way, ensuring no active accounts after working hours.

Geen super-administrators meer
Topicus KeyHub has no super administrators or other accounts with unlimited access. System administrators are actual system administrators who are responsible for the application, not the access the application provides. Elevated privileges can only be gained by following a break glass procedure which involves the four-eyes principle. The risk and impact of fraud and security breaches are minimized as there is no 'one account to rule them all'.

Single Sign-On (SSO) with user-consent
Any group in Topicus KeyHub can offer Single Sign-On access to applications. Using either SAML2 or OAuth2 (OIDC) members of a specific group can gain SSO access to a specific application. Remove a user from a group and his SSO-privilege is instantly withdrawn. User consent and an extensive audit trail provide complete control of single sign-on solutions.

02 MORE TRANSPARENCY AND CONTROL

Decentralized authorisation
Groups and teams themselves determine who is allowed access to their specific set of applications or servers. Group managers are responsible for their group and determine whether someone may join or should be removed. All events that occur within a specific group are transparent to all group members, which raises social control and awareness of access management. Decentral authentication removes the need for a central administration to grant access.

Audit trail and access governance
Any event is transparent to the people who are connected to that event. Enabling an account on a server is visible to all other members of that same group. Events are recorded in the audit trail in a human readable format. The dashboard of Topicus KeyHub presents all information regarding the groups you are member of and the role you have in each of those groups. Whether it is a shared 2FA-code that was copied or a group that was activated, every event is logged. This is a big step towards ISO 27001 and GDPR compliance.

Access control and password management
In Topicus KeyHub, every group has their own password vault and every user has their own personal password vault. Therefore, Topicus KeyHub provides a complete solution for password management and access control. Effortless application of passwords, secrets and secure files is created with the browser extension and the command-line interface.

03
FLEXIBILITY AND CONNECTIVITY

External integrations

Any event generated by Topicus KeyHub can be sent to an external system. Stream every log item to a SIEM or update a custom dashboard or Slack-channel instantly upon access to a critical database server. Transparency of access events helps to create awareness.

Command-line interface

The Topicus KeyHub command-line interface enables machine-to-machine integrations. Access and creation of shared secrets in vaults can be automated. Reduce risks of plain-text passwords in build-scripts or integrate access management into DevOps-environments.

Withdraw access of former employees

Central authentication ensures that users who are deactivated in the Identity Provider cannot log on to Topicus KeyHub anymore. Furthermore, access to a specific group can be withdrawn by removing an employee from the group with a single click. The threat of former employees still having access is mitigated with Topicus KeyHub. And in compliance with the GDPR, access to teams or projects they no longer work on can easily be withdrawn.

“Every employee requires their unique set of access to applications, accounts or servers to work efficiently.”

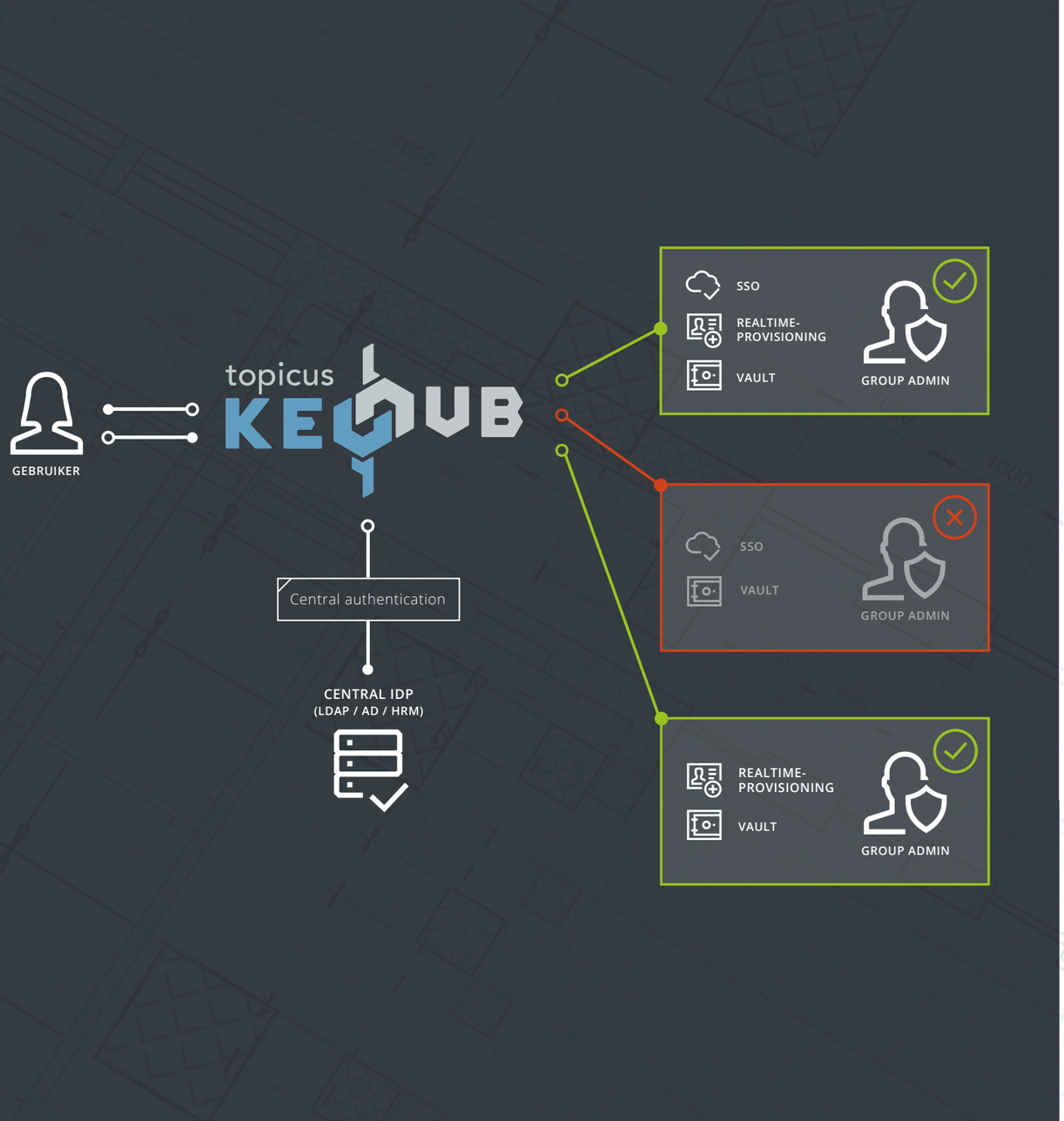
HOW DOES TOPICUS KEYHUB WORK?

Topicus KeyHub acts as a gatekeeper that secures and manages access to the entire server and application landscape. For this the authentication is performed at central level by authenticating users against the corporate identity provider. Additionally, 2-factor authentication is performed. After successful authentication, decentralized authorization takes over to determine which access an employee has.

Decentralized authorization provides the possibility of assigning specific access to specific groups of people and places the responsibility at this group level rather than a central IT department. This principle is shown in the illustration.

Topicus KeyHub divides an organisation into various groups. This division can be as broad or specific as required. Every group grants access to a set of servers, applications and shared passwords. Groups are managed by group managers, who are responsible for who may join the group.

This removes the traditional responsibility of the IT department to manage the access rights of all employees. Additionally, there is no super admin role in Topicus KeyHub, which implies that no user has access to everything.



Topicus KeyHub distinguishes three levels of access. Single Sign-On with KeyHub as the Service Provider is the most secure. SSO access is granted depending on the specific groups an employee is member of. If SSO is not possible, real-time provisioning is the next level of access. A group in Topicus KeyHub can be connected to an LDAP or Active DIrectory. Activating the group either creates or activates the user's personal account in the connected directory. The account is then provisioned with the specific access rights configured in Topicus KeyHub. Once activated, accessing the connected applications or servers is possible for a certain time slot, after which the accounts are deactivated and access to the systems is no longer possible.

The final level of access is account sharing. Account information can be stored in a group vault in Topicus KeyHub. Members of the group have access to these shared accounts, which can consist of passwords, secrets, files or 2FA-codes. Every time a secret is read by a user, this is logged in the audit log.

Topicus KeyHub can be set up alongside other security measures already in place. It integrates easily with most system architectures and additional benefits are gained within a single day.

TOPICUS KEYHUB IN ÉÉN OVERZICHT

Authentication

Central authentication

Integrates with multiple LDAPs or Active Directories

2-factor authentication

Authorisation

No super administrator or god mode

4-eyes principle

Time-based activation of accounts on LDAP/AD-systems

Real-time provisioning of accounts on LDAP/AD-systems

Custom groups with access to applications, servers and password vaults

Responsibility per group at group manager level

Single sign-on with SAML2 / OAuth2

Password management

Group-based password manager

2FA on shared accounts

Personal password vault for each user

Browser extensions for easy access

Awareness

Readable audit trail

Every event within your groups is visible

Provide a reason before activating an account

Transparency on all events

Connectivity

Webhooks on audit records

Command-line interface

Quick and gradual Installation

Easy and intuitive user interface

TOPICUS KEYHUB

Reduces management costs

Accelerates productivity of new employees

Minimizes risks of former employees

Simplifies ISO 27001, ISAE-3402 and SOC-II

Raises awareness among employees

Increases security

MORE INFORMATION?

Visit our website via www.topicus-keyhub.com, email us at keyhub@topicus.nl or call: +31 (0)85 065 3011. We would love to discuss the possibilities of Topicus KeyHub for your organisation!

Powered by topicus