

TrendMiner Success Series - Admin Track

June 17th, 2026

Identity & Permission Management in TrendMiner

Welcome to the webinar. We will start momentarily.





Listen only mode



**Use the question area
in the side panel**

Q&A at the end



**A recording + slides will be made
available after the webinar**

In today's session

Portal architecture

Where identity management lives in TrendMiner

User roles

Three roles, three levels of access

Access management & permissions

Controlling who sees what type of data

ConfigHub miscellaneous

API clients, system notification group, lockout & recovery

Identity providers

Local, LDAP, or SAML – choose wisely, best practices & pitfalls

Future improvements

What's coming?

Closing and questions

Wrap up



Portal architecture

Where identity management lives in TrendMiner

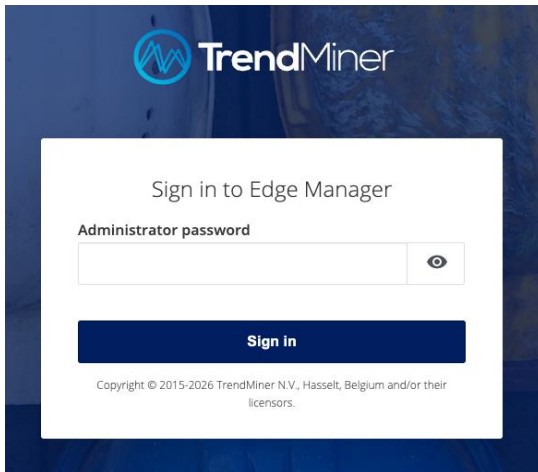
Portal Architecture

From appliance access in EdgeManager to identity management in ConfigHub

EdgeManager

- Only password require for login
- ConfigHub entry & recovery option

Your journey starts here



The screenshot shows the login interface for Edge Manager. At the top left is the TrendMiner logo. The main heading is "Sign in to Edge Manager". Below it is a label "Administrator password" followed by a text input field with a toggle eye icon. A dark blue "Sign in" button is positioned below the input field. At the bottom, there is a small copyright notice: "Copyright © 2015-2026 TrendMiner N.V., Hasselt, Belgium and/or their licensors."

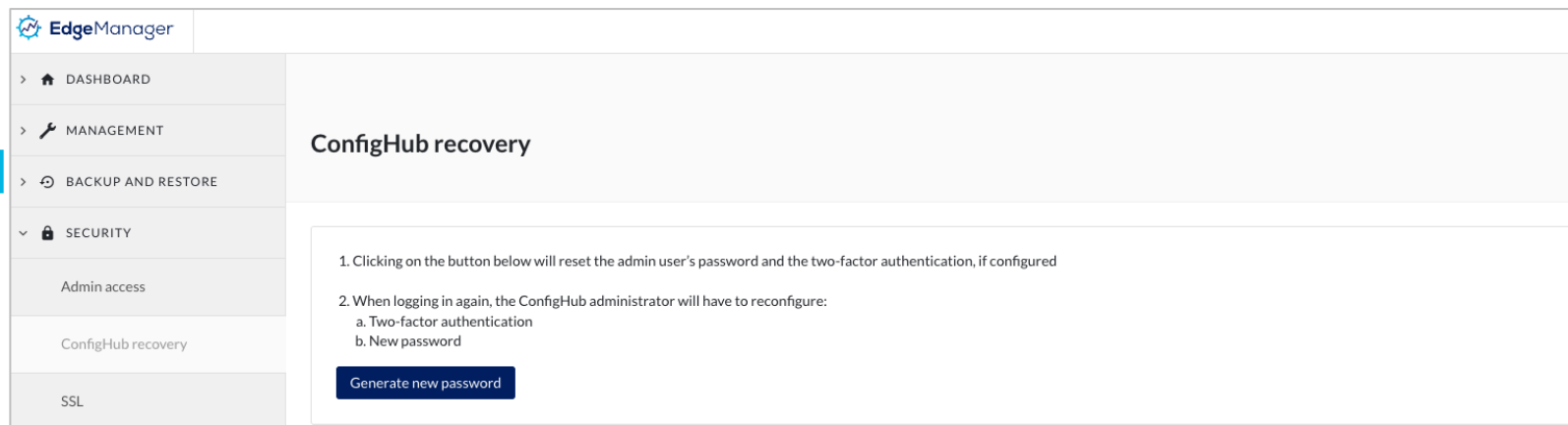


ConfigHub

- Hardcoded 'admin' account with enforced 2FA
- Identity Providers Management
- Users, Groups, Client Management
- Access Management
- Certificates Management
- Requires **System Administrator** role to access

Lost Access to ConfigHub?

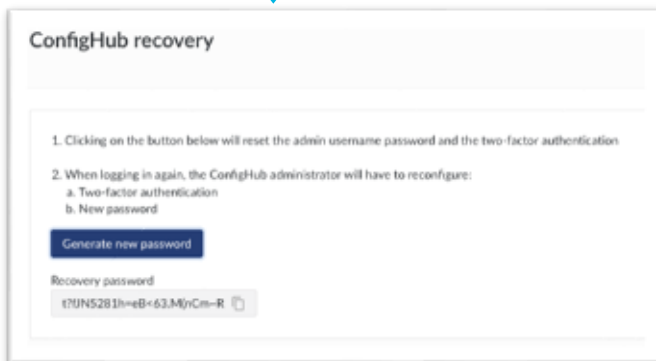
Resetting the 'admin' password 2FA from Edge Manager



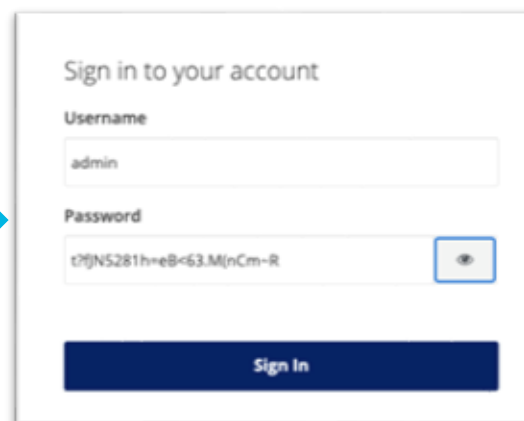
The screenshot shows the Edge Manager interface. On the left is a navigation menu with the following items: DASHBOARD, MANAGEMENT, BACKUP AND RESTORE, SECURITY (expanded), Admin access, ConfigHub recovery, and SSL. The main content area is titled "ConfigHub recovery" and contains the following instructions:

1. Clicking on the button below will reset the admin user's password and the two-factor authentication, if configured
2. When logging in again, the ConfigHub administrator will have to reconfigure:
 - a. Two-factor authentication
 - b. New password

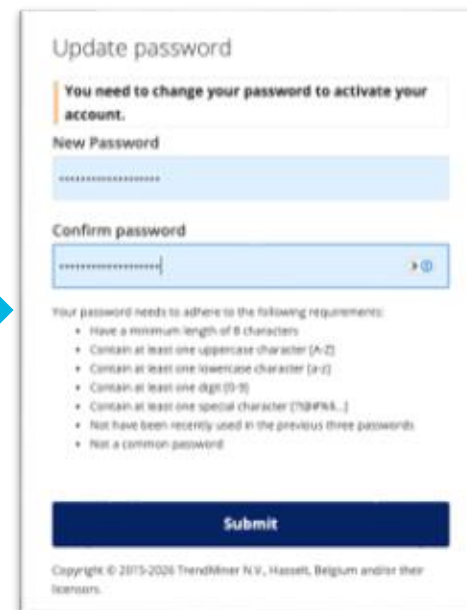
Below the instructions is a blue button labeled "Generate new password".



This is a zoomed-in view of the "ConfigHub recovery" page. It shows the instructions from the previous screenshot. At the bottom, a "Recovery password" field displays the generated password: `t?jNS281h=eB<63.M(nCm-R`.



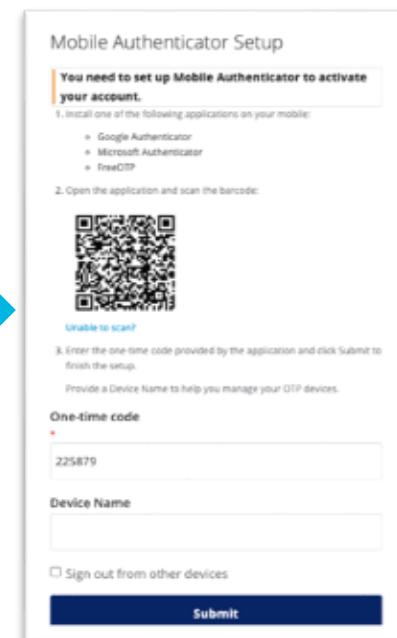
This is the "Sign in to your account" page. The "Username" field contains "admin". The "Password" field contains the recovery password: `t?jNS281h=eB<63.M(nCm-R`. A "Sign In" button is at the bottom.



This is the "Update password" page. It prompts the user to change their password to activate their account. It includes fields for "New Password" and "Confirm password". Below these fields, a list of password requirements is shown:

- Have a minimum length of 8 characters
- Contain at least one uppercase character [A-Z]
- Contain at least one lowercase character [a-z]
- Contain at least one digit [0-9]
- Contain at least one special character [!@#%&...]
- Not have been recently used in the previous three passwords
- Not a common password

A "Submit" button is at the bottom.



This is the "Mobile Authenticator Setup" page. It instructs the user to install a mobile authenticator application and scan the QR code. A QR code is displayed. Below it, a "One-time code" field contains the code "225879". A "Device Name" field is also present. A "Submit" button is at the bottom.

ConfigHub Recovery – Watch Out For These


Common pitfalls during 2FA setup

Mobile Authenticator Setup

1. Install one of the following applications on your mobile:

- FreeOTP
- Microsoft Authenticator
- Google Authenticator

2. Open the application and scan the barcode:



Unable to scan?

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

One-time code

Invalid authenticator code.

Device Name

Sign out from other devices

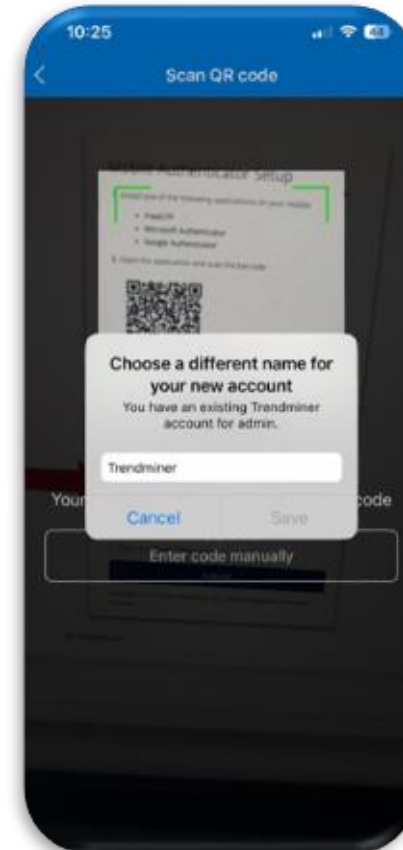
Submit

Copyright © 2015-2026 TrendMiner N.V., Hasselt, Belgium and/or their licensors.

- check NTP is enabled and synchronised in Edge Manager

NTP enabled	Yes	NTP synchronized	Yes
-------------	-----	------------------	-----

- If managing multiple TrendMiner instances - create a separate 2FA profile



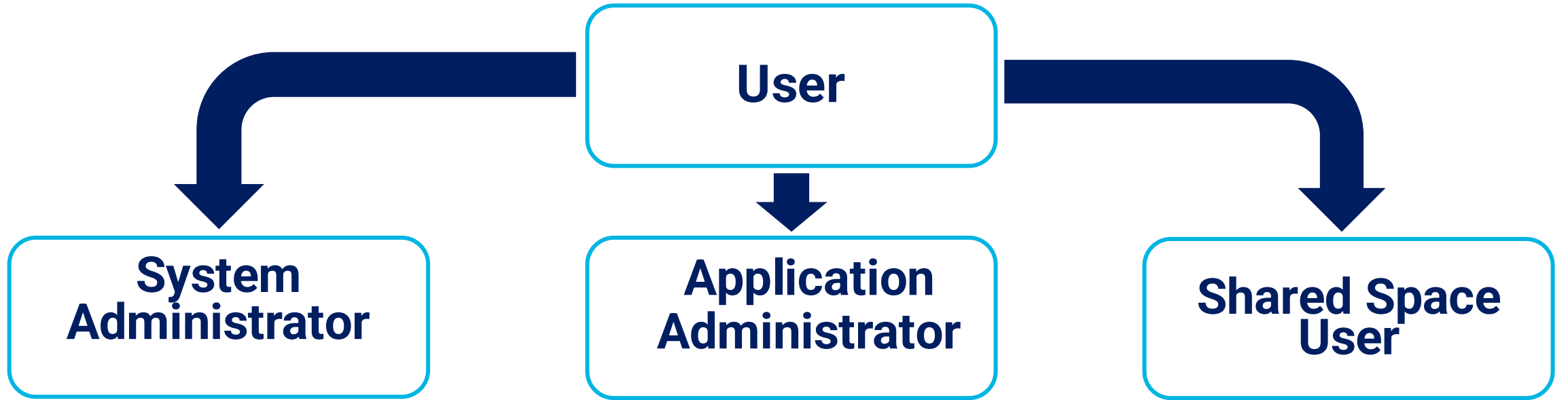


User Roles

Three roles, three levels of access

Configurable roles in ConfigHub

Who can do what?



- Have **ConfigHub Access**
- Can manage majority of TrendMiner
- + all permissions of an Application Administrator

- Does not have **ConfigHub Access**
- Default access to access management's entities
- Can perform application administrator tasks such as
 - Managing tag indexes
 - Managing Asset permissions in ContextHub
 - Managing context items & permission in ContextHub

- Same as default user, but with 1-year login timeout
- Best for prolonged dashboard/content display



Access management & permissions

Controlling who sees what type of data

Access Management in ConfigHub

The three building blocks of data access control

Domain

What type of resource?

Entity

Which specific resource?

Members

Who gets the permission?

DATASOURCE

Historian/time series data

TIMESERIES_BUILDER

Notebooks,
Custom Calculations

For DATASOURCE

Datasource Name:

Exactly as configured in the ConfigHub (e.g. Site1)

ALL

Wildcard – grant access to all datasources. Only available for DATASOURCE domain

For TIMESERIES_BUILDER

NOTEBOOK:

Access to ML-Hub notebooks

CUSTOM_CALCULATIONS :

Access to custom calculations in the tag builder

User

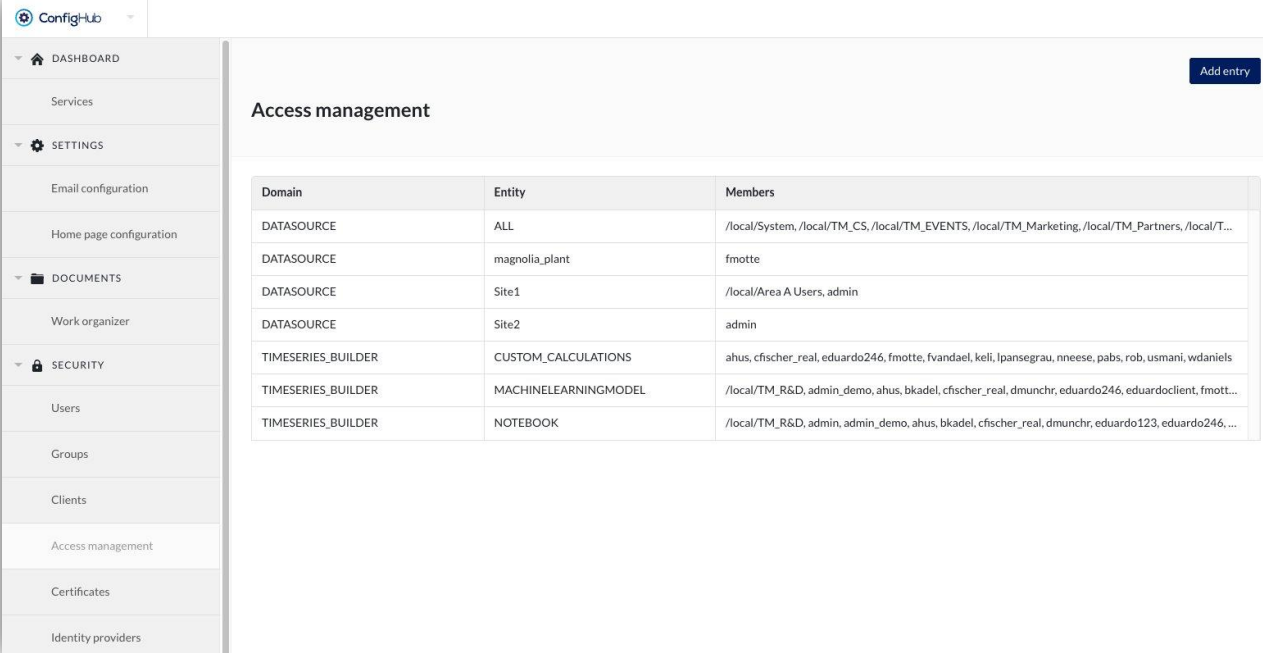
An individual user account

Group

Either local or groups synced from external IDP

Client

A client ID for API or external system integration



The screenshot shows the ConfigHub interface with a sidebar menu on the left and an 'Access management' page on the right. The sidebar includes options like DASHBOARD, SERVICES, SETTINGS, DOCUMENTS, SECURITY, and IDENTITY PROVIDERS. The main content area displays a table with columns for Domain, Entity, and Members. An 'Add entry' button is visible in the top right corner of the table area.

Domain	Entity	Members
DATASOURCE	ALL	/local/System,/local/TM_CS,/local/TM_EVENTS,/local/TM_Marketing,/local/TM_Partners,/local/T...
DATASOURCE	magnolia_plant	fmotte
DATASOURCE	Site1	/local/Area A Users, admin
DATASOURCE	Site2	admin
TIMESERIES_BUILDER	CUSTOM_CALCULATIONS	ahus, cfscher_real, eduardo246, fmotte, fvandael, keil, lpansegrau, nneese, pabs, rob, usmani, wdaniels
TIMESERIES_BUILDER	MACHINELEARNINGMODEL	/local/TM_R&D, admin_demo, ahus, bkadel, cfscher_real, dmunchr, eduardo246, eduardoclient, fmott...
TIMESERIES_BUILDER	NOTEBOOK	/local/TM_R&D, admin, admin_demo, ahus, bkadel, cfscher_real, dmunchr, eduardo123, eduardo246, ...

! Permissions on assets and context data are managed in ContextHub, not in ConfigHub (yet)!

Asset Permissions

Managing Asset Permissions via ContextHub

The screenshot shows the ContextHub interface for managing asset permissions. On the left sidebar, the 'Asset permissions' option is highlighted with a red box and the number '2'. Below it, the 'DIGITAL TWIN MANAGER' section is also highlighted with a red box and the number '3'. At the bottom left, a gear icon is highlighted with a red box and the number '1'. In the main content area, a search bar contains 'pi201' and a list of assets includes 'PI2018 AF2', which is highlighted with a red box and the number '4'. The right pane shows the 'Access for PI2018 AF2' configuration, including 'INHERITED PERMISSIONS' (No inherited permissions found), 'ASSET PERMISSIONS' (Name: Read context items), and an 'Overview' section for the 'Everyone' group. A dropdown menu for 'Read context items' is open, showing options: 'Read context items' (selected), 'Browse', and 'No access'.

- Assign an asset tree permission type to the selected users or Everyone
- Group assignment is not supported

The screenshot shows the TrendHub interface. The top navigation bar includes 'TrendHub' and 'Assets'. A search bar contains 'PI2018' and a dropdown menu is open, showing a search result for 'PI2018 AF2' with a right-pointing arrow.

User browsing an Asset tree in TrendHub



ConfigHub miscellaneous

API clients, system notification group, lockout & recovery

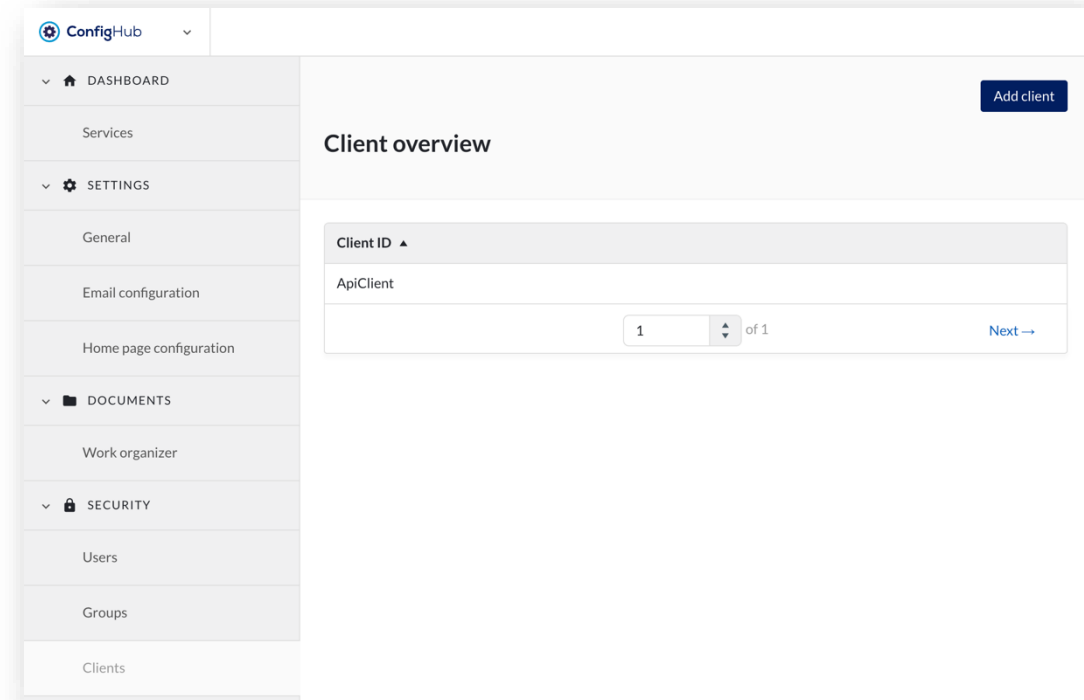
Clients in ConfigHub

Secure access to TrendMiner APIs for external systems

- Every client is built on two credentials – a Client ID and a Client Secret



- Only System Admins can create and manage clients
- Regenerating the secret will immediately break any integration using the old one
- Don't forget to add client to Access Management – without it the integration authenticates but gets no data



System Notification Group in ConfigHub

How the “*tm-confighub-notifications*” group keeps admins informed?

- Non deletable built-in system group
- Alerts members even when offline
- Add system admins who own the config and data integrations

The screenshot shows the ConfigHub interface. On the left is a sidebar with 'ConfigHub' at the top, followed by 'Work organizer', 'SECURITY', 'Users', 'Groups', 'Clients', and 'Access management'. The main area is titled 'Group overview' and contains a search bar with 'tm-' and a table with one row: 'tm-confighub-notifications' with path '/tm-confighub-notifications'. A modal window on the right shows 'tm-confighub-notifications' details, including 'GROUP DETAILS' (Name: tm-confighub-notifications, Path: /tm-confighub-notifications) and 'MEMBERS' (bkadel - Bipin Kadel).

Notifications includes

- Tag synchronization errors
- Webhook delivery failures
- Failed context item writes to external systems

Tag sync failed for PI2024



○ monitors@trendminer.com <monitors@trendminer.com>

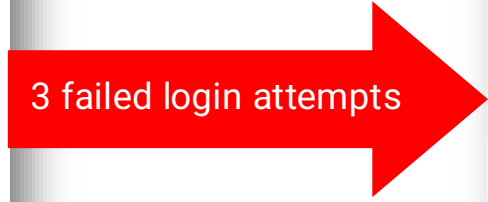
To: ● Bipin Kadel

An issue occurred while syncing tags from the data source PI2024. Please check ConfigHub for more details.

Account Lockout in ConfigHub

3 failed attempts, one unlock button

The screenshot shows the ConfigHub user management interface for a user named 'stijna'. The user's name is highlighted with a green box. The 'Update' button in the top right corner is also highlighted with a green box. The user's role is set to 'Application Administrator' and 'System Administrator'. The 'Change password' button at the bottom is highlighted with a green box. The 'Delete user' link is visible in red text.



The screenshot shows the ConfigHub user management interface for the same user, 'stijna', but now the user is locked. The text 'stijna (Locked)' is highlighted with a red box. The 'Unlock' button in the top right corner is highlighted with a red box. The 'Change password' button at the bottom is highlighted with a red box. The 'Delete user' link is visible in red text.



Identity providers

Local, LDAP, or SAML – choose wisely, best practices & pitfalls

Identity Providers

Understanding your options before choosing

Local	LDAP	SAML Best choice
<ul style="list-style-type: none">• Username/password login• No integration• Users & Groups managed in TrendMiner• No 2FA• Users can be soft-deleted	<ul style="list-style-type: none">• Username/password login• Synced from LDAP server (daily/weekly, or manual)• Users & Groups managed in external IdP• No 2FA• Users can be soft-deleted (Once deleted/removed on the AD)• One time mapping	<ul style="list-style-type: none">• Single SignOn login• Synced from SAML only at successful user login (user+group)• Users & Group Managed in external IdP• 2FA if configured in IdP• Users cannot be deleted• One time mapping
All		

- Support groups
- Can be combined



Migration supported in both directions



Migration not yet supported

SAML / SSO

Best Practices

Category	Configuration item	Recommended setting	Why	What we're preventing	Priority
NameID configuration	NameID format	Set to persistent	Treats the identifier as a stable, long-term handle across sessions.	Duplicate accounts created each time the user re-authenticates.	Critical
	Source attribute	Entra ID: user.userprincipalname with ToLowercase	SAML identifiers are case-sensitive — lowercase enforces consistency.	Silent duplicate accounts from casing differences at login.	Critical

Configuration on identity provider's side

The screenshot shows the 'Manage claim' configuration in the Microsoft Azure portal. The 'Name identifier format' is set to 'Persistent'. A 'Manage transformation' dialog is open, showing the following configuration:

- Transformation *: ToLowercase()
- Parameter 1 *: Attribute (selected)
- Attribute name *: user.userprincipalname

Configuration on SP (TrendMiner) side

The screenshot shows the 'SAML-Azure' configuration page on the SP (TrendMiner) side. The configuration includes:

- Name: SAML-Azure
- Base domain: cs.trendminer.net
- NameID Policy Format: Persistent
- Principal Type: Subject NameID
- Sign Assertion: Signed (checked)
- Identity provider metadata file: Browse files (checked)
- Enable Attributes Mapping: checked

SAML / SSO

Best Practices

Category	Configuration item	Recommended setting	Why	What we're preventing	Priority
Group & Claims	Group claims – Source attribute	sAMAccountName or display name — never Object ID	Human-readable names make group management in ConfigHub practical.	ConfigHub filled with unreadable GUIDs instead of group names.	High

The screenshot shows the 'Group Claims' configuration page in the Microsoft Azure portal. The page title is 'Group Claims' and the subtitle is 'Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your a...'. The page contains several sections: 'Which groups associated with the user should be returned in the claim?' with radio buttons for 'None', 'All groups', 'Security groups', 'Directory roles', and 'Groups assigned to the application' (selected). Below this is the 'Source attribute *' dropdown menu, which is highlighted with a red box and has a red arrow pointing to it from the table above. The dropdown menu shows 'sAMAccountName' selected. Other options in the dropdown include 'Group ID', 'sAMAccountName', 'NetBiosDomain\sAMAccountName', 'DNSDomain\sAMAccountName', 'On Premises Group Security Identifier', and 'Cloud-only group display names'. The page also shows 'Required claim' and 'Additional claims' tables.

⚠ Caution

By default, the Group ID will be selected as Source Attribute. This corresponds to the Object ID of the Azure AD group, typically a 37-character string in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. The group will be identified in Confighub as this long identifier as well, so for human readability and admin usability, it is recommended to change the Source attribute.

LDAP / AD

Best Practices

Category	Configuration item	Recommended setting / value	Why	What we're preventing	Priority
Security & connectivity	Manager DN account	Dedicated service account with non-expiring password	Password expiry on a regular account breaks sync without warning.	Sudden LDAP sync failures when the account password expires.	Critical
	Dedicated OU / CN	Create a TrendMiner-specific OU in AD for users and groups	Scoping to a dedicated OU reduces filter complexity and avoids the 4000-char limit.	Search filter exceeding the limit and failing to sync.	High
Directory structure	User Base DN	Point to specific OU — never the root DC	A broad Base DN scans the entire directory, increasing sync time and load.	Slow syncs and hitting the 10k user limit	High

The screenshot shows the ConfigHub interface for Active Directory / LDAP Configuration. The left sidebar contains navigation options: DASHBOARD, SERVICES, SETTINGS, DOCUMENTS, and SECURITY. The main content area is titled 'Active Directory / LDAP Configuration' and includes a sub-header 'Please configure server settings.' Below this, there are several input fields for configuration:

- Name:** TM-LDAP
- Vendor:** Active Directory
- Provider URL:** ldaps://ad.trendminer.net
- Manager DN:** cn=managerServiceAccount,CN=Users,DC=ad,DC=trendminer,DC=net
- Manager password:** [Redacted]
- User base DN:** OU=DedicatedUsersOU,DC=ad,DC=trendminer,DC=net
- User search filter:** (objectCategory=Person)



Future improvements

What's next

Future Improvements

What's next

SAML user management — coming to ConfigHub

- Link and unlink federated user mappings
- Delete incorrectly mapped or duplicate SAML users
- Eliminate the need for Keycloak console access or database manipulation for user remediation

License-based roles

- More user roles definitions based on skill & usage of TrendMiner
- Admin can assign a license role to a “Group”
- Centralized view of license distribution and usage, & reporting in ConfigHub



Closing & Questions

Wrap up

Pages referenced in this webinar

Useful resources

- ConfigHub Recovery

<https://documentation.trendminer.com/en/confighub-access-recovery.html>

- Admin Roles Compare

<https://documentation.trendminer.com/en/admin-roles-compared.html>

- Access Management

<https://documentation.trendminer.com/en/step-4--connect.html#UUID-81563b2a-df2e-35c2-5fde-b7618656a1ef>

- System group tm-confighub-notifications

https://documentation.trendminer.com/en/confighub-153661.html#UUID-46d6c470-c2f4-eca9-f4c3-47a2037f4463_bridgehead-id235497298089334

- Clients

<https://documentation.trendminer.com/en/confighub-153661.html#UUID-9c3c59bf-a73c-63c3-e399-4757ad797c96>

- Asset Permission

<https://userguide.trendminer.com/en/asset-permissions.html>

- Context Permission

<https://userguide.trendminer.com/en/context-item-type-permissions.html#UUID-7fc9bbf0-fd45-d590-8cd0-dd6f0c6ce0bb>

- Identity Providers

<https://documentation.trendminer.com/en/confighub.html#UUID-ab24ff45-8946-5d4d-c11f-7a8e0d8ada8a>

- Unlock User Account

https://documentation.trendminer.com/en/confighub-153661.html#UUID-fd63ac9c-3ab8-c883-efac-4d0409c80324_bridgehead-idm234469471868871

Tip: ask your favorite AI chatbot to help out (but always verify against our docs)

Save the dates

TrendLab EU

Eindhoven, NL, September 23rd - 24th

TrendLab US

Houston, US, October 7th - 8th

Questions?