TrendMiner Success Series - Admin Track

June 17th, 2026

Identity & Permission Management in TrendMiner

Welcome to the webinar. We will start momentarily.

TrendMiner

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

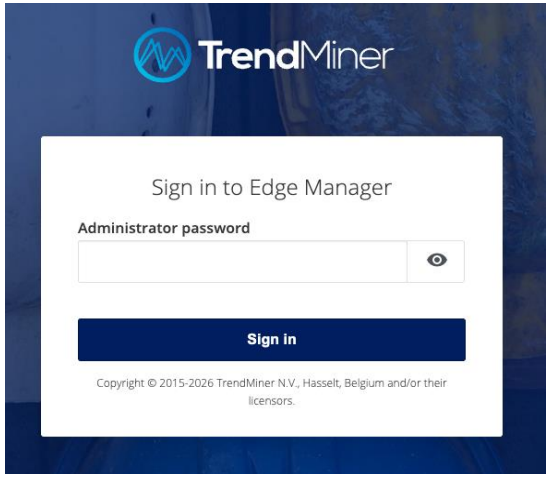
Portal Architecture

From appliance access in EdgeManager to identity management in ConfigHub

EdgeManager

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

Your journey starts here



KEYCLOAK

ConfigHub

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

TrendHub

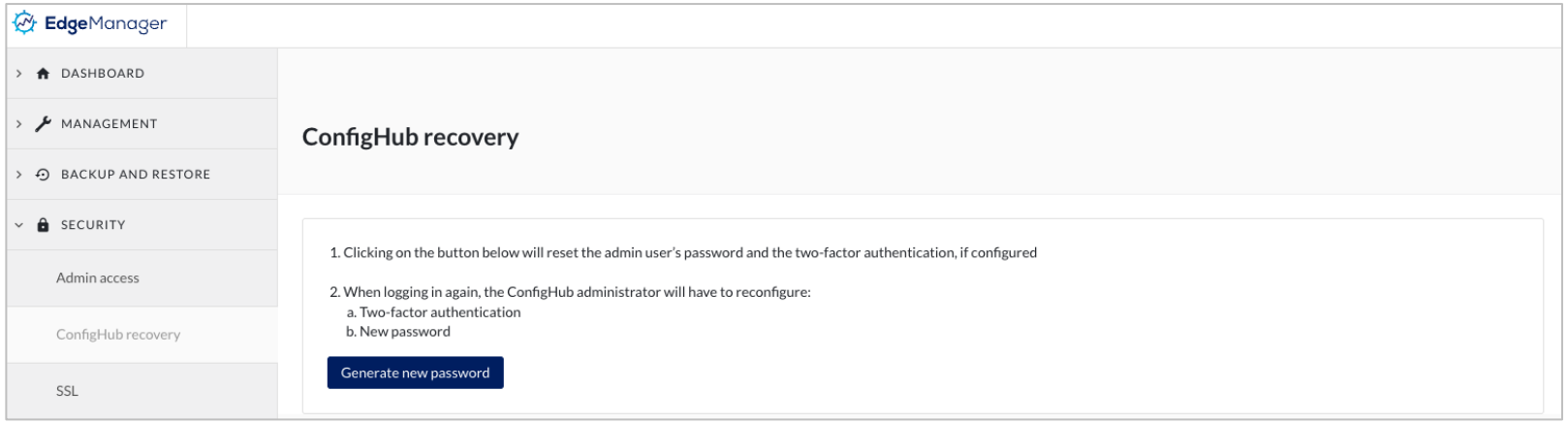
DashHub

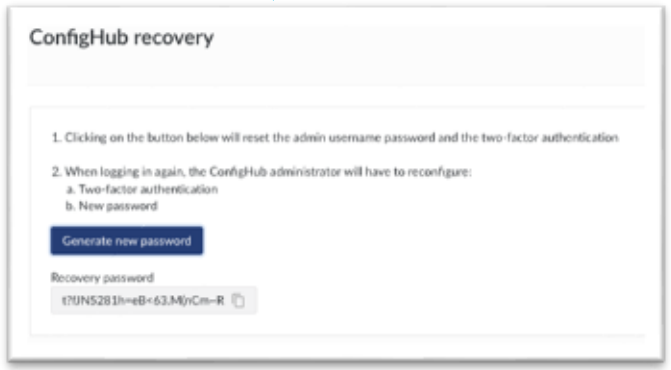
ContextHub

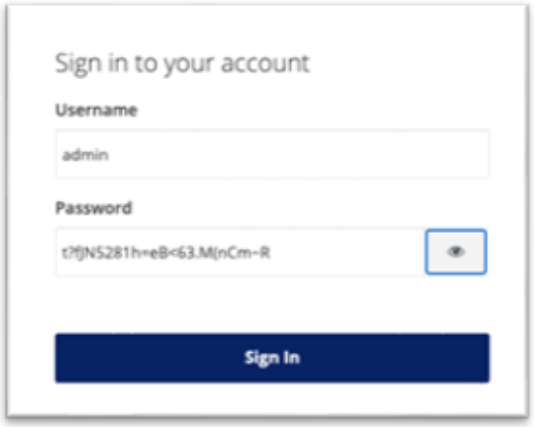
MLHub

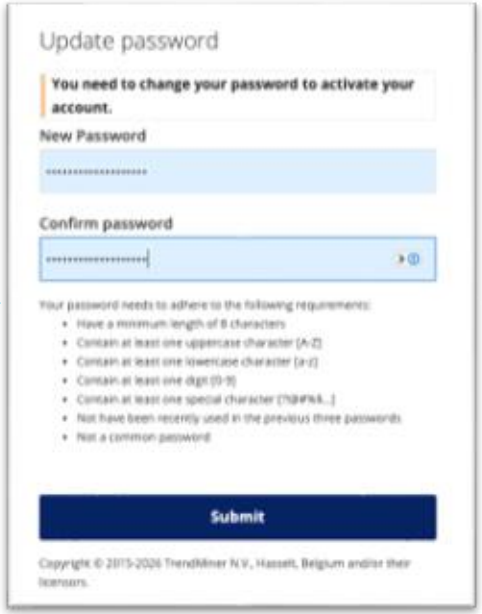
Lost Access to ConfigHub?

Resetting the ‘admin’ password 2FA from Edge Manager





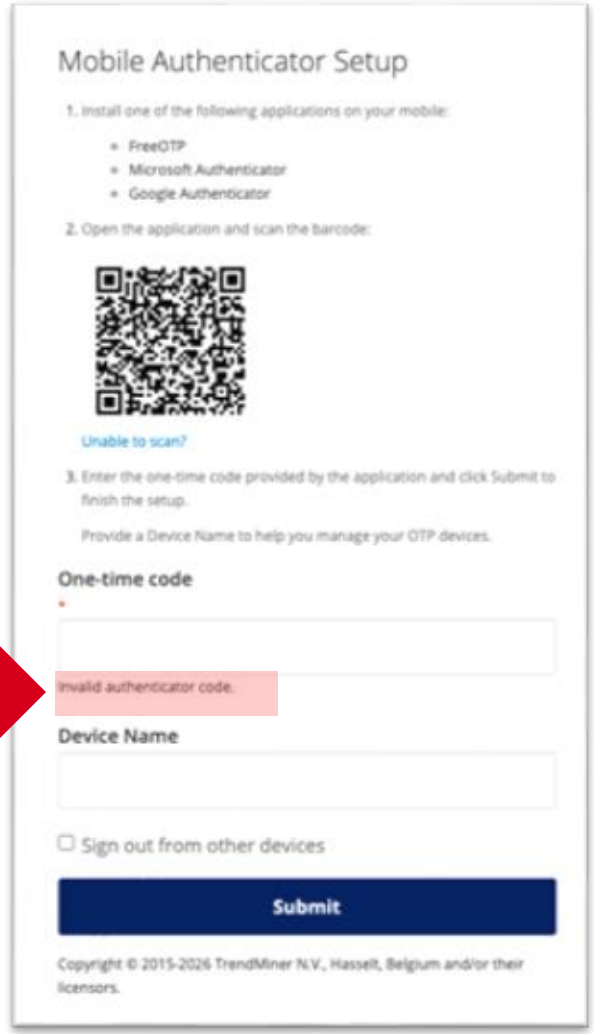




TrendMiner

ConfigHub Recovery — Watch Out For These

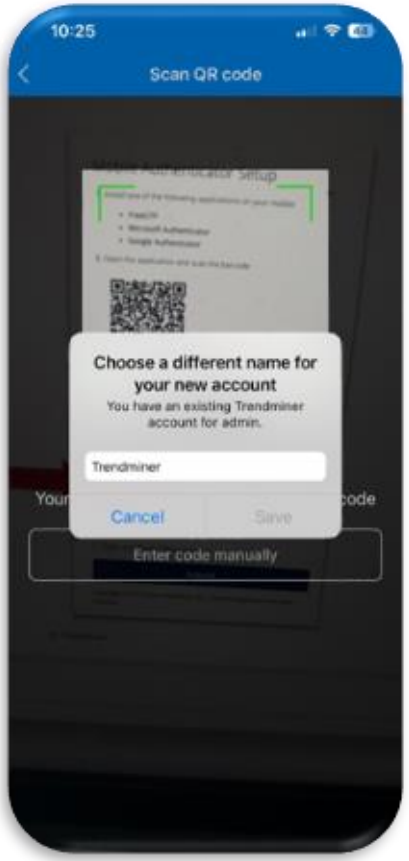
Common pitfalls during 2FA setup



- 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



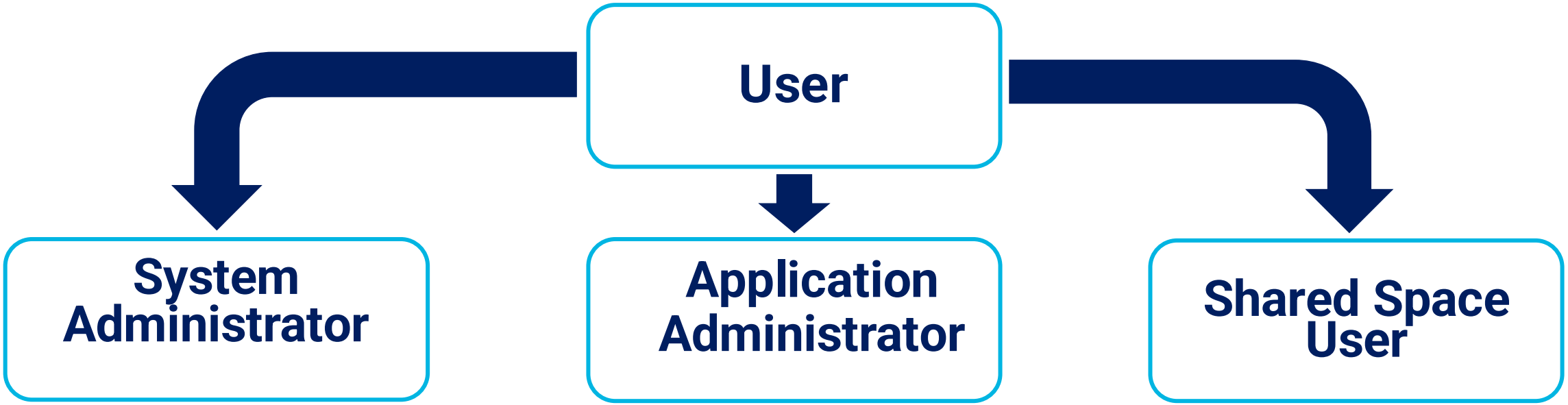
TrendMiner

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?

DATASOURCE
Historian/time series data

TIMESERIES_BUILDER
Notebooks,
Custom Calculations

Entity
Which specific resource?

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

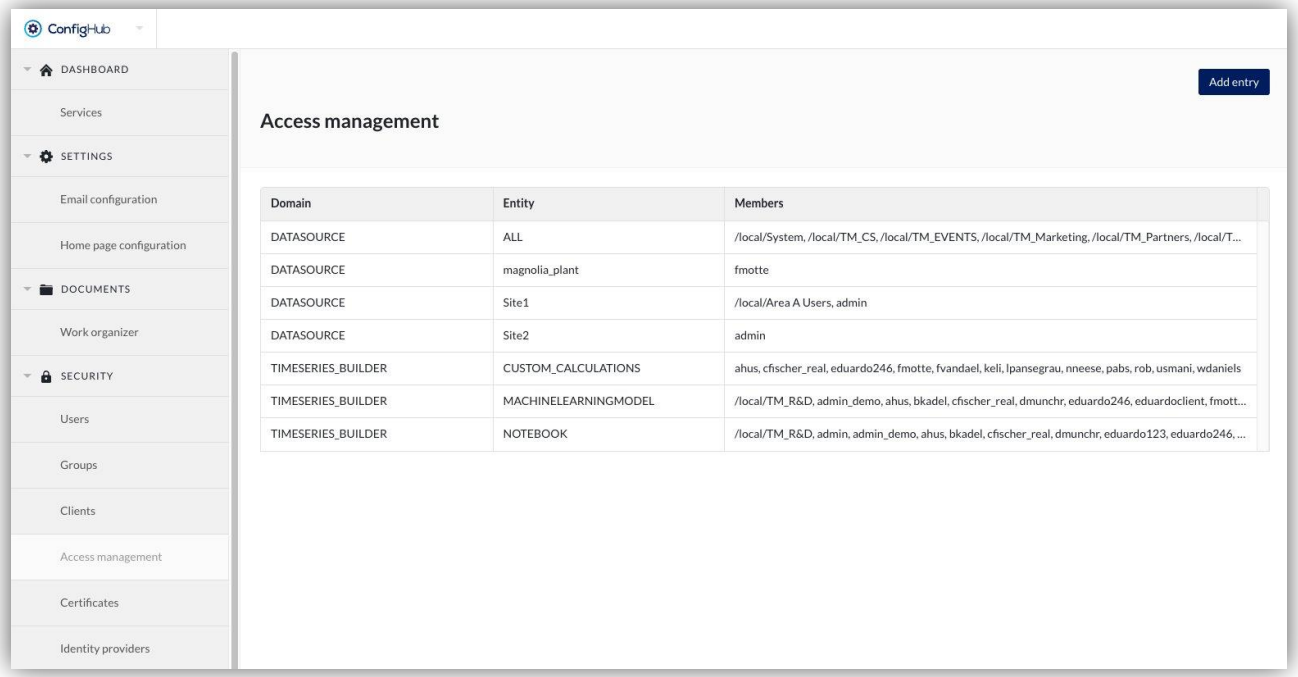
CUSTOM_CALCULATIONS :
Access to custom calculations in the tag builder

Members
Who gets the permission?

User
An individual user account

Group
Either local or groups synced from external IDP

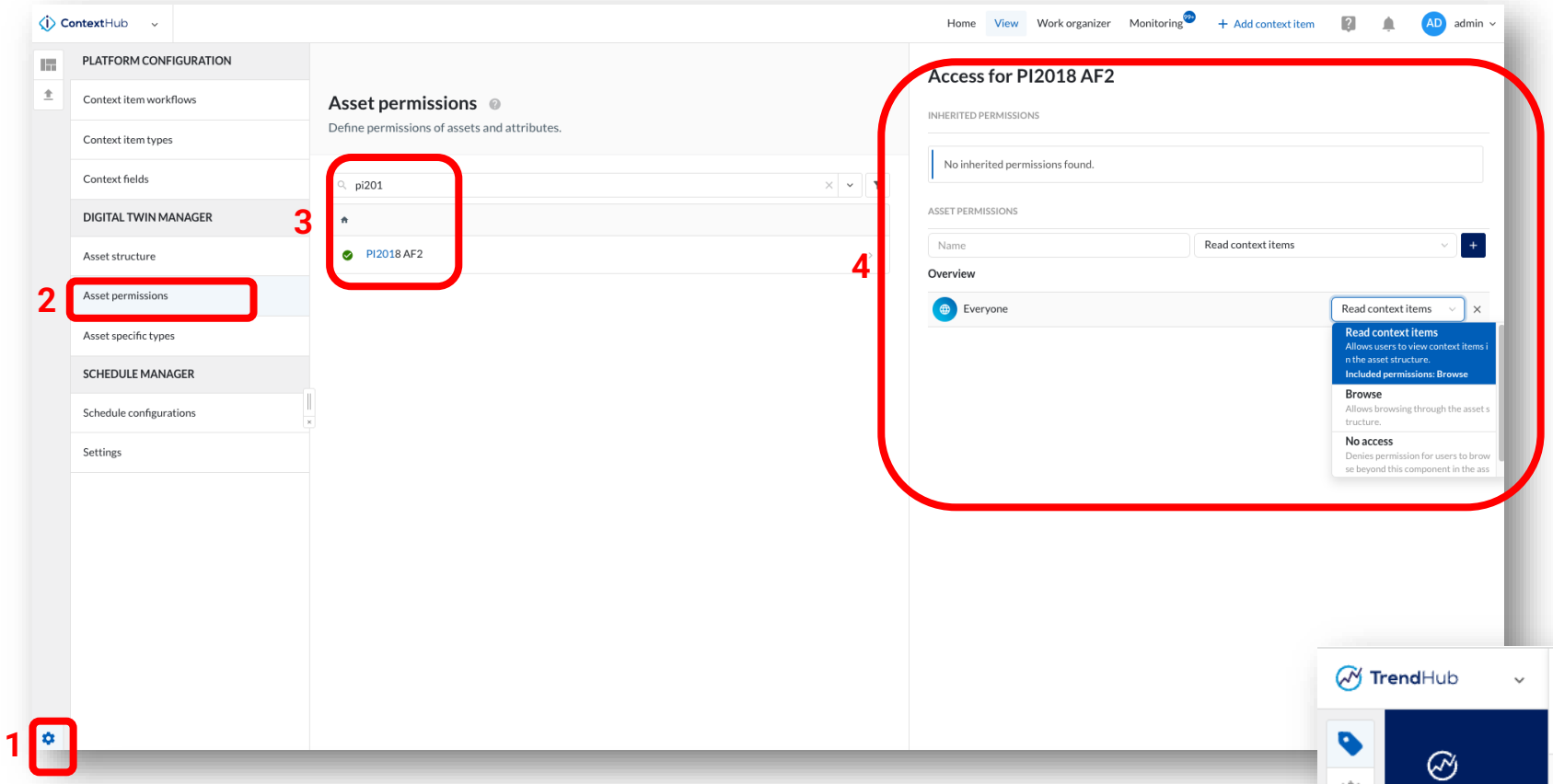
Client
A client ID for API or external system integration



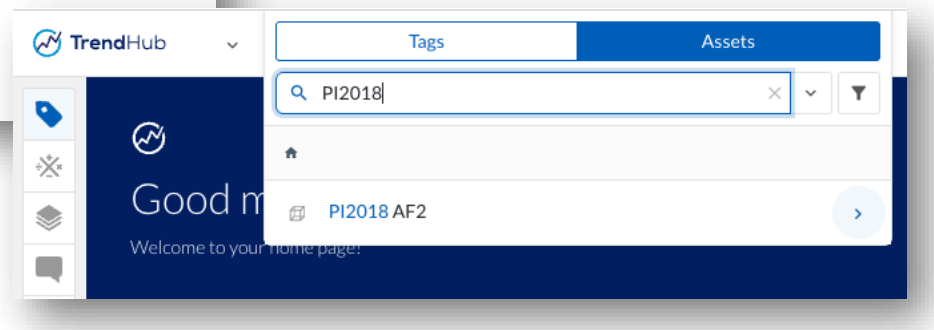
! Permissions on assets and context data are managed in ContextHub, not in ConfigHub (yet)!

Asset Permissions

Managing Asset Permissions via ContextHub



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

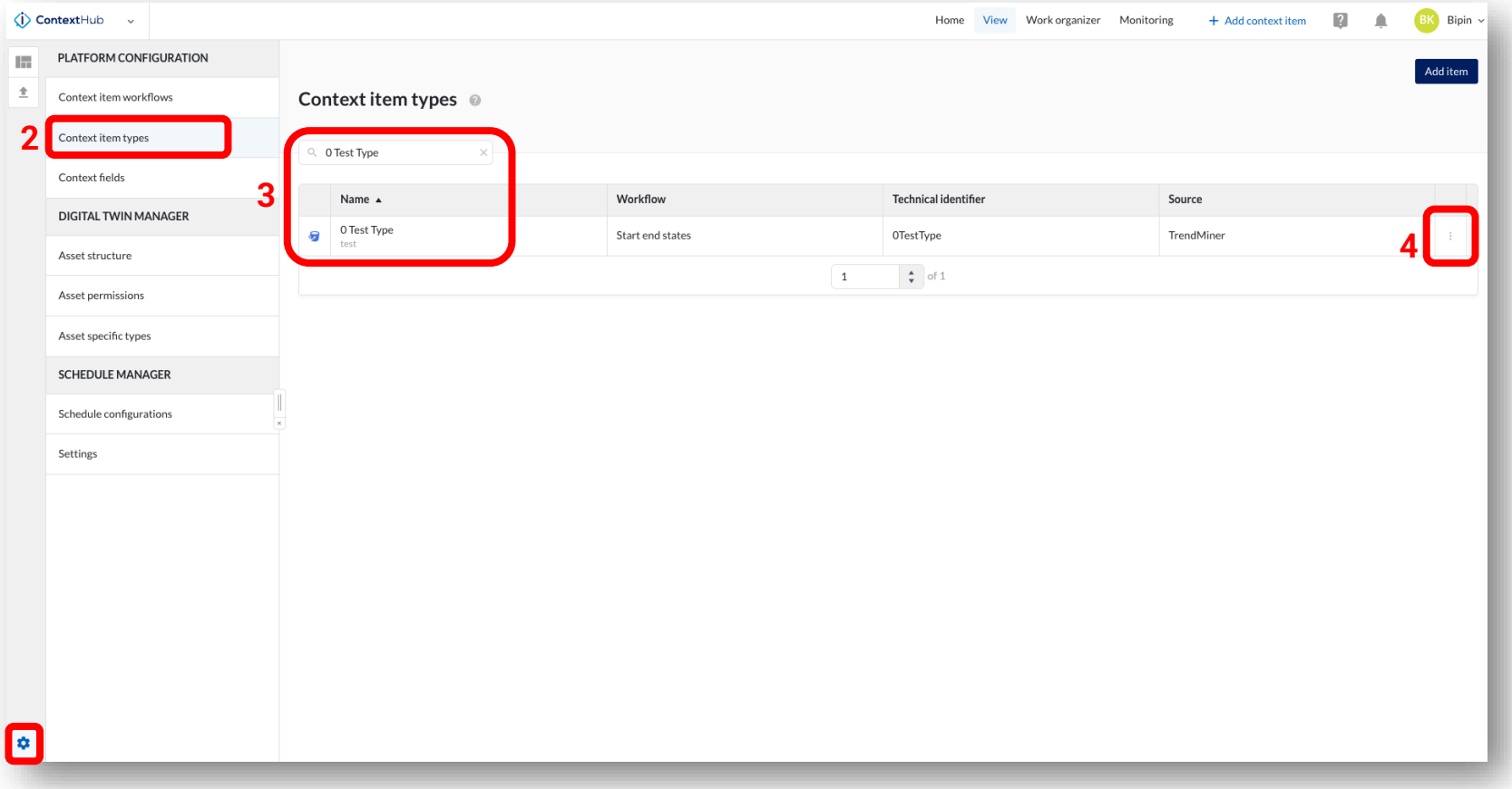


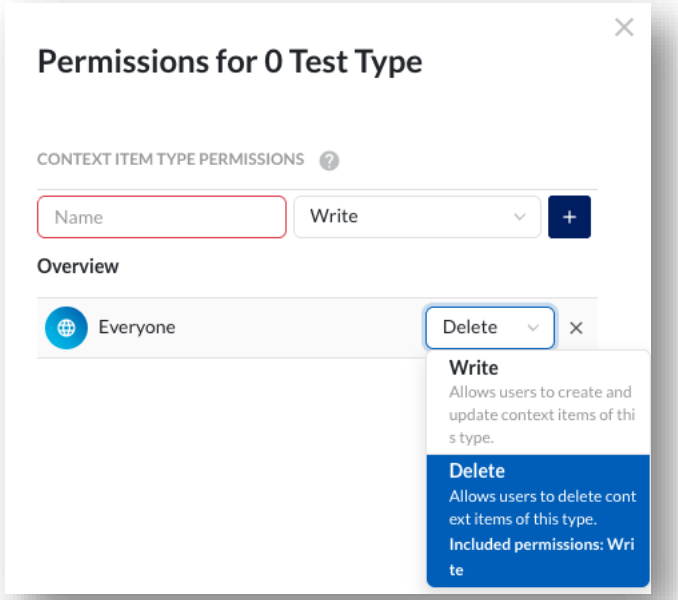
User browsing an Asset tree in TrendHub

TrendMiner

Context Items Permissions

Managing Context item type permissions via ContextHub





- Assign ‘Write’ or ‘Delete’ permission type to the selected users or Everyone
- Group assignment is not supported

TrendMiner

ConfigHub miscellaneous

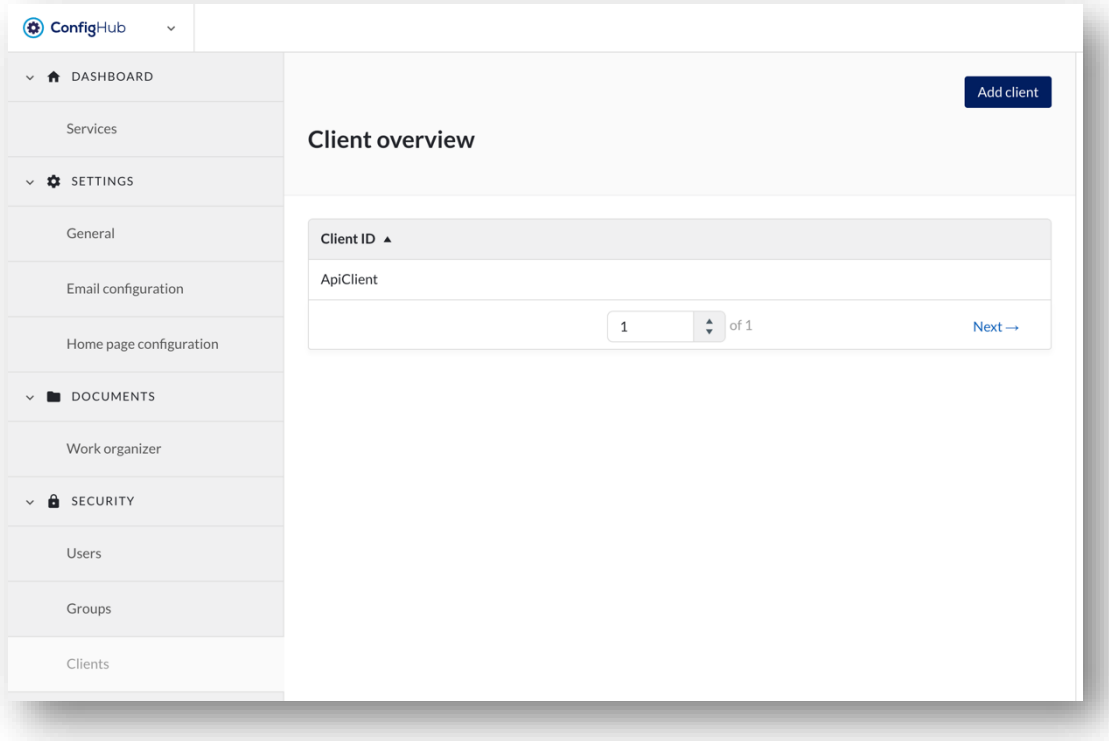
API clients, system notification group, lockout & recovery

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

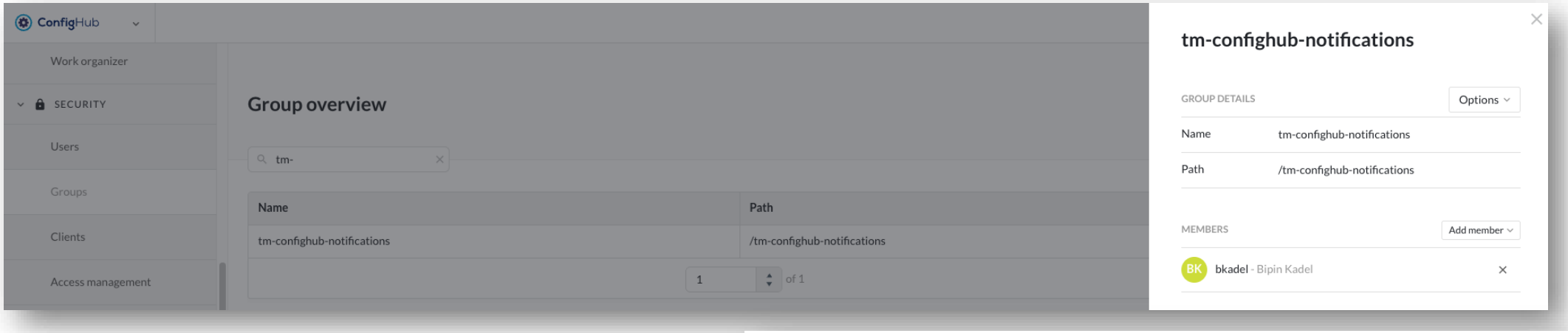
- Only System Admins can create and manage clients
- Regenerating the secret will immediately break any integration using the old one
- Don’t forget to add client to Access Management — without it the integration authenticates but gets no data



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



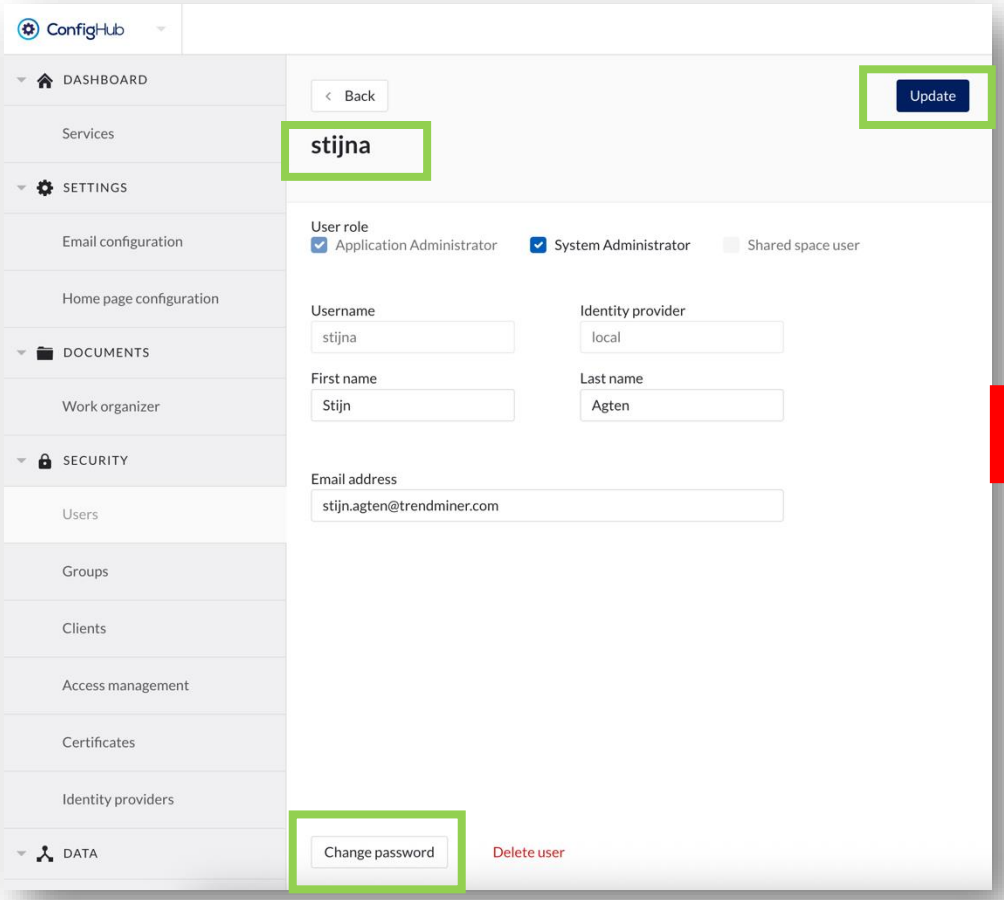
Notifications includes

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

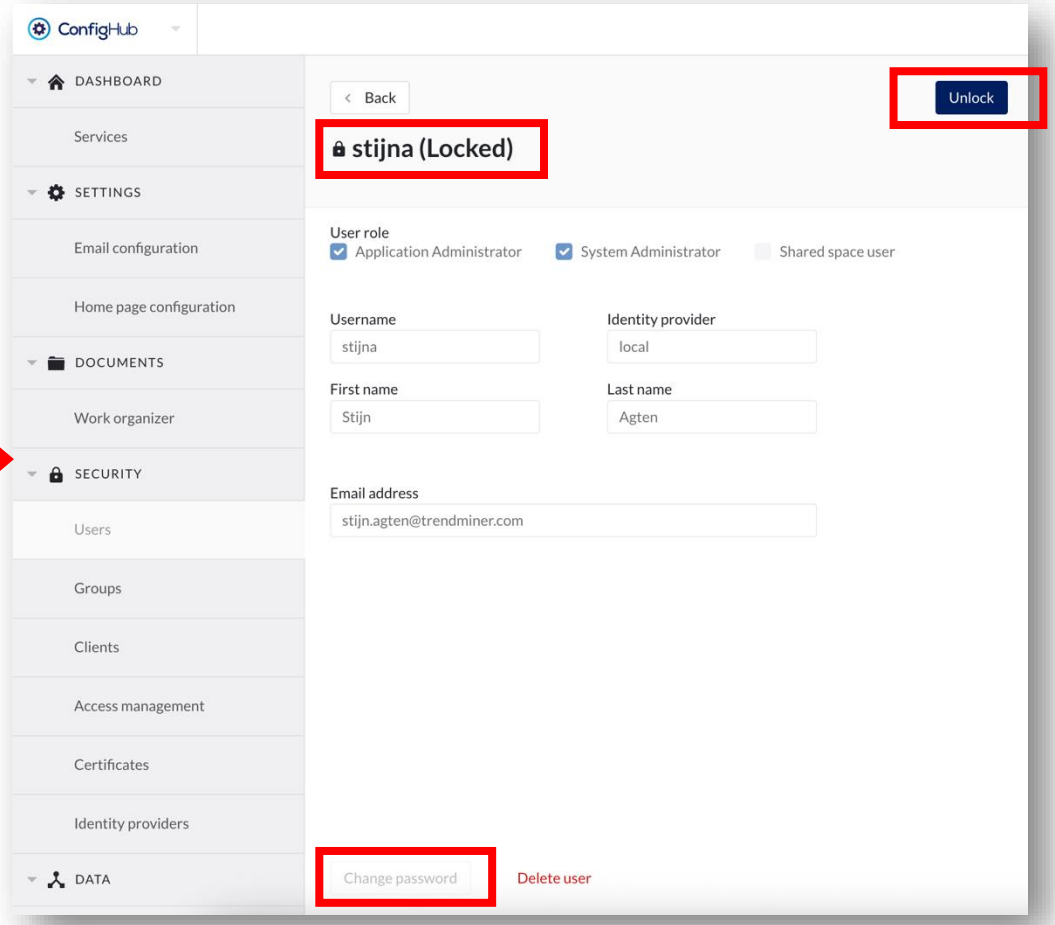
TrendMiner

Account Lockout in ConfigHub

3 failed attempts, one unlock button



3 failed login attempts



TrendMiner

Identity providers

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

Identity Providers

Understanding your options before choosing

Local

- Username/password login
- No integration
- Users & Groups managed in TrendMiner
- No 2FA
- Users can be soft-deleted

LDAP

- 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

SAML

Best choice

- 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

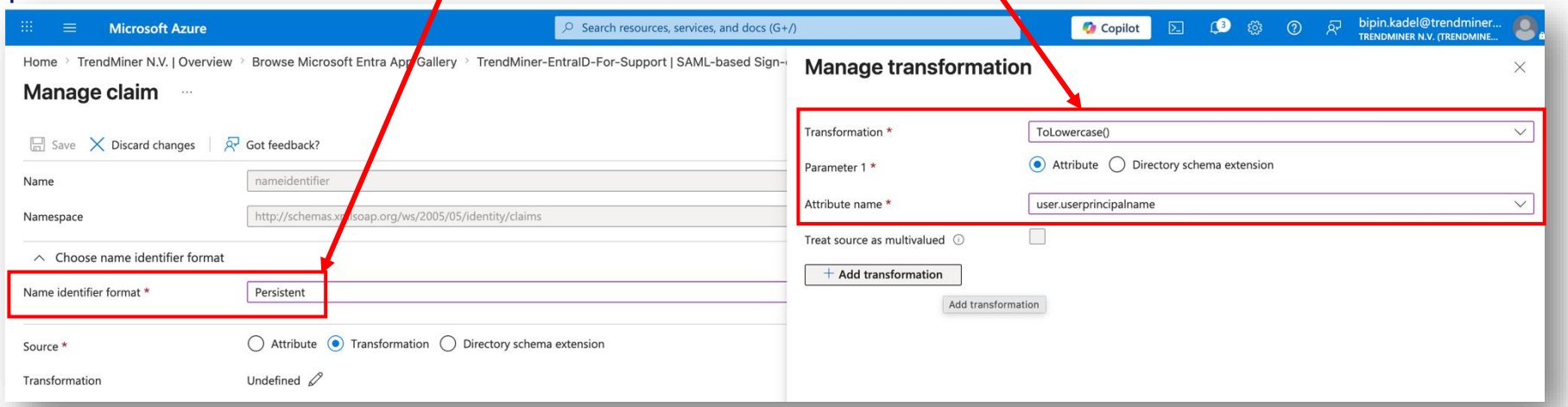
TrendMiner

SAML / SSO

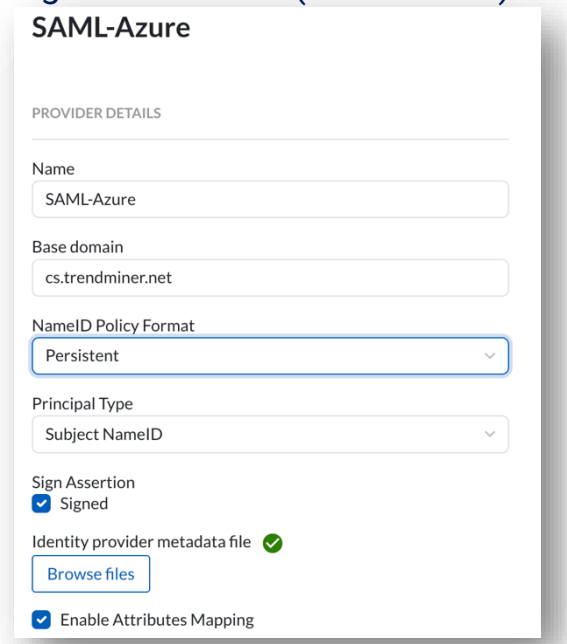
Best Practices

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



Configuration on SP (TrendMiner) side

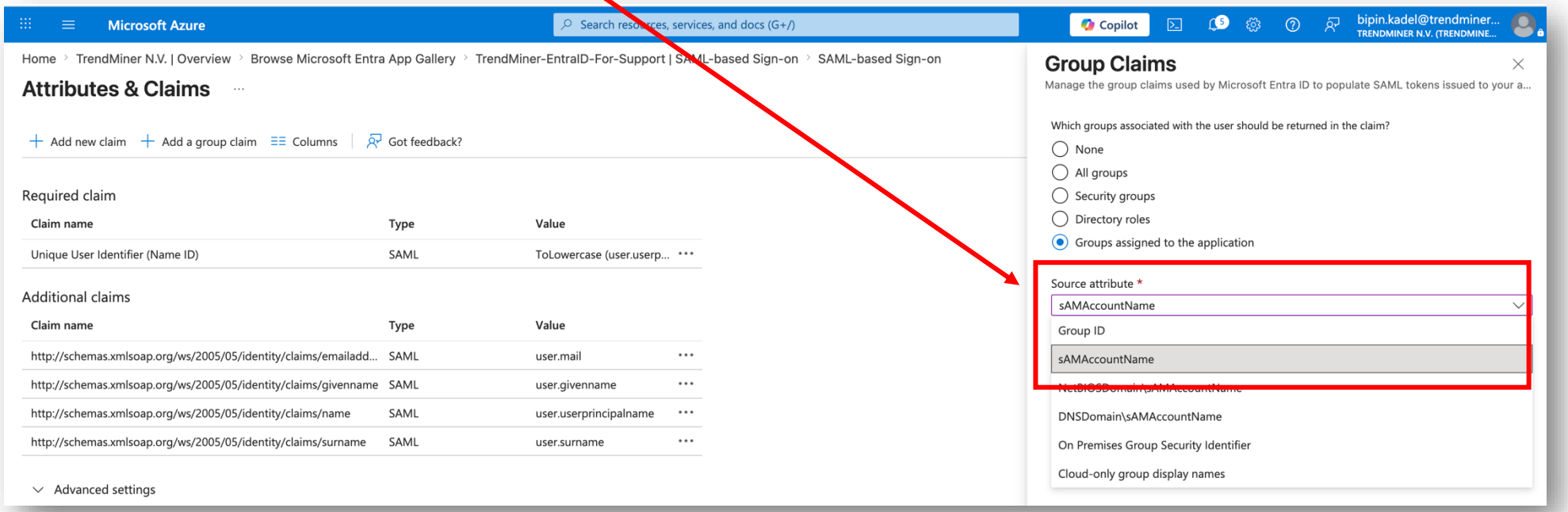


TrendMiner

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



Caution

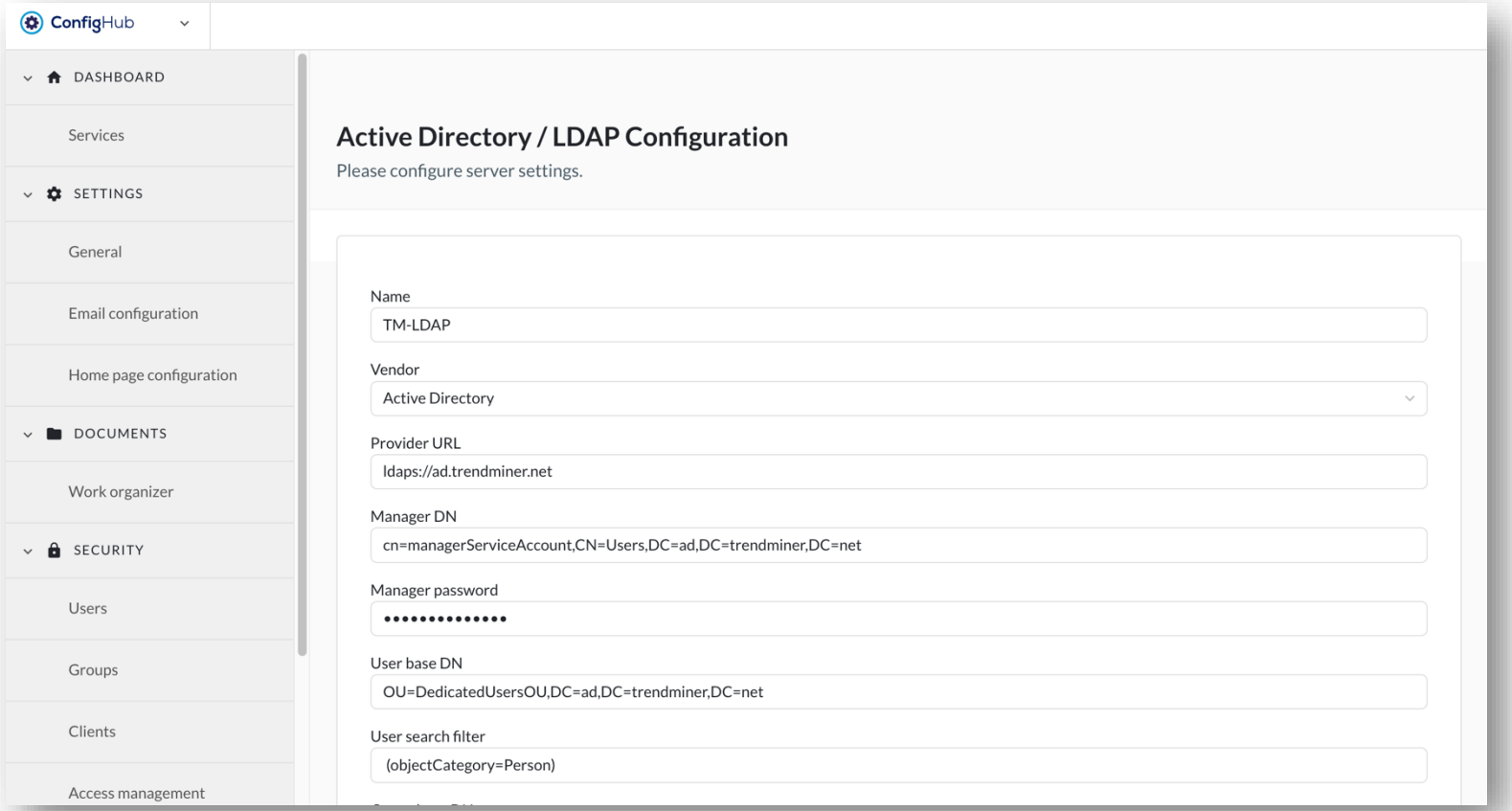
By default, the Group ID will be selected as Source Attribute. This corresponds to the Object ID of the Azure AD group, typically a 37-character string in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. The group will be identified in Confighub as this long identifier as well, so for human readability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

TrendMiner

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
Directory structure	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
	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



TrendMiner

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?