Cyxtera™

Controller Administration

Authenticating and authorizing admins

AppGateSDP

Access, evolved.

Cyxtera proprietary

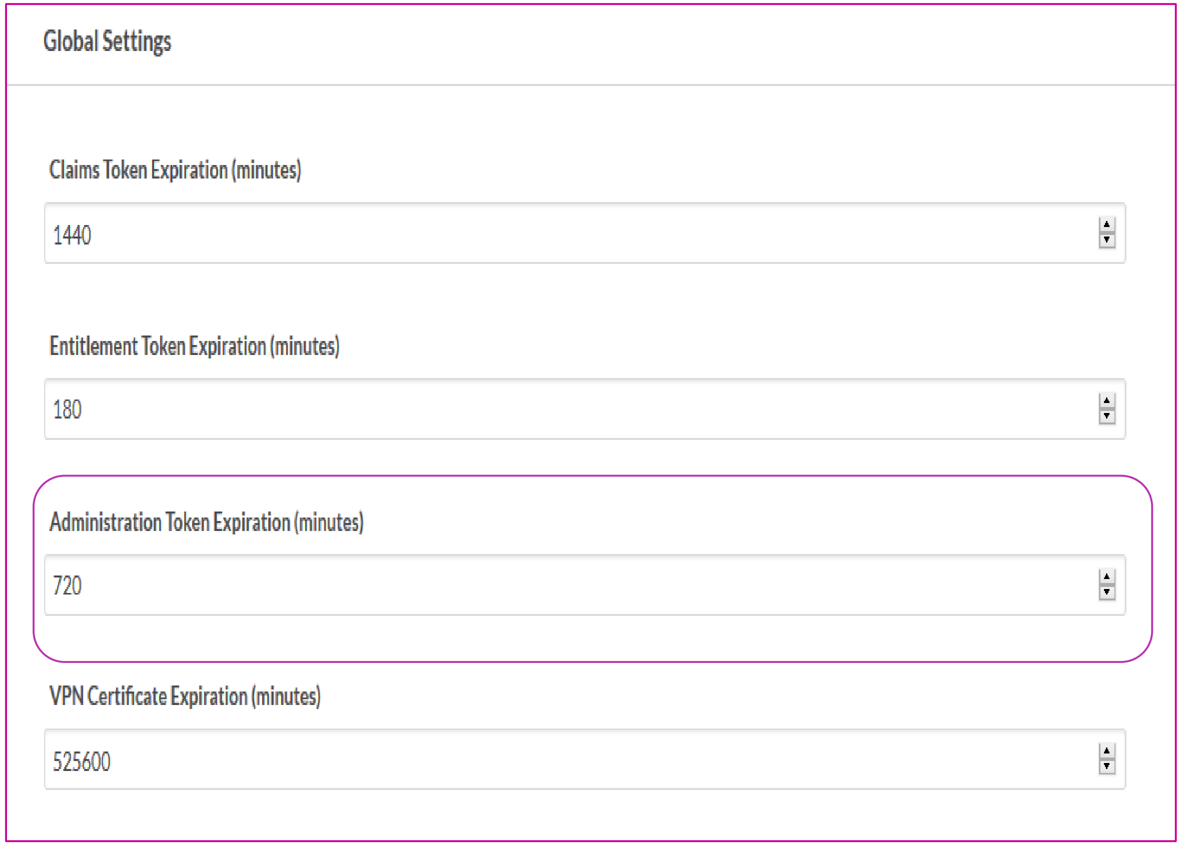
Configuring admin users

- The same philosophy as for user access is applied:
  - Identity providers are the same: LDAP, RADIUS,SAML or local database
  - Like user Entitlements, Admin Roles need to be assigned to a Policy
  - The Policy Assignment Criteria perform similar checks (is member of group, etc.)
  - Two factor authentication can be mandated
- The biggest differences are:
  - Authentication
    - Admins are logging into a normal web app (admin UI) not the client
  - Two factor authentication
    - Done **'up front'** not as a Remedy Action

Setting admin login parameters

Like normal users in the system administrators will receive a token

- Token is a cookie defining their rights
- Token lifetime can be set…
- Default is 12 hours



Global Settings

Claims Token Expiration (minutes)

1440

Entitlement Token Expiration (minutes)

180

Administration Token Expiration (minutes)

720

VPN Certificate Expiration (minutes)

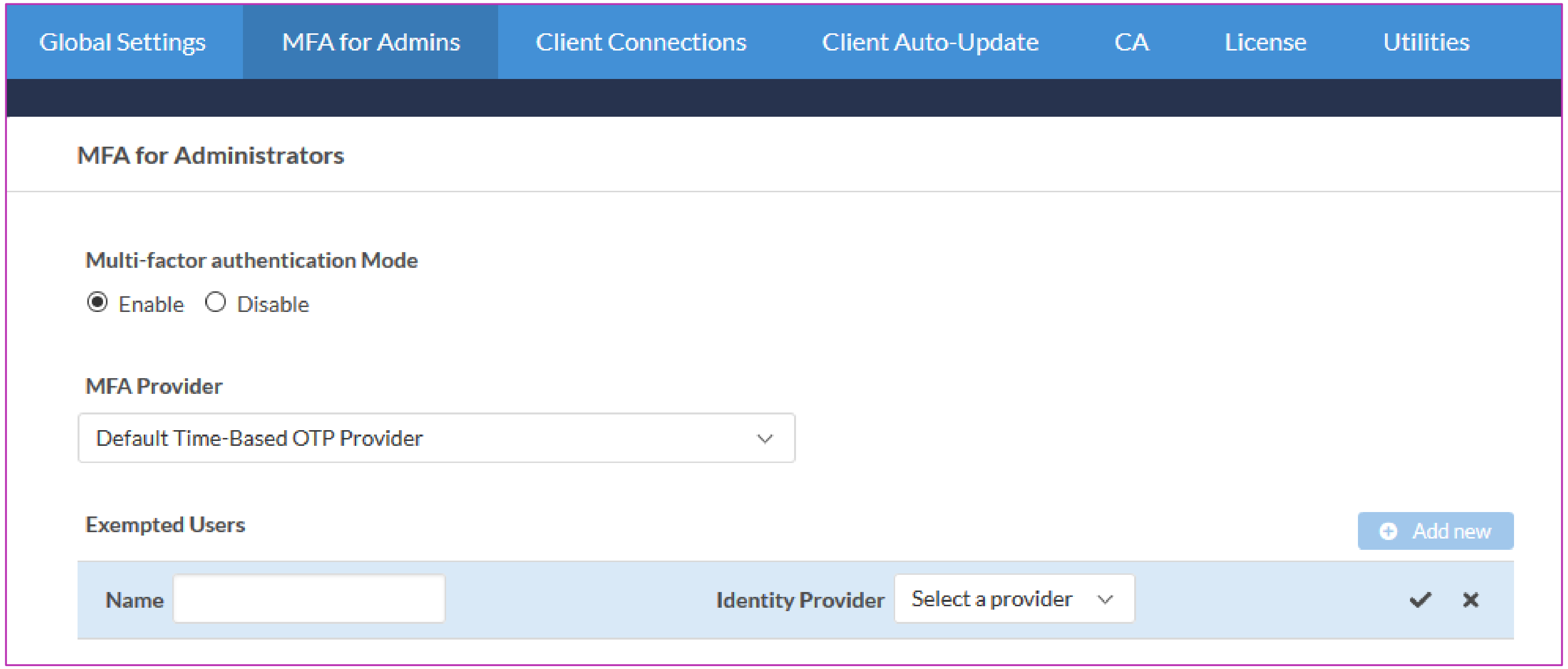
525600

MFA for Admins

AppGateSDP
Access, evolved.

Setting MFA for admin

- It is also possible to force administrators to use two-factor authentication
  - Same MFA providers available
  - MFA done at login time
- And specific users can be exempted
  - These would normally include the credentials used by external API users



MFA for Administrators

Multi-factor authentication Mode

● Enable ○ Disable

MFA Provider

Default Time-Based OTP Provider

Exempted Users

Name		Identity Provider	Select a provider	✓ ✕

Cyxtera™

Admin privilege system

AppGateSDP

Access, evolved.

Admin Privilege System

- Works based on list of Privilege -> Target [Scope]
- Privilege and Targets are predefined (picklist)
- Scope is admin defined (depends on the system configuration)

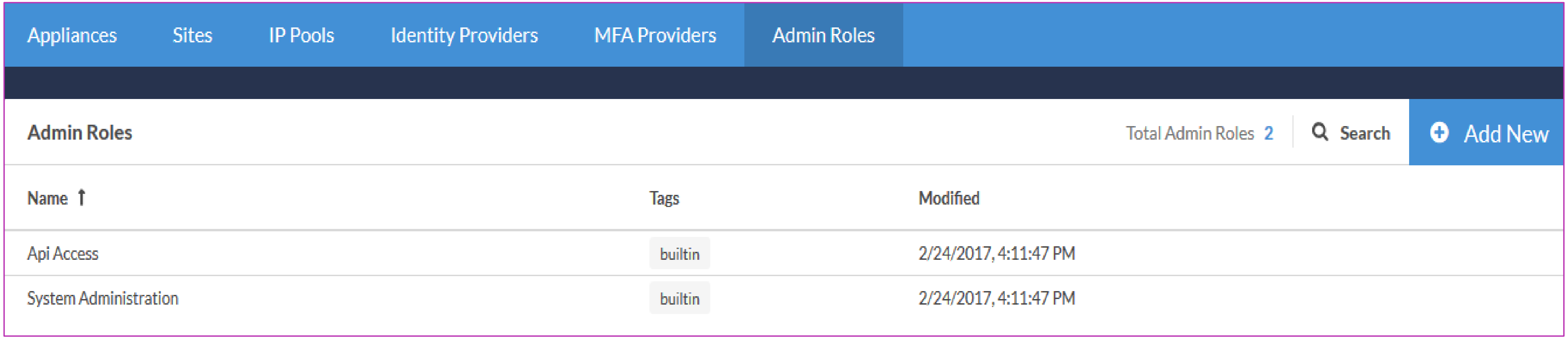
Admin privilege system

Examples….

Privilege	Target	Scope
View	Policy	All Items or Tag or ID
View	AuditLogs	None
Create	Policy	with ‘Default tags’
Revoke	Token	None

Admin Privilege System

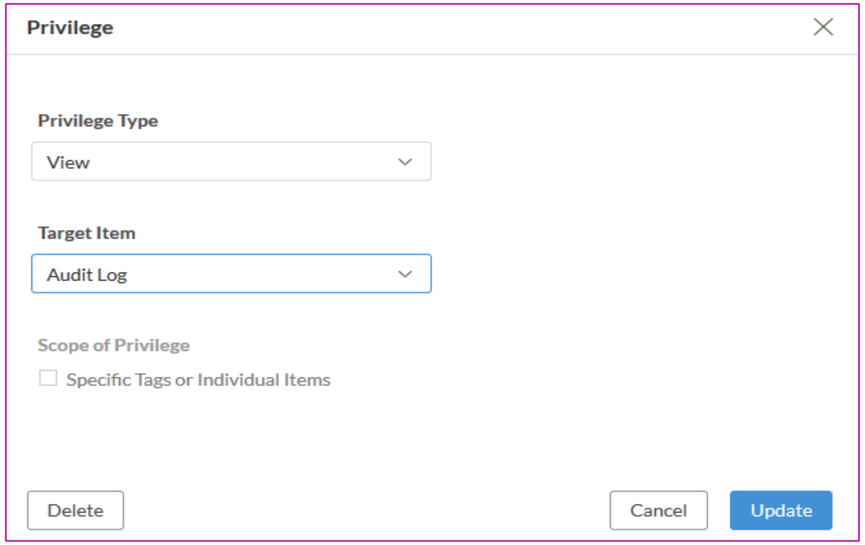
- There are two built in Admin Roles
  - API Access: gives rights to the system objects that relate to provisioning access
  - System Administration: gives full access



Name ↑	Tags	Modified
Api Access	builtin	2/24/2017, 4:11:47 PM
System Administration	builtin	2/24/2017, 4:11:47 PM

Admin privilege system

- You can create as many new Admin Roles as required
- Multiple privileges can be assigned
- In this example Admin can view:
  - Audit logs



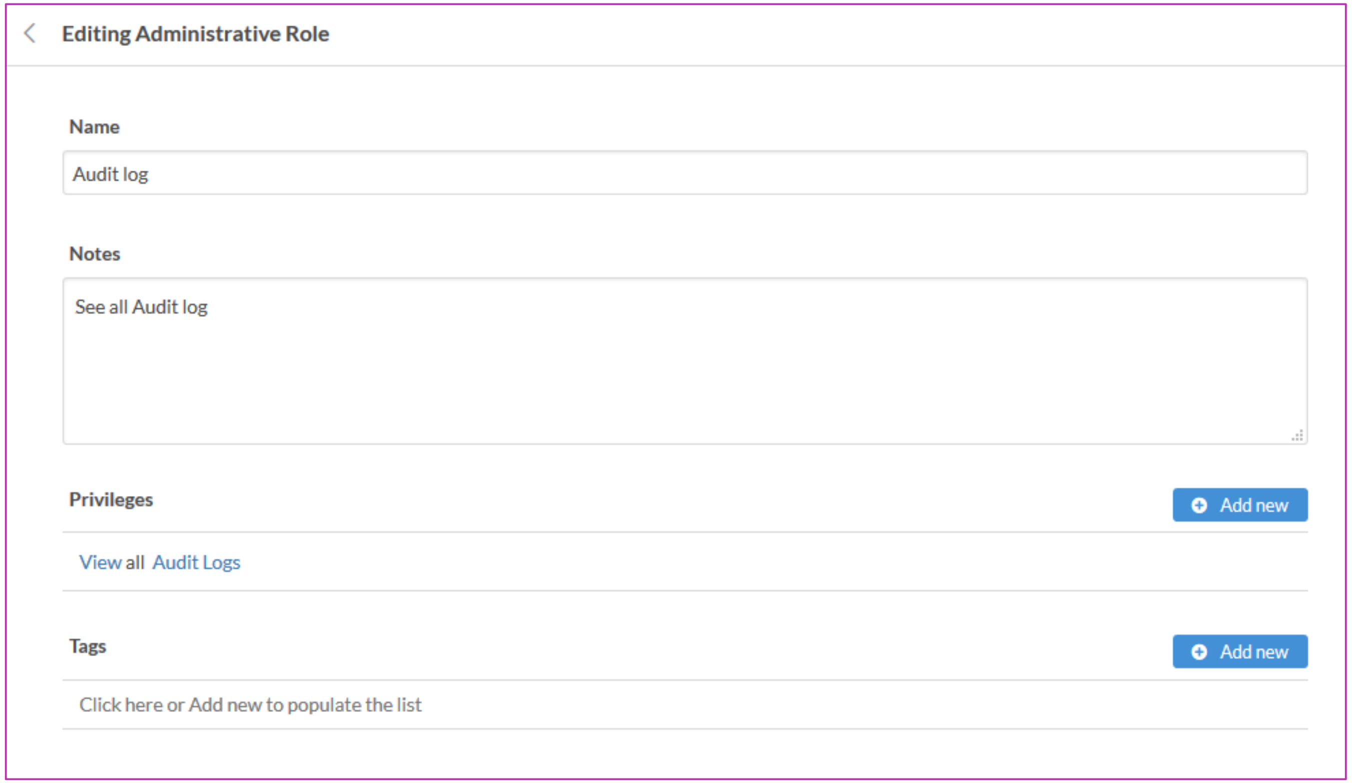
Privilege

Privilege Type: View

Target Item: Audit Log

Scope of Privilege

□ Specific Tags or Individual Items



Editing Administrative Role

Name: Audit log

Notes: See all Audit log

Privileges

View all Audit Logs

Tags

Click here or Add new to populate the list

What you have learnt

- You can configure admin users like normal users
- You can add MFA
  - But Admins have to enter this up front (web interface)
  - You can exclude specific users from MFA for API access
- You can then set up admin rights based on:
  - Privilege
  - Target
  - [Scope]

Lab 7. Configuring Admin access

- Lab 8
- Lab 9

Controller Admin

The end

AppGateSDP

Access, evolved.

Cyxtera proprietary