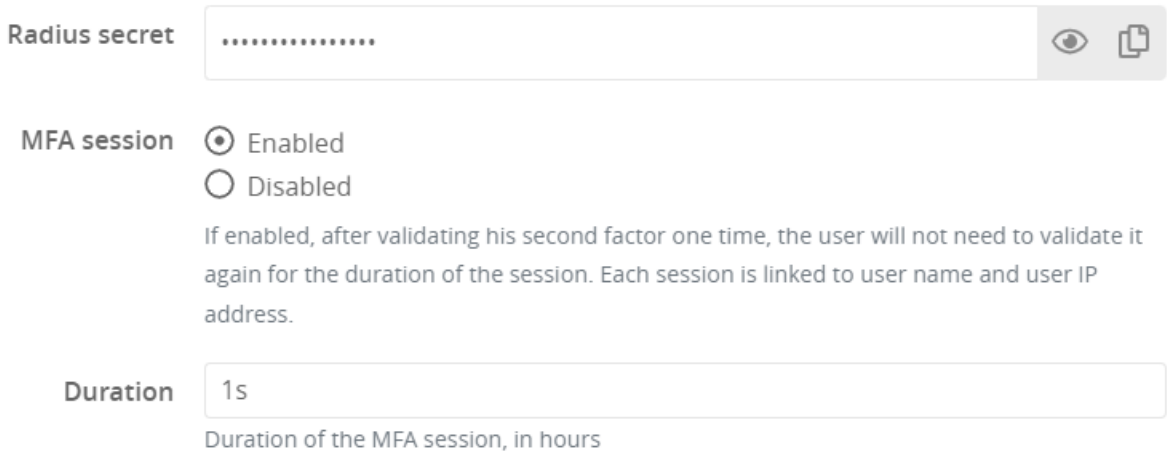
New features

Contents

- Non-systematic MFA when accessing targets through the Bastion
- Trustelem custom admin console

Non-systematic MFA when accessing targets through the Bastion

The feature concerns exclusively the WALLIX Authenticator offer since it is a feature intended for MFA via Radius on the Bastion.
Customers don’t want to authenticate through MFA each time they want access to a target, but Radius doesn’t allow this behavior.
Fortunately, thanks to Trustelem it is possible to bypass this limitation.
Now, on a Trustelem Bastion application, when you activate Radius, you can also activate an MFA session



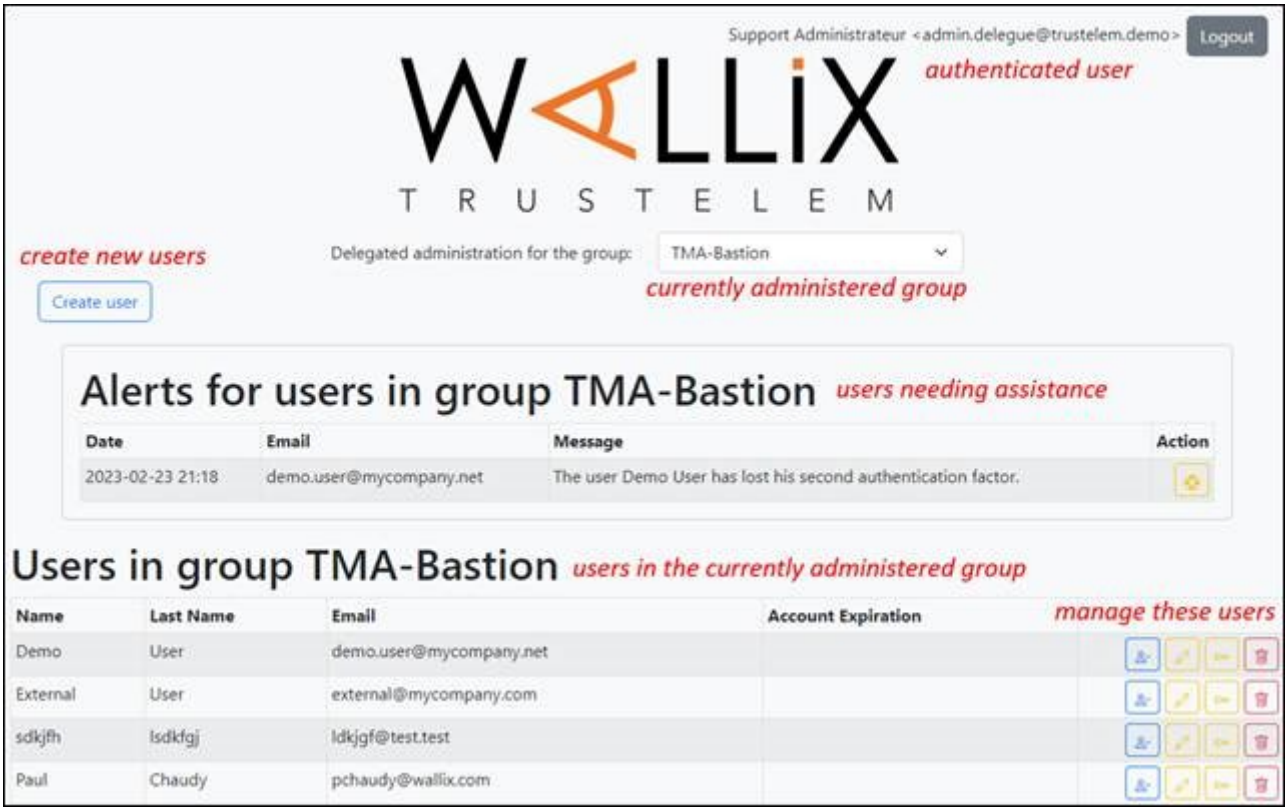
What is this for?
If a user authenticates with Radius on the Bastion linked to this application, then for the duration defined on Trustelem and as long as he remains on the same network, he will not be asked to provide his 2nd factor again.

For example, a user authenticates on the Bastion GUI and enters his login / password then his 2nd factor. 1 hour later he authenticates to the Bastion via SSH, and he won't have to enter the 2nd factor again. The only setting which has to be done on the Bastion side, is to activate the "Use

mobile device for Two-Factor Authentication (2FA)" option for Radius authentication.

Trustelem custom admin console

It concerns both WALLIX Trustelem and WALLIX Authenticator.
The delegated admin was created to respond to a simple observation: all Trustelem administrators have full control over the subscription, there is no possibility of limiting their admin entitlements. Still, each customer has different needs with regards to admin entitlements, according to the way they manage users, applications and other Trustelem objects: some of them want delegated admin rights for managing groups, others for managing authorizations or accessing logs of a subset of applications... Thus, we have implemented an application framework for creating custom admin consoles. Technically, it is a web GUI which formats/displays the result of Trustelem API calls. As a result, we can offer almost any administration function (create users, reset passwords, display logs, etc.) and give access only to selected users.
Using this framework, an admin console for managing authorization of users to applications through groups membership has been developed then adapted for different clients and prospects.



Example of real use case:
A customer configures access to the Bastion for its internal users via Active Directory + Trustelem Radius authentication.
Problem: he wants his external provider to use Access Manager but doesn't want to spend time in the administration of this population on Active Directory or locally on the Bastion.
To his point of view, the external provider should be responsible of his users management.
The customer creates on Trustelem a group linked with the Bastion (with LDAP, for the targets access) and the Access Manager (with SAML, for the authentications). Then he activates automatic

MFA enrolment for this group.
After that, he gives the administration of this group through a Delegated Admin tool (like the one in the screenshot above) to the external provider, with a 10 account creations limitation to prevent license abuse. The final result is that the external provider can create a limited number of accounts via the Delegated Admin and these users will have direct access to the Access Manager, with MFA and with the right authorizations to targets.

Delegated admin documentation

Many other usecases can be addressed with specific development: a SoW is to be issued.

Revision #3
Created 23 March 2023 13:44:26 by WALLIX Admin
Updated 25 October 2023 10:02:16 by WALLIX Admin