Trustelem news

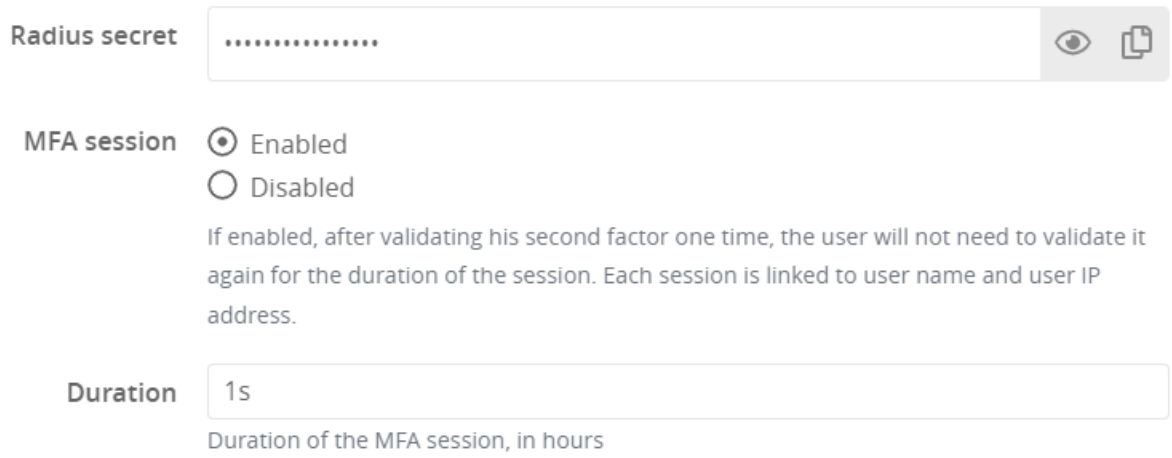
- New features
- Incidents
- Unavailability

New features

Contents

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

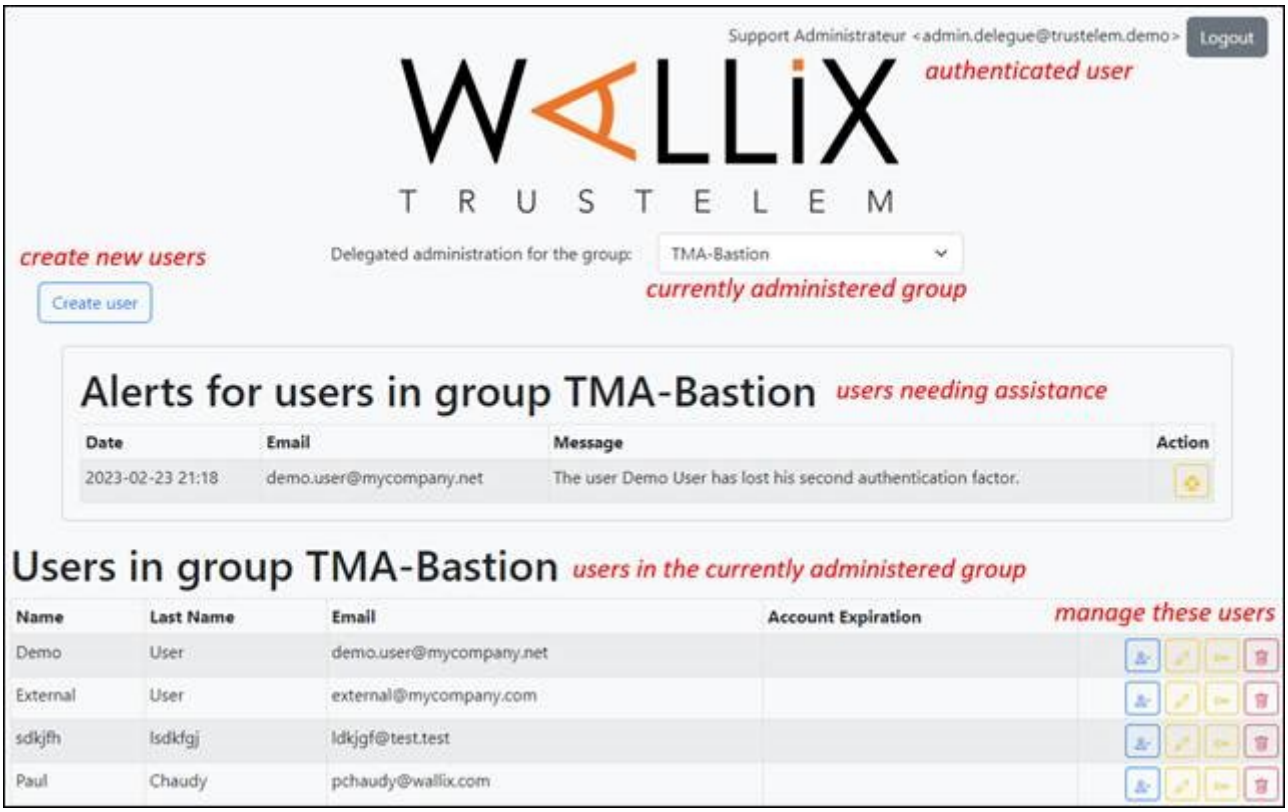


What is this for?
If a user authenticates with Radius on the Bastion linked to this application, then for the duration defined on Trustelem and as long as he remains on the same network, he will not be asked to provide his 2nd factor again.

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.

Incidents

2024/02/20

Incident window: 4:24 p.m. -> 4:37 p.m.
Cause: internal maintainance error at our hosting provider
Impacts: Trustelem service unavailable

- A configuration change by our hosting provider made the Trustelem service unavailable, the hosting provider is currently investigating

2024/02/19

Incident window: 5:12 p.m. -> 5:27 p.m. 6:19 p.m. -> 6:20 p.m.
Cause: internal maintainance error at our hosting provider
Impacts: Trustelem service unavailable

- A configuration change by our hosting provider made the Trustelem service unavailable

2023/09/29

Incident window: 02:39 p.m. -> 03:03 p.m.
Cause: internal maintainance error at our hosting provider
Impacts:

- A configuration change by our hosting provider to remove an internal server used for a datacenter migration caused a routing error, rendering our site unreachable. Our monitoring detected the situation immediately and the configuration change was reverted immediately

2023/09/20

Incident window: 10:20 a.m. -> 10:27 a.m.
Cause: internal maintainance operation at our hosting provider
Impacts:

- Due to a network configuration change on our reverse proxies (mandatory for a maintainance operation), the Trustelem service was unavailable for a few minutes

2023/07/17

Incident window: 10:41 a.m. -> 02:17 p.m.
Cause: a preliminary analysis seems to point out an issue with the nginx configuration - handled by our hosting provider - due to an exhaustion of the number of worker connections
Impacts:

- Degraded service with internal errors (HTTP error 500).

Handling the incident: after identifying the cause, we restarted the service to dicrease the used workers. A point will be made asap with our hosting provider to see how this limitation can be removed.

2023/05/09

Incident window: 00:00 a.m. -> 02:30 p.m.
Cause: IOS push certificate was expired.
Impacts:

- Authentication through push notifications on IOS was not working

Handling the incident: after identifying the cause, the certificate was renewed, fixing the problem.

2023/05/02

Incident window: 10:17 a.m. -> 10:30 a.m.
Cause: files descriptors exhaustion issue.
Impacts:

- Partial internal error failures on login pages

Handling the incident: our primary production server encountered a files descriptors exhaustion issue causing partial failures on connexions. Those failures were detected immediately by our monitoring and a restart of the service instantly solved the instability. Our watchdog process properly detected the issue but was not designed to provide enough detailed information on the file descriptor usage on our system, therefore we are working on improving our monitoring tools to be able to identify the root cause of any future similar issue.

2023/03/21

Incident window: 11:47 a.m. -> 1:00 p.m.
Cause: malfunction of the production HTTP outbound proxy, following a configuration problem at our hosting service provider during a migration. Our hosting service provider went back on the configuration.
Impacts:

- MFA authentication by WALLIX Authenticator (push notification) impossible
- MFA authentication via SMS not possible
- authentications with Azure AD impossible

Handling the incident: the problem was detected within a few minutes and dealt with our hosting service provider as quickly as possible at our host

Unavailability

2023 (SLA: 99.94%)

Programmed maintenance: 50 min (datacenter migration)
Incidents:

- 2023-09-29: 24 min of unavailable service
- 2023-09-20: 7 min of unavailable service (network error)
- 2023-07-17: 216 min of degraded service
- 2023-05-02: 13 min of degraded service
- 2023-03-21: 77 min of degraded service

2022 (SLA > 99.99%)

Programmed maintenance: 0 min
Incidents: 20 min of degraded service

2021 (SLA > 99.99%)

Programmed maintenance: 0 min
Incidents: < 1 min

2020 (SLA > 99.99%)

Programmed maintenance: 0 min
Incidents: < 1 min

2019 (SLA > 99.99%)

Programmed maintenance: 0 min
Incidents: < 1 min

2018 (SLA > 99.99%)

Programmed maintenance: 24 min
Incidents: < 1 min

2017 (SLA > 99.99%)

Programmed maintenance: 58 min
Incidents: < 1 min

2016 (SLA > 99.99%)

Programmed maintenance: 68 min
Incidents: < 1 min

2015 (SLA = 99.98%)

Programmed maintenance: 120 min
Incidents: 124 min