Access rules

Contents

What access rules are?

- Permissions help define how users can access which apps.
- They can ask for simple authentications (login + password), multi factors authentications (login + password + 2nd factor) or deny an access
- They can be managed using the tab **Access rules** of Trustelem admin page.
- They can be managed using the API
- They are some default access rules defined on **Security settings** / **General** / **Default authentication level for users** which allow to control multiple applications access rules with one setting.
- For web authentication, you can have a rule depending on the user public IP. If the IP is known the rule **internal** applies, if not the rule **external** applies.

If possible, an access rule should always apply to a group.
Doing that you only have to add users to the right groups to manage the access.
It is also a way to have a limited number of access rules and a better visibility.
Of course you can still search for a user in the **Access rules** tab to see which permissions are applied, even if they are related to a group.

Priorities

When a user / group is affected by more than one access rule for a single application, the following priorities apply:

- 1/ A user access rule wins over a group access rule, whether it is more restrictive or not
- 2/ The most restrictive access rule wins

In summary:

Access forbidden (user) > 2 factors (user) > 1 factor (user) > Access forbidden (group) > 2 factors (group) > 1 factor (group)

Example

John Doe is in groups "Customer Success" and "Support" and he wants to authenticate on salesforce.

Permissions defined:

- Subscription default: internal -> 1 factor | external -> 2 factors
- Customer Success for salesforce: internal -> 1 factor | external -> 2 factors
- Support for salesforce: internal -> 2 factors | external -> forbidden
- John Doe for salesforce: internal -> no rule | external -> 2 factors

No permission is set to the **default** value, so this setting doesn't apply.
For **internal** zone we have 1 factor (customer success) and 2 factors (support) for groups and no rule specified for his account --> the authentication will use 2 factors
For external zone we have 2 factors (customer success) and forbidden (support) for groups and 2 factors for his account --> the authentication will use 2 factors again.

--> John needs 2 factors to access salesforce for both internal and external zone.

Web authentication - Apps SAML, OpendID Connect, and No SSO

Permissions for this apps may depend on the user's public IP address.
In this case, the internal IPs must be defined on **Security settings** / **General** / **Internal network**.
Internal IPs are usually the public IPs of the company offices.
If the user has a known public IP, the access rule for **internal zone** applies, if not the access rule for **external zone** applies

Possible values:

- **no rule**: does not apply any rule, so other permissions can remain active
  *For instance, if you want to overload an existing **external zone** permission, and not a **internal zone** permission, you can set the **internal zone** permission to **no rule***
- **Default**: apply the default rule defined in **Security settings** / **General** / **Default authentication level for users**
- **1 factor**: only one authentication factor is needed to access the application (login + password OR certificate OR Kerberos)
- **2 factors**: two authentication factors are needed to access the application
- **Forbidden**: the user can’t access the application

LDAP authentication

LDAP applications do not provide users public IP, so there are no **internal** and **external** permissions.
1 factor or 2 factors LDAP permissions allow the application to:

- source users --> **LDAP search**
- authenticate users with permission --> **LDAP bind**

If a user doesn't have a LDAP 1 or 2 factors permission, the application can't find him with a search request

Possible values:

- **no rule**: does not apply any rule, so users can't be sourced and can't be authenticated
- **1 factor**: users can be sourced, and only one authentication factor is needed to access the application
- **2 factors**: users can be sourced, and two authentication factors are needed to access the application. LDAP is not designed for MFA, so if you use this permission:
  - If the user provides login + password and have WALLIX Authenticator, Trustelem will only answer after the validation of a push notification (**only possible if the app have a timeout long enought)
  - If the user provides login + password and doesn't have WALLIX Authenticator, the authentication will failed
  - The user can provides his login + password and TOTP code sticked together (for instance: mypasswordTOTP)
- **Forbidden**: the user can’t access the application and can't be sourced

Radius authentication

Radius applications do not provide users public IP, so there are no **internal** and **external** permissions.

Possible values:

- **no rule**: does not apply any rule, so users can't be authenticated
- **Always allow**: accept the authentication if the login is known, without any verification on the password/2nd factor
  This permission is used in specific scenarios, when you defined a radius authentication in addition to another authentication (AD usually) and you want some users to authenticate using 2nd factors, and some users using only 1 factor.
- **2nd factor only**: only the second factor are needed to access the application. *This permission is used when you have a radius authentication in addition to another authentication (AD usually).*
- **2 factors**: two authentication factors are needed to access the application.
  If the application supports Radius in 2 steps (Access Request then Challenge request) you can provide login + password then MFA
  If the application doesn't support Radius in 2 steps, you can provide login + password and code sticked together

- **Forbidden**: the user can’t access the application

Revision #10
Created 1 July 2022 08:00:30 by WALLIX Admin
Updated 25 October 2023 08:33:57 by WALLIX Admin