Network zones

Network zones (currently optional)

Besides the internal and external zones, you can define your own **network zones**, for example a branch office, a partner's network or a list of countries, and give each one its own authentication level.

Defining zones

Zones are defined on **Security settings** / **General** / **Network zones** (up to 64 zones). Each zone has:

- **Name**: shown in the access rules
- **Matches on**:
  - **IP addresses**: one address, range or CIDR block per line
  - **Country**: one or more countries, found from the user's IP address
- **Default authentication level for users**: the level the zone applies when an access rule uses **Default** for it. **Same as external zone** uses the external zone's default level.
- **Authentication level for Trustelem admin console**: the level administrators need to sign in to the admin console from this zone

Which zone applies:

1. The **internal network** always wins: an address in the internal network is in the internal zone, even if a network zone also matches it
2. Otherwise the network zones are checked from top to bottom and **the first matching zone wins**: use the arrows to change their priority
3. If no zone matches, or the origin of the connection can't be determined, the **external** zone applies

You can't save a zone setting that would forbid your own access to the admin console from where you are connected.

Zone levels in access rules

Once a zone is defined, every access rule shows a line for it. **Possible values:**

- **Same as external zone**: the rule applies its **external** level to users coming from this zone. This is the value of every rule until you change it, so defining a zone changes nothing for existing rules.
- **Default**: applies the zone's **Default authentication level for users**
- **1 factor**: only one authentication factor needed
- **2 factors**: two authentication factors needed
- **Forbidden**: the user can't access the application from this zone

Example

Company offices are in the internal network. A "Partners" zone lists the salesforce access rule for the group "Sales" is: internal -> 1 factor | external -> 2 factors | Partners -> Forbidden.

- A salesperson at the office signs in with 1 factor
- The same salesperson on a partner's network can't access salesforce
- From anywhere else, 2 factors are needed

Renaming and deleting zones

- Renaming a zone or changing its addresses keeps the levels the access rules set for it
- Deleting a zone removes it from every access rule: users from its adds set for the zone they then fall into (usually external). Before saving, a warning tells you how many access rules set a level for the zone you are deleting.
- A new zone never takes over the levels set for a deleted zone, even with the same name

LDAP and Radius applications do not provide the user's IP, so zones do not apply to them.

Revision #4
Created 27 September 2026 20:05:44 by WALLIX Admin
Updated 29 September 2026 08:24:28 by WALLIX Admin