Integration with Active Directory

SafeUTM provides the possibility of one-way synchronization with a domain based on Microsoft Active Directory.

Only accounts are imported, excluding passwords. When the user undergoes the authorization procedure, verification is carried out by means of Active Directory.

> Integration with Windows Server 2008 (only R2), 2012, 2016, and 2019 is supported.

Features of Using Integration with Multiple Active Directory Domains

When integrating SafeUTM with multiple domains, the following limitations apply:

- From the Active Directory domain tree, only the data of the domain controller to which SafeUTM is connected is imported into SafeUTM.
- With Single Sign-On authorization, when the browser is opened for the first time, the user will be offered a choice of domains for authorization. The selection will be saved using a cookie and will be used at the next authorization. If you want to change the domain, delete the cookie (for the local SafeUTM IP address).

Using Security Groups and Accounts Imported from LDAP as Filter Rule Objects

Security groups and accounts imported from Active Directory can be used as filter rule objects in the following sections:

- **Firewall**
- **Application control**
- **Traffic Shaping**
- **Content Filter**

Usage example:

1. Import accounts and/or security groups from Active Directory in the **Users -> User & Group** section (for more details, see **Import of Users**). This example imports the AD security group **Domain Users:**

2. Go to the section where you want to use a group or account imported from Active Directory. For example, in Application Control:

Application control ⌄
Working

Configure rule

Title
Rule_1

Applies to
AD Domain Users ⊗   ▼

Protocols
Amazon ⊗   ▼

Action

⦿ Deny

◯ Allow

Description

Save   Cancel

3. Fill in the required fields and click **Save**.