

Import AD users to be used for Device/Web Control policies

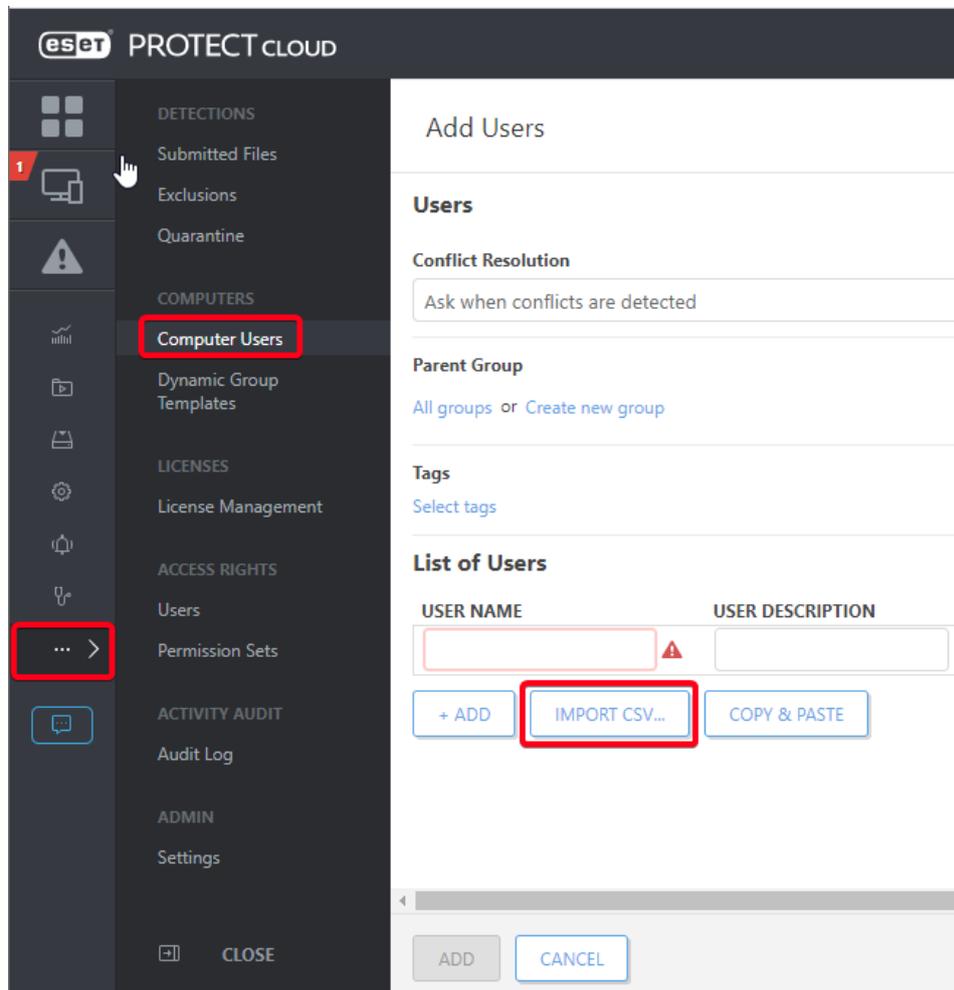
Mitchell | ESET Nederland - 2021-03-09 - [Comments \(0\)](#) - [ESET PROTECT \(Cloud\)](#)

1. export AD users to CSV using powershell:

```
Get-ADUser -Filter * -Properties * | Select-Object Name, Description, Mail, MobilePhone, Office, title, department, sid | export-csv -path c:\allusers.csv
```

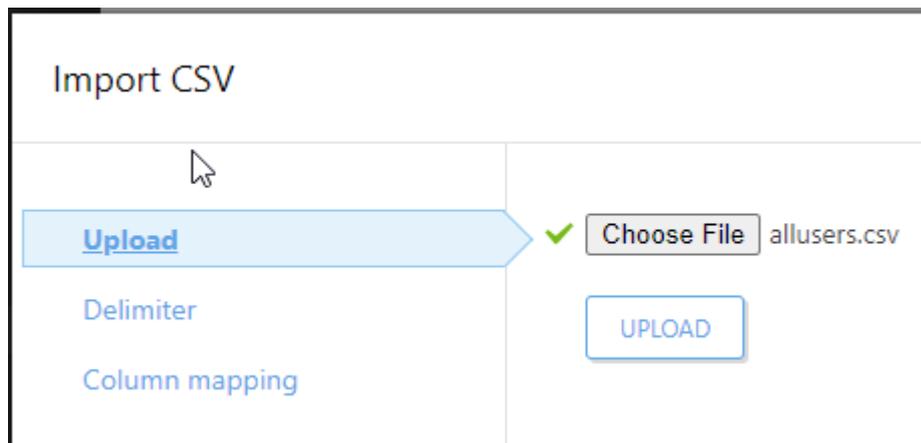
2. Import CSV in EPC:

1. More > Computer Users > IMPORT CSV...:

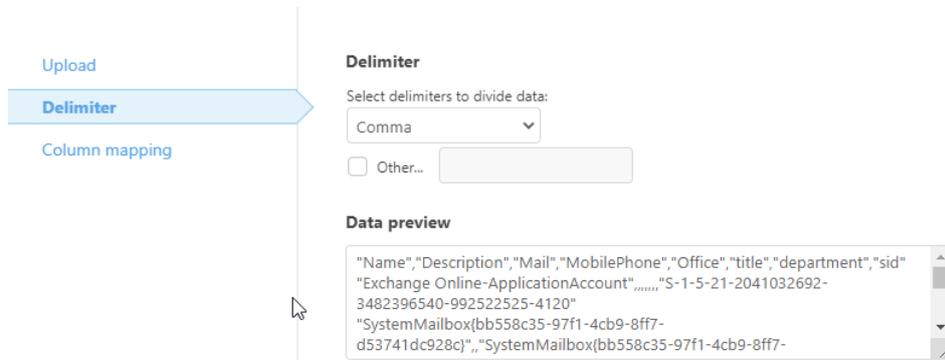


The screenshot shows the ESET PROTECT Cloud interface. On the left, a dark sidebar contains a menu with categories: DETECTIONS, COMPUTERS, LICENSES, ACCESS RIGHTS, ACTIVITY AUDIT, and ADMIN. The 'Computer Users' item under the COMPUTERS category is highlighted with a red box. Below it, a 'More' menu (three dots) is also highlighted with a red box. The main content area is titled 'Add Users' and contains several sections: 'Users', 'Conflict Resolution' (with a dropdown set to 'Ask when conflicts are detected'), 'Parent Group' (with options 'All groups' or 'Create new group'), 'Tags' (with a 'Select tags' link), and 'List of Users'. The 'List of Users' section has two input fields: 'USER NAME' and 'USER DESCRIPTION'. Below these fields are three buttons: '+ ADD', 'IMPORT CSV...' (highlighted with a red box), and 'COPY & PASTE'. At the bottom of the dialog, there are 'ADD' and 'CANCEL' buttons.

2. Choose the CSV file created in step 1 and click on UPLOAD.



3. Select the right delimiter. (Comma in this case):



4. Select "First line of CSV contains headings", Columns should be automatically filled in correctly now, if this is not the case correct them manually.

Import CSV

Upload
Delimiter
Column mapping

CSV headings ⓘ
 First line of CSV contains headings

CSV column

TABLE COLUMN	CSV COLUMN
USER NAME	Name (Exchange Online-ApplicationAccount)
USER DESCRIPTION	Description ()
EMAIL ADDRESS	Mail ()
PHONE	MobilePhone ()
OFFICE	Office ()
JOB POSITION	title ()
TEAM NAME	department ()
SID	sid (S-1-5-21-2041032692-3482396540-992522525-4120)

Table preview

USER NAME	USER DESCRIPTION	EMAIL ADDRESS	PHONE	OFFICE	JOB POSITION	TEAM NAME	SID
Exchange Online-ApplicationA...							S-1-5-21-2041032692-3482396540-992522525-4120
SystemMailb...97f1-4cb9-8ff7-d53741dc92...	SystemMailb...97f1-4cb9-8ff7-d53741dc92...						S-1-5-21-2041032692-3482396540-992522525-4120

BACK CONTINUE IMPORT CANCEL

5. Finish by clicking IMPORT.

3. You can now use these user objects when creating Web/Device Control policies:

1. User list > Edit > Add

Edit rule [?] [X] [Close] [Search] [Severity] [Time slots]

Name: Untitled

Enabled:

Type: Category-based Action

Access rights: Block

Apply during: Ⓜ ≥ 7.0 Always

URL Category: Social Networking

Use Group: Use Group

Logging severity: Warning

User list: Edit

User or Group Security Identifiers [?] [X]

S-1-5-21-2041032692-3482396540-992522525-1604

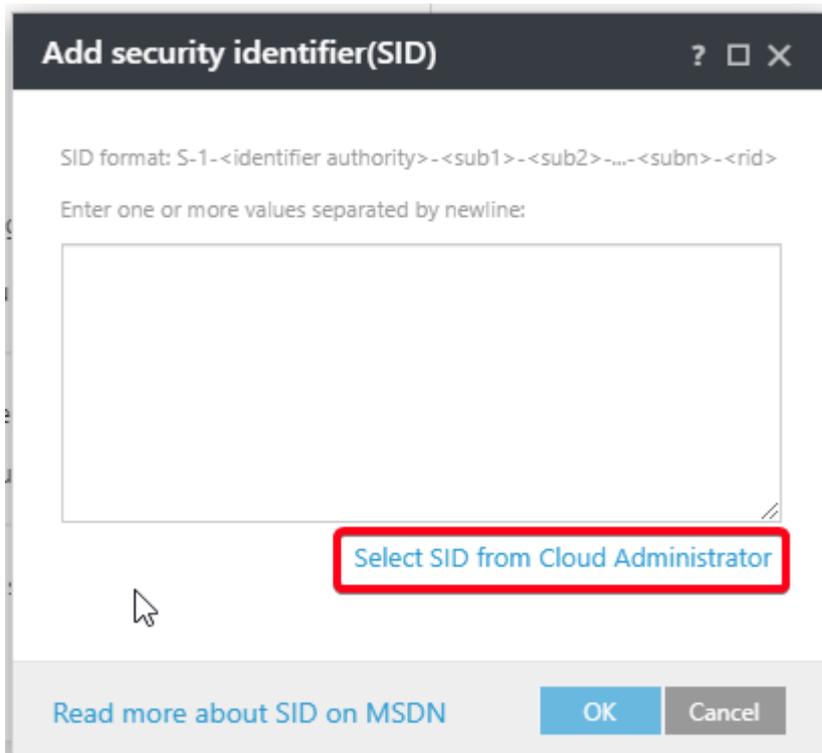
Add Edit Remove

OK Cancel

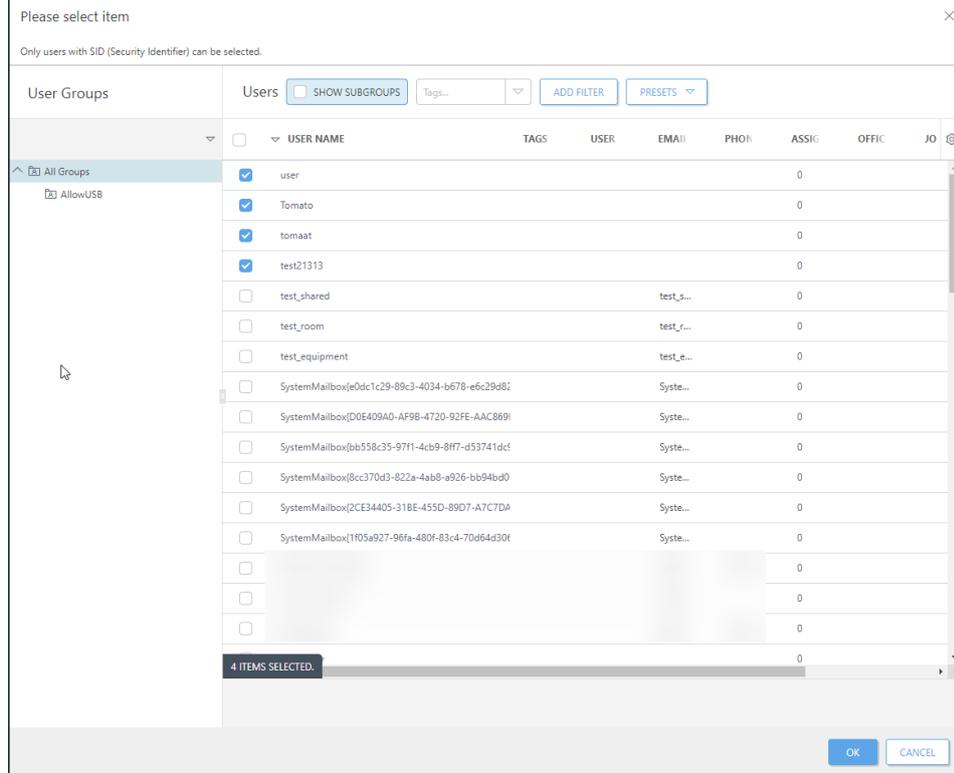
Save Cancel

OK

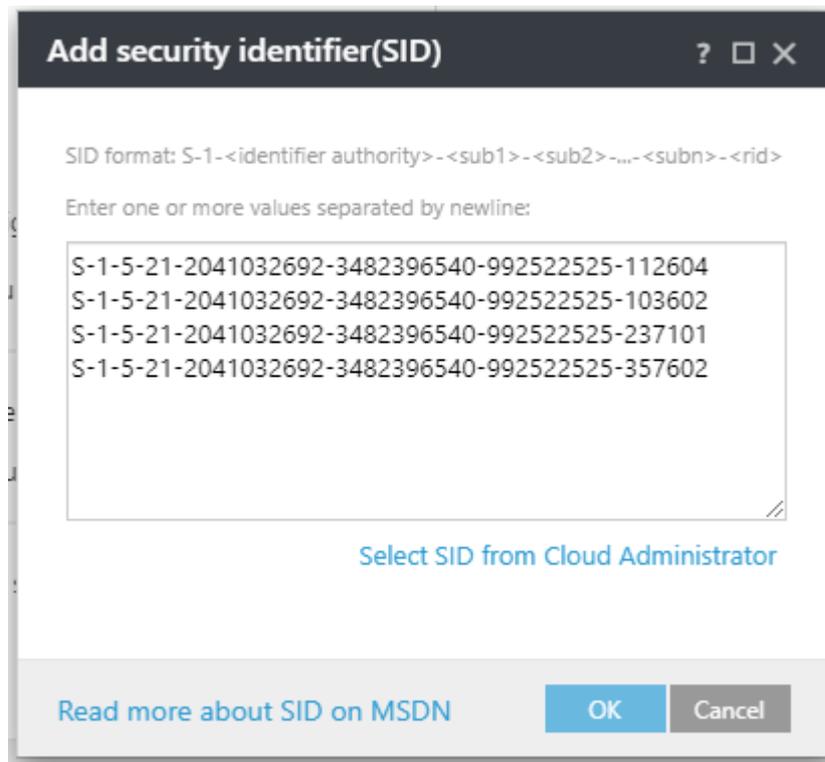
2. Select SID from Cloud Administrator:



3. Select the users you want to apply this rule on:



4. SID's will now be listed and you can save your rule.



Note: It is not possible to import AD groups, but you can create "groups" (comparable to OU) in the "Computers Users" overview for easier access. (do note that users can only be part of once of such groups)

Related Content

- [Security baseline policy voor | ESET Protect Cloud](#)
- [Multifactorauthenticatie toepassen en eerste client uitrollen in | ESET Protect Cloud](#)
- [Security voor de client nu in de cloud! | ESET Protect Cloud](#)