Configuring Active Directory

Your organization may want to have users authenticate to Lumeta Enterprise Edition using Active Directory (AD). This arrangement—with an assist from you—maps AD user-rights to the Lumeta system and controls what individual users can see and control when logged in to a Lumeta Command Center. Your contribution is to tell the Lumeta system how to apply rules to map groups, organizations, and roles by creating a csv group mapping file. The group mapping file you create specifies the mapping.

For more on organizations, roles, and permissions, see the About Organizations, Zones & Users page.

Update

In the groupmapping mechanism, a list of AD groups separated by the pipe symbol (|) can now be set as 'superuser' (or the column can be left blank).

Sample format:

group2|group4|group1	Manager/Development	superuser
group5|group4|group6	Viewer/Sales	

When an AD (new) user logins into Lumeta, a user account is created along with roles mapped to the user's AD groups. If these AD groups are defined as 'superuser', all the users in AD group will be designated at Lumeta superusers. Changes to groupmapping data take effect when the users associated with those records login to the Lumeta system.

Let's assume, for example, that Active Directory contains (or has defined) these groups and we want to assign users to particular roles in Lumeta, remembering that each Lumeta role is always paired with an organization defined in Lumeta.

Example AD Groups	Customer-Defined Lumeta Organizations	Actual Lumeta Roles
vp	NA	SysAdmin (no GUI access)
admin	EMEA	Viewer (read-only)
security	APAC	Manager (read + write)
na		
emea		
apac		

And you want these **rules** to apply to your Lumeta users:

1. Vice presidents should get read-only access in all organizations

	Group	Role+Organization
1	vp	Viewer/NA
2	vp	Viewer/EMEA
3	vp	Viewer/APAC

That portion of the group mapping CSV file would look like this:

vp,Viewer/NA

vp,Viewer/EMEA

vp,Viewer/APAC

Notice that the CSV example contains only two columns—the first for AD group name and the next the Lumeta role + organization. The two columns are separated by a comma (,). Any row containing more than two columns is considered an invalid row.

2. Admins should get SysAdmin roles in their own regions

	Group	Role+Organization
1	admin|na	SysAdmin/NA
2	admin|emea	SysAdmin/EMEA
3	admin|apac	SysAdmin/APAC

The AD users in row #1 are members of *both* the **admin** and **na** groups. The Lumeta users in row #1 are SysAdmins for the NA organization. That portion of the group mapping file would look like this:

admin|na,SysAdmin/NA

admin|emea,SysAdmin/EMEA

admin|apac,SysAdmin/APAC

3. People on the Security team should have Viewer and Manager roles in some regions.

	Group	Role+Organization
1	security|na|emea	Viewer/NA
2	security|na|emea	Manager/NA
3	security|na|emea	Viewer/EMEA
4	security|na|emea	Manager/EMEA
5	security|na|emea	Viewer/APAC
6	security|na|emea	Viewer/APAC
7	security|apac	Manager/APAC
8	security|apac	Viewer/NA
9	security|apac	Viewer/EMEA

AD users in row #7 are members of *both* the **security** and **apac** groups and in Lumeta have a Manager role in the APAC organization. That portion of the group mapping file would look like this:

security|na|emea,Viewer/NA

security|na|emea,Manager/NA

security|na|emea,Viewer/EMEA

security|na|emea,Manager/EMEA

security|na|emea,Viewer/APAC

security|apac,Viewer/APAC

security|apac,Manager/APAC

security|apac,Viewer/NA

security|apac,Viewer/EMEA

The contents of the assembled CSV file would look like this:

vp,Viewer/NA

vp,Viewer/EMEA

vp,Viewer/APAC

admin|na,SysAdmin/NA

admin|emea,SysAdmin/EMEA

admin|apac,SysAdmin/APAC

security|na|emea,Viewer/NA

security|na|emea,Manager/NA

security|na|emea,Viewer/EMEA

security|na|emea,Manager/EMEA

security|na|emea,Viewer/APAC

security|apac,Viewer/APAC

security|apac,Manager/APAC

security|apac,Viewer/NA

security|apac,Viewer/EMEA

CSV File Rules

The rules we've introduced are as follows:

1. Each line in the group mapping file starts with a list of AD groups followed by a role/organization pair.
2. If there is more than one group, separate by a vertical bar (|)
3. Each role must be paired with its organization, separated by a forward slash (/)
4. Users are assigned roles for every in which their AD groups match

The ***admin*** and ***manager*** users and see these roles by default.

User Name	Full Name	Roles
admin	Default administrative user	Organization1(SysAdmin,Viewer)
manager	Default management user	Organization1(Manager,Viewer)

To map Active Directory (AD) groups and roles to Lumeta organizations, here's the process.

Prerequisites

1. Ensure that Groups and Users have already been set up in an Active Directory (AD) server before beginning this procedure. See https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal to learn how.

2. Find out the credentials to your organization's AD server. Here are the types of information you'll need and an example of most (We've masked the name of our Active Directory server):

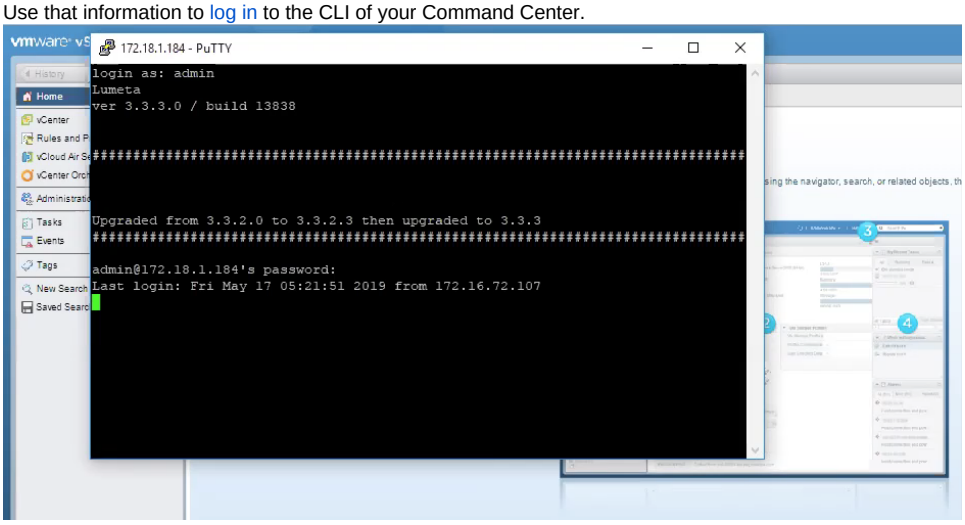
```
Server:
Realm: DEV.COM
Domain: DEV
username: Administrator
password: ******
```

Active Directory CLI Commands

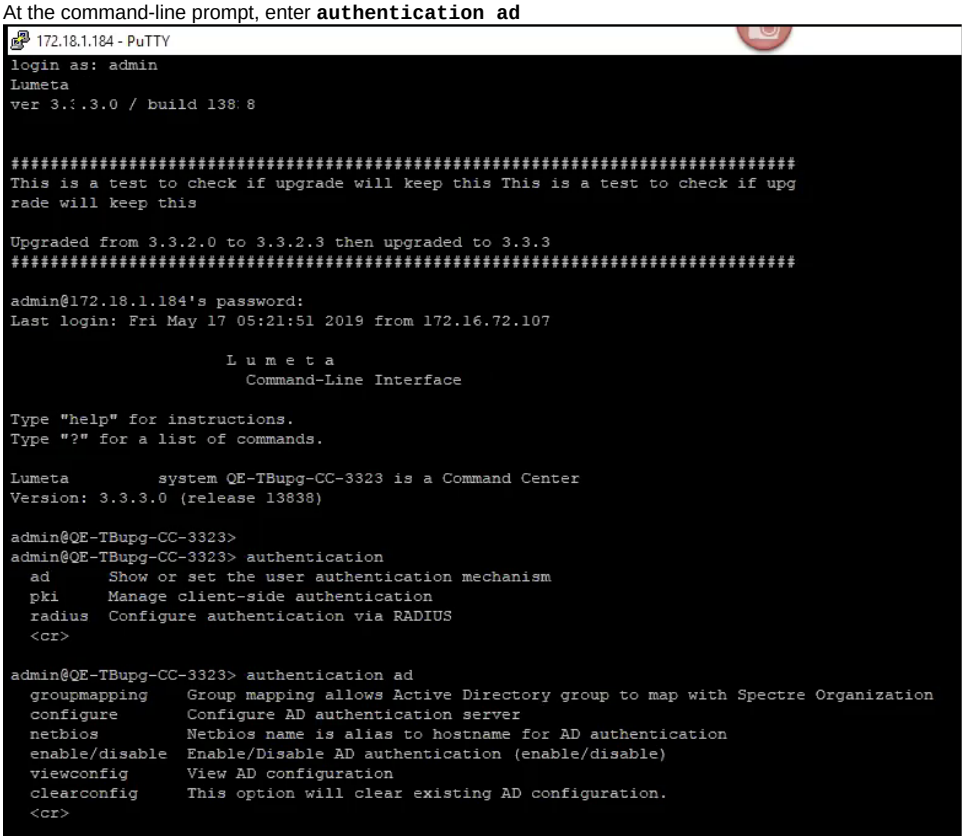
To configure Active Directory on Lumeta Enterprise Edition:

1. Identify the Host Name or IP Address of your Command Center.

2. Use that information to log in to the CLI of your Command Center.



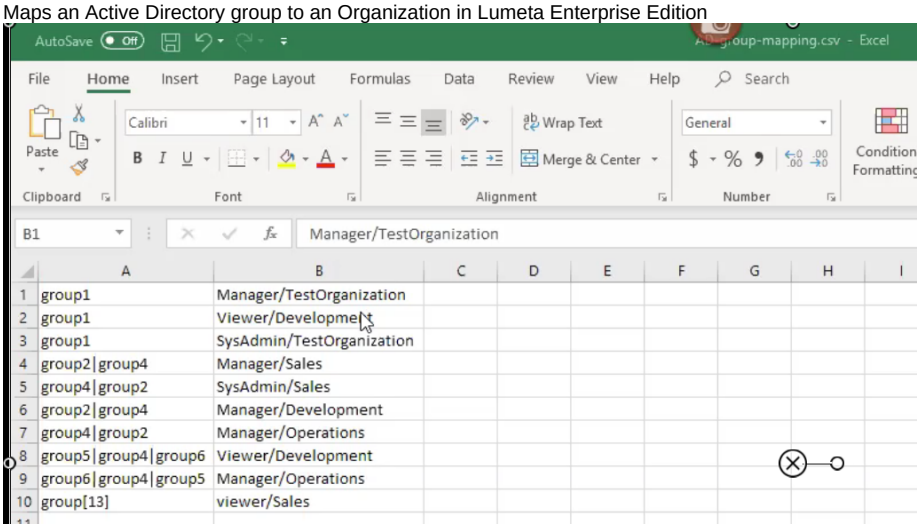
3. At the command-line prompt, enter **`authentication ad`**



4. As you can see in the illustration above, these are the available AD Authentication CLI commands. Each of these, their purpose and syntax follow along with a screencap. The Active Directory CLI commands are presented here in the order they are presented on the CLI menu. Although not fixed, the order of operations is likely to be 1) configure, 2) viewconfig, 3) netbios, 4) enable 5) groupmapping. This order of operations in the last column of the table below.

CLI Command	Description & Example
groupmapping	

Maps an Active Directory group to an Organization in Lumeta Enterprise Edition




```
admin@QE-TBupg-CC-3323> authentication ad groupmapping
  append      To add/append new records to the groupmapping data
  overwrite   overwrites existing groupmapping data
  download    downloads existing groupmapping data into csv file
```

```
admin@QE-TBupg-CC-3323> authentication ad groupmapping append
  String  "/path/to/local/file" or  "user@host:/path/to/remote/file"

admin@QE-TBupg-CC-3323> authentication ad groupmapping append admin@172.18.1.184:/home/admin/AD-group-mapping.csv
Retrieving file...
FIPS mode initialized
The authenticity of host '172.18.1.184 (172.18.1.184)' can't be established.
RSA key SHA1 fingerprint is e8:cd:69:9f:1a:ff:85:dc:fa:24:a4:5c:96:1f:d8:5d:cc:67:46:0a.
Are you sure you want to continue connecting (yes/no)? yes
```

`authentication ad groupmapping append path/to/local/file`

`authentication ad groupmapping append admin@172.18.1.184:/home/admin/AD-group-mapping.csv`

If your Active Directory mapping introduces new Organizations, you will need to create those organizations in the Command C

`organization new name-of-new-organization`

```
Following organizations does not exists: Sales, Development, TestOrganization, Operations
admin@QE-TBupg-CC-3323> organization new Sales
admin@QE-TBupg-CC-3323> organization new Development
admin@QE-TBupg-CC-3323> organization new TestOrganization
admin@QE-TBupg-CC-3323> organization new Operations
admin@QE-TBupg-CC-3323> organization list
Development
Operations
Organization1
QAtestORG001
QAtestORG002
QAtestORG003
Sales
TestOrganization
admin@QE-TBupg-CC-3323>
```

configure

Configures an Active Directory authentication server

```
admin@QE-TBupg-CC-3323> authentication ad configure win                    .com DEV.COM DEV Administrator
Enter Administrator's password:
Configuration saved
```

`authentication ad configure <AD server> <realm> <domain> <username> <password>`

netbios

The netbios is an alias for the hostname used in Active Directory authentication. It's only required if your hostname is more th

In this example, the hostname of the Command Center is longer than the maximum number of characters allowed, so AD cou a too-long hostname.

```
admin@QE-TBupg-CC-3323> authentication ad enable
  <cr>

admin@QE-TBupg-CC-3323> authentication ad enable
Our netbios name can be at most 15 chars long, 'QE-TBupg-CC-3323' is 16 chars long.
Invalid configuration.  Exiting....
```

	This command would create a hostname on the AD server with the name "TestAD." `admin@QE-TBupg-CC-3323> authentication ad netbios testAD`

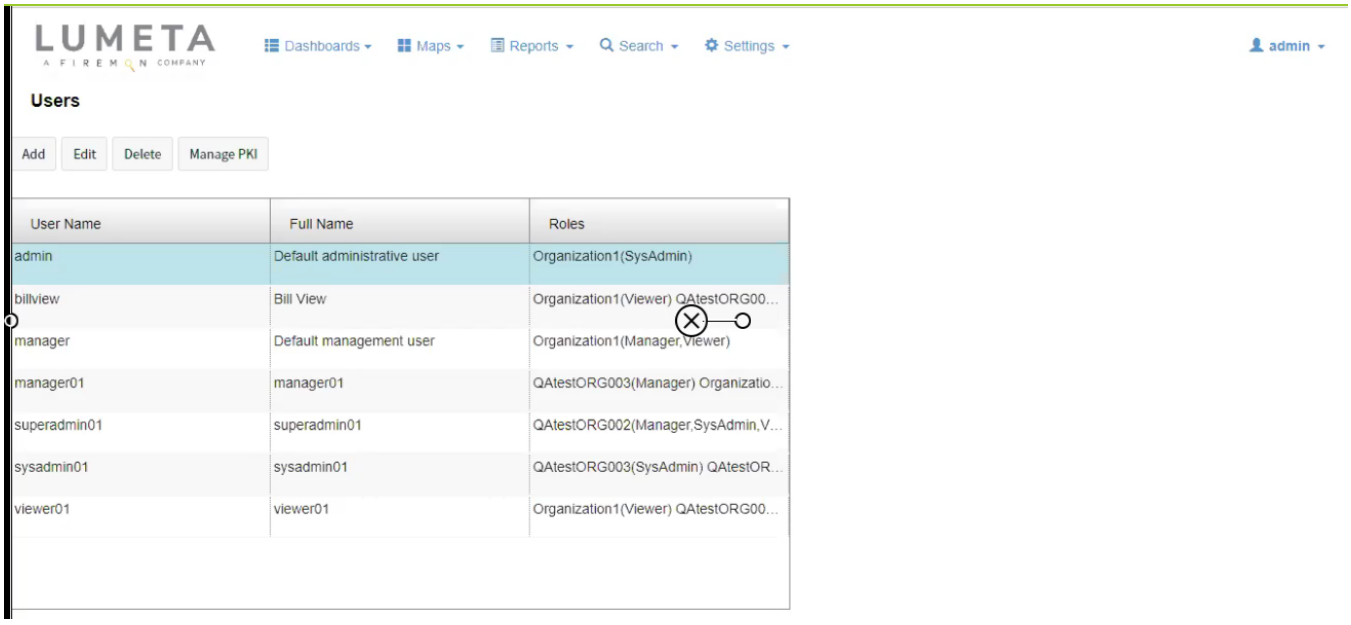
enable/disable	Enables and disables an AD authentication
	`authentication ad <enable|disable>`
	`admin@QE-TBupg-CC-3323> authentication ad enable`
	`enabled`
	`Joined 'TESTAD'  to dns domain 'dev.com'.`
	`Join AD requires restarting lumeta-webapp service. This may take a minute or two`
	`Restarting lumeta-webapp service...`
	`admin@QE-TBupg-CC-3323>`

viewconfig	Displays the current AD configuration. The two examples below show a not joined/disabled AD server and a joined/enabled A
	`admin@QE-TBupg-CC-3323> authentication ad viewconfig`
	`Workgroup : DEV`
	`Domain Name : DEV.COM`
	`AD server : win .com`
	`Netbios : Not configured`
	`Join status : Not Joined`
	`AD authentication : disabled`
	`admin@QE-TBupg-CC-3323>`
	`admin@QE-TBupg-CC-3323> authentication ad viewconfig`
	`Workgroup : DEV`
	`Domain Name : DEV.COM`
	`AD server : win .com`
	`Netbios : testAD`
	`Join status : Joined`
	`AD authentication : enabled`
	`admin@QE-TBupg-CC-3323>`

clearconfig	Clears the current AD configuration
	`Active Directory server is already configured. Clear existing configuration to continue`
	`admin@QE-TBupg-CC-3323> authentication ad clearconfig`
	`Are you sure? [Y/N]: y`
	`Configuration cleared`

Viewing Users in Lumeta

When an AD user logs in to Lumeta, and browses to Settings > Users, users, groups, and organizations to which he has been given rights in the AD server groupings—and only those—are visible.


LUMETA
A FIREMON COMPANY
Dashboards
Maps
Reports
Search
Settings
admin
Users
Add
Edit
Delete
Manage PKI
User Name
Full Name
Roles
admin
Default administrative user
Organization1(SysAdmin)
billview
Bill View
Organization1(Viewer) QAtestORG00...
manager
Default management user
Organization1(Manager,Viewer)
manager01
manager01
QAtestORG003(Manager) Organizatio...
superadmin01
superadmin01
QAtestORG002(Manager,SysAdmin,V...
sysadmin01
sysadmin01
QAtestORG003(SysAdmin) QAtestOR...
viewer01
viewer01
Organization1(Viewer) QAtestORG00...