

GSM: Central Authentication

Content

- [Configuration of the Greenbone Security Manager](#)
- [Example: Univention Corporate Server](#)

Introduction

The Greenbone Security Manager (GSM) can be connected to central authentication services. You can then use your directory service to allow certain users to connect to the GSM and use their usual credentials to log in. It is also possible to set their role in the GSM and additional user preferences through the directory service.

Some directory services are directly supported by Greenbone. This includes an installation package which extends the management interface to include a special page for the GSM.

- Univention Corporate Server 2.3

You will find a step by step guide including installation packages for the products listed above on this page.

Configuration of the Greenbone Security Manager

When not configured otherwise, the Greenbone Security Manager uses a custom independent authentication system. Users with the role "Admin" are able to create, modify and delete other users.

To use an LDAP directory service through the GSM, the following steps must be taken.

1. When using a central authentication method it becomes necessary that user passwords are transmitted between the GSM and the LDAP directory service and thus a secure communication is required. Using the CA certificate of the LDAP directory service the service can be set as trusted in the GSM. This is done through the CLI admin interface (see also the manual "GSM Command Line Interface: Administrator Guide"). Use ssh to connect to the admin interface (i.e. do not use the console directly, you will not be able to use the "paste" method there):

```
gsm> ldapcacertdownload
Please paste the BASE64 Certificate into the CLI, END with CTRL-D
```

The examples below show where the certificate can be found and how it should be prepared.

The certificate is checked immediately for validity. If the certificate is generally valid, the result will be an "OK" message. Self signed certificates are accepted but will result in a notice.

If the certificate submitted is empty (i.e. CTRL-D was pressed immediately), the installed certificate is removed, returning the GSM to the default behaviour regarding authentication.

- The address of the directory service can be set through the web interface of the Greenbone Security Assistant by navigating to Administration->Users (this option is of course only available to users with the role "Admin"):

Setting	Value
Enable	<input checked="" type="checkbox"/>
LDAP Host	192.168.1.1
Auth. DN	uid=%s,cn=users,o=yourcompany,c

Enable: Activate the use of this LDAP directory service by selecting "Enable".

LDAP Host: The address of the directory service.

Please note: This has to be the address that is named in the CA certificate

If you are using Univention Corporate Server, you can find this address in the "About Univention Directory Manager" dialog (select "About UDM" in the top right corner of the web interface).

Auth. DN: The DN which is used by your directory service for authentication. You can place the login name using "%s".

A locally configured user "Smith" on the GSM takes precedence over a user "Smith" in the connected directory service.

- Please note:** A reboot of the GSM is necessary to activate both changes.

Example: Univention Corporate Server 2.3

The Univention Corporate Server (UCS) by [Univention GmbH](#) includes an LDAP management system which can be extended to explicitly support the GSM.

- First the GSM needs to be equipped with the SSL certificate of the UCS CA. The following file on the UCS is required:

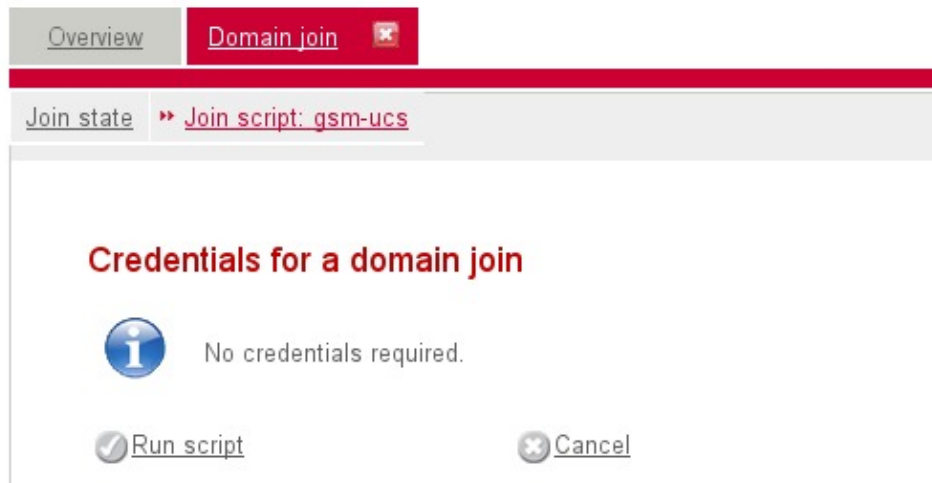
```
/etc/univention/ssl/ucsCA/CAcert.pem
```

Use the contents of this file for the GSM command "ldapcertdownload" as described above.

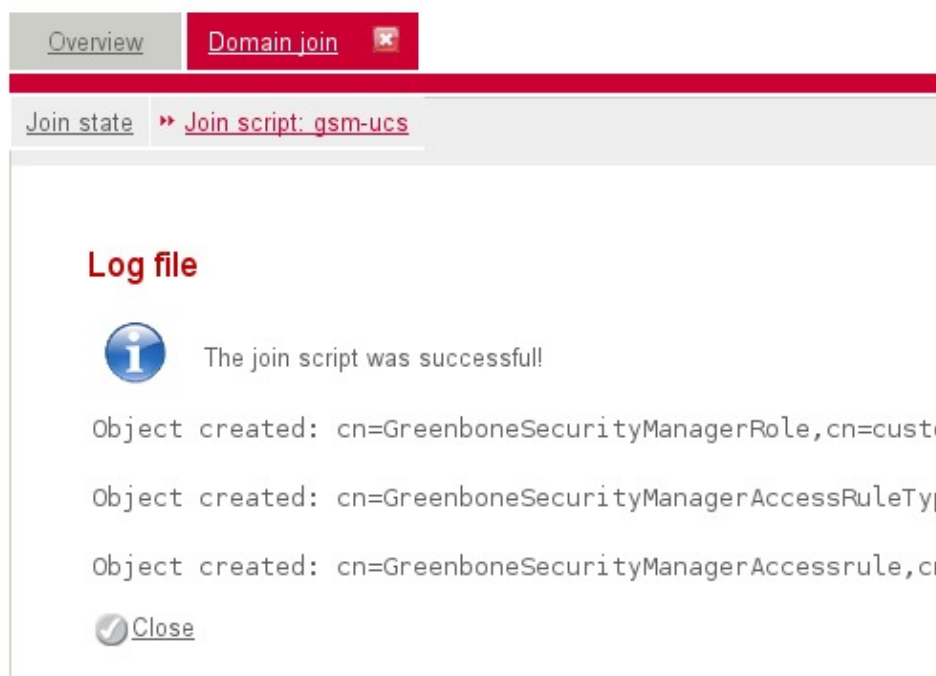
- Greenbone Networks provides an extension to the UCS management system by the way of the installation package `gsm-ucs_1.0-3_i386.deb`. Download this package and use the following command to install it on the GSM:

```
dpkg -i gsm-ucs_1.0-3_i386.deb
```

- Now use the Univention Management Console (UMC) to join the gsm-ucs domain by pressing the "Run script" button.



This should lead to the following success message:



4. Now the Univention Directory Manager (UDM) can be used to assign GSM specific roles and access restrictions to users. The default setting for existing users is to not allow them as GSM users (i.e. the *User Role* is set to *none*).

The tab for the settings for the Greenbone Security Manager becomes visible as soon as you check the "Show the advanced settings" checkbox.

The following example shows how the user "alice" can be allowed to access the GSM, but only to scan a single system ("192.168.1.1"):

Modify alice (User) Show the advanced settings

General User account Mail Contact Organisation Private contact Linux/UNIX

[Univention Directory Manager View] [Desktop settings] [UMC access] [Options]

Windows Groups Windows Advanced **Greenbone Security Manager** [Passwords] [Mail quota]

Greenbone Security Manager

User Role: user (dropdown) Type of Accessrule: allow (dropdown)

Access Rule Specification: 192.168.1.1

Cancel

The user is assigned a GSM role:

- ◆ *none* means that the GSM allows no connection with this user.
- ◆ *user* means that the user can connect as a regular GSM user.
- ◆ *admin* means that the user can connect to the GSM as an user with administrative privileges.

Additionally, the access to target systems can be restricted by selecting a rule type and the targets this rule should apply to:

- ◆ *allow* - allows access to the defined target.
- ◆ *allow all* - allows unrestricted access.
- ◆ *deny* - allows access to all targets excluding the ones listed.

The targets can be defined using the "Access Rule Specification" text field. The CIDR notation (e.g. "192.168.13.2/31") can be used. Multiple targets must be separated by commas (e.g. "192.168.14.12,192.168.14.13").

5. Once the users have been successfully set up they can use their usual password to connect to the GSM and to perform vulnerability management for the target systems they are allowed to access.