

# GSM: Zentrale Nutzerverwaltung

## Inhalt

- [Konfiguration des Greenbone Security Manager](#)
- [Beispiel: Univention Corporate Server](#)

## Einleitung

Der Greenbone Security Manager (GSM) erlaubt eine Anbindung an zentrale Benutzer-Management-Systeme. In einem solchen Verzeichnisdienst können dann einzelne Benutzer für die Verwendung des GSM freigeschaltet werden und sich mit ihren üblichen Zugangsdaten anmelden. Auch die Rolle sowie weitere Nutzer-Einstellungen können konfiguriert werden.

Einige Verzeichnisdienst-Produkte werden von Greenbone direkt unterstützt. Das beinhaltet vor allem ein fertiges Installationsmodul welches die Management-Oberfläche um eine spezielle Seite für den GSM erweitert.

- Univention Corporate Server 2.3

Eine Schritt-für-Schritt Anleitung für diese Produkte inklusive der Installationspakete finden Sie auf dieser Seite.

## Konfiguration des Greenbone Security Manager

Im Auslieferungszustand benutzt der Greenbone Security Manager (GSM) zur Authentifizierung ein eigenes, unabhängiges System. Benutzer mit der Rolle "Admin" können andere Benutzer anlegen, löschen, ändern.

Um einen LDAP Verzeichnisdienst über den GSM zu verwenden müssen folgende Schritte ausgeführt werden.

1. Da bei einer zentralen Authentifizierung Benutzer-Passworte vom GSM an den LDAP Verzeichnisdienst übertragen werden müssen ist eine abgesicherte Kommunikation zwingend notwendig. Mit dem CA-Zertifikat des LDAP Verzeichnisdienstes wird beim GSM der Dienst als vertrauenswürdig gesetzt. Dies erfolgt über die CLI-Admin-Oberfläche (siehe auch Handbuch "GSM Command Line Interface: Administrator Guide"). Melden Sie sich per ssh an (also nicht an der Konsole direkt, sonst funktioniert die "Paste"-Methode nicht):

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

In den unten aufgeführten Beispielen wird gezeigt wo man das Zertifikat findet und wie man es vorbereitet.

Es wird unmittelbar eine Gültigkeitsprüfung des Zertifikats ausgeführt. Ist es grundsätzlich verwendbar, wird es mit "OK" quittiert. Selbstsignierte Zertifikate werden akzeptiert, es wird aber mit einer Meldung auf diesen Umstand hingewiesen.

Wird ein leerer Inhalt eingeben (also direkt CTRL-D) wird das bisherige Zertifikat entfernt und damit der Auslieferungszustand wiederhergestellt.

- Die Adresse des Verzeichnisdienstes wird in der Web-Oberfläche Greenbone Security Assistant eingestellt: Über die Navigation unter Administration->Users (das geht natürlich nur mit der Rolle "Admin"):

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

Save

*Enable:* Aktivieren Sie die Verwendung dieses LDAP Verzeichnisdienstes in dem Sie "Enable" einschalten.

*LDAP Host:* Die Adresse des Verzeichnisdienstes.

**Beachten Sie:** Dies muss die Adresse sein, die auch im CA-Zertifikat enthalten ist.

Für Univention Corporate Server finden Sie den eingestellten Server-Namen in den Allgemeinen Informationen über den Univention Directory Manager (in der Web-Oberfläche oben rechts "Über UDM" anwählen).

*Auth. DN:* Der DN der in Ihrem Verzeichnisdienst zur Authentifizierung verwendet wird. Sie können mit "%s" den Login-Namen plazieren.

Ein Lokal auf dem GSM konfiguriertes Anwender "Mueller" hat Vorrang vor dem Anwender "Mueller" des angeschlossenen Verzeichnisdienstes.

- Beachten Sie,** dass nun ein Neustart des GSM notwendig ist um die beiden Änderungen zu aktivieren.

## Beispiel: Univention Corporate Server 2.3

Der Univention Corporate Server (UCS) der [Univention GmbH](#) beinhaltet ein LDAP Managementsystem. Es kann um explizite Unterstützung des GSM erweitert werden.

- Als erstes muss der GSM mit dem SSL Zertifikat der CA des UCS ausgestattet werden. Vom UCS wird dafür folgende Datei benötigt:

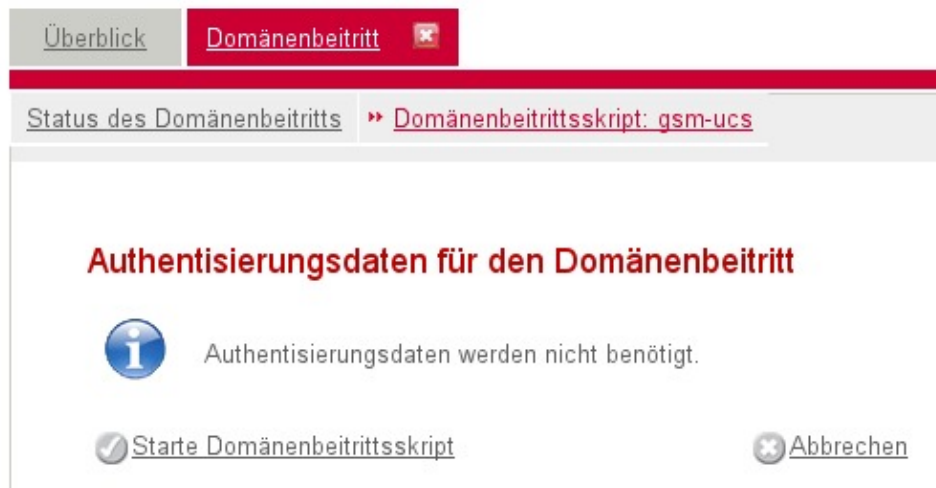
```
/etc/univention/ssl/ucsCA/CAcert.pem
```

Verwenden Sie den Inhalt dieser Datei für das GSM-Kommando "ldapcacertdownload" wie oben beschrieben.

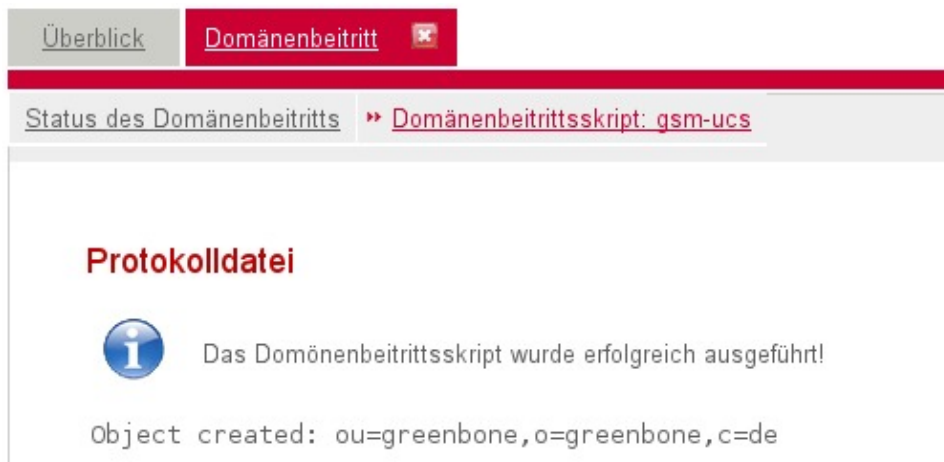
- Greenbone Networks stellt eine Erweiterung des UCS Management-Systems in Form des Installationspaketes `gsm-ucs_1.0-3_i386.deb` zur Verfügung. Laden Sie dieses herunter und installieren Sie es wie folgt auf dem UCS Master:

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

- Nun führen Sie über die Univention Management Console (UMC) den Beitritt der `gsm-ucs` Domäne aus in dem Sie auf "Starte Domänenbeitrittsskript" klicken.



Dies sollte mit einer entsprechenden Erfolgsmeldung quittiert werden:



- Nun können Nutzern über den Univention Directory Manager (UDM) GSM-spezifische Rollen und Zugriffsbeschränkungen zugewiesen werden. Die Voreinstellung für neue oder bereits existierende Nutzer ist, dass diese nicht als GSM-Nutzer anerkannt werden (die *User Role* ist dann *none*).

Der Reiter für die Einstellungen zum Greenbone Security Manager wird sichtbar, sobald Sie den Schalter "Zeige die erweiterten Einstellungen" anwenden.

Das folgende Beispiel zeigt, wie dem Nutzer "alice" erlaubt wird, mit dem GSM genau ein System ("192.168.1.1") zu scannen:

Bearbeite alice (Benutzer)  Zeige die erweiterten Einstellungen

---

**Greenbone Security Manager**

User Role:

Type of Accessrule:  (dropdown menu with options: allow all, allow, allow all, deny)

Access Rule Specification:

Dem Nutzer wird eine GSM-Rolle zugewiesen:

- ◆ *none* bedeutet, dass der GSM keine Anmeldung mit dem entsprechenden Nutzer erlaubt.
- ◆ *user* bedeutet, dass der GSM den entsprechenden Nutzer wie einen regulären Nutzer behandelt.
- ◆ *admin* bedeutet, dass der GSM den entsprechenden Nutzer wie einen Nutzer mit Administrator-Rechten behandelt.

Zusätzlich kann der Zugriff auf Ziel-Systeme von diesem Nutzer eingeschränkt werden. Hierzu wird zunächst der Regeltyp und danach das oder die eigentlichen Ziele definiert:

- ◆ *allow* - erlaubt den Zugriff auf das oder die definierten Ziele.
- ◆ *allow all* - erlaubt den unbeschränkten Zugriff.
- ◆ *deny* - erlaubt den Zugriff auf alle bis auf das oder die definierten Ziele.

Das oder die Ziele werden in dem Text-Feld (Access Rule Specification) definiert. Es kann die CIDR-Notation (z.B. "192.168.13.2/31") verwendet werden. Mehrere Ziele werden durch Kommata getrennt (z.B. "192.168.14.12,192.168.14.13").

5. Die entsprechend eingerichteten Nutzer können sich nun mit gewohntem Passwort auf dem GSM anmelden und das Schwachstellen-Management für die erlaubten Zielsysteme durchführen.