



How to configure Active Directory authentication with TLS on Red Hat Satellite 6?

🔒 SOLUTION VERIFIED - Updated October 6 2021 at 8:45 AM - English ▼

Environment

- Red Hat Satellite 6.3 or later
- Active Directory

Issue

- How to configure Active Directory authentication with TLS on Satellite 6.3 or later?
- Active Directory authentication with Red Hat Satellite 6.3 or later
- Logging in with an LDAP account results in an SSL error:

```
SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate
verify failed OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 state=SSLv3 read
server certificate B: certificate verify failed
app/models/auth_sources/auth_source_ldap.rb:50:in `authenticate'
app/models/user.rb:190:in `try_to_login' app/controllers/users_controller.rb:71:in
`login' app/models/concerns/foreman/thread_session.rb:33:in `clear_thread'
lib/middleware/catch_json_parse_errors.rb:9:in `call'
```

Resolution

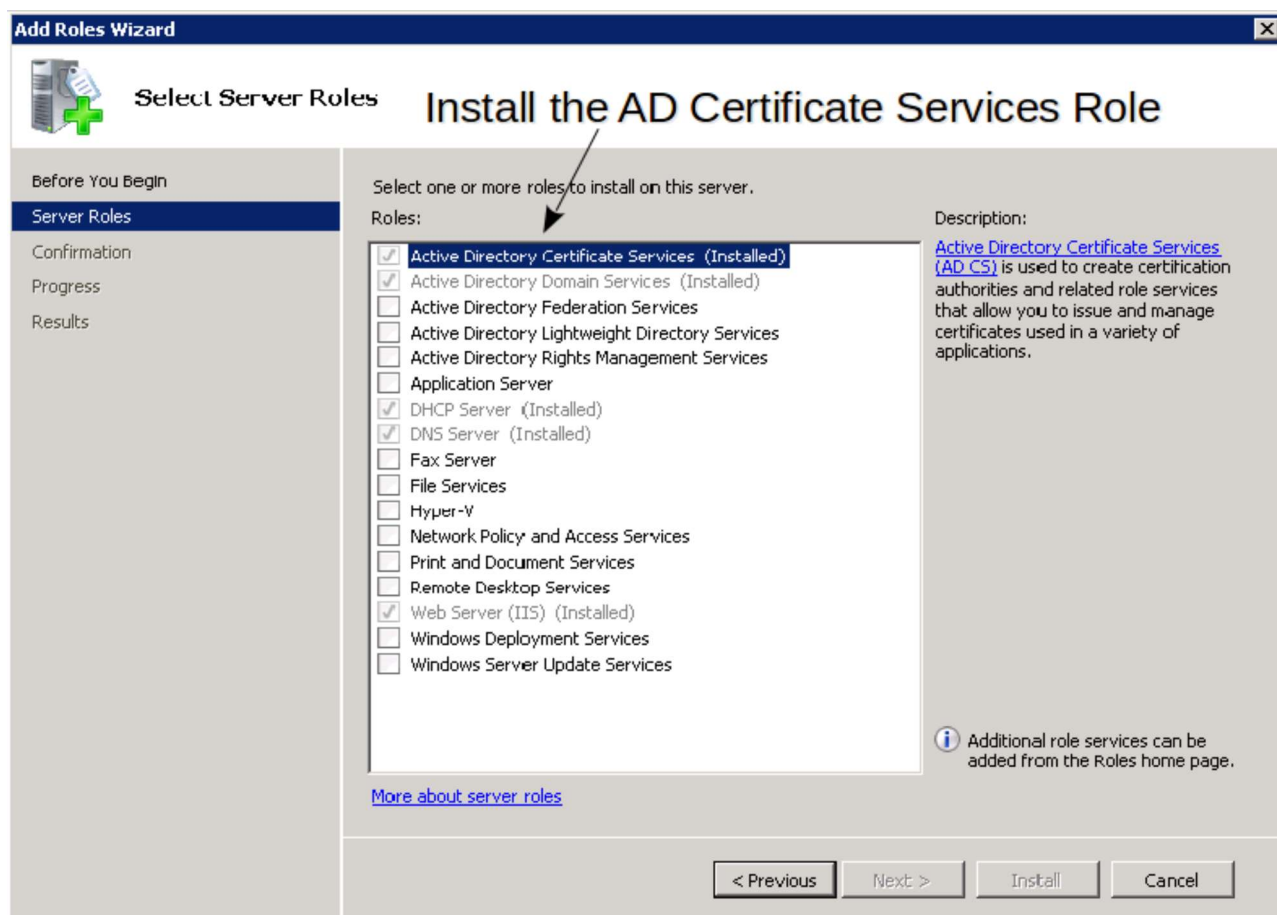
This solution is for creating a certificate in Active Directory, which can then be installed on the Satellite Servers base system, to enable secure LDAP (LDAPS).

The procedure to configure Red Hat Satellite to use **AD as an LDAP** server is Using LDAP. This procedure is only required if you are using AD as an LDAP server. This method does not provide single-sign on.

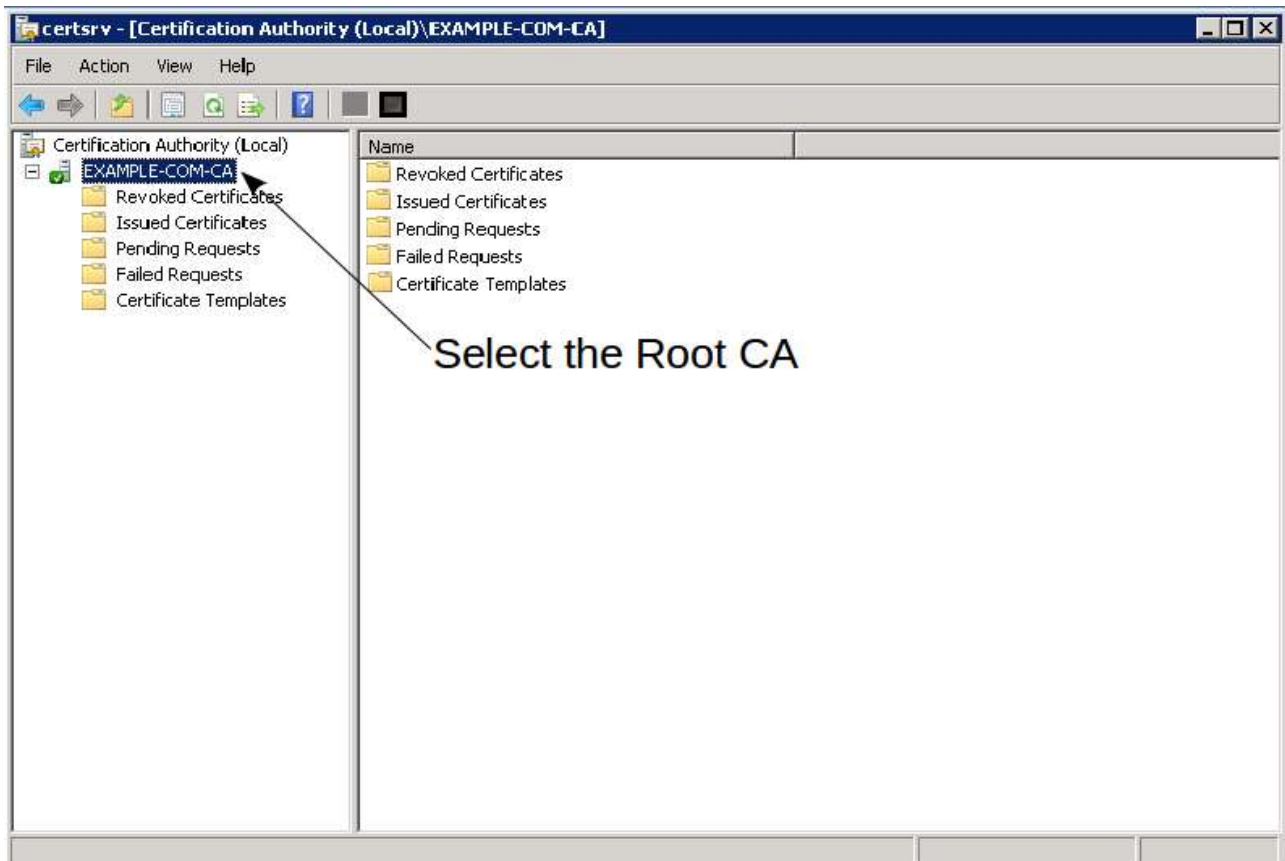
Note that when the use of AD is required, Red Hat recommends using AD directly as described in Using Active Directory. This method uses **Kerberos for authentication**, which allows for **single sign-on**, and does not require the certificate described here.

If **secure LDAP**(Lightweight Directory Access Protocol) to an Active Directory server is required, the following solution is available.

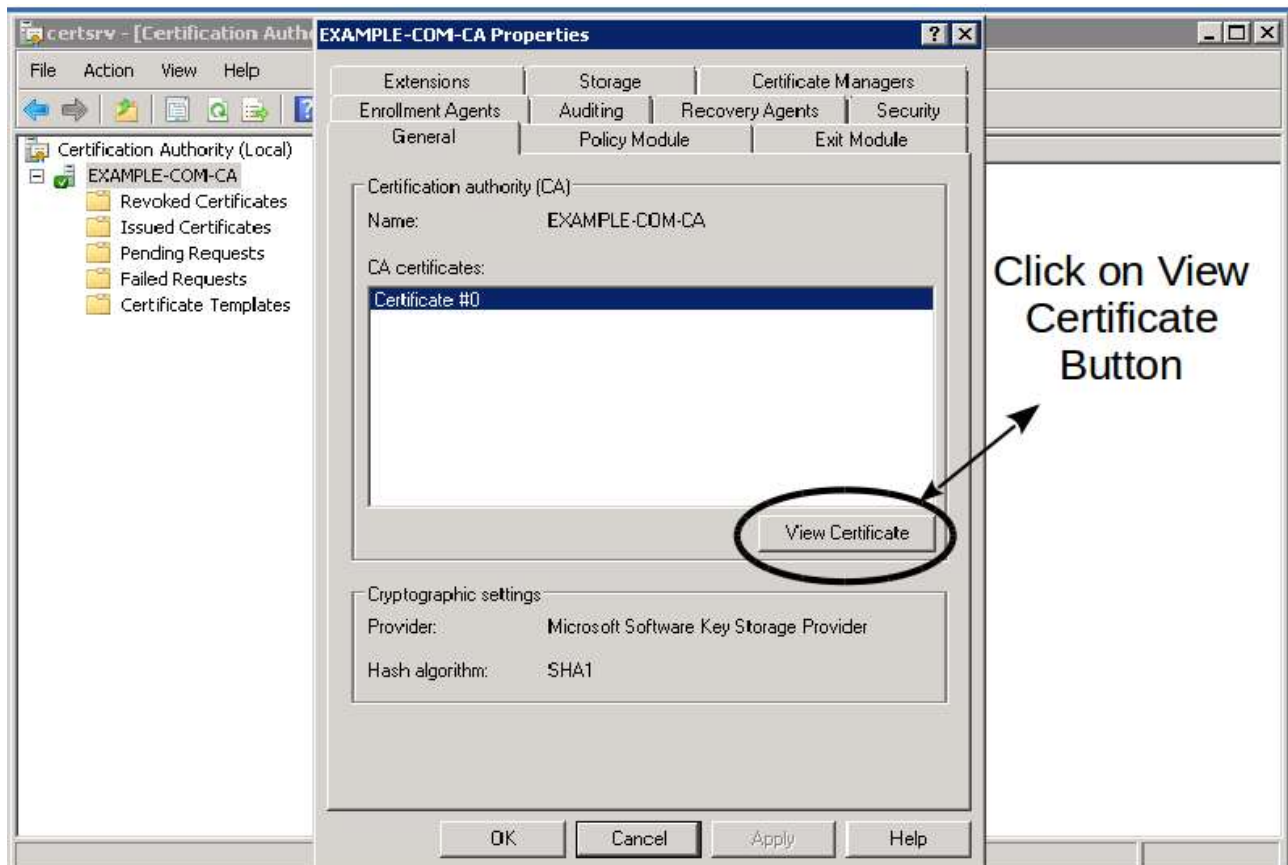
1. Install the Active Directory Certificate services role:



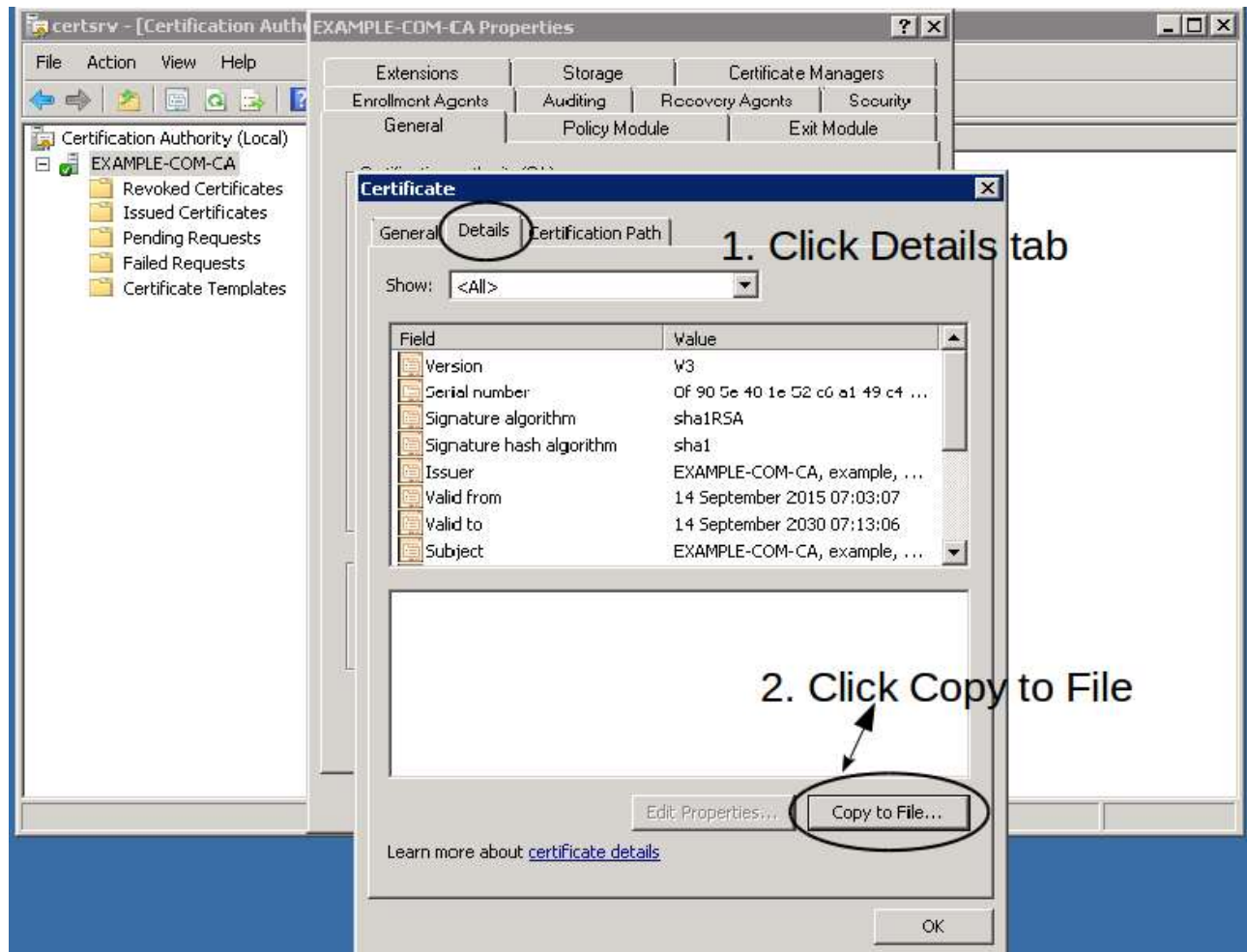
2. Select the Root CA server from the Active Directory Certificate Services console:



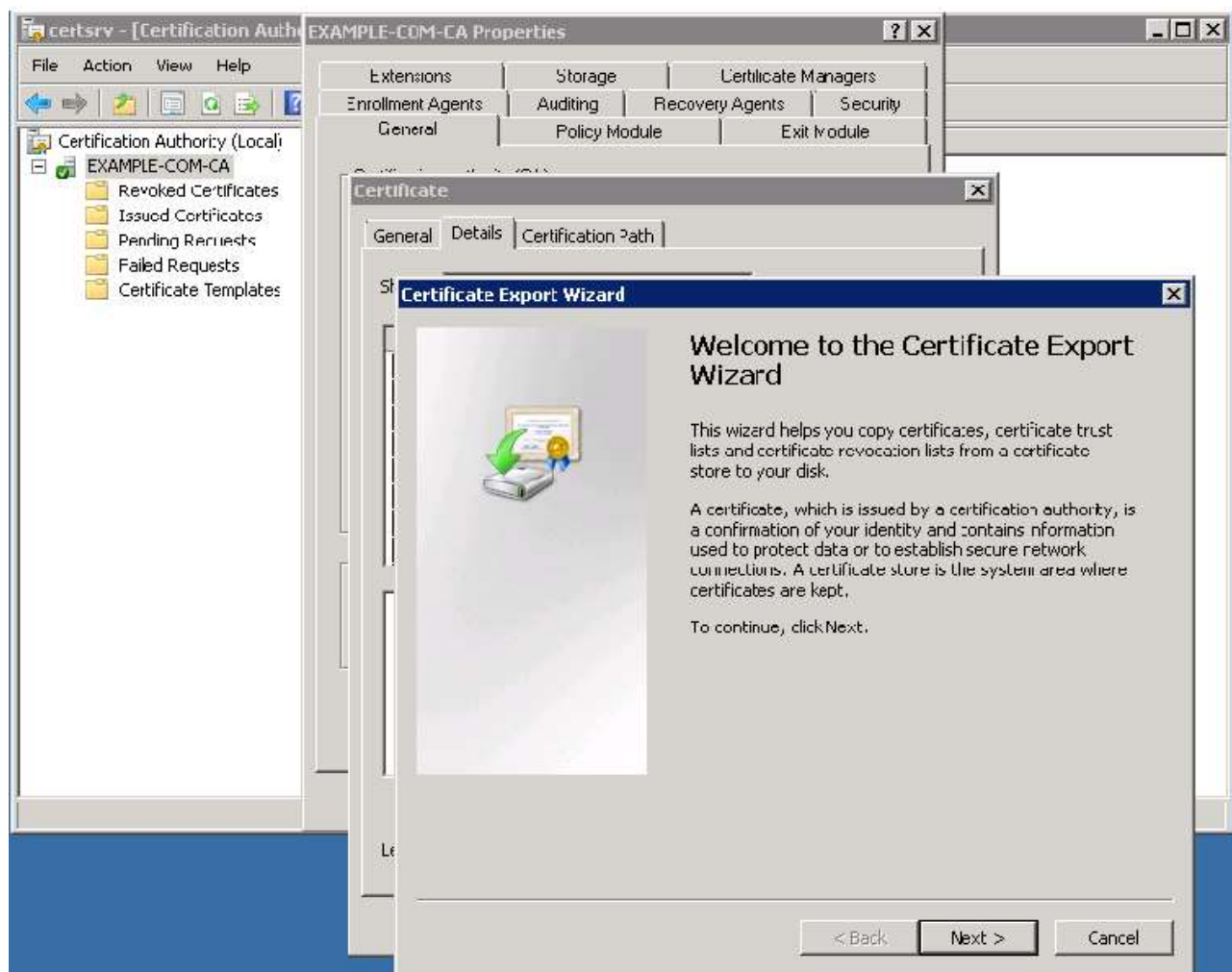
3. Right click on the Root CA server and click on its properties:



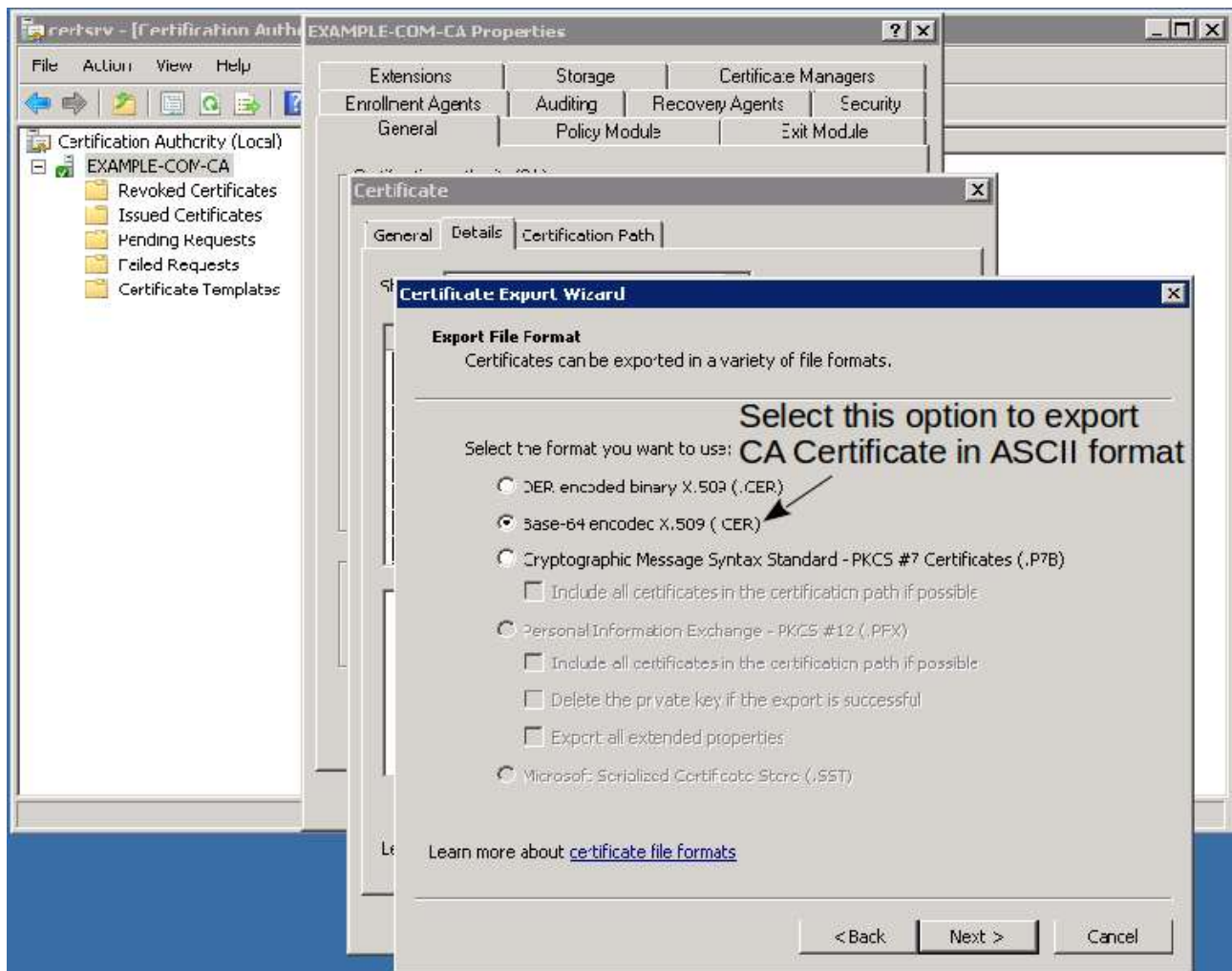
4. Click the **Details** tab and then click on **Copy to File** Button to export Active Directory CA certificate:



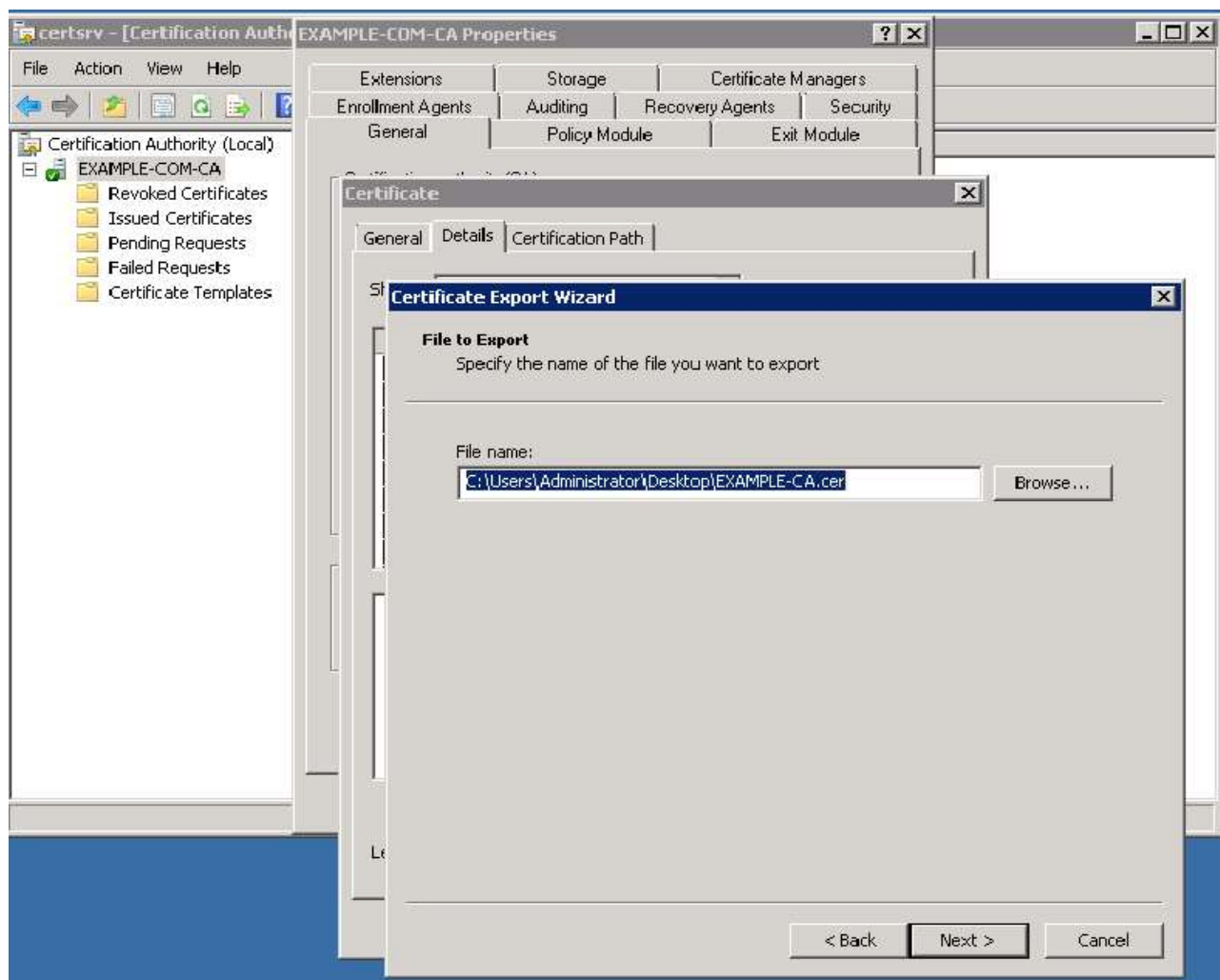
5. Select **Next** on the CA Certificate export wizard:



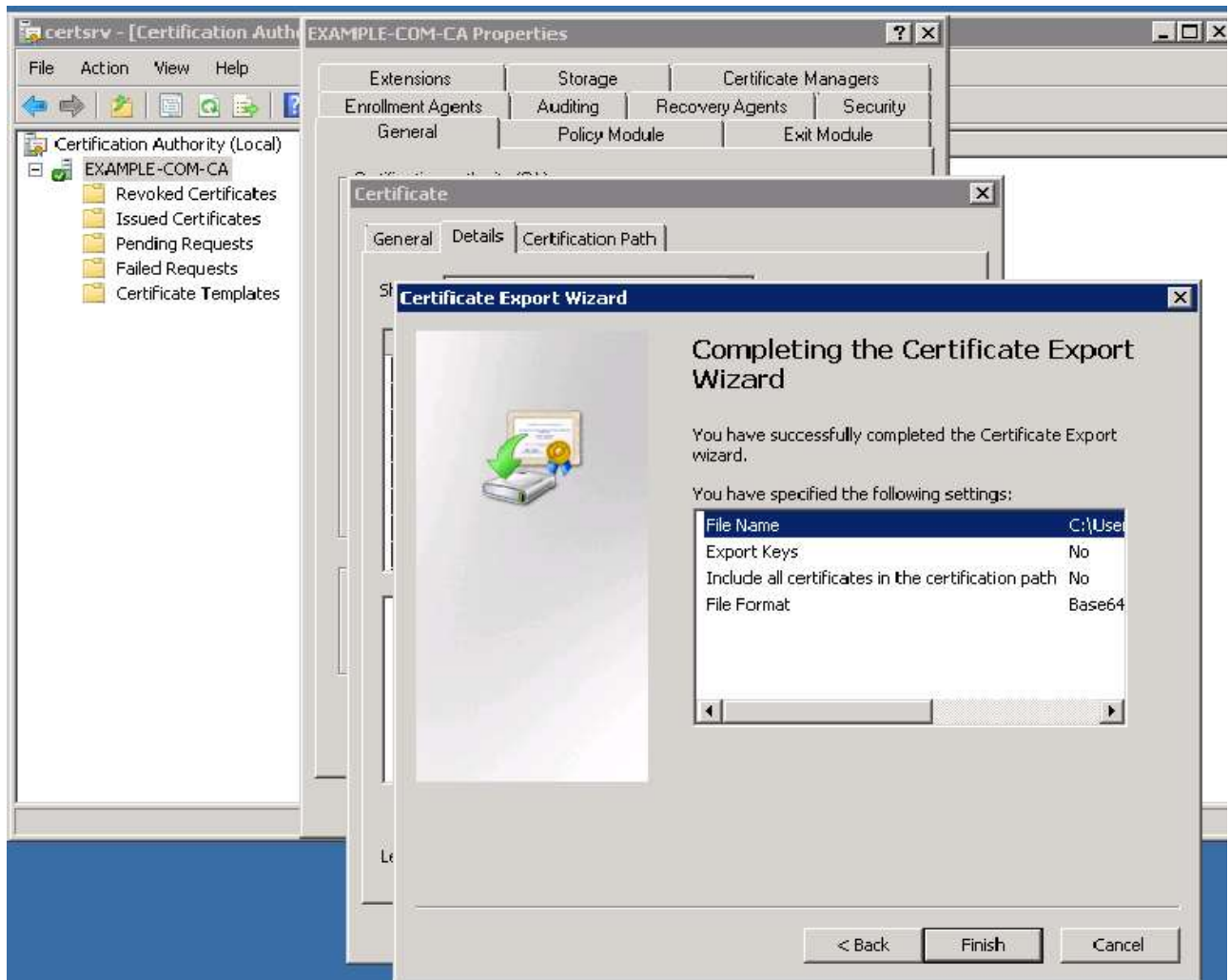
6. Select **Base-64 encoded X.509** option to export the CA certificate in ASCII mode:



7. Specify the path and file name of the CA certificate to export:



8. Review the details of the CA certificate export wizard and click on **Finish** to complete the export process:



9. Alternatively, Active Directory CA certificates can be generated from the **Windows Command Prompt** seen here:

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>certutil -ca.cert c:\Users\Administrator\Desktop\EXAMPLE-CA.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDaTCCA1GgAwIBAgIQD5BeQB5SxqPJxPAyUEuAHDANBgkqhkiG9w0BAQUFADBH
MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCZImiZPyLGBGRYHhZhhbXsZTEx
MBUGA1UEAxMORUhhbTUBMRs1DT00tQ0EwHhcNMjUwOTU0MDEzMzUwOTU0MDE0
MDE0MzA2WjBhMRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCZImiZPyLGBGRYH
ZXhhbXsZTExMBUGA1UEAxMORUhhbTUBMRs1DT00tQ0EwggEiMA0GCSqGSIb3DQEB
AQUAA41BDwAwggEKAoIBAQDJJQ+uUFUZYPLhKooG1MNjkk5wWUz1+flsU/kNMCi
p1nAuSBgU8ZdkDGW9uhsRPTPfP7eG4xfi6D/9NGI3h6OZDZh26hGF5fW53Iak0NT
cYiLOYFPEAgfK2KF3P1aBch6ifC9m00eh97001aJRA04XQBRUk35E/RargAKUAM
L2Ukkg6emsAPBCeAIXBzr/8e/qPk1v19Sxqe3pWwIUc+lgOk/eGbsrR3cR1NPurQ
yubh4YzneUBGno26Gw7vS3bZPcMC5RsEH5vUUiitt/P90RCdkdggx/jU546YU0eF
XUhoQtnX+GfHzKBiZLjyeMGtJ5XjHSsixa9LdIf3A3dAgMBAAGjUTBPMAsGA1Ud
DwQEAwIBhJAAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbT70r2eb0sBLLJXCC5p
OqTJWbXv0DAQBgkrBgEAAyI3FQEEAwIBADANBgkqhkiG9w0BAQUFAAOCQAQEAoprI
A45EbH84WjQUGCgpJZLCY9TwdFpP6H/ME1gntFcm+9Ug19v/uU0/PyAuoJqs/gcL
mlws6GjxCU+xxnKUWjBvAwoHs8A8x01nP1uP09Brnx91whp+MK4Zz0r0cU0H
X1pUIE1UG/6v1OC1ehIwYPa/Xc1thHnZq4G715jpQycU11tg1A/9nizmMvNmJm3ma
41Zw95Q6EdLUSeho0hpr1yAdinLPnXUMtm7asf0LSqZ1BsWxxf2QhiauW3QdD/v0
x42PxDkP1J4ShlwK5ec/jNLDB94fmL0z0Xv23DwDdWC0EcmMfG0qvBuLCHYzrZzv
qeoKu56oSwZ0zDXSog==
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.

C:\Users\Administrator>

```


10. Copy over the exported CA Certificate file to the Red Hat Satellite 6.3 or later server and execute the following commands:

```
# openssl x509 -inform DER -in EXAMPLE-CA.cer -out example.crt # install example.crt /etc/pki/tls/certs/ # ln -s example.crt /etc/pki/tls/certs/$(openssl x509 -noout -hash -in /etc/pki/tls/certs/example.crt).0
```

- **Note:** Make sure the certificate is in **PEM** format (Example: example.crt). Ensure the **CA chain** is complete and has all the required Certificate Authorities inside the bundle. (Root + Intermediate CAs).

```
# openssl s_client -connect <FQDN_AD>:636 -CAfile example.crt -showcerts -state
```

11. Restart the httpd service:

- RHEL 7:

```
[root@satellite ~]# systemctl restart httpd.service
```

- RHEL 6:

```
[root@satellite ~]# service httpd restart
```

12. Configure LDAP Authentication on Red Hat Satellite 6.1. Click **Administer** ---> **LDAP authentication** and configure it as per the following screenshots:

LDAP server

Account

Attribute mappings

Name *

Active Directory

Server *

dc.example.com

LDAPS

☒

Port *

636

Server type *

Active Directory

Cancel

Submit

LDAP server

Account

Attribute mappings

Account username

EXAMPLE\satellite

Use this account to authenticate, *optional*

Account password

Use this account to authenticate, *optional*

Base DN

DC=example,DC=com

Groups base DN

LDAP filter

Automatically create accounts in Foreman

☒

LDAP users will have their Satellite 6 account automatically created the first time they log into Satellite 6

Cancel

Submit

LDAP server

Account

Attribute mappings

Locations

Organizations

Attr Login

sAMAccountName OR userPrincipalName

e.g. uid

Attr Firstname

givenName

e.g. givenName

Attr Lastname

sn

e.g. sn

Attr Mail

mail

e.g. mail