APPLICATION NOTE

BECKMAN COULTER
Life Sciences

MET ONE 3400+ LDAP & Active Directory connection Guide

Revision C

1. Revision History

Revision	Date of last Revision	Reason for Change
A	29-APR-2021	Created initial document
B	02-JUN-2021	Added info about case sensitive group names to 5
C	17-NOV-2021	Changed explanation for TLS ON/OFF in section 5

2. Preface

This document describes the steps necessary to connect the MET ONE 3400+ to a network using Lightweight Active Directory (LDAP) and Microsoft Active Directory. After the connection is established, you will be able to logon via the WebGUI and the local interface of the MET ONE 3400+ with domain credentials, which are mapped to one of the three roles in the MET ONE 3400+: Admin, Manager, Technician.

3. Requirements

In order to successfully connect, the following requirements must be met:

- MET ONE 3400+ should be running version 1.0.13 or above
- MET ONE 3400+ must be connected via Wifi or cable to the local network
- Port 636 on the designated or local Windows Domain Controller (DC) must be reachable from the MET ONE 3400+
- Active Directory (AD) must be set up for encrypted LDAP (LDAPS). [Steps necessary are explained in this guide]
- LDAPS requires the issuing of a certificate for the DC, which can either be done from an internal or 3rd party Certification Authority (CA). Also, you will need to export the public key from the mentioned certificate and import it as an *.CER file into the MET ONE 3400+. The used certificate must be valid for Server Authentication, so it must contain the “Extended Usage OID” 1.3.6.1.5.5.7.3.1 [Steps necessary are explained in this guide]
- You will need the Fully Qualified Domain Name (FQDN) of DC and the name of the Windows Domain.
- A minimum of one AD group (should include one or more users) which will be mapped to either Admin, Manager or Technician role on the MET ONE 3400+

4. Active Directory Configuration

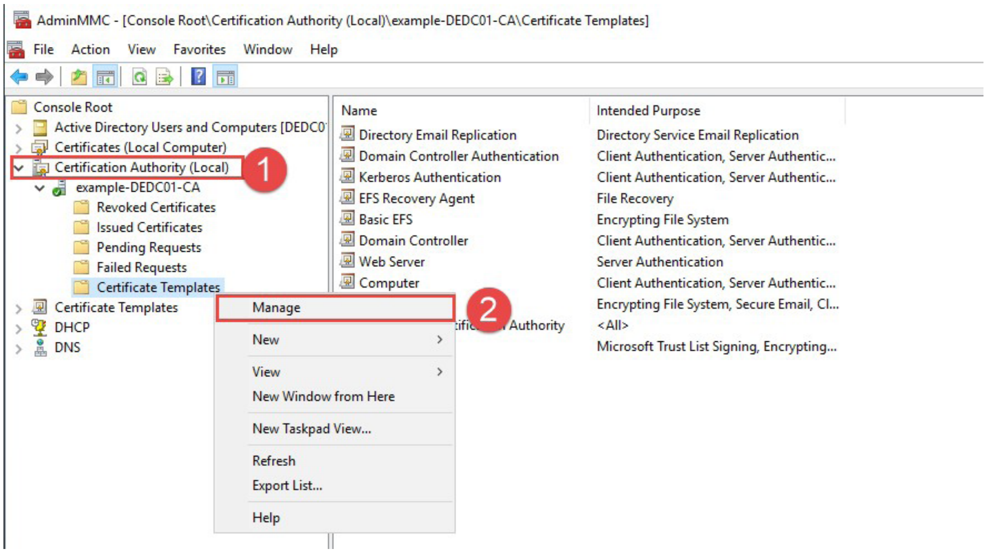
4.1 LDAPS

If LDAPS is already deployed for AD you can skip this paragraph and jump to 4.2.

In order to enable LDAPS you'll need to issue a certificate for the DC. This can be done using an internal CA which is the scenario explained here. I assume that the CA is already deployed; instructions for this are beyond the scope of this guide. If you cannot use an internal CA then you'll have to request a certificate from a 3rd party CA, which is also beyond the scope of this guide.

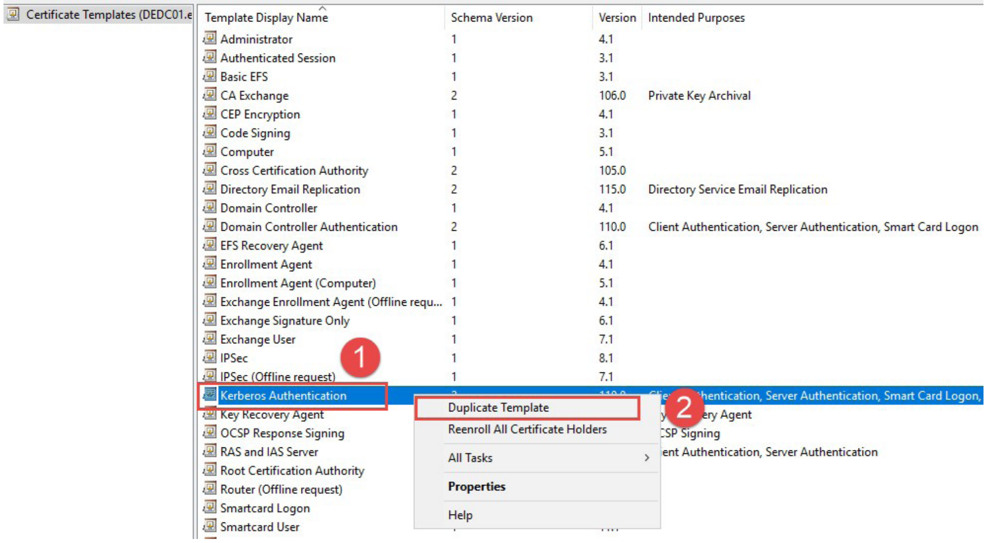
4.1.1 Create Certificate Template

Log on to the CA Management console and right click on "Templates", choose "Manage".



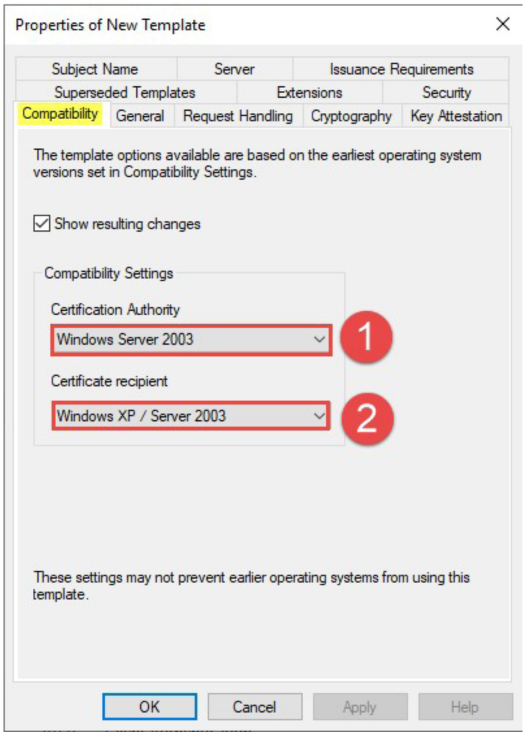
Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
ific Authority	<All>
	Microsoft Trust List Signing, Encrypting...

Right click "Kerberos Authentication" and choose "Duplicate Template".


Certificate Templates (DEDC01.e
1
2
Duplicate Template
Reenroll All Certificate Holders
All Tasks
Properties
Help

Template Display Name	Schema Version	Version	Intended Purposes
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication			hentication, Server Authentication, Smart Card Logon,
Key Recovery Agent			ery Agent
OCSP Response Signing			CSP Signing
RAS and IAS Server			ent Authentication, Server Authentication
Root Certification Authority			
Router (Offline request)			
Smartcard Logon			
Smartcard User			

Configure the Template according to the following screenshots; at the end click “Apply” and “Ok” to save the settings:



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

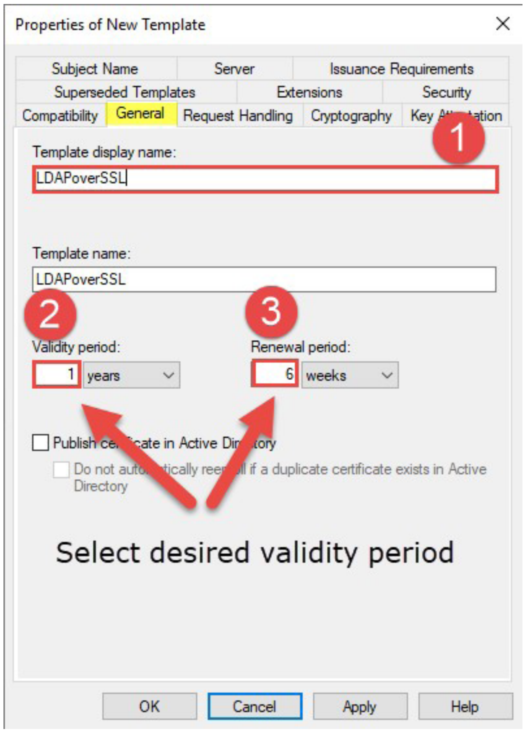
Certification Authority

Windows Server 2003

Certificate recipient

Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.



Template display name:

LDAPoverSSL

Template name:

LDAPoverSSL

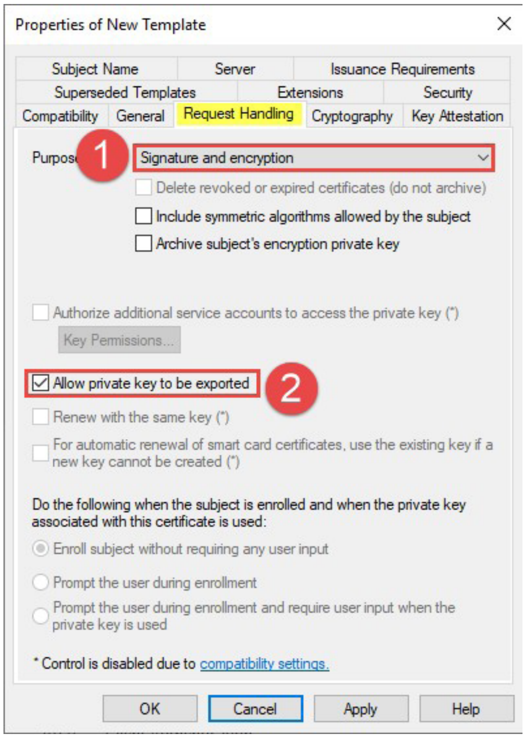
Validity period: 1 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

Select desired validity period



Properties of New Template

Subject Name | Server | Issuance Requirements
Superseded Templates | Extensions | Security
Compatibility | General | Request Handling | Cryptography | Key Attestation

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)
□ Include symmetric algorithms allowed by the subject
□ Archive subject's encryption private key

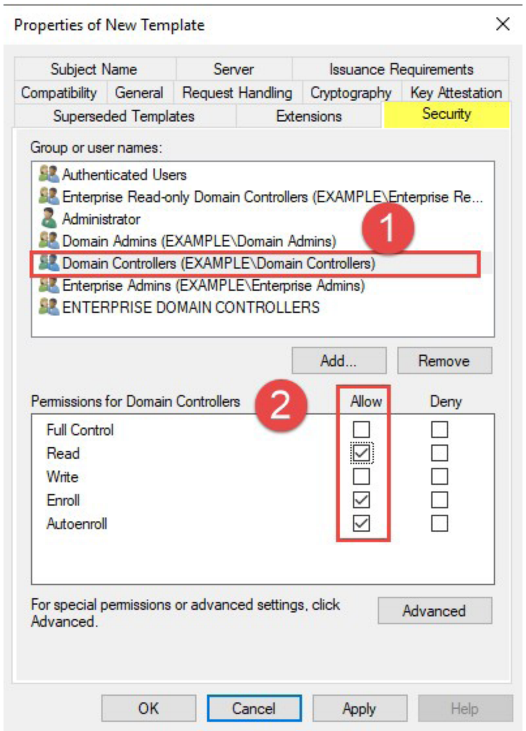
□ Authorize additional service accounts to access the private key (*)
Key Permissions...

☑ Allow private key to be exported
□ Renew with the same key (*)
□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input
○ Prompt the user during enrollment
○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



Properties of New Template

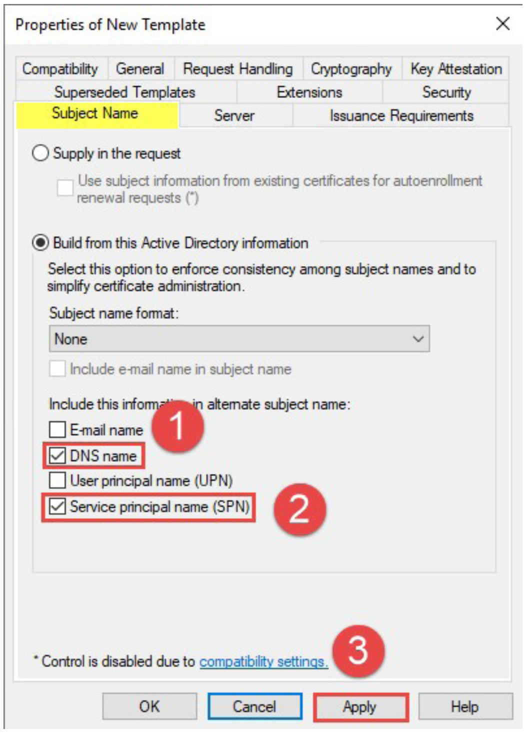
Subject Name | Server | Issuance Requirements
Compatibility | General | Request Handling | Cryptography | Key Attestation
Superseded Templates | Extensions | Security

Group or user names:

- Authenticated Users
- Enterprise Read-only Domain Controllers (EXAMPLE\Enterprise Re...
- Administrator
- Domain Admins (EXAMPLE\Domain Admins)
- Domain Controllers (EXAMPLE\Domain Controllers)
- Enterprise Admins (EXAMPLE\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Domain Controllers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

☑ DNS name

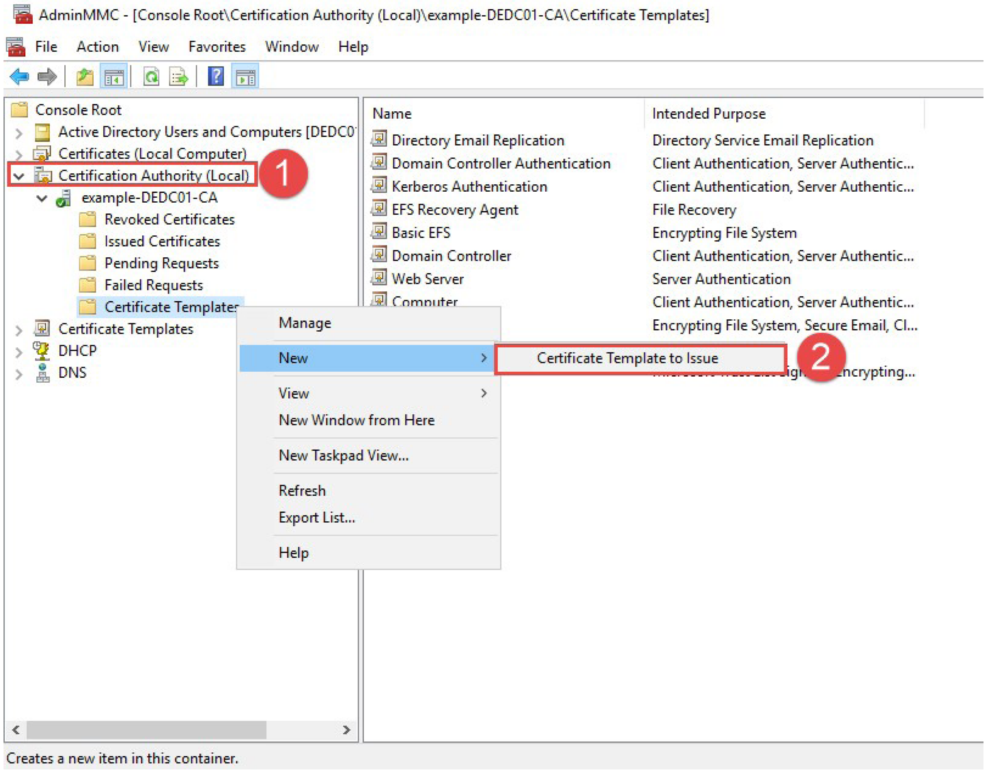
□ User principal name (UPN)

☑ Service principal name (SPN)

* Control is disabled due to compatibility settings.

Close the “Certificate Templates Console” and return to the “Certificate Authority Console”.

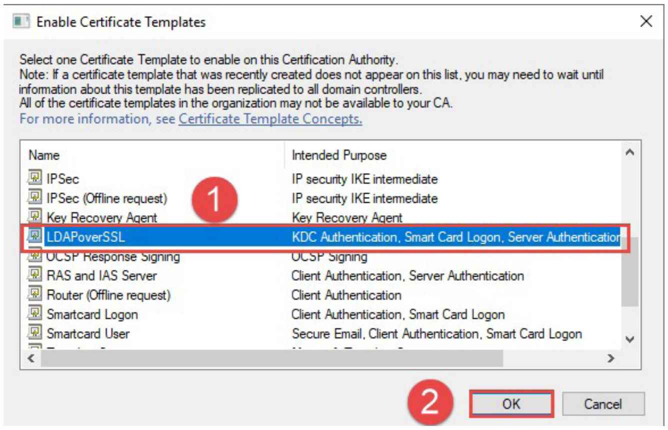
Right click “Certificate Templates” and select “New → Certificate Template to Issue”.



AdminMMC - [Console Root\Certification Authority (Local)\example-DEDC01-CA\Certificate Templates]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Users and Computers [DEDC0
Certificates (Local Computer)
Certification Authority (Local)
1
example-DEDC01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Certificate Templates
DHCP
DNS
Manage
New
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Certificate Template to Issue
2
Creates a new item in this container.

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
	...ncrypting...

Choose the created Template “LDAPoverSSL” and confirm with “OK”.



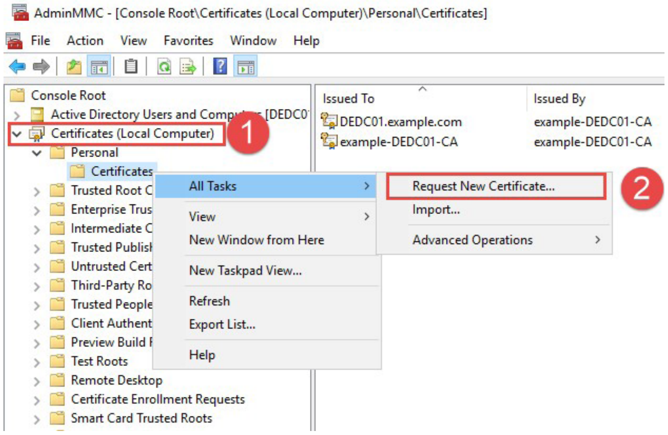
Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
LDAPoverSSL	KDC Authentication, Smart Card Logon, Server Authentication
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon

4.1.2 Issue certificate to DC

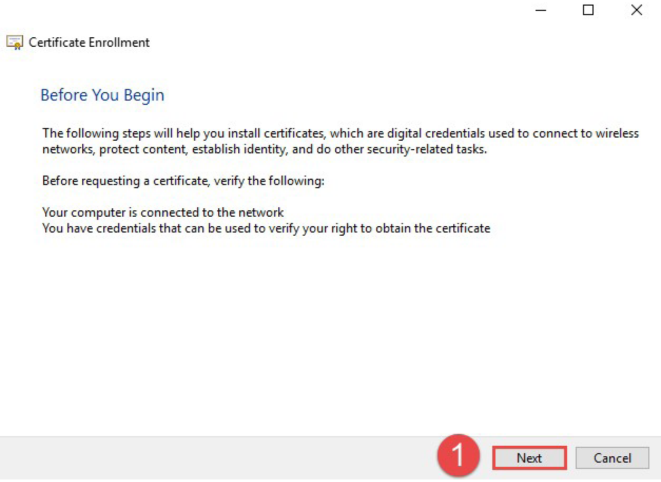
Open the “Certificates Console” for the local computer on the DC and right click on “Certificates,” then choose “All Tasks →Request a New Certificate…”.



AdminMMC - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By
DEDC01.example.com	example-DEDC01-CA
example-DEDC01-CA	example-DEDC01-CA

Proceed as shown in the following screenshots:



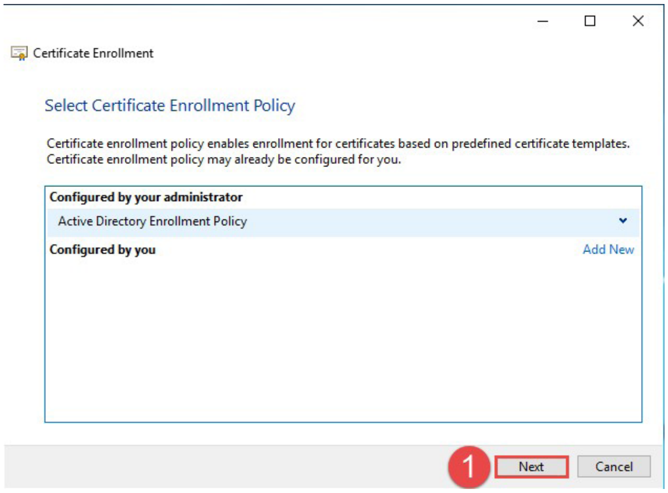
Certificate Enrollment

Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate



Certificate Enrollment

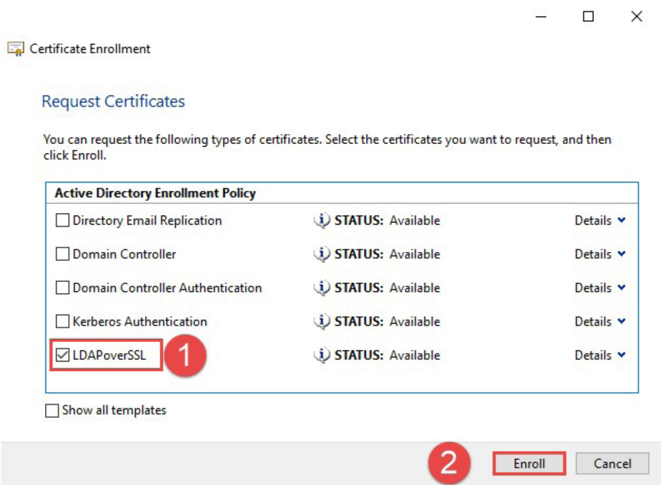
Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you



Certificate Enrollment

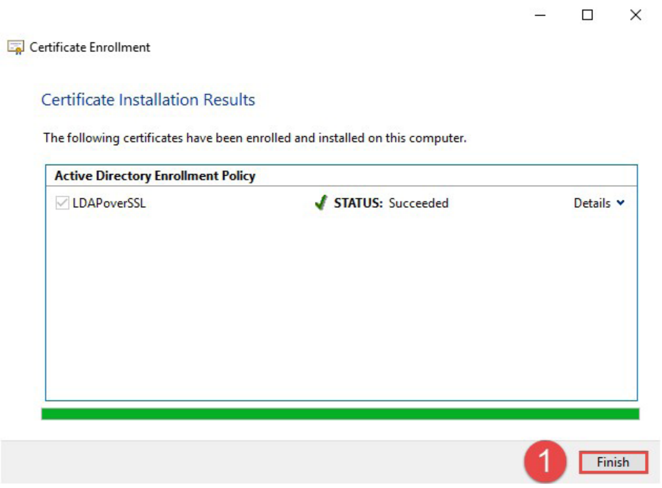
Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

☐ Directory Email Replication	**STATUS:** Available	Details
☐ Domain Controller	**STATUS:** Available	Details
☐ Domain Controller Authentication	**STATUS:** Available	Details
☐ Kerberos Authentication	**STATUS:** Available	Details
☑ LDAPoverSSL	**STATUS:** Available	Details

☐ Show all templates



Certificate Enrollment

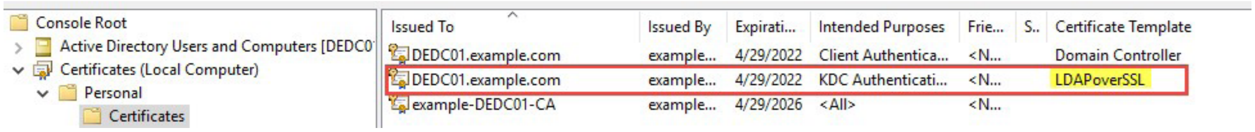
Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

☑ LDAPoverSSL	✓ **STATUS:** Succeeded	Details

The issued certificate will now show up in the console; you can verify the template used in the column “Certificate Template”.


Console Root
Active Directory Users and Computers [DEDC0
Certificates (Local Computer)
Personal
Certificates

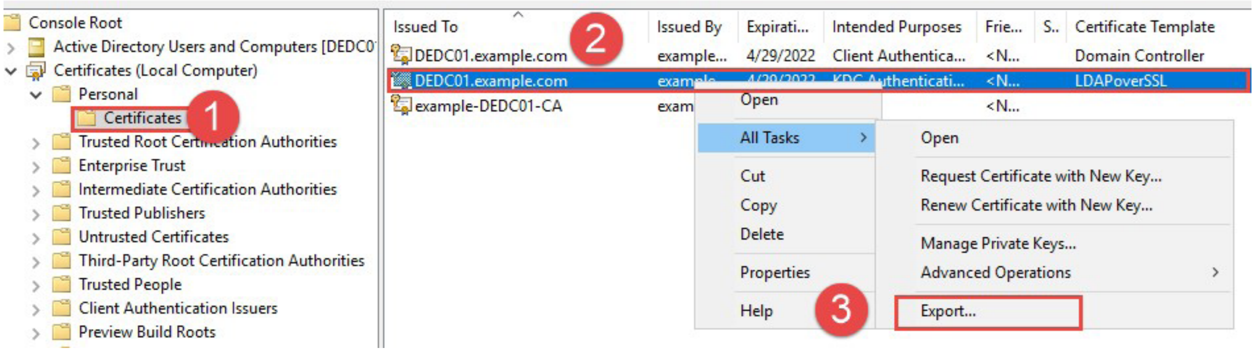
Issued To	Issued By	Expirati...	Intended Purposes	Frie...	S..	Certificate Template
DEDC01.example.com	example...	4/29/2022	Client Authentica...	<N...		Domain Controller
DEDC01.example.com	example...	4/29/2022	KDC Authenticati...	<N...		LDAPoverSSL
example-DEDC01-CA	example...	4/29/2026	<All>	<N...		

In order to activate LDAPS you may need to reboot the DC.

4.2 Export certificate

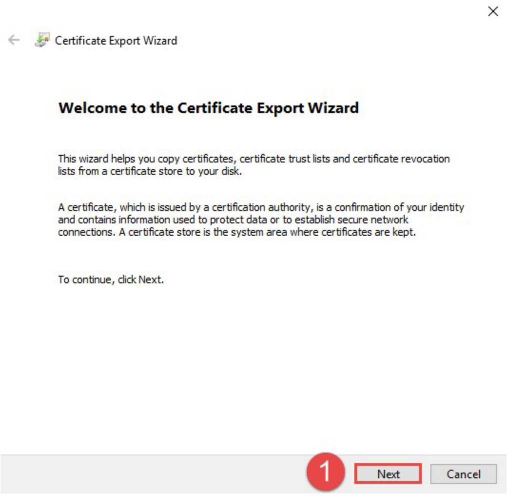
If you requested a certificate for the DC from a 3rd party CA please adjust the instructions according to your certificate name.

Open the “Certificates Console” for the local computer on the DC. Right click the issued certificate found in “Personal → Certificates” and select “Export…”.


Console Root
Active Directory Users and Computers [DEDC0
Certificates (Local Computer)
Personal
Certificates
1
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
2
Open
All Tasks
Cut
Copy
Delete
Properties
Help
3
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

Issued To	Issued By	Expirati...	Intended Purposes	Frie...	S..	Certificate Template
DEDC01.example.com	example...	4/29/2022	Client Authentica...	<N...		Domain Controller
DEDC01.example.com	example...	4/29/2022	KDC Authenticati...	<N...		LDAPoverSSL
example-DEDC01-CA	exam			<N...		

Proceed as shown in the following screenshots:

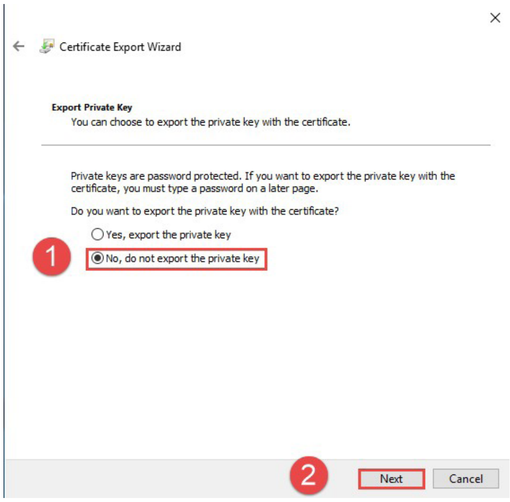


Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Export Wizard

Export Private Key

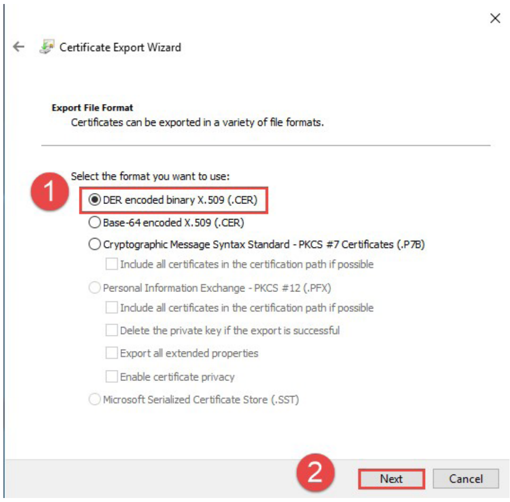
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

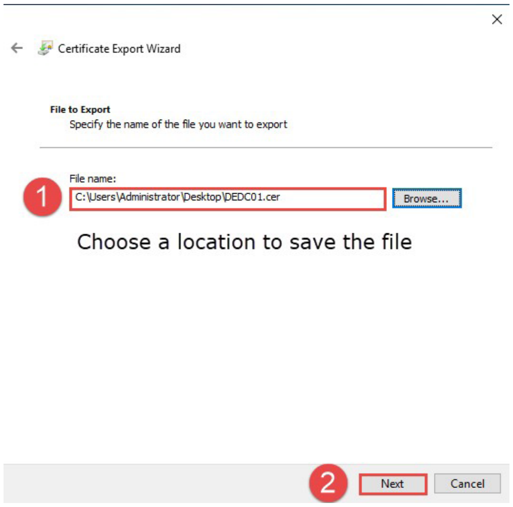
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

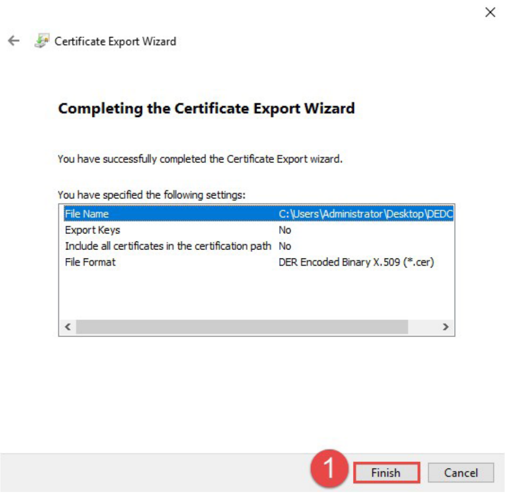
File to Export

Specify the name of the file you want to export

File name:

C:\Users\Administrator\Desktop\DEDC01.cer

Choose a location to save the file



Certificate Export Wizard

Completing the Certificate Export Wizard

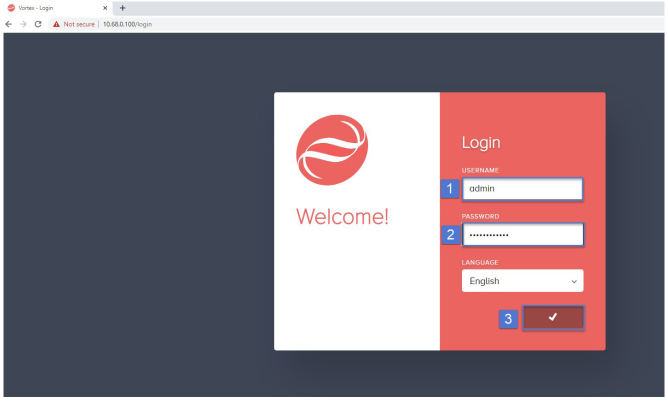
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\DEDC
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

5. LDAP configuration MET ONE 3400+

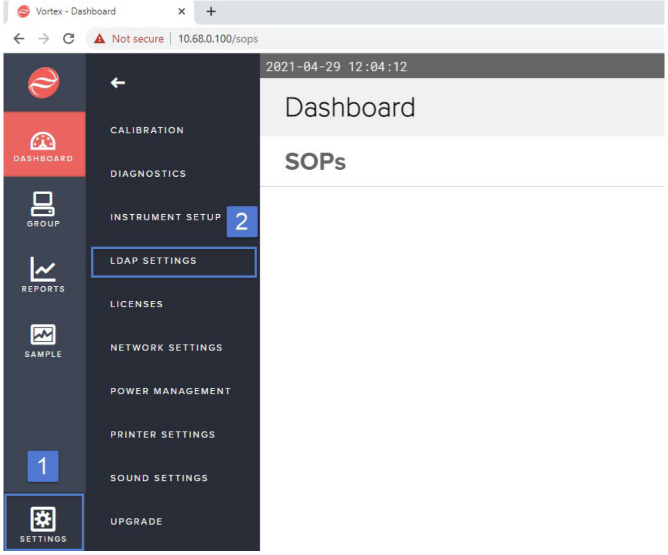
Log on the WebGUI of the MET ONE 3400+ with an admin account via web browser (Chrome is preferred).



Vortex - Login

Not secure | 10.68.0.100/login

Select “Settings → LDAP Settings” from the left column.



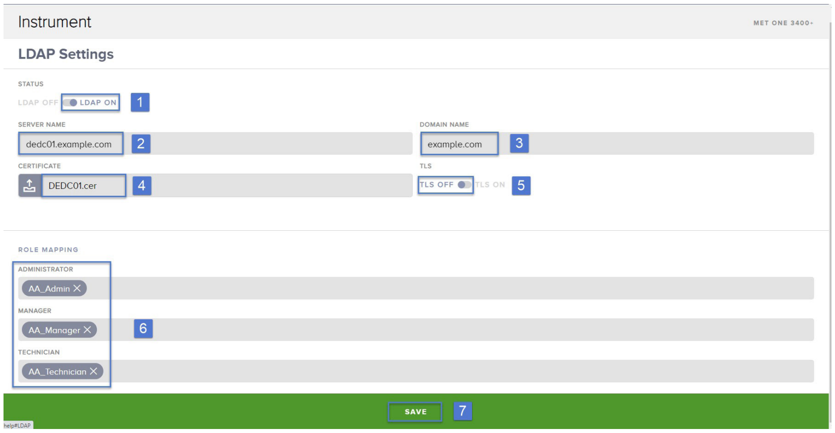
Vortex - Dashboard

Not secure | 10.68.0.100/sops

2021-04-29 12:04:12

1. Enable LDAP Settings.
2. Insert FQDN of DC (e.g. server.target.com or server.low.target.com).
3. Insert domain name (e.g. target.com or low.target.com).
4. Choose *.CER file exported in 4.2.
5. Switch TLS to "TLS OFF" in order to use port 636; "TLS ON" would use port 389 which is used for unencrypted traffic or encrypted traffic with LDAP START_TLS command in MS AD.
6. Insert at least one AD group (**NOTE:** The AD group names are case sensitive; be sure to write them as they appear in your MS AD).
7. Hit "Save".

See next Page for screenshot.



Instrument

LDAP Settings

STATUS: LDAP OFF ● LDAP ON 1

SERVER NAME: dedc01.example.com 2

DOMAIN NAME: example.com 3

CERTIFICATE: DEDC01.cer 4

TLS: TLS OFF ● TLS ON 5

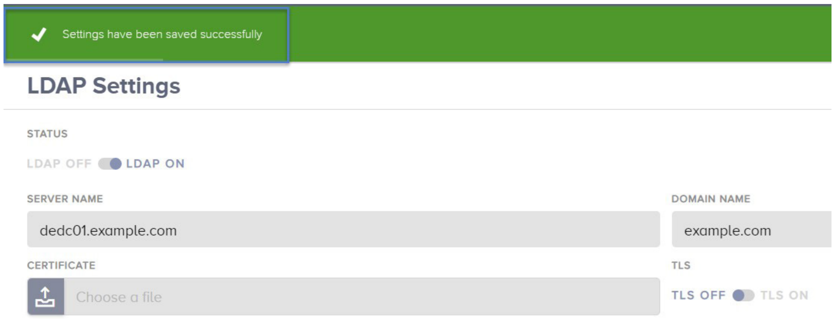
ROLE MAPPING

ADMINISTRATOR: AA_Admin ✕

MANAGER: AA_Manager ✕ 6

TECHNICIAN: AA_Technician ✕

A green label appears to indicate success.



✓ Settings have been saved successfully

LDAP Settings

STATUS: LDAP OFF ● LDAP ON

SERVER NAME: dedc01.example.com

DOMAIN NAME: example.com

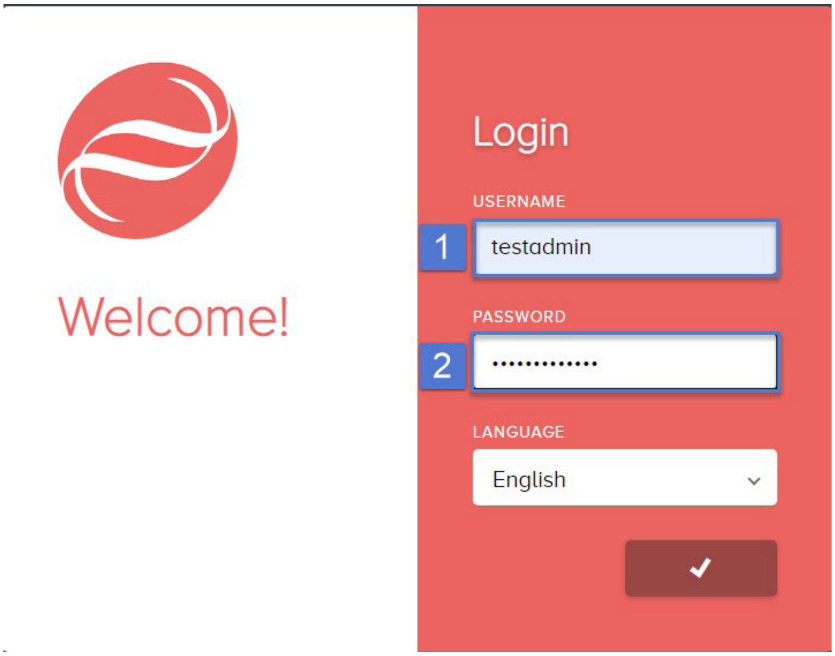
CERTIFICATE: Choose a file

TLS: TLS OFF ● TLS ON

5.1 MET ONE 3400+ login with domain credentials

If not already done, log off from the MET ONE 3400+ WebGUI and log in again using AD credentials.

1. USERNAME: Use the plain username **NO** AD extension (e.g. AD Logon name “testadmin@example.com” just use “testadmin”)
2. PASSWORD: AD username’s password



Login

USERNAME

1 testadmin

PASSWORD

2 •••••••••••••

LANGUAGE

English

For Beckman Coulter’s worldwide office locations and phone numbers, please visit Contact Us at beckman.com