1. Revision History

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

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”.

Right click “Kerberos Authentication” and choose “Duplicate Template”:
Configure the Template according to the following screenshots; at the end click “Apply” and “Ok” to save the settings:
Close the “Certificate Templates Console” and return to the “Certificate Authority Console.

Right click “Certificate Templates” and select “New → Certificate Template to Issue”.
Choose the created Template “LDAPoverSSL” and confirm with “OK”.

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...”.

Proceed as shown in the following screenshots:
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
- Configured by you

Next  Cancel

Certificate Enrollment

Request Certificates

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

- Directory Email Replication
- Domain Controller
- Domain Controller Authentication
- Kerberos Authentication
- LDAP/PowerSSL

Show all templates

Email  Cancel

Certificate Enrollment

Certificate Installation Results

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

- Directory Email Replication
- Domain Controller
- Domain Controller Authentication
- Kerberos Authentication
- LDAP/PowerSSL

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

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...”.

Proceed as shown in the following screenshots:
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).

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

A green label appears to indicate success.
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