

Setting Up OpenVMS Users Active Directory Authentication

1 General Description and Prerequisites

This document describes setting up the Active Directory (AD) Authentication on the OpenVMS workstation(s) connected to a Windows domain.

The purpose of this document is to unify the user authentication process for all of the existing computers on a particular Windows domain, regardless of the computer type and operating system (OS), as long as it is either Windows or OpenVMS. As soon as a user attempts to login to a workstation, the OS acquires the username and password. These are verified by the domain controller against the AD database. As a result, locally defined passwords become irrelevant (except in rare cases where a user tries to login to an OpenVMS workstation locally).

Therefore, in order to log into SCADA, a user must have both the AD (domain) account and the VMS account (on all VMS nodes this must have the right to login). Additionally, the user's VMS account should be configured to allow external (relative to the node) authentication. If the user does not have an OpenVMS account on a particular node(s) or the account is not properly configured, logging in to SCADA will not be possible.

The list of prerequisites that need to be met in order to make the setup successful, are as follows:

- OpenVMS workstations (Nodes) are not clustered. However, this may change in the future and will be appropriately documented.
- All nodes should run OpenVMS version 8.4.2 or later. For older versions, the procedure should be retested and revised, if necessary.
- Not all accounts can be externally authenticated. Only specific customer accounts are allowed to be treated this way (otherwise, MISER – or even the whole OpenVMS system – would become dysfunctional or unsupported). There are three service accounts that intentionally are not configured to allow the AD authentication. These are: "hsq", "system", and "ucx".
- A person performing this procedure should have system privileges in order to perform the setup successfully.

2 Setup Overview

The steps to perform the setup are:

1. Collect information about the Windows domain and system users from the customer.
2. Create setup files (by HSQ personnel) based on the collected data (development stage).
3. Copy the setup files onto one of the customer nodes.
4. Run the setup command procedure.
5. Reboot all the nodes.

These steps are described in detail below.

3 Collecting Customer-Related Information

There are several items that the customer must provide prior to the actual development:

- The IP address (DNS name) of the authenticating server.
- The name of a proxy user account to be used by LDAP service.
- The password for the proxy account.
- Location in the directory where the authentication records are kept.
- A list of usernames to be externally authenticated. This list must contain two usernames for every user account (Windows AD username and OpenVMS username), which may be the same or different for each user.

NOTE: For ease of system maintenance, it is recommended that these names be identical.

The User List can be modified at any time (as described below).

Refer to [Appendix A – Customer Inquiry Form](#) for the inquiry form template.

4 Creating Setup Files

This step is performed by HSQ technicians and is described in a different HSQ-internal User Note (*AD-LDAP Authentication*). This produces several files:

- An LDAP ACME configuration file (`LDAPACME$CONFIG-STD.INI`) along with the `LDAPACME$CONFIG-STD.INI_TEMPLATE` default version of this file provided by VMS.
- An LDAP username database (`LDAP_LOCALUSER_DATABASE.TXT`).
- An ACME start file (`ACME$START.COM`) and its original version: `ACME$START.COM_TEMPLATE`.
- A user account modification file (`LDAP_ACCOUNTMODIFY.COM`).
- A command file disassociating the user accounts from external authentication (`LDAP_ACCOUNTOFF.COM`).
- A VMS system startup command file (`SYSTARTUP_VMS.COM`) along with the default: `SYSTARTUP_VMS.COM_TEMPLATE` version of this file.

OPENVMS ACTIVE DIRECTORY AUTHENTICATION

- An ACME system installation file (SYS\$LOGIN_SWITCH.COM) as well as the default file version: SYS\$LOGIN_SWITCH.COM_TEMPLATE.
- A command file performing the per-node AD authentication setup (AD_NODE_SETUP.COM).
- A command file initiating the network-wide setup (AD_SETUP.COM).
- A command file initiating the local node setup (AD_SETUP_LOCAL.COM).
- A command file setting up AD authentication for a new user (AD_NEWUSER.COM).
- A command file turning off AD authentication (AD_UNINSTALL.COM).

These files comprise two groups: those used only during the setup procedure and those used during system use. Therefore, it is very important to maintain the files belonging to the second group secure (while the rest can be easily backed up and/or removed from the system). The critical files are:

- The LDAP ACME configuration file (LDAPACME\$CONFIG-STD.INI).
- The LDAP username database (LDAP_LOCALUSER_DATABASE.TXT).
- The ACME start file (ACME\$START.COM).
- The VMS system startup command file (SYSTARTUP_VMS.COM).
- The command file setting up AD authentication for a new user (AD_NEWUSER.COM).

5 Copying the Setup Files and Running Setup

While performing the setup (installer) the HSQ engineer connects to one of the customer's nodes while having all of the setup files available. All of these files should be copied to an arbitrary (distribution) directory (by default, the installer's home directory).

REMINDER: The account that is used should have system rights in order to make the setup successful.

As soon as the files are copied, the procedure can be started. In order to start it, the command below should be issued (if repeated, it should still be started from the distribution directory):

```
$ @AD_SETUP
```

Or, if the AD Authentication is to be installed only on one node (e.g., after adding a new node to the system, where all of the other nodes are already have it installed), the command should look like below:

```
$ @AD_SETUP_LOCAL
```

NOTE: After the procedure is completed, every effected node needs to be rebooted in order to make the new functionality available. The node(s) rebooting schedule is beyond the scope of this document and must be performed by the customer.

As soon as the procedure is successfully executed, the AD Authentication is ready for use.

6 Making Changes to the User Database

As long as the AD Authentication is setup and working properly on all system nodes, a new user may be added who would also be externally authenticated.

In order to do that, a user should login with system privileges and:

- Run the **UAL MISER** utility to add the user to the SYSUAF database (follow the UAL prompts and answer the questions).
- Run the new user AD Authentication command file (`AD_NEWUSER.COM`) by entering:

```
$ @SYS$MANAGER:AD_NEWUSER < Win_username> [<VMS_username>]
```

Where, <Win_username> is the Windows username for the added account, while <VMS_username> denotes the corresponding OpenVMS account name.

If the username contains blank spaces, they should be in quotes.

If the second parameter)<VMS_username>) is omitted, the command file assumes these names are identical.

7 Turning AD Authentication Off

It may become necessary under the circumstances to reinstate the traditional SYSUAF-based user authentication on the VMS nodes. In order to do this:

- Run the uninstall command file:

```
$ @SYS$MANAGER:AD_UNINSTALL [ALL]
```

When the "ALL" parameter is not present, the uninstallation gets performed on the current node only, while if it is specified, it affects all currently connected nodes.

- Manually reboot the affected node(s).

OPENVMS ACTIVE DIRECTORY AUTHENTICATION

Appendix A Customer Inquiry Form

- IP address (DNS name) of an authenticating server: _____

- Distinguished name of a proxy user account to be used by the LDAP service:

- Password for the above proxy account: _____

- Location in the directory where the authentication records are kept:

- List of usernames:

	<u>Windows (AD) username</u>	<u>VMS username (if different)</u>
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____
6.	_____	_____
7.	_____	_____
8.	_____	_____
9.	_____	_____
10.	_____	_____
11.	_____	_____
12.	_____	_____
13.	_____	_____
14.	_____	_____
15.	_____	_____
16.	_____	_____

Use additional sheet(s) if needed.