



How to change passwords for AD Users UDS 4.0



#SmartDigitalWorkplace
VIRTUAL CABLE

Index

Introduction	2
Import and configure the Virtual Appliance	3
Publish access to the credential change server	6
User with permissions to modify credentials	9
Redirect on expired Parameter	11
THE SMART DIGITAL WORKPLACE SOLUTION BY VIRTUAL CABLE	12
About UDS Enterprise.....	12
About Virtual Cable	12

Introduction

This document guides the administrators of a VDI environment with UDS Enterprise through the implementation of an alternative method to allow changing passwords to users belonging to a Microsoft “**Active Directory**” (AD) authenticator.

The procedure will require a new virtual machine (provided by the UDS Enterprise team in Virtual Appliance format). It will be necessary to import it to the virtual platform used.

This method, in addition to allowing the modification of a user’s password at any time, may also be used to indicate a new password to users who, due to security policies, need to change it because of the expiration of the current one.

The main requirements to change a user’s password are:

- **Resources for the Virtual Appliance:** 2 vCPU, 1024 MB of vRAM and 4 GB of disk space.
- **“Active Directory” server configuration:** It is necessary that the communication between UDS Server and the Ad Server is performed via LDAPS (LDAP over SSL).
- **Credentials:** A user with permissions will be required to modify the credentials of the users (it is not necessary to use an administrator user, the delegation of permissions can be used).

Import and configure the Virtual Appliance

The first task that you will perform in order to enable the change of passwords of users of an “**Active Directory**” directly from the UDS Enterprise VDI environment will be to import a server in Virtual Appliance format.

This VM is available for download in OVA format in the following repository:

<http://images.udsenderprise.com/files/AD-Password-Changer/>

NOTE: If you need to have this server in another format, it is recommended to decompress the *.ova file and extract the *.vmdk disk, which can be converted to other formats (.vhd, .qcow2, etc...) with tools such as [qemu-img](#), [StarWind](#), etc...

```
Debian GNU/Linux 11 uds tty1
Hint: Num Lock on
uds login: _
```

Login to the machine with the following credentials:

- User: root
- Password: uds

```

IMPORTANT NOTES:
* This machine is provided as a very basic Active Directory web password updater server, without any security add-on.
* Change root password (ssh root login is ENABLED by default)
* Provide a custom name for this machine. you can use hostnamectl set-hostname --static YOUR_SERVER_NAME to do this.
* Protect access to this machine, because it contains defaults that are publicly available, such as root password.
* Consider updating the software (using apt, dselect, etc..) as a first step before using it in any environment (production or not)
* Update the keyboard layout if needed: use dpkg-reconfigure keyboard-configuration, then service keyboard-setup restart for this. Default keyboard lang is Spanish
* Set the timezone: use dpkg-reconfigure tzdata

You will need to take security actions (such as changing passwords, enabling firewall, etc...) in order to secure this machine.

Remember to setup your installation editing the file on: /var/server/server/settings.py

Default listen address of nginx server: 0.0.0.0 (all addresses)

Default network mode: DHCP

Last login: Wed Mar  9 10:27:49 CET 2022 on tty1
Detected IP: 192.168.111.139
root@adpw:~# _

```

Once the session is started, you will be able to see different notes to help with the configuration of this machine:

- You can change the name (Hostname) of the machine with the command:
`hostname set-hostname --static YOUR_SERVER`
- Change the keyboard layout with the command:
`dpkg-reconfigure keyboard-configuration`
- Change the time zone with the command:
`dpkg-reconfigure tzdata`

The network configuration of the machine is configured via DHCP by default, so you must indicate a static IP address. In order to do this, edit the file `/etc/network/interfaces` and indicate a static IP address:

```

GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens160
iface ens160 inet static
    address 192.168.0.9
    netmask 255.255.240.0
    gateway 192.168.0.1
    
```

Once you have the new server with IP connectivity, configure the script responsible for connecting to the AD server to modify the password of the users.

Edit the file `/var/server/server/settings.py` and indicate the following data:

```

GNU nano 5.4 settings.py *
#####
Settings for the server.
#####

import os
import django

# Start settings for AD. Customize THIS
AD_SERVER = '192.168.0.9' # Server. Must support LDAPS or change password will not work
AD_BASEDN = 'dc=uds,dc=local'
AD_USER = 'administrator@vc.local' # Must be an administrator user
AD_PASSWORD = 'KNeLbHGtK22' # Password for this user
UDS_BROKER = 'https://demo.udsenterprise.com' # UDS Broker URL
# End settings
# SECURITY WARNING: keep the secret key used in production secret!
SECRET_KEY = '88d5o-%1t)_q5113#kmago-a&ox5i+aci5511j27'
    
```

- **AD_Server:** IP address or name of the AD Server (for proper operation, the SSL connection must be enabled on the server).
- **AD_BASEDN:** Indicate the DN BASE in this format: `dc=xxx,dc=xxx`
- **AD_USER:** User with permissions that will be used to change the password (it does not need to be an administrator user; delegated permissions can be used).
- **AD_PASSWORD:** Password of the user “AD_USER”.
- **UDS Broker:** IP address of the UDS Server where the user will be redirected.

Once all the data necessary for integration with AD are configured, save the changes and publish access to this server in the UDS login portal to allow users to change credentials.

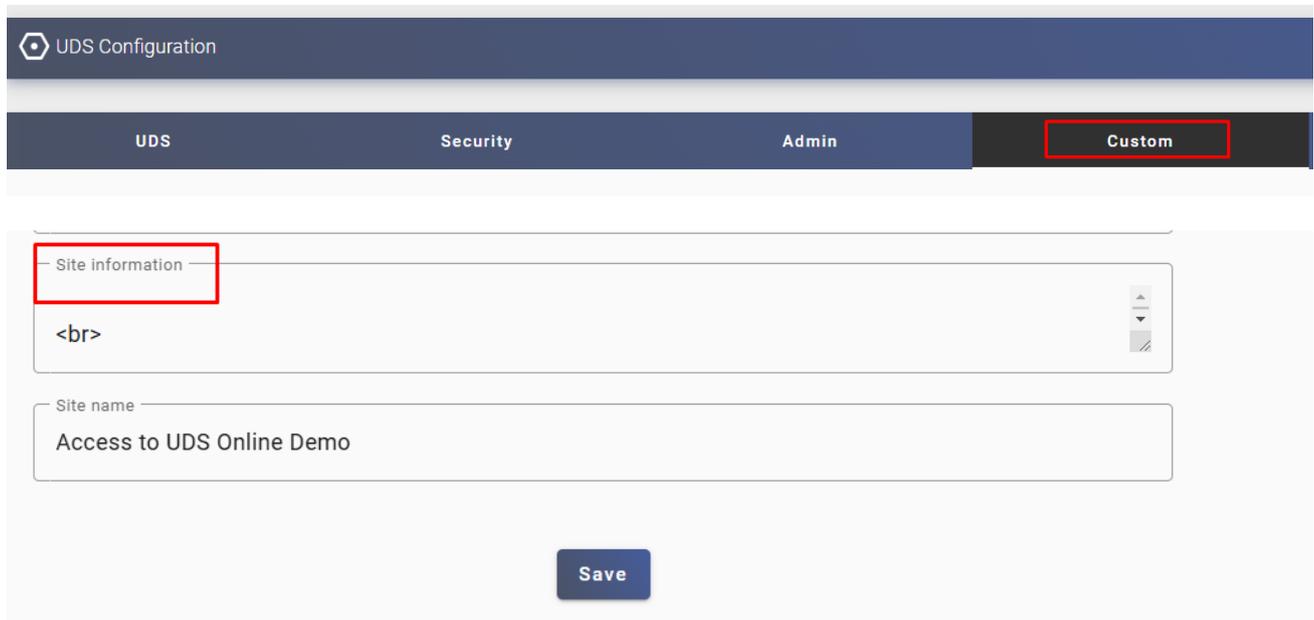
Note: For security reasons, it is recommended to change the “Secret_key” that appears by default on the machine.

Publish access to the credential change server

Once the new AD user credential change server is configured, you must make it accessible from the UDS login portal. To perform this task, you can modify the UDS login page itself by modifying the HTML code of the page or use the advanced configuration parameter “**Site information**”.

The following examples shows how to add access to the credential change server from “**Site information**” parameter:

Access the dashboard of UDS (with user with administration permissions), **Tools – Configuration – Custom – Site information**:



The screenshot shows the UDS Configuration dashboard. At the top, there is a navigation bar with tabs for 'UDS', 'Security', 'Admin', and 'Custom'. The 'Custom' tab is selected and highlighted with a red box. Below the navigation bar, there is a form with two main sections. The first section is labeled 'Site information' and is highlighted with a red box. It contains a text area with the HTML code '
'. The second section is labeled 'Site name' and contains the text 'Access to UDS Online Demo'. At the bottom of the form, there is a 'Save' button.

In this field you add, for example, the following data:

```
<div align="center"><a href="https://192.168.0.9" target="_blank">Password change AD Users</a></div>
```

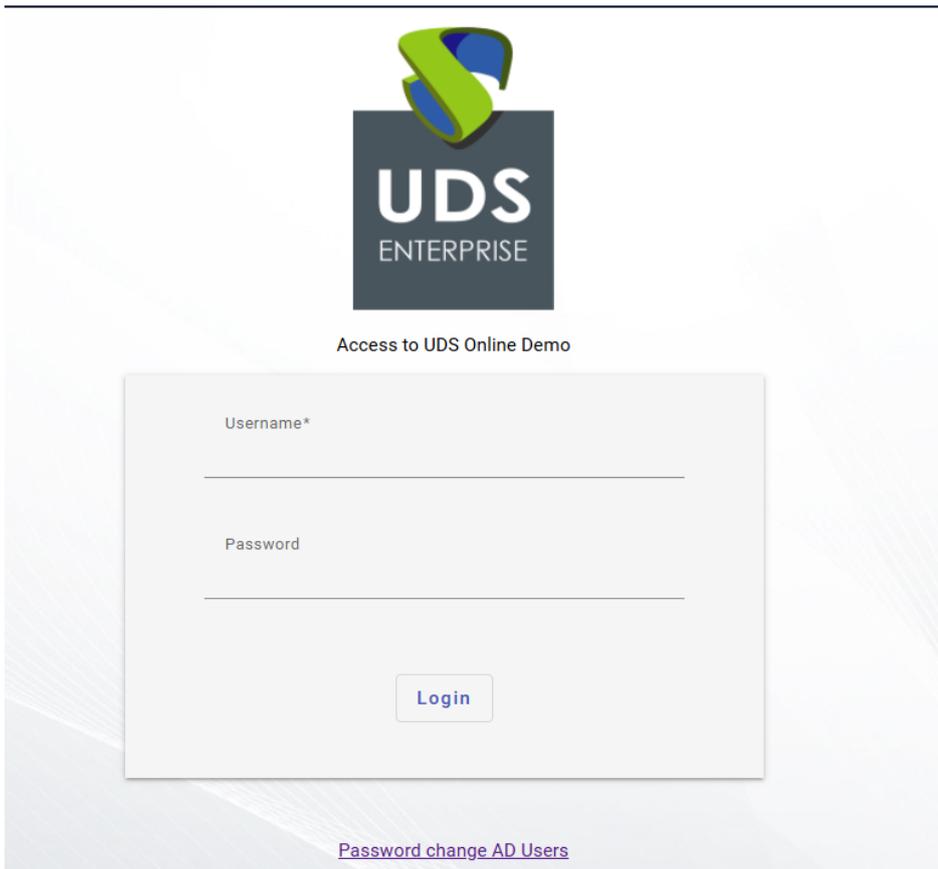
Site information

```
<div align="center"><a href="https://192.168.0.9" target="_blank">Password change AD Users</a></div>
```

NOTE: You will have to indicate the IP address or name of the credential change server and a descriptive text for the link.

Save the changes and reboot the UDS Server, now on our login page you will have access to this server:

When accessing the server, a new window will appear allowing you to change the user's password:



UDS
ENTERPRISE

Access to UDS Online Demo

Username*

Password

Login

[Password change AD Users](#)

Password update

AD User(user@domain.xxx)

Current password

New password

Repeat new password

Once modified, the system will indicate if the change has been made correctly and you can close the window:

Updated password

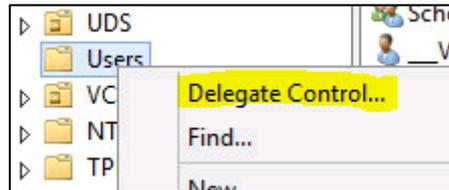
Your password was updated successfully.

You can now close this window.

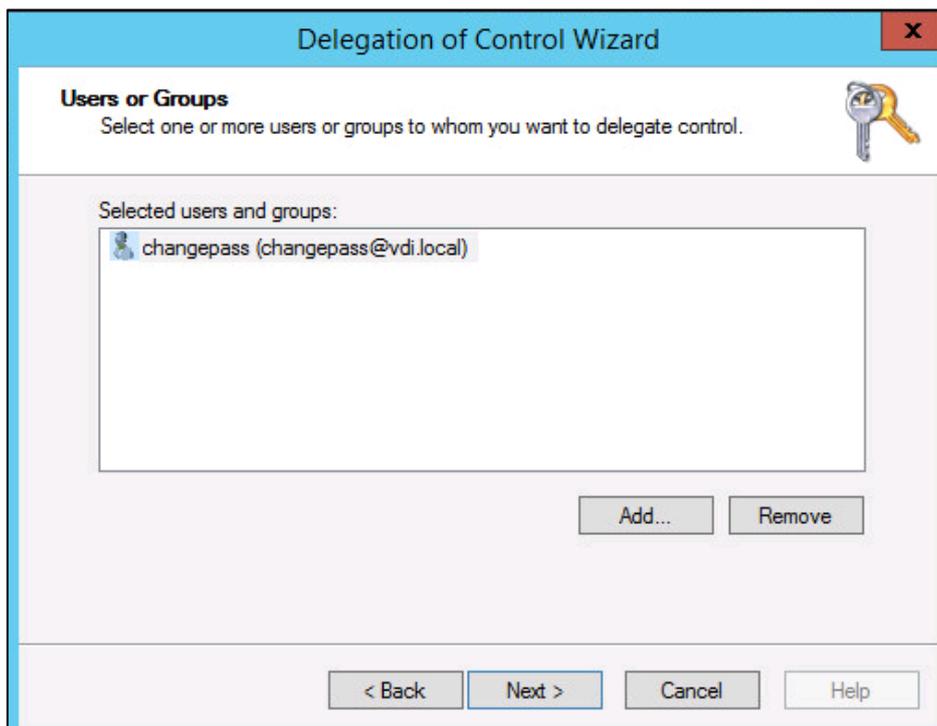
User with permissions to modify credentials

As indicated above, it is not necessary to use an administrator user in the password change machine, you can use a user with delegated permissions.

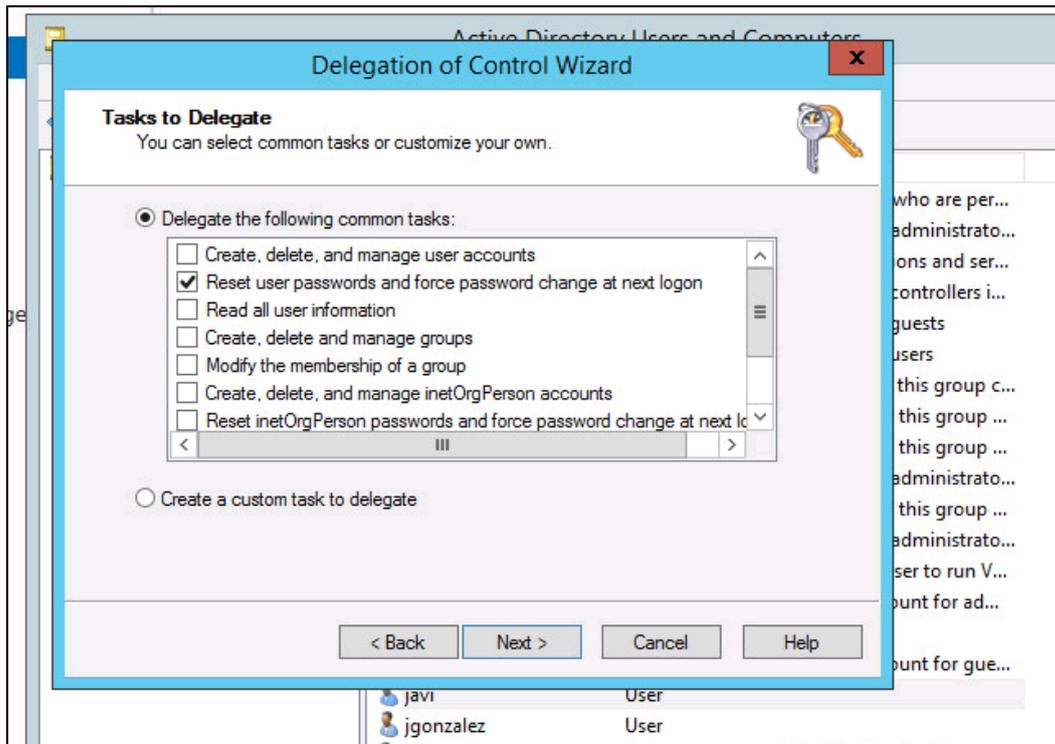
To do this, select the organizational unit (OU) where the users will be allowed to modify their password and select **“Delegate Control”**.



Indicate the user that will be allowed to modify the passwords (and that you have previously entered in the password change machine):



Select: "Reset user passwords and force password change at the next logon":



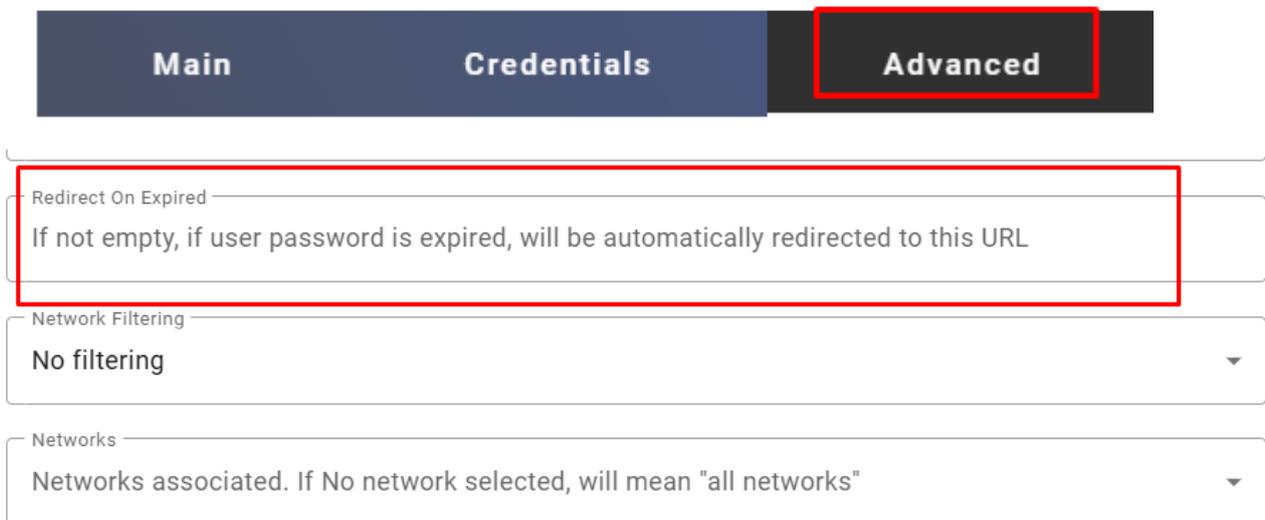
And finish the wizard.

Redirect on expired Parameter

From version 3.6 of UDS Enterprise it will be possible to redirect the user directly to a specific URL if it is detected that their password is expired.

Editing an Active Directory authenticator, in the advanced section:

Edit Authenticator



Main **Credentials** **Advanced**

Redirect On Expired
If not empty, if user password is expired, will be automatically redirected to this URL

Network Filtering
No filtering

Networks
Networks associated. If No network selected, will mean "all networks"

Thanks to this parameter we will be able to redirect directly to our password change server or any other dedicated server.

THE SMART DIGITAL WORKPLACE SOLUTION BY VIRTUAL CABLE

About UDS Enterprise

[UDS Enterprise](#) is a new software concept for creating a **fully customized workplace virtualization** platform. It provides **secure 24x7 access** from **any location and device** to all applications and software of an organization or educational center.

It allows you to combine Windows and Linux **desktop and application virtualization** in a single console, as well **as remote access** to Windows, Linux and macOS computers. Its Open Source base guarantees **compatibility with any third-party technology**. It can be deployed on-premises, in a public, private, hybrid or **multicloud**. You can even combine several environments at the same time and perform automatic and **intelligent overflows** to optimize performance and efficiency. All with a **single subscription**.

About Virtual Cable

[Virtual Cable](#) is a company specialized in the digital **transformation of the workplace**. The company develops, supports and markets UDS Enterprise. It has recently been recognized as an **IDC Innovator in Virtual Client Computing** worldwide. Its team of experts has designed **smart digital workplace solutions (VDI, vApp and remote access to physical computers)** tailored to each sector to provide a unique user experience fully adapted to the needs of each user profile. Virtual Cable professionals have **more than 30 years** of experience in IT and software development and more than 15 years in virtualization technologies. **Everyday millions of Windows and Linux virtual desktops** are deployed with UDS Enterprise around the world.