AD Password Mail Service © 2017 WizardSoft https://wizardsoft.nl

AD Password Mail Service Introduction

WizardSoft AD Password Mail Service (WSPMS) is a lightweight password self-service utility that allows end-users to reset their Windows Active Directory passwords quick & safe by e-mail. They only a 'registered' personal e-mail account for this. WSPMS runs on one of your Active Directory domain controllers. It services users that are a member of selected security groups and connects through IMAP and SMTP to a dedicated or shared mailbox that is used for password service requests, e.g. passwordservice@mycomany.com . It monitors service e-mails with specific subjects from your users. WSPMS works standalone and only needs an outgoing IMAP and SMTP client-connection to your mail server to function. It supports the IMAP IDLE feature so it can process new e-mails instantly.

How it works

Determine which users will be allowed to reset their password through the AD Password Mail Service. You do this by creating (or reusing if appropriate) one or more AD security group(s) and add selected users to these group(s). WSPMS will create unique registration codes for each user and makes these available to you in the formatted plain text file Export.txt . You can use this file to distribute the registration codes with instructions to your users (e.g. combine/merge with MS Word documents to create a letter for each user, or deliver in any other way). Alternatively, when "AutoSendRegistrationRequests" is enabled, WSPMS sends a one-time instructional e-mail to each user with a valid e-mail address set up in the "userPrincipalName" or "mail" Active Directory attribute and who did not register yet. This e-mail includes their unique register code. Once a user has its unique registration code she can register to the password service by sending an e-mail with subject 'register XXXXXXXX' from her personal e-mail account to the WSPMS company mailbox.

Once registered, a user that wishes to reset her password can simply send an e-mail with subject 'reset' to the WSPMS company mailbox. A mail with a unique code is send back to the user to confirm and validate the request. Once validated by replying, the new one-time-password will be send out to the user.

The user is guided through this process by instructional e-mails from WSPMS. Each service e-mail is based on an HTML template and is fully customizable. Inline images (e.g. company logo's) are supported.

20-user trial and licensing

PMS will run in 20-user trial mode if no license key is entered. This means that the total number of users in the configured security groups must not exceed 20. AD Password Mail Service pricing is based on the total number of users in all configured security groups and is subscription based. A subscription gives you usage rights, updates and e-mail support for 1 year. We are open to feature requests and will seriously consider these if they help more customers.

Prerequisites

Please create a dedicated mailbox account for the AD Password Mail Service OR create a new shared mailbox and give at least one account access to this shared mailbox (e.g. MS Office 365: Edit Shared Mailbox/mailbox delegation: Full Access and Send As rights). The mailbox must be able to receive external e-mails and accessible through IMAP (e.g. MS Office 365: Check Edit Shared Mailbox/mailbox features/IMAP: Enabled). If you use MS Office 365, please turn off the Office 365 clutter feature (outlook.office.com/owa/PasswordService@mycompany.com/?opath=/options/clutter). Login at least once in this mailbox (webmail) with the same credentials that you will use for WSPMS and send and receive a couple of test e-mails to make sure it is configured correctly.

Installation

To install, run the batch file install.cmd as administrator on one selected domain controller. A reboot is NOT needed. The installer performs the following tasks:

- Create the folder %ProgramFiles%\WSPMS
- Copy required files, including WSPMS.exe
- Create a ADPasswordMailService task to start servicing register and password change requests

Configuration

To configure the AD Password Mail Service, you open the configuration text file setup.ini . This file is utf-8 encoded and is formatted like name<any number of tabs & spaces>value . The name-value pairs are separated by line breaks <crlf>. A line that starts with a ';' is considered a comment and can be used to document settings. The e-mail templates are in the Templates subfolder. You can insert any Active Directory user attribute in send e-mails by using the notation $property$, e.g. $givenName$.

Name	Description	Example
ServiceSecurityGroups	; -separated list of AD security groups that contain the users who are serviced by WSPMS.	PasswordService
DenyDomains	; -separated list of e-mail domains that are prevented from being registered for password recovery.	mycompany.com
SmtpServer	SMTP server used to send e-mail	smtp.office365.com
SmtpTls	Initiated secured TLS SMTP connection (1 is true, 0 is false).	1
SmtpSsl	Use SSL SMTP connection	0
SmtpUser	User for sending e-mail	passwordservice@mycompany.com
SmtpPassword	Password for sending e-mail	MyPassword
SmtpFromName	Displayed 'from name' used in send e-mails	Password Service
SmtpFromAddress	Used 'from address' used in send e-mails	passwordservice@mycompany.com
SmtpPort	Port used for SMTP connection.	587
ImapServer	IMAP server used to connect to the dedicated or shared WSPMS mailbox.	outlook.office365.com
ImapSsl	Use SSL IMAP connection	1
ImapUser	User for retrieving e-mail	utility@mycompany.com\passwordservice (shared mailbox) OR passwordservice@mycompany.com (unique mailbox)
ImapPassword	Password for retrieving e-mail	MyPassword
ImapPort	Port used for IMAP connection	993
AutoSendRegistrationRequests	WSPMS sends registration instructions to each user that has a valid e-mail address set up in AD (userPrincipalName OR mail attribute)	1
MsgRegistrationRequestSubject	Subject used for registration request	Please register for the Password Service of MyCompany
MsgRegistrationRequestFile	Template used for registration request	MsgRegistrationRequest.html
MsgRegistrationResultSubject	Subject used for registration confirmation	Your Password Service registration

MsgRegistrationResultFile	Template used for registration confirmation	MsgRegistrationResult.html
MsgResetValidationSubject	Subject used for password reset validation	Please confirm password reset
MsgResetValidationFile	Template used for password reset validation	MsgResetValidation.html
MsgResetResultSubject	Subject used for password reset result	Your password is reset
MsgResetResultFile	Template used for password reset result	MsgResetResult.html
MsgNotificationSubject	Subject used for general notifications	Password Service notification
MsgNotificationFile	Template used for general notifications	MsgNotification.html
TextDeniedDomain	Text inserted in the notification e-mail for 'Denied domain' status.	Your e-mail address domain is not allowed for password recovery registration. Please try again using another e-mail account.
TextMailNotValidated	Text inserted in the notification e-mail for 'Mail not validated' status.	Your e-mail address is not registered yet. You must first register your e-mail address by sending an e-mail with subject 'register YOUR_REGISTRATION_CODE'.
TextAlreadyRegistered	Text inserted in the notification e-mail for 'E-mail already registered' status.	An e-mail address is already registered. Please contact IT if you need to change your registered e-mail address.

Testing

Next you can test the mail server communication by opening a command console (cmd.exe) and run the command WSPMS.exe /test .

After adjusting the templates to your liking you can (re)start the ADPaswordMailService scheduled task to apply the new settings.

In the Export subfolder you find a file export.txt . This file contains all usernames and registration codes. You need to hand out the unique registration codes to your users only once.

Example end-user process

1. End-user sends an e-mail to passwordservice@mycompany.com with subject register 49KVFUUR. The subject is case-insensitive and can include any other words. The way the code is generated maximizes clarity; no ambiguous characters are used.
2. The user receives a confirmation e-mail with instructions how to reset her password in the future.
3. To reset the user simply sends an e-mail to passwordservice@mycompany.com with subject reset.
4. The user receives a validation e-mail with the request to reply to this mail.
5. After replying, a new one-time-password is received. You can also add your password complexity rules.

If you must unregister a user, you can do so by running ADPMS.exe /unregister:username1;username2;… This will remove the e-mail address and generate a new registration code for each specified user.

Web forms

You can easily add another registration and reset method by creating a web form that sends e-mails to the PSM mailbox. Do not ‘fake’ the from-address because this can cause problems with spam filters. You can append ‘mail user@domain’ to the subject to specify the user who made the request.

Register form layout
-Your recovery e-mail address: EMAIL
-Your unique registration code: CODE
-If it is a public form add a captcha to prevent spam

Send e-mail from webserver with subject: register CODE mail EMAIL

Reset form layout
-Your recovery e-mail address: EMAIL
-If it is a public form add a captcha to prevent spam

Send e-mail from webserver with subject: reset mail EMAIL

This is a perfectly safe option because the user needs her unique registration code for registration and still needs access to her mailbox to validate a password reset request.

An PHP example solution is included in the WebForms folder:

- registration.php
- reset.php
- captcha.php