TPAM Security Product Client for Windows 2.5.6

Security Product Client for Windows Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SPCW Security Product Client for Windows Guide
Updated - May 2018
Version - 2.5.6

Contents

Security Product Client for Windows (SPCW) Guide

Introduction

The security product client for windows (SPCW) was developed to enhance the Windows® management capabilities of the TPAM security appliance.

SPCW adds the ability to manage Windows systems without requiring common native Windows communication ports (137-139, 445), which may be disabled at perimeter security points. The SPCW client uses a secure encrypted SSHv2 connection with the TPAM appliance. The communication port (default of port 22) can be specified during configuration.

Many additional management features are also offered with SPCW. The ability to change passwords for COM+, and Metabase/IIS objects, for example.

SPCW also functions with TPAM to provide secure sessions to Windows systems.

This guide will illustrate the installation procedure for the software client, and provide explanation for the many configuration choices available.

Install SPCW

To install and configure the SPCW client, perform the following steps:

1. Add the SPCW system/s to TPAM. See Add SPCW system in TPAM for details.
2. If upgrading to a new version of SPCW, you must remove the old SPCW client. See Remove old SPCW client for details.
3. Copy and unzip the new SPCW zip file to the client server. See Copy and unzip SPCW install file for details.
4. If installing the client in 64-bit hardware, install 64-bit component that is required. See Install 64-bit hardware component for details.

5. Complete the SPCW configuration, either through the interactive or silent method. See Interactive SPCW configuration and Silent SPCW configuration.

Add SPCW system in TPAM

To add a new SPCW system in TPAM:

1. Select **Systems, Accounts, & Collections | Systems | Add System** from the menu.
2. Enter the system name and network address.
3. Select one of the following platforms:

- **SPCW 2**
- **SPCW (DC) 2**, if the appliance is a domain controller
- **SPCW Pwd**, if the old and/or new password needs to be provided to a command executed by SPCW after a successful password change operation. If this platform is selected, enter one of the following in the Password Release On Change box:
    - Old - the old password is supplied to the command
    - New - the new password is supplied to the command
    - Both - the new and old password are supplied to the command

4. If SPCW Pwd is selected, see SPCW Pwd platform setup.
5. Click the Connection tab to configure the functional account that TPAM will use to connect to the system.
6. If the SPCW client is being used by TPAM for account management, download the SSH key used for communication with the TPAM appliance. Save this information, it will be needed in a later step.

    TIP: We recommend setting the Connection Timeout to 120 seconds to allow enough time for the client to finish processing tasks.

7. Click the **Save Changes** button.

Remove old SPCW client

There is no upgrade available to take an existing SPCW installation to version2.5.6 . Old SPCW versions must be removed prior to installing version2.5.6 .

Dump existing configuration file

Before removing the old SPCW version there is a tool to dump the configuration of an existing SPCW installation to a file that can be used when installing the new version.

This tool is DumpConfig.exe. It can be used to create a file in the initial configuration file format discussed above. DumpConfig.exe can be invoked as shown below.

- `>DumpConfig.exe` - This option outputs the configuration to stdout (screen). The output may be redirected to a file if desired.
- `>DumpConfig.exe /file` - This option outputs the configuration to file espcwInstallData.xml.
- `>DumpConfig.exe /file <filename>` - This option outputs the configuration to the specified filename.

If using domain accounts as functional accounts, then the configuration data output by this tool must be modified to provide the relevant domain account password prior to using the configuration file for a new SPCW installation. This is required since SPCW does not store the domain account password and has no way to retrieve it. The XML tags for the TPAM account password and the PSM account password are included in the output with values ParAccountPasswordUnknown and EgpAccountPasswordUnknown, respectively.

Note that no restart is required when the old SPCW version is removed followed by installation of the new SPCW version.

IMPORTANT: This tool dumps the configuration data to a screen or file in clear text. There are no passwords in the configuration data, but those customers that have encrypted the configuration file used by SPCW should realize that `DumpConfig.exe` displays everything in clear text and should take appropriate measures to limit access to `DumpConfig.exe`.

See Obfuscate tool for options on how to avoid putting clear text passwords in the initial configuration file during a silent installation.

Remove old client

Once you have the old configuration file saved, remove the old SPCW client.

To remove the client:

1. Select **Start | My Computer | Add or Remove Programs**.
2. Select the eDMZ Client for Windows in the list of currently installed programs.
3. Click the **Remove** button.
4. Click the **Yes** button on the confirmation window.
5. Restart your computer to complete the process.

Copy and unzip SPCW install file

To unzip the file:

1. Copy the zip file containing the installation files onto the computer on which you wish to install the client. The location of this file is not important.
2. Unzip (extract) the contents of the zip file

Install 64-bit hardware component

If installing on 64-bit hardware, browse to the ...\64bit-Client directory and double-click the setup.exe icon to install a component of the client required on 64-bit hardware. Proceed through all the standard Windows installer prompts.

A silent install of this package is possible by using the following command:

```
> msiexec /i eDMZLSAx64.msi /quiet
```

Interactive SPCW configuration

To perform an interactive SPCW configuration:

1. Browse to the appropriate directory under …\OS-Installers based on the operating system of the computer on which you are installing the client. If installing on Windows 2000, Windows XP, or Windows Server 2003, browse to …\OS-Installers\2K-XP-2K3\Full. Browse to …\OS-Installers\Vista-2K8-7\Full if installing on Windows Vista, Windows Server 2008, or higher.
2. Click the **setup.exe** icon to launch the client installation file.
3. Click the **Next** button.
4. Specify the installation folder. Click the **Next** button.
5. Click the **Next** button to start the installation. Once the install is complete the SPCW configuration interface launches.
6. Complete the boxes as described in SPCW configuration settings.
7. Click the **Apply** button.

   IMPORTANT: If the **Cancel** button is clicked at any point during the installation, any changes already applied will be rolled back and the installation will abort.
8. Click the **Account Setup** tab.
9. Complete the fields on this screen as described in SPCW account setup.

10. Click the **OK** button. Upon clicking of the OK button, a few windows will be displayed briefly while the installation proceeds. This is followed by a dialog informing the user that the computer must be restarted for changes to take effect.
11. Restart the computer to complete the installation.

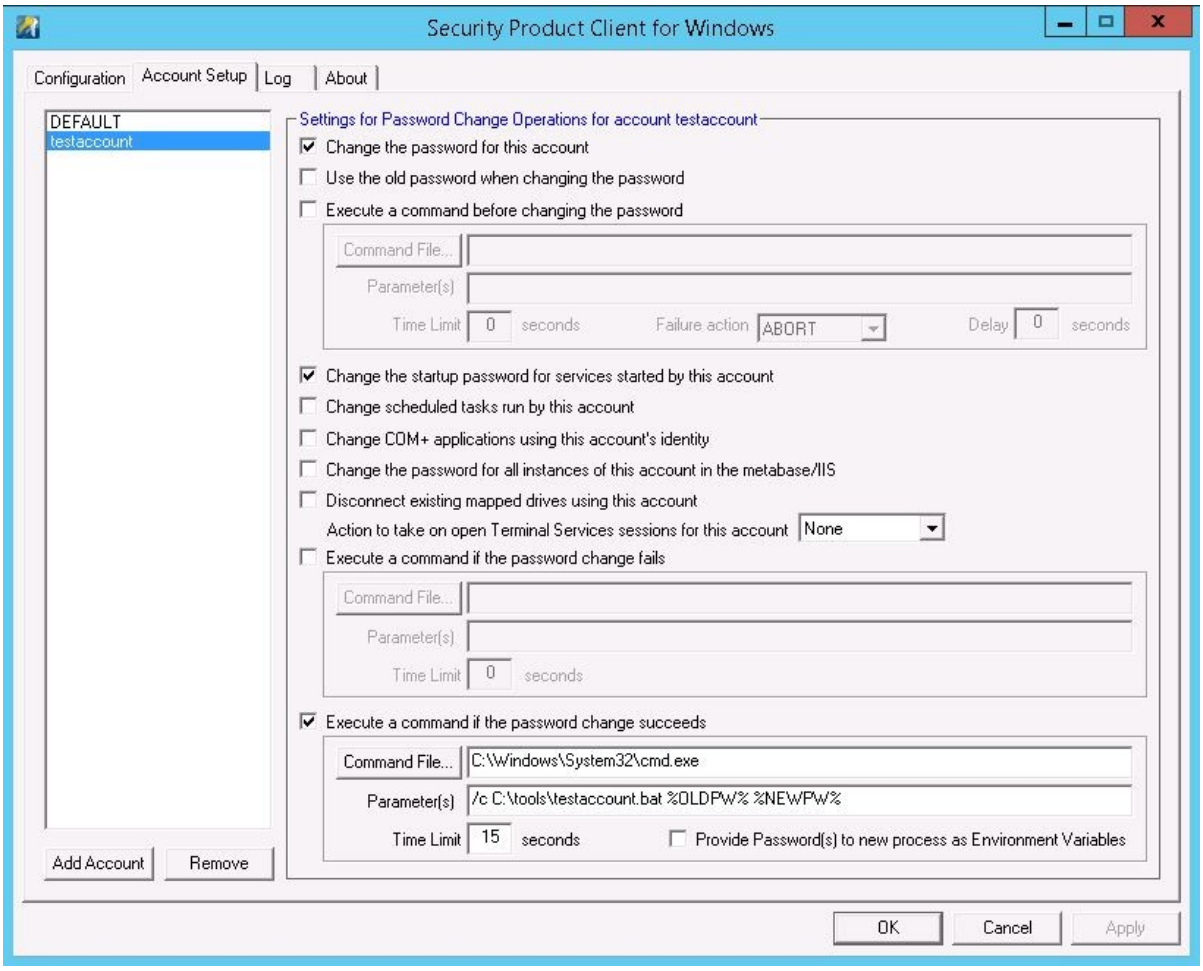
SPCW Pwd platform setup

When SPCW Pwd platform is selected in the TPAM interface, you must also configure custom account settings within SPCW to specify that the password(s) should be provided as parameters to the command.

For the option Execute a command if the password change succeeds, the user can specify the tags `%OLDPW%` and/or `%NEWPW%` as parameters to the command, and if TPAM has indicated that the password(s) can be provided to the command, the old and/or new password will be substituted for these tags when invoking the target command. This is configured on the TPAM Systems Details tab in the **Password Release on Change** box.

An alternate method of providing the old and/or new password to the command invoked under option "Execute a command if the password change succeeds" is to have SPCW provide the old/new password(s) to the command as environment variables. This can be enabled via the check box **Provide Password(s) to new process as Environment Variables**. The invoked command can retrieve the passwords from the environment variables named `SPCW_OLD_PASSWORD` and `SPCW_NEW_PASSWORD`. For security reasons, it is suggested that the invoked command read and clear the environment variables as soon as possible after the process is started.

The image below shows how to configure the SPCW client to pass the parameters to a BAT file. In this example, it is passing the old password and the new password as parameters to testaccount.bat.



As an example, the file testaccount.bat contains the following two lines:

```
@echo off
echo For testaccount, the old password was %1, new password is %2 >>
c:\tools\testaccount.log
```

After a few runs, testaccount.log contains:

```
C:\tools>type testaccount.log
For testaccount, the old password was NJu9Oe, new password is 14WhQFyY
For testaccount, the old password was 14WhQFyY, new password is dwx0Vq
For testaccount, the old password was dwx0Vq, new password is ziR8G7
```

IMPORTANT: There is no generic way to provide the account name to the invoked BAT file, so the only way for the BAT file to know which account it is acting upon is to have custom account setup for each account that requires this capability.

Within the custom account setup, you could invoke an account specific BAT file as done in this example. Alternatively, you could specify the account name as a parameter to a generic BAT file. This could be done with parameters similar to the following.

```
"/c c:\tools\generic.bat testaccount %OLDPW% %NEWPW%"
```

This still requires custom account setup, but it eliminates the need for multiple BAT files.

Limitation: When changing the password for tasks, services, etc. run by a domain account on a system set up in TPAM as a dependent system of the account, TPAM does not provide the old password to SPCW when changing the password on the dependent system. Therefore, only the new password is available to the command invoked by SPCW.

Silent SPCW configuration

A silent install of the client is also possible. Since the silent install does not raise the GUI to add the required configuration data, the data must be specified in an initial configuration file. This file must be created and made available to the installer before the silent installation is performed. See Initial configuration file for details.

To perform silent SPCW configuration:

1. Create or use existing (from previous install) initial configuration file in appropriate directory.
2. In the SPCW directory, browse to the appropriate directory under …\OS-Installers based on the operating system of the computer on which you are installing the client.

- If installing on Windows 2000, Windows XP, or Windows Server 2003, browse to …\OS-Installers\2K-XP-2K3\Full, and execute the following command. > msiexec /i SetupSpcw.msi /quiet [/forcerestart]
- If installing on Windows Vista, Windows Server 2008 or higher, browse to …\OS-Installers\Vista-2K8-7\Full , and execute the following command. > msiexec /i SetupSpcwNET.msi /quiet [/forcerestart]

NOTE: Windows Installer version prior to 3.0 need to use option /qn instead of /quiet, and the forcerestart option is not available.

Make sure the computer is restarted by either including the /forcerestart option to the msiexec command or manually restarting the computer.

SPCW configuration settings

The table below explains all the field options available on the SPCW Configuration tab.

Table 1: SPCW configuration settings

Field	Description
Password Management Functional Account	The name of the account that TPAM will use for account management on this system. If a local

Field	Description
	account is used, the account will be created on the local Windows system by the application. This account will have Administrator privilege. When specifying the account, a non-existent account name must be specified since the application will create the account. If a domain account is used, the domain account must already exist and needs to be in the Domain Admins group. The password for the domain account must be provided. The domain account must be provided in UPN format.
Password Management TPAM/DPA Network Addresses	The network addresses for TPAM servers and DPAs that will manage passwords on this machine. These addresses may be IP addresses or FQDNs. The values here may include addresses for the standalone or primary TPAM server, the TPAM Replica, Non-Failover Replica, and DPAs. Multiple addresses must be separated by commas. Additionally, the addresses may include wildcards, using "*" for multiple characters and "?" for single characters. For example, 192.168.0.* would match addresses 192.168.0.0 through 192.168.0.255, while 192.168.0.? would match addresses 192.168.0.0 through 192.168.0.9. Wildcards are also allowed in FQDNs, *.mycompany.-com for example.
DSS Public Key	If the client is being used by TPAM for account management, the SSH key used for communication between TPAM and this computer must be set up. This key is downloaded from the TPAM interface as part of the system set up in TPAM. See Add SPCW system in TPAM for details.
Session Management Functional Account	The name of the account that PSM will use to establish the SSH tunnel to the server for creating secure, recorded RDP sessions to this system. If a local account is used, the account will be created on the local Windows system by the application. This account will have Administrator privilege. When specifying the account, a non-existent account name must be specified since the application will create the account. If a domain account is used, the domain account must already exist and needs to be in the Domain Admins group. The password for the domain account must be provided only if a password management functional account is not provided.

Field	Description
Session Management TPAM/DPA Network Addresses	The network addresses for TPAM servers and DPAs that are used to create secure, recorded sessions to this server. These addresses may be IP addresses or FQDNs. The values here may include addresses for the standalone or primary PAM server, the TPAM Replica, Non-Failover Replica, and DPAs. Multiple addresses must be separated by commas. Additionally, the addresses may include wildcards, using "*" for multiple characters and "?" for single characters. For example, 192.168.0.* would match addresses 192.168.0.0 through 192.168.0.255, while 192.168.0.? would match addresses 192.168.0.0 through 192.168.0.9. Wildcards are also allowed in FQDNs, *.mycompany.com for example.
Listening Port	The TCP/IP port on which the client will listen for SSH connections from TPAM. The default port is 22.
Encrypt Configuration and Account Data	If selected, the configuration and account setup data required by the SPCW client will be encrypted.

SPCW account setup

Add any accounts that you want to manage with settings different from the DEFAULT account. You may also change the settings for the DEFAULT account. The DEFAULT account settings are used for any account not specifically added and configured.

To add a new account:

1. Click the **Add Account** button.
2. Enter a name for the account and click the **OK** button.
3. Select/Clear the check boxes as desired.
4. Enter any commands to be executed.
5. Click the **Apply** button.

To edit the DEFAULT account:

1. Select the DEFAULT account in the list.
2. Select/Clear the check boxes as desired.
3. Enter any commands to be executed.
4. Click the **Apply** button.

Initial configuration file

An initial configuration file can be used during installation to specify configuration and account settings for the SPCW client. To do this, create a file named espcwInstallData.xml in the same directory as the .msi file before performing the silent install discussed above. An example and description of the contents of the initial configuration file are provided below.

Note that XML format validation is very rudimentary. XML start tags and end tags are allowed, but empty element tags are not allowed. For instance, the tag <changesvcs/> will cause a validation failure and the installation will fail.

NOTE: This file must be encoded using UTF-8 or 8-bit ANSI character set.

```
<espcwdata>
    <configuration>
        <paracct>edmzpar</paracct>
        <paracctpassword>passwordForParacct</paracctpassword>
        <paraddress>192.168.30.6</paraddress>
        <egpacct>eguardpost</egpacct>
        <egpacctpassword>passwordForEgpacct</egpacctpassword>
        <egpaddress>192.168.30.4,192.168.30.*</egpaddress>
        <port>22</port>
        <encryptFiles>1</encryptFiles>
        <parkey>ssh-dss AAAAB345ZX1...snip...AZ457Z85kC9g==</parkey>
        <egpkey>ssh-dss AAAAB345ZX1...snip...AZ457Z85kC9g==</egpkey>
</configuration>
<defaultaccountsettings>
    <changepass>Y</changepass>
    <useoldpass>Y</useoldpass>
    <preenabled>N</preenabled>
    <prepath></prepath>
    <precmd></precmd>
    <preargs></preargs>
    <pretimeout>0</pretimeout>
    <prefailureaction>ABORT</prefailureaction>
    <predelay>0</predelay>
    <changesvcs>Y</changesvcs>
    <changetasks>Y</changetasks>
    <changecomplus>N</changecomplus>
```

```
        <changemeta>N</changemeta>
        <terminatefso>N</terminatefso>
        <termsrvaction>N</termsrvaction>
        <failenabled>N</failenabled> <failpath></failpath>
        <failcmd></failcmd>
        <failargs></failargs>
        <failtimeout>0</failtimeout>
        <successenabled>N</successenabled>
        <successpath></successpath>
        <successcmd></successcmd>
        <successargs></successargs>
        <successtimeout>0</successtimeout>
        <successpwasenvvar>N</successpwasenvvar>
</defaultaccountsettings>
<accounts>
        <account>
                <name>account1</name>
                <changepass>Y</changepass>
                <useoldpass>Y</useoldpass>
                <preenabled>Y</preenabled>
                <prepath>C:\WINDOWS\system32</prepath>
                <precmd>cmd.exe</precmd>
                <preargs>/c "C:\bats\myprecmd.bat"</preargs>
                <pretimeout>10</pretimeout>
                <prefailureaction>ABORT</prefailureaction>
                <predelay>2</predelay>
                <changesvcs>Y</changesvcs>
                <changetasks>Y</changetasks>
                <changecomplus>Y</changecomplus>
                <changemeta>Y</changemeta>
                <terminatefso>Y</terminatefso>
                <termsrvaction>D</termsrvaction>
                <failenabled>Y</failenabled>
                <failpath>C:\WINDOWS\system32</failpath>
                <failcmd>cmd.exe</failcmd>
                <failargs>/c "C:\bats\myprecmd.bat"</failargs>
```

```
            <failtimeout>10</failtimeout>
            <successenabled>Y</successenabled>
            <successpath>C:\WINDOWS\system32</successpath>
            <successcmd>cmd.exe</successcmd>
            <successargs>/c "C:\bats\mysuccesscmd.bat"</successargs>
            <successtimeout>10</successtimeout>
            <successpwasenvvar>Y</successpwasenvvar>
</account>
<account>
                <name>account2</name>
                <changepass>N</changepass>
                <useoldpass>N</useoldpass>
                <preenabled>Y</preenabled>
                <prepath>C:\WINDOWS\system32</prepath>
                <precmd>cmd.exe</precmd>
                <preargs>/c "C:\bats\myprecmd.bat"</preargs>
                <pretimeout>12</pretimeout>
                <prefailureaction>CONTINUE</prefailureaction>
                <predelay>0</predelay>
                <changesvcs>N</changesvcs>
                <changetasks>N</changetasks>
                <changecomplus>N</changecomplus>
                <changemeta>N</changemeta>
                <terminatefso>N</terminatefso>
                <termsrvaction>L</termsrvaction>
                <failenabled>N</failenabled>
                <failpath></failpath>
                <failcmd></failcmd> <failargs></failargs>
                <failtimeout>0</failtimeout>
                <successenabled>N</successenabled>
                <successpath></successpath>
                <successcmd></successcmd>
                <successargs></successargs>
                <successtimeout>0</successtimeout>
                <successpwasenvvar>N</successpwasenvvar>
    </account>
</accounts>
</espcwdata>
```

The table below gives a description and possible values for all the XML tags.

Table 2: XML tag values

XML tag	Description	Allowed Values
espcwdata	This element	Mandatory <configuration> element, and optional <defaultaccountsettings> and

XML tag	Description	Allowed Values
	contains the configuration and account settings data.	<accounts> elements
configuration	This element contains the configuration settings.	All elements shown in example within the configuration element are mandatory.
paracct	This element defines the Password Management functional account to be created.	A valid account name. Specify <paracct></paracct> if no Password Management functional account should be created.
paracctpassword	The password for paracct when paracct is a domain account. Use the Obfuscate tool if desired to avoid putting a clear text password in the configuration file.	Specify <paracct-password></paracctpassword> if password is not required, for example when using a local functional account.
paraddress	This element defines the TPAM/DPA network address(es) used for password management.	TPAM/DPA network address(es). If multiple addresses are to be specified, separate with commas. Use <paraddress></paraddress> if no TPAM/DPA addresses are to be specified.
egpacct	This element defines the Session Management functional account to be created.	A valid account name. Specify <egpacct></egpacct> if no Session Management functional account should be created.
egpacctpassword	The password for egpacct when egpacct is a domain account. Use the Obfuscate tool if desired to avoid putting a clear text password in the configuration file.	Specify <egpacct-password></egpacctpassword> if password is not required, for example when using a local functional account.
egpaddress	This element defines the TPAM/DPA	TPAM/DPA network address(es). If multiple addresses are to be specified,

XML tag	Description	Allowed Values
	network address(es) used for session management.	separated with commas. Use <egpaddress></egpaddress> if no TPAM/DPA addresses are to be specified.
port	This element defines the TCP/IP port on which the client will listen for SSH connections from TPAM.	A valid port number.
encryptFiles	Specifies if configuration and account settings data file should be encrypted.	0 or 1 0 indicates that the file should not be encrypted. 1 indicates that the file should be encrypted.
parkey	The DSS public key from the TPAM performing password management.	The entire contents of the DSS public key file.
egpkey	The DSS public key from the TPAM performing session management.	The entire contents of the DSS public key file.
defaultaccountsettings	This element contains the DEFAULT account settings.	All elements shown in example within defaultaccountsettings element are optional.
changepass	Change the password for this account.	Y or N
useoldpass	Use the old password when changing the password.	Y or N
preenabled	Execute a command when changing the password.	Y or N
prepath	Location of precmd	Path specifying location of command to be executed.
precmd	Command to be	filename.extension to be executed

XML tag	Description	Allowed Values
	executed when changing the password.	
preargs	Arguments for the command specified in precmd.	Arguments to be passed to precmd
pretimeout	Time limit, in seconds.	Number
prefailureaction	Failure action	ABORT or CONTINUE
predelay	Delay, in seconds	Number
changesvcs	Change the startup password for services started by this account.	Y or N
changetasks	Change scheduled tasks run by this account	Y or N
changecomplus	Change COM+ applic-ations using this account's identity.	Y or N
changemeta	Change the password for all instances of this account in the metabase/IIS.	Y or N
terminatefso	Disconnect existing mapped drives using this account.	Y or N
termsrvaction	Action to take on open Terminal Services sessions for this account	N for None D for DISCONNECT L for LOGOFF
failenabled	Execute a command if the password change fails	Y or N
failpath	Location of failcmd	Path specifying location of command to be executed
failcmd	Command to be	filename.extension to be executed

XML tag	Description	Allowed Values
	executed if the password change fails.	
failargs	Arguments for the command specified in failcmd.	Arguments to be passed to failcmd
failtimeout	Time limit, in seconds	Number
successenabled	Execute a command if the password change succeeds	Y or N
successpath	Location of successcmd	Path specifying location of command to be executed
successcmd	Command to be executed if the password change succeeds	filename.extension to be executed
successargs	Arguments for the command specified in successcmd	Arguments to be passed to successcmd
successtimeout	Time limit, in seconds	Number
successpwasenvvar	Provide password(s) to new process as environment variables.	Y or N
accounts	This element contains settings for one or more accounts.	One or more <account> elements. This element is optional.
account	This element contains settings for a single account.	All elements shown in example within account element are optional, with the exception of <name> which is mandatory.
name	The name of the account set up within an <account> element.	An account name. If an <account> element is specified, this element is mandatory.

Obfuscate tool

To avoid putting clear text passwords in the initial configuration file used during a silent installation, the Obfuscate.exe application can be used to obfuscate a password, and the obfuscated password can then be used in the initial configuration file. The Obfuscate.exe application is run from a command prompt and requires a single parameter which is the password to be obfuscated.

```
> Obfuscate.exe ThisIsMyPassword

BEGIN.573d394b22365f5223666367213e543d527e603d51373845483d675f2179.END
```

Copy and paste the entire outputted string, including `BEGIN` and `END`, as the value for the password in the initial configuration file.

Troubleshooting/FAQ

This section provides guidance on a few issues that are sometimes encountered by customers.

Q: I cannot get Test System to work. What could be the problem?

A: There are several things to check:

- If SPCW was just installed, make sure the Windows system was restarted after installation to complete required initialization of components.
- Make sure the functional account name defined in SPCW matches the functional account name for the system defined in TPAM.
- Make sure the correct TPAM address is defined in the SPCW list of TPAM/DPA network addresses.
- Ensure the appropriate DSS public key has been imported into SPCW.
- Ensure the SPCW Listening Port matches the port defined for the system in TPAM.

Q: Test System works if affinity settings for the system indicate to use the local PPM appliance, however it does not work if I set affinity to use a DPA. How can I fix this?

A: Make sure the correct DPA address(es) are defined in the SPCW list of TPAM/DPA network addresses.

Q: During a password change operation, the failure message "The specified network password is not correct" is displayed. What does this mean?

A: This means that there is a mismatch between the password for the account on the Windows system and the password stored in TPAM for that account, and SPCW is attempting to use the incorrect TPAM password during the password change attempt. You can clear the check box labeled "Use the old password when changing the password" in SPCW for that account. This will cause SPCW to set the new password without using the old password. After the passwords are in sync again, you can select the check box again if so desired.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product