



## Privileged Account Management Manual

# Table of Contents

1	OVERVIEW.....	4
2	PASSWORDSTATE WEB SERVER SYSTEM REQUIREMENTS.....	7
3	POWERSHELL AND SECURE SOCKETS LAYER (SSL) PROTOCOL .....	8
4	PASSWORD RESET SCRIPT REQUIREMENTS .....	9
5	PASSWORD VALIDATION SCRIPT REQUIREMENTS .....	18
6	PASSWORD DISCOVERY SCRIPT REQUIREMENTS .....	19
7	ENABLING POWERSHELL REMOTING PER HOST .....	21
8	ENABLING POWERSHELL REMOTING VIA GROUP POLICY .....	22
9	HOSTS IN NON-TRUSTED DOMAINS .....	27
10	ACCOUNT DISCOVERY AND PASSWORD RESETS BETWEEN NON-TRUSTED DOMAINS, OR AGAINST WORKGROUP COMPUTERS .....	28
11	LOCAL ADMINISTRATOR ACCOUNT PASSWORD RESETS WITHOUT THE USE OF A PRIVILEGED ACCOUNT CREDENTIAL.....	29
12	PASSWORD RESETS AND ACCOUNT VALIDATION FOR LINUX ROOT ACCOUNTS .....	30
13	STRUCTURE OF A PASSWORD RESET SCRIPT .....	32
14	SSH TEMPLATE SCRIPTS .....	33
14.1	SSH TEMPLATE - REMOTE COMMANDS.....	33
14.2	SSH TEMPLATE - REMOTE SHELL .....	35
14.3	SSH TEMPLATE SUCCESS AND ERROR CONDITIONS .....	36
14.4	CREATING SSH TEMPLATE SCRIPTS .....	37
15	POWERSHELL SCRIPT VARIABLES.....	40
16	ON PREMISE ACTIVE DIRECTORY PASSWORDS .....	42
16.1	PRIVILEGED ACCOUNT CREDENTIAL .....	42
16.2	ADD APPROPRIATE DOMAINS TO THE ACTIVE DIRECTORY DOMAINS SCREEN .....	43

---

16.3	CONFIGURE A PASSWORD LIST FOR PASSWORD RESETS .....	44
16.4	CONFIGURE A PASSWORD FOR PASSWORD RESETS .....	45
16.5	TRIGGERING A RESET .....	47
17	PASSWORD RESET QUEUING SYSTEM.....	48
18	PASSWORD RESET DEPENDENCY RECORDS .....	51
18.1	ANATOMY OF A PASSWORD DEPENDENCY RESET .....	53
19	HOST AND ACCOUNT DISCOVERIES .....	54
19.1	EXPLANATION OF DISCOVERY JOBS .....	54
19.2	SETTING UP A HOST DISCOVERY .....	55
19.3	SETTING UP AN ACCOUNT DISCOVERY .....	58
19.4	ACTIVE DIRECTORY DISCOVERY JOB EXPLAINED .....	58
19.5	LOCAL ADMIN DISCOVERY .....	60
19.6	WINDOWS DEPENDENCIES DISCOVERY .....	62
19.7	DATABASE ACCOUNT DISCOVERY .....	64
20	OFFICE 365 AND MICROSOFT ENTRA ID ACCOUNTS .....	66
20.1	POWERSHELL MODULE REQUIREMENTS .....	66
20.2	MICROSOFT ENTRA ID PERMISSIONS .....	66
20.3	OFFICE 365 AND ENTRA ID HEARTBEATS .....	67
21	INSTALLING ORACLE DATA ACCESS COMPONENTS (ODAC) .....	68
22	VMWARE ESXI ACCOUNTS - POWERCLI POWERSHELL MODULE .....	69
23	REMOTE SITE LOCATIONS AGENT .....	70
24	PASSWORD RECORD EXAMPLES .....	71
24.1	OFFICE 365/AZURE AD ACCOUNTS: .....	71
24.2	WORKGROUP/NON-DOMAIN LOCAL ADMINISTRATORS .....	72
24.3	DATABASE ACCOUNTS (MICROSOFT SQL SERVER, ORACLE, POSTGRE, MYSQL, MARIADB) .....	73
24.4	IBM IMM ACCOUNTS .....	74
24.5	SSH ACCOUNTS WITH PUBLIC/PRIVATE KEY AUTHENTICATION .....	75

---

24.6	CISCO IOS ENABLE ACCOUNT .....	76
24.7	DELL iDRAC ACCOUNTS.....	77

# 1 Overview

Passwordstate can automate the management of privileged accounts, by discovering accounts on your network, resetting the account passwords and performing “heartbeats” on these passwords so you can be sure the passwords are in sync. Below is a list of account types that Passwordstate natively manages:

- Microsoft Active Directory, Local Administrator Windows Accounts, Windows Scheduled Tasks, Windows Services, IIS Application Pools, SQL Accounts, COM+ Components, Office 365 and Microsoft Entra ID Accounts
- Cisco Routers and Switches
- Linux Accounts - including root (CentOS, Debian, Fedora, Mac OS X, Mint, Open SUSE, Oracle Linux, Oracle Solaris, RedHat Linux, Scientific Linux, Solaris, SUSE Enterprise Desktop, SUSE Enterprise Server, Ubuntu)
- MySQL Accounts
- Oracle Accounts
- MariaDB Accounts
- Palo Alto Firewalls
- PostgreSQL Accounts
- HP iLO out of band management cards
- HP H3C switches and routers
- HP Procurve switches and routers
- F5 BIG-IP Load Balancers
- IBM's IMM out of band management cards
- Dell's iDRAC out of band management cards
- VMWare ESX Accounts
- Juniper Junos devices
- Juniper ScreenOS firewalls Accounts
- Fortigate Firewall Accounts
- SonicWALL Firewall Accounts

## Custom Powershell Reset Scripts

If you have a system that is not natively supported as in the list above, you have the ability to write your own custom scripts and use them in Passwordstate to manage the accounts on those systems. This feature also allows you to add in your custom operating system with a logo of your choice. You can also clone existing scripts and modify them to add in functionality if desired.

### Custom Powershell “Dependency” Scripts

Passwordstate has a feature where you can add in custom PowerShell scripts to perform task of your choice, as a dependency when a password has been successfully updated. For example, you may want to update some documentation or send some information about the newly reset password to the API of your Help Desk software. Or maybe you need to use the new password on another application so you will automate the newly reset password being sent to that 3<sup>rd</sup> party software.

When creating a custom script of this nature, you can use a number of built-in variables to pull information from Passwordstate and insert this data into your scripts. These variables can be found in section **PowerShell Script Variables** of this guide.

### SSH Templates

If you have a system that is not natively supported in the list above, that uses SSH as the communication protocol, there is a feature where you can build your own scripts based off SSH Templates. This allows you to simply issue a series of commands in sequential order, or all on one line to perform the password reset. You then set your own “**success**” and “**error**” conditions. This means you do not need to write the entire reset script, but as long as you know the native commands to perform a password reset on that system, as if you were doing it right within the SSH shell, you can build your own reset scripts easily.


### Password Heartbeat/Validation/Discovery

Passwordstate allows you to perform ‘**validation**’ tasks to ensure the passwords stored in Passwordstate are accurate compared to what is being used on remote hosts. You’re also able to ‘**discover**’ many different types of accounts on devices on your network, and Passwordstate does all this without the need to install any agents on those remote devices. Examples of what Passwordstate can discover are Local Windows or Linux accounts, accounts on Windows services or IIS Application pools, or maybe local accounts on your Fortigate firewall or Cisco switch.

When running a discovery job, you can put it in to “**Simulation**” mode, and this will report back to you what it finds but it won’t add any data into Passwordstate. It’s a good way to validate what accounts are being discovered without fear of affecting any production system. If you want, you can have the password reset immediately with a strong random password of your choice, a static password of your choice, or maybe you want to add the account into Passwordstate without doing a password reset at all, the choice is yours.

## No Agents Required

Click Studios designed the Password Reset, Heartbeat and Discovery features to make use of Microsoft's PowerShell scripting capabilities, to eliminate the need to install custom agents on remote Hosts. These Reset, Heartbeat & Validation features can also be used on Hosts in non-trusted domains.

 Note: If you do have strict firewalling between various networks, or manage client's infrastructure over the Internet, there is also a **Remote Site Agent** which can be deployed which can communicate securely over HTTPS with additional encryption to protect your data. This agent can execute all these Password Resets, Discovery and Validation scripts on those remote networks and report the results back into your core Passwordstate website, so it's all centrally managed within one console. See section **Remote Site Locations** for more information

## 2 Passwordstate Web Server System Requirements

To make use of the PowerShell Password Reset Scripts, the below components may need to be set up on your Passwordstate Web Server:

- **Microsoft .Net Framework 4.7.2** or higher (*mandatory*)

To check .NET version, run this command in Powershell ISE on your web server:

```
$Release = (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\').Release
If ($Release -ge '461808')
{Write-Host ".NET Framework 4.7.2 or high is installed. No action required"}
else
{Write-Host ".NET Frame needs to be updated"}
```

Installation of .NET Framework can be achieved by:

- Windows Updates
- Installed as a **'Server Feature'** on Server OS
- Installed as a Windows Feature through Add/Remove Programs on Windows 10, 11
- Installed manually via this link: <https://support.microsoft.com/en-au/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows>
- **PowerShell 5.0** or higher (*mandatory*)
- **Microsoft Visual C++ 2013 Runtime** - <https://www.microsoft.com/en-au/download/details.aspx?id=40784> (*mandatory - this will automatically be installed for you when installing Passwordstate*)
- **Azure Az PowerShell Module** (*only required for Office 365 or Azure AD Accounts*)
- **VMWare PowerCLI Powershell Module** (*only required for VMWare ESXi accounts if SSH is disabled on your devices*)
- **Oracle Data Access Components (ODAC)** (*only required for Oracle database Passwords*)
- **Remote Server Administration Tools (RSAT)** (*only required for On-Premise Active Directory Accounts – Can be added as a 'Feature' on Windows Server OS, or installed manually if you are hosting Passwordstate on Windows 10/11*): <https://www.microsoft.com/en-us/download/details.aspx?id=45520>



### 3 PowerShell and Secure Sockets Layer (SSL) protocol

By default, any PowerShell scripts that use the Invoke-Command cmdlet, do not use the -UseSSL parameter.

This option can be enabled on the screen Administration -> System Settings -> Miscellaneous tab, or if using Remote Site Locations agents, it can be enable per remote site record.

The -UseSSL cmdlet uses the Secure Sockets Layer (SSL) protocol to establish a connection to the remote computer.

WS-Management encrypts all PowerShell content transmitted over the network. The UseSSL parameter is an additional protection that sends the data across an HTTPS, instead of HTTP.

For more information, please refer to Microsoft documentation here - <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-7.3>

## 4 Password Reset Script Requirements

There are different System Requirements, and host configurations, depending upon which Password Reset scripts you would like to use. The following table describes the possible scenarios.

- 🚩 Note 1: For detailed information about open ports, refer to “**Passwordstate Open Port Requirements**” on Click Studios website: <https://www.clickstudios.com.au/documentation/>
- 🚩 Note 2: If you are using the **Remote Site Locations Agent**, this has the same system requirements as your Passwordstate web server, and the hosts on that network will have the same requirements as the table below
- 🚩 Note 3: All Linux Distributions such as **Redhat, Mint, Ubuntu, Mac OS X**, etc are all consolidated under the Account type of **Linux** in the table below.
- 🚩 Note 4: **VMWare ESXi** accounts can use either **SSH** or **HTTPS** to connect. If you use SSH, choose the **Linux Reset** script option. If you prefer to use HTTPS, check the **VMWare ESXi** requirements in the table below
- 🚩 Note 5: For **Windows** operating systems, Server 2012 R2 and above are supported

Account Type	Port Requirements	Passwordstate Web Server Requirements	Privileged Account Required?	Notes
Active Directory	9389, 389 or 636, 88, 464	1. <b>RSAT Tools</b> needs to be installed on web server – See section <b>On Premise Active Directory Passwords</b> in this documentation below for more information.	Yes	1. Privileged Account must have <b>Account Operator</b> rights when changing passwords on the domain, or delegate equivalent permissions 2. If you need to change passwords for accounts which have <b>Domain Admin</b> rights, then your Privileged Account may also need Domain Admin rights, or delegate equivalent permissions
Cisco IOS	22	None	Yes or No – See Notes →	1. When resetting Cisco accounts, a <b>Privilege Level 15</b> type account must be used in order to perform the reset. This is either for a Privileged Account Credential if being used, or the account on the password record itself, if not using a Privileged Account Credential

				<ol style="list-style-type: none"><li>When resetting the <b>enable</b> password, you must use a Privileged Account Credential which will SSH to the Cisco device, and this account performs the password reset for enable. The Username field for the password record itself must be named as '<b>enable</b>'</li><li>This script will work if the account's password is of type '<b>secret</b>' or '<b>password</b>'</li><li>If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li><li>If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li></ol>
Dell iDRAC	22	None	No – See Notes →	<ol style="list-style-type: none"><li>The reset script for this account type does not use a Privileged Account, so assigning one to the password record is not recommended as it will have no effect</li><li>The user will connect into the <b>iDrac</b> as itself and reset its own password</li><li>Requires <b>RACADM</b> tools to be installed on the <b>iDRAC card</b></li><li><b>iDrac</b> cards with firmware version 4.40 or high has replaced <b>getconfig</b> command with <b>get</b> command. <b>get</b> commands no longer return the index number of the user account, so you must manually set the index number for each account running on these firmware versions. See <b>iDrac</b> example in <b>section Dell iDrac Accounts</b> in this documentation below for more information.</li><li>If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li></ol>

				6. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user
<b>F5 BIG-IP</b>	22	None	<b>Yes</b>	1. Accounts in <b>BIG-IP</b> appliances can be configured with Terminal Access of type ' <b>Advanced Shell</b> ' or ' <b>TMSH</b> '. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset Script
<b>F5 BIG-IP</b>	22	None	<b>Yes</b>	1. Accounts in <b>BIG-IP</b> appliances can be configured with Terminal Access of type ' <b>Advanced Shell</b> ' or ' <b>TMSH</b> '. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset Script
<b>Fortigate</b>	22	None	<b>No</b> – See Notes →	<p>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</p> <p>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</p>
<b>HP H3C</b>	22	None	<b>Yes</b>	None
<b>HP iLO</b>	22	None	<b>No</b> – See Notes →	<p>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</p> <p>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</p>
<b>HP Procurve</b>	22	None	<b>Yes or No</b> – See Notes →	1. The only account which has permissions to change passwords is the <b>Manager</b> account. If you are wanting to reset the password for the <b>Operator</b> account, you need to

				associate a Privileged Account Credential to the password record - where the Privileged Account Credential is the <b>Manager</b> account
<b>IBM IMM</b>	22	None	<b>Yes or No</b> – See Notes →	<ol style="list-style-type: none"> <li>1. When resetting passwords on IBM IMM cards, you must know the <b>LoginID</b> of the account you wish to reset passwords for. In order to use this script, you must configure <b>Generic Field 1</b> on the <b>PasswordList</b> named as '<b>LoginID</b>'. See <b>IBM IMM Accounts</b> in this documentation below for more information.</li> </ol>
<b>Juniper Junos</b>	22	None	<b>No</b> – See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>
<b>Juniper NetScreen ScreenOS</b>	22	None	<b>Yes</b> – See Notes →	<ol style="list-style-type: none"> <li>1. The Privileged Account can be used to reset the root account, and any other non-root accounts</li> </ol>
<b>Linux</b>	22	None	<b>Yes or No</b> – See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. See section <b>Password Resets and Account Validation for Linux Root Accounts</b> in this documentation below for more information.</li> <li>3. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> <li>4. If your <b>root</b> account has SSH abilities, it will connect to the host and reset its own password. If SSH for <b>root</b> is disabled, you'll need to assign a Privileged Account that will connect</li> </ol>

				<p>to the host and reset the <b>root</b> password. See section <b>Password Resets and Account Validation for Linux Root Accounts</b> in this documentation below for more information.</p> <ol style="list-style-type: none"> <li>When resetting passwords for <b>Mac OS X</b>, no Privileged Account Credential is required, as OSX prevents one account from updating the keychain of another account</li> <li>Public/Private Key authentication can also be used with the Privileged Account Credential to connect to the Host. See example in Section SSH Accounts with Public/Private Key Authentication in this documentation below for more information.</li> <li>Please note that for '<b>root</b>' accounts, the password value for the root account in Passwordstate must be correct before any password resets can occur. This means that if you are using a Linux Account Discovery Job, and a root account is discovered and added into a Password List, then you must edit the password record and make the following changes: <ul style="list-style-type: none"> <li>Untick the option '<b>Password Enabled for Resets</b>'</li> <li>Reset the password to the correct value save the record</li> <li>Edit the record again, tick the 'Password Enabled for Resets', and save the record again</li> </ul> </li> </ol>
<b>MariaDB</b>	3306	None	<b>No</b> – See Notes →	<ol style="list-style-type: none"> <li>If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>

<b>MS SQL Server</b>	1433	None	<b>Yes or No</b> – See Notes →	<ol style="list-style-type: none"> <li>1. Firewall allows access on SQL Server port – default port is <b>1433</b> for SQL Standard and above, and SQL Express can use a Dynamic Port – generally <b>49260</b></li> <li>2. You must also have the <b>TCP/IP Protocol</b> enabled for SQL Server, and this can be done using the SQL Server Configuration Manager Utility, under the section <b>SQL Server Network Configuration</b> -&gt; <b>Protocols</b> for &lt;InstanceName&gt;. Generally, this is not enabled for SQL Server Express</li> <li>3. The Privileged Account Credential you are using to perform resets must have the '<b>ALTER ANY LOGIN</b>' permission as minimum in order to perform resets. The Privileged Account Credential can be either an SQL Account, or an Active Directory Account - if an AD Account, the Username field must be in the format of <b>domain\Username</b>. If no Privileged Account Credential is being used, an SQL Account can change its own password without any special privileges required in SQL Server.</li> <li>4. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>5. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>
<b>MySQL Server</b>	3306	None	<b>No</b> – See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>

<b>Office 365 and Microsoft Entra ID</b>	NA	<ol style="list-style-type: none"> <li>1. <b>Azure Az PowerShell module</b> – See <b>section Office 365 and Microsoft Entra ID Accounts</b> in this documentation below for more information.</li> <li>2. Internet access</li> </ol>	Yes or No – See Notes →	<ol style="list-style-type: none"> <li>1. See section <b>Office 365 and Microsoft Entra ID Accounts</b> in this documentation below for more information.</li> <li>2. Username in password record must be the Entra ID “<b>User principal name</b>” of the account being reset – See <b>Password Record Examples</b> section further down in this guide</li> <li>3. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the Tenant and reset its own password</li> <li>4. If you do assign a Privileged Account, this Privileged Account will connect to the Tenant and reset the password for the user</li> </ol>
<b>Oracle DB Server</b>	1521	<b>Oracle Data Access Components (ODAC)</b> – See <b>Section 4</b> in this documentation below for more information.	Yes or No – See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>
<b>Palo Alto</b>	22	None	No – See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> <li>3. Public/Private Key authentication can also be used with the Privileged Account Credential to connect to the Host. See section <b>SSH Accounts with Public/Private Key Authentication</b> in this documentation below for more information.</li> </ol>



PostgreSQL	5432	None	Yes or No: See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>
SonicWALL	22	None	Yes or No: See Notes →	<ol style="list-style-type: none"> <li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li> <li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li> </ol>
Windows OS	5985 or 5986	None	Yes or No: See Notes →	<ol style="list-style-type: none"> <li>1. <b>PowerShell 3.0</b> or above required on Remote Host</li> <li>2. <b>PowerShell Remoting</b> enabled on Remote Host</li> <li>3. If you are performing resets <b>Local Administrator Windows Accounts on Non-Trusted Active Directory Domains</b>, or against <b>WorkGroup</b> computers, see section <b>Account Discovery and Password Resets between Non-Trusted Domains, or against Workgroup Computers</b> in this documentation below for more information.</li> <li>4. If you edit the scheduled task and make a change, then you will need to confirm the current password when saving changes. Doing this removes the domain from the Scheduled Task and prevents Passwordstate from discovering it. Ensure you type in your username as <b>domain\username</b> when saving a Scheduled Task</li> <li>5. Port 5985 uses <b>HTTP</b> and this is the default Powershell protocol. Port 5986 uses <b>HTTPS</b> and the <b>-UseSSL</b> parameter on all Invoke-Command cmdlets. Search <b>Administration</b> -&gt;</li> </ol>

				<b>System Settings</b> in Passwordstate for <b>usessl</b> to toggle this setting on or off.  6. Powershell traffic through HTTP is still encrypted, but HTTPS is an extra layer of security
<b>VMWare ESXi</b>	443	<b>VMWare PowerCLI Powershell module</b> – See section <b>VMWare ESXi Accounts - PowerCLI Powershell Module</b> in this documentation below for more information.	<b>Yes or No:</b> See Notes →	<ol style="list-style-type: none"><li>1. If you do not assign a Privileged Account on your password record for this account, the user will attempt to connect to the host and reset its own password</li><li>2. If you do assign a Privileged Account, this Privileged Account will connect to the Host and reset the password for the user</li></ol>


### Open Ports Requirements

For a full list of open port requirements for Password Resets, you can refer to section '**Password Resets**' in the following document -

[https://www.clickstudios.com.au/downloads/version9/Passwordstate\\_Open\\_Port\\_Requirements.pdf](https://www.clickstudios.com.au/downloads/version9/Passwordstate_Open_Port_Requirements.pdf)

## 5 Password Validation Script Requirements

Password Validation (**Account Heartbeats**) is also achieved using a variety of different PowerShell scripts, and each of the Validations Scripts has the same System Requirements as the equivalent Password Reset Script.

- 🚩 Note 1: Validations can also be performed manually in the User Interface of Passwordstate, either from the 'Actions' dropdown menu for a password record, or when you open the password record you will also see the following Heartbeat icon 
- 🚩 Note 2: For Windows operating systems, Server 2012 R2 and above are supported

### Open Ports Requirements


For a full list of open port requirements for Password Resets, you can refer to section '**Account Validation (Heartbeats)**' in the following document - [https://www.clickstudios.com.au/downloads/version9/Passwordstate\\_Open\\_Port\\_Requirements.pdf](https://www.clickstudios.com.au/downloads/version9/Passwordstate_Open_Port_Requirements.pdf)


## 6 Password Discovery Script Requirements

The following Discovery jobs are provided to help discover Local Admin Accounts on your network, and various 'Windows Resources' – such as Windows Services, IIS Application Pools and Scheduled Tasks, database accounts, network accounts, etc:

- Active Directory accounts
- Cisco IOS accounts
- Fortigate accounts
- HP H3C accounts
- Juniper Junos accounts
- Linux and MAC accounts
- Microsoft SQL Database accounts
- MariaDB Database accounts
- MySQL Database accounts
- Oracle Database accounts
- PostgreSQL Database accounts
- SonicWALL accounts
- Windows Dependency accounts such as domain accounts used on Windows Services, IIS Application Pools and Windows Scheduled Tasks
- VMWare ESXi accounts

 Note 1: Each of the Discovery jobs above have the same System Requirements as their respective Password Reset Scripts

 Note 2: For SQL Server account discoveries, the Privileged Account Credential you are using to perform resets must have the '**ALTER ANY LOGIN**' permission as minimum. The Privileged Account Credential can be either an **SQL Account**, or an **Active Directory Account** - if an Active Directory account, the Username field must be in the format of **domain\Username**. Your SQL Server must be configured in mixed-mode authentication in order to discover SQL Accounts.

 Note 3: For Windows operating systems, Server 2012 R2 and above are supported

🚩 Note 3: The Active Directory '**Password Reset**' and '**Account Discovery**' features requires the '**Remote Server Administration Tools (RSAT)**' to be installed on your Passwordstate web server, or where you have deployed the 'Remote Site Locations Agent'. On Windows Server Operating Systems, you can install this by running the following PowerShell command (run PowerShell as Admin):

#### **Add-WindowsFeature RSAT-AD-PowerShell**

If your Passwordstate web server is running Windows 10 Operating System, please see this link to get these RSAT tools installed:

<https://docs.microsoft.com/en-US/troubleshoot/windows-server/system-management-components/remote-server-administration-tools>

#### **Open Ports Requirements**

For a full list of open port requirements for Password Resets, you can refer to section '**Account Discoveries**' in the following document -

[https://www.clickstudios.com.au/downloads/version9/Passwordstate\\_Open\\_Port\\_Requirements.pdf](https://www.clickstudios.com.au/downloads/version9/Passwordstate_Open_Port_Requirements.pdf)

## 7 Enabling PowerShell Remoting per Host

All versions of Windows Desktop Operating Systems, and Windows Server 2008, do not have PowerShell Remoting enabled by default. It can be enabled on each Host individually by following these steps:

- On the destination Host, run PowerShell as an Administrator
- Now type **Enable-PSRemoting –Force**

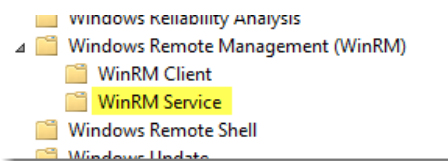
Running this command performs the following:

- Sets the 'Windows Remote Management' service to Automatic (delayed), and starts it
- Enables a HTTP listener
- Adds a firewall exception

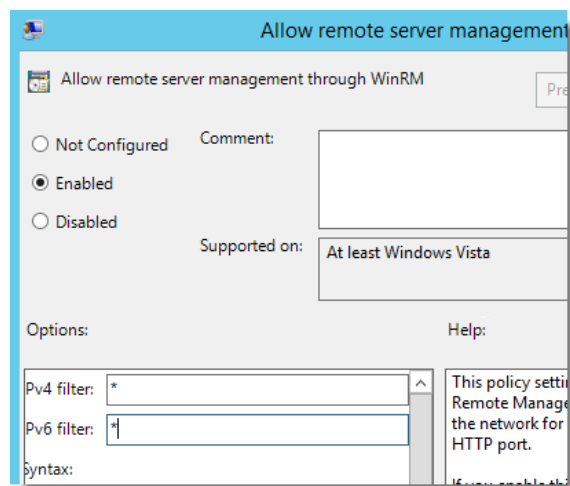
## 8 Enabling PowerShell Remoting via Group Policy

To enable PowerShell Remoting for multiple hosts at a time in your environment, you can use Group Policy to make the required changes. The following instructions provide detail of how to do this (screenshots here are from a Windows Server 2012 R2 domain controller):

- Open the Group Policy Management Console
- Create or use an existing Group Policy Object, open it, and navigate to **Computer Configuration -> Policies -> Administrative templates -> Windows Components**
- Here you will find the available Group Policy settings for Windows PowerShell, WinRM and Windows Remote Shell:

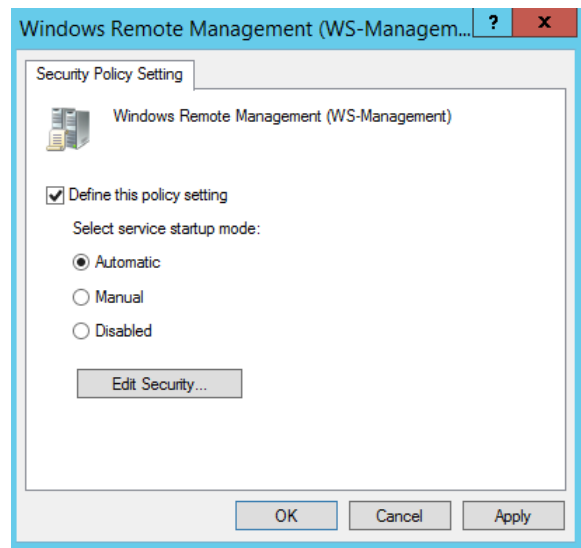


- Open “**Allow remote server management through WinRM**” setting
- Enable the Policy and set the IPv4 and IPv6 filter values to \*



- Click OK

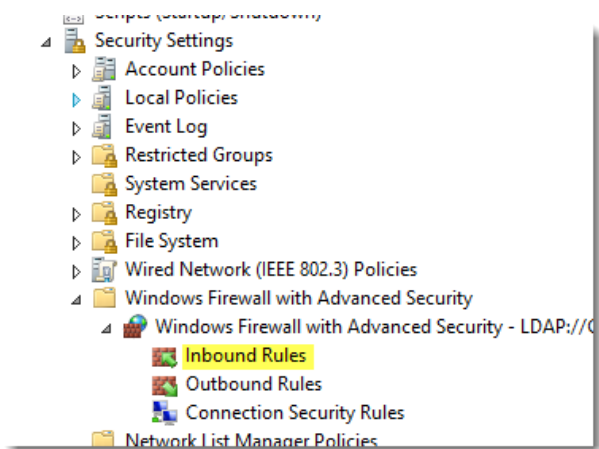
- Navigate to **Windows Settings -> Security Settings -> System Services**
- Select **Windows Remote Management (WS-Management) Service** and set the start-up mode to Automatic



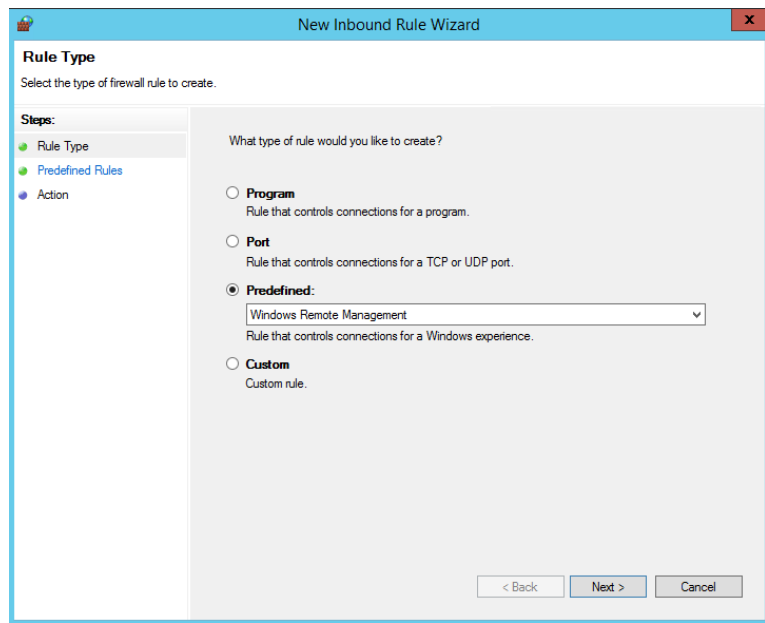
- Click OK



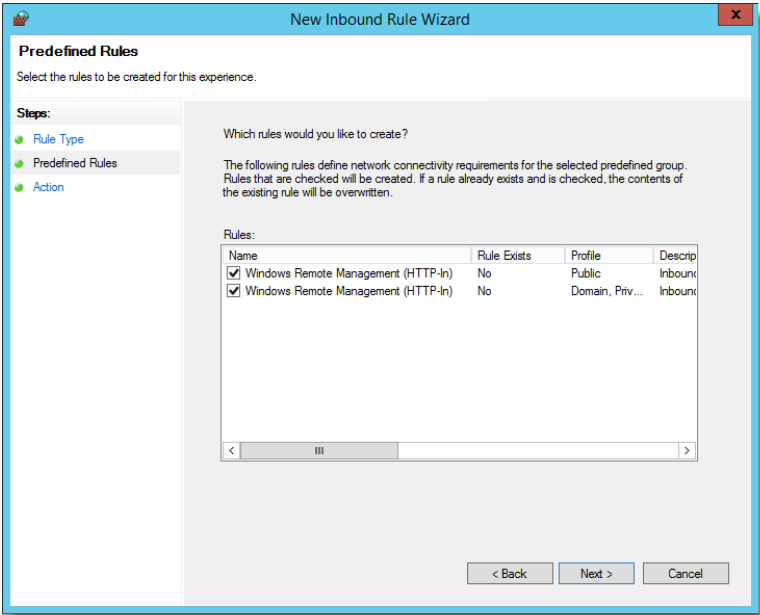
- You need to create a new Inbound Rule under **Computer Configuration-> Policies -> Windows Settings -> Windows Firewall with Advanced Security-> Inbound Rules**:



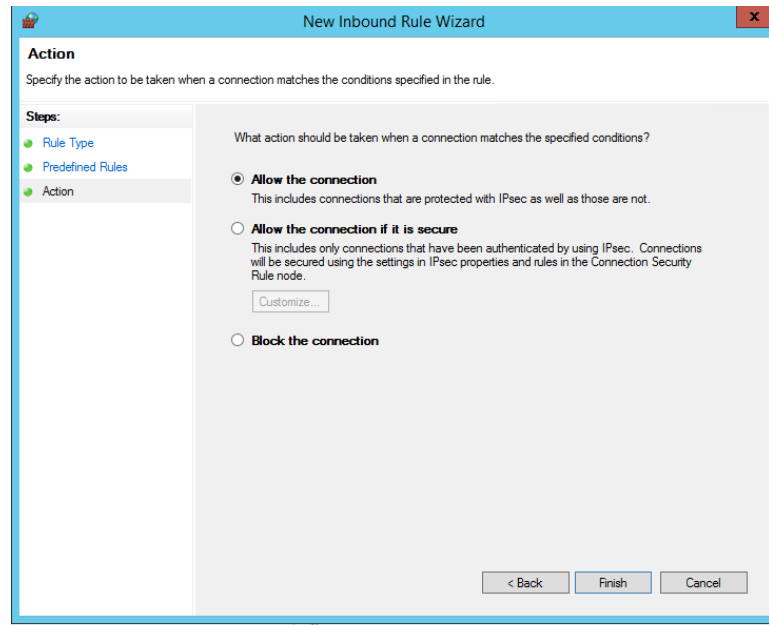
- The WinRM port numbers are predefined as “**Windows Remote Management**”:



- With WinRM 2.0, the default http listener port is TCP 5985.



- Select **“Allow the Connection”**



- Close the Group Policy Editor
- Link the PowerShell Settings GPO to correct OU for testing
- Run gpupdate on your test computers, or reboot them

## 9 Hosts in Non-Trusted Domains

It is also possible to perform Password Reset, Validations and Discoveries for hosts which are in non-trusted domains. For this to occur, the following is required:

- Functioning DNS so domain controllers and Hosts can be contacted
- Firewall ports must be open to allow traffic through. Please refer to the following Open Ports documents which describes all features/modules of Passwordstate - [https://www.clickstudios.com.au/downloads/version9/Passwordstate\\_Open\\_Port\\_Requirements.pdf](https://www.clickstudios.com.au/downloads/version9/Passwordstate_Open_Port_Requirements.pdf)
- A Privileged Account Credential must be supplied on the screen **Administration -> Passwordstate Administration -> Privileged Account Credentials**, in FQDN format i.e. [user@mydomain.com](mailto:user@mydomain.com)
- The Active Directory Domain information needs to be added on the screen **Administration -> Passwordstate Administration -> Active Directory Domains**, and then linked to the relevant Privileged Account Credential you created in the above step
- When adding host records on the Hosts screen, it is recommended the Host names are specified using FQDN i.e. [serverabc@mydomain.com](mailto:serverabc@mydomain.com)

## 10 Account Discovery and Password Resets between Non-Trusted Domains, or against Workgroup Computers

If you are wanting Passwordstate to perform Account Discovery and Password Resets between non-trusted domains, or on computers which are not joined to the domain, you will need to configure PowerShell on your Passwordstate Web Server to “trust” all remote hosts. You can do this by running the following PowerShell command:

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -value *
```

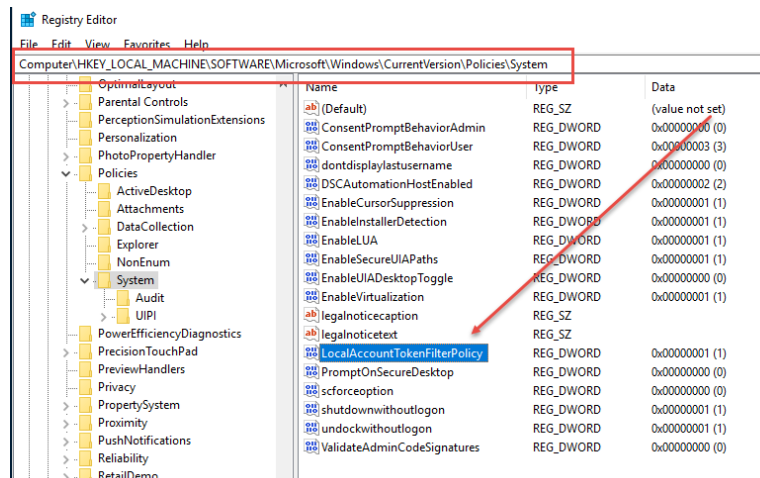
Account Discoveries on Work Group machines will also need to enable the following registry key on the remote host to avoid ‘WinRM’ errors, which are related to UAC blocking Powershell Remoting sessions when used with the Invoke-Command Powershell commandlet, which is what we use to do discoveries.

Path = **HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**

Registry Key Name = **LocalAccountTokenFilterPolicy**

Type = **REG\_DWORD**

Data = **1**

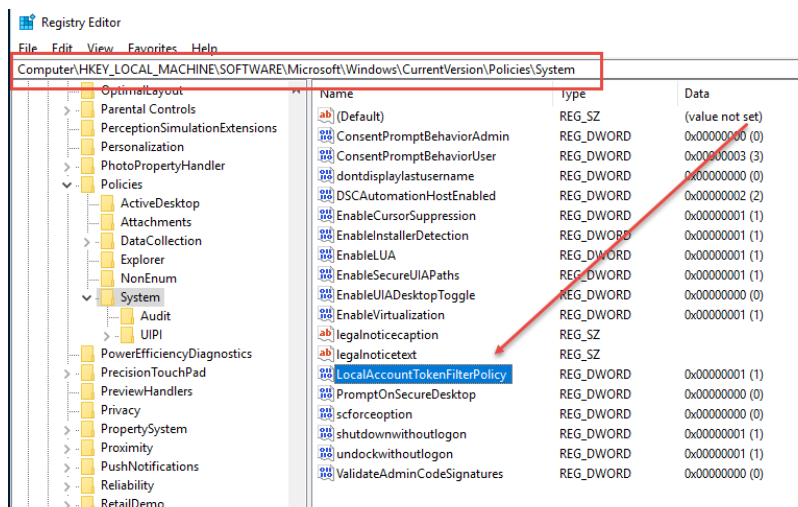


Please restart the Passwordstate Windows Service after making these changes.

## 11 Local Administrator Account Password Resets Without the Use of a Privileged Account Credential

If you are wanting to perform Password Resets on Windows Local Administrator Accounts, but not associated a Privileged Account Credential with the password record in Passwordstate i.e. reset the password using its own account, then you may need to add/enable the following registry key on the remote host to avoid 'Access Denied' PowerShell Remoting issues.

- Path = **HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
- Registry Key Name = **LocalAccountTokenFilterPolicy**
- Type = **REG\_DWORD**
- Data = **1**



## 12 Password Resets and Account Validation for Linux Root Accounts

By default, most Linux Operating Systems do not allow you to SSH in using the root account – for security reasons.

Because of this restriction, it is recommended on the root password record in Passwordstate, that you select a 'Privileged Account Credential' which can SSH into the Linux Host, and perform Password Resets and Account Heartbeats.

Example Screenshots of a Password Record configured to use a Privileged Account to reset and validate a root account:

**Edit Password**

Please edit the password below, stored within the '**Linux Accounts**' Password List (Tree Path = \Infrastructure).

**password details** **notes** **security** **reset options** **heartbeat options**

**Password Reset Script and Privileged Account Credentials**

Please select the appropriate Password Reset Script, and Privileged Account Credential, in order to perform the password reset.

Password Reset Script: **Reset Linux Password**

Privileged Account: **msand on Redhat01**

**Password Reset Schedule**

☐ When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:  
00 Hour 00 Minute, and add 90 Days to the Expiry Date

**Heartbeat Validation Options**

Select the **Password Validation Script** to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:

**Validate Password for Linux Account**

☒ Use the Privileged Account Credential selected on the 'Reset Options' tab to perform the authentication for this validation (only used for Linux root accounts if required):

**Validate Password every day at:**  
09 Hour 36 Minute

Save Cancel

Password Reset tasks will be queued if Password updated. Save Cancel

In order to perform an Account Heartbeat in Passwordstate for the root account, when using a different Privileged Account credential, changes are required to each of the Sudoers file on your Linux desktops/servers. Below are the changes required:

- Open the Sudoers file with visudo using the following command:

**Sudo visudo -f /etc/sudoers**

- When editing the Sudoers file, scroll to the bottom and add the following two lines, entering in the appropriate username you use in Passwordstate as your Privileged Account:

**## Enable sudo rootpw for Passwordstate Privileged Account**  
**Defaults:<username> rootpw**

### Password Reset Implications

With this change above to the sudoers file, this has implications for password resets for the root account, as the “current” password value for the root account must be set correctly in Passwordstate for this to work. Below is example PowerShell code for how password resets are occurring with this type of configuration:

```
echo -e '$OldPassword\n$NewPassword\n$NewPassword' | sudo -S passwd $UserName
```

The \$ symbol represent parameters passed to the reset script, and \$OldPassword in this case is the current value of the password stored in Passwordstate.

### Account Discovery Implications

If you are wanting to configure an Account Discovery Job for root accounts, this requirement for password resets to have the current password stored for the root account in Passwordstate can cause complications. The two options for this are:

- If your root accounts on all machines use the same password value, then on the Discovery Job you can specify this password to be set on discovery
- If the above is not possible, then each of the accounts added into Passwordstate will need to be modified after they are discovered, and have the password set with the correct value. To do this you can edit the password record and:
  - Untick the option 'Password Enabled for Resets'
  - Reset the password to the correct value save the record
  - Edit the record again, tick the 'Password Enabled for Resets', and save the record again

Once this is done, schedule and manual password resets can occur for your root accounts.

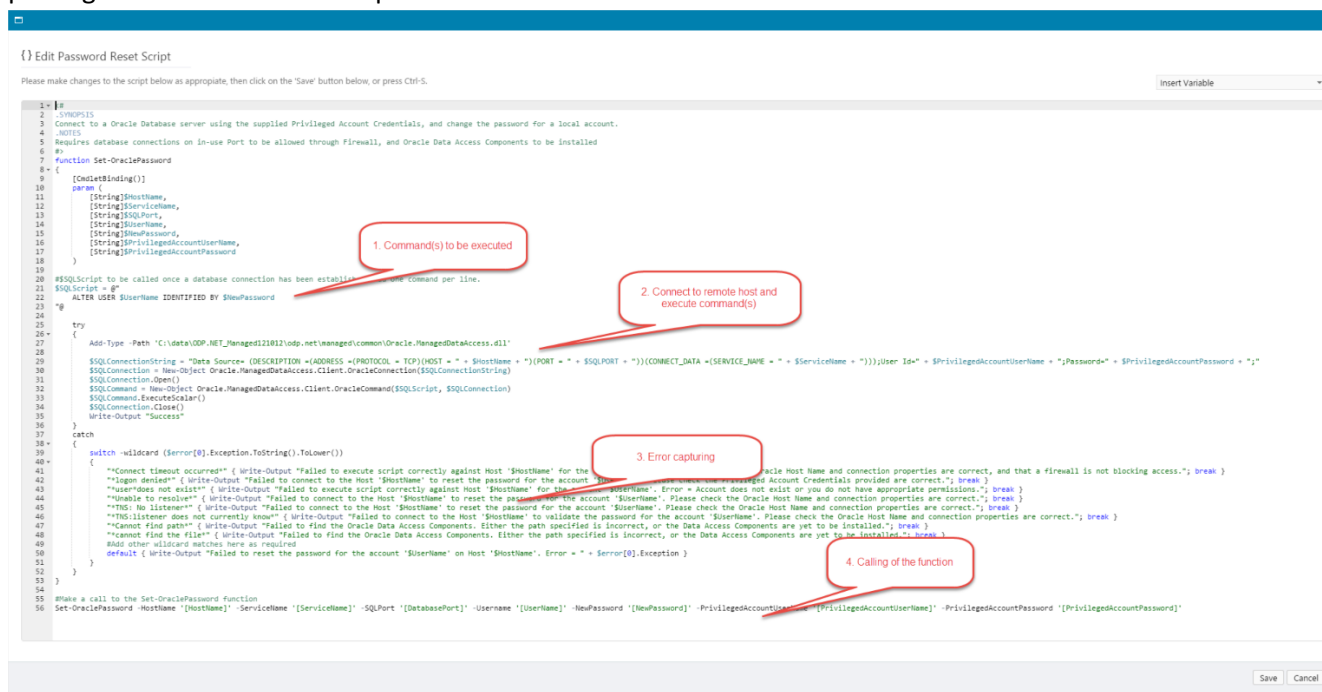


## 13 Structure of a Password Reset Script

When creating your own Password Reset Scripts, we recommend that you copy one of ours as a basis for your own. We recommend this so that the Passwordstate Windows Service understands when the script has been executed successfully, or has failed.

There are 4 key areas in all of our scripts, and there is a screenshot below which highlights these areas. They are:

1. Command(s) to be executed - this is the actual work done on the remote host to reset a password
2. Connect to remote host to execute command(s) - this connectivity method will vary on the host, but generally it is done via PowerShell Remoting, SSH connection, or a direct connection to a database server
3. Error Capturing - this is where we try and capture as many of the error scenarios as possible. The error messages here will be included in the email report you receive when a Password Reset attempt has failed for whatever reason
4. Calling the function - this is what initiates the call to all the 3 steps above it. The variables you see here, enclosed in square brackets [], are replaced in real-time by the Passwordstate Windows Service when the reset occurs - it queries relevant data from the password record, the host record, and possibly the privileged account record if required



## 14 SSH Template Scripts

With some default PowerShell Scripts provided by Click Studios, we use an SSH Library from a company called Chilkat. Due to licensing restrictions of this SSH .NET Assembly, customers are not allowed to clone our scripts which use this assembly, and then modify it for their own needs.

To help you build your own custom scripts for systems that use the SSH connection protocol, Click Studios has included two new '**SSH Templated**' Powershell scripts, which allow you to specify SSH command line parameters to be passed to the remote system. The two types of Templates Scripts are:

- Remote Commands
- Remote Shell

Please see details below for further instructions on these two templated scripts.

### ***14.1 SSH Template - Remote Commands***

Typically, this template is used for sending single line commands to the remote host, and receiving output back. Equivalent scripts within Passwordstate which execute commands in this manner are:

- Reset F5 BIG-IP Account Password – AS
- Reset F5 BIG-IP Account Password – TMSH
- Reset IBM IMM Account Password
- Reset Linux Password

Below is a screenshot of an example for resetting the password on a Redhat Linux account. In the example below, you can see that variables from a password record can be passed in the commands as well, and these are replaced real-time when the script executes. The example below shows **[NewPassword]**, and **[UserName]**:

### ➤ Edit Password Reset Script

Please make changes to the script's settings as appropriate below, then click on the 'Save' button. Please refer to the Security Administrator's Manual for instructions for each of these tabs.

script details

commands to execute

success and error conditions

Please specify your reset commands as appropriate, and reorder them in the order they need to be executed in.

Command

Comment

Add

Actions	Order	Command	Comment
▼	⋮	echo -e \$'[NewPassword]\n[NewPassword]'   passwd [UserName]	Reset Command

Save

Cancel

Please see section **16.4 'SSH Template Variables'** below for a comprehensive list of variables you can issue in your commands.

## 14.2 SSH Template - Remote Shell

Typically, this template is used for opening a pseudo terminal on the remote host, and executing one or more commands within the terminal session, where you can also 'wait' for an expected result back from the operating system. Equivalent scripts which execute commands in this manner are:

- Reset Cisco Host Password
- Reset Dell iDRAC Account Password
- Reset Fortigate Password
- Reset Juniper Junos Password
- Reset Palo Alto Password
- Reset SonicWALL Password

Below is a screenshot of an example for resetting the password on a **Palo Alto Firewall** account. In addition to the commands being issued, you can also 'Wait' for a certain response from a command, before moving onto the next command. If you do not need to wait for a certain response, then simply include the \* symbol:

[Edit Password Reset Script](#)

Please make changes to the script's settings as appropriate below, then click on the 'Save' button. Please refer to the Security Administrator's Manual for instructions for each of these tabs.

script details

commands to execute

success and error conditions

Please specify your reset commands as appropriate, and reorder them in the order they need to be executed in.

Command

Wait For Output

Comment

\*

Add

Actions	Order	Command	Wait For Output	Comment
▼	::	configure	*[edit]*	
▼	::	set mgt-config users [UserName] password	*Enter password*	
▼	::	[NewPassword]	*	
▼	::	[NewPassword]	*	
▼	::	commit	*[edit]*	
▼	::	exit	*Exiting configuration mode*	
▼	::	exit	*	

Save

Cancel

### 14.3 SSH Template Success and Error Conditions

With the SSH Templated Scripts we provide, it is recommended you specify both "**success**" and "**error**" condition capturing, if possible. Some operating systems/devices, do not return any sort of "success" message after a successful password reset, so it is important in this instance to specify as many "error" capturing conditions as possible - otherwise the scripts will assume a successful reset has completed.

In our SSH template scripts, we have our own built in error capturing for any sort of connectivity issues to the remote host. The error capturing details you provide are designed to report errors once you are already connected to this host, within the SSH session.

Below is a screenshot of success and error capturing for Linux machines. When you determine which "**commands to execute**" for your device, it is recommended that during your testing within the SSH session, you try and capture as many possible errors as you can.

#### ➤ Edit Password Reset Script

Please make changes to the script's settings as appropriate below, then click on the 'Save' button. Please refer to the Security Administrator's Manual for instructions for each of these tabs.

script details

commands to execute

success and error conditions

The Templated Scripts provide error capturing for host connectivity, and you are also able to add your own Success and Error Condition checking for the execution of commands on the 'Commands to Execute' tab.

Please refer to the Security Administrators guide for recommendations on specifying Success and Error Condition capturing.

Result Type

Results Match

☒ Error Condition ☐ Success Condition

Add

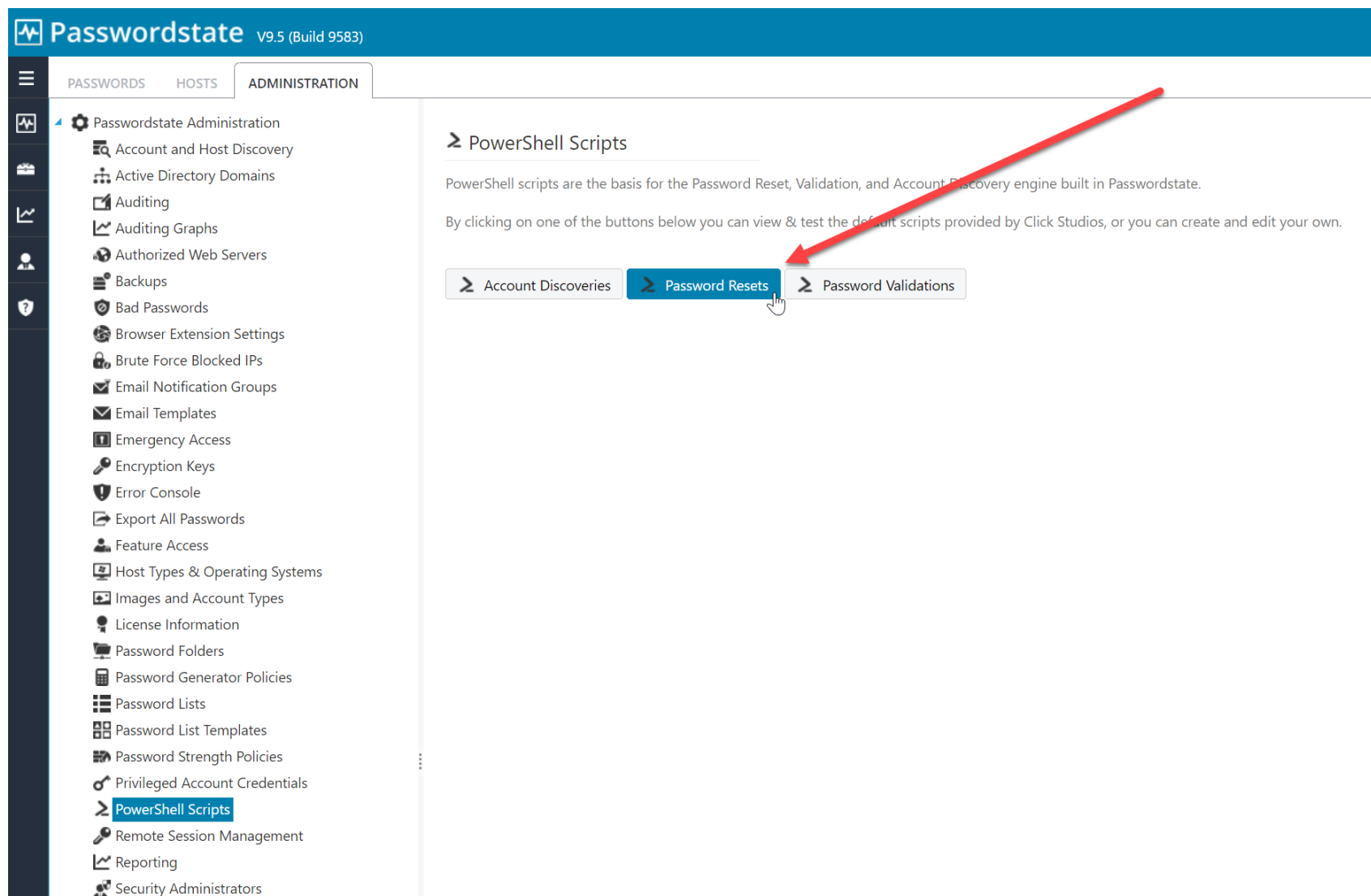
Actions	Results Match	Results Type
▼	updated successfully	Success Condition
▼	BAD PASSWORD: it is WAY too short	Error Condition
▼	Failed preliminary check	Error Condition
▼	unknown user name	Error Condition
▼	Weak password	Error Condition
▼	You must choose a longer password	Error Condition

Save

Cancel

## 14.4 Creating SSH Template Scripts

To create a new script, navigate to **Administration -> Powershell Scripts -> Password Resets**:



Click on **Add New Script**

➤ Password Reset Scripts

Below are all the Password Reset Scripts you can associate with a password record, to be executed when the password is updated.

Script Filters

☒ Show all Scripts ☐ Show only Inbuilt Scripts

Actions	Script Name	Description
⚙	➤ Cisco Small Business	Cisco Small Business
⚙	➤ Cisco Small Business Remote Shell	Cisco Small Business Remote Shell
⚙	➤ Custom Fortigate Script	Used for Firmware devices 6.4.7
⚙	➤ Reset Active Directory Password	Reset the password for an Active Directory account
⚙	➤ Reset Cisco Host Password	Reset the password on a Cisco switch Or router
⚙	➤ Reset Dell iDRAC Account Password	Reset Dell iDRAC Account Password
⚙	➤ Reset F5 BIG-IP Account Password - AS	Reset F5 BIG-IP Account Password - Advanced Shell Terminal Access
⚙	➤ Reset F5 BIG-IP Account Password - TMSH	Reset F5 BIG-IP Account Password - TMSH Terminal Access
⚙	➤ Reset Fortigate Password	Reset the password for a Fortigate account
⚙	➤ Reset HP H3C Password	Reset HP H3C Account Password

Page: 1

Return Previous Screen | **Add New Script** | Toggle Visibility of Web API IDs | Grid Layout Actions...

Give your script a **Name** and **Description** of your choice, and copy the contents from the SSH Template of your choice:

➤ Add Password Reset Script

Please specify the script's settings below, then click on the 'Save' button.

**Note:** The actual editing of the script can be done on the previous page once you save this record, by clicking on the 'Script Name' hyperlink you see within the grid view.

script details

Please specify the settings as appropriate below.

Script Name : \*

Script Description : \*

Copy Script Contents From :

Please note after clicking Save, you need to edit the script properties and specify the commands you would like to send to this script, before it can be associated with a Password record.

Save Cancel

You can now **Edit Script Settings**, and begin building your commands. When ready, you can test your script by choosing the **Test Script Manually** option on the **Actions** menu:

## ➤ Password Reset Scripts

Below are all the Password Reset Scripts you can associate with a password record, to be executed when the password is updated.

Script Filters

☒ Show all Scripts
 ☐ Show only Inbuilt Scripts

Actions	Script Name	Description
<div> <div>⊕</div> <div> <div>✖ Delete</div> <div>{ } Edit Script Settings</div> <div>▶ Test Script Manually</div> </div> </div>	➤ Cisco CBS-200 Switches	Cisco Small Business Series switches
		Used for Firmware devices 6.4.7
		Reset the password for an Active Directory account
		Reset the password on a Cisco switch Or router
⊖	➤ Reset Dell iDRAC Account Password	Reset Dell iDRAC Account Password
⊖	➤ Reset F5 BIG-IP Account Password - AS	Reset F5 BIG-IP Account Password - Advanced Shell Terminal Access
⊖	➤ Reset F5 BIG-IP Account Password - TMSH	Reset F5 BIG-IP Account Password - TMSH Terminal Access
⊖	➤ Reset Fortigate Password	Reset the password for a Fortigate account
⊖	➤ Reset HP H3C Password	Reset HP H3C Account Password
⊖	➤ Reset HP iLO Password	Reset HP iLO Account Password

⏪ ⏴

1 2 3 4 ⏵ ⏩

[Return Previous Screen](#) | 
 [Add New Script](#) | 
 [Toggle Visibility of Web API IDs](#) | 
 

Grid Layout Actions... ▾

Once you can confirm your script works well, you will be able to assign it to any password record where the Password List is **Enabled for Resets**.



## 15 PowerShell Script Variables

Below are the variables which can be included in the PowerShell Scripts Click Studios provide, or the ones you add into Passwordstate yourself.

Variables which have '**SecureString**' appended to the variable name, will be passed as an encrypted Secure String value to the PowerShell script. This is useful for customers who choose to enable full PowerShell logging at the operating system level, where various PowerShell data can be logged into the Windows Application Event Log. By default, this level of logging is not enabled in Windows.

- [HostName]
- [RemoteConnectionPort]
- [OperatingSystem]
- [UserName]
- [OldPassword]
- [OldPasswordSecureString]
- [NewPassword]
- [NewPasswordSecureString]
- [EnablePassword]
- [PrivilegedAccountUserName]
- [PrivilegedAccountPassword]
- [PrivilegedAccountPasswordSecureString]
- [KeyType]
- [PrivilegedAccountPassPhrase]
- [PrivilegedAccountPrivateKey]
- [URL]
- [GenericField1]
- [GenericField2]
- [GenericField3]
- [GenericField4]
- [GenericField5]
- [GenericField6]
- [GenericField7]
- [GenericField8]
- [GenericField9]
- [GenericField10]

- [GenericField1SecureString]
- [GenericField2SecureString]
- [GenericField3SecureString]
- [GenericField4SecureString]
- [GenericField5SecureString]
- [GenericField6SecureString]
- [GenericField7SecureString]
- [GenericField8SecureString]
- [GenericField9SecureString]
- [GenericField10SecureString]

## 16 On Premise Active Directory Passwords

Passwordstate can reset the password for many different types of systems, including Active Directory accounts. This section guides you through the process of setting up an On Premise Active Directory account for automatic resets.

Most other Password Resets are similar in nature to this example below, but for those that require slight customizations, there is more information about these in the **Password Record Examples** section below in this manual.

The Active Directory '**Password Reset**' and '**Account Discovery**' features requires the '**Remote Server Administration Tools (RSAT)**' to be installed on your Passwordstate web server, or where you have deployed the '**Remote Site Locations Agent**'. On Windows Server Operating Systems, you can install this by running the following PowerShell command (run PowerShell as Admin):

### Add-WindowsFeature RSAT-AD-PowerShell

If your Passwordstate web server is running Windows 10/11 Operating System, please see this link to get these RSAT tools installed:

<https://docs.microsoft.com/en-US/troubleshoot/windows-server/system-management-components/remote-server-administration-tools>

### 16.1 Privileged Account Credential

For Passwordstate to be able update passwords in Active Directory, it needs to use a domain account with elevated privileges to do so. While it's possible to customize permissions in Active Directory, generally adding your Privileged Account to the "**Account Operators**" security group in Active Directory will be enough to reset the passwords for most accounts.

If you are resetting passwords on accounts with a higher level of permission, such as a Domain Administrator account, you may need to elevate the permissions on your privileged account to achieve a successful reset.

To add a Privileged Account, first ensure you have created a user in Active directory and add it to the "**Account Operators**" security group. Next, in Passwordstate, go to **Administration** -> **Privileged Account Credentials**, and click the **Add** button. On the screen, enter a **Description**, enter the username in the form of **domain\username**, select the account type as "**Active Directory**", and set the current password for the account in Active Directory.

**Add Privileged Account Details**

Please specify details as appropriate below, then click on the Save button. Once the record has been saved you need to apply permissions.

**Note:** If no permissions are applied to this account, then it cannot be used to perform any Account Discovery or Password Resets.

**privileged account credentials** **public key authentication**

Please specify appropriate details below, then click on the Save Button.

Description \*

UserName \*

For Active Directory Accounts, specify the format of domain\userid.

Site Location

Account Type

Password

Confirm Password

Link To Password

If you link this Privileged Account to a password record which is enabled for Password Resets, then the Privileged Account Credential password will be updated once the password reset is complete. **Note:** Only passwords which have been enabled for Reset, plus match the UserName above, will be visible here.

## 16.2 Add Appropriate Domains to the Active Directory Domains Screen

By default, you should already have one Active Directory Domain added to the screen **Administration -> Active Directory Domains**. If you want to synchronize password changes with other domains which aren't listed, then you must add them to this screen. Ensure you assign your Privileged Account that you created in the step above:

**Passwordstate V9.0 (Build 9000)**

**ADMINISTRATION**

- Account and Host Discovery
- Active Directory Domains**
- Auditing
- Auditing Graphs
- Authorized Web Servers
- Backups and Upgrades
- Bad Passwords
- Browser Extension Settings
- Brute Force Blocked IPs
- Email Notification Groups
- Email Templates
- Emergency Access
- Encryption Keys
- Error Console
- Export All Passwords
- Feature Access
- Host Types & Operating Systems
- Images and Account Types
- License Information
- Password Folders

**Edit Active Directory Domain**

To edit the selected Active Directory Domain, please fill in the details below.

AD Domain NetBIOS Name \*

FQDN

AD Domain LDAP Query String \*

Domain Controller FQDN

e.g. adserver1.clickstudios.com.au (this should only be required if you need to connect to a specific domain controller to improve performance of the Active Directory synchronization process)

Site Location

Account with Read Access

Default Domain ☒ Default Domain

Used For Authentication ☒ Yes ☐ No (Show domain in dropdown list on Authentication Screens)

Protocol ☒ LDAP (Port 389) ☐ LDAPS (Port 636)

16.3 Configure a Password List for Password Resets

Now that the domain and privileged account is set, we need to configure a Password List so that it is enabled for Password Resets. To do this you need to check the option 'Enable Password Resets' on your Password List:

**Add New Password List**

To add a new Password List, please fill in the details below for each of the various tabs.

**Note:** You will receive **Administrator** permissions to the Password List once it is created (unless you're copying permissions from another Password List).

Please note: A setting on your Preferences screen, or a User Account Policy applied to your account, has configured various settings for new Password Lists.

password list details | customize fields | guide | api key & settings

Please specify Password List settings manually below.

**Password List Details**

Site Location: Internal

Password List \*: Active Directory Accounts

Description:

Image: useraccounts.png

Password Strength Policy \*: Default Policy

Password Generator Policy \*: Default Password Generator

Code Page \*: Use Passwordstate Default Code Page

Additional Authentication \*: None Required

**Password List Settings**

☒ This will be a Shared Password List

☒ Enable Password Resets - allows password resetting with other systems

☐ Enable One-Time Password Generation

☒ Allow Password List to be Exported

☐ Time Based Access Mandatory

☐ Disable Inheritance of any upper level folder permission propagation

☐ Multiple Approvers Mandatory - a total of 1 approver(s) are required for this List

☒ Prevent Password reuse for the last 5 passwords

**Copy Details & Settings From**

Copying a Template or another Password List's fields/settings on this screen, except for any API Key.

Web Site Logins

☐ Link this Password List to the selected Template

**Copy Permissions From**

If you would like to copy permissions from an existing Password List, please select the appropriate option below.

**Default Password Reset Schedule**

Please specify the default settings for 'Reset Options' added to this Password List.

☒ Enable the the Password Reset Schedule for reset at a random time between the two time

Setting this option above will also enable the **Account Type** field on your Password List, which will allow you select any type of managed account when adding in a new password record:

**Edit Password List Properties**

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

password list details | customize fields | guide | api key & settings

Below you can specify which fields are available, which ones are required fields, and select one or more of their options accordingly.

**Standard Fields**

Field Name	Required	Hide Column
<input checked="" type="checkbox"/> Title	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> User Name	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Description	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Account Type	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> URL	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password Strength	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Expiry Date	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Notes	<input type="checkbox"/>	<input type="checkbox"/>

## 16.4 Configure a Password for Password Resets

When adding in a new account into your Password List that is enabled for resets, you should specify the following:

1. Enable the option to perform **Password Resets** and **Heartbeats**
2. Select the '**Active Directory**' Account Type
3. Select the appropriate Domain by searching for it
4. Specify the **Username** of the account
5. Setting an **Expiry date** will trigger an automatic reset once it occurs
6. Clicking the **Heart** icon will do a live test to see if the password is in sync with Active Directory

**Add New Password**

Add new password to 'Active Directory Accounts' Password List (Tree Path = \).

password details	notes	security	reset options	heartbeat options
<p>Title *</p> <p>Managed Account</p> <p>Account Type</p> <p>Domain</p> <p>UserName</p> <p>Description</p> <p>Expiry Date</p> <p>Password Generator</p> <p>Password *</p> <p>Confirm Password *</p> <p>Password Strength</p> <p>Compliance Strength</p> <p>Strength Status: 8 more characters</p> <p><input checked="" type="checkbox"/> Compliance Mandatory <input checked="" type="checkbox"/> Prevent Bad Password Usage</p>				

1. Arrow pointing to the 'reset options' tab.

2. Arrow pointing to the 'Enabled for Resets' checkbox.

3. Arrow pointing to the 'Active Directory' account type dropdown.

4. Arrow pointing to the 'Domain' search field.

5. Arrow pointing to the 'Expiry Date' field.

6. Arrow pointing to the heart icon in the password field.

Buttons: Save, Save & Add Another, Cancel

On the **Reset Options** tab, you must also select the Privileged Account Credential with sufficient permissions to reset the password in Active Directory. The **Password Reset Script** will automatically be selected for you, and if you want to set a future time and date for when to automatically reset the password again, set the appropriate option under the **Password Reset Schedule**:

**Add New Password**

Add new password to 'Active Directory Accounts' Password List (Tree Path = \).

password details notes security **reset options** heartbeat options

**Password Reset Script and Privileged Account Credentials**

Please select the appropriate Password Reset Script, and Privileged Account Credential, in order to perform the password reset.

Password Reset Script: Reset Active Directory Password

Privileged Account: Active Directory Account used to Reset Passwords

Not all Reset Scripts require a Privileged Account. See KB Article in menu Help -> User Manual.  
Active Directory Accounts do not require you to select a Reset Script.

**Password Reset Schedule**

☒ When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:  
00 Hour 00 Minute, and add 90 Day(s) to the Expiry Date.

Save Save & Add Another Cancel

Under the **Heartbeat Options** tab, a **Validation Script** will be automatically set for you, and you can choose a **custom time of the day** to perform a Heartbeat:

**Edit Password**

Please edit the password below, stored within the 'Active Directory Accounts' Password List (Tree Path = \).

password details notes security **reset options** **heartbeat options**

**Heartbeat Validation Options**

Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct.

Validate Password for Active Directory Account

☐ Use the Privileged Account Credential selected on the 'Reset Options' tab to perform the authentication for this validation (only used for Linux accounts if required):

**Validate Password every day at:**  
07 Hour 15 Minute

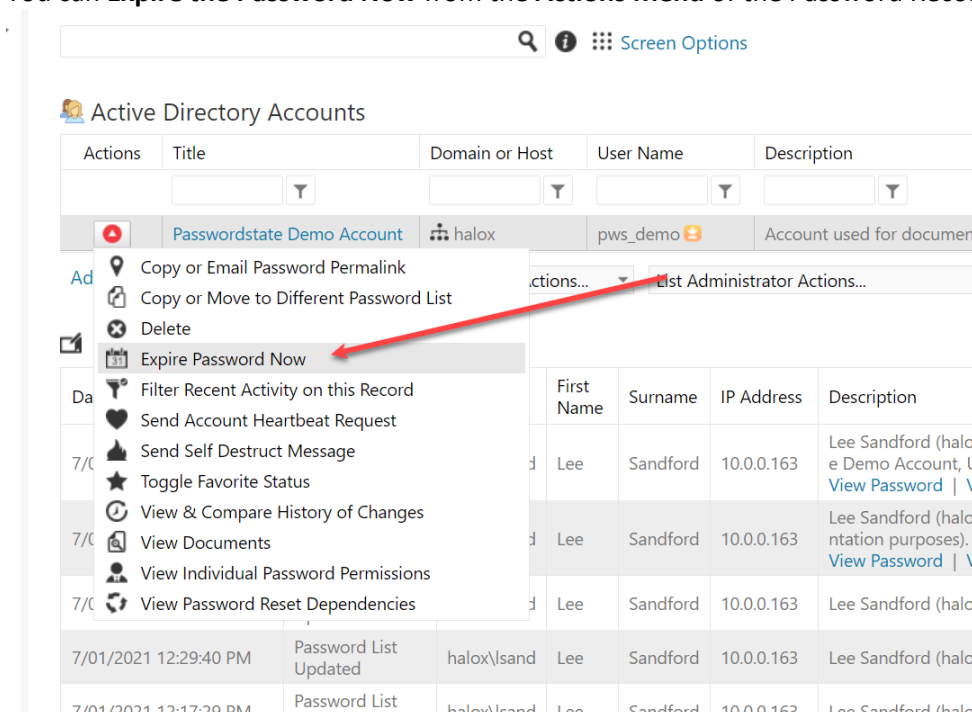
Password Reset tasks will be queued if Password updated.

Save Cancel

## 16.5 Triggering a Reset

There are a few different ways a password can be reset once you have set up your record:

1. If you open the record, and set a new password, and then save your changes, this will then update the password in Active Directory
2. If the **Expiry Date** on the password record expires, this will change the password to a random password, based on the **Password Generator Policy** you have set on your **Password Record**
3. You can **Expire the Password Now** from the **Actions Menu** of the Password Record:



- Note 1:** If a Scheduled reset was to fail for any reason, no changes will be made to the password record, and the Expiry Date field will not be updated. By not updating the Expiry Date field, another attempted reset will occur at the same time the following day.
- Note 2:** It's not recommended to set up a standard user Active directory account to do automatic resets as per the above example. If Passwordstate were to automatically reset a user account, then that user would not be able to log into Passwordstate to retrieve the new password. Resetting Active Directory accounts in Passwordstate is mainly designed for things like Privileged Service Accounts, or shared accounts, not user's primary domain accounts.

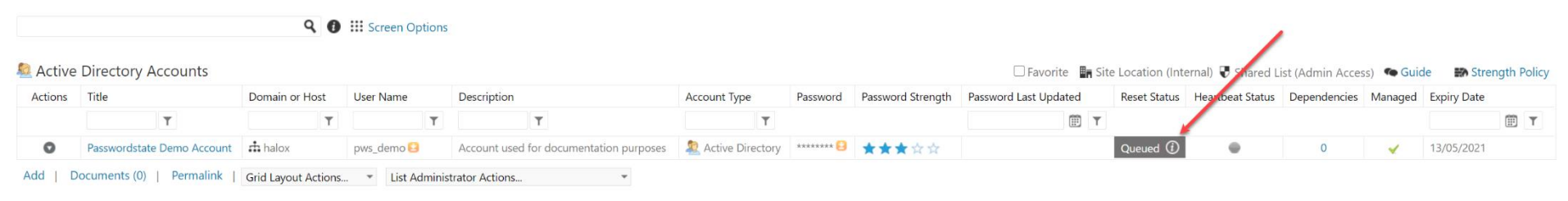


## 17 Password Reset Queuing System

There are various conditions in which a password reset can be triggered, and they are:

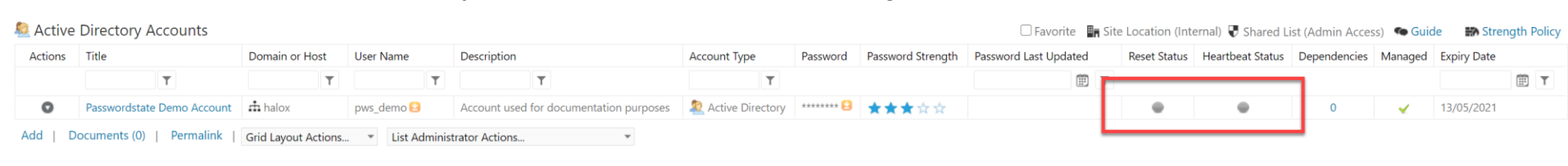
1. Someone manually changes the value of the password on the **Edit Password** screen
2. When someone manually updates the value of the password via the **API**
3. A **Scheduled Reset** occurs
4. The '**Change Password On Check In**' option is selected for a record, for the **Check In/Check Out** feature
5. When the option to reset a password is selected for **Time Based Access permissions** to individual password records
6. When **Expiring the Password Now** via the **Actions Menu** on the Password Record

When any of the above events are triggered, the password record is added to a queue to perform the reset. No changes will be made to the password record itself, until the queued record has finished processing. In the Passwords grid, it will show the record is queued, and clicking on the **white Information icon**, will filtering the auditing records for you for this account and refresh the **Reset Status Grid**.



Actions	Title	Domain or Host	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
<a href="#">Add</a>	<a href="#">Documents (0)</a>	<a href="#">Permalink</a>	Grid Layout Actions...		List Administrator Actions...				Queued ⓘ		0	✓	13/05/2021

The **Reset Status** and **Heartbeat Status** are **Grey** in color if no action has ever been taken against the Password Record:



Actions	Title	Domain or Host	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
<a href="#">Add</a>	<a href="#">Documents (0)</a>	<a href="#">Permalink</a>	Grid Layout Actions...		List Administrator Actions...						0	✓	13/05/2021

They will be **Green** if the last **Password Reset** or **Heartbeat** was successful, and **Red** indicates the last reset or heartbeat was not successful, in which case you should investigate the cause for this. To investigate why a Password Reset or Heartbeat has failed, look in the **Recent Activity Grid**, or possibly in the **Auditing Data** under **Tools -> Auditing**, or **Administration -> Auditing**.

As you can see in the example below, my Password Reset failed because I did not have the Active Directory module for PowerShell installed on the Passwordstate web server, which is available when installing RSAT Tools (Pre-requisite outlined in **Section 2** of this document):

The screenshot displays the Passwordstate V9.0 (Build 9000) interface. The left sidebar shows the navigation menu with 'Reports', 'Auditing', 'Auditing Graphs', and 'Scheduled Reports'. The main content area is divided into two sections: 'Active Directory Accounts' and 'Recent Activity'.

**Active Directory Accounts Table:**

Actions	Title	Domain or Host	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
	Passwordstate Demo Account	halox	pws_demo	Account used for documentation purposes	Active Directory	*****	★★★★☆		●	●	0	✓	13/05/2021

**Recent Activity Grid:**

Date	Activity	UserID	First Name	Surname	IP Address	Description
7/01/2021 1:19:22 PM	Password Reset Removed from Queue	WindowsService	Windows Service	Account	10.0.0.91	The Passwordstate Windows Service removed the account 'Passwordstate Demo Account' (Password List = \Active Directory Accounts, UserName = pws_demo, Description = Account used for documentation purposes) from the Queue as the Process Reset Task is now complete. This account relates to an Active Directory account on the domain halox (halox.net). <a href="#">View Password</a>   <a href="#">View History</a>
7/01/2021 1:19:22 PM	Password Reset Failed	WindowsService	Windows Service	Account	10.0.0.91	The Passwordstate Windows Service failed to reset the password for 'pws_demo' (Active Directory Accounts) with the Active Directory domain 'halox.net'. As a result, no changes have been made to this record in Passwordstate. Error = Failed to reset the password for the account 'pws_demo' in Active Directory domain 'halox.net'. It appears you do not have the Active Directory module for Powershell installed on your s <a href="#">View Password</a>   <a href="#">View History</a>   <a href="#">View Failed Reset History</a>
7/01/2021 1:14:46 PM	Password Reset Added to Queue	halox\lsand	Lee	Sandford	10.0.0.163	Lee Sandford (halox\lsand) manually modified the Password for account 'Passwordstate Demo Account' (Password List = \Active Directory Accounts, UserName = pws_demo, Description = Account used for documentation purposes), resulting in a record being added to the queue to perform appropriate Password Reset tasks. This account relates to an Active Directory account on the domain halox (halox.net). <a href="#">View Password</a>   <a href="#">View History</a>
7/01/2021 1:14:37 PM	Password Screen Opened	halox\lsand	Lee	Sandford	10.0.0.163	Lee Sandford (halox\lsand) opened the Edit Password screen for password 'Passwordstate Demo Account' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = Passwordstate Demo Account, UserName = pws_demo, Description = Account used for documentation purposes). <a href="#">View Password</a>   <a href="#">View History</a>
7/01/2021 1:13:09 PM	Password Screen Opened	halox\lsand	Lee	Sandford	10.0.0.163	Lee Sandford (halox\lsand) opened the Edit Password screen for password 'Passwordstate Demo Account' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = Passwordstate Demo Account, UserName = pws_demo, Description = Account used for documentation purposes). <a href="#">View Password</a>   <a href="#">View History</a>

Page 1 of 3, items 1 to 5 of 11.

After installing the RSAT Tools, the next Password Reset is successful:

The screenshot shows the 'Active Directory Accounts' interface. At the top, there's a search bar and 'Screen Options'. Below, a table lists accounts. The 'Passwordstate Demo Account' is highlighted. A red box highlights the 'Reset Status' column, showing a green circle indicating success. Below the table, the 'Recent Activity' section shows a log of events. A red box highlights the entry: 'The Passwordstate Windows Service successfully reset the password for 'pws\_demo' (Active Directory Accounts) with the Active Directory domain 'halox.net'.' The entry includes a timestamp, activity type, user ID, first name, surname, IP address, and a description. The interface also includes a 'Change page' dropdown and a 'Page 1 of 4, items 1 to 5 of 18' indicator.

Actions	Title	Domain or Host	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
	Passwordstate Demo Account	halox	pws_demo	Account used for documentation purposes	Active Directory	*****	★★★★☆	7/01/2021 1:38:43 PM			0		13/05/2021

Date	Activity	UserID	First Name	Surname	IP Address	Description
7/01/2021 1:38:43 PM	Password Reset Removed from Queue	WindowsService	Windows Service	Account	10.0.0.91	The Passwordstate Windows Service removed the account 'Passwordstate Demo Account' (Password List = 'Active Directory Accounts, UserName = pws_demo, Description = Account used for documentation purposes) from the Queue as the Process Reset Task is now complete. This account relates to an Active Directory account on the domain halox (halox.net).
7/01/2021 1:38:43 PM	Password Reset Successful	WindowsService	Windows Service	Account	10.0.0.91	The Passwordstate Windows Service successfully reset the password for 'pws_demo' (Active Directory Accounts) with the Active Directory domain 'halox.net'.
7/01/2021 1:38:43 PM	Password Updated	WindowsService	Windows Service	Account	10.0.0.91	The Passwordstate Windows Service successfully reset the password for 'pws_demo' (Active Directory Accounts) with the Active Directory domain 'halox.net'.
7/01/2021 1:38:29 PM	Password Reset Added to Queue	halox\lsand	Lee	Sandford	10.0.0.163	Lee Sandford (halox\lsand) manually modified the Password for account 'Passwordstate Demo Account' (Password List = 'Active Directory Accounts, UserName = pws_demo, Description = Account used for documentation purposes), resulting in a record being added to the queue to perform appropriate Password Reset tasks. This account relates to an Active Directory account on the domain halox (halox.net).
7/01/2021 1:38:22 PM	Password Screen Opened	halox\lsand	Lee	Sandford	10.0.0.163	Lee Sandford (halox\lsand) opened the Edit Password screen for password 'Passwordstate Demo Account' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = Passwordstate Demo Account, UserName = pws_demo, Description = Account used for documentation purposes).

If needed, you can also monitor the status of all queued records to all Password Lists you have access to on the screen Resets -> Queued Password Resets, as per the screenshot below. This will also show auditing data for all the queued records you see on his screen.

The screenshot shows the 'Passwordstate V9.0 (Build 9000)' interface. The left sidebar has a menu with 'Tools' expanded, showing 'Account Discovery', 'Have I Been Pwned Password Check', 'Password Generator', 'Password Resets In Progress' (highlighted with a red arrow), and 'Self Destruct Message'. The main area is titled 'Password Resets In Progress' and contains a description: 'Below are all the pending Password Reset tasks in the Queue at the moment, as well as most recent auditing data for these queued records. You can use the Queue to view the status of the tasks and to view the auditing data for the tasks.' There's a toggle for 'Enable Debug Logging' set to 'No'. Below, a section titled 'Password Reset Queue' shows a table with columns: 'Actions', 'Queued At', 'Title', 'Domain or Host', and 'UserName'. The table is empty, with the text 'No records to display.' below it. At the bottom, there are buttons for 'Refresh Both Grids', 'Export', 'Purge Queue', and a 'Grid Layout Actions...' dropdown. A 'Recent Activity' section is partially visible at the bottom.

## 18 Password Reset Dependency Records

In addition to performing Password Resets for accounts, you can also add various 'dependencies' to a password record, which can also trigger a Password Reset script after the password for the account has been successfully reset.

A typical example of this would be where the account is an Active Directory account, and it's being used as the "**identity**" for operations of Windows Services, Scheduled Tasks, IIS Application Pools or COM+ Components.

Alternatively, you can execute any type of PowerShell script that you supply, and this script does not need to necessarily need to be associated with a Host Record. Adding in your own custom scripts can be achieved under **Administration -> Powershell Scripts – Scripts – Password Reset**.

To add a "**dependency**" to a password record, you can either select the '**View Password Reset Dependencies**' menu item, or click the count in the **Dependencies** Column in the grid:

The screenshot displays the Passwordstate V9.0 (Build 9000) interface. The left sidebar shows the navigation menu with 'Active Directory Accounts' selected. The main grid displays a list of accounts under the 'Active Directory Accounts' section. The grid has columns for Actions, Title, Domain or Host, User Name, Description, Account Type, Password, Password Strength, Password Last Updated, Reset Status, Heartbeat Status, Dependencies, Managed, and Expiry Date. A red arrow points to the 'Dependencies' column header, which shows a count of 0. Another red arrow points to the 'View Password Reset Dependencies' menu item in the left sidebar. Below the grid, there is a detailed view of a password reset event, showing the account 'pws\_demo' and the user 'Lee Sandford'.

Actions	Title	Domain or Host	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
	Passwordstate Demo Account	halox	pws_demo	Account used for documentation purposes	Active Directory	*****	★★★★☆	7/01/2021 1:38:43 PM			0	✓	13/05/2021

First Name	Surname	IP Address	Description
Lee	Sandford	10.0.0.163	Lee Sandford (halox\Isand) granted Mark Sandford Modify Access to the Password List called 'Active Directory Accounts'.
sService	Windows Service	10.0.0.91	The Passwordstate Windows Service removed the account 'Passwordstate Demo Account' (Password List = 'Active Directory Accounts', UserName = pws_demo, Description = Account used for documentation purposes) from the Queue as the Process Reset Task is now complete. This account relates to an Active Directory account on the domain halox (halox.net).
sService	Windows Service	10.0.0.91	The Passwordstate Windows Service successfully reset the password for 'pws_demo' (\Active Directory Accounts) with the Active Directory domain 'halox.net'.
sService	Windows Service	10.0.0.91	The Passwordstate Windows Service successfully reset the password for 'pws_demo' (\Active Directory Accounts) with the Active Directory domain 'halox.net'.

Then click on “Add Dependency”

Password Reset Dependencies

Below are all the linked Password Reset tasks, or Post Reset tasks, for the password 'Passwordstate Demo Account'.

Hosts Filters

Host Name :  Host Type :  Operating System :  Database Server Type :

Actions	Order	Host Name	UserName	Script Name	Dependency Type
No records to display.					

[Back to Passwords](#) | [Add Dependency](#) |

On this screen below, choose the type of dependency you wish to add. If it is a **Windows Service**, **IIS Application Pool**, **Scheduled Task** or **COM+ Component**, a script will be assigned automatically for you. If you choose the Ignore button, this gives you the ability to assign your own PowerShell script.

Ensure you set the **Dependency Name** correctly, and then link it to the **Host** where the dependency resides:

Add Dependency

To link the password 'Passwordstate Demo Account' to a Host and Password Reset Script, please fill in the details below as appropriate.

script and host selection

Password Reset or Post Reset Script

Please select the appropriate Password Reset Script.

Password Reset Script:

Note: If you wish to execute a script Post Reset, you do not need to select a dependency, or Host record below to link it to - you can execute any custom script you like. The order in which scripts are executed can also be changed on the previous screen.

Windows Account Dependency

If the selected Password Reset Script is for one of the Windows Account 'Dependencies' types below, enter appropriate details here.

Dependency Name:

Dependency Type: ☐ Ignore ☒ Windows Service ☐ IIS Application Pool ☐ Scheduled Task ☐ COM+ Component

Link to Host(s)

If you want to execute the script above against one or more hosts, please select them below.

Host Name:  Host Type:  Operating System:

Database Server Type:

Hosts Search Results

Applied to Host(s):

>>  
<<

Note: This dependency will use the selected Privileged Account Credential to execute, of which is selected for the password record itself.

### ***18.1 Anatomy of a Password Dependency Reset***

As an example, in your environment you may have a domain account that is configured to “Log on As” on multiple Windows Services, across many different machines. It’s possible to set up this Active Directory Account, and have multiple “Dependencies” as per above example for each service the account is used on.

When a successful password reset occurs on the account in your Password Record, it will trigger each of the dependency scripts one at a time, which in this example will reset the password on all of the Windows Services.

If the password is not successfully updated in Active Directory for any reason, no dependencies will be updated.

## 19 Host and Account Discoveries

### 19.1 Explanation of Discovery Jobs

So far in this manual we've covered how to manually set up password records for automatic resets, with or without dependencies. There is a way to fully automate this using our Account Discoveries.

For all Discovery Jobs in Passwordstate bar the **Active Directory Accounts** job, you'll first need to import your **Hosts** into Passwordstate. A Host is otherwise known as a **Windows Desktop/Server**, **Linux Desktop/Server**, **Switch** or **Firewall** device.

Hosts can be added manually into the system one by one under the **Hosts** tab in Passwordstate, **Imported via CSV** file or there is a **Hosts Discovery Job** that will import all **Windows Servers** and/or **Desktops** in **Active Directory**. If your Linux machines are stored in Active Directory, the Host discovery job can automatically import these too.

As the Host Discovery job is only looking in AD, no specific system requirements are necessary, except you'll need a domain account with privileges to query Active Directory.

The following Account Discovery jobs are available:

1. Active Directory Accounts
2. Cisco IOS Accounts
3. Fortigate Accounts
4. HP H3C Accounts
5. Juniper Junos Accounts
6. Linux and Mac Accounts
7. MS SQL Database Accounts
8. MySQL Database Accounts
9. Oracle Database Accounts
10. PostgreSQL Database Accounts
11. SonicWALL accounts
12. Windows Dependency Accounts - Windows Services, IIS Application Pools and Scheduled Tasks which are configure to use a domain account as their identity
13. Windows Local Admin Accounts

- 🚩 Note 1: If discovering accounts on a Mac, the option to reset the password on discovery will be ignored, as another account (the Privileged Account Credential) cannot update the keychain for a different account - this is by design by Apple
- 🚩 Note 2: For the 'Active Directory Accounts' discovery job, this job should not be used for Privileged AD Accounts which are used on Windows Services, IIS App Pools and Scheduled Tasks - you should use the Windows Dependency Discovery Job for that purpose
- 🚩 Note 3: For the 'MS SQL Database Accounts' discovery job, the Privileged Account to be used to can be either a SQL Account, or an Active Directory account

## 19.2 Setting up a Host Discovery

Setting up a Host Discovery job can be done by going to **Hosts** tab -> **Hosts Home** -> **View Host Discovery Jobs** -> **Add Discovery Job**:

Passwordstate V9.0 (Build 9000)

PASSWORDS HOSTS ADMINISTRATION

Search Hosts ...

Hosts Home

- Click Studios
- Customers
- Firewalls
- Internal Infrastructure
- MySQL Servers
- Switches

### Host Discovery Jobs

Below are all the Host Discovery jobs added to Passwordstate, for querying Active Directory for host records.

Actions	Job Name	Description	Job
	<input type="text"/>	<input type="text"/>	<input type="text"/>
▼	Import Server Hosts	Import Server Hosts	H
▼	Test Import	Test Import	H
▼	Windows Server 2019 Discovery	Find all Windows Server 2019 machines in Sandbox OU	H

[Return to Hosts Home](#) | [Add Discovery Job](#) | [Grid Layout Actions](#)



On this page, you have the following options available to you:

1. Which Active Directory domain to query
2. To query specific AD OUs, you can click on the '**Active Directory OUs**' tab and specify them here
3. Run the job in **Simulation Mode** – This will execute the job, but not add any data into Passwordstate. This is handy to see what will happen before adding any data into your production system
4. Which type of Hosts you want to discover, based on the **Operating System**
5. Only discover Hosts which have been logged into based on a set date i.e. only machines logged into since July 2020
6. You can also set the **Tag** field for a Host to be the value of the Active Directory OU it belongs to
7. You also need to specify the '**Privileged Account**' identity which will be used to query your Active Directory Domain. These Privileged Account Credentials can be added/editing/updated on the screen **Administration** -> **Privileged Account Credentials**
8. The **Schedule** for how often you want the Discovery Job to be executed

**Edit Hosts Discovery Job**

To edit settings for the Discovery job below, please make changes as appropriate and then click on the 'Save' button.

discovery job settings | **active directory ous** | schedule

Discovery Job Name \* : Windows Server 2019 Discovery

Description \* : Find all Windows Server 2019 machines in Sandbox OU

Simulation Mode \* : Internal

Active Directory Domain \* : halox.net

Active Directory OUs : Please specify at least one OU on the 'Active Directory OUs' tab.

Simulation Mode : ☐ Simulation Mode will email you the results without adding/adding any data in the database

**Discovery Search Criteria**

Please select which search options you would like to define for the Discovery Job.

Discover hosts with the following Operating Systems: Windows Server 2019

Only discover Hosts where the Host Logged on date is greater than or equal to : [Date Picker]

**Discovery Actions**

Populate the Host's Tag field with the Organizational Unit (OU) it belongs to:

☒ Yes ☐ No

When a new Host is found, set its Remote Connection Properties to :

☒ RDP ☐ SSH ☐ Telnet ☐ VNC Port Number: 3389

If an existing Host in Passwordstate is no longer found in any of the OUs specified, perform the following action for the Host record in Passwordstate:  
(Note: Host records will not be deleted if there are Password records associated with them)

☒ Do Nothing ☐ Set it to Unmanaged ☐ Delete it

**Privileged Account Credentials**

Please select which Privileged Account Credential will be used to execute this Discovery Job.

Passwordstate Host Discovery Account

Save Cancel

When creating the discovery job, you will automatically be given permissions to edit it. You can grant permissions for any other Passwordstate user so they can also help you administer and monitor the discovery jobs.

- 🚩 Note: When query Active Directory for Hosts, it is the value of the OperatingSystem AD Attribute which is queried. If you go to the screen **Administration -> Passwordstate Administration -> Host Types & Operating Systems**, you can see what attribute is currently set for each different operating system.
- 🚩 Note: If you have configured emails in Passwordstate, anyone who has access to the discovery job will receive an email each time the job executes, advising the results

The Actions Menu allows you to run the Discovery job immediately, disable or enable the job, view the previous results and apply permissions.

The screenshot shows the 'Host Discovery Jobs' page. At the top, there's a search icon and the title 'Host Discovery Jobs'. Below it, a text line states: 'Below are all the Host Discovery jobs added to Passwordstate, for querying Active Directory for host records.' A table lists three jobs: 'Import Server Hosts', 'Test Import', and 'Windows Server 2019 Discovery'. The 'Windows Server 2019 Discovery' job is selected, and its context menu is open. Red callout boxes with numbers 1 through 4 point to specific elements: 1 points to the 'Import Server Hosts' job name, 2 points to the 'Run Discovery Job Now' action, 3 points to the 'View Discovery Job History' action, and 4 points to the 'View Permissions' action.

Actions	Job Name	Description	Job Type
	<input type="text"/>	<input type="text"/>	<input type="text"/>
	Import Server Hosts	Import S... Hosts	Hosts
	Test Import	Test Import	Hosts
	Windows Server 2019 Discovery	Find all Windows Server 2019 machines in Sandbox OU	Hosts

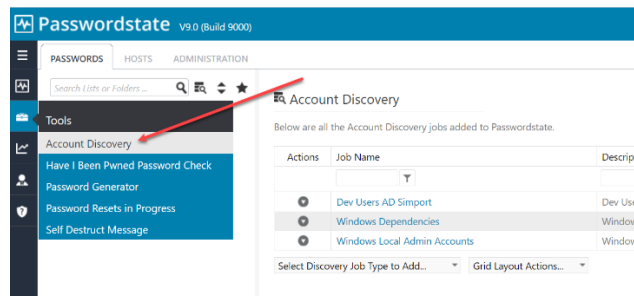
Context menu for 'Windows Server 2019 Discovery':

- Delete
- Run Discovery Job Now
- Toggle Status - Enabled or Disabled
- View Discovery Job History
- View Permissions

If a discovery job is successful, you will be able to see the imported Hosts under **Hosts** tab -> **Hosts Home** -> **View All Host Records**.

### 19.3 Setting up an Account Discovery

There are many different types of Account Discoveries which you can set up, and these can be found under **Tools -> Account Discovery**. As a Passwordstate Administrator, you can view and manage Account Discoveries that other users have set up under **Administration -> Account and Host Discoveries**.



**Active Directory Accounts** is the only job which does not scan Hosts attached to your network, rather this job scans Active Directory itself, and an explanation of this job can be found in **Section 19.4** below.

All other discovery jobs reach out to the host on the network, and will scan the host for any new accounts and add them into Passwordstate if they do not already exist. As with all Discovery jobs, you can run them in Simulation Mode so you do not impact production data.

### 19.4 Active Directory Discovery Job Explained

When creating an Active directory job, you have the following options available to you:

1. Which **Domain** you will be querying
2. Whether or not to run the job in **Simulation Mode**
3. Should the Discovery job report back all accounts it finds, or just the new ones? This can be handy if you want to troubleshoot a discovery job that you think may not be finding a specific account
4. You can either query one or more specific **OUs**, or **Security Groups**. In the example below, I'm discovering accounts in a specific Security Group
5. You can filter what accounts are discovered based on usernames, comma separated if you have multiple

6. If you want Passwordstate to automatically manage the passwords for the accounts the Discovery Job finds, you should select “**Enabled for Resets**” and “**Enabled for Heartbeats**”. If you deselect these options, the Discovery job will add the account into Passwordstate for you, but it will never manage the password for it, unless you explicitly tell the Password record to do so at a later date
7. The Password List you select needs to have the “**Enabled Password Resets**” option enabled on the actual Password List. If you do not have that Password List setting configured, it will not be available for you to choose from on your Discovery job. If the account is found in another Password List when the discovery executes, it will **not** add in a duplicate record
8. Option number 8 on the example below allows you to set a static password, or generate a random one for every account that is discovered

The screenshot shows the 'discovery job settings' form with the following annotations:

- 1: Discovery Job Name (Contractor Administrator Accounts)
- 2: Description (Track and maintain shared contractor Active Directory accounts)
- 3: Report on the following (Only newly Discovered Accounts)
- 4: Discover Accounts in Security Groups (Contractor Admin Accounts)
- 5: Exclude Accounts based on Username match (pwt\_demo\_pwt\_write)
- 6: Set the 'Managed Account' settings for newly discovered accounts (Enabled for Resets, Enabled for Heartbeat)
- 7: Add the newly discovered Accounts to the following Password List (Active Directory Accounts)
- 8: Set the password value in Passwordstate to be a randomly generated one (No) or set it to the following value:
- 9: Upon discovery, perform an immediate Password Reset for the account, based on the value of the password setting above: Yes
- 10: Privileged Account Credentials (Active Directory Account used to Reset Passwords)

### 19.5 Local Admin Discovery

Passwordstate has several different types of Local Admin account discovery jobs available to you, depending on the Operating system. When discovering Accounts on various Hosts, there are many options available to you:

1. Whether or not to run the job in **Simulation Mode**
2. Should the Discovery job report back all accounts it finds, or just the new ones? This can be handy if you want to troubleshoot a discovery job that you think may not be finding a specific account
3. You can filter on the type of Hosts you want to query, based on the **Operating System** type, or various other filters
4. If the Local Administrators group is in a different language, you can change the name of it so the discovery is successful
5. If you want Passwordstate to automatically manage the passwords for the accounts the Discovery Job finds, you should select “**Enabled for Resets**” and “**Enabled for Heartbeats**”. If you deselect these options, the Discovery job will add the account into Passwordstate for you, but it will never manage the password for it, unless you explicitly tell the Password record to do so at a later date
6. The Password List you select needs to have the “**Enabled Password Resets**” option enabled on the actual Password List. If you do not have that Password List setting configured, it will not be available for you to choose from on your Discovery job. If the account is found in another Password List when the discovery executes, it will **not** add in a duplicate record
7. As it's not possible to decrypt most passwords for discovered accounts, you will need to specify what password will be recorded in Passwordstate initially for the account, or you can generate a random one. You also have the option to perform a password reset for any newly discovered accounts
8. When new records are added to the selected Password List, you have the option to also specify some detail for the **Title** and **Description** fields.
9. You also need to specify the **Privileged Account Credential** to use when interrogating your Hosts on the network - this account will need sufficient privileges to interrogate the Host for local accounts - generally an account with Admin (elevated privileges) is required here



Note: Screenshots for all of the above points are on the next page

## Edit Windows Local Admin Accounts Discovery Job

To edit settings for the Discovery job below, please make changes as appropriate and then click on the 'Save' button.

discovery job settings

schedule

hosts to be queried

Discovery Job Name \*

Server Local Account Discovery

Description \*

Server Local Account Discovery

Site Location \*

Internal

Simulation Mode

☒ Simulation Mode will email you the results without adding/updating any data in the database

Report on the following:

☒ Only newly Discovered Accounts ☐ All Discovered Accounts - New or Existing

Discovery Search Criteria

Please select filtering options for which Hosts you wish to query for new accounts, as well as any filtering options for the names of accounts.

Host Types:

All Items checked

Operating Systems:

Windows Server 2019

Host Name Filter:

(Filter for hosts for matches like mydomain.com)

Tag Filter:

OU=Sandbox Testing DC=halox,DC=net

(Filter for hosts based on a value within Tag Field)

Exclude Hosts based on Host Name match:

hyperv0

Exclude Hosts based on Tag Field match:

Discover Accounts by Username match:

(leave blank to discover all accounts, or separate values using commas)

Exclude Accounts based on Username match:

(separate values using commas)

Local Administrators Group Name:

Administrators

(If required, you can comma separate different Security Group Names here - generally only required for Hosts configured for non English languages)

Discovery Actions

Please select appropriate options below when a new Accounts are discovered.

Set the 'Managed Account' settings for newly discovered accounts: (these settings can be changed after the record has been created if needed)

Enabled for Resets ☒ Enabled for Heartbeat ☒

Add the newly discovered Accounts to the following Password List: (New records will inherit the 'Default Schedule' from this Password List)

\\Sandbox Passwords\Windows Passwords

Set the password value in Passwordstate to be a randomly generated one ☐ Yes ☒ No or set it to the following value:

Passwordstate2019 this is only set in Passwordstate, unless you use the option below.

Upon discovery, perform an immediate Password Reset for the account, based on the value of the password setting above:

☒ Yes ☐ No

Set the following password 'Security' settings when newly discovered account are added to Passwordstate:

Password Requires Check Out ☐ Change Password On Check In ☐ Check In Automatically ☐ 01 Hour(s) 00 Minute(s)

or newly discovered accounts, use the following format for the naming of the Title and Description Fields: \*

(You can use the following variables within each of these fields [HostName] and [UserName], and they will be replaced accordingly)

Title [HostName]\[UserName] Description Local Administrator Account on [HostName]

For newly discovered accounts, assign the following Password Reset Script to the account:

Reset Windows Password

Privileged Account Credentials

Please select which Privileged Account Credentials will be used to execute this Discovery Job, and also to perform any Password Resets for discovered accounts.

Account to Discovery Hosts in AD


Save

Cancel

## 19.6 Windows Dependencies Discovery

It's possible to also discovery various '**Windows Dependencies**' on your network that are using domain accounts as their identity to run under i.e. **Windows Services, IIS Application Pools & Scheduled Tasks**. When setting up such a Discovery Job, the following options are available:

1. You need to select which '**Dependencies**' you want to try and discover - Windows Services, IIS Application Pools or Scheduled Tasks - can you select all of them as part of the same Discovery Job if you want
2. The rest of the options are very similar to discovery of other types of Accounts, as specified above
3. If you do not wish to automatically configure the discovered accounts to perform scheduled resets, you can set the '**Managed Account**' option to No. The later within the Password List, you can enable this option for one or more records at a time

 Edit Windows Dependency Discovery Job

To edit settings for the Windows Dependency Discovery job below, please make changes as appropriate and then click on the 'Save' button.

discovery job settings | **schedule** | hosts to be queried

Please update appropriate options for the Discovery Job below, and set the schedule as required.

Discovery Job Name \* : Windows Dependency Discovery

Description \* : Windows Dependency Discovery

Site Location \* : Internal

Active Directory Domain \* : halox.net Only accounts from this selected domain will be discovered

Simulation Mode : ☐ Simulation Mode will email you the results without adding/updating any data in the database

Report on the following: : ☒ All Discovered Dependencies - New, Existing or No Dependencies

Discovery Search Criteria

Please select which search options you would like to define for the Discovery Job.

Discover the following Dependencies configured to use an Active Directory account: **1**

☒ Windows Services ☐ IIS Application Pools ☐ Scheduled Tasks

Discover Dependencies on Hosts with the following Operating Systems: 7 items checked

Host Name Filter: webserv01 (Filter for hosts for matches like mydomain.com)

Tag Filter: (Filter for hosts based on a value within tag field)

Exclude Hosts based on Host Name match:

Exclude Hosts based on Tag Field match:

Discovery Actions

When a newly discovered Active Directory Account (being used by a Dependency) is found, check the 'Managed Account' option for the account to enable automatic scheduled resets: (If you select No, you can enable this option for one or more records at a later time - from within the appropriate Password List)

☒ Yes ☐ No **3**

Add newly discovered Active Directory Accounts (being used by a Dependency) to the following Password List

(Newly added password records will inherit the Default Schedule Options from this Password List)

\ Sandbox Passwords\Active Directory Test Accounts

When new accounts are discovered, set the initial password in Passwordstate to be: \*

Welcome01 this is only set in Passwordstate, and not in AD or on any Hosts, until the first Password Reset occurs.

When adding new password records to Passwordstate, use the following format for the naming of the Title and Description Fields: \*

(You can use the following variables within each of these fields [hostname], [username] and [domainOrHostDescription], and they will be replaced accordingly)

Title [username] Description [domainOrHostDescription] Account

Set the following password 'security' settings when a new account is added to Passwordstate:

Password Requires Check Out ☐ Change Password On Check In ☐ Check In Automatically 01 Hour(s) 00 Minute(s)

Privileged Account Credentials

Please select which Privileged Account Credentials will be used to execute this Discovery Job, and also to perform any Password Resets for discovered accounts.

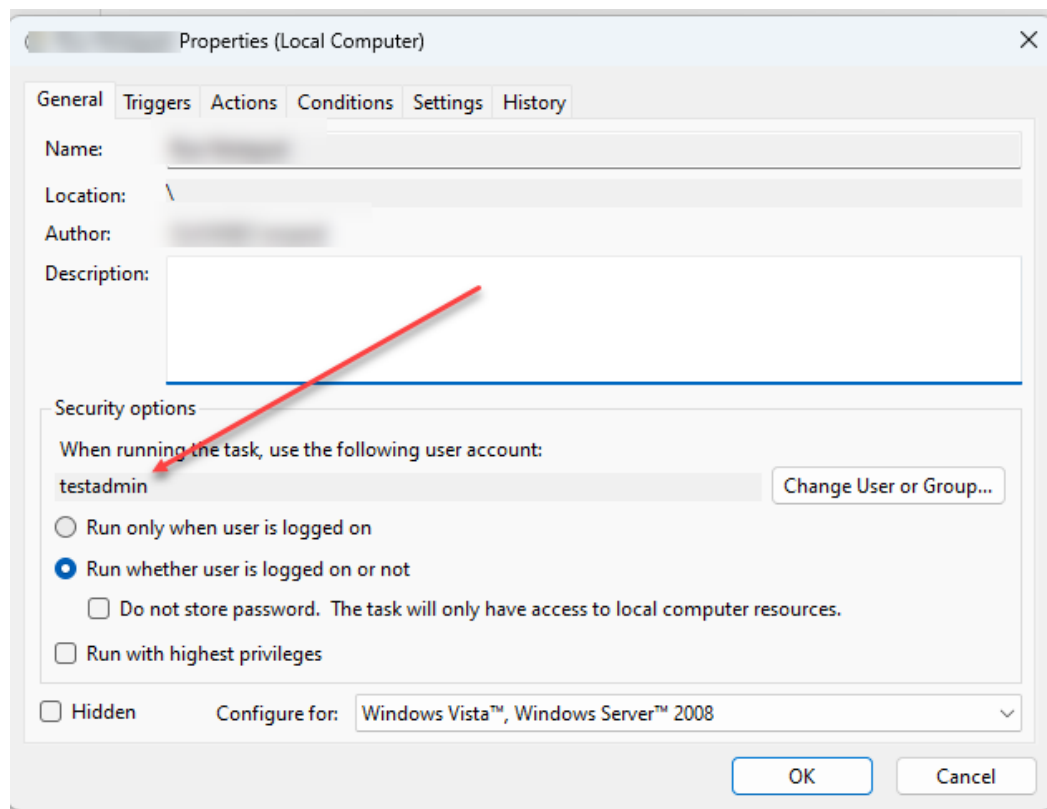
Account to Discovery Hosts in AD

Save Cancel

Microsoft Windows also has a bug for Scheduled Tasks, where it can strip the Host Name, or Domain Name prefix for the account being used on the scheduled task, if you manually make any changes to the task – see screenshot below.

To overcome this bug, the following logic is used during discovery – by reading the appropriate XML file in the folder C:\Windows\System32\Tasks:

1. Check if the account is a local Windows account on the Host
2. If no local Windows Account is found, then it is assumed the account is an Active Directory account. On occasion, the “UserId” element in the XML file can also appear as the account SID, in which case we look up the account details in the registry. As the domain NetBIOS has been stripped from the account details, we will use the domain value that is selected on the Discovery Job itself.





## 19.7 Database Account Discovery

Passwordstate can also discovery accounts in various different types of databases. The options for these discovery jobs are exactly the same as the Local Admin Account discovery jobs, but in order to scan databases on your servers, the Host you have stored in Passwordstate needs to have the database information set.

Below is an example of a server that is hosting a Microsoft SQL Server instance, and you'll notice the Database Type, Instance and Port number are set.

The screenshot displays the Passwordstate V8.9 (Build 8993) interface. On the left, a navigation pane shows a list of hosts, with 'webserver01.halox.net' selected. The main area is titled 'Host Dashboard' and contains an 'Edit Host' form. The form is divided into two tabs: 'host details' and 'notes'. The 'host details' tab is active, showing a 'General Host Properties' section. This section includes fields for Host Name, Title, Tag, Site Location, Host Type, Operating System, Internal IP, External IP, MAC Address, Session Recording, Virtual Machine, Virtual Machine type, Database Server Type, Database Instance, Database Port Number, and Host Heartbeat. Red arrows point to the 'Database Server Type' (SQL Server), 'Database Instance' (mssqlserver), 'Database Port Number' (1433), and 'Host Heartbeat' (22 Hour 10 Minute) fields. The 'Remote Connection Properties' section is also visible at the bottom.

**Host Dashboard**

**Edit Host**

Please make changes below for the selected Host as appropriate, then click on the 'Save' button.

**host details** **notes**

Please specify details for the Host as appropriate.

**General Host Properties**

Host Name: \* webserver01.halox.net  
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Title:   
If the Title field has a value, this will be displayed in the Hosts Navigation Tree instead.

Tag: CN=Computers,DC=halox,DC=net  
Can be any descriptive Tag you want, which is also included in Host search results.

Site Location: Internal

Host Type: \* Windows

Operating System: \* Windows Server 2019

Internal IP:   
External IP:   
MAC Address:

Session Recording: \* ☐ Yes ☒ No (record all remote sessions for this Host)

Virtual Machine: \* ☒ Yes ☐ No

Virtual Machine type:   
☐ Amazon ☐ Azure ☒ HyperV ☐ Google Cloud ☐ VirtualBox ☐ VMware ☐ Xen

Database Server Type: SQL Server

Database Instance: mssqlserver  
This is for an SQL Server Instance, Oracle Service Name, or PostgreSQL database name - if required.

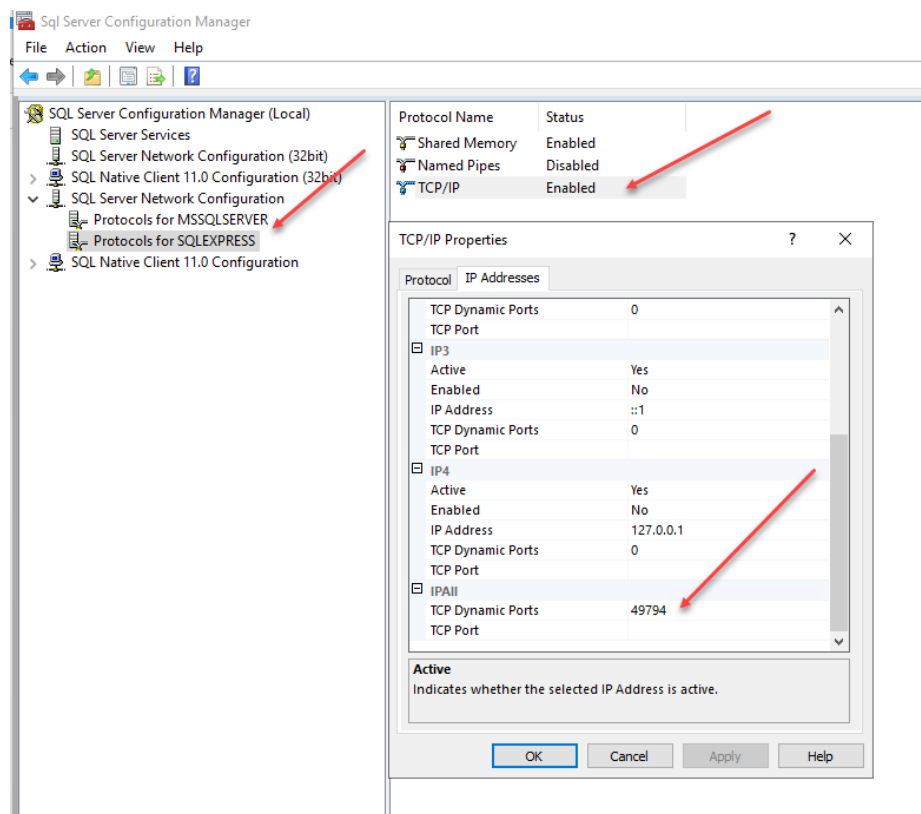
Database Port Number: 1433  
If using default ports, blank values will generally work here.

Host Heartbeat: 22 Hour 10 Minute (time each day a Heartbeat is executed)

**Remote Connection Properties**

By specifying appropriate settings below, this will allow a remote connection to the host directly from within Passwordstate.

Please Note: **MS SQL Server Discovery** jobs can work when there are multiple instances of SQL Server installed on the same Host. Within Passwordstate, you need to specify the correct instance names, and ports being used. If dynamic ports are being used, you need to look up the port number using the SQL Server Configuration Management tool, as per the screenshot below.



## 20 Office 365 and Microsoft Entra ID Accounts

### 20.1 Powershell Module Requirements

In order to perform Password Resets and Account Heartbeat validations, you must first install the **Azure Az PowerShell** module on your Passwordstate Web Server. To do this, open PowerShell as an **'Administrator'** and type in the following command:

```
Install-Module -Name Az -AllowClobber -Scope AllUsers
```

Accept the two prompts to install the module, and wait for it to complete – it can take several minutes to complete. Best practice is to reboot your server after making this change.

If you have the old legacy Powershell module installed (**AzureRM**), this is being deprecated in February 2024 by Microsoft. You will need to uninstall this module after the Azure Az module is installed, as per this Microsoft article: <https://learn.microsoft.com/en-us/powershell/azure/uninstall-az-ps?view=azps-10.4.1#uninstall-the-azurerm-module>

To achieve this, run this command in an elevated command prompt:

```
Uninstall-AzureRm
```

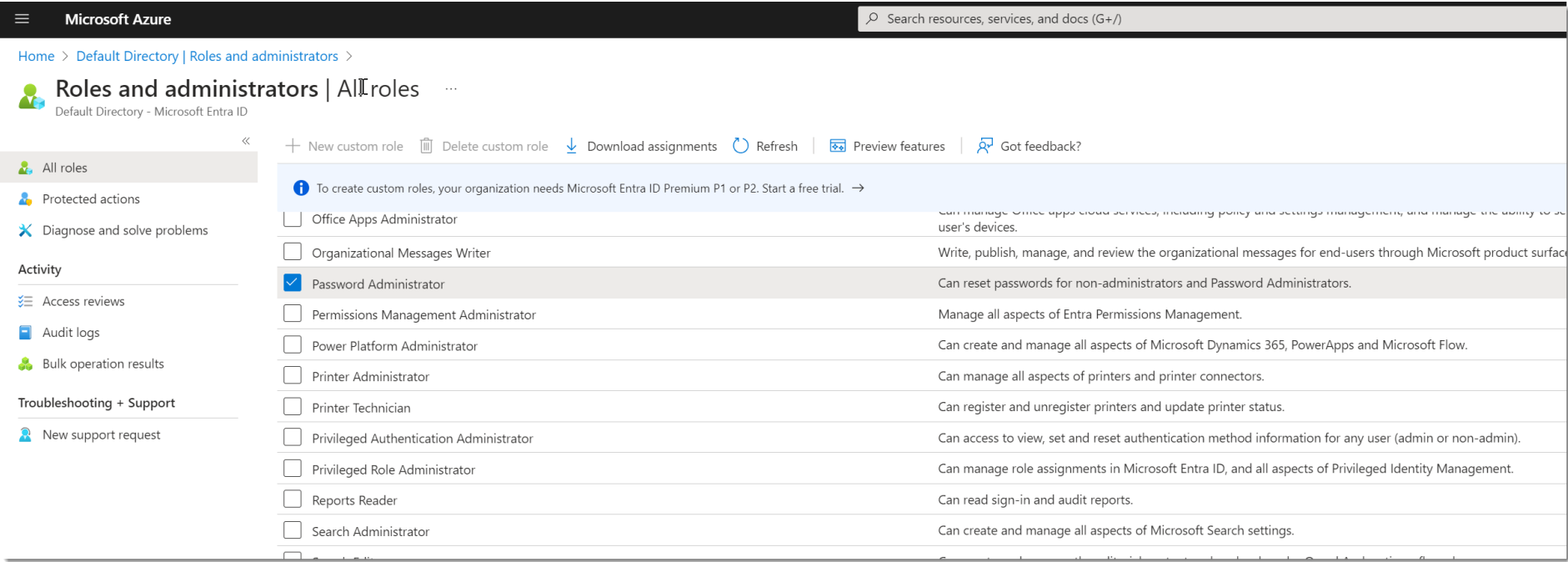
Your Passwordstate web server must have Internet access to reach out to your Azure tenant when installing and using this PowerShell module.

### 20.2 Microsoft Entra ID Permissions

A standard user in Microsoft Entra ID cannot reset their own password when using the Powershell module. You can either grant the user access to reset their own password, or you can use a privileged account in Entra ID to reset passwords on behalf of users.

The **Password Administrator** role in Microsoft Entra ID will allow a user to reset their own password, or will give your privileged account enough permissions to reset another user's password. Screenshot of this role can be found below.

Please refer to Microsoft documentation for detailed and current information about password reset permissions required in **Microsoft Entra ID**.



20.3 Office 365 and Entra ID Heartbeats

When performing a heartbeat on an Office365 or Entra ID account to check if it is valid, to check if it is valid, it will attempt to login into the tenant as part of the Powershell script that gets executed. If the account has **Multi factor Authentication** (MFA) applied to their account, then there is no way to automate this process.

Auditing in Passwordstate will alert you if a heartbeat has failed due to MFA limitations, and you should disable the heartbeat option on your password records for these accounts, to prevent reoccurring failed heartbeat attempts.

## 21 Installing Oracle Data Access Components (ODAC)

If you wish to perform password resets for **Oracle** database user accounts, you need to install the Oracle Data Access Components on the Passwordstate web server, and modify the path to these components in the two Passwordstate PowerShell scripts. To do this, please follow these instructions:

- Download **ODP.NET\_Managed\_ODAC122cR1.zip** from <http://www.oracle.com/technetwork/database/windows/downloads/index-090165.html>
- Unzip the contents to a directory of your choice on the Passwordstate Web Server (not within the Passwordstate folder though)
- Open a command prompt as an Administrator and change to the x64 directory inside where you extracted the Oracle zip file, i.e. **cd c:\oracleodp\odp.net\managed\x64**
- Now type **configure.bat** and press the enter key. The screen will output a series of commands and then advise “**The operation completed successfully.**”
- If the path you’ve installed the data access components to is different to **c:\oracleodp**, then you will need to go to the screen **Administration -> System Settings -> Password Reset Options** tab, and update the path on that screen
- Now restart the Passwordstate Windows Service

## 22 VMWare ESXi Accounts - PowerCLI Powershell module

By default, Passwordstate will use a standard script which uses SSH to connect to VMWare servers, to reset passwords on local accounts, perform account heartbeats or discover accounts on the servers.

This Powershell module written by VMWare will connect to your servers over HTTPS on port 443, and can also perform all Resets, Heartbeats and Account Discoveries.

To use the PowerCLI Powershell module, you must install this on your Passwordstate web server, or anywhere you may have the Remote Site Locations agent installed. This can be installed by opening Powershell as an Administrator, and running the command below, and more information about this can be found here: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-F02D0C2D-B226-4908-9E5C-2E783D41FE2D.html>

### Install-Module VMware.PowerCLI -Force

This Powershell module also has a built-in feature which can upload statistics and usage of the **PowerCLI** module. This can upload anonymous statistics about your usage, but best practice is to turn this feature off, by running the following command on your Passwordstate webserver in Powershell:

**Set-PowerCLIConfiguration -Scope AllUsers -InvalidCertificateAction Ignore -ParticipateInCEIP \$false -Confirm:\$false**



**Warning:** This VMware module uses a parameter called **Set-VMHostAccount** which does not currently accept SecureString values to be passed to it. If you have detailed Powershell logging enabled at the operating system level, this command will log passwords for resets in clear text in the Powershell Event Logs. We'd recommend turning off Powershell logging on your webserver if using this module, otherwise use the existing Linux/SSH scripts instead. Heartbeats and Discoveries are not affected by this.

## 23 Remote Site Locations Agent

If you have environments located behind firewalled environments, or look after client's networks with only Internet access to them, then you are able to deploy a Remote Site Agent to each network – please note additional license subscription is required for this.

With this Remote Site Agent, it has the same system requirements for account discovery, password reset, and account heartbeats as your internal network does.

This agent will communicate securely over HTTPS back to your Passwordstate API through a single port. Not only is the traffic passed in encrypted format within the HTTPS tunnel, but each Site Location also has its own In-Transit Encryption Key with further encrypts all traffic within the HTTP Body using 256bit AES Encryption.

-  Note 1: The server where you deploy the agent also requires PowerShell 5.0 or above, and the Agent is installed as a Windows Service. A Microsoft SQL Server is not required, as it uses a local SQLite database to store various data.
-  Note 2: If you'd like more information about how this Remote Site Agent works, please contact Click Studios support.

## 24 Password Record Examples

In **Section 16** of this document, we've given an example of how to set up an Active Directory account for automatic password resets, and heartbeats. The same settings and principles apply when adding in other types of accounts, like Windows or Linux accounts. For example, you choose an **Account Type**, set the **Username** and **Password**, and possibly assign a **Privileged Account**.

There are some other Account Types which require some additional information, and this is explained below:

### 24.1 Office 365/Azure AD Accounts:

When setting up an Office 365 or Azure AD account, you do not set a Domain, rather you enter the username in as [username@office365domain.com](#) format:

**Edit Password**

Please edit the password below, stored within the 'Office 365 Accounts' Password List (Tree Path = \IT Department\Windows Team).

password details | notes | security | reset options | heartbeat options | website fields | un >

Title \* Adam Wilson Office 365 Account

Managed Account ☒ Enabled for Resets ☒ Enabled for Heartbeat

Account Type Office 365

Domain or Host

Username awils@clickstudios.onmicrosoft.com

Description

URL https://portal.azure.com/

Expiry Date

Password Generator Default Password Generator

Password \* .....

Confirm Password \* .....

Password Strength ★★★★★☆ Compliance Strength ★★★★★

Strength Status: 4 more characters

One-Time Password Authenticator

Issuer Please click the icon to the right to upload and scan your QR Code.

One Time Password

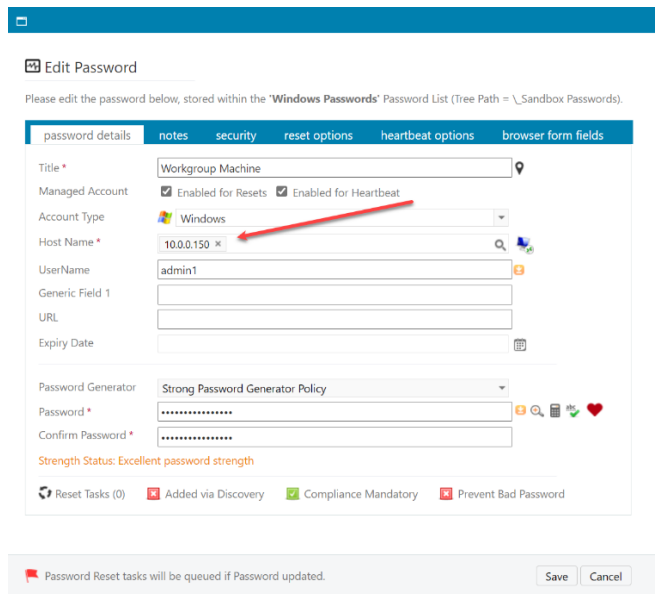
Reset Tasks (1) Added via Discovery Compliance Mandatory Prevent Bad Password

Password Reset tasks will be queued if Password updated. Save Cancel



## 24.2 Workgroup/Non-Domain Local Administrators

If you do not have functioning DNS for your WorkGroup computer, you should add the Host into Passwordstate using the IP Address. You then set the IP Address on the Password Record:



**Edit Password**

Please edit the password below, stored within the 'Windows Passwords' Password List (Tree Path = \\_Sandbox Passwords).

password details | notes | security | reset options | heartbeat options | browser form fields

Title \* Workgroup Machine

Managed Account ☒ Enabled for Resets ☒ Enabled for Heartbeat

Account Type Windows

Host Name \* 10.0.0.150

UserName admin1

Generic Field 1

URL

Expiry Date

Password Generator Strong Password Generator Policy

Password \* .....

Confirm Password \* .....

Strength Status: Excellent password strength

Reset Tasks (0) ☒ Added via Discovery ☒ Compliance Mandatory ☒ Prevent Bad Password

Password Reset tasks will be queued if Password updated.

Save Cancel


Other Prerequisites for WorkGroup machines to allow for password resets and heartbeats:

1. On your Passwordstate webserver, execute the following Powershell command to trust all hosts: **Set-Item WSMAN:\localhost\Client\TrustedHosts -value \*** (It's possible to specify your workgroup server instead of the wildcard \* if you prefer)
2. Ensure you have enabled Powershell Remoting on the Workgroup machine. To do this open Powershell "As Administrator" and execute **enable-psremoting -force**
3. On the same Workgroup machine, you must enable remote connections to the server for your Administrator account. To do this, open Powershell "As Administrator" and execute the command below, which adds a registry key to your system. This is a Microsoft requirement and you can read more about it in this link: [https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_remote\\_troubleshooting?view=powershell-5.1](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_troubleshooting?view=powershell-5.1)

**New-ItemProperty -Name LocalAccountTokenFilterPolicy -Path `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` -PropertyType DWord -Value 1**

### 24.3 Database Accounts (Microsoft SQL Server, Oracle, PostGre, MySQL, MariaDB)

For database accounts, the Host must be configured with the appropriate database type, instance and port number:

 Edit Host

Please make changes below for the selected Host as appropriate, then click on the 'Save' button.

host details notes

Please specify details for the Host as appropriate.

**General Host Properties**

Host Name: \*   
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Title:   
If the Title field has a value, this will be displayed in the Hosts Navigation Tree instead.

Tag:   
Can be any descriptive Tag you want, which is also included in Host search results.

Site Location:

Host Type: \*

Operating System: \*

Internal IP:

External IP:

MAC Address:

Session Recording: \* ☐ Yes ☒ No (record all remote sessions for this Host)

Virtual Machine: \* ☒ Yes ☐ No

Virtual Machine Type: ☐ Amazon ☐ Azure ☒ HyperV ☐ Google Cloud ☐ VirtualBox ☐ VMware ☐ Xen

Database Server Type:   
This is for an SQL Server Instance, Oracle Service Name, or PostgreSQL database name - if required.

Database Instance:

Database Port Number:   
If using default ports, blank values will generally work here.

## 24.4 IBM IMM Accounts

IBM IMM accounts require you to also set the **LoginID** of the account, and this means you will have to enable **Generic Field 1** on your Password List as a “Text Field”, and name it as **LoginID**:

**Edit Password List Properties**

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

password list details | customize fields | guide | api key & settings

Below you can specify which fields are available, which ones are required fields, and select one or more Generic Fields and configure their options accordingly.

**Standard Fields**

Field Name	Required	Hide Column
<input type="checkbox"/> Title	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> User Name	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Description	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Account Type	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> URL	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password Strength	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Expiry Date	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Notes	<input type="checkbox"/>	<input type="checkbox"/>

**Generic Fields** (click on Field Names to rename)

Field Name	Required	Encrypt	Hide Column	Field Type
<input checked="" type="checkbox"/> LoginID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field
<input type="checkbox"/> Generic Field 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field
<input type="checkbox"/> Generic Field 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field

Now when adding in your account into a password record, you set the LoginID as follows, and this ID can be found in your IMM Console:

**Edit Password**

Please edit the password below, stored within the 'IBM IMM Accounts' Password List (Tree Path = \\_Sandbox Passwords).

password details | notes | security | reset options | heartbeat options

Title \* IMM\test

Managed Account ☒ Enabled for Resets ☒ Enabled for Heartbeat

Account Type IBM | IBM IMM

Host Name \* imm.halox.net

UserName test

Description

LoginID 4

Expiry Date

Password Generator Default Password Generator

## 24.5 SSH Accounts with Public/Private Key Authentication

If the Privileged Account you use to reset other SSH Accounts uses a Public/Private key to authenticate, you can set your **Private Key** and **Passphrase** on this screen – It will connect using the Passphrase instead of the standard password, and then perform the reset for the appropriate account.

The screenshot displays the Passwordstate Administration interface. The left sidebar contains a navigation menu with various system settings. The main content area is titled 'Edit Privileged Account Details' and includes a note about permissions. Below this, there are two tabs: 'privileged account credentials' and 'public key authentication'. The 'public key authentication' tab is active, showing fields for 'Key Type' (OpenSSH or Putty), 'PassPhrase', 'Confirm PassPhrase', and 'Private Key'. The 'Private Key' field contains the text 'Private Key has been previously saved...'. At the bottom right of the form are 'Save' and 'Cancel' buttons.

Passwordstate V8.9 (Build 8993)

PASSWORDS HOSTS ADMINISTRATION

- ✓ Passwordstate Administration
  - Account and Host Discovery
  - Active Directory Domains
  - Auditing
    - Auditing Graphs
  - Authorized Web Servers
  - Backups and Upgrades
  - Bad Passwords
  - Browser Extension Settings
  - Email Notification Groups
  - Email Templates
  - Emergency Access
  - Encryption Keys
  - Error Console
  - Export All Passwords
  - Feature Access
  - High Availability Nodes
  - Host Types & Operating Systems
  - Images and Account Types
  - License Information
  - Password Folders
  - Password Generator Policies
  - Password Lists
    - Password List Templates
    - Password Strength Policies
  - Privileged Account Credentials**
  - PowerShell Scripts

### Edit Privileged Account Details

Please update details as appropriate below for the Privileged Account Details.

**Note:** If no permissions are applied to this account, then it cannot be used to perform any Account Discovery or Password Resets.

**privileged account credentials** public key authentication

Please specify appropriate details below for Public Key Authentication if required.

Key Type: ☐ OpenSSH ☒ Putty

PassPhrase:

Confirm PassPhrase:

Private Key: Private Key has been previously saved...

Save Cancel

## 24.6 Cisco IOS Enable Account

If your Privileged Account needs the Enable password to perform the password reset, you can set this on this screen:

The screenshot shows the Passwordstate V8.9 (Build 8993) interface. The left sidebar contains a navigation menu with various options, including 'Privileged Account Credentials' which is highlighted. The main area displays the 'Edit Privileged Account Details' form. The form has two tabs: 'privileged account credentials' and 'public key authentication'. The 'privileged account credentials' tab is active. The form fields include: Description (Cisco Priv Account), UserName (Isand), Site Location (Internal), Account Type (Cisco IOS), Password (masked), Confirm Password (masked), Cisco Enable Password (masked), and Link To Password (Not Required). A red box highlights the 'Cisco IOS' account type, and a red arrow points to the 'Cisco Enable Password' field. Below the 'Link To Password' field, there is a note: 'If you link this Privileged Account to a password record which is enabled for Password Resets, then the Privileged Account Credential password will be updated once the password reset is complete. Note: Only passwords which have been enabled for Reset, plus match the UserName above, will be visible here.'

Save Cancel

## 24.7 Dell iDrac Accounts

**Dell iDrac 9** accounts that are running **Firmware 4.40** or higher require you to also set the **ID** of the account, and this means you will have to enable **Generic Field 1** on your Password List as a **“Text Field”**, and name it as **LoginID**:

⚙ Edit Password List Properties

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

password list details | customize fields | guide | api key & settings

Below you can specify which fields are available, which ones are required fields, and select one or more Generic Fields and configure their options accordingly.

**Standard Fields**

Field Name	Required	Hide Column
<input type="checkbox"/> Title	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> User Name	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Description	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Account Type	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> URL	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password Strength	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Expiry Date	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Notes	<input type="checkbox"/>	<input type="checkbox"/>

**Generic Fields** (click on Field Names to rename)

Field Name	Required	Encrypt	Hide Column	Field Type
<input checked="" type="checkbox"/> LoginID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field
<input type="checkbox"/> Generic Field 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field
<input type="checkbox"/> Generic Field 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field

Now when adding in your account into a password record, you set the **LoginID** as follows:

🏠 Add New Password

Add new password to 'Dell iDrac Accounts' Password List (Tree Path = \IT Department\Windows Team).

password details | notes | security | reset options | heartbeat options

Title \*

Managed Account ☒ Enabled for Resets ☒ Enabled for Heartbeat

Account Type

Host Name

UserName

Description

LoginID

Expiry Date

You can find the ID number of your iDrac Account in the Dell web console:

iDRAC9 | Enterprise

Dashboard

System

Storage

Configuration

Maintenance

iDRAC Settings

iDRAC Settings

Overview

Connectivity

Services

Users

Settings

Local Users

Details

Add

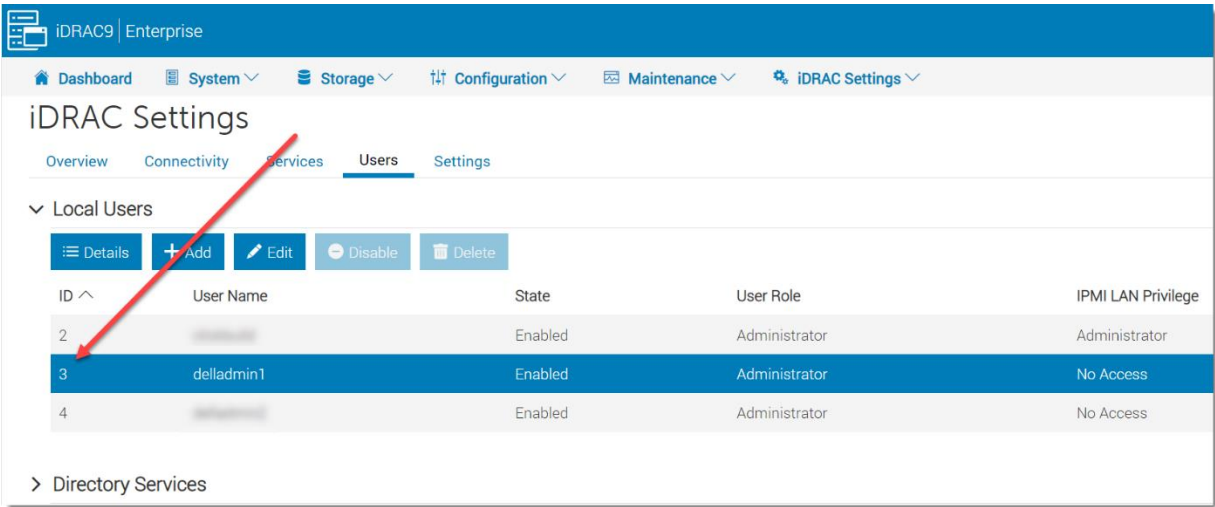
Edit

Disable

Delete

ID ^	User Name	State	User Role	IPMI LAN Privilege
2		Enabled	Administrator	Administrator
3	delladmin1	Enabled	Administrator	No Access
4		Enabled	Administrator	No Access

Directory Services



The screenshot shows the iDRAC9 Enterprise web console interface. The top navigation bar includes links for Dashboard, System, Storage, Configuration, Maintenance, and iDRAC Settings. The main content area is titled 'iDRAC Settings' and has tabs for Overview, Connectivity, Services, Users, and Settings. The 'Users' tab is selected, showing a section for 'Local Users'. Above the user list are buttons for Details, Add, Edit, Disable, and Delete. The user list is a table with columns: ID, User Name, State, User Role, and IPMI LAN Privilege. There are three users listed: ID 2 (User Name: [redacted], State: Enabled, User Role: Administrator, IPMI LAN Privilege: Administrator), ID 3 (User Name: delladmin1, State: Enabled, User Role: Administrator, IPMI LAN Privilege: No Access), and ID 4 (User Name: [redacted], State: Enabled, User Role: Administrator, IPMI LAN Privilege: No Access). A red arrow points to the ID number 3 of the 'delladmin1' user. Below the table is a link for 'Directory Services'.

ID	User Name	State	User Role	IPMI LAN Privilege
2	[redacted]	Enabled	Administrator	Administrator
3	delladmin1	Enabled	Administrator	No Access
4	[redacted]	Enabled	Administrator	No Access