Click Studios

Passwordstate

Password Discovery, Reset and Validation

Requirements

Table of Contents

1 Overview

In Passwordstate, through the use of PowerShell scripts, you're able to reset passwords for the following:

- Local accounts on Windows Servers/PCs
- Windows Services which are configured to use an account as its 'Log On As' identity
- Internet Information Services Application Pools which are configure to use an account as its 'Identity'
- Scheduled Tasks which are configured to run under the security context of user account
- Microsoft SQL Server accounts
- MySQL Server accounts
- Oracle accounts
- Linux/Unix accounts
- Cisco switch/router accounts
- Juniper Networking and Firewalls
- VMWare ESx Accounts
- COM+ Component Passwords
- Out-of-Band Management Cards – HP iLO, Dell iDrac & IBM IMM
- F5 BIG-IP Load Balancers
- You can also create your own scripts to perform any sort of processing when a Password is updated within Passwordstate

You are also able to perform certain 'validation' tasks to ensure the passwords in Passwordstate are accurate compared to what is being used on remote hosts, and your also able to 'discover' Local Administrator Accounts, and various other 'Windows Dependencies – such as Windows Services, IIS Application Pools and Scheduled Tasks.

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

Note: Passwordstate can also reset Active Directory accounts, but uses native .NET code for this instead of PowerShell scripts.

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. See Remote Site Locations documentation below for more information

2 Passwordstate Web Server System Requirements

To make use of the PowerShell Password Reset Scripts, the following is required on your Passwordstate Web Server:

- Microsoft Windows Server 2008 R2 & IIS 7.5
- Microsoft Windows Server 2012 & IIS 8.0
- Microsoft Windows Server 2012 R2 & IIS 8.5
- Microsoft Windows Server 2016 & IIS 10.0
- Windows 7 & IIS 7.5
- Windows 8 & IIS 8.0
- Windows 10 & IIS 10.0
- Microsoft .Net Framework 4.5
- PowerShell 4.0 or Higher
- Oracle Data Access Components (ODAC) if you want to reset Oracle Passwords
- Microsoft Visual C++ 2013 Runtime - https://www.microsoft.com/en-au/download/details.aspx?id=40784 (this will automatically be installed for you)

3 Hosts in Non-Trusted Domains

It is also possible to perform Password Reset and Validations 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. Typical ports which need to be opened are:
    a. PowerShell Remoting - TCP/5985 & TCP/5986
    b. SSH – TCP/22
    c. Telnet – TCP/23
    d. Microsoft SQL Server – TCP/1433
    e. MySQL Server – TCP/3306
- A Privileged Account Credential must be supplied on the screen Administration -> Passwordstate Administration -> Privileged Account Credentials, in FQDN format i.e. 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 Credentials
- And when added host records on the Hosts screen, it is recommended the Host names are specified using FQDN i.e. serverabc@mydomain.com

4 Installing Oracle Data Access Components (ODAC)

If you wish to perform password resets for Oracle 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_Managed121012.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 directory "c:\oracleodp\odp.net\managed\x64" – the path will be different for you depending on where you unzipped the file
- Now type "configure.bat" and press the enter key. The screen will output a series of commands and then read "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 here
- Now restart the Passwordstate Windows Service

5 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 heartbeat as your internal network does, but the agent can communicate securely over HTTPS back to your Passwordstate API on 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 2: Where you deploy the agent also requires PowerShell 4.0 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.

6 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.

Windows Server 2008, Server 2008 R2, Windows 7

Script	Requirements
Reset Local Windows Accounts	• PowerShell 2.0 or above • PowerShell Remoting enabled
Reset Window Services Accounts	• PowerShell 2.0 or above • PowerShell Remoting enabled
Reset Scheduled Task Accounts	• PowerShell 2.0 or above • PowerShell Remoting enabled
Reset IIS Application Pool Accounts	• PowerShell 2.0 or above • PowerShell Remoting enabled • Server 2008 (not R2) requires the II7 PowerShell Snap-In to be installed on the target host - http://www.iis.net/downloads/microsoft/powershell • Also requires the following PowerShell Cmdlet to be run in order for scripts to be run (default is Restricted on these operating systems): Set-ExecutionPolicy RemoteSigned
Reset COM+ Component Passwords	• PowerShell 2.0 or above • PowerShell Remoting enabled

Windows Server 2012, Server 2012 R2, Server 2016, Windows 8, Windows 10

Script	Requirements
Reset Local Windows Accounts	• PowerShell 3.0 or above, and PowerShell Remoting enabled (these are default settings)
Reset IIS Application Pool Accounts	• PowerShell 3.0 or above, and PowerShell Remoting enabled (these are default settings) • Also requires 'Set-ExecutionPolicy RemoteSigned' to be set
Reset Scheduled Task Accounts	• PowerShell 3.0 or above, and PowerShell Remoting enabled (these are default settings)
Reset Window Services Accounts	• PowerShell 3.0 or above, and PowerShell Remoting enabled (these are default settings)
Reset COM+ Component Passwords	• PowerShell 3.0 or above • PowerShell Remoting enabled

SQL Server, MySQL, Cisco Switches/Routers, Linux/Unix Hosts, HP iLO Cards and VMWare

Script	Requirements
Reset Microsoft SQL Server Accounts	• Firewall allows access on SQL Server port – default port is 1433 for SQL Standard and above, and SQL Express can use a Dynamic Port – generally 49260 • You must also have the TCP/IP Protocol enabled for SQL Server, and this can be done using the SQL Server Configuration Manager Utility, under the section SQL Server Network Configuration -> Protocols for <InstanceName>. Generally this is not enabled for SQL Server Express
Reset MySQL Server Accounts	• Firewall allows access on MySQL Server port – default port is 3306
Reset Cisco Switch/Router Accounts	• Remote connections using SSH
Reset Linux/Unix Accounts	• Remote connections using SSH • Microsoft Visual C++ 2013 Runtime - https://www.microsoft.com/en-au/download/details.aspx?id=40784
Reset HP iLO Card Accounts	• Remote connections using SSH
Reset VMWare ESX Accounts	• Remote connections using SSH

7 Password Validation Script Requirements

The following PowerShell Scripts are provided to validate the password stored within Passwordstate, matches what is in use on the Host:

- Validate Password for Active Directory Account
- Validate Password for Cisco Account
- Validate Password for Dell iDRAC Account
- Validate Password for F5 BIG-IP Account
- Validate Password for HP H3C Account
- Validate Password for HP iLO Account
- Validate Password for HP Procurve Account
- Validate Password for IBM IMM Account
- Validate Password for Juniper Junos Account
- Validate Password for Juniper ScreenOS Account
- Validate Password for Linux Account (also used for Macs and VMWare ESX)
- Validate Password for MySQL Account
- Validate Password for Oracle Account
- Validate Password for SQL Account
- Validate Password for Windows Account

- Each of the Validation Scripts above have the same System Requirements as the Password Reset Scripts.
- Note: Active Directory Accounts can also be validated within Passwordstate, either using the  icon when the Password Edit screen is open.

8 Password Discovery Script Requirements

As of Build 8000 of Passwordstate, the following PowerShell Scripts 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, ect:

- Get-CiscoAccounts.ps1
- Get-Dependencies.ps1
- Get-H3CAccounts.ps1
- Get-JunosAccounts.ps1
- Get-LinuxAccounts.ps1
- Get-LocalAdminAccounts.ps1
- Get-MSSQLAccounts.ps1
- Get-MySQLAccounts.ps1
- Get-OracleAccounts.ps1

These scripts are located in the folder /setup/scripts, and are imported and encrypted in the Passwordstate database.

The following two Discovery Scripts also require Windows Management Instrumentation (WMI) - TCP/135, to be enabled on the Host – this is WMI executing locally on the Host once PowerShell Remoted in, and not a remote WMI connection from the Passwordstate web server:

- Get-LocalAdminAccounts.ps1 (Discover Windows Local Admin Accounts)
- Get-Dependencies.ps1 (Discover Windows Account Dependencies)

Each of the Discovery Scripts above have the same System Requirements as their respective Password Reset Scripts

9 Possible Errors and Their Cause

With each of the default PowerShell Scripts provided, there are certain exceptions which are captured and reported in the event of a failure. The following table summarises possible failures and their relevant fixes.

Reset Local Windows Accounts

Error	Fix
It appears the Host is not online, or PowerShell Remoting is not enabled	This error effectively means PowerShell Remoting to the host is not possible, for any of the reasons given in the error message.
The Privileged Account password appears to be incorrect, or the account is currently locked	To update a local Windows account, the script must be passed the credentials of a 'Privileged Account' i.e. a domain account with permissions to logon to remote servers/PCs. This error indicates the username or password for the Privileged Account is incorrect, or the account is currently locked. Privileged Accounts can be found on the screen Administration -> Privileged Account Credentials
There are currently no logon servers available to service the logon request	There are no logon servers available (domain controller) to validate the use of the Privileged Account Credential being used to connect to the remote host
The referenced account is currently locked out and may not be logged on to	The account you are trying to reset the password for is currently locked and cannot be logged onto
UserName does not exist	The local account no longer exists

Reset Window Services Accounts

Error	Fix
The Privileged Account password appears to be incorrect, or the account is currently locked	To update a password for a Windows Service, the script must be passed the credentials of a 'Privileged Account' i.e. a domain account with permissions to logon to remote servers/PCs. This error indicates the username or password for the Privileged Account is incorrect, or the account is currently locked. Privileged Accounts can be found on the screen Administration -> Privileged Account Credentials
It appears the Host is not online, PowerShell Remoting is not enabled	This error effectively means either the Host Name is incorrect, or PowerShell Remoting is not enabled.
Please check the Windows Service Name is correct	It's possible the Windows Service name is incorrectly (the Display Name), or it doesn't exist anymore
Please ensure the username is valid and the Privileged Account Credentials being used has the required permissions	It's possible the Privileged Account Credentials doesn't have the required permissions to change service passwords, and/or Restart Windows Services
Please check the account credentials used for the Log On As identity are correct	The Windows Service could not be restarted as the account being used for the Log On As identity looks to be incorrect – the password may be wrong

Reset IIS Application Pool Accounts

Error	Fix
It appears the Host is not online, or PowerShell Remoting is not enabled	This error effectively means PowerShell Remoting to the host is not possible, for any of the reasons given in the error message.
The Privileged Account password appears to be incorrect, or the account is currently locked	To update a password for an IIS Application Pool, the script must be passed the credentials of a 'Privileged Account' i.e. a domain account with permissions to logon to remote servers/PCs. This error indicates the username or password for the Privileged Account is incorrect, or the account is currently locked. Privileged Accounts can be found on the screen Administration -> Privileged Account Credentials
Unable to restart Application Pool	It's possible the restarting of the Application Pool was delayed, of failed. You will need to manually check the reason why
Application Pool not found	It appears the Application Pool name is incorrect, or doesn't exist anymore
Please ensure the username is valid and the Privileged Account Credentials being used has the required permissions	It's possible the Privileged Account Credentials doesn't have the required permissions to change service passwords, and/or Restart Windows Services
It appears execution of PowerShell scripts has not been enabled on this Host. Please run the PowerShell command Set-ExecutionPolicy RemoteSigned	This error relates to Server 2008 R2 when execution of scripts hasn't been enabled on the server

Reset Scheduled Task Accounts

Error	Fix
It appears the Host is not online, or PowerShell Remoting is not enabled	This error effectively means PowerShell Remoting to the host is not possible, for any of the reasons given in the error message.
The Privileged Account password appears to be incorrect, or the account is currently locked	To update a password for a Scheduled Task, the script must be passed the credentials of a 'Privileged Account' i.e. a domain account with permissions to logon to remote servers/PCs. This error indicates the username or password for the Privileged Account is incorrect, or the account is currently locked. Privileged Accounts can be found on the screen Administration -> Privileged Account Credentials

Reset Microsoft SQL Server Accounts

Error	Fix
Please check SQL details are correct, and that a firewall is not blocking access	Possibly the SQL Server details supplied are incorrect (server name, instance name or port number), or a firewall is blocking access – default port is 1433
Account does not exist or you do not have permission	The SQL Server account could not be found, or the Privileged Account Credentials supplied does not have the permissions to change passwords.
Please check the Privileged Account Credentials provided are correct	Possibly the Privileged Account Credentials supplied are incorrect

Reset MySQL Server Accounts

Error	Fix
Please check the Host is online, or if a Firewall is blocking access	Possibly the MySQL Server details supplied are incorrect (server name or port number), or a firewall is blocking access – default port is 3306
Please check the Privileged Account Credentials provided are correct	Possibly the Privileged Account Credentials supplied are incorrect

Reset Cisco Switch/Router, Linux/Unix, HP iLO Card, and VMWare ESX Accounts

Error	Fix
The enable password appears to be incorrect	Possibly the Privileged Account Credentials supplied for the 'enable' statement is incorrect
Please check the Host is online, and accessible on the network	Possibly the host is not currently accessible on the network – either turned off, network issue, or a firewall blocking SSH access
Please check the correct port is specified and username/password are correct	The SSH connection was denied as the UserName and Password supplied appear to be incorrect

10 Enabling PowerShell Remoting per Host

On Windows 7 and Server 2008, PowerShell Remoting is not 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

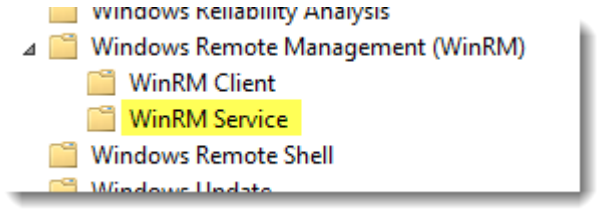
Running this command performs the following:

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

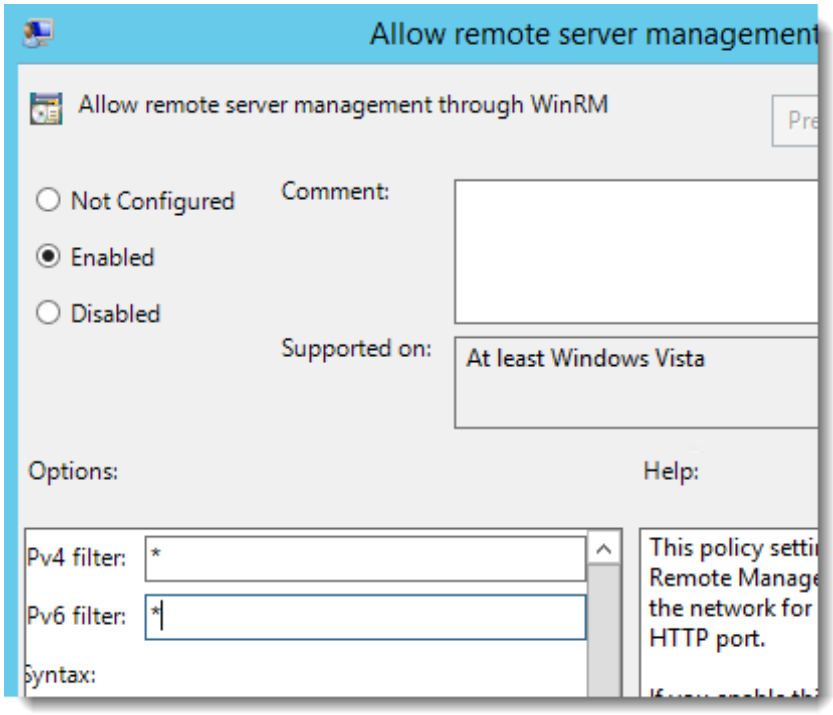
11 Enabling PowerShell Remoting via Group Policy

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 (this applies to a Windows Server 2012 R2 domain controller):

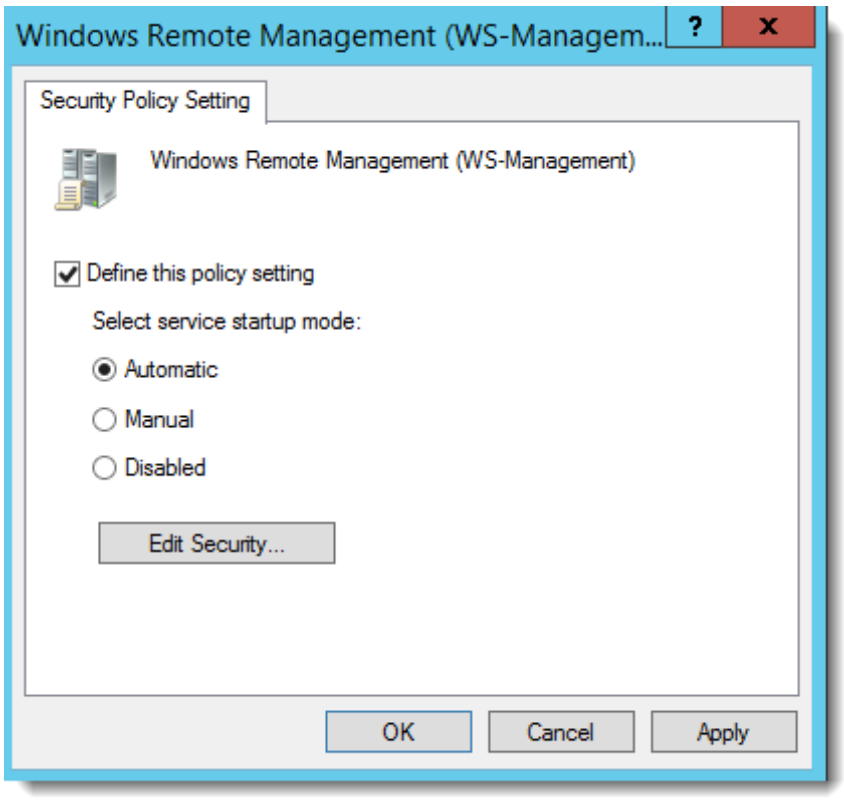
- Open the Group Policy Management Console
- Create or use an existing Group Policy Object, open it, and navigate to Computer Configuration -> Policies -> Administrative templates -> Windows Components
- Here you will find the available Group Policy settings for Windows PowerShell, WinRM and Windows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



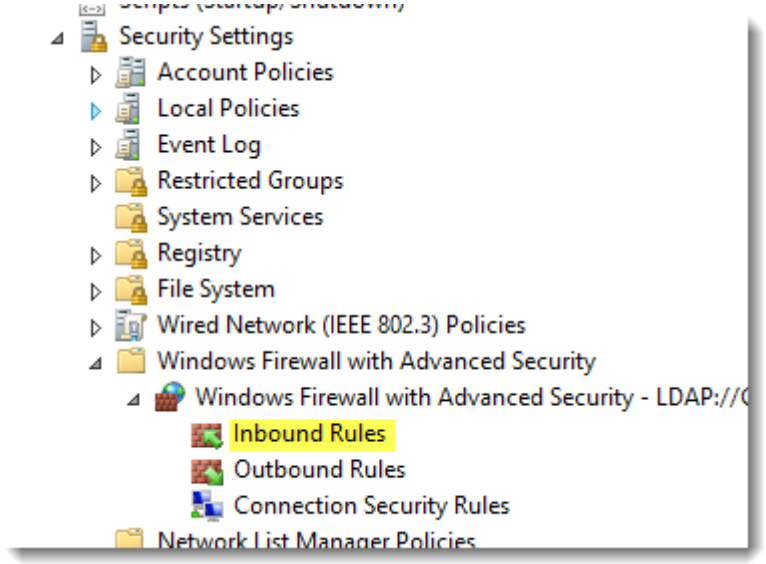
- Open “Allow remote server management through WinRM” setting
- Enable the Policy and set the IPv4 and IPv6 filter values to *



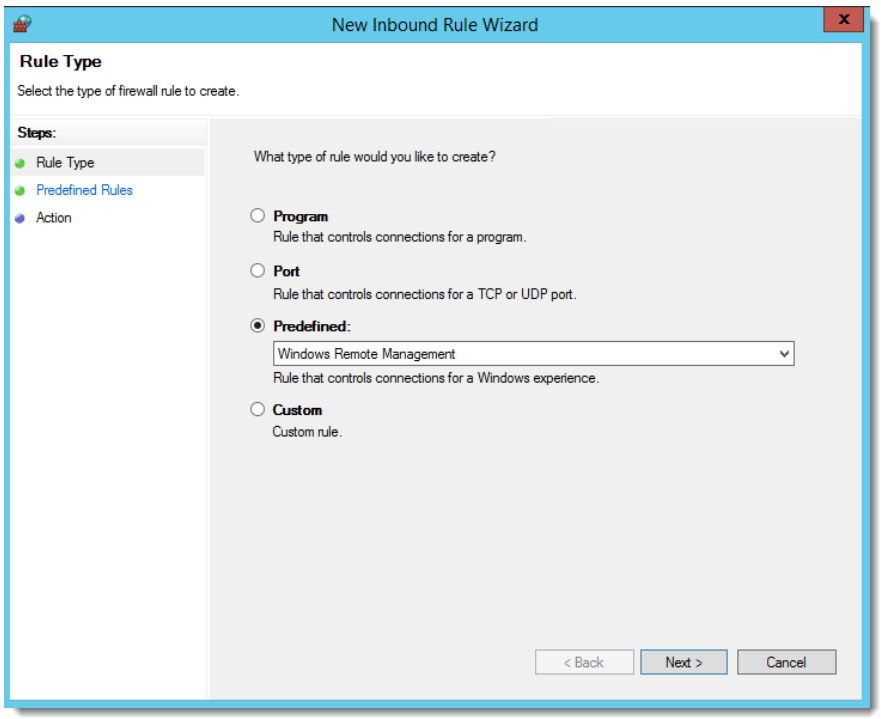
- Click OK
- Navigate to Windows Settings -> Security Settings -> System Services
- Select Windows Remote Management (WS-Management) Service and set the startup mode to Automatic



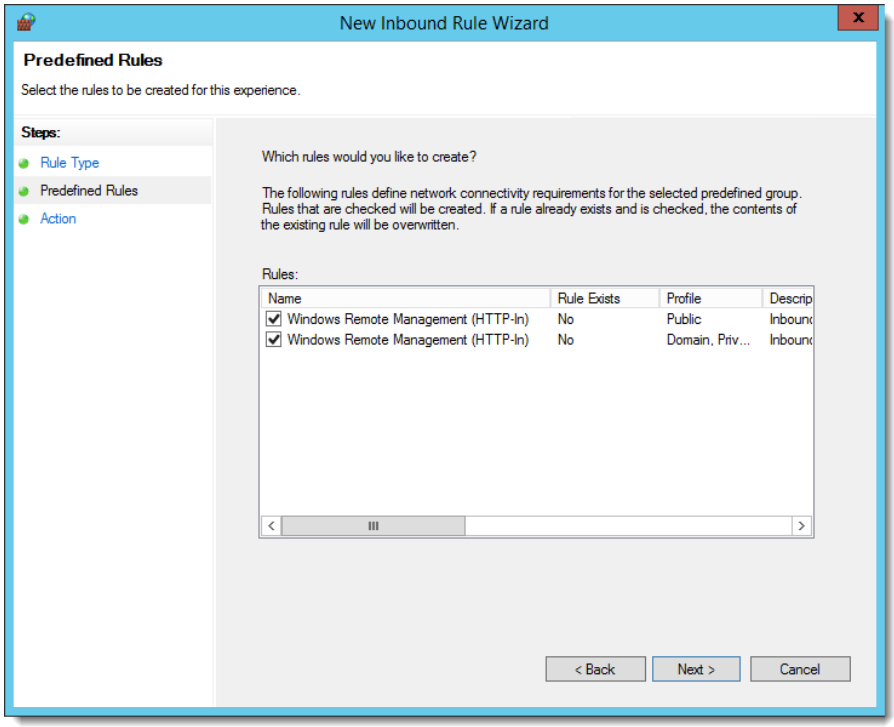
- Click OK
- You need to create a new Inbound Rule under Computer Configuration->Policies->Windows Settings->Windows Firewall with Advanced Security->Windows Firewall with Advanced Security->Inbound Rules:

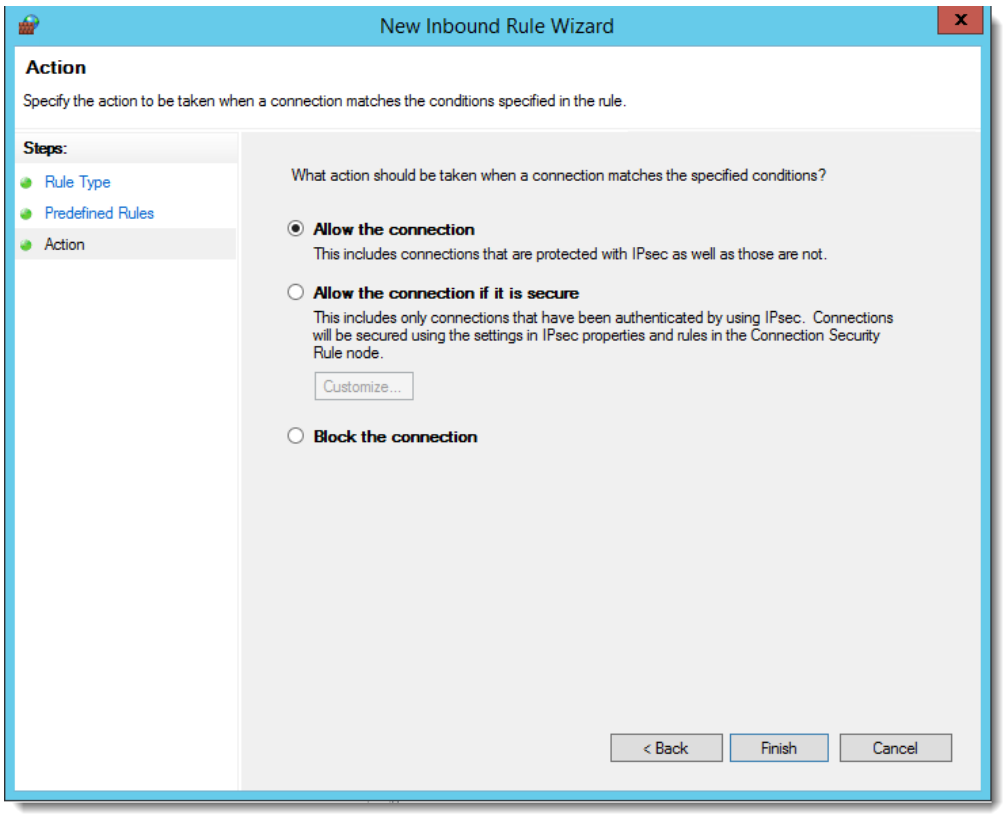


- The WinRM port numbers are predefined as “Windows Remote Management”:



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





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

12 Account Discovery and Password Resets between Non-Trusted Active Directory 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:

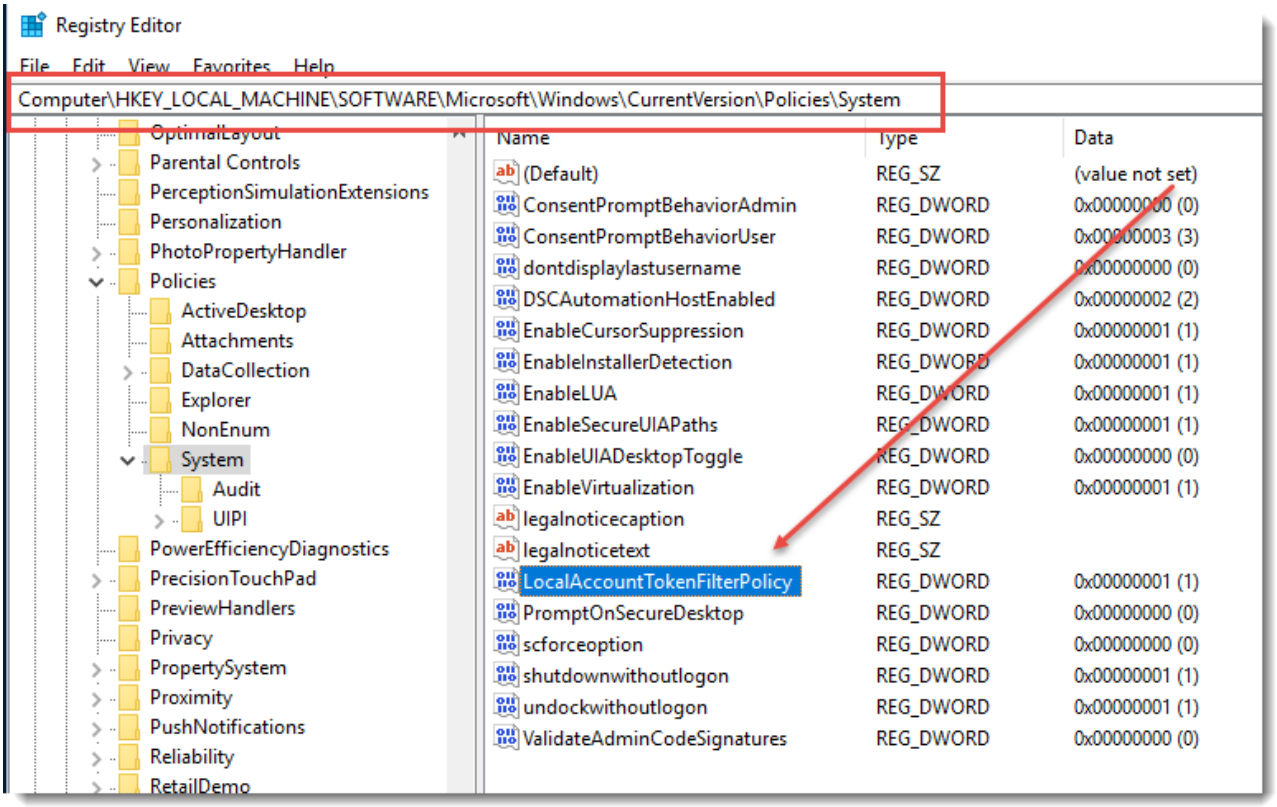
```
Set-Item WSMAN:\localhost\Client\TrustedHosts -value *
```

Please restart the Passwordstate Windows Service after making this change.

13 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



14 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.

In order for this functionality to work, changes are required to each of the Sudoers file on your Linux desktops/servers. Below are the changes required:

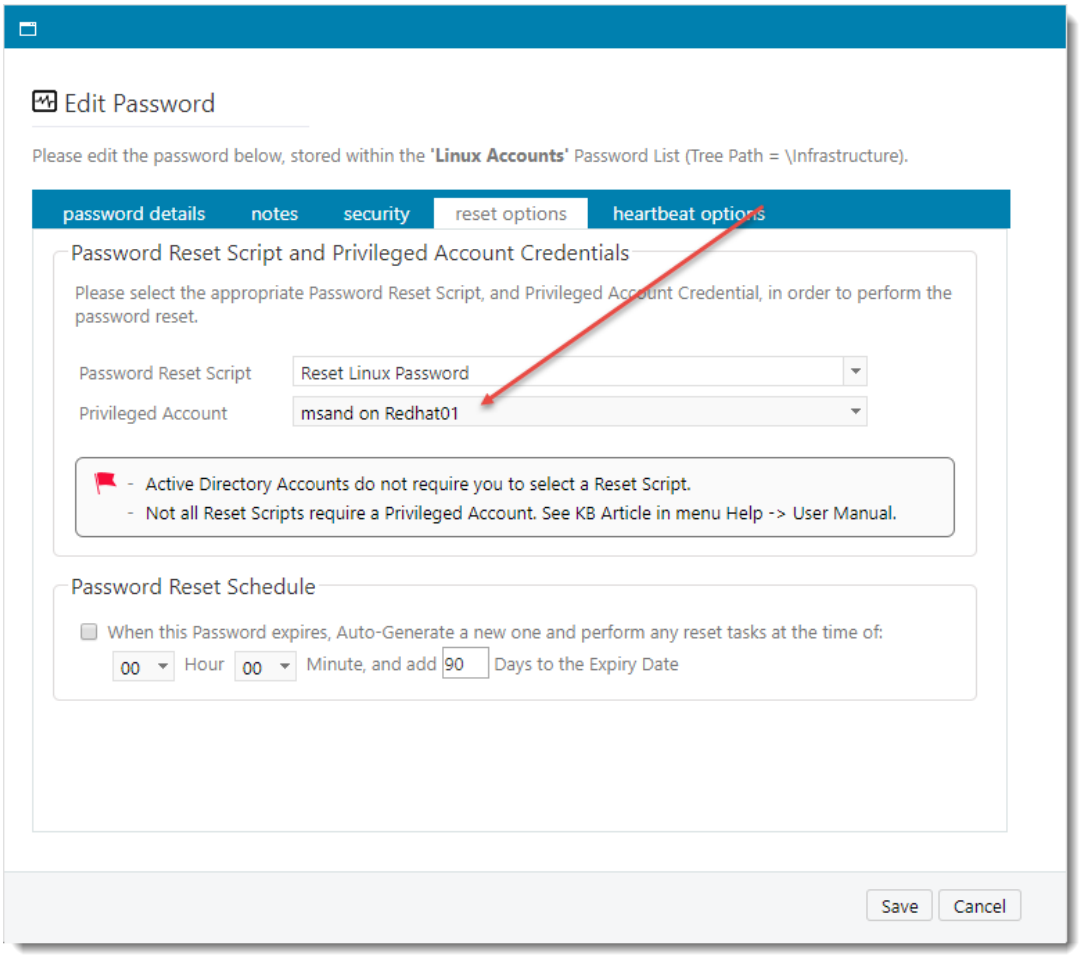
- Open the Sudoers file with visudo using the following command:

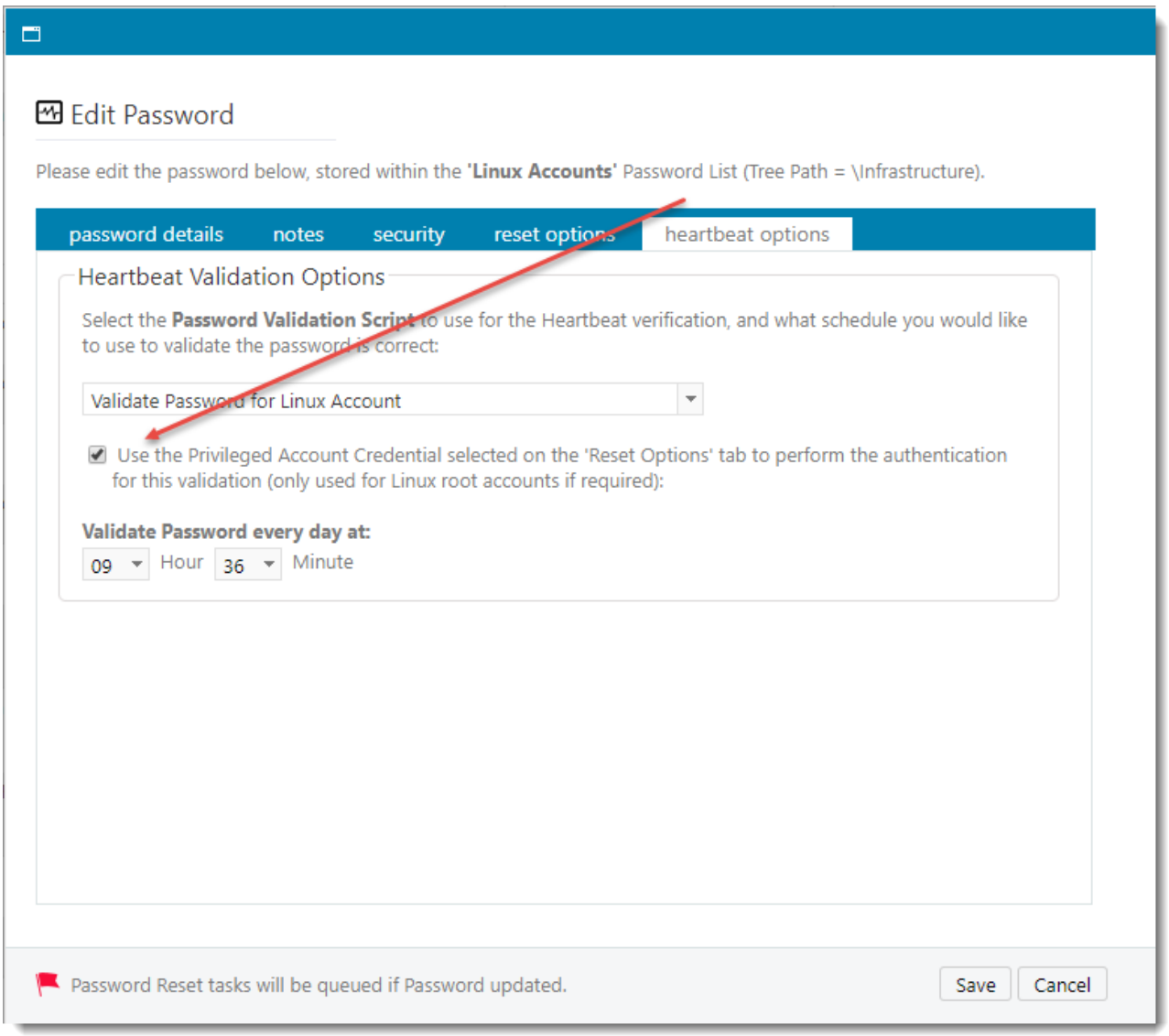
  Sudo visudo -f /etc/sudoers

- 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

Please note: If you make this change for the Privileged Account Credential, then only this account can only be used to reset the 'root' account, and no others on that Linux host. If you have other accounts on the Linux host which require password resets, you will need to use a separate Privileged Account Credential which is not configured as per the instructions above.





- Please note that for password resets to occur for 'root' accounts, the password value for the root account in Passwordstate must be correct before any 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:
    - 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.