SmartProfiler-SecID Assessment
Security & Health Monitoring

SmartProfiler Security Document for End Users/Organizations/Security Team

Version 1.1

DynamicPacks
TECHNOLOGIES

Update: 01 January 2025

Security Document for SmartProfiler Product

Product*: SmartProfiler SecID*

Guide Version: *1.1*

Table of Contents

1. About SmartProfiler

SmartProfiler for Active Directory and M365 is designed to mitigate security risks in the AD and Microsoft 365 environments by performing an advanced assessment and implementing the real-time monitoring to capture threats in real-time. Active Directory is a primary source for Authentication and Authorization for users and business applications. Microsoft doesn't provide out of the box tools that can be used to perform health & risk assessment of Active Directory environment. SmartProfiler AD-OnPrem Security Tool can be used to perform Active Directory assessment for multiple AD forests and provide an assessment report which includes issues and recommendations to fix the issues. Whereas SmartProfiler for AVD Assessment is designed to find bottlenecks/issues in the existing AVD environment and help in finding the missing settings recommended by Microsoft for improving the performance of the AVD environment. AVD Assessment can also check if the configuration is consistent across the host pools.

Business Outcome

Active Directory, Microsoft 365 and Azure Virtual Desktop will be protected, and a thorough assessment will ensure the Active Directory and Microsoft 365 are operating per CIS/NIST CSF 2.0 compliance standards. The AVD Assessment will ensure the AVD environment is operating as per best practices and recommendations by Microsoft.

Business Key Performance Indicators

The SmartProfiler for Active Directory, Microsoft 365, and AVD will perform an advanced assessment in your production environment and be able to uncover hidden issues in the environment. Once all the issues are uncovered the customer IT Team will work to resolve the issues identified to ensure smooth functioning of Active Directory, M365 and AVD components. The AD Real-Time Monitoring component of SmartProfiler will ensure that emerging threats are captured and notified as soon as possible.

Solution Capabilities, Features, Enablers, and NFRs

Below table highlights the capabilities of each SmartProfiler product:

Product	Capabilities
SmartProfiler for Active Directory	• Active Directory Advanced Assessment (300 Checks) • AD Permissions Analyzer • AD Issues Fixer • AD Real-Time Monitoring • GPO Settings Checker • CIS/NIST GPO Compliance Checker

	• Advanced and customized reporting • Domain Controllers security analyser • AD Smart Queries
SmartProfiler for Microsoft 365	• Supports CIS V3.0 Tests. • Additional Tests (139) • Compliance and Security Assessment
SmartProfiler for AVD	• Performance Improvement Assessment • Misconfiguration Assessment • Configuration Consistency Assessment across host pools.
SmartProfiler for Entra ID and Azure-Infra	• Improve Security Posture of Entra ID and Azure-Infra Environment • Misconfiguration Assessment • Supports CIS Tests

2. SmartProfiler Requirements

The following requirements need to be met in order to install and execute SmartProfiler products.

SmartProfiler for Active Directory

SmartProfiler for Active Directory requirements must be met as mentioned below:

- SmartProfiler computer should be joined to Active Directory domain.
- Microsoft Word and Excel need to be installed on SmartProfiler computer in order to generate reports.
- The communication ports have been opened between SmartProfiler computer and PDC Emulator of each Active Directory domain.
- PS Remoting needs to be enabled on all Domain Controllers in order to run the Active Directory tests that belong to Domain Controllers. PS Remoting will be required:
    - There are 60 Domain Controller tests that need to be executed to check security status of all domain controllers.
    - AD Discovery requires connectivity to PDC Emulator via PS Remoting.

SmartProfiler for Microsoft 365

SmartProfiler for Microsoft 365 requires Public Internet connection to connect to Microsoft 365 Tenants.

SmartProfiler for AVD Assessment

SmartProfiler for AVD requires Public Internet connection to connect to Microsoft Azure Tenants.

SmartProfiler for Entra ID and Azure-Infra Assessment

SmartProfiler for Entra ID and Azure Infra requires Public Internet connection to connect to Microsoft Azure Tenants

3. Infrastructure Size and Performance

The infrastructure will be sized to meet the following performance characteristics for SmartProfiler.

Hardware/Item	CPU	Memory	Storage
A Virtual Machine running SmartProfiler application/Console. **Note**: The Console can be installed on multiple computers connecting to Real-Time Agent. Both Real-Time Agent and SmartProfiler console can be installed on the same computer.	2 vCPUs	16 GB	10 GB
A Virtual Machine running SmartProfiler Real-Time Agent for processing Real-Time Alerts.	2 vCPUs	16 GB	10 GB

4. Disabling Antivirus or Excluding SmartProfiler Folders

SmartProfiler executes PowerShell based scripts to perform assessment of target. You are required to disable Antivirus completely or exclude C:\Users\Public\SmartProfiler folder from Antivirus so SmartProfiler processes can execute the assessment flawlessly.

5. PowerShell Modules Requirements

SmartProfiler makes use of Microsoft provided PowerShell Modules for running assessment. The SmartProfiler can install required PowerShell Modules automatically from within the console. However, to ensure the SmartProfiler can install PowerShell Modules automatically, it requires a working Internet Connection to PowerShell-Gallery.com web site.

SmartProfiler for Active Directory

If SmartProfiler is running on Windows Server Operating System, execute below PowerShell commands from an elevated PowerShell prompt:

- Add-WindowsFeature -Name RSAT-AD-PowerShell
- Add-WindowsFeature -Name GPMC
- Add-WindowsFeature -Name RSAT-DNS-Server
- Add-WindowsFeature -Name RSAT-ADDS-Tools

If SmartProfiler is running on Windows Client System, execute below PowerShell commands from an elevated PowerShell prompt:

- Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
- Add-WindowsCapability -Online -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0
- Add-WindowsCapability -Online -Name Rsat.Dns.Tools~~~~0.0.1.0

SmartProfiler for VMware

SmartProfiler requires following VMware PowerCLI Modules to be installed:

- **Install-Module -Name VMware.PowerCLI -RequiredVersion 13.1.0.21624340**Add-

  To install PowerCLI offline on a disconnected computer, please check Security Questions and Answers section.

SmartProfiler for DHCP Server

SmartProfiler requires following DHCP Modules to be installed:

- **Install-Module -Name DHCPServer**

SmartProfiler for Microsoft 365

Microsoft 365 CIS Assessment can be done from both Windows Server or Windows client. Please execute below PowerShell commands in order to install required PowerShell modules for assessment.

- Install-Module -Name MicrosoftTeams -Scope CurrentUser -Force -MinimumVersion '4.4.1' -AllowClobber
- Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser -Force -MinimumVersion '2.0.5' -AllowClobber
- Install-Module -Name MSOnline -force -AllowClobber
- #Install-Module -Name AzureAD -force -AllowClobber
- Install-Module –Name Microsoft.Online.SharePoint.PowerShell -RequiredVersion 16.0.24322.12000 -Force -AllowClobber
- Install-module -Name AzureADPreview -Force -AllowClobber
- Install-Module -Name Microsoft.Graph.Intune -Force -AllowClobber
- Install-Module -Name Microsoft.Graph -Scope CurrentUser -Force -MinimumVersion '1.9.6' -AllowClobber
- Install-Module -Name Microsoft.Graph.Identity.DirectoryManagement -Force -AllowClobber
- Install-Module -Name Microsoft.Graph.Identity.SignIns -Force -AllowClobber
- Install-Module -Name Microsoft.Graph.Users -Force -AllowClobber
- Install-Module -Name Microsoft.Graph.Applications -Force -AllowClobber
- Install-Module -Name PnP.PowerShell -Force -AllowClobber

SmartProfiler for AVD Assessment

SmartProfiler for AVD Assessment can install required PowerShell Modules automatically during the AVD Assessment execution. However, the following modules need to be installed on the SmartProfiler computer:

- Install-Module -Name AVD.DesktopVirtualization -Force -AllowClobber
- Install-Module -Name Az.Azure -Force -AllowClobber

SmartProfiler for Entra ID, Azure-Infra and CIS Assessment

SmartProfiler for Entra ID, Azure-Infra and CIS Assessment can install required PowerShell Modules automatically during the Assessment execution process. However, the following modules need to be installed on the SmartProfiler computer:

- Install-Module -Name MSOnline -force -AllowClobber
- Install-Module -Name AzureAD -force -AllowClobber
- Install-module -Name AzureADPreview -Force -AllowClobber
- Install-module -Name Az.PostgreSql -Force -AllowClobber
- Install-Module -Name Az.Accounts -RequiredVersion 2.19.0 -Force -AllowClobber
- Install-Module Az.Security -Force

Azure CLI 64-bit Latest Version from below URL:

- https://learn.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli

6. SmartProfiler Execution Permission

SmartProfiler is a Desktop Application designed to perform security, health and risk assessment of Microsoft 365, Active Directory and Azure Virtual Desktop tenants. When performing an assessment of technologies, the SmartProfiler requires necessary permissions to the Assessment target. Below table provides a guidance on what permissions to be made available when running assessment for each technology:

Technology/Target	Permissions Needed	Remark
Microsoft 365 Tenant	• Global Reader Account OR Global Admin Account • Global Reader and Global Admin Account to be a Non-MFA Account If Global Reader Account is used, then it should be part of following Microsoft 365 Roles: Global Reader Compliance Administrator Compliance Data Administrator SharePoint Administrator **Note**: Please check Security Questions and Answers as to understand when to use Global Reader and Global Admin account for assessment.	When executing SmartProfiler for Microsoft 365 you need to provide a Global Reader Account / Global Admin Account to connect to Microsoft 365 Tenant and collect required data for assessment. Non-MFA Global Reader / Global Admin Account is needed to run unattended assessment.
Microsoft 365 Tenant	Admin Consent for Microsoft.Graph module for below Read Permissions:	Note that Mobile Device Management Category includes 22 tests which require Admin Consent (read permission) by

	• DeviceManagementApps.Read.All •DeviceManagementConfiguration.Read.All •DeviceManagementServiceConfig.Read.All • Directory.Read.All "AuditLog.Read.All", "Reports.Read.All", "Policy.Read.All", "Directory.Read.All", "IdentityProvider.Read.All", "Organization.Read.All", "Securityevents.Read.All", "ThreatIndicators.Read.All", "SecurityActions.Read.All", "User.Read.All", "UserAuthenticationMethod.Read.All", "Mail.Read", "MailboxSettings.Read", "DeviceManagementManagedDevices.Read.All", "DeviceManagementApps.Read.All", "DeviceManagementServiceConfig.Read.All", "DeviceManagementConfiguration.Read.All", "SharePointTenantSettings.Read.All", "AccessReview.Read.All", "RoleManagement.Read.All"	using a Global Admin account before tests in Mobile Device Management category can show results. The Admin Consent is also required for Microsoft Graph module.
Active Directory Forest – AD Assessment	• Domain Admin Account if Active Directory Forest is running with a Single Domain. • Enterprise Admin Account if Active Directory Forest is running with multiple AD Domains in order to access all AD Domains.	All Domain Controllers in each domain must be reachable to perform a complete assessment. **Note**: The Active Directory Assessment can be executed using a Normal Domain User account. In that case the 56 Domain Controllers tests will not be executed.
Active Directory Forest – AD Assessment Scheduler	• Domain Admin Account if Active Directory Forest is running with a Single Domain. • Enterprise Admin Account if Active Directory Forest is running with multiple AD Domains in order to access all AD Domains.	The AD Assessment Scheduler Service requires a Service Account that is member of Domain Admins or Enterprise Admins. **Note**: The Active Directory Assessment Scheduler Service can be executed using a Normal Domain User account. In that case the 56 Domain Controllers tests will not be executed.
Active Directory Forest – Real-Time Monitoring	SmartProfiler Active Directory Real-Time Monitoring requires a normal Domain User	

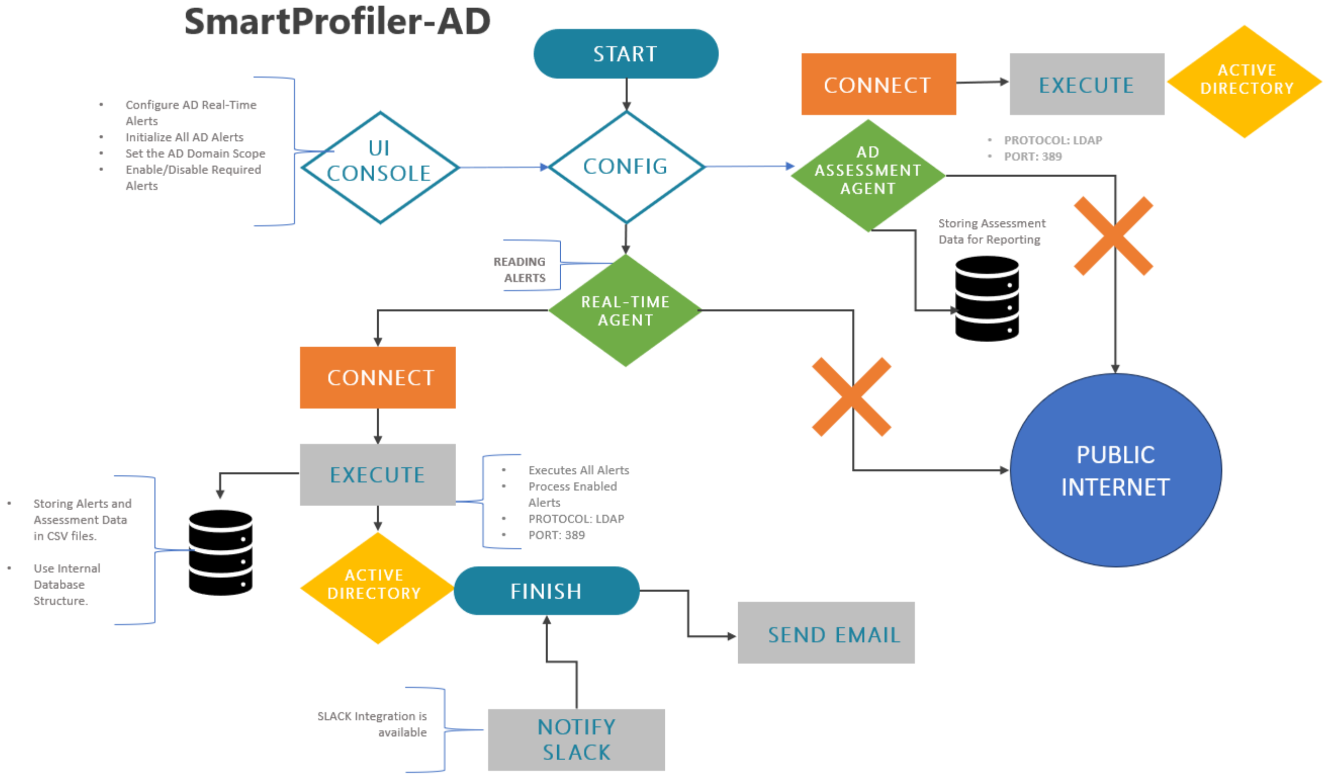
	account to execute and process all Active Directory Real-Time Alerts.	The Real-Time Service Account must be configured with Password Never Expires attribute.
Active Directory Forest – DC Health Checker and Notifier	SmartProfiler Active Directory DC Health Checker and Notifier requires a Domain Admin or Enterprise Admin Account.	The DC Health Checker Service Account must be configured with Password Never Expires attribute.
Azure Virtual Desktop Tenant	• Create Azure AD Application (SPN) in Azure Tenant. • SPN to have Owner Permission on Subscription where host pools are hosted. • Session Hosts have Azure Script Extension Enabled to execute scripts remotely.	SPN details are required before AVD Assessment can be performed: • Azure Subscription ID • Azure Tenant ID • SPN ID (Application ID) • SPN Secret • SPN Display Name
Azure Tenant **[For Entra ID, Azure-Infra and CIS Assessment]**	Create Azure AD Application (SPN) in Azure Tenant. SPN to have certain permissions as listed below: “AuditLog.Read.All", "Reports.Read.All", "Policy.Read.All", "Directory.Read.All", "IdentityProvider.Read.All", "Organization.Read.All", "Securityevents.Read.All", "ThreatIndicators.Read.All", "SecurityActions.Read.All", "User.Read.All", "UserAuthenticationMethod.Read.All", "Mail.Read", "MailboxSettings.Read", "DeviceManagementManagedDevices.Read.All", "DeviceManagementApps.Read.All", "UserAuthenticationMethod.ReadWrite.All", "DeviceManagementServiceConfig.Read.All", "DeviceManagementConfiguration.Read.All", "SharePointTenantSettings.Read.All", "AccessReview.Read.All", "RoleManagement.Read.All **Note**: The SPN to be set as an owner on the Subscription in order to run a complete assessment.	SPN details are required before Azure CIS Assessment can be performed: • Azure Subscription ID • Azure Tenant ID • SPN ID (Application ID) • SPN Secret • SPN Display Name

	Since SmartProfiler also supports Azure Infra and Entra ID, ensure to have permissions to read data from On-Prem Active Directory.	

7. SmartProfiler Communication Architecture

SmartProfiler Active Directory Communication Architecture

The below diagram shows how SmartProfiler Active Directory components connect with each other and communicate to Domain Controllers.



The SmartProfiler AD Real-Time Agent (installed as Windows Service) communicates to Domain Controller over default port and Protocol (LDAP:389). Even the Active Directory Assessment communicates over the same protocol. Real-Time and AD Assessment Agents do not connect to Public Internet for any communication. SmartProfiler uses Internal Database to store required data for real-time monitoring and assessment. The data type is volatile and keep changing based on the alert data fetched from Active Directory. No data is stored on Public Internet.

SmartProfiler Microsoft 365 Communication Architecture

The SmartProfiler for Microsoft 365 uses default ports (HTTPS) for communicating with Microsoft 365 Tenants. The SmartProfiler M365 Execution Console implements built-in agent that executes the tests using Microsoft Graph PowerShell Module. The following section in the document explains execution sequence for each technology including Microsoft 365.

SmartProfiler AVD Communication Architecture

The SmartProfiler for Microsoft AVD uses default ports (HTTPS) for communicating with Azure AVD Tenants. The SmartProfiler AVD Execution Console implements built-in agent that executes the tests using Microsoft Graph PowerShell Module. The following section in the document explains execution sequence for each technology including Azure AVD.

8. Network Communications

All communication to and from SmartProfiler Application - including the user interface and associated SmartProfiler Agent/Services are secured using the using the default LDAP/LDAPS traffic.

- There are no unsecured external HTTP or HTTPS calls within the SmartProfiler applications (particularly for Microsoft 365 Assessment).
- All communication with Azure and Microsoft 365 uses OAuth2 access tokens for Microsoft Graph, API operations and HTTPS for PowerShell operations.
- SmartProfiler Application Rewrite Services communicates with Azure and Microsoft 365 Tenants using TLS 1.2 encrypted data channels.
- Agents installed on the SmartProfiler computer communicate within an internal network and no data is sent out.
- For alerting purposes, SmartProfiler uses Email Notification to the email addresses configured in the email templates. The SmartProfiler will use default SMTP port or SMTP ports can be configured in the email templates.

9. SmartProfiler Execution Sequence

The below process shows how SmartProfiler collects data from target. A target can be a Microsoft 365 Tenant, Active Directory Forest, or an Azure Virtual Desktop Tenant. The execution

SmartProfiler utilizes the Power of Microsoft PowerShell Scripting language. The PowerShell modules, designed by Microsoft, are used to collect Microsoft 365 Tenant, Active Directory and Azure Virtual Desktop Tenants. SmartProfiler provides an execution framework. When you click on “Execute Assessment” button on SmartProfiler, the following events take place:

- **Connect to Target**: SmartProfiler connects to Microsoft 365 Tenant or Active Directory or Azure Virtual Desktop Tenant as follow:
  - ***For Microsoft 365***: If the target is an Microsoft 365 Tenant, then connection is made to all Microsoft 365 services which includes Exchange Online, MSOnline, SharePoint Online, Teams, and OneDrive. The connection is made using the Global Admin/Reader Account which was specified when registering the Microsoft 365 Tenant.

  Note: Please check Security Questions and Answers in this document to understand when to use Global Reader and Global Admin Account for assessment in this document.

  - **For Active Directory**: If the target is an Active Directory Forest, then connection is made to all Active Directory domains to ensure Domain Admin or Enterprise Account that was

provided during AD Forest License can connect to Active Directory domains for data collection.
    - **For Azure Virtual Desktop**: If the target is an Azure Virtual Desktop Tenant, then the connection is made using the SPN details provided.
- **Account Permissions Check:**
    - **For Microsoft 365**: Next, SmartProfiler checks to ensure Global Reader Account is part of all Microsoft 365 roles. In case SmartProfiler finds Global Reader is not part of one or more roles it notifies on the screen and asks you to correct the membership of Global Reader Account.
    - **For Active Directory**: Next, SmartProfiler checks to ensure Domain or Enterprise Account can connect to all Active Directory domains and a successfully Active Directory discovery can be performed. If the discovery is successful, SmartProfiler will show AD Sites, AD Domains and Domain Controllers discovered as part of the AD Discovery process.
    - **For Azure Virtual Desktop**: Next, SmartProfiler checks to ensure it can discover all Host Pools in the Azure Subscription. If during AVD Discovery if you do not see host pools and application groups, then make sure to check SPN has enough permission on the target Azure Subscription.
- **Execute PowerShell Modules**: Finally, SmartProfiler executes all PowerShell scripts and collects the required data and stores data in CSV files on the local machine.

At no point during Execution SmartProfiler makes any changes to the Target Environment. SmartProfiler is a pure READ-ONLY product.

Note: In case you need to see all the PowerShell scripts are executed as part of the execution, you can switch to “Manage Modules” tab in SmartProfiler to see the PowerShell code that executes.

10. SmartProfiler and Data Security

SmartProfiler doesn’t require a database before the assessment can be executed. All data collected during execution is stored in CSV files on the location machine where SmartProfiler is installed under **C:\Users\Public\SmartProfiler\SmartProfilerAssessment\Data** folder.

The CSV data is collected for each test, and it creates a file for each test. For example, when executing “Test Microsoft 365 Users Licenses”, it creates CSV file by name “Test-Office-365-Users-Licenses-<Tenant Name>_DATA.CSV” file to store data for the test.

The data stored in CSV files are required for following purposes:

- SmartProfiler needs to present an Assessment Summary in console using the CSV files for each test.
- When generating a Word Report, the data is collected from each CSV file and then a report is generated.
- Each CSV file contains affected objects. In case you need to see the affected objects list you can refer to the test’s CSV files.

Once the Assessment is completed you can safely delete the above folder and uninstall SmartProfiler from the machine. Please see the "**Security Questions and Answers**" section in this document before you decide to delete data.

Important: SmartProfiler will NOT delete data from above folder if the product is uninstalled. You are required to delete \Data folder manually if you wish to delete all data gathered by SmartProfiler.

11. Location of Customer Data

When a customer Installs and run the Assessment for Microsoft Active Directory, Microsoft 365, and Microsoft AVD, the data will be kept in the SmartProfiler computer. The SmartProfiler computer will have an internal database that will be used by the SmartProfiler Agents for processing. When an assessment report is generated, the process pulls the data located on the SmartProfiler computer.

12. Privacy and Protection of Customer Data

At no point during the assessment the tool will connect to Public Internet or any FTP endpoints. All data is secured at rest using AES 256-bit encryption. Service account passwords and password hashes (while already encrypted at-rest) are additionally encrypted with AES 256-bit encryption using Microsoft Encryption.

13. Data Impact and Modeling

The following table provides a list of frequently asked questions for Data Impact and Modeling.

Does this solution require the use of company data?	NO
Does this solution require the use of employee data?	NO
Does this solution move large amounts of data?	NO
Does this solution introduce a new data model?	NO

14. Service Level Agreement

Technical Issues related to SmartProfiler for AD and M365 will be supported by DynamicPacks Team during the business hours and all security incidents will be supported during business and non-business hours. Product Technical Issues, AD Real-Time related issues, support for customization, support for implementation and assessment of Active Directory and M365.

15. Business Continuity Plan

Application to SmartProfiler AD Real-Time Monitoring which will be installed on a single virtual machine running in production IT environment. There is no HA requirement for the application. Real-Time monitoring instances keep sending an email of availability of its components. If a component is not available or AD Real-Time Service stops an email will be sent to IT Team.

16. Security Risks & Mitigation

Risks

No risks as the product will be implemented to mitigate the risks. However, SmartProfiler for Active Directory, Microsoft 365 and Azure AVD Assessment stores or provide an option to execute the assessment under below conditions:

Product/Component	Credential Requirement	Can Use Locally Logged On or MS Prompt Login?	Require Storing Credentials?
SmartProfiler for AD Assessment	Domain Admin OR Enterprise Admin	Can use Locally Logged On Credentials	Optional
SmartProfiler AD Real-Time Service	Normal Domain User	Not Supported	Require storing Normal Domain User Account credentials in SmartProfiler Database.
SmartProfiler AD Assessment Scheduler	Domain Admin OR Enterprise Admin	Not Supported	Require storing Domain Admin or Enterprise Admin Credentials in SmartProfiler database.
SmartProfiler for M365 Assessment	Global Reader OR Global Admin Account	Can use Microsoft Login Prompt for Assessment	Optional but helps in unattended assessment.
SmartProfiler for M365 Assessment Scheduler	Global Reader OR Global Admin Account	Not Supported	Require storing SPN Details such as Certificate Thumbprint for Scheduler Service.
SmartProfiler for AVD Assessment	Azure SPN Details	Not Supported	Require storing Azure SPN Details for unattended assessment.
SmartProfiler for Entra ID, Azure-Infra and CIS Assessment	Azure SPN Details	Not Supported	Require storing Azure SPN Details for unattended assessment.
SmartProfiler Email Notification	Email Sender Password	Not Supported	Require storing Email Sender password in email templates.

Risks Mitigations

To mitigate the risks for credentials and to ensure no one can use the credentials used by the SmartProfiler, the credentials for Active Directory, Microsoft 365 Tenant (if stored) and Email Sender will be stored in an encrypted format. Solution will use two-layer-encryption mechanism in which, in turn, protects against compromises.

17. Solution Compliance with IT Policies

Policy	Compliance	Reason for non-compliance
Access Control Policy	Compliant	
Asset Management Policy	Not Applicable	
Availability Management Policy	Compliant	
Budget and Accounting for IT Services Policy	Not Applicable	
Compliance Policy	Not Applicable	
Contact with Authorities and Special Interest Groups	Not Applicable	
Data Protection Policy	Compliant	
Email Security Policy	Compliant	
End User Security Policy	Not Applicable	No end user data is touched.
HR Information Security Policy	Not Applicable	
Information Security Incident and Problem Management Policy	Not Applicable	
Information Security Management System Policy	Not Applicable	
Information Systems Acquisition, Development, and Maintenance Policy	Not Applicable	
ISMS Manual	Not Applicable	
IT Service Continuity Policy	Not Applicable	
Network Security Policy	Not Applicable	
Operations Management Policy	Not Applicable	
Physical and Environmental Security Policy	Not Applicable	
Risk Manual	Not Applicable	

18. Security Question and Answers

Q. Does SmartProfiler perform any write operations to Target?

A. No, SmartProfiler is a read-only product and at no point during assessment a write operation is performed to the target.

Q. Does SmartProfiler connects to Public Internet for sending any information to DynamicPacks?

A. SmartProfiler doesn't connect to DynamicPacks or any other Public Endpoints for storing data. Even the license file is provided offline for activation.

Q. Does SmartProfiler use PowerShell Designed by Microsoft?

A. SmartProfiler uses PowerShell Modules designed by Microsoft. All PowerShell Modules used by SmartProfiler are available on PowerShell Gallery which is managed by Microsoft.

Q. Can I see what all PowerShell Scripts are executed as part of SmartProfiler execution?

A. We provide "Manage Modules" tab as part of SmartProfiler that can be used to check PowerShell code for each test. However, "Manage Modules" tab is only available in Licensed Version.

Q. What data is stored in CSV files generated by SmartProfiler?

A. CSV files only contain "Affected objects" data. For example, in the case of Microsoft 365 if a test needs to check list of users or admins that do not have MFA enabled then CSV file will only contain those affected users/admins. Similarly, if AD Assessment for SmartProfiler finds orphaned domain controllers in Active Directory Forest then only orphaned domain controllers will be listed in CSV file.

Q. Can SmartProfiler for Microsoft 365 CIS Assessment execute under the Global Reader Account?

A. SmartProfiler for Microsoft 365 CIS Assessment can execute 90% tests using the Global Reader Account provided Global Reader Account is member of all required Microsoft 365 Roles. The SharePoint tests (12 of them) cannot be executed using the Global Reader Account. If you would like to execute SharePoint tests as part of the assessment, then we recommend using a Global Admin account. Global Reader Account cannot access SharePoint portal sites and settings as it a technical limitation imposed by Microsoft.

Q. My Customer/Organization security Team is not allowing the SmartProfiler for Microsoft 365 to run using a Global Admin Account? What can be done in this situation?

A. In these circumstances, we advise utilizing a Global Reader Account to run the assessment initially. This account will be able to run 90% of the tests automatically and will also produce a report. Please notify the Security Team that a Global Admin account is required in order to run SharePoint tests. If Security Team agrees to run the assessment using a Global Admin account, then select just "SharePoint Tests" in the execution console and then execute.

Q. Is SmartProfiler secure when connecting to Target using PowerShell modules?

A. Since PowerShell Modules used by SmartProfiler are designed by Microsoft and since all "Connect-xxxxx" commands perform a secure connection to Microsoft 365, Active Directory and Azure Virtual Desktop Tenants, the data collected from above targets is transferred securely to the SmartProfiler machine.

Q. Does SmartProfiler delete all data collected after preparing Assessment Report?

A. There is no provision in SmartProfiler to delete all data once the assessment report is prepared. It is because some environments might take longer time to complete assessment and in case you need to see the affected objects list you will not be able to see it if you have already deleted the data. You will be required to perform assessment again if you need to see the affected objects list.

Q. Does Active Directory Assessment require PS Remoting enabled on the Domain Controllers?

A. • PS Remoting needs to be enabled on all Domain Controllers in order to run the Active Directory tests that belong to Domain Controllers. There are 60 tests that need to be executed to check security status of all domain controllers. These tests are checked to ensure Domain Controllers do not have any risks.

Q. Does SmartProfiler Products interact with any other technologies in the production environment?

A. No. SmartProfiler only communicates with the required technology components as below:

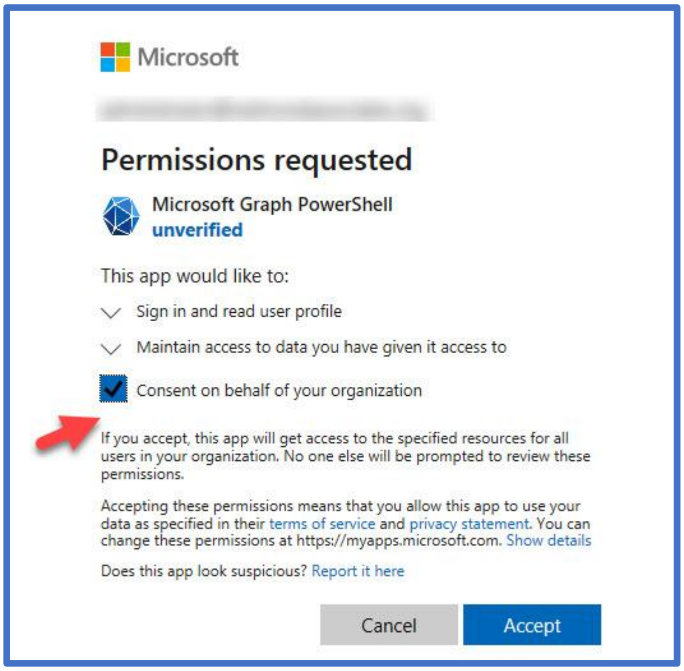
- For Active Directory: SmartProfiler connects to Domain Controllers over port 389 using LDAP protocol.
- For Microsoft 365: SmartProfiler connects to Microsoft 365 Tenants using HTTPS and Microsoft Graph PowerShell Modules.
- For AVD: SmartProfiler connects to Azure Tenants using HTTPS and uses Microsoft Azure AVD PowerShell Modules to perform assessment.

Q. Is there any command that we can use to grant Microsoft.Graph API Permissions to Microsoft 365 Tenant?

A. Grant Consent Option can be used to grant admin consent to Microsoft.Graph from within the SmartProfiler Assessment Execution Console. In case consent needs to be granted manually before executing the assessment, please use below PowerShell Command:

```
Connect-MgGraph -ContextScope Process -Scopes "AuditLog.Read.All", "Reports.Read.All",
"Policy.Read.All", "Directory.Read.All", "IdentityProvider.Read.All", "Organization.Read.All",
"Securityevents.Read.All", "ThreatIndicators.Read.All", "SecurityActions.Read.All", "User.Read.All",
"UserAuthenticationMethod.Read.All", "Mail.Read", "MailboxSettings.Read",
"DeviceManagementManagedDevices.Read.All", "DeviceManagementApps.Read.All",
"UserAuthenticationMethod.ReadWrite.All", "DeviceManagementServiceConfig.Read.All",
"DeviceManagementConfiguration.Read.All", "SharePointTenantSettings.Read.All",
"AccessReview.Read.All", "RoleManagement.Read.All"
```

In the next step the process will check if the Admin Consent has already been granted to Microsoft.Graph. If not granted, then you will be presented with a prompt as shown below:



Microsoft

[redacted]

Permissions requested

Microsoft Graph PowerShell
unverified

This app would like to:

- Sign in and read user profile
- Maintain access to data you have given it access to

☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

You need to check the box "**Consent on behalf of your organization**" and then click on "Accept" button to continue.

Q. Are there any Firewall Ports that we need to open in order to install and run SmartProfiler?

A. SmartProfiler for Active Directory, Microsoft 365 and AVD executes over specific ports. However, the SmartProfiler makes use of default communication ports and protocols for communicating with endpoints as explained in the table below. Please ensure to open these ports from the SmartProfiler computer to the target.

Product	Target	Port	Protocol
SmartProfiler for Active Directory	PDC Emulator of each AD Domain Active Directory Web Services	389 or SSL 9389	LDAP or LDAPS LDAP or LDAPS
SmartProfiler for M365	Microsoft 365 Tenant	443	HTTPS
SmartProfiler for AVD	Microsoft Azure Tenant	443	HTTPS

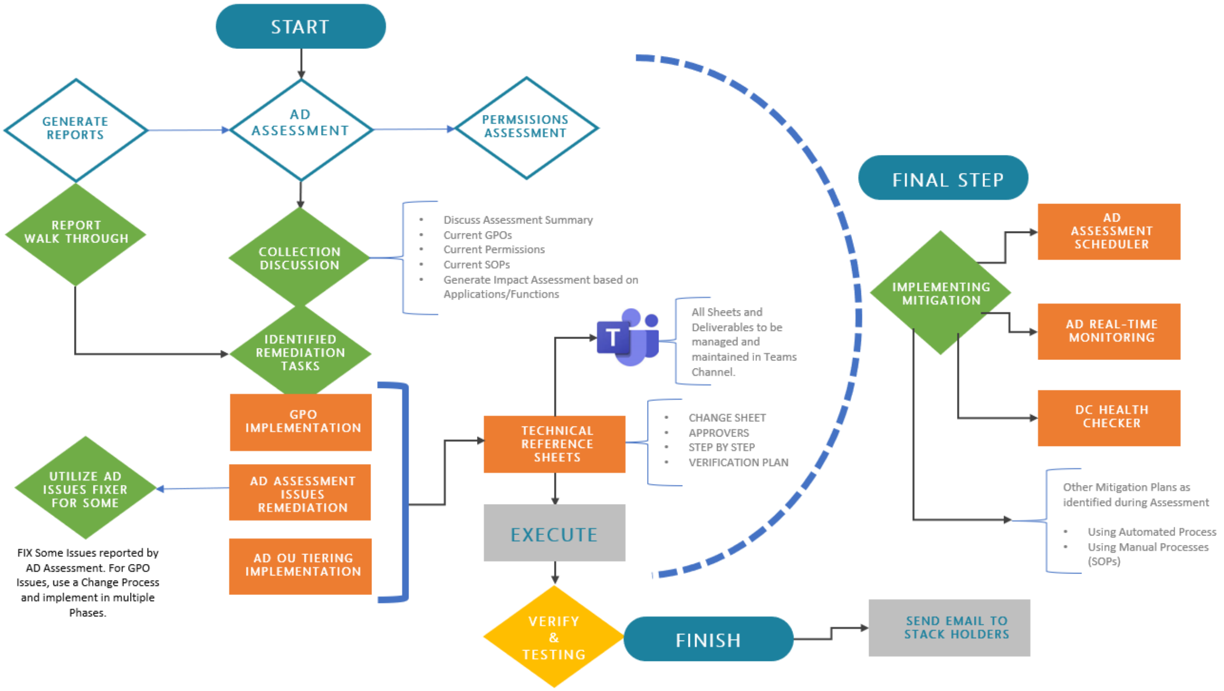
Q. Can anyone log on the SmartProfiler Application?

A. No. SmartProfiler requires a username and password to log on to the application. The Username and password are created when the first tenant or AD Forest is registered. A Tenant or AD Forest can only be registered by supplying correct credentials such as Domain Admin account for registering AD Forest and Global Reader/Admin account for registering Microsoft 365 or Azure Tenants.

Q. Does DynamicPacks help in remediating the issues reported by the SmartProfiler for Active Directory and what is the engagement process:

A. DynamicPacks Team can help in remediating AD Issues reported by the SmartProfiler for Active Directory. We, at DynamicPacks, have an expert AD Team who follows a steady approach for fixing the issues as shown in below diagram:

AD Assessment Engagement Process


START
GENERATE REPORTS
AD ASSESSMENT
PERMSISIONS ASSESSMENT
REPORT WALK THROUGH
COLLECTION DISCUSSION
Discuss Assessment Summary
Current GPOs
Current Permissions
Current SOPs
Generate Impact Assessment based on Applications/Functions
IDENTIFIED REMEDIATION TASKS
GPO IMPLEMENTATION
AD ASSESSMENT ISSUES REMEDIATION
AD OU TIERING IMPLEMENTATION
UTILIZE AD ISSUES FIXER FOR SOME
FIX Some Issues reported by AD Assessment. For GPO Issues, use a Change Process and implement in multiple Phases.
All Sheets and Deliverables to be managed and maintained in Teams Channel.
TECHNICAL REFERENCE SHEETS
CHANGE SHEET
APPROVERS
STEP BY STEP
VERIFICATION PLAN
EXECUTE
VERIFY & TESTING
FINISH
SEND EMAIL TO STACK HOLDERS
FINAL STEP
IMPLEMENTING MITIGATION
AD ASSESSMENT SCHEDULER
AD REAL-TIME MONITORING
DC HEALTH CHECKER
Other Mitigation Plans as identified during Assessment
Using Automated Process
Using Manual Processes (SOPs)

For any questions related to SmartProfiler security please contact us at Info@Microsoft-Assessment.com or Support@Microsoft-Assessment.com.

A. How can I install VMware PowerCLI modules manually on a disconnected computer:

Q. Follow the instructions explained below to install manually:

How to Install PowerCLI Offline

Not all servers can be connected to the internet due to security policies or other reasons. In this case, you can install VMware PowerCLI by using offline installation methods.

Installing PowerCLI offline by copying files

The first offline method to install PowerCLI involves using files downloaded from PS Gallery. The first steps are similar to the steps explained above when we need to find the module packages and install them in our Windows system.

1. Find the PowerCLI module in PowerShell Gallery:

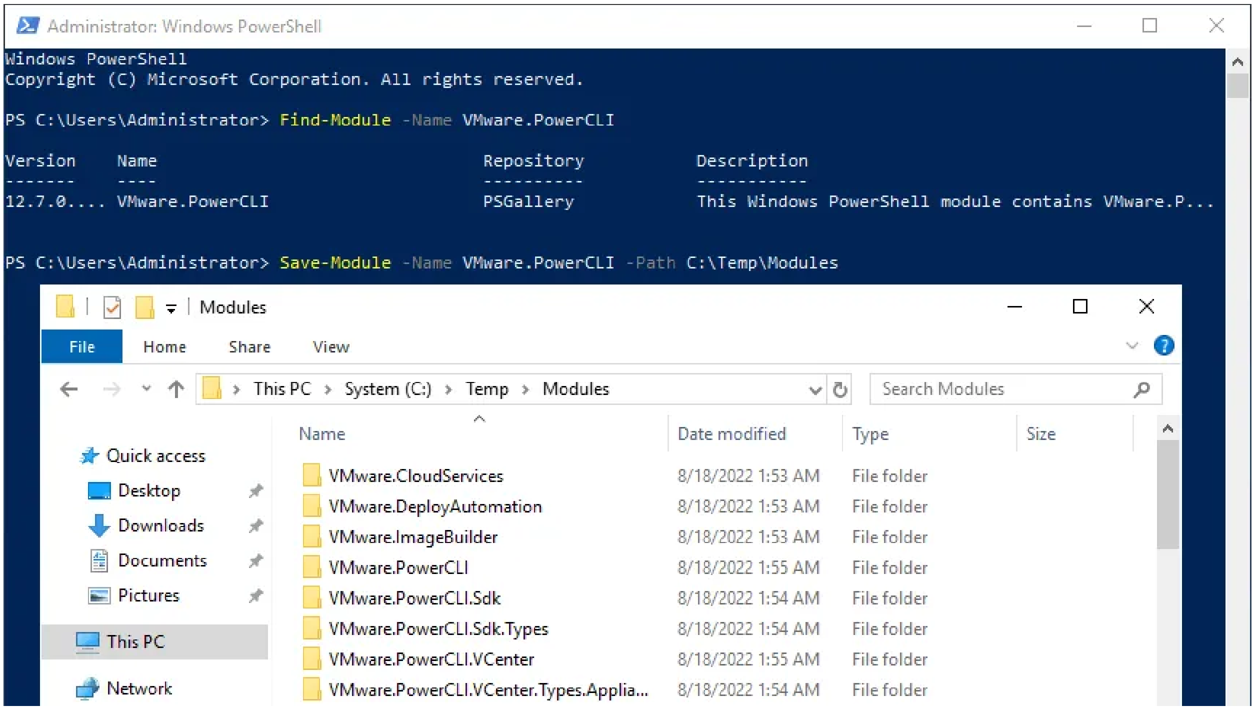
```
Find-Module -Name VMware.PowerCLI
```

2. Download and save the PowerCLI module files for PowerShell to a specified directory, for example, **C:\Temp\Modules\** with the command like:

```
Save-Module -Name VMware.PowerCLI -Path <path>
```

In our case, the exact command with the correct path is:

Save-Module -Name VMware.PowerCLI -Path C:\Temp\Modules



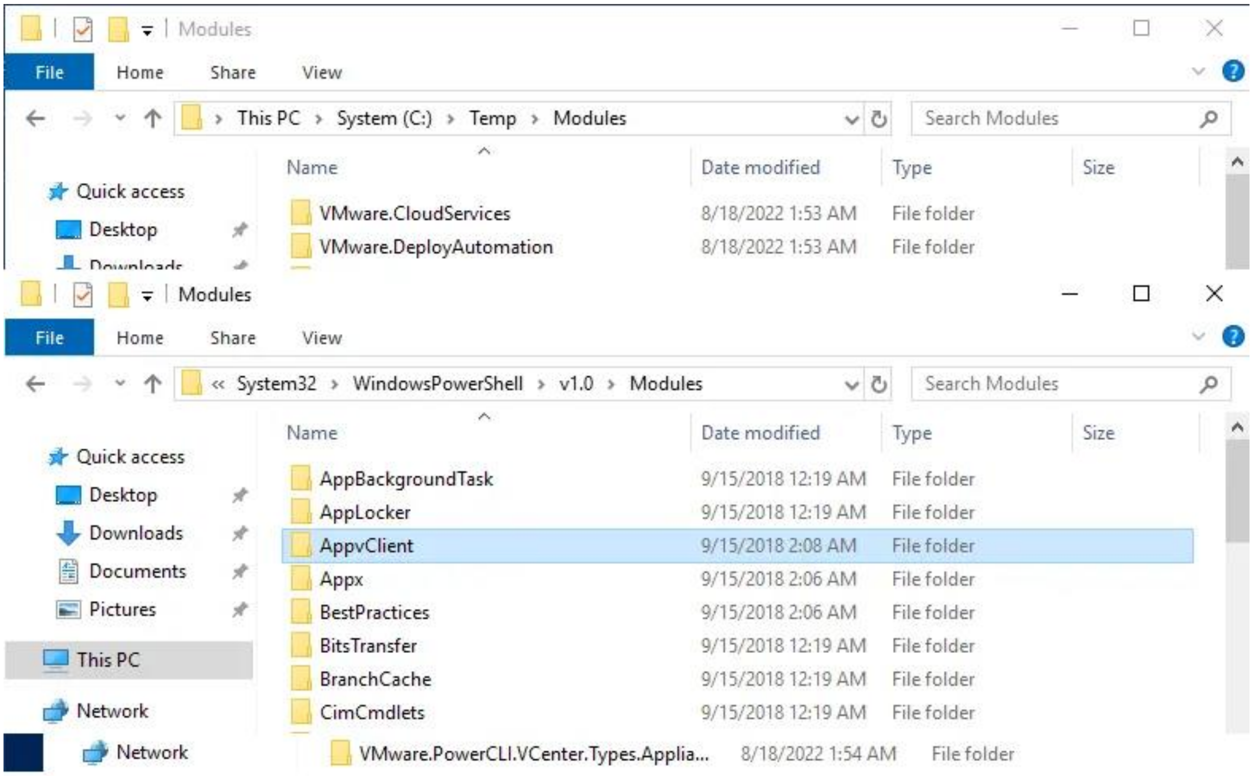
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Find-Module -Name VMware.PowerCLI

Version    Name                                Repository           Description
-------    ----                                ----------           -----------
12.7.0.... VMware.PowerCLI                     PSGallery            This Windows PowerShell module contains VMware.P...


PS C:\Users\Administrator> Save-Module -Name VMware.PowerCLI -Path C:\Temp\Modules
```

Name	Date modified	Type	Size
VMware.CloudServices	8/18/2022 1:53 AM	File folder	
VMware.DeployAutomation	8/18/2022 1:53 AM	File folder	
VMware.ImageBuilder	8/18/2022 1:53 AM	File folder	
VMware.PowerCLI	8/18/2022 1:55 AM	File folder	
VMware.PowerCLI.Sdk	8/18/2022 1:54 AM	File folder	
VMware.PowerCLI.Sdk.Types	8/18/2022 1:54 AM	File folder	
VMware.PowerCLI.VCenter	8/18/2022 1:55 AM	File folder	
VMware.PowerCLI.VCenter.Types.Applia...	8/18/2022 1:54 AM	File folder	

3. Copy the downloaded files from the **C:\Temp\Modules\** directory of your computer to a computer that is not connected to the internet.

Place the copied files to **C:\Windows\System32\WindowsPowerShell\v1.0\Modules**

Administrator rights are required.



Name	Date modified	Type	Size
VMware.CloudServices	8/18/2022 1:53 AM	File folder	
VMware.DeployAutomation	8/18/2022 1:53 AM	File folder	

Name	Date modified	Type	Size
AppBackgroundTask	9/15/2018 12:19 AM	File folder	
AppLocker	9/15/2018 12:19 AM	File folder	
AppvClient	9/15/2018 2:08 AM	File folder	
Appx	9/15/2018 2:06 AM	File folder	
BestPractices	9/15/2018 2:06 AM	File folder	
BitsTransfer	9/15/2018 12:19 AM	File folder	
BranchCache	9/15/2018 12:19 AM	File folder	
CimCmdlets	9/15/2018 12:19 AM	File folder	
VMware.PowerCLI.VCenter.Types.Applia...	8/18/2022 1:54 AM	File folder	

4. Unblock the downloaded files:

cd "C:\Program Files\WindowsPowerShell\v1.0\Modules"

Get-ChildItem * -Recurse | Unblock-File

5. PowerCLI installation is completed. Now you should be able to use vSphere PowerCLI on a computer that is not connected to the internet.

How to install PowerCLI offline from a ZIP archive

VMware provides an offline installer, which you can download and use to install PowerCLI offline on multiple computers.

1. Download the ZIP archive containing PowerCLI module files from the official VMware website:

https://developer.vmware.com/web/tool/vmware-powercli

The file name looks like *VMware-PowerCLI-12.7.0-20091289.zip* and the file size is about 100 MB.

2. Copy the downloaded ZIP archive to a computer that is not connected to the internet.

3. Extract the files to the directory where PowerShell modules are installed in Windows, for example, to

C:\Windows\System32\WindowsPowerShell\v1.0\Modules

4. PowerCLI installation is completed.

A. What are the ports required from SmartProfiler-SecID to Active Directory?

Q. Please ensure to open below default Active Directory ports from SmartProfiler-SecID to domain controllers:

Ports required for AD communication

The following ports are required for basic AD communication:

- TCP/UDP port 53: DNS
- TCP/UDP port 88: Kerberos authentication
- TCP/UDP port 135: RPC
- TCP/UDP port 137-138: NetBIOS
- TCP/UDP port 389: LDAP
- TCP/UDP port 445: SMB
- TCP/UDP port 464: Kerberos password change
- TCP/UDP port 636: LDAP SSL
- TCP/UDP port 3268-3269: Global catalog
- TCP port 636
- TCP port 9389 – For Active Directory Web Service

A. What are the ports required from SmartProfiler-SecID to VMware?

Q. Please ensure to open below default ports from SmartProfiler-SecID to VMware ESXi hosts and vCenter:

- TCP port 443
- TCP Port 8084

Note that SmartProfiler-SecID makes use of VMware PowerCLI and Port 8084 being the VUM SOAP server port is required to be opened.

***