TECHNICAL SPECIFICATIONS

NCPROTECT™

The following technical requirements represent the minimum recommended configuration for installing the NC Protect v6.2. Nucleus Cyber recognizes that each deployment is different and can advise how your specific environment should be configured to ensure optimal performance. For the complete list of requirements and details, refer to the Product Installation Guide.

Client Browser

Browsers supported by SharePoint:

- Internet Explorer® version 11.0 or greater
- Mozilla Firefox® (latest publicly released version)
- Google Chrome® (latest publicly released version)
- Apple Safari (latest publicly released version)

Hardware Requirements

For on-premises installations

- 64-bit, four or eight core CPU (depending on the deployment size)
- At least 8GB RAM

Software Requirements

For on-premises installations

- Microsoft SharePoint 2010, 2013, 2016, Foundation or greater
- Microsoft Windows 2008 Server Service Pack 1 and later
- 64-bit version of Microsoft SQL Server 2008 /2012/2014 (latest publicly released version)
- Microsoft® SQL Server® 2008 R2 Reporting Services or later (optional)
- Microsoft .NET Framework 3.51(SP2010); 4.5 (SP2013)
- Microsoft Active Directory RMS or Azure for Encryption (optional)

Software Requirements

For SharePoint Online installations

- SharePoint Online
- Microsoft Azure Subscriptions

Access to Azure Active Directory

- Pay-as-you-go
- Azure Rights Management (optional)
- PowerShell v5.1
- Microsoft .NET Framework 4.5
- Windows Azure AD Rights Management Administration
- Windows Azure Active Directory Module for Windows PowerShell

Questions?

For more information on the required technical specifications, or to discuss your specific enterprise requirements, please contact our Customer Support.

Online https://nucleuscyber.com/support/

Email support@nucleuscyber.com

NCPROTECT™

TECHNICAL SPECIFICATIONS

Supported Documents

Scanning

- **O365/SharePoint/File Shares:** The following default document types can be scanned using NC Protect: TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF*, .APSX, .HTM, .HTML, list items and events such as calendar entries.
- **Teams:** Conversations, Chats, Attachments and File types as above across Team Channels, Chat and Files locations.
- **Yammer:** Posts, Attachments and Files types as above
- **Exchange:** Scanning of email messages (MSG)

** Note: A PDF iFilter (e.g. Foxit PDF iFilter or Adobe PDF iFilter 9 for 64-bit platforms) is required for PDF documents to be scanned against privacy policies.*

Classification

NC Protect (on-premises installations only) can apply metadata fields on contents within File Share locations and the following SharePoint and Office 365 list/library types: Document library, Pages library, Generic list, Events list (calendar) and Tasks list.

Encryption

NC Protect uses Microsoft Rights Management to encrypt files. NC Protect can encrypt any file type not only the files natively supported by Microsoft Rights management. However, file formats that are not natively supported will require Rights Management Services Client 2.1.

NC Protect for Office 365

- Supported on NC Protect for Office 365, NC Protect web install, NC Protect 2013 and above.
- Secure Store Service to be configured for 'Passports' to be created and stored. Passports are used to define the credentials that will be used to access and process Office 365 (SharePoint Online and OneDrive) content. Refer to the following site to configure Secure Store Service in SharePoint: https://docs.microsoft.com/en-us/SharePoint/administration/configure-the-secure-store-service

NC Protect for File Shares

- Supported on NC Protect web install, NC Protect 2013 and above.
- The file system must be on a Microsoft Windows server and in the same AD domain or a domain trusted by the domain hosting the SharePoint farm.
- Secure Store Service to be configured for 'Passports' to be created and stored. Passports are used to define the credentials that will be used to access and process file share content.

NC Protect for Teams

- Supported on NC Protect for Office 365, NC Protect web install, NC Protect 2013 and above.
- Dynamic Access and Secure Document Rules supported for Teams Web App only. (*Teams Desktop App coming soon.)*
- Secure Store Service to be configured for 'Passports' to be created and stored. Passports are used to define the credentials that will be used to access and process Teams content. Refer to the following site to configure Secure Store Service in SharePoint: https://docs.microsoft.com/en-us/SharePoint/administration/configure-the-secure-store-service

NC Protect for Yammer

- Supported on NC Protect for Office 365, NC Protect web install, NC Protect 2013 and above.
- Secure Store Service to be configured for 'Passports' to be created and stored. Passports are used to define the credentials that will be used to access and process Yammer content. Refer to the following site to configure Secure Store Service in SharePoint: https://docs.microsoft.com/en-us/SharePoint/administration/configure-the-secure-store-service

NC Protect for Dropbox

(In Public Preview – GA Coming Soon)

Supported on NC Protect for Office 365, NC Protect web install, NC Protect 2013 and above.