

NC PROTECT™

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
- 64-bit version of Microsoft SQL Server 2012 and later
- Microsoft SQL Server® 2012 Reporting Services or later (optional)
- Microsoft .NET® Framework 4.0 and later
- Microsoft Active Directory® RMS or Azure for Encryption (optional)

For standalone Windows Server installations

- Microsoft Windows Server 2012 and later
- Internet Information Server 8.0 and later
- Microsoft .NET Framework 4.0 and later
- 64-bit version of Microsoft SQL® Server 2012 and later
- File Share, Dropbox, Teams and Yammer Assets: Access to these assets is granted through a Passport.

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

Supported Capabilities

Scanning

- **Office 365/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

Apply metadata fields on contents within SharePoint and Office 365 list/library types and associated Teams and Yammer libraries: Document library, Pages library, Generic list, Events list (calendar) and Tasks list.

Encryption

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

Conditional Access and Usage Rights

Content and Context aware augmentation of access and enforcement of usage rights for file visibility and access, application of secure viewer and dynamic watermarks, and rights management to control editing, downloading, copy and paste, etc.

- SharePoint 2010 and above
- Office 365 (SharePoint Online)
- Microsoft Teams (Web App, Desktop App coming soon)
- Windows file shares (coming soon)
- Dropbox (coming soon)

Supported Platforms

Office 365®

- Scanning, Classification and at-rest Encryption supported on NC Protect 2013 and above.
- Conditional access and usage rights features supported on NC Protect for Office 365.

SharePoint®

- Scanning, Classification and at-rest Encryption supported on NC Protect 2010 and above.
- Conditional access and usage rights features supported on NC Protect 2010 and above.

Microsoft Teams®

- Scanning, Classification and at-rest Encryption supported on NC Protect IIS Server, NC Protect 2013 and above.
- Conditional access and usage rights features supported for on NC Protect for Office 365 (*Teams Web App only, Teams Desktop App coming soon*).

Yammer®

- Scanning, Classification and at-rest Encryption supported on NC Protect IIS Server, NC Protect 2013 and above.

Windows® File Shares

- Scanning, Classification and at-rest encryption supported on NC Protect web install, NC Protect 2010 and above (*Conditional access and usage rights features coming soon*).
- The file system must be on a Microsoft Windows server and be in the same AD domain as the server or SharePoint farm where NC Protect is installed or in a trusted domain.

Dropbox®

- Scanning, Classification and at-rest Encryption supported on NC Protect IIS Server, NC Protect 2013 and above.