

NC PROTECT™

The following technical requirements represent the minimum recommended configuration for installing NC Protect version 8. Nucleus Cyber recognizes that each deployment is different and can advise on how your specific environment should be configured to ensure optimal performance. For the complete list of requirements and details, please refer to the Product Installation Guide.

Software Requirements

For Microsoft 365 installations

- SharePoint Online
- Microsoft Azure Subscriptions (e.g. Pay-as-you-go)
- Azure Active Directory
- Azure Information Protection P1

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 4.5 and later
- Microsoft Active Directory® RMS or Azure for Encryption
- Internet Information Server 7.5 and later

For standalone Windows Server installations

- Microsoft Windows Server 2012 and later
- Internet Information Server 8.0 and later
- Microsoft .NET Framework 4.5 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.
- Microsoft URL Rewrite Module 2.0 for IIS
- Windows PowerShell 5.1
- Microsoft Active Directory® RMS or Azure for Encryption

Client Browser

Browsers supported by SharePoint®:

- Microsoft Edge (latest publicly released version)
- Google Chrome® (latest publicly released version)
- Mozilla Firefox® (latest publicly released version)
- Apple Safari (latest publicly released version)

Azure Requirements

For Microsoft 365 installations

- Azure app service, Azure SQL and Azure Storage resources and scale up capability should be configured as appropriate for client use case

Microsoft Teams App Requirements

- iOS (iPhone) v3.4.1
- IOS (iPad MINI) v12.4.9
- Android (Samsung) v1416/1.0.0.2021040701
- Windows 10 v1.4.00.8872

Hardware Requirements

For on-premises installations

- 64-bit, four or eight core CPU (depending on the deployment size)
- At least 16GB RAM

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 & Apps

Scanning, Classification & Encryption At-Rest

Detect and alert presence of sensitive data within files, emails, and chat messages. Apply metadata classification on files and items. Encrypt at-rest any file type supported natively by Microsoft encryption technologies and additional file types with the appropriate Microsoft client install.

Microsoft 365 - SharePoint Online, SharePoint Server:

- The following default document types can be scanned using NC Protect: .TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF*, .ASPX, .HTM, .HTML, CAD (.dgn, .dwf, .dwx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cfx2), .png, .jpg, .jpeg, .tif, .tiff, .bmp, list items and events such as calendar entries* with NC Protect 8 and above.
- Classification and encryption at-rest of SharePoint contents within list and libraries - Document library, Pages library, Generic list, Events list (calendar) and Tasks list with NC Protect 6.0 and above.

OneDrive:

- Scanning, classification, and encryption at-rest of file types as above with NC Protect 6.0 and above.

Microsoft Teams:

- Scanning and classification of channel posts, chats, attachments, and file types as above across Team Channels, Chat and Files locations with NC Protect 6.3 and above.
- Encryption at rest of files types as above with NC Protect 6.3 and above

Microsoft Yammer:

- Scanning and classification of posts, attachments, and file types as above with NC Protect 6.0 and above.
- Encryption at rest of files types as above with NC Protect 6.0 and above

Microsoft 365 - Exchange Online, Exchange Server:

- Scanning, classification, and encryption at rest of email messages (MSG) with NC Protect 6.0 and above.

Windows File Shares:

- Scanning, classification, and encryption at-rest of file types as above with NC Protect 6.0 and above.
- The file system must be on a Microsoft Windows server and be in the same AD domain as the server where NC Protect is installed or in a trusted domain.

Nutanix Files:

- Scanning, classification, and encryption at-rest of file types as above with NC Protect 6.3 and above.
- The file system must be on a Nutanix Files server and be in the same AD domain as the server where NC Protect is installed or in a trusted domain.

Dropbox:

- Scanning, classification, and encryption at-rest of file types as above with NC Protect 6.0 and above.

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

Conditional Access, Encryption In-Transit & Usage Rights

Attribute-based augmentation of access and enforcement of usage rights for file, emails, and chat messages. Encrypt in-transit, enforce read only within web-based file viewer, apply Dynamic Watermarks and control user editing, copying, printing and download rights.

Microsoft 365 - SharePoint Online:

- Conditional access, encryption in-transit and usage rights supported on NC Protect 6.3 and above.

SharePoint Server:

- Conditional access, encryption in-transit and usage rights supported on NC Protect version 6.0 and above.

OneDrive:

- Conditional access, encryption in-transit and usage rights supported on NC Protect 7.0 and above.

Microsoft Teams:

- Conditional access, encryption in-transit and usage rights supported on NC Protect 7.0 and above.

Microsoft 365 - Exchange Online

- Conditional access, encryption in-transit and usage rights supported on NC Protect 7.0 and above.

Exchange Server:

- Conditional access, encryption in-transit and usage rights supported on NC Protect version 6.0 and above.

Windows File Shares:

- Conditional access, encryption in-transit and usage rights supported on NC Protect version 6.3 and above.

Nutanix Files:

- Conditional access, encryption in-transit and usage rights supported on NC Protect version 6.3 and above.