

# NC PROTECT™

## TECHNICAL SPECIFICATIONS

The following technical requirements represent the minimum recommended configuration for installing NC Protect version 8.5. archTIS 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

#### For SharePoint on-premises installations

- Microsoft SharePoint® 2016, 2019, SE or greater
- 64-bit version of Microsoft SQL® Server 2012 and later
- Microsoft SQL Server 2012 Reporting Services or later (optional)
- Microsoft .NET® Framework 4.7.1 and later
- Microsoft Active Directory® RMS or Azure® for Encryption
- Internet Information Server 8.5 and later

#### For standalone Windows Server installations

- Microsoft Windows Server 2012 and later
- Internet Information Server 8.5 and later
- Microsoft .NET Framework 4.7.1 and later
- 64-bit version of Microsoft SQL® Server 2012 and later
- File Share (WebDAV)
- Microsoft® URL Rewrite Module 2.0 for IIS
- Windows PowerShell 5.1
- Microsoft Active Directory® RMS or Azure for Encryption

### CLIENT BROWSER

- 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

- Teams iPhone App - Requires iOS 15.0 or later
- Teams Desktop App - Windows 10

### 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://www.archtis.com/support/> | Email: [ncprotect-support@archtis.com](mailto:ncprotect-support@archtis.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, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cfx2), .png, .jpg, .jpeg, .tif, .tiff, .bmp, list items and events such as calendar entries\*.
- Classification and encryption at-rest of SharePoint contents within list and libraries - Document library, Pages library, Generic list, Events list (calendar) and Tasks list.

#### OneDrive

- Scanning, classification, and encryption at-rest of file types as above.

#### Microsoft Teams

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

#### Microsoft 365 - Exchange Online, Exchange Server

Scanning, classification, and encryption at rest of email messages (MSG).

#### Windows File Shares

- Scanning, classification, and encryption at-rest of file types as 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.
- 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.

#### Secure Reader

The following document types are supported by the Secure Reader: .TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF\*, .ASPX, .HTM, .HTML, .EML, .MSG, CAD (.dgn, .dwf, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cfx2), .png, .jpg, .jpeg, .tif, .tiff, .bmp, list items and events such as calendar entries\*.

#### NC Encrypt

The NC Encrypt add-on module enables encryption of files at rest in SharePoint Online and SharePoint Server via Bring Your Own Key (BYOK) or built-in key generation that uses AES-256 bit encryption that is FIPS140-2 compatible.

## CONDITIONAL ACCESS, ENCRYPTION IN-TRANSIT & USAGE RIGHTS

NC Protect provides 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.

These capabilities (Conditional access, encryption in-transit and usage rights) are supported in the following platforms:

- Microsoft 365
- SharePoint Online
- SharePoint Server
- OneDrive
- Microsoft Teams
- Microsoft 365 - Exchange Online
- Exchange Server
- Windows File Shares
- Nutanix Files



archTIS.com | info@archtis.com | Australia | United States | United Kingdom



Copyright 2023 archTIS Limited. All rights reserved. archTIS, the archTIS logo, NC Protect, NC Protect logo, NC Encrypt, and the NC Encrypt logo are trademarks of archTIS Limited. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective holders.