

NC PROTECT™

FOR MICROSOFT 365 (M365)

V9.0.6 TECHNICAL SPECIFICATIONS

The following technical requirements represent the minimum recommended configuration for installing NC Protect for Microsoft 365 SharePoint Online version 9.0.6. 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.

SUPPORTED M365 ENVIRONMENTS

- Microsoft 365 Commercial
- GCC High
- DOD365

SOFTWARE REQUIREMENTS

Microsoft 365 installations

- SharePoint Online M365 Business Basics license (minimum)
- Microsoft Azure Subscriptions (e.g. Pay-as-you-go)
- Microsoft Entra ID free license (minimum)
- Microsoft 365 Business Premium - (optional minimum license required for Purview sensitivity label integration)
- Microsoft Purview Information Protection (MPIP) - M365 E5 Information Protection and Governance license active and registered (optional minimal license required for MPIP applied encryption)
- Microsoft Teams Desktop and Web App (latest publicly released version)

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

Scale up capability for the following components should be configured as appropriate for client use case.

- Azure Storage resources
- PostgreSQL
- Container Apps
- Azure storage
- Redis

INSTALLATION REQUIREMENTS

For the installation, Azure administration rights are required with the following software installed locally:

- PowerShell 7

CAPABILITIES

Classification

Apply metadata classification to files and items. Supports multi-label classification.

Alternatively use or augment existing classifications from Microsoft Purview Information Protection (MPIP) sensitivity labels.

Default document types that can be classified/tagged 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.

NC Protect can also apply Purview sensitivity labels to .XLSX, DOCX, and PPTX files.

Dynamic Encryption

NC Protect policies can utilize Microsoft Purview Information Protection (MPIP) encryption capabilities to dynamically apply conditional encryption.

Secure Reader

Document types supported by the Secure Reader: .TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF*, .VSD, .VSDX, .HTM, .HTML, .EML, .MSG, CAD (.dgn, .dwf, .dwg, .dxf, .iges, .plt, .stl), .png, .jpg, .jpeg, .bmp, list items and events such as calendar entries.

Conditional Access & Usage Rights

NC Protect provides data-centric, attribute-based policies to control file access and apply protection:

- Apply conditional access, usage and sharing rights based on any combination of metadata, Microsoft Purview Information Protection sensitivity labels, file and user attributes.
- Encrypt files based-on the policy at-rest using MPIP.
- Enforce read-only access using the built-in web-based Secure Reader.
- Apply dynamic watermarks and visual markings.
- Control editing, copying, printing and download rights.
- Set file access expiration.

INTEGRATIONS

SIEM Applications

Ingest NC Protect's user activity and protection logs into Microsoft Sentinel or Splunk for further analysis and downstream actions to build additional insights from the data and cross-correlate it with your ecosystem, streamline investigation, automate responses, and more.

ISEC7 CLASSIFY Integration

NC Protect extracts ISEC7 classification labels from office documents to allow policy application based on the embedded labels. NC Protect does not currently apply any labeling via ISEC7 CLASSIFY.

Formats currently supported for label extraction include: .DOCX, .PPTX, and .XLSX.

QUESTIONS?

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

Customer Help Center including Knowledgebase and Ticketing Portal: <https://help.archtis.com/> (login required)
No Help Center Account? Submit a ticket at: <https://www.archtis.com/support/> | Email: support@archtis.com



[archTIS.com](https://www.archtis.com) | info@archtis.com | Australia | United States | United Kingdom

