NCENCRYPT™

DATA ENCRYPTION & KEY MANAGEMENT FOR MICROSOFT 365®, SHAREPOINT SERVER® & FILE SHARES

Executive Summary

Ensure that your organization's business-critical data protection meets applicable regulatory and business requirements.

NC Protect adds granular access and protection controls to business-critical content in Microsoft applications by applying attribute-based access control (ABAC) and data protection policies that you define.

While dynamic classification and access control are NC Protect's first line of defense, when paired with Microsoft Purview Information Protection (MPIP) Azure RMS or NC Encrypt, it can encrypt the content immediately – limiting the audience to only credentialed users.

Key Benefits

- Enables compliance with GDPR, HIPAA and other privacy regulations with encryption and dynamic access control capabilities.
- Maintains control of your encryption keys in the Cloud.
- Adds dynamic at rest and in motion encryption capabilities
- Encrypt files and SharePoint list column values dynamically based on defined policies.
- Quick and easy to set up with system generated or your own encryption keys.
- Offers centrally controlled and granular security policies to alleviate dependency on user behavior.
- Supports BYOK with connectors to third party key management platforms.
- Agentless design for easy deployment and management.

WHY USE ENCRYPTION TO IMPROVE DATA SECURITY?

Encryption of sensitive data is important for data security and compliance - especially with the surge in the remote workforce and number of collaboration channels available today.

There are several points to keep in mind about the security and encryption of your documents and files; especially highly sensitive or regulated enterprise data such as personally identifiable information (PII), protected health information (PHI), intellectual property (IP), M&A and Board documents, as well as Defense and supply chain information:

- Encryption ensures that your sensitive data stays protected in case it is leaked or shared accidentally.
- The ability to identify and encrypt sensitive data is mandatory for certain compliance regulations (e.g., HIPAA/PHI, GDPR/PII).
- You should have dynamic fail-safe processes in place to encrypt highly sensitive, regulated or classified files shared via email.
- Data classification should be leveraged to set proper access permissions and encrypt sensitive or regulated data.

DATA ENCRYPTION YOUR WAY

Dynamically encrypt Microsoft 365 data in SharePoint Online and OneDrive, as well as SharePoint Server on-premises and File Shares to keep it protected no matter where it is stored or travels—in use, in motion and at rest.

NC Protect provides flexible options to encrypt your data and manage encryption keys:

- Out of the box NC Protect adds additional protection capabilities to the standard Microsoft Purview Information Protection (MPIP) and RMS controls that you may already own. Combining these Microsoft controls with NC Protect allows you to apply real-time protection of sensitive and business-critical data. NC Protect's ABAC policies dynamically apply encryption and other data protections based on file and user context according to defined policies.
- Available as an add on module to NC Protect, NC Encrypt provides encryption capabilities for organizations that do not have RMS, have third party key management in place or require independent key management. NC Encrypt combines encryption with the access permission policies from NC Protect to provide a more effective way to centrally set your security posture. With NC Encrypt, you manage encryption keys and security policies out-of-the-box or via connectors to leading HSM key management platforms, including Thales CipherTrust Manager.

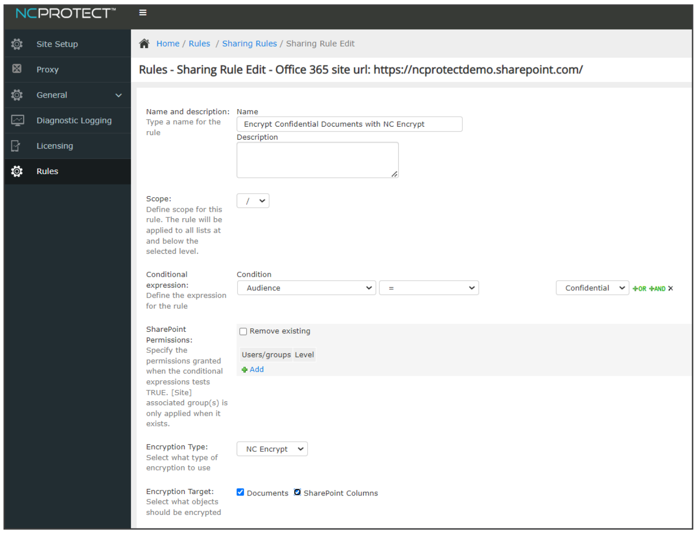
NCENCRYPT™

FLEXIBLE ENCRYPTION OPTIONS

NC Encrypt provides encryption capabilities out-of-the-box for organizations using NC Protect that prefer to manage their own encryption keys. NC Encrypt enables additional encryption and decryption capabilities using a company's own master key. A default AES-256 based encryption key will be dynamically created to get you started.

From the moment that you install NC Encrypt, your documents are secured immediately by the system generated encryption key. At any time in the future, you can switch to Bring Your Own Key (BYOK) via the NC Protect administration portal.

NC Encrypt's automatic key generation, key management and transfer to production procedures ensure that change control procedures, validation and testing phases are fully transparent and documented, while your data remains protected and encrypted.



Home / Rules / Sharing Rules / Sharing Rule Edit

Rules - Sharing Rule Edit - Office 365 site url: https://ncprotectdemo.sharepoint.com/

Name and description: Type a name for the rule

Name: Encrypt Confidential Documents with NC Encrypt

Description:

Scope: Define scope for this rule. The rule will be applied to all lists at and below the selected level. — /

Conditional expression: Define the expression for the rule

Condition: Audience = Confidential +OR +AND ✕

SharePoint Permissions: Specify the permissions granted when the conditional expressions tests TRUE. [Site] associated group(s) is only applied when it exists.

☐ Remove existing

Users/groups	Level

+ Add

Encryption Type: Select what type of encryption to use — NC Encrypt

Encryption Target: Select what objects should be encrypted — ☑ Documents ☑ SharePoint Columns

Above left: Easily build encryption into data protection policies in NC Protect's central policy manager.

KEY CAPABILITIES

Encrypt Files & SharePoint Columns

- Dynamic policy-driven encryption of individual files in supported applications and SharePoint columns.
- Encrypt any documents, including MPIP protected/encrypted documents.
- Apply different at rest encryption methodologies to meet your security needs using NC Encrypt, Microsoft Purview Information Protection (MPIP), or CipherTrust Manager, or a combination of these depending on the file and use case.

Remote Key Management

- Exclusive, customer-only control of encryption keys for M365 (Microsoft controlled environment).
- Enables keys to be stored in specific geographical locations for data sovereignty and compliance.
- Keys and key management performed by NC Protect in customer on-premises server.
- Data encryption keys transferred from on-premises to NC Protect in customer Azure tenancy with point-to-point encrypted payload.

Bring Your Own Key (BYOK) Support

- Supply and manage your own keys or use NC Encrypt's dynamically created keys.
- Manage and automate key rotation.
- Provides connectors for third party key management platforms.

Strong Encryption

- Uses secure AES-256 bit encryption that is FIPS 140-2 compatible.

Centrally Manage Encryption and Access

- Control encryption and access policies across all M365 apps, SharePoint Online, SharePoint Server, File Shares and/or hybrid environments from the NC Protect administration portal.

Reporting & Auditing

- Real-time activity logging and reporting tracks permitted and denied access requests, and actions taken with authorized files.

SUPPORTS ENCRYPTION ACROSS THESE APPLICATIONS

SharePoint Online & On-Premises

OneDrive

Office 365

File Shares

archTIS

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