Encrypted SMB

SMB security enhancements

- Article
- 05/18/2023
- 15 contributors

Feedback

In this article

Show 2 more

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI version 21H2, Windows 11, Windows 10

This article explains the SMB security enhancements in Windows Server and Windows.

SMB Encryption

SMB Encryption provides SMB data end-to-end encryption and protects data from eavesdropping occurrences on untrusted networks. You can deploy SMB Encryption with minimal effort, but it might require other costs for specialized hardware or software. It has no requirements for Internet

Protocol security (IPsec) or WAN accelerators. SMB Encryption can be configured on a per share basis, for the entire file server, or when mapping drives.

Note

SMB Encryption does not cover security at rest, which is typically handled by BitLocker Drive Encryption.

You can consider SMB Encryption for any scenario in which sensitive data needs to be protected from interception attacks. Possible scenarios include:

- You move an information worker's sensitive data by using the SMB protocol. SMB Encryption offers an end-to-end privacy and integrity assurance between the file server and the client. It provides this security regardless of the networks traversed, such as wide area network (WAN) connections maintained by non-Microsoft providers.
- SMB 3.0 enables file servers to provide continuously available storage for server applications, such as SQL Server or Hyper-V. Enabling SMB Encryption provides an opportunity to protect that information from snooping attacks. SMB Encryption is simpler to use than the dedicated hardware solutions that are required for most storage area networks (SANs).

Windows Server 2022 and Windows 11 introduce AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption. Windows automatically negotiates this more advanced cipher method when connecting to another computer that supports it. You can also mandate this method through Group Policy. Windows still supports AES-128-GCM and AES-128-CCM. By default, AES-128-GCM is negotiated with SMB 3.1.1, bringing the best balance of security and performance.

Windows Server 2022 and Windows 11 SMB Direct now support encryption. Previously, enabling SMB encryption disabled direct data placement, making RDMA performance as slow as TCP. Now data is encrypted before placement, leading to relatively minor performance degradation while adding AES-128 and AES-256 protected packet privacy. You can enable encryption using Windows Admin Center, Set-SmbServerConfiguration, or UNC Hardening group policy.

Furthermore, Windows Server failover clusters now support granular control of encrypting intra-node storage communications for Cluster Shared Volumes (CSV) and the storage bus layer (SBL). This support means that when using Storage Spaces Direct and SMB Direct, you can encrypt east-west communications within the cluster itself for higher security.

Important

There is a notable performance operating cost with any end-to-end encryption protection when compared to non-encrypted.

Enable SMB Encryption

You can enable SMB Encryption for the entire file server or only for specific file shares. Use one of the following procedures to enable SMB Encryption.

Enable SMB Encryption with Windows Admin Center

1. Download and install Windows Admin Center.
2. Connect to the file server.
3. Select **Files & file sharing**.
4. Select the **File shares** tab.
5. To require encryption on a share, select the share name and choose **Enable SMB encryption**.
6. To require encryption on the server, select **File server settings**.
7. Under **SMB 3 encryption**, select **Required from all clients (others are rejected)**, and then choose **Save**.

Enable SMB Encryption with UNC Hardening

UNC Hardening lets you configure SMB clients to require encryption regardless of server encryption settings. This feature helps prevent interception attacks. To configure UNC Hardening, see MS15-011: Vulnerability in Group Policy could allow remote code execution. For more information on interception attack defenses, see How to Defend Users from Interception Attacks via SMB Client Defense.

Enable SMB Encryption with Windows PowerShell

1. Sign into your server and run PowerShell on your computer in an elevated session.
2. To enable SMB Encryption for an individual file share, run the following command.

   PowerShell Copy

   ```
   Set-SmbShare –Name <sharename> -EncryptData $true
   ```

3. To enable SMB Encryption for the entire file server, run the following command.

PowerShell Copy

```
Set-SmbServerConfiguration –EncryptData $true
```

4. To create a new SMB file share with SMB Encryption enabled, run the following command.

   PowerShell Copy

   ```
   New-SmbShare –Name <sharename> -Path <pathname> –EncryptData $true
   ```

Map drives with encryption

1. To enable SMB Encryption when mapping a drive using PowerShell, run the following command.

   PowerShell Copy

   ```
   New-SMBMapping -LocalPath <drive letter> -RemotePath <UNC path> -RequirePrivacy $TRUE
   ```

2. To enable SMB Encryption when mapping a drive using CMD, run the following command.

   Windows Command Prompt Copy

   ```
   NET USE <drive letter> <UNC path> /REQUIREPRIVACY
   ```

Considerations for deploying SMB Encryption

By default, when SMB Encryption is enabled for a file share or server, only SMB 3.0, 3.02, and 3.1.1 clients are allowed to access the specified file shares. This limit enforces the administrator's intent of safeguarding the data for all clients that access the shares.

However, in some circumstances, an administrator might want to allow unencrypted access for clients that don't support SMB 3.x. This situation could occur during a transition period when mixed client operating system versions are being used. To allow unencrypted access for clients that don't support SMB 3.x, enter the following script in Windows PowerShell:

PowerShell Copy

```
Set-SmbServerConfiguration –RejectUnencryptedAccess $false
```

Note

We do not recommend allowing unencrypted access when you have deployed encryption. Update the clients to support encryption instead.

The preauthentication integrity capability described in the next section prevents an interception attack from downgrading a connection from SMB 3.1.1 to SMB 2.x (which would use unencrypted access). However, it doesn't prevent a downgrade to SMB 1.0, which would also result in unencrypted access.

To guarantee that SMB 3.1.1 clients always use SMB Encryption to access encrypted shares, you must disable the SMB 1.0 server. For instructions, connect to the server with Windows Admin Center and open the **Files & File Sharing** extension, and then select the **File shares** tab to be prompted to uninstall. For more information, see How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows.

If the **–RejectUnencryptedAccess** setting is left at its default setting of **$true**, only encryption-capable SMB 3.x clients are allowed to access the file shares (SMB 1.0 clients are also rejected).

Consider the following issues as you deploy SMB Encryption:

- SMB Encryption uses the Advanced Encryption Standard (AES)-GCM and CCM algorithm to encrypt and decrypt the data. AES-CMAC and AES-GMAC also provide data integrity validation (signing) for encrypted file shares, regardless of the SMB signing settings. If you want to enable SMB signing without encryption, you can continue to do so. For more information, see Configure SMB Signing with Confidence.
- You might encounter issues when you attempt to access the file share or server if your organization uses wide area network (WAN) acceleration appliances.
- With a default configuration (where there's no unencrypted access allowed to encrypted file shares), if clients that don't support SMB 3.x attempt to access an encrypted file share, Event ID 1003 is logged to the Microsoft-Windows-SmbServer/Operational event log, and the client receives an **Access denied** error message.
- SMB Encryption and the Encrypting File System (EFS) in the NTFS file system are unrelated, and SMB Encryption doesn't require or depend on using EFS.
- SMB Encryption and the BitLocker Drive Encryption are unrelated, and SMB Encryption doesn't require or depend on using BitLocker Drive Encryption.

Preauthentication integrity

SMB 3.1.1 is capable of detecting interception attacks that attempt to downgrade the protocol or the capabilities that the client and server negotiate by use of preauthentication integrity. Preauthentication integrity is a mandatory feature in SMB 3.1.1. It protects against any tampering with Negotiate and Session Setup messages by using cryptographic hashing. The resulting hash is

used as input to derive the session's cryptographic keys, including its signing key. This process enables the client and server to mutually trust the connection and session properties. When the client or the server detects such an attack, the connection is disconnected, and event ID 1005 is logged in the Microsoft-Windows-SmbServer/Operational event log.

Because of this protection, and to take advantage of the full capabilities of SMB Encryption, we strongly recommend that you disable the SMB 1.0 server. For instructions, connect to the server with Windows Admin Center and open the **Files & File Sharing** extension, and then select the **File shares** tab to be prompted to uninstall. For more information, see How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows.

New signing algorithm

SMB 3.0 and 3.02 use a more recent encryption algorithm for signing: Advanced Encryption Standard (AES)-cipher-based message authentication code (CMAC). SMB 2.0 used the older HMAC-SHA256 encryption algorithm. AES-CMAC and AES-CCM can significantly accelerate data encryption on most modern CPUs that have AES instruction support.

Windows Server 2022 and Windows 11 introduce AES-128-GMAC for SMB 3.1.1 signing. Windows automatically negotiates this better-performing cipher method when connecting to another computer that supports it. Windows still supports AES-128-CMAC. For more information, see Configure SMB Signing with Confidence.

Disabling SMB 1.0

SMB 1.0 isn't installed by default starting in Windows Server version 1709 and Windows 10 version 1709. For instructions on removing SMB1, connect to the server with Windows Admin Center, open the **Files & File Sharing** extension, and then select the **File shares** tab to be prompted to uninstall. For more information, see How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows.

If it's still installed, you should disable SMB1 immediately. For more information on detecting and disabling SMB 1.0 usage, see Stop using SMB1. For a clearinghouse of software that previously or currently requires SMB 1.0, see SMB1 Product Clearinghouse.

Related links

- Overview of file sharing using the SMB 3 protocol in Windows Server

- Windows Server Storage documentation
- Scale-Out File Server for application data overview

Revision #1
Created 23 December 2023 07:46:34 by ColtM
Updated 13 June 2024 01:28:02 by ColtM