Microsoft OneDrive for Business

Microsoft 365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add M=Modify D=Delete	Description of Change
V0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Table of Contents

This page is intentionally blank.

1 Introduction

OneDrive for Business is a cloud-based file storage system with online editing and collaboration tools for Microsoft Office documents and is part of Office 365. OneDrive for Business facilitates synchronization across multiple devices and enables secure, compliant, and intelligent collaboration with multiple people.

This security baseline applies guidance from industry benchmarks on how to secure cloud solutions on Azure.

1.1 Assumptions

These baseline specifications assume that the agency is using OneDrive for Business, not personal or school versions; and allowing access using both OneDrive application sync and the browser-based client.

It is also assumed that the agency will use Azure Active Directory to authenticate accounts and authorize applications.

The **License Requirements** sections of this document assume the organization is using an Microsoft 365 E3 or G3 license level. Therefore, only licenses not included in E3/G3 are listed.

1.2 Resources

2 Baseline

2.1 Anyone Links SHOULD Be Turned Off

Unauthenticated sharing (Anyone links) is used to share data without authentication and users are free to pass it on to others outside the agency. To prevent users from unauthenticated sharing of content, turn off Anyone sharing for users outside the tenant when accessing content in SharePoint, Groups, or Teams.

2.1.1 Policy

- Anyone links SHOULD be disabled.

2.1.2 Resources

- Limit accidental exposure | Microsoft Docs

2.1.3 License Requirements

- N/A

2.1.4 Implementation

Note: OneDrive settings can be more restrictive than the SharePoint setting, but not more permissive.

To turn off Anyone links for the agency:

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, expand **Policies,** then select **Sharing**.
3. Set the SharePoint external sharing settings to **New and existing guests**, then set OneDrive to **New and existing guests**.
4. Click **Save**.

To turn off Anyone links for a site:

1. In the **SharePoint admin center** left navigation pane, expand **Sites,** and select **Active sites**.
2. Select the site to configure.
3. In the ribbon, select **Sharing**.
4. Ensure that **Sharing** is set to **New and existing guests**.
5. Click **Save**.

2.2 Expiration Date SHOULD Be Set for Anyone Links

Files that are stored in SharePoint sites, Groups, and Teams for months and years could lead to unexpected modifications to files if shared with unauthenticated people. Configuring expiration times for Anyone links can help avoid unwanted changes. If Anyone links are enabled, the expiration date SHOULD be set to thirty days or as determined by mission needs or agency policy.

2.2.1 Policy

- An expiration date SHOULD be set for Anyone links.
- Expiration date SHOULD be set to thirty days.

2.2.2 Resources

- Best practices for unauthenticated sharing | Microsoft Docs

2.2.3 License Requirements

- N/A

2.2.4 Implementation

To set an expiration date for Anyone links across the agency (**Note**: Anyone links must be enabled).

1. Open the **SharePoint admin center.**
2. In the left-hand navigation pane, expand **Policies**, and then select **Sharing**.
3. Under **Choose expiration and permissions options for Anyone links**, select the **These links must expire within this many days** check box.
4. Enter the number of days in the box, and then click **Save**.

To set an expiration date for Anyone links on a specific site:

1. Open the **SharePoint admin center**, expand **Sites**, and then select **Active sites**.
2. Select the site to change, and then select **Sharing**.
3. Under **Advanced settings for Anyone links**, under **Expiration of Anyone links**, clear the **Same as organization-level setting** check box.
4. Select the **These links must expire within this many days** option and enter a number of days in the box.
5. Click **Save**.

2.3 Link Permissions SHOULD Be Set to Enabled Anyone Links to View

The Anyone links default to allow people to edit files, as well as edit and view files and upload new files to folders. To allow unauthenticated sharing but keep unauthenticated people from modifying the agency's content, consider setting the file and folder permissions to **View**.

2.3.1 Policy

- Anyone link permissions SHOULD be limited to View.

2.3.2 Resources

- Set link permissions | Microsoft Docs

2.3.3 License Requirements

- N/A

2.3.4 Implementation

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, expand **Policies**, then select **Sharing**.
3. Under **Advanced settings for Anyone links**, set the file and folder permissions to **View**.

2.4 OneDrive Client SHALL Be Restricted to Windows for Agency-Defined Domain(s)

Configuring OneDrive to sync only to agency-defined domains ensures that users can only sync to agency-managed computers.

2.4.1 Policy

- OneDrive Client for Windows SHALL be restricted to agency-Defined Domain(s).

2.4.2 Resources

- Allow syncing only on computers joined to specific domains – OneDrive | Microsoft Docs

2.4.3 License Requirements

- N/A

2.4.4 Implementation

1. Open the **SharePoint admin center.**
2. In the left-hand navigation pane, select **Settings** and sign in with an account that has admin permissions for the agency.
3. Select **Sync**.
4. Select the **Allow syncing only on computers joined to specific domains** check box.
5. Add the Globally Unique Identifier (GUID) of each domain for the member computers that the agency wants to be able to sync.

   Note: Add the domain GUID of the computer domain membership. If users are in a separate domain, only the domain GUID that the computer account is joined to is required.

   Important: This setting is only applicable to Active Directory domains. It does not apply to Azure Active Directory (AAD) domains. If agency devices are only Azure AD joined, consider using a Conditional Access Policy instead.
6. Click **Save**.

2.5 OneDrive Client SHALL Be Restricted to Sync with Mac for Agency-Defined Devices

Set restrictions on whether users can sync items to non-domain joined machines, control the list of allowed domains, and manage whether Mac clients (which do not support domain join) can sync.

2.5.1 Policy

- OneDrive Client Sync SHALL only be allowed only within the local domain.

2.5.2 Resources

- Set-SPOTenantSyncClientRestriction (SharePointOnlinePowerShell) | Microsoft Docs

2.5.3 License Requirements

- N/A

2.5.4 Implementation

The **Set-SPOTenantSyncClientRestriction** cmdlet can be used to enable the feature for tenancy and set the domain GUIDs in the safe recipients list. When this feature is enabled, it can take up to 24 hours for the change to take effect. However, any changes to the safe domains list are reflected within five minutes.

```
Set-SPOTenantSyncClientRestriction -Enable -DomainGuids "786548DD-877B-4760-A749-6B1EFBC1190A; 877564FF-877B-4760-A749-6B1EFBC1190A" -BlockMacSync:$false
```

2.6 OneDrive Client Sync SHALL Only Be Allowed Within the Local Domain

Configuring OneDrive to sync only to agency-defined domains ensures that users can only sync to agency-managed computers.

2.6.1 Policy

- OneDrive Client Sync SHALL be restricted to the local domain.

2.6.2 Resources

- Allow syncing only on computers joined to specific domains | Microsoft Documents

2.6.3 License Requirements

- N/A

2.6.4 Implementation

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, select **Settings**.
3. Next to **OneDrive**, click **Sync** to display synchronization settings.
4. On the **Sync settings** page, confirm that **Allow syncing only on computers joined to specific domains** is checked and that a domain GUID displays in the box below it.

2.7 Legacy Authentication SHALL Be Blocked

Modern authentication, based on Active Directory Authentication Library (ADAL) and Open Authorization 2 (OAuth2), is a critical component of security in Office 365. It provides the device authentication and authorization capability of Office 365, which is a foundational security component. If modern authentication is not required, this creates a loophole that could allow unauthorized devices to connect to OneDrive and download/exfiltrate enterprise data. For this reason, it is important to make sure that only apps that support modern authentication are allowed to connect, assuring that only authorized devices are allowed to access enterprise data.

2.7.1 Policy

- Legacy Authentication SHALL be blocked.

2.7.2 Resources

- Control access from unmanaged devices | Microsoft Documents

2.7.3 License Requirements

- N/A

2.7.4 Implementation

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, click **Policies** > **Access Control** > **Device access**.
3. Click **Apps that don't use modern authentication** to display the device access settings.
4. On the **Apps that don't use modern authentication** page, select the **Block access** option.

3 Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors
Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors
Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).

Appendix A Configuring On-Premises Devices

A 1 Limit Syncing to Agency-defined Equipment within the Agency (Tenants)

OneDrive includes a sync client that allows users to synchronize their files from the OneDrive cloud service to their desktop/laptop computer. This allows them to interact with a local copy of the files in a way that is very similar to working with regular local files on their computer.

Resources

Use OneDrive policies to control sync settings - OneDrive | Microsoft Docs