WHITEPAPER

MSP360 Managed Backup - Security Best Practices

This guide is aimed to help MSP360 customers properly configure Managed Backup in order to minimize the impact of accidental or malicious file changes and malware infections, including ransomware. The document covers best practices for settings in the Managed Backup web console, the backup agents, and deployed backup plans, including some recommended best practices for you and your customer environments.

Managed Console best practices

Enable Two-Factor Authentication

Two-Factor Authentication (2FA) adds a second layer of login security for the main administrator and sub-admin accounts. You can use Google Authenticator or Microsoft Authenticator with your iOS or Android mobile devices to require a second code be entered when logging into Managed Backup.

To enable 2FA on the main Administrator account, login as the main administrator, go to Settings - General. Click the **Enable Two-Factor Authentication (2FA)** button and download and run either the MSP360 Control application or any third-party Authenticator apps on your mobile device. Click the Add Account and scan the barcode on the Managed Backup screen. The account is now secured with 2FA access.

After you switch the 2FA option on, you will see the generated **2FA Recovery Codes** that can be used to access the console in case of emergency – for instance, if you accidentally remove yourself from the **Allowlist**. Click the **Salve to File** link. These codes can be used for authentication within the console, so, for security reasons, keep them in a place with limited access.

To enable 2FA on a sub administrator, create the new account under Administrators, then have the subadmin log into Managed Backup and navigate to the Administrators screen and follow the instructions above. You can also force 2FA to be switched on for all your sub-administrators: under the root account, go to the **General** tab, **Settings** section, mark the **Force Two-Factor Authentication** for all administrators checkbox, and click Save.

Once complete, your admin accounts will be secured with 2FA access. If someone should accidentally save their login password in a browser or someone gains access to an admin password, they will not be able to log into Managed Backup without access to the admin's mobile device.

Use IAM Role Access to your AWS S3 Storage

When creating your AWS S3 Storage in Managed Backup, use Identity and Access Management (IAM) Roles instead of the classic Access / Secret Keys. IAM roles do not have associated access keys, so there are no credentials to steal. Instead, temporary access is granted so backup and restore plans can access S3 storage.

Configuring your S3 accounts in Managed Backup with IAM Roles is detailed in this help article.

Added Security with General Agent Options

In MSP360 Managed Backup, you can also protect the backup agents that are installed on the endpoints. Here are some additional security settings that restrict access and functionality in the deployed backup agents:

You can disable your customers from accessing the installed Managed Backup agent by unchecking the **Enable Backup Agent** option in Settings – Global Agent Options. This prevents any end-users from accessing the agent and making changes.

If you leave the agent accessible, you can prevent someone manually deleting backed up files from the Storage tab by unchecking the **Enable ability to delete files from the Storage tab** (disabled by default) option.

If you want to restrict someone from changing backup or restore plans, you can uncheck either or both, **Allow to Edit Backup plans** and **Allow to Edit Restore Plans**. This feature limits the backup\restore plan edit from the endpoint agent, while you can still edit the plans using the Managed Console.

It recommended to keep the option **Ebable Pre\Post Actions** disabled. This prevents adding and running additional scripts before and\or after the backup plan execution.

If you do not plan to allow remote access to the remote machine running the Managed Backup agent, then uncheck **Allow Remote Access to computer** on the "Connect" tab.

Create Unique User Accounts for each Customer

User accounts are used to authenticate your customer's computers with the Managed Backup service. It's best to use one or more user accounts per customer. At a minimum, create a new user account for each customer. However, if the customer is large or if it contains different groups of computers (e.g. servers vs endpoints) or different internal departments (e.g. accounting vs HR) that need to be managed differently, consider creating a user account for each group. Remember, user accounts not only authenticate, but are also used to assign storage and can be used to create deployments with specific rules. As always, these accounts should be secured with a strong, unique password (never share passwords between user accounts). Currently, when you authorize the computer on the Computers page, it creates the individual user for each endpoint.

Use IP Allowlists to Allow Access only from Approved Network Locations

You can prevent access to the management console from computers that are not in an approved IP address range. To do this, go to **Settings – IP Allowlisting** and enable the option. Enter a set of IP addresses or IP address ranges and Save. Once enabled, if someone should try to access the management console from an unknown location, the connection will be rejected.

Follow the Principle of Least Privileges when Creating Admins

The principle of least privileges states that an administrator (in our case) should have only those permissions that are necessary for their job, and no more. This is vital, as your administrators shouldn't be able to compromise your security accidentally or on purpose. In the Organization - Administrators section, you can

granularly customize the permissions for each of your administrators – for instance, assign each administrator to a specific company.

Backup Agents – Security Best Practices

Always Test and Install the Latest Agent Versions

It's always a good idea to use the latest agents released for Windows, Linux, and Mac. New versions not only contain new and updated features, but also stability, performance, and security enhancements. You can easily create a new download for the latest version from **Downloads**, test it in your environment from the sandbox which can be enabled from **Downloads - Options**. When you've approved the new release, click the Make Public option so deployed agents are automatically updated the next time they start a backup or restore.

To ensure Automatic Updates are enabled, click the **Options** in **Downloads** menu, and make sure the option to **Allow Automatic Update** is checked.

Use Cloud Storage for all Important Backups

If you work with regulated data like medical records, sensitive data like legal or accounting, or want to make sure any data you are backing up is using the best security against disaster / malware, then you must back up to the cloud. You can clone the existing backup job and edit the backup destination there. The cloud helps protect your backups from malware or a bad actor that can easily access your local backups from the network.

Lock Agents with a Master Password

In addition to the agent features mentioned above, you can also optionally set a master password to allow access to the agent (this will also restrict access to the underlying Managed Backup APIs from the client). To enable this feature, you need to use the Backup – Backup Template option. Backup Templates allow you to create a configuration – a default set of options and backup / restore plans that can be easily applied to one or more computers through Rules. Rules allow you to deploy to a customer, user account, or a specific computer. To enable the option, check **Protect Console with a Master Password** in the Settings section during the creation of the new configuration. Additionally, it is recommended to protect the command line interface with this password. To do this, switch on the **Protect CLI** with Master Password option.

Backup Plans – Security Best Practices

Enable Immutability

Immutability is currently the highest level of backup protection possible. Immutable backups are not prone to ransomware, unattended access, or human factors. Even if you lose all your data, an immutable backup will help you to rebuild everything from scratch, using clean, uncorrupted data.

In MSP360 Managed Backup, immutability is supported for Amazon S3, Wasabi and BackBlaze storage providers. To create an immutable backup in MP360 Managed Backup, proceed to the Backup - Storage Accounts section, choose an account, and click the gear icon. Here, you can add a new bucket with immutability enabled or edit an existing bucket. To create an immutable backup, create a backup plan, reach the **Retention Policy** step, switch on the **GFS** feature and specify periods of retention for daily/weekly/yearly backups, click **Enable Immutability** and confirm that you want to make backups unchangeable.

Always Encrypt Backups

You should encrypt all backups. Enable 256-bit AES encryption and set a strong password for every backup plan. It's also good practice to use different passwords for each customer and more than one within a single customer, when needed. Encrypting the backup is easy and a strong password protects the backup data against brute force decryption techniques and may also be required for regulatory compliance. Regardless, it's best to encrypt always for best protection.

If your cloud storage offers a server-side encryption option, you should use it. Server-side encryption adds an additional layer of encryption on top of client-side encryption and helps protect your data in the rare case where someone steals a hard drive from the cloud vendor.

Make sure all network traffic is encrypted. If a storage option is available with an **SSL / TLS** option, then you should use it to ensure all traffic between the agent and the storage account is fully encrypted.

MSP360 doesn't store encryption passwords, so if you lose them for any reason, we can not help with their recovery and the data can not be restored. To protect against this, it's recommended to enable the **Password Recovery Service**, located in **Settings** menu. It uses private and public key, where the private key must be stored somewhere on your computer securely.

Fully Document and Test your Backups and Disaster Recovery Plans

Make sure to fully document and test your BDR plans. Test recovery scenarios to make sure you can adhere to your committed restore time objectives. This will help you avoid mistakes and extended restore times when it's important you restore critical customer data as soon as possible. It's recommended to run the test restorations at least every 3 months.

Apply a 3-2-1 Backup Rule to your Backup Strategy

The **3-2-1 backup** rule requires you keep 3 copies of your data (live data, plus two backups), you use 2 different storage media, and you have 1 copy offsite. You can run separate local and cloud backups. The local backups can be used for faster restores. The cloud backups provide the disaster recovery protection from natural disaster and malware attacks and can be protected from any deletion with **Immutability** feature.

Adjust your Retention Policies Accordingly

Retention policies determine how long backups are kept and how many backup versions you want to keep. In most cases, you should keep enough versions to avoid any malware attacks overwriting backup data with corrupted / encrypted file versions. Storing backups for less than 2 weeks can decrease the security of your backups.

Avoid Manual File Operations of Backup Storage Outside Managed Backup

Managed Backup automatically keeps track of all files sent to backup storage and stores this information in a local repository on each client. The repository is used to easily detect changes in files and improve backup speed. All backup plan executions and any modifications made in the Storage tab in the agents are automatically tracked in the local repository. However, if you make changes to files in backup storage outside of the Managed Backup interface, the repository and backup storage will be out-of-sync and require you run a Consistency Check. Consistency checks bring the repository in sync again with backup storage. However, it's best to avoid this process altogether by making sure any changes to backup storage are performed in Managed Backup.