# Guide for updating Veeam Backup *for Microsoft 365*

**Karinne Bessette,**

Technologist,
Product Strategy,
Veeam Software

Updating anything in an environment can be a very stressful process and is easily the least favorite task of any IT team. This is in large part due to the unknowns that can happen while updating any products or components. No one wants to modify something that is currently working, bringing on the mentality of "if it's not broke, don't fix it". This common rule can be a double edge sword that leaves your environment open to security vulnerabilities and dated product features. Considering this problem, I think Grace Hopper said it best "The most dangerous phrase in the language is, 'we've always done it this way'". This post is a guide for the reasons and process for updating Veeam® Backup *for Microsoft 365*.

## Latest features

Beyond security concerns, the greatest reason to upgrade a product is because of the new and enhanced features, Veeam Backup *for Microsoft 365* is no exception to this rule. Veeam Backup *for Microsoft 365* is our solution to backing up Microsoft's Software as a Service offering, Microsoft 365. Microsoft 365 is continuously updating and enhancing their software in order to meet customers' constantly evolving needs. When the updates roll into the frontend interface for users they may only see minor differences, but the backend connectors undergo larger and more complex changes. When connectors update, Veeam is able to offer new and enhanced features for customers.

Veeam Backup *for Microsoft 365* v6 introduced two major features; backup copy to low-cost object storage and web-based self-service restore portal. The backup copy to low-cost object storage allows customers to tier off older backup chains to an archival storage so they can save money on long term backups. This also allows customers to meet compliance for additional copies of data. Web-based self-service restore portal offers two restore options: self-service restore and restore operator. Self-service allows all users to restore their own data by logging into the portal with their Microsoft sign on. The restore operator role allows delegation rights to be assigned to users to perform restore operations for other users or shared resources.

Every major release of Veeam Backup *for Microsoft 365* offers new features at no additional cost to the customer. Along with major releases, there are patches released in-between that are just as critical to the function of the product. As mentioned above, Microsoft patches the frontend continually, but they also deprecate or modify the connectors that many products use to connect with the Microsoft 365 data. When this happens products will release patches to keep functionality available for customers.

## Prepare for the update

Before starting the update process, there are some steps that ensure there are as few issues as possible. Before starting these steps it's important to keep in mind that every environment is different and may have additional concerns to address. An example of this is if your company received a custom patch through support. The patch could be in the product, or the patch may need to be modified for the current version. To mitigate repeating past mishaps, take the following steps and incorporate them into your internal process documentations then modify as needed.

1. When updating the product, there will be a gap in backups and restores while the update is in progress. Sending out a communication and creating a maintenance window will mitigate end user confrontation. The time it will take to update will vary depending on the size of the jet database on the server.
   If the repository is a block storage type, then the jet database is the size of the repository. If the repository is an object storage type, then the jet database only contains cache and is about one percent of the size of the data on object storage. To estimate the time it will take the server to update, take the size of the jet database per terabyte times 30 minutes.

2. If you are manually downloading the patch or update from the website instead of using the update feature in the console, make sure to check that the files' MD5 or SHA1 hash matches the download page. If a package is downloaded and needs extracted from a zip file then make sure the file has been unblocked, learn more (here).

3. Check that the server still meets (System requirements).

4. Check to see if there are any new permissions required for the update in the (Permission change log).

5. In order to backup Microsoft Teams, Microsoft requires customers to request access to the Microsoft Teams API, (read more here).

6. If you have worked with Veeam support on any special private fixes and you are not sure if it's included into the patch, (open ticket with support for confirmation).

7. It is not possible to update from a beta version of the product to a generally available version. The beta and all components must be uninstalled and a fresh installation performed.

This is a list of the top issues a that customer might run into if not properly vetted. However, for the full list of update information be sure to always read the release notes. The release notes for all versions of the product can be found in this (Knowledge Base article). Along with a list of known limitations, the release notes will advise what versions are compatible for the update.

## The upgrade

Once the pre checks are done and the maintenance window has started its time to upgrade. This process has a couple of steps and post checks to ensure everything is working as intended. This may include checking restoration for the compliance officer or updating internal documentation. The update process will vary depending on if you are updating to a whole new version or just applying a minor update.

Minor update:

1. To check if there are any updates use the drop-down menu in the upper left-hand corner and select Upgrade. The window will pop up and display when the server was last updated and last checked for new updates.
2. Selecting next will display when updates are currently available. Select install to start the update process. Follow the steps in the wizard to apply the latest update. Keep in mind that to start the update there can be no backup or restore jobs running.
   a. If the server is up to date, simply select finish.

Version update:

1. Once the pre-check sheet has been checked download the latest version of the Veeam Backup *for Microsoft 365* from the [download page]. Veeam login will be required to download the product.
2. After ISO has been downloaded, and the hash has been checked, it's time to install the software. Execute the ISO and run the Veeam.Setup.exe and select update to start the Installation wizard. At this time all backup and restore jobs need to be stopped and the console closed.
3. The installation wizard will have several options for various situations. For basic install or update select the first option, Veeam Backup *for Microsoft 365*. This wizard will update the console on the server as well as all restoration wizards.
4. The install will take some time depending on how large the jet database is on the server. Reference the 'prepare' section above for more on estimating install time. Afterwards, completely reboot the server.
5. Next some components will need to be updated.
   a. Proxies will be the first component to update since the proxies are the connection points to the repositories. To [update proxies] head to the Backup Infrastructure view on the lower left hand side and select Backup Proxies from the Inventory Pane. Right-click on each proxy and select Upgrade… when upgrading the proxy the credentials for the proxy will need to be provided.
   b. After completing the proxies head to [Backup Repositories] in the Inventory pane. Right-click on each repository and select 'Upgrade…'.
   c. If the backup server was a version behind prior to updating it might be necessary to update the [jobs]. To update the jobs select the Organizations view on the lower left side of the console. Right click on each job and select 'Upgrade…'.

6. Lastly, verify the [organization settings] and test authentication. Navigate to the Organizations view and right-click on the organization in the Inventory Pane under Organizations then select 'Edit Organization…'. run through this wizard to verify at the end the organization connections are green.
   a. It is recommended, going forward, to only use modern authentication because basic authentication APIs are set to be deprecated with Microsoft. Bonus, if modern authentication is selected with no legacy APIs the wizard can automatically deploy the authentication enterprise application in Azure. Some limitations on modern authentications exist at this time, read more [here].

After the update has completed and you have verified the organization it's time to run the jobs. Monitor the job runs for a few cycles to ensure they run as expected. Lastly, test the restore processes for each of the [restore explorers] to make sure the data restores as expected.

## Troubleshooting

No matter how you prepare for an upgrade there is always the possibility something goes wrong. Every environment is different, making it impossible to plan or test every configuration. Here are a couple of helpful check points to start with:

1. Sometimes we overlook some of the basics when we dive down the path of trying to troubleshoot an issue. I would venture to say many of us are guilty of this. With this in mind, our top cases in support for update issues often involve the space running out on the server and whether or not an update has worked after a reboot. So, our first step is double checking the basics; reboot the server and make sure there is plenty of drive space.
2. If updating to a major version, try confirming the server is on the [latest patch though the main menu].
3. Double check the hash on the downloaded ISO matches the hash on the download page. Try right clicking on the ISO and running as administrator to rule out some of the credential permission issues.
4. Do a quick search on the [forums] with over 70,000 members or this [custom search engine] which is updated and maintained regularly, more info [here]. Many support members with uncommon issues or errors look them up with a quick search in this engine to see if there is already a solution. This engine searches across the top Veeam communities and resources.

When an unforeseen issue happens to a group of customers Veeam will release a knowledge base article or a patch to assist with or correct the issue. Here are the top articles — at the time of this blog — that are recommended to customers:

1. First one is "Upgrade to Veeam Backup *for Microsoft 365* 6.0 Fails Due to Invalid Rest Service Certificate" which is [KB4295]. The surface error message is generic in this case, advising you to check logs for details, but the knowledge base article walks you through where to find the log. The message should be one of the last things written in the log and match the time the update was attempted.
2. Next is a patch that resolves various issues including three upgrade scenarios. Check out patch P20220413 in [KB4285] to see if any of these scenarios relate and then apply the patch.

If these points have been checked and you are still having issues, then it might be time to open a support case. Here is what you will need:

1. Before calling into support you will need to provide a [**support case**] number.
2. To open a support ticket you will need the specific version and build of components on the server as well as the version you are attempting update to. On the main menu in the upper left corner, under Help and Support, select about, this will show the build number.
3. Any error message or behavior experienced while trying to update the server.
4. If any custom patches or settings were applied from support that are in your record, add this to the ticket.
5. If any steps mentioned above were done, then add that to the ticket and feel free to post a link to this blog for reference. Details help support members more accurately handle tickets and get resolutions faster.
6. Collecting [**logs**] from the server will be required on the case. When collecting logs, select all components and use the default option to collect logs for the last seven days. There are two levels of logs on the standard and [**extended logging**]. Standard logging is the default setting because it takes up less space, but support might request that you enable extended logging and replicate the issue for a more detailed account the issue. If the issue is quick to replicate then it is recommended to enable extended logs, replicate the issue and export just as stated before. These logs will be sufficient for most cases, but additional logging and information might be requested.
7. If you started a forums post or found the same issue in another forums post but are unsure how to proceed, update that in the ticket with a link to the post.
8. Note if any additional contacts, phone numbers or email addresses need to be added to the support ticket otherwise the contact information on the account will be used.

Pro tip, there is no harm putting this same information into a post on our [**forums**] to get more resources on the case. Disclaimer: logs can contain information about the infrastructure in an environment so consider scrubbing any data when posting log snips. Veeam has a strong technical community who can provide tips and advice. A portion of our development and other resources, like our Veeam Vanguards and Legends, spend time here (look for the green users). If you do post on the forums, it is good manners to add your case number so future customers can get help on similar issues.

## Conclusion

Upgrading is not everyone's favorite thing to do but with some preparation it can be a less painful process and, in the end, leave you with a more secure environment. On top of being more secure most versions provide access to features and components that make your job easier. If something does go amiss, then you can always reach out to our support team or forums community for help. Once the update process has completed, go update any internal documentation with any of the lessons you learned and the current version. This will make the process smoother for you and others in the future. For more information on updating the server or steps going forward check out some of the informational links below.

For additional resources check out the following:

- Product web page
- User guides
- Veeam R&D Forums
- Veeam Custom Google Search Engine
- Best Practice Guide
- On-Demand Training

## About the Author

Karinne Bessette is a Technologist at Veeam on the product strategy team. A strong technical background in network and security, well-versed in Microsoft 365 and Azure platforms. Credentials include Cisco Security (CCNA) and Cisco Routing & Switching (CCNA), CompTIANetwork+, Security, CompTIA A, Project +, and Linux Professional Institutes Essentials, Microsoft AZ-900 and AZ-103, Veeam VMCE2019 and VMCE2020, and VMware vExpert2020. Follow Karinne on Twitter @RinBytes or @Veeam.