

VMC Cloud Audit for January-March 2020

March 4th, 2020

Overview & Executive Summary

I performed a cloud audit for several of the Visit Mendocino County's cloud based information systems, looking at the security settings for each account as well as looking through the audit logs for suspicious or unusual activity. I audited the following systems: Dropbox, GSuite, and LastPass.

Issues Discovered









No major problems were discovered, but a few things require additional attention:

1. **Dropbox:** ONLY FIVE (5) OF THE ACTIVE EIGHT (8) DROPBOX FOR BUSINESS USERS HAVE TWO FACTOR AUTHENTICATION (2FA) TURNED ON FOR THEIR ACCOUNTS. VMC SHOULD TRY TO GET 100% OF USERS TO ENABLE 2FA. THE MISSING THREE: DAPHNE HANEY, KATHY JANES, MCTC OFFICE ACCOUNT.
2. **Google:** CURRENTLY FOUR (4) USERS, TRAVIS, RAMON, KATRINA, EMILY, AND TOM, ARE USING TWO-STEP VERIFICATION FOR G SUITE. VMC SHOULD TURN ON TWO-FACTOR AUTHENTICATION FOR ALL REMAINING ACTIVE G SUITE ACCOUNTS.
3. **Google:** RICHARD STROM STILL HAS AN ACTIVE G SUITE ACCOUNT WITH THE ORGANIZATION (richard@visitmendocino.com) IF THIS IS NOT BEING USED, IT SHOULD BE DEACTIVATED.
4. **Dropbox:** A NUMBER OF EVENTS, MOSTLY AROUND SHARING FILES WITH MEMBERS OUTSIDE OF THE ORGANIZATION, WERE DISCOVERED IN THE LOG FILES AND REQUIRE FURTHER ATTENTION.

Dropbox Audit

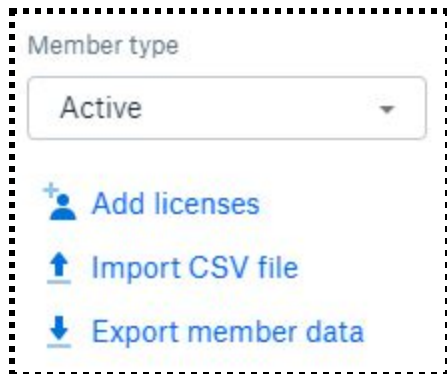
Review of Active Accounts and 2FA

There are no unexpected member accounts in Visit Mendocino County's Dropbox for Business account. Five out of eight members have two-step verification enabled, an increase of three users from the previous cloud audit! As of 3/4/20, Travis, Ramon, Emily, Katrina, and Tom have two-step verification turned on.

Name	Status	Usage	Two-step verification
 Ramon Jimenez ramon@visitmendocino.com	Team admin	9.06 GB	• Enabled
 Tom Jacobson tom@visitmendocino.com	Team admin	2 MB	• Enabled
 Travis Scott travis@visitmendocino.com	Team admin	45.22 GB	• Enabled
 Daphne Haney acct@visitmendocino.com	Member	1.61 MB	• Optional
 Emily Saengarun emily@visitmendocino.com	Member	787.18 MB	• Enabled
 Kathy Janes kathy@visitmendocino.com	Member	71.21 MB	• Optional
 katrina kessen katrina@visitmendocino.com	Member	7.49 GB	• Enabled
 MCTC Office office@visitmendocino.com	Member	21.01 GB	• Optional

Export Dropbox Member Data

From the Members tab, choose Export member data link. This will create a report in a folder in VMC's Dropbox. Travis will receive an email once the report is ready.



Member type

Active

+ Add licenses

↑ Import CSV file

↓ Export member data

Member Data Report 03/04/19

First name	Last name	Role	Status	Usage (MB)	2FA
Ramon	Jimenez	Team admin	Active	9,275.14	Enabled
Tom	Jacobson	Team admin	Active	2	Enabled
Travis	Scott	Team admin	Active	46,306.18	Enabled
Emily	Saengarun	Member	Active	787.18	Enabled
Katrina	Kessen	Member	Active	7,665.14	Enabled
Daphne	Haney	Member	Active	1.61	Optional
Kathy	Janes	Member	Active	71.21	Optional
MCTC	Office	Member	Active	21,515.43	Optional

In addition, there are three additional accounts not listed here: Richard Strom, Alison DeGrassi, and Donna Hannaford. Alison's and Richard's accounts have both been deleted with all contents transferred to Travis. Donna's account was disconnected as of 8/8/2016. VMC should check with Dropbox to make sure they are not being charged for the two (2) unused licenses.

Check Space Remaining

Make sure that Visit Mendocino County is not running out of space.

VMC Dropbox Storage Space 03/04/202: Using 85.06 GB of 3 TB

Team overview

Members ⓘ	Space used	Renewal date
8 View members	85.1 GB / 5 TB Request space	Apr 20, 2020

There is currently no problem with the amount of storage.

App Integrations

Visit Mendocino County has over 20 different 3rd party apps that have access to the organization's Dropbox account. These will need to be reviewed by VMC's management as this is beyond the scope of this cloud audit. However, any apps that are not used frequently by the organization should be disconnected as any 3rd party access presents a potential security risk. The complete list of apps can be reviewed here:

https://www.dropbox.com/team/admin/settings/app_actions

Check Notification Settings

Under the Notifications tab, make sure that all notifications are turned on like this:

General Security **Notifications** Connected apps

Alerts

Email me when:

- I delete a large number of files
- A new browser is used to sign in
- A new device is linked
- A new app is connected

Files

Email me about:

- Activity in shared folders (weekly digest)

News

Email me about:

- New features and updates
- Tips for Dropbox Business
- Tips on using Dropbox Paper
- Dropbox feedback surveys

As of **03/04/2020** all notifications are set correctly.

Review Alternative Signon Methods

Under Settings, Single Signon, make sure that the option to sign in using Google credentials is turned OFF. **As of 03/04/2020 this setting was correct.**

Alternative sign-in options

Google sign-in


Members can sign in with either their Google or Dropbox account credentials. Google and Dropbox email addresses must match for sign-in to work


On Off


Trusted Teams

Under settings, make sure there are no trusted teams. A trusted team is a way for an external attacker to gain access to all aspects of Dropbox, and as of **03/04/2020** there were no trusted teams added.

Account

 **Team profile**
Change your team name, choose your language, add a logo, and more

 **Trusted teams**
Join forces with admins on other Dropbox teams to coordinate settings and security

 **Early access**
Test the latest features and give feedback to the Dropbox team

Review Membership Approval

Make sure both settings here are off. New members can only be added to VMC's Dropbox explicitly by an Admin account. **As of 03/04/2020 these settings were correct.**

Settings > Membership approval

Coworkers can find the team
Allow coworkers to be able to find the team when not invited. On Off

Team members can suggest to invite other coworkers
Allow coworkers to send you suggestions for people to invite. On Off

Review Dropbox Activity Report

Run an **activity report** for the last quarter and download it. Make sure that all days since the last report was run are included. Run the report from the Activity tab. The report will show up in the Dropbox Business reports folder, accessible to any Dropbox Admin account.

Look through the report for entries where the name and/or email do not match a known VMC account. These are most often created when someone accesses a folder or file through Dropbox.

Here are some events to review:

12/12/2019 16:15	amy zhou	Downloaded file/folder from shared link
12/12/2019 16:15	amy zhou	Opened shared link
2/6/2020 12:08	Anderson Valley Winegrowers Assn.	Added users and/or groups to shared file/folder
2/6/2020 12:08	Anderson Valley Winegrowers Assn.	Invited user to Dropbox and added them to shared file/folder
12/26/2019 11:36	Brendan McGuigan	Downloaded file/folder from shared link
12/26/2019 11:36	Brendan McGuigan	Opened shared link
12/26/2019 11:32	Brendan McGuigan	Opened shared link
12/26/2019 11:31	Brendan McGuigan	Downloaded file/folder from shared link
12/26/2019 11:31	Brendan McGuigan	Opened shared link
12/26/2019 11:28	Brendan McGuigan	Opened shared link

12/19/2019 14:25	Brendan McGuigan	Downloaded file/folder from shared link
12/19/2019 14:24	Brendan McGuigan	Opened shared link
1/24/2020 14:18	Brianna Sainez	Requested access to shared file/folder
1/24/2020 14:17	Brianna Sainez	Added shared folder to own Dropbox
1/24/2020 14:16	Brianna Sainez	Acquired membership of shared file/folder by accepting invite
2/26/2020 14:46	Cally Dym	Previewed shared file/folder
2/26/2020 14:46	Cally Dym	Acquired membership of shared file/folder by accepting invite
12/3/2019 16:57	Carrie Bell	Acquired membership of shared file/folder by accepting invite
12/5/2019 9:21	Jancine Tremblay	Opened shared link
2/6/2020 13:18	Joe Webb	Added shared folder to own Dropbox
2/6/2020 13:18	Joe Webb	Acquired membership of shared file/folder by accepting invite
12/15/2019 7:15	Judith Shamir	Added file/folder to Dropbox from shared link
2/24/2020 8:58	Juris SteprÄns	Acquired membership of shared file/folder by accepting invite
2/13/2020 11:38	Mendocino WineGrowers	Added users and/or groups to shared file/folder
2/12/2020 10:30	Rene Poyant	Acquired membership of shared file/folder by accepting invite

12/4/2019 15:39	Rich Melvin	Opened shared link
3/2/2020 12:25	richard strom	Deleted all files from unlinked device
2/8/2020 16:24	Sarah Wuethrich	Added shared folder to own Dropbox
2/8/2020 16:24	Sarah Wuethrich	Acquired membership of shared file/folder by accepting invite
12/10/2019 13:28	Scott Connolly	Previewed shared file/folder
12/10/2019 13:23	Scott Connolly	Requested access to shared file/folder
2/11/2020 14:01	Slack	Created shared link
1/22/2020 12:18	teresa raffo	Invited user to Dropbox and added them to shared file/folder
2/7/2020 18:10	Trevor Sweaza	Added users and/or groups to shared file/folder
2/7/2020 18:07	Trevor Sweaza	Added users and/or groups to shared file/folder

GSuite Audit

Review Two-Step Verification

Google allows GSuite Admins to enforce Two-step verification (also known as two-factor authentication) for users. Visit Mendocino County does not currently require all users to use two-step verification. As of **03/04/2020** four users are using two-step verification: Travis, Ramon, Emily, and Tom. Visit Mendocino County should seriously consider enforcing two-step verification for all users.

Review Admin Audit Log

A review of the GSuite Admin log file shows that the alison@visitmendocino.com account had some major changes, all of which were expected. Travis suspended the account, removed it as a Super Admin user, changed the password, and changed all of the recovery information (secondary email, mobile phone number) to prevent the previous account owner from re-accessing the account. In addition, the Super Admin role was assigned to two different accounts: Ramon@visitmendocino.com and jennifer@visitmendocino.com. **All other events in the Admin Audit log were as expected.**

LastPass Audit

From an Admin account (Travis, Tom, Joh, Ramon) download the LastPass audit trail for the previous three months. Do this by going to the Admin Console: Reports: *** (menu item at top right): Export Report. Make sure to select the date range first!

Check for Suspicious Events

The main thing to look for are suspicious events in the LastPass audit trail. These are:

- New users added
- Old users removed
- Export of vault contents
- Accounts shared with people external to the organization
- Two-Factor Authentication (2FA) added / removed

As of **03/04/2020**, for the period from 12/01/19 to 03/04/20 there were no events of the above types. **All logged activities looked normal and expected.**

Check for Employee Usage

One red flag is if employees are not using LastPass. If an employee of Visit Mendocino County has a LastPass account but is not using it to log into accounts, that means they are using some other way of accessing those accounts - by using personal passwords (not unique / randomized passwords) or relying on a browser or some other program other than LastPass Teams to remember passwords.

All employees are using LastPass on a daily and weekly basis to access sites. Kathy Janes has been logging in to LastPass on a more regular basis, which is a big improvement from last quarter. Ramon has been helping her use and understand LastPass, which is very helpful. Additional attention should be paid to her LastPass usage to make sure she is actually logging in to any sites she needs access to. John Kuhry, a retired board member of Visit Mendocino County who has Administrative access to LastPass, has also not logged in at all during that time period. Visit Mendocino plans to transition John's LastPass account to current board member Cally Dym.