

Cloud app security

Does the Coro Security Platform offer Multi-Factor Authentication (MFA)?

Yes, you can **enable MFA** from the console. In addition, all individually supported cloud applications support MFA.

Can Coro control accessibility to Microsoft Sharepoint using IP restrictions?

Yes, Coro can control accessibility to Microsoft Sharepoint using Microsoft 365 **Access Permissions**.

For more information, see **Setting Permissions for your cloud applications**.

Why does the Activity Log of a Malware in Cloud Drive ticket indicate that remediation of a suspected malicious file failed?

A failed remediation activity within a **Malware in Cloud Drive** ticket indicates that the file was remediated by the native cloud application.

The screenshot displays the Coro Security Platform interface. On the left, a ticket list shows one ticket titled "Malware in Cloud Drive" with a cloud icon and a green checkmark, dated "Oct, 25 2023, 9:17 AM". The main panel shows the details for ticket ZY07-384, which is "Closed on Oct, 25 2023, 9:24 AM". The "Activity Log" section contains the following entries:

- Failed: Deleting file eicar_com.zip of user [redacted] in Google Workspace has been denied by the service** (Wed, Oct 25, 9:24 AM by [redacted]). This entry is highlighted with a pink box.
- Ticket ZY07-384 has been logged and referenced for audit reports (Wed, Oct 25, 9:24 AM by [redacted]).
- Ticket ZY07-384 (Malware in Cloud Drive) has been closed (Wed, Oct 25, 9:24 AM by [redacted]).
- Failed: Moving file eicar_com.zip of user [redacted] in Google Workspace to Suspected folder has been denied by the service** (Wed, Oct 25, 9:24 AM by [redacted]). This entry is also highlighted with a pink box.

An "UNDO" button is visible next to the "closed" entry.

For more information, see **Malware detection in cloud drives**.