Setting Permissions for your cloud applications

For Coro to monitor and report security issues, at least one cloud application must be connected.



Coro supports the ability to set access permissions for connected cloud applications. In other words, you can allow access to an application based on whether a user meets a defined set of criteria.

To configure access permissions for a service:

1. Log into the Coro console and go to Control Panel > Cloud Security.

2. From your list of connected cloud application, select the corresponding Access Permissions button:

0		ম	٥	000	\sim	٢	TS
< Control F	anel						
	Security and control access to cloud applications and data						
0	Microsoft 365 Connected			ACCES	S PERMIS	SIONS	
G	Google Workspace Connected			ACCES	S PERMIS	SIONS	
₩	Dropbox Connected			ACCES	S PERMIS	SIONS	

3. On the Access Permissions page for your application, select + NEW PERMISSIONS to add a new permission rule:

0				ম	٥	°		0	TS		
« Control Panel 🦳 « Cloud Applica	ations										
S Microsoft 365 Access Permissions							+ NEW PERMISSIONS				
Allow access to Microsoft 365	from specific countries/IP addresses										
Groups	Allowed Countries / IPs	Description	Au	Automatic Remediation							
Demo Coronet	United States		No	ne					:		