

Office 365 Integration [SOAR Support]

PLATFORM FEATURE UPDATE

Adlumin's Office 365 integration now has built-in support for the platform's **Security Orchestration Automation and Response (SOAR)**. This configuration will automatically disable an account when an analytic algorithm determines there is an extremely high likelihood of a compromise across Office 365/Azure services. For example, a successful access event from a foreign country or impossible travel. For this feature to operate nominally you must have Adlumin clients deployed to your domain controllers and be using the Office 365/Azure API integration.

To learn more about enabling Adlumin SOAR support for Office 365, navigate to *Devices > Network Security > Office 365 > Azure API Credentials* within the platform.

The screenshot shows the 'Office 365 data' configuration page in the Adlumin interface. The page is titled 'Office 365 data' and includes a navigation menu with options like Log Management, Account Analysis, Custom Detections, Detection Exclusions, Documentation, and Azure API Configuration. The 'Azure API Credentials' section is active, showing instructions on how to enter credentials and a note that SOAR functionality requires a Microsoft 365 E5 subscription. There are two toggle switches for 'API Credential Capabilities': 'Logging' and 'SOAR', both of which are currently turned 'On'. Below these are input fields for 'Client ID', 'Client Secret', 'Tenant ID', and 'Domain Name'. At the bottom of the configuration section, there are 'Disable' and 'Add' buttons. Below the configuration section is a table titled 'Active Domains' with columns for Domain Name, Client ID, Tenant ID, Secret, Logging, SOAR, and Delete. The table contains one entry for 'adlumin.com'.

Domain Name	Client ID	Tenant ID	Secret	Logging	SOAR	Delete
adlumin.com	f8e17304-8d63-403f-97cf-7a1425c50965	3f421e5b-4341-4aed-9229-b47245693b53	*****	✓	✓	🗑️