Filename: microsoft-ms101-5-4-1-configure-connected-apps
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Cloud App Security (CAS)
EpisodeName: Configure Connected Apps
Description: Adam and Wes discuss what steps need to be taken to configure connected apps successfully.

Configure Connected Apps

Implement Microsoft 365 Security and Threat Management (30-35%)

Implement Cloud App Security (CAS)
• Configure Cloud App Security (CAS)
• Configure Cloud App Security (CAS) Policies
• Configure Connected Apps
• Design Cloud App Security (CAS) Solution
• Manage Cloud App Security (CAS) Alerts
• Upload Cloud App Security (CAS) Traffic Logs

==========

Configure Connected Apps

App connectors use the APIs of app providers to enable greater visibility and control by Microsoft Cloud App Security over the apps you connect to.

Each service has its own framework and API limitations such as throttling, API limits, dynamic time-shifting API windows, and others.

Multi-instance support:

Cloud App Security supports multiple instances of the same connected app. For example, if you have more than one instance of Salesforce (one for sales, one for marketing) you can connect both to Cloud App Security. You can manage the different instances from the same console to create granular policies and deeper investigation. This support applies only to API connected apps, not to Cloud Discovered apps or Proxy connected apps.

NOTE: Multi-instance is not supported for Office 365 and Azure.

Prerequisites:

```
• For some apps, it may be necessary to white list IP addresses to enable
```

Cloud App Security to collect logs and provide access for the Cloud App Security console.

```
• For each app that you want to connect with the Cloud App Security API
```

integration, Microsoft recommends creating an admin service account dedicated to Cloud App Security.

NOTE: ExpressRoute - Cloud App Security is deployed in Azure and fully integrated with ExpressRoute. All interactions with the Cloud App Security apps and traffic sent to Cloud App Security, including upload of discovery logs, is routed via ExpressRoute public peering for improved latency, performance, and security. There are no configuration steps required from the customer side.

How it works:
https://docs.microsoft.com/en-us/cloud-app-security/enable-instant-visibility-protection-and-governance-actions-for-your-apps