Filename: microsoft-ms101-5-1-1-cloud-app-security-overview
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Cloud App Security (CAS)
EpisodeName: Cloud App Security Overview
Description: Adam and Wes overview what the Microsoft Cloud App Security solution is.

Cloud App Security Overview

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

==========

Cloud App Security Overview

Microsoft Cloud App Security is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

What are the differences between Microsoft Cloud App Security and Office 365 Cloud App Security?

Microsoft Cloud App Security - a comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.

Office 365 Cloud App Security - a subset of Microsoft Cloud App Security that provides enhanced visibility and control for Office 365. Office 365 Cloud App Security includes threat detection based on user activity logs, discovery of Shadow IT for apps that have similar functionality to Office 365 offerings, and control app permissions to Office 365.

https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365

What are the differences in discovery capabilities for Azure Active Directory and Microsoft Cloud App Security?

Azure Active Directory Premium P1 includes Azure Active Directory Cloud App Discovery at no additional cost. This feature is based on the Microsoft Cloud App Security Cloud Discovery capabilities.

https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-aad

Prerequisites:

```
• Your organization must have a license to use Cloud App Security. Azure AD
```

Premium P1 for limited capabilities; EMS E5 for full capabilities.

```
• After you have a license for Cloud App Security, you will receive an email
```

with activation information and a link to the Cloud App Security portal.

```
• To set up Cloud App Security, you must be a Global Administrator or a
```

Security Administrator in Azure Active Directory or Office 365.

NOTE: It's important to understand that a user who is assigned an admin role will have the same permissions across all of the cloud apps that your organization has subscribed to. This is regardless of whether you assign the role in the Microsoft 365 admin center, or in the Azure classic portal, or by using the Azure AD module for Windows PowerShell.

```
• To run the Cloud App Security portal, use Internet Explorer 11, Microsoft
```

Edge (latest), Google Chrome (latest), Mozilla Firefox (latest), or Apple Safari (latest).

```
• For portal access, it's necessary to add the following IP addresses to your
```

Firewall's allow list to provide access for the Cloud App Security portal:
104.42.231.28

Office 365 URLs and IP address ranges:
https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

Network requirements:
https://docs.microsoft.com/en-us/cloud-app-security/network-requirements

Office 365 and Azure AD roles with access to Cloud App Security

By default, the following Office 365 and Azure Active Directory (Azure AD) admin roles have access to Cloud App Security:

```
• Global administrator and Security administrator: Admins with Full access
```

have full permissions in Cloud App Security. They can add admins, add policies
and settings, upload logs and perform governance actions.

```
• Compliance administrator: Has read-only permissions and can manage alerts.
```

Can create and modify file policies, allow file governance actions, and view
all the built-in reports under Data Management.

```
• Security reader: Has read-only permissions and can manage alerts. The
```

Security reader is restricted from doing the following actions:

```
    • Create policies or edit and change existing ones
    • Performing any governance actions
    • Uploading discovery logs
    • Banning or approving third-party apps
    • Accessing and viewing the IP address range settings page
    • Accessing and viewing any settings pages
    • Accessing and viewing the Discovery settings
    • Accessing and viewing the App connectors page
    • Accessing and viewing the Governance log
    • Accessing and viewing the Manage snapshot reports page


• Global reader: Has full read-only access to all aspects of Microsoft
```

Cloud App Security. Cannot change any settings or take any actions.