[New Deployment Method] Bicep Re-registration of Azure Environment

Purpose: Document steps and prerequisites for re-registering the Azure Production environment with CSPM

Change Request: CHG0063001

Date: 11/25/2025

Prerequisites:

1. User performing authorizing the CrowdStrike application must have Global Admin Entra ID role
2. **Azure roles for deploying resources:** Owner role at tenant root group
3. Directory tenant ID: e004fb9c-b0a4-424f-bcd0-322606d5df38
4. **Region for deploying CrowdStrike Infrastructure:** eastus2

- By default, CrowdStrike deploys log ingestion resources to the region assocaited with our CID, which is westus. However, we only deploy resources in eastus2 or Central US.

5. **Subscription ID**: 3b3c809e-79f3-4073-9d3d-bf060fd9d65e (Core Network Security Services)

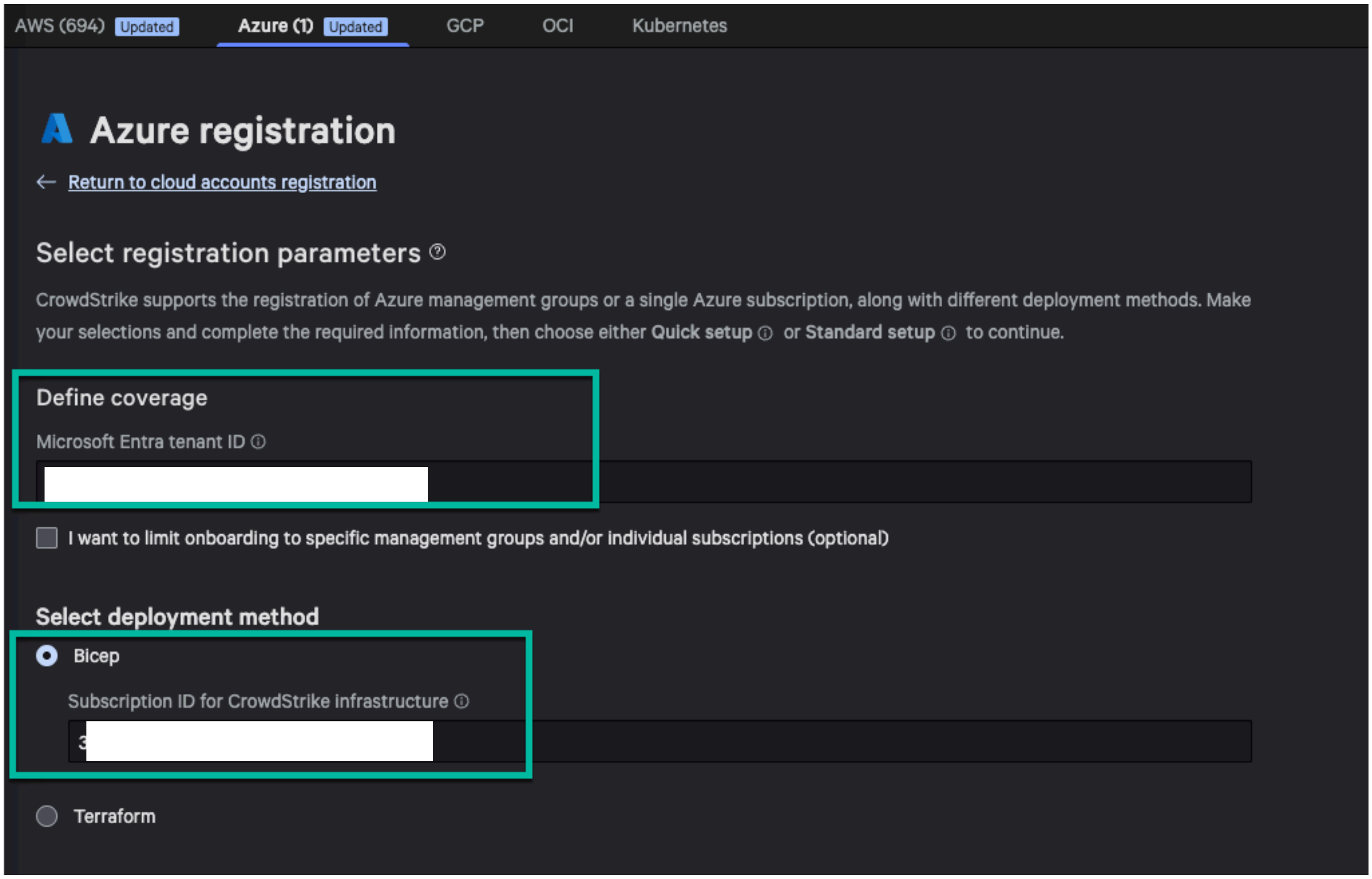
- Subscription where our resource group and log ingestion resources will live:

6. **Customer Generated API client ID**: e7a494f6d990435b946db34e47a99e25
7. **API Secret Value**: Please go to the Azure Key Vault zhe2-cloudsec-kv-prod-01 and obtain secret value.

- API key will be used for Azure Re-registration to CSPM. This API key is required if we want to enable RTVD.

Step 1: Define coverage

- Registering the Tenant Root Group will monitor all **current** and **future** subscriptions in the tenant



Azure registration

← Return to cloud accounts registration

Select registration parameters ⓘ

CrowdStrike supports the registration of Azure management groups or a single Azure subscription, along with different deployment methods. Make your selections and complete the required information, then choose either **Quick setup** ⓘ or **Standard setup** ⓘ to continue.

Define coverage

Microsoft Entra tenant ID ⓘ

[redacted]

□ I want to limit onboarding to specific management groups and/or individual subscriptions (optional)

Select deployment method

● Bicep

Subscription ID for CrowdStrike infrastructure ⓘ

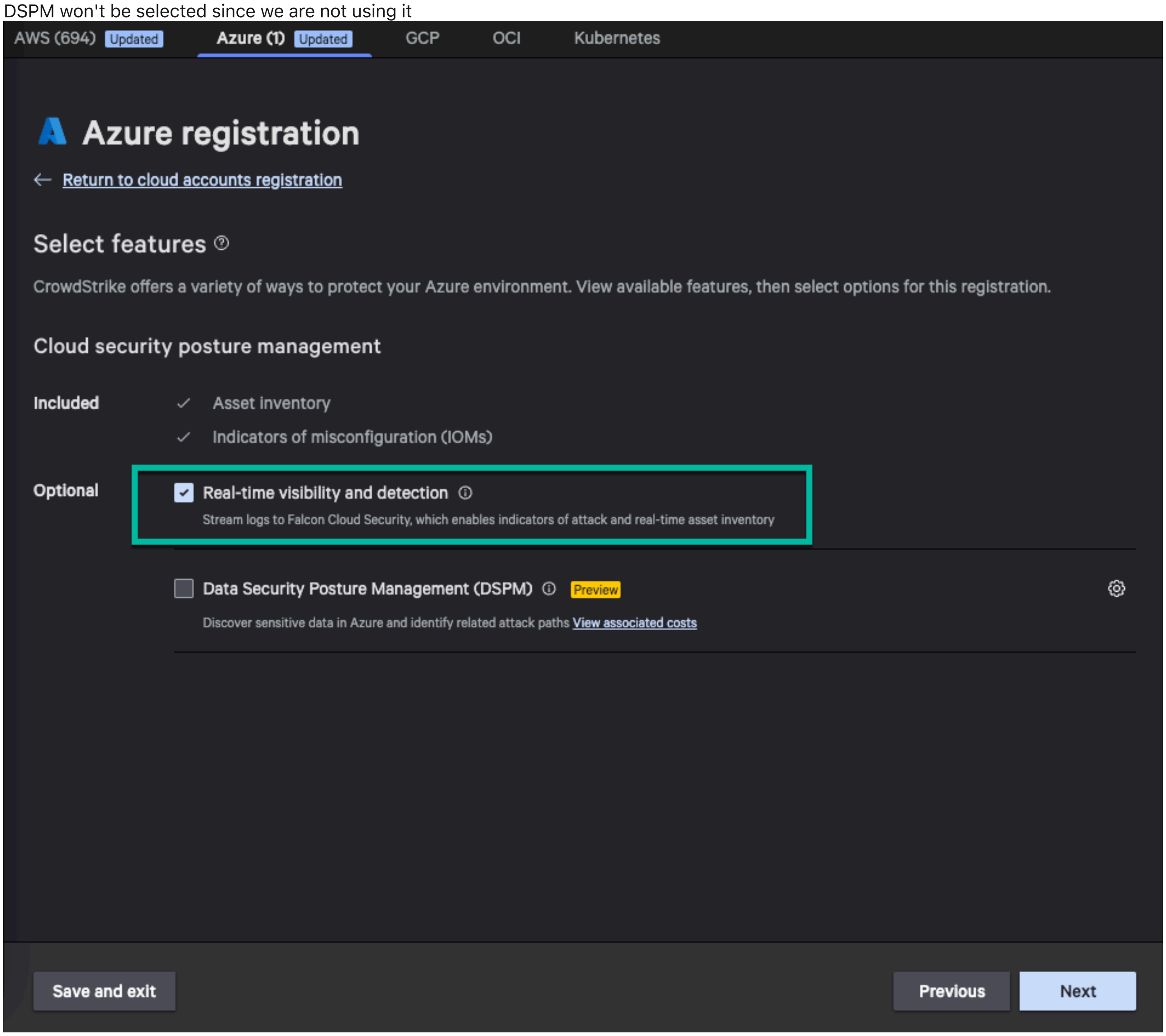
[redacted]

○ Terraform

Step 2: Select Real-time visibility and detection (RTVD)

- IOMs are enabled by default

- DSPM won't be selected since we are not using it



Azure registration

← Return to cloud accounts registration

Select features

CrowdStrike offers a variety of ways to protect your Azure environment. View available features, then select options for this registration.

Cloud security posture management

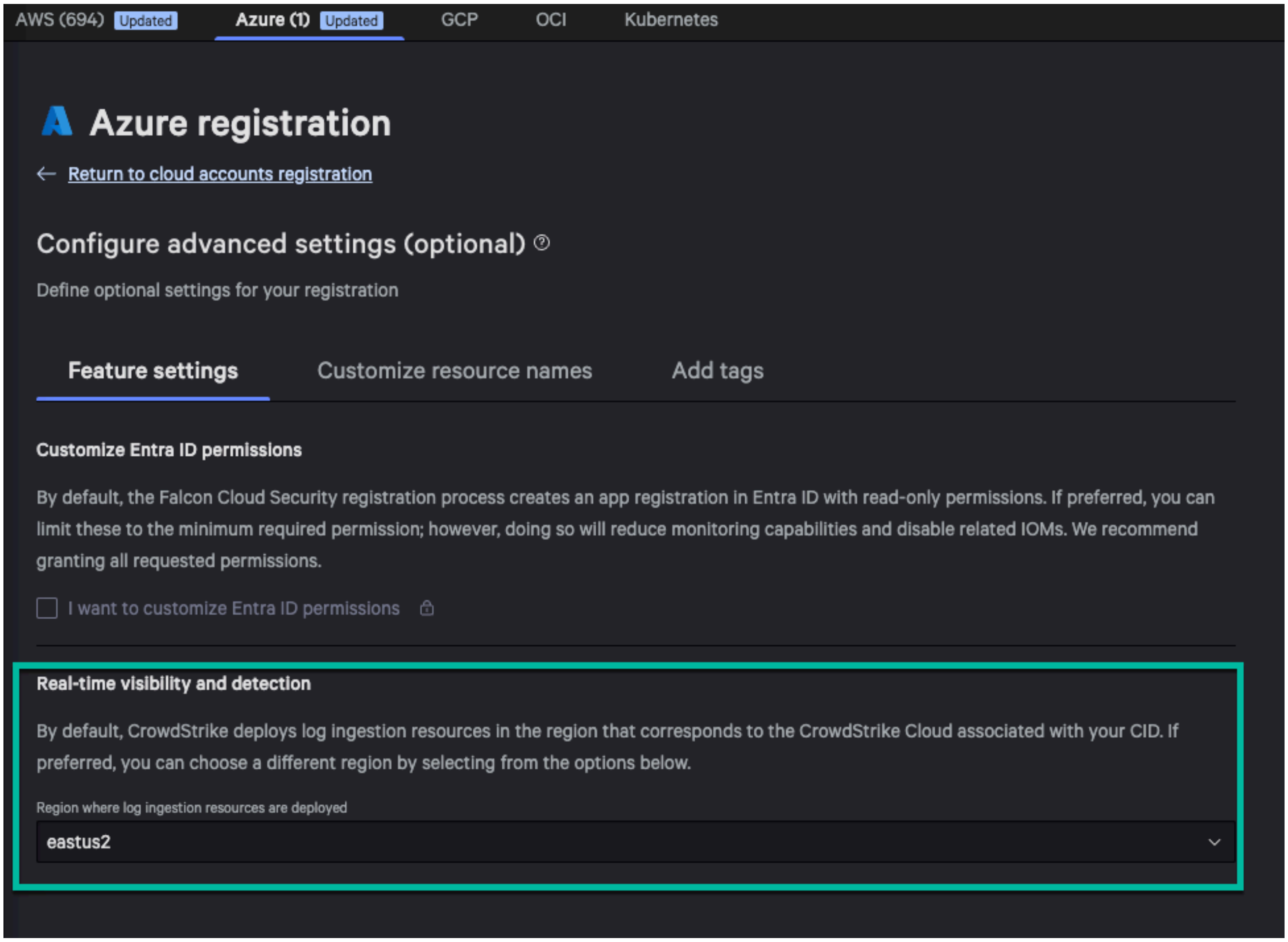
Included
✓ Asset inventory
✓ Indicators of misconfiguration (IOMs)

Optional
☑ Real-time visibility and detection
Stream logs to Falcon Cloud Security, which enables indicators of attack and real-time asset inventory

☐ Data Security Posture Management (DSPM) Preview
Discover sensitive data in Azure and identify related attack paths View associated costs

Step 3: Region selection

- By defaut, CrowdStrike deploys log ingestion resources in the region that corresponds to the CrowdStrike cloud associated with our CID. However, at Emory, we deploy our resources in eastus2, not west US, which appears to be where our default CrowdStrike cloud is located.



Azure registration

Return to cloud accounts registration

Configure advanced settings (optional)

Define optional settings for your registration

Customize Entra ID permissions

By default, the Falcon Cloud Security registration process creates an app registration in Entra ID with read-only permissions. If preferred, you can limit these to the minimum required permission; however, doing so will reduce monitoring capabilities and disable related IOMs. We recommend granting all requested permissions.

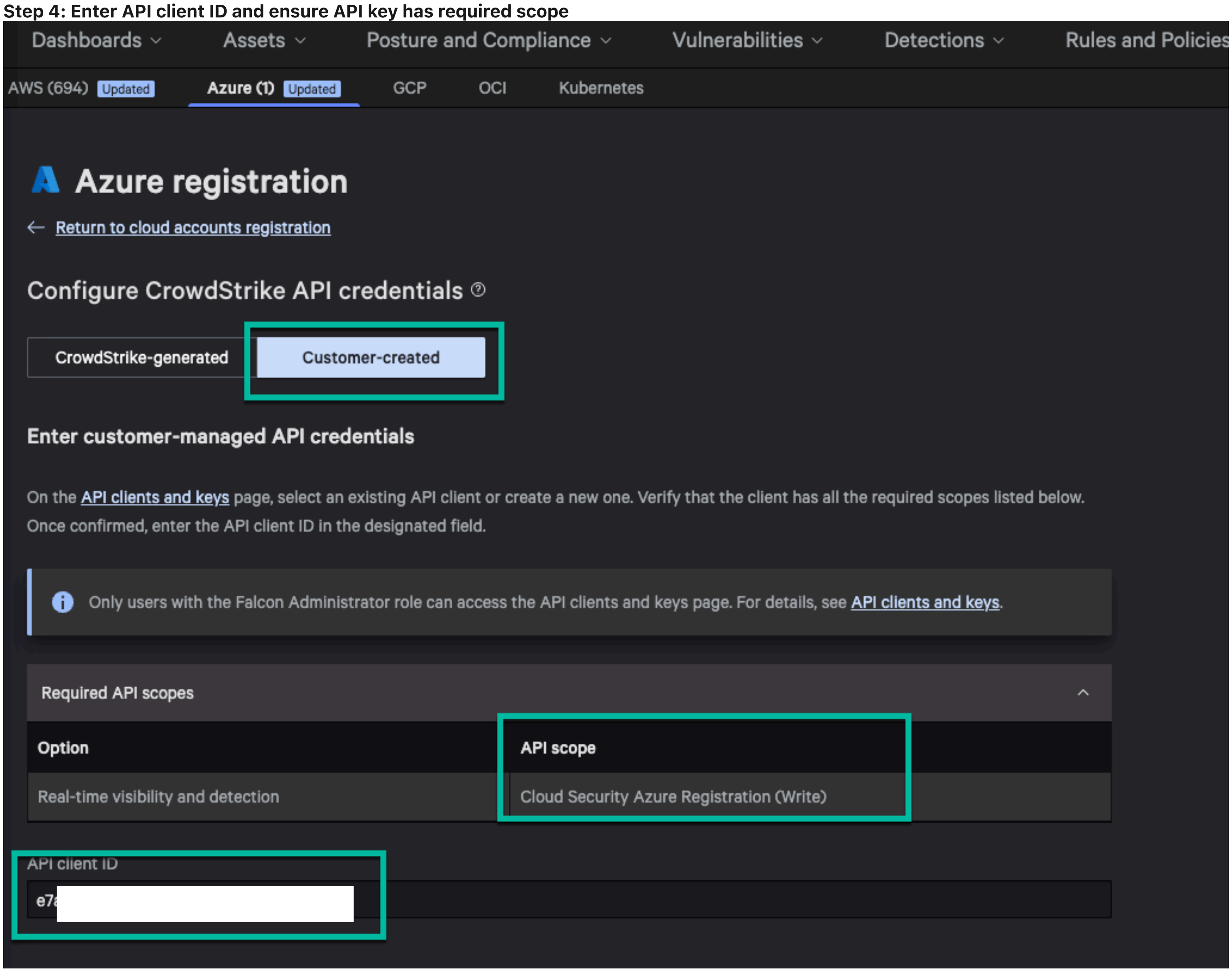
□ I want to customize Entra ID permissions

Real-time visibility and detection

By default, CrowdStrike deploys log ingestion resources in the region that corresponds to the CrowdStrike Cloud associated with your CID. If preferred, you can choose a different region by selecting from the options below.

Region where log ingestion resources are deployed: eastus2

Step 4: Enter API client ID and ensure API key has required scope



Azure registration

← Return to cloud accounts registration

Configure CrowdStrike API credentials

Enter customer-managed API credentials

On the API clients and keys page, select an existing API client or create a new one. Verify that the client has all the required scopes listed below. Once confirmed, enter the API client ID in the designated field.

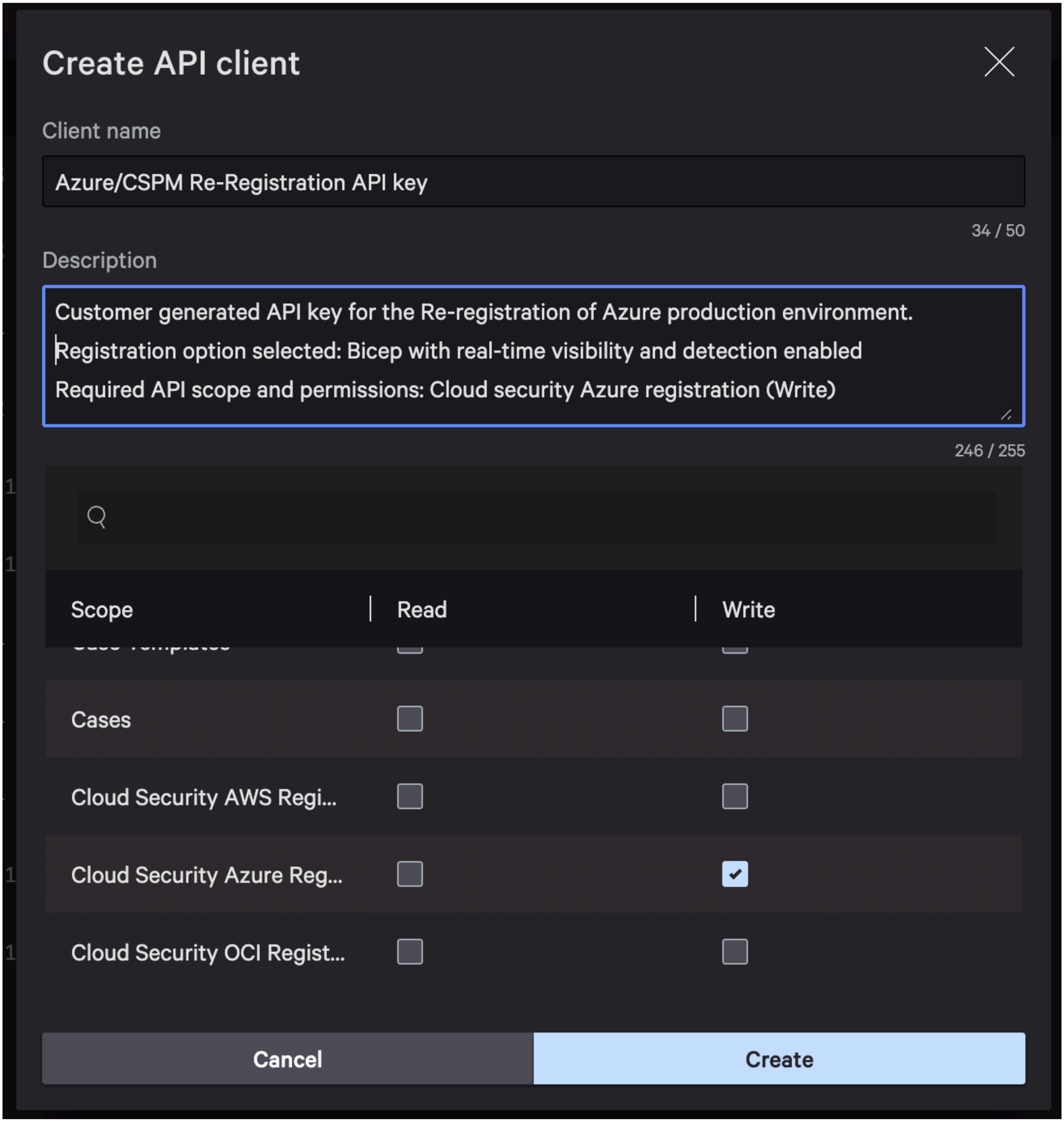
Only users with the Falcon Administrator role can access the API clients and keys page. For details, see API clients and keys.

Required API scopes

Option	API scope
Real-time visibility and detection	Cloud Security Azure Registration (Write)

API client ID: e7[redacted]

Below is screenshot from Falcon CSPM where I created the customer generated API key that has the required API scope (cloud security azure registration (write)



Create API client

Client name

Azure/CSPM Re-Registration API key

34 / 50

Description

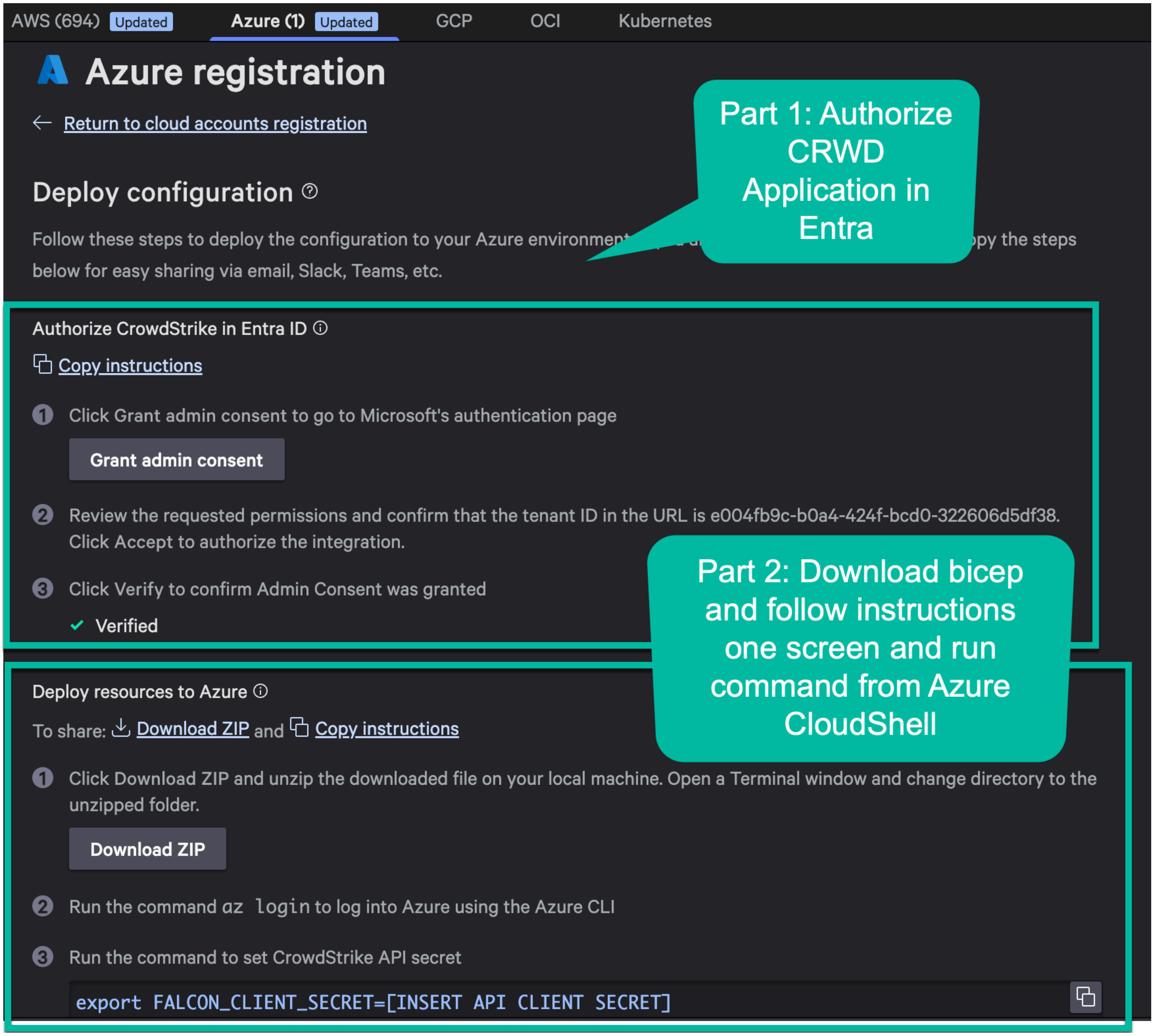
Customer generated API key for the Re-registration of Azure production environment.
Registration option selected: Bicep with real-time visibility and detection enabled
Required API scope and permissions: Cloud security Azure registration (Write)

246 / 255

Scope	Read	Write
Cases	□	□
Cloud Security AWS Regi...	□	□
Cloud Security Azure Reg...	□	☑
Cloud Security OCI Regist...	□	□

Step 5: Deploy Configuration

- **Part 1: Authorize CrowdStrike app in Entra ID by clicking grand admin consent**
- During re-registration, in the console, Security will provide instructions from console to Global admin to grant admin consent to the CrowdStrike owned application to obtain these permissions to our Entra ID tenant.



Azure registration

← Return to cloud accounts registration

Part 1: Authorize CRWD Application in Entra

Deploy configuration ?

Follow these steps to deploy the configuration to your Azure environment, … py the steps below for easy sharing via email, Slack, Teams, etc.

Authorize CrowdStrike in Entra ID ⓘ

Copy instructions

1. Click Grant admin consent to go to Microsoft's authentication page

   Grant admin consent

2. Review the requested permissions and confirm that the tenant ID in the URL is e004fb9c-b0a4-424f-bcd0-322606d5df38. Click Accept to authorize the integration.

3. Click Verify to confirm Admin Consent was granted

   ✓ Verified

Part 2: Download bicep and follow instructions one screen and run command from Azure CloudShell

Deploy resources to Azure ⓘ

To share: Download ZIP and Copy instructions

1. Click Download ZIP and unzip the downloaded file on your local machine. Open a Terminal window and change directory to the unzipped folder.

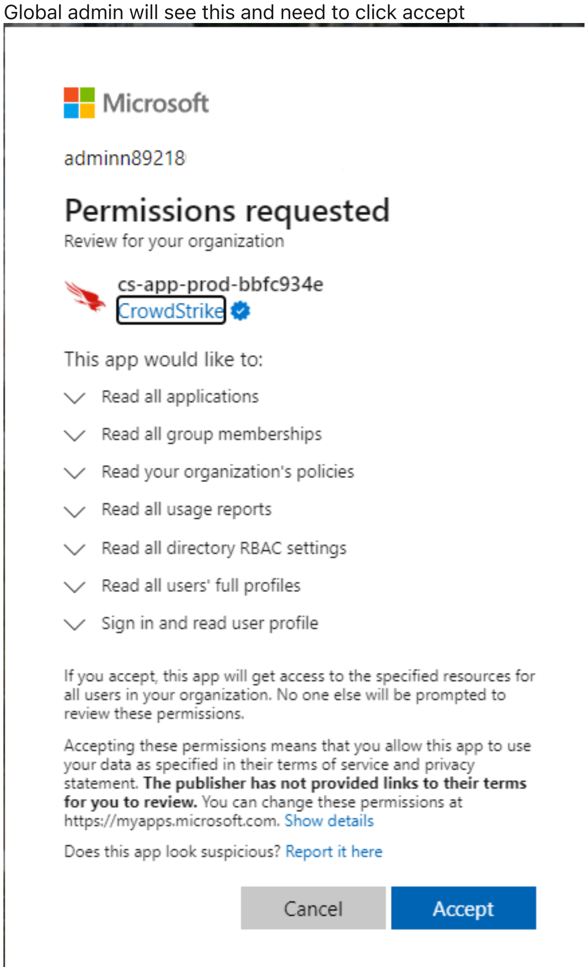
   Download ZIP

2. Run the command `az login` to log into Azure using the Azure CLI

3. Run the command to set CrowdStrike API secret

```
export FALCON_CLIENT_SECRET=[INSERT API CLIENT SECRET]
```

Global admin will see this and need to click accept



Microsoft

adminn89218

Permissions requested

Review for your organization

cs-app-prod-bbfc934e

CrowdStrike

This app would like to:

- Read all applications
- Read all group memberships
- Read your organization's policies
- Read all usage reports
- Read all directory RBAC settings
- Read all users' full profiles
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

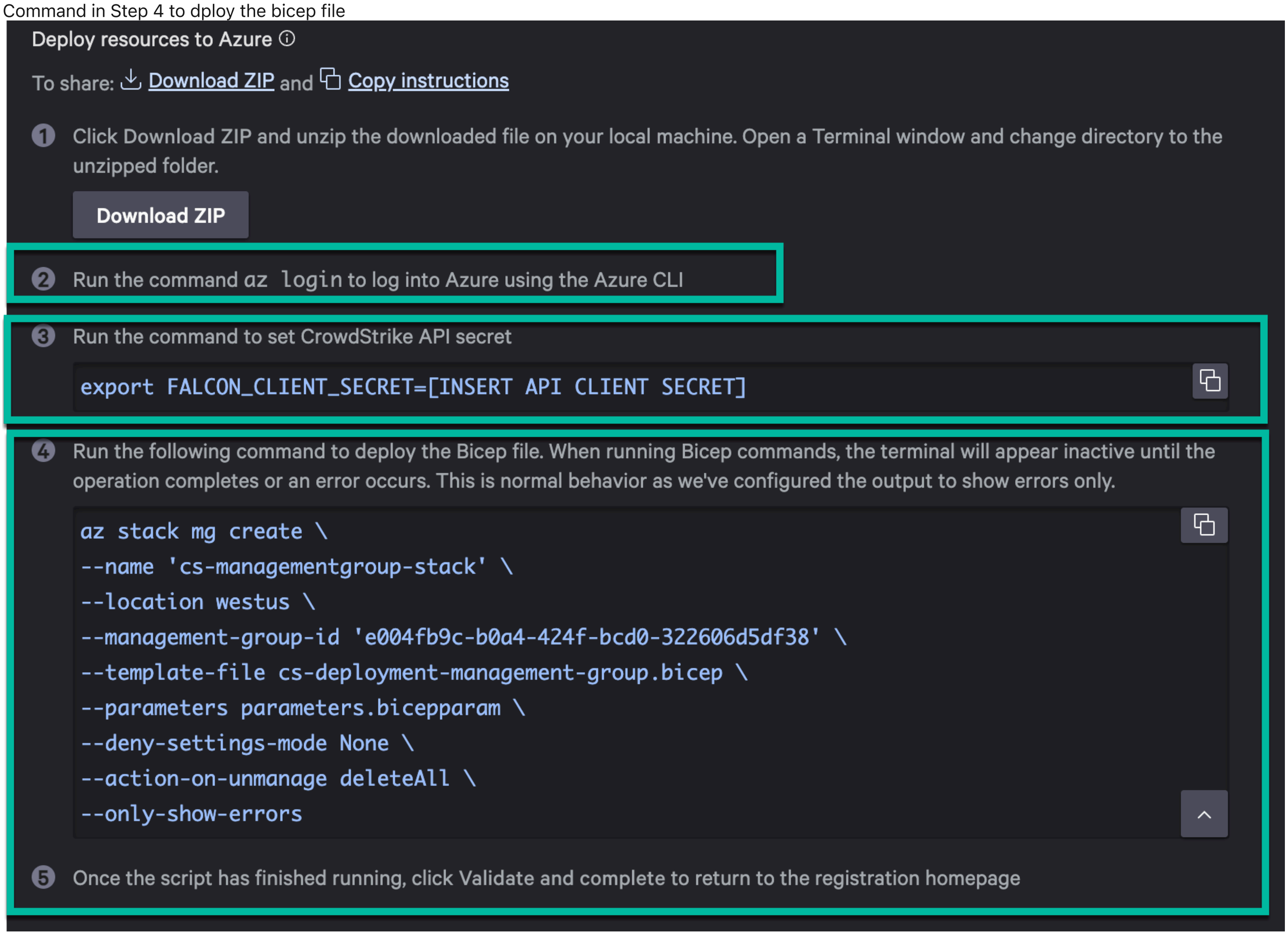
Does this app look suspicious? Report it here

Part 2: Deploy resources to Azure

IMPORTANT: Run bicep script in Azure CloudShell via Bash and change westus to "eastus2"

- We ran the bicep registration script inside Windows CMD via Azure CLI and there were permission issues. CrowdStrike recommends we run it in Azure CloudShell via Bash as the bicep script is made for Azure CloudShell.
- Security will need to provide secret value of API key to Global Admin
- Infra will sign into Azure using Azure CloudShell
- Command to set CrowdStrike API secret in step 2

- Command in Step 4 to dploy the bicep file



Deploy resources to Azure ⓘ

To share: Download ZIP and Copy instructions

1 Click Download ZIP and unzip the downloaded file on your local machine. Open a Terminal window and change directory to the unzipped folder.

2 Run the command `az login` to log into Azure using the Azure CLI

3 Run the command to set CrowdStrike API secret

```
export FALCON_CLIENT_SECRET=[INSERT API CLIENT SECRET]
```

4 Run the following command to deploy the Bicep file. When running Bicep commands, the terminal will appear inactive until the operation completes or an error occurs. This is normal behavior as we've configured the output to show errors only.

```
az stack mg create \
--name 'cs-managementgroup-stack' \
--location westus \
--management-group-id 'e004fb9c-b0a4-424f-bcd0-322606d5df38' \
--template-file cs-deployment-management-group.bicep \
--parameters parameters.bicepparam \
--deny-settings-mode None \
--action-on-unmanage deleteAll \
--only-show-errors
```

5 Once the script has finished running, click Validate and complete to return to the registration homepage

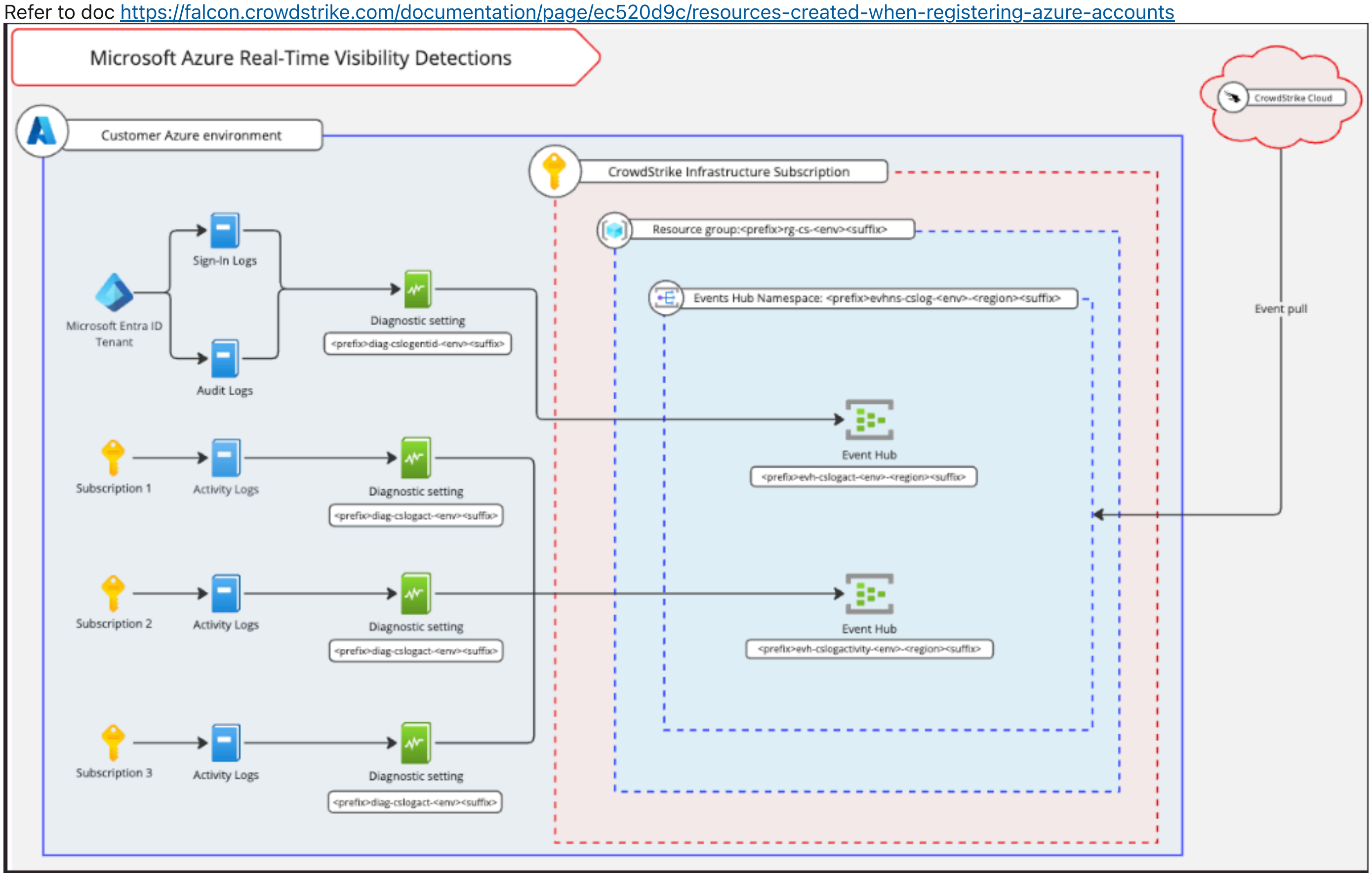
Step 5: Validate

1. Double check if all the resources were created and the diagnostic settings were set up
2. Click validate and complete from CSPM Console
3. Check CSPM console after 2 hours for the accounts

==

Resources created for new registration:

- Refer to doc https://falcon.crowdstrike.com/documentation/page/ec520d9c/resources-created-when-registering-azure-accounts


Microsoft Azure Real-Time Visibility Detections
CrowdStrike Cloud
Customer Azure environment
CrowdStrike Infrastructure Subscription
Resource group:<prefix>rg-cs-<env><suffix>
Events Hub Namespace: <prefix>evhns-cslog-<env>-<region><suffix>
Event pull
Sign-In Logs
Microsoft Entra ID Tenant
Audit Logs
Diagnostic setting
<prefix>diag-cslogentid-<env><suffix>
Event Hub
<prefix>evh-cslogact-<env>-<region><suffix>
Subscription 1
Activity Logs
Diagnostic setting
<prefix>diag-cslogact-<env><suffix>
Subscription 2
Activity Logs
Diagnostic setting
<prefix>diag-cslogact-<env><suffix>
Event Hub
<prefix>evh-cslogactivity-<env>-<region><suffix>
Subscription 3
Activity Logs
Diagnostic setting
<prefix>diag-cslogact-<env><suffix>

1. Diagnostic settings will be created for the Entra ID tenant which will send tenant sign-in logs and audit logs to the event hub.
2. Diagnostic settings for each Azure subscription which will send activity logs to the event hub.

- Note not all subscriptions will have diagnostic settings set up if they do not have Microsoft.Insights enabled. Most of the resources that will not have will be in the Resource-Restricted management group.

3. Resource group that will contain all of the resources required for RTVD

- rg-cs-prod

4. Event Hub namespace that will hold the Event Hubs

- evhns-cslog-adcsgt2jo5t3s

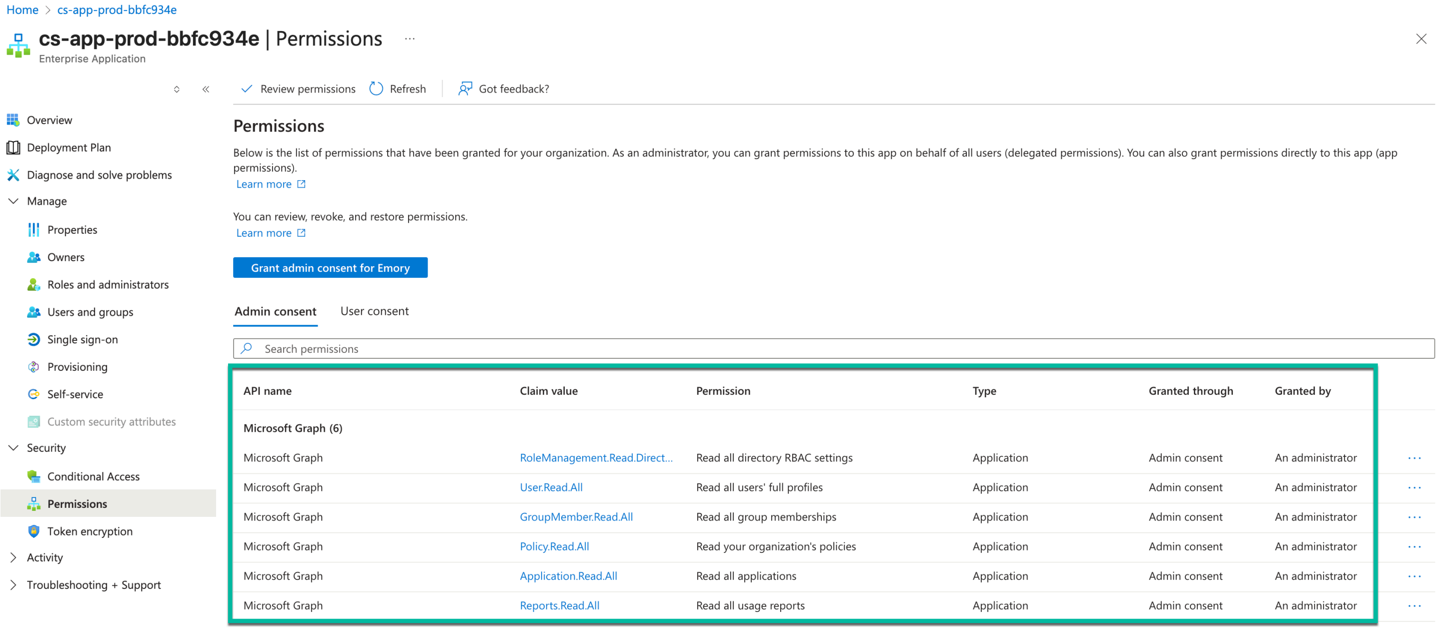
5. Event Hubs for Entra ID that ingests the sign in and audit logs from the diagnostic settings

- evh-cslogentid-prod-eastus2

6. Event hub for all the subscriptions. It will ingest activity logs from the diagnostic settings

- evh-cslogact-prod-eastus2

7. Enterprise Application (**cs-app-prod-bbfc934e**) that will have access to our entra ID tenant. The Azure Event Hubs data Receiver role is assigned to the Enterprise Application, which gives CrowdStrike the ability pull logs from the event hubs.



cs-app-prod-bbfc934e | Permissions

Enterprise Application

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions).

Learn more

You can review, revoke, and restore permissions.

Learn more

API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (6)					
Microsoft Graph	RoleManagement.Read.Direct...	Read all directory RBAC settings	Application	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent	An administrator
Microsoft Graph	GroupMember.Read.All	Read all group memberships	Application	Admin consent	An administrator
Microsoft Graph	Policy.Read.All	Read your organization's policies	Application	Admin consent	An administrator
Microsoft Graph	Application.Read.All	Read all applications	Application	Admin consent	An administrator
Microsoft Graph	Reports.Read.All	Read all usage reports	Application	Admin consent	An administrator

8. Azure RBAC custom role will be created once in the root management group, since we registered the whole tenant.

- Custom Role: role-csreader-e004fb9c-b0a4-424f-bcd0-322606d5df38

---

9. Azure Policy, which creates the diagnostic settings for each subscription for RTVD.

- CrowdStrike Activity Log Collection

10. Managed identity to run the powershell scripts when registering using Bicep.

- id-csscriptrunner-prod

Key Takeaways:

- We had to run the bicep command within Azure CloudShell and NOT Windows CMD via Azure CLI. Running from Windows CMD caused permission issues.
- We had to disable the resource restricted initiative from the Resource Restricted management group and then have Josh Presely re-deploy bicep script via Azure CloudShell via Bash.
- 16 subscriptions are disabled so IOAs are inactive in CSPM
- All other subscriptions have IOMs and IOAs enabled including resource restricted management group. After enabling the resource restricted initiative, no resources should be created in the student subscriptions so no costs will occur
- Any future subscriptions onboarded to our tenant should have IOM and IOA enabled and diagnostic settings should automatically be configured from the Azure Policy and because we registered the environment at the tenant root group.