



YOU DESERVE THE BEST SECURITY

HARMONY CONNECT IDプロバイダ連携 簡易設定ガイド～AZURE AD 編～

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
システム・エンジニアリング本部

- ・ 本ドキュメントは、検証、ハンズオン研修等での利用を目的としているため、一部の設定手順のみを記載しています。
- ・ 本番環境の設定は、Administration Guide 等に基づいて行ってください。
- ・ 本手順書と、Administration Guide、SK等の記述内容が異なる場合は、原則、本手順書以外のドキュメントの内容が優先されます。
- ・ 本手順書は、2022年1月現在の設定内容、UIに基づいて作成されています。

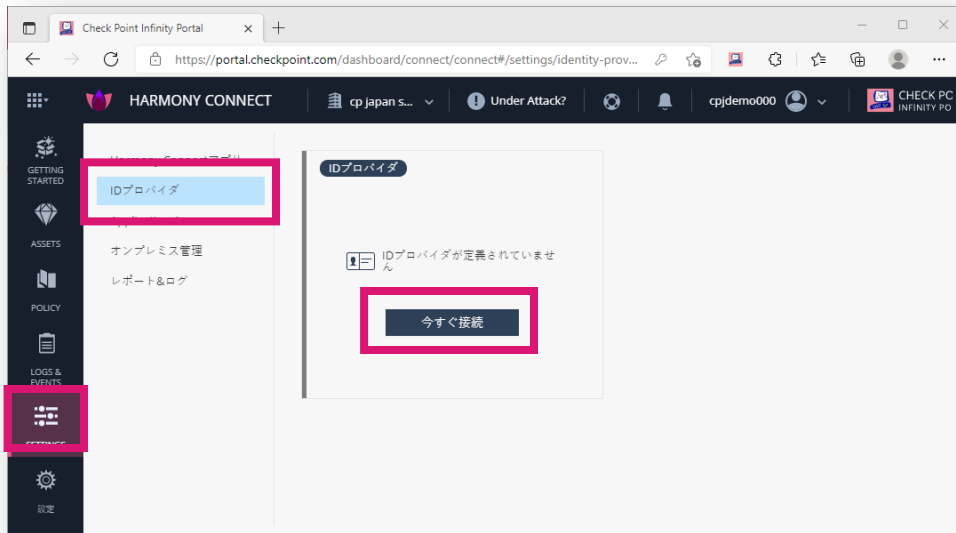
Agenda

- ユーザの作成 [Azure AD 連携]
- ConnectApp のマニュアルインストール
- AzureAD での認証連携設定

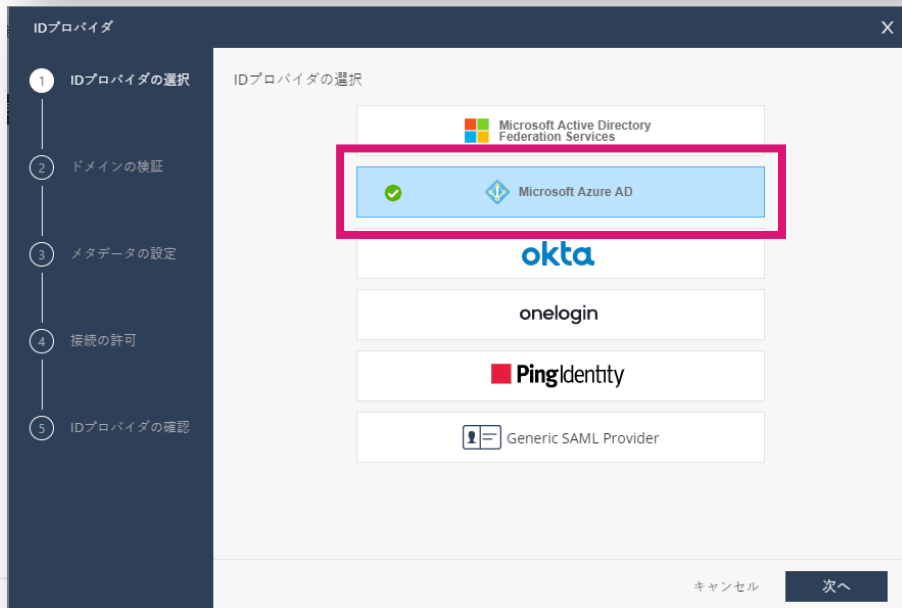
YOU DESERVE THE BEST SECURITY

ユーザの作成 [Azure AD 連携] (1 / 6)

1. 「SETTINGS > ID プロバイダ」を選択する
2. 「今すぐ接続」を押す



3. 「Microsoft Azure AD」を選択して、「次へ」を押す



ユーザの作成 [Azure AD 連携] (2 / 6)

IDプロバイダ

1 IDプロバイダの選択

2 **ドメインの検証**

3 接続の許可

4 メタデータの設定

5 ディレクトリ統合の設定

6 IDプロバイダの確認

エンドユーザは企業のメールアドレスを使って認証を行います。EメールドメインをInfinity Portalアカウントにマッピングしてセキュリティポリシーを実施するには、企業ドメインを指定してください。

ドメイン (0アイテム)

smb-se.checkpoint.sc

このドメインに属するユーザの認証は、このInfinity Portalアカウントでのみ利用できます。

このレコードをパブリックDNSサーバに追加して、ドメインの所有者を検証してください。

レコードタイプ: TXT

ホスト: 空白にしてください。

値: 183cfabe-53b...2d-a269-909d0ef2569f

詳細は管理ガイドを参照してください

DNS アウトソーシングサービスの設定画面でホスト名を空白にできない場合は、@を入力する

4. 登録するドメインを管理する DNS サーバの TXTレコードに表示されている値を設定する

5. Azure AD のドメイン名を入力して、「+」を押す

- 「+」は隠れ気味の時があるので注意

IDプロバイダ

1 IDプロバイダの選択

2 **ドメインの検証**

3 接続の許可

4 メタデータの設定

5 ディレクトリ統合の設定

6 IDプロバイダの確認

エンドユーザは企業のメールアドレスを使って認証を行います。EメールドメインをInfinity Portalアカウントにマッピングしてセキュリティポリシーを実施するには、企業ドメインを指定してください。

ドメイン (count, plural, =0 {{0アイテム}} 1 {{#アイテム}} その他 {{#アイテム}})

例: mycompany.com

smb-se.checkpoint.sc

このドメインに属するユーザの認証は、このInfinity Portalアカウントでのみ利用できます。

このレコードをパブリックDNSサーバに追加して、ドメインの所有者を検証してください。

レコードタイプ: TXT

ホスト: 空白にしてください。

値: 183cfabe-53b...2d-a269-909d0ef2569f

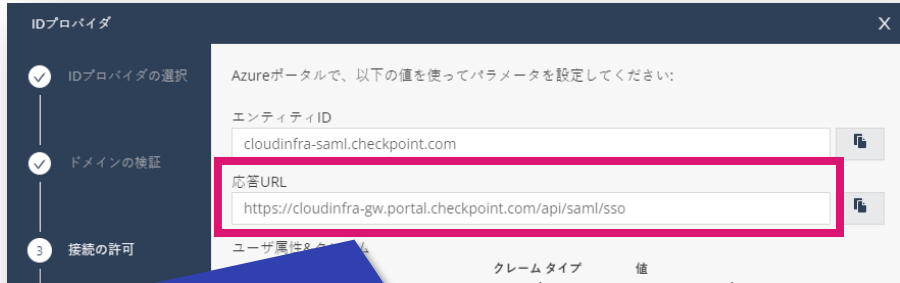
詳細は管理ガイドを参照してください

戻る 次へ

ドメイン認証に成功すると、ドメイン名が表示される

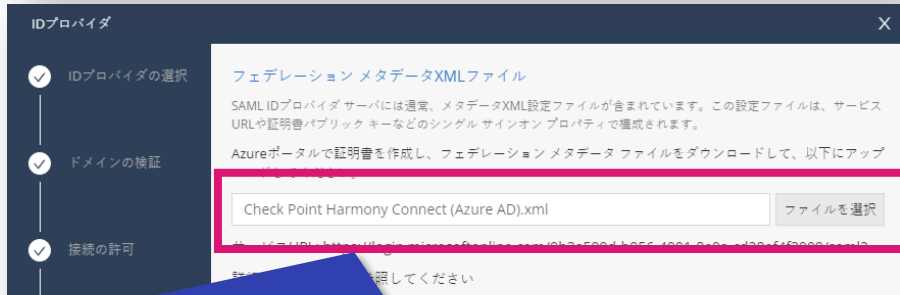
6. ドメイン認証に成功したことを確認して、「次へ」を押す

ユーザの作成 [Azure AD 連携] (3 / 6)



Azure AD > エンタープライズアプリケーション
> Check Point Harmony Connect(Azure AD)
> シングルサインオン > 基本的な SAML 構成
に、設定する

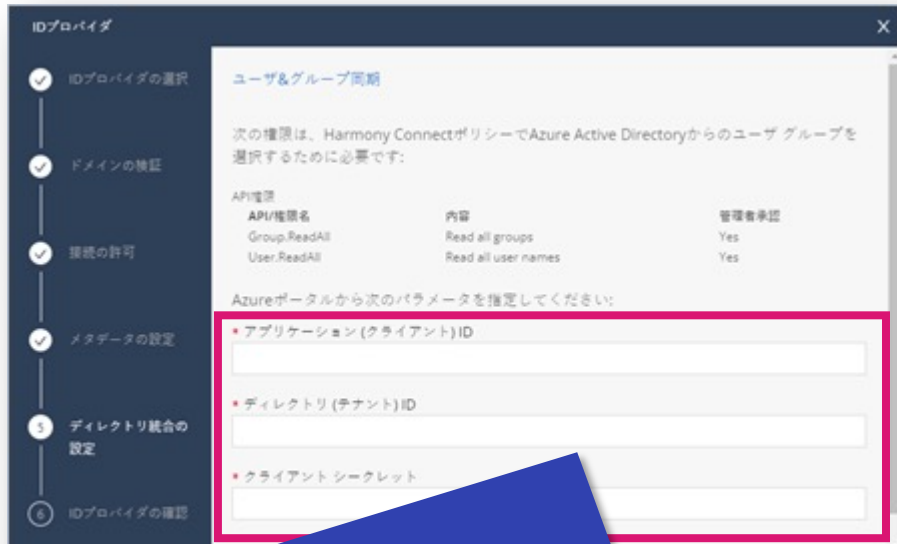
7. 応答 URL を、Azure AD へ設定して、「次へ」を押す
 - Azure AD のギャラリーアプリケーションを使用する場合、エンティティ ID は設定済みのため入力不要



Azure AD > エンタープライズアプリケーション
> Check Point Harmony Connect(Azure AD)
> シングルサインオン > SAML 署名証明書
の「フェデレーションメタデータ XML」をアップロード

8. Azure AD からダウンロードした、「フェデレーションメタデータ XML」ファイルをアップロードして、「次へ」を押す

ユーザの作成 [Azure AD 連携] (4 / 6)



9. Azure AD から以下の3つの値をコピーして、
入力する

10. 「次へ」を押す

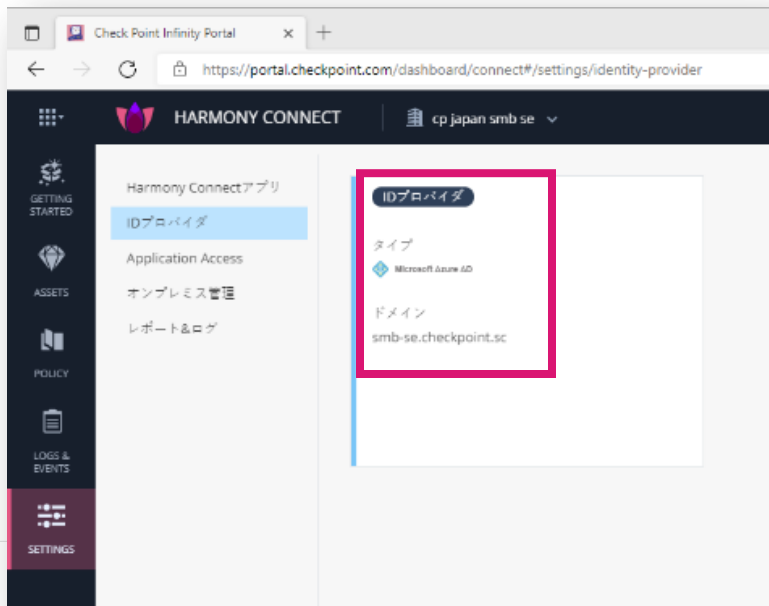
- アプリケーション ID
 - アプリの登録 > Check Point Harmony Connect (Azure AD) の 概要ページ
- ディレクトリ(テナント) ID
 - アプリの登録 > Check Point Harmony Connect (Azure AD) の 概要ページ
- クライアントシークレット
 - アプリの登録 > 証明書とシークレットで、新しいクライアントシークレットを作成し、クライアントシークレットの「値」をコピー

ユーザの作成 [Azure AD 連携] (5 / 6)

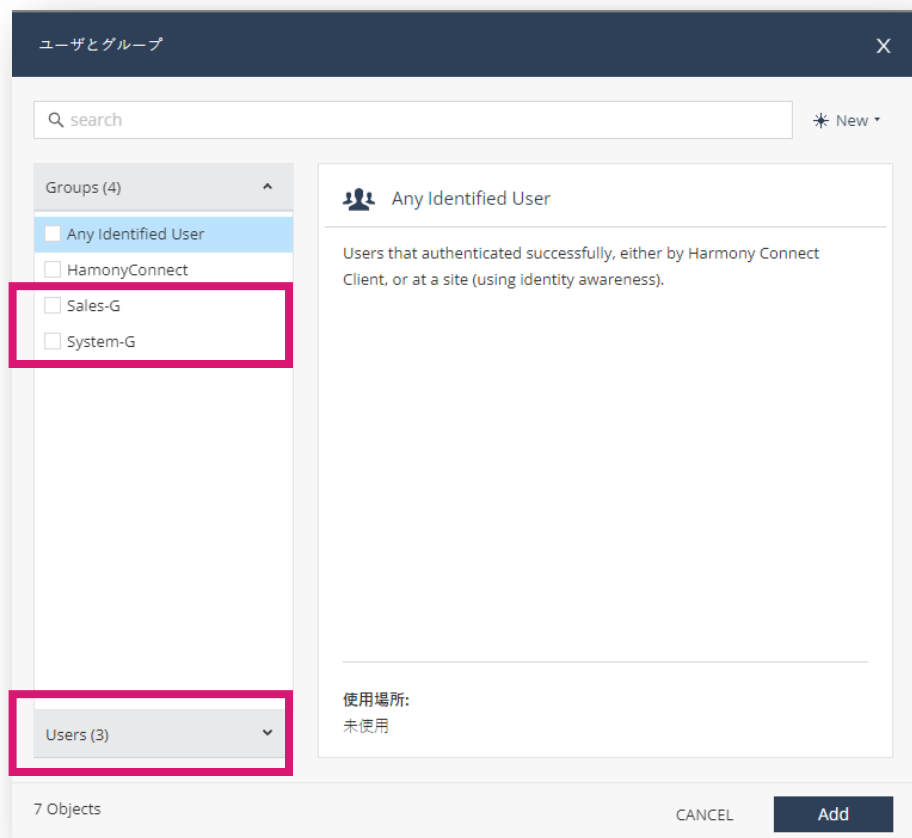
11.ID プロバイダの設定内容を確認して、「ID プロバイダの追加」を押す



12.Harmony Connect への ID プロバイダの追加が完了



ユーザの作成 [Azure AD 連携] (6 / 6)

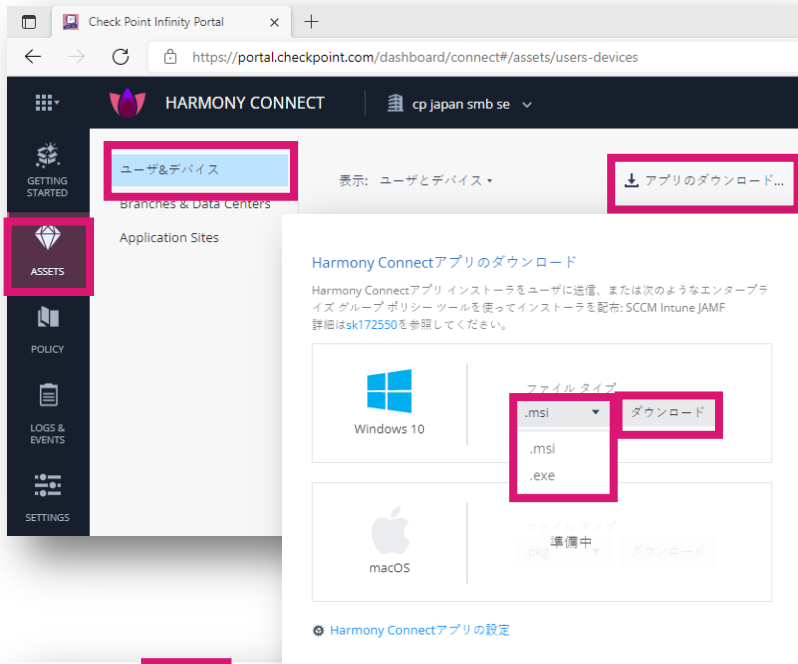


13. ID プロバイダと Harmony Connect との間で、ユーザとグループの同期が完了すると、「POLICY > アクセスコントロール > インターネットアクセス」のオブジェクトに、ID プロバイダの「ユーザ」と「グループ」が自動追加される

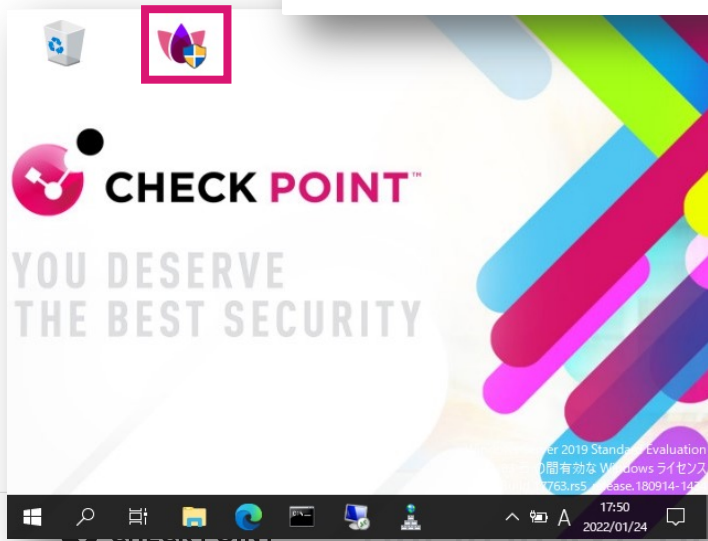
- 「ユーザ」、「グループ」の同期が可能な ID プロバイダは、Azure AD、Okta、PingID のみ

14. 「ユーザ」と「グループ」は、Access Control のルール作成時に「ソース（送信元）」として指定可能

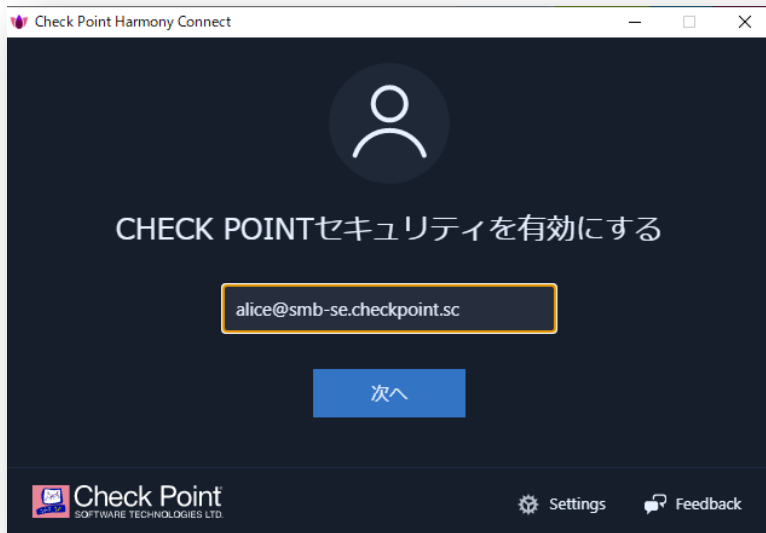
ConnetApp のマニュアルインストール（1 / 4）



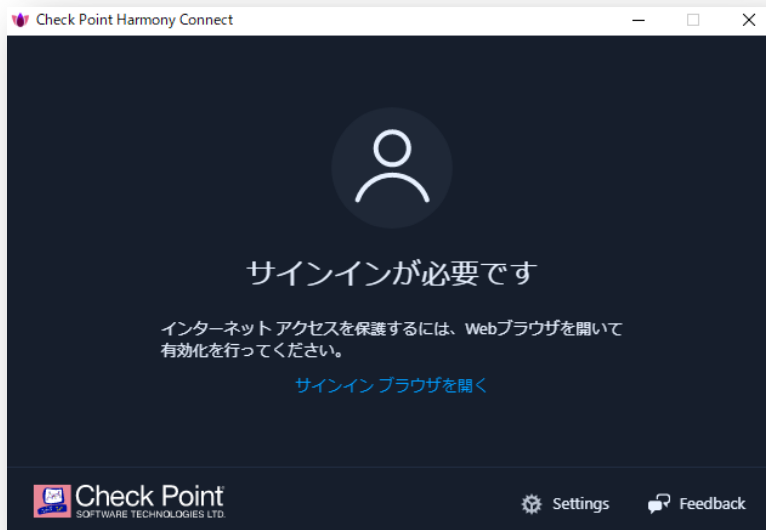
1. 「ASSETS > ユーザ&デバイス」を選択する
2. 「アプリのダウンロード」を押す
3. ファイルタイプを選択して「ダウンロード」を押してダウンロードする
4. インストールファイルをダブルクリックする



ConnetApp のマニュアルインストール（2 / 4）

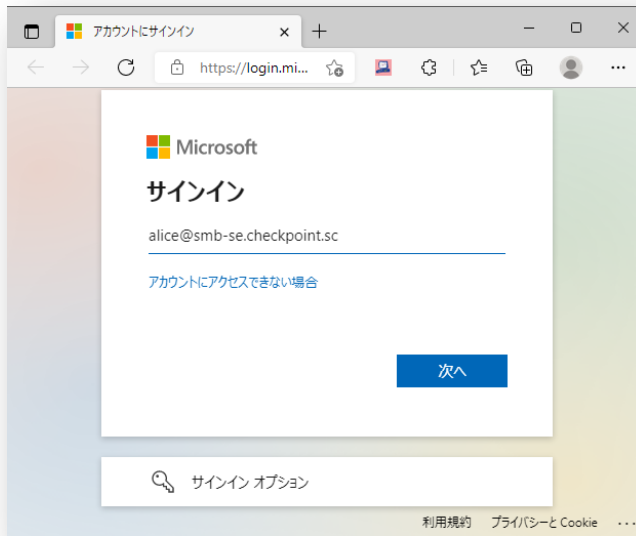


6. 認証ダイアログボックスが表示されるので、「ユーザ名（メールアドレス形式）」を入力し、「次へ」を押す

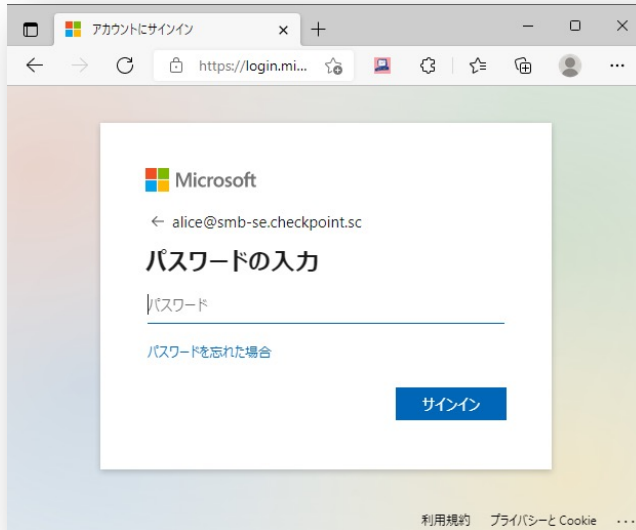


7. サインインを求められるので、「サインイン ブラウザを開く」を押す

ConnetApp のマニュアルインストール（3 / 4）

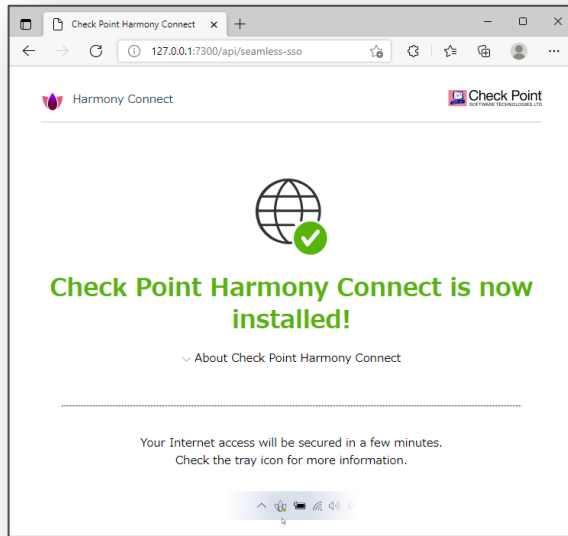


8. サインインページで「ユーザ名（メールアドレス形式）」を入力し、「次へ」を押す

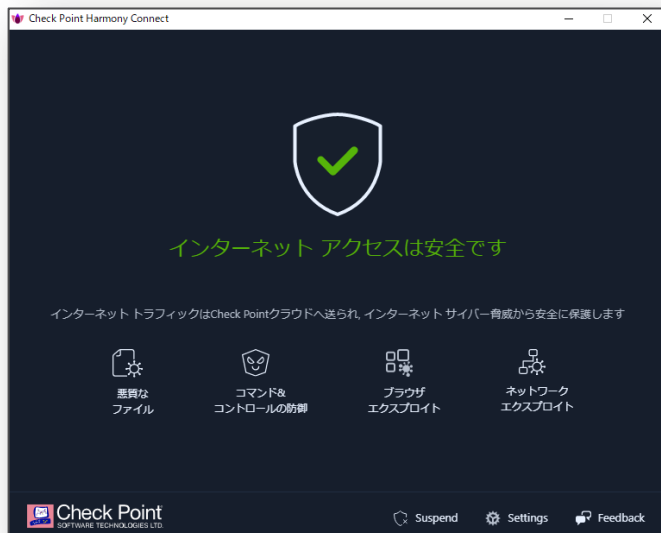


9. 「パスワード」を入力し、「サインイン」を押す

ConnetApp のマニュアルインストール（4 / 4）

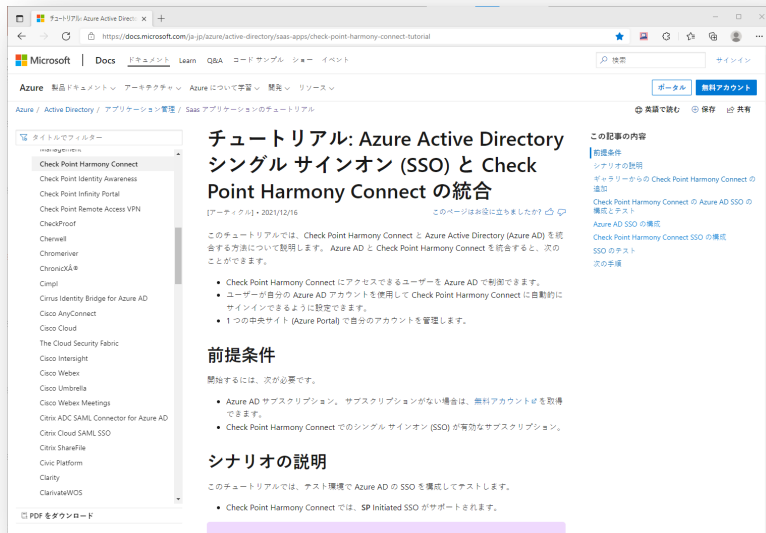


10. サインインが完了すると、ConnectApp のインストールが完了する



11. インストールが完了すると、自動的に Harmony Connect がトラフィックの保護を開始する

Azure AD での認証連携設定 (1 / 10)



1. 基本的には Microsoft が公開しているチュートリアルに沿って設定すればよいが、一部設定が不足している

- [チュートリアル: Azure Active Directory シングルサインオン \(SSO\) と Check Point Harmony Connect の統合](#)
- <https://docs.microsoft.com/ja-jp/azure/active-directory/saas-apps/check-point-harmony-connect-tutorial>

2. Azure AD SSO の構成の流れ

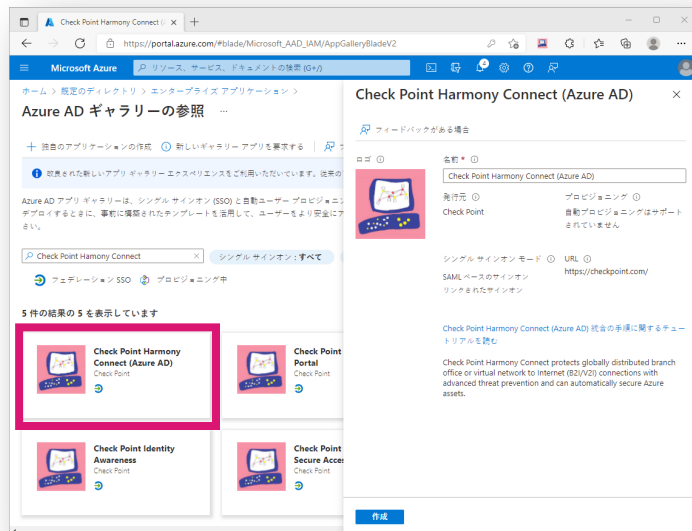
- I. エンタープライズアプリケーションの作成
- II. SSO 方式の選択
- III. SAML 構成の設定
- IV. 属性とクレームの確認
- V. フェデレーション メタデータ XML のダウンロード
- VI. クライアントシークレットの作成
- VII. API のアクセス許可設定
- VIII. ユーザ、グループの割り当て

Azure AD での認証連携設定 (2 / 10)

エンタープライズアプリケーション > すべてのアプリケーション (プレビュー)



3. エンタープライズアプリケーション画面で、「新しいアプリケーション」をクリックする

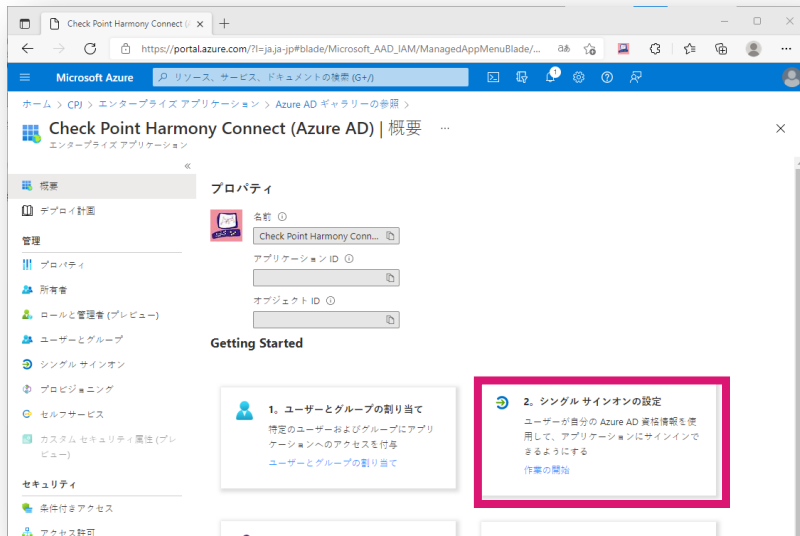


4. Azure AD ギャラリーで、「Check Point Harmony Connect」のキーワードで検索する
5. 「Check Point Harmony Connect (Azure AD)」を選択する
6. 「作成」を押す

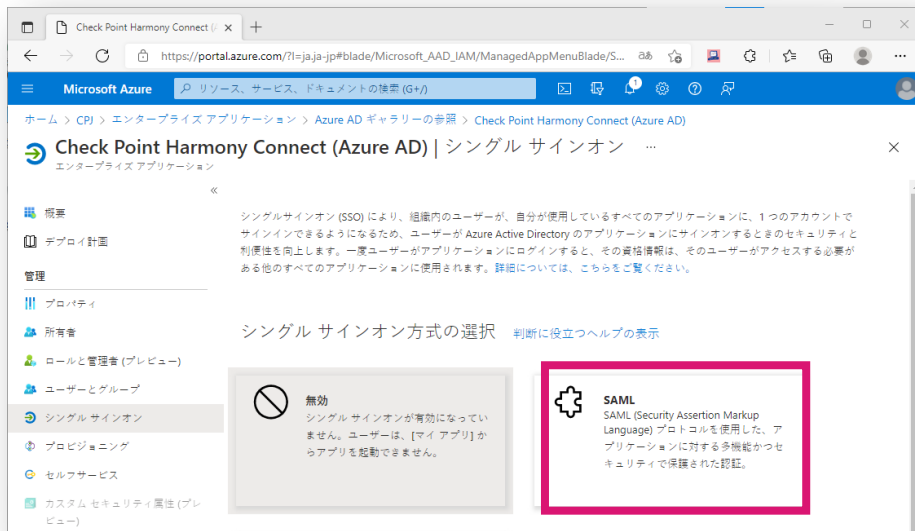
Azure AD での認証連携設定 (3 / 10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > 概要

7. 「シングルサインオンの設定」をクリックする



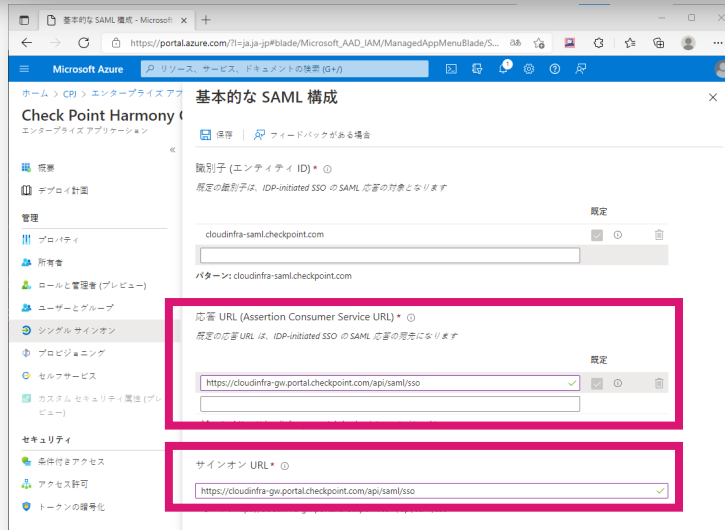
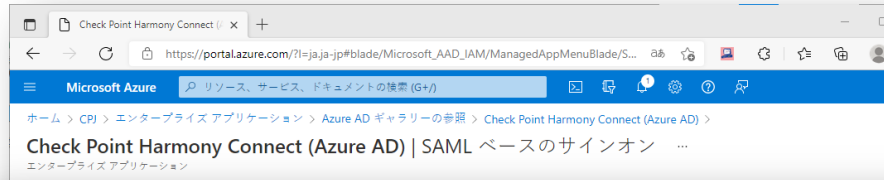
8. 「SAML」をクリックする



Azure AD での認証連携設定 (4 / 10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > シングルサインオン

9. 「基本的な SAML 構成」欄の「編集」をクリックする



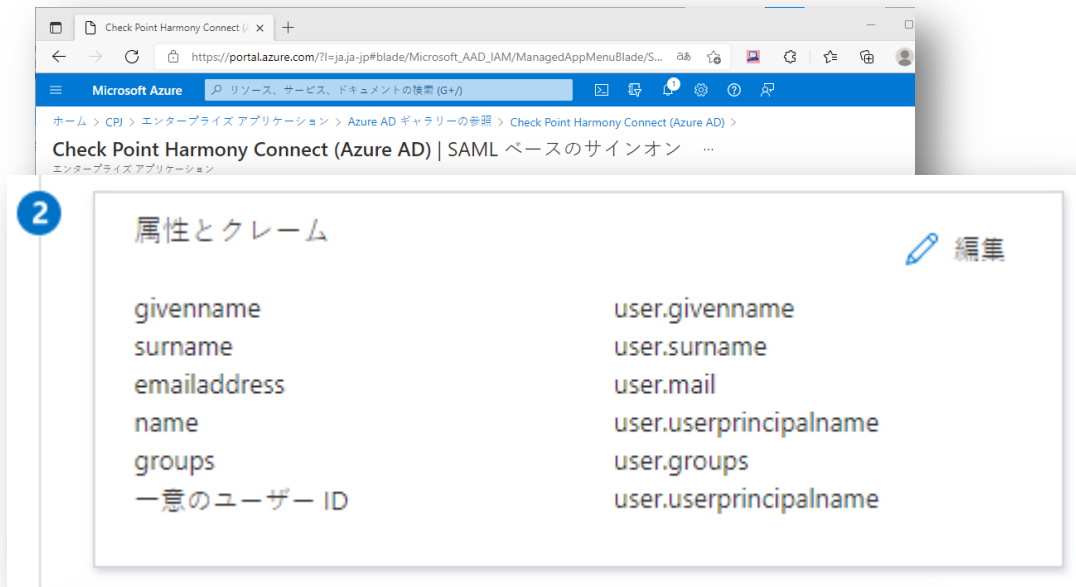
10. 「応答URL」、「サインオンURL」欄に、以下のURLを入力する

- <https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso>

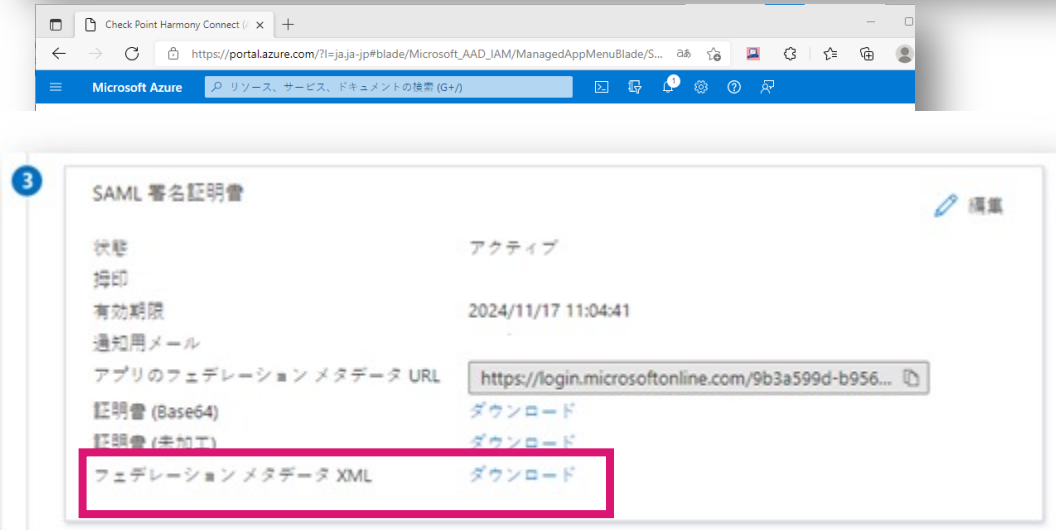
Azure AD での認証連携設定 (5 / 10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > シングルサインオン

11. 「属性とクレーム」の表示と、Harmony Connect の「接続の許可」の画面の「ユーザ属性とクレーム」とが同じであることを確認する

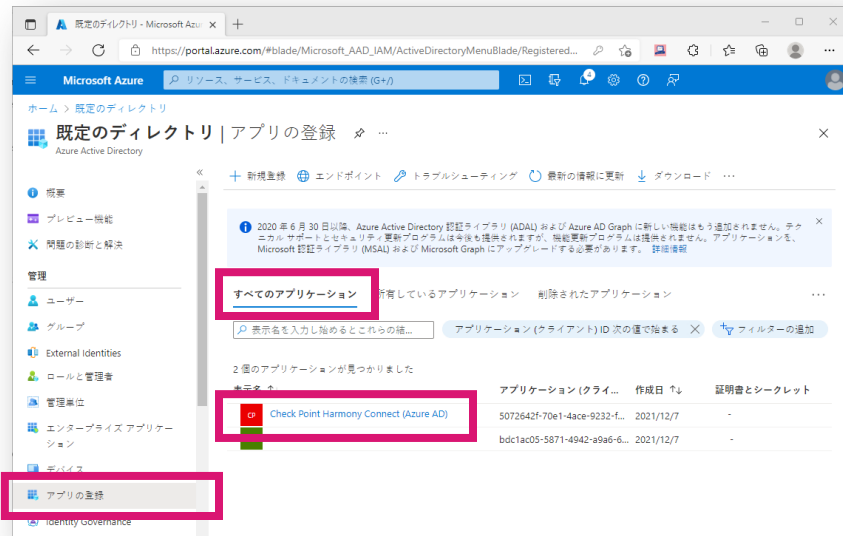


12. 「SAML 署名証明書」欄の「フェデレーションメタデータ XML」をダウンロードし、Harmony Connect の「メタデータの設定」の画面でアップロードする



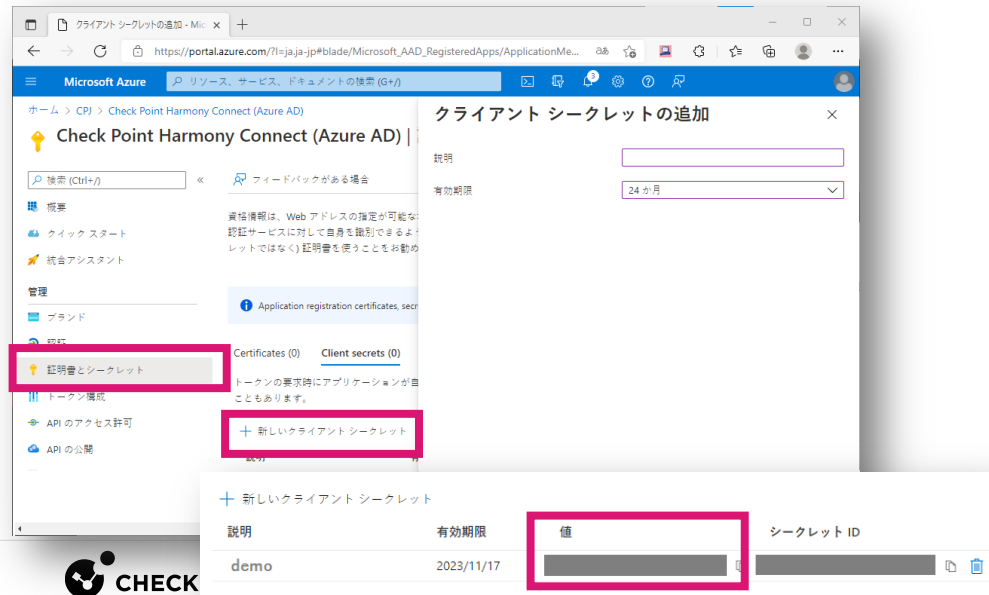
Azure AD での認証連携設定 (6 / 10)

アプリの登録 > Check Point Harmony Connect (Azure AD)



13. 「アプリの登録」画面で、「すべてのアプリケーション」をクリックする

14. 「Check Point Harmony Connect (Azure AD)」が表示されるのでクリックする



15. 「証明書とシークレット」をクリックする

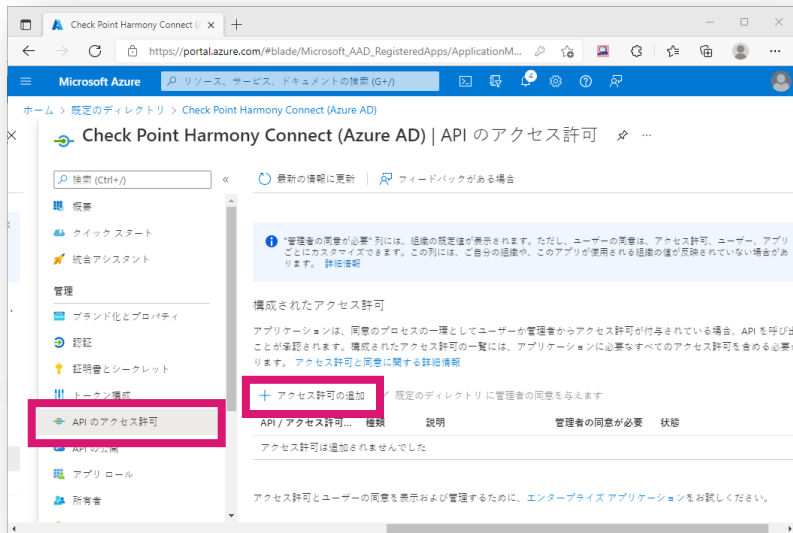
16. 「新しいクライアントシークレット」をクリックして、クライアントシークレットを追加する

- 「説明」、「有効期限」は、任意

17. 作成されたクライアントシークレットの「値」をコピーして、Harmony Connect の「ディレクトリ統合の設定」画面に入力する

Azure AD での認証連携設定 (7 / 10)

アプリの登録 > Check Point Harmony Connect (Azure AD)



18. 「API のアクセス許可」をクリックする

19. 「アクセス許可の追加」をクリックする



20. 「API アクセス許可の要求」画面で、「Microsoft Graph」を選択する

Azure AD での認証連携設定 (8 / 10)

アプリの登録 > Check Point Harmony Connect (Azure AD)

API アクセス許可の要求

Microsoft Graph
https://graph.microsoft.com/ [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可
アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可
アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデーモンとして実行されます。

アクセス許可を選択する [すべて展開](#)

アクセス許可を入力し始めると、これらの結果がフィルター処理されます

アクセス許可 管理者の同意が必要

Group (1)

- Group.Create ①
Create groups はい
- Group.Read.All ①
Read all groups はい
- Group.ReadWrite.All ①
Read and write all groups

User (1)

- User.Export.All ①
Export user's data
- User.Invite.All ①
Invite guest users to the organization
- User.ManageIdentities.All ①
Manage all users' identities
- User.Read.All ①
Read all users' full profiles
- User.ReadWrite.All ①
Read and write all users' full profiles

[アクセス許可の追加](#) [破棄](#)

21. 「API アクセス許可の要求」画面で、「アプリケーションの許可」を選択する

22. ロールの一覧が表示されるので、以下のアクセス許可を有効にする

- Group.Read.All
- User.Read.All

Check Point Harmony Connect (Azure AD) | API のアクセス許可

検索 (Ctrl+F) 最新の情報に更新 フィードバックがある場合

概要
クイックスタート
統合アシスタント

管理
ブランド化とプロパティ
認証
証明書とシークレット
トークン構成

API のアクセス許可

API の公開
アプリ ロール
所有者
ロールと管理者 | プレビュー
マニフェスト
サポート + トラブルシューティング

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

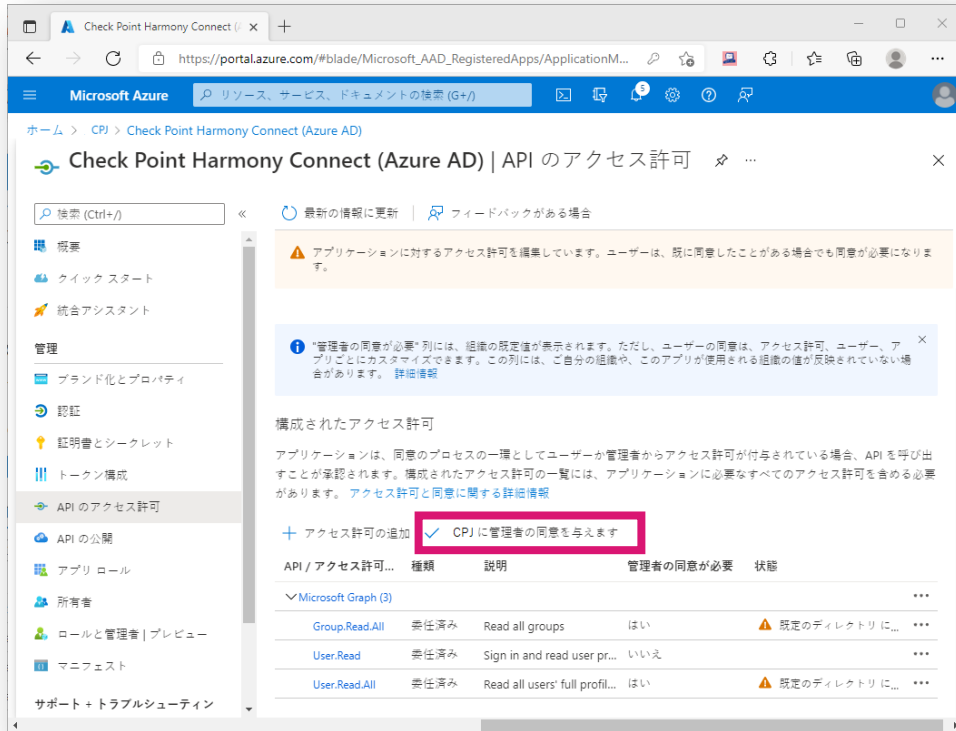
+ アクセス許可の追加 既定のディレクトリに管理者の同意を与えます

API / アクセス許可...	種類	説明	管理者の同意が必要	状態
Microsoft Graph (3)				
Group.Read.All	委任済み	Read all groups	はい	既定のディレクトリに...
User.Read	委任済み	Sign in and read user pr...	いいえ	...
User.Read.All	委任済み	Read all users' full profil...	はい	既定のディレクトリに...

Azure AD での認証連携設定 (9 / 10)

アプリの登録 > Check Point Harmony Connect (Azure AD)

22. 「 [ディレクトリ名] に管理者の同意を与えます」 をクリックして、API アクセス許可に管理者の同意を与える。



API / アクセス許可...	種類	説明	管理者の同意が必要	状態
▼ Microsoft Graph (3)				
Group.Read.All	委任済み	Read all groups	はい	✓ 既定のディレクトリに...
User.Read	委任済み	Sign in and read user pr...	いいえ	✓ 既定のディレクトリに...
User.Read.All	委任済み	Read all users' full profil...	はい	✓ 既定のディレクトリに...

Azure AD での認証連携設定 (10 / 10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD)

The screenshot shows the Azure portal interface for configuring Check Point Harmony Connect. The left sidebar has 'ユーザーとグループ' (Users and Groups) highlighted. The main content area shows a table of users and groups with columns for '表示名' (Display Name), 'オブジェクトの種類' (Object Type), and '割り当てられたロール' (Assigned Role). A modal dialog titled 'ユーザーとグループ' (Users and Groups) is open, showing a search bar and a list of users with their email addresses. The dialog also has a section for '選択したアイテム' (Selected Items) which is currently empty.

表示名	オブジェクトの種類	割り当てられたロール
alice	ユーザー	Default Access
bob	ユーザー	Default Access
char	ユーザー	Default Access
dozle	ユーザー	Default Access
emma	ユーザー	Default Access

ユーザーとグループ

alice
alice@smb-se.checkpoint.sc

bob
bob@smb-se.checkpoint.sc

選択したアイテム

項目が選択されていません

選択

23. 「ユーザーまたはグループの追加」をクリックする

24. 「割り当ての追加」画面で、「ユーザーとグループ」をクリックする

25. 「ユーザーとグループ」画面に、Azure AD のユーザーとグループが表示されるので、Harmony Connect を利用するユーザー、グループを選択する

- Harmony Connect に「グループ」を割り当てるためには、Azure AD Premium P1、P2 等のライセンスが必要です



THANK YOU

