



Mist Access Assurance Identity Provider - Entra ID 設定

ジュニパーネットワークス株式会社

Version 1.0

JUNIPER
NETWORKS

Driven by
Experience™

はじめに

- ❖ 本マニュアルは、『Identity Provider - Entra ID 設定』について説明します
- ❖ 手順内容は 2025年9月 時点の Mist Cloud にて確認を実施しております
実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
<https://www.juniper.net/documentation/us/en/software/mist/product-updates/latest.html>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります
各種設定内容の詳細は下記リンクよりご確認ください
[Mist Documentation](#)
[Juniper Mist Access Assurance Guide](#)
- ❖ 他にも多数の Mist 日本語マニュアルを「ソリューション&テクニカル情報サイト」に掲載しております
<https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html>
- ❖ **本資料の内容は資料作成時点におけるものであり事前の通告無しに内容を変更する場合があります**
また本資料に記載された構成や機能を提供することを条件として購入することはできません
- ❖ 本資料に記載されている会社名、製品名およびロゴは、各社の商標または登録商標です

An abstract visualization of a network or data flow, rendered in vibrant green. It features a dense, glowing structure of interconnected points and lines, forming a complex, organic shape that resembles a large, curved leaf or a stylized letter 'J'. The background is a dark, almost black space, which makes the bright green particles and lines stand out prominently. The overall effect is one of dynamic energy and intricate connectivity.

更新履歷



Identity Providers

Entra ID/OAuth

Entra ID 設定

Entra ID(Azure AD)/OAuth Overview

Entra ID/OAuth のアプリケーションを登録します

アプリの登録

新規登録 > アプリケーション名を設定 > 登録

アプリケーション(クライアント)ID

ディレクトリ(テナント)ID

証明書またはシークレットの追加

証明書とシークレット

新しいクライアントシークレット

説明

有効期限

クライアントシークレット

認証

パブリッククライアントフローを許可する > 保存

APIのアクセス許可

Microsoft Graph

- User.Read - Delegated
- User.Read.All - Application
- Group.Read.All - Application
- Device.Read.All - Application

ユーザ・グループの追加



クライアントシークレットの値は作成直後のみ確認できます
忘れずにコピーしてください



Organization > Identity Providers > Add IDP

[Name] を入力します

[OAuth] を選択します

[Azure] を選択します

[OAuth Tenant ID] を入力します

[Domain Names] を入力します

[OAuth Client Credential(CC) Client Id] を入力します

[OAuth Client Credential(CC) Client Secret] を入力します

[OAuth ROPC Client Id] を入力します

Entra ID 設定

Entra ID アプリの登録

1. Entra ID(旧 Azure Active Directory) にアクセスします
2. [アプリの登録] を選択し、[新規登録] をクリックします

ホーム > [Organization Name]

[Organization Name] | アプリの登録 ☆ ...

◇ << **+ 新規登録** 🌐 エンドポイント ✖ トラブルシューティング 🔄 最新の情報に更新 ↓ ダウンロード 📄 プレビュー機能 | 👤 フィードバックがある場合

External Identities
ロールと管理者
管理単位
代理管理者パートナー
エンタープライズ アプリケーション
デバイス
アプリの登録
Identity Governance
アプリケーション プロキシ
カスタム セキュリティ属性
ライセンス
テナント間同期
Microsoft Entra Connect

すべてのアプリケーション 所有しているアプリケーション 削除されたアプリケーション

🔍 表示名またはアプリケーション (クライアント) ID を入力し始めると結果がフィ... **+ フィルターの追加**

このアカウントは、このディレクトリ内のどのアプリケーションの所有者の一覧にも含まれていません。

ディレクトリ内のすべてのアプリケーションを表示

Entra ID 設定

登録

3. [名前] を入力、[サポートされているアカウントの種類]を選択、[登録] をクリックします

アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。

Mist AA IdP ✓

サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

この組織ディレクトリのみに含まれるアカウント (のみ - シングル テナント)

任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)

任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント) と個人用の Microsoft アカウント (Skype、Xbox など)

個人用 Microsoft アカウントのみ

[選択に関する詳細...](#)

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

プラットフォームの選択 ▼ 例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります [?](#)

登録

Entra ID 設定

概要 アプリケーション(クライアント)ID / ディレクトリ(テナント)ID

4. [アプリケーション(クライアント) ID] と[ディレクトリ(テナント) ID] をコピーします
5. [証明書またはシークレットの追加] をクリックします

ホーム > [redacted] | アプリの登録 >

Mist AA IdP

検索

削除 エンドポイント プレビュー機能

概要

- クイック スタート
- 統合アシスタント
- 問題の診断と解決
- 管理
- サポート + トラブルシューティング

基本

表示名	Mist AA IdP	クライアントの資格情報	証明書またはシークレットの追加
アプリケーション (クライアント) ID	8064712b-05ea-486e-8ca[redacted]	リダイレクト URI	リダイレクト URI を追加する
オブジェクト ID	cd3fef53-a76b-4d4e-95c4-4ddbada4a5557	アプリケーション ID の URI	アプリケーション ID URI の追加
ディレクトリ (テナント) ID	d1db1fde-f083-4f59-b3db[redacted]	ローカル ディレクトリでのマネージド アプリケーション	Mist AA IdP

サポートされているアカウントの種類
[所属する組織のみ](#)

概要 ドキュメント

Entra ID 設定

証明書とシークレット クライアントシークレットの追加

有効期限は実運用にあわせて適度な期間に設定してください



6. [証明書とシークレット] を選択、 [+新しいクライアントシークレット] をクリックします
[説明] を入力、 [有効期限] を選択し、 [追加] をクリックします

ホーム > [] | アプリの登録 > Mist AA IdP

Mist AA IdP | 証明書とシークレット

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

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

フィードバックがある場合

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンをめめものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではな

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (0)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列で

+ 新しいクライアント シークレット

説明	有効期限	値
このアプリケーションのクライアント シークレットは作成されていません。		

クライアント シークレットの追加

説明: Mist AA IdP クライアントシークレット

有効期限: 推奨: 180 日 (6 か月)

推奨: 180 日 (6 か月)

推奨: 180 日 (6 か月)

90 日 (3 か月)

365 日 (12 か月)

545 日 (18 か月)

730 日 (24 か月)

カスタム

追加 キャンセル

Entra ID 設定

証明書とシークレット クライアントシークレットのコピー

忘れずにコピーしてください



7. クライアントシークレットの [値] をコピーします

ホーム > [] | アプリの登録 > Mist AA IdP

Mist AA IdP | 証明書とシークレット

検索 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
- 問題の診断と解決
- 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
 - マニフェスト
- サポート + トラブルシューティング

お時間があれば、フィードバックをお寄せください。 →

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (1)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID
Mist AA IdP クライアントシークレット	2025/3/25	KP08Q~_AUjgWtCR0I1B5MdZihaYH...	fc81fe9-757e-46f0-a9dd-0e6a5ee...

作成直後のみ値をコピーできます

Entra ID 設定

パブリッククライアントフローを許可する

8. [認証] を選択、[パブリッククライアントフローを許可する] の項目で [はい] に選択します
[保存] をクリックします

ホーム > [] | アプリの登録 > Mist AA IdP

Mist AA IdP | 認証

検索

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

問題の診断と解決

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

マニフェスト

サポート + トラブルシューティング

プラットフォーム構成

このアプリケーションが対象としているプラットフォームまたはデバイスによっては、リダイレクト URI、特定の認証設定、プラットフォームに特有のフィールドなど追加構成が必要となる場合があります。

+ プラットフォームを追加

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか？

この組織ディレクトリのみに含まれるアカウント (上平 和也 のみ - シングル テナント)

任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)

判断に役立つヘルプの表示...

警告: サポートされている機能が一時的に異なるため、既存の登録に関して個人用 Microsoft アカウントを有効にしないでください。個人アカウントを有効にする必要がある場合、マニフェスト エディターを使用して有効にできます。 [これらの制限に関する詳細情報。](#)

詳細設定

パブリック クライアント フローを許可する

次のモバイルとデスクトップのフローを有効にする:

はい いいえ

- アプリによってプレーンテキスト パスワードを収集する (リソース所有者のパスワード資格情報フロー) [詳細情報](#)
- キーボードなし (デバイス コード フロー) [詳細情報](#)
- ドメイン参加済みの Windows の SSO (Windows 統合認証フロー) [詳細情報](#)

アプリ インスタンス プロパティのロック

アプリケーション インスタンスの変更ロックを構成します。 [詳細情報](#) 構成

保存 破棄

Entra ID 設定

API のアクセス許可 Microsoft Graph

9. [API のアクセス許可] を選択、[Microsoft Graph] をクリックします

The screenshot shows the Microsoft Entra ID portal interface. On the left, the navigation pane includes 'API のアクセス許可' (API Access), which is highlighted with a red box. The main content area is titled 'API アクセス許可の要求' (API Access Requirements). Under the heading 'よく使用される Microsoft API' (Commonly used Microsoft APIs), the 'Microsoft Graph' API is highlighted with a red box. The description for Microsoft Graph reads: 'Office 365, Enterprise Mobility + Security, Windows 10 の大量のデータを活用しましょう。Microsoft Entra ID、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。' (Use the vast amount of data from Office 365, Enterprise Mobility + Security, Windows 10. Use Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, etc. via a single endpoint for access.)

Entra ID 設定

API のアクセス許可 アクセス許可の追加

10. アクセス許可を追加します(右表参照)

API アクセス許可の要求

Microsoft Graph
https://graph.microsoft.com/ ドキュメント

委任済みの許可

アプリケーションの許可

検索できます

右表の値をそれぞれ許可します

クリック

アクセス許可の追加

Microsoft Graph	種類
User.Read	委任済み
User.Read.All	アプリケーション
Group.Read.All	アプリケーション
Device.Read.All	アプリケーション

Entra ID 設定

API のアクセス許可 管理者の同意を与える

Microsoft Graph API を使用して情報を
フェッチするために必要なアクセス許可をアプリ
ケーションに付与する必要があります



11. [{テナント名}]に管理者の同意を与えます をクリックし、ポップアップ画面で[はい]をクリックします

Mist AA IdP | API のアクセス許可

管理者の同意の確認を与えます。

自分の代わりに付与済みのアクセス許可は影響を受け

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。詳細情報

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 に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Device.Read.All	アプリケーション	Read all devices	はい	に付与されて...
Group.Read.All	アプリケーション	Read all groups	はい	に付与されて...
User.Read	委任済み	Sign in and read user profile	いいえ	...
User.Read.All	アプリケーション	Read all users' full profiles	はい	に付与されて...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、エンタープライズ アプリケーションをお試しください。

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Device.Read.All	アプリケー...	Read all devices	はい	に付与されました
Group.Read.All	アプリケー...	Read all groups	はい	に付与されました
User.Read	委任済み	Sign in and read user profile	いいえ	に付与されました
User.Read.All	アプリケー...	Read all users' full profiles	はい	に付与されました

Entra ID 設定

user/group

User を追加します

登録したアプリから user/group 情報を参照できるように設定してください(説明は割愛)



Entra ID 設定

user/group

group を追加します

The screenshot shows the Microsoft Entra ID Groups management console. The main area displays a list of groups with the following columns: 名前 (Name), オブジェクト ID (Object ID), グループの種類 (Group Type), and メンバーシップの種類 (Membership Type). Three groups are listed, all of which are Microsoft 365 groups with assigned membership. The search bar is empty, and the search mode is set to 'Include the following values'.

<input type="checkbox"/>	名前 ↑	オブジェクト ID	グループの種類	メンバーシップの種類
<input type="checkbox"/>	[REDACTED]	d03502d3-76e[REDACTED]	Microsoft 365	割り当て済み
<input type="checkbox"/>	[REDACTED]	f9a2c0c6-7bf0[REDACTED]	Microsoft 365	割り当て済み
<input type="checkbox"/>	[REDACTED]	ec139509-e8c[REDACTED]	Microsoft 365	割り当て済み

Entra ID 設定

Add IDP - Entra ID/OAuth

1. [Organization] から [Identity Providers] をクリックします
2. [Add IDP] をクリックします

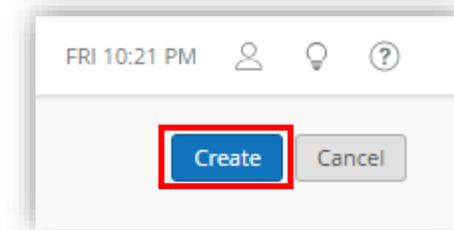
The screenshot displays the Juniper management console interface. On the left, a dark blue sidebar contains navigation items: Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is divided into sections: Admin, Access, WAN, Wired, and Wireless. Under the 'Access' section, 'Identity Providers' is highlighted with a red box. A modal window titled 'Identity Providers' is open, showing a table with columns 'Name', 'IDP Type', and 'Default IDP'. The table is empty, and the text 'There are no identity providers.' is displayed. The 'Add IDP' button in the top right corner of the modal is also highlighted with a red box.

Name	IDP Type	Default IDP
There are no identity providers.		

Entra ID 設定

Add IDP - Entra ID/OAuth

3. Entra ID に追加したアプリを参照し各項目を設定、[Create] をクリックします



アプリの登録

新規登録 > アプリケーション名を設定 > 登録

アプリケーション(クライアント)ID

ディレクトリ(テナント)ID

証明書またはシークレットの追加

証明書とシークレット

新しいクライアントシークレット

説明

有効期限

クライアントシークレット

認証

パブリッククライアントフローを許可する > 保存

APIのアクセス許可

Microsoft Graph

- User.Read - Delegated
- User.Read.All - Application
- Group.Read.All - Application
- Device.Read.All - Application

ユーザ・グループの追加



Name
EntralID

Configuration

IDP type
 LDAPS OAuth Mist Edge Proxy

OAuth Type
Azure

OAuth Tenant ID ⓘ
b7aeraasd-7a68sdjf-asdgvgaadsfaer

Domain Names
.net

Default IDP ⓘ

OAuth Client Credential (CC) Client Id ⓘ
20wefas-df28-9kloaa4e

OAuth Client Credential (CC) Client Secret ⓘ
..... [Reveal](#)

OAuth Resource Owner Password Credential (ROPC) Client Id ⓘ
20wefas-df28-9kloaa4e

[Name] を入力します

[OAuth] を選択します

[Azure] を選択します

[OAuth Tenant ID] を入力します

[Domain Names] を入力します

[OAuth Client Credential(CC) Client Id] を入力します

[OAuth Client Credential(CC) Client Secret] を入力します

[OAuth ROPC Client Id] を入力します



THANK YOU

JUNIPER
NETWORKS®

Driven by
Experience™