Zscaler Private Access(ZPA)

基本操作ガイド

Rev.1.1
2024年 4月

ノックス株式会社

目次

本書について

本書は Zscaler の導入時にスムーズに設定が行えることを目指した導入マニュアルです。

本書は基本的な設定・流れの把握を目的としています。また、難解さを極力避けるようにしていますので、一部内容に関して不足や補足が必要な個所がある場合がありますが、本書の趣旨をご理解の上、ご利用いただきますようお願い申し上げます。

なお、詳細な内容解説については、恐れ入りますが英語版の各種ドキュメントおよびヘルプをご参照くださいますようお願い申し上げます。

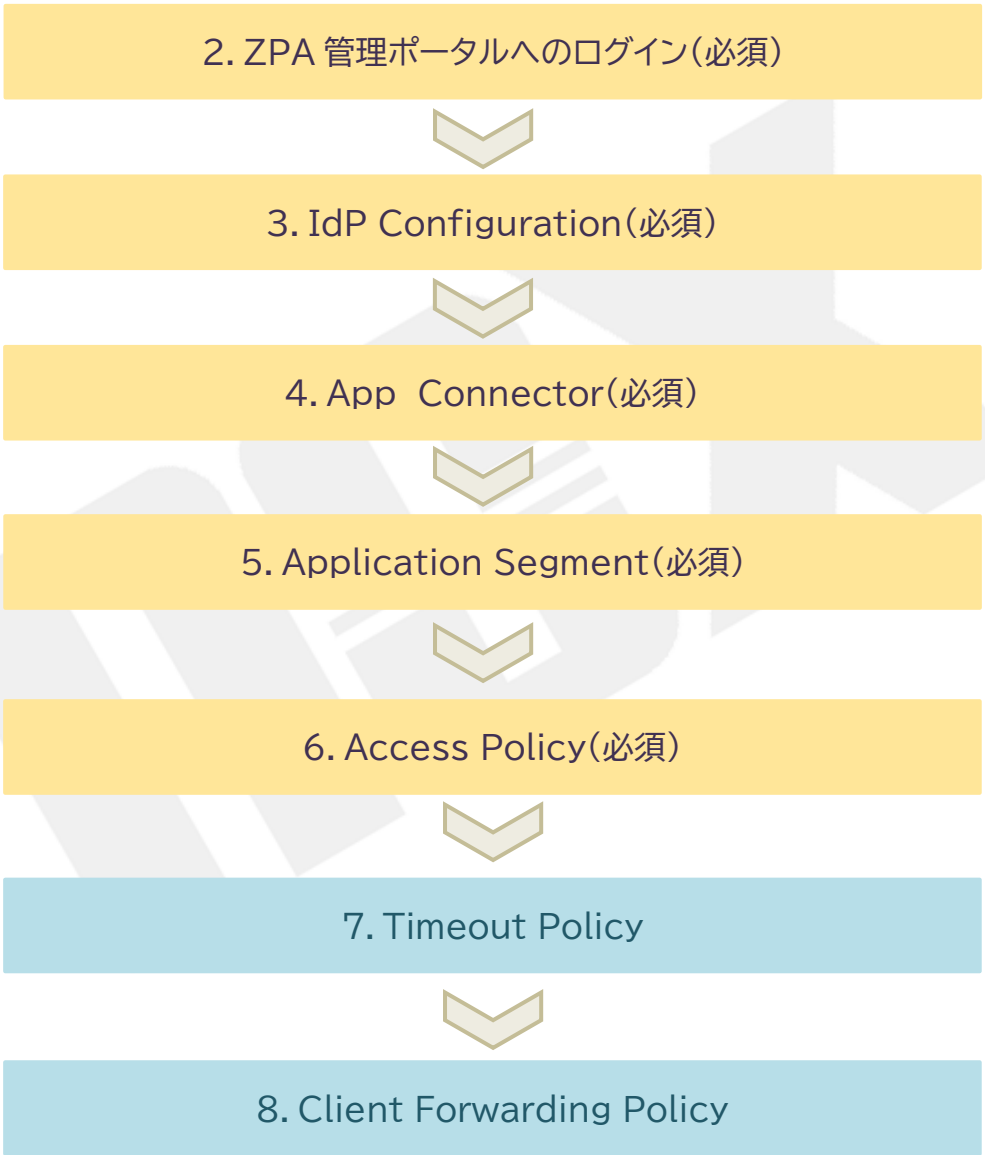
ヘルプページ：https://help.zscaler.com/
通信要件：
https://config.zscaler.com/zscaler.net/zscaler-app
https://config.zscaler.com/private.zscaler.com/zpa

1. ZPA 設定の流れ

1-1. 概要

Zscaler Private Access(ZPA)の基本的な設定手順について説明します。

1-2. ZPA サービス設定フロー



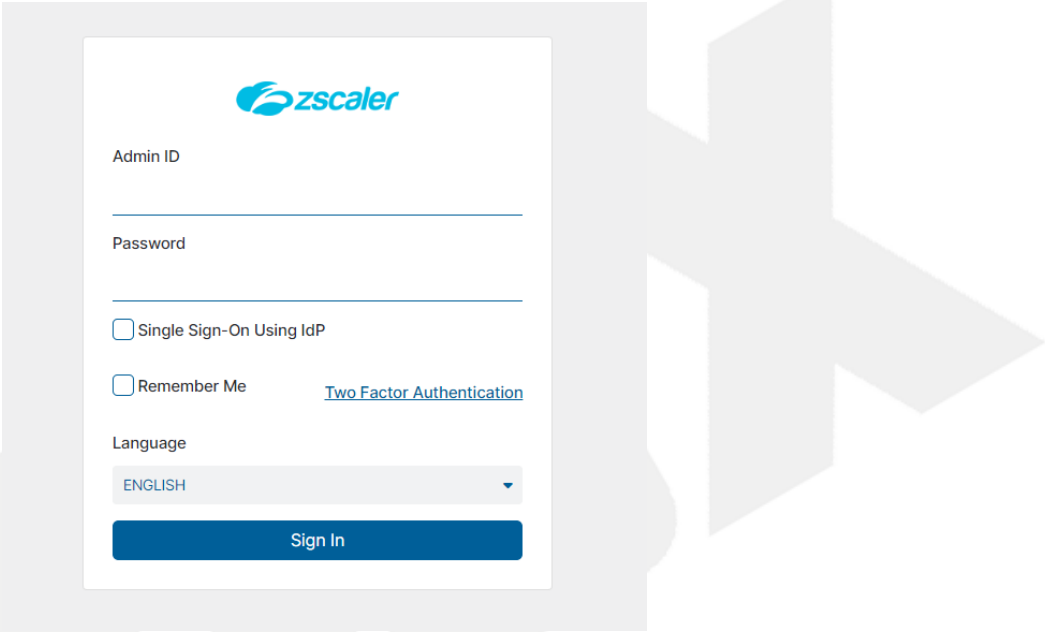
2. ZPA 管理ポータルへのログイン

2-1. 概要

ZPA 管理ポータルへのログイン方法について説明します。

2-2. ZPA 管理ポータルへのログイン方法

(1) 弊社からご連絡したログイン ID、パスワードを使用して、ZPA 管理ポータルへログインをします。
ポータルサイトの URL は「admin.private.zscaler.com」です。



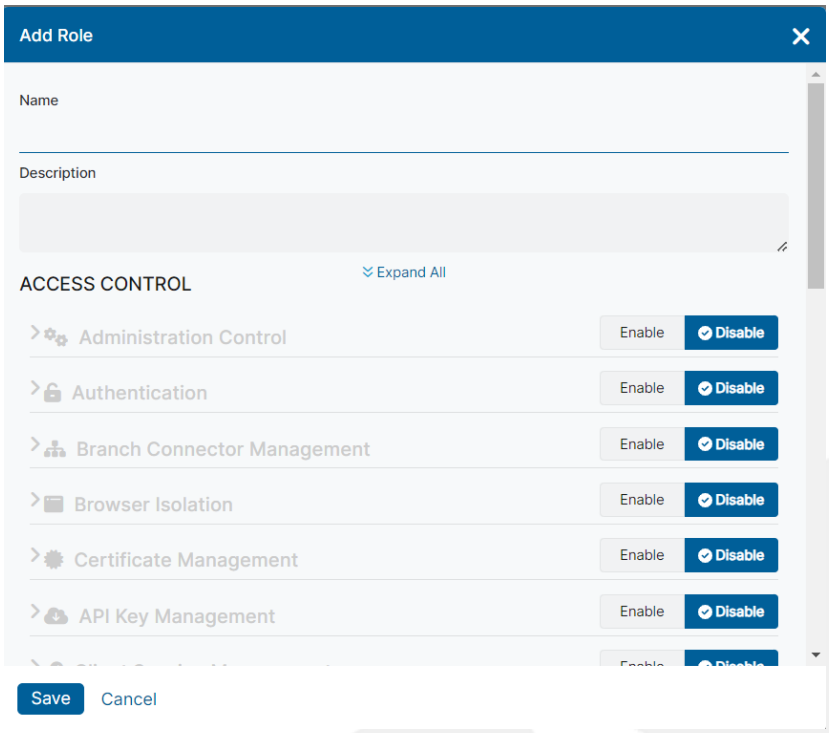
2-3. ZPA 管理ポータルの管理者設定方法

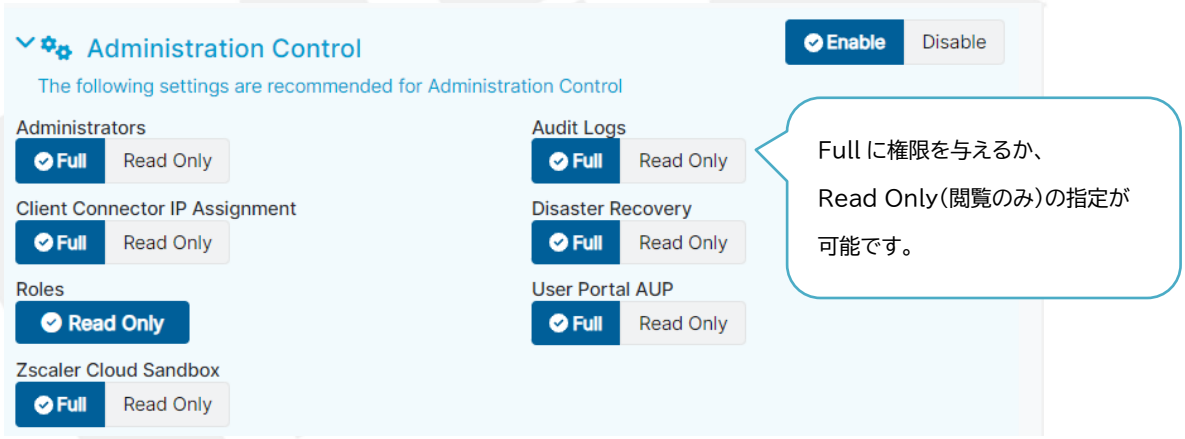
本項では ZPA 管理ポータルにログインをすることができる管理者の設定方法について説明します。

2-3-1. 管理者ロールの設定方法

管理者ロールでは、それぞれの管理者に対してどのような権限を与えるかをロールとして設定します。

(1) ZPA 管理ポータルを開きます。
(2) 左側メニューより、「Configuration Control」>「Administration Control」>「Roles」より管理者に与えられる権限を設定します。
(3) 右上の「Add Role」をクリックします。
(4) それぞれのメニューに対しての権限を設定し、「Save」をクリックします。



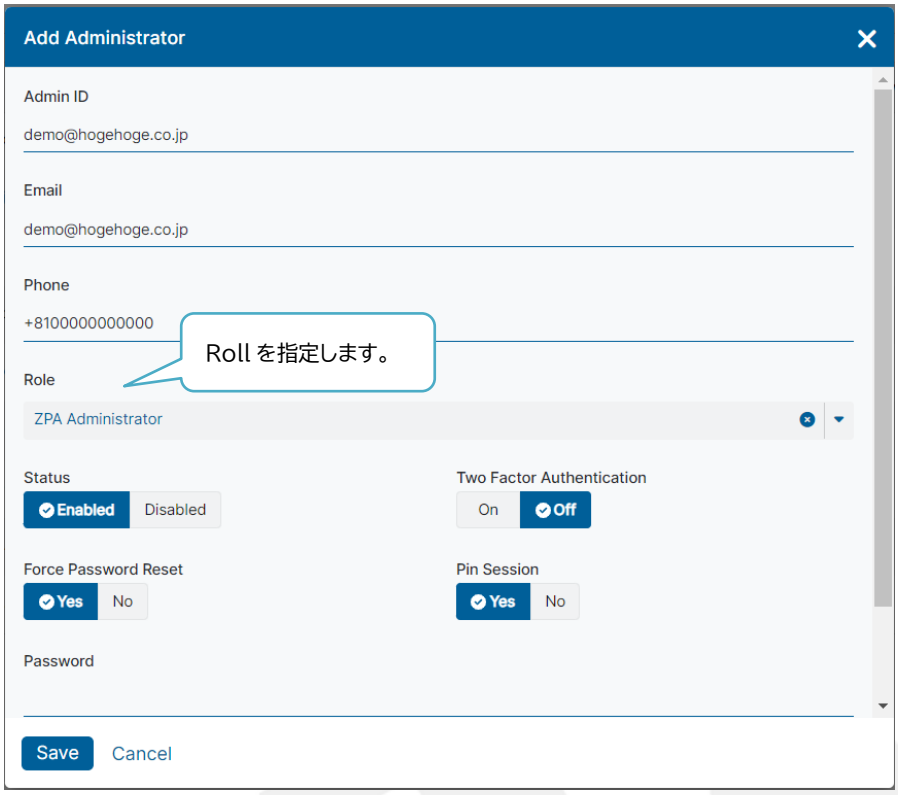


2-3-2. 管理者の追加方法

(1) ZPA ポータルを開き、左側メニュー「Configuration Control」>「Administration Control」>「Administrators」をクリックします。

(2)「Add Administrator」をクリックします。

(3)設定内容を入力し、「Save」をクリックします。


Add Administrator
Admin ID
demo@hogehoge.co.jp
Email
demo@hogehoge.co.jp
Phone
+8100000000000
Roll を指定します。
Role
ZPA Administrator
Status
Enabled
Disabled
Two Factor Authentication
On
Off
Force Password Reset
Yes
No
Pin Session
Yes
No
Password
Save
Cancel

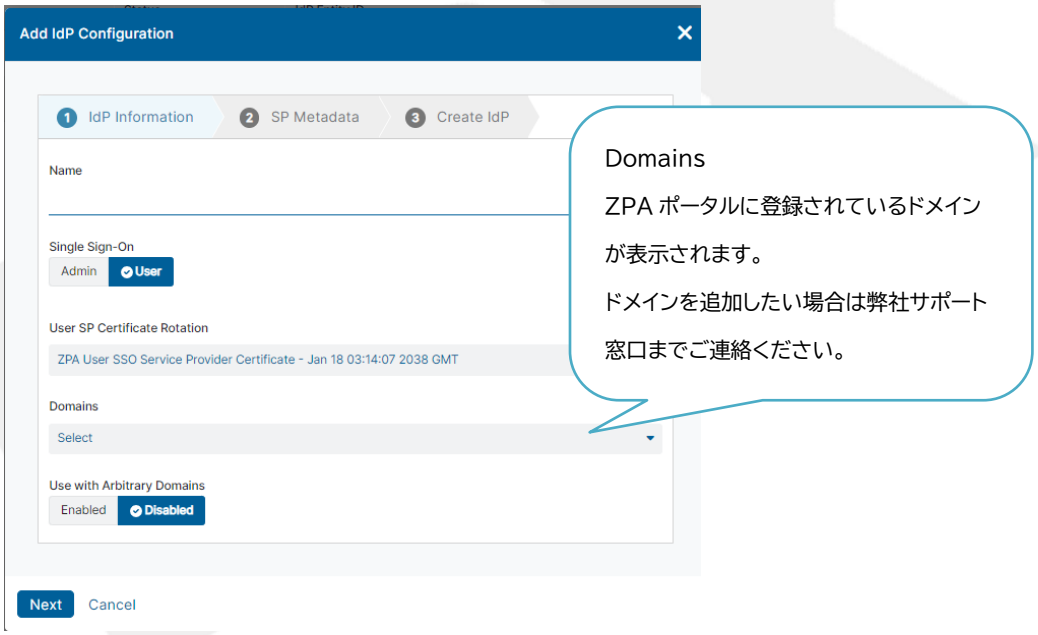
3. IdP Configuration

3-1. 概要

ZPA を利用するためには、SAML 認証が必要となります。
ZPA で SAML 認証を行うにあたり、ご利用の IdP との連携のための設定が必要です。
本項では IdP の設定方法について説明します。

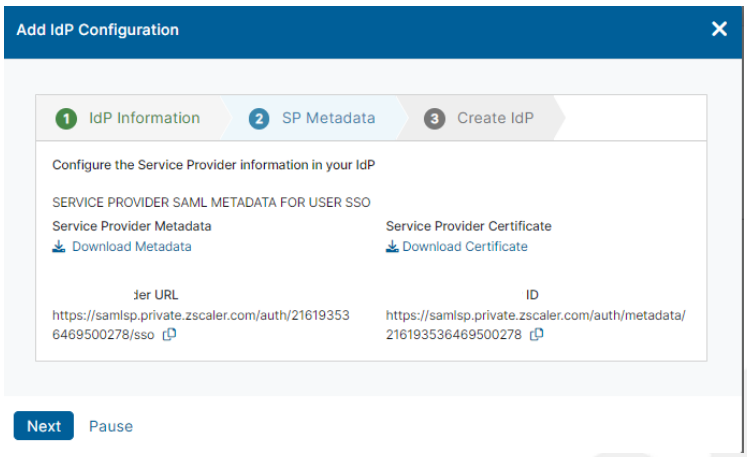
3-2. IdP の設定方法

(1) ZPA ポータルを開き、左側メニュー「Authentication」>「User Authentication」>「IdP Configuration」をクリックします。
(2)「Add IdP Configuration」をクリックします。
(3)必要事項を入力し、「Next」をクリックします。

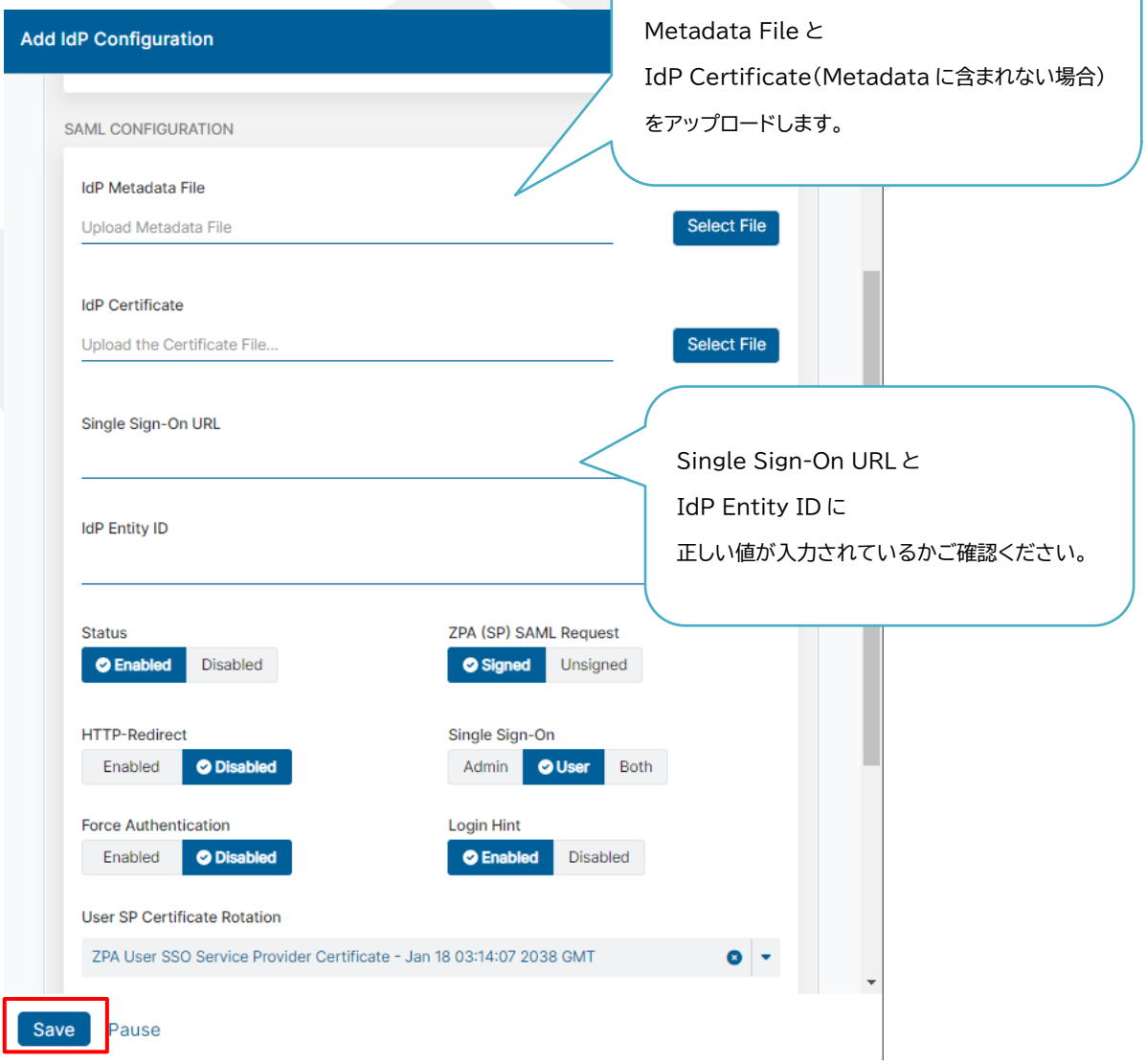


Name：半角英数で入力します。
Single Sign-On：ユーザー認証用か、管理ポータルにログインをする管理者の認証用かを選択します。
Domains：認証に利用をするドメインを選択します。

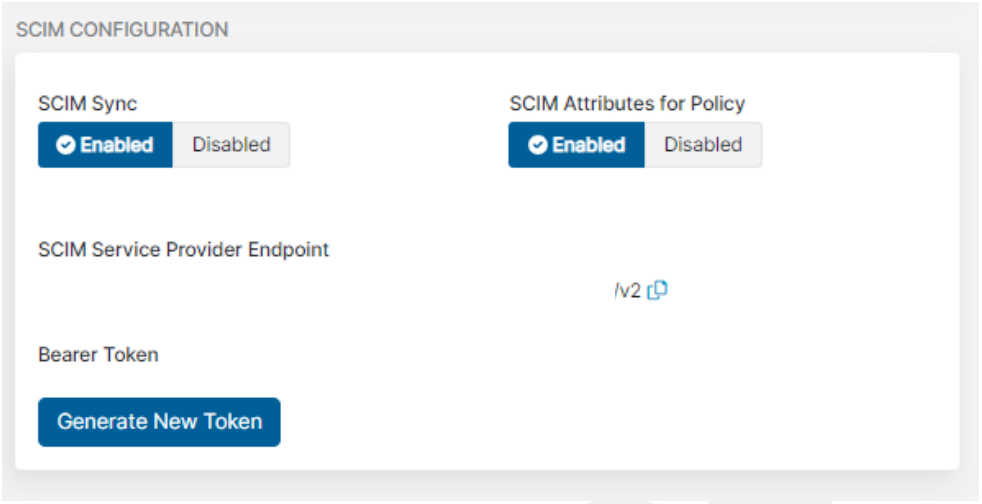
（4）IdP 側での設定が必要な、Metadata や Service Provider URL 等が表示されるので、情報を控えて、「Pause」をクリックします。
ご利用の IdP 側で控えた情報の設定が必要です。



（5）各設定項目を入力し、「Save」をクリックします。



ご利用の IdP 側が SCIM に対応している場合は、SCIM の利用が可能です。
SCIM を利用する場合は下記設定を有効にご設定ください。



「SCIM Service Provider Endpoint」の情報を控えます。
「Generate New Token」をクリックし、トークンを発行後 IdP 側での設定が必要となります。

4. App Connector

4-1. 概要

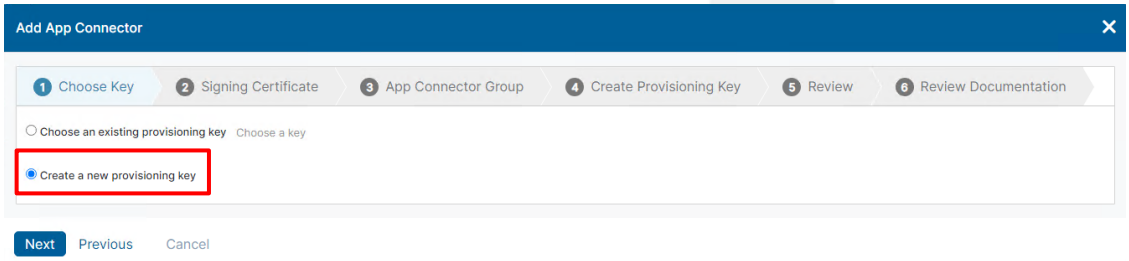
本項では App Connector の設定方法について説明します。

4-2. Provisioning Key の作成

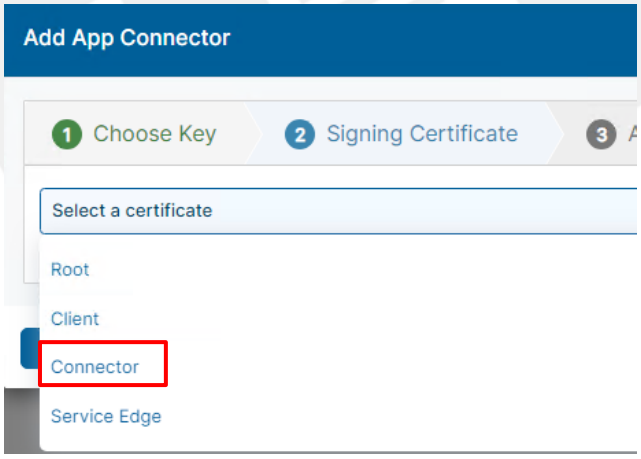
(1) ZPA ポータルを開き、左側メニュー「Configuration＆Control」>「Private Infrastructure」>「App Connectors」をクリックします。

(2)「Add App Connector」をクリックします。

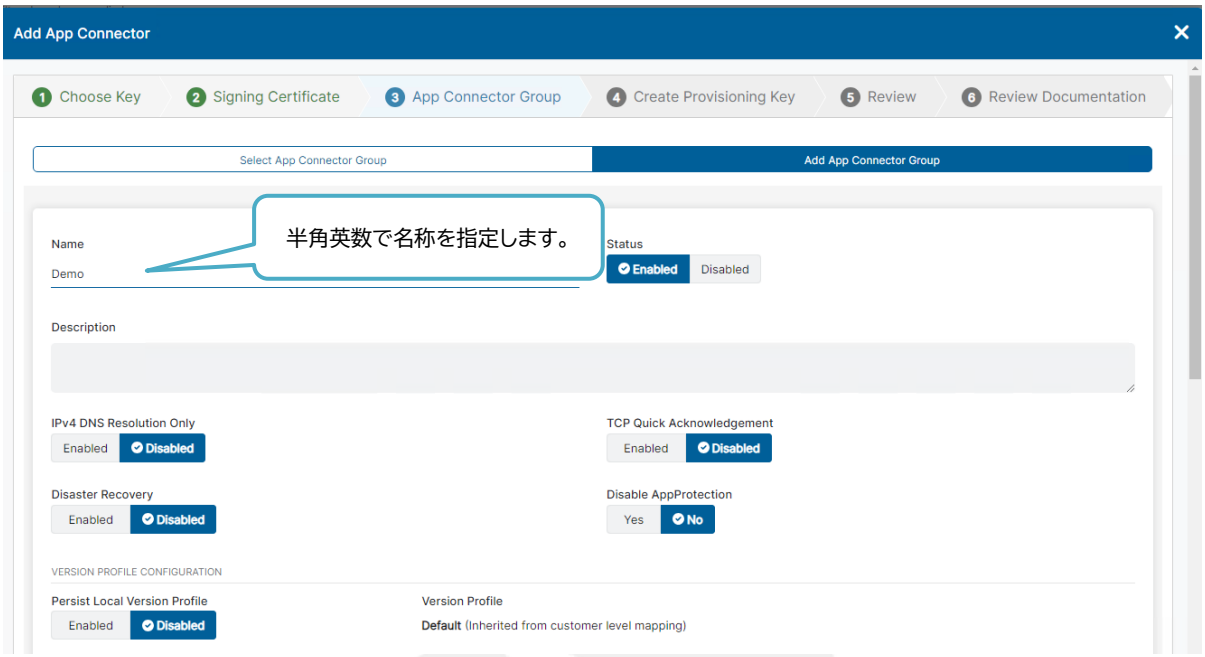
(3)「Create a new provisioning key」を選択し、「Next」をクリックします。

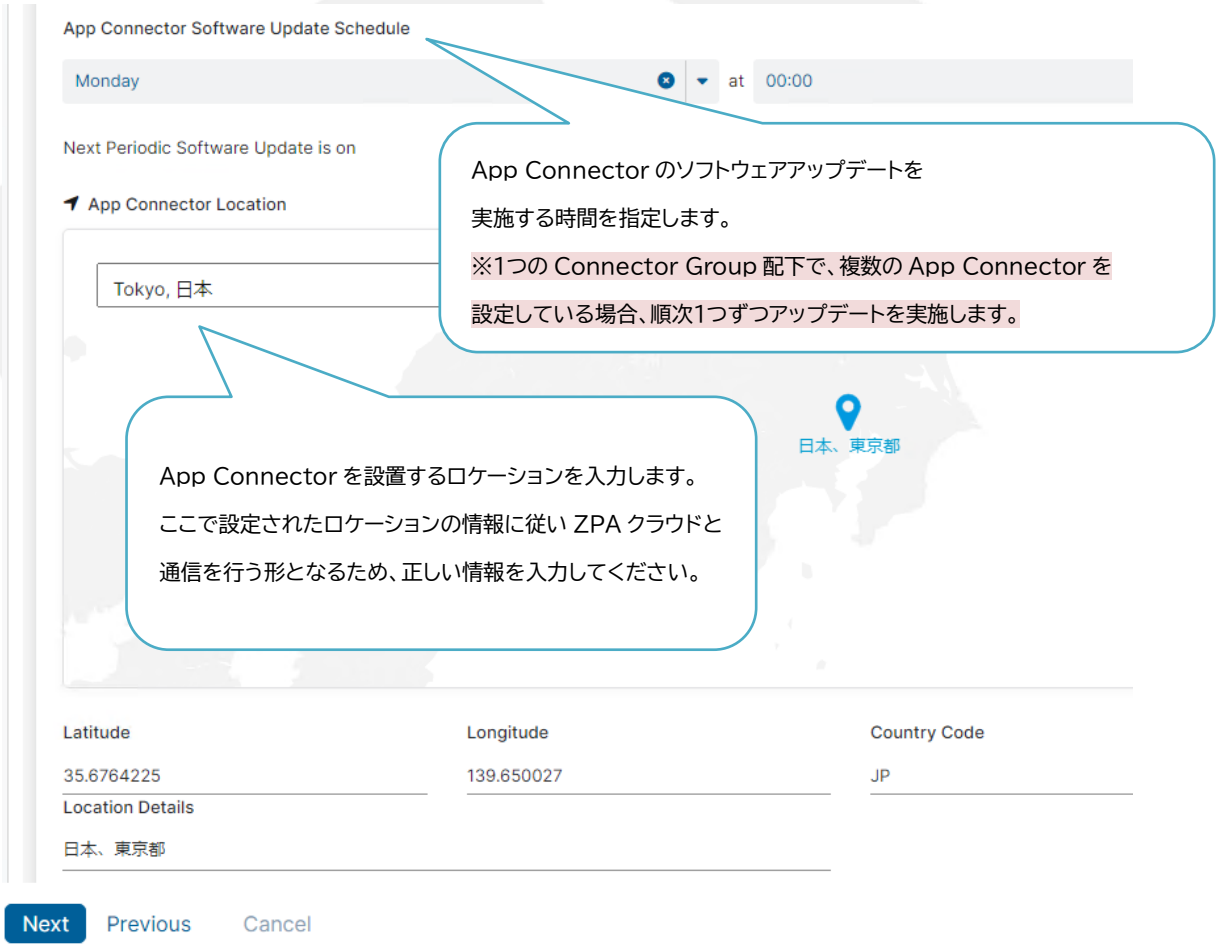


(4)「Select a certificate」のプルダウンを開き「Connector」を選択し、「Next」をクリックします。



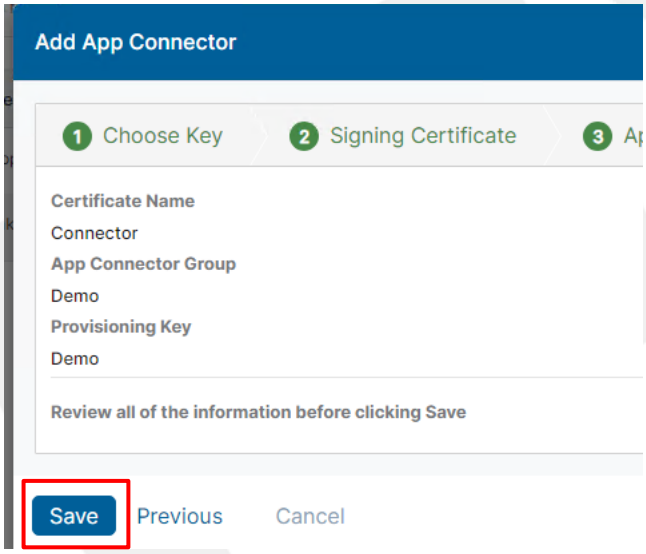
（5）「Add Connector Group」のタブを選択し、各設定項目を入力し「Next」をクリックします。





（6）Provisioning Key の名称を定義します。

（7）内容を確認の上、「Save」をクリックします。



（8）Provisioning Key が表示されるので、メモ帳などに控えておきます。

4-3. App Connector の作成

本項ではApp Connectorの作成方法について説明します。
本書では例として Vmware プラットフォームに App Connector の作成を実施しています。
サポートプラットフォームは下記の通りです。

サポートプラットフォーム
-Amazon Web Service（AWS）
-CentOS

-Oracle
-Redhat
-Microsoft Azure
-Microsoft Hyper−V
-Vmware アプライアンス(Vmware vCenter)
-Vmware アプライアンス（vSphere Hypervisor (ESXi)）
-Nutanix
-Docker
-Openshift

4-3-1. App Connector のデプロイ

App Connector を各プラットフォームの手順に従ってデプロイします。
各プラットフォームのデプロイの手順に関しましては下記URLをご確認ください。

AmazonWeb Services(AWS)
https://help.zscaler.com/zpa/connector-deployment-guide-amazon-web-services

CentOS, Oracle, Red Hat
https://help.zscaler.com/zpa/connector-deployment-guide-centos-oracle-and-redhat

Microsoft Azure
https://help.zscaler.com/zpa/connector-deployment-microsoft-azure

Microsoft Hyper-V
https://help.zscaler.com/zpa/connector-deployment-guide-microsoft-hyper-v

VMware
https://help.zscaler.com/zpa/connector-deployment-guide-vmware-platforms

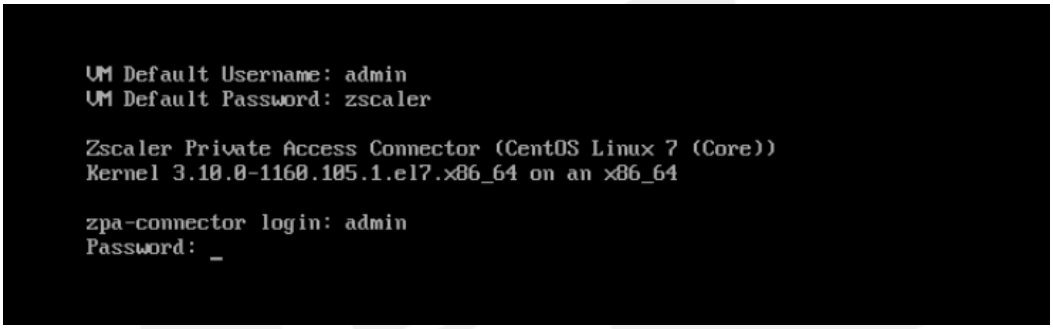
Nutanix
https://help.zscaler.com/zpa/app-connector-deployment-guide-nutanix-ahv

Docker
https://help.zscaler.com/zpa/app-connector-deployment-guide-docker

OpenShift
https://help.zscaler.com/zpa/app-connector-deployment-guide-openshift

4-3-2. App Connector コンソールへのログイン

App Connector コンソールへログインをします。
デフォルトのユーザー名とパスワードは以下の通りです。



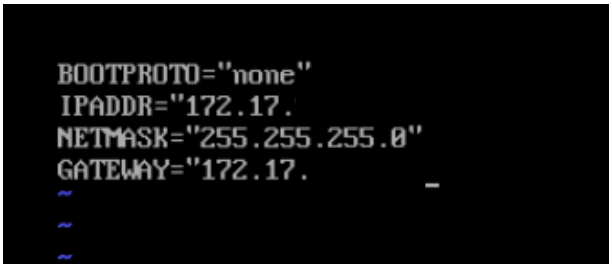
Username：admin
Password：zscaler

4-3-3. ネットワークアドレスの設定

ネットワークアドレスの設定を行います。

(1) スタティック IP の場合、「sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0」を実行し、ネットワークの設定を下記のように書き換えます。

BOOTPROTO=”none”
IPADDR=“xxx.xxx.xxx.100”（App Connector の IP）
NETMASK=”255.255.255.0”
GATEWAY=“xxx.xxx.xxx.254”（デフォルトゲートウェイの IP）

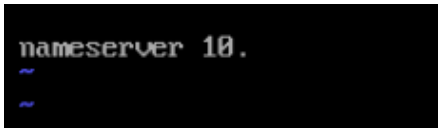


(2)「sudo systemstl restart network」を実行し、ネットワーク設定を再起動します。

4-3-4. DNS サーバーの設定

DNS サーバーの設定を行います。

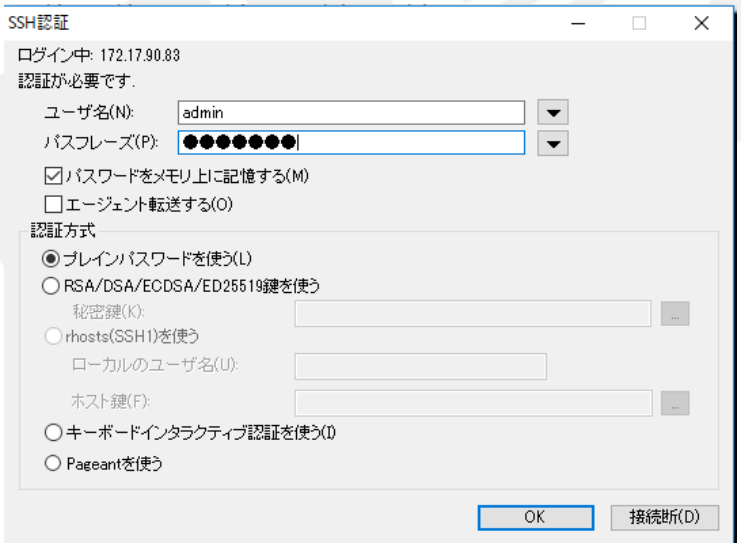
(1)「sudo vi /etc/resolv.conf」を実行し、参照先の DNS サーバーを下記のように指定します。
nameserver xxx.xxx.xxx.xxx(任意のアドレス)



4-3-5. Provisioning Key の適用

ZPA ポータル側で作成をした Provisioning Key を App Connector に適用します。

(1)「sudo systemctl start sshd」を実行し、SSH を起動させ、SSH にて管理アクセスを実施します。



(2)「sudo systemctl stop zpa-connector」を実行し、App Connector を一時停止します。

(3)下記2つのコマンドを実行します。
「sudo touch /opt/zscaler/var/provision_key」
「sudo chmod 644 /opt/zscaler/var/provision_key」

(4)「sudo vi /opt/zscaler/var/provision_key」を実行し、発行された Provisioning Key をコピー＆ペーストします。

(5)「sudo cat /opt/zscaler/var/provision_key」を実行し、Provisioning Key の内容が正しいかを確認します。

(6)「sudo systemctl start zpa-connector」を実行し、App Connector を起動します。

(7)「sudo systemctl status zpa-connector」を実行し、ステータスが「Active」になっていることを確認します。

(8)ZPA 管理ポータル内、「Configuration＆Control」>「Private Infrastructure」>「App Connectors」にて作成した App Connector が追加されていることを確認します。

5. Application Segment

5-1. 概要

ZPA の対象としたいアプリケーションを登録したものを「Application Segment」と呼んでいます。

本項では「Application Segment」の設定方法について説明します。

5-2. Application Segment の作成

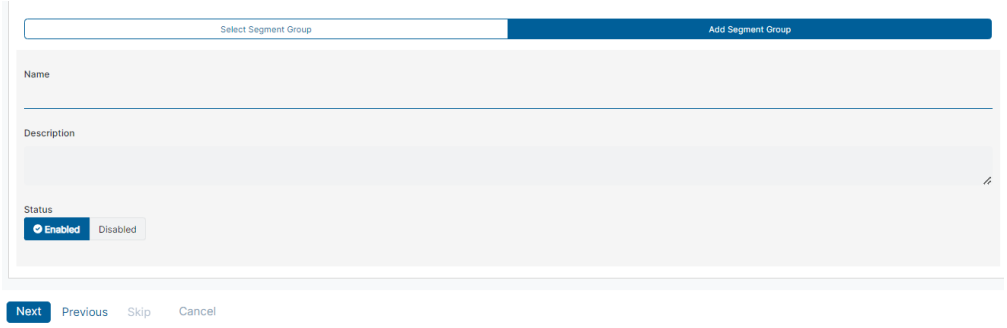
Application Segment の作成方法について説明します。

(1) ZPA 管理ポータルを開き、「Resource Management」>「Application Management」>「Application Segments」をクリックします。

(2)「Add Application Segment」をクリックします。

(3)各種設定を入力し、「Next」をクリックします。

（4）「Add Segment Group」のタブを選択し、各種設定を入力し、「Next」をクリックします。
ここでは Application Segments に紐づける「Segment Group」を定義します。
Segment Group を指定したポリシーの作成が可能です。



(5)「Add Server Group」のタブを選択し、各種設定を入力し、「Next」をクリックします。
ここでは、「Server Group」を定義します。

(6)設定内容を確認し、「Save」をクリックします。

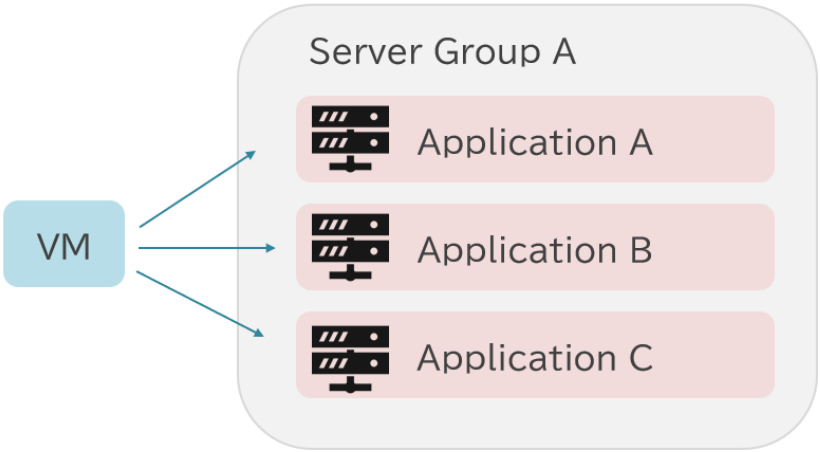
5-3. 【補足】Server Group/Servers の推奨設定

5-3-1. 推奨設定

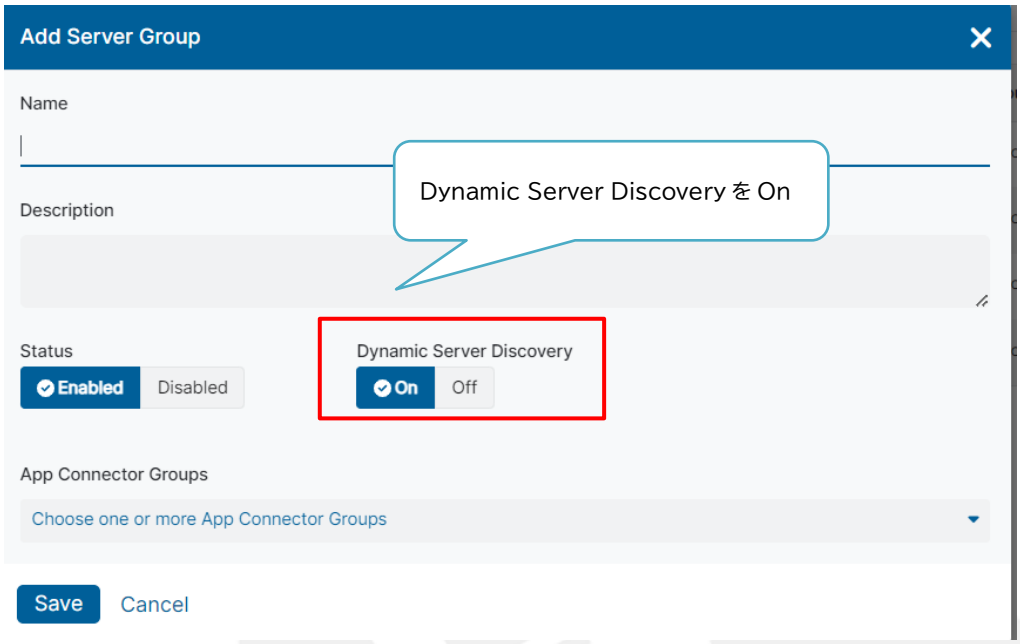
複数のサーバーやアプリケーションに接続をする場合、「Server」単体を設定せず、「Dynamic Server Discovery」を有効化した Server Groups を設定します。
基本的に「Servers」の設定は使用しません。

Dynamic Server Discovery を有効にすることで IP アドレスでの指定や FQDN に加えてワイルドカードを使用することが可能となります。

(例)複数のサーバーやアプリケーションにアクセスする構成



(1) ZPA ポータルを開き、左側メニュー「Configuration＆Control」をクリックし、「Server Groups」をクリックします。
(2)「Add Server Groups」をクリックします。
(3)設定内容を入力し、「Save」をクリックします」

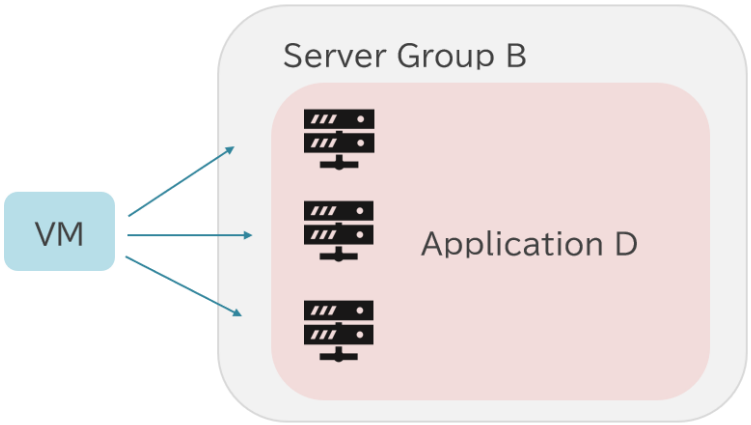


※「Server Groups」の追加は、「Application Segment」作成時でも可能です。

5-3-2. 例外設定

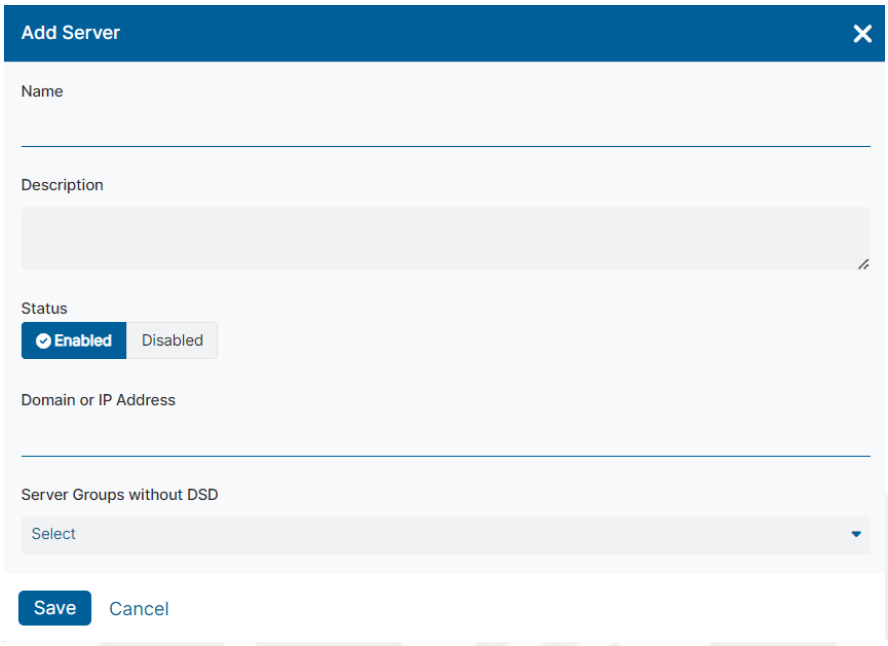
基本的に「Servers」の設定は利用しませんが、下記のような構成の場合は「Servers」に各サーバーのアドレスを登録します。

(例)単一のアプリケーションを複数のサーバーで構成している場合



「Servers」に各サーバーのアドレスを登録し、「Server Group」にて登録済みの各サーバーを指定することで、App Connector 側でロードバランシングを行うことが可能です。

(1) ZPA ポータルを開き、左側メニュー「Configuration＆Control」をクリックし、「Servers」をクリックします。
(2)「Add Server」をクリックします。
(3)設定内容を入力し、「Save」をクリックします



(4)ZPA ポータルを開き、左側メニュー「Configuration＆Control」をクリックし、「Server Groups」をクリックします。
(5)「Add Server Groups」をクリックします。
(6)「Dynamic Server Discovery」を Disable に変更の上、設定内容を入力し、「Save」をクリックします

6. Access Policy

6-1. 概要

ZPA 経由でのアクセスを実現するために、作成した Application Segment に対してのアクセス制御用のポリシーの作成が必要です。
本項では Access Policy の設定方法について説明します。

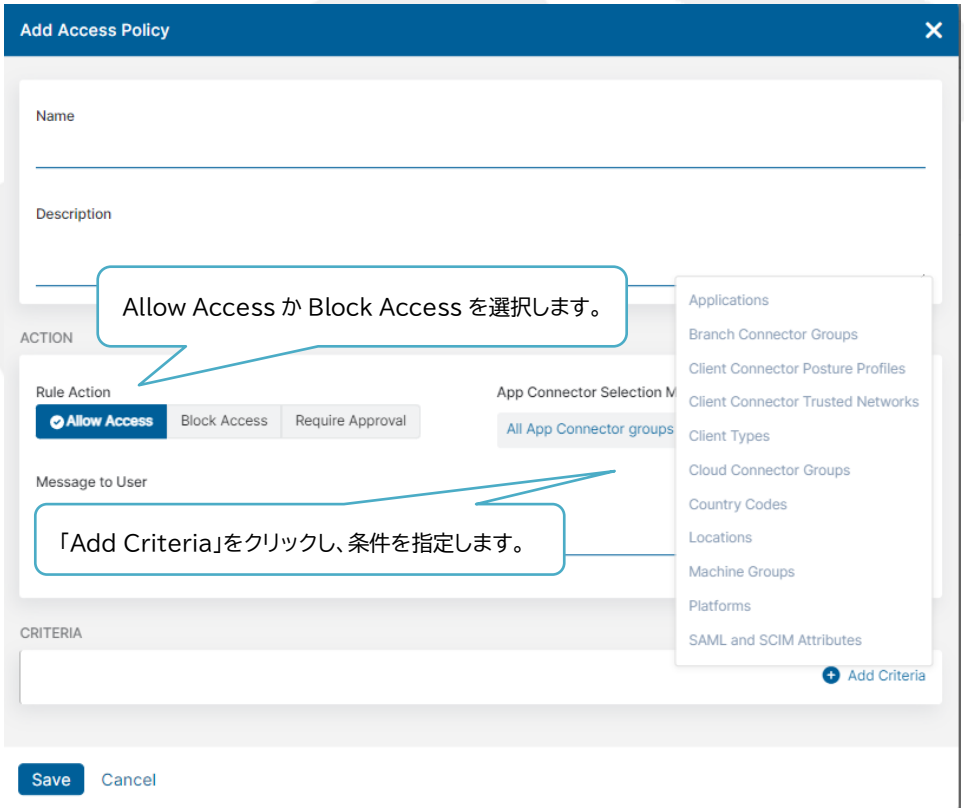
6-2. Access Policy の作成

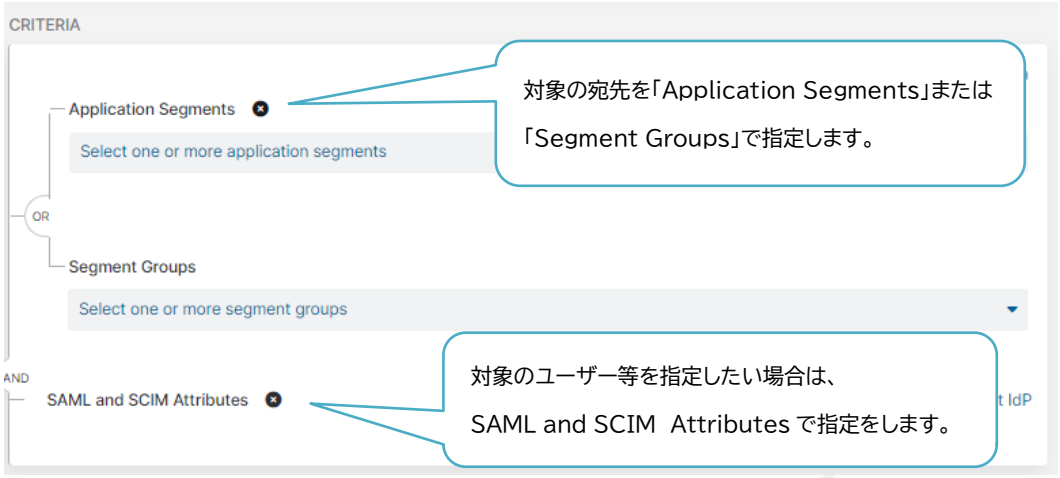
Access Policy の作成方法について説明します。

(1) ZPA 管理ポータルを開き、左側メニュー「Policy」>「Access Policy」をクリックします。

(2)「Add Rule」をクリックします。

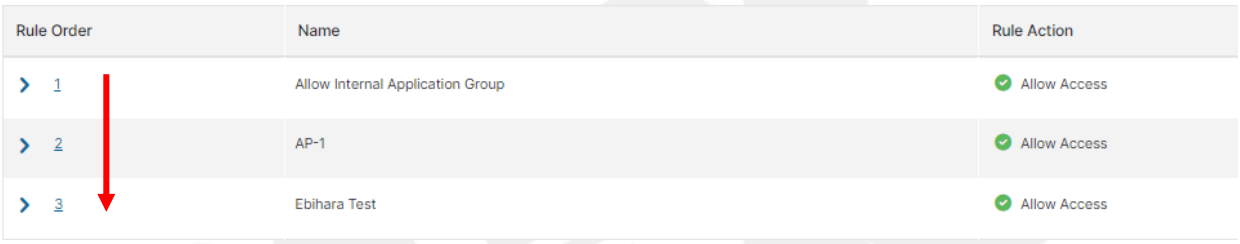
(3)設定内容を入力し「Save」をクリックします。





6-3. 【補足】ポリシーの Rule Order について

ポリシーは「Rule Order」が若い順に評価されます。



左側の数字をクリックし、任意の数字を入力することで Rule Order の順番を変更することが可能です。

7. Timeout Policy

7-1. 概要

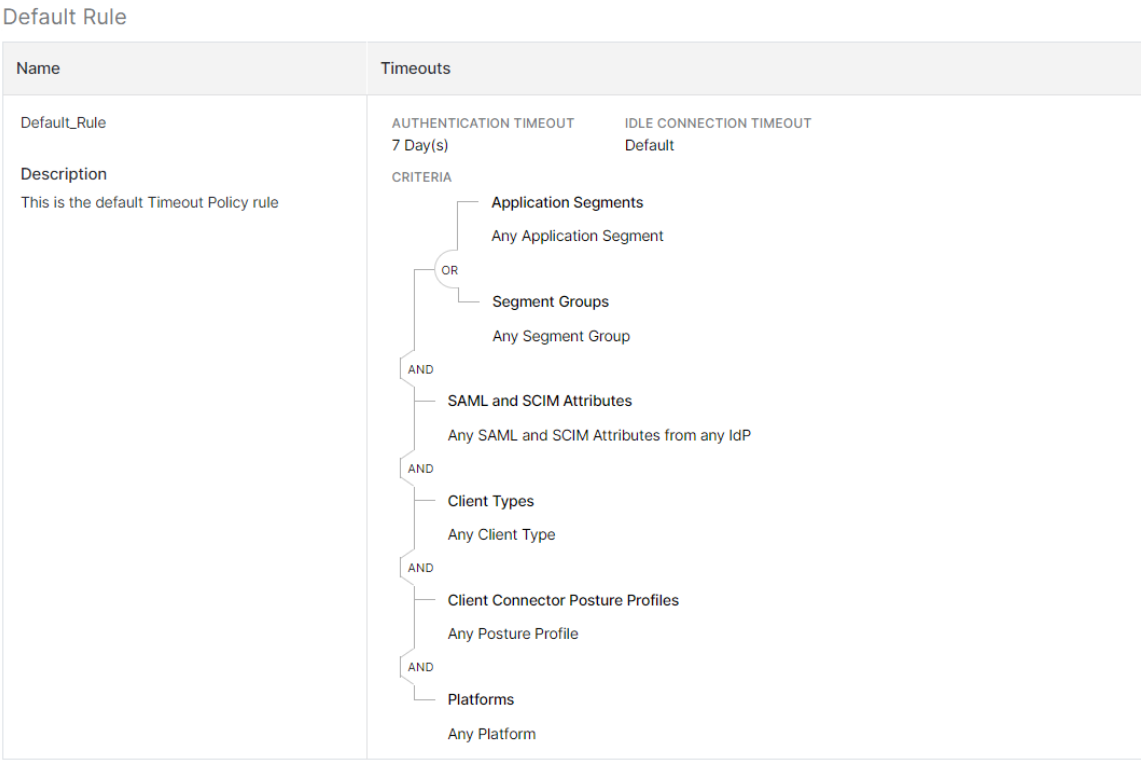
ZPA はリモートアクセスを実現するための製品なので、機密性の高い情報にアクセスをする場合があります。そのため、一定の期間ごとに再認証を求めるためのポリシーを Timeout Policy を作成することで定義することが可能です。

本項では Timeout Policy の設定方法について説明します。

7-2. Default Timeout Policy

ZPA 側で用意されているデフォルトのタイムアウトポリシーは 7 日間で設定されています。

最後に ZPA で認証を行ってから 7 日経過後に ZPA の対象の宛先にアクセスをした際に再認証が求められる動作となります。



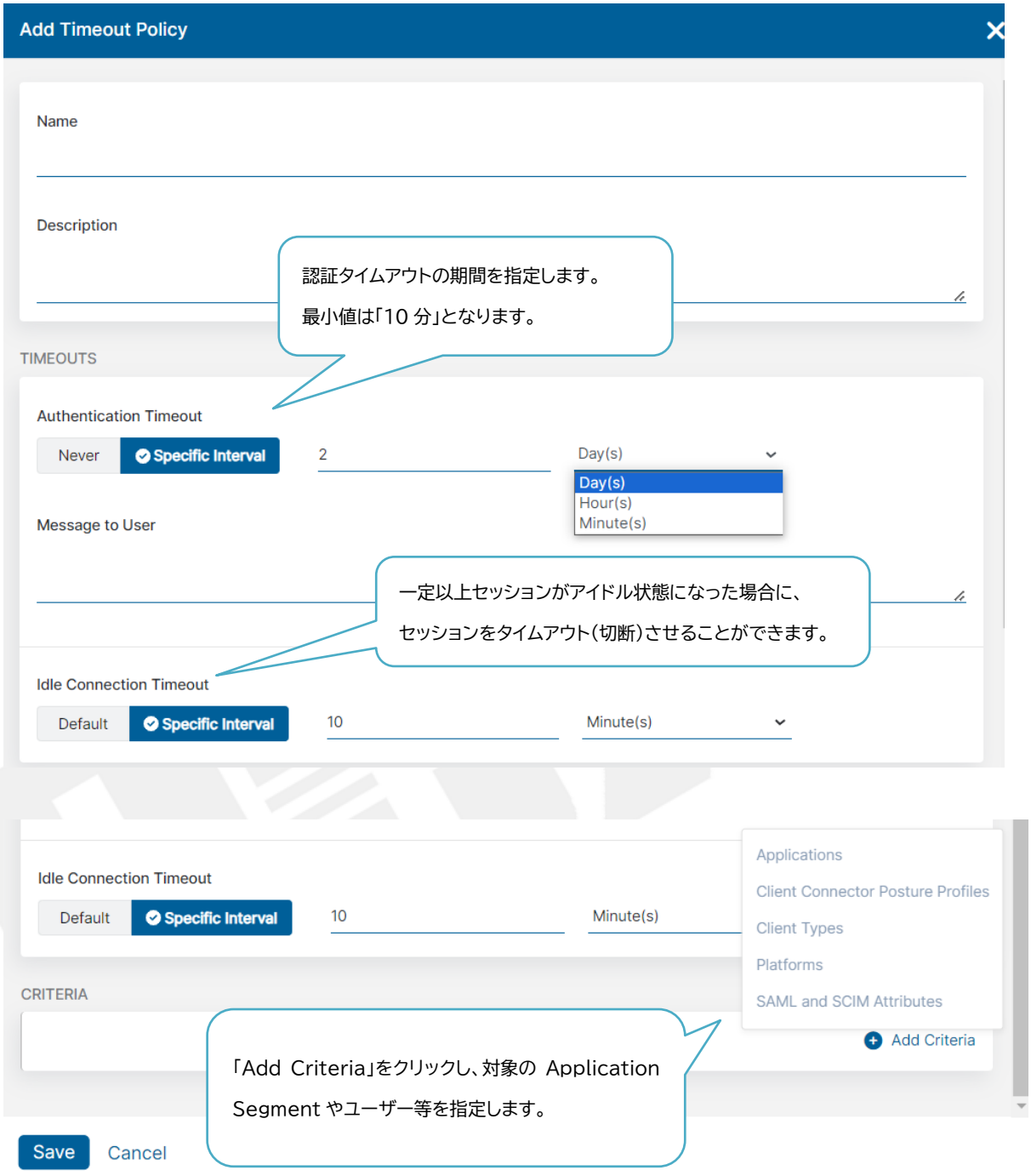
7-3. Timeout Policy の作成

Timeout Policy の作成方法について説明します。

(1) ZPA ポータルを開き、左側メニュー「Policy」>「Timeout Policy」をクリックします。

(2)「Add Rule」をクリックします。

（3）設定内容を入力し「Save」をクリックします。



8. Client Forwarding Policy

8-1. 概要

Client Forwarding Policy は ZPA から除外したい宛先がある場合に利用するためのポリシーとなります。ZPA から除外をしたい宛先がある場合は、下記の手順で設定を行います。

(1) 除外をしたい対象の宛先を登録した Application Segments を作成する

(2) 上記(1)で作成をした Application Segments を指定した Client Forwarding Policy を作成する

本項では、Client Forwarding Policy の設定方法について説明します。

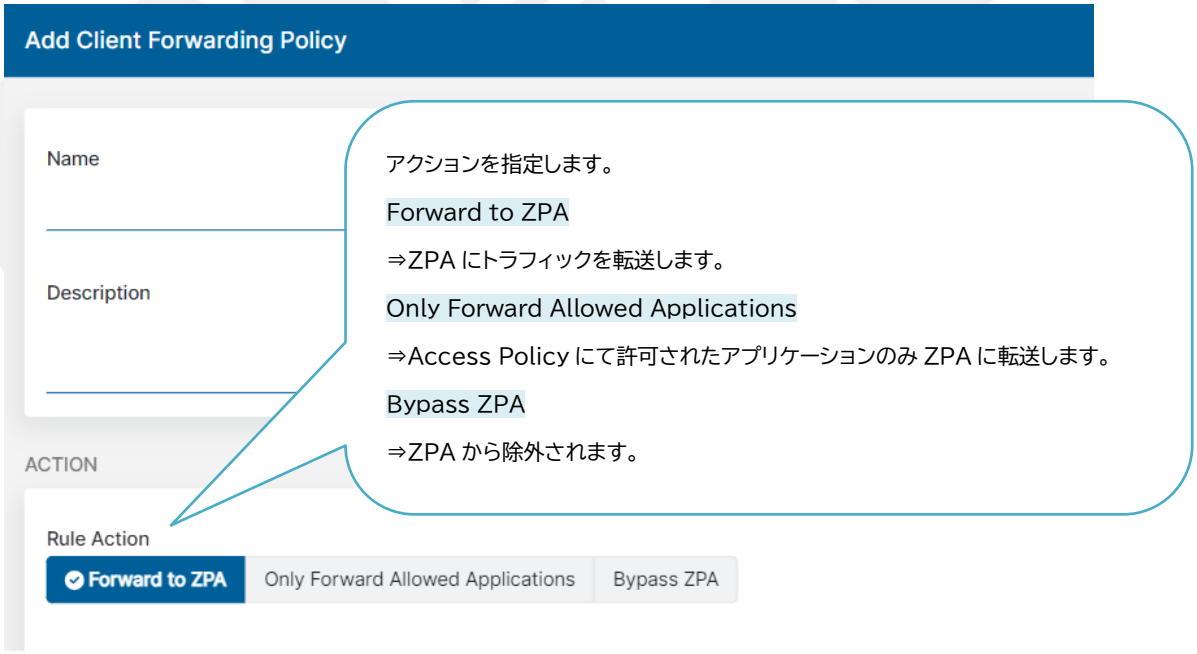
8-2. Client Forwarding Policy の作成

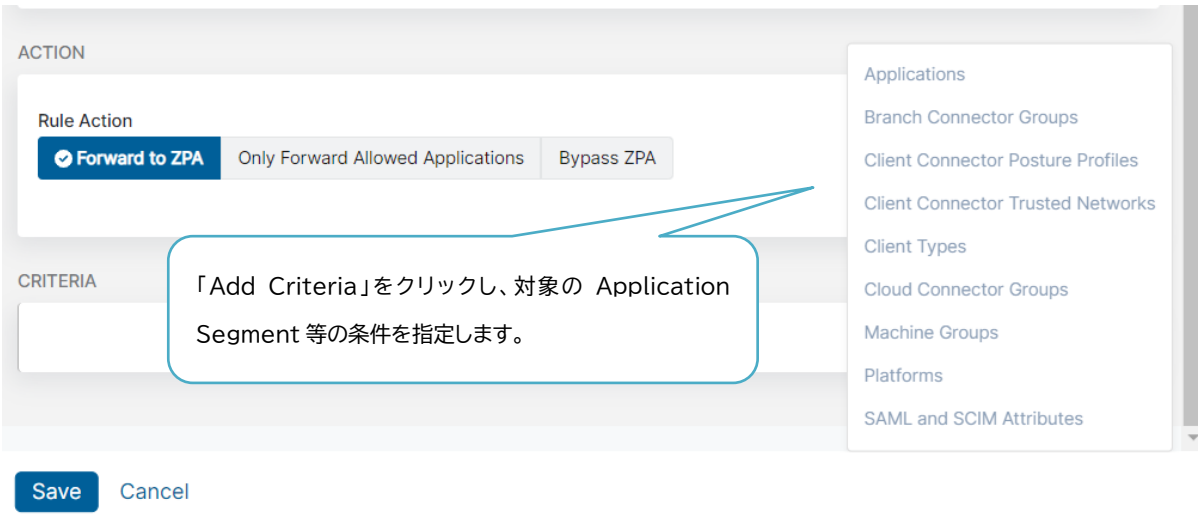
Client Forwarding Policy の作成方法について説明します。

(1) ZPA ポータルを開き、左側メニュー「Policy」>「Client Forwarding Policy」をクリックします。

(2)「Add Rule」をクリックします。

(3) 設定内容を入力し「Save」をクリックします




ACTION
Rule Action
Forward to ZPA
Only Forward Allowed Applications
Bypass ZPA
CRITERIA
「Add Criteria」をクリックし、対象の Application Segment 等の条件を指定します。
Applications
Branch Connector Groups
Client Connector Posture Profiles
Client Connector Trusted Networks
Client Types
Cloud Connector Groups
Machine Groups
Platforms
SAML and SCIM Attributes

Save
Cancel