



Zscaler Client Connector(ZCC) 基本操作ガイド

Rev.1.1

2023年 10月

ノックス株式会社



- ※ 本出版物の著作権はノックス株式会社が権利を保有しています。本出版物の配布は、Zscaler サービスのサブスクリプション購入者による使用のみを目的としています。
- ※ 本出版物中に用いられている商標については、全て該当する会社が権利を保有しています。
- ※ 当社の許可なく、本出版物の複製・転載・配布を禁じます。
- ※ 本出版物は無保証で提供されるものであり、当社は本製品についてその商品性、特定の目的に対する適合性、使用による権利侵害の不発生を保証するものではなく、かつこれに限定されずいかなる事項についても明示的または暗示的に保証しません。
- ※ 本出版物には技術的内容に関して不適切な部分および誤植部分が含まれている恐れがあります。当社は事前の通知なく本出版物の内容を改訂する場合があります。
- ※ クラウド側のバージョンアップにより設定項目が追加、変更される可能性があります。予めご了承の程お願いいたします。

Copyright(C)2023ノックス株式会社

目次

1. ZCC 設定の流れ	6
1-1. 概要	6
1-2. ZCC サービス設定フロー	6
2. ZCC 管理ポータルへのログイン	7
2-1. 概要	7
2-2. ZCC ポータルへのログイン方法	7
2-2-1. ZIA ポータルからのアクセス方法	7
2-2-2. ZPA ポータルからのアクセス方法	7
3. FORWARDING PROFILE	9
3-1. 概要	9
3-2. ON TRUSTED NETWORK(社内ネットワーク)の設定	9
3-3. ドライバーの設定	10
3-4. ZIA のトラフィック転送方法の設定	11
3-4-1. トラフィック転送方法の種類	11
3-4-2. ネットワークの種類	12
3-4-3. トラフィック転送方法の設定手順	13
4. APP PROFILE	14
4-1. 概要	14
4-2. APP PROFILE の設定方法	14
5. CLIENT CONNECTOR APP STORE	19
5-1. 概要	19
5-2. ZCC インストーラーのダウンロード方法について	19
5-3. GA 版と限定版の違いについて	19
5-4. 自動アップデートの設定方法について	20
6. 端末の ZCC 画面について	22
6-1. 概要	22
6-2. ZCC の画面について	22
7. ENROLLED DEVICES	24

7-1. 概要	24
7-2. DEVICE OVERVIEW	24
7-3. 「REMOVE」について	24
7-3-1. Remove の手順について	24
8. CLIENT CONNECTOR SUPPORT	26
8-1. 概要	26
8-2. APP FAIL OPEN	26
8-2-1. 設定方法について	26
8-3. DEVICE CLEANUP	27
8-3-1. 設定方法について	27
8-4. ADVANCED CONFIGURATION	28
8-4-1. 手順について	28
9. インストールオプションについて	29
9-1. 概要	29
9-2. 指定可能なインストールオプションについて	29
10. ポリシーアップデートの間隔	32
10-1. 概要	32
10-2. ポリシーアップデートの間隔について	32
11. バイパス設定	33
11-1. 概要	33
11-2. 手順について	33
11-2-1. Z-Tunnel1.0	33
11-2-2. Z-Tunnel2.0	34

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>

1. ZCC 設定の流れ

1-1. 概要

Zscaler Internet Access(ZIA)サービスの利用手順を説明します。

1-2. ZCC サービス設定フロー

2. ZCC 管理ポータルへのログイン(必須)



3. Forwarding Profile(必須)



4. App Profile(必須)



5. Client Connector Store(ZCC のインストール) (必須)



8. Client Connector Support

2. ZCC 管理ポータルへのログイン

2-1. 概要

ZCC 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. ZCC ポータルへのログイン方法

ZCCポータルへはご利用のZIAポータル、またはZPAポータルからアクセスをします。

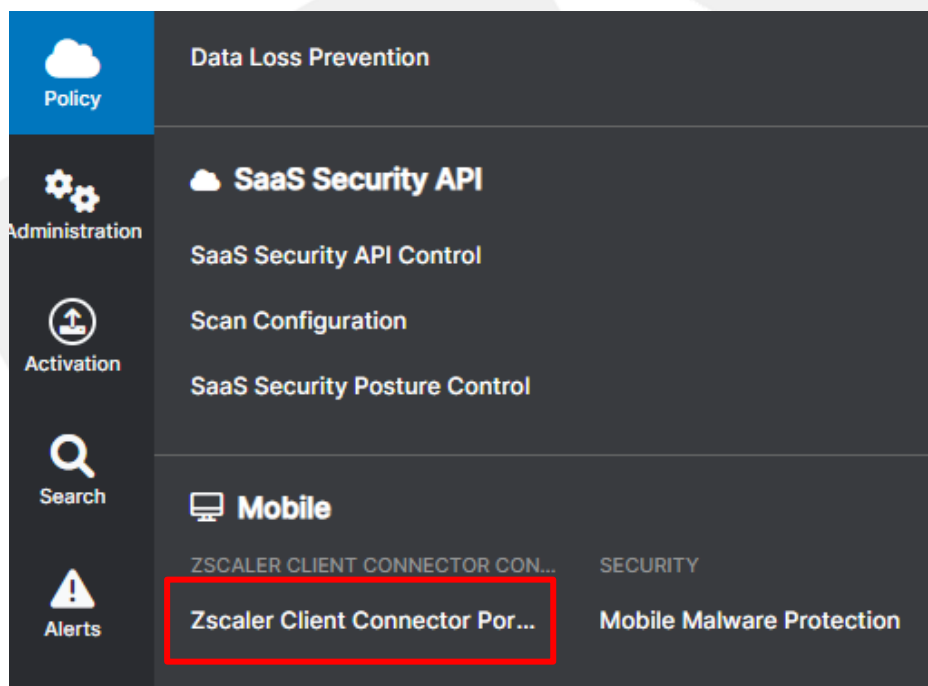
2-2-1. ZIA ポータルからのアクセス方法

(1) ZIA 管理ポータルを開きます。

ポータルサイトの URL は「admin.zscalerthree.net」(※)です。

admin.zscalerthree.net の赤字部分はご契約のクラウド名を入力してください。

(2) 左側メニューより「ポリシー」→「Zscaler Client Connector Portal」を選択します。

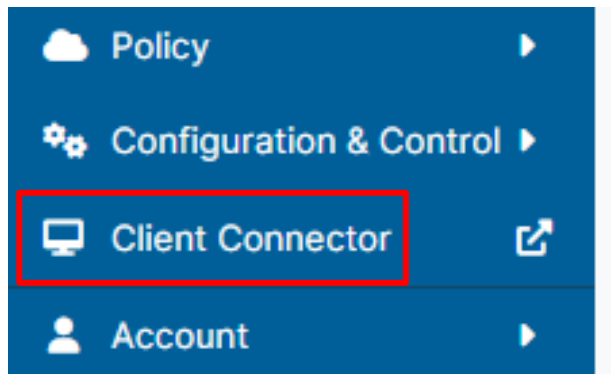


2-2-2. ZPA ポータルからのアクセス方法

(1) ZPA 管理ポータルを開きます。

管理ポータルの URL は「admin.private.zscaler.com」です。

(2) 左側メニューより「Client Connector」を選択します。



MOEX

3. Forwarding Profile

3-1. 概要

Forwarding Profile では主に下記 2 点の設定を行います。

(1) トラフィックの転送方法

(2) 社内ネットワークの判定方法

(ZCCは接続されているネットワークによって社内/社外の判定を行い、動作を変更することが可能です)

3-2. On Trusted Network(社内ネットワーク)の設定

Zscalerでは社内ネットワークを「On Trusted Network」

社外ネットワークを「Off Trusted Network」と呼んでおります。

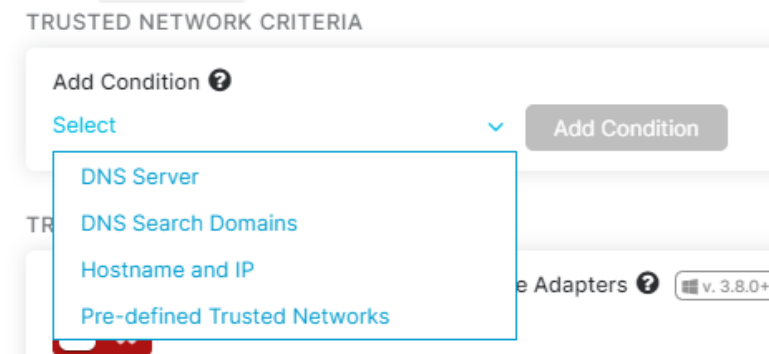
本項では、何をもって「On Trusted Network」と判断するかを設定します。

(1) ZCCポータルを開き、上側メニュー「Administration」→「Forwarding Profile」
→「Add Forwarding Profile」をクリックします。

(2) 「Trusted Network Criteria」→「Add Condition」にて「Trusted Network」の
判断基準を選択します。

Zscaler 社の推奨は「DNS Server」または「DNS Search Domain」です。

ネットワークインターフェースに割り振られた値を見て判断をするため、Trusted Network の
判断を行うために通信をする必要がなく、通信環境や何らかの要因で名前解決に失敗したとい
ったことに左右されないためとなります。



- DNS Server

端末のネットワークインターフェースに割り当てられる DNS で判断をします。

- DNS Search Domains

端末のネットワークインターフェースに割り振られる DNS サーチドメインで判断をします。

- Hostname and IP

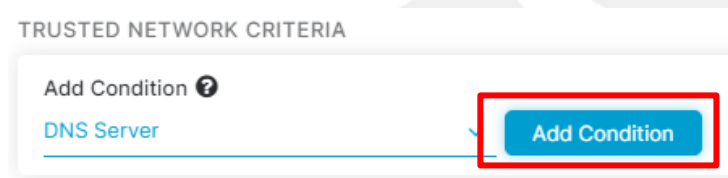
名前解決をした結果が、登録されているものと一致するかどうかで判断をします。

- Pre-defined Trusted Network

事前に定義されたものを選択します。

ZCC ポータル内、「Administration」>「Trusted Networks」にて設定が可能です。

- (3) 上記4つのうちいずれかを選択し、「Add Condition」をクリックします。
(複数を組み合わせることも可能です)



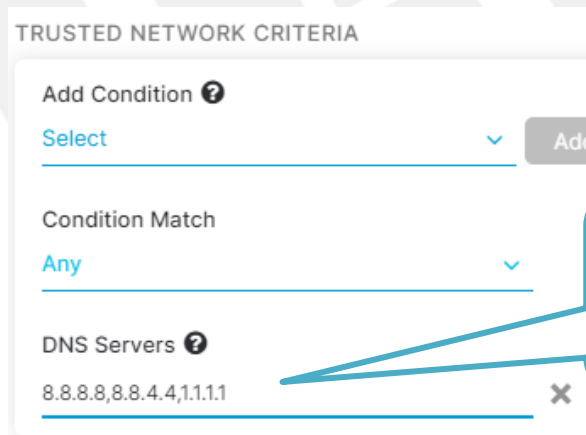
TRUSTED NETWORK CRITERIA

Add Condition ?

DNS Server

Add Condition

- (4) 設定内容を入力します。



TRUSTED NETWORK CRITERIA

Add Condition ?

Select

Condition Match

Any

DNS Servers ?

8.8.8.8,8.8.4.4,1.1.1.1

「,(カンマ)」区切りで複数の値を設定することが可能です。

3-3. ドライバーの設定

本項ではドライバーの設定を行います。

Zscalerでは「Route Based」と「Packet Filter Based」の2つのドライバーが用意されています。

-Route Based

端末のルーティングテーブルを制御して通信をハンドリングします。

他のルーティングテーブルを書き換えるようなアプリケーションと処理がバッティングしてしまい意図した動作にならない可能性があります。

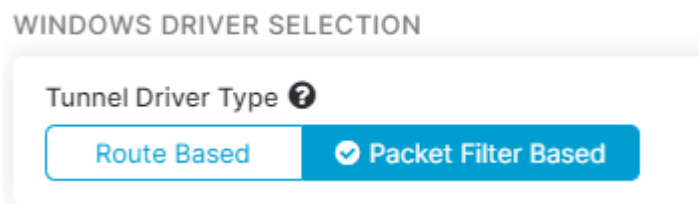
また、Route Basedでは Z-Tunnel2.0 をご利用いただけません。

-Packet Filter Based

ドライバレベルで通信をハンドリングします。

メーカーの推奨は、「Packet Filter Based」となります。

(1) 「Forwarding Profile」→「Windows Driver Selection」にてドライバーを選択します。



3-4. ZIA のトラフィック転送方法の設定

本項では ZIA へのトラフィック転送方法を設定します。

3-4-1. トラフィック転送方法の種類

トラフィック転送方法として「Tunnel(Tunnel1.0/2.0)」、「Tunnel With Local Proxy」、「Enforce Proxy」、「None」の4つあります。



「Tunnel」「Tunnel With Local Proxy」が ZCC を利用するイメージで、「Enforce Proxy」「None」は ZCC がオフのイメージとなります。

-Tunnel1.0

TCP80/443 の通信をすべて Z-Tunnel に転送する

Mobile 端末(iOS、Android)は Tunnel1.0 のみサポートされています。

-Tunnel2.0

ポートに関わらずすべてのトラフィックを Z-Tunnel に転送する

Z-Tunnel2.0 をご利用の場合は、メーカーに機能有効化の申請が必要になる場合があります。

Mobile 端末(iOS、Android)は Z-Tunnel2.0 未対応です。

-Tunnel With Local Proxy

ブラウザ/OS の PAC ファイルを参照するトラフィックのみが対象となります。

127. 0. 0. 1:9000(リスニングポート)に向けられたトラフィックが Z-Tunnel に転送されます。

-Enforce Proxy

Forwarding Profile 内にて設定したプロキシの設定を OS のプロキシ設定に強制する動作をします。

-None

ZCC で何も制御をしないという動作をします。

3-4-2. ネットワークの種類

ZCC は接続されているネットワークの種類を識別し、ネットワークの種類ごとに動作を変えることが可能です。

基本的に「On Trusted Network」「Off Trusted Network」「VPN Trusted Network」の 3 つあります。

-On Trusted Network

「Trusted Network Criteria」の条件にマッチしたネットワーク(社内ネットワーク)

-Off Trusted Network

「Trusted Network Criteria」の条件にマッチしないネットワーク(社外ネットワーク)

-VPN Trusted Network

フルトンネル型の VPN に接続している場合

3-4-3. トラフィック転送方法の設定手順

(1) 「Forwarding Profile」→「Forwarding Profile Action for ZIA」にて ZIA へのトラフィック転送方法の設定をします。

(2) それぞれのネットワークにてトラフィック転送方法を選択します。

(3) 「Forwarding Profile」→「Forwarding Profile Action for ZPA」にて ZPA の設定をします。

※記載のない項目につきましては Zscaler の Help ページをご確認ください。

4. App Profile

4-1. 概要

App Profile では ZCC をどのように動作させるかといった設定を行います。
本項では App Profile の基本的な設定手順、設定項目について説明します。

対象の OS ごとに App Profile の作成が必要です。

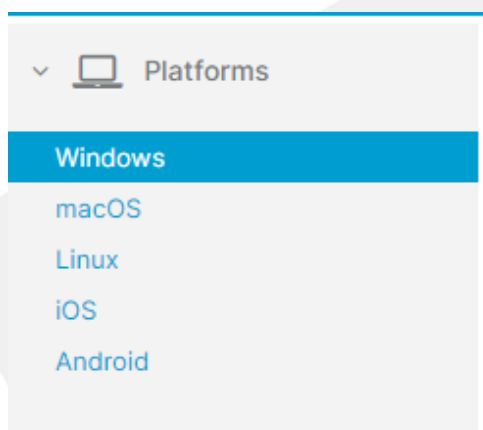
本書では「Windows」を例にとって説明します。

(基本的な設定方法についてはどの OS でも同じです)

4-2. App Profile の設定方法

(1) ZCC ポータルを開き、上側メニュー「App Profile」をクリックします。

(2) 左側「Platforms」より、App Profile を作成したいプラットフォームを選択します。



「Windows」「MacOS」「Linux」「iOS」「Android」が選択可能です。

※Chrome OS は「Android」に含まれます。

(3) 「Add Windows Policy」をクリックします。

(4) 設定内容を入力します。

GENERAL

Rule Order
19

User Groups
None Selected All

Enable

Users
None Selected

-Rule Order

ルールの順番を選択します。ルールが上のプロファイルから評価し、マッチするプロファイルを使用します。

-User Groups/Users

プロファイルを適用したいユーザーをグループ単位、またはユーザー単位で指定します。

Logout Password Optional

Password to Disable ZIA Optional

Password to Disable ZDX v. 3.5.0+ Optional

Uninstall Password v. 4.0.0+ Optional

Exit Password v. 3.5.0+ Optional

Password to Disable ZPA v. 3.6.0+ Optional

「v.O.O.O」は記載のあるバージョン以降で利用が可能な機能です。

-パスワード類

ユーザーがそれぞれの操作をした際にパスワードの入力を求めることが可能です。

Forwarding Profile
Default

Log Mode
Default (Current:Debug)

Install Zscaler SSL Certificate

Log File Size in MB
100

Log Mode と Log Size はデフォルト値のままで OK です

-Forwarding Profile

Forwarding Profile を指定します。

App Profile を分けることで、ユーザー毎にトラフィックの転送方法を変更することが可能です。

-Install Zscaler SSL Certificate

有効にしておくことで、App Profile 適用時に SSL インспекション用の証明書を自動でダウンロードします。

-Log Mode

ZCC のログのモードを選択します。

「Error」<「Warn」<「Info」<「Debug」の順にログが詳細になります。

-Log File Size in MB

ZCC のログのサイズを入力します。

設定した値を超えるログは古いものから順に削除されます。

Machine Token  v. 3.2.0+

None Selected

Machine Authentication Required 

 v. 3.4.0+

Disable Loopback Restriction 



Override WPAD 



Restart WinHTTP Service 



Reactivate Internet Security After (In Mins) 

0

-Disable Loopback Restriction

他のアプリケーションでリスニングポート(127.0.0.1:9000)を利用させないようにしている制限を無効にする設定です。

-Reactivate Internet Security After(In Mins)

ZIA がオフになった場合に、設定されている時間(分)を経過すると自動的に ZIA を ON にする機能です。

<p>Tunnel Internal Client Connector Traffic ?</p> <p><input type="checkbox"/> × v. 2.1.2+</p>	<p>Cache System Proxy ?</p> <p><input type="checkbox"/> × v. 3.0.2+</p>
<p>Prioritize IPv4 over IPv6 ? v. 3.4.0+</p> <p><input type="checkbox"/> ×</p>	<p>Use V8 JavaScript engine based PAC parser ?</p> <p><input type="checkbox"/> × v. 3.5.0+</p>
<p>Disable Parallel IPv4 and IPv6 DNS requests ?</p> <p><input checked="" type="radio"/> None <input type="radio"/> Enable <input type="radio"/> Disable v. 3.5.0+</p>	<p>ZIA Posture Profile ? v. 4.0.0+</p> <p><input checked="" type="radio"/> None <input type="radio"/> Selected</p>
<p>Send Disable Service Reason ?</p> <p><input type="checkbox"/> × v. 3.7.0+</p>	<p>Use Zscaler Notification Framework ?</p> <p><input type="checkbox"/> × v. 3.8.0+</p>
<p>Enable Zscaler Client Connector Revert ?</p> <p><input type="checkbox"/> × v. 3.9.0+</p>	<p>Notify Users before ZPA Authentication Expires ?</p> <p><input type="checkbox"/> × v. 4.2.0+</p>

-Cache System Proxy

ZCC 起動時の Windows のシステムプロキシの設定をキャッシュする機能です。

PAC CONFIGURATION

Custom PAC URL ?

Optional

Fallback to Gateway Domain ? v. 3.9.0+

Use Preferred Port from PAC for Z-Tunnel 1.0 ? v. 4.2.0+

Use Preferred Port from PAC for Z-Tunnel 2.0 ? v. 4.2.0+

-Custom PAC URL

ZCC が読むための PAC を設定します。

ZIA ポータル内、「管理」>「PAC ファイル」にて作成した PAC ファイルを指定します。

ZIA で接続するデータセンター (ZEN) を指定したい場合や、Z-Tunnel から除外したい宛先がある場合に利用する PAC となります。

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY ?

+

-Hostname or IP Address bypass for VPN Gateway

バイパスをしたい宛先がある場合に指定をします。

Destination Exclusions for IPv4 ? v. 2.0.0+

Use Enter to Add Multiple Items +

10.0.0.0/8	✕
172.16.0.0/12	✕
192.168.0.0/16	✕
224.0.0.0/4	✕

Destination Inclusions for IPv4 ? v. 2.0.0+

Use Enter to Add Multiple Items +

0.0.0.0/0	✕
-----------	---

-Destination Exclusions for IPv4
Z-Tunnel2.0 から除外したい宛先を入力します。

-Destination Inclusions for IPv4
Z-Tunnel2.0 に含めたい宛先を入力します。

※記載のない項目につきましては Zscaler の Help ページをご確認ください。

5. Client Connector App Store

5-1. 概要

Client Connector App Store では ZCC のインストーラーのダウンロードや、自動アップデートの設定を行います。

5-2. ZCC インストーラーのダウンロード方法について

本項では、ZCC インストーラーのダウンロードの方法について説明します。

- (1) ZCC ポータル内、「Administration」>「Client Connector App Store」をクリックし、「NEW RELEASES」のタブを開きます。

Application Version	Release Notes	EXE URL (32 bit)	MSI URL (32 bit)	EXE URL (64 bit)	MSI URL (64 bit)	Enable Build
4.2.0.190		↓	↓	↓	↓	<input checked="" type="checkbox"/>
4.1.0.102		↓	↓	↓	↓	<input checked="" type="checkbox"/>
4.1.0.98		↓	↓	↓	↓	<input checked="" type="checkbox"/>
4.1.0.89		↓	↓	↓	↓	<input checked="" type="checkbox"/>
4.0.0.89		↓	↓	↓	↓	<input checked="" type="checkbox"/>
4.0.0.80		↓	↓	↓	↓	<input type="checkbox"/>

- (2) 対象の OS を選択し、ダウンロードボタンをクリックします。

5-3. GA 版と限定版の違いについて

ZCC には「GA 版 (General Availability)」と「限定版 (Limited Availability)」の 2 種類あります。

-GA 版 (General Availability)

比較的使用実績が多いバージョンです。

限定版で発覚した不具合についてその多くが修正されたバージョンとなります。

また、限定版で追加された機能や仕様変更による動作に問題がないことが利用実績から確認できたバージョンとなり、安定動作が見込めるバージョンです。

新機能を利用したい等の理由がない限りは GA 版の利用を推奨しています。

-限定版(Limited Availability)

大きな機能の追加や、仕様の変更があり動作実績の少ないバージョンです。
GA 版と比較すると不具合が含まれる可能性が高いものとなります。
メーカーサポートは限定版についても GA 版と同様に受けることが可能です。

5-4. 自動アップデートの設定方法について

ZCC は自動でアップデートが実施されるよう設定をすることが可能です。
本項では自動アップデートの設定方法について説明します。

- (1) ZCC ポータル内、「Administration」>「Client Connector App Store」をクリックし、「NEW RELEASES」のタブを開きます。
- (2) 自動アップデートの対象としたいバージョンの「Enable Build」を有効にします。

General Availability						Limited Availability
Platform						
Windows macOS Linux						
Available Zscaler Client Connector Versions						
Application Version	Release Notes	EXE URL (32 bit)	MSI URL (32 bit)	EXE URL (64 bit)	MSI URL (64 bit)	Enable Build
4.2.0.190	📄	📄	📄	📄	📄	<input checked="" type="checkbox"/>
4.1.0.102	📄	📄	📄	📄	📄	<input checked="" type="checkbox"/>
4.1.0.98	📄	📄	📄	📄	📄	<input checked="" type="checkbox"/>
4.1.0.89	📄	📄	📄	📄	📄	<input checked="" type="checkbox"/>
4.0.0.89	📄	📄	📄	📄	📄	<input checked="" type="checkbox"/>
4.0.0.80	📄	📄	📄	📄	📄	<input type="checkbox"/>

- (3) ZCC ポータル内、「Administration」>「Client Connector App Store」>「UPDATE SETTINGS」のタブを開き、「Add Configuration」をクリックします。
- (4) 「Add App Store Group Policy」をクリックし、設定内容を入力し、「Update」をクリックします。

Version to Install では手順(1)で Enable Build を有効化したバージョンのみ指定が可能です。

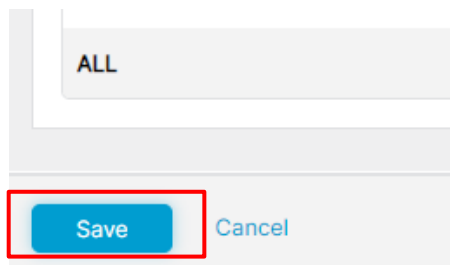
- Groups : アップデートの対象としたいグループを指定します。
(※ZPAのみをご利用の場合は、グループベースでのアップデートは不可となります)
- Version to Install : アップデートのバージョンを指定します。

Use 64-Bit Installer for Windows ?



※64bit 版の自動アップデートをするためにはメーカーに機能有効化の申請が必要です。

(5)「Save」をクリックします。



6. 端末の ZCC 画面について

6-1. 概要

本項では ZCC の画面について説明します。

6-2. ZCC の画面について

ZCC を開くと下記のような画面が表示されます。

左側のメニューよりそれぞれの項目を選択することができます。

Connectivity	
Username	
Service Status	ON TURN OFF
Network Type	Off-Trusted Network
Server	165.225.96.55:443
Client	172.17.31.130
Time Connected	火, 7 25 2023 05:41:34 午後
Tunnel Version	v2.0 - DTLS

Statistics	
Total Bytes Sent	2.68 MB
Total Bytes Received	12.69 MB

-Username

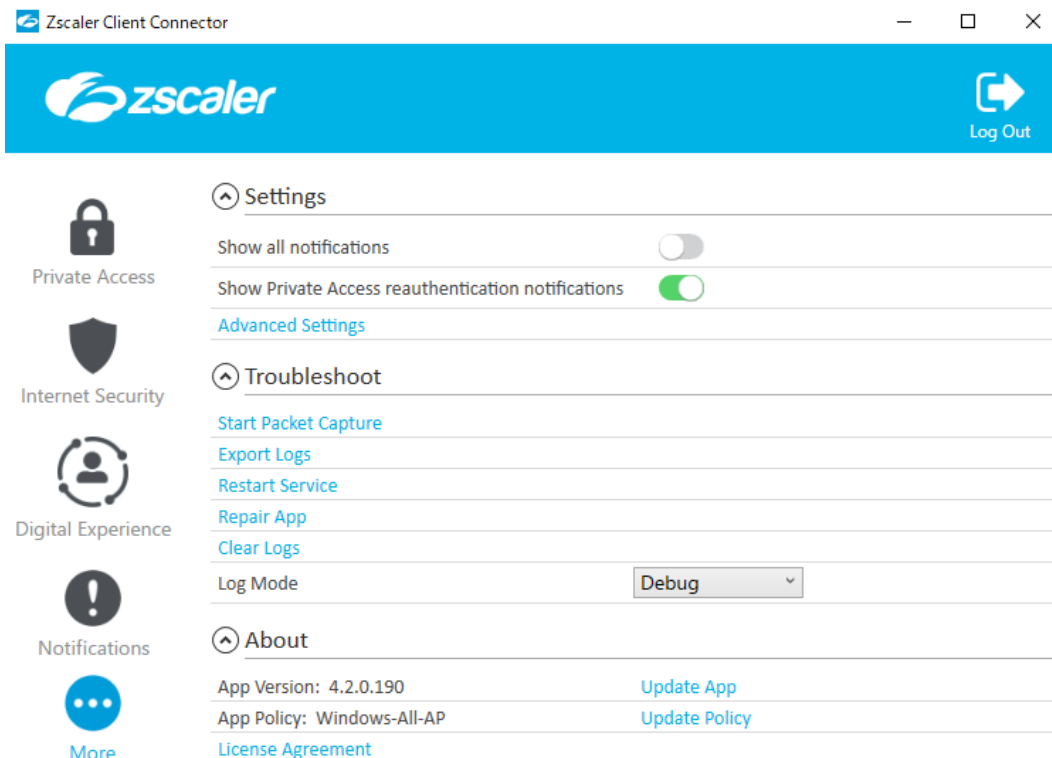
ZCC にログインをしているユーザーが表示されます。

-Service Status

それぞれのサービスのステータスを確認することができます。

-Network Type

現在接続されているネットワークのタイプが表示されます。



-Start Packet Capture

パケットキャプチャを開始します。

何も操作をしない場合は、5 分間で自動的に停止します。「Stop Packet Capture」をクリックすることで任意のタイミングで止めることが可能です。

-Export Logs

ZCC のログをエクスポートします。

パケットキャプチャを取得した場合、パケットキャプチャもログの中に含まれます。

-Restart Service

ZCC のサービスをリスタートします。

-Repair App

アプリのドライバとサービスを再インストールし、アプリの修復をします。

-Clear Logs

ログをクリアします。

7. Enrolled Devices

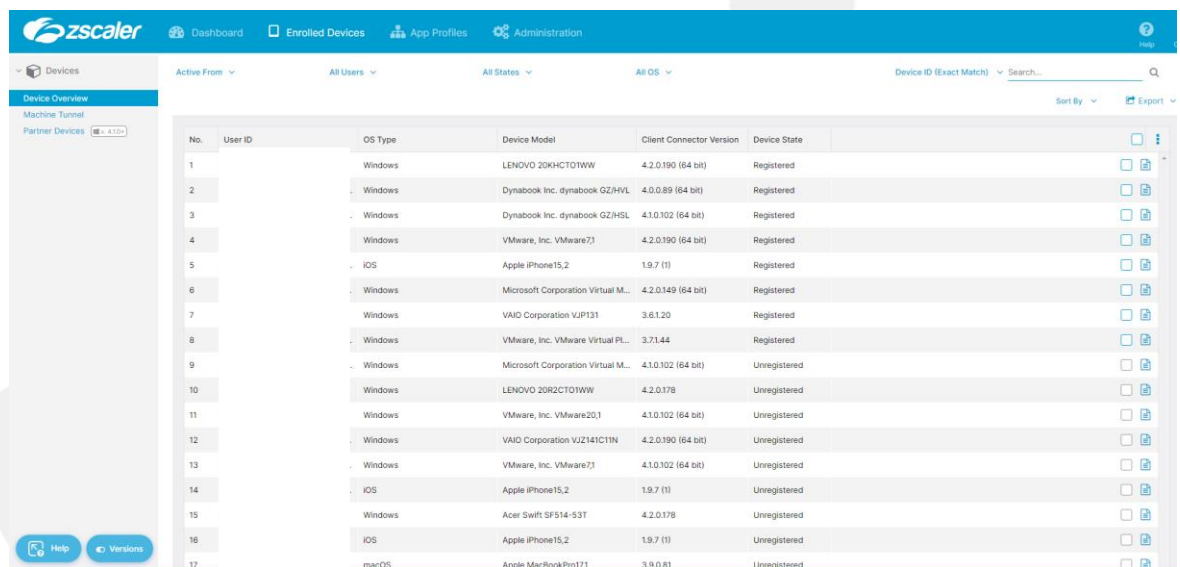
7-1. 概要

「Enrolled Devices」には ZCC にログインをしたことのある端末の一覧が表示されます。各端末のログイン状況などの情報を確認したり、管理者側で ZCC からログアウトさせたりすることが可能です。

本項では、「Enrolled Devices」のについて説明します。

7-2. Device Overview

「Device Overview」には ZCC にログインのしたことのある端末が一覧で表示されています。



No.	User ID	OS Type	Device Model	Client Connector Version	Device State
1		Windows	LENOVO 20KHCT01WW	4.2.0.190 (64 bit)	Registered
2		Windows	Dynabook Inc. dynabook GZ/HVL	4.0.0.89 (64 bit)	Registered
3		Windows	Dynabook Inc. dynabook GZ/HSL	4.1.0.102 (64 bit)	Registered
4		Windows	VMware, Inc. VMware7J1	4.2.0.190 (64 bit)	Registered
5		iOS	Apple iPhone15,2	1.9.7 (I)	Registered
6		Windows	Microsoft Corporation Virtual M...	4.2.0.149 (64 bit)	Registered
7		Windows	VAIO Corporation VJ1P131	3.6.1.20	Registered
8		Windows	VMware, Inc. VMware Virtual PL...	3.71.44	Registered
9		Windows	Microsoft Corporation Virtual M...	4.1.0.102 (64 bit)	Unregistered
10		Windows	LENOVO 20R2CT01WW	4.2.0.178	Unregistered
11		Windows	VMware, Inc. VMware201	4.1.0.102 (64 bit)	Unregistered
12		Windows	VAIO Corporation VJZ141C11N	4.2.0.190 (64 bit)	Unregistered
13		Windows	VMware, Inc. VMware7J1	4.1.0.102 (64 bit)	Unregistered
14		iOS	Apple iPhone15,2	1.9.7 (I)	Unregistered
15		Windows	Acer Swift SF514-53T	4.2.0.178	Unregistered
16		iOS	Apple iPhone15,2	1.9.7 (I)	Unregistered
17		macOS	Apple MacBookPro171	3.9.0.81	Unregistered

-Device State

デバイスのステータスを確認することができます。

Registered:ログイン中

Unregistered:ログアウト中

Removed:管理者が強制的に ZCC からログアウトさせたデバイス

7-3. 「Remove」について

管理者が管理ポータル上から強制的に ZCC からログアウトさせることが可能です。

本項ではログアウト(Remove)の手順について説明します。

7-3-1. Remove の手順について

(1) Remove には 2 つの手順があります。

Force Remove ではデバイスを 1 台ずつ Remove させることが可能です。

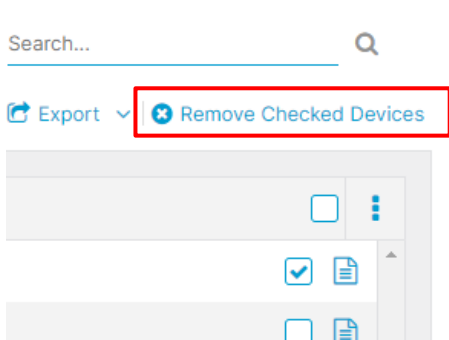
Soft Remove では複数のデバイスを指定し、Remove させることが可能です。

<Soft Remove>

(1) ZCC ポータル内、「Enrolled Devices」> Remove したい端末の右側チェックボックスにチェックを入れます。

No.	User ID	OS Type	Device Model	Client Connector Version	Device State	
1		Windows	LENOVO 20KHCT01WW	4.2.0.190 (64 bit)	Registered	<input checked="" type="checkbox"/>
2		Windows	Dynabook Inc. dynabook GZ/HVL	4.0.0.89 (64 bit)	Registered	<input type="checkbox"/>
3		Windows	Dynabook Inc. dynabook GZ/HSL	4.1.0.102 (64 bit)	Registered	<input checked="" type="checkbox"/>
4		Windows	VMware, Inc. VMware7,1	4.2.0.190 (64 bit)	Registered	<input type="checkbox"/>
5		iOS	Apple iPhone15,2	1.9.7 (1)	Registered	<input checked="" type="checkbox"/>

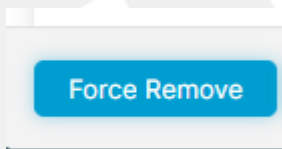
(2) 右上、「Remove Checked Devices」をクリックします。



<Force Remove>

(1) Remove したい端末の右側、ノートアイコンをクリックします。

(2) 「Force Remove」をクリックします。



8. Client Connector Support

8-1. 概要

「Client Connector Support」では ZCC をカスタマイズするための設定を行うことができます。

本項では、「Client Connector Support」の設定内容について説明します。

8-2. APP FAIL OPEN

「App Fail Open」ではフェイルオープンの設定をします。

ZIA のサービスエッジに何らかの理由で接続できなかった場合や、カフェなどの Wi-Fi 接続時にキャプティブポータルを検知した際にトラフィックをどのように処理するのかを設定します。

8-2-1. 設定方法について

(1) ZCC ポータル内、「Administration」>「Client Connector Support」>「APP FAIL OPEN」のタブを開きます。

(2) それぞれの項目で設定をします。

The screenshot shows the configuration interface for Client Connector Support. It is divided into two main sections: APP FAIL OPEN and CAPTIVE PORTAL. Under APP FAIL OPEN, there are two conditional settings, both currently set to 'Send Traffic Direct'. The first setting is 'If Public Service Edge is Not Reachable, Then' and the second is 'If Zscaler Client Connector Tunnel Setup Fails, Then'. Under CAPTIVE PORTAL, there is one setting: 'If Captive Portal Detected, Then Disable Web Security for (In Minutes)', which is currently set to 0.

-If Public Service Edge is Not Reachable, Then
ZIA のサービスエッジに接続できない場合のオプションを指定します。

-If Zscaler Client Connector Tunnel Setup Fails, Then
ZCC がトンネルのセットアップに失敗した際のオプションを指定します。

Send Traffic Direct**Disable Internet Access****Send Traffic Direct**

ZIA をバイパスしてインターネットに直接アクセスをします。

Disable Internet Access

HTTP/HTTPS のトラフィックをブロックします。その他のトラフィックに関しては許可されます。

-If Captive Portal Detected, Then Disable Web Security for(In Minutes)

Captive Portal を検出した際に、設定された分数 ZIA を無効にする機能です。

設定された分数が経過すると、自動的に ZIA が ON になります。

8-3. DEVICE CLEANUP

Device Clean up ではデバイスの自動クリーンアップの設定をします。

一定期間利用のなかったデバイスを自動的にログアウトさせたり、Removed 状態のデバイス(管理者にて強制的にログアウトさせたデバイス)を Enrolled Devices の一覧から自動的に削除したりすることが可能です。

8-3-1. 設定方法について

(1) ZCC ポータル内、「Administration」>「Client Connector Support」>「DEVICE CLEANUP」のタブを開きます。

(2)それぞれの項目で設定をします。

Force Remove Oldest Device After User Enrolls ⓘ
8 devices

Automatically Force Remove Inactive Devices After ⓘ
Never days

Permanently Delete Removed Devices After ⓘ
180 days

-Force Remove Oldest Device After User Enrolls

1 ユーザーが本項目で指定した数値以上のデバイスでログインを実施した場合に一番古いデバイスを自動的に「Removed」状態にします。

8~16 の間で設定が可能です。

「Never」を指定している場合は、17 台目のデバイスでログインを試みた際にエラーが出力されます。自動でデバイスが ZCC からログアウトされることはありません。

-Automatically Force Remove Inactive Devices After
指定された期間クラウドに接続がないデバイスを自動的に「Removed」状態にします。

-Permanently Delete Removed Devices After
Removed 状態のデバイスを本項目で指定した期間経過後に自動的に Enrolled Devices の一覧から削除します。

8-4. ADVANCED CONFIGURATION

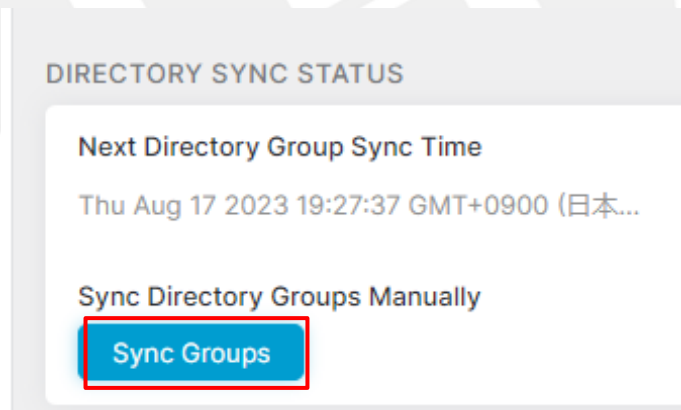
ZIA ポータル上で、グループを新規に作成した場合や変更した場合、ZCC ポータルにその内容が ZCC ポータル上に同期されるまでにタイムラグがあります。

ADVANCED CONFIGURATION より手動で即時に ZIA ポータルのグループ情報を ZCC ポータルに同期することが可能です。

8-4-1. 手順について

(1) ZCC ポータル内、「Administration」>「Client Connector Support」>「ADVANCED CONFIGURATION」のタブを開きます。

(2)「Sync Groups」をクリックします。



9. インストールオプションについて

9-1. 概要

ZCC はインストール時に、インストールオプションを指定することが可能です。

本項では ZCC に指定可能なインストールオプションの種類と、指定方法について説明します。

9-2. 指定可能なインストールオプションについて

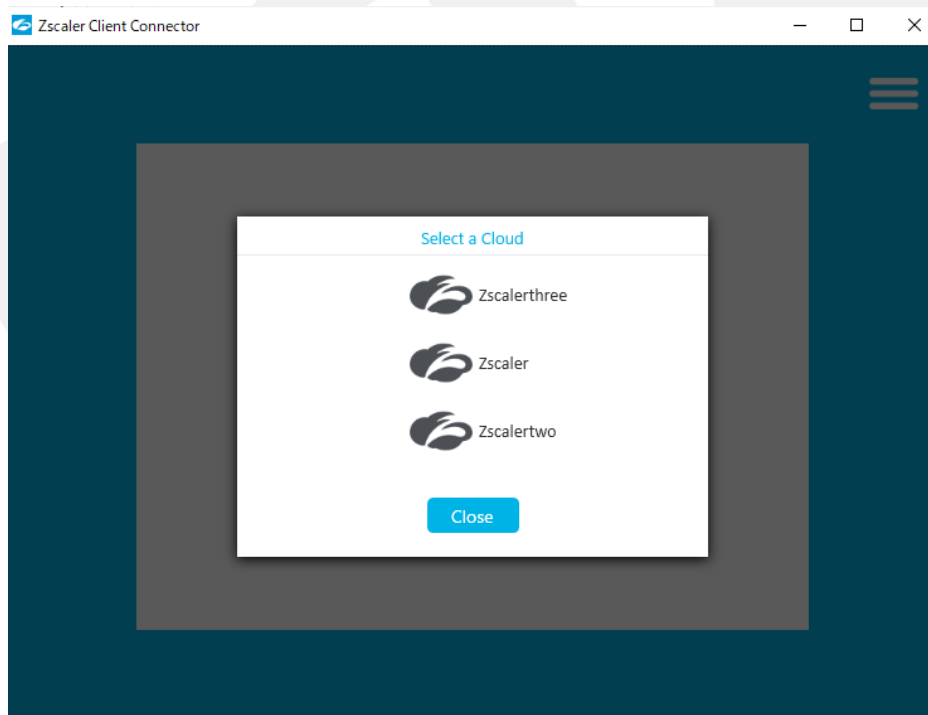
本項では、ZCC に指定可能なインストールオプションについて説明します。

(1) CLOUDNAME

複数のテナントをご利用の場合に有効なオプションです。

Cloudname のオプションを指定することで、ユーザー側でどのテナントにログインをするかの選択がなくなります。

また、後に説明をする Strict Enforcement のオプションを指定したい場合に必要なオプションとなります。



コマンドで指定をする場合、下記のように記載します。

CLOUDNAME=<organization's cloud name in lowercase>

Zscalerthree のテナントをご利用の場合、以下のように記載します。

CLOUDNAME=zscalerthree

(2) HIDEAPPUIONLAUNCH

ZCC インストール後に ZCC アプリのウィンドウを強制的に非表示にさせるオプションです。システムトレイの ZCC アイコンをクリックすることで、いつでもウィンドウを開くことが可能です。

コマンドで指定をする場合、下記のように記載します。

```
HIDEAPPUIONLAUNCH=1
```

(3) POLICYTOKEN

ユーザーが ZCC にログインをする前に、適用する App Profile を指定することができるオプションです。

ログイン後は、グループやユーザー単位で指定された App Profile が適用される形となります。

本オプションは Strict Enforcement のオプションを指定する場合にのみ有効なオプションです。

指定をする App Profile 内で、連携している SAMLIdP のログインページがバイパスされている必要があります。

コマンドで指定をする場合、下記のように記載します。

```
POLICYTOKEN=<policy token from the Zscaler Client Connector Portal>
```

ポリシートークンは ZCC ポータル内、「App Profile」>「Policy Token」より確認が可能です。



上記のポリシーを指定したい場合は、以下のように記載します。

```
POLICYTOKEN=333035373A333A36353433656430612D346538612D343530622D396566352D356236373737383439366530
```

(4) STRICTENFORCEMENT

ユーザーが ZCC にログインをするまで、インターネットアクセスを許可させないというオプションです。

Tunnel モード、または Tunnel With Local Proxy をご利用の場合にのみ有効なオプションです。

Strict Enforcement オプションを指定するためには、併せて「Cloudname」と「Policy Token」を指定する必要があります。

コマンドで指定をする場合、下記のように記載します。
strictEnforcement=1

(5) USERDOMAIN

Userdomain のオプションを指定することで、ユーザーID の入力を省略することができます。
SAMLIdP をご利用の場合、ユーザーは連携された SAMLIdP の認証画面にリダイレクトされます。

コマンドで指定をする場合、下記のように記載します。
USERDOMAIN=<organization's domain name>



10. ポリシーアップデートの間隔

10-1. 概要

ZCC はインターバルで、ZCC ポータル上の設定の変更の有無や、アップデートの有無、プロファイルの変更の有無などをチェックしています。

10-2. ポリシーアップデートの間隔について

(1) PAC ファイル更新のチェック

15 分ごとに実施されます。

(2) プロファイルや、ZCC ポータル上の設定変更のチェック

1 時間ごとに実施されます。

PAC ファイルの URL が変更された場合は、プロファイルの変更と見なされるためこのチェックのタイミングに更新される動作となります。

(3) ZCC アップデートのチェック

2 時間ごとに実施されます。

チェックのタイミングでアップデートが必要な場合はアップデートが実施されます。

※端末の ZCC で「Update Policy」や「Update App」をクリックすることで任意のタイミングで更新することが可能です。

11. バイパス設定

11-1. 概要

Zscaler を経由させたくない宛先がある場合、バイパスの設定を行うことで Zscaler から除外をすることが可能です。

本項ではバイパスの設定方法について説明します。

11-2. 手順について

それぞれのトラフィック転送方法におけるバイパスの設定手順について説明します。

11-2-1. Z-Tunnel1.0

Z-Tunnel1.0 はバイパスの手順が 2 通りありますので、どちらかの方法にて設定をします。

(1) HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY に除外したい宛先を登録します。

下記項目に除外対象としたい宛先の FQDN または IP アドレスを登録することで除外が可能です。

ZCC ポータル内、「App Profile」>「HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY」

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY ?

Use Enter to Add Multiple Hostnames or IP Addresses

www.nox.co.jp

www.example.com

1.1.1.1

+

×

×

×

(2) Custom PAC を指定します。

下記項目に除外対象の宛先を追記した PAC をご指定ください。

ZCC ポータル内、「App Profile」>「Custom PAC URL」

PAC CONFIGURATION

Custom PAC URL 

<https://pac.zscalertwo.net/>

11-2-2. Z-Tunnel2.0

Z-Tunnel2.0 は IP アドレスベースでバイパスをする場合と、FQDN ベースでバイパスをする場合で設定方法が異なります。

また、FQDN ベースでバイパスを実施する場合、ご利用の ZCC のバージョンによって設定方法が異なります。

本項ではそれぞれの設定方法について説明します。

<IP アドレスベースのバイパス>

(1) ZCC ポータル内、「App Profile」>「Z-Tunnel2.0 CONFIGUTATION」>「Destination Exclusions for IPv4」に除外をしたい宛先の IP アドレスを登録します。

<FQDN ベースのバイパス>

ZCCバージョン 3.7 以前

(1) Forwarding Profile に除外対象の宛先を記載した PAC ファイルを指定します。


ZCC ポータル内、「Administration」>「Forwarding Profile」>

「FORWARDING ACTION FOR ZIA」>「Configure System Proxy Settings」>

「Use Automatic Configuration Script」

Configure System Proxy Settings

System Proxy Settings

Proxy Action Type 

Enforce 

Use Automatic Configuration Script 

<https://pac.zscalertwo.net/>

Execute GPO Update

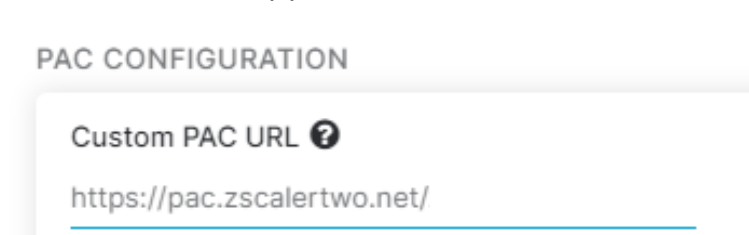
下記例のように、Z-Tunnel2.0 から除外をするという内容を記載した PAC ファイルを指定します。

(例)

```
if (dnsDomainIs(host, "<domain>"))
return "PROXY ${ZAPP_TUNNEL2_BYPASS}";
```

(2) App Profile に除外対象の宛先を記載した PAC ファイルを指定します。

ZCC ポータル内、「App Profile」>「Custom PAC URL」



対象の宛先をダイレクトに接続するという内容を記載した PAC ファイルを指定します。

(例)

```
if (dnsDomainIs(host, "<domain>"))
return "DIRECT";
```

ZCC バージョン 3.8 以降

ZCC バージョン 3.8 以降をご利用の場合は、こちらがメーカー推奨の設定方法となります。

(1) Forwarding Profile にて下記 2 つの設定項目を有効にします。

ZCC ポータル内、「Administration」>「Forwarding Profile」>

「FORWARDING PROFILE ACTION FOR ZIA」>「Advanced Z-Tunnel2.0 Configuration」

-Redirect Web Traffic to Zscaler Client Connector Listening Proxy

-Use Z-Tunnel 2.0 for Proxied Web Traffic

Redirect Web Traffic to Zscaler Client Connector Listening Proxy 



Use Z-Tunnel 2.0 for Proxied Web Traffic  v. 3.8.0+ v. 3.9.0+



(2) Custom PAC を指定します。

下記項目に除外対象の宛先を追記した PAC をご指定ください。

ZCC ポータル内、「App Profile」>「Custom PAC URL」

PAC CONFIGURATION

Custom PAC URL 

<https://pac.zscalertwo.net/>

11-2-3. Tunnel With Local Proxy

(1) Forwarding Profile に除外対象の宛先を記載した PAC ファイルを指定します。

ZCC ポータル内、「Administration」>「Forwarding Profile」>

「FORWARDING ACTION FOR ZIA」>「Configure System Proxy Settings」>

「Use Automatic Configuration Script」

Configure System Proxy Settings

System Proxy Settings 

Proxy Action Type 

Enforce 

Use Automatic Configuration Script 

<https://pac.zscalertwo.net/>

Execute GPO Update

11-2-4. PAC URL の確認箇所

プロキシ除外の設定を行う際に指定をする PAC の URL の確認箇所について説明します。

PAC は下記箇所で作成した際に生成される URL を指定します。

ZIA ポータル内、「管理」>「PAC ファイル」

PACファイル

+ PACファイルの追加

No.	Name	Description	Domain	Hosted URL
1	proxy.pac	Service Default.	zscalertwo.net	https://pac.zscalertwo.net/zscalertwo.net/proxy.pac
2	recommended.pac	Recommended PAC	zscalertwo.net	https://pac.zscalertwo.net/zscalertwo.net/recommended.pac
3	mobile_proxy.pac	Service Default.	zscalertwo.net	https://pac.zscalertwo.net/zscalertwo.net/mobile_proxy.pac
4	kerberos.pac	Service Default.	zscalertwo.net	https://pac.zscalertwo.net/zscalertwo.net/kerberos.pac

