



【連携機器】Pulse Secure PSA300 【Case】証明書とユーザーID/パスワードによるハイブリッド認証

Rev1.0

株式会社ソリトンシステムズ



はじめに

本書について

本書はオールインワン認証アプライアンス NetAttest EPS と、Pulse Secure 社製 SSL-VPN アプ ライアンス PSA300 の証明書とパスワードによるハイブリッド認証について設定例を示したもので す。設定例は管理者アカウントでログインし、設定可能な状態になっていることを前提として記述し ます。 アイコンについて

アイコン	説明
(پ	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機
	器の破損の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と 若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び PSA300の操作方法を記載したものです。 すべての環境での動作を保証するものではありません。

NetAttest は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。 本文中に ™、®、©は明記していません。

<mark>Seliton</mark> 目次

1. 構成
1-1 構成図
1-2 環境
1-2-1 機器
1-2-2 認証方式
1-2-3 ネットワーク設定4
2. NetAttest EPS の設定5
2-1 初期設定ウィザードの実行5
2-2 システム初期設定ウィザードの実行6
2-3 サービス初期設定ウィザードの実行7
2-4 ユーザーの登録8
2-5 クライアント証明書の発行9
3. PSA300の設定10
3-1 基本設定 10
3-1-1 インターフェイスの設定10
3-1-2 システム時刻設定11
3-1-3 Hosts 設定(任意)12
3-2 PSA300の証明書に関する設定13
3-2-1 SSL に関する設定(参考) (PSA300)13
3-2-2 CSR の生成(PSA300)14
3-2-3 サーバー証明書署名要求 (NetAttest EPS)16
3-2-4 サーバー証明書の発行 (NetAttest EPS)17
3-2-5 サーバー証明書のダウンロード (NetAttest EPS)18
3-2-6 CA 証明書の取得 (NetAttest EPS)18
3-2-7 サーバー証明書のインポート (PSA300)
3-2-8 CA 証明書のインポート (PSA300)
3-3 PSA300の VPN 接続に関する設定23
3-3-1 RADIUS/Certificate Serverの設定23
3-3-2 VPN Rolesの設定24
3-3-3 VPN Access Policyの設定26
3-3-4 Authentication Realmsの設定27

	3-3-5 Sign-In Policyの設定	29
	3-3-6 IP プールの設定	30
4. W	Vindows 版 Pulse Secure クライアントの設定	32
4	4-1 PC への証明書のインストール	32
4	4-2 Pulse Secure クライアントの取得と接続	33
5. iC	OS版 Pulse Secure クライアントの設定	35
!	5-1 iOS へのデジタル証明書のインポート	35
!	5-2 Pulse Secure への接続	36
6. A	Android 版の Pulse Secure クライアント設定	37
(6-1 Android へのデジタル証明書のインポート	37
(6-2 Pulse Secure クライアントの接続設定	38

1.構成



1-1 構成図

以下の環境を構成します。

- 証明書の配布には NetAttest EPS-ap を使用
- 接続するクライアント端末の IP アドレスは、NetAttest D3 の DHCP サーバーから 払い出す

1.構成



3

1-2 環境

1-2-1 機器

製品名	メーカー	役割	バージョン	
NetAttest EPS-ST05	ソリトンシステムズ	CA/RADIUS サーバー	4.10.4	
PSA300	Pulse Secure	SSL-VPN サーバー	9.0R3.1	
VAIO Pro PB	VAIO	クライアントPC	Windows 10 64bit	
iPad Air 2	Apple	クライアントタブレット	iOS 12.1.4	
Xperia XZ	ソニーモバイルコミュニケーションズ	クライアントスマートフォン	Android 7.0.0	
NetAttest EPS-ap-ST05	ソリトンシステムズ	証明書配布サーバー	2.2.5	
NetAttest D3-SX15	ソリトンシステムズ	DHCP サーバー	4.2.17	

1-2-2 認証方式

デジタル証明書とユーザーID/パスワードによるハイブリッド認証

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)	
NetAttest EPS-ST05	192.168.1.2/24			
PSA300	Inside: 192.168.10.1/24 Outside: 10.10.10.1/24	UDP 1812	secret	
NetAttest EPS-ap	192.168.1.3/24			
NetAttest D3 10.10.10.3/24				
無線アクセスポイント 10.10.10.2/24		-	-	
Client 端末 DHCP		-	-	

2. NetAttest EPS の設定

2-1 初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは 「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から 「http://192.168.2.1:2181/」にアクセスしてください。

下記のような流れでセットアップを行います。

- 1. システム初期設定ウィザードの実行
- 2. サービス初期設定ウィザードの実行
- 3. RADIUS クライアントの登録
- 4. 認証ユーザーの追加登録
- 5. 証明書の発行



2-2 システム初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

その後、システム初期設定ウィザードを使用し、以下の項目を設定します。

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- メインネームサーバーの設定



項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2.NetAttest EPS の設定

2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定(全般)
- RADIUS サーバーの基本設定(EAP)
- RADIUS サーバーの基本設定(証明書検証)
- NAS/RADIUS クライアント設定

CA種別選択			
CANDERIN	л−⊦са ∨		
CANCER			
● 内部で新しい鍵を生成する			
公開減方式	RSA 🛩		
鍵長	2048 🗸		
○ 外部HSMデバイスの鍵を使	Ulliga		
要求の署名			
要求署名アルゴリズム	SHA256 V		
CA情報			
	TestCA		
国名	日本	~	
都道府积名	Tokyo		
市区町村名	Shinjuku		
会社名(組織名)	Soliton Systems		
部署名			
E-mailアドレス			
CA署名設定			





NAS/RADIUSクライアンナ名	RadiusClient01	
	を有効にする	
	~	
	● NAS/RADIUS クライアント ● NASのみ ● RADIUS クライアントのみ	
記題月	0	
	192.168.1.1	
シークレット		
所属するNASグループ	×	
	戻る	次へ

項目	値
優先順位	EAP 認証タイプ
1	TLS
2	PEAP

項目	値
NAS/RADIUS クライアント名	RadiusClient01
IPアドレス	192.168.1.1
シークレット	secret

2-4 ユーザーの登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

[ユーザー] - [ユーザー一覧]から、「追加」 ボタンでユーザー登録を行います。

NetAttest EPS			ログオン中: admin ● トップページ ● 該定條存 ● ログオフ
 naepsexample.com システム設定 システム管理 証明機関 DFCPサーバー LDAPサーバー RADILSサーバー ユーザー ユーザー管 エクスポート インポート 		<i>ヴルー</i> プ ▼	ザーまで
■ ユーサーバスワードボリシー ■ デフォルトユーザープロファイル ■ ゲスト		 ユーザー 振跃対象: ユーザー情報 基本情報 姓 名 E-Mail 詳細情報 	設定 新規
項目	値	認証情報 ユーザーDD 	user01
姓	user01	パスワード(
ユーザーID	user01		相停止
パスワード	password		OK キャンセル 適用
NetAttest EPS	2-ザ		ログオン中: admin (・) トッナページ (ロ) 該定保存 (も) ログオフ
 システム設定 システム管理 部明機関 DHCPサーバー LDAPサーバー 	ユーザー ● 一部 ● 完全 詳細オ <u>ブションの設定</u> エクスポート	<i>Ğル</i> − ∃ ⊻ 2	ーザーまで 検索 道加
■ RADIUSサーバー ■ ユーザー		ユーザーID	ユーザー削除時の証明書失効オブション 最終認証成功日時 証明書 タスク
■ ユーザー一覧 ■ エクスポート	test user	test	第行 変更 削除
■ インボート ■ ユーザーバスワードポリシー	user01	<u>user01</u>	第67 支更 削除
■ デフォルトユーザーブロファイル ■ ゲスト			



2-5 クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

[ユーザー] - [ユーザー一覧]から、該当するユーザーのクライアント証明書を発行します。

(クライアント証明書は、user01.p12 という名前で保存)

NetAttest EPS				(harto	(2) (2) (2)	
	~					
■ naepsexample.com ■ システム設定	ב 📥	げ──覧				
■ システム管理	ユーザー	● 一部 ● 完全	グループ 💙 ニュ	ーザーまで 検索		
■ 証明機関 ■ DHC Pサーバー	詳細オブションの	設定				
■ LDAPサーバー	TIXADER					追加
■ RADIUSサーバー				<u></u>	- ザー削除時の証明	書失効オブション
■ ユーザー		名前	<u>ユーザー</u> DD	最終認証成功日時	証明書	タスク
■ エクスポート		test user	<u>test</u>		発行変	更削除
		user01	<u>user01</u>		発行 変	更削除
■ エーサーハスワートホリシー ■ デフォルトユーザープロファイル						
■ ゲスト						
			編集対象: user01			
			基本情報			
				user01		
			名			
			E-Mail			
			詳細情報			0
			STET ###P			
			コーザーID	user01		
			有効期限			
			● 日数 365 ● 日付 2016 ✔ :	日 年 7 V月 9 V日 23 V	✔時 59 ✔分 59 №	わまで
			証明書ファイルオブション			
			パスワード			
項目		値	バスワード(確認)			
正田書有効期限		365	※パスワードが空間の場合に	ま、ユーザーのパスワードを使用		
		505	✓ PKCS#12ファイルに証明	月機関の証明書を含める		
PKCS#12 ファイルに証明機関	目の・・・	チェック有			発行	キャンセル
					↓	
					•	
		🔤 📤 ユーザー証明	書のダウンロード			
		ユーザー証明書ダウンロ	コードの準備ができました。対象	なをファイルに保存して	Fália 5	ウンロード
					and the second s	

Spliton

3. PSA300の設定

3-1 基本設定

3-1-1 インターフェイスの設定

PSA300の設定は WebUI で行います。(サブネットの設定は CLI から) PSA300のインターフェイスの設定は、下記の通りです。

[Ethernet0] Internal Port

社内 LAN に接続。管理 interface としても使用

S Pulse Secure							
Pulse Connect Secure							
🗄 System							
Status ,	Network	> Internal Port >					
Configuration >	Setti	ngs					
Clusterion							
IF-MAP Federation	9.:0	Network Settings					
Log/Monitoring	0	Internal Port - Settings					
Reports +		The second part in the second parts					
Behavioral Analytics	Overv	nternal Port External Port	VLANS Routes Hosts VPN Tunneling Proxy Se	rver			
E Authentication	Setting	s Virtual Ports ARP Cache ND Cache					
Endpoint Security	Entra	the extended at the second stick the sec	on Channes hatten at the bottom of the same				
Auth. Servers	Enter t	the network settings and click the Sa	ve changes button at the bottom of the page.				
Administrators							
Admin Realms >	TPV4 Se	ettings					
Admin Roles >		citings					
User Realms		* IP Address:	192.168.1.1				
User Roles		* Netmask:	255 255 255 0	111日			
Resource Profiles >		& Default Catavan	102 169 1 254				
Resource Policies		Default Gateway:	192.100.1.254				
Pulse Secure Client		Note: If you need to specify static routes,	you can do so on the <u>Static Routes</u> page.	TD Addroc	c	102 168 1 1	I
				IF Addres	3	192.100.1.1	
				Netmask		255.255.255.0	
				Dofault C	atoway	102 169 1 254	
					aleway	192.100.1.204	

[Ethernet1] External Port

Pulse Secure クライアントによる接続を受付ける interface

Pulse Secure			
Pulse Connect Secure			
System Status Configuration Network Clustering IF-MAP Federation Log/Monitoring	Itehung External Port > Settings		
Reports Behavioral Analytics Authentication	Overview Internal Port External Port Settings Virtual Ports ARP Cache ND Cache	VLANS Routes Hosts VPN Tunneling Prox	sy Server
Endpoint Security Auth. Servers Administrators Admin Realms	Enter the network settings and click the Sa	ve Changes button at the bottom of the page.	
Admin Roles Users User Realms User Roles	, Use Port • • Enabled O Disabled		
Resource Profiles Resource Policies Pulse Secure Client Enterprise Onboarding Maintenance System	IPV4 Settings Enable IPv4 Disable IPv Note: Changing above setting might r	4 start some services. This restart might drop all the conne	ctions to the Pulse Connect Secure.
Import/Export Push Config Archiving Troubleshooting	* IP Address: * Netmask:	10.10.10.1 255.255.255.0	項目
	* Default Gateway: Note: If you need to specify static routes,	10.10.254 you can do so on the <u>Static Routes</u> page.	IP Addre
			Netmask

項目	値
IP Address	10.10.10.1
Netmask	255.255.255.0
Default Gateway	10.10.10.254

3-1-2 システム時刻設定

NetAttest EPS と同じ時刻を設定します。

[Status]-[System Date & Time]-[Edit]から設定します。

S Pulse Secure					
Pulse Connect Secure				Help Guid	ance Switch to New UI Sign Out
System	Status >				
Network >	System Status Overvie	W			
IF-MAP Federation >	A Warning				
Reports > Behavioral Analytics >	"Pulse Connect Secure License "PSA with maximum concurrent	e (VPN remote access) 10 Concurrent Session of users all features 4 week license" - licen	ons - Perpetual" - license will expire in 90 days ar	nd 23 hours.	
Authentication Signing In →	One or more Certificate(s) has	s expired or due to expire. Please click here	for details		
Endpoint Security > Auth. Servers	Centrally manage all of your P	ulse Secure solutions from anywhere with P	Pulse One Try Now		
Administrators Admin Realms →	Notification Alert: Pulse Netwo	rk Connect (NC) and Pulse Windows Secure	Application Manager (WSAM) clients will be EOL	'ed from Q2'2019. Customers are recomm	dismiss until next upgrade nended to migrate to Pulse
Admin Roles Users	Desktop Client before the EOL	to get continued maintenance. For more infi	ormation, please refer to <u>ISB43810.</u>		dismiss until next upgrade
User Realms > User Roles > Description	Activity Overview Active L	Jsers Cloud Secure Cloud Application Vi	isibility Meeting Schedule Virtual Desktop Ses	ssions Devices Admin Notification	
Resource Policies > Pulse Secure Client >	Critical Events	System Capacity Utilization	Graphs display last 1 hour		
Enterprise Onboarding >	Page Settings	Concurrent Users (<u>Edit</u> ¥ <u>Download</u>)			
System > Import/Export >	System Version 9.0R3.1 (build 64015) Deveload Package	6			
Push Config > Archiving >	Uptime 26 minutes, 11 seconds	4			
Troubleshooting >	Last Config Update Thu Feb 7 10:29:35 2019		· · · · · · · · · · · · · · · · · · ·		
	System Date & Time Edit 2019-02-07 10:31:43 AM	U9:40 U9:50 10 Concurrent users VPN Tunnel Users	:00 10:10 10:20		
	Logging Disk: 0% Full	Concurrent Meeting Graph (<u>Edit</u> 🗣 <u>Download</u>)			
	Max Licensed Users: 200	1.0			
	Concurrent Connections for 0	0.5			
	Authorization only Access: ActiveSync Connections: 0	0.0			
		09:40 09:50 10	:00 10:10 10:20		
		Hits Per Second (Edit T Download)			
		500 m	I. Jì		
			\\\ \		
		0 09:40 09:50 10 ■ Hits ■ Web Hits ■ File Hits ■ Clien	:00 10:10 10:20 ht-Server Hits		
		Concurrent SSL Connections (Edit Townload)			
		4.0	нининини П		
		3.0	, Г		
		1.0			
		0.0 09:40 09:50 10	:00 10:10 10:20		
		(Dill and Vietual (Swan) Memory Utilization (Edit			
		e. 0			
		¢; t v 2,0	ያ ኪሌ ነ		
		5 2.0 ×			
		0.0-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	0:00 10:10 10:20		
		hroughput (<u>Edit</u>			
		100 k			
		50 k			
		0	:00 10:10 10:20 Internal in Internal out		
		🗖 Internal Hulticast in 🗖 Internal Mult	icast out		
		Rates Per Minute (<u>Edit</u> 🗣 <u>Download</u>)			
		0.0-0:40 09:50 10	00 10:10 10:20		
		HC	anterigica ina a saccessiai via		
Licensed to 0311M5RWK0N8 Copyright © 2001-2018 Puls	Q111S se Secure, LLC. All rights reserved.				



3-1-3 Hosts 設定(任意)

本検証環境には、DNS サーバーを設置していないため、NetAttest EPS の IP アドレスを Hosts に 登録します。「Network」-「Hosts」から設定します。

Pulse Secure				
ulse Connect Secure			Help Guidance Switch	to New UI Sign Out
System Status Configuration Configuration Clustering F-MAP Federation Clustering Seports Sehavioral Analytics Signing In	Network > Hosts Network Setti Hosts Overview Internal Port This shows the current Ho or remove entries	Ings : External Port Management Port OST table for this port. These mapping	VLANs Routes Hosts VPN Tunnelin s are automatically created, but if necess	g Proxy Server
Auth. Servers	IP	Name(s)	Comment	
Admin Realms	102.169.1.2			Add
er Realns i ier Roles i source Profiles i source Policies i des Secure Client i terprise Onboarding i daintemance ystem i nport/Export i sch Config i				
roubleshooting			項目	値
			IP	192.168.1.
			Name	naeps.local

3-2 PSA300の証明書に関する設定

3-2-1 SSL に関する設定(参考)(PSA300)

SSL に関するセキュリティ設定を行います。[Configuration]-[Security]から設定します。

Security	
Licensing Pulse One Security Certificates DMI Agent Inbound SSL Options Outbound SSL Options Health Check	NCP Sensors Client Types Pulse Collaboration Virtual Deski Options Miscellaneous Advanced
DoD Certification option When this option is enabled, the web service will be placed in 3	NTC Mode. NDcPP and FIPS Modes will also be turned on and all no
UTurn on JITC mode	
SSL NDcPP Mode option When this option is enabled, the web service will be placed in f	NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS cipl
UTurn on NDcPP mode	
SSL FIPS Mode option When this option is enabled, the web service will be play prerequisite for NDcPP Mode.	ced in FIPS Mode, the cipher strength will be set to Medium, and al
□ Turn on FIPS mode	
Inbound Settings	
Allowed SSL and TLS Version The older SSL V2 protocol has known security issues addressed	d by SSL V3 and TLS. It is no longer supported.
 Accept only TLS 1.2 and later (maximize security) Accept only TLS 1.1 and later Accept only TLS 1.0 and later Accept SSL V3 and TLS (maximize compatibility) 	
Allowed Encryption Strength Strong ciphers (rated by the number of bits in the cipher) impr cipher with the fastest data transfer rate, regardless of its relation	rove the security of SSL encryption, but some browsers may only s tive encryption strength. Changing the encryption strength will cau
 PFS - Perfect Forward Secrecy SuiteB - Accept only SuiteB ciphers (Requires an ECC cert Maximize Security (High Ciphers) Maximize Compatibility (Medium Ciphers) Custom SSL Cipher Selection 	ificate)
▶Show Selected Ciphers	
Encryption Strength option Normally, the allowed encryption strength is enforced after an weak cipher from establishing a connection. Changing this opti	SSL session is established, so that a user that connects using a dis on will cause the web service to restart.
Do not allow connections from browsers that only accept	weaker ciphers
Key Exchange Options If the Allowed Encryption Strength includes any DH ciphers, th	e system uses 1024bit DHE key exchange by default. The option b
🖲 Use 2048bit Diffie-Hellman key exchange	
SSL Legacy Renegotiation Support option When this option is enabled, renegotiation with clients and sen Changing this option will cause the web service to restart.	vers, which dont support the new TLS Renegotiation Info extensior
Enable support for SSL legacy renegotiation	
Common entions	
SSL Handshake Timeout option	
By default, the SSL handshake has a timeout of 60 seconds. U	se the text box below to set a different value.
坝 目	
Allowed SSL and TLS Version	Accept Only SSL V3 and TLS V1
Allowed Encryption Strength	Accept Only 128-bit and greater
SSL Legacy Renegotiation Support option	Enable support for SSL legacy renegotiation

3-2-2 CSRの生成(PSA300)

PSA300 で CSR(Certificate Signing Request)を生成します。

[Configuration]-[Certificates]-[Device Certificates]の「New CSR」より

CSR を作成します。「Create CSR」をクリックすると、以下の画面に遷移します。

uise connect secure		
System		
Status	Configuration > Certificates >	
Configuration	New Certificate Signin	a Request
Network	•	
Clustering	Use this page to create a new	Certificate Signing Request (CSR) to send to your Certificate Authority of choic
IF-MAP rederation		
Reports	(e.g. secure company com)	PSA300
Reports Rehavioral Analytics	Organization Name:	
Authentication	(e.g., Company Inc.)	Example Corporation
Signing In	Org. Unit Name:	
Endpoint Security	(e.g., IT Group)	
Auth. Servers	Locality:	Shiniuku
Administrators	(e.g., SomeCity)	
Admin Realms	State (fully spelled out): (e.g., California)	Токуо
Admin Roles	Country (2 letter code):	
Users	(<i>i.e.</i> , US)	JP
User Realms	Email Address:	
User Roles		
Resource Profiles	Кеу Туре:	● RSA ○ ECC
Resource Policies	Key Length:	1024 ✓ bits
Pulse Secure Client	· · · ·	
Enterprise Onboarding		
Maintenance		
System	Please enter some random ch	aracters to augment the system's random key generator.
Import/Export	We recommend that you enter	er approximately twenty characters.
Archiving	Random Data:	
Troubleshooting	(used for key generation)	•••••
rioubleanooting	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
		Create CSR

Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
Common Name	PSA300
Organization Name	Example Corporation
Locality	Shinjuku
State	Tokyo
Country	JP
Random Data	password

[Step1. Send CSR to Certificate Authority for signing]の文字列すべてをコピーし、テキスト データで保存します。

S Pulse Secure						
Pulse Connect Secure						
E System						
Status >	CSR created successfully					
Configuration > Network >	Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority.					
Clustering → IF-MAP Federation → Log/Monitoring →	The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you wil process.					
Reports >						
Behavioral Analytics	Configuration >					
Authentication	Pending Certificate Signing Request					
Signing In >	CSR Details					
Auth Servers	Compon Name: PSA300					
- Administrators	Created: 3/7/2019 16:6:28					
Admin Realms	Oro Name: Example Corporation Locality: Shiniyku					
Admin Roles	Org. Hunts. Example of portable Example on Market State: Tokyo					
- Users	Email Address: Country:JP					
User Realms	Key Size: 1024 bits					
User Roles						
Resource Profiles	Back to Device Certificates					
Resource Policies	Step 1 Send CSP to Certificate Authority for signing					
Pulse Secure Client	Step 1. Send CSK to CER the a Cartificate Authority (CA) you need to cany the enceded text below, including the BEGIN and END lines					
Enterprise Onboarding >	wave:					
Maintenance	weys.					
System >	 Save the text as a .cert file and attach it to an email message to the CA 					
Import/Export >	Paste the text into an email message to the CA					
Push Config >	Paste the text into a Web form provided by the CA					
Archiving Troubleshooting	Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.					
	BEGIN CERTIFICATE REGUEST					
	MI IBZZCCAUÇCAQAWXZELMAKGAL UEBMCSLAXD jAMBqNVBAqMBVRva31vMRewDwYD					
	VQQHDAhTaGluanVrdTEcMBoGA1UECgwTRXhhbXBsZSBDb3Jwb3JhdGlvbjEPMA0G					
	AlUEAwwGUFNBMZAWMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQtyyyYQa9 🗸					
	0MstOFuZKJvUz3FYxZmlbedHvTFjSt6IxFDI5tTWlAJmD4rdBJMfqnkGtsFPQFAo					
	Ctop 2 Impart signed partificate					
	When you receive the signed certificate file from the CA select it below and click Import. This will add the signed certificate a					
	when you receive the signed certificate me nom the CA, select it below and thick import. This will add the signed certificate a					
	Signed certificate: 参照					
	Import					
Licensed to 0311M5PW/K0M	1801115					

Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

3-2-3 サーバー証明書署名要求 (NetAttest EPS)

PSA300 で生成した CSR を基に NetAttest EPS で PSA300 のサーバー証明書を発行します。 NetAttest EPS の管理者向け証明書サービスページ(https://192.168.1.2/certsrva/)にアクセス し、証明書要求を行います。下記の手順で CSR をインポートします。

Not Attoot EDC		ログオン	'中: admin
NetAttest EPS		() トップページ 🕖	閉じる
 記明書サービス - TestCA CA情報 ダウンロード 記明書要求 記明書確認 	証明書要求-ブロファイルの選択 このPCでは、以下の証明書要求を作成できます。 <u>CA証明書</u> クライアント証明書 電子メール保護証明書 <u>Psec証明書</u> スマートカードログオン証明書 コード署名証明書 WEBサーバー証明書 ドメインコントローラ証明書 カスタム証明書 SCEPカスタム証明書 EPS-ap用SCEP証明書 既存証明書の更新を要求する		

WEBサーバー証明書 名前 (***) 名前 (***) 国名 指定しない 移道府県名 市区町村名 会社名(組織名) 会社名(組織名) 部署名 E-mailアドレス 別名 : プリンシバル名 詳細オプションの設定 FKCS#107ア・イルによる証明書要求を指じる 参照	の作成		
WEBサーバー証明書 名前 (***) 名前 (***) 国名 指定しない 都道府県名 市区町村名 会社名(組織名) 部署名 E-mail/FL/ス 財名 : プリンシバル名 詳細オブションの設定 PKCS#107ァイルによる証明書要求を閉じる 参照			
名前 (**) 国名 指定しない 都道府県名 市区町村名 会社名(組織名) お署名 正 予署名 正 財名 : ウリンシバル名 詳細オブションの設定 PKCS#10ファイルによる証明書要求を問じる 参照	WEBサーバー証明書		
国名 指定しない 都道府県名 市区町村名 市区町村名 会社名(組織名) 会社名(組織名) 部署名 正 フリンシバル名 財名 ・ 井田太 フションの設定 FKCS#10ファイルによる証明書要求を閉じる 参照	名前		(必須)
都道府県名 市区町村名 市区町村名 会社名(組織名) 部署名 部署名 防害 カリンシバル名 詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる C:\Temp\19020T_CSR.txt 参照	国名	指定しない	~
市区町村名 会社名(組織名) 部署名 E-mailアドレス 別名 ■ プリンシバル名 詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる て.\Temp\190207_CSR.txt 参照	都道府県名		
 会社名(組織名) 部署名 正mailアドレス 別名 ■ プリンシバル名 詳細オブションの設定 PKCS#10ファイリルによる証明書要求を閉じる [C:\Temp\190207_CSR.txt] 	市区町村名		
部署名 E-mailアドレス 別名 ・ プリンシバル名 詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる C:\Temp\190207_CSR.txt 参照	会社名(組織名)		
E-mailアドレス 別名 *・ プリンシバル名 詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる C:\Temp\190207_CSR.txt 参照	部署名		
別名 ・ ・ ・ 詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる C:\Temp\190207_CSR.txt	E-mailアドレス		
詳細オブションの設定 PKCS#10ファイルによる証明書要求を閉じる C:\Temp\190207_CSR.txt 参照	別名 ■ プリンシバル名		
PKCS#10ファイルによる証明書要求を閉じる C:\Temp\190207_CSR.txt 参照	詳細オプションの設定		
C:\Temp\190207_CSR.txt 参照	PKCS#10ファイルによる証明書要求を閉	<u>105</u>	
	C:\Temp\190207_CSR.txt	参照	



3-2-4 サーバー証明書の発行 (NetAttest EPS)

サーバー証明書要求の承認・発行を行います。

CA 管理ページ(http://192.168.2.1:2181/caadmin/)にアクセスし、「保留」状態のサーバー証明 書を発行します。

Net Attest EDC							グオン中: admin
NetAttest EPS					● トップページ	🕒 設定保存	📵 ログオフ
E naeps.example.com E CA情報 要求管理 E 証明書管理 E CRL管理	要 求リスト	新					
■ 証明機関ログ	大態 受付日時	送信元	ブロファイル/証明書目的	申請者		クライアント	
	✔ 保留 2019/03/07 16:	07:42 CAadm:admin Serial:10 Cn:user01	0 WEBサーバー証明書 (unknown)	CN=PSA300,O=Example Corpor	ration,L=S		確認
			/ <mark>7 > 16 ></mark> 07 <mark>> </mark> 59 > まで				
Copyright © 2004-2018, Soliton Systems K.	.K., All rights reserved.						



3-2-5 サーバー証明書のダウンロード (NetAttest EPS)

サーバー証明書をダウンロードするために再度、管理者向け証明書サービスページにアクセスします。「証明書の確認」を選択すると状態が「発行」になっていますので、サーバー証明書をダウン ロードします。

NetAttest EPS							ログオンロ ① トップページ 〇 日	中: admin 閉じる
■ 証明書サービス - TestCA	証明書確	3						
 CA情報 ダウンロード 証明書要求 	■要求一覧■							
■証明書確認	状態	<u>申請日時</u>	プロファイル	証明書目的	<u>申請者</u>		タスク	
	発行			(unknown)	CN=PSA300,O=Example Corporation,L=Shin	インストール	ダウンロード 削除	

3-2-6 CA 証明書の取得 (NetAttest EPS)

管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式を選択します。

NetAttest EPS	ログオン中 () トップページ) 日	: admin 比る
 証明書サービス - naeps.example.com CA情報 ダウンロード 証明書要求 証明書確認 	ダウンロード CA証明書ダウンロード PEM DER CA証明書インストール CA証明書ダウンロード CA証明書ダウンロード OCSP署名証明書ダウンロード PEM DER CRLダウンロード PEM DER GRI ダウンロード PEM DER	

3-2-7 サーバー証明書のインポート (PSA300)

NetAttest EPS で発行したサーバー証明書をインポートします。CSR を作成したページの[Step 2. Import signed certificate]で、サーバー証明書(nausercert-pem.cer)をインポートします。

S Pulse Secure	
Pulse Connect Secure	
- System	
Status CSR created	successfully
Configuration Your CSR wa	as created successfully. See below for instructions on sending the CSR to a Certificate Authority.
Clustering The certifica	to approval process may take several days. When you receive the signed cartificate from the Cartificate Authority, you will
IF-MAP Federation process.	te approval process may take several days, when you receive the signed certificate norm the Certificate Automicy, you will
Log/Monitoring	
Reports	
Behavioral Analytics Configuration >	artificate Signing Poquest
Signing In	artificate Signing Request
Endpoint Security CSR De	atails
Auth. Servers Common	Name: PSA300
- Administrators Created:	3/7/2019 16:6:28
Admin Realms Org. Name	e: Example Corporation Locality: Shinjuku
Admin Roles Org. Unit	Name: State: Tokyo
- Users Email Add	Iress: Country:JP
User Realms Key Size:	1024 bits
User Roles	
Back to Device	<u>ce Certificates</u>
Pulse Secure Client Step 1. Send	d CSR to Certificate Authority for signing
Enterprise Onboarding To se	end the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines,
Maintenance Ways	5:
System +	• Save the text as a .cert file and attach it to an email message to the CA
Import/Export	Paste the text into an email message to the CA
Push Config +	Paste the text into a Web form provided by the CA
Archiving Troubleshooting Note	a: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.
	BEGIN CEDTIFICATE DECNIPST
MIII	BIGIN GIANTITUTI KAUNI
VQQI	HDAhTaGluanVrdTEcMBoGA1UECgwTRXhhbXBsZSBDb3Jwb3JhdGlvbjEPMA0G
Alu	EAwwGUFNBMZAWMIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBqQQQtyyyYQa9
UMST	tordskjansshinsedHalllsteilktnistimitelmidikershökeo
Sten 2 Im	nort signed certificate
Wh	por source continuance
Sig	yned certificate: 参照
	mport
Licensed to 0311M5RWK0N8Q111S	

S Pulse Secure			
Pulse Connect Secure			Help Guidance Switch to New UI Sign Ou
System Status Configuration Network Clustering IF-MAP Federation Log/Monitoring Reports	Configuration > Certificates > Device Certificate Licensing Pulse One Security Certificate Device Centificates Trusted Client CAs Trusted Server	DMI Agent NCP Sensors Client Types Pulse C CAs Code-signing Certificates Client Auth Certificates Certificate	ollaboration Virtual Desktops User Record Synchronization IKEv2 SAML
Behavioral Analytics Authentication Signing In Endpoint Security	Specify the Device Certificate(s). If you don't Inport Certificate & Key	nave a certificate yet, you can create a CSR and import t	he resulting signed certificate. If necessary, you can add custom Intermediate CA
Auth. Servers	Certificate issued to	Issued by	Valid Dates
Administrators	PSA300	TestCA	Mar 7 07:03:12 2019 GMT to Mar 6 07:08:12 2020 G
Admin Realms > Admin Roles > Users Users User Realms > User Roles > Resource Profiles >	TestCA	TestCA	Feb 7 01:50:16 2019 GMT to Feb 7 01:55:16 2020 GM
Resource Policies >	New CSR Delete		
Second Citerit For a second Citerit For a second Citerit Maintenance System Import/Export Push Config Archiving Troubleshooting	Certificate Signing Requests		Created

Licensed to 0311M5RWK0N8Q111S



3-2-8 CA 証明書のインポート (PSA300)

NetAttest EPS からダウンロードした CA 証明書を PSA300 にインポートします。

[Configuration]-[Certificates]-[Trusted Client CAs]の「Import CA Certificate」から、CA 証明 書(nacacert-pem.cer)をインポートします。

続いて、インポートされた CA 証明書をクリックし、CRL の設定を行います。

Secure Secure	
Pulse Connect Secure	Help
System Status Configuration Network IF-MAP Federation	Configuration > Certificates > Trusted Client CAs > Import Trusted Client CA
Log/Monitoring Reports Behavioral Analytics Authentication	Certificate file
Auth. Servers Administrators Admin Realms	Import from: ファイルを選択 選択されていません
Admin Roles Users User Realms User Roles Resource Profiles	Import Certificate
Resource Policies Pulse Secure Client Enterprise Onboarding Maintenance	
System > Import/Export > Push Config > Archiving > Troubleshooting >	
Licensed to 0311M5RWK0N	N6Q1115

S Pulse Secure				
Pulse Connect Secure			Help G	uidance Switch to New UI Sign Out
🗄 System				
Status >	Configuration > Certificates >			
Configuration >	Trusted Client CAs			
Network +				
Clustering >				
Log/Monitoring	Configuration			
Reports >	Certificates			
Behavioral Analytics >	Licensing Pulse One Security Certificates DMI Agent NCP Sensor	S Client Types Pulse Collaboration	Virtual Desktops User Record Synchroniz	ation IKEv2 SAML Mobile VPN Tur
🗄 Authentication	Device Castificates Texted Client City Texted Server City Cadevication Castificates C	tiont Auth Centificates Centificates Validity Ch	ark	
Signing In +	Server detailed and an and a most of server and a code signing detailed as			
Endpoint Security >				
- Administrators	Port Selection for OCSP and CRL Traffic			
Admin Realms >	Internal Port External Port Managem	ent Port		
Admin Roles >	Note: Port Selection settings are node-specific. Please configure the settings individually for differe	nt nodes in cluster		
🗄 Users				
User Realms >	Save			
User Roles >	Care			
Resource Policies >				
Pulse Secure Client >	Users can be required to present valid client-side certificates to sign in(see the	e realm-specific Certificate Authentica	tion Policy page). Specify trusted certificate au	thorities.
Enterprise Onboarding >				
Maintenance	Auto-Import options Proxy Settings Import CA Certificate Delete			
System >	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
Push Config >		Yoo	2018/11/15 - 2028/11/12	Lies CPLs
Archiving >		tes	2018/11/15 - 2028/11/12	USE CRES
Troubleshooting >				
Licensed to 0311MSRWK0N	R01115			
Copyright © 2001-2018 Pu	ise Secure, LLC, All rights reserved.			



「Client certificate status checking」のいくつかの項目にチェックを入れ、

次に、「CRL Checking Options」をクリックします。

S Pulse Secure				
Pulse Connect Secure				Help Guidance Switch to New UI Sign Out
System	Configuration > Trusted Client CAs >			
Configuration > Network >	Trusted Client CA			
Clustering IF-MAP Federation	Catificate			
Log/Monitoring > Reports >	Certificate			
Behavioral Analytics >	Issued To: > TestCA			
Signing In >	Issued By: TestCA Valid Dates: Nov 15 00:40:4	2 2018 GMT - Nov 12 00:45:42 2028 GMT		
Auth. Servers	Details: • Other Certificate	a Details		
Administrators	Renew Certificate			
Admin Roles →				
User Realms Vser Roles Vser Roles	Client soutificate status checking			
Resource Profiles	chent certificate status checking			
Resource Policies Pulse Secure Client O None				
Maintenance	Use OCSP (Online Certification State Use CDLs (Cartificate Devector Line)	us Protocol)		
System Import/Export	Use OCSP with CRL fallback	sts)		
Push Config > Archiving >	 Inherit from root CA 			
Troubleshooting >	✓ Verify Trusted Client CA			
	In addition to verifying the validity of client or repeat up the chain until reaching the root true	ertificates, you can also verify that this trusted client CA is valid. E isted client CA.	nabling this will check the revocation status of this certificate, based on th	he issuer's certificate status checking configuration, and
	Trusted for Client Authentication			
	Uncheck here to exclude the CA from being to	usted for client certificate authentication, if this CA was added for	other trusting purpose such as SAML signature verification or machine ce	rtificate validation.
	Participate in Client Certificate	Negotiation		
	Indicating whether this CA will be sent t	the browser for client certificate selection. To stop a client certificate selection.	cate being prompted by the browser, this flag of all the upper level CAs in	the CA chain of the certificate should be deselected.
	Skip Revocation check when OCSP	CDP server is not available		
	Accept client certificate if CDP Server or OCS	P Responder is not reachable/resolvable.		
	Advanced Certificate Processing Settings			
	Note: Enabling the certificate polic to be rejected.	y settings below will cause path validation to	comply strictly with RFC 5280. This may cause som	ne previously accepted certificate paths
	Initial Inhibit Policy Mapping			
	Policy mapping for certificate path is inhibited			
	Initial Require Explicit Policy			
	Path must be valid for at least one of the cert	ficate policies in the Initial Policy Set below		
	Initial Policy Set:	A set of certificate policy identifiers nami	19	
		the policies that are acceptable to the certificate user		
		One policy per line. e.g. // 1.3.6.1.4.1		
		2.16.840.1.101.3.2.1 Empty value indicates any policy		
	Save Changes			
	CRL Settings	fy the oppoint validity of user certificates, and are obtained from	CRI distribution points (CDP). To enable CRI checking, click CRI Checking	Options and specify the options
	CRL Checking Options Update	Now Enable Disable		
	D CBL distribution points		Ctatus Last Lindated	Next Lindate
	No CRL checking		Status Last Optiated	Next opuare

Licensed to 0311M5RWK0N8Q111S Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
Client certificate status checking	
- Use CRLs	選択
- Verify Trusted Client CA	有効
- Trusted for Client Authentication	有効
- Participate in Certificate Negotiation	有効



「CRL Distribution Points(CDP)」で「Manually configured CDP」を選択し、「CDP URL」に CRL の保存場所 URL を記載します。

~	
Q	Dulco Socuro
~	Pulse Secure

v		
Pulse Connect Secure		
- System		
Status	Conferentian > Trusted Cli	
Configuration	CPL Checking C	Intions
Network	CRE CHECKING C	puons
Clustering	Specify the CRL distr	ibution point(s) from which to download the CRL, as well as how often to download.
IF-MAP Federation		
Log/Monitoring	Use: Manually conf	figured CDP T
Reports	•	
Behavioral Analytics	Specify a HTTP o	r LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, enter the appropriate credentials as well.
Authentication		
Signing In	Primary CD	P
Endpoint Security	CDD UDL.	http://doi.doi.doi.doi.doi.doi.doi.doi.doi.doi.
Auth. Servers	CDP URL:	nitp://192.166.1.2/cens/cens.cn
- Administrators		HTTP example:
Admin Realms	•	Incp//server.domain.com/ass/domain.case/ver.ch
Admin Roles	>	dap://ldap.domain.com:6000/CN=ldap.CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=com?certificateRevocationList?base?obje
- Users	Admin DN:	(LDAP only)
User Realms	Bacoword:	((000 cch))
User Roles	Password.	
0 0 01		

項目	値
CDP URL	http://192.168.1.2/certs/certs.crl



3-3 PSA300の VPN 接続に関する設定

3-3-1 RADIUS/Certificate Serverの設定

「Auth. Servers」の「New RADIUS Server」にて RADIUS サーバーを追加します。

Secure Secure								
Pulse Connect Secure								
- System								
Status >	Auth Convers >							
Configuration >	New RADIUS	Server						
Network >	nen nubioio							
Clustering >							_	
IF-MAP Federation →	* Name:	EPSTEST	-		Label to reference this serve	er.		
Log/Monitoring →								
Reports >	NAS-Identifier:	Pulse Sec	ure Appliance		Name of the device as know	vn to RADIUS s	erver	
Behavioral Analytics >>								
- Authentication	Primary Server							
Signing In →								
Endpoint Security	* RADIUS Server	:	192.168.1.2	Name or IP address				
Auth. Servers	* Authoptication	Dorts	1010					
 Administrators 	Authentication	Port:	1012					
Admin Realms >	* Shared Secret:		•••••					
Admin Koles	* Accounting Port		1813	Port used for RADIUS accounting, if applicable		le		
User Realms		Addross:			IDv4/IDv6 addross		_	
User Roles >	NAS IFV4/IFV0	Audress.			IPV4/IPV0 address			
Resource Profiles >				項目			値	
Resource Policies >>	* Timeout:		30 seco					
Pulse Secure Client >	* Retries:		0	Name F		FPSTEST		
Enterprise Onboarding >			<u> </u>			2131	201	
- Maintenance					dontifior		Dulco	Socuro Applianco
System >	Users authent	ticate usin	ig tokens or o	NAS-1	uentinei		ruise	Secure Appliance
Import/Export >	Note: If you sele and this credentia	ct this, the d al will not be	levice will send th used in automati		-			
Push Config >	Radius Server 192.168.1.2					168.1.2		
Archiving >								
I roubleshooting +	bubleshooting			Authentication Port		1812		
		Shared Secret se		secret				
				Accou	nting Port		1813	

次に「Auth. Servers」の「New Server」より「Certificate Server」を追加します。

ulse Connect Secure					
System					
Status	Auth Servers >				
Configuration	New Certificate Server				
Network	•				
Clustering	P				
IF-MAP Federation	÷				
Log/Monitoring	Name:	naeps.local		Label to reference this server.	
Reports)				
Behavioral Analytics	User Name Template:	<certdin.cin></certdin.cin>		Template for constructing user n	iami
Authentication		The template can contain	textual characters as well as va	riables for substitution. Variables show	uld b
Authentication Signing In	>	The template can contain expressions and policy co	textual characters as well as va nditions. All of the certificate va	riables for substitution. Variables shou riables are available.	uld t
Authentication Signing In Endpoint Security	b b	The template can contain expressions and policy co Examples:	textual characters as well as va nditions. All of the certificate va	iriables for substitution. Variables shou riables are available.	uld t
Authentication Signing In Endpoint Security Auth. Servers	> >	The template can contain expressions and policy co Examples: <certdn.cn></certdn.cn>	textual characters as well as va nditions. All of the certificate va First CN from the subject DN	iriables for substitution. Variables shou riables are available.	uld t
Authentication Signing In Endpoint Security Auth. Servers Administrators	>	The template can contain expressions and policy co Examples: <certdn.cn> <certattr.serialnumber></certattr.serialnumber></certdn.cn>	textual characters as well as va nditions. All of the certificate va First CN from the subject DN Certificate serial number	riables for substitution. Variables shou riables are available.	uld t
Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms	> >	The template can contain expressions and policy co Examples: <certdn.cn> <certattr.serialnumber> <certattr.altname.xxx></certattr.altname.xxx></certattr.serialnumber></certdn.cn>	textual characters as well as va inditions. All of the certificate va First CN from the subject DN Certificate serial number Where xxx can be:	riables for substitution. Variables shou riables are available.	ald f
Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles	> > >	The template can contain expressions and policy co Examples: <certdn.cn> <certattr.serialnumber> <certattr.altname.xxx></certattr.altname.xxx></certattr.serialnumber></certdn.cn>	textual characters as well as va nditions. All of the certificate va First CN from the subject DN Certificate serial number Where xxx can be: Email The Email alternate na	riables for substitution. Variables shou riables are available. me	uld t
Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles)))	The template can contain expressions and policy co Examples: <certdn.cn> <certattr.serialnumber> <certattr.altname.xxx></certattr.altname.xxx></certattr.serialnumber></certdn.cn>	textual characters as well as va inditions. All of the certificate va First CN from the subject DN Certificate serial number Where xxx can be: Email The Email alternate na UPN The Principal Name alternate	rriables for substitution. Variables shou riables are available. me emate name	uld t
Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles Users Users)))	The template can contain expressions and policy co Examples: <certdn.cn> <certattr.serialnumber> <certattr.altname.xxx></certattr.altname.xxx></certattr.serialnumber></certdn.cn>	textual characters as well as va inditions. All of the certificate va First CN from the subject DN Certificate serial number Where xxx can be: Email The Email alternate na UPN The Principal Name alt etc	riables for substitution. Variables shou riables are available. me ernate name TTE E	id t /古
Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles Users User Realms User Realms	 > > > > 	The template can contain expressions and policy co Examples: <certdn.n> <certattr.serialnumber> <certattr.altname.xxx> <certdntext></certdntext></certattr.altname.xxx></certattr.serialnumber></certdn.n>	textual characters as well as va inditions. All of the certificate va First CN from the subject DN Certificate serial number Where xxx can be: Email The Email alternate na UPN The Principal Name alt etc The complete subject DN	riables for substitution. Variables shou riables are available. me 項目	値



3-3-2 VPN Rolesの設定

[User Roles]-[New User Role]よりユーザーに割り当てるロールの設定を行います。

ここでは、許可する VPN 接続方法等を指定します。Pulse Secure client にチェックを入れます。

Image: Second Columbia Af Refare Af Refare Bit Second Columbia Bit Second C					
Average					
intermediation if if default in the image is a second second and in the later of the second and intermediate is the second a					
Production Name: Production Second Carlow Contract Contract <t< td=""><td></td></t<>					
Second Call Name: VPARCales Second Call Control Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Second Call Enable Cloud Application Visibility Second Call Second Call Second Call Second Application Manager Second Application Manager Second Application Manager Second Application Manager Second Application Manager Second Application Manager Second Application Manager Second Application Manager					
Same: VPARcles Description: Prime: Sector Prime: Sector<					
gin gin Server Vindows Files, WinklyNPS Server Server Server Server Server Server Server Vindows Server Vindows version Server Server Server Server Server Vindows version Server <					
Ministerior Ministerior Network Network <td></td>					
Server in the server is a part of the server for the server is a secret of the secret is secret of the server is a secret of the secret is secret of the secret of th					
Reading Options Section and appearance options are specified in Default Detacop. Obeck the following if this role should override these defaults. Image: Ima					
Role • and • Session options • • • • • and •					
definition VLAN/Source IP © Session Options U to Options U to Options U to Options Puble Secure Client Dynamically deliver Puble Secure client to Windows and MAC OSX users Enable Cloud Application Visibility onfig 0 onfig 0 onfig 0 onfig 0 onfig 0 web Enable Cloud Application Visibility onfig 0 web Elfest, Windows Elfest, Windows Nete: On Windows Mobile, Puble Secure client is delivered via WEAM Bisocone 0 Web Elfest, Windows Elfest, Windows Nete: On Windows Mobile, Puble Secure client is delivered via WEAM Bisocone 0 Windows version Nete: On Windows Mobile, Puble Secure client is delivered via WEAM Web Elfest, Windows Interprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features deabled here may be granted by other roles Option Web Elfest Enterprise Obboarding Check the Enterprise Obboard profiles to enable for this user role, and specify any role					
Secure Culture Western Uptions W Dig Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX uses Enable Cloud Application Visibility Western Construction Access Features Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Web Files, Windows Files, UMIX/NFS Telnet/SSH Secure Application Manager Windows version Terminal Services Windows version Terminal Services Windows version Terminal Services Windows version Terminal Services Windows and profiles to anable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles Secure Application Terminal Services Windows Version Terminal Services Westings VPN Tunneling (ncludes 3KEv2) Enterprise Device Onboarding Check the Enterprise Onboarding (versi, with and Certificate Profiles) Serve Changes					
Utbody Total and a specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Web Files, Windows Secure Application Manager Windows version Terminal Services Windows version Terminal Services Windows Windows Terminal Services Wintuk Saccess Meetings VPN Tunneling (includes IKEv2) Enterprise Device Onboarding (includes IKEv2) Enterprise Device Onboarding (VPH, Writ and Certificate Profiles) Secure Mail Enterprise Onboarding Secure Mail Enterprise Onboarding VPN Lynes Secure Mail Enterprise Onboarding (VPH, Writ and Certificate Profiles)					
Access Features Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Web Files, Windows Files, WINX/NFS Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Windows Version Descure Application Manager Java Version Terminal Services Windows Version Terminal Services Windows Version Terminal Services Windows Version Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles at specify any role-based options. Note that features disabled here may be granted by other roles at specify any role-based options. Note that features disabled here may be granted by other roles at specify any role-based options. Note that features disabled here may be granted by other roles at the specific Onboarding (vote, wifi and Certificate Profiles) Secure Mail Enterprise Onboarding (vote, wifi and Certificate Profiles) Secure Mail Enterprise Onboarding (vote, wifi and Certificate Profiles) 10 2011115500000000000000000000000000000					
exhoding Access Features Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Web Files, Windows Files, UNIX/NFS Telnet/SSH Secure Application Manager Windows Version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java Version Terminal Services Wintub Sectors WPN Tunneling Check the Enterprise Device Onboarding Check the Enterprise Device Onboarding Check the Enterprise Onboarding Check the Enterprise Onboarding Secure Mail Enterprise Onboarding Winduw Secure Save Changes					
Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.					
Create the teaches to analyse for this user role, and specify any role-based options, hote that reaches displace here may be granted by other roles assigned to the user. Web Files, Windows Files, WINX/NFS Secure Application Manager Windows version Ferminal Services Virtual Desktops HTML5 Access Meetings VPN Tunneling (includes IKEv2) Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user. Seve Changes					
Web Files, Windows Files, UNIX/NFS Telnet/SSH Secure Application Manager Windows version Iterminal Services Virtual Desktops HTML5 Access Meetings VPN Tunneling VPN Tunneling Includes IKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboarding Interprise Onboarding WNH, Writ and Certificate Profiles) Secure Mail Enterprise Onboarding (VPN, Writ and Certificate Profiles)					
Files, Windows Files, UNIX/NFS Telnet/SSH Secure Application Manager Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java version Terminal Services Windows Version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java version Terminal Services Windows Secure Secure Windows Mobile, Pulse Secure client is delivered via WSAM Java version Terminal Services Wintub Sectops HTML5 Access Metings VPN Tunneling (Includes JKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles of Secure Mail Enterprise Onboarding (VPN, wfi and Certificate Profiles) Save Changes Interprise Onboarding 10 2011/165/WMORECOLLS Key Change					
Control of the cont					
Telnet/SSH Secure Application Manager Windows Version Java version Terminal Services Windows Version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java version Terminal Services Windows Devices Windows Version Interview Windows Version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java version HTML5 Access Meetings V VPN Tunneling (includes IKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles of Secure Mail Enterprise Onboarding Save Changes Save Changes 00 2011MSW0000021115 10 2021105 Pulse Secure, LLC, All rights reserved.					
Secure Application Manager Windows version Java version Terminal Services Winto Secure Secure clent is delivered via WSAM Java version Terminal Services Winto Secure Secure Clent is delivered via WSAM Winto Desktops HTML5 Access Meetings VPN Tunneling (includes JKEv2) Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles at Secure Mail Enterprise Onboarding Save Changes Save Changes 10 0311MSWW000201115 12 0302-1015 Builes Secure, LLC, All rights reserved.					
Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM Java version Terminal Services Virtual Desktops HTML5 Access Meetings WPN Tunneling VPN Tunneling (includes IKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboarding Check the Enterprise Device Onboarding (VPM, Wift and Certificate Profiles) Secure Mail Enterprise Onboarding Save Changes Image:					
D Java version Terminal Services Virtual Desktops HTML5 Access Meetings VPN Tunneling (includes 1KEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles a Secure Mail Enterprise Onboarding (VPM, Wift and Certificate Profiles) Save Changes To 0311M5WW000E01115 You Desk Secure, LLC, All rights reserved.					
Constant of the second					
In Climital Desktops ● Virtual Desktops ● HTML5 Access ● Meetings ● VPN Tunneling (includes JKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify any role-based options. Note that features disabled here may be granted by other roles at a specify at a spe					
HTML5 Access Meetings VPN Tunneling (includes IKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles a Secure Mail Enterprise Onboarding (VPN, Wifi and Certificate Profiles) Save Changes To 0311M5WK00Ne03115 to 0311M5WK00Ne					
Image: Second Seco					
VPN Tunneling (includes JKEv2) Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles a Secure Mail Enterprise Onboarding (VPM, Wifi and Certificate Profiles) Save Changes To 0311MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK0080911 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 031MSWK008091115 to 040 to 0					
Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles a Secure Mail Enterprise Onboarding (VPN, Wifi and Certificate Profiles) Save Changes Save Changes QUE2018 Secure, LLC, All rights reserved.					
Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles. Secure Mail Enterprise Onboarding (VPH, Wifi and Certificate Profiles) Save Changes To 0311MSRWK00801115 to 0311MSRWK00801115 to 0311MSRWK00801115 to 0311MSRWK00801115					
Enterprise Device Onboarding Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles Secure Mail Enterprise Onboarding (VPN, Wrif and Certificate Profiles) Save Changes Save Changes To 0311M5RWK008021115 C 2001-2018 Data Secure, LLC, All rights reserved.					
Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles Secure Mail Enterprise Onboarding (VPN, Wrif and Certificate Profiles) Save Changes Save Changes (0 0311M5RWK00R021115 C 00311M5RWK00R021115 C 2001-2018 Data Secure, LLC, All rights reserved.					
Secure Mail Enterprise Onboarding (VPN, Wifi and Certificate Profiles) Save Changes Save Changes 可目目 10 0311MSRWKONRQ1115 12 2001-2018 Pulse Secure, LLC. All rights reserved.	signed to the us				
• Secure Mail • Enterprise Onboarding (VPN, Writ and Certificate Profiles) Save Changes Save Changes • 0 0311MSRWKONRQ1115 • 0 0311MSRWKONRQ1115 • 0 2001-2018 Pulse Secure, LLC. All rights reserved.					
Save Changes Save Changes 00311MSRWKON8Q1115 © 2001-2018 Pulse Secure, LLC. All rights reserved.					
Save Changes Save Changes I G 0011MSRWK0N8Q1115 t © 2001-2018 Pulse Secure. LLC. All rights reserved.					
to 0311MSWK0NeQ111S t © 2001-2019 Pulse Secure, LLC, All rights reserved.					
Save Changes 項目 值 to 0311MSRWK0N8Q111S to 2001-2018 Pulke Secure. LLC. All rights reserved.					
to 0311MSRWK0N8Q111S t © 2001-2018 Pulse Secure, LLC. All rights reserved.					
to 0311M5RWK0N8Q111S t © 2001-2018 Pulse Secure, LLC. All rights reserved.					
Control Para Decire, Control Para Decire, Control Para					
Name VPNRoles					
Options Session Opt					
	ons				
UI Ontions	ons				
	ons				
Pulse Secur	ons				
UI Options	ONS				

Access features

VPN Tunneling



次に、画面上タブの「Web」より「New Bookmark」を選択し、以下を設定します。 ※本設定は任意です。本設定をすることで、ログイン後、登録した BookMark が表示されます。

S Pulse Secure				
Pulse Connect Secure				Help Guidance Switch to New UI Sign Out
- System				
Status				
Configuration	Roles > VPNRol	es >		
Network	, New We	DOOKIIIAIK		
Clustering	- F			
IF-MAP Federation	- P			
Log/Monitoring	* Type:		Standa	ard 🔻
Reports	Name:		Home	Page
Behavioral Analytics	Descrip	tion:		
- Authentication	Descrip	cion.		
Signing In	- F			
Endpoint Security	- F			h
Auth. Servers				
- Administrators				
Admin Realms				
Admin Roles	Bookmark To			
- Users				
User Realms	* URL: http://	//102.169.1.150/aalitar	aha html	Example: http://www.domain.com/
User Roles	> nup.	/192.106.1.150/Solitor	nnp.ntmi	bookmark URL.
Resource Profiles	- F-		_	
Resource Policies	- F			
Pulse Secure Client	> Disalau Ontin			
Enterprise Onboarding	Display Optio	ns		
- Maintenance		Alson is a stress state to a		
System	, Open	the bookmark in	a new wi	ldow
Import/Export	▶ 🗆 R	ead-only browser ac	ddress bar	
Push Config	• D	o not display the We	eb browser	's menu and toolbar
Archiving	+			
Troubleshooting	•			
	Save Change	5		
	Sava C	hanges Save + Nev		
	* in	dicates required field	vv	

項目	値
Name	Home Page
URL	http://192.168.1.150/solitonhp.html



3-3-3 VPN Access Policyの設定

[Resource Policies]-[Web]の「New Policy」でアクセスポリシーの設定を行います。「Roles」で 作成した Role(VPNRoles)を選択し、選択したロールとポリシーの紐付けを行います。「Resources」 で定義した接続に対して、VPNRoles が適用されます。

Pulse Connect Secure System Status Configuration	Resource Policies New Polici	> <u>VPN Tunneling Access Control</u> > Y	Help Guidance	2 Switch to New UI Sign Out
Network + Clustering +	_			
IF-MAP Federation Log/Monitoring Reports Behavioral Analytics Authentication Signing In	* Name: Description:	VPN Access Policy	Required: La	abel to reference this policy.
Endpoint Security	-			
Administrators Admin Realms Admin Roles	Resources			
Users		Specify the resources for which t	his policy applies, one per line.	
User Roles + Resource Profiles + Resource Policies +	IPv4 Resources:	http://*:80/* 192.168.0.0./16:*/*	Examples: tcp://*:1-1024 tcp://*:80,443 udp://10.10.10.0/24:* //10.10.10.10/255.255	.255.255
Pulse Secure Client + Enterprise Onboarding + Maintenance System + Import/Export +	IPv6 Resources:		<pre>Louid.10.0/24 Examples: tcp://[2001:dbs:1]:80,443 udp://[2001:dbs:1]:1-1024 icmpv6://[2001:dbs:1]:464] 2001:dbs:11 [2001:dbs:1] [2001:dbs:1]</pre>	1
Push Config Archiving Troubleshooting	FQDN Resources:		[2001:db8::1-2001:db8::ffff Examples: www.mywebsite.com *.mywebsite.com] e resolved to IPv4 addresses only.
	Roles			
		Policy applies to ALL Policy applies to SELI Policy applies to all n Available roles: Onboard SAMLtest Users credential demo	roles ECTED roles Dies OTHER THAN those selected bel Selected roles: -> VPNRoles ->	low
	Actions			
		 Allow access Deny access Use Detailed Rules(a 	vailable after you click 'Save Change	25')
	Save Changes		項目	値
		Save Changes Save as	Name	VPN Access Policy
	AD10VC	* indicates required field	Resources	http://*:80/*
Copyright © 2001-2018 Pu	Ise Secure, LLC. All r	ights reserved.		192.168.0.0./16:*/*
			Roles	Policy applies to SELECTED
			Selected roles	VPNRoles



3-3-4 Authentication Realms の設定

[User Realms]-[New User Realms]レルムの設定を行います。

「Authentication」に Certificate Server(naeps.local)を指定、「Additional authentication server」 には RADIUS(EPSTEST)を指定します。

本設定をすることで、証明書認証+ユーザーID/Password での認証が可能になります。

Secure Secure		
Pulse Connect Secure		
System Status Configuration Network Clustering	User Realms > New Authentication Real	lm
IF-MAP Federation Log/Monitoring Reports Behavioral Analytics Authentication Signing In Endpoint Security Auth. Servers Administrators	* Name: Description:	VPNRealms
Admin Realms Admin Roles Users User Relams Resource Profiles Resource Policies Pulse Secure Client Enterprise Onboarding Maintenance	Servers Specify the servers to use for authentication Authentication: User Directory/Attribute: Accounting: Device Attributes:	n and authorization. To create or manage servers, see the <u>Servers</u> page. naeps.local None ▼ None ▼ None ▼ None ▼
System , Import/Export , Push Config , Archiving , Troubleshooting ,	Additional Authentication Server Enable additional authentication You can specify an additional authentication below, in which case the user will not be pr	on server n server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on the sigr rompted for the credential.
	Enable adaptive authenticati Note: Adaptive authentication is supporte authentication server selected as authent Authentication #2: Username is:	ion ed by leveraging the behavioral analytics. Enable behavioral analytics on 'System->Behavioral Analytics->Con itication server above. EPSTEST specified by user on sign-in page predefined as: USER>
	Password is:	 specified by user on sign-in page predefined as: <password></password> Mask static password End session if authentication against this server fails

項目	値
Name	VPNRealms
Authentication	naeps.local
Additional authentication server	EPSTEST



次に、画面上タブの Role Mapping」よりユーザーとロールの紐付け設定を行います。

「…then assign roles」では VPNRoles を指定します。

Secure Secure			
Pulse Connect Secure			
- System			
Status >			
Configuration >	Dolo Manning Pulo		
Network >	коге маррину ките		
Clustering >	Rule based on: Username	Undate	
IF-MAP Federation >		opolio	
Log/Monitoring >	* Name: TESTRoleMAP		
Reports >	Name. TESTROIEMAP		
Benavioral Analytics >	n I 11		
Authentication	Kule:11 username		
Endopsiot Security			
Auth, Servers	is 🔻 \star	If more than one username should match, enter one username per lin	e. You can use * wildcards.
- Administrators			
Admin Realms >			
Admin Roles >			
- Users			
User Realms >			
User Roles >	then assign these roles		
Resource Profiles >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			
Resource Policies >>	Available Roles: Selected	1 Roles:	
Pulse Secure Client →	Users Add -> VPNRole	es 🔺	
Enterprise Onboarding >			
- Maintenance	Remove		
System >			
Import/Export >			
Push Config P			
Troubleshooting	Stop processing rules when this rule	matches	
	To manage roles, see the Roles configuration page.		
		тар <u></u>	店
		現日	10
		News	TECTDALAMAD
		мате	TESTROIEMAP

Role if username…

... then assign these roles

is:*

VPNRoles



3-3-5 Sign-In Policyの設定

[Sign In]-[Sign-in Policies]の「New URL」からサインインポリシーの設定を行います。ここでの設定が VPN クライアント(Pulse Secure クライアント)で接続する際の接続先 URL になります。「Authentication realm」では、VPNRealms を指定します。

Pulse Connect Secure				
System				
Status	Signing In > Sign-in Policies >			
Configuration	New Sign-In Policy			
Network				
Clustering	User type: Users Administrators Meeting Authorization Only Access			
IF-MAP Federation	Sign-in LIPL * */vintest/ Format: <host>/signthing * as</host>			
Reports	Sign force representation of the second			
Behavioral Analytics	Description:			
Authentication				
Signing In	Default Sign-In Page V			
Endpoint Security	Sign-in page: To create or manage pages, see <u>Sign-In pages</u> .			
Auth. Servers	Meeting URL: */meeting/ •			
Administrators				
Admin Realms				
Admin Roles	A share to share the state of t			
Users				
User Realms	2			
User Roles	Specify how to select an authentication realm when signing in.			
Resource Profiles				
Resource Policies	• User types the realm name			
Pulse Secure Client	The user must type the name of one of the available authentication realms.			
Maintenance				
System	User picks from a list of authentication realms The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is as o			
Import/Export				
Push Config	Authentication page or the Administrator Authentication page.			
Archiving +				
Troubleshooting	Available realms: Selected realms:			
	Users A Add -> VPNRealms A Move Up			
	Remove Move Down			
	Configure SignIn Notifications			
	Configure SignIn Notifications			
	Configure SignIn Notifications			
	Configure SignIn Notifications Pre-Auth Sign-in Notification			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Rest-Auth Sign-in Notification			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Advanced Settings			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Notification Advanced Settings Enable redesigned pages for this Sign-in Policy			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for cloud Secure access.			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Secure access.			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Secure access.			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Secure access. Save Changes			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Becure access. Save Changes			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Secure access. Save Changes Save Changes			
	Configure SignIn Notifications Pre-Auth Sign-in Notification Post-Auth Sign-in Notification Advanced Settings Enable redesigned pages for this Sign-in Policy Note: Redesigned pages are used only for Cloud Secure access. Save Changes Save Changes			

1115		
Secur	User Type	Users
	Sign-in URL	*/vpntest/
	Authentication realm	User picks from a list authentication realms
	Selected realms	VPNRealms



3-3-6 IP プールの設定

[Resource Policies]-[VPN Tunneling Connection Profiles]で、VPN クライアントに払い出す IP アドレス(IP プール)等のネットワーク設定を行います。

			Help Guida			
Resource Policies	> VPN Tunneling Connection Profiles >					
New Profi	le					
" Name:	VPN-TEST		Required: Label to reference this profile.			
Description:						
	Save Changes Save as Conv					
IPv4 address as	ssignment					
	Specify how IPv4 addresses are assigned to clients.					
	DHCP convers					
-	Specify the name or IPv4 address for up to 3 DHCP servers					
	DHCP options					
	Specify any DHCP options that should be sent to the DHCP Server. E option value, and option value type. Option values can be token repl	inter the option number, laced values.				
	Note: Please refer to Admin Guide for more details.					
	Delete					
	Option Number Option Value	Option Type				
		String Add				
	132.168.1.200-192.168.1.210 10.10.1.1-10.10.5.20 10.10.10.10-100	0				
IPv6 address as	IPv6 address assignment					
	Specify the assignable IPv6 address ranges for this profile, one per line This Option is not supported for Cluster Specific Configuration in Config	-Only Active-Active WAN Cluster.				
	Note: Please refer to Admin Guide for details.	Examples:				
		2001:DB8::5:100-20 2001:DB8::6:0/112	001:DB8::5:00			
		(2001-DB97-50				
		2001;DB8::7:50				
Connection Sett	ings	2001:D88::7:50				
Connection Sett	ings	2001;D88::7:50				
Connection Sett	tings : • ESP (maximize performance)	2001/D88/17/50	(This is 19v4 specific settings)			
Connection Sett	tings : • ESP (maximize performance) UDP port:	2001:DB8::750 4500 For 1	(This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u>			
Connection Sett	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout:	2001:088:750 4500 For 1 15) (This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u> seconds (15-65335 seconds)			
Connection Sett	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based):	20 2001/08417150 4500 For 1 15 20	O (This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u> seconds (13-65335 seconds) minutes (20-86400 minutes)			
Connection Sett	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred):	4500 For 1 15 20 0	(This is IPv4 specific settings) Pv6 please go to: IPv6 UDP settings seconds (19-65335 seconds) minutes (20-86400 minutes) bytes (0 implies no limits)			
Connection Sett	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred): Replay Protection: CDD Transector Ook (do EDL fallback timeout):	4500 For 1 15 20 0	(This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u> seconds (12-65335 seconds) minutes (20-6400 minutes) bytes (0 implies no limits)			
Connection Set	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred): Replay Protection: ESP Transport Only (No SSL fallback, this setting is for Encryotion:	2/2 2003/088/17/59 4500 For 1 15 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
Connection Set	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred): Replay Protection: ESP Transport Only (No SSL fallback, this setting is for Encryption:	2/2 2003/084:17:50 4500 For T 15 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u> seconds (12-63335 seconds) minutes (20-64400 minutes) bytes (0 implies no limits) AES128/MD5 (MD5 is insecure. Option is not recomm AES128/SHA1			
Connection Set	tings : • ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred): Replay Protection: ESP Transport Only (No SSL fallback, this setting is for Encryption:	2/2 2003/084:17:50 4500 For 7 15 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(This is IPv4 specific settings) Pv6 please go to: <u>IPv6 UDP settings</u> seconds (15-65335 seconds) minutes (20-66400 minutes) bytes (0 implies no limits) AES128/MD5 (MD5 is insecure. Option is not recomm AES128/MD5 (MD5 is insecure. Option is not recomm			
Connection Set	tings ESP (maximize performance) UDP port: ESP to SSL fallback timeout: Key lifetime (time based): Key lifetime (bytes transferred): Replay Protection: ESP Transport Only (No SSL fallback, this setting is for Encryption:	2 2001/084/7/59 44500 For 1 15 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				

項目	値
Name	VPN-TEST
IP Address Pool	192.168.1.200 - 192.168.1.210





	To override the standard D	NS settings, specify custo	iom settings for this profile here.
DNS Settings:	O IVE DNS Settin	gs	
	Manual DNS Se	ttings	
	Primary DNS:	192.168.1.102	IPv4/IPv6 address
	Secondary DNS:		IPv4/IPv6 address
	DNS Domain(s):		Example: "company.com, company.net"
	WINS:		Name or IP address
	O DHCP DNS Sett	ings (only applica	able if DHCP Server is chosen)
Auto-allow	Auto-allow IP's	in DNS/WINS se	ettings (only for split-tunnel enabled mode)
Split Tunnel DNS	 Search d 	lient DNS first, the	an the device
Search Order:	O Search t	he device's DNS se	ervers first, then client
	Search of Sea	device DNS only	
	Notes:		
	These settings	apply only to syste	ems with Solit Tunneling enabled and do not apply to third-party clients
	 For Windows 8 	clients, selecting e	either the first or second radio button sends DNS requests to both the server and client's DNS at
	 Windows 10 w DNS requests 	ill always send the to the server's DNS	DNS request to the server's DNS first then the client's DNS, so selecting either the first or secon 5 first.
	 OSX does not 	support sending DN	NS requests to only the Pulse Secure gateway's DNS. So, for OSX clients, clicking the third radio
	 For Windows P 	tton. Phone and Windows	s machines running the In-Box VPN client, checking the third radio button sends all DNS requests
	DNS. Having e	ther other button o	checked causes only DNS requests matching the DNS domains (listed above) to go to the gatewa
	to the cherit's i		
Proxy Server Settings			
Proxy Server Settings	Specify a proxy server f No proxy server Automatic (URL 	for use in this connection r . for PAC file on ano	n profile, if appropriate. other server)
Proxy Server Settings	Specify a proxy server f No proxy server Automatic (URL Server address:	for use in this connection r for PAC file on ano v: 10 minute	n profile, if appropriate. other server)
Proxy Server Settings	Specify a proxy server f No proxy server Automatic (URL Server address: Update Frequence Defrash New 	for use in this connection r for PAC file on ano cy: 10 minute	n profile, if appropriate. other server) 25
Proxy Server Settings	Specify a proxy server f A to proxy server Automatic (URL Server address: Update Frequence Refresh Now	for use in this connection if for PAC file on ano y: 10 minute	n profile, if appropriate. other server) 25
Proxy Server Settings	Specify a proxy server No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu	for use in this connection r for PAC file on ano sy: 10 minute ination	n profile, if appropriate. other server) as
Proxy Server Settings	Specify a proxy server f No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server:	for use in this connection r for PAC file on ano y: 10 minute mation	n profile, if appropriate. other server) as
Proxy server settings	Specify a proxy server f No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client - Disable client -	for use in this connection r for PAC file on ano ry: 10 minute mation -side proxy setting	n profile, if appropriate. other server) as Port: 0 Port: 0 TS
Proxy server settings	Specify a proxy server of No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s	for use in this connection r for PAC file on ano vy: 10 minute minute ration -side proxy setting ide proxy setting	n profile, if appropriate. es Port: 0 19 19
Proxy server settings	Specify a praxy server 4 No proxy server Automatic (URL Server address: Update Frequence Refresh Now Manual configu Server: Preserve client Disable client-s	for use in this connection r for PAC file on ano cy: 10 minute ration -side proxy setting	n profile, if appropriate. other server) as Port: 0 ngs ja
Proxy server settings Roles	Specify a proxy server 4 No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client- Disable client-s	for use in this connection r for PAC file on ano vy: 10 minute iration -side proxy setting les	n profile, if appropriate. other server) as Port: 0 ngs p
Roles	Specify a proxy server 4 No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s Disable to ALL rol Dicy applies to ALL rol	for use in this connection r for PAC file on ano vy: 10 minute mation -side proxy setting les TED roles	n profile, if appropriate. other server) as port: 0 ngs J5
Roles Proxy server settings	Specify a proxy server (No proxy server (Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve Clent Disable client-s Disable client-s Disable sto ALL rol Displies to ALL rol Displies to ALL rol Displies to ALL rol	for use in this connection r for PAC file on ano for PAC file on ano y: 10 minute ration -side proxy setting les TED roles is OTHER THAN tho	n profile, if appropriate. other server) as port: 0 ngs gs see selected below
Roles Proxy server settings Roles Proxy server settings	Specify a proxy server d No proxy server Automatic (URL Server address: Update Frequence Refresh Now Manual configu Server: Preserve client Disable client-s Dicy applies to ALL rol olicy applies to SELEC olicy applies to SELEC ble roles:	for use in this connection r for PAC file on ano r rotion ration -side proxy setting les TED roles tes OTHER THAN tho Selected roles:	n profile. If appropriate. other server) ss Port: 0 port: 0 ss selected below
Roles Ques	Specify a proxy server of No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s Disable client-s Dicy applies to ALL rol Dicy applies to SELECC Dicy applies to all role able roles: Internet to the server of the server	for use in this connection r for PAC file on ano cy: 10 minute rration -side proxy setting les rED roles s OTHER THAN tho Selected roles: VPNR0es =	n profile. If appropriate. other server) as port: 0 ngs ps see selected below ::
Roles Ques	Specify a proxy server d No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s blicy applies to ALL rol blicy applies to ALL rol	for use in this connection r for PAC file on ano r ration -side proxy setting les TED roles is OTHER THAN tho Selected roles VPNRoles	n profile, if appropriate. other server) as port: 0 ngs ps see selected below a:
Roles Q Proxy server settings	Specify a proxy server d No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s Disable client-s	for use in this connection r for PAC file on ano ration -side proxy setting ide proxy setting les TED roles is OTHER THAN tho Selected roles: VPNRoles •	n profile, if appropriate. other server) as port: 0 ngs gs se selected below ::
Roles Proxy server settings Prox	Specify a proxy server d No proxy server d Automatic (URL Server address: Update Frequenc Refresh Now Manual configue Server: Preserve client Disable client-s Dicy applies to ALL rol Dicy applies to SELEC Dicy applies to SELEC	for use in this connection	n profile, if appropriate. st Port: 0 ng5 j5 ose selected below ::
Roles Proxy server settings Proxy sett	Specify a proxy server d No proxy server Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s Dicy applies to ALL rol obley applies to ALL rol obley applies to SELEC bity applies to all role able roles: Add -> Remove	for use in this connection r for PAC file on ano r ration -side proxy setting resonance of the setting resonance of the setting resonance of the setting resonance of the setting so OTHER THAN tho Selected roles	n profile, if appropriate. st Port: 0 ngs gs bse selected below s:
Roles Proxy server settings Roles Prox Proxy server settings Prox	Specify a proxy server d No proxy server d Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve client Disable client-s blicy applies to ALL rol blicy	for use in this connection r for PAC file on ano vy: 10 minute ration -side proxy setting reaction	n profile. If appropriate. st port: 0 ngs port: 0 see selected below ::
Roles © Prover Settings © Pro © Pro Availa Users Save Changes Save	Specify a proxy server d No proxy server d Automatic (URL Server address: Update Frequenc Refresh Now Manual configu Server: Preserve Clent Disable client-s Dicy applies to ALL rol Dicy	for use in this connection r for PAC file on ano r ration -side proxy setting les TED roles is OTHER THAN tho Selected roles VPNRoles	n profile, if appropriate. as Port: 0 ngs ps se selected below ::

Licensed to 0311M5RWK0N8Q111S Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
DNS Settings	Manual DNS Settigns
	192.168.1.102
Selected Roles	VPNRoles



4. Windows 版 Pulse Secure クライアントの設定

4-1 PC への証明書のインストール

NetAttest EPS から発行したデジタル証明書を PC にインポートする方法として、下記の方法などがあります。

- 1) NetAttest EPS-ap を使い、SCEP で取得する方法
- 2) PC に証明書ファイル(PKCS#12 形式)と CA 証明書を配置し、証明書インポートウィザー ドを使ってインポートする方法

上記いずれかの方法で CA 証明書とユーザー証明書をインポートします。 本手順では証明書のインポート方法については割愛いたします。



4-2Pulse Secure クライアントの取得と接続

Pulse Secure クライアントをダウンロードし、接続を行います。

「https://10.10.10.1/vpntest」にアクセスし、ユーザー証明書の選択とユーザーID/パスワードの入力を行います。

Windows セキュリティ × 証明書の選択	S Pulse Secure
サイト 10.10.1 に対する資格情報が必要です: user01 発行者: TestCA	Welcome to Pulse Connect Secure
有効期間: 2019/02/06 から 2020/02/06 証明書のプロパティを表示します その他	Secondary username user01 Secondary password Sign In
OK キャンセル	

表示されるページの「開始」ボタンをクリックし、クライアントソフトウェアのダウンロードを行う と自動的に Pulse Secure に接続されます。

「開始」
e -× (H) + / × 切断



4. Windows 版 Pulse Secure クライアントの設定

2回目以降は、Pulse Secure Client を起動し、ユーザー名/パスワードを入力して接続してください。





5. iOS 版 Pulse Secure クライアントの設定

5-1 iOS へのデジタル証明書のインポート

iOS 12 以降では、OS のストアにインポートしたクライアント証明書は、VPN 接続で利用できな くなりました。

EPS-ap を使用して証明書を配布する場合には、同時に VPN プロファイルも配布することで、VPN 接続時の認証に証明書を使用可能になります。

本資料では、EPS-apを使用して証明書の配布を行っています。

iOS 12 以降を使用する場合は、Pulse Secure Client v7.0.0 以降をご利用ください。

↓ iOS 10.3 以降は、OS の仕様によりプライベート認証局の CA 証明書をインポートする場合、インポートした証明書を手動で信頼させる必要があります。

VPN 設定			
	VPN		
接続名	Pulse Secure		
VPNサーバー	10.10.10.1/vpnt	est	
接続のタイプ	Pulse Secure	~	
保護領域			
役割			
:	オンデマンドVPI	N	
該当するドメインまたはホスト		要求があった時の処理	操作
		常(こ確立 🗸	追加
		·	
プロキシ			
構成	なし 🗸		
適用 キャンセル			

EPS-ap プロファイル管理ページの[プロファイル]-[VPN]-[接続タイプ]



\$ user01

5-2 Pulse Secure への接続

App Store からインストールした Pulse Secure クライアントを起動します。

EPS-ap を使用して証明書と VPN プロファイルを配布した場合、アプリ側で設定を行う必要はありません。Pulse Secure クライアントを起動し、VPN 接続を行います。

	Pulse Secure		
接続			
Pulse Secure 10.10.10.1/vpntest			
	接続		
	10.10.10.1	キャンセル	
	S Pulse Secure		
	Pulse Connect Secure		
user01			
•••••			
	Sign In	項目	値
	1	Secondary username	User01
		Secondary password	password
	↓		
	Pulse Secure		
接続			
• Pulse Secure https://10.10.10.1		***	
	接続中		

00:59:43



6. Android 版の Pulse Secure クライアント設定

6-1 Android へのデジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を Android デバイスにインポートする方法として、 下記の方法などがあります。

- 1) NetAttest EPS-ap を使い、SCEP で取得する方法
- 2) デジタル証明書をメールに添付して Android デバイスに送り、インポートする方法
- 3) HTTP アクセス可能なサーバーに証明書をアップロードして、インポートする方法

上記いずれかの方法で Android OS の「VPN とアプリ」に CA 証明書とユーザー証明書をインポートします。本手順では証明書のインポート方法については割愛いたします。

6-2 Pulse Secure クライアントの接続設定

Google Play からインストールした Pulse Secure クライアントを起動し、下記設定を行います。

S Pulse Secure	○ パスワード
Pulse Secure Client A	 ファイル上の証明書 KeyStore 内の証明書
ようこそ! ご使用の企業 E メール アドレスまた は会社から提供された URL を 入力し	○ ソフトトークン
てください。 10.10.10.1/vpntest	ок
送信	
	← 証明書を選択 エイリアスを入力して確認するか、KeyStore か
パージョン情報 サポート	ら選択してください 証明書のエイリアス
 ✓ ✓ 接続の追加 	確認または KeyStore から選択
デフォルトの接続に設定します。	キャンセル
接続名 https://10.10.10.1/vpntest 	
https://10.10.10.1/vpntest ユーザ名 オプション/	▼ 証明書を選択
^{認証タイプ} KeyStore 内の証明書	tsoliton E=tsoliton@example.com ,CN=tsoliton,O=Example Co. Ltd,L=SHINJUKU,ST=TOKYO,C=JP
証明書のエイリアス user01 領域	user01 CN=user01,0=Example Corporation,C=JP
オプション	PKCS#12ファイル(拡張子は. pfxまたは. p12)から証明書をインストールできます。
オプション	インストール
キャンセル 追加	 拒否 許可 計 計 計



作成した接続情報を選択し、ユーザーID/パスワードを入力してください。

ホーム 接続 ● https://10.10.10.1/vpntest ttps://10.10.10.1/vpntest 接続				
接続	ホーム			
S Pulse Secure	接続			
Pulse Connect Secure	https://	10.10.10.1/vp .10.1/vpntest	ntest	
user01		切图	断	
	user01			00:59:46
Sign In				
	♠	\$	Ø	≡

改訂履歴

日付	版	改訂内容
2019/03/29	1.0	初版作成