



AAA の RADIUS サーバ

この章では、AAA 用に RADIUS サーバを設定する方法について説明します。

- [AAA 用の RADIUS サーバについて \(1 ページ\)](#)
- [AAA の RADIUS サーバのガイドライン \(21 ページ\)](#)
- [AAA 用の RADIUS サーバの設定 \(21 ページ\)](#)
- [RADIUS サーバの認証および認可のテスト \(28 ページ\)](#)
- [AAA 用の RADIUS サーバのモニタリング \(28 ページ\)](#)
- [AAA 用の RADIUS サーバの履歴 \(29 ページ\)](#)

AAA 用の RADIUS サーバについて

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine (ISE)
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバでの次の認証方式をサポートします。

- PAP : すべての接続タイプの場合。
- CHAP および MS-CHAPv1 : L2TP-over-IPsec 接続の場合。
- MS-CHAPv2 : L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシモード : RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークンサーバ、RSA/SDI から RADIUS の各接続。



(注) MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用するプロトコルとしてイネーブルにするには、トンネルグループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネルグループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザ認証

ASA は、RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウントिंग属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性 (VSA) は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されている RADIUS サーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザ認可に使用可能な、サポートされている RADIUS 属性の一覧を示します。



- (注) RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、アカウント開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

Cisco ACS 5x および Cisco ISE では、バージョン 9.0(1) の RADIUS 認証を使用する IP アドレスの割り当ての IPv6 Framed IP アドレスはサポートされません。

表 1: サポートされる RADIUS 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前 (Business-hours など)
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカルプールの名前
Allow Network Extension Mode	Y	64	ブール	シングル	0 = 無効 1 = 有効
Authenticated User Idle Timeout	Y	50	整数	シングル	1 ~ 35791394 分

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-DN-Field	Y	67	文字列	シングル	有効な値 : UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモートアクセスセッション (IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL) に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモートアクセスセッション (IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL) に対して表示されるバナー文字列。 Banner2 文字列は Banner1 文字列に連結されます (設定されている場合)。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効 1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効 1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
クライアントタイプ	Y	150	整数	シングル	1 = Cisco VPN Client (IKEv1) 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN (IKEv2)
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-Only	Y	122	整数	シングル	0 = 無効 1 = 有効
Group-Policy	Y	25	文字列	シングル	リモートアクセス VPN セッションのグループポリシーを設定します。 バージョン 8.2.x 以降では、IETF-RADIUS-Class の代わりにこの属性を使用します。 次の形式のいずれかを使用できます。 - グループ ポリシー名 - OU=グループ ポリシー名 - OU=グループ ポリシー名;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IE-Proxy-Exception-List		82	文字列	シングル	改行 (\n) 区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-Keep-Alive-Interval	Y	68	整数	シングル	10 ~ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ~ 10 秒
IKE-Keep-Alive	Y	41	ブール	シングル	0 = 無効 1 = 有効
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効 1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効 1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP (認可のみ) 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効 1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバアドレス (スペース区切り)

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Backup-Servers	Y	59	文字列	シングル	1=クライアントが設定したリストを使用する 2=クライアントリストをディセーブルにして消去する 3=バックアップサーバリストを使用する
IPsec-Client-Firewall-Name		57	文字列	シングル	クライアントにファイアウォールポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルトドメイン名を 1 つだけ指定します (1 ~ 255 文字)。
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効 1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効 1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効 1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ~ 49151。デフォルトは 10000 です。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Require-Client-Auth	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There (AYT) で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティアソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します (1 ~ 255 文字)。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効 1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカルプール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
L2TP-Encryption		21	整数	シングル	ビットマップ：1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効 1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： Engineering, Sales ダイナミック アクセス ポリシーで使用する管理属性。グループポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ~ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ~ 1800 秒
PerfctForwardSecurtyEnable	Y	88	ブール	シングル	0 = いいえ 1 = はい

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
PPTP-Encryption		20	整数	シングル	ビットマップ：1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効 1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client-Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems (Cisco Integrated Client を使用) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (Cisco Intrusion Prevention Security Agent を使用)
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Individual-User-Auth	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client (CIC) Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効 1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効 1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 = クライアントレス 2 = クライアント 3 = クライアントのみ Session Subtype が適用されるのは、Session Type (151) 属性の値が 1、2、3、または 4 の場合のみです。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPsec VPN (IKEv2) 3 = クライアントレス SSL VPN 4 = クライアントレス電子メールプロキシ 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマートトンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
Smart-Tunnel-Auto-Signon	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効 1 = 有効
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルトサービスをイネーブルにする 5 = デフォルトクライアントレスをイネーブルにする (2 と 4 は使用しない)
SVC-Ask-Timeout	Y	132	整数	シングル	5 ~ 120 秒

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ~ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ~ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ~ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列 (モジュールの名前)
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ~ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列 (プロファイルの名前)
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ~ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ~ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネルグループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPsec (IKEv1) 8 = L2TP/IPsec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 と 4 は相互排他。0 ~ 11、16 ~ 27、32 ~ 43、48 ~ 59 は有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効 1 = 有効
VLAN	Y	140	整数	シングル	0 ~ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセスリスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効 1 = 有効
WebVPN-Auto-HTTPS	Y	124	文字列	シングル	予約済み
WebVPN-Certificate-File	Y	101	整数	シングル	0 = 無効 1 = 有効
WebVPN-Content-Filter-Params	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL (たとえば http://example.com)
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列 (500 文字以内)
WebVPN-Download-Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効 1 = 有効
WebVPN-File-Save-Dialog-Enable	Y	96	整数	シングル	0 = 無効 1 = 有効
WebVPN-File-Save-Entry-Enable	Y	95	整数	シングル	0 = 無効 1 = 有効
WebVPN-Global-HTTPS-Options	Y	78	文字列	シングル	オプションのワイルドカード (*) を使用したカンマ区切りの DNS/IP (たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com)
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HomePageFilter	Y	228	ブール	シングル	クライアントレスホーム ページをスマートトンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-Policies	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート (例 : http=10.10.10.10:80、https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert	Y	148	整数	シングル	0 ~ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ~ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-Enable	Y	98	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効 1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Post-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。このテキストでクライアントレスポータル ホームページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout	Y	149	整数	シングル	0 ～ 30。0 = デイセーブル。
WebVPN-Smart-Cad-Removal-Discmat	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル自動サインオンリストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SSL-Client-Auth-Req	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマートトンネルネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-Client-Auth-Ent	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-Client-Auth-Key-Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-Client-Auth-Req-Id	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keep-Alive-Freq	Y	107	整数	シングル	15 ~ 600 秒、0=オフ
WebVPN-SVC-Idle-Timeout	Y	108	整数	シングル	5 ~ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Ent	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ~ 1406 バイトです。
WebVPN-SVC-Idle-Timeout	Y	109	整数	シングル	5 ~ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ~ 10080 分、0=オフ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPNSVCKeyMethod	Y	111	整数	シングル	0 (オフ)、1 (SSL)、2 (新しいトンネル)
WebVPNSVCCompression	Y	112	整数	シングル	0 (オフ)、1 (デフォルトの圧縮)
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザ ID
WebVPNUploadMaxSize	Y	158	整数	シングル	0x7fffffff
WebVPNURLEntryEnable	Y	93	整数	シングル	0 = 無効 1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 2: サポートされる IETF RADIUS 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性 (VSA 3076、#25) を使用することをお勧めします。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative : ユーザは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt : ユーザは exec プロンプトへのアクセスを許可されています。 • .remote-access : ユーザはネットワークアクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード

ACCT_DISC_USER_REQ = 1

ACCT_DISC_LOST_CARRIER = 2

ACCT_DISC_LOST_SERVICE = 3

ACCT_DISC_IDLE_TIMEOUT = 4

ACCT_DISC_SESS_TIMEOUT = 5

ACCT_DISC_ADMIN_RESET = 6

切断の理由コード

ACCT_DISC_ADMIN_REBOOT = 7

ACCT_DISC_PORT_ERROR = 8

ACCT_DISC_NAS_ERROR = 9

ACCT_DISC_NAS_REQUEST = 10

ACCT_DISC_NAS_REBOOT = 11

ACCT_DISC_PORT_UNNEEDED = 12

ACCT_DISC_PORT_PREEMPTED = 13

ACCT_DISC_PORT_SUSPENDED = 14

ACCT_DISC_SERV_UNAVAIL = 15

ACCT_DISC_CALLBACK = 16

ACCT_DISC_USER_ERROR = 17

ACCT_DISC_HOST_REQUEST = 18

ACCT_DISC_ADMIN_SHUTDOWN = 19

ACCT_DISC_SA_EXPIRED = 21

ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバのガイドライン

ここでは、AAA 用の RADIUS サーバを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

- シングルモードで最大 100 個のサーバグループ、またはマルチモードでコンテキストごとに 4 つのサーバグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

AAA 用の RADIUS サーバの設定

ここでは、AAA 用に RADIUS サーバを設定する方法について説明します。

手順

ステップ 1 ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2 [RADIUS サーバ グループの設定（22 ページ）](#)。

ステップ 3 [グループへの RADIUS サーバの追加（25 ページ）](#)。

ステップ 4 （任意） [認証プロンプトの追加（27 ページ）](#)。

RADIUS サーバ グループの設定

認証、許可、またはアカウントिंगに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウン リストから RADIUS サーバ タイプを選択します。

ステップ 5 [Accounting Mode] を選択します。

- [Simultaneous]：グループ内のすべてのサーバにアカウントング データを送信します。
- [Single]：1 つのサーバにだけアカウントング データを送信します。

ステップ 6 グループ内で障害の発生したサーバを再度アクティブ化する方法（[Reactivation Mode]）を設定します。

- [Depletion]、[Dead Time]：グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバを再度アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。

- [timed] : 30 秒のダウン時間の後、障害が発生したサーバを再度アクティブ化します。

ステップ 7 [Max Failed Attempts] に、次のサーバを試す前にグループ内の RADIUS サーバに送信する要求の最大数を指定します。

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバが応答しない場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバグループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間続くと（デフォルトの再アクティブ化モードとデッド時間を使用する場合）、ただちにフォールバック方式が使用されます。非応答時間をデフォルト値から変更するには、[Dead Time] の変更方法を参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

ステップ 8 （任意）適切なオプションを選択して、RADIUS 中間アカウント更新メッセージの定期的な生成をイネーブルにします。

これらのオプションが関連するのは、このサーバグループを AnyConnect またはクライアントレス SSL VPN に使用している場合のみです。

- [Enable interim accounting update] : [Update Interval] オプションを選択せずにこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウント更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウント更新アップデートが生成されます。
- [Update Interval] : 対象のサーバグループにアカウント更新レコードを送信するように設定されたすべての VPN セッションのアカウント更新レコードの定期的な生成と伝送をイネーブルにします。これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 です。

(注) ISE サーバが含まれるサーバグループには、両方のオプションを選択します。ISE は、ASA などの NAS デバイスから受信するアカウント更新レコードに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウント更新メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブセッションについて ISE に定期的に中間アカウント更新メッセージを送信するように、グループを設定します。

ステップ 9 （任意）このグループに AD エージェントまたは Cisco Directory Agent (CDA) サーバしか含まれていない場合は、[Enable Active Directory Agent Mode] を選択します。

CDA または AD エージェントはアイデンティティ ファイアウォールで使用されるサーバであり、完全な機能を備えた RADIUS サーバではありません。このオプションを選択すると、このグループをアイデンティティ ファイアウォール専用として使用できます。

ステップ 10 (任意) このサーバグループをリモートアクセス VPN で ISE ポリシーを適用するために使用する場合、次のオプションを設定します。

- [Enable dynamic authorization] : AAA サーバグループの RADIUS の動的認可 (ISE 許可変更、CoA) サービスをイネーブルにします。VPN トンネルでサーバグループを使用すると、対応する RADIUS サーバグループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバグループを ISE と併せてリモートアクセス VPN で使用する場合にのみ動的認可をイネーブルにします。
- [Dynamic Authorization Port] : 動的認可をイネーブルにする場合、RADIUS CoA 要求のリッスンポートを指定できます。デフォルト値は 1700 です。有効な範囲は 1024 ~ 65535 です。
- [Use authorization only mode] : 認証に ISE を使用しない場合は、RADIUS サーバグループに対し認可専用モードをイネーブルにします。これは、サーバグループを認可に使用するとき、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバグループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバグループを使用する可能性があるからです。

ステップ 11 (任意) [VPN3K Compatibility Option] を設定して、RADIUS パケットから受信したダウンロード可能 ACL を Cisco AV ペアの ACL と結合するかどうかを指定します。

このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

- [Do not merge] : ダウンロード可能 ACL は Cisco AV ペアの ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。これがデフォルトのオプションです。
- **Place the downloadable ACL after Cisco AV-pair ACL**
- **Place the downloadable ACL before Cisco AV-pair ACL**

ステップ 12 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバグループが [AAA Server Groups] テーブルに追加されます。

ステップ 13 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

グループへの RADIUS サーバの追加

RADIUS サーバをグループに追加するには、次の手順を実行します。

手順

-
- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバグループをクリックします。
- ステップ 2** [Servers in the Selected Group] 領域（下側のペイン）で、[Add] をクリックします。
サーバグループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ 3** 認証サーバが存在するインターフェイス名を選択します。
- ステップ 4** グループに追加するサーバのサーバ名または IP アドレスを追加します。
- ステップ 5** タイムアウト値を追加するか、デフォルトのままにします。[Timeout] フィールドには、バックアップサーバへ要求を送信する前に、ASA がプライマリサーバからの応答を待機する時間を秒単位で指定します。
- ステップ 6** ダウンロード可能な ACL で受信されたネットマスクを ASA でどのように処理するかを指定します。次のオプションから選択します。
- [Detect automatically] : ASA で、使用されているネットマスク表現のタイプが判定されます。ASA は、ワイルドカードネットマスク表現を検出した場合、標準ネットマスク表現に変換します。

(注) 一部のワイルドカード表現は明確な検出が困難なため、この設定を選択した場合には、ワイルドカードネットマスク表現が誤って標準ネットマスク表現として検出されることもあります。
 - [Standard] : ASA は、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカードネットマスク表現からの変換は実行されません。
 - [Wildcard] : ASA は、RADIUS サーバから受信したダウンロード可能な ACL に、ワイルドカードネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。
- ステップ 7** この ASA を介して RADIUS 認可サーバにアクセスするユーザに共通のパスワードを指定します。このパスワードは大文字と小文字が区別されます。この情報は、RADIUS サーバ管理者に伝えてください。

(注) RADIUS 認証サーバ (認可サーバではない) に対しては、共通のパスワードは設定しないでください。

このフィールドを空白のままにした場合は、RADIUS 認可サーバにアクセスする際のパスワードには、各ユーザ名が使用されます。

RADIUS 認可サーバを認証に使用することは避けてください。共通パスワードやユーザ名を転用したパスワードは、ユーザごとに一意のパスワードに比べ、安全性が低くなります。

このパスワードは、RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。

ステップ 8 二重認証を使用し、トンネルグループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしていない場合、このチェックボックスをオンにすれば、そのサーバから非 MS-CHAPv2 認証要求が送信されるようになります。

ステップ 9 ASA からサーバへ接続を試行した後、次に試行するまでの待機時間を、1 ～ 10 秒の間で指定します。

(注) その後の再試行の間隔は、入力した再試行間隔の設定にかかわらず、常に 50 ミリ秒または 100 ミリ秒です。これは意図された動作です。

ステップ 10 [Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 11 ユーザのアカウンティングに使用するサーバポートを指定します。デフォルトのポートは 1646 です。

ステップ 12 ユーザの認証に使用するサーバポートを指定します。デフォルトのポートは 1645 です。

ステップ 13 ASA で RADIUS サーバを認証する際に使用される共有秘密キーを指定します。設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 14 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバグループに追加されます。

ステップ 15 [AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

RADIUS サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジテキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワードプロンプトの上に表示されます。認証プロンプトを指定しなかった場合は、ユーザが RADIUS サーバで認証中に以下の内容が表示されます。

Connection Type	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

手順

- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。
- ステップ 2** ログイン時にユーザ名とパスワードプロンプトの上に表示するメッセージとして追加するテキストを、[Prompt] フィールドに入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	文字制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

- ステップ 3** [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証の試みが RADIUS サーバによって承認または拒否されたことを示す、異なる状態のプロンプトを表示できます。

これらのメッセージテキストをそれぞれ指定した場合、ASA では、RADIUS サーバにより認証されたユーザに対しては [User accepted message] テキストが表示され、認証されなかったユーザに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザ承認メッセージテキストおよびユーザ拒否メッセージテキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

RADIUS サーバの認証および認可のテスト

ASA が RADIUS サーバに接続してユーザを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択します。

ステップ 2 サーバが [AAA Server Groups] テーブル内に存在するサーバグループをクリックします。

ステップ 3 [Servers in the Selected Group] テーブルでテストするサーバをクリックします。

ステップ 4 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ ([Authentication] または [Authorization]) をクリックします。

ステップ 6 ユーザ名を入力します。

ステップ 7 認証をテストする場合は、ユーザ名に対応するパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテストメッセージが ASA からサーバへ送信されます。テストが失敗した場合は、エラーメッセージが表示されます。

AAA 用の RADIUS サーバのモニタリング

AAA 用の RADIUS サーバのステータスのモニタリングについては、次のコマンドを参照してください。

- [Monitoring] > [Properties] > [AAA Servers]

このペインには、RADIUS サーバの実行コンフィギュレーションが表示されます。

- [Tools] > [Command Line Interface]

このペインでは、さまざまな非インタラクティブコマンドを発行し、結果を表示することができます。

AAA 用の RADIUS サーバの履歴

表 3: AAA 用の RADIUS サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の RADIUS サーバ	7.0(1)	AAA 用の RADIUS サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]
ASA からの RADIUS アクセス要求パケットおよびアカウントिंग要求パケットでの主なベンダー固有属性 (VSA) の送信	8.4(3)	4 つの新しい VSA : Tunnel Group Name (146) および Client Type (150) は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type (151) および Session Subtype (152) は、ASA からの RADIUS アカウントिंग要求パケットで送信されます。4 つのすべての属性が、すべてのアカウントING要求パケットタイプ (開始、中間アップデート、および終了) に送信されます。RADIUS サーバ (ACS や ISE など) は、認可属性やポリシー属性を強制適用したり、アカウントINGや課金のためにそれらの属性を使用したりできます。

