システム プロファイル

AAA

認証、許可、およびアカウンティング（AAA）機能は、Cisco SD ルーティングデバイスにログインしているユーザーの認証、ユーザーに与える権限の決定、およびアクションのアカウンティングの実行をサポートします。

次の表では、AAA 機能を設定するためのオプションについて説明します。

Local

フィールド	説明
Add AAA User	
Name	ユーザの名前を入力します。ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。 次のユーザー名は予約されているため、設定できません。backup、basic、bin、daemon、games、gnats、irc、list、lp、mail、man、news、nobody、proxy、quagga、root、sshd、sync、sys、uucp、および www-data。また、viptela-reserved で始まる名前は予約されています。

フィールド	説明
Password	ユーザーのパスワードを入力します。パスワードは MD5 ダイジェスト文字列で、タブ、復帰、改行などの任意の文字を含めることができます。詳細については、RFC 7950「The YANG 1.1 Data Modeling Language」のセクション 9.4 を参照してください。 各ユーザー名にはパスワードが必要です。ユーザーは自分のパスワードを変更できます。 管理ユーザーのデフォルトパスワードは admin です。このパスワードから変更することを強く推奨します。
Confirm Password	ユーザーのパスワードをもう一度入力します。
Privilege	特権レベル 1 または 15 から選択します。 • [Level 1]：ユーザー EXEC モード。読み取り専用です。アクセスできるコマンドは ping などに限定されています。 • [Level 15]：特権 EXEC モード。reload コマンドなど、すべてのコマンドにアクセスできます。また設定の変更も可能です。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです。
公開キーチェーンの追加	
SSH RSA Key	[ssh-rsa] を選択します。

RADIUS

フィールド	説明
Add Radius Server	
IP Address (v4 or v6)	RADIUS サーバーホストの IP アドレスを入力します。
Acct Port	802.1X および 802.11i アカウンティング情報を RADIUS サーバーに送信するために使用する UDP ポートを入力します。 範囲：0 ～ 65535。 デフォルト：1813
Auth Port	RADIUS サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：1812

フィールド	説明
Retransmit	デバイスが RADIUS 要求をサーバーに再送信する回数を入力します。 デフォルト：3 秒
Timeout	要求を再送信する前に、デバイスが RADIUS 要求への応答を待機する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key*	認証と暗号化のために、Cisco SD ルーティングデバイスから RADIUS サーバーに渡されるキーを入力します。
Key Type	[Protected Access Credential (PAC)] またはキータイプを選択します。

TACACS サーバー

フィールド	説明
Add TACACS Server	
IP Address (v4 or v6)	TACACS+ サーバーホストの IP アドレスを入力します。
Authentication Port	TACACS+ サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：49
Timeout [second]	デバイスが TACACS+ 要求への応答を待機してから、要求を再送信する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key	認証と暗号化のために、Cisco SD ルーティングデバイスから TACACS+ サーバーに渡されるキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、TACACS+ サーバーで使用する AES 暗号化キーと一致させる必要があります。

アカウンティング

フィールド	説明
アカウンティングルールの追加	
Rule Id	アカウンティングルール ID を入力します。

フィールド	説明
Method	アカウンティング方式リストを指定します。次のいずれかを選択します。 • [commands]：特定の特権レベルに関連付けられた特定の個々の EXEC コマンドに関するアカウンティング情報を提供します。 • [exec]：ネットワーク アクセス サーバーでユーザー名、日付、開始および終了時間などのユーザー EXEC ターミナルセッションに関するアカウンティングレコードを提供します。 • [network]：ネットワークに関連するあらゆるサービス要求にアカウンティングを実行します。 • [system]：ユーザーに関連付けられていないすべてのシステムレベルのイベント（リロードなど）に対してアカウンティングを実行します。 （注） システムアカウンティングを使用しており、システムのスタートアップ時にアカウンティング サーバが到達不能である場合、システムに約 2 分間アクセスできません。
Start Stop	イベントの開始時にアカウンティング開始通知を送信し、イベントの終了時にレコード停止通知を送信する場合は、このオプションを有効にします。
Groups	以前に設定した TACACS グループを選択します。このアカウンティングルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

許可

フィールド	説明
Console	コンソールアクセスコマンドの認証を実行するには、このオプションを有効にします。
Config Commands	コンフィギュレーション コマンドの認証を実行するには、このオプションを有効にします。
認証ルールの追加	
Rule Id	認証ルール ID を入力します。
Method	[Commands] を選択します。これにより、ユーザーが入力するコマンドが許可されます。
Level	許可するコマンドの権限レベル（1 または 15）を選択します。この権限レベルを持つユーザーが入力したコマンドが許可されます。

フィールド	説明
Authenticated	認証されたユーザーにのみ認証ルールパラメータを適用するには、このオプションを有効にします。このオプションを有効にしない場合、ルールはすべてのユーザーに適用されます。
Group(s)	以前に設定したTACACSグループを選択します。この認証ルールが定義するパラメータは、このグループに関連付けられているTACACSサーバーによって使用されます。

802.1X

フィールド	説明
Authentication Param	認証パラメータを有効にします。
Accounting Param	アカウンティングパラメータを有効にします。

認証と承認の順序

フィールド	説明
Server Auth Order	[local] を選択します。

バナー

バナー機能は、システムログインバナーの設定に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、次のいずれかを選択します。

次の表では、バナー機能を設定するためのオプションについて説明します。

フィールド	説明
Name	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Login	ログインプロンプトの前に表示するテキストを入力します。ストリングの長さは、最大 2048 文字まで可能です。改行を挿入するには、\n と入力します。

フィールド	説明
Message of the Day	ログインバナーの前に表示する今日のメッセージのテキストを入力します。ストリングの長さは、最大 2048 文字まで可能です。改行を挿入するには、\n と入力します。

グローバル

グローバル機能は、HTTP、HTTPS、Telnet、IP ドメインルックアップ、およびその他のいくつかのデバイス設定など、デバイス上のさまざまなサービスを有効または無効にするのに役立ちます。

次の表では、グローバル機能を構成するためのオプションについて説明します。

サービス

フィールド	説明
HTTP Server	HTTP サーバーを有効または無効にします。
HTTPS Server	セキュア HTTPS サーバーを有効または無効にします。
FTP Passive	パッシブ FTP を有効または無効にします。
Domain Lookup	ドメインネームシステム（DNS）ルックアップを有効または無効にします。
ARP Proxy	プロキシ ARP を有効または無効にします。
RSH/RCP	デバイスでリモートシェル（RSH）とリモートコピー（rcp）を有効または無効にします。
Line Virtual Teletype (Configure Outbound Telnet)	アウトバウンド Telnet を有効または無効にします。
Cisco Discovery Protocol（CDP）	Cisco Discovery Protocol（CDP）を有効または無効にします。
Link Layer Discovery Protocol (LLDP)	リンク層検出プロトコル（LLDP）を有効または無効にします。
HTTP Client Source Interface	すべての HTTPS クライアント接続に送信元インターフェイスのアドレスを入力します。

NAT

フィールド	説明
NAT 64 UDP Timeout	UDP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：300 秒（5 分）
NAT 64 TCP Timeout	TCP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：3600 秒（1 時間）
NAT TCP Timeout	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：3600 秒（1 時間）
NAT 64 UDP Timeout	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：300 秒（5 分）

認証

フィールド	説明
HTTP Authentication	HTTP認証モードを選択します。 許容値：Local、AAA デフォルト：Local

SSH Version

フィールド	説明
SSH Version	SSHバージョンを選択します。 デフォルト：無効

Other Settings

フィールド	説明
TCP Keepalives (In)	着信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Keepalives (Out)	発信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Small Servers	小規模な TCP サーバー（ECHO など）を有効または無効にします。
UDP Small Servers	小規模な UDP サーバー（ECHO など）を有効または無効にします。
Console Logging	コンソールロギングを有効または無効にします。デフォルトでは、ルータはすべてのログメッセージをコンソールポートに送信します。
IP Source Routing	IP ソースルーティングを有効または無効にします。IP ソースルーティングは、パケットの発信元が、パケットが宛先に到達するために使用するパスを指定できるようにする機能です。
VTY Line Logging	デバイスがログメッセージをリアルタイムで vty セッションに表示することを有効または無効にします。
SNMP IFINDEX Persist	デバイスの再起動時に保持および使用されるインターフェイス インデックス（ifIndex）値を提供する SNMP IINDEX パーシステンスを有効または無効にします。
Ignore BOOTP	BOOTP サーバーを有効または無効にします。有効にすると、デバイスは 0.0.0.0 から送信される BOOTP パケットをリッスンします。無効にすると、デバイスはこれらのパケットを無視します。

ロギング

ロギング機能は、ローカルハードドライブまたはリモートホストへのロギングを構成するのに役立ちます。

次の表では、ロギング機能を設定するためのオプションについて説明します。

フィールド	説明
Max File Size(In Megabytes)	syslog ファイルの最大サイズを入力します。syslog ファイルは、ファイルサイズに基づいて 1 時間ごとにローテーションされます。ファイルサイズが設定値を超えると、ファイルがローテーションされ、syslog プロセスに通知されます。 範囲：1 ～ 20 MB デフォルト：10 MB

フィールド	説明
Rotations	最も古いファイルを破棄するまでに作成できる syslog ファイルの数を入力します。 範囲：1 ～ 10 デフォルト：10

TLS プロファイル

フィールド	説明
Add TLS Profile	
TLS Profile Name	TLS プロファイル名を入力します。
TLS Version	TLS バージョンを選択します。 • TLSv1.1 • TLSv1.2
Authentication Type*	サーバーを選択します。

フィールド	説明
Cipher Suite List	TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。 暗号スイートのリストを以下に示します。 • [aes-128-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_128_sha • [aes-256-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_256_sha • [dhe-aes-cbc-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [dhe-aes-gcm-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2（TLS1.2 以上） • [ecdhe-ecdsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2（TLS1.2 以上）SuiteB • [ecdhe-rsa-aes-cbc-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2（TLS1.2 以上） • [ecdhe-rsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2（TLS1.2 以上） • [rsa-aes-cbc-sha2]：暗号化タイプ tls_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [rsa-aes-gcm-sha2]：暗号化タイプ tls_rsa_with_aes_gcm_sha2（TLS1.2 以上）

サーバ

フィールド	説明
サーバの追加	
IPv4 Address	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog サーバーを削除するには、エントリの右側にあるごみ箱のアイコンをクリックします。
VRF	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530

フィールド	説明
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
Severity	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重大度を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable	このオプションを有効にすると、TLS を介した syslog が許可されます。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Custom Profile]：TLS プロファイルを選択するには、このオプションを有効にします。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Profile]：IPv4 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。
IPv6 サーバーの追加	
IPv6 Address*	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog サーバーを削除するには、エントリの右側にあるごみ箱のアイコンをクリックします。

フィールド	説明
VRF	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
Priority	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重大度を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable	このオプションを有効にすると、TLS を介した syslog が許可されます。
TLS Properties Custom Profile*	TLS プロファイルを選択するには、このオプションを有効にします。
TLS Properties Profile	IPv6 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。

NTP

Network Time Protocol（NTP）は、サーバーとクライアントの分散ネットワークがネットワーク全体で時刻を同期できるようにするプロトコルです。NTP 機能は、Cisco SD-WAN ネットワークで NTP 設定を行うのに役立ちます。

次の表では、NTP 機能を設定するためのオプションについて説明します。

サーバ

フィールド	説明
サーバの追加	
Hostname/IP address	NTP サーバーの IP アドレスか、NTP サーバーへの到達方法を認識している DNS サーバーの IP アドレスを入力します。
VRF to reach NTP Server*	NTP サーバーに到達するために使用する VRF 名を入力します。32 文字以内の英数字で指定します
Set authentication key for the server	MD5 認証を有効にするために、NTP サーバーに関連付けられた MD5 キーを指定します。 キーを有効にするには、[Authentication] の [Trusted Key] フィールドでキーを「trusted」とマークする必要があります。
Set NTP version	NTP プロトコルソフトウェアのバージョン番号を入力します。 範囲：1 ～ 4 デフォルト：4
Set interface to use to reach NTP server	NTP パケットの発信に使用する特定のインターフェイスの名前を入力します。このインターフェイスは、NTP サーバーと同じ VPN 内にある必要があります。そうでない場合、設定は無視されます。
Prefer this NTP server*	複数の NTP サーバーが同じストラタムレベルにあり、そのうちの 1 つを優先する場合は、このオプションを有効にします。別のストラタムレベルのサーバーについては、Cisco SD ルーティングは最上位のストラタムレベルのサーバーを選択します。

認証

フィールド	説明
認証キーの追加	
Key Id	MD5 認証キー ID を入力します。 範囲：1 ～ 65535
MD5 Value*	MD5 認証キーを入力します。クリアテキストキーまたは AES 暗号化キーを入力します。

Advanced

フィールド	説明
Authoritative NTP Server	サポートされている 1 つまたは複数のルータをプライマリ NTP ルータとして設定する場合は、ドロップダウンリストから [Global] を選択し、このオプションを有効にします。 このオプションを有効にすると、次のフィールドが表示されます。 **Stratum**：プライマリ NTP ルータのストラタム値を入力します。ストラタム値は、基準クロックからのルータの階層的距離を定義します。 有効な範囲：1 ～ 15 の整数。値を入力しない場合、システムはルータの内部クロックのデフォルトストラタム値である 8 を使用します。
Source	NTP 通信の出口インターフェイスの名前を入力します。設定されている場合、システムは NTP トラフィックをこのインターフェイスに送信します。 たとえば、**GigabitEthernet1** または **Loopback0** と入力します。

SNMP

アプリケーション層の簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の対話用の通信標準規格を提供します。このプロトコルは、ネットワークデバイスのモニタリングや管理に共通して使用される標準化された言語を定義します。SNMP 機能は、Cisco SD ルーティングデバイスで SNMP 機能を設定するのに役立ちます。

次の表では、SNMP 機能を設定するためのオプションについて説明します。

SNMP

表 *1 : Advanced*

フィールド	説明
Shutdown	デフォルトでは、SNMP は有効になっています。
Contact Person	Cisco SD ルーティングデバイスの管理を担当するネットワーク管理担当者の名前を入力します。これには、最大 255 文字を使用できます。
Location of Device	デバイスのロケーションの説明を入力します。これには、最大 255 文字を使用できます。

SNMP Version

表 *2 :* 基本 *(Basic)*

フィールド	説明
SNMP バージョン（SNMP Version）	次の SNMP バージョンのいずれかを選択します。 • SNMP v2 • **SNMP v3**
SNMP v2：ビューの追加	
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco SD ルーティングデバイス MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にして OID をビューから除外します。

フレキシブルポート速度

フレキシブルポート速度機能は、Cisco Catalyst 8500-12X4QC ルータにのみ適用されます。この機能を使用して、要件に基づいて 100GE、40GE、10GE、または 1GE として動作するようにインターフェイスを設定します。ポートタイプに対して行った変更は、設定グループをデバイスに適用した後にのみ有効になります。

フレキシブルポート速度機能を使用してポート設定を更新すると、一部のポートが有効になり、他のポートが無効になる場合があります。たとえば、デフォルトでは C8500-12X4QC はベイ 1 を 10GE モードで、ベイ 2 を 40GE モードで動作させます。ベイ 1 のモードは、10GE、40GE、または 100GE にできます。ベイ 1 を 100GE に設定すると、ベイ 0 のすべてのポートが無効になります。詳細については、Cisco Catalyst 8500-12X4QC デバイスガイドの「Bay Configuration」[英語] を参照してください。

Cisco Catalyst 8500-12X4QC プラットフォームの各ベイのポートオプションの詳細については、『*Cisco Catalyst 8500 Series Edge Platforms Data Sheet*』の C8500-12X4QC 製品概要を参照してください。

一部のパラメータには範囲のドロップダウンリストがあり、パラメータ値として [Global]、[Device Specific]、または [Default] を選択できます。以下に示す表の説明に従って、次のオプションのいずれかを選択します。

パラメータの範囲	範囲の説明
グローバル（地球のアイコン）	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。
デバイス固有（ホストのアイコン）	デバイス固有の値がパラメータに使用されます。 [Device Specific] を選択すると、フィールドにキーの値を入力できます。キーは、パラメータの識別に役立つ一意の文字列です。デフォルトのキー値を変更するには、フィールドに新しい文字列を入力します。 デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。
デフォルト（チェックマークで示されます）	デフォルト設定を持つパラメータには、デフォルト値が表示されます。

基本設定

パラメータ名	説明
Port Type	次のポートの組み合わせのいずれかを選択します。 • 12 ports of 1/10GE + 3 ports of 40GE • 8 ports of 1/10GE + 4 ports of 40GE • 2 ports of 100GE • 12 ports of 1/10GE + 1 port of 100GE • 8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE • 3 ports of 40GE + 1 port of 100GE デフォルトは、[12 ports of 1/10GE + 3 ports of 40GE] です。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。