管理設定

管理

[管理] ページから、ATA Web ページへの Web アクセスを管理し、リモート構成とネットワーク管理のためのプロトコルを有効にします。

ウェブ アクセス管理

管理 > **管理にある** > **Web アクセス管理**ページから、ATA の管理へのアクセスの設定を構成します。

Cisco ATA 192 Web アクセス管理フィールド

Cisco ATA 192 Web ページへのアクセスは、デフォルトで有効になっています。管理者アクセスを使用すると、オフィスネットワーク内のコンピューターから設定を管理できます。Web アクセスを使用すると、別のサブネットまたはインターネット上のコンピューターから接続することができます。

ATA Web ページにアクセスするには、Web ブラウザを起動して、アドレスバーに URL を入力します。URL には、指定されたプロトコル、ATA の WAN IP アドレス、および指定されているポート番号が含まれている必要があります。たとえば、HTTPS プロトコル、WAN IP アドレスの 203.0.113.50、ポート 80 では、次のように入力します。https://203.0.113.50:80

表 *1 : Cisco ATA 192 Web* アクセス管理の設定

フィールド	説明
管理者アクセス	この機能は、イーサネット (LAN) ポート経由で接続されているデバイスからの ATA Web ページへのアクセスを制御します。 **有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。 デフォルトの設定はイネーブルです。LAN に接続されているコンピュータから ATA を管理および設定する場合は、この機能を有効にする必要があります。
Web ユーティリティへのアクセス	WAN のデバイスからの ATA Web ページへのアクセスに使用するプロトコルを選択します。**HTTP** または **HTTPS** を選択します。セキュアなインターネットアクセスの場合は、HTTPS を選択します。デフォルト値は HTTP です。
リモート管理ポート	WAN 上のデバイスから ATA Web ページにアクセスするために使用するポート番号を入力します。デフォルトのポート番号は 80 です。

Cisco ATA 191 Web アクセスフィールド

表 *2 : Cisco ATA 191 Web* アクセスの設定

フィールド	説明
管理者アクセス	この機能は、イーサネット (LAN) ポート経由で接続されているデバイスからの ATA Web ページへのアクセスを制御します。 **有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。 デフォルトの設定はイネーブルです。LAN に接続されているコンピュータから ATA を管理および設定する場合は、この機能を有効にする必要があります。
Web ユーティリティへのアクセス	WAN のデバイスからの ATA Web ページへのアクセスに使用するプロトコルを選択します。**HTTP**、**HTTPS**、または両方のエントリを選択します。セキュアなインターネットアクセスの場合は、HTTPS を選択します。デフォルト値は HTTP です。

Remote Access フィールド

表 *3 : Remote Access* 設定

フィールド	説明
Remote Management	ATA の WAN 側にあるデバイスから ATA web ページにアクセスできるようにします。たとえば、オフィスまたは自宅のコンピュータから別のサブネットに接続することができます。 **有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。 デフォルト設定では [Disabled] になっています。ページのこのセクションの他のフィールドは、この機能を有効にした場合にのみ使用できます。デフォルトの管理者ログイン資格情報を使用してこの機能を有効にしようとすると、資格情報を変更するように求められます。**OK**をクリックして、警告メッセージを承認します。**管理** > **管理にある** > **ユーザーー覧**ページから、パスワードを変更します。詳細については、ユーザリスト (パスワード管理) （7 ページ）を参照してください。
Web ユーティリティへのアクセス	ATA の WAN 側のデバイスからの ATA web ページへのアクセスに使用するプロトコルを選択します。**HTTP** または**HTTPS** を選択します。 セキュアなインターネットアクセスの場合は、**HTTPS** を選択します。デフォルト値は **HTTP** です。 Web ブラウザにアドレスを入力するときは、指定されたプロトコルを含めるようにします。たとえば、HTTPS プロトコル、203.0.113.50 の WAN IP アドレス、デフォルトのリモート管理ポート 80 の場合は、次のように入力します。 **`https://203.0.113.50:80`**
リモート アップグレード	リモート管理を有効にした場合は、ATA の WAN 側のデバイスからのファームウェアアップグレードを許可するかどうかを選択します。**有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。デフォルト値は [Disabled] です。 この設定は、コンピュータが LAN から設定ユーティリティに接続されている場合にのみ変更できます。

フィールド	説明
許可されているリモート IP アドレス	この機能を使用して、デバイスの IP アドレスに基づいて ATA Web ページへのアクセスを制限することができます。任意の外部 IP アドレスからのアクセスを許可するために、**任意の IP アドレス**を選択します。外部 IP アドレスまたは IP アドレスの範囲を指定するには、2 番目のラジオボタンを選択し、目的の IP アドレスまたは範囲を入力します。デフォルト設定は任意の IP アドレスです。
リモート管理ポート	ATA の WAN 側のデバイスから ATA web ページにアクセスするために使用するポート番号を入力します。デフォルトのポート番号は 80 です。 Web ブラウザにアドレスを入力するときは、指定されたポートを含めるようにします。たとえば、HTTPS プロトコル、203.0.113.50 の WAN IP アドレス、デフォルトのリモート管理ポート 80 の場合は、次のように入力します。 https://203.0.113.50:80

TR-069

管理 > **管理 にある** > **TR-069**ページから、TR-069 CPE WAN Management Protocol (CWMP) を介して自動設定サーバ (ACS) との通信を設定します。TR-069 (Technical Report 069) は、大規模な展開においてすべての音声デバイスおよびその他の顧客宅内機器（CPE）を管理するための共通プラットフォームを提供します。CPE と ACS の間の通信を提供します。

以下の説明のとおり設定を入力します。変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

表 *4 : TR-069* の設定

フィールド	説明
ステータス	リモートプロビジョニングを有効にするには**有効**をクリックするか、またはこの機能を無効にするには**無効**をクリックします。デフォルト設定では [Disabled] になっています。
[ACS URL]	ACS の URL。形式は https://xxx.xxx.xxx.xxx:port または xxx.xxx.xxx.xxx ort:p にする必要があります。xxx.xxx.xxx.xxx は、ACS サーバのドメイン名または IP アドレスです。 IP アドレスとポート番号の両方を入力する必要があります。
[ACSユーザ名（ACS Username）]	ACS のユーザ名。デフォルトのユーザ名は、組織単位識別子 (OUI) です。この値は必須であり、ACS に設定されているユーザ名と一致する必要があります。

フィールド	説明
[ACSパスワード（ACS Password）]	ACS のパスワード。この値は必須であり、ACS に設定されているパスワードと一致している必要があります。
接続 リクエスト ポート	接続リクエストに使用するポート
[接続要求ユーザ名（Connection Request Username）]	接続リクエストのユーザ名。この値は、ACS に設定されている接続リクエストのユーザ名と一致する必要があります。
[接続要求パスワード（Connection Request Password）]	接続リクエストのパスワード。この値は、ACS に設定されている接続リクエストパスワードと一致する必要があります。
[定期通知インターバル（Periodic Informal Interval）]	[定期通知有効] が有効の場合、CPE が ACS との接続を試行する間隔を秒数で入力します。デフォルト値は 86,400 秒です。
[定期通知有効（Periodic Inform Enable）]	**有効** をクリックして ACS への接続リクエストを有効化するか、**無効**をクリックしてこの機能を無効にします。
ダウンロードのお申し込み	この設定が適用されている場合、ACS は、ATA からリクエストを受信した後で、ダウンロード RPC を呼び出すことができます。

SNMP

管理>**管理**>**にある SNMP** ページから、シンプルネットワーク管理プロトコル (SNMP) を ATA に設定します。

SNMP は、ネットワーク管理者がネットワーク上で発生する重要なイベントの管理、モニタ、および通知の受信を可能にするネットワークプロトコルです。ATA は SNMPv2 および SNMPv3 をサポートしています。

SNMP エージェントとして動作し、SNMP ネットワーク管理システムから SNMP コマンドに応答します。標準 SNMP の [取得]、[次へ]、および [セット] コマンドをサポートしています。また、設定されたアラーム状態が発生したときに SNMP マネージャに通知するための SNMP トラップを生成します。たとえば、リブート、電力サイクル、インターネット (WAN) イベントなどがあります。

以下の説明のとおり設定を入力します。変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

SNMP 設定

表 *5 : SNMP Parameters*

フィールド	説明
[有効（Enabled）]、[無効（Disabled）]	**有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。デフォルト設定では [Disabled] になっています。
信頼された IPv4	任意の IPv4 アドレスからのアクセスを許可する場合は**任意**を選択します (推奨されません)。 **アドレス**をクリックして 、SNMP から ATA にアクセスできる単一の SNMP マネージャーまたはトラップエージェントの IPv4 アドレスとサブネットマスクを指定します。
信頼された IPv6	任意の IPv6 アドレスからのアクセスを許可する場合は**任意**を選択します (推奨されません)。 **アドレス**をクリックして 、SNMP から ATA にアクセスできる単一の SNMP マネージャーまたはトラップエージェントの IPv6 アドレスとプレフィックス長を指定します。
ゲット/トラップ コミュニティ	SNMP GET コマンドの認証に使用するコミュニティ文字列を入力します。デフォルト値は public です。
Set Community	SNMP SET コマンドの認証に使用するコミュニティ文字列を入力します。デフォルト値は [プレイベート] です。

SNMPv3 設定

表 *6 : SNMPv3* パラメータ

フィールド	説明
[有効（Enabled）]、[無効（Disabled）]	**有効**をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。デフォルト設定では [Disabled] になっています。
読み取り/書き込みユーザ	SNMPv3 認証用のユーザ名を入力します。デフォルト値は v3rwuser です。
Auth-Protocol	ドロップダウンリストから SNMPv3 認証プロトコル (**HMAC-MD5**または **HMAC-SHA**) を選択します。
Auth-Password	認証パスワードを入力します。

フィールド	説明
PrivProtocol	ドロップダウンリストからプライバシー認証プロトコルを選択します（**なし**または**CBC-DES**）。CBCDESを選択すると、送信されるメッセージのデータ部分がprivKeyによって暗号化されます。
プライバシー パスワード（Privacy Password）	使用する認証プロトコルのキーを入力します。

トラップの設定

表 *7:* トラップ パラメータ

フィールド	説明
[IPアドレス(IP Address)]	SNMP マネージャまたはトラップエージェントの IP アドレス。
ポート（Port）	トラップメッセージを受信するために、SNMP マネージャまたはトラップエージェントが使用するSNMPトラップポート。有効なエントリは、162 または 1025 ~ 65535 です。デフォルト値は 162 です。
SNMPバージョン	SNMP マネージャまたはトラップエージェントによって使用されている SNMP のバージョン。リストからバージョンを選択します。

ユーザリスト(パスワード管理)

ATA web ページの 2 つのユーザアカウントを管理するには、**管理** > **管理にある** > **ユーザリスト**ページから行います。ユーザレベルのアカウントは、限定された機能のセットを変更するアクセス権を持っています。

IVR の場合は、[システム] ページでこれらのパスワードを設定することができます。

パスワードの更新

手順

ステップ 1 ユーザリストテーブルで、更新するアカウントの鉛筆アイコンをクリックします。

ステップ 2 [ユーザアカウント] ページで、以下の説明に従ってユーザ名とパスワードを入力します。

- ユーザ名：ユーザ名を入力します。
- 古いパスワード (管理者アカウントのみ): 既存のパスワードを入力します。

- 新しいパスワード: 32 文字以内で新しいパスワードを入力します。
- パスワードの確認: 確認のため、パスワードを再度入力します。

ステップ 3 変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

Bonjour

管理 > **管理にある** > **Bonjour** ページから、Bonjour を 有効または無効にします。Bonjour は、LAN 上のコンピューターやサーバなどのネットワークデバイスを検出するサービス検出プロトコルです。これは、使用しているネットワーク管理システムで必要になる場合があります。この機能が有効になっている場合、ATA は、Bonjour のサービスレコードを定期的にローカルネットワーク全体にマルチキャストして、その存在を通知します。

有効をクリックしてこの機能を有効にするか、**無効**をクリックして無効化します。デフォルトの設定はイネーブルです。

変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

リセット ボタン

有効をクリックして リセットボタンを有効にするか、**無効**をクリックして無効化します。デフォルトの設定はイネーブルです。

変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

SSH

管理 > **管理** > **にある SSH** から、SSH 関連の設定を行います。

表 *8 : SSH* 設定

フィールド	説明
User Name	SSH のログインユーザ名を設定
パスワード	SSH のログイン パスワードを設定します。
SSH アクセス（SSH Access）	SSHアクセスを有効または無効に設定します。

対数

ATA では、ネットワーク上で発生するさまざまなイベントに対して、着信、送信、および DHCPの各リストを記録できます。着信ログには、受信したインターネットトラフィックの発信元IPアドレスと宛先ポート番号の一時リストが表示されます。発信ログには、発信インターネットトラフィックのローカルIPアドレス、宛先URL/IPアドレス、およびサービスとポートの番号の一時リストが表示されます。

デバッグ ログ モジュール

管理 > **ログモジュールにある** > **デバッグ ログ モジュール**ページから、ログを有効にし、設定を構成します。

- ベストプラクティスとして、必要な場合にのみロギングを有効にして、調査が終了したときにログを無効にすることを推奨します。ロギングはリソースを消費し、システムのパフォーマンスに影響を与える可能性があります。
- このページでは、デバッグメッセージをすべての重要度レベルで表示するモジュールを選択できます。

デバッグ ログ設定

管理>**ログにある**>**デバッグ ログ サーバ**ページでデバッグログサーバを有効にした場合、ATA はデバッグメッセージを 1 台のサーバに送信します。

以下の説明のとおり設定を入力します。変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

表 *9*: デバッグ ログ設定

フィールド	説明
デバッグ ログ サイズ	ログファイルの最大サイズ（KB）を入力します。128～1024 の範囲の値を指定できます。
IPv4 アドレス	メッセージを送信するデバッグ ログ サーバの IPv4 アドレスを入力します。
IPv6 アドレス	メッセージを送信するデバッグ ログ サーバの IPv6 アドレスを入力します。
ポート（Port）	サーバで使用するポートを入力します。有効値は 1 ～ 65535 です。

デバッグログビューアー

管理 > **ログにある** > **デバッグログビューアー**ページでロギングが有効になっている場合は、[ログビューア] ページからログをオンラインで表示し、システムログファイルをコンピューターにダウンロードすることができます。ログの内容を制限するには、含めるエントリの種類を選択するか、キーワードを指定します。

ロギングのイネーブル化と設定の注意事項については、デバッグ ログ モジュール （9 ページ）を参照してください。

表 *10*: デバッグ ログ設定

フィールド	説明
ログをダウンロード	このボタンをクリックすると、コンピューターにログの内容がファイルとしてダウンロードされます。ダイアログボックスでは、ファイルを開いたり保存したりできます。メモ帳などのテキスト エディタでファイルを開くことができます。
ログの消去	ログからすべてのエントリを削除するには、このボタンをクリックします。
[フィルタ（Filter）]	キーワードを入力すると、ビューアーに表示されるログエントリを絞り込むことができます。ページには、キーワードを含むエントリだけが表示されます。

イベントログの設定

管理 > **ログ** > **にあるイベントログ設定**ページから、必要なイベントログを収集します。イベントログメッセージは、UDP トランスポートタイプを使用して、SYSLOG プロトコルを介して送信されます。

トラブルシューティングの際には、イベントログ設定を使用します。次の4つのイベントカテゴリが定義されています。

- DEV: デバイス情報。デバイスの起動とネットワーク接続が準備されると、メッセージが送信されます。
- SYS: システム関連の情報。デバイスの起動とネットワーク接続が準備されている間に 1 回メッセージが送信されます。
- CFG: プロビジョニングのステータスと設定ファイルの変更。設定またはネットワークステータスの変更によってプロビジョニングサービスが再起動するたびにメッセージが送信されます。
- REG: 各回線の登録ステータス。登録ステータスが変化するたびにメッセージが送信されます。

以下の説明のとおり設定を入力します。変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

表 *11* : イベントログ設定

フィールド	説明
アドレス（Address）	イベントログサーバのアドレスを設定します。
ポート（Port）	イベントログサーバポートを設定します。 Default value: 514
フラグ	イベントログフラグを設定すると、ビット単位の値になります。設定リストは次のとおりです。 • `<Dev>:1(0x01)` • `<SYS>:2(0x01<<1)` • `<CFG>:4(0x01<<2)` • `<REG>:8(0x01<<3)` デフォルト値:15 (すべてのイベント)

PRT ビューアー

管理 > **ログにある** > **PRT ビューアー**を使用して、問題レポートツール (PRT) ファイルを生成し、ダウンロードすることができます。

変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

表 *12* : 問題レポート ツール設定

フィールド	説明
PRTアップロード URL	PRT ログのアップロード URT を設定します。
[PRTアップロード方法（PRT Upload Method）]	PRT ログのアップロード方法、**POST** または **PUT** を設定します。
[PRT最大タイマー（PRT Max Timer）]	PRT 最大タイマーを設定します。有効範囲は 15 - 1440 分です。 無効化済み: 0
問題レポート ツールログ	ユーザによって ATA 上に生成された PRT ファイルを一覧表示します。

フィールド	説明
PRT の生成	このボタンをクリックすると、コンピューター上のファイルとして PRT のコンテンツが生成され、ダウンロードされます。ダイアログボックスでは、ファイルを開いたり保存したりできます。

PCM ビューアー

管理 > **ログにある** > **PCM ビューア–**から、ダウンロードして PCM を表示します。

ATA を使用すると、PCM ログファイルをキャプチャして、コールを開始するためのユーザオフフックを作成できます。

変更を行った後で、**送信**をクリックして設定を保存するか、**キャンセル**をクリックして、設定を保存したページを再表示します。

表 *13 :* ログビューア設定

フィールド	説明
PCM キャプチャの有効化	キャプチャ PCM を有効または無効にします。
期間	PCM キャプチャの継続時間を秒単位で入力します。有効な範囲は、20 ～ 300 秒です。
PCM ファイルリスト	ユーザがキャプチャする PCM ファイルを一覧表示します。

CSS ダンプ

管理 > **ログにある** > **CSS ダンプ**ページから、CSS ダンプファイルを設定し、ダウンロードします。

表 *14 : CSS* ダンプの設定

フィールド	説明
CSS メモリ ダンプ	CSS メモリダンプ機能を **有効**または**無効**に設定します。 デフォルト値：Disabled
CSS メモリダンプファイル	ATA 上の CSS メモリダンプファイルストアを表示します。ダウンロードするファイルの名前をクリックします。
更新	**更新**をクリックして CSS メモリダンプファイルを更新します。

工場出荷時の初期状態

管理 > **工場出荷時のデフォルト** ATA Web ページから、ATA をデフォルト設定にリセットします。

または、**リセット**ボタンを20秒間押し続けます。ユーザが変更可能なデフォルト以外の設定は失われます。これには、ネットワークおよびサービスプロバイダーのデータが含まれる場合があります。

次の作業を実行できます。

- ルータの初期設定を復元: **はい**を選択して、設定したカスタムデータ (ルータ) 設定を削除します。**送信**をクリックすると、デフォルト設定が復元されます。
- 音声の初期設定を復元: **はい**を選択して、ATA Web ページの音声ページ上で設定したカスタム設定を削除します。**送信**をクリックすると、デフォルト設定が復元されます。

ファームウェア アップグレード

管理 > **ファームウェアアップグレード**ページから、ATA のファームウェアをアップグレードします。ATA の問題が発生している場合や、新しいファームウェアに使用する機能がある場合以外は、アップグレードする必要はありません。

⚠

注意 ファームウェアのアップグレードには数分かかる場合があります。プロセスが完了するまでは、電源をオフにしたり、ハードウェアリセットボタンを押したり、現在のブラウザの[戻る]ボタンをクリックしたりしないでください。

始める前に

ファームウェアをアップグレードする前に、ATA 用ファームウェアアップグレードファイルをダウンロードします。

手順

ステップ 1 **[参照]** をクリックして、ダウンロードしたアップグレードファイルの場所を選択します。

ステップ 2 ファームウェアをアップグレードするには、**[アップグレード]** ボタンをクリックします。

構成管理

管理 > **設定の管理**ページから、ATA の構成設定をバックアップまたは復元します。

バックアップ コンフィギュレーション

管理 > **設定の管理** > **バックアップの設定**ページを使用して、ATA の設定をファイルにバックアップします。これらの同じ設定を ATA に後から復元することができます。

[バックアップ]ボタンをクリックして、ATA の設定情報を保存します。ダイアログボックスが表示されたら、cfg ファイルを保存する場所を選択します。

ヒント: バックアップを作成した日時を含む名前にファイル名を変更します。

構成の復元

管理 > **設定の管理** > **復元設定**ページから、ATA の設定を以前のバックアップから復元します。設定を復元する前に、現在の設定をバックアップしておくことを推奨します。

手順

ステップ 1 **参照**をクリックして、コンピュータ上の .cfg ファイルを探します。

ステップ 2 **復元**をクリックして、選択したファイルから設定を復元します。

リブート

管理 > **リブート**ページから、ATA Web ページからの ATA の電源を入れ直すことができます。もう 1 つの方法は、 **リセット** > **再起動**ボタンを押す方法です 。

リブートボタンをクリックして ATA の電源を入れ直します警告メッセージが表示されたら、情報を読み、**OK** をクリックして ATA をリブートするか、**キャンセル**をクリックして操作を中止します。ATA およびすべての接続されたデバイスは、この操作中にネットワーク接続を失います。