

Yealink

Yealink Teams[®] HD IP Phone 管理者 ガイド



目次

内容

序文	6
関連ドキュメント.....	6
表記規則と表記規則.....	6
推奨参照.....	7
はじめに	7
初期化プロセスの概要.....	7
ROMファイルのロード.....	8
VLAN の設定.....	8
DHCP (Dynamic Host Configuration Protocol) サーバのクエリ.....	8
プロビジョニングサーバーへの連絡.....	8
ファームウェアのアップデート.....	8
リソースファイルのダウンロード.....	8
起動の確認.....	9
Teams機能ライセンス.....	9
Webユーザーインターフェースを介したライセンスのインポート.....	10
ライセンス設定のインポート.....	10
デバイスネットワーク	10
IPv4 および IPv6 ネットワーク設定.....	11
IP アドレッシングモードの設定.....	11
IPv4 Configuration.....	11
IPv6 Configuration.....	14
IPv4 のDHCP オプション.....	16
IPv4 でサポートされるDHCP オプション.....	17
DHCPオプション160とオプション161.....	17
DHCPオプション66、オプション43、カスタムオプション.....	18
DHCPオプション42およびオプション2.....	18
DHCPオプション12.....	20
DHCPオプション60.....	20
IPv6 のDHCP オプション.....	21
IPv6 でサポートされるDHCP オプション.....	21
VLAN.....	21
LLDP設定.....	21
CDP 設定.....	22
手動VLAN 設定.....	23
DHCP VLAN 設定.....	25
VLAN 変更設定.....	26
Wi-Fi.....	26
Wi-Fi 設定.....	26

インターネットポートとPC ポート.....	28
対応伝送方式.....	28
インターネットポートとPC ポートの設定.....	29
802.1 x 認証.....	30
802.1 x 認証設定.....	30
プロキシサーバー.....	32
プロキシサーバーの設定.....	32
デバイスプロビジョニング.....	33
考慮すべきプロビジョニングポイント.....	34
起動ファイル、設定ファイル、リソースファイル.....	34
起動ファイル.....	34
設定ファイル.....	38
リソースファイル.....	41
ファイルのダウンロードプロセス.....	41
プロビジョニング方法.....	42
プロビジョニング方法の優先順位.....	42
手動プロビジョニング.....	43
セントラルプロビジョニング.....	47
プロビジョニングサーバーのセットアップ.....	49
対応プロビジョニングプロトコル.....	49
サポートされるプロビジョニングサーバー検出方法.....	50
プロビジョニングサーバーの設定.....	51
Microsoft Teams & Skype for Business Admin Center でのデバイスのプロビジョニング.....	50
デバイス管理.....	50
デバイス情報の編集.....	50
デバイスの表示要素のカスタマイズ.....	50
デバイスの詳細の表示.....	54
デバイスへの設定プロファイルの割り当て.....	54
診断デバイス.....	54
デバイスソフトウェアのアップデート.....	54
デバイスの再起動.....	55
構成プロファイル管理.....	55
構成プロファイルの作成.....	55
構成プロファイルの編集.....	56
デバイスへの設定プロファイルの割り当て.....	56
ファームウェアアップグレード.....	56
各デバイスモデルのファームウェア.....	56
ファームウェアアップグレードの設定.....	57
CP960 スター接続機能の使用.....	57
スター接続機能の設定ガイドライン.....	58
CP960 スター接続機能の設定.....	59
例: CP960 スター接続機能の設定.....	57

デバイスのカスタマイズ	57
言語	57
言語表示設定	58
言語のカスタマイズ	59
例: デバイス表示のカスタム言語の設定	63
スクリーンセーバー	63
スクリーンセーバーの設定	64
バックライト	66
バックライトの明るさと時間の設定	67
日時	67
時間帯	68
NTP 設定	69
DST 設定	71
時刻と日付の手動設定	75
時刻と日付形式の設定	75
音色	76
対応音色	77
トーン設定	77
ボリューム	78
ボリューム構成	78
省電力	79
省電力設定	79
電源LEDインジケータ	81
電源 LED インジケータの設定	82
Bluetooth	82
Bluetooth 設定	83
共通領域電話 (Common Area Phone)	84
通話機能	84
コールキュー	84
コールパークとリトリリーブ	84
セキュリティ機能	85
ユーザーと管理者の識別	85
ユーザーおよび管理者の識別設定	85
ユーザーアクセスレベルの設定	86
電話ロック	87
電話機のロック設定	87
トランスポート層セキュリティ	87
対応暗号スイート	88
サポートされる信頼済み証明書とサーバ証明書	88
TLS 設定	91
設定ファイルの暗号化	92
設定ファイル暗号化ツール	93
設定ファイルの暗号化と復号	93
暗号化と復号の設定	93
例: 構成ファイルの暗号化	95

ハイブリッドモード	96
ハイブリッドモードの設定	97
ページング設定	97
SIP アカウント登録の設定	101
アカウントコーデックの設定	104
ローカルディレクトリの設定	106
デバイス管理	107
デバイス管理設定	107
USB Camera UVC30 Room の管理	107
UVC30 カメラのアップグレード	108
カメラログのエクスポート	108
トラブルシューティング方法	108
ログファイル	108
ローカルログ	109
Syslog ログ	113
パケットキャプチャ	116
WEB ユーザー・インターフェースを通じた、パケットの取り込み	116
イーサネットソフトウェアキャプチャ設定	117
設定ファイルの分析	118
デバイスからのBIN ファイルのエクスポート	118
デバイスからBINファイルをインポートする	118
すべての診断ファイルのエクスポート	119
装置の状況	119
デバイスステータスの表示	119
デバイスと設定のリセット	120
デバイスをデフォルトの工場出荷時設定にリセットする	120
デバイスをカスタム出荷時設定にリセットする	120
カスタム出荷時設定ファイルの削除	121
デバイスの再起動	121
電話機のユーザーインターフェースを使用したデバイスの再起動	121
ウェブ・ユーザー・インターフェースを使ったデバイスの再ブート	122
電話機の現在の画面のキャプチャ	122
電話機のユーザーインターフェースを使用した画面キャプチャの有効化	122
Webユーザーインターフェースを介した装置の現在のスクリーニングの取得	122
トラブルシューティングソリューション	123
IP アドレスの問題	123
デバイスがIP アドレスを取得しない	123
IP コンフリクト	123
YealinkデバイスでIPv6を設定する際の特定のフォーマット	124
日時の問題	124
時刻・日付が正しく表示されない	124
ディスプレイの問題	124
デバイスの LCD 画面のダミー	124

デバイスに「オフライン」と表示される	124
ファームウェアとアップグレードの問題	125
デバイスファームウェアのアップグレードに失敗する	125
デバイスは設定を更新しません。	125
システムログの問題	125
プロビジョニングサーバー(FTP/TFTP サーバー)からシステムログをエクスポートできませんでした	125
Syslog サーバからのシステムログのエクスポートに失敗する	125
パスワードの問題	126
管理者パスワードを復元する	126

序文

Yealink管理者ガイドでは、デバイスネットワークのセットアップ、Teamsデバイスのプロビジョニングと管理に関する一般的なガイダンスを提供します。このガイドはエンドユーザーではなく、管理者を対象としています。

Yealink MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/CP960/VP59 Microsoft Teams デバイスは、Microsoft との連携デバイスです。管理者として、このガイドで以下のことができます:

- Microsoft Teams & Skype for Business Admin Center でTeams デバイスを管理します。
- プロビジョニングサーバーを設定します。
- 機能と設定を使用してデバイスをプロビジョニングします。
- デバイスのトラブルシューティング、アップデート、およびメンテナンスを行います。

このガイドの詳細は、ファームウェアを実行している次のYealink デバイ스에適用されます:

- T58A/T56A/T55A Teams IP 電話: 58.15.0.118 以降
- CP960 Teams IP Phone: 73.15.0.111 以降
- VP59 Teams IP Phone: 91.15.0.50 以降
- MP58/MP58-WH/MP56/MP54 Teams IP Phone: 122.15.0.27 以降

規制および安全に関するすべてのガイダンスについては、「Yealink 製品規制に関する通知」ガイドをお読みください。

- [関連ドキュメント](#)
- [表記規則と表記規則](#)
- [推奨参照](#)

関連ドキュメント

以下の関連ドキュメントを入手できます:

- 『クイックスタートガイド』では、デバイスの組み立て方法と、デバイスで利用可能な最も基本的な機能の設定方法について説明します。
- 『ユーザーガイド』では、電話のユーザーインターフェイスまたはWeb ユーザーインターフェイスを介してデバイスで使用可能な基本機能と高度な機能を設定および使用する方法について説明します。
- 『Auto Provisioning Guide』(オートプロビジョニングガイド)では、起動ファイルと設定ファイルを使用してデバイスをプロビジョニングする方法について説明します。

オートプロビジョニングガイドは、プロビジョニングサーバーを使用してYealink Teams デバイスをプロビジョニングするための基本的なガイダンスとして機能します。初心者の場合は、このガイドが役に立ちます。

サポートまたはサービスについては、Yealink 販売店にお問い合わせいただくか、Yealink テクニカルサポートオンライン(<http://support.yealink.com/>) をご覧ください。

表記規則と表記規則

Yealink のドキュメントには、いくつかの表記規則と表記規則が含まれています。

テキスト内情報のタイプを区別するには、次の基本的な表記規則を理解しておく必要があります:

記号	説明
太字	メニュー、メニュー選択、ソフトキー、ディレクトリ名などのWeb/Phone ユーザインターフェース項目が、プロシージャやユーザアクションに参与している場合に強調表示されます(たとえば、「設定」>「デバイス設定」を選択します)。テキストの強調にも使用されます(Important! など)。
イタリック体	テキストを強調するために使用され、値または入力例を示します(例の形式: http(s)://[IPv6address])。

また、条件情報を区別するために、以下の記述規則を知っておく必要があります:

記号	説明
<>	特定の情報を入力する必要があることを示します。たとえば、次のような場合です。<MAC> には、デバイスの12桁のMACアドレスを入力します。<deviceIPAddress> が表示された場合は、デバイスのIPアドレスを入力します。
>	メニューから項目を選択する必要があることを示します。たとえば、Settings > Device Settings(デバイス設定)は、次から Device Settings(デバイス設定)を選択する必要があることを示します。設定メニュー。

推奨参照

このガイドに含まれていない他のYealink製品の設定および管理の詳細については、Yealinkテクニカルサポートの製品サポートページを参照してください。

Yealink デバイスの最新のリリースノートまたはその他のガイドにアクセスするには、Yealink テクニカルサポートでお使いのデバイスのドキュメントダウンロードページを参照してください。

RFC (Request for Comments) ドキュメントを見つけるには、<http://www.ietf.org/rfc/rfcNNNN.txt>と入力します。(NNNN はRFC 番号) をブラウザの場所フィールドに入力します。

このガイドでは、主にT58A Teams 電話を例に説明します。他のTeamsデバイスの詳細については、Yealink Teams device固有のユーザーガイドを参照してください。

その他の参考情報については、この管理者ガイド全体のハイパーリンクまたはWeb情報を参照してください。

はじめに

この章では、Teams デバイスの基本的な初期化手順について説明します。

- [初期化プロセスの概要](#)
- [起動の確認](#)
- [Teams機能ライセンス](#)

初期化プロセスの概要

デバイスの初期化プロセスは、ネットワーク接続とローカルネットワーク内のデバイスの操作を担当します。デバイスをネットワークおよび電気供給に接続すると、デバイスの初期化プロセスが開始されます。

- [ROMファイルのロード](#)

- [VLAN の設定](#)
- [DHCP \(Dynamic Host Configuration Protocol\) サーバのクエリ](#)
- [プロビジョニングサーバへの連絡](#)
- [ファームウェアのアップデート](#)
- [リソースファイルのダウンロード](#)

ROMファイルのロード

ROMファイルは、デバイスのフラッシュメモリに格納されています。デバイスは工場出荷時にROM ファイルがプリロードされています。初期化の間、デバイスはROMファイルをロードして実行するブートストラップローダを実行します。

VLAN の設定

デバイスをスイッチに接続する場合、スイッチは(LLDPまたはCDPを使用する場合)スイッチに定義されたVLAN情報をデバイスに通知します。その後、デバイスはネットワーク設定のDHCP 要求を続行できます(DHCP を使用している場合)。

DHCP (Dynamic Host Configuration Protocol) サーバのクエリ

この装置は、DHCPサーバに質問することができます。

ネットワーク接続が確立されると、デバイスは初期化中にDHCP サーバから次のネットワークパラメータを取得できます:

- IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- プライマリDNS
- セカンダリDNS

デフォルトでは、デバイスはこれらのパラメータをDHCPv4 から取得します。いずれかのパラメータがDHCP サーバから提供されていない場合は、デバイスのネットワークパラメータを手動で設定できます。

プロビジョニングサーバへの連絡

プロビジョニングサーバから設定を取得するようにデバイスを設定すると、プロビジョニングサーバに接続され、起動時に起動ファイルと設定ファイルをダウンロードします。デバイスは、設定ファイルに書き込まれた設定を解決および更新できます。デバイスがプロビジョニングサーバからコンフィギュレーションを取得しない場合、デバイスはフラッシュメモリに保存されているコンフィギュレーションを使用します。

ファームウェアのアップデート

設定ファイルでファームウェアのアクセスURL を定義すると、デバイスはプロビジョニングサーバからファームウェアをダウンロードします。ダウンロードしたファームウェアファイルのMD5 値がフラッシュメモリに保存されているものと異なる場合、デバイスはファームウェアアップデートを実行します。

デバイスがプロビジョニングサーバからファームウェアをダウンロードしない場合は、ファームウェアを手動でアップグレードできます。

リソースファイルのダウンロード

デバイスは、設定ファイルに加えて、サービスを提供する前にリソースファイルを必要とする場合があります。これらのリソースファイルはオプションですが、特定の機能を展開する場合は、これらのファイルが必要です。

起動の確認

電源およびネットワークに接続すると、デバイスは初期化プロセスを開始します:

1. MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/VP59 の電源LED インジケータが赤色に点灯します。CP960のミュートタッチキーLEDインジケータが赤く点灯します。
2. 起動すると、液晶画面に“Initializing... Please wait” (または“Initializing...”)と表示されます。
3. デバイスは言語選択インターフェースに入ります。

Teams機能ライセンス

Yealink は、Microsoft Team 用に設定されたMP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/CP960/VP59 デバイスを提供します。デフォルトでは、Teams 機能ライセンスが組み込まれており、ユーザーはTeams 機能を持つ Yealink デバイスを直接使用できます。デバイスがまだライセンスをインポートしていない場合、画面は次のように表示されます:



Please import the license
IP 10.81.6.42

デバイスを通常使用するには、ライセンスをアップロードする必要があります。

Teams 機能ライセンスとデバイスバージョンについては、次の点に注意する必要があります。

- ライセンスを適用してインポートするには、Teams ビルドへのOpen SIP ビルドアップグレードが必要です。
- Skype for Business へのTeams アップグレードには、追加ライセンスは必要ありません。また、その逆も同様です。
- Teamsは、このリリースからOpen SIP にダウングレードすることはできません。Teams電話機が一時的なライセンス(デモテスト用)を受けていて、Open SIP に戻る場合は、Yealink サポートTeamsに連絡して、ロック解除ライセンスのテクニカルサポートを受けてください。
- 最新のTeams にアップグレードすると、以前のTeams バージョンにダウングレードすることはできなくなります。

Teams機能ライセンスの購入については、販売店または営業担当者にお問い合わせください。

注: Skype for Business ファームウェアを実行しているデバイスがSkype for Business 機能ライセンスをインポートされている場合は、Teamsファームウェアにアップグレードした後にライセンスをインポートする必要はありません。

- [Webユーザーインターフェースを介したライセンスのインポート](#)
- [ライセンス設定のインポート](#)

関連情報

[ファームウェアアップグレード](#)

Webユーザーインターフェースを介したライセンスのインポート

デバイスがライセンスをインポートしていない場合、またはライセンスの有効期限が切れている場合は、ライセンスを手動でインポートする必要があります。

手順

1. Webユーザーインターフェースで、「セキュリティ」>「ライセンス」と選択します。
2. 「ライセンスファイルのロード」(または「ライセンスファイルのアップロード」)ブロックで、白いボックスをクリックしてローカルシステムからライセンスを選択します。
3. アップロードをクリックします。

ライセンス設定のインポート

次の表に、ライセンスのインポートに使用できるパラメータを示します。

パラメータ	lync_license_dat.url ^[1]	<y0000000000xx>.cfg
説明	Teams 機能ライセンスのアクセスURL を設定します。 例: lync_license_dat.url = http://192.168.1.20/License_\$MAC.dat デバイスは、オートプロビジョニング中に"\$MAC" という文字をMAC アドレスに置き換えます。例えば、1 つのT58A Teams デバイスのMAC アドレスは00156543EC97 です。オートプロビジョニングを実行すると、デバイスは、プロビジョニングサーバーアドレス "http://192.168.1.20" からLicense_00156543ec97.dat ファイルをダウンロードするように要求します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	セキュリティ> ライセンス	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。


デバイスネットワーク

Yealink Teamsデバイスは、イーサネットローカルエリアネットワーク(LAN)上で動作します。ローカルエリアネットワークは、組織やYealink Teams デバイスによって異なる多くのネットワーク設計に対応するように構成できます。

- [IPv4 および IPv6 ネットワーク設定](#)
- [IPv4 のDHCP オプション](#)
- [IPv6 のDHCP オプション](#)
- [VLAN](#)
- [Wi-Fi](#)
- [インターネットポートとPC ポート](#)
- [802.1x 認証](#)
- [プロキシサーバー](#)

IPv4 および IPv6 ネットワーク設定

Teamsデバイスは、IPv4 アドレッシングモード、IPv6 アドレッシングモード、およびIPv4&IPv6 デュアルスタックアドレッシングモードをサポートします。有線ネットワークに接続すると、デバイスは DHCP(Dynamic Host Configuration Protocol)サーバーから IPv4 または IPv6 ネットワーク設定を取得できます(ネットワークがサポートしている場合)。IP 設定の管理を容易にするため、反復的な手動データ入力を排除できる自動DHCP を使用することをお勧めします。IPv4 またはIPv6 ネットワーク設定を手動で構成することもできます。

注: Teamsデバイスは、RFC 2131 で文書化されたDHCPv4 仕様と、RFC 3315 で文書化されたDHCPv6 仕様に準拠しています。

- [IP アドレッシングモードの設定](#)
- [IPv4 Configuration](#)
- [IPv6 Configuration](#)

IP アドレッシングモードの設定

次の表に、IP アドレッシングモードの設定に使用できるパラメータを示します。

パラメータ	static.network.ip_address_mode ^[1]	<MAC>.cfg
説明	IP アドレッシングモードを設定します。	
許容値	0-IPv4 1-IPv6 2-IPv4 & IPv6	
デフォルト	0	
Web UI	ネットワーク> 基本設定> インターネットポート> モード(IPv4/IPv6)	
電話機のUI	☰>「設定」>「デバイス設定」>(管理者のみ(既定のパスワード: admin))>「ネットワーク」>「WANポート」>IP モード	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

IPv4 Configuration

次の表に、IPv4 の設定に使用できるパラメータを示します。

パラメータ	static.network.internet_port.type ^[1]	<MAC>.cfg
説明	IPv4 のインターネットポートタイプを設定します。 注意: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。	
許容値	0-DHCP 2-Static IP	
デフォルト	0	
Web UI	ネットワーク> 基本設定> IPv4 設定> 設定タイプ	

電話機のUI	☰ 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別	
パラメータ	static.network.internet_port.ip ^[1]	<MAC>.cfg
説明	IPv4 アドレスを設定します。 注意: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定され、 "static.network.internet_port.type" が2 (Static IP) に設定されている場合にのみ。	
許容値	IPv4 アドレス	
デフォルト	空白	
Web UI	ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(静的IP) > IP アドレス	
電話機のUI	☰ 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(静的IP) > IP アドレス	
パラメータ	static.network.internet_port.mask ^[1]	<MAC>.cfg
説明	IPv4サブネットマスクを設定します。 注意: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定され、 "static.network.internet_port.type" が2 (Static IP) に設定されている場合にのみ機能	
許容値	サブネットマスク	
デフォルト	空白	
Web UI	ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(静的IP) > サブネットマスク	
電話機のUI	☰ 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(静的IP) > サブネットマスク	
パラメータ	static.network.internet_port.gateway ^[1]	<MAC>.cfg
説明	IPv4デフォルトゲートウェイを設定します。 注記: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定され、 "static.network.internet_port.type" が2 (Static IP) に設定されている場合にのみ。	
許容値	IPv4 アドレス	
デフォルト	空白	
Web UI	ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(静的IP) > デフォルトゲートウェイ	
電話機のUI	☰ 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(静的IP) > 既定のゲートウェイ	
パラメータ	static.network.static_dns_enable ^[1]	<y0000000000xx>.cfg

説明	<p>これにより、静的DNS 機能のオン/オフがトリガーされます。</p> <p>注意: "static.network.internet_port.type" が0 (DHCP) に設定されている場合にのみ機能します。</p>	
許容値	<p>0-オフにすると、デバイスはDHCP から取得したIPv4 DNS を使用します。</p> <p>1-オンにすると、デバイスは手動で設定された静的IPv4 DNS を使用します。</p>	
デフォルト	0	
Web UI	ネットワーク > 基本設定 > IPv4 設定 > 静的DNS	
パラメータ	static.network.primary_dns ^[1]	<MAC>.cfg
説明	<p>プライマリIPv4 DNS サーバを設定します。</p> <p>注意: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。DHCP環境では、"static.network.static_dns_enable" が1(On) に設定されていることも確認</p>	
許容値	IPv4 アドレス	
デフォルト	空白	
Web UI	<p>ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(静的IP) > プライマリDNS</p> <p>または、ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(DHCP) > 静的DNS(有効) > プライマリDNS</p>	
電話機のUI	<p>☰ > 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(静的IP) > プライマリDNS</p> <p>または > 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(DHCP) > IPv4 静的DNS (有効) > プライマリDNS ☰</p>	
パラメータ	static.network.secondary_dns ^[1]	<MAC>.cfg
説明	<p>セカンダリIPv4 DNS サーバを設定します。</p> <p>注意: "static.network.ip_address_mode" が0 (IPv4) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。DHCP環境では、"static.network.static_dns_enable" が1(On) に設定されていることも確認</p>	
許容値	IPv4 アドレス	
デフォルト	空白	
Web UI	<p>ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(静的IP) > セカンダリDNS</p> <p>または、ネットワーク > 基本設定 > IPv4 設定 > 設定タイプ(DHCP) > 静的DNS(有効) > セカンダリDNS</p>	
電話機のUI	<p>☰ > 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(静的IP) > セカンダリDNS</p> <p>または > 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 > WAN ポート > IPv4 種別(DHCP) > IPv4 静的DNS(有効) > セカンダリDNS ☰</p>	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

IPv6 Configuration

IPv6 ネットワーク用にデバイスのネットワーク設定を構成する場合は、SLAAC (ICMPv6)、DHCPv6 を使用するか、IP アドレスを手動で入力して、デバイスのIP アドレスを設定できます。ネットワーク環境がIPv6 をサポートしていることを確認します。詳細については、ISP にお問い合わせください。

デバイスでSLAAC とDHCPv6 の両方を有効にすると、サーバーはSLAAC またはDHCPv6 のいずれかからIPv6 アドレスとその他のネットワーク設定を取得するデバイスを指定できます。SLAAC サーバーが動作していない場合、デバイスはDHCPv6 経由でIPv6 アドレスとその他のネットワーク設定を取得しようとします。

次の表に、IPv6 の設定に使用できるパラメータを示します。

パラメータ	static.network.ipv6_internet_port.type ^[1]	<MAC>.cfg
説明	IPv6 のインターネットポートタイプを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。	
許容値	0-DHCP 1-静的IP	
デフォルト	0	
Web UI	ネットワーク> 基本設定> IPv6 設定> 設定タイプ	
電話機のUI	☰> 「設定」> 「デバイス設定」> 「ネットワーク」(既定のパスワード: admin) > 「WAN ポート」> 「IPv6 種別」	
パラメータ	static.network.ipv6_internet_port.ip ^[1]	<MAC>.cfg
説明	IPv6 アドレスを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定され、"static.network.ipv6_internet_port.type" が1 (Static IP) に設定されている場合に。	
許容値	IPv6アドレス	
デフォルト	空白	
Web UI	ネットワーク> 基本設定> IPv6 設定> 設定タイプ(静的IP) > IP アドレス	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))> 「ネットワーク」> WAN ポート> IPv6 種別(静的IP) > IP アドレス	
パラメータ	static.network.ipv6_prefix ^[1]	<MAC>.cfg
説明	IPv6プレフィックスを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定され、"static.network.ipv6_internet_port.type" が1 (Static IP) に設定されている場合	
許容値	0 ~ 128 の整数	
デフォルト	64	

Web UI	ネットワーク> 基本設定> IPv6 設定> 設定種別(静的IP)> IPv6 プレフィックス(0 ~128)	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> WAN ポート> IPv6 種別(静的IP)> IPv6 IP プレフィックス(0 ~128)	
パラメータ	static.network.ipv6_internet_port.gateway ^[1]	<MAC>.cfg
説明	IPv6 デフォルトゲートウェイを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定され、 "static.network.ipv6_internet_port.type" が1 (Static IP	
許容値	IPv6アドレス	
デフォルト	空白	
Web UI	ネットワーク> 基本設定> IPv6 設定> 設定タイプ(静的IP)> デフォルトゲートウェイ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> WAN ポート> IPv6 種別(静的IP)> 既定のゲートウェイ	
パラメータ	static.network.ipv6_static_dns_enable ^[1]	<MAC>.cfg
説明	静的IPv6 DNS 機能のオン/オフをトリガします。 注意: "static.network.ipv6_internet_port.type" が0 (DHCP) に設定されている場合にのみ機能します。	
許容値	0-オフにすると、デバイスはDHCP から取得したIPv6 DNS を使用します。 1-オンにすると、デバイスは手動で設定された静的IPv6 DNS を使用します。	
デフォルト	0	
Web UI	ネットワーク> 基本設定> IPv6 設定> IPv6 静的DNS (または静的IPv6 DNS)	
パラメータ	static.network.ipv6_primary_dns ^[1]	<MAC>.cfg
説明	プライマリIPv6 DNS サーバを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。DHCP環境では、 「static.network.ipv6_static_dns_enable」が1(On)に設定されている。	
許容値	IPv6アドレス	
デフォルト	空白	
Web UI	ネットワーク> 基本設定> IPv6 設定> 設定タイプ(静的IP)> プライマリDNS または、ネットワーク> 基本設定> IPv6 設定> 設定タイプ(DHCP)> 静的DNS(有効)> プライマリDNS	

電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> WAN ポート> IPv6 種別(静的IP)> プライマリDNS または> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> ☰ WANポート> IPV6タイプ(DHCP)> IPV6 Static DNS(Enable)> プライマリDNS	
パラメータ	static.network.ipv6_secondary_dns ^[1]	<MAC>.cfg
説明	セカンダリIPv6 DNS サーバを設定します。 注意: "static.network.ip_address_mode" が1 (IPv6) または2 (IPv4 & IPv6) に設定されている場合にのみ機能します。DHCP環境では、「static.network.ipv6_static_dns_enable」が1(On)に設定されている。	
許容値	IPv6アドレス	
デフォルト	空白	
Web UI	ネットワーク> 基本設定> IPv6 設定> 設定タイプ(静的IP)> セカンダリDNS または、ネットワーク> 基本設定> IPv6 設定> 設定タイプ(DHCP)> 静的DNS(有効)> セカンダリDNS	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> WAN ポート> IPv6 種別(静的IP)> 秒。DNS または> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> ☰ WANポート> IPV6タイプ(DHCP)> IPV6 Static DNS(Enable)> セカンダリDNS	
パラメータ	static.network.ipv6_icmp_v6.enable ^[1]	<MAC>.cfg
説明	電話機がSLAAC (ステートレスアドレス自動設定)経由でIPv6ネットワーク設定を取得することを有効または無効にします。 注意: "static.network.ipv6_internet_port.type" が0 (DHCP) に設定されている場合にのみ機能します。	
許容値	0-Disabled 1-Enabled	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > ICMPv6 ステータス> アクティブ	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

IPv4 のDHCP オプション

Teamsデバイスは、DHCPオプションを介して、IPv4ネットワークにおけるIPv4関連パラメータを取得することができます。

 注記: DHCP オプションの詳細については、RFC 2131 またはRFC 2132 を参照してください。

- [IPv4 でサポートされるDHCP オプション](#)
- [DHCPオプション160とオプション161](#)
- [DHCPオプション66、オプション43、カスタムオプション](#)
- [DHCPオプション42およびオプション2](#)
- [DHCPオプション12](#)

- [DHCPオプション60](#)

IPv4 でサポートされるDHCP オプション

次の表に、デバイスでサポートされるIPv4 の一般的なDHCP オプションを示します。

パラメータ	DHCPオプション	説明
サブネットマスク	1	クライアントのサブネットマスクを指定します。
タイムオフセット	2	クライアントのサブネットのオフセットを Coordinated からの秒単位で指定します。 世界時(UTC)。
ルータ	3	クライアントのサブネット上のルータのIP アドレスのリストを指定します。
タイムサーバー	4	クライアントが使用できるタイムサーバのリストを指定します。
ドメインネームサーバー	6	クライアントが使用できるドメインネームサーバーのリストを指定します。
ログサーバ	7	クライアントが使用できるMIT-LCS UDP サーバのリストを指定します。
ホスト名	12	クライアントの名前を指定します。
ドメインサーバー	15	DNS 経由でホスト名を解決するときにクライアントが使用するドメイン名を指定します。
ブロードキャストアドレス	28	クライアントのサブネットで使用中のブロードキャストアドレスを指定します。
ネットワークタイムプロトコルサーバー	42	IP アドレスでクライアントが使用できるNTP サーバのリストを指定します。
ベンダ特有の情報	43	ベンダー固有の情報を特定します。
ベンダークラス識別子	60	ベンダータイプを特定します。
TFTP サーバ名	66	DHCP ヘッダーの「sname」フィールドがDHCP オプションに使用されている場合は、TFTP サーバを識別します。

DHCPオプション160とオプション161

Yealink Teams デバイスは、起動時に DHCP カスタムオプションを検出することで、プロビジョニングサーバーアドレスの取得をサポートします。

DHCP Option 66 が使用できない場合、プロビジョニングサーバのURL またはIP アドレスでカスタムオプション (160 または161) を使用できます。デバイスは、プロビジョニングサーバアドレスを取得するためのオプション160 または161 を自動的に検出します。

DHCP オプション 160 またはオプション 161 を使用するには、DHCP 有効機能が有効で、カスタムオプションが設定されていることを確認します。

- [DHCPオプション160およびオプション161構成](#)

DHCPオプション160およびオプション161構成

次の表に、DHCPオプション160または161を設定するために使用できるパラメータを示します。

パラメータ	static.auto_provision.dhcp_option.enable ^[1]	<y0000000000xx>.cfg
説明	これにより、DHCPオプション機能のオン/オフがトリガされます。	
許容値	0-Off 1-On	
デフォルト	1	
Web UI	設定 > オートプロビジョニング > DHCP 有効	
パラメータ	static.auto_provision.dhcp_option.list_user_options ^[1]	<y0000000000xx>.cfg
説明	プロビジョニングサーバアドレスを要求するためのカスタムDHCP オプションを設定します。複数のDHCP オプションはカンマで区切ります。 注意: "static.auto_provision.dhcp_option.enable" が1 (On) に設定されている場合にのみ機能します。	
許容値	128 ~ 254 の整数	
デフォルト	160,161	
Web UI	設定 > オートプロビジョニング > カスタムオプション	


[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

DHCPオプション66、オプション43、カスタムオプション

起動中に、デバイスはプロビジョニングサーバアドレスを取得するためのカスタムオプション、オプション66、またはオプション43を自動的に検出します。プロビジョニングサーバアドレスの取得の優先順位は、custom option > option 66 (TFTP サーバを識別) > option 43 のようになります。

Teams デバイスは、起動時にオプション 43を検出することで、Auto Configuration Server (ACS) アドレスを取得できます。

DHCP オプションを介してサーバアドレスを取得するには、デバイスで DHCP オプションを設定していることを確認します。このオプションは、DHCP サーバで定義されているものに従っている必要があります。

 注: DHCP サーバでプロビジョニングサーバを検出するためのDHCP オプションの設定に失敗した場合は、プロビジョニングサーバアドレスを自動的に検出する別の方法が必要です。1つの可能性として、要求されたプロビジョニングサーバアドレスでDHCP INFORM クエリに回答するセカンダリDHCP サーバに接続することができます。詳細については、RFC 3925を参照してください。
単一の代替DHCP サーバが応答する場合、これは、プライマリDHCP サーバが有効なプロビジョニングサーバアドレスで応答するシナリオと機能的に同等です。DHCPサーバが反応しない場合、INFORM問合わせ処理は再度行われ、時間が切れるまで再度行われます。

DHCPオプション42およびオプション2

Yealink Teamsデバイスは、DHCPによって提供されるNTPサーバアドレスを使用することができます。

DHCPオプション42は、IPアドレス別にクライアントが利用可能なNTPサーバのリストを特定するために使用される。NTP サーバは、優先順位に従って一覧表示する必要があります。

DHCPオプション2は、協調ユニバーサルタイム(UTC)から秒単位でクライアントのサブネットのオフセットを指定するために使用されます。

関連情報

NTP 設定

DHCPオプション12

DHCP を使用する場合は、デバイスのホスト名を指定できます。DHCP クライアントは、オプション12 を使用して、事前定義されたホスト名をDHCP 登録サーバに送信します。名前は、ローカルドメイン名(RFC 2132 に基づく)で修飾される場合とされない場合があります。文字制限については、RFC 1035 を参照してください。

- [DHCPオプション12 ホスト名の設定](#)

DHCPオプション12 ホスト名の設定

以下の表に、DHCPオプション12 hostnameの設定に使用できるパラメータを列挙します。

パラメータ	static.network.dhcp_host_name ^[1]	<y0000000000xx>.cfg
説明	デバイスにDHCP オプション12 ホスト名を設定します。	
許容値	99文字以内の文字列	
デフォルト	T58A : SIP-T58 T56A : SIP-56A CP960 : SIP-CP960 T55A : SIP-T55A VP59 : VP59 MP54 : MP54 MP56 : MP56 MP58/MP58-WH: MP58	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

DHCPオプション60

DHCPオプション60は、DHCP顧客のベンダーおよび機能性を特定するために使用されます。オプション60 の形式を設定できます。デフォルトのベンダークラスID は“yealink”です。

- [DHCPオプション60構成](#)

DHCPオプション60構成

次の表に、DHCPオプション60の設定に使用できるパラメータを示します。

パラメータ	static.auto_provision.dhcp_option.option60_value ^[1]	<y0000000000xx>.cfg
説明	DHCPオプション60の値(デバイスのベンダー名)を設定します。	
許容値	99文字以内の文字列	
デフォルト	yealink	
Web UI	設定> オートプロビジョニング> DHCP オプション値	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

IPv6 のDHCP オプション

Teams装置は、DHCPオプションを介して、IPv6ネットワーク内のIPv6関連パラメータを取得することができます。

- [IPv6 でサポートされるDHCP オプション](#)

IPv6 でサポートされるDHCP オプション

次の表に、Yealink Teams デバイスでサポートされるIPv6 の一般的なDHCP オプションを示します。

パラメータ	DHCPオプション	説明
DNSサーバー	23	クライアントが使用できるDNS サーバのリストを指定します。
DNSドメイン検索リスト	24	クライアントにドメイン検索リストを指定します。
SNTPサーバ	31	クライアントが使用できるSNTP(Simple Network Time Protocol)サーバーのリストを指定します。
情報更新時間	32	クライアントがDHCPv6から取得した情報を更新するまでの待機時間の上限を指定します。

VLAN

デバイスのVLAN 設定の目的は、デバイスによって生成されたパケットにVLAN 情報を含むタグを挿入することです。デバイスのポート(インターネットポートとPC ポート)にVLAN が適切に設定されている場合、デバイスはこれらのポートからのすべてのパケットにVLAN ID のタグを付けます。スイッチは、IEEE Std 802.3 に記載されているように、タグ内のVLAN ID に従って、タグ付きパケットを受信し、対応するVLAN に転送します。

デバイス上のVLAN は、通常のPC への同時アクセスを可能にします。この機能を使用すると、PC をデバイスにデジーチェーン接続し、PC と電話の両方の接続を同じ物理Ethernet ケーブルを介してトランクできます。

デバイスは、手動設定に加えて、LLDP、CDP、またはDHCP を介したVLAN の自動検出もサポートします。割り当ては、LLDP/CDP を介した割り当て、手動設定、DHCP を介した割り当ての順に有効になります。

- [LLDP設定](#)
- [CDP 設定](#)
- [手動VLAN 設定](#)
- [DHCP VLAN 設定](#)
- [VLAN 変更設定](#)

LLDP設定

LLDP (Linker Layer Discovery Protocol) は、ベンダーに依存しないLink Layer プロトコルです。これにより、デバイスは、プロトコルも使用しているネットワーク上の直接接続されたデバイスとデバイス関連の情報を送受信したり、他のデバイスに関する情報を保存したりできます。

LLDP機能がデバイスで有効になっている場合、デバイスは、その情報を直接接続されたLLDP対応スイッチに定期的にアドバタイズします。デバイスは、接続されたスイッチからLLDPパケットを受信することもできます。アプリケーションタイプが「音声」の場合、デバイスはLLDPパケットから取得したVLAN設定を更新するかどうかを決定します。デバイスのVLAN 設定が異なる場合

スイッチから送信されたものから、デバイスはアップデートとリブートを実行します。これにより、デバイスは任意のスイッチに接続し、VLAN ID を取得してから、呼制御との通信を開始できます。

次の表に、LLDP の設定に使用リストパラメータを示します。

パラメータ	static.network.lldp.enable ^[1]	<y0000000000xx>.cfg
説明	デバイスのLLDP機能を有効または無効にします。	
許容値	0-無効 1-有効にすると、デバイスはLLDP経由でVLAN IDの決定を試みます。	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > LLDP > アクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> LLDP > LLDPステータス	
パラメータ	static.network.lldp.packet_interval ^[1]	<y0000000000xx>.cfg
説明	デバイスがLLDP依頼を送信する間隔(秒)を設定します。 注:「static.network.lldp.enable」が1(Enabled)に設定されている場合にのみ機能します。	
許容値	1 ~ 3600 の整数	
デフォルト	60	
Web UI	ネットワーク> 高度な設定 > LLDP > Packet Interval(1-3600s)	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> LLDP > LLDPインターバル	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

CDP 設定

CDP (Cisco Discovery Protocol)を使用すると、デバイスは、プロトコルも使用しているネットワーク上の直接接続されたデバイスとの間でデバイス関連情報を送受信したり、他のデバイスに関する情報を保存したりできます。

CDP 機能がデバイスで有効になっている場合、デバイスは、直接接続されたCDP 対応スイッチに定期的にその情報をアドバタイズします。デバイスはまた、接続されたスイッチからCDPパットを受け取ることができる。デバイスのVLAN 設定がスイッチから送信されたVLAN 設定と異なる場合、デバイスは更新とリブートを実行します。これにより、デバイスを任意のスイッチに接続し、それらのVLAN ID を取得してから、呼制御との通信を開始できます。

次の表に、CDP の設定に使用できるパラメータを示します。

パラメータ	static.network.cdp.enable ^[1]	<y0000000000xx>.cfg
説明	CDP 機能を有効または無効にします。	
許容値	0-無効 1-有効にすると、電話機はCDP を介してVLAN ID の決定を試みます。	
デフォルト	1	

Web UI	ネットワーク> 詳細設定> CDP > アクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > CDP > CDP ステータス	
パラメータ	static.network.cdp.packet_interval ^[1]	<y0000000000xx>.cfg
説明	電話機がCDP 要求を送信する間隔(秒)を設定します。 注:「static.network.cdp.enable」が1 (Enabled)に設定されている場合にのみ機能します。	
許容値	1 ~ 3600 の整数	
デフォルト	60	
Web UI	ネットワーク> 高度な設定 > CDP > CDP Interval (1~3600s)	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > CDP > CDP間隔	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

手動VLAN 設定

VLAN は、不履行でデバイスで無効になっています。インターネットポートとPC ポートにVLAN を手動で設定できます。デバイスでVLAN を設定する前に、ネットワーク管理者からVLAN ID を取得する必要があります。

PC ポートはCP960 には適用されず、インターネットポートのVLAN のみを手動で設定できます。次の表に、VLAN を手動で設定するために使用できるパラメータを示します。

パラメータ	static.network.vlan.internet_port_enable ^[1]	<y0000000000xx>.cfg
説明	インターネットポートのVLAN を有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	ネットワーク> 高度な設定 > VLAN > WAN ポート> アクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > VLAN > WANポート	
パラメータ	static.network.vlan.internet_port_vid ^[1]	<y0000000000xx>.cfg
説明	インターネットポートのVLAN ID を設定します。 注意: “static.network.vlan.internet_port_enable” が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	1 ~ 4094 の整数	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > VLAN > WAN ポート> VID	

電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」> > VLAN > WANポート> VID	
パラメータ	static.network.vlan.internet_port_priority ^[1]	<y0000000000xx>.cfg
説明	インターネットポートのVLAN プライオリティを設定します。7 が最高の優先順位、0 が最低の優先順位です。 注意: “static.network.vlan.internet_port_enable” が1 (Enabled) に設定されている場合のみ機能します。	
許容値	0 ~7 の整数	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > VLAN > WAN ポート> 優先順位	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」> > VLAN > WANポート> 優先順位	
パラメータ	static.network.vlan.pc_port_enable ^[1]	<y0000000000xx>.cfg
説明	PC ポートのVLAN を有効または無効にします。 注意: “static.network.pc_port.enable” が1 (Auto Negotiation) に設定されている場合のみ機能します。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
対応デバイス	CP960以外のすべてのデバイス	
Web UI	ネットワーク> 高度な設定 > VLAN > PC ポート> アクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」> > VLAN > PC ポート	
パラメータ	static.network.vlan.pc_port_vid ^[1]	<y0000000000xx>.cfg
説明	PC ポートのVLAN ID を設定します。 注意: “static.network.pc_port.enable” が1 (Auto Negotiation) に設定され、“static.network.vlan.pc_port_enable” が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	1 ~4094 の整数	
デフォルト	1	
対応デバイス	CP960以外のすべてのデバイス	
Web UI	ネットワーク> 高度な設定 > VLAN > PC ポート> VID	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」> > VLAN > PC ポート> VID	
パラメータ	static.network.vlan.pc_port_priority ^[1]	<y0000000000xx>.cfg

説明	PC ポートのVLAN プライオリティを設定します。7 が最高の優先順位、0 が最低の優先順位です。 注意: “static.network.pc_port.enable” が1 (Auto Negotiation) に設定され、 “static.network.vlan.pc_port_enable” が1 (Enabled)
許容値	1 ~ 7 の整数
デフォルト	0
対応デバイス	CP960以外のすべてのデバイス
Web UI	ネットワーク> 高度な設定 > VLAN > PC ポート> 優先順位
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > VLAN > PC ポート> 優先順位

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

DHCP VLAN 設定

Yealink Teams デバイスは、DHCP 経由のVLAN 検出をサポートします。VLAN 検出方法がDHCP に設定されている場合、デバイスは有効なVLAN ID のDHCP オプションを調べます。事前定義されたオプション132 は、デフォルトでVLAN ID を供給するために使用されます。VLAN ID を要求するために使用されるDHCP オプションをカスタマイズできます。

次の表に、DHCP VLAN 検出の設定に使用できるパラメータを示します。

パラメータ	static.network.vlan.dhcp_enable ^[1]	<y0000000000xx>.cfg
説明	デバイスのDHCP VLAN 検出機能を有効または無効にします。	
許容値	0 - 無効 1 - 有効	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > DHCP VLAN > アクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > DHCP VLAN	
パラメータ	static.network.vlan.dhcp_option ^[1]	<y0000000000xx>.cfg
説明	機器がVLAN設定を取得するDHCPオプションを設定します。最大5つのDHCP オプションを設定し、カンマで区切ることができます。	
許容値	1 ~ 255 の整数	
デフォルト	132	
Web UI	ネットワーク> 高度な設定 > DHCP VLAN > オプション(1-255)	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin))>「ネットワーク」> > DHCP VLAN > オプション	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

VLAN 変更設定

次の表に、VLAN 変更の設定に使用リストパラメータを示します。

パラメータ	static.network.vlan.vlan_change.enable ^[1]	<y0000000000xx>.cfg
説明	デバイスが現在のVLAN 割り当て方法を使用してVLAN ID を取得できない場合に、VLAN 割り当て方法の低い優先度を使用してVLAN ID を取得するか、VLAN 機能を閉じるかを有効または無効にします。 各方式の優先順位はLLDP/CDP > 手動 > DHCP VLAN です。	
許容値	0- 無効 1- 有効にすると、デバイスは、より高いプライオリティ方式を使用してVLAN ID の取得に失敗した場合に、より低いプライオリティ方式を使用しようとします。すべての方法が試行されると、デバイスはVLAN 機能を無効にします。	
デフォルト	0	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

Wi-Fi

Wi-Fi 機能を使用すると、デバイスを組織のワイヤレスネットワークに接続できます。

 注記: T56A/T55A/MP54 の場合、Wi-Fi USB ドングルWF50 がデバイスに接続されていることを確認してください。

- [Wi-Fi 設定](#)

Wi-Fi 設定

次の表に、Wi-Fi の設定に使用できるパラメータを示します。

パラメータ	static.wifi.function.enable ^[1]	<y0000000000xx>.cfg
説明	Wi-Fi 機能を有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	1	
パラメータ	static.wifi.enable	<y0000000000xx>.cfg
説明	Wi-Fi モードを有効または無効にします。 注意: 「static.wifi.function.enable」が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	ネットワーク > Wi-Fi > Wi-Fi アクティブ(またはWi-Fi)	
電話機のUI	☰ > 設定 > デバイス設定 > Wi-Fi > Wi-Fi	

パラメータ	static.wifi.X. 標識 ^[2]	<y0000000000xx>.cfg
説明	<p>特定のワイヤレスネットワークのプロファイル名を設定します。</p> <p>注意: "static.wifi.function.enable" と "static.wifi.enable" が1 (Enabled) に設定されている場合にのみ機能します。</p>	
許容値	32文字以内の文字列	
デフォルト	空白	
パラメータ	static.wifi.X. ssid ^[2]	<y0000000000xx>.cfg
説明	<p>特定のワイヤレスネットワークのSSID を設定します。</p> <p>SSID は、ワイヤレスアクセスポイントにアクセスするための一意の識別子です。</p> <p>注意: 「static.wifi.function.enable」と「static.wifi.enable」が1 (Enabled) に設定されている場合にのみ機能します。</p>	
許容値	32文字以内の文字列	
デフォルト	空白	
パラメータ	static.wifi.X. プライオリティ ^[2]	<y0000000000xx>.cfg
説明	<p>特定のワイヤレスネットワークの優先順位を設定します。5</p> <p>が最高の優先順位、1 が最低の優先順位です。</p> <p>注意: "static.wifi.function.enable" と "static.wifi.enable" が1 (Enabled) に設定されている場合にのみ機能します。</p>	
許容値	1 ~5 の整数	
デフォルト	1	
パラメータ	static.wifi.X.security_mode ^[2]	<y0000000000xx>.cfg
説明	<p>特定のワイヤレスネットワークのセキュリティモードを設定します。</p> <p>注意: "static.wifi.function.enable" と "static.wifi.enable" が1 (Enabled) に設定されている場合にのみ機能します。</p>	
許容値	NONE, WEP, WPA/WPA2 PSK, 802.1x EAP	
デフォルト	なし	
パラメータ	static.wifi.X.cipher_type ^[2]	<y0000000000xx>.cfg
説明	<p>特定のワイヤレスネットワークの暗号化タイプを設定します。</p> <p>「static.wifi.X.security_mode」がNONE に設定されている場合、このパラメータの許可値はNONE です。</p> <p>「static.wifi.X.security_mode」が802.1x EAP に設定されている場合、このパラメータの許可値はPEAP、TLS、TTLS、またはPWD です。</p> <p>注:「static.wifi.function.enable」と「static.wifi.enable」が1(イネーブル)に設定されている場合のみ有効です。</p>	
許容値	NONE、PEAP、TLS、TTLS、PWD	
デフォルト	なし	
パラメータ	static.wifi.X. 暗証番号 ^[2]	<y0000000000xx>.cfg

説明	特定のワイヤレスネットワークのパスワードを設定します。 注意: "static.wifi.function.enable" と "static.wifi.enable" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	64文字以内の文字列	
デフォルト	空白	
パラメータ	static.wifi.X.eap_type ^[2]	<y0000000000xx>.cfg
説明	特定のワイヤレスネットワークのEAP 認証モードを設定します。 注意: 「static.wifi.function.enable」と「static.wifi.enable」が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	TTLS、PEAP、またはTLS	
デフォルト	空白	
パラメータ	static.wifi.X.eap_user_name ^[2]	<y0000000000xx>.cfg
説明	特定のワイヤレスネットワークのEAP 認証ユーザ名を設定します。 注意: "static.wifi.function.enable" と "static.wifi.enable" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	64文字以内の文字列	
デフォルト	空白	
パラメータ	static.wifi.X.eap_password ^[2]	<y0000000000xx>.cfg
説明	特定のワイヤレスネットワークのEAP 認証パスワードを設定します。 注意: 「static.wifi.function.enable」と「static.wifi.enable」が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	64文字以内の文字列	
デフォルト	空白	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

[2]X X はWi-Fi ID です。X=1-5 です。

インターネットポートとPC ポート

Yealink Teamsデバイスは、インターネットポートとPCポートの2つのイーサネットポートをサポートします。デバイスのPCポートを有効または無効にすることができます。

PC ポートは、CP960 デバイスには適用されません。

- [対応伝送方式](#)
- [インターネットポートとPC ポートの設定](#)

対応伝送方式

デバイスのインターネットポートとPCポートのための3つのオプションの伝送構成方法:

- オートネゴシエーション
- 半二重(10Mbps または100Mbps で送信)
- 全二重(10Mbps、100Mbps、1000Mbps で送信(CP960 には適用されません))

自動ネゴシエーションは、デフォルトでデバイスのインターネットポートとPC ポートの両方に設定されます。

インターネットポートとPC ポートの設定

次の表に、インターネットポートとPC ポートの設定に使用できるパラメータを示します。

パラメータ	static.network.pc_port.enable ^[1]	<y0000000000xx>.cfg
説明	PC ポートを有効または無効にします。	
許容値	0-無効 1-オートネゴシエーション	
デフォルト	1	
対応デバイス	CP960以外のすべてのデバイス	
Web UI	ネットワーク> PC ポート> PC ポートアクティブ	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」>> PC ポート	
パラメータ	static.network.internet_port.speed_duplex ^[1]	<y0000000000xx>.cfg
説明	インターネットポートの送信方法を設定します。 注:電話機がギガビットイーサネットをサポートするスイッチに接続されている場合、伝送速度を1000Mbps/オートネゴシエーションに設定して、1000Mbps で伝送できます。このパラメータは変更しないことをお勧めします。	
許容値	0-オートネゴシエーション 1-全二重10Mbps 2-全二重100Mbps 3-半二重10Mbps 4-半二重100Mbps 5-Full Duplex 1000Mbps(CP960 には適用されません)	
デフォルト	0	
Web UI	ネットワーク> 高度な設定 > ポートリンク> WAN ポートリンク	
パラメータ	static.network.pc_port.speed_duplex ^[1]	<y0000000000xx>.cfg
説明	PC ポートの送信方法を設定します。 注: 電話機がギガビットイーサネットをサポートするスイッチに接続されている場合、送信速度を1000Mbps/オートネゴシエーションに設定して、1000Mbps で送信できます。このパラメータは変更しないことをお勧めします。	
許容値	0-オートネゴシエーション 1-全二重10Mbps 2-全二重100Mbps 3-半二重10Mbps 4-半二重100Mbps 5-Full Duplex 1000Mbps	

デフォルト	0	
対応デバイス	CP960以外のすべてのデバイス	
Web UI	ネットワーク > 高度な設定 > ポートリンク > PC ポートリンク	
パラメータ	static.network.vlan.pc_port_mode ^[1]	<y0000000000xx>.cfg
説明	<p>PC ポートでVLAN が有効になっている場合に、電話機がPC ポートのパケットを処理する方法を設定します。</p> <p>注: パケットがインターネットポートからPC ポートに送信される時は、パケットのタグがPC ポートに設定されているタグと同じ場合は削除し、それ以外の場合はパケットを直接転送します。</p>	
許容値	<p>0-パケットがPCポートからインターネットポートに送信されると、電話機はパケットを直接転送します。</p> <p>1-パケットがPC ポートからインターネットポートに送信され、パケットにVLAN タグがない場合、電話はPC ポートに設定されたタグでパケットにタグを付けて転送します。</p>	
デフォルト	1	
対応デバイス	CP960以外のすべてのデバイス	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

802.1 x 認証

Yealink Teams IP Phones では、802.1X 認証のために次の手順をサポートしています:

- EAP-MD5
- EAP-TLS (デバイスとCA 証明書が必要、パスワードは不要)
- EAP-PEAP/MSCHAPv2(CA 証明書が必要)
- EAP-TTLS/EAP-MSCHAPv2(CA 証明書が必要)
- EAP-PEAP/GTC(CA 証明書が必要)
- EAP-TTLS/EAP-GTC(CA 証明書が必要)
- EAP-FAST (EAP 帯域内プロビジョニングをサポート、プロビジョニング方法が認証プロビジョニングの場合はCA 証明書が必要)

802.1X認証の詳細については、Yealink 802.1X認証を参照してください。

- [802.1x 認証設定](#)

802.1 x 認証設定

次の表に、802.1x認証を設定するために使用できるパラメータを示します。

パラメータ	static.network.802_1x.mode ^[1]	<y0000000000xx>.cfg
説明	それは、802.1xの認証方法を設定する。	

許容値	0-EAP-None、802.1x認証は不要です。 1-EAP-MD5 2-EAP-TLS 3-EAP-PEAP/MSCHAPv2 4-EAP-TTLS/EAP-MSCHAPv2 5-EAP-PEAP/GTC 6-EAP-TTLS/EAP-GTC 7-EAP-FAST	
デフォルト	0	
Web UI	ネットワーク > 高度な設定 > 802.1x > 802.1xモード	
電話機のUI	☰ > [設定] > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 802.1x > 802.1x モード	
パラメータ	static.network.802_1x.identity ^[1]	<y0000000000xx>.cfg
説明	それは、ユーザー名を802.1x認証用に設定します。 注:「静的.network.802_1x.mode」が1,2,3,4,5,6,7に設定されている場合のみ有効です。	
許容値	32文字以内の文字列	
デフォルト	空白	
Web UI	ネットワーク > 高度な設定 > 802.1x > アイデンティティ	
電話機のUI	☰ > [設定] > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 802.1x > アイデンティティ	
パラメータ	static.network.802_1x.md5_password ^[1]	<y0000000000xx>.cfg
説明	それは、パスワードを802.1x認証用に設定します。 注意:「静的.network.802_1x.mode」が1,3,4,5,6,7に設定されている場合のみ有効です。	
許容値	32文字以内の文字列	
デフォルト	空白	
Web UI	ネットワーク > 高度な設定 > 802.1x > MD5 Password	
電話機のUI	☰ > [設定] > デバイス設定 > (管理者のみ(既定のパスワード: admin) > 「ネットワーク」 802.1x > MD5 パスワード	
パラメータ	static.network.802_1x.root_cert_url ^[1]	<y0000000000xx>.cfg
説明	CA 証明書のアクセスURL を設定します。 証明書の形式は、*.pem、*.crt、*.cer、または*.der である必要があります。 注意: “static.network.802_1x.mode” が2、3、4、5、6、または7 に設定されている場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	空白	

Web UI	ネットワーク > 高度な設定 > 802.1x > CA 証明書	
パラメータ	static.network.802_1x.client_cert_url ^[1]	<y0000000000xx>.cfg
説明	デバイス証明書のアクセスURL を設定します。証明書の形式は*.pem にする必要があります。 注意: "static.network.802_1x.mode" が2 (EAP-TLS) に設定されている場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	ネットワーク > 高度な設定 > 802.1x > デバイス証明書	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

プロキシサーバー

プロキシサーバーを使用するようにネットワークを設定できます。

- [プロキシサーバの設定](#)

プロキシサーバの設定

次の表に、プロキシサーバの設定に使用できるパラメータを示します。

パラメータ	static.network.proxy.mode ^[1]	<y0000000000xx>.cfg
説明	プロキシサーバーを有効または無効にします。	
許容値	0-無効 1-有効にすると、プロキシサーバー情報を手動で設定できます。	
デフォルト	0	
Web UI	ネットワーク > プロキシ > プロキシ(有線ネットワークのみ)	
電話機のUI	☰ > 設定 > デバイス設定 > プロキシ(デフォルトパスワード: admin) > プロキシ	
パラメータ	static.network.proxy.type	<y0000000000xx>.cfg
説明	プロキシタイプを設定します。 注意: "static.network.proxy.mode" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	0-Socks5 1-HTTP 接続	
デフォルト	0	
パラメータ	static.network.proxy.hostname	<y0000000000xx>.cfg
説明	プロキシサーバのIP アドレスまたはドメイン名を設定します。 注意: "static.network.proxy.mode" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	99文字以内の文字列	
デフォルト	空白	

Web UI	ネットワーク> プロキシ> プロキシホスト名(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシホスト名	
パラメータ	static.network.proxy.port ^[1]	<y0000000000xx>.cfg
説明	プロキシサーバのポートを設定します。 注意: "static.network.proxy.mode" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	1 ~ 65535 の整数	
デフォルト	空白	
Web UI	ネットワーク> プロキシ> プロキシポート(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシポート	
パラメータ	static.network.proxy.bypass_address	<y0000000000xx>.cfg
説明	アクセスするプロキシサーバに適用されないホスト名またはIP アドレスを設定します。 複数のホスト名またはIP アドレスは、カンマで区切ります。 注意: "static.network.proxy.mode" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	ネットワーク> プロキシ> プロキシサーバー使用しないアドレス(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシのバイパス	
パラメータ	static.network.proxy.test_address	<y0000000000xx>.cfg
説明	プロキシサーバのテストURL を設定します。 プロキシサーバに接続すると、電話機は指定されたURL にネットワーク要求を送信しようとします。URL にアクセスできない場合、電話機はプロキシサーバへの接続に失敗します。 注意: 「static.network.proxy.mode」が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	https://www.google.com	
Web UI	ネットワーク> プロキシ> テスト用プロキシドメイン名(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシ構成をテストするプロキシドメイン名	
パラメータ	static.network.proxy.enable	<y0000000000xx>.cfg
説明	プロキシサーバー認証を有効または無効にします。 注意: "static.network.proxy.mode" が1 (Enabled) に設定されている場合にのみ機能します。	

許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	ネットワーク> プロキシ> 認証の有効化	
電話機のUI	☰(その他)> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> 認証の有効化	
パラメータ	static.network.proxy.username ^[1]	<y0000000000xx>.cfg
説明	プロキシサーバ認証用のユーザ名を設定します。	
許容値	256 文字以内の文字列	
デフォルト	空白	
Web UI	ネットワーク> プロキシ> プロキシユーザー名(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシユーザー名	
パラメータ	static.network.proxy.password ^[1]	<y0000000000xx>.cfg
説明	プロキシサーバ認証のパスワードを設定します。	
許容値	256 文字以内の文字列	
デフォルト	空白	
Web UI	ネットワーク> プロキシ> プロキシパスワード(有線ネットワークのみ)	
電話機のUI	☰> 設定> デバイス設定> プロキシ(デフォルトパスワード: admin)> プロキシパスワード	
パラメータ	static.network.proxy.sip.enable	<y0000000000xx>.cfg
説明	プロキシサーバを使用するためのSIP を含むすべての通信を有効または無効にします。	
許容値	0-無効、SIP UDP およびアウトバウンドはプロキシサーバを使用しません。 1-有効	
デフォルト	0	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

デバイスプロビジョニング

この章では、プロビジョニングサーバーを使用してデバイスを設定するための基本的な手順について説明します。詳細については、『Yealink Teams HD IP Phones Auto Provisioning Guide』を参照してください。

- [考慮すべきプロビジョニングポイント](#)
- [起動ファイル、設定ファイル、リソースファイル](#)
- [プロビジョニング方法](#)
- [プロビジョニングサーバーのセットアップ](#)

考慮すべきプロビジョニングポイント

Microsoft Teams & Skype for Business Admin Center またはプロビジョニングサーバーを使用してデバイスをデプロイできます。

- Microsoft Teams & Skype for Business Admin Center でデバイスをプロビジョニングすると、企業内のデバイスの集中管理を効率的に実現できます。
- 環境にプロビジョニングサーバーがあり、一括デバイスを展開する場合は、一次構成方法として中央プロビジョニング方法を使用することをお勧めします。プロビジョニングサーバーは、デバイスをインストール、設定、アップグレード、および管理するときに柔軟性を最大化し、サーバーに設定を保存できるようにします。プロビジョニングサーバーは、ローカルエリアネットワーク(LAN)またはインターネット上の任意の場所にセットアップできます。

関連情報

[Microsoft Teams & Skype for Business Admin Center でのデバイスのプロビジョニング](#)

起動ファイル、設定ファイル、リソースファイル

起動ファイル、設定ファイル、およびリソースファイルを使用して、デバイスの機能を設定したり、デバイスに機能設定を適用したりできます。これらのファイルは、UltraEdit などのテキストエディタを使用して作成または編集できます。

テンプレートファイルについては、ディストリビュータまたはYealink FAE に問い合わせることができます。テンプレートファイルは <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage> から入手することもできます。

- [起動ファイル](#)
- [設定ファイル](#)
- [リソースファイル](#)
- [ファイルのダウンロードプロセス](#)


起動ファイル

Teamsデバイスは起動ファイルをサポートします。起動ファイルは、複数のデバイスの機能と設定をカスタマイズできるように柔軟性を最大限に高めます。

ブートファイルを使用すると、ダウンロードする設定ファイルを指定できます。さまざまな展開シナリオでデバイスをプロビジョニングすることが効果的です:

- すべてのデバイスについて
- デバイスのグループの場合
- 特定のデバイスモデルの場合
- 単一のデバイスの場合

Teamsデバイスは、共通ブートファイルとMAC 指向ブートファイルの2 種類のブートファイルをサポートします。デフォルトのブートテンプレートファイル「y000000000000.boot」を使用して、コピーを作成して名前を変更することで、MAC 指向ブートファイルを作成できます。

 **注意:** ブートファイルを使用するかどうかは、展開シナリオに応じて選択できます。ブートファイルを使用しない場合は、Configuration Files(設定ファイル)に進んでください。

- [共通ブートファイル](#)
- [MAC 指向ブートファイル](#)
- [起動ファイルの属性](#)
- [起動ファイルのカスタマイズ](#)


共通ブートファイル

y000000000000.boot という名前の共通ブートファイルは、すべてのデバイスに有効です。共通の起動ファイルを使用すると、単一のデバイスではなく、すべてのデバイスに共通の機能設定を適用できます。

MAC 指向ブートファイル

MAC 指向の起動ファイルの名前は<MAC>.boot です。特定のデバイスに対してのみ有効です。このように、デバイスごとに変更を行うことで、各デバイスを制御する権限が高くなります。

コピーを作成し、ブートテンプレートファイル(y000000000000.boot)の名前を変更することで、各デバイスのMAC 指向ブートファイルを作成できます。たとえば、デバイスのMAC アドレスが00156574B150 の場合、テンプレートファイルの名前を00156574b150 boot に変更します。(小文字)。


 ヒント: MAC アドレスは、固有の12桁のシリアル番号で、各デバイスに割り当てられます。デバイスの背面にあるバーコードから取得できます。

起動ファイルの属性

次の表に、ブートテンプレートファイルで知っておく必要がある属性を示します。

属性	説明
#!version:1.0.0.1	最初の行に配置する必要があります。編集や削除は行わないでください。
include:config<xxx.cfg>inc lude:config "xxx.cfg"	各"include"ステートメントは、構成ファイルの場所を指定できます。設定ファイルの形式は*.cfg にする必要があります。 山かっこまたは二重引用符で囲まれた場所は、次の2つの形式をサポートします: <ul style="list-style-type: none"> 相対パス(ブートファイルに対する相対パス): たとえば、sip.cfg、HTTP Directory/sip.cfg 絶対パス(またはURL): たとえば、http://10.2.5.258/Teams.cfgこの場所は、特定のCFG ファイルを指している必要があります。
[\$MODEL]	[\$MODEL]は、特定の電話機モデルの設定を指定するために追加できます。 \$MODEL は、電話機のモデル名を表します。 有効なデバイスモデル名は、MP58、MP56、MP54、T58A、T56A、T55A、CP960、VP59 です。 複数のデバイスモデルはカンマで区切られます。たとえば、[T58A, T56A] です。
overwrite_mode	上書きモードを有効または無効にします。上書きモードは、ブートファイルで指定された設定ファイルに適用されます。中央プロビジョニングによって事前にプロビジョニングされたパラメータにのみ影響することに注意してください。 1-(有効) - 設定ファイル内のパラメータの値が空白のままの場合、または設定ファイル内の非静的パラメータが削除またはコメントアウトされた場合、工場出荷時のデフォルト値が有効になります。 0:(無効)-設定ファイル内のパラメータの値が空白のまま、削除された、またはコメントアウトされた場合、事前設定された値が保持されます。 注記: 上書きモードは起動ファイルでのみ使用できます。ブートファイルが使用されているが、パラメータ"overwrite_mode" の値が設定されていない場合、上書きモードはデフォルトで有効になります。

属性	説明
特定モデル。excluded_mode	<p>除外モードを有効または無効にします。除外モードは、起動ファイルで指定された設定ファイルに適用されます。</p> <p>0-無効(追加モード)にすると、デバイスは独自のモデル固有の設定ファイルをダウンロードし、その他のモデル未指定の設定ファイルをダウンロードします。</p> <p>1-有効(除外モード)にすると、デバイスは独自のモデル固有のコンフィギュレーションファイルをダウンロードしようとします。サーバに独自のモデル固有のコンフィギュレーションファイルが見つからない場合は、モデル未指定のコンフィギュレーションファイルをダウンロードします。</p> <p>注記: 除外モードは起動ファイルでのみ使用できます。ブートファイルが使用されているが、パラメータ「specific_model.excluded_mode」の値が設定されていない場合、除外モードはデフォルトで無効になります。</p>

 ヒント: “#” で始まる行はコメントと見なされます。“#” を使用すると、ブートファイルに任意のコメントを作成できます。

起動ファイルのカスタマイズ

手順

1. 起動テンプレートファイルを開きます。
2. 設定ファイルを追加するには、ファイルにinclude:config <> またはinclude:config "" を追加します。それぞれが別々の行から始まります。
3. ダウンロードする設定ファイルを指定します。
次に例を示します。
 - include:config<configure/Teams.cfg>
 - include:config "http://10.2.5.206/configure/account.cfg"
 - include:config "http://10.2.5.206/configure/screensaver.cfg"
4. 特定の電話機モデルの設定ファイルを指定するには、include:config <> またはinclude:config "" の前に特定の電話機モデルを追加します。複数の電話機モデル名はカンマで区切られます。次に例を示します。
 - [T58A, CP960]include:config<configure/Teams.cfg>
 - [T56A]include:config "http://10.2.5.206/configure/account.cfg"
 - ## ファイルTeams.cfg はT58A およびCP960 電話機にのみ適用され、ファイルaccount.cfg はT56A 電話機にのみ適用されます。
5. 上書きモードと除外モードを指定します。次に例を示します。
 - overwrite_mode = 1
 - specific_model.excluded_mode = 1
6. 起動ファイルを保存し、プロビジョニングサーバーに配置します。

関連情報


[起動ファイルの属性](#)

設定ファイル

Yealink デバイスは、共通CFG ファイルとMAC 指向CFG ファイルの2 つの設定テンプレートファイルをサポートしています。これらの設定ファイルには、2 種類のパラメータが含まれています:

- Static: パラメータは、static.network.lldp.enable のように、プレフィックス「static.」で始まります。
- Non-static: パラメータはプレフィックス「static.」で始まりません(例: phone_setting.phone_lock.enable)。

プロビジョニングサーバーに保存されている設定ファイルを介して、一連のデバイスを自動的に展開および維持できます。

注:不正アクセスから保護するために、設定ファイルを暗号化できます。設定ファイルの暗号化の詳細については、「設定ファイルの暗号化」を参照してください。

- [共通CFGファイル](#)
- [MAC CFGファイル](#)
- [構成ファイルのカスタマイズ](#)

共通CFGファイル


共通のCFG ファイル<y0000000000xx>.cfg には、言語やボリュームなど、デバイスの基本動作に影響するパラメータが含まれています。同じ機種すべての機器に有効です。共通CFGファイルには、機器モデルごとに固定名称があります。

以下の表に、各デバイスモデルの共通CFG ファイルの名前を示します:

デバイスモデル	共通CFGファイル
T58A	y000000000058.cfg
T56A	y000000000056.cfg
T55A	y000000000099.cfg
CP960	y000000000073.cfg
VP59	y000000000091.cfg
MP58/MP58-WH	y000000000135.cfg
MP56	y000000000122.cfg
MP54	y000000000134.cfg

MAC CFGファイル

Yealink デバイスは、MAC 指向ファイルとMAC-local CFG ファイルの2 つのMAC CFG ファイルをサポートしています。これらは両方ともデバイスのMAC アドレスの名前です。たとえば、デバイスのMAC アドレスが00156574B150、MAC 指向CFG ファイルの名前は00156574b150.cfg(小文字)、MACローカルCFGファイルの名前は00156574b150-local.cfg(小文字)。

注記: MAC アドレスは、一意の12桁のシリアル番号で、各デバイスに割り当てられます。デバイス背面のバーコードから入手できます。

- [MAC 指向CFG ファイル](#)
- [MAC-local CFGファイル](#)

MAC 指向CFG ファイル


MAC 指向CFG ファイル。デバイスのMAC アドレスの名前が付けられます。たとえば、デバイスのMAC アドレスが00156574B150 の場合、MAC 指向CFG ファイルの名前は00156574b150.cfg です。(小文字)。アカウント登録など、特定のデバイスに固有のパラメータが含まれます。MAC 専用のデバイスにのみ有効です。

MAC-local CFGファイル

MAC-local CFG ファイル、<MAC>-local.cfg と名付けられています。Webユーザーインターフェースまたは電話ユーザーインターフェース(時間および日付形式の変更など)を介して行う静的でないパラメータに関連する変更。

MAC-local.cfg ファイルは、ファイルが更新されるたびにプロビジョニングサーバにアップロードされます。ファイルはWebユーザーインターフェースでダウンロードすることができます。

このファイルは、プロビジョニング優先度メカニズムを有効にした場合にのみ生成されます。このファイルはデバイスにローカルに保存され、ファイルが更新されるたびにプロビジョニングサーバにアップロードできます。このファイルを使用すると、デバイスがオートプロビジョニングを実行しても、ユーザーはパーソナライズされた設定を保持できます。

 注:プロビジョニングプライオリティメカニズムを有効にする前に行った非静的な変更は、生成されたMACローカルファイルに保存されませんが、以前の設定は引き続きデバイスで有効になります。静的変更は<MAC>-local.cfg に保存されません。ファイル。

プロビジョニングプライオリティメカニズムは、パラメータ
"static.auto_provision.custom.protect"によって有効になります。

- [MAC-local CFG ファイルの設定](#)
- [MAC-local CFG ファイルのクリア](#)

MAC-local CFG ファイルの設定

MAC-local CFG ファイルの生成に使用できるパラメータを次の表に示します。

パラメータ	static.auto_provision.custom.protect	<y0000000000xx>.cfg
説明	オートプロビジョニング後にユーザーの個人用設定を保持するために、デバイスを有効または無効にします。 注:プロビジョニングの優先順位メカニズム(電話ユーザーインターフェース/Webユーザーインターフェース> センtralプロビジョニング> 工場出荷時のデフォルト)は、このパラメータの値が1 (有効)に設定されている場合にのみ有効になります。ブートファイルで「overwrite_mode」が1 に設定されている場合、このパラメータの値は1 (有効)に設定されます。	
許容値	0-無効 1-有効、<MAC>-local.cfg ファイルが生成され、ウェブユーザーインターフェイスまたは電話ユーザーインターフェイスを介して設定されたパーソナライズされた非静的設定は、オートプロビジョニング後も保持されます。	
デフォルト	1	

MAC-local CFG ファイルのクリア

デバイスが新しいユーザに提供されても、最後のユーザによって設定された多数のパーソナライズされた設定がデバイスに保存されている場合、または設定が間違っているためにエンドユーザに何らかの問題が発生した場合は、ユーザのパーソナライズされた設定をクリアできます。

- パスの電話ユーザーインターフェースを介して: > Settings > Device Settings > Debug (デフォルトパスワード: admin) > Reset user settings.
- パスのWeb ユーザーインターフェースから、「設定」>「アップグレード」>「ユーザ設定のリセット」の順に選択します。

 注意: Reset user settings オプションは、“static.auto_provision.custom.protect = 1” を設定した場合

構成ファイルのカスタマイズ

コピーを作成し、設定テンプレートファイル(Teams.cfg、screensaver.cfg など) の名前を変更することで、いくつか

の新しいCFG ファイルを作成できます。設定テンプレートファイルのパラメータを再配置できます。

必要なパラメータを含む独自の設定ファイルを作成します。この柔軟性は、デバイスのグループに特定の設定を適用する場合に特に便利です。

- [設定ファイルのカスタマイズ](#)
- [設定ファイルの属性](#)

設定ファイルのカスタマイズ

手順

1. 設定テンプレートファイルをコピーして名前を変更します。たとえば、Teams.cfg です。
2. Teams.cfg のパラメータを再配置し、それらの有効な値を設定します。次に例を示し

ます。

```
phone_setting.phone_lock.enable= 1
```

```
screensaver.wait_time= 60
```

3. 特定の電話機モデルのパラメータを指定するには、対応するパラメータの前に特定の電話機モデルを追加します。異なる電話機モデルの名前はカンマで区切られます。

次に例を示します。

```
[T58A,CP960]phone_setting.phone_lock.enable= 1
```

```
[T58A]features.bluetooth_enable= 1
```


これらのパラメータは、独自の特定の電話機モデルにのみ適用されます。

4. 設定ファイルを保存し、プロビジョニングサーバに配置します。

設定ファイルの属性

次の表に、設定テンプレートファイルで知っておく必要がある属性を示します。

属性	説明
#!version:1.0.0.1	最初の行に配置する必要があります。編集や削除は行わないでください。
Configuration Parameter=Valid Value (screensaver.wait_time =60)	<p>特定の設定をデバイスに適用するためのパラメータと値を指定します。</p> <ul style="list-style-type: none"> • 各設定パラメータと値は等号で区切ります。 • 1 行に設定パラメータを1 つだけ設定 • 設定パラメータと値を同じ行に配置し、行を改行しないでください。
[\$MODEL]	<p>[\$MODEL] は、特定のデバイス・モデルの値を指定するために、構成パラメータの前に追加できます。\$MODEL は、電話機モデルを表します。</p> <p>有効なデバイスモデル名は、MP58、MP56、MP54、T58A、T56A、T55A、CP960、VP59 です。</p> <p>複数の電話機モデルはカンマで区切られます。たとえば、[T58A, CP960] です。</p> <p>注記: デバイスは、モデル固有の設定と、それらのモードで指定された設定を更新します。</p>

 ヒント: “#” で始まる行はコメントと見なされます。“#” を使用すると、ブートファイルに任意のコメントを作成できます。

リソースファイル

リソースファイルはオプションですが、特定の機能が採用されている場合は、これらのファイルが必要です。プロビジョニングサーバーにリソースファイルを配置する必要があります。デバイスは、オートプロビジョニング中に設定ファイルに加えてリソースファイルを要求します。

i ヒント: リソースファイルを使用する目的のデバイスを指定する場合は、リソースファイルのアクセスURLをMAC 指向CFG ファイルで指定する必要があります。オートプロビジョニング中、デバイスは設定ファイルに加えてリソースファイルを要求します。

- [対応リソースファイル](#)

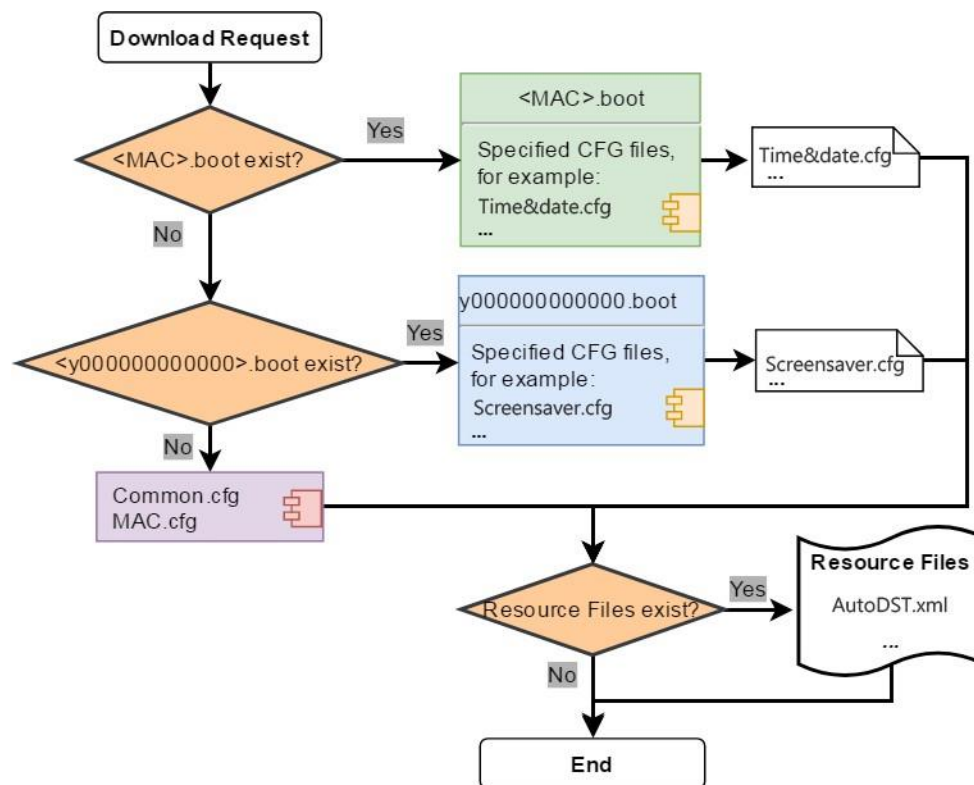
対応リソースファイル

Yealink は、必要に応じてファイルを直接編集できるように、リソースファイルのテンプレートをいくつか提供しています。次の表に、Yealinkのサプライ品のリソースファイルを示します:

テンプレートファイル	ファイル名	説明	セクションで参照する
AutoDST Template	AutoDST.xml	タイムゾーンとDST 設定を追加または変更します。	DST 設定
言語パック	たとえば、 000.GUI.English.lang1. English_note.xml1. English.js	表示する言語ファイルをカスタマイズする 電話/Web ユーザー インターフェイス。	言語のカスタマイズ

ファイルのダウンロードプロセス

デバイスをプロビジョニングすると、デバイスは次のフローチャートに従って、プロビジョニングサーバーから起動ファイル、設定ファイル、およびリソースファイルのダウンロードを要求します:



新しくダウンロードされた設定ファイルのパラメータは、以前にダウンロードされたファイルの同じパラメータをオーバーライドします。

注記: パラメータ「specific_model.excluded_mode」は、ダウンロードするブートファイルで参照される設定ファイルを決めます。

プロビジョニング方法

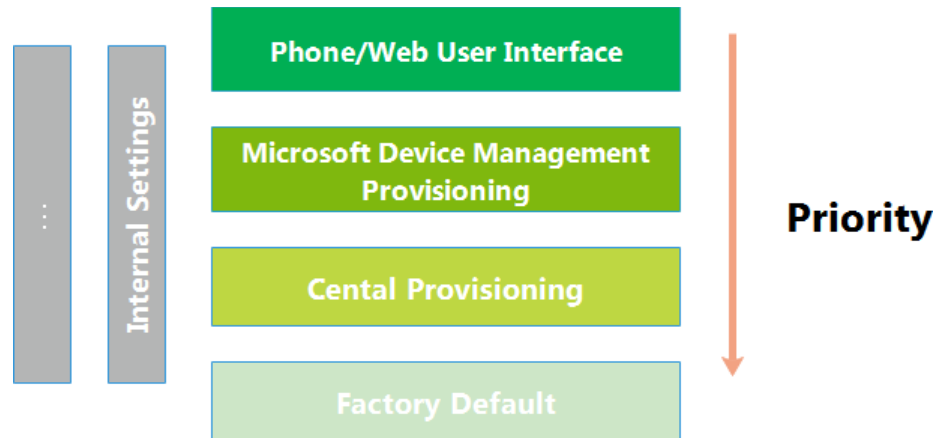
Teams デバイスは、プロビジョニングサーバーで次の方法を使用して設定できます：

- セントラルプロビジョニング: セントラルプロビジョニングサーバに保存された設定ファイル。
- 手動プロビジョニング: Web ユーザーインターフェイスまたは電話ユーザーインターフェイスでの操作。
- [プロビジョニング方法の優先順位](#)
- [手動プロビジョニング](#)
- [セントラルプロビジョニング](#)

プロビジョニング方法の優先順位

プロビジョニング方法の中には、設定の優先順位があります。優先順位の高いプロビジョニング方法を使用して行う設定は、優先順位の高いプロビジョニング方法を使用して行う設定よりも優先されます。

構成パラメーターの変更の優先順位は、次のとおりです(最高から最低):



注意: プロビジョニング優先順位のメカニズムは、「static.auto_provision.custom.protect」が1 に設定されている場合にのみ有効になります。このパラメータの詳細については、MACローカルCFGファイル設定を参照してください。

静的パラメータには優先順位はありません。プロビジョニングに使用している方法(Web ユーザーインターフェイスまたは電話ユーザーインターフェイスまたは設定ファイル)に関係なく有効になります。

静的パラメータは、プレフィックス「static.」で始まるパラメータです。たとえば、オートプロビジョニング/ネットワーク/syslog に関連付けられたパラメータや内部設定(プログラムの実行に使用される一時的な設定)などです。

関連情報

[Microsoft Teams & Skype for Business Admin Center でのデバイスのプロビジョニング](#)

手動プロビジョニング

この方法では、デバイスごとに設定変更を実行できます。

- [Webユーザー・インターフェイス・アクセス](#)
- [電話ユーザーインターフェイス](#)


Webユーザー・インターフェイス・アクセス

Web ユーザーインターフェイスを介してデバイスを設定する場合は、アクセス用のユーザー名とパスワードが必要です。管理者の場合、デフォルトのユーザー名とパスワードは「admin」(大文字と小文字が区別されます)、ユーザーの場合、デフォルトのユーザー名とパスワードは「user」(大文字と小文字が区別されます)です。

- [ウェブ・ユーザー・インターフェイスにアクセスする](#)
- [Webサーバタイプの構成](#)
- [CFG 設定ファイルのデバイスへのインポート](#)
- [デバイスからのCFG 設定ファイルのエクスポート](#)

ウェブ・ユーザー・インターフェイスにアクセスする

手順

1. 移動先  > 設定 > デバイス設定 > バージョン情報。
2. PC のWeb ブラウザのアドレスバーにデバイスのIP アドレスを入力します。
たとえば、IPv4 の場合: <http://192.168.0.10>または192.168.0.10、IPv6 の場合:
[http://\[2005:1:1:215:65ff:fe64:6e0a\]](http://[2005:1:1:215:65ff:fe64:6e0a]) または[2005:1:1:215:65ff:fe64:6e0a]

3. ユーザー名とパスワードを入力します。
4. ログインをクリックします。

Webサーバタイプの構成

Yealink Teams デバイスは、Web ユーザーインターフェイスにアクセスするためにHTTP とHTTPS の両方のプロトコルをサポートします。Webサーバタイプを設定できます。Webサーバタイプは、Webユーザーインターフェイスのアクセスプロトコルを決定します。HTTP/HTTPS プロトコルを使用してWeb ユーザーインターフェイスにアクセスすることを無効にすると、ユーザとユーザの両方がWeb ユーザーインターフェイスにアクセスできなくなります。

次の表に、Webサーバタイプの設定に使用できるパラメータを示します。

パラメータ	static.wui.http_enable ^[1]	<y0000000000xx>.cfg
説明	それは、ユーザーがHTTPプロトコルを使用してデバイスのウェブユーザーインターフェイスにアクセスすることを可能にするか、または無効にする。	
許容値	0-Disabled 1-Enabled	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > Web サーバ> HTTP	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> Web サーバ> HTTP ステータス	
パラメータ	static.network.port.http ^[1]	<y0000000000xx>.cfg
説明	ユーザーがHTTP プロトコルを使用してデバイスのWeb ユーザーインターフェイスにアクセスするためのHTTP ポートを設定します。	
許容値	1 ~ 65535 の整数	
デフォルト	80	
Web UI	ネットワーク> 高度な設定 > Web サーバ> HTTP ポート(1 ~ 65535)	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> Web サーバ> HTTPポート	
パラメータ	static.wui.https_enable ^[1]	<y0000000000xx>.cfg
説明	それは、ユーザーがHTTPSプロトコルを使用してデバイスのウェブユーザーインターフェイスにアクセスすることを可能にするか、または無効にする。	
許容値	0-Disabled 1-Enabled	
デフォルト	1	
Web UI	ネットワーク> 高度な設定 > Web サーバ> HTTPS	
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」)> Web サーバ> HTTPS ステータス	
パラメータ	static.network.port.https ^[1]	<y0000000000xx>.cfg
説明	ユーザがHTTPS プロトコルを使用してデバイスのWeb ユーザーインターフェイスにアクセスするためのHTTPS ポートを設定します。	

許容値	1 ～65535 の整数
デフォルト	443
Web UI	ネットワーク> 高度な設定 > Web サーバ> HTTPS ポート(1 ～65535)
電話機のUI	☰> 設定> デバイス設定> (管理者のみ(既定のパスワード: admin)>「ネットワーク」> Web サーバ> HTTPS ポート

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

CFG 設定ファイルのデバイスへのインポート

Webユーザーインターフェースを介して、現地からデバイスに構成ファイルをインポートすることができます。設定ファイルには、デバイス機能の変更が含まれており、これらの変更は設定ファイルがインポートされた直後に有効になります。

手順

1. Webユーザーインターフェースから、「設定」>「設定」>「CFG設定」に進みます。
2. 「CFG 設定ファイルのインポート」ブロックで、白いボックスをクリックして、ローカルシステムからCFG 設定ファイルを選択します。
3. インポートをクリックします。

デバイスからのCFG 設定ファイルのエクスポート

デバイスの設定ファイルをローカルにエクスポートし、デバイスの現在の機能設定を変更できます。これらの変更を、Webユーザーインターフェースを介してコンフィギュレーションファイルをインポートすることで、どのデバイスにも適用できます。

このタスクについて

5 種類のCFG 設定ファイルをローカルシステムにエクスポートできます:

- <MAC>-local.cfg:これには、電話機のユーザインターフェイスおよびWeb ユーザインターフェイスを介して行われた非静的パラメータに関連付けられた変更が含まれます。「static.auto_provision.custom.protect」が1 (Enabled) に設定されている場合にのみエクスポートできます。
- <MAC>-all.cfg:これには、電話機のユーザインターフェイス、Webユーザーインターフェイス、および設定ファイルを使用して行われたすべての変更が含まれます。
- <MAC>-static.cfg:静的設定(ネットワーク設定など)に関連するすべての変更が含まれます。
- <MAC>-non-static.cfg:電話機のユーザインターフェイス、Webユーザーインターフェイス、および設定ファイルを使用して行われた静的でないパラメータに関連するすべての変更が含まれます。
- <MAC>-config.cfg:これには、設定ファイルを使用して行われた静的でないパラメータに関連付けられた変更が含まれます。“static.auto_provision.custom.protect” が1 (Enabled) に設定されている場合にのみエクスポートできます。

手順

1. Webユーザーインターフェースから、「設定」>「設定/ログ」>「CFG設定」に進みます。
2. 「CFG 設定ファイルのエクスポート」ブロックで、「エクスポート」を選択してファイルのダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。

電話ユーザーインターフェイス

電話ユーザーインターフェイスを使用すると、ユーザと管理者が設定を使用できるようになりますが、

> 設定 ≡ Device Settings > Admin only(デバイス設定 > 管理者のみ)オプションは管理者のみが使用でき、

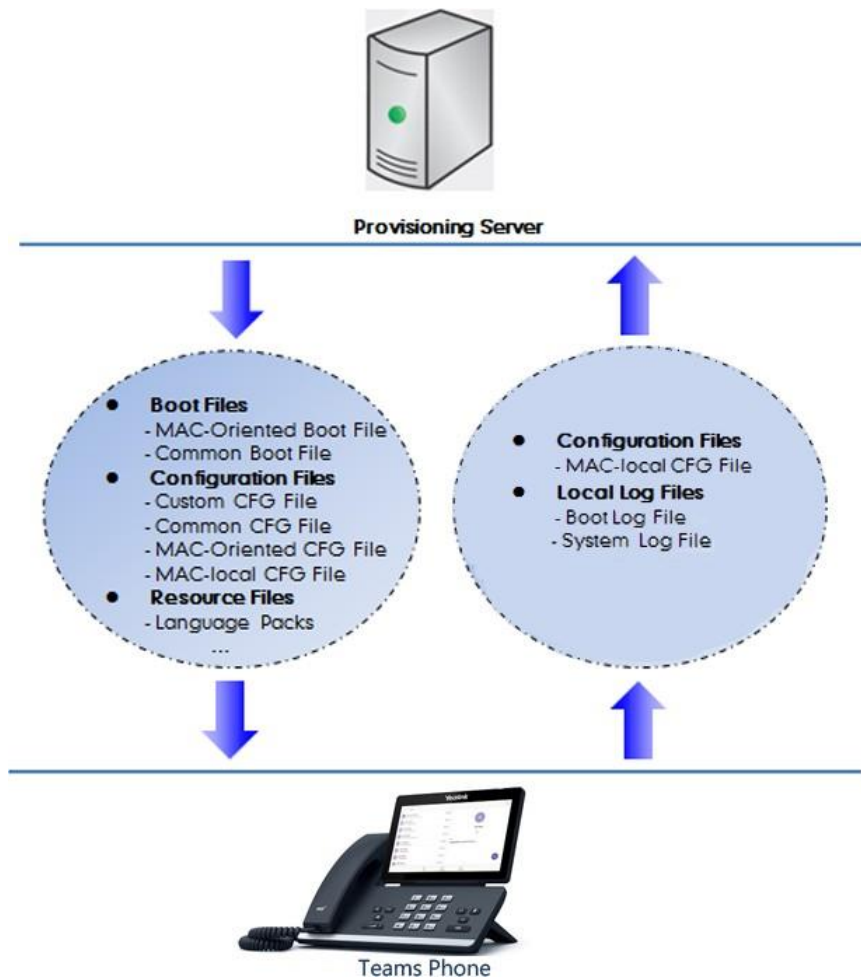
管理者パスワードが必要です(デフォルト: admin)。

デバイスは、デバイスごとに電話ユーザーインターフェイスを介して設定できます。

セントラルプロビジョニング

セントラルプロビジョニングを使用すると、設定したプロビジョニングサーバから複数のデバイスをプロビジョニングし、セントラルプロビジョニングサーバ内のすべてのデバイスの設定ファイルを維持できます。

次の図は、セントラルプロビジョニング方法を使用する場合に、デバイスがプロビジョニングサーバとどのように相互運用するかを示しています：



設定ファイルを使用してデバイスをプロビジョニングし、機能と設定を変更することを、セントラルプロビジョニング方式と呼びます。テキストベースの編集アプリケーションを使用して設定ファイルを編集し、設定ファイルをプロビジョニングサーバに保存できます。Teamsデバイスは、プロビジョニングサーバから一元的にプロビジョニングできます。プロビジョニングサーバの詳細については、「プロビジョニングサーバのセットアップ」を参照してください。

Teamsデバイスは、起動時にプロビジョニングサーバのアドレスを取得できます。次に、デバイスはプロビジョニングサーバから設定ファイルをダウンロードし、設定ファイルに書き込まれた設定を解決して更新します。このプロセス全体をオートプロビジョニングと呼びます。オートプロビジョニングの詳細については、『Yealink Teams HD IP Phones Auto Provisioning Guide』を参照してください。

- オートプロビジョニング設定の構成

オートプロビジョニング設定の構成

次の表に、オートプロビジョニングの設定に使用できるパラメータを示します。

パラメータ	static.network.attempt_expired_time ^[1]	<y0000000000xx>.cfg
説明	HTTP/HTTPS 接続用のファイルを転送するためのタイムアウト間隔(秒)を設定します。	
許容値	1 ~ 20 の整数	
デフォルト	10	
パラメータ	static.auto_provision.power_on	<y0000000000xx>.cfg
説明	電源投入時にオートプロビジョニングを実行するかどうかをデバイスに設定します。	
許容値	0-Off 1-オンにすると、デバイスはパワーオン時にオートプロビジョニングを実行します。	
デフォルト	1	
Web UI	設定> オートプロビジョニング> 電源オン	
パラメータ	静的。auto_provision.repeat.enable	<y0000000000xx>.cfg
説明	それは、オン/オフの繰り返しの特徴を引き起こす。	
許容値	0- Off 1-On	
デフォルト	0	
Web UI	設定> オートプロビジョニング> 繰り返し	
パラメータ	静的。auto_provision.repeat.minutes	<y0000000000xx>.cfg
説明	デバイスがオートプロビジョニングを繰り返し実行する間隔(分)を設定します。 注意: "static.auto_provision.repeat.enable" が1 (On) に設定されている場合にのみ機能します。	
許容値	1 ~ 43200 の整数	
デフォルト	1440	
Web UI	設定> オートプロビジョニング> 間隔(分)	
パラメータ	static.auto_provision.weekly.enable	<y0000000000xx>.cfg
説明	これにより、デバイスは毎週オートプロビジョニングを実行するようにトリガされます。	
許容値	0-Off 1-オンにすると、デバイスは毎週オートプロビジョニングプロセスを実行します。	
デフォルト	0	
Web UI	設定> オートプロビジョニング> 毎週	
パラメータ	static.auto_provision.weekly.dayofweek	<y0000000000xx>.cfg

説明	<p>デバイスが毎週オートプロビジョニングを実行する曜日を設定します。</p> <p>例: <code>static.auto_provision.weekly.dayofweek= 01</code></p> <p>つまり、デバイスは毎週日曜日と月曜日にオートプロビジョニング処理を実行します。</p> <p>注意: "<code>static.auto_provision.weekly.enable</code>" が1 (On) に設定されている場合にのみ機能します。</p>	
許容値	<p>0,1,2,3,4,5,6 またはこれらの数字の組み合わせ</p> <p>0-日曜</p> <p>1-月曜</p> <p>2-火曜日</p> <p>3-水曜日</p> <p>4-木曜日</p> <p>5-金曜日</p> <p>6-土曜日</p>	
デフォルト	0123456	
Web UI	設定> オートプロビジョニング> 曜日	
パラメータ	<code>static.auto_provision.weekly.begin_time</code> <code>static.auto_provision.weekly.end_time</code>	<y0000000000xx>.cfg
説明	<p>デバイスが毎週オートプロビジョニングを実行するための開始/終了時刻を設定します。</p> <p>注意: "<code>static.auto_provision.weekly.enable</code>" が1 (On) に設定されている場合にのみ機能します。</p>	
許容値	00:00 から23:59 までの時間	
デフォルト	00:00	
Web UI	設定> オートプロビジョニング> 時間	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

プロビジョニングサーバーのセットアップ


プロビジョニングサーバーを使用して、デバイスを設定できます。プロビジョニングサーバーにより、デバイスのアップグレード、メンテナンス、および設定を柔軟に行うことができます。構成ファイルは通常、このサーバー上にあります。

- [対応プロビジョニングプロトコル](#)
- [サポートされるプロビジョニングサーバー検出方法](#)
- [プロビジョニングサーバーの設定](#)

対応プロビジョニングプロトコル

Yealinkデバイスは、プロビジョニングのために複数のトランスポートプロトコルをサポートします:

- Trivial File Transfer Protocol (TFTP)
- ファイル転送プロトコル(FTP)
- Hyper Text Transfer Protocol – Secure (HTTPS)
- ファイル転送プロトコル– セキュア(FTPS)

 注意: FTP 方式には、アクティブとパッシブの2種類があります。デバイスはアクティブFTP と互換性はありません。

プロビジョニングサーバアドレス(http://xxxxxxxなど) でトランスポートプロトコルを指定できます。指定しない場合は、TFTPプロトコルを使用する。

サポートされるプロビジョニングサーバ検出方法

デバイスは、ネットワーク設定を確立した後、ソフトウェアのアップデートと設定を取得するためにプロビジョニングサーバを検出する必要があります。

デバイスは、プロビジョニングサーバアドレスを検出するために、次の方法をサポートします:

- DHCP: DHCP オプションを使用して、プロビジョニングサーバのアドレスまたはURL をデバイスに提供できます。デバイスがDHCP プロトコルを使用してIP アドレスを要求する場合、結果の応答には、プロビジョニングサーバアドレスを含むオプション66 (IPv4 の場合) またはカスタムオプション(設定されている場合) が含まれることがあります。
- 静的: 電話のユーザインターフェイスまたはWeb ユーザインターフェイスを介して、サーバアドレスを手動で設定できます。
- [DHCP プロビジョニング設定](#)
- [静的プロビジョニング設定](#)

DHCP プロビジョニング設定

ネットワーク環境に応じて、IPv4 またはカスタムDHCP オプションの使用を選択できます。IPv4 またはカスタムDHCP オプションは、DHCP サーバで定義されているものに従っている必要があります。

次の表に、DHCP プロビジョニングの設定に使用できるパラメータを示します。


パラメータ	static.auto_provision.dhcp_option.enable	<y0000000000xx>.cfg
説明	これにより、DHCP 有効機能のオン/オフがトリガされます。	
許容値	0-Off 1-オンにすると、デバイスはDHCPオプションを検出してプロビジョニングサーバアドレスを取得します。	
デフォルト	1	
Web UI	設定> オートプロビジョニング> DHCP 有効	
パラメータ	static.auto_provision.dhcp_option.list_user_option	<y0000000000xx>.cfg
説明	プロビジョニングサーバアドレスを要求するためのカスタムDHCP オプションを設定します。複数のDHCP オプションはカンマで区切ります。 注意: "static.auto_provision.dhcp_option.enable" が1 (On) に設定されている場合にのみ機能します。	
許容値	128 ~254 の整数	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> カスタムオプション	

静的プロビジョニング設定

静的プロビジョニング方法を使用するには、プロビジョニングサーバを設定するときに、最初にプロビジョニング

サーバーアドレスを取得する必要があります。

プロビジョニングサーバーのアドレスには、IP アドレス、ドメイン名、またはURL を指定できます。ユーザー名とパスワードがプロビジョニングサーバーアドレスの一部として指定されている場合、たとえば、サーバーがサポートしている場合にのみhttp://user:pwd@server/dir,が使用されます。

 注意: URL には、バックスラッシュの代わりにスラッシュを含める必要があり、スペースを含めることはできません。エスケープ文字はサポートされません。

プロビジョニングサーバーアドレスの一部としてユーザー名とパスワードが指定されていない場合は、デバイスに設定されているプロビジョニングサーバーのユーザー名とパスワードが使用されます。

次の表に、静的プロビジョニングの設定に使用できるパラメータを示します。


パラメータ	static.auto_provision.server.url	<y0000000000xx>.cfg
説明	プロビジョニングサーバーのアクセスURL を設定します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> サーバーURL	
パラメータ	static.auto_provision.server.username	<y0000000000xx>.cfg
説明	サーバアクセスをプロビジョニングするためのユーザ名を設定します。	
許容値	32文字以内の文字列	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> ユーザー名	
パラメータ	static.auto_provision.server.password	<y0000000000xx>.cfg
説明	サーバアクセスをプロビジョニングするためのパスワードを設定します。	
許容値	32文字以内の文字列	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> パスワード	

プロビジョニングサーバーの設定

プロビジョニングサーバーは、ローカルLAN またはインターネット上の任意の場所にセットアップできます。これが最初のプロビジョニングサーバーのセットアップである場合は、推奨事項として次の手順を使用します。


手順

1. プロビジョニングサーバーアプリケーションをインストールするか、3CDaemon などの適切な既存のサーバーを見つけます。
2. アカウントとホームディレクトリを作成します。
3. アカウントのセキュリティ権限を設定します。
4. ブートファイルと設定ファイルを作成し、必要に応じて編集します。
5. 起動ファイル、設定ファイル、およびリソースファイルをプロビジョニングサーバーにコピーします。
6. 静的プロビジョニングを実行する場合は、プロビジョニングサーバーのアドレスを取得します。

 ヒント: 通常、すべてのデバイスは同じサーバアカウントで設定されますが、サーバアカウントは設定を便利にパーティション化する手段を提供します。各アカウントにサーバー上の一意のホームディレクトリを与え、設定を行単位で変更します。

Microsoft Teams & Skype for Business Admin Center でのデバイスのプロビジョニング

Microsoft Teams & Skype for Business Admin Centerにより、管理者はYealink Teamsデバイスの集中管理を効率的に実現できます。デバイス管理プラットフォームでは、構成プロファイルのカスタマイズし、使用されるすべてのデバイスを更新できます。

注: 管理できるのは、Microsoft Teams & Skype for Business Admin Center サービスを開いたオンラインアカウントでログインしたデバイスのみです。

- [デバイス管理](#)
- [構成プロファイル管理](#)

デバイス管理

デバイスは、Microsoft Teams & Skype for Business Admin Center で直接監視および管理できます。

- [デバイス情報の編集](#)
- [デバイスの表示要素のカスタマイズ](#)
- [デバイスの詳細の表示](#)
- [デバイスへの設定プロファイルの割り当て](#)
- [診断デバイス](#)
- [デバイスソフトウェアのアップデート](#)
- [デバイスの再起動](#)

デバイス情報の編集

デバイス名、組織アセットタグを編集したり、デバイスのメモを追加したりできます。一度に編集できるデバイスは1つだけです。


手順

1. デバイス > デバイスの管理 > すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで目的のデバイスをクリックします。
3. デバイスリストの左上にある「編集」をクリックします。
4. ポップアップメニューの右側からデバイス情報を編集します。
5. 保存をクリックします。

デバイスの表示要素のカスタマイズ

デバイスリストに表示されるテーブル要素をカスタマイズできます。

手順

1. デバイス > デバイスの管理 > すべてのデバイスと移動します。
2.  デバイスリストの右上に。
3. テーブル要素をオンまたはオフにします。
4. 保存をクリックします。

デバイスの詳細の表示

デバイスの基本情報、アップデート情報、ソフトウェアアップデートステータス、および実行したアクションを表示できます。

手順

1. デバイス> デバイスの管理> すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで対応するデバイス名をクリックして、デバイスの詳細ページを入力します。
明細(詳細)をクリックしてソフトウェアアップデートのステータスを表示するか、History(履歴)をクリックして、デバイスに対して実行したアクションを表示できます。

デバイスへの設定プロファイルの割り当て

デバイスに設定プロファイルを割り当てる前に、プラットフォームに設定プロファイルがあることを確認してください。

手順

1. デバイス> デバイスの管理> すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで目的のデバイスをクリックします。
3. デバイスリストの左上にある「Assign configuration」をクリックします。
4. ポップアップメニューの右側から構成プロファイルを検索します。
5. 保存をクリックします。
構成プロファイルはデバイスで有効になります。

関連タスク

[構成プロファイルの作成](#)

診断デバイス

診断機能を使用すると、問題の根本原因をすばやく見つけて、問題のトラブルシューティングを行うことができます。診断デバイスの後、診断ファイルをダウンロードして確認する必要があります。

手順

1. デバイス> デバイスの管理> すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで目的のデバイスをクリックします。
3. デバイスリストの上部にある Diagnostics(診断)をクリックします。
「Log files will retrieved from the selected device(s). Wold you wall to proceed?」と表示されます。
4. Proceed をクリックします。
ログファイルは、正常に診断されると、選択したデバイスから取得されます。
5. 「すべてのデバイス」リストで対応するデバイス名をクリックして、デバイスの詳細ページを入力します。
6. 履歴を選択し、ダウンロードをクリックしてログファイルをダウンロードします。

デバイスソフトウェアのアップデート

デバイスのすべてのソフトウェアを最新バージョンに更新するには、Microsoft Teams & Skype for Business Admin Center をワンクリックします。

このタスクについて

選択したデバイス上のすべてのソフトウェアがアップデートされます。

手順

1. デバイス> デバイスの管理> すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで目的のデバイスをクリックします。
3. デバイスリストの上部にある「更新」をクリックします。
「選択したデバイスのすべてのソフトウェアが最新バージョンにアップデートされます。続行しますか?」と表示されます。
4. とにかく更新をクリックします。
デバイスの現在のファームウェアは、数分後に自動的に更新されます。


デバイスの再起動

手順

1. デバイス> デバイスの管理> すべてのデバイスと移動します。
2. 「すべてのデバイス」リストで目的のデバイスをクリックします。
3. デバイスリストの上部にある「再起動」をクリックします。
「選択したデバイスが再起動します。続行しますか?」と表示されます。
4. とにかく再起動をクリックします。
デバイスが再起動されます。

構成プロファイル管理

デバイスは、設定プロファイルを使用して設定できます。構成プロファイルは、デバイスを管理するための一般設定、デバイス設定、およびネットワーク設定を提供します。これにより、集中型デバイス配置を簡単に実現できます。すべての設定は、プロファイルの展開設定に従ってデバイスに送信されます。デバイスでサポートされていない設定は、デバイスにプッシュされません。

 **メモ:** 言語設定では、英語(米国)、中国語_S(簡体字、PRC)、中国語_T(繁体字、台湾)、フランス語(フランス)、ドイツ語、イタリア語、ポーランド語、ポルトガル語(ポルトガル語)、スペイン語、トルコ語、ロシア語、オランダ語、およびJapanese のみがデバイスでサポートされます。他の言語を選択した場合、言語設定は有効になりません。

- [構成プロファイルの作成](#)
- [構成プロファイルの編集](#)
- [デバイスへの設定プロファイルの割り当て](#)

関連情報

[言語](#)

構成プロファイルの作成

手順

1. デバイス> デバイスの管理> 構成プロファイルと移動します。
2. 構成プロファイルリストの左上にある「新規構成プロファイル」をクリックします。
3. 構成プロファイルの名前と説明を編集します。
4. 一般設定、機器設定、ネットワーク設定を行います。
デバイスの電話ロック機能を有効にすると、ユーザーは無効にできません。
5. 保存をクリックします。

構成プロファイルの編集

設定ファイルの名前、説明、および設定を編集できます。

手順

1. デバイス> デバイスの管理> 構成プロファイルと移動します。
2. 「構成ファイル」リストで目的の構成ファイルをクリックします。
3. 構成プロファイルリストの左上にある「編集」をクリックします。
4. 構成プロファイルを編集します。
5. 保存をクリックします。

デバイスへの設定プロファイルの割り当て


手順


1. デバイス> デバイスの管理> 構成プロファイルと移動します。
2. 「構成ファイル」リストで目的の構成ファイルをクリックします。
3. 設定プロファイルリストの上部にある「デバイスに割り当てる」をクリックします。
4. ポップアップメニューの右側からデバイスを検索します。
5. 保存をクリックします。
構成プロファイルはデバイスで有効になります。

ファームウェアアップグレード

ファームウェアアップグレードには3つの方法があります:

- 手動で、Webユーザーインターフェースを介して、単一デバイスのローカルシステムから。
- 大量のデバイスのプロビジョニングサーバーから自動的に。
- Microsoft Teams & Skype for Business Admin Center を1 回クリックして、すべてのデバイスソフトウェアを最新バージョンにアップグレードします。これは、Teams ファームウェアを実行しているデバイスにのみ適用されます。

 注: 最新のファームウェアを実行しているデバイスを以前のファームウェアバージョンにダウングレードしないことをお勧めします。新しいファームウェアは古い設定パラメータと互換性がありますが、その逆はありません。

 注意: T58A/T56A Teams デバイスの場合、ファームウェアを58.15.0.20 から58.15.0.41 (またはそれ以降) にアップグレードする場合は、最初に58.15.0.26 にアップグレードしてから、ファームウェアを58.15.0.41 (またはそれ以降) にアップグレードする必要があります。

- [各デバイスモデルのファームウェア](#)
- [ファームウェアアップグレードの設定](#)

関連タスク

[デバイスソフトウェアのアップデート](#)

各デバイスモデルのファームウェア

最新のファームウェアは、<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage> からダウンロードできます。

次の表に、各デバイスモデルの関連するファームウェア名と最新のファームウェア名を示します(X は実際のファー

ムウェアバージョンに置き換えられます)。

デバイスモデル	関連ファームウェア名	ファームウェア名
T58A/T56A/T55A	58. x.x.x.rom	58.15.0.118.rom
CP960	73. x.x.x.rom	73.15.0.111.rom
VP59	91. x.x.x.rom	91.15.0.40.rom
MP58/MP58-WH/MP56/ MP54	122. x.x.x.rom	122.15.0.27.rom

ファームウェアアップグレードの設定

ファームウェアをアップグレードする前に、以下を知っておく必要があります:

- デバイスがWeb ユーザーインターフェイスを介してファームウェアをアップグレードしているときに、ブラウザを閉じて更新しないでください。
- デバイスがファームウェアをアップグレードしているときは、ネットワーク・ケーブルと電源ケーブルを抜かないでください。次の表に、ファームウェアのアップグレードに使用できるパラメータを示します。

パラメータ	static.firmware.url ^[1]	<y0000000000xx>.cfg
説明	ファームウェアファイルのアクセスURL を設定します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	設定> アップグレード> ファームウェア更新	
パラメータ	over_the_air.url.bth58	<y0000000000xx>.cfg
説明	BTH58 ハンドセットのファームウェアファイルのアクセスURL を設定します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	設定> アップグレード> ファームウェア更新	

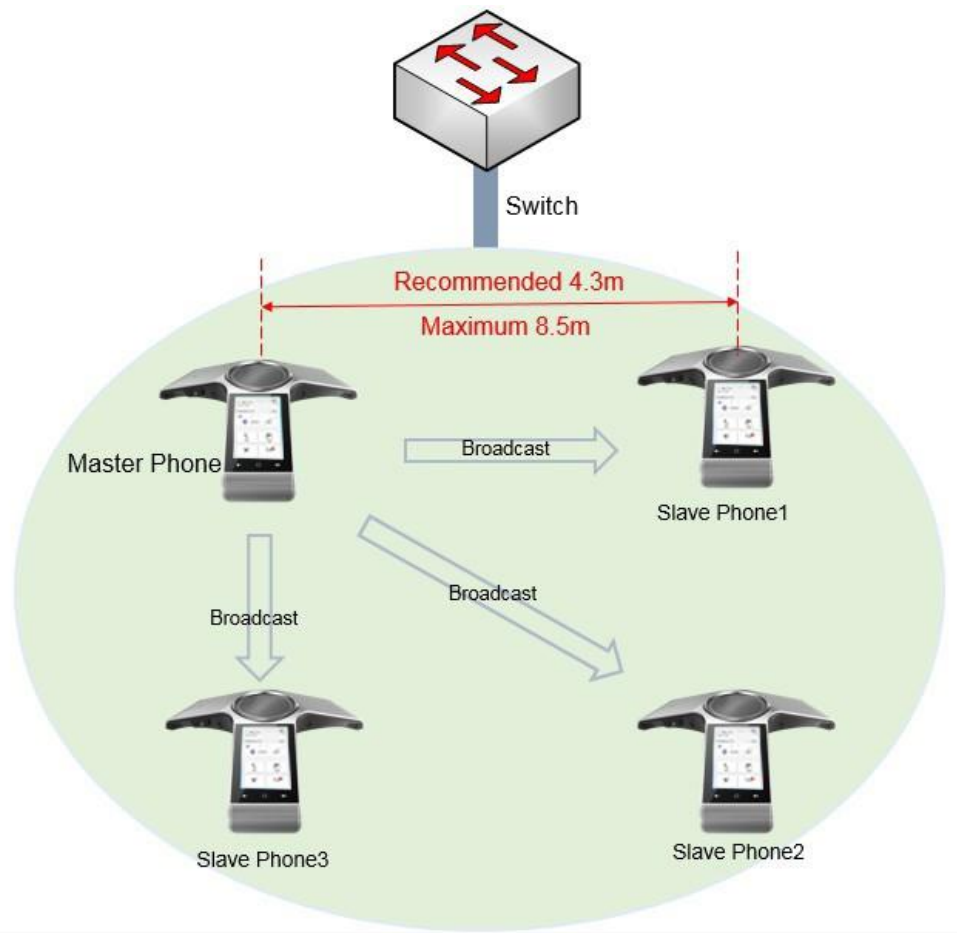
^[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

CP960 スター接続機能の使用

大規模な会議室では、最大4 台のCP960 会議電話をスターレイアウトで展開できます。1 台はマスター電話、もう1 台はスレーブ電話です。マスタ電話機はすべての機能を保持しますが、スレーブ電話機はDND やコールミュートなど、マスタ電話機の一部の主要機能のみを同期します。接続後、主にスレーブフォンをスピーカーやマイクとして使用します。

この機能により、ユーザはマスターフォンまたはスレーブフォンのいずれかでコールを制御できます。また、会議室から離れた場所にいる場合でも、すべての参加者が相手を明確に聞くことができます。

スター接続グループの設定例を次に示します:



- [スター接続機能の設定ガイドライン](#)
- [CP960 スター接続機能の設定](#)
- [例: CP960 スター接続機能の設定](#)

スター接続機能の設定ガイドライン

CP960 のスター接続機能を設定する場合は、以下の手順を知っておく必要があります:

- すべての電話機が同じサブネットに展開されていることを確認します。
- すべての電話機で同じファームウェアバージョンが実行されていることを確認します。
- CP960 電話機は、有線ネットワークのスターレイアウトでのみ展開できます。
- マスターフォンがブロードキャストステータスでない場合、スレーブフォンは再起動後に自動的に再接続されません。
- スレーブ電話機は、壁紙やコンタクトアバターなど、マスター電話機の一部のカスタム機能を同期できません。
- スレーブ電話機のWeb ユーザーインターフェイスにアクセスすることはできません。
- マスター電話機のWeb ユーザーインターフェイスを介してファームウェアをアップグレードすると、マスター電話機のみがアップグレードされます。アップグレード後、ファームウェアバージョンが異なるため、スレーブ電話機はマスター電話機から切断されます。
- オートプロビジョニング経由でファームウェアをアップグレードすると、マスター電話機とスレーブ電話機の両方がアップグレードされます。

CP960 スター接続機能の設定

次の表に、CP960 スター接続機能の設定に使用できるパラメータを示します。

パラメータ	features.cp_star_connection.master.enable	<y0000000000xx>.cfg
説明	電話機をマスタ電話機にするかどうかを指定します。	
許容値	0- マスターフォンではない 1- マスターフォンでは、自動的に4桁のPIN番号が生成され、ブロードキャストが送信されます。ユーザは、電話機にスター接続グループを手動で作成する必要はありません。	
デフォルト	0	
電話機のUI	☰> 設定> デバイス設定> 管理者のみ(デフォルトパスワード: admin)> CPスター接続> グループの作成	
パラメータ	features.cp_star_connection.slave.X. mac ^[1]	<y0000000000xx>.cfg
許容値	マスタ電話機のスレーブ電話機のMAC アドレスを指定します。 設定後、このMAC アドレスを持つ電話機は、マスタ電話機との接続を許可されます。 例: features.cp_star_connection.slave.1.mac = 805EC0092F4B MAC アドレスは大文字と小文字が区別されず、MAC アドレスの形式80:5E:C0:09:2F:4B が無効であることに注意してください。 注意: "features.cp_star_connection.master.enable" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	MACアドレス	
デフォルト	空白	
パラメータ	features.cp_star_connection.master.mac ^[2]	<y0000000000xx>.cfg
説明	スレーブ電話機のマスタ電話機のMAC アドレスを指定します。 設定後、電話機はマスター電話機によって作成されたスター接続グループにこのMAC アドレスで参加できます。 例: features.cp_star_connection.master.mac=805EC0092F33 MAC アドレスは大文字と小文字が区別されず、MAC アドレスの形式80:5E:C0:09:2F:4B が無効であることに注意してください。 注意: "features.cp_star_connection.master.enable" が0 (Disabled)に設定されていて、電話機がマスタ電話機から接続を許可されている場合にのみ機能します。	
許容値	MACアドレス	
デフォルト	空白	

[1]X X はスレーブ電話機ID です。X = 1-3。

[2]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

関連情報

例: CP960 スター接続機能の設定

例: CP960 スター接続機能の設定

シナリオ条件

電話機A のMAC アドレスは805EC0092F33 です。電

話機B のMAC アドレスは805EC0092F4B です。電話

機C のMAC アドレスは805EC009223B です。電話機

D のMAC アドレスは805EC0033E2B です。

すべての電話機が同じサブネットにあり、同じファームウェアバージョンを実行しています。

電話機A をマスター電話機として動作させ、電話機B、電話機C、電話機D をスレーブ電話機として動作させます。

次の例は、電話機の設定を示しています:

例

#####電話機A(マスター電話機)の場合#####

```
features.cp_star_connection.master.enable=1 cp_star_connection.sla
```

```
ve.1.mac=805EC0092F4B
```

```
features.cp_star_connection.slave.2.mac=805EC009223B
```

```
features.cp_star_connection.slave.3.mac=805EC0033E2B #####電
```

```
話機B、C、D (スレーブ電話機)#####
```

```
features.cp_star_connection.master.enable=0features.cp_star_conn
```

```
ection.master.mac=805EC0092F33再起動後、電話機A、B、C、D
```

はスター接続グループになります。

デバイスのカスタマイズ

さまざまな設定をカスタマイズすることで、Teams デバイスをよりパーソナライズできます。

- [言語](#)
- [スクリーンセーバー](#)
- [バックライト](#)
- [日時](#)
- [音色](#)
- [ボリューム](#)
- [省電力](#)
- [電源LEDインジケータ](#)
- [ブルートゥース](#)

言語

Teamsデバイスは複数の言語をサポートします。電話のユーザーインターフェースおよびウェブユーザーインターフェースで使用する言語は、それぞれ必要に応じて指定することができます。

言語パックについては、代理店またはYealink FAE にお問い合わせください。言語パックは、
<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>から入手することもできます。

次の表に、電話機のユーザインターフェイスとWebユーザインターフェイスでサポートされる使用可能な言語と関連する言語パックを示します。

電話ユーザインターフェイス/エンドポイント		Webユーザーインターフェイス		
言語	言語パック	言語	言語パック	メモ言語パック
英語	000. GUI.English.lang	英語	1. English.js	1. English_note.xml
中国語簡体字	001. GUI.Chinese_S.lang	中国語簡体字	2. Chinese_S.js	2. Chinese_S_note.xml
繁体字中国語	002. GUI.Chinese_T.lang	繁体字中国語	3. Chinese_T.js	3. Chinese_T_note.xml
フランス語	003. GUI.French.lang	フランス語	4. French.js	4. French_note.xml
ドイツ語	004. GUI.German.lang	ドイツ語	5. German.js	5. German_note.xml
イタリア語	005. GUI.Italian.lang	イタリア語	6. Italian.js	6. Italian_note.xml
ポーランド語	006. GUI.Polish.lang	ポーランド語	7. Polish.js	7. Polish_note.xml
ポルトガル語	007. GUI.Portuguese.lang	ポルトガル語	8. Portuguese.js	8. Portuguese_note.xml
スペイン語	008. GUI.Spanish.lang	スペイン語	9. Spanish.js	9. Spanish_note.xml
トルコ語	009. GUI.Turkish.lang	トルコ語	10. Turkish.js	10. Turkish_note.xml
ロシア語	010. GUI.Russian.lang	ロシア語	11. Russian.js	11. Russian_note.xml
オランダ	011. GUI.Netherlands.lang	オランダ	12. Netherlands.js	12. Netherlands_note.xml
日本語	012. GUI.Japanese.lang	日本語	13. Japanese.js	13. Japanese_note.xml

- [言語表示設定](#)
- [言語のカスタマイズ](#)
- [例: デバイス表示のカスタム言語の設定](#)

言語表示設定

電話機のユーザーインターフェイスに表示されるデフォルトの言語は、起動時にユーザーが選択した言語によって異なります。Webブラウザに、デバイスがサポートしていない言語が表示されている場合、Webユーザーインターフェイスには、デフォルトで英語が表示されます。電話のユーザーインターフェイスとWebユーザーインターフェイスの言語をそれぞれ指定できます。

次の表に、言語表示の設定に使用できるパラメータを示します。


パラメータ	lang.gui	<y0000000000xx>.cfg
説明	デバイスに表示する言語を設定します。	
許容値	英語、中国語_S、中国語_T、フランス語、ドイツ語、イタリア語、ポーランド語、ポルトガル語、スペイン語、トルコ語、ロシア語、オランダ語、日本語、またはカスタム言語名。	
デフォルト	英語	

電話機のUI	☰ > 設定 > デバイス設定 > 言語 一般電話の場合: > 設定 > デバイス設定 > 言語(デフォルトパスワード: admin)☰	
パラメータ	lang.wui	<y0000000000xx>.cfg
説明	それは、ウェブユーザー・インターフェース上に表示する言語を設定する。	
許容値	英語、中国語_S、中国語_T、フランス語、ドイツ語、イタリア語、ポーランド語、ポルトガル語、スペイン語、トルコ語、ロシア語、オランダ語、日本語、またはカスタム言語名。	
デフォルト	英語	
Web UI	Webユーザー・インターフェースの右上隅に	

言語のカスタマイズ

電話機のユーザーインターフェイスまたはWeb ユーザーインターフェイスに表示する言語ファイルのカスタマイズできます。

言語パックについては、代理店またはYealink FAE に問い合わせることができます。言語パックは、<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>から入手することもできます。

 注記: 新しく追加された言語は、デバイス上のフォントライブラリでサポートされている必要があります。カスタム言語ファイルの文字がデバイスでサポートされていない場合、デバイスには代わりに「?」が表示されます。

- [デバイス表示カスタマイズ用言語](#)
- [Web Display カスタマイズの言語](#)

デバイス表示カスタマイズ用言語

使用可能な言語は、デバイスに現在ロードされている言語パックによって異なります。また、デバイスに言語パックをロードすることで、デバイス表示に使用できる新しい言語(使用可能な言語リストには含まれていません)を追加することもできます。

- [デバイス表示用の言語パックのカスタマイズ](#)
- [デバイス表示設定のカスタム言語](#)

デバイス表示用の言語パックのカスタマイズ

電話機のユーザーインターフェイス用に新しい言語パックを追加する場合は、言語パックを「X.GUI.name.lang」としてフォーマットする必要があります(X は012 から始まり、「name」は言語名に置き換えられます)。言語名が既存のものと同じ場合、既存の言語パックは新しくアップロードされたものによって上書きされます。新しい言語パックのファイル名は既存のものと同じにしないことをお勧めします。

 注意: 言語ファイルを変更するには、言語パックの名前を変更しないでください。

1. 目的の言語テンプレートファイル(000.GUI.English.lang など)を開きます。

2. 等号の右側の二重引用符内の文字を変更します。等号の左側の項目は変更しないでください。

以下に、電話機のユーザインタフェースの言語パック“000.GUI.English.lang”の一部を示します:

```

000.GUI.English.lang x
1 [Lang]
2 Name=English
3 FONT=Tahoma
4
5 [Translate]
6
7 " is offline"=" is offline"
8 " s"=" s"
9 "#"="#"
10 "(Empty)"="(Empty)"
11 "(No Name)"="(No Name)"
12 "*"="*"
13 "<New Item>"="<New Item>"
14 "0s"="0s"
15 "102s"="102s"
16 "108s"="108s"
17 "114s"="114s"
18 "12 Hour"="12 Hour"
19 "120s"="120s"
20 "12s"="12s"
21 "15s"="15s"
22 "1800s"="1800s"
23 "18s"="18s"
24 "24 Hour"="24 Hour"
25 "24s"="24s"
26 "300s"="300s"
27 "30s"="30s"
28 "36s"="36s"
29 "3rd-party VMR"="Third-party VMR"
30 "42s"="42s"
31 "48s"="48s"
32 "54s"="54s"
33 "600s"="600s"
34 "60s"="60s"
35 "66s"="66s"
36 "6s"="6s"
    
```

Do not modify the item on the left of equal sign.

Modify the item (e.g., Key As Send).

3. 言語パックを保存し、プロビジョニングサーバに配置します。


デバイス表示設定のカスタム言語

次の表に、デバイスディスプレイのカスタム言語を設定するために使用リストパラメータを示します。

パラメータ	gui_lang.url	<y0000000000xx>.cfg
説明	電話ユーザインタフェースのカスタム言語パックのアクセスURLを設定します。 複数の言語パックを同時にデバイスにダウンロードすることもできます。	
許容値	511文字以内のURL	
デフォルト	空白	
パラメータ	gui_lang.delete	<y0000000000xx>.cfg
説明	電話ユーザインタフェースの指定された言語パックまたはすべてのカスタム言語パックが削除されます。	

許容値	http://localhost/allまたはX.GUI.name.lang X 012 から始まり、“name” は言語名に置き換えられます。
デフォルト	空白

Web Display カスタマイズの言語

言語ファイルを変更したり、Web 表示用の新しい言語を追加したりできます。ノート言語パックをカスタマイズすることもできます。アイコンに音符情報が表示されます。  ウェブ・ユーザー・インターフェースの。

- Web 表示用の言語パックのカスタマイズ
- ノート表示用の言語パックのカスタマイズ
- Web およびノート表示設定のカスタム言語

Web 表示用の言語パックのカスタマイズ

Webユーザーインターフェースに新しい言語パックを追加する場合、言語パックは「X.name.js」として形式化する必要があります(Xは13から始まります)。「name」は言語名に置き換えられます。言語名が既存のものと同じ場合、新しくアップロードされた言語ファイルは既存のものをオーバーライドします。新しい言語パックのファイル名は既存のものと同じにしないことをお勧めします。

 注意: 言語ファイルを変更するには、言語パックの名前を変更しないでください。

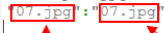

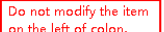
1. ASCIIエディタを使用して、必要な言語テンプレートパック(例:1.English.js)を開きます。
2. コロンの右側の二重引用符内の文字を変更します。コロンの左側の変換項目は変更しないでください。

Webユーザーインターフェース用言語パック「1.English.js」の一部を以下に示します:

```

0 .....10 .....20 .....30 .....40 .....50 .....
1  var _objTrans =
2  {
3  {
4    " Call Number Filter":"Call Number Filter",
5    " Distinctive Ring Tones":"Distinctive Ring Tones",
6    " Do you want to reboot ?":"Do you want to reboot?",
7    "(1~4s)":"(1~4s)",
8    "***Inc. All Rights Reserved":"***Inc. All Rights Reserved",
9    ".CSV file template":".CSV file template",
10   ".XML file template":".XML file template",
11   "01.jpg":"01.jpg",
12   "01-exp50.jpg":"01-exp50.jpg",
13   "02.jpg":"02.jpg",
14   "02-exp50.jpg":"02-exp50.jpg",
15   "03.jpg":"03.jpg",
16   "03-exp50.jpg":"03-exp50.jpg",
17   "04.jpg":"04.jpg",
18   "04-exp50.jpg":"04-exp50.jpg",
19   "05.jpg":"05.jpg",
20   "05-exp50.jpg":"05-exp50.jpg",
21   "06.jpg":"06.jpg",
22   "06-exp50.jpg":"06-exp50.jpg",
23   "07.jpg":"07.jpg",
24
25
26
27
28   "100Mbps Full Duplex":"100Mbps Full Duplex",
29   "100Mbps Full Duplex":"100Mbps Full Duplex",
30   "100Mbps Half Duplex":"100Mbps Half Duplex",
31   "1024kb/s":"1024kb/s",
32   "10-exp50.jpg":"10-exp50.jpg",
33   "10Mbps Full Duplex":"10Mbps Full Duplex",
34   "10Mbps Half Duplex":"10Mbps Half Duplex",
35   "10min":"10min",

```

Do not modify the item on the left of colon. Modify the item

3. 言語パックを保存し、プロビジョニングサーバに配置します。

ノート表示用の言語パックのカスタマイズ

ノートの新しい言語パックを追加する場合、ノート言語パックは「X.name_note.xml」としてフォーマットする必要があります(X は12 から始まり、「name」は言語名に置き換えられます)。ノート言語名が既存のものと同じ場合、アップロードされた新しいノート言語パックは既存のものをオーバーライドします。

新しいノート言語パックのファイル名は既存のものと同じにしないことをお勧めします。

1. XMLエディタを使用して、希望の紙幣言語テンプレートパック(例:1.English_note.xml)を開きます。
2. メモフィールドのテキストを変更します。メモ名は変更しないでください。

以下は、Webユーザーインターフェース用のノート用語パック「1.English_note.xml」の一部を示しています:

```

1.English_note.xml x
<?xml version="1.0" encoding="utf-8"?>
<notedata>
<status>
  <note name = "version">
    <head>Description:</head>
    <text>It shows the current firmware version and hardware version of the device.</text>
  </note>
  <note name = "DeviceCertificate">
    <head>Description:</head>
    <text>It shows the Device Certificate of the device.</text>
  </note>
  <note name = "network">
    <head>Description:</head>
    <text>It shows the IP address mode of the device.</text>
  </note>
  <note name = "network-ipv4">
    <head>Description:</head>
    <text>It shows the basic IPv4 network configurations.</text>
  </note>
  <note name = "network-ipv6">
    <head>Description:</head>
    <text>It shows the basic IPv6 network configurations.</text>
  </note>

```

3. 言語パックを保存し、プロビジョニングサーバに配置します。

Web およびノート表示設定のカスタム言語

デバイスに新しい言語(Wuilan など)を追加する場合は、「13.Wuilan.js」および「13.Wuilan_note.xml」という名前の言語ファイルをダウンロード用に準備します。更新後、Webユーザーインターフェースの右上隅に新しい言語選択「Wuilan」が表示され、この新しい言語が選択されると、新しいノート情報がアイコンに表示されます。

次の表に、Web およびノート表示用のカスタム言語を設定するために使用できるパラメータを示します。

パラメータ	wui_lang.url	<y0000000000xx>.cfg
説明	Webユーザーインターフェース用カスタム言語パックのアクセスURLを設定します。	
許容値	511文字以内のURL たとえば、http://localhost/X.GUI.name.lang X 012 から始まり、“name” は言語名に置き換えられます。	
デフォルト	空白	
パラメータ	wui_lang_note.url	<y0000000000xx>.cfg
説明	Webユーザーインターフェース用カスタムノート言語パックのアクセスURLを設定します。	

許容値	511文字以内のURL たとえば、http://localhost/X.name_note.xml X 13から始まり、“name”は言語名に置き換えられます。	
デフォルト	空白	
パラメータ	wui_lang.delete	<y0000000000xx>.cfg
説明	指定された、またはすべてのカスタムWeb 言語パックと、Web ユーザインタフェースのノート言語パックが削除されます。	
許容値	http://localhost/allやhttp://localhost/Y.name.js	
デフォルト	空白	

例: デバイス表示のカスタム言語の設定

以下の例では、カスタム言語ファイル「015.GUI.English_15.lang」と「016.GUI.English_16.lang」をアップロードし、電話機のユーザーインターフェースに表示するために「015.GUI.English_15.lang」を指定する設定を示します。これらの言語ファイルはカスタマイズされ、プロビジョニングサーバ「192.168.10.25」に配置されます。

例

gui_lang.url=

http://192.168.10.25/015.GUI.English_15.langgui_lang.url=htt

p://192.168.10.25/016.GUI.English_16.langlang.gui=English_1

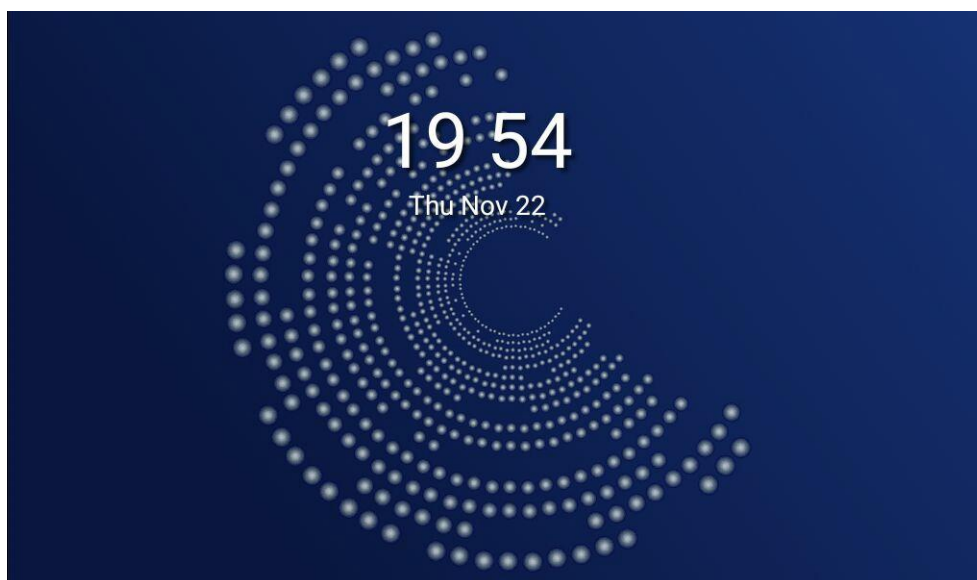
5

プロビジョニング後、電話機のユーザーインターフェースの言語は「015.GUI.English_15.lang」で定義したカスタム言語に変更されます。電話機のユーザーインターフェース(> 設定 > デバイス設定 > 言語)で、新しい言語選択「English_15」と「English_16」を見つけることもできます。☰

スクリーンセーバー

デバイスがあらかじめ設定された待機時間アイドル状態になると、スクリーンセーバーが自動的に起動します。デバイスのキーを押すか、タッチスクリーンをタップすると、スクリーンセーバーを停止し、いつでもアイドル状態の画面に戻ることができます。デバイスがあらかじめ設定された待機時間だけアイドル状態に戻ると、スクリーンセーバーが再び開始されます。

初期設定では、スクリーンセーバーの起動時にデバイス画面に内蔵画像が表示されます。その他の内蔵スクリーンセーバーの背景を表示するようにデバイスを設定できます。また、カスタムスクリーンセーバーの背景を表示するようにデバイスを設定することもできます。T58A Teams デバイスに表示される内蔵スクリーンセーバーを以下に示します:



- [スクリーンセーバーの設定](#)

スクリーンセーバーの設定

次の表に、スクリーンセーバーの設定に使用できるパラメータを示します。

パラメータ	screensaver.enable	<y0000000000xx>.cfg
説明	スクリーンセーバーを有効または無効にします。	
許容値	0-無効 1-有効	
デフォルト	1	
Web UI	設定> プリファレンス> スクリーンセーバー> スクリーンセーバー	
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> スクリーンセーバー> スクリーンセーバー有効 コモンエリアフォンの場合:> 設定> デバイス設定> スクリーンセーバー(管理者のみ:デフォルトパスワード: admin)> スクリーンセーバー有効☰	
パラメータ	screensaver.wait_time	<y0000000000xx>.cfg
説明	スクリーンセーバーが起動する前に、デバイスがアイドル状態で待機する時間(秒)を設定します。	
許容値	30-30s 60-1min 300-5min 600-10min 900-15min 1800-30min 3600-1h 7200-2h	

デフォルト	900	
Web UI	設定> 環境設定> スクリーンセーバー> スクリーンセーバー待機時間	
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> スクリーンセーバー> スクリーンセーバー待機時間 コモンエリアフォンの場合:> 設定> デバイス設定> スクリーンセーバー(管理者のみ:デフォルトパスワード: admin)> スクリーンセーバー待機時間☰	
パラメータ	screensaver.type	<y0000000000xx>.cfg
説明	表示するスクリーンセーバーの種類を設定します。	
許容値	0-システム、LCDスクリーンは内蔵ピクチャを表示します。 4-カスタムでは、液晶画面にカスタムスクリーンセーバー画像(「screen saver.upload_url」というパラメータで設定されています)が表示されます。複数の画像がアップロードされた場合、デバイスは60 秒ごとにすべての画像を交互に表示します。	
デフォルト	空白	
Web UI	設定> 好み> Screensaver タイプ	
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> スクリーンセーバータイプ コモンエリアフォンの場合:> 設定> デバイス設定> スクリーンセーバー(管理者のみ:デフォルトパスワード: admin)> スクリーンセーバータイプ☰	
パラメータ	screensaver.upload_url	<y0000000000xx>.cfg
説明	カスタムスクリーンセーバーの背景のアクセスURL を設定します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	Settings > Preference > Screensaver > Screensaver Type(Custom) > Upload Screensaver	
パラメータ	スクリーンセーバーの背景	<y0000000000xx>.cfg
説明	スクリーンセーバーの背景を設定します。	

許容値	デフォルト。 jpg 01.png 02.png 03.png 04.png 05.png 06.png 07.png 08.png
デフォルト	Default.jpg
Web UI	設定> 環境設定> スクリーンセーバー> スクリーンセーバータイプ(システム)> スクリーンセーバーの背景 設定> 環境設定> スクリーンセーバー> スクリーンセーバーの種類(カスタム)> スクリーンセーバー
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> スクリーンセーバー> スクリーンセーバーの種類(システム)> スクリーンセーバーの背景 コモンエリアフォンの場合:> 設定> デバイス設定> スクリーンセーバー(管理者のみ:既定のパスワード: admin)> スクリーンセーバータイプ(システム)> スクリーンセーバーの背景☰
パラメータ	スクリーンセーバー。削除 <y0000000000xx>.cfg
説明	指定した、またはすべてのカスタムスクリーンセーバーの背景を削除します。 例: カスタムスクリーンセーバーの背景をすべて削除: screensaver.delete= http://localhost/all カスタムスクリーンセーバーの背景を削除する(Screencapture.jpg など): screensaver.delete = http://localhost/Screencapture.jpg
許容値	文字列
デフォルト	空白

バックライト

デバイスがアクティブ(使用中)のときに、LCDバックライトの明るさを変更できます。デバイスが一定時間アイドル状態になると、LCDバックライトの明るさが自動的に変化します。

LCDバックライトの明るさと時間は、次の設定で変更できます:

Backlight Active Level: デバイスがアクティブなときのLCD バックライトの輝度レベルです。

Backlight Time: デバイスが非アクティブのときにLCD バックライトの明るさを変更する遅延時間です。バックライト時間には、次の設定が含まれます:

- 常時オン:バックライトは常時オンです。
- 15s、30s、1min、2min、5min、10min、または30min:指定した時間(秒)が経過してデバイスが非アクティブになると、バックライトが変更されます。
- [バックライトの明るさと時間の設定](#)

バックライトの明るさと時間の設定

次の表に、画面のバックライトの明るさと時間を設定するために使用できるパラメータを示します。

パラメータ	電話設定。active_backlight_level	<y0000000000xx>.cfg
説明	デバイスがアクティブなときのLCD バックライトの強度を設定します。	
許容値	1 ~10 の整数	
デフォルト	8	
Web UI	設定> 環境設定> バックライト> バックライトアクティブレベル	
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> バックライト> バックライトアクティブレベル	
パラメータ	電話設定。backlight_time	<y0000000000xx>.cfg
説明	デバイスが非アクティブのときにLCD バックライトの強度を変更するための遅延時間(秒)を設定します。	
許容値	0-Always On 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 1800-30min	
デフォルト	0	
Web UI	設定> 環境設定> バックライト> バックライト時間(秒) 設定> 一般> 一般情報> バックライト時間	
電話機のUI	☰> 設定> デバイス設定> ディスプレイ> バックライト> バックライト時間	

日時

Teamsデバイスはローカルクロックを維持します。SNTP (Simple Network Time Protocol)タイムサーバーから時刻と日付を取得して最も正確な時刻を取得し、サマータイム(サマータイム)を設定してサマータイムを有効に活用し、エネルギーを節約するか、または時刻と日付を手動で設定するかを選択できます。アイドル画面では、時刻と日付をいくつかの形式で表示できます。

- [時間帯](#)
- [NTP 設定](#)

- DST 設定
- 時刻と日付の手動設定
- 時刻と日付形式の設定

時間帯

次の表に、タイムゾーンの場所の設定に使用できる値を示します。

時間帯	時間帯名	時間帯	時間帯名
-12	国際日付ライン西	+4	Abu Dhabi, Muscat, Baku, Izhevsk, Samara (RTZ 3), Port Louis, Tbilisi, Yerevan
-11	協定世界時-11	+4:30	カブール
-10	ハワイ	+5	Ashgabat, Tashkent, Ekaterinburg (RTZ 4), Isiamabad, Karachi
-9:30	フランスのポリネシア	+5:30	Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura
-9	アラスカ	+5:45	カトマンズ
-8	Baja California, Pacific Time (US & Canada)	+6	Astana, Dhaka, Novsibirsk (RTZ5)
-7	アリゾナ、チワワ、ラパス、マザトラン、マウンテンタイム(米国とカナダ)	+6:30	ヤンゴン(ラングーン)
-6	中米、中部時間(米国およびカナダ)、グアダラハラ、メキシコシティ、モンテレイ、サスカチュワン	+7	バンコク、ハノイ、ジャカルタ、クラスノヤルスク(RTZ 6)
-5	Bogota, Lima, Quito, Rio Branco, Chetumal, Eastern Time (US & Canada), Indiana (East), Havana, Nassau	+8	北京、重慶、ホンコン、ウルムクイ、イルクトスク(RTZ 7)、クアラルンプール、シンガポール、ペルス、台湾、ウラアンバター
-4	アスンシオン、アトランティックタイム(カナダ)、キューアバ、ジョージタウン、ラパス、マナウス、サンファン、カラカス、バミューダ	+8:45	ユークラ
-3:30	ニューファウンドランド	+9	大阪、札幌、東京、ソウル、ヤクトスク(RTZ)
-3	Brasilia, Buenos Aires, Cayenne, Fortaleza, Greenland, Montevideo, Salvador, Santiago	+9:30	アデレード、ダーウィン
-2	協定世界時-02、MidAtlanticOld	+10	Brisbane, Canberra, Melbourne, Sydney, Guam, Port Moresby, Hobart, Magadan, Viadivostok, Magadan (RTZ9)
-1	Azores, Cabo Verde Is.	+11	Chokurdakh (RTZ 10), Solomon Is, New Caiedonia, Hobart, Magadan, Lord Howe Island

時間帯	時間帯名	時間帯	時間帯名
0	Casablanca, Coordinated Universal Time, Dublin, Edinburgh, Lisbon, London, Monrovia, Reykjavik, SpainCanary Islands	+12	Anadyr, Petropavlovk-Kamchatsky (RTZ 11), Auckland, Wellington, Coordinated Universal Time+12, Fiji, Petropavlovsk-Kamchatsky - Old
+1	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna, Belgrade, Bratislava, Budapest, Ljubljana, Prague, Brussels, Copenhagen, Madrid, Paris, Sarajevo, Skopje, Warsaw, Zagreb, ルクセンブルク	+13	フィジー、サモア、ヌクアロファ
+2	Amman, Athens, Bucharest, Beirut, Cairo, Damascus, E. Europe, Harare, Pretoria, Helsinki, Kyiv, Riga, Sofia, Tlin, Vilnius, Istanbul, Jerusalem, Kaliningrad (RTZ 1), Tripoli, Windhoek, Gaza	+13:45	チャタム諸島
+3	イスタンブール、バグダッド、クウェート、リヤド、ミンスク、モスクワ、サンクトペテルブルク、ヴォルゴグラード(RTZ 2)、ナイロビ	+14	キリティマティア일랜드
+3:30	テヘラン		

NTP 設定

必要に応じて、目的のエリアにNTP タイムサーバを設定できます。NTP time server 住所は、DHCP server が提供することも、手動で構成することもできます。

- [NTP 設定](#)

NTP 設定

次の表に、NTP の設定に使用できるパラメータを示します。

パラメータ	local_time.manual_ntp_srv_prior	<MAC>.cfg
説明	デバイスがDHCP サーバによって提供されるNTP サーバアドレスを使用するためのプライオリティを設定します。	
許容値	0- High(DHCPサーバが優先的に提供するNTPサーバアドレスを使用) 1- 低(手動で優先的に設定されたNTP サーバアドレスを使用)	
デフォルト	0	
Web UI	「設定」>「日付と時間」>「DHCPによるNTP優先」	
パラメータ	local_time.dhcp_time	<MAC>.cfg
説明	DHCPサーバが提供するオフセット時間でデバイスを時間を更新することを可能にするか、無効にします。 注: グリニッジ標準時GMT 0 からのオフセット時間にのみ使用できます。	

許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	設定> 日付と時間 > DHCP 時刻	
電話機のUI	☰☞ 設定> デバイス設定> 時刻と日付> DHCP 時刻> DHCP 時刻	
パラメータ	local_time.ntp_server1	<MAC>.cfg
説明	それは、NTPサーバ1のIPアドレスまたはドメイン名を設定します。デバイスはNTPサーバ1から現在の時間と日付を取得します。	
許容値	IPアドレスやドメイン名	
デフォルト	cn.pool.ntp.org	
Web UI	「設定」>「日付と時間」>「プライマリサーバ」	
電話機のUI	☰☞ 設定> デバイス設定> 時刻と日付> 一般> NTP サーバ1	
パラメータ	local_time.ntp_server2	<MAC>.cfg
説明	それは、IPアドレスまたはNTPサーバ2のドメイン名を設定する。 NTP サーバ1 が設定されていないか(パラメータ「local_time.ntp_server1」で設定)、アクセスできない場合、デバイスはNTP サーバ2 に時刻と日付を要求します。	
許容値	IPアドレスやドメイン名	
デフォルト	pool.ntp.org	
Web UI	設定>日付と時間 > セカンダリサーバ	
電話機のUI	☰☞ 設定> デバイス設定> 時刻と日付> 一般> NTP Server2	
パラメータ	local_time の間隔。	<MAC>.cfg
説明	デバイスがNTP サーバから時刻と日付を更新する間隔(秒)を設定します。	
許容値	15 ~86400 の整数	
デフォルト	1000	
Web UI	設定> 日付と時間 > 更新間隔(15 ~ 86400s)	
パラメータ	local_time.time_zone	<MAC>.cfg
説明	デバイスがNTP サーバから時刻と日付を更新する間隔(秒)を設定します。	

許容値	-12~+14 使用可能なタイムゾーンについては、「タイムゾーン」を参照してください。	
デフォルト	+8	
Web UI	設定>日付と時間>タイムゾーン	
パラメータ	local_time.time_zone_name	<MAC>.cfg
説明	タイムゾーン名を設定します。 注意: "local_time.summer_time" が2 (Automatic) に設定され、パラメータ "local_time.time_zone" が事前に設定されている必要がある場合にのみ機能します。	
許容値	32文字以内の文字列 使用可能なタイムゾーン名は、"local_time.time_zone" で設定されたタイムゾーンによって異なります。使用可能なタイムゾーン名については、「タイムゾーン」を参照してください。	
デフォルト	中国(北京)	
Web UI	設定>日付と時間>タイムゾーン	
電話機のUI	☰⇒ 設定> デバイス設定> 時刻と日付> 一般> 場所	

DST 設定

必要に応じて、任意のエリアにDSTを設定できます。デフォルトでは、DSTはAutomaticに設定されているので、現在のタイムゾーン構成から自動的に調整できます。

タイムゾーンと対応するDST 事前設定は、AutoDST ファイルに存在します。DST がAutomatic に設定されている場合、デバイスはAutoDST ファイルからDST 構成を取得します。

必要に応じてAutoDST ファイルをカスタマイズできます。AutoDST ファイルでは、毎年お住まいの地域のタイムゾーンとDST 設定を追加または変更できます。

- [DST ファイルの自動カスタマイズ](#)
- [DST 設定](#)

DST ファイルの自動カスタマイズ

カスタマイズする前に、AutoDST ファイルを取得する必要があります。DST テンプレートについては、代理店またはYealink FAE にお問い合わせください。サマータイムテンプレートは、<http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage> から入手することもできます。

- [自動DST ファイル属性](#)
- [自動DST ファイルのカスタマイズ](#)

自動DST ファイル属性

次の表に、テンプレートファイルの各属性の説明を示します:

属性	型	値	説明
szTime	必要	[+/-][X]:[Y], X=0~14, Y=0~59	時間帯
szZone	必要	文字列(コンテンツが複数の都市の場合、サマータイムを同じにしておくのが最善です)	時間帯名

属性	型	値	説明
iType	オプション	0/1 0: 日付によるサマータイム 1: 週別サマータイム	サマータイムの種類 (DST を設定する場合、この項目が必要です。)
szStart	オプション	月/日/時(iType=0 の場合) 月: 1~12 日: 1~31 時: 0 (午前0 時)~23 月/週/曜日/時(iType=1 の場合) 月: 1~12 月の週: 1~5(最終週)週の日: 1~7 時: 0 (午前0 時)~23	DSTの開始時刻
szEnd	オプション	szStartと同じ	DSTの終了時刻
szOffset	オプション	-300 ~300 の整数	DST のオフセット時間(分)

自動DST ファイルのカスタマイズ

手順

1. AutoDST ファイルを開きます。
2. 新しいタイムゾーンを追加するには、`<DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset="" /> between<DSTData>and</DSTData>` を追加します。

3. DST 属性値は二重引用符で囲んで指定します。次に例を示します。

夏時間30分の新しいタイムゾーン(+6 Paradise)を追加します:

<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30" />

```
AutoDST.xml x
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" />
<DST szTime="+5" szZone="Russia (Chelyabinsk)" />
<DST szTime="+5:30" szZone="India (Calcutta)" />
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30" />
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />
```

既存のタイムゾーン「+5 Pakistan(Islamabad)」のDST 設定を変更し、既存のタイムゾーン「+5:30 India(Calcutta)」のDST 設定を追加します。

```
AutoDST.xml* x
<DST szTime="+3:30" szZone="Iran (Teheran)" iType="0" szStart="3/22/0" szEnd="9/22/0" szOffset="60" />
<DST szTime="+4" szZone="Armenia (Yerevan)" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="60" />
<DST szTime="+4" szZone="Georgia (Tbilisi)" iType="1" szStart="3/5/7/4" szEnd="10/5/7/5" szOffset="60" />
<DST szTime="+4" szZone="Kazakhstan (Aktau)" />
<DST szTime="+4" szZone="Russia (Samara)" />
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" szOffset="60" />
<DST szTime="+5:30" szZone="India (Calcutta)" />
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />
<DST szTime="+6:30" szZone="Myanmar (Naypyitaw)" />
<DST szTime="+7" szZone="Russia (Krasnoyarsk)" />
<DST szTime="+8" szZone="Thailand (Bangkok)" />
<DST szTime="+8" szZone="China (Beijing)" />
<DST szTime="+8" szZone="Singapore (Singapore)" />
```

4. このファイルを保存してプロビジョニングサーバーに配置します。

関連情報

時間帯

DST 設定

次の表に、DST の設定に使用できるパラメータを示します。

パラメータ	local_time.summer_time	<MAC>.cfg
説明	サマータイム(DST)機能を設定します。	
許容値	0-Disabled 1-Enabled 2-Automatic	
デフォルト	2	
Web UI	設定> 日付と時間> 夏時間	
電話機のUI	☰> 設定> デバイス設定> 時刻と日付> 一般> 夏時間	
パラメータ	local_time.dst_time_type	<MAC>.cfg
説明	サマータイム(DST)タイプを設定します。 注意: "local_time.summer_time" が1 (Enabled) に設定されている場合にのみ機能します。	

許容値	0- 日付によるサマータイム 1- 週別サマータイム	
デフォルト	0	
Web UI	設定> 日付と時間> 固定タイプ	
パラメータ	local_time.start_time	<MAC>.cfg
説明	サマータイム(DST)の開始時刻を設定します。 注意: "local_time.summer_time" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	日付別月/日/時/DST では、次のマッピングを使用します: 月: 1=1 月、2=2 月、。。。、12=12 月 日: 1= 月の最初の日。。。、31= 月の最後の日 時: 0=0am, 1=1am, ..., 23=11pm 月/週/曜日/曜日別日DSTの月/時、次のマッピングを使用します: 月: 1=1 月、2=2 月、。。。、12=12 月 月の週: 1= 月の最初の週。。。、5= 月の最後の週 曜日: 1=月曜日、2=火曜日、。。。、7=日曜日 時刻: 0=0am, 1=1am, ..., 23=11pm	
デフォルト	1/1/0	
Web UI	設定> 日付と時間> 開始日	
パラメータ	local_time.end_time	<MAC>.cfg
説明	サマータイム(DST)の終了時刻を設定します。 注意: "local_time.summer_time" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	日付別月/日/時/DST では、次のマッピングを使用します: 月: 1=1 月、2=2 月、。。。、12=12 月 日: 1= 月の最初の日。。。、31= 月の最後の日 時: 0=0am, 1=1am, ..., 23=11pm 月/週/曜日/曜日別日DSTの月/時、次のマッピングを使用します: 月: 1=1 月、2=2 月、。。。、12=12 月 月の週: 1= 月の最初の週。。。、5= 月の最後の週 曜日: 1=月曜日、2=火曜日、。。。、7=日曜日 時刻: 0=0am, 1=1am, ..., 23=11pm	
デフォルト	12/31/23	
Web UI	設定> 日付と時間> 終了日	
パラメータ	ローカル時間。offset_time	<MAC>.cfg

説明	サマータイム(DST)のオフセット時間(分)を設定します。 注意: "local_time.summer_time" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	-300 ~ 300 の整数	
デフォルト	空白	
Web UI	設定> 日付と時間> オフセット(分)	
パラメータ	auto_dst.url	<MAC>.cfg
説明	DST ファイル(AutoDST.xml) のアクセスURL を設定します。 注記: "local_time.summer_time" が2 (Automatic) に設定されている場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	空白	

時刻と日付の手動設定

デバイスがNTP タイムサーバから時刻と日付を取得できない場合は、手動で時刻と日付を設定できます。

次の表に、時刻と日付を手動で設定するために使用できるパラメータを示します。

パラメータ	local_time.manual_time_enable	<MAC>.cfg
説明	手動設定から時刻と日付を取得するためのデバイスの有効 / 無効を切り替えます。	
許容値	0-無効(NTP サーバーから時刻と日付を取得) 1-有効(手動設定から時刻と日付を取得)	
デフォルト	0	
Web UI	設定> 日付と時間> 手動時刻	
電話機のUI	☰> 設定> デバイス設定> 時刻と日付> 一般> 書式> 手動設定	

時刻と日付形式の設定

時刻と日付は、日、月、または年の形式の日付形式へのオプションや、12 時間または24 時間の時刻形式など、さまざまな時刻と日付の形式でカスタマイズできます。また、必要に応じて日付形式をカスタマイズすることもできます。

次の表に、時刻と日付形式の設定に使用できるパラメータを示します。

パラメータ	local_time.time_format	<MAC>.cfg
説明	時刻形式を設定します。	

許容値	0-時12 は、AM またはPM を指定した12 時間形式で時刻が表示されます。 1-時間24 の場合、時刻は24 時間形式で表示されます(たとえば、午後2:00 は14:00 と表示されます)。	
デフォルト	1	
Web UI	設定> 時刻と日付> 時刻形式	
電話機のUI	☰> 設定> デバイス設定> 時刻と日付> 時刻と日付の書式> 時刻の書式	
パラメータ	local_time.date_format	<MAC>.cfg
説明	日付形式を設定します。	
許容値	0-WWW MMM DD 1-DD-MMM-YY 2-YYYY-MM-DD 3-DD/MM/YYYY 4-MM/DD/YY 5-DD MMM YYYY 6-WWW DD MMM 7-MM/DD/YYYY 以下のマッピングを使用する: "WWW"は週の略称を表し、"DD"は2桁の日を表します; 「MM」は2桁の月を表します; 「MMM」は月の最初の3文字を表します; "YYYY"は4桁の年を表し、"YY"は2桁の年を表します。	
デフォルト	0	
Web UI	設定> 日付と時間 > 日付形式	
電話機のUI	☰> 設定> デバイス設定> 時刻と日付> 時刻と日付の書式> 日付の書式	

音色

デバイスがダイヤル画面にあるときは、警告音が鳴ります。トーンをカスタマイズしたり、専用のトーンセット(国によって異なります)を選択して、デバイスのさまざまな条件を示すことができます。CP960 電話には適用されません。

- [対応音色](#)
- [トーン設定](#)

対応音色

Teams デバイスで使用されるデフォルトのトーンは、US トーンセットです。デバイスで使用可能なトーンセット:

- オーストラリア
- オーストリア
- ブラジル
- ベルギー
- チリ
- 中国
- チェコ語
- チェコETSI
- デンマーク
- フィンランド
- フランス
- ドイツ
- イギリス
- ギリシャ
- ハンガリー
- リトアニア
- インド
- イタリア
- 日本
- メキシコ
- ニュージーランド
- オランダ
- ノルウェー
- ポルトガル
- スペイン
- スイス
- スウェーデン
- ロシア
- 米国

トーン設定

トーンの設定に使用できるパラメーターを次の表に示します。

パラメータ	音声。国	<y0000000000xx>.cfg
説明	電話機の国別トーンを設定します。 注: CP960 電話機には適用されません。	
許容値	Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States	
デフォルト	カスタム	
Web UI	設定> トーン> 国を選択	
パラメータ	voice.tone.dial	<y0000000000xx>.cfg

許容値	<p>発信音をカスタマイズします。</p> <p>tone list = element[,element] [,element]...場所</p> <p>要素= [!]Freq1[+Freq2][+Freq3][+Freq4] / 継続時間</p> <p>Freq: トーンの周波数です(範囲は200 ~ 4000Hz)。0Hz に設定すると、トーンが再生されないことを意味します。</p> <p>トーンは、最大4 つの異なる周波数で構成されます。</p> <p>継続時間:ダイヤルトーンの継続時間(ミリ秒)は、0 ~ 30000ms の範囲です。</p> <p>1 つの条件に最大8 つの異なるトーンを設定し、カンマで区切ることができます。(たとえば、250/200,0/1000,200+300/500,200+500+800+1500/1000)。</p> <p>電話機でトーンを1 回再生する場合は、トーンの前に感嘆符「!」を追加します(たとえば、!250/200,0/1000, 200+300/500,200+500+800+1500/1000)。</p> <p>注意: 「voice.tone.country」が「Custom」に設定されている場合にのみ機能します。CP960 電話機には適用されません。</p>	
Web UI	設定> トーン> ダイヤル	
パラメータ	features.ringer_device.is_use_headset	<y0000000000xx>.cfg
説明	電話機の着信音デバイスを設定します。	
許容値	<p>0-スピーカーを使用</p> <p>1-ヘッドセットの使用</p> <p>2-ヘッドセットとスピーカーを使用</p>	
デフォルト	0	
Web UI	設定> 音> 着信音デバイス	
電話機のUI	☰> 設定> デバイス設定> トーン	

ボリューム

電話機の使用中に、現在接続されているオーディオデバイス(ハンドセット、スピーカーフォン、またはヘッドセット)の送信音量を設定できます。

- [ボリューム構成](#)

ボリューム構成

次の表に、ボリュームの設定に使用できるパラメータを示します。

パラメータ	voice.handset.tia4965.enable	<y0000000000xx>.cfg
説明	通話中の音量が基準値を超えた場合に、通話後に音量レベル11にリセットする機能を有効または無効にします。	

許容値	0-無効 1-有効にすると、通話中の受話器の音量レベルがレベル12/13/14/15に調整された場合、通話後に音量レベルが自動的に11にリセットされます。つまり、次の通話の場合、最初の音量レベルは11になります。	
デフォルト	1	
パラメータ	voice.headset.tia4965.enable	<y000000000xx>.cfg
説明	現在の通話の音量レベルが標準を超えた場合に、通話後にヘッドセットの音量レベルをレベル11にリセットする機能を有効または無効にします。	
許容値	0-無効 1-有効にすると、現在の通話に対するヘッドセットの音量レベルがレベル12/13/14/15に調整された場合、通話後に音量レベルは自動的に11にリセットされます。つまり、次の通話の場合、最初の音量レベルは11になります。	
デフォルト	1	

省電力

省電力機能は、液晶のバックライトと液晶ディスプレイを消灯させ、省エネルギーにつなげます。デバイスが一定時間アイドル状態になった後、デバイスは省電力モードに入ります。また、デバイスイベントが発生した場合（たとえば、デバイスが着信した場合、デバイスのキーを押した場合、またはタッチスクリーンをタップした場合）、デバイスは省電力モードを終了します。

注記: デバイスでスクリーンセーバーが有効になっている場合でも、省電力モードが実行されます。たとえば、デバイスが5分間アイドル状態になった後でスクリーンセーバーが起動するように設定され、電話が15分間アイドル状態になった後で省電力モードがバックライトとスクリーンをオフにするように設定されている場合、スクリーンセーバーが10分間オンになった後でバックライトとスクリーンがオフになります。

- [省電力設定](#)

省電力設定

省電力を有効または無効にしたり、営業時間とオフ時間に異なるアイドルタイムアウトを設定したりできます。

- **営業時間:**営業時間の開始時間と終了時間を指定します。営業時間を変更して、仕事に影響を与えないようにすることができます。
- **アイドルタイムアウト(分):**電話機が省電力モードに入るまでの時間を指定します。次の3種類のアイドルタイムアウトを指定できます:

アイドルタイムアウトを指定できます:

- **営業時間アイドルタイムアウト:**営業時間のアイドルタイムアウトを指定します。
- **「オフ時間アイドルタイムアウト」:**営業時間以外のアイドルタイムアウトを指定します。
- **ユーザ入力延長アイドルタイムアウト:**IP Phone を使用した後に適用されるアイドルタイムアウトを指定します(たとえば、電話機のキーを押したり、ハンドセットをピックアップ/ハングアップしたりします)。

デフォルトでは、Office Hours Idle Timeout はOff Hours Idle TimeOut よりもはるかに長くなります。電話機を使用する場合、適用されるアイドルタイムアウト(User Input Extension Idle Timeout またはOffice Hours/Off Hours Idle TimeOut)は、最も高い値を持つタイムアウトです。

注: VP59/MP54/MP58/MP58-WH Teams 電話機の場合、省電力機能を無効にすると、電話機は自動的に省電力モードに入り、電話機が72時間非アクティブになったときに画面を保護します。省電力が無効になっている場合、LCD に画像の残像が生じることがあります。

次の表に、省電力を設定するために使用できるパラメータを示します。

パラメータ	features.power_saving.intelligent_mode	<y0000000000xx>.cfg
説明	省電力インテリジェントモードを有効または無効にします。	
許容値	0-無効にすると、翌日に営業時間が到着しても、電話機は省電力モードのままになります。 1-有効にすると、翌日営業時間になると、電話機は営業時間を自動的に識別し、省電力モードを終了します。	
デフォルト	1	
Parameter	features.power_saving.enable	<y0000000000xx>.cfg
説明	省電力機能を有効または無効にします。	
許容値	0-無効にすると、電話機は自動的に省電力モードに入り、電話機が72 時間非アクティブなときに画面を保護します。LCD 上で画像のパーシスタンスが発生する場合があります。 1-有効	
デフォルト	1	
Web UI	設定> 省電力> 省電力	
パラメータ	features.power_saving.office_hour.idle_timeout	<y0000000000xx>.cfg
説明	営業時間中に電話機が省電力モードに入るまでのアイドル状態で電話機が待機する時間(分)を設定します。 例: features.power_saving.office_hour.idle_timeout= 600 営業時間内に600 分(10 時間)非アクティブ化されると、電話機は省電力モードに入ります。	
許容値	1 ~960 の整数	
デフォルト	120	
Web UI	設定> 省電力> 営業時間アイドルタイムアウト	
パラメータ	features.power_saving.off_hour.idle_timeout	<y0000000000xx>.cfg
説明	オフィス以外の時間帯にIP Phone が省電力モードに入る前に、電話機がアイドル状態で待機する時間(分)を設定します。 例: features.power_saving.off_hour.idle_timeout= 5 IP Phone は、営業時間外に5 分間非アクティブ化されると、省電力モードに入ります。	
許容値	1 ~10 の整数	
デフォルト	10	
Web UI	設定> 省電力> オフ時間アイドルタイムアウト	

パラメータ	features.power_saving.user_input_ext.idle_timeout	<y000000000xx>.cfg
説明	<p>電話機が省電力モードに入る前に、アイドル状態(非アクティブになった後)で電話機が待機する最小時間(分)を設定します。</p> <p>例: features.power_saving.user_input_ext.idle_timeout= 5</p>	
許容値	1 ~30 の整数	
デフォルト	10	
Web UI	設定> 省電力> ユーザ入力延長アイドルタイムアウト	
パラメータ	features.power_saving.office_hour.mondayfeatures.power_saving.office_hour.tuesdayfeatures.power_saving.office_hour.wednesdayfeatures.power_saving.office_hour.thursdayfeatures.power_saving.office_hour.fridayfeatures.power_saving.office_hour.saturdayfeatures.power_saving.office_hour.sunday	<y000000000xx>.cfg
説明	<p>これは、その日の営業時間の開始時刻と終了時刻を設定します。開始時刻と終了時刻はカンマで区切られます。</p> <p>例: features.power_saving.office_hour.monday= 7,19</p>	
許容値	0 ~23 の整数	
デフォルト	7,19 - 月曜日、火曜日、水曜日、木曜日、金曜日の場合。7,7 - 土曜日、日曜日の場合。	
Web UI	設定> 省電力> 月曜日/火曜日/水曜日/木曜日/金曜日/土曜日/日曜日	

電源LEDインジケータ

電源LED インジケータは、電源ステータスと電話ステータスを示します。CP960 には適用されません。

電源LED インジケータの動作は、次のシナリオで設定できます:

- 電話が着信する
- 電話が話中です
- 電話機がボイスメールを受信する
- 電話機がコールをミスした
- [電源 LED インジケータの設定](#)

電源 LED インジケータの設定

次の表に、電源 LED インジケータの設定に使用できるパラメータを示します。

パラメータ	phone_setting.ring_power_led_flash_enable	<y0000000000xx>.cfg
説明	電話機が着信を受けたときに点滅する電源LED インジケータを有効または無効にします。	
許容値	0-無効(電源 LED インジケータが点滅しない) 1-有効(電源LEDインジケータが赤色で速く点滅(300ms))	
デフォルト	1	
Web UI	機能> 電源LED >着信ランプを点滅	
パラメータ	phone_setting.mail_power_led_flash_enable	<y0000000000xx>.cfg
説明	電話機がボイスメールを受信したときに点滅する電源LED インジケータを有効または無効にします。	
許容値	0-無効(電源 LED インジケータが点滅しない) 1-有効(電源LEDインジケータがゆっくりと赤色に点滅(1000ms))	
デフォルト	1	
Web UI	機能> 電源LED > 音声/テキストメールランプ点滅	
パラメータ	phone_setting.talk_and_dial_power_led_enable	<y0000000000xx>.cfg
説明	電話機がビジー状態のときに電源LED インジケータをオンにすることを有効または無効にします。	
許容値	0-無効(電源LED インジケータが消灯) 1-Enabled(有効)(電源 LED インジケータが赤色に点灯)	
デフォルト	0	
Web UI	機能> 電源LED >通話/ダイヤルランプ点灯	
パラメータ	phone_setting.missed_call_power_led_flash.enable	<y0000000000xx>.cfg
説明	電話機が不在着信になったときに点滅する電源LED インジケータを有効または無効にします。	
許容値	0-無効(電源 LED インジケータが点滅しない) 1-有効(電源LEDインジケータがゆっくりと赤色に点滅(1000ms))	
デフォルト	1	
Web UI	機能> 電源LED >不在着信電源ランプ点滅	

Bluetooth

Bluetooth は、10m (32 フィート) の範囲内で低帯域幅のワイヤレス接続を可能にします。最高のパフォーマンスを発揮する範囲は1 ~2 メートル(3 ~6 フィート) です。

BluetoothヘッドセットやBluetooth端末と本機をペアリングして接続します。

T56A/T55A/MP54 Teams 電話機の場合は、Bluetooth USB ドングルBT41 が電話機に接続されていることを確認します。

- [Bluetooth 設定](#)

Bluetooth 設定

Bluetoothモードの起動/解除や、電話機のBluetooth機器名称の個人設定ができます。設定済みのBluetooth機器名が、他の機器のスキャンリストに表示されます。他のBluetoothデバイスが電話機を識別してペアリングするのに役立ちます。

次の表に、Bluetooth の設定に使用できるパラメータを示します。

パラメータ	static.bluetooth.function.enable ^[1]	<y0000000000xx>.cfg
説明	Bluetooth 機能を有効または無効にします。 注: T58A/T56A/T55A/MP58/MP58-WH/MP56/MP54 Skype for Business Phone にのみ適用されます。	
許容値	0-Disabled 1-Enabled	
デフォルト	1	
パラメータ	features.bluetooth_enable	<y0000000000xx>.cfg
説明	それはBluetoothモードをオンまたはオフに起動します。	
許容値	0- Off 1-On	
デフォルト	1 (MP56の場合は0)	
電話機のUI	≡(その他) > 設定 > デバイス設定 > Bluetooth > Bluetooth	
Web UI	機能 > Bluetooth > Bluetooth 有効	
パラメータ	features.bluetooth_adapter_name	<y0000000000xx>.cfg
説明	Bluetooth装置名を設定します。 注: 「features.bluetooth_enable」が1 (On) に設定されている場合にのみ機能します。	
許容値	64文字以内の文字列	
デフォルト	T58A : Yealink-T58 T56A: Yealink-T56A T55A: Yealink-T55A VP59: Yealink-VP59 CP960: Yealink-CP960 MP54: Yealink-MP54 MP56: Yealink-MP56 MP58/MP58-WH: Yealink-MP58	
電話機のUI	≡(その他) > 設定 > デバイス設定 > Bluetooth > デバイス名	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

共通領域電話(Common Area Phone)

一般的に、コモン・エリア・フォンは、例えば、受付エリア、ロビー、または会議電話など、多くの人が電話をかけることができるロビーまたは別のエリアのようなエリアに配置される。コモン・エリア・フォンは、ユーザではなくデバイスとして設定され、自動的にネットワークにサインインできます。

組織にコモン・エリア・フォンを配置するには、電話システムのアカウントを設定する必要があります。共通エリア電話の特定の機能にアクセスできます：

- **CAP アカウント:** コール機能があります。また、システム管理者が Microsoft Teams & Skype for Business Admin Center で有効にしている場合は、検索機能もあります。
- **ミーティングアカウント:** スケジュールされたミーティングにのみ参加できます。

コモン・エリア・フォンのアカウントを設定する方法の詳細については、「Microsoft Teams の Common Area Phone ライセンスの設定」を参照してください。

通話機能

この章では、Teams デバイスでコール機能を設定する方法を示します。

- [コールキュー](#)
- [コールパークとリトリーブ](#)

コールキュー

コールキューは、ヘルプデスクやカスタマーサービスデスクなど、着信コールをグループ番号(着信エージェント)にルーティングしてキューに入れる機能です。

コールキューが設定されている電話番号に誰かがコールすると、最初にグリーティングが聞こえ(設定されている場合)、次にキューに入れられ、使用可能なコールエージェントを待機します。発信者は保留中で待機中に音楽を聞きます。

保留中に再生されるグリーティングと音楽を設定し、コールキューの配布方法として「出席者」、「シリアル」、または「ラウンドロビン」のいずれかを選択できます。すべての新規および既存のコールキューには、デフォルトでアテンダントルーティングが選択されます。アテンダントルーティングが使用されている場合、キュー内の最初のコールはすべてのコールエージェントを同時に呼び出します。コールをピックアップする最初のコールエージェントがコールを取得します。

コールキュー機能は、MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A Teams 電話にのみ適用されます。コールキューの作成方法については、「クラウドコールキューの作成」を参照してください。

コールパークとリトリーブ

コールパークと検索は、ユーザがクラウド内の Teams サービスでコールをホールドさせる機能です。コールがパークされると、サービスはコール取得用の一意のコードを生成します。コールをパークしたユーザまたは他のユーザは、そのコードを使用してコールを取得できます。

コールパークおよびリトリーブ機能は、デフォルトで無効になっています。ユーザに対して有効にし、コールパークポリシーを使用してユーザグループを作成できます。一連のユーザに同じポリシーを適用すると、ユーザはコールをパークおよび取得できます。

コールパークとリトリブの設定方法の詳細については、Microsoft Teams の「コールパークとリトリブ」を参照してください。

セキュリティ機能

- [ユーザーと管理者の識別](#)
- [電話ロック](#)
- [トランスポート層セキュリティ](#)
- [設定ファイルの暗号化](#)

ユーザーと管理者の識別

デフォルトでは、一部のメニューオプションは特権レベル(ユーザーと管理者)によって保護されており、それぞれに独自のパスワードが設定されています。また、Webユーザーインターフェースおよび電話ユーザーインターフェースで設定のアクセス権限をカスタマイズすることもできます。Yealink Phone は、admin、var、user のアクセスレベルをサポートしています。

ウェブユーザーインターフェースにログインしたり、デバイスの高度な設定にアクセスしたりする場合、管理者として、さまざまなメニューオプションにアクセスするための管理者のパスワードが必要です。管理者のデフォルトのユーザー名とパスワードは「admin」です。ユーザーとユーザーの両方がWeb ユーザーインターフェースにログインでき、すべてのユーザーオプションが表示されます。ユーザーのデフォルトのユーザー名とパスワードは「user」です。

セキュリティ上の理由から、デフォルトのユーザーまたは管理者パスワードはできるだけ早く変更する必要があります。詳細メニューオプションは管理者によって厳密に使用されるため、ユーザーは管理者権限を持っている場合にのみ設定できます。

- [ユーザーおよび管理者の識別設定](#)
- [ユーザーアクセスレベルの設定](#)

ユーザーおよび管理者の識別設定

次の表に、ユーザーと管理者の識別情報を設定するために使用できるパラメータを示します。

パラメータ	static.security.user_name.user	<y0000000000xx>.cfg
説明	デバイスのWeb ユーザーインターフェースアクセス用にユーザーのユーザー名を設定します。	
許容値	32文字以内の文字列	
デフォルト	利用者	
パラメータ	static.security.user_name.admin	<y0000000000xx>.cfg
説明	デバイスのWeb ユーザーインターフェースアクセスの管理者のユーザー名を設定します。	
許容値	32文字以内の文字列	
デフォルト	管理者	
パラメータ	static.security.user_name.var	<y0000000000xx>.cfg
説明	デバイスのWeb ユーザーインターフェースアクセス用にvar のユーザー名を設定します。 注意: "static.security.var_enable" が1 (Enabled) に設定されている場合にのみ機能します。	
許容値	32文字以内の文字列	
デフォルト	var	

パラメータ	静的セキュリティ。user_password	<y000000000xx>.cfg
説明	<p>ユーザーまたは管理者のパスワードを設定します。</p> <p>デバイスは、デフォルトのユーザーパスワードとして「user」、デフォルトの管理者パスワードとして「admin」を使用します。</p> <p>有効な値の形式は<username>: <new password> です。</p> <p>例:</p> <p>静的セキュリティ。user_password= user:123 は、user のパスワードを123 に設定することを意味します。</p> <p>静的セキュリティ。user_password= admin:456 は、administrator のパスワードを456 に設定することを意味します。</p> <p>注:デバイスは、パスワードでASCIIキャラクター32-126(0x20-0x7E)をサポートします。パスワードは、Webユーザーインターフェースのみで空に設定できます。</p>	
許容値	32文字以内の文字列	
デフォルト	利用者	
Web UI	セキュリティ> パスワード	
電話機のUI	<p>☰> Settings > Device Settings > Admin Password (デフォルトパスワード: admin)</p> <p>注: 電話機のユーザーインターフェイスを使用してユーザーパスワードを変更することはできません。</p>	

ユーザーアクセスレベルの設定


詳細については、『Yealink SIP IP Phones Configuration Guide for User Access Level』を参照してください。次の表に、ユーザーアクセスレベルの設定に使用できるパラメータを示します。

パラメータ	static.security.var_enable ^[1]	<y000000000xx>.cfg
説明	3レベルのアクセス権限(admin、user、var)を有効または無効にします。	
許容値	<p>0-Disabled</p> <p>1-Enabled</p>	
デフォルト	0	
パラメータ	static.web_item_level.url ^[1]	<y000000000xx>.cfg
説明	3レベルのアクセス権限を定義するファイルのアクセスURLを設定します。	
許容値	511文字以内のURL	
デフォルト	空白	

電話ロック

Teams電話機をロックして、不正使用を防ぐことができます。電話機がロックされたら、全員がパスワードを入力してロックを解除する必要があります。

セキュリティ要件の高いユーザは、Microsoft Teams & Skype for Business Admin Center によって電話機のロックを有効にして、自分で無効にできないようにすることができます。

 注意:電話ロック機能は、一般市内電話では使用できません。

- [電話機のロック設定](#)

関連タスク

[構成プロファイルの作成](#)

関連情報

[Microsoft Teams & Skype for Business Admin Center でのデバイスのプロビジョニング](#)

電話機のロック設定

次の表に、電話ロックの設定に使用できるパラメータを示します。

パラメータ	電話設定。phone_lock.enable	<y0000000000xx>.cfg
説明	電話ロック機能を有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	機能> 電話ロック> 電話ロック有効	
電話機のUI	☰> 設定> デバイス設定> 電話ロック> ロック有効	
パラメータ	phone_setting.phone_lock.lock_time_out	<y0000000000xx>.cfg
説明	電話機を自動的にロックする間隔(秒)を設定します。	
許容値	30 ~ 3600 の整数	
デフォルト	900	
Web UI	機能> 電話ロック> アイドルタイムアウト(30~3600s)	
電話機のUI	☰> 設定> デバイス設定> 電話ロック> アイドルタイムアウト	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

トランスポート層セキュリティ

TLS は、通信のプライバシーを提供し、メッセージ送信のセキュリティを管理する一般的に使用されるプロトコルで、デバイスが他のリモートパーティと通信し、盗聴や改ざんを防止するように設計された方法でプロビジョニング用の HTTPS URL に接続できるようにします。

Yealink デバイスは、TLS 1.0、TLS 1.1、および TLS 1.2 をサポートします。

- [対応暗号スイート](#)

- サポートされる信頼済み証明書とサーバ証明書
- TLS 設定

対応暗号スイート

暗号スイートは、TLS/SSLネットワークプロトコルを使用してネットワーク接続のセキュリティ設定をネゴシエートするために使用される、認証、暗号化、およびメッセージ認証コード(MAC)アルゴリズムの名前付きの組み合わせです。

Yealinkデバイスは、次の暗号スイートをサポートしています:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

サポートされる信頼済み証明書とサーバ証明書

この装置は、TLSクライアントまたはTLSサーバーの役割を果たすことができます。TLS 機能では、trusted という用語とサーバ証明書を使用します。これらはCA 証明書およびデバイス証明書とも呼ばれます。

TLSは、TLSハンドシェイクを行うために、下記のセキュリティ証明書を要求する:

- **信頼された証明書:** デバイスがサーバとのTLS 接続を要求する場合、デバイスはサーバから送信された証明書を検証して、信頼された証明書リストに基づいて信頼されているかどうかを判断する必要があります。**最大10 個のカスタム証明書をアップロードできます。**
信頼できる証明書ファイルの形式は*.pem、*.cer、*.crt、および*.der である必要があり、最大ファイルサイズは5MB です。

- **サーバ証明書:**クライアントがデバイスとのTLS接続を要求すると、デバイスは認証のためにサーバ証明書をクライアントに送信します。デバイスには、一意のサーバ証明書と汎用のサーバ証明書の2種類の組み込みサーバ証明書があります。
デバイスにアップロードできるサーバ証明書は1つだけです。古いサーバ証明書は新しい証明書によって上書きされます。サーバ証明書ファイルの形式は*.pem および*.cer である必要があり、最大ファイルサイズは5MBです。
- **一意のサーバ証明書:** デバイス(MAC アドレスに基づく)に固有で、Yealink 認証局(CA)によって発行されます。
- **汎用サーバ証明書:** Yealink 認証局(CA)によって発行されます。一意の証明書が存在しない場合にのみ、デバイスは認証のために汎用証明書を送信できます。

デバイスは、信頼された証明書リストに基づいてサーバ証明書を認証できます。信頼済み証明書リストとサーバ証明書リストには、デフォルト証明書とカスタム証明書が含まれています。デバイスが受け入れる証明書のタイプ(デフォルト証明書、カスタム証明書、またはすべての証明書)を指定できます。

共通名検証機能を使用すると、デバイスは接続サーバから送信された証明書の共通名を強制的に検証できます。セキュリティ検証ルールはRFC 2818 に準拠しています。

- [サポートされる信頼済み証明書](#)

サポートされる信頼済み証明書

Yealink Teams デバイスは、デフォルトで次のCAを信頼します:

- DigiCert High Assurance EV Root CA
- ドイツテレコムルートCA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrustグローバルCA
- GeoTrust グローバルCA2
- GeoTrustプライマリ認証局
- GeoTrustプライマリ認証局G2
- GeoTrustユニバーサルCA
- GeoTrustユニバーサルCA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2

- VeriSign Class 4 Public Primary Certification Authority – G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- バルティモア・サイバートラスト・ルート
- DSTルートCA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust 外部CA ルート
- Go Daddy Class 2 認証局
- クラス2 プライマリCA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID ルートCA
- DigiCert グローバルルートG2
- DigiCert グローバルルートG3
- DigiCert グローバルルートCA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority – G2
- Entrust.net 認証局(2048)
- GeoTrustプライマリ認証局- G3
- GlobalSignルートCA
- GlobalSign ルートCA – R2
- スターフィールドルート認証局- G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign クラス3 セキュアサーバーCA – G2
- VeriSign クラス3 セキュアサーバーCA – G3
- Thawte SSL CA
- StartCom認証局
- StartCom認証局G2
- スターフィールドサービスルート認証局- G2
- RapidSSL CA
- Go Daddy Root Certificate Authority – G2
- Cybertrust グローバルルート
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA認証局
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- YealinkルートCA
- Yealink Equipment Issuing CA

- SIPコア

メモ: Yealink は、最も一般的に使用されるCA 証明書の組み込みリストの維持に努めています。メモリの制約により、証明書の完全なセットを保証することはできません。証明書を使用している場合、商用認証局から依頼を送信できますが、上記のリストには含まれていません。この時点で、特定のCA 証明書をデバイスにアップロードできます。

TLS 設定

次の表に、TLS の設定に使用できるパラメータを示します。

パラメータ	static.security.trust_certificates ^[1]	<y0000000000xx>.cfg
説明	信頼済み証明書リストにリストされているサーバ証明書のみを信頼するようにデバイスを有効または無効にします。	
許容値	0-無効にすると、サーバーから送信された証明書が有効かどうかに関係なく、デバイスはサーバーを信頼します。 1-有効にすると、デバイスは信頼された証明書リストに基づいてサーバ証明書を認証します。認証が成功した場合にのみ、デバイスはサーバを信頼します。	
デフォルト	1	
Web UI	セキュリティ>認証済証明書> 認証済証明書のみ許可	
パラメータ	static.security.ca_cert ^[1]	<y0000000000xx>.cfg
説明	デバイスがTLS 接続を認証するための信頼済み証明書リストの証明書のタイプを設定します。	
許容値	0-デフォルト証明書 1-カスタム証明書 2-すべての証明書	
デフォルト	2	
Web UI	セキュリティ>認証済証明書> CA 証明書	
パラメータ	static.security.cn_validation ^[1]	<y0000000000xx>.cfg
説明	サーバから送信された証明書のCommonName またはSubjectAltName を強制的に検証するデバイスを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	セキュリティ>認証済証明書> 共通名確認	
パラメータ	static.trusted_certificates.url	<y0000000000xx>.cfg
説明	接続サーバの認証に使用されるカスタム信頼証明書のアクセスURL を設定します。 例： static.trusted_certificates.url= http://192.168.1.20/tc.crt メモ: アップロードする証明書は、*.pem、*.crt、*.cer、または*.der 形式である必要があります。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	セキュリティ>認証済証明書>認証済証明書ファイルのアップロード	

パラメータ	static.trusted_certificates.delete	<y0000000000xx>.cfg
説明	アップロードされたすべての信頼済み証明書を削除します。	
許容値	http://localhost/all	
デフォルト	空白	
パラメータ	static.security.dev_cert ^[1]	<y0000000000xx>.cfg
説明	デバイスがTLS 認証のために送信するデバイス証明書のタイプを設定します。	
許容値	0- デフォルト証明書 1- カスタム証明書	
デフォルト	0	
Web UI	セキュリティ> サーバ証明書> デバイス証明書	
パラメータ	static.server_certificates.url	<y0000000000xx>.cfg
説明	デバイスが認証のために送信する証明書のアクセスURL を設定します。 注: アップロードする証明書は*.pem または*.cer 形式である必要があります。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	セキュリティ> サーバ証明書> サーバ証明書ファイルのアップロード	
パラメータ	static.server_certificates.delete	<y0000000000xx>.cfg
説明	アップロードされたサーバ証明書をすべて削除します。	
許容値	http://localhost/all	
デフォルト	空白	
パラメータ	static.phone_setting.reserve_certs_enable	<y0000000000xx>.cfg
説明	デバイスが出荷時のデフォルトにリセットされた後、カスタム証明書を予約することを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

設定ファイルの暗号化

Yealink Teamsデバイスは、暗号化されたファイルをサーバーからダウンロードし、サーバーにアップロードする前/時にファイルを暗号化できます。

MAC オリエンテッドCFG ファイル(<MAC>.cfg)、共通CFG ファイル(y0000000000xx.cfg)、MAC-local CFG ファイル(<MAC>-local.cfg)、またはその他のカスタムCFG ファイル(Teams.cfg、account.cfg など)の構成ファイルを暗号化できます。

ファイルを暗号化/復号化するには、AES キーを設定する必要がある場合があります。

注記: AES キーは16 文字にする必要があります。サポートされている文字は、0 ~ 9、A ~ Z、a ~ z、特殊文字: # \$ % * + , - です。: = ? @ [] ^ _ { } ~ .

- [設定ファイル暗号化ツール](#)
- [設定ファイルの暗号化と復号](#)
- [暗号化と復号の設定](#)
- [例: 構成ファイルの暗号化](#)

設定ファイル暗号化ツール

Yealinkは、設定ファイル用に3つの暗号化ツールを提供します:

- Config_Encrypt_Tool.exe (Windows プラットフォームのグラフィカルツール経由)
- Config_Encrypt.exe (Windows プラットフォームのDOS コマンドライン経由)
- yealinkencrypt (Linux プラットフォーム用)

暗号化ツールは、16 文字の対称キー(構成ファイルの場合は同じまたは異なるキー)を使用して、平文構成ファイル(account.cfg、<y0000000000xx>.cfg、<MAC>.cfg) を(1 つずつまたはバッチで) 暗号化し、以前と同じファイル名の暗号化された構成ファイルを生成します。

また、これらのツールは、デバイスに組み込まれているものと同じ固定キーを使用して平文16 文字対称キーを暗号化し、<xx_Security>.enc という名前の新しいファイルを生成します(xx は構成ファイルの名前です。例えば、y000000000058_Security.enc for y000000000058.cfg ファイル、account_Security.cfg.fg.)。これらのツールは、構成ファイルごとに平文16 文字対称キーを格納するために、Aeskey.txt という名前の別の新しいファイルを生成します。

設定ファイルの暗号化と復号

暗号化された設定ファイルをプロビジョニングサーバーからダウンロードして、機密情報(ログインパスワード、登録情報など)の不正アクセスや改ざんから保護できます。

セキュリティ上の理由から、暗号化された設定ファイル<xx_Security>.enc ファイルをプロビジョニングサーバーのルートディレクトリにアップロードする必要があります。オートプロビジョニング中、デバイスは最初に起動ファイルをダウンロードしてから、参照されている設定ファイルをダウンロードするように要求します。たとえば、デバイスは暗号化されたaccount.cfg をダウンロードします。ファイル。

デバイスは<account_Security>.enc ファイルのダウンロード(有効な場合)を要求し、組み込みキー(key1 など)を使用してプレーンテキストキー(key2 など)に復号します。次に、デバイスはaccount.cfg を復号化します。key2を使ったファイル復号化後、デバイスは構成ファイルを解決し、構成設定をデバイスシステムに更新します。

暗号化と復号の設定

次の表に、暗号化と復号の設定に使用できるパラメータを示します。

パラメータ	static.auto_provision.update_file_mode	<y0000000000xx>.cfg
説明	暗号化されたファイルのダウンロードのみを有効または無効にします。	
許容値	<p>0-無効にすると、デバイスは設定ファイル(たとえば、sip.cfg、account.cfg、<MAC>-local.cfg)および<MAC>-contact.xml をダウンロードします。ファイルが暗号化されているかどうかに関係なく、オートプロビジョニング中にサーバーからのファイル。その後、デバイスはこれらのファイルを解決し、設定をデバイスシステムに更新します。</p> <p>1-有効にすると、デバイスはオートプロビジョニング中にサーバーから暗号化された設定ファイル(sip.cfg、account.cfg、<MAC>-local.cfg など)または<MAC>-contact.xml ファイルのみをダウンロードし、これらのファイルを解決して設定をデバイスシステムに更新します。</p>	
デフォルト	0	

パラメータ	static.auto_provision.aes_key_in_file	<y0000000000xx>.cfg
説明	暗号化されたAES キーを使用してコンフィギュレーションファイルを復号化するデバイスを有効または無効にします。	
許容値	<p>0-無効にすると、デバイスで設定されたプレーンテキストのAES キーを使用して、暗号化された設定ファイルが復号化されます。</p> <p>1-有効にすると、デバイスは<xx_Security>.enc をダウンロードします。ファイル(たとえば、オートプロビジョニング中に<sip_Security>.enc,<account_Security>.enc)、これらのファイルをデバイスの組み込みキー(key1 など)を使用してそれぞれプレーンテキストキー(key2、key3 など)に復号化します。その後、デバイスは対応するキー(key2、key3 など)を使用して暗号化された設定ファイルを復号化します。</p>	
デフォルト	0	
パラメータ	static.auto_provision.aes_key_16.com	<y0000000000xx>.cfg
説明	<p>Common CFG/ Custom CFG ファイルを暗号化/復号するためのプレーンテキストAES キーを設定します。</p> <p>有効な文字には、0 ~ 9、A ~ Z、a ~ z、および次の特殊文字もサポートされています。# \$ % * +、-、.: = ? @ [] ^ _ { } ~ .</p> <p>例:</p> <p>static.auto_provision.aes_key_16.com= 0123456789abcdef</p> <p>注意: 復号化の場合、“static.auto_provision.aes_key_in_file” が0 (Disabled) に設定されている場合にのみ機能します。ダウンロードしたMAC 指向ファイルが暗号化され、パラメータ“static.auto_provision.aes_key_16.mac” が空白のままの場合、デバイスはパラメータ“static.auto_provision.aes_key_16.com” で設定されたAES キーを使用してMAC 指向ファイルの暗号化/復号化を試みます。</p>	
許容値	16文字	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> 共通AES キー	
パラメータ	static.auto_provision.aes_key_16.mac	<y0000000000xx>.cfg
説明	<p>MAC 指向ファイル(<MAC>.cfg,<MAC>-local.cfg および<MAC>-contact.xml)を暗号化/復号するためのプレーンテキストAES キーを設定します。</p> <p>有効な文字には、0 ~ 9、A ~ Z、a ~ z、および次の特殊文字もサポートされています。# \$ % * +、-、.: = ? @ [] ^ _ { } ~ .</p> <p>例:</p> <p>static.auto_provision.aes_key_16.mac= 0123456789abmins</p> <p>注意: 復号化の場合、“static.auto_provision.aes_key_in_file” が0 (Disabled) に設定されている場合にのみ機能します。ダウンロードしたMAC 指向ファイルが暗号化され、パラメータ“static.auto_provision.aes_key_16.mac” が空白のままの場合、デバイスはパラメータ“static.auto_provision.aes_key_16.com” で設定されたAES キーを使用してMAC 指向ファイルの暗号化/復号化を試みます。</p>	
許容値	16文字	
デフォルト	空白	
Web UI	設定> オートプロビジョニング> MAC 向けAES キー	

例: 構成ファイルの暗号化

次の例では、“Config_Encrypt_Tool.exe” を使用してaccount.cfg を暗号化する方法について説明します。ファイル。他の2つの暗号化ツールの詳細については、『Yealink Configuration Encryption Tool User Guide』を参照してください。

デバイスが他の設定ファイルを処理する方法は、account.cfg ファイルと同じです。

手順

1. 「Config_Encrypt_Tool.exe」をダブルクリックして、アプリケーションツ



ルを起動します。メインページのスクリーンショットを以下に示します:

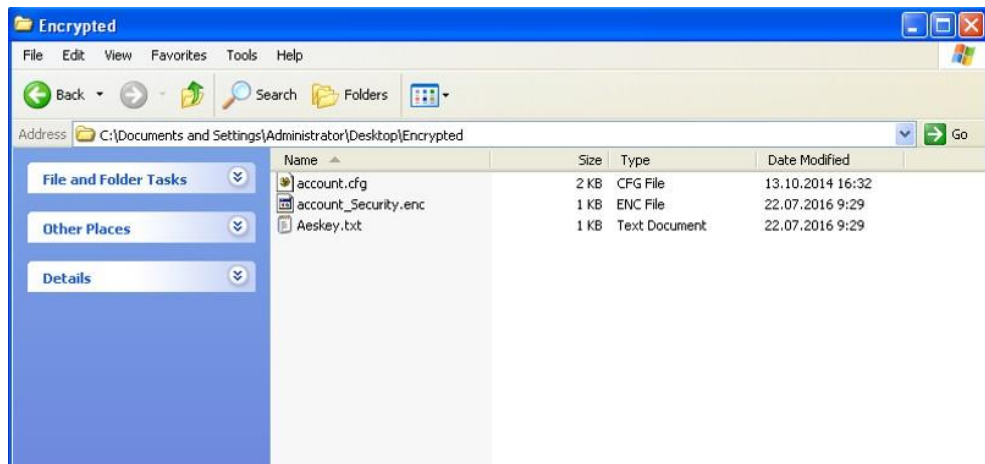
2. アプリケーションツールを起動すると、アプリケーションツールが配置されているディレクトリに「Encrypted」という名前のファイルフォルダが自動的に作成されます。
3. 「参照」をクリックして、「ファイルの選択」フィールドでローカルシステムから設定ファイル(たとえば、account.cfg)を探します。
複数の構成ファイルを選択するには、最初のファイルを選択した後、Ctrlキーを押して保持し、その他のファイルを選択することができます。
4. 参照をクリックして、対象ディレクトリフィールドでローカルシステムから対象ディレクトリを見つけます。
このツールでは、デフォルトでファイルフォルダ“Encrypted”がターゲットディレクトリとして使用されます。
5. (オプション)「AES モデル」フィールドに目的の無線ボックスをオンにします。
「手動」ラジオボックスを選択すると、「AES KEY」フィールドにAES KEYを入力するか、「再生成」を選択してAES KEYフィールドにAES KEYを生成できます。設定ファイルは、AES KEYフィールドのAES KEYを使用して暗号化されます。
Auto Generate ラジオボックスをオンにすると、コンフィギュレーションファイルはランダムなAES KEYを使用して暗号化されます。設定ファイルのAES キーは異なります。

6. 暗号化をクリックして、設定ファイルを暗号化します。



7. [OK]をクリックします。

ターゲットディレクトリが自動的に開きます。暗号化されたCFG ファイル、暗号化されたキーファイル、および Aeskey.txt ファイルにプレーンテキストのAES キーが保管されています。



ハイブリッドモード

Teams デバイスは、Survivability App モードと Teams App モードのハイブリッドモードをサポートします。この機能は、ローカルMS サーバーとの接続が切断されるシナリオに適しています。また、SIPソリューションから Teamsソリューションに移行する顧客にも適用できます。移行期間中は、企業内に SIP アカウントユーザーと Teams アカウントユーザーの両方が存在し、これら2つのグループがグループ内で相互に通信できるようにします。

- [ハイブリッドモードの設定](#)
- [ページング設定](#)
- [SIP アカウント登録の設定](#)
- [アカウントコーデックの設定](#)
- [ローカルディレクトリの設定](#)

ハイブリッドモードの設定

次の表に、ハイブリッドモードの設定に使用できるパラメータを示します。

パラメータ	features.hybrid_mode.enable	<y0000000000xx>.cfg
説明	ハイブリッドモード機能を有効または無効にします。	
許容値	0-無効にすると、ハイブリッドモードの設定は電話機のユーザーインターフェイスに表示されず、アカウントとディレクトリの設定はウェブユーザーインターフェイスに表示されません。 1-有効	
デフォルト	0	
パラメータ	features.hybrid_mode.quick_ball.enable	<y0000000000xx>.cfg
説明	クイックボールを有効または無効にして、Teams APPとSurvivability APPをすばやく切り替えることができます。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
電話機のUI	☰ 設定 > デバイス設定 > ハイブリッドモード > クイックボール	
パラメータ	features.hybrid_mode.sip_callwaiting.enable	<y0000000000xx>.cfg
説明	これは、SIP 着信コールが割込通話に設定され、フローティングウィンドウがTeamsコール中にSIP 着信コールを要求するように設定します。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	

ページング設定

ハイブリッドモードが有効になっている場合、電話機でページング機能を使用できます。

次の表に、ページング機能の設定に使用できるパラメータを示します。

パラメータ	linekey.X. 型 ^[1]	<y0000000000xx>.cfg
説明	キー機能を設定します。	
許容値	0-N/A 15-Line 24-Paging 66-ページングリスト	
デフォルト	15 (VP59/MP58/MP58-WH/T58A/T56A: X= 1-16; MP54/T55A/CP960: 1) 0 (他の行キー)	

Web UI	DSSキー > ラインキー > ラインキー-X > タイプ	
電話機のUI	☰ > 設定 > デバイス設定 > DSS キー > DSS キー-X > タイプ	
パラメータ	linekey.X. 回線 ^[1]	<y0000000000xx>.cfg
説明	ラインキー機能を適用するように目的のラインを設定します。	
許容値	1	
デフォルト	1	
Web UI	DSSキー > ラインキー > ラインキー-X > ライン	
電話機のUI	☰ > 設定 > デバイス設定 > DSS キー > DSS キー-X > アカウントID	
パラメータ	linekey.X. 数値 ^[1]	<y0000000000xx>.cfg
説明	ラインキー機能の値を設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	DSSキー > ラインキー > ラインキー-X > 値	
電話機のUI	☰ > 設定 > デバイス設定 > DSS キー > DSS キー-X > 値	
パラメータ	linekey.X. 標識 ^[1]	<y0000000000xx>.cfg
説明	電話画面に表示されるラベルを設定します。 これはオプションの設定です。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	DSSキー > ラインキー > ラインキー-X > ラベル	
電話機のUI	☰ > 設定 > デバイス設定 > DSS キー > DSS キー-X > ラベル	
パラメータ	linekey.X. 拡張 ^[1]	<y0000000000xx>.cfg
説明	マルチキャストページンググループのチャンネルを設定します。	
許容値	0 ~ 31	
デフォルト	空白	
Web UI	DSSキー > ラインキー > ラインキー-X > 内線	
電話機のUI	☰ > 設定 > デバイス設定 > DSS キー > DSS キー-X > エクステンション	
パラメータ	features.auto_linekeys.enable	<y0000000000xx>.cfg
説明	特定のアカウントに関連付ける複数の回線キーの割り当てを有効または無効にします。 注意: 行キーの数は“account.X.number_of_linekey”によって決まります。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
パラメータ	Account.X.number_of_linekey ^[2]	<y0000000000xx>.cfg

説明	最初の未使用のアカウントから、特定のアカウントに割り当てるラインキーの数を設定します。 回線キーが使用されている場合、電話機は次の未使用のDSS キーにスキップします。	
許容値	1 ~ 999 の整数	
デフォルト	1	
パラメータ	multicast.codec	<y0000000000xx>.cfg
説明	マルチキャストページング用にコーデックを設定します。	
許容値	PCMU、PCMA、G729、G722	
デフォルト	G722	
パラメータ	multicast.paging_address.X.ip_address ^[3]	<y0000000000xx>.cfg
説明	ページングリスト内のマルチキャストページンググループのIPアドレスとポート番号を設定します。	
許容値	IP アドレス: ポート(224.0.0.1-239.255.255.255 ポート: 0-65535)	
デフォルト	空白	
Web UI	連絡先> マルチキャストIP > ページングリスト> ページングアドレス	
電話機のUI	☰> 設定> デバイス設定> ページングリスト> 編集> アドレス	
パラメータ	multicast.paging_address.X. 標識 ^[3]	<y0000000000xx>.cfg
説明	これは、ページングリストに表示されるマルチキャストページンググループの名前を設定します。マルチキャストページングコールを発信すると、電話画面に表示されます。	
許容値	文字列	
デフォルト	空白	
Web UI	連絡先> マルチキャストIP > ページングリスト> ラベル	
電話機のUI	☰> 設定> デバイス設定> ページングリスト> 編集> ラベル	
パラメータ	multicast.paging_address.X. チャンネル ^[3]	<y0000000000xx>.cfg
説明	ページングリスト内のマルチキャストページンググループのチャンネルを設定します。	
許容値	0:古いファームウェアバージョンまたはYealink Phone を実行しているすべてのYealink Phone がチャンネル0 をリッスンするか、ページンググループ内のサードパーティが使用可能なデバイスがRTP ストリームを受信できます。 1 ~ 25:チャンネルをリッスンするように事前設定された電話機はRTPストリームを受信できます。 26 ~ 30-チャンネルを聴くように事前に構成されたYealink phoneはRTP streamを受信することができます。	
デフォルト	0	
Web UI	連絡先> マルチキャストIP > ページングリスト> チャンネル	
電話機のUI	☰> 設定> デバイス設定> ページングリスト> 編集> チャンネル	
パラメータ	multicast.listen_address.X.ip_address ^[3]	<y0000000000xx>.cfg
説明	電話機がリッスンするマルチキャストアドレスとポート番号を設定します。	

許容値	IP アドレス: ポート(224.0.0.1-239.255.255.255 ポート: 0-65535)	
デフォルト	空白	
Web UI	連絡先> マルチキャストIP > マルチキャストリスニング> リスニングアドレス	
パラメータ	multicast.listen_address.X. 標識 ^[3]	<y0000000000xx>.cfg
説明	マルチキャストページングコールを受信したときに電話画面に表示されるラベルを設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	連絡先> マルチキャストIP > マルチキャストリスニング> ラベル	
パラメータ	multicast.listen_address.X. チャンネル ^[3]	<y0000000000xx>.cfg
説明	電話機がリスンするチャンネルを設定します。	
許容値	<p>0:電話機は、古いファームウェアバージョンを実行している電話機から、チャンネル0 をリスンする電話機から、または使用可能なサードパーティデバイスから、事前設定されたマルチキャストアドレスのRTPストリームを受信できます。</p> <p>1 ~25:電話機は、Yealink 電話機からチャンネル1 ~25 の事前設定されたマルチキャストアドレスのRTP ストリームをそれぞれ受信できます。</p> <p>26 ~30:電話機は、Yealink 電話機からチャンネル26 ~30 の事前設定されたマルチキャストアドレスのRTP ストリームをそれぞれ受信できます。</p>	
デフォルト	0	
Web UI	連絡先> マルチキャストIP > マルチキャストリスティング> チャンネル	
パラメータ	multicast.受信優先度.有効	<y0000000000xx>.cfg
説明	電話機にアクティブなマルチキャストページングコールがある場合に、着信マルチキャストページングコールを処理する電話機を有効または無効にします。	
許容値	<p>0-無効にすると、電話機にアクティブなマルチキャストページングコールがある場合、電話機は着信マルチキャストページングコールを無視します。</p> <p>1-有効にすると、電話機は、優先度の高い着信マルチキャストページングコールを受信し、優先度の低い着信コールを無視します。</p>	
デフォルト	1	
Web UI	連絡先> マルチキャストIP > マルチキャストリスティング> ページングプライオリティアクティブ	
パラメータ	multicast.受信優先度.優先度	<y0000000000xx>.cfg
説明	<p>進行中の音声コール(マルチキャストページングコールではなく通常の電話コール)の優先順位を設定します。</p> <p>1 が最高の優先順位、31 が最低の優先順位です。</p>	

許容値	0:無効。音声があると、すべての着信マルチキャストページングコールが自動的に無視され ます。 通話中です。 1-1 2-2 3-3 ... 31-31 他の値に設定されている場合、電話機は着信マルチキャストページングコールを受信します。 音声電話がかかってきたときに、優先順位の高いものから優先順位の低いものを無視します。 進捗確認
デフォルト	31
Web UI	連絡先> マルチキャストIP > マルチキャストリスナリング> ページング割り込み

[1]X X はラインキーID です。X=1-27 です。

[2]X X はアカウントID です。VP59/MP58/MP58-WH/MP56/T58A/T56A の場合、X=1-16、MP54/T55A/CP960 の場合、X=1 となります。

[3]X X の範囲は1 ~31 です。

SIP アカウント登録の設定

サバイバビリティアプリモードでは、電話機にSIP アカウントを登録できます。

次の表に、SIP アカウント登録の設定に使用できるパラメータを示します。

パラメータ	account.X. イネーブル ^[1]	<MAC>.cfg
説明	特定のアカウントを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	アカウント> 登録> 破線アクティブ	
パラメータ	account.X. 標識 ^[1]	<MAC>.cfg
説明	LCD画面に表示するラベルを設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> ラベル	
パラメータ	account.X.display_name ^[1]	<MAC>.cfg
説明	特定のアカウントの表示名を設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> 表示名	

パラメータ	account.X.auth_name ^[1]	<MAC>.cfg
説明	特定のアカウントのレジスタ認証のユーザー名を設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> 登録名	
パラメータ	account.X.user_name ^[1]	<MAC>.cfg
説明	特定のアカウントの登録ユーザー名を設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	会計> 登録> ユーザー名	
パラメータ	account.X. 暗証番号 ^[1]	<MAC>.cfg
説明	特定のアカウントのレジスタ認証のパスワードを設定します。	
許容値	99文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> パスワード	
パラメータ	account.X.outbound_proxy_enable ^[1]	<MAC>.cfg
説明	電話機がアウトバウンドプロキシサーバに依頼を送信することを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	アカウント> 登録> アウトバウンドプロキシサーバの有効化	
パラメータ	account.X.outbound_proxy.Y. 住所 ^{[1][2]}	<MAC>.cfg
説明	アウトバウンドプロキシサーバYのIPアドレス(またはドメイン名)を設定します。	
許容値	256文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> アウトバウンドプロキシサーバ	
パラメータ	Account.X.outbound_proxy.Y.wanport ^{[1][2]}	<MAC>.cfg
説明	アウトバウンドプロキシサーバYのポートを設定します。	
許容値	0 ~ 65535 の整数	
デフォルト	5060	
Web UI	アカウント> 登録> アウトバウンドプロキシサーバY > ポート	
パラメータ	account.X.outbound_proxy_fallback_interval ^[1]	<MAC>.cfg
説明	フォールバックサーバがコール制御を引き継いだ後、登録要求を送信することによって、機能しているアウトバウンドプロキシサーバが使用可能かどうかを電話機が検出する時間間隔(秒)を設定します。	
許容値	0 ~ 65535 の整数	

デフォルト	3600	
Web UI	アカウント> 登録> プロキシフォールバック間隔	
パラメータ	account.X.sip_server.Y. 住所 ^{[1][2]}	<MAC>.cfg
説明	SIP サーバY のIP アドレス(またはドメイン名)を設定します。	
許容値	256 文字以内の文字列	
デフォルト	空白	
Web UI	アカウント> 登録> SIP サーバY > サーバホスト	
パラメータ	Account.X.sip_server.Y.wanport ^{[1][2]}	<MAC>.cfg
説明	SIPサーバYのポートを構成します。	
許容値	0 ~65535 の整数	
デフォルト	5060	
Web UI	アカウント> 登録> SIP サーバY > ポート	
パラメータ	account.X.sip_server.Y. 期限切れ ^{[1][2]}	<MAC>.cfg
説明	SIPサーバYの登録有効期限(秒)を設定します。	
許容値	30 ~2147483647 の整数	
デフォルト	3600	
Web UI	アカウント> 登録> SIP サーバY > サーバの有効期限	
パラメータ	account.X.sip_server.Y.retry_counts ^{[1][2]}	<MAC>.cfg
説明	SIP サーバY が使用できない場合、またはSIP サーバY からの応答がない場合に、電話機が依頼を再送信する再試行時間を設定します。	
許容値	0 ~20 の整数	
デフォルト	3	
Web UI	アカウント> 登録> SIP サーバY > サーバ再試行回数	
パラメータ	account.X.sip_server.Y.transport_type ^{[1][2]}	<MAC>.cfg
説明	特定のアカウントのトランスポートプロトコルのタイプを設定します。	
許容値	0-UDP 1-TCP 2-TLS 3-DNS-NAPTR は、サーバポートが指定されていない場合、電話機はサービスタイプとポートに対してDNS NAPTR およびSRV クエリを実行します。	
デフォルト	0	
Web UI	アカウント> 登録> SIP サーバY > トランスポート	

[1]X X はアカウントID です。MP58/MP58-WH/MP56/VP59/T58A/T56A の場合はX=1-16、MP54/T55A/CP960 の場合はX=1 となります。

[2]Y はサーバID です。Y=1-2。

アカウントコーデックの設定

サバイバビリティアプリモードでは、特定のアカウントのコーデックを有効にできます。

次の表に、アカウントコーデックの設定に使用できるパラメータを示します。

パラメータ	account.X.codec.<payload_type>.enable ^[1]	<MAC>.cfg
説明	指定されたオーディオコーデックを有効または無効にします。オーディオコードの名称(ペイロードタイプ): g722_1c_48kpbs-G.722.1c(48kb/s) g722_1c_32kpbs-G.722.1c(32kb/s) g722_1c_24kpbs-G.722.1c(24kb/s) g722_1_24kpbs-G.722.1(24kb/s) g722-G722 pcmu-PCMU pcma-PCMA g729-G729 g726_16-G726-16 g726_24-G726-24 g726_32-G726-32 g726_40-G726-40 g723_53-G723_53 g723_63-G723_63 opus-Opus ilbc-iLBC	
許容値	0-Disabled 1-Enabled	

デフォルト	<p>オーディオコーデックがG.722.1c(48kb/s)のときデフォルト値が1、オーディオコーデックがG.722.1c(32kb/s)のときデフォルト値が1、G.722.1c(24kb/s)のときデフォルト値が1、G.722.1(48kb/s)のときデフォルト値が1、G722(G722)のときデフォルト値が1;</p> <p>オーディオコーデックがPCMU の場合はデフォルト値が1、オーディオコーデックがPCMA の場合はデフォルト値が1、オーディオコーデックがG729 の場合はデフォルト値が1、オーディオコーデックがG726-16 の場合はデフォルト値が0、オーディオコーデックがG726-24 の場合はデフォルト値が0、オーディオコーデックがG726-32 の場合はデフォルト値が0、オーディオコーデックがG726-40 の場合はデフォルト値が0、オーディオコーデックがG723_53 の場合はデフォルト値が0、オーディオコーデックがG723_63 の場合はデフォルト値が0、オーディオコーデックがOpus の場合はデフォルト値が0;</p> <p>オーディオコーデックがiLBC の場合、デフォルト値は0 です。</p>	
Web UI	アカウント> コーデック> オーディオコーデック	
パラメータ	account.X.codec.<payload_type>.priority ^[1]	<MAC>.cfg
説明	<p>有効なオーディオコーデックの優先順位を設定します。</p> <p>オーディオコードの名称(ペイロード_タイプ):</p> <p>g722_1c_48kpbs-G.722.1c(48kb/s) g722_1c_32kpbs-G.722.1c(32kb/s) g722_1c_24kpbs-G.722.1c(24kb/s)</p> <p>g722_1_24kpbs-G.722.1(24kb/s)</p> <p>g722-G722</p> <p>pcmu-PCMU</p> <p>pcma-PCMA</p> <p>g729-G729</p> <p>g726_16-G726-16</p> <p>g726_24-G726-24</p> <p>g726_32-G726-32</p> <p>g726_40-G726-40</p> <p>g723_53-G723_53</p> <p>g723_63-G723_63</p> <p>opus-Opus</p> <p>ilbc-iLBC</p>	

許容値	0 ~16 の整数	
デフォルト	オーディオコーデックがG722.1c(48kb/s)の場合、デフォルト値が1、オーディオコーデックがG722.1c(32kb/s)の場合、デフォルト値が2、オーディオコーデックがG722.1c(24kb/s)の場合、デフォルト値が3、オーディオコーデックがG722.1(24kb/s)の場合、デフォルト値が4、オーディオコーデックがG722(G722)の場合、デフォルト値は5となります；オーディオコードがPCMUの場合、デフォルト値が6、オーディオコードがPCMUの場合、デフォルト値が7、オーディオコードがG729の場合、デフォルト値が8、オーディオコードがG726_16の場合、デフォルト値が0、オーディオコードがG726_24の場合、デフォルト値が0、オーディオコードがG726_32の場合、デフォルト値が0、オーディオコードがG726_40の場合、デフォルト値が0、オーディオコードがG723_53の場合、デフォルト値が0、オーディオコードがG723_63の場合、デフォルト値が0、オーディオコードがオパスの場合、デフォルト値は0；オーディオコーデックがiLBC の場合、デフォルト値は0 です。	
Web UI	アカウント> コーデック> オーディオコーデック	
パラメータ	account.X.codec.opus.para ^[1]	<MAC>.cfg
説明	Opus オーディオコーデックのサンプルレートを設定します。	
許容値	opus-fb-Opus-FB (48KHz) opus-swb-Opus-SWB (24KHz) opus-wb-Opus-WB (16KHz) opus-mb-Opus-MB (12KHz) opus-nb-Opus-NB (8KHz)	
デフォルト	opus-fb	
Web UI	アカウント> コーデック> Opus サンプルレート	

[1]X X はアカウントID です。MP58/MP58-WH/MP56/VP59/T58A/T56A の場合はX=1-16、MP54/T55A/CP960 の場合はX=1 となります。

ローカルディレクトリの設定

サバイバビリティアプリモードでは、ローカルの連絡先ファイルをインポートできます。ローカルディレクトリには、最大1000 件の連絡先と48 件のグループを保存できます。

次の表に、ローカルの連絡先ファイルのインポートに使用できるパラメータを示します。

パラメータ	local_contact.data.url	<y0000000000xx>.cfg
説明	ローカル連絡先ファイル(*.xml) のアクセスURL を設定します。	

許容値	511文字以内のURL
デフォルト	空白
Web UI	連絡先> ローカルディレクトリ> ローカルディレクトリファイルのインポート

デバイス管理

デバイス管理機能を有効にすると、電話機の情報をYealink Device Management Platform に報告できます。Yealink Device Management Platform では、電話機の情報を表示したり、電話機を管理したりできます。

- [デバイス管理設定](#)

デバイス管理設定

次の表に、デバイス管理機能の設定に使用できるパラメータを示します。

パラメータ	static.dm.enable ^[1]	<y0000000000xx>.cfg
説明	デバイス管理機能を有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
パラメータ	static.dm.server.address ^[1]	<y0000000000xx>.cfg
説明	デバイス管理プラットフォームのサーバアドレスを設定します。	
許容値	文字列	
デフォルト	空白	
パラメータ	static.dm.server.port ^[1]	<y0000000000xx>.cfg
説明	デバイス管理プラットフォームのポートを設定します。	
許容値	0 ~ 65535 の整数	
デフォルト	443	

[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

USB Camera UVC30 Room の管理

UVC30ルームをVP59Teams 電話機に接続して、テレビ電話をかけることができます。接続後、カメラのファームウェアをアップグレードしたり、カメラログをエクスポートしたりできます。

- [UVC30 カメラのアップグレード](#)
- [カメラログのエクスポート](#)

UVC30 カメラのアップグレード

接続されているUVC30 を最新バージョンにアップデートできます。

手順

1. WEBユーザーインターフェースから、カメラ>アップグレードへ。
2. Upgrade ブロックで、白いボックスをクリックしてローカルシステムから最新のファームウェアを選択します。
3. アップロードをクリックします。
「uvc ファームウェアのアップデートには数分かかります。電源を切らないでください!」と表示されます。
4. [OK]をクリックします。
カメラの現在のファームウェアは、数分後に自動的に更新されます。

カメラログのエクスポート

カメラログをエクスポートして、カメラの問題の分析に役立てることができます。

手順

1. WEBユーザーインターフェースから、カメラ>アップグレードへ。
2. Log ブロックで、Export をクリックしてファイルのダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。

トラブルシューティング方法

Yealink Teams デバイスは、ログファイル、パケット、ステータスインジケータなど、さまざまな形式のフィードバックを提供します。これは、システムの問題をより簡単に見つけて修正するのに役立ちます。

- [ログファイル](#)
- [パケットキャプチャ](#)
- [設定ファイルの分析](#)
- [すべての診断ファイルのエクスポート](#)
- [装置の状況](#)
- [デバイスと設定のリセット](#)
- [デバイスの再起動](#)
- [電話機の現在の画面のキャプチャ](#)

ログファイル

Yealink Teams デバイスは、ブートログとシステムログの2つの異なるログファイルにイベントを記録できます。ログファイルをローカルに生成するか、Syslog サーバにリアルタイムで送信するかを選択できます。これらのログファイルを使用して、情報、分析、およびトラブルシューティングのデバイスを生成できます。

- [ローカルログ](#)
- [Syslog ログ](#)

ローカルログ

ローカルログを有効にし、重大度レベルを指定して、ログをローカルに保持するか、ローカルログファイルをプロビジョニングサーバーにアップロードするかを選択できます。ローカル・ログ・ファイルは、ウェブ・ユーザー・インターフェースを介して同時にエクスポートすることができます。

- [ローカルログ設定](#)
- [ローカルPC へのログファイルのエクスポート](#)
- [ログファイルの表示](#)

ローカルログ設定

次の表に、ローカルログの設定に使用できるパラメータを示します。

パラメータ	Static.local_log.enable	<y0000000000xx>.cfg
説明	<p>ログをローカルに記録するデバイスを有効または無効にします。</p> <p>注意: この機能を無効にしないことをお勧めします。</p>	
許容値	<p>0-無効にすると、デバイスはログファイル(<MAC>-boot.log)へのログの記録を停止し、<MAC>-sys.log) ローカル。以前に記録されたログファイルは、引き続きデバイスに保持されます。</p> <p>1-有効にすると、デバイスはログファイル(<MAC>-boot.log)へのログの記録を続行します。<MAC>-sys.log) ローカル。ローカルログファイルをプロビジョニングサーバーまたは特定のサーバーにアップロードするか、ローカルシステムにエクスポートできます。</p>	
デフォルト	1	
Web UI	設定> 設定/ログ> ローカルログの有効化	
電話機のUI	☰> Settings > Device Settings > Debug(デフォルトパスワード: admin) > Log enable	
パラメータ	Static.local_log.level	<y0000000000xx>.cfg
説明	<p>これは、レンダリングされるローカル・ログ情報の最下位レベルを構成します。<MAC>-sys.log ファイル。</p> <p>ログレベルを選択すると、同等以上の重大度レベルのすべてのイベントが含まれ、それより低い重大度レベルのイベントは除外されます。選択したログレベルによって、ログに記録するイベントの最低重大度が決まります。</p>	
許容値	<p>0-システムが使用不可</p> <p>1-すぐに実行する必要があるアクション</p> <p>2- 重大な状態</p> <p>3-エラー状態</p> <p>4- 警告状態</p> <p>5- 正常だが重大な状態</p> <p>6-informational</p>	
デフォルト	6	
Web UI	設定>設定/ログ> ローカルログレベル	
電話機のUI	☰> 設定 > デバイス設定 > デバッグ(デフォルトパスワード: admin) > ログレベル	
パラメータ	static.local_log.max_file_size	<y0000000000xx>.cfg

説明	<p>デバイスに保存できるログファイル(<MAC>-boot.log および<MAC>sys.log)の最大サイズ(KB)を設定します。</p> <p>このサイズを超えようとしている場合は、</p> <p>(1) パラメータ「static.auto_provision.local_log.backup.enable」によってローカルログファイルがサーバにアップロードされるように設定されている場合、バックアップが正常に完了すると、デバイスはデバイス上のすべてのローカルログファイルをクリアします。</p> <p>(2) 「static.auto_provision.local_log.backup.enable」が0 (Disabled) に設定されている場合、デバイスはデバイスの最も古いログ情報からログの半分を消去します。</p>	
許容値	2048 ~20480 の整数	
デフォルト	20480	
Web UI	設定>設定/ログ> 最大ログファイルサイズ(2048-20480KB)	
パラメータ	static.auto_provision.local_log.backup.enable	<y0000000000xx>.cfg
説明	<p>ローカルログファイル(<MAC>-boot.log)をアップロードするデバイスを有効または無効にします。</p> <p><MAC>-sys.log) プロビジョニングサーバーまたは特定のサーバーへ。</p> <p>メモ: アップロードパスは、パラメータ“static.auto_provision.local_log.backup.path”によって設定されます。</p>	
許容値	<p>0-無効</p> <p>1-有効にすると、次のいずれかの場合に、デバイスはローカルログファイルをプロビジョニングサーバーまたは特定のサーバーにアップロードして、これらのファイルをバックアップします:</p> <ul style="list-style-type: none"> - オートプロビジョニングがトリガーされる; - ローカル・ログ・ファイルのサイズが、パラメータ“static.local_log.max_file_size”によって構成された最大値に達する; - パラメータ「static.auto_provision.local_log.backup.upload_period」で設定されたアップロード期間に従って、ローカルログファイルをアップロードする時間です。 	
デフォルト	0	
パラメータ	static.auto_provision.local_log.backup.upload_period	<y0000000000xx>.cfg
説明	<p>ローカルログファイル(<MAC>-boot.log および<MAC>sys.log)がプロビジョニングサーバーまたは特定のサーバにアップロードされる期間(秒)を設定します。</p> <p>注意: 「static.auto_provision.local_log.backup.enable」が1 (Enabled)に設定されている場合にのみ機能します。</p>	
許容値	30 ~86400 の整数	
デフォルト	30	
パラメータ	static.auto_provision.local_log.backup.path	<y0000000000xx>.cfg

説明	<p>ローカルログファイル(<MAC>-boot.log および<MAC>-sys.log)のアップロードパスを設定します。空白のままにすると、デバイスはローカルログファイルをプロビジョニングサーバーにアップロードします。</p> <p>相対URL (/upload など)を設定すると、デバイスはプロビジョニングサーバのアクセスURLからルートディレクトリを抽出してローカルログファイルをアップロードします。</p> <p>プロトコル(tftp など)を使用して絶対URLを設定すると、デバイスは目的のプロトコルを使用してローカルログファイルをアップロードします。プロトコルがない場合、デバイスはファイルのアップロードにオートプロビジョニングと同じプロトコルを使用します。</p> <p>例:</p> <pre>static.auto_provision.local_log.backup.path= tftp://10.3.6.133/upload/</pre> <p>注意: "static.auto_provision.local_log.backup.enable" が1 (Enabled) に設定されている場合にのみ機能します。</p>	
許容値	1024文字以内のURL	
デフォルト	空白	
パラメータ	static.auto_provision.local_log.backup.append	<y0000000000xx>.cfg
説明	アップロードされたローカルログファイル(<MAC>-boot.log および<MAC>-sys.log)が既存のファイルを上書きするか、既存のファイルに追加されるかを設定します。	
許容値	<p>0- 上書き</p> <p>1- 追加(TFTP サーバには適用されません)</p>	
デフォルト	0	
パラメータ	static.auto_provision.local_log.backup.append.limit_mode	<y0000000000xx>.cfg
説明	プロビジョニングサーバまたは特定のサーバのローカルログファイル(<MAC>-boot.log および<MAC>-sys.log)が最大ファイルサイズに達したときの動作を設定します。	
許容値	<p>0- 削除を追加すると、サーバは古いログを削除し、デバイスはログのアップロードを続行します。</p> <p>1- Append Stop、デバイスはログのアップロードを停止します。</p>	
デフォルト	0	
パラメータ	static.auto_provision.local_log.backup.append.max_file_s	<y0000000000xx>.cfg
説明	ローカルログファイル(<MAC>-boot.log)の最大サイズ(KB)を設定します。 <MAC>-sys.log) は、プロビジョニングサーバまたは特定のサーバに保存できます。	
許容値	200 ~65535 の整数	
デフォルト	1024	
パラメータ	static.auto_provision.local_log.backup.bootlog.upload_wait_ti	<y0000000000xx>.cfg
説明	デバイスが起動後にローカルログファイル(<MAC>-boot.log)をプロビジョニングサーバまたは特定のサーバにアップロードするまでの待機時間(秒)を設定します。	
許容値	1 ~86400 の整数	

ローカルPC プロシージャへのログファイル

のエキスポート

1. Webユーザーインターフェースから、「設定」>「設定」>「ローカルログ」に進みます。
2. ローカルログの有効化をオンにする
3. 「ローカルログレベル」ドロップダウンメニューから目的の値を選択します。
デフォルトのローカル・ログ・レベルは“6”です。
4. 「最大ログ・ファイル・サイズ」フィールドにログ・ファイルの制限サイズを入力します。
5. Confirm(確認)をクリックして変更を受け入れます。
6. 問題を再現します。
7. エクスポートをクリックしてファイルのダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。

ログファイルの表示

正しいログが得られたかどうかは、次のキーフィールドで確認できます：

- <0+emerg>
- <1+アラート>
- <2+crit>
- <3+エラー>
- <4+warning>
- <5+notice>
- <6+情報>

デフォルトのローカル・ログ・レベルは6です。

次の図は、ブートログファイルの一部(805EC031960A-boot.log など)を示しています：

```

0 10 20 30 40 50 60 70 80 90 100
1 <46>Thu Jan 1 08:00:09 syslogd started: BusyBox v1.10.3
2 <128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
3 <128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
4 <128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > Version :1.2.1.7 for release
5 <128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
6 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
7 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
8 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
9 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
10 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
11 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
12 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
13 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
14 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
15 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
16 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
17 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
18 <131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
19 <128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
20 <128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > Version :1.0.0.6 for release
21 <128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
22 <128>Jan 1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
23 <133>Jan 1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
24 <46>Thu Jan 1 08:00:12 syslogd started: BusyBox v1.10.3
25 <128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
26 <128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
27 <128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > Version :8.0.1.3 for release
28 <128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
29 <128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
30 <132>Jan 1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
31 <134>Jan 1 08:00:12 sys [532]: SRV <6+info > running in normal mode, mode 0
32 <134>Jan 1 08:00:12 sys [532]: SRV <6+info > Set Init SystemTime: 2018-11-23
33 <134>Nov 23 00:00:00 sys [532]: SRV <6+info > emac get: wan speed 0000003f, lan speed 0000003f
34 <134>Nov 23 00:00:00 sys [532]: SRV <6+info > wan_support_speed 0000005f, lan_support_speed 0000005f

```

boot.log ファイルは、すべての重大度レベルのログを報告しま

す。次の図は、sys ログファイルの一部を示しています：

```

0 .....10.....20.....30.....40.....50.....60.....70.....80.....90.....100
1|<46>Thu Jan 1 08:00:09 syslogd started: BusyBox v1.10.3
2|<128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
3|<128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
4|<128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > Version :1.2.1.7 for release
5|<128>Jan 1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
6|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
7|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
8|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
9|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
10|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
11|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
12|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
13|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
14|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
15|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
16|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
17|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
18|<131>Jan 1 08:00:11 cfg [316]: CFG <3+error > invalid key without '.'
19|<128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
20|<128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > Version :1.0.0.6 for release
21|<128>Jan 1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
22|<128>Jan 1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
23|<133>Jan 1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
24|<46>Thu Jan 1 08:00:12 syslogd started: BusyBox v1.10.3
25|<128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
26|<128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
27|<128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > Version :8.0.1.3 for release
28|<128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
29|<128>Jan 1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
30|<132>Jan 1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
31|<134>Jan 1 08:00:12 sys [532]: SRV <6+info > running in nomal mode, mode 0
32|<134>Jan 1 08:00:12 sys [532]: SRV <6+info > Set Init SystemTime: 2018-11-23
33|<134>Nov 23 00:00:00 sys [532]: SRV <6+info > emacs get: wan speed 0000003f, lan speed 0000003f
34|<134>Nov 23 00:00:00 sys [532]: SRV <6+info > wan_support_speed 0000005f, lan_support_speed 0000005f
35|<134>Nov 23 00:00:00 sys [532]: SRV <6+info > set client

```

<MAC>-sys.log ファイルは、設定された重要度レベル以上のログを報告します。たとえば、<MAC>-sys.log ファイルに報告されるログの重大度レベルを4 に設定した場合、重大度レベルが0 ~4 のログがすべて報告されます。

Syslog ログ

Syslog メッセージをSyslog サーバにリアルタイムで送信するようにデバイスを設定することもできます。

IP アドレスやホスト名、サーバタイプ、ファシリティ、ログに記録するイベントの重大度レベルなどのSyslog の詳細を指定できます。また、メッセージのログにデバイスのMAC アドレスを付加することもできます。

- [Syslog ログ設定](#)
- [Syslog サーバでのSyslog メッセージの表示](#)

Syslog ログ設定

次の表に、syslog ロギングの設定に使用できるパラメータを示します。

パラメータ	static.syslog.enable	<y0000000000xx>.cfg
説明	Syslog サーバにログメッセージをリアルタイムでアップロードするデバイスを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	設定>設定/ログ> Syslog > Syslog の有効化	
パラメータ	static.syslog.server	<y0000000000xx>.cfg
説明	Syslog サーバにログをエクスポートするときに、Syslog サーバのIP アドレスまたはドメイン名を設定します。	
許容値	IPアドレスやドメイン名	

デフォルト	空白	
Web UI	設定 > 設定 > Syslog > Syslog サーバ	
パラメータ	static.syslog.server_port	<y0000000000xx>.cfg
説明	Syslog サーバのポートを設定します。 例: static.syslog.port= 515	
許容値	1 ~ 65535 の整数	
デフォルト	514	
Web UI	設定 > 設定 > Syslog > Syslog サーバ > ポート	
パラメータ	static.syslog.transport_type	<y0000000000xx>.cfg
説明	Syslog サーバにログメッセージをアップロードするときにデバイスが使用するトランスポートプロトコルを設定します。	
許容値	0-UDP 1-TCP 2-TLS	
デフォルト	0	
Web UI	設定 > 設定/ログ > Syslog > Syslog 転送タイプ	
パラメータ	static.syslog.level	<y0000000000xx>.cfg
説明	Syslog に表示される Syslog 情報の最下位レベルを設定します。 ログレベルを選択すると、同等以上の重大度レベルのすべてのイベントが含まれ、それより低い重大度レベルのイベントは除外されます。選択したログレベルによって、ログに記録するイベントの最低重大度が決まります。	
許容値	0- 緊急: システムが使用不可 1- アラート: アクションをただちに実行する必要があります 2- Critical: 重大な状態 3- Critical: エラー状態 4- 警告: 警告条件 5- 警告: 正常だが重大な状態 6- Informational: informational messages	
デフォルト	6	
Web UI	設定 > 設定 > Syslog > Syslog レベル	
パラメータ	static.syslog.facility	<y0000000000xx>.cfg
説明	ログメッセージを生成する機能を設定します。 注記: 詳細については、RFC 3164 を参照してください。	

許容値	0-カーネルメッセージ 1-ユーザーレベルのメッセージ 2-mail system 3-システムデーモン 4-syslogd 6-line printer subsystem(よって内 部的に生成されるセキュリティ/許可メッセージ (注1)5-messages 7-ネットワークニュースサブシステム 8-UUCPサブシステム 9-クロックデーモン(注2) 10-セキュリティ/許可メッセージ(注1) 11-FTPデーモン 12-NTP サブシステ ム13 ログ監査(注1) 14 ログアラート(注1) 15- クロックデーモン(注2) 16- 局所使用 0(local0) 17- 局所使用 1(local1) 18- 局所使用 2(local2) 19- 局所使用 3(local3) 20- 局所使用 4(local4) 21- 局所使用 5(local5) 22- 局所使用 6(local6) 23-局所使用7(local7)	
デフォルト	16	
Web UI	設定> 設定> Syslog > Syslog 機能	
パラメータ	static.syslog.prepend_mac_address.enable	<y0000000000xx>.cfg
説明	Syslog サーバにエクスポートされたログメッセージの前にMAC アドレスを追加するデバイスを有効または無効にします。	
許容値	0-Disabled 1-Enabled	
デフォルト	0	
Web UI	設定>設定/ログ> Syslog > Syslog Prepend MAC	

Syslog サーバでのSyslog メッセージの表示

syslogファイルは、syslog server上の希望のファイルに表示することができます。syslog サーバと場所が異なる場合があります。詳細については、ネットワークリソースを参照してください。

次の図に、syslog の一部を示します:

```

Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection, Java:239)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection, Java:222)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http2.Http2Codec.writeRequestHeaders(Http2Codec, Java:1111)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.CallServerInterceptor.intercept(CallServerInterceptor, Java:50)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:121)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.proxy.GlobalRequestInterceptor.intercept(GlobalRequestInterceptor, Java:291)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.connection.ConnectInterceptor.intercept(ConnectInterceptor, Java:45)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:121)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.cache.CacheInterceptor.intercept(CacheInterceptor, Java:93)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:121)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.BridgeInterceptor.intercept(BridgeInterceptor, Java:93)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:126)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain, Java:121)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at okhttp3.RealCall.getResponseWithInterceptorChain(RealCall, Java:200)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at retrofit2.RealCall.execute(RealCall, Java:77)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at retrofit2.OkHttpCall.execute(OkHttpCall, Java:180)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at retrofit2.ExecutorCallAdapterFactory$ExecutorCallbackCall.execute(ExecutorCallAdapterFactory, Java:91)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.HttpCallExecutor$RetrofitRequestExecutor.execute(HttpCallExecutor, Java:459)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.HttpCallExecutor.executeInternal(HttpCallExecutor, Java:216)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor, Java:147)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor, Java:129)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor, Java:118)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.service.files.PresenceServiceAppData.setUnfi@dPresence(PresenceServiceAppData, Java:299)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.data.AppData.setMyStatus(AppData, Java:2240)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at com.microsoft.skype.teams.calling.call.CallPresenceCall.handleMessage(CallPresence, Java:66)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at android.os.Handler.dispatchMessage(Handler, Java:90)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at android.os.Looper.loop(Looper, Java:135)
Nov 22 00:09:35 apic[590]: ANDR<3>error > 1155 1524 E SetUnfi@dPresence: at android.os.HandlerThread.run(HandlerThread, Java:61)

```

パケットキャプチャ

パックは、ウェブ・ユーザー・インターフェースを介してパックを取り込むか、イーサネット・ソフトウェアを利用するかの二つの方法で取り込むことができます。トラブルシューティングの目的で、キャプチャされたパケットを分析できます。

- WEB ユーザー・インターフェースを通じた、パケットの取り込み
- イーサネットソフトウェアキャプチャ設定

WEB ユーザー・インターフェースを通じた、パケットの取り込み

Yealink Teams デバイスの場合は、パケットファイルをローカルシステムにエクスポートして分析できます。Yealink Teams デバイスは、パケットをキャプチャするために次の2つのモードをサポートします:

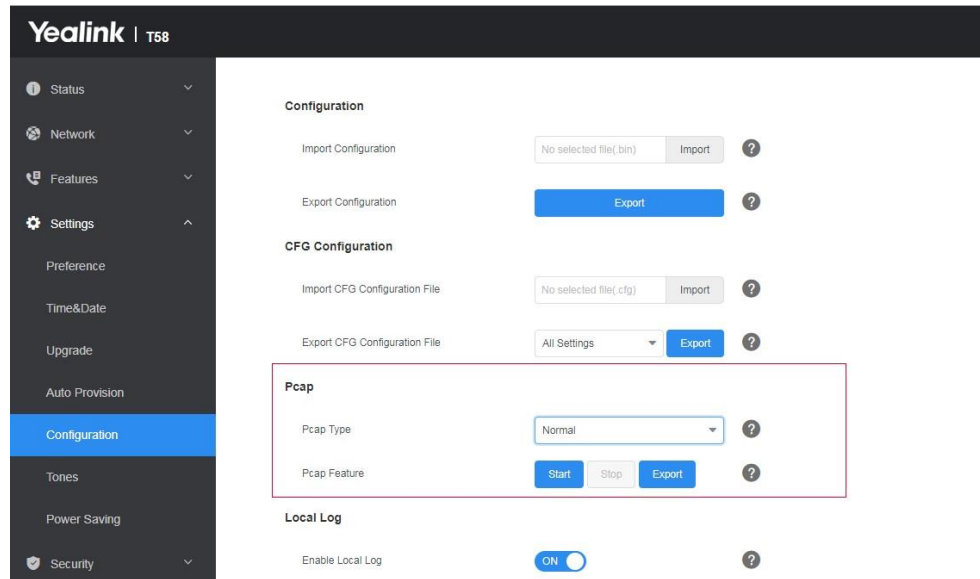
- **Normal:**キャプチャ停止後にパケットファイルをエクスポートします。
- **拡張:**キャプチャ中にパケットファイルをエクスポートします。
- 通常の方法でのパケットのキャプチャ
- 拡張された方法でのパケットのキャプチャ

通常の方法でのパケットのキャプチャ

手順

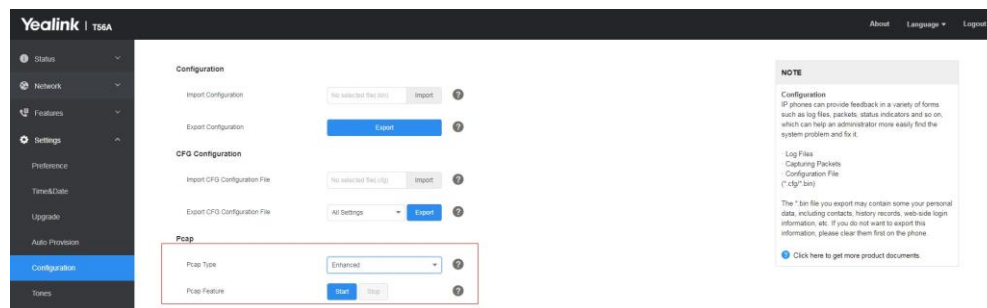
1. Webユーザーインターフェースから、「設定」>「設定」に進みます。
2. 「Pcap 種別」ドロップダウンメニューから「通常」を選択します。
3. 「Pcap 機能」フィールドで、「開始」を選択して信号トラフィックのキャプチャを開始します。
4. 問題を再現して、スタックトレースを取得します。
5. Pcap Feature フィールドでStop をクリックしてキャプチャを停止します。

6. Export(エクスポート)をクリックしてファイルのダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。



エンハンス手順でのパケットのキャプチャ

1. Webユーザーインターフェースから、「設定」>「設定」に進みます。
2. 「Pcap 種別」ドロップダウンメニューから「拡張」を選択します。
3. 「Pcap 機能」フィールドの「開始」を選択して、信号トラフィックのキャプチャを開始します。
4. 問題を再現して、スタックトレースを取得します。
5. Pcap Feature フィールドでStop をクリックしてキャプチャを停止します。
6. Export(エクスポート)をクリックしてファイルのダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。



イーサネットソフトウェアキャプチャ設定

イーサネットソフトウェアを使用したパケットのキャプチャは、次の2つの方法で選択できます:

- HUB からのデータパケットの受信: デバイスとPC のインターネットポートを同じHUB に接続してから、Sniffer、Ethereal、またはWireshark ソフトウェアを使用して信号トラフィックをキャプチャします。
- PC ポートからのデータパケットの受信: 電話機のインターネットポートをインターネットに接続し、電話機のPCポートをPC に接続します。信号トラフィックをキャプチャする前に、電話機がインターネットポートから受信したデータパケットをPC ポートにスパンできることを確認してください。CP960 電話機には適用されません。
- [スパン対PC ポートの設定](#)

ミラーリング ポートの設定

次の表に、PC ポートへのミラーリング設定するために使用できるパラメータを示します。

パラメータ	static.network.span_to_pc_port ^[1]	<y0000000000xx>.cfg
説明	WANポートからPCポートに受信されたデータパックにわたるデバイスを可能にするか、無効にします。 注意: “static.network.pc_port.enable” が1 (Auto Negotiation) に設定されている場合にのみ機能します。	
許容値	0-無効 1-有効にすると、インターネットポートからのすべてのデータパケットをPCポートで受信できます。	
デフォルト	0	
Web UI	ネットワーク > 高度な設定 > ミラーリング > PCポートにミラーリング	

[1]このパラメータを変更すると、変更を有効にするために電話機が再起動します。

設定ファイルの分析

設定が間違っていると、デバイスへの影響が悪くなる場合があります。設定ファイルをエクスポートして、デバイスの現在の設定を確認し、必要に応じてトラブルシューティングを行うことができます。また、設定ファイルをインポートして、すばやく簡単に設定を行うこともできます。

デバイスの現在の設定を変更するには、BINファイルの代わりにエクスポートされたCFGファイルを編集することをお勧めします。config.bin ファイルは暗号化されたファイルです。config.bin ファイルの詳細については、Yealink 販売店にお問い合わせください。

- [デバイスからのBINファイルのエクスポート](#)
- [デバイスからBINファイルをインポートする](#)

デバイスからのBINファイルのエクスポート

手順

1. Webユーザインターフェースから、Settings > Configuration > Configurationに進んでください。
2. Export Configuration ブロックで、Export をクリックしてファイルダウンロードウィンドウを開き、ファイルをローカルシステムに保存します。

デバイスからBINファイルをインポートする

手順

1. Webユーザインターフェースから、Settings > Configuration > Configurationに進んでください。
2. Import Configuration ブロックで、白いボックスをクリックしてローカルシステムからBIN 設定ファイルを選択します。
3. 「インポート」をクリックして、構成ファイルをインポートします。

- [BINファイルのインポートURL設定](#)

BINファイルのインポートURL設定

次の表に、BINファイルのインポートURLの設定に使用できるパラメータを示します。

パラメータ	static.configuration.url ^[1]	<y0000000000xx>.cfg
説明	カスタム設定ファイルのアクセスURL を設定します。 メモ: カスタム設定ファイルのファイル形式は*.bin である必要があります。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	設定> 設定/ログ> 設定インポート	


[1]このパラメータを変更すると、デバイスが再起動して変更が有効になります。

すべての診断ファイルのエクスポート

Yealink デバイスは、問題の分析に役立つ3種類の診断ファイル(Pcapトレース、ログファイル(boot.log および sys.log)とBIN 設定ファイルを含む)をサポートしています。これらのファイルは、必要に応じて一度にエクスポートしてトラブルシューティングできます。エクスポートされた診断ファイルのファイル形式は*.tar です。

手順

1. Webユーザーインターフェースから、「設定」>「設定」に進みます。
2. 「すべての診断ファイルのエクスポート」フィールドで「開始」を選択して、信号トラフィックのキャプチャを開始します。システムログレベルは自動的に6に設定されます。
3. 問題を再現します。
4. Export All Diagnostic Files(すべての診断ファイルのエクスポート)フィールドで Stop(停止)をクリックしてキャプチャを停止します。
5. Export(エクスポート)をクリックしてファイルのダウンロードウィンドウを開き、診断ファイルをローカルシステムに保存します。<MAC>-DiagnoseInfo.tarDiagnoseInfo.tar という名前の診断ファイルがローカルシステムに正常にエクスポートされます。

注: 診断ファイルをエクスポートした後、ticket.yealink.com でチケットを作成し、問題を説明することができます。その後、Yealink サポートTeamsが根本原因の特定に役立ちます。

装置の状況

デバイスステータスに関する利用可能な情報:

- バージョン情報(ファームウェアバージョン、ハードウェアバージョン、パートナーAPPバージョン、企業ポータルバージョン、Teamsバージョン)。
- ネットワークステータス(IPv4 ステータスまたはIPv6 ステータス、およびIP モード)。
- デバイス証明書
- デバイスステータス(MACアドレスとデバイスタイプ)
- [デバイスステータスの表示](#)

デバイスステータスの表示

> 設定> デバイス設定に移動すると、電話のユーザーインターフェイスからデバイスのステータスを表示できます。
> バージョン情報。デバイスのステータスは、ウェブユーザーインターフェイスを使用して表示することもできます。

手順

1. コンピュータでWeb ブラウザを開きます。
2. ブラウザーの住所バーにIPアドレスを入力し、キーを押します。
たとえば、IPv4 の場合は「http://192.168.0.10」、IPv6 の場合は「http://[2005:1:1:1:215:65ff:fe64:6e0a]」です。
3. ログインページにユーザー名(admin)とパスワード(admin)を入力します。
4. ログインをクリックしてログインします。
デバイスステータスは、Webユーザインターフェースの最初のページに表示されます。

デバイスと設定のリセット


一般的に、デバイスの使用中にいくつかの一般的な問題が発生することがあります。すべてのトラブルシューティングの提案を試しても、デバイスを工場出荷時の構成にリセットできますが、問題は解決しません。デバイスを工場出荷時の設定にリセットすると、フラッシュパラメータがクリアされ、ログファイル、ユーザーデータ、キャッシュされたデータが削除され、管理者パスワードがadmin にリセットされます。リセットすると、すべてのカスタム設定が上書きされます。

- [デバイスをデフォルトの工場出荷時設定にリセットする](#)
- [デバイスをカスタム出荷時設定にリセットする](#)
- [カスタム出荷時設定ファイルの削除](#)

デバイスをデフォルトの工場出荷時設定にリセットする

手順

1. Webユーザインターフェースから、「設定」>「アップグレード」をクリックします。
2. 「Reset to Factory」フィールドで「Reset to Factory」をクリックします。
WEBユーザインターフェースは、「工場にリセットしたいか?」というメッセージを促す。
3. 「OK」をクリックしてリセットを確認します。
起動後、デバイスは工場出荷時の状態に正常にリセットされます。

注: デバイスのリセットには数分かかる場合があります。デバイスが正常に起動するまで電源を切らないでください。

デバイスをカスタム出荷時設定にリセットする

カスタム出荷時設定機能を有効にしたら、カスタム出荷時設定ファイルをインポートしてから、デバイスをカスタム出荷時設定にリセットできます。

手順

1. Webユーザインターフェースから、「設定」>「設定」>「ファクトリー設定」をクリックします。
 2. 「Import Factory Configuration」フィールドで、白いボックスをクリックしてローカルシステムからカスタムの出荷時設定ファイルを選択します。
 3. インポートをクリックします。
カスタム出荷時設定ファイルが正常にインポートされたら、デバイスをカスタム出荷時設定にリセットできます。
- [カスタム出荷時設定](#)

カスタム出荷時設定

次の表に、カスタムファクトリの設定に使用できるパラメータを示します。

パラメータ	静的機能。custom_factory_config.enable	<y0000000000xx>.cfg
説明	Custom Factory Configuration(カスタム工場設定)機能を有効または無効にします。	

許容値	0-無効 1-有効にすると、「Import Factory Configuration」項目がデバイスのWeb ユーザーインターフェースのパス「設定」>「Configuration」に表示されます。カスタムファクトリーの構成ファイルをインポートするか、ウェブユーザーインターフェースを介してユーザーが定義した工場構成を削除することができます。	
デフォルト	0	
パラメータ	static.custom_factory_configuration.url	<y0000000000xx>.cfg
説明	カスタム出荷時設定ファイルのアクセスURL を設定します。 注意: "static.features.custom_factory_config.enable" が1 (Enabled) に設定され、カスタム出荷時設定ファイルのファイル形式が*.bin である必要がある場合にのみ機能します。	
許容値	511文字以内のURL	
デフォルト	空白	
Web UI	設定> アップグレード> 出荷時設定にリセット	

カスタム出荷時設定ファイルの削除

ユーザ定義の工場設定をWebユーザーインターフェースで削除できます。

手順

1. Webユーザーインターフェースから、「設定」>「設定」>「ファクトリー設定」をクリックします。
2. 「工場出荷時設定の削除」フィールドから「削除」をクリックします。
WEBユーザーインターフェースは、「ユーザーが定義した工場構成を確実に削除しているか」というメッセージを促す。
3. OK をクリックして、カスタム出荷時設定ファイルを削除します。
インポートしたカスタムファクトリーファイルが削除されます。リセット後、デバイスはデフォルトの工場出荷時設定にリセットされます。


デバイスの再起動

デバイスをローカルで再起動できます。

- [電話機のユーザーインターフェイスを使用したデバイスの再起動](#)
- [ウェブ・ユーザー・インターフェイスを使ったデバイスの再ブート](#)

電話機のユーザーインターフェイスを使用したデバイスの再起動

手順

1. 移動先  > 設定 > デバイス設定 > 再起動。
2. 電話機の再起動を選択します。
デバイスを再起動するかどうかを確認するプロンプトが表示されます。
3. [OK]を選択します。

ウェブ・ユーザー・インターフェースを使ったデバイスの再ブート

手順

1. 設定 > アップグレードをクリックします。
2. Reboot(再起動)をクリックしてデバイスを再起動します。
WEBユーザー・インターフェースは、メッセージ「システムの再起動?」を促す。
3. OK をクリックして、再起動を確定します。
デバイスは再起動時に開始されます。デバイスの再起動には数分かかる場合があります。

電話機の現在の画面のキャプチャ

アクションURIを使用して、電話機の画面表示をキャプチャできます。電話機はHTTP またはHTTPS GET 依頼を処理できます。URIフォーマットは、`http(s)://<deviceIPAddress>/screencapture`である。撮影した画像はBMPまたはJPEG形式で保存されます。


URI「`http(s)://<deviceIPAddress>/screencapture/download`」を使用して画面表示をキャプチャしてから、画像(JPGファイルとして保存され、電話機モデルとキャプチャ時間で名前が付けられます)をローカルシステムにダウンロードすることもできます。

電話機の現在の画面をキャプチャする前に、電話機のAction URI の信頼できるIP アドレスにコンピュータのIP アドレスが含まれていることを確認します。画面表示をキャプチャすると、WebブラウザがWebユーザインターフェースログインのユーザー名とパスワードを覚えていない場合、IP電話から管理者のユーザー名とパスワードを入力するように指示される場合があります。

- [電話機のユーザーインターフェースを使用した画面キャプチャの有効化](#)
- [Webユーザーインターフェースを介した装置の現在のスクリーニングの取得](#)

電話機のユーザーインターフェースを使用した画面キャプチャの有効化

手順

1. 移動先  > Settings > Device Settings > Debug (デフォルトパスワード: admin) > Screen Capture.
2. スクリーンキャプチャを有効にします。

Webユーザーインターフェースを介した装置の現在のスクリーニングの取得

始める前に

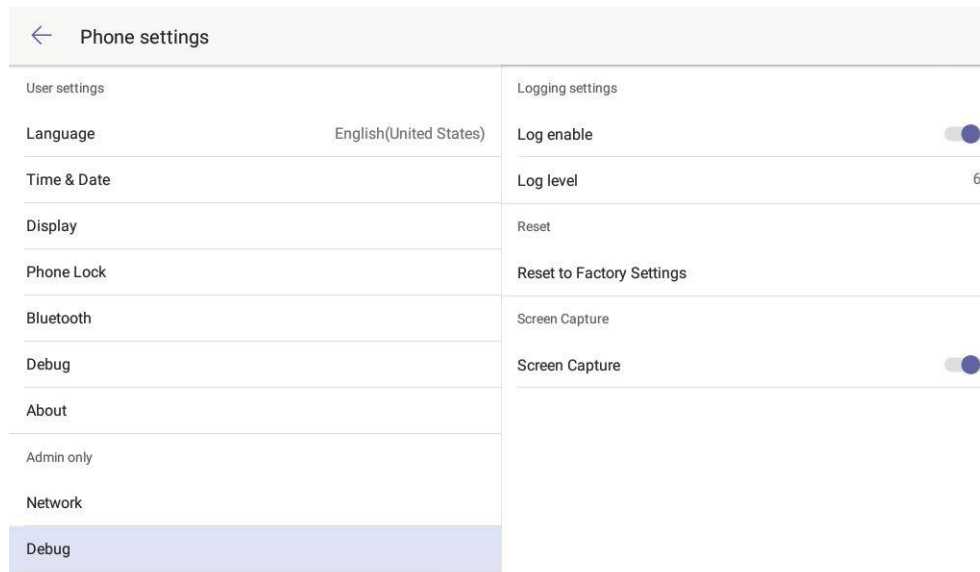
電話機の現在の画面をキャプチャする前に、電話機のユーザーインターフェースを介して画面キャプチャ機能が有効になっていることを確認します。

手順

リクエストURI を入力します(たとえば、ブラウザーのアドレスバーで`http://10.2.20.252/screencapture`)を入力し、キーボードのエンターキーを押します)。

コンピュータを使用して電話機の現在の画面を初めてキャプチャする場合は、WebブラウザがWebユーザインターフェースログインのユーザー名とパスワードを記憶していない場合は、管理者のユーザー名とパスワードを入力するように求められます。

ブラウザには、電話機の現在の画面の画像が直接表示されます。イメージをローカルシステムに保存できます。



トラブルシューティングソリューション

このセクションでは、Teams デバイスの使用中に発生する可能性がある一般的な問題の解決策について説明します。このセクションに記載されていないケースが発生した場合は、Yealink 販売店にお問い合わせください。

- [IP アドレスの問題](#)
- [日時の問題](#)
- [ディスプレイの問題](#)
- [ファームウェアとアップグレードの問題](#)
- [システムログの問題](#)
- [パスワードの問題](#)

IP アドレスの問題

- [デバイスがIP アドレスを取得しない](#)
- [IP コンフリクト](#)
- [YealinkデバイスでIPv6を設定する際の特定のフォーマット](#)

デバイスがIP アドレスを取得しない

次のいずれかを実行します:

- イーサネットケーブルがデバイスのインターネットポートに接続されていて、イーサネットケーブルが緩んでいないことを確認します。
- イーサネットケーブルが損傷していないことを確認します。
- IP アドレスと関連するネットワークパラメータが正しく設定されていることを確認します。
- ネットワークスイッチまたはハブが動作可能であることを確認します。

IP コンフリクト

次のいずれかを実行します:

- デバイスで使用可能な別のIP アドレスをリセットします。

- パスの電話ユーザインターフェイスを介してネットワーク設定を確認します。☰ > 設定 > デバイス設定 > (管理者のみ(既定のパスワード: admin) > ネットワーク) > WAN ポート > IPv4 種別(またはIPv6)。「Static IP」を選択した場合は、代わりに「DHCP」を選択します。

YealinkデバイスでIPv6を設定する際の特定のフォーマット

シナリオ1:

デバイスがIPv6住所を取得した場合、ウェブユーザインターフェイスにアクセスするURLの形式は、「[IPv6住所]」または「http(s):/[IPv6住所]」です。

たとえば、デバイスのIPv6 アドレスが「fe80::204:13ff:fe30:10e」の場合、Web ユーザーインターフェイスにアクセスするには、PC のWeb ブラウザのアドレスバーにURL (たとえば、「[fe80::204:13ff:fe30:10e]」または「http(s)://[fe80:204:13ff:fe30:10e]」) を入力できます。

シナリオ2:

Yealink デバイスは、FTP、TFTP、HTTP、およびHTTPS プロトコルを使用した設定ファイルまたはリソースファイルのダウンロードをサポートしています。これらのプロトコルのいずれかをプロビジョニングに使用できます。

IPv6 アドレスを取得するためにデバイスをプロビジョニングする場合、プロビジョニングサーバーはIPv6 をサポートし、プロビジョニングサーバーのアクセスURL の形式は「tftp://[IPv6 アドレスまたはドメイン名]」にすることができます。たとえば、プロビジョニングサーバーアドレスが「2001:250:1801::1」の場合、プロビジョニングサーバーのアクセスURL は「tftp://[2001:250:1801::1]/」にすることができます。プロビジョニングの詳細については、『Yealink Teams HD IP Phones Auto Provisioning Guide』を参照してください。

日時の問題

- [時刻・日付が正しく表示されない](#)

時刻・日付が正しく表示されない

デバイスがNTP サーバから時刻と日付を自動的に取得するように設定されているかどうかを確認します。デバイスがNTP サーバにアクセスできない場合は、時刻と日付を手動で設定します。

ディスプレイの問題

- [デバイスの LCD 画面のダミー](#)
- [デバイスに「オフライン」と表示される](#)

デバイスの LCD 画面のダミー

次のいずれかを実行します:

- デバイスが機能的なACアウトレットに適切に接続されていることを確認します。
- デバイスがオンになっているスイッチで制御されるソケットに接続されていることを確認します。
- デバイスが電源タップに接続されている場合は、コンセントに直接接続します。
- デバイスの電源がPoEの場合は、PoE準拠のスイッチまたはハブを使用していることを確認します。

デバイスに「オフライン」と表示される

デバイスに利用可能なネットワークがない場合、デバイスは「オフライン」と表示されます。デバイスが有線ネットワークに接続されていることを確認します。

ファームウェアとアップグレードの問題

- デバイスファームウェアのアップグレードに失敗する
- デバイスは設定を更新しません。

デバイスファームウェアのアップグレードに失敗する

次のいずれかを実行します:

- ターゲットファームウェアが現在のファームウェアと同じでないことを確認します。
- ターゲットファームウェアがデバイスモデルに適用可能であることを確認します。
- 現在のファームウェアまたはターゲットファームウェアが保護されていないことを確認します。
- アップグレード中に電源がオンで、ネットワークが使用可能であることを確認します。
- ウェブユーザーインターフェイスを介してファームウェアをアップグレードする際に、ウェブブラウザが閉じられていないか、更新されていないことを確認する。

デバイスは設定を更新しません。

次のいずれかを実行します:

- 構成が正しく設定されていることを確認します。
- デバイスを再起動します。一部の構成では、有効にするために再起動が必要です。
- 構成がデバイスモデルに適用可能であることを確認します。
- 構成は、サーバーからのサポートに依存する場合があります。

システムログの問題

- プロビジョニングサーバー(FTP/TFTP サーバー)からシステムログをエクスポートできませんでした
- Syslog サーバからのシステムログのエクスポートに失敗する

プロビジョニングサーバー(FTP/TFTP サーバー)からシステムログをエクスポートできませんでした

次のいずれかを実行します:

- FTP/TFTP サーバがダウンロードされ、ローカルシステムにインストールされていることを確認します。
- デバイスのWeb ユーザーインターフェイスを介してFTP/TFTP サーバアドレスが正しく設定されていることを確認します。
- デバイスを再起動します。設定を有効にするには、再起動が必要です。

Syslog サーバからのシステムログのエクスポートに失敗する

次のいずれかを実行します:

- syslog サーバが、デバイスからエクスポートされたsyslog ファイルを保存できることを確認します。
- デバイスのWeb ユーザーインターフェイスを介してsyslog サーバアドレスが正しく設定されていることを確認します。
- デバイスを再起動します。設定を有効にするには、再起動が必要です。

パスワードの問題

- [管理者パスワードを復元する](#)

管理者パスワードを復元する

工場出荷時にリセットすると、デフォルトのパスワードを復元できます。すべてのカスタム設定は、リセット後に上書きされます。