



Lenovo

ThinkSmart View

検証ガイド

このドキュメントは、お客さまが製品を展開いただく際の参考用途として作成したものです。ソフトウェアの仕様変更などにより、本ドキュメントの記載事項と実際の設定内容は異なる場合がありますので、ご了承ください。本ドキュメントに記載の内容を実行した結果として生じた接続性に関する問題やデータの消去などの影響について責任を負いかねます。あらかじめご了承ください。



初めに

本書について

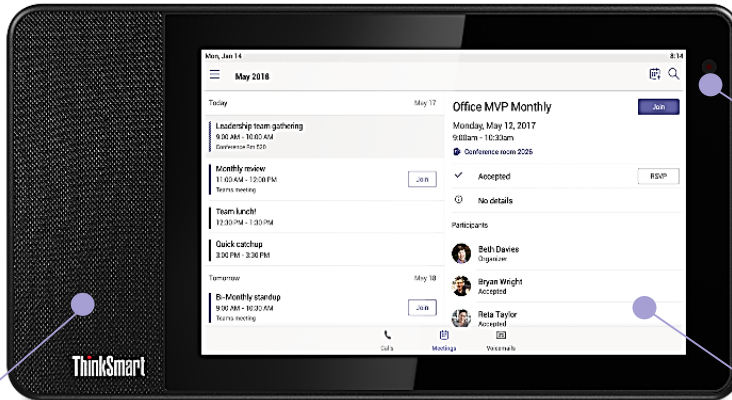
このドキュメントは、ThinkSmart Viewをお客さま環境で検証いただくにあたって一般的に必要な手順をまとめたものです。ハードウェアの紹介、事前準備～初期設定に加え、使い方、管理までをカバーしています。

目次

- 第1章 ThinkSmart Viewの外観
- 第2章 事前準備と初期設定
- 第3章 ThinkSmart View使いこなす
- 第4章 デバイス設定
- 第5章 デバイス管理
- 第6章 PowerShellの活用

第1章 ThinkSmart Viewの外観

正面

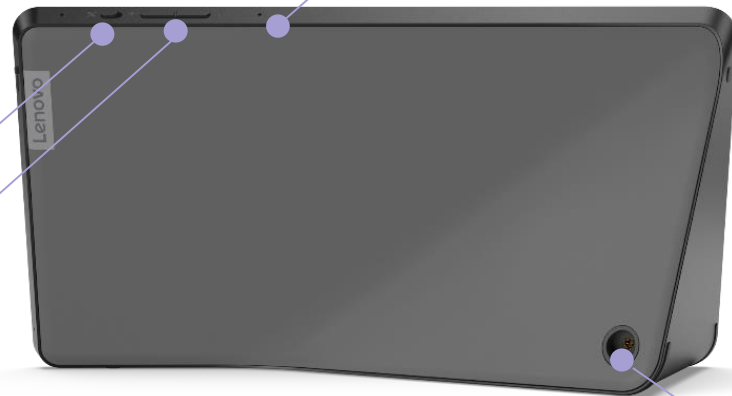


5Mピクセルカメラ
(プライバシーシャッター付き)

スピーカー

8"マルチタッチパネル

背面



マイク

マイクミュートスイッチ

ボリュームボタン

電源ジャック

右側面



プライバシーシャッタースイッチ

左側面



第2章 事前準備と初期設定

事前準備

ThinkSmart Viewをご利用いただくために必要な環境は以下の通りです。

1. アカウントの準備

ThinkSmart ViewにサインインするOffice 365のアカウントをあらかじめご用意ください。
ライセンス要件に関してはマイクロソフトから公開されている情報をご参照ください。
<https://products.office.com/ja-jp/microsoft-teams/voice-calling>

従業員それぞれが利用する場合はユーザーアカウントを、
共用スペースに設置する場合にはリソースアカウントの作成が必要です。

2. ハードウェアの準備

パッケージに含まれているもの

- ThinkSmart View 本体
- ACアダプター

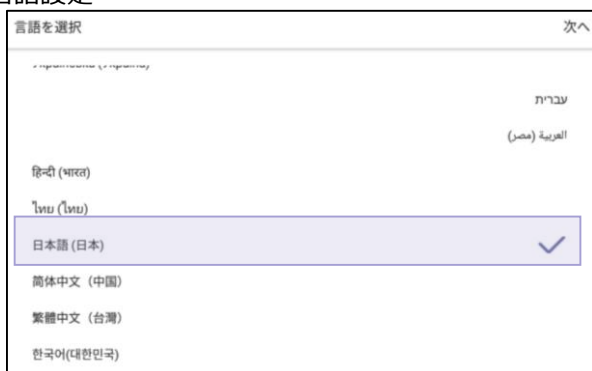
お客さまにご用意いただくもの

- 適切なライセンスが付与されたOffice 365 (Azure AD) アカウント
- インターネットアクセスが可能な無線LAN環境
- Bluetooth接続のヘッドセット (必要な場合)

初期設定

ThinkSmart ViewにACアダプターを挿入することでデバイスが起動します。
チュートリアルに沿ってデバイスの設定がはじまります。

① 言語設定



② Wi-Fi接続の設定

※SSIDステルスの場合は最下部の“ネットワーク追加”を選択し入力





③ Bluetoothデバイスの接続設定

※ThinkSmart Viewは本体にマイクとスピーカーを内蔵しています。

ヘッドセットへの接続が必要ない場合、後ほど設定する場合はスキップして問題ありません。



Microsoft Teams ヘサインイン

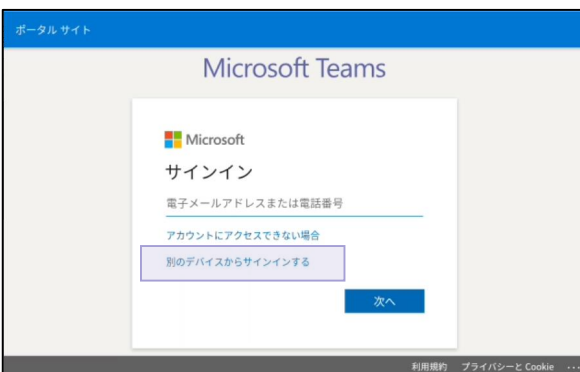
アカウント/パスワードの入力、もしくは別のAAD Join済のデバイス経由でのサインインが可能です。

Azure AD Join済のデバイスからのサインインする方法を紹介します。

① 「サインインする」をタップ



② 「別のデバイスからサインインする」をタップ

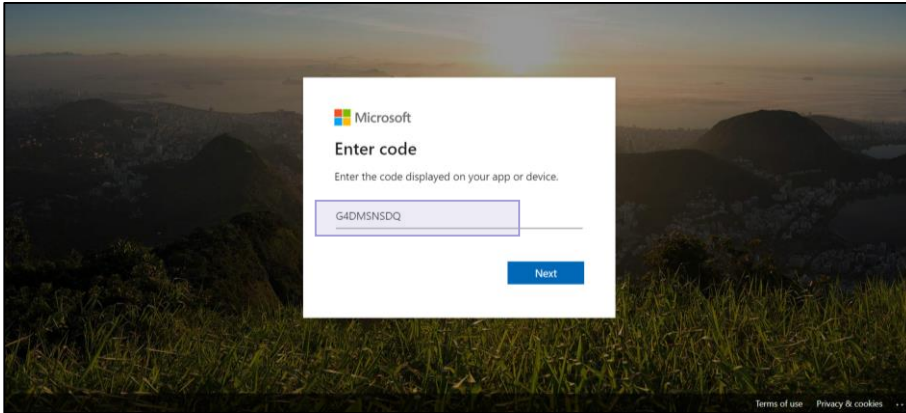


③ ワンタイムパスコードを確認





- ③ Azure AD参加済のWindows PCから「<https://Microsoft.com/devicelogin>」にアクセスの上、ThinkSmart Viewに表示したワンタイムパスコードを入力ください。



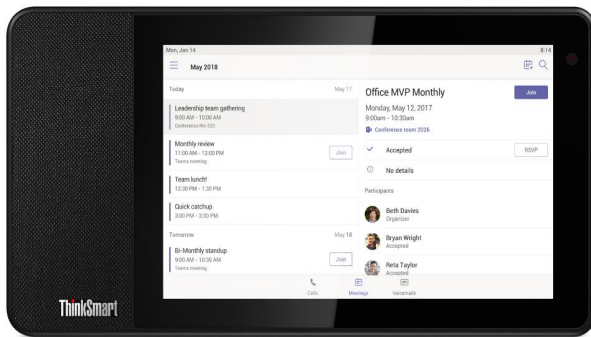
- ④ ThinkSmart View上で「OK」をタップします。Teamsへサインインが完了しました。



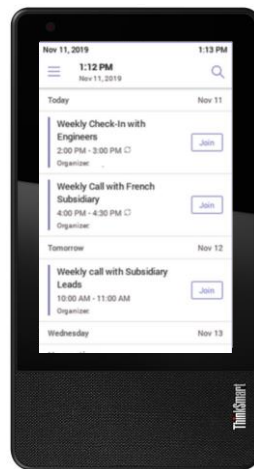
第3章 ThinkSmart View 使いこなす

利用シナリオ

ThinkSmart Viewは固定席やホームオフィスの利用だけでなく、フリーアドレスエリアや電話ブースへの設置などにも対応した、場所を問わない働き方に最適な一台です。



ユーザーサインインモード



電話ブースモード



共用電話機モード

ユーザーサインインモード（ユーザーアカウントでのサインイン）

レイアウト





通話画面 レイアウト

4月 22, 2020 午後11:55

通話

短縮ダイヤル

ディレクトリの連絡先検索

通話履歴

通話履歴

短縮ダイヤルへ追加

ダイヤルパット

通話

予定表

ボイスメール

短縮ダイヤルから削除

通話を発信

会議画面 レイアウト

3月 13, 2020 午後3:57

予定表

ミーティング詳細確認

ディレクトリの連絡先検索

※现阶段では日本語入力はサポートされていません

ミーティング参加

※Skype for Business会議への参加はサポートされません

新しい会議

予約表

通話

予定表

ボイスメール

ボイスメール画面 レイアウト

3月 23, 2020 午前9:55

ボイスメール

再生速度設定

ボイスメールの再生

ボイスメールの文字訳

削除

ディレクトリの連絡先検索

ボイスメール発信者情報確認

通話開始

通話

予定表

ボイスメール



共用電話機モード

「CommonAreaPhoneSignIn」モードが有効となったアカウントでサインインすると、ThinkSmart Viewを共用電話機モードご利用いただくことが可能です。

- 電話の発信と受信が可能
- ホットデスク機能を利用可能（有効・無効の設定はPowerShellにてアカウントベースで可能）



電話ブースモード

「MeetingSignIn」モードが有効となったアカウントでサインインすると、ThinkSmart Viewを電話ブースモードでご利用いただくことが可能です

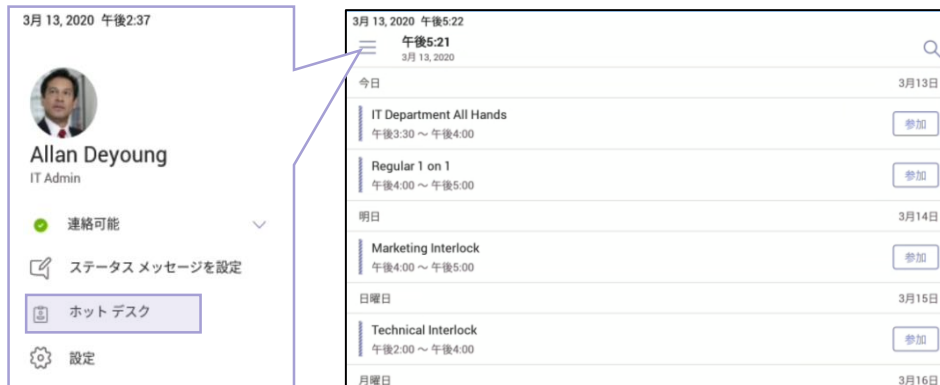
- ミーティングの参加が可能
- ミーティングの詳細はThinkSmart Viewで確認不可
- ディレクトリの連絡先検索で、ビデオ通話発信可能
- ホットデスク機能を利用可能（有効・無効の設定はPowerShellにてアカウントベースで可能）





ホットデスク モードの利用

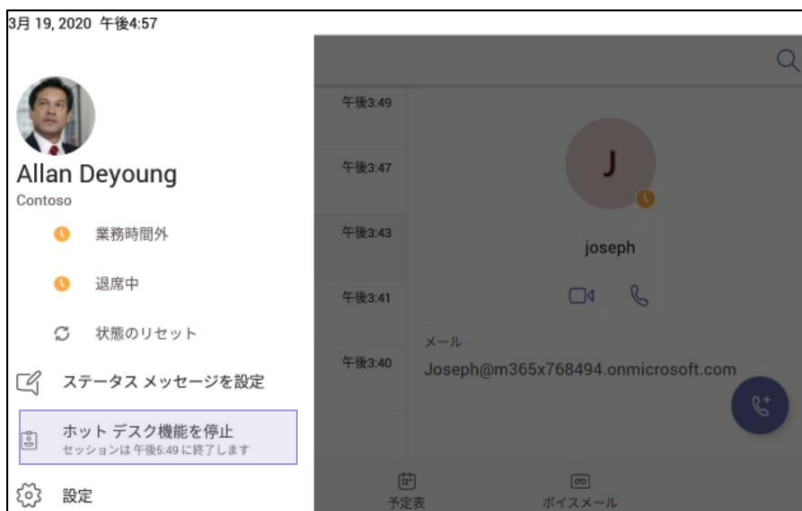
① 左上の「☰」をタップして、「ホットデスク」をタップするとサインイン画面が表示されます。



② サインインすることで、不特定多数のユーザーが端末を利用するシーンをサポートします。



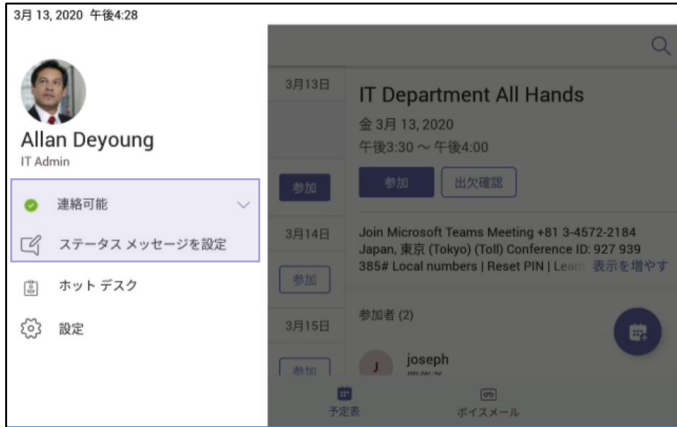
③ 離席時には左上の「☰」をタップして、「ホットデスク機能を停止」をタップすることでサインアウトが可能です。ユーザーが一定時間端末を操作していない場合に、自動的にサインアウトする設定とすることも可能です。
*ホットデスクモードの自動サインアウトまでの時間はPowerShell経由で任意に設定可能です。





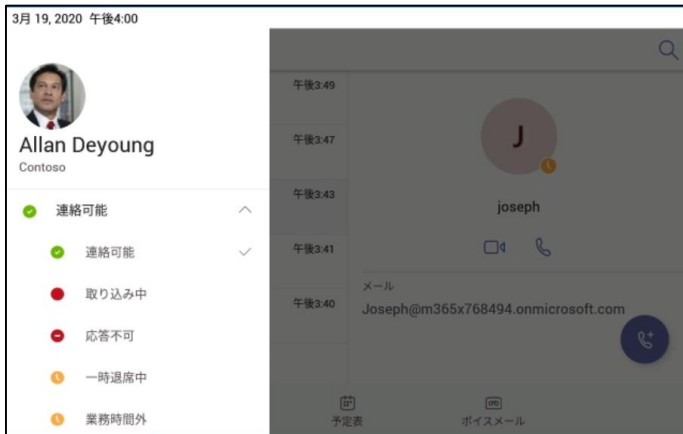
Teamsアプリの設定

画面の左上の ≡ をタップすると、カラムメニューが表示されます。
カラムメニューよりTeamsの状態変更及びステータスメッセージの設定が可能です。



状態設定

✓ をタップして状態設定メニューを開いて、
状態設定メニューの中から選択ください。



ステータスメッセージ設定

他のユーザーが自分にメッセージ送った場合に自動返信するメッセージの設定ができます。

3月19, 2020 午後4:15

✕ ステータスメッセージを設定 ✓

I am out of office today for off site meeting. Please contact me via phone if urgent. Thank you.

ステータスメッセージを入力

ステータスメッセージの自動送信オン/オフ

他のユーザーが自分にメッセージを送った場合に表示する
他のユーザーがあなたにメッセージを送ったり @メンションしたりした場合に、ステータスが表示されます。

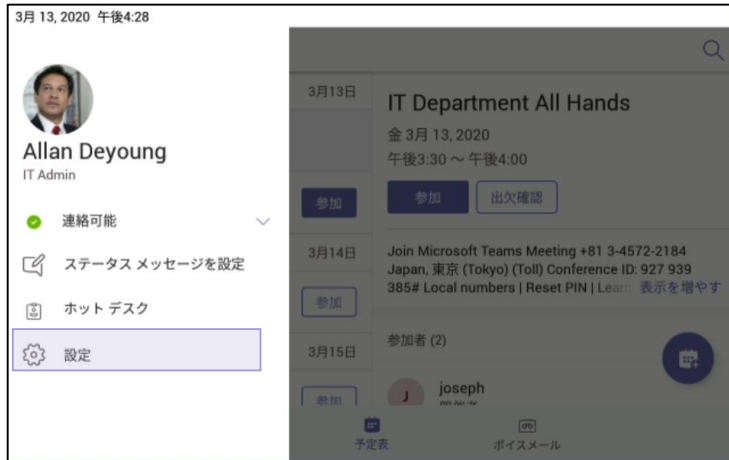
次の日時の後にクリア 3月19日 午後11:59

- クリアしない
- 1時間
- 4時間
- 今日
- 今週
- ユーザー設定





画面の左上の **☰** をタップすると、カラムメニューが表示されます。
 カラムメニューより「設定」をタップすると、Teamsのテーマと通話ロックなどの設定ができます。



プロフィール、通話ロック、ヘルプとフィードバック

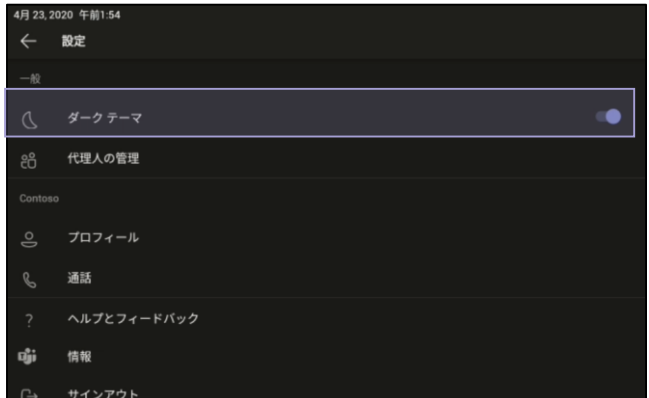


ダークテーマ

テーマを切り替えるには、アプリを再起動する必要があります。(再起動時サインイン不要)



ダークテーマオフ

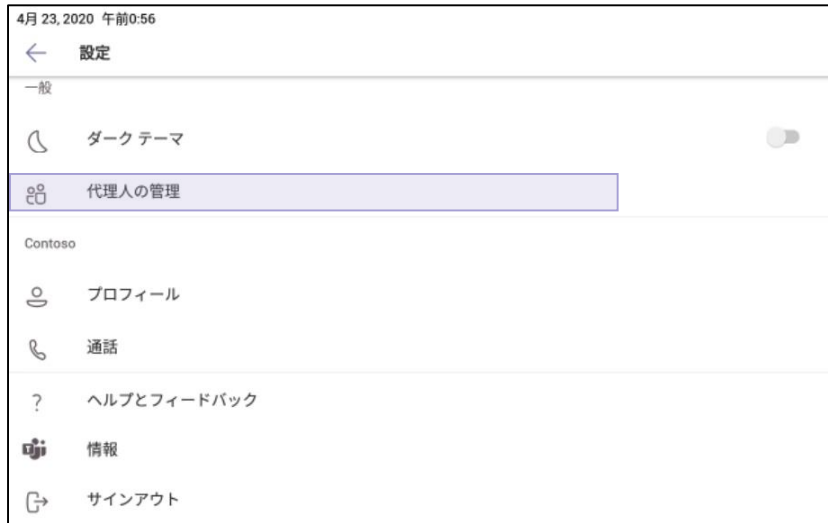


ダークテーマオン





代理人の管理



設定したい代理人をディレクトリで検索

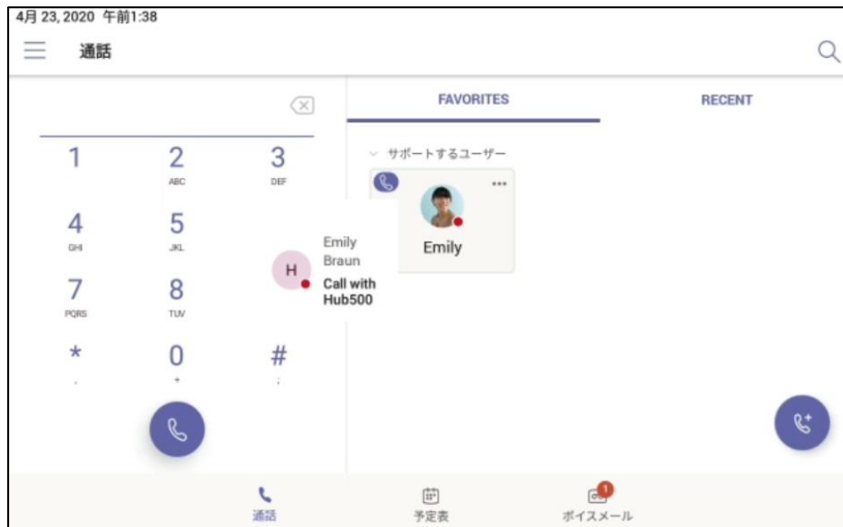


代理人の権限を設定

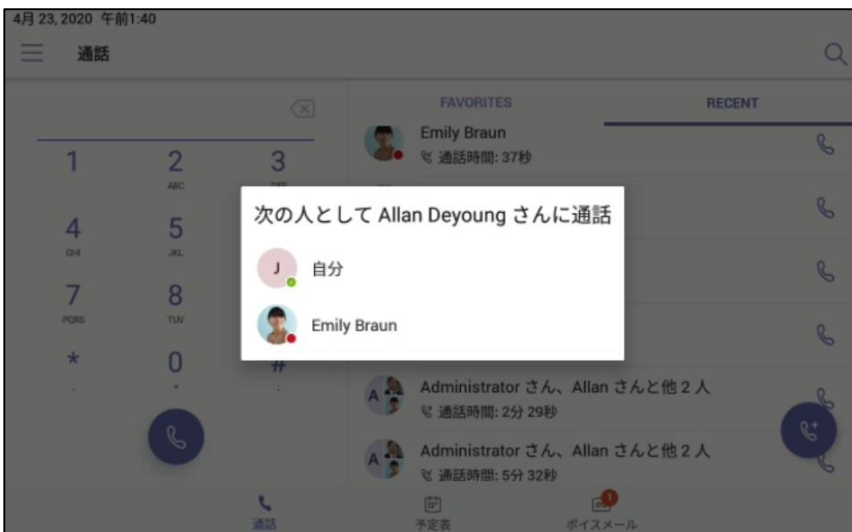




設定された代理人はの委託人の通話状態を確認可能です。





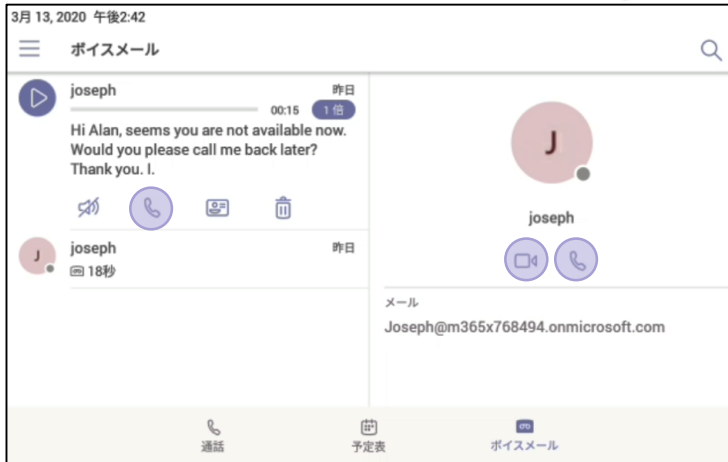
設定された代理人は委託人の代理として設定された権限で通話の受発信が可能です。








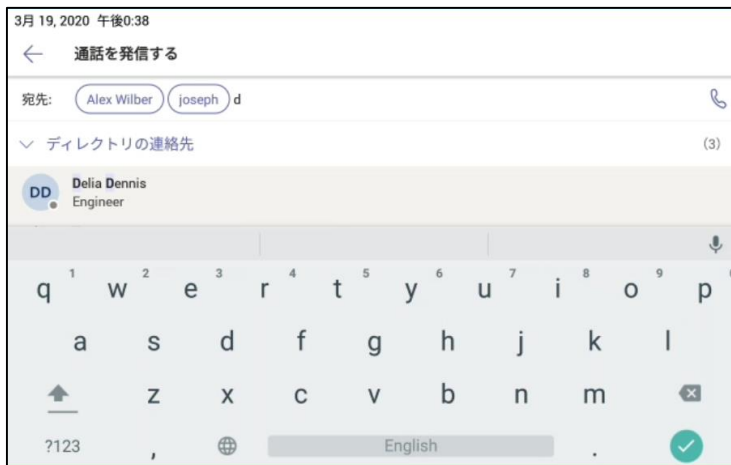
通話の開始

ThinkSmart View 上に表示している連絡先と通話したい場合、 もしくは  をタップすることで通話開始可能です。

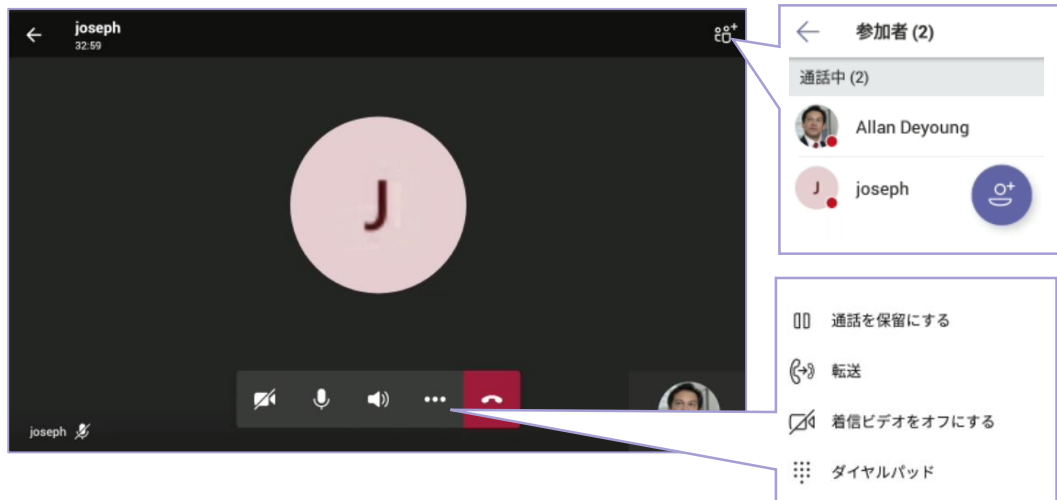


ディレクトリの連絡先を検索して1対1及びグループ通話を開始可能です。

- ①  もしくは  をタップ
- ② ディレクトリの連絡先を検索して、宛先に追加（複数宛先追加可能）
- ③  をタップして通話開始



ビデオ電話開始後、参加者の確認と追加、ビデオとスピーカマイクのオンオフ、そして通話の転送と保留などができます。

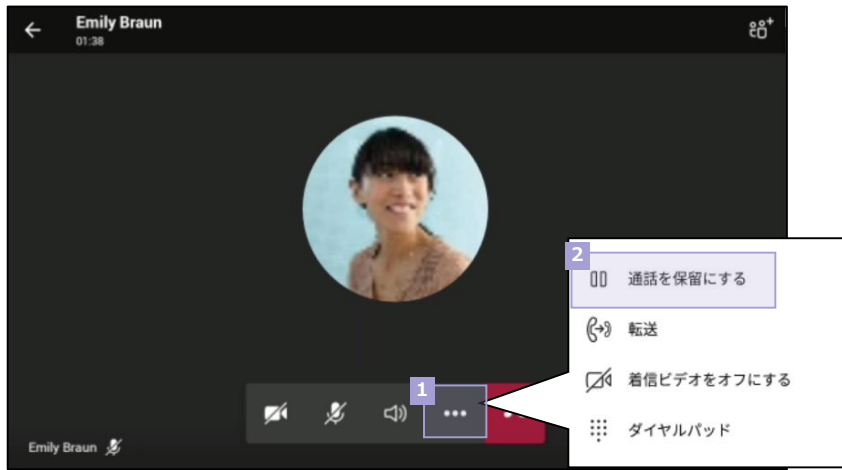




通話の保留と転送

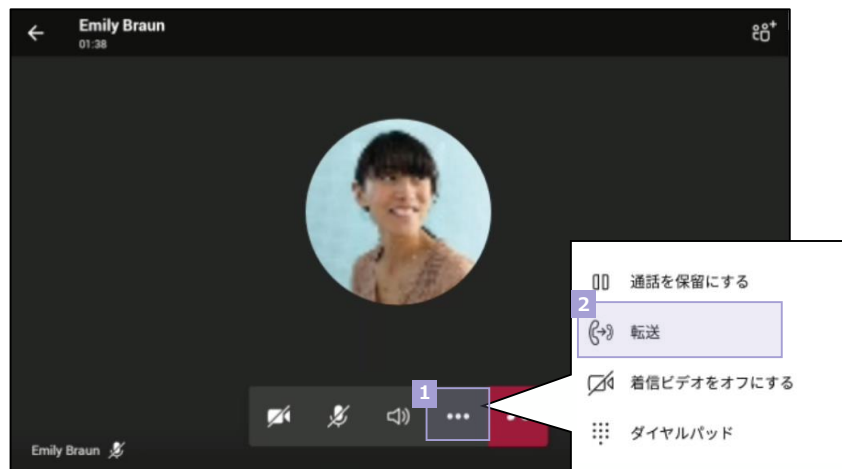
通話を保留にする場合

- ① 「…」をタップし
- ② 「通話を保留にする」をタップ

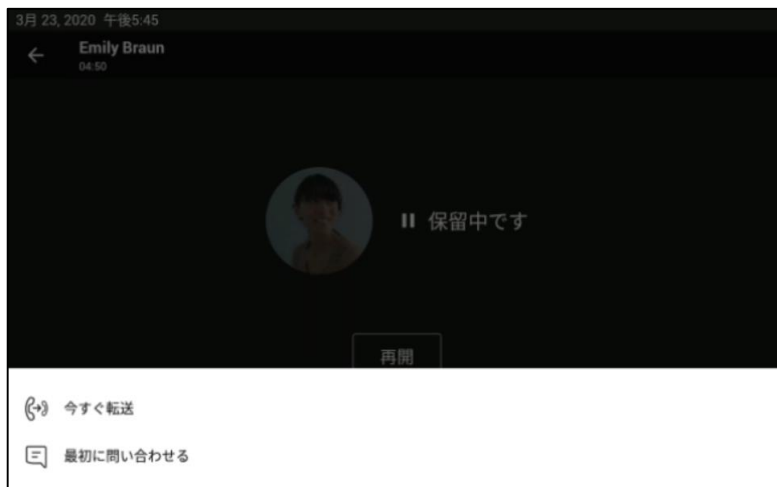


通話を転送する場合

- ① 「…」をタップし
- ② 「転送」をタップ



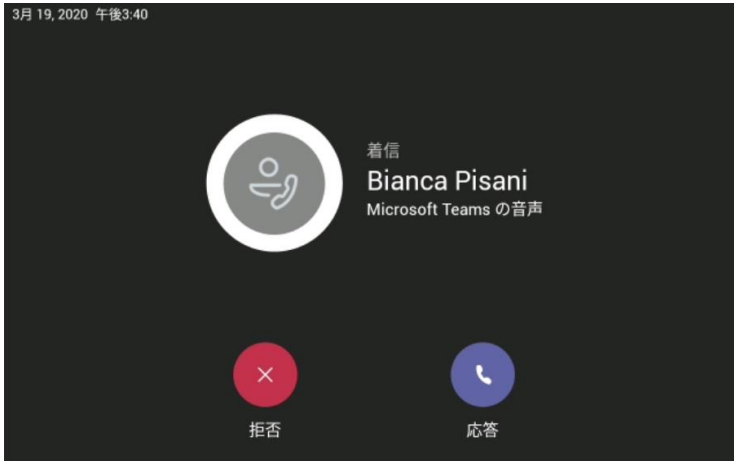
- ③ 「今すぐ転送」もしくは「最初に問い合わせる」をタップして転送



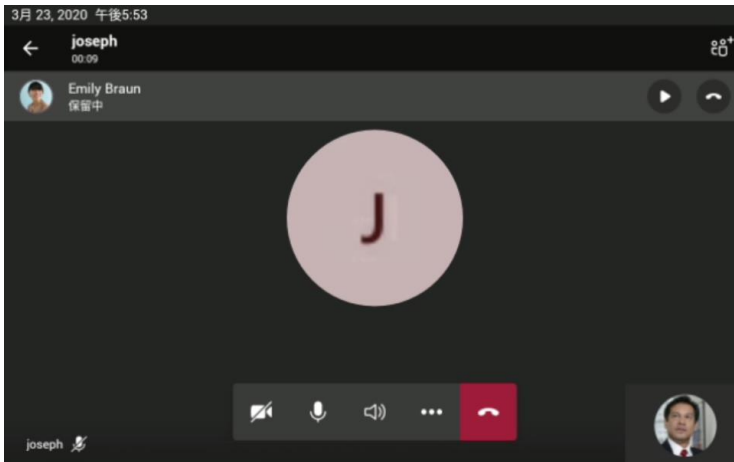


保留

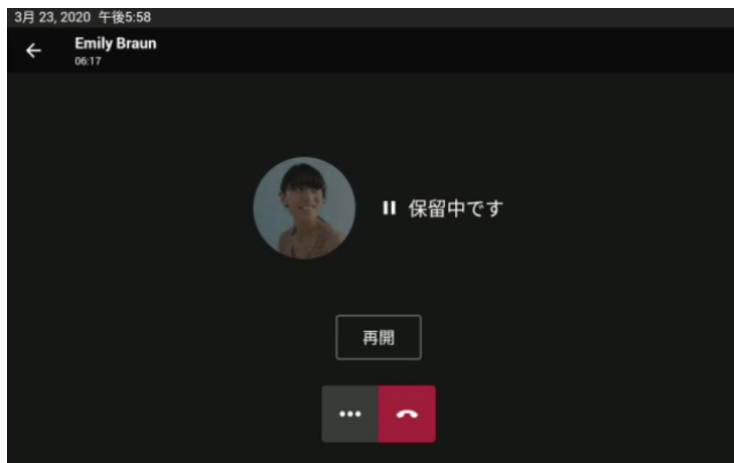
通話中別の通話リクエストが入ると、「拒否」もしくは「応答」を選択可能です。



「応答」を選択した場合、元々通話中の電話が保留されます。



通話完了したら、保留中の電話を保留解除できます。



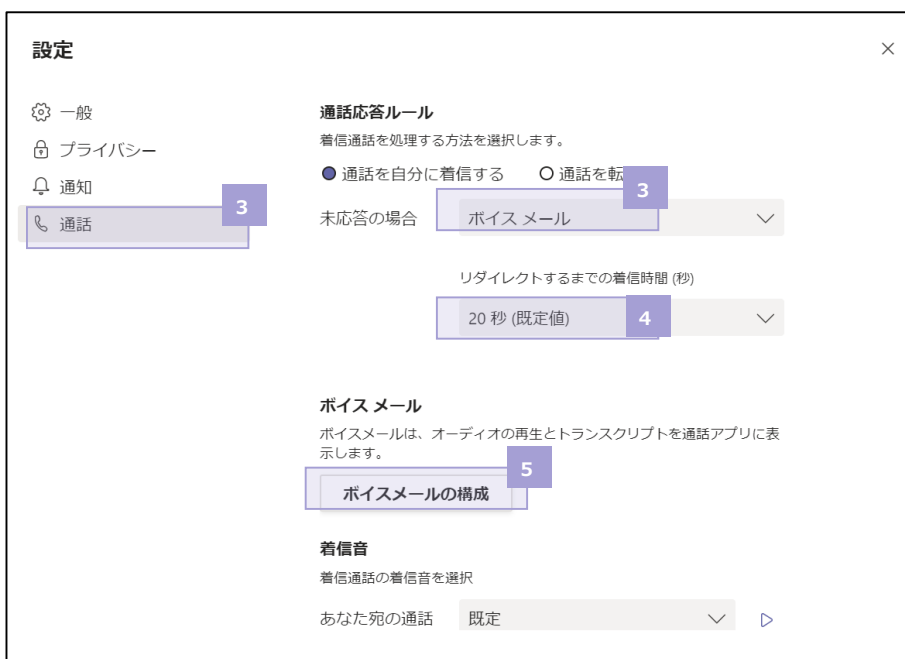


ボイスメールについての設定（PC上）

ボイスメール トランスクリプションに対するサポートは 2017 年 3 月時点で追加されており、すべての組織とユーザーに対して既定で有効になっています。Windows PowerShell を使用し、所属する組織のトランスクリプションを無効にすることができます。


ユーザー単位でのボイスメールの有効

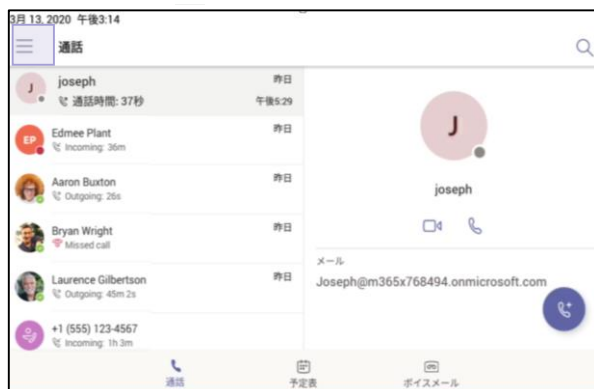
- ① PC上のTeamsアプリを開き、右上のある丸写真をタップして、カラムメニューを開く
- ② カラムメニュー状の「設定」をタップして、設定メニューを開く
- ③ 通話設定で「未応答の場合」を「ボイスメール」に設定
- ※「何もしない」と設定された場合、ボイスメールが無効されます
- ④ リダイレクトするまでの着信時間を設定
- ⑤ ボイスメールの構成をタップして応答メッセージの録音などが設定可能



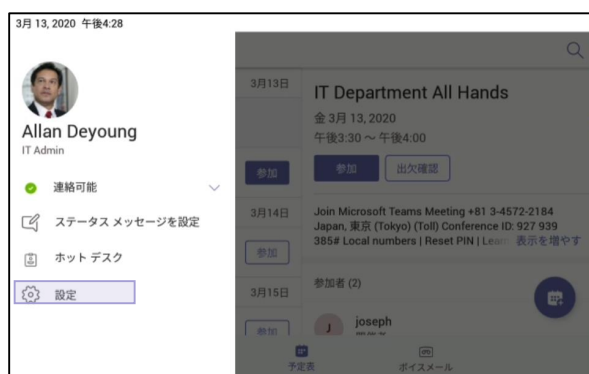
第4章 デバイス設定

端末設定画面に入る

- 1) 画面の左上の  をタップすると、カラムメニューが表示されます。



- 2) 表示したカラムメニュー内「設定」をタップして、Teams関連の設定画面に入ります。



- 3) Teams関連設定画面で「デバイスの設定」をタップして端末設定画面に入ります。





言語設定

言語設定を変更したい場合、ターゲット言語を選定して一番上に入れ替える必要があります。
 ※言語設定変更によりMicrosoft Teamsアプリの再起動が行われます。再起動の後サインインは不要です。

← 端末の設定	
システム	
言語設定	ja Deutsch (Deutschland) ≡
時刻と日付	Ελληνικά (Ελλάδα) ≡
表示	English (United Kingdom) ≡
ユーザー補助	English (United States) ≡
ネットワークと接続	English (United States, Computer) ≡
WLAN	
Bluetooth	Español (España) ≡
	Español (Estados Unidos) ≡
詳細情報	
法的情報	Eesti (Eesti) ≡
	Suomi (Suomi) ≡

時刻と日付

時刻と日付を設定によりデバイスの時間を設定することができます。

← 端末の設定	
システム	日付と時刻の自動設定 <input checked="" type="checkbox"/>
言語設定	ja ネットワークから提供された時刻を使用する
時刻と日付	日付設定
	Mar 18, 2020
	時刻設定
	10:29
	タイムゾーンの選択
	日本標準時
	24時間表示 <input type="checkbox"/>
	1:00 PM
	日付形式
	Mar 18, 2020

表示

明るさの調整について、手動調節と自動調節ができます。

← 端末の設定	
システム	
言語設定	ja 明るさのレベル
	スクリーンタイムアウト
時刻と日付	
表示	明るさの自動調節 <input type="checkbox"/>
ユーザー補助	
ネットワークと接続	
WLAN	
Bluetooth	
詳細情報	
法的情報	





スクリーンタイムアウトを1分から1時間まで設定可能です。

端末の設定		スリープ	
システム	明るさのレベル	<input type="radio"/> 5分	
言語設定 ja	スクリーンタイムアウト	<input checked="" type="radio"/> 10分	
時刻と日付	明るさの自動調節 <input checked="" type="checkbox"/>	<input type="radio"/> 15分	
表示		<input type="radio"/> 20分	
ユーザー補助		<input type="radio"/> 25分	
ネットワークと接続		<input type="radio"/> 30分	
WLAN		<input type="radio"/> 45分	
Bluetooth		<input type="radio"/> 1時間	
詳細情報			
法的情報			

ユーザー補助

デバイスに表示される文字が読みやすくするための高コントラストテキストモードの有効化、文字サイズの調整及び色補正が設定可能です。

システム	高コントラストテキスト <input checked="" type="checkbox"/>
言語設定 ja	大テキスト
時刻と日付	色補正
表示	ダウンロード済みサービス
ユーザー補助	
ネットワークと接続	
WLAN	
Bluetooth	
詳細情報	
法的情報	

ネットワークと接続

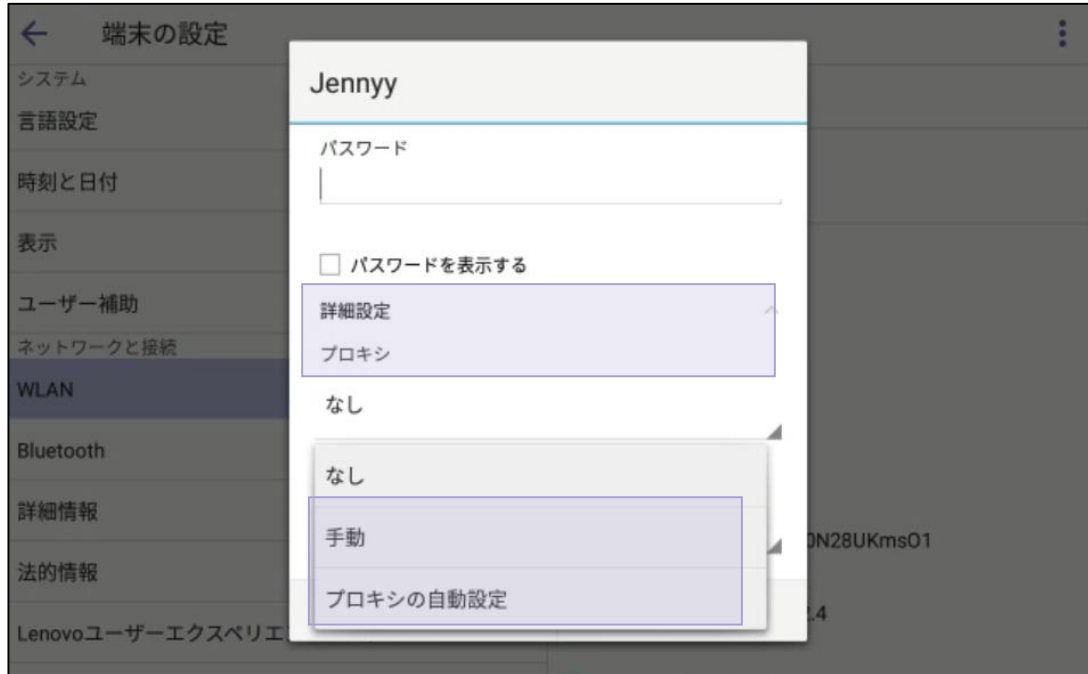
無線LANの接続とBluetoothデバイスのペアリングが設定可能です。

端末の設定	
表示	ON <input checked="" type="checkbox"/>
ユーザー補助	他の端末には「Lenovo CD-18781Y」として表示されます
ネットワークと接続	ペア設定したデバイス
WLAN	新しいデバイスとペア設定する
Bluetooth	端末名 Lenovo CD-18781Y
詳細情報	スマートフォンの Bluetooth アドレス: 3C:91:80:B2:40:42
法的情報	
Lenovoユーザーエクスペリエンスプログラム	
電話のロック	
電話を再起動	



Proxy設定については、WLAN設定内で

- 1) 詳細設定をタップ
- 2) プロキシの項目で「手動」もしくは「プロキシの自動設定」をタップ
- 3) プロキシ情報をインプット



詳細情報

以下の通り、詳細情報が確認可能です。

- ① IPアドレス
- ② WLAN MAC
- ③ Bluetooth MAC
- ④ ファームウェアバージョン
- ⑤ パートナアプリケーションバージョン
- ⑥ Company portalバージョン
- ⑦ Teamsのバージョン
- ⑧ モデルとシリアル番号



法的情報

ライセンスと契約書などが確認可能です。

詳細情報	サードパーティ ライセンス
法的情報	システムのWebViewライセンス
Lenovoユーザーエクスペリエンスプログラム	Lenovo使用許諾契約書
電話のロック	Lenovoプライバシーポリシー
電話を再起動	オープンソース情報
管理者設定	オープンソースライセンス
デバッグ	壁紙
ネットワーク構成	航空写真の提供: ©2014 CNES / Astrium, DigitalGlobe, Bluesky
パスワード/サインアウト	

電話のロック

PINを設定して電話ロックをかけることができます。
 1分から1時間まで電話ロックタイムアウトが設定可能です。
 PINは4桁以上である必要があります。

← 端末の設定	
詳細情報	有効化/無効化 <input checked="" type="checkbox"/>
法的情報	電話ロックタイムアウト
Lenovoユーザーエクスペリエンスプログラム	電話ロックPIN
電話のロック	
電話を再起動	
管理者設定	
デバッグ	
ネットワーク構成	
パスワード/サインアウト	



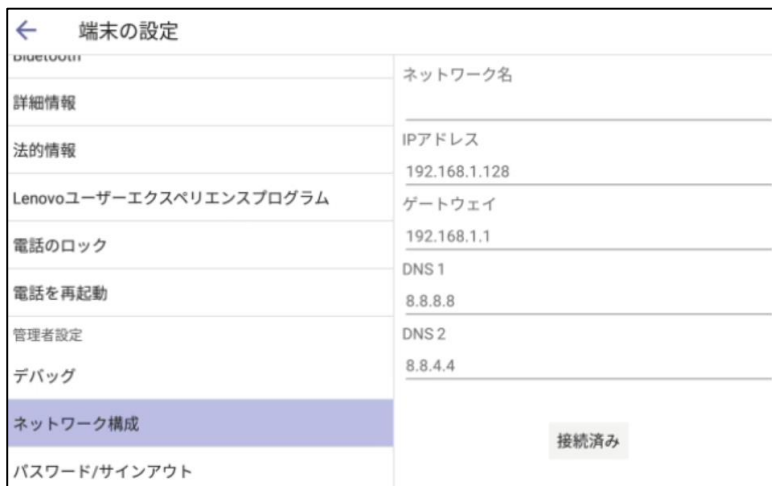


管理者設定

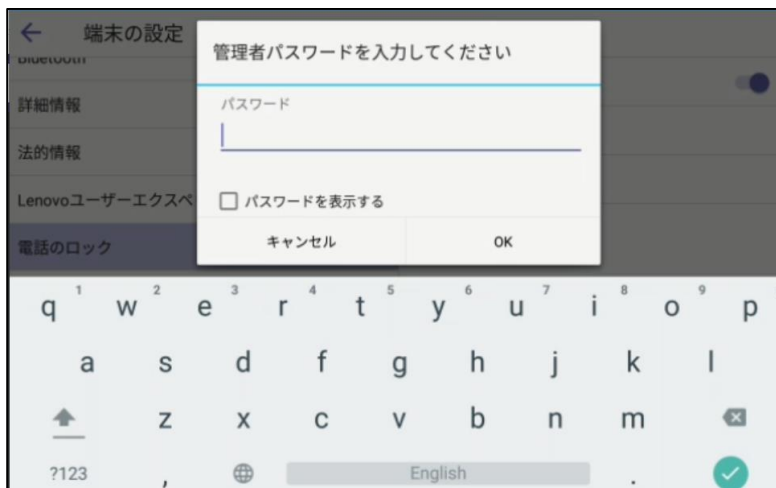
デバッグするためのログレベルや、ログの有効及びデバイスのリセットができます。



ネットワーク構成が設定できます。



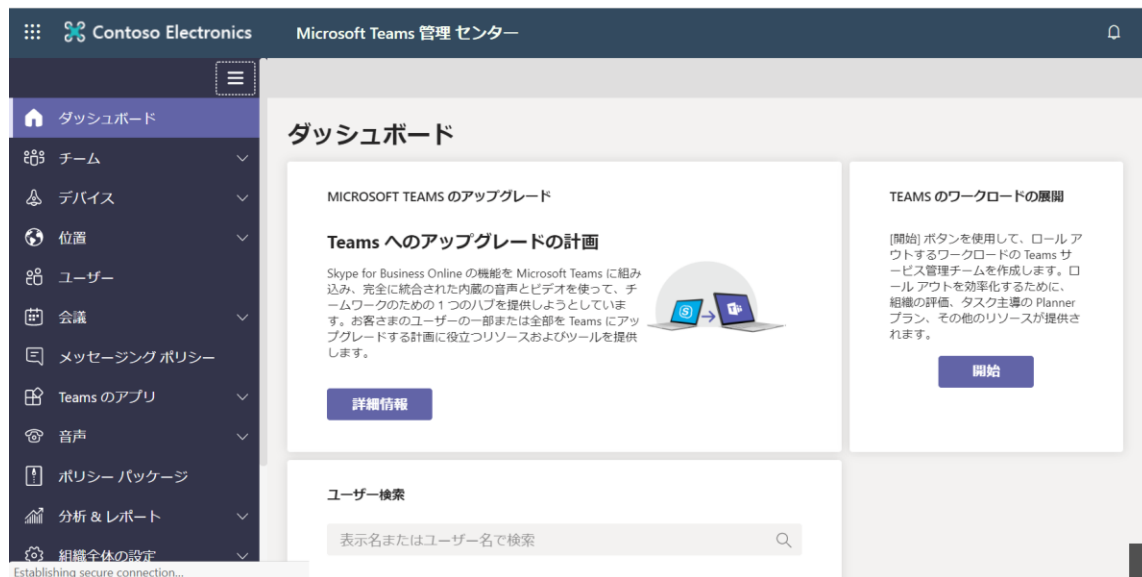
管理者設定を変更する場合、管理者パスワードの入力が必要です。デフォルト管理者パスワードは空白です。
※下記の画面で入力せずに直接「OK」をタップください。



第5章 デバイス管理

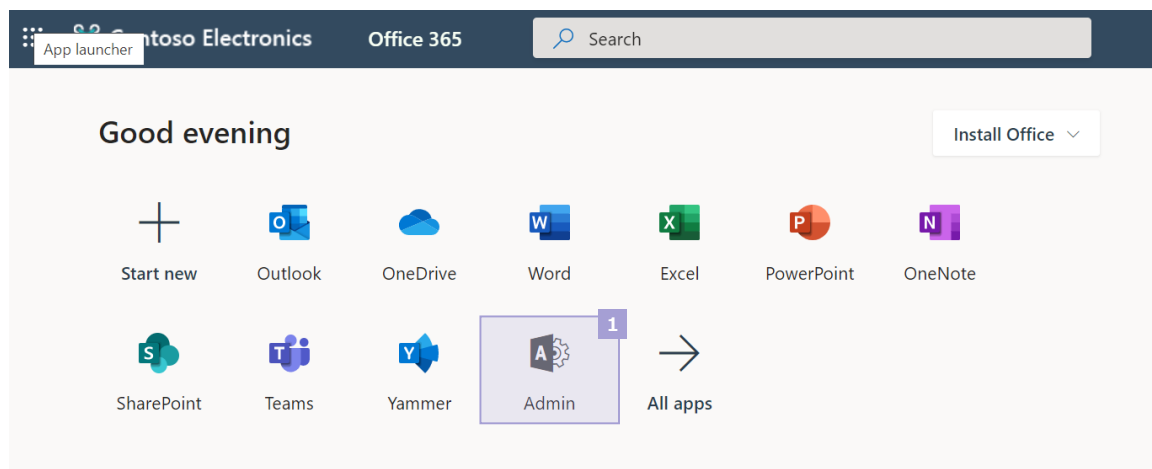
Microsoft Teams 管理センターを利用してデバイス管理

ThinkSmart Viewの管理はMicrosoft Teams 管理センターから行うことが可能です。



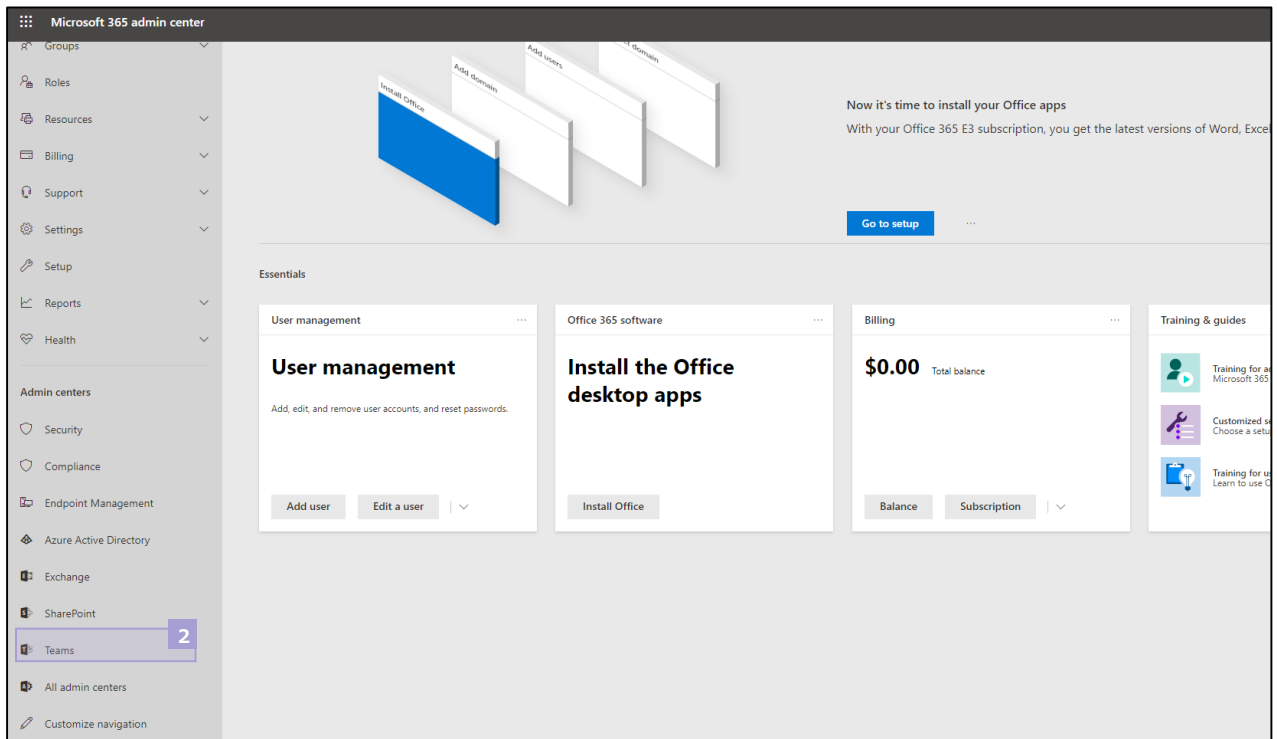
Microsoft Teams管理センターを開く

- ① 管理者アカウントでOffice.comへサインインした後、「Admin」をクリックしてMicrosoft 365 管理センターを開きます。



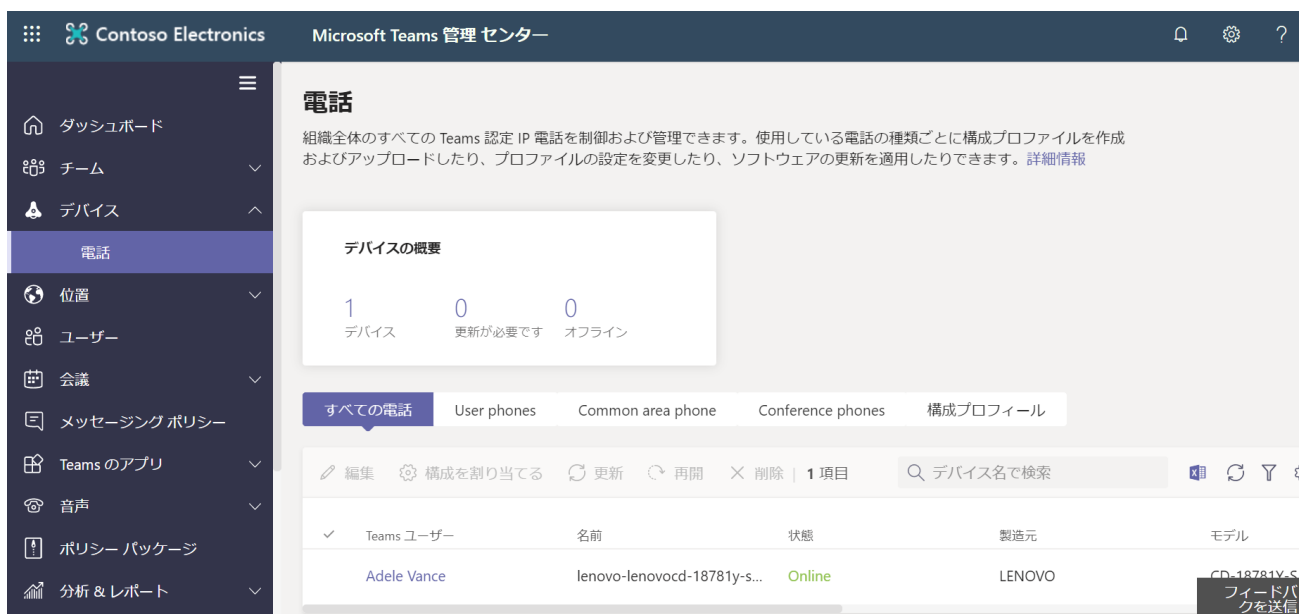


② 「Microsoft 365 管理センター」で「Show All」→「Teams」をクリックして、Microsoft Teams管理センターを開きます。



デバイス情報確認

「Microsoft Teams管理センター」から「デバイス」→「電話」を開くと、登録済のデバイス一覧が確認できます。





デバイスプロファイル設定

「構成プロファイル」機能から、デバイスプロファイルの確認と作成が可能です。
作成したプロファイルをデバイスに割り当てることによりデバイスの管理と設定の標準化ができます。
構成可能な項目は以下の通りです。

構成プロファイル \ 新規

名前

説明

一般

- デバイスのロック オン
 - タイムアウト 30 秒
 - デバイス ロックPIN 123456
- 言語 英語 (米国)
- タイムゾーン (UTC-12:00) 国際日付変更線 西側
- 日付の形式 DD/MM/YYYY
- 時刻の形式 12 時間 (午前/午後)

デバイスの設定

- オン
 - スクリーン セーバーを表示する
 - タイムアウト 30 秒
 - ディスプレイのバックライトの明るさ
 - ディスプレイのバックライトのタイムアウト 15 分
 - ハイコントラストを表示します オフ
 - サイレント モード オフ
 - 勤務時間 08:00 17:00
 - 節電 オフ
 - スクリーン キャプチャ オフ

ネットワーク設定

- DHCP が有効 オン
- ログ有効 オフ
- ホスト名 ホスト
- ドメイン名 domain.com
- IP アドレス 10.5.140.156
- サブネット マスク 255.255.255.0
- デフォルトゲートウェイ 10.5.140.1
- プライマリ DNS 10.5.140.225
- セカンダリ DNS 10.5.140.101
- デバイスのデフォルトの管理者パスワード
- ネットワーク PC ポート オフ

保存 キャンセル



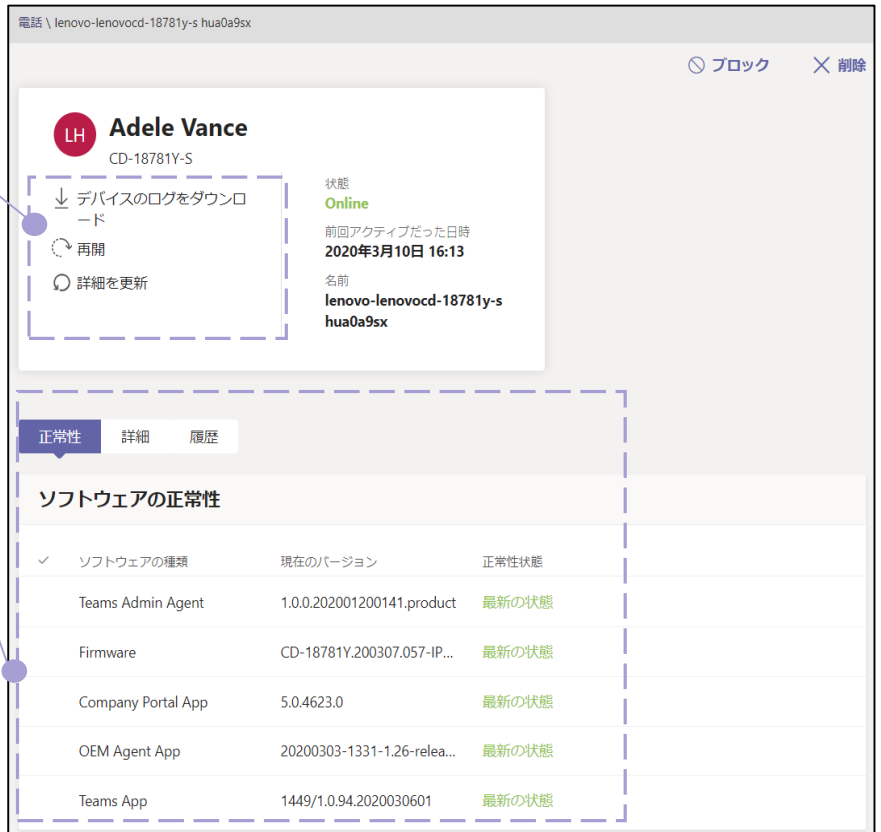
リモート管理

“Teams ユーザー”列に表示されたユーザー名をタップすることで、ユーザーが利用しているデバイスの個別管理が可能です。



デバイスのリモート管理

- デバイスのログをダウンロード
- デバイスのリモート再起動
- ブロック
- 削除

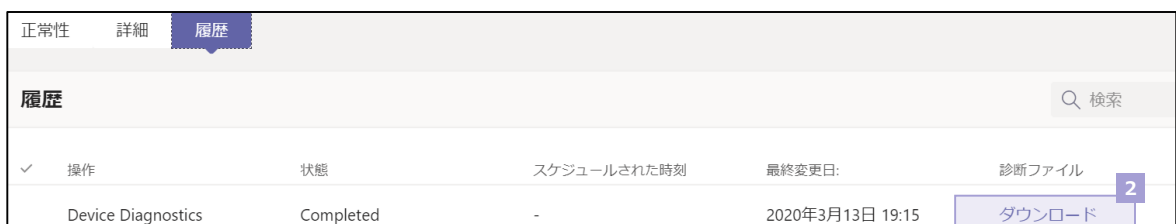


情報確認

- 状態確認 (オンライン/オフライン)
- ソフトウェアバージョンの確認
- シリアル番号
- IPアドレス

デバイスログファイルのダウンロード

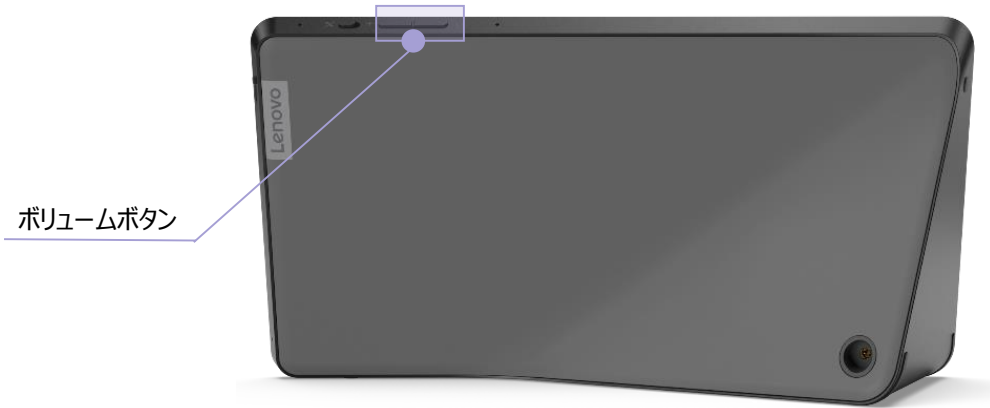
- ① デバイスのログをダウンロードをクリック
- ② 履歴ページに診断ファイル項目の下で、ダウンロードをクリック





ファクトリーリセット

デバイスのボリュームボタン（+と-）を同時に約10秒長押しすることで、ファクトリーリセットができます。



ボリュームボタン

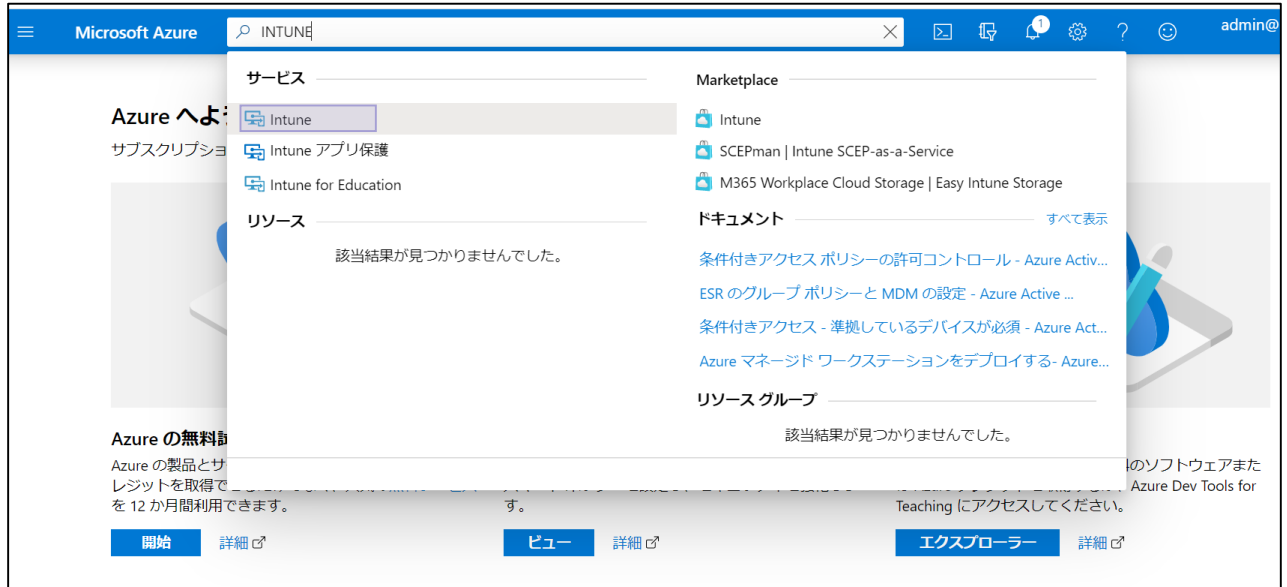




Azure Active Directory 管理センターを利用してデバイス管理

Azure Active Directory 管理センターで、「デバイスのポリシー準拠」と「条件付きアクセス」ポリシーの設定により、ユーザーが会社のセキュリティポリシーに準拠していないデバイスでのTeamsへのサインインをブロックすることができます。

Azure Active Directory 管理センター <https://portal.azure.com/>へ管理者権限でサインインください。検索ボックスで「Intune」を入力して検索して、Intuneポータルへ移動ください。



デバイスのポリシー準拠を設定

Intuneポータルの左側のメニュー欄から「デバイスのポリシー準拠」をクリックして、デバイスのポリシー準拠設定画面に入ります。





「ポリシー」→「+ポリシーの作成」で新しいポリシーの作成を始めます。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Microsoft Intune > デバイスのポリシー準拠 | ポリシー

デバイスポリシー準拠 | ポリシー

検索 (Ctrl+) | + ポリシーの作成 | 列 | フィルター | 最新の情報に更新 | エクスポート

Android デバイスマネージャーの1つ以上のコンプライアンスポリシーに、アクティブな Mobile Threat Defense コネクタを持たない、構成済みのデバイス脅威レベル設定があります。ここをクリックして、Android デバイスマネージャーの Mobile Threat Defense コネクタをセットアップしてください。

名前を検索	プラットフォーム	ポリシーの種類	割り当て済み	最終変更
Contoso MDM Compliance Policy for iOS	iOS/iPadOS	iOS コンプライアンスポリシー	はい	19/6/14 午前8:16
Teams Phone Android	Android デバイス管...	Android コンプライアンス ポリ...	はい	20/3/25 午後2:44

「名前」の項目にポリシー名をインプットして、プラットフォームの項目を「Androidデバイス管理者」に選択ください。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Microsoft Intune > デバイスのポリシー準拠 | ポリシー > ポリシーの作成 > Android コンプライアンス ポリシー > デバイスの正常性

ポリシーの作成 × Android コンプライアンス ポ... × デバイスの正常性 □ ×

名前 * ThinkSmart View用ポリシー ✓

説明 説明の入力... ✓

プラットフォーム * Android デバイスマネージャー ✓

設定 構成 >

場所 構成 >

コンプライアンス非対応に対する... 1個が構成済み >

スコープ(タグ) 0個のスコープが選択されました >

設定を構成するカテゴリを選択します。

- デバイスの正常性 > 7個の設定が使用可能
- デバイスのプロパティ > 2個の設定が使用可能
- システムセキュリティ > 10個の設定が使用可能

デバイス管理者によって管理されているデバイス [i] ブロック 構成されていません

ルート化されたデバイス [i] ブロック 構成されていません

デバイスは、デバイス脅威レベル以下であることが必要 [i] 構成されていません

Google Play プロテクト [i] 必要 構成されていません

Google Play サービスが構成されています [i] 必要 構成されていません

最新のセキュリティプロバイダー [i] 必要 構成されていません

アプリの脅威のスキャン [i] 必要 構成されていません

SafetyNet デバイスの構成証明 [i] 構成されていません

「構成」→「デバイスの正常性」の下の「デバイス管理者によって管理されているデバイス」の項目を「構成されていません」を選択ください。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > Microsoft Intune > デバイスのポリシー準拠 | ポリシー > ポリシーの作成 > Android コンプライアンス ポリシー > デバイスの正常性

ポリシーの作成 × Android コンプライアンス ポ... × デバイスの正常性 □ ×

名前 * ThinkSmart View用ポリシー ✓

説明 説明の入力... ✓

プラットフォーム * Android デバイスマネージャー ✓

設定 構成 >

場所 構成 >

コンプライアンス非対応に対する... 1個が構成済み >

スコープ(タグ) 0個のスコープが選択されました >

設定を構成するカテゴリを選択します。

- デバイスの正常性 > 7個の設定が使用可能
- デバイスのプロパティ > 2個の設定が使用可能
- システムセキュリティ > 10個の設定が使用可能

デバイス管理者によって管理されているデバイス [i] ブロック 構成されていません

ルート化されたデバイス [i] ブロック 構成されていません

デバイスは、デバイス脅威レベル以下であることが必要 [i] 構成されていません

Google Play プロテクト [i] 必要 構成されていません

Google Play サービスが構成されています [i] 必要 構成されていません

最新のセキュリティプロバイダー [i] 必要 構成されていません

アプリの脅威のスキャン [i] 必要 構成されていません

SafetyNet デバイスの構成証明 [i] 構成されていません



OSのバージョンを制限する必要がある場合、「構成」→「デバイスのプロパティ」の下で最小OSバージョンと最大OSバージョンが設定可能です。

The screenshot shows the Microsoft Azure portal interface for configuring an Android compliance policy. The breadcrumb trail is: ホーム > Microsoft Intune > デバイスのポリシー準拠 | ポリシー > ポリシーの作成 > Android コンプライアンス ポリシー > デバイスのプロパティ. The 'ポリシーの作成' (Policy Creation) pane on the left shows the policy name 'ThinkSmart View用ポリシー' and the platform 'Android デバイス管理者'. The 'Android コンプライアンス ポリシー' (Android Compliance Policy) pane in the center shows a list of categories: 'デバイスの正常性' (7 settings available), 'デバイスのプロパティ' (2 settings available), and 'システム セキュリティ' (10 settings available). The 'デバイスのプロパティ' (Device Properties) pane on the right is highlighted, showing 'オペレーティング システムのバージョン' (Operating System Version) with '最小 OS バージョン' (Minimum OS version) and '最大 OS バージョン' (Maximum OS version) fields, both currently set to '構成されていません' (Not configured).

「構成」→「システムセキュリティ」の下の項目を組織のコンプライアンスポリシーに基づいて構成ください。

The screenshot shows the Microsoft Azure portal interface for configuring system security settings for an Android compliance policy. The breadcrumb trail is: ホーム > デバイスのポリシー準拠 | ポリシー > Android | プロパティ > Android コンプライアンス ポリシー > システム セキュリティ. The 'Android | プロパティ' (Android | Properties) pane on the left shows the policy name 'Android' and the platform 'Android デバイス管理者'. The 'Android コンプライアンス ポリシー' (Android Compliance Policy) pane in the center shows a list of categories: 'デバイスの正常性' (7 settings configured), 'デバイスのプロパティ' (2 settings configured), and 'システム セキュリティ' (10 settings configured). The 'システム セキュリティ' (System Security) pane on the right is highlighted, showing various security options: 'パスワードの最小文字数' (Minimum password length) set to 8, 'パスワードが要求されるまでの非アクティブの最長時間 (分)' (Maximum inactivity time before password required) set to 15 minutes, 'パスワードの有効期限が切れるまでの日数' (Number of days before password expires) set to 40, '再使用を禁止するパスワード世代数' (Number of password generations to disallow reuse) set to 4, '暗号化' (Encryption) with 'デバイス上のデータストレージの暗号化' (Encrypt data on device) set to '必要' (Required), 'デバイスのセキュリティ' (Device security) with '提供元不明のアプリをブロックする' (Block apps from unknown publishers) set to 'ブロック' (Block), 'ポータル サイト アプリのランタイム整合性' (Runtime integrity for portal site apps) set to '必要' (Required), 'デバイスでの USB デバッグをブロックする' (Block USB debugging on device) set to 'ブロック' (Block), and '制限アプリ' (Restricted apps) with an 'エクスポート' (Export) button.



「コンプライアンス非対応に対する」の項目で準拠していないデバイスでのアクションのシーケンスを指定できます。

The screenshot shows the 'Microsoft Azure' portal interface. The breadcrumb trail is: ホーム > Microsoft Intune > デバイスのポリシー準拠 | ポリシー > ポリシーの作成 > アクション > アクションパラメーター. The main content area is divided into three panels: 'ポリシーの作成', 'アクション', and 'アクションパラメーター'. In the 'ポリシーの作成' panel, the '名前' field contains 'ThinkSmart View用ポリシー' and the 'プラットフォーム' is set to 'Android デバイス管理者'. In the 'アクション' panel, a table lists actions with columns for 'アクション', 'スケジュール', and 'メッセージ テンプレート'. The first row shows 'デバイスに非準拠のマー...' with a '即時' schedule. In the 'アクションパラメーター' panel, the 'スケジュール' dropdown is set to 'コンプライアンス違反となつてからの日数' and the value '0' is entered in the adjacent field.

設定したデバイスポリシーに準拠していないデバイスでのTeamsへのサインインをブロック

Intuneポータルで「条件付きアクセス」→「ポリシー」→「新しいポリシー」をタップして、ポリシーの作成を開始します。

The screenshot shows the 'Microsoft Azure' portal interface for creating a new Conditional Access policy. The breadcrumb trail is: ホーム > Microsoft Intune > 条件付きアクセス | ポリシー > 新規. The main content area is divided into three panels: 'Microsoft Intune', '条件付きアクセス | ポリシー', and '新しいポリシー'. In the '新しいポリシー' panel, the 'ポリシー名' field contains 'teams phone'. Below this, a list of baseline policies is shown: 'Baseline policy: Require MFA for admins (プレビュー)', 'Baseline policy: End user protection (プレビュー)', 'Baseline policy: Block legacy authentication (プレビュー)', and 'Baseline policy: Require MFA for Service Management (プレビュー)'. The 'teams phone' policy is selected.

「名前」の項目でポリシーの名前を入力ください。
ユーザーとグループの項目でポリシーのターゲットユーザーとグループを構成ください。

The screenshot shows the 'Microsoft Azure' portal interface for configuring the 'ユーザーとグループ' (Users and Groups) section of a policy. The breadcrumb trail is: ホーム > Microsoft Intune > 条件付きアクセス | ポリシー > teams phone > ユーザーとグループ. The main content area is divided into two panels: 'teams phone' and 'ユーザーとグループ'. In the 'teams phone' panel, the '名前' field contains 'アクセス制御'. In the 'ユーザーとグループ' panel, the '対象' (Target) dropdown is set to '対象外' (Excluded). Underneath, there are radio buttons for 'なし' (None), 'すべてのユーザー' (All users), and 'ユーザーとグループの選択' (Select users and groups), with the last one selected. There are also checkboxes for 'すべてのゲストおよび外部ユーザー (プレビュー)' (All guest and external users), 'ディレクトリ ロール (プレビュー)' (Directory roles), and 'ユーザーとグループ' (Users and groups), with the last one checked.



「クラウド アプリまたは操作」の項目で「すべてのクラウド アプリ」を選択ください

The screenshot shows the Microsoft Azure portal interface. On the left, the 'teams phone' policy is being edited. Under the '割り当て' (Assignment) section, 'クラウド アプリまたは操作' (Cloud apps or actions) is selected, and 'すべてのクラウド アプリ' (All cloud apps) is chosen. On the right, the 'クラウド アプリまたは操作' configuration pane shows 'このポリシーが適用される対象を選択する' (Select the target for this policy) with 'クラウド アプリ' (Cloud apps) selected. Under '対象' (Target), '対象外' (Exclude) is selected, and 'すべてのクラウド アプリ' (All cloud apps) is chosen. A warning message at the bottom states: '自分自身をロックアウトしないでください。このポリシーは Azure portal に影響します。実行する前に、自分または他のユーザーのアクセスをテストしてください。' (Do not lock yourself out. This policy affects the Azure portal. Test your access before running it.)

「条件」→「デバイスのプラットフォーム」の項目で、「Android」を選定ください。

The screenshot shows the '条件' (Conditions) configuration pane for the 'teams phone' policy. Under 'デバイスのプラットフォーム' (Device platform), '任意のデバイス' (Any device) is selected, and 'Android' is checked. Other options like 'iOS', 'Windows Phone', 'Windows', and 'macOS' are unchecked. The '構成' (Configuration) section shows 'はい' (Yes) selected. The '対象' (Target) section shows '任意のデバイス' (Any device) selected, and 'デバイスのプラットフォームの選択' (Select device platform) is also selected.

許可の項目で下記のように設定ください。

The screenshot shows the '許可' (Permissions) configuration pane for the 'teams phone' policy. Under '適用するコントロールを選択してください。' (Select the controls to apply.), 'アクセス権の付与' (Grant access) is selected. Under '多要素認証を要求する' (Require multi-factor authentication), 'デバイスが準拠しているとしてマーク済みである必要があります' (Must be marked as compliant) is checked. Other options like 'ハイブリッド Azure AD 参加済みのデバイスが必要' (Require hybrid Azure AD joined devices), '承認されたクライアント アプリが必要' (Require approved client apps), and 'アプリの保護ポリシーが必要' (Require app protection policies) are unchecked. A note at the bottom states: '複数のコントロールの場合' (When multiple controls are selected).



「レポートの有効化」で「オン」を選択して保存ください。

アクセス制御

許可 ① >

1 個のコントロールが選択され...

セッション ① >

0 個のコントロールが選択され...

ポリシーの有効化

レポート専用 オン オフ

条件付きアクセスはすべてのク
ライアントアプリをサポートす
るようになりました。このポリ
シーを保存すると、既存の動作
に影響する可能性があります。
既存の動作を変更しない場合
は、クライアントアプリの選択
を更新してください。

[保存](#)

上記の設定により、ターゲットユーザーが準拠していないデバイスでのTeamsへのサインインをブロックすることができます。ユーザーが準拠していないThinkSmart Viewでサインインしようとすると、下記のようなエラーメッセージが表示されます。



Intuneポータル上でも失敗したサインインの履歴が確認できます。

ホーム > Microsoft Intune > ユーザー | サインイン

ユーザー | サインイン
Contoso - Azure Active Directory

すべてのユーザー
削除済みのユーザー
パスワードリセット
ユーザー設定
問題の診断と解決

アクティビティ
サインイン

ダウンロード | トラブルシューティング | 更新 | 列 | フィードバックがある場合

許可された時刻: 過去 7 日間 | 日付を次の基準で表示: ローカル | フィルターの追加

許可された時刻	要求 ID	ユーザー	アプリケーション	状態	IP アドレス
2020/3/26 11:24:32	53a2507b-dd54-476...	Allan Deyoung	Microsoft Teams	失敗	175.171.184.160
2020/3/26 11:24:32	9f181c9b-12b6-4acc...	Allan Deyoung	Microsoft Teams	中断	175.171.184.160
2020/3/26 11:24:01	167f1b4c-ecd2-4a63...	Allan Deyoung	Microsoft Authentica...	成功	175.171.184.160
2020/3/26 11:23:53	c6303b13-7a79-4fcd...	Allan Deyoung	Microsoft Intune Co...	成功	175.171.184.160



サインイン失敗した履歴をタップして、詳細が確認できます。

The screenshot shows the Microsoft Azure portal interface for user sign-in management. The main view is a table of sign-in attempts. The first row is highlighted, showing a failed sign-in attempt for user Allan Deyoung on 2020/3/26 at 11:24:32. Below the table, the 'Details' section for this failed attempt is expanded, showing the policy 'teams phone' and the result '失敗' (Failed).

許可された時刻	要求 ID	ユーザー	アプリケーション	状態	IP アドレス
2020/3/26 11:24:32	53a2507b-dd54-476...	Allan Deyoung	Microsoft Teams	失敗	175.171.184.160
2020/3/26 11:24:32	9f181c9b-12b6-4acc...	Allan Deyoung	Microsoft Teams	中断	175.171.184.160
2020/3/26 11:24:01	167f1b4c-ecd2-4a63...	Allan Deyoung	Microsoft Authentica...	成功	175.171.184.160
2020/3/26 11:23:53	c6303b13-7a79-4fcd...	Allan Deyoung	Microsoft Intune Co...	成功	175.171.184.160
2020/3/26 10:59:37	52a289f0-384b-4753...	Allan Deyoung	Microsoft Intune Co...	成功	175.171.184.160
2020/3/26 10:59:26	27b289d4-6950-409...	Allan Deyoung	Microsoft Authentica...	成功	175.171.184.160
2020/3/26 10:59:20	4ac2cc2e-a063-45f1...	Allan Deyoung	Microsoft Intune Co...	成功	175.171.184.160
2020/3/26 10:46:55	a965c384-8707-408...	Adele Vance	Microsoft Teams	成功	175.171.184.160
2020/3/26 10:42:54	3970a2c5-b257-40b...	Adele Vance	Microsoft Teams	成功	175.171.184.160
2020/3/26 10:30:23	765f72fa-2eaf-4d20...	Adele Vance	Microsoft Teams	失敗	175.171.184.160

詳細

基本情報 場所 デバイス情報 認証の詳細 **条件付きアクセス** レポート専用 (プレビュー) 追加の詳細

ポリシー名	制御の許可	セッション制御	結果
teams phone	準拠しているデバイスが必要		失敗

ユーザー リスク ポリシーやサインイン リスク ポリシーのために、サインインは中断される可能性があります (ブロックされている、MFA チャレンジを受けているなど)。現在、このタブには条件付きアクセス ポリシーのみが表示されます。

デバイス情報の項目からユーザー利用したデバイスが準拠していないことを確認できます。
※準拠している場合項目の後ろに「はい」がついています。

The screenshot shows the 'Device Information' details page for a failed sign-in attempt. The 'Device Information' tab is selected, showing details for a Chrome Mobile device on an Android 8 operating system. The 'Compliant' status is highlighted in green, indicating the device is compliant.

項目	値
デバイス ID	7bef7d57-474e-48aa-8b2f-859751f0a239
ブラウザ	Chrome Mobile 61.0.3163
オペレーティングシステム	Android 8
準拠している	はい
マネージド	はい
結合の種類	Azure AD registered

第5章 PowerShellの活用

ユーザーモードの変更

Microsoft Teams IP Phone appは3つのモード（ユーザーサインインモード、専用電話機モード、電話ブースモード）で動作可能です。ユーザーサインインモードはMicrosoft Teams IP Phoneのすべての機能（通話、予定表及びボイスメール）を利用可能です。専用電話機モードもしくは電話ブースモードを利用したい場合、PowerShell経由で当該アカウントの属性を変更する必要があります。

事前準備（アカウントの管理を行うPCの要件）

Windows のバージョン

- Windows 10、Windows 8.1、Windows 8、または Windows 7 Service Pack 1 (SP1)
- Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、または Windows Server 2008 R2 SP1

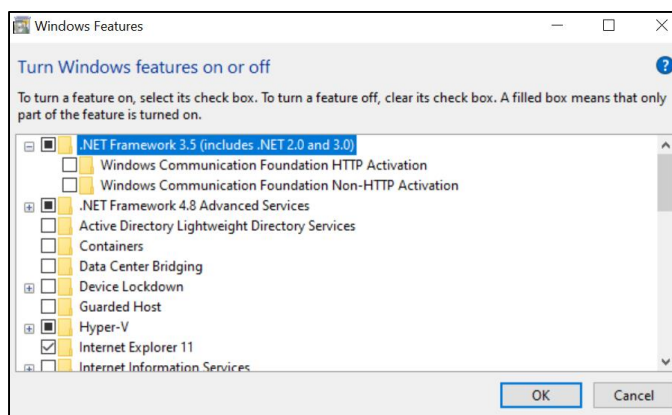
Windows Management Frameworkのバージョン

Windows 8、Windows 7 Service Pack 1 (SP1)、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 SP1 の場合は、Windows Management Framework 5.1 をダウンロードしてインストールください。

URL: <https://www.microsoft.com/en-us/download/details.aspx?id=54616>

Microsoft .NET Framework 3.5. x 機能を有効化

[Windows 機能の有効化または無効化] の項目の下の[.NET Framework 3.5 (.NET 2.0 および 3.0 を含む)] の項目に☑を入れてください。



PowerShellの実行ポリシーを設定

1. Windows PowerShell を管理者として実行
2. 次のコマンドを実行して、PowerShellの実行ポリシーを設定

PowerShell コマンド

```
Set-ExecutionPolicy RemoteSigned
```



ポリシー変更について確認が求められた場合には「Y」を入力してEnterを押してください。

3. 次のコマンドを実行して、Windows Remote Managementを設定

PowerShell コマンド

```
winrm qc
```

「WinRM はこのコンピューター上で要求を受信するように設定されていません。」のような内容が表示された場合は、「Y」を入力してEnterで先に進んでください。

4. 次のコマンドを実行して、基本認証が有効になっていることを確認
「Basic = true」であれば設定完了

PowerShell コマンド

```
winrm get winrm/config/client/auth
```

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\guoye2> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Users\guoye2> winrm qc
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Start the WinRM service.
Set the WinRM service type to delayed auto start.

Make these changes [y/n]? Y

WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
WSManFault
    Message
        ProviderFault
            WSManFault
                Message = WinRM firewall exception will not work since one of the network connection types on this machi
ne is set to Public. Change the network connection type to either Domain or Private and try again.

Error number: -2144108183 0x80338189
WinRM firewall exception will not work since one of the network connection types on this machine is set to Public. Chang
e the network connection type to either Domain or Private and try again.
PS C:\Users\guoye2> winrm get winrm/config/client/auth
Auth
    Basic = true
    Digest = true
    Kerberos = true
    Negotiate = true
    Certificate = true
    CredSSP = false

```

Skype for Business Online Connector モジュールのインストール

Step1. Microsoft [ダウンロードセンター](https://www.microsoft.com/en-us/download/details.aspx?id=39366)からモジュールをダウンロード
<https://www.microsoft.com/en-us/download/details.aspx?id=39366>

Step2. SkypeOnlinePowershell.exe ファイルをダブルタップしてインストール

Step3. Windows PowerShell セッションを管理者の資格情報で開始

Step4. モジュールにアクセスするには、Windows PowerShell セッションで次のコマンドを実行

PowerShell コマンド

```
Import-Module "C:\Program Files\Common Files\Skype for Business
Online\Modules\SkypeOnlineConnector\SkypeOnlineConnector.psd1"
```





※ 参考資料: <https://docs.microsoft.com/en-us/skypeforbusiness/set-up-your-computer-for-windows-powershell/download-and-install-the-skype-for-business-online-connector>

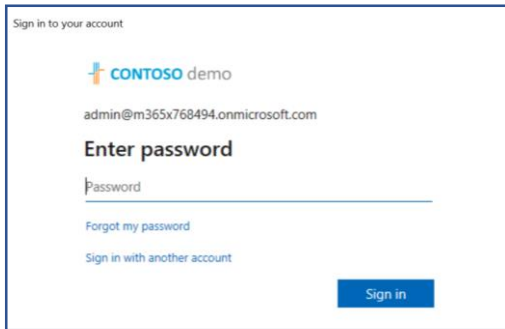
Skype for Business Onlineと接続

Step1. 管理者権限でSkype for Business Onlineと接続

PowerShell コマンド

```
Import-Module SkypeOnlineConnector
$sfbo = New-CsOnlineSession -UserName xxx@M365XXXXXXXXX.OnMicrosoft.com
Import-PSSession $sfbo
```

Step2. 管理者アカウントでサインイン

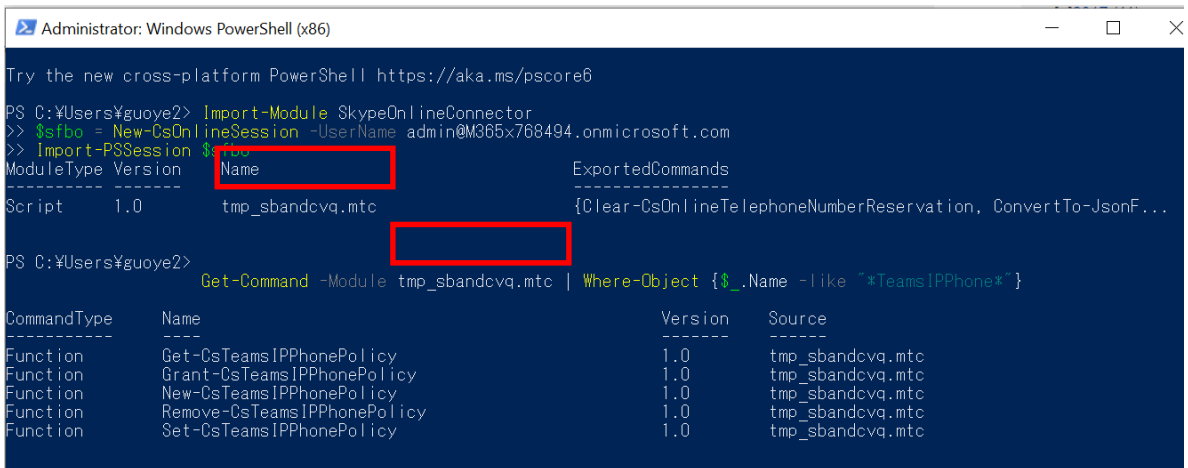


Step3. 下記のコマンドを利用してTeamsIPPhone利用可能なcmdletsをリストアップ

*赤い部分は前のコマンド1実行完了後、表示したNameの動的な値です。

PowerShell コマンド

```
Get-Command -Module tmp_sbandcvq.mtc | Where-Object {$_.Name -like "*TeamsIPPhone*"}
```





サインインモードの変更

現行設定を確認

PowerShell コマンド

```
Get-CsTeamsIPPhonePolicy
```

アカウントに電話ブースモードを割り当て

PowerShell コマンド

```
New-CsTeamsIPPhonePolicy -Identity "ユーザー指定 (例: MRSI)" -SignInMode MeetingSignIn  
Grant-CsTeamsIPPhonePolicy -PolicyName "ユーザー指定 (例: MRSI)" -Identity "ユーザー指定 (例:  
1234@M365xxxx. OnMicrosoft.com) "
```

上のコマンドの実行により、ThinkSmart Viewをアカウント1234@M365xxxx. OnMicrosoft.comでサインインする場合、ThinkSmart Viewを電話ブースモードで利用可能です。

PowerShell コマンド

```
New-CsTeamsIPPhonePolicy -Identity "ユーザー指定 (例: CAPSI)" -SignInMode  
CommonAreaPhoneSignIn  
Grant-CsTeamsIPPhonePolicy -PolicyName "CAPSI" - Identity "ユーザー指定 (例:  
5678@M365xxxx. OnMicrosoft.com) "
```

上記コマンドの実行により、ThinkSmart Viewをアカウント5678@M365xxxx. OnMicrosoft.comでサインインする場合、ThinkSmart Viewを共用電話機モードで利用可能です。

ホットデスクモードの有効化

Step1.

デフォルトでログインさせるリソースアカウントをCommonAreaPhone or MeetingRoomUIに設定

Step2. "AllowHotDesking"のフラグが"True"になっていることを確認

PowerShell コマンド

```
Get-CsTeamsIpPhonePolicyコマンド
```

AllowHotDeskingがFalseの場合、以下のコマンドで変更可能

PowerShell コマンド

```
Set-CsTeamsIpPhonePolicy -Identity "ユーザグループ指定" -AllowHotDesking $True
```

ホットデスクモード自動終了時間の設定

ユーザーが一定の時間、ThinkSmart View上で操作していない場合、強制的にサインアウトさせることができます。タイムアウト時間についての設定はPowerShellより管理できます。下記のコマンドをご参照ください。

PowerShell コマンド

```
Set-CsTeamsIpPhonePolicy -Identity "ユーザグループ指定" -HotDeskingIdleTimeoutInMinutes 分数
```


**Smarter
technology
for all**

Lenovo