Ivanti Neurons for MDM 92管理者ガイド

2023年7月

目次

Ivanti Neurons for MDM について

Ivanti Neurons for MDM は、モバイルセキュリティ対する新しいアプローチであり、高い拡張性、セキュリティ、更新の利便性を備えたインフラで統合エンドポイント管理(UEM)ソリューションを提供することにより、世界中の何百万台ものデバイスをサポートします。

- スピーディーな更新:ソフトウェアとセキュリティの更新を自動的に取得し、新しい機能は提供と同時に利用可能です。
- オンデマンドの拡張性:ビジネスニーズの変化に応じて導入規模を調節できます。容量計画の心配は要りません。
- ハードウェアコストを最小化:クラウドベースのサービスなら、オンプレミスのハードウェアを維持する必要がなく、管理に必要な物理的スペースはゼロです。
- 高い稼働率と可用性。
- 既存の投資を最大限に活用:ITリソースをハードウェアのメンテナンスからビジネスに価値を付加する戦略的な業務に移すことができます。

本リリースの「新しい機能の概要」ページ6をご覧ください。

新しい機能の概要

このセクションでは、本リリースの新しい機能や機能拡張について概説します。機能や機能拡張に関する参考文献やドキュメンテーションも適宜提供します。

「一般的な機能と機能拡張」下

「Androidの機能」ページ9

「iOS、macOS、tvOSの機能」ページ10

「Windowsの機能」ページ11

「Mobile Threat Defenseの機能」ページ11

一般的な機能と機能拡張

- **iOSデバイス、macOSデバイス、Androidデバイス用に追加されたレポートカラム: [レポートデータ]** タブに、[スケジュール済みのレポート] 用の新しいレポートカラムが追加されています。新しいレポートカラムを選択するには **[すべてのカラムを選択]** チェックボックスを使用して、リストに表示されているすべてのカラムを選択できます。

- **AppStoreFront CAへのSID組み込みのサポート:** このリリースから、LDAPユーザー向けのすべての新規デバイス登録で、AppStoreFront認証機関にSIDが含まれます。既存のデバイスに対してSIDを割り当てる必要がある場合は、そのデバイスを再登録する必要があります。また、このリリースから、AppStoreFront認証機関は、証明書が期限切れになった時点でSIDを付けて自動的に更新されます。

- **Sentryルート証明書の配布オプションの編集サポート:** 管理者は、Sentryルート証明書構成のデフォルトの配布を、配布ページから編集できるようになりました。Sentryルート構成はタイプ証明書であるため、カスタム配布を介して他のスペースに委譲できるようになりました。また、構成を他のスペースに委譲することにより、カスタムスペース管理者に編集許可を提供することもできます。詳細については、「AppTunnelの設定」ページ778を参照してください。

- **ルールビルダーに新しい属性が追加されています:** ルール、配布、またはグループを作成し、SCIMカスタム属性に照らして同期できるように、ルールビルダーにカスタムIDP属性が追加されています。詳細については、「配布フィルター」ページ371と「属性」ページ1044を参照してください。
- **ネイティブクライアント向けのアプリカタログにより、MAM-Onlyデバイス用のGoクライアントアプリケーションに追加される、Apps@Workタブ:** ネイティブクライアント向けのアプリカタログ構成により、MAM-Onlyデバイスのデバイス登録中に、Goクライアントアプリケーションに Apps@Workタブが追加されます。Apps@Workタブには、アプリカタログからのアプリケーションのリストが表示されます。これは、Ivanti Neurons for MDMリリース92以降のみに当てはまります。
- **管理対象Apple IDの新規オプション:** パターンマッチング用に、管理対象Apple IDに**userUPN**ドメインオプションが追加されています。詳細については、「Ivanti Neurons for MDMとAzure Active Directoryユーザーソースとの接続」ページ1223、「ユーザープロビジョニング-Azure Active Directory」ページ1136、「Apple Business Managerでのユーザー登録」ページ106、「LDAPサーバーの構成」ページ1146を参照してください。

- **デバイスログ内にあるアプリインストール詳細の表示と検索**：このリリースから、[デバイスの詳細] > [ログ] > [詳細] カラムで、アプリケーションのインストールの詳細を表示できます。新たに追加された検索バーで、特定のステータスを検索することもできます。すべてのデバイスに関して、ステータスとして以下の詳細が示されます。

  - アプリ名、アプリバージョン、バンドル、またはパッケージID
  - インストールのステータス
  - エラーとエラーの理由
    例：appOrConfigName=Name:<アプリ名>;Identifier=<バンドルID>;iTunesStoreId:<iTunes ID>;Status:<Appleからのステータスまたはエラーの理由>version: <アプリバージョン>

  Windowsデバイスに関しては、ステータスとして以下の詳細が表示されます。

  - バンドルIDまたはパッケージID、ステータス、エラーを含む
    例：
    - タイプの場合 - アプリケーションインベントリとステータス - 承諾 - 表示 - アプリタイプ
    - タイプの場合 - アプリケーションインベントリとステータス - 送信 - 何も表示しない
    - タイプの場合 - インストール/アンインストールとステータス - 成功/失敗/送信中 - 表示：バンドルIDまたはパッケージID、ステータス、名前、バージョン、エラーを含む

  詳細については、デバイスログの検索 >「デバイスの基本」ページ165を参照してください。

- **更新されたデバイスクリーンアップ設定**：デバイスクリーンアップ設定が更新され、次のプロセスが追加されました。

  - **ワイプ保留中デバイスの削除**：このリリースから、ワイプされる予定のデバイスを削除できます。
  - **撤去保留中のデバイスを撤去**：このリリースから、撤去される予定のデバイスを撤去できます。

  詳細については、「デバイスクリーンアップ設定」ページ1050を参照してください。

- **デバイスからのアプリのアンインストール(除外または再配布)のサポート**：管理者は、iOSデバイスおよびmacOSデバイスからアプリを除外または再配布できるようになりました。詳細については、「デバイスの基本」ページ165とアプリの除外または再配布を参照してください。

Androidの機能

- **Android EnterpriseデバイスでのIvanti TunnelとVPNの構成**：Ivanti TunnelとVPNの構成は、Android Enterpriseモードのデバイスでは廃止されました。Ivanti Tunnelアプリ用のマネージド構成を使用することをお勧めします。詳細については、「Tunnel」ページ777と「VPN構成」ページ823を参照してください。
- **ネットワークログとセキュリティログの委譲のサポート**：AMAPIモードでネットワークログとセキュリティログの委譲がサポートされるようになりました。詳細については、「アプリのカタログ」ページ286を参照してください。
- **Androidデバイスの再割り当て**：管理者は、Androidデバイスの所有権をあるユーザーから別のユーザーに移せるようになりました。これには、SUEM-Premiumライセンスが必要です。詳細については、「Androidデバイスの再割り当て」ページ253を参照してください。
- **Androidデバイスの再割り当て**：Androidデバイスの再割り当ては、SUEM-Pのみで利用できます。
- **キオスクモード可アプリ**：管理者は、共有キオスクモードでフォルダーを作成し、これらのフォルダーにアプリを移動できます。詳細については、「ロックダウン＆キオスク：Android Enterprise」ページ571を参照してください。
- **WhiteLabel設定の機能拡張**：WhiteLabel設定に新たな機能拡張が追加されました。詳細については、Help@Workを参照してください。

iOS、macOS、tvOSの機能

- **Apple宣言型デバイス管理のサポート:** Appleの宣言型デバイス管理は、マネージドデバイスがそれぞれの独自の管理設定を積極的かつ自律的に、より少ない通信で利用できるようにする、現代的な管理プロトコルです。宣言型デバイス管理は、新たに登録されたデバイスの場合は登録中に、すでに登録済みのデバイスの場合はチェックイン中に有効化されます。

  宣言型デバイス管理は、次のような資格のあるデバイス上では、自動的に有効化されます。

  - macOS 13以降を搭載したコンピューター
  - iOS 16またはiPadOS 16以降を搭載したデバイス
  - iOSまたはiPadOS 15以降でユーザー登録をサポートする宣言型デバイス管理を介して登録されたデバイス。
  - tvOS 16以降を搭載したApple TVデバイス

  このリリースでは、次のようなステータスチャネルについても宣言型管理のサポートを追加します。

  - OSバージョンに対する変更
  - パスコードコンプライアンス
  - 現在のパスコード

    つまり、パスコードコンプライアンスのステータスの変更、あるいはOSバージョンの変更があるたびに、デバイスはリアルタイムでサーバーと通信します。これにより、自動化されたアクションやコンプライアンスポリシーが、はるかに迅速に、リアルタイムでトリガーされます。
    詳細については、「デバイスの基本」ページ165を参照してください。

- **イーサネット構成およびWiFi構成での証明書複数選択のサポート:** イーサネット構成およびWiFi構成では、[信頼性のあるサーバー証明書名]フィールドから複数の証明書を選択できるようになりました。詳細については、「イーサネット構成(macOS)」ページ917と「Wi-Fi構成」ページ865を参照してください。

- **配布対象の構成と優先度の高いアプリケーションは、「自動デバイス登録」されるデバイスの設定中にインストールされます:** このリリースから、DEPプロファイルで **[構成および優先度の高いアプリケーションがデバイスにプッシュされるまで待機]** オプションが有効になっている場合は、配布対象の構成と優先度の高いアプリケーションはすべて、「自動デバイス登録」されるデバイスの設定中にバックグランドでデバイスにインストールされます。詳細については、「デバイス登録」ページ1162をご参照ください。

Windowsの機能

- **Windows 10+デバイスへのソフトウェア更新のインストール:** Windows 10+デバイスへのソフトウェア更新のインストール – Windows 10+デバイスのソフトウェアを更新する場合、[更新のインストール元となるブランチ] オプションが更新されています。詳細については、「ソフトウェア更新」ページ668を参照してください。
- **Windows向けの新しいIvanti Apps@Workアプリ:** Apps@Workアプリに次のような変更が行われました。
  - Ivantiロゴによるリブランディング
  - 汎用版のApps@WorkのIDがMobileIronAtWorkEMMからIvantiAtWorkUEMに更新されました。
  - Apps@Workのバージョンシリーズが「9.6.0.0」から「10.0.0.0」に更新されました。

  すでにApps@Workアプリをデバイスにインストール済みのテナントでリリースのアップグレードを行った場合は、Ivantiにリブランディングされ Apps@Workアプリがアプリカタログに追加されます。ただし、リブランディングされたバージョンは、自動的にはデバイスに配布されず、手動配布を実行する必要があります。新規テナントの場合は、リブランディング後のバージョンのみがアプリカタログで利用可能になります。このバージョンは、デフォルトでは **[全員に配布]** に設定されます。
- **Microsoft Defender for Endpoint(旧称Windows Advanced Threat Protection) 構成のサポート:** Microsoft Defender for Endpointを使用することでお客様は、Microsoft Purviewおよびその他のAzureサービスを活用できます。詳細については、「Microsoft Defender for Endpoint」ページ722を参照してください。
- **Autopilotインストール中のO365アプリのインストール:** O365アプリ構成を、Autopilot登録ワークフローの実行中にインストールできるようになりました。デバイスがエンドユーザーにリリースされた時点で、O365アプリはすでに利用可能であり、デバイスにインストールされた状態になっています。詳細については、「Windows Autopilotプロファイルの構成」ページ1202を参照してください。
- **デバイスグループを作成するための新しいハードウェア属性:** [デバイスグループを作成] セクションと [カスタムポリシー] セクションに新しいハードウェア属性(メーカー、全デバイス容量、メモリ合計(MB))が追加されました。詳細については、「デバイスグループ」ページ182を参照してください。

Mobile Threat Defenseの機能

Mobile Threat Defense(MTD)は、デバイス、ネットワーク、アプリケーションに影響を与えるモバイル脅威や脆弱性からマネージドデバイスを保護します。最新リリースに該当するMTD関連の機能については、Ivantiの製品ドキュメンテーションページの [MOBILE THREAT DEFENSE] セクションから、お使いのプラットフォームに対応するMobile Threat Defenseソリューションガイドを参照してください。

MTDガイドの各バージョンには、サーバー環境とクライアント環境の両方で完全にテストされ、提供されているMobile Threat Defense機能がすべて含まれます。サーバーリリースとクライアントリリースの差により、新しいバージョンのMTDガイドは、シリーズの最終リリースで機能が完全に動作するようになってから公開されます。

はじめに

このセクションでは、Ivanti Neurons for MDMポータル全体にわたる相互作用を必要とする機能のセットアップと使用法の概要について説明します。このセクションは以下のトピックを含みます。

ソリューション概要

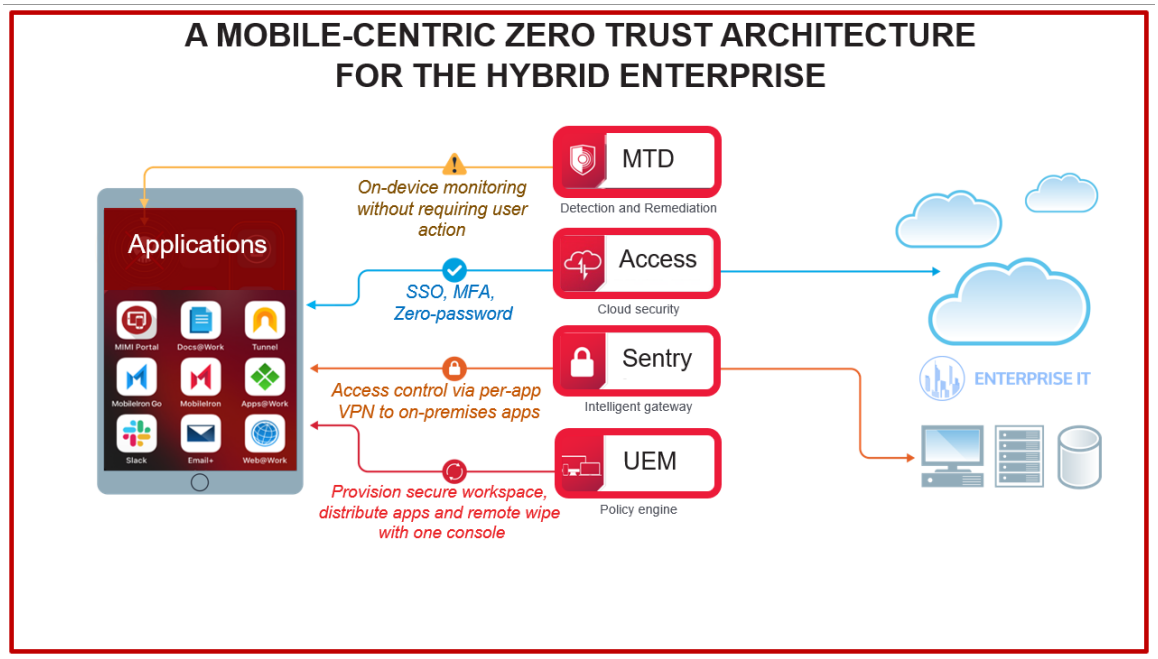
企業ネットワーク外のモバイルデバイスやその他のエンドポイントからビジネスデータに継続的にアクセスするには、セキュリティに重点を置く必要があります。現在のセキュリティニーズに対応するために、企業は以下のような方法を検討する必要があります。

- 携帯電話やノートパソコンなどのエンドポイントのプロビジョニング
- 一連の必須データに基づくアクセス許可
- 保存データと通信中データの保護
- 必要に応じた対策の実施

現在のこの問題に対するIvantiソリューションは、このすべての課題に対応します。エンドポイントを監視し、アダプティブなポリシーをトリガーして脅威の対策、デバイスの隔離、コンプライアンス維持を実行できます。合わせて、以下のコンポーネントを利用すると、モバイルを中心ゼロトラストのフレームワークを実現するのに役立ちます。

- **Ivanti Neurons for MDM** - これを利用すると、ユーザーの役割に応じたアプリ、設定、ポリシーを備えたセキュアなワークスペースをあらゆるデバイス上に構築できます。ユーザーは、生産性の向上のために必要なリソースに簡単かつ安全にアクセスできます。
- **Sentry** - オンプレミスのリソースへのセキュアなアクセスに役立つインラインのインテリジェントなゲートウェイです。
- **Access** – ユーザー、デバイス、アプリ、ネットワークの種類、脅威の有無などの確認に役立ちます。アダプティブなアクセス制御チェックがゼロトラストモデルの基盤です。Accessは、シングルサインオンとクラウド上のセキュリティを提供します。
- Mobile Threat Defense - Ivanti Neurons for MDMとMobile Threat Defense(MTD) を組み合わせることにより、保存データと通信中データを最先端の暗号化で保護し、脅威の監視によってデバイス、ネットワーク、アプリレベルの攻撃を検出します。

次の図はソリューションの概要を示します。



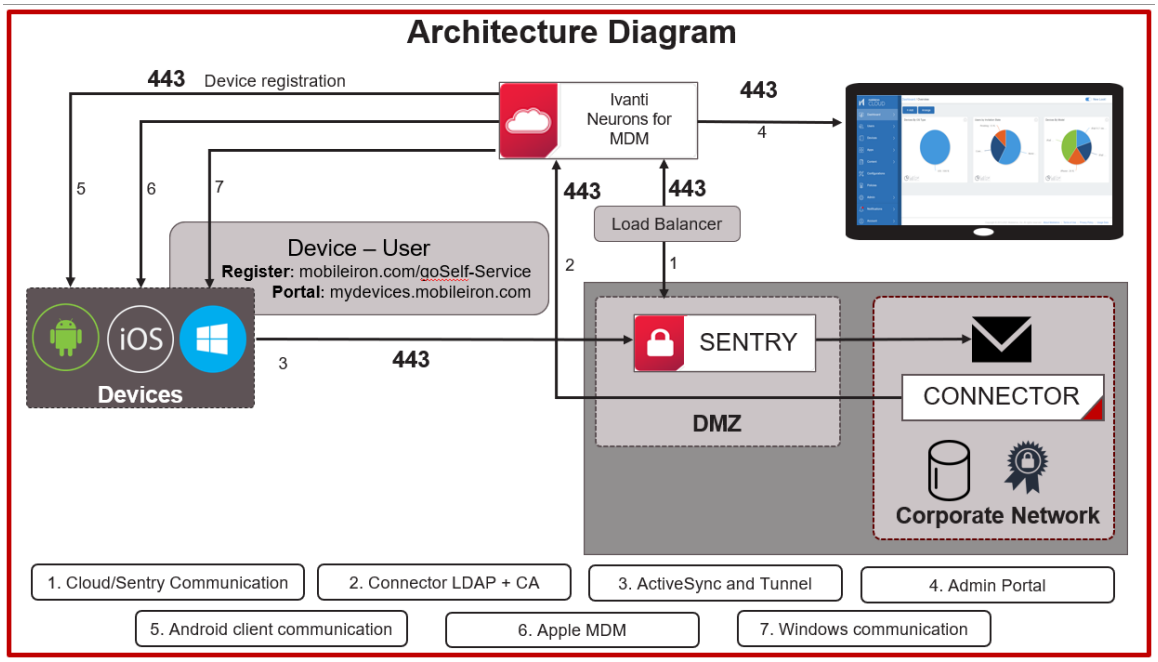
重要な機能

Ivanti Neurons for MDM プラットフォームは、IT部門への可視化と制御で、重要なビジネスデータにアクセスする企業所有または従業員所有のモバイルデバイスやデスクトップのセキュリティ、管理、監視を実現します。Ivanti Neurons for MDM プラットフォームは、社内で使用される従業員の多様なデバイスを保護し、デバイスのライフサイクル全体を管理できます。

- ポリシーの構成管理と適用
- アプリの配布と管理
- デスクトップデバイスのスクリプト管理と配布
- デバイスアクション
- アクセス制御と多要素認証
- 脅威検出と修復

アーキテクチャの図

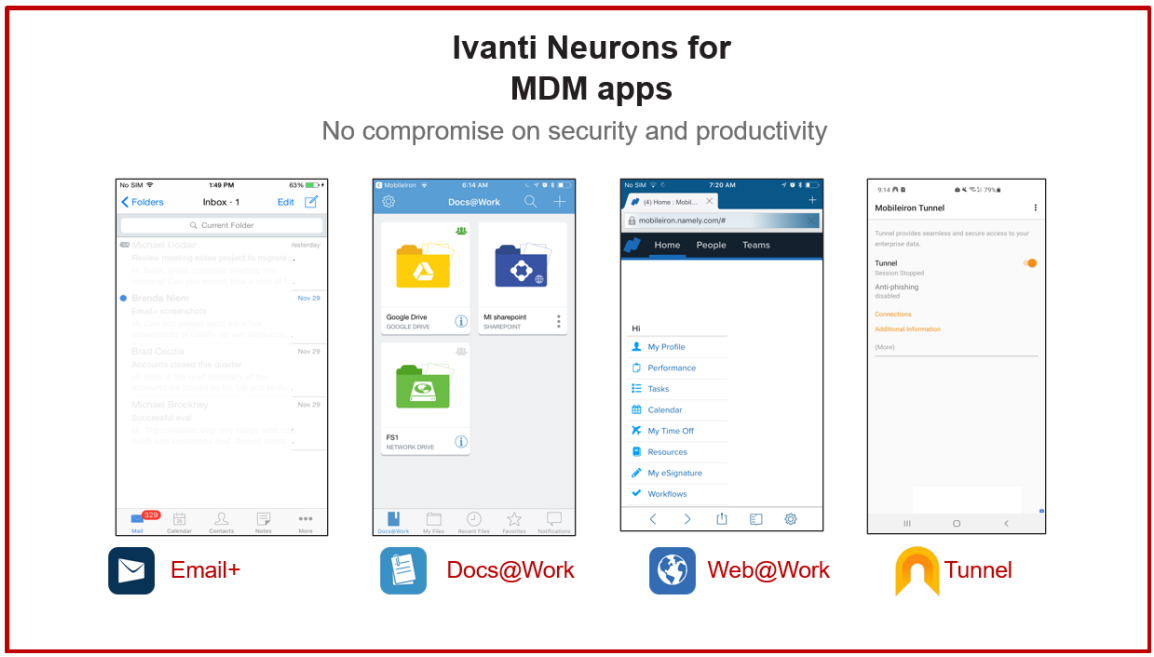
以下の図は Ivanti Neurons for MDM UEMプラットフォームのアーキテクチャ概要を示します。



Ivanti Neurons for MDM アプリケーション

- **アプリカタログ** – アプリカタログは、カスタマイズ可能な企業向けアプリストアです。IT管理者はプライベートアプリまたは自社開発アプリをエンドユーザーのデバイスに直接発行できます。アプリカタログをAppleのボリューム購入プログラムと組み合わせることで、iOSデバイス上のモバイルアプリのセキュアな配布を促進できます。さらにIvantiは、iOSマネージドアプリやAndroid Enterpriseの機能を利用することもできます。これにより、両方の高度なアプリセキュリティ機能に対し、アプリレベルの設定やセキュリティポリシーをIvanti Neurons for MDM UEMプラットフォーム内で簡単に構成することができます。
- **Email+** - iOSとAndroidに対応するクロスプラットフォームのセキュアなPIMアプリです。Email+は、社内のActiveSyncサーバーと通信することにより、社有および個人のデバイス上でセキュアなメール、カレンダー、連絡先、タスク機能を提供します。
- **Docs@Work** - Microsoft SharePointなどのリポジトリ、Box、Dropboxなどのクラウドサービス上のコンテンツへのアクセス、コンテンツの作成、編集、マークアップ、共有のセキュアな実行を可能にします。これは、ユーザーが出先でも最大限の生産性を発揮するために重要です。
- **Web@Work** - 企業のユーザーが社内イントラネットにあるウェブコンテンツにセキュアにアクセスできるようにするためのセキュアなブラウザです。Web@Workを利用すると、企業データへのアクセスを許可されたユーザーにのみ限定することができます。Web@WorkをApp Tunnelと併用すると、通信中の企業データのセキュリティが確保されます。Web@Workでは、ユーザーが社内Webリソースに短時間で容易にセキュアにアクセスできます。

次の図はIvanti Neurons for MDM アプリケーションを示します。



役割

管理者 - エンタープライズ管理者は、以下のタスクに責任を負います。

- ワークスペースのメール、アプリ、設定、Wi-FiやVPNなどの接続に、企業ユーザーがシームレスかつセキュアにアクセスできるようにする。
- 従業員のデバイス上で個人データとビジネスデータを分離し、ビジネスデータが個人のアプリに漏えいしないように、また、IT部門が不用意に個人データにアクセスしないようにする。

ユーザー – 企業ユーザーとして、安全な最新のモバイルデバイス、デスクトップ、クラウドサービスからビジネスアプリケーションや個人データにシームレスにアクセスすることができます。ユーザーとして実行できる各種タスクに関する詳細については、「ユーザー」ページ78を参照してください。

はじめに

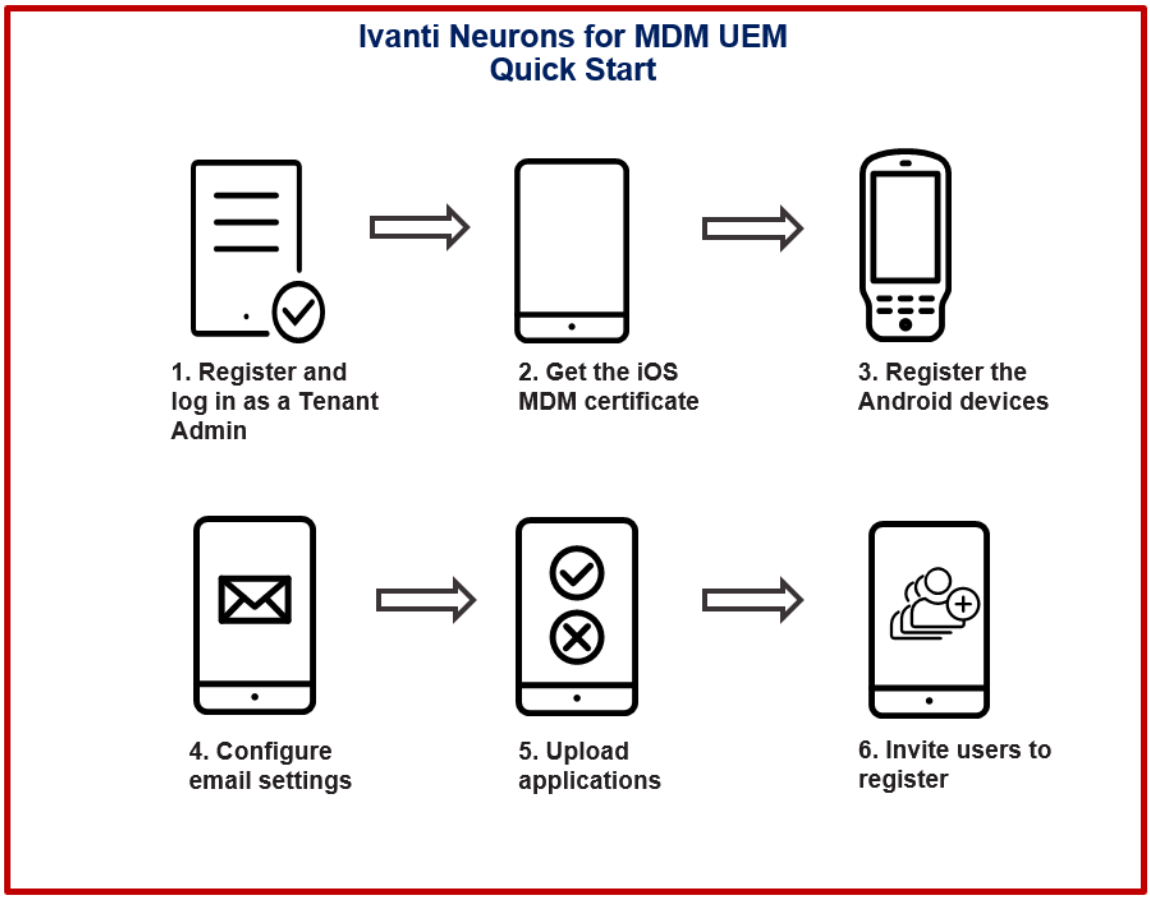
新規ユーザーとして登録された方は、このセクションに記載されている手順に従うとすぐにIvanti Neurons for MDMサービスを導入展開していただけます。

Ivanti Neurons for MDMプラットフォームの配信登録後、Ivantiがお客様のIvanti Neurons for MDMテナントを作成します。登録したメールアドレスにメールが届きます。そのメールには、お客様の会社用に作成されたテナントに関する以下の情報が記載されたPDFが含まれています。

- ご購入いただいたソフトウェアバンドルに関する情報
- テナントのURLおよびスーパー管理者のログイン認証情報
- サポートコミュニティとFAQへのアクセス方法 Ivanti Neurons for MDM
- 技術文書のアクセスとソフトウェアのダウンロードを行う場所

Ivanti, Incではソフトウェアキーは提供されません。スーパー管理者の認証情報でIvanti Neurons for MDMテナントにログインし、利用規約に同意することで、Ivanti Neurons for MDM製品が有効化されます。

以下の図で、Ivanti Neurons for MDMを開始する手順について説明します。



手順

1. テナント登録メールに記載されているURLをクリックします。パスワードリセットのプロンプトが表示されます。
2. パスワードを変更します。
3. IDとパスワードを使用してテナントアカウントにログインします。ウェルカムウィザードが表示されます。
4. **[ウェルカム]** フォームに詳細を入力し、利用規約と合意事項に同意し、**[続行]** をクリックします。
5. iOS MDM証明書をインストールするには、「MDM証明書のインストール」ページ1184を参照してください。

> 後でiOSデバイスを管理したい場合は、iOS MDM証明書のインストールをスキップすることができます。その後、ウィザードの指示に従い、企業のAndroidデバイスを登録します。iOS MDM証明書のインストールをスキップすると、iOSデバイスを登録できなくなります。ユーザーには、iOSデバイスの登録が有効化されていないというメッセージが表示されます。

6. Android Enterprise(AE) モードでAndroidデバイスを登 録 するには、「マネージド Google Playアカウント (Android Enterpriseアカウント) 」 ページ1263を参 照してください。その後 、ウィザード にはメールアカウント セットアップのプロンプト が表 示されます。

   > 後 でAndroidデバイスを管 理したい場 合 は、Androidマネージド Google Playアカウント 登 録 をス キップすることができます。マネージド Google Playアカウント 登 録 をスキップすると、Android Enterpriseデバイスを登 録 できなくなります。Androidデバイスをデバイス管 理 者 に登 録 すること はできますが、マネージド Google Playやアプリ構 成 のような主 要 機 能 は使 用 できません。

7. メール設 定 およびActiveSyncを構 成 するには、「Exchange構 成 」 ページ736および「Eメール構 成 」 ページ 732を参 照してください。

8. **[続 行]** をクリックします。パスコード の作 成 プロンプト が表 示されます。

9. パスコード のタイプを選 択し、**[続 行]** をクリックします。

10. アップロードしたいアプリを選 択し、**[続 行]** をクリックします。

11. ユーザーのメールアドレスを指 定し、**[続 行]** をクリックします。ユーザーはモバイルデバイスを登 録 するため のメールを受 信します。構 成 の概 要 が表 示されます。

12. **[完 了]** をクリックします。ダッシュボード ページが表 示されます。

13. 詳しく見 るには、次 の手 順 を実 行します。

    - **[ユーザー]** を開きます。招 待 されているすべてのユーザーが表 示されます。
    - **[アプリ]** を開きます。アップロードしたすべてのアプリが表 示されます。
    - **[構 成]** を開きます。登 録 時 にプッシュしたすべての構 成 が表 示されます。

管 理 者 として実 行 できる各 種 タスクの詳 細 は、「管 理 」 ページ1042セクションを参 照してください。

ブラウザの言 語 設 定

サポートされていない言 語 をブラウザ言 語 に設 定している場 合 、ユーザーはポータルのデフォルト 言 語 として [en_US](米 国 英 語) を選 択 できます。

macOS 10.15+デバイスで実 行 するSafariブラウザで言 語 を設 定 するには、以 下 の手 順 に従 います。

1. macOSデバイスで **[システム環 境 設 定]** を開きます。
2. **[言 語 と地 域] > [一 般]** を開きます。

3. **[en_US]**(または任 意 の言 語) を **[優 先 する言 語]** に設 定 します。

Ivanti Neurons for MDM and Access の未 定 義 のナビゲーション インターフェイス

一 部 のクラスターの新 規 のお客 様 には、Ivanti Neurons for MDM とナビゲーションインターフェイスの統 一 された Accessが提 供 されます。Ivanti Neurons for MDM 管 理 者 認 証 情 報 でログインしてください。Accessのオプション は、独 立 したタブとして左 のナビゲーションペインに表 示 されます。Accessの詳 細 とAccessの設 定 方 法 は、製 品ドキュメンテーションから [Access] をクリックしてください。

統 一 ナビゲーションインターフェイスには、以 下 の機 能 があります。

- Ivanti Neurons for MDM とAccessの両 方 への統 一 ログイン。
- 左 ナビゲーションペインに Ivanti Neurons for MDM とAccessを切 り替 える製 品 選 択 機 能 。
- 製 品 選 択 の記 憶 : 初 回 ログイン時 には Ivanti Neurons for MDM 管 理 ポータルが表 示 されます。2回 目 以 降 のログインでは、初 回 ログイン時 の製 品 選 択 を反 映 し、Ivanti Neurons for MDM またはAccessが 表 示 されます。
- Ivanti Neurons for MDM とAccessの両 方 に対 応 する左 ナビゲーションペイン。
- 統 一 アカウント設 定 ペインに、アップグレードオプション、ドキュメンテーション、サポートポータル、パスワード 変 更 、サインアウトなどへのリンク。

Androidデバイスを管 理 するデバイス管 理 者 (DA) モード - 廃 止

Androidデバイスを管 理 するデバイス管 理 者 (DA) モードは、Ivanti Neurons for MDM 78から段 階 的 に廃 止 されています。

Ivanti Neurons for MDM 78で新 しいテナントを作 成 した新 規 ユーザーはDAモードでデバイス(Android 6以 降) を登 録 できません。Android 6～ Android 9でDA登 録 を有 効 化 する必 要 のある新 規 テナントはIvantiのサポートに問 い合 わせる必 要 があります。

- Android 10以 降 のデバイスのDAモード への登 録 は引 き続 きブロックされます。
- 既 存 ユーザー(既 存 のDAの有 無 を問 わず) による既 存 DAデバイス(Android 6～ Android 11) の管 理 に変 更 はありません。しかし Ivanti Neurons for MDM 78にアップグレードした場 合 、既 存 のテナントでAndroid 10+を実 行 する新 規 登 録 デバイスはDAモードで実 行 できません。既 存 のテナントでは、Android 6～ Android 9のデバイスのみDAモードで登 録 できます。

- Coreインスタンスから Ivanti Neurons for MDM R78へDAデバイスを移行する場合、移行を開始する前に、Android Enterpriseが有効化されていて、1つ以上のシステム構成がターゲットセット(PO、DO、COPEのいずれか)に配布されていることを確認してください。移行後のデバイスの撤去を防ぐには、この手順が必須です。

DA登録の種類	既存テナント(78にアップグレード)	新しい78テナント(アップグレードなし)
10以降のデバイスの新規DA登録	許可されていません	許可されていません
10より前のデバイスの新規DA登録	許可されました	許可されていません
10以降の既存DAデバイス	引き続きアクティブ	不適用
10より前の既存DAデバイス	引き続きアクティブ	不適用
10以降の移行DAデバイス	撤去	撤去
10より前の移行DAデバイス	引き続きアクティブ	撤去

macOSデバイスの構成

ここではIvanti Neurons for MDM内のmacOSデバイスの一般的な設定手順や関連コンテンツを列記し、概要をご紹介します。すべてのmacOS関連トピックは*Ivanti Neurons for MDM管理者ガイド*でお読みいただけます。

目次

デバイスの登録

ほとんどのユーザーがまずデバイスを登録します。以下のいずれかの方法で、登録プロセスを開始できます。

- 1人以上のエンドユーザーに招待状を送る(iReg登録)。詳細については、デバイス登録セクションの*macOSデバイス登録*トピックを参照してください。
- Device EnrollmentおよびApple Business Managerでのユーザー登録

詳細はデバイス登録を参照してください。

ユーザー招待テンプレートの構成

エンドユーザー招待メールをブランディングし、エンドユーザーにとって見慣れたデザインにすることができます。詳細はメールテンプレートのブランディングを参照してください。

デバイス登録のプロセスは、ユーザーに知られている名前やロゴを入れてカスタマイズできます。詳細はユーザーブランディングを参照してください。

詳細は登録確認メールの構成と使用を参照してください。

ゼロ・サインオン機能の設定

ゼロ・サインオン関連の情報は*Access*ガイドの「Accessでのゼロ・サインオン」を参照してください。

ゼロタッチ自動登録については、「新規デバイス登録のための設定の構成」セクションの手順13のユーザ設定を参照してください。

macOS対応Mobile@Workクライアントの設定

macOS対応Mobile@Workアプリは以下を提供します:

- macOSデバイスでのスクリプト記述機能
- エンドユーザー向けのApp Catalog
- プッシュ通知
- 自動Device Enrollment登録用のユーザーオンボーディング(ようこそ/ステータス)画面

Mobile@Workをエンドユーザーにプッシュする前に、「macOS対応Mobile@Work」 ページ628が作成されており、ターゲットのmacOSデバイスに配布されるように設定されていることを確認してください。

macOSデバイスのユーザーオンボーディングは、自動Device Enrollmentプロセス中に有効化できます。Device Enrollmentが完了すると同時に、macOS対応Mobile@Workと各種プロファイル、構成、アプリがデバイスにプッシュされます。

macOSシェルスクリプトの設定

Ivanti Neurons for MDMでは、独自のmacOSシェルスクリプトを作成した後、Ivanti Neurons for MDMにアップロードし、マネージドmacOSデバイスで実行することができます。macOS対応Mobile@Workスクリプト構成を使用してスクリプトを構成してください。macOS対応Mobile@Workは、スクリプトの実行結果をIvanti Neurons for MDMに戻します。これは、デバイスログに表示されます。デバイスログは、macOSデバイスの **[ログ]** タブにあるデバイス詳細ページから確認できます。スクリプトリポジトリの作成、アップロード、管理については、すべてのスクリプトを参照してください。

macOSデバイスでシェルスクリプトを実行する前に、ユーザーがmacOS対応Mobile@Workアプリをデバイスで実行し、macOS対応Mobile@Work構成をデバイスにプッシュしていることを確認してください。スクリプトは1回または反復的に実行可能です。Ivanti Neurons for MDMでスクリプトを使用することにより、管理者はデバイスから情報を収集し、カスタム属性としてIvanti Neurons for MDMに保存することもできます。たとえばmacOSデバイスのJavaバージョンを知りたい場合、その情報を収集してカスタムデバイス属性でデバイスごとに保存できます。詳細はmacOS対応Mobile@Workの*macOS対応Mobile@Workスクリプト構成の作成*をご参照ください。

macOS構成の設定

構成とは、デバイスに送信する設定の集合体です。たとえば、構成を使用すると、これらのデバイス上のVPN設定やパスコード要件を自動的に設定することができます。この場合、**[構成]**ページを使用して、構成の選択、設定、配布を行います。多くの構成の種類が利用できます。このページでは、以下の構成を含め、使用可能なmacOS構成のリストを閲覧できます。

- Wi-Fi
- パスコード
- VPN
- 暗号化DNS
- FileVault 2
- FileVaultリカバリキー
- macOSのファイアウォール
- macOSの制約
- macOS AppStoreの制約
- macOS Finder設定
- macOSカーネル拡張ポリシー
- Active Directory(macOS)
- Office 365自動アカウント作成(macOS)

カスタム構成では、定義済みの構成ファイルをインポートおよび配布できます。

macOSポリシーの設定

ポリシーは、デバイスの要件、およびデバイスがその要件を遵守しなかった場合にどうなるかについて定義するものです。各ポリシーは、ルールとコンプライアンスアクション(ルール違反の場合に何が起こるか)で構成されています。**[ポリシー]** ページでは、ポリシーの選択、設定、配布を行うことができます。データ保護/暗号化の無効化および許可されたアプリはmacOS関連のポリシーです。カスタムポリシーでは、デバイスやユーザーの属性、セクション基準、値、指定するコンプライアンスアクションに基づいてカスタムポリシーを作成できます。

macOSアプリの配布

Ivanti Neurons for MDM Ivanti は、AppleのMDMプロトコルおよびMobile@Workアプリを使用したmacOSアプリの配布をサポートしています。管理者は以下のいずれかまたは両方を選択可能です。

- AppleのMDMプロトコル - 管理者は、所定のPKG形式(配布形式)のみ自社開発アプリとしてアップロードできます。また、Mac App Storeからアプリを配布することも可能です(Appleの「Appとブック」ライセンスサポートを含む)。ただしこの方法で管理者がDMGおよび他のPKG形式を配布することはできません。
- macOS対応Mobile@Workアプリ - ユーザーにアプリを配布する方法として、管理者はMobileIron Packager(MIP)アプリを使用して、任意のPKG、DMG、.appファイルをMIPファイルに変換できます。MIPファイルを社内開発アプリケーションとして Ivanti Neurons for MDM にアップロードします。

> Ivanti Neurons for MDM のMac PackagerユーティリティはMobileIronソフトウェアダウンロードからダウンロードします。

管理者はMobile@Workを使用し、DMG、PKG、.app形式の自社開発アプリを配布できます。Mac App Storeでのみ提供されるアプリの場合、管理者は「Appとブック」ライセンス機能を含むAppleネイティブのMDMを引き続き使用できます。

レポートおよび他の情報の確認

ダッシュボードは、登録されたデバイスおよびユーザーに関する重要な統計を示します。ダッシュボード上の各セクションをウィジェットと呼びます。

他の情報は以下の手順で確認します:

- 通知確認 - **[ダッシュボード > [通知]** ページを開き(または右上のベルアイコンをクリック)、通知を確認して必要なアクションを実行します。

- レポート - **[ダッシュボード] > [レポート]** ページで統合エンド管理(UEM)システムのデータにアクセスします。
- 監査証跡 - **[ダッシュボード] > [監査証跡]** ページを開き、Ivanti Neurons for MDM 内のすべてのエンティティで実行された活動の時系列記録にアクセスします。この機能を有効にするには、**[管理] > [インフラストラクチャ] > [監査証跡]** から **[監査証跡を有効化]** をクリックします。
- アプリ情報 - **[ダッシュボード] > [アプリ情報]** ページを開き、アプリの配布状況や他の情報を閲覧および分析します。

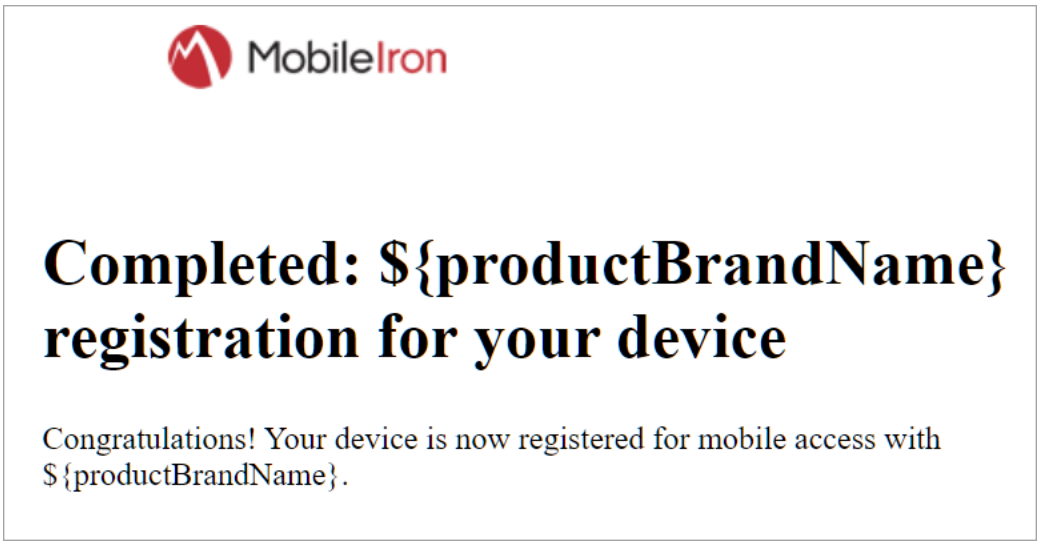
登録確認メールの構成と使用

管理者は、ユーザーが登録を完了した後、メールを構成またはトリガーすることができます。このメールには、登録を終えたユーザーへの注意事項などが含まれます。管理者はユーザーを招待する際にこのメールの送信を有効化します。s

手順は以下のとおりです。

- **機能の構成：**
  - メールテンプレートを構成します。

    英語のメールテンプレートはデフォルトで以下のようになっていますが、「メールテンプレートのブランディング」ページ1304の「メールテンプレートのカスタマイズ」ページ1305に記載された指示に従い、目的に合わせて変更が可能です。

  - 登録確認メールをオンにします。「ユーザー設定」ページ89の「ユーザー登録確認メールの構成」ページ100を参照してください。
- **機能の使用：**
  - 「ユーザーの招待」ページ140の説明に従ってユーザーに登録招待メールを送信します。ユーザーの登録が完了すると、Ivanti Neurons for MDM はユーザーに登録確認メールを送信します。

ポリシーコンプライアンス通知メールの構成と使用

管理者は、ポリシーコンプライアンス通知メールテンプレートに、カスタム/許可されたアプリポリシーのメール送信アクションがコンプライアンス違反のデバイスを持つユーザーに送信するメールをラップすることができます。以下のプロセスで構成を説明します:

- **機能の構成:**
  - **メールテンプレートを構成します。**

    英語のメールテンプレートはデフォルトで以下のようになっていますが、「メールテンプレートのブランディング」ページ1304の「メールテンプレートのカスタマイズ」ページ1305に記載された指示に従い、目的に合わせて変更が可能です、

  - **ポリシーコンプライアンス通知テンプレートをオンにします。**このテンプレートは、カスタム/許可されたアプリポリシーのメール送信アクションを使用して作成するメッセージとともに機能します。Ivanti Neurons for MDM は、メールアクションに指定した情報をポリシーコンプライアンス通知テンプレートに挿入します。ポリシーコンプライアンスメールテンプレートは、カスタム/許可されたアプリポリシーの作成または編集時にオンにすることができます。カスタムポリシーまたは許可されたアプリのポリシーコンプライアンス通知テンプレートを有効化する方法については、「カスタムポリシーの追加」ページ994と「許可されたアプリポリシーの作成」ページ1027をそれぞれ参照してください。

- **機能の使用：**
    - ポリシー通知テンプレートを有効化した状態で、デバイスがカスタム/許可されたアプリポリシーのコンプライアンス違反になった場合、Ivanti Neurons for MDM は、ポリシー通知テンプレートにメールをラップした上で、デバイス所有者にメールを送信します。この機能を使用するのは Ivanti Neurons for MDM ですが、ユーザーが上記のように機能を設定してください。

オンデマンド機能

Ivanti Neurons for MDM にはいくつかのオンデマンド機能があり、デフォルトでは無効化されています。これらの機能はパフォーマンスに多少の影響を与える可能性があり、まだ本番環境での展開準備が万全とは言えません。

デフォルトでは無効になっているオンデマンド機能を、テナントデバイス上で1つ以上有効化してみたいとお考えの管理者は、サポートまでお問い合わせください。

以下の表は、文書化されているオンデマンド機能のリストです。

機能	説明	プラットフォーム	ライセンス
Windows 10機能	Windows 10デバイスを対象とする機能です。	Windows 10	• 旧：Gold • 新：Secure EUM 過去と現在の製品については「パッケージ」ページ1321をご覧ください。
アプリカタログのURLをクリップボードにコピー	管理者がアプリカタログのURLをアプリ用クリップボードにコピーできます。このURLはメールでユーザーに配布可能です。ユーザーが登録デバイスからリンクをクリックすると、アプリのあるアプリカタログがブラウザで開き、ユーザーはそこからアプリのインストールを選択できます。 このURLを意図したユーザーに限って配布することは、管理者の責任です。	• iOS • macOS	不適用（テナント固有）
アプリとしてのWebクリップ設定	ユーザー向けのアプリカタログでWebアプリケーションを提供するには、Webクリップをアプリカタログ内のアプリとして設定します。Webクリップは構成として定義できますが、構成は管理者しかプッシュできません。ユーザーはWebアプリケーションを自分のデバイスにインストールするか、オプトアウトするかを選択できますが、Webクリップ構成をオプトアウトすることはできません。	iOS	不適用（テナント固有）

機能	説明	プラットフォーム	ライセンス
許可リストにあるデバイスの登録	[ユーザ] > [ユーザ設定] > [デフォルトデバイス登録設定] で、許可リストのシリアル番号に基づくデバイス登録を許可します。	• iOS • macOS	不適用(テナント固有)
証明書ベースの認証	証明書ベースの認証機能では、管理者がデジタル証明書とテナント指定のホスト名またはバニティホスト名でログインする機能です。この認証設定は **[管理]** タブの [バニティホスト構成] を使用して構成できます。	この機能はプラットフォームに依存しません。	不適用(テナント固有) この機能はNA3クラスター環境でのみ、なおかつサポートが有効化した場合のみ使用可能です。
専用デバイス構成(会社所有シングルユース: COSU) の作成	管理者は、Android Enterpriseの専用デバイス(会社所有シングルユース: COSU) 構成を使用して、特定の目的に使用する専用デバイスを構成できます。COSU構成は仕事用マネージドデバイス(デバイス所有者モード) に配布され、キオスクモードでユーザがアプリを1つだけ使用できるようにします。	Android Enterprise	Silver
ダッシュボードのアイドル時間	既定では、ダッシュボードの非アクティブ時間は 15 日に設定されています。テナントのニーズに応じて更新できます。最大値は 30 日です。非アクティブ時間を長くする必要がある場合は、サポート チームまでお問い合わせください。	この機能はプラットフォームに依存しません。	

Android Enterprise デバイス サポートの準 備

このセクションでは、Android Enterprise デバイスの最 低 ネットワーク要 件 について説 明します。Androidデバイスは通 常 、ファイアウォールのインバウンドポートを開 かなくても正 しく機 能します。しかし、管 理 者 がAndroidエンタープライズデバイス用 のネットワーク環 境 を設 定 する際 に注 意 する必 要 のあるアウトバウンド接 続 は数 多 くあります。

以 下 の表 に挙 げたネットワーク変 更 はすべてではなく、変 更 される場 合 があります。ここには、エンタープライズマネジメントAPIおよびGMSアプリの現 在 と過 去 のバージョンに対 応 する既 知 のエンドポイントが含 まれます。

次 の表 の一 覧 にあるポートのほかに、Android Enterprise デバイスは Ivanti Neurons for MDM へのアクセスが必 要 です。

次 の表 は、Android Enterprise デバイスの要 件 の一 覧 です。

宛先ホスト	ポート	目的
play.google.com android.com google-analytics.com googleusercontent.com gstatic.com *.gvt1.com *ggpht.com dl.google.com android.clients.google.com	TCP/443 TCP, UDP/5528-5230	Google Playと更新(APK、アプリロゴなど) gstatic.com、googleusercontent.com - ユーザー生成コンテンツ(ストア内のアプリアイコンなど)を含む *.gvt.com, *.ggpht, dl.google.com、android.clients.google.com - アプリと更新、PlayStore APIをダウンロード
*googleapis.com	TCP/443	UEM/Google APi/PlayStore API
accounts.google.com	TCP/443	認証
fcm.googleapis.com fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging(たとえば「[デバイス]を探す」、構成のプッシュなどのUEMコンソール <-> DPC通信)
pki.google.com clients1.google.com	TCP/443	証明書失効
clients[2...6]. google.com	TCP/443	クラッシュレポート、Chrome Bookmark Sync、時刻同期(tlsdate)など、多様なGoogleバックエンドサービスが共有するドメイン

Googleは特定のIPを提供しません。したがって、以下のGoogleのASN 15169(http://bgp.he.net/AS15169#_prefixes) に挙げてあるIPブロックに含まれるすべてのIPアドレスへの外向きの接続をファイアウォールに許容させる必要があります。

Googleのピアやエッジノード のIPはAS15169ブロックに入っていません。Googleのエッジネットワークについては、https://peering.google.com/をご覧ください。

ダッシュボード

ダッシュボードは、登録されたデバイスおよびユーザーに関する重要な統計を示します。ダッシュボード上の各セクションをウィジェットと呼びます。各ウィジェットについて、以下の項目を定義します。

- 表示されるデータのカテゴリ(デバイスやユーザーなど)
- データのグループ分けの方法(OSビルドバージョンやモデル別、など)
- データのフィルタリングの方法(iOSデバイスのみを表示、OSビルドバージョンを表示など)
- データの表示方法(円グラフ、棒グラフなど)

このセクションは以下のトピックを含みます。

- 「ウィジェットの操作」ページ37
- 「アプリ情報」ページ50
- 「スケジュール済みのレポートの使用」ページ56
- 「カスタムレポートの使用」ページ67

ウィジェットの操作

このセクションは以下のトピックを含みます。

ダッシュボードは、登録されたデバイスおよびユーザーに関する重要な統計を示します。ダッシュボード上の各セクションをウィジェットと呼びます。各ウィジェットについて、以下の項目を定義します。

- 表示されるデータのカテゴリ(デバイスやユーザーなど)
- データのグループ分けの方法(OSバージョンやモデル別、など)
- データのフィルタリングの方法(iOSデバイスのみを表示するなど)
- データの表示方法(円グラフ、棒グラフなど)

ウィジェットの追加

1. **[追加]**(右上)をクリックします。
2. ウィジェットに名前を割り当てます。
3. データカテゴリを選択します。
4. 表示のフィルタリングオプションを入力します。
5. デフォルトの表示の種類を選択します(円グラフ、棒グラフ、線グラフ)。
6. **[完了]**をクリックします。

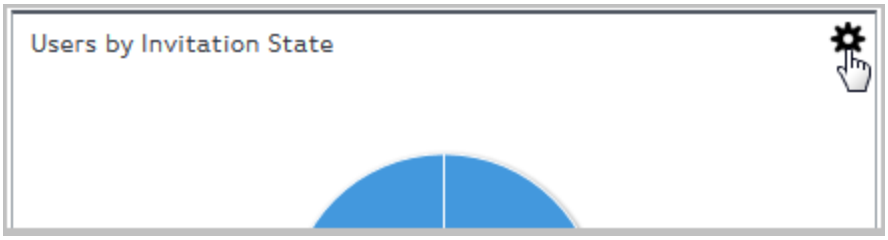
ウィジェットの配置

ウィジェットは常に1行に3つ表示されます。ただし、ウィジェットの表示順は変更することができます。

1. [配置](右上)をクリックします。
2. ウィジェットを表示させたい順でボックスをドラッグします。
3. **[OK]** をクリックします。

ウィジェットの編集

1. ウィジェットの[設定]アイコン(右上)をクリックします。



2. **[編集]** を選択します。
3. 変更を加えます。
4. **[完了]** をクリックします。

通知の確認

ベルのアイコン(右上)をクリックするか、**[ダッシュボード]** > **[通知]** ページを開くと、通知を確認し、必要であれば以下の基準に応じて対処することができます。

- コンポーネントの種類
  - アプリ
  - LDAP
  - AAD
  - デバイス許可リスト

- 「Appとブック」
- iOS
- [Android]
- テナント
- CA
- コネクタ
- Device Enrollmentサーバートークン

- 通知の種類
  - 有効期限
  - データ同期
  - 使用制限
  - 管理者アクション
  - サーバー認証エラー
  - 検証エラー
  - ステータスの変更
- Severity (重大度)
  - クリア
  - 情報
  - 重要
  - 警告

管理者は、APPコンポーネントを選択し、特定アプリの通知すべてを [通知] ページで簡単に確認できます。これはベルの通知セクションでも可能です。Google Playアプリに対して新しい許可を承認する必要がある場合、管理者が通知をクリックして承認すれば、各アプリのページを開く必要がありません。

Ivanti Neurons for MDM のお客様/テナントは、Android Go アプリがアプリカタログにインポートされていない場合でも、Android Go 承認通知を受信します。

ユーザーパスワード有効期限/ID変更通知の確認

管理者は、**[通知]** ページで近い将来のパスワード有効期限を確認することができます。また、パスワード有効期限の2週間と1日前には、対応ユーザーのリストを含むCSVレポートファイルへのリンクとともに通知も受けます。パスワードの期限が切れた後は、通知が生成されません。

管理者は、最後のLDAP同期中にID(UID)の変更が検出されたユーザーをリストアップした通知も確認できます。

通知のクリア

通知は、必要に応じて **[通知]** ページから手動でクリアできます。

1. **[通知]**ページの **[アクション]** カラムでクリアしたい通知をクリックします。**[通知のクリアを確認]** ウィンドウが表示されます。
2. **[通知をクリア]** をクリックします。クリアすると、**[ステータス]** カラムの通知ステータスが **[クリア済み]**に変わります。

> クリアされた通知の総数が **[通知]** ページに表示されます。

レポート

[ダッシュボード] > **[レポート]** ページでは、統合エンド管理(UEM)システムのデータにアクセスできます。たとえば管理者は、デバイスやブロックするデバイスのレポートを作成する際、フィルターオプションを使用してデバイススペース名やカスタムデバイス属性などの情報をレポートに追加できます。その場合、レポートにはデバイススペース名のカラムとデバイスカスタム属性のカラムが追加されます。カスタムデバイス属性は、レポート作成の際、フィルタリングオプションから使用します。管理者は、デバイスに使用するカスタムデバイス属性キーをリストから選び、使用可能な演算子を選択してください。

Ivanti Neurons for MDM 76以降、すべてのレポートテンプレートの演算子には標準演算子があります。以下のテンプレートの演算子は本リリースで標準化されています。

- [ダッシュボード] > [レポート] > [レポートを作成]

以下はレポートのワークフローです。

1. 選択 - 定義済みのレポートテンプレートを選択します。
2. 範囲を定義 - データをレポート化する期間を定めます。
3. 詳細を設定 - レポートに名前を付け、カスタマイズします。

4. 実行またはスケジュール - 即座にレポートを生成するか、スケジュールを作成します。
5. 共有 - レポートの受信者を指定します。

関連トピック:

- [ダッシュボード] > [レポート(スケジュール済み)]
- [ダッシュボード] > [レポート(カスタム)]

クイック検索: [レポート] タブに移動します。クイック検索フィールドでは、以下の列で検索が可能です。検索文字列にスペースや特殊文字を含めてもかまいません。

- 名前
- 説明
- テンプレート名

監査証跡

監査証跡は、Ivanti Neurons for MDM 内のすべてのエンティティに対して実行された活動を捉えた時系列の記録です。管理者、エンドユーザー、システム自体の各種コンポーネントなど、すべての行為者によるものを含みます。Ivanti Neurons for MDM リリース80以降、すべてのテナントについてデフォルトで監査証跡が有効化されています。テナントは [デバイスチェックイン監査証跡] をオプトインまたはオプトアウトできます。リリース80前に監査証跡を有効化していたテナントでは、引き続きチェックインが有効化されます。他のすべてのテナントのデバイスではチェックイン証跡が無効化されます。Android デバイスを再登録すると、[監査証跡] ページに、現在登録されているデバイスステータスが [再登録デバイスアクション実行済み] と表示され、前のエントリが [デバイスの撤去アクション実行済み] と表示されます。詳細については、「デバイス登録(iOS、macOS、Android)」 ページ204

追跡される操作は以下のとおりです。

- デバイスの追加、撤去、ワイプ、削除、更新
- デバイスでのチェックイン強制
- デバイス所有者の変更
- ユーザー設定(デバイス登録、デバイス制限、利用規約の設定)の作成、削除、更新
- デバイスのロック/ロック解除
- 構成の作成、編集、削除、優先度決定

- ポリシーの作成、編集、削除
- 構成の配布グループにおける変更
- ユーザーの作成、編集、削除(LDAPユーザーの作成は含まない)
- ユーザーグループの作成、編集、削除
- 配布フィルターの作成、編集、削除
- LDAPサーバーの作成、編集、削除
- LDAPサーバーと同期する状況:
  - LDAP同期開始
  - LDAP同期成功
  - LDAP同期放棄(ユーザー削除数が構成の閾値を超えた場合に生じます)
  - LDAP同期部分放棄(同期中に不良エントリがあった場合に生じます)
  - LDAPサーバーが追加されました
  - LDAPサーバーが編集されました
  - LDAPサーバーが削除されました
  - LDAPサーバー同期が開始しました
  - LDAPサーバー同期に失敗しました
  - LDAPサーバー同期が完了しました
- アプリの作成、編集、削除
- アプリ構成の作成、編集、削除
- スクリプトの作成、編集、削除
- 管理LDAPエンティティの削除
- LDAP設定の変更
- LDAP証明書のアップロード

- アプリケーション アイコンが変 更 されます。

監 査 証 跡 の有 効 化

Ivanti Neurons for MDM 内 で実 行 される動 作 をキャプチャするには、監 査 証 跡 機 能 をオンにする必 要 があります。

1. **[管 理] > [インフラストラクチャ] > [監 査 証 跡]** を選 択 します。**[監 査 証 跡]** ページが表 示 されます。
2. **[監 査 証 跡 を有 効 化]** をクリックします。**[監 査 証 跡 を有 効 化 しますか?]** ウィンドウが表 示 され、ユーザーに有 効 化 の確 定 を求 めます。
3. **[監 査 証 跡 を有 効 化 しますか?]** ウィンドウで **[監 査 証 跡 を有 効 化]** をクリックします。

   監 査 証 跡 機 能 は有 効 化 すると無 効 化 できません。無 効 化 する場 合 はサポートにお問 い合 わせください。

4. **[監 査 証 跡 をエクスポート]** フィールドでトグルバーを **[ON]** にスライドし、監 査 証 跡 のエクスポートを構 成 します。監 査 証 跡 のエクスポートでは、すべての監 査 証 跡 情 報 を特 定 のサーバーロケーションにエクスポートおよびアップロードします。監 査 証 跡 のエクスポートはSSH File Transfer Protocol(SFTP) を通 じて実 行 されます。サーバーはデフォルトポートからアクセスできる必 要 があります。ユーザーは監 査 証 跡 エクスポート設 定 から、監 査 証 跡 のアーカイブを特 定 のロケーションに毎 日 自 動 的 にアップロードするよう設 定 可 能 です。詳 細 については監 査 証 跡 のエクスポートを参 照 してください。

監 査 証 跡 活 動 の閲 覧

[ダッシュボード] の **[監 査 証 跡]** ページで追 跡 した活 動 を閲 覧 できます。行 (ロウ) の項 目 がデフォルトの列 幅 を超 え、列 (カラム) の境 界 線 によって隠 れている場 合 、省 略 記 号 が表 示 され、省 略 記 号 の上 にマウスを置 くとツールチップとして行 項 目 が完 全 に表 示 されます。

この表 示 では以 下 の情 報 が表 示 されます。

カラム名	説明
名前	デバイスの名前またはユーザー設定の名前を表示します。たとえば、デバイス活動についてはデバイス名を表示します。ハイパーリンクをクリックすると活動詳細ページが開きます。 デバイスに関連付けられたユーザーがいる場合、デバイス所有者のユーザー名もデバイス名の下に表示されます。 デバイス詳細ページを見るには、デバイス名の横にある **[デバイスを開く]** リンクをクリックします。デバイス詳細ページの **[監査証跡を開く]** ハイパーリンクをクリックすると、監査証跡の活動の詳細が表示されます。
種類	トリガーされる活動の種類。 ログイン活動の「アカウント」など。
カテゴリ	活動のカテゴリ。 構成、ポリシーなど。
最後の活動	最後に実行された活動。 作成、削除など。
最後のユーザー	活動を実行したユーザー。
実行時:	活動の実行日時は24時間形式でのみ表示されます。

活動詳細表示

活動詳細表示(内側の層)には、エンティティ表示の **[名前]** 列の下にあるリンクをクリックしてアクセスします。ここには、そのエンティティの過去の活動証跡すべてが列記されます。この表示では以下の情報が表示されます。行(ロウ)の項目がデフォルトの列幅を超え、列(カラム)の境界線によって隠れている場合、省略記号が表示され、省略記号の上にマウスを置くとツールチップとして行項目が完全に表示されます。

カラム名	説明
アクションの時刻	アクションが実行されてからの時間。
活動	実行された具体的なアクションの説明。 アプリカタログへのアプリ追加など。
実行者：	活動を実行したユーザー。
変更 - 変更前と変更後	アイコンをクリックすると、**[監査証跡の変更 - 変更前と変更後]** ウィンドウに監査証跡比較の詳細が表示されます。

[監査証跡変更 - 変更前と変更後] ウィンドウには以下の情報が表示されます。

カラム名	説明
属性	変更された属性の名前を表示します。 **createdAt**など。
前	アクションが実行される前の属性値。
後	アクションが実行された後の属性値。

カラムヘッダーの右上にある **[カラムをカスタマイズ]** 設定アイコンでは、該当のカラム名のチェックボックスを選択または選択解除し、リストビューでカラムを表示/非表示にできます。

監査証跡活動のフィルタリング

[フィルタ] オプションでは、監査証跡活動を絞り込み、リストとして表示できます。以下は、利用可能なフィルタリングオプションです。

フィルタリングオプション	説明
日付範囲でフィルタリング	開始日と終了日のフィールドで日付範囲を選択します。範囲を選択すると、選択した日付範囲に実行された監査証跡活動のリストが表示されます。このフィルタリングオプションはいずれの表示オプション(グループ化または拡張)でも使用できます。 終了日を現在の日付として選択できる日付範囲は最大で15日間です。
カテゴリ (拡張表示にのみ適用)	次の選択肢からカテゴリを選択します。 • **ポリシー** • **デバイス管理** • **ユーザー管理** • **ユーザー設定管理** • **LDAP** • **構成** • **管理ポータルアクセス** • **アプリケーション管理** • **Azureデバイスコンプライアンス** 拡張表示でカテゴリーのカラムはデフォルトで非表示です。

フィルタリングオプション	説明
種類 (拡張表示にのみ適用)	以下の **[エンティティの種類]** オプションを選択します。 • **アカウント** • **デバイス** • **登録認証** • **デバイスの上限** • **利用規約** • **コンプライアンス レポート** 拡張表示で種類のカラムはデフォルトで非表示です。
活動 (拡張表示にのみ適用)	表示させたい具体的な活動を選択します。選択肢は以下のとおりです。 • **削除** • **更新配布** • **強制チェックイン** • **構成エラーをクリア** • **撤去** • **ログイン** • **更新** • **所有者を更新** • **ワイプ** • **ロック** • **Intune コンプライアンスの更新**

フィルタリングオプション	説明
[名前] (拡張表示にのみ適用)	デバイスの名前またはユーザー設定の名前で絞り込みます。
実行者:	活動を実行したユーザーで絞り込み。
ステータス	ログインステータスで絞り込みます。以下が選択肢です。 • **成功** • **失敗**

表示の順序は活動が実行された日時によって決まります。

カラムヘッダーの右上にある **[カラムをカスタマイズ]** 設定アイコンを使用すると、チェックボックスを選択または選択解除し、リストビューで該当のカラム名を表示/非表示にできます。

デフォルトではページ内に50件の活動がリストアップされます。活動が50件より多い場合は、ページ下の **[次へ]** ボタンをクリックし、さらに活動を表示させます。ページ下部の **[表示]** フィールドで該当の表示オプションをクリックすることも可能です。たとえば、**[100]** をクリックすると最近の100件が表示されます。

監査証跡活動の検索

検索フィールドでは、入力したキーワードに基づいて監査証跡活動を検索および表示できます。現在、クイック検索を実行すると、プロパティ名を含め文字列全体がインデックスされます。Ivanti Neurons for MDM 76以降はプロパティ値のみインデックスされます。ユーザーは、クイック検索を実行する際、詳細カラムにある詳細キーを提供する必要がありません。入力したキーワードは以下のいずれのカラムにも適用可能です。

- **名前**(デバイス名またはユーザー名)
- **種類**
- **カテゴリ**
- **実行者:**
- **詳細**

活動カラムの値は検索できません。

表示される結果は、入力したキーワードがカラムの値に含まれる監査証跡の活動も含みます。たとえば、検索フィールドに入力したキーワードが [nny] の場合、[名前] カラムに [Johnnydoe] の値が入っている監査証跡の活動が表示されます。

監査証跡のCSVファイルへのエクスポート

[監査証跡] ページの [CSVにエクスポート] オプションを使用して、監査証跡レコードをエクスポートできます。

手順

1. **[ダッシュボード]** > **[監査証跡]** を開きます。
2. **[アクション]** ドロップダウンメニューをクリックし、**[CSVにエクスポート]** オプションを選択します。または、日付範囲でフィルタリングしてから、[CSVにエクスポート] オプションを選択できます。
   エクスポート レポートの処理にしばらく時間がかかる旨のポップアップ メッセージが表示されます。この要求が完了するまで待ってから、別の要求を送信してください。
3. **[ダウンロード]** をクリックします。レポートをダウンロードするためのリンクが記載されたメールが送信されます。
4. (任意) レポートを削除するには **[削除]** をクリックします。

[ダッシュボード] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

アプリ情報

このセクションは以下のトピックを含みます。

アプリ情報はダッシュボード内にあり、以下のアプリ配布を閲覧および分析するための機能です。

- インストールを必要とする社内アプリ配布
- インストールを必要とするパブリックアプリ配布
- 非マネージドiOSアプリ
- インストールされたマネージドアプリの上位10件
- 最も評価の高い自社開発アプリ上位5件

インストールを必要とするアプリ上位5つの分析：これらは、多数のユーザーに配布された社内またはパブリックアプリの中で、比較的インストール率が低いアプリです。非マネージドiOSアプリグラフは、デバイス上の非マネージドアプリに関する情報を提供します。ここで、非マネージドアプリのリストとそれらがインストールされているデバイスを表示し、アプリをマネージドアプリに変換することができます。これらは、配布を改善するために管理者の注意や操作を必要とする配布アプリです。これらのグラフは、すでにアプリをインストールしているデバイスを示しています。円グラフは、パブリックアプリと社内アプリの大まかな配布状況を示し、アプリのインストールを必要とするデバイス数の分析を助けるだけでなく、グラフの特定の領域をクリックすれば、そのアプリの詳細情報を見ることも可能です。また、1つのアプリの特定バージョンの配布状況を示すシングル配布グラフを追加することもできます。

ダッシュボードには、過去15日間にチェックされたデバイスの情報のみが表示されます。

アプリ配布の表示

[ダッシュボード] の下の **[アプリ]** ページには、以下のグラフがあります。

- インストールを必要とする社内アプリ配布
- インストールを必要とするパブリックアプリ配布
- 非マネージドiOSアプリ

デフォルトでは自社開発アプリ5つ、市販アプリ5つ、非マネージドiOSアプリのグラフが表示されます。グラフは左から非インストール率が高い順に並んでいます。

円グラフは2色でインストール状態を示します。青はアプリがインストールされたデバイス数を示します。赤はインストールが必要なデバイス数を示します。各色の領域の上にマウスを置くとデバイス数が表示されます。

グラフの右上の削除オプションをクリックするとグラフを削除できます。

アプリ詳細の表示

円グラフの中心にはインストールの必要なデバイス数も表示されます。たとえば「750/1000」とはデバイス1,000台のうち750台にインストールが必要であることを示します。

円グラフは3色でアプリの配布状況を示します。

- 青はアプリがインストールされたデバイス数を示します。グラフの青い領域をクリックすると **[デバイス]** ページが開きます。**[デバイス]** ページの **[アプリバージョン]** 列にはインストールしたアプリのバージョンとインストールした日付が表示されます。

  > 左パネルの **[バージョン]** セクションでオプションを選択すると、インストールされたアプリバージョンごとにデバイスを確認できます。

- 赤はアプリのインストールが必要なデバイス数を示します。グラフの赤い領域をクリックすると **[デバイス]** ページが開きます。**[デバイス]** ページではアプリのインストールが必要なデバイスを確認できます。

グラフの中央にはアプリのアイコンがあります。アイコンをクリックすると、**[アプリ]** > **[アプリカタログ]** のアプリ詳細ページが開きます。

このページで **[アプリをインストールしたデバイス]** タブをクリックすると、選択したアプリをインストールしたデバイスのリストが表示されます。

[アプリをインストールしていないデバイス] をクリックすると、選択したアプリをインストールしていないデバイスのリストが表示されます。

シングルアプリ配布グラフの追加

アプリページにあるアプリの特定のバージョンについてシングル配布円グラフを追加できます。赤はアプリをインストールすべきデバイスのリストを示します。これらのグラフはアプリの配布に関する以下の情報を視覚的に表示します。

- アプリの特定のバージョンをインストールしたデバイス
- アプリの他のバージョンをインストールしたデバイス
- アプリをインストールしていないデバイス

手順

1. **[アプリ]** ページの **[+追加]** をクリックします。**[アプリグラフを追加]** ウィンドウが表示されます。
2. **[グラフの種類]** ドロップダウンリストから **[シングルアプリ配布]** を選択します。
3. シングルアプリ配布グラフを見たいアプリリストのチェックボックスを選択します。

   [アプリを検索] フィールドにアプリ名を入力しても特定のアプリを検索できます。

4. **[グラフを追加]** をクリックします。シングルアプリ配布グラフがアプリページに表示されます。

   アプリはリストから9個まで選択できます。

グラフの中心には特定のアプリバージョンをインストールしたデバイス数が表示されます。

たとえば「5/10」とはデバイス10台のうち5台に特定のアプリバージョンがインストールされていることを示します。

円グラフは3色でアプリの配布状況を示します。

- 緑はアプリの特定バージョンがインストールされたデバイス数を示します。グラフの緑の領域をクリックすると **[デバイス]** ページが開きます。ここには、アプリの特定バージョンをインストールしたデバイスのリストが表示されます。左パネルの **[アプリバージョン]** セクションでオプションを選択すると、インストールされたアプリバージョンごとにデバイスを確認できます。
- 薄い緑はアプリの他のバージョンがインストールされたデバイス数を示します。グラフの薄い緑の領域をクリックすると **[デバイス]** ページが開きます。ここには、アプリの他のバージョンをインストールしたデバイスのリストが表示されます。左パネルの **[アプリバージョン]** セクションでバージョンオプションを選択すると、インストールされたアプリバージョンごとにデバイスを確認できます。

- 赤はアプリがインストールされていないデバイス数を示します。各色の領域の上にマウスを置くとデバイス数が表示されます。グラフの赤い領域をクリックすると**[デバイス]**ページが開きます。ここには、アプリをインストールしていないデバイスのリストが表示されます。左パネルにはアプリカタログからアプリが入手可能になる日付も表示されます。

グラフの中央にはアプリのアイコンがあります。アイコンをクリックすると、**[アプリ] > [アプリカタログ]**のアプリ詳細ページが開きます。このページで**[アプリをインストールしたデバイス]**タブをクリックすると、選択したアプリをインストールしたデバイスのリストが表示されます。**[アプリをインストールしていないデバイス]**をクリックすると、選択したアプリをインストールしていないデバイスのリストが表示されます。

グラフの右上の削除オプションをクリックするとグラフを削除できます。

非マネージドiOSアプリグラフの追加

非マネージドiOSアプリグラフをアプリページに追加すると、非マネージドアプリのリストを特定し、表示することができます。このグラフは、管理者が非マネージドiOSアプリをカタログに追加すると、自動的に表示されます。管理者は必要に応じてこのグラフを削除または追加できます。

手順

1. **[アプリ]**ページの**[+追加]**をクリックします。**[アプリグラフを追加]**ウィンドウが表示されます。
2. **[グラフの種類]**ドロップダウンリストから**[非マネージドiOSアプリ]**を選択します。
3. **[グラフを追加]**をクリックします。非マネージドiOSアプリのグラフが**[アプリ]**ページに表示されます。

このグラフは、アプリカタログ内にある非マネージドのアプリ数を表示します。グラフの一番下には、以下の詳細を記載した3つのカラムがあります。

- **非マネージドiOSアプリを持つデバイス** - 非マネージドiOSアプリの数を示します。リンクをクリックすると、[非マネージドiOSアプリを持つデバイス] ウィンドウに非マネージドアプリのあるデバイスのリストが表示されます。
- **アプリカタログ内の総アプリ数** - アプリカタログで提供されているアプリの総数を表示します。
- **非マネージドiOSアプリ(%)** - 非マネージドiOSアプリの割合を示します。

アプリがすでにiTune App Storeからインストールされている場合は、このアプリとデータをマネージドアプリに変換できます。そのようなアプリからマネージドアプリに変換するには:

1. **[非マネージドiOSアプリを持つデバイス]カラム**で数字のリンクをクリックします。**[非マネージドiOSアプリ]**ウィンドウが表示されます。

2. リストから1つ以上の非マネージドアプリを選択し、[非マネージドiOSアプリ] の下の数字リンクをクリックします。選択したアプリがマネージドアプリに変換され、次のチェックイン時にステータスが更新されます。

> **[CSVにエクスポート]** リンクをクリックすると、非マネージドアプリに関するデータをCSV形式でエクスポートできます。

インストールされたマネージドアプリ上位10件の追加

アプリページの「インストールされたマネージドアプリ上位10件」のグラフを使用すると、インストールされたマネージドアプリの上位10件を特定し、表示することができます。管理者は必要に応じてこのグラフを削除または追加できます。

「インストールされたマネージドアプリ上位10件」のグラフは、デフォルトで **[アプリ]** ページにあります。グラフが削除されている場合、管理者が **[アプリ]** ページから追加できます。

手順

1. **[アプリ]** ページの **[+追加]** をクリックします。**[アプリグラフを追加]** ウィンドウが表示されます。
2. **[グラフの種類]** ドロップダウンリストから **[インストールされたマネージドアプリ上位10件]** を選択します。
3. **[グラフを追加]** をクリックします。インストールされたマネージドアプリ上位10件のグラフが **[アプリ]** ページに表示されます。

インストールされたマネージドアプリ上位10件は、**[表示]** ドロップダウンリストで選択したカテゴリーに基づいて表示できます。選択可能なカテゴリー:

- **すべてのアプリ**(デフォルト選択)
- **自社開発アプリ**
- **市販アプリ**

グラフのそれぞれのバーが具体的なアプリを示し、アプリ名も表示されます。バーの上にカーソルを置くと、プラットフォーム(Android、iOS、Windows) とアプリをインストールしたデバイス数が表示されます。

特定のアプリのバーをクリックすると、**[デバイス]** ページが開き、アプリをインストールしたデバイスの詳細が表示されます。デバイスページの左パネルにはアプリをインストールしたデバイス数が表示されます。左パネルのXボタンをクリックすると、ダッシュボードの **[アプリ]** ページに戻ります。

グラフ右上の削除オプションをクリックするとグラフを削除できます。

最も評価の高い自社開発アプリ5件の追加

アプリページの「最も評価の高い自社開発アプリ5件」のグラフでは、最も評価の高い自社開発アプリ5件を特定し、表示することができます。管理者は必要に応じてこのグラフを削除または追加できます。

「最も評価の高い自社開発アプリ5件」のグラフは、デフォルトで **[アプリ]** ページにあります。グラフが削除されている場合、管理者が **[アプリ]** ページから追加できます。

手順

1. **[アプリ]** ページの **[+追加]** をクリックします。**[アプリグラフを追加]** ウィンドウが表示されます。
2. **[グラフの種類]** ドロップダウンリストから **[最も評価の高い自社開発アプリ5件]** を選択します。
3. **[グラフを追加]** をクリックします。最も評価の高い自社開発アプリ5件のグラフが **[アプリ]** ページに表示されます。

このグラフは、アプリのロゴ経由でデータと星の数による評価を表示します。星の数による評価は、星の絵と整数で表示されます(最高評価は5)。アプリを評価したユーザー数も表示されます。

アプリに対する評価の数は、その管理者が管理するデバイスに限らず、そのアプリの全ユーザーの評価を含みます。評価は、自分の登録デバイスのApps@Workからそのアプリを見た各ユーザーによるものであり、そのアプリに対するすべての評価の平均です。

特定のアプリをクリックすると、**[アプリの詳細]** ページが開き、アプリの詳細情報が表示されます。

グラフ右上の削除オプションをクリックするとグラフを削除できます。

スケジュール済みのレポートの使用

ライセンス: Silver

スケジュール済みのレポート機能では、すぐに使えるパッケージング済みのテンプレートを使用し、さまざまなメトリクスでレポートをスケジュールし、生成することができます。ユーザーがこの機能を使用するには、システム管理者またはシステム読み取り専用の役割が必要です。現在のところ、作成できるレポートの最大数は40です。

デバイスで複数のTunnelインスタンスが作成されている場合、ポリシー違反レポートで同じデバイスが複数のレコードを持つことがあります。これはスタンダードレポートでもカスタムレポートでも同様です。

レポートの生成

レポートのスケジュールと生成を行えます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[レポートを作成]** をクリックし、[レポートテンプレートを選択] ページを表示します。

3. 構成したオプションからレポートのテンプレートを選択します。

   - ブロックされたデバイス - Sentryによって現在アクセスがブロックされているデバイスに関するレポート。
   - **デバイス** - システム内のすべてのパーティション上のデバイスに関するレポート。
   - **ポリシー違反** - システム内のポリシー違反に関するレポート。
   - **ユーザー** - システム内のユーザーに関するレポート。
   - **ユーザーパスワード有効期限ステータス** - システム内のユーザーのパスワード有効期限のステータスに関するレポート。
   - **最も利用されているアプリ** - システム内のすべてのアプリケーションをインストール回数順に並べたレポート。
   - **非マネージドアプリ** - システム内の非マネージドアプリケーションに関するレポート。
   - **すべてのアプリケーション** - 自分が管理しているデバイス内のすべてのアプリケーションに関するレポート。

4. **[次へ]** をクリックします。

   [レポートの詳細] ページが表示されます。

   - **[レポート名]** を入力します。
   - (任意) レポートの **[説明]** を入力します。

   以下のオプションから **[イベント範囲]** を選択します。
   既存のレポートの場合：

   - **すべてのイベント**
   - **前日**
   - **前の週**
   - **前月**

- **以前の範囲** - 前のリリースのIvanti Neurons for MDM管理ポータルで範囲スライダーを使用して作成したレポートが表示されます。レポート用の上記オプションのいずれかを管理者が選択して保存すると、[以前の範囲] オプションは表示されなくなります。この範囲値は [レポートの要約] ページで確認できます。

新規レポートの場合：

- **すべてのイベント**
- **前日**
- **前の週**
- **前月**

5. **[次へ]** をクリックします。[レポートデータ] ページが表示されます。
6. **[レポートカラム]** セクションでカラムを追加、削除、順序変更するには、**[カラムをカスタマイズ]** をクリックします。または、カラム名をクリックして、追加したカラムを削除します。
7. (任意) リストに表示されているすべてのカラムを選択するには、**[すべてのカラムを選択]** チェックボックスを選択します。
8. 過去に生成したカラムに戻すには、**[デフォルト設定を回復]** をクリックします。カスタマイズなしのカラムに戻すには、**[レポートテンプレートを選択]** ページからいずれかのテンプレートを選択します。
9. **[高度なフィルター]** セクションで、特定のルールに基づいてフィルターを作成します。

> すべてのレポートですべてのフィルターオプションを利用できるわけではありません。利用可能なフィルターのリストについての詳細は、この手順の下にある「フィルター」 ページ60トピックを参照してください。

> レポートを作成するときには、Windows デバイスで次の新しいハードウェア属性を使用できます。BitLocker暗号化、OSエディション、システムバージョン、マザーボードのメーカー、マザーボードの製品名、マザーボードのステータス、BIOSのメーカー、BIOS バージョン、ハードドライブのパーティション、光学ドライブタイプ、CPU 名、CPU ステータス。

10. (任意) 別のルールを追加するには **[+]** アイコンをクリックし、別のルールグループを追加するには **[グループを追加]** アイコンをクリックします。

11. **[次へ]** をクリックします。[レポートスケジュール] ページが表示されます。

12. レポートをダウンロードする際は、次のいずれかの形式を選択します。

    - CSV
    - PDF
    - **CSVとPDF**

      PDFレポートファイルの場合、カラムは10本までです。[レポートチャート] セクションには、PDFレポートに含まれることになる2種類のチャートが表示されます。

      [すべてのアプリケーション] レポートはCSV形式のみサポートします。

13. 繰り返しを設定することにより自動的に実行されるレポートを設定するには、**[自動スケジュール]** をクリックします。または、**[手動]** をクリックしてレポートを1回実行すると、このレポートはメールで送信されます。

    - 次の **[反復レポート]** オプションのいずれかを選択します。
      - **毎日**
      - **毎週**
      - **月単位**
      - **前のスケジュール** - 既存のレポートの場合
    - **[開始日]** と **[終了日]** を選択します(任意)。

14. **[次へ]** をクリックします。[レポート配布] ページが表示されます。レポートの受信者を選択します。

15. (任意) **[外部メールアドレスを追加]** リンクをクリックして、外部メールIDを追加します。

16. **[完了]** をクリックします。**[レポート配布]** の **[要約]** が表示されます。

17. (任意) **[編集]** をクリックしてレポートを部分的に変更します。

18. **[保存]** をクリックします。

19. ダウンロードアイコンをクリックして、レポートの形式を選択します。レポートをダウンロードするための **[レポートをダウンロード]** ボタンが含まれているメールが、レポートの受信者に送信されます。

フィルター

ルールオプション	説明
アクティベーションロック有効	アクティベーションロック有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「アクティベーションロック有効は次と等しい：はい」。
App Tunnelステータス	**[ブロック]** または **[許可]** のApp Tunnelステータスのルール。 ルールの例：「App Tunnelステータス次と等しい：ブロック」。
バッテリー残量	デバイスのバッテリー残量を示す値。 ルールの例：「バッテリー残量は次と等しい：1080」 バッテリー残量の値は秒数で入力してください。
クライアントの前回のチェックイン	クライアントの最終チェックインの日付範囲に基づくルール。 ルールの例：「クライアントの前回のチェックインが次の範囲内：04/02/2019 06:00:00,04/05/2019 17:00:00」
コンプライアンスステータス	**[はい]** または **[いいえ]** の準拠状態に基づくルール。 ルールの例：「コンプライアンスステータスは次と等しい：はい」。
現在の国名	現在の国名を入力します。 ルールの例：「コンプライアンスステータスは次と等しい：フランス」
現在のMCC	現在のモバイル国コードに基づくルール。

ルールオプション	説明
	ルールの例：「現在のMCCは次と等しい：410」
現在のMNC	現在のモバイルネットワークコードに基づくルール。 ルールの例：「現在のMNCは次と等しい：06」
Device Enrollment有効	Device Enrollment有効を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「Device Enrollment有効は次と等しい：はい」
Device Enrollmentに登録済み	Device Enrollmentに登録済みを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「Device Enrollmentに登録済みは次と等しい：はい」
データ保護	デバイス上でデータ保護が有効化されているかどうかを示します。**[はい]** か **[いいえ]** のいずれかの値となります。 ルールの例：「データローミング保護は次と等しい：はい」
データローミング有効	データローミング有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「データローミング有効は次と等しい：はい」
デバイスブロックステータス	デバイスブロックのステータスに基づくルール。 ルールの例：「デバイスブロックステータスは次と等しい：ブロック」
デバイスID	具体的なデバイスIDまたはデバイスID範囲に関するルール。

ルールオプション	説明
	ルールの例：「デバイスIDは次より大きい：45」。x
ホームMCC	ホームのモバイル国コードに基づくルール。 ルールの例：「ホームMCCは次と等しい：310」
ホームMNC	ホームのモバイルネットワークコードに基づくルール。 ルールの例：「ホームMNCは次と等しい：510」
IMEI	具体的なIMEI値に関するルール。 ルールの例：「IMEIは次から始まる：9900」。
招待ステータス	以下のいずれかの招待ステータスオプションを選択してください。 • **なし** • **保留中** • **有効期限切れ** • **完了** ルールの例：「招待ステータスは次と等しい：保留中」。

ルールオプション	説明
ロケーターサービス有効	位置情報サービス有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「位置情報サービス有効は次と等しい：はい」
隔離ステータス	位置情報サービス有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「隔離ステータスは次と等しい：はい」
登録：	デバイスが登録された日時の範囲を選択するルール。 ルールの例：「登録が次の範囲内：10/03/2017 09:00:00, 10/20/2017 17:00:00」。
ローミング	ローミングを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「ローミングは『はい』」
ステータス	以下のいずれかの招待ステータスオプションを選択してください。 • **アクティブ** • **撤去保留中** • **撤去を送信しました** • **リタイヤ済み** • **撤去を取り消しました** • **ワイプ保留中** • **ワイプを送信しました** • **ワイプ済み**

ルールオプション	説明
	• **ワイプを取り消しました** ルールの例：「ステータスは次と等しい：撤去保留中」。
ボイスローミング有効	ボイスローミング有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「ボイスローミングは『はい』」
Wi-Fi MACアドレス	特定のMacアドレス値を入力します。 ルールの例：「Wi-Fi MACアドレスは次と等しくない：00-14-22-01-23-45」。
iCloudバックアップ有効	iCloudバックアップ有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「iCloudバックアップ有効は次と等しい：はい」
iTunes Storeアカウントアクティベーションステータス	iTunes Storeアカウントアクティベーションステータスを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「iTunes Storeアカウントアクティベーションステータスは次と等しくない：いいえ」。
プラットフォームの種類	[すべてのアプリケーション] レポートに適用されます。
ソース	[すべてのアプリケーション] レポートに適用されます。
カスタム属性	[すべてのアプリケーション] レポートに適用されます。

ルールオプション	説明
管理対象	[すべてのアプリケーション] レポートと[最も利用されているアプリケーション] レポートに適用されます。
アプリ識別子	[すべてのアプリケーション] レポートのデフォルトです。
MEID	[非マネージドアプリ] レポートに適用されます。

[スケジュール済みのレポート] ページからのレポートに対するアクションの実行

[スケジュール済みのレポート] ページで、さまざまなアクションを実行できます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[スケジュール済みのレポート]** ページで、**[アクション]** ドロップダウンメニューをクリックし、以下のいずれかのオプションを選択します。

アクションオプション	実行されるアクション
表示	レポートを表示できます。
編集	レポートを編集できます。このレポートでは、前回のリリースで選択されていた範囲も [以前の範囲] として確認できます。
今すぐ実行	レポートを実行します。
CSV のダウンロード	レポートをCSV形式でダウンロードします。
PDF のダウンロード	レポートをPDF形式でダウンロードします。
削除	レポートを削除します。

レポートの詳細の表示

レポートの詳細を表示し、作成したレポートに対してアクションを実行できます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[スケジュール済みのレポート]** ページで、詳細を表示するレポートの名前をクリックします。そのレポートのページが開きます。
3. このページで、[レポートの要約] と [レポート履歴] を確認できます。

詳細は[カスタムレポートの使用]を参照してください。

カスタムレポートの使用

ライセンス: Gold

カスタムレポート機能では、すぐに使えるテンプレートを使用し、さまざまなメトリクスでレポートのカスタマイズと生成が可能です。ユーザーがこの機能を使用するには、システム管理者またはシステム読み取り専用の役割が必要です。現在のところ、作成できるレポートの最大数は40です。

このセクションは以下のトピックを含みます。

「レポートの生成」下

「レポートに関するアクションの実行」ページ76

「レポートの詳細の表示」ページ76

レポートの生成

レポートのスケジュールと生成は、Ivanti Neurons for MDM管理ポータルで行えます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[レポートを作成]** をクリックし、[レポートテンプレートを選択] ページを表示します。

3. 構成したオプションからレポートのテンプレートを選択します。

   - **ブロックされたデバイス** - Sentryによって現在アクセスがブロックされているデバイスに関するレポート。
   - **デバイス** - システム内のすべてのパーティション上のデバイスに関するレポート。
   - **ポリシー違反** - システム内のポリシー違反に関するレポート。
   - **ユーザー** - システム内のユーザーに関するレポート。
   - **ユーザーパスワード有効期限ステータス** - システム内のユーザーのパスワード有効期限のステータスに関するレポート。
   - **最も利用されているアプリ** - システム内のすべてのアプリケーションをインストール回数順に並べたレポート。
   - **非マネージドアプリ** - システム内の非マネージドアプリケーションに関するレポート。
   - **すべてのアプリケーション** - 自分が管理しているデバイス内のすべてのアプリケーションに関するレポート。

4. **[次へ]** をクリックします。[レポートの詳細] ページが表示されます。
5. **[レポート名]** を入力します。
6. (任意) レポートの **[説明]** を入力します。
7. 以下のオプションから **[イベント範囲]** を選択します。
   既存のレポートの場合：

   - **すべてのイベント**
   - **前日**
   - **前の週**
   - **前月**
   - **以前の範囲** - 前のリリースのIvanti Neurons for MDM管理ポータルで範囲スライダーを使用して作成したレポートが表示されます。レポート用の上記オプションのいずれかを管理者が選択して保存すると、[以前の範囲] オプションは表示されなくなります。この範囲値は [レポートの要約] ページで確認できます。

   新規レポートの場合：

- **すべてのイベント**
- **前日**
- **前の週**
- **前月**

8. **[次へ]** をクリックします。[レポートデータ] ページが表示されます。
9. **[カスタマイズ]** をクリックし、カスタムレポートを生成します:

> **[ダッシュボード] > [レポート]** ページで、[テンプレート名] カラムに括弧で囲まれて「カスタム」と表示されている場合は、そのレポートがカスタマイズされていることを示します。

10. **[レポートカラム]** セクションでカラムを追加、削除、順序変更するには、**[カラムをカスタマイズ]** をクリックします。または、カラム名をクリックして、追加したカラムを削除します。
11. (任意) リストに表示されているすべてのカラムを選択するには、**[すべてのカラムを選択]** チェックボックスを選択します。
12. 過去に生成したカラムに戻すには、**[デフォルト設定を回復]** をクリックします。カスタマイズなしのカラムに戻すには、**[レポートテンプレートを選択]** ページからいずれかのテンプレートを選択します。デフォルトのカラムはロックアイコンで示されます。
13. **[高度なフィルター]** セクションで、特定のルールに基づいてフィルターを作成します。

> すべてのレポートですべてのフィルターオプションを利用できるわけではありません。利用可能なフィルターのリストについての詳細は、この手順の下にある「フィルター」 ページ71トピックを参照してください。

> レポートを作成するときには、Windows デバイスで次の新しいハードウェア属性を使用できます。BitLocker暗号化、OSエディション、システムバージョン、マザーボードのメーカー、マザーボードの製品名、マザーボードのステータス、BIOSのメーカー、BIOS バージョン、ハードドライブのパーティション、光学ドライブタイプ、CPU 名、CPU ステータス。

14. (任意) 別のルールを追加するには **[+]** アイコンをクリックし、別のルールグループを追加するには **[グループを追加]** アイコンをクリックします。
15. **[次へ]** をクリックします。[レポートスケジュール] ページが表示されます。

16. レポートをダウンロードする際は、次のいずれかの形式を選択します。

    - **CSV**
    - **PDF**
    - **CSVとPDF**

      PDFレポートファイルの場合、カラムは10本までです。[レポートチャート] セクションには、PDFレポートに含まれる2種類のチャートが表示されます。

      [すべてのアプリケーション] レポートはCSV形式のみサポートします。

17. 繰り返しを設定することにより自動的に実行されるレポートを設定するには、**[自動スケジュール]** をクリックします。または、**[手動]** をクリックしてレポートを1回実行すると、このレポートはメールで送信されます。

    - 次の **[反復レポート]** オプションのいずれかを選択します。
      - **毎日**
      - **毎週**
      - **月単位**
      - **前のスケジュール** - 既存のレポートの場合
    - **[開始日]** と **[終了日]** を選択します(任意)。

    [今すぐ実行] オプションを選んだ場合は1回のみレポートが生成されます。同じテンプレートでスケジュール済みのレポートも生成できます。このようなレポートでは **[ダッシュボード]** > **[レポート]** ページの [頻度] と [次のスケジュール] のカラムに [スケジュールなし] のステータスが表示されます。

18. **[次へ]** をクリックします。[レポート配布] ページが表示されます。レポートの受信者を選択します。
19. (任意) **[外部メールアドレスを追加]** リンクをクリックして、外部メールIDを追加します。
20. **[完了]** をクリックします。**[レポート配布]** の **[要約]** が表示されます。
21. (任意) **[編集]** をクリックしてレポートを部分的に変更します。
22. **[保存]** をクリックします。

23. ダウンロードアイコンをクリックして、レポートの形式を選択します。レポートをダウンロードするための **[レポートをダウンロード]** ボタンが含まれているメールが、レポートの受信者に送信されます。

フィルター

ルールオプション	説明
アクティベーションロック有効	アクティベーションロック有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「アクティベーションロック有効は次と等しい：はい」。
App Tunnelステータス	**[ブロック]** または **[許可]** のApp Tunnelステータスのルール。 ルールの例：「App Tunnelステータス次と等しい：ブロック」。
バッテリー残量	デバイスのバッテリー残量を示す値。 ルールの例：「バッテリー残量は次と等しい：1080」 バッテリー残量の値は秒数で入力してください。
クライアントの前回のチェックイン	クライアントの最終チェックインの日付範囲に基づくルール。 ルールの例：「クライアントの前回のチェックインが次の範囲内：04/02/2019 06:00:00,04/05/2019 17:00:00」
コンプライアンスステータス	**[はい]** または **[いいえ]** の準拠状態に基づくルール。 ルールの例：「コンプライアンスステータスは次と等しい：はい」。
現在の国名	現在の国名を入力します。 ルールの例：「コンプライアンスステータスは次と等しい：フランス」
現在のMCC	現在のモバイル国コードに基づくルール。

ルールオプション	説明
	ルールの例：「現在のMCCは次と等しい：410」
現在のMNC	現在のモバイルネットワークコードに基づくルール。 ルールの例：「現在のMNCは次と等しい：06」
Device Enrollment有効	Device Enrollment有効を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「Device Enrollment有効は次と等しい：はい」
Device Enrollmentに登録済み	Device Enrollmentに登録済みを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「Device Enrollmentに登録済みは次と等しい：はい」
データ保護	デバイス上でデータ保護が有効化されているかどうかを示します。**[はい]** か **[いいえ]** のいずれかの値となります。 ルールの例：「データローミング保護は次と等しい：はい」
データローミング有効	データローミング有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「データローミング有効は次と等しい：はい」
デバイスブロックステータス	デバイスブロックのステータスに基づくルール。 ルールの例：「デバイスブロックステータスは次と等しい：ブロック」
デバイスID	具体的なデバイスIDまたはデバイスID範囲に関するルール。

ルールオプション	説明
	ルールの例：「デバイスIDは次より大きい：45」。x
ホームMCC	ホームのモバイル国コードに基づくルール。 ルールの例：「ホームMCCは次と等しい：310」
ホームMNC	ホームのモバイルネットワークコードに基づくルール。 ルールの例：「ホームMNCは次と等しい：510」
IMEI	具体的なIMEI値に関するルール。 ルールの例：「IMEIは次から始まる：9900」。
招待ステータス	以下のいずれかの招待ステータスオプションを選択してください。 • **なし** • **保留中** • **有効期限切れ** • **完了** ルールの例：「招待ステータスは次と等しい：保留中」。
ロケーターサービス有効	位置情報サービス有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「位置情報サービス有効は次と等しい：はい」
隔離ステータス	位置情報サービス有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「隔離ステータスは次と等しい：はい」

ルールオプション	説明
登録：	デバイスが登録された日時の範囲を選択するルール。 ルールの例：「登録が次の範囲内：10/03/2017 09:00:00, 10/20/2017 17:00:00」。
ローミング	ローミングを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「ローミングは『はい』」
ステータス	以下のいずれかの招待ステータスオプションを選択してください。 • **アクティブ** • **撤去保留中** • **撤去を送信しました** • **リタイヤ済み** • **撤去を取り消しました** • **ワイプ保留中** • **ワイプを送信しました** • **ワイプ済み** • **ワイプを取り消しました** ルールの例：「ステータスは次と等しい：撤去保留中」。
ボイスローミング有効	ボイスローミング有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「ボイスローミングは『はい』」
Wi-Fi MACアドレス	特定のMacアドレス値を入力します。

ルールオプション	説明
	ルールの例：「Wi-Fi MACアドレスは次と等しくない：00-14-22-01-23-45」。
iCloudバックアップ有効	iCloudバックアップ有効化を **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「iCloudバックアップ有効は次と等しい：はい」
iTunes Storeアカウントアクティベーションステータス	iTunes Storeアカウントアクティベーションステータスを **[はい]** または **[いいえ]** で表現するルール。 ルールの例：「iTunes Storeアカウントアクティベーションステータスは次と等しくない：いいえ」。
プラットフォームの種類	[すべてのアプリケーション] レポートに適用されます。
ソース	[すべてのアプリケーション] レポートに適用されます。
カスタム属性	[すべてのアプリケーション] レポートに適用されます。
管理対象	[すべてのアプリケーション] レポートと [最も利用されているアプリケーション] レポートに適用されます。
アプリ識別子	[すべてのアプリケーション] レポートのデフォルトです。
MEID	[非マネージドアプリ] レポートに適用されます。

レポートに関するアクションの実行

[スケジュール済みのレポート] ページで、さまざまなアクションを実行できます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[スケジュール済みのレポート]** ページで、**[アクション]** ドロップダウンメニューをクリックし、以下のいずれかのオプションを選択します。

アクションオプション	実行されるアクション
表示	レポートを表示できます。
編集	レポートを編集できます。
今すぐ実行	レポートを実行します。
CSV のダウンロード	レポートをCSV形式でダウンロードします。
PDF のダウンロード	レポートをPDF形式でダウンロードします。
削除	レポートを削除します。

レポートの詳細の表示

レポートの詳細を表示し、作成したレポートに対してアクションを実行できます。

手順

1. **[ダッシュボード]** > **[レポート]** に進みます。
2. **[スケジュール済みのレポート]** ページで、詳細を表示するレポートの名前をクリックします。そのレポートの

ページが開きます。

3. 以下のオプションから1つ選択します。

アクションオプション	実行されるアクション
トグル	レポートを有効または無効にできます。
今すぐ実行	レポートを実行します。
表示	レポートの詳細を表示できます。[アクション]ドロップダウンメニューを使用して、次のいずれかのタスクを実行します。 • **無効化** • **最新のCSV/PDFをダウンロード**(CSVであれ、PDFであれ、CSVとPDFであれ、選択したレポートのタイプに基づいて、[ダウンロード]オプションが表示されます) • **履歴** • **削除**
削除	レポートを削除します。

ユーザー

モバイルデバイスの登録に誰かを招待する前に、その人物のユーザーエントリを作成する必要があります。また、Ivanti Neurons for MDM を使用してデバイスの管理またはコンテンツの公開をサポートする人物のユーザー(管理者) を作成する必要もあります。

このセクションは以下のトピックを含みます。

ユーザーの追加

このセクションは以下のトピックを含みます。

同時に1人あるいは複数のユーザーを追加できます。多くのユーザーを追加した場合、フィルタリングにより、必要なユーザーのみを表示することもできます。

そのほか、このページでユーザーについてできることは以下のとおりです。

- ユーザーグループへの割り当て、ユーザーグループからの削除
- メッセージの送信
- 登録の招待
- 役割の割り当て
- パスワードの変更
- 削除

すべてのデバイス所有者プロファイルはデバイスアカウントに割り当てられます。割り当てられるデバイスの数に関して、デバイスアカウントに制限はありません。ユーザーアカウントには仕事用プロファイル(従業員所有)が割り当てられます。

ユーザーの追加

手順

1. **[ユーザー]** を開きます。
2. **[+追加]**(右上)をクリックします。
3. **[ユーザー1人]** を選択します。
4. フォームにユーザーの情報を入力します。
   - Eメールアドレス
   - 名
   - 性

   [ユーザー名]フィールドには入力したEメールアドレスが表示されます。ほとんどの場合、このデフォルトは変更しないでください。詳細はユーザー名編集のタイミングを参照してください。
5.

   このユーザーの表示名を変更したい場合は、**[表示名]** フィールド内のデフォルトテキストを編集します。
6. パスワードを割り当てたい場合は、**[パスワード]** および **[パスワードを確認]** フィールドに入力します。
   - パスワードを割り当てる場合は、それをデバイス登録のためにユーザーに伝達する必要があります。
   - パスワードを割り当てない場合、ユーザーはデバイス登録中にパスワードを作成する必要があります。
7. ドロップダウンリストから **[ロケール]** を選択します。
8. **管理対象Apple ID**を入力します。既存のApple IDとの競合を避けるため、管理対象Apple IDのサブドメインとして「appleid」を含めることができます。user@appleid.yourdomain.comなどです。サブドメインはApple Business Manager上の有効かつ検証済みのサブドメインである必要があります。

   現在のアカウントの管理対象Apple IDでアクティブなUser Enrollmentデバイスがある場合、異なる管理対象Apple IDでアカウントを更新できません。
9. 1つ以上のユーザーグループを指定します(任意)。「アクティブ」または「撤去保留中」ステータスのデバイスがある場合、管理対象Apple IDを更新できません。
10. このユーザーを招待する前にその他の機能を設定したい場合は、**[今すぐ招待状を送信]** オプションを選択解除します。これを解除しないと、**[完了]** をクリックすると招待メールが送信されます。
11. **[完了]** をクリックするとユーザーが追加されます。

Androidデバイスの場合、デバイスアカウントは、1つのローカルサービスアカウントを使用して多数のデバイスを登録できるシングルユーザーマネージドデバイスを想定しています。新規ユーザーを作成する際には、デバイス所有者マネージドGoogle Playアカウント登録のためのデバイスアカウント(デフォルトのユーザーアカウントではなく)を有効化できます。

[Android Enterpriseデバイスアカウント] のチェックボックスを選択すると、このアカウントに結び付くAndroid Enterprise仕事用マネージドデバイス登録に自動的にGoogleデバイスアカウントが指定されます。

Androidデバイスのローカルまたは LDAPユーザーを編集する際、ユーザーに関連付けられたAndroid enterpriseデバイス所有者マネージドGoogle Playアカウントデバイスには、次のデバイスチェックイン時にデバイスアカウントが指定されます。ただし、以下の条件を満たす場合に限ります。

- **[Android enterpriseデバイスアカウント]** のチェックボックスを選択することにより、機能が有効化されている。
- Androidデバイス上のGoアプリバージョンが47以降である。

複数のユーザーの追加

手順:

1. **[ユーザー]** を開きます。
2. **[+追加]**(右上)をクリックします。
3. **[複数のユーザー]** を選択します。
4. デフォルトでは**手動で**メールアドレスを入力します。ユーザーのメールアドレスをコンマで区切って入力または貼り付けます。

   例:jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
5. このユーザーを招待する前にその他の機能を設定したい場合は、**[今すぐ招待状を送信]** オプションを選択解除します。

   これを解除しないと、**[完了]** をクリックすると招待メールが送信されます。
6. **[完了]** をクリックするとユーザーが追加されます。

ファイルのアップロードによる複数ユーザーの追加

手順:

1. **[ユーザー]** を開きます。
2. **[+追加]**(右上) をクリックします。
3. **[複数のユーザー]** を選択します。
4. **[CSVをアップロード]** を選択します。
5. **[CSVテンプレートをダウンロード]** をクリックします。
6. テンプレートを編集し、各ユーザーについて以下の情報を入力します。
   - ユーザーID(必須)
   - Eメールアドレス(必須)
   - パスワード
   - 名
   - 姓
   - 表示名
   - ユーザーグループ
   - カスタム属性

   これらは、ユーザー1人を追加するときに入力する情報と同じです。ファイル内のエントリは10,000件までです。
7. ファイルを保存します。
8. ファイルを選択するには、アップロードエリアにドラッグするか、**[CSVをアップロード]** を選択します。
9. アップロードしたユーザー情報が表示された後、必要な編集を実行してください。
10. **[次へ]**(右下) をクリックします。
11. すぐに招待状を送信したくない場合は、**[招待状を送信しない]** を選択します。
12. **[完了]** をクリックします。

管理者の追加

手順:

1. **[追加]**(右上)をクリックします。
2. **[ユーザー1人]**を選択します。
3. フォームにユーザーの情報を入力します。
   - Eメールアドレス
   - 名
   - 性

   [ユーザー名]フィールドには入力したEメールアドレスが表示されます。
4. このユーザーの表示名を変更したい場合は、**[表示名]**フィールド内のデフォルトテキストを編集します。
5. **[パスワード]**フィールドにパスワードを割り当てます。
6. **[パスワードを確認]**フィールドにパスワードを再度入力します。
7. **[完了]**をクリックするとユーザーが追加されます。
8. デバイスの管理をサポートしてくれる人物にパスワードを伝えます。

nobodyユーザー

nobodyユーザーとは、削除不可能なデフォルトユーザーです。サービスは、ユーザーが関連付けられていないデバイス、例えば撤去済みユーザーにこのユーザーを適用します。

デバイス登録PIN情報の表示

デバイス登録認証タイプが[PINのみ]に設定されている場合、新規ユーザーを追加する際に生成された登録PIN情報が管理者に表示されます。この情報によりユーザーのデバイス登録を助けることができます。

- ユーザーが1人の場合、PINは**[ユーザー]** > **[ユーザーを登録に招待]**で表示するか、ユーザー詳細ページのPIN情報セクションでも確認できます。
- ユーザーが複数の場合、PINは[ユーザーリスト]ページのカラムに、[PINステータス(有効または期限切れ)]、[PIN発行済み]、[PIN有効期限切れ]と並んで表示されます。

[ユーザー]ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管 理
- ユーザー管 理

ユーザーグループ

このセクションは以下のトピックを含みます。

- 「動的管理ユーザーグループの作成」下
- 「手動管理ユーザーグループの作成」ページ87
- 「重複するユーザーグループのいずれか1つからユーザーグループを作成する」ページ87

複数のユーザーにアプリと役割を割り当てられるよう、ユーザーグループを作成します。たとえば、すべての部門マネージャーをアプリやコンテンツの管理者にしたい場合は、マネージャーグループを作成できます。

管理するユーザーグループは、以下のいずれかの方法で作成できます。

- **動的管理(最も一般的):** ローカルおよびLDAPユーザーが、所定のルールや属性に基づいて動的にグループに追加またはグループから削除されます。
- **手動管理(限定目的):** ユーザーを手動でグループに追加またはグループから削除します。必要な許可数が少なく、テスト目的のみの場合は、手動管理グループを推奨します。

[検索] フィールドにテキストを入力すると、そのテキストで始まる名前がすべて表示されます。

- 検索結果は、テキストの入力中、一致する可能性のあるリストとしてリアルタイムで表示されます。
- その後のアクションに一致する可能性のあるリストから目的のユーザーグループ名を選択します。
- 検索結果の一致では大文字と小文字が区別されます。

動的管理ユーザーグループの作成

手順

1. **[+追加]** をクリックします。
2. **[名前]** フィールドにユーザーグループ名を入力します。
3. (任意) **[説明を追加]** をクリックし、ユーザーグループの説明を入力します。
4. **[動的管理(最も一般的)]** オプションをクリックします。

5. 必要に応じてルールや属性を設定します。以下は、利用可能なルールのオプションです。
    - カスタムLDAP属性
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname
    - デフォルトLDAP属性
        - samAccountName
        - userPrincipalName
    - デフォルトユーザー属性
        - email_address
        - distinguished_name
        - last_name
        - display_name
        - first_name
        - ユーザーグループ
        - カスタムユーザー属性
    - ユーザーグループDN
    - ユーザーグループGUID
    - ユーザーグループ名
6. 各ルールについてローカルユーザーかLDAPユーザーを選択します。**ユーザーグループ**フィルター基準を使用すれば、サブグループに入れたり除外したりすることができます。
7. 「+」アイコンをクリックしてルールを追加します。
   追加したルールには**ANY**または**ALL**の条件フィルタを設定できます。
8. 「+」アイコンの隣の階層をクリックしてルールのグループを作成します。

9. ルール選択オプションの下に表示されるテキストクエリーにあるユーザーグループのルールと属性を確認します。

10. **[結果]** セクションで、構成した基準に一致するユーザーの詳細を確認します。ルールや属性を追加または変更すると、一致するユーザーが表示されます(存在する場合)。

11. **[保存]** をクリックすると構成したユーザーグループが保存されます。

手動管理ユーザーグループの作成

1. **[+追加]** をクリックします。

2. グループ名を入力します。

3. (任意) **[説明を追加]** をクリックし、説明を入力します。

4. **[手動管理(限定目的)]** オプションを選択します。

5. **[ユーザを検索]** フィールドで、グループに含める各ユーザのEメールアドレスを入力します。
   入力すると、一致するユーザーが検索され、存在すれば表示されます。

6. グループに追加したいユーザーを選択します。必要に応じてさらにユーザーを検索し、追加できます。

7. **[保存]** をクリックします。

> 手動管理のユーザーグループを作成した後、そのグループを動的管理ユーザーグループに追加することも可能です。この場合、手動管理ユーザーグループの編集が動的管理ユーザーグループの規則を破ることはありません。動的管理ユーザーグループに追加した手動管理ユーザーグループは削除できません。

重複するユーザーグループのいずれか1つからユーザーグループを作成する

Ivanti Neurons for MDM 92以降、ルールビルダーで「ユーザグループ名」属性が選択されている場合、管理者ポータルは重複するユーザグループ数と、重複するグループを識別するGUID番号を表示します。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。

2. **[ユーザー]** > **[ユーザーグループ]** を開きます。

3. **[+追加]** をクリックします。[ユーザーグループを作成] ウィザードが開きます。

    a. **[名前]** フィールドで名前を指定します。

    b. ルールビルダーから **[ユーザーグループ名]** を選択し、**[次と等しい]** を選択し、重複するグループ名の*1*つを選択します。

    c. さらにルールを追加するには、+プラスアイコンをクリックします。

    d. **[ユーザーグループGUID]** > **[次と等しい]** を選択します。

    e. 重複するユーザーグループ名とGUIDのリストが表示されているテーブルからGUIDをコピー＆ペーストします。結果には、新規グループに追加される関連ユーザーが表示されます。

    f. **[保存]** をクリックします。これで、リストされたユーザーが、作成された新しいユーザーグループに追加されます。

[ユーザーグループ] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- ユーザー管理

ユーザー設定

このセクションは以下のトピックを含みます。

ユーザー設定では、デバイス登録オプションを定義します。複数の種類があります。

- **デバイス登録設定**: パスワード、PIN、またはその両方による認証、Apple 登録タイプ、デバイスを設定します。
    - これまでSAML auth/IdPを設定すると、SAML認証がデバイス登録とポータル認証の両方に使用されていました。リリース79.1以降、トグルボタンが装備され、管理ポータルへのアクセスとデバイス登録に異なる認証方式を選択できるようになりました。バイパストグルはデバイス登録にのみ使用します。

      この機能はPINのみの認証タイプではサポートされません。

- **デバイス制限設定**: 1人のユーザーが登録できるデバイスの数を設定します。

- **ワイプの上限設定**: 一度にワイプできるデバイスの最大数に対する制限を設定します。
- **セルフサービスポータル認証設定**: セルフサービスポータルのパスワード認証の種類を設定します。
- **パスワードの複雑さ設定**: デバイス登録に使用されたローカルアカウントのパスワードの複雑さとポリシーのパラメータを設定し、管理ポータルとセルフサービスポータルにアクセスします。
- **利用規約の設定**: 各デバイス登録についてユーザに表示される利用規約を設定します。
- **ユーザー招待リマインダー設定**: ユーザー招待リマインダーメールを送信する日付と頻度を設定します。
- **ユーザー登録確認設定**: ユーザー登録確認メールの送信機能を制御します。ソリューションの概要は、「登録確認メールの構成と使用」ページ27を参照してください。また、具体的なユーザー設定の方法については、以下の「ユーザー登録確認メールの構成」ページ100を参照してください。
- **ユーザー仕事用スケジュール設定**: ユーザー仕事用スケジュールを構成、所定の非勤務時間はSentryからマネージドデバイスへのすべての通信をブロックできるかどうかを管理します。「つながらない権利」が法律で認められている地域に有用です。
- **管理ポータル認証設定**: Ivanti Neurons for MDM が管理者にパスワードのみ、またはパスワードとPINを入力させるかどうかを管理します。

[すべてのユーザー] グループ向けにデフォルト設定を編集したり、カスタム設定を追加してそれらを別のユーザーグループに割り当てたりすることができます。

デフォルト設定の編集

ロックアイコンのある設定の **[編集]** リンクをクリックします。デフォルト設定は削除できません。

カスタム設定の追加

[特定のユーザーグループに設定を追加] リンクをクリックします。

カスタム設定の削除

Xアイコンをクリックします。

新規デバイス登録のための設定の構成

新規デバイス登録のための最小OSバージョン、認証タイプ、デバイス所有者を指定できます。Ivanti Neurons for MDMの旧バージョンで生成されたデバイス登録URLは、最新バージョンでは機能しません。管理者は、デバイス登録用のデバイス登録URLを生成する必要があります。

デバイス登録の許可リスト化

デバイス登録を許可リスト化するオプションは、デフォルトユーザー設定でのみ利用でき、カスタムユーザー設定にはありません。CSVファイルは、少数のデバイスを許可リスト化するシリアル番号とカスタムデバイス属性を記載したテンプレートを使ってアップロードできます。許可リストは、1つ以上の既存のカスタムデバイス属性を入れて作成します。これにより、登録後にデバイスグループまたはスペースに属性を割り当てることができます。

カスタム属性を作成するには **[管理]** > **[属性]** を開きます。許可リスト機能が有効化されていてデバイスのシリアル番号がCSVファイルに入っていない場合、iOS、macOSデバイスは、iRegを通じて登録できません。CSVファイルに重複したシリアル番号がある場合、最後に入力されたものが考慮され、それに関連するカスタムデバイス属性が、登録中のデバイス割り当てに使用されます。

[デバイス許可リスト] オプションが有効になっている場合、許可リストに入っているデバイスのみがIvanti Neurons for MDMへの登録を許可されます。この機能は、Webベースの登録プロセスを通じて登録されるデバイスのみに適用されます。すでにIvanti Neurons for MDMに登録されているデバイスには影響しません。登録後、デバイスのシリアル番号がCSVファイルから削除されてもデバイスは撤去されません。CSVファイルに記載されているユーザーは任意であり、ユーザーがCSVファイルに記載されていて有効なユーザーである場合のみ割り当てられます。

新しいCSVファイルをアップロードしたい場合は、既存のCSVファイルを削除して新しいファイルをアップロードしてください。許可リスト化はiRegでのみサポートされています。Goクライアントが必要な場合は、ゼロタッチ登録を選択してください。AppConnectやThreat Defenseのような機能が動作するためには、Goクライアントがシステムにインストールされている必要があります。アプリ内登録はサポートしないため、ユーザーはまずiRegでデバイスを登録し、その後でGoアプリをアプリカタログからデバイスにプッシュします。ユーザーがアプリのインストールを受け入れると、デバイスがマネージドデバイスとなり、すべての機能は登録後に引き続き動作するようになります。ゼロタッチ構成は、AppConnectステータスがActiveまたはInactiveのデバイスでは使用できません。AppConnectがNoneの場合のみ使用できます。AppConnectステータスは、iRegを通じた登録の後、Goクライアントがデバイス上で起動されるまでNoneになっています。

手順

1. Ivanti Neurons for MDMにログインします。
2. **[ユーザ]** > **[ユーザ設定]** を開きます。
3. **[デバイス登録設定]** で **[+特定のユーザグループの設定を追加]** をクリックします。

4. デフォルトの **[デバイス登録認証タイプ]** 設定を編集するか、新しい設定を追加します。
5. **[名前]** フィールドに名前を入力します。
6. (任意) 設定の説明を入力します。
7. **[OS設定]** セクションで、iOS、macOS、Windowsの最小OSバージョンを定義します。

   [最低バージョンを有効にする] トグルボタンを選択し、ドロップダウンリストからOSバージョンを選択します。

   > [最低バージョンを有効にする] 設定は、DEPデバイス登録には適用されません。

8. **Android**の場合：
   - **[最小セキュリティパッチ]** オプション(Androidのみ)を有効化し、以下のドロップダウンリストで期間を指定します。
     - **日**
     - **カ月**
     - **年**
   - **[メーカーの許可リスト/ブロックリスト]** オプションを有効化し、以下のいずれかを指定します。
     - **許可リストを作成** - これらのメーカーのデバイスのみ登録を許可します。
     - **ブロックリストを作成** - これらのメーカーのデバイスの登録を防止します。

       メーカーを追加するには：

       a. **[メーカーを追加]** をクリックします。

       b. **[メーカーの名前]** フィールドにメーカーの名前を入力します。

       c. **[保存]** をクリックします。追加したメーカー名がテーブルに表示されます。

       > メーカー名では大文字と小文字が区別されます。追加したメーカー名を編集または削除するには、メーカーの **[編集]** または **[削除]** オプションをクリックします。

9. [Apple Enrollment] セクションでApple Enrollmentの種類を選択します。

- **デバイス登録**
- **User Enrollment** - iOSおよびiPadOSデバイスにはデフォルトでUser Enrollmentが適用されます。
- (任意) **macOSデバイス(macOS 10.15+)を含める** - macOSデバイスにもUser Enrollmentを適用する場合に選択します。

10. **[登録招待方法(iOSとAndroidのみ)]** セクションでは、**[MAM のみの登録]** を有効化します。

> このオプションはMAM Onlyデバイスの登録でのみ有効化してください。有効化した場合、ユーザーはパブリックアプリストアにリダイレクトされ、そこからAppStationクライアントアプリをダウンロードすることになります。

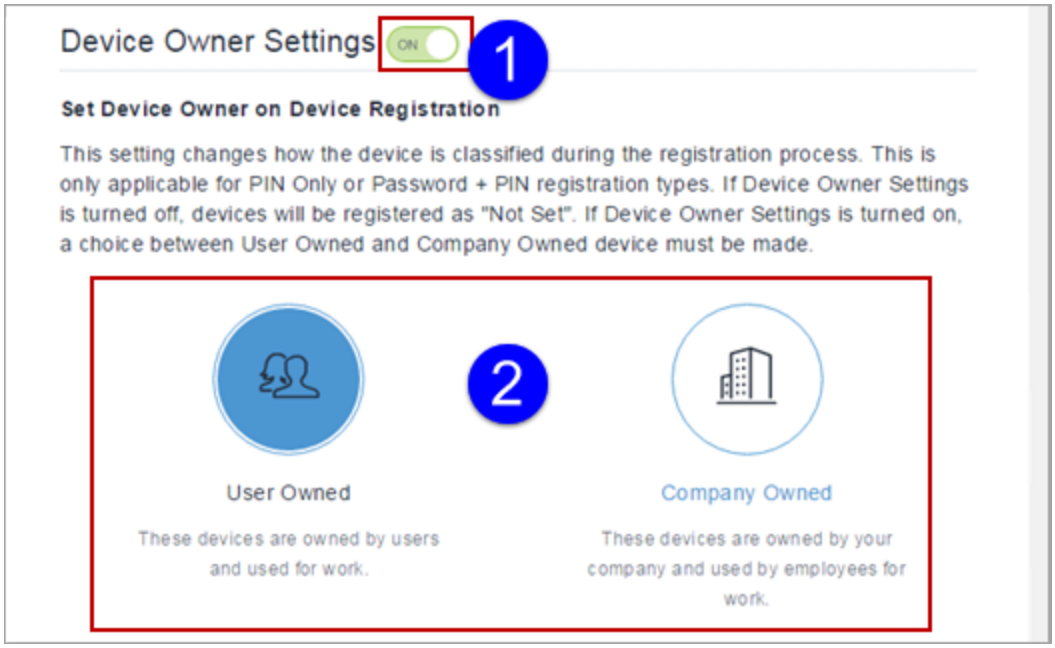
11. **[デバイス登録認証タイプ]** セクションで、**[登録タイプを選択]** ドロップダウンから次の登録タイプオプションのいずれかを選択します。デバイス登録を使用する場合は、デバイス登録構成が選択と一致することを確認してください。
    - **パスワードのみ**
    - **PIN のみ** このオプションを選択すると、[IdP デバイス登録認証のバイパス] トグルボタンがロックされます。
    - **パスワードとPIN**

      > アカウントアクティベーションを完了するためにPINを受信することがあります。

> この設定は通常の登録とDevice Enrollment登録の両方に反映されます。

12. PIN の場合、次の項目を指定します。デバイス登録中、必要であれば **[PINを再送信]** をクリックできます。
    - **PINの有効期間:** PINが有効である期間(1～30日)。
    - **PINの長さ:** 文字数(4～12文字)。
    - **ユーザーに新規PINの要求を許可**(忘れた場合あるいは有効期限が切れた場合)。
13. **[デバイス所有者設定]** をオンにし、**[ユーザー所有]** または **[会社所有]** をクリックすることも可能です。この設定は登録プロセス中にデバイスの分類を変更します。

- **[デバイス所有者設定]** がオンで、管理者がデバイスを「ユーザー所有」とマークしている場合、ユーザーによるデバイスの登録中およびセルフサービスポータルで、デバイスを「ユーザー所有」または「会社所有」とマークするオプションが表示されます。User Enrollment登録デバイスの場合、管理者の選択に関係なく、デフォルトのデバイス所有者の設定は「ユーザー所有」となります。
- 監視対象デバイスの場合、デバイス所有者設定は「会社所有」となります。



14. 設定を配信したいユーザーグループ(1つ以上)について **[追加 +]** をクリックします。
15. (iOSおよびmacOSデバイス専用のオンデマンド機能) または、**[デバイス許可リスト]** オプションをオンにし、許可リスト化したシリアル番号に基づくデバイス登録を許可します。
16. **[次へ]** をクリックします。[ユーザ設定配布] ページが開きます。
17. ユーザグループ配布を選択します。
18. **[完了]** をクリックします。
19. ユーザに招待を送信します。詳細については、「ユーザーの招待」ページ140をご参照ください。

次の点に注意してください。

[PIN のみ] オプションを使用してユーザデバイスが登録された場合、認証用の PIN が記載された登録確認電子メールがユーザに送信されます。

- PINがユーザーのメールIDに送信されます。
- ユーザーがデバイス登録ページにPINを入力します。
- PIN が正しい場合は、登録プロセスを完了する必要があります。

SAMLベースのIDプロバイダー(IdP) を設定しているユーザーは、Ivanti Neurons for MDMでデバイス登録中にPINでの認証が可能です。デバイス登録認証の種類はPINとパスワードでなければなりません。PIN およびパスワード機能はセキュリティの高い二要素認証として機能します。この場合、該当のユーザーによるデバイス登録は以下の手順となります。

- PINがユーザーのメールIDに送信されます。
- ユーザーがデバイス登録ページにPINを入力します。
- PINが正しい場合、ユーザーはIdPのログインページにリダイレクトされ、そこでIdPのユーザー名とパスワードを入力します。
- IdPの認証情報が正しい場合、ユーザーはデバイスにリダイレクトされ、登録プロセスを完了します。

ユーザーあたりのデバイス制限の構成

手順

1. デフォルトの **[デバイス制限]** 設定を編集するか、新しい設定を追加します。
2. 編集するか、設定を識別するための名前を割り当てます。
3. 設定の説明を入力します。これは省略可能です。
4. ドロップダウンから制限を選択します。
5. 設定を配信したいユーザーグループ(1つ以上) について **[追加 +]** をクリックします。
6. **[保存]** をクリックします。

デバイスワイプ制限の構成

手順

1. デフォルトの**デバイスワイプ制限**設定を編集します。
2. **[すべてのユーザーに対してワイプ制限を有効化(デフォルトの役割を含む)]**オプションをオンにします。
3. **[ユーザーが1回にワイプできるデバイスの最大台数]**フィールドに、1回にワイプできるデバイス数の上限を入力します。デフォルト値は1です。デバイスのワイプ制限として設定できる最大値は200です。
4. **[完了]**をクリックします。

セルフサービスポータル認証の構成

手順

1. デフォルトの**[セルフサービスポータル認証]**設定を編集するか、**[+特定のユーザーグループの設定を追加]**をクリックして新規設定を追加します。
2. 編集するか、設定を識別するための名前を割り当てます。
3. 設定の説明を入力します。これは省略可能です。
4. ドロップダウンから**[セルフサービスポータル認証形式]**を選択します。以下のいずれかのオプションを選択できます。
   - パスワード
   - 証明書
5. **[次へ]**をクリックします。
6. この構成を配布するユーザーグループを1つ以上選択します。
7. **[完了]**をクリックします。

パスワードの複雑さの設定

デバイス登録に使用されたローカルアカウントのパスワードの複雑さとポリシーのパラメーターを設定し、管理ポータルとセルフサービスポータルにアクセスできます。

以下に設定するパスワードの長さ、特性、ポリシーが、パスワードのセキュリティを決定します。

これは、ユーザーが有効なパスワードを選択する難しさも左右します。エンドユーザーがローカルアカウントから管理ポータルにアクセスする際にセキュアパスワードを使用させたい場合は、デバイス登録時にPINを使用し、パスワードの複雑さがデバイス登録を妨げないようにしてください。**[ユーザー設定] > [デバイス登録設定]** で「デバイス登録認証」タイプの設定を使用して、デバイス登録の認証モードを選択します。

手順

1. デフォルトの **[パスワードの複雑さ]** 設定を編集します。
2. 以下のパスワードの複雑さを設定します。

設定	操作内容
Minimum Password Length (パスワードの最小文字数)	スライダーでパスワードの最小文字数を指定し、ユーザーが短くセキュアでないパスワードを作成しないようにします。 範囲は8～32です。
必要な特性	パスワードを選択したときに満たす必要のあるパスワードの特性数を指定します。満たす必要のある特性の最小数は3です(連邦機関では4)。
特殊文字(記号)が必要	パスワードに含める英数字以外の文字の数を指定します。
必要な大文字数	パスワードに含める大文字のアルファベットの数を指定します。
小文字が必要	パスワードに含める小文字のアルファベットの数を指定します。
数字が必要	パスワードに含める数字の数を指定します。
パスワードの検証	
数字の連続を許可	連続する数字の数を指定します。 例:123
文字の繰り返しを許可	反復するアルファベットの数を指定します。 例:bbc

3. 以下の行動に関するパスワードポリシーを設定します。

設定	操作内容
保持するパスワード履歴	新しいパスワードを何回設定すれば古いパスワードを再使用できるかをスライダーで指定します。 範囲は3～36です。
パスワード有効期間	スライダーを動かし、ユーザーパスワードの有効期限を日数で指定します。 範囲は30～365日です。
無活動タイムアウト	スライダーを動かし、管理ポータルまたはセルフサービスポータルのセッション時間が非アクティブになるまでのユーザーの無活動時間を指定します。 範囲は5～60(分)です。
ログイン失敗の閾値	ログインに何回失敗すれば5分間のアカウントロックアウトがかかるかをスライダーで指定します。 範囲は2～5です。 失敗が閾値内にある場合は、ユーザーにロックアウトに関するメッセージと後でログインを試すよう促すメッセージが表示されます。 失敗が閾値を超えた場合、ユーザーにはロックアウトに関するメッセージと、指定した時間(分数)の後にログインを試すよう促すメッセージが表示されます。

4. **[完了]**をクリックします。パスワードの複雑さのデフォルト設定を変更しても、既存のローカルアカウントの古いパスワードは変更されません。期限切れの時点で、ユーザーはパスワードの更新を求められます。管理者は、管理ポータルにログインする際、パスワードのリセット方法についてヘルプデスクに問い合わせることができます。

デバイス登録では、PINのみの登録モードを推奨します。

利用規約の定義

手順

1. 新しい**利用規約**設定を作成します。
2. 設定を識別するための名前を指定します。
3. 設定の説明を入力します。これは省略可能です。
4. **[ユーザに確認]**を選択します。オプションを選択します。
5. 表示するタイトルとテキストを入力します。
6. 設定を配信したいユーザーグループ(1つ以上)について **[追加 +]** をクリックします。
7. **[保存]**をクリックします。

一度承諾された利用規約を削除することはできません。ただし、**[ユーザに確認]**をオフにすると、新しい登録の確認をオフにできます。オプションを選択します。

ユーザー招待リマインダーメールの構成

管理者は、この設定を利用してユーザー招待リマインダーメールを送信し、デバイス登録を推進することができます。

手順

1. 既存の**[ユーザー招待リマインダー設定]**を編集するか、新しいものを追加します。
2. 編集するか、設定を識別するための名前を割り当てます。
3. 設定の説明を入力します。これは省略可能です。
4. **[ユーザー招待リマインダー]**オプションがオンになっていることを確認してください。
5. [開始日と終了日を定義]領域で、リマインダーメールの送り始めと終わりの時期を選択します。

   送信可能なメールは最大30通です。この上限をリセットするには、管理者が招待を再送信する必要があります。

6. [頻度を定義]領域では、リマインダーメールを送信したい頻度を選択します。
7. **[次へ]**をクリックします。

8. この構成の配布を選択します。
9. **[完了]** をクリックします。

ユーザー登録確認メールの構成

管理者は、登録を完了した新規ユーザーにメールを送信できます。

手順

1. 既存の **[ユーザー登録確認設定]** を編集するか、新しいものを追加します。
2. 編集するか、設定を識別するための名前を割り当てます。
3. 設定の説明を入力します。これは省略可能です。
4. **[ユーザー登録の完了時に確認メールを送信]** がオンになっていることを確認します。
5. **[次へ]** をクリックします。
6. この構成の配布を選択します。
7. **[完了]** をクリックします。

ユーザー仕事用スケジュール設定の構成

管理者は、ユーザーの「ユーザー仕事用スケジュール」を構成することで、所定の非勤務時間はSentryからマネージドデバイスへのすべての通信をブロックすることができます。これは「つながらない権利」が法律で認められている地域に有用です。

手順

1. **[ユーザ]** を選択します。
2. **[ユーザー設定]** を選択します。
3. **ユーザー仕事用スケジュール設定** のセクションで、**[+特定のユーザーグループの設定を追加]** を選択します。
4. 設定の名前を入力します。
5. 設定をオンにします。
6. タイムゾーンを選択します。

7. Ivanti Neurons for MDM がExchange ActiveSyncプロトコル、AppConnect対応アプリ、マネージドアプリをブロックする時間帯を設定します。
8. **[次へ]** をクリックします。
9. 配布を設定した後、**[完了]** をクリックします。

変更がこのデバイスに適用されるまでに最大1時間15分かかる場合があります。

管理ポータル認証設定の構成

管理者は、ユーザーのログインを認証する認証タイプを設定できます。ここで、パスワードのみ、またはパスワードとPINの両方のいずれをユーザーに求めるかを設定します。

手順

1. 既存の **[管理ポータル認証設定]** を編集するか、新規に追加します。
2. 編集するか、設定を識別するための名前を割り当てます。
3. 設定の説明を入力します。これは省略可能です。

4. **[管理ポータル認証タイプ]** で以下のいずれかのオプションを選択します。

オプション	説明
パスワード	パスワードのみでログインを認証する場合に選択します。 アカウントアクティベーションを完了するためにPINを受信することがあります。
パスワードとPIN	パスワードとPINでログインを認証する場合に選択します。 このオプションを選択すると、以下のフィールドが表示されます。 • **PINの有効期間:** ドロップダウンリストからPINの有効期間を分単位で選択します。範囲は1～15です。 • **PINの長さ:** PINの文字数をドロップダウンリストから選択します。範囲は4～12です。 LDAP管理アカウントではなく、ローカルアカウントでのみ選択可能です。
ユーザーによる新しいPINの要求を許可	ユーザーによる新しいPINの要求を許可する場合に選択します。

5. **[次へ]** をクリックします。
6. この構成の配布を選択します。
7. **[完了]** をクリックします。

SAMLベースのIDプロバイダー(IdP)を設定しているユーザーは、Ivanti Neurons for MDMで管理ポータルへのPIN認証が可能です。管理ポータル認証の種類はPINとパスワードでなければなりません。この機能はセキュリティの高い二要素認証として機能します。この場合、該当のユーザーによるログインは以下の手順となります。

- PINがユーザーのメールIDに送信されます。
- ユーザーが管理ポータルログインページにPINを入力します。
- PINが正しい場合、ユーザーはIdPのログインページにリダイレクトされ、そこでIdPのユーザー名とパスワードを入力します。
- IdPの認証情報が正しい場合、ユーザーは管理ポータルにリダイレクトされ、登録プロセスを完了します。

管理ポータルにログインする際、ユーザーが **[パスワードを忘れた]** をクリックすればパスワードをリセットできます。次の画面でユーザーは新しいパスワードと、メールアドレスに送信されてくるPIN(前回のユーザー認証モード設定に基づく)を入力します。必要に応じて **[PINを再送信]** をクリックします。ユーザが2回目のパスワードのリセット要求を送信するには、最初の要求から15分間待機する必要があります。

この構成をデバイスに配布すると、ユーザーがパスワードやPINを使用してのログインに連続して失敗した場合(デフォルトは5回)にアカウントがロックされ、画面にユーザーへのメッセージが表示されます。

ユーザーのブランディング

ユーザーのブランディングでは、ユーザーが認識する名前とロゴでデバイス登録プロセスをカスタマイズできます。次の方法で、ユーザーに表示されるブランディングをカスタマイズできます。

- 登録URLのカスタムホスト名を設定する
- 登録メールおよび登録画面にロゴを表示する
- 登録操作中にカスタムファビコンを表示する

ライセンス: Gold

前提条件:

- カスタムURLで使用するホスト名を決めます。次の要件を満たす必要があります。
  - スペースを含まないこと
  - 特殊文字を含まないこと
- 次の要件を満たすロゴファイルを取得します。
  - PNG形式
  - 580 x 80ピクセル
- 次の要件を満たすファビコンファイルを取得します。
  - PNG形式
  - 64 x 64ピクセル

手順:

1. **[ユーザー] > [ユーザーのブランディング]** へ進みます。
2. **[カスタマイズ]**(右上)をクリックします。
3. **[ホスト名]** フィールドに、URLのホスト名として使用する短縮名を入力します。
4. **[利用可能性をチェック]** をクリックし、入力したホスト名が誰かほかの人によって使用されていないかどうかを確認します。
5. そのホスト名が利用不可の場合、別の名前を入力します。

6. **[URLプレビュー]** にある登 録URLをメモします。
7. **[次 へ]** をクリックします。
8. **[ロゴ]** で、**[ファイルを選 択]** をクリックし、登 録 メールと登 録 画 面 で使 用 するロゴをアップロードします。
9. **[次 へ]** をクリックします。
10. **[ファビコン]** で、**[ファイルを選 択]** をクリックし、登 録 操 作 中 の Ivanti Neurons for MDM ファビコンに表 示 するファビコンをアップロードします。
11. **[完 了]** をクリックします。

Apple Business Managerでのユーザー登録

このセクションは以下のトピックを含みます。

対象：

- iOS 13.0からIvanti Neurons for MDMがサポートする最新版を搭載した非監視対象デバイスである。
- macOS 10.15またはサポートされる以降のIvanti Neurons for MDMバージョンを搭載したデバイス。

Apple Business Managerは、ITチームが、デバイス導入、コンテンツの購入と配布、組織内の役割管理を自動化するためのツールです。Apple Business ManagerにはUser Enrollment機能、すなわち、個人所有デバイスの業務利用(BYOD)を認める企業向けの登録オプションがあります。User Enrollmentとは、企業に必要なレベルのセキュリティを備え、ユーザープライバシーの保護を大幅に強化したMDMプロトコルの修正バージョンです。

User Enrollmentでは、管理者は次のことを実行できます。

- マネージドアプリのインストールと削除
- ネットワーク構成のインストールと削除
- マネージドアプリとアカウントを対象とした部分VPNのインストール
- パスワード使用の要求

User Enrollment有効化の要件

User Enrollment有効化の要件は以下のとおりです。いずれかを満たしていない場合は、登録タイプがデバイス登録になります。

- Ivanti Neurons for MDMによってサポートされる最新版を搭載した非監視対象デバイス、またはmacOS 10.15またはサポートされる以降のIvanti Neurons for MDMバージョンを搭載したデバイス。
- [Apple Enrollmentの種類] フィールドのユーザー設定が [User Enrollment] に設定されている。
- Apple Business Managerアカウント。
    - Apple Appライセンスアカウントは同じApple Business Managerアカウントの一部である必要があります。
    - Apple Business Manager内で、アカウントが [ロケーション] に表示されている場合は、同じロケーションのApps and Booksが必要となります。新しいロケーションの追加が必要な場合もあります(例 : 西海岸)。
- 管理対象Apple ID - 各登録済みデバイスに指定される管理対象Apple ID。
    - 管理対象Apple IDは、MDM管理とアプリライセンス供与の認証要素となります。
    - MDMがアプリとメディアをプッシュする際には、デバイスに関連付けられている管理対象Apple IDに必要なAppleライセンスが指定されます。
    - Apple IDはユーザーデータと見なされるため、GDPRコンプライアンスの一環として、Managed Apple IDはユーザーリストとユーザー詳細ページ内で非表示となります。
    - 管理対象Apple IDは最初にApple School Managerに利用され、現在はApple Business ManagerのUser Enrollmentに利用されています。

      > デバイスの管理対象Apple IDと「Appとブック」のロケーショントークンは、同じApple Business Managerアカウントの組織に由来する必要があります。

      異なる場合、アプリのライセンス割り当てが失敗したときにIvanti Neurons for MDM管理ポータルに通知が表示されます。
- フェデレーション認証用に設定されたMicrosoft Azure Active Directory、またはApple Business Managerで手動で作成され、検証済みのドメインを持つApple ID。
    - フェデレーション認証の使い方は、Appleの「Apple Business Managerユーザーガイド」を参照してください。ログインが必須です。
- LDAPに同期されているデバイスユーザーは、デバイス管理の役割を指定され、管理対象Apple IDに関連付けられます。

[ユーザー] リストページと [デバイス] リストページでは、すべてのユーザーについて管理対象Apple IDカラムを追加し、表示することができます。[デバイス] リストページでは、User Enrollment登録済みカラムを追加し、User Enrollmentデバイスのステータスを表示します。ユーザーとデバイスをエクスポートすると、これらのカラムもCSVファイルに含まれます。

登録の優先度

- User Enrollmentは、iOS対応GoクライアントとiReg経由でサポートされます。
- 自動Device EnrollmentとApple Configurator登録の場合は常にデバイス登録となります。
- デバイスにMAM構成が適用される場合、MAM登録のほうがUser Enrollmentより優先されます。
- Auth-OnlyとUser Enrollmentの両方の要件を満たす場合は、User Enrollmentが優先されます。
- Go for iOSクライアントでデバイスを再エンロールする場合、Ivanti Neurons for MDMにおける登録タイプの変更に関係なく、登録タイプはデバイス登録中のタイプと同じになります。たとえば、ユーザー登録されたデバイスの場合、Ivanti Neurons for MDMでDevice Enrollmentのタイプに変更し、Goクライアントからデバイスを再エンロールしても、デバイスはデバイス登録ではなくユーザー登録のままとなります。

標準的なMDM登録とUser Enrollmentの違い

このセクションでは、標準的なMDM登録とApple Business ManagerでのUser Enrollmentの違いを説明します。

標準的なMDM登録

以下のリストは、標準的なMDM登録のIvanti Neurons for MDMサーバーに実行できることです。ただし、User Enrollmentモードではできません。

MDMサーバーは:

- デバイスを消去できません。
- デバイスユーザーがデバイスにインストールした個人用のアプリを表示できません。
- ユーザーがインストールしたアプリをMDMマネージドアプリに変換できません。
- デバイスパスコードは消去できません (例: デバイスのロック解除)。
- 長い複雑なデバイスパスコード要件を設定できません。

- デバイス全体のVPNまたはWi-Fiプロキシを設定できません。また、携帯電話(セルラー)機能の管理は一切できません。
- UDID、シリアル番号、IMEIなどのデバイス識別子を表示できません。
- デバイス全体にかかる制限の多くを適用できません(アプリコンテンツの評価制限など)。iCloudのブロックや監視対象の制限も適用できません。

Apple Business Managerでのユーザー登録

User Enrollmentでもやはり、企業アプリ、アカウント、データの管理に必要なすべてをMDMサーバーが実行できます。

User Enrollmentは:

- 自社開発アプリやユーザーベースの(Apple) Apps and Booksライセンス経由のアプリをインストールできます。
  - ライセンスは申し込み順で使用され、管理対象Apple IDによって消費されます。
  - User Enrolledデバイスにインストールしたアプリが使用するライセンスは、デバイス登録デバイスにインストールされた同じアプリが使用するライセンスとは異なります。
  - Apple Apps and Booksアプリケーションのライセンスの種類をユーザー詳細ページの[ライセンス使用状況]タブで確認します。登録タイプは[User Enrollment]または[Device Enrollment]と表示されます。
- パスコードペイロード設定を強制します。例:
  - allowSimple = false
  - forcePIN = true
  - minLength = 6
- 企業管理対象アプリ、証明書、プロファイルに関連するクエリーデータ。
- MDMによってインストールされたアプリ、メール、連絡先、カレンダー用にPer-App VPNを設定します。
- マネージドオープンイン、マネージド連絡先、ロック画面上のマネージドデータなど、複数の制限を適用します。

企業データは独立したApple File System(APFS)ボリュームに保存されます。これは登録時に作成され、デバイスユーザーデータとは別に暗号化されています。このボリュームは、マネージドアプリ、企業用Notes、企業用iCloud Drive文書、企業用Keychainエントリー、マネージドメール添付ファイルおよび本文、カレンダー添付ファイルによって保存されたデータを含みます。MDMの登録を解除するとボリュームとキーが破壊されます。

第三者のアプリはすべて個人用アプリかIvanti Neurons for MDMによるマネージドアプリのいずれかです。MDMサービスは、デバイスユーザーがすでにインストールしたアプリの管理を開始できません。この場合、管理者は個人用アプリを削除してからMDMを通じてアプリをインストールするようデバイスユーザーに依頼する必要があります。MDMサービスは、ユーザーがすでにインストールしたアプリの管理を開始できません。しかし、NotesやFilesなど一部のシステムアプリは仕事用アカウントと個人用アカウントの両方をサポートします。

macOSデバイスのUser Enrollment

User Enrollmentは、macOS 10.15またはIvanti Neurons for MDMがサポートする以降のバージョンを搭載したデバイスでサポートされます。

- macOS対応Mobile@WorkはmacOS User Enrollment登録デバイスに対応しません。
    - macOS User Enrollment登録デバイスにアプリが配布されても、アプリはMDMからデバイスにプッシュされません。
    - したがって、Packager(MIP)アプリのアプリ管理やスクリプト管理といったMobile@Work機能はmacOS User Enrollment登録デバイスではサポートされません。
- macOS User Enrollment登録デバイスにおけるアプリ依存性と挙動の変化。
    - MDMはメインのアプリを配布する前に必須アプリがインストール済みかどうかを確認できないため、macOS User Enrollment登録デバイスでは、アプリ依存性への対応はベストエフォートとなります。
    - アプリと構成は、macOS User Enrollment登録デバイスのユーザーおよびユーザーグループに配布可能です。しかし、アプリは常に[インストール済み]ではなく**[インストール]**ボタンを表示します。MDMはmacOS User Enrollment登録デバイスのインストール状態を表示できないためです。
    - インストール済みのアプリは[要求されたアプリ]として**[デバイス]** > **[アプリインベントリ]**ページに表示されます。これは、アプリがインストールされたのかされていないのか、macOS User Enrollment登録デバイスがインベントリレポートでIvanti Neurons for MDMサーバーに通知しないためです。
- アプリの配布フィルターでは、User Enrollment登録および自動Device Enrollment登録の属性を必要に応じてカスタム配布に使用できます。

- ユーザーベースのライセンスでは、管理対象Apple IDを使用してApple Apps and Booksアプリをインストールできます。デバイスベースのライセンスではできません。アプリカタログはApple Apps and Booksアプリしか表示しません。
- 許可されていない構成、ポリシー、アクションもあります。以下の手順ですべての構成とポリシーのリストをご覧ください。
    - サポートされていない構成をmacOS User Enrollment登録デバイスに配布しようとしても、配布やデバイスへの適用は行われず、場合によっては [制限 - これは有効な要求タイプではありません] などのメッセージが表示されます。
    - 同様に、サポートされない管理デバイスアクションもIvanti Neurons for MDM UIで通知されます。
    - サポートされないレポートはIvanti Neurons for MDMによって送信されません。

以下は、macOS User Enrollment登録デバイスへの配布がサポートされていない構成とポリシーです。

- パスコード
- トンネル
- Tunnel(オンデマンド)
- VPN構成
- Office 365自動アカウント作成
- macOSカーネル拡張ポリシー
- プライバシー設定
- macOSの制約
- ソフトウェア更新
- AirPrint
- MIクライアントプライバシー
- FileVault 2
- FileVaultリカバリキー
- Firewall (ファイアウォール)
- アプリケーションポリシールール

- 証明書設定
- システムポリシー制御
- システムポリシーマネージド
- macOS AppStoreの制約
- macOSディスク焼き付けの制約
- macOS Finder設定
- macOS対応Mobile@Work
- macOS対応Mobile@Workのスクリプト
- 許可メディアの制御
- タイムサーバー
- 許可されたアプリポリシー

User EnrollmentとDevice Enrollmentの違い

このセクションでは、User EnrollmentとDevice Enrollmentの違いを説明します。

User Enrollmentは、iOS 13.0およびmacOS 10.15からサポートされる最新版を搭載したデバイスに適用されます。iOS 13.0およびmacOS 10.15より前のデバイスは、デバイスユーザーがUser Enrollmentを許可されているかどうかに関係なく「Device Enrollment」と見なされます。

Apple Business ManagerのUser Enrollmentは、ワイプやロック解除に対応しません。そのような機能が実行されないにもかかわらず、ユーザーポータルにはそれらのオプションがあります。

TABLE 1.

User EnrollmentとDevice Enrollmentの比較			
機能	**ユーザ登録**	**MAM**	**デバイス登録**
デバイスの消去とユーザーの個人用アプリの表示			
マネージドから非マネージド、またはその逆への変更			

TABLE 1. (CONT.)

User EnrollmentとDevice Enrollmentの比較			
機能	**ユーザ登録**	**MAM**	**デバイス登録**
デバイスパスコードのクリア、デバイス全体のVPNやWi-Fiプロキシの設定、携帯電話機能の管理			
UDID、シリアル番号、IMEIなどのデバイス識別子の表示			
監視対象制限の適用			(監視対象デバイスのみ)
アプリおよびアカウントのインストールと設定			
MDMによってインストールされたアプリ、メール、連絡先、カレンダー用のPer-App VPNの設定			
マネージドオープンイン、マネージド連絡先、ロック画面上のマネージドデータなど、複数の制限の適用			
企業管理対象アプリ、証明書、プロファイルに関連するデータのクエリー			

Ivanti Neurons for MDM を Apple Business Manager に接続する

このセクションではApple Business ManagerでのUser Enrollmentを有効化する方法を説明します。

前提条件

- ユーザーにはApple Business Managerアカウントが必要です。https://business.apple.com/を参照してください。
- iOSデバイスを管理するにはApple MDM証明書を要求し、インストールする必要があります。

User Enrollmentを有効化するローカルユーザーの作成

このセクションでは、ローカルユーザーとLDAPユーザーの作成と非監視対象AppleデバイスのUser Enrollment設定について説明します。User Enrollmentは、監視対象デバイスやAppleのDevice Enrollmentで登録したデバイスには作用しません。

手動管理(固定)ユーザーグループの作成

これは1回きりの手順です。すでにこのグループを作成している場合は、「User Enrollmentの対象となるユーザーの作成」セクションへ進んでください。

手順

1. **[ユーザー]** > **[ユーザーグループ]** を開きます。
2. 「User Enrollment Group」など、手動管理(固定)ユーザーグループを作成し、User Enrollmentのデバイス登録タイプを持つユーザーを追加します。
3. **[保存]** をクリックします。

デバイス登録タイプ設定の作成

これは1回きりの手順です。すでにこのグループを作成している場合は、「User Enrollmentの対象となるユーザーの作成」セクションへ進んでください。User Enrollment登録デバイスの場合、デフォルトのデバイス所有者の設定は「ユーザー所有」となります。

手順

1. **[ユーザー]** > **[ユーザー設定]** を開きます。
2. [デバイス登録設定] セクションで **[+特定のユーザーグループの設定を追加]** をクリックします。
3. デバイス登録タイプがUser Enrollmentのユーザーに対して、UE登録など新しい設定を作成します。
4. [Apple Enrollment] セクションで **[User Enrollment]** をApple Enrollmentの種類として選択します。
5. **[次へ]** をクリックします。
6. [ユーザー設定配布] ページで、「User Enrollment Group」など新しく作成されたユーザーグループを選択します。
7. **[完了]** をクリックします。

User Enrollmentの対象となるローカルユーザーの作成

前準備として、手動管理ユーザーグループとUser Enrollmentのデバイス登録設定を作成します。

手順

1. **[ユーザー]** を開きます。
2. **[+追加] > [ユーザー1人]** をクリックします。

   新規ユーザーの情報を入力し、「User Enrollment Group」など新しく作成されたユーザーグループに追加します。詳細については、ユーザートピックの*ユーザーの追加*を参照してください。

User Enrollmentを有効化するLDAPユーザーのインポート

前提条件

- 前準備として、LDAPリソースにアクセスするIvanti Neurons for MDM Connectorを設定します。
- **[管理対象Apple ID]** 設定が **[パターン]**(ユーザーのメールアドレス) に設定されていることを確認します。管理対象Apple IDのパターンが他と重複していないことを確認してください。同じ管理対象Apple IDが別のアカウントに存在する場合、管理対象Apple IDでアカウントが更新されません。
- (任意)「appleid」サブドメインを含めて、既存のApple IDとの競合を避けます。
- LDAPからユーザーをインポートし、User Enrollmentに招待することができます。インポートしたLDAPユーザーは、Ivanti Neurons for MDMと同期した管理対象Apple IDを持ちます。これはUser Enrollmentの必須要件です。

手順

1. **[ユーザー]** を開きます。
2. **[+追加] > [LDAPからユーザーを招待]** をクリックします。
3. LDAPサーバーエントリ中の **[ユーザーを選択]** をクリックします。
4. [LDAPユーザーを追加] ページで、ユーザー、グループ、OUの名前を検索フィールドを入力します。
5. 新規ユーザーやグループを追加するには、追加したいエントリの横にある **[+追加]** をクリックします。
6. **[完了]** をクリックします。

User Enrollmentを有効化するAADユーザーのインポート

前準備として、Ivanti Neurons for MDMとMicrosoft Azure Active Directory(AAD) を連携します。

AADユーザーをUser Enrollmentに招待することができます。インポートしたAADユーザーは、Ivanti Neurons for MDMと同期した管理対象Apple IDを持ちます。これはUser Enrollmentの必須要件です。

手順

1. **[管理]** > **[AzureADユーザーソース]** を開きます。
2. 設定を編集します。
3. **[このAADを有効化]** を選択します。
4. [管理対象Apple ID] 設定で、次のいずれかのオプションを選択します。
   - **パターン**
     - **ユーザーのメールアドレス** - Managed Apple IDのパターンは一意となるようにしてください。同じ管理対象Apple IDが別のアカウントに存在する場合、管理対象Apple IDでアカウントが更新されません。
     - または、**[userUPN]** を選択します。
5. (任意)「appleid」サブドメインを含めて、既存のApple IDとの競合を避けます。
6. **[AADからインポートしたユーザーを自動的に招待]** を選択します。AADからIvanti Neurons for MDMにインポートしたユーザーには自動的に登録招待メールが送信されます。
7. **[保存]** をクリックします。

デバイスユーザーがUser Enrollmentを使用して登録する方法

このセクションでは、Apple User Enrollmentに登録するためにデバイスユーザーが実行すべき操作を説明します。

手順

1. 登録したいiOSデバイスで、リンクおよびエンドユーザーを登録リンク(mobileiron.com/goなど)に導くテキストを含む招待メールを開きます。
2. Safariで登録リンクを開きます。

   ログインページが表示されます。デバイスユーザーはローカルユーザーまたはLDAPの認証情報を使用してログインします。

   登録ページにプロファイルがダウンロードされたというメッセージが表示されます。
3. **[設定]** をタップします。[設定] ページが表示されます。
4. **[(会社名)に登録]** をタップします。
5. [User Enrollment] ページが表示されます。

[デバイスを登録] をタップします。たとえば [私のiPhoneを登録] をタップします。

[キャンセルしてプロファイルを削除] をタップすると、再び最初から登録手続きが始まります。

6. 表示されるのは、Appleアカウントまたはフェデレーションアカウントのいずれかのログイン画面です。管理対象Apple IDのパスワードを入力します。(管理対象Apple IDがログインページの一番上に表示されます。)

   サインインしたままにするオプションが表示された場合は選択してください。

   ページに [登録に成功しました] と表示されます。

トラブルシューティングにおけるデバイスログの利用

ユーザー登録デバイスのエラーや問題を解決するには、まずデバイスログを点検します。

手順

1. **[デバイス]** を開きます。
2. デバイスをクリックして [デバイス詳細] ページを表示します。[User Enrollment登録済み] フィールドと [登録済み管理対象Apple ID] フィールドを確認できます。
3. **[ログ]** タブを選択します。
4. [フィルター] 領域で、アクション名 (チェックアウト、デバイス名、Bootstrapトークン設定、Bootstrapトークン取得など)、ステータス、開始日、終了日などのフィルターを使用してデバイスログを絞り込みます。
5. [アクション] カラムで目のアイコンをクリックし、Enrollment IDなどデバイスログの詳細を表示させます。
6. **[OK]** をクリックします。

アカウント主導のUser Enrollment

対象

- iOS 15+搭載のデバイス

iOS 15+搭載のデバイスを対象としたアカウント主導のUser Enrollmentは、個人所有デバイスの業務利用(BYOD)を認める企業向けのオプションです。アカウント主導のUser Enrollmentとは、企業に必要なレベルのセキュリティを備え、ユーザープライバシーの保護を大幅に強化したMDMプロトコルとApple Business ManagerによるUser Enrollmentの修正バージョンです。

前提条件

アカウント主導のUser Enrollmentの要件は以下のとおりです。

- iOS 15+搭載の非監視対象デバイス
- Ivanti Neurons for MDM内のユーザーアカウントが管理対象Apple IDが持っていること(学校または勤務先のAppleアカウント)

発見サービスのセットアップ

企業が企業ドメインを所有している場合、たとえばそのドメインがacme.comの場合は、ユーザーの管理対象Apple IDはusername@acme.comとなります。企業のサービス発見を有効化するには、次のような既知のエンドポイントを提供する必要があります。

GET https://acme.com/.well-known/com.apple.remotemanagement

エンドポイントは、Ivanti Neurons for MDMクラスター登録ベースURLを含んだ次のようなJSONオブジェクトを返します。

/c/i/reg/userenroll.mobileconfig

Ivanti Neurons for MDM URLは、httpではなくhttpsで始まります。

例:

```
{

 "サーバ":[
```

```
  {
   "Version": "mdm-byod",
   "BaseURL": "https://<your polaris cluster>/c/i/reg/userenroll.mobileconfig"
   }
  ]
}
```

詳細については、次のURLにある情報を参照してください。

https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers

デバイスユーザーがアカウント主導のUser Enrollmentを使用して登録する方法

このトピックでは、アカウント手動のUser Enrollmentを登録するためにデバイスユーザーが実行する必要のある操作を説明します。

手順

1. iOSデバイスで、**[設定]** > **[一般]** > **[VPNとデバイス管理]** を開きます。
2. **[勤務先または学校のアカウントでサインインしてください]** を開きます。
3. 勤務先または学校のアカウントのメールアドレスを入力します。メールアドレスが以下の形式であることを確認してください。
   username@<企業ドメイン名>。例: username@acme.com
4. ログインページでは管理対象Apple IDが自動入力され、iRegのフローとなります。Ivanti Neurons for MDMの認証資格情報を必ず入力します。
5. 勤務先または学校のアカウント認証情報を入力し、**[続行]** をクリックします。
6. 2要素認証後にデバイス登録が完了します。

ユーザーライセンス

Ivanti Neurons for MDM のユーザーベースのライセンスにより、登 録 できるユーザーの数 、ユーザーライセンスあたりに許 可 されるデバイスの数 、デバイスへの配 布 用 に構 成 できるコンテンツの量 、および利 用 できる機 能 が定 義 されます。ユーザー数 の上 限 に近 付 くと[管 理] ページに赤 い三 角 形 が表 示 されます。コンテンツの上 限 に近 付 くと、サービスでさらなる追 加 が差 し止 められ、上 限 に近 付 いていることを示 すメッセージが表 示 されます。

計 画 すべきユーザーライセンス数 を判 断 するには、以 下 の点 を考 慮 してください。

- Secure UEMまたはSecure UEM Premiumパッケージで購 入 した場 合 、ユーザーライセンスあたり5台 まで登 録 できます。
- ユーザーが5台 より多 くのデバイスを登 録 すると、追 加 のユーザーライセンスが申 請 されます。
- ユーザーが申 請 できるユーザーライセンス数 に制 限 はありません。
- デバイスが撤 去 されたりワイプされたりすると、ライセンスは取 り消 されます。

例 えば、ユーザー1は、仕 事 の初 日 に仕 事 用 の電 話 を登 録 し、ユーザーライセンスを申 請 します。翌 週 、個 人 用 の電 話 2台 とタブレットを同 じライセンスで登 録 します。タブレットをもう1台 登 録 すると、デバイスが5台 になるため、2つ目 のユーザーライセンスを申 請 します。個 人 用 の電 話 が盗 まれ、そのデバイスをワイプすると、2つ目 のユーザーライセンスは取 り消 されます。

ユーザーのデバイス/ライセンス数 の表 示

手 順 :

1. **[ユーザー]** を開 きます。
2. ユーザーのリンクをクリックします。

左 のペインに、ライセンスの使 用 状 況 を含 むユーザー情 報 が表 示 されます。

ユーザーの管 理

このセクションは以 下 のトピックを含 みます。

- 「タイムアウト情報」ページ162
- 「システム利用分析のオプトアウト」ページ163

Cisco ISE操作へのAPIユーザー追加

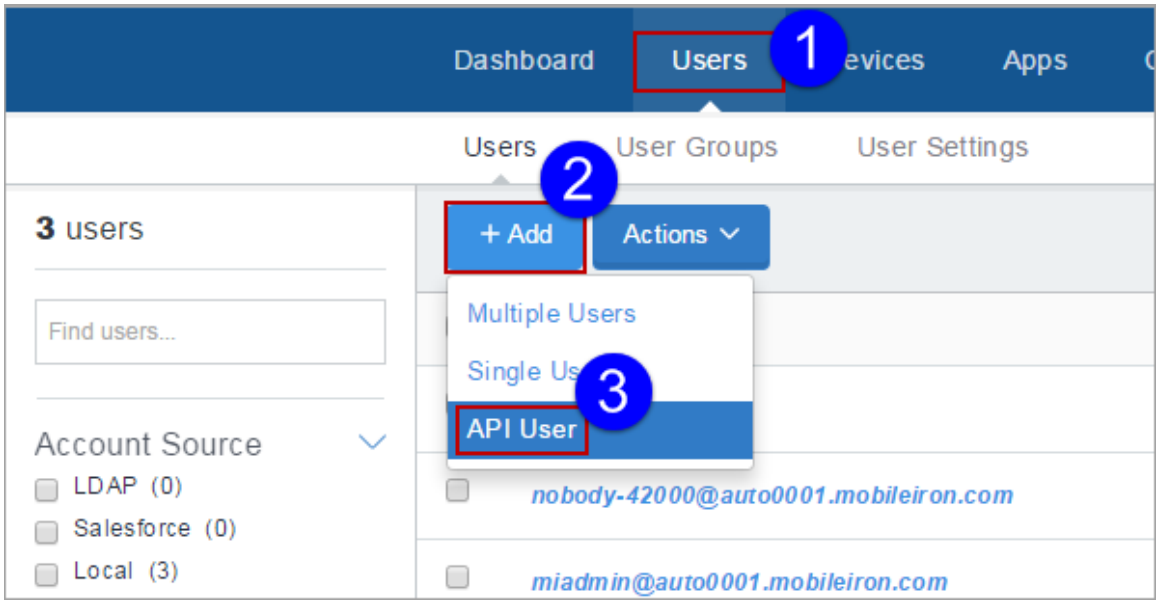
Ivanti Neurons for MDMでCisco ISEがCisco ISE APIと対話できるようにする「Cisco ISE操作」役割を持つAPIユーザーを追加できます。このユーザーを作成した後、このユーザーのCisco ISE内での認証情報を使用して、Ivanti Neurons for MDMに対するAPI呼び出しを認証します。これらのAPI呼び出しにより、Cisco ISEは、デバイス情報の取得、デバイスに対するフル/コーポレートワイプやPINロックなどの操作実行、デバイスへのメッセージ送信を実行できます。

APIユーザーは管理ポータルにログインできません。APIの使用を許可するだけです。

デフォルトでは、テナントのスーパー管理者のみが「Cisco ISE操作」の役割を持ちます。スーパー管理者は、この役割を持つべき他のユーザーをシステム内で明示的に選択し、役割を割り当てる必要があります。その後、[Cisco ISE操作]の役割に割り当てられたユーザーが、システム内でその他の適切なユーザーにこの役割を割り当てます。

手順

1. **[ユーザー]** タブをクリックします。



2. **[追加]** をクリックします。
3. **[APIユーザー]** を選択します。

4. 表示されるフォームにユーザーの情報を入力します：

   - Eメールアドレス
   - 名
   - 性

   > [ユーザー名] フィールドには入力したEメールアドレスが表示されます。ほとんどの場合、このデフォルトは変更しないでください。[ユーザー名編集のタイミング] を参照してください。

5. このユーザーの表示名を変更したい場合は、**[表示名]** フィールド内のデフォルトテキストを編集します。
6. **[パスワード]** と **[パスワードを確認]** フィールドに入力してパスワードを指定します。
7. **[役割を割り当てる]** セクションで選択されている **[API管理Cisco ISE操作]** の役割をそのままにします。
8. **[完了]** をクリックするとユーザーが追加されます。

[ユーザー] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- ユーザー管理

ユーザーへの役割の割り当て

役割を割り当てることで、ユーザーに対してIvanti Neurons for MDMのデータや機能へのアクセス権を付与できます。ユーザーまたはユーザーグループに直接役割を割り当てることができます。役割を**ユーザーグループ**[1]に割り当てると、その役割がグループ内のすべてのユーザーに与えられます。

デフォルトでは、ユーザーに「ユーザー読み取り専用」役割は割り当てられません。Ivanti Neurons for UEMとIvanti Neurons for MDMの両方にアクセスできるテナントの場合、[役割]ページとその関連オプションは非表示になります。

ユーザーがその時点で持っていない権限を割り当てることはできません。ユーザーに割り当てられていない権限と役割は選択肢に表示されません。この場合、エラーメッセージが表示されます。Ivanti Neurons for MDMの管理者またはパートナーの管理者がパートナーの管理者に対して役割を割り当てようとすると、Ivanti Neurons for MDMは、パートナーの管理者はこの操作をサービスプロバイダーポータルで実行しなければならないことを伝えるメッセージを表示します。

役割の詳細は、役割管理をご覧ください。

手順：

1. 次の手順に従います。
   - **[ユーザー] > [ユーザー]** *または*
   - **[ユーザー] > [ユーザーグループ] を開きます。**
2. 1人または複数のユーザーまたはユーザーグループを選択します。
3. **[アクション]** をクリックします。
4. ユーザー詳細ページまたはユーザーグループ詳細ページで **[役割を割り当てる]** をクリックするか、ユーザーリストまたはユーザーグループリストページから **[役割を付加]** を選択します。
5. 以下のうち、1つまたは複数の割り当てたい役割を選択します。
   - システム管理 | スペース共通
   - システム読み取り専用 | スペース共通

[1] a list of users that you want to treat in the same way.

- ユーザー管理 | スペース共通
- ユーザー読み取り専用 | スペース共通
- LDAPユーザーのインポートおよび招待 | スペース共通
- デバイス管理 | スペース特有
- デバイス読み取り専用 | スペース特有
- アプリ& コンテンツ管理 | スペース特有
- アプリ& コンテンツ読み取り専用 | スペース特有
- デバイスアクション | スペース特有
- Cisco ISE操作 | スペース共通
- スケジュールタスクの管理 | スペース共通
- 共通プラットフォームサービス(CPS) | スペース共通
- 低ユーザー影響移行管理 | スペース共通
- カスタムデバイス登録 | スペース共通
- Microsoft Graph編集 | スペース共通
- ワイプを送信/取り消す | スペース共通
- Microsoft Graph表示 | スペース共通
- Accessインテグレーションの管理 | スペース共通

6. **[次へ]** をクリックします。
7. 選択した役割がスペース依存の場合は、スペース依存の役割すべてについてスペースを選択します。

   スペースが1つしかない場合 (デフォルトスペース) は、スペース依存の役割を割り当てる際にスペース指定の手順がスキップされます。

   スペース依存の場合、要約ページにスペース名がデフォルトスペースと表示されます。
8. 割り当てる役割の要約を確認し、**[完了]** をクリックします。

ヘルプデスクのスタッフに基本的なデバイスアクションの使用許可を与える

ヘルプデスクの役割は、通常、スタッフのデータ閲覧を許可することです。しかし、組織によっては基本的なデバイスアクションを含めたい場合もあります。

- 強制チェックイン
- ロック
- ロックの解除
- メッセージを送信
- 撤去
- ワイプ

手順

アクションに権限を与えることができます。

1. **[ユーザー]** > **[ユーザー]** *または* **[ユーザー]** > **[ユーザーグループ]** を開きます。
2. 1人または複数のユーザーまたはユーザーグループを選択します。
3. **[アクション]** をクリックします。
4. ユーザー詳細ページまたはユーザーグループ詳細ページで **[役割を割り当てる]** *を選択するか*、ユーザーリストまたはユーザーグループリストページから **[役割を付加]** を選択します。
5. **[デバイス読み取り専用]** を選択します。
6. **[デバイスアクション]** を選択します。
7. **[完了]** をクリックします。

ユーザーが期待どおりの権限を持つようにするため、デバイスアクションを選択する前に、[デバイス読み取り専用] を選択してください。

ユーザーの役割

ユーザロールによって、Ivanti Neurons for MDM で表示できるページや、実行できる操作が決まります。割り当てることができる役割と、その内容を次の表にまとめます。

役割	説明	スペース特有
システム管理	管理者が、MDM認証やアプリカタログ設定などのテナントレベルの設定を管理できます。	いいえ
読み取り専用システム	管理者が、MDM認証やアプリカタログ設定などのテナントレベルの設定を閲覧できます。	いいえ
ユーザー管理	管理者が、ユーザーの追加や削除、役割の指定、ユーザーグループへのユーザー追加を実行できます。	いいえ
ユーザー読み取り専用	管理者が、ユーザーおよびユーザーグループのほか、アプリカタログとコンテンツカタログを閲覧できます。	いいえ
デバイス管理	管理者が、デバイスグループ、構成、ポリシーを管理し、すべてのデバイスアクションを実行できます。	はい
読み取り専用デバイス	管理者が、デバイスグループ、構成、ポリシーを閲覧できます。	はい
アプリ& コンテンツ管理	管理者が、アプリやコンテンツの追加、配布、削除を実行できます。	はい
アプリ& 読み取り専用コンテンツ	AppConnectタスクを含むユーザー、アプリ、コンテンツのデータを表示	はい

役割	説明	スペース特有
デバイスアクション	管理者が開始できるデバイスアクションの例： • 強制チェックイン • ロック • ロックの解除 • メッセージを送信 • 撤去 • ワイプ [デバイスアクション]を選択する前に、[デバイス読み取り専用]を選択してください。選択しない場合、ユーザーに必要な許可が与えられません。	はい
LDAPユーザーのインポートおよび招待	管理者が、LDAPユーザーを登録し、デバイス登録を促す招待状を送信できます。	いいえ
Cisco ISE操作	管理者がCisco ISE統合に必要なAPIを起動できます。	いいえ
スケジュールタスクの管理	管理者がさまざまな管理業務のスケジュールタスクを作成および管理できます。	いいえ
共通プラットフォームサービス(CPS)	管理者が共通プラットフォームサービスを利用できます。	いいえ
低ユーザー影響移行管理	管理者が低ユーザー影響移行の設定を管理できます。	いいえ
カスタムデバイス登録	管理者がカスタムデバイス登録を使用してデバイスを登録できます。	いいえ
Microsoft Graphを編集	Office 365アプリを保護するMicrosoft GraphのAPI設定を管理者が編集できます。	いいえ

役割	説明	スペース特有
Microsoft Graphを表示	Office 365アプリを保護するMicrosoft GraphのAPI設定を管理者が表示できます。	いいえ
ワイプを送信/取り消す	デバイスへのワイプコマンド送信、または発行したワイプコマンドの実行前の取り消しを管理者が実行できます。	いいえ
Accessインテグレーションの管理	管理者がAccessインテグレーションを管理できます。	いいえ

詳細は役割の割り当てを参照してください。

ユーザーの検索とフィルタリング

このセクションは以下のトピックを含みます。

ユーザーの検索

多くのユーザーを追加した後には、フィルタや検索を利用するとユーザーエントリを迅速に見つけるのに役立ちます。

手順

1. **[ユーザー]** を開きます。
2. 検索ボックスに文字を入力します。

ユーザー詳細検索の使用

詳細検索のオプションでは、管理者がルールに基づいてユーザーを検索し、特定の基準を満たすデバイスを識別および表示します。[ANY (OR)] または [ALL (AND)] オプションを使用すれば、ルールオプションをネストでまとめることができます。ルールに一致するユーザーは、セクションの下に表示されます。ルールは、次の演算子を使用して作成できます。

- 開始：
- 終了：
- 含む
- 次を含みません：
- 次で開始しません：
- 次で終了しません：
- は次より以下：

- は次より大きい：
- は範囲内です
- は次と等しい：
- は次と等しくない：

Ivanti Neurons for MDM 92以降、ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM管理者は重複するユーザーグループ数と、重複するグループを識別する対応するGUID番号を表示します。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

手順

1. [ユーザー] ページから **[詳細検索]** リンクをクリックします。
2. ユーザーが少なくとも1つのルールを満たす必要がある場合は **[いずれか]**、ユーザーがすべてのルールを満たす必要がある場合は **[すべて]** をクリックします。
3. ユーザーグループ、カスタムユーザー属性、カスタムLDAP属性など、検索基準を定義するルールを作成します。
4. (任意) [+] をクリックし、必要に応じて他のルールを作成します。
5. (任意) **[保存]** をクリックしてクエリを保存します。
6. **[検索]** をクリックします。検索基準に一致するユーザーのリストがページに表示されます。

ユーザーに対する検索クエリの読み込み

手順

1. [ユーザー] ページから **[詳細検索]** リンクをクリックします。
2. フォルダーアイコンをクリックします。**[詳細検索]** ウィンドウが表示されます。**[クエリを読み込む]** セクションに、作成された検索クエリのリストが表示されます。このセクションには以下の情報が表示されます。
   - **クエリ名** - 読み込まれたクエリの名前。
   - **クエリの内容** - 検索クエリを定義するルールの内容を表示します。
   - **アクション** - クエリに実行するアクションを選択します。

3. **[アクション]** カラムの **[クエリを読み込む]** をクリックすると、読み込まれたクエリに定義された基準に一致するユーザーのリストが表示されます。
   読み込んだクエリを削除するには、削除アイコンをクリックします。

ユーザーのフィルタリング

フィルタのサイドナビゲーションバーには、さまざまなセクションが表示され、ユーザの一覧全体から特定のユーザを検索できます。[フィルタの管理] ウィザードには、すべてのセクションが表示され、フィルタのナビゲーションバーに表示するセクションを選択できます。

手順

1. **[ユーザー]** を開きます。

2. [フィルタの管理] ウィザードの一覧にあるセクションの該当するチェックボックスをクリックします。次のセクションから検索できます。

   - 管理者
   - Googleステータス
   - 招待ステータス
     - 完了(ユーザーが招待状を受け取っており、返答している。)
     - 期限切れ(ユーザーが期日までに返答しなかった。)
     - 未招待(このユーザーをまだ招待していない。)
     - 保留(ユーザーの返答を保留中。)
   - パスワードの有効期限
     - 期限あり(パスワードの有効期限オプションが有限の日数に設定されているユーザー。)
     - 無期限(パスワードの有効期限オプションが無期限に設定されているユーザー。)
   - ユーザーグループ(希望の**ユーザーグループ**[1]を選択します。)
   - ユーザソース
     - LDAP
     - AAD
     - 登録者
     - Salesforce
     - ローカル

[1] a list of users that you want to treat in the same way.

- 同期
  - 直接同期 - LDAPサーバーから直接同期されたユーザーをリストする
  - 同期していません - LDAP サーバーから削除されたユーザーをリストする
  - 間接同期 - LDAPサーバーから間接的に同期されたユーザーをリストする
  - 非該当

3. (任意) **[既定値の復元]** をクリックすると、選択内容が既定のフィルタに復元されます。フィルタナビゲーションバーには、選択したセクションが表示されます。[フィルタの管理] ウィザードですべてのチェックボックスをオフにした場合は、フィルタのサイドナビゲーションバーにすべてのセクションが表示されます。
4. [フィルタの管理] ウィザードの外の任意の場所をクリックすると、ウィザードが終了します。
5. フィルタのサイドナビゲーションバーを閉じるには x アイコンをクリックします。サイドナビゲーションバーをもう一度開くには、**[フィルタ]** をクリックします。

ユーザーグループへのユーザーの割り当て

このセクションは以下のトピックを含みます。

- 「[ユーザー] ページからのユーザー割り当て」下
- 「[ユーザーグループ] ページからのユーザーの割り当て」下

ユーザーグループへのユーザーの割り当ては、以下のようなタスクの繰り返しを回数を最小限に抑えるために有効な方法です。

- アプリの配信
- 役割の割り当て

[ユーザー] ページからのユーザー割り当て

1. **[ユーザー]** を開きます。
2. 作業対象のユーザーを選択します。
3. **[アクション]** をクリックします。
4. **[グループへ割り当てる]** を選択します。
5. グループを選択するか、**[新規作成]** をクリックして新規グループを開始します。
6. **[保存]** をクリックします。

[ユーザーグループ] ページからのユーザーの割り当て

1. **[ユーザー]** > **[ユーザーグループ]** へ進みます。
2. 作業対象のユーザーグループを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[ユーザーの割り当て]** を選択します。

5. 各 ユーザーのメールアドレスを入 力します。

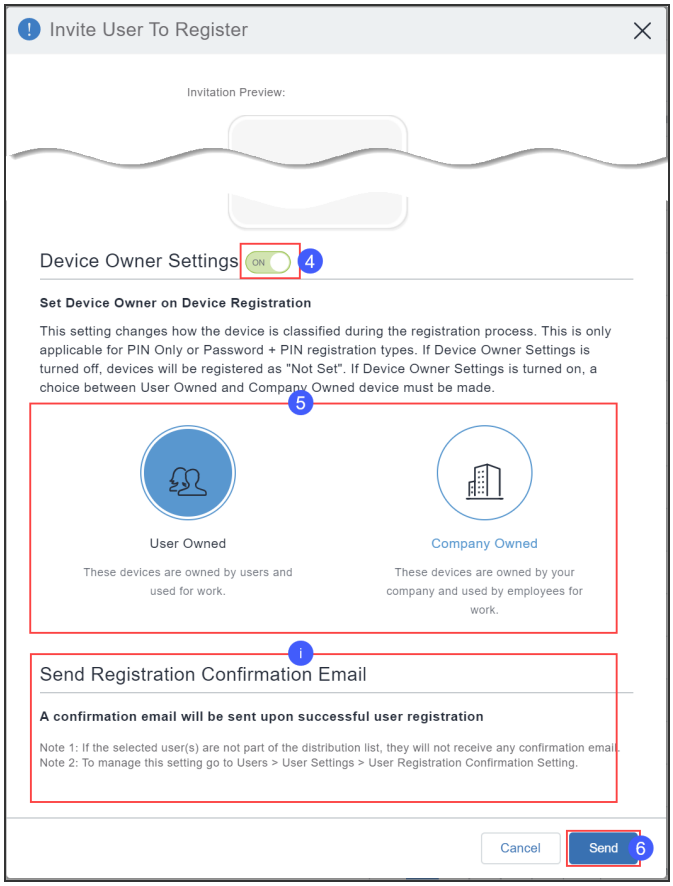
6. **[ユーザーの割り当 て]** をクリックします。

ユーザーの招待

ユーザーの追加時に、ユーザーにデバイス登録の招待を行う機会があります。実際、このオプションはデフォルトで選択されています。招待を受けたユーザーは、登録に必要な情報を含むメールメッセージを受け取ります。**[ユーザー]** > **[ユーザー]** ページからユーザーを招待(または再招待)することもできます。

手順

1. **[ユーザー]** を開きます。
2. 招待するユーザーを選択します。
3. **[アクション]** > **[招待の送信]** を選択します。招待状のプレビューが表示され、デバイスの所有権を **[ユーザー所有]** または **[会社所有]** に設定するためのオプションが示されます。



4. または **[デバイス所有者設定]** をオンにします。

5. **[ユーザー所有]** または **[会社所有]** をクリックします。この設定は登録プロセス中にデバイスの分類を変更します。これはPIN専用またはパスワード + PIN登録タイプにのみ適用されます。**[デバイス所有者設定]** がオフの場合、デバイスは「未設定」として登録されます。監視されたデバイスの場合、デバイス所有者設定は「会社所有」です。

6. **[送信]** をクリックします。PIN に基づくデバイス登録が実行された場合、ユーザの登録された電子メールアドレスに PIN が送信されます。QR コードの登録が設定されている場合は、QR コードが送信されます。

7. **[OK]** をクリックします。

> 登録確認メール機能が「登録確認メールの構成と使用」ページ27に記載されたとおりに有効化されている場合、登録が正常に完了すると、ユーザーが登録確認メールを受信するというリマインダーも表示されます。メールを送信するには、ユーザを「ユーザー設定」ページ89 の「ユーザー登録確認メールの構成」ページ100 にある配布リストに入れる必要があります。

詳細はLDAPユーザーのインポートを参照してください。

ユーザーの有効化と無効化

このセクションは以下のトピックを含みます。

- 「ローカルユーザーの有効化と無効化」下
- 「LDAPユーザーの有効化と無効化」下

ローカルユーザーとLDAPユーザーは有効または無効の状態にすることが可能です。この状態に基づき、ユーザー有効条件を使用してカスタムポリシーを作成し、条件に応じたアクションをルールビルダーで設定できます。たとえば、無効なローカル/LDAPユーザーに帰属するデバイスを撤去するカスタムポリシールールを設定できます。

ローカルユーザーの有効化と無効化

ローカルユーザーを作成すると、デフォルトで有効な状態になります。

手順

1. **[ユーザー]** を開きます。
2. ローカルユーザーの表示名をクリックします。
3. **[編集]** をクリックします。**[認証が必要]** ウィンドウが表示されます。
4. 管理者パスワードを入力し、**[認証]** をクリックします。

   > パスワードの入力に何度か失敗し、「パスワードの複雑さ設定」の「ログイン失敗の閾値」を超えると、アカウントはロックされ、現在のセッションからログアウトされます。

5. ローカルユーザーを有効または無効にするには **[有効化]** オプションを選択または選択解除します。
6. **[保存]** をクリックします。

LDAPユーザーの有効化と無効化

LDAPユーザーは、Microsoft Active Directoryに対してのみ有効化または無効化が可能です。Microsoft Active Directoryでユーザーアカウントのプロパティを開き、**[アカウント]** タブをクリックした後、**[アカウント]** オプションダイアログボックスのチェックボックスを選択またはクリアすると、**UserAccountControl**属性に数値が割り当てられます。属性に指定された値が、有効になったオプションをWindowsに伝えます。UserAccountControl属性に値を割り当てると、Ivanti Neurons for MDMとのLDAP同期の後、ユーザーステータスが反映されます。

指定可能な値は以下のとおりです。

- 512 - 有効。
- 514 - 無効。
- 66048 - 有効、パスワード無期限。
- 66050 - 無効、パスワード無期限。

ユーザーアカウントの表示

手順

1. **[スタート]** をクリックします
2. **[プログラム]** を開きます。
3. **[管理ツール]** を開きます。
4. **[Active Directory ユーザーとコンピューター]** をクリックします。

詳細については、https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-proを参照してください。

Ldp.exeツールまたはAdsiedit.mscスナップインを使用して、属性を表示および編集できます。熟練した管理者だけが、これらのツールでActive Directoryを編集してください。どちらのツールも、オリジナルのWindowsインストールメディアからサポートツールをインストールすると利用可能です。

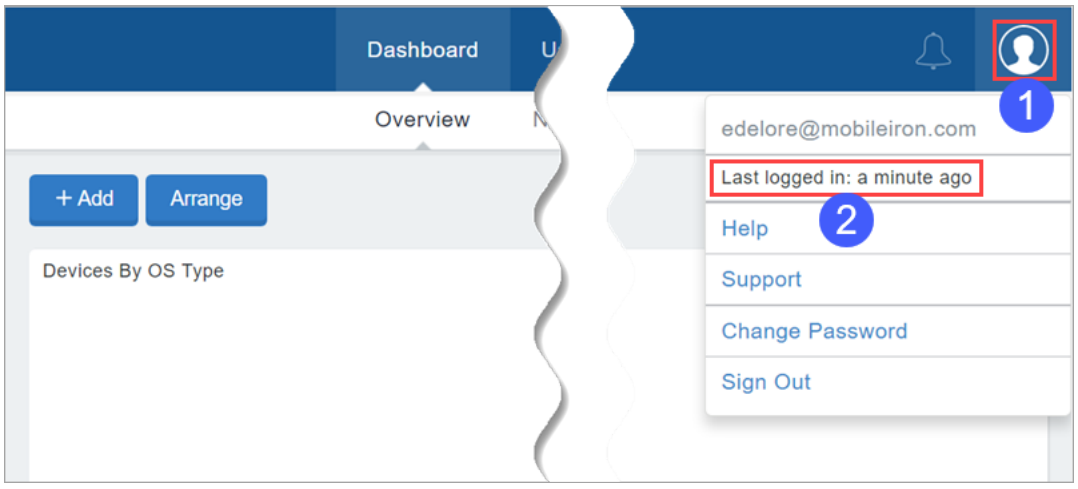
複数の管理者ログインの管理

複数のIvanti Neurons for MDM管理ポータルセッションがサポートされていますので、管理者は同時にさまざまなポータルページを表示できます。管理者は、複数のログインを記録するため、自分の最後のログイン日を閲覧できます。

前回の管理者ログインの表示

手順

1. アカウントアイコンをクリックします。



2. **[最後のログイン:]** が表示されます。

パスワードの変更

このセクションは以下のトピックを含みます。

システム管理の役割を持つユーザーがいる場合は、スーパーユーザーまたは現在ログインしているユーザーのみに **[パスワードの変更]** オプションが表示されます。

Ivanti Neurons for MDMのパスワードを変更することができます。アクセス権があれば、他のユーザーのパスワードも変更できます。

手順

1. アカウントアイコン(右上)をクリックします。

2. プルダウンメニューから **[パスワードの変更]** を選択します。
3. 現在のパスワードを入力します。
4. 新しいパスワードを入力します。
5. 新しいパスワードを再度入力します。
6. パスワードを無期限に設定するには、**[パスワードを無期限に設定]** を選択します。

   パスワードを無期限に設定すると、[ユーザー] > [ユーザー設定] > [パスワードの複雑さ] の設定で定義した **[パスワード有効期限]** が上書きされます。

7. **[完了]** をクリックします。

> ローカルアカウントパスワードを期限ありにリセットするには、**[パスワードを無期限に設定]** を選択解除します。このオプションを選択解除すると、ユーザーに適用されていた以前のパスワード有効期限がポップアップウィンドウに示されます。

[ユーザー] タブからのパスワード変更

手順

1. **[ユーザー]** を開きます。
2. ユーザーの表示名をクリックします。
3. **[編集]**(左上)をクリックします。**[認証が必要]** ウィンドウが開きます。管理者(ローカルユーザーまたはLDAPユーザー)はユーザーを編集する前に管理者パスワードの入力と認証を求められます。
4. 管理者パスワードを入力し、**[認証]** をクリックします。

> パスワードの入力に何度か失敗し、「パスワードの複雑さ設定」の「ログイン失敗の閾値」を超えると、アカウントはロックされ、現在のセッションからログアウトされます。

5. **[現在のパスワード]** フィールドに現在のパスワードを入力します。

> このフィールドは、他のユーザーのパスワードを変更する場合は表示されません。

6. **[パスワードの変更]** フィールドに新しいパスワードを入力します。
7. 新しいパスワードを確認します。
8. **[保存]**(左上)をクリックします。

パスワードを無期限にする

1. **[ユーザー]** を開きます。
2. 1人以上のユーザーを選択します。
3. **[アクション]** をクリックします。

4. **[パスワード無期限を割り当てる]** を選択します。**[ローカルアカウントパスワードを無期限に設定]** ウィンドウが表示されます。

5. **[Submit]** をクリックします。

パスワード無期限設定の削除

1. **[ユーザー]** を開きます。

2. 1人以上のユーザーを選択します。

3. **[アクション]** をクリックします。

4. **[パスワード無期限を削除]** を選択します。**[ローカルアカウントパスワード無期限を削除]** ウィンドウが表示されます。

5. **[送信]** をクリックします。この設定を削除すると、ユーザーには以前のパスワード有効期限が適用されます。

テナント管理者のユーザー名の変更

新しいテナント管理者を容易に導入できるよう、テナント管理者のユーザー名を変更することができます。テナント管理者を削除することはできないため、テナント管理者を別のユーザー名に変えるという方法がとられます。

この機能は、次のようなシナリオの際に便利です。

すべての役割を持つユーザーがテナント管理者のユーザー名を変更する

1. テナント管理者が退職します。
2. ユーザー管理者の役割を持つユーザーがテナント管理者のユーザー名、メールアドレス、名、姓、およびパスワードを新しいテナント管理者用に変更します。

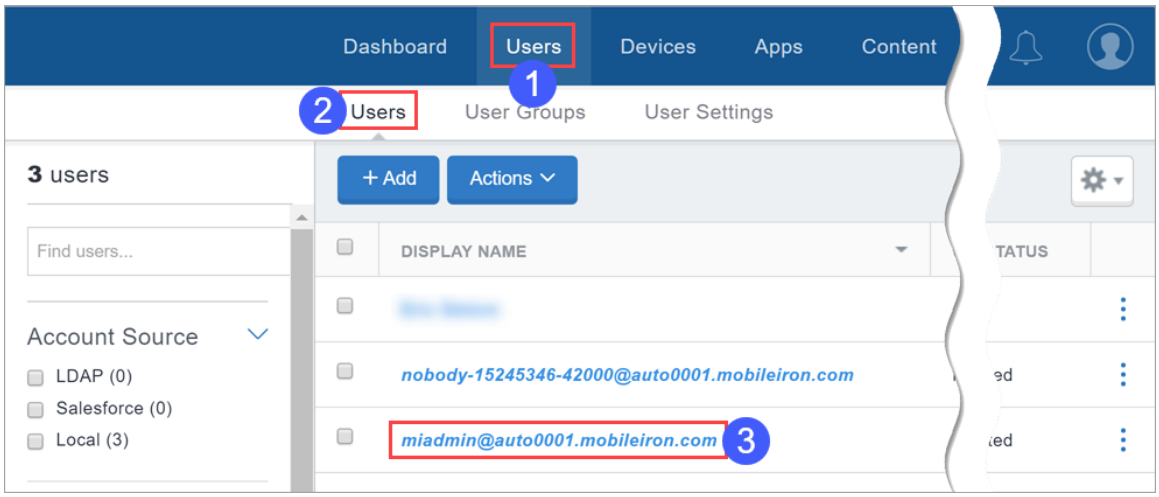
   役割の割り当てとパスワードの変更についての詳細は、役割の割り当てとパスワードの変更を参照してください。

退職する前に、テナント管理者がユーザー名を新しいテナント管理者に変更する

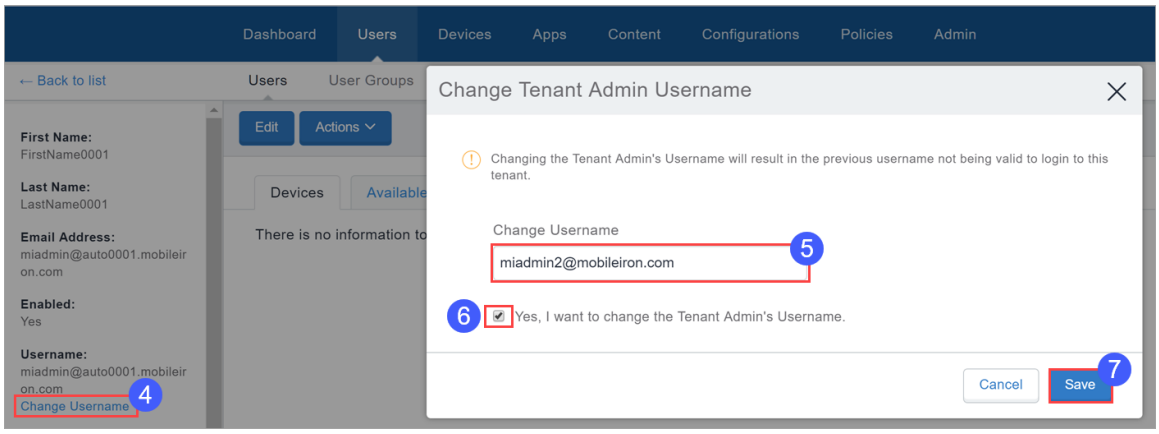
1. 退職するテナント管理者は、退職する前にユーザー名とパスワードを変更します。
2. 退職するテナント管理者は、この情報を新しいテナント管理者に引き継ぎます。

テナント管理者のユーザー名の変更

1. **[ユーザー]** を選択します。



2. **[ユーザー]** サブタブを選択します。
3. テナント管理者の表示名をクリックします。



4. **[ユーザー名を変更]** をクリックします。
5. 新しいユーザー名を入力します。
6. **[はい、テナント管理者のユーザー名を変更します]** の隣にあるチェックボックスをクリックしてチェックマークを付けます。
7. **[保存]** をクリックします。

メッセージの送信

このセクションは以下のトピックを含みます。

- 「ユーザーへのメッセージの送信」下
- 「デバイスへのメッセージの送信」次のページ

既知のユーザーならば誰にでもメッセージを送信することができます。メッセージは、Eメールまたは**プッシュ通知**[1]となります。デバイスを登録しているユーザーのみ、Push通知を受信できます。

前提条件

- iOSデバイスの場合、Goクライアントがインストールされていることを確認します。
- macOSデバイスの場合、Mobile@Workクライアントがインストールされていることを確認します。

ユーザーへのメッセージの送信

1. **[ユーザー]** > **[ユーザー]** へ進みます。
2. メッセージを送信するユーザーを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[メッセージを送信]** を選択します。
5. Eメールを送信したくない場合は、**[Eメールを送信する]** チェックボックスを選択解除します。
6. Eメールを信する場合は、件名とメッセージ本文を入力します。
7. Push通知を送信する場合は、**[Push通知を送信する]** チェックボックスを選択し、メッセージ本文を入力します。
8. **[送信]** をクリックします。

[1]a message or alert that is sent to the device.

デバイスへのメッセージの送信

1. **[デバイス]** > **[デバイス]** に進みます。
2. メッセージを送信するデバイスを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[メッセージを送信]** を選択します。
5. デバイス名のリンクをクリックして [デバイス詳細] ページを開き、**[メッセージを送信]**  アイコンをクリックすることも可能です。
6. Eメールを送信したくない場合は、**[Eメールを送信する]** チェックボックスを選択解除します。
7. Eメールを信する場合は、件名とメッセージ本文を入力します。
8. Push通知を送信する場合は、**[Push通知を送信する]** チェックボックスを選択し、メッセージ本文を入力します。

   プッシュ通知メッセージにはユーザーがアクセス可能なURLも含めることができます。

9. **[送信]** をクリックします。
   プッシュ通知を送信すると、ユーザーのデバイス画面のツールバーにベルのアイコンが表示されます。ユーザーがベルのアイコンをタップすると、受信した通知の履歴が表示され、操作を実行したり、通知を削除したりできます。

ユーザーグループからのユーザーの削 除

このセクションは以 下 のトピックを含 みます。

- 「[ユーザー] ページからのユーザーの削 除 」 下
- 「[ユーザーグループ] ページからのユーザーの削 除 」 下

ユーザーグループからユーザーを削 除 すると:

- そのグループに割り当 てられているすべての役 割 がユーザーから削 除 されます
- そのグループに割り当 てられているすべてのアプリが利 用 ユーザーの**アプリカタログ**[1]で利 用 できなくなります
- 削 除 可 能なものとして構 成されているアプリは、ユーザーのデバイスから削 除 されます

[ユーザー] ページからのユーザーの削 除

1. 作 業 対 象 のユーザーを選 択します。
2. **[アクション]**(右 上) をクリックします。
3. **[グループから削 除]** を選 択します。
4. グループを選 択します。
5. **[削 除]** をクリックします。

[ユーザーグループ] ページからのユーザーの削 除

1. 詳 細を表 示したいユーザーグループをクリックします。
2. **[編 集]**(右 上) をクリックします。

[1]a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

3. 削除したいユーザーの隣にある **[削除]** リンクをクリックします。
4. **[保存]**(右上)をクリックします。

ユーザーの削除

このセクションは以下のトピックを含みます。

- 「ローカルユーザーを削除した場合の影響」下
- 「LDAPユーザーはどうですか？」下

手順

1. **[ユーザ]** > **[ユーザ]** へ進みます。
2. ユーザーのエントリを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[削除]** を選択します。

Ivanti Neurons for MDM の管理者またはパートナーの管理者がパートナーの管理者を削除しようとすると、Ivanti Neurons for MDMは、パートナーの管理者はこの操作をサービスプロバイダーポータルで実行しなければならないことを伝えるメッセージを表示します。

ローカルユーザーを削除した場合の影響

- 削除したユーザーに関するすべての情報は、システムから削除されます。
- ユーザーに関連付けられているデバイスは撤去されます。
- ユーザーがアップロードしたコンテンツは残ります。
- 削除されたユーザーのアカウントでのデバイス登録は許可されません。

LDAPユーザーはどうですか?

- LDAPサーバーが無効になっている場合、LDAPユーザーを永久に削除することはできません。LDAPデータの次の同期時に削除されたLDAPユーザーが復元されます。
- LDAPサーバーやグループが削除された場合、LDAPユーザーはローカルユーザーとなり、削除可能となります。

- ユーザーがLDAPから削除された場合、そのユーザーはCloudからは削除されません。同期ステータスは「NO_SYNC」に切り替わりますが、そのユーザーが削除されることはありません。

ユーザーのエクスポート

管理者はIvanti Neurons for MDMからユーザーの一覧をエクスポートできます。

ユーザーデバイス登録のPINをCSVファイルにエクスポートした場合、PINは、セキュリティ上の理由から実際のPINではなく「****」と表示されます。

手順

1. **[ユーザー]** > **[ユーザー]** へ進みます。
2. リストから1人以上のユーザーを選択します。
3. **[CSV にエクスポート]** をクリックします。

ポップアップメッセージが表示され、レポートのエクスポートの処理には少し時間がかかることが通知されます。要求を送信した後、要求が完了するまで待ってから、次の要求を送信する必要があります。レポートの準備が完了すると、生成されたレポートをダウンロードまたは削除するよう促すメッセージが表示されます。レポートをダウンロードするためのリンクが記載された電子メールも送信されます。

[カスタム ユーザ] および **[LDAP]** 属性詳細は、他の詳細情報とともに CSV ファイルにエクスポートすることもできます。

ユーザーを追加した際のフィールド値に+、-、=、@のいずれかの文字が含まれていると、エクスポートしたCSVファイル内のユーザーデータには、当該フィールドの先頭に自動的に一重引用符 (') が挿入され、パイプ(|) 記号がバックスラッシュ(\ )とともに追加されます。これは、Excelのインジェクションの脆弱性を防止するために行われます。

ユーザーへのカスタム属性の割り当て

部署などのカスタムユーザー属性を1人以上のユーザーに割り当てることができます。各属性には対応の値があり、構成やユーザーグループの作成などのタスクに利用できます。カスタム属性を1人以上のユーザに割り当てることができます。

手順

1. 必要に応じて新しいカスタム属性を作成するには **[管理]** > **[同期]** > **[属性]** を開きます。
2. **[ユーザー]** を開きます。
3. 1人以上のユーザーを選択します。
4. **[アクション]** をクリックします。
5. **[カスタム属性を割り当てる]** を選択します。
6. 以下のオプションから1つ選択してください：
   - 既存の値があってもすべての属性の割り当て(上書き)を強制します。
   - 値が空の場合のみ上書きし、属性に既存の値があればスキップします。
7. 割り当てたい属性を選択し、その値を入力します(値を空にすることは許可されていません)。
8. **[割り当てる]** をクリックします。

関連トピック：

- 「属性」ページ1044
- 「変数」ページ471

ユーザーからのカスタム属性の削除

1人以上のユーザーからカスタム属性を削除できます。

この操作は元に戻すことができないため、慎重に進めてください。

手順

1. **[ユーザー]** を開きます。
2. 1人以上のユーザーを選択します。
3. **[アクション]** をクリックします。
4. **[カスタム属性を削除]** を選択します。
5. 削除する属性を選択します。
6. **[削除]** をクリックします。

関連トピック:

- 「属性」ページ1044
- 「変数」ページ471

ユーザーロケールの変更

デフォルトでは、ユーザーロケールはテナントのロケールに設定されています。必要であれば、単一ユーザーのロケールを変更できます。

手順

1. **[ユーザー]** を開きます。
2. ユーザーの表示名をクリックします。
3. **[編集]** をクリックします。**[認証が必要]** ウィンドウが表示されます。
4. 管理者パスワードを入力し、**[認証]** をクリックします。

   > パスワードの入力に何度か失敗し、「パスワードの複雑さ設定」の「ログイン失敗の閾値」を超えると、アカウントはロックされ、現在のセッションからログアウトされます。

5. [ロケール] フィールドで **[変更]** をクリックします。
6. **[ユーザーロケールを変更]** ウィンドウで、**[ユーザーロケールの変更先:]** ドロップダウンリストから必要なロケールを選択します。
7. **[完了]** をクリックします。
8. **[保存]** をクリックします。

ユーザー名の編集

ユーザーの追加時にEメールアドレスとして入力したテキストが自動的にユーザー名となります。大抵の場合、次のような理由からこのデフォルトのユーザー名をそのままにしておくことをお勧めします。

- Eメール形式のユーザー名が必要だから。
- **構成**[1]においてユーザー名変数を使用するのに便利であり、メールアドレスも使用できるから。

ユーザー名を編集する稀なケースとしては、既存のユーザー名と競合した場合が挙げられます。ユーザー名はデバイス管理システム全体を通じて一意でなければならないからです。たとえば、組織内の2つの部署がデバイス管理システムにサインアップした場合などには、競合が発生する可能性があります。

ユーザー名の競合が発生した場合

ユーザー名の競合によりユーザーを追加できない場合は、Eメールアドレス形式で別のユーザー名を入力します。Eメールアドレスは、実際のEメールアカウントに対応していなくて構いません。たとえば、次のEメールアドレスを変更できます。

ksmith@mycompany.com

を

ksmith21@mycompany.comに変更できます。

ユーザー名を編集した場合、変数としてそのユーザー名を含む構成が、このユーザーには機能しなくなります。代わりに、Eメールアドレス変数を使用した別の構成を作成してください。

[1]collections of settings that you send to devices.

位置情報データ収集の免除

このセクションは以下のトピックを含みます。

- 「iOSデバイスの場合」下
- 「Androidデバイスの場合」下

プライバシー構成を適用して位置情報データの収集を有効にしている場合、デバイスユーザーはこの構成を上書きできます。

iOSデバイスの場合

iOSデバイスユーザーは、次の設定で位置情報サービスをオフにすることで、デバイス管理システムに位置情報データが送信されるのを防止できます。

[設定] > [プライバシー] > [位置情報サービス]

Androidデバイスの場合

Androidデバイスユーザーは、位置情報設定をオフにすることで、位置情報データの収集を防止できます。この設定の場所は、メーカーによって異なります。Androidデバイスユーザーにも、位置情報データの要求を受け入れるようプロンプトが表示されます。

タイムアウト情報

管理ポータルの無活動タイムアウトは5～15分、タイムアウトは24時間です。

手順

1. **[ユーザー]** > **[ユーザー設定]** を開きます。
2. デフォルトの **[パスワードの複雑さ]** 設定を編集します。
3. [パスワードポリシー] セクションで **[無活動タイムアウト]** スライダーを動かし、管理ポータルまたはセルフサービスポータルのセッション時間が非アクティブになるまでのユーザーの無活動時間を指定します。範囲は5～15(分)です。
4. **[完了]** をクリックします。

システム利用分析のオプトアウト

匿名の診断/利用データは製品改良の目的で収集されます。

利用データの独占権を保持する場合は、システム利用分析の送信をオプトアウトできます。

手順

1. Ivanti Neurons for MDM管理ポータルのページ最下部にある **[利用データ]** リンクをクリックします。**[利用データ]** ウィンドウが表示されます。
2. **[診断/利用データを送信]** チェックボックスを選択解除します。
3. **[保存]** をクリックします。

デバイス

このセクションは以 下 のトピックを含 みます。

デバイスの基本

このセクションは以下のトピックを含みます。

[デバイス] ページの各エントリは、Ivanti Neurons for MDM で登録されたモバイルデバイスを示すほか、デバイスに関する重要な情報を掲載しています。デバイスリストのページには、デバイスと以下の情報が表示されます。

- 名前
- Eメールアドレス
- 電話番号
- OS
- デバイスの種類
- ステータス
- 最新のチェックイン
- 違反回数
- スペース
- 法的所有者(共有iPadの場合)

Wi-Fi IPアドレスはIvanti Neurons for MDMサーバーに報告されます。IPアドレスの変更はチェックインごとに報告されます。GDPR対応のIPアドレスは、デバイスリストとデバイス詳細のページにオプションとして表示されます。この機能を使用するには、iOS対応Go 5.5以降およびAndroid対応Go 72以降(Ivanti Neurons for MDMが対応する最新版まで)を通じてデバイスを登録する必要があります。

新しいGDPRフィールド(IPアドレス、eSIM IDなど)がIvanti Neurons for MDMリリースで追加され、新しいフィールドを非表示にしたい場合、すでにGDPRを構成済みの管理者はGDPRプロファイルを編集する必要があります。

デバイスリストをスプレッドシート形式(CSV)にエクスポートすると、装置識別子(EID)がOS属性として表示されます。EIDとモバイルEID(MEID)(存在する場合)は、それぞれ最初にEID文字列またはMEID文字列が付いています。

Ivanti Neurons for MDMサーバーは、同じデバイスが異なるクライアント識別子で異なる複数のテナントに登録されているケースを処理できません。サーバーは、同じデバイスが異なるクライアント識別子で同じテナントに登録されたインスタンスのみ処理できます。

デバイスの管理

手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. **[デバイス]**を開きます。
3. 1つまたは複数のデバイスを選択します。
4. **[アクション]**ドロップダウンリストからアクションを選択します。

次の表は[デバイス]ページから使用可能なフィールドの一覧です。

カテゴリ	アクション
共通	• グループへ追加 • AppConnectのロック解除 • カスタム属性を割り当てる • ユーザーに割り当てる • リモートデスクトップを無効化 • リモートデスクトップを有効化 • Bluetoothを有効化/無効化 • チェックインの強制 • ロック • カスタム属性を削除 • 再起動/シャットダウン • デバイスコンプライアンスステータスの同期 • デバイスの撤去 • メッセージを送信 • 所有者を設定 • ロック解除 • ワイプ
iOS	• 法的所有者に割り当てる(共有iPadのみ) • iOSシステムアプリを再インストール • タイムゾーンを設定
macOS	• macOS自動管理者パスワードを設定 • ファームウェアパスワードの設定/変更 • リカバリロックを設定/変更

カテゴリ	アクション
[Android]	• キオスクモードを開始 • キオスクモードの終了
Windows 10	PINのリセット(モバイルデバイスのみ)

デバイスでアクションを実行する

[アクション] メニュー (省略記号ボタン) では、選択したデバイスでさまざまなアクションを実行できます。

手順

1. デバイス名をクリックします。デバイス詳細ページが開きます。
2. [アクション](三点)メニューをクリックし、以下のいずれかのデバイスアクションを実行します。
   - **デバイス名の変更**
   - **デバイスを削除**
   - **グループメンバーを編集**
   - **Bluetoothを有効化/無効化**
   - **Ivanti Bridgeを使用したスクリプトとアクション**
   - **Ivanti Bridgeログのプル**
   - **所有権を放棄**
   - **デバッグログをリクエスト**
   - **デバイスを再起動/シャットダウン**
   - **撤去**
   - **所有者を設定**
   - **リカバリロックを設定/変更**
   - **ワイプ**

デバイスのタイムゾーン設定

対象：iOS 14.0+以降、tvOS 14.0+以降のデバイス

このアクションに位置情報サービスは不要です。デバイスのタイムゾーン設定はデバイスのデバイス詳細ページにも表示されます。デバイスのタイムゾーン変更はIvanti Neurons for MDMサーバーにも反映されます。

[自動日時を強制]制限が[iOS制約構成]で有効化されている場合は、このデバイスアクションによってエラーが生じます。

手順

1. 1つまたは複数のデバイスを選択します。
2. 選択したデバイスの**[アクション]** > **[タイムゾーンを設定]**をクリックします。
3. タイムゾーンの文字列は、オルソンタイムゾーンID形式で入力します。例：太平洋/ミッドウェー
4. **[タイムゾーンを設定]**をクリックします。

基準によるデバイスのリスト化

フィルタのサイドナビゲーションバーを使用すると、デバイスの一覧から特定のデバイスを検索して表示できます。[スペース]ドロップダウンリストを使用すると、すべてのスペースまたは特定のスペースを選択して、デバイスと関連する情報を表示できます。検索はバンドルバージョンとディスプレイバージョンのいずれでも可能です。[デバイス]ページにはデバイスのバンドルバージョンとディスプレイバージョンの両方が表示されます。

[デバイスグループ]ページから(**[デバイス数]**カラムのデバイス数のハイパーリンクをクリックして)、または**[アプリインベントリ]**ページから(**[インストール数]**カラムのインストール数のハイパーリンクをクリックして)移動する場合、デバイスをページに表示するスペース名がメッセージに表示されます。

詳細なデバイス情報の表示

エントリの[名前]カラム内のリンクをクリックすると、デバイス詳細ページが表示されます。[デバイス詳細]ページには、以下の情報を含む複数のタブがあります。

- **概要** - 次の表は、[概要] タブに表示されるすべての詳細を一覧にしています。

セクション名	説明
一般	◦ デバイスの位置情報 ◦ 製造者 ◦ Wi-Fi MACアドレス ◦ WiFi-IPアドレス(Androidデバイス) ◦ ネットワークテザリング済み - (iOSデバイス) ◦ シリアル番号 ◦ 代替シリアル番号(Androidデバイス) - デバイス管理者またはデバイス所有者モードのSamsungデバイスに適用される、メーカー指定のシリアル番号。 ◦ ストレージ使用 - デバイス上の使用中(Windowsを除く) および使用可能な内部ストレージ ◦ 使用可能なバッテリ(Android) ◦ バッテリ状態 (Android) - 充電中、放電中、充電完了、充電停止中 ◦ 推定バッテリー残量(Windows) ◦ 推定バッテリー動作時間(Windows) ◦ 利用可能な更新(macOS) ◦ 利用可能な更新の名前(macOS) ◦ OSバージョン ◦ OSビルドバージョン ◦ 補足的ビルドバージョン ◦ 補足的OS/バージョンエクストラ ◦ Appleシリコンデバイス ◦ ファームウェアバージョン ◦ デバイスソース

セクション名	説明
	◦ 法的所有者 ◦ マルチユーザーモード ◦ タイムゾーン ◦ システム更新(Androidデバイス) ◦ Zebraパッチバージョン(Androidデバイス) ◦ 最後のホットフィックスID - (Windowsデバイス) ◦ インストールされた最後のホットフィックス - (Windowsデバイス)
設定	◦ デバイス名 ◦ デバイスの識別子 ◦ デバイスGUID ◦ Device Enrollmentデバイス(Appleデバイス) ◦ 登録済みのDevice Enrollmentデバイス(Appleデバイス) ◦ 自動Device Enrollment有効 ◦ 自動Device Enrollment登録済み ◦ User Enrollment登録済み(Appleデバイス) ◦ 登録済みの管理対象Apple ID(Appleデバイス) ◦ デバイスグループ ◦ 言語 ◦ MDMデバイス識別子 ◦ デバイスクライアントID ◦ クライアントアプリのバージョン ◦ クライアントアプリのバンドルID

セクション名	説明
	◦ クライアント登録 ◦ EASデバイス識別子 ◦ アクティベーションロック有効 ◦ Appleの宣言型管理が有効 ◦ アクティベーションロックバイパスコード ◦ 利用規約 ◦ オーナーシップ ◦ iTunesアカウントアクティブ ◦ デバイス位置情報サービス有効 ◦ 検疫済み ◦ Sentryによるブロック ◦ Accessによるブロック ◦ コンプライアンスアクションによるブロック ◦ APNS対応 ◦ 監視モード(iOS、macOSデバイス) - 監視デバイスを識別します。デバイスがITチームの直接管理下にあることは変わりません。監視モードにより、他のデバイス機能(フィールドサービスデバイス、小売POSデバイスなど)、ホスピタリティやサービスでのデバイス「貸し出し」、学生たちによる教室のデバイスの共有が可能になります。 ◦ PINをワイプ - PINを表示するには **[表示]** をクリックします。 ◦ マネージドmacOS管理者ユーザー(macOSデバイス)

セクション名	説明
	◦ デバイス暗号化ステータス(macOSデバイス) ◦ FileVault暗号化有効 ◦ 個人リカバリキー使用 ◦ 機関リカバリキー使用 ◦ Bootstrapトークンを利用できます ◦ システム完全性保護有効 ◦ ファームウェアパスワード ◦ パスワード ◦ 変更保留中 ◦ コマンドステータス ◦ オプションROMを許可 ◦ リカバリロック ◦ パスワード ◦ リカバリロック有効 ◦ ファイアウォール設定(macOSデバイス) ◦ ファイアウォール有効 ◦ すべての受信をブロック ◦ ステルスモード ◦ アプリケーションファイアウォールステータス(macOSデバイス) ◦ iCloudへの前回のバックアップ(iOSデバイス) ◦ パスコードロック猶予期間(iOSデバイス) ◦ Android ID

セクション名	説明
	◦ Androidセキュリティパッチレベル(Androidデバイス) ◦ キオスクモード(Androidデバイス) ◦ Android SafetyNet認証タイプ(Androidデバイス) ◦ Androidエンタープライズ対応(Androidデバイス) ◦ Android Work有効(Androidデバイス) ◦ Samsung SAFE対応(Androidデバイス) ◦ Android仕事用マネージドデバイス(デバイス所有者)有効 ◦ 会社所有デバイス上のAndroid仕事用プロファイル有効 ◦ 仕事用プロファイルを持つAndroidマネージドデバイス ◦ 会社所有デバイス上のAndroid仕事用プロファイルのロック有効 ◦ Help@Workの提供 ◦ Zebra対応 ◦ Secure Appsステータス ◦ Secure Apps暗号化ステータス ◦ セキュアアプリ暗号化モード ◦ FCM有効
Windows情報保護(Windowsデバイス)	◦ WIP ◦ アプリロッカー構成済み ◦ EDP強制設定
テレフォニー	◦ 電話番号 ◦ セルラーテクノロジー ◦ IMSI ◦ ICCID

セクション名	説明
	◦ IMEI ◦ IMEI 2 - (デュアルSIMポートのあるAndroidデバイスのみ。Android 8.0以降に適用) ◦ MEID ◦ デバイスの位置情報 ◦ キャリア ◦ ホームMCC ◦ ホームMNC ◦ 現在の国名 ◦ 本国 ◦ セルラーテクノロジー ◦ ローミング ◦ 現在の通信事業者 ◦ 現在のMCC ◦ 現在のMNC ◦ データローミング ◦ 音声ローミング サポートされるiOSデバイスの場合、これらの特性が複数のeSIMアクティブサービスサブスクリプションについて表示されます。
Azureデバイスコンプライアンス	◦ Azureデバイス識別子 ◦ Azureデバイスコンプライアンスステータス ◦ Azureクライアントステータスコード ◦ Azureデバイスコンプライアンスレポート時間

セクション名	説明
	◦ Azure Intuneデバイスユーザー UPN
バッテリ情報	◦ バッテリレベル - Android OS で報告された現在のバッテリ充電レベルが表示されます。 ◦ バッテリ正常性状態 - Android OS で報告された情報 ◦ バッテリ充電状態 - Android OS で報告された情報 ◦ バッテリ正常性割合 (OEM 固有) - Zebra デバイスなどのサポートされているデバイス製造元のバッテリ正常性の割合 ◦ バッテリ製造日 (OEM) - Zebra デバイスなどのサポートされているデバイス製造元のバッテリ製造日 ◦ バッテリ充電サイクル (OEM) - Zebra デバイスなどのサポートされているデバイス製造元について完了したサイクルの合計数

- **構成** - 適用された**構成**[1]の詳細。詳細は「構成の操作」ページ424をご参照ください。
- **インストール済みのアプリ**- デバイスにインストールされているアプリケーションの詳細。インストールされているアプリの現行バージョンのインストール日が **[アプリ報告日]** カラムの下に表示されます。

> 検疫を終了したデバイスのアプリインストール日は、デバイスの検疫解除日です。

> Android Enterpriseデバイスの場合は、インストール済みアプリの利用状況の詳細を、日、週、月、年でソートして表示することもできます。これらの詳細を表示するには、**[構成設定]** セクションにある **[アプリの利用状況データの収集を有効にする]** オプションを選択している必要があり、選択すると、**[アプリの利用状況 - 日]**、**[アプリの利用状況 - 週]**、**[アプリの利用状況 - 月]**、**[アプリの利用状況 - 年]** の各オプションを選択してアプリの利用状況の詳細を表示できるようになります。

[1]collections of settings that you send to devices.

- **利用可能なアプリ** - デバイスで利用可能なアプリケーションの詳細。[ステータス] カラムに、デバイス上でのアプリケーションのインストールステータスが示されます。
    - アクション - [配布] と [除外] - アプリをデバイスに配布する場合は、[アクション] カラムの **[除外]** オプションは [利用可能] になり、**[配布]** オプションは [使用不可] になります。アプリが除外されている場合は、[除外] ボタンは [使用不可] になり、[配布] オプションは [利用可能] になります。

    > アプリのインストールステータスは、管理対象のアプリケーションについてのみキャプチャされます。管理対象外アプリのアプリケーションインストールステータスは、「インストールされていません」と表示されます。正しいインストールステータスを表示するには、アプリケーションを「管理対象」に変換する必要があります。
    > アプリのインストールステータスによるソートはサポートされていません。

- **AppConnectアプリ** - インストールされているAppConnectアプリの詳細。
- **ポリシー** - 適用されている**ポリシー**[1]の詳細。侵害されたデバイスの場合、[違反] カラムで違反の理由にチェックを入れます。デバイスがルート化されている場合、システムは **[違反]** 列に理由を表示します。

優先度(1 = 最高)	違反
1。	プラグインが侵害されています
2	クライアントが改ざんされています
3	デバイス製造業者が不明です: 不明
4	疑わしいフォルダーが検出されました: [パス]
5	疑わしいバイナリが検出されました: [パス]
6	フォルダー/データがブラウズ可能またはフォルダー/データ/データがブラウズ可能
7	/system/app/Superuser.apkが見つかりました
8	パッケージマネージャーが侵害されています
9	疑わしいアプリが検出されました: [パッケージ]

[1] sets of requirements and compliance actions defined for devices.

- **証明書** - インストール済みの証明書の詳細。
  証明書を使用する際は[利用の種類]のカラムをご確認ください。証明書がデバイス固有の場合は、利用の種類が「デバイス」と表示されます。証明書がユーザー固有の場合は、利用の種類が「ユーザー」と表示されます。
- **Sentry** - Sentryの情報(ActiveSyncアソシエーション)
- **属性** - カスタム属性およびデバイス属性
- **ユーザー** - 監視対象のMacOSデバイスについてアクティブユーザーのリストを表示します。

  [ユーザー] タブが強化され、管理対象Apple IDがハイパーリンクで表示されるようになりました。これをクリックすると、[共有 iPad] のユーザーアカウントの詳細ページにリダイレクトされます。
- **ログ** - デバイスフィルターの表示とカスタマイズ
- **ハードウェア** - ハードウェアインベントリの詳細(システム、マザーボード、BIOS、ハードドライブ、CD-ROM、プロセッサ、物理メモリ)

ユーザーおよびカスタム属性のデバイスへの一括割り当てまたは変更

[アップロード経由で一括割り当て] 機能では、CSVファイルをアップロードし、デバイスへのユーザーやカスタム属性の一括割り当てまたは変更が可能です。

手順

1. デバイスページから **[アップロード経由で一括割り当て]** アイコン(アクションボタンの隣)をクリックします。
2. (任意) **[テンプレートをダウンロード]** をクリックし、編集およびアップロード可能なCSVテンプレートファイルを保存します。
3. CSVファイルを準備した後、**[ファイルを選択]** をクリックし、CSVファイルの位置をブラウズして、CSVファイルをファイルデータセクションにドラッグ＆ドロップします。
4. 以下のオプションから1つ選択してください:
   - **既存の値があってもすべての属性の割り当て(上書き)を強制**
   - **値が空の場合のみ上書きし、属性に既存の値があればスキップ**
5. **[アップロード]** をクリックします。

CSV ファイルへのデバイスのエクスポート

[デバイス] ページの **[CSVにエクスポート]** オプションを使用して、特定のデバイスのデバイス詳細をエクスポートできます。

手順

1. **[デバイス]** を開きます。
2. すべてまたは複数のスペースを選択して、特定のスペースに関連する情報を表示します。
3. デバイス数のリンクをクリックします。選択したスペースに関連する [デバイス] 一覧ページが表示されます。
4. **[CSVにエクスポート]** オプションをクリックして、デバイスリストと関連詳細をCSVファイルにエクスポートします。エクスポート レポートの処理にしばらく時間がかかる旨のポップアップ メッセージが表示されます。この要求が完了するまで待ってから、別の要求を送信するようにしてください。レポートの準備が完了すると、レポートをダウンロードまたは削除するよう促すメッセージが表示されます。
5. **[ダウンロード]** をクリックします。レポートをダウンロードするためのリンクが記載された電子メールも送信されます。
6. (任意) レポートを削除するには **[削除]** をクリックします。

デバイスログの検索

手順

1. **[デバイス]** > **[デバイス]** を開き、任意のエントリの **[名前]** 列リンクをクリックします。
2. **[ログ]** タブをクリックします。
3. [アクション]、[ステータス]、[開始日]、[終了日] のフィルターを使用して表示されたメッセージを絞り込みます。

4. [デバイスの詳細] カラムに、次のような、アプリケーションのステータスが表示されます。

   すべてのデバイスに関して、ステータスとして以下の詳細が示されます。

   - アプリ名、アプリバージョン、バンドル、またはパッケージID
   - インストールのステータス
   - エラーとエラーの理由
     例：appOrConfigName=Name:<アプリ名>;Identifier=<バンドルID>;iTunesStoreId:<iTunes ID>;Status:<Appleからのステータスまたはエラーの理由>version: <アプリバージョン>

   Windowsデバイスに関しては、ステータスとして以下の詳細が表示されます。

   - バンドルIDまたはパッケージID、ステータス、エラーを含む
     例：
   - タイプの場合 - アプリケーションインベントリとステータス - 承諾 - 表示 - アプリタイプ
   - タイプの場合 - アプリケーションインベントリとステータス - 送信 - 何も表示しない
   - タイプの場合 - インストール/アンインストールとステータス - 成功/失敗/送信中 - 表示：バンドルIDまたはパッケージID、ステータス、名前、バージョン、エラーを含む

[デバイス] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- 読み取り専用デバイス

デバイスグループ

このセクションは以下のトピックを含みます。

- 「デバイスグループの追加」下
- 「デバイスグループの削除」ページ187
- 「CSV ファイルへのデバイスのエクスポート」ページ188

[デバイスグループ] ページでは、同様に扱いたいデバイスのリストを作成できます。ポリシーと構成を定義して、デバイス グループに割り当てることができます。Ivanti Neurons for MDMによって作成されるデフォルトのデバイスグループは次のとおりです。

- すべてのデバイス
- Androidデバイス
- Android Enterpriseデバイス
- iOSデバイス
- tvOSデバイス
- macOSデバイス
- Windowsデバイス

特定のデバイスグループに割り当てられたアプリの詳細は、そのデバイスグループの **[アプリ]** タブに表示されます。

tvOSデバイスグループはiOSデバイスグループのサブセットです。したがって、tvOSデバイスグループに適用される構成とポリシーは、iOSデバイスグループによって上書きされる場合があります。

デバイスグループの追加

お持ちのライセンスのタイプによっては、特定の基準を満たすデバイスを識別するためのルールに基づいて、新しいデバイスグループを追加できます。ルールに一致するデバイスは、ルールビルダーセクションの下に表示されます。[ANY (OR)] または [ALL (AND)] オプションを使用すればネストでまとめることができます。ルールは、次の演算子を使用して作成できます。

- は次から始まる
- 終了：
- 含む
- 次を含みません：
- 次で開始しません：
- 次で終了しません：
- は次より以下：
- は次より大きい：
- は範囲内です
- は次と等しい：
- は次と等しくありません：
- は空白ではない
- は空白である

ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM管理者は、重複するユーザーグループ数と、重複するグループを識別するGUID番号を表示します。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

Bronzeライセンス：

ルールは以下の基準でデバイスを識別します。

- デバイスの種類
- OS - オペレーティングシステム(自動入力)
- OSバージョン
- ユーザーグループ

Silver ライセンス：

ルールは以下の基準でデバイスを識別します。

- AAD登録済み
- 代替シリアル番号(Androidのみ - デバイス管理者またはデバイス所有者モードのSamsungデバイスに適用)
- Android専用デバイス
- Androidエンタープライズ対応
- 仕事用プロファイルを持つAndroidマネージドデバイス
- Android SafetyNet認証タイプ
- Android Work有効
- Android仕事用マネージドデバイス(デバイス所有者)有効
- Android仕事用プロファイル有効
- 会社所有デバイス上のAndroid仕事用プロファイル有効
- APNS対応
- 自動Device Enrollment有効
- Azureデバイス識別子
- Azureデバイスコンプライアンスステータス
- Azureクライアントステータスコード
- Azureデバイスコンプライアンスレポート時間
- BitLocker暗号化
- Sentryによるブロック
- Accessによるブロック
- Bootstrapトークンを利用できます
- バルクプロビジョニングの種類(Apple Configurator、なし、自動Device Enrollment登録済み)
- キャリア
- クライアントの前回のチェックイン

- クライアント登録
- コンプライアンス
- コンプライアンスアクションによるブロック
- 現在の国名(ドロップダウンリストから現在の国名を選択)
- 現在のMCC
- 現在のMNC
- カスタムデバイス属性
- カスタムLDAP属性
- カスタムユーザー属性
- データローミング
- デバイス登録時刻
- デバイスソース
- デバイスの種類
- 表示名
- 暗号化有効
- ハードドライブのパーティション
- 本国名(ドロップダウンリストから現在の本国名を選択)
- ホームMCC
- ホームMNC
- IPアドレス
- キオスクモード
- 最新のチェックイン
- MAM のみ

- 製造者
- OS
- OSエディション
- OSバージョン
- オーナーシップ
- 電話番号
- 検疫済み
- リカバリロック有効
- ローミング
- Secure Appsステータス
- シリアル番号
- ステータス
- 監視対象
- システムバージョン
- 全デバイス容量
- メモリ合計(MB)
- TPMバージョン
- ロック解除トークンを利用できます(iOS)
- User Enrollment有効
- ユーザーグループ
- 音声ローミング
- macOS個人リカバリキーがエスクローされました
- macOSリカバリキーの種類

手順

1. **[追加]** をクリックします。
2. グループの名前を入力します。
3. 任意でグループの説明を入力します。
4. 作成したいデバイスグループの種類を選択します。
   - **動的管理**：ルールを使用してグループに入れるデバイスを定義します。
   - **手動管理**：グループに含めるデバイスのユーザーを入力します。
5. 動的管理グループ：
   a. グループを定義するルールを作成します。

      例：OSはiOS

   b. **[+]** をクリックし、必要に応じて追加のルールを作成します。

      例：デバイスはiPhone 5S

   c. デバイスが少なくとも1つのルールを満たす必要がある場合は、**[いずれか]** をクリックします。
   d. デバイスがすべてのルールを満たす必要がある場合は、**[すべて]** をクリックします。
6. 手動管理グループ：
   a. 追加したいデバイスのユーザー名を入力します。
   b. 表示されたリストからデバイスを選択します。
   c. すべてのデバイスがリストに表示されるまでaとbの手順を繰り返します。
7. **[保存]** をクリックします。

デバイスグループの削除

手順

1. **[デバイス]** > **[デバイスグループ]** を開きます。
2. 削除したいデバイスグループのチェックボックスをクリックします。
3. **[デバイスグループの削除]** をクリックします。

CSV ファイルへのデバイスのエクスポート

[デバイスグループ] ページの **[CSVにエクスポート]** オプションを使用して、特定のデバイスグループのデバイス詳細をエクスポートできます。

手順

1. **[デバイス]** > **[デバイスグループ]** を開きます。
2. すべてまたは複数のスペースを選択して、特定のスペースに関連する情報を表示します。
3. デバイスグループ数のリンクをクリックします。選択したスペースに関連する [デバイス] 一覧ページが表示されます。
4. **[CSVにエクスポート]** オプションをクリックして、デバイスリストと関連詳細をCSVファイルにエクスポートします。エクスポート レポートの処理にしばらく時間がかかる旨のポップアップ メッセージが表示されます。この要求が完了するまで待ってから、別の要求を送信してください。
5. **[ダウンロード]** をクリックします。レポートをダウンロードするためのリンクが記載されたメールが送信されます。
6. (任意) レポートを削除するには **[削除]** をクリックします。

[デバイスグループ] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- 読み取り専用デバイス

非マネージドデバイス

このセクションは以下のトピックを含みます。

- 「デバイスのブロック」下
- 「デバイスのブロック解除」下
- 「デバイスリストからのデバイスクリア」次のページ

ライセンス: Silver

SentryのEメールアクセス制御を設定した場合、Eメールシステムにアクセスする未登録デバイスは非管理デバイスと呼ばれます。非管理デバイスがデフォルトでEメールを利用できるかどうかは、Sentryの設定時に定義します。その後、それらのデバイスのEメールアクセスを手動で許可またはブロックすることも可能です。

[非マネージドデバイス] ページは5分ごとに更新されます。したがって、管理の変更は即座には反映されません。

デバイスのブロック

手順

1. デバイスを選択します。
2. **[アクション]** > **[ブロック]** を選択します。

デバイスは、**[アクション]** > **[許可]** または **[アクション]** > **[削除]** を選択するまでブロックされます。

デバイスのブロック解除

手順

1. デバイスを選択します。
2. **[アクション]** > **[許可]** を選択します。

デバイスは、**[アクション]** > **[ブロック]** または **[アクション]** > **[削除]** を選択するまで引き続きEメールにアクセスできます。

デバイスリストからのデバイスクリア

手順

1. デバイスを選択します。
2. **[アクション]** > **[削除]** を選択します。

次にデバイスがEメールシステムにアクセスしようとすると、このリストにデバイスが再び表示されます。その時点で、前に適用したブロックまたは許可のアクションを再び行ってください。

アプリのインベントリ

このセクションは以下のトピックを含みます。

- 「アプリの表示のフィルタリング」下
- 「アプリがインストールされているデバイスの表示」次のページ
- 「アプリリストの表示」次のページ
- 「デバイスにインストールされているWin32アプリの表示」次のページ
- 「カスタム表示許可の作成」ページ193
- 「アプリインベントリのエクスポート」ページ194

アプリインベントリとは、登録されたデバイス上で検出されるアプリのリストです。管理者はこのページを使用して、登録されたデバイスで使用されているアプリに関する情報を取得できます。次のような問いに答えることができます。

- 最も人気のあるアプリはどれですか?
- iOSデバイスはApp Storeから直接アプリを入手しますか?
- オプションの**自社開発アプリ**[1]を何人のAndroidユーザーがダウンロードしましたか?
- 古いバージョンのアプリを使用しているデバイスは何台ありますか?

アプリの表示のフィルタリング

[デバイス] > **[アプリインベントリ]** ページを表示すると、すべてのアプリがリスト表示されます。このリストを特定のアプリに絞り込むには、フィルタ(左ペイン)を使用します。たとえばGoogle Playのプライベートアプリのみ表示するようリストを絞り込むには、**[ソース]** セクションで **[プライベート]** を選択します。

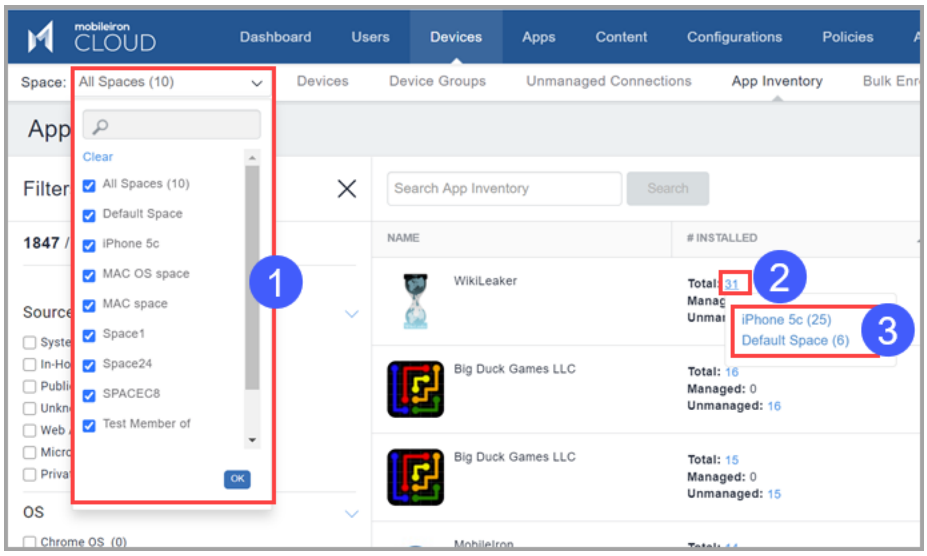
ドロップダウンリストから複数のスペースを選択すると、すべてまたは複数のスペースのデバイスのアプリインベントリを表示可能です。表示されたアプリの上にポインターを置くとデバイス数が表示されます。デバイス数をクリックするとアプリを含むすべてのデバイスが表示されます。各アプリインベントリのレコードはスペースごとにグループ化されています。

---

[1] an app distributed by the device management service rather than downloaded from a public app store.

アプリ名またはバンドル/パッケージ ID を使用して検索できます。

複数のスペースを選択し、**[インストール数]** カラムの **[合計]** の値にポインターを置くと、デバイススペースごとのインストール数が表示されます。1 2 3



アプリがインストールされているデバイスの表示

[インストール数] カラムに表示されている **[マネージド]**、**[非マネージド]**、**[すべて]** カラムのいずれかをクリックします。

アプリリストの表示

アプリインベントリでアプリの **[要求された番号]** をクリックすると、アプリを要求したデバイスが表示されます。これはMAM-Onlyデバイスにのみに適用されます。

デバイスにインストールされているWin32アプリの表示

デバイスのプライバシー構成で、そのデバイス上の全アプリの情報収集が許可されている場合、アプリインベントリにはそのデバイス上のWin32アプリが表示されます。そのデバイスのプライバシーポリシーを構成できます。

手順

1. [デバイス] ページの指示に従い、対象のデバイスにどのプライバシー構成を適用するかを判断します。
2. **[構成]** に進みます。

3. ステップ1で確認したプライバシー構成について：
    a. 構成を選択します。
    b. [Edit] をクリックします。
    c. **[アプリインベントリを収集]** で、**[デバイス上のすべてのアプリ]** を選択します。
    d. **[完了]** をクリックします。

カスタム表示許可の作成

ユーザー用のカスタム表示許可を指定できます。

手順

1. **[管理]** を開きます。
2. **[役割管理]** を開きます。
3. **[役割を追加]** をクリックします。
4. **[スペース特有の役割]** オプションを選択します。
5. **[名前]** フィールドにユーザー名を入力します。
6. **[デバイス]** メニューから **[アプリインベントリ]** をクリックします。
7. **[表示]** チェックボックスを選択します。
8. **[デバイス]** メニューから **[デバイスアクション]** をクリックします。
9. **[保存]** をクリックします。
10. メインメニューで **[ユーザー]** を開きます。
11. 作成した新しいユーザーをクリックします。
12. **[役割を割り当てる]** をクリックします。
13. **[アプリ | スペース特有]** チェックボックスを選択し、**[次へ]** をクリックします。
14. 作成した役割に割り当てられた許可が **[概要]** ページに表示されます。
15. **[完了]** をクリックします。

16. 新規ユーザーとしてログインします。
17. メインメニューから **[デバイス]** をクリックします。
18. **[アプリインベントリ]** をクリックします。
19. ユーザーに許可されたアプリのみが **[アプリインベントリ]** ページに表示されます。

アプリインベントリのエクスポート

管理者は、**[CSVにエクスポート]** オプションを使用してアプリインベントリレポートを要求できます。

手順

1. **[デバイス]** > **[アプリインベントリ]** に移動します。
2. リストからインベントリを選択します。
3. **[CSVにエクスポート]** をクリックします。

ポップアップメッセージが表示され、レポートのエクスポートの処理に少し時間がかかることが通知されます。要求を送信した後は、要求が完了するまで待ってから、次の要求を送信する必要があります。レポートの準備が完了したら、生成されたレポートをダウンロードまたは削除するためのメッセージが表示されます。レポートをダウンロードするためのリンクが記載された電子メールも送信されます。

[アプリインベントリ] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- デバイス読み取り専用

デバイスの管 理

このセクションは以 下 のトピックを含 みます。

- 「リカバリロックの設 定 または変 更 」 ページ283

Windowsデバイスの導入

このセクションは以下のトピックを含みます。

- 「概要」下
- 「デバイス管理」下
- 「Windows デバイス登録」下
- 「Windows Update 管理」次のページ
- 「アプリの配布と管理」次のページ
- 「アプリ制御」ページ200
- 「Windows デバイス管理構成」ページ200
- 「Windows デバイスコンプライアンス」ページ201
- 「Windows アプリおよびハードウェア インベントリ」ページ201

概要

Ivanti Neurons for MDM では、構成、登録、プロビジョニング、保護、アプリケーション、管理、監視、ソフトウェア更新、OS 更新、除却までの HoloLens 2 エンドツーエンド デバイスライフサイクル管理を含む、すべての Windows ノート PC およびデスクトップ PC を管理できます。

デバイス管理

サポートされている Windows デバイス:

- Windows PC 10+
- Microsoft HoleLens 2

デバイス管理とレポート機能の詳細については、「デバイス」ページ164をご参照ください。

Windows デバイス登録

Ivanti Neurons for MDM は、次のような、Windowsデバイス用の標準的なデバイス登録方法をすべてサポートしています。

- 手動登録
- バルク登録
- SCCM とIvanti EPM の使用
- Windows Autopilot
- AAD 登録

登録方法の詳細については、「Microsoft Azureの使用」ページ1215を参照してください。

マルチユーザーサポートについては、「Windowsデバイスにおけるマルチユーザーサポート」ページ1217を参照してください。

Windows Update 管理

- Windows update の構成とスケジュール - Windows update を構成してスケジュール設定するには、構成 -「ソフトウェア更新」ページ668を使用して構成を作成します。
- Windows Update 管理 - Windows 10 Update Management を使用して更新する Windows 10 デバイスで報告された更新を表示して承認できます。この機能では、不要またはテスト済みでない更新がデバイスにインストールされるのを防止します。詳細については、「Windows 10の更新管理」ページ958をご参照ください。

アプリの配布と管理

ユーザは、Windows アプリケーションのアプリライフサイクル全体 (インポート、構成、スケジュール、配布、更新、削除) を管理できます。

サポートされているアプリタイプ:

- 自社開発
- MSB
- 公開ストア

サポートされているアプリ拡張:

- MSI
- MSIX

- APPX
- APPX バンドル
- EXE (Bridge)

Windows アプリの管理の詳細については、「アプリ構成」ページ337をご参照ください。アプリ更新を自動化するには、「Windowsアプリスケジューリング」ページ961および「構成の操作」ページ424をご参照ください。

アプリ制御

アプリ制御構成により、アプリをデバイスレベルで許可リストまたはブロックリストに分類できます。すでにインストールされているアプリは非表示になり、起動できなくなります。App Storeには引き続きアプリが表示されますが、ダウンロードや起動はできません。アプリ制御構成が配布されたデバイスはすべて、この構成を使用し、許可されたアプリポリシー設定を無視します。アプリ制御構成は、対象デバイス上で同じアプリを参照するアプリ関連ポリシーすべてに優先します。

詳細については、「アプリ制御構成：デバイスごとにインストールするアプリを制御」ページ445をご参照ください。

Windows デバイス管理構成

Windows 10+ PC および Microsoft HoloLens 2 のサポートには次の機能が含まれています。

- デバイスの登録
- 「パスコード構成」ページ651
- 「Exchange構成」ページ736
- 「設定」ページ423
- 「デバイス」ページ164
- 「アプリ」ページ284
- 「Windowsアプリスケジューリング」ページ961
- 「アプリ制御構成：デバイスごとにインストールするアプリを制御」ページ445
- 「Windows 10の更新管理」ページ958
- 「Ivanti Neurons for MDM から Azure へのデバイス ステータスの報告」ページ1244
- 「Windows Autopilotプロファイルの構成」ページ1202

- 「カスタム構成を使用したデバイスへのSyncMLプッシュ」ページ441
- 「ポリシー」ページ987
- Windows の制約
- ID 証明書
- Windows Hello for Business
- Wi-Fi および VPN プロファイル

このデバイスタイプによってサポートされていないHoloLensデバイスに配布された構成は、[デバイスの詳細] の [構成] タブに、配布済みの構成として報告されません。

Windows 機能 (Windows PC でのみサポート):

- 「Ivanti Bridge」ページ410
- 「Windows BIOS構成」ページ962
- 「Windows BitLocker」ページ975
- 「Windowsキオスク構成」ページ976
- 「Windowsライセンス構成」ページ985
- 「EMAサーバー統合構成」ページ921
- 「プリンター設定」ページ936
- 「ブロートウェア削除構成」ページ941
- 「ADMX(GPO) ブラウザ」ページ1211

Windows デバイス コンプライアンス

Microsoft Azureで Ivanti Neurons for MDM を設定すると、Windows 10を実行するWindowsデスクトップとタブレットを使用するユーザーがシームレスに登録できます。Azure テナント統合を構成して、Windows デバイス コンプライアンスを有効にするには、「Microsoft Azureの使用」ページ1215をご参照ください。

Windows アプリおよびハードウェア インベントリ

Windows アプリ インベントリ

アプリインベントリとは、登録されたデバイス上で検出されるアプリのリストです。このページを利用して、登録されたデバイスで使用されるアプリに関する情報を取得します。詳細については、「アプリのインベントリ」ページ191をご参照ください。

プライバシー構成でデバイス上の全アプリの情報収集が許可されている場合、アプリインベントリにデバイス上のWin32アプリが表示されます。

アプリインベントリ間隔の構成

複数のアプリソースタイプのインベントリには、Windows 10アプリインベントリコレクション間隔を設定できます。間隔は、デバイスからすべてのアプリを収集するようプライバシー構成が設定されている場合に使用します。

詳細については、「アプリインベントリ間隔の構成」ページ1212をご参照ください。

Windows ハードウェア インベントリ

Windows 10以上のデバイスからのハードウェア情報の収集を有効化します。これらの詳細は、Bridgeを使用して取得します。詳細については、「ハードウェアインベントリ」ページ1213をご参照ください。

macOSデバイスにおけるAppleリモートデスクトップのセットアップ

このセクションは以下のトピックを含みます。

- 「macOSデバイスにおけるAppleリモートデスクトップの有効化」下
- 「macOSデバイスにおけるAppleリモートデスクトップの無効化」下

macOSデバイスにおけるAppleリモートデスクトップの有効化

Apple Remote Desktop機能では、画面共有機能を有効にし、デバイスをリモートで管理できます。Apple Remote Desktop機能は、macOS 10.14.4以降の監視対象デバイスで使用できます。

手順

1. **[デバイス]** で1台以上のmacOS監視対象デバイスを選択します。
2. そのデバイスの **[アクション]** > **[リモートデスクトップを有効化]** アクションをクリックします。
3. **[リモートデスクトップを有効化]** をクリックして確定します。

macOSデバイスにおけるAppleリモートデスクトップの無効化

手順

1. **[デバイス]** で1台 以 上 のmacOS監 視 対 象 デバイスを選 択 します。
2. そのデバイスの **[アクション]** > **[リモートデスクトップを無 効 化]** アクションをクリックします。画 面 共 有 機 能 は無 効 です。デバイスをリモートで管 理 することはできません。

デバイス登録(iOS、macOS、Android)

このセクションは以下のトピックを含みます。

- 「管理プロファイルの手動インストール」次のページ
- 「招待状の送信(iOS、macOS、Android)」次のページ
- 「エンドユーザーに対しアプリのダウンロードを指示する(iOSおよびAndroid)」ページ206

ほとんどのユーザーがまずデバイスを登録します。以下のいずれかの方法で、登録プロセスを開始できます。

- 1人以上のエンドユーザーに招待状を送る(iReg登録)
- エンドユーザーに対しGoのダウンロードを指示する(アプリ内登録)

iOSデバイスやmacOSデバイスのMDM登録が失敗して、「*プロファイルのインストール失敗。SCEPサーバーが無効な応答を返しました*」というエラーが表示された場合、デバイスユーザーは、デバイス登録プロセスを最初から再度開始する必要があります。大抵の場合、これが発生するのは、デバイスにプロファイルがダウンロードされた後、デバイスユーザーがiOSデバイスやmacOSデバイスのMDM登録プロセスを完了するまでにかかった時間が、予想よりも長かった場合です。詳しい説明については、Ivantiサポートまでお問い合わせください。

Ivanti Neurons for MDMは、macOSデバイスでシングルユーザー(ローカルユーザーまたは登録済みのActive Directory [AD] ユーザー)のユーザーレベル管理をサポートします。管理者は、ユーザーのデバイス管理、およびデバイスプロファイルとユーザープロファイルの適用を行い、その結果としてApp Store、アプリの配布、構成、ポリシー(Apps@Work、制約、セキュリティを含む)を使用します。

ADユーザーのmacOSデバイスを管理するには、ADユーザーが登録中にログインしたユーザーである必要があります。他の非登録ユーザーは、登録ユーザー専用のプロファイル(ID証明書、VPNなど)を閲覧できません。ただし、デバイスレベルの構成は、すべてのログインユーザーが閲覧し、使用できます。

Ivanti Neurons for MDMエンドユーザーは、デバイス登録プロセスを開始する前に、Ivanti Neurons for MDM内にアカウントを持っている必要があります。LDAPユーザーの場合、ConnectorとLDAPサーバーを設定し、LDAPサーバーからユーザーをインポートしておく必要があります。ローカルユーザーにとってこれは、ユーザーの追加を意味します。

Ivanti Neurons for MDM Ivanti Neurons for MDMの旧バージョンで生成されたデバイス登録URLは、最新バージョンでは機能しません。管理者は、デバイス登録用のデバイス登録URLを生成する必要があります。

管理プロファイルの手動インストール

対象：

- iOS 12.2以降、Ivanti Neurons for MDMがサポートする最新版まで。
- macOS 11.0以降、Ivanti Neurons for MDMがサポートする最新版まで

iOS デバイス登録

iOSデバイスでのアプリ内登録：

- Go appを使用したデバイス登録中に、プロファイルをインストールする手順のページが表示されます。
- **[ダウンロードされたプロファイルのインストール]** オプションをクリックし、**[理解しました]** をクリックします。
- ダウンロードしたプロファイルは数分間有効となり、その後は再登録が必要となります。

macOS デバイス登録

macOSデバイスでセルフサービスポータルを通じて登録する場合、ユーザーは以下を実行する必要があります。

手順

1. 自分の認証情報でログインします。
2. [管理プロファイルをインストール] ページでプロファイルがユーザーのローカルシステムにダウンロードされます。
3. ダウンロードしたプロファイルをダブルクリックすると、ユーザーのシステム環境設定に表示されます。

   ユーザーが制限時間内にインストールしない場合、プロファイルが無効になります。

4. システム環境設定で **[プロファイル]** を開きます。プロファイルがデバイスにダウンロードされると、ユーザーにはプロファイルリンクのあるWebページが表示されます。**[プロファイル]** をクリックして設定アプリを開きます。
5. **[インストール]** をクリックして管理プロファイルをインストールします。
6. インストールの手順を継続し、完了させます。プロンプトに応じてシステムパスワードを入力します。

招待状の送信 (iOS、macOS、Android)

招待を送信して、登録プロセスを開始します。Ivanti Neurons for MDM Cloudでは、エンドユーザーにデバイス登録を促す招待状を以下の方法で送信できます。

- スタートアップ ウィザード
- [1人 以 上 のユーザを追 加] する場 合
- [ユーザ] ページ([アクション] > [招 待 の送 信])

エンドユーザが招 待 をなくした場 合 は、招 待 に記 載 されている URL を共 有 できます。URL の末 尾 に **/go** を追 加 したことを確 認 してください。

パスワードが設 定 された Ivanti Neurons for MDM アカウントを所 有 しているエンドユーザは、招 待 がなくても登 録 プロセスを開 始 できます。招 待 に記 載 されている URL を送 信 できます。

エンドユーザーに対 しアプリのダウンロードを指 示 する(iOSおよびAndroid)

Go アプリケーションは Android および iOS デバイス向 けに提 供 されています。公 開 アプリストアからアプリケーションをダウンロードし、アプリケーションから登 録 プロセスを開 始 する手 順 をエンドユーザに提 示 することができます。電 子 メール招 待 には次 の情 報 が記 載 されています。

- 登 録 ページへのリンク
- ワンタイム PIN (管 理 者 が設 定 した場 合)
- 次 の手 順 に関 する基 本 情 報

アカウントのパスワードを設 定 していない場 合 は、パスワードをエンドユーザの会 社 用 電 子 メールアドレスに送 信 できます。認 証 にLDAPを使 用 している場 合 は、ネットワークの認 証 情 報 が必 要 であることをエンドユーザーに伝 達 してください。

ユーザが登 録 中 にMDMプロファイルを完 全 にインストールしない場 合 、Ivanti Neurons for MDMは定 期 的 にプッシュ通 知 をデバイスに送 信 し、ユーザに登 録 プロセスの完 了 を促 します。

ユーザはユーザ名 とパスワードを使 用 するか、QR コードをスキャンして Go app からデバイス登 録 を開 始 できます。詳 細 は次 のとおりです。

- **ユーザ名** : 電 子 メールアドレス
- **パスワード**: [ユーザ設 定] で指 定 されている場 合 。一 時 パスワードは管 理 者 が定 義 します。
- **QR コード**: Ivanti Neurons for MDM セルフサービスポータルから QR コードを生 成 します。**[QR コードのスキャン]** オプションを使 用 して QR コードをスキャンすると、デバイスのカメラにアクセスする権 限 を付 与 するように求 めるメッセージが画 面 に表 示 されます。アクセス権 を付 与 した後 、カメラで QR コードをスキャンし、デバイスを登 録 します。このオプションは、Android 9 以 降 および iOS 14 以 降 のバージョンでサポートされます。

エンドユーザがモバイルデバイスで登録電子メールを受信した場合は、リンクをタップすると、登録処理が開始します。ノートまたはデスクトップPCで電子メールを受信した場合は、モバイルデバイスのブラウザでURLを入力し、登録処理を開始します。

エンドユーザのアカウントに、Ivanti Neurons for MDMユーザアカウントに定義されたパスワードが設定されていない場合、あるいはユーザ設定で登録PINを必要としている場合は、ワンタイムPINが含まれます。PINの入力後、パスワードが存在しない場合は、アカウントのパスワードを設定するよう指示するプロンプトが表示されます。

Android Enterpriseデバイスでは、登録が完了すると、会社所有のデバイスまたは仕事用マネージドデバイスで仕事用プロファイルに対するすべての手動でインストールされたCA証明書がアンインストールされます。

iOSデバイスの再登録

デバイスを再登録する場合は、次のように行います。

1. お使いのデバイスでGoクライアントを起動します。
2. **[設定]** > **[トラブルシューティング]** > **[デバイスの再登録]** を開きます。再登録のプロセスが開始され、確認のプロンプトがいくつか表示されます。
3. それらのプロンプトで **[はい]** をタップします。

プロファイルのインストール中に **[キャンセル]** をタップすると、登録プロセスが停止し、Ivanti Neurons for MDMサーバーがデバイスMDMを無効化します。

再登録プロセスを再開するには、既にダウンロード済みのプロファイルを再インストールする必要があります。ダウンロードしたプロファイルの有効期間はわずか数分で、その後はGoクライアントから再登録を実行する必要があります。

Android デバイスの再登録

既存のアクティブなエントリを手動で消去せずに、除却、ワイプ、または削除処理を実行すると、管理者がデバイスを再登録できます。この方法は、新しいエントリと既存のエントリが同じテナントに属する場合に再登録するときに、特に役立ちます。Ivanti Neurons for MDM管理ポータルの[デバイス]ページには、次のように、デバイスのステータスが表示されます。

- **アクティブ** - デバイス登録が成功しました
- **非アクティブ** - デバイスはリセットされ、非アクティブ状態が表示されます。

- **ワイプ済み** - デバイスはリセットされ、ワイプ済み状態が表示されます。
- **リセット済み** - デバイスはリセットされ、次回の登録までサーバでアクティブ状態になります。

[監査証跡] ページには、Android デバイスのデバイス登録、再登録、非アクティブ状態が表示されます。詳細については、「ウィジェットの操作」ページ37をご参照ください。

Android 9.x 以前のバージョンでは、再登録後に、1 件のエントリが表示されます。Android 10.x 以降のバージョンでは、複数のエントリが表示されます。ただし、最新のエントリのみがアクティブになり、古いエントリは非アクティブ状態になります。

デバイスの登録(Windows 10+のPCおよびMicrosoft Hololens 2)

このセクションは以下のトピックを含みます。

- 「手動登録」下
  - 「招待状の送信」次のページ
  - 「エンドユーザー登録の完了」次のページ
- 「Windows Autopilot」ページ211
- 「AAD標準登録」ページ212

デバイス登録プロセスは次の2種類です。

- 手動登録
  - 招待
  - エンドユーザーの登録
- Windows Autopilot
- プロビジョニングパッケージ登録とPINを使用してSCCMとIvanti EPMを使用 PINでのパッケージ登録のプロビジョニングをご参照ください。
- バルク登録

手動登録

ほとんどのユーザーがまずデバイスを登録します。以下のいずれかの方法で、登録プロセスを開始できます。

- 招待状をメール送信する
- 登録用のURLにユーザーを導く

- エンドユーザーは、デバイス登録プロセスを開始する前に、Ivanti Neurons for MDM 内にアカウントを持っている必要があります。LDAPユーザーの場合、ConnectorとLDAPサーバーを設定し、LDAPサーバーからユーザーをインポートしておく必要があります。ローカルユーザーにとってこれは、ユーザーの追加を意味します。
- Ivanti Neurons for MDM の旧バージョンで生成されたデバイス登録URLは、最新バージョンでは機能しません。管理者は、デバイス登録用のデバイス登録URLを生成する必要があります。

招待状の送信

ほとんどの場合、まず招待状を送信することから登録プロセスを始めます。Ivanti Neurons for MDM では、エンドユーザーにデバイス登録を促す招待状を以下の方法で送信できます。

- [スタートアップウィザード] 内
- [1人以上のエンドユーザーを追加] する場合
- [ユーザー] ページ(**[アクション] > [招待状の送信]**) 内

エンドユーザーが招待状を見失ってしまった場合、デスクトップまたはラップトップ上で受信した場合、あるいは何らかの理由で受信し損ねた場合には、招待状にリストされたURLを送信することができます。サービスURLの末尾に**/go**を追加してください。

パスワード設定済みの Ivanti Neurons for MDM アカウントを所有しているエンドユーザーは、招待状がなくても登録プロセスを開始できます。招待状内にリストされているURL宛に送信できます。

エンドユーザー登録の完了

デバイスユーザーに、登録プロセスを完了する方法を伝えます。以下の指示をテンプレートとし、必要に応じて変更を加えてください。

手順

1. お使いのWindows 10+のPCのブラウザを開いてください。
2. mobileiron.com/goを開きます。
   登録URLが記載された新しいページに自動的に移動します。
3. 登録URLをクリップボードにコピーします。
4. **[設定]** ページの一番下にある **[アカウント追加]** をタップします。

5. 受け取った招待状に関連付けられているEメールアドレスを入力します。

   ユーザーのIvanti Neurons for MDMユーザー名がIvanti Neurons for MDMに入力されたユーザーのメールアドレスに一致しない場合は、メールアドレスの入力を求められたときにユーザー名を入力するようユーザーに伝えてください。

6. コピーしたWorkplaceサーバーURLを次のテキストフィールドに貼り付けます。
7. **[サインイン]** をタップします。
8. 次のフィールドにパスワードを入力します。
9. 他のフィールドは空白のままにします。
10. **[サインイン]** をタップします。
11. **[アカウント追加]** 画面の **[完了]** をクリックします。
    Workplace開始画面に、アカウントが追加されたことが表示されます。

Windows Autopilot

Windows Autopilotは、管理者が新しいデバイスを仕事で使えるようにするためのセットアップや事前設定に役立つMicrosoftの機能です。Autopilot機能は、WindowsデスクトップまたはHoloLens2デバイスの迅速で信頼性の高い、シームレスなプロビジョニングを支援します。さらにAutopilot機能は、以下のタスクの実行にも役立ちます。

- Azure Active Directory(AAD) へのデバイスの自動追加
- MDM サービスへのデバイスの自動登録
- デバイスの作成と、デバイスのプロファイルに基づく構成グループへの自動割り当て
- 登録体験のカスタマイズ
- 構成とポリシーの適用
- 必要なアプリケーションのインストール

Ivantiは、Autopilotプロファイルのすべてのモードに対応しています。

- ユーザー主導
- ユーザー主導の事前プロビジョニング(旧White Glove)

- 自己導入モード

詳細は「Windows Autopilotプロファイルの構成」ページ1202を参照してください。

デバイスのセキュリティおよび不正使用に関し、すべてのAutopilot Windowsデバイスは、TenantLockdown CSP機能を使用してテナントにロックすることができます。この機能を使用するには、Autopilotオプションを使用してデバイスを登録する必要があります。この構成は、デバイスレベルで適用されます。「TenantLockdown CSP」ページ1210を参照してください。

AAD 標準登録

ユーザがAADテナントに追加されると、勤務先アカウントから直接デバイスを登録できます。

手順

1. Windows デバイスで **[設定]** > **[アカウント]** > **[勤務先のアカウントまたは学校のアカウントにアクセス]** をクリックします。
2. [勤務先のアカウントまたは学校のアカウントの追加] を選択し、**[接続]** をクリックします。
3. 勤務先アカウントの電子メールアドレスを指定します。

デバイスは自動的にIvanti Neurons for MDMに登録されます。

PINでのパッケージ登録のプロビジョニング

管理者はSCCMまたはIvanti Endpoint Managerによって管理されているデバイスをIvanti Neurons for MDMに登録できます。配布パッケージツールを使用すると、ダウンタイムやエンドユーザの中断なく、Ivanti Neurons for MDM Modern ManagementへのWindowsデバイスの移行を合理化できます。シームレスな移行を実現するには、Ivanti Neurons for MDMコンソールから固有の配布パッケージをダウンロードし、既存の管理ツールまたはドメインを使用して配布します。パッケージが実行されると、エンドポイントはIvanti Neurons for MDMにサイレントに登録され、管理が継続されます。このアプローチにより、管理者はまずデバイスを簡単に移行し、その後、無線でデバイスを構成するという柔軟性が得られます。デバイスのIvanti Neurons for MDMへのサイレント登録が完了すると、そのデバイスはMDMと結合され、2つの管理権限によって共同管理されます。管理者がIvanti Neurons for MDM内で目的のWindows体験を構成したら、古い管理プラットフォームは廃止され、Ivanti Neurons for MDMがデバイスの唯一の管理機関となります。

デバイスがMicrosoft Endpoint Manager (MEM) (旧称 SCCM) から移行されている場合は、このルールが適用されません。既存のMEMクライアントは、MEMプラットフォームが廃止されるまで、(共同管理モードではなく) 共存モードで機能を継続します。共存モードを有効化すると、MEMクライアントは特定の機能を自動的に無効化し、それらのワークロードがIvanti Neurons for MDMによって提供されるようになります。詳細については、Microsoft の共存ドキュメントをご覧ください。

MEMおよび他のサードパーティ管理プラットフォームを使用した場合の具体的な動作に関し、Ivantiでは、まずお客様の環境でIvanti Neurons for MDM導入パッケージツールをテストすることをお勧めします。

前提条件

- ユーザアカウントは、LDAP、AD (AAD)、ローカルユーザアップロード、または他のID統合を使用して、Ivanti Neurons for MDMにインポートする必要があります。
- すべてのデバイスにはWindows Configuration Designerがインストールされている必要があります。
- PINに基づく登録を有効にするIvanti Neurons for MDM
- ユーザ名にはスペースを使用しないでください。これにより、ユーザデバイスの移行が失敗する場合があります。

  - このツールは、AADを利用しない環境に配布できます。
  - Ivanti Neurons for MDM Modern Windows管理スイートの主な要素はAADを必要としません。共同管理または共存には、移行中の影響を回避するために、サイレント登録時に特定のワークロード/構成を配布する必要があります。

- 配布パッケージは現在のところ、SCCMおよびIvanti Endpoint Managerでのみサポートされています。

手順

1. **[管理 > Windows > 配布パッケージ]** をクリックします。
2. **[ユーザ]** または **[ユーザグループ]** を選択してPINを生成し、**[配布パッケージのダウンロード]**(.zipファイル) をクリックします。
3. 配布パッケージはSCCM / Ivanti Endpoint Manager管理者に提供されます。管理者はパッケージを解凍して、該当する管理対象のデバイスに転送します。この手順を実行する方法については、構成マネージャのパッケージとプログラムをご参照ください。
4. 転送後、管理者がリモートでデバイスの `setup.ps1` スクリプトをトリガーします。スクリプトのトリガーについては、構成マネージャからのスクリプトと配布をご参照ください。
5. デバイスがIvanti Neurons for MDM上に登録されます。

ユーザーに対して生成されたPINは24時間のみ有効です。PINの有効期限が切れたら、新しいPINを生成する必要があります。

PINを含むファイルは、登録の試みが完了した後でデバイスから削除されます。

SCCM デバイスを登録する Ivanti Neurons for MDM

手順

1. 選択したユーザのIvanti Neurons for MDMから配布関連ファイルをすべてダウンロードします。
2. 登録するアカウントまたはグループを選択します。

3. SCCM を使用してクライアント デバイスにパッケージ ファイルを配布する:

    a. 必要なクライアントが SCCM に存在しているかどうかを確認します。Windows-configuration-designer がクライアントに存在しない場合、管理者はデザイナーをプッシュし、クライアントに配布する必要があります。

    b. SCCM サーバで、フォルダを作成し、配布 zip ファイルをコピーして、ファイルの内容を展開します。

    c. ファイルがクライアント デバイスに展開されるフォルダの内容をコピーする .bat ファイルを作成します。

    d. SCCM で **[ソフトウェア ライブラリ] > [アプリケーション管理] > [パッケージ]** に移動し、フォルダの内容をクライアントにコピーするパッケージを作成します。内容をコピーする保存先フォルダを入力します。

    e. パッケージをデバイスまたはデバイスの場所に配布します。

    f. [監視] セクションでは、配布ステータスを監視し、ファイルがクライアントの保存先フォルダにコピーされたことを確認できます。

4. スクリプトを実行してデバイスを登録する:

    a. **[ソフトウェア ライブラリ] > [スクリプト]** に移動し、スクリプトを作成します。

    b. スクリプトの名前を入力し、解凍されたフォルダから PowerShell スクリプト **setup.ps1** をインポートします。

    c. スクリプトを承認し、ターゲット デバイスでスクリプトを実行します。

    d. **[今すぐ開始]** を選択し、**[保存]** をクリックします。スケジュールされたタスクにより、スクリプトの実行が開始します。正常に実行されると、ステータスが緑色になります。

5. デバイス登録を検証するには、**[設定]** > **[プロビジョニング パッケージの追加と削除]** > **[詳細]** に移動します。

Ivanti Endpoint Manager デバイスを登録する Ivanti Neurons for MDM

手順

1. 選択したユーザの Ivanti Neurons for MDM から配布関連ファイルをすべてダウンロードします。
2. 登録するアカウントまたはグループを選択します。

ケース1: 同じユーザ名でデバイスを登録するには、デバイス名が考慮されます。この場合、電子メールアドレスは有効なユーザ電子メールアドレスではありません。ADドメインが付いたデバイス名の電子メールアドレスは登録電子メールアドレスと見なされます。管理者はアカウントをLocalSystemAccountに設定し、setup.ps1を主ファイルとして使用して、PowerShell実行を開始する必要があります。

ケース2: デバイスの場所のファイルの修正に関する制限がない場合、デバイスを登録するには、有効なユーザ電子メールアドレスが考慮されます。登録ではログインユーザの電子メールアドレスを使用します。この登録を有効にするには、管理者はアカウントを現在のユーザアカウントに設定し、setup.ps1を主ファイルとして使用して、PowerShell実行を開始する必要があります。

ケース3: デバイスの場所のファイルの修正に関する制限がある場合、デバイスを登録するには、有効な電子メールアドレスが考慮されます。登録ではログインユーザーの電子メールアドレスを使用します。このケースには、次の2つのサブケースがあります。

- 登録では2つのスクリプトを使用します。**setupEPMCopyContentsToTempFolderStep2.ps1** で別の配布パッケージを作成し、現在のユーザアカウントで実行します。ファイルは一時的な場所にコピーされます。**setupEPMCopyContentsToTempFolderStep2.ps1** で別の配布パッケージを作成し、Local System Accountで実行します。

  > パッケージファイルが含まれているフォルダの修正に関して、デバイスユーザーに制限がある場合。ファイルを一時フォルダにコピーし、ユーザーIDを確認して、PowerShellパッケージを作成します。PowerShell packageは**setupEPMCopyContentsToTempFolderStep2.ps1**スクリプトで実行されます。インストール後、一時フォルダは削除されます。

- UACを有効/無効にする

  a. レジストリエントリを更新して、UAC制御を無効にし、コンピュータを再起動する

  b. 現在のユーザのアカウントでsetup.ps1を使用して、PowerShellパッケージを実行する

  c. レジストリエントリを更新して、UAC制御を有効にし、コンピュータを再起動する

3. PowerShell パッケージを作成する:

   a. 必要なクライアントが Endpoint Manager に存在しているかどうかを確認します。

   b. ファイルを C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\ にコピーします。このフォルダ内でサブフォルダを作成し、ファイルを展開します。

   c. パッケージの作成: **[配布 > 配布パッケージ > 新規 > Windows > PowerShell]**。

   > 管理者は、デバイスで設定された制限レベルに基づいて、さまざまなデバイスにパッケージを配布できます。

   d. [主ファイル] セクションで、パッケージ名を入力し、ファイルがコピーされたフォルダから setup.ps1 をアップロードします。

   e. [追加のファイル] セクションで、**[追加]** を使用して残りのファイル (setup.ps1 スクリプト以外) をコピーします。

   f. [アカウント] セクションで現在のユーザーのアカウントを選択します。

   g. **[保存]** をクリックします。

4. スケジュールされたタスクを作成する:

   a. 作成したパッケージを選択し、右クリックして、**[スケジュールされたタスクの作成]** を選択します。スケジュールされたタスクが作成されている。

   b. デバイスをドラッグし、スケジュールされたパッケージ セクションに追加します。

   c. スケジュールされたパッケージを右クリックし、**[プロパティ]** を選択します。

   d. パッケージを検証します。

   e. [タスク タイプ] の下で **[プッシュ]** を選択します。

   f. **[今すぐ開始]** を選択し、**[保存]** をクリックします。スケジュールされたタスクにより、スクリプトの実行が開始します。正常に実行されると、ステータスが緑色になります。

5. デバイス登録を検証するには、**[設定]** > **[プロビジョニング パッケージの追加と削除]** > **[詳細]** に移動します。あるいは、管理者がデバイスの診断ログの下でデバイス登録を検証できます。

Windows デバイスでの一括登録の使用

一括登録機能では、Ivanti Neurons for MDM で複数のAndroidデバイスを迅速に登録できます。

前提条件：

- Azure AD (AAD) Premium アカウントを使用して、ユーザアカウントを Ivanti Neurons for MDM でインポートする必要があります。
- すべてのデバイスには Windows Configuration Designer がインストールされている必要があります。

手順：

1. Ivanti Neurons for MDM とAAD テナントを関連付けます。Windows 10デバイスにおけるAADとUEMの連携をご参照ください。
2. **[Windows Configuration Designer]** アプリを使用して、**[デスクトップデバイスのプロビジョニング]** を選択します。画面で [新しいプロジェクト] ウィンドウが表示されます。
3. 以下の情報を入力します。
   - 名前 - プロジェクトの一意の名前
   - プロジェクト フォルダ - プロジェクトを保存するデバイスの場所
   - 説明 - 任意のプロジェクトの説明
4. **[完了]** をクリックすると、[新しいプロジェクト] ウィンドウが閉じ、一連のステップが実行されます。

   デバイスのセットアップ

5. デバイスの一意の名前を入力します。名前には、シリアル番号 (%SERIAL%) またはランダムな文字を含めることができます。
6. Windows をアップグレードしているか、共有するデバイスを構成しているか、プリインストール済みソフトウェアを削除している場合は、任意でプロダクトキーを入力できます。

   ネットワークの設定

7. 任意で、初回の起動時に、接続する Wi-Fi ネットワークデバイスを構成できます。ネットワークデバイスが構成されていない場合は、デバイスの初回の起動時に、有線ネットワーク接続が必要です。

   アカウント管理

8. **[Azure AD で登録]** を選択し、**[一括トークンの有効期限]** を入力して、**[一括トークンの取得]** をクリックします。
9. Azure AD 認証資格情報を入力し、一括トークンを取得します。

10. **[すべてのアプリのサインイン状態を維持]** ページで **[いいえ。このアプリにのみサインイン]** をクリックします。

    - 一括トークンが正常に取得されたら、[次へ] をクリックして、パッケージを作成します。
    - Azure ポータル - ユーザプリンシパル名 (package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com など) でユーザとプロビジョニング パッケージが作成されます。ファイル (ランタイム ppkg ツール) をストレージデバイスにコピーします。

    > 一括トークンを作成する AAD ユーザ。パッケージ ユーザの多要素認証を有効にしないでください。確認するには、そのユーザーについてOOBEとAAD Joinを実行する必要があります。

11. (Azure で作成された) パッケージ ユーザを作成し、Ivanti Neurons for MDM と同期します。

プロビジョニング パッケージに含まれるフラッシュドライブを使用して、デバイスを一括登録します。既存のデバイスをダブルクリックすると、OOBE 後のエクスペリエンスを実行することもできます。最初の試行でパッケージをインストールできなかった場合は、2 回目の試行も失敗します。新しいデバイスが Ivanti Neurons for MDM で作成され、AAD がパッケージユーザに属しているかどうかを確認します。

パスコード設定の変更

このセクションは以下のトピックを含みます。

- 「割り当てられたパスコード構成の変更」下
- 「異なるパスコード構成の割り当て」下

デバイスに割り当てられた [パスコード構成] を使用し、パスコード設定を変更します。以下の操作が行えます。

- 割り当てられた構成の設定を変更する

  または

- 異なるパスコード構成を割り当てる

構成に対して行った変更は、その構成が割り当てられているすべてのデバイスに影響します。

割り当てられたパスコード構成の変更

手順

1. **[デバイス]** を開きます。
2. リスト内のデバイスのエントリを探します。
3. **[名前]** カラム内のリンクをクリックします。

   パスコード構成が割り当てられている場合は、それが [構成] タブに表示されます。

4. [構成] タブで **[パスコード構成]** リンクをクリックします。
5. **[編集]**(右上)をクリックします。
6. 変更を加えます。

異なるパスコード構成の割り当て

手順

1. 必要な構成を誰かが作成済みであることを確認します。
2. **[デバイス]** を開きます。
3. リスト内のデバイスのエントリを探します。
4. **[名前]** カラム内のリンクをクリックします。

デバイス名の変更

管理者は手動でデバイス名を変更できます(構成のデバイス名編集を使わずに)。

対象:

- iOS監視対象デバイス
- macOS 10.10+デバイス

手順

1. **[デバイス]** を開きます。
2. リスト内のデバイスのエントリを探します。
3. 以下のいずれかの手順を実行してください。
   - **[デバイス名]** のカラムがない場合は、右側の設定アイコン(歯車)をクリックし、**[デバイス名]** を選択して追加します。
   - **[名前]** カラム内のリンクをクリックすると、デバイス詳細ページが表示されます。
4. デバイス名の横にある鉛筆型の **[編集]** アイコンをクリックします。
5. 新しいデバイス名を入力し、チェックマークをクリックします。
6. [デバイス名を上書き] ディスプレイボックスの説明を確認し、**[OK]** をクリックします。

変更された名前はデバイスの次のチェックイン時にプッシュされます。このアクションは元に戻せません。

[デフォルトデバイス名] がすでに構成で設定されている場合、このアクションによって名前が上書きされます。

デバイスの検索とフィルタリング

このセクションは以下のトピックを含みます。

デバイスの検索

ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM管理ポータルには、重複するユーザーグループ数と、重複するグループを識別するGUID番号が表示されます。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

手順

1. **[デバイス]** を開きます。
2. **[検索]** フィールドにデバイス名を入力します。その文字列を含むすべてのデバイスがリストされます。

デバイスのフィルタリング

フィルタのサイドナビゲーションバーには、さまざまなセクションが表示され、デバイスの一覧全体から特定のデバイスを検索できます。[フィルタの管理]ウィザードには、すべてのセクションが表示され、フィルタのナビゲーションバーに表示するセクションを選択できます。

手順

1. **[デバイス]** を開きます。
2. フィルタのサイドナビゲーションバーの一覧にあるセクションの該当するチェックボックスをクリックします。
   例:
   - **ユーザー有効化** のセクションから **[はい]** を選択し、ユーザーが有効状態にあるデバイスのみを表示します。

- カスタム属性をデバイスに割り当てている場合は、設定アイコン(右上)をクリックするとこれらの属性に基づいてデバイスを絞り込むことができます。
- **状態**セクションで **[撤去]** と **[iOS]** を選択すると、撤去されたiOSデバイスのみ表示されます。

3. (任意) **[既定値の復元]** をクリックすると、選択内容が既定のフィルタに復元されます。フィルタナビゲーションバーには、選択したセクションが表示されます。[フィルタの管理] ウィザードですべてのチェックボックスをオフにした場合は、フィルタのサイドナビゲーションバーにすべてのセクションが表示されます。
4. [フィルタの管理] ウィザードの外の任意の場所をクリックすると、ウィザードが終了します。
5. (任意) フィルタのサイドナビゲーションバーを閉じるにはxアイコンをクリックします。サイドナビゲーションバーをもう一度開くには、**[フィルタ]** をクリックします。

> ◦ stopwords.txtファイル(Apache SOLRサーバ構成に含まれる)のリストで定義されているストップワードのいずれかを使用した場合、その単語にはインデックスが作成されません。このため、ストップワードを含むエンティティは、検索結果に表示されません。
>
> ◦ エンティティには、デバイス、ユーザー、グループ、属性、アプリケーション、証明書、監査証跡、コンテンツ、通知モジュールなどがあります。
>
> ◦ ストップワードには、a、an、if、be、intoなどがあります。

詳細検索の使用

詳細検索のオプションでは、ルールに基づいてデバイスを検索し、具体的な基準でデバイスの識別と表示が可能です。ルールは、「は次から始まる:」、「は次で終わる:」、「は次を含む:」、「は次を含まない:」、「は次から始まらない:」、「は次で終わらない:」、「は次より小さい:」、「は次より大きい:」、「が次の範囲内:」、「は次と等しい:」、「は次と等しくない:」などの演算子を使用して作成します。[ANY (OR)] または [ALL (AND)] オプションを使用すれば、ルールオプションをネストでまとめることができます。ルールに一致するデバイスは、セクションの下に表示されます。

ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM管理ポータルには、重複するユーザーグループ数と、重複するグループを識別するGUID番号が表示されます。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

手順

1. [デバイス] ページから **[詳細検索]** リンクをクリックします。[詳細検索] ウィザードが開きます。
2. 次のオプションのいずれかをクリックします。

- デバイスが少なくとも1つのルールを満たす必要がある場合は、**[いずれか]** をクリックします。
- **すべて**-デバイスはすべてのルールと一致する必要があります。

3. 検索基準を定義するルールを作成します。**例：**「APNS対応は次と等しい：はい」。
4. (任意) **[+]** をクリックし、必要に応じて他のルールを作成します。
5. **[検索]** をクリックします。検索基準に一致するデバイスのリストがページに表示されます。

> - iOS 14.0+デバイスの場合、デバイスのeSIM ID(EID) はデバイス詳細ページに表示されます。eSIM ID(EID) では、通信会社が特定のデバイスにSIMを割り当てることができます。eSIM ID(EID) フィールドはGDPR対応です。
> - 新しいGDPRフィールド(IPアドレス、eSIM IDなど) がIvanti Neurons for MDMリリースで追加され、新しいフィールドを非表示にしたい場合、すでにGDPRを構成済みの管理者はGDPRプロファイルを編集する必要があります。
> - [詳細検索] には、デバイスのリカバリロックのステータスが表示されます。

検索クエリのロード

保存した検索クエリのリストを表示できます。

手順

1. [詳細検索] をクリックし、フォルダアイコンをクリックします。**[クエリを読み込む]** セクションに、作成された検索クエリのリストが表示されます。次の詳細が表示されます。
   - **クエリ名** - 読み込まれたクエリの名前。
   - **クエリの内容** - 検索クエリを定義するルールの内容を表示します。
   - **アクション** - クエリに実行するアクションを選択します。
2. **[アクション]** カラムの **[クエリを読み込む]** をクリックすると、読み込まれたクエリに定義された基準に一致するデバイスのリストが表示されます。
3. **[削除]** をクリックすると、読み込まれたクエリが削除されます。

デバイス所有者の使用

このセクションは以下のトピックを含みます。

- 「QRコードまたはNFCバンプを使用したAndroid Enterpriseデバイスのプロビジョニング」次のページ
- 「クライアントトークンを使用したAndroid Enterpriseデバイスのプロビジョニング」ページ231

ライセンス: Gold

デバイスは、登録後、会社所有または従業員所有に指定できます。この指定は、ユーザーが使用しているデバイスが個人所有なのか会社所有なのかに基づくポリシーの管理に役立ちます。正しいライセンスがあれば、デバイスグループ作成のルールに所有者を利用できます。

新規デバイスまたは工場出荷時設定にリセットしたデバイスでは、Provisionerアプリを使用し、以下のいずれかの方法でデバイス所有者モードをプロビジョニングします。

- NFC(Near Field Communication) バンプ
- QRコード読み取り

NFCバンプでは、新規デバイスまたは工場出荷時設定にリセットしたデバイスに対してマスターまたはテンプレートデバイスをタップし、プロビジョニングします。

QRコード読み取りでは、新規デバイスまたは工場出荷時設定にリセットしたデバイスの画面をタップしてWi-Fiネットワークを構成し、デバイスのプロビジョニング準備ができたらコードを読み取ります。

NFCまたはQRコードを使用してデバイス所有者モードのプロビジョニングをする際、プロビジョナーアプリが登録トークンを受け入れます。登録時に、この登録トークンがサーバーに送信されます。これがサーバーにあり、デバイスがユーザーに割り当てられた場合に限り、デバイスが正常に登録されます。

デバイス所有者モードになると、Goクライアントがデバイスを制御し、デバイスがIvanti Neurons for MDM に登録されてユーザーがプロビジョニングプロセスを終了できなくなるまで画面をロックします。デバイス所有者モードはキオスクモードもサポートします。構成については、ロックダウン& キオスク構成を参照してください。

重要

- デバイス所有者モードでデバイスを撤去すると、デバイスは工場出荷時設定にリセットされます。
- デバイス所有者モードのすべてのデバイスは、任意ですべてのシステムアプリを有効化できます。
- 1つのデバイスで同時にアクティブにできるデバイス所有者モードは1つだけです。

- Android Enterprise対応のデバイスのみを、デバイスオーナーモードにプロビジョニングできます。
- デバイス所有者モードのSamsung Knox Standardデバイスの場合、Samsung ELMライセンスをアクティベートするようユーザーにプロンプトが表示されます。このプロンプトは、デバイス所有者モードのSamsungデバイスで、Goクライアントアプリが旧リリースからIvanti Neurons for MDMがサポートする最新リリースのバージョンにアップグレードされたときにも表示されます。アクティベートの後は、[デバイス設定] > [シリアル番号] フィールドに表示されるのと同じシリアル番号がデバイス詳細ページに表示されます。

QRコードまたはNFCバンプを使用したAndroid Enterpriseデバイスのプロビジョニング

QRコードまたはNFCバンプを使用してAndroid Enterpriseデバイスをプロビジョニングするには、Google Playからプロビジョナーアプリをダウンロードし、マスターデバイスにインストールする必要があります。

互換コンポーネント

Provisionerバージョン: 1.3.0

Provisionerは以下と互換性を持つ、または協調して動作します。

項目	バージョン
Android OS (プロビジョニングされるデバイス)	• NFCを使用する場合、5.0またはサポートされる以降のバージョンが必要。 • QRコードを使用する場合、7.0またはサポートされる以降のバージョンが必要。 デバイスはAndroid Enterprise対応でなければなりません。
Android OS(マスターデバイス)	5.1から最新版まで。 NFCバンプを使用する場合、デバイスにNFC機能が必要です。QRコードの場合は必要ありません。
Android Enterpriseで有効な、UEMサーバー製品	次のいずれかです。 Ivanti Neurons for MDM、または許可のラベルが付けられたIvanti Neurons for MDM。
Androidクライアントアプリ	Provisionerにより、クライアントアプリの最新バージョンがプロビジョニングされたデバイスに自動的にインストールされます。

前提条件

Android Enterprise デバイスを仕事用マネージド デバイスとしてプロビジョニングするには、次のことが必要です。

- Android Enterprise関連の必要な構成が定義されていて、登録済みのデバイスに適用されるようにすること。

  デフォルトのAndroid Enterprise：仕事用マネージド デバイス構成をデバイスで有効化すること。

- サーバー上でAndroid Enterpriseを有効化すること。
- ProvisionerアプリをインストールしたNFC対応Androidデバイス(NFCを使用する場合のみ)をマスターにす

ること。

- Android Enterprise対応のデバイスをプロビジョニングすること

Androidビームを有効化してNFCバンプを利用するには：

手順

1. デバイスの **[設定]** に進みます。
2. **[ネットワーク]** > **[無線ネットワーク]** を開きます。
3. **[接続]** セクションで **[共有 & 接続]** を選択します。
4. **NFC** スイッチを **[オン]** にします。
5. **[Androidビーム]** スイッチを **[オン]** にします。

AndroidビームとNFCを有効化する手順はデバイスによって異なる場合があります。

仕事用マネージドデバイスとなるAndroid Enterpriseデバイスのプロビジョニング

手順

1. AndroidマスターデバイスでGoogle PlayからProvisionerアプリをダウンロードし、インストールします。
2. マスターデバイス上でProvisionerを起動します。
3. プロビジョニング方法としてNFCまたはQRコードを選択します。
4. **[プロビジョニングするアプリ]** をタップし、プロビジョニングするデバイスにインストールするクライアントアプリを選択します。

このクライアントアプリを選択：	このUEMサーバーに登録：
実施	Ivanti Neurons for MDM
At Work UEM	(許可ラベルの) Ivanti Neurons for MDM

5. Provisionerアプリの残りのフィールドを入力します。対応しているWi-Fiタイプが存在する場合は、一部のフィールドが自動入力されます。QRコードを選択した場合、Wi-Fiフィールドは表示されません。次のガイドラインに従います。

フィールド	利点
プロビジョニングのアプリを選択	GoまたはAt Work
タイムゾーン	デバイスに設定するタイムゾーンを入力します。
ロケール	デバイスに設定するロケールを入力します。
すべてのシステムアプリを有効化	チェックボックスをクリックしてすべてのシステムアプリを有効化します。
Wi-Fiネットワーク SSID	ターゲットデバイスが使用するWi-Fi SSIDを入力します。
Wi-Fiセキュリティの種類	Wi-Fiセキュリティの種類を入力します。
Wi-Fiのパスワード	Wi-Fiのパスワードを入力します。
バルク登録	一括登録機能は任意です。一括登録を使用するには、ホスト名が必要です。ユーザー名を入力し、クイックスタートオプションを選択することも可能です。一括登録機能をスキップするには、フィールドを空白で残します。

6. **[続行]** をタップします。

7. **[NFC]** を選択した場合、**[続行]** をタップします。マスタデバイスに **[デバイスを動かしてください]** が表示されます。下の **[NFCバンプ]** セクションに進んでください。

   [QR コード] を選択すると、マスタデバイスの画面に [**この QR コードをスキャンしてください**] が表示されます。下の **[QRコード]** セクションに進んでください。

   NFCバンプの場合、下記手順を使用

8. ターゲットデバイスがAndroidのようこそ画面を表示していることを確認します。
9. スターデバイスと対象デバイスの背面同士を合わせ、NFC転送を開始します。NFC転送が成功すると対象デバイスから音が鳴り、クライアントアプリのダウンロードが始まります。Wi-Fi接続が確立できない場合、またはデバイスがクライアントアプリをダウンロードできない場合、デバイスは自動的に工場出荷時の状態にリセットされます。
10. ようこそ画面以外の画面が表示されたり、音が鳴ったりしたら、デバイスを離してかまいません。通常、数秒で終了します。デバイスが暗号化されていない場合は、続行前に暗号化プロセスが始まります。

    デバイスをマスターデバイスに「バンプ」することで、引き続き他のデバイスをプロビジョニングできます。ターゲットデバイスに [ようこそ] 画面が表示され、マスタデバイスには [デバイスを動かしてください] 画面が表示されます。

    QRコードプロビジョニングの場合、下記手順を使用

11. ターゲットデバイスがAndroidのようこそ画面を表示していることを確認します。
12. ターゲットデバイスのAndroidのようこそ画面の同じ場所を6回タップします。
13. プロンプトに従い、WiFiネットワークを構成すると、セットアップウィザードがターゲットデバイスにQRリーダーをダウンロードします。
14. QRリーダーがダウンロードされると、カメラが起動します。
15. ターゲットデバイスをマスターデバイスの数センチ上に持ち、QRコードを読み取らせます。セットアップウィザードがクライアントアプリのダウンロードに進みます。クライアントアプリをダウンロードできない場合、デバイスは自動的に工場出荷時の状態にリセットされます。
16. マスターデバイスのQRコードを読み取ることで、引き続き他のデバイスをプロビジョニングできます。ターゲットデバイスはスキャンのためのカメラが準備されている必要があります。マスタデバイスには [このQRコードをスキャンしてください] 画面が表示されます。
17. QRコードは [共有] アイコンをタップしてエクスポート可能です。エクスポートのオプションはデバイスによって異なります。

クライアントトークンを使用したAndroid Enterpriseデバイスのプロビジョニング

NFCバンプやQRコードによる方法を使用する代わりに、ブランドを冠したクライアントトークンを使用して、デバイス所有者モードでAndroid Enterpriseデバイスをプロビジョニングできます。この方法では、トークンでデバイスにサインオンし、デバイス所有者モードでGoまたはAt Workクライアントの自動インストールとプロビジョニングを簡単に行います。

Android 6またはサポートされる以降のバージョンを使用してマネージドGoogle Playアカウントでプロビジョニングされたデバイスでは、ブランド入りのクライアントトークンがサポートされます。詳細は「Android UEM Developers」のガイドをご覧ください。https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

この方法を使用するための要件：

- Android Enterpriseアカウントで登録されていること。
- デバイスがAndroid Enterprise対応であること。
- デバイスがAndroid 6から最新版までを使用していること。
- 新規デバイスまたは工場出荷時設定にリセットしたデバイスであること。

構成（Android 5.0+を実行するデバイス）：

手順

1. Ivanti Neurons for MDMポータルで **[構成]** を開きます。
2. **[+追加]** をクリックします。
3. **[ロックダウン＆キオスク：Android Enterprise]** を選択します。

   [ロックダウン＆キオスク：Android Enterprise構成の作成] ページが表示されます。
4. 構成名と説明を入力します。

   ロックダウンの種類を選択します。
5. **[仕事用マネージドデバイス（デバイス所有者）]** をクリックします。

   Androidデバイス所有者ロックダウン設定のオプションが表示されます。

   任意で以下を選択します。

   - Wi-Fiを無効化、またはWi-Fi設定を無効化
   - カメラを無効化
   - Bluetoothを無効化
   - Bluetooth設定を禁止

- スクリーンキャプチャを無効化
- マスターボリュームをミュート
- アプリ制御を禁止
- 認証情報を禁止
- 緊急ブロードキャストを禁止
- モバイルネットワークを禁止
- テザリングを禁止
- VPNを禁止
- 工場出荷時設定へのリセットを禁止
- 工場出荷時設定へのリセットを有効化。

  > 工場出荷時設定へのリセットの後でデバイスをプロビジョニングできる許可済みのGoogleアカウントID(整数値)のリストを指定することも可能です。またはヘルプアイコンの上にマウスを置くと、許可済みアカウントの取得方法が表示されます。

- アカウント変更を禁止
- NFC(ビーム発信)を無効化
- 発信を禁止
- セーフブートを禁止
- 位置情報共有を禁止
- デバッグ機能を禁止
- アプリ検証を確認
- SMSを禁止
- マイクのミュート解除を禁止
- オートタイムを無効化
- オートタイムゾーンを無効化

- データローミングの無効化
- Wi-Fiスリープを無効化
- 入力方法を制限
- アクセシビリティサービスを制限
- USBファイル転送を無効化
- 外付けメディアを無効化
- キーガードを無効化(PIN/パスコードが設定されている場合は無効)
- 電源接続時に画面のオン状態を維持
- ウィンドウの作成を禁止
- 最初の使用ヒントをスキップ

6. **[システムアプリを有効化/無効化]** セクションでは、以下のシステムアプリの有効化または無効化を選択することも可能です。

項目	バージョン
システムアプリのプリセット	
ビルトインカメラ	トグルボタンをクリックし、ビルトインカメラアプリを**ON**または**OFF**にします。
ビルトイン電話	トグルボタンをクリックし、ビルトイン電話アプリを**ON**または**OFF**にします。
システムアプリパッケージ名	プリセットシステムアプリ以外のシステムアプリを有効化または無効化する場合は、「+」アイコンをクリックし、システムアプリパッケージ名を追加します。システムアプリを削除するには、「-」アイコンをクリックします。

任意で **[キオスクモード]** を有効化します。

次の設定が表示されます。

- タスクモードのロックを有効化
- キオスクを自動で入力(初期セットアップ時のみ)
- クイック設定を無効化
- ユーザーがWi-Fiの設定にアクセスできるようにする
- ユーザーがBluetoothの設定にアクセスできるようにする
- ユーザーが位置情報の設定にアクセスできるようにする
- ユーザーによるアプリケーション更新延期を許可
- ユーザーが日時設定にアクセスできるようにする
- ユーザーがネットワークの設定にアクセスできるようにする
- ユーザーによる言語の選択を許可
- 共有デバイスを有効化(以下のオプションを選択)
  - ログインを有効化
  - ログアウトを有効化(タイムアウト設定を時間単位で指定)

7. 任意でデフォルトまたはカスタムブランディングオプションをドロップダウンリストから選択します。
8. 任意でキオスクモードを終了するためのキオスク終了PINを作成します。
9. 任意でキオスクモードでユーザーが利用できるアプリの許可リストを作成します。

デバイスのプロビジョニング

手順

1. デバイスの電源を入れ、Wi-Fiパスワードを入力します。デバイスが別のパスワードを入力するよう求める場合があります。
2. **[アカウント検証]** 画面でAndroid Enterpriseトークンを入力します。**[次へ]** をクリックします。
3. **[Googleサービス]** 画面で **[インストール]** をクリックします。
4. 利用規約を承諾します。

5. [仕事用デバイスのセットアップ] 画面で **[次へ]** をクリックします。GoまたはAt Workクライアントがデバイスにダウンロードされ、インストールされます。これでデバイスがデバイス所有者モードになります。

関連トピック

- Android一括登録の使用
- デバイスグループ

仕事用プロファイルを持つマネージドデバイス

会社所有デバイス上の仕事用プロファイルを持つマネージドデバイスとは、企業所有のAndroidエンタープライズデバイスで、個人データを他のデータと分離した状態のデバイスです。このモードは2種類のプロファイルをサポートします。仕事用アプリはマネージドプロファイルに、個人用アプリはユーザープロファイルに導入します。会社所有デバイス上の仕事用プロファイルを持つマネージドデバイスのモードは、デバイス所有者モードにプロビジョニングされたデバイスに仕事用プロファイルを持つマネージドデバイスの構成を配布することで作成されます。

仕事用プロファイルを持つマネージドデバイスのロックダウン設定については、「ロックダウン＆キオスク: Android Enterprise」ページ571をご覧ください。

このモードでは、Android 8.0以降(最新版まで)が必要です。

アプリの構成、複数のプロファイルにわたるアプリのウィジェット共有、クライアント証明書エイリアス、ID証明書は、仕事用プロファイルを持つマネージドデバイスに適用可能です。

以下の構成は、仕事用プロファイルを持つマネージドデバイスに適用可能です。

- アドバンストパスコード
- Always-on VPN
- 証明書
- ID証明書
- Googleアカウント
- パスコード
- Samsungフォンの制約
- 脅威防御
- Wi-Fi
- デフォルトのアプリランタイム許可
- SafetyNet認証
- パスコード
- Threat Defenseローカルアクション

Android一括登録の使用

一括登録機能では、Ivanti Neurons for MDM で複数のAndroidデバイスを迅速に登録できます。

ライセンス: Silver

一括登録を使用する前に次のタスクを実行してください。

1. Android Debug Bridge(adb) を含むAndroid SDKを、デバイス構成に使用するコンピュータ上にインストールします。
   Android Debug Bridgeの詳細については、http://developer.android.com/tools/help/adb.htmlをご覧ください。

2. USBデバッグを有効化します。
   Androidデバイス上でUSBデバッグを有効化する手順は、Androidのリリースによって異なります。USBデバッグの有効化に関する詳細については、http://developer.android.com/tools/device.htmlを参照してください。

3. 各デバイスにGoクライアントをインストールします。

4. USBケーブル経由でデバイスを登録に使用するプロビジョニングコンピュータに接続します。

Goを起動し、Android Debug Bridge(adb) シェルを使用してサーバーに登録することができます。Android Debug Bridgeは、WindowsまたはiOSターミナルユーティリティのコマンドラインから使用できるツールです。これを使用することで、接続されたAndroidデバイスと通信できるようになります。adbシェルからのコマンドフォーマット:

> adb shell

```
$ am start -a android.intent.action.MAIN -d
"mirp://na1.mobileiron.com?key=value&key=value" -n
com.mobileiron.anyware.android/com.mobileiron.polaris.manager.ui.StartActivity
```

登録する関連データのエンコードには、登録プロトコル(**mirp**) が使用されます。

有効なキーと値:

キー	利点
ユーザー	iRegを使用する場合は、ユーザー名フィールドに入力されるユーザーのメールアドレス。 必須.
パスワード	ユーザーのパスワード
pin	ユーザーの登録PIN
quickStart	**[TRUE] にセットすると、スプラッシュ画面が表示されますが、すぐに表示が消えます。**ようこそ画面でスピナーが [続行] ボタンに変わると、[続行] をタップしなくても自動的に画面が切り替わります。また、この合理化されたプロビジョニングフローは全デバイスで生じます。 • プライバシーとショートカットに関するユーザープロンプトは省略されます。 • Zebraデバイスでは、ユーザープロンプトなしにクライアントが自身に管理者特権を与えます。必要最小バージョンはZebra MX 4.3です。 **[FALSE] にセットすると、スプラッシュ画面が通常通りに表示され、ようこそ画面を表示するには [続行] をタップしなければなりません。**オプション。デフォルトは [FALSE] となっています。

一括登録には、パスワード、PINまたはトークンの使用が求められます。

このコマンド例では、サーバー、ユーザー、パスワード、PIN、quickStartが指定されています。

```
am start -a android.intent.action.MAIN -d
"mirp://ppp183.auto.mobileiron.com?user=miadmin@auto0001.mobileiron.com&passwo
rd=P@$$W0R3&pin=12345&quickStart=true" -
n com.mobileiron.anyware.android.qa/com.mobileiron.polaris.manager.ui.StartAct
ivity
```

一括登録スクリプトの例

自分で一括登録スクリプトを作成する際、このスクリプト例を利用することができます。このスクリプト例では、プロビジョニングマシンに接続されているすべてのデバイスを同じユーザーとパスワードで登録することになります。

```
for i in `adb devices | grep -v devices |

do

    echo "Registering $i"

    adb -s $i shell "am start -a android.intent.action.MAIN -d
\"mirp://<servername?user=user email addresspassword=password

done
```

考えられるエラーメッセージ

一括登録の使用時に発生する可能性のあるエラーを次に紹介します。

エラー	解決策
mirpスキームが見つかりません	mirpスキームを使用するコマンド例：`am start -a android.intent.action.MAIN -d "xxxmirp://?`
URLが無効です	データ文字列が送信されていない場合に発生します。URLが正しいことを確認してください。
サーバー情報が見つかりません	サーバー情報がないか、正しく入力されていません。
ユーザー情報が見つかりません	ユーザーキーが入力されていることを確認してください。
パスワード/PIN情報が見つかりません	PINまたはパスワードキーが入力されていることを確認してください。

CSVファイルのアップロードを使用するデバイスの一括登録

一括登録では、デバイス識別子を使用し、複数のAndroidデバイスを登録できます。CSVファイルをアップロードし、デバイスを一括で追加できます。

手順

1. **[デバイス]** ページで **[一括登録]** タブをクリックします。**[一括登録]** ページが表示されます。
2. **[追加]** をクリックします。
3. **[プロファイル名]** テキストフィールドで、プロファイルの名前を入力します。任意で **[+説明を追加]** をクリックし、CSVファイルの説明を入力します。
4. **[CSVをアップロード]** セクションで、**[CSVテンプレートをダウンロード]** をクリックし、CSVテンプレートをダウンロードします。既存の形式を使用し、ファイルを編集してデバイスを追加できます。

   一括登録 CSV では一度に最大 200000 を登録できます。

5. CSVファイルを編集し保存したら、**[CSVをアップロード]** をクリックし、CSVファイルをアップロードします。アップロードの成功を示すメッセージが表示されます。

   行に含まれている情報が不十分であると、CSVのアップロードが失敗する場合があります。各レコードには、少なくともシリアル番号とメーカー情報、またはIMEI値が含まれている必要があります。

   追加したCSVファイルを削除するには、「-」アイコンをクリックします。別のCSVファイルを選択してアップロードするには、**[別のファイルを選択]** リンクをクリックします。

6. オプション: **[トークンなしの一 括 アップロードとカスタム属 性 の割り当 て]** を選 択 すると、トークンの生 成 なしにすべての種 類 のデバイスを一 括 登 録 できます。このオプションがデフォルトで選 択 されていません。

   トークンなしの一 括 登 録 は、IMEIまたはシリアル番 号 とメーカー名 の組 み合 わせ(カスタム属 性 の有 無 に関 係 なく) がアップロードされたCSVファイルに記 載 されている場 合 にも適 用 可 能 です。しかし、デバイスの登 録 は、CSVファイルでアップロードされた属 性 値 の正 しさによって決 まります。以 下 の表 は、一 括 登 録 に入 力 された属 性 値 の組 み合 わせに基 づく結 果 のシナリオを説 明 したものです。

シナリオ	入 力 した属 性 値			デバイス登 録 ステータス
	IMEI	シリアル番 号	メーカー	
1。	正	誤	誤	デバイスが登 録 される
2	誤	正	正	デバイスが登 録 される
3	誤	誤	正	デバイスが登 録 されていません
4	誤	正	誤	デバイスが登 録 されていません

   メーカー名 は大 文 字 と小 文 字 を区 別 しません。

7. **[ユーザーの選 択]** フィールドでは、任 意 でユーザーを選 択 できます。
   [登 録 トークン] カラムに登 録 トークンが表 示 されます。登 録 トークンを再 読 み込 みするには、**[再 読 み込 み]** をクリックします。
   [トークン有 効 期 限] カラムにトークンの有 効 期 限 が表 示 されます。トークン有 効 期 限 を延 長 するには、**[延 長]** をクリックします。トークンを延 長 する日 数 を **[延 長 日 数]** フィールドに入 力 します。

   指 定 する日 数 は、7～99の範 囲 とします。デフォルトのトークン有 効 期 限 は、7日 です。
   [トークンなしの一 括 アップロードとカスタム属 性 の割り当 て] のオプションを選 択 した場 合 、このページは表 示 されません。

8. **[完 了]** をクリックします。

アップロード後 、アップロードしたCSVファイルの以 下 の詳 細 が **[プロファイルの一 括 登 録]** ページの表 に表 示 されます。

設定	説明
プロファイル名	プロファイルの名前。
説明	プロファイルの説明。
前回の変更	CSVファイルの前回の変更日。
タイプ	プロファイルの情報。既定では、[自己管理]に設定されています。
デバイスの数	一括登録対象のデバイスの数。
関連ユーザー	関連ユーザーの名前。ユーザーを変更するには、**[ユーザーを変更]** リンクをクリックします。
アクション	以下のアクションのいずれかを実行できます。 **既存のインベントリをダウンロード** - このボタンをクリックすると、プロファイルで使用可能なすべてのデバイスの詳細情報がダウンロードされます。 **表示** - このリンクをクリックすると、一括登録のためにアップロードしたプロファイルの詳細が表示されます。 **編集** - プロファイル詳細情報を編集します。1つのデバイスオプションが選択されているときにのみ使用できます。 **削除** - このリンクをクリックすると、アップロードしたプロファイルが削除されます。確認ウィンドウで、**[はい]** をクリックし、アップロードしたプロファイルの削除を確定します。

CSVファイルのアップロード中に生成されたトークンを登録に使用する必要があります。誤ったトークンを入力すると、通常のIRegフローにリダイレクトされ、IDとパスワードの入力が必要となります。

アクション

[プロファイル詳細の表示] セクションで一括登録プロファイルを表示するときに、[プロファイル詳細の表示] ページにある [アクション] タブから他のタスクを実行できます。

- **さらにデバイスを追加** - このオプションを使用して、その他のデバイスをプロファイルに追加できます。**IMEI番号**、**製造元**、**シリアル番号**、**カスタム属性**情報を入力する必要があります。入力したら、**[保存]**をクリックします。
- **構成の修正** - このオプションを使用して、既存の構成を修正できます。**Ivanti 固有の鍵**を追加し、**[定義済みの Android System Extras]** または **[カスタム Android システム キー]** に変更して、**[更新]** をクリックします。
- **QR コードを生成** - このオプションを使用して、プロファイルに一括登録で使用する QR コードを生成します。
- **トークンを更新** - トークンを更新するか、トークンの有効期間を延長します。
- **削除** - 選択したプロファイルからデバイスを削除します。デバイスを選択し、[削除] ボタンをクリックすると、確認ポップアップが画面に表示されます。**[削除]** をクリックします。
- **編集** - 選択したプロファイルからデバイスを編集します。デバイスを選択して、**[編集]** ボタンをクリックする必要があります。

Samsung KNOX Mobile Enrollmentの使用

Samsung Knox Mobile Enrollmentでは、条件を満たすSamsungデバイスを管理者がIvanti Neurons for MDMに登録できます。 Knox Mobile Enrollmentにより、デバイスは承認済みの再販業者からエンドユーザーに直接発送され、Go Androidクライアントが自動的に設定済みの登録データをダウンロードします。詳細は、Samsung Knox Mobile Enrollment for Android Enterpriseをご覧ください。

要件

- IMEI別デバイスリスト
- IMEIまたはシリアル番号、およびオプションでユーザー名と登録パスワードが含まれている、デバイスの一覧が含まれているCSVファイル
- Ivanti Neurons for MDM(現行リリース)
- モバイル登録が許可されたSamsung Knoxアカウント
- サポートされているSamsungデバイス サポートされているSamsungデバイスの一覧はこちらから入手できます。

Oculusデバイスの登録

Ivanti Neurons for MDM でQuest for Businessデバイス(Oculusデバイス)を管理できるようになりました。現在Metaでは、Oculus for Business(OFB)デバイスとQuest for Business(QFB)デバイスをMDM向けにサポートしています。デバイスをMDMで利用できるようにするための基本的なタスクをいくつかMetaコンソールで実行した後、Ivanti Neurons for MDMに登録する必要があります。

デバイス マネージャの Meta Workplaceコンソールで、Oculusデバイスフリートを登録できます。Oculus Business Workplaceには、登録済みのメールアドレスに共有された認証情報を使用してログインする必要があります。ホームページには、[すべてのデバイス] 情報が[デバイス フリート] セクションに表示されます。[デバイスフリート] セクションには、[デバイス管理] で利用可能なすべてのデバイスの概要が表示されます。表示される詳細情報は、デバイス名、デバイスのステータス、OS(オペレーティングシステム)、モデルなどです。

このセクションは以下のトピックを含みます。

- Oculusデバイスを登録するための必須条件
  - 「デバイスマネージャーでのMDMアプリのセットアップ」下
  - 「Oculusデバイスのセットアップ」次のページ
- MobileIron GoにOFBデバイスを登録する
  - 「Ivanti Neurons for MDMコンソールで」ページ248
  - 「Goクライアントで」ページ248

Oculusデバイスを登録するための必須条件

デバイスマネージャーでのMDMアプリのセットアップ

デバイス/ヘッドセットはプロビジョニングされ、最低で**v28**の**Oculus for Business**に更新されます。Metaコンソール上で、管理者がデバイスマネージャでMDMをセットアップし、この特定のMDMサービスにOculusデバイスをマップする必要があります。

手順

1. **Oculus Business Workplace**のホームページで、**[アプリ]**を選択します。
2. **[アプリ ライブラリ]**で、インストールするサードパーティ製MDMアプリをクリックし、**[更新]**をクリックします。
3. **[モバイルデバイス管理]**の下のリストから、アプリ用の適切なMDMを選択し、**[アプリの更新]**をクリックします。
4. MDMのインストール先となるOculusデバイスヘッドセットをクリックします。デバイス情報が画面に表示されます。
5. **[詳細情報]**タブで、**[モバイル デバイス マネージャ]**までスクロールします。
6. **[MDM 機関]**オプションの横の**[編集]**ボタンをクリックします。

   デフォルトでは、[Oculusデバイスマネージャー]オプションが選択されます。[MDM機関アプリ]を選択し、[MDM機関アプリ]リストから**[MobileIron Go]**を選択する必要があります。

7. **[保存]**をクリックします。[デバイス]が自動的にリセットされますので、セットアップアプリを使用してOculusデバイスをセットアップする必要があります。

Oculusデバイスのセットアップ

[デバイス セットアップ] アプリを使用してOculus Quest 2ヘッドセットデバイスを追加できます。ユーザーが各自のAndroidデバイスでこのアプリをダウンロードしてインストールできるように、このアプリを、必要なユーザーと共有する必要があります。

手順

1. **[デバイス フリート]** セクションで、**[未構成デバイス]** をクリックします。
2. **[セットアップアプリの取得]** をクリックします。**[ダウンロードリンクの送信]** ページが画面に表示されます。
3. リストからチーム メンバーを1人以上選択するか、**[受信者を追加]** をクリックしてリストから選択します。
4. **[リンクの送信]** をクリックします。選択したユーザーには、**[デバイスセットアップ]** アプリをインストールするためのリンクが記載されたメールが送信されます。
5. メールの **[デバイス セットアップ アプリのダウンロード]** リンクをクリックして、**デバイスセットアップアプリ**を各自のAndroidデバイスにインストールします。

   > ダウンロードした後、このアプリはデバイスのアプリストアに表示されません。デバイスの [ダウンロード] セクションから取得してインストールする必要があります。

6. Androidデバイスで **[Oculus for Business]** アプリを開きます。
7. Oculusデバイスの電源ボタンを2秒間押して、電源を入れます。
8. Bluetoothをオンにし、セットアップが完了するまでAndroidデバイスをOculusデバイスに近づけておきます。
9. AndroidデバイスのBluetoothを使用して、Oculusデバイスを検索します。
10. 必要なOculusデバイスが見つかった後、そのデバイスをWi-Fiネットワークに接続してセットアップを完了する必要があります。
11. **[Wi-Fi情報の入力]** をクリックして、ネットワーク名とパスワードを入力し、**[保存]** をクリックします。これで、OculusデバイスがWi-Fiネットワークに接続されます。
12. **[セットアップの開始]** をクリックします。セットアップが進行中である旨の通知が画面に表示されます。セットアップ中は、アプリを閉じたり、ヘッドセットを操作したりしないでください。

    確認のメッセージが画面に表示されます。引き続き、**[さらにデバイスを検索]** ボタンを使って別のデバイスを検索できます。

OFBデバイスをMobileIron Goに登録する

Ivanti Neurons for MDMコンソールで

Ivanti Neurons for MDMコンソールでOFBデバイスをMobileIron Goに登録できます。ただし、仕事用マネージドデバイス非GMSモード(AOSP)構成(**[構成]**の下)をこれらのOFBデバイスグループに配布する必要があります。

Goクライアントで

MobileIron Goクライアントで OFBデバイスを登録できます。OFBデバイスを登録するには、以下のタスクを実行する必要があります。

- OFBセットアップアプリを使用してセットアップを完了した後、引き続き、OFBヘッドセットに関する画面上の指示に従い、デバイスのセットアップを完了します。
- MobileIron Goアプリが自動的に起動しますので、ログイン認証情報を入力し、MDMの指示に従って登録を完了する必要があります。

これで、デバイスがDOモードでプロビジョニングされ、MDMで管理されるように設定されました。

デバイスでのBluetooth有効化

対象：

- iOS 11.3+
- macOS 10.13.4+

デバイスのBluetoothは有効化も無効化も可能です。

手順

1. **[デバイス] ページ**のデバイスに移動します。
2. 以下のいずれかのアクションを実行します。
   - リストからデバイスを選択します。
   - デバイス名をクリックしてデバイス詳細ページを表示します。
3. **[アクション]** メニューから **[Bluetoothを有効化/無効化]** をクリックします。
4. **[OK]** をクリックします。

変更はデバイスの次のチェックイン時にプッシュされます。

iOS更新のスケジュールを設定

対象：

- iOS 9.0+監視対象Device Enrollmentデバイス
- iOS 10.3+監視対象デバイス

iOSデバイスに対して最新のiOSバージョンへの更新をスケジュールしてください。監視されたiOSデバイスバージョンの **[デバイス]** > **[アクション]** メニューオプションの **[OS バージョンの更新]** には、デバイスに適用されるiOSバージョンのリストのみが表示されます。

手順

1. [デバイス] ページのデバイスに移動します。
2. デバイス名をクリックしてデバイス詳細ページを表示します。
3. **[アクション]** メニューで **[OS バージョンの更新]** をクリックします。
4. **[OS バージョンの更新]** ウィザードで、iOSバージョンを確認し、**[更新後のバージョン]** ドロップダウンリストからOSバージョンを選択します。

   同等以下のバージョンを入力すると、ターゲットiOSバージョンは現在のバージョンよりも上でなければならないというエラーメッセージが表示されます。

5. **[更新]** をクリックします。

iOSデバイスがスケジュールされ、デバイスのチェックイン時に利用可能な最新バージョンのiOSに更新されます。デバイスにパスコードがある場合、MDMがデバイスに更新を送信すると、デバイスが更新をキューに入れ、ユーザーはインストールを開始するためにパスコードの入力を指示されます。詳細はソフトウェア更新を参照してください。

iOSシステムアプリの再 インストール

対 象：

- iOS 11.3+デバイス

iOSデバイスのiOSシステムアプリを再 インストールします。

手 順

1. [デバイス] ページを開きます。または、デバイスの名 前をクリックし、デバイス詳 細 ページからアクションを実 行します。
2. 1つ以 上 のiOSデバイスを選 択します。
3. **[アクション]** メニューから **[iOSシステムアプリを再 インストール]** をクリックします。
4. [iOSシステムアプリを再 インストール] のディスプレイボックスで、デバイスにインストールする1つ以 上 のシステムアプリを選 択します。
5. **[アプリを再 インストール]** をクリックします。

アプリケーションは、デバイスのチェックイン時 に選 択した対 応 する iOS デバイスにインストールされます。この方 法でインストールされるシステム アプリケーションは、管 理 対 象 のアプリケーションとは見 なされません。対 応 デバイスが選 択 されていない場 合 は、システムアプリがインストールされないというメッセージが表 示 されます。

詳 細 はソフト ウェア更 新 を参 照してください。

新しいユーザーへのデバイスの割り当て

ユーザーの役割やユーザーと会社との関係の変更に伴い、登録済みの既存デバイスを新しいユーザーに再プロビジョニングする必要がある場合があります。以下の手順は、デバイスの撤去や再登録の手間を省きます。

手順:

1. [デバイス] ページのデバイスに移動します。
2. デバイス名をクリックしてデバイス詳細ページを表示します。
3. **[ユーザーに割り当てる]**  アイコンをクリックします。

   > または、**[デバイス]** ページでデバイスを選択し、**[アクション]** メニューから **[ユーザーに割り当てる]** オプションをクリックできます。

4. **[ユーザの検索]** にユーザ名を入力します... フィールド。
5. 必要なユーザーを選択します。
6. **[ユーザーに割り当てる]** をクリックします。
   デバイスがそのユーザー向けにプロビジョニングされます。

> ユーザーベースおよびデバイスベースのライセンスの場合、割り当てデバイス制限を超えているユーザーにデバイスを割り当てられることに気づくかもしれません。これは、デバイス制限の意図が、個人デバイスの業務利用(BYOD)においてデバイスの登録を制限することにあるためです。

ユーザーベース、デバイスベースのライセンスの場合、デバイス制限の適用は道理に合いません。デバイスベースのライセンスであれば、システム内のデバイス総数が変わらないのでお客様のコストは変わりません。ユーザーベースのライセンスなら、むしろこのチェックがないほうがお客様に有利です。たとえばU1～U5の5人のユーザーが5台ずつデバイスを持っているとします。ユーザーベースのライセンスでは5件のライセンスを使用します。しかし、U4とU5のデバイス2台をU1とU2に移動すれば、使用するライセンスは5件から3件に減ります。

Androidデバイスの再割り当て

管理者は、Androidデバイスの所有権をあるユーザーから別のユーザーに移せるようになりました。再割り当てのプロセス中、Android Enterpriseモードでは、デバイスの管理プロファイルが再構成されるか、または現在のユーザーから新しいユーザーに再マップされます。再割り当ては、Android Management API(AMAPI) デバイスを除くすべてのAndroid Enterpriseデバイスで実行でき、GoogleドメインのAndroid Enterpriseでは実行できません。

デバイスの再割り当ては、同じモードのデバイスのみで実行できます。たとえば、「仕事用マネージドデバイス」モードのデバイスを、同じモードの別のユーザーに再割り当てすることができます。

デバイス再割り当てのプロセスには、次のステータスがあります。

- 開始済み
- 成功
- 失敗
- 保留中

デバイスの最後の再割り当てのステータスを、**[デバイス詳細]** ページ -> **[概要]** タブ -> **[再割り当ての最後のステータス]**で確認できます。

手順

1. **[デバイス]** を開きます。
2. リストから1台以上のデバイスを選択します。
3. **[アクション]** リストから、**[ユーザーに割り当てる]** をクリックします。
4. または、任意のデバイス名をクリックできます。**[デバイス詳細]** ページが開きます。**[ユーザーに割り当てる]** アイコンをクリックして [ユーザーに割り当てる] 画面を表示し、目的のユーザーを選択します。
5. **[ユーザーに割り当てる]** をクリックします。選択したオプションが検証されて、選択したデバイスを選択したユーザーに再割り当てできるかどうかがチェックされます。

   検証と再割り当てが正常に終了すると、確認のメッセージが画面に表示されます。

   選択可能な最大数である10台のデバイスを選択していた場合は、「割り当てが開始されました」というメッセージが画面に表示されます。11台以上のデバイスを選択していた場合は、「検証が進行中です」というポップアップが画面に表示されます。

Androidデバイスの再割り当ては、以前に登録済みのユーザーからのデータ残りを排除することに焦点を当てて独自に構築された革新的なソリューションであり、SUEM-Premium SKUのみで利用できます。

デバイスのチェックインの強制

デバイスは、Ivanti Neurons for MDM に接続(チェックイン)し、情報のやり取りを行う必要があります。チェックインは一定の間隔で予定されています。デバイスに対し、オンデマンドでチェックインするようプロンプトを表示することもできます。デバイスのチェックインを強制することにより、**構成**[1]の適用、**ポリシー**[2]の更新などのプロセスを迅速化することができます。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択します。
3. **[アクション]** をクリックします。
4. **[強制チェックイン]** を選択します。
5. [デバイス名] リンクをクリックしてデバイス詳細ページを開き、**[強制チェックイン]**  アイコンをクリックして **[OK]** をクリックすることも可能です。

チェックインにおいて構成インストールコマンドの処理中にデバイス側に障害が生じた場合、Ivanti Neurons for MDM は、後のチェックインで自動的に構成のインストールを再試行しません。管理者は、デバイスのデバイス詳細ページから手動で構成のインストールを再試行する必要があります。これには、[構成] タブを開き、エラー構成を選択して **[インストールを再試行]** をクリックします。

[1]collections of settings that you send to devices.

[2]sets of requirements and compliance actions defined for devices.

デバイスの位置検索

デバイスの位置検索機能を許可している場合、当該デバイスの前回の既知の位置を表示できます。この機能を有効にするには、位置情報データを収集し、構成をデバイスに適用するようプライバシー構成を編集する必要があります。デバイスもこの機能をサポートし、ユーザーが位置情報データの共有に合意する必要があります。

手順

1. **[デバイス]** ページのデバイスに移動します。
2. **[名前]** カラム内のリンクをクリックします。
3. **[概要]** タブで **[デバイスの位置情報]** の下のリンクをクリックします。

ページに以下の情報が表示されます。

フィールド名	説明
最後に居た場所	デバイスが最後に検出された日時を表示します。
座標	デバイスの緯度(南北位置)と経度(東西位置)を表示します。

デバイスの位置マップもページに表示されます。

デバイスのロック

デバイスの画面ロックを起動できます。ロックは、デバイスが異なれば動作が多少異なります。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択します。
3. **[アクション]** をクリックします。
4. **[ロック]** を選択します。
5. または、デバイス名のリンクをクリックして [デバイスの詳細] ページを開き、**[ロック]**  アイコンをクリックして、**[OK]** をクリックします。
6. AppConnect Androidアプリの場合、[ロック] コマンドはコンテナからユーザーを締め出すだけでなく、デバイスもロックします。ユーザーが再ログインするには、デバイスにはデバイスパスコード、AppConnectアプリにはAppConnectパスコードを使用します。
7. iOS 7デバイスの場合、メッセージや電話番号を入力できます(オプション)。
   これらのオプションにより、デバイスがロックされた理由とロック解除のための電話番号に関する情報をデバイスユーザーに提供することができます。
8. macOSデバイスの場合、ユーザーはデバイスにアクセスする際にパスコードとして6桁のPINの入力を求められます。画面ロックを続行するには、デバイスユーザーは次の操作を行う必要があります。
   a. PINを入力します。
   b. デバイスをロックすることを確認するチェックボックスをクリックします。
   c. **[はい、ロックします]** をクリックします。

> macOSでは、デバイスのロックパスコードの設定時にユーザーがオプションのロック画面のメッセージおよび電話番号を追加できます。

9. ChromeOSデバイスの場合、ロック操作を実行すると、「ユーザーがデバイスをロックするには、アクセスするためのパスコードを入力する必要があります」というポップアップウィンドウが画面に表示されます。**[ロック]** をクリックすると、デバイスステータスが **[無効化を送信しました]** に更新されます。更新後のデバイスステータスは、定期的なデバイス同期の後で可視になります。

デバイスをロックする別の方法：

- デバイスユーザーは、セルフサービスポータル経由でもロック操作を実行できます。
- 管理者は、管理者ポータル経由でもロック操作を実行できます。

Apple紛失モードにあるデバイスの管理

このセクションは以下のトピックを含みます。

- 「紛失モードの有効化」下
- 「紛失モードアクションの実行」下
- 「紛失モードを無効化」次のページ

対象：iOS 10.3+監視対象デバイス

監視対象デバイスはIvanti Neurons for MDMを通じて紛失モードに設定できます。すなわち、デバイスが紛失したことをAppleサーバーに報告し、記録されている最後の位置情報を取得します。デバイスが見つかれば紛失モードを無効化します。

紛失モードの有効化

デバイスを紛失モードにすることで、デバイスが紛失したことをAppleサーバーに報告します。デバイスを紛失モードにした後、

- デバイスを撤去すると紛失モードを無効化できません。
- デバイスをワイプするとデバイスの位置特定または追跡ができません。

手順

1. **[デバイス]**を開きます。
2. デバイスのチェックボックスを選択します。
3. **[アクション]** > **[iOSのみ]** > **[紛失モード]**を選択します。
4. 紛失デバイスモードセクションで**[紛失モードを有効化]**オプションを選択し、iOSデバイスを紛失モードにします。

紛失モードアクションの実行

紛失モードを有効化した後、紛失デバイスモードセクションから以下のアクションを実行できます。

- **メッセージ/電話番号をiPhoneにプッシュする**
  - 紛失デバイスのロック画面に表示するメッセージを入力します。
  - 紛失デバイスのロック画面に表示する電話番号を入力します。デバイスを見つけた人が連絡するためです。
- デバイスロック
- **デバイス位置情報を更新**

  デバイスをワイプするとデバイスの位置は特定できません。
- **紛失モード音を再生**

  デバイスを紛失モードから削除するか、ユーザーがデバイスで音を無効化するまで音は止まりません。

紛失モードを無効化

デバイスが見つかった場合、または紛失モードを誤って有効化した場合は、紛失モードを無効化します。

紛失したデバイスがIvanti Neurons for MDMから撤去されている場合、紛失モードの無効化は機能しません。

手順

1. **[デバイス]** を開きます。
2. デバイスのチェックボックスを選択します。
3. **[アクション]** > **[iOSのみ]** > **[紛失モード]** を選択します。
4. 紛失デバイスモードセクションで **[デバイスの紛失モードが有効化されています]** オプションを解除します。

デバッグログのリクエスト

iOS、macOS、Android仕事用マネージドデバイスにリクエストを送信すると、デバイスのトラブルシューティング目的でデバッグログを取得できます。[デバイス] ページで「デバッグログをリクエスト」コマンドを使用し、アクションとイベントの成功または失敗をデバッグログにキャプチャします。

この機能には以下のクライアントが必要です。

- iOSデバイスの場合、iOS対応Go 5.3.0またはサポートされる以降のバージョン。Ivanti EPMMからIvanti Neurons for MDMに移行されたデバイスの場合、iOS対応のMobile@Work 12.2.0またはサポートされる以降のバージョン。
- macOSデバイスの場合、macOS対応Mobile@Work 1.5またはサポートされる以降のバージョン。
- Android仕事用マネージドデバイスの場合、Go 65 for Androidまたはサポートされる以降のバージョン。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択し、デバイス名のリンクをクリックしてデバイス詳細ページを開きます。
3. アイコンをクリックします。
4. **[デバッグログをリクエスト]** を選択し、**[OK]** をクリックします。

リクエストが送信され、デバイスにあるログの準備ができると、管理者に通知が送信され、デバイスログに表示されます。デバイスログは、リンクをクリックしてダウンロードすることも可能です。

デバイスの撤去

デバイスを撤去すると、Ivanti Neurons for MDM との関連付けが終了します。デバイスを撤去するのは以下のような状況が考えられます。

- ユーザーが退職した場合
- ユーザーがデバイスを交換した場合
- 完了した管理タスクをもう一度やり直す必要がある場合(初めからやり直し)

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[撤去]** を選択します。
5. デバイス名のリンクをクリックしてデバイス詳細ページを開き、 アイコンをクリックすることも可能です。
6. **[撤去]** を選択し、**[OK]** をクリックします。

デバイスの所有権の放棄

会社所有デバイス上の仕事用プロファイルモードのAndroidデバイスが対象です。

会社所有デバイス上の仕事用プロファイルモードのデバイスでデバイス所有権を放棄すると、仕事用プロファイルが削除され、デバイスがIvanti Neurons for MDMから撤去されます。個人用のアプリとデータには影響を与えません。エンドユーザーはデバイスを個人用デバイスとして使用し、すべてのデバイス管理機能と設定にアクセスできるようになります。

デバイスはGoogle Zero TouchまたはKnox Mobile Enrollmentポータルから削除する必要があります。

デバイスの所有権を放棄する理由には以下があります:

- ユーザーが退職した場合
- ユーザーがデバイスを交換した場合

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択します。
3. **[デバイス詳細ページ]** をクリックし、アイコンをクリックします。
4. **[所有権を放棄]** を選択します。

デバイスのワイプ

デバイスをワイプすると、すべてのデータが削除され、デバイスが工場出荷時のデフォルト設定に戻ります。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスを選択します。
3. **[アクション]**(右上)をクリックします。
4. **[ワイプ]** を選択します。
5. デバイス名のリンクをクリックして [デバイス詳細] ページを開き、 アイコンをクリックすることも可能です。**[ワイプ]** を選択し、**[OK]** をクリックします。
6. (任意、iOS 11+のデバイスの場合) **[データプランを保護]** オプションを選択します。
7. (任意、iOS 11.3+のデバイスの場合) **[近接性設定をスキップ]** オプションを選択します。
8. macOSデバイスの場合、6桁のPINをパスコードとしてデバイスに送信できます。デバイスでは、ユーザーがデバイスにアクセスする際にPINの入力が求められます。ワイプ操作を続けるにはデバイスユーザーが以下を行う必要があります。
   a. PINを入力します。
   b. チェックボックスを選択してデバイスワイプ操作を確定します。
   c. **[はい、このデバイスをワイプします]** をクリックします。
9. ChromeOSデバイスの場合、**[デバイスの詳細]** ページまたは **[デバイス一覧]** ページからワイプ操作を実行すると、ポップアップウィンドウ「デバイスをワイプすると、工場出荷時の設定に戻り、デバイス上のデータが失われる可能性があります。ワイプのアクションは、プラットフォームにより異なります」が画面に表示されます。
   a. デバイスのワイプ操作を実行することを確認するには、「ワイプを元に戻せないことを理解します」チェックボックスを選択します。
   b. **[ワイプ]** をクリックしてデバイスをワイプします。

デバイスステータスが「**ワイプを送信しました**」に変わります。更新後のデバイスステータスは、定期的なデバイス同期の後で可視になります。

Android Enterpriseデバイスでは、デバイス再起動後のロック状態でもデバイスの **[ワイプ]** アクションを実行できます。

[ワイプが保留中です] 状態のAndroidデバイスは、**[デバイスの詳細]** ページにある **[デバイスを削除]** オプションを使用して削除できます。削除されたデバイスは、サーバーとの接続を失い、コンプライアンス違反となります。したがって、ユーザーはそのデバイスを工場出荷時状態にリセットした後、再登録する必要があります。

デバイスの削除

デバイスを撤去した後、削除することができます。デバイスを削除すると、すべてのページから削除されます。デバイスのステータスが [撤去] あるいは [撤去待ち] の場合のみ、デバイスを削除できます。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスに移動します。
3. **[名前]** カラム内のリンクをクリックします。
4. **[デバイスの削除]** リンク(左ペイン) をクリックします。
5. 表示された警告をお読みください。
6. 本当にデバイスを削除したい場合は、確認のためチェックボックスを選択します。
7. **[削除]** をクリックします。

デバイスのロック解 除

このセクションは以 下 のトピックを含 みます。

- 「Androidデバイスのロック解 除 」下
- 「Androidアプリ対 応 AppConnectのロック解 除 」次 のページ
- 「iOSデバイスのロック解 除 」次 のページ
- 「ChromeOSデバイスのロック解 除 」ページ269

デバイスをロック解 除 するには:

デバイスの画 面 ロックを解 除 できます。ロック解 除 は、デバイスが異 なれば動 作 が多 少 異 なります。

手 順

1. **[デバイス]** > **[デバイス]** に進 みます。
2. デバイスを選 択します。
3. **[アクション]** をクリックします。
4. **[ロック解 除]** を選 択します。
5. または、デバイス名 のリンクをクリックして [デバイスの詳 細] ページを開き、**[ロック解 除]**  アイコンをクリックして、**[OK]** をクリックします。

Androidデバイスのロック解 除

ロック解 除 コマンドを受 信 したAndroidアプリは、パスコードをリセットしようとします。 次 の表 は、さまざまなデバイスモード のAndroidデバイスのロック解 除 について説 明します。

	デバイス管理者	デバイス所有者	プロファイル所有者
Android 7以降	デバイス管理デバイスはロック解除されません。デバイスパスコードは空白または「0000」にリセットされません。	デバイスパスコードはクリアするか、クリアできなければ「0000」に設定する必要があります。次に、パスコード構成が存在する場合、新しいデバイスパスコードを設定するようプロンプトが表示されます。	パスワードを「0000」にリセットし、仕事用本人確認(Work Challenge)構成がある場合、ユーザーは仕事用本人確認制約に従って新しい仕事用本人確認を設定するよう強制されます。
Android 6以前	デバイスパスコードはクリアするか、クリアできなければ「0000」に設定してかまいません。デバイスパスコード構成が存在する場合、新しいデバイスパスコードを設定するようプロンプトが表示されます。例：Samsung S7では、ロック解除コマンドでデバイスパスワードがクリアされます。		デバイスでのプロファイルロック解除とパスワードリセットはサポートされません。

Android Enterpriseデバイスでは、デバイス再起動後のロック状態でもデバイスの**[ロック解除]**アクションを実行できます。

Androidアプリ対応AppConnectのロック解除

AppConnectアプリの場合、ユーザーが誤ったパスコードで何度もログインしたためにロックされたコンテナのロックは、**AppConnectロック解除**コマンドで解除できます。このロック解除はデバイスのロック解除ではありません。

iOSデバイスのロック解除

ロック解除コマンドを受信したiOSアプリは、デバイスからパスコードを削除します。パスコード構成で新しいパスコードが必要と規定されている場合、デバイスユーザーはパスコード構成の規則に従った新しいパスコードを設定するよう指示されます。この変更は60分以内に行ってください。60分を過ぎると、新しいパスコードを設定しない限り、アプリを使用できなくなります。

ChromeOSデバイスのロック解 除

ChromeOSデバイスを削 除して **[ロック解 除]** オプションをクリックすると、画 面 にポップアップが表 示 され、「ロックを解 除 すると現 在 のパスコード がクリアされ、ユーザーがデバイスにアクセスすることができます。 ロック解 除 は、プラットフォームにより異 なります」と示 されます。 **[ロック解 除]** をクリックすると、デバイスステータスが [ロック解 除 を送 信 しました] に更 新 されます。 更 新 後 のステータスは、定 期 的 なデバイス同 期 の後 で可 視 になります。

デバイスの再起動とシャットダウン

このセクションは以下のトピックを含みます。

- 「デバイスの再起動」下
- 「デバイスのシャットダウン」次のページ

対象：Android 7.0+(マネージドデバイス)、監視対象のiOS 10.3+(iOSとtvOS)、macOS 10.13+およびWindows 10+のデバイス

管理者は、デバイスの詳細ページから個別に、またはデバイスリストページからまとめて、iOSまたはtvOSの監視対象デバイスを再起動またはシャットダウンできます。

デバイスの再起動

手順

1. **[デバイス]** を開きます。
2. デバイスに移動します。
3. **[名前]** カラム内のリンクをクリックします。
4. **[アクション]** ボタンをクリックします。
5. **[デバイスを再起動/シャットダウン]** をクリックします。

   サポートされていないデバイスは再起動できません。

6. 表示された警告をお読みください。
7. (任意)再起動時にパスコードをクリアするオプションを選択してください。パスコードがクリアされない場合、デバイスはパスコードを要求し、再起動後にWi-Fiに接続しません。
8. まだ選択されていなければ **[デバイスを再起動]** を選択します。

9. 本当にデバイスを再起動したい場合は、**[デバイスに送信]** をクリックします。そうでなければ **[取り消し]** をクリックします。

> Androidデバイスの場合、管理者は、[デバイス詳細] ページの **[稼働時間]** でデバイスがいつ再起動されたかを確認できます。

[デバイス] リストページから複数のサポートされるデバイスを再起動することも可能です。この場合、デバイスを選択し、**[アクション]** > **[デバイスを再起動/シャットダウン]** をクリックして画面上の指示に従います。

デバイスのシャットダウン

手順

1. **[デバイス]** を開きます。
2. デバイスに移動します。
3. **[名前]** カラム内のリンクをクリックします。
4. **[アクション]** ボタンをクリックします。
5. **[デバイスを再起動/シャットダウン]** をクリックします。

> サポートされていないデバイスは再起動できません。

6. 表示された警告をお読みください。
7. **[デバイスをシャットダウン]** を選択します。
8. 本当にデバイスをシャットダウンしたい場合は、**[デバイスに送信]** をクリックします。そうでなければ **[取り消し]** をクリックします。

[デバイス] リストページから複数のサポートされるデバイスをシャットダウンすることも可能です。この場合、デバイスを選択し、**[アクション]** > **[デバイスを再起動/シャットダウン]** をクリックして画面上の指示に従います。

制約パスワードのクリア(iOSのみ)

監視対象のiOS 8デバイス上でユーザーが設定した制約パスワードをクリアできます。この操作は、アクティブなデバイスでのみ利用可能です。

手順

1. [デバイス] > [デバイス] に進みます。
2. デバイスのエントリを選択します。
3. [アクション] > [制約パスワードを解除] を選択します。
4. プロンプトが表示されたら操作を確認します。

デバイスのSentry連携の削除

Sentry連携は、デバイスへのメールアクセスを制御するアプリトンネリングやActiveSync対応のメールシステムを目的としてデバイスに適用されます。必要であれば、以下の方法で、任意のデバイスのSentry連携を削除できます。

手順

1. **[デバイス]** を開きます。
2. **[名前]** カラムで、Sentry連携を削除したいデバイスのデバイスリンクをクリックします。
3. **[Sentry]** タブをクリックします。
4. **[アクション]** カラムの **[削除]** をクリックします。

デバイスへのカスタム属性の割り当て

社内IDなどのカスタムデバイス属性を1つあるいは複数のデバイスに割り当てることができます。各属性には対応の値があり、構成やデバイスグループの作成などのタスクに利用できます。カスタム属性を作成した後は、デバイスに割り当てることができます。属性の管理の詳細については、「属性」ページ1044をご参照ください。

手順

1. 管理ポータルにログインします。
2. **[デバイス]** を開きます。
3. 1つまたは複数のデバイスを選択します。
4. **[アクション]** をクリックします。
5. **[カスタム属性を割り当てる]** を選択します。
6. 以下のオプションから*1*つ選択してください：
   - 既存の値があってもすべての属性の割り当て(上書き)を強制します。
   - 値が空の場合のみ上書きし、属性に既存の値があればスキップします。
7. 割り当てたい属性を選択し、その値を入力します(値を空にすることは許可されていません)。
8. **[割り当てる]** をクリックします。

この値の**カスタムデバイス属性**は、**[デバイス詳細]** ページからCSV形式にエクスポートできます。

デバイスからのカスタム属性の削除

この操作は元に戻すことができないため、慎重に進めてください。カスタム属性を1つ以上のデバイスから削除するには：

手順

1. **[デバイス]** を開きます。
2. 1つまたは複数のデバイスを選択します。
3. **[アクション]** をクリックします。
4. **[カスタム属性を削除]** を選択します。
5. 削除する属性を選択します。
6. **[削除]** をクリックします。

アプリフィードバックの同期とフェッチ

Androidデバイスにインストールされたアプリにリクエストを送信し、アプリの最新のアプリ構成ステータスの詳細を取得します。リクエストを送信すると、デバイスのアプリ構成フィードバックレポートが届きます。

手順

1. **[デバイス]** を開きます。
2. リクエストを送信したいデバイスをクリックします。
3. **[アクション]** をクリックします。
4. **[アプリフィードバックを同期およびフェッチ]** を選択します。アプリ構成フィードバックを同期およびフェッチするリクエストが送信されます。[クライアントの前回のチェックイン] フィールドの隣の [アプリフィードバックの前回の同期] フィールドが更新されます。
5. **[インストール済みのアプリ]** タブで、**[アプリフィードバック]** 列の **[詳細を表示]** リンクをクリックします。**[アプリフィードバック]** ウィンドウが表示されます。
   キー - アプリから受信したフィードバックに基づき、(アプリの管理対象アプリ構成で) 報告された設定の詳細情報と配置を提供します。
   タイムスタンプ - キーの日付と時刻。
   重大度 - キーの重大性を指定。例:「情報」、「エラー」
   メッセージ - アプリ構成フィードバックから受信したメッセージのタイプ。例:「失敗」
   データ - アプリ構成フィードバックから受信したデータの詳細。

アプリカタログからのアプリ構成フィードバックの閲覧

アプリカタログから特定のアプリのアプリ構成フィードバックレポートを閲覧することができます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. 詳細を見たいアプリを選択します。
3. **[アプリ構成フィードバック]** タブをクリックします。**[デバイス数]** カラムは、アプリ構成フィードバックレポートの各キーについてデバイス数 (ハイパーリンク) を表示します。

4. デバイス数のハイパーリンクをクリックすると、デバイスの詳細が表示されます。たとえば、ハイパーリンクの5をクリックするとデバイス5台の詳細が表示されます。表の上にあるキーと重大度の組み合わせに対して以下の詳細が表示されます。
   メールアドレス - ユーザー名を指定。ユーザー名のリンクをクリックすると、**[デバイス] > [デバイス詳細]** の **[インストール済みのアプリ]** タブが開きます。
   デバイスの種類 - デバイスの機種を指定。
   OS - Android OSのバージョン番号。
   シリアル番号 - デバイスのシリアル番号。
   タイムスタンプ - 最後に更新された日付と時刻。
   メッセージ - アプリ構成フィードバックから受信したメッセージのタイプ。例:「失敗」
   データ - アプリ構成フィードバックから受信したデータの詳細。

Androidデバイスのアプリ構成フィードバックエラー通知は、ベルの形のアイコン(右上)をクリックするか、**[ダッシュボード] > [通知]** ページで確認できます。通知のリンクをクリックすると、**[アプリ構成フィードバック]** タブが開き、アプリフィードバックレポートが表示されます。

デバイスがワイプまたは撤去されると、アプリ構成フィードバックレポートは削除され、表示されなくなります。7日以上前のデータは、24時間ごとに実行されるバックグラウンドジョブがパージします。

PINのリセット

対象：Windows 8、10のモバイルデバイス

管理者はWindowsモバイルデバイスのPINをリセットできます。この場合、そのデバイスに対して新しいPINが生成されます。これは、ユーザーが会社所有デバイスのPINをリセットせずに退職してしまった場合などに便利です。

手順

1. **[デバイス]** を開きます。
2. デバイスが関連付けられているユーザー名をクリックしてデバイス詳細ページを開きます。
3. 全般セクションのPINの行で **[リセット]** をクリックします。
4. PINリセットウィンドウでチェックボックスを選択し、PINリセットを確定します。
5. **[はい、実行します]** をクリックします。

この処理には数分かかる場合があります。デバイスがオンであることを確認してください。デバイス詳細ページで **[表示]** をクリックすると、リセット後に新しく指定されたPINを確認できます。

ファームウェアパスワードの設定

対象：macOS 10.13またはサポートされる以降のバージョン。

管理者は、macOSデバイスのファームウェア(EFI)パスワードを設定または更新できます。ファームウェアパスワードは、macOSデバイスが、ユーザーが選択した起動ディスク以外の社内または社外のストレージデバイスから起動するのを防ぎます。これにより、ほとんどのスタートアップキーの組み合わせも使用できなくなります。

手順：

1. **[デバイス]** を開きます。
2. 1台のデバイスのファームウェアパスワードを設定または変更するには：
   a. デバイスが関連付けられているユーザー名をクリックしてデバイス詳細ページを開きます。
   b. 全般セクションで **[ファームウェアパスワード]** を展開し、**[パスワードを設定]** をクリックするか、デバイスのアクションメニューから **[ファームウェアパスワードを設定/変更]** をクリックします。
   c. このセクションには以下の情報が表示されます。
      a. **パスワード** - パスワードまたは可能性のあるパスワードのリスト。

      > 管理者はファームウェアパスワードを設定する際、コマンドをデバイスに送信します。デバイスが速やかに応答しない場合、パスワードが一時的に保存され、このフィールドに表示されます。デバイスが承認を送り、デバイスが再起動されるまで、新しいパスワードは有効になりません。それまでの間、可能性のあるパスワードがすべて表示されます。デバイスが再起動され、パスワードの変更が承認されると、不要なパスワードはすべてクリアされます。

      b. **変更保留中** - パスワードの変更が保留中かどうかを示します。
      c. **コマンドステータス** - パスワード変更が成功であったか失敗であったかを示します。
      d. **OptionROMを許可** - オプションROMが有効化されるかどうかを示します。デフォルトでは、[いいえ]に設定されています。
3. 複数のデバイスのファームウェアパスワードを設定または変更するには：

a. デバイスを選択します。

b. [アクション] メニューで **[ファームウェアパスワードの設定/変更]** をクリックします。

4. 現在のパスワードと新しいパスワードを入力します。
   初めて設定する場合、現在のパスワードは空白でかまいません。
   パスワードをリセットするには新しいパスワードのフィールドを空白にします。

5. **[保存]** をクリックします。

サポートされるmacOSバージョンを搭載したデバイスのみ新しいパスワードに更新されます。サポートされていないデバイスはスキップされます。

個人リカバリキーの再発行

対象：macOS対応Mobile@Work1.66またはサポートされる以降のバージョンを搭載したmacOSデバイス。

他のMDMソリューションからIvanti Neurons for MDMの移行に際して、登録前に個人リカバリキー(PRK)が発行されている場合、管理者は登録時に新しいPRKの再発行をOSに要求できます。これによりキーがIvanti Neurons for MDMに保存されます。

PRKアクティビティの監査証跡ログは以下の手順で閲覧できます：

1. **[ダッシュボード] > [監査証跡]**を開きます。
2. [種類]フィルターで**[個人リカバリキー]**を選択します。[デバイス管理]カテゴリーにPRKエントリーが表示されます。これには「個人リカバリキーが閲覧されました」などのアクティビティが含まれます。

前提条件

この手順を実行する前に、次の構成をデバイスに配布してください：

- macOS対応Mobile@Work構成。
- FileVaultリカバリキー構成。

手順

1. デバイス上で新しいPRKを生成するスクリプトをサポートまで請求します。
2. 「deviceprk」という名前でデバイスのカスタム属性を作成します。これがスクリプト内で使用されます。
3. **[管理] > [すべてのスクリプト]**でリポジトリにスクリプトをアップロードします。その際、カスタム属性「deviceprk」を選択します。
4. 前のMDMソリューションからPRKを取得できなかったデバイスについては、動的なデバイスグループを作成します。デバイスグループのルールを次のように選択します：「**プラットフォーム=macOS**、**暗号化有効が[はい]**、**エスクローされたmacOS個人リカバリキーが[いいえ]**、**macOSリカバリキーの種類が[個人]**」
5. macOS対応Mobile@Work構成を作成します。その際、リポジトリからPRKスクリプトを選択します。新しいデバイスグループに構成を配布します。

6. スクリプトのスケジュールを設定し、1日1回、または必要に応じて実行します。スクリプトは実行の都度、ユーザーのパスワードを求めます。デフォルトではスクリプト実行のタイムアウトが60秒です。対応するmacOS対応Mobile@Work構成で **[最大実行時間]** フィールドを300秒に設定し、タイムアウトを延長することをお勧めします。

- 暗号解読キーは、デバイスの [デバイス暗号化ステータス] セクションのデバイス詳細ページにあります。[FileVault 暗号化有効] フィールドの横の **[表示]** をクリックします。
- PRKを取得すると、デバイスがデバイスグループから外れます。したがってスクリプト構成が適用されなくなり、デバイスから削除されます。
- スクリプトを使用してMDMがデバイスのリカバリキーを取得すると、スクリプトはデバイスからアンインストールされます。

関連トピック:

- 「属性」ページ1044
- 「すべてのスクリプト」ページ1291
- 「デバイスグループ」ページ182
- 「macOS対応Mobile@Work」ページ628
- 「FileVaultリカバリキー」ページ520

リカバリロックの設定または変更

対象：macOS 11.5+

管理者は、Appleシリコンを実行しているmacOSデバイスのデバイス再起動のリカバリロックを設定または変更することができます。リカバリロックを設定すると、パスコードを入力しない限り、macOSデバイスをリカバリモードで起動できなくなります。

手順：

1. **[デバイス]** を開きます。
2. 起動のリカバリロックを設定または変更するには：
   a. デバイスが関連付けられているユーザー表示名をクリックしてデバイス詳細ページを開きます。以下のいずれかの手順を実行してください。
   b. 概要セクションで **[リカバリロック]** を展開し、**[パスワードを設定]** をクリックするか、**[パスワードを変更]** をクリックします。または、**[アクション]**（三点）をクリックし、**[リカバリロックを設定/変更]** をクリックします。
   c. **[リカバリロックを設定/変更]** ダイアログボックスで、次のことを行います。
      a. **現在のパスワード：**ここに現在のパスワードを入力します。初めて設定する場合は空白のままにします。
      b. **パスワード：**設定したいパスワードを入力します。
      c. **パスワードの確認：**設定したいパスワードを再度入力します。
3. **[リカバリロックを設定/変更]** をクリックします。

概要の **[リカバリロック有効]** にリカバリロックのパスコードのステータスが表示されます。

管理者は、既存のパスワードを削除し、**[リカバリロックを設定/変更]** をクリックすることでパスコードをクリアすることもできます。

アプリ

このセクションは以 下 のトピックを含 みます。

アプリのカタログ

このセクションは以下のトピックを含みます。

アプリカタログを管理するには [アプリカタログ] ページを使用します。アプリカタログは、ユーザーが使用できるようになっているモバイルアプリのアプリを一覧表示します。これには、ユーザが公開アプリストアからダウンロードできるアプリと、Ivanti Neurons for MDM (自社開発アプリ) を使用して配布するアプリが含まれます。AppConnect対応アプリ、iOS向けGoクライアント、macOS向けM@Wも、ビジネスアプリとしてアプリカタログのページで利用できるため、構成や配布のためにそれらのアプリをインポートするプロセスが簡素化されます。MAM Onlyデバイスでは、iOSユーザーがアプリカタログを開いたときに、証明書を選択してこれらのアプリへのアクセスを認証するよう指示が表示されます。

AppleのM1チップセットMacBookはiPhoneとiPad VPPアプリに対応しています。対応するiPhoneおよびiPad VPPアプリをプッシュできるのは管理者のみです。このオプションをアプリカタログからユーザーがインストールすることはできません。

Androidデバイスが含まれているIvanti Neurons for MDMテナントの場合、2021年3月末までにAndroid Enterpriseが有効化されないと、管理者はそれらの名前を持つアプリを検索できなくなります。この変更に関するお知らせは、アプリカタログページにアクセスするとバナーメッセージに表示されます。このバナーメッセージは、それらのテナントでAndroid Enterpriseが有効化されるまで、また「このメッセージを再び表示しない」チェックボックスオプションの選択が解除されるまで、引き続き表示されます。

- macOSのパブリックアプリにはサイレントアプリインストールを使用できません。macOSアプリは、デバイスベースのライセンスでApple Apps and Booksを通じてでも、登録時のサイレントアプリインストールでも展開可能です。
- Goアプリを Ivanti Neurons for MDM サーバーにアップロードしているときに、**[マネージドアプリに変換]** オプションを選択する必要がある場合は、**[デバイスにインストール]** オプションも有効化する必要があります。
- Sonim XP5sデバイスではアプリカタログとアプリのインストールがサポートされていません。
- Androidは、管理者特権が有効になっているアプリのアンインストールを許可しません。そのようなアプリをアンインストールするには、**[デバイス設定]** > **[セキュリティ]** > **[デバイス管理者]** を開き、デバイス管理者特権を無効化してください。それからアプリをアンインストールします。
- 自社開発アプリは、アプリを圧縮または難読化した状態ではアップロードできません。
- 共有iPadでは市販アプリがサポートされません。
- Appleの、アプリカタログ内の企業間(B2B) iOSアプリに関する制約により、**[詳細]** タブにアプリの説明とスクリーンショットが表示されません。
- アプリカタログや管理ポータルでアプリを検索した場合、検索結果は、**アプリ名**、**コメント**、**説明**、**バージョンの表示**、および**最新情報**に基づいたものになります。これらのフィールドと一致するアプリデータが検索された場合に、検索結果として表示されます。

アプリの機能のライセンス

以下のアプリカタログの機能には、追加のライセンスが必要です。

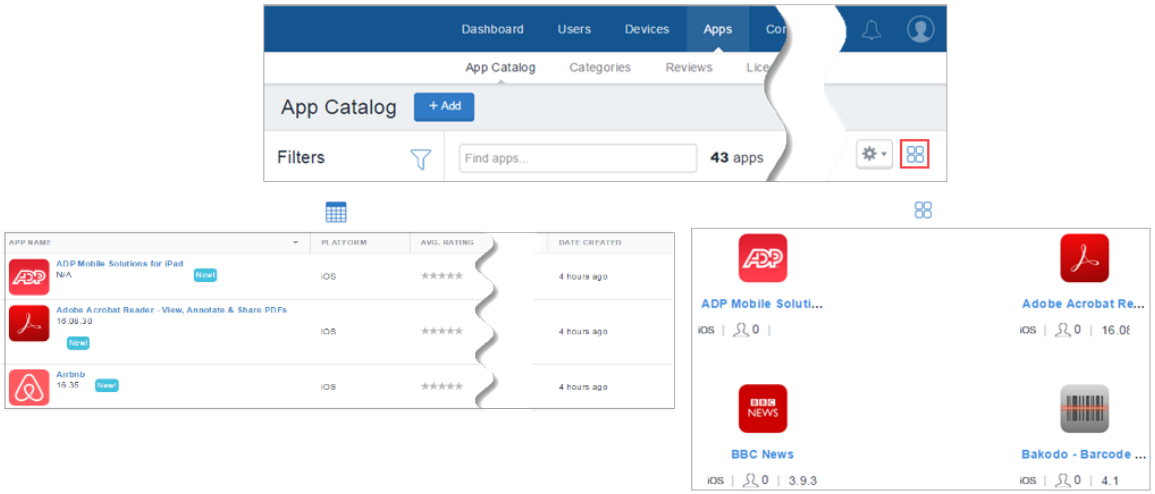
- アプリのサイレントインストール/アンインストール: Silverライセンス
- アプリごとの構成 : Goldライセンス
- AppConnectカスタム構成 : Gold ライセンス
- Android Enterprise カスタム構成 : シルバー ライセンス

Androidデバイスがキオスクモードの場合:

Androidデバイスがキオスクモードの場合は、社内アプリのみインストール可能です。パブリックアプリをインストールできますが、これらのアプリをインストールする前にデバイスのキオスクモードを終了する必要があります。また、キオスクモードのデバイスで使用できるアプリは、会社によって承認済みまたは許可リストに登録済みのアプリに限定されます。Android 4.1を使用するデバイス上で、承認済みアプリが、許可リストに含まれないアプリを起動した場合、そのアプリは立ち上がりますがすぐに最小化されます。Android 5.0を使用するデバイス上では、許可リストに含まれるアプリから起動された未承認のアプリは、そのまま利用することができます。

リストとグリッドビューの切り替え

[アプリカタログ] 画面の右端にあるリストまたはグリッドのアイコンをクリックします。



Android Enterprise向けGoogle Playストアアプリの追加

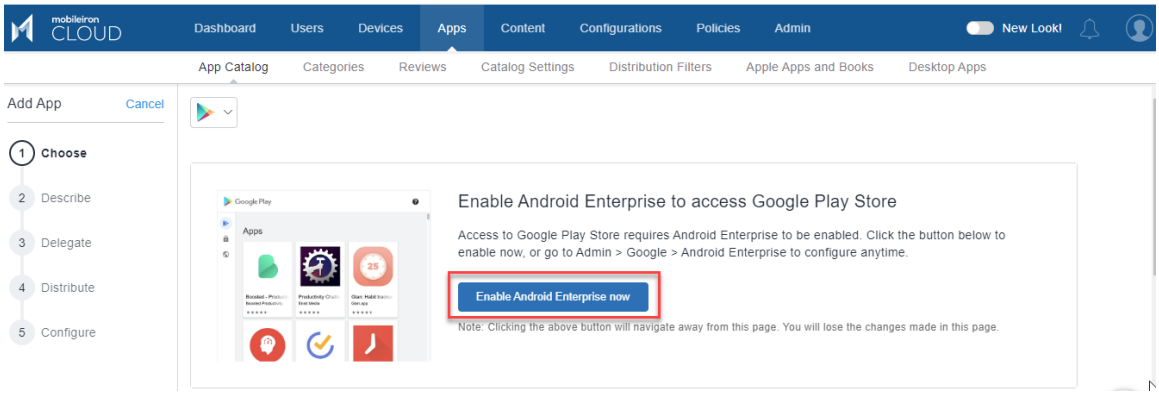
- Google Playストアからアプリカタログにアプリを追加し、ユーザーに提供しましょう。Android EnterpriseのGoogle Playストアからアプリを追加するには、アプリをアプリカタログに含めることを承認する必要があります。

- Android Enterpriseデバイス用のGoogle Playストアのレイアウトには移行デバイス用のホームページがあり、Coreから管理できます。また、Ivanti Neurons for MDMへのクイックリンクからIvanti Neurons for MDMで管理するすべてのアプリケーションを表示できます。Ivanti Neurons for MDMリリース80以降、Android EnterpriseデバイスをCoreからIvanti Neurons for MDMに移行する際、CoreとIvanti Neurons for MDMのアプリカタログで共通のアプリケーションのみがデバイスの仕事用プロファイルのGoogle Playストアで表示されます。Ivanti Neurons for MDMアプリカタログにあるすべてのアプリケーションを表示させたい場合はIvanti Neurons for MDMボタンをクリックします。

Android Enterpriseデバイス用のGoogle Playストアのレイアウトには移行デバイス用のホームページがあり、Coreから管理できます。また、Ivanti Neurons for MDM へのクイックリンクから Ivanti Neurons for MDM で管理するすべてのアプリケーションを表示できます。Ivanti Neurons for MDM リリース80以降、Android EnterpriseデバイスをCoreから Ivanti Neurons for MDM に移行する際、CoreとIvanti Neurons for MDM のアプリカタログで共通のアプリケーションのみがデバイスの仕事用プロファイルのGoogle Playストアで表示されます。[Ivanti Neurons for MDM] ボタンをクリックすると、Ivanti Neurons for MDM アプリケーション カタログで使用できるすべてのアプリケーションが表示されます。

前提条件

- Android Enterpriseに、Google Playストアのアプリケーションへのアクセスおよびアプリカタログへの追加を許可する必要があります。



Procedure

1. **[アプリ] > [アプリカタログ]** へ進みます。
2. **[追加]**(左上)をクリックします。

   ドロップダウンリストから [Google Play] を選択し、Google Playストアのアプリを検索します。Android Enterpriseが登録されていると、Google Play iFrameが表示されます。

3. 検索フィールドからアプリを検索し、アプリをクリックします。
4. アプリをユーザーに提供することを承認する場合は、**[承認]** をクリックします。確認ウィンドウが表示され、アプリに提供されるアクセスの詳細を確認できます。**[承認]** をクリックします。

   承認したアプリは、後で **[未承認]** をクリックすることで承認を取り消すことができます。

5. 新しいアプリ許可リクエストを処理するには、以下のオプションのいずれかを選択します。

オプション	説明
承認設定	
アプリが新しい許可を要求しても承認を維持	ユーザーが更新済みアプリをインストールできるようにします。
アプリが新しい許可を要求した場合は承認を取り消し	再承認されるまでアプリをストアから削除します。
承認設定	
購読者を追加	メールアドレスを入力し、承認したアプリが新しい許可を要求したときに購読者にメールで通知します。

6. **[保存]** をクリックします。

パブリックストアからのアプリ追加

公共のストアからアプリカタログにアプリを追加し、ユーザーに提供できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[追加]** をクリックします。
3. 希望のアプリを選択する:
   a. 公共のアプリストアを選択します。
   b. アプリ名を入力します。
   c. リストからアプリを選択します。
   d. **[次へ]** をクリックします。

4. ユーザーにアプリの説明をする：

   a. カテゴリを追加または削除します。

   b. オプションの説明を入力します。

   c. **[次へ]** をクリックします。

5. アプリ配信を定義する：

   a. 配信オプションを選択します。

   b. **[詳細オプションとアプリ構成]** セクションを展開します。

      次のガイドラインに従って、オプションに情報を入力します。

設定	操作内容
デバイスにインストール	登録後すぐにインストールを開始するには、このオプションを選択します。ユーザーは、以下の場合を除き、アプリのインストールの確認を求められます。 • デバイスがアプリのインストールとアプリの更新に関して監視対象のiOSデバイスである。 • デバイスがアプリ更新に関して非監視対象のiOSデバイスである。 • ユーザーがApps and Booksプログラムに登録済みである。 • デバイスがSamsung Knoxデバイスで、以下のサイレントインストールオプションが選択されている。 iOSパブリックアプリをデバイスに初めてインストールすると、ユーザーがアプリを再インストールするための「再インストール」ボタンがアプリカタログに表示されます。 再インストールは、デバイス上のアプリのバージョンがiOSアプリストアのバージョンと異なる場合に実行します。
エンドユーザーのアプリカタログでアプリを表示しない	ユーザーにデバイス上でアプリカタログを見せたくない場合に選択します。
アプリインストール優先度を設定	ユーザーのオンボーディング中、アプリのインストールの優先度として、高、中、低を選択します。ユーザーのオンボーディング中、優先度が高いアプリのみがインストールされます。

設定	操作内容
所定の回数だけ失敗するとアプリの再プッシュを一時停止 (iOSのみ)	トグルスイッチを [オン] にすると、再プッシュ失敗回数が所定数を超えた場合、次のようにアプリの再プッシュが保留されます。 **再プッシュを停止する回数** - 再プッシュを停止するまでの再プッシュ失敗回数を入力します。値は**1**～**999**の値を入力してください。 **プッシュ失敗後にプッシュを再試行するまでの時間** - 再プッシュに失敗してから再び再プッシュが可能になるまでの時間数を入力します。**3**～**48**の値を入力してください。
(Androidのみ) Samsung Knoxデバイスにサイレントインストール	このオプションは、公共アプリには適用されません。
(iOSとmacOSのみ) Per-App VPNをこのアプリで有効化	このアプリでPer-App VPN構成を使用するには、このオプションを選択します。 ドロップダウンリストからPer App VPN構成の使用を選択します。 macOSの場合は、Tunnel Per-App VPN構成のみ選択してください。
(iOSのみ) iCloudおよびiTunesへのバックアップ防止	このアプリに関連するデータがiCloudおよびiTunesにバックアップされないようにするには、このオプションを選択します。

設定	操作内容
(iOSのみ) 登録解除時にアプリを削除	デバイスがIvanti Neurons for MDMの管理対象から外れた場合にこのアプリを削除するには、このオプションを選択します。
(iOSのみ) AppConnectカスタム構成	AppConnect対応アプリの場合は、カスタム構成の基本設定を指定するキーと値を入力します。利用可能なキーについては、アプリのドキュメントを参照してください。
iOS 7+マネージドアプリ設定	iOS 7+マネージドアプリとしてこのアプリに定義されたキーと値を入力します。サポートされているキーの情報については、アプリのドキュメントを参照してください。

Android Enterprise アプリには別のオプションが設けられます。

c. **[次へ]** をクリックします。

d. プロモーションオプションを選択します。

- 未注目
- 注目リスト
- 注目バナー
- [注目バナー] を選択した場合は、次の詳細を指定します。
  a. **タイトル** - アプリケーションのタイトルを指定します
  b. **説明** - アプリケーションの詳細を指定します
  c. **バナースタイル** - バナーの色を選択します

e. **[+説明を追加]** をクリックし、構成の簡単な説明を入力します。

f. 任意で構成の配布を変更します。

g. **[完了]** をクリックするとアプリ構成が保存されます。

h. **[完了]** をクリックします。

アプリカタログでWindowsアプリを検索する場合、次のようにドロップダウンリストの **[アプリ名]** オプションまたは **[アプリストアID]** オプションを使用することで、厳密に一致するアプリを検索できます。

- **アプリ名** - このオプションを選択し、アプリ名を指定します
- **アプリストアID** - このオプションを選択し、アプリストアIDを指定します

アプリストアIDによる検索では、Win32ストアのアプリ(「X」で始まるアプリID) には対応していません。

自社開発アプリの追加

社内アプリは、以下のファイル形式でアプリカタログにアップロードできます。サイズの大きいファイルは、アップロードに数分かかる場合があります。自社開発アプリのバージョン数は最大100です。これを超えた場合、Ivanti Neurons for MDM システムはアプリケーションの最も古いバージョンを消去します。アプリケーションのアップロードと消去の状況は監査証跡ページで確認できます。

Mobile@Workから返されるMIPアプリインベントリは、いくつかのアプリで正しくない場合があります。Mobile@Workでは、デフォルトの場所にインストールされていないアプリのインストール状況を検出できない場合があります。このようなアプリでは、検出スクリプトを追加することで、デバイス上のアプリの正しい状態を識別できるようになります。Mobile@Workは、検出スクリプトの終了コードが0の場合に、アプリが存在していると判断します。その他の終了コードの場合は、アプリはインストールされていないものと判断されます。検出されたアプリに基づいて、Mobile@Workはそのデバイスのインベントリレポートを作成します。

- IPA (iOS)
- MIP(Packager macOSアプリ)
- PKG (macOS)
- APK (Android)
- APPX、APPXBUNDLE、EXE、MSI(Windows)

スクリプトを含むPKG、またはスクリプトを含むPKGを持つDMGなどのアプリケーションの場合、macOS対応Mobile@Workは、正常なインストールリクエストのみを検出できます。アプリが検出されなかった場合、あるいはインストールされたスクリプトが削除された場合は報告されません。したがって、Ivanti Neurons for MDMサーバーはインストールコマンドを再送することができません。アプリのダウンロード中に接続が切断された場合、チェックインを行ってアプリのインストールを再試行してください。MIPアプリの場合、PKG、またはスクリプトの入ったPKGを持つDMGによってインストールされたデバイスからアプリが削除されていても、クライアントデバイスの受信フォルダ内にPKGのエントリが存在する場合、Mobile@WorkはMIPアプリをインストールしません。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[追加]**(左上)をクリックします。
3. アプリファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択]** をクリックしてファイルシステムから選択し、**[確定]** をクリックします。
4. **[次へ]**(右下)をクリックします。

5. ユーザーにアプリの説明をし、必須アプリを構成します。

   a. カテゴリを追加します。

   b. macOSパッケージを追加する際に、パッケージファイルに複数のアプリ(Microsoft Officeパッケージと Cisco AnyConnectパッケージなど) が含まれている場合、選択した基本アプリを使用してパッケージがインストールされていることを識別します。Per-App VPNが構成されている場合は、これらのアプリに適用されます。

   c. オプションの説明を入力します。

   d. **MSI製品コード**：MSIアプリをアップロードする際、MSIアプリの製品コードがこのフィールドに自動的に入力されます。

   e. **オーバーライドURL**：任意のアプリソースURLオーバーライドを入力し、異なるソースからのアプリのダウンロード、またはローカルネットワーク(HTTP、HTTPS) 経由での大型ファイル(Microsoft Officeのインストールメディアなど) の取得を許可します。このオプションには、セキュアな内部ネットワークへのアクセス、およびアプリが保存されている代替サーバーの手動同期が必要です。必要なインフラを確保するまで値は入力しないでください。この値は、特定のアプリのアプリ設定を編集中に編集できます。

      - iOSアプリの場合、アプリのオーバーライドURLは、HTTP形式またはHTTPS形式のみでなければなりません。
      - AndroidアプリとmacOSアプリの場合、アプリのオーバーライドURLは、HTTPS形式のみでなければなりません。
      - macOSアプリの場合、URLの最後が拡張子(.pkg) であることが必要です。

   f. **コマンドライン** (Windows 32ビットMSIアプリのみ)：任意のコマンドラインスイッチの入力により、MSIファイルの展開中にパッケージに入っていない詳細情報を指定します。たとえば、インストールログを出力ファイルに書くには、このフィールドに「/log output.txt」と入力します。これによりC:\Windows\System32フォルダーにoutput.txtファイルが作成されます。デフォルトでは、MSIアプリのアップロード中、サイレントインストールを示すコマンドラインオプション「/qn」が自動入力されます。

      アップロードするMSIアプリのパッケージ名をコマンドライン引数の一部として追加しないでください。追加した場合、アプリのパッケージ名をコマンドライン引数から削除しない限り、アップロードが制限されます。追加リンクにはサポートされるコマンドラインオプションすべてのリストが含まれます。このリンクはアプリの [表示と編集] モードで表示されます。

   g. Win32の.EXEのみ：管理者用PowerShellモードを使用してブリッジ経由でインストールされます。ブリッジ機能は、利用可能であれば自動的に使用されます。

- **ディスプレイバージョンとバンドルバージョン**の整合性を維持するためのバージョンの更新
- インストーラー(.EXE)の場所
- インストーラーのコマンドラインパラメーター:ファイルをサイレントに実行するための引数(例:/SILENTまたは/VERY SILENT)は必須です
- ユーザーとして実行するインストーラー:ユーザーの認証情報を使用してインストールするには、[ユーザーとして実行]オプションを選択します

h. Packager macOSアプリの場合、必須アプリを構成します(任意)。必須アプリの機能概要については、「Packager自社開発macOSアプリを理解する」を参照してください。

i. **起動URL**:AppStationでアプリを起動するカスタムURLを入力します。AppStationによるMAM Only導入形態での配布のために非AppConnectアプリを追加する場合にのみ必要であり、iOSアプリにのみ適用されます。

j. アプリ委譲を構成します。

> 必須アプリを委譲し、それが、非デフォルトスペースからのアプリに対する必須アプリになると、まず必須関係を削除してからでないと、そのアプリの委譲解除を実行できなくなります。

k. **[次へ]**をクリックします。

l. **[次へ]**をクリックします。

6. (オプション)アプリのスクリーンショットを追加します。
7. (任意)アプリ(iOSアプリ、MacOSアプリ、Windowsアプリ)のアイコンを追加または置換します。
8. **[次へ]**をクリックします。
9. Packager macOSアプリの場合、アプリインストールの前や後に実行するインストールスクリプトを定義または選択します。検索ボックスに入力する、またはリンクをクリックしてスクリプトのリストを表示し、以下のいずれかまたは両方のスクリプトを選択します。**[次へ]**をクリックします。
   - **プリインストールスクリプト** - スクリプト名を入力し、アプリのインストール前に実行するスクリプトを選択します。プリインストールスクリプトはクライアントからスクリプト実行成功ステータスを受信するまで実行または再試行されます。その後で初めてインストールコマンドが送信されます。スクリプトの実行ステータスはデバイス詳細ページの**[ログ]**タブに表示されています。

- **ポストインストールスクリプト** - スクリプト名を入力し、アプリのインストール後に実行するスクリプトを選択します。
- **アンインストールスクリプト**：アプリがデバイスに配布されなくなったことを検出したときにサーバーがデバイスに送信するスクリプト名を入力します。
- **検出スクリプト**：アプリを検出するためにサーバーがデバイスに送信するスクリプト名を入力します。アプリの検出スクリプトの結果は、デバイス上のアプリのデフォルトのインベントリ結果よりも優先されます。アプリがデバイスに配信されているか否かにかかわらず、すべてのアプリの検出スクリプトがデバイスに送信され、デバイス上のアプリの存在を評価します。

  検出スクリプトのサンプルは以下のとおりです。

```
#!/bin/bash
app_name="Name of the App"
count="$(system_profiler SPApplicationsDataType | grep "$app_name" -c)"
echo "$app_name count $count"
if [ $count -ge 1 ]
then
 echo "$app_name is installed"
else
 echo "$app_name is not installed"
 exit 1
fi
 exit 0
```

スクリプトは **[管理] > [すべてのスクリプト]** ページから作成できます。アプリをアップグレードする場合は、スクリプトを古いアプリからコピーし、アップグレード済みのアプリで実行することも可能です。この手順を省略し、後でアプリを編集してスクリプトを設定してもかまいません。

10. アプリ配信を定義する：
    a. 配信オプションを選択します。
    b. **[詳細オプションとアプリ構成]** セクションを展開します。
    c. 次のガイドラインに従って、オプションに情報を入力します。

設定	操作内容
デバイスにインストール	登録後すぐにインストールを開始するには、このオプションを選択します。ユーザーは、以下の場合を除き、アプリのインストールの確認を求められます。 • このデバイスは監視対象のiOSデバイスです。 • デバイスがSamsung Knoxデバイスで、以下のサイレントインストールオプションが選択されている。
エンドユーザーのアプリカタログでアプリを表示しない	ユーザーにデバイス上でアプリカタログを見せたくない場合に選択します。

アプリインストール優先度を設定	ユーザーのオンボーディング中、アプリのインストールの優先度として、高、中、低を選択します。ユーザーのオンボーディング中、優先度が高いアプリのみがインストールされます。

所定の回数だけ失敗するとアプリの再プッシュを一時停止(iOSのみ)	トグルスイッチを[オン]にすると、再プッシュ失敗回数が所定数を超えた場合、次のようにアプリの再プッシュが保留されます。 **再プッシュを停止する回数** - 再プッシュを停止するまでの再プッシュ失敗回数を入力します。値は**1**～**999**の値を入力してください。 **プッシュ失敗後にプッシュを再試行するまでの時間** - 再プッシュに失敗してから再び再プッシュが可能になるまでの時間数を入力します。**3**～**48**の値を入力してください。
(Androidのみ) Samsung Knoxデバイスにサイレントインストール	ユーザーにSamsung Knoxデバイスへのインストールを指示したくない場合に選択します。

(iOSとmacOSのみ) Per-App VPNをこのアプリで有効化	このアプリでPer-App VPN構成を使用するには、このオプションを選択します。 ドロップダウンリストからPer App VPN構成の使用を選択します。 macOSの場合は、Tunnel Per-App VPN構成のみ選択してください。
(iOSのみ) iCloudおよびiTunesへのバックアップ防止	このアプリに関連するデータがiCloudおよびiTunesにバックアップされないようにするには、このオプションを選択します。
(iOSのみ) 登録解除時にアプリを削除	デバイスがIvanti Neurons for MDMの管理対象から外れた場合にこのアプリを削除するには、このオプションを選択します。

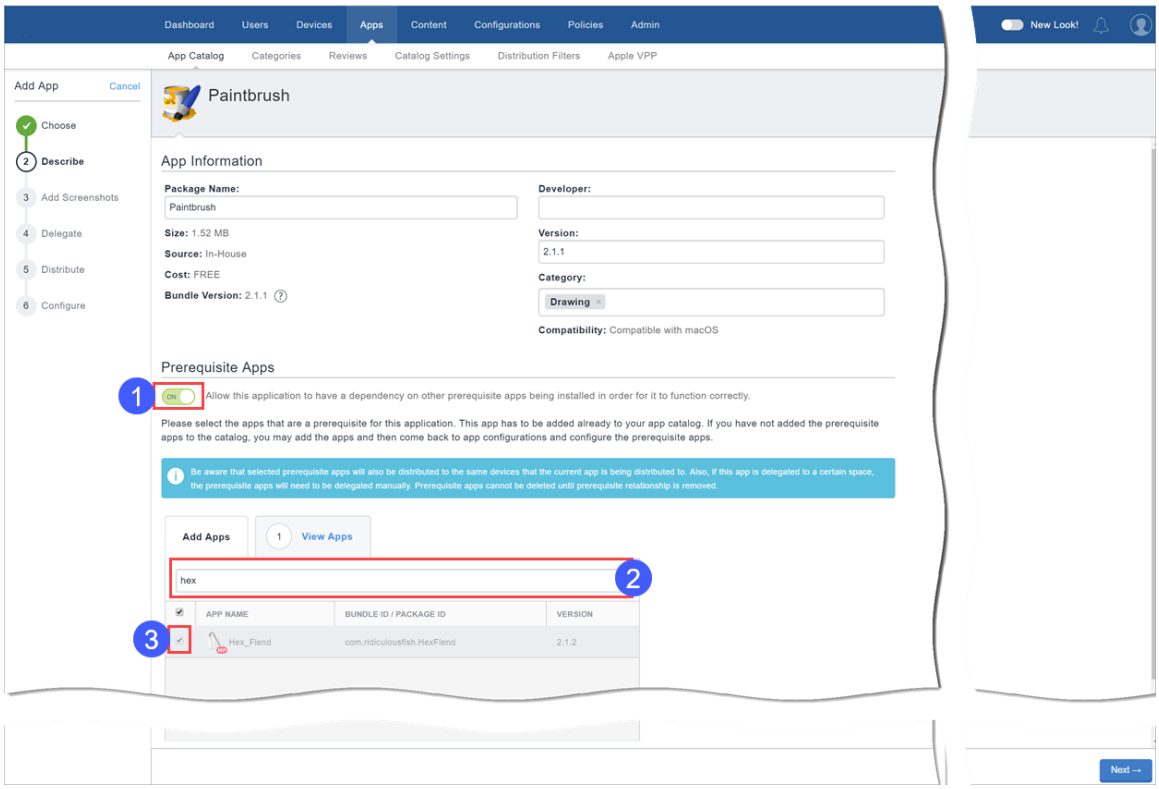
(iOSのみ) AppConnectカスタム構成	AppConnect対応アプリの場合は、カスタム構成の基本設定を指定するキーと値を入力します。利用可能なキーについては、アプリのドキュメントを参照してください。
iOS 7+マネージドアプリ設定	iOS 7+マネージドアプリとしてこのアプリに定義されたキーと値を入力します。サポートされているキーの情報については、アプリのドキュメントを参照してください。

d. **[次へ]** をクリックします。

11. プロモーションオプションを選択します。
    - 未注目
    - 注目リスト
    - バナー
12. **[完了]** をクリックします。

Packager自社開発macOSアプリを理解する

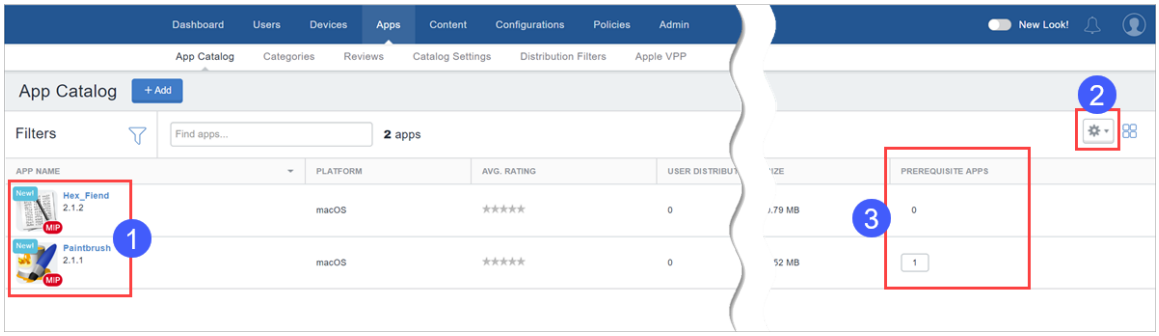
Packager自社開発macOSアプリをインポートする場合、管理者はまず「必須アプリ」機能を有効化し(1)、管理者がインポートするアプリをインストールする前にインストールしておかなければならない必須アプリを検索(2)、および選択(3)します。



インポートすると、Packager自社開発macOSアプリがアプリカタログに表示され、MIPバッジが下に表示されます1。その後、カラム設定2を追加し、を使用し、[必須アプリ] カラム3を追加し、依存関係のある、つまり、必須アプリを持つアプリを一覧表示することができます。

- MIP、非MIP、市販アプリ(Apps and BooksおよびmacOS App Storeの市販アプリ) は、必須アプリとして検索と選択が可能です。
- Apps and Books必須アプリをサイレントにインストールするには、ユーザーがApps and Booksライセンスに同意する必要があります。
- 非Apps and Booksの市販必須アプリについては、管理者が市販アプリを明示的に配布し、ユーザーが市販アプリをインストールする必要があります。市販アプリ(Apps and Booksアプリと非Apps and Booksアプリ) を必須アプリリストに表示させるには、アプリカタログにインポートする必要があります。ソースカラムには必須アプリのタイプが表示されます。
- 非MIPの必須アプリがある非MIPの自社開発アプリをインストールするには、MDMチェックインが必要です。
- ユーザーは非Apps and Booksの必須アプリを手動でインストールする必要があります。

- Apps and Booksトークンが削除された、またはライセンスが足りなくなった場合、必須アプリとして選択されたApps and Booksアプリもメインアプリもインストールされません。管理者はベストプラクティスに従い、そのようなApps and Booksアプリの事例について事前にユーザーに伝達する必要があります。

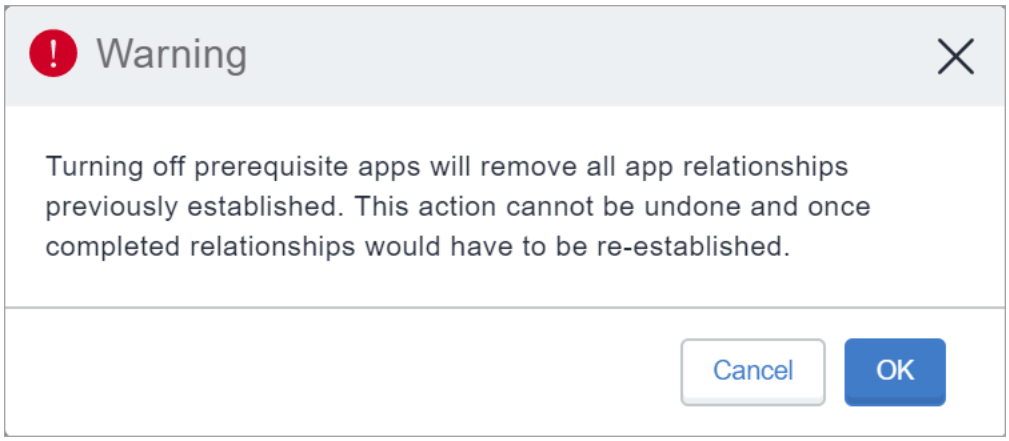


必須アプリも、明示的に配布されている場合は、独立したアプリとしてユーザーがインストールできます。ユーザーが必須アプリをアンインストールしようとした場合：

- 次のデバイスチェックイン時に再び必須アプリがインストールされます。
- 同じデバイス上に依存するメインアプリがない場合は、必須アプリがアンインストールされます。
- 必須アプリが明示的に配布されていない場合、必須アプリはメインアプリとともにアンインストールされます。
- 必須アプリが明示的に配布されている場合、必須アプリはデバイスに残ります。
- 必須アプリに依存アプリがある場合、必須アプリはデバイスに残ります。

必須アプリ機能のオフ

依存関係のあるアプリや必須アプリの更新、削除、委譲など、これらのアプリを操作する場合には、アプリの依存関係または必須ステータスが実行しようとしている操作に及ぼす影響についてのシステムプロンプトが表示される場合があります。たとえば、あるアプリの必須アプリ機能をオフにしようとすると、次のプロンプトが表示されます。



- あるアプリの必須アプリ機能をオフにすると、その必須アプリに関する詳細はクリアされます。これには、サブスペースからの必須アプリの自動委譲および委譲解除が含まれます。
- Apps@Workでは、内部のクライアントに必須アプリがまだインストールされていない依存アプリには、インストールボタンが表示されません。
- ユーザーがユーザーのデバイスに依存性のある自社開発アプリをインストールしようとすると、まず必須アプリがインストールされ(すでにインストールされていない場合) 、その後にメインアプリがインストールされます。これには数分かかることがあります。依存アプリのリストは、インストールの有無とともにユーザーに表示されます。

スペースからの必須アプリの委譲および委譲解除

- アプリ(メインアプリ) に関連付けられている必須アプリは、メインアプリがサブスペースに委譲されるときに自動的に委譲されます。
- メインアプリがサブスペースから委譲解除されると、必須アプリが明示的に配布されていない場合は必須アプリも委譲解除されます。ただし、複数のメインアプリに関連付けられた必須アプリは、委譲解除されません。
- 必須アプリが明示的に委譲されている場合には、自動的に委譲解除されることはありません。

Android Enterprise自社開発アプリのデバイス許可の委譲

Android Enterpriseで管理されているデバイスやAMAデバイスに適用できる自社開発アプリには、委譲許可を割り当てることができます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[アプリカタログ]** で、デバイス許可を委譲したいアプリを選択します。
3. **[アプリ構成]** タブをクリックします。
4. [委譲デバイス許可(自社開発のAndroid Enterpriseアプリ)] で、アプリに必要な権限を選択します。

   AMAPIを使用するのはCOSU導入のみです。詳細については、AMAPIのセクションを参照してください。

   - **サードパーティアプリランタイム許可の構成**
   - **サードパーティアプリの非表示および保留**
   - **証明書の管理**
   - **アプリ構成の管理**
   - **アプリアンインストールのブロックの管理**
   - **システムアプリの有効化の管理**
   - **証明書選択の管理**(AMAPIモードではサポートされません)
   - **アンインストールされたアプリ保持の管理**(AMAPIモードではサポートされません)
   - **ネットワークログ収集の管理**(一度に1つのアプリのみでサポートされます)
   - **セキュリティログ収集の管理**(一度に1つのアプリのみでサポートされます)
   - **既存のアプリのインストール管理**(AMAPIモードではサポートされません)
   - **パッケージのインストールと削除**(AMAPIモードではサポートされません)

   サポートされるすべてのAndroidデバイス所有者モードデバイス(7.0以降)には、パッケージのインストールと削除のオプションがあります。他の委譲許可は、Android 8.0以降にのみ適用されます。
5. 配布オプションを **[アプリを利用する全員]**、**[なし]**、**[カスタム]** から選択します。
6. **[保存]** をクリックします。

iOS社内アプリのプロビジョニングプロファイルステータス表示

iOS自社開発アプリのアプリカタログページにあるプロビジョニングプロファイルステータスを表示します。プロファイル名の横にあるツールチップは、プロファイルの有効期限の残りを日数で表示します。このステータスは、社内アプリのプロビジョニングプロファイルがいつ期限切れになるのか確認する際に便利です。

このステータスは、プロファイルの期限切れが原因でインストールされないアプリのトラブルシューティングにも役立ちます。適切なプロビジョニングプロファイルがない場合、アプリはインストールされても起動しません。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. 右上の歯車アイコンをクリックするとカラムが表示されます。
3. **[プロビジョニングプロファイル]** を選択し、アプリカタログページにあるアプリリストのカラムを表示します。

プロビジョニングプロファイルの詳細は、アプリ詳細ページの [プロビジョニングプロファイル設定] セクションにもあります。

iOS自社開発アプリのプロビジョニングプロファイル更新

プロビジョニングプロファイルは、特定のiOS自社開発アプリに適用されます。アプリのプロビジョニングプロファイル情報はアプリの詳細ページにあります。iOS社内アプリをデバイスで起動するには、期限の切れていないプロビジョニングプロファイルが必要です。期限が切れている場合は、アプリ詳細ページにプロファイルをアップロードし、プロビジョニングプロファイルを更新してください。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. プロビジョニングプロファイルの更新が必要なアプリをクリックします。アプリの詳細ページが表示されます。
3. **[編集]** をクリックします。
4. **[プロビジョニングプロファイル]** セクションで **[ファイルを選択]** をクリックします。
5. アップロードするプロビジョニングプロファイルファイル(.mobileprovision file extension) を選択し、**[保存]** をクリックします。

Google Playへの社内アプリ追加

自社開発アプリをGoogle Playのプライベートチャネルにアップロードし、Android Enterprise有効デバイスに配布できるようにIvanti Neurons for MDMにインポートします。

手順

1. Googleのプライベートアプリコンソールにログインしてください：https://play.google.com/apps/publish
2. 左メニューの **[すべてのアプリケーション]** をクリックします。
3. **[新しいアプリケーションを作成]** をクリックし、アプリケーションの名前を入力します。
4. **[APKをアップロード]** をクリックし、作成した.apkファイルをアップロードします。
5. **[ストアの目録]** をクリックします。
   - 説明文とその要約版を入力します。
   - 全タブのスクリーンショットをアップロードします。
   - 高解像度アイコンをアップロードします。
   - フィーチャーグラフィックアイコン(graphic.png) をアップロードします。
   - カテゴリ分類に必要な情報、問い合わせ先、プライバシーポリシーを入力します。
   - アプリ評価のための質問表に記入します。
6. **[価格と配布]** をクリックします。
   必要な情報をすべて入力すると、ページ最上部に [公開準備完了] と表示されます。
7. Ivanti Neurons for MDM の [アプリケーション] タブに移動します。
8. **[利用可能なカタログを再読み込み]** をクリックしてプライベートアプリを同期します。

> アプリの公開には数時間かかる場合があります。

Android Enterpriseデバイス対応Webアプリの追加

Webアプリとは、任意のWebサイトへのリンクであり、ショートカットとしてデバイスにインストールされます。Webアプリは他のアプリと同様に動作します。つまり、アプリと同じ基準で配布可能です。アプリカタログに表示され、ユーザーによって他のアプリと同様にインストールされます。ただしWebアプリには1つしかバージョンがなく、サイレントインストールには対応しません。WebアプリはWebクリップを使用して構成としてデバイスにインストールされますが、アプリとして動作します。

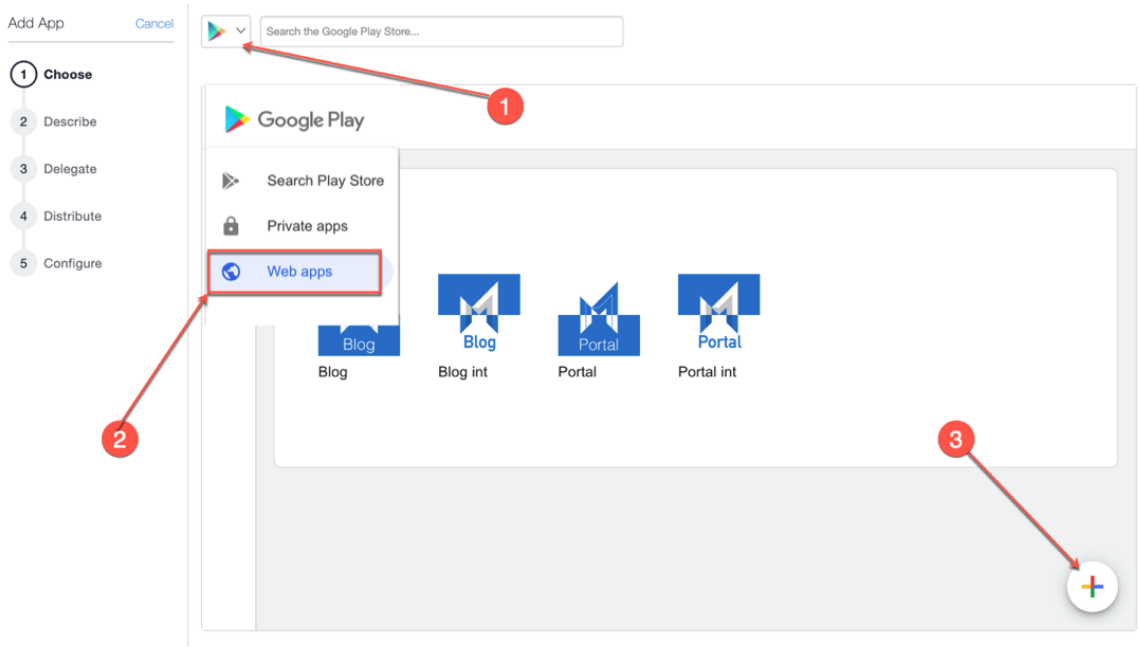
ユーザー向けのアプリカタログでWebアプリを提供するには、Webクリップをアプリカタログ内のアプリとして設定します。Webクリップは構成として定義できますが、構成は管理者しか配布できません。ユーザーはWebアプリを自分のデバイスにインストールするか、オプトアウトするかを選択できますが、Webクリップ構成をオプトアウトすることはできません。

Android Enterpriseでは、Webアプリとは、仕事用プロファイル内部のGoogle Chrome上で実行される、埋め込まれた形のWebアプリです。これは、Android Enterprise内のVPNソリューションやSSOソリューションに結合できます。作成されたWebアプリは、他のAndroidアプリと同様に動作し、必要に応じて配布できます。Webアプリを実行するには会社所有デバイス上の仕事用プロファイルにChromeをインストールする必要があります。

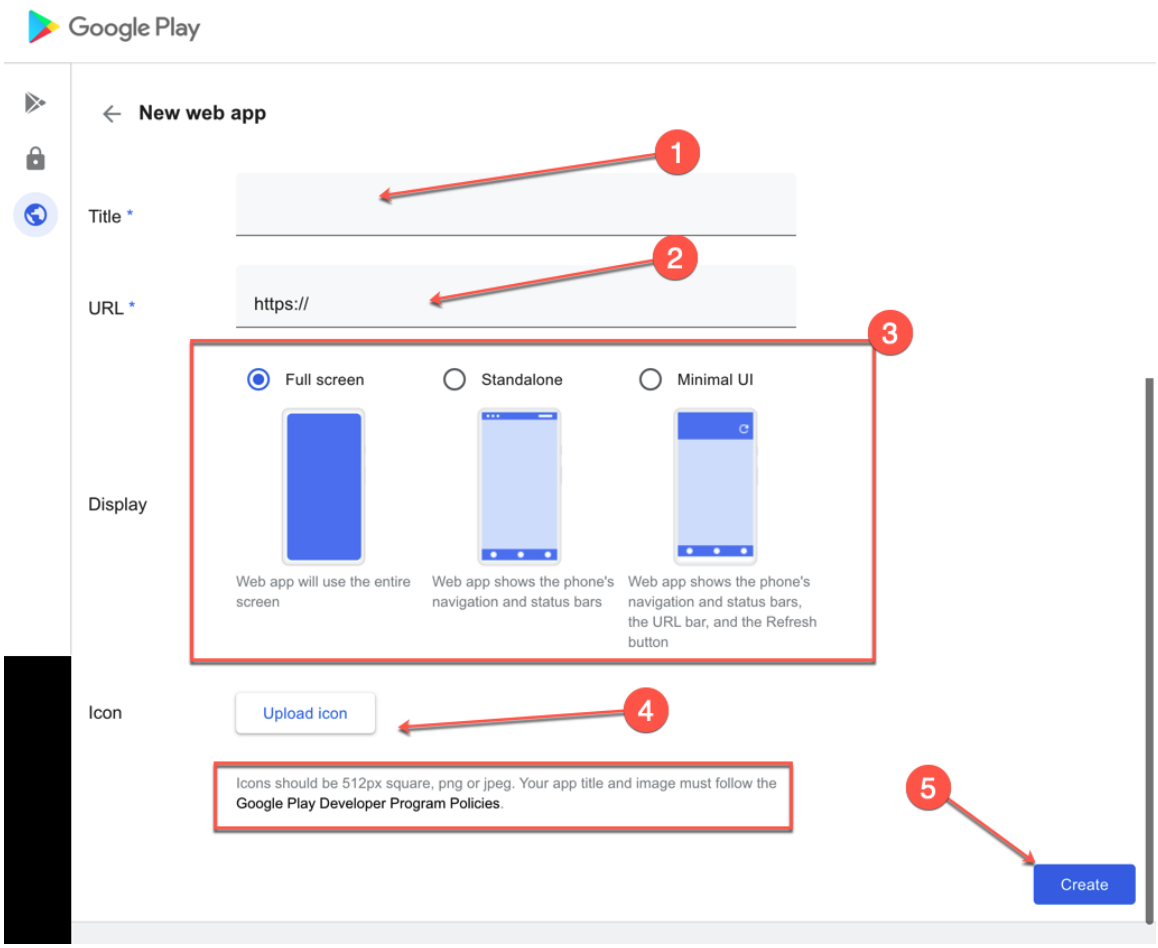
この機能の使用に関して問題がある場合は、管理者からサポートにお問い合わせください。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[+追加]**(左上)をクリックします。
3. ドロップダウンリストから **[Google Play]** を選択し、Google Playストアのアプリを検索します。Android Enterpriseが登録されている場合は、Google Play iFrameが表示されます。
4. **[Webアプリ]** をクリックします。



5. ユーザーにアプリの説 明をする:



   a. アプリのタイト ルまたは名 前

   b. アプリURL

   c. Webアプリの表 示タイプ

   d. アップロード アイコン(512ピクセル四 方 のPNGまたはJPEG画 像)

6. **[作 成]** をクリックします。iFrameにアプリが公 開されるのを待 ちます。これには数 分 かかることがあります。閉じて後 で再 び開いてもかまいません。

7. Webアプリを公 開した後 、アプリをアプリカタログにインポートして配 布します。Webアプリアイコンをクリックします。

8. 下へスクロールして **[選択]** をクリックします。
9. カテゴリーと任意の説明を追加します。
10. **[次へ]** をクリックします。
11. 以下のアプリ委譲オプションから1つ選択します。
    - このアプリをすべてのスペースに委譲
    - このアプリをすべてのスペースに委譲しない
12. **[次へ]** をクリックします。
13. アプリケーションの配布オプションを選択します。
14. **[完了]** をクリックします。

Webアプリは、追加した後、いつでも必要に応じて編集できます。手順は以下のとおりです。

1. **[アプリカタログ]** ページで既存のWebアプリの名前をクリックします。
2. **[編集]** をクリックし、Webアプリフィールドを編集します。

iOSデバイス対応Webアプリの追加

Webアプリとは、任意のWebサイトへのリンクであり、ショートカットとしてデバイスにインストールされます。Webアプリは他のアプリと同様に動作します。つまり、アプリと同じ基準で配布可能です。アプリカタログに表示され、ユーザーによって他のアプリと同様にインストールされます。ただしWebアプリには1つしかバージョンがなく、サイレントインストールには対応しません。WebアプリはWebクリップを使用して構成としてデバイスにインストールされますが、アプリとして動作します。

ユーザー向けのアプリカタログでWebアプリを提供するには、Webクリップをアプリカタログ内のアプリとして設定します。Webクリップは構成として定義できますが、構成は管理者しか配布できません。ユーザーはWebアプリを自分のデバイスにインストールするか、オプトアウトするかを選択できますが、Webクリップ構成をオプトアウトすることはできません。

この機能の使用に関して問題がある場合は、管理者からサポートにお問い合わせください。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[+追加]**(左上)をクリックします。
3. **[Webアプリ]** をクリックします。
4. ユーザーにアプリの説明をする:
   a. アプリ名
   b. アプリURL
   c. プラットフォームの種類
   d. アプリアイコン
   e. カテゴリを追加または削除します。
   f. フルスクリーン - Webアプリをフルスクリーンアプリケーションとして表示する場合に選択します。
   g. 削除可能 - Webアプリを削除可能にする場合に選択します。
   h. **[次へ]** をクリックします。
5. 以下のアプリ委譲オプションから1つ選択します。
   - このアプリをすべてのスペースに委譲
   - このアプリをすべてのスペースに委譲しない
6. **[次へ]** をクリックします。
7. アプリケーションの配布オプションを選択します。
8. **[完了]** をクリックします。

Web アプリケーションの編集

Webアプリは、追加した後、いつでも必要に応じて編集できます。

手順

1. **[アプリカタログ]** ページで既存のWebアプリの名前をクリックします。
2. **[編集]** をクリックし、Webアプリフィールドを編集します。

アプリケーションの低速展開

低速展開設定では、管理者が新しいバージョンのアプリケーションを自動的に段階的にデバイスに展開できます。[スローロールアウトの配布方式を使用] のオプションは、アプリケーションの次のリリースを展開するときに表示されます。Ivanti Neurons for MDM 管理ポータルでは、低速展開が一時停止されているときでも、アプリケーションを編集できます。

1つのリリースにスローロールアウトを設定すると、最新の設定と同じパーセンテージが次のリリースにも適用されます。配布を100%に設定した場合、アプリケーション配布の一時停止が可能です。ただし配布ターゲットを100%に設定した場合、UIがパーセンテージを0%にリセットするため、次のバージョンのターゲットパーセンテージは手動で設定する必要があります。

手順

1. **[アプリカタログ]** > **[アプリ]** を開き、いずれかの配布モードオプションを選択します。
2. **[セレクションサマリーにおけるデバイスのカスタム%(スローロールアウト)]** のオプションを選択します。
3. **[スローロールアウト設定]** から **[配布のターゲット%を指定]** のスライダーをドラッグします。
4. **[確認]** をクリックした後、**[完了]** をクリックします。最新のアプリバージョンのステータスが表示されます。[アプリカタログ] ページで表にスローロールアウトのステータスが表示されます。

[アプリカタログ] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。アプリケーションとコンテンツの管理ロールが必要です。

詳細検索の使用

詳細検索オプションを使用すると、特定の基準を満たすアプリを識別して表示するためのルールに基づいてアプリを検索できます。これらのルールは、「等号」、「は次より小さい:」、「は次より大きい:」、「は次と等しい:」、「は次と等しくない:」などの、適切な演算子を使用して作成できます。[ANY (OR)] または [ALL (AND)] オプションを使用すれば、ルールオプションをネストでまとめることができます。ルールに一致するアプリは、セクションの下に表示されます。

検索に使用するカスタム属性値では大文字と小文字が区別されます。

手順

1. [アプリカタログ] ページの **[詳細検索]** リンクをクリックします。[詳細検索] ウィザードが開きます。
2. 次のオプションのいずれかをクリックします。
   - **いずれか:** 少なくともルールの1つと一致するアプリを検索する場合
   - **すべて:** すべてのルールと一致するアプリを検索する場合
3. 検索基準を定義するルールを作成します。**例:**「APNS対応は次と等しい:はい」。

4. (任意) **[+]** をクリックし、必要に応じて他のルールを作成します。
5. **[検索]** をクリックします。検索基準に一致するアプリのリストが表示されます。

検索クエリのロード

保存した検索クエリのリストを表示できます。

手順

1. [詳細検索] をクリックし、フォルダアイコンをクリックします。**[クエリを読み込む]** セクションに、作成された検索クエリのリストが表示されます。次の詳細が表示されます。
   - **クエリ名** - 読み込まれたクエリの名前。
   - **クエリの内容** - 検索クエリを定義するルールの内容を表示します。
   - **アクション** - クエリに実行するアクションを選択します。
2. **[アクション]** カラムの **[クエリを読み込む]** をクリックすると、読み込まれたクエリに定義された基準に一致するアプリのリストが表示されます。
3. **[削除]** をクリックすると、読み込まれたクエリが削除されます。

関連トピック

- 「ユーザーの役割」ページ128
- 「アプリカタログからのアプリ削除」ページ366
- 「アプリ依存性の導入」ページ396

Apps@Work (iOS、Android、Windows、macOS)

Apps@Work はソフトウェアおよびアプリケーションの安全な配布を支援するエンタープライズ アプリケーション ストアフロントです。Apps@work は iOS、Android、macOS、Windows デバイス版が提供されています。Apps@Workの企業用AppStoreが、iOS、Android、およびmacOS版のIvanti Go appクライアントおよびMobile@Workクライアントと統合されます。Windows デバイスでは、ネイティブ スタンドアロン アプリケーションです。このセクションは以下のトピックを含みます。

- 「iOS Apps@Work」下
- 「Android Apps@Work」ページ319
- 「macOS Apps@Work」ページ319
- 「Windows Apps@Work」ページ320

iOS Apps@Work

Apps@work ネイティブ アプリストアは自動的に Go クライアントとともに配布されます。管理者によるアクションは必要ありません。Apps@work タブは Go クライアントのタスクバーに表示されます。各ユーザのこのタブには、会社で承認されたアプリケーションが表示され、インストールできます。詳細については、「iOS Apps@Work AppStore Features」ページ322をご参照ください。

アプリケーション更新に関する iOS Apps@Work エンドユーザ通知は、既定で有効です。この設定を変更する場合は、「カタログ設定」ページ391の「**通知**」トピックをご参照ください。

既に iOS Apps@Work Webclip を使用している場合

レガシー iOS Apps@Work webclip が導入されている場合は、既定ではネイティブ統合されたアプリケーション カタログがありません。iOS Apps@Work ネイティブ カタログに移行し、Apps@work webclip をデバイスから削除する場合は、次の手順を実行します。

構成のプッシュ

Go クライアント アプリケーションからネイティブ アプリストア エクスペリエンスで Apps@Work を提供するには、管理者がネイティブ クライアントのアプリケーション カタログ構成をデバイスにプッシュする必要があります。詳細については、「構成の操作」ページ424をご参照ください。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** > [フィルタ] に移動し、**[クライアント サービス]** を選択します。すべてのクライアント構成が一覧表示されます。
3. **[ネイティブ クライアントのアプリケーション カタログ]** を選択します。[ネイティブ クライアント構成のアプリケーション カタログ] ページが開きます。
4. **配布の編集** アイコンをクリックします。[配布の編集] ページが開きます。
5. 以下のオプションから1つ選択してください：
   - **すべてのデバイス**
   - **デバイスなし** - どのデバイスにも配布しない場合
   - **カスタム** - デバイス、デバイス グループ、ユーザ、ユーザ グループを選択できます
6. 構成が配布された後、ユーザは Go クライアント バージョン83以降にアップグレードする必要があります。Apps@Work タブは Go app クライアントに表示されます。

> デバイスで Go クライアントが使用できないため、iReg を使用して登録されたデバイスでは構成をプッシュできません。ネイティブ アプリケーション カタログを取得するには、Go app クライアントをインストールする必要があります。詳細については、「デバイス登録 (iOS、macOS、Android)」 ページ 204 をご参照ください。

iOS Apps@Work Webclip の削除

Apps@Work Webclip をデバイスに配布し、既に Apps@Work ネイティブ エクスペリエンスに移行した場合は、iOS Apps@Work webclip を削除できます。

手順

1. **[構成]** を開きます。
2. 構成のフィルタ – **Apple App Catalog**。
3. **[編集]** をクリックします。
4. **[配布]** で **[デバイスに配布しない]** を選択します。
5. **[保存]** をクリックします。

Android Apps@Work

Apps@work ネイティブ アプリストアは自動的に MI Go クライアントとともに配布されます。管理者によるアクションは必要ありません。Apps@work タブは Mi Go クライアントのタスクバーに表示されます。各ユーザのこのタブには、会社で承認されたアプリケーションが表示され、インストールできます。詳細については、「[管理] - [Android Enterprise]」 ページ1277 をご参照ください。

macOS Apps@Work

MacOs Apps@work は macOS Mobile@Work クライアントと統合されています。デバイスがIvanti Neurons for MDMに登録されると、クライアントが切り替わり、Apps@Workとして表示されます。新しく作成されたテナントでは、Apple App Catalog Webclip 構成が macOS デバイスにプッシュされません。必要に応じて、管理者は Apps@work Webclip 構成を macOS デバイスに配布できます。詳細については、「macOSデバイスの構成」 ページ22をご参照ください。

macOSアプリの配布

- Ivanti は Apple MDM プロトコルで Mobile@Work を使用した macOS アプリケーションの配布をサポートします。管理者は以下のいずれかまたは両方を選択可能です。
    - AppleのMDMプロトコル - 管理者は、所定のPKG形式(配布形式)のみ自社開発アプリとしてアップロードできます。また、Mac App Storeからアプリを配布することも可能です(Appleの「Appとブック」ライセンスサポートを含む)。ただしこの方法で管理者がDMGおよび他のPKG形式を配布することはできません。
    - macOS対応Mobile@Workアプリ - ユーザーにアプリを配布する方法として、管理者はMobileIron Packager(MIP)アプリを使用し、任意のPKG、DMG、.appファイルをMIPファイルに変換できます。MIPファイルを自社開発アプリとしてIvanti Neurons for MDMにアップロードします。
- ソフトウェアダウンロードサイトからユーティリティをダウンロードできます。
- 管理者はMobile@Workを使用し、DMG、PKG、.app形式の自社開発アプリを配布できます。Mac App Storeでのみ提供されるアプリの場合、管理者は「Appとブック」ライセンス機能を含むAppleネイティブのMDMを引き続き使用できます。詳細については、「macOSデバイスの構成」 ページ22をご参照ください。

Windows Apps@Work

Apps@Work はスタンドアロンのネイティブ アプリケーションで、Microsoft Store からダウンロードするか、Ivanti Neurons for MDM から直接プッシュできます。Windows 10以上のデバイスでは、Ivanti Neurons for MDM で Windows 公開アプリケーションと社内アプリケーションを使用できます。Apps@Work はサポートされている Windows 10以降のデバイスでサイレント インストールされます。

詳細は「アプリ構成」ページ337をご参照ください。

Windows Apps@Work の使用

Apps@Workにより、Windows 10デバイス上のWindows公開アプリや自社開発アプリをIvanti Neurons for MDMで利用できるようになります。Apps@Workは、サポートされているWindows 10デバイスにサイレント インストールされます。

Apps@Work 証明書認証

Windows Apps@Work で証明書認証を使用するには、次の手順を実行します。

1. **[管理] > [Windows] > [Apps@Work 証明書認証]** に移動します。
2. 設定を**オン**にします。

   設定を**オフ**にすると、ユーザ名とパスワードを使用する必要があります。

Windows対応のApps@WorkではSAMLがサポートされません。

Apps@Work用にアプリを構成するには:

1. Windowsアプリを選択します。
2. **[アプリ構成]** タブをクリックします。
3. **[デバイスにインストール]** をクリックします。
   Windows自社開発アプリの構成は、サイレントインストールフラグ、またはApps@Workを使用したインストールのいずれかに設定できます。パブリックアプリは、サイレントインストールに設定できません。
4. 任意で、Apps@workカタログにアプリを表示するか非表示にするかを選択します。
   この選択は社内アプリのみ可能です。

5. **[プロモーション]** タブをクリックします。

> 現在、Apps@Work ではバナープロモーションがサポートされていないため、使用可能なオプションは **[特集]** および **[特集以外]** です。
> 市販アプリでは **[プロモーション]** オプションのみ表示されます。

iOS Apps@Work AppStore Features

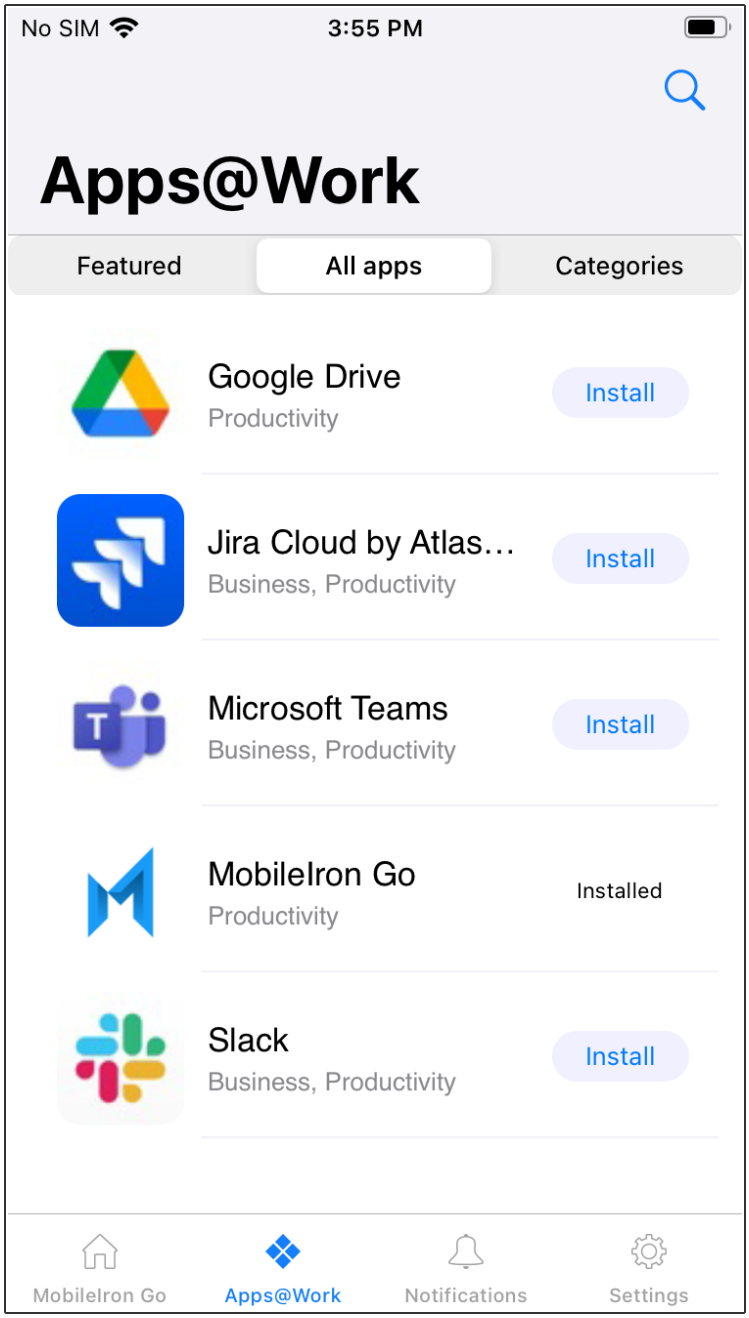
Apps@Work タブには次 の機 能 があります。

- 「 Go アプリケーションから Apps@Work タブにアクセス」 下 から Apps@Work タブにアクセス
- 「検 索 」 ページ324
- 「 アプリのインストール - ボタン状 態 」 ページ326
- 「特 集 されたアプリケーションとバナー」 ページ330
- 「アプリケーション更 新 通 知 」 ページ332
- 「設 定 -デバイス」 ページ332

Go アプリケーションから Apps@Work タブにアクセス

手 順

1. iOS デバイスから Go app にログインします。
2. **Apps@Work** アイコンをタップします。[すべてのアプリケーション] と [カテゴリ] という2つの既 定 のタブを使 用できます。



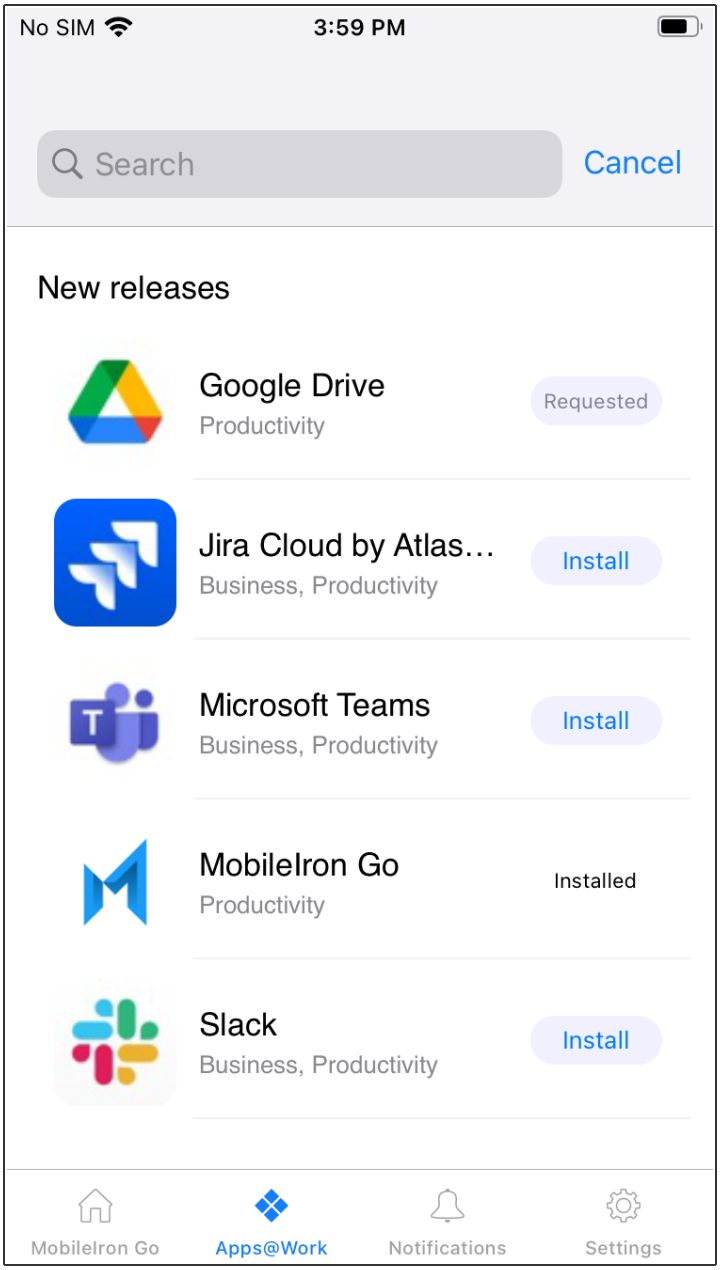
3. **[すべてのアプリ]** タブをタップします。[すべてのアプリケーション] リストにはすべてのアプリケーションがアルファベット順に表示されます。
4. **[カテゴリ]** タブをタップします。[カテゴリ] タブには、アプリケーションが含まれるカテゴリのみが表示されます。
   - 各カテゴリには存在するアプリケーションの数が表示されます。
   - [カテゴリ] タブの下の [アプリケーション] 行は、すべてのインストールされているアプリケーションが表示されたリスト項目です。[アプリケーション] 行は常に最初のカテゴリで、残りのカテゴリはアルファベット順に表示されます。
   - アプリケーションがインストールされていないと、MyApps リストに [なし] と表示されます。
   - カテゴリをクリックすると、カテゴリに固有のすべてのアプリケーションが一覧表示され、[インストール] オプションが表示されます。**[インストール]** をクリックして各アプリケーションを個別にインストールするか、**[すべてインストール]** をクリックしてカテゴリのすべてのアプリケーションをインストールします。各アプリケーションのインストールを許可するように指示されます。

検索

手順

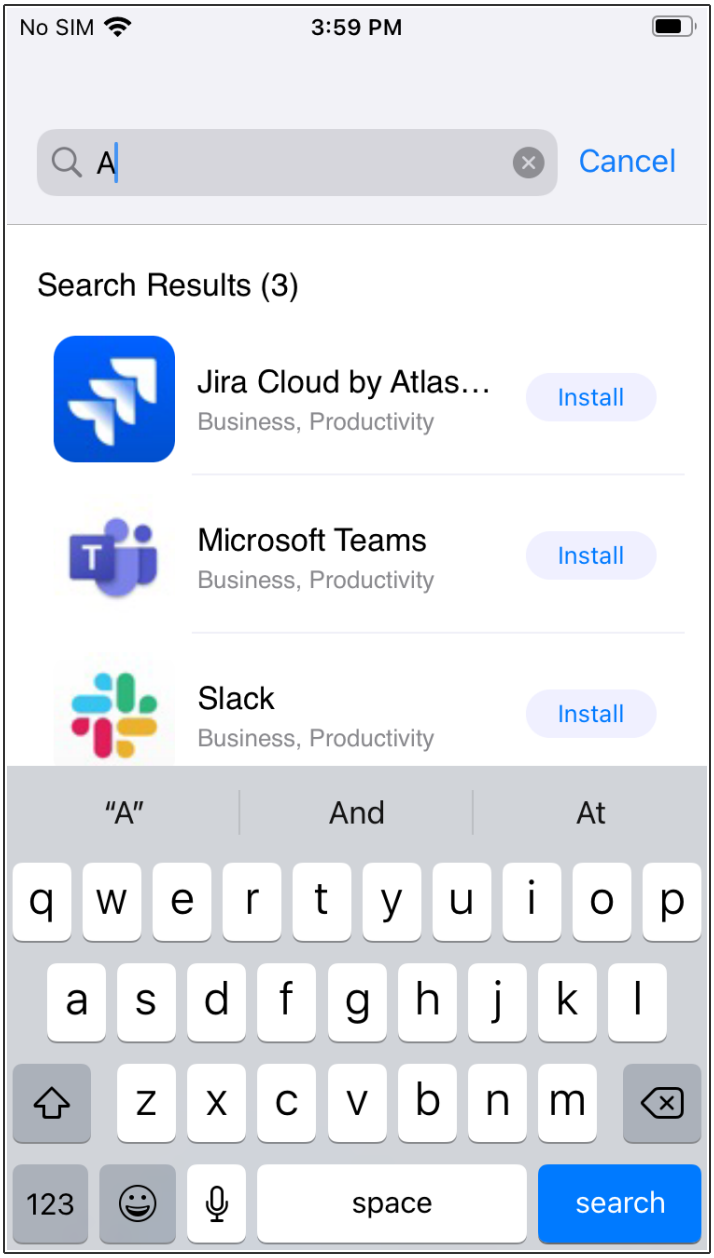
1. iOS デバイスから Go app にログインします。
2. **Apps@Work** アイコンをタップします。
3. 検索 (レンズ) アイコンをタップすると、次を検索します。

- **新しいリリース**-検索バーにテキストを入力していないときに表示される新しくリリースされたアプリケーションの一覧



- 文字を入力すると、検索フィールドで動的に予測され、一致するアプリケーションが表示されます。
- 検索結果件数は下位見出しとして表示されます。

- **[インストール]** ボタンをタップすると、詳 細 ページに移 動 せずに、アプリケーションがインストールされます。



アプリのインストール - ボタン状 態

アプリケーションのインストールでは、サーバが要 求 を処 理し、アプリケーションをデバイスにプッシュする必 要 があるため、インストール ボタンにはリアルタイムの進 行 状 況 が表 示 されません インストール ボタンの状 態 は [インストール] > [要 求 済 み] > [インストール済 み] に変 わります。

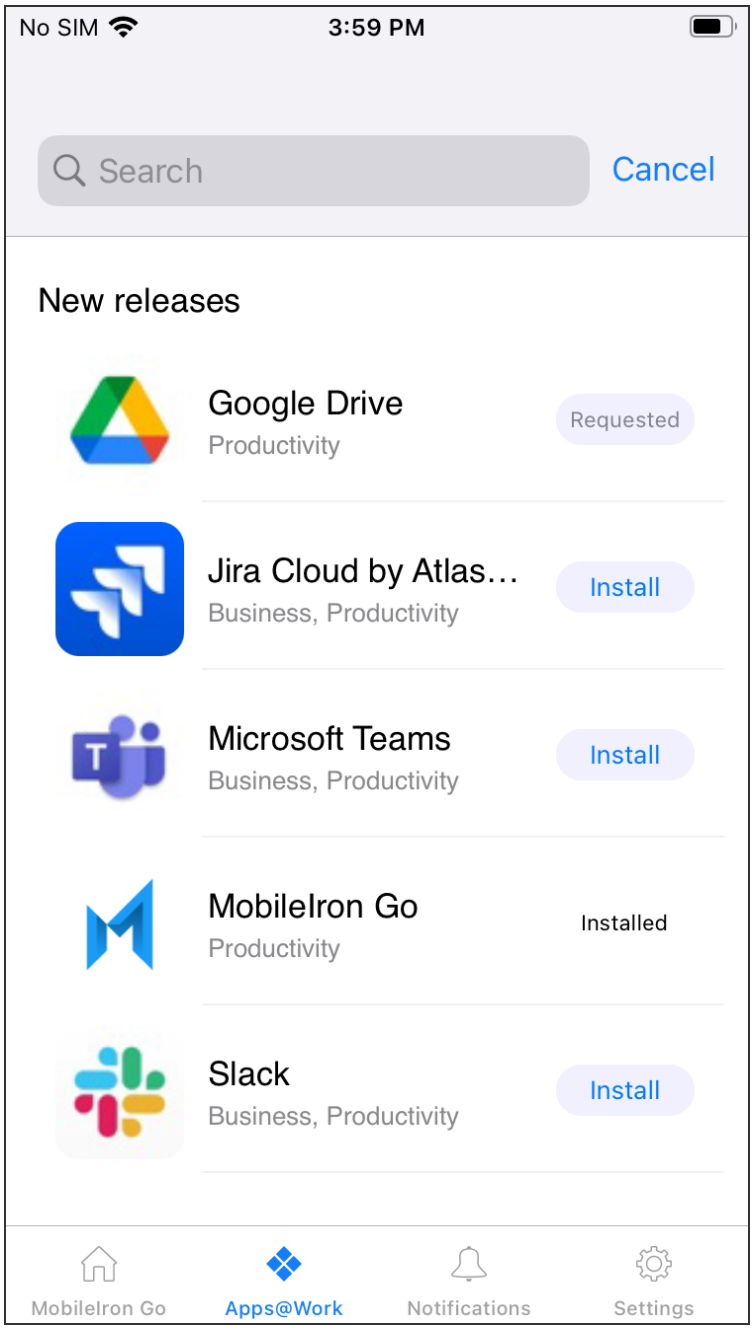
手順

1. iOS デバイスから Go app にログインします。
2. **Apps@Work** アイコンをタップします。

3. **[インストール]** をタップすると、ステータス通 知 が次 のように表 示 されます。

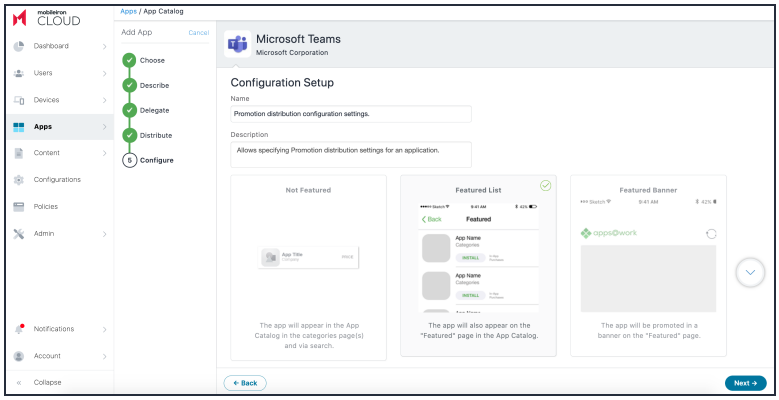
   - 初 めて、インストールが要 求 されたことを示 すアラート メッセージが表 示 されます。
   - [要 求 済 み] ボタンをタップします。アラート メッセージが表 示 されます。

   [インストール済 み] ステータスはボタンではありません。



特集されたアプリケーションとバナー

[特集] タブは管理者がプッシュした構成に基づいて表示されます。[特集] タブは、更新がないときの既定のランディング ページです。

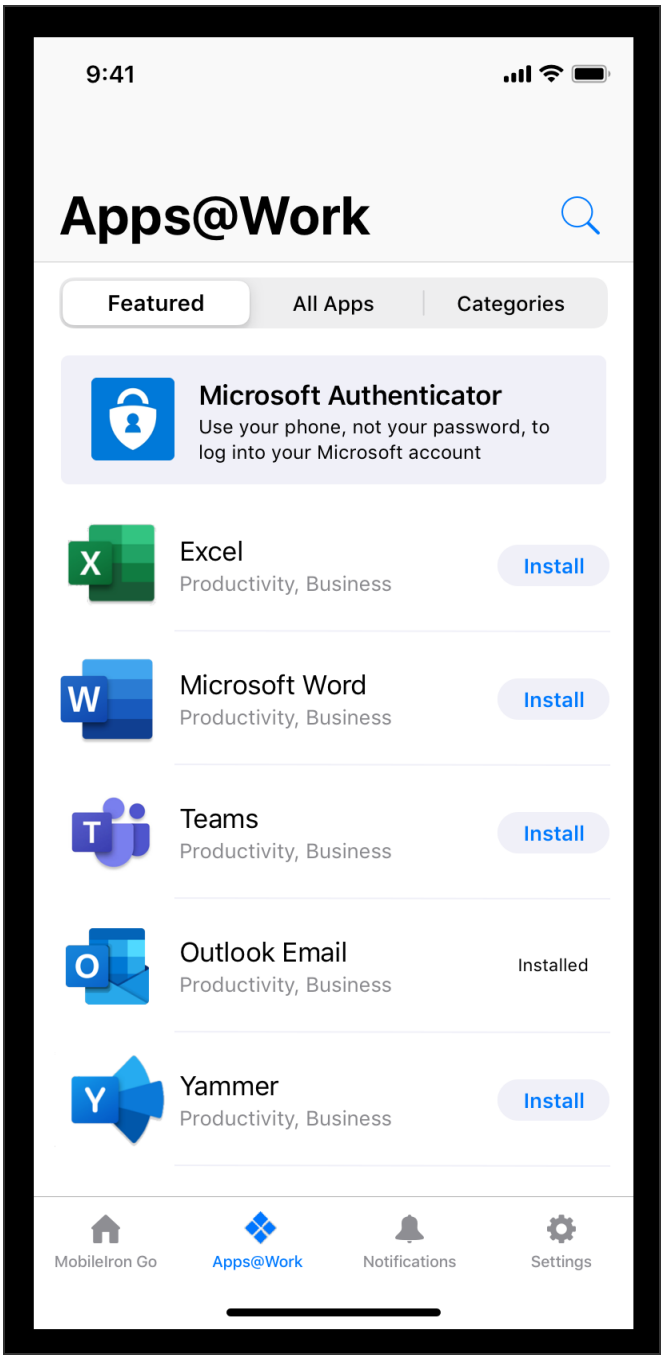


手順

1. iOS デバイスから Go app にログインします。
2. **Apps@Work** アイコンをタップします。

3. **[特集]** タブをタップします。

   - 特集されたアプリケーション バナーにはバナーに1つのアプリケーションが表示されます。
   - 特集されたアプリケーションには、すべての特集されたアプリケーションが一覧表示されます。

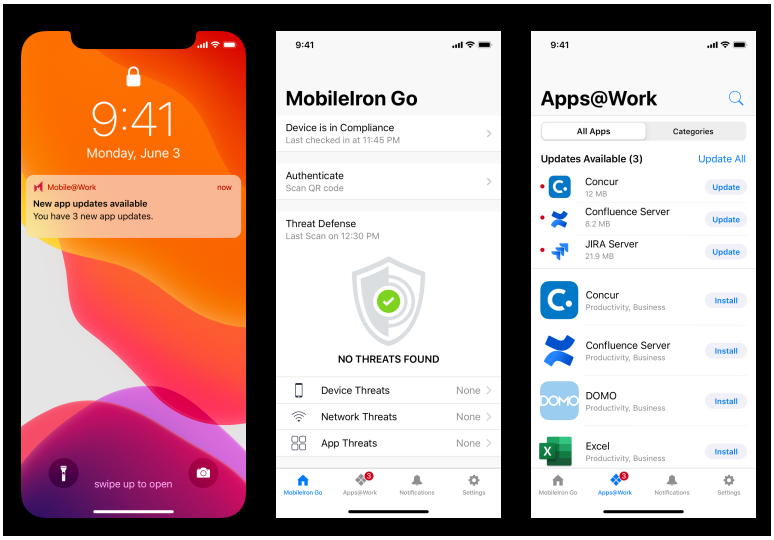


アプリケーション更新通知

アプリケーション更新が利用可能になると、デバイスで通知が表示されます。通知には利用可能な更新があるアプリケーションの数が表示されます。通知をクリックすると、Apps@Work が開きます。

手順

1. iOS デバイスから Go app にログインします。Apps@Work アイコンには、更新が保留中のアプリケーションの件数が表示されます。
2. アプリケーション更新通知をタップすると、Apps@Workの [すべてのアプリ] タブに移動します。次の情報が表示されます。
   - [すべてのアプリケーション] タブの下の [使用可能な更新] サブセクションには、更新可能なアプリケーションの件数が表示されます。
   - 更新が必要なすべてのアプリケーションに赤色のドット アイコンが表示されます。



設定 -デバイス

手順

1. iOS デバイスから Go app にログインします。
2. **[設定]** アイコンをタップします。
   - [デバイス] タブは [設定] の下にあります。
   - [デバイス] は [認証] の下の明細項目として表示されます。

アプリ詳 細 の表 示

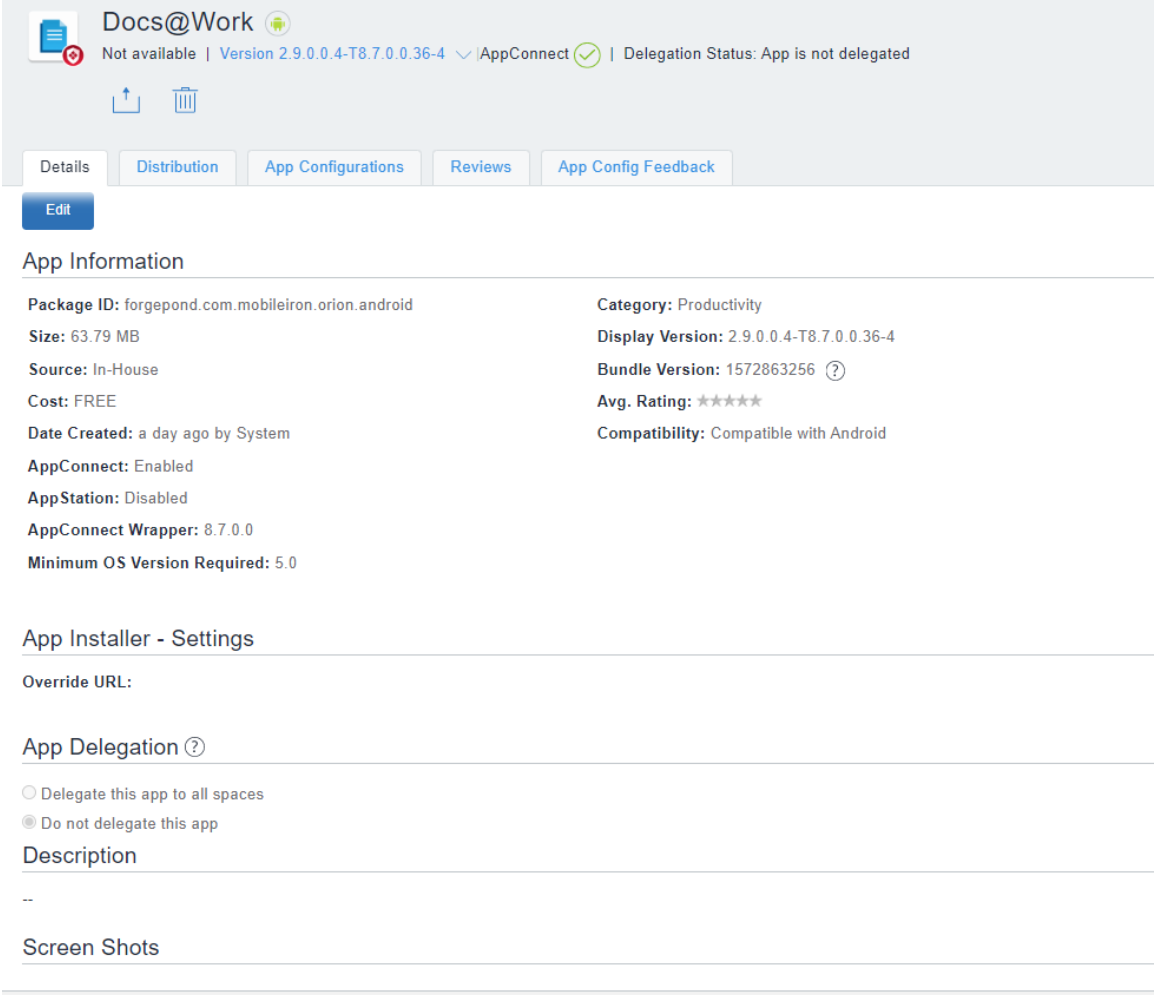
カタログ内 のどのアプリについても、アプリカタログからアプリ詳 細 に進 むことができます。アプリ詳 細 のページには、ディスプレイバージョン(例 : 1.5.0) 、バンド ルバージョン(例 : 1.5.0.42) 、最 小 OSバージョン(例 : Android 5.0) など、アプリの詳 細 情 報 が表 示 されます。

[最 小 OSバージョン] フィールド に指 定 されたバージョン以 外 のアプリはApps@Workカタログに表 示 されません。したがってそのようなアプリはデバイスに配 布 できません。[最 小 OSバージョン] フィールド はアプリの監 査 証 跡 の一 部 としても表 示 されます。

手 順

1. **[アプリ]** をクリックします。
2. **[アプリカタログ]** をクリックします。
3. アプリを選 択 します。

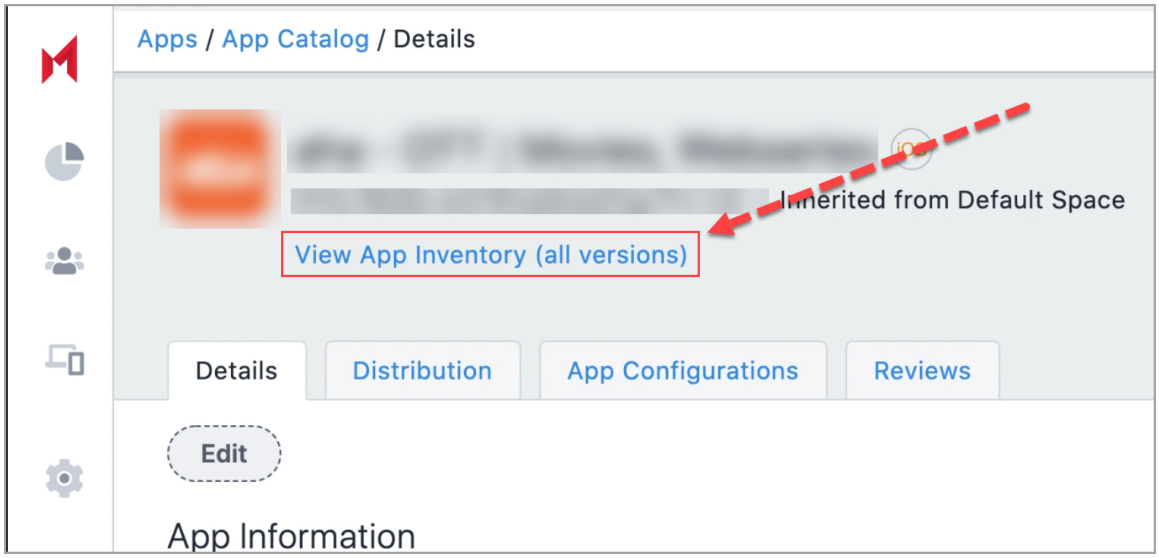
   [アプリの詳 細] ウィンド ウが表 示 されます。参 考 用 のサンプル ウィンド ウ:



- iOSの自社開発アプリの場合、アプリ詳細ページで **[プロビジョニングプロファイル有効期限]** を確認できます。
- アプリ情報に、すべてのiOSおよびiPadOS VPPアプリのオプションとして、**[アプリ配布時にM1デバイスへのインストールを許可]** が表示されるようになりました。管理者は、M1 macOSデバイスにインストールできるiOSまたはiPad VPPアプリケーションに対してのみ、**[アプリ配布時にM1デバイスへのインストールを許可]** オプションを有効化する必要があります。このオプションを有効化した場合のみ、アプリケーションのインストール中に管理者に対してM1 macOSデバイスが表示されます。マネージドアプリ構成は、M1 Mac デバイスの iOS VPP アプリケーションでサポートされます。
- [デバイスの詳細] に **[必須アプリ]** のトグルボタンが追加されました。管理者は、このオプションを選択し、メインのアプリの前提条件となるアプリを追加することができます。

アプリ詳細ページからアプリインベントリ情報を表示する

アプリインベントリ情報を表示するには、**[アプリ インベントリの表示 (すべてのバージョン)]** をクリックすると、**[デバイス] > [アプリ インベントリ]** にそのアプリのバンドル ID でフィルタリングされた一覧が表示されます。



アプリ構成

このセクションは以下のトピックを含みます。

- 「アプリの機能のライセンス」下
- 「複数のアプリに共通する構成手順」次のページ

アプリ構成では、ユーザーのデバイスに展開したそれぞれのアプリのインストール、プロモーションおよび配布をカスタマイズできます。アプリには、自社開発アプリ、パブリックストアのアプリ、またはIvanti Neurons for MDMアプリが含まれます。独自の名前を付け、各受信者に合わせて特別に構成することで、さまざまなユーザーやグループにアプリを柔軟に配布することができます。自社開発アプリのバージョン数は最大100です。これを超えた場合、Ivanti Neurons for MDMシステムはアプリケーションの最も古いバージョンを消去します。アプリケーションのアップロードと消去の状況は監査証跡ページで確認できます。

アプリカタログ内またはマネージドアプリ構成プロファイル内のアプリのアプリ構成値を変更するときは、デバイスで新しい構成値を受信するために、1回または2回のデバイスチェックインが必要です。

アプリの機能のライセンス

以下の機能には、追加のライセンスが必要です。

- アプリのサイレントインストール/アンインストール: Silverライセンス
- アプリごとの構成：Goldライセンス
- AppConnectカスタム構成：Gold ライセンス

将来のデバイスタイプをWindows OSで定義することはできないため、複数のアプリケーションパッケージがある場合は良好なグループ管理が必要です。このような場合、適切なバージョンのアプリをインストールする唯一の方法は、管理者が正しいグループを正しいアプリケーションに使用することです。

複数のアプリに共通する構成手順

まずこれらの手順を実行してから、展開したいそれぞれのアプリの構成手順に進んでください。同じアプリの複数の構成を設計し、それぞれの構成に一意の名前を付けることができます。展開戦略に合わせて、それぞれの構成に独自の配布およびプロモーションのレベルを設定できます。自社開発アプリのバージョン数は最大100です。これを超えた場合、Ivanti Neurons for MDM システムはアプリケーションの最も古いバージョンを消去します。アプリケーションのアップロードと消去の状況は監査証跡ページで確認できます。ユーザー、ユーザーグループ、デバイス、デバイスグループの最大数100までアプリケーションを導入可能です。アプリケーション カタログに追加するアプリケーションを選択できます。Ivanti Neurons for MDM では、iOS の [インストール/更新要求の送信] コマンドが非同期プロセスです。[インストール/更新要求の送信] コマンドを使用すると、Ivanti Neurons for MDM 管理ポータルに次のメッセージが表示されます。

- プロセスがバックグラウンドで実行され続けている
- プロセスが完了した
- プロセスが成功したか、エラーがあるかどうかを示すステータス

手順

1. **[アプリ]** > **[アプリカタログ]** を開き、**[+追加]** をクリックします。
2. プルダウンメニューを使用して、[App Store]、[Google Play] または [自社開発アプリストア] を選択し、カタログに追加するアプリを選びます。
   ライセンス契約によっては、アプリをお使いのカタログに追加できる場合もあります。
3. 任意でアプリの [カテゴリ] を編集します。
4. 任意で **[説明]** フィールドにアプリの簡単な説明を追加します。
5. **[次へ]** をクリックします。

6. アプリのこの構成の配布レベルを選択します。
   - **全員用** - すべてのユーザーの対応デバイスにアプリが追加されます。
   - **該当なし** - アプリは将来の配布用にステージングされます。
   - **カスタム配布** - 以下のいずれかを選択します。
     - **ユーザー/ユーザーグループ** - このアプリは、選択されたユーザーまたはユーザーグループにのみ配布されます。
       ユーザーを選択するには **[ユーザー]** タブをクリックします。
       ユーザーグループを選択するには **[ユーザーグループ]** タブをクリックします。
     - **デバイス/デバイスグループ** - このアプリは、選択されたデバイスまたはデバイスグループにのみ配布されます。
       デバイスを選択するには **[デバイス]** タブをクリックします。
       デバイスグループを選択するには **[デバイスグループ]** タブをクリックします。
7. **[次へ]** をクリックします。

インストールオプションの構成

インストール構成オプションを選択できます。

手順

1. **[アプリケーションのインストール構成の設定]** をクリックするか、**[+]** アイコンをクリックして別の構成を追加すると、**[構成設定]** ページが表示されます。
2. **[名前]** フィールドに構成の名前を入力します。
3. 任意で **[説明]** フィールドにインストール構成の簡単な説明を入力します。
4. **[デバイスインストール構成]** オプションを選択します。
5. 以下のオプションから1つ選択してください。
   - **デバイスでインストールが必要**
   - **デバイス登録時にのみインストール**

6. 次のオプションを選択します。
   - **Samsung Knox WorkspaceとZebraデバイスにサイレントインストール** (Android のみ)
   - **エンドユーザーのアプリカタログでアプリを表示しない**。
   - **アプリ更新モード** (AMAPIデバイスにも対応)。(Android のみ)
     このオプションを使用し、以下の3つのモードのいずれかでアプリを最新版に更新してください。
     - **デフォルト**:アプリ更新モードオプションを選択すると、まずこのモードが選択されます。このモードではアプリの提供開始から24時間以内に更新が実行されます。
     - **90日間延期**:この更新モードを選択すると、アプリの更新を90日間延期できます。90日後、アプリはマネージドGoogle Play構成の他の設定に基づき、自動的に更新されます。
     - **高優先度**:この更新モードを選択し、ユーザーのデバイスがオンラインの場合、アプリはGoogle Playストアに公開されるとすぐに更新されます。
   - **アプリケーション インストールの優先度を設定** - 詳細については、「アプリケーション優先度の構成」トピックをご参照ください。
7. 選択したアプリによっては他の構成オプションも表示される可能性があります。これらのオプションを利用して複数のキーと値のペアを追加できる場合もあります。そのような場合は **[+追加]** をクリックし、キーと値のペアを入力します。詳細については、「アプリのカタログ」 ページ286の**公開ストアからアプリケーションを追加**をご参照ください。
8. (macOS 11+) アプリをマネージドアプリとしてインストールし構成するには、以下のオプションを選択します。
   - **マネージドアプリとしてインストール**
   - **マネージドアプリに変換**

   macOS 12.0以降、ユーザー登録デバイスでマネージドアプリがサポートされます。

アプリ優先度の構成

デバイスの初回登録時には(具体的には登録日時から20分以内)、デバイスにアプリを受信する順序を定義できます。必須アプリは登録時にプッシュされ、インストールされます。これにより、特定のアプリを他のアプリより優先してダウンロード可能です。たとえばTunnelとメールEmailアプリを、他の重要でないアプリの前にダウンロードするなどです。この機能は、市販アプリにもプライベートアプリにも適用されます。必須アプリは依存アプリの前にプッシュされます。

この機能はiOS(AppStation for iOSを除く) デバイス、Android(Android for Enterpriseを除く) デバイス、macOS (自社開発PKGアプリ、Apple App、Apple Booksアプリ) デバイス、およびWindowsデバイスでサポートされています。

この機能は新規登録デバイスで使用します。デフォルトでは、すべてのアプリが優先度「中」に設定されています。このプロセスにおいて、ユーザーはカタログ内の任意のアプリを手動でインストールすることを選択できます。たとえそのアプリが、インストール時にリソースを競合し、優先度「高」のアプリよりも前にキューに入る可能性がある場合であっても、かまいません。

Windowsアプリの場合は、ブリッジアプリの優先度が他のどのアプリよりも高くなります。

[アプリインストール優先度を設定] オプションを使用してアプリの優先度を設定する手順については、前のセクション「インストールオプションの構成」を参照してください。アプリに対して「高」、「中」、「低」の優先度を設定できます。同じ優先度のアプリは特定の順序なしにインストールされます。ユーザーがすでにアプリをインストールしている場合、アプリ更新中はアプリの優先度が使用されません。

Apple アプリケーション管理構成設定の選択

これらの設定はこのアプリのみに適用され、**[アプリ] > [カタログ設定]** で選択されているグローバル設定より優先されます。**Appleアプリ管理** 設定を選択するには:

手順

1. **[Appleアプリ設定]** をクリックするか、**[+]** アイコンをクリックして別の構成を追加すると、**[構成設定]** ページが表示されます。
2. **[名前]** フィールドに構成の名前を入力します。
3. **[説明]** フィールドに構成の簡単な説明を入力します。
4. **[Apple 管理設定]** の次のオプションを1つ以上選択または選択解除します。
   - **iCloudおよびiTunesへのバックアップを防止**
   - **登録解除時にアプリを削除**
   - (iOS 14.0+) **このアプリの削除とオフロードを許可** - このオプションの選択を解除すると、ユーザーはマネージドアプリを削除およびオフロードできなくなります。
   - (任意) **Apple マネージドアプリ構成** を追加
5. **[更新]** をクリックします。

アプリのプロモーションレベルの選択

アプリケーションの昇格のレベルを設定できます。

手順

1. **[プロモーション配布構成の設定]** をクリックするか、**[+]** アイコンをクリックして別の構成を追加すると、**[プロモーション構成]** ページが表示されます。
2. **[編集]** をクリックします。
3. **[名前]** フィールドにプロモーション配布構成の設定の名前を入力します。
4. 任意で **[説明]** フィールドに構成の簡単な説明を入力します。
5. アプリに与えたいプロモーションレベルとして、**[未注目]**、**[注目リスト]**、**[注目バナー]** 使用のいずれかを選択します。**[未注目]** を選択した場合、アプリはリストされません。
6. [注目バナー] を選択した場合は、次の詳細を指定します。
   a. **タイトル** - アプリケーションのタイトルを指定します
   b. **説明** - アプリケーションの詳細を指定します
   c. **バナースタイル** - バナーの色を選択します
7. **[+説明を追加]** をクリックし、構成の簡単な説明を入力します。
8. 任意で構成の配布を変更します。
9. **[完了]** をクリックするとアプリ構成が保存されます。

AppTunnelトラフィックルールの構成

Sentryを使用してサービスへのアクセスを許可するトラフィックルールを定義するには、AppTunnel構成を使用します。

AppTunnel構成の追加については、*「Ivanti Neurons for MDM のためのAppConnectガイド」*の「AppTunnel構成の追加」を参照してください。

マネージドアプリの構成

手順

1. **[+]** アイコンをクリックし、構成ページを開きます。
2. **[+説明を追加]** をクリックし、構成の簡単な説明を入力します。
3. **[+追加]** をクリックし、キーと値を入力します。
4. 配布レベルを選択します。
5. **[次へ]** をクリックします。

Per-App VPNを使用した各アプリのVPNの構成

手順

1. **[+]** アイコンをクリックし、構成ページを開きます。
2. **[名前]** フィールドにこのアプリのVPNの名前を入力します。
3. **[+説明を追加]** をクリックし、構成の簡単な説明を入力します。
4. **[Per-App VPNをこのアプリで有効化]** をクリックし、[Per-App VPN構成] を選択します。
5. (任意) macOSアプリの場合、**[指定要件]** ストリングを識別子 "\%s\" の形式で入力します。たとえば識別子 "com.google.Chrome" です。このフィールドを使用し、複数パッケージのmacOSアプリがTunnelのようなPer-App VPNを使用できるようにします。
6. **[このアプリ構成の配布]** 方法を選択します。
7. **[次へ]** をクリックします。

Appleマネージドアプリ構成の使用

Appleマネージドアプリの構成では、インストールしたマネージドアプリを詳細に設定できます。アプリには、構成パラメーターが実装されている場合も、開発者によって実装が制限されている場合もあります。そのような制限のあるアプリでは、構成オプションが限られる場合があります。Apple管理対象アプリケーションを構成できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. アプリを選択します。
3. **[アプリ構成]** タブをクリックします。

4. **[Appleマネージドアプリ構成]** または **[+]** ボタンをクリックします。
   Appleマネージドアプリ構成では、いくつかデフォルト構成が設定されています。

5. 必要に応じて **[追加]** をクリックし、別の構成を追加します。構成の名前をクリックして構成を編集することも可能です。

6. **[構成ソース]** でいずれかの **[ソースタイプ]** オプションを選択します。

   - **AppConfig Community** - このオプションはコミュニティリポジトリにアプリ構成仕様があるアプリでのみ利用可能です。このオプションがある場合はデフォルトで選択されています。

   - **.xml仕様の使用** - アプリのスキーマをアップロードし、アプリ構成の特定のバージョンをプッシュする場合は、このオプションを選択します。**[ファイルを選択]** をクリックして.xmlファイルをアップロードします。.xmlファイルには必ずバンドルIDとバージョンを含めます。ファイル内のバンドルIDがアプリのバンドルIDと一致しない場合、エラーメッセージが表示されます。

   - **なし** - アプリにどのスキーマも適用したくない場合に選択します。**[AppConfig Community]** オプションがない場合は、これがデフォルトで選択されています。
     アップロードした.xmlファイルは **[構成ソース]** セクションに表示されます。アップロードした.xmlファイルを削除する場合は削除アイコンをクリックします。

7. **[Appleマネージドアプリ設定]** では、構成オプションを設定し、キーと値のペアを入力できます。

- **[追加]** をクリックして、キーと値のペアをマネージドアプリ構成に追加し、iRegまたはApple Device Enrollment中にGoクライアントごとに登録名情報を取得します。
  キー/値のペアのデータ型を選択してください(文字列、整数、ブーリアン、ロング浮動小数点、ダブル、日付、文字列配列、整数配列、ダブル配列、浮動小数点配列、ロング配列)。

  以下のキーと値のペアをマネージドアプリ構成に追加し、iRegまたはApple Device Enrollment中にGoクライアントごとに登録名情報を取得します。

キー	値	種類
registration.username	${userEmailAddress}	文字列
registration.token	${zeroTouchClientRegistrationNonce}	STRING
registration.token.expirationSeconds	${zeroTouchClientRegistrationNonceExpiresAtSeconds}	文字列
registration.url	${clientRegistrationUrl}	文字列

- エンドユーザーがIvanti Goアプリケーションを終了させる場合は、**[編集]** をクリックして、アプリケーションが次のいずれかを行うように設定します。

キー	値	種類
デフォルト通知を表示するには、次の値を使用します。		
enableAppTerminationNotification	True/Falseまたは1/0	ブールまたは文字列
カスタム通知を表示するには、次の値を使用します。		
appTerminationNotificationMessage	Custom notification	文字列
enableAppTerminationNotification	True/Falseまたは1/0	ブールまたは文字列

- **.plistの使用** - .plistファイルは一括アップロードするための複数のキーと値のペアを含みます。**[ファイルを選択]** をクリックして.plistファイルをアップロードします。検証済みのplistデータが **[Appleマネージドアプリ設定]** 表に表示されます。

  > ネストした辞書を持つplistは無効です。

8. **[更新]** をクリックして入力を保存します。

アプリケーション構成設定の複製

管理されたアプリケーションの構成設定を複製し、同じ設定を他のデバイスに適用できます。複製された設定の名前を変更し、内容を変更することもできます。

[Android]

Android デバイスで構成設定を複製できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. 構成設定を複製するアプリケーションを選択します。
3. **[アプリ構成]** をクリックします。
4. **[アプリケーション構成概要]** セクションには、Android デバイスで使用可能な構成 (**Android 用マネージド構成**、**デバイスにインストール**、**プロモーション**、**委任されたデバイス アクセス権**、**Google Play リリース**) の一覧が表示されます。
5. 任意の使用可能な構成をクリックします。
6. **[アクション]** の下で **[複製]** をクリックして、複製プロセスを開始します。
7. 既定では、複製された構成名は <複製された構成名のコピー> です。ただし、**[名前]** ボックスに任意の名前を入力すると、名前を変更できます。
8. (任意) **[説明]** ボックスに複製された設定に関する情報を入力します。
9. **[続行]** をクリックします。

確認ウィンドウが表示され、アプリケーション構成設定の複製が完了したことを示します。アプリケーション構成概要と複製されたアプリケーションには、複製されたバージョンが表示されます。

iOS

iOS デバイスで管理対象アプリケーションの構成設定を複製できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. 構成設定を複製するアプリケーションを選択します。
3. **[アプリ構成]** をクリックします。

4. **[アプリケーション構成概要]** セクションには、iOS デバイスで使用可能な構成 (**デバイスにインストール**、**Apple アプリケーション設定**、**プロモーション**、**AppConnect カスタム構成**、**アプリケーショントンネル**、**Apple 管理対象アプリケーション構成**、**アプリケーション VPN 単位**) の一覧が表示されます。
5. 複製する任意の構成をクリックします。
6. **[アクション]** の下で **[複製]** をクリックして、複製プロセスを開始します。
7. 既定では、複製された構成名は <複製された構成名のコピー> です。ただし、**[名前]** ボックスに任意の名前を入力すると、名前を変更できます。
8. (任意) **[説明]** ボックスに複製された設定に関する情報を入力します。
9. **[ソースタイプ]** リストから構成ソースを選択します。
10. **[Apple 管理対象アプリケーション設定]** セクションで**キー**、**値**を入力し、リストから **[タイプ]** を選択します。**キー**、**値**、**タイプ**については、**Apple 管理対象アプリケーション構成の使用**をご参照ください。
11. **[続行]** をクリックします。
    確認ウィンドウが表示され、アプリケーション構成設定の複製が完了したことを示します。**[Apple 管理対象アプリケーション構成]** セクションには、複製されたバージョンが表示されます。

Windows

Windows デバイスでアプリケーション構成設定を複製できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. 構成設定を複製するアプリケーションを選択します。
3. **[アプリ構成]** をクリックします。
4. **[アプリケーション構成概要]** セクションには、**[デバイスにインストール]** および **[プロモーション]** 構成が表示されます。
5. 複製する任意の構成をクリックします。
6. **[アクション]** の下で **[複製]** をクリックして、複製プロセスを開始します。
7. 既定では、複製された構成名は <複製された構成名のコピー> です。ただし、**[名前]** ボックスに任意の名前を入力すると、名前を変更できます。

8. (任意) **[説明]** ボックスに複製された設定に関する情報を入力します。

9. **[続行]** をクリックします。

確認ウィンドウが表示され、アプリケーション構成設定の複製が完了したことを示します。アプリケーション構成概要と複製されたアプリケーションには、複製されたバージョンが表示されます。

社内カタログに含めるWindows 10アプリの選択

社内アプリカタログに追加するアプリを選択してください。社内アプリケーション、Microsoft Store アプリケーション、Microsoft for Business アプリケーションは Windows 10でサポートされています。Windows 10は、許可または禁止を選択したアプリに基づき、デバイスで直接コンプライアンスを実行します。

Windows 10のチェックイン間隔はデフォルトで60分に1回です。デバイスおよびアプリ状態の最新情報を取得するため、デバイス強制チェックインを実行することも可能です。

サポートされるアクション:

- 新しいアプリのアップロード
- サイレントインストール
- Apps@Workからの手動インストール
- アプリの新バージョンの追加
- アプリの削除

サポートされる形式:

- APPX
- APPXBUNDLE
- MSIラップされたWin32 - バンドル済みWin32アプリ
- MSIX(RS5以降のWindows 10デバイスで対応)
- .EXE (bridge を使用)

Ivanti Neurons エージェント アプリは、**Windows** デバイスの**アプリカタログ**で提供されています。管理者は **Ivanti Neurons エージェント** アプリを社内アプリとして配布できます。それに応じて、このアプリを Windows デバイスで配布できます。

Windows 10アプリケーションの構成

手順

1. メインナビゲーションバーで **[デバイス]** をクリックします。
2. Ivanti Neurons for MDM に登録したWindows 10デバイスを選択します。
3. **[アプリ]** > **[アプリカタログ]** をクリックします。
4. アプリを選択します。
5. **[アクション]** プルダウンメニューを使用して、アプリを追加するか、カタログからアプリを削除します。
   任意でアプリの新バージョンを追加してください。
   - **[アクション]** プルダウンメニューをクリックします。
   - **[新しいバージョンを追加]** を選択します。
   - カタログを開き、アプリの新バージョンを選択します。
   - **[更新および保存]** をクリックすると[アプリ情報]画面が表示されます。
6. **[バージョン]** プルダウンメニューで使用するバージョンを選択します。
7. **[編集]** をクリックすると、詳細の変更を開始できます。
   - 必要に応じて **[カテゴリ]** を編集します。
   - 必要に応じて **[説明]** を入力します。
   - 必要に応じてスクリーンショットを追加します。
8. **[保存]** をクリックします。
9. **[配布]** タブをクリックし、**[編集]** をクリックすると、配布レベルの変更を開始できます。
10. **[保存]** をクリックします。
11. **[アプリ構成]** タブをクリックすると現在の構成の要約が表示されます。
12. 必要に応じて、アプリの説明を入力します。
13. アプリ構成要約ページで **[デバイスにインストール]** をクリックします。
    サイレントインストールがデフォルトで、これは変更できません。

14. 左側のナビゲーションペインにある **[プロモーション]** をクリックし、**[プロモーション配布構成の設定]** をクリックし、プロモーションレベルを変更します。

    - **[編集]** をクリックしてプロモーションレベル設定を変更します。
    - 構成の名前を入力します。
    - 構成の説明を入力します。
    - プロモーションレベルを選択します。
    - **[更新]** をクリックして変更を保存します。

15. **[レビュー]** タブをクリックするとレビューに関する情報が表示されます。
    必要に応じてレビューデータをスプレッドシートにエクスポートします。

Windows 10アプリ構成設定の編集

手順

1. **[ポリシー]** > **[構成]** をクリックします。
2. **[+追加]** をクリックします。
3. **[Windowsアプリ制御]** を選択し、**[Windowsアプリ制御構成の作成]** 画面を開きます。
4. 構成の **[名前]** と **[説明]** を入力します。
5. アプリタイプを以下のように定義します。

    - 許可(許可リストに含まれる) - これらのアプリのみ許可されます。デバイス上になければ、サイレントにインストールされます。
    - 禁止(ブロックリストに含まれる) - これらのアプリは、デバイス上に存在する場合でも起動するとブロックされます。

6. アプリタイプとアプリ識別子のルール定義を指定します。
7. **[アプリ検索]** をクリックし、**[Windows 10アプリを検索]** 画面を開きます。
8. Windowsストアで検索するアプリ名を入力します。
9. 表示されたアプリの中から選択し、アプリ識別子に追加します。

10. [アプリの種類] プルダウンメニューからアプリ識別子に定義されたパスを設定することにより、特定のパスを使ってアプリを許可または禁止したり、そのパスにインストールされているすべてのアプリをブロックしたりすることも可能です。
    アプリの種類 **[Publisher/PFN Equals]** は、PFNをサポートするWindows 10 MobileとWindows 10 デスクトップ向けです。**[EXE/Win32 Equals]** は、Windowsデスクトップにのみ使用します。

11. **[次へ]** をクリックします。

12. 配布レベルを選択します。

    - **すべてのデバイス**。
    - **[デバイスがありません]**
    - **カスタム** - アプリを受け取るユーザーまたはグループを入力します。

13. **[完了]** をクリックします。

14. ルール定義を編集することにより、アプリの種類の選択とアプリ識別子の指定が可能です。

    - **[アクション]** プルダウンメニューをクリックします。
    - **[新しいバージョンを追加]** を選択します。
    - アプリの新バージョンを選択します。
    - **[更新および保存]** をクリックすると **[アプリ情報]** 画面が表示されます。

Windows用の [インストール後にデバイスを再起動する] オプションの構成

[インストール後にデバイスを再起動する] オプションを使用して、アプリのインストール後にデバイスが再起動されるように構成できます。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. リストからWindows固有の任意のアプリを選択します。
3. **[アプリ構成]** > **[デバイスにインストール]** > **[アプリケーションのインストール構成の設定]** を開きます。
4. **[編集]** をクリックし、**[インストール後にデバイスを再起動する]** オプションをオンに設定します。
5. デバイスの再起動のスケジュールを選択します。

6. **[更新]** をクリックします。

   スケジュール済みの時刻にデバイスが再起動されます。

市販アプリや、ビジネス向けMicrosoft Store(MSB) アプリの場合は、**[アプリ構成]** セクションで **[Windows デバイスにサイレント インストール]** をオンに設定する必要があります。

Apps@Workを使用したアプリのインストール

Apps@Workを使用してアプリをインストールするには:

1. **[Apps@Work]** アプリをクリックします。
   Apps@Workログインダイアログには、管理者のメールアドレスとサーバーURLがあらかじめ入力されています。
2. 自分のパスワードを入力し、[サインイン] をクリックすると、アプリのページが表示されます。
3. インストールするアプリを選択します。必須アプリがクライアントにまだインストールされていない場合、必須アプリに依存するアプリをインストールすることはできません。
   iOSデバイス対応Apps@Workの場合、任意で **[すべてをインストール]** ボタンをクリックし、すべてのアプリをインストールすることができます。このオプションは、**[新規リリース]**、**[注目アプリ]**、**[カテゴリ]** 画面に表示されます。

   Apps and Booksアプリのライセンスへの同意を過去に拒否している場合、Apps and Booksアプリはインストールされません。
4. **[更新および保存]** をクリックすると **[アプリ情報]** 画面が表示されます。

関連トピック:

- 「アプリのカタログ」ページ286

アプリへのカスタム属性の割り当て

カスタム属性を作成した後は、1つ以上のアプリケーションに割り当てることができます。各属性には対応の値があり、アプリケーション グループの作成などのタスクに利用できます。属性の管理の詳細については、「属性」ページ1044をご参照ください。

個別のアプリケーションのカスタム属性を作成して割り当てる

カスタム属性を1つのアプリケーションに割り当てることができます。

手順

1. 管理ポータルにログインします。
2. **[アプリ]** > **[アプリカタログ]** に移動します。
3. アプリケーションを選択し、**[属性]** をクリックします。
4. **[+新規追加]** をクリックして、**[属性名]** ドロップダウンメニューから値を選択します。
5. **[値]** フィールドで属性値を指定します。
6. **[保存]** をクリックします。カスタム属性がアプリケーションに追加されます。

カスタム属性を複数のアプリケーションに割り当てる

カスタム属性を1つ以上のアプリケーションに割り当てることができます。複数のアプリケーションを選択すると、カスタム属性がすべてのバージョンのアプリケーションに適用されます。特定のアプリケーションを選択し、[属性] タブに移動して、特定のアプリケーションのカスタム属性詳細を変更できます。

手順

1. 管理ポータルにログインします。
2. **[アプリ]** > **[アプリカタログ]** に移動します。
3. 1つ以上のアプリケーションのチェックボックスをオンにします。
4. **[アクション]** をクリックします。
5. **[カスタム属性を割り当てる]** を選択します。[アプリへのカスタム属性の割り当て] ウィザードが表示されます。
6. 以下のオプションから*1*つ選択してください。
   - 既存の値があってもすべての属性の割り当て(上書き)を強制します。
   - 値が空の場合のみ上書きし、属性に既存の値があればスキップします。
7. 1つ以上の属性のチェックボックスをオンにします。

8. [値] フィールドで値を指定します (空の値は許可されません)。
9. **[割り当てる]** をクリックします。カスタム属性が選択したアプリケーションのすべてのバージョンに割り当てられます。
10. (任意) 1 つのアプリケーションバージョンのカスタム属性を変更する場合は、[バージョン] ドロップダウンからアプリケーションバージョンを選択し、[編集] をクリックします。

この値の**カスタム アプリ属性**を使用すると、**[デバイス詳細]** ページからレポートを作成し、CSV 形式にエクスポートできます。

Android用マネージド構成

このセクションは以下のトピックを含みます。

- 「Android Enterpriseマネージド構成の使用」下
- 「自社開発アプリのアプリ制約と権限」ページ359
- 「Android EnterpriseでのGmail設定」ページ360

Ivanti Neurons for MDMがAndroid Enterprise対応の場合は、アプリごとにAndroid Enterprise構成を利用できます。

Android Enterpriseマネージド構成の使用

1. **[アプリ]** をクリックします。
2. **[アプリカタログ]** をクリックします。
3. Anroid Enterprise構成を使用するアプリを選択します。
4. **[アプリ構成]** をクリックします。
5. **[Android用マネージド構成]** をクリックします。
6. 構成の名前を入力します。
7. 任意で説明を入力します。
8. マネージド構成フィールドを使用してマネージド構成の動作を構成します。

設定	説明
アプリが複数のプロファイルでウィジェットを共有するのをブロック	有効化すると、アプリがサイレントインストールされていない場合に限り、アプリが複数のプロファイルでウィジェットを共有するのをブロックします。無効のままにすると、Android Enterpriseプロファイルに展開された信頼できるアプリがホーム画面にウィジェットを表示するため、ユーザーがログインせずに情報にアクセスできます。
ユーザーによるアプリのアンインストールをブロック	有効化すると、Ivanti Neurons for MDM がアプリをサイレントインストールした後、ユーザーがアプリをアンインストールするのをブロックします。
最小バージョンコード	アプリがデフォルトの更新動作を上書きするために必要な最小バージョンコードを設定します。デバイスに現在インストールされているアプリのバージョンコードが指定の最小バージョンコードより低い場合は、アプリが即座に最新版に更新されます。
インストール時に自動起動	インストール後、自動的にアプリを起動したい場合に選択します。この機能はアプリがデバイス上に新しくインストールされた場合 (バージョン更新ではなく) のみ使用可能です。仕事用プロファイルおよび会社所有デバイス上の仕事用プロファイルの場合、Goアプリが前面でアクティブである必要があります。 仕事用プロファイルおよび会社所有デバイス上の仕事用プロファイルの場合、ユーザーが複数のアプリをプッシュすると、Android 10以降の制約により、1つのアプリのみ自動的に起動します。

マネージド構成

管理者は、デバイスに送信できるアプリ構成フィールドと、送信しないアプリ構成フィールドを制御できます。一般的に、構成を別のデバイスにプッシュするときに、既定値が設定されます。[マネージド構成]セクションの **[デバイスにプッシュ]** 設定で、**[すべての設定をプッシュ]** または **[値が定義されている設定のみをプッシュ]** を選択します。

各Android Enterpriseアプリ構成には、テキストフィールドごとに証明書を有効化するボタンがあり、クリックすると、テキストフィールドが証明書のドロップダウンリストに変わります。設定すれば、それらの証明書がユーザーの操作なしにサイレントに適用されます。
証明書を有効化した既存のフィールドは、フィールドの隣のボタンをクリックすればテキストフィールドに変更可能です。証明書を有効化したフィールドに変更したテキストフィールドも、同じボタンをクリックすることで再びテキストフィールドに戻すことができます。(デフォルトのドロップダウンフィールドはテキストフィールドに変更できません)。

> テナントに設定されたID証明書がない場合、証明書有効化ボタンでテキストフィールドをドロップダウンリストに変更しても、ドロップダウンリストには「なし」の選択肢しか表示されません。

9. **[許可を管理]** をクリックし、API 23以降とAndroid 6.0以降をターゲットとするアプリ用のランタイム許可を選択および構成します。
   特定のアプリケーションに適用される危険な許可だけが、選択リストに表示されます。危険な許可すべて(連絡先の読み出し、デバイス上のアカウント検索、通話ログの書き込みなど)のリストは、https://developer.android.com/guide/topics/permissions/requesting.html#perm-groupsにあります。
   - 許可は、アプリケーションが許可を要求したときにのみ適用されます。
   - ユーザーが過去に許可を承認または拒否したときは許可が適用されません。

   各許可に割り当て可能な権利には以下が含まれます。
   - 自動付与
   - 自動拒否。この設定は注意して使用してください。
   - デフォルト/グローバル
10. 配布オプションを **[アプリを利用する全員]**、**[なし]**、**[カスタム]** から選択します。
11. **[保存]** をクリックします。

自社開発アプリのアプリ制約と権限

管理者は、自社開発アプリについて、アプリ制約の設定や、権限の制限または付与を行えます。この機能を利用できるのは、公開アプリに対してのみでした。自社開発アプリにも利用できるように、この機能が拡張されました。

管理者は、自社開発アプリで **[アプリ制約]** 機能と **[権限]** 機能が利用可能になるようにするため、自社開発アプリを再アップロードする必要があります。既存のアプリを削除してから、新規バージョンをアップロードすることを推奨します。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. リストから **[自社開発]** アプリを選択します。
3. **[アプリ構成]** をクリックします。
4. **[Android用マネージド構成]** をクリックします。
5. **[追加]** をクリックします。

   [アプリ制約] セクションが画面に表示されます。
6. 利用可能な制約に対して必要な値を入力します。
7. **[許可を管理]** を選択します。

   [許可を選択] ウィンドウが画面に表示されます。
8. リストから必要な権限を選択し、**[選択]** をクリックします。
9. **[ランタイム許可]** セクションで、選択した権限の値を設定します。
10. **[このアプリ構成の配布]** セクションで、次のいずれかの **[アプリ配布]** オプションを選択します。
    - **アプリを利用する全員**
    - **該当なし**
    - **カスタム**
11. **[保存]** をクリックします。

    選択した制約と権限が自社開発アプリに適用されます。

Android EnterpriseでのGmail設定

Ivanti Neurons for MDM をAndroid Enterprise用に設定している場合、Android EnterpriseデバイスでGmailを使用できます。Android EnterpriseでGmailを設定するには

1. **[アプリ] > [アプリカタログ]** へ進みます。
2. Anroid Enterprise構成を使用するGmailアプリを選択します。[構成設定] セクションが表示されます。
3. 構成の名前を入力します。
4. 任意で説明を入力します。
5. **[マネージド構成]** フィールドを使用してマネージド構成の動作を構成します。

> **[すべて展開]** および **[すべて折りたたむ]** オプションは、ネストされた制限または階層制限でのみ

使用できます。

設定	説明
デバイスへのプッシュ	すべての設定をプッシュ - 値が設定されていないトグルを含め、すべてのトグルを有効にします。 値が定義されている設定のみをプッシュ - 値が定義されているすべてのトグルを有効にし、値が設定されていないトグルを無効にします。 通常は、既定の設定が既に利用可能です。ただし、管理者は、必須のアプリ構成設定を選択するか、デバイスに送信する必要がある変数を編集できます。
メールアドレス	置換変数を入力してメールアドレスを指定します。一般には「$emailaddress$」と入力します。UEMはこのフィールドを使用してユーザーの認証情報をActive Directoryから引き出します。
ホスト名またはホスト	「hostname.company.com:443/path」など、Active Syncサーバーのホスト名を入力します。
ユーザー名	ユーザーのActive Directoryユーザー名には変数を使用します。これは直接ユーザー名 (janedoe) またはテンプレート型の値 ($username$) として指定できます。
認証タイプ	許可された認証タイプを含む文字列を選択します。
SSLを要求	選択した場合、ホスト名とともに使用されるポート番号でSSLを有効化および要求します。
すべての証明書を信頼	信頼できない証明書を自動的に承諾する場合のみ選択します。テスト環境でデバッグまたは開発を行う場合のみ、このオプションを使用してください。
ログイン証明書エイリアス	ActiveSyncサーバーへの認証に使用するログイン証明書のエイリアスを入力します。
非マネージドアカウントを許可	これを選択すると、このマネージド構成に指定されたアカウント以外に、ユーザーが任意のExchangeアカウントを追加または削除できます。
デフォルトメール署名	送信するすべてのメールのテキストの最後に追加するデフォルトのメール署名の文字列を入力します。
デフォルト同期ウィンドウ	EAS(Exchange Active Sync) と同期する時間枠を示す0～5の値を入力します。

6. **[次へ]** をクリックします。

7. 配布オプションを **[アプリを利用する全員]**、**[なし]**、**[カスタム]** から選択します。
8. **[保存]** をクリックします。

Google Playアプリの管理

特定のグループまたは個人にGoogle Playアプリから展開するバイナリを定義できます。この展開は、Android enterprise展開に適用されます。アプリ開発者がアルファまたはベータチャネルアプリを展開するには、組織も許可リストに入れる必要があります。

1. **[アプリ]** をクリックします。
2. **[アプリカタログ]** で、Google Playリリース構成を設定するアプリを選択します。
3. **[アプリ構成]** タブをクリックします。
4. **[Google Playリリース]** をクリックします。

   Googleリリース構成はAndroid Enterpriseアプリにのみ適用されます。新しく追加されたアプリにGoogleリリース構成が選択されていない場合には、デフォルトで [製品] オプションが適用されます。

5. **[追加]** をクリックします。
6. 構成の名前を入力します。
7. 任意で説明を入力します。
8. ドロップダウンリストから、このアプリを受信したユーザーとデバイスが利用できるバイナリを選択します。選択肢は次のとおりです。
   - **製品**
   - **アルファ**
   - **ベータ**

     製品オプションは、デバイスにすでにプッシュされているアプリにデフォルトで適用されます。

9. 配布オプションを **[アプリを利用する全員]**、**[なし]**、**[カスタム]** から選択します。

   カスタムの場合、アプリはデバイスフィルターとともにユーザーグループ内に配布されます。

10. **[保存]** をクリックします。

複数のリリース構成の優先度決定

複数のGoogleリリース構成を追加する場合、Googleリリース構成を適用する優先度を付けることができます。

1. **[アプリ構成]** で **[構成の優先度決定]** をクリックします。

   このボタンは複数の構成がリストにある場合のみ表示されます。

2. 構成のリストから、適用する優先度の高い順にリストに並ぶようドラッグ&ドロップします。
3. **[更新]** をクリックします。

   最も優先度の高い構成を削除すると、その下にあった構成が最も高い優先度になります。

アプリカタログからのアプリ削除

アプリカタログから公共/社内アプリを削除することができます。必須アプリを削除することはできません。必須アプリを削除する前に、アプリを編集して必須関係を削除する必要があります。アプリがデバイスにインストールされている場合は、次にデバイスにチェックインしたときに削除されます。サイレント アプリケーション インストール/アンインストールは、デバイス管理モードでは Samsung および Zebra デバイスでサポートされ、デバイス所有者モードではすべてのデバイスでサポートされます。

自社開発アプリの場合は、確認ウィンドウが画面に表示されます。削除処理を続行することの確認を選択し、**[アプリの削除]** をクリックする必要があります。複数のアプリを削除するときに一部のアプリを削除できない場合は、削除できないアプリの情報とその理由が画面のウィンドウに表示されます。

アプリカタログで 1 つ以上のアプリを削除するときには、次の条件が適用されます。

- 1 つのバージョンの自社開発を削除できない場合は、どのバージョンも削除できません。
- 1 つのバージョンの自社開発アプリが必須アプリの場合、そのアプリは削除できず、どのバージョンも削除できません。
- 自社開発アプリのすべてまたは一部をアプリカタログから削除することを選択すると、選択した自社開発アプリのすべてのバージョンが削除されます。
- スペースから委譲された自社開発アプリは削除できません。

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. アプリのリンクをクリックします。
3. **[アクション]** > **[カタログから削除]** を選択します。
4. アプリを削除した場合の影響について警告を読みます。

   この警告は、「Appとブック」ライセンス(iOS) とアプリのレビュー(すべてのOS) も削除されることを説明しています。
5. [アプリを削除する結果を理解しています] チェックボックスをオンにして、削除処理を続行します。
6. **[アプリを削除する]** をクリックします。

社内アプリのアップグレード

自社開発アプリをアップグレードする手順は次のとおりです。

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. アップグレードするアプリを選択します。
3. **[アクション]** > **[新しいバージョンの追加]** を選択します。
4. **[アプリをアップロード]** エリアにアプリをドラッグアンドドロップするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。
5. アプリの旧バージョンをどうするか、以下のいずれかのオプションを選択します。
   - **説明、スクリーンショット、配布、アプリの必須要件およびアプリ構成を変更しない:** アプリカタログの旧バージョンを新バージョンに交換します。
   - **説明、スクリーンショット、配布、アプリの必須要件またはアプリ構成を変更する:** アプリカタログに新旧両方のバージョンを保持します。
6. **[最新情報]** に、新バージョンの変更点を説明するテキストを入力します。

   このテキストは、ユーザーがアプリのインストールを選択する際にデバイスに表示されます。
7. 説明、スクリーンショット、配布のオプションを変更する場合は、それらの変更を完了します。
8. **[完了]** をクリックします。

   アプリの旧バージョンをカタログに保持する場合、**[アプリ]** > **[アプリカタログ]** にはエントリ1つのみ表示されます。左端のペインは、エントリによって説明されるアプリ数を表示します。その後、新しいバージョンを削除すると、インストールされたデバイス上で自動的に旧いバージョンが取って代わります。

アプリのバージョンリストの表示

管理者は、同じバージョンで異なるアーキテクチャのアプリをアップロードできます。

Procedure手順

1. **[アプリ]** > **[アプリカタログ]** にあるアプリのリンクをクリックします。
2. **[バージョン]** タブをクリックします。
   カタログ内に同じアプリの複数のバージョンがある場合、それらはドロップダウンとして表示されます。同じバージョン番号で異なるアーキテクチャの複数のアプリがアップロードされた場合、ドロップダウンリストがサポートされるアーキテクチャの詳細を表示します。サポートされるアプリのアーキテクチャは、**[アプリ情報]** にも表示されます。

Androidアプリのパッケージ名の検索

Google Playストアから入手可能な**パブリックアプリの場合：**

1. WebブラウザでGoogle Playストアアプリを探します。
2. アプリを選択します。
3. ブラウザに表示されたURLを調べます。

   パッケージ名は、以下のようにid=の後に記載されています。

   https://play.google.com/store/apps/details?id=<package name>

Playストアで提供していない自社開発アプリやその他のアプリの場合は、Package Name Viewerや類似のアプリをGoogle Playストアからダウンロードしてみてください。

カテゴリ

このセクションは以下のトピックを含みます。

- 「カテゴリの追加」下
- 「カテゴリの削除」下

カテゴリは、アプリのタイプを説明するものであり、ユーザがアプリカタログを参照する際にアプリを系統立てるのに役立ちます。どのアプリにも1つ以上のカテゴリを割り当てる必要があります。一般的なアプリカテゴリのリストは、Ivanti Neurons for MDM の使用開始時に表示されます。このページを使用してアプリカテゴリを管理します。

カテゴリの追加

ここで、あるいはアプリをアプリカタログに追加するときに新規カテゴリを追加できます。

1. **[追加]**(左下)をクリックします。
2. カテゴリ名を入力します。

   カテゴリでは大文字と小文字が区別されません。MINEはMineと同じとみなされます。
3. **[保存]** をクリックします。

カテゴリの削除

- カテゴリの隣のXをクリックします。

[アプリカテゴリ] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です:

- アプリ& コンテンツ管理

配布フィルター

このセクションは以下のトピックを含みます。

- 「配布フィルターの構成」下
- 「管理者代理用の配布フィルター構成」ページ374

インストールできるアプリを制限するには、配布フィルターを使用します。配布フィルターを使用すると、デバイスに適用されるアプリのみをアプリカタログに表示することができます。

ライセンス: Silver

次のフィルターは、デフォルトで使用可能になっています。

- **Android Enterprise有効アプリ** - アプリ配布をAndroid Enterprise有効デバイスのみに限定するフィルター。
- **iPad専用アプリ** - アプリ配布をiPadデバイスのみに限定するフィルター。
- **iPhone専用アプリ** - アプリ配布をiPhoneデバイスのみに限定するフィルター。

配布フィルターの構成

1. **[アプリ] > [配布フィルター]** へ進みます。
   ここには、デフォルトのアプリフィルターと作成されたアプリフィルターがリスト表示されています。
2. **[+追加]** をクリックし、**[配布フィルターを作成]** ダイアログにアクセスします。
3. 該当するフィールドに名前と説明を入力します。

4. ルール定義を選択します。これらのルールは、「は次を含む:」、「は次より小さい:」、「は次より大きい:」、「が次の範囲内:」、「は次と等しい:」、「は次と等しくない:」などの演算子を使用して作成します。[ANY (OR)] または [ALL (AND)] オプションを使用すればネストでまとめることができます。アプリ配布フィルターは次のとおりです。
   - Accessによるブロック
   - APNS対応
   - 仕事用プロファイルを持つAndroidマネージドデバイス
   - Android Work有効
   - Android仕事用マネージドデバイス(デバイス所有者)有効
   - 会社所有デバイス上のAndroid仕事用プロファイル有効
   - クライアントの前回のチェックイン
   - クライアント登録
   - コンプライアンス
   - コンプライアンスアクションによるブロック
   - 現在の国名
   - 現在のMCC
   - 現在のMNC
   - カスタムデバイス属性
   - カスタムLDAP属性
   - カスタムユーザー属性
   - カスタムIDP属性
   - デバイスの種類
   - 本国
   - ホームMCC
   - ホームMNC
   - キオスクモード
   - 製造者
   - OSバージョン
   - オーナーシップ
   - 電話番号
   - ローミング
   - Secure Appsステータス
   - 監視対象
   - Sentryによるブロック
   - User Enrollment登録済み
   - 自動Device Enrollment登録済み
5. **[配布フィルターを作成]**をクリックします。

6. 必要に応じて、更新するカスタムフィルターを選択します。
   a. **[編集]** をクリックすると、**[配布フィルターを更新]** ページが表示されます。
   b. 該当するフィールドに名前と説明を入力します。
   c. プルダウンメニューを使用して、フィルターのルールを定義します。
   d. **[配布フィルターを更新]** をクリックします。
7. アプリを選択します。
8. [アプリの詳細] ページで **[配布]** タブを選択します。
9. **[編集]** をクリックします。
10. [アプリ配布] オプションを選択します。
    - **全員**
    - **該当なし**
    - **カスタム**

    [配布フィルター] セクションは、**[全員]** または **[カスタム]** の配布オプションを選択した場合にのみ表示されます。
11. 配布フィルターオプションを選択します。
    a. **[既存の配布フィルタを検索...]** にフィルタ名を入力します。フィールドにフィルター名を入力します。
    b. 新規フィルターを追加する場合は、**[+配布フィルターを追加]** をクリックします。

アプリをカタログに追加する前に、配布フィルターを作成したり、アプリに割り当てることができます。配布フィルターの変更は、そのフィルターを使用するアプリの配布に影響を与えます(すべてのスペースで) 。

フィルターが設定されており、**[アプリ配布時にM1デバイスへのインストールを許可]** が有効になっている場合、結果にはmacOS M1デバイスが表示されます。**[アプリ配布時にM1デバイスへのインストールを許可]** が有効化されており、[配布フィルター] が **[全員]** または **[カスタム]** のいずれかになっている場合、iOS VPPアプリがすべてのMacデバイスで利用可能となります。macOS関連属性の配布フィルターは、iOSアプリではサポートされていません。

管理者代理用の配布フィルター構成

管理者代理は、作成して配布プロセス中に委譲スペースで各アプリに追加したフィルターを管理および編集できます。管理者代理は、デフォルトスペースで作成した配布フィルターを他のスペースで使用できませんが、委譲アプリには使用できます。

管理者代理は、アクセス権を持つ所定のスペースで配布フィルターを作成、管理、編集できます。配布フィルターは、それが作成されたスペースでのみ使用できます。アプリ配布フィルターは委譲できません。

アプリとシステムの管理役割を持つ管理者代理が配布フィルターを使用してアプリを委譲スペースに追加した場合は、自分のスペースにあるデバイスと他のスペースにあるデバイスの詳細を見ることができます。

システム管理またはシステム読み取り専用の役割を持つユーザーは、どのスペースでも配布フィルターを作成、更新、削除できません。

アプリおよびコンテンツマネージャーの役割を持つ管理者代理は、配布フィルターにアクセスできない場合があります。このため以下は実行できません。

- 配布フィルターを使用したアプリの作成。これは、管理者代理としてログインし、アプリを追加する場合に生じます。
- システム読み取り専用以上の役割を持つ管理者代理は、配布フィルターでアプリを追加できます。システム管理役割を持たない管理者代理は、配布フィルターなしでアプリを追加可能です。

管理者代理は、以下のオプションの選択により、アプリカタログで委譲ステータスをフィルターできます。

- 委譲済み
- 委譲されていません

レビュー

このセクションは以下のトピックを含みます。

レビューとは、ユーザーがアプリカタログにあるアプリについて提供するコメントや評価(星)のことです。レビューは、アプリのインストールを検討しているユーザーに対しても貴重な情報を提供してくれます。**[レビュー]** ページを使用して評価とレビューを確認したり、削除したりします。古いものや不適切なレビューや評価は削除しても構いません。

- デバイスユーザーのみが、アプリの評価とレビューを作成したり編集することができます。
- デバイスユーザーは、自分の評価やレビューを編集することができますが、削除はできません。
- アプリのレビューを削除できるのは管理者のみです。
- アプリの評価は削除できません。アプリに付けられた評価(星)は、後でユーザーの評価およびレビュー機能を無効化した場合でも、**[アプリ]** > **[アプリカタログ]** ページに残ります。

評価とレビューの確認

- **[アプリ]** > **[レビュー]** を開くと、自分が配布したアプリのユーザーレビューと評価(星)をすべて読むことができます。
- **[アプリ]** > **[アプリカタログ]** に移動すると、**[平均評価]** 列が表示され、レビューの合計件数と平均評価が示されます。
- **[アプリ]** > **[アプリカタログ]** へ進み、**[アプリ名]** をクリックし、**[レビュー]** タブで具体的なアプリの評価とレビューを確認します。

評価とレビューの無効化

1. **[アプリ]** > **[カタログ設定]** へ進みます。
2. **[エンドユーザーのアプリカタログでの評価とレビューを有効にする]** のチェックを解除します。

3. **[保存]** をクリックします。

レビューの削除

1. **[アプリ]** > **[レビュー]** へ進みます。
2. レビューを選択します。
3. ページの右上にある **アクション** ボタンをクリックします。
4. **[削除]** を選択します。
5. **[レビューの削除]** 確認ダイアログで **[はい]** をクリックします。

[レビュー] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です:

- アプリ& コンテンツ管理

Appleの「Appとブック」

このセクションは以下のトピックを含みます。

ライセンス: Silver

Appleの「Appとブック」画面は、アプリカタログ設定でAppleの「Appとブック」を設定している場合にのみ表示されます。この画面に、Appleの「Appとブック」を通じてAppleデバイス用に購入したアプリライセンスが表示されます。この画面では以下を実行できます。

- カタログに含める「Appとブック」アプリの選択
- 「Appとブック」アプリのライセンス配布

アプリケーションとApps and Books の配布の詳細については、Ivanti コミュニティ記事 Ivanti Neurons for MDM: How to Distribute Apps with VPP をご覧ください。

Apple Booksが提供されていない国や地域もあります。Appleの「Appとブック」経由でアプリのライセンスを配布するには、Apple社が提供するsTokenにアクセスする必要があります。

同じスペース内の複数のAppleの「Appとブック」アカウントへのライセンス配布

- 同じアプリが複数の「Appとブック」アカウントに存在する場合、アカウントの優先順にライセンスが配布されます。
- 同じアプリが複数の「Appとブック」アカウントに存在し、優先度の高い「Appとブック」アカウント内のアプリライセンスが足りない場合、次に優先度の高いアカウントからライセンスが配布されます。ただし、次に優先度の高いアカウントのライセンス配布リストに、ユーザーまたはデバイスがある場合に限ります。
- ライセンスは取り消されず、「Appとブック」アカウントの優先度変更時に再度割り当てられます。アプリは、最初のアカウントからライセンスを配布されます。最初のアカウントのライセンスが足りない場合、次に優先度の高いアカウントからアプリにライセンスが配布されます。
- ユーザーは、アプリカタログのページからアプリのすべてのライセンスを取り消すことが可能です。このアクションにより、使用可能なすべての「Appとブック」アカウントからそのアプリのライセンスが取り消されます。
- 予約ライセンスは、「Appとブック」アカウントの優先度より優先されます。

デバイスベースおよびユーザーベースのライセンス配布

アプリのライセンスがデバイスベースであるかユーザーベースであるかは、割り当て方法によって決まります。アプリライセンスをデバイスに割り当てた場合は、デバイスベースのライセンスとなります。アプリライセンスをユーザーに割り当てた場合は、ユーザーベースのライセンスとなります。

Apps and Books アプリケーションをデバイスにインストールするとき、またはそのアプリケーションのトークンが発行されたときに、ライセンスが配布されます。アプリに利用可能なライセンスがない場合、ユーザーは、自身でアプリをインストールし、料金を支払うこともできます。必須「Appとブック」アプリに関してユーザーがユーザーベースのライセンスをすでに割り当てられている場合、アプリは「Appとブック」ライセンスではなく既存のユーザーベースのライセンスを使用してインストールされます。

[共有iPad]の場合、「Appとブック」はデバイスベースのライセンスが選択されているかどうかに関係なく、デバイスベースのライセンスに基づいてインストールされます。

デバイスベースのライセンスオプションの使用

デバイスベースのライセンスの場合、ユーザーが「Appとブック」に登録する必要はありません。必須アプリは自動的にインストールされます。会社管理のデバイスで、IT部門が所有するApple IDを取り扱う必要はありません。

デバイスのチェックイン時に、デバイスはシリアルナンバーで識別され、利用可能なライセンスがあれば必須アプリがインストールされます。利用可能なライセンスがなければ、アプリはインストールされません。アプリのライセンスが予約されている場合、アプリのインストール時にデバイスベースのライセンス割り当ては行われません。

デバイスベースの「Appとブック」ライセンスを使用して導入されたアプリのアプリケーション更新は管理者によって制御されます。

アプリの更新方法を制御するには、**[アプリ]** > **[アプリカタログ]** で **[アプリ構成/デバイスにインストール]** タブを開きます。ここで、次のデバイスチェックイン時に即座に更新するか、新しいバージョンの公開と同時に自動的に更新するかを選択できます。

重要: デバイスベースのライセンスを企業間(B2B)または生産性向上アプリに割り当てる前に、アプリがデバイスベースのライセンス付与に対応しているかどうか、アプリ開発者に確認してください。

ユーザーベースのライセンスオプションの使用

ユーザーベースのライセンスは、デバイスの紛失または盗難、または新しいデバイスへのアップグレードにより、ユーザーがデバイスを変更しても有効です。ユーザーベースのライセンスでは、ユーザーがまずAppleの「Appとブック」に登録する必要があります。登録は手動操作であり、エンドユーザーがアプリカタログ内で実行しなければなりません。ユーザーがAppleの「Appとブック」に登録するまで必須「Appとブック」アプリはインストールされません。

アプリが必須「Appとブック」アプリであり、ライセンス配布がユーザーベースの場合:

- ユーザーが「Appとブック」プログラムに登録されていない場合、必須アプリのインストールは行われません。
- ユーザーが「Appとブック」プログラムに登録され、ライセンスが利用可能であれば、必須アプリをインストールできます。
- ユーザーが「Appとブック」プログラムに登録されていても、利用可能なライセンスがない場合は、アプリはインストールされません。

カタログへの「Appとブック」アプリの追加

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. アプリを選択し、**[アプリカタログに追加]** をクリックします。**[次へ]** をクリックします。
3. オプションで、アプリの説明を追加します。**[次へ]** をクリックします。
4. 配布オプションを選択します。**[次へ]** をクリックします。
5. **[アプリ構成]** タブをクリックします。
6. 任意で **[デバイスにインストール]** を選択します。この構成オプションでは、管理対象のiOSデバイス上でユーザーにプロンプトが表示されることなく、アプリがインストールされます。
7. 必要に応じて、別の構成を選択します。

「Appとブック」セキュアトークン情報ページには、以下のトークン情報が表示されます。

- 作成日
- 位置情報(トークンにこの情報が含まれる場合)
- 有効期限

「Appとブック」アカウントの追加

Ivanti Neurons for MDM では、1つのスペース内の複数の「Appとブック」セキュアトークンを追加することにより、複数の「Appとブック」アカウントを追加できます。

スペース内に「Appとブック」セキュアトークンを追加するには、以下の手順を実行してください。

1. **[アプリ]** > **[Appleの「Appとブック」]** を開きます。
2. **[+「Appとブック」sTokenを追加]** をクリックします。
3. 名前を入力し、トークンファイルを選択します。
4. 任意で **[全ユーザーに「Appとブック」アプリを自動配布]** オプションの選択を解除します。デフォルトではこのオプションが選択されていて、FCFSライセンスの配布に全ユーザーグループが使用されます。

5. **[過去の「Appとブック」ライセンスからすべてのデータをクリア]** オプションを選択し、このトークンに関連付けられているすべてのアプリライセンスを削除することも可能です。
6. **[保存]** をクリックします。

アカウントを追加すると、追加されたすべての「Appとブック」アカウントのリストがテーブル内に表示されます。

「Appとブック」セキュアトークンの更新

手順

1. **[アプリ]** > **[Appleの「Appとブック」]** を開きます。
2. 「Appとブック」アカウント名をクリックします。
3. [トークン] タブで **[sTokenを更新]**(.stokenファイル) をクリックします。
4. トークン名を入力し、トークンファイルを選択します。
5. 任意で **[全ユーザーに「Appとブック」アプリを自動配布]** オプションの選択を解除します。デフォルトではこのオプションが選択されていて、FCFSライセンスの配布に全ユーザーグループが使用されます。
6. **[過去の「Appとブック」ライセンスからすべてのデータをクリア]** オプションを選択し、このトークンに関連付けられているすべてのアプリライセンスを削除することも可能です。
7. **[更新]** をクリックします。

[トークン] タブで **[「Appとブック」ライセンス使用情報を再同期]** をクリックすると、Appleの「Appとブック」サービスからすべてのアプリおよびライセンス情報がフル同期されます。この操作は、Ivanti Neurons for MDMにあるライセンス割り当て情報が正しくない場合のみ必要です。そのような間違いは、Appleの「Appとブック」APIに矛盾がある場合に発生する場合があります。

「Appとブック」アカウントの優先度の更新

管理者は、スペース内の各「Appとブック」アカウントにライセンス使用に関する優先度を設定できます。「Appとブック」アカウントの優先度によってライセンス配布システムが予測可能になり、ユーザーやデバイスが複数の「Appとブック」アカウントから同じアプリのライセンスを受け取る資格を持つ場合の問題が解決されます。

手順

1. **[アプリ]** > **[Appleの「Appとブック」]** を開きます。
2. 必要な「Appとブック」アカウント名の **[優先度を編集]** をクリックします。

3. [優先度を編集] ウィンドウで新しい優先度を選択します。
4. **[保存]** をクリックします。

「Appとブック」セキュアトークンの削除

「Appとブック」セキュアトークンを一度削除すると復元すできません。トークンを削除した場合：

- 予約トークンを持つアプリでは、そのトークンが削除されます。
- 支払い済みの有料アプリは、引き続きカタログに残り、ユーザーは個人として支払いを続けることができます。
- 会社の「Appとブック」アカウント経由でエンドユーザーがインストールしたアプリについて、ユーザーが使用継続を希望する場合は、個人アカウントへの移行が必要となります。移行については、ユーザーに30日間の猶予期間が与えられます。

手順

1. **[アプリ] > [Appleの「Appとブック」]** を開きます。
2. 「Appとブック」アカウント名をクリックします。
3. [トークン] タブで **[削除]** をクリックします。
4. [「Appとブック」セキュアトークン削除] ウィンドウで、**[はい、「Appとブック」セキュアトークンを削除します]** を選択して確定します。
5. **[削除]** をクリックします。

カタログ内にある「Appとブック」アプリのライセンス配布

1. メインメニューから **[アプリ] > [Appleの「Appとブック」]** を選択します。

   「Appとブック」アカウントのリストが表示されます。各アカウントの下に、「Appとブック」プログラムを通じて購入したアプリのリストが表示されます。

2. アプリを選択し、**[ライセンスを配布]** をクリックします。
3. [「Appとブック」ライセンス] セクションで、**[申し込み順]**、**[予約]**、または **[禁止]** の配付オプションを選択します。

ユーザーごとのアプリライセンス表示

[ライセンス使用状況] タブでは、ユーザーのライセンス設定を表示できます。

1. **[ユーザー]** タブをクリックします。
2. ユーザーを選択します。
3. **[ライセンス利用]** タブをクリックします。

   「Appとブック」ライセンスの種類とライセンス割り当ての詳細とともに、アプリのリストが表示されます。

ユーザーごとの各アプリのライセンス利用状況を表示するには:

1. Ivanti Neurons for MDM のメインメニューで **[ユーザ]** に移動します。
2. ユーザーを選択します。

   デフォルトでは **[デバイス]** タブが表示されます。
3. **[ライセンス使用]** タブをクリックします。

   ユーザーのデバイスにインストールされている全アプリのリストが、ライセンスステータス付きで表示されます。デバイスのシリアル番号が、デバイスベースのライセンスの [「Appとブック」ライセンスの種類] カラムに表示されます。

   - アプリ名
   - アプリのバージョン
   - アプリのコスト
   - アプリの割り当て日
   - 「Appとブック」ライセンスの種類
   - アクション(ライセンスステータス)

各アプリの「Appとブック」ライセンス使用状況を表示することもできます。

1. Ivanti Neurons for MDM のメインメニューで **[アプリケーション]** > **[アプリケーション カタログ]** に移動します。
2. アプリを選択します。
3. **[Apps and Books ライセンス]** タブがあればクリックします。

4. アカウント名をクリックします。「Appとブック」プログラム経由で購入したアプリのみがこのタブに表示されます。

   「Appとブック」ライセンスの種類ごとに別のタブが表示されます。

ライセンスの種類とログ	説明
申し込み順(FCFS) - この種類のライセンスを受け取るユーザーグループを選択するオプションがあります。	• ユーザー要求アプリ - ユーザーがインストールすることを選んだアプリ。ユーザーベースのライセンスがデフォルトです。 • 必須アプリ - 必須であり、**[デバイスにインストール]** の設定を使用して管理構成によってインストールされるアプリ。これらのアプリは、デフォルトでデバイスベースのライセンスを使用します。
予約	予約ライセンスは、FCFSライセンスよりも優先されます。ここでは、アプリの[予約]ライセンスを割り当てるユーザーまたはデバイスを選択できます。
禁止	このアプリのライセンスを持つことを認めないユーザーを入力します。ユーザーがアプリをインストールすることはできますが、その場合は購入しなければなりません。
アクティビティログ	ユーザー、割り当てられた「Appとブック」ライセンスの種類、割り当てられた日、およびそのライセンスに対して最近行ったアクションを表示します。

デバイスごとに各アプリの詳細なライセンス利用状況を表示するには:

1. Ivanti Neurons for MDM のメインメニューで **[デバイス]** に移動します。
2. デバイスを選択します。
3. **[インストール済みアプリ]** タブをクリックします。

選択したデバイスにインストールされている全マネージドアプリのリストが、ライセンスステータス付きで表示されます。

- アプリ名
- アプリのバージョン
- 対応プラットフォーム
- アプリのソース
- アプリのサイズ
- 「Appとブック」ライセンスの種類
- iOSアプリの場合はアプリが報告(インストール)された日付

「Appとブック」ライセンスの使用状況

「Appとブック」ライセンスの使用状況は、「Appとブック」通知で把握できます。通知の基準値は以下のように定義されます。

- ライセンスの50%以上が使用されると情報通知が発行されます。
- ライセンスの70～80%が使用されると警告通知が発行されます。
- ライセンスの90～100%が使用されると危険通知が発行されます。
- 使用が50%を下回ると通知が解除されます。

各アプリのライセンス情報を表示するには:

1. **[アプリ] > [Appleの「Appとブック」]** をクリックします。

   以下を含むライセンス情報が表示されます。

   - アプリ名
   - ライセンスの費用
   - 利用可能なライセンス数
   - 使用済みのライセンス数

2. ライセンス通知の詳細を見るには、**[ダッシュボード] > [通知]** を開きます。

[通知] ページが表示されます。

3. 通知のタイトルをクリックすると詳細が表示されます。使用可能な通知はダッシュボードを参照してください。

「Appとブック」ライセンス使用状況通知

送信基準	重大度	通知の種類	コンポーネントの種類
50%使用済み	情報	ライセンス使用状況	「Appとブック」
70%使用済み	警告	ライセンス使用状況	「Appとブック」
80%使用済み	警告	ライセンス使用状況	「Appとブック」
90%使用済み	アラート	ライセンス使用状況	「Appとブック」
100%使用済み	アラート	ライセンス使用状況	「Appとブック」

「Appとブック」ライセンス使用状況の表示

あるユーザーに特有のライセンス使用状況の詳細は、ライセンスカラムのライセンス使用状況テーブル内に表示されます。

1. アプリをクリックします。
2. **[ライセンス利用]** タブをクリックします。
3. 検索フィールドにユーザー名を入力します。

アプリの「Appとブック」ライセンス取り消し

以下の場合、「Appとブック」ライセンスは取り消されます。

- デバイスがアクティブでない場合 (撤去またはワイプ) 。
- 「Appとブック」アプリが削除された場合。
- デバイスベースのライセンスは、デバイスの撤去時に無効化されます。
- 「Appとブック」トークンが削除された場合。

アプリのa「Appとブック」ライセンスを取り消すには:

1. **[アプリ]** > **[アプリカタログ]** の下のアプリを選択します。
2. **[Appleの「Appとブック」ライセンス]** タブがあればクリックします。
3. 以下のいずれかの操作を実行します。
   a. **[すべてのライセンスを取り消す]** をクリックし、すべてのユーザまたはデバイスからすべてのライセンスを取り消します。
   b. **[アクティビティログ]** タブをクリックします。**[アクション]** のカラムで、ユーザーまたはデバイスごとにライセンスを個別に取り消します。

- iOSデバイスの場合、Appleは、「Appとブック」ライセンスが取り消された後、「Appとブック」アプリに30日間の猶予期間を設けています。したがって、「Appとブック」アプリは引き続きインストール可能です。
- macOSデバイスの場合、「Appとブック」ライセンスが取り消された後も、アプリはデバイス上に残ります。

ユーザーの「Appとブック」ライセンスを取り消すには:

1. アプリをクリックします。
2. **[ライセンス利用]** タブをクリックします。
3. ライセンスへのアクセスを削除すべきユーザーの **[ライセンスの無効化]** をクリックします。

ユーザーが削除された、またはユーザーがデバイスからMDMプロファイルを削除した場合は、「Appとブック」ライセンスが自動的に取り消されます。

「Appとブック」認証エラー通知

Appleの「Appとブック」サービスの使用中に認証エラーが発生する場合があります。このような「Appとブック」認証エラー通知には、以下があります。

エラー通知	アクション
認証トークンは無効です	有効な「Appとブック」sTokenをアップロードしてください
トークンの有効期限が切れています	会社のアカウントを使用して、新しいトークンをオンラインで生成してください
sTokenが無効化されています	有効な「Appとブック」をアップロードしてください
ログインが必要です	「Appとブック」サービスにログインしてください

macOSおよびiOSデバイスにおける「Appとブック」の動作

iOS対応「Appとブック」

アクション	デバイスベースのライセンス	ユーザーベースのライセンス
ユーザーへの配布から「Appとブック」アプリを削除する	アプリがユーザーのデバイスでアンインストールされます	アプリがユーザーのデバイスでアンインストールされます
「Appとブック」アプリの委譲を解除する	非デフォルトスペースにあるすべてのデバイスからアプリがアンインストールされます	非デフォルトスペースにあるすべてのデバイスからアプリがアンインストールされます
「Appとブック」アプリをデフォルトまたはカスタムスペースから削除する	すべてのデバイスからアプリがアンインストールされます	すべてのデバイスからアプリがアンインストールされます

macOS対応「Appとブック」

アクション	デバイスベースのライセンス	ユーザーベースのライセンス
ユーザーへの配布から「Appとブック」アプリを削除する	アプリはユーザーのデバイスでアンインストールされません	不適用
「Appとブック」アプリの委譲を解除する	非デフォルトスペースにあるすべてのデバイスからアプリがアンインストールされません	不適用
「Appとブック」アプリをデフォルトまたはカスタムスペースから削除する	アプリはすべてのデバイスからアンインストールされません	不適用

デバイスがスペースを移動したときの「Appとブック」ライセンス供与

デバイスを新しいスペースに移動すると、デバイスまたはデバイス所有者に割り当てられていた「Appとブック」ライセンスは取り消されます。新しいスペースによっては新しい「Appとブック」ライセンスが割り当てられます。

「Appとブック」ライセンスの供与シナリオは以下のとおりです。

シナリオ	供与
ソーススペースでデバイスまたはデバイス所有者に「Appとブック」ライセンスが割り当てられていて、移動先スペースにも同じアプリの「Appとブック」ライセンスがある場合。	移動先スペースの「Appとブック」トークンからライセンスを割り当てます。
ソーススペースでデバイスまたはデバイス所有者に「Appとブック」ライセンスが割り当てられていて、移動先スペースに同じアプリの「Appとブック」ライセンスがない場合。	ソーススペースの「Appとブック」トークンからライセンスを取り消します。
ソーススペースではデバイスまたはデバイス所有者に「Appとブック」ライセンスが割り当てられておらず、移動先スペースにはインストールされた何らかの「Appとブック」アプリの「Appとブック」ライセンスがある場合。	移動先スペースの「Appとブック」トークンからライセンスを割り当てます。

[アプリカテゴリ] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です:

- アプリ& コンテンツ管理

カタログ設定

このセクションは以下のトピックを含みます。

- 「Appleアプリ管理設定の変更」下
- 「App Storeのデフォルト地域の設定」次のページ
- 「iOSアプリ更新の有効化/無効化」ページ393
- 「アプリの評価とレビューの有効化/無効化」ページ393
- 「iOS/macOSの「Appとブック」sToken(ライセンス: Gold)のアップロードまたは更新」ページ394
- 「Ivanti Neurons for MDM サービスからのiOS/macOSの「Appとブック」sTokenの削除」ページ394

[アプリ] > **[カタログ設定]** ページで、アプリカタログのすべてのアプリケーションに適用する設定を構成します。次の操作ができます。

- デバイスチェックイン中にアプリ更新を含める
- iCloudおよびiTunesへのバックアップを防止する(iOSのみ)
- App Storeのデフォルト地域を設定する(AppleとMicrosoft)
- デバイスの登録解除時にiOSアプリを削除する
- Ivanti Neurons for MDM の [評価とレビュー] を有効にする
- iOS および macOS の Apps and Books トークンをアップロード (Gold ライセンスが必要)

Appleアプリ管理設定の変更

アプリ個別にアプリ管理構成が作成されていない限り、これらの設定は全アプリに適用されます。

1. 以下のチェックボックスの1つまたは複数を選択またはクリアします:
   - **デバイスチェックイン中にアプリを更新** (デフォルトで選択)
   - **iCloudおよびiTunesへのバックアップを防止**

- **登録解除時にアプリを削除**

2. **[保存]** をクリックします。

通知

1. **[アプリの新規バージョンが Apple App Store および Google Play ストアで入手可能になったときにシステム通知を生成]** の下のドロップダウンリストをクリックし、次のいずれかのオプションを選択します。
   - **1週間に1回**
   - **1日に1回**
2. **[AppCatalog で利用可能な新しいアプリケーション更新のエンドユーザ通知を生成]** の下のドロップダウンリストをクリックし、次のいずれかのオプションを選択します。
   - **1週間に1回**
   - **1日に1回**

App Store のデフォルト地域の設定

アプリカタログの設定で、AppleとMicrosoftのApp Storeのデフォルト地域を設定します。

1. App Storeのデフォルト地域セクションで：
   - **[Apple App Storeの地域]** を選択します。
   - **[Microsoft App Storeの地域]** を選択します。
2. 最後に選択したApp Storeの地域を各管理者のデフォルト地域として使用するオプションを選択またはクリアします。このオプションを選択した場合、App Storeの地域は各管理者が最後に選択した地域に設定され、その前の設定を上書きします。管理者がこの機能を初めて使用する場合、デフォルトの地域は、その前に設定されていた地域になります。
3. **[保存]** をクリックします。

iOSアプリ更新の有効化/無効化

1. **[デバイスチェックイン中にアプリを更新]** をオンまたはオフにします。
   - デフォルトではこのオプションが選択されています。
   - クリアすると、あらゆるデバイスチェックイン(管理者による強制チェックインを含む)にアプリ更新が含まれません。
   - しかし、デバイスのアプリカタログから強制チェックインをクリックすれば、手動でアプリを更新できます。
   - 新規アプリのインストール、その他のすべての構成や設定はデバイスチェックイン中に更新されます。
2. **[保存]** をクリックします。

マネージドアプリの場合、管理者はアプリ詳細ページの **[更新]** ボタンをクリックし、手動でアプリストアからアプリを最新バージョンに更新できます。

ユーザーのデバイスの場合、ユーザーがアプリカタログメニューの **[強制チェックイン]** ボタンをクリックしてデバイスをチェックインすると、アプリ更新、その他の構成や更新が行われます。

このような設定により、エンドユーザーはアプリの更新時期を選択できます。

- データ料金がかかるのを防ぐには、Wi-Fiに接続するのを待ちます。
- アプリ更新によって都合の悪いときにロックアウトされるのを防ぎます。

アプリの評価とレビューの有効化/無効化

これにより、ユーザーはアプリを評価してレビューを書き、他のユーザーに読んでもらうことができます。

1. **[エンドユーザーのアプリカタログで評価とレビューを有効化]** を選択するか選択解除します。
2. **[保存]** をクリックします。

「Appとブック」sTokenの形式が変わりました。先行リリースでは文字列でしたが、現在はvpptokenファイル形式のテキストファイルに保存された文字列になりました。このファイルを管理者コンソールに直接アップロードし、処理してください。「Appとブック」アカウントページが行進され、「Appとブック」の組織名と有効期限が表示されるようになりました。

iOS/macOSの「Appとブック」sToken(ライセンス: Gold) のアップロードまたは更新

1. **[「Appとブック」 sTokenを追加]** を選択します。
2. **[エイリアス名]** フィールドにsTokenファイルの名前を入力します。
3. sTokenファイルを指定のエリアにドラッグ＆ドロップするか、**[ファイルを選択]** をクリックしてsTokenファイルを指定します。
4. **[保存]** をクリックするか、sTokenファイルを更新する場合は **[更新]** をクリックします。
5. [Apple「Appとブック」] ページを開き、このトークンに関連付けられているアプリを表示します。

Ivanti Neurons for MDMの前のリリースで、個々のユーザーに「Apps and Books」トークンが予約されている場合は、それらのユーザのトークンがまだ予約されているかどうか確認し、必要ならば再度予約する必要があります。

Ivanti Neurons for MDM サービスからのiOS/macOSの「Appとブック」sTokenの削除

ユーザーが必要としなくなったアプリは、無効化し、必要に応じて再び割り当てることができます。アプリがiOS/macOS向けMDMによってマネージドアプリとして展開されていた場合は、アプリと全データを即座に削除できます。

1. 削除するアプリを選択します。
2. **[削除]** をクリックします。
   警告ダイアログが表示されます。
3. ユーザーに30日間の猶予を与え、以下を行わせることも可能です。
   - 自分のデータの保存
   - 個人用として同じアプリの購入
   - この「Appとブック」アカウントでインストールしたアプリを個人アカウントに移動し、利用を継続する

[カタログ設定] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。次の役割が必要です。

- アプリ& コンテンツ管 理

アプリ依存性の導入

自社開発アプリケーションのバンドルをアップロードすると、Ivanti Neurons for MDM がアプリケーションをスキャンして依存性を識別します。依存性が見つかった場合は、アプリ追加ウィザードの3番目の手順でリスト表示します。あらゆるアプリケーションの依存性について、管理者は依存性ファイルのアップロードを選択できます。ただし、依存性ファイルのアップロードなしにインストールできないアプリケーションもあります。

特定のアプリケーションをインストールするときには、管理者がアプリケーションの依存関係を設定できます。このような場合、1つ以上のアプリケーションがメインのアプリケーションにタグ付けすることができます。ユーザがメインのアプリケーションをインストールしようとすると、メインのアプリケーションとともにインストールされる依存関係のアプリケーションについて通知されます。

この機能は、iOS、Android、Windows、、macOS デバイスでのみサポートされます。

アプリケーションの依存性と前提条件について次の点に注意してください。

- 管理者は、アプリケーションをデバイスにインストールするための前提条件となる依存アプリケーションを設定できます。前提条件アプリケーションには、社内アプリケーション、公開アプリケーション、非公開アプリケーション (Android)、VPP アプリケーションを指定できます。
- 今回、[アプリカタログ] ページの [必須アプリ] カラムに、必須アプリケーションの数が表示されるようになりました。数字にカーソルを合わせると、必須アプリケーションのリストが表示されます。
- メインのアプリケーションのインストールがトリガーされると、必須アプリケーションが直接ダウンロードされます。
- メインのアプリケーションが委譲されている場合は、関連する必須アプリケーションが自動委譲されます。
- 必須関係が削除されないかぎり、アプリカタログから必須アプリケーションを削除することはできません。
- あるアプリケーションに複数のバージョンがある場合、バージョンによって必須アプリケーションが異なる場合があります。
- [監査証跡] ページでは、iOS、Android、macOS の前提条件アプリケーションの追加、削除、自動委任が記録されます。
- 管理者またはエンドユーザーが必須アプリケーションをインストールする場合は、メインのアプリケーションをインストールする前に必須アプリケーションがインストールされます。すべての必須アプリケーションがインストールされる前にデバイスチェックインが実行されると、すべての必須アプリケーションがアンインストールされます。

アプリケーションが依存性ファイルを必要とする場合でも、Ivanti Neurons for MDM はアプリ導入の際にファイルのアップロードを要求しません。

Samsung デバイスでは、管理者が前提条件アプリケーションを [キオスクモード許可されたアプリケーション] リストに追加します。[許可されたアプリ] リストに追加された前提条件アプリケーションは、[ブラックリストのアプリケーション] リストに追加されません。

Samsung 以外のデバイスでは、メインのアプリケーションが [キオスクモード許可されたアプリケーション] リストに追加された場合、前提条件アプリケーションをバックグラウンドでサイレントで実行してください。管理者がキオスクモードでこのアプリケーションを設定する場合にのみ、キオスクモードに前提条件アプリケーションを表示できます。

Windows デバイス - Bridge アプリケーションが配布されない前提条件アプリケーションで、メインのアプリケーションがサイレントで配布される .exe の場合。依存関係が削除されると、Bridge アプリケーションがアンインストールされますが、.exe はこのステップの後に失敗します。管理者は、Bridge アプリケーションが既定で配布されないことを確認してください。

Windows デバイス - メインのアプリケーションが対話形式で配布され、メインのアプリケーションに配布されない前提条件アプリケーションがある場合は、前提条件アプリケーションが最初にインストールされ、成功します。ただし、メインのアプリケーションのインストールが失敗した場合は、前提条件アプリケーションがただちにアンインストールされます。失敗したメインのアプリケーションのインストールが再試行されるのは、ユーザがインストール要求をトリガーしたときだけです。

自社開発アプリの追加

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[追加]** をクリックします。
3. アプリファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択]** をクリックしてファイルシステムから選択し、**[確定]** をクリックします。
4. **[次へ]**(右下) をクリックします。Ivanti Neurons for MDM は、アプリに依存性ファイルがないかスキャンし、**[アプリ依存性]** テーブルにリスト化します。
5. アプリ情報を見て正しいアプリを選択していることを確認します。

6. **[アクション]** カラムのアップロードアイコンをクリックしてください。**[依存性をアップロード]** ウィンドウが表示されます。
7. **[ファイルを選択]** をクリックし、ファイルのローカルコピーを指定して **[アップロード]** をクリックします。
8. Ivanti Neurons for MDM は、アプリのオプションパッケージを調べ、あればオプションパッケージ表に追加します。リストにある場合は、アクションカラムのアップロードアイコンをクリックしてください。[オプションパッケージをアップロード] ウィンドウが表示されます。
9. アプリ情報を見て正しいアプリを選択していることを確認します。
10. **[ファイルを選択]** をクリックし、ファイルのローカルコピーを指定して [アップロード] をクリックします。
11. **[次へ]** をクリックします。
12. (任意) アプリのスクリーンショットを追加し、**[次へ]** をクリックします。
13. アプリケーションに別の必須アプリケーションが必要な場合。
    a. **[必須アプリ]** セクションからオプション **[オン]** を選択します。
    b. **[アプリの追加]** タブで必須アプリケーションを検索します。
    c. アプリケーションを選択します。
    d. **[保存]** をクリックします。
14. アプリの配布を定義し、**[次へ]** をクリックします。
15. アプリ構成セクションを定義し、**[完了]** をクリックします。次にデバイスが Ivanti Neurons for MDM と同期すると、アプリが依存性ファイルとともにデバイスに導入されます。

> [依存性を追加] ボタンをクリックすると、依存性を追加できます。アップロード後、追加した依存性は [アプリ依存性] テーブルにもリスト化されます。管理者が手動で「コンテンツのみ」のオプションパッケージを追加することも可能です。このタイプのパッケージはバージョンに依存しません。

必須アプリの追加

メインのアプリケーションに必須アプリケーションを追加できます。メインのアプリケーションの複数のバージョンにそれぞれ異なる前提条件を追加できます。[アプリカタログ] ページでは、説明、スクリプト、スクリーンショット、配布、アプリの前提条件、アプリの構成を既存のアプリケーションバージョンと同じままにするか、必要な関連アプリケーションを変更するかを選択できます。メインのアプリケーションとの関連性を削除せずに、必須アプリケーションを削除することはできません。

[監査証跡] ページで、対応している必須アプリケーションが以下のように特定のフィールドに表示されるようになりました。

[監査証跡] ページのサポートされている iOS、Android、、macOS アプリケーションの [前提条件アプリケーション] セクションには、次のフィールドが表示されます。

- appVersionId
- 名前
- platformAppId

以下のフィールドを含む自動委譲または委譲解除された必須アプリケーションが表示されます。

- dmPartitionDistributionType
- dmPartitionDistributionReason

手順

1. **[アプリカタログ]** からアプリケーションを選択します。
2. **[編集]** をクリックします。
3. **[アプリ委譲]** までスクロールし、オプション **[このアプリをすべてのスペースに委譲]** を選択します。
4. **[保存]** をクリックします。

> 複数のアプリケーションを委譲し、メインのアプリケーションからの委譲を削除するよう選択した場合、必須アプリケーションが自動的に委譲から削除されることはありません。

Android enterpriseによるDivide Productivityの導 入

Divide Productivity は PIM アプリであり、Android Enterprise デバイスに配 布 できます。

1. **[アプリ]** > **[アプリカタログ]** へ進 みます。
2. **[ビジネスアプリ]** から **[Divide Productivity]** をクリックします。
3. 追 加 のカテゴリーや説 明 を入 力 します。
4. **[次 へ]** をクリックします。
5. 表 示 される承 認 事 項 に同 意 します。
6. **[次 へ]** をクリックします。
7. 配 信 オプションを選 択 します。
8. **[詳 細 オプションとアプリ構 成]** を展 開 します。
9. 以 下 のガイドラインを使 用 してオプションを有 効 化 します。

設定	操作内容
ユーザーによるアプリのアンインストールをブロック	サイレントインストールされたアプリをユーザーがアンインストールできないようにする場合に選択します。
メールアドレス	変数を使用し、アプリに関連するEメールアドレスを定義します。
パスワード	変数を使用し、Eメールアカウントのパスワードを定義します。これを空欄にしておくと、ユーザーに入力を求めるプロンプトが表示されます。
ホスト	メールサーバーのホスト名を入力します。ActiveSyncサーバーの完全修飾ドメイン名を入力してください。Standalone Sentryを使用している場合は、その完全修飾ドメイン名 (FQDN) を入力します。 例 : mySentry.mycompany.com
サーバーの種類	メールサーバーの種類を選択します。
ユーザー名	変数を使用し、Eメールアカウントのユーザー名を定義します。
SSL必須	ホストフィールドで指定したサーバーに対し、httpsを使用したセキュア通信を希望する場合に選択します。
すべての証明書を信頼	信頼できない証明書を自動的に承諾する場合のみ選択します。 通常、このオプションを選択するのはテスト環境を使用している場合だけです。

設定	操作内容
デフォルトメール署名	すべてのEメールに使用するデフォルトのEメール署名を入力します。 エンドユーザーは、これをいつでも変更できます。デバイスのユーザーが変更した場合、それ以降のこのフィールドの変更は無効です。
Eメール添付ファイルの最大サイズ	添付可能なファイルの最大サイズを入力します。
タスク有効化	タスクを同期化する場合に選択します。
ログイン証明書エイリアス	ログイン証明書のエイリアスを入力します。
S/MIME署名証明書エイリアス	現在サポートされていません。
S/MIME暗号化証明書エイリアス	現在サポートされていません。
詳細オプション	
デバイスにインストール	アプリをインストールするようユーザーにプロンプトを表示する場合に選択します。
Samsung Knoxデバイスにサイレントインストール	Samsung Knoxデバイスにアプリを自動的にインストールする場合に選択します。
エンドユーザーのアプリカタログでアプリを表示しない	デバイスのアプリカタログにアプリを表示したくない場合に選択します。

10. プロモーションオプションを選択します。
11. **[完了]** をクリックします。

Provisionerアプリの設定

このセクションは以下のトピックを含みます。

- 「プロビジョニングの要件」下
- 「Androidビームを有効化してNFCバンプを利用する」次のページ
- 「会社所有デバイスのプロビジョニング」次のページ
- 「デバイスの登録」ページ405
- 「デバイス登録ステータスの確認」ページ406

Provisioner は Ivanti Neurons for MDM のアプリで、企業が所有するデバイスをプロビジョニングし、仕事用の管理対象デバイスとして登録して、デバイス所有者モードに設定するために使用されます。

会社管理のデバイスには、会社のプロファイルのみが含まれ、個人用プロファイルは含まれません。管理者は、カメラ、通話、SMS、ネットワークなどのデバイス機能を制限できる20以上のロックダウンをデバイス上に設定できます。

Provisioner アプリは、NFC バンプの Android Enterprise 対象デバイスの構成を開始するデバイスで必要です。会社所有のデバイをプロビジョニングするには、Provisionerアプリをマスターデバイスにインストールし、NFC(Near Field Communication) バンプを使用して新規デバイスをプロビジョニングします。バンプとは、2つのデバイス同士を軽くぶつけることです。デバイスは、次のクライアントアプリのいずれかを使うようプロビジョニングできます。

- Go とIvanti Neurons for MDM の使用
- At Work UEM(ブランドなしのクライアントアプリ、Ivanti Neurons for MDM と併用)

プロビジョニングの要件

企業所有の Android Enterprise デバイスを仕事用管理対象デバイスにプロビジョニングするには:

- プロビジョニング前に、企業所有のネイティブ Android Enterprise 対応デバイスを初期設定にリセットする必要があります。
- Android Enterprise 構成を定義し、Android デバイスグループに適用する必要があります。
- Provisionerアプリをインストールし、マスターまたはテンプレートとして機能するよう指定されたNFC対応のAndroidデバイス。

- プロビジョニングする Android Enterprise 対応デバイス。
- Provisionerアプリ。
  Google PlayからAndroid対応 Provisionerアプリをダウンロードします。

Androidビームを有効化してNFCバンプを利用する

手順

1. デバイスの **[設定]** に進みます。
2. **[ワイヤレス& ネットワーク]** に進み、**[その他]** をクリックします。
3. **[NFC]** チェックボックスを選択します。
4. **[Androidビーム]** をクリックし、スイッチを **[ON]** にスライドします。

実際の手順は、お使いのデバイスで若干異なる場合があります。

会社所有デバイスのプロビジョニング

手順

1. ProvisionerアプリをAndroidマスターデバイスとして使用するデバイス上にインストールします。
2. マスターデバイス上でProvisionerを起動します。
3. ドロップダウンリストからアプリを選択します。

4. Provisionerアプリによって求められる情報を入力します。対応しているWi-Fiタイプが存在する場合は、一部のフィールドが自動入力されます。次のガイドラインに従います。

フィールド	値
プロビジョニングのアプリを選択	Go (Ivanti Neurons for MDM で使用するために選択) At Work UEM(ブランドなしのクライアントアプリ、Ivanti Neurons for MDM 併用する場合に選択)
Wi-Fiネットワーク SSID	マスターデバイスが使用するWi-Fi SSIDを入力します。
Wi-Fiセキュリティの種類	Wi-Fiセキュリティの種類を入力します。
Wi-Fiのパスワード	Wi-Fiのパスワードを入力します。
タイムゾーン	現在のローカルのタイムゾーンを入力します。
ロケール	ロケールを入力します。

5. **[続行]** をクリックします。
   [デバイスを動かしてください] 画面がマスタデバイス上に表示されます。

6. 対象デバイスをオンにし、Androidのようこそ画面が表示されたら、マスターデバイスと対象デバイスの背面同士を押し当て、NFC転送を開始します。
   NFC転送が成功したら、対象デバイスから音が鳴り、選択されたクライアントアプリのダウンロードが続行されます。デバイスが暗号化されていない場合は、続行前に暗号化プロセスが始まります。

7. デバイスをバンプすることで、追加のデバイスのプロビジョニングを続行できます。対象デバイスにようこそ画面が表示され、マスターデバイスには **[デバイスをバンプ]** 画面が表示されます。

デバイスの登録

会社所有のデバイスをNFCバンプを使用してプロビジョニングすると、選択されたクライアントアプリがインストールされます。クライアントアプリを立ち上げ、デバイスを登録します。

デバイス登録ステータスの確認

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスのリンクをクリックして詳細を表示します。
3. デバイスのステータスが左のペインにリストされます。

Windows アプリケーションの管理

ユーザーは、(インポート、構成、スケジュール、配布、更新、削除) で、ユーザーは Windows アプリケーションのアプリライフサイクル全体を管理できます。アプリの配布とアプリの更新処理は、MDM コンソール経由でサポートされています。Windows アプリと他のアプリの管理の詳細については、「アプリ構成」ページ337、「アプリ情報」ページ50、「アプリのカタログ」ページ286をご参照ください。

サポートされているアプリタイプ

- 自社開発 (「アプリのカタログ」ページ286セクションの**自社開発アプリの追加** にあるオプションを確認してください)
- MSB (Microsoft Store for Business integration)
- 公開ストア (ネイティブ Microsoft ストア統合を使用) Microsoft Store Region は [アプリ] > [カタログ設定] で設定できます。詳細については、「アプリのカタログ」ページ286セクションの**公開ストアからのアプリの追加** を参照してください。

サポートされているアプリ拡張

- MSI
- MSIX
- APPX
- APPX バンドル
- EXE(「Ivanti Bridge」ページ410経由)

アプリ制御

アプリ制御構成は、デバイス単位でアプリインストールを制御します。詳細については、「アプリ制御構成：デバイスごとにインストールするアプリを制御」ページ445をご参照ください。

パッケージと依存関係

次のさまざまな機能を使用できます。

1. Windows アプリはすべてのタイプのアプリケーションの必須要件として設定できます。アプリ必須要件を設定する方法については、「アプリ依存性の導入」ページ396をご参照ください。
2. APPX および APPX バンドルのアプリ依存性と他のパッケージ依存性。「アプリ詳細の表示」ページ334ページで、**[アプリ依存性とその他のパッケージ]** セクションを確認します。
3. Win32 アプリは、正しい製品コード (MSI)、コマンドライン、変数の選択をサポートします。共通コマンドラインオプションの一覧はこちらをご参照ください。

スクリプト

スクリプトは Ivanti Bridge クライアント経由でサポートされます。スクリプトの設定については、「Ivanti Bridge」ページ410 をご参照ください。

Ivanti Bridge がデバイスにインストールされると、次のようにスクリプトを配布できます。

- Ivanti Bridge を使用したスクリプトとアクションのデバイスレベル
- Ivanti Bridge 構成を使用 ([構成] > [Bridge] に移動)

インストール前およびインストール後のスクリプトとファイル

.exeファイルと.MSIファイルの場合

PowerShellのインストール前およびインストール後のスクリプト、レジストリスクリプト、およびWindows実行可能 (.exe) ファイルの構成、ならびにWindowsアプリ用の他のタイプのファイルのダウンロードを、アプリ詳細レベルで実行できます。

新しいインストール前またはインストール後のスクリプトまたはファイルを追加する場合、Ivanti Bridge画面が表示されます。スクリプトまたはファイルの添付や、スクリプト引数の追加に加え、ファイルのターゲットの場所の指定も行えます。アプリインストールコマンドをデバイスに送信するためには、その前に、インストール前スクリプトがデバイス上で正常に実行されている必要があります。インストール前およびインストール後のスクリプトとファイルは、コンソールにアップロードされたときの順序と同じ順序で実行/インストールされます。インストール前スクリプトのダウンロードまたはインストールが失敗すると、それ以上アプリのインストールを進めることはできません。

インストール後スクリプトが失敗した場合は、[デバイスの詳細] ページの [デバイスログ] セクションでエラーを確認できます。また、インストール後のアクションが失敗した場合、インストール前のスクリプト/ダウンロード済みファイル、およびインストール済み .exe ファイルを元に戻すことはできません。

[スクリプトとファイルの優先順位付け] オプションを使用して、インストール前またはインストール後に実施されるスクリプトとファイルを順序変更できます。このオプションは、使用可能なスクリプトやファイルが少なくとも2つ以上ある場合にのみ利用できます。このオプションを使用する場合、インストール前またはインストール後のどちらか一方のセクション内でファイルやスクリプトをドラッグアンドドロップできます。セクションをまたいだドラッグアンドドロップはできません。

インストールの動作と構成

Windows アプリケーションは次の機能をサポートします。

- サイレントインストール
- 「Windowsアプリスケジューリング」 ページ961
- 再起動オプション

インストール動作の詳細については、「アプリ構成」 ページ337をご参照ください。

(ブリッジを使用してインストールする) MSIアプリとEXEアプリは、ユーザーレスMDMセッションを使用したインストールをサポートしています。

たとえば、次のシナリオがあります。

- デバイスが再起動され、まだユーザーがログインしていない
- ユーザーが Windows セッションからログアウトした
- デバイスがオートパイロット ユーザーレス (自己配布または事前プロビジョニング) モードで登録された
- アプリケーションがデバイスレベルでインストールされていない

たとえば、オートパイロット登録中や、誰もWindowsデバイスで作業していない夜間など、効率的な方法でMSIアプリをインストールできます。MSIでEXEの簡易再圧縮が使用される場合、インストールできますが、アップグレードまたは削除はできません。実際のMSIパッケージはCSPに接続しています。他のアプリケーションタイプは、ユーザのログイン後にインストールされます。

Tunnel for Windows (Per-App VPN)

Tunnelはスタンドアロンのネイティブ Windows アプリケーションです。現在、デバイスへの配布用として Microsoft Store で提供されています。Per-App VPN構成を作成します。Sentry配布が必要です。Tunnelアプリを構成するには、**[構成]** > **[+追加]** > [Tunnelの検索]に移動します(Windowsデバイスをサポートする構成を選択します)。Sentryプロファイルを選択し、設定を構成すると、Sentry経由でアプリデータのトンネリングを開始できます。Sentryサーバーを設定するには、**[管理]** > **[インフラストラクチャ]** > **[Sentry]** に移動します。

アプリのインベントリ

Windowsデバイスフリートにインストールされたアプリケーションおよびソフトウェアインベントリは次の2つのレベルで追跡できます。

- デバイス全体でインストールされたアプリケーションを確認するには、**[デバイス]** > **[アプリのインベントリ]** に移動します。
- デバイスレベルでインベントリを確認するには、[デバイス]に移動して、デバイスを選択し、[インストール済みのアプリ]をクリックします。

管理者はWindowsアプリケーションインベントリ収集間隔を設定できます。[管理] > [Windows] > [アプリインベントリの間隔]に移動します。間隔は、デバイスからすべてのアプリを収集するようプライバシー構成が設定されている場合に使用します。プライバシー構成を設定するには、[構成] > [+追加]に移動して、プライバシーを検索し、[デバイス上のすべてのアプリのアプリインベントリの収集]を選択します。収集するアプリの種類を選択します。

企業アプリカタログ (Apps@Work)

お客様はApps@Workを使用して、Windowsデバイスで企業カタログを有効化できます。Apps@WorkはNeurons for UEMのアプリカタログ経由で提供され、配布されます。詳細については、「Apps@Work (iOS、Android、Windows、macOS)」ページ317をご参照ください。

Ivanti Bridge

このセクションは以下のトピックを含みます。

Ivanti Bridgeは、1つのコンソールと通信チャネルを使用して、Windows 10のモバイルおよびデスクトップ運用を統合します。Bridgeにより、PCを管理するUEM機能が拡張され、組織は大幅に低いコストと高い効率性で、PCとモバイルの両方に一貫したセキュリティを確保できます。Ivanti Bridgeを使用すると、企業は、サポートされているWindowsモバイルデバイスと同じように、Windows 10デスクトップデバイスで1つのプロトコルを使用し、OSのレガシーアプリケーションに情報を送信できます。

Ivanti Bridgeを使用すると、IT部門は、重要な機能を失うことなく、UEM上でWindows管理業務を現代化することができます。システムイメージ、ドメイン参加、デバイスへの複数の通信チャネルなしに、既存のポリシーとスクリプトを適用することも可能です。

Ivanti Bridgeを使用すると、組織は次のことができるようになります。

- UEMでPCを完全に制御する
- リモート(無線)でPCを管理する
- デスクトップのイメージングの必要を減らす
- UEMが採用しているPowerShellスクリプトでGPOベースのコマンドを利用する
- レジストリを簡単に編集/管理する
- MSIラップされていないWin32アプリを楽に導入する
- ファイルシステムを可視化する

Ivanti Bridgeは Windows 10 Pro または Windows 10 Enterprise デスクトップデバイスでのみ使用され、ARM プロセッサではサポートされていません。Ivanti Bridge は Windows 10 Home デスクトップ デバイスをサポートしません。

Bridgeがサポートするファイル形式

Ivanti Bridge は次のファイルタイプをサポートします。

- PowerShell

  Bridgeを使用してデバイスにプッシュされたPowerShellスクリプトは、名前付き引数をサポートします。

  64ビットのWindows 10デスクトップデバイスでは、64ビットのPowerShellスクリプトがサポートされます。

  > Powe iShell スクリプトをデバイスに送信した後に結果を想定するサーバ側の Bridge タイムアウトは約20分です。タイムアウトは失敗として記録されます。ただし、デバイスのスクリプトは引き続き動作します。

  > Powe iShell スクリプト実行のプロセスを想定するデバイス側の Bridge タイムアウトは約60分です。60分後、プロセスは終了します。スクリプトの出力は保存されず、新しい失敗がサーバに送信されます。

  > サーバ側およびデバイス側のタイムアウトは失敗として記録されます。2回目のタイムアウトが経過し、スクリプトで何らかの出力が実行された場合は、出力はサーバ側に記録されません。

- レジストリ
- VBスクリプト
- Win32アプリケーション導入の.EXE

  > 管理者がWin32(.EXE) ファイルをデバイスにプッシュする場合 (自社開発のWindowsアプリとしてなど) 、使用可能であればBridge機能が自動的に使用されます。ファイルをサイレントに実行するには引数の入力が必須です(/SILENT、/VERYSILENTなど) 。
  > .EXEアプリは、Admin PowerShellモードを使用し、Bridgeからインストールできます。Windowsデバイスの場合、ユーザーの認証情報を使用してインストールするには、[ユーザーとして実行] を選択してください。

Ivanti Bridge を使用すると、次の主な分野でデバイスを強化できます。

- **レジストリ:** レジストリ値の読み出し、書き込み、更新。
- **ファイル:** ファイルの検証、読み出し、コンテンツの更新。

- **アプリケーション導入：**.EXEベースのアプリケーションをデスクトップ機器にインストールする機能を追加。これらのアプリケーションは、Ivanti Neurons for MDM サーバまたはクラウドのコンテンツ配信ネットワーク (CDN) に常駐できます。

Bridgeのセットアップ

Ivanti Bridge を設定するには、管理者が次の手順を次の順序で完了する必要があります。

1. 「Bridge ライセンスの認証」下
2. 「Bridgeモバイルアプリケーションのインストール」下
3. デバイスに永久使用または1回使用の「デバイスへのスクリプトのアップロード」下する

Bridge ライセンスの認証

Ivanti Bridge はレガシー Gold パッケージと現在の Secure UEM パッケージの一部です。

Bridgeモバイルアプリケーションのインストール

Ivanti Bridge ライセンスを認証した後は、次のように、Bridge モバイル アプリケーションをインストールできます。

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[+追加]** をクリックします。
3. [ビジネスアプリ] セクションで **[Ivanti Bridge]** をクリックします。
4. 詳細を記入し、カスタマイズした後、購入したライセンスに従って、必要なデバイスにBridgeモバイルアプリケーションを配布します。
   [Windowsデバイスにサイレントインストール] オプションを有効化している場合、Bridgeモバイルアプリケーションはサイレントにインストールされ、デバイスでBridgeサービスの実行が開始されます。

Bridgeアプリはデフォルトでアプリカタログに追加され、デフォルトですべてのデバイスに配布されます。

デバイスへのスクリプトのアップロード

管理者は、新しいBridge構成の作成により、永久使用のスクリプトをデバイスにアップロードできます。

1. **[構成] > [+追加]** を開きます。
2. **[Ivanti Bridge]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [構成設定] セクションで、手順7の表のとおりに残りを設定します。
    1. **[スクリプトファイル]** カテゴリ設定を入力し、デバイスにプッシュまたは実行するインストールスクリプトを指定します。
    2. (任意) **[スクリプトファイルを元に戻す]** カテゴリー設定を入力し、デバイスにプッシュまたは実行するアンインストールスクリプトを指定します。これは、デバイス撤去や構成削除などの際に有用となります。
    3. (任意) **[Outlookを構成]** オプションを選択し、Bridgeを使用してデバイスにMicrosoft Outlookを構成します。

        Outlook 2010、2013にのみ対応しています。
6. **[次へ]** をクリックします。
7. この構成の配布を選択します。
   これらのデバイス操作には強制チェックインが自動的に実行されます。

カテゴリ	設定	操作内容
	名前	この構成を識別する名前に入力します。
	説明	この構成の目的を明示する説明を入力します。
スクリプトファイル	**全バージョン(Windows 10+デスクトップ)**	
	スクリプトファイル	有効なスクリプトまたは実行ファイル(.ps1、.reg、.exe)を選択します。 • 指定したスクリプトファイルまたは実行可能ファイル(.ps1、.reg、.exe)が自動的に実行されます。 • その他のファイル形式はターゲットフォルダーにコピーされるだけです。
	スクリプト引数	スクリプトファイルの引数リストを指定します。 •  Win32(.exe)ファイルの場合は、ファイルをサイレントに実行する引数を入力します(/SILENT、/VERYSILENTなど)。これは必須です。
	ターゲットフォルダー	スクリプトファイルのターゲットフォルダーを指定します。 • ターゲットフォルダーを指定しない場合、%TEMP%システム環境変数の値がターゲットフォルダーとして使用されます。
取り消しスクリプトファイル	**全バージョン(Windows 10+デスクトップ)**	

	スクリプトファイル	有効なスクリプトまたは実行ファイル (.ps1、.reg、.exe) を選択します。 • 指定したスクリプトファイルまたは実行可能ファイル(.ps1、.reg、.exe) が自動的に実行されます。 • その他のファイル形式はターゲットフォルダーにコピーされるだけです。
	スクリプト引数	スクリプトファイルの引数リストを指定します。 • Win32(.exe) ファイルの場合は、ファイルをサイレントに実行する引数を入力します (/SILENT、/VERYSILENTなど) 。これは必須です。
	ターゲットフォルダー	スクリプトファイルのターゲットフォルダーを指定します。 • ターゲットフォルダーを指定しない場合、%TEMP%システム環境変数の値がデフォルトで使用されます。

デバイスへの1回使用のスクリプトのアップロード

管理者は1回使用 (その場限り) のスクリプトをデバイスにアップロードできます。

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイス名リンクをクリックし、[デバイス詳細] ページを開きます。これが1回使用のスクリプトがプッシュ/実行されるWindows 10デスクトップです。
3. アイコンをクリックして、**[Ivanti Bridge を使用したスクリプトとアクション]** をクリックします。
4. 名前を入力します。
5. スクリプトファイルセクションで、上記の表に従い、デバイスにプッシュ/実行するスクリプトを指定します。

6. [**Apply**] をクリックします。
   スクリプト実行がキューになり、完了までに少し時間がかかる場合があります。[ログ] タブを開き、ステータスを確認してください(出力または失敗メッセージ) 。これらのデバイス操作には強制チェックインが自動的に実行されます。

Bridgeログ

この機能により、アプリケーションのトラブルシューティングおよび診断の目的で、個々のデバイスのIvanti Bridgeログを取得できます。ログは次のデバイスチェックイン時に送信されます。スケジュール設定した次の同期を待つか、強制デバイスチェックインを実行してログを取得してください。

デバイスからログを取得するには:

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイス名リンクをクリックし、[デバイス詳細] ページを開きます。これが1回使用のスクリプトがプッシュ/実行されるWindows 10デスクトップです。
3. アイコンをクリックし、**[Ivanti Bridge ログの取得]** をクリックします。**[Ivanti Bridge ログの取得]** ウィンドウが表示されます。
4. 以下のオプションから1つ選択してください。
   単一ログ - Ivanti Neurons for MDM にデバイス上の最新のBridgeログの取得を要求します。
   すべてのログ - Ivanti Neurons for MDM にデバイス上のすべてのBridgeログ(最大30日間) の取得を要求します。
5. **[ログを取得]** をクリックします。デバイスがログを Ivanti Neurons for MDM に送信すると、デバイス詳細ページの [ログ] タブからBridgeのログを閲覧できます。

   [すべてのログ] オプションで送信されたログはzipファイルのみでダウンロード可能となります。

Bridge 前回のチェックイン

[デバイス] ページの [Bridge 前回のチェックイン] 列には、Bridge サービスの前回のチェックイン日時が表示されます。[列のカスタマイズ] オプションを使用すると、この列を [デバイス] ページに追加できます。既定では列は表示されません。

この列を表示するには、**[デバイス]** > **[列のカスタマイズ]** > **[Bridge チェックイン]** をクリックします。

エクスポートされたデータには、Bridge の前回のチェックイン詳細情報もあります (該当する場合)。

Bridge サービス障害回復

Bridge サービス障害回復は、Bridge 2.1.14 バージョンで導入されました。既定では、このバージョンは、すべてのユーザのアプリケーション カタログにインポートされます。ごくまれに、Bridge サービスが不明な理由で失敗する場合があります。このような場合、サポートは、Bridge 2.1.14以降のバージョンで提供されています。

コンテンツ

[コンテンツ] ページでは、外部ソースによりホストされているコンテンツを配布します。コンテンツには、営業用プレゼンテーション、画像、スプレッドシート、ドキュメントなど、ユーザーがダウンロード可能なファイルが含まれます。

このセクションは以下のトピックを含みます。

コンテンツの管 理

このセクションは以 下 のトピックを含 みます。

- 「ホスト型 コンテンツの配 布 」次 のページ
- 「コンテンツの削 除 」ページ421

ホスト型 コンテンツは、外 部 URLによるダウンロード可 能 なコンテンツの配 布 に対 応しています。外 部 URLは、ダウンロード可 能 なPDFまたはEPUBまたはIBOOKファイルにのみつながるものとし、外 部 URLにはこれらの拡 張 子 が必 要 となります。

VPP Bookライセンスの配 布 には対 応していません。したがって、iTunes Store IDに基 づくApple Booksの配 布 にも対 応していません。

Ivanti Neurons for MDM からプッシュされたコンテンツにアクセスするには、BooksまたはPagesアプリを使 用してください。これらには [ライブラリ] セクションでアクセスできます。

iBookおよびEPUB形 式 のコンテンツは、iOS 8+ iPadデバイス(Goldライセンス) に配 布 可 能 です。これらの形 式 は、AppleがiPadに対してしか社 内 配 布 をサポートしていないため、iPad限 定 となります。iOS 9デバイスにこの制 限 はありません。

これらの形 式 についてはコンテンツプレビューを利 用 できません。

PDFコンテンツの場 合 、iOS 8+デバイスのiBookアプリにドキュメントをプッシュすることも可 能 です。

ホスト型コンテンツの配布

新しいドキュメントをIvanti Neurons for MDMにアップロードすることはできませんが、コンテンツをホスティングした場所のパス(URL)をデバイスグループに配布することは可能です。

手順

1. **[コンテンツ]** > **[ホスト型コンテンツ]** を開きます。
2. **[+追加]** をクリックします。
3. 次の情報を入力します。
   - タイトル
   - 作者
   - カテゴリ
   - 説明(任意)
4. **[ホスト型コンテンツパス]** フィールドにアップロードしたいファイルのURLを入力します。
5. **[次へ]** をクリックします。
6. 必要な変更を配信に加えます。
7. **[完了]** をクリックします。

ホスト型コンテンツを変更する場合は、前のコンテンツを削除し、新しいホスト型コンテンツを追加して配布する必要があります。

URL以外の設定を変更するには:

1. **[コンテンツ]** > **[ホスト型コンテンツ]** を開きます。
2. **[名前]** カラム内のドキュメントへのリンクをクリックします。
3. 編集アイコンをクリックします。
4. 必要な変更を加えます。
5. **[次へ]** をクリックします。

6. 必要な変更を配信に加えます。
7. **[完了]** をクリックします。

コンテンツの削除

1. **[名前]** カラム内のドキュメントへのリンクをクリックします。
2. **[アクション]** > **[このドキュメントを削除]** を選択します。
3. 確認のためチェックボックスをクリックします。
4. **[ドキュメントの削除]** をクリックします。

ドキュメントを削除すると:

- システムから削除されます。
- コンテンツカタログで見ることができなくなります。
- ダウンロードしたデバイスから削除されます。

[コンテンツ] ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。次の役割が必要です。

- アプリ& コンテンツ管理

カテゴリ

このセクションは以下のトピックを含みます。

- 「カテゴリの追加」下
- 「カテゴリの削除」下

2017年4月15日に発表されたコンテンツサポート終了の一環として、新規コンテンツを追加する機能が無効化されました。現在アップロード済みのコンテンツは、引き続きApple iBookへの配布と使用が可能です。

カテゴリとは、**コンテンツカタログ**[1]内の**コンテンツ**[2]のタイプを説明するものです。カテゴリは、ユーザーが必要なものを見つけやすいようコンテンツを系統立てるのに役立ちます。コンテンツカタログに追加されたどの項目にも、1つ以上のカテゴリを割り当てる必要があります。

カテゴリの追加

手順

1. **[追加]**(左下)をクリックします。
2. カテゴリ名を入力します。カテゴリは大文字と小文字の区別がありません。
3. **[保存]**をクリックします。

カテゴリの削除

カテゴリの横にある[X]をクリックしてカテゴリを削除できます。

[コンテンツ(コンテンツ)]ページでタスクを実行できない場合、必要な権限を持っていない可能性があります。次の役割が必要です。

- アプリ& コンテンツ管理

[1]files that are published by and distributed to users.

[2]a list of files that have been published by and distributed to users. A typical catalog might include sales presentations, images, spreadsheets, and documents.

設定

構成とは、デバイスに送信する設定の集合体です。たとえば、構成を使用すると、デバイス上のVPN設定やパスコード要件を自動的に設定することができます。お使いのシステムの既存の構成は、[構成] ページに一覧表示されます。

このセクションは以下のトピックを含みます。

構成の操作

このセクションは以下のトピックを含みます。

構成とは、管理者がデバイスに送信する設定の集合体です。たとえば、構成を使用すると、デバイス上のVPN設定やパスコード要件を自動的に設定することができます。お使いのシステムの既存の構成は、[構成] ページに一覧表示されます。[構成] ページから複数の構成を選択し、複数のデバイスにまとめてプッシュできます。これらの構成は、スペース固有のデバイスにプッシュできます。他のスペースのデバイスは影響を受けません。構成は、単一スペースまたは複数スペースにプッシュするか、または一度にすべてのスペースにプッシュすることができます。

多くの構成の種類が利用できます。構成は次のような基本的カテゴリに分類されます。

- セキュリティ
- ユーザーリソース
- エンタープライズネットワークアクセス
- セルラーネットワーク
- その他(追加の構成)

ほとんどの構成で、以下のアクションを実行できます。

- 追加
- 編集
- 複製
- 削除
- 特定のデバイスから1つ以上の構成を除外
- 特定のデバイスに1つ以上の除外済み構成をプッシュ

一部の構成ではアクションが制限されています。

- 追加や複製を実行できない構成があります。iOSアクティベーションロックはこのタイプの構成の一例です。したがって、構成を追加する際に一覧表示されるタイトルには、これらの構成は含まれません。これらの構成は、[Configurations] ページの一覧にのみ表示されます。
- システム定義の構成は、編集や削除を行えません。iOS EnrollmentのSCEPはこのタイプの構成の一例です。
- 一部の構成は、削除不可に指定、あるいはデバイスから再インストールが可能です。これらの構成は除外したり、デバイスにプッシュしたりできません。

構成の表示のフィルタリング

[構成] ページには、すべての構成がリスト表示されます。このリストを特定の構成に絞り込むには、OSおよび構成の種類のフィルター(左ペイン) を使用します。たとえばmacOSの構成のみ表示するようリストを絞り込むには、**[OS]** セクションで **[macOS]** を選択します。

ドロップダウンリストから複数のスペースを選択すると、すべてまたは複数のスペースのデバイスの構成を表示可能です。表示された構成の上にマウスを置くと、ポップアップウィンドウにスペースのリストが表示されます。構成の詳細ページを開くにはスペースをクリックします。

既存の構成を名前で検索するには、構成名を **[検索]** フィールドに入力します。

Ivanti Neurons for MDM リリース81以降、グローバル管理者はスペース管理者に、すべてのデバイス向けおよびカスタム配信オプション向けの動的生成ID証明書の編集を委譲できるようになりました。

構成の追加

このオプションはドロップダウンリストで1つのスペースが選択された場合のみ有効となります。

1回に配布できる構成ファイルは最大100件です。

手順

1. **[追加]** をクリックします。
2. 作成したい構成の種類を選択します。
3. **[次へ]** をクリックします。
4. この構成をすぐに有効にしたくない場合は、**[この構成を有効化]** オプションを選択解除します。

5. 構成の配布レベルを選択します。

   - **すべてのデバイス** - 利用可能なすべてのデバイスに構成を配布します。複数のスペースに構成を委譲するには、次のいずれかのオプションを選択します。

     - **他のスペースに適用しない**。
     - 複数のスペースに構成を委譲する場合、**[配布の概要]** > **[他のスペースにあるデバイスにも適用する]** を選択します。
       - **[スペース管理者に配布の編集を許可]** チェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

   - **デバイスなし** - 後で配布する場合はこの構成を選択します。
   - **カスタム** - この構成を送信する具体的なデバイス群を定義してください。複数のスペースに構成を委譲するには、次のいずれかのオプションを選択します。

     - **他のスペースに適用しない**。
     - **[配布の概要]** > **[他のスペースにあるデバイスにも適用する]**。
       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

     > 管理者はカスタム配布オプションを使用し、カスタム構成をデバイス、デバイスグループ、ユーザー、ユーザーグループに配布できます。ユーザーまたはユーザーグループへの構成の割り当てまたは配布は、以下の構成では使用できません。

     - Android Enterprise：仕事用プロファイル(Android for Work)
     - Android Enterprise：仕事用マネージドデバイス(Android for Work)
     - Android Enterprise：仕事用プロファイルを持つマネージドデバイス/会社所有デバイス上の仕事用プロファイル
     - 仕事用マネージドデバイス非GMSモード(AOSP) デバイス用の、Android仕事用マネージドデバイス(デバイス所有者)

6. サービスがスペースを定義している場合は、構成を他のスペースに適用するかどうかとその優先度を指定します。
7. **[完了]** をクリックします。

デバイス上にプロファイルをインストールする代わりに、デバイスにコマンドを発行する構成の場合は、デバイスに適用される構成が構成の詳細リストに表示されません。

構成をデバイスにプッシュする

デバイス上で除外した構成を再インストールしたい場合は、構成をプッシュできます。

手順

1. **[デバイス]** > **[デバイス]** を開きます。
2. デバイス名をクリックして詳細ページを表示します。
3. **[構成]** に進みます。
4. 該当するチェックボックスにチェックを入れて、デバイスにプッシュする特定の構成を選択します。
5. **[プロファイルをプッシュ]** をクリックします。
6. 1つの構成をプッシュするには、**[アクション]** カラムから **[プッシュ]** をクリックします。

構成を複数のデバイスにプッシュする

[構成] ページから複数の構成を選択し、複数のデバイスにまとめてプッシュできます。

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[構成]** に進みます。
3. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。
4. **[アクション]** をクリックし、**[選択した構成をデバイスへプッシュ]** を選択します。[構成のプッシュ] ウィザードが開き、すべての構成とそのプッシュステータスが表示されます。
5. **[有効な構成をプッシュ]** をクリックします。構成はすべてのデバイスに一括でプッシュされます。**[デバイス]** > **[構成]** タブで、特定のデバイスに対して除外した構成はプッシュされません。

構成の除外

過去に配布された構成は、デバイスから手動で削除または除外できます。

手順

1. **[デバイス]** > **[デバイス]** を開きます。
2. デバイス名をクリックして詳細ページを表示します。
3. **[構成]** に進みます。
4. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。
5. **[プロファイルを除外]** をクリックします。

   1つの構成を除外するには、**[アクション]** カラムから **[除外]** をクリックします。選択した構成が、[除外された構成] タブにリスト表示されます。

除外された構成のプッシュ

手順

1. **[デバイス]** > **[デバイス]** を開きます。
2. デバイス名をクリックして詳細ページを表示します。
3. **[構成]** > **[除外した構成]** を開きます。
4. デバイスにプッシュする構成を1つ以上選択します。
5. **[プロファイルをプッシュ]** をクリックします。
6. 1つの構成をプッシュするには、**[アクション]** カラムから **[プッシュ]** をクリックします。

構成のエクスポート

選択したスペースから、選択した構成またはすべての構成の詳細を個別のファイルにエクスポートできます。

手順

1. **[構成]** に進みます。
2. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。

3. **[アクション]** > **[選択した構成と詳細をエクスポート]** をクリックします。すべての構成をエクスポートする場合は、**[すべての構成と詳細をエクスポート]** を選択します。

   YAMLファイル群がZIPファイルに含まれます。レポートには選択したスペース内の既存の構成すべての詳細が含まれます。

すべての構成をエクスポート

サポートが診断に利用できるよう、構成ファイルをエクスポートして送信します。YAML形式ファイルで構成ファイル1つをエクスポートすることも、.zipファイルですべての構成をエクスポートすることも可能です。エクスポートしたい構成に応じて、[構成] ページの異なる領域にある複数のファイルをエクスポートできます。

手順

1. **[構成]** に進みます。
2. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。
3. **[アクション]** > **[選択した構成と詳細をエクスポート]** をクリックします。すべての構成をエクスポートする場合は、**[すべての構成と詳細をエクスポート]** を選択します。

   YAMLファイル群がZIPファイルに含まれます。レポートには選択したスペース内の既存の構成すべての詳細が含まれます。

カスタマイズされた構成のエクスポート

手順

1. **[構成]** に進みます。
2. **[+追加]** をクリックして構成を選択します。
3. 次の手順で構成をカスタマイズします。
4. **[次へ]** をクリックします。
5. 配布レベルを選択します。
6. **[完了]** をクリックします。
7. **[構成]** ページのリストから作成した構成を選択します。
8. **[アクション]** プルダウンメニューをクリックし、**エクスポート。**
   構成名と_yyyymmdd.yamlというタイムスタンプのファイルがデバイスにダウンロードされます。

既存の構成のエクスポート

手順

1. **[構成]** に進みます。
2. 既存の構成を選択します。
3. **[アクション]** プルダウンメニューをクリックし、**[エクスポート]** をクリックします。
   構成名と_yyyymmdd.yamlというタイムスタンプのファイルがダウンロードされます。

構成のインポート

構成詳細情報を含むYAMLファイルをインポートできます。構成を編集するには、YAMLファイルの詳細情報を編集し、構成を選択して、ファイルをインポートできます。更新された値は構成に表示されます。複数の構成またはスペースが選択されている場合、[インポート] ボタンが無効になります。正しくないファイルタイプを選択すると、エラーメッセージが表示されます。構成で必要な詳細情報以外が含まれているYAMLファイルを選択すると、エラーメッセージが表示されます。

手順

1. **[構成]** に進みます。
2. 構成を選択し、**[インポート]**、**[ファイルの選択]** をクリックして、YAMLファイルを選択し、**[インポート]** をクリックします。YAMLファイルと構成詳細がインポートされます。

YAMLファイルを使用した構成の作成

YAMLファイルをから構成を作成できます。配布関連の指定はYAMLファイルの範囲ではありません。既定では、配布は [デバイスなし] に設定されています。

手順

1. **[構成]** に進みます。
2. **[インポート]**、**[ファイルの選択]** をクリックして、YAMLファイルを選択し、**[インポート]** をクリックします。
   YAMLファイルと構成詳細がインポートされます。[構成の作成] ページが開き、YAMLファイルに追加されたすべての詳細情報が表示されます。

3. 配布タイプの*いずれか*を選択します。
   - **すべてのデバイス**
   - **デバイスなし**
   - **カスタム**
4. 構成の詳細情報を確認し、次の配布の概要オプションの*いずれか*を選択します。

   一部の構成の配布の概要は表示されません。

   - **他のスペースに適用しない**
   - **他のスペースにあるデバイスに適用する**
5. 構成の新しい名前が既存の構成の名前と一致する場合は、エラーメッセージが表示されます。**[OK]**、**[戻る]** をクリックして、構成名を編集します。
6. **[次へ]** をクリックした後、**[完了]** をクリックします。

構成の編集

構成を開き、構成の詳細情報を直接編集するか、すべての必要な詳細情報を含むYAMLファイルをインポートできます。複数の構成またはスペースが選択されている場合、[インポート] ボタンが無効になります。

手順

1. **[構成]** に進みます。
2. 構成を選択して開き、編集 (鉛筆) アイコンをクリックして、構成を編集します。
3. あるいは、[構成の編集] ページで **[インポート]** アイコンをクリックし、YAMLファイルを選択して、**[インポート]** をクリックします。[構成の編集] ページが開き、YAMLファイルに追加されたすべての詳細情報が表示されます。

4. 構成の詳細情報を確認し、次の配布の概要オプションのいずれかを選択します。

   一部の構成の配布の概要は表示されません。

   - **他のスペースに適用しない**。
   - **他のスペースにあるデバイスに適用する**

     既定では、配布は [デバイスなし] に設定されています。

5. **[次へ]** をクリックします。
6. **[次へ]** をクリックした後、**[完了]** をクリックします。

構成の削除

選択した構成を削除できます。

手順

1. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。
2. **[アクション]** > **[削除]** をクリックします。

自社開発アプリ更新のスケジュール

デバイスのチェックイン時には Ivanti Neurons for MDM で自動的に社内アプリケーションが更新されます。管理者は、サーバのタイムゾーンに基づいて、社内アプリケーション更新をスケジュールできます。アプリの更新は、スケジュールされた時間帯にデバイスがチェックインしたときのみ実行されます。アプリ更新のスケジュールはデフォルトで無効化されています。

この構成は、更新にのみ適用され、新規インストールには適用されません。[インストール/更新を送信] コマンドを使用すると、iOSアプリの自動更新スケジュールを上書きできます。自動更新がアプリレベルまたはカタログレベルで有効になっている場合は、スケジュールされたアプリ構成よりも優先され、アプリはチェックイン時に即座に更新されます。

この構成は、次のアプリケーションタイプにのみ適用されます。

- iOS自社開発アプリ。
- Android自社開発アプリ(DOモードのみ) 。
- .pkgおよび.MIP形式のmacOSアプリ。
- Windowsアプリ。

前提条件

構成が期待どおりに機能するには、以下の前提条件を満たす必要があります。

- アプリは必ずiOS/Android向けに管理します。macOSの場合、アプリはマネージドまたは非マネージドの状態になります。
- [アプリケーション構成] で [デバイスにインストール] が有効化されていることを確認します。
- デバイスはスケジュールされた時間帯にチェックインする必要があります。

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[構成]** に進みます。
3. **[Add]** をクリックします。[構成を追加] ページが開きます。
4. **[アプリ自動更新]** を検索します。[アプリ自動更新構成の作成] ページが開きます。
5. **[名前]** フィールドで名前を指定します。
6. **[構成設定]** セクションでドロップダウンリストから **[タイムゾーン]** を選択します。
7. ドロップダウンリストから **[開始時刻]** を選択し、**[時間]** もドロップダウンリストから選択します。
8. **[次へ]** をクリックします。
9. 必要なユーザー/デバイスグループを選択し、**[この構成を有効化]** のチェックボックスをクリックします。
10. **[完了]** をクリックします。構成が適用されると、所定のスケジュールでのみアプリが更新されます。

[構成] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- 読み取り専用デバイス

関連トピック:

- スペース
- 構成の優先度決定

ユーザーセルフサービスポータル構成の作成

企業ユーザーとして、セルフサービスポータルを使用してデバイスや証明書を管理することができます。[マイデバイス] タブには登録したデバイスが表示されます。

[マイデバイス] タブからは以下のタスクを実行できます。

- ロック
- ロックの解除
- 撤去
- セキュアアプリパスコードのリセット

[マイ証明書] タブからは以下のタスクを実行できます。

- 証明書をアップロード

1回に配布できる構成ファイルは最大100件です。

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[追加]** をクリックします。
3. **[ユーザーセルフサービスポータル構成の作成]** を検索します。
4. **[次へ]** をクリックします。
5. この構成をすぐに有効にしたくない場合は、**[この構成を有効化]** オプションを選択解除します。

6. 構成の配布レベルを選択します。

   - **すべてのデバイス** - 利用可能なすべてのデバイスに構成を配布します。複数のスペースに構成を委譲するには、次のいずれかのオプションを選択します。

     - **他のスペースに適用しない**。

     - 複数のスペースに構成を委譲する場合、**[配布の概要]** > **[他のスペースにあるデバイスにも適用する]** を選択します。

       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

   - **デバイスなし** - 後で配布する場合はこの構成を選択します。

   - **カスタム** - この構成を送信する具体的なデバイス群を定義してください。複数のスペースに構成を委譲するには、次のいずれかのオプションを選択します。

     - **他のスペースに適用しない**。

     - **[配布の概要]** > **[他のスペースにあるデバイスにも適用する]**。

       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

7. サービスがスペースを定義している場合は、構成を他のスペースに適用するかどうかとその優先度を指定します。

8. **[完了]** をクリックします。

デバイス上にプロファイルをインストールする代わりに、デバイスにコマンドを発行する構成の場合は、デバイスに適用される構成が構成の詳細リストに表示されません。

カスタム構成

このセクションは以下のトピックを含みます。

- 「カスタム構成の定義」下
- 「カスタム構成設定」次のページ

ライセンス: Silver

対象: iOS、macOS、Android、Windows

説明

あらかじめ定義した構成ファイルをインポートおよび配布できます。

有効な構成ファイルの形式は次のとおりです。

OS	有効な構成ファイル形式
iOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
[Android]	.xml。現在、Zebraデバイスでこの機能がサポートするのは.xml構成ファイルのみです。
Windows	SyncML

カスタム構成の定義

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。

3. 検索フィールドに「カスタム」と入力し、**[カスタム]** 構成をクリックします。
   カスタム構成の詳細ページが表示されます。
4. このページで設定を構成します。参考値は、カスタム構成設定セクションの表をご覧ください。
5. **[次へ]** をクリックして配布設定を行います。
6. (macOSデバイス) 構成の必要に応じて、**[この構成は誰に適用されますか？]** 設定を選択します。
   - デバイス全体(一般的に使用)
   - 特定ユーザー(現在の登録ユーザー)
7. **[完了]** をクリックします。

カスタム構成設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
OSを選択	OSアイコンをクリックし、選択したアイコンに対応する構成ファイルをアップロードします。
ファイルを選択	このオプションはOS選択後に表示されます。構成ファイルをドラッグ＆ドロップボックスにドラッグするか、**[ファイルを選択]** ボタンをクリックして構成ファイルを選択します。

カスタムCSP構成(Windowsのみ)

カスタムCSP構成はWindowsデバイスでのみ作成できます。[Choose OS] セクションから [Windows OS] を選択すると、次の2つのオプションが表示されます。

オプション1 - CSP XMLファイル - このオプションを選択し、**ファイルを選択** 設定の場合と同じプロセスに従います。

オプション2 - カスタムCSP OMA-URIスキーマノード

手順

1. リストから [カスタムCSP OMA-URIスキーマノード] オプションを選択します。[カスタムCSP構成] セクションが画面に表示されます。
2. **[アクション]** で [+] ボタンをクリックして、各種OMA-URIフィールドを使用した構成の作成を開始します。
3. 以下のフィールドを含む **[行を追加]** ポップアップウィンドウが画面に表示されます。
   - 説明 - 設定に関する一般情報を任意に入力します
   - OMA-URI - 設定として使用するOMA-URIを入力します
   - データタイプ - この設定で使用するデータタイプを選択します(DATE、FLOAT、BASE64、NODE、XML、BINARY、CHARACTER、TIME、BOOLEAN、INTEGER)
   - 値 - 選択したデータタイプに関連付けられた値を入力します
   - アクセスタイプ - Add、Delete、Exec、Replace、Get
4. **[保存して閉じる]** をクリックして、詳細が指定されたウィンドウを閉じます。別の行を作成するには **[保存して追加]** をクリックします。
5. **[次へ]** をクリックします。
6. 配布のモードを選択し、**[完了]** をクリックします。

関連トピック

- カスタム構成を使用したデバイスへのSyncMLプッシュ
- 構成を作成するには

カスタム構成を使用したデバイスへのSyncMLプッシュ

独自のSynchronization Markup Language(SyncML) 構成ファイルを作成することも、サードパーティのソースから取得して、カスタム構成に追加することでカスタム機能を実装することもできます。

サポート対象のプラットフォーム:

- Windows 10 Mobile
- Windows 10デスクトップ

サポートされているデバイス:

- Windows 10+
- Microsoft HoloLens 2

手順

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[カスタム構成]** をクリックすると、**[カスタム構成の作成]** ページが表示されます。
4. 構成の名前を入力します。
5. Windows OSアイコンをクリックします。
6. インターフェイスにSyncMLをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックしてファイルを指定し、デバイスへのアップロードを選択します。

   Ivanti Neurons for MDM は、ファイル内のコードのバリデーションチェックを実行しません。

7. **[次へ]** をクリックします。

カスタムSyncMLログ

Windowsデバイスに送信されたSyncMLコマンドと、これらのコマンドに対するデバイスからのSyncML応答は、[デバイスログ] タブで確認できます。このログ情報は、**WindowsカスタムSyncML**構成を送信した後で利用可能になります。システムがカスタムSyncML構成を送信した場合、この構成のステータスは、SyncML応答に関係なく、デバイスのその構成の [構成] タブ上では常に [インストール済み] になります。

ホーム画面レイアウト構成

ホーム画面レイアウト構成により、ホーム画面のアプリ、フォルダー、Webクリップのレイアウトが定義されます。

このセクションは以下のトピックを含みます。

- 「ホーム画面レイアウト構成の定義」下
- 「ホーム画面レイアウト構成の設定」次のページ

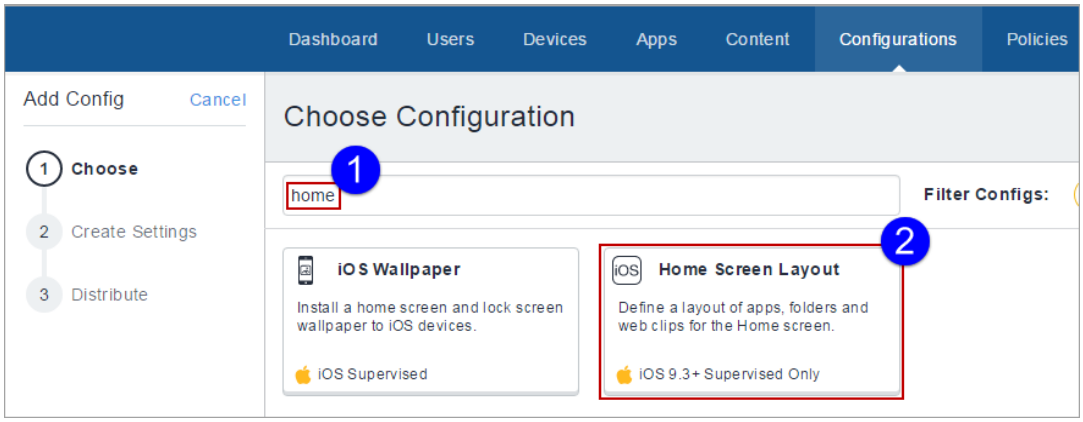
ライセンス: Silver

対象デバイス: iOS 9.3+監視対象のみ

ホーム画面レイアウト構成の定義

手順

1. **[構成]** を開き、**[+追加]** をクリックします。
2. 検索フィールドに「home」と入力し、**[ホーム画面レイアウト]** 構成をクリックします。ホーム画面レイアウト構成の詳細ページが開きます。

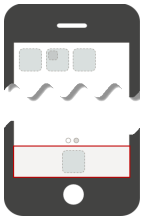


3. このページで設定を構成します。参考値は、ホーム画面レイアウト構成の設定セクションの表をご覧ください。
4. **[次へ]** をクリックして配布設定を行います。共有iPadデバイスの場合は、**[デバイス]** チャネルまたは **[ユー**

ザー] チャネルを選択します。詳細については、「構成の操作」ページ424をご参照ください。

5. **[完了]** をクリックします。

ホーム画面レイアウト構成の設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ドック	[+] アイコンをクリックして、この図でハイライトされているホーム画面のドックにアプリまたはWebクリップを追加した後、画面に表示される指示に従ってください。  Appleバンドル ID(「com.apple」で始まります) を入力することで、システムアプリを手動で追加できます。たとえば、「Files」アプリを追加する場合は「om.apple.DocumentsApp」と入力します。
ページ1	⊕ をクリックし、アプリまたはWebクリップを以下の図でハイライトされているホーム画面のページ領域に追加した後、画面に表示される指示に従ってください。

設定	操作内容
	 [ページを追加]をクリックして、電話表示に別のページを追加できます。

アプリ制御構成：デバイスごとにインストールするアプリを制御

アプリ制御構成により、アプリをデバイスレベルで許可リストまたはブロックリストに分類できます。すでにインストールされているアプリは非表示になり、起動できなくなります。App Storeには引き続きアプリが表示されますが、ダウンロードや起動はできません。この構成が配布されたすべてのデバイスはこの構成を使用し、許可されたアプリポリシー設定を無視します。この構成は、対象デバイス上で同じアプリに関連するアプリ関連ポリシーすべてに優先します。

この構成は、対象デバイス上で同じアプリに関連するアプリ関連ポリシーすべてに優先します。Windows 10デバイスの場合、制限がデバイスレベルで生じるため、アプリルールを実行するには構成が唯一の方法です。

アプリ制御構成によって作成できるもの:

- **許可リスト：**明示的にこのリストに追加されたアプリのみ許可します。他のアプリはデバイスにインストールできません。
- **ブロックリスト：**指定したアプリのインストールを禁止します。

サポートされるデバイス

アプリ制御構成により、以下のデバイスで各種アプリをブロックリストまたは許可リストに分類できます。

- 会社所有デバイス上のAndroid仕事用プロファイル
- iOS 9.3+監視対象のみ
- tvOS 11+
- Windows

アプリ制御構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします
3. 表示された**[構成を選択]**フィールドに**[アプリ制御]**と入力し、**[アプリ制御]**構成を選択します。

4. 構成の名前と説明を入力します。
5. OSを選択し、使用しているOSに該当するセクションの指示に従います。

会社所有デバイス上のAndroid仕事用プロファイル

ユーザーは最大50件のアプリケーションIDを許可リストまたはブロックリストのグループに追加できます。

手順

1. **[個人用アプリの許可リストを作成]** または **[個人用アプリのブロックリストを作成]** を選択し、許可リストまたはブロックリストに入れるアプリケーションのリストを追加します。
2. アプリケーションID(com.example.com) を入力し、**[追加]** をクリックします。
3. **[次へ]** をクリックし、配布オプションを選択します。
4. **[完了]** をクリックします。

iOS 9.3監視対象デバイス

手順

1. 許可リスト、ブロックリストのいずれを作成するかを選択します。
2. **[アプリを追加]** をクリックします。
3. 次のタブのいずれかまたは両方をクリックすることによって、許可リスト化またはブロックリスト化するアプリを選択します。
   - **[ルックアップで追加]** をクリックしてApp Storeまたはアプリカタログからアプリを検索および選択します。
   - Appleシステムアプリの場合のみ、**[手動で追加]** をクリックし、AppleバンドルIDを入力してアプリを選択できます。
4. **[許可リスト]** または **[ブロックリスト]** タブをクリックすると、許可リスト化またはブロックリスト化するよう選択したアプリのリストが表示されます。
5. (任意) **[すべてのWebクリップを含める]** オプションを選択します。
6. **[次へ]** をクリックし、配布オプションを選択します。
7. **[完了]** をクリックします。

Windowsデバイス

手順

1. **[許可]** または **[禁止]** を選択し、許可リストまたはブロックリストに分類するアプリケーションのリストを追加します。
2. **[ルールの定義]** セクションでリストから **[アプリの種類]** を選択します。
3. **[アプリ識別子]** ボックスに識別子名を入力し、具体的なアプリを検索します。または **[ルックアップアプリ]** リンクから新しいダイアログを開き、Windows専用のアプリ識別子を検索します。
4. (任意) **[アプリの説明]** ボックスにアプリの説明を入力します。
5. **[+追加]** リンクを使用し、アプリを許可リストまたはブロックリストに分類するルールの定義を追加します。
6. **[次へ]** をクリックし、配布オプションを選択します。
7. **[完了]** をクリックします。

アプリ通知構成

選択したアプリからユーザーが通知を受け取る方法を選択します。

対象：iOS 9.3+監視対象デバイス。

アプリ通知構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに[通知]と入力し、**[アプリ通知]**構成をクリックします。アプリ通知の[構成設定]ページが表示されます。
4. 構成の名前と説明を入力します。
5. アプリストアで検索するか、バンドルIDを入力して手動でアプリを追加します。
6. アプリ通知設定を適用するアプリを選択します。

7. 通知設定を構成します。選択できる通知は次のとおりです。
    - 通知を許可
        - 通知センターに表示
        - サウンド
        - バッジアプリアイコン
        - ロック画面に表示
        - (iOS 12.0+監視対象) CarPlayを使用する際に重要なアラートを表示
        - (iOS 12.0+監視対象) 重要なアラートの起動を許可(「おやすみモード」を無視)
    - 警告スタイルのロックを解除
        - バナー
        - モーダル警告
        - なし
    - (iOS 12.0+監視対象) グループ化の種類
        - 自動
        - アプリ別
        - オフ
    - (iOS 14.0+) 通知プレビューの種類 - デバイスの通知メッセージプレビューに表示するプレビューの種類を選択します。
        - ユーザー制御 - デバイス上のアプリのユーザー設定に従ってメッセージプレビューを表示します。
        - 常時 - メッセージプレビューを表示します。
        - ロック解除の場合 - デバイスのロックが解除されている場合のみメッセージプレビューを表示します。
        - 表示しない - アプリは [通知] にメッセージプレビューを表示しません。
8. **[次へ]** をクリックして配布設定を行います。
9. **[完了]** をクリックします。

詳細は構成を作成するにはを参照してください。

構成のエクスポート

サポートが診断に利用できるよう、構成ファイルをエクスポートして送信します。YAML形式ファイルで構成ファイル1つをエクスポートすることも、.zipファイルですべての構成をエクスポートすることも可能です。

手順

エクスポートの構成

エクスポートしたい構成に応じて、[構成] ページの異なる領域にある複数のファイルをエクスポートできます。

すべての構成をエクスポート：

1. **[構成]** に進みます。
2. 該当するチェックボックスにチェックを入れて、特定の構成を選択します。
3. **[アクション]** > **[選択した構成と詳細をエクスポート]** をクリックします。すべての構成をエクスポートする場合は、**[すべての構成と詳細をエクスポート]** を選択します。

   YAMLファイル群がZIPファイルに含まれます。レポートには選択したスペース内の既存の構成すべての詳細が含まれます。

カスタマイズした構成のエクスポート：

1. **[構成]** に進みます。
2. **[+追加]** をクリックして構成を選択します。
3. 次の手順で構成をカスタマイズします。
4. **[次へ]** をクリックします。
5. 配布レベルを選択します。
6. **[完了]** をクリックします。
7. **[構成]** ページのリストから作成した構成を選択します。
8. **[アクション]** プルダウンメニューをクリックし、**エクスポート**。
   構成名と_yyyymmdd.yamlというタイムスタンプのファイルがデバイスにダウンロードされます。

既存の構成をエクスポート：

1. **[構成]** に進みます。
2. 既存の構成を選択します。
3. **[アクション]** プルダウンメニューをクリックし、**[エクスポート]** をクリックします。
   構成名と_yyyymmdd.yamlというタイムスタンプのファイルがダウンロードされます。

構成の優先度決定

構成で複数のデバイスグループを選択する場合、同じタイプの複数の構成が特定のデバイスに割り当てられる場合があります。同じタイプの構成が同じデバイスに適用されると、定義された優先度によって、適用される構成が決定されます。最も優先度の高い構成の数字が最も小さくなります。たとえば、優先度が1001の構成は、優先度が1002の構成よりも優先度が高いということになります。サービスによって数字は自動的に割り当てられます。

Wi-Fi優先度はデバイスに適用されず、優先度から除外されます。

このオプションは、ページに同じ種類の構成が複数あり、ドロップダウンリストで1つのスペースが選択された場合のみ使用できます。構成の優先度を変更できます。

手順

1. **[構成]** に進みます。
2. 構成を選択しない状態で、**[アクション] > [構成の優先度決定]** を選択します。

   [アクション] が表示されない場合、優先度を必要とする複数の構成は存在しません。
3. 矢印を使用して構成を移動し、最も優先すべき構成が最上部にくるようにします。

   鍵のアイコンは、構成内のすべてのデバイスの配布設定を編集しない限り、構成の優先度を変更できないことを示します。
4. **[保存]** をクリックします。

   最大400の構成の優先度を設定できます。

[構成] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です:

- デバイス管理
- デバイス読み取り専用

構成の管理

このセクションは以下のトピックを含みます。

- 「AppConnect構成」ページ476
- 「セキュリティ構成」ページ480
- 「ユーザーリソース構成」ページ726
- 「エンタープライズネットワークアクセス構成」ページ759
- 「セルラー」ページ876
- 「その他の構成」ページ882

構成のタイプ

このセクションは以下のトピックを含みます。

- 「構成の検索」下
- 「セキュリティ」次のページ
- 「ユーザリソース」ページ463
- 「エンタープライズネットワークアクセス」ページ466
- 「セルラーネットワーク」ページ468
- 「その他の構成」ページ469
- 「デバイス同期構成」ページ469

構成の検索

[構成の選択] ページで検索およびフィルタ機能を使用して、適用する構成を検索します。

手順

1. **[構成]** を選択します。
2. リストから構成を選択するか、**[+追加]** ボタンをクリックします。

   [構成を選択] ページが表示されます。
3. リストから構成を選択するか、以下を実行します。
   - 検索ボックスに構成名を入力する
   - 検索ボックスの右にあるフィルターアイコンをクリックし、プラットフォームに適合する構成の種類を表示させる
4. 構成ボタンをクリックし、構成設定オプションにアクセスします。

詳細については、「構成の操作」ページ424をご参照ください。

セキュリティ

種類	操作内容	これらのデバイスの場合	必要なライセンス
Android Enterprise	Android Enterpriseオプションを指定します。	Android Enterprise	Silver
AppConnectデバイス	デバイスでセキュリティ設定 AppConnect 対応のアプリを指定します。	• [Android] • iOS	Gold
Azure Active Directory(Azureテナント)	Ivanti Neurons for MDM を Azure Active Directory に接続すると、管理対象のデバイスのデバイスコンプライアンスステータスを使用して、Microsoft 365アプリへの条件付きアクセスが可能です。	• iOS • Android	• 新規のユーザー: Secure UEM Premium • 既存のユーザー: Platinum
証明書	サーバーとの信頼を確立します。	• Android • iOS • macOS	
「証明書の透明性」ページ506	デバイスプロファイルに一度だけ表示される証明書の透明性適用を制御します。	• iOS • macOS • tvOS	
デバイスログ	ネットワークログとセキュリティログなどの追加のログをデバイスから取得します。	• Android Enterprise	
Android暗号化	は暗号化を開始するようにユーザーに指示します。	[Android]	

種類	操作内容	これらのデバイスの場合	必要なライセンス
暗号化DNS	VPNを設定せずにセキュリティの強化が可能です。	• iOS • macOS	Gold
MobileIron Threat Defense	デバイス、ネットワーク、アプリケーションに影響を与えるモバイル脅威や脆弱性からマネージドデバイスを保護します。	• Android • iOS	
Threat Defense ローカルアクション	Threat Defenseを有効化したクライアントが脅威を検出した際、サポート対象のAndroidデバイスに実行するローカルアクションをデバイス構成で定義し、配布します。	[Android]	
FileVault 2	ボリュームのコンテンツに完全なXTS-AES 128ディスク暗号化を実行できます。	macOS	Gold
FileVaultリカバリキー	FileVaultリカバリキーを企業サーバーにリダイレクトするための設定を決定します。	macOS	Gold
ID証明書	• サーバーに対してデバイスを認証します。 • ネットワークリソースに対してデバイスを認証します。	• [Android] • iOS • macOS	

種類	操作内容	これらのデバイスの場合	必要なライセンス
iOS iOSアクティベーションロック	監視対象デバイス上のAppleアクティベーションロック機能を有効にします。	iOS	Silver
iOSカスタム構成	各アプリが作成したiOS構成プロファイルを配布します。	iOS	
iOSの制約	• デバイスの機能をロックダウンします。 • デバイスの機能を有効にします。	iOS	
会議室ディスプレイ	Apple TVで会議室ディスプレイモードをオンにします。	tvOS 10.2以上	
ロックダウン＆キオスク：Android	• デバイスの機能をロックダウンします。 • デバイスの機能を再度有効にします。 • キオスク機能を適用します。	[Android]	
ロックダウン＆キオスク：Android Enterprise	• Androidエンタープライズで制限する機能やアプリを定義します。 • キオスク機能を適用します。	Android 5.0 +	

種類	操作内容	これらのデバイスの場合	必要なライセンス
ロックダウン＆キオスク：Samsung Know Standard	• Samsung Knox Standardデバイスで制限する機能やアプリを定義します。 • キオスク機能を適用します。	Samsung Knox	
macOSのファイアウォール	macOSデバイスのセキュリティ設定画面からアクセス可能なアプリケーションファイアウォールの設定を管理します。 管理者は、pingコマンドによって発見されないデバイスを指定することにより、ステルスモードを有効化できます。	macOS 10.12+	Gold
macOSの制約	macOSデバイスで有効な制約を決定します。	macOS	Gold
macOS AppStoreの制約	macOS AppStoreで有効にする制約を決定します。	macOS	Gold
macOSディスク焼き付けの制約	macOSでのディスク焼き付けの制約を管理します。	macOS	Gold

種類	操作内容	これらのデバイスの場合	必要なライセンス
macOS対応Mobile@Work	macOS対応Mobile@Workの実行ルールを作成し、配布します。	macOS	Gold
macOS対応Mobile@Workスクリプト	macOS対応Mobile@Workに配布するスクリプトを作成します。	macOS	Gold
「ID設定」ページ642	同じプロファイルに含まれるIDペイロードを参照するユーザーのキーチェーン内のID設定項目を特定します。	macOS	Gold
「証明書設定」ページ637	同じプロファイルに含まれる証明書ペイロードを参照するユーザーのキーチェーン内の証明書設定項目を特定します。	macOS	Gold
許可メディアの制御	物理メディアのマウント、アンマウントおよび取り出しオプションを構成します。	macOS	Gold
macOS Finder設定	macOSでのFinderアプリの設定を管理します。	macOS	Gold
macOSカーネル拡張ポリシー	ユーザーが承認したカーネル拡張の読み込みの制約と設定を制御します。	macOS	Gold

種類	操作内容	これらのデバイスの場合	必要なライセンス
「Active Directory (macOS)」ページ 638	認証とセキュリティを Active Directory(AD) に依存するソフトウェアサービスにアクセスするには、macOSデバイスをADドメインにバインドする詳細オプションを構成します。	macOS	Gold
「Office 365自動アカウント作成 (macOS)」ページ 644	ユーザー情報とオプションを構成し、すべての Microsoft Office 365 アプリについて初期構成を設定します。	macOS	Gold
Appleアプリカタログ	は、Web クリップ経由で Apple アプリカタログへのアクセスを管理します。	• iOS • macOS	Silver
マネージドドメイン	信頼できる電子メールおよび Web ドメインを指定します。	• iOS 8+	
パスコード	• パスコードを必須にします。 • パスコードの長さと内容を指定します。 • パスコードの要件を変更します。	• [Android] • iOS • macOS	
「プライバシー設定 (macOS)」ページ 656	どのアプリがシステムサービス、システムファイル、およびシステムリソースにアクセスするのを許可するかを構成します。	macOS	Gold

種類	操作内容	これらのデバイスの場合	必要なライセンス
認証	クラウドサービス/デスクトップログインのパスワードレス認証を提供します。	• macOS • Windows	
「プライバシー構成」ページ661	ローカルデータが収集されるかどうかを指定します。	• iOS • [Android] • Windows	
「クライアントプライバシーステートメント情報」ページ667	Go クライアントでユーザーにプライバシーポリシーを表示します。	• [Android] • Androidエンタープライズ • iOS	
「クライアントプライバシー」ページ660	MixPanel経由でデータを収集するよう構成します。データには、問題を解決して高品質のサービスを維持するためのデバイス情報と使用情報が含まれます。	• iOS • macOS	
ソフトウェア更新	OS 更新のルールを作成して配布します。	• iOS • macOS • Windows	
「タイムサーバー」ページ677	デバイスがカスタムタイムサーバーに接続するのを許可します。	macOS	Gold
Webコンテンツフィルター	Safariコンテンツをコントロールします。	監視対象 iOS 7	Silver

種類	操作内容	これらのデバイスの場合	必要なライセンス
Windows情報保護	企業データを保護するためのWindows情報保護(WIP)設定を定義します。	Windows 10以上	Gold
Windowsの制約	Windows Phoneデバイスで利用できる機能を決定します。	Windows Phone	

ユーザリソース

種類	操作内容	これらのデバイスの場合	必要なライセンス
CalDAV	• CalDAVサーバーへのアクセスを設定します(Googleカレンダーなど)。	• iOS	
CardDAV	• CardDAVサーバーへのアクセスを設定します(Googleコンタクトなど)。	• iOS	
Eメール	• POP/IMAP Eメールへのアクセスを設定します(Gmailなど)	• iOS	
Exchange	• Android/iOSモバイルデバイスでActiveSyncベースのEメール(Outlookなど)へのアクセスを設定します。 • macOSデバイスでExchange Web Services(EWS)ベースのEメールを設定します。 • デバイスへの同期頻度を定義します • Eメールのセキュリティを定義します	• [Android] • iOS • macOS	• Sentry経由のExchangeはmacOSではサポートされていません。 • 同期の経過日数のメールフラグはmacOSには該当しません。

種類	操作内容	これらのデバイスの場合	必要なライセンス
Google	• iOS 9.3.2+デバイスをGoogleアカウントに接続するGoogleアカウント構成を作成します。 • Googleシステム内の連絡先に電話をかけるときに使用するアプリを指定します。	• iOS	
フォント	• ドキュメントを正しく表示するために必要な標準外のフォントをインストールします	• iOS	
署名済みカレンダー	• インターネットカレンダーの署名を設定します	• iOS	
Webクリップ	• Webページへのショートカット(アイコン)を表示します	• iOS • macOS	
コンテンツキャッシュ	• コンテンツキャッシュサービスによりApp Storeソフトウェアのローカルコピーを許可します。 • 連携したクライアントでのソフトウェア/アプリダウンロードを高速化します。	• macOS	

エンタープライズネットワークアクセス

種類	操作内容	これらのデバイスの場合	必要なライセンス
AirPlay	• メディアを表示する別のデバイスへのアクセスを設定します	• iOS • macOS	Silver
AirPrint	• 無線印刷を設定します	• iOS • macOS	Silver
Always-on VPN	• ユーザーの操作なしでVPNサーバーへのアクセスを設定します。	• Android 7.0+ • iOS 8+	• Androidエンタープライズ対応Gold • iOS対応Silver
デフォルトのアプリランタイム許可	• Androidエンタープライズデバイスに展開したアプリのランタイム許可構成を設定します。	• Android API 23+をターゲットとしてビルドされ、Androidエンタープライズデバイスで Android 6.0+を実行するアプリ	
教育	• リーダーおよびメンバー向けのApple Educationペイロードとclassroomアプリを構成します。	• 監視対象 iOS 9.3+	Gold
グローバルプロキシ	• プロキシサーバーにHTTPトラフィックを送るようにデバイスを設定します	• 監視対象の iOS 7	Silver

種類	操作内容	これらのデバイスの場合	必要なライセンス
LDAP	• 企業ディレクトリへのアクセスを設定します	• iOS	
トンネル	• defines a per-app VPN connection between a client and Sentry using Tunnel	• iOS 7+ • Windows 10+	
Bridge	• IT部門は、重要な機能を失うことなく、UEM上でWindows管理業務を現代化することができます。	• Windows 10+デスクトップ	Bridge ライセンス
macOSサーバー	• アカウントタイプと関連設定を構成したmacOSサーバーアカウントを定義します。これによりユーザーはサーバー上でファイル共有をアクティベートできます。	• iOS 10+	
Per-App VPN	• 特定のアプリとVPNサーバー間の接続を設定します	• iOS	Silver
シングルサインオン	• 指定された管理対象のアプリにおいてシングルサインオンを設定します	• iOS	
マルチユーザーセキュアサインイン	• Webクリップ経由で安全なマルチユーザログインを設定する	• iOS	

種類	操作内容	これらのデバイスの場合	必要なライセンス
VPN	• VPNサーバーへのアクセスを設定します	• [Android] • Windows • iOS • macOS	
VPNオンデマンド	• ドメイン、ホスト名などに基づきVPNサーバーへのアクセスを設定します。	• iOS	
Wi-Fi	• 無線ネットワークへのアクセスを設定します	• [Android] • Windows • iOS • macOS	

セルラーネットワーク

種類	操作内容	これらのデバイスの場合	必要なライセンス
APN	• デバイスのセルラーアクセスポイント名を設定します	• iOS	
セルラー	• セルラーネットワークアクセスを設定します	• iOS	
「iOS Telecomのプリセット構成」ページ880	• ローミング制限のデフォルト値を設定します • 個人ホットスポット制限のデフォルト値を設定します	• iOS	

その他の構成

種類	操作内容	これらのデバイスの場合	必要なライセンス
Apple TV	• Apple TVの言語とロケールを定義します	• 監視対象のiOS 7	Silver
デフォルトのデバイス名	• 変数を使用してデフォルトのデバイス名を定義します	• 監視対象のiOS 8	Silver
iOS壁紙	• ホーム画面をインストールし、画面背景をロックします	• 監視対象のiOS 7	Silver
macOS壁紙	• ホーム画面/ロック画面の壁紙をデバイスにインストールします。壁紙はユーザーが変更できますが、配布された壁紙はデバイスから削除できません。		任意
Single Appモード	• デバイスの、指定されたアプリの利用を制限します	• 監視対象のiOS 7	Silver
「関連付けられたドメイン構成」ページ 883	• 関連付けられたドメイン構成は、アプリを関連付けられたドメインにマッピングするディクショナリです。 • 関連付けられたドメインは、拡張可能アプリSSO、ユニバーサルリンク、パスワード自動入力などの機能とともに使用できます。	macOS 10.15+	Gold

デバイス同期構成

デバイス同期設定では、デバイス上で監視できるリストデータポイントが提供されます。デバイス同期構成は編集できません。チェックした設定の一覧を表示できます。

手順

1. **[構成]** に進みます。
2. **[デバイス同期構成]** をクリックします。**[デバイス同期構成]** ページの [詳細] タブに選択された項目の一覧が表示されます。

設定	読み取り間隔の分数
証明書リスト	
デバイス情報	60
インストール済みアプリのリスト	60
マネージドアプリリスト	60
プロファイルリスト	60
プロビジョニングプロファイルリスト	60
制限	60
セキュリティ情報	60
iOS 9+	
更新を確認	1440

関連トピック

- 変数
- 「構成の操作」ページ424

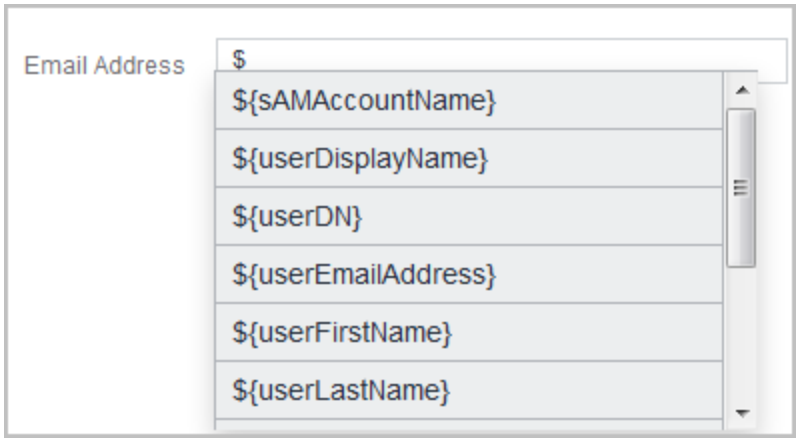
変数

特定の構成フィールド内で変数を利用し、任意のユーザーに特有の値を示すことができます。変数をサポートしているフィールドで $ を入力すると、サポートされている変数のリストが表示されます。このセクションは以下のトピックを含みます。

- 「サポートされているユーザ アカウント変数」下
- 「サポートされているデバイス変数」ページ473

サポートされているユーザ アカウント変数

ユーザ変数

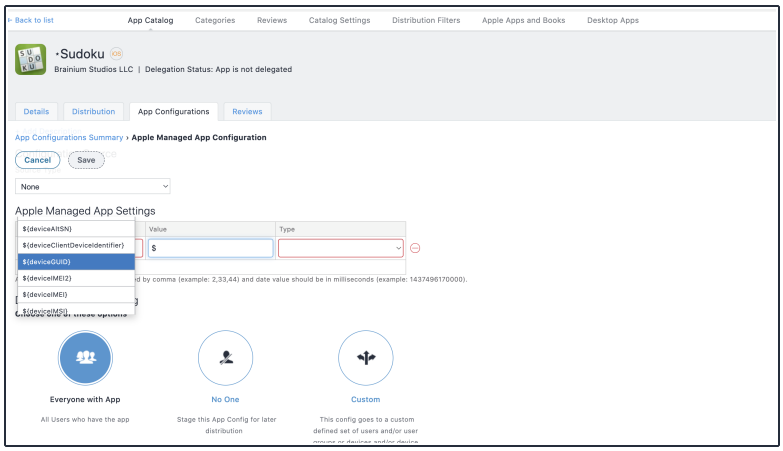


変数キー	値の説明
${department}	部署属性 (Active Active Directory が必要)
${edipi}	説明なし
${managedAppleId}	ユーザーの管理対象 Apple ID
${sAMAccountName}	sAMAccountName 属性 (Active Directoryが必要)
${userCN}	識別名から共通名 (CN) 属性を抽出 (LDAP が必要)
${userDisplayName}	表示名
${userDN}	識別名 (LDAP が必要)
${userEmailAddressDomain}	メールアドレスのドメイン部分 (@の後)
${userEmailAddressLocalPart}>	メールアドレスのローカル部分 (@の前)
${userEmailAddress}	メールアドレス
${userFirstName}	名
${userLastName}	姓
${userLocale}	ロケール
${userOU}	識別名から組織ユニット (OU) 属性を抽出 (LDAP が必要)
${userREALM}	Kerberos領域情報 (Active Directoryが必要)
${userUIDDomain}	ログインIDのドメイン部分 (@の後)
${userUIDLocalPart}	ログインIDのローカル部分 (@の前)
${userUID}	ログインID(メールアドレス形式)
${userUPN}	userPrincipalName属性 (Active Directoryが必要)

サポートされているデバイス変数

デバイス変数を使用して、モバイルデバイスに関する情報を指定します。

デバイス変数



変数キー	値の説明
${clientLastCheckin}	クライアントの最後のチェックイン日(MDMまたはクライアントの直近のチェックイン)
${deviceAltSN}	代替シリアル番号
${deviceClientDeviceIdentifier}	クライアントアプリケーションに使用される識別子
${deviceGUID}	グローバルで一意のデバイス識別子
${deviceIccIdentifier}	説明なし
${deviceIMEI2}	IMEI2
${deviceIMEI}	IMEI
${deviceIMSI}	IMSI
${deviceLastCheckin}	デバイスの最後のチェックイン日(MDMまたはクライアントの直近のチェックイン)
${deviceMdmChannelId}	内部デバイス識別子
${deviceMdmDeviceIdentifier}	MDMに使用される識別子
${deviceMEIdentifier}	説明なし
${deviceModel}	機種
${deviceName}	デバイス名
${devicePhoneNumber}	デバイス電話番号
${devicePK}	クラスタ固有のデバイス識別子
${deviceSN}	シリアル番号
${deviceUDID}	iOS UDID
${deviceWifiMacAddress}	Wi-Fi MACアドレス

メールテンプレート変数

変数キー	値の説明
${policyMessageContent}	説明なし
${policyMessageTitle}	説明なし

タイムスタンプ変数

変数キー	値の説明
${timestampMS}	現在のタイムスタンプ(UNIXエポックからのミリ秒数)

ポリシーテンプレート変数

変数キー	値の説明
${nameOfPolicy}	侵害されたポリシー名
${nextAction}	メッセージ送信後に実行される次の階層型コンプライアンスアクション(待機および撤去とは異なる)
${nonComplianceTime}	デバイスがコンプライアンス違反状態の日数
${policyViolationFirstTime}	ポリシー違反が最初にトリガーされた時のタイムスタンプ(UTC DD-MM-YYYY形式)
${ruleConditions}	ルール定義(今表示されているとおりのクエリ文字列)

関連トピック:

- 「属性」ページ1044

AppConnect構 成

このセクションは以 下 のトピックを含 みます。

AppConnectの概要

ライセンス: Gold

AppConnectは、iOSおよびAndroidデバイス上のデータを保護するためにアプリをコンテナ化する機能です。AppConnectが対応するアプリはそれぞれセキュアなコンテナになり、そこに含まれるデータの暗号化、不正アクセスからの保護、および削除を可能にします。各ユーザーは様々なビジネスアプリを持っているため、アプリのコンテナごとにその他のアプリのセキュア・コンテナに接続されます。このコネクションを通じて、AppConnect対応アプリはドキュメントなどのデータを共有できるようになります。Ivanti Neurons for MDM は、ポリシーを使用してAppConnect対応アプリを管理します。

AppConnectの詳細とAppConnectアプリの設定および展開方法については、*「Ivanti Neurons for MDM のためのAppConnectガイド」*を参照してください。

セキュアアプリのステータス

[デバイス] > **[デバイス]** ページから **[概要]** ページを表示したいデバイスをクリックします。このページではユーザーがセキュアアプリのステータスと以下の情報を確認できます。

- **セキュアアプリのステータス** - AppConnectが有効か無効かを示します。
- **セキュアアプリ暗号化のステータス** - AppConnectパスコードが有効か無効かを示します。
- **セキュアアプリ暗号化モード** - 暗号化モード(AES 256など) を示します。

これらのフィールドは以下としても使用できます:

- ユーザーがデバイスの検索/絞り込みを行う際に表示されるデバイスエントリを絞るためのフィルター(左ペイン) 。
- 動的管理デバイスを作成するときのルール。
- 定義されたルールに従ってアプリを配布するデバイスを絞り込むため配布フィルター。

管理者は、各セキュアアプリのコンテナポリシーと構成ステータス(インストール済み、適用済み、送信済み、インストール保留) をデバイス詳細ページの **[構成]** タブで確認できます。

AppConnectパスコード

このセクションは以下のトピックを含みます。

- 「パスコードの変更/リセット」下
- 「iOSデバイス用のセキュアアプリパスコードをリセットするワンタイムPINの生成」次のページ

AppConnectパスコードを要求することができます。これは、セキュアアプリパスコードとも呼ばれます。AppConnectパスコードによるシングルログインでは、デバイスユーザーがすべてのセキュアアプリにアクセスできます。管理ポータルで、AppConnectパスコードのルールを構成できます。AppConnectパスコードは、デバイスのロックを解除するためのパスコードとは異なります。

パスコードの変更/リセット

ユーザーはAndroidデバイス対応のSecure Apps ManagerアプリおよびGo for iOSアプリでセキュアアプリパスコードを変更またはリセットできます。ただし変更やリセットがAppConnect構成で許可されている場合に限ります。iOSデバイスの場合:

手順

1. Go for iOSアプリを開きます。
2. **[セキュアアプリ]** をクリックします。
3. **[認証]** をクリックします。
4. **[セキュアアプリパスコードを変更]** をクリックし、指示に従ってパスコードを変更/リセットします。

Androidデバイスの場合:

1. Secure Apps Managerアプリを開きます。
2. オプションメニューから **[パスコードを変更]** をクリックします。
3. パスコードをリセットするには **[パスワードを忘れた]** をクリックします。

iOSデバイス用のセキュアアプリパスコードをリセットするワンタイムPINの生成

管理者はIvanti Neurons for MDMの構成により、パスコードを忘れたiOSデバイスユーザーによるセキュアアプリ(AppConnect)パスコードのリセットを許可することができます。このオプションを構成すると、ユーザー名とパスワードでIvanti Neurons for MDMに登録したデバイスユーザーは、その認証情報をiOS対応Go 3.1.0またはサポートされる以降のバージョンに入力して認証を受け、セキュアアプリパスコードをリセットできます。しかし、パスワードとPINを忘れたデバイスユーザーには別の認証方法が必要です。

手順

1. Ivanti Neurons for MDMで、管理者がiOS AppConnectデフォルト構成(または他のiOS AppConnect構成)の**[セキュアアプリパスコード]**オプションをオンにします。
2. ユーザーは、セルフサービスユーザーポータルで**[セキュアアプリパスコードをリセット]**オプションをクリックし、特定のiOSデバイス用のワンタイムPINを生成した後、以下の指示に従います。このワンタイムPINは30分間有効です。
3. デバイス上のGo for iOSで、忘れたセキュアアプリパスコードをリセットする指示に従います。
4. ユーザー認証情報を求められたときは、ユーザー名とワンタイムPIN(通常のパスコードの代わりに)を入力します。
5. これでユーザーのセキュアアプリパスコードがリセットされます。

セキュリティ構成

このセクションは以下のトピックを含みます。

- 「認証」ページ647
- 「Appleアプリカタログ」ページ649
- 「マネージドドメイン」ページ650
- 「パスコード構成」ページ651
- 「プライバシー設定(macOS)」ページ656
- 「クライアントプライバシー」ページ660
- 「プライバシー構成」ページ661
- 「クライアントプライバシーステートメント情報」ページ667
- 「ソフトウェア更新」ページ668
- 「セキュリティ設定の構成」ページ676
- 「タイムサーバー」ページ677
- 「Webコンテンツフィルター」ページ678
- 「Windowsファイアウォール」ページ683
- 「Windows情報保護」ページ688
- 「Windowsの制約」ページ695
- 「Windowsデスクトップ制約」ページ703
- 「Windows 10のデスクトップ設定」ページ706
- 「Windows Hello for Business構成」ページ711
- 「Play Integrity(旧称SafetyNet Attestation)」ページ713
- 「高度なAndroidパスコードおよびロック画面」ページ714
- 「Microsoft Defender for Endpoint」ページ722
- 「証明書ベースの認証」ページ723

Android Enterprise

ライセンス: Silver

Android Enterprise構成は、サポートされているデバイスに対して有効なAndroid Enterpriseオプションを定義します。各種デバイスグループに別の構成を作成することができるほか、デフォルト構成の編集のみで済ませることもできます。Android Enterpriseに対応しているデバイスの一覧については、Android公式ページを参照してください。

Android Enterprise 設定

設定	操作内容
名前	この構成を識別する名前を入力します。
説明	この構成の目的を明示する説明を入力します。
スクリーンキャプチャを無効化 (Android 5.0+)	デバイスがネイティブのスクリーンキャプチャ機能を使用できないようにする場合に選択します。
アプリ制御を無効化 (Android 5.0 +)	ユーザーが[設定]や[ランチャ]でアプリを変更できないようにする場合に選択します。
認証情報の構成を禁止 (Android 5.0 +)	ユーザーがユーザーの認証情報を設定できないようにする場合に選択します。
プロファイル間のコピー/貼り付けを禁止 (Android 5.0 +)	デバイスが他のAndroid Enterprise仕事用プロファイルにコピー/貼り付けできないようにする場合に選択します。
アカウント変更を禁止 (Android 5.0 +)	ユーザーがアカウントの追加や削除をできないようにする場合に選択します。
ビーム発信を禁止 (Android 5.0+)	ユーザーがNFCを使用したアプリデータの送信をできないようにする場合に選択します。
位置情報共有を禁止 (Android 5.0 +)	Webサイトとアプリがデバイスユーザーに位置情報の共有を指示できないようにする場合に選択します。

設定	操作内容
入力方法を制限 (Android 5.0+)	許可されたパッケージの名前のリストを指定することで、入力方法を制限する場合に選択します。許可リストに入れられたパッケージがない場合は、システムの入力方法のみが許可されます。入力方法は、仕事用アプリだけでなく、デバイス全体に対して制限されます。
アクセシビリティサービスを制限 (Android 5.0 +)	許可されたパッケージの名前のリストを指定することで、入力方法を制限する場合に選択します。許可リストに入れられたパッケージがない場合は、システムのアクセシビリティサービスのみが許可されます。入力方法は、仕事用アプリだけでなく、デバイス全体に対して制限されます。
発信者IDを無効化 (Android 6.0 +)	着信の際、仕事用プロファイルの発信者ID情報がデバイスに表示されるかどうかを設定します。

関連トピック

- Android Enterpriseの設定

既定の Android Enterprise 構成の編集

グローバル管理者は、スペース管理者がカスタムスペースで次の既定の Android Enterprise 構成の配布を編集することを許可できます。

- Android Enterprise：会社所有のデバイスの仕事用プロファイル(Android for Work)
- Android Enterprise：仕事用マネージドデバイス(Android for Work)
- Android Enterprise: 仕事用プロファイルを持つAndroidマネージドデバイス

上記の構成のいずれかの配布を編集する

手順

1. [構成] タブで編集する構成を選択します。
2. 編集アイコンをクリックします。
3. **[次へ]** をクリックします。
4. 次のいずれかの構成配布レベルを選択します。
   - すべてのデバイス: すべてのデバイスに構成を配布します。
     a. [配布の概要] セクションで [他のスペースにあるデバイスに適用] を選択します。
     b. [スペース管理者に配布の編集を許可] を選択します。
   - カスタム - この構成を送信する具体的なデバイスグループを定義してください。
     a. [デバイスグループ配布を定義] で、設定を配布したいデバイスタイプの横にあるチェックボックスを選択します。[デバイスグループを検索] 検索フィールドにデバイスグループ名を入力し、デバイスグループを検索することも可能です。
     b. [スペース管理者に配布の編集を許可] を選択します。
5. **[完了]** をクリックします。

この構成をスペースに適用する際、スペース管理者はカスタムスペースの配布アイコンをクリックすることで配布を編集できます。

Android Enterprise の設定

このセクションは以下のトピックを含みます。

ライセンス: Silver

Android Enterprise は Google が提供するプログラムであり、モビリティ管理者は次のことができるようになります。

- 仕事用データと個人用データの分離
- 企業アプリのセキュリティ確保と管理
- システムアプリの制御 (Camera、Galleryなど)
- Android Enterprise コンテナで一元的にアプリケーションをプロビジョニング、構成します。
- 情報漏洩 (スクリーンキャプチャ) の防止

Android Enterpriseを管理するUEMサーバーとしてIvanti Neurons for MDMを構成できます。Android Enterprise にはAndroid 3.0以上が必要です。Android Enterprise、デバイス所有者および管理対象プロファイル– 従業員所有の2つの構成がサポートされています。

サポートされるデバイス

Ivanti Neurons for MDM 現在サポートされているのは、Android 5.0を実行し、メーカーによってAndroid Enterpriseが有効化されているデバイス上のAndroid Enterpriseのみです。Android 5.0を実行しているデバイスでキオスクモードを使用するには、Android Enterprise が必要です。

前提条件

Googleにまだドメインを登録していない場合は、まずGoogleの以下のウェブサイト上でプログラムに登録する必要があります。

https://admin.google.com.

このプロセスでは以下を実行します。

- ドメインを取得する(ユーザーのEメールアドレスに一致するドメイン)
- トークンを受け取る
- JSONクライアントIDをダウンロードする

Ivanti Neurons for MDMでAndroid Enterpriseをセットアップする場合、両方の項目が必須です。

処理後、取得したドメインを所有することを証明する方法を記載したEメールをお送りします。

会社がすでに自社ドメイン名を使用してGoogle Apps for Workに登録している場合は、Android Enterpriseを有効化する方法についてhttps://support.google.com/work/android/answer/6174062をご覧ください。

Ivanti Neurons for MDMをAndroid Enterpriseに接続する

Android Enterpriseにサインアップした後、Ivanti Neurons for MDMをUEMサーバーとしてセットアップします。

Android Enterpriseの認証情報の入手

手順

1. **[管理] > [Android Enterprise]** に移動します。
2. **[Googleデベロッパーコンソール]** をクリックします。
3. 最初に表示されたリンクをクリックし、Googleデベロッパーコンソールに進みます。

4. ドロップダウンメニューから **[プロジェクトを作成]** を選択します。
5. プロジェクトの名前を入力します。
6. サービス利用規約に同意します。
7. **[作成]** をクリックします。
8. **API** をクリックします。
9. **[API]** を選択します。
10. 検索フィールドに**「emm」**と入力し、Google Play EMMを検索します。
11. **Google Play EMM API**リンクをクリックします。
12. **[APIを有効化]** をクリックします。
13. **[認証資格情報]** をクリックします。
14. **[サービスアカウント]** を選択します。
15. **[作成]** をクリックするとJSONファイルが保存されます。

Android Enterprise MDMトークンをIvanti Neurons for MDMに追加する

手順

1. https://admin.google.comにログインします。
2. **[セキュリティ]** をクリックします。
3. Android Enterprise設定が表示されない場合、**[詳細を表示]** をクリックします。
4. **[Android Enterprise 設定]** を選択します。
5. **[エンタープライズモビリティ管理プロバイダーの管理]** にMDMトークンをコピーします。
6. Ivanti Neurons for MDMポータルに戻ります。
7. **[完了]** をクリックします。
8. ボックス2で、コピーしたMDMトークンを貼り付けます。
9. **[ドメイン]** フィールドに、Googleで取得したドメインを入力します。
10. **[ファイルを選択]** をクリックし、ダウンロードしたJSONファイルをアップロードします。

11. **[接続]** をクリックします。
    接続に成功すると、**[Googleに接続]** というメッセージが表示されます。

12. ボックス3で、**[認証]** をクリックして、Ivanti Neurons for MDMにGoogleユーザーデータへのアクセスを付与することを示します。

13. **[承諾]** をクリックします。
    メッセージ「**ユーザーに接続**」がIvanti Neurons for MDMポータルに表示されます。

Ivanti Neurons for MDMとGoogleとの間でユーザーを同期させる

Android Enterprise を Ivanti Neurons for MDMIvanti Neurons for MDM で管理された Android ユーザに配布する前に、各ユーザには Google Admin Portal で対応するレコードが必要です。Ivanti Neurons for MDMと Google Admin Portalとの間でユーザー情報を同期させるために必要なステップは、組織のディレクトリサービス(AD/LDAP) との統合をセットアップ済みであるかどうかによって異なります。

Active Directory/LDAPユーザー

Ivanti Neurons for MDMとのAD/LDAP統合をセットアップ済みである場合は、Google Apps Directory Syncを使用して、Google Admin PortalとのAD/LDAP統合をセットアップする必要があります。詳細は、https://support.google.com/a/answer/106368?hl=enを参照してください。

ローカルユーザー

Ivanti Neurons for MDMでローカルユーザーのみを作成し、ディレクトリサービスと統合するつもりがない場合、それらのユーザーをGoogle Admin Portalと同期させるには、以下のステップを完了します。

手順

1. https://admin.google.comからGoogle管理ポータルにログインします。

2. **[ユーザー]** をクリックします。

3. 右下隅の **[ユーザーの追加]** または **[複数ユーザーの追加]** のアイコンをクリックします。

4. Android Enterpriseを使用するIvanti Neurons for MDMユーザーごとに、Ivanti Neurons for MDMユーザーと同じユーザー名およびEメールアドレスを使用して、Googleユーザーを追加します。

5. Google Admin Portalに追加したIvanti Neurons for MDMユーザーごとに、Ivanti Neurons for MDMポータルで以下のステップを行います。
   a. [ユーザ] タブでユーザ名リンクをクリックすると、ユーザの詳細情報が表示されます。
   b. **[Googleユーザーディレクトリとユーザーを同期]** を選択します。
   c. **[Googleユーザーディレクトリと同期]** をクリックします。
   d. Google ステータスが [有効] であることを確認します。

Android Enterprise をサポートされているデバイスに配布する

Android Enterprise を配布するには、次の2つの構成が必要です。

- Android Enterprise: 会社所有のデバイス構成の仕事用プロファイルは、Android Enterpriseを有効化します。
- ロックダウン & キオスク構成は、適用する Android Enterprise 制限を定義します。

登録したデバイスの撤去

BYOD シナリオでは、会社所有デバイスでデバイス管理者から Android Enterprise 仕事用プロファイルに移行する際に、デバイスを除却して再登録する必要はありません。デバイスのワイプや撤去は、デバイス管理者からデバイス所有者モードに移行する場合のみ必要です。

撤去アクションのデバイス所有者/拡張プロファイル所有者/会社所有の個人が有効化モードで登録されたデバイスを選択すると、「撤去コマンドは組織が所有するデバイスではサポートされていない」ことを示すポップアップが画面に表示されます。

デバイスの導入

手順

1. Ivanti Neurons for MDMポータルで **[構成]** を開きます。
2. **[Android Enterprise: 仕事用プロファイル]** をクリックします。
3. **[編集]** をクリックします。
4. **[次へ]** をクリックします。
5. **[すべてのデバイス]** または **[カスタム]** を選択します。
6. **[カスタム]** を選択した場合は、Android for Work設定を受信すべきデバイスグループを検索し、選択します。
7. **[完了]** をクリックします。
8. **[リストに戻る]**(左上) をクリックします。
9. **[+追加]** をクリックします。
10. **[ロックダウン & キオスク: Android Enterprise]** をクリックします。
11. **[名前]** フィールドに構成を識別するテキストを入力します。

12. **[ロックダウンの種類を選択]**で、**[仕事用プロファイル]** をクリックします。
13. 対象デバイスに適用したいロックダウン設定を選択します。
14. **[次へ]** をクリックします。
15. **[すべてのデバイス]** または **[カスタム]** を選択します。
16. [カスタム] を選択した場合は、Android Enterprise設定を受け取る必要があるデバイスグループを検索して選択します。
17. **[完了]** をクリックします。

導入後は、作成したプロファイルを変更できません。代わりに、新しいAndroid Enterprise構成を作成し、これを導入する必要があります。

導入の確認

Android Enterpriseが導入されたことを、以下の方法で確認できます。

- **[ユーザー]** > **[ユーザー]** からユーザーのエントリを探し、その**Googleステータス**が **[有効]** であることを確認します。
- **[デバイス]** > **[デバイス]** の下でデバイスのリンクをクリックしてから、**Android Enterprise** のステータスが **[有効]** であることを確認します。

ユーザーの**Googleステータス**は **[有効]** である必要があります。これが有効でなければ、ユーザーはデバイスを登録できません。

GSuiteを利用していない企業の場合、マネージドGoogle Playアカウントの方法を使用することで、ユーザーをAndroid Enterpriseに登録できます。Android Enterpriseがマネージド Google Playアカウントとしてセットアップされた場合は、Android Enterpriseデバイスが登録されるまで、ユーザーは **[Googleステータス: 有効化済み]** として表示されません。マネージド Google Playアカウントの詳細はマネージド Google Playアカウントをご覧ください。

Android Enterpriseアプリの導入

Android Enterprise用に開発されたアプリには、Ivanti Neurons for MDMを通じて構成できるオプションが含まれている場合があります。

手順

1. Ivanti Neurons for MDMポータルで、**[アプリ] > [アプリカタログ]**を開きます。
2. Google Playストアでアプリを検索します。
3. アプリのエントリをクリックします。
4. Android Enterpriseユーザーに代わって承認事項を承諾します。
5. **[次へ]** をクリックします。
6. 配信オプションを選択します。
7. **[詳細オプションとアプリ構成]** を展開します。
8. 次のガイドラインに従って、オプションに情報を入力します。

設定	説明
デバイスにインストール	登録後すぐにインストールを開始するには、このオプションを選択します。デバイスがSamsung Knoxデバイスで、以下のサイレントインストールオプションが選択されている場合を除き、ユーザーにアプリのインストールを確認するメッセージが表示されます。
エンドユーザーのアプリカタログでアプリを表示しない	ユーザーにデバイス上でアプリカタログを見せたくない場合に選択します。
Samsung Knoxデバイスにサイレントインストール	ユーザーにSamsung Knoxデバイスへのインストールを指示したくない場合に選択します。

設定	説明
アプリインストール優先度を設定	Android Enterpriseアプリの場合は、特定のアプリのダウンロードを他のアプリより優先させることができます。たとえばTunnelとメールアプリを、他の重要でないアプリの前にダウンロードするなどです。選択可能な優先度は以下のとおりです。 • **高** • **中**(デフォルト) • **低** この設定は、自社開発アプリ、公開アプリ、非公開アプリ、およびWebアプリに適用されます。自社開発アプリはクライアント経由、市販アプリと非公開アプリはGoogle経由でインストールされます。アプリの優先度は同じチャネルでインストールされたアプリにのみ適用されます。

設定	説明
Wi-Fiに接続したときのみインストール	これを選択すると、デバイスがWi-Fiに接続している場合のみアプリをインストールします。
充電中にのみインストール	これを選択すると、デバイスが充電中の場合のみアプリをインストールします。
アイドル状態のときのみインストール	これを選択すると、デバイスがアイドル状態のとき(ユーザーが特に何かに使用していないとき)のみアプリをインストールします。
インストール時に自動起動	インストール後、自動的にアプリを起動する場合に選択します。この機能はアプリがデバイス上に新しくインストールされた場合(バージョン更新ではなく)のみ使用可能です。

9. **[次へ]** をクリックします。
10. プロモーションオプションを選択します。
11. **[完了]** をクリックします。

ビジネスアプリの構 成

アプリカタログの[ビジネスアプリ] セクションで、次 のようなAndroid Enterpriseアプリを入 手 できます。

- 生 産 性 の分 割
- 電 子 メール+
- トンネル
- Gmail

Android Enterprise：仕事用マネージドデバイス非GMSモード(AOSP)

Ivanti Neurons for MDMは、仕事用マネージドデバイス非GMSモード(AOSP)デバイスのデバイス所有者登録を、Google Mobile Services(GMS)を必要とせずにサポートしています。これはシステム構成であり、管理者は構成を追加できません。管理者が配布または配布を停止することは可能です。

手順

1. ユーザ認証資格情報を使用して、Ivanti Neurons for MDM にログインします。
2. Android Enterprise：仕事用マネージドデバイス非GMSモード(AOSP)の**[構成を検索]**します。
3. 構成を編集し、適切なデバイスグループに配布します。たとえばAndroidデバイスです。
4. **[完了]**をクリックします。

仕事用マネージドデバイス非GMSモード(AOSP)の機能を完全に動作させるためには、Ivanti Neurons for MDMテナントでAndroid Enterpriseを有効にする必要があります。

Android仕事用本人確認

このセクションは以下のトピックを含みます。

- 「Android仕事用本人確認(Work Challenge)構成の作成:」下
- 「構成設定」ページ501

ライセンス: Silver

Android仕事用本人確認(Work Challenge)構成は、ユーザーが仕事用プロファイルのデータとアプリにアクセスするためのセキュアパスワードを設定します。Android Enterprise仕事用プロファイルが必要です。

実装上の注意:

- 管理者は、デバイスパスワードポリシーと仕事用プロファイルパスワードポリシーを独立して適用できます。

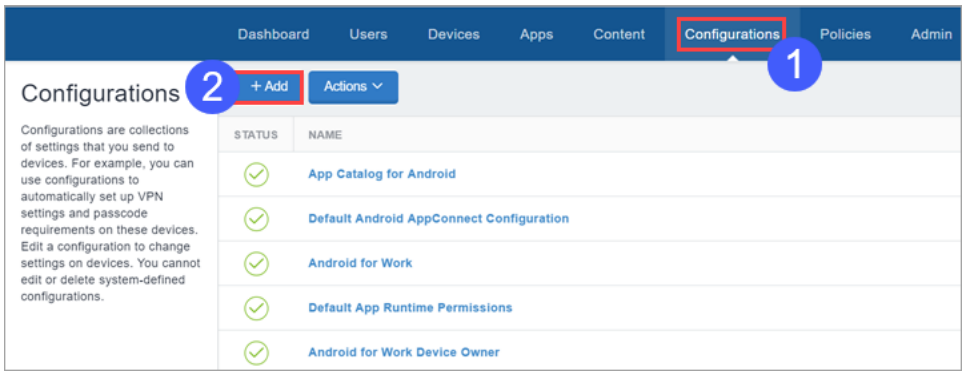
  Android 7.0より古いデバイスはこの機能をサポートしないため、それらにはIvanti Neurons for MDMはこの構成を送信しません。

- Ivanti Neurons for MDMは、Android Enterprise仕事用プロファイルがあるデバイスにのみ、この構成を送信します。

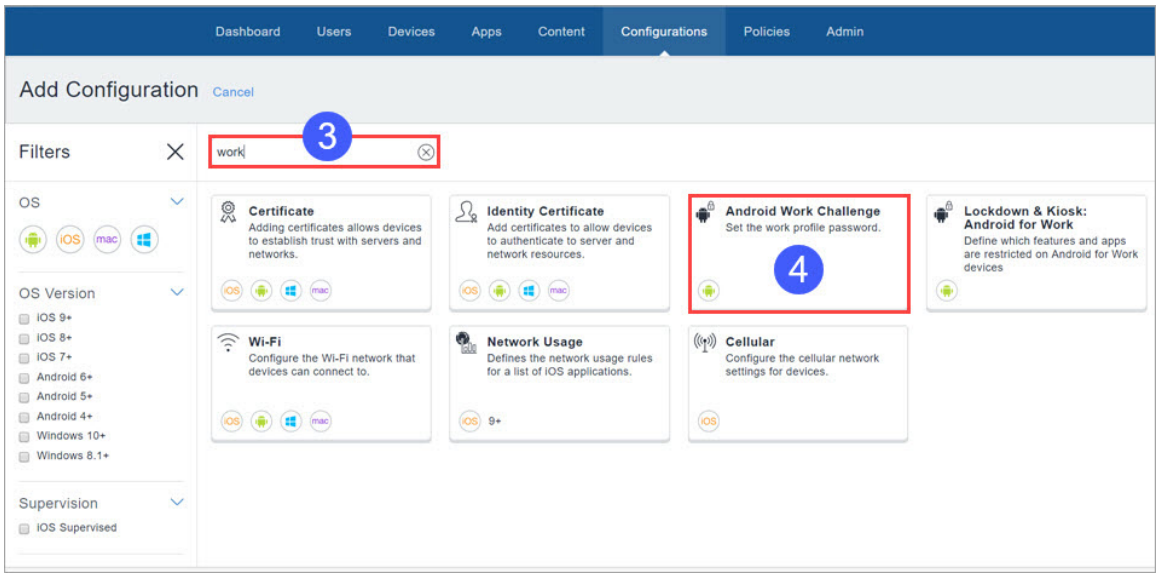
Android仕事用本人確認(Work Challenge)構成の作成:

手順

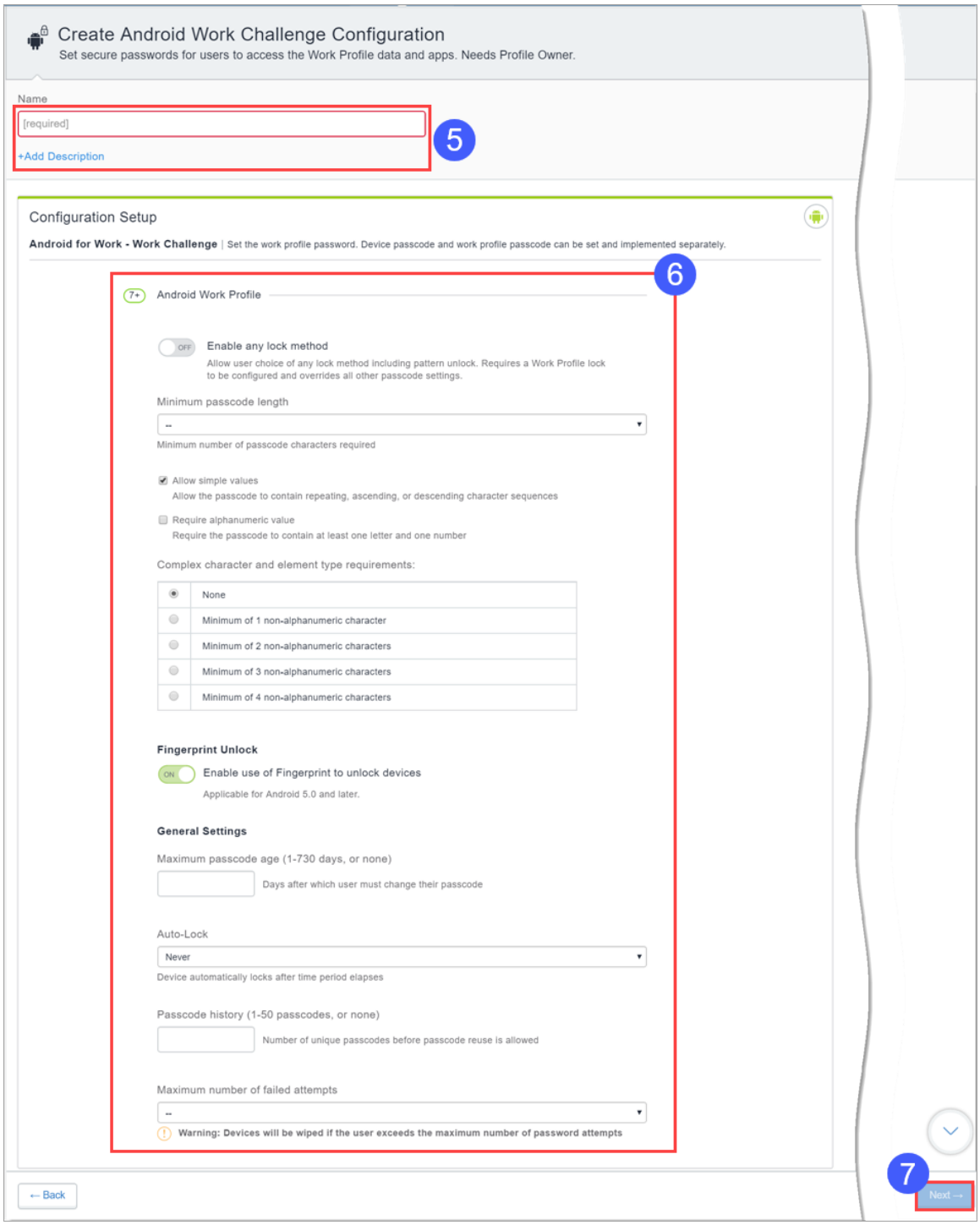
1. **[構成]**をクリックします。



2. **[+追加]**をクリックします。

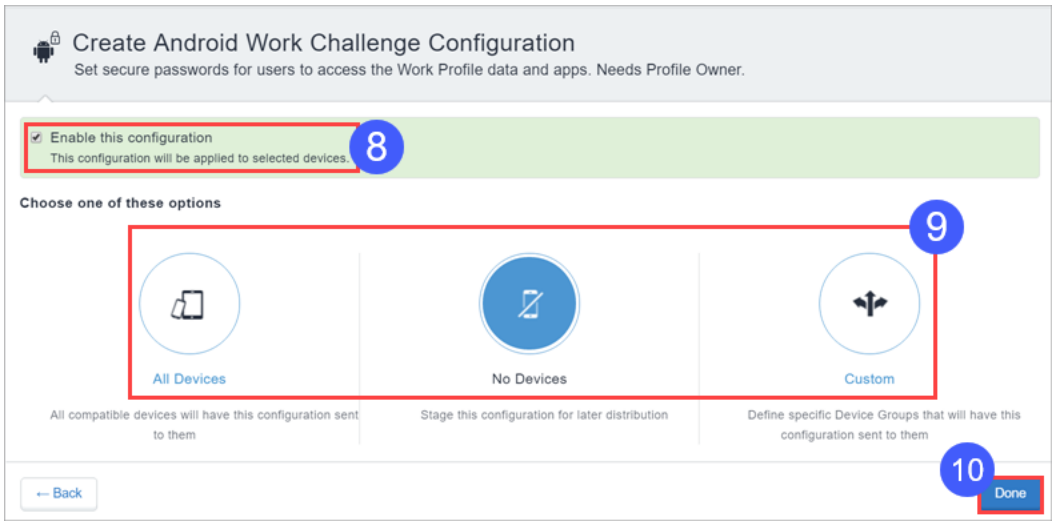


3. 検索フィールドに「仕事用(work)」と入力します。
4. **[Android仕事用本人確認(Work Challenge)]** 構成を選択します。



5. 構成名を入力し、必要に応じて説明も入力します。
6. 構成設定フィールドを使用して構成を作成します。設定の詳細は構成設定をご覧ください。

7. **[次へ ->]** をクリックします。



8. 必要であれば構成を有効化します。
9. すべてのデバイスに配布、カスタマイズしたデバイス群に配布、どのデバイスにも配布しない、のいずれかに配布設定を行います。
10. **[完了]** をクリックします。

構成設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
あらゆるロック方式を有効化	パターンロック解除を含め、あらゆるロック方式の選択をユーザーに許可します。他のすべてのパスコード設定をオーバーライド
パスコードの最小文字数	パスコードの最小文字数を4～16から選択します。
シンプルな値を許可	繰り返し、昇順または降順の文字列を含むパスコードを許可する場合に有効化します。

設定	操作内容
英数字の値が必要	パスコードに、アルファベット1つ以上と数字1つ以上を含める必要がある場合に有効化します。
複雑な文字と要素タイプ特性	以下のいずれかの複雑な文字と要素タイプの要件を設定します。 • なし • 英数字以外の文字が1文字以上 • 英数字以外の文字が2文字以上 • 英数字以外の文字が3文字以上 • 英数字以外の文字が4文字以上
指紋によるロック解除	ユーザーが指紋でデバイスのロックを解除できるようにする場合に有効化します。
パスコードの最大有効期間	パスコードの有効期間を0～730日から選択します。
オートロック	デバイスにオートロックがかかるまでの時間を選択します。0～15分から選択してください。
パスコードの履歴	パスコードをいくつ使用すれば再び同じパスコードを使用できるかを0～50から指定します。
入力失敗の最大回数	何回まで入力を失敗できるかを選択します。**警告：ユーザーによるパスワードの入力失敗回数がこの最大回数を超えた場合、Ivanti Neurons for MDMはそのデバイスをワイプします。**

証明書構成

証明書構成では、デバイスに配信される証明書を特定します。証明書により、デバイスはサーバーとネットワークリソースとの信頼を確立することができます。リリース76以降はv3の証明書のみサポートします。

管理者は、スマートカードログオンやカスタムオブジェクトID(OID) 用のIvanti Neurons for MDM 証明書を生成できるようになりました。以下の認証オプションに対応する証明書を生成可能です。

- クライアント認証 - デフォルトで有効
- IPSEC – 任意、管理者が有効化
- スマートカードログオン – 任意、管理者が有効化
- カスタムOID – 任意、管理者が有効化

この機能は以下の認証機関(CA) にのみ対応します:

- ローカル証明書機関
- 仲介認証機関
- 外部認証機関 - NDESサーバー内でCAテンプレートのアプリケーションポリシーを設定し、IPSEC、スマートカードログオン、カスタムOIDをサポートします。
- オンプレミスのSCEP認証機関

構成の配布

Ivanti Neurons for MDMリリース91以降、グローバル管理者は、すべてのデバイス向けおよびカスタム配布オプション向けの証明書構成の編集を、スペース管理者に委譲できるようになりました。証明書構成の場合、[この構成をすべてのスペースで利用可能にします] オプションを選択できます(任意) 。このオプションを選択すると、証明書構成をすべてのスペースで利用できるようになり、Exchange、Wifi、VPN、Per-App VPN、およびその他の適用可能な構成で使用できます。このオプションは、証明書構成を、個別の構成として配布するのではなく、関連する構成の一部として(デフォルト以外のスペースにある) デバイスに配布するだけでよい場合に使用できます。

手順

1. [名前] フィールドに名前を入力します。
2. 証明書ファイルをアップロードします。

3. **[次へ]** をクリックします。
4. **[この構成を有効化]** オプションを選択します。
5. 以下の配布オプションから1つ選択します。
   - **すべてのデバイス**。以下のオプションから1つ選択してください：
     - **他のスペースに適用しない**。
     - **他のスペースにあるデバイスに適用する**。
       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。
   - **デバイスなし**（デフォルト）
   - **カスタム**。以下のオプションから1つ選択します。
     - **他のスペースに適用しない**。
     - **他のスペースにあるデバイスに適用する**。
       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

   スペースに関係なく、証明書構成はすべてのスペースに対して構成し、すべてのデバイスに配布し、他のデバイススペースのすべてのデバイスに適用できます。
6. **[完了]** をクリックします。

証明書設定

管理者はオンプレミスの非SCEP認証機関を設定できます。

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[管理]** > **[インフラ]** > **[証明書管理]** > **[認証機関]** を開きます。

3. **[+追加]** をクリックします。以下のオプションが表示されます。
   - **Ivanti Neurons for MDM が提供するローカル認証機関を作成する。**
   - **既存の CA で Ivanti Neurons for MDM のローカル CA に署名する。**
   - **公的に信頼されているCloud認証機関に連携する。**
   - **オンプレミスのSCEP認証機関を連携する。**
   - **オンプレミスの非SCEP認証機関を連携する。**
4. 必要に応じて以下のフィールドに入力します。

設定	操作内容
名前	この構成を識別する名前に入力します。
URL	管理者がOpenTrustから取得する OpenTrust CA URL。
パスワード	認証証明書のパスワードを入力します。
認証証明書	OpenTrust/ IDnomicが提供する.p12ファイル形式を許可します。
TLS CA証明書チェーン	OpenTrust/ IDonomicが提供するPEMファイル形式を許可します。

5. **[完了]** をクリックします。

オンプレミスの非SCEP認証機関を設定した後、ID証明書を作成する必要があります。プロフィールIDに基づき、すべての必須フィールドを入力して設定を完了してください。

次の2つの理由で SCEP CA 証明書生成が失敗し、ステージ2タイムアウトに達した場合は、通知が生成されます。

1. Connector に接続できません
2. CA サーバーに接続できません

証明書の透明性

対象：iOS 12.1.1、macOS 10.14.2、tvOS 12.1.1およびサポートされる以降のバージョン。

デバイスプロファイルに一度だけ表示される証明書の透明性適用を制御します。複数の証明書を含めることができ、必要に応じてドメインを無効化できます。

証明書の透明性構成の作成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[証明書]** と入力し、**[証明書の透明性]** 構成をクリックします。
4. 名前と構成の説明を入力します。
5. **[無効化されるドメイン]** を指定します。複数のドメインを追加するには **[+ドメインを追加]** をクリックします。先頭のピリオドはサブドメインに一致させるために使用できますが、ドメイン一致ルールはトップレベルドメイン内のすべてのドメインと一致してはなりません。たとえば、「.example.com」と「.example.co.uk」は許可されますが、「.com」と「.co.uk」は許可されません。ワイルドカードのドメインはサポートされていません。
6. アルゴリズム(SHA 256) の選択後、**[証明書のハッシュ]** を指定します。複数の証明書のハッシュを追加するには **[+追加]** をクリックします。
7. **[次へ]** をクリックして配布設定を行います。
8. **[完了]** をクリックします。

subjectPublicKeyInfoディクショナリのハッシュキーで指定されたデータを生成するには、PEMエンコードされた証明書に対して次のコマンドを使用します。

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -
pubin - outform der | openssl dgst -sha256 -binary | base64
```

お使いの証明書がDERエンコードされている場合は、次のコマンドを使用します。

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -
pubin - outform der | openssl dgst -sha256 -binary | base64
```

詳細は構成を作成するにはを参照してください。

証明書失効チェック構成

この構成により、管理者は失効した証明書をデバイスから確認できます。管理者は認証機関(CA)を指定し、構成を通じてそのCAにリンクするすべての証明書の失効チェックを有効化することができます。

対象: iOS 14.2+

手順

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[証明書]** と入力し、**[証明書失効チェック]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. アルゴリズムを**SHA 256**に設定し、ルート証明書の**ハッシュ**を入力します。

   > ハッシュでは、証明書の公開鍵のBase64エンコード(バイナリ)したSHA-256ハッシュを入力する必要があります。Apple OSに対応する信頼できるルート証明書については、Appleドキュメンテーションを参照してください。この構成には複数のルート証明書を追加できます。

5. **[次へ]** をクリックします。
6. **[この構成を有効化]** オプションを選択します。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

自律 Single Appモード構成の作成

自律 Single Appモード構成では、特定のアプリケーションのみがデバイスで実行されることを保証できます。ユーザーが別のアプリケーションを起動しようとした場合でも、構成によって特定のアプリケーションのみが起動されます。

手順

1. **[構成]** > **[追加]** > **[自律 Single Appモード]** を選択します。
2. 次のガイドラインに従ってアプリおよびその他の設定を定義します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成設定	**バンドルID** - (必須) 一意のバンドルID。2つのディクショナリでBundleIdentifier値が同じで、TeamIdentifier値が異なる場合は、エラーと見なされ、プロファイルがインストールされません。
	チーム識別子 - (必須) アプリが署名されるときに使用される、開発者のチーム識別子。

3. **[次へ]** をクリックします。
4. **[配布]** 画面で、この構成を受信するグループを選択します。
5. **[完了]** をクリックします。

DNSプロキシ構成の作成

Ivanti Neurons for MDM管理者は、[DNSプロキシ構成] を使用して、iPhoneデバイスおよびiPadデバイスのユーザー用にDNSプロキシ設定を構成できます。DNSプロキシペイロードを使用して、DNSプロキシネットワーク拡張およびその他のベンダー固有値を提供するアプリケーションを指定できます。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** に進みます。
3. 検索フィールドに **[DNS]** と入力し、**[DNS]** の **[プロキシ構成]** をクリックします。
4. 名前と構成の説明を入力します。

5. DNSプロキシ構成のための次の設定を入力します。
   - アプリバンドル識別子(必須)。
   - プロバイダバンドル識別子。
   - プロバイダ構成(キーと値)。
6. **[次へ]** をクリックします。
7. **[この構成を有効化]** オプションを選択します。
8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
9. **[完了]** をクリックします。

デバイスログ構成

デバイスログ構成では、Androidデバイスのネットワークおよびセキュリティログを有効にできます。

デバイスログ構成の作成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドで、**デバイスログ**を入力し、構成を選択します。
4. 名前と構成の説明を入力します。
5. **[構成設定]** セクションで、いずれかまたは両方のオプションを選択します。
   - ネットワークログを有効にする
   - セキュリティログを有効にする

セキュリティとネットワークのログ記録がサポートされているAndroidバージョンについては、下記の**セキュリティログ表**の下にある各表を参照してください。

6. **[アプリの利用状況]** セクションで、データの利用状況情報を収集するための **[アプリケーション利用データの収集を有効化]** オプションを選択します。このオプションを有効にした場合、ユーザーはデバイスのデータ利用状況を収集するためのアクセス許可を認めるように要求されます。

   - アプリケーションの利用状況データを収集 - アプリカタログ内のアプリについてアプリケーション利用データを収集する場合に選択します

   アプリの利用状況データは1日1回収集され、前日の利用状況が表示されます。当日の利用状況は報告されません。エンドユーザーは、この情報を取得するための許可を与えるように要求されます。デバイスメーカーによっては、OEMConfig(マネージド構成)を使用している完全にマネージド型のデバイス上では、この許可の事前付与が許されている場合もあります。この機能にはSecure UEM Premiumライセンスが必要です。

7. デバイスメーカーによっては、OEMConfig(マネージド構成)を使用している完全にマネージド型のデバイス上では、この許可の事前付与が許されている場合もあります。
8. **[次へ]** をクリックして配布設定を行います。
9. **[完了]** をクリックします。

セキュリティログ表

デバイスの種類	サポートされている Android バージョン
仕事用マネージドデバイスと仕事用マネージドデバイス非GMSモード(AOSP)	7, 8, 9, 10, 11, 12, 13
仕事用プロファイルを持つマネージドデバイス	8, 9, 10
仕事用プロファイル	不適用
会社所有デバイス上の仕事用プロファイル	11, 12, 13

ネットワークログ表

デバイスの種類	サポートされている Android バージョン
仕事用マネージドデバイスと仕事用マネージドデバイス非GMSモード(AOSP)	8, 9, 10, 11, 12, 13
仕事用プロファイルを持つマネージドデバイス	8, 9, 10

デバイスの種類	サポートされている Android バージョン
仕事用プロファイル	12, 13
会社所有デバイス上の仕事用プロファイル	12, 13

デバイスログ構成をデバイスにインストールした後、ユーザーはデバイス管理およびネットワークログに関する情報が含まれている通知を受信します。**[OK]** をクリックして通知内容を承諾します。

デバッグログの要求

手順

1. Ivanti Neurons for MDM にログインします。
2. **[デバイス]** > **[デバイス詳細]** を開きます。
3. **[概要]** セクションで、**[強制チェックイン]** ボタンの横にある3点メニューボタンをクリックします。
4. **[デバッグログをリクエスト]** を選択します。
5. 以下の2つのオプションから1つ選択してください：
   - 不具合レポートを除外 - このオプションを選択し、[次へ] をクリックすると、画面に確認ウィンドウが表示されます。**[デバッグログをリクエスト]** をクリックします。ユーザーはこのオプションに同意する必要がありません。このログでは選択した Android デバイスの不具合レポートが除外されます。
   - 不具合レポートを含める - このオプションを選択し、[次へ] をクリックすると、画面に確認ウィンドウが表示されます。**[デバッグログをリクエスト]** をクリックします。ユーザーは、不具合レポートを共有するために同意する必要があります。Android デバイスの場合、ユーザーは、デバイスログを送信し、不具合レポートを含めるように指示されます。

Android暗号化

暗号化構成は、デバイス管理者モードにあるAndroidデバイスのデバイスの暗号化要件を定義します。デバイスの暗号化は、企業の機密データが既知のジェイルブレイクやルートの悪用によってアクセスされないことを保証します。暗号化では、デバイスのデータが読み取り不能な形式で保存されるため、誰かがデバイスを盗んでもデータにアクセスすることはできません。

暗号化を有効にすると、デバイスユーザーにデバイスの暗号化を促してデバイスのパスコード設定を要求します。パスコードとは、データを解読し読み取れるようにするものです。データの暗号化は、パスコードが設定された際に、Androidエンタープライズ(仕事用プロファイルまたはマネージドデバイス)またはiOSデバイスで自動的に有効になります。暗号化している間はデバイスを使用することができません。暗号化が一度オンになると、オフにするにはデバイスをリセットして工場出荷時の状態に戻す必要があります。

暗号化設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
デバイスの暗号化を有効にする	この構成を受信するすべての暗号化対応Androidデバイスで暗号化をオンにするには、この設定を選択します。

Android暗号化構成は、Android 11で稼働するデバイス管理者モードのSamsungデバイスでは廃止されています。この暗号化は、デフォルトでは、デバイスパスコードが設定されている場合にAndroid Enterpriseデバイスでサポートされています。

詳細は構成を作成するにはを参照してください。

暗号化DNS

ライセンス: Gold

対象:

- iOS 14.0またはサポートされる以降のバージョン。
- macOS 11.0またはサポートされる以降のバージョン

暗号化DNSの構成により、VPNの構成なしでセキュリティの強化が可能です。

このセクションは以下のトピックを含みます。

- 暗号化DNSの構成
- 暗号化DNS構成の設定

暗号化DNSの構成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[DNS]** と入力し、**[暗号化DNS]** 構成をクリックします。
4. 名前と構成の説明を入力します。
5. 暗号化DNS構成の設定を入力します。
6. **[次へ]** をクリックします。
7. **[この構成を有効化]** オプションを選択します。
8. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム

9. **[完了]** をクリックします。

暗号化DNS構成の設定

次の表の設定を使用して暗号化DNSを構成します。設定の詳細はAppleドキュメンテーションを参照してください。

設定	説明
DNS設定	暗号化DNSサーバーの構成を定義する辞書。
DNPプロトコル	DNSサーバーとの通信に使用する暗号化トランスポートプロトコルを指定します。以下のプロトコルから1つ選択してください。 • HTTPS • TLS
サーバーURL	RFC 8484に定義されたDNS-over-HTTPSサーバーのURIテンプレート。URLはhttps://の形式とし、サーバー証明書の確認にはURLのホスト名またはアドレスを使用します。サーバーアドレスが記載されていない場合、URL内のホスト名またはアドレスを使用してサーバーアドレスを判断します。このキーはDNSプロトコルがHTTPSの場合のみ存在します。
サーバーアドレス	DNSサーバーIPアドレス文字列の順不同リスト。IPv4アドレスとIPv6アドレスが混在する場合があります。 **[追加]** をクリックして1つまたは複数のサーバーアドレスを追加します。
補足的一致ドメイン	DNSサーバーを使用するDNSクエリーを判断するドメイン文字列のリスト。指定されていない場合、すべてのドメインがDNSサーバーを使用します。 1つまたは複数のドメインを追加するには **[追加]** をクリックします。
ユーザーによるDNS設定の無効化を禁止	ユーザーがDNS設定を無効化することを禁止します。このキーは監視対象のデバイスにのみ対応しています。
要求ルール	DNS設定を定義するルール群。ルールがない場合、システムは常にDNS設定を適用します。 **[+要求ルールを追加]** をクリックすると1つ以上の要求ルールを追加できます。
Network (ネットワーク)	この辞書が現在のネットワークに一致する場合に実行するアクション。以下のアクションから1つ選択してください:

設定	説明
	• **連携**：辞書が一致する場合はDNS設定を適用します。 • **連携解除**：辞書が一致する場合はDNS設定を適用しません。 • **連携を評価**：辞書が一致する場合、ドメインごとの例外付きでDNS設定を適用します。
連携評価	このネットワークオプションには以下の設定があります。 • **ドメインアクション** - 指定したドメインに対するDNS設定動作。以下のアクションから1つ選択してください： ◦ **決して連携しない** - 指定したドメインにDNS設定を使用しない。 ◦ **必要に応じて連携** - 指定したドメインにDNS設定の使用を許可する。 • **ドメイン** - この評価を適用するドメイン。1つまたは複数のドメインを追加するには **[+追加]** をクリックします。
ルール	以下のパラメータと指定した値を一致させる1つまたは複数のルールを追加するには **[+追加]** をクリックします。
DNSのドメインが一致	ドメイン名のリスト。指定したリスト内のドメイン名のいずれかがデバイスの検索ドメインリスト内のいずれかのドメインに一致する場合、このルールが一致します。
DNSのサーバーアドレスが一致	IPアドレスのリスト。ネットワークの指定したDNSサーバーのいずれかがIPアドレスリスト内のアドレスのいずれかに一致する場合、このルールが一致します。
SSIDが一致	現在のネットワークと照合するSSIDのリスト。ネットワークがWi-Fiネットワークでないか、そのSSIDがリスト内にない場合、一致ではありません。 任意のSSIDと照合するにはこのキーと対応のリストを省略します。
インターフェイスの種類が一致	インターフェイスの種類。指定されている場合、主なネットワークインターフェイスハードウェアが指定した種類に一致する場合のみこのルールが一致します。次の種類から1つを選択します。 • イーサネット • Wi-Fi • セルラー

設定	説明
URL文字列のプローブ	プローブするURL。リダイレクトなしにこのURLの取得に成功する場合(200 HTTPステータスコードを戻す)、このルールが一致します。

詳細は構成を作成するにはを参照してください。

脅威防御

対象：

- iOS対応Goクライアントバージョン3.2.0またはサポートされる以降のバージョン。
- Android対応Goクライアントバージョン52またはサポートされる以降のバージョン。

Ivanti Neurons for MDMには、アクティベーショントークンを配布してThreat Defenseを有効化する機能があります。この技術は、AndroidおよびiOSクライアント対応のGoに統合されています。Threat Defenseは、デバイス、ネットワーク、アプリケーションに影響を与えるモバイル脅威や脆弱性からマネージドデバイスを保護します。

この構成をIvanti Neurons for MDMで有効化し、デバイスに適用すると、Threat Defenseライブラリが Goクライアントで有効化されます。Threat Defenseサービスは、ライセントークンを削除し、クライアントにライセンス構成を再送信することで無効化できます。

Threat Defenseの監視対象：

- デバイスレベル: システムパラメータ、構成、ファームウェア、ライブラリ。ここから疑わしい、または悪意のある活動を特定。
- ネットワークレベル: モバイルデバイスを出入りするネットワークトラフィックおよび疑わしい接続。
- アプリレベル: リスク評価とコード分析を通じて、リーキーな(企業データを危険にさらす可能性のある)アプリおよび悪意あるアプリ。

最新ドキュメンテーション

最新の脅威防御の方法については、Ivanti Neurons for MDM製品ドキュメンテーションの製品ドキュメンテーションサイトにある*Ivanti Neurons for MDM脅威防御ソリューションガイド*を参照してください。

FileVault 2

ライセンス: Gold

FileVault 2は、ボリュームのコンテンツに完全なXTS-AES 128ディスク暗号化を実行できます。

FileVault 2を有効化した場合、以下の設定が構成可能となります。

カテゴリ	設定

FileVault 2ユーザー設定	• 指定ユーザーがログアウトするまでFileVaultの有効化を延期
	  • FileVault有効化のプロンプトを常にユーザーに表示
	  • ユーザーがFileVault有効化を回避できる最大回数
	• ユーザーのログアウト時にFileVault有効化を要求しない

出力パス	リカバリキーとコンピューター情報plistが保存される場所へのパスを入力します。
個人リカバリキー	• 個人リカバリキーを作成 • FileVaultの有効化後、個人リカバリキーをユーザーに表示 **Note:** このオプションは、**[個人リカバリキーを作成]**を有効化している場合にのみ表示されます。デフォルトでは無効化されています。 • 機関リカバリーキーの有効化：キーチェーンの使用 - このペイロードで証明書情報が提供されない場合、/Library/Keychains/FileVaultMaster.keychainで作成済みのキーチェーンを使用します。 以下のオプションから1つ選択してください。

カテゴリ	設定
	• 証明書をアップロード • 証明書 • ユーザーシステム上でのキーチェーン使用

FileVaultリカバリキー

ライセンス: Gold

FileVaultリカバリキーの構成は、FileVaultリカバリキーの企業サーバーへのリダイレクトおよびエスクローを決定します。

macOSデバイスは構成の再プッシュ時にリカバリキーの送信を停止するため、FileVaultリカバリキーの除外と再プッシュの構成は無効化されています。

次のオプションを設定できます。

設定	説明
名前	この構成を識別する名前に入力します。
説明	(任意)この構成の目的を明示する説明を入力します。
macOS 10.13より前の構成設定	
回復キーをIvanti Neurons for MDMテナントに保存	Ivanti Neurons for MDMがテナントにキーを保存できるようにする場合に選択します。必要であれば、[デバイス詳細]ページからキーを解読できます。
URLをサーバーにリダイレクト	以下の設定を入力します。 • Appleの代わりにFDEリカバリキーを送信する**リダイレクトURL**を入力してください。URLはhttps://で始まる必要があります。 • ドロップダウンリストから証明書を選択します。PKCS1フォーマットの証明書のみサポートされます。
macOS 10.13以降の構成設定	
場所	(必須)リカバリキーがエスクローされる場所の短い説明を入力します。このテキストはメッセージに挿入され、FileVaultを有効化する際

設定	説明
	にユーザーに表示されます。
デバイスキー	(任意) ユーザーがパスワードを忘れたと思われる場合にヘルプテキストに含める文字列を入力します。

FileVaultオプション構成

この構成により管理者は、FileVaultを有効化または無効化したり、システムがスタンバイ状態になったときにFileVaultキーを破棄することができます。

対象：macOS 10.7+

手順

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[FileVault]** と入力し、**[FileVaultオプション]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. [構成設定] セクションで、必要なオプションを選択します。
   - システムがスタンバイモードに入るときにFileVaultキーを破壊する
   - ディスク全体の暗号化の無効化を許可しない
   - ディスク全体の暗号化の有効化を許可しない
5. **[次へ]** をクリックします。
6. **[この構成を有効化]** オプションを選択します。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし（デフォルト）
   - カスタム
8. **[完了]** をクリックします。

ID証明書

このセクションは以下のトピックを含みます。

- ID証明書設定
- 構成の配布

ID証明書構成では、モバイルデバイスの証明書認証メカニズムを定義します。ID証明書とは、X.509証明書(.p12または.pfx)です。ID証明書は認証機関をソースとして動的にも生成できます。開始する前に、モバイルデバイスへの証明書配信を計画する方法を把握しておく必要があります。必要な認証機関も構成しておいてください。

リリース91以降、AppleデバイスのデバイスID証明書は、有効期限切れになる前の30日以内に自動的に更新されます。iOSデバイスは、定期的なデバイスチェックインフローの一部として、更新済みのMDM証明書をIvanti Neurons for MDMから受け取ります。ただし、オフラインになっている期間が長すぎて、証明書期限切れ前の更新が行われていたであろうチェックインよりも前にすでにMDM証明書が期限切れになっていたiOSデバイスは、Ivanti Neurons for MDMへの再登録が必要になります。

- 新しいID証明書を作成する際、SHA-1証明書は使用できなくなりました。他のアルゴリズムを選択してください。証明書を更新する際、旧い証明書がSHA-1を使用していれば、同じSHA-1アルゴリズムを使用可能です。旧い証明書がSHA-1より新しいアルゴリズムを使用している場合、SHA-1には変更できません。
- ID証明書を構成した後、**[構成をテストして続行]**をクリックし、テスト証明書の発行と有効性検証を行います。主体者名がローカル認証機関と同じ場合、動的に生成された新規または既存のID証明書構成に対してこのテストを実行すると、エラーが表示される場合があります。このエラーメッセージが表示された場合は、ID証明書の主体者名を、ローカル認証機関の主体者名とは異なるものに変更する必要があります。既存のID証明書構成の主体者名が変更されると、証明書が再発行され、構成が再プッシュされます。
  テスト証明書の発行なしで構成を作成し、**動的生成**証明書を配布するオプションを設定している場合は、**[続行]**をクリックしてください。
- 既存のID証明書構成の編集中に(これは順次TunnelまたはAppTunnelのセキュリティプロファイルで使用されます)、必要に応じて**[アクション]**メニューから**[キャッシュした証明書をクリアし、最近更新した新しい証明書を発行]**オプションを選択できます。キャッシュされていない証明書は自動的に再発行されます。

- AndroidアプリにID証明書が割り当てられている場合、ユーザーのアプリがID証明書を取得し、証明書を使用する許可を(アプリではなく)ユーザーが与えるためのプロンプトが表示されることはありません。これにはEmail+、Gmailなどすべてのアプリが含まれます。
- Email+は、ユーザーが入力した[ID証明書]で構成することができ、アプリ構成としてAndroid Enterpriseデバイスにプッシュし、割り当てることができます。これは、会社所有デバイス上の仕事用プロファイルとデバイス所有者モードにのみ適用されます。

ID証明書設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
証明書の配布	設定する証明書配布の種類を選択します。 • **シングルファイル:** デバイスに配布する既存の証明書をアップロードします。 • **動的生成:** ローカルまたは外部の証明書機関を利用し、要求に応じて証明書を作成します。 • **ユーザー提供:** ユーザーによってアップロードされる証明書の種類のラベルを作成します。作成した後、ユーザーは作成したラベル(オプション)をセルフサービスポータルで閲覧し、そのラベルに対応する証明書をアップロードできます。 • **デバイス認証情報:** 派生認証の用途を以下のいずれかに指定してください。 ◦ 認証 ◦ 暗号化 ◦ 署名 ◦ 復号化 •

設定	操作内容
	• **SCEP構成**: SCEPサーバーからの証明書を要求する方法を指定します。以下の構成から1つ選択してください。 ◦ Apple 構成 ◦ Windows構成 選択により、残りのフォームに表示されるオプションが決まります。
すべてのアプリにプライベートキーへのアクセスを許可 (macOS 10.10+)	**適用先:** 1つのファイル、動的に生成、ユーザ提供、SCEP Apple 構成 ID 証明書。 (任意) PKCS#12証明書の場合は、**[すべてのアプリにプライベートキーへのアクセスを許可]** オプションを有効化し、すべてのアプリがプライベートキーにアクセスできるようにします。 たとえばこのキーは、VPNに使用する証明書へのアクセスを許可するため、ユーザーからパスワードが要求された場合などに使用できます。
シングルファイル	
ID証明書データ	証明書ファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択する]** をクリックしてファイルシステムから選択します。
パスワード	PKCS#12証明書ファイルを保護するパスワードを入力します。このパスワードはプロンプトなしでのインストールに使用されます。
動的生成	
ソース	ドロップダウンからローカル認証機関を選択します。**[管理]** > **[証明書管理]** でこのCAを作成しておく必要があります。
テスト証明書の発行なしで構成を作成	テスト証明書の発行なしで構成を作成する場合にチェックチェックボックスを選択します。

設定	操作内容
Windowsのみ - ターゲット証明書ストア	管理者はWindowsデバイスでターゲット証明書ストアを選択できるようになりました。
ユーザー提供	
証明書表示名	証明書名を入力します。この証明書の名前はテナントに固有であり、ユーザーは証明書をアップロードする際にセルフサービスポータルで名前を見ることができます。
プライベートキーを削除	*n*(1～30) 日後に証明書のプライベートキーを削除する場合に選択します。 この操作にはIvanti Neurons for MDMが提供するAPIを使用できます。APIの詳細は*Ivanti Neurons for MDM APIガイド*をご覧ください。 プライベートキーが削除された後でこの証明書を構成に使用しようとすると(アプリケーションの認証やWi-FiまたはVPN構成のプッシュなど) 、タスクは失敗します。プライベートキーを削除する前に必ずタスクを実行してください。
プライベートキーを削除するまでの日数	証明書のプライベートキーがクリアされる日数(1～30) を選択します。デフォルト値は2日です。
派生認証情報	
派生認証情報の使用	以下のいずれかを選択します。 • **認証** - 派生認証情報を認証に使用することを指定します。 • **暗号化** - 派生認証情報の用途を暗号化に指定します。 • **署名** - 派生認証情報を署名に使用することを指定します。

設定	操作内容
	• **復号化** - 派生認証情報の用途を復号化に指定します。
ブランド	使用する派生認証情報プロバイダーを次から選択します。 • **Entrust** • **Intercede** • **Purebred** カスタム派生認証情報を追加する方法は、**派生認証情報プロバイダー**を参照してください。
ACME構成 - iOS/iPadOS16+にのみ該当	
クライアント識別子	特定のデバイスを識別する一意の文字列
ディレクトリURL	(必須) ACMEサーバーのディレクトリURL。このURLには、httpsスキームを使用する必要があります。
拡張キー使用法	値は文字列の配列です。各文字列はドット表記のOIDです。たとえば、["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"] はクライアント認証とメール保護を示します。 デバイスは、ACMEサーバーが発行する証明書の場合に、このフィールドを要求します。ACMEサーバーは、自身が発行した証明書内ではこのフィールドをオーバーライドまたは無視する場合があります。
キーサイズ	(必須) KeySizeの有効値は、KeyTypeとHardwareBoundの値に依存します。特定の要件については、それぞれのキーを参照してください。
キータイプ	(必須) 生成するキーペアの種類。
タイトル名	(必須) デバイスは、ACMEサーバーが発行する証明書の場合に、このサブジェクトを要求します。ACMEサーバーは、自身が発行した証明書内ではこのフィールドをオーバーライドまたは無視する場合があります。OIDと値の配列として表されるX.500名の表現 たとえば、/C=US/O=Apple Inc./CN=foo/1.2.5.3=barは、以下に相当します。

設定	操作内容
	[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]] ドット区切りの数字でOIDを表現でき、国(C)、地域(L)、州(ST)、組織(O)、組織ユニット(OU)、共通名(CN)はそれぞれショートカットです。 型:[文字列]
サブジェクトの別名	ACMEサーバーが発行する証明書の場合にデバイスが要求するサブジェクト別名。ACMEサーバーは、自身が発行した証明書内ではこのフィールドをオーバーライドまたは無視する場合があります。
キーの使用	この値はビットフィールドです。 ビット0x01は、デジタル署名を示します。 ビット0x10はキーの承諾を示します。 デバイスは、ACMEサーバーが発行する証明書の場合に、このキーを要求します。ACMEサーバーは、自身が発行した証明書内ではこのフィールドをオーバーライドまたは無視する場合があります。
バインドされたハードウェア	[バインドされたハードウェア] がtrueに設定されていると、プライベートキーがデバイスにバインドされ、そうなると、キータイプはECSECPrimeRandomでなければならず、キーサイズは256または384でなければなりません。
証明	trueの場合、デバイスは、デバイスを記述する構成証明と生成されたキーをACMEサーバーに提供します。[証明] がtrueの場合は、[バインドされたハードウェア] もtrueであることが必要です。
SCEP 構成 - Apple 構成	
ID証明書(SCEP)	SCEPサーバーを指定する場合に選択します。

設定	操作内容
ローカル証明書機関	**[管理]** > **[証明書管理]** ですでに作成してあるローカル認証機関を指定する場合に選択します。このオプションを選択したときに表示されるドロップダウンからローカル証明書機関を選択します。
URL	SCEPサーバのURLを入力します。
CA識別子	認証機関によって提供された識別子を入力します。
タイトル名	OIDと値をコンマで区切って配列するX.500名を入力します。一般に、サブジェクトはユーザーの完全修飾ドメイン名にします。たとえば、C=US,DC=com,DC=MobileIron,OU=InfoTechやCN=www.mobileiron.comとします。 また、OIDに変数を追加してサブジェクトをカスタマイズすることができます。たとえばCN=www.mobileiron.com-$DEVICE_CLIENT_ID$です。 設定を簡素化するために、$USER_DN$変数を使用して[サブジェクト]にユーザーのFQDNを入力することができます。 主体者名にはバックスラッシュ(\)を使用しないでください。
主体者別名タイプ	証明書テンプレートの属性に基づき、RFC 822名、DNS名、URI、または「なし」を選択します。
主体者別名値	対応するタイプの値を入力します。最初に「$」の文字を入力すると、可能なカスタムLDAPおよびAAD属性のドロップダウンリストが表示されます。リストから適切なカスタム属性を選択してください。 AAD値を使用する場合は、「onPremisesImmutableId」のみサポートされます。fn:base64tohex(${onPremisesImmutableId})を入力してください。
NTのプリンシパル名	Microsoft環境の主体者別名を入力します。これは通常ユーザーのUPN(ユーザーのプリンシパル名)を含むよう構成されます。
チャレンジ	(任意)事前共有シークレットとして自動登録に使用されて

設定	操作内容
	います。
再試行	最初に「保留」というステータスが返された後、認証を再試行できる回数をリストから選択して設定します。
再試行遅延	再試行までの間、待機する秒数をリストから選択して設定します。
キーサイズ	1024、2048、4096ビットのいずれかを選択します。
デジタル署名として使用	証明書を署名に使用できる場合に選択します。
キー暗号化として使用	証明書を暗号化に使用できる場合に選択します。
CAフィンガープリント	認証機関がHTTPを使用している場合は、CAの証明書のフィンガープリントとして使用される16進数を入力します。MD5フィンガープリントがサポートされています。 希望に応じて、証明書からフィンガープリントを作成することができます。証明書を目的の部分にドラッグアンドドロップするか、**[証明書から作成]**をクリックし、ファイルシステムから証明書を選択します。
SCEP構成 - Windows構成	
CA(認証機関)	**[管理]** > **[証明書管理]**ですでに作成してある認証機関を指定する場合に選択します。このオプションを選択したときに表示されるドロップダウンから認証機関を選択します。
タイトル名	OIDと値をコンマで区切って配列するX.500名を入力します。一般に、サブジェクトはユーザーの完全修飾ドメイン名にします。たとえば、C=US,DC=com,DC=MobileIron,OU=InfoTechやCN=www.mobileiron.comとします。 また、OIDに変数を追加してサブジェクトをカスタマイズすることができます。たとえばCN=www.mobileiron.com-$DEVICE_CLIENT_ID$です。

設定	操作内容
	設定を簡素化するために、$USER_DN$変数を使用して[サブジェクト]にユーザーのFQDNを入力することができます。 主体者名にはバックスラッシュ(\)を使用しないでください。
主体者別名タイプ	**[追加]**をクリックし、証明書テンプレートの属性に基づいてRFC 822名、DNS名、URI、または「なし」を選択します。
再試行	最初に「保留」というステータスが返された後、認証を再試行できる回数をリストから選択して設定します。
再試行遅延	再試行までの間、待機する秒数をリストから選択して設定します。
キーの長さ	キーサイズを1024、2048、4096から選択します。
用途を選択	少なくとも1つ選択します。 • デジタル署名として使用 - 証明書を署名に使用できる場合に選択します。 • キー暗号化として使用 - 証明書を暗号化に使用できる場合に選択します。
有効性	有効期間を日数、月数、年数で選択します。
CA親指指紋	認証機関がHTTPを使用している場合は、CAの証明書のフィンガープリントとして使用される16進数を入力します。MD5フィンガープリントがサポートされています。 希望に応じて、証明書からフィンガープリントを作成することができます。証明書を目的の部分にドラッグアンドドロップするか、**[証明書から作成]**をクリックし、ファイルシステムから証明書を選択します。
ハッシュアルゴリズムファミリー	SHA-2またはSHA-3アルゴリズムを選択します。

仕事用本人確認(Work Challenge)パスコードを設定せずにデバイスの仕事用プロファイルにID証明書を適用する場合、デバイスは仕事用本人確認パスコードではなくデバイスパスコードの入力を求めます。

構成の配布

Ivanti Neurons for MDM リリース81以降、グローバル管理者はスペース管理者に、すべてのデバイス向けおよびカスタム配信オプション向けの動的生成ID証明書の編集を委譲できるようになりました。動的生成証明書の場合は、**[この構成をすべてのスペースで利用可能にする]** オプションを選択することも可能です。このオプションは、動的生成ID証明書をすべてのスペースに提供し、Exchange、Wi-Fi、VPNのほか、マネージドアプリ構成などの他の構成でも使用可能にします。このオプションは、動的生成ID証明書を、関連する構成の一部としてのみデバイス(非デフォルトスペース)に配布する必要があり、個別の構成としては配布しない場合に使用できます。

手順

1. 前述の表にある情報を使用して、ID証明書の設定フィールドに入力します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。
4. (オプション) **[この構成をすべてのスペースで利用可能にする]** を選択します。
5. 以下の配布オプションから1つ選択します。
   - **すべてのデバイス**。以下のオプションから1つ選択してください:
     - **他のスペースに適用しない**。
     - **他のスペースにあるデバイスに適用する**。
       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。
   - **デバイスなし**(デフォルト)
   - **カスタム**。以下のオプションから1つ選択します。
     - **他のスペースに適用しない**。
     - **他のスペースにあるデバイスに適用する**。
       - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

> スペースに関係なく、動的生成ID証明書はすべてのスペースに対して構成し、すべてのデバイスに配布し、他のデバイススペースのすべてのデバイスに適用できます。

6. **[完了]** をクリックします。

Appleアクティベーションロック構成

ライセンス: Silver

このセクションは以下のトピックを含みます。

- iOSアクティベーションロックの有効化
- 監視対象デバイスにおけるiOSアクティベーションロック機能の有効化
- macOSアクティベーションロックの有効化
- 監視対象デバイスにおけるmacOSアクティベーションロック機能の有効化
- iOSアクティベーションロックバイパスコードの使用
- iOSアクティベーションロックバイパスコードのクリア

アクティベーションロックは、紛失したり盗難にあったデバイスが誰かに使われるのを防ぐために設計されたAppleの機能です。「...を探す」を有効化した後、iCloudアカウントとそのデバイスのハードウェア識別子とのマッピングがAppleのアクティベーションサーバーに保存されます。その時点で、既存のApple IDとパスワードを入力せずに、「...を探す」のオフ、デバイスの消去、または再アクティベートができなくなります。ユーザー以外の誰かがデバイスをワイプし、その後、再アクティベートして利用しようとすると、設定アシスタントにApple IDとパスワードを入力するよう指示されます。

監視対象デバイス上でエンドユーザーが「[デバイス]を探す」機能を有効にしている場合は、アクティベーションロックを無効化しても、この機能は無効化されません。デバイスがリセットまたはリモートでワイプされた場合、設定アシスタントがユーザーに行動を促します。

アクティベーションロックは、管理者に対し、監視対象デバイスの盗難防止のためのより多くのオプションを提供するものです。しかし、これは主にコンシューマー向けの機能であるため、企業の管理者のほとんどがアクティベーションロックを無効にしていると考えられます。次の表は、企業責任の展開のためのオプションをまとめたものです。

デバイスの種類	結果
企業が責任を持ち非監視対象にしているもの	• 監視対象デバイスでは、アクティベーションロックはデフォルトで無効化されています。 • デバイスユーザーがアクティベーションロックをオンにすることはできません。
企業が責任を持ち非監視対象にしているもの	• エンドユーザーがユーザー自身のApple IDでiCloudにサインインし、Find My Deviceをオンにするとすぐに、アクティベーションロックが有効化されます。 • Ivanti Neurons for MDM などのMDMサーバーは、監視対象でないデバイスのアクティベーションロックを制御できません。デバイスユーザーは、個人の認証情報でアクティベーションをロックできるため、退職後にデバイスユーザーのリソースは残りません。

iOSアクティベーションロックの有効化

対象：iOS 7+監視対象

この構成は、「...を探す」機能を有効にしている監視対象デバイス(iOS 7以降)に適用されます。管理者または他のユーザーがデバイスをワイプ、アクティベート、または「[デバイス]を探す」機能を無効化しようとすると、Appleアクティベーションロック画面が表示されます。先へ進むには、iTunesの認証情報またはBypassコードを入力する必要があります。

監視対象デバイスのBypassコードは、アクティベート時に保存され、デバイス詳細に表示されます。Bypassコードは、監視対象デバイスの「アクティベーションロッククリア」コマンドを使用してリモートで送信可能です。ただし、デバイスを再アクティベートしたり「[デバイス]を探す」機能をオフにしたりする際は、コードを手動で入力する必要があります。

すべてのスペースに1つのアクティベーションロック構成しか作成できません。

監視対象デバイスにおけるiOSアクティベーションロック機能の有効化

手順

1. デバイスで**「...を探す」**機能を有効化します。
2. **[構成]**に進みます。
3. 既存の構成のリストから、**[Appleアクティベーションロック]**構成を選択します。

4. **[編集]** をクリックします。
5. iOS 7+監視対象セクションで、**[アクティベーションロックを有効化]** をクリックします。
6. **[完了]** をクリックします。
7. デバイスを登録します。

macOSアクティベーションロックの有効化

対象：macOS 10.15+監視対象

この構成はmacOS 10.15以降の監視対象デバイスに適用されます。macOSのアクティベーションロックは、Apple T2セキュリティチップを搭載したMacにのみ適用されます。監視対象デバイスをアップグレードまたは新規インストールした場合、および既存登録デバイスをアップグレードした場合、アクティベーションロックはデフォルトでオフになっています。それらのデバイスで「...を探す」機能を有効化してもアクティベーションロックは自動的に有効化されません。

管理者または他のユーザーがデバイスをワイプ、アクティベート、または「...を探す」機能を無効化しようとすると、Appleアクティベーションロック画面が表示されます。先へ進むには、iTunesの認証情報またはBypassコードを入力する必要があります。監視対象デバイスのBypassコードは、アクティベート時に保存され、デバイス詳細に表示されます。Bypassコードは、監視対象デバイスの「アクティベーションロッククリア」コマンドを使用してリモートで送信可能です。ただし、デバイスを再アクティベートしたり「...を探す」機能をオフにしたりする際は、コードを手動で入力する必要があります。

すべてのスペースに1つのアクティベーションロック構成しか作成できません。

監視対象デバイスにおけるmacOSアクティベーションロック機能の有効化

手順

1. デバイスで「...を探す」機能を有効化します。
2. **[構成]** に進みます。
3. 既存の構成のリストから、**[Appleアクティベーションロック]** 構成を選択します。
4. **[編集]** をクリックします。
5. macOS 10.15+監視対象セクションで、**[アクティベーションロックを有効化]** をクリックします。
6. **[完了]** をクリックします。
7. デバイスを登録します。

iOSアクティベーションロックバイパスコードの使用

iOSアクティベーションロックが有効な状態でデバイスをワイプすると、バイパスコードがAppleのアクティベーションサーバーとIvanti Neurons for MDM管理者インターフェイスに保持されます。

手順

1. **[デバイス]** を開きます。
2. デバイスを選択します。
3. **[アクション]** > **[ワイプ]** をクリックします。デバイスが再起動するまでに数分かかることがあります。
4. デバイスにApple IDとパスワードの入力を求めるプロンプトが表示されたら、**Apple ID**を空白にしてください。
5. **パスワード**のフィールドにバイパスコードを入力します。
6. **[次へ]** をクリックします。
7. 設定を進めます。

iOSアクティベーションロックバイパスコードのクリア

iOSアクティベーションロックをIvanti Neurons for MDM管理者インターフェイスでクリアすると、バイパスコードはAppleのアクティベーションサーバーから削除されますが、Ivanti Neurons for MDM管理者インターフェイスのデバイス情報には残ります。

手順

1. **[デバイス]** を開きます。
2. デバイスを選択します。
3. **[構成]** を選択します。
4. **[Appleアクティベーションロック]** を選択します。
5. **[編集]** をクリックします。
6. iOS 7+監視対象セクションで、**[アクティベーションロックを有効化]** を無効にします。
7. **[完了]** をクリックします。
8. **[デバイス]** を開きます。

9. デバイスを選択します。
10. **[アクション] > [ワイプ]** をクリックします。デバイスが再起動するまでに数分かかることがあります。これで、新しいユーザーのAppleIDとパスワードでデバイスを設定できます。
11. 設定を進めます。

iOSアクティベーションロックのクリアのステータスが次のようにインターフェイス上に表示されます。

ステータス	結果
保留中	• サーバーがAppleにアクティベーションロックのクリアコードを送信しています。
送信済み	• Appleがアクティベーションロックのクリアコードの受信を認識しました。
失敗	• サーバーがAppleにコードを送信できませんでした。 • Appleがエラーを報告しました。

iOSカスタム構成

iOSのカスタム構成により、AppleのiPhone構成ユーティリティなど、別のアプリによって作成されたiOS構成プロファイルをアップロードし配信することができるようになります。

iOSカスタム設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ファイルデータ	構成ファイルをドラッグするか、**[ファイルを選択する]** をクリックしてファイルシステムから選択します。

詳細は構成を作成するにはを参照してください。

iOSの制約

iOS制約とは、デバイスの主要ユーザーが、そのiOSデバイスで他のユーザーが実行できる操作を制御するための設定です。これらの設定はAppleによって定義され、Ivanti Neurons for MDMによって管理されています。

共有iPadにこの構成を配布する際には、デバイスチャネルまたはユーザーチャネルを選択します。これはそれぞれに異なる構成を配布し、デバイスチャネルまたはユーザーチャネルのみに制限をかける際に有用です。

iOS制約設定

カテゴリ	設定	操作内容
	名前	この構成を識別する名前に入力します。
	説明	この構成の目的を明示する説明を入力します。
デバイス機能	**iOSの全バージョン**	**デバイス機能の使用を許可します。**
	スクリーンショットと画面の録画を許可	iOS内蔵のスクリーンキャプチャ機能を利用し、デバイスユーザーがスクリーンキャプチャを取ることを許可する場合に選択します。
	リモート画面監視を許可(iOS 9.3以降)	ユーザーにリモート画面の監視を許可する場合に選択します。
	プロンプトなしのマネージドクラスルーム画面強制監視を許可(監視対象のみ - iOS 10.3+)	(iPadのみに適用)監視対象のiPadがマネージドクラスを持つよう構成されていて、画面にプロンプトなしのメッセージの表示を許可する場合に選択します。
	ローミング中の自動同期を許可	デバイスが国外にあるときにメールアカウントの同期を許可する場合に選択します。
	Siriの使用を許可	パーソナルアシスタントアプリをサポートするデバイスにおいて、その使用を許可する場合に選択します。
	デバイスロック時のSiriの使用を許可	デバイスのロック中でもパーソナルアシスタントアプリの使用を許可する場合に選択します。
	Siriの単語フィルターを	Siriの単語フィルターを有効化する場合に選択

カテゴリ	設定	操作内容
	有効化(監視対象のみ)	します。
	音声ダイヤルを許可	ユーザーに対し、デバイスへの音声入力による連絡先または電話番号へのダイヤルを許可する場合に選択します。
	アプリ内購入を許可	ユーザーにデバイスで動作するアプリを通じた購買を許可する場合に選択します。
	デバイスロック時のPassbookの使用を許可	デバイスロックされているときにPassbook通知を許可する場合に選択します。
	ロック画面でのコントロールセンターを許可	ロック画面からコントロールセンターにアクセスできるようにする場合に選択します。
	ロック画面での通知表示を許可	通知をロック画面に表示できるようにする場合に選択します。
	ロック画面でのToday表示を許可	ロック画面からToday表示にアクセスできるようにする場合に選択します。
	管理対象のアプリから管理対象でないアプリへのオープンインを許可	**Goldライセンスが必要です**。 管理対象のアプリやアカウントのドキュメントを管理対象でないアプリやアカウントで開けるようにする場合に選択します。このオプションを無効にすると、管理対象のアプリやアカウントから管理対象でないアプリやアカウントへのドキュメントのやり取りを防止することができます。たとえば、会社のドキュメントを私的なアプリでは開けないようにすることができます。このオプション(オフ)とマネージドドメイン構成を併用すると、マネージドドメインからダウンロードしたデータがマネージドアプリでしか開けなくなります。
	管理対象でないアプリから管理対象のアプリへのオープンインを許可	**Goldライセンスが必要です**。

カテゴリ	設定	操作内容
		管理対象でないアプリやアカウントのドキュメントを管理対象のアプリやアカウントで開けるようにする場合に選択します。このオプションを無効にすると、管理対象でないアプリやアカウントから管理対象のアプリやアカウントへのドキュメントのやり取りを防止することができます。たとえば、会社のメールを使用して私的なドキュメントを送信できないようにすることができます。このオプション(オフ)とマネージドドメイン構成を併用すると、非マネージドドメインからダウンロードしたデータはマネージドアプリで開けなくなります。
	初回のAirPlayペアリングでパスコードを要求	デバイスの初回のペアリングを許可するためにユーザーがiOSデバイスに入力すべきパスコードを表示するよう、Apple TVに要求する場合に選択します。
	AirPlay受信リクエストのパスワードを強制(tvOS 10.1まで)	AirPlayリクエスト受信に際して常にユーザーにパスワードの入力を求める場合に選択します。 デフォルト:選択なし
	iOSの全バージョン監視対象	
	Apple Booksを許可	Apple Booksアプリへのアクセスを許可する場合に選択します。
	iBooks Storeの不適切な内容を含む性的なコンテンツを許可(iOSとtvOS 11.3以降)	アダルトに分類されているiBooks Storeマテリアルのダウンロードをユーザーに許可する場合に選択します
	アカウント変更を許可	監視対象にあるiOS 7デバイスを使用しているユーザーがメールアカウントを追加したり、設定済みのメールアカウントに変更を加えたりできるようにする場合に選択します。

カテゴリ	設定	操作内容
	アプリのセルラーデータの変更を許可	ユーザーにアプリのセルラーデータ設定の変更を許可する場合に選択します。
	「友達を探す」の変更を許可	ユーザーに「友達を探す」アプリの設定の変更を許可する場合に選択します。
	Configurator以外のホストのペアリングを許可	iTunes同期のホストペアリングを許可する場合に選択します。このオプションを有効にすると、監視対象デバイスが管理ホスト以外のMacのiTunesと同期できるようになります。このオプションを無効にすると、管理ホストを除くすべてのホストペアリングが無効になります。管理ホスト証明書がまったく設定されていない場合は、すべてのペアリングが無効です。
	AirDropを許可	デバイス上でAirDropの使用を許可する場合に選択します。AirDropは、近隣のユーザーとのファイル共有を可能とするAppleの臨時Wi-Fiシステムです。この機能を制限することにより、機密性の高いドキュメントが不正なデバイスあるいはセキュアでないデバイスに漏えいすることを防ぎます。
	Touch ID / Face IDがデバイスをロック解除することを許可	Touch ID / Face IDによるデバイスのロック解除を許可する場合に選択します。
	Spotlight検索がインターネット検索結果を返すのを許可	Spotlightがインターネット検索結果を返すのを許可する場合に選択します。

カテゴリ	設定	操作内容
	アプリのSingle Appモードを許可	iOS監視対象デバイスで自動的にSingle Appモードを開始するアプリのバンドルIDリストをカンマ区切りで入力します。たとえば、学生に対してカスタム試験アプリを指定することができます。学生がそのアプリを起動したらアプリはすぐにSingle Appモードになり、試験中は他のリソースを使えないようになります。この機能は、自律的なSingle Appモード用に開発されたアプリにのみ適用されます。監視対象にするにはApple Configuratorを使用します。
	iOS 8+	
	企業レベルのブックのバックアップを許可	MDMを使用してデバイスにプッシュされたiBooks、ePubおよびPDFドキュメントの個人のバックアップを許可する場合に選択します。
	企業レベルのブックメモとハイライトの同期を許可	企業のブックに追加された注記やハイライトのiTunesへの同期を許可する場合に選択します。
	Apple Watch手首検出を強制	Apple Watchを装着している人がいなければ画面通知を非表示にする場合に選択します。
	iOS 8+監視対象	
	予測キーボードを許可	入力中の単語をiOSが予測できるようにし、ユーザーが3つの候補から1つをタップで選択して入力できるようにする場合に選択します。
	キーボードオートコレクトを許可	Bluetoothキーボードでのオートコレクトの使用を許可する場合に選択します。
	キーボードスペルチェックを許可	Bluetoothキーボードでのスペルチェックの使用を許可する場合に選択します。
	キーボード定義参照を許可	Bluetoothキーボードでの定義参照を許可する場合に選択します。

カテゴリ	設定	操作内容
	Touch ID指紋認証/Face ID顔認証の変更を許可	Touch IDまたはFace ID設定の変更を許可する場合に選択します。
	iOS 9+監視対象	
	iPad上のキーボードショートカットを許可	iPad上でキーボードショートカットを許可する場合に選択します。
	壁紙の変更を許可	ユーザーに壁紙画像の変更を許可する場合に選択します。
	Apple Watchとのペアリングを許可	iPhoneとApple Watchのペアリングを許可する場合に選択します。
	デバイス名の変更を許可	ユーザーにデバイス名の変更を許可する場合に選択します。
	企業向けアプリの信頼設定の変更を許可	ユーザーに企業向けアプリの信頼設定の変更を許可する場合に選択します。
	iOS 9.3+監視対象	
	通知設定の変更を許可	ユーザーに通知設定の変更を許可する場合に選択します。
	iOS 9.3.2+監視対象	
	診断送信の変更を許可	Appleへの診断データ送信に関する設定変更を許可する場合に選択します。
	iOS 10+監視対象	
	Bluetoothの変更を許可	監視対象デバイスでユーザーによるBluetooth設定の変更を許可する場合に選択します。これは、共有iPadで教育用Classroomアプリを使用し、アプリの実行にBluetoothが必要な場合などに使用します。
	iOS 10.3+監視対象	

カテゴリ	設定	操作内容
	口述記録を許可	ユーザーがiPhoneまたはiPadに文字入力の代わりに話すことを許可する場合に選択します。
	iOS 11+監視対象	
	AirPrintを許可	AirPrint機能での無線印刷を許可する場合に選択します。
	AirPrintの認証情報保存を許可	AirPrintユーザー名とパスワードのキーチェーン保存を許可する場合に選択します。
	AirPrintのiBeaconディスカバリを許可	ユーザーがAirPrintプリンターのiBeacon検出を設定するのを許可する場合に選択します。
	VPN構成の追加を許可	ユーザーによるVPN構成作成を許可する場合に選択します。
	AirPrintの信頼性のあるTLS要件を強制	TLS印刷通信用の信頼できる証明書を許可する場合に選択します。 デフォルト：選択なし
	システムアプリの削除を許可	システムアプリの削除を許可する場合に選択します。
	携帯電話プラン設定の変更を許可	ユーザーによる携帯電話プラン設定の変更を許可する場合に選択します。
	新しい近くのデバイスの設定を許可	ユーザーによる新しい近くのデバイスの設定を許可する場合に選択します。
	プロンプトなしでClassroomクラスに自動参加	ユーザーがプロンプトなしでClassroomクラスに自動参加するのを許可する場合に選択します。 デフォルト：選択なし
	Classroomがプロンプトなしでアプリとデバイスをロックすることを許可	ユーザーへのプロンプトなしでClassroomがアプリとデバイスをロックすることを許可する場合に選択します。

カテゴリ	設定	操作内容
		デフォルト：選択なし
	パスワードやクレジットカード情報がSafariやAppに自動入力される場合、その前に、強制的にユーザーが認証を行うようにする	デバイス所有者は、パスワードやクレジットカード情報がSafariやアプリケーションに自動入力される前に、強制的に認証する必要があります。 デフォルト：False
	iOS 11.3+	
	リモートアプリとのペアリングを許可（tvOS 11.3以降）	デバイスとリモートアプリのペアリングを許可する場合に選択します。
	AirPlayリクエストの受信を許可（tvOS 11.3以降）	AirPlayリクエストの受信を許可する場合に選択します。
	iOS 11.3+監視対象	
	USB制限モードを許可	ユーザーにUSB制限モードへのアクセスを許可する場合に選択します。
	ソフトウェア更新を30日間延期（iOS 11.3、tvOS 12.2以降、監視対象デバイスのみ）	ソフトウェア更新を遅らせたい日数を入力する場合に選択します。デフォルトは30日で、最大は90日です。 デフォルト：選択なし
	Classroom非マネージドクラスを出る際に教師の許可を要求	ユーザーが教師の許可を得てClassroom非マネージドクラスを出ることを許可する場合に選択します。
	iOS 12+監視対象	
	自動日時を強制（iOS 12.0およびtvOS 12.2以降）	日付と時刻の「自動設定」機能をオンにする場合に選択します。ユーザーはこれをオフにできません。 デフォルト：False

カテゴリ	設定	操作内容
	eSIM設定の変更を許可(iPhone XS、iPhone XS Max、iPhone XR - iOS 12.1以降のバージョン)	サポートされるデバイスでユーザーによるeSim構成の変更を許可する場合に選択します。またこのオプションにより、ユーザーはデバイスの設定から携帯電話プランの追加や削除ができなくなります。 デフォルト:True
	iOS 12.2+監視対象	
	個人ホットスポット設定の変更を許可	ユーザーによる個人ホットスポット設定の変更を許可する場合に選択します。 デフォルト:True
	iOS 13.0+	
	Filesのネットワークドライブアクセスを許可	ユーザーがFilesアプリでネットワークドライブに接続するのを許可する場合に選択します。 デフォルト:True
	FilesのUSBドライブアクセスを許可	ユーザーがFilesアプリで接続した任意のUSBデバイスに接続するのを許可する場合に選択します。 デフォルト:True
	iOS 13.0+監視対象	
	連続経路キーボードを許可	連続経路キーボード(スワイプまたはトレースタイピング)を有効化する場合に選択します。 デフォルト:True
	デバイスのスリープを許可	デバイスのスリープを有効化する場合に選択します。 デフォルト:True
	「デバイスを探す」を許可	Find Myアプリで「[デバイス]を探す」を有効化する場合に選択します。

カテゴリ	設定	操作内容
		デフォルト：True
	「友達を探す」を許可	Find Myアプリで「友達を探す」を有効化する場合に選択します。 デフォルト：True
	Wi-Fi電源を強制的にオン	Wi-Fi出力をオンにすることを許可する場合に選択します。 デフォルト：False
	iOS 13.4+	
	共有iPadのゲストセッションを許可	Falseの場合、共有iPadで一時セッションを利用できません。 デフォルト：True
	iOS 14.0+	
	Appleのパーソナライズド広告を許可	Falseの場合、Appleのパーソナライズド広告が制限されます。Appleはユーザー情報をターゲティング広告に使用できなくなります。これによって受信する広告数が少なることはないかもしれませんが、ユーザーに関連する広告が少なくなります。 デフォルト：True
	iOS 14.0+監視対象	
	App Clipsを許可	Falseの場合、ユーザーはApp Clipsを追加できず、デバイス上の既存のApp Clipsは削除されます。 デフォルト：True
	iOS 14.2+監視対象	

カテゴリ	設定	操作内容
	NFCを許可	Falseの場合、NFCは無効になります。監視対象デバイスが必要です。iOS 14.2以降で使用可能です。 デフォルト：True
	iOS 14.5+	
	自動ロック解除を許可	管理者は既存のallowAutoUnlock制約を使用してこの機能を管理できます。Falseの場合、自動ロックが禁止されます。macOS 10.12以降、iOS 14.5以降に対応しています。 デフォルト：True
	オンデバイスのみの文字起こしを強制	Trueの場合、文字起こしを目的としたSiriサーバーへの接続を無効化します。 デフォルト：False
	iOS 14.5+監視対象	
	ペアリングされていない外部ブートでの回復を許可	Trueの場合、ペアリングしていないデバイスによるブートでの回復が許可されます。 デフォルト：False
	許可済みネットワークのみにWi-Fi接続を強制	Trueの場合、構成プロファイルで設定されたWi-Fiネットワークにのみ接続するよう制限がかかります。 デフォルト：False **[許可済みネットワークのみにWi-Fi接続を強制]** 制約が有効でWi-Fi構成がデバイスに配布されていない場合、Wi-Fi接続は切断されます。
	iOS 15+	

カテゴリ	設定	操作内容
	オンデバイスのみの翻訳を強制	Trueの場合、デバイスは翻訳目的でSiriサーバーに接続しません。 デフォルト：False
	マネージドペーストボードを要求	Trueの場合、コピーと貼り付けの機能が`allowOpenFromManagedToUnmanaged`および`allowOpenFromUnmanagedToManaged`制約を尊重します。 デフォルト：False
	iOS 15.2以上	
	メールプライバシー保護を許可	オフの場合、デバイスでは、メールプライバシー保護が無効です。iOS 15.2以降で使用可能です。 Ivanti Neurons for MDM管理ポータルで[メールプライバシー保護を許可]構成がインストールされ、有効にされると、デバイスで[メールアクティビティの保護]トグルが有効になり、次のオプションが表示されます。 • **IPアドレスを非表示** - 電子メール送信者は、電子メールをオンラインアクティビティに関連付けたり、位置情報を判定したりできません。 • **すべてのリモートコンテンツをブロックする** - 電子メールの送信者は受信側の電子メールアクティビティを表示できません。 デフォルト：True
	iOS 15.4以上	
	Apple TVの自動スクリーンセーバーを許可(tvOS 15.4以降)	オフの場合、Apple TVの自動スクリーンセーバーが無効になります。tvOS 15.4以降で使用可能です。

カテゴリ	設定	操作内容
		デフォルト：True
	iOS 16.0+	
	高速セキュリティ対応インストールを許可	対応を無効化する場合。ユーザーは高速セキュリティ対応をインストールできません。
	高速セキュリティ対応削除を許可	ユーザーが対応を元に戻せないようにする場合。ユーザーは高速セキュリティ対応を削除できません。
アプリケーション	**iOSの全バージョン**	デバイス上のアプリケーションへのアクセスを有効化します。
	アプリのインストールを許可	ユーザーがApple App Storeからアプリをインストールできるようにする場合に選択します。App Storeを無効化し、ホーム画面からアイコンを削除する場合は選択しません。
	カメラ使用の許可	ユーザーにカメラの操作を許可する場合に選択します。カメラを無効化し、ホーム画面からアイコンを削除する場合は選択しません。
	Safariの使用を許可	Safari Webブラウザの使用を許可する場合に選択します。Safari Webブラウザを無効化し、ホーム画面からアイコンを削除し、さらにユーザーがWebクリップを開けないようにする場合は選択しません。
	オートフィルを許可	Safariのオートフィル機能を有効にする場合に選択します。
	不正警告を強制	ユーザーが不正または信用できないWebサイトとして特定されているサイトを閲覧するのを防ぐようSafariに指示する場合に選択します。
	JavaScriptを許可	SafariのJavaScriptサポートを有効にする場合に選択します。
	ポップアップをブロック	Safariのポップアップをブロックする場合に選択します。

カテゴリ	設定	操作内容
	iOSの全バージョン監視対象	
	アプリの削除を許可	ユーザーにデバイスからのアプリの削除を許可する場合に選択します。
	Game Centerの使用を許可	Game Centerへのアクセスを許可する場合に選択します。
	Game Centerの友人追加を許可	ユーザーにGame Centerへの友人の追加を許可する場合に選択します。
	マルチプレイヤーゲームを許可	ユーザーにマルチプレーヤー型のゲームの使用を許可する場合に選択します。
	iMessageを許可	iMessageの使用を許可する場合に選択します。
	cookieを承諾	[承諾する]、[常に承諾する]、[訪問したことのあるサイトからは承諾する] などを選択します。
	FaceTimeを許可	カメラが有効になっていて、ユーザーにFaceTimeの実行を許可する場合に選択します。
	iOS 8+	
	管理アプリケーションのクラウド同期の使用を許可	管理アプリケーションのクラウド同期の使用を許可する場合に選択します。
	アクティビティの継続を許可	Handoffに対応するアプリ内のアクティビティの継続を許可する場合に選択します。
	iOS 8+監視対象	
	ポッドキャストの使用を許可	ポッドキャストの使用を許可する場合に選択します。
	iOS 9+	
	新しい企業向けアプリ作成者を信頼	ユーザーに新しい企業向けアプリへのアクセスを許可する場合に選択します。

カテゴリ	設定	操作内容
	iOS 9+監視対象	
	App Storeを許可	ユーザーにApple App Storeへのアクセスを許可する場合に選択します。
	アプリの自動ダウンロードを許可	アプリによるファイル、データ、更新のダウンロードを許可する場合に選択します。ユーザーにはプロンプトが表示されます。
	Newsアプリを許可	Newsアプリの使用を許可する場合に選択します。
	iOS 9.3+監視対象	
	iTunes Radioを許可	iTunesラジオの使用を許可する場合に選択します。
	Apple Musicを許可	Apple Musicの使用を許可する場合に選択します。
	許可リストのアプリバンドルID	文字列に挙げたバンドルIDのみ表示や起動を許可する場合に選択します。すべてのWebクリップを許可するにはcom.apple.webappを含めます。
	ブロックされているアプリバンドルID	文字列に挙げたバンドルIDを表示または起動させない場合に選択します。すべてのWebクリップを制限するにはcom.apple.webappを含めます。
	iOS 13.0+監視対象	
	iTunes Storeの使用を許可	iTunes Music Storeの使用を許可する場合に選択します。iTunes Music Storeを無効化し、ホーム画面からアイコンを削除する場合は選択しません。

カテゴリ	設定	操作内容
iCloud	**iOSの全バージョン**	iCloudサービスへのアクセスを許可します。
	バックアップを許可	AppleのiCloudサービスを介したデータのバックアップを許可する場合に選択します。
	ドキュメント同期を許可	AppleのiCloudサービスを介したドキュメントの同期を許可する場合に選択します。
	フォトストリームの許可	AppleのiCloudサービスを介した、他のiOSデバイスとの写真の同期を許可する場合に選択します。
	共有フォトストリームを許可(禁止するとデータ損失の原因になる場合があります)	共有写真の同期を許可する場合に選択します。 このオプションを選択していない場合、写真が失われる可能性があります。
	キーチェーン同期を許可	キーチェーンの同期を許可する場合に選択します。
	iOS 9+	
	iCloudフォトライブラリを許可	iCloudフォトライブラリへのアクセスを許可する場合に選択します。
	iOS 15+監視対象	
	Cloud Privateリレーを許可	Falseの場合、iCloud Privateリレーは無効化されます。デフォルト:True

カテゴリ	設定	操作内容
セキュリティおよびプライバシー	**iOSの全バージョン**	セキュリティポリシーとプライバシーポリシーを許可します。
	無線配信による証明書の更新を許可	root証明書の無線更新を許可する場合に選択します。
	Ad Trackingを制限	Ad Tracking制限機能の使用を求める場合に選択します。
	iOSの全バージョン監視対象	
	構成プロファイルのインストールを許可	ユーザーに構成プロファイルと証明書のインタラクティブなインストールを許可する場合に選択します。
	アシスタントユーザーの生成コンテンツを許可	SiriがWebからユーザー生成のコンテンツをクエリするのを許可する場合に選択します。
	iOS 8+監視対象	
	リセットUIでユーザーがすべてのコンテンツおよび設定を消去するのを許可	デバイス上のiOSリセットUIで「すべてのコンテンツおよび設定の消去」を有効にする場合に選択します。
	スクリーンタイムを許可	スクリーンタイムを許可する場合に選択します([設定] > [スクリーンタイム])。
	Appleへの診断データの送信を許可	Appleへの診断データの自動送信を許可する場合に選択します。
	ユーザーによる信頼されていないTLS証明の承諾を許可	信頼できないHTTPS証明書の容認をデバイスユーザーに許可する場合に選択します。このオプションが選択されていない場合、デバイスはユーザーにプロンプトを表示することなく自動的に信頼できないHTTPS証明書を拒否します。
	暗号化バックアップを強制	iTunes経由での暗号化されたバックアップを要求する場合に選択します。SCEP要件のため、自動的に選択されます。

カテゴリ	設定	操作内容
	ユーザーにすべてのトランザクションでiTunes Storeパスワードの入力を強制	App Storeトランザクションを行う際は毎回iTunesパスワードを入力することをデバイスユーザーに強制する場合に選択します。このオプションが選択されていない場合、デバイスユーザーは一度の認証で複数のトランザクションを実行できます。
	iOS 9+	
	AirDropを管理されていない宛先として扱う	ユーザーにAirDropファイル共有へのアクセスを許可する場合に選択します。 デフォルト：False
	iOS 9+監視対象	
	デバイスのパスコードの変更を許可	ユーザーにデバイスのパスコード名の変更を許可する場合に選択します。
	iOS 12+	
	マネージドアプリが非マネージド連絡先アカウントに連絡先を書き込むことを許可	マネージドアプリが非マネージド連絡先アカウントに連絡先を書き込むことを許可する場合に選択します。 デフォルト：False
	iOS 12+監視対象	
	パスワードオートフィルを許可	iOSのオートフィルパスワード機能を有効にし、Safariやアプリで保存したパスワードを使用するかどうか尋ねる場合に選択します。

カテゴリ	設定	操作内容
	近くのデバイスによるパスワード要求の共有を許可	ユーザーのデバイスが近くのデバイスからパスワードを要求するのを許可する場合に選択します。
	パスワード共有を許可	ユーザーにAirdropパスワード機能とのパスワード共有を許可する場合に選択します。
	非マネージドアプリがマネージド連絡先アカウントから連絡先を読み出すことを許可	非マネージドアプリがマネージド連絡先アカウントから連絡先を読み出すことを許可する場合に選択します。 デフォルト：False

カテゴリ	設定	操作内容
コンテンツの評価		アプリとメディアへのアクセスを制御します。
	不適切な内容を含む音楽、ポッドキャスト、iTunes Uメディア(iOS 13+監視対象のみ、tvOS 11.3以降)の再生を許可	iTunes Storeから販売される際、レコードラベルなど性的な表現が露骨なコンテンツには、コンテンツプロバイダによってアダルトとしてのマークが付されます。
	評価エリア	アプリ、テレビ番組、映画に対するレーティング選択との関連で地域を変更するには、ドロップダウンリストから地域を選択します。

	動画	デバイスに保存されている映画のレーティング上限を以下から選択します。 • 映画を許可しない • G • PG • PG-13 • R • NC-17 • すべての動画を許可
	TV番組	デバイスに保存されているテレビ番組のレーティング上限を以下から選択します。 • TV番組を許可しない • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • すべてのTV番組を許可する

	アプリ	デバイスに保存されているアプリのレーティング上限を以下から選択します。 • アプリを許可しない • 4+ • 9+ • 12+ • 17+ • すべてのアプリを許可する

詳細は構成を作成するにはを参照してください。

会議室ディスプレイ

対象：tvOS 10.2およびサポートされる以降のバージョン。

この構成は、Apple TVで会議室ディスプレイモードをオンにします。会議室ディスプレイモードに設定すると、Apple TVがそのモードに固定され、他の用途では使用できません。

tvOS 10.2以降、監視対象のApple TVデバイスを会議室ディスプレイモードに設定可能となりました。会議室ディスプレイモードは、背景画像とスクリーンセーバーをApple TVのデバイス設定で手動で設定しない限り、対象Apple TVデバイスの壁紙を黒に固定し、デフォルトのスクリーンセーバーをダウンロードします。会議室ディスプレイ構成で設定されたメッセージも表示可能です。

会議室ディスプレイ構成は自動的に適用され、デバイスがこのモードにある間はアプリがインストールされます。会議室ディスプレイモードに設定されたデバイスは、再起動した場合、ホーム画面を表示することなく自動的にロック画面に戻ります。

Apple TVデバイスがシングルアプリモードの場合、または会議室ディスプレイにシングルアプリモードが適用されている場合、会議室ディスプレイはシングルアプリモードより優先されます。また、Apple TVデバイスがイーサネット経由でネットワークに接続している場合、会議室ディスプレイが自動的にWi-Fiネットワークを表示してAirPlay共有に参加することはありません。会議室ディスプレイ構成のカスタムメッセージフィールドを使用すると、この説明を画面に表示することができます。

会議室ディスプレイ構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに**[会議]**と入力し、**[会議室ディスプレイ]**構成をクリックします。
4. 名前と構成の説明を入力します。
5. **カスタムメッセージ**を指定します。これは、会議室ディスプレイモードの画面に表示されるカスタムメッセージです。
6. **[次へ]**をクリックして配布設定を行います。
7. **[完了]**をクリックします。

詳細は構成を作成するにはを参照してください。

ロックダウン& キオスク: Androidデバイス管 理 者 モード

ロックダウン& キオスク: Androidデバイス管 理 者 モード 構 成 では、Androidデバイスの一 部 の機 能 が無 効 化 され、キオスクモード でユーザーが利 用 できるアプリの許 可 リスト が作 成 されます。

Androidデバイス管 理 者 モード 構 成 は廃 止 されており、Android 8以 降 のバージョンのデバイスではサポートされていません。 Android 8以 降 のバージョンでのキオスクロックダウンには、Android Enterprise ロックダウンを使 用 することをお勧 めします。

Androidデバイスがキオスクモード の場 合 、設 定 やアプリを変 更 するオプションを制 限 できます。

- [ロックダウン& キオスク: Androidデバイス管 理 者 モード 構 成] ページでアプリを追 加 し、設 定 を選 択 します。
- 設 定 アイコンを使 用 して設 定 を変 更 するオプションは、キオスクモード で利 用 可 能 です。
- 設 定 構 成 オプションを選 択 せずにアプリを選 択 すると、設 定 アイコンがキオスクモード で表 示 されなくなります。
- 構 成 にアプリを含 めないことを選 択 した場 合 は、設 定 アイコンが表 示 されません。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ロックダウン設定：すべてのAndroidデバイスの機能を無効化します。	
Wi-Fiを無効化	無線LANへのアクセスをオフにする場合に選択します。
カメラを無効化	カメラアクセスをオフにする場合に選択します。
Bluetoothを無効化	Bluetooth機能をオフにする場合に選択します。 このオプションを使用する場合は注意が必要です。Ivantiは、ハンズフリーでのBluetoothアクセスが無効になるため、音声を無効にしないことを推奨します。運転中のデバイスのハンズフリー使用に関する法規制が一般的になりつつあるためです。
キオスクモード設定：特定の少数のアプリだけ動作させ、デバイスをキオスクとして利用できるようにします。 キオスクモード設定はAndroid 8.0以降のデバイスには適用されません。このようなデバイスの場合、デバイス詳細ページのキオスクステータスにUNSUPORTED_ON_DEVICEと表示されます。	
キオスクモードを有効化	Androidデバイス上でキオスクモードを構成する場合に選択します。
クイック設定を無効化	キオスクモードでクイック設定を無効化する場合に選択します。
ユーザーがWi-Fiの設定にアクセスできるようにする	ユーザーがWi-Fi設定を変更し、希望の無線ネットワークに接続できるようにする場合に選択します。
ユーザーがBluetoothの設定にアクセスできるようにする	ユーザーがBluetooth設定を変更し、追加のBluetoothデバイスをペアリングできるようにする場合に選択します。

ユーザーが位置情報の設定にアクセスできるようにする	ユーザーが位置情報設定にアクセスできるようにする場合に選択します。
ユーザーによるアプリケーション更新延期を許可	ユーザーによるアプリケーション更新延期を許可する場合に選択します。
キオスク終了PIN	エンドユーザーがキオスクモードを終了させるために入力しなければならない4ケタのコードを入力します。
アプリの許可リストを作成：許可されたアプリのリストにアプリを追加することにより、キオスクモードでユーザーが利用可能になります。ドラッグ&ドロップでアプリを順番に配置するとそれらがキオスクモードランチャに表示されます。 許可されたアプリのリストにアプリケーションを追加しても、デバイス上のアプリにはインストールされません。アプリのカタログ内の適切なユーザーおよびユーザーグループに各アプリを配布するようにしてください。	
ビルトインアプリ	キオスクモードで許可されるアプリグループ内にリストされたネイティブアプリを含めるには、[+追加]をクリックします。 上記のロックダウン設定でダイヤラーまたはカメラを無効化している場合は、許可されたアプリリストに追加できません。
アプリのカタログ	キオスクモードで許可されるアプリグループ内のアプリカタログからリストされたアプリを含めるには、[+追加]をクリックします。
その他のアプリ	Google Playストアで提供されていないアプリのパッケージ名を追加するには、[追加+]をクリックします。
キオスクモード可アプリ	キオスクモードで許可されるアプリグループからアプリを削除するには、Xをクリックします。キオスクデバイスに表示されるアプリの順序を変更するには、ドラッグ&ドロップします。

Knox Standard 4.0以降のSamsungデバイスの場合、マルチユーザー機能がキオスクモードに自動的にロックダウンされています。

Samsung以外のデバイスの場合、Android 8.0以降ではキオスクモードがサポートされていません。Android 8.0以降の場合、IvantiではAndroid Enterpriseのロックダウン機能をキオスクモードに使用することを推奨します。

関連トピック:

- Android対応キオスクモードの設定
- 構成を作成するには

Android対応キオスクモードの設定

このセクションは以下のトピックを含みます。

- キオスクモードのリモート起動
- キオスクモードの終了

ライセンス: Silver

Androidデバイス対応キオスクモードでは、指定のアプリのみにデバイスの使用を制限できます。キオスクモードを利用し、仕事用のアプリのみ使用する従業員向けにデバイスを設定することも可能です。

Androidデバイスをキオスクモード、またはキオスク付きのデバイス所有者モード用に準備する場合は、キオスクモードでユーザーが利用できるようにするアプリの許可リストを作成する必要があります。デバイス所有者を利用しているデバイスの場合は、ドラッグ＆ドロップで許可されたアプリリストにアプリを追加し、アプリの構成時にキオスクモードランチャに表示される順序でアプリを配置できます。詳細は、ロックダウン＆キオスク構成を参照してください。

前提条件

Androidデバイス対応キオスクモードを構成する前に、以下を必ず確認してください。

- Goをデバイスにインストールした。
- キオスク構成で必要なアプリがアプリカタログに入っている。
- キオスクモードで動作するデバイスにアプリカタログが配布されている。

  SonimXP5Sデバイスはキオスクモードをサポートしません。

- キオスク構成で必要なアプリがインストールされている。
- (任意) Androidキオスクのブランディングを設定する。

キオスクモードは Android 5.1および6.0でサポートされています。Samsung Knox以外のデバイスはデバイス所有者モードに設定し、不要なアプリケーションの使用を防止する必要があります。

重要: 一部のデバイスは、画面オーバーレイなどキオスクモードを回避する機能を持っています。Samsung Galaxy S6 EdgeのPeople Edgeもそのような機能の例です。これらは、デバイスを導入する前に管理者がオフにすることをお勧めします。

手順

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[ロックダウン& キオスク: Androidデバイス管理者モード]** をクリックします。
4. **[設定を作成]** 画面で、少なくとも **[キオスクモード設定]** セクションを完成させます。
5. **[配布]** 画面で、この構成を受信するデバイスグループを選択します。
6. **[完了]** をクリックします。
7. Samsung以外のデバイスについては、さらに以下の手順を行います。
   a. **[デバイス]** > **[デバイス]** を開きます。
   b. キオスクモードを有効にしたいデバイスを選択します。
   c. **[アクション]** > **[チェックインの強制]** を選択します。
   d. デバイスで、**[キオスクモード]** ボタンをタップします。
   e. デバイスの **[ホーム]** ボタンを押します。
   f. **[ランチャーを選択]** ダイアログが表示されたら **[Goキオスクランチャー]** をタップし、**[常に]** を選択します。この機能に適切なランチャを確実に使用するためには、この手順が必要です。この手順を実行しない場合、ユーザーがランチャの選択を求められます。

キオスクモードのリモート起動

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. 画面に[キオスクモード]カラムを追加します。
3. キオスクモードを有効にしているが、現在、キオスクモードではないデバイスを選択します。
4. **[アクション]** > **[キオスクモードを開始]** を選択します。

キオスクモードの終了

構成でPINを設定すると、デバイスでキオスクモードを終了できます。

手順

1. **[設定]** アイコンをタップします。
2. **[キオスクモードの終了]** を選択します。
3. 指示に従って **[キオスクPIN]** フィールドをタップします。
4. キオスクPINを入力します。

ポータルから特定のデバイスのキオスクモードを終了することも可能です。

手順

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイスの詳細を表示します。
3. **[アクション]** > **[キオスクモードを終了]** を選択します。

以下の方法でキオスクモードを終了することも可能です。

- 構成の削除
- 構成の無効化
- 構成からのデバイスグループ削除

Android共有デバイスキオスクの設定

企業では、ユーザーの特定の役割にカスタマイズした専用Androidデバイスをスタッフに提供することがあります。デバイス上のアプリや構成はユーザーのプロファイルによって異なります。たとえば技術系の従業員は自分に必要なアプリ群を持ち、メンテナンス担当のユーザーは別のアプリ群にアクセスします。

Android共有デバイスキオスクモードは、デバイスを共有するさまざまなユーザーグループに対応するアプリフィルターとして機能します。共有デバイスキオスクにログインしたユーザーは、自分の役割に必要なアプリしか見ることができません。共有デバイスキオスクの大きなメリットは、同じデバイスでもユーザーグループによって異なるアプリ群にアクセスできることです。ユーザーが共有デバイスキオスクからログアウトすると、アプリやユーザーデータ(履歴を含む)は、次にログインしたユーザーには表示されません(アプリに再インストールがマークされている場合)。共有デバイスキオスクは、Androidエンタープライズで管理するデバイスとマネージドGoogle Playアカウントでのみ使用可能です。

共有デバイスキオスクには、ステージングユーザーと共有キオスクユーザーの2種類のユーザー、そしてそれらのユーザーに対応する2つ以上のポリシーが必要です。ステージングユーザーは、共有デバイス上にログイン画面を表示させます。また、実際のキオスクデバイスに他のユーザーのログインを許可する特殊な管理ユーザーでもあります。共有デバイスキオスクユーザーがログインに成功すると、ステージングポリシーが共有キオスクポリシーに交代します。キオスクユーザーは、デバイスに指定されたポリシーに従ってインストールされたアプリにアクセスします。複数の共有キオスクポリシーを作成することは可能ですが、キオスクデバイス上で同時に有効化できるキオスクポリシーは1つだけです。キオスクユーザーが共有キオスクからログアウトすると、デバイスはステージングユーザーとステージングポリシーに戻ります。

ステージングユーザーは、ログインページにしかアクセスできません。したがって、ステージングポリシーはこのユーザー専用に作成する必要があります。一方、共有デバイスキオスクユーザーは、共有デバイスキオスクユーザー用のポリシーに定義したアプリ群にアクセスできます(当然、共有デバイスのキオスクデバイスに許可されたアプリケーションをインストールする必要があります。)共有デバイスのキオスクポリシーにより、以前にインストールしたすべてのアプリケーションから許可されたアプリケーションを絞り込むフィルタを作成できます。Android共有キオスクポリシーにアプリを直接アップロードすることはできません。通常は、組織に応じて、共有キオスクユーザーまたはユーザーグループに専用の共有キオスクポリシーを作成します。たとえば、昼勤務と夜勤務の従業員が別の役割を持ち、別のアプリ群にアクセスする必要のある企業もあるでしょう。このような場合は、昼勤務用のポリシーと夜勤務用のポリシーを作成します。

共有デバイスキオスクの有効化については、「ロックダウン& キオスク: Android Enterprise」 ページ571をご覧ください。

ロックダウン& キオスク: Android Enterprise

ロックダウン& キオスク: Android Enterpris構 成 では、Android Enterpriseデバイスの一 部 の機 能 が無 効 化 され、キオスクモード でユーザーが利 用 できるアプリの許 可 リスト が作 成 されます。

このセクションは以 下 のトピックを含 みます。

- ロックダウン設 定
- 仕 事 用 プロファイル
- 仕 事 用 マネージド デバイスのロックダウン設 定
- 仕 事 用 プロファイルを持 つマネージド デバイス(Android 8～ 10)と会 社 所 有 デバイス上 の仕 事 用 プロファイル(Android 11以 降)

ロックダウン設定

設定	説明
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ロックダウンの種類を選択	構成したいロックダウン設定の種類を選択します。 • 仕事用プロファイル • 仕事用マネージドデバイス(デバイス所有者およびキオスクモード設定) • 仕事用プロファイルを持つマネージドデバイス/会社所有デバイス上の仕事用プロファイルのロックダウン設定 会社所有デバイス上の仕事用プロファイルのロックダウン設定は、Android 11以降のデバイスにのみ適用されます。 1つの構成につき、許可されている種類は1つのみです。表示されるオプションは、選択した種類により異なります。 仕事用マネージドデバイス(デバイス所有者)と「会社所有デバイス上の仕事用プロファイル」構成を持つマネージドデバイスを同じデバイスに配布した場合、仕事用プロファイル構成を持つマネージドデバイスが優先されます。

仕事用プロファイル

Android Enterpriseデバイスで特定の機能を無効化します。

設定	操作内容	対象デバイス
スクリーンキャプチャを無効化	デバイスのビルトイン画面キャプチャ機能を利用できないようにする場合に選択します。	• Android 5.0+
アプリ制御を禁止	ユーザーが[設定]やランチャでアプリケーションを変更できないようにする場合に選択します。	• Android 5.0+
構成認証情報を禁止	ユーザーがユーザーの認証情報を構成できないようにする場合に選択します。	• Android 5.0+
プロファイル間のコピー貼り付けを禁止	プロファイル間で情報をコピー/貼り付けをできないようにする場合に選択します。	• Android 5.0+
アカウント変更を禁止	ユーザーがアカウントの追加や削除をできないようにする場合に選択します。	• Android 5.0+
Beamの送信を禁止	ユーザーがNFCを使用してアプリデータを送信できないようにする場合に選択します。	• Android 5.1+
位置情報共有を禁止	ユーザーがデバイスの位置情報をアプリに公開できないようにする場合に選択します。	• Android 5.0+
デバッグ機能を禁止	デバイスでデバッグ機能を無効化する場合に選択します。このオプションはデフォルトでオンになっています。	• Android 5.0+

設定	操作内容	対象デバイス
アプリ検証を確認	デバイスでアプリケーション検証機能を許可する場合に選択します。このオプションはデフォルトでオンになっています。 このオプションをオフにすると、デバイスごとに異なるデフォルト動作に戻ります。	• Android 5.0+
デバイス上の不明なソースを無効化	デバイスが不明なソースからアプリをインストールするのを防ぐ場合に選択します。 この設定をデバイスで有効にするには、この機能を有効化するGoogle Playの更新を実行する必要があります。	• Android 5.0+

設定	操作内容	対象デバイス
入力方法を制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、許可リスト化されたIMEパッケージ名を制限します。デバイスは、許可リスト化されたパッケージ入力方式とデフォルトのシステム入力方式の両方に対応します。 ユーザーはデフォルトのシステム入力方式と許可リスト化されたパッケージ入力方式を切り替えることができます。 Android 10+の場合、仕事用プロファイル側のIMEアプリにのみ許可リスト化が適用されます。それより前のAndroidバージョンについては、許可リスト化がデバイス全体のIMEアプリに適用されます(仕事用プロファイル内外を問わず)。	• Android 5.0+
アクセシビリティサービスを制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、仕事用アプリのアクセシビリティサービスを制限する場合に選択します。許可リスト化されたパッケージがない場合は、システムアクセシビリティサービスのみ許可されます。	• Android 5.0+

設定	操作内容	対象デバイス
仕事用プロファイル内で不明なソースを無効化	仕事用プロファイル内で不明なソースからのダウンロードを許可しない場合に選択します。	• Android 5.0+
システムアプリを有効化/無効化	**[システムアプリパッケージ名]** フィールドを通じてパッケージ名の2つのリストを指定することにより、導入するシステムアプリケーションを有効化/無効化する場合に選択します。 この機能を使用し、Google Playに公開されていないシステムアプリへのアクセスを管理してください。 アプリをアプリカタログとシステムアプリリストの両方に追加することはできません。	• Android 5.0+
発信者IDを無効化	着信の際、仕事用プロファイルの発信者ID情報がデバイスに表示されるかどうかを設定します。	• Android 6.0+
Bluetooth経由での連絡先共有を禁止	デバイスが連絡先をBluetooth経由で他のデバイスと共有できないようにする場合に選択します。	• Android 6.0+
検索経由での連絡先共有を禁止	ユーザーが仕事用連絡先を個人用電話アプリから検索できないようにする場合に選択します。	• Android 7.0+
オートフィルを禁止	オートフィルを禁止する場合に選択します。	• Android 8.0+

設定	操作内容	対象デバイス
個人用プロファイルで仕事用アプリ通知を禁止	仕事用プロファイルの通知を制限する場合に選択します。	• Android 8.0+
印刷を禁止	すべてのアプリからの印刷を制限する場合に選択します。	• Android 9.0+
プロファイルへの共有を禁止	ユーザーが個人データをデバイスの仕事用プロファイルに共有するのを禁止する場合に選択します。	• Android 9.0+

設定	操作内容	対象デバイス
仕事用プロファイルカレンダーへのアクセスを許可	すべてのアプリまたは個人側にある一部のアプリが仕事用プロファイル内のカレンダー情報にアクセスできるようにする場合は、以下のいずれかを選択します。 • **個人用プロファイルのすべてのアプリ** - すべてのアプリが仕事用プロファイル内のカレンダー情報にアクセスすることを許可します。 • **個人用プロファイルの以下のアプリのみ** - 以下のテキストフィールドにアプリのバンドルIDをカンマ区切りで入力します。ここで個人側で選択されたアプリだけが、仕事用プロファイル内のカレンダー情報へのアクセスを許可されます。 個人側のアプリが共有カレンダーにアクセスするには、専用のAPIを実装する必要があります。	• Android 10.0+

設定	操作内容	対象デバイス
アプリのプロファイル横断型許可リスト化を有効化	チェックボックスを選択すると、ユーザーが仕事用プロファイル内にある特定のアプリからの情報をデバイスの個人側と共有できます。 **[許可リストアプリ]** フィールドにアプリのパッケージIDを入力するとアプリが許可リストに入り、コンマ区切りで表示されます。 デフォルトでは無効化されています。	• Android 11.0+
5G ネットワークスライシングを有効にする	選択すると、会社所有デバイスの仕事用プロファイルで5Gネットワークスライシングオプションが提供されます。 デフォルトでは無効化されています。	• Android 12.0+

仕事用マネージドデバイスのロックダウン設定

Android 5.0+において、仕事用マネージドデバイス(デバイス所有者) の特定の機能を無効化します。

設定	説明
Wi-Fiを無効化	無線LANへのアクセスをオフにする場合に選択します。
Wi-Fi設定を無効化	ワイヤレス設定へのアクセスをオフにする場合に選択します。
カメラを無効化	カメラアクセスをオフにする場合に選択します。
Bluetoothを無効化 (Android 8.0+)	Bluetooth機能をオフにする場合に選択します。 このオプションを使用する場合は注意が必要です。Ivantiは、ハンズフリーでのBluetoothアクセスが無効になるため、音声を無効にしないことを推奨します。運転中のデバイスのハンズフリー使用に関する法規制が一般的になりつつあるためです。
Bluetooth設定を禁止 (Android 8.0+)	Bluetooth設定へのアクセスをオフにする場合に選択します。
スクリーンキャプチャを無効化	デバイスのビルトイン画面キャプチャ機能を利用できないようにする場合に選択します。
マスターボリュームをミュート	マスターボリュームをミュートする場合に選択します。
アプリ制御を禁止	ユーザーが[設定]やランチャでアプリケーションを変更できないようにする場合に選択します。
認証情報を禁止	ユーザーがユーザーの認証情報を構成できないようにする場合に選択します。
緊急ブロードキャストを禁止	緊急ブロードキャストを禁止する場合に選択します。

設定	説明
モバイルネットワークを禁止	モバイルネットワークへのアクセスをオフにする場合に選択します。 Wi-Fiが無効の場合、無効にすることはできません。
テザリングを禁止	あるデバイスがインターネット接続を使用して別のデバイスへインターネットアクセスを提供するためのオプションであるテザリングをオフにする場合に選択します。
VPNを禁止	VPN接続をオフにする場合に選択します。
工場出荷時設定へのリセットを禁止	ユーザーがデバイスを工場出荷時設定へ戻せないようにする場合に選択します。
工場出荷時設定へのリセットを有効化	ユーザーがデバイスを工場出荷時設定に戻すのを許可する場合に選択します。 工場出荷時設定へのリセットの後でデバイスをプロビジョニングできる許可済みのGoogleアカウントID(整数値)のリストを指定することも可能です。またはヘルプアイコンの上にマウスを置くと、許可済みアカウントの取得方法が表示されます。
アカウント変更を禁止	ユーザーがアカウントの追加や削除をできないようにする場合に選択します。
NFC(ビーム発信)を禁止	ユーザーがNFCを使用してアプリデータを送信できないようにする場合に選択します。
発信を禁止	ユーザーによる発信を禁止する場合に選択します。
セーフブートを禁止 (Android 6.0+)	ユーザーがセーフブートモードでデバイスを再起動できないようにする場合に選択します。
位置情報共有を禁止	ユーザーがデバイスの位置情報をアプリに公開できないようにする場合に選択します。
デバッグ機能を禁止	デバイスでデバッグ機能を無効化する場合に選択します。このオプションはデフォルトでオンになっています。

設定	説明
アプリ検証を確認	デバイスでアプリケーション検証機能を許可する場合に選択します。このオプションはデフォルトでオンになっています。 このオプションをオフにすると、デバイスごとに異なるデフォルト動作に戻ります。
SMSを禁止	ユーザーがSMSメッセージの送受信をできないようにする場合に選択します。
マイクのミュート解除を禁止	ユーザーがデバイスのマイクのミュートを解除できないようにする場合に選択します。
オートタイムを禁止	ユーザーが自動時間変更をできないようにする場合に選択します。
オートタイムゾーンを禁止	ユーザーがタイムゾーン変更によるデバイスの自動的な時間調整を有効化できないようにする場合に選択します。
サーバーと時刻を同期 (Android 9.0+)	最初は登録時、その後はチェックイン後24時間ごとに、デバイスにIvanti Neurons for MDMサーバーとの時間同期を許可する場合に選択します。このオプションは、**[オートタイムを無効化]**を選択した場合のみ表示されます。
タイムゾーンを設定 (Android 9.0+)	タイムゾーンの文字列は、オルソンタイムゾーンID形式 (例：太平洋/ミッドウェー) で指定します。
データローミングの無効化	デバイスのローミング時のデータ交換をオフにする場合に選択します。
Wi-Fiスリープを無効化	デバイスがスリープモードにあるときにWi-Fiのオン状態を維持する場合に選択します。

設定	説明
入力方法を制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、許可リスト化されたIMEパッケージ名を制限します。デバイスは、許可リスト化されたパッケージ入力方式とデフォルトのシステム入力方式の両方に対応します。 ユーザーはデフォルトのシステム入力方式と許可リスト化されたパッケージ入力方式を切り替えることができます。 Android 10+の場合、デバイス側のIMEアプリにのみ許可リスト化が適用されます。それより前のAndroidバージョンについては、許可リスト化がデバイス全体のIMEアプリに適用されます。
アクセシビリティサービスを制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、仕事用アプリのアクセシビリティサービスを制限する場合に選択します。許可リスト化されたパッケージがない場合は、システムアクセシビリティサービスのみ許可されます。
USBファイル転送を無効化	USBファイル転送を無効化する場合に選択します。
外付けメディアを無効化	外付けメディアを無効化する場合に選択します。
キーガードを無効化(PIN/パスコードが設定されている場合は無効)	キーガードを無効化する場合に選択します。このオプションを選択しても、パスワード、PIN、パターンが設定されている場合は影響を与えません。 キーガードを無効化した後、パスワード、PIN、パターンを設定した場合も、キーガードの無効化が中止されます。
電源接続時は画面のオン状態を維持	電源に接続したときは画面をオンのままにする場合に選択します。デバイスを電源に接続している間は、画面が暗くなることはあってもオフにはなりません。 この設定は、自動ロックやパスコード設定の無活動タイムアウトが設定されていない場合に限って有効です。
ウィンドウの作成を禁止	アプリが、特定のオーバーレイウィンドウ(アラートやトースト通知など)を表示しないようにする場合に選択します。

設定	説明
最初の使用ヒントをスキップ	システムリコメンデーションを有効化し、最初のアプリ起動時にユーザー向けチュートリアルや他の基本的な説明をスキップする場合に選択します。
デバイス上の不明なソースを禁止	デバイスが不明なソースからアプリをインストールするのを禁止する場合に選択します。
ロック画面のメッセージを設定 (Android 7.0+)	デバイスに表示するロック画面のメッセージを設定する場合に選択します。ロック画面のメッセージをテキストフィールドに入力します(256文字まで)。このオプションを有効化すると、ユーザーが[設定]でメッセージを設定できなくなり、管理者が設定したメッセージがユーザーに表示されます。 「ロック画面のメッセージを設定」を有効化した後、管理者がロック画面のメッセージを設定しない場合でも、ユーザーは[設定]でメッセージを設定できず、ユーザーには何のメッセージも表示されません。
画面の明るさを設定	デバイスの画面の明るさを設定する場合に選択します。 • 手動 - 手動で数値(0～255)を入力する場合に選択します • 適応的 - 明るさをデバイスに設定させる場合に選択します [明るさの構成を禁止]オプションを有効にしてから、デバイスの画面の明るさを設定することをお勧めします。
スクリーンタイムアウトを設定	スクリーンタイムアウトの期間(秒)を設定する場合に選択します。 [スクリーンタイムアウトの構成を禁止]オプションを有効にしてから、デバイスの画面の明るさを設定することをお勧めします。
画面の向きを設定	画面の向きを設定する場合に選択します。ドロップダウンリストから、画面の向きを0度、90度、180度、または270度に設定できます。 デフォルトではこのオプションは選択されていません。Goアプリのバージョン89以降では、キオスク時にデバイスをポートレートモードのままにするには、このオプションを選択し、値を0に設定する必要があります。

設定	説明
システムアプリを有効化/無効化	**[システムアプリパッケージ名]** フィールドを通じてパッケージ名の2つのリストを指定することにより、導入するシステムアプリケーションを有効化/無効化する場合に選択します。この機能を使用し、Google Playに公開されていないシステムアプリへのアクセスを管理してください。 アプリをアプリカタログとシステムアプリリストの両方に追加することはできません。
Android 8.0+	
オートフィルを禁止	ユーザーがオートフィル機能を使用するのを禁止する場合に選択します。
Bluetooth共有を禁止	ユーザーがデバイスでBluetooth接続を共有するのを禁止する場合に選択します。
バックアップサービスを無効化	バックアップサービスを無効にする場合に選択します。
Android 9.0+	
印刷を禁止	ユーザーによる印刷を禁止する場合に選択します。
機内モードを禁止	デバイス全体に関して機内モードを禁止する場合に選択します。
アンビエントディスプレイを禁止	ユーザーがアンビエントディスプレイを使用するのを禁止する場合に選択します。
明るさの構成を禁止	ユーザーが明るさを設定するのを禁止する場合に選択します。 [画面の明るさモードを設定]を定義してから、このオプションを選択することをお勧めします。
日時の構成を禁止	日付、時刻、タイムゾーンの設定を禁止する場合に選択します。

設定	説明
位置情報の構成を禁止	ユーザーが位置情報プロバイダーを無効化するのを禁止する場合に選択します。
スクリーンタイムアウトの構成を禁止	ユーザーがスクリーンタイムアウトまでの時間を変更するのを禁止する場合に選択します。 [スクリーンタイムアウトを設定]値を定義してから、このオプションを選択することをお勧めします。
Android 12.0+	
充電時にのみUSBを有効にする	選択すると、充電時にのみUSBポートを有効にします。
Android 13.0+	
最低限必要なWi-Fiセキュリティの設定	次のように最低限必要なWi-Fiセキュリティを設定する場合に、このオプションを使用します。 • 最低セキュリティ要件なし –最低限のセキュリティが必要ない場合に、このオプションを選択します。 • 個人ネットワークベースのセキュリティ– WEP、WPA/WPA2/WPA3など、個人のWi-Fiネットワークをブロックする場合は、このオプションを選択します。 • エンタープライズEAPネットワークベースのセキュリティ – EAPプロトコルベースのWi-Fiネットワークをブロックする場合は、このオプションを選択します。 • エンタープライズ192ネットワークベースのセキュリティ - EAP企業ベースのWi-Fiネットワークをブロックする場合は、このオプションを選択します。 最低限の基準を満たしていない既存のデバイスはすべて切断されます。 デバイスの詳細の**[一般] > [Wi-Fiセキュリティレベル]**に、最低限必要なWi-Fiセキュリティレベルが表示されます(ある場合)。

設定	説明
キオスクモード設定：キオスクモードは、カスタマイズされたランチャ経由によるアプリへのアクセス制限を含むデバイスに、追加の制限を適用します。	
キオスクモードを有効化	Androidデバイス上でキオスクモードを構成する場合に選択します。 • ユーザーが共有キオスクモードにログインしてログアウトした場合、そのユーザー名は次回のログイン時にもGoクライアントで利用可能です。共有キオスクモードでは、Goクライアントに現在使用中の7つのユーザー名が保存されます。 • 共有キオスクモードがIDP認証に対応するようになりました。このため、Ivanti Neurons for MDM がIDPで構成されていれば、共有キオスクモードをIDP認証で利用できます。

設定	説明
タスクモードのロックを有効化	Androidデバイスでロックタスクモードを有効化する場合に選択します。有効化すると、デバイスがキーガード、ステータスバー、セーフモードを表示可能になります。このオプションはデフォルトでは無効化されています。 以下は、Android 9またはサポートされる以降のバージョンでロックタスクモードが有効化された場合に表示される追加設定です。 **設定アイコン** - デバイス設定アプリに依存するシステム機能に、アプリがアクセスできるようになります。デバイス設定を許可することで、アプリからのBluetoothペアリングなどの場面で、ロックタスクモード違反を回避できます。特定のアプリではこの設定を有効のままにしておくことをお勧めします。 **システム情報** - 日時、接続、バッテリー、バイブレーションモードをステータスバーに表示します。このオプションはデフォルトでは無効化されています。 **キーガード**(デフォルトで有効) - ロックタスクモードでキーガードを有効にします。 **グローバルアクション**(デフォルトで有効) - ユーザーが電源ボタンを長押ししたときに表示されるメニューを有効化します。このオプションが無効化されている場合、ユーザーはデバイスの電源を切れない場合があります。 **ホームボタン** - ホームボタンを有効化します。このオプションはデフォルトでは無効化されています。有効化すると、以下のサブオプションが表示されます: • **概要ボタン**(デフォルトで無効) - ロックタスクモードで概要ボタンおよび概要画面を有効化します。 • **通知**(デフォルトで無効) - ロックタスクモードで通知を有効化します。これはステータスバー上のアイコン、ヘッドアップ通知、拡張可能な通知シェードを含みます。 ホームボタンオプションが有効化されていない場合、ユーザーはマルチウィンドウ機能を使用できません。
キオスクを自動で入力(初期セットアップ時のみ)	構成を適用すると、キオスクモードを自動的に許可する場合に選択します。

設定	説明
Android 5デバイスのクイック設定を無効化	Android 5を実行するデバイスのキオスクモードでクイック設定を無効化する場合に選択します。
Android 6+とすべてのSamsungデバイスのクイック設定を無効化	Android Enterpriseデバイス(バージョン6から最新版まで) およびSamsungデバイスのキオスクモードでクイック設定を無効化する場合に選択します。 この設定を無効化しても、デバイスの通知アイコンと通知音はブロックされません。
ユーザーがWi-Fiの設定にアクセスできるようにする	ユーザーがWi-Fi設定を変更し、希望の無線ネットワークに接続できるようにする場合に選択します。
ユーザーがBluetoothの設定にアクセスできるようにする	ユーザーがBluetooth設定を変更し、追加のBluetoothデバイスをペアリングできるようにする場合に選択します。
ユーザーが位置情報の設定にアクセスできるようにする	ユーザーが位置情報設定にアクセスできるようにする場合に選択します。
ユーザーによるアプリケーション更新延期を許可	ユーザーによるアプリケーション更新延期を許可する場合に選択します。
ユーザーが日時設定にアクセスできるようにする	ユーザーが日時設定にアクセスできるようにする場合に選択します。

設定	説明
ユーザーがネットワークの設定にアクセスできるようにする	ユーザーがモバイルネットワーク設定にアクセスできるようにする場合に選択します。
ユーザーによる言語の選択を許可	ユーザーによる言語設定へのアクセスを許可する場合に選択します。

設定	説明
共有デバイスを有効化	共有デバイスキオスクでは、デバイスが複数のエンドユーザーに共有されます。このオプションによりキオスクモードのデバイスも共有が許可されます。 • **ログインを有効化**：このオプションはキオスク管理ユーザー用です。デバイスにこのオプションを設定すると、エンドユーザーが共有デバイスキオスクにログインするためのユーザーログイン画面が表示されます。 ログイン有効化オプションは、ユーザーがAndroid Enterpriseデバイスアカウントユーザー(ステージングユーザー)として作成された場合のみ表示されます。 **[ドメイン置換を使用]**を選択し、適切にドメインを入力します。 このオプションではユーザー名のドメインサフィックスが確認されます。ドメインサフィックスがない場合、システムは自動的にドメインサフィックスをユーザー名の最後に追加します。 • **ログアウトを有効化**：デバイスにこのオプションを設定した場合、ログインしたユーザーが許可リストにあるアプリにアクセスできます。このユーザーにはログアウトのオプションが表示されますが、キオスクは終了できません。ユーザーが共有デバイスキオスクからログアウトすると、別のユーザーが共有デバイスキオスクにログインし、管理者が構成したアプリを閲覧できます。 • アプリのリサイクルアイコンは、ログインごとにアプリを再インストールする場合に使用します。このオプションはローカルにデータをキャッシュするアプリに使用されます。 管理者が発行したキオスク終了PINがあれば、ユーザーはキオスクモードを終了できます。 • **タイムアウト**：タイムアウトを時間単位で指定します。たとえばタイムアウトが2時間に設定され、エンドユーザーが共有デバイスキオスクからログアウトできない場合、ログアウトは2時間後に自動的に実行されます。 **[タイムアウト]**フィールドは**[ログアウトを有効化]**オプションが選択されている場合のみ表示され、入力は任意です。 デバイス詳細ページの**[Android enterpriseキオスクからサインアウト]**オプションをクリックしても、共有キオスクモードからエンドユーザーをログアウトできます。

設定	説明
FIDO 認証を許可 (デバイスで Google Chrome アプリが必要)	このオプションをオンにすると、共有キオスクを使用しているときに、ユーザーの FIDO 認証を使用できます。ユーザーがデバイスへのログインで FIDO キーを使用することを許可します。 Google Chrome は唯一のサポートされているブラウザです。共有キオスクで利用可能にするには、FIDO 認証用にデバイスで提供する必要があります。
ユーザーによる明るさと自動回転の構成を許可	ユーザーが明るさと自動回転を設定するのを許可する場合に選択します。
マルチウィンドウを有効化	Samsungデバイス(デバイス所有者キオスク) で複数アプリの同時表示を許可する場合に選択します。 ロックタスクモードでマルチウィンドウを許可するには、次のロックタスクモードオプションも有効化する必要があります。 • **ホームボタン** • **概要ボタン**
キオスクのブランディング	デフォルトまたはカスタムブランディングオプションをドロップダウンリストから選択します。
キオスク終了 PIN	ユーザーがキオスクモードを終了させるために入力しなければならない6桁のPINを入力します。PINでは6～10桁にする必要があります。このPINは、キオスクモードですべてのデバイスに適用されます。 以前、キオスクPINの長さは4桁でした。以前のバージョンから Ivanti Neurons for MDM 82へのアップグレード後も、引き続き4桁のPINをご使用いただけます。ただし、設定を変更した場合は、PINの長さを新しい要件 (6～10桁) に合わせて設定する必要があります。 Goアプリは、ブルートフォース攻撃からデバイスを保護します。詳細はAndroid対応Goのドキュメンテーションを参照してください。

設定	説明
アプリの許可リストを作成：許可されたアプリのリストにアプリを追加することにより、キオスクモードでユーザーが利用可能になります。ドラッグ＆ドロップでアプリを順番に配置するとそれらがキオスクモードランチャに表示されます。 許可されたアプリのリストにアプリケーションを追加しても、デバイス上のアプリにはインストールされません。アプリのカタログ内の適切なユーザーおよびユーザーグループに各アプリを配布するようにしてください。	
ビルトインアプリ	キオスクモードで許可されるアプリグループ内にリストされたネイティブアプリを含めるには、[+追加]をクリックします。 キオスクモード可アプリの設定には、次のオプションがあります。 • **アプリのユーザーデータのクリア:** このオプションを有効化すると、ユーザーがキオスクからログアウトしたときに、すべてのアプリケーションデータがユーザーの操作なしで自動的に消去されます。 アプリケーションでこのオプションを使用するには、キオスクモード設定で **[共有デバイスを有効化]** を選択します。 ◦ Google Chromeとwebviewパッケージに関しては、ユーザーデータのクリアを有効化してアプリの許可リストに追加してもアプリデータがクリアされません。この2つのパッケージのアプリデータをクリアするとキオスクがクラッシュする可能性があるためです。 ◦ アプリランチャーのないシステムアプリのアプリデータはクリアされません(キオスク内外の両方で)。 • **アプリを非表示にする:** このオプションを有効化すると、アプリは他のアプリからアクセスされますが、キオスクランチャからは起動できません。 上記のロックダウン設定でダイヤラーまたはカメラを無効化している場合は、許可されたアプリリストに追加できません。
アプリのカタログ	キオスクモードで許可されるアプリグループ内のアプリカタログからリストされたアプリを含めるには、[+追加]をクリックします。

設定	説明
その他のアプリ	Google Playストアで提供されていないアプリのパッケージ名を追加するには、[追加 +] をクリックします。 Samsungデバイスの場合、管理者は以下のダイヤラー/システムパッケージを許可リスト化し、キオスクモードで機能させることにより、キオスクモードでダイヤラー機能を有効化する必要があります。 • 通話 – com.samsung.android.incallui • Phone – com.samsung.android.dialer(許可リスト化が必要であり、管理者はユーザーが2つのダイヤラーを選択できるという問題を防ぐため、このパッケージの非表示オプションを選択する必要がある) • 通話 – com.sec.phone • 通話設定 – com.samsung.android.app.telephonyui • ダイヤルアシスト – com.sec.providers.assisteddialing • 通話ログバックアップ/復元 – com.android.calllogbackup • ダイヤラストレージ – com.android.providers.telephony • 電話 – com.android.server.telecom • 電話 – com.android.phone • スマート通話 – com.samsung.android.smartcallprovider • WiFi 通話 – com.sec.unifiedwfc
キオスクモード可アプリ	キオスクモードで許可されるアプリグループからアプリを削除するには、[X] をクリックします。キオスクデバイスに表示されるアプリの順序を変更するには、ドラッグ&ドロップします。 **フォルダーの追加** - このオプションを使用して、このセクションの下にフォルダーを作成し、1つ以上のアプリをこのフォルダーに移動できます。フォルダーは最大2レベルまで作成できます。一方のフォルダーにコピーしたアプリを他方のフォルダーにコピーすることはできません。1つのフォルダーでサポートされるアプリは25個のみです。

Knox Standard 4.0以降のSamsungデバイスの場合、マルチユーザー機能がキオスクモードに自動的にロックダウンされています。

仕事用プロファイルを持つマネージドデバイス

Android 8.0+対応の仕事用プロファイルを持つマネージドデバイスにおいて特定の機能を無効化します。

一部の機能は、会社所有デバイス上の仕事用プロファイルで無効化できます(Android 11以降のデバイス)。

設定	説明
マネージドデバイスロックダウン設定	
Wi-Fiを無効化	ワイヤレスLANへのアクセスをオフにする場合に選択します。(Android 11以上のデバイスは対象外)
Wi-Fi設定を無効化	ワイヤレス設定へのアクセスをオフにする場合に選択します。
カメラを無効化	カメラアクセスをオフにする場合に選択します。
Bluetoothを無効化	Bluetooth機能をオフにする場合に選択します。 このオプションを使用する場合は注意が必要です。Ivantiは、ハンズフリーでのBluetoothアクセスが無効になるため、音声を無効にしないことを推奨します。運転中のデバイスのハンズフリー使用に関する法規制が一般的になりつつあるためです。
Bluetooth設定を禁止	Bluetooth設定へのアクセスをオフにする場合に選択します。
マスターボリュームをミュート	マスターボリュームをミュートする場合に選択します。(Android 11以降のデバイスは対象外)
緊急ブロードキャストを禁止	緊急ブロードキャストを禁止する場合に選択します。
モバイルネットワークを禁止	モバイルネットワークへのアクセスをオフにする場合に選択します。 Wi-Fiが無効の場合、無効にすることはできません。
テザリングを禁止	あるデバイスがインターネット接続を使用して別のデバイスへインターネットアクセスを提供するためのオプションであるテザリングをオフにする場合に選択します。
VPNを禁止	VPN接続をオフにする場合に選択します。(Android 11以降のデバイスは対象外)
工場出荷時設定へのリセットを無効化	ユーザーがデバイスを工場出荷時設定へ戻せないようにする場合に選択します。(Android 11以降のデバイスは対象外)

設定	説明
工場出荷時設定へのリセットを有効化	ユーザーがデバイスを工場出荷時設定に戻すのを許可する場合に選択します。 工場出荷時設定へのリセットの後でデバイスをプロビジョニングできる許可済みのGoogleアカウントID(整数値)のリストを指定することも可能です。またはヘルプアイコンの上にマウスを置くと、許可済みアカウントの取得方法が表示されます。
発信を禁止	ユーザーによる発信を禁止する場合に選択します。
セーフブートを禁止 (Android 6.0+)	ユーザーがセーフブートモードでデバイスを再起動できないようにする場合に選択します。
デバッグ機能を禁止	デバイスでデバッグ機能を無効化する場合に選択します。このオプションはデフォルトでオンになっています。
アプリ検証を確認	デバイスでアプリケーション検証機能を許可する場合に選択します。このオプションはデフォルトでオンになっています。 このオプションをオフにすると、デバイスごとに異なるデフォルト動作に戻ります。
SMSを禁止	ユーザーがSMSメッセージの送受信をできないようにする場合に選択します。
マイクのミュート解除を禁止	ユーザーがデバイスのマイクのミュートを解除できないようにする場合に選択します。
オートタイムを禁止	ユーザーが自動時間変更をできないようにする場合に選択します。
オートタイムゾーンを禁止	ユーザーがタイムゾーン変更によるデバイスの自動的な時間調整を有効化できないようにする場合に選択します。
データローミングの無効化	デバイスのローミング時のデータ交換をオフにする場合に選択します。
サーバーと時刻を同期 (Android 9.0+)	最初は登録時、その後はチェックイン後24時間ごとに、デバイスにIvanti Neurons for MDM サーバーとの時間同期を許可する場合に選択します。このオプションは、**[オートタイムを無効化]**を選択した場合のみ表示されます。

設定	説明
タイムゾーンを設定 (Android 9.0+)	タイムゾーンの文字列は、オルソンタイムゾーンID形式 (例：太平洋/ミッドウェー) で指定します。
Wi-Fiスリープを無効化	デバイスがスリープモードにあるときにWi-Fiのオン状態を維持する場合に選択します。(Android 11以降のデバイスは対象外)
入力方法を制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、作業アプリケーションの入力方法を制限する場合に選択します(Android 11以上のデバイスは対象外)。 デバイスは、許可リスト化されたパッケージ入力方式とデフォルトのシステム入力方式の両方に対応します。 ユーザーはデフォルトのシステム入力方式と許可リスト化されたパッケージ入力方式を切り替えることができます。 Android 10+では、入力方法はデバイス側にのみ適用されます。さもなければ、デバイス全体に制限されます。
アクセシビリティサービスを制限	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、仕事用アプリのアクセシビリティサービスを制限する場合に選択します。許可リスト化されたパッケージがない場合は、システムアクセシビリティサービスのみ許可されます。 Android 10+では、入力方法は仕事用アプリのみに制限されます。さもなければ、デバイス全体に制限されます。
USBファイル転送を無効化	USBファイル転送を無効化する場合に選択します。
外付けメディアを無効化	外付けメディアを無効化する場合に選択します。
デバイス上の不明なソースを禁止	デバイスが不明なソースからアプリをインストールするのを防ぐ場合に選択します。 この設定をデバイスで有効にするには、この機能を有効化するGoogle Playの更新を実行する必要があります。

設定	説明
ロック画面のメッセージを設定 (Android 7.0+)	デバイスに表示するロック画面のメッセージを設定する場合に選択します。ロック画面のメッセージをテキストフィールドに入力します(256文字まで)。このオプションを有効化すると、ユーザーが[設定]でメッセージを設定できなくなり、管理者が設定したメッセージがユーザーに表示されます。 「ロック画面のメッセージを設定」を有効化した後、管理者がロック画面のメッセージを設定しない場合でも、ユーザーは[設定]でメッセージを設定できず、ユーザーには何のメッセージも表示されません。
画面の明るさを設定	デバイスの画面の明るさを設定する場合に選択します。 • 手動 - 手動で数値(0～255)を入力する場合に選択します • 適応的 - 明るさをデバイスに設定させる場合に選択します [明るさの構成を禁止]オプションを有効にしてから、デバイスの画面の明るさを設定することをお勧めします。 変更を行うことをユーザーが許可されている場合は、これらの設定は、次回チェックイン時に管理者定義の設定にリセットされます。 この設定は、会社所有デバイス上の仕事用プロファイルモードの場合、Android 11以降のバージョンのデバイスではサポートされていません。

設定	説明
スクリーンタイムアウトを設定	スクリーンタイムアウトの期間(秒)を設定する場合に選択します。 [スクリーンタイムアウトの構成を禁止]オプションを有効にしてから、デバイスの画面の明るさを設定することをお勧めします。 変更を行うことをユーザーが許可されている場合は、これらの設定は、次回チェックイン時に管理者定義の設定にリセットされます。 この設定は、会社所有デバイス上の仕事用プロファイルモードの場合、Android 11以降のバージョンのデバイスではサポートされていません。
画面の向きを設定	画面の向きを設定する場合に選択します。ドロップダウンリストから、画面の向きを0度、90度、180度、または270度に設定できます。 この設定は、会社所有デバイス上の仕事用プロファイルモードの場合、Android 11以降のバージョンのデバイスではサポートされていません。
オートフィルを禁止(Android 8.0+)	オートフィルを禁止する場合に選択します。(Android 11以降のデバイスは対象外)
Bluetooth共有を禁止(Android 8.0+)	ユーザーがデバイスでBluetooth接続を共有するのを禁止する場合に選択します。
バックアップサービスを無効化(Android 8.0+)	バックアップサービスを無効にする場合に選択します。(Android 11以降のデバイスは対象外)
印刷を禁止(Android 9.0+)	すべてのアプリケーションから印刷を制限する場合に選択します。(Android 11以上のデバイスは対象外)
機内モードを禁止(Android 9.0+)	デバイス全体に関して機内モードを禁止する場合に選択します。

設定	説明
アンビエントディスプレイを禁止(Android 9.0+)	ユーザーがアンビエントディスプレイを使用するのを禁止する場合に選択します。(Android 11以降のデバイスは対象外)
明るさの構成を禁止(Android 9.0+)	ユーザーが明るさを設定するのを禁止する場合に選択します(Android 11以降のデバイスには適用されません)。 [画面の明るさモードを設定]を定義してから、このオプションを選択することをお勧めします。
日時の構成を禁止(Android 9.0+)	日付、時刻、タイムゾーンの設定を禁止する場合に選択します。
位置情報の構成を禁止(Android 9.0+)	ユーザーが位置情報プロバイダーを無効化するのを禁止する場合に選択します。
スクリーンタイムアウトの構成を禁止(Android 9.0+)	ユーザーがスクリーンタイムアウトまでの時間を変更するのを禁止する場合に選択します。(Android 11以降のデバイスは対象外) [スクリーンタイムアウトを設定]値を設定してから、このオプションを選択することをお勧めします。
システムエラーダイアログを禁止(Android 9.0+)	システムエラーダイアログを禁止する場合に選択します。(Android 11以上のデバイスは対象外)
スクリーンキャプチャを無効化(Android 11.0+)	デバイスのビルトイン画面キャプチャ機能をオフにする場合に選択します。選択した場合、デバイスの個人側でスクリーンキャプチャが禁止されます。
Android 12.0+	
充電時にのみUSBを有効にする	選択すると、充電時にのみUSBポートを有効にします。
Android 13.0+	

設定	説明
最低限必要なWi-Fiセキュリティの設定	次のように最低限必要なWi-Fiセキュリティを設定する場合に、このオプションを使用します。 • 最低セキュリティ要件なし –最低限のセキュリティが必要ない場合に、このオプションを選択します。 • 個人ネットワークベースのセキュリティ– WEP、WPA/WPA2/WPA3など、個人のWi-Fiネットワークをブロックする場合は、このオプションを選択します。 • エンタープライズEAPネットワークベースのセキュリティ – EAPプロトコルベースのWi-Fiネットワークをブロックする場合は、このオプションを選択します。 • エンタープライズ192ネットワークベースのセキュリティ - EAP企業ベースのWi-Fiネットワークをブロックする場合は、このオプションを選択します。 最低限の基準を満たしていない既存のデバイスはすべて切断されます。 デバイスの詳細の **[一般] > [Wi-Fiセキュリティレベル]** に、最低限必要なWi-Fiセキュリティレベルが表示されます(ある場合) 。
仕事用プロファイルロックダウン設定	
スクリーンキャプチャを無効化	デバイスのビルトイン画面キャプチャ機能を利用できないようにする場合に選択します。
アプリ制御を禁止	ユーザーが [設定] やランチャでアプリケーションを変更できないようにする場合に選択します。
構成認証情報を禁止	ユーザーがユーザーの認証情報を構成できないようにする場合に選択します。
プロファイル間のコピー貼り付けを禁止	プロファイル間で情報をコピー/貼り付けをできないようにする場合に選択します。

設定	説明
アカウント変更を禁止	ユーザーがアカウントの追加や削除をできないようにする場合に選択します。
NFC(ビーム発信)を禁止(Android 5.1+)	ユーザーがNFCを使用してアプリデータを送信できないようにする場合に選択します。
位置情報共有を禁止	Webサイトとアプリがデバイスユーザーに位置情報の共有を指示できないようにする場合に選択します。
デバッグ機能を禁止	デバイスでデバッグ機能を無効化する場合に選択します。このオプションはデフォルトでオンになっています。
アプリ検証を確認	デバイスでアプリケーション検証機能を許可する場合に選択します。このオプションはデフォルトでオンになっています。 このオプションをオフにすると、デバイスごとに異なるデフォルト動作に戻ります。
仕事用プロファイル内で不明なソースを無効化	仕事用プロファイル内で不明なソースからのダウンロードを許可しない場合に選択します。
システムアプリを有効化/無効化	**[システムアプリパッケージ名]**フィールドを通じてパッケージ名の2つのリストを指定することにより、導入するシステムアプリケーションを有効化/無効化する場合に選択します。この機能を使用し、Google Playに公開されていないシステムアプリへのアクセスを管理してください。 アプリをアプリカタログとシステムアプリリストの両方に追加することはできません。
発信者IDを無効化(Android 5.0+)	着信の際、仕事用プロファイルの発信者ID情報がデバイスに表示されるかどうかを設定します。
Bluetooth経由での連絡先共有を禁止(Android 6.0+)	デバイスが連絡先をBluetooth経由で他のデバイスと共有できないようにする場合に選択します。
検索経由での連絡先共有を禁止(Android 7.0+)	ユーザーが仕事用連絡先を個人用電話アプリから検索できないようにする場合に選択します。

設定	説明
オートフィルを禁止 (Android 8.0+)	オートフィルを禁止する場合に選択します。(Android 11以降のデバイスは対象外)
個人用プロファイルで仕事用アプリ通知を禁止 (Android 8.0+)	仕事用プロファイルの通知を制限する場合に選択します。
印刷を禁止 (Android 9.0+)	すべてのアプリからの印刷を制限する場合に選択します。(Android 11以降のデバイスは対象外)
プロファイルへの共有を禁止 (Android 9.0+)	ユーザーが個人データをデバイスの仕事用プロファイルに共有するのを禁止する場合に選択します。
入力方法を制限 (Android 10.0+)	**[パッケージ名]** フィールドに許可リスト化されたパッケージ名のリストを指定することにより、許可リスト化されたIMEパッケージ名を制限します (Android 11+のデバイスは対象外)。 デバイスは、許可リスト化されたパッケージ入力方式とデフォルトのシステム入力方式の両方に対応します。 ユーザーはデフォルトのシステム入力方式と許可リスト化されたパッケージ入力方式を切り替えることができます。 入力方法は、仕事用プロファイル側にインストールされたIMEアプリに適用されます。デバイス側にインストールされたアプリがこのロックダウン機能で許可リスト化されていても、仕事用プロファイル側でアプリが利用することはできません。

設定	説明
仕事用プロファイルカレンダーへのアクセスを許可 (Android 10.0+)	すべてのアプリまたは個人側にある一部のアプリが仕事用プロファイル内のカレンダー情報にアクセスできるようにする場合は、以下のいずれかを選択します。 • **個人用プロファイルのすべてのアプリ** - すべてのアプリが仕事用プロファイル内のカレンダー情報にアクセスすることを許可します。 • **個人用プロファイルの以下のアプリのみ** - 以下のテキストフィールドにアプリのバンドルIDをカンマ区切りで入力します。ここで個人側で選択されたアプリだけが、仕事用プロファイル内のカレンダー情報へのアクセスを許可されます。 個人側のアプリが共有カレンダーにアクセスするには、専用のAPIを実装する必要があります。
アプリのプロファイル横断型許可リスト化を有効化 (Android 11.0+)	チェックボックスを選択すると、ユーザーが仕事用プロファイル内にある特定のアプリからの情報をデバイスの個人側と共有できます。 **[許可リストアプリ]** フィールドにアプリのパッケージIDを入力するとアプリが許可リストに入り、コンマ区切りで表示されます。 デフォルトでは無効化されています。
最大プロファイルタイムアウトを有効化 (Android 11.0+)	仕事用プロファイルがオフになってから、Ivanti Neurons for MDM がデバイス上の個人用アプリを保留するまでの最大時間を選択します。時間は72～8,760時間で設定できます。8,760時間は1年に相当します。 オプションを選択したときのデフォルト値は72時間です。 デバイスユーザーには、仕事用プロファイルをオンにして保留アプリを有効化するようメッセージが表示されます。Android 11+で会社所有デバイス上の仕事用プロファイルモードのデバイスで利用可能です。
5G ネットワークスライシングを有効にする (Android 12.0+)	選択すると、会社所有デバイスの仕事用プロファイルで 5G ネットワークスライシングオプションを提供します。 デフォルトでは無効化されています。

詳細は構成を作成するにはを参照してください。

ロックダウン& キオスク: Samsung Knox Standard

[ロックダウン& キオスク: Samsung Knox Standard] 構成は、Samsung Knox Standardデバイスの一部の機能を無効化し、キオスクモードでユーザーが利用できるアプリの許可リストを作成します。

Samsung KNOX Standard構成は廃止されており、Android 9以降のバージョンを搭載したデバイスではサポートされていません。

ロックダウン設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
Samsung Knoxロックダウン設定: Samsung Knoxデバイスのみで特定の機能を無効にします。	
Wi-Fiを無効化	無線LANへのアクセスをオフにする場合に選択します。
カメラを無効化	カメラアクセスをオフにする場合に選択します。
Bluetoothを無効化	Bluetooth機能をオフにする場合に選択します。
Bluetoothオーディオオンリーを許可	Bluetooth音声機能だけをオンにする場合に選択します。
モバイルデータを無効化	デバイス同士が至近距離にあるときのデータ交換をオフにする場合に選択します。 Wi-Fiが無効の場合、無効にすることはできません。
GPSを無効化	GPSをオフにする場合に選択します。
Phone Dialerを無効化	この電話アプリをオフにする場合に選択します。
SDカードの無効化	SDカードアクセスをオフにする場合に選択します。
Googleバックアップを無効化	Googleサーバーへのバックアップをオフにする場合に選択します。
コピー/貼り付けを無効化	コピー/ペースト機能へのアクセスをオフにする場合に選択します。
NFCを無効化	デバイス同士が至近距離でデータ通信を行うためのNFC (Near-field Communication) をオフにする場合に選択します。

マイクロフォンを無効化	デバイスマイクロフォンへのアプリのアクセスをオフにする場合に選択します。
スクリーンキャプチャを無効化	デバイスのビルトイン画面キャプチャ機能をオフにする場合に選択します。このオプションをオンにすると、Goのスクリーンキャプチャが許可されません。スクリーンキャプチャは禁止されます。
Bluetoothテザリングの無効化	あるデバイスがインターネット接続を使用して別のデバイスへインターネットアクセスを提供するためのオプションであるBluetoothテザリングをオフにする場合に選択します。
USBデバッグを無効化	USBデバッグ機能をオフにする場合に選択します。
USBテザリングの無効化	あるデバイスがインターネット接続を使用して別のデバイスへインターネットアクセスを提供するためのオプションであるUSBテザリングをオフにする場合に選択します。
Wi-Fiテザリングの無効化	あるデバイスがインターネット接続を使用して別のデバイスへインターネットアクセスを提供するためのオプションであるWi-Fiテザリングをオフにする場合に選択します。
ネイティブブラウザを無効化	ユーザーがAndroidブラウザへアクセスできないようにする場合に選択します。
YouTubeを無効化	ユーザーがYouTubeへアクセスできないようにする場合に選択します。
工場出荷時設定へのリセットを無効化	ユーザーがデバイスを工場出荷時設定へ戻せないようにする場合に選択します。
OTAアップグレードを無効化	デバイスファームウェアの無線アップグレードをオフにする場合に選択します。 警告：**[OTAアップグレード]**が有効になっている場合は、**[設定変更の無効化]**をしないでください。**[OTAアップグレード]**が有効になっている場合に**[設定変更の無効化]**を行うと、設定の変更にはアップグレードが必要なため、デバイスが機能しなくなる恐れがあります。
ボイスローミングを無効化	デバイスのローミング時の音声通話へのアクセスをオフにする場合に選択します。
USBメディアプレーヤーを無効化	USBメディアプレーヤーをオフにする場合に選択します。
Google Playを無効化	Google Playへのアクセスをオフにする場合に選択します。
データローミングの無効化	デバイスのローミング時のデータ交換をオフにする場合に選択します。

不明なソースを無効化	Goアプリを除き、Google Playストア以外からのアプリのインストールを無効化する場合に選択します。
デバイス管理者特権停止を無効化	ユーザーがGoからデバイスの管理者特権をオフにできないようにする場合に選択します。
設定変更を無効化	デバイス設定アプリへのアクセスをオフにする場合に選択します。 警告：**[OTAアップグレード]** が有効になっている場合は、**[設定変更の無効化]** をしないでください。**[OTAアップグレード]** が有効になっている場合に **[設定変更の無効化]** を行うと、設定の変更にはアップグレードが必要なため、デバイスが機能しなくなる恐れがあります。
キオスクモード設定： キオスクモードは、カスタマイズされたランチャ経由によるアプリへのアクセス制限を含むデバイスに、追加の制限を適用します。 Android バージョン8.1以前に該当します。Androidバージョン9.0には、Androidエンタープライズマネージドデバイスキオスク構成を使用してください。	
キオスクモードを有効化	Androidデバイス上でキオスクモードを構成する場合に選択します。
ユーザーがWi-Fiの設定にアクセスできるようにする	ユーザーがWi-Fi設定を変更し、希望の無線ネットワークに接続できるようにする場合に選択します。
ユーザーがBluetoothの設定にアクセスできるようにする	ユーザーがBluetooth設定を変更し、追加のBluetoothデバイスをペアリングできるようにする場合に選択します。
ユーザーによるアプリケーション更新延期を許可	ユーザーによるアプリケーション更新延期を許可する場合に選択します。
GPS位置情報設定	以下のいずれかのGPS位置情報設定を選択してください。 • 位置情報を無効化 • 位置情報を有効化 • ユーザーによる選択を許可

キオスク終了PIN	エンドユーザーがキオスクモードを終了させるために入力しなければならない4ケタのコードを入力します。
アプリの許可リストを作成：許可されたアプリのリストにアプリを追加することにより、キオスクモードでユーザーが利用可能になります。ドラッグ＆ドロップでアプリを順番に配置するとそれらがキオスクモードランチャに表示されます。 許可されたアプリのリストにアプリケーションを追加しても、デバイス上のアプリにはインストールされません。アプリのカタログ内の適切なユーザーおよびユーザーグループに各アプリを配布するようにしてください。	
ビルトインアプリ	キオスクモードで許可されるアプリグループ内にリストされたネイティブアプリを含めるには、[+追加]をクリックします。 上記のロックダウン設定でダイヤラーまたはカメラを無効化している場合は、許可されたアプリリストに追加できません。
アプリのカタログ	キオスクモードで許可されるアプリグループ内のアプリカタログからリストされたアプリを含めるには、[+追加]をクリックします。
その他のアプリ	Google Playストアで提供されていないアプリの[パッケージ名]を追加するには、[追加+]をクリックします。
キオスクモード可アプリ	キオスクモードで許可されるアプリグループからアプリを削除するには、Xをクリックします。キオスクデバイスに表示されるアプリの順序を変更するには、ドラッグ＆ドロップします。

Android 4.4またはサポートされる以降のバージョンでキオスクモードを使用する場合、複数ユーザーに対応するSamsungデバイスは、キオスクモードの間、自動的にマルチユーザー機能をロックダウンします。

詳細は[構成を作成するには]を参照してください。

macOSのファイアウォール

ライセンス: Gold

macOSのファイアウォールは、macOSデバイスのセキュリティ設定画面からアクセス可能なアプリケーションファイアウォール設定を管理します。

対象: macOS 12.3+

- **ビルトインソフトウェアで受信接続を許可** - オンにすると、ビルトインソフトウェアで受信接続を許可します。
- **ダウンロードした署名済みのソフトウェアで受信接続を許可する** - オンにすると、ダウンロードした署名済みのソフトウェアで受信接続を許可します。

対象: macOS 12.0+

- **ログを有効にする** - オンにすると、ログが有効になります。
- **ログのタイプを指定します。**
  - **調整**
  - **概要**
  - **詳細**

対象: macOS 10.12+

ファイアウォールを有効化をクリックする際には、以下のオプションのうち1つ以上を選択できます。

- **すべての受信接続をブロック** - オンの場合、すべての受信接続のブロックが有効になります。
- **ステルスモードを有効にする** - オンの場合、ステルスモードが有効になります。
- **アプリケーション** - アプリケーションと、ファイアウォールで制御された接続の一覧

- 構成はシステムを対象とするプロファイルに存在しなければなりません。2つ以上のプロファイルがこの構成を含む場合、最も制約の厳しい設定群が使用されます。
- **[ダウンロードされた署名付きソフトウェアを自動的に許可]** および **[内蔵ソフトウェアを自動的に許可]** オプションはサポートされていません。しかし、この構成がある場合は、両方のオプションが強制的にONになります。

- 管理者は、pingコマンドによって発見されないデバイスを指定することにより、ステルスモードを有効化できます。

macOSの制約

ライセンス: Gold

macOSの制約は、macOSデバイスで有効にする制約を決定します。

macOSデバイスでは以下の機能の有効化または無効化を設定できます。

macOSのバージョン	機能
10.11+	• カメラを許可 • iCloudドキュメント同期を許可 **監視対象のみ:** • Spotlightインターネット検索結果を許可
10.11.2+	定義参照を許可
10.12+	• iCloudキーチェーン同期を許可 • 「どこでもMy Mac」を許可 • 「Macを探す」を許可 • メモ、リマインダー、またはLinkedInへの共有を許可 • ブックマーク同期を許可 • macOSのiCloudメールサービスを許可 • macOSのiCloudカレンダーサービスを許可 • macOSのiCloudアドレスブックサービスを許可 • iCloudリマインダーサービスを許可 • 自動ロック解除を許可 **監視対象のみ:** Apple Musicを許可
10.12.4+	• 指紋でのロック解除を許可

macOSのバージョン	機能
10.13+	• iTunesファイル共有を許可 • コンテンツのキャッシュを許可 • 壁紙の変更を許可 **監視対象のみ:** • AirPrintを許可 • AirPrintのiBeaconディスカバリを許可 • AirPrintの信頼性のあるTLS要件を強制 • AirDropを許可 • Game Centerを許可
10.13.4+	**監視対象のみ:** 設定した日数だけソフトウェア更新を延期(30～90日) デフォルト:30日間
10.14+	**監視対象のみ:** 近くのデバイスによるパスワード要求の共有を許可

macOSのバージョン	機能
10.14.4+	• スクリーンショットを許可 • リモート画面監視を許可 **監視対象のみ:** • クラスルームへの参加を自動的に許可 • クラスルームがクラスから出る許可をリクエストするのを許可 • クラスルームがプロンプトなしでアプリとデバイスをロックすることを許可 • プロンプトなしのマネージドクラスルーム画面強制監視を許可
11.0+	**監視対象のみ:** アプリのソフトウェア更新の強制延期を許可
11.3+	強制的な指紋タイムアウト **既定**: 48時間 **前提条件**: デバイスで Touch ID を構成する必要があります。
11.3+	**監視対象のみ:** • ソフトウェア更新強制メジャーOSインストール延期遅延 • ソフトウェア更新強制マイナーOSインストール延期遅延 • ソフトウェア更新強制非OSインストール延期遅延 • メジャーソフトウェア更新遅延を強制

macOSのバージョン	機能
12+	**監視対象のみ:** • コンテンツ消去と設定を許可 • **allowCloudPrivateRelay**: macOS デバイスでプライベート リレーをオンに設定している場合は、ネットワークトラフィックが暗号化されるため、インターネット アクティビティがプライベートになり、保護されます。この制限には、監視対象のデバイスが必要です。
macOS 13.0+	

macOSのバージョン	機能
	• **高速セキュリティ対応インストールを許可** - 応答を無効化します。ユーザーは高速セキュリティ対応をインストールできません。 • **高速セキュリティ対応削除を許可** - ユーザーが対応を元に戻せないようにします。ユーザーは高速セキュリティ対応を削除できません。 • **ユニバーサルコントロールを許可** - ◦ オンにすると、構成で、プライマリデバイスの入力デバイスを使用して、セカンダリ表示デバイスを制御できます。 ◦ オフに設定すると、セカンダリ表示デバイスを追加することはできますが、プライマリ入力デバイスで制御できません。 • **UI構成プロファイルインストールを許可** - オフの場合、構成によって、macOSデバイスでは、プロファイル、構成、証明書のインストールが許可されません。 • **USB制限モードを許可** - オンに設定すると、デバイスが入力デバイスでリモートで接続できないようにロックします。デバイスでは、[アクセサリの接続を許可]オプションが灰色で表示されます。

macOS AppStoreの制約

ライセンス: Gold

macOS AppStoreの制約では、macOS AppStoreで有効にする制約を定義します。

次のオプションを設定できます。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成設定	
macOSのバージョン	**機能**
10.9+	アプリのインストールを管理ユーザーに制限します。
10.10+	• アプリのインストールをソフトウェア更新のみに制限します。 • ユーザーによるアプリ採用を無効化します。 • ソフトウェア更新通知を無効化します。
10.11+	アプリのインストールをMDMインストール済みアプリとソフトウェア更新に制限します。

構成の配布

手順

1. 上記の表を使用してオプションを設定します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。

4. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
5. **[完了]** をクリックします。

macOSディスク焼き付けの制約

ライセンス: Gold

macOSディスク焼き付けの制約では、macOSでのディスク焼き付けの制約を管理します。macOS Finder設定の構成により、macOSのFinderアプリからディスク焼き付けオプションを有効化または無効化できます。

次のオプションを設定できます。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成設定	
設定	**操作内容**
ディスク焼き付けを許可	• オン • オフ • Require Authentication (認証が必要)

構成の配布

手順

1. 上記の表を使用してオプションを設定します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。
4. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)

- カスタム

5. **[完了]** をクリックします。

許可メディアの制御

ライセンス: Gold

許可メディアの制御構成では、macOSにおけるログアウト時のさまざまな物理メディアのマウント、アンマウントおよび取り出しを管理します。

次のオプションを設定できます。

<table>
<tr><th>設定</th><th>操作内容</th></tr>
<tr><td>名前</td><td>この構成を識別する名前に入力します。</td></tr>
<tr><td>説明</td><td>この構成の目的を明示する説明を入力します。</td></tr>
<tr><td colspan="2">構成設定</td></tr>
<tr><td>メディアタイプごとのマウント制御</td><td></td></tr>
<tr><td colspan="2">各メディアタイプのマウント制御をオンにし、マウント設定を実行します。マウント制御をオフにすると、OSのデフォルト設定が適用されます。</td></tr>
<tr><td>メディアタイプ</td><td>マウント設定</td></tr>
<tr><td>CD
DVD
BD</td><td>認証により読み取り専用
マウントを拒否
メディアを取り出す</td></tr>
<tr><td>空のCD
空のDVD
空のBD
DVD-RAM
ディスクイメージ
内蔵ハードディスク
外付けハードディスク
ネットワークディスク</td><td>読み取り専用
マウントを拒否
メディアを取り出す
認証</td></tr>
<tr><td colspan="2">USB HDD、USBフラッシュドライブストレージ、SDカードなどの外付けハードディスク。
CD、DVD、BDなどの読み取り専用メディアは、デフォルトで読み取り専用としてマウントされます。</td></tr>
<tr><td colspan="2">メディアタイプごとのアンマウント制御</td></tr>
</table>

設定	操作内容
各メディアタイプのアンマウント制御をオンにし、アンマウント設定を実行します。アンマウント制御をオフにすると、OSのデフォルト設定が適用されます。各メディアタイプに[マウントを拒否]を設定する場合は注意してください。	
メディアタイプ	**マウント設定**
• CD • DVD • BD • 空のCD • 空のDVD • 空のBD • DVD-RAM • ディスクイメージ • 内蔵ハードディスク • 外付けハードディスク • ネットワークディスク	• アンマウントを拒否 • 認証
[ログアウト時に取り出す] 設定	

設定	操作内容
ユーザーがログアウトすると自動的に取り出されるメディアタイプ。	
メディアタイプ	
• CD • DVD • BD • 空のCD • 空のDVD • 空のBD • DVD-RAM • ディスクイメージ • 外付けハードディスク • ネットワークディスク	

構成の配布

手順

1. 上記の表を使用してオプションを設定します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。
4. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
5. **[完了]** をクリックします。

macOS Finder設定

ライセンス: Gold

macOS Finder設定では、macOSでのFinderアプリの設定を管理します。

次のオプションを設定できます。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成設定	
設定	**操作内容**
Finderでのディスク焼き付けのサポートを無効化	• オンにする • オフにする

構成の配布

手順

1. 上記の表を使用してオプションを設定します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。
4. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
5. **[完了]** をクリックします。

macOSカーネル拡張ポリシー

対象：macOS 10.13.2またはサポートされる以降のバージョン。

ユーザーが承認したカーネル拡張の読み込みの制約と設定を制御します。

macOSカーネル拡張ポリシー構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに**[カーネル]**と入力し、**[macOSカーネル拡張ポリシー]**構成をクリックします。
4. 構成の名前と説明を入力します。
5. **[ユーザーによるオーバーライドを許可]**オプションを選択すると、ユーザーが、以下の構成で明示的に許可されていないカーネル拡張も承認できるようになります。
6. [許可チーム識別子]および[カーネル拡張]セクションで、**[+追加]**をクリックし、許可チーム識別子とカーネル拡張を追加します。カーネル拡張はパッケージのバンドル識別子です。各チーム識別子について、複数の有効な署名済みカーネル拡張名をポップアップウィンドウに追加できます。
7. **[追加]**をクリックします。
8. **[次へ]**をクリックして配布設定を行います。
9. **[完了]**をクリックします。

詳細は構成を作成するにはを参照してください。

macOS対応Mobile@Work

このセクションは以下のトピックを含みます。

- macOS対応Mobile@Work構成とスクリプト実行のワークフロー
- macOS対応Mobile@Work構成の作成
- macOSデバイスのユーザーオンボーディングの有効化
- macOS対応Mobile@Workスクリプト構成の作成
- 「macOS対応Mobile@Workのクリーンアンインストール」ページ633

Ivanti Neurons for MDMでは、独自のmacOSシェルスクリプトを作成した後、Ivanti Neurons for MDMにアップロードし、マネージドmacOSデバイスで実行することができます。スクリプトリポジトリの作成、アップロード、管理については、すべてのスクリプトをご覧ください。

macOSデバイスのユーザーは、Mobile@Work for macOS 1.1以降を使用してデバイスの撤去を開始できます。撤去のオプションは、[Mobile@Workについて]の画面で**[アンインストール]**をクリックすると表示されます。Ivanti Neurons for MDMでは、デバイスのステータスを**[デバイス]**ページと[デバイス詳細]ページで確認できます。

Mobile@Work for macOS 1.5以降では、MDM登録の完了を待たずに、登録後に直ちにApps@Workが開きます。

Mobile@Work for macOSで、アプリケーションタイルをクリックして、そのアプリケーションの[アプリの詳細]ページを表示します。このページには、アプリの説明、スクリーンショット、評価、レビューが表示されます。

macOS対応Mobile@Workは、インベントリレポートでPackager自社開発macOSアプリがインストールされているかどうかをIvanti Neurons for MDMサーバーに通知します。

前提条件

アプリカタログでは、macOS対応Mobile@Workクライアントがビジネスアプリとして提供されています。macOSデバイスでシェルスクリプトを実行する前に、macOS対応のMobile@Workを使用し、Ivanti Neurons for MDMにデバイスを登録するようユーザに指示してください。

手順

1. macOSアプリケーション用のMobile@Workをダウンロードする。https://support.mobileiron.com/support/CDL.html で PKG ファイルとして提供されています。ダウンロードサイトの認証資格情報の取得については、この Ivanti お客様フォーラムの記事をご覧ください。
2. macOS対応Mobile@WorkのPKGファイルをセキュアサーバーにアップロードする。このサーバーはデバイスユーザーからアクセスできる必要があります。
3. macOS対応Mobile@Workのインストールファイルの URLをメールまたはメッセージでデバイスユーザーと共有する。
4. ユーザーに以下を指示する:
   a. macOS対応Mobile@Workをデバイスにダウンロードしてインストールします。
   b. macOS対応Mobile@Workを使用したIvanti Neurons for MDMでのデバイスの登録

macOS対応Mobile@Work構成とスクリプト実行のワークフロー

手順

1. macOS対応Mobile@Work構成を設定および配布します。
2. スクリプトをIvanti Neurons for MDMにアップロードするためのmacOS対応Mobile@Workスクリプト構成を設定して配布します。スクリプトは暗号化され、テナント固有の署名済み証明書で署名されています。スクリプトを解読するキーは、スクリプト(暗号化および署名済み)のダウンロードURLとともにデバイスに送信されます。
3. Ivanti Neurons for MDM は、macOS対応Mobile@Workを使用し、macOSデバイスでスクリプトを実行します。macOS対応Mobile@WorkはIvanti Neurons for MDMを定期的にポーリングし、実行を待っているスクリプトがないか確認します。キューの中にスクリプトがあれば、Mobile@Workがスクリプトをダウンロードし、Ivanti Neurons for MDMで定義した設定に基づいてmacOSデバイス上で実行します。
4. macOS対応Mobile@Workは、スクリプトの実行結果をIvanti Neurons for MDMに戻します。これは、デバイスログに表示されます。デバイスログは、macOSデバイスの **[ログ]** タブにあるデバイス詳細ページから確認できます。

macOS対応Mobile@Work構成の作成

macOS対応Mobile@Work構成のデフォルトシステム構成は提供されています。しかし、デフォルトではデバイスに配布されません。

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[work]** と入力し、**[macOS対応Mobile@Work]** 構成をクリックします。
4. 構成の名前と説明を入力します。
5. **[最大実行時間]** を秒で入力し、スクリプトが実行可能な時間を指定します。デフォルト値は60秒です。
6. **[最大応答サイズ]** をキロバイト(KB)で入力し、Ivanti Neurons for MDMに戻すスクリプトの出力の応答サイズ上限を指定します。これは、スクリプト実行の際に戻されるstdoutまたはstderrデータです。デフォルト値は1 KBです。
7. **[チェックイン間隔]** を分で入力し、macOSアプリ対応のMobile@WorkがIvanti Neurons for MDMにチェックインする頻度を指定します。デフォルト値は15分です。
8. (任意) macOSデバイスのユーザーオンボーディングの有効化セクションの手順に従ってmacOSデバイスのユーザーオンボーディングを有効化します。
9. **[次へ]** をクリックして配布設定を行います。
   a. 以下の配布レベルを選択します。
   b. **全員用** - すべてのユーザーの対応デバイスにアプリが追加されます。
   c. **該当なし** - アプリは将来の配布用にステージングされます。
   d. **カスタム配布** - 以下のいずれかを選択します。
      - **ユーザー/ユーザーグループ** - このアプリは、選択されたユーザーまたはユーザーグループにのみ配布されます。
        ユーザーを選択するには **[ユーザー]** タブをクリックします。
        ユーザーグループを選択するには **[ユーザーグループ]** タブをクリックします。
      - **デバイス/デバイスグループ** - このアプリは、選択されたデバイスまたはデバイスグループにのみ配布されます。
        デバイスを選択するには **[デバイス]** タブをクリックします。
        デバイスグループを選択するには **[デバイスグループ]** タブをクリックします。
10. **[完了]** をクリックします。

macOSデバイスのユーザーオンボーディングの有効化

macOSデバイスのユーザーオンボーディングは、自動Device Enrollmentプロセス中に次のように有効化できます。

- Device Enrollmentが完了すると同時に、macOS対応Mobile@Work(バージョン1.68以降が必要)と各種プロファイル、構成、アプリがデバイスにプッシュされます。
- macOSクライアント対応Mobile@Workおよび他のアプリは、以下の場合に限ってデバイスにプッシュされます。
  - アプリが自社開発PKGアプリまたはApple Apps and Books市販アプリの場合。
  - アプリのサイレントインストール設定がTrueの場合。設定は **[アプリ]** > [アプリ詳細] > **[アプリ構成]** > **[デバイスにインストール]** ページにあります。
  - [アプリの優先度] が「高」に設定されている場合。デフォルトで、macOS対応Mobile@Workクライアントアプリの優先度は「高」に設定されています(変更できません)。**そうでない場合、ユーザーオンボーディングのプロセスが失敗する場合があります**。
  - アプリは、デバイス、ユーザーグループ、デバイスグループのいずれかに配布するよう構成します。
- macOS対応Mobile@Workのインストールと登録の後、macOSデバイスは、残りのプロファイル、構成、アプリの構成/インストールが終わるまで、キオスクモードになります(ユーザーはデバイスを制御できません)。進行はステップで表示されます。

Ivanti Neurons for MDMがサポートするmacOS対応Mobile@Work1.73以降のバージョンでは、以下の追加機能がサポートされます。

- ユーザーオンボーディングのプロセスは、デバイスのDevice Enrollmentが完了するとまもなく完了します。たとえ管理者がMobile@Work構成でユーザーオンボーディングを有効化していても、ユーザーオンボーディングが時間切れになった後は(通常はデバイス登録後20分)、ユーザーオンボーディングのプロセスが開始されません。これにより、デバイスが通常の利用状況にあるときにユーザーオンボーディングキオスクモードになることを防ぎます。
- macOS対応Mobile@Workクライアントではユーザーオンボーディングのプロセスがステップで表示されます。構成は第1ステップの一環としてインストールされます。
- 優先度の高いアプリは最初にインストールされます。高優先度のアプリはそれぞれ1ステップと見なされます。Packagerアプリはステップの一環と見なされません。
- ユーザーオンボーディングが終わった後でも残りのアプリはバックグラウンドで引き続きインストールされます。デバイスでインストールが始まる、またはアプリケーションがデバイスに実際にインストールされると、アプリケーションはインストール済みとマークされます。
- ユーザーオンボーディングの後は、デバイス詳細ページから各デバイスにプッシュされる構成とアプリを確認できます。詳細はログに記載されます。

手順

1. macOS対応Mobile@Work構成の作成の手順に従ってMobile@Work for macOSの構成を作成します。
2. **[ユーザオンボーディングを有効化]** オプションを選択します。
3. 以下の情報を入力します。
   - **ユーザーオンボーディングのタイムアウト値** - デバイスの初期セットアップにおいてアプリのインストールと構成にかかるおおよその時間を入力します。macOSデバイスのユーザーオンボーディングはデフォルトでは120秒でタイムアウトになりますが、必要に応じて変更可能です。
   - **ユーザーのランディングページURL** - オンボーディング完了後、ユーザーに表示するランディングページのURLを入力します。
4. **[次へ]** をクリックして配布設定を行います。
5. **[完了]** をクリックします。

macOS対応Mobile@Workスクリプト構成の作成

macOS対応Mobile@Workのスクリプト構成は、複数作成し、デバイスに配布できます。この構成を使用し、リポジトリ(**[管理]** > **[すべてのスクリプト]**) からスクリプトを選択してmacOS対応Mobile@Workに配布します。

macOS対応Mobile@Work 1.66以降のバージョンでは、デバイスでのスクリプト実行をスケジュールできます。macOS対応Mobile@Workのクライアントバージョン1.66より前でデバイスでのスクリプト実行をスケジュールした場合、スクリプトは1回だけ実行されます。macOS対応Mobile@Workのクライアントを1.4から1.66にアップグレードすると、すべてのmacOSクライアント構成がデバイスに再配布されます。

前提条件

- **[管理]** > **[すべてのスクリプト]** を開き、この構成で使用可能およびデバイスに配布可能なスクリプトのアップロードと管理を行います。
- macOS対応Mobile@Work構成を設定し、デバイスに配布します。さもなければ、macOS対応Mobile@Workスクリプト構成はエラー状態になります。

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[work]** と入力し、**[macOS対応Mobile@Workスクリプト]** 構成をクリックします。
4. 構成の名前と説明を入力します。

5. **[スクリプトを選択]** フィールドにスクリプトの名前を入力し、ドロップダウンリストからスクリプトを選択します。
6. [スクリプト入力] セクションに、スクリプト入力ラベルとスクリプトに関連するスクリプト変数が表示されます。上書きする必要がある場合は、代わりのスクリプト変数 ({$userWorkEmailAddress}など) と代わりのデフォルト値 (john.doe@company.comなど) を入力します。
7. [スクリプト実行] セクションで、以下のいずれかのスケジュールオプションを選択します。
   - 導入時に1回実行
   - 反復実行
8. 反復実行を選択する場合、以下を指定してください。
   - 使用するタイムゾーン - デバイスの現地時刻またはUTC時刻を選択します。スクリプトは、このフィールドで選択した時刻で実行されます。
   - 実行開始日 - 開始日を選択します。
   - 実行終了日 - 終了日を選択します(開始日以降)。
   - スクリプト実行 - 毎日または毎週を選択し、時 (24時制)、分、日を適宜入力します。
9. **[次へ]** をクリックして配布設定を行います。
10. **[完了]** をクリックします。

macOS対応Mobile@Workのクリーンアンインストール

macOS対応Mobile@Workのインストール中に **[登録解除時にアプリを削除] (マネージドアプリにのみ適用)** を有効化済みで、Ivanti Neurons for MDM管理者ポータルからデバイスの撤去を開始する場合、macOS対応Mobile@Workアプリケーションとアンインストールスクリプトはデバイスから削除されるだけです。プロセスとスクリプトがバックエンドで実行されるのを防ぐため、新規ユーザーのデバイス登録または既存ユーザーの撤去中は、以下のオプションをIvanti Neurons for MDM管理者ポータルで選択解除し、アンインストールスクリプトが実行されて関連プロセスとスクリプトをバックエンドから削除するようにしてください。

手順

1. Ivanti Neurons for MDM管理者ポータルにログインします。
2. **[アプリ]** > **[Mobile@Work]** > **[アプリ構成]** > **[アプリ構成の概要] リスト** > **[Appleアプリ設定]** > **[Appleアプリケーション管理構成の設定]** を開きます。

3. **[構成設定]** ページで、以下のオプションの選択を解除します。
    - **登録解除時にアプリを削除(マネージドアプリにのみ適用)**。

関連トピック:

- [管理] > [すべてのスクリプト]
- 構成を作成するには

macOSソフトウェア更新ルール構成

管理者は「macOSソフトウェア更新ルール」下の定義により、デバイスのソフトウェア更新ポリシーを構成できます。

対象：macOS 10.7+

Procedure

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[macOS]** と入力し、**[macOSソフトウェア更新設定]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. 「macOSソフトウェア更新ルール」下 から必要な構成を選択します。
5. **[次へ]** をクリックします。
6. **[この構成を有効化]** オプションを選択します。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

macOSソフトウェア更新ルール

管理者は以下のようにルールのリストから選択できます。

これらのルールがデバイスに適用されている場合、ユーザーはこれらの設定を変更できません。

- リリース前インストールを許可。
- 自動：
  - 更新を確認
  - 新しい更新が公開されたときにダウンロード
  - macOS更新をインストール
  - アプリストアからアプリ更新をインストール
  - システムデータファイルとセキュリティ更新をインストール
- アプリのインストールを管理ユーザーに制限。
- ソフトウェア更新カタログのURLを追加するオプション(macOS 11+は非対応)。

証明書設定

対象：macOS 10.12またはサポートされる以降のバージョン。

同じプロファイルに含まれる証明書ペイロードを参照するユーザーのキーチェーン内の証明書設定項目を特定します。

この構成は、メールアドレスまたはURLのいずれかに証明書を紐付けるために使用されます。証明書をメールアドレスに紐付けると、Mailアプリはそのメールアカウントにそれを使用します。WebサイトのSSL証明書が信用できない場合、証明書設定を追加すると、Webサイトにアクセスする際にブラウザが警告メッセージを表示しなくなります。

証明書設定構成の作成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[設定]** と入力し、**[証明書設定]** 構成をクリックします。
4. 構成の名前と説明を入力します。
5. [構成設定] セクションで、**[名前]** フィールドに優先証明書が要求されているメールIDまたは名前を入力します。
6. **[証明書UUID]** フィールドで、証明書を選択します。
7. **[次へ]** をクリックして配布設定を行います。
8. **[完了]** をクリックします。

関連トピック:

- 「ID設定」ページ642
- 構成を作成するには

Active Directory(macOS)

対象：macOS 10.9またはサポートされる以降のバージョン。

認証とセキュリティをActive Directory(AD) に依存するソフトウェアサービスにアクセスするには、macOSデバイスをADドメインにバインドする詳細オプションを構成します。

このセクションは以下のトピックを含みます。

- Active Directory構成の作成
- Active Directoryの設定

Active Directory構成の作成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[プライバシー]** と入力し、**[Active Directory]** 構成をクリックします。
4. 構成の名前と説明を入力します。
5. 設定の内容は下のActive Directory設定表のとおりです。
6. **[次へ]** をクリックして配布設定を行います。
7. **[完了]** をクリックします。

Active Directoryの設定

設定	操作内容
Active Directoryの設定 - 基本	
ホスト名	(必須) ホスト名、すなわち登録するActive Directoryのドメインを入力します。
ユーザー名	ドメイン登録に使用するアカウントのユーザー名を入力します。

設定	操作内容
パスワード	ドメイン登録に使用するアカウントのパスワードを入力します。
AD組織ユニット	登録するコンピューターオブジェクトが追加される組織ユニット(OU)を入力します。
ADマウントスタイル	次のオプションのいずれかを選択し、使用するネットワークホームプロトコルを表示します。 • AFP • SMB
Active Directoryの設定 - 詳細	
ADCreateMobileAccountAtLoginキーを有効化	ADCreateMobileAccountAtLoginキーを有効または無効にします。 追加オプション: ログイン時にモバイルアカウントを作成。
ADWarnUserBeforeCreatingMAキーを有効化	ADWarnUserBeforeCreatingMAキーを有効または無効にします。 追加オプション: モバイルアカウントの作成前にユーザーに警告。
ADForceHomeLocalキーを有効化	ADForceHomeLocalキーを有効または無効にします。 追加オプション: ローカルのホームディレクトリを強制。
ADUseWindowsUNCPathキーを有効化	ADUseWindowsUNCPathキーを有効または無効にします。 追加オプション: ADからのUNCパスを使用してネットワークホームロケーションを入手。

設定	操作内容
ADAllowMultiDomainAuthキーを有効化	ADAllowMultiDomainAuthキーを有効または無効にします。 追加オプション: フォレスト内の任意のドメインからの認証を許可。
デフォルトユーザーシェル	/bin/bashなどのデフォルトユーザーシェルを入力します。
ユーザーUIDを属性にマッピング	ユーザーUIDを指定した属性にマッピングする場合に選択します。
ユーザーGIDを属性にマッピング	ユーザーGIDを指定した属性にマッピングする場合に選択します。
グループGIDを属性にマッピング	グループGIDを指定した属性にマッピングする場合に選択します。
優先するドメインサーバー	このドメインサーバーを優先します。
名前空間の規則	以下のいずれかのユーザーアカウント命名規則を選択します。 • ドメイン(デフォルト) • フォレスト
パケット署名	以下のパケット署名オプションから1つ選択します。 • 許可(デフォルト) • 無効化 • 必須
パケット暗号化	以下のパケット暗号化オプションから1つ選択します。 • 許可(デフォルト) • 無効化

設定	操作内容
	• 必須 • SSL
指定したActive Directoryグループによる管理を許可	指定したActive Directoryグループによる管理を許可する場合に選択します。 **[追加]** をクリックして1つまたは複数のグループを追加します。
ダイナミックDNSを制限	指定したインターフェイス(en0、en1など) にダイナミックDNSの更新を制限する場合に選択します。 **[追加]** をクリックして1つまたは複数のインターフェイス名を追加します。
パスワード変更間隔	コンピューター信頼アカウントのパスワードの変更間隔を日数で指定します。ゼロにはできません。

詳細は構成を作成するにはを参照してください。

ID設定

対象：macOS 10.12またはサポートされる以降のバージョン。

同じプロファイルに含まれるIDペイロードを参照するユーザーのキーチェーン内のID設定項目を特定します。

macOSデバイスでは、ID設定により、Webサイトに使用したいID(キー/値のペア)を選択できます。ID設定(URLとIDで構成される)をデバイスにプッシュすると、ID設定が**[キーチェーンアクセス] -> [すべての項目]**([種類]が[ID環境設定]になる)にリスト表示されます。次にSafariからそのURLに接続しようとすると、デバイスが構成済みの証明書を表示します。

Ivanti Neurons for MDMは、AppStore URLのペイロードと使用する認証情報を使い、デフォルトシステムの[ID設定]構成を作成します。

macOS 10.12以降でSafariからmacOSアプリカタログにアクセスすると、ユーザーには、ID証明書をキャッシュするようシステムパスワードプロンプトが表示されます。次にmacOSアプリカタログにアクセスする際にプロンプトが表示されないようにするには、初回アクセス時に[常に許可]を選択する必要があります。

macOSバージョン10.12未満のSafariや他のブラウザでは、macOSデバイスから新しいブラウザセッションでmacOSアプリカタログにアクセスする際、証明書とシステムパスワードのプロンプトが表示されます。

ID設定構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに**[設定]**と入力し、**[ID設定]**構成をクリックします。
4. 構成の名前と説明を入力します。
5. [構成セットアップ]セクションで、**[名前]**フィールドにメールIDまたは、DNSホスト名、またはサービスを一意的に特定する名前を入力します。
6. **[証明書UUID]**フィールドで、証明書を選択します。
7. **[次へ]**をクリックして配布設定を行います。
8. **[完了]**をクリックします。

関連トピック:

- 「証明書設定」ページ637
- 構成を作成するには

Office 365自動アカウント作成(macOS)

対象:

- サポートされるmacOSデバイス。
- 推奨されるMicrosoft Office 365アプリのバージョンは、16.13x以降です。

ユーザー情報とオプションを構成し、すべてのMicrosoft Office 365アプリについて初期構成を設定します。

このセクションは以下のトピックを含みます。

- Office 365自動アカウント作成構成の作成
- Office 365自動アカウント作成設定

Office 365自動アカウント作成構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに**[オフィス]**と入力し、**Office 365自動アカウント作成**構成をクリックします。
4. 構成の名前と説明を入力します。
5. 次のOffice 365自動アカウント作成設定表に記載されている設定を入力します。
6. **[次へ]**をクリックして配布設定を行います。
7. **[完了]**をクリックします。

Office 365自動アカウント作成設定

設定	操作内容
Officeアクティベーションメールアドレス	ユーザーのメールアドレスを入力します。
Office自動サインイン	初回実行画面を出したくない場合に選択します。O365認証などの必須情報のみユーザーにプロンプト表示します。
デフォルトはローカルで「開く」「保存」	パネルの「開く」/「保存」を、「オンラインロケーション」ではなく「Mac上」に強制する場合に選択します。
起動時に最新情報を表示	起動時に最新情報を表示する場合に選択します。
Visual Basicマクロ実行状態	以下のオプションから1つ選択してください： • 警告付きで無効 • 警告なしで無効 • 警告なしで有効
Visual Basic外部ダイナミックライブラリを無効化	Visual Basicの外部依存性を無効化する場合に選択します。
Visual Basicによるシステムのバインドを許可	マクロがDECLAREを使用してsystem() OS APIにバインドするのを許可する場合に選択します。このAPIにより、マクロが任意の外部プロセスを実行し、それらにコマンドライン上で任意のデータを渡すことができます。
Visual BasicによるPopenへのバインドを無効化	マクロがDECLAREを使用してpopen() OS APIにバインドするのを許可する場合に選択します。このAPIにより、マクロが任意の外部プロセスを実行し、それらにコマンドライン上で任意のデータを渡すことができます。
Visual Basic Macスクリプトを無効化	マクロがApple Script Visual Basic APIを起動するのを許可する場合に選択します。

詳細は構成を作成するにはを参照してください。

認証

対象：

- macOS 10.13およびサポートされる以降のバージョン
- Windows 10およびサポートされる以降のバージョン

認証構成を使用し、クラウドサービスやデスクトップのログインにパスワードレス認証を使用します。各デバイスに認証構成は1つだけです。

前提条件

- ゼロ・サインオンライセンスが必要です。
- Ivanti Neurons for MDM はAccessへの登録が必要です(Accessプロファイルを設定する必要があります) 。

> - 認証を構成した後でAccessプロファイルの登録を解除することはできません。これはAccessプロファイルが認証構成によって参照されるためです。
> - Accessプロファイルに変更があった場合は、認証構成をmacOSデバイスに再配布します。Windowsデバイスの場合、新しいCLI値をコピーして新しいアプリに使用します。

認証構成の作成

Procedure

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[認証]** と入力し、**[認証]** 構成をクリックします。
4. 構成の名前と説明を入力します。
5. ドロップダウンリストから **[デスクトップID証書]** を選択します。
6. 以下のOSオプションのいずれかまたは両方を選択してください：
   - macOS
   - Windows

7. macOSの場合：

   a. カスタムデータ領域で **[+追加]** をクリックし、デバイスにプッシュするカスタムデータのキーと文字の値を追加します。

   b. **[次へ]** をクリックして配布設定を行います。

   c. **[完了]** をクリックします。

8. Windows 10デバイスの場合、以下のように、この構成がWindows対応Authenticator MSIアプリのコマンドライン引数の生成に役立ちます。

   a. **[完了]** をクリックすると認証構成が完了します。

   b. **[構成]** ページで認証構成を閲覧し、表示されたコマンドラインテキストをコピーします。このテキストは、認証アプリをWindowsデバイスに配布する場合に必要となります。

認証構成をWindowsデバイスに適用すると、構成はインストール保留状態になります。機能には影響がないので、これは無視してかまいません。

詳細は構成を作成するにはを参照してください。

Appleアプリカタログ

対象：iOSとmacOS

Appleアプリカタログ構成は、Webクリップ経由でのAppleアプリカタログへのアクセスを管理します。Ivanti Neurons for MDM リリース83以降では、Go アプリケーションから Apps@Work ネイティブ エクスペリエンスに移行できます。新しく作成されたテナントでは、既定では、Apps@work Webclip 構成は iReg またはクライアントからインストールされた iOS デバイスに配布されません。管理者は、iReg またはクライアントから登録されたデバイスに手動で webclip 構成を配布する必要があります。

iOSデバイスとiPadデバイスでは、検索要求の行パラメータが10を超えていても、Apps@Work Webクリップの検索結果には、10個のアプリケーションのみが表示されます。

手順

管理者は、このシステム定義の構成を以下の手順で編集できます。

1. **[構成]** に進みます。
2. **[Appleアプリカタログ]** をクリックします。
3. **[配布を編集]** をクリックします。
4. 以下の配布オプションから1つ選択します。
   - 全デバイス - 互換性のあるすべてのデバイスが、この構成の送信を受けます。
   - デバイスなし - Appleアプリカタログへのアクセスを無効化するか、この構成を今後の配布用にします。
   - カスタム - この構成の送信を受ける特定のデバイスグループを定義します。
5. **[保存]** をクリックします。

マネージドドメイン

ライセンス: Silver

マネージドドメイン構成では、iOS 8+上のMailおよびSafariにとって信頼できるドメインを指定できます。構成をデバイスに適用すると、デバイスのMailおよびSafariで、構成で指定されなかったドメイン(信頼できない)がハイライト表示されます。この構成と制約構成を組み合わせると、Safariで許可するデータダウンロードをコントロールできます。

マネージドドメイン設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
マネージドメールドメイン	**[+追加]**をクリックし、mycompany.comのようにドメインを入力します。
マネージドWebドメイン	**[+追加]**をクリックし、mycompany.comのようにドメインを入力します。

詳細は構成を作成するにはを参照してください。

パスコード構成

Ivanti Neurons for MDMにおいてまず設定する項目の1つが(スタートアップウィザードを利用)、パスコード構成です。この構成は、デバイスの画面ロック機能に関する設定を定義します。

パスコード設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
シンプルな値を許可	PINまたはパスワードにおける連続する文字や数字の使用を制限します。 **iOSおよびAndroid:** 繰り返し、昇順または降順の文字列を含む、セキュリティ強度の低いPINまたはパスコードを許可する場合に選択します。 例:1111、1234、abcd。 Androidデバイスでこのオプションの選択を解除すると、複雑なPINが強制的にパスコードとなります。たとえば、文字の繰り返し、昇順または降順の文字列は使用できません。 **Windows 10 Mobile:** 同じ数字や連番の数字を含むセキュリティ強度の低いパスコードを許可する場合に選択します。 例:1111、1234。
英数字の値が必要	パスコードに最低アルファベット1文字と数字1つを含めることを要求します。

設定	操作内容
	iOSおよびAndroid：パスコードが英文字と数字を必ず含むようにしたい場合に選択します。 **Windows 10 Mobile**：選択すると、Microsoftの標準に基づく強力なパスワードを保証します。
パスコードの最小文字数	リストから数字を選択し、パスコードの最小文字数を設定します。 **Windows 10デスクトップ**：ローカルアカウントには6文字以上のパスコードが必要です。
複雑な文字の最小文字数	**iOSおよびAndroid**：リストから数字を選択し、数字または英文字ではない文字の最低文字数を設定します。 **Windows 10 Mobile**：非対応。 **Windows 10デスクトップ**：ローカルアカウントには3文字以上の複雑な文字が必要です。
パスコードの最大有効期間	デバイスユーザーがパスコードをリセットしなければならなくなる経過日数を入力します。パスコードの最大有効期間を設定したくない場合は、このフィールドを空白のままにしてください。
オートロック	リストから間隔の値を選択し、デバイスの画面が自動的にロックされるまでアイドル状態でいる時間の長さを定義します。
あらゆるロック方式	**Androidのみ**。パターンロック解除を含、め、あらゆるロック方式の選択をユーザーに許可します。上記のパスコード設定はこのデバイスに適用されません。

設定	操作内容
パスコードの履歴	パスコードを再利用できるようになるまで、ユーザーが入力しなければならない一意のパスコードの数を設定する数字を入力します。たとえば、このフィールドを4に設定すると、ユーザーは最初のパスコードを再利用できるようになるまで4つのパスコードを設定しなければならないことになります。
デバイスロックの時間設定	リストから間隔の値を選択し、ロック画面の表示と、ユーザーがデバイスのロック解除のためのパスコードを入力しなければならなくなるタイミングとの間隔を設定します。 **Windows 10 Mobile はサポートされていません。**
入力失敗の最大回数	リストから数字を選択し、デバイスユーザーが連続して誤ったパスコードを入力してもデバイスがリセットおよびワイプされない最大回数を設定します。 **警告:** ユーザーによるパスコード入力の失敗が最大回数を超えるとデバイスがワイプされます。このオプションの使用には注意が必要です。
(macOSのみ) 次のログイン時にパスコード規則を適用	これを選択すると、ユーザーの次のログイン時に、パスワードポリシーに適合するパスワードに変更するようmacOSがプロンプトを表示できます。 デフォルトではこのオプションは選択されていません。 macOS 10.13以降のバージョンに適用されます。
(macOSのみ) 失敗したログインのリセットまでの分数	ログイン試行の最大失敗回数に達した後、ログインがリセットされるまでの分数を指定します。

設定	操作内容
	このフィールドを有効にするため、試行の最大失敗回数が設定されていることを確認してください。macOS 10.10以降で利用できます。
SmartLock	**Android 5.0デバイスでAndroidエンタープライズプロファイルにある場合を除く:** **Android 6.0以降:** ユーザーがSmartLock機能を利用したデバイスのロック解除を選択することを許可または禁止します。SmartLock機能は、ユーザーがデバイスの近くにいつとき、デバイスが特定の場所にあるとき、デバイスが信頼できるデバイスにペアリングされているときなど、所定の状況でデバイスのロックを自動的に解除します。
指紋によるロック解除	**Android 5.0デバイスでAndroidエンタープライズプロファイルにある場合を除く:** **Android 6.0以降:** ユーザーが指紋を利用したデバイスのロック解除を選択することを許可または禁止します。
ロック画面通知 (Androidエンタープライズのみ)	**仕事用マネージドデバイス(デバイス所有者用)の通知を有効化** 仕事用マネージドデバイスのロック画面における通知を許可または禁止 **仕事用プロファイルの未編集通知を有効化** **Android 6.0以降:** 仕事用プロファイルデバイスのロック画面における未編集通知を許可または禁止

設定	操作内容
	この設定を有効化すると、通知は受信しますが、内容は「ポリシーによって非表示」と表示されます。内容(メール/プッシュ通知)はアプリからのみ閲覧可能です。

詳細は構成を作成するにはを参照してください。

プライバシー設定(macOS)

対象: macOS 10.14またはサポートされる以降のバージョン。

どのアプリがシステムサービス、システムファイル、およびシステムリソースにアクセスするのを許可するかを構成します。この構成が、[システム環境設定] > [セキュリティとプライバシー] > [プライバシー] にあるmacOSデバイス上の設定を制御します。

プライバシー設定構成の作成

Procedure

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[プライバシー]** と入力し、**[プライバシー設定]** 構成をクリックします。
4. 構成の名前と説明を入力します。

5. ページ上に表示されたアプリケーションのいずれかに移動します。関連情報は、Appleドキュメンテーションを参照してください。

   a. macOS 10.14+の場合、構成可能なアプリケーションと設定は次のとおりです：

      - アクセシビリティ - アクセシビリティサブシステムでアプリに対するポリシーを指定します。
      - アドレスブック - 連絡先アプリが管理する連絡先情報に対するポリシーを指定します。
      - Appleイベント - 制限付きのAppleEventsを別のプロセスに送信するアプリに対するポリシーを指定します。
      - カレンダー - カレンダーアプリが管理するカレンダー情報に対するポリシーを指定します。
      - カメラ - システムカメラ。カメラへのアクセスはプロファイルで付与できません(拒否のみ可能)。
      - マイク - システムマイク。マイクへのアクセスはプロファイルで付与できません(拒否のみ可能)。
      - 写真 - 写真アプリが~/Pictures/.photoslibraryで管理する写真。
      - ポストイベント - アプリケーションがCoreGraphics APIを使用してCGEventsをシステムのイベントストリームに送信するためのポリシーを指定します。
      - リマインダー - リマインダーアプリが管理するリマインダー情報に対するポリシーを指定します。
      - システムポリシー(全ファイル) - アプリケーションに全保護ファイル(システム管理ファイルを含む)へのアクセスを許可します。
      - システムポリシー(管理ファイル) - アプリケーションにシステム管理に使用されている一部のファイルへのアクセスを許可します。

b. macOS 10.15+の場合、構成可能なアプリケーションと設定は次のとおりです：

- ファイルの使用 - ファイルプロバイダーによって管理されるファイルをユーザーが使用していることを、ファイルプロバイダーアプリケーションが認識することを許可します。
- すべてのプロセスからイベントを受信 - アプリケーションがCoreGraphicsとHID APIを使用し、すべてのプロセスからCGEventsとHIDイベントを受信することを許可します。これらのイベントへのアクセスはプロファイルで付与できません(拒否のみ可能)。許可オプションのチェックを外します。
- メディアライブラリにアクセス - アプリケーションがApple Music、音楽/動画機能、メディアライブラリにアクセスすることを許可します。
- システムディスプレイのスクリーンキャプチャ - アプリケーションがシステムディスプレイのコンテンツを取得する(読む)ことを許可します。コンテンツへのアクセスはプロファイルで付与できません(拒否のみ可能)。許可オプションのチェックを外します。
- 音声データを認識し、Appleに送信 - アプリケーションがシステムの音声認識機能を使用し、音声データをAppleに送信することを許可します。
- ユーザのデスクトップフォルダにあるファイルにアクセス - アプリケーションがユーザのデスクトップフォルダにあるファイルにアクセスすることを許可します。
- ユーザーのドキュメントフォルダーにあるファイルにアクセス - アプリケーションがユーザーのドキュメントフォルダーにあるファイルにアクセスすることを許可します。
- ユーザーのダウンロードフォルダーにあるファイルにアクセス - アプリケーションがユーザーのダウンロードフォルダーにあるファイルにアクセスすることを許可します。
- ネットワークボリュームにあるファイルにアクセス - アプリケーションがネットワークボリュームにあるファイルにアクセスすることを許可します。
- リムーバブルボリュームにあるファイルにアクセス - アプリケーションがリムーバブルボリュームにあるファイルにアクセスすることを許可します。

6. 構成したいアプリケーションそれぞれについて **[アクション] > [追加]** をクリックします。

7. 以下のIDディクショナリキーに値を入力します。
    - 識別子 - 設定の名前。例："us.zoom.ZoomPresence"
    - 識別子のタイプ - バンドルIDまたはパスを選択します。例："Bundle ID"
    - コード要件 - バンドルIDまたはパスの値を指定します。例："identifier "us.zoom.ZoomPresence" and anchor apple generic"
    - 静的コード(TrueまたはFalse)
    - 許可(TrueまたはFalse)
    - コメント
8. **[保存]**をクリックします。
9. (任意)既存のプライバシー設定を削除するには、アプリケーションの下で**[アクション]** > **[削除]**をクリックします。
10. **[次へ]**をクリックして配布設定を行います。
11. **[完了]**をクリックします。

詳細は構成を作成するにはを参照してください。

クライアントプライバシー

エンドユーザーから匿名データを収集するよう構成します。これには、製品の問題を把握し、高品質のサービスを維持するためのデバイス情報や使用情報が含まれます。

対象：

- macOS対応Mobile@Work 1.67またはサポートされる以降のバージョン。
- iOS対応Go 3.5.0またはサポートされる以降のバージョン。

MIクライアントプライバシー構成の作成

手順

1. **[構成]**を選択します。
2. **[+追加]**をクリックします。
3. 検索フィールドに**[プライバシー]**と入力し、**[クライアントプライバシー]**構成をクリックします。
4. 構成の名前と説明を入力します。
5. 位置情報に基づくウェイクアップで**[SLCを有効化]**オプションを選択します。Significant-Change Location Serviceは、ユーザーの位置が15分(デフォルト)またはそれ以上の所定の時間内に大幅に変わっていた場合のみ、Go for iOSアプリに最新の位置情報を提供する省エネ機能です。このサービスを有効化すると、位置変更時にGoアプリがバックグラウンドで起動し、チェックインします。
6. MixPanel経由のデータ収集で、**[MixPanel状態を有効化]**オプションが無効になっている場合は有効にします。デフォルトでは有効化されています。
7. **[次へ]**をクリックして配布設定を行います。
8. **[完了]**をクリックします。

詳細は構成を作成するにはを参照してください。

プライバシー構成

プライバシー構成は次の条件を定義します。

- 位置情報データがデバイスで収集され、デバイス管理システムに送信されます。
- 管理者がデバイスをワイプできるかどうか
- アプリインベントリをすべてのアプリについて収集するか、アプリカタログに表示されているアプリについてのみ収集するか

プライバシー設定

デバイスワイプおよびデバイス上の全アプリのインベントリ収集は、ユーザー登録済みデバイスには適用されません。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
位置情報データを収集	位置情報データの収集を有効化する場合に選択します。**[デバイス]** ページでデバイスの位置情報を表示します。 • iOSデバイスの場合、デバイスに表示される位置情報は、ネットワークの位置情報にのみ基づいています。 • Androidデバイスの場合、位置情報は、ネットワークの位置情報とGPSの位置情報(利用可能な場合)の両方に基づいています。 • Windowsデバイスの場合、位置情報は、デバイスチェックイン時に取得した緯度と経度の値に基づいています。 デバイス上での位置情報の収集が可能である場合、現在地は4時間ごとに更新されます。デバイスが撤去されるか、プライバシー構成が無効化または削除された場合はデバイス管理システムから位置情報データが削除されます。 デバイスユーザは、デバイス上の位置情報データの収集をオフにすることができます。
デバイスワイプのアクションを無効化	管理者がデバイスをワイプできないようにする場合に選択します。ユーザー(従業員)所有のデバイスについては、このオプションの選択を検討してください。

ユーザーに位置情報サービスの有効化を指示	選択すると、ユーザーは任意で、デバイスの検索などの位置情報サービス、Wi-Fi、MTDの使用を許可または禁止できます。完全に管理されたデバイスでは、管理者がこのオプションを無効化することを選択した場合、これを自動付与できます。

アプリインベントリを収集	アプリカタログにあるかどうかに関係なく、デバイスにインストールされているすべてのアプリの情報を収集する場合は、**[アプリインベントリを収集]** を選択します。 **アプリカタログにある**アプリ、すなわちデバイスにインストールされていてアプリカタログにも表示されているアプリの情報のみ収集する場合は、**[デバイス上のアプリ]** を選択します。 **[デバイス上のすべてのアプリ]** を選択し、デバイス上のすべてのアプリに関する情報を収集します。このオプションはWindows 10+デバイスに適用されます。次のアプリソースタイプインベントリが表示され、デフォルトで選択されています。 • **非App Storeインベントリを有効化** - MDMでプッシュされた、またはエンドユーザーがアプリを手動でアンパックしてローカルでデバイスにインストールした自社開発アプリ(汎用アプリ)の場合。 • **App Storeインベントリを有効化** - Microsoft StoreまたはApps@workストアから手動でインストールしたアプリの場合。 • **システムインベントリを有効化** - MicrosoftによってWindows 10 OSとともにプリインストールされているアプリの場合。

	• **Win32インベントリを有効化** - MDMを通じたプッシュでインストールされている、またはエンドユーザーによってデバイスに直接インストールされているMSI、EXEなどのシステム32アプリの場合。 これらのアプリソースタイプインベントリのみを選択し、アプリの情報を選択的に収集することも可能です。 ⓘ 非App StoreインベントリまたはWin32インベントリを選択していない場合でも、MDMでインストールしたアプリはアプリインベントリに表示されます。 ⓘ アプリカタログについてのみアプリインベントリを収集するデフォルト構成がプライバシー構成で使用されていると、.EXEインベントリも収集されます。アプリカタログのアプリについてのみ収集する場合、すべてのアプリについて一貫性をもってインベントリが収集される必要があります。 アプリカタログで利用可能な最新のアプリ、MSIアプリ、およびEXEアプリのインベントリは、これらの各バリアントに属しているアプリが少なくとも1つ配布されたときにのみ、取得されます。
Android Enterprise devices (7.0以上) の設定	
次の設定を構成し、Android Enterpriseデバイスにプライバシーポリシーを設定します。	

組織名	デバイスを管理する組織の名前を入力します。
組織色	ユーザーの画面の背景に表示される組織色を選択します。
短いメッセージ	ユーザーが管理者によってロックされた機能を使用しようとしたときに表示される簡潔なメッセージを入力します。
長いメッセージ	ユーザーが短いメッセージをクリックしたときに表示される長いメッセージを入力します。このメッセージは、ユーザーに付与された制限に関する詳細を提供します。

詳細は構成を作成するにはを参照してください。

クライアントプライバシーステートメント情報

対象：Android、Android Enterprise、iOSデバイスまたはサポートされる以降のバージョン。

Goクライアントのプライバシーステートメント情報をユーザーに配布するための構成。これはシステム定義の構成であり、配布設定の構成のみが編集可能です。

ユーザーに表示される情報には、次の構成の一部として構成された詳細が含まれます。

- プライバシー
  - 位置情報データの収集
  - アプリインベントリの収集
  - Android 7.0+：
    - 組織名
    - 組織色
    - 短いメッセージ
    - 長いメッセージ
- クライアントプライバシー
  - SLC - 大幅な位置情報変更によりデバイスが定期的にウェイクアップ
  - 位置情報に基づくウェイクアップの最小間隔
  - MixPanel状態を有効化
- モバイルデバイス管理 - MDMアクセス権(ユーザー登録デバイスには適用されません)
  - デバイスロックとパスコードの削除
  - デバイス消去
  - ネットワーク情報(電話/SIM番号、MACアドレス)

ソフトウェア更新

対象：

- iOS 10.3+とtvOS 12.0+の監視対象デバイス
- macOS デバイス
- Windows 10+デバイス

  OS更新のルールを作成し、配布します。

  このセクションは以下のトピックを含みます。

  - iOS/tvOSデバイスのソフトウェア更新の構成
  - 非 DEP および DEP macOS デバイスのソフトウェア更新の構成
  - Windowsデバイスのソフトウェア更新の構成

iOS/tvOSデバイスのソフトウェア更新の構成

手順

監視モードのiOS/tvOSデバイスがOS更新の送信を受けることを許可するには：

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[ソフトウェア更新]** をクリックします。
4. **[iOS/tvOS]** をクリックし、構成設定セクションを表示します。
5. **[OS更新が監視対象デバイスに自動的にインストールされるのを許可する]** オプションを選択します。
6. 以下のオプションから1つ選択してください：
   - 最新版に更新する
   - 特定のバージョンに更新する - たとえばiOSバージョンを11.3.0と入力します。

7. 以下のインストールアクションから1つ選択してください：
   - デフォルト
   - ダウンロードのみ
   - 早急にインストール
8. 以下の更新時刻オプションを選択します。
   - Start time (開始時刻)
   - End time (終了時刻)
   - タイムゾーン
9. **[次へ]** をクリックします。
10. **[この構成を有効化]** オプションを選択します。
11. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
12. **[完了]** をクリックします。

> - iOSデバイスに特定のバージョンのOS更新をインストールする場合は、そのデバイスに対応するバージョンを選択する必要があります。無効なバージョンや利用不可のバージョンを選択すると、デバイスのソフトウェア更新が無視されます。
>
> - デバイスにパスコードがある場合、MDMがデバイスに更新を送信すると、デバイスが更新をキューに入れ、ユーザーはインストールを開始するためにパスコードの入力を指示されます。
> - 「iOSの制約」ページ540の `enforcedSoftwareUpdateDelay` を有効にして、ソフトウェア更新のデバイスでの手動スキャンによって、この構成でダウンロードされた特定のバージョンが削除されないようにします。

非 DEP および DEP macOS デバイスのソフトウェア更新の構成

Apple Business Manager のデバイス登録プロファイルでは、デバイスを一括で購入し、認証中に自動的にこれらのデバイスを MDM に登録できます。詳細については、「デバイス登録」ページ1162をご参照ください。

次の手順を実行すると、非 DEP および DEP macOS デバイスに OS 更新を送信できます。

手順

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[ソフトウェア更新]** をクリックします。
4. **[macOS]** をクリックし、構成設定セクションを表示します。
5. **[macOSソフトウェア更新を有効化]** オプションを選択します。

6. デバイスの更新の種類を選択します。各更新について、再起動を必要としない更新も選択可能です。

   - OS更新
   - クリティカルな更新
   - 構成データ更新
   - ファームウェア更新
   - 非クリティカル更新

   管理者は、**[非クリティカル更新]** の有効化によって非クリティカルなmacOSの更新を管理(インストール/スケジュール)できます。このオプションは既存のテナントではデフォルトで無効化されており、必要に応じて管理者がアップグレード後に明示的に有効化する必要があります。

   [OS更新] で、管理者が特定のmacOSバージョンに対してデバイスを更新することができます。

   macOS更新はすべて次のようなアクションで構成することができます。

   - デフォルト
   - 通知のみ
   - 後でインストール
   - 強制再起動をインストール
   - ダウンロードのみ
   - 早急にインストール

   - 優先度
     デフォルト - 低
     可能性のある値 - 低、高
   - 最大ユーザー遅延
     使用可能な値 - 正数
     [後でインストール] オプションを選択したときにのみ使用できます。

7. 以下の更新時刻オプションを選択します。
    - Start time (開始時刻)
    - End time (終了時刻)
    - タイムゾーン
8. **[次へ]** をクリックします。
9. **[この構成を有効化]** オプションを選択します。
10. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
11. **[完了]** をクリックします。

Windowsデバイスのソフトウェア更新の構成

手順

Windowsの更新スケジュールを構成するには:

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[ソフトウェア更新]** をクリックします。
4. **[Windows]** をクリックし、構成設定セクションを表示します。
5. Windowsデバイスのバージョンに応じて、以下のオプションを入力します。
6. **[次へ]** をクリックします。
7. **[この構成を有効化]** オプションを選択します。
8. 以下の配布オプションから1つ選択します。

- すべてのデバイス
- デバイスなし(デフォルト)
- カスタム

9. **[完了]** をクリックします。

Windows 10+デバイスのソフトウェア更新

- 更新ソース - 以下のいずれかのソースを選択します。
  - 企業向けWSUS
  - Microsoft Update および/または企業向けWSUS
- 企業WSUSサーバーへのURL
- 代替イントラネットMicrosoft更新サーバー
- 「信頼できる発行者」からの更新を許可 - 更新ソースを信頼できる発行者に限定します。
- 自動更新方法 - プルダウンメニューから以下のいずれかのオプションを選択します。
- 予定されたインストール日 - 更新の頻度を設定します。
- 予定されたインストール時刻 - 更新のインストール時刻を選択します。
- 従量制の接続を使用した更新の自動ダウンロードを許可 - 有効または無効にします。
- Windows更新スキャンを引き起こす更新延期ポリシーを許可しない - 有効または無効にします。
- 猶予付き再起動期限 - 再起動期限までの日数を選択します。
- 猶予付き再起動期限の保留 - 再起動期限を保留する日数を選択します。
- 猶予付き再起動への移行スケジュール - 移行スケジュールを再開するまでの日数を選択します。
- 空のコンテンツURLを更新/入力
- MOアプリダウンロード制限 - 以下のオプションから1つ選択してください。
  - アプリとその更新のMOダウンロード制限を無視しない
  - アプリとその更新のMOダウンロード制限を無視(無制限ダウンロードを許可)

- MO更新ダウンロード制限 - 以下のオプションから1つ選択してください。
  - OS更新のMOダウンロード制限を無視しない
  - OS更新のMOダウンロード制限を無視(無制限ダウンロードを許可)
- プレビュービルドを管理 - 以下のオプションから1つ選択してください。
  - プレビュービルドを無効化
  - 次のリリースが公開された時点でプレビュービルドを無効化
  - プレビュービルドを有効化
- 更新の自動再起動警告通知スケジュール - 自動再起動警告通知までの分数を選択します。
- 再起動警告リマインダー - 再起動警告リマインダーを設定するまでの時間数を選択します。
- 自動更新スケジュール - 自動更新の頻度を選択します。
- 更新の自動再起動通知 - 更新のための自動再起動通知をオンにします。

Windows 10.0.14393より前のデバイスのソフトウェア更新

テレメトリー制限がデバイスで無効化されている場合、以下の設定は使用できません。

- アップグレード/更新を一時停止 - 変更を後の日付に遅らせるにはオンにします。
- 更新延期期間 - 選択すると最大で4週間延期できます。
- アップグレード延期 - オンにするとアップグレードが延期されます。
- アップグレード延期期間 - 選択すると最大で8カ月延期できます。

Windows 10.0.14393以降のデバイスのソフトウェア更新

- 更新のインストール元となるブランチ - デバイスが更新を受け取るブランチをIT管理者が設定できます。
  - 半期チャネル(対象指定)
  - 半期チャネル
- 機能更新(アップグレード) - Windows 10 Professional、Windows 10 Enterprise、Windows 10 Educationのみでサポートされます。

- 更新を一時停止
- 延期期間 - 選択すると最大で180日間延期できます。

- クオリティ更新(更新) - Windows 10 Professional、Windows 10 Enterprise、Windows 10 Education、Windows 10 Mobile Enterpriseのみでサポートされます。
  - 更新を一時停止
  - 延期期間 - 選択すると最大で30日間延期できます。

Windows 10.0.17083以降のデバイスのソフトウェア更新

- 機能更新:
  - 機能更新アンインストール期間 - 機能更新をアンインストールするまでの日数を選択します。

Windows 110.0.17763以降のデバイスのソフトウェア更新

- ユーザーによる「更新を一時停止」アクセスを無効化
- ユーザーによるUXWUアクセスを無効化(Windows更新スキャン、ダウンロード、インストール)
- 更新通知レベル - 以下のオプションから1つ選択してください。
  - デフォルトのWindows更新通知を使用
  - 再起動警告を除くすべての通知をオフ
  - 再起動警告を含むすべての通知をオフ
- 機能更新:
  - 更新インストール時の自動再起動までの期限 - 自動的に再起動して更新をインストールするまでの日数を選択します。
  - 猶予付き再起動期限 - 猶予付き再起動期限の日数を選択します。
  - 猶予付き再起動期限の保留 - 再起動期限を保留する日数を選択します。
  - 猶予付き再起動への移行スケジュール - 移行スケジュールを再開するまでの日数を選択します。

セキュリティ設定の構成

管理者は、デバイスのセキュリティ設定構成を通じたユーザーによるファイアウォール設定、ロックメッセージ、パスワード変更の変更を管理または制限できます。

対象：macOS 10.10+

Procedure

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[セキュリティ]** と入力し、**[セキュリティ設定]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. 必要な構成を選択します。
   - ファイアウォール設定の変更を無効化
   - ロックメッセージの変更を無効化
   - パスワードの変更を無効化
5. **[次へ]** をクリックします。
6. **[この構成を有効化]** オプションを選択します。
7. 以下のいずれかのチャネルオプションを選択し、構成を適用します。
   - デバイスチャネル(最も一般的)
   - ユーザーチャネル(現在の登録ユーザー)
8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
9. **[完了]** をクリックします。

タイムサーバー

対象：macOS 10.12.4およびサポートされる以降のバージョン。

デバイスがカスタムタイムサーバーに接続するのを許可するタイムサーバー構成を作成します。

タイムサーバー構成の作成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[時間]** と入力し、**[タイムサーバー]** 構成をクリックします。
4. 名前と構成の説明を入力します。
5. **[NTPサーバー]** を指定します。
6. **[タイムゾーン]** の文字列を、オルソンタイムゾーンID形式（例：太平洋/ミッドウェー）で指定します。オルソンタイムゾーン形式を取得するには、管理者のmacOSデバイス上で "`/usr/sbin/systemsetup -listtimezones`" コマンドを実行してください。
7. **[次へ]** をクリックして配布設定を行います。
8. **[完了]** をクリックします。

詳細は構成を作成するにはを参照してください。

Webコンテンツフィルター

ライセンス: Silver

Webコンテンツフィルタ構成では、iOS 7+デバイスのWebアクセスを制限します。

Webコンテンツフィルタ設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
許可されたWebサイト	**アダルトコンテンツを制限:** iOSの自動フィルターに基づいてWebサイトへのアクセスをブロックしたい場合はこのオプションを選択します。これらのフィルタは、高い精度で不適切なコンテンツのWebサイトをブロックしようと試みます。 **特定のWebサイトのみ:** アクセス可能なWebサイトを手動でリスト化する場合は、このオプションを選択します。 **プラグイン(iOS 8監視対象のみ):** サードパーティのプラグインを使用する場合は、このオプションを選択します。
許可されたURL	このオプションは、[アダルトコンテンツを制限]を選択した場合にのみ利用可能です。 許可されたURLを入力します。各文字列は必ず以下のいずれかから始まらなければなりません。 • http:// • https:// 同じサイトでhttp://とhttps://の両方を許可したい場合は、2つの別のURLを入れてください。

設定	操作内容
	任意の許可URLと最初のいくつかの文字が一致するすべてのURLにアクセスできます。 例：http://www.someCompanySite.comを許可すると、以下へのアクセスも許可されます。 • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs これらのURLは、iOS自動フィルターによってブロックされていても、アクセスすることができます。
拒否リスト URL を使用	このオプションは、[アダルトコンテンツを制限] を選択した場合にのみ利用可能です。 ブロックリストのURLを入力します。各文字列は必ず以下のいずれかから始まらなければなりません。 • http:// • https:// 同じサイトでhttp://とhttps://の両方をブロックしたい場合は、それぞれのURLを入れてください。 任意のブロックリストURLと最初のいくつかの文字が一致するすべてのURLがブロックされます。 例：http://www.someCompanySite.comをブロックすると、以下へのアクセスもブロックされます。 • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs これらのURLは、iOS自動フィルターによって許可されている場合でもブロックされます。

設定	操作内容
許可リスト化されたブックマーク	このオプションは、[特定のWebサイトのみ] を選択した場合のみ利用可能です。 任意で、Safariでブックマークを追加するフォルダーを入力します。 例： /Sales/Products/ これがなければ、ブックマークはデフォルトのブックマークディレクトリに追加されます。
フィルター名	このオプションは [プラグイン] を選択した場合のみ利用可能です。 このフィルターを識別するために表示するテキストを入力します。
識別子	このオプションは [プラグイン] を選択した場合のみ利用可能です。 フィルタリングサービスを提供するプラグインのバンドルIDを入力します。
サービスアドレス	このオプションは [プラグイン] を選択した場合のみ利用可能です。 オプション：プラグインに必要なサーバーアドレスがあれば入力します。この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。
組織	このオプションは [プラグイン] を選択した場合のみ利用可能です。

設定	操作内容
	オプション：プラグインに必要な組織ストリングがあれば入力します。 この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。
ユーザー名	このオプションは [プラグイン] を選択した場合のみ利用可能です。 オプション：プラグインサービスに必要なユーザー名があれば入力します。この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。
パスワード	このオプションは [プラグイン] を選択した場合のみ利用可能です。 オプション：プラグインサービスに必要なパスワードがあれば入力します。この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。
証明書	このオプションは [プラグイン] を選択した場合のみ利用可能です。 オプション：プラグインサービスがユーザーを認証するために必要な証明書があれば入力します。この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。
Webkitトラフィックをフィルター	このオプションは [プラグイン] を選択した場合のみ利用可能です。 フィルターにWebkitトラフィックを含める場合に選択します。
ソケットトラフィックをフィルター	このオプションは [プラグイン] を選択した場合のみ利用可能です。

設定	操作内容
	フィルターにソケットトラフィックを含める場合に選択します。
カスタムデータ	このオプションは [プラグイン] を選択した場合のみ利用可能です。 オプション: プラグインサービスに必要なキー/値のペアがあれば追加します。この値が必要かどうかは、プラグインのドキュメンテーションを読んで判断します。

詳細は構成を作成するにはを参照してください。

Windowsファイアウォール

Windowsファイアウォール構成では、Windowsファイアウォールのプロファイル設定のほか、デバイスに適用したいカスタムルール群を構成できます。この構成は、ドメイン外のデバイスの管理に使用し、企業ネットワークに接続する全システムにかかるネットワークセキュリティ脅威のリスクを軽減します。

Windowsファイアウォールの構成

手順

1. **[構成]** > **[+追加]** を開きます。
2. **[ファイアウォール]** 構成を選択します。
3. **Windows**アイコンをクリックします。
4. 構成の名前を入力します。

5. ファイアウォール構成の説明を入力します。
6. [構成設定] セクションで、次の表に記載されているように残りの設定を指定します。

設定	操作内容
プロファイル	
有効化	プロファイルを有効化するにはスイッチをONにスライドさせます。
種類	プロファイルの種類を表示します。 例：ドメイン
デフォルトのインバウンドアクション	インバウンドトラフィックに実行するデフォルトアクションを選択します。 **許可**：トラフィックを許可 **ブロック**：トラフィックをブロック
デフォルトのアウトバウンドアクション	アウトバウンドトラフィックに実行するデフォルトアクションを選択します。 **許可**：トラフィックを許可 **ブロック**：トラフィックをブロック

7. ルールを追加するには、**[+追加]** をクリックして以下の設定を構成します。

設定	操作内容
ルール	
オン	プロファイルを有効化するにはスイッチをスライドさせます。
ルール名	このルールを識別する名前を入力します。
説明	このルールの目的を明示する説明を入力します。
方向	ルールを適用するトラフィックの方向を選択します。 • **イン**: インバウンドトラフィック • **アウト**: アウトバウンドトラフィック • **両方**: 両方向
アクション	実行するアクションを選択します。 • **許可**: トラフィックを許可 • **ブロック**: トラフィックをブロック
プロファイル	ルールを適用するプロファイルを選択します。 • **すべて** • **ドメイン** • **非公開** • **公開**
アプリ	パッケージファミリー名 (PEN) または実行可能アプリへのフルパスを入力します。
Protocol (プロトコル)	ルールを適用するプロトコルを以下から選択します。 • **TCP** • **UDP**

設定	操作内容
	• **ICMP**
ローカルアドレス範囲	ローカルIPv4/IPv6アドレス範囲またはサブネットマスクを入力します。
ローカルポート範囲	ローカルポートまたはポート範囲をカンマ区切りで入力します。 例：20,50,100-120
リモートアドレス範囲	リモートIPv4/IPv6アドレス範囲またはサブネットマスクを入力します。
リモートポート範囲	ローカルポートまたはポート範囲をカンマ区切りで入力します。 例：20,50,100-120
インターフェイスの種類	以下からインターフェイスの種類を選択します。 • **すべて** • **リモートアクセス** • **ワイヤレス** • **LAN** • **モバイルブロードバンド** インターフェイスの種類が選択されていない場合、デフォルトオプションの **[すべて]** が適用されます。

8. **[次へ]** をクリックします。

9. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
10. **[完了]** をクリックします。

Windows情報保護

ライセンス: Gold

対象：Windows 10+

Windows情報保護(WIP)構成は、企業データを保護するためのWIP設定を定義します。この構成は、管理下で登録されているデバイスに適用できます。また、デバイスの[概要]ページで、構成されたデバイスに関するWIPの詳細を確認することもできます。

Windows向けのWindows情報保護設定

手順

1. **[構成] > [+追加]** を開きます。
2. **[Windows情報保護]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [構成設定]セクションで、次の表に記載されているように残りの設定を指定します。
6. **[次へ]** をクリックします。
7. この構成の配布を選択します。

カテゴリ	設定	操作内容
	名前	この構成を識別する名前に入力します。
	説明	この構成の目的を明示する説明を入力します。
企業情報	**全バージョン(Windows 10+デスクトップ/Mobile)**	
	保護されたドメイン名	データ保護ポリシーが構成されているIDのリストを指定します。これらのIDに関連付けられているメールおよびその他のデータは、企業データとみなされ、保護されます。 • これは、「|」で区切られたドメインのリストであり、WindowsのUIではリストに最初に記載されているドメインがプライマリIDとみなされます。 • 例:「domain1.com|domain2.co.uk」
	ネットワークドメイン名	企業の境界を構成するドメインのリストを指定します。これらのドメインのいずれかからデバイスに送信されるデータは、企業データとみなされ、保護されます。 • これらの位置情報は、企業データの安全な共有先とみなされます。 • これは、ドメインのカンマ区切りリストです。 • 例:「mail.domain3.com, domain4.com」

カテゴリ	設定	操作内容
	クラウドリソース	保護が必要なクラウド内にホストされた企業リソースドメインのリストを含みます。これらのリソースへの接続は、企業データとみなされます。 1つ以上のドメイン名を指定します。オプションのプロキシアドレスは括弧で囲みます。 • たとえば、「domainname1.com, domainname2 (10.0.0.1)」です。 • プロキシがクラウドリソースとペアリングされている場合、このクラウドリソースへのトラフィックは指定されたプロキシサーバー(ポート80上)を経由して企業ネットワークにルートされます。 • このフィールドに指定するすべてのプロキシアドレスは、以下の内部プロキシサーバーフィールドにも入力する必要があります。
	IP範囲	企業ネットワーク内のコンピューターを定義する企業IP範囲を設定します。これらのコンピューターからのデータは、企業データの一部とみなされて保護されます。これらの位置情報は、企業データの安全な共有先とみなされます。これは、IPv4およびIPv6範囲のカンマ区切りリストです。 • これは、IPv4およびIPv6範囲のカンマ区切りリストです。 • クライアントが構成リストを受け入れる必要があり、ヒューリスティックを用いてその他のサブネットの検索を行わない場合には、**[IP範囲は信頼できます]**オプションを選択します。

カテゴリ	設定	操作内容
	中立リソース	業務用または個人用のリソースに使用できるドメイン名のリストを指定します。
	プロキシサーバー	プロキシサーバーのカンマ区切りリストを指定します。このリストにあるサーバーは企業ではないとみなされます。 • 例：「157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59」 • クライアントがプロキシの構成リストを受け入れる必要があり、その他の業務プロキシの検出を行わない場合には、**[プロキシサーバーは信頼できます]**オプションを選択します。
	内部プロキシサーバー	内部プロキシサーバーのカンマ区切りリストを指定します。 • 例：「157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59」 • これらのプロキシは、管理者によってインターネット上の特定のリソースに接続するよう構成されています。これらは、企業ネットワークの位置情報であるとみなされます。プロキシは、EnterpriseCloudResourcesポリシーの構成において、これらのプロキシを通じて照合されたクラウドリソースへトラフィックを強制するようにするためにのみ利用されます。
データ保護	**全バージョン(Windows 10+デスクトップ/Mobile)**	

カテゴリ	設定	操作内容
	強制レベル	次の強制レベルから1つ選択します。 • オフ - 保護なし(それまで暗号化されていたデータの暗号化が解除されます)。 • サイレント - データを暗号化し、データが保護された後でデバイス上の活動を監視します。ユーザーには、ネガティブなデータ/アプリ情報のアカウントに関するプロンプトが表示されません。 • オーバーライド - サイレントモードとほぼ同様ですが、それに加えて、アプリまたはデータが不適切に使用されている場合には、ユーザーが実行中の操作を続行するかキャンセルするかを選択するプロンプトが表示されます。 • ブロック - サイレントモードとほぼ同様ですが、それに加えて、アプリまたはデータが不適切に使用されている場合には、ユーザーが実行中の操作がブロックされ、操作がブロックされた理由を示す警告がユーザーに表示されます。 [オフ] モードを除き、企業データまたはリソースを使用することが想定されていなかったデータまたはアプリは、デバイスにログオンされることになります。当該のデータは、別の構成サービスプロバイダー(CSP)を使用してデバイスから削除できます。

カテゴリ	設定	操作内容
	データリカバリー証明書	暗号化されたファイルのデータリカバリーに使用できるリカバリー証明書を指定します。 • これは、暗号化ファイルシステム(EFS)のデータリカバリーエージェント(DRA)証明書と同じです。ただし、この証明書はグループポリシーではなくMDMを介して配信されます。 また、次のオプションのうち1つ以上を選択することもできます。 • ユーザーによる解読を許可 • 登録解除時に取り消す • EDPアイコンを表示 • ロック下で保護を要求(Windows 10 Mobileのみ)
RMS	**全バージョン(Windows 10+デスクトップ/Mobile)**	
	Azure RMSを許可	WIP向けにAzure権限管理(Azure RMS) 暗号化を許可するかどうかを指定します。
	RMSテンプレートID	RMS暗号化にTemplateID GUIDを使用することを指定します。RMSテンプレートでは、管理者が、RMS保護されたファイルへのアクセスを誰に、どの程度の時間にわたって許可するかを詳しく構成することができます。
アプリ制御	**全バージョン(Windows 10+デスクトップ/Mobile)**	
	[アプリ] > [アプリカタログ] ページにおいてWIPの値で構築されたアプリの集合を指定します。次のパラメーターセットを使用してアプリのルール定義を指定します。	

カテゴリ	設定	操作内容
	アプリの種類	次のアプリの種類から1つを選択します。 • Publisher/PFN Equals - PFNをサポートしているWindows 10 Mobileと Windows 10デスクトップに適用されます。 • EXE/Win32 Equals - Windowsデスクトップにのみ適用されます。
	アプリ識別子	表示されたアプリの中から選択し、アプリ識別子に追加します。**[アプリ検索]** をクリックすることもできます。
	アプリの説明	アプリの説明を入力します。

Windowsの制約

Windows制約構成は、Windows搭載デスクトップ/モバイルデバイスで有効にする機能を決定します。

Windows制約設定

カテゴリ	設定	操作内容
	名前	この構成を識別する名前に入力します。
	説明	この構成の目的を明示する説明を入力します。
デバイスの機能	**全バージョン(Windows 10デスクトップ/Mobile、Windows 8.1デスクトップ/Mobile)**	
	Wi-Fiのオフロードを無効化	デバイスが互換性のあるネットワークにアクセスし、許可されたワイヤレスネットワーク用のデータを保存するのを防ぐ場合に選択します。
	インターネット共有を無効化	デバイスが別のワイヤレスデバイスを通じてインターネットにアクセスできないようにする場合に選択します。
	位置情報を無効化	位置情報サービスを無効にする場合に選択します。
	セルラーデータローミングを無効化	デバイスがセルラーモードにあるときにデータローミングを無効にする場合に選択します。
	Bluetoothを無効化	デバイスがBluetooth接続を確立できないようにする場合に選択します。
	ローミング中またはセルラーネットワーク上ではVPNを無効化	デバイスがWi-Fi上にないとき、VPN接続を確立できないようにする場合に選択します。
	8.1 Windows Phone 8.1のみ	
	Wi-Fiホットスポット報告を無効化	デバイスがホットスポット情報を自動的にMicrosoftに報告できないようにする場合に選択します。
	8.1+ Windows Phone 8.1/Windows 10 Mobile	

カテゴリ	設定	操作内容
	Wi-Fiを無効化	デバイスがワイヤレスネットワークにアクセスできないようにする場合に選択します。
	Wi-Fiの手動構成を無効化	Ivanti Neurons for MDMが定義した以外のワイヤレスネットワークにデバイスがアクセスできないようにする場合に選択します。
	NFCを無効化	デバイスが他のデバイスに接触したり近接したりすることで無線通信を確立できないようにする場合に選択します。
	手動でのルート証明書のインストールを無効化	エンドユーザーが手動でルートや仲介認証をインストールできないようにする場合に選択します。
テレメトリー - デバイスによる診断/利用テレメトリーデータの送信を許可	**Windows 10のみ**	
	テレメトリーレベル	データレポートに関して以下のいずれかのテレメトリーレベルを選択してください: • **セキュリティ** - 接続ユーザー体験、テレメトリーコンポーネント設定、マルウェア削除ツール、Windows Defenderに関する情報を送信。 • **基本** - クオリティ関連データ、アプリ互換性、アプリ利用データ、セキュリティレベルからのデータを含む基本的デバイス情報を送信。 • **拡張** - Windows、Windows Server、System Center、アプリの使用とパフォーマンスを含む詳細情報を送信。詳細な信頼性データ、および基本レベルとセキュリティレベル両方からのデータも含みます。

カテゴリ	設定	操作内容
		• **フル(デフォルト)** 問題を特定し、修正に役立つすべてのデータに加え、セキュリティ、基本、拡張レベルからのデータを送信。
データ損失の防止(DLP)	**全バージョン(Windows 10デスクトップ/Mobile、Windows 8.1デスクトップ/Mobile)**	
	カメラを無効化	エンドユーザーがカメラアプリを使用できないようにする場合に選択します。
	SDカードへのアクセスを無効化	デバイスがストレージカードにアクセスできないようにする場合に選択します。
	8.1 Windows Phone 8.1のみ	
	オフラインの[名前を付けて保存]を無効化	エンドユーザーがOfficeハブのファイルを[名前を付けて保存]できないようにする場合に選択します。
	オフライン共有を無効化	エンドユーザーがOfficeハブのファイルを共有できないようにする場合に選択します。
	8.1+ Windows Phone 8.1/Windows 10 Mobile	
	コピー/貼り付けを無効化	エンドユーザーがアプリ間でデータのコピーや貼り付けができないようにする場合に選択します。
	スクリーンキャプチャを無効化	エンドユーザーがデバイスでスクリーンキャプチャ機能を使用できないようにする場合に選択します。
	音声録音を無効化	エンドユーザーが音声録音機能を使用できないようにする場合に選択します。
	USB大容量記憶装置を無効化	エンドユーザーがUSB経由でデスクトップからデバイスのストレージにアクセスできないようにする場合に選択します。
データ使用量	**Windows 10以上**	

カテゴリ	設定	操作内容
	3G接続のコスト	以下のオプションから1つ選択してください： • **無制限** - 接続に制限がなく、利用料金や容量の制限もありません。 • **固定** - 所定のデータ量を上回ると、接続に利用料金と容量の制限がかかります。 • **変動** - バイト単位で接続に料金がかかります。
	4G接続のコスト	
Defender	**Windows 10以上**	
	Defenderリアルタイム監視機能を無効化	Defenderリアルタイム監視機能を無効化する場合に選択します。
Device Guard	**Windows 10以上**	
	仮想化ベースのセキュリティ(VBS) を無効化	仮想化ベースのセキュリティがセキュリティサービスのサポートを提供するのを禁止する場合に選択します。
	仮想化ベースのセキュリティを使用したCredential Guard	以下のオプションから1つ選択してください： • **無効化** - 仮想化ベースのセキュリティを使用したCredential Guardを無効化します。 • **UEFIロックありで有効化** - UEFI(Unified Extensible Firmware Interface) ロックありで、仮想化ベースのセキュリティを使用したCredential Guardを有効化します。 • **ロックなしで有効化** - UEFIロックなしで、仮想化ベースのセキュリティを使用したCredential Guardを有効化します。
	プラットフォームセキュリティレベル(プラットフォームセキュリティ機能が必要)	以下のオプションから1つ選択してください： • **セキュアブートありのVBS** - セキュアブートありで仮想化ベースのセキュリティを有効化する場合に選択します。

カテゴリ	設定	操作内容
		• **セキュアブートおよびダイレクトメモリアクセスありのVBS** - セキュアブートおよびダイレクトメモリアクセス(DMA) ありで仮想化ベースのセキュリティを有効化する場合に選択します。
プライバシー	**Windows 10以上**	
	広告IDを無効化	広告IDを無効化する場合に選択します。
	アプリ/OSによるアクティビティフィードの公開を無効化	アプリ/OSによるアクティビティフィードの公開を無効化する場合に選択します。
Windowsとアプリケーション	**全バージョン(Windows 10デスクトップ/Mobile、Windows 8.1デスクトップ/Mobile)**	
	メール以外のサービスを提供するMicrosoftアカウントを無効化	エンドユーザーがMicrosoftアカウントをEメール以外のサービスの認証に使用できないようにする場合に選択します。
	Microsoft以外のアカウントを無効化	エンドユーザーがMicrosoft以外のアカウントでEメールを構成できないようにする場合に選択します。
	Cortanaパーソナルアシスタントを無効化	エンドユーザーがMicrosoftのパーソナルアシスタントにアクセスできないようにする場合に選択します。
	位置情報に基づく検索を無効化	検索アプリがデバイスの位置情報を使用できないようにする場合に選択します。
	Developer Unlockを無効化	エンドユーザーがアプリをサイドローディングできないようにする場合に選択します。デバイスをMDMに登録したときのデフォルトモードではサイドローディングが許可されています。
	11+のEnterpriseエディション	
	タスクバーのTeamsチャットアイコンの設定	以下のオプションから1つ選択してください：

カテゴリ	設定	操作内容
		• **表示**：チャットアイコンがデフォルトでタスクバーに表示されます。ユーザーが[設定]で表示と非表示を切り替えることができます。 • **非表示**：チャットアイコンがデフォルトで非表示となります。ユーザーが[設定]で表示と非表示を切り替えることができます。 • **無効**：チャットアイコンが表示されず、この場合はユーザーが[設定]で表示と非表示を切り替えることができません。 • **構成なし**：チャットアイコンの挙動は、お使いのWindowsエディションのデフォルト設定によって決まります。 変更は、Windowsデバイスを再起動するまで適用されません。
	Windows Phone 10+	
	Microsoft Storeからのアプリの自動更新を無効化	Microsoft Storeからのアプリの自動更新を禁止する場合に選択します。
	Microsoft Storeからプリインストールまたはダウンロードされたすべてのアプリの起動を無効化	エンドユーザーが、Microsoft Storeからプリインストールまたはダウンロードされたすべてのアプリを起動できないようにする場合に選択します。 WindowsのEnterpriseとEducationのエディションのみサポートします。
	アプリをバックグラウンドで実行	以下のオプションから1つ選択してください： • **ユーザーが制御**：バックグラウンドでのアプリ実行をユーザーが制御できます。

カテゴリ	設定	操作内容
		• **強制許可**：バックグラウンドでのアプリ実行を許可します。 • **強制拒否**：バックグラウンドでのアプリ実行を禁止します。
	Windows Phone 8.1のみ	
	画像検索機能からの画像保存を無効化	エンドユーザーがBing Visionが検索する画像を保存できないようにする場合に選択します。
	8.1+ Windows Phone 8.1/Windows 10 Mobile	
	Microsoft Storeを無効化	エンドユーザーがMicrosoftのアプリストアにアクセスできないようにする場合に選択します。
	Internet Explorerを無効化	エンドユーザーがInternet Explorerにアクセスできないようにする場合に選択します。
	Action Centerからのアラートを無効化	ロック画面の上にAction Centerのアラートを表示しないようにする場合に選択します。
セキュアブラウザ設定	**10+ Windows 10デスクトップ/Mobile**	
	デスクトップでブラウザのポップアップを無効化	(デスクトップデバイスのみ) Microsoft Edgeブラウザでポップアップブラウザウィンドウを無効化する場合に選択します。
	パスワードマネージャーを無効化	デバイス上でのパスワードのローカル保存と管理を無効化する場合に選択します。
その他の制約	**全バージョン(Windows 10デスクトップ/Mobile、Windows 8.1デスクトップ/Mobile)**	
	UEMからの登録解除機能および職場アカウント削除機能を無効化	エンドユーザーがUEMへの登録を解除したり、社内アカウントイメージを削除したりできないようにする場合に選択します。
	Windows Phone 10+	

カテゴリ	設定	操作内容
	コントロールパネルとハードウェアキーの組み合わせを使用したユーザーによるデバイスの工場出荷時状態へのリセットを無効化	エンドユーザーがデバイスロック猶予期間を設定するのを防ぐ場合に選択します。
	ユーザーがデバイス設定中にネットワークに接続する必要があります(Autopilotプロファイルが必要)	Autopilot機能を使用して登録されたすべてのWindowsデバイスをTenantLockdownでロックできるようにするには、このオプションを選択します。
	8.1+ Windows Phone 8.1/Windows 10 Mobile	
	デバイス暗号化を要求	社内ストレージの暗号化をオンにする場合に選択します。このオプションは、一度オンにするとUEMサーバーでは変更できません。
	ユーザーによるデバイスロック猶予期間設定を無効化	ユーザーがデバイスロック猶予期間を設定するのを防ぐ場合に選択します。

Windows Phone 8.1デバイスはこのシリアル番号を報告しません。

Windowsデスクトップ制約

対象：Windows10デスクトップ

このセクションは以下のトピックを含みます。

- Windowsデスクトップ制約の構成
- リムーバブルストレージデバイスの許可リスト作成

管理者は、デバイスの以下へのユーザーアクセスを制限することにより、Windows 10マネージドデスクトップデバイスのOS情報を制御できます。

- コントロールパネル
- タスクマネージャー
- エクスプローラー
- レジストリエラー

上記の機能により、ユーザーはデバイスに多くの変更を加えることができます。管理者は、このようなシステムレベルの制御機能へのアクセスを制限することにより、セキュリティを確保できます。

これにはBridgeが必要です。詳細は「Ivanti Bridge」 ページ410をご覧ください。

Windowsデスクトップ制約の構成

手順

1. **[構成] > [+追加]** を開きます。
2. **[Windowsデスクトップ制約]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。

5. [構成設定] セクションで、次の表に記載されているように残りの設定を指定します。

設定	操作内容
タスクマネージャー	アクセスを拒否するものについて **[アクセスを拒否]** にチェックを入れます。
コントロールパネル	
レジストリエディター	
ファイルエクスプローラー	エクスプローラーの機能を制限するには **[機能を制限]** にチェックを入れます。例：地図ネットワークドライブの削除。 制限されている機能のリストを表示するには、リンクをクリックします。
リムーバブルストレージ	
リムーバブルストレージのアクセスモード	• **読み取りアクセスを制限**：アクセスをすべて拒否する最も厳しい設定です。 • **書き込みアクセスを制限**：アクセスが制限されます。ただし、不正なデータの削除やデバイスをウイルスに感染させる機能などは防止されます。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし（デフォルト）
   - カスタム
8. **[完了]** をクリックします。

> 構成を完全に有効にするには、構成を適用した後でデバイスを再起動する必要があります。

リムーバブルストレージデバイスの許可リスト作成

許可されるストレージデバイスの許可リストを作成したい場合は、まず以下の手順に従います。

- 許可したいUSBストレージデバイスをPCに接続します。
- デバイスマネージャーを開き、USBコントローラーをクリックします。
- 各コントローラーの設定でデバイス情報を確認します。
- 許可リストの作成に使用するデバイス情報を保存します。

リムーバブルストレージデバイスの許可リストを作成するには：

手順

1. **[Windowsデスクトップ制約]** 構成ページで **[許可リストのリムーバブルストレージ]** セクションにある **[+追加]** をクリックします。
2. **[ハードウェアIDを追加]** ウィンドウで、許可リストに追加したい1つ以上のデバイスのハードウェアIDを入力します。
3. **[ハードウェアIDを追加]** をクリックします。許可リストに入れたハードウェアIDのリストは **[許可リストのリムーバブルストレージ]** セクションに表示されます。

> ハードウェアIDを編集またはリストから削除するには、[**アクション**] 列の編集または削除オプションを選択します。
> 構成を完全に有効にするには、構成を適用した後でデバイスを再起動する必要があります。

Windows 10のデスクトップ設定

Windows 10のデスクトップ設定では、デスクトップ設定をカスタマイズし、Windows 10デバイスにプッシュできます。この構成により、以下のデスクトップ設定を構成できます。

- デスクトップ背景画像
- ロック画面画像
- カスタムスクリーンセーバーのアップロード
- デスクトップショートカット

これにはBridgeが必要です。詳細は「Ivanti Bridge」 ページ410をご覧ください。

手順

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[Windows 10のデスクトップ設定]** 構成を選択します。**[Windows 10のデスクトップ設定]** ページが表示されます。
3. **[名前]** フィールドに適切な設定名を入力します。

4. （任意）+**説明を追加**リンクをクリックして、構成の説明を追加します。

5. **[構成設定]** セクションで、以下の設定を構成します。

設定	説明
ファイル送信	デスクトップ設定のファイル配信オプションを次のいずれかから選択します。 • **ファイルをアップロード** - 設定を Ivanti Neurons for MDM にアップロードします。 • **URLをオーバーライド** - ダウンロードする設定ファイルとオーバーライド URLを提供します。
デスクトップ壁紙設定	**[ファイルの選択]** をクリックして、壁紙画像を検索してアップロードします。サポートされているファイル形式は BMP、JPG、JPEG、PNG です。
ロック画面壁紙設定 (ロック画面の壁紙設定は、Windows 10 Pro デバイスでは **サポートされません**)	**[ファイルを選択]** をクリックし、壁紙画像をアップロードします。 サポートされるファイル形式は.bmp、.jpg、.jpeg、.pngです。
スクリーンセーバー設定	**[ファイルを選択]** をクリックし、スクリーンセーバーファイルを指定してアップロードします。 Windows対応の.SCRファイルのみアップロードしてください。 スクリーンセーバーモードのロックを解除するパスワードを設定する場合は、**[スクリーンセーバーのパスワード保護]** を選択します。

設定	説明
	スクリーンセーバー タイムアウト 時間 (分) を選択します。
デスクトップショートカット	デバイスのデスクトップに追加するデスクトップショートカットを設定するには、**[ショートカットを追加]** をクリックします。**[ショートカットを追加]** ウィンドウが表示されます。以下のオプションを使用して表を埋めてください。 • **場所** - Windowsデバイス上でショートカットが表示される場所を入力します。 • **ターゲットパス** - ショートカットの行先となるローカルパス、UNCパス、またはドライブ文字を入力します。ターゲットパスはURLでもかまいません。 • **引数** - ターゲットファイルを開くときに使用する引数を入力します。 • **ワーキングディレクトリ** - ターゲットが要求するファイルを含むフォルダーパスを入力します。 • **アイコンファイル** - 有効なWindows .icoファイルをアップロードします。 オプションを構成後、**[ショートカットを追加]** をクリックします。

6. **[次へ]** をクリックします。

7. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
8. **[完了]** をクリックします。

Windows Hello for Business構成

この構成により管理者はデバイスでWindows Helloのセットアップを実行します。Windows Helloのセットアップにはデバイスにサインインするピンを設定する必要があります。

対象：Windows 10

Procedure手順

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[Windows]** と入力し、**[Windows Hello for Business]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. **[Windows 10デバイスでWindows Hello for Businessを有効化/無効化]** をトグルして、**[オン]** を選択します。

   > トグルスイッチはデフォルトでオンに設定されています。Windows Hello for Businessを無効化しても、デバイスからPINは削除されません。

5. **[PINの複雑さ]** を設定します。
6. 必要な構成を選択します。
   - Windows Hello for Business用のTPM(Trusted Platform Module) が必要
   - スマートカード証明書としてWindows Hello for Business証明書を使用
   - Windows Hello for BusinessのPINジェスチャーの代わりに顔や指紋などの生体ジェスチャーを使用
   - Windows Hello顔認証機能に顔の特徴の認識に対応する高度ななりすまし防止機能が必要
   - 動的ロック
   - ユーザーによるFIDO2セキュリティキーでのサインインを許可
7. **[次へ]** をクリックします。
8. **[この構成を有効化]** オプションを選択します。

9. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
10. **[完了]** をクリックします。

Play Integrity(旧称SafetyNet Attestation)

Play Integrity(旧称SafetyNet) は、GoogleのPlay Integrity APIを使用したAndroidデバイスのセキュリティと互換性の評価に役立ちます。構成した場合、定期的にデバイスを分析し、デバイスが改ざんされたかどうか判断することができます。

手順

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[Play Integrity]**構成を選択します。**[Play Integrity構成]** ページが表示されます。
1. **[名前]** フィールドに、Play Integrity構成の適切な名前を入力します。
2. +[**説明を追加**] リンクをクリックし、構成の説明を追加します。このフィールドはオプションです。
3. **[構成設定]** セクションで、デバイスでセキュリティおよび互換性チェックを評価するために適用される最小間隔 (時間) を入力します。値は 1 ～ 24 の範囲です。
4. **[次へ]** をクリックして以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
5. **[完了]** をクリックします。

高度なAndroidパスコードおよびロック画面

Androidデバイスにおける高度なAndroidパスコードおよびロック画面の構成により、デバイスのセキュリティを維持することができます。この構成は、デバイスにおけるデバイスパスコード、および会社所有デバイス上の仕事用プロファイルのパスコード設定に適用されます。

この構成をデバイスに適用すると、既存のパスコードや仕事用本人確認の構成があっても適用されなくなります。

仕事用プロファイルおよび会社所有デバイス上の仕事用プロファイルに関し、Android 12以降のデバイスでは、デバイスレベルのパスコードのパスコードクオリティが廃止されます。また、管理者がパスワードの複雑さ設定を有効にしていない場合、既存のパスコードの質設定は、Go appによって自動的にパスワードの複雑さ設定に変換されます。

手順

1. **[構成]** > **[+追加]** を開きます。
2. **[高度なAndroidパスコードおよびロック画面]** 構成を選択します。
3. 構成の名前と説明を入力します。
4. **[構成設定]** セクションで、以下の設定を構成します。

設定	操作内容
デバイスパスコード	
デバイスパスコードを要求	トグルスイッチを **[オン]** にします。
パスコードの複雑性 (Android v12.0+)	
[パスコードの複雑性] 設定は、**[パスコードクオリティ]** 設定より優先されます。**[デバイスパスコードを要求]** オプションがONになっており、**[パスコードの複雑性]** が設定されている場合、**[パスコードクオリティ]** 設定は無視されます。	

設定	操作内容
パスコードの複雑性を有効化	トグルスイッチを **[オン]** にし、以下のいずれかを選択します。 • **なし** - パターン、PIN、英数字/アルファベット文字列に関する複雑性を使用しない。 • **低** - パターンまたは数字4桁以上のパスコードを設定。 • **中** - 以下のいずれかのパスコードを設定：数字(4桁以上)、アルファベット(4文字以上)、英数字(4文字以上)。 • **高** - 以下のいずれかのパスコードを設定：数字(8桁以上)、アルファベット(6文字以上)、英数字(6文字以上)。
パスコードの性質	以下のドロップダウンリストからパスコードの性質を選択します。 • **生体認証** - 顔認証などの生体認証によるロック解除を許可します。 • **何か** - パスワードを要求しますが、種類の制限は設定しません。 • **数字** - 少なくとも数字を含むパスワードを要求します。 • **複雑な数字** - 少なくとも数字を含み、重複(4444など)や順序(1234など)のないパスワードを要求します。 • **アルファベット** - 少なくともアルファベットや他の記号を含むパスワードを要求します。

設定	操作内容
	• **英数字** - 少なくとも数字とアルファベット(または他の記号)を含むパスワードを要求します。 • **複合** - 数字、アルファベット、特殊文字を含むパスワードを要求します。
最小文字数	スライダーでパスワードの最小文字数を指定し、ユーザーが短くセキュアでないパスコードを作成しないようにします。範囲は4～16です。
パスコードの有効期限	以下のフィールドに値を入力します。 • **有効期限** - パスコードの有効期間を日数で指定します。 • **履歴保存** - パスコードを何回変更すれば同じパスコードを再び使用できるかを指定します。 • **最大失敗回数** - ユーザーが誤ったパスコードを何回入力すれば企業データがデバイスからワイプされるかを指定します。 • **無活動タイムアウト** - セッションが切れるまでのユーザーの無活動時間の最大値を指定します。
キーガード機能を管理	以下のチェックボックスオプションから必要なキーガード機能を有効化します。 • **指紋を有効化** • **セキュアカメラを有効化** • **すべての通知を有効化** デバイス所有者モードの場合。

設定	操作内容
	• **すべてのトラストエージェントを有効化 デバイス管理者とデバイス所有者モードのみ。** • **虹彩スキャンを有効化** Android 9.0+またはSamsungのみ。 • **顔認識によるロック解除を有効化** Android 9.0+またはSamsungのみ。

スマートロックを管理 (Android 6.0+)	トグルスイッチを **[オン]** にすると、スマートロック構成を管理できます。
	以下のチェックボックスオプションから必要なスマートロックを有効化します。
	• **Bluetoothロック解除を有効化**
	  • 音声/動画デバイスを無効化
	  • コンピューターデバイスを無効化
	  • 医療用デバイスを無効化
	  • 画像処理デバイスを無効化
	  • その他のデバイスを無効化
	  • ネットワーキングデバイスを無効化
	  • ペリフェラルデバイスを無効化
	  • 電話を無効化
	  • おもちゃのデバイスを無効化
	  • 未分類のデバイスを無効化
	  • ウェアラブルデバイスを無効化
	• **NFCロック解除を有効化**

設定	操作内容
	• 非セキュアタグを有効化 • セキュアタグを有効化 • **場所(位置情報)を有効化** • 設定した場所(自宅以外)を有効化 • **顔認識によるロック解除(Samsungの顔認識によるロック解除など)を有効化** • **オンボディロック解除を有効化** • **音声認識によるロック解除を有効化**
仕事用プロファイルパスコード(本人確認)(Android 7.0+)	
仕事用プロファイルパスコード(本人確認)を要求	トグルスイッチを **[オン]** にします。
パスコードの複雑性(Android v12.0+)	
パスコードの複雑性を有効化	トグルスイッチを **[オン]** にし、以下のいずれかを選択します。 • **なし** - パターン、PIN、英数字/アルファベット文字列に関する複雑性を使用しない。 • **低** - パターンまたは数字4桁以上のパスコードを設定。 • **中** - 以下のいずれかのパスコードを設定:数字(4桁以上)、アルファベット(4文字以上)、英数字(4文字以上)。

設定	操作内容
	• **高** - 以下のいずれかのパスコードを設定：数字（8桁以上）、アルファベット（6文字以上）、英数字（6文字以上）。
パスコードの性質	以下のドロップダウンリストからパスコードの性質を選択します。 • **生体認証** - 顔認証などの生体認証によるロック解除を許可します。 • **何か** - パスワードを要求しますが、種類の制限は設定しません。 • **数字** - 少なくとも数字を含むパスワードを要求します。 • **複雑な数字** - 少なくとも数字を含み、重複（4444など）や順序（1234など）のないパスワードを要求します。 • **アルファベット** - 少なくともアルファベットや他の記号を含むパスワードを要求します。 • **英数字** - 少なくとも数字とアルファベット（または他の記号）を含むパスワードを要求します。 • **複合** - 少なくとも数字、アルファベット、特殊文字を含むパスワードを要求します。
パスコードの有効期限	以下のフィールドに値を入力します。 • **有効期限** - パスコードの有効期間を日数で指定します。

設定	操作内容
	• **履歴保存** - パスコードを何回変更すれば同じパスコードを再び使用できるかを指定します。 • **最大失敗回数** - ユーザーが誤ったパスコードを何回入力すれば企業データがデバイスからワイプされるかを指定します。 • **無活動タイムアウト** - セッションが切れるまでのユーザーの無活動時間の最大値を指定します。 **強力な認証のタイムアウト**(プロファイル所有者、デバイス所有者、および仕事用プロファイルを持つマネージドデバイスのAndroid 8.0+のデバイスにのみ適用可能) - 二次認証(指紋、生体認証)を使用したデバイスのロック解除がタイムアウトするまでの時間を分数で指定します。このフィールドは **[パスコードの性質]** オプションとして **[生体認証]** または **[何か]** が選択されている場合にのみ適用されます。 最小は60分、最大は4320分です。このフィールドが空白になっている場合は、デバイスに対して何も設定されていないということになります。
キーガード機能を管理	以下のチェックボックスオプションから必要なキーガード機能を有効化します。 • **指紋を有効化** • **セキュアカメラを有効化**

設定	操作内容
	• **すべてのトラストエージェントを有効化** • **虹彩スキャンを有効化** Android 9.0+またはSamsungのみ。 • **顔認識によるロック解除を有効化** Android 9.0+またはSamsungのみ。

5. **[次へ]** をクリックします。
6. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
7. **[完了]** をクリックします。

Microsoft Defender for Endpoint

以前Windows Advanced Threat Protectionと呼ばれていたMicrosoft Defender for Endpoint(MDE) 構成を使用することで、お客様は、MDEサービスへのデバイスのオンボードとオフボードを行えます。

手順

1. **[構成] > [+追加]** を開きます。
2. **[Microsoft Defender for Endpoint]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [構成設定] セクションで、次の表に記載されているように残りの設定を指定します。

設定	説明
BLOBのオンボーディングまたはオフボーディング	Microsoft Defender for Endpointセキュリティセンターサイトから、BLOBのオンボーディングまたはオフボーディングを貼り付けます。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

証明書ベースの認証

Ivanti Neurons for MDMは、管理者がデジタル証明書とテナント指定の(バニティ)ホスト名を使用してログインできるようにする、証明書ベースの認証をサポートしています。これを有効化し、設定すると、管理者は基本的な認証(ユーザー名とパスワード)ではなくデジタル認証でログインできます。

この機能はデフォルトで無効化されています。テナントでこの機能を有効にするには、管理者がサポートに問い合わせる必要があります。この機能はNA3クラスター環境でのみ、なおかつサポートが有効化した場合のみ使用可能です。テスト済みのスーパー管理ユーザー名とパスワードを必ず準備してください。証明書ベースの認証が有効化された後、バニティドメインの設定が正常に完了するまで、それらの認証情報がログインに使用できる唯一の認証情報となります。

手順

1. **[管理]** タブで **[バニティホスト構成]** を選択します。
2. [バニティホスト構成] ページで次のオプションを設定します。

設定	操作内容
バニティドメインの作成	バニティドメインの名前を入力します。これはデジタル証明書でログインできる企業IDに近いドメイン名です。
信頼できる発行CAの証明書をアップロード	**[ファイルを選択]** をクリックし、管理者に証明書を発行するCAの証明書を選択してアップロードします。 証明書の失効チェックを有効化するには **[この証明書の証明書ステータス検証設定を有効化]**(任意)を選択します。 ⓘ このオプションはデフォルトで有効に設定されています。証明書の失効チェックを無効化する場合は選択を解除してください。 さらに証明書を追加するには **[さらに追加]** をクリックします。 ⓘ 証明書形式が.p7b、.pem、.der、.crt、.cerのいずれかであることを確認してください。
証明書属性マッピング	証明書属性マッピングでは、管理者のアカウント属性に対する証明書ID要素のマッピングを構成します。 **[証明書から]** フィールドでは以下の証明書要素のいずれかを選択します。

設定	操作内容
	• **NTのプリンシパル名** • **RFC 822名** **[変数へ]** フィールドでは以下の管理者のアカウント属性のいずれかを選択します。 • **ユーザーUPN** • **$UserEmailAddress** • **$EDIPI**

3. **[保存]** をクリックします。

   バニティホストがアクセス可能になるまで数分かかる場合があります。

ユーザーリソース構 成

このセクションは以 下 のトピックを含 みます。

CalDAV構成

CalDAV構成では、CalDAVインターネット標準を使用してWebカレンダーへのアクセスを定義します。

CalDAVの設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ホスト名とポート	カレンダーサーバーのホスト名とポートを入力します。
プリンシパルURL	カレンダーサーバーにアクセスするためのURLを入力します。
ユーザー	アクセスに使用するユーザー名を入力します。
パスワード	アクセスに使用するパスワードを入力します。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL)のみを選択し、使用してください。
アプリごとのVPN	**必須事項:** CalDAV構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで設定済みの[Per-App VPN構成]を選択します。 **対象:** iOS 14+

詳細は構成を作成するにはを参照してください。

CardDAV構成

CardDAVでは、CardDAVインターネット標準を使用してWebアドレス帳へのアクセスを定義します。

CardDAVの設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ホスト名とポート	アドレス帳サーバーのホスト名とポートを入力します。
プリンシパルURL	アドレス帳サービスにアクセスするためのURLを入力します。
ユーザー名	アクセスに使用するユーザー名を入力します。
パスワード	アクセスに使用するパスワードを入力します。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL)のみを選択し、使用してください。
アプリごとのVPN	**必須事項:** CardDAV構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで設定済みの[Per-App VPN構成]を選択します。 **対象:** iOS 14+
iOS 10+	
通信サービスの規則	CardDAVシステム内の連絡先に電話をかけるときのデフォルトアプリを選択します。

詳細は構成を作成するにはを参照してください。

Google構成

Googleアカウント構成は、iOS 9.3.2またはAndroid 6.0デバイス、またはサポートされる以降のバージョンとGoogleアカウントを連携させます。GoogleアカウントにはAndroid Enterpriseが必要です。この構成では、複数のGoogleメールアドレスおよびユーザーが認証後に有効化する任意のGoogleサービスを設定できます。

手順

1. **[構成] > [+追加]** を開きます。
2. **[Googleアカウント]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。

5. [構成設定]セクションで、次の表のとおりに残りを設定します。

6.

設定	操作内容
iOS 9.3.2以降、Android 6.0以降	
名前	この構成を識別する名前に入力します。
アカウントの説明	アカウントの表示名を入力します。
アカウント名	アカウントユーザーのフルネームを入力します。
メールアドレス	アカウントのGoogleメールアドレスを入力します。
アプリごとのVPN	**必須事項**：Googleアカウント構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで設定済みの[Per-App VPN構成]を選択します。 **対象**：iOS 14+
iOS 10+	
通信サービスの規則	以下のオプションのいずれかを選択し、Googleシステム内の連絡先に電話をかけるときのデフォルトアプリを選択します。 • **アプリカタログおよびシステムアプリから**：アプリ名の最初の数文字を入力して検索します。 • **バンドルID(Appleシステムアプリのみ)**：システムアプリバンドルIDを入力します。バンドルIDは「com.apple」で始まる必要があります。

7. **[次へ]**をクリックします。

8. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
9. **[完了]** をクリックします。

Googleアカウント構成がデバイスに適用されると、Goクライアントがユーザーにログインを指示します。

詳細は構成を作成するにはを参照してください。

Eメール構成

Eメール構成では、デバイスのPOPまたはIMAP Eメールを設定します。

Eメールの設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
アカウントの説明	このEメールアカウントを識別するために使用するテキストを入力します。
アカウントの種類	IMAPまたはPOPを選択します。IMAPを選択した場合、パスの接頭辞も入力できます。使用可能なアカウントの種類については、各インターネットサービスプロバイダ(ISP)までお問い合わせください。接頭辞は、一般的に、すべてのIMAPフォルダを受信トレイに表示する際に必要となります。接頭辞を必要とするISPは通常、設定する特定の接頭辞について情報を提供しています。
ユーザー表示名	Eメールアカウントを識別するために使用するテキストを入力します。ユーザーはこの値をデバイス上でも設定できるという点に注意してください。
Eメールアドレス	アカウントのEメールアドレスを指定する変数を入力します。
移動を許可	Eメールがこのアカウントから移動するのを防ぐ必要がない場合に選択します。
S/MIMEの有効化	S/MIME暗号化サポートを有効にする場合に選択します。次に署名と暗号化証明書を選択します。

設定	操作内容
	証明書のキャッシュが必要です。ID証明書の構成で使用されている認証機関でキャッシュが有効化されていることをご確認ください。 **iOS 10.3+:** **[S/MIME署名]**と**[S/MIME暗号化]**フィールドで以下のいずれかを選択します。 • オフ • オン • ユーザー選択 **iOS 12.0+:** • ユーザーがS/MIME署名設定をオーバーライドできるようにする • ユーザーがS/MIME署名IDを選択できるようにする • ユーザーがS/MIME暗号化設定をオーバーライドできるようにする • ユーザーがS/MIME暗号化IDを選択できるようにする 必要に応じて**[S/MIMEメッセージごとの署名と暗号化を有効化]**します。
Mail Dropを許可	このアカウントでMail Dropを許可する場合に選択します。Mail Dropによりユーザーは、メールに添付するファイルをiCloudに保存し、そのリンクをメールで送信することにより、重いファイルでもメール添付で送信できます。Mail Dropの詳細は以下をご覧ください: https://support.apple.com/

設定	操作内容
アプリごとのVPN	Appleは、Mailドメインにおける多数の異なるPer-App VPNプロファイルの関連付けをサポートしています。Per-App VPNを使用したIMAPとPOP3のメール設定もサポートされました。 **必須事項**：メール構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで **[Per-App VPN構成]を選択します**。

受信メール

設定	操作内容
メールサーバーおよびポート	このアドレスについては各ISPまでお問い合わせください。
ユーザー名	受信メールサーバーにアクセスするためのユーザー名を入力します。多くの場合、Eメールアドレスと同一となります。お使いのISPが形式を提供しています。
認証の形式	ISPによって定義された認証の種類を選択します。
パスワード	受信メールサーバーにアクセスするためのパスワードを入力します。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL)のみを選択し、使用してください。

送信メール

設定	操作内容
メールサーバーおよびポート	このアドレスについては各ISPまでお問い合わせください。

設定	操作内容
ユーザー名	送信メールサーバーにアクセスするためのユーザー名を入力します。多くの場合、Eメールアドレスと同一となります。お使いのISPが形式を提供しています。
認証の形式	ISPによって定義された認証の種類を選択します。
パスワード	送信メールサーバーにアクセスするためのパスワードを入力します。
受信パスワードと送信パスワードが同じ	SMTP認証でPOP/IMAPのパスワードと同じものを使用する場合に選択します。
Mail内のみで使用	この構成をEメールクライアントのみが使用するようにしたい場合に選択します。ネイティブEメールクライアントを使用してコンテンツを送信するアプリなど、Eメールを送信するその他のアプリは、この構成を使うことができません。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL)のみを選択し、使用してください。

Exchange構成

Exchange構成では、AndroidデバイスとiOSデバイスの場合はActiveSyncベースのメール、macOSデバイスの場合はExchange Web Services(EWS) ベースのメールを設定します。

Exchange構成は、SamsungではAndroid 9で廃止されています。Android 9以降のバージョンのSamsungデバイスの場合、Exchange構成は、デバイス管理者モードではサポートされていません。

Exchangeの設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
Exchangeホスト	Sentryをメールのアクセス制御に使用する場合は、Sentryサーバーのホスト名を入力してください。そうでなければ、ActiveSyncサーバのアドレスを入力します。*
移動を許可	**iOSおよびAndroid:** メールがこのアカウントから移動するのを防ぐ必要がない場合に選択します。 **Windows 10:** 該当しません。
S/MIMEの有効化	S/MIME暗号化サポートを有効にする場合に選択します。次に署名と暗号化証明書を選択します。 証明書のキャッシュが必要です。ID証明書の構成で使用されている認証機関でキャッシュが有効化されていることをご確認ください。 **iOS 10.3+:** **[S/MIME署名]** と **[S/MIME暗号化]** フィールドで以下のいずれかを選択します。 • オフ • オン • ユーザー選択

設定	操作内容
	iOS 12.0+： • ユーザーがS/MIME署名設定をオーバーライドできるようにする • ユーザーがS/MIME署名IDを選択できるようにする • ユーザーがS/MIME暗号化設定をオーバーライドできるようにする • ユーザーがS/MIME暗号化IDを選択できるようにする 必要に応じて **[S/MIMEメッセージごとの署名と暗号化を有効化]** します。
最近のメールアドレスを同期	デバイスとサーバー間で最近連絡したメールアドレスを同期したい場合に選択します。
Mail内のみで使用	この構成をメールクライアントのみが使用するようにしたい場合に選択します。ネイティブEメールクライアントを使用してコンテンツを送信するアプリなど、Eメールを送信するその他のアプリは、この構成を使うことができません。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL) のみを選択し、使用してください。
交換ペイロードにOAuthを有効化	iOS 12.0+とmacOS 10.14+： OAuthを使用した認証を有効化する場合に選択します。 有効の場合、OAuthを使用した認証をサポートするメールアプリで次の追加設定が可能になります。 • OAuthサインインURL • OAuthトークン要求URL
ドメイン	ユーザーに対してプロンプトを表示したい場合を除き、このメールアカウントのドメインを入力します。
ユーザー	このアカウントのEメールアドレスを示す変数を入力します。
アカウントのパスワード	ユーザーに対してプロンプトを表示したい場合を除き、このアカウントのパスワードを入力します。

設定	操作内容
Eメールアドレス	このアカウントのEメールアドレスを示す変数を入力します。
同期するメールの経過日数	メールがデバイスとサーバー間の同期を行う日数を選択します。
アプリごとのVPN	**必須事項:** Exchange Active Sync構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで設定済みの[Per-App VPN構成]を選択します。 **対象:** iOS 14+
AndroidとWindows	
カレンダーを同期	**AndroidおよびWindows 10:** デバイスとサーバー間でカレンダーを同期させる場合に選択します。 **Samsungデバイス:** この設定は使用されません(デフォルトでON)。 **Android Email+アプリ:** この設定が使用されます。
連絡先を同期	**AndroidおよびWindows 10:** デバイスとサーバー間で連絡先を同期させる場合に選択します。 **Samsungデバイス:** この設定は使用されません(デフォルトでON)。 **Android Email+アプリ:** この設定が使用されます。
メールを同期	**AndroidおよびWindows 10:** デバイスとサーバー間でメールを同期させる場合に選択します。 **Samsungデバイス:** この設定は使用されません(デフォルトでON)。 **Android Email+アプリ:** この設定は使用されません(デフォルトでON)。
タスクを同期	**AndroidおよびWindows 10:** デバイスとサーバー間でタスクを同期させる場合に選択します。 **Samsungデバイス:** この設定は使用されません(デフォルトでON)。 **Android Email+アプリ:** 該当しません。
iOS 13.0+	

設定	操作内容
• カレンダーを同期 • 連絡先を同期 • メールを同期 • メモを同期 • リマインダーを同期	カレンダー、連絡先、メール、メモ、リマインダーなど、同期するOutlook Exchange機能を個別に指定します。 それぞれについて、**[有効化]**と**[ユーザーによるオーバーライドを許可]**オプションを選択または選択解除します。 少なくとも以下のいずれかの同期を有効化してください。いずれか1つの同期を無効化しても、ユーザーによるオーバーライドを許可した場合は、ユーザーによる有効化が可能です。
ID証明書	デバイスを証明書を使用してサーバーに対して認証したい場合は、リストからID証明書を選択します。ID証明書構成を使用してすでに構成済みの場合にのみ、このリスト内に証明書が表示されます。
[Android]	
証明書に基づくの認証のみを使用	Exchangeサーバーへの唯一の認証手段として選択したID証明書を使用します。
すべてのSSL証明書の受け入れ	デバイスユーザーが、すべてのSSL証明書を承諾するようにAndroidデバイスを設定できるようにする場合に選択します。この設定は、Android Email+とSamsung Knox Emailに適用されます。 • デバイスユーザーが無意識にデバイスを攻撃にさらしてしまう恐れがあるため、この設定を有効にする場合は注意してください。 • Sentry証明書が自己署名または不明の証明書の場合は、このオプションを有効化する必要があります。
Exchangeアプリの優先度	Androidデバイスでデフォルトで構成されるメールクライアントを選択します(Android Email+とSamsung Email) 。 Exchangeアプリの優先を有効化したすべてのテナントのアプリカタログにEmail+アプリが追加されます。
iOS 10+	
通信サービスの規則	CardDAVシステム内の連絡先に電話をかけるときのデフォルトアプリを選択します。
Windows 10+のみ	

設定	操作内容
Outlookを構成	Microsoft Outlookをデバイスに構成する場合に選択します。 このオプションはBridgeが有効化されている場合のみサポートされます。

*このフィールドに対応する変数がある場合に、そのリストを参照するには、$ を入力してください。

フォント構成

フォント構成では、iOS 7デバイスに追加のTrueTypeまたはOpenTypeフォントファイルを提供できます。次の表はフォントの設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
フォントのアップロード	フォントファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択する]** をクリックしてファイルシステムから選択します。フォントファイルは、.otfまたは.ttfファイルでなければなりません。

詳細は構成を作成するにはを参照してください。

署名済みカレンダー構成

署名済みカレンダー構成では、公共のWebカレンダーへのアクセスを定義します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
URL	カレンダーにアクセスするためのURLを入力します。*
ユーザー	アクセスに使用するユーザー名を入力します。*
パスワード	アクセスに使用するパスワードを入力します。
SSLを使用	デバイスとサーバー間の通信には、セキュアソケットレイヤー(SSL)のみを選択し、使用してください。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

Web クリップ構成の作成

Webクリップとは、iOSデバイスからWebサイトまたはWebページへのショートカットです。Webクリップ構成を使用すると、デバイス上に標準のWebクリップが作成されます。特定のWebサイトを起動するWebクリップアイコンをiOSデバイスに追加できます。Webクリップでは、デバイスのホーム画面でブックマークをすばやく検索し、使用できます。サイトのMobile Safari表示経験のパラメータの一部を制御することもできます。

手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. **[構成]**をクリックします。
3. **[+追加]**をクリックします。
4. Webクリップ構成を検索して選択します。
5. このページで設定を構成します。参考値は、**Webクリップ構成設定**トピックの表をご覧ください。
6. **[次へ]**をクリックして配布設定を構成します。
7. **[カスタム]**を選択し、**[デバイス/デバイスグループ]**を選択します。
8. **[完了]**をクリックします。

Webクリップ構成設定

次の表はWebクリップ構成設定の一覧を示します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ラベル	デバイスの画面上でショートカットの下に表示したいテキストを入力します。*
URL	Web クリップがアクセスする URL を入力します。*
削除可能	チェックボックスをオンにすると、デバイスユーザーが Web クリップを削除することを許可します。
アイコン	アイコンファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択する]** をクリックしてファイルシステムから選択します。
合成済みアイコン	Safariの新しいバージョンで追加された特殊効果を削除する場合に選択します。
フルスクリーン	ブラウザ内のコンテンツではなく、フルスクリーンモードでWebクリップを表示する場合に選択します。
マニフェスト範囲を無視	選択すると、Safari ブラウザを表示せずに外部 Web サイトに移動することを許可します。このオプションは、全画面が選択されている場合には無効です。
ターゲット アプリケーション バンドル ID	URL を開くアプリケーションを指定したアプリケーション バンドル ID **例**: com.google.chrome.ios

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

関連トピック:

- iOS対応マルチユーザーセキュアサインイン
- 構成を作成するには

Office 365のインストール

ライセンス: Silver

対象：Windows 10+

Office 365のインストールの設定

Office 365のインストールとは、選択したデバイスにOffice 365をインストールまたはアンインストールする際に適用可能な構成の設定です。構成設定は、Microsoft Officeの導入ツールを使用してxml形式で定義した後、ファイルをアップロードします。ファイルをアップロードした後、選択したデバイスに構成オプションをプッシュします。

手順

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[Office 365のインストール]** を選択します。**[Office 365のインストール]** ページが表示されます。
3. **[名前]** フィールドに適切な構成名を入力します。
4. **[+説明を追加]** をクリックして構成の説明を追加します。このフィールドの記入は任意です。

5. **[構成設定]** セクションで、以下のフィールドを更新します。

フィールド名	説明
Office 365のインストール用構成ファイル	**[ファイルを選択]** ボタンをクリックし、Office 365をインストールするための定義済み設定を含むXML形式の構成ファイルを探して選択します。例：<Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> 構成ファイルがXML形式で、構成設定ファイルを追加した後に、緑のチェックマークが表示されていることを確認してください。
Office 365のアンインストール用構成ファイル	**[ファイルを選択]** ボタンをクリックし、Office 365をアンインストールするための定義済み設定を含むXML形式の構成ファイルを探して選択します。例：<Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> 構成ファイルがXML形式で、構成設定ファイルを追加した後に、緑のチェックマークが表示されていることを確認してください。

6. **[次へ]** をクリックします。

7. 以下のいずれかのオプションを選択し、デバイスに設定を配布します。

オプション	説明
この構成を有効化	チェックボックスを選択すると、選択したデバイスにこの構成が適用されます。チェックボックスを外すと、構成がすでにデバイスに適用されている場合は削除されます。
すべてのデバイス	すべてのデバイスに設定を配布します。
デバイスなし	デバイスへの設定の配布を保留します。
カスタム	定義したデバイスグループに設定を配布します。設定を配布したいデバイスタイプの横にあるチェックボックスを選択します。**[デバイスグループを検索]** 検索フィールドにデバイスグループ名を入力し、デバイスグループを検索することも可能です。新しいデバイスグループを作成する場合は、ページ下部の **[新しいデバイスグループを作成]** リンクをクリックします。詳細は、デバイスグループをご覧ください。 デバイスカテゴリを選択する際は、選択したデバイスカテゴリのデバイスユーザーリストの詳細(**氏名**、**電話番号**、**デバイスの種類**)を **[配布の概要]** セクションで確認できます。

8. 選択したデバイスに設定をプッシュするには、**[完了]** をクリックします。

Windows GPO設定

ライセンス: Bridge

対象：Windowsデスクトップ

Windows GPO設定の構成

グループポリシーオブジェクト(GPO)とは、デバイスでしていいことといけないことの許可を定義する設定の集合です。GPO設定を管理できるBridge設定を持つことは前提要件です。詳細については、Ivanti Bridgeをご覧ください。

GPOメタデータがデータベースにアップロードされていない場合は、サイト管理者にお問い合わせください。GPO構成は、BridgeからPowerShellスクリプトでデバイスに展開されます。GPO設定を使用するには、具体的な設定を構成し、デバイスにプッシュします。

手順

1. **[構成]**タブで**[+追加]**をクリックします。
2. **[Windows GPO設定]**構成を選択します。**[Windows GPO設定]**ページが表示されます。
3. **[名前]**フィールドに適切なWindows GPO設定名を入力します。
4. **[+説明を追加]**リンクをクリックし、構成の説明を追加します。このフィールドはオプションです。
5. **[構成設定]**セクションで**[+追加]**をクリックします。をクリックします。**[Windowsグループポリシーオブジェクト(GPO)]**ウィンドウが表示されます。
6. 左ペインのGPO階層ツリーで関連コンポーネントをクリックし、GPOを選択します。GPO階層ツリーは、ポリシー設定のパスを表現しています。また、GPO設定の名前を検索フィールドに入力することで、特定のGPO設定を検索することも可能です。
   GPO設定を選択すると、選択したGPO設定の詳細が右ペインに表示されます。

7. **[設定ステータス]** フィールドで以下の設定オプションを選択できます。

オプション	説明
構成なし	既存のGPO設定を削除します。
有効	GPO設定を有効化します。
無効	GPO設定を無効化します。

8. **[設定値]** フィールドに適切なGPO名を入力します。

このフィールドは **[有効]** オプションが **[設定ステータス]** で選択されている場合のみ編集できます。

別の設定値を追加するには、+ アイコンをクリックします。設定値を追加する必要のないGPO設定もあります。テキスト値の形で [設定値] にデータを指定する必要がある場合もあります。そのような設定では、利用可能なドロップダウン値から値を選択します。

9. **[保存して閉じる]** をクリックし、GPOを保存してウィンドウを閉じます。さらにGPOを追加したい場合は、**[保存してさらに追加]** をクリックすると、保存した後にGPOウィンドウが閉じません。
追加されたGPO設定は、**[構成設定]** セクションに表示されます。

> **[アクション]** 列の対応アイコンをクリックすると、GPO設定を編集または削除できます。

オプション	説明
この構成を有効化	チェックボックスを選択すると、選択したデバイスにこの構成が適用されます。チェックボックスを外すと、構成がすでにデバイスに適用されている場合は削除されます。
すべてのデバイス	すべてのデバイスに設定を配布します。
デバイスなし	デバイスへの設定の配布を保留します。
カスタム	定義したデバイスグループに設定を配布します。設定を配布したいデバイスタイプの横にあるチェックボックスを選択します。**[デバイスグループを検索]** 検索フィールドにデバイスグループ名を入力し、デバイスグループを検索することも可能です。新しいデバイスグループを作成する場合は、ページ下部の **[新しいデバイスグループを作成]** リンクをクリックします。詳細は、デバイスグループをご覧ください。 デバイスカテゴリを選択する際は、選択したデバイスカテゴリのデバイスユーザリストの詳細(**氏名**、**電話番号**、**デバイスの種類**)を **[配布の概要]** セクションで確認できます。

10. 選択したデバイスにGPO設定をプッシュするには、**[完了]** をクリックします。

BitLocker暗号化構成

ライセンス: Bridge

対象 : Windowsデスクトップ

このセクションは以下のトピックを含みます。

- BitLocker暗号化の設定
- BitLocker設定の表示

BitLocker暗号化の設定

BitLocker暗号化は、ハードドライブとリムーバブルドライブ上でデバイスの暗号化を強制し、データを保護する機能です。BitLocker暗号化を管理できるBridge設定を持つことが前提要件です。詳細はBridgeをご覧ください。BitLocker暗号化構成は、デバイスの暗号化設定に役立ちます。

手順

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[BitLocker暗号化]** 構成を選択します。**[BitLocker暗号化]** ページが表示されます。
3. **[名前]** フィールドに適切なBitLocker暗号化名を入力します。

4. **[+説明を追加]** リンクをクリックし、構成の説明を追加します。このフィールドはオプションです。

5. [構成設定]セクションで、以下の設定を構成します。

設定	説明
暗号化の方式と種類	暗号のキーサイズに応じて暗号化アルゴリズムの種類を選択します。以下のオプションが使用できます。 • **AES-CBL 128ビット** • **AES-CBL 256ビット**
すべてのハードウェアドライブを暗号化	すべてのハードウェアドライブを暗号化する設定は、トグルボタンをクリックして**ON**または**OFF**にできます。 デバイス上のいずれかのハードウェアドライブがすでに暗号化されている場合、その構成の編集は適用されません。編集で暗号化処理を元に戻すことはできないからです。
ドライブを選択	暗号化を必要とするドライブを選択します。例：**C:** さらにドライブを追加するには**[+追加]**をクリックします。 **[すべてのハードウェアドライブを暗号化]**設定がオンの場合、このフィールドは表示されません。

設定	説明
ドライブの種類に対応するハードウェアベースの暗号化	TPM(Trusted Platform Module) とは、コンピューターのマザーボードに組み込まれた耐タンパー性を高めるチップです。TPMを搭載したコンピューターでBitLocker暗号化またはデバイス暗号化を使用する場合、キーの一部はTPMに保存されます。ドロップダウンリストから、以下のハードウェアベースの暗号化設定オプションを選択することができます。 • **起動時にTPMが必要** • **TPMに起動PINが必要** • **TPMを使用しない** TPMオプションは、OSドライブとTPMバージョン1.2以降にのみ適用されます。 ハードウェアベースの暗号化設定をデバイスに適用すると、この設定は編集できなくなります。 デバイスにBitLocker構成がすでに設定されている場合、TPMオプションの異なる2番目のBitLocker構成をプッシュすることはできません。
次の構成チェックボックスオプションを選択します(任意) 。 • **BitLockerによって保護されていない固定ドライブへの書き込みアクセスを拒否** • **BitLockerによって保護されていないリムーバブルドライブへの書き込みアクセスを拒否**	

設定	説明
暗号化前のデバイスアクション	以下のいずれかのオプションを選択し、完全に解読されていない、またはすでにキープロテクターのあるドライブの処理方法を決定します。 • **暗号化を停止** - 選択したドライブのいずれかがすでに暗号化されている場合は暗号化を停止します。 • **Ivanti Neurons for MDM に回復パスワードストアがない選択したドライブを復号** - Ivanti Neurons for MDM内に回復パスワードがないドライブのみに適用するには、このオプションを選択します。
リカバリオプション	ユーザーがパスワードを忘れた場合はリカバリオプションを使用します。これによりデバイス詳細ページからパスワードを取得できます。設定できるリカバリオプションは以下のとおりです。 • **リカバリを無効化** • **パスワードを使用し、ADに保存** • **パスワードを使用し、ADとMobileIronに保存**
再起動間隔	構成をデバイスにプッシュすると、再起動が指示されます。暗号化は再起動後に開始されます。再起動間隔を構成するには、ドロップダウンダウンリストからデバイスを再起動させる間隔を選択します。再起動間隔の最小は1分、最大は120分(2時間)です。

設定	説明
再起動メッセージ	デバイスに表示する再起動メッセージを入力します。 必要であれば、起動パスワードまたは起動PINもユーザーに表示されます。ユーザーは、メモを取るか、再起動後の指示に応じて入力します。

6. **[次へ]** をクリックします。

7. 以下のいずれかのオプションを選択し、デバイスに設定を配布します。

設定	説明
この構成を有効化	チェックボックスを選択すると、選択したデバイスにこの構成が適用されます。チェックボックスを外すと、構成がすでにデバイスに適用されている場合は削除されます。
すべてのデバイス	すべてのデバイスに設定を配布します。
デバイスなし	デバイスへの設定の配布を保留します。
カスタム	定義したデバイスグループに設定を配布します。設定を配布したいデバイスタイプの横にあるチェックボックスを選択します。**[デバイスグループを検索]** 検索フィールドにデバイスグループ名を入力し、デバイスグループを検索することも可能です。新しいデバイスグループを作成する場合は、ページ下部の **[新しいデバイスグループを作成]** リンクをクリックします。詳細は、デバイスグループをご覧ください。 デバイスカテゴリを選択する際は、選択したデバイスカテゴリのデバイスユーザーリストの詳細(**氏名**、**電話番号**、**デバイスの種類**)を**[配布の概要]** セクションで確認できます。

8. 選択したデバイスに設定をプッシュするには、**[完了]** をクリックします。

BitLocker設定の表示

デバイスのBitLocker設定は、**[BitLocker設定]** セクションの下のデバイス詳細ページ(**[デバイス]** > **[デバイス]** > **[(デバイス名)]**) で閲覧できます。デフォルトでは詳細が非表示になっています。

各フィールドの横にある表示(目の形)アイコンをクリックすることで、以下の詳細を表示できます。

設定	説明
リカバリパスワード	このオプションが選択されている場合、リカバリパスワードがWindowsによって生成され、BitLocker構成をプッシュした後にIvanti Neurons for MDMに戻されます。デバイスがリカバリモードを通過するとき、ユーザーはこのパスワードの入力を求められます。 複数のデバイスが暗号化されている場合、同じリカバリパスワードを使用する必要があります。 リカバリパスワードは、リカバリオプション **[パスワードを使用し、ADとMobileIronに保存]** が選択されている場合のみ公開されます。
暗証番号	起動用の6桁のPINを表示します。PINは、BitLocker構成設定で **[TPMに起動PINが必要]** オプションを選択した場合のみ表示されます。
起動パスワード	デバイスに設定されている起動パスワード。起動パスワードは、BitLocker構成設定で **[TPMを使用しない]** オプションを選択した場合のみ表示されます。
TPMバージョン	構成されているTPMバージョンを表示します。

フィールドによっては、BitLocker構成設定の設定に基づき、**[非該当]** が表示される場合もあります。

- 暗号化のステータスは、デバイス詳細ページの [デバイス暗号化ステータス] の下に表示されます。
- BitLockerが適用されるデバイスの全デバイスに同じ起動パスワードまたはPINが使用されます。
- すでにドライブが暗号化され、パスワードが保存されているデバイスの2番目のドライブを暗号化する構成を作成すると、古いパスワードは上書きされます。このため、リカバリパスワードオプションは、デバイスの1つのドライブにのみ使用することをお勧めします。

エンタープライズネット ワークアクセス構 成

このセクションは以 下 のトピックを含 みます。

AirPlay構成

ライセンス: Silver

AirPlay構成では、メディアを表示する別のデバイスへのアクセスを設定します。次の表はAirplay設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
許可リスト	許可されたAirPlayの各宛先のデバイスIDを入力します。IDをリストしないと、AirPlayの宛先は制限されません。 **対象:** iOS 7.0+、macOS 10.10+(監視対象)。
デバイス設定	既知のAirPlayの各宛先についてデバイスID(macOS)またはデバイス名(iOS)とパスワードを入力します。

詳細は構成を作成するにはを参照してください。

AirPrint構成

ライセンス: Silver

AirPrint構成では、無線印刷を設定します。次の表はAirPrint設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
AirPrint設定	**IPアドレス:** AirPrintプリンターのIPアドレスを入力します。 **リソースパス:** AirPrintプリンターに関連するリソースパスを入力します。これは_ipps.tcp Bonjourレコードのrpパラメータに相当します。 例: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. リソースパスでは大文字と小文字が区別されます。 **ポート:** AirPrint出力先のリスニングポートを入力します。 これが指定されていない場合、AirPrintはデフォルトポートを使用します。Apple標準ポートの詳細は、https://support.apple.com/ja-jp/HT202944をご覧ください。 **強制TLS:** TLS(トランスポートレイヤセキュリティ)によってセキュリティを確保された接続を有効化します。デフォルトでは無効になっています。

AirPrint構成をmacOSにインストールすると、プリンターの詳細が**AirPrint**構成を通じてデバイスにプッシュされます。ユーザーは、**[システム環境設定]** > **[プリンターとスキャナー]** > **[+]** をクリックし、自動入力されたプリンターの詳細を確認できます。ユーザーは **[追加]** 画面で **[デフォルト]** を選択した後、必要なプリンター プロファイルを選択する必要があります。これにより必要なプリンターが **[プリンターとスキャナー]** に追加されます。

詳細は構成を作成するにはを参照してください。

Always On VPN構成

ライセンス:

- **Android Enterprise 用の Gold**
- **iOS対応 Silver**

Always-on VPN構成の場合、ユーザーは何もアクションを実行しなくても自動的にVPN(利用可能な場合)に接続されます。この機能には、Android 7.0 +またはiOS 8+に加え、IKEv2プロトコルをサポートするVPNプロバイダーが必要です。

Android 用のAlways On VPN設定

Always On VPN構成は、Android 7.0以上を搭載したAndroid Enterpriseデバイスに送信されます。仕事用プロファイルを持つマネージドデバイス(Android 8.0+)では、VPN構成が仕事用プロファイルに適用されます。

> Device Enrollment タイプとして**AMA**を指定して、デバイスを**COSU**モードで導入した場合、**Always On**構成のアプリがそのデバイスにプッシュされると、**Always On**構成もそのデバイスにプッシュされます。

この構成を有効化するには、アプリカタログからアプリを選択するか、パッケージ名を入力してください。

iOS 用のAlways On VPN 設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
セルラーとWi-Fiに同じトンネル構成を使用	セルラーまたはWi-Fiネットワークのどこに接続が確立されるかに関係なく、VPN接続に1対のサーバー識別子を定義する場合に選択します。
サーバー	VPNサーバーのホスト名またはIPアドレスを入力します。
ローカル識別子	以下のいずれかの形式のIKEv2クライアント識別子: • FQDN

設定	操作内容
	• UserFQDN • アドレス • ASN1DN
リモート識別子	以下のいずれかの形式のリモート識別子： • FQDN • UserFQDN • アドレス • ASN1DN
EAPを有効化	拡張認証を有効する場合に選択します。
マシン認証	EAPの有効化が選択されていない場合のみ利用できます。 以下のいずれかを選択します。 • 証明書 • 共有シークレット
EAP認証	EAPの有効化が選択されている場合のみ利用できます。 以下のいずれかを選択します。 • 証明書 • ユーザー名/パスワード
共有シークレット	マシン認証に共有シークレットが選択されている場合のみ利用できます。接続の共有シークレットを入力します。
証明書	マシン認証に証明書が選択されている場合のみ利用できます。使用する証明書を選択します。その証明書がIKEクライアント認証に送信されます。拡張認証を使用する場合、この証明書をEAP-TLSに使用可能です。

設定	操作内容
アカウント	EAP認証にユーザー名/パスワードが選択されている場合のみ利用できます。VPNサーバーのアカウントIDを入力します。
パスワード	EAP認証にユーザー名/パスワードが選択されている場合のみ利用できます。VPNサーバーのパスワードを入力します。
デッドピア検出の間隔	以下のいずれかを選択します。 • なし(無効) • 低(1時間毎にkeepaliveを送信) • 中(30分毎にkeepaliveを送信) • 高(10分毎にkeepaliveを送信)
暗号化アルゴリズム	以下のいずれかを選択します。 • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
完全性アルゴリズム	以下のいずれかを選択します。 • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512

設定	操作内容
Diffie Hellmanグループ	Diffie Hellman鍵交換グループを選択します。
分単位の有効期間	SA有効期間(リキー間隔)を分単位で入力します。有効値は10～1440です。
ボイスメール	ボイスメールをAlways On VPNの適用外にするには、[トンネル経由のトラフィックを許可]を選択します。適用外にしない場合は[トラフィックをドロップ]を選択します。
AirPrint	AirPrintトラフィックをAlways On VPNの適用外にするには、[トンネル経由のトラフィックを許可]を選択します。適用外にしない場合は[トラフィックをドロップ]を選択します。
セルラーサービス	モバイル通信サービストラフィックをAlways On VPNの適用外にするには、[トンネル経由のトラフィックを許可]を選択します。適用外にしない場合は[トラフィックをドロップ]を選択します。
VPNトンネル外のキャプティブWebシートからのトラフィックを許可	VPNトンネル外のキャプティブWebシートからのトラフィックを許可する場合に選択します。
VPNトンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可	VPNトンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可し、キャプティブネットワーク処理を実行する場合に選択します。
キャプティブネットワークアプリバンドル識別子	トラフィックがVPNトンネル外でキャプティブネットワーク処理を実行できるキャプティブネットワークアプリのバンドルIDをリスト化します。キャプティブネットワークアプリは、キャプティブ環境で動作するために他の資格を必要とする場合があります。

詳細は構成を作成するにはを参照してください。

デフォルトのアプリランタイム許可

対象：Android API 23+をターゲットとしてビルドされ、Android EnterpriseデバイスでAndroid 6.0+を実行するアプリ。

管理者は、Android Enterpriseデバイスに展開したアプリのランタイム許可構成を設定できます。API 23(以降)をターゲットとして構築され、Android 6.0以降を実行するアプリは、ランタイムにユーザーに許可を求めることができます。デフォルトアプリランタイム許可構成は、これらのアプリランタイム許可のデフォルトを設定します。Ivanti Neurons for MDMでは、この構成が既定で作成されます。このデフォルトシステム構成を編集するか、必要に応じて新規構成を作成してください。

特定アプリ向けの許可は、一般的なアプリ許可構成より優先されます。自社開発アプリにはグローバル許可が適用されます。社内アプリにアプリ単位の許可を設定することはできません。

グローバルランタイム許可の設定

管理者は、デフォルトのアプリランタイム許可を編集し、その構成を以下のように配布できます。

Procedure手順

1. **[構成]**に進みます。
2. 以下のいずれかのアクションを実行します。
   - デフォルトのシステム構成を編集するには、**[デフォルトのアプリランタイム許可]**をクリックし、**[編集]**をクリックします。
   - 新しい構成を追加するには、**[追加]** > **[デフォルトのアプリランタイム許可]**をクリックします。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [構成設定]セクションで、以下のいずれかのデフォルトランタイム許可を設定します。
   - ユーザープロンプト(デフォルトオプション)
   - 自動付与
   - 自動拒否(注意して使用)
6. **[次へ]**をクリックします。

7. **[この構成を有効化]** オプションを選択します。

   このオプションを選択しない場合、構成はどのデバイスにも適用されません。以前に適用されていた場合は、すべてのデバイスから削除されます。

8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
9. **[完了]** をクリックします。

特定アプリ向けランタイム許可の設定

管理者は、以下の手順で各アプリのデフォルトランタイム許可を設定できます。

手順

1. **[アプリ]** を開きます。
2. アプリ名をクリックします。
3. **[アプリ構成]** > **[Android Enterprise]** をクリックします。
4. **[追加]** か構成名をクリックし、既存の構成を編集します。
5. 名前、説明、制約などの構成オプションを設定します。
6. [ランタイム許可] セクションで **[許可を管理]** をクリックします。
7. 表示されるウィンドウで許可を選択し、**[選択]** をクリックします。
   特定のアプリケーションに適用される危険な許可だけが、選択リストに表示されます。危険な許可すべて(連絡先の読み出し、デバイス上のアカウント検索、通話ログの書き込みなど)のリストは、https://developer.android.com/guide/topics/permissions/requesting.html#perm-groupsにあります。
   - 許可は、アプリケーションが許可を要求したときにのみ適用されます。
   - ユーザーが過去に許可を承認または拒否したときは許可が適用されません。
8. [ランタイム許可] セクションで、以下のいずれかのデフォルトランタイム許可を選択します。

- デフォルト/グローバル(デフォルトオプション)
- 自動付与
- 自動拒否(注意して使用)

9. [このアプリ構成の配布] セクションで、以下のいずれかの配布オプションを選択します。
   - アプリを利用する全員
   - 該当なし
   - カスタム
10. **[保存]** をクリックします。

教育

ライセンス: Gold

対象: 監視対象のiOS 9.3+

リーダーおよびメンバー向けのApple Educationペイロードと Classroomアプリを構成します。次の表はEducationの設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成の種類	次の種類から1つを選択します。 • リーダー • メンバー
この構成を有効化	• 選択したデバイスにこの構成を適用する場合に選択します。 • 選択を解除すると、過去に適用されていたすべてのデバイスからこの構成が削除されます。
配布する	以下の配布オプションから1つ選択します。 • すべてのデバイス • デバイスなし • カスタム

詳細は構成を作成するにはを参照してください。

グローバルプロキシ構成

ライセンス: Silver

グローバルプロキシ構成では、プロキシサーバーにHTTPトラフィックを送るようにデバイスを設定します。次の表はグローバルプロキシの設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
種類	**[手動]** または **[自動]** を選択します。**[手動]** を選択した場合、プロキシサーバーのホスト名とポート、およびプロキシサーバーへのユーザー名とパスワード(任意)が必要となります。**[自動]** を選択した場合、プロキシ自動設定(PAC) URLを入力できます。
ホスト名とポート	**[手動]** を選択した場合、プロキシサーバーのホスト名とポート番号を入力します。
ユーザー	(オプション) プロキシサーバにアクセスするためのユーザ名。*
パスワード	(オプション) プロキシサーバーにアクセスするためのパスワード。
PAC URL	(オプション) **[自動]** を選択した場合、プロキシ構成を定義するPACファイルのURLを入力できます。この設定を空白のままにした場合、デバイスはWebプロキシ自動検出プロトコル(WPAD) を使用してプロキシを検出します。
PACに到達できない場合は直接接続を許可	(iOS 7以降) 何らかの理由でデバイスがPACファイルにアクセスできないときに直接接続を許可する場合に選択します。
バイパスするプロキシがキャプティブネットワークに接続するのを許可	(iOS 7以降) プロキシをバイパスし、キャプティブネットワークのログインページを表示することを許可する場合に選択します。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

LDAP構成

LDAP構成では、企業ディレクトリへのアクセスを設定します。次の表はLDAPの設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ホスト名	LDAP サーバのホスト名を入力します。*
ユーザー	LDAPアカウントにアクセスするためのユーザ名を入力します。*
パスワード	LDAPアカウントにアクセスするためのパスワードを入力します。
SSLを使用	LDAPサーバーとの接続にSSLを使用したい場合に選択します。
検索設定	アカウントに少なくとも1つのエントリを入力します。各エントリは、検索の開始元となるLDAPツリー内のノードを表します。[+] ボタンをクリックして新しいエントリを追加し、続いてそのエントリを編集します。 エントリは、次の値で構成されます。 説明：検索設定の目的を説明します。 範囲：**[ベース]**、**[サブツリー]** または **[ワンレベル]** を選択し、検索の範囲を示します。**[ベース]** はノード レベルのみ、**[サブツリー]** はノードとすべてのチルドレン、**[ワンレベル]** はノードと1レベルのチルドレンを、それぞれ示します。 検索ベース: 指定されたノードへの概念経路（たとえばou = people、o = mycorp）。

アプリごとのVPN	**必須事項**：LDAP構成でPer-App VPNを設定する前にTunnelまたはPer-App VPNを構成してください。 ドロップダウンメニューで設定済みの[Per-App VPN構成]を選択します。 **対象**：iOS 14+
iOS 10+	
通信サービスの規則	LDAPシステム内の連絡先に電話をかけるときのデフォルトアプリを選択します。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

macOSサーバー構成

macOSサーバー構成は、アカウントタイプと設定を構成したmacOSサーバーアカウントを定義します。この構成によりユーザーはサーバー上でファイル共有をアクティベートできます。

対象：iOS 10+

macOSサーバーの構成

手順

1. **[構成]** > **[+追加]** を開きます。
2. **[macOSサーバー]** 構成を選択し、**[macOSサーバー構成を作成]** ページを表示します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. **[ホスト名]** を入力し、サーバーアドレスを指定します。
6. **[ユーザー名]** を入力し、ユーザーのログイン名を指定します。
7. (オプション) ユーザーの **[パスワード]** を入力します。
8. (オプション) アカウントの **[説明]** を入力します。
9. (任意) 構成されたアカウントの下に、ドキュメントのサーバーに接続する際に使用する **[ポート]** 番号を入力します。ポート番号が指定されていない場合、デフォルトのポート番号が使われます。
10. **[次へ]** をクリックします。
11. この構成の配布を選択します。

Tunnel

バージョン2.1+のTunnelアプリで使用するPer-App VPN構成を作成します。Sentryプロファイルを選択し、設定を構成すると、Sentry経由でアプリデータのトンネリングを開始できます。

Android Enterpriseデバイスの場合、Per-App構成は廃止されています。アプリカタログ内にある、Ivanti Tunnel用のマネージド構成を使用する必要があります。

最新ドキュメンテーション

最新のTunnelの使用方法は、製品ドキュメンテーション > **[アプリ]** に公開されています。お使いのTunnelのバージョンに適切な説明書を選択してください。

AppTunnelの設定

AppTunnelは、各アプリコンテナと企業ネットワーク間のアプリごとのセッションセキュリティを提供することにより、アプリデータを保護します。

このセクションは以下のトピックを含みます。

- Sentryが証明書でAppTunnelを使用するよう設定する
- Sentry証明書のアップロード
- AppTunnelを使用するようアプリを設定する
- AppTunnelサービス名について

Sentryが証明書でAppTunnelを使用するよう設定する

前提条件

- AppTunnelは、対応しているSentryの最新版に依存しています。AppTunnelの設定タスクを開始する前に、Sentryのインストールを完了してください。
- SCEP IDを使用したい場合：
  - ローカルまたは外部の認証機関を追加します。Connectorのインストールが必要です。
  - アプリID証明書構成を追加します。これが、AppTunnelを構成する際に使用する動的配布です。

認証にX.509証明書を使用するActiveSyncまたはAppTunnel、またはその両方が、プロファイルに割り当てられているSentryサーバーを使用するように構成できます。

手順

1. **[管理] > [Sentry]** を開きます。
2. **[+ Sentryプロファイルを追加]** をクリックします。
3. **[証明書によるActiveSync/App Tunnel認証]** をクリックします。

4. **[次 へ]** をクリックします。

5. 次の表のガイドラインを使用し、**[グローバル設定]** ページを完了します。

表：[管理] > [Sentry] のグローバル設定	
設定	**操作内容**
[名前]	このプロファイルを識別する名前を入力します。
説明	このプロファイルの目的を明示する説明を入力します。
外部ホスト名とポート	Sentryのホスト名とポートを入力します。
デバイス認証モード	
1つの証明書を2要素認証に使用	認証に1枚の証明書を使用する場合にこれを選択します。まだ証明書をアップロードしていない場合は、選択したオプションの下に表示されるエリアでアップロードできます。
証明書を選択	デバイス認証に必要なグループ証明書をアップロードするには： a. **[Add]** をクリックします。**[証明書を追加]** ウィンドウが表示されます。 b. **[証明書名]** フィールドに証明書の名前を入力します。 c. PKCS12ファイルを保護するパスワードを入力します。 d. **[ファイルを選択]** をクリックしてグループ証明書をアップロードします。ファイル形式が、.p7b、.p12、.pfx、.pem、.der、.crt、.cer のいずれかであることを確認してください。
証明書失効リスト(CRL)を有効化	デバイスが提示する証明書をCAが発行するCRL(証明書失効リスト)に照らして検証する場合に選択します。
非管理デバイス動作のデフォルト設定	

表：[管理] > [Sentry] のグローバル設定	
設定	**操作内容**
非マネージドデバイスによるメール/データ受信を許可	Ivanti Neurons for MDMによって管理されていないデバイスへのデータアクセスをブロックする必要がないかどうかを選択します。

6. **[次へ]** をクリックします。

7. **[Sentryサーバー構成]** ページで、以下のフィールドを構成します。

表：[管理] > [Sentry] のSentryサーバー構成	
設定	操作内容
リスナープロトコル	以下のいずれかのプロトコルを選択します。 • **HTTPSのみ** • **HTTPのみ** • **HTTPSおよびHTTP**
Httpsポート	Httpsポート番号を入力します。リスナープロトコルに「HTTPのみ」が選択されている場合、このフィールドは表示されません。
Httpポート	Httpポート番号を入力します。リスナープロトコルに「HTTPSのみ」が選択されている場合、このフィールドは表示されません。
Sentry TLSサーバー証明書/キー	
Sentryの自己署名証明書を使用	Ivanti Neurons for MDM サービスによって作成された自己署名証明書を使用し、このプロファイルの一部としてSentryに送信する場合に選択します。この証明書は、Sentryとモバイルデバイスとの間の通信のために使用されます。
追加	認証に必要な自身の証明書をアップロードするには：

表：[管理] > [Sentry] のSentryサーバー構成	
設定	操作内容
	a. **[Add]** をクリックします。**[証明書を追加]** ウィンドウが表示されます。 **[Sentryの自己署名証明書を使用]** の選択を解除した場合のみ、このオプションが表示されます。 b. **[証明書名]** フィールドに証明書の名前を入力します。 c. PKCS12ファイルを保護するパスワードを入力します。 d. **[ファイルを選択]** をクリックし、証明書をアップロードします。ファイル形式が、.p7b、.p12、.pfx、.pem、.der、.crt、.cer のいずれかであることを確認してください。 e. **[追加]** をクリックします。 アップロードしたTLSサーバー証明書 (Sentryのメインページや他のプロファイルからアップロードした証明書を含む) はすべてSentry TLSサーバー証明書/キーセクションに表示されます。認証に必要なTLS証明書を選択するには、証明書の隣のラジオボタンをクリックします。
プロトコル	必要な受信プロトコルと送信プロトコルを選択します。
暗号スイート	暗号はSentryとのSSL暗号化通信に使用されます。一般に強力な暗号が推奨されます。旧いデバイスには弱い暗号化が必要となる場合があります。デフォルトでは強力な暗号が選択されています。それに加えて使いたい暗号を選択してください。少なくとも1つの暗号を選択する必要があります。

8. **[次へ]** をクリックします。
9. 表示されるサービスのうち1つ以上を追加します。
10. **[保存]** をクリックします。

登録されたSentryは、[未構成Sentryサーバー] セクションの [Sentry] ページに表示されます。Sentryにプロファイルを割り当てるには、**[アクション]** カラムの **[割り当てる]** をクリックします。

Sentry証明書のアップロード

Ivanti Neurons for MDM は、Sentryプロファイルの作成時にTLSサーバー証明書とグループ証明書をアップロードします。これらの証明書を **[Sentry証明書]** セクションの **[Sentry]** ページからアップロードすることもできます。

Ivanti Neurons はアップロード時に Sentry 証明書を検証し、証明書で見つかった条件に応じて次の種類の情報を返します。

条件	情報タイプ
リーフ証明書に認証機関へのチェーンが含まれていない、またはアップロードされたファイルに認証機関が含まれていません。	エラー
利用可能なルート証明機関がありません。	警告
ルート証明機関が、リーフ証明書の中間証明機関をサインオフしていません。	警告

Ivanti Neurons for MDM は、この記事のルールに照らした検証も行います。

手順

1. **[TLSサーバ証明書]** セクションで **[追加]** をクリックします。**[証明書を追加]** ウィンドウが表示されます。
2. **[証明書名]** フィールドに証明書の名前を入力します。
3. PKCS12ファイルを保護するパスワードを入力します。
4. **[ファイルを選択]** をクリックしてグループ証明書をアップロードします。ファイル形式が、.p7b、.p12、.pfx、.pem、.der、.crt、.cerのいずれかあることを確認してください。
5. **[Add]** をクリックします。アップロードされた証明書が表に表示されます。
6. TLSサーバー証明書を削除するには、**[アクション]** カラムの [削除] アイコンをクリックします。

いずれかのSentryプロファイルでTLSサーバー証明書が使用されている場合、TLSサーバー証明書を削除することはできません。削除しようとするとエラーメッセージが表示されます。

グループ証明書を追加するには

手順

1. **[グループ証明書]** セクションで **[追加]** をクリックします。**[証明書を追加]** ウィンドウが表示されます。
2. **[証明書名]** フィールドに証明書の名前を入力します。
3. PKCS12ファイルを保護するパスワードを入力します。
4. **[ファイルを選択]** をクリックしてグループ証明書をアップロードします。ファイル形式が、.p7b、.p12、.pfx、.pem、.der、.crt、.cerのいずれかあることを確認してください。
5. **[追加]** をクリックします。

アップロードしたグループ証明書を削除するには、**[アクション]** カラムの [削除] アイコンをクリックします。

Sentryルート証明書の編集

管理者は、Sentryルート証明書構成の配布を編集することが可能です。また、configを他のスペースに委譲することにより、カスタムスペース管理者に編集許可を提供することもできます。

1. **[構成]** に進みます。
2. **[Sentryルート証明書]** を検索します。
3. 編集アイコンをクリックします。
4. 証明書を配布するデバイスまたはデバイスグループに対応するチェックボックスを選択します。または、デバイスまたはデバイスグループに対応するチェックボックスの選択を解除します。
5. 適宜、次のオプションのいずれかを [配布の概要] セクションから選択します。
   - **他のスペースに適用しない**
   - **他のスペースにあるデバイスに適用する**
6. (任意) チェックボックス **[スペース管理者に配布の編集を許可]** をクリックします。
7. **[保存]** をクリックします。
8. 警告メッセージが表示されます。**[はい]** をクリックして確定します。

AppTunnelを使用するようアプリを設定する

Sentryの最新説明書は、製品ドキュメンテーションで [Sentry] をクリックしてください。使用中のSentryバージョンに対応する説明書を選択します。

AppTunnelサービス名について

AppTunnelサービスは、AppConnectアプリのトンネリング先となるバックエンドサービスを定義します。

最新の使用方法は、製品ドキュメンテーションに公開されています。お使いのSentryおよびAppConnectのバージョンに適切な説明書を選択してください。

Per-App VPN構成

ライセンス: Silver

対象: iOSデバイス

Per-App VPN構成では、以下の特定のアプリの仮想プライベートネットワークアクセスを設定します。

- Per-App VPN設定
- IPsec(Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- カスタムSSL
- Palo Alto Networks GlobalProtect

> Per-App VPN構成は、アプリ構成に依存します。Per-App VPN構成は、アプリ構成のセットアップ中に作成されます。Per-App VPN構成が削除または配布停止されると、ネットワークからアプリが切り離され、アプリ構成に誤動作が生じます。

Per-App VPN設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
接続の種類	構成するVPNの種類を選択します。 残りの設定は、この選択に依存します。
オンデマンドVPNの有効化	オンデマンドVPNを確立するドメインおよびホスト名にこの構成を使用する場合に選択します。

iOS規則を有効化 ([オンデマンドVPNを有効化]が選択されている場合のみ)	iOSおよびmacOSの場合、以下を設定できます。 • trueと判断されたネットワークへの接続の許可または禁止、および許可または無視を設定するネットワークルール。 • trueと判断されたネットワークへの接続を必要時に許可する、あるいはすべて許可しない接続ルール。 ネットワークルールの場合、次のタイプのパラメーターを指定できます。 • DNSのドメインが一致 • DNSのサーバーアドレスが一致 • SSIDが一致 • URL文字列のプローブ • インターフェイスの種類が一致 接続ルールの場合、次のタイプのパラメーターを指定できます。 • DNSのドメインが一致 • DNSのサーバーアドレスが一致 • SSIDが一致 • URL文字列のプローブ • インターフェイスの種類が一致 • ドメイン • DNSサーバー • URLプローブ

オンデマンド専用アプリが有効	Per-App VPNオンデマンドを有効化するときに選択します。
ドメイン	
Safariドメイン(iOS)	リストのエントリーそれぞれがSafariでVPN接続をトリガーするドメインを指定する必要があります。ドメイン名はwww.apple.comの形式で入力します。
iOS 14.0+とmacOS 11.0+	
関連ドメイン	1つ以上の関連ドメインを指定します。そのいずれかのドメイン内におけるサーバーへの接続はPer-App VPNと関連付けられます。
除外ドメイン	1つ以上の除外ドメインを指定します。そのいずれかのドメイン内におけるサーバーへの接続はPer-App VPNから除外されます。
iOS 13+とmacOS 10.15+	
メールドメイン	**[+追加]**をクリックし、メールでこのVPN接続をトリガーする1つ以上のドメイン名を入力します。ドメイン名はwww.apple.comの形式で入力します。
連絡先ドメイン	**[+追加]**をクリックし、連絡先でこのVPN接続をトリガーする1つ以上のドメイン名を入力します。ドメイン名はwww.apple.comの形式で入力します。

カレンダードメイン	**[+追加]** をクリックし、カレンダーでこのVPN接続をトリガーする1つ以上のドメイン名を入力します。ドメイン名はwww.apple.comの形式で入力します。
iOS 9以降	
プロバイダーの種類 (iOS 9+)	以下のいずれかのトンネルプロバイダーを選択してください： • アプリプロキシ - アプリレイヤでトラフィックをトンネリングします。アプリプロキシプロバイダーの詳細は、Appleドキュメンテーションをご覧ください。 • パケットトンネル - IPレイヤでトラフィックをトンネリングします。パケットトンネルプロバイダーの詳細は、Appleドキュメンテーションをご覧ください。

IPsec (Cisco)

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
マシン認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
ユーザーPINを含む	ユーザーにPINの入力を要求する場合に選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Cisco AnyConnect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
グループ	接続の認証に使用するグループを入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Juniper SSL

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
領域	接続の認証に使用する認証領域を入力します。
役割	接続の認証に使用する認証役割を入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	**証明書**は使用するユーザー認証方法です。以下のフィールドが使用できます。 **認証情報**：使用するID証明書を選択します。ユーザー提供の証明書はiOSデバイスでのみ利用可能です。

プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。 次のオプションを選択します。 • VPNオンデマンドを有効化 - オンデマンドでVPNを構築するドメインもしくはホスト名を追加します。 • iOS規則を有効化 • オンデマンドマッチアプリ有効
Safariのドメイン	Safariのドメインを追加するには **[+追加]** をクリックします。
プロバイダーの種類 (iOS 9.0+)	**パケットトンネル**は、デフォルトでトンネルプロバイダーのタイプとして選択されています。 パケットトンネルプロバイダーの詳細は、Appleドキュメンテーションをご覧ください。

F5 SSL

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

SonicWALL Mobile Connect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ログイングループまたはドメイン	接続の認証に使用するログイングループまたはドメインを入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Aruba VIA

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

設定	操作内容
識別子	このカスタムSSL VPNの識別子を逆DNSフォーマットで入力します（com.mycompany.myserverなど）。
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	証明書認証のみサポートされます。

証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。
(iOS 9.0+) iOSメインおよびサブVPNディクショナリにプロバイダーの種類を含める	plist(あらかじめ定義した構成ファイル)の生成中にプロバイダーの種類を含める場合に選択します。

Palo Alto Networks GlobalProtect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。
カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	証明書はユーザー認証方法です。 **[認証情報]** フィールドで使用するID証明書を選択してください。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

構成の配布

Ivanti Neurons for MDMリリース91以降、グローバル管理者は、すべてのデバイス向けおよびカスタム配布オプション向けのPer-App VPN構成の編集を、スペース管理者に委譲できるようになりました。Per-App VPN構成の場合、[この構成をすべてのスペースで利用可能にします] オプションを選択できます(任意)。

配布の変更は、特定のスペースにのみ適用されます。その他のすべてのスペースは、デフォルトのスペース配布設定を継承します。

手順

1. 前述の表にある情報を使用して、フィールドに構成設定を入力します。
2. **[次へ]** をクリックします。
3. **[この構成を有効化]** オプションを選択します。
4. 以下の配布オプションから1つ選択します。
    - **すべてのデバイス**。以下のオプションから1つ選択してください:
        - **他のスペースに適用しない**。
        - **他のスペースにあるデバイスに適用する**。
            - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。
    - **デバイスなし**(デフォルト)
    - **カスタム**。以下のオプションから1つ選択します。
        - **他のスペースに適用しない**。
        - **他のスペースにあるデバイスに適用する**。
            - **[スペース管理者に配布の編集を許可]** のチェックボックスを選択すると、委譲スペース管理者が特定のスペースの配布を編集できるようになります。

詳細は構成を作成するにはを参照してください。

シングルサインオン構成

Ivanti Neurons for MDM は拡張可能SSO構成と拡張可能SSO Kerberos構成で拡張可能シングルサインオンを実現します。実装にはIDプロバイダーのアプリ拡張(Microsoft Authenticatorなど)が必要です。拡張可能SSO実装により、ユーザーは1回の認証で企業リソースにアクセスできます。ユーザは、その後のログインで認証を求められません。想定されているIDプロバイダの設定情報については、「IDプロバイダーの構成」ページ1130をご参照ください。

このセクションは以下のトピックを含みます。

- シングルサインオンアカウント設定
- 拡張可能シングルサインオンアカウント設定
- 拡張可能シングルサインオンKerberosアカウント設定

シングルサインオンアカウント設定

対象: iOS 7.0以降、Ivanti Neurons for MDMがサポートする最新版まで。

iOSデバイスのマネージドアプリやApple Safariブラウザに関しては、次の設定を使用してKerberosベースの企業SSOを構成してください。

この構成にはTunnelとSentryが必要です。詳細は「*Tunnel for iOS Guide*」の「Setting up single sign-on with Kerberos」をご参照ください。

設定	説明
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ユーザ名	Kerberos プリンシパル名を入力します。
ケルベロスの領域名	Kerberos の領域名を入力します。
証明書	**iOS 8 でGold ライセンス:** ケルベロスの認証情報更新に使用する証明書を選択します。
URL接頭辞の一致	HTTP上でのケルベロス認証にこのアカウントを使用するために一致していなければならないURL接頭辞のリスト。
SSO対応許可リストアプリケーション	アプリカタログからアプリを追加して、それらをSSO用に許可リスト化します。 たとえばApple Safariを追加するには「Safari」と入力します。 この種類の構成を使用してSSOを利用できるアプリが許可リストに指定されていない場合は、内蔵のiOSアプリなど、iOS SSOに対応するすべてのアプリがSSOを利用できます。

拡張可能シングルサインオンアカウント設定

対象:

- iOS 13.0以降、Ivanti Neurons for MDMがサポートする最新版まで。
- macOS 10.15以降、Ivanti Neurons for MDMがサポートする最新版まで。

次の設定を使用して汎用拡張タイプでSSO拡張プロファイルを構成し、さまざまな認証方式によるネイティブアプリとWebサイトのSSOを可能にします。

macOS 10.15.xデバイス用のユーザーチャネルで構成がプッシュされている場合、拡張可能SSOは機能しません。

設定	説明
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
SSOの種類を選択	次のSSOタイプから1つを選択します。 • **認証情報** ◦ アプリ拡張を通じて認証可能な**ホスト**名またはドメイン名を1つ以上入力します。ホストまたはドメイン名は大文字小文字の違いがあっても一致と見なされます。インストールされたすべての拡張可能SSOペイロードのすべてのホスト/ドメイン名に重複は許可されません。「.」で始まるホストはワイルドカードサフィックスであり、すべてのサブドメインに一致します。それ以外のホストは完全な一致である必要があります。 ◦ **領域**名を入力します。この値の大文字と小文字は適切に使用してください。 • **リダイレクト** ◦ アプリ拡張がSSOを実行するIDプロバイダーの**URL**接頭辞を1つ以上入力します。URLはhttp://またはhttps://で始まる必要があり、スキームとホスト名は大文字小文字の違いがあっても一致と見なされます。クエリパラメータとURLフラグメントは許可されません。インストールされているすべての拡張可能SSOペイロードのURLに重複は許可されません。
拡張識別子	特定のURLにSSOを実行するアプリ拡張のバンドル識別子を入力します。
チーム識別子	アプリ拡張のチーム識別子。 このキーはmacOSで必要となり、他では無視されます。
カスタムデータ	1つ以上のカスタムデータをキー/値のペアとして入力します。
認証方法 (macOS 13以上のみ)	• パスワード • ユーザSecure Enclaveキー
登録トークン	トークンを入力します。 認証方法のいずれかを選択すると、このフィールドが有効になります。

拡張可能シングルサインオンKerberosアカウント設定

対象：

- iOS 13.0以降、Ivanti Neurons for MDMがサポートする最新版まで。
- macOS 10.15以降、Ivanti Neurons for MDMがサポートする最新版まで。

以下の設定を使用し、Kerberos拡張でSSOを実行するアプリ拡張を構成します。

macOS 10.15.xデバイス用のユーザーチャネルで構成がプッシュされている場合、拡張可能SSO Kerberosは機能しません。

設定	説明
基本設定	
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ユーザ名	Kerberos プリンシパル名を入力します。
領域	Kerberos の領域名を入力します。
証明書	Kerberos認証情報の更新に使用する証明書を選択します。
URL接頭辞	HTTP上でのケルベロス認証にこのアカウントを使用するために一致していなければならないURL接頭辞のリスト。
高度な設定	
自動ログインを許可	Falseの場合、キーチェーンにパスワードを保存できません。 デフォルトでは有効化されています。
ユーザー設定を遅らせる	Trueの場合、管理者がアプリSSOツールで有効化する、またはKerberosチャレンジを受信するまで、ユーザーはKerberos拡張機能の設定を指示されません。このオプションは、macOS 11から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
ユーザープレゼンスが必要	Trueの場合、キーチェーンエントリにアクセスする際に、ユーザーがTouch ID、Face ID、パスコードのいずれかを入力する必要があります。
認証情報キャッシュを監視	Falseの場合、一致する次のKerberosチャレンジまたはネットワーク状態の変化で認証情報が求められます。認証情報が期限切れまたは紛失した場合は新しく作成されます。このオプションは、macOS 11から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。 デフォルトでは有効化されています。
キャッシュ名	使用するKerberosキャッシュのGeneric Security Service(GSS) 名を入力します。このオプションは廃止されています。
ドメイン領域マッピング	領域名をキーとして入力します。値は領域に対応するDNSサフィックスの文字列です。 **[+追加]** をクリックして1つまたは複数のキー/値ペアを追加します。
デフォルト領域	複数のKerberos拡張構成がある場合、このプロパティがデフォルト領域を指定します。

設定	説明
使用サイト自動検出	Falseの場合、Kerberos拡張機能が自動的にLDAPとDNSを使用してADサイト名を判断することはありません。 デフォルトでは有効化されています。
サイトコード	Kerberos拡張が使用すべきActive Directoryサイト名を入力します。
複製時間	Active Directoryドメイン内の変更を複製するのにかかる秒数を入力します。Kerberos拡張機能はこれを使用してパスワードの変更禁止期間を確認します。このオプションは、macOS 11から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。このオプションは廃止されています。
認証情報バンドルID ACL	**[+追加]**をクリックし、認証時にTicket Granting Ticket(TGT) にアクセスできるバンドルIDのリストを追加します。
マネージドアプリをバンドルID ACLに含める	Trueの場合、Kerberos拡張機能はマネージドアプリのみに認証情報の使用を許可します。認証情報バンドルID ACLが指定されている場合は、それに追加となります。このオプションは、iOS 14、またはサポートされている最近のバージョンのIvanti Neurons for MDMに適用されます。
Kerberosアプリをバンドル ID ACLに含める	Trueの場合、Kerberos拡張により、Ticket Viewerやklistなどの標準的なKerberosユーティリティが認証情報にアクセスし、それを使用できるようになります。macOS 12以降で使用可能。
カスタムユーザー名ラベル	「ユーザー名」ではなく、Kerberos 拡張で使用されているカスタムユーザー名ラベルを入力します。たとえば、「会社 ID」などです。このオプションは、macOS 11から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
ヘルプテキスト	Kerberosのログインウィンドウの一番下に表示されるテキストを入力します。ヘルプ情報または免責事項を表示する目的で使用できます。このオプションは、iOS 14およびmacOS 11から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。

設定	説明
認証情報使用モード	この設定は他のプロセスによるKerberos拡張認証情報の使用に影響を与えます。以下のいずれかを使用してください。 • 常時(デフォルト) - サービスプリンシパル名(SPN)がKerberos拡張ホストの文字列に一致すれば、拡張認証情報が常に使用されます。呼び出し側のアプリがcredentialBundleIDACLにない場合は認証情報が使用されません。 • 指定がない場合 - 呼び出し側によって別の認証情報が指定されておらず、SPNがKerberos拡張ホスト文字列に一致する場合のみ、この認証情報が使用されます。呼び出し側のアプリがcredentialBundleIDACLにない場合は認証情報が使用されません。 • Kerberosのデフォルト - 認証情報を選択するデフォルトのKerberosプロセスが使用され、通常はデフォルトのKerberos認証情報が使用されます。この機能をオフにするのと同じです。 (任意) **[LDAPにTLSを要求]** を選択します。
優先されるKerberosキー配布センター	優先されるKerberosキー配布センターを追加します。 優先されるKDCを追加するには **[+追加]** をクリックします。
	プラットフォーム SSO 認証フォールバックを許可 - オンにして、[プラットフォーム SSO TGT を使用] もオンの場合、ユーザーは手動でサインインできます。macOS 12以降
	Kerberos のみを実行 - オンの場合、Kerberos 拡張は Kerberos 要求のみを処理します。macOS 13以降。
	プラットフォーム SSO TGT を使用 - オンの場合、この構成は、新規要求せずに、プラットフォーム SSO の TGT を使用します。macOS 13以降。
パスワード設定	
パスワード変更を許可	Falseの場合、パスワード変更が不可になります。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。 デフォルトでは有効化されています。
パスワード変更URL	ユーザーがパスワード変更を開始したときにユーザーのデフォルトのWebブラウザで起動するURLを入力します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。

設定	説明
パスワードの複雑性を許可	Trueの場合、パスワードは、Active Directoryの「複雑さ」の定義を満たしている必要があります。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
Minimum Password Length (パスワードの最小文字数)	ドメインにおけるパスワードの最小文字数を入力します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
パスワード有効期限切れ通知	パスワード有効期限切れの通知がユーザーに送信されてからパスワードの有効期限切れまでの日数を入力します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。 デフォルト値は15日です。
パスワード有効期限切れオーバーライド	このドメインでパスワードを使用できる日数を入力します。ほとんどのドメインでは自動的に計算されます。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。(このオプションは廃止されました)
パスワード要求テキスト	ドメインのパスワード要件のテキスト版を入力します。pwReqComplexityまたはpwReqLengthが指定されていない場合にのみ使用します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
パスワード履歴数	このドメインで再使用できない過去のパスワード数を入力します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
パスワードの最小変更禁止期間	このドメインのパスワード変更禁止期間の最小値(日数)を入力します。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。
ローカルパスワードの同期許可	Falseの場合、パスワード同期が不可になります。 ユーザーがモバイルアカウントでログインしている場合は機能しません。このオプションは、macOS 10.15から、Ivanti Neurons for MDMでサポートされている最新バージョンまで適用されます。

詳細は構成を作成するにはを参照してください。

iOS対応マルチユーザーセキュアサインイン

マルチユーザー対応のWebクリップでは、Ivanti Neurons for MDMに登録されているiOSデバイスに複数のユーザーがログイン/ログアウトできます。ユーザーに関連付けられているプロファイル、アプリ、構成は、初回ログイン時にデバイスにプッシュされます。ユーザーは作業が終わった後、Webクリップを開き、「ログアウト」を選択します。これでデバイスはnobodyユーザーに割り当てられ、ログインしていたユーザーのプロファイル、アプリ、構成(構成やアプリがnobodyユーザーに配布されていない限り)が削除されます。ログアウト後、Webクリップはリセットされ、次のユーザーがログインによって自分のカスタム構成、アプリ、ポリシーを取得します。マルチユーザーセキュアサインイン機能の使用にデバイス監視は必要ありません。マルチユーザーサインイン機能の詳細は、サポートナレッジベースの記事「Ivanti Neurons for MDM: iOS対応マルチユーザーセキュアサインイン」を参照してください。

対象: iOSデバイス(ユーザ登録デバイスには適用されません)

このセクションは以下のトピックを含みます。

- サポートされる認証情報
- nobodyユーザーについて
- デバイスへのサインイン
- デバイスからのサインアウト

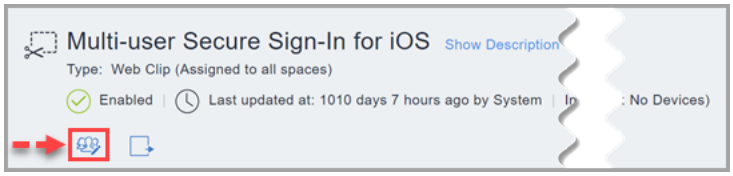
サポートされる認証情報

マルチユーザーセキュアWebクリップへのログインにはユーザー名とパスワードが必要です。PINベースの登録とSAML 2.0 IdPベースの登録はマルチユーザーセキュアWebクリップではサポートされません。

手順

1. **[構成]**に進みます。
2. **[iOS対応マルチユーザーセキュアサインイン]**をクリックします。必要に応じて、検索機能で複数の構成ページがあるかどうか確認します。**[+追加]**を選択してもこの構成にはアクセスできません。

3. **[配布を編集]** または対応のアイコンをクリックし、適切なデバイスグループにWebクリップを配布します。



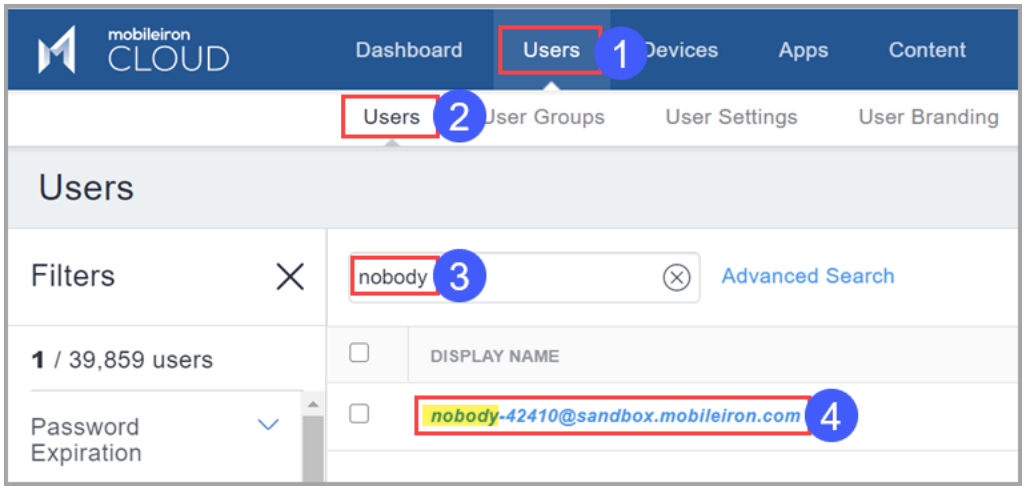
ユーザーグループに配布する場合は、ユーザーグループに結び付く動的デバイスグループを作成します。

4. 以下の配布オプションのいずれかを選択します。Webクリップは常にnobodyユーザーまたはnobodyユーザーに関連するデバイスグループに配布する必要があることにご注意ください。これはデフォルトではないため、必ずnobodyユーザーに配布していることを確認します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム

5. **[保存]** をクリックします。

***nobody*ユーザーについて**

Webクリップを通じてデバイスからログアウトすると、デバイスはnobodyユーザーと呼ばれる専用ユーザーでIvanti Neurons for MDMに登録された状態になります。ユーザーのログアウト時にアプリや構成をデバイスから削除したい場合は、そのようなアプリや構成がnobodyユーザーに配布されていないことを確認してください。ユーザーがセキュアサインインのWebクリップからサインアウトした後も特定の構成、たとえばWi-Fiをデバイス上に残したい場合は、それらの構成をnobodyユーザーにも配布しておきます。



つまり、アプリと構成を配布するユーザーグループとデバイスグループには常に注意が必要です。アプリを全員に配布し、ユーザーがデバイスからサインアウトするときにアプリを削除したい場合は、nobodyユーザーを含まないユーザーグループを作成するのがベストプラクティスです。カスタム属性を使えば、「マルチユーザー」のユーザーグループとnobodyユーザーのみを含む別のユーザーグループを簡単に作成できます。まず [管理] > [システム] > [属性] で「マルチユーザーオーナー」と呼ばれるユーザー属性を作成し、nobodyユーザーに「Yes」または「True」の値を指定してください。その後、その属性の値に基づいてユーザーグループやデバイスグループを作成します。

デバイスへのサインイン

ユーザーはiOSデバイスにサインインし、デバイスを自分に割り当てることができます。ログイン後、必要なすべてのアプリケーション、ポリシー、構成、証明書がデバイスにプッシュされます。

デバイスからのサインアウト

ユーザーは自分のiOSデバイスを使用後、サインアウトできます。サインアウトすると、アプリケーション、ポリシー、構成、証明書がデバイスから削除され、サインイン前の状態になります。これで、別のユーザーによるサインインが可能となります。

詳細はマルチユーザサインインブランディングをご参照ください。

Android APN設定の構成

Android APN設定の構成では、パブリックネットワーク上のデバイスに必要なアクセスポイント名(APN)を設定できます。この構成は、Android Enterprise仕事用マネージドデバイス、および会社所有デバイス上の仕事用プロファイルを持つマネージドデバイス(Androidバージョン9.0またはサポートされる以降のバージョン)に適用されます。

手順

1. **[構成] > [+追加]** を開きます。
2. **[Android APN設定]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [構成設定] セクションで、以下のオプションを構成します。

設定	説明
エントリー名	アクセスポイント設定の名前を入力。
アクセスポイント名	アクセスポイントの名前を入力。
アクセスポイントタイプ	アクセスポイントの種類を以下から選択： • **デフォルト** • **DUN** • **IMS** • **緊急** • **MMS** • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
MVNOの種類	仮想移動体通信事業者(MVNO)の種類を以下から選択： • **なし** • **SPN** • **IMSI** • **GID** • **ICCID**

設定	説明
Bearer	データ送信に使用されるベアラサービスの種類を以下から選択： • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN** • **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**

設定	説明
APNプロトコル	APNに必要なAPNプロトコルを以下から選択： • **なし** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP**(ポイントツーポイントプロトコル) • **非構造化**
APNローミングプロトコル	APNに必要なAPNローミングプロトコルを以下から選択： • **なし** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP**(ポイントツーポイントプロトコル) • **非構造化**
APNを有効化/無効化	APN構成をオンにする。
通信事業者ID	通信事業者IDの数値を入力。

設定	説明
認証タイプ	認証プロトコルの種類を以下から選択： • **なし** • **PAP**(Password Authentication Protocol) • **CHAP**(Challenge-Handshake Authentication Protocol) • **PAPまたはCHAP**
ユーザー名	ログインユーザー名を入力。
パスワード	ログインパスワードを入力。
パスワードの確認	確認のためパスワードを再入力。
ポート番号	ポート番号を入力(1～65535の数値)。
プロキシアドレス	プロキシアドレスの種類。
Mobile Country Code	Mobile Country Codeを入力。
Mobile Network Code	Mobile Network Codeを入力。
MMSプロキシアドレス	MMSプロキシアドレスを入力。
MMSポート番号	MMSポート番号を入力(1～65535の数値)。
MMSサーバーアドレス(mmsc)	MMSサーバーアドレスを入力。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。

- **すべてのデバイス**
- **デバイスなし**(デフォルト)
- **カスタム**

8. **[完 了]** をクリックします。

デバイスが以 下 の値 を持 つ既 存 のAPN構 成 がある場 合 、以 下 のフィールドに同 じ値 を持 つAPN構 成 を追 加 することはできません。

- Mobile Country Code
- Mobile Network Code
- アクセスポイント名
- プロキシアドレス
- ポート番 号
- MMSプロキシアドレス
- MMSポート番 号
- MMSサービスアドレス
- APNを有 効 化 /無 効 化
- MVNOの種 類
- APNプロトコル
- APNローミングプロトコル

Android APN設 定 の構 成 は、手 動 で、または通 信 事 業 者 によってデバイス内 ですでに構 成 されている他 のAPN設 定 より優 先 されます。

VPN構成

対象：

- Android(Android Enterpriseデバイスでは廃止されています。アプリカタログ内にある特定のVPN用のマネージド構成を使用する必要があります)
- Windows
- iOS
- macOS

VPN構成では、特定のアプリへの仮想プライベートネットワークの設定を定義します。

手順

1. **[構成]** > **[+追加]** を開きます。
2. **[VPN]** 構成を選択します。
3. 構成の**名前**を入力します。
4. 説明を入力します。
5. 以下の説明に従ってVPNを設定します。
6. (iOS 9.0+のみ) ドメイン一致のセクションで **[+追加]** をクリックし、1つ以上の一致するドメイン (例：company.com) を入力します。ドメインが次に指定したドメインのいずれかである場合、プロキシ接続を使用します。
7. **[次へ]** をクリックします。
8. (macOSのみ) [配布] ページで、以下のいずれかの配布オプションを選択します。
   - デバイスチャネル - 設定はデバイス上のすべてのユーザーに有効です。標準的なオプションです。
   - ユーザーチャネル - 設定はデバイス上の現在の登録ユーザーにのみ有効です。
9. この構成の残りの配布オプションを選択します。
10. **[完了]** をクリックします。

VPN設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
接続の種類	構成するVPNの種類を選択します。 残りの設定は、この選択に依存します。

プロトコルと設定は以下のとおりです。

- L2TP(Ivanti Goではサポートされていません)
- PPTP(Ivanti Goではサポートされていません)
- IPsec(Cisco) (Ivanti Goではサポートされていません)
- Cisco AnyConnect(Ivanti Goでサポートされています)
- Juniper SSL(Ivanti Goではサポートされていません)
- NetMotion VPN(Ivanti Goではサポートされていません)
- Pulse Secure(Ivanti Goでサポートされています)
- F5 SSL(Ivanti Goではサポートされていません)
- SonicWALL Mobile Connect(Ivanti Goではサポートされていません)
- Aruba VIA(Ivanti Goではサポートされていません)
- Custom SSL(Ivanti Goではサポートされていません)
- Palo Alto Networks GlobalProtect(Ivanti Goでサポートされています)
- KEv2(Windowsのみ) (Ivanti Goではサポートされていません)
- IKEv2(Ivanti Goではサポートされていません)

L2TP

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	使用する認証方式として、**[パスワード]** または **[RSA SecureID]** を選択します。
共有シークレット	接続の開始に必要な場合は、共有シークレットパスコードを入力します。
すべてのトラフィックを送信	すべてのネットワークトラフィックにこの接続を使用するにはこのオプションを選択します。このオプションは、特に公衆網においてデータを危険から保護するのに役立ちます。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

PPTP

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	使用する認証方式として、**[パスワード]** または **[RSA SecureID]** を選択します。
暗号化レベル	接続のデータ暗号化レベルとして、**[なし]**、**[自動]** または **[最高(128ビット)]** を選択します。
すべてのトラフィックを送信	すべてのネットワークトラフィックにこの接続を使用するにはこのオプションを選択します。このオプションは、特に公衆網においてデータを危険から保護するのに役立ちます。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

IPsec (Cisco)

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
マシン認証	使用する認証方式として、**[共有シークレット/グループ名]** または **[証明書]** を選択します。
グループ名	[共有シークレット/グループ名] 認証 使用するグループの名前を指定します。ハイブリッド認証を使用する場合、文字列の末尾が "[hybrid]" である必要があります。
共有シークレット	[共有シークレット/グループ名] 認証 共有シークレットパスコードを入力します。
ハイブリッド認証を使用	[共有シークレット/グループ名] 認証 ハイブリッド認証を指定する場合に選択します。ハイブリッド認証では、サーバーが証明書を提供し、クライアントが事前共有キーを提供します。
パスワード確認	[共有シークレット/グループ名] 認証 接続時にユーザーにパスワードの入力を要求するかどうかを指定します。

証明書	*[証明書] 認証* 使用するID証明書を選択します。
ユーザーPINを含む	*[証明書] 認証* ユーザーにPINの入力を要求する場合に選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Cisco AnyConnect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
グループ	接続の認証に使用するグループを入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 **[証明書]** を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
領域	接続の認証に使用する認証領域を入力します。

役割	接続の認証に使用する認証役割を入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 **[証明書]** を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

NetMotion VPN

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。**[証明書]** を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

F5 SSL

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を入力します。 **[証明書]** を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	[手動] または [自動] を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

SonicWALL Mobile Connect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ログイングループまたはドメイン	接続の認証に使用するログイングループまたはドメインを入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 [証明書]を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Aruba VIA

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 **[証明書]** を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	[手動] または [自動] を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

設定	操作内容
識別子	このカスタムSSL VPNの識別子を逆DNSフォーマットで入力します（com.mycompany.myserverなど）。
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*

カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 [証明書]を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Palo Alto Networks GlobalProtect

Windows PhoneとAndroidデバイスには適用されません。

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。
カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	使用するユーザー認証方式として、**[パスワード]** または **[証明書]** を選択します。 [証明書]を選択すると、以下のフィールドが利用できるようになります。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

IKEv2 (Windowsのみ)

設定	操作内容
サーバー	VPNサーバーのホスト名またはIPアドレスを入力します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

設定	操作内容
サーバー	VPNサーバーのホスト名またはIPアドレスを入力します。
ローカル識別子	以下のいずれかの形式のIKEv2クライアント識別子： • **FQDN** • **UserFQDN** • **アドレス** • **ASN1DN**
リモート識別子	以下のいずれかの形式のリモート識別子： • **FQDN** • **UserFQDN** • **アドレス** • **ASN1DN**
マシン認証	**[EAPを有効化]** が選択されていない場合のみ利用できます。 以下のいずれかを選択します。 • 証明書 • 共有シークレット
EAP認証	**[EAPを有効化]** が選択されている場合のみ利用できます。 以下のいずれかを選択します。 • 証明書 • ユーザー名/パスワード

共有シークレット	マシン認証に共有シークレットが選択されている場合のみ利用できます。接続の共有シークレットを入力します。
証明書	マシン認証に証明書が選択されている場合のみ利用できます。使用する証明書を選択します。その証明書がIKEクライアント認証に送信されます。拡張認証を使用する場合、この証明書をEAP-TLSに使用可能です。
EAPを有効化	拡張認証を有効する場合に選択します。
アカウント	EAP認証にユーザー名/パスワードが選択されている場合のみ利用できます。VPNサーバーのアカウントIDを入力します。
パスワード	EAP認証にユーザー名/パスワードが選択されている場合のみ利用できます。VPNサーバーのパスワードを入力します。
デッドピア検出の間隔	以下のオプションから1つ選択してください: • **なし(無効)** • **低(1時間毎にkeepaliveを送信)** • **中(30分毎にkeepaliveを送信)** • **高(10分毎にkeepaliveを送信)**
サーバー証明書発行者の共通名	(任意) - サーバー証明書発行者の共通名。IKEサーバーが証明書発行者に基づいた証明書要求をサーバーに送信するようになります。
サーバー証明書の共通名	(任意) - IKEv2サーバーによって送信された証明書の検証に使用されるサーバー証明書の共通名
IP4およびIP6サブネット属性を使用	(任意) IP4とIP6のサブネット属性を使用することを選択します。

IKEv2 Mobility and Multihoming Protocol(MOBIKE)を有効化	(任意)デフォルト設定は0です。MOBIKE(複数のIPアドレスでWi-Fiとセルラーリンクの両方に接続されている場合、マルチホームのモバイルデバイスをサポートする機能)が有効化されます。これはデフォルトで有効になっています。1に設定するとMOBIKEが無効化されます。
Perfect Forward Secrecy(PFS)を有効化	(任意)1に設定すると、IKEv2接続の場合のPFSが有効になります。デフォルト設定は0です。
IKEv2リダイレクトを有効化	(任意)デフォルト設定は0です。サーバーからリダイレクト要求を受信する場合は、IKEv2接続がリダイレクトされます。これはデフォルトで有効になっています。1に設定するとIKEv2リダイレクトが無効化されます。
NAT keepaliveを有効化	ネットワークアドレス変換を有効化し、NATとIKEピアとの間にトラフィックがない場合に、NATエントリが削除されないようにします。
NAT keepaliveの間隔	NAT keepaliveが有効になっている場合、これはデバイスにkeepaliveパケットが送信される時間(秒)です。
暗号化アルゴリズム	以下のオプションから1つ選択してください: • **DES** • **3DES** • **AES-128** • **AES-256**(デフォルト) • **AES-128 GCM** • **AES-256 GCM**

完全性アルゴリズム	以下のオプションから1つ選択してください： • **SHA2-256**（デフォルト） • **SHA2-384** • **SHA2-512**
Diffie Hellmanグループ	以下のオプションから1つ選択してください： • **1**。 • **2**（デフォルト） • **5** • **14** • **15** • **16** • **17** • **18**
分単位の有効期間	SA有効期間（リキー間隔）を分単位で入力します。有効値は10～1440です。

プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

*このフィールドに対応する変数がある場合に、そのリストを参照するには、$ を入力してください。

詳細は構成を作成するにはを参照してください。

VPNオンデマンド

対象：iOSデバイス

VPNオンデマンド構成では、ドメイン、ホスト名などに基づきVPNサーバーへのアクセスを設定します。

VPNオンデマンド設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
接続の種類	構成するVPNの種類を選択します。 残りの設定は、この選択に依存します。

オンデマンドVPNの有効化	オンデマンドVPNを確立するドメインおよびホスト名にこの構成を使用する場合に選択します。

iOS規則を有効化 ([オンデマンドVPNを有効化]が選択されている場合のみ)	iOSおよびmacOSの場合、以下を設定できます。 • trueと判断されたネットワークへの接続の許可または禁止、および許可または無視を設定するネットワークルール。 • trueと判断されたネットワークへの接続を必要時に許可する、あるいはすべて許可しない接続ルール。 ネットワークルールの場合、次のタイプのパラメーターを指定できます。 • DNSのドメインが一致 • DNSのサーバーアドレスが一致 • SSIDが一致 • URL文字列のプローブ • インターフェイスの種類が一致 接続ルールの場合、次のタイプのパラメーターを指定できます。 • DNSのドメインが一致 • DNSのサーバーアドレスが一致 • SSIDが一致 • URL文字列のプローブ • インターフェイスの種類が一致 • ドメイン名 • DNSサーバー • URLプローブ

プロバイダーの種類 (iOS 9+)	以下のいずれかのトンネルプロバイダーを選択してください: • アプリプロキシ - アプリレイヤでトラフィックをトンネリングします。アプリプロキシプロバイダーの詳細は、Appleドキュメンテーションをご覧ください。 • パケットトンネル - IPレイヤでトラフィックをトンネリングします。パケットトンネルプロバイダーの詳細は、Appleドキュメンテーションをご覧ください。

プロトコルと設定は以下のとおりです。

- IPsec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- カスタムSSL
- Palo Alto Networks GlobalProtect

IPsec (Cisco)

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
マシン認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
ユーザーPINを含む	ユーザーにPINの入力を要求する場合に選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Cisco AnyConnect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
グループ	接続の認証に使用するグループを入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Juniper SSL

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
領域	接続の認証に使用する認証領域を入力します。
役割	接続の認証に使用する認証役割を入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]:** プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]:** プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]:** プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL:** プロキシの完全修飾URLを入力します。

NetMotion VPN

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	証明書はユーザー認証方法です。 **[認証情報]**: 使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

F5 SSL

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

SonicWALL Mobile Connect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ログイングループまたはドメイン	接続の認証に使用するログイングループまたはドメインを入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Aruba VIA

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

カスタムSSL

設定	操作内容
識別子	このカスタムSSL VPNの識別子を逆DNSフォーマットで入力します（com.mycompany.myserverなど）。
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。*
カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	証明書認証のみサポートされます。
証明書	使用するID証明書を選択します。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

Palo Alto Networks GlobalProtect

設定	操作内容
サーバー	VPNサーバーのIPアドレスまたはホスト名を入力します。
アカウント	接続の認証に使用するユーザーアカウントを入力します。
カスタムデータ	このVPNのカスタムデータを定義するキー値ペアを入力します。
ユーザー認証	証明書はユーザー認証方法です。 **[認証情報]** フィールドで使用するID証明書を選択してください。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。 **[手動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 **[自動] を選択すると、**以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

Wi-Fi構成

対象：

- Android
- Windows
- iOS
- macOS

このセクションは以下のトピックを含みます。

Wi-Fi設定

- WEP、WPA/WPA2/WPA3、任意(個人)の設定
- WEPエンタープライズ、WPA/WPA2/WPA3エンタープライズ、任意(法人)の設定
- iOSとmacOS

Wi-Fi設定

Wi-Fi構成では、無線ネットワークへのアクセスを設定します。

ユーザーは、デバイス上のWi-Fi設定の一部を変更できます。しかし、デバイスのOSによって、MDMサーバーが変更に関する情報を受け取る場合と受け取らない場合があります。したがって、デバイス上の構成をサーバー上の構成で上書きするよう、構成が自動的にデバイスに再プッシュされることはありません。

Procedure手順

1. **[構成]** > **[+追加]** を開きます。
2. **[Wi-Fi]** 構成を選択します。
3. 構成の**名前**を入力します。
4. 説明を入力します。
5. 以下の説明に従ってWi-Fiを設定します。

6. **[次へ]** をクリックします。
7. (macOSのみ) [配布] ページで、以下のいずれかの配布オプションを選択します。
   - デバイスチャネル - 設定はデバイス上のすべてのユーザーに有効です。標準的なオプションです。
   - ユーザーチャネル - 設定はデバイス上の現在の登録ユーザーにのみ有効です。
8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
9. **[完了]** をクリックします。

次の表はWi-Fiの設定を示します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
サービスセット識別子 (SSID)	これらの設定を適用する無線ネットワークの名前を入力します。このフィールドでは、大文字と小文字が区別されます。
自動参加	デバイスが対応するWi-Fiネットワークに自動的に接続するようにする場合に選択します。このオプションが選択されていない場合、デバイスユーザーがネットワークに接続するにはデバイスでネットワーク名をタップする必要があります。
隠しネットワーク	ネットワークアクセスをブロードキャストしない場合は、このオプションを選択します。
キャプティブネットワーク検出を無効化(iOS 10+)	管理者はWi-Fiキャプティブバイパスモードを有効化または無効化できます。Appleは、キャプティブポータルの存在を検出すると、ログイン画面を開いてアクセスを要求します。キャプティブポータルの検出を無効化し、ユーザーが手動でWebブラウザを起動すればキャプティブネットワークのポータルログインがトリガーされるようにもできます。この新しい設定は、ISEキャプティブポータルがログイン画面のポップアップを妨げ、デバイスがインターネットに接続していないのに接続しているとユーザーが誤解する場合に有用です。
プロキシの設定	**[手動]** または **[自動]** を選択し、プロキシを構成します。

設定	操作内容
	[手動] を選択すると、以下のフィールドが追加で利用できるようになります。 • **[サーバーおよびポート]**: プロキシサーバーのネットワークアドレスとポート番号を入力します。* • **[認証]**: プロキシへの接続に必要な場合は、有効なユーザー名を入力します。* • **[パスワード]**: プロキシへの接続に必要な場合は、有効なパスワード名を入力します。 追加したホスト名を削除するには、「-」アイコンをクリックします。 **[自動]** を選択すると、以下のフィールドが追加で利用できるようになります。 • **プロキシサーバーURL**: プロキシの完全修飾URLを入力します。
セキュリティの種類	ネットワークにアクセスするために必要なセキュリティ対策を入力します。 • いずれの種類(個人) • いずれの種類(法人) • WEP • WEPエンタープライズ • WPA • WPAエンタープライズ • WPA2 • WPA2エンタープライズ • WPA3 • WPA3 Enterprise WPA3/WPA3エンタープライズはiOS 13+に対応します。

設定	操作内容
	Windowsは、WPA、WPAエンタープライズ、WPA2、およびWPA2エンタープライズをサポートします。

WEP、WPA/WPA2/WPA3、任意(個人)の設定

設定	操作内容
パスワード	(オプション) このネットワークにアクセスするためのパスワードを入力します。それ以外の場合、デバイスユーザーは、ネットワークにアクセスするために必要な何らかのパスワードをパスワードを入力するためのプロンプトが表示されます。

WEPエンタープライズ、WPA/WPA2/WPA3エンタープライズ、任意(法人)の設定

設定	操作内容
プロトコル	
承認済みEAP形式	ネットワークへのアクセスに使用できるEAPの種類を選択します。 • TLS • TTLS - 内部IDフィールドでは、OSデフォルト、PAP、CHAP、MSCHAP、MSCHAPv2、EAPなどいずれかの認証プロトコルを選択します。 • PEAP • LEAP(AMAPI登録デバイスではサポートされません) • EAP-SIM • EAP-AKA • EAP-FAST(AMAPI登録デバイスではサポートされません) Windows Phoneは、LEAP、EAP-SIM、EAP-AKA、EAP-FASTなどの複数のEAPタイプをサポートしません。ただし、現在AMAPIは単一のEAPのみサポートします。
EAP-FAST	認証方法を定義するEAP-FASTオプションを選択します。 • **PACを使用:** プロキシ自動構成(PAC)を使用する場合に選択します。

設定	操作内容
	• **PACのプロビジョニング:** PACのプロビジョニングを許可する場合に選択します。選択しない場合、デバイス上ですでにプロビジョニングされているPACのみ使用することができます。このオプションは [PAC使用] を選択した場合にのみ利用可能です。 • **匿名プロビジョンPAC:** サーバー認証なしでPACのプロビジョニングを許可する場合に選択します。このオプションは [PACのプロビジョニング] を選択した場合にのみ利用可能です。
認証	
ユーザー名	ネットワークアクセスに必要なユーザー名を指定します。これを空欄にしておくと、デバイスユーザーに入力を求めるプロンプトが表示されます。*
接続ごとのパスワードを使用	デバイスユーザーに対し、接続ごとにパスワードを求めるプロンプトを表示する場合に選択します。デバイスが同じネットワークに再接続される場合、デバイスユーザーにはネットワークへの接続の再認証を求めるプロンプトが表示されます。このオプションはAMAPI登録デバイスではサポートされません。
パスワード	(オプション) このネットワークにアクセスするためのパスワードを入力します。それ以外の場合、デバイスユーザーは、ネットワークにアクセスするために必要な何らかのパスワードをパスワードを入力するためのプロンプトが表示されます。
ID証明書	(オプション) 認証情報を識別するために使用する証明書を選択します。ID証明書構成では、利用可能な各ID証明書を定義します。
認証証明書 (Windows デバイスのみで利用可能)	次の3つの証明書ストアのいずれか1つを選択して証明書を選び、Wi-Fi ネットワークに接続します。 • コンピューターまたはユーザー: このオプションを選択し、そのユーザーがログインしていない場合、認証証明書はコンピューターのストアから選ばれます。そのユーザーがログインしている場合、ユーザーのストアから特定の証明書が選ばれます。 • コンピューター: このオプションを選択すると、認証証明書はコンピューターのストアから選ばれます。 • ユーザー: このオプションを選択すると、認証証明書はユーザーのストアから選ばれます。

設定	操作内容
	デフォルトでは、[ユーザー] オプションが選択されています。
外部識別子	(任意) TLS、TTLS、PEAP、およびEAP-FASTの場合、デバイスユーザーにIDを非表示にすることを許可する場合に選択します。ユーザーの実際の名前は暗号化されたトンネルの内側でのみ表示されます。このオプションにより、攻撃者にとっては認証中のユーザーの名前がプレーンテキストとしては見えないため、セキュリティが強化されます。
ドメイン	EAPの種類がTLSとTTLSの場合にサポートされます。
信頼性	
信頼性のある証明書 (AMAPI登録デバイスではサポートされません)	チェックボックスを選択して、リストから複数の証明書を選択します。
信頼性のあるサーバー証明書名	**[+追加]** をクリックし、1つ以上の信頼できるサーバー証明書を入力します。 (任意) [**信頼の例外を許可**] を選択すると、ユーザがダイアログウィンドウから信頼性を決定することができます。

iOSとmacOS

設定	操作内容
全バージョン	
ネットワークの種類	このネットワークを以下として扱う場合に選択: • 標準 • レガシーホットスポット • Passpoint
許可されたプロキシPACのフォールバック	(オプション) PACファイルが利用できない場合に、デバイスが直接宛先に接続することを許可します。
設定モード (任意)	添付する接続モードの種類を含む文字列群。 • システム: ユーザーがデバイスにログインする前にWi-Fiに接続します。

設定	操作内容
	• ログインウィンドウ: ユーザーがデバイスにログインした後にWi-Fiが利用可能になります。 現在、設定モードは、[システム] モードと[ログインウィンドウ] モードの両方が有効になっている場合にのみ機能します。
Passpoint設定	このセクションの設定は、ネットワークの種類にPasspointを選択した場合に表示されます。
ドメイン名	Passpointのネゴシエーションに使用するドメイン名を入力します。
ローミングパートナーのPasspointのネットワークに接続	(オプション) ローミングサービスプロバイダーへの接続を許可する場合に選択します。
ローミングコンソーシアムの組織識別子	(オプション) このWi-Fiプロファイルでサポートされているエンティティに対してIEEEが割り当てた識別子を入力します。
ネットワークアクセス識別子の領域名	(オプション) Passpointのネゴシエーションに使用するネットワークアクセス識別子の領域名を入力します。
MCCとMNCのペア	(オプション) Passpointのネゴシエーションに使用するMobile Country Code(MCC) とMobile Network Code(MNC) のペアを入力します。各文字列は必ず6桁となります。
表示される通信事業者名	(オプション) 表示する通信事業者名を入力します。
Cisco QoSファストレーン	このセクションの設定はCiscoファストレーン構成に適用されます。設定には、L2/L3マーキング用のアプリの許可リスト化、内蔵音声/動画サービス(FaceTimeやWi-Fi Callingなど) の音声/動画トラフィックの許可リスト化などがあります。
QoSマーキングを制約	選択しない場合、ネットワークがCisco QoSファストレーンをサポートしていればすべてのアプリがL2/L3マーキングを使用します。選択した場合、表示される **[アプリを選択]** 設定でL2/L3マーキングに含めたいアプリを追加します。選択されていないアプリはL2/L3マーキングを使用しません。
QoSマーキングを有効化	L3マーキングを無効化し、Wi-Fiネットワークに送信されるトラフィックにL2マーキングだけを使用します。選択しない場合、システムはWi-Fiを Cisco QoSファストレーンネットワークに関連しないものと扱います。

設定	操作内容
許可リストのApple音声/ビデオ通話	FaceTimeやWi-Fi Callingなどの内蔵音声/動画サービスの音声/動画トラフィックを許可リストに含めるかどうかを指定します。
アプリを選択	L2/L3マーキングに含めたいアプリを追加するのに使用します。選択されていないアプリはL2/L3マーキングを使用しません。
iOS 10+	
Cisco QoSファストレーン	このセクションの設定はCiscoファストレーン構成に適用されます。設定には、L2/L3マーキング用のアプリの許可リスト化、内蔵音声/動画サービス(FaceTimeやWi-Fi Callingなど) の音声/動画トラフィックの許可リスト化などがあります。
QoSマーキングを制約	選択しない場合、ネットワークがCisco QoSファストレーンをサポートしていればすべてのアプリがL2/L3マーキングを使用します。選択した場合、表示される **[アプリを選択]** 設定でL2/L3マーキングに含めたいアプリを追加します。選択されていないアプリはL2/L3マーキングを使用しません。
QoSマーキングを有効化	L3マーキングを無効化し、Wi-Fiネットワークに送信されるトラフィックにL2マーキングだけを使用します。選択しない場合、システムはWi-FiをCisco QoSファストレーンネットワークに関連しないものと扱います。
許可リストのApple音声/ビデオ通話	FaceTimeやWi-Fi Callingなどの内蔵音声/動画サービスの音声/動画トラフィックを許可リストに含めるかどうかを指定します。
アプリを選択	L2/L3マーキングに含めたいアプリを追加するのに使用します。選択されていないアプリはL2/L3マーキングを使用しません。
iOS 10.3+監視対象	
Wi-F許可リスト作成を有効化	デバイスが接続できるWi-Fiネットワークを決定します。複数のWi-Fi構成が存在する場合は、最も制限の厳しいものが適用されます。
iOS 14.0+	
MACアドレスのランダム化を無効化	AppleはiOS 14.0で、デバイスによるWi-Fi MACアドレス報告のデフォルト動作を変更し、新しい接続に関してデバイスの実際のWi-Fi MACアドレスではなく、ランダムなアドレスを報告するようにしました。この機能は、キャプティブポータルやMACアドレスのフィルタリングを使用している企業において予期しない動作を引き起こすことがあります。

設定	操作内容
	管理者は、Wi-Fi構成を編集し、このオプション(デフォルトではオフ) をオンにすることにより、**[MACアドレスのランダム化を無効化]** できます。これですべてのデバイスにWi-Fi構成が再度プッシュされます。このオプションにより、ネットワークのプライバシー保護レベルが低下したという警告がデバイス設定に表示されます。 ただし、デバイスユーザーがデバイスの設定から手動でオンまたはオフにすることは可能です。
Android 11+	
MACアドレスのランダム化	• 無効：ユーザーがデバイスにログインする前にWi-Fiに接続されます。 • 有効 - 自動：ユーザーがデバイスにログインした後にWi-Fiが利用可能になります。 • 有効 - 非永続的 • 有効 - 永続的

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

セルラーネットワーク構成

このセクションは以下のトピックを含みます。

- 「APN構成」ページ875
- 「セルラー」ページ876
- 「iOS Telecomのプリセット構成」ページ880
- 「eSIM構成」ページ881

APN構成

APN 構成はデバイスのセルラーアクセスポイント名を設定します。iOS 7の場合、代わりにセルラー構成を使用します。

APN設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
アクセスポイント名	対応するアクセスポイント名を入力します。名前は通常、通信事業者提供のサービスによって定義されます。
アクセスポイントのユーザー名	このアクセスポイントで許可されたユーザ名を入力します。*
アクセスポイントのパスワード	入力したユーザー名に対応するパスワードを入力します。
プロキシサーバーとポート	APNプロキシのIPアドレスまたはURLおよびポート番号を入力します。
EnableXLAT464	アクセスポイント名 (APN) を有効にするには、このチェックボックスをオンにします。このオプションにより、IPv6のみのネットワーク上でIPv4サービスが提供されます。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

詳細は構成を作成するにはを参照してください。

セルラー

対象：iOS 7.0+

このセクションは以下のトピックを含みます。

- デフォルトAPNのセルラー設定
- データAPNのセルラー設定
- ローミング中のセルラーアクセスの制御
- セルラーアクセスの制御

セルラー構成では、デバイスのセルラープロファイルを設定します。iOS 7.0以降を実行するデバイスでセルラーネットワーク設定を構成します。企業によっては、リモートネットワークアクセスまたは特別料金プランの固有のアクセスポイント名(APN)にアクセスを許可する、携帯電話事業者と契約する企業もあります。構成パラメータについては、携帯電話事業者にご相談ください。

- 一度に複数のセルラープロファイルをインストールすることはできません。
- APNプロファイルがすでにインストールされている場合は、セルラープロファイルをインストールできません。

[構成済みのAPN形式]ドロップダウンボックスでは、以下のAPN形式に対応するセルラー設定を構成できます。

- デフォルト & データAPN
- デフォルトAPN
- データAPN

すべての構成について、構成を特定する名前と説明(任意)を入力します。

デフォルトAPNのセルラー設定

デフォルトのAPN設定	操作内容
APN名	対応するアクセスポイント名を入力します。名前は通常、通信事業者提供のサービスによって定義されます。
APN認証の形式	(任意) 以下のいずれかを選択します。 • CHAP(challenge handshake authentication protocol) • PAP(password authentication protocol)
ユーザー名	(オプション) 認証に使用するユーザー名を入力します。
パスワード	(オプション) 認証に使用するパスワードを入力します。

データAPNのセルラー設定

データAPN設定	操作内容
APN名	対応するアクセスポイント名を入力します。名前は通常、通信事業者提供のサービスによって定義されます。
APN認証の形式	(任意)以下のいずれかを選択します。 • CHAP(challenge handshake authentication protocol) • PAP(password authentication protocol)
ユーザー名	(オプション)認証に使用するユーザー名を入力します。
パスワード	(オプション)認証に使用するパスワードを入力します。
プロキシサーバー	プロキシサーバーを指定します。
プロキシーサーバーのポート	プロキシサーバーポートを指定します。
10.3+	
許可されたプロトコルマスク	IPv4、IPv6、または両方を選択します。
国内ローミング中の許可されたプロトコルマスク	IPv4、IPv6、または両方を選択します。
ローミング中の許可されたプロトコルマスク	IPv4、IPv6、または両方を選択します。

ローミング中のセルラーアクセスの制御

デバイスがローミング状態の場合、一部またはすべてのマネージドアプリのセルラーデータへのアクセスを制限することができます。

手順

1. Ivanti Neurons for MDM のメインナビゲーションメニューで、**[ポリシー]** タブを開きます。
2. **[+追加]** をクリックします
3. **[新しいネットワーク利用構成]** をクリックします。
   [ネットワーク利用構成の作成] ページが表示されます。
4. **[全マネージドアプリを禁止]** チェックボックスを選択すると、ローミング中または常時、マネージドアプリがセルラーデータにアクセスするのをブロックします。
5. チェックボックスにチェックを入れないでおくと、マネージドアプリの名称やバンドルIDを指定して、セルラーデータの受信をブロックすることができます。
6. [アプリ] フィールドのプルダウンメニューを使用して、名前またはバンドルIDでアプリを探します。

セルラーアクセスの制御

いつでも、一部またはすべてのマネージドアプリのセルラーデータへのアクセスを制限することができます。限定的にアプリを使用することはできますが、セルラーデータへアクセスすることはできなくなります。

手順

1. Ivanti Neurons for MDM のメインナビゲーションメニューで、**[ポリシー]** タブを開きます。
2. **[+追加]** をクリックします
3. **[新しいネットワーク利用構成]** をクリックします。
   [ネットワーク利用構成の作成] ページが表示されます。
4. **[全マネージドアプリを禁止]** チェックボックスを選択すると、いつでも、マネージドアプリがセルラーデータにアクセスするのをブロックします。
5. 任意でチェックボックスにチェックを入れないでおくと、セルラーデータの受信をブロックするマネージドアプリを指定できます。
6. [アプリ] フィールドのプルダウンメニューを使用して、名前またはバンドルIDでアプリを探します。

詳細は構成を作成するにはを参照してください。

iOS Telecomのプリセット構成

iOS Telecomのプリセット構成では、ローミング制限やホットスポット制限のデフォルト値を設定します。

iOS Telecomのプリセット設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ローミング中にデバイスがボイスサービスを使うことを許可	音声ローミングを有効にする場合に選択します。音声ローミングの可用性は、通信事業者によって異なります。
ローミング中にデータサービスを利用することをデバイスに許可	データローミングを有効にする場合に選択します。 データローミングを有効にすると、デバイス上の音声ローミングも有効化されます。
ユーザーによるパーソナルホットスポットの使用を許可	パーソナルホットスポット機能を有効にする場合に選択します。この機能の可用性は、通信事業者によって異なります。

詳細は構成を作成するにはを参照してください。

eSIM構成

eSIM構成は、`RefreshCellularPlans`コマンドでデバイスのセルラーネットワークを構成します。管理者はセルラーネットワークをデバイスにマッピングする前に、eSIMの通信事業者URLを取得する必要があります。

対象：iOS、iPadOS

手順

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[eSIM]** と入力し、**[eSIM]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. **[iOS/iPadOS]** をクリックします。
5. 通信事業者URLを入力します。
6. **[次へ]** をクリックします。
7. **[この構成を有効化]** オプションを選択します。
8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし（デフォルト）
   - カスタム
9. **[完了]** をクリックします。

その他の構成

このセクションは以下のトピックを含みます。

- 「関連付けられたドメイン構成」次のページ
- 「Android ファイル転送構成」ページ884
- 「Apple TVの構成」ページ890
- 「AirPlay構成」ページ760
- 「AirPlayミラーリング」ページ891
- 「ブラウザの設定」ページ894
- 「iOSのSingle Appモードの構成」ページ902
- 「iOS MDMプロファイルの構成」ページ905
- 「macOS MDM プロファイルの構成」ページ907
- 「コンテンツキャッシュ」ページ909
- 「Androidショートカットの作成」ページ914
- 「 デバイス名設定」ページ915
- 「イーサネット構成 (macOS) 」ページ917
- 「EMAサーバー統合構成」ページ921
- 「デバイスの壁紙構成」ページ922
- 「ロック画面メッセージ構成」ページ926
- 「スクリーンセーバー構成の作成」ページ928
- 「ユーザーのスクリーンセーバーの構成」ページ929
- 「macOSシステム拡張の構成」ページ931

- 「MAM のみ 」ページ932
- 「マネージドGoogle Play構 成 」ページ933
- 「プリンター設 定 」ページ936
- 「ブロートウェア削 除 構 成 」ページ941
- 「Samsungフォンの制 約 構 成 」ページ942
- 「Single Appモード構 成 」ページ944
- 「スタートメニューとタスクバー」ページ948
- 「システム更 新 構 成 」ページ951
- 「Windows 10の更 新 管 理 」ページ958
- 「Windowsアプリスケジューリング」ページ961
- 「Windows BIOS構 成 」ページ962
- 「Windows BitLocker」ページ975
- 「Windowsキオスク構 成 」ページ976
- 「Windowsライセンス構 成 」ページ985
- 「ソフトウェア更 新 の推 奨 頻 度 の構 成 」ページ986

関 連 付 けられたドメイン構 成

ライセンス: Gold

関 連 付 けられたドメイン構 成 は、アプリを関 連 付 けられたドメインにマッピングするディクショナリです。 関 連 付 けられたドメインは、拡 張 可 能 アプリSSO、ユニバーサルリンク、パスワード自 動 入 力 などの機 能 とともに使 用 できます。

関 連 付 けられたドメイン設 定 は次 のとおりです。

設定	操作内容
名前	この構成を識別する名前に入力します。
アプリケーション識別子	(必須)ドメインを関連付けるアプリID。
関連ドメイン	(必須)アプリに関連付けられるドメイン。各文字列の形式は「service:domain」です。ドメインは www.example.com のような完全修飾ホスト名にしてください。
直接ダウンロードを有効にする	オンにすると、このドメインのデータが、CDN経由ではなく、直接ダウンロードされます。このドメインのエンタイトルメント値は service:domain?mode=managed に設定する必要があります。そうでない場合、この値は無視されます。macOS 11以降で使用可能。 **デフォルト:** False

Android ファイル転送構成

Googleでは、Android 11の一部として、デバイス上でのアプリからのストレージアクセスについて大幅な変更を行いましたが、これは企業がデバイス上の特定のアプリへのファイル送信をどのように管理するか、という点にも影響を及ぼしました。これらの変更を考慮し、多くの大企業では、デバイスがAndroid 11以降にアップグレードする際にデバイスやアプリにファイルを配布することの課題に直面しています。ハードウェアベンダ製の特定のAPIに依存するアプローチを取る企業にとって、メーカーやOSバージョンの異なるさまざまなデバイスに対して同じ取り組み方をすることには、制限があります。

Ivantiでは、Androidのバージョンやハードウェアベンダに依存しないファイル転送ソリューションを開発しました。このソリューションは、Androidの標準の*コンテンツプロバイダ*機能に依存します。*コンテンツプロバイダ*を使用することでIvantiのGoアプリは、UEM経由でプッシュされるファイルごとに、デバイス上の一意の場所を生成できます。

このファイル転送構成は、「完全に管理されたデバイス」モードのAndroidデバイスで利用できます。この構成を使用することで管理者は、同一デバイス上に存在する許可されたさまざまなアプリ間で共有される、デバイス上のファイルを転送するためのオプションを提供できます。他のアプリは、どのような理由にもそれらのファイルを使用できます。使用例としては、JavaScriptを使用したアプリ構成の初期化、あるいはPDFや動画を使用した会社情報の表示があります。Ivantiのファイル転送構成にアップロードされたファイルはどれも、Ivanti Goが対応するconfigや関連付けられたファイルを受信したときにIvanti Goによってダウンロードされます。ファイルはIvanti Go内に安全に保存されます。

他のアプリは自由にこのファイルにアクセスすることはできません。

アプリサンドボックス内のダウンロードされたファイルはどれも、*ContentURI*または*URI*とも呼ばれる一意の場所によって参照されます。カスタム属性は、デバイス上のすべてのファイルのContentURI値をサーバーに保持するために使用されるものであり、管理者がデバイス上のファイルの可用性を判定する際や、動的デバイスグループを形成する際に役立つものであり、マネージドアプリ構成を使用してターゲットアプリにContentURIを伝達する際には必須となるものです。

Ivanti以外のアプリについては、管理者はサードパーティアプリ開発者にこのアプローチのサポート状況(一般に「消費側のFileProviderベースのContentURI」と呼ばれます)を確認する必要があります。

前提条件:

- ファイル転送操作に使用される新しいデバイスベースのカスタム属性を追加します。ファイル転送操作ごとに、一意のカスタム属性を作成する必要があります。各カスタムデバイス属性には、デバイスからのcontentURI(ファイルの場所)を、configあたり1ファイルのみ保存できます。

手順

1. **[構成]** > **[構成を追加]** > **[ファイル転送]** を開きます。**[ファイル転送構成を作成]** ページが開きます。
2. **[名前]** ボックスに構成の名前を入力します。
3. 構成の **[説明]** を入力します。

   構成設定

4. **[転送するファイル]** セクションで、ドラッグアンドドロップオプションを使用するか、**[ファイルを選択]** オプションを使って参照して、転送するファイルを選択します。デフォルトでは、ファイルサイズの上限は50 MBです。
5. 次の **[デバイスへのダウンロード]** オプションを1つ以上選択します(任意)。
   - **従量制ネットワークでのダウンロードを許可** - 選択すると、従量制ネットワークでもファイルのダウンロードを続行します。
   - **電源に接続が必要** - 選択すると、ファイル転送処理中にデバイスが電源に接続していることを確認します。
   - **デバイスのアイドル状態が必要** - 選択すると、ファイル転送処理中にデバイスをアイドル状態にします。
6. 次の2つのオプションのうち1つを使用して、ファイルを他のアプリと共有します。
   - **Android管理対象アプリ構成を使用して転送** - このオプションは、ターゲットアプリが自身の管理対象アプリ構成を使用してコンテンツURIを消費できる場合にのみ使用します。

- **デバイス上のインテントを使用して転送** - インテントはアプリ固有です。このオプションを使用してファイルを共有するには、ターゲットアプリのドキュメンテーションを参照して、下のインテントセクションに情報を入力します。インテントを使用すると、ファイルをアプリと共有できるようになった時点でIvanti Goアプリがデバイス上でメッセージをブロードキャストできるようになります。

Android管理対象アプリ構成を使用して転送

手順

1. **[デバイスベースの既存のカスタム属性を選択して、このファイルを他のアプリと共有]** フィールドに、既存の属性名(例:**カスタム-ファイル名**)を入力します。詳細については、「デバイスへのカスタム属性の割り当て」ページ274を参照してください。

   カスタム属性の名前は、このファイル転送操作のためだけに使用する、新しい、一意の属性でなければなりません。各カスタムデバイス属性には、デバイスからのcontentURI(ファイルの場所)を、configあたり1ファイルのみ保存できます。

2. **次のアプリ名またはパッケージ名またはその両方にアクセスできるようにする:** アプリ名は[アプリ名]セレクタから選択し、[パッケージ名]は追加できます。

   これらは、ファイルへのアクセスが許可される唯一の認証済みパッケージとなります。

   - **アプリ名** - [アプリ名]セレクタからアプリ名を選択できます。
   - **パッケージ名** - この領域にバンドルIDを入力できます。例:
     ```
     com.mobileiron.filetransfer.android3
     ```
     複数のパッケージ名を入力する場合は、セミコロン(;)で区切ります。

3. **[保存]** をクリックします。[構成]ページに新しいファイル転送構成が表示されます。

ターゲットアプリの構成

手順

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. ファイルを受信するターゲットアプリを選択します。
3. **[アプリ構成]** > **[Android用マネージド構成]** に移動します。
4. 新しい構成を作成するか、既存の構成を使用します。

アプリには、「マニフェスト情報」またはその他のプロパティなどの設定が含まれている場合があり、管理者はその設定を使用して、置換変数を定義することや、ファイルの場所をターゲットアプリに伝達することができます。たとえばIvanti Velocityアプリの場合は、[アプリ構成]ダイアログボックス > **[フェッチ構成]** > **[マニフェスト情報]** フィールドに置換変数を入力します。例：$Custom-File-Name$

5. 配布を選択します。

6. **[保存]** をクリックします。

デバイス上のインテントを使用して転送

手順

1. **[ファイルパスをインテント「エクストラ」に渡すための既存のデバイス属性を選択する]** フィールドに、新しいカスタム属性名（例：deviceIntentURI）を入力します。

   カスタム属性は、あらゆるデバイスに関して場所（URI / ContentURI）値をサーバーに保持するために使用されるものであり、管理者がデバイス上のファイルの可用性を判定する際に役立ちます。詳細については、「デバイスへのカスタム属性の割り当て」ページ274を参照してください。

2. **[特定のアプリ名またはパッケージ名にアクセスできるようにする]** フィールドに、**[アプリ名]** または **[パッケージ名]** を入力します。例：Velocity

   これらは、ファイルへのアクセスが許可される唯一の認証済みパッケージとなります。

3. [インテント-標準] セクションに、次の詳細を入力します。

   - **演算タイプ** - ドロップダウンリストから、**アクティビティの開始** / **サービスの開始** またはその他の同様の選択肢を、アプリに応じて選択します。ターゲットアプリの開発者の説明に応じて、またはターゲットアプリのドキュメンテーションを参照して、このフィールドに適した正しい値を選択します。

   - **クラス名**（任意）- ターゲットアプリの開発者の説明に応じて、またはターゲットアプリのドキュメンテーションを参照して、このフィールドに適した正しい値を選択します。

   - **アクション** - アクションを次の値に設定します。

     ```
     com.wavelink.nameofapp.action.INSTALL_CONFIG
     ```

     または同様の、アプリに応じた値に設定します。

   - **カテゴリ** - セミコロン(;) 区切りの値を入力します。

- **MIMEの種類**(任意) - 管理者のホストサーバーでは、custom.mobileconfigファイルを、アプリケーション/構成のMIMEの種類とともに設定する必要があります。これにより、デバイスのMDMプロファイルがダウンロードされ、デバイスにインストールされます。ターゲットアプリの開発者の説明に応じて、またはターゲットアプリのドキュメンテーションを参照して、このフィールドに適した正しい値を選択します。
- **フラグ**(任意) - 使用するフラグの数を選択します。ターゲットアプリの開発者の説明に応じて、このフィールドに適した正しい値を選択します。

4. KEY、TYPE、VALUE(任意)の下で**[インテント - 追加]**値を指定します。その他の特定のパラメータについては、OEMアプリのドキュメンテーションを参照してください。ターゲットアプリの開発者の説明に応じて、またはターゲットアプリのドキュメンテーションを参照して、このフィールドに適した正しい値を選択します。
5. **[保存]**をクリックします。
6. [構成]ページで、この新しいファイル転送構成を選択した後、**[アクション]** > **[ラベルに適用]**を選択します。**[ラベルに適用]**ダイアログボックスが開きます。
7. 適したラベルを選択し、**[適用]**をクリックします。

   ファイルの転送/他のアプリとの共有は、ターゲットアプリからのログ、またはデバイスからのログを収集することによってのみ検証できます。

ファイルのダウンロードステータスの検証

カスタム属性は、各デバイス上のあらゆるファイルの場所(ContentURI)値をサーバーに保持するために使用されるものであり、管理者がデバイス上のファイルの可用性を判定する際に役立ちます。

手順

1. **[デバイス]** > **[デバイス]**を開きます。
2. ファイル転送構成の配布先であった特定のデバイスを選択します。
3. [デバイスの詳細]ページで、デバイスを選択した後、**[アクション]** > **[デバイスのチェックインを強制]**を選択します。
4. [構成]タブの下に、ファイル転送構成が**[適用済み]**というステータスで表示されていることを確認します。
5. [カスタム属性]タブの下で、新しいカスタム属性の名前(例:「Custom-File-Name$」)がその関連値とともに表示されていることを確認します。これにより、デバイス上のファイルのストレージ場所に関する情報が提供され、ファイルがデバイスにローカルにダウンロードされ、Ivanti Goアプリサンドボックス内で利用できることが示されます。

ファイルの転送 / 他のアプリとの共有は、ターゲットアプリからのログ、またはデバイスからのログを収集することによってのみ検証できます。

Apple TVの構成

ライセンス: Silver

Apple TVの構成により、Apple TVの言語とロケールが定義されます。

Apple TVの設定は以下のとおりです。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
言語	UIの言語を指定する2文字の言語コードを入力します。
ロケール	そのUIの国と言語の組み合わせを指定するロケールIDを入力します。

詳細は構成を作成するにはを参照してください。

AirPlayミラーリング

ライセンス: Gold

AirPlayミラーリングとは、Apple TVを使用しているモニター上にiOSデバイスの画面を表示できる機能です。Apple TVとiOSデバイスは、同じWi-Fiネットワークに接続する必要があります。この機能には以下のデバイスが必要です。

- iOS 7以降のデバイス - 監視対象
- macOS 10.10以降のデバイス - 監視対象
- Apple TVのバージョン - 監視対象
- AirPlay

非iOSデバイスの管理を可能にする変更は元に戻せません。

このセクションは以下のトピックを含みます。

- Apple AirPlayの構成
- モバイルデバイスでのAirPlayの設定
- Apple TVと連動するモニターの設定
- iOSデバイスとApple TVの接続

Apple AirPlayの構成

AirPlay構成設定の詳細については、AirPlay構成をご覧ください。

手順

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[AirPlay]** をクリックします。
4. 該当するフィールドに構成の名前と説明を入力します。
5. 対応するすべてiOSバージョンについて、デバイス名とパスワードを入力します。
6. 必要に応じて **[+追加]** をクリックし、別のデバイスを追加します。

7. 任意で、監視対象iOS 7以降のデバイスまたはmacOS 10.10以降に関してはデバイスIDを許可リストに追加します。
8. **[次へ]** をクリックします。
9. 配布レベルを選択します。
10. **[完了]** をクリックします。

モバイルデバイスでのAirPlayの設定

手順

1. Apple Configuratorを設定します。
2. **[デバイス]** > **[デバイス]** を開きます。
3. そのデバイスの [詳細] ページに表示するiOSデバイスの名前をクリックします。
4. アイコンをクリックします。
5. **[AirPlayミラーリング]** を選択し、AirPlayミラーリングダイアログを表示します。
6. プルダウンメニューからApple TVデバイスを選択します。
7. スキャン時間を秒数で入力し、選択したデバイスを検索する制限時間を指定します。
8. Apple TVデバイスのパスワードを入力します。
9. **[リクエストを送信]** をクリックします。

Apple TVと連動するモニターの設定

手順

1. Apple TVに接続されたモニター上で、**[設定]** > **[プロファイル]** を開きます。
2. **[Ivanti Neurons for MDM Apple Configurator]** を選択します。
3. **[プロファイルを追加]** をクリックします。
4. アイコンをクリックします。
5. **[AirPlayミラーリング]** を選択し、AirPlayミラーリングダイアログを表示します。

6. プルダウンメニューからApple TVデバイスを選択します。
7. スキャン時間を秒数で入力し、選択したデバイスを検索する制限時間を指定します。
8. Apple TVデバイスのパスワードを入力します。
9. **[リクエストを送信]** をクリックします。

iOSデバイスとApple TVの接続

手順

1. Apple TVデバイスをモニターに接続します。
2. Apple TVリモートを使用して、**[設定]** > **[アカウント]** > **[ホームシェアリング]** を開き、ホームシェアリングをオンにします。
3. **iOSデバイス**を、**AppleTVデバイス**と同じWi-Fiネットワークに接続します。
4. **iOS**デバイス上でリモートアプリを開きます。
5. **[リモート設定]** 画面から **[ホームシェアリング]** を有効化します。

ブラウザの設定

ブラウザ設定では、Windows 10デバイスでGoogle Chrome、Mozilla Firefox、Microsoft Edge、Internet Explorerの設定や制限を構成できます。

これにはBridgeが必要です。詳細は「Ivanti Bridge」 ページ410をご覧ください。

ブラウザ設定を適用する前に、ブラウザがデバイスにインストールされていることを確認してください。

ブラウザ設定を構成するには:

1. **[構成] > [+追加]** を開きます。
2. **[ブラウザ設定]** 構成を選択します。
3. 構成の名前を入力します。

4. 説明を入力します。

5. [構成設定] セクションで、次の表に記載されているように残りの設定を指定します。

設定	操作内容
ブラウザ	設定が必要なブラウザタイプを選択します。 • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**

ブラウザ設定	次のオプションを設定します。 **ブラウザを許可：** • **パスワードの保存を許可** • **セーフブラウジングモードを許可** • **古いプラグインをブラウザに残すことを許可** **ChromeとFirefox：** • **ブラウザ履歴の削除を許可** **ChromeとInternet Explorer：** • **ブラウザの印刷を許可** • **新規タブページURL** **Chromeのみ：** • **ブックマークバーにアプリショートカットを表示** • **ホームボタンを表示** • **Googleとのデータ同期を許可** • **Chromeを閉じてもバックグラウンドアプリの実行を継続** **Firefoxのみ：** • **拡張機能のインストールを許可** **nternet Explorerのみ：** • **Webサイトからのデータダウンロードを許可**

ブラウザのお気に入り	**[+追加]** をクリックします。 **[ブラウザのお気に入りを追加]** ウィンドウが表示されます。次のフィールドを設定してください。 • **表示名**：お気に入りの表示名を入力します。 • **URL**：ブラウザのお気に入りのURLを入力します。 **[追加]** をクリックします。 追加したブラウザのお気に入りの詳細情報がページに表示されます。設定を編集するには、**[アクション]** カラムの編集アイコンをクリックします。ブラウザのお気に入りを削除するには、削除アイコンをクリックします。 **ブラウザのお気に入りフォルダー名**：お気に入りのリストを表示するブラウザのお気に入りフォルダー名を入力します。 ブラウザのお気に入りはCSV形式でも追加できます。CSVファイルをアップロードするには： a. [CSVファイルをアップロード] をクリックします。アップロードするCSVファイルをブラウズして選択します。 b. **[アップロード]** をクリックします。 CSVファイル内の詳細情報は以下の形式で追加します。 • 最初のカラム(表示名)にはお気に入りの表示名を指定します。例：ショッピング • 2番目のカラム(URL)にはお気に入りのURLを指定します。例：https://amazon.com

Webサイトセキュリティ	以下のWebサイトセキュリティ設定を構成します: **すべてのWebサイト(ChromeとFirefox)** • **Cookieをブロック** • **Javascriptをブロック** • **プラグインをブロック** • **ポップアップをブロック** 特定のWebサイト(Chromeのみ) **ブロックリストに入れるWebサイト(ChromeとEdge)**:ブロックリストに入れるWebサイトを追加します。 **[+追加]**をクリックします。**[ブロックリストのWebサイトを追加]**ウィンドウが表示されます。 **[WebサイトのURL]**に、ブロックリストに入れるWebサイトのURLを入力します。 **[アクセス]**フィールドで、**[ブロック]**を選択するとWebサイトがブロックリストに入ります。デフォルトのオプションは**[許可]**です。 **[追加]**をクリックします。

ブラウザ拡張機能	**許可された拡張機能タイプ(Chromeのみ)**：次のいずれかのオプションを選択します。 • **拡張機能** • **ユーザースクリプト** • **テーマ** • **パッケージ型アプリ** • **ホスト型アプリ** • **プラットフォームアプリ** **ブラウザ拡張機能ソース(Chromeのみ)**： ブラウザ拡張機能ソースを追加するには **[+追加]** をクリックします。ブラウザ拡張機能ソースを追加した後は、**[アクション]** カラムで必要なオプションをクリックすることにより、ソースを編集または削除できます。 **強制インストール拡張機能(Chromeのみ)**： 拡張機能を強制インストールするには **[+追加]** をクリックします。 強制インストール拡張機能を追加した後は、**[アクション]** カラムで必要なオプションをクリックすることにより、ソースを編集または削除できます。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

iOSのSingle Appモードの構成

ライセンス: Silver

Single Appモードは、iOSデバイスを指定されたアプリのみの利用に制限します。たとえば、組織が開発したカスタムアプリしか利用できないようデバイスを設定することができます。

手順

1. **[構成] > [Single Appモード]** を選択します。
2. 次のガイドラインに従ってアプリおよびその他の設定を定義します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
アプリを選択	アプリの選択方法を選びます。 • アプリカタログおよびシステムアプリから：Ivanti Neurons for MDM アプリカタログとシステムアプリ(Appleデバイスのデフォルトでインストール済み) から検索する場合に選択します。 • アプリの名前を入力し、アプリリストに表示されたら選択します。 • **バンドルIDを入力：**選択したいシステムアプリの固有識別子を入力する場合に選択します。このオプションは、**[アプリカタログおよびシステムアプリから]** オプションでシステムアプリが見つからない場合に使用してください。
タッチを無効にする	タッチスクリーンを無効にする場合に選択します。
デバイスローテーションを無効化	デバイスローテーションの感知を無効にする場合に選択します。
音量ボタンを無効化	デバイスの音量ボタンを無効にする場合に選択します。
通知音を無効化	デバイスの通知音を無効にする場合に選択します。
スリープ/スリープ解除ボタンの無効化	デバイスのスリープ/スリープ解除ボタン(デバイスの枠の右上) を無効にする場合に選択します。
自動ロックを無効化	操作しないままの状態の後でもスリープにならないようにする場合に選択します。
VoiceOverの有効化	VoiceOver画面リーダーを有効にする場合に選択します(アクセシビリティ機能) 。
ズーム機能を有効にする	ズーム機能を有効にする場合に選択します(アクセシビリティ機能) 。

色の反転を有効化	色の反転調整を有効にする場合に選択します(アクセシビリティ機能)。
Assistive Touchを有効にする	Assistive Touchを有効にする場合に選択します(アクセシビリティ機能)。
選択項目の読み上げを有効化	選択項目の読み上げを有効にする場合に選択します(アクセシビリティ機能)。
モノラルオーディオを有効化	ステレオとモノラルのオーディオ切り替えを有効にする場合に選択します(アクセシビリティ機能)。
VoiceOverの調整	デバイスがVoiceOverの調整を行えるようにする場合に選択します。
ズーム機能の調整	デバイスユーザーがズーム機能の調整を行えるようにする場合に選択します。
色の反転の調整	デバイスユーザーが色の反転の調整を行えるようにする場合に選択します。
Assistive Touchの調整	デバイスユーザーがAssistive Touchの調整を行えるようにする場合に選択します。

3. **[次へ]** をクリックします。
4. **[配布]** 画面で、この構成を受信するデバイスグループを選択します。
5. **[完了]** をクリックします。

使用するアプリとしてダイヤラーを構成した場合は、デバイスがSingle Appモードになったときにホームボタンが機能します。

iOS MDMプロファイルの構成

iOS MDM構成は、Ivanti Neurons for MDM のアクセス制限を定義します。iOS MDM構成には2種類あります。

- **iOS MDM - 一括プロビジョニング:** 企業が購入し、大量配布の一環としてプロビジョニングしたデバイスに使用します。
- **iOS MDM - 個別プロビジョニング:** 1台ずつプロビジョニングしたデバイスに使用します。監視対象およびユーザー登録デバイスには適用されません。

すべてのスペースにいずれか1種類が提供され、許可されます。

iOS MDM構成の編集

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** に進みます。
3. 編集したいiOS MDM構成を選択します。
4. 構成を編集するには、鉛筆 (編集) アイコンをクリックします。

5. 以下のガイドラインを使用して変更します。

設定	操作内容
MDMアクセス権	
デバイスロックとパスコード削除を許可	チェックを外した場合、パスコードコンプライアンス構成を強制できません。
デバイス消去を許可	チェックを外した場合、デバイスワイプを強制できません。
ネットワーク情報(電話/SIM番号、MACアドレス)のクエリーを許可	チェックを外した場合、デバイスがネットワーク情報レポートから除外されます。 このオプションのチェックを外した場合、デバイスリスト画面とデバイス詳細画面で、報告されなくなったネットワーク情報に[N/A]が表示されます。また、対象となるデバイスにローミングポリシーを強制できなくなります。
プロファイル削除パスワード	
プロファイルを削除するためのパスワード	パスワードを指定します。デバイスからプロファイルを削除するときには、パスワードを入力するように指示されます。
必須アプリを追加(iOS 15+)	
ルックアップで追加	アプリ名を入力し、App Storeでアプリを検索して必須アプリを選択します。 追加できるアプリは1回に1つです。1つのアプリを選択すると、他が無効化されます。
手動で追加	アプリのiTunes IDを入力します。

6. **[完了]**をクリックします。

変更は、変更を行った後にプロビジョニングされるデバイスにのみ適用されます。

macOS MDM プロファイルの構成

macOS MDM構成により、Ivanti Neurons for MDMのアクセス制限を定義します。macOS MDM構成は、1台ずつプロビジョニングしたデバイスに対して個別にプロビジョニングされます。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** に進みます。
3. 編集したいmacOS MDM構成を選択します。
4. 構成を編集するには、鉛筆 (編集) アイコンをクリックします。
5. 以下のガイドラインを使用して変更します。

設定	操作内容
デバイスロックとパスコード削除を許可	チェックを外した場合、パスコードコンプライアンス構成を強制できません。
デバイス消去を許可	チェックを外した場合、デバイスワイプを強制できません。
ネットワーク情報 (電話/SIM番号、MACアドレス) のクエリーを許可	チェックを外した場合、デバイスがネットワーク情報レポートから除外されます。 このオプションのチェックを外した場合、デバイスリスト画面とデバイス詳細画面で、報告されなくなったネットワーク情報に [N/A] が表示されます。また、対象となるデバイスにローミングポリシーを強制できなくなります。
プロファイル削除パスワード	
プロファイルを削除するためのパスワード	パスワードを指定します。デバイスからプロファイルを削除するときには、パスワードを入力するように指示されます。

6. **[完了]** をクリックします。

   変更は、変更を行った後にプロビジョニングされるデバイスにのみ適用されます。

コンテンツキャッシュ

ライセンス: Gold

対象: macOS 10.13.4またはサポートされる以降のバージョン。

コンテンツキャッシュサービスの構成により、App Storeソフトウェアのローカルコピーを有効化し、連携したクライアントがソフトウェアやアプリを短時間でダウンロードできるようにします。

コンテンツキャッシュ構成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[キャッシュ]** と入力し、**[コンテンツキャッシュ]** 構成をクリックします。
4. 名前と構成の説明を入力します。
5. コンテンツキャッシュ構成の設定を入力します。
6. **[次へ]** をクリックします。
7. **[この構成を有効化]** オプションを選択します。
8. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
9. **[完了]** をクリックします。

コンテンツキャッシュ構成の設定

次の表の設定を使用してコンテンツキャッシュを構成します。設定の詳細はAppleドキュメンテーションを参照してください。

設定	説明
システムによるキャッシュコンテンツの自動パージを許可 (macOS 10.15またはサポートされる以降のバージョン)	他のアプリケーションでディスク領域が必要なときに自動的にキャッシュからコンテンツを消去できます(例:コンピュータで空きディスク領域が低下しているとき)。 デフォルトでは有効化されています。
個人キャッシュを許可	ユーザーのiCloudデータをキャッシュします。クライアントがこの設定の変更を反映するには時間(数時間から数日)がかかる場合があります。すぐには影響が見られません。 デフォルトでは有効化されています。
共有キャッシュを許可	アプリやソフトウェアの更新などiCloud以外のコンテンツをキャッシュします。クライアントがこの設定の変更を反映するには時間(数時間から数日)がかかる場合があります。すぐには影響が見られません。 デフォルトでは有効化されています。
コンテンツキャッシュの自動有効化を許可	可能な限り自動的にコンテンツキャッシュを有効化し、無効化を防ぎます。
自動有効化有線キャッシュを許可 (macOS 10.15.4またはサポートされる以降のバージョン)	可能な限りインターネット接続共有を自動的に有効化し、インターネット接続共有の無効化を防ぎます。
有線キャッシュを禁止	有線キャッシュを禁止します。[有線キャッシュを禁止]オプションは[有線キャッシュの自動有効化を許可]より優先されます。
キャッシュ制限	コンテンツキャッシュに使用されるディスクスペースの最大バイト数。0はディスクスペースを無限に使用することを意味します。 デフォルト値は0です。

設定	説明
データパス	キャッシュしたコンテンツを保存するディレクトリへのパス。この設定を手動で変更しても、キャッシュしたコンテンツが古い場所から新しい場所に自動的に移動するわけではありません。コンテンツを自動的に移動するには、コンテンツキャッシュ画面の共有設定を使用します。 値は/Library/Application Support/Apple/AssetCache/Dataである(または終了する)必要があります。
ディスプレイアラートを許可 (macOS 10.15またはサポートされる以降のバージョン)	コンテンツキャッシュは例外的な条件(アラート)をシステム通知として画面の上角に表示します。
デバイスをアウェイク状態に維持 (macOS 10.15またはサポートされる以降のバージョン)	コンテンツキャッシュがオンである限りコンピューターがスリープ状態になるのを防ぎます([システム環境設定] > [共有] > [コンテンツキャッシュがオン])。
リスン範囲	対処するクライアントIPアドレス範囲を説明する辞書群。
最初のIPアドレス	リスン範囲にあるクライアントの最初のIPアドレス。
最後のIPアドレス	リスン範囲にあるクライアントの最後のIPアドレス。
IPアドレスの種類	以下のオプションから1つ選択してください: • IPv4(デフォルト) • IPv6
リスン範囲のみ許可	コンテンツキャッシュはリスン範囲にあるクライアントにのみコンテンツを提供します。
ピアおよびペアレントとのリスンを許可	コンテンツキャッシュはリスン範囲、ピアリスン範囲、ペアレントの和集合にあるクライアントにコンテンツを提供します。 デフォルトでは有効化されています。

設定	説明
ローカルサブネットのみ許可	コンテンツキャッシュは同じイミディエートローカルネットワークにあるクライアントにのみコンテンツを提供します。コンテンツキャッシュが到達可能でも他のネットワーク上のクライアントにはコンテンツが提供されません。このオプションがオンの場合、リスン範囲は無視されます。 デフォルトでは有効化されています。
クライアントIDをログ	コンテンツキャッシュはコンテンツを要求するクライアントのIPアドレスとポート番号を記録します。
ペアレント選択ポリシー	以下のポリシーオプションから1つ選択します。 • 最初に利用可能 • URLパスハッシュ • ラウンドロビン(デフォルト) • ランダム • 利用可能なスティッキー
ペアレント	Appleからの直接ダウンロードまたはAppleへの直接アップロードではなく、このキャッシュのダウンロード元またはアップロード先となる他のコンテンツキャッシュのローカルIPアドレス群。 **[+追加]** をクリックして1つまたは複数のIPアドレスを追加します。
ピアローカルサブネットのみ許可	コンテンツキャッシュは、同じイミディエートローカルネットワーク上の他のコンテンツキャッシュとのみピアリングします。デバイスと同じパブリックIPアドレスを使用するコンテンツキャッシュではありません。 デフォルトでは有効化されています。
ポート	コンテンツキャッシュがアップロードやダウンロードの要求に応えるTCPポート番号。空いているポートをランダムに選択する場合はポートを0に設定します。 デフォルト値は0です。
パブリック範囲	Ivanti Neurons for MDM サーバーがクライアントとコンテンツキャッシュのマッチングに使用するパブリックIPアドレス範囲を説明した辞書群。

設定	説明
最初のIPアドレス	パブリック範囲にあるサーバーの最初のIPアドレス。
最後のIPアドレス	パブリック範囲にあるサーバーの最後のIPアドレス。
IPアドレスの種類	以下のオプションから1つ選択してください： • IPv4(デフォルト) • IPv6

詳細は構成を作成するにはを参照してください。

Androidショートカットの作成

ショートカットは、許可リストに含まれるブラウザを使用するキオスクモードでのみ利用可能です。ブラウザは、ロックダウン& キオスク

構成で許可リストに含まれている必要があります。ショートカットはIvanti Neurons for MDMキオスクランチャーに表示されます。

手順

1. **[構成]** に進みます。> **[+追加]** を開きます。
2. **[Androidショートカット]** をクリックして **[Androidのショートカット構成の作成]** ページを表示します。
3. **[名前]** フィールドに構成の名前を入力します。
4. **[説明]** フィールドに構成の説明を入力します。
5. **[ラベル]** フィールドにショートカット用の一意のラベルを入力します。
6. **[URL]** フィールドにショートカットのターゲットのURLを入力します。
7. 任意で、アイコンフィールド内のファイルをドラッグ& ドロップするか、**[ファイルを選択]** をクリックして目的のファイルに移動することで、ショートカット用のアイコンを選択します。
8. **[次へ]** をクリックします。

デバイス名設定

ライセンス: Silver

既定のデバイス名構成により、登録または登録後レベルでデバイスにプッシュされる新しい構成を作成し、デバイスの名前を指定できます。管理者は、**監視された iOS 8デバイス**の既定のデバイス名のみを定義できます。デバイス名を作成するには、以下の変数を使用できます。

- デバイスのシリアルナンバー
- デバイスのIMEI
- デバイスモデル
- Ivanti Neurons for MDM ユーザー名 (ローカルユーザーのみ)
- LDAP組織ユニット(OU)
- LDAP共通名(CN)

たとえば、デバイスのシリアルナンバーから始まり、LDAPで定義された組織で終わるデバイス名は、${deviceSN}-${userOU}となります。

既定のデバイス名設定 (iOS)

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
デバイス名	使用可能なデバイスとLDAP属性を含め、デフォルトのデバイス名のフォーマットを入力します。* 最終的なデバイス名が63文字を超えると、デバイスに正しく表示されるように切り捨てられます。
説明	この構成の目的を明示する説明を入力します。

このフィールドに対応する変数がある場合に、そのリストを参照するには、$を入力してください。

デバイス名設定 (Android)

Android デバイス名は Go app で取得できます。管理者がデバイス詳細レポートを生成すると、デバイスモデルや製造元の名前ではなく、実際のデバイス名が表示されます。ユーザがデバイス名を変更した場合、次回レポートを生成するときに、新しい名前が表示されます。該当するデバイス名は、**[デバイス]** > **[設定]** > **[デバイス名]** に表示されます。

イーサネット構成 (macOS)

ライセンス: Gold

対象: macOS 10.13+またはサポートされる以降のバージョン。

管理者は各種のイーサネットインターフェイスを構成できます イーサネットの構成に使用できるペイロードは以下のとおりです。

- グローバルイーサネット
- 第1アクティブイーサネット
- 第1イーサネット
- 第2アクティブイーサネット
- 第2イーサネット
- 第3アクティブイーサネット
- 第3イーサネット

イーサネットを構成するペイロードには、デフォルトフォールバックのグローバル、第1、第1アクティブ、第2、第2アクティブ、第3、第3アクティブイーサネットインターフェイスがあります。Appleには、第1、第1アクティブ、第2、第2アクティブ、第3、第3アクティブイーサネットインターフェイスのインストールに関して既知の問題があります。

イーサネット構成

手順

1. **[構成]** を選択します。
2. **[+追加]** をクリックします。
3. 検索フィールドに **[イーサネット]** と入力し、**[イーサネット]** 構成を選択します。
4. 名前と構成の説明を入力します。
5. ドロップダウンリストから構成設定を選択します。

6. イーサネット構成設定を入力します。
7. **[次へ]** をクリックします。
8. **[この構成を有効化]** オプションを選択します。
9. 以下のいずれかのチャネルオプションを選択し、構成を適用します。
   - デバイスチャネル(最も一般的)
   - ユーザーチャネル(現在の登録ユーザー)
10. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
11. **[完了]** をクリックします。

イーサネット構成設定

次の表の設定を使用してイーサネットを構成します。設定の詳細はAppleドキュメンテーションを参照してください。

設定	説明
プロトコル	
承認済みEAPタイプ	ネットワークへのアクセスに使用できるEAPの種類を選択します。 • TLS(トランスポートレイヤセキュリティ):TLSとは、インターネット上の2つのコンピューター間で暗号化されたセッションを確立するプロトコルです。これがサーバーを識別し、ハッカーによるデータの傍受を防ぎます。 • TTLS - **内部ID**フィールドでは、OSデフォルト、PAP、CHAP、MSCHAP、MSCHAPv2、EAPなどいずれかの認証プロトコルを選択します。 • PEAP • LEAP • EAP-SIM:**[RANDのEAP SIM番号]** フィールドでドロップダウンリストからRAND数を選択します。 • EAP-AKA

設定	説明
	• EAP-FAST：認証方法を定義するEAP-FASTオプションを選択します。 ◦ **PAC使用：**プロキシ自動構成（PAC）の使用を選択します。 ◦ **PACをプロビジョニング：**PACのプロビジョニングを許可する場合に選択します。選択しない場合、デバイス上ですでにプロビジョニングされているPACのみ使用することができます。このオプションは［PAC使用］を選択した場合にのみ利用可能です。 ◦ **匿名プロビジョンPAC：**サーバー認証なしでPACのプロビジョニングを許可する場合に選択します。このオプションは［PACのプロビジョニング］を選択した場合にのみ利用可能です。
認証	**ユーザー名：**ネットワークアクセスに必要なユーザー名を指定します。これを空欄にしておくと、デバイスユーザーに入力を求めるプロンプトが表示されます。 • 接続ごとのパスワードを使用：デバイスユーザーに対し、接続ごとにパスワードを求めるプロンプトを表示する場合に選択します。デバイスが同じネットワークに再接続される場合、デバイスユーザーにはネットワークへの接続の再認証を求めるプロンプトが表示されます。接続が初期化されるたびにパスワードが要求されます。 • ネットワークに接続する際にワンタイムパスワードの入力を指示：パスワードは構成がデバイスにプッシュされたときに1度だけ要求されます。ネットワークへの接続と切断のたびにパスワードが要求されることはありません。 **パスワード：**（任意）このネットワークにアクセスするためのパスワードを入力します。それ以外の場合、デバイスユーザーは、ネットワークにアクセスするために必要な何らかのパスワードをパスワードを入力するためのプロンプトが表示されます。 **外部ID：**（任意）TTLS、PEAP、およびEAP-FASTの場合、デバイスユーザーにIDを非表示にすることを許可する場合に選択します。ユーザーの実際の名前は暗号化されたトンネルの内側でのみ表示されます。このオプションにより、攻撃者にとっては認証中のユーザーの名前がプレーンテキストとしては見えないため、セキュリティが強化されます。 **システムモード認証情報ソースID：**コンピューター認証にはシステムモードが使用されます。システムモードを使用した認証はユーザーがコンピューターにログインする前に実行されます。システムモードは一般に、ローカル認証機関が発行するコンピューターのX.509認証（EAP-TLS）を使用した認証のために構成されます。
信頼性	**信頼性のある証明書：**チェックボックスを選択して、リストから複数の証明書を選択します。 **信頼性のあるサーバー証明書名：**証明書名を追加します。 • **信頼の例外を許可：**信頼性の決定をユーザーが（ダイアログボックスで）行えるようにします。

設定	説明
	• **TLS証明書を要求** **EAP認証で許可される最大TLSバージョン** **EAP認証で許可される最小TLSバージョン** **信頼性のあるTLS証明書：MobileIron Agent CA証明書**

詳細は構成を作成するにはを参照してください。

EMAサーバー統合構成

EMAサーバー統合構成では、Windows 10デバイスを構成済みのIntel EMAサーバーにリンクできます。構成済みIntel EMAサーバーにデバイスをリンクするには、元のEMAエージェントのインストールディレクトリを提供し、新しいEMAサーバーからEMAエージェントの.mshファイルをアップロードする必要があります。

これにはBridgeが必要です。詳細はBridgeをご覧ください。

手順

1. **[構成]** > **[+追加]** を開きます。
2. **[EMAサーバー統合]** 構成を選択します。
3. 構成の名前を入力します。
4. [構成設定] セクションで **[ファイルを選択]** をクリックし、EMAエージェントの.mshファイルを選択します。

   .mshファイルは、EMAサーバーからダウンロードできるEMエージェントポリシーファイルです。

5. 元の **[EMAエージェントインストールディレクトリ]** フィールドに、元のEmaAgent.exeファイルがインストールされた場所を入力します。
6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

デバイスの壁紙構成

ライセンス：Silver

デバイスの壁紙構成は、デバイス所有者モードのAndroid 7.0デバイス、または会社所有の個人対応 (COPE) デバイス (Android 11 EPO モードデバイスを除く) のホーム画面とロック画面のデフォルトの壁紙画像を決定します。デバイスのユーザーは、デバイスに配布された壁紙を自由に変更できます([設定] > [壁紙 & 明るさ]) 。

Android壁紙設定

Androidデバイスのデフォルト壁紙画像を定義するには：

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[デバイスの壁紙]** をクリックします。
4. Androidアイコンをクリックし、Androidの構成設定セクションを表示した後、次のように設定します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
Androidの壁紙をアップロード	
ホーム画面およびロック画面に同じ画像を使用	両方の画面用に1枚の画像をアップロードする場合に選択します。
ホーム画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。
ロック画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。

5. **[次へ]** をクリックします。

6. 以下の配布オプションから1つ選択します。
   - **すべてのデバイス**
   - **デバイスなし**(デフォルト)
   - **カスタム**
7. **[完了]** をクリックします。

> アップロードする画像は.jpgまたは.png形式とします。

iOS壁紙設定

iOSデバイス用のデフォルトの壁紙画像を定義できます。

> この設定は、監視対象デバイスにのみ適用されます。

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[デバイスの壁紙]** をクリックします。

4. iOSアイコンをクリックし、iOSの構成設定セクションを表示した後、次のように設定します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
iPhoneの壁紙をアップロード	
ホーム画面およびロック画面に同じ画像を使用	iPhone用に1枚の画像をアップロードすることを選択します。
ホーム画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。
ロック画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。
iPadの壁紙をアップロード	
ホーム画面およびロック画面に同じ画像を使用	iPad用に1枚の画像をアップロードすることを選択します。
ホーム画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。
ロック画面	画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。

5. **[次へ]** をクリックします。

6. 以下のオプションから1つ選択してください：
   - **すべてのデバイス**
   - **デバイスなし**（デフォルト）
   - **カスタム**
7. **[完了]** をクリックします。

> アップロードする画像は縦1164 x 横640の.jpgまたは.png形式とします。

macOS壁紙設定

macOSデバイスのデフォルト壁紙画像を定義するには：

1. **[構成]** に進みます。
2. **[+追加]** をクリックします。
3. **[デバイスの壁紙]** をクリックします。
4. macOSアイコンをクリックし、macOSの構成設定セクションを表示します。
5. デスクトップ画像へのパスを入力します。
6. **[次へ]** をクリックします。
7. 以下のオプションから1つ選択してください：
   - **すべてのデバイス**
   - **デバイスなし**（デフォルト）
   - **カスタム**
8. **[完了]** をクリックします。

> 壁紙は制約に基づいて変更できます。macOS制約構成 **[壁紙の変更を許可]** が有効になっていると、壁紙を変更できます。

詳細は構成を作成するにはを参照してください。

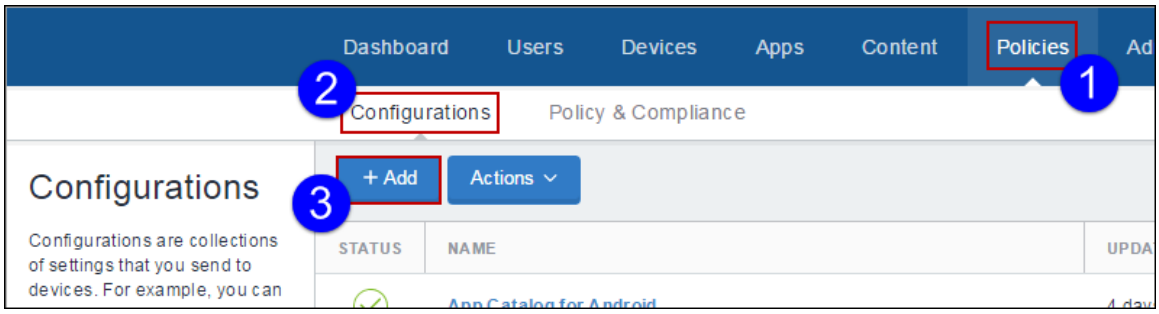
ロック画 面 メッセージ構 成

ログイン画 面 とロック画 面 にメッセージとアセットタグを表 示します。対 象 となるのは、iOS 9.3またはサポートされる以 降 のバージョンを搭 載した監 視 対 象 デバイスです。

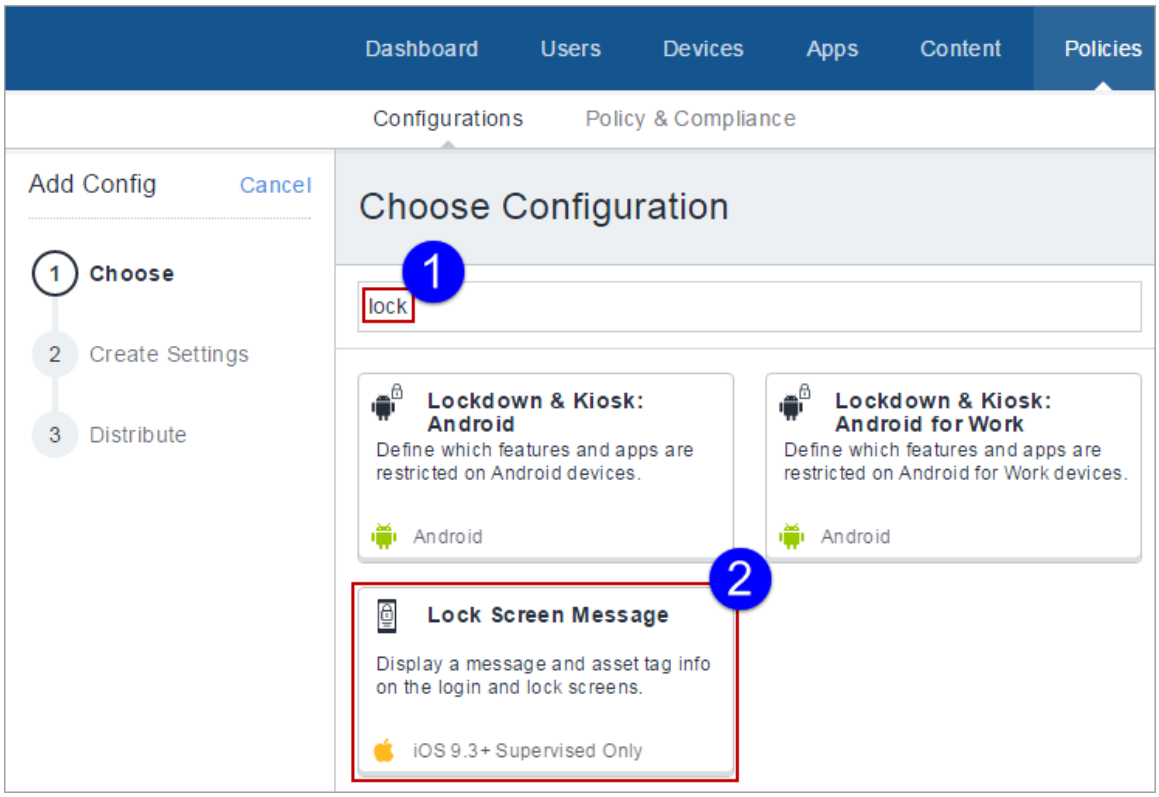
ロック画 面 メッセージ構 成 の作 成

手 順

1. **[構 成]** を選 択します。
2. **[+追 加]** をクリックします。



3. 検 索 フィールドに **[ロック]** と入 力し、**[ロック画 面 メッセージ]** 構 成 をクリックします:



ロック画面メッセージ構成の詳細ページが表示されます。

4. このページで設定を構成します。値の説明については、[ロック画面メッセージ構成の設定]セクションの表を参照してください。

5. **[次へ]** をクリックし、配布設定を構成した後、**[完了]** をクリックします。

ロック画面メッセージ構成の設定

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ロック画面の注釈	このテキストはログインウィンドウとロック画面に表示されます。
アセットタグ情報	このテキストはログインウィンドウとロック画面の最下部に表示されます。

詳細は構成を作成するにはを参照してください。

スクリーンセーバー構成の作成

スクリーンセーバー構成では、パスワード、アイドル時間、モジュールのパスと名前などのオプションを追加できます。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** をクリックします。
3. **[+追加]** をクリックします。
4. 検索フィールドで screen と入力し、**[スクリーンセーバー]** をクリックします。

   [スクリーンセーバーの作成] 構成の詳細ページが表示されます。
5. このページで設定を構成します。参考値は、「**スクリーンセーバー構成設定**」の表をご覧ください。
6. **[次へ]** をクリックし、配布設定を構成した後、**[完了]** をクリックします。

スクリーンセーバー構成設定

設定	操作内容
名前 (必須)	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
パスワード確認チェックボックス	チェックボックスをオンにすると、スクリーンセーバーを解除または停止するときに、デバイスユーザはパスワードを入力する必要があります。macOS 10.13 以降で使用可能。
パスワードの遅延を確認	遅延時間を秒で指定します。
ログイン ウィンドウ アイドル時間	スクリーンセーバーが起動するまでのアイドル時間を秒で指定します。
スクリーンセーバー モジュールへのパス	スクリーンセーバー モジュールのパスを指定します。
スクリーンセーバー モジュールの名前 (必須)	スクリーンセーバーの名前を入力します。

詳細は構成を作成するにはを参照してください。

ユーザーのスクリーンセーバーの構成

ユーザーのスクリーンセーバー構成では、パスワード、アイドル時間、モジュールのパスと名前などのオプションを追加できます。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[構成]** をクリックします。
3. **[+追加]** をクリックします。

4. 検索フィールドにscreenと入力し、**[ユーザのスクリーン セーバ]** をクリックします。

   [ユーザーのスクリーンセーバー構成の作成] 詳細ページが表示されます。

5. このページで設定を構成します。値の説明については、トピック「**ユーザーのスクリーンセーバー構成の設定**」の表をご参照ください。

6. **[次へ]** をクリックし、配布設定を構成した後、**[完了]** をクリックします。

ユーザーのスクリーンセーバー構成の設定

設定	**操作内容**
名前 (必須)	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
アイドル時間	スクリーンセーバーが起動するまでのアイドル時間を秒で指定します。
スクリーンセーバー モジュールへのパス	スクリーンセーバー モジュールのパスを指定します。
スクリーンセーバー モジュールの名前 (必須)	スクリーンセーバーの名前を入力します。

詳細は構成を作成するにはを参照してください。

macOSシステム拡張の構成

システム拡張の構成により、カーネルレベルのアクセスなしに、ドライバー拡張、ネットワーク拡張、エンドポイントセキュリティ拡張などの拡張タイプをインストール可能になります。

対象：macOS 10.15+

Procedure 手順

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[拡張]** と入力し、**[システム拡張]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. **[許可システム拡張]** で **[許可チーム識別子]** と **[許可システム拡張]** を **[+追加]** します。
5. **[許可システム拡張タイプ]** で **[許可チーム識別子]** と **[許可システムタイプ]** を **[+追加]** します。
6. **[ユーザーによるオーバーライドを許可]** にチェックを入れます。
7. **[次へ]** をクリックします。
8. **[この構成を有効化]** オプションを選択します。
9. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
10. **[完了]** をクリックします。

> macOS 12では、`RemovableSystemExtensions` により、アプリケーションのアンインストール中に、管理者の承認がなくても、システム拡張を無効化できます。

MAM のみ

Ivanti Neurons for MDM では、iOSデバイスとAndroidデバイスをMAMのみと指定し、それらのデバイスに対してモバイルアプリ管理(MAM)を提供できます。MAM Only導入により、デバイス自体を管理することなく、アプリの配布と管理が可能です。MAMのみの導入は、MAMのみの導入のためのIvanti Neurons for MDMクライアントであるAppStationを通じて行います。MAM Onlyの構成と導入の方法は、以下をご覧ください。

Androidデバイスの場合：AppStation for Android製品ドキュメンテーション

iOSデバイスの場合：AppStation for iOS製品ドキュメンテーション

すでにGoのMAM Onlyで導入されている場合は、継続してお使いいただけます。ただし新しいMAM Only導入については、IvantiはAppStationをお勧めします。

マネージドGoogle Play構成

管理者は、Google PlayストアがAndroid Enterpriseデバイス上のアプリを更新するのに使用する自動更新設定を構成できます。

自動更新設定を構成するには:

1. **[構成] > [+追加]** を開きます。
2. **[マネージドGoogle Play構成]** を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。

5. [構成設定]セクションで、Google Playからアプリを更新するオプションを選択します。

設定	操作内容
ユーザー定義	デバイスユーザーは、アプリを自動更新に設定し、アプリのメンテナンス時間帯設定で更新のタイミングを設定できます。 a. **[開始時刻]**フィールドで、アプリ更新を実行する時刻を選択します。 b. **[時間枠]**フィールドで更新を実行する時間枠(時間単位)を選択します。時間枠は1～24時間で設定します。 アプリは、開始時刻から選択した時間枠内のどこかで更新されます。たとえば開始時刻を午後6時、時間枠を12時間に設定した場合、アプリは午後6時から翌朝6時のどこかで更新されます。
なし	Google Playストアはデバイス上のアプリを自動的に更新しません。
Wi-Fiのみ	Google Playストアは、セルラーではなくWi-Fiに接続した場合のみ、デバイス上のアプリを自動的に更新します。
常に	Google Playストアは、セルラーでもWi-Fi接続でも、デバイス上のアプリを自動的に更新します。

6. **[次へ]**をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム

8. **[完了]** をクリックします。

プリンター設定

Ivanti Neurons for MDM では、プリンタープロファイルを作成し、デバイスに追加できます。これにはBridgeが必要です。詳細はBridgeをご覧ください。

プリンタープロファイルをデバイスに送信する際、プリンターがアクティブでない場合は検出されません。

Windowsデバイス用にプリンターを設定するには:

1. **[構成] > [+追加]** を開きます。
2. **[プリンター設定]** 構成を選択します。
3. 構成の名前を入力します。

4. **[Windows]** オプションを選 択します。

5. **[構成設定]** セクションで、以下の設定を構成します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
Windowsプリンター設定	
共有プリンター	**[共有プリンター]** オプションを選択すると、プリンターは他のデバイスと共有されます。次のフィールドを設定してください。 **名前**: プリンター構成の名前を入力します。 **説明**: プリンターの説明を入力します。 **プリントサーバー**: プリントサーバーのIPアドレスを入力します。 **共有プリンター名**: プリンター名を入力します。
ネットワーク接続プリンター	**[ネットワーク接続]** オプションを選択すると、プリンターは接続したネットワーク内のデバイスからのみアクセス可能となります。次のフィールドを設定してください。 **名前**: プリンター構成の名前を入力します。 **説明**: プリンターの説明を入力します。 **プリンター名**: ネットワーク内のプリンターの名前を入力します。 **プリンターホストアドレス**: プリンターのホストIPアドレスを入力します。

設定	操作内容
	プリンターポート番号：ネットワークのポート番号を選択します。 **プリンタードライバー名**：プリンタードライバーの名前を入力します。 **プリンタードライバーURL**：プリンタードライバーのURLを入力します。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

macOSデバイス用にプリンターを設定するには:

1. **[構成] > [+追加]** を開きます。
2. **[プリンター設定]** 構成を選択します。
3. 構成の名前を入力します。
4. **[macOS]** オプションを選択します。

5. **[プリンター構成の作成]** セクションで、以下を設定します。

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
構成設定	次のフィールドを更新し、macOSデバイス用のプリンターを設定します。 • ローカルプリンターを許可 • デフォルトのプリンター表示名 • フッターフォント名 • フッターフォントサイズ • ユーザープリンターのリスト • + プリンターを追加

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

ブロートウェア削除構成

ブロートウェア削除構成では、デバイスにインストールされているアプリケーションのうち、強制的に削除する必要のあるアプリケーションを選択できます。この構成を利用するには、Bridge設定を持つことが前提要件です。詳細はBridgeをご覧ください。

アプリを実行またはアンインストールするには:

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[ブロートウェアを削除]** 構成を選択します。**[ブロートウェア削除構成]** ページが表示されます。
3. **[名前]** フィールドに適切な構成名を入力します。
4. **[+説明を追加]** をクリックして構成の説明を追加します。このフィールドの記入は任意です。
5. **[構成設定]** セクションで、削除またはアンインストールするアプリを選択します。デスクトップアプリリストに表示されたアプリ名を使用し、検索フィールドでアプリを検索することも可能です。

   > **[ブロートウェア削除]** 構成を作成する前に、**[アプリ]** > **[デスクトップアプリ]** > **[アプリをフェッチ]** を開いてアプリをフェッチする必要があります。これを実行しないと、**[ブロートウェア削除]** 構成の作時に検索または選択できるアプリケーションがない状態となります。

   .appx、.appxbundles、.xap、.msiのファイルタイプは削除できますが、.exeはできません。
6. 詳細オプションで、以下を設定します。

オプション	説明
この構成を実行する間隔:	構成を実行する間隔(分単位)を設定します。
ログオン時に実行	チェックボックスを選択すると、ログオン時に構成が実行されます。
アンインストール後の強制再起動を抑制	チェックボックスを選択すると、アプリのアンインストール後に強制再起動されません。

Samsungフォンの制約構成

構成

Samsungフォンの制約構成により、Samsungデバイスで通話制約や例外を設定することができます。これらの制約ではユーザーが発信または受信できる電話番号を制限します。

対象：Knox SDK2.0以降を実行するすべてのSamsungデバイス。

Samsungフォンの制約を構成するには：

1. **[構成]** タブで **[+追加]** をクリックします。
2. **[Samsungフォンの制約]** 構成を選択します。**[Samsungフォンの制約構成]** ページが表示されます。
3. **[名前]** フィールドに適切な構成名を入力します。
4. **[+説明を追加]** をクリックして構成の説明を追加します。このフィールドの記入は任意です。

5. **[構成設定]** セクションで、以下のオプションを構成します。

オプション	説明
着信通話	
ブロックされる番号	[追加] アイコンをクリックし、番号とJava正規表現を追加して着信に関する制約を定義します。
許可リストに含まれる番号	[追加] アイコンをクリックし、番号とJava正規表現を追加して、着信をブロックする多数の番号の中から許可する番号を定義します。 ブロックされている番号がない場合、このオプションの効力はありません。
発信通話	
ブロックされる番号	[追加] アイコンをクリックし、番号とJava正規表現を追加して発信に関する制約を定義します。
許可リストに含まれる番号	[追加] アイコンをクリックし、番号とJava正規表現を追加して、発信をブロックする多数の番号の中から許可する番号を定義します。 ブロックされている番号がない場合、このオプションの効力はありません。

6. 選択したデバイスに設定をプッシュするには、**[完了]** をクリックします。

デバイスが撤去されたときは、すべての通話制約がデバイスから削除されます。

詳細は構成を作成するにはを参照してください。

Single Appモード構成

構成

ライセンス：Silver

Single Appモードは、iOSデバイスを指定されたアプリのみの利用に制限します。たとえば、組織が開発したカスタムアプリしか利用できないようデバイスを設定することができます。

Single Appモード構成

設定	操作内容
名前	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
アプリを選択	アプリの選択方法を選びます。 • **アプリカタログおよびシステムアプリから:** Ivanti Neurons for MDM アプリカタログとシステムアプリ(Appleデバイスのデフォルトでインストール済み) から検索する場合に選択します。 • アプリの名前を入力し、アプリリストに表示されたら選択します。 • **バンドルIDを入力:** 選択したいシステムアプリの固有識別子を入力する場合に選択します。このオプションは、**[アプリカタログおよびシステムアプリから]** オプションでシステムアプリが見つからない場合に使用してください。
タッチを無効にする	タッチスクリーンを無効にする場合に選択します。
デバイスローテーションを無効化	デバイスローテーションの感知を無効にする場合に選択します。
音量ボタンを無効化	デバイスの音量ボタンを無効にする場合に選択します。
通知音を無効化	デバイスの通知音を無効にする場合に選択します。
スリープ/スリープ解除ボタンの無効化	デバイスのスリープ/スリープ解除ボタン(デバイスの枠の右上) を無効にする場合に選択します。
自動ロックを無効化	操作しないままの状態の後でもスリープにならないようにする場合に選択します。
VoiceOverの有効化	VoiceOver画面リーダーを有効にする場合に選択します(アクセシビリティ機能) 。
ズーム機能を有効にする	ズーム機能を有効にする場合に選択します(アクセシビリティ機能) 。
色の反転を有効化	色の反転調整を有効にする場合に選択します(アクセシビリティ機能) 。

Assistive Touchを有効にする	Assistive Touchを有効にする場合に選択します(アクセシビリティ機能)。
選択項目の読み上げを有効化	選択項目の読み上げを有効にする場合に選択します(アクセシビリティ機能)。
モノラルオーディオを有効化	ステレオとモノラルのオーディオ切り替えを有効にする場合に選択します(アクセシビリティ機能)。
VoiceOverの調整	デバイスがVoiceOverの調整を行えるようにする場合に選択します。
ズーム機能の調整	デバイスユーザーがズーム機能の調整を行えるようにする場合に選択します。
色の反転の調整	デバイスユーザーが色の反転の調整を行えるようにする場合に選択します。
Assistive Touchの調整	デバイスユーザーがAssistive Touchの調整を行えるようにする場合に選択します。

詳細は構成を作成するにはを参照してください。

スタートメニューとタスクバー

ユーザーのスタートメニューのレイアウトを定義して、使用可能なアプリケーションを定義し、不要なアプリケーションを削除できます。Windows 10および11バージョンでは、スタートメニューのレイアウトが異なるため、別の機能がサポートされます。

スタートメニューとタスクバーの構成を設定するには:

1. **[構成] > [+追加]** を開きます。
2. **[Windowsスタートメニュー& タスクバー]** 構成を選択します。
3. 構成の名前を入力します。
4. Windows 固有のバージョンを選択します。

   Windows 10デバイス:
5. **[構成設定]** セクションで、以下の設定を構成します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ゴールデンデバイスを選択	アプリをスタートメニューとタスクバーにプロビジョニングするWindows 10デバイスを選択します。

6. **[デバイスからスタートメニューレイアウトをフェッチ]** をクリックし、以下のオプションを構成します。

7.

設定	操作内容
スタートメニューとタスクバーのレイアウト	必要に応じて以下のオプションを選択し、アプリのリストを非表示にします。 • **なし** • **すべてのアプリリストを非表示** • **すべてのアプリリストを非表示にし、設定アプリで「スタートメニューにアプリを表示」を無効化** • **すべてのアプリリストを非表示にし、すべてのアプリボタンを削除し、設定アプリで「スタートメニューにアプリを表示」を無効化**
スタートメニューのレイアウト	
スタートメニューをカスタマイズ	**[はい]** をクリックすると、スタートメニューとレイアウトパラメータをカスタマイズできます。
タスクバー	
タスクバーをカスタマイズ	タスクバーをカスタマイズするには **[はい]** をクリックします。
タスクバーにピン留めした既存のショートカットを削除してから、新しいショートカットを追加	**[はい]** をクリックすると、既存のピン留めされたタスクバーショートカットを削除してから、カスタムタスクバーを追加します。
アプリの種類	アプリの種類を指定します。
アプリ	アプリのIDを指定します。
復元	**[復元]** リンクをクリックすると、元のゴールデンデバイスからタスクバーが復元されます。 行の矢印アイコンをドラッグし、特定の行の位置を上下に移動します。 ロウを削除する場合は削除アイコンをクリックします。

	新しいロウを追加するには **[新規追加]** ボタンをクリックします。

Windows 11デバイス

8. **[構成設定]** セクションで、以下の設定を構成します。

設定	操作内容
[名前]	この構成を識別する名前に入力します。
説明	この構成の目的を明示する説明を入力します。
ゴールデンデバイスを選択	アプリをスタートメニューの [ピン留め済み] セクションに設定するWindows 11デバイスを選択します。

9. **[デバイスからスタートメニューレイアウトをフェッチ]** をクリックします。

   ゴールデンデバイスから設定をフェッチした後は、スタートメニューの [ピン留め済み] セクションに設定されたすべてのアプリは、管理者がレビューできるように表示されます。

10. **[保存]** をクリックして、すべての該当するデバイスとユーザーグループに構成を配布します。

> ベンダーの問題で構成が配布されない場合は、ピン留めされたアプリは元の構成のままです。ただし、新しい設定が配布されると、前のレイアウトは上書きされ、新しいレイアウトが適用されます。

システム更新構成

管理者は、デバイスユーザーによるAndroid 6.0またはサポートされる以降のバージョンでのシステム更新管理を制限することができます。この機能は、Androidエンタープライズデバイスにのみ適用されます。

構成するには：

1. **[構成] > [+追加]** を開きます。
2. **[システム更新]** 構成を選択します。
3. 構成の名前を入力します。

4. 説明を入力します。

5. [構成設定]セクションで、以下のオプションを構成します。

設定	説明
自動	新しいファームウェアが提供されるとシステム更新をサイレントに適用します。
延期	システム更新のインストールを30日間延期します。システムは30日後、デバイスユーザーに更新のインストールを促すメッセージを表示します。
ウィンドウ表示(ローカルタイム)	システム更新をサイレントに適用する時間帯を選択します。 **[開始時刻]**と**[終了時刻]**を選択してください。
フリーズ期間	指定した期間はシステム更新を凍結します。 このオプションはAndroid 9.0以降のデバイスに適用されます。 **[フリーズ期間を追加]**をクリックします。 フリーズ期間の**[開始日]**と**[終了日]**を選択します。 各フリーズ期間を90日より長くすることはできません。複数のフリーズ期間を追加することは可能です。次のフリーズ期間は前回の終了日から60日後から開始できます。 フリーズ期間を削除するには、削除アイコンをクリックします。
Zebraファームウェア構成	Zebraデバイス(Androidバージョン8.0またはサポートされる以降のバージョン)のオペレーティングファームウェアをアップグレードまたは更新するには、**[Zebra OTAを構成]**を選択します。これはデバイス所有者モードの場合のみです。 Zebra OTAの更新を構成するには、**[管理] > [ファームウェア管理] > [Zebra OTA]**からIvanti Neurons for MDM OTAサービスを有効化する必要があります。また、ZebraデバイスがCloud上になければなりません。ポップアップにZebraの認証情報を入力してください。認証情報を再生成するには、直接Zebraに問い合わせる必要があります。

設定	説明
	このオプションを選択すると、登録されたZebraデバイスのリストが表示されます。 ファームウェアを選択し、デバイスモデルに適用する方法は次のとおりです。 a. Zebraデバイスの **[アクション]** カラムで以下のいずれかのアクションを実行します: • **なし**: デバイスモデルに何のアクションも実行されません。 • **フルアップグレード**。**[ターゲットのZebraファームウェアを選択]** ウィンドウで、デバイスモデルに適用するフルアップグレードのファームウェアバージョンを選択します。 **フルアップグレード**プロセス中は、ポート443のみが必要です。 **[検索]** フィールドにビルドIDに含まれる文字を入力すると、ビルドIDに基づいてアップグレードを検索できます。ビルドIDはソートされ、降順に表示されます(最新のものが一番上)。 **[パッチアップグレード]** オプションは、Android 11以上のデバイスでは利用**できません**。

設定	説明

設定	説明
Samsung e-FOTA構成	**[Samsung e-FOTAを構成]** を選択し、Samsungデバイスのオペレーティングファームウェア(Knoxバージョン2.7.1以降) にアップグレードまたは更新します。これは、会社所有デバイス上の仕事用プロファイルモードのマネージドデバイスにのみ適用されます。 Samsung e-FOTA対応デバイスが登録されていない場合、それを伝えるメッセージがページに表示されます。 Samsung e-FOTAの更新を構成するには、**[管理] > [ファームウェア管理] > [Samsung E-FOTA]** からSamsung e-FOTAライセンスを有効化する必要があります。このオプションを選択すると、登録されたSamsungデバイスのリストが表示されます。 ファームウェアを選択し、デバイスモデルに適用する方法は次のとおりです。 a. Samsungデバイスの **[アクション]** カラムで以下のいずれかのアクションを実行します: • **最新**: 最新のファームウェアバージョンが適用されます。このオプションがデフォルトで選択されています。 • **強制**: [ターゲットのSamsungファームウェアを選択] ウィンドウで、デバイスモデルに強制(ユーザーの介入なしで) 適用するファームウェアバージョンを選択します。この操作を実行すると、15分以内にファームウェアのダウンロードが始まります。 • **ターゲット**: [ターゲットのSamsungファームウェアを選択] ウィンドウで、デバイスモデルに適用するファームウェアバージョンを選択します。 「強制」や「ターゲット」を実行する際、デバイスに対応するファームウェアがない場合は、それを伝えるメッセージがページに表示されます。

設定	説明
	b. **デバッグFWを有効化**(任意):**[デバッグFWを有効化]**オプションを有効化し、構成を適用すると、デバイスはダミーファームウェアにアップグレードされます。Samsungデバイスファームウェアのダミーファームウェアでは、管理者が、実際にはデバイス上の何も変更することなく、システム更新構成の動作をテストすることができます。 ダミーファームウェアではなく実際のファームウェア更新にアップグレードするには、管理者が**[デバッグFWを有効化]**オプションを無効化してから構成を適用する必要があります。 c. [**Apply**]をクリックします。

6. **[次へ]**をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]**をクリックします。

Samsung E-FOTA構成(終了)

Samsung E-FOTA構成は、2022年7月に廃止されています。そのため、この構成を新規デバイスで利用することはできません。既存のこの構成を使用しているデバイスでは、この構成の無効化のみを行えます。

Windows 10の更新管理

管理者は、Windows 10 Update Management を使用して更新する Windows 10 デバイスで報告された更新を表示して承認できます。この機能では、不要またはテスト済みでない更新がデバイスにインストールされるのを防止します。

更新管理機能を使用するには、デバイスの **[ソフトウェア更新]** 構成で **[更新の承認を要求]** オプションを有効化しておく必要があります。この構成をデバイスに適用して初めて、インストール可能な更新をデバイスが報告し、承認を待つようになります。

更新の管理

1. **[管理]** > **[Windows更新]** を開きます。ページに以下の更新情報が表示されます。

   作成日: 更新が作成された日付。
   タイトル: 更新の種類とサポート技術情報 (Microsoft Knowledge Base) 番号。

   > 更新をクリックすると説明が表示されます。

   分類: 更新の種類を指定します。例: セキュリティ更新。

   配布: 更新の配布対象。たとえば、更新を全デバイスに配布する場合は **[「すべて]」** と表示します。

   > 更新を所定のグループ数に配布する場合は、配布の数を表示します。たとえば、3つのグループにだけ配布する場合は「3」と表示します。

   また、更新が必要なデバイスに配布されたかどうかを表示できます。次の列に表示されている数字は、さまざまなカテゴリの更新に該当するデバイスの数を示します。

   - 資格があるデバイス
   - インストールされたデバイス
   - 失敗したデバイス
   - 再起動が保留中のデバイス

   この数字のいずれかをクリックすると、[デバイス] ページにフィルタリングされたビューが表示され、更新のステータスを確認し、必要なアクションを実行できます。

2. 更新を確認し、更新のチェックボックスをクリックすることでデバイスに配布したい更新を選択してください。

3. **[アクション]** で **[配布を設定]** をクリックします。
4. **[Windowsの更新配布]** ウィンドウで、以下のいずれかの配布オプションを選択します。

   すべてのデバイス: すべてのデバイスに更新を配布します。

   デバイスなし: デバイスへの更新配布を保留します。
   カスタム: 指定したデバイスグループに更新を配布します。
5. **[保存]** をクリックします。

更新の検索とフィルタリング

更新は、以下の基準に基づいて検索およびフィルタリングが可能です。

- サポート技術情報ID
- 配布の構成

サポート技術情報IDに基づくフィルタリング:

1. **[Windows 10の更新管理]** ページの簡易検索フィールドにナレッジベースIDを入力します (検索フィールドの数値のみ。
   例:KB4056892の場合は、4056892と入力。検索基準に一致する更新がページに表示されます。

   > **[サポート]** および **[詳細]** リンクをクリックすると、更新に関する詳細情報が得られます。**[サポート]** は、更新のサポート情報を提供するMicrosoftのWebページにリンクしています。**[詳細]** は、サポート技術情報など更新に関する詳細情報を公開するMicrosoftのWebページにリンクしています。

配布の構成に基づくフィルタリング

[Windows 10更新管理] ページで、配布の構成に基づく以下のフィルタリングオプションを選択します。

- **すべて:** すべての更新を表示します。
- **構成済み:** デバイスに配布された更新のリストを表示します。
- **未構成:** 配布が指定されていない更新のリストを表示します。

  > 構成済みと未構成のフィルターは実行された配布に基づくため、**デバイスなしの配布**も含みます。

デバイスの更新表示

各デバイスの詳細な更新情報は以下の手順で確認します。

1. **[デバイス]** > **[デバイス]** に進みます。
2. デバイス名をクリックして詳細ページを表示します。
3. **[更新]** タブを開きます。保留中(管理者に更新が承認されたが、デバイスへのインストールが報告されていない)、失敗、インストール済みの更新が表示されます。

ダッシュボードの通知ページには、新しいWindows更新に関する通知も表示されます。通知には、通知の作成日、取得可能な通知の数、通知の目的が含まれます。Windows更新通知は、管理ポータルの右上角からも閲覧できます。

Windowsアプリスケジューリング

Windowsデスクトップアプリは非常に大きく、企業にとって重要な時間帯にネットワークやサーバーに大きな負荷を長時間にわたってかける場合があります。Windowsアプリスケジューリング機能では、アプリ(特に大型のアプリ)をデバイスにインストールする時刻を指定できます。

アプリスケジューリングを構成するには:

1. **[アプリ]** > **[アプリカタログ]** へ進みます。
2. **[追加]** をクリックして、Windows アプリを選択し、**[アプリの追加]** ウィザードの次のステップに進みます。
3. ステップ 5 (構成) で、**[アプリケーション構成設定のインストール]** をクリックすると、**[構成設定]** ページが表示されます。
4. **[インストールをスケジュール]** チェックボックスを選択します。

   > **[インストールをスケジュール]** チェックボックスは、サイレントインストールが有効化されている場合のみ表示されます。

5. アプリのインストールの**開始時間**と**終了時間**を選択します。
6. アプリのインストールの**開始日**と**終了日**を選択します。

   > スケジュールされた日付が過ぎた場合に実行されるアクションとして、次の 2 つのいずれかを選択することもできます。**次回のチェックイン中にインストール**または**インストールしない**。

7. アプリ構成配布オプションを選択します。**アプリを利用する全員**、**該当なし**、または**カスタム**。
8. **[完了]** をクリックします。

   > スケジューリングを必要とするアプリはApps@Workに追加しないでください。
   > ストアアプリのサイレントインストールはサポートされないため、ストアアプリにはアプリスケジューリングを適用できません。

Windows BIOS構成

管理者はLenovoデバイスでWindows BIOSを設定できます。この構成を設定するには、BIOS設定をサポートするLenovoデバイスが1台以上登録されている必要があります。

構成するには:

1. **[構成] > [+追加]** を開きます。
2. **[WindowsBIOS]** 構成を選択します。
3. 構成の名前を入力します。
4. 説明を入力します。
5. [デバイス機種選択] セクションでドロップダウンリストからデバイス機種を選択します。

6. [構成設定] セクションで、以下のオプションを構成します。

登録されている具体的なデバイス機種によって設定のリストは異なります。

設定	操作内容
AMT制御	以下のいずれかを選択します。 • **無効化** • **有効化**
適応的熱管理AC	以下のいずれかを選択します。 • **バランス状態** • **最大パフォーマンス**
適応的熱管理バッテリー	以下のいずれかを選択します。 • **バランス状態** • **最大パフォーマンス**
Always on USB	以下のいずれかを選択します。 • **無効化** • **有効化**
BIOSPasswordAtBootDeviceList	以下のいずれかを選択します。 • **無効化** • **有効化**
再ブート時のBIOSパスワード	以下のいずれかを選択します。 • **無効化** • **有効化**
無人ブート時のBIOSパスワード	以下のいずれかを選択します。 • **無効化** • **有効化**

エンドユーザーによるBIOS更新	以下のいずれかを選択します。 • **無効化** • **有効化**
Bluetoothアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
ブートデバイスリストのF12オプション	以下のいずれかを選択します。 • **無効化** • **有効化**
ブートディスプレイデバイス	以下のいずれかを選択します。 • **DisplayPort** • **ドックディスプレイ** • **HDMI** • **LCD**
ブートモード	以下のいずれかを選択します。 • **診断** • **クイック**
ブート順序ロック	以下のいずれかを選択します。 • **無効化** • **有効化**

BootTimeExtension	以下のいずれかを選択します。 • **1。** • **10** • **2** • **3** • **5** • **無効化**
下カバーの改ざん検出	以下のいずれかを選択します。 • **無効化** • **有効化**
CPU電源管理	以下のいずれかを選択します。 • **自動** • **無効化**
Computraceモジュールアクティベーション	以下のいずれかを選択します。 • **無効化** • **有効化**
データ実行防止	以下のいずれかを選択します。 • **無効化** • **有効化**
イーサネットLANアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**

イーサネットLANオプションROM	以下のいずれかを選択します。 • **無効化** • **有効化**
指紋パスワード認証	以下のいずれかを選択します。 • **無効化** • **有効化**
指紋プレデスクトップ認証	以下のいずれかを選択します。 • **無効化** • **有効化**
指紋リーダーアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
指紋リーダーの優先度	以下のいずれかを選択します。 • **外部** • **内部のみ**
指紋セキュリティモード	以下のいずれかを選択します。 • **高** • **通常**
Fn Ctrlキー交換	以下のいずれかを選択します。 • **無効化** • **有効化**

FnKeyAsPrimary	以下のいずれかを選択します。 • **無効化** • **有効化**
FnSticky	以下のいずれかを選択します。 • **無効化** • **有効化**
IPv4ネットワークスタック	以下のいずれかを選択します。 • **無効化** • **有効化**
IPv6ネットワークスタック	以下のいずれかを選択します。 • **無効化** • **有効化**
内蔵カメラアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
InternalStorageTamper	以下のいずれかを選択します。 • **無効化** • **有効化**
キーボードビープ音	以下のいずれかを選択します。 • **無効化** • **有効化**

ロックBIOS設定	以下のいずれかを選択します。 • **無効化** • **有効化**
メモリカードスロットアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
マイクロフォンアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
Minimum Password Length (パスワードの最小文字数)	以下のいずれかを選択します。 • **4** • **5** • **6** • **7** • **8** • **9** • **10** • **11** • **12** • **無効化**

NFFControl	以下のいずれかを選択します。 • **無効化** • **有効化**
Nfcアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
AC接続でオン	以下のいずれかを選択します。 • **無効化** • **有効化**
PasswordBeep	以下のいずれかを選択します。 • **無効化** • **有効化**
パスワードカウント超過エラー	以下のいずれかを選択します。 • **無効化** • **有効化**
Tpmクリアの物理的プレゼンス	以下のいずれかを選択します。 • **無効化** • **有効化**
Tpmプロビジョニングの物理的プレゼンス	以下のいずれかを選択します。 • **無効化** • **有効化**

ラピッド・スタート・テクノロジー	以下のいずれかを選択します。 • **無効化** • **有効化**
セキュアブート	**[有効化]** を選択
セキュアロールバック防止	以下のいずれかを選択します。 • **無効化** • **有効化**
セキュリティチップ	以下のいずれかを選択します。 • **アクティブ** • **無効化** • **有効化** • **非アクティブ**
スマートカードスロットアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
SpeedStep	以下のいずれかを選択します。 • **無効化** • **有効化**
起動オプションキー	以下のいずれかを選択します。 • **無効化** • **有効化**

TXT機能	以下のいずれかを選択します。 • **無効化** • **有効化**
グラフィックスメモリ合計	以下のいずれかを選択します。 • **256 MB** • **512 MB**
タッチパッド	以下のいずれかを選択します。 • **自動** • **無効化**
TrackPoint	以下のいずれかを選択します。 • **自動** • **無効化**
USB30モード	以下のいずれかを選択します。 • **自動** • **無効化** • **有効化**
USB BIOSサポート	以下のいずれかを選択します。 • **無効化** • **有効化**
USBポートアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**

Uefi Pxeブート優先度	以下のいずれかを選択します。 • **IPv4ファースト** • **IPv6ファースト**
VTd機能	以下のいずれかを選択します。 • **無効化** • **有効化**
バーチャライゼーション・テクノロジー	以下のいずれかを選択します。 • **無効化** • **有効化**
Wake On LAN	以下のいずれかを選択します。 • **ACのみ** • **ACおよびバッテリー** • **無効化** • **有効化**
ワイヤレスLANアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**
ワイヤレスWANアクセス	以下のいずれかを選択します。 • **無効化** • **有効化**

7. **[次へ]** をクリックします。

8. 以下の配布オプションから1つ選択します。
    - すべてのデバイス
    - デバイスなし(デフォルト)
    - カスタム
9. **[完了]** をクリックします。

Windows BitLocker

管理者は、デバイスのGUIDとリカバリパスワードを記載したExcelファイルのアップロードにより、暗号化したWindows 10デバイス群のリカバリキーを一括更新できます。

リカバリキーを一括更新するためのExcelファイルをアップロードするには：

1. **[管理] > [Windows BitLocker]** を開きます。
2. **[サンプルのCSVファイルをダウンロード]** をクリックし、サンプルのCSVファイルをダウンロードするとともに、.csvファイルの例を参照します。
3. レコードを作成し、BitLockerリカバリキー用の.csvファイルに追加します。
4. **[リカバリパスワードをアップロード]** をクリックします。
5. **[ファイルを選択]** をクリックし、作成した.csvファイルをアップロードします。
6. **[アップロード]** をクリックします。以前アップロードしたキーで新しいファイルをアップロードすると、古いエントリが上書きされます。

> 1回のアップロードで最大1,000件のレコードを送信できます。アップロードが成功すると、各デバイスのデバイス詳細にキーが表示されます。

Windowsキオスク構成

Windowsキオスク構成では、Windows 10デバイスでシングルアプリまたはマルチアプリのキオスクを設定できます。この構成を適用すると、キオスクユーザーは、キオスクアプリ以外の機能へのアクセスが制限されます。この構成には、Windows Bridgeの有効化が必要です。

構成の適用には以下の3つのモードがあります。

- シングルアプリケーション
- マルチアプリケーション(Windowsデバイスからアプリケーションのリストをフェッチ)
- マルチアプリケーション(スタートメニュー構成から既存のレイアウトを選択)

Windowsキオスク構成に使用するアプリケーションは、Windowsキオスクモードを開始する前にデバイス上に存在する必要があります。

Windowsキオスク構成を構成するには:

1. **[構成] > [+追加]** を開きます。
2. **[Windowsキオスク構成]** を選択します。
3. 構成の名前を入力します。

4. 説明を入力します。

5. [構成設定] セクションで、次の表に記載されているように残りの設定を指定します。

設定	操作内容
キオスクモードの選択：以下の3つのオプションのいずれかを選択します。	
シングルアプリケーション	デバイスでシングルアプリケーションキオスクモードを構成する場合に選択します。 a. **[Windowsデバイスを選択(任意)]** セクションでWindows 10デバイスを選択します。**[デバイスからアプリをフェッチ]** をクリックし、デバイスからアプリのリストをフェッチします。アプリデータをフェッチするには、選択したデバイスが管理下にあり、チェックインしている必要があります。 手順をスキップするには、**[この手順をスキップ。必要であれば後で実行できます]** のチェックボックスを選択します。 b. フェッチしたリストからアプリを追加するには、**[フェッチしたアプリリストから追加]** をクリックします。 c. アプリの **[名前]** カラムのラジオボタンをクリックし、シングルアプリを選択します。**[新規追加]** をクリックし、新しいアプリをリストに追加します。リストからアプリを削除するには、削除アイコンをクリックします。

マルチアプリケーション (Windowsデバイスからアプリケーションのリストをフェッチ)	デバイスでマルチアプリケーションキオスクモードを構成する場合に選択します。 a. **[Windowsデバイスを選択(任意)]** セクションでWindows 10デバイスを選択します。**[デバイスからアプリをフェッチ]** をクリックし、デバイスからアプリのリストをフェッチします。アプリデータをフェッチするには、選択したデバイスが管理下にあり、チェックインしている必要があります。 手順をスキップするには、**[この手順をスキップ。必要であれば後で実行できます]** のチェックボックスを選択します。 b. **[キオスクアプリとスタートメニューのレイアウト]** で **[フェッチしたアプリリストから追加]** をクリックします。**[キオスクアプリを選択]** ウィンドウが表示されます。フェッチしたリストからアプリ(1つまたは複数)を選択し、**[選択したアプリを使用]** をクリックします。

	c. [追加の許可アプリ] セクションで **[フェッチしたアプリリストから追加]** をクリックします。**[キオスクアプリを選択]** ウィンドウが表示されます。フェッチしたリストからアプリ(1つまたは複数)を選択し、**[選択したアプリを使用]** をクリックします。 追加の許可されたアプリとは、**[キオスクアプリとスタートメニューのレイアウト]** で選択したアプリに依存すると考えられるアプリです。「許可アプリ」がなければ、たとえスタートメニューにアプリケーションアイコンが表示されてもOSはそのアプリケーションを実行できません。 d. **[新規追加]** をクリックし、新しいアプリをリストに追加します。リストからアプリを削除するには、削除アイコンをクリックします。リスト内のアプリはドラッグして必要な場所に移動できます。 e. **[マルチアプリのその他の設定]** で必要なオプションを選択します。 • **電源ボタンを非表示** • **ユーザータイルを非表示** • **タスクバーを非表示**

マルチアプリケーション(スタートメニュー構成から既存のレイアウトを選択)	スタートメニューレイアウト構成をすでに作成している場合は、構成をインポートし、このオプションの選択によってマルチアプリケーションモードの構成に使用できます。 a. **[レイアウトを選択]** セクションで、過去にスタートメニュー構成として設定されたレイアウトを選択します。適切なレイアウトパラメータを持つ作成済みの構成が、下のドロップダウンリストに表示されます。 b. [マルチアプリのその他の設定] で必要なオプションを選択します。 • **電源ボタンを非表示** • **ユーザータイルを非表示** • **タスクバーを非表示**

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

> 構成を完全に有効にするには、適用後にデバイスを再起動するか、Windowsキオスク構成を更新する必要があります。マルチアプリキオスク構成に使用するアプリケーションによっては、デバイスを2回再起動する必要があります。最初のログイン時には表示されないアイコンがあるかもしれませんが、2回目の再起動後にログインすると表示されます。

キオスク構成の適用、削除、更新の後には、デバイスを再起動する必要があります。デバイスのアクションメニューから [デバイスを再起動/シャットダウン] コマンドを実行してください。再起動しない場合、以下が生じます。

- キオスク構成を適用しても、デバイスが自動的にキオスクモードにならない。
- 適用したキオスク構成を削除しても、デバイスが自動的にキオスクモードを終了しない。
- デバイスが実行中のキオスク構成を変更しない。

キオスク構成を適用したデバイスが、更新済みの構成を受信した場合、デバイス上のWindows OSが既存のキオスクユーザーを削除し、新しいキオスク構成で新しいキオスクユーザーを1人作成します。現行ユーザーのセッションは、デバイスの再起動によって明示的に終了する必要があります。

マルチアプリキオスク構成には「.lnk」ファイル、シングルアプリキオスク構成には「.exe」ファイルを使用することをお勧めします。デバイスからインポートしたスタートメニュー構成は「.lnk」形式です。「.exe」アプリケーションによっては、「.exe」アプリケーション用に手動で作成したスタートメニュー項目がマルチアプリキオスク構成のスタートメニューに表示されない場合があります。

たとえば、Windows Media Playerは、以下の「.lnk」ファイルのいずれかを使用してスタートメニューに追加できます。

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

このアプリを、以下の「.exe」ファイルのいずれかを使用して直接追加すると、最初の「.exe」パスが上記の「.lnk」ファイルの中で使用されていても、対応のアイコンが表示されません。

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

シングルアプリキオスク構成の場合、exeファイルに引数を追加できます。E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. しかし、マルチアプリ構成の場合、引数のあるexeアプリのアイコンがスタートメニューに表示されません。引数のあるexeアプリをマルチアプリキオスク構成に表示させたい場合は、内部に引数を持つ「.lnk」ファイルを使用してください。シングルアプリキオスク構成では「.lnk」が作用しません。

マルチアプリキオスクモードにおける依存関係

マルチアプリキオスクモードの場合、Win32/64アプリケーションには [追加の許可されたアプリ] セクションで依存関係を追加する必要があります。シングルアプリキオスクモードの場合、追加の許可されたアプリは不要です。

例1: Windows Media Playerアプリをマルチアプリキオスクモードで使用する場合、以下の依存関係が必要です。

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

最初の依存関係は、対応の「.lnk」ファイルから呼び出されるアプリバイナリです。2番目は、最初の依存関係から呼び出されるワンタイムウィザードです。

「許可されたアプリ」がなければ、たとえスタートメニューにアプリケーションアイコンが表示されてもOSはそのアプリケーションを実行できません。

例2: Internet Explorerの場合、以下のリストにある項目を設定していれば、アイコンがスタートメニューに表示されます。

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- C:\Program Files\internet explorer\iexplore.exe
- %ProgramFiles%\Internet Explorer\iexplore.exe

Internet Explorerには以下の依存関係が必要です。

- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Program Files (x86)\Internet Explorer\ExtExport.exe
- C:\Program Files (x86)\Internet Explorer\ieinstal.exe
- C:\Program Files (x86)\Internet Explorer\ielowutil.exe

最初の依存関係は、「.lnk」項目にのみ必要なアプリバイナリです。もう1つの依存関係はワンタイムウィザードです。最初の依存関係がなければ、OSはポップアップを出してアプリをブロックします。他の依存関係が欠けている場合、OSからの通知なく、アプリケーションが起動直後に閉じます。

Windowsライセンス構成

Windowsライセンス構成は、Windows 10 ProからWindows 10 Enterpriseなどデバイス上のOSをアップグレードします。この構成によって、Windows 10デスクトップデバイスのプロダクトキーのアクティベートまたは変更も可能です。

Windowsライセンスをアップグレードにするには：

1. **[構成] > [+追加]** を開きます。
2. **[Windowsライセンス]** 構成を選択します。
3. 構成の名前を入力します。
4. **[構成設定]** セクションでWindows**プロダクトキー**を入力します。
5. **[次へ]** をクリックします。
6. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
7. **[完了]** をクリックします。

ソフトウェア更新の推奨頻度の構成

管理者には、ユーザーがリリースを表示して、最も大きな数字(最新)のリリース、最も小さな数字(最も古い)のリリース、またはそのいずれかへの更新を許可するオプションがあります。

対象: iOS +、iPadOS14.5+(監視対象)

Procedure

1. **[構成]** > **[+追加]** を開きます。
2. 検索フィールドに **[ソフトウェア更新の推奨]** と入力し、**[ソフトウェア更新の推奨頻度]** 構成をクリックします。
3. 構成の **[名前]** と **[説明]** を入力します。
4. ドロップダウンから必要な構成設定を選択します。
   - 両方のソフトウェア更新バージョンを提示
   - 小さな数字の(最も古い)ソフトウェア更新バージョンを提示します
   - 最も大きな数字(最新)のソフトウェア更新バージョンのみを提示します
5. **[次へ]** をクリックします。
6. **[この構成を有効化]** オプションを選択します。
7. 以下の配布オプションから1つ選択します。
   - すべてのデバイス
   - デバイスなし(デフォルト)
   - カスタム
8. **[完了]** をクリックします。

ポリシー

ポリシーは、デバイスの要件、およびデバイスがその要件を遵守しなかった場合にどうなるかについて定義するものです。各ポリシーは、ルールとコンプライアンスアクション(ルール違反の場合に何が起こるか)で構成されています。**[ポリシー]** ページを使用して、ポリシーの選択、設定、配布を行うことができます。

このセクションは以下のトピックを含みます。

ポリシーの操作

このセクションは以下のトピックを含みます。

ポリシーの実行

ポリシーは、デバイスの要件、およびデバイスがその要件を遵守しなかった場合にどうなるかについて定義するものです。各ポリシーは、ルールとコンプライアンスアクション(ルール違反の場合に何が起こるか)で構成されています。**[ポリシー]** ページを使用して、ポリシーの選択、設定、配布を行うことができます。

利用できるポリシーには次のような種類があります。

種類	操作内容
侵害されたデバイス	脱獄(iOS)またはroot化(Android)したデバイスにフラグを付けます。 なぜシステムがAndroidデバイスがルート化によって侵害されているとフラグを付けたか、違反理由を見るには: 1. **[ポリシー]** タブをクリックします。 2. **[侵害を受けたデバイス]** リンクをクリックします。 3. **[実行中の違反]** タブをクリックします。 4. [違反]列で違反の理由にチェックを入れます なぜシステムがAndroidデバイスがルート化によって侵害されているとフラグを付けたか、違反理由を見るには:

<table>
<tr><th>種類</th><th>操作内容</th></tr>
<tr><td></td><td>

[ポリシー] タブをクリックします。
[侵害を受けたデバイス] リンクをクリックします。
[実行中の違反] タブをクリックします。
[違反] 列で違反の理由にチェックを入れます理由は以下のいずれかとなります。

<table>
<tr><th>優先度(1 = 最高)</th><th>違反</th></tr>
<tr><td>1。</td><td>プラグインが侵害されています</td></tr>
<tr><td>2</td><td>クライアントが改ざんされています</td></tr>
<tr><td>3</td><td>デバイス製造業者が不明です:不明</td></tr>
<tr><td>4</td><td>疑わしいフォルダーが検出されました:[パス]</td></tr>
<tr><td>5</td><td>疑わしいバイナリが検出されました:[パス]</td></tr>
<tr><td>6</td><td>フォルダー/データがブラウズ可能またはフォルダー/データ/データがブラウズ可能</td></tr>
<tr><td>7</td><td>/system/app/Superuser.apkが見つかりました</td></tr>
<tr><td>8</td><td>パッケージマネージャーが侵害されています</td></tr>
<tr><td>9</td><td>疑わしいアプリが検出されました:[パッケージ]</td></tr>
</table>
</td></tr>
<tr><td>データ保護/暗号化無効(macOS のみ)</td><td>パスコードや暗号化を有効にしていないmacOSデバイスにフラグを付けます。</td></tr>
<tr><td>国際ローミング</td><td>国際ローミング課金が発生する可能性のあるデバイスにフラグを付けます。ステータスは、デバイスのチェックイン時に更新されます。

iOSの場合、iOSによって設定され、報告されたローミングフラグを使用します。コンプライアンスアクションは、最初の違反時のみ行われます。</td></tr>
</table>

種類	操作内容
MDMまたはデバイス管理の無効化	MDMを無効化したデバイスは、チェックイン中に他のポリシー、または構成やアプリのデルタ処理に対して評価されません。
接続なし	指定された時間範囲だけ、Ivanti Neurons for MDMとの接続がなかったデバイスにフラグを付けます。 指定した時間の範囲や日数(2～3から23～24)だけデバイスのチェックインがなかったときのアクションを選択します。
MIクライアント接続なし(iOSのみ)	指定された時間範囲だけ、Ivanti Neurons for MDMとの接続がなかったIvanti Neurons for MDMクライアントにフラグを付けます。 指定した時間の範囲や日数(2～3から23～24)だけクライアントのチェックインがなかったときのアクションを選択します。 これはiRegを通じて登録されたデバイスにも適用されます このポリシーは、クライアントがない場合、またはクライアントが所定の期間だけチェックインしていない場合にコンプライアンス違反とマークします。
許可されたアプリ	許可アプリや必須アプリに関するルールに違反するデバイスにフラグを付けます。
カスタムポリシー	指定した条件や関連操作に基づいてカスタムポリシーを作成します。

コンプライアンスアクション

以下のコンプライアンスアクションが使用できます。

コンプライアンスアクション	操作内容
モニター	Ivanti Neurons for MDMの[デバイス]ページでデバイスにフラグを設定します。これはデフォルトでオンになっています。
ブロック	前回のチェックイン詳細の時点で、ポリシー違反があった後に、デバイスがSentryまたはAccess経由でのリソースへのアクセスを試行した場合、デバイスをブロックするようにAccess/Sentryに指示します。
ユーザーにメッセージを送信	• Ivanti Neurons for MDMの[デバイス]ページでデバイスにフラグを設定します。

コンプライアンスアクション	操作内容
	• デバイスのオーナーにEメールを送信します。 • デバイスにPush通知を送信します。
検疫	• デバイスからほとんどの構成を削除します。 • 例外：パスコード構成、Wi-Fi専用デバイスのWi-Fi構成、制約構成（iOS）。 • Ivanti Neurons for MDMによってインストールされたすべてのアプリケーションが削除されます。 • iBookおよびePubファイルを含め、Ivanti Neurons for MDMによって配布されたすべてのコンテンツを削除します。 • Ivanti Neurons for MDMカタログへのアクセスをブロックします。 • 追加アプリのインストールのプロンプトを一時停止します。 • AppConnect対応アプリへのアクセスをブロックします。 • AppConnect対応アプリのサポートを含みます。 • オンの場合、検疫デバイスの個人側にあるアプリが保留中となり、それを機能させるには、ユーザーがデバイスのコンプライアンス問題に対処する必要があることを示します。企業所有デバイスの仕事用プロファイルとしてプロビジョニングされたAndroid 11+のデバイスでサポートされます。

既存のポリシーの検索

[ポリシー] ページでフィルターと検索機能を使用することで、1つまたは複数の既存のポリシーを検索できます。

手順

1. **[ポリシー]** に進みます。
2. **[フィルター]** をクリックすると、特定の基準に一致するポリシーをリストアップすることができます。
3. 1つ以上のフィルター基準を選択します。
4. 既存のポリシーを名前で検索するには、ポリシー名を **[検索]** フィールドに入力します。

ポリシーの追加

手順

1. **[ポリシー]** に進みます。
2. **[+追加]**(右上)をクリックします。
3. ポリシーの種類を選択します。
4. 設定を完了させます。
5. このポリシーの対象とするデバイスグループを選択します。

   1回に配布できる構成ファイルは最大100件です。

6. **[完了]** をクリックします。

ポリシーの編集

手順

1. **[ポリシー]** に進みます。
2. 必要なポリシーの [アクション] カラムで **[編集]**(鉛筆)アイコンをクリックします。
3. 変更を加えます。
4. 変更を保存します。

ポリシーの削除

手順

1. **[ポリシー]** に進みます。
2. 必要なポリシーの [アクション] カラムで **[削除]** アイコンをクリックします。
3. **[はい]** をクリックして確定します。

[ポリシー] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- 読み取り専用デバイス

詳細はポリシーの優先度決定を参照してください。

カスタムポリシー

ポリシー

ライセンス: Platinum

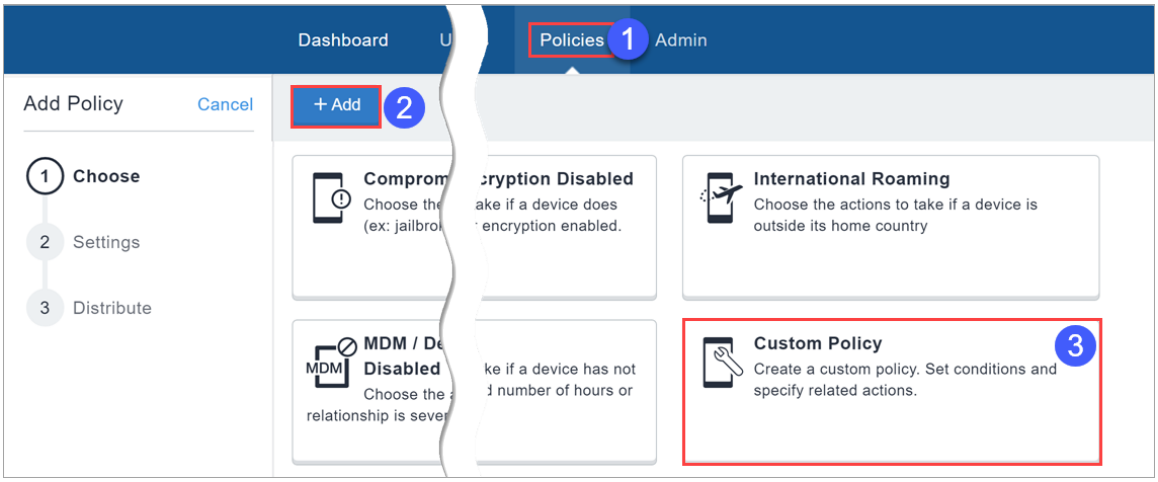
対象デバイス: Android、iOS、macOS、Windows

デバイスやユーザーの属性、セクション基準、値、指定するコンプライアンスアクションに基づいてカスタムポリシーを作成できます。

カスタムポリシーを定義する際にはAndroidセキュリティパッチレベル設定も使用可能です。

カスタムポリシーの追加

1. **[ポリシー]** に進みます。



2. **[+追加]** をクリックします。
3. **[カスタムポリシー]** を選択します。
4. カスタムポリシーに名前を付けます。
5. 必要であれば **[+説明を追加]** をクリックして詳細を追加します。

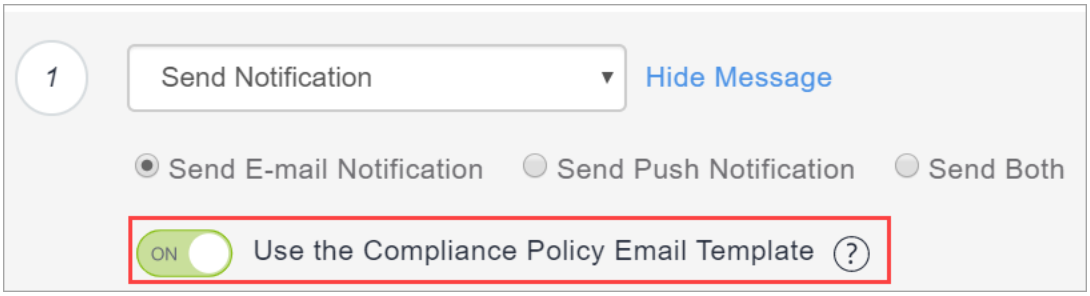
6. Rule Builderを使用し、条件がtrueと判断された場合にアクションをトリガーする条件を定義します。条件の作成に関するガイダンスについては、条件設定の理解を参照してください。Ivanti Neurons for MDM 92以降、ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM Administratorは重複するユーザーグループ数と、重複するグループを識別するGUID番号を表示します。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

7. 指定した条件を満たした場合に実行するコンプライアンスアクションを選択します(以下のデフォルトアクションを参照)。**「待機」**アクションを他のアクションの間に追加することにより、デバイスユーザーは、次のアクションが実行される前にデバイスを修正し、コンプライアンスを回復できます。たとえば、警告メッセージを送り、24時間経ってから検疫を適用します。

8. デフォルトでオフになっている **[デバイスがコンプライアンス状態に戻ったときに通知を送信]** オプションを選択します。

   - **メールを送信** - デバイスがコンプライアンス状態に戻ったときに、デバイスユーザーのメールアドレスに通知メールを送信します。

     - **[コンプライアンスポリシーメールテンプレートの使用]** オプションをオンにし、ここで設定するメッセージを、「メールテンプレートのブランディング」 ページ1304の「メールテンプレートのカスタマイズ」 ページ1305に記載されているとおりにポリシー通知メールテンプレートに挿入します。概要は、「ポリシーコンプライアンス通知メールの構成と使用」 ページ28をご覧ください。



     - メッセージをカスタマイズして任意の置換変数を含めることにより、受信者にポリシー違反に関する詳細や他の関連情報を与えることもできます。以下の属性タイプをクリックし、完全な変数リストを表示してください。

       - ${nameOfPolicy}、${nextAction}、${nonComplianceTime}を含むポリシー属性
       - ${sAMAccountName}、${userCN}、${userEmailAddressDomain}を含むユーザー属性
       - ${deviceClientDeviceIdentifier}、${deviceIMEI}、${deviceModel}を含むデバイス属性
       - **[管理] > [属性]** ページから作成したカスタムデバイス/ユーザー/LDAP属性

   - **プッシュ通知を送信** - デバイスがコンプライアンス状態に戻ったときにプッシュ通知を送信します。
   - **両方を送信** - デバイスがコンプライアンス状態に戻ったときに、デバイスユーザーのメールアドレスに通知メールを送信し、デバイスにプッシュ通知も送信します。メッセージをカスタマイズして任意の置換変数を含めることにより、前に「メールを送信」で述べた情報を与えることもできます。

デフォルトアクション:

- **モニター** - 現在、常に選択されています。段階的コンプライアンスアクションを利用するにはSentryバージョン9.0.0以降が必要です。
- **何もしない**
- **通知を送信**
  - **メールを送信** - デバイスユーザーのメールアドレスにデバイスのコンプライアンス違反を通知するメールを送信します。
    - ポリシー通知メールテンプレートは上記のように使用します。
    - メッセージをカスタマイズして任意の置換変数を含めることにより、受信者にポリシー違反に関する詳細や他の関連情報を与えることもできます。これによりコンプライアンス違反デバイスのユーザーは、ポリシー違反に関する情報を得て適切な対策を取ることができます。以下の属性タイプをクリックし、完全な変数リストを表示してください。
      - ${nameOfPolicy}、${nextAction}、${nonComplianceTime}を含むポリシー属性
      - ${sAMAccountName}、${userCN}、${userEmailAddressDomain}を含むユーザー属性
      - ${deviceClientDeviceIdentifier}、${deviceIMEI}、${deviceModel}を含むデバイス属性
      - **[管理] > [属性]** ページから作成したカスタムデバイス/ユーザー/LDAP属性
  - **プッシュ通知を送信** - デバイスがコンプライアンス違反であることを伝えるプッシュ通知を送信します。
  - **両方を送信** - デバイスユーザーのメールアドレスにデバイスのコンプライアンス違反を通知するメールを送信し、デバイスにプッシュ通知も送信する場合に選択します。メッセージをカスタマイズして任意の置換変数を含めることにより、前に「メールを送信」で述べた情報を与えることもできます。
- **ブロック** - Sentryを使用し、マネージドデバイスによるメールとAppConnect対応アプリケーションへのアクセスをブロックします。ブロックアクションを利用するにはSentryバージョン9.0.0以降が必要です。
- **撤去** - デバイスを撤去します。**このアクションは取り消しができません**。たとえば、ユーザー有効条件を使用し、すべての無効なユーザーのデバイスを撤去するルールも設定できます。
- **待機** - ユーザーが違反を修正できるよう、所定の時間(時間または日数)だけアクションを遅らせます。デバイスがコンプライアンス違反を続けた場合には、さらなるアクションが実行されます。

- **検疫** - 以下のアクションにより、アプリ、コンテンツ、サーバーへのアクセスを停止します。

(任意)追加検疫アクション	**説明**
マネージドアプリを隔離	Ivanti Neurons for MDM マネージドアプリをデバイスから削除し、「新規アプリダウンロードをブロック」オプションを有効化して、デバイスにアプリが再インストールされるのをブロックします。 以下のオプションから1つ選択してください: • **すべてのアプリケーション** • **指定したアプリケーション** - 検索または手動で1つ以上のアプリを追加します(バンドルIDまたはパッケージ名を使用)。**[アプリを表示]** タブをクリックすると、追加されたアプリのリストが表示されます。[アプリストアへのアクセスをブロック] というデフォルトの検疫アクションは利用できません。 特定のデバイスでは、検疫アクションによりアプリがデバイスから削除されることはありません。これは特定のデバイス制限によるものです。
新規アプリダウンロードをブロック	デバイスへの新規アプリのダウンロードを防止します。 以下のオプションから1つ選択してください: • **すべてのアプリケーション** • **指定したアプリケーション** - 検索または手動で1つ以上のアプリを追加します(バンドルIDまたはパッケージ名を使用)。**[アプリを表示]** タブをクリックすると、追加されたアプリのリストが表示されます。[アプリストアへのアクセスをブロック] というデフォルトの検疫アクションは利用できません。

	デフォルトではこのオプションが選択され(すべてのアプリケーションと指定したアプリケーションの両方)、選択を解除することはできません。これでアプリがデバイスに再インストールされるのを防ぎます。
コンフィグレーションの削除	Ivanti Neurons for MDM 構成をデバイスから削除します。 以下のオプションから1つ選択してください: • **すべての構成** • **指定した構成** - リストから1つ以上の構成を選択するか、構成を検索します。**[選択した構成]** タブをクリックすると、選択した構成のリストが表示されます。
指定した構成をプッシュ	カスタムコンプライアンスの一環として指定した構成を配布します。 このリストは、以下の基準を満たす構成を含みます。 • 有効な構成 • 非システム構成 • 検疫可能な構成 • 現在のスペースで作成された、またはデフォルトスペースから委譲された構成 検疫不可能な構成のリストは、検疫不可能な構成を参照してください。 詳細については、「指定した構成のプッシュ」ページ 1001セクションの、この手順の後を参照してください。
コンテンツを削除	Ivanti Neurons for MDM によって配布されたアプリに関連するすべてのコンテンツとメディアをデバイスから削除します。

個人用アプリを保留	検疫デバイスの個人側にあるアプリを保留中であり、それを機能させるには、ユーザーがデバイスのコンプライアンス問題に対処する必要があることを示します。企業所有デバイスの仕事用プロファイルとしてプロビジョニングされたAndroid 11+のデバイスでサポートされます。
デフォルトの検疫アクション - これらのアクションは常に実行されます。	
App Storeへのアクセスをブロック	デバイスがIvanti Neurons for MDM経由でアプリストアにアクセスするのを防止します。
コンテンツストアへのアクセスをブロック	デバイスがIvanti Neurons for MDM経由でコンテンツストアにアクセスするのを防止します。
AppConnectをブロック	デバイスがAppConnect機能を使用するのを防止します。
AppTunnelをブロック	デバイス上のアプリケーションがAppTunnel経由でコンテンツとサーバーにアクセスするのを防止します。
ActiveSyncをブロック	デバイスがActiveSyncサーバー経由でメールにアクセスするのを防止します。

1. **[はい]** のチェックボックスをクリックし、このポリシーが過去にデバイスに適用されたことがあった場合、階層型ポリシーの追加によってポリシーと過去に適用されたコンプライアンスアクションがリセットされることを理解したことを承認します。次のデバイスチェックインで新しいカスタムポリシーが有効になります。撤去を選択した後、**[はい]** をクリックして操作を取り消せないことを確認します。
2. **[次へ]** をクリックし、ポリシーとアクションを適用するデバイスを構成します。
3. **[完了]** をクリックします。

次の表は、Ivanti Neurons for MDMが検疫アクションの開始プログラムである場合の、各種Androidデバイス上の検疫動作を示します。

デバイス	検疫動作
Goクライアントアプリでデバイス管理モードのSamsungデバイス	• マネージド市販アプリおよび自社開発アプリの両方をアンインストール • 特定のプロファイルを削除(MobileIron Threat Defenseなどを除く)

デバイス	検疫動作
Goクライアントアプリでデバイス管理モードのSamsung以外のデバイス AppStationアプリによるMAM	• マネージド市販アプリおよび自社開発アプリの両方のアンインストールまたは非表示には対応していません • 特定のプロファイルを削除(MobileIron Threat Defenseなどを除く)
GoクライアントアプリでAndroid Enterprise	• マネージド市販アプリおよび自社開発アプリの両方を非表示 • 特定のプロファイルを削除(MobileIron Threat Defenseなどを除く)

指定した構成のプッシュ

カスタムコンプライアンスの一環として指定した構成を配布します。デバイスがコンプライアンス違反になったときに構成セットを配布するよう、カスタムポリシーを構成してください。デバイスのステータスが非コンプライアンスからコンプライアンスに変わった場合、修復アクションの一環としてデバイスを前の状態にリセットします。

[指定した構成をプッシュ]タブで非委譲構成を持つカスタムポリシーを管理者が委譲しようとするとエラーが発生します。

以下は、所定の条件下で構成がカスタムポリシーによってプッシュされるときの挙動です。

条件	挙動
優先度を設定した2つの同じ種類の構成が選択されています	優先度の高い構成がデバイスにプッシュされます。
優先度が設定されていない2つの同じ種類の構成が選択されている	両方の構成がデバイスにプッシュされ、予期しない挙動につながる場合があります。
カスタムポリシーで定義された優先度をサポートする同じ種類の構成がデバイスにすでに存在するとき	カスタムポリシーに定義されている構成が優先され、デバイスにプッシュされます。デバイスに既存の構成が優先度に関係なく削除されます(カスタムポリシーに定義されている構成より優先度が高い場合でも)。
カスタムポリシーで定義された優先度をサポートしない同じ種類の構成がデバイスにすでに存在するとき	カスタムポリシーに定義されている構成がデバイスにプッシュされます。両方の構成がデバイスに存在することになり、予期しない挙動につながる場合があります。
カスタムポリシーを作成した後に構成の優先度が変更されている場合	デバイスチェックインの際、カスタムポリシーの一環であれば、最も優先度の高い構成がプッシュされます。
両方の条件を満たしているとき: • 条件A:違反のあるデバイスで、過去にカスタムポリシーの一環として構成がプッシュされている(そしてそれがデバイス上に既存の同じ種類の構成より優先されたとき) • 条件B:違反が修復され、デバイスの隔離が終了している	カスタムポリシーに定義されている構成が削除され、既存のデバイスグループのアプリケーションを通じて検疫前のデバイス上の同じ種類の構成がプッシュされます。これによりデバイスは元の状態に戻ります。

検疫アクションで、[指定した構成をプッシュ]とともに[検疫を削除]を選択している場合、以下のルールにご注意ください。

- すべての構成を削除 + 指定した構成をプッシュ:この場合、デバイスからすべての構成が削除され、[指定した構成をプッシュ]から選択した構成がデバイスにプッシュされます。
- 両方の選択で共通の構成を使用して、(1つのカスタムポリシーで)指定した構成を削除し、(別のカスタムポリシーで)指定した構成をプッシュします。2つの異なる準拠ポリシーで構成が選択されるため、最も厳しいアプローチが適用されます。例:構成はデバイスから削除されます。

カスタムポリシーは、デフォルトのスペースからカスタムスペースに委譲できます。カスタムポリシーを委譲するには、[指定した構成をプッシュ] タブでカスタムポリシーに言及されている構成をスペースに委譲する必要があります。

[デバイス] ページでデバイス名をクリックし、デバイスの詳細ページを開いてください。[構成] タブでは、デバイスにプッシュされる構成の配布方法が [配布方法] のカラムに表示されます。配布方法は「デバイスグループ」か「コンプライアンスアクション」です。

構成ページでは、デバイスグループとコンプライアンスアクション経由で各構成を受け取ったデバイス数をIvanti Neurons for MDMが表示します。

条件設定の理解

次の表は、規則の構築に使用できるフィールドについての説明です。

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
APNS対応	このフィールドはデバイスがAPNS対応かどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android
Bootstrapトークンを利用できます	このフィールドはデバイスがBootstrapトークンを利用できるかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	macOS
クライアントの前回のチェックイン	このフィールドは、クライアントの前回のチェックイン時間を示します。	可能性のある演算子： • は次より以下： • は次より大きい： 最後のチェックイン時間の数値を入力します。時間の長さについて次を選択します。 • 時間 • 日 例：クライアントの最後のチェックインは過去12時間以内です。	iOS/macOS/Android

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
クライアント登録	このフィールドは、登録されたクライアントのステータスを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android
侵害	このフィールドは、デバイスがルート化/侵害されているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 取り得る値は次のとおりです。 • 脱獄またはルート化されている • 侵害されていません	iOS/Android
現在の国名	このフィールドは、デバイスが現在接続されていることを報告するモバイル国コード(MCC)またはモバイルネットワークコード(MNC)に対応する現在の国の名前を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 値は本国名を示すドロップダウンリストの値となります。	iOS/macOS/Android
現在のMCC	このフィールドは現在のモバイル国コードを示します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません：	iOS/macOS/Android

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
現在のMNC	このフィールドは現在のモバイルネットワークコードを示します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません：	iOS/macOS/Android
カスタムデバイス属性	このフィールドは、属性の値を検証する規則の条件として既存のカスタムデバイス属性を追加することを許可します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません： • 含む • 次を含みません： 値は、スペースとUnicode文字を含むASCII文字列でもかまいません。	iOS/macOS/Android/Windows
カスタムLDAP属性	このフィールドは、属性の値を検証する規則の条件として既存のカスタムLDAP属性を追加することを許可します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません： • 含む • 次を含みません： 値は、スペースとUnicode文字を含むASCII文字列でもかまいません。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
カスタムユーザー属性	このフィールドは、属性の値を検証する規則の条件として既存のカスタムユーザー属性を追加することを許可します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません： • 含む • 次を含みません： 値は、スペースとUnicode文字を含むASCII文字列でもかまいません。	iOS/macOS/Android/Windows
データローミング	このフィールドは、属性の値を検証する規則の条件としてデータローミングを使用することを許可します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。 デバイスがこのフィールドに関する情報を提供していない場合、デフォルト値は「いいえ」となります。	iOS/Android

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
デバイスの種類	このフィールドは、デバイスモデルを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了： 値はテキスト値となります。	iOS/macOS/Android/Windows
暗号化有効	このフィールドは、デバイスの暗号化/データ保護が有効化されているかどうかを示します。	はい - デバイスの暗号化/データ保護が有効化されています。 いいえ - デバイスの暗号化/データ保護が有効化されていません。	iOS/Android/Windows
GUID	このフィールドはデバイスのGUIDを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了：	iOS/macOS/Android/Windows
本国	このフィールドは、デバイスのSIMまたはeSIMがにプログラミングされているモバイル国コード(MCC)またはモバイルネットワークコード(MNC)に対応する本国名を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 値は本国名を示すドロップダウンリストの値となります。	iOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
失敗したWindows Updateがあります	このフィールドは、デバイスが最新の更新ルールに対してコンプライアンス違反かどうかを示します。	はい - デバイスが最新の更新に適合していません。 いいえ - デバイスが最新の更新に適合しています。	Windows
ホームMCC	このフィールドは自宅のモバイル国コードを示します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません：	iOS/macOS/Android
ホームMNC	このフィールドは自宅のモバイルネットワークコードを示します。	検証する属性の値を入力します。可能性のある演算子： • は次と等しい： • は次と等しくありません：	iOS/macOS/Android
IMEI	このフィールドは第1のSIMスロットのIMEI番号を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了：	iOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
IMEI2	このフィールドは第2のSIMスロットのIMEI番号を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了：	Android
IMSI	このフィールドはSIMカードのIMSI番号を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了：	Android/Windows
最新のチェックイン	このフィールドでは、MDMチャネル経由でのマネージドデバイスの前回のチェックイン時間に関連する条件を設定します。	可能性のある演算子： • は次より以下： • は次より大きい： 最後のチェックイン時間の数値を入力します。時間の長さについて次を選択します。 • 時間 • 日 例：前回のチェックインは12時間以上前です。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
最後のホットフィックスID	このフィールドでは、前回のホットフィックスIDに関連する条件を設定します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • は次より以下： • は次より以下または同等： • は次より大きい： • は次以上または同等： • 含む • 次を含みません： • 開始： • 次で開始しません： • 終了： • 次で終了しません：	Windows
インストールされた最後のホットフィックス	このフィールドでは、前回インストールされたホットフィックスに関連する条件を設定します。	可能性のある演算子： • は次より以下： • は次より大きい：	Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
ロケーターサービス有効	このフィールドは、デバイスでデバイスロケーターサービス(「iPhoneを探す」など)が有効化されているかどうか示します。	可能性のある演算子: • は次と等しい: • は次と等しくありません: [はい]か[いいえ]のいずれかの値となります。	iOS
製造者	このフィールドでは、ユーザーがデバイスのメーカーに関する条件を設定できます。	可能性のある演算子: • は次と等しい: • は次と等しくありません: 取り得る値は次のとおりです。 • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
MDM管理	このフィールドは、デバイスでMDM/デバイス管理が有効化されているかどうかを示します。	可能性のある演算子: • は次と等しい: • は次と等しくありません: [はい]か[いいえ]のいずれかの値となります。	iOS/macOS/Android

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
OS	このフィールドは、デバイスのOSタイプを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 取り得る値は次のとおりです。 • macOS • Android • iOS • Windows	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
OSビルドバージョン	このフィールドは、デバイスのOSビルドバージョンを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • は次より以下： • は次より以下または同等： • は次より大きい： • は次以上または同等： • 含む • 次を含みません： • 開始： • 次で開始しません： • 終了： • 次で終了しません：	iOS/macOS/Android/Windows
OSバージョン	このフィールドは、デバイスのOSバージョンを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • は範囲内です： 値はテキストとなります。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
オーナーシップ	このフィールドは、デバイスの所有者タイプを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 取り得る値は次のとおりです。 • ユーザー所有 • 設定なし • 会社所有	iOS/macOS/Android/Windows
プロファイル準拠パスコード	このフィールドは、デバイスのパスコードがプロファイルの要件に適合しているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android
個人ホットスポット有効	このフィールドは、デバイス上で個人ホットスポット機能が有効かどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。 個人ホットスポット設定は一部の通信事業者にのみ対応しています。	iOS

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
電話番号	このフィールドはデバイスの電話番号を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 含む • 開始： • 終了：	iOS/Android/Windows
ローミング	このフィールドは、デバイスのローミングステータスを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/Android/Windows
Sentryによるブロック	デバイスがSentryによってブロックされているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
ステータス	このフィールドは登録ステータスを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 可能性のあるデフォルト値は「アクティブ」です。 デバイスの状態を「アクティブ」に限定するため、カスタムポリシーにおいて他の可能な値は削除されています。これは、ポリシー評価がデバイスチェックイン時にのみ実行され、アクティブなデバイスだけがチェックインしてポリシーを評価されるためです。	iOS/macOS/Android
シリアル番号	このフィールドはデバイスのシリアル番号を示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • 開始： • 終了：	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
監視対象	このフィールドは、デバイスが監視されているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS
補足的ビルドバージョン	このフィールドは、デバイスの補助的ビルドバージョンを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • は次より以下： • は次より以下または同等： • は次より大きい： • は次以上または同等： • 含む • 次を含みません： • 開始： • 次で開始しません： • 終了： • 次で終了しません： • は空白ではない • は空白である	iOS/macOS

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
補足的OS/バージョンエクストラ	このフィールドは、デバイスの補助的OSビルドバージョンを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： • は次より以下： • は次より以下または同等： • は次より大きい： • は次以上または同等： • 含む • 次を含みません： • 開始： • 次で開始しません： • 終了： • 次で終了しません： • は空白ではない • は空白である	iOS/macOS
ユーザー有効	このフィールドは、ユーザーが有効化されているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
ユーザーグループ	このフィールドは、ユーザーグループを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません：	iOS/macOS/Android/Windows
音声ローミング	このフィールドは、デバイス上で音声ローミングが有効かどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。 音声ローミング設定は一部の通信事業者にのみ対応しています。 音声ローミングを無効化するとデータローミングも無効化されます。 デバイスがこのフィールドに関する情報を提供していない場合、デフォルト値は「は次と等しくない：」となります。	iOS
Accessによるブロック	デバイスがAccessによってブロックされているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android/Windows

UIフィールド	説明	可能性のある値	サポート対象のプラットフォーム
コンプライアンス	デバイスが準拠しているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： 可能性のある値は [準拠] と [非準拠] です。	iOS/macOS/Android/Windows
コンプライアンスアクションによるブロック	デバイスがブロックされているかどうかを示します。	可能性のある演算子： • は次と等しい： • は次と等しくありません： [はい] か [いいえ] のいずれかの値となります。	iOS/macOS/Android/Windows

検疫不可能な構成

以下の表は検疫不可能な構成のリストです。

OS	検疫不可能な構成
Android	• Androidアプリのカタログ • Android暗号化 • Android enterprise • Android Enterpriseアプリ • Android Zebra • フィッシング対策保護 • Android仕事用本人確認 • デバイスのパスコード

OS	検疫不可能な構成
	• ファイルのダウンロード • ロックダウン& キオスク: Androidデバイス管理者モード • ロックダウン& キオスク: Samsung Knox Standard • MAM のみ • 仕事用プロファイルを持つマネージドデバイス/会社所有デバイス上の仕事用プロファイル • 仕事用マネージドデバイス(デバイス所有者) • Samsungフォンの制約 • SafetyNet認証 • 会社所有デバイス上の仕事用プロファイル
iOSとmacOS	• フィッシング防御(iOS) • アプリ通知(iOS) • AppStationサイト(iOS) • Filevaultリカバリキー(macOS) • Filevault 2(macOS) • グローバルプロキシ(iOS) • ホーム画面レイアウト(iOS) • iOSアプリ制御 • iOSの制約 • iOSソフトウェア更新(iOS) • macOSのファイアウォール

OS	検疫不可能な構成
	• macOSソフトウェア更新 • MAM Only(iOS) • MI クライアントプライバシー(iOS/macOS) • ネットワーク利用 (iOS) • Office 365アカウント作成 (macOS) • Single Appモード (iOS) • システムポリシー制御 (macOS) • システムポリシー管理 (macOS) • システムポリシールールオプション(macOS) • タイムサーバー(macOS) • Webコンテンツフィルター(iOS)
Windows	• Windowsアプリ制御 • Windows制約 DDF(データ定義ファイル) • Windowsファイアウォール • Windowsネットワークプロキシ • Windowsの制約 • Windowsの更新
すべて	• アクティブディレクトリ • クライアントサービス • モバイル デバイスの管理 • MobileIron Threat Defense アクティベーション • MobileIron Threat Defense ローカルアクション

OS	検疫不可能な構成
	• パスコード • プライバシー • プライバシー声明 • ServiceConnect • 同期

[ポリシー] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- デバイス管理
- 読み取り専用デバイス

許可されたアプリの監視と制御

ライセンス: Silver

インストールされるアプリを制御するには、許可されたアプリポリシーを作成します。このポリシーは、MobileIron Packager(MIP) 自社開発macOSアプリもサポートします。このポリシーには以下の情報が含まれます。

- **許可リストアプリ**[1]
- **ブロックリストアプリ**[2]
- **必須アプリ**[3]
- **コンプライアンスアクション**[4]

1つのアプリが必須アプリとブロックリストアプリの両方に指定されている場合、必須リストに照らしての評価が優先されます。たとえば、アプリA1が必須リストとブロックリストの両方に入っている場合、このデバイスのアプリポリシー評価は以下のようになります:

- A1がデバイスにインストールされているとき、デバイスはコンプライアンス適合
- A1がデバイスにインストールされていないとき、デバイスはコンプライアンス違反

サポートされるデバイス

- Android 4.2またはサポートされる以降のバージョン
- iOS 8.0またはサポートされる以降のバージョン
- macOS 10.12またはサポートされる以降のバージョン

前提条件

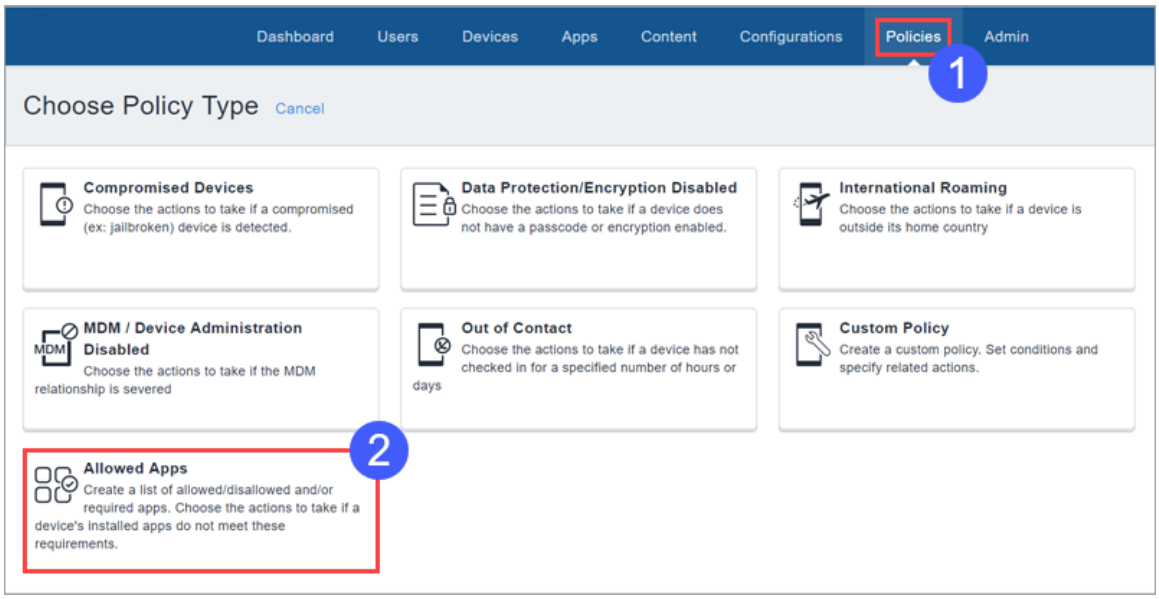
---

[1]applications that are allowed on a device. A device that has other apps installed is considered out of compliance.
[2]applications that are not approved for installation on a device. A device that has any of these apps installed is considered out of compliance.
[3]applications that must be installed on a device. A device that is missing any of these apps is considered out of compliance.
[4]automated responses to a device that violates rules for managed devices.

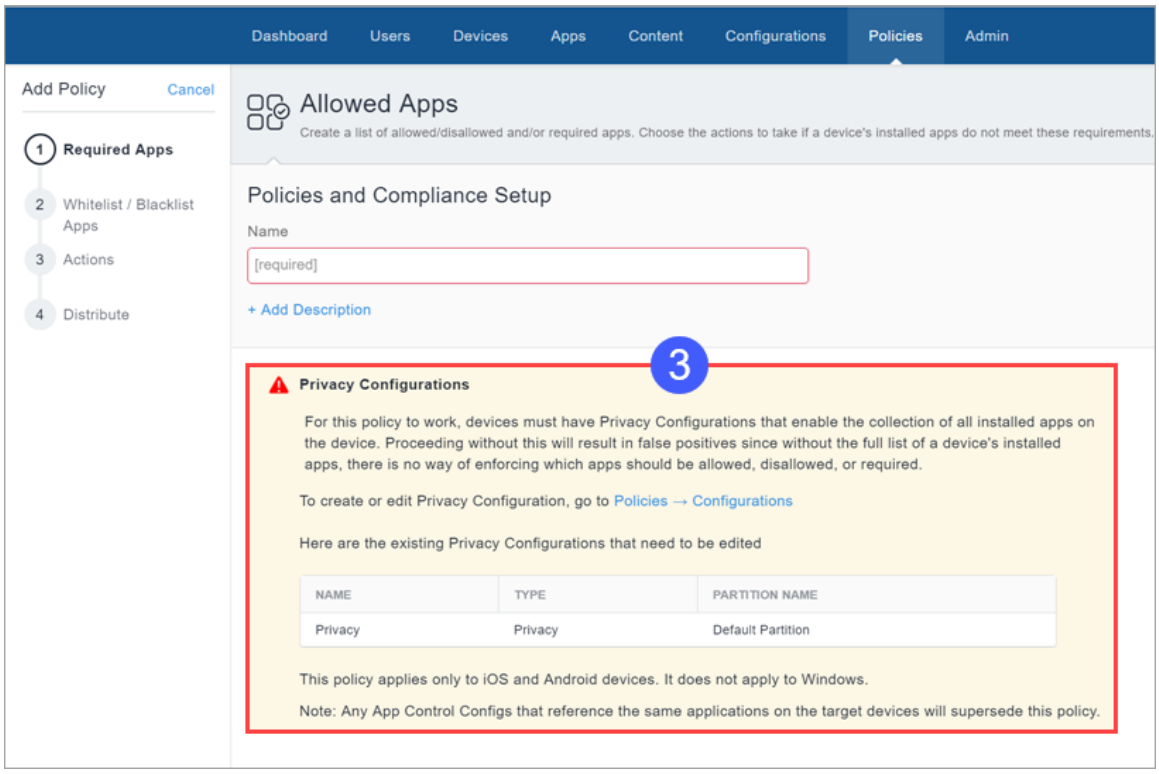
- 許可されたアプリポリシーが正しく機能するには、デバイスに指定されたプライバシー構成が、アプリ情報の収集を許可する必要があります。許可されたアプリポリシーを適用しようとするデバイスのプライバシー構成を確認してください。

どの構成が影響を受けるか確信がない場合：

1. **[ポリシー]** に進みます。



2. **[許可されたアプリ]** をクリックします。



3. **[プライバシー構成]** で編集する必要のある構成を確認します。
4. **[構成]** に進みます。
5. 確認したプライバシー構成のそれぞれについて：
   a. 構成を選択します。
   b. **[編集]** をクリックします。
   c. **[アプリインベントリを収集]** で、**[デバイス上のすべてのアプリ]** を選択します。
   d. **[完了]** をクリックします。

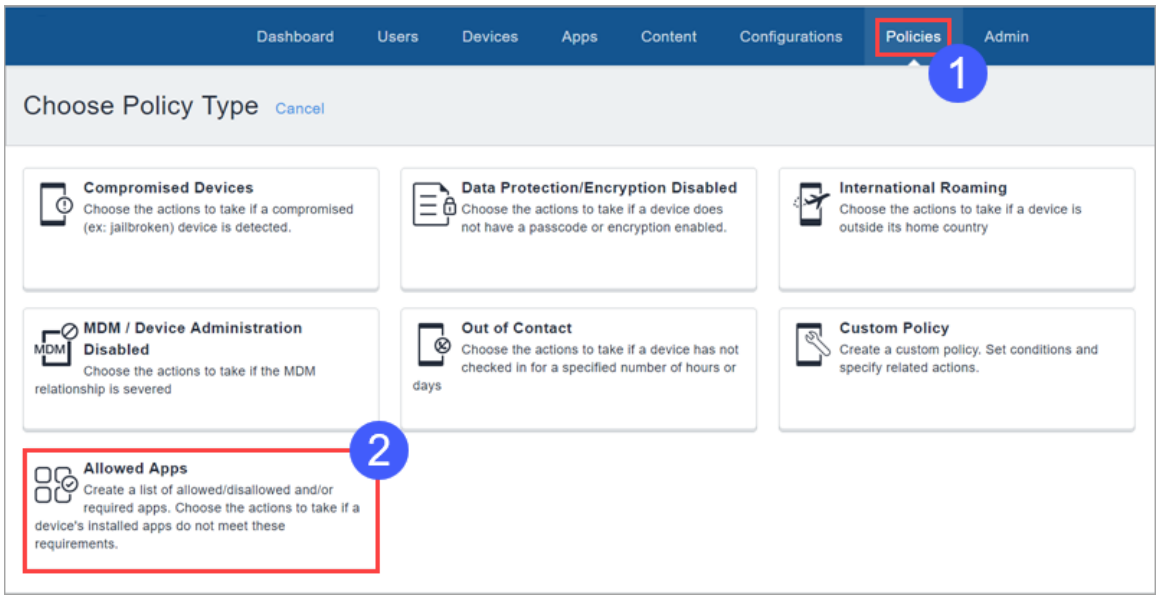
許可されたアプリポリシーの作成

前提条件

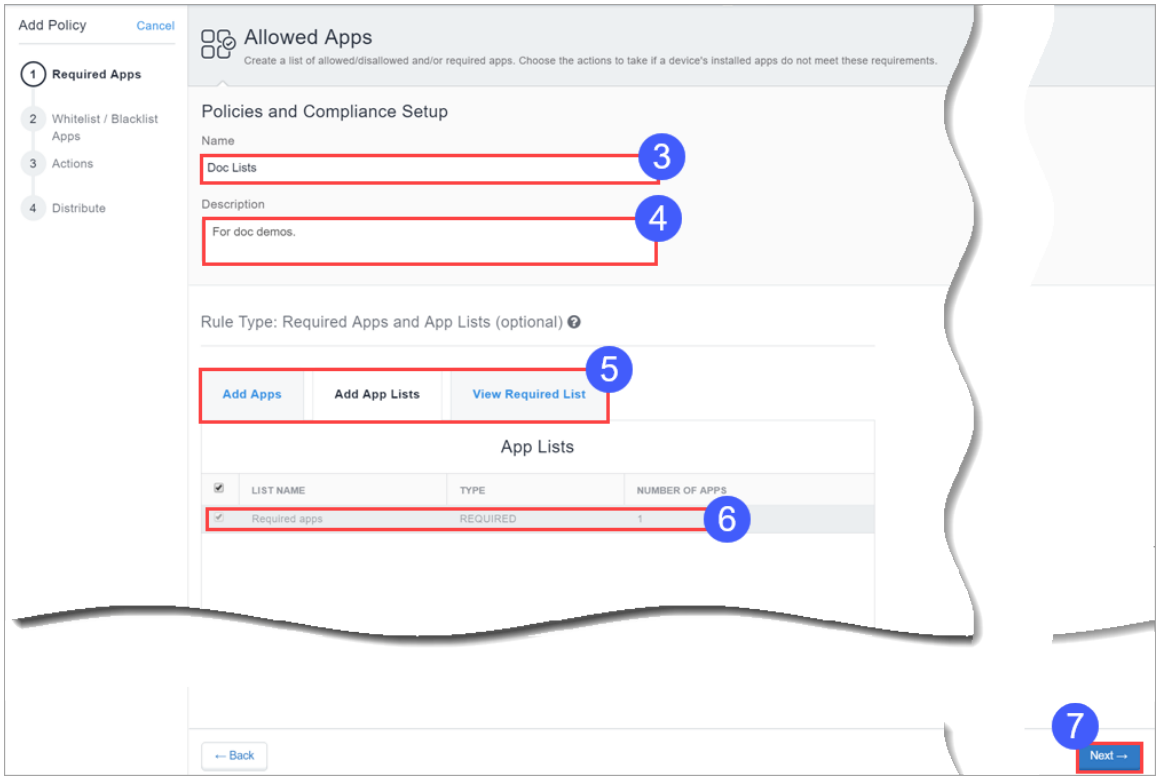
- Android Enterpriseに、Google Playストアへのアクセスおよび許可されたアプリのポリシーへの新しいアプリケーション追加を許可します。

手順

1. **[ポリシー]** から **[+追加]** をクリックします。



2. **[許可されたアプリ]** をクリックします。

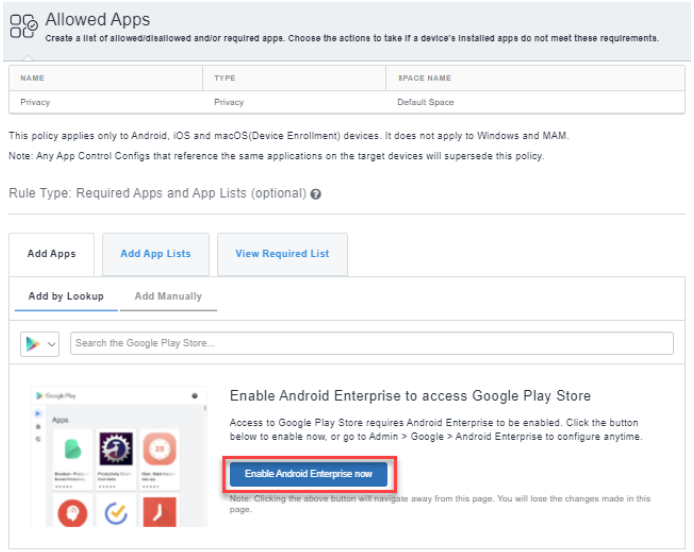


3. **[名前]** フィールドにこのポリシーの名前を入力します。

4. **[説明]** フィールドに、ポリシーの目的を説明する任意のテキストを入力します。

   次のタブのいずれかまたは両方をクリックすることによって、許可リスト化またはブロックリスト化するアプリを選択します。

- [ルックアップで追加]をクリックしてApp Storeまたはアプリカタログからアプリを検索および選択します。Android EnterpriseがGoogle Playストアにアクセスできることを確認します。

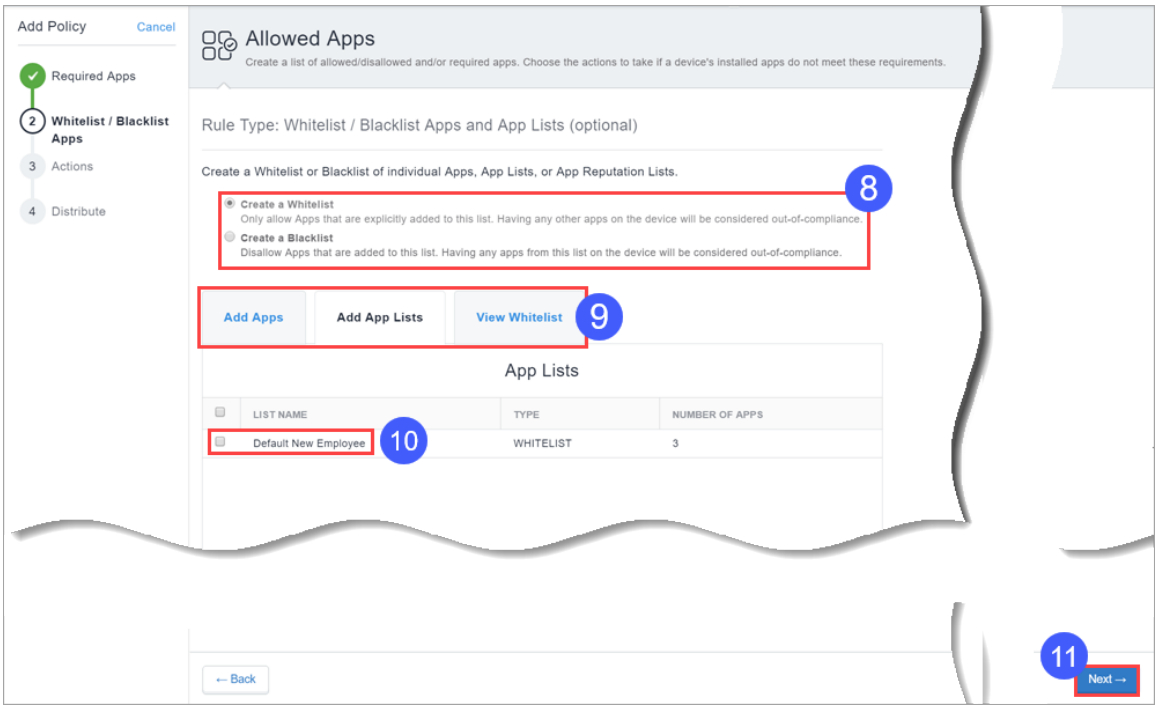


- **[手動で追加]**をクリックし、Android、iOS、macOSシステムアプリのいずれかのバンドルIDを入力してアプリを選択します。

5. **[アプリリストを追加]**タブから必要な必須アプリリストを選択します。
6. 表示されるフィールドを使用して必須アプリやアプリリストを選択します。

> **[必須リストを表示]**タブをクリックすると、これまでに選択したアプリのリストが表示されます。

7. **[次へ]**をクリックします。



8. 許可リスト、ブロックリストのいずれを作成するかを選択します。

   1つのデバイスに許可リストとブロックリストの両方を同時に設定することはできません。許可リストを作成すれば、それ以外はすべてブロックリストということになります。

9. **[許可リスト/ブロックリストアプリとアプリリスト]** セクションを使用してアプリとアプリリストを選択します。

   - **[アプリリストを追加]** タブから必要なアプリリストを選択します。

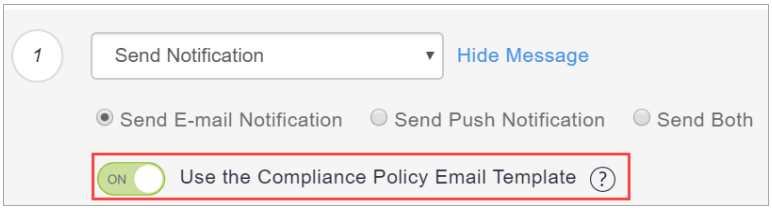
10. 表示されるフィールドを使用して必須アプリやアプリリストを選択します。

    [許可リストまたはブロックリストを表示] タブをクリックすると、これまでに選択したアプリのリストが表示されます。

11. **[次へ]** をクリックします。

12. デバイスがコンプライアンスから外れた場合のアクションを選択します。

アクション	操作内容
モニター	現在、常に選択されています。段階的コンプライアンスアクションを利用するにはSentryバージョン9.0.0以降が必要です。
何もしない	デバイスがコンプライアンス違反でもアクションを実行しない場合に選択します。
通知を送信	

メールを送信	デバイスユーザーのメールアドレスにデバイスのコンプライアンス違反を通知するメールを送信する場合に選択します。
	• **[コンプライアンスポリシーメールテンプレートの使用]** オプションをオンにし、ここで設定するメッセージを、「メールテンプレートのブランディング」ページ1304の「メールテンプレートのカスタマイズ」ページ1305に記載されているとおりにポリシー通知メールテンプレートに挿入します。概要は、「ポリシーコンプライアンス通知メールの構成と使用」ページ28をご覧ください。
	 
	• メッセージをカスタマイズして任意の置換変数を含めることにより、受信者にポリシー違反に関する詳細や他の関連情報を与えることもできます。これによりコンプライアンス違反デバイスのユーザーは、ポリシー違反に関する情報を得て適切な対策を取ることができます。以下の属性タイプをクリックし、完全な変数リストを表示してください。
	  • ${BlockedlistAppsInViolation}、${requiredAppsInViolation}、${AllowlistAppsInViolation}を含むポリシー属性
	  • ${sAMAccountName}、${userCN}、${userEmailAddressDomain}を含むユーザー属性
	  • ${deviceClientDeviceIdentifier}、${deviceIMEI}、${deviceModel}を含むデバイス属性

アクション	操作内容
プッシュ通知を送信	デバイスがコンプライアンス違反であることを伝えるプッシュ通知を送信する場合に選択します。
両方を送信	デバイスユーザーのメールアドレスにデバイスのコンプライアンス違反を通知するメールを送信し、デバイスにプッシュ通知も送信する場合に選択します。メッセージをカスタマイズして任意の置換変数を含めることにより、前に「メールを送信」で述べた情報を与えることもできます。
待機	ユーザーが違反を修正できるよう、所定の時間だけアクションを遅らせる場合に選択します。デバイスがコンプライアンス違反を続けた場合には、さらなる対策が実行されます。
ブロック	Sentryを使用し、マネージドデバイスによるメールとAppConnect対応アプリケーションへのアクセスをブロックします。
検疫	以下の表のアクションにより、アプリ、コンテンツ、サーバーへのアクセスを停止する場合に選択します。[すべてのアプリを削除] アクションは許可されません。
デバイスがコンプライアンス状態に戻ったときに通知を送信します。	

アクション	操作内容

メールを送信	デバイスがコンプライアンス状態に戻ったときに、デバイスユーザーのメールアドレスに通知メールを送信します。
	• ポリシー通知メールテンプレートは上記のように使用します。
	• メッセージをカスタマイズして任意の置換変数を含めることにより、受信者にポリシー違反に関する詳細や他の関連情報を与えることもできます。以下の属性タイプをクリックし、完全な変数リストを表示してください。
	  • ${nameOfPolicy}、${nextAction}、${nonComplianceTime}を含むポリシー属性
	  • ${sAMAccountName}、${userCN}、${userEmailAddressDomain}を含むユーザー属性
	  • ${deviceClientDeviceIdentifier}、${deviceIMEI}、${deviceModel}を含むデバイス属性
	  • **[管理] > [属性]** ページから作成したカスタムデバイス/ユーザー/LDAP属性

プッシュ通知を送信	デバイスがコンプライアンス状態に戻ったときにプッシュ通知を送信します。
両方を送信	デバイスがコンプライアンス状態に戻ったときに、デバイスユーザーのメールアドレスに通知メールを送信し、デバイスにプッシュ通知も送信します。メッセージをカスタマイズして任意の置換変数を含めることにより、前に「メールを送信」で述べた情報を与えることもできます。

Platinumライセンスをお持ちの場合は、許可されたアプリポリシーが段階的コンプライアンスアクションをサポートします。

(任意)追加検疫アクション	説明
マネージドアプリを隔離	Ivanti Neurons for MDM マネージドアプリをデバイスから削除し、「新規アプリダウンロードをブロック」オプションを有効化して、デバイスにアプリが再インストールされるのをブロックします。

(任意)追加検疫アクション	説明
	以下のオプションから1つ選択してください: • **すべてのアプリケーション** • **指定したアプリケーション** - 検索または手動で1つ以上のアプリを追加します(バンドルIDまたはパッケージ名を使用)。**[アプリを表示]** タブをクリックすると、追加されたアプリのリストが表示されます。[アプリストアへのアクセスをブロック] というデフォルトの検疫アクションは利用できません。 特定のデバイスでは、検疫アクションによりアプリがデバイスから削除されることはありません。これは特定のデバイス制限によるものです。
新規アプリダウンロードをブロック	デバイスへの新規アプリのダウンロードを防止します。 以下のオプションから1つ選択してください: • **すべてのアプリケーション** • **指定したアプリケーション** - 検索または手動で1つ以上のアプリを追加します(バンドルIDまたはパッケージ名を使用)。**[アプリを表示]** タブをクリックすると、追加されたアプリのリストが表示されます。[アプリストアへのアクセスをブロック] というデフォルトの検疫アクションは利用できません。
コンフィグレーションの削除	Ivanti Neurons for MDM 構成をデバイスから削除します。 以下のオプションから1つ選択してください: • **すべての構成** • **指定した構成** - リストから1つ以上の構成を選択するか、構成を検索します。**[選択した構成]** タブをクリックすると、選択した構成のリストが表示されます。
コンテンツを削除	Ivanti Neurons for MDM によって配布されたアプリに関連するすべてのコンテンツとメディアをデバイスから削除します。
個人用アプリを保留	検疫デバイスの個人側にあるアプリを保留中であり、それを機能させるには、ユーザーがデバイスのコンプライアンス問題に対処する必要があることを示します。企業所有デバイスの仕事用プロファイルとしてプロビジョニングされたAndroid 11+のデバイスでサポートされます。

(任意)追加検疫アクション	説明
デフォルトの検疫アクション - これらのアクションは常に実行されます。	
App Storeへのアクセスをブロック	デバイスがIvanti Neurons for MDM経由でアプリストアにアクセスするのを防止します。
コンテンツストアへのアクセスをブロック	デバイスがIvanti Neurons for MDM経由でコンテンツストアにアクセスするのを防止します。
AppConnectをブロック	デバイスがAppConnect機能を使用するのを防止します。
AppTunnelをブロック	デバイス上のアプリケーションがAppTunnel経由でコンテンツとサーバーにアクセスするのを防止します。
ActiveSyncをブロック	デバイスがActiveSyncサーバー経由でメールにアクセスするのを防止します。

13. **[次へ]** をクリックします。
14. 配布を構成します。
15. **[完了]** をクリックします。

許可されたアプリポリシーの優先度を上げるまたは下げる方法については、ポリシーの優先度決定を参照してください。

ポリシーの優先度決定

許可されたアプリポリシーは、構成と同様、優先度をサポートします。優先度は、同じ種類のポリシーのうち、どれをどのデバイスグループに配布するかを決定します。同じデバイスが複数のデバイスグループに見られる場合にも有用です。たとえばポリシー優先度によって、以下の場合のポリシー配布が決定されます。

- 「必須アプリA」をデバイスグループ1に配布、
- 「必須アプリB」をデバイスグループ2に配布、そして
- ユーザーのデバイスが両方のデバイスグループに属する。

ポリシーの優先度は以下のように決定します。

1. **[ポリシー]** > **[ポリシー& コンプライアンス]** を開きます。
2. **[アクション]** > **[ポリシーの優先度決定]** を選択します。**[アクション]** が表示されない場合、優先度を必要とする複数のポリシーは存在しません。
3. 矢印を使用し、優先度が高いもの(上)から低いもの(下)へとポリシーを並べます。鍵のアイコンは、ポリシー内のすべてのデバイスの配布設定を編集しない限り、ポリシーの優先度を変更できないことを意味します。
4. **[保存]** をクリックします。

Windowsハードウェアのポリシー

通常のハードウェアインベントリチェックを継続することにより、ハードウェアアイテムがWindows 10デバイスに追加、コピー、削除、置換、または移動されたかを判断します。Windowsハードウェアポリシーでは、監視するハードウェアの種類を指定し、デバイス上のハードウェアに変更が検出されたときに実行するアクションを選択できます。

1. **[ポリシー]** に進みます。
2. **[+追加]** をクリックします。
3. **[Windowsハードウェア]** を選択します。
4. ハードウェアポリシーに名前を付けます。
5. 必要であれば **[+説明を追加]** をクリックして詳細を追加します。
6. **[ハードウェアルールを定義]** セクションで、以下のオプションを構成します。

オプション	説明
ハードウェアオブジェクト	以下のオプションからハードウェアの種類を選択します。 • **BIOS** • **ハードウェアドライブ** • **CD-ROMドライブ** • **プロセッサ** • **物理メモリ**
変更イベント	チェックするハードウェアイベントの種類を選択します。 • **追加** • **コピー** • **削除** • **置換** • **移動**

アクションを選択	実行されるアクションの種類を選択します。
	• **何もしない**
	• **通知を送信**：以下のオプションのいずれかを選択します。
	  • **メール通知を送信** - **[メールメッセージ]** セクションに件名と本文を入力し、通知を送信します。
	  • **プッシュ通知を送信** - プッシュ通知メッセージを入力します。
	  • **両方を送信** - メールメッセージとプッシュ通知メッセージを入力します。
	• **待機**：ドロップダウンリストから待機する日数/時間を選択します。
	  • **日数は1～31**の範囲。
	  • **時間は1～24**の範囲。

	• **検疫** - 以下の検疫オプションのいずれかを選択します。
	任意の追加検疫アクション
	  • **マネージドアプリを隔離** - **[すべてのアプリケーション]** または **[指定したアプリケーション]** を選択します([検索] フィールドでアプリ名を検索して選択) 。
	  • **新規アプリダウンロードをブロック** - デバイスへのアプリのダウンロードをブロックします。**[すべてのアプリケーション]** または **[指定したアプリケーション]** を選択します([検索] フィールドでアプリ名を検索して選択) 。
	  • **構成を削除** - デバイスから構成を削除します。**[すべての構成]** または **[指定した構成]** を選択します([検索] フィールドで構成を検索して選択) 。
	  • **コンテンツを削除** - 配布されたアプリに関連するすべてのコンテンツをデバイスから削除します。
	デフォルトの検疫アクション
	  • **アプリストアへのアクセスをブロック**
	  • **コンテンツストアへのアクセスをブロック**
	  • **AppConnectをブロック**
	  • **AppTunnelをブロック**
	  • **ActiveSyncをブロック**
	• **ブロック**

	• **撤去** このアクションは元に戻せません。 コンプライアンスアクションを追加または削除するには、「プラス」または「マイナス」のアイコンをクリックします。

7. **[次へ]** をクリックします。
8. 以下の配布オプションから1つ選択します。
   - **すべてのデバイス**
   - **デバイスなし(デフォルト)**
   - **カスタム**
9. **[完了]** をクリックします。

管理

管理セクションでは、Ivanti Neurons for MDMポータルからユーザー、デバイス、構成を管理する方法を説明します。以下のセクションは、管理者として実行できるすべてのタスクのリストを含みます。

システム

このセクションは以下のトピックを含みます。

属性

[属性] ページを使用して、次のタスクを実行します。

- ユーザー、デバイス、アプリで記録できる情報のタイプを管理します。
- Ivanti Neurons for MDM で追跡される標準タイプの情報を表示します。

カスタムユーザー属性には、部署または内部 ID といった情報が含まれます。各属性には対応する変数があり、グループのビルドや構成の配布に使用できます。

ユーザールールグループ条件の作成中に、カスタム属性に数値が設定されている場合、Ivanti Neurons for MDMは整数演算をサポートしません。

カスタム属性の作成

手順

1. 管理ポータルにログインします。
2. **[管理]** > **[システム]** > **[属性]** に移動します。
3. **[カスタム属性]** で **[+追加]** をクリックします。
4. **[属性名]** フィールドに属性を意味するテキストを入力します。

   入力したテキストを利用し、**[利用]** フィールド内に対応の変数が作成されます。

5. 以下の **[属性タイプ]** オプションから任意の属性タイプを選択します。
   - **ユーザー**
   - **デバイス**
   - **アプリ**
   - **IDP**(詳細については、「ユーザープロビジョニング-Azure Active Directory 」 ページ1136 または「Ivanti Neurons for MDMとAzure Active Directoryユーザーソースとの接続 」 ページ1223) を参照してください。

6. [属性タイプ] が [デバイス] の場合、次の **[データタイプ]** オプションのいずれかを選択します。
   - **数字**
   - **テキスト**
7. **[追加]** をクリックします。

   作成したカスタムユーザー属性は [属性] ページの **[追加された管理者]** セクションに表示されます。

カスタム属性の組み合わせ ${deviceattribute} + ${custom-attribute} + ${userattribute} + ${Static String} はどんな順序でもサポートされます。

カスタム属性の名前変更

カスタム属性の名前変更により、以下のエンティティで使用されるそのカスタム属性の参照すべての名前が変更されます。

- カスタムポリシー
- ユーザーグループ
- デバイスグループ
- アプリ配布フィルター
- スペース

構成、招待メールテンプレート、ポリシーコンプライアンスオプションにおけるメール/プッシュメッセージなど、他のエンティティにおけるカスタム属性の参照は更新されません。

手順

1. **[追加された管理者]** で、名前を変更したい属性の隣にある **[+編集]** をクリックします。
2. **[属性名]** フィールドに属性の新しい名前を入力します。

   入力したテキストを利用し、**[利用]** フィールド内に対応の変数が作成されます。
3. **[保存]** をクリックします。

カスタム属性の削除

カスタム属性を削除すると、その値はすべての関連ユーザーまたはデバイスから削除されます。元に戻すことはできません。

以下のエンティティのいずれかに使用されているカスタム属性は削除できません。

- カスタムポリシー
- ユーザーグループ
- デバイスグループ
- アプリ配布フィルター
- スペース

カスタム属性を削除する前に、エンティティからカスタム属性を削除してください。

削除したい属性が上記のエンティティで参照されていない場合、属性の隣にある **[削除]** をクリックすると確認のポップアップメッセージが表示されます。アクションを確認し、**[削除]** をクリックします。

システム属性の表示

システム属性は、ユーザーが変数として構成に使用できる定義済みの属性です。詳細な一覧は、[**管理** > **システム** > **属性**] ページの [**システム属性**] セクションに表示されます。システム属性には以下の種類の属性が含まれます。

- ユーザ属性
- デバイス属性
- メールテンプレート属性
- システム属性
- タイムスタンプ属性
- AADカスタムユーザー属性
- ポリシー属性

ユーザ属性

ユーザ属性を使用して、ユーザに関する情報を指定します。

キー	説明
${department}	部署属性 (Active Active Directory が必要)
${edipi}	説明なし
${managedAppleId}	ユーザの管理対象 Apple ID
${sAMAccountName}	sAMAccountName 属性 (Active Directoryが必要)
${userCN}	識別名から共通名 (CN) 属性を抽出 (LDAPが必要)
${userDisplayName}	表示名
${userDN}	識別名 (LDAP が必要)
${userEmailAddressDomain}	メールアドレスのドメイン部分 (@の後)
${userEmailAddressLocalPart}>	メールアドレスのローカル部分 (@の前)
${userEmailAddress}	メールアドレス
${userFirstName}	名
${userLastName}	姓
${userLocale}	ロケール
${userOU}	識別名から組織ユニット (OU) 属性を抽出 (LDAPが必要)
${userREALM}	Kerberos領域情報 (Active Directoryが必要)
${userUIDDomain}	ログインIDのドメイン部分 (@の後)
${userUIDLocalPart}	ログインIDのローカル部分 (@の前)
${userUID}	ログインID(メールアドレス形式)
${userUPN}	userPrincipalName属性 (Active Directoryが必要)

デバイス属性

デバイス属性を使用して、モバイルデバイスに関する情報を指定します。

キー	説明
${clientLastCheckin}	クライアントの最後のチェックイン日 (MDMまたはクライアントの直近のチェックイン)
${deviceAltSN}	代替シリアル番号
${deviceClientDeviceIdentifier}	クライアントアプリケーションに使用される識別子

キー	説明
${deviceGUID}	グローバルで一意のデバイス識別子
${deviceIccIdentifier}	説明なし
${deviceIMEI2}	IMEI2
${deviceIMEI}	IMEI
${deviceIMSI}	IMSI
${deviceLastCheckin}	デバイスの最後のチェックイン日(MDMまたはクライアントの直近のチェックイン)
${deviceMdmChannelId}	内部デバイス識別子
${deviceMdmDeviceIdentifier}	MDMに使用される識別子
${deviceMEIdentifier}	説明なし
${deviceModel}	機種
${deviceName}	デバイス名
${devicePhoneNumber}	デバイス電話番号
${devicePK}	クラスター固有のデバイス識別子
${deviceSN}	シリアル番号
${deviceUDID}	iOS UDID
${deviceWifiMacAddress}	Wi-Fi MACアドレス

カスタム属性を作成し、管理対象のアプリ構成でこの属性を参照しているときに、属性値が更新されると、管理対象のアプリ構成で参照された属性も更新され、管理対象のアプリ構成がもう一度デバイスにプッシュされます。

カスタム属性またはデバイス属性が更新され、構成がデバイスにプッシュされたときは、Androidキオスクのブランディング構成も更新する必要があります。

アプリ属性

アプリ属性を使用して、アプリケーションの情報を指定し、カスタムアプリケーショングループを作成します。

キー	説明
${appAdded}	アプリカタログに日付アプリケーションが追加されました
${appName}	アプリケーションの名
${appOsPlatform}	アプリケーションのオペレーティングシステム
${appPackageId}	アプリケーションのバンドルIDまたはパッケージID
${appSource}	アプリケーションのインポート元のソースを説明します。
${IsVpp}	iOSまたはmacOSアプリケーションがVPPかどうかを説明します

メールテンプレート属性

キー	説明
${policyMessageContent}	説明なし
${policyMessageTitle}	説明なし

タイムスタンプ属性

変数キー	説明
${timestampMS}	現在のタイムスタンプ(エポックからのミリ秒数)

ポリシーテンプレート属性

キー	説明
${nameOfPolicy}	侵害されたポリシー名
${nextAction}	メッセージ送信後に実行される次の階層型コンプライアンスアクション(待機および撤去とは異なる)
${nonComplianceTime}	デバイスがコンプライアンス違反状態の日数
${policyViolationFirstTime}	ポリシー違反が最初にトリガーされた時のタイムスタンプ(UTC DD-MM-YYYY形式)
${ruleConditions}	ルール定義(今表示されているとおりのクエリ文字列)

関連トピック:

- 「ユーザーへのカスタム属性の割り当て」ページ157
- 「デバイスへのカスタム属性の割り当て」ページ274

- 「ユーザーからのカスタム属性の削除」ページ158
- 「デバイスからのカスタム属性の削除」ページ275
- 「変数」ページ471

デバイスクリーンアップ設定

デバイスクリーンアップにより、使用されていないデバイスのデバイスライフサイクルを自動化します。指定した日数の間に接触がなかったデバイスを撤去できます。指定した日数の間、撤去されていたデバイスを、削除できます。[監査証跡] ページには、[デバイスを撤去]、[デバイスを削除]、および [ワイプ済みデバイスを削除] の設定がキャプチャされます。

Android Enterpriseモードのデバイスは、デバイスクリーンアップ設定から除外されます。

前提条件

この設定にアクセスするには、システム管理役割の権限が必要です。

デバイスを撤去

手順

1. **[管理]**> **[システム]** > **[デバイスクリーンアップ]** を開きます。[デバイスクリーンアップ] ページが開きます。
2. **[デバイスを撤去]** を選択します。
3. 「**デバイスを撤去**」表を使用して、詳細を指定します。
4. **[チェックインしていないデバイスのリストを表示]** をクリックします。指定した日数の間にチェックインしていないデバイスのリストが表示されます。
5. **[デバイスを今すぐ撤去]** をクリックするか、またはデバイスの撤去をスケジュールできます。
6. 指定したデバイスがIvanti Neurons for MDM管理ポータルによって撤去されます。
7. **[保存]** をクリックして設定を保存します。
8. (任意) 値を更新した場合、**[リセット]** をクリックすると、設定を初期設定に戻せます。

デバイスを撤去

フィールド	説明
次の日数以上チェックインされていないデバイスを撤去する	日：デフォルトは30日で、許可される最大日数は365日です。
各セッションで撤去するデバイスの最大数	100、500、または1000を選択します(デフォルト - 100) 。
スケジュールに従ってデバイスを自動的に撤去	事前に設定したスケジュールに基づいてデバイスを撤去するには、このチェックボックスを選択します。
撤去のスケジュール構成	次のオプションのいずれかを選択して、撤去の頻度を設定します。 • **毎日** - デバイスを毎日撤去する場合に設定します。 • **毎週** - 撤去を予定する曜日を指定します。 • **毎月** - 毎月の第1日目にデバイスを撤去する場合に設定します。

撤去済みデバイスの削除

手順

1. **[管理]**> **[システム]** > **[デバイスクリーンアップ]** を開きます。[デバイスクリーンアップ] ページが開きます。
2. **[撤去済みデバイスを削除]** を選択します。
3. 「**撤去済みデバイスを削除**」表を使用して、詳細を指定します。
4. **[撤去済みデバイスのリストを表示]** をクリックします。指定した日数の間に撤去されていたデバイスのリストが表示されます。
5. **[撤去済みデバイスを今すぐ削除]** をクリックするか、またはデバイスの削除をスケジュールできます。
6. 指定したデバイスがIvanti Neurons for MDM管理ポータルによって削除されます。
7. **[保存]** をクリックして設定を保存します。
8. (任意) 値を更新した場合、**[リセット]** をクリックすると、設定を初期設定に戻せます。

撤去済みデバイスの削除

フィールド	説明
撤去されてから、次の日数以上経過したデバイスを削除する	日：デフォルトは30日で、許可される最大日数は365日です。
各セクションで削除する撤去デバイスの最大数	100、500、または1000を選択します(デフォルト - 100) 。
スケジュールに従って撤去済みデバイスを自動的に削除	事前に設定したスケジュールに基づいてデバイスを撤去するには、このチェックボックスを選択します。
削除のスケジュール構成	次のオプションのいずれかを選択して、削除の頻度を設定します。 • **毎日** - デバイスを毎日削除する場合に設定します。 • **毎週** - 削除を予定する曜日を指定します。 • **毎月** - 毎月の第1日目に撤去済みデバイスを削除する場合に設定します。

ワイプ済みデバイスの削除

手順

1. **[管理]**> **[システム]** > **[デバイスクリーンアップ]** を開きます。[デバイスクリーンアップ] ページが開きます。
2. **[ワイプ済みデバイスを削除]** を選択します。
3. 「**ワイプ済みデバイスを削除**」表を使用して、詳細を指定します。
4. **[ワイプされたデバイスのリストを表示]** をクリックします。指定した日数の間に撤去されていたデバイスのリストが表示されます。
5. **[ワイプ済みデバイスを今すぐ削除]** をクリックするか、またはワイプ済みデバイスの削除をスケジュールできます。
6. 指定したデバイスがIvanti Neurons for MDM管理ポータルによって削除されます。

7. **[保存]** をクリックして設定を保存します。
8. (任意) 値を更新した場合、**[リセット]** をクリックすると、設定を初期設定に戻せます。

ワイプ済みデバイスの削除

フィールド	説明
ワイプされてから、次の日数以上経過したデバイスを削除する	日：デフォルトは30日で、許可される最大日数は365日です。
各セッションで削除するワイプ済みデバイスの最大数	100、500、または1000を選択します(デフォルト - 100) 。
スケジュールに従ってワイプ済みデバイスを自動的に削除	事前に設定したスケジュールに基づいてワイプ済みデバイスを削除するには、このチェックボックスを選択します。
ワイプ済みの削除のスケジュール構成	次のオプションのいずれかを選択して、削除の頻度を設定します。 • **毎日** - ワイプ済みデバイスを毎日削除する場合に設定します。 • **毎週** - 削除を予定する曜日を指定します。 • **毎月** - 毎月の第1日目にワイプ済みデバイスを削除する場合に設定します。

ワイプ保留中デバイスの削除

手順

1. **[管理]** > **[システム]** > **[デバイスクリーンアップ]** を開きます。[デバイスクリーンアップ] ページが開きます。
2. **[ワイプ保留中デバイスの削除]** を選択します。
3. 「**ワイプ保留中デバイスの削除**」表を使用して、詳細を指定します。
4. **[ワイプ保留中デバイスのリストを表示]** をクリックします。指定した日数の間にワイプされる予定であるデバイスのリストが表示されます。

5. **[ワイプ保留中デバイスを今すぐ削除]** をクリックするか、またはワイプ保留中デバイスの削除をスケジュールできます。
6. 指定したデバイスがIvanti Neurons for MDM管理ポータルによって削除されます。
7. **[保存]** をクリックして設定を保存します。
8. (任意) 値を更新した場合、**[リセット]** をクリックすると、設定を初期設定に戻せます。

ワイプ保留中デバイスの削除

フィールド	説明
ワイプ保留期間が次の日数を超えたデバイスを削除	日：デフォルトは30日で、許可される最大日数は365日です。
各セッションで削除するワイプ保留中デバイスの最大数	100、500、または1000を選択します(デフォルト - 100) 。
スケジュールに従ってワイプ保留中デバイスを自動的に削除	事前に設定したスケジュールに基づいてワイプ済みデバイスを削除するには、このチェックボックスを選択します。
ワイプ保留中の削除のスケジュール構成	次のオプションのいずれかを選択して、削除の頻度を設定します。 • **毎日** - ワイプ保留中デバイスを毎日削除する場合に設定します。 • **毎週** - 削除を予定する曜日を指定します。 • **毎月** - 毎月の第1日目にワイプ保留中デバイスを削除する場合に設定します。

撤去保留中のデバイスの撤去

手順

1. **[管理]**> **[システム]** > **[デバイスクリーンアップ]** を開きます。[デバイスクリーンアップ] ページが開きます。
2. **[撤去保留中のデバイスを撤去]** を選択します。
3. 「**撤去保留中のデバイスを撤去**」表を使用して、詳細を指定します。

4. **[撤去保留中デバイスのリストを表示]** をクリックします。指定した日数の間に撤去される予定であるデバイスのリストが表示されます。
5. **[撤去保留中のデバイスを今すぐ強制撤去]** をクリックするか、または撤去保留中デバイスの撤去をスケジュールできます。
6. 指定したデバイスがIvanti Neurons for MDM管理ポータルによって撤去されます。
7. **[保存]** をクリックして設定を保存します。
8. (任意) 値を更新した場合、**[リセット]** をクリックすると、設定を初期設定に戻せます。

撤去保留中のデバイスの撤去

フィールド	説明
次の日数以上チェックインしていない撤去保留中のデバイスを撤去する	日：デフォルトは30日で、許可される最大日数は365日です。
各セッションで撤去する撤去保留中のデバイスの最大数	100、500、または1000を選択します(デフォルト - 100)。
撤去保留中のデバイスをスケジュールに従って自動的に撤去	事前に設定したスケジュールに基づいて撤去保留中デバイスを撤去するには、このチェックボックスを選択します。
撤去保留中の撤去のスケジュール構成	次のオプションのいずれかを選択して、削除の頻度を設定します。 • **毎日** - 撤去保留中デバイスを毎日撤去する場合に設定します。 • **毎週** - 撤去保留中デバイスの撤去を予定する曜日を指定します。 • **毎月** - 毎月の第1日目に撤去保留中デバイスを撤去する場合に設定します。

GDPRプロファイル

Ivanti Neurons for MDM管理ポータルに [GDPRプロファイル] ページが追加され、ユーザーグループにGDPRプロファイルを割り当てることが可能になりました。GDPRプロファイルは、個々のユーザーではなく、ユーザーグループに対してのみ割り当てることができます。

次の点に注意してください。

- 特定のユーザーグループにGDPRプロファイルを割り当てるには、まずそのGDPRプロファイルを有効化する必要があります。
- GDPRプロファイルを無効化すると、そのユーザーグループに既に割り当てられているプロファイル制限はすべてオフになります。
- GDPRプロファイルを有効化すると、一部のフィールドでは、編集機能が制限されるかまたは無効になります。

GDPRプロファイルを割り当てた後に非表示になるフィールド

GDPRプロファイルを持つユーザーがいる場合、Ivanti Neurons for MDMは、そのユーザーの情報を表示する際に、デフォルトでは次のフィールドを非表示にします。

- **ユーザーID**
- **ユーザー名**
- **Eメールアドレス**
- **シリアル番号**
- **ICCID**
- **IMSI**
- **MEID**
- **IPアドレス**
- **電話番号**
- **IMEI**
- **eSIM識別子**

GDPRプロファイルの有効化

GDPRプロファイルを有効化し、Ivanti Neurons for MDM管理ポータルおよびデバイス上で非表示にする必要のある特定のフィールドを選択できます。

Procedure手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. **[管理]** > **[システム]** > **[GDPRプロファイル]** を開きます。
3. **[有効化]** をクリックします。
4. 編集(鉛筆)アイコンをクリックします。
5. 非表示にする必要のあるフィールドを選択します。
6. **[保存]** をクリックします。選択したフィールドがマスキングされ、その特定のユーザーの値が非表示になります。

ユーザーグループへのGDPRプロファイルの割り当て

GDPRプロファイルを有効化した後、特定のユーザーグループに割り当てることができます。

Procedure手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. **[ユーザー]** > **[ユーザーグループ]** を開きます。
3. リストからユーザーグループを選択します。
4. **[アクション]** ドロップダウンリストをクリックし、**[GDPRプロファイルを割り当てる]** を選択します。その特定のグループの全ユーザーにGDPRプロファイルが割り当てられ、選択されたすべての値が管理ポータルおよび全ユーザーデバイスで非表示になります。

> 管理者は「すべてのユーザー」グループにも属しているため、「すべてのユーザー」グループにはGDPRプロファイルを割り当てないでください。

通知メール

ライセンス: Silver

通知の重要度に応じて通知メールを受信するユーザーのメールアドレスリストを設定できます。

通知メールの機能は任意であり、必要に応じてオンまたはオフにしてください。この機能を利用するにはシステム管理者の役割が必要です。

1. **[管理] > [通知メール]** を選択します。**[通知メール]** ページが表示されます。
2. [通知メール設定] セクションで、**[ON]** をクリックすると通知メール機能が有効になります。
3. **[受信者を追加]** をクリックします。**[受信者を追加]** ウィンドウが表示されます。
4. **[受信者を追加]** のウィンドウで、以下のフィールドを更新します。
   - 受信者のメールID - 通知を送信する必要のある相手のメールIDを入力します。
   - 送信する通知の種類 - チェックボックスを使用して通知の種類を選択します。選択可能な通知の種類は以下のとおりです: **重要な通知**、**警告通知**、**情報通知**。
5. **[OK]** をクリックします。表に設定の詳細が表示されます。
6. **[保存]** をクリックして変更を適用します。

役割管理

役割(ロール)とは、パッケージ化された許可のグループであり、管理ユーザーに一連の許可を付与すると同時に、特定領域の機能の制御を制限するためのものです。Ivanti Neurons for MDMには、割り当て(または編集)可能な一連のシステム役割と、カスタム役割の作成機能があります。Ivanti Neurons for MDM 92以降は、カテゴリーに基づいて特定の許可を検索すると、UIの特定の役割や許可に関連するすべてのオプションが表示されます。依存する許可として追加された許可には、ツールチップが表示されます。

[役割管理]ページとその関連オプションは、Ivanti Neurons for UEMとIvanti Neurons for MDMの両方にアクセスできる集約型テナントでは非表示になります。

2種類の許可があるため、役割も2種類となります。

- **スペース特有の役割** - 許可はスペース-特有であるため、特定のスペースのみに適用されます。スペース内のデバイス管理やアプリ管理がその例です。
- **スペース共通の役割** - 許可は本質的にすべての役割に適用されます。MDM認証やアプリカタログ設定などの、テナントレベルの設定がその例です。

カスタム役割の作成

スペース共通またはスペース特有のカスタム役割を作成できます。許可を選択すると、依存する許可が自動的に選択されます。したがって、カスタム役割を割り当てられたユーザーは、デバイスページかデバイス詳細ページを開いたときに利用可能な特定のアクション(撤去、ワイプなど)のみ実行できます。

[ユーザー登録PINを表示]カスタム役割を適用すると、ユーザーは、自分と同じアクセスレベル、または自分より低い特権を持っている他のユーザーのPINを表示できます。またそれらのユーザーは、他のユーザーのPINを作成することはできません。

新しく作成されたカスタム役割は自動的には誰にも割り当てられません。テナントのスーパー管理者がまず必要な管理ユーザーに割り当て、その管理ユーザーが後で必要に応じて他のユーザーに割り当てます。

手順

1. **[管理]** > **[役割管理]** を開きます。
2. **[+役割を追加]** をクリックします。
3. **[役割を作成]** ページで新しい役割の**名前**を入力してください。

4. (任意) 新しい役割の説明を追加します。
5. **役割の種類**から以下の役割の種類のいずれかを選択します。
   - **スペース共通の役割**
   - **スペース特有の役割**
6. **許可**から必要な詳細許可を選択します。

   管理者とユーザーの権限については以下の表を参照してください。
7. **[保存]** をクリックします。

次の表に、カスタム役割の作成に使用できる許可、役割、属性をリストします。

役割の種類	許可のカテゴリ	詳細許可
スペース共通の役割		
管理		
	カスタム属性を管理	• カスタム属性を追加 • カスタム属性を削除 • カスタム属性を編集 • カスタム属性を表示
	サポート管理者	• サポート管理者を追加 • サポート管理者を削除 • サポート管理者を無効化 • サポート管理者を表示 & ログイン履歴を表示
	認証機関	• 認証機関を追加 • 認証機関を削除
	コネクタ	• Connectorログを追加 • Connectorログを削除 • Connectorを表示 • Connectorを更新

役割の種類	許可のカテゴリ	詳細許可
	LDAP管理	• ユーザー/グループ/OUを追加 • サーバーを追加 • サーバーを参照 • サーバーを削除 • サーバーを検索 • サーバーを同期 • ユーザー/グループ/OUを削除 • サーバーを表示 このセクションのすべてのLDAP権限には [Connectorを表示] の権限が必要です。これらのLDAP権限のいずれかを選択すると、Connectorセクションで自動的に選択されます。
	ライセンス供与の管理	
		ライセンスの表示
ユーザー		

役割の種類	許可のカテゴリ	詳細許可
	ユーザー管理アクション	• ユーザーを表示 • ユーザーを更新 • ユーザーにメッセージを送信 • ユーザーに役割を付加/割り当てる • ユーザーを作成 • ユーザーを削除 • ユーザーを招待 • ユーザー登録PINを表示
	カスタムユーザー属性を指定	• 属性を削除 • 属性を表示 • 属性を追加/編集
	ユーザーグループ	• ユーザーグループを表示 • ユーザーグループを編集 • ユーザーグループに役割を付加/割り当てる • ユーザーグループを作成 • ユーザーグループを削除
デバイス		

役割の種類	許可のカテゴリ	詳細許可
	バルク登録	• 一括登録の作成 • 一括登録の更新 • ユーザを一括登録に割り当て • 一括登録の表示 • 一括登録の削除
スペース特有の役割		
デバイス		

役割の種類	許可のカテゴリ	詳細許可
	デバイスアクション	• デバイスをユーザーに割り当てる • デバイスアクティベーションロックをクリア • デバイスを削除 • デバイス紛失モードを無効化 • デバイス紛失モードを有効化 • デバイス強制チェックイン • デバイスロック • デバイスロック解除 • デバイス強制ログアウト • デバイスシステムアプリを再インストール • デバイスを再起動 • iOSデバイス更新のスケジュールを設定 • デバイスの所有者を解除 • デバイス撤去 • デバイス撤去を取り消し • デバイスをシャットダウン • デバイスの表示 • デバイスをワイプ • デバイスワイプを取り消し

役割の種類	許可のカテゴリ	詳細許可
		• デバイスの OS バージョンを更新 • アップロード経由で一括割り当て
	カスタムデバイス属性を指定	• デバイスカスタム属性を追加/編集 • デバイスカスタム属性を削除 • デバイスカスタム属性を表示 このセクションのすべての [カスタムデバイス属性を指定] の権限にはデバイス読取り権限が必要です。これらの [カスタムデバイス属性を指定] の権限のいずれかを選択すると、[デバイスアクション] セクションで自動的に選択されます。
	デバイス構成	• プロファイルを除外 • プロファイルをプッシュ • 除外プロファイルをプッシュ • エラー時にインストールを再試行
	デバイスグループ	• デバイスグループを追加 • デバイスグループを削除 • デバイスグループを編集 • デバイスグループを表示

役割の種類	許可のカテゴリ	詳細許可
	バルク登録	• 一括登録の作成 • 一括登録の更新 • ユーザを一括登録に割り当て • 一括登録の表示 • 一括登録の削除
	アプリのインベントリ	• アプリインベントリを表示
構成		
	構成	• 構成を表示/エクスポート • 構成を編集/優先度決定 • 構成を追加/複製 • 構成を削除
ポリシー		
	ポリシー	• ポリシーの表示 • ポリシーを編集/優先度決定 • ポリシーを追加/複製 • ポリシーを削除

役割を編集するには、[管理] > [役割管理] ページを開き、その役割の名前に対応する **[アクション]** の編集アイコンをクリックします。ユーザーはスペース共通の役割をスペース特有の役割に(またはその逆にも) 編集できません。

関連トピック:

- ユーザーにカスタム役割を割り当てる方法は役割の割り当てをご覧ください。
- デフォルトの役割リストはユーザーの役割を参照してください。

スペース

このセクションは以 下 のトピックを含 みます。

スペース

ライセンス: Silver

スペースは、管理委譲の目的で統合エンドポイント管理(EMM)システムを個別の管理エンティティに区切るために使われます。組織階層を反映してスペースを作成することも可能です。Ivanti Neurons for MDM は、デフォルトスペースと呼ばれる一括管理エンティティと、委譲スペースと呼ばれる多数の下位管理エンティティによる単一レベルの委譲をサポートします。すべてのUEMシステムはデフォルトスペース付きで作成されています。

[スペース] ページとその関連オプションは、Ivanti Neurons for UEMとIvanti Neurons for MDMの両方にアクセスできる集約型テナントでは非表示になります。

スペースにより、以下のシステムコンポーネントの委譲管理が可能となります。ユーザーとユーザーグループは現時点では委譲できません。

- デバイス
- 設定
- ポリシー
- デバイスグループ
- アプリケーション
- アプリカタログ
- Appleの「Appとブック」トークン

少なくとも1つの委譲スペースを持つテナントで管理者がIvanti Neurons for MDM管理ポータルにログインすると、管理者には管理ポータルログインプロモポップアップが表示されます。プロモポップアップは委譲スペースの作成後、および委譲スペースがすでに作成された後のユーザーログイン時には表示されません。

グローバル/委譲スペース管理者の役割

デフォルトスペースにアクセスする適切な役割を持つ管理者ユーザーは「グローバル管理者」と呼ばれます。デフォルトスペースへのアクセスには、読み取り専用と読み取り/書き込みアクセスがあります。適切な管理者の役割を持つグローバル管理者は、委譲スペースを作成し、それらを管理する「管理者代理」を指定できます。管理者代理は、1つまたは複数の委譲スペースの管理者として指定可能です。

特定の管理者がアクセスできるスペースは、[デバイス] タブと[アプリ] タブの左上角にあるスペース選択用ドロップダウンに表示されます。スペースを閲覧および管理するには、スペースのドロップダウンで必要なスペースに切り替えてください。

グローバル管理者は、デフォルトスペースに加え、すべての委譲スペースを可視化し、制御できます。管理者代理は、グローバル管理者によって指定されたスペースのみ可視化し、制御できます。グローバル管理者は、委譲スペースに対する集中管理権限を持ち、管理者代理は自分が委譲されたスペースを管理する自主権限を持ちます。この自主権限レベルは、委譲が継承されたか、デフォルトスペースからコピーされたかによって決まります。

以下は、さまざまなユーザーの役割と彼らが実行できるタスクです。

委譲スペースにおける継承アプリ

- 委譲時に既存の評価とレビューは継承され、筆者のユーザー名を含め、委譲スペース内でユーザーに表示されます。
- 管理者代理は、継承アプリの評価/レビューを削除できません。
- 管理者代理は、継承アプリの評価/レビューをエクスポートできます。
- 委譲スペースのユーザーは、継承アプリに評価/レビューを追加できます。
- 委譲スペースのユーザーは、筆者のユーザー名を含め、委譲スペースのユーザーが追加した評価/レビューを閲覧できます。

委譲スペースにおけるアプリ(継承ではなく追加)

- グローバル管理者だけが **[アプリ] > [カタログ設定] > [評価とレビュー]** からレビューを有効化または無効化できます。
- 委譲スペースのユーザーは、評価/レビューを追加できます。
- 管理者代理は、同じ委譲スペースのユーザーが追加したレビューを削除できます。
- デフォルトスペースを含め、他の委譲スペースのユーザーは、各委譲スペースのユーザーが追加した評価/レビューを閲覧できません。
- 管理者代理は、すべてのユーザーが追加したレビュー(ユーザー名も含む)をエクスポートできます。

デフォルトスペースにおける委譲アプリ

- グローバル管理者は、委譲スペースのユーザーが追加した評価/レビューを削除できます。
- グローバル管理者は、委譲スペースのユーザーが追加したものを含め、すべての評価/レビューをエクスポートできます。
- デフォルトスペースのユーザーは、委譲スペースのユーザーが追加した評価/レビュー(ユーザー名を含む)を閲覧できます。

委譲スペースの優先度

UEMシステムのデフォルトスペースは、常に優先度が最低になります。他の委譲スペースに対する相対的な優先度は、グローバル管理者が設定し、いつでも変更可能です。委譲スペースは、管理ポータルの[管理]タブにあるスペースページに優先度の高い順に表示されています。

継承またはコピーによる委譲

委譲管理においては、システムコンポーネントが、デフォルトスペースから継承またはコピーされたかどうかが重要な概念となります。

スペースの管理

スペースでは、デバイスグループを指定し、別の管理者に管理させることができます(委譲管理)。スペースの管理者は、スペース内のデバイスに適用される**構成**[1]および**ポリシー**[2]を定義することができます。スペース作成後、各スペースを、関連するまたは適切な管理者に割り当てることができます。既定のスペースを編集または削除することはできません。

ユーザは使用可能なすべてのスペースではなく、割り当てられたスペースのみを表示できます。現時点では、この設定は、**デバイス**、**デバイス グループ**、**アプリ**、**アプリ インベントリ**、**コンテンツ**、**構成**、**ポリシー**、**証明書管理**モジュールにのみ適用されます。これらのモジュールのいずれかの表示中に[スペース]リストから選択したスペースは、そのモジュールに対して管理者が指定した既定の選択内容として保存されます。これらの設定は現在のログインセッションだけではなく、将来のセッションでも保存されます。

作成したスペースは、デフォルトスペースからすべての構成を継承します。したがって、デフォルトパーティション内に後で作成する構成は、その他のスペースにも適用可能です。ただし、既存の構成に加えられた変更は引き継がれません。

作成したスペースは、その時点でデフォルトスペースに存在するポリシーのコピーのみ受け取ります。デフォルトスペース内に後で作成するポリシーは、デフォルトスペースにのみ適用されます。

スペースに含めるデバイスを定義するルールを作成します。これらのルールは、「は次から始まる:」、「は次で終わる:」、「は次を含む:」、「は次を含まない:」、「は次から始まらない:」、「は次で終わらない:」、「は次より小さい:」、「は次より大きい:」、「が次の範囲内:」、「は次と等しい:」、および「は次と等しくない:」演算子を使用してフィルタリングできます。[ANY (OR)] または [ALL (AND)] オプションを使用すればネストでまとめることができます。ルールの精度はルールの最後に表示されるテキストを使用して確認可能です。

以降、ルールビルダーで「ユーザーグループ名」属性が選択されている場合、Ivanti Neurons for MDM Administratorは重複するユーザーグループ数と、重複するグループを識別するGUID番号を表示します。また、このルールの下の表には、重複するユーザーグループのリストと、ユーザーグループ名、GUID、ソース、識別名(DN)などの詳細が表示されます。

ルールは以下によってデバイスを特定します。

[1] collections of settings that you send to devices.

[2] sets of requirements and compliance actions defined for devices.

- AAD登録済み
- APNS対応
- 代替シリアル番号(Androidのみ - デバイス管理者またはデバイス所有者モードのSamsungデバイスに適用)
- Android 5Gネットワークスライシングが有効
- Android仕事用マネージドデバイス非GMSモード(AOSP)有効
- Android 専用デバイス
- Androidエンタープライズ対応
- 仕事用プロファイルを持つAndroidマネージドデバイス
- Android SafetyNet認証タイプ
- Android Work有効
- Android仕事用マネージドデバイス(デバイス所有者)有効
- Android Workプロファイル有効
- 会社所有デバイス上のAndroid仕事用プロファイル有効
- 自動Device Enrollment登録済み
- Autopilot 登録済み
- Azureクライアントステータスコード
- Azureデバイスコンプライアンスレポート時間
- Azureデバイスコンプライアンスステータス
- Azureデバイス識別子
- Sentryによるブロック
- Accessによるブロック
- Bootstrapトークンを利用できます
- バルクプロビジョニングの種類(Apple Configurator、なし、自動Device Enrollment登録済み)

- キャリア
- クライアントの前回のチェックイン
- クライアント登録
- コンプライアンス
- コンプライアンスアクションによるブロック
- 現在の国名(ドロップダウンリストから現在の国名を選択)
- 現在のMCC
- 現在のMNC
- カスタムデバイス属性
- カスタムLDAP属性
- カスタムユーザー属性
- データローミング
- デバイスソース
- デバイスの種類
- 表示名
- 暗号化有効
- 本国名(ドロップダウンリストから現在の本国名を選択)
- ホームMCC
- ホームMNC
- IPアドレス
- キオスクモード
- 最新のチェックイン
- MAM のみ

- 製造者
- マルチユーザーモード
- OS
- OSバージョン
- オーナーシップ
- 電話番号
- 検疫済み
- リカバリロック有効
- ローミング
- Secure Appsステータス
- シリアル番号
- ステータス
- 監視対象
- 補足的ビルドバージョン
- 補足的OS/バージョンエクストラ
- ロック解除トークンを利用できます(iOS)
- User Enrollment登録済み
- ユーザーグループ
- ユーザー名
- 音声ローミング
- macOS個人リカバリキーがエスクローされました
- macOSリカバリキーの種類

これらの規則は**Silver**以上のライセンスでのみ利用可能です。

スペースの作成

手順

1. **[管理]** > **[スペース]** を開きます。
2. **[管理]** をクリックします。
3. **[新規スペースを作成]** をクリックします。
4. **[プレビュー]** をクリックすると、スペースに割り当てられるデバイスを確認できます。
5. スペース内のデバイスが良ければ、**[保存]** をクリックします。

> 削除するには、作成したスペースの削除アイコンをクリックします。

スペースの優先度決定

Ivanti Neurons for MDM は表示順でスペースを評価します。順番を変更するには、スペース定義の右上隅にある矢印をクリックします。

スペースへの管理者割り当て

手順

1. **[ユーザー]** を開きます。
2. 管理者となるユーザーを検索します。
3. ユーザーをクリックして詳細を表示します。
4. **[アクション]** > **[役割の割り当て]** を選択します。
5. **[デバイス管理]** を選択します。
6. **[デバイス管理]** で、この管理者のスペースを選択します。
7. **[完了]** をクリックします。

この管理者がログインすると、割り当てられたスペース内のデバイス、構成、ポリシーのみが表示されます。

構成またはポリシーの複製

構成やポリシーを少しだけ変更する必要がある場合は複製できます。複製した構成やポリシーを異なるデバイスグループに関連づけることも可能です。スペース内ではすべてのポリシーを複製できます。スペース内では、ユーザー提供のID証明書とThreat Defenseを除き、すべての構成を複製できます。以下の構成はデフォルトスペースから他のスペースへも複製可能です。

- iOSの制約
- Webクリップ
- 証明書
- パスコード
- SCEP(iOSとWindows)
- ID証明書(動的生成)

- 構成やポリシーの種類の名前をスペース内で重複させることはできません。構成やポリシーの他のプロパティは複製してかまいません。
- 構成は、管理者がアクセス権を持つすべてのスペースに複製されます。構成を複製するのにグローバル管理者である必要はありません。

構成またはポリシーの複製

手順

1. 複製したいものに応じて **[構成]** または **[ポリシー]** を開きます。
2. 構成またはポリシーのリンクをクリックして詳細を表示します。
3. **[複製]** アイコンをクリックします。
4. ポップアップウィンドウに**名前**と**説明**(任意)を入力します。
5. **[次へ]** をクリックします。
6. 必要に応じて構成やポリシーを修正します。
7. **[次へ]** をクリックします。

8. 配布を構成します。
9. **[完了]** をクリックします。

詳細はスペースの例を参照してください。

スペースの例

このトピックでは、管理者がスペースをどのように利用できるかの例を挙げます。

位置ごとの管理者

ACME, Inc. は北米と欧州に事業所があります。言語およびタイムゾーンの問題から、ACMEは米国内の管理者が北米のデバイスを管理し、ドイツ国内の管理者が欧州のデバイスを管理するようにしたいと考えています。

これらのスペースを設定するために、ACMEは次の変更を行いました。

1. 欧州のユーザ向けにIvanti Neurons for MDM でユーザグループを作成。
2. 北米のユーザー向けのIvanti Neurons for MDM 内にユーザーグループを作成。
3. 以下のルールで欧州のスペースを作成：

   ユーザーグループ＝欧州
4. 以下のルールで北米のスペースを作成：

   ユーザーグループ＝北米
5. 各スペースのデバイス管理の役割を適切な管理者に割り当てる。

ACMEには現在、以下のスペースがあります。

- 欧州
- 北米
- デフォルト

位置ごとOSごとの管理者

ACMEは、Androidのエキスパートのみがデバイスを管理すべきであると考えました。Androidのエキスパートを北米の組織に1名、欧州の組織に1名追加しました。そこで新たに2つのスペースが必要となります。

スペースを追加するため、ACMEは次の変更を行いました。

1. 以下のルールで欧州Androidのスペースを作成：

   ユーザーグループ＝欧州

OS = Android

2. 以下のルールで北米Androidスペースを作成：

   ユーザーグループ＝北米

   OS = Android

3. 各スペースのデバイス管理の役割を適切な管理者に割り当てる。

ACMEには現在、以下のスペースがあります。

- 欧州Android
- 北米Android
- 欧州
- 北米
- デフォルト

エグゼクティブ向け管理者

ACMEのエグゼクティブは、エグゼクティブらは特別な管理者から特別なサービスを受けることを必要としていると判断しました。このリストには最重要のエグゼクティブのみが掲載されます。

このスペースを追加するため、ACMEは次の変更を行いました。

1. 以下のルールでエグゼクティブスペースを作成：

   ユーザー名 = jdoe@acme.com

   ユーザー名 = gkunz@acme.com

   ユーザー名 = prizzo@acme.com

   ユーザー名 = fvanhoff@acme.com

2. このスペースを **[スペース]** ページのリスト最上部に移動。

   そうでなければ、Androidデバイスのエグゼクティブが誤った管理者の担当となってしまいます。

3. スペースのデバイス管理の役割を特別な管理者に割り当てる。

ACMEには現在、以下のスペースがあります。

- エグゼクティブ
- 欧州Android
- 北米Android
- 欧州
- 北米
- デフォルト

その他すべてのデバイスの管理者

ACMEが日本で新たにオフィスを開設する際には、誰かが日本スペースを作成するまで、追加のデバイスがデフォルトスペースの管理者に割り当てられることになります。

デバイスの委 譲

スペースは、デバイスを個 別 の管 理 エンティティに区 切 るために使 われます。スペースのメンバーシップは作 成 するルールによって決 まります。デバイス委 譲 により、グローバル管 理 者 はUEMシステム内 のデバイスを区 切 り、独 立 して管 理 できます。デバイスが委 譲 されると、それらのデバイスへのアクセスは特 定 の管 理 者 代 理 グループに割 り当 てられ、管 理 責 任 が分 散 されます。

委 譲 デバイスはデバイスグループに分 け、各 グループに異 なるカスタム構 成 を適 用 できます。デフォルトスペースや他 のスペースのデバイスに影 響 はありません。

委 譲 デバイスに対 するルールの作 成

スペースに対 して定 義 するルールにより、そのスペースに属 するデバイスが決 まります。デバイスは1つのスペースにしか帰 属 できません。作 成 したスペースのルールに合 わないデバイスは、自 動 的 にデフォルトスペースに属 します。

1. いずれかのルールを満 たしていれば、デバイスをこの定 義 に含 めたいという場 合 は、**[いずれか]** を選 択 します。
2. すべてのルールを満 たしている場 合 にのみデバイスをこの定 義 に含 めたいという場 合 は、**[すべて]** を選 択 します。
3. ドロップダウンから次 のルールの種 類 のうち1つを選 択 します。
   - **カスタムLDAP属 性 :** LDAP属 性 に基 づいたルール。
   - **OS:** デバイスのオペレーティングシステムに基 づく4つのルール。
   - **ユーザーグループ:** デバイスのユーザーグループに基 づく4つのルール(デバイス管 理 サービス内 で定 義) 。
   - **ユーザー名 :** デバイスに関 連 付 けられたユーザー名 に基 づく4つのルール。
4. 選 択 したルールの種 類 の基 準 を定 義 します。
   - **カスタムLDAP属 性 :** LDAP設 定 で構 成 されたカスタムLDAP属 性 の名 前 を入 力 します。
   - **OS:** Android、iOS、macOSまたはWindowsを選 択 します。
   - **ユーザーグループ**:ドロップダウンに表 示 されているユーザーグループの中 から1つ選 択 します。**[ユーザー] > [ユーザーグループ]** でユーザーグループが定 義 されています。
   - **ユーザー名 :** ユーザー名 の種 類 。

5. このスペースに別 のルールを追 加 するには、これまでのルールの隣 の [+] をクリックします。

6. **[プレビュー]** をクリックすると、スペースに割り当 てられるデバイスを確 認 できます。

7. スペース内 のデバイスが良 ければ、**[保 存]** をクリックします。

あるスペースのルールに合 わなくなったデバイスは、条 件 を満 たす次 のスペースに自 動 的 に移 動 されます。既 存 のスペースのルールに合 わないデバイスは、デフォルトスペースに移 動 されます。たとえば、ユーザーをユーザーグループから削 除 すると、そのユーザーのデバイスが別 のスペースに移 動 する場 合 があります。別 のスペースへの移 動 により、ポリシーや構 成 が変 更 される場 合 もあります。

アプリの委譲

アプリ委譲により、グローバル管理者がIvanti Neurons for MDM内のアプリを区切り、独立して管理できます。グローバル管理者は、市販アプリと自社開発アプリを一括して調達および配布すると同時に、委譲スペースによる分離と制御を維持できます。

アプリの一括配布により、グローバル管理者は、アプリ構成とアプリの配布ルールを通じてアプリの管理機能を事前に定義できます。その後、アプリを委譲し、委譲スペースのアプリカタログで提供します。

これで委譲したアプリが、その委譲スペースに属するデバイスのユーザーに配布されます。アプリケーションが委譲されると、それらのアプリケーションへのアクセスは特定の管理者代理グループに割り当てられ、管理責任が分散されます。

アプリケーションを委譲するには、まず1つ以上の委譲スペースを定義する必要があります。委譲したアプリケーションは、すべてのスペースに割り当てられます。アプリ委譲スペースは以下に分類されます。

- デフォルトスペース
- 委譲スペース

委譲スペースへのアプリの追加

グローバル管理者および管理者代理は、委譲スペースにアプリを追加できます。アプリは、追加された委譲スペースのアプリカタログにのみ表示されます。過去に委譲したアプリをデフォルトスペースから委譲スペースに追加しようとすると、エラーが発生します。この場合、まずデフォルトスペースでアプリの継承を無効化すると、委譲スペースに追加できます。詳細は、「構成の操作」ページ424の**「構成の追加」**を参照してください。

委譲スペースにおけるアプリの配布

デフォルトスペースからアプリが委譲されると、配布ルールが継承されます。このアプリは、アプリの配布ルールに適合する委譲スペースに割り当てられたすべてのデバイスに配布されます。

Ivanti Neurons for MDMリリース81以降、グローバル管理者はスペース管理者に、すべてのデバイス向けおよびカスタム配信オプション向けの動的生成ID証明書の編集を委譲できるようになりました。

> 配布の変更は、特定のスペースにのみ適用されます。その他のすべてのスペースは、デフォルトのスペース配布設定を継承します。

詳細は、「構成の操作」ページ424の**「構成の追加」**を参照してください。

サポート管理者

サービスサポートチームがあなたの役割および権限でログインできるように、一時的なサポート管理者を作成します。このユーザーは7日間で自動的に期限切れとなります。あるいは随時アクセス権を停止することができます。サポート管理者を作成すると、サポートチームの問題解決がスムーズに行われるようになります。

サポート管理者の作成

手順

1. **[サポート管理者]** ページで **[サポートユーザーの追加]** をクリックします。
2. **[ユーザーの作成]** をクリックして確定します。

   この手順により、デバイス管理サービスサポートチームにEメールが送信されます。

   サポートチームメンバーが新規アカウントをアクティベーションするまで、**[表示名]** フィールドが「(無効)」と表示されます。最終的な表示名は次のような形式となります。

   support-[ランダムID]-[ユーザ名]@[会社].com

   サポート管理者が作成されたら、**[管理]** > **[サポート管理者]** を選択すると、既存のサポート管理者のリストを直接見ることができます。したがって、追加のサポートユーザーを作成したい場合は、上記の手順2に直接進んでください。

ユーザー履歴の表示

[サポート管理者] ページで **[ユーザー履歴]** をクリックするとサポート管理者のログイン履歴を表示できます。[サポート管理者] ページに表示されるログイン履歴データは過去90日間のデータに限られます。

サポート管理者のアクセス権終了

手順

1. **[サポート管理者]** ページで、削除したいアカウントの右側の **[削除]** リンクをクリックします。
2. プロンプトが表示されたら、**[ユーザーの削除]** をクリックして確定します。

サポート管理者のアクセス権の一時停止

[サポート管理者] ページで、一時停止したいアカウントの右側の **[無効化]** リンクをクリックします。

[管理] > [システム使用通知]

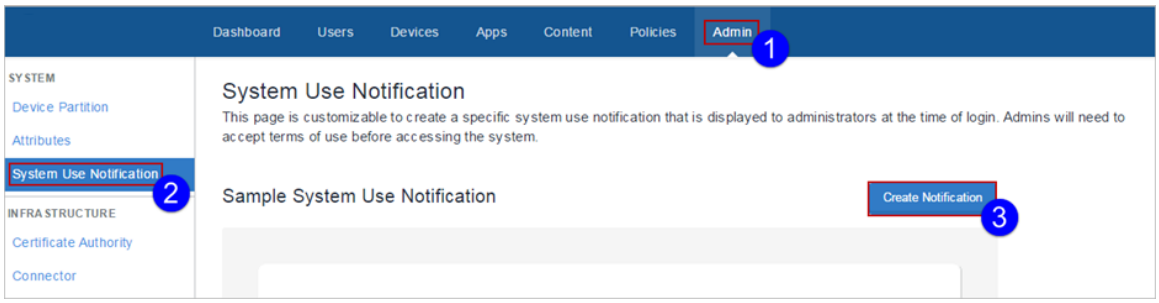
ライセンス: Silver

システム使用通知機能により、ログイン時に管理者に表示されるシステム使用通知をカスタマイズできます。ここで管理者は、システムにアクセスする前に利用規約に同意する必要があります。

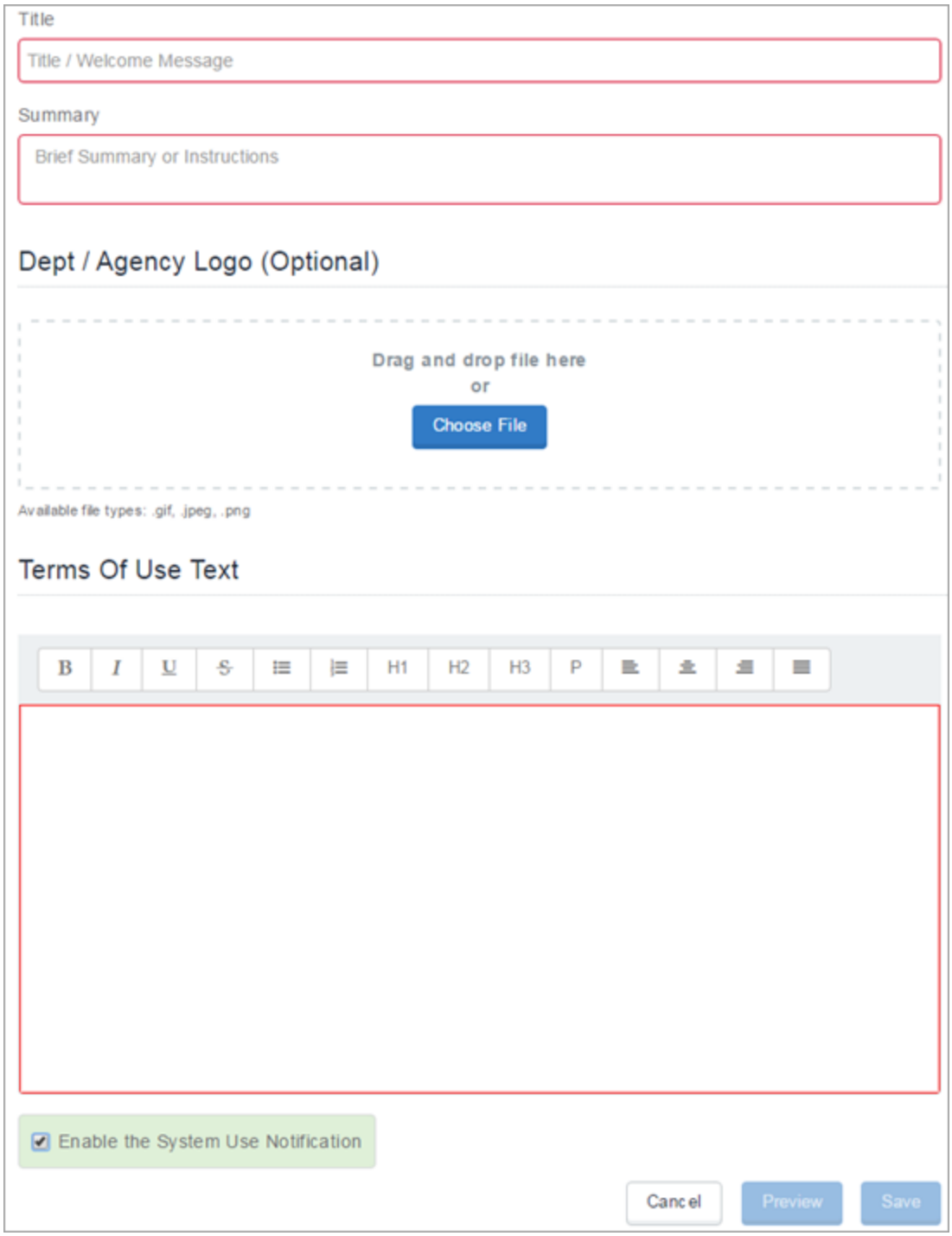
システム使用通知の作成

手順

1. **[管理] > [システム使用通知]** を選択します。
2. **[通知を作成]** をクリックします。



システム使用通知の詳細ページが表示されます。



3. **[タイトル]** フィールドにタイトルを入力します。

4. **[概要]** フィールドに概要または指示を入力します。
5. 必要であればロゴを選択します。
6. **[利用規約のテキスト]** フィールドに利用規約の文章を入力します。これが、管理者がログイン時に同意しなければならない文章です。
7. 通知をオンにするには **[システム使用通知を有効化]** チェックボックスにチェックを入れます。
8. **[プレビュー]** をクリックすると、システム使用通知のプレビューが起動します。
9. システム使用通知が良ければ **[保存]** をクリックします。

インフラ

このセクションは以下のトピックを含みます。

- 「Help@Workライセンス: Platinumサポート : Ivanti Neurons for MDMがサポートするAndroidデバイスとiOSデバイスHelp@Work for Android/iOSでは、AndroidおよびiOSデバイスのユーザーをリモートでサポートできます。Help@Work for Android/iOSは、TeamViewer QuickSupportアプリをベースとしています。Help@Work for Android/iOSを使用するにはTeamViewerのアカウントが必要です。アカウントをお持ちでない場合は、teamviewer.comで詳細をご覧ください。Help@Workでは、ユーザーがボタンを1つ押せばヘルプデスクの担当者と画面を共有できるため、iOS 11.0+/Androidデバイスの問題解決が大幅に楽になります。ユーザーは問題を言葉で説明する時間を節約でき、ITスタッフはトラブルシューティングの効率を高めることができます。MAM Only iOSデバイスではサポートされていません。キオスクモードのAndroidデバイス所有者デバイスではTeamViewerがサポートされています。TeamViewer起動コマンドは、アプリが終了またはデバイスが再起動すると停止します。Androidデバイスでは、Teamviewer QuickSupportアプリがインストールされていない場合、ユーザーはアプリをダウンロードするように求められます。iOSデバイスでは、アプリをアプリカタログを介してプッシュする必要があります。あるいは、デバイスにインストール済みの場合は、マネージドアプリに変換する必要があります。セッションをアプリケーションに適用するには、Teamviewer QuickSupportアプリがフォアグラウンドにある必要があります。無人モードでは、TeamViewer ホスト アプリケーションが必要です。リモートセッションに対応するには、管理者によってインストールされるデスクトップアプリケーションのバージョンが、クライアントデバイスにインストールされるQuicksupportバージョンと互換性を持つ必要があります。Help@Work for Android/iOSの設定以下は、Help@Work for Android/iOSのブランディングと配布に関する1回限りの設定手順です。[管理] タブを開きます。[インフラ] で [Help@Work] をクリックします。Help@WorkにはTeamViewerが必要です。[TeamViewer のアクティブ化] セクションで [今すぐアクティブ化] ボタンをクリックして、[TeamViewer 有人] または [TeamViewer 無人 (Android のみ)] オプションのいずれかを有効にします。TeamViewerライセンス契約の内容を確認し、[同意する] をクリックして続行します。これで企業用ライセンスがアクティブ化されました。TeamViewerはIvantiの顧客を認識し、アクセスを許可します。[アクティベーションの削除] オプションは、TeamViewer を起動した時点で利用可能になります。[TeamViewerの起動] セクションの下にある [アクティベーションの削除] をクリックすると、[アクティベーション削除の確認] ウィンドウが画面に表示されます。[アクティベーションの削除] をクリックすると、TeamViewerのアクティベーションが削除され、次に、サポート対象のすべてのデバイス上のHelp@Work機能が削除されます。ただし、その後のステージで、既存のアカウントまたは別のアカウントを使用してTeamViewerをアクティベートできます。無人モードのTeamViewerアカウントを削除する場合は、無人モードが有効になっている関連デバイスのプロビジョニングを解除する必要があります。関連デバイスのプロビジョニングを解除するには、関連デバイスからのTeamViewerアプリの配布を未配布の状態に戻し、強制チェックインを実行する必要があります。TeamViewerアプリがすべてのデバイスから削除されたことを確認してから、アカウントのバインディングを管理コンソールから削除します。TeamViewerアプリがすべてのデバイスから削除されたことを確認してから、アカウントのバインディングを管理コンソールから削除します。標準的なアプリ配布ワークフローを使用してリモートセッションを開始したい場合、TeamViewerアプリをユーザーに配布します。これは有人および無人モードに固有です。管理者がデバイスを制御する場合は、TeamViewer のユニバーサル アドオンまたは OEM/モデル固有のアドオンもデバイスに配布する必要があります。手順については、アプリ構成をご参照ください。Help@Work for Android/iOSを使用したリモート

セッションの開始Help@Work for Android/iOSの典型的なセッションは、エンドユーザーのヘルプ要請から始まります。ユーザーのデバイスでHelp@Workセッションを開始する手順は以下のとおりです。Ivanti Neurons for MDM で [デバイス] に移動します。[デバイスリスト] ページで、サポートが必要なデバイスをクリックします。[アクション] メニューから、Androidデバイスの場合は [TeamViewerリモート制御を開始]、iOSデバイスの場合は [リモートディスプレイ] をクリックします。2つのオプションが表示されます。有人モード (既定) - このオプションでは、TeamViewer Quick Support アプリケーションをインストールし、ターゲット デバイスでホワイトリストに追加する必要があります。無人モード (Android のみ) - このオプションでは、TeamViewer Host アプリケーションをインストールし、ターゲット デバイスでホワイトリストに追加する必要があります。ホスト名をホワイトリストに入れる必要がある場合や、コンテンツのセキュリティポリシーをオーバーライドする必要がある場合は、サポートチームまでお問い合わせください。無人モード オプションはキオスクモードでも動作します。[TeamViewer 統合] ページから有効にします。無人リモート制御には、デバイスに TeamViewer ホスト アプリケーションをインストールし、デバイスでワンタイム認証を設定して、MI アドオンライセンスを取得する必要があります。ワンタイム アクティベーションの場合、TeamViewer ホストアプリが初めてインストールされ起動したときにアクセス権プロンプトが表示されます。必要に応じて、管理者は、インストール後に、「自動起動 (管理対象のアプリ構成の設定)」TeamViewer アプリを使用できます。ライセンス数は TeamViewer ホスト アプリケーション配布に基づいて計算されます。TeamViewer ホスト アプリケーションがデバイスに配布される場合、1つの無人リモート ホスト セッション ライセンスが使用されます。TeamViewer ホストアプリのほかに、他のアドオンアプリが必要になる場合があります。その場合は、キオスクまたは共有キオスクモードで許可してください。デバイスモデルやメーカーによっては、他のアドオンが必要になる場合もあります。Google Pixel デバイスでは、この権限付与が永続せず、セッションごとに権限の同意が必要です。管理者が有効なTeamViewerトークンを持っている場合、デスクトップクライアントがデバイスのサポートセッションを開始します。持っていない場合、管理者がTeamViewerにログインし、許可を受ける必要があります。削除セッションをすばやく開始するために、管理者は事前にデスクトップアプリケーションにログインできます。TeamViewerのインストールユーザーのリモートデバイスにアクセスし、サポートを提供するには、TeamViewerアプリをデスクトップにインストールします。TeamViewerをインストールするには：Mac、Windows、Androidに対応するTeamViewerフルバージョンのインストールパッケージを以下からダウンロードします。https://www.teamviewer.com/ja/download/ TeamViewerインストールプログラムを起動します。[基本インストール] を選択します。[企業/商用] を選択します。[同意する - 終了] をクリックします。TeamViewerアカウントの取得TeamViewerを利用してサポートを提供するには、TeamViewerアカウントが必要です。TeamViewerアカウントの取得方法は以下のとおりです。https://login.teamviewer.com/を開きます。Eメールアドレス、名前、パスワードを入力します。[登録] をクリックします。2番目の手順で入力したメールアカウントを使用し、TeamViewerアカウントのアクティブ化メールを受信します。メールの指示に従い、TeamViewerアカウントをアクティブ化します。TeamViewerセッションIDの確認TeamViewerは、管理者のコンピューターとユーザーのモバイルデバイスの間に接続を確立すると、セッションIDを生成します。生成されたセッションIDは、マネージドアプリ構成を使用してIvanti Neurons for MDMからTeamViewer QuickSupportアプリに渡されます。その後、アプリがそのセッションIDを使用してデバイス上のTeamViewerクライアントを呼び出します。iOSの場合、セッションIDは30分後に期

限 切 れになります。ユーザーはTeamViewer EULAへの同 意 を求 められます。 」ページ1125

- 「インフラID」ページ1129

- 「LDAPサーバーの構成ライセンス：SilverLDAPサーバーとConnectorを構成すると、企業ディレクトリからユーザーやグループをインポートできます。少なくとも1つのConnectorをインストールした後に、1つ以上のLDAPサーバーを追加できます。LDAPサーバーを追加すると、次の項目が構成されることになります。LDAPサーバーへの接続ターゲットディレクトリのデータを表示するために必要な検索語インポートするディレクトリの部分ディレクトリの選択した部分に自動的にユーザーを招待するかどうか。LDAPサーバーの追加後、このページに戻りLDAPサーバー情報の編集または選択したLDAPユーザーの変更を行うことができます。LDAPユーザーの構成後、LDAPユーザーをインポートする必要があります。LDAPユーザーのインポートをご覧ください。LDAPユーザー名は、ローカルユーザー名と同様、グローバルに一意である必要があります。ユーザーが同じユーザー名でローカルアカウントをすでに持っていないか、または、2件以上のテナントを持つ組織の場合はユーザー名がすでに別のテナントに関連付けられていないか、確認してください。LDAPサーバーの追加手順[+サーバーを追加]をクリックします。次の情報を入力します。設定操作内容名前このサーバーを識別する名前を入力します。説明このサーバーの目的を明示する説明を入力します。ディレクトリURLディレクトリのURLを入力します。以下のいずれかの形式を使用してください。ldap://IPアドレスまたはldaps://IPアドレスまたは例：ldap://myserver1.mycompany.com:389ユーザーID次の特徴を持つアカウントのユーザーIDを入力します。LDAPサーバーによって管理されているLDAPサーバーをバインドし、ユーザー、グループ、組織単位のサブツリーを検索できるこれは通常、ディレクトリ管理者の認証情報(DN、つまり識別名、とパスワード)を有するアカウントです。パスワードアカウントのパスワードを入力します。パスワードの確認アカウントのパスワードを再入力します。ディレクトリ種類サポートされているディレクトリのリストからディレクトリの種類を選択します。Microsoft Active DirectoryLDAPを開くその他(OpenLDAP対応)[接続をテストして続行]をクリックします。この手順により、ここまで入力した情報が検証されます。情報が有効であると認められると、サービスはLDAPの命名コンテキストを読み出し、それを使用して次ページのいくつかのフィールドに入力します。LDAP URLに接続できなくても、次の手順に進めます。ただし、接続が解決されるまで機能が制限される場合があります。残りの設定を完了させます。設定操作内容ディレクトリフェイルオーバーのURLセカンダリディレクトリのURLを入力します。次のフォーマットを使用します。ldap://IPアドレスまたは例：ldap://myserver2.mycompany.com:389同期間隔LDAPサーバーからLDAPデータを同期する間隔を入力します。デフォルト値は15分です。ターゲットのLDAPデータをすべて正常に同期し終わり、LDAP設定がニーズに合っていることを確認したら、この間隔を増やすことを検討してください。同期放棄を有効化リロードされたデータセットが大幅に減少している場合は、LDAP同期データを自動的に破棄するという設定を選択します。このオプションは、LDAPシステムの部分的な異常動作によってサービスに故障の原因となる不必要なアップデートが発生したり、登録済みのデバイスから構成が削除されるといった状況を防ぐものです。LDAP設定またはLDAPサーバーに大幅な変更を加える予定がある場合は、このオプションが選択されていないことを確認してください。このLDAPサーバーを有効化このLDAPサーバーをサービスで使用するという設定を選択します。このLDAPサーバーを撤去するか、サービス停止にする場合は、この設定を解除します。セカンドLDAPサーバーに対する構成済みのフェイルオーバーによりこのサーバーが自動的に置き換えられますが、このオプションを利用すると、事前に計画を立て、フェイルオーバー中の短時間の接続不能状態を回避することができます。インポートされたユーザーを自動的に招待するLDAPサーバーからインポートされたユーザーに自動的に招待状を送る場合に選択します。CA

証明書をアップロード[ファイルを選択]をクリックし、このLDAPサーバーにインストールされているCA発行のTLS証明書ををアップロードします。CA証明書は複数アップロードできます。参照元追跡マルチフォレストのドメインを使用している場合のみ該当します。このオプションは、要求されたオブジェクトのコピーがターゲットのドメインコントローラにない場合に、別のドメインコントローラを使用するかどうかを示します。参照元を使用したい場合は[フォロー]を選択します。別のドメインコントローラを使用しない場合は[無視]を選択します。[スロー]も現在のところ[無視]と同じ効果を持ちます。[フォロー]を選択するとLDAP認証が遅くなります。検索結果のタイムアウトLDAPサーバーから同期したデータの閲覧時にパフォーマンスの問題が発生したり、結果が不完全であったりする場合には、このタイムアウトの値を増やします。検索結果数LDAPサーバーから一度に返すべきレコードの最大数を設定します。パフォーマンス改善のためにこの設定の変更が必要となるようなシナリオは以下のとおりです。LDAPサーバーが非常に遠方にあるか、待ち時間の長いリンクの先にある場合。この場合は、検索結果が大きければ、小さな検索結果よりも読み出しに時間がかかるため、小さなセットを定義することで、更新されたデータのサブセットをより迅速に表示できるようになります。LDAPの規模が大きく、毎回の検索で膨大な結果セットが返される場合。この場合は、パフォーマンスに問題がなければ、より大きな結果セットを定義すると、少ない検索回数ですべてのデータを返すことができるようになります。[次へ]をクリックします。次のガイドラインを利用して、LDAPサーバーとの統合を構成します。設定操作内容グループメンバー形式[DN]または[UID]を選択し、検索で識別名とユーザーIDのいずれを使うかを示します。OU検索属性組織単位レベルでの検索基準を指定します。ベースDN検索のrootとしたい、あるいはそこから検索を始めたいレベルの識別名を入力します。この選択により他のフィールドのデフォルト値が決まりますが、それらは必要に応じて変更することができます。オブジェクトGUID必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびOU名の変更を越えて組織単位を一意に識別する属性です。属性名必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。説明必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。属性DN必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。フィルタの検索必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。範囲を検索ターゲットに対するLDAPの階層の部分を選択します。ベース(検索ベースエントリのみのレベル) ワンレベル(検索ベースの下のレベル) サブツリー(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー) ユーザー検索属性任意のディレクトリレベルでのユーザー検索のための基準を指定します。ベースDN検索を始めるレベルの識別名を入力します。属性UID必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。オブジェクトGUID必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびユーザー名の変更を越えてユーザーを一意に識別する属性です。属性DN必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。名必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。性必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。表示名必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。Eメールアドレス必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。プリンシパル名必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。ロケール必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。所属メンバー必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。フィルタの検索必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更しま

す。範囲を検索ターゲットに対するLDAPの階層の部分を選択します。ベース(検索ベースエントリのみのレベル) ワンレベル(検索ベースの下のレベル) サブツリー(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー) 管理対象Apple IDLDAPユーザーの管理対象Apple IDの同期を選択します。なしパターン - ユーザーのメールアドレスuserUPN任意で[「appleid」サブドメインを含める] オプションを選択し、既存のApple IDとの競合を避けます。+カスタム属性の追加(オプション) ディレクトリサービスからデバイス管理に適用したいカスタムユーザー属性を7つまで指定します。これにより、各属性は、変数をサポートする構成フィールドの${attributeName}によって参照されます。重要:このオプションを使用するには、LDAPサーバー全体を通じてカスタム属性を一貫して実装しておく必要があります。実装に含まれるLDAPサーバーの1つがこの属性を使用していない場合、この属性に依存する機能が意図通りに機能しないことがあります。グループ検索属性 ベースDN検索を始めるレベルの識別名を入力します。オブジェクトGUID必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびグループ名の変更を越えてグループを一意に識別する属性です。属性DN必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。属性名必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。説明必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。メンバー必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。フィルタの検索必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。範囲を検索ターゲットに対するLDAPの階層の部分を選択します。ベース(検索ベースエントリのみのレベル) ワンレベル(検索ベースの下のレベル) サブツリー(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー) [参照] または [検索] をクリックします。構成により想定されたデータが返されていることを確認します。ディレクトリ内で既知の項目を参照または検索することにより、これを実行できます。[次へ] をクリックします。カスタムLDAP属性の削除カスタムLDAP属性を削除し、その値を関連ユーザー/デバイスから削除します。手順[管理] > [属性] を開きます。[カスタム属性] セクションで、削除したいLDAP属性の隣にある [削除] リンクをクリックします。確認ウィンドウが表示されます。[削除] をクリックして削除を確定します。[削除] ボタンはデフォルトで無効化されています。[カスタム属性の削除が元に戻せないことを理解します。] オプションのチェックボックスを選択し、[削除] ボタンを有効化してください。LDAPサーバー情報の編集手順[管理] > [LDAP] を開きます。LDAPサーバーエントリの [アクション] 列から [編集] アイコンを選択し、[LDAPサーバーに接続] ページを表示させます。必要な変更を施します。[接続をテストして続行] をクリックします。LDAP URLに接続できなくても、次の手順に進んでかまいません。ただし、接続が解決されるまで機能が制限される場合があります。[参照] または [検索] をクリックします。構成により想定されたデータが返されていることを確認します。ディレクトリ内で既知の項目を参照または検索することにより、これを実行できます。[完了] をクリックします。LDAPユーザーのインポート手順[ユーザー] を開きます。[+追加] > [LDAPからユーザーを招待] をクリックします。LDAPサーバーエントリ中の [ユーザーを選択] をクリックします。[LDAPユーザーを追加] ページで、ユーザー、グループ、OUの名前を検索フィールドを入力します。新規ユーザーやグループを追加するには、追加したいエントリの横にある [+追加] をクリックします。[次へ] をクリックします。招待状を送信するかどうかを選択します。誰も招待しない後で招待を送信するには、[ユーザ] > [ユーザ] へ進み、[アクション] > [招待を送信] を選択して招待を送信します。すべて招待 [完了] をクリックします。選択したユーザー、グループ、組織単位の更新手順[管理] > [LDAP] を開きます。LDAPサーバーエントリの [アクション] カラムから [ユーザーを管理] アイコンを

選択し、[LDAPユーザーを追加] ページを表示します。新規ユーザーやグループを追加するには、検索フィールドにユーザー名またはグループ名を入力します。追加したいエントリの横にある [+追加] をクリックします。ユーザー、グループ、OUを削除するには、削除したいエントリの横にある削除アイコンをクリックします。[完了] をクリックします。LDAP同期放棄通知の有効化LDAP同期放棄通知の有効化により、LDAP環境への予期しない大規模な変更による機能停止が防止されます。手順[管理] > [LDAP] を開きます。LDAPサーバーエントリの [アクション] 列から [編集] アイコンを選択し、[LDAPサーバーに接続] ページを表示させます。[同期放棄を有効化] チェックボックスをオンにします。同期放棄を実行する基準となるリロード済みLDAPデータの割合を入力します。[接続をテストして続行] をクリックします。LDAP URLに接続できなくても、次の手順に進めます。ただし、接続が解決されるまで機能が制限される場合があります。[完了] をクリックします。LDAPサーバーエントリ中の [今すぐ同期] アイコンをクリックします。LDAP から Ivanti Neurons for MDM へ同期される変更が、所定の放棄割合を上回る場合、警告通知が生成されます。変更が設定した割合を再び下回った場合は、通知が解除されます。送信基準Severity (重大度)通知の種類コンポーネントの種類コンポーネントLDAP同期放棄警告データ同期LDAPLDAPサーバー名LDAP同期復元情報データ同期LDAPLDAPサーバー名部分的同期放棄は、1つ以上のユーザーレコードがLDAPからの同期に失敗した場合に生成されます。この場合、同期できなかったユーザーのリストがCSVファイルとして添付されます。ユーザーが属性の不足によって放棄された場合は、欠けている属性のリストもエクスポートされたCSVファイルに含まれます。LDAPサーバーからの変更の同期 [LDAP] ページで、LDAPサーバーエントリ中の [今すぐ同期] アイコンをクリックします。LDAPSサーバーへの接続に関するトラブルシューティングLDAPS(LDAP over SSL) サーバーへの接続に問題が発生した場合は、証明書に問題がある可能性があります。問題を解消するには: LDAPSサーバー上で自己署名証明書を使用していないことを確認してください。LDAPS証明書の有効期限切れ、無効化がないか確認してください。また、ホスト名の不一致がないか確認してください。確認後、自動LDAP同期を待つか、LDAPサーバーエントリ中の [管理] > [LDAP] > [今すぐ同期] アイコンを使用して手動で同期します。[LDAP] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。システム管理読み取り専用システム 」ページ1146

- 「[Sentry]」ページ1157

Access

対象：iOSおよびAndroidデバイス。

Accessは、あらゆるデバイスやアプリでシームレスで生産的なユーザー体験を実現しながら、ビジネスデータのセキュリティを確保します。また、ユーザーがセキュアでないデバイス、アプリ、クラウドサービスから企業向けクラウドサービスにアクセスできないようデータ境界を確立します。

最新ドキュメンテーション

Accessの詳細とAccessの設定方法は、製品ドキュメンテーションから [Access] をクリックしてください。使用中のAccessバージョンに対応する説明書を選択します。

アプリリスト

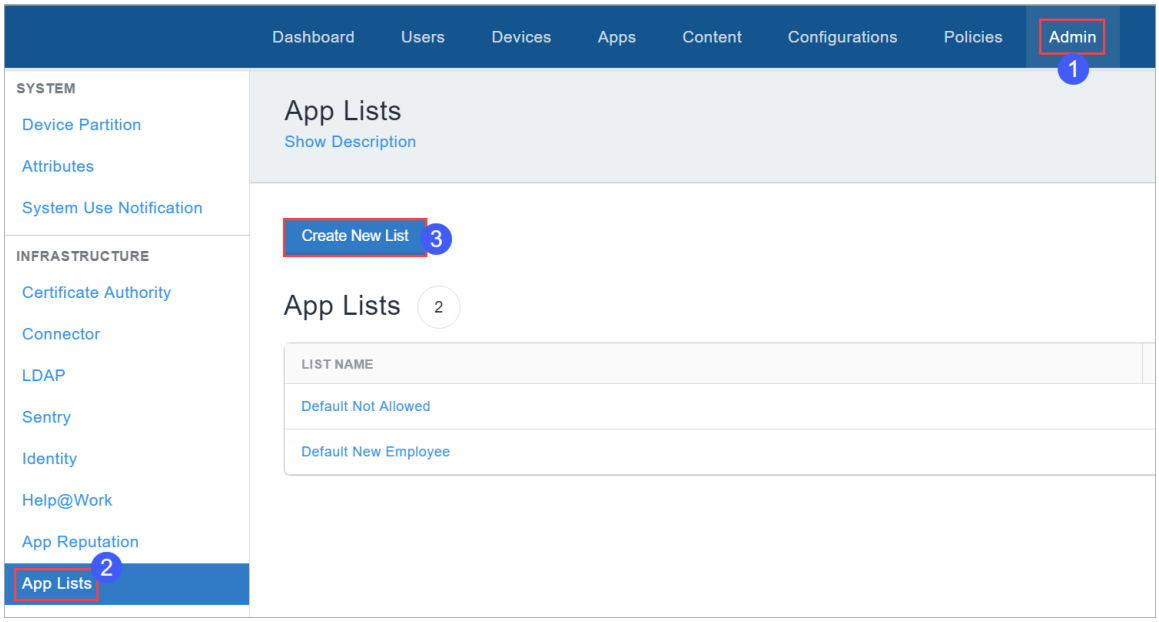
ライセンス: Silver

許可されたアプリポリシーで、必須アプリ、許可リストアプリ、ブロックリストアプリのリストを作成し、デバイスにインストールされたアプリがアプリリストの要件を満たさない場合に実行するアクションを指定できます。許可されたアプリポリシーで参照されている可能性があるため、いったん作成したアプリリストは編集できません。許可されたアプリポリシーに参照されているアプリリストを削除することもできません。

アプリリストの作成

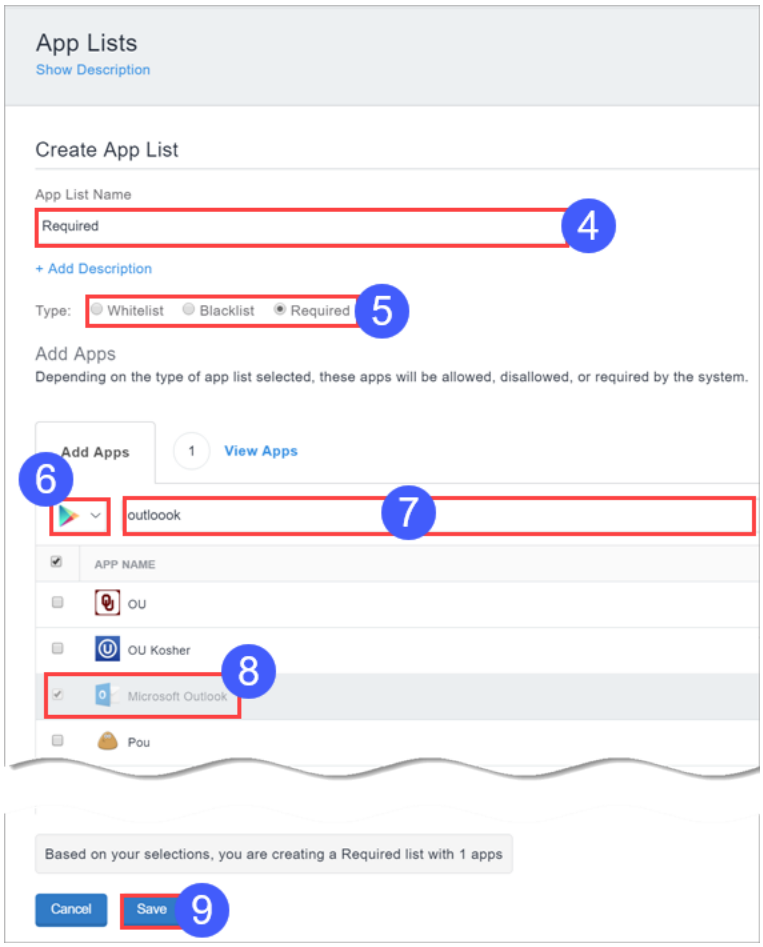
手順

1. **[管理]** をクリックします。



2. **[アプリリスト]** をクリックします。

3. **[新規リストを作成]** をクリックします。



4. リストの名前を設定します。
5. リストの種類を **[許可リスト]**、**[ブロックリスト]**、**[必須]** から選択します。
6. アプリの種類を **[App Store]**、**[OS Xストア]**、**[Google Play]**、**[アプリカタログ]** から選択します。
7. 検索基準を入力して選択肢を絞り込みます。
8. チェックボックスを利用してアプリを選択します。複数の検索基準を使用したり、複数のチェックボックスを有効にしたりすることも可能です。

   [アプリを表示] タブをクリックすると、これまでに選択したアプリのリストが表示されます。
9. **[保存]** をクリックします。

これで許可されたアプリポリシーを構成する際に、このリストを使用できます。

[アプリリスト] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

監査証跡のエクスポート

監査証跡のエクスポートとは、すべての監査証跡情報を特定のサーバーロケーションにエクスポートおよびアップロードする機能です。サーバーはデフォルトポートからアクセスできる必要があります。ユーザーは監査証跡エクスポート設定から、監査証跡のアーカイブを特定のロケーションに毎日自動的にアップロードするよう設定可能です。

監査証跡のエクスポートは、LinuxベースおよびWindowsベースのSFTPサーバーでのみ可能です。

監査証跡エクスポート設定を構成するには:

1. **[管理]** > **[インフラストラクチャ]** > **[監査証跡]** を選択します。**[監査証跡]** ページが表示されます。
2. **[監査証跡]** ページで **[ON]** をクリックし、監査証跡のエクスポートを有効化します。

   [エクスポート] セクションで、以下のフィールドを更新します。

機能	説明
エクスポートの形式	監査証跡をエクスポートする形式を以下から選択します。 • **JSON** • **CEF**(Common Event Format) CEFログメッセージは以下のデフォルト値を含みます。 • バージョン: CEFバージョン番号。現在サポートされているバージョンはv25です。 • デバイス ベンダー: Ivanti Inc • デバイス製品: Ivanti Neurons for MDM • デバイスバージョン: イベント生成時点で最新の Ivanti Neurons for MDM バージョン • デバイスイベントクラスID: 証跡に固有のエンティティID • 名前: エンティティ名と証跡ごとのアクション 例: プロモーション配布構成設定の作成 • 重大度: イベントの重要性を指定。例: 低 CEFログメッセージには、以下のキーと値のペアを集めた拡張フィールドもあります。 • CS1、CS1Label: createdAt、entityType、entityName、actionTypeなどの監査証跡メタデータ • CS2、CS2Label: 行為者情報 • CS3、CS3Label: アクション状態の前 • CS4、CS4Label: アクション状態の後 CEFエクスポートでは、いずれかのフィールド(CS3やCS4のキー) が所定の制限値を超えると、実際の値の代わりに「Value for this key exceeds mapped dictionary key allowed length(このキーの値は対応の辞書キーに許可された長さを超えています) 」のテキストが入ります。

機能	説明
サーバー	監査証跡をエクスポートするサーバー名を入力します。
ユーザー	サーバーにログインするユーザー名を入力します。
パスワード	サーバーログインパスワードを入力します。
サーバーパス	サーバーのパスを入力し、サーバーに所定のパスが存在することを確認します。例：/Users/Test/Export
キー交換アルゴリズム	送信用SFTP構成の監査ログをエクスポートするためのキー交換アルゴリズムを選択します。 デフォルトでは次のキー交換アルゴリズムが選択されています。 • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **diffie-hellman-group-exchange-sha256**（デフォルト選択）
暗号化方式	送信用SFTP構成の監査ログをエクスポートするための暗号化方式を選択します。デフォルトでは次の暗号化方式が選択されています。 • **aes128-ctr** • **aes192-ctr** • **aes256-ctr**（デフォルト選択）
HMAC	送信用SFTP構成の監査ログをエクスポートするためのHMACアルゴリズムのリストを選択します。 デフォルトでは**hmac-sha1**がHMACアルゴリズムに選択されています。

上記に挙げたフィールドは、構成済みの場合、読み取り専用になっています。構成済みのフィールドを編集するには、**[編集]**ボタンをクリックします。管理者がすでにSFTPエクスポートを構成している場合、アップグレードの後はすべてのキーアルゴリズムが選択されています。

3. サーバー接続をテストし、監査証跡エクスポートの構成を保存するには、**[接続をテストして保存]**をクリックします。

アーカイブに保存された監査証跡ファイルは、JSON形式で.zipファイルになっています。

すべてのフィールドの構成設定を確認した上で、監査証跡エクスポート設定を保存してください。無効な値がフィールドに入力されている場合はエラーメッセージが表示されます。

証明書管理

ライセンス：Silver

証明書認証の利用は、モバイルデバイスのセキュリティを確保する効果的な方法です。証明書は、パスワードよりもセキュリティ効果が高く、1つの認証情報でVPN、無線ネットワーク、Eメールなどを保護することができます。組織が外部証明機関にアクセスする場合、Connectorを利用してアクセスすることができます。組織が認証機関へのアクセス権を持たない場合、Ivanti Neurons for MDMを認証機関として利用することができます。また、別の証明書機関に対する仲介証明書機関としても利用できます。Ivanti Neurons for MDMが生成した証明書は自己署名証明書と呼ばれます。

- 新しいID証明書を作成する際、SHA-1証明書は使用できなくなりました。他のアルゴリズムを選択してください。証明書を更新する際、旧い証明書がSHA-1を使用していれば、同じSHA-1アルゴリズムを使用可能です。旧い証明書がSHA-1より新しいアルゴリズムを使用している場合、SHA-1に戻すことはできません。
- ローカルまたは外部認証機関の構成中に **[Ivanti Neurons for MDMにIDをキャッシュ]** オプションを選択し、Ivanti Neurons for MDMサービスに証明書を保存します。必要の都度、キャッシュをクリアして証明書を生成します。
- 既存の証明書の編集中に、必要に応じて **[アクション]** メニューから **[キャッシュした証明書をクリアし、最近更新した新しい証明書を発行]** オプションを選択してください。キャッシュされていない証明書は自動的に再発行されます。
- システム効率を高めるには、First In First Out (FIFO) キューを使用し、管理者が作成した構成の証明書をオフラインで生成します。構成をオフラインで生成する間、構成状態は、**デバイス詳細** ページの **[構成]** タブにある **[ステータス]** 列で **[証明書生成保留中]** となります。証明書が生成されると、構成は **[インストール保留中]** 状態に移行し、自動強制チェックインを通じて証明書とともにデバイスにプッシュされます。
- DigiCert PKIプラットフォームまたはGlobalSignの社外認証機関によって署名された証明書を含め、すべての認証機関の証明書は、デバイスの撤去、ワイプ、証明書の再生成時に取り消されます。

管理者は、スマートカードログオンやカスタムオブジェクトID(OID)用のIvanti Neurons for MDM証明書を生成することができます。以下の認証オプションに対応する証明書を生成可能です。

- クライアント認証 - デフォルトで有効
- IPSEC – 任意、管理者が有効化
- スマートカードログオン – 任意、管理者が有効化
- カスタムOID – 任意、管理者が有効化

この機能は以下の認証機関にのみ対応します:

- ローカル証明書機関
- 仲介認証機関
- 外部認証機関 - NDESサーバー内でCAテンプレートのアプリケーションポリシーを設定し、IPSEC、スマートカードログオン、カスタムOIDをサポートします。

デバイス管理者モード、アプリステーションモード、またはその他の非Android Enterpriseモードにおいて、Samsung APIを使用しているSamsungデバイスでは、証明書管理はサポートされません。Samsungの推奨に基づいて、Androidキーストアへの移行を検証することをお勧めします。

詳細については、「証明書構成」ページ503を参照してください。

オンプレミスのSCEP認証機関への接続

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. Connectorをインストールし構成します(**[管理]** > **[Connector]**) 。詳細については、「コネクタ」ページ1119 をご参照ください。
3. **[管理]** > **[インフラストラクチャ]** > **[証明書管理]** を開きます。
4. **[認証機関]** セクションの下で **[追加]** セクションをクリックします。
5. **[オンプレミスのSCEP認証機関を追加]** を選択し、**[続行]** をクリックします。
6. この構成を識別する名前に入力します。
7. 次の認証機関の種類から1つを選択します。
   - Microsoft
   - EJBCA

- 汎用SCEPサーバー
  汎用SCEPサーバーオプションは、静的チャレンジパスワードを持つほとんどのSCEPサーバーで利用できます。

8. 表示されたフォームに入力します。
9. **[完了]** をクリックします。

外部認証機関の作成

第三者の認証機関を使用したい場合は、このオプションを選択してください。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで **[追加]** をクリックします。
2. [認証機関を追加] ページの [外部認証機関を作成] で **[続行]** をクリックします。
3. 外部認証機関としてGlobalSignまたはDigiCert PKIプラットフォームを選択します。
4. 表示されるフォームの残りのフィールドに入力します。
5. **[完了]** をクリックします。

外部認証機関の証明書の表示

証明書の詳細を表示させ、この認証機関の中間/オルタネートルート証明書をアップロードして保存済みの既存証明書と置き換えることができます。

手順

1. **[証明書管理]** ページの **[認証機関]** で、外部認証機関の隣にある **[アクション]** をクリックし、さらに **[証明書を表示]** をクリックします。**[証明書を表示]** ウィンドウが表示されます。
2. **[証明書を表示]** ウィンドウで、**[証明書をアップロード]** をクリックします。**[証明書をアップロード：外部CA]** ウィンドウが表示されます。
3. **[ファイルを選択]** をクリックし、アップロードする証明書を選択します。
4. **[完了]** をクリックします。

仲介認証機関の作成

- 証明書が必要な場合は、CSRを生成し、それを署名機関に提出します。署名機関から証明書を受け取ったら、証明書をアップロードします。
- すでに必要な証明書がある場合は、それをアップロードします。

CSR(証明書署名要求)の生成

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで **[追加]** をクリックします。
2. [認証機関を追加] セクションの [仲介認証機関を作成] で **[CSRを生成]** をクリックします。
3. 表示されたフォームに入力します。
4. **[生成]** をクリックします。
5. BEGIN CERTIFICATE REQUESTからEND CERTIFICATE REQUESTまでの内容をテキスト ファイルにコピーします。
6. ファイルを認証機関に送信します。
7. **[完了]** をクリックします。

署名済み証明書のアップロード

認証局から署名された証明書を受信すると、署名された証明書をアップロードできます。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで、生成したCSRのエントリを検索します。
2. 次に **[アクション] > [新しい署名済み証明書]** を選択します。
3. **[ファイルの選択]** をクリックします。
4. 新しく署名された証明書を選択します。
5. **[完了]** をクリックします。

既存の証明書のアップロード

このトピックでは、署名された証明書をアップロードする方法について説明します。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで **[追加]** をクリックします。
2. [認証機関を追加] セクションの [仲介認証機関を作成] で **[既存のIDをアップロード]** をクリックします。
3. **[名前]** フィールドで、この証明書を他の証明書と区別する名前を入力します。
4. **[アップロード]** をクリックします。
5. 証明書を選択します。
6. 証明書のパスワードを入力します。
7. **[アップロード]** をクリックします。

仲介認証機関の証明書の表示

証明書の詳細を表示させ、認証機関のCRL(証明書失効リスト) URLを取得することができます。

手順

1. **[認証機関]** セクションで、認証機関の隣にある **[アクション]** をクリックし、**[証明書を表示]** をクリックします。**[証明書を表示]** ウィンドウが表示されます。
2. **[証明書を表示]** ウィンドウの **[CRL URL]** フィールドにURLが表示されます。
3. **[コピー]** をクリックするとURLをクリップボードにコピーし、別のアプリケーションに貼り付けることができます。このURLは、Office 365の構成において認証機関が発行した証明書を承認する際に使用できます。

スタンドアロン認証機関の作成

完全にスタンドアロン(ローカルおよび自己署名)の新しい認証機関を作成したい場合は、このオプションを選択してください。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで **[追加]** をクリックします。
2. [認証機関を追加] ページの [スタンドアロン認証機関を作成] で **[続行]** をクリックします。
3. 表示されたフォームに入力します。
4. **[生成]** をクリックします。

スタンドアロン認証機関の有効期限設定

スタンドアロン(ローカル)の認証機関の有効期限を設定できます。デフォルトで証明書の期限は30年に設定されています。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで、スタンドアロン認証機関の隣にある **[アクション]** をクリックします。
2. **[編集]** をクリックします。
   [認証機関を編集] ウィンドウが表示されます。
3. [クライアント証明書テンプレート] セクションの **[証明書有効期限]** フィールドに新しい有効期間を日数で入力します。
4. **[保存]** をクリックします。

ローカル認証機関によって発行された証明書の有効期限切れが近い場合、またはすでに有効期限が切れている場合、通知とメール(オプションで有効になっている場合)を受け取ることがあります。

- 証明書の有効期限が切れるまでの日数に関する通知 - 証明書の有効期限までの間、事前に設定した間隔で通知が生成されます。最初の通知は、有効期限の365日前に発生し、その後、有効期限の180日、60日、45日、7日前に追加の通知が生成されます。この通知の受信は、**[管理]** > **[証明書管理]** > **[アクション]** > **[新しい署名済み証明書をアップロード]** を開いて証明書を置き換えるまで続きます。
- 期限切れの証明書に関する通知 - 証明書の期限が切れたときに通知が送信されます。通常のサービスを再開するには、証明書を置き換える必要があります。
- 新しい有効な証明書がアップロードされたときの通知 - 署名済みの新しい証明書がアップロードされると、通知が送信されます。

スタンドアロン認証機関の証明書の表示

証明書の詳細を表示させ、ローカル認証機関のCRL(証明書失効リスト)URLを取得することができます。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで、ローカル認証機関の隣にある **[アクション]** をクリックし、さらに **[証明書の表示]** をクリックします。**[証明書を表示]** ウィンドウが表示されます。
2. **[証明書を表示]** ウィンドウの **[CRL URL]** フィールドにURLが表示されます。

3. **[コピー]** をクリックするとURLをクリップボードにコピーし、別のアプリケーションに貼り付けることができます。このURLは、Office 365の構成においてローカル認証機関が発行した証明書を承認する際に使用できます。

認証機関のCRLの有効期限の表示

ローカル認証機関または仲介認証機関のCRLライフタイムの表示と編集を実行できます。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで、ローカル認証機関の隣にある **[アクション]** をクリックし、さらに [**編集**] をクリックします。**[認証機関を編集]** ウィンドウが表示されます。
2. **[認証機関を編集]** ウィンドウに、CRLライフタイムの値が表示されます。デフォルトの最小値は24時間です。入力できる最大値は、10950時間です。
3. CRLライフタイムの値を編集し、**[保存]** をクリックします。

クラウド認証機関の作成

クラウド認証機関を使用したい場合は、このオプションを選択してください。

手順

1. **[証明書管理]** ページの **[認証機関]** セクションで **[追加]** をクリックします。
2. [認証機関を追加] ページの [クラウド認証機関を作成] で **[続行]** をクリックします。
3. クラウド認証機関を選択します。以下から選択：
   - **Atos IDnomic CMS**
   - **DigiCert PKIプラットフォーム**
   - **Entrust**
   - **GlobalSign**
4. 表示されるフォームの残りのフィールドに入力します。
5. **[完了]** をクリックします。

証明書の詳細検索

詳細検索のオプションでは、管理者がルールを使用して発行済みの証明書を検索し、特定の基準を満たす証明書を識別および表示します。これらのルールは、「は次から始まる:」、「は次で終わる:」、「は次を含む:」、「は次を含まない:」、「は次から始まらない:」、「は次で終わらない:」、「は次より小さい:」、「は次より大きい:」、「が次の範囲内:」、「は次と等しい:」、「は次と等しくない:」などの演算子を使用して作成します。[ANY (OR)] または [ALL (AND)] オプションを使用すれば、ルールオプションをネストでまとめることができます。ルールに一致する発行済みの証明書は、セクションの下に表示されます。Ivanti Neurons for MDM リリース76以降では、すべての証明書管理テンプレートの通信事業者が標準の通信事業者です。以下のテンプレートの演算子は本リリースで標準化されています。

- [管理] > [証明書管理] > [発行された証明書] > [詳細検索]

発行された証明書の詳細検索

手順

1. **[証明書管理]** ページの **[発行された証明書]** で **[詳細検索]** リンクをクリックします。
2. ユーザーが少なくとも1つのルールを満たす必要がある場合は **[いずれか]**、証明書がすべてのルールを満たす必要がある場合は **[すべて]** をクリックします。
3. 以下の属性について検索基準を定義するルールを作成します。
   - **CA**
   - **構成名**
   - **有効期限**
   - **プライベートキー**
   - **OS**
   - **シリアル番号**
   - **ステータス**
   - **利用の種類**
   - **ユーザー**
4. (任意) [+] をクリックし、必要に応じて他のルールを作成します。

5. (任意) **[保存]** をクリックしてクエリを保存します。
6. **[検索]** をクリックします。検索基準に一致するユーザーのリストがページに表示されます。

ユーザが指定した証明書の詳細検索

手順

1. **[証明書管理]** ページの **[ユーザが指定した証明書]** で **[詳細検索]** リンクをクリックします。
2. ユーザーが少なくとも1つのルールを満たす必要がある場合は **[いずれか]**、証明書がすべてのルールを満たす必要がある場合は **[すべて]** をクリックします。
3. 以下の属性について検索基準を定義するルールを作成します。
   - **証明書名**
   - **有効期限**
   - **発行者:**
   - **アップロード日:**
4. (任意) [+] をクリックし、必要に応じて他のルールを作成します。
5. (任意) **[保存]** をクリックしてクエリを保存します。
6. **[検索]** をクリックします。検索基準に一致するユーザーのリストがページに表示されます。

発行された証明書に対する検索クエリのロード

保存した検索クエリーのリストを表示するには:

手順

1. **[証明書管理]** ページの **[発行された証明書]** で **[詳細検索]** リンクをクリックします。
2. フォルダーアイコンをクリックします。**[詳細検索]** ウィンドウが表示されます。**[クエリを読み込む]** セクションに、作成された検索クエリのリストが表示されます。このセクションには以下の情報が表示されます。
   - **クエリ名** - 読み込まれたクエリの名前。
   - **クエリの内容** - 検索クエリを定義するルールの内容を表示します。
   - **アクション** - クエリに実行するアクションを選択します。

3. **[アクション]** カラムの **[クエリを読み込む]** をクリックすると、発行された証明書のうち、読み込まれたクエリに定義された基準に一致する証明書のリストが表示されます。
   読み込んだクエリを削除するには、削除アイコンをクリックします。

[CSVにエクスポート] をクリックすると、検索結果のレポートの内容をCSVファイルにダウンロードし、後で参照または分析することができます。

発行された証明書の有効期限の表示

[発行された証明書] セクションの **[有効期限(日数)]** カラムには、有効期間が残り30日未満になった証明書の残りの有効日数が表示されます。過去30日以内にすでに証明書の有効期限が切れている場合、証明書の **[有効期限(日数)]** カラムは有効期限が切れてからの日数を表示します。

詳細は外部認証機関用のSCEP構成を参照してください。

CSVにエクスポート

後から参照または分析するために、証明書をCSVファイルにエクスポートできます。

手順

1. **[証明書管理]** ページで、次のタブのいずれかに移動します。
   - **認証機関**
   - **発行された証明書**
   - **ユーザが指定した証明書**
2. **[CSV にエクスポート]** をクリックします。
3. **[ダウンロード]** をクリックします。
4. (任意)レポートを削除するには **[削除]** をクリックします。

外部認証機関用のSCEP構成

この機能は、Windows 10デバイスの外部認証機関に対応するSimple Certificate Enrollment Protocol(SCEP)構成のサポートを可能にします。

外部認証機関の設定

まず、外部認証機関を設定する必要があります。すでに外部認証機関がある場合は、次のセクションに進んでください。

1. **[管理]** > **[インフラストラクチャ]** > **[証明書管理]** を開きます。
2. **[+追加]** をクリックします。
3. 認証機関の名前を入力します。
4. プルダウンメニューを使用して、**[認証機関の種類]** にMicrosoftを選択します。
5. **[SCEP URL]** を入力します。
6. **[ユーザー名]** と**[パスワード]** を入力します。
7. **[チャレンジURL]** を入力します。
8. **[保存]** をクリックします。

SCEP構成

ここからSCEP構成に進みます。

1. **[構成]** > **[+追加]** を開きます。
2. Windowsアイコンを選択します。
3. **[ID証明書]** を選択すると、**[ID証明書構成を作成]** ページが開きます。
4. 構成の名前を入力します。
5. **[証明書の配布]** プルダウンメニューのSCEP構成のリストから **[Windows構成]** を選択します。
6. 外部認証機関を選択します。

7. 証明書の配布の詳細を入力します。
   - 主体者を入力します。たとえば、`CN=${userEmailAddress}` です。
   - **[再試行]** プルダウンメニューから再試行の回数を選択します。
   - **[再試行遅延]** プルダウンメニューから再試行の間隔を選択します。
   - **[キーの長さ]** プルダウンメニューからキーのサイズを選択します。
   - 証明書使用オプションを1つ以上選択してください。
   - **[有効性]** フィールドとプルダウンメニューから時間の長さを入力します。
   - CA親指指紋を入力します。

     SCEP チャレンジ URL に移動し、CA サムプリントをコピーしてここで貼り付けるか、**[証明書から作成]** をクリックして、CA サムプリントを作成できる証明書をアップロードします。
   - **[ハッシュアルゴリズムファミリー]** オプションから1つ以上のハッシュアルゴリズムを選択します。
8. **[次へ]** をクリックします。

派生認証情報プロバイダー

派生認証情報プロバイダーのページには、証明書の配布に使用される派生認証情報プロバイダーのリストが表示されます。ここで、デフォルトの派生認証情報プロバイダーを指定し、使用する他の派生認証情報プロバイダーも追加します。

デフォルトの派生認証情報プロバイダーを設定するには:

1. **[管理] > [派生認証情報プロバイダー]** を開きます。ページには以下の派生認証情報プロバイダーが表示されます。
   - **Entrust**
   - **Intercede**
   - **Purebred**
2. デフォルトに設定したいプロバイダーについて、**[アクション]** カラムの下の **[デフォルトに設定]** をクリックします。設定すると、そのプロバイダーの **[デフォルトプロバイダー]** カラムの下にチェックマークアイコンが表示されて、デフォルトの認証情報プロバイダーであることを示します。

カスタム派生認証情報プロバイダーを追加するには:

1. **[管理] > [派生認証情報プロバイダー]** を開きます。
2. **[+追加]** をクリックします。
3. 派生認証情報プロバイダーの名前を **[名前]** カラムのテキストフィールドに入力します。
4. **[保存]** をクリックします。
   追加したカスタム派生認証情報プロバイダーは **[ID証明書]** 構成の派生認証情報配布を設定する際、**[ブランド]** フィールドの選択肢として表示されます。

派生認証情報プロバイダーを削除するには **[アクション]** カラムで **[削除]** をクリックします。

デフォルトに設定されている派生認証情報プロバイダーは削除できません。

コネクタ

ライセンス：Silver

Cloud Connectorは、Ivanti Neurons for MDM サービスからLDAPサービスや認証機関(CA)などの企業リソースへのアクセスを提供します。アクセスしたいリソース1つに対して1つのConnectorを設定します。

Amazon Web Services(AWS)でホストされているMicrosoft Active DirectoryまたはLDAPサーバーを使用する場合は、AWSで Ivanti Neurons for MDM Connectorをホストできます。オンプレでないConnectorが必要です。

Connectorは、ソフトウェアの最新バージョンに自動的に更新されます。

最新の Ivanti Neurons for MDM Connector インストールガイドについては、https://help.ivanti.com/#106 を開き、「Connector」を検索してください。

Connectorホスティングオプション

Ivanti Neurons for MDM Connectorは、オンプレのデータセンターでもAmazon Web Services(AWS)でもホスト可能です。

- AWSでホストされているMicrosoft Active Directory、またはAWSの自己管理型のMicrosoft ADを使用している場合は、ConnectorをAWSでホストしてください。この場合、オンプレのConnectorは不要です。
- LDAPサーバーやCAなど、オンプレのリソースにアクセスする場合は、オンプレのConnectorを設定してください。

AWSでConnectorをホスト

AWSでConnectorをホストすれば、AWSにホストされる以下のMicrosoft Active Directoryオプションをご利用いただけます。

- Microsoft Active Directory対応AWSディレクトリサービス
- Amazon VPCの顧客管理型Microsoft Active Directory

Microsoft Active Directory対応AWSディレクトリサービスの詳細は、以下をご覧ください：https://aws.amazon.com/directoryservice。Amazon VPCにおけるMicrosoft Windows ServerとMicrosoft Active Directoryのホストについては、AWSのドキュメンテーションをご覧ください。Ivanti Neurons for MDM Connectorは、Windows Server 2012、2012 R2、2015をサポートしています。

AWS で Ivanti Neurons for MDM Connector AMI を設定する

Ivanti Neurons for MDM Connector AMI を設定するには、次の手順を実行します。

1. 管理者認証情報でAWSにログインします。
2. AWSサービスページで **[コンピューティング]** から **[EC2]** を選択します。
3. **[イメージ]** を展開し、左ペインから **[AMI]** を選択します。
4. 右ペインのドロップダウンリストから **[パブリックイメージ]** を選択します。
5. 「Ivanti Neurons for MDM Cloud Connector」などのキーワードを使用して、Ivanti Neurons for MDM Connector を検索します。
6. リストからConnectorの最新バージョンを選択し、**[起動]** をクリックします。
7. 『*Ivanti Neurons for MDM Connector インストールガイド*』の「Deploying MobileIron Connector in AWS」セクションに記載されている Connector のインストール手順に従います。このドキュメントは、https://help.ivanti.com/mi/help/en_us/cld/<バージョン>/inst/default.htm から入手できます。バージョンはインストールしている Ivanti Neurons for MDM Connector のバージョンです。たとえば、バージョン74の Ivanti Neurons for MDM Connectorのガイドは、https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htmにあります。

オンプレでConnectorをホスト

データセンターでオンプレミスで Ivanti Neurons for MDM Connector をホスティングするには、**[コネクタのダウンロード]** をクリックして、Ivanti Neurons for MDM Connector をダウンロードして設定します。ダウンロードしたパッケージを展開し、パッケージに含まれる Ivanti Neurons for MDM Connectorインストールガイドの指示に従って設定してください。

Connectorログへのアクセス

Connector ログには Connector サービスからアクセスし、Connector 関連の問題解決に役立てることができます。これにはシステムマネージャーまたはシステム読み取り専用の役割が必要です。

1. **[管理]** > **[Connector]** を選択し、[Connector] ページを開きます。
   Connectorのインターフェイスは、Connectorの状態(有効または無効)、Connector名、接続(接続あり、または接続なし)、バージョン番号、ログレベル、アクション(Connectorを無効化または削除)を表示します。

2. **[ログレベル]** プルダウンメニューを使用してレベルを選択します。
   使用可能なログレベルが低い順にプルダウンメニューに表示されます。

   - エラー
   - 警告
   - 情報
   - デバッグ
   - トレース

   情報レベルはデフォルトのログレベル設定です。別のログレベルを選択すると、同期アイコン  が回転し、選択されたログレベルで情報が収集されていることを示します。ログレベルは1時間後に情報レベルにリセットされます。トレースレベルは最高のログレベル設定です。このレベルでは、他の全レベルの全メッセージが収集されます。同期アイコンは、要求の間、表示されます。

3. 必要であれば、同期アイコン  にカーソルを置くと取り消しアイコン  が表示されます。取り消しアイコンをクリックすると、ログレベル変更が取り消されます。

4. 要求アイコンにカーソルを置くと要求情報が表示されます。要求アイコン  をクリックすると、現在のログフォルダーにあるファイルを.zipファイルで要求できます。
   要求が実行されるとログファイルが.zipファイルに追加されます。 新しい要求が実行されると前の要求の.zipファイルは削除されます。

5. 必要であれば、同期アイコン  にカーソルを置くと取り消しアイコン  になります。取り消しアイコンをクリックすると要求が中止されます。
   要求を完了前に取り消した場合、前のログ.zipファイルがサーバーから削除されているため、ダウンロードアイコン  が表示されません。Connector上の元のログファイルは要求すればまだ取得できます。

6. 要求が完了した後にダウンロードアイコン  をクリックすると、最新の要求で収集したログファイルを含むログ.zipファイルがダウンロードされます。
   ログファイル名の形式は`kocab.log`です。ダウンロードした.zipファイル名は、サーバー名、接続バージョン、タイムスタンプ(日、月、年、時刻)で構成され、形式は`<Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip`となります。アーカイブに保存された.zipファイル名の形式は`kocab.yyyy-mm-dd.0.log.gz`です。
7. 任意で **[アクション]** プルダウンメニューをクリックし、Connectorを無効化または削除できます。

[Connector] ページが見えない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

詳細はConnectorへのhttpproxyコマンド使用を参照してください。

ConnectorへのHttpproxyコマンド使用

Ivanti Neurons for MDM でConnector構成を簡単に編集できる新しいklishシェルコマンドが作成されました。このコマンドを使用すると、ログイン情報や、Connectorを構成するその他のパラメータを変更できます。

これらの要件により、今回のリリースではHttpproxyコマンドが利用できるようになりました。

- klishシェル

Connectorを構成するには

1. klishシェルにログインします。
2. 利用可能なklishシェルコマンドのリストを表示するには、[?] を入力します。
3. **[Httpproxy]** と入力すると、次のパラメータの現在の値が表示されます。
    a. 有効
    b. スキーム
    c. サーバ
    d. 認証タイプ
    e. ユーザー名
    f. パスワード

4. **[httpproxy ?]** と入力すると、httpproxyで利用できるリストコマンドが表示されます。
    a. authtype - httpプロキシの認証タイプを [なし]、[基本]、[NTLM] のいずれかに設定します
    b. disable - httpプロキシを無効化します
    c. enable - httpプロキシを有効化します
    d. host - httpプロキシのホストを設定します(FQDNか、httpまたはhttpsのいずれかのIP)
    e. password - httpプロキシの認証パスワードを設定します
    f. port - httpプロキシのポートを設定します
    g. scheme - httpプロキシのスキームを設定します(httpまたはhttps)
    h. show - 現在のhttpプロキシ設定を表示します
    i. username - httpプロキシの認証ユーザー名を設定します
5. 上のリストにあるコマンドを使用して、Connectorインスタンスを設定します。

Help@Work

ライセンス: Platinum

サポート: Ivanti Neurons for MDMがサポートするAndroidデバイスとiOSデバイス

Help@Work for Android/iOSでは、AndroidおよびiOSデバイスのユーザーをリモートでサポートできます。Help@Work for Android/iOSは、TeamViewer QuickSupportアプリをベースとしています。Help@Work for Android/iOSを使用するにはTeamViewerのアカウントが必要です。アカウントをお持ちでない場合は、teamviewer.comで詳細をご覧ください。

Help@Workでは、ユーザーがボタンを1つ押せばヘルプデスクの担当者と画面を共有できるため、iOS 11.0+/Androidデバイスの問題解決が大幅に楽になります。ユーザーは問題を言葉で説明する時間を節約でき、ITスタッフはトラブルシューティングの効率を高めることができます。MAM Only iOSデバイスではサポートされていません。

キオスクモードのAndroidデバイス所有者デバイスではTeamViewerがサポートされています。

TeamViewer起動コマンドは、アプリが終了またはデバイスが再起動すると停止します。

Androidデバイスでは、Teamviewer QuickSupportアプリがインストールされていない場合、ユーザーはアプリをダウンロードするように求められます。iOSデバイスでは、アプリをアプリカタログを介してプッシュする必要があります。あるいは、デバイスにインストール済みの場合は、マネージドアプリに変換する必要があります。

セッションをアプリケーションに適用するには、Teamviewer QuickSupportアプリがフォアグラウンドにある必要があります。無人モードでは、TeamViewer ホスト アプリケーションが必要です。

リモートセッションに対応するには、管理者によってインストールされるデスクトップアプリケーションのバージョンが、クライアントデバイスにインストールされるQuicksupportバージョンと互換性を持つ必要があります。

Help@Work for Android/iOSの設定

以下は、Help@Work for Android/iOSのブランディングと配布に関する1回限りの設定手順です。

1. **[管理]** タブを開きます。
2. [インフラ] で **[Help@Work]** をクリックします。
3. **Help@Work**にはTeamViewerが必要です。[TeamViewer のアクティブ化] セクションで **[今すぐアクティブ化]** ボタンをクリックして、**[TeamViewer 有人]** または **[TeamViewer 無人 (Android のみ)]** オプションのいずれかを有効にします。
4. TeamViewerライセンス契約の内容を確認し、**[同意する]** をクリックして続行します。これで企業用ライセンスがアクティブ化されました。TeamViewerはIvantiの顧客を認識し、アクセスを許可します。

> **[アクティベーションの削除]** オプションは、TeamViewer を起動した時点で利用可能になります。**[TeamViewerの起動]** セクションの下にある **[アクティベーションの削除]** をクリックすると、**[アクティベーション削除の確認]** ウィンドウが画面に表示されます。**[アクティベーションの削除]** をクリックすると、TeamViewerのアクティベーションが削除され、次に、サポート対象のすべてのデバイス上の Help@Work機能が削除されます。ただし、その後のステージで、既存のアカウントまたは別のアカウントを使用してTeamViewerをアクティベートできます。

> 無人モードの**TeamViewer**アカウントを削除する場合は、無人モードが有効になっている関連デバイスのプロビジョニングを解除する必要があります。関連デバイスのプロビジョニングを解除するには、関連デバイスからの**TeamViewer**アプリの配布を未配布の状態に戻し、強制チェックインを実行する必要があります。TeamViewerアプリがすべてのデバイスから削除されたことを確認してから、アカウントのバインディングを管理コンソールから削除します。

5. TeamViewerアプリがすべてのデバイスから削除されたことを確認してから、アカウントのバインディングを管理コンソールから削除します。
6. 標準的なアプリ配布ワークフローを使用してリモートセッションを開始したい場合、TeamViewerアプリをユーザーに配布します。これは**有人**および**無人**モードに固有です。管理者がデバイスを制御する場合は、TeamViewer のユニバーサルアドオンまたは OEM/モデル固有のアドオンもデバイスに配布する必要があります。手順については、アプリ構成をご参照ください。

Help@Work for Android/iOSを使用したリモートセッションの開始

Help@Work for Android/iOSの典型的なセッションは、エンドユーザーのヘルプ要請から始まります。

ユーザーのデバイスでHelp@Workセッションを開始する手順は以下のとおりです。

1. Ivanti Neurons for MDM で **[デバイス]** に移動します。
2. [デバイスリスト] ページで、サポートが必要なデバイスをクリックします。

3. [アクション] メニューから、Androidデバイスの場合は **[TeamViewerリモート制御を開始]**、iOSデバイスの場合は **[リモートディスプレイ]** をクリックします。2つのオプションが表示されます。

   - 有人モード (既定) - このオプションでは、**TeamViewer Quick Support** アプリケーションをインストールし、ターゲット デバイスでホワイトリストに追加する必要があります。
   - 無人モード (Android のみ) - このオプションでは、**TeamViewer Host** アプリケーションをインストールし、ターゲット デバイスでホワイトリストに追加する必要があります。

   ホスト名をホワイトリストに入れる必要がある場合や、コンテンツのセキュリティポリシーをオーバーライドする必要がある場合は、サポートチームまでお問い合わせください。

   無人モード オプションはキオスク モードでも動作します。[TeamViewer 統合] ページから有効にします。無人リモート制御には、デバイスに TeamViewer ホスト アプリケーションをインストールし、デバイスでワンタイム認証を設定して、MI アドオン ライセンスを取得する必要があります。ワンタイム アクティベーションの場合、TeamViewer ホストアプリが初めてインストールされ起動したときにアクセス権プロンプトが表示されます。必要に応じて、管理者は、インストール後に、「自動起動 (管理対象のアプリ構成の設定)」TeamViewer アプリを使用できます。ライセンス数は TeamViewer ホスト アプリケーション配布に基づいて計算されます。TeamViewer ホスト アプリケーションがデバイスに配布される場合、1つの無人リモート ホスト セッション ライセンスが使用されます。TeamViewer ホストアプリのほかに、他のアドオンアプリが必要になる場合があります。その場合は、キオスクまたは共有キオスクモードで許可してください。デバイスモデルやメーカーによっては、他のアドオンが必要になる場合もあります。

   Google Pixel デバイスでは、この権限付与が永続せず、セッションごとに権限の同意が必要です。

4. 管理者が有効なTeamViewerトークンを持っている場合、デスクトップクライアントがデバイスのサポートセッションを開始します。持っていない場合、管理者がTeamViewerにログインし、許可を受ける必要があります。

削除セッションをすばやく開始するために、管理者は事前にデスクトップアプリケーションにログインできます。

TeamViewerのインストール

ユーザーのリモートデバイスにアクセスし、サポートを提供するには、TeamViewerアプリをデスクトップにインストールします。TeamViewerをインストールするには:

1. Mac、Windows、Androidに対応するTeamViewerフルバージョンのインストールパッケージを以下からダウンロードします。
   https://www.teamviewer.com/ja/download/
2. TeamViewerインストールプログラムを起動します。
3. **[基本インストール]** を選択します。
4. **[企業/商用]** を選択します。
5. **[同意する - 終了]** をクリックします。

TeamViewerアカウントの取得

TeamViewerを利用してサポートを提供するには、TeamViewerアカウントが必要です。TeamViewerアカウントの取得方法は以下のとおりです。

1. https://login.teamviewer.com/を開きます。
2. Eメールアドレス、名前、パスワードを入力します。
3. **[登録]** をクリックします。
4. 2番目の手順で入力したメールアカウントを使用し、TeamViewerアカウントのアクティブ化メールを受信します。
5. メールの指示に従い、TeamViewerアカウントをアクティブ化します。

TeamViewerセッションIDの確認

TeamViewerは、管理者のコンピューターとユーザーのモバイルデバイスの間に接続を確立すると、セッションIDを生成します。

1. 生成されたセッションIDは、マネージドアプリ構成を使用してIvanti Neurons for MDMからTeamViewer QuickSupportアプリに渡されます。その後、アプリがそのセッションIDを使用してデバイス上のTeamViewerクライアントを呼び出します。iOSの場合、セッションIDは30分後に期限切れになります。
2. ユーザーはTeamViewer EULAへの同意を求められます。

インフラID

このセクションは以 下 のトピックを含 みます。

IDプロバイダーの構成

ライセンス: Silver

IDプロバイダー(IdP) を構成し、Ivanti Neurons for MDM へのデバイス登録、管理ポータルへのアクセス、セルフサービスポータルへのアクセスを希望するユーザーを認証します。オンプレミス LDAP 対応ユーザディレクトリが必要です。Ivanti Neurons for MDM は、すべての SAML 2.0 対応 IdP と連携できます。Microsoft Azure AD認証(Azure AD) 、Microsoft ADFS(Active Directory Federation Services) 、Okta、OneLogin、PingOne、Ping IdentityのPingFederateは、Ivanti Neurons for MDM に対応することが検証されています。

これまでSAML auth/IdPを設定すると、SAML認証がデバイス登録とポータル認証の両方に使用されていました。トグルボタンが提供され、管理ポータルのアクセスとデバイス登録で異なる認証方法を選択できます。バイパストグルはデバイス登録にのみ使用します。

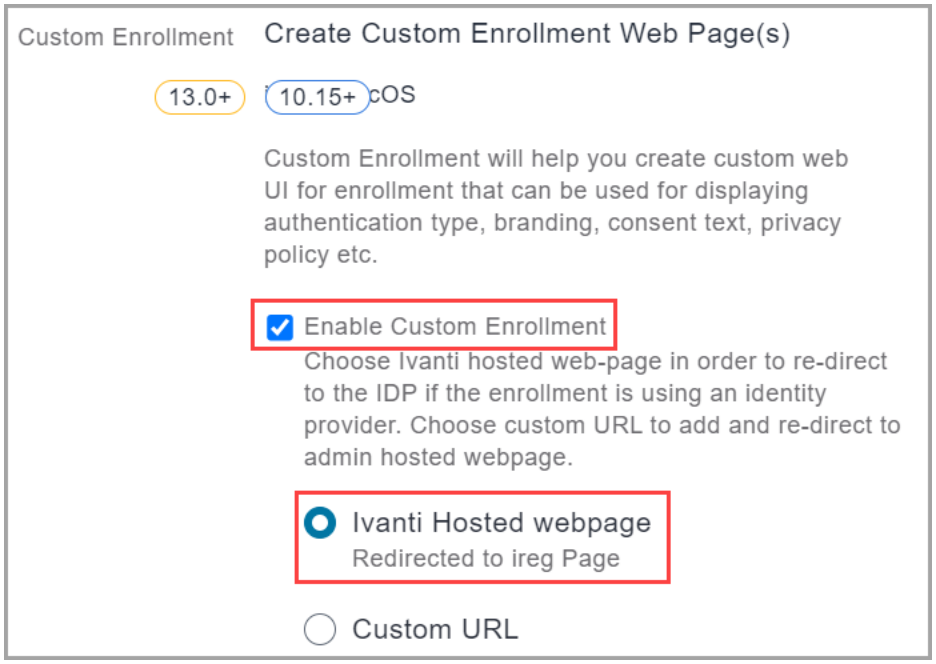
デバイス登録中に、管理者は ID プロバイダオプションを回避できます。このようにすると、ユーザは ID プロバイダページでの認証ではなく、PIN を使用した認証を選ぶことができます。

概要

- Microsoft ADまたは他のオンプレLDAPディレクトリを使用している場合は、Ivanti Neurons for MDM に接続し、ユーザーをインポートするようConnectorを設定する必要があります。ConnectorまたはLDAPの設定が完了していない場合は完了させてください。
- IdPが追加されると、ユーザー認証は自動的にLDAPからIdPに切り替わります。
- IdPプロバイダーは1つにしてください。
- IdPにアクセスできなくなった場合は、Ivanti Neurons for MDM テナント管理者(TA) アカウントを使用してこの管理ポータルにアクセスし、トラブルシューティングを行います。TAはローカルアカウントであり、外部認証を必要としません。Ivanti Neurons for MDM がプロビジョニングされ、組織の技術担当者または同等の担当者に情報が提供されるとTAアカウントが作成されます。TAアカウント情報をお持ちでない場合は、サポート担当者にお問い合わせください。
- Ivanti Neurons for MDM では、Windows 10デバイス登録中のユーザー認証にMicrosoft Azure Active Directory(Azure AD) を使用できます。

> IdPベンダーが提供したツールを使用し、LDAPユーザーの認証タイプを設定します。IdPの認証方式は Ivanti Neurons for MDM の設定より優先されます。Ivanti Neurons for MDM 認証設定は、**[ユーザー] > [ユーザー設定] > [デバイス登録設定] > [デバイス登録認証タイプ]** にあります。

- Apple Device EnrollmentおよびConfiguratorデバイス登録は、ユーザー認証にIdPを使用しません。
- Apple Business ManagerのiOSデバイス登録とmacOSデバイス登録で機能するようにIDプロバイダを構成するには、**[管理] > [Apple] > [デバイス登録]** > *[デバイス登録プロファイルを編集]* にある**カスタム登録を有効化**と、関連する**Ivantiがホストしている Webページ**設定を有効にする必要があります。詳細はこちらの「「デバイス登録」ページ1162」をご覧ください。



IdP設定の種類

Ivanti Neurons for MDM の [ID] ページが、以下の種類のIdPプロバイダーの設定を導いてくれます。

- **Ivanti Neurons for MDM IdP の設定** - サポートされている Ivanti Neurons for MDM IdP プロバイダは、Azure AD、OneLogin、Okta、PingOne です。
- **オンプレIdP設定** - サポートされるオンプレIdPプロバイダーはADFS 3.0、PingFederate 8.2.1、PingFederate 8.1.3です。
- **汎用IdP設定** - これは、Microsoft ADFS、Okta、OneLogin、PingFederateを使用していない場合の汎用設定パスです。

IDプロバイダー(IdP)の構成

手順

1. **[管理]** > **[ID]** > **[SAML 認証]** を開きます。
2. IDプロバイダの設定の種類をクリックします。
   - **Ivanti Neurons for MDM IdP設定**
   - **オンプレIdP設定**
   - **汎用IdP設定**
3. 対応のIIdPを選択します。ステップ3で **[汎用IdP設定]** を選択した場合は、このステップをスキップし、ステップ5に進んでください。
4. 選択したIdPに応じて表示される、画面上の指示に従います。
5. **[完了]** をクリックします。

管理者は、IdPを使用した最初の認証から2時間までシングルサインオンが可能です。

必要な可能性のある設定タスク

選択したIdPに応じて、関連する以下のページやステップに進みます。

IdP	手順
• Azure AD • Okta • OneLogin • PingOne	• IdPにアップロードするキーを生成します。 • IdPにログインし、生成したキーをアップロードします。 • IdPからメタデータファイルをエクスポートし、Ivanti Neurons for MDM にインポートします。
• ADSF 3.0 • PingFederate 8.2.1 • PingFederate 8.1.3	• Ivanti Neurons for MDM からメタデータファイルをダウンロードします。 • ADFSの [証明書利用者の信頼] を設定するか、PingFederateの [SP接続] を設定し、Ivanti Neurons for MDM メタデータファイルをインポートします。 • IdPからメタデータファイルをエクスポートし、Ivanti Neurons for MDM にインポートします。

• 汎用IdP	1. Ivanti Neurons for MDM からメタデータ ファイルをダウンロードします。 2. IdP ベンダーから提供された手順に従い、「サービス プロバイダ」として Ivanti Neurons for MDM サービスに接続するための IdP サーバーまたはサービスを構成します。 a. 上記ステップ1のメタデータファイルをIdPにアップロードします。この構成ファイルは、SAML 2.0 IDプロバイダーと通信するSAML 2.0サービスプロバイダーとして Ivanti Neurons for MDM を有効化するための必須情報を含みます。標準的なSAML 2.0のURL、証明書、設定はメタデータファイルに含まれます。 Ivanti Neurons for MDM は SAML 2.0対応 IdP がサービスプロバイダからエクスポートされた XML メタデータをインポートおよび処理できることを想定しています。 b. IdPがRSA-SHA1を使用してSAML認証要求に署名するよう構成します。認証要求の検証に使用される署名証明書に関する情報は、ステップ1でダウンロードしたメタデータファイルに含まれます。 c. SAML 応答にユーザー名を含めるようにする IdP の構成が Ivanti Neurons for MDM に送信されました。IdPからのSAML応答の [Name Id] 要素でユーザー名を指定します。 3. IdPからメタデータファイルをエクスポートし、Ivanti Neurons for MDM にインポートします。 4. (任意) - SAML 認証要求にユーザ名を含める: 認証要求にユーザーを認証するユーザー名を含め、IdP で認証するときに追加のユーザー入力を削除します。このオプションを有効にすると、認証失敗が発生する場合があります。IdP 検証についてわからない場合は、**[この変更の影響を理解しています]** オプションを選択し、**[SAML 認証要求にユーザー名を含める]** 設定を **[オン]** に切り替えます。 Ivanti Access は、この設定の検証された IdP です。

ローカルユーザーによるIdP認証のバイパス

IdPまたは Ivanti Neurons for MDM の接続がダウンし、Ivanti Neurons for MDM 側からのトラブルシューティングが必要な場合、一部の管理者は、LDAPやIdPなどの外部システムによる認証に頼らず、Ivanti Neurons for MDM にログインできる必要があります。システム管理者の役割を持つローカルユーザーのみIdP認証をバイパスできます。

IdP認証をバイパスするローカルユーザーのリストを作成します。

手順

1. **[管理]** > **[ID]** をクリックします。
2. [IdP認証をバイパスするローカルユーザー] セクションで **[+ユーザーを追加]** をクリックします。
3. システム管理者の役割を持つローカルユーザーだけを表示したリストから、少数のユーザーを選択してください。
4. **[保存]** をクリックします。

IdP認証をバイパスするローカルユーザーのリストからユーザーを削除するには、削除したいエントリの横にある削除アイコンをクリックします。

[ID] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

ユーザープロビジョニング-Azure Active Directory

AADユーザーソースの代わりに、Azure Active Directory(AAD) ユーザープロビジョニングが導入されています。ユーザプロビジョニング Azure AD は SCIM プロトコルを使用して AAD とIvanti Neurons for MDM を同期し、一部のユーザとグループの同期を可能にします。ユーザプロビジョニング Azure AD は SCIM プロトコルを使用して、Azure AD から Ivanti Neurons for MDM に転送されたユーザとグループオブジェクトを自動的に作成および更新します。Ivanti Neurons for MDM 管理者は、ディレクトリサービス全体を同期させるか、特定のユーザーオブジェクトとグループオブジェクトをIvanti Neurons for MDMと同期させるかを選択できます。現在の Azure AD との統合のように、ユーザおよびグループ プロビジョニング プロセスは自動化されます。Azure AD でユーザまたはグループの変更が行われる場合は、同じ変更が Ivanti Neurons for MDM で反映されます。最も重要な違いは、ユーザプロビジョニング Azure AD では、特定のユーザとグループに対してプロビジョニングできるという点です。これにより、管理者は、Ivanti Neurons for MDM で追加、更新、無効化されるユーザとグループを特定するためにより厳密に制御できます。Ivanti Neurons for MDM 管理ポータルの [ユーザプロビジョニング Azure AD] ページには、Azure AD から Ivanti Neurons for MDM へのユーザおよびユーザグループ移行のワークフロー ステージが表示されます。

ユーザー名の値はIvanti Neurons for MDM内で一意であるため、ユーザーが既にプロビジョンされている場合は、Azure ADで [ユーザープリンシパル名] 属性を更新することはできません。

このセクションは以下のトピックを含みます。

- 「トークンの生成 Ivanti Neurons for MDM」下
- 「Azure AD との間の接続を確立する Ivanti Neurons for MDM」次のページ
- 「割り当てられたユーザとグループのプロビジョニング」ページ1139
- 「すべてのユーザとグループのプロビジョニング」ページ1139
- 「グループのプロビジョニングの確認」ページ1140

トークンの生成 Ivanti Neurons for MDM

Azure ADユーザープロビジョニングを開始するには、Ivanti Neurons for MDMでトークンとターゲットURLを生成します。

必ずトークンとターゲット URL を保存してください。

一度に生成できるトークンの数は最大2個です。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[管理]** > **[ID]** > **[ユーザ プロビジョニング]** を開きます。
3. **[ID プロバイダ (IdP) の選択]** ドロップダウンリストから **[Azure AD]** を選択します。
4. 新しいトークンを生成するには、**[生成]** をクリックします。通知メッセージが表示されます。**[生成]** をクリックします。新しいページが開き、トークンの詳細とターゲットの SCIM URLが表示されます。
5. **[コピー]** をクリックすると、トークンまたはSCIM URLのいずれかがコピーされます。
6. ページを更新します。**[ユーザープロビジョニングのAzure AD] ページ**に、トークンステータス表が表示されます。

Ivanti Neurons for MDMからのトークン ステータスの変更

既存のトークンの状態を変更できます。

手順

1. **[ユーザープロビジョニングのAzure AD]** ページで **[選択]** ドロップダウンメニューをクリックします。
2. **[選択]** をクリックし、トークンに対して次の変更を行います。
   - **アクティブに設定**
   - **非アクティブに設定**
   - **更新**
   - **削除**

Azure AD との間の接続を確立する Ivanti Neurons for MDM

Azure AD Enterprise アプリケーションでユーザーとグループを作成した後、Azure ADとIvanti Neurons for MDMの間の接続を確立することができます。

移行に関する考慮事項

- AAD ユーザ ソースからユーザ プロビジョニング Azure AD (SCIM) に移行するときに、[すべてのユーザとグループを同期] を選択します。
- ユーザとグループが SCIM AAD ソースで更新された後、Azure で [Azure プロビジョニング] ページに戻り、[割り当てられたユーザとグループのみを同期] オプションを使用して、ユーザ プロビジョニング Azure AD で管理される特定のユーザとグループを設定します。

- 同期が完了した後は、Azure で定義されていないユーザとグループを Ivanti Neurons for MDM の [ユーザとグループ] リストから削除できます。
- 移行が開始すると、[AAD ユーザソース] ページに読み取り専用でアクセスできます。

手順

1. Azure ADポータルにログインします。
2. **[企業アプリケーション]** を開き、**[+ 自分のアプリケーションを作成]** に移動します。[自分のアプリケーションの作成] ウィンドウが開きます。
3. アプリケーションの名前 (**既定: Non-gallery**) を指定し、**[作成]** をクリックします。例: Ivanti Neurons for MDM ユーザプロビジョニング。
4. **[プロビジョニング]** > **[プロビジョニングの編集]** > **[管理者認証情報]** を開きます。
5. Ivanti Neurons for MDM 管理ポータルからターゲットのSCIM URLをコピーして、Azure ADポータルの **[テナントURL]** フィールドに貼り付けます。
6. Ivanti Neurons for MDM からトークンをコピーして、Azure AADポータルの **[シークレット トークン]** フィールドに貼り付けます。
7. 以下のいずれかの手順を実行してください。
   a. **[割り当てられたユーザとグループのみを同期]** を選択します。詳細については、「割り当てられたユーザとグループのプロビジョニング」をご参照ください。
   b. **[すべてのユーザとグループを同期]** を選択します。詳細については、「すべてのユーザとグループのプロビジョニング」をご参照ください。

   > 移行するユーザの [すべてのユーザとグループを同期] オプションを選択します。

8. **[試験接続]** をクリックします。緑色のチェックが入ったポップアップが表示され、接続が確認されます。
9. **[保存]** をクリックします。

手順

1. Azure ADポータルの **[プロビジョニング]** ページから **[マッピング]** を展開します。
2. **[Azure Active Directoryユーザーのプロビジョニング]** をクリックします。[属性マッピング] ページが開きます。
3. サポートされていない属性を対象に **[削除]** をクリックします。

割り当てられたユーザとグループのプロビジョニング

Azure ADとIvanti Neurons for MDMとの間で接続が確立された後、ユーザーやグループをプロビジョニングできます。

グループのプロビジョニング中には、Azure ADはネストされたグループのメンバーを選択したグループに追加しません。同期処理中、Azure ADは直下のメンバーとグループの名前のみをグループに追加し、下位グループのメンバーは追加しません。

手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. アプリケーションで、**[ユーザーとグループ]** > **[+ユーザー/グループを追加]**に移動します。[割り当てを追加]ページが開きます。
3. **[検索]**フィールドからユーザまたはグループを検索し、**[選択]**をクリックしてから**[割り当て]**をクリックします。[ユーザーおよびグループ]ページが開きます。
4. 対応するユーザまたはグループのチェックボックスをオンにします。
5. **[プロビジョニング]**をクリックし、**[プロビジョニングを開始]**をクリックします。成功した構成の詳細情報が表示されます。

すべてのユーザとグループのプロビジョニング

Azure ADとIvanti Neurons for MDM間の接続が確立したら、ユーザまたはグループのプロビジョニングを実行できます。

手順

1. **[プロビジョニング]**をクリックし、**[プロビジョニングを開始]**をクリックします。プロビジョニングが成功するとその詳細が表示され、ユーザーがIvanti Neurons for MDMにプロビジョニングされます。

割り当てられたユーザーのプロビジョニングの確認

割り当てられたユーザーがAzure ADポータルでプロビジョニングされた後、Ivanti Neurons for MDM管理ポータルでプロビジョニングを確認します。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. メインメニューで、**[ユーザー]** タブを開きます。プロビジョニングされたユーザーは、このページのユーザーのリストに表示されます。

   プロビジョニング プロセスには最大で1時間かかる場合があります。

グループのプロビジョニングの確認

グループがAzure ADポータルでプロビジョニングされた後、Ivanti Neurons for MDMでプロビジョニングを確認します。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインします。
2. **[ユーザ]** タブ> **[ユーザ グループ]** を開きます。プロビジョニングされたグループは、このページのグループのリストに表示されます。

   プロビジョニング プロセスには最大で1時間かかる場合があります。

設定の編集

このトピックでは、Azure Active Directory 設定の構成について説明します。

手順

1. **[管理] > [Microsoft Azure] > [ユーザ プロビジョニング Azure AD]** に移動します。
2. **[トークンの生成]** をクリックして、トークンをコピーします。
3. ページを更新します。[AAD設定] ページが開きます。
4. **[設定の編集]** をクリックします。
5. **AAD からインポートしたユーザを自動的に招待** - AAD からIvanti Neurons for MDMにインポートしたユーザに自動的に登録招待メールを送信するかどうかを管理します。
6. **管理対象Apple ID** - AADユーザーの管理対象Apple IDを同期する場合に選択します。
   - **なし**
   - **パターン**
     - **ユーザーのメールアドレス**
     - (任意) [「appleid」サブドメインを含める] オプションを選択し、既存のApple IDとの競合を避けます。
7. (任意) **カスタム属性の追加** - デバイス管理に適用したいカスタム ユーザ属性をディレクトリ サービスから指定します。これにより、各属性は、変数をサポートする構成フィールドの${attributeName}によって参照されます。このオプションを使用するには、すべてのAADサーバーにカスタム属性を一貫して実装しておく必要があります。実装に含まれるいずれかのAADサーバーがこの属性を使用していない場合、この属性に依存する機能が意図通りに機能しないことがあります。**[設定の編集]** セクションの **[カスタム属性]** 表の **[属性タイプ]** 列には **IDP** 属性が表示されます。
8. AAD設定を変更した後、[**変更の保存**] をクリックします。

SCIMユーザープロビジョニングにおける属性の構成

このセクションでは、ユーザープロビジョニング中における、Azure AD用のカスタム属性とエンタープライズ属性の作成方法を説明します。

属性のマッピング

接続が確立された後、Azure ADとIvanti Neurons for MDMとの間で属性をマッピングできます。Ivanti Neurons for MDM では、以下のAzure AD属性をサポートしています。

コア属性

- id(urn:ietf:params:scim:schemas:core:2.0:id)
- userName("urn:ietf:params:scim:schemas:core:2.0:User:userName")
- displayname("urn:ietf:params:scim:schemas:core:2.0:User:displayName")
- active("urn:ietf:params:scim:schemas:core:2.0:User:active")
- name("urn:ietf:params:scim:schemas:core:2.0:User:name")
- userType(urn:ietf:params:scim:schemas:core:2.0:User:userType)
- emails(urn:ietf:params:scim:schemas:core:2.0:User:emails)
- locale("urn:ietf:params:scim:schemas:core:2.0:User:locale")

更新操作が許可される属性の一覧

- displayName
- emails
- name
- active
- id
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User

カスタム属性

スキーマ - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

エンタープライズ属性

現在、部署属性のみがサポートされています。

スキーマ - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

手順

1. Ivanti Neurons for MDM管理ポータルにログインします。
2. **[管理]** > **[ID]** > **[ユーザープロビジョニング]** に移動します。
3. **[設定を編集]** で **[+カスタム属性を追加]** をクリックします。
4. **[属性名]** フィールドに名前を入力します
5. **[変更の保存]** をクリックします。
6. [管理] > [システム] > [属性] ページに属性がリストされて利用できるようになります。
7. この属性は、IDP属性タイプとして示され、削除アクションのみを実行できます。
8. Azure ADポータルにログインします。
9. **[ホーム]** > **[企業アプリケーション]** を開き、SCIMアプリケーションをクリックします。
10. **[マッピング]** セクションで **[Azure Active Directoryユーザーのプロビジョニング]** をクリックします。
11. **[詳細オプションを表示]** チェックボックスを選択します。
12. **[customappssoの属性リストを編集]** をクリックします。
13. Ivanti Neurons for MDMのUIで作成したカスタム属性用に新規エントリーを入力します。
14. カスタム/エンタープライズ(部署)属性のスキーマを次のように追加します。
    カスタム属性 - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custom attribute>**

    エンタープライズ属性 - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
15. **[変更の保存]** をクリックします。
16. **[新規マッピングの追加]** をクリックし、ドロップダウンメニューからソース属性とターゲット属性を選択します。
17. **[Ok]** をクリックし、**[マッピングの保存]** をクリックします。

18. **[ホーム]** > **[企業アプリケーション]** を開き、SCIMアプリケーション > **[ユーザーとグループ]** をクリックします。
19. ユーザー名をクリックします。[プロファイル] ページが開きます。
20. 属性に関連付けられている値がこの [プロファイル] ページに表示されているかどうかを確認します。
21. (任意) SCIMアプリケーション > **[プロビジョニング]** > **[オンデマンドでプロビジョニング]** をクリックし、特定のユーザーを検索して、**[プロビジョニング]** をクリックします。上述の手順で実行した新規属性マッピングを検証するには:
22. Ivanti Neurons for MDM 管理ポータルにログインします。
23. **[ユーザー]** > **[ユーザー]** へ進みます。
24. ユーザーを選択し、**[属性]** タブをクリックして、属性値を確認します。属性がその特定のユーザーにマップされています。

重要な注意点

- メールアドレスは、ユーザーやメンバーのプロビジョニングと移行のための必須フィールドです。
- SCIMは、Microsoft Azure ADからIvanti Neurons for MDMへの、一方向のプロビジョニングを提供します。Ivanti Neurons for MDM は、いかなる同期オプションも提供しません。SCIMでプロビジョニングされたユーザーまたはグループをIvanti Neurons for MDMから削除した場合は、そのユーザーまたはグループをMicrosoft Azure ADからも削除してください。
- Microsoft Azure ADのSCIMアプリケーションマッピングウィンドウでは、1つの属性(ソースまたはターゲット)を1回だけ使用できます。同じソースを特定のターゲット属性に2回マップすることはできません。
- 停止中のユーザーを、SCIMを使用してプロビジョニングする、あるいはIvanti Neurons for MDMに移行することはできません。
- 現在、Ivanti Neurons for MDMはSCIMイベント通知をサポートしていません。
- 移行またはプロビジョニングにかかる時間は、対象となるユーザーまたはグループの数に依存します。
- Microsoft Azureはプロビジョニング間隔を制御します。この間隔は約40分以上です。
- 再プロビジョニング中にMicrosoft Azure ADが再試行するのは、失敗したエントリーのみです。プロビジョニングが成功した、または失敗したユーザーを確認するためのプロビジョニングログを、Microsoft Azure ADからダウンロードできます。

- 異なるソースからのグループの重複は、SCIMでは許可されません。
- プロビジョニングされたユーザーをMicrosoft Azure ADからハード削除した場合、そのユーザーはIvanti Neurons for MDMでは無効化されます。
- プロビジョニングされたユーザーグループをMicrosoft Azure ADから削除した場合、そのグループはIvanti Neurons for MDMでは削除され、その削除されたグループに属する個別のメンバーは、無効化されて「すべてのユーザーグループ」に関連付けられます。
- プロビジョニングされたグループのプロビジョニングされたメンバーをMicrosoft Azure ADでハード削除した場合、そのメンバーはIvanti Neurons for MDMでは無効化されますが、Ivanti Neurons for MDM内のグループにはまだ関連付けられています。
- 属性(エンタープライズ属性またはカスタム属性)マッピングがアプリから削除された場合、その削除された属性の値はまだIvanti Neurons for MDMに反映されています。
- プロビジョニングされたユーザーのユーザー属性は、空白または空の値で更新され、その更新された属性値はIvanti Neurons for MDMには反映されません。
- Microsoft AADからSCIMへの移行中または更新中にユーザー属性FNameおよびLName (name.formatted) が空白である場合、移行または更新は失敗します。
- Azure AD内のユーザーを削除した場合、対応するSCIM APIは、そのユーザーを完全に削除するのではなく、ソフト削除を実行し、そのユーザーのステータスをアクティブから停止中に変更します。ユーザーを完全に削除する場合は、Ivanti Neurons for MDM管理ポータルにログインし、その停止中/無効化されたユーザーを手動で削除します。

関連トピック:

「ユーザープロビジョニング-Azure Active Directory」ページ1136

「属性」ページ1044

LDAPサーバーの構成

ライセンス：Silver

LDAPサーバーとConnectorを構成すると、企業ディレクトリからユーザーやグループをインポートできます。少なくとも1つのConnectorをインストールした後に、1つ以上のLDAPサーバーを追加できます。

LDAPサーバーを追加すると、次の項目が構成されることになります。

- LDAPサーバーへの*接続*
- ターゲットディレクトリのデータを表示するために必要な*検索語*
- *インポート*するディレクトリの部分
- ディレクトリの選択した部分に自動的に*ユーザーを招待*するかどうか。

LDAPサーバーの追加後、このページに戻りLDAPサーバー情報の編集または選択したLDAPユーザーの変更を行うことができます。

LDAPユーザーの構成後、LDAPユーザーをインポートする必要があります。LDAPユーザーのインポートをご覧ください。
LDAPユーザー名は、ローカルユーザー名と同様、グローバルに一意である必要があります。ユーザーが同じユーザー名でローカルアカウントをすでに持っていないか、または、2件以上のテナントを持つ組織の場合はユーザー名がすでに別のテナントに関連付けられていないか、確認してください。

LDAPサーバーの追加

手順

1. **[+サーバーを追加]**をクリックします。
2. 次の情報を入力します。

設定	操作内容
名前	このサーバーを識別する名前を入力します。
説明	このサーバーの目的を明示する説明を入力します。

ディレクトリURL	ディレクトリのURLを入力します。以下のいずれかの形式を使用してください。 ldap://IPアドレス または ldaps://IPアドレス または 例：ldap://myserver1.mycompany.com:389
ユーザーID	次の特徴を持つアカウントのユーザーIDを入力します。 • LDAPサーバーによって管理されている • LDAPサーバーをバインドし、ユーザー、グループ、組織単位のサブツリーを検索できる これは通常、ディレクトリ管理者の認証情報（DN、つまり識別名、とパスワード）を有するアカウントです。
パスワード	アカウントのパスワードを入力します。
パスワードの確認	アカウントのパスワードを再入力します。
ディレクトリ種類	サポートされているディレクトリのリストからディレクトリの種類を選択します。 • Microsoft Active Directory • LDAPを開く • その他（OpenLDAP対応）

3. **[接続をテストして続行]** をクリックします。

   この手順により、ここまで入力した情報が検証されます。

   - 情報が有効であると認められると、サービスはLDAPの命名コンテキストを読み出し、それを使用して次ページのいくつかのフィールドに入力します。
   - LDAP URLに接続できなくても、次の手順に進めます。ただし、接続が解決されるまで機能が制限される場合があります。

4. 残りの設定を完了させます。

設定	操作内容
ディレクトリフェイルオーバーのURL	セカンダリディレクトリのURLを入力します。次のフォーマットを使用します。 ldap://IPアドレスまたは 例：ldap://myserver2.mycompany.com:389
同期間隔	LDAPサーバーからLDAPデータを同期する間隔を入力します。デフォルト値は15分です。ターゲットのLDAPデータをすべて正常に同期し終わり、LDAP設定がニーズに合っていることを確認したら、この間隔を増やすことを検討してください。
同期放棄を有効化	リロードされたデータセットが大幅に減少している場合は、LDAP同期データを自動的に破棄するという設定を選択します。このオプションは、LDAPシステムの部分的な異常動作によってサービスに故障の原因となる不必要なアップデートが発生したり、登録済みのデバイスから構成が削除されるといった状況を防ぐものです。LDAP設定またはLDAPサーバーに大幅な変更を加える予定がある場合は、このオプションが選択されていないことを確認してください。
このLDAPサーバーを有効化	このLDAPサーバーをサービスで使用するという設定を選択します。このLDAPサーバーを撤去するか、サービス停止にする場合は、この設定を解除します。セカンドLDAPサーバーに対する構成済みのフェイルオーバーによりこのサーバーが自動的に置き換えられますが、このオプションを利用すると、事前に計画を立て、フェイルオーバー中の短時間の接続不能状態を回避することができます。
インポートされたユーザーを自動的に招待する	LDAPサーバーからインポートされたユーザーに自動的に招待状を送る場合に選択します。
CA証明書をアップロード	**[ファイルを選択]**をクリックし、このLDAPサーバーにインストールされているCA発行のTLS証明書ををアップロードします。CA証明書は複数アップロードできます。
参照元追跡	マルチフォレストのドメインを使用している場合のみ該当します。このオプションは、要求されたオブジェクトのコピーがターゲットのドメインコントローラにない場合に、別のドメインコントローラを使用するかどうかを示します。

設定	操作内容
	• 参照元を使用したい場合は **[フォロー]** を選択します。 • 別のドメインコントローラを使用しない場合は **[無視]** を選択します。 • **[スロー]** も現在のところ **[無視]** と同じ効果を持ちます。 **[フォロー]** を選択するとLDAP認証が遅くなります。
検索結果のタイムアウト	LDAPサーバーから同期したデータの閲覧時にパフォーマンスの問題が発生したり、結果が不完全であったりする場合には、このタイムアウトの値を増やします。
検索結果数	LDAPサーバーから一度に返すべきレコードの最大数を設定します。パフォーマンス改善のためにこの設定の変更が必要となるようなシナリオは以下のとおりです。 • LDAPサーバーが非常に遠方にあるか、待ち時間の長いリンクの先にある場合。この場合は、検索結果が大きければ、小さな検索結果よりも読み出しに時間がかかるため、小さなセットを定義することで、更新されたデータのサブセットをより迅速に表示できるようになります。 • LDAPの規模が大きく、毎回の検索で膨大な結果セットが返される場合。この場合は、パフォーマンスに問題がなければ、より大きな結果セットを定義すると、少ない検索回数ですべてのデータを返すことができるようになります。

5. **[次へ]** をクリックします。
6. 次のガイドラインを利用して、LDAPサーバーとの統合を構成します。

設定	操作内容
グループメンバー形式	**[DN]** または **[UID]** を選択し、検索で識別名とユーザーIDのいずれを使うかを示します。
OU検索属性	組織単位レベルでの検索基準を指定します。

ベースDN	検索のrootとしたい、あるいはそこから検索を始めたいレベルの識別名を入力します。この選択により他のフィールドのデフォルト値が決まりますが、それらは必要に応じて変更することができます。
オブジェクトGUID	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびOU名の変更を越えて組織単位を一意に識別する属性です。
属性名	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
説明	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
属性DN	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
フィルタの検索	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
範囲を検索	ターゲットに対するLDAPの階層の部分を選択します。 • **ベース**(検索ベースエントリのみのレベル) • **ワンレベル**(検索ベースの下のレベル) • **サブツリー**(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー)
ユーザー検索属性	任意のディレクトリレベルでのユーザー検索のための基準を指定します。
ベースDN	検索を始めるレベルの識別名を入力します。
属性UID	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
オブジェクトGUID	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびユーザー名の変更を越えてユーザーを一意に識別する属性です。
属性DN	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。

名	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
性	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
表示名	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
Eメールアドレス	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
プリンシパル名	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
ロケール	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
所属メンバー	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
フィルタの検索	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
範囲を検索	ターゲットに対するLDAPの階層の部分を選択します。 • **ベース**(検索ベースエントリのみのレベル) • **ワンレベル**(検索ベースの下のレベル) • **サブツリー**(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー)

管理対象Apple ID	LDAPユーザーの管理対象Apple IDの同期を選択します。
	• **なし**
	• **パターン** -
	  • **ユーザーのメールアドレス**
	  • **userUPN**
	• 任意で **[「appleid」サブドメインを含める]** オプションを選択し、既存のApple IDとの競合を避けます。

+カスタム属性の追加	(オプション) ディレクトリサービスからデバイス管理に適用したいカスタムユーザー属性を7つまで指定します。これにより、各属性は、変数をサポートする構成フィールドの${attributeName}によって参照されます。 **重要:** このオプションを使用するには、LDAPサーバー全体を通じてカスタム属性を一貫して実装しておく必要があります。実装に含まれるLDAPサーバーの1つがこの属性を使用していない場合、この属性に依存する機能が意図通りに機能しないことがあります。
グループ検索属性	
ベースDN	検索を始めるレベルの識別名を入力します。
オブジェクトGUID	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。これは、時間およびグループ名の変更を越えてグループを一意に識別する属性です。
属性DN	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
属性名	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
説明	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
メンバー	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
フィルタの検索	必要に応じて、お使いのLDAP環境に合うようデフォルト値を変更します。
範囲を検索	ターゲットに対するLDAPの階層の部分を選択します。 • **ベース**(検索ベースエントリのみのレベル) • **ワンレベル**(検索ベースの下のレベル) • **サブツリー**(検索ベースDNの下のディレクトリ情報ツリーにあるサブツリー)

7. **[参照]** または **[検索]** をクリックします。

8. 構成により想定されたデータが返されていることを確認します。

   ディレクトリ内で既知の項目を参照または検索することにより、これを実行できます。

9. **[次へ]** をクリックします。

カスタムLDAP属性の削除

カスタムLDAP属性を削除し、その値を関連ユーザー/デバイスから削除します。

手順

1. **[管理]** > **[属性]** を開きます。
2. **[カスタム属性]** セクションで、削除したいLDAP属性の隣にある **[削除]** リンクをクリックします。確認ウィンドウが表示されます。
3. **[削除]** をクリックして削除を確定します。

> **[削除]** ボタンはデフォルトで無効化されています。**[カスタム属性の削除が元に戻せないことを理解します。]** オプションのチェックボックスを選択し、**[削除]** ボタンを有効化してください。

LDAPサーバー情報の編集

手順

1. **[管理]** > **[LDAP]** を開きます。
2. LDAPサーバーエントリの **[アクション]** 列から **[編集]** アイコンを選択し、[LDAPサーバーに接続] ページを表示させます。
3. 必要な変更を施します。
4. **[接続をテストして続行]** をクリックします。
   LDAP URLに接続できなくても、次の手順に進んでかまいません。ただし、接続が解決されるまで機能が制限される場合があります。
5. **[参照]** または **[検索]** をクリックします。
6. 構成により想定されたデータが返されていることを確認します。
   ディレクトリ内で既知の項目を参照または検索することにより、これを実行できます。
7. **[完了]** をクリックします。

LDAPユーザーのインポート

手順

1. **[ユーザー]** を開きます。
2. **[+追加]** > **[LDAPからユーザーを招待]** をクリックします。
3. LDAPサーバーエントリ中の **[ユーザーを選択]** をクリックします。
4. [LDAPユーザーを追加] ページで、ユーザー、グループ、OUの名前を検索フィールドを入力します。
5. 新規ユーザーやグループを追加するには、追加したいエントリの横にある **[+追加]** をクリックします。
6. **[次へ]** をクリックします。
7. 招待状を送信するかどうかを選択します。
   - 誰も招待しない
     後で招待を送信するには、**[ユーザ]** > **[ユーザ]** へ進み、**[アクション]** > **[招待を送信]** を選択して招待を送信します。
   - すべて招待
8. **[完了]** をクリックします。

選択したユーザー、グループ、組織単位の更新

手順

1. **[管理]** > **[LDAP]** を開きます。
2. LDAPサーバーエントリの **[アクション]** カラムから **[ユーザーを管理]** アイコンを選択し、[LDAPユーザーを追加] ページを表示します。
3. 新規ユーザーやグループを追加するには、検索フィールドにユーザー名またはグループ名を入力します。
4. 追加したいエントリの横にある **[+追加]** をクリックします。
5. ユーザー、グループ、OUを削除するには、削除したいエントリの横にある削除アイコンをクリックします。
6. **[完了]** をクリックします。

LDAP同期放棄通知の有効化

LDAP同期放棄通知の有効化により、LDAP環境への予期しない大規模な変更による機能停止が防止されます。

手順

1. **[管理] > [LDAP]** を開きます。
2. LDAPサーバーエントリの **[アクション]** 列から **[編集]** アイコンを選択し、[LDAPサーバーに接続] ページを表示させます。
3. **[同期放棄を有効化]** チェックボックスをオンにします。
4. 同期放棄を実行する基準となるリロード済みLDAPデータの割合を入力します。
5. **[接続をテストして続行]** をクリックします。
   LDAP URLに接続できなくても、次の手順に進めます。ただし、接続が解決されるまで機能が制限される場合があります。
6. **[完了]** をクリックします。
7. LDAPサーバーエントリ中の **[今すぐ同期]** アイコンをクリックします。
   LDAPからIvanti Neurons for MDMへ同期される変更が、所定の放棄割合を上回る場合、警告通知が生成されます。変更が設定した割合を再び下回った場合は、通知が解除されます。

送信基準	Severity (重大度)	通知の種類	コンポーネントの種類	コンポーネント
LDAP同期放棄	警告	データ同期	LDAP	LDAPサーバー名
LDAP同期復元	情報	データ同期	LDAP	LDAPサーバー名

部分的同期放棄は、1つ以上のユーザーレコードがLDAPからの同期に失敗した場合に生成されます。この場合、同期できなかったユーザーのリストがCSVファイルとして添付されます。ユーザーが属性の不足によって放棄された場合は、欠けている属性のリストもエクスポートされたCSVファイルに含まれます。

LDAPサーバーからの変更の同期

[LDAP] ページで、LDAPサーバーエントリ中の **[今すぐ同期]** アイコンをクリックします。

LDAPSサーバーへの接続に関するトラブルシューティング

LDAPS(LDAP over SSL) サーバーへの接続に問題が発生した場合は、証明書に問題がある可能性があります。

問題を解消するには:

- LDAPSサーバー上で自己署名証明書を使用していないことを確認してください。
- LDAPS証明書の有効期限切れ、無効化がないか確認してください。また、ホスト名の不一致がないか確認してください。

確認後、自動LDAP同期を待つか、LDAPサーバーエントリ中の **[管理]** > **[LDAP]** > **[今すぐ同期]** アイコンを使用して手動で同期します。

[LDAP] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

[Sentry]

Sentryは、モバイルデバイスとActiveSync対応Eメールシステムを結ぶゲートウェイとして機能するコンポーネントです。Sentryにより、Eメールにアクセスできるデバイスを制御できます。Sentryは、仮想マシンにインストールできるISOファイルとしてダウンロードできます。組織は、ロードバランサーを使用して複数の(冗長)Sentryを維持することを検討する必要があります。

ライセンス：Silver

最新ドキュメンテーション

Sentryの最新説明書は、製品ドキュメンテーションで [Sentry] をクリックしてください。

最新のSentryインストール方法は、*「Standalone Sentryオンプレインストールガイド」*の適切なバージョンをご覧ください。

Sentryのアップグレード方法は、*「Sentryガイド」*の適切なバージョンをご覧ください。Sentryガイドの以下のセクションをご覧ください。

- Standalone Sentry System Manager UIを使用したアップグレード方法は、「Standalone Sentryソフトウェア更新」をご覧ください。
- Standalone Sentryコマンドラインインタフェース(CLI)を使用したアップグレード方法は、「CLIを使用したアップグレード」をご覧ください。

アップグレードする前に、Standalone Sentryのアップグレード先のバージョンのリリースノートをご覧ください。

Appleの設 定

このセクションは以 下 のトピックを含 みます。

Apple Configurator

このページを使用して、iOSデバイス上でIvanti Neurons for MDMデバイス管理をセットアップするためのApple Configuratorを準備することができます。Apple Configuratorは大規模のiOSデバイスの展開を非常に容易にします。さらに、Configuratorでは管理者がiOSデバイスを監視対象にすることができ、これによりレベルの高い構成および管理機能を可能にします。Apple Configuratorの詳細は、Mac App Storeをご覧ください。

基本的な手順は次のとおりです。

1. Ivanti Neurons for MDMテナントからMDMプロファイルをエクスポートします。
2. ConfiguratorにMDMプロファイルをインポートします。
3. Configuratorを使用し、テザードされたデバイスにMDMプロファイルを適用します。

デバイスのデフォルトユーザーの定義

Apple Configuratorで構成されたデバイスは、別のユーザーを選択しない限り、Ivanti Neurons for MDMではnobodyユーザーに割り当てられます。

1. **[構成されたデバイスを以下に割り当てる]** フィールドをクリックします。
2. 選択したいIvanti Neurons for MDMユーザーのユーザー名を入力し始めます。
3. ユーザー名がドロップダウンリストに表示されたら選択します。
4. **[保存]** をクリックします。

Apple Configuratorを使用したアプリのインストール

Apple Configuratorを使用してアプリをインストールする前に:

- Apple App Storeへのアクセスは、デバイス構成によって制限されています。
- アプリのインストールは、デバイス構成によって許可されています。
- デバイス構成に使用するコンピュータ上に、Apple Configuratorがインストールされている必要があります。

Apple Configuratorを使用してアプリをインストールするには:

1. Ivanti Neurons for MDM で **[管理] > [Apple Configurator]** を選択します。
2. 登録デバイス切換を [オン] にします。
3. 次のいずれかをクリックします。
   - **デフォルトユーザーのplist**
   - **特定ユーザーのplist** - 特定ユーザーのユーザー名またはメールIDを入力します。
4. Apple Configuratorで、**[準備] > [アプリ]** を開きます。
5. **[準備] > [設定] を開き、[監視] を無効化します**。
6. [iOSのアップデート] で、**[デバイスをアップデートしない]** を選択します。
7. **[準備]**(Apple Configuratorの下) をクリックします。
   デバイスにチェックインすると、デバイス上のインストール済みアプリのリストにアプリが表示されるようになります。

UEMサーバーを使用したアプリのインストール

UEMサーバーを使用してアプリをインストールするには:

1. [アプリ] タブの社内ストアからアプリをアップロードします。
2. アプリを選択します。
3. **[アプリ構成]** タブをクリックします。
4. **[デバイスにインストール]** を選択します。
   構成設定を完了させます。
5. **[アクション] > [チェックインの強制]** を選択します。

エンドユーザーが実行すべき内容

Appleの場合、エンドユーザーが一度Goを起動する必要があります。この操作を行わないと、Ivanti Neurons for MDM 位置情報機能が正しく動作しません。これは、エンドユーザーに自分の位置が追跡されるということを認識してもらうための措置です。

注: Configuratorを使用してデバイスをSingle Appモードで展開している場合は、このアプローチは実行できません。

[Apple Configuratorのインストール] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- 読み取り専用システム

デバイス登録

Apple Business Manager のデバイス登録では、デバイスを一括で購入し、認証中に自動的にこれらのデバイスを MDM に登録できます。参加する場合、Ivanti Neurons for MDM をこれらのデバイスを管理するMDMサーバーとして利用できます。詳細はhttps://business.apple.com/をご覧ください。

Ivanti Neurons for MDM とDevice Enrollmentの連携

Ivanti Neurons for MDM をDevice Enrollment用のMDMサーバーとして使用するには、Ivanti Neurons for MDM でApple Business Managerサーバートークンをセットアップします。

各 Apple Business Managerサーバーについて、Ivanti Neurons for MDMで次の操作を実行できます。

- 接続をテスト
- Device Enrollmentプロファイルを追加
- パブリックキーをダウンロード
- Device Enrollmentフル同期 - フル同期を開始します。完了に時間がかかることがあります。同期が完了すると、[前回の同期] カラムで情報を見ることができます。フル同期がすでに進行中の場合はフル同期を開始できません。
- 新規トークンをアップロード
- 削除

[認証を編集] と **[Device Enrollmentデバイス属性を指定]** アクションは、Device Enrollment(MDM サーバー) ではなくDevice Enrollmentプロファイルについて実行可能となります。

手順

1. **[管理]** > **[Apple]** > **[Device Enrollment]** を開きます。
2. **[ダウンロードキー]** をクリックします。
3. Ivanti Neurons for MDMキーを保存します。
4. **business.apple.com**をクリックします。
5. Device Enrollment対応のApple認証情報を使用してサインインします。

6. Apple Device Enrollmentサイトで：
    a. **[開始]** をクリックします。
    b. Appleのサービスの認証に使用する信頼できる電話を選択します。
    c. 選択された電話に送信する検証コードを入力します。
    d. **[MDMサーバーを追加]** をクリックします。
    e. サービスで利用する仮想MDMサーバーを識別する名前を入力します。
    f. **[次へ]** をクリックします。
    g. 先にダウンロードしておいたパブリックキーをアップロードします。
    h. **[次へ]** をクリックします。
    i. **[お使いのサーバートークン]** をクリックしてトークンをダウンロードします。
    j. **[完了]** をクリックします。
7. Ivanti Neurons for MDMで **[アップロード]** をクリックします。
8. **[次へ]** をクリックします。

9. 認証オプションを選択します。

   - **ユーザーに登録/ログインを指示**

     ユーザーはユーザー名とパスワードの入力を求められます。ユーザーはパスワードまたはPINをパスワードフィールドに入力します。認証に関するパスワードとPINの設定は [ユーザー] > **[ユーザー設定]** で行います。

   - **ユーザーログインをスキップ**

     nobody(匿名)ユーザーまたは定義済みのユーザーに割り当てられているデバイスは、後で **[デバイス]** ページから特定のユーザーに再割り当てが可能です。

     以下のオプションから1つ選択してください:

     - **1人のユーザーを定義して全デバイスを割り当てる**
     - **全デバイスを匿名ユーザー1人に割り当てる**

   選択されたオプションが、[ユーザー設定] の選択肢より優先されます。

10. **[アップロード]** をクリックし、ステップ3で受領したキーをインストールします。
11. 表示されているフォームに入力し、Device Enrollmentデバイスのプロファイルを定義します。

設定	操作内容
名前	このDevice Enrollmentプロファイルを識別する名前を入力します。
説明	プロファイルの説明を入力します。
部署	このプロファイルに関連付けられている組織内の部署の名前を入力します。
監視モード	構成や制限において追加管理を有効化します。iOS 13+およびmacOS 10.15+のデバイスでは、このオプションがデフォルトで有効化されています。

設定	操作内容
iOS更新を自動的にダウンロードおよびインストール	(iOS 9.0+のみ) **[設定] > [iTunes & App Store]** で自動ダウンロードオプションを選択した場合、OS更新は自動的にダウンロードされますが、デバイス登録プロファイルオプションがオフの場合でも、インストールはされません。この設定は、Device Enrollment登録済みの監視対象デバイスに適用されるiOSソフトウェア更新設定がある場合に優先されます。この設定の変更はすべて、デバイスのリセットがなくてもDevice Enrollment登録済みの監視対象デバイスに適用されます。
MDM削除可能	デバイスの登録後、ユーザーがMDMから登録を解除できないかどうかを定義します。 この設定は共有iPadには適用されません。
MDM必須要件	アクティベーションプロセス中に、ユーザーが、MDMのインストールをスキップできないかどうかを定義します。iOS 13+およびmacOS 10.15+のデバイスでは、このオプションがデフォルトで有効化されています。
ペアリングを許可	(iOS 13+、macOS 10.15+は対象外) iTunes同期などのホストペアリング機能を許可します。有効なペアリング証明書を持つホストに対し、ペアリングが常に許可されます。
証明書	**[+追加]** をクリックして証明書をアップロードします。
サポート電話番号	デバイスユーザーがサポートを依頼できる電話番号を入力します。
Eメールアドレスをサポート	デバイスユーザーがサポートを依頼で

設定	操作内容
	きるメールアドレスを提供します。
カスタム登録	(iOS 13.0+ and macOS 10.15+) カスタム登録Webページを作成します。Device Enrollmentでユーザーを認証するカスタムWebページ(Web View) を指定します。このページには、認証の形式、ブランディング、同意する文章、プライバシーポリシーなどのカスタム情報を表示します。詳細は、以下の手順で「*Device Enrollmentカスタム*Webページの追加」セクションをご覧ください。 • **[カスタム登録を有効化]** を選択し、この機能を有効化します。 • https://mycustomweburl.com など、**URL**を入力します。このURLが、Web Viewでユーザーに提示するカスタムURLの値を定義します。
マルチユーザー	(iOS 13.4+) ビジネス向け共有iPad 企業において、パーソナライズされた経験を維持しながら、複数の従業員間でデバイスを共有させることができます。 デバイスで共有iPadを有効化するには **[マルチユーザーモード]** を選択します。詳細はビジネス向け共有iPadを参照してください。

設定	操作内容
	• この設定は、Apple Educationには適用されません。 • マルチユーザー設定を変更するには **[監視モード]** 設定を選択します。
割り当て量	(iOS 13.4+) ビジネス向け共有iPad 単位はメガバイト(MB)で、デバイス内で1人のユーザーに割り当てられているストレージの容量を示します。値が小さすぎる場合、デフォルトの割り当て量がデバイスに割り当てられます。
常駐ユーザー	(iOS 13.4+) ビジネス向け共有iPad この値は、デバイス上に持続的に存在する、または常駐するユーザー数を示します。この値がデバイスがサポートするユーザーの最大数より大きい場合、MDMサーバーは最大ユーザー数をデフォルトとして使用します。 管理者は割り当て量または常駐ユーザー数を指定できます。両方の値がある場合、MDMサーバーはデフォルトで割り当て量を使用します。
ユーザーセッションタイムアウト	(iOS 14.5+) ビジネス向け共有iPad

設定	操作内容
	ユーザーセッションのタイムアウト時間(秒)を示します。ユーザーセッションは指定の時間だけ動作がなければ自動的にログアウトとなります。最小値は30秒です。この値を0に設定するとタイムアウトがなくなり、デバイスのデフォルトタイムアウトが適用されます。 1～29の値は無効です。1～29に設定するとデフォルトのタイムアウトに設定されます。
一時セッションタイムアウト	(iOS 14.5+) ビジネス向け共有iPad ゲストまたは一時セッションのタイムアウト時間(秒)を示します。一時セッションは指定の時間だけ動作がなければ自動的にログアウトとなります。最小値は30秒です。この値を0に設定するとタイムアウトがなくなり、デバイスのデフォルトタイムアウトが適用されます。 1～29の値は無効です。1～29に設定するとデフォルトのタイムアウトに設定されます。
一時セッションのみ	(iOS 14.5+) ビジネス向け共有iPad Trueの場合、ユーザーにはゲスト用ウェルカム画面のみ表示され、ユーザーはゲストユーザーとしてのみログインできます。

設定	操作内容
	Falseの場合、ユーザーは管理対象Apple IDでサインインできます(既存の挙動)。 デフォルト:False
管理されたApple IDの既定のドメイン	(iOS 16.0+)ビジネス向け共有iPad ドメインのリストを指定します。ユーザーはQuickTypeキーボードのドメインのリストから各自のアカウントドメインを選択できます。
オンライン認証猶予期間	(iOS 16.0+)ビジネス向け共有iPad ユーザーがネットワークに接続せずにログインできる日数を指定します。 この値をゼロに設定すると、毎回オンライン認証が強制的に実行されます。 **デフォルト**:0
タイムゾーン	デバイスのタイムゾーンを指定します。 **例**:太平洋/ミッドウェー

以下の設定オプションで、デバイスアクティベーション中にユーザーがスキップしてもよい手順を定義します。

設定オプション
• パスコードの入力をスキップ - これを選択すると、Apple Pay設定のスキップとTouch ID設定のスキップが自動的に有効化されます。 • 位置情報サービスをスキップ • バックアップからの復元をスキップ • Androidからの「iOS移行」をスキップ • 利用規約をスキップ • Apple IDおよびiCloudへのサインインをスキップ - これを選択すると、Apple Pay設定のスキップが自動的に有効化されます。 • Touch ID設定をスキップ(iPhone 5s、6、6+、iPad Air 2、iPad Mini 3のみ) - これを選択すると、Apple Pay設定のスキップが自動的に有効化されます。 • Apple Pay設定をスキップ(iPhone 6、6+、iPad Air 2、iPad Mini 3のみ) • Zoom設定をスキップ • Siriをスキップ • 診断情報の自動送信をスキップ • クラウドストレージをスキップ(iOS 10.3、macOS 10.13.4以降) • ディスプレイ色設定をスキップ(iOS 9、macOS 10.14以降) • ホームボタン感度をスキップ • キーボード選択画面をスキップ • オンボーディング情報画面をスキップ - この情報はユーザー向けです。カバーシート、マルチタスキング& コントロールセンターなど。 • Apple Watch移行画面をスキップ • 「アピアランスを選択」画面をスキップ(iOS 13.0+およびmacOS 10.14+)

設定オプション
• スクリーンタイムをスキップ(iOS 12.0+およびmacOS 10.15+) • プライバシーをスキップ(macOS 10.13.4、tvOS 11.3以降) • 携帯電話プランペインの追加をスキップ(iPhone Xs、iPhone Xs Max、iPhone XR) • ログインページにカスタムテキストを表示 - テキストボックスにカスタムテキストメッセージを入力する場合には、このオプションを選択します。このメッセージは、Device Enrollmentの設定中にデバイスのログインページに表示され、エンドユーザーの作業に役立つ情報を提供します。 • 自動詳細設定 - このオプションを選択すると、設定アシスタントがデバイスの設定画面を自動的に進めます。デフォルトはfalseです。tvOSおよびmacOS 11以降でサポートされています。自動詳細設定はWi-Fi接続では機能しません。デバイスにはイーサネット接続が必要です。 • 住所条件 - 住所条件ペインをスキップします。(iOS 16+)
iOS
• ソフトウェア更新をスキップ(12.0+) • 開始ペインをスキップ(13.0+) • iMessageとFaceTimeをスキップ(12.0+) • 復元完了をスキップ(14.0+) • 更新完了をスキップ(14.0+)
macOS
• iCloud Analytics画面をスキップ • True Toneディスプレイ画面をスキップ(macOS 10.13.6+) - (任意) True Toneディスプレイ画面をスキップする場合に選択します。 • アクセシビリティをスキップ(macOS 11.0+) • Watchでロック解除をスキップ(macOS 12.0+)

設定オプション
tvOS
• Apple TVホーム画面レイアウト同期画面をスキップ • Apple TVプロバイダーサインイン画面をスキップ • 「タップして設定」オプションをスキップ • Aerialスクリーンセーバー設定をスキップ
macOSアカウント設定アシスタントオプション
• 管理アカウント作成をスキップ • プライマリ設定アカウント作成をスキップ • プライマリアカウントをレギュラーユーザーとして作成(チェックがなければ管理者として)
デバイス登録の設定中にデバイス構成を待機
• 構成および優先度の高いアプリケーションがデバイスにプッシュされるまで待機 - 構成および優先度の高いアプリケーションをデバイスにプッシュしてから、残りのデバイス登録設定画面に進む場合に選択します。この設定によりエンドユーザーは、必要な構成と優先度の高いアプリケーションがデバイスにプッシュされるまでデバイスを使用できなくなります。 • 時間制限 - デフォルトの時間制限は3分です。最大で10分に設定できます。 この機能を有効化するには、Device Enrollmentプロファイルの編集中に **[監視モード]** オプションを選択します。

12. **[保存]** をクリックします。
    次の表は、**[管理]** > **[Apple]** > **[デバイス登録]** ページで入力されます。

設定	操作内容
[名前] (列見出しをクリックすると、アルファベット順に並べ替えられます。) この列の項目を検索するには [検索] フィールドを使用します	MDM サーバ名
Apple アカウント名 (列見出しをクリックすると、アルファベット順に並べ替えられます。) この列の項目を検索するには [検索] フィールドを使用します	管理対象 Apple ID
デバイス数	割り当てられたデバイスの数
登録プロファイル	割り当てられたデバイス登録プロファイルの数
前回同期日時 (列見出しをクリックすると、アルファベット順に並べ替えられます。)	前回接続日時
トークンの有効期限 (列見出しをクリックすると、アルファベット順に並べ替えられます。)	トークン有効期限

- Apple Device Enrollmentに新規デバイスを追加する際、Ivanti Neurons for MDM が新規デバイスを検出するまでに最長で15分かかる場合があります。その後、新規デバイスに登録プロファイルが割り当てられます。Device Enrollmentに新規デバイスを追加できない場合は、**[ダッシュボード]** > **[通知]** を開き、Device Enrollmentに関するAppleからの通知を確認してください。EULAに更新がある場合は、新しいEULAを承諾する手順がメールで通知されます。

- Apple Device Enrollment経由での登録中、テナントに存在するすべてのカスタムデバイス属性を閲覧し、デバイスに割り当てることができます。
- 共有 macOS デバイスでは、`ListUsers` コマンドを実行すると、デバイスのすべてのローカル ユーザのリストと、デバイスを登録したユーザの前回のチェックイン詳細情報のみが表示されます。

Device Enrollmentプロファイルの編集

手順

1. **[管理]** > **[Apple]** > **[Device Enrollment]** を開きます。
2. Apple Business Managerサーバー(Appleのサイトで作成したもの) の名前をAppleアカウント名のカラムから見つけます。
3. Enrollmentプロファイルカラムで数字のリンクをクリックします。
4. 具体的なプロファイルで **[アクション]** > **[Device Enrollmentプロファイルを編集]** を開きます。
5. プロファイルを更新および保存します。

- Device Enrollmentプロファイルが編集された場合、変更済みプロファイルのデバイス数がすぐに更新されます。
- Appleのサイトでサーバートークンを更新している場合は、既存のトークンが無効となります。ただし、トークンの有効期限を含むDevice Enrollmentページの表示内容は、新しいトークンをアップロードするまで変更されません。

デバイス登録プロファイルには、次の詳細情報が含まれます。

設定	操作内容
プロファイル名 (列見出しをクリックすると、アルファベット順に並べ替えられます。)	このDevice Enrollmentプロファイルを識別する名前を入力します。
説明 (列見出しをクリックすると、アルファベット順に並べ替えられます。)	プロファイルの説明を入力します。
部署	このプロファイルに関連付けられている組織内の部署の名前を入力します。

設定	操作内容
(列見出しをクリックすると、アルファベット順に並べ替えられます。)	
サポート電話番号 (列見出しをクリックすると、アルファベット順に並べ替えられます。)	デバイスユーザーがサポートを依頼できる電話番号を入力します。
デバイス数	プロファイルのデバイス数が表示されます。
アクション	プロファイルの管理

複数のDevice Enrollmentプロファイルの管理

各Apple Business Managerサーバーに対してDevice Enrollmentプロファイルは複数作成できます。これにより異なるデバイス群に異なる構成を配布します。1つのDevice Enrollmentプロファイルから別のDevice Enrollmentプロファイルへデバイスを移動することも可能です。

手順

1. **[管理]** > **[Apple]** > **[Device Enrollment]** を開きます。
2. Apple Business Managerサーバーの名前をAppleアカウント名のカラムで探します。
3. Enrollmentプロファイルカラムで数字のリンクをクリックします。
4. 新しいDevice Enrollmentプロファイルを作成し、選択したサーバーに関連付けるには **[新規プロファイルを作成]** をクリックします。プロファイルを作成および保存します。

5. 各プロファイルを管理するには、**[アクション]** をクリックし、以下のいずれかを選択します。

   - **デフォルトのプロファイルに設定** - 同じ仮想サーバー内でのデフォルトのプロファイルに設定します。新しいデバイスを登録するとこのデフォルトプロファイルを受信します。
   - **プロファイルを編集** - 既存のプロファイルを編集します。
   - **認証を編集** - Device Enrollment認証設定を編集します。
   - **Device Enrollmentデバイス属性を指定** - 管理者は、デバイスのカスタム属性を利用し、追加プロパティをこれらのオブジェクトと関連付けます。これにより、そのプロパティをグループのビルドや構成の配布に利用可能となります。
   - **削除** - デフォルトのプロファイルは削除できません。デフォルト以外のプロファイルを削除すると、関連するすべてのデバイスがデフォルトのプロファイルに割り当てられます。

6. 同じ仮想サーバー内で(異なるApple Business Managerサーバー間ではなく) 1つのプロファイルから別のプロファイルへ登録済みデバイスを移動するには、[デバイス数] カラムで数字のリンクをクリックします。プロファイルの再割り当てはまだ登録されていないデバイスに適用されます。

   a. デバイス1台を移動するには、特定のデバイスについて **[Enrollmentプロファイルを割り当てる]** をクリックし、ドロップダウンリストからプロファイルを選択して **[割り当てる]** をクリックします。

   b. 複数のデバイスを移動するには、デバイスを選択し、**[アクション]** > **[Enrollmentプロファイルを割り当てる]** を開いた後、ドロップダウンリストからプロファイルを選択して **[割り当てる]** をクリックします。

- Device Enrollmentプロファイルが編集された場合、変更済みプロファイルのデバイス数がすぐに更新されます。
- Appleのサイトでサーバートークンを更新している場合は、既存のトークンが無効となります。ただし、トークンの有効期限を含むDevice Enrollmentページの表示内容は、新しいトークンをアップロードするまで変更されません。

Device EnrollmentカスタムWebページの追加

対象: iOS 13.0、macOS 10.15、およびサポートされる以降のバージョン

カスタム登録セクションでは、Device Enrollmentでユーザーを認証するカスタムWebページ(Web View) を指定できます。このページには、認証の形式、ブランディング、同意する文章、プライバシーポリシーなどのカスタム情報を表示します。

手順

1. **[管理]** > **[Apple]** > **[Device Enrollment]** を開きます。
2. Appleのサイトで作成したサーバー名を探します。
3. **[アクション]** > **[Device Enrollmentプロファイルを編集]** を開きます。
4. カスタム登録セクションで **[カスタム登録を有効化]** を選択します。
5. 以下のオプションから1つ選択してください：

    - **MobileIronがホストするWebページ** - 登録がMicrosoft Active Directory Federation Services (ADFS) やOktaなどのIDプロバイダー(IDP) を使用している場合はIDプロバイダー(IDP) にリダイレクトされます。IDP以外の認証を使用するIvanti Neurons for MDMユーザーの場合はセルフサービスポータルにリダイレクトされる場合もあります。
    - **カスタムURL** - https://mycustomweburl.comなどのURLを入力します。このURLが、新しいDevice Enrollmentデバイスまたは消去したデバイスの初期設定中に読み込まれるWeb Viewでユーザーに提示するカスタムURLの値を定義します。このフィールドを使用し、独自の認証UIと認証方法を定義してください。ユーザーの認証後、MDM登録プロファイルがダウンロードされます。

Device EnrollmenカスタムWebページのワークフロー

このセクションでは、Device EnrollmenカスタムWebページの機能とカスタムWebページ(Web View) 作成手順を詳細に指定します。

URLフィールドに指定されたカスタムWebページが初めて読み込まれたとき：

- 構成Web URLは**https**形式で、**GET**リクエストです。このWebページはパブリック証明書を使用する必要があります。
- 登録を開始したAppleデバイスにより、GETリクエストにカスタムヘッダー「**x-apple-aspen-deviceinfo**」が付加されます。これには、デバイス属性のplistを含むCMS(暗号メッセージ構文) エンベロープのbase64エンコーディングが含まれます。これは、トークンベースのデバイス登録における当初のPOSTリクエストで提供されるのと同じ形式の同じ情報です。

その後、カスタムWebページが読み込まれたとき：

- デバイスユーザは、管理者のホストサーバが**custom.mobileconfig**ファイルをクライアントに提供するまで、カスタムWebページ(Web View) を使用します。Ivanti Neurons for MDMサーバーは、MDMプロファイルのバイトコードを返します。管理者のホストサーバーでは、custom.mobileconfigファイルを**application/x-apple-aspen-config**のMIMEタイプともに設定する必要があります。これにより、デバイスのMDMプロファイルがダウンロードされ、デバイスにインストールされます。

- Ivanti Neurons for MDMの認証用として、Webページには認証ユーザー名とパスワード情報を含める必要があります。Ivanti Neurons for MDMでは別のユーザを作成し、そのユーザにIvanti Neurons for MDMサーバURL(https://micloudDomain.com/c/i/dep/custom.mobileconfigなど) でMDMプロファイルを取得するカスタム登録の役割を指定することをお勧めします。
- デバイスを登録し、MDMプロファイルをIvanti Neurons for MDMから取得するため、管理者のホストWebサーバーはIvanti Neurons for MDMサーバーURLへのPOSTコールを実行する必要があります。また、デバイスがGET URLにアクセスし、カスタムWebページを読み込む際に、ヘッダー「x-apple-aspen-deviceinfo」とデバイスが提供する値を渡す必要があります。登録ユーザーIDが提供されない場合、デバイスはnobodyユーザーとして登録されます。その他の情報は以下をご覧ください。
  - デバイスがDevice Enrollmentプロファイルに設定されたカスタムURLにアクセスすると、管理者のホストWebサーバーはデバイスが提示するヘッダー「x-apple-aspen-deviceinfo」を取得します。
  - そのデバイスのMDMプロファイルと関連ユーザーを取得するため、管理者のホストWebサーバーはIvanti Neurons for MDMサーバーURLに対してヘッダー「x-apple-aspen-deviceinfo」のPOSTコールを実行する必要があります。これは、Ivanti Neurons for MDMのユーザーIDを要求パラメータとする基本的な認証情報 (https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.comなど) を含みます。ユーザーにはカスタム登録の役割が指定されます。
  - 管理者のホストWebサーバーは、バイトコードを受け取った後、応答ヘッダー「Content-Disposition = attachment;filename="profile.mobileconfig」と「Content-Type = application/x-apple-aspen-config」を設定することにより、バイトコードをデバイスにダウンロードします。
- Web Viewが閉じ、OSがプロファイルのインストールを試みます。これはMDM登録プロファイルでなければなりません。

Ivanti Neurons for MDM は、MDMプロファイルが戻されたユーザーIDを認証しません。したがって管理者は、MDMプロファイルを要求する前にユーザーIDについて必要な認証を実行する必要があります。

iOSの場合、消去済みデバイスの最初のセットアップ時にこのワークフローを実行できます。macOSの場合、Setup Assistantで、あるいはSetup AssistantでDevice Enrollmentをスキップした場合はProfiles設定ペインでもこのワークフローを実行できます。

カスタムWebページ作成に関する開発者向けの情報は、以下のAppleドキュメンテーションをご覧ください:

- Web View
- Web Viewを通じた認証

- Webサイトのデスクトップ版またはモバイル版を表示できる簡単なiPadのWebブラウザを実装するサンプルコード

Device Enrollment認証設定の編集

手順

1. **[管理]** > **[Apple]** > **[Device Enrollment]** を開きます。
2. Appleのサイトで作成したサーバー名を探します。
3. **[アクション]** > **[認証の編集]** を選択します。

モバイルアカウントのBootstrapトークン管理

対象：macOS 10.15およびサポートされる以降のバージョンを搭載し、Apple School ManagerまたはApple Business Managerを使用してMDMにデバイス登録されたデバイス。

Ivanti Neurons for MDM は、モバイルアカウントのBootstrapトークン管理をサポートします。Bootstrapトークンにより、モバイルアカウントがFileVaultを使用するmacOSデバイスにサインインできます。この機能により、ログインするすべてのモバイルアカウントが自動的にSecureTokenを受け取ります。この機能は暗号化されたマシンに複数のユーザーがログインする場合に便利です。

マネージド管理アカウントがデバイスにログインする場合：

- 初回ログイン時にMDMサーバーからBootstrapトークンが要求されます。
- MDMサーバーがBootstrapトークンを提供する場合、デバイスがアカウントのSecureTokenを自動的に作成します。
- デバイスがユーザーのFileVaultを有効化します。

[Bootstrapトークン利用可] は、デバイス詳細ページのフィールドであり、新しいデバイスグループやカスタムポリシーを作成する際のフィルター属性でもあります。

トラブルシューティングや検証の場合はデバイスのデバイス詳細ページを開いてください。[Bootstrapトークンを取得]、[Bootstrapトークンを設定] のアクション名を使用したフィルターでデバイスログを絞り込みます。

Device Enrollmentを使用したマネージドmacOS管理者アカウントの設定

Ivanti Neurons for MDM は、工場出荷時の状態にリセットしたデバイスや初めて起動したデバイスでのDevice Enrollment登録をサポートしています。Device Enrollmentの使用により、macOSデバイス上で管理者アカウントを作成できます。Ivanti Neurons for MDMIvanti Neurons for MDM Ivanti Neurons for MDM は、macOSの任意登録しかサポートしないため、iOSデバイスにのみ適用されるDevice Enrollmentプロファイルの [MDM必須要件] フィールドを無視します。

手順

1. **[管理] > [Apple] > [Device Enrollment]** を開きます。
2. Appleのサイトで作成したサーバー名を探します。
3. **[アクション] > [Device Enrollmentプロファイルを編集]** を開きます。
4. macOSアカウント設定アシスタントオプションから次のいずれかを選択します。
   - **管理者アカウント作成をスキップ** - 表示でも非表示でも、管理者アカウントの作成を禁止するには、このオプションを選択します。**[マネージドmacOS管理者アカウントを設定]** セクション(以下に説明) で管理者アカウントの作成を許可するには、このオプションの選択を解除します。
   - **プライマリ設定アカウント作成をスキップ** - macOSデバイスでプライマリアカウントの設定をスキップするには、このオプションを選択します。管理者アカウントのほかのユーザーアカウントは作成されません。マネージドmacOS管理者アカウントを作成するには、別のセクション **[マネージドmacOS管理者アカウントを設定]** が表示されます(以下に説明) 。このアカウントはユーザー& グループに対して非表示にすることも可能です。
   - **プライマリアカウントをレギュラーユーザーとして作成 (チェックがなければ管理者として)** - 登録の一環として非管理者の標準アカウントを作成するには、このオプションを選択します。それでも管理者が管理者アカウントを作成し、デバイスにプッシュすることは可能です。マネージドmacOS管理者アカウントを作成するには、別のセクション **[マネージドmacOS管理者アカウントを設定]** が表示されます(以下に説明) 。このアカウントはユーザー& グループに対して非表示にすることも可能です。
5. マネージドmacOS管理者アカウントを作成するには、上のいずれかを選択した後、以下の情報を **[マネージドmacOS管理者アカウントを設定]** セクションに入力してください。
   - フルネーム
   - アカウント名
   - パスワード

- パスワードの確認
- (任意)ユーザー& グループのマネージド管理者アカウントを非表示

6. **[プライマリ設定アカウント作成をスキップ]** を選択しない場合、次の情報を **[プライマリアカウントを設定]** セクションに入力します。これにより、マネージドローカルユーザーの短縮名が管理者の短縮名に設定され、マネージド管理者アカウントのユーザーチャネルサポートが追加されます。
   - **フルネーム**
   - **短縮名**
   - (任意) **エンドユーザーによる変更を防止** - この設定は「フルネーム」や「短縮名」に代替変数があり、空と評価されている場合にはオーバーライドされます。これを選択した場合、以下のいずれかのオプションが適切に設定されている場合に限り、このプライマリ管理者アカウント設定が適用されると理解したことを確認してください。
     a. 認証設定画面で[ユーザー登録/ログインを指示]が選択されている。
     b. MobileIronがホストするWebページが登録のカスタマイズに選択されている。
7. マネージド管理者アカウントのユーザーチャネルサポートを有効化するには **[プライマリ設定アカウント作成をスキップ]** を選択します。管理者の短縮名にはマネージドローカルユーザーの短縮名を設定します。
8. **[保存]** をクリックします。

ローカルのmacOS管理者アカウントパスワードの変更

管理者は、Device Enrollment中にセットアップアシスタントが作成したローカルのmacOS管理者アカウントのローカルパスワードを変更できます。

対象: macOS 10.11またはサポートされる以降のバージョン。

手順

1. **[デバイス]** を開きます。
2. デバイスが関連付けられているユーザー名をクリックしてデバイス詳細ページを開きます。
3. [アクション] メニューで **[[macOS管理者パスワードを設定]** をクリックします。これは[デバイスリスト]ページで1つ以上のデバイスを選択しても実行できます。
4. パスワードを入力します。
5. **[保存]** をクリックします。

CSVにエクスポート

Ivanti Neurons for MDM デバイス登 録 済 みのデバイスをCSVファイルにエクスポートできます。

手 順

1. **[管 理]** > **[Apple]** > **[デバイス登 録]** を開きます。
2. **[デバイス数]** 列 の下 の、特 定 のデバイス数 リンクをクリックします。
3. **[CSVにエクスポート]** オプションをクリックして、デバイスリストと関 連 詳 細 をCSVファイルにエクスポートします。レポートの準 備 が完 了 すると、レポートをダウンロードまたは削 除 するよう促 すメッセージが表 示 されます。レポートをダウンロードするためのリンクが記 載 された電 子 メールも送 信 されます。
4. **[ダウンロード]** をクリックします。
5. (任 意) レポートを削 除 するには **[削 除]** をクリックします。

セットアップ アシスタントの構成

構成セットアップ アシスタントでは、iOS および macOS デバイスのデバイス設定中にスキップまたは追加するセットアップ画面を選択できます。

手順

1. Ivanti Neurons for MDM 管理コンソールにログインします。
2. **[構成]** に進みます。
3. **[セットアップ アシスタント]** を選択します。
4. 鉛筆 (編集) アイコンをクリックします。
5. デバイスから特定のセットアップ画面をスキップするには、チェックボックスをオンにします。
6. **[完了]** をクリックします。
7. **[デバイス チャネル]** を選択します。
8. **[すべてのデバイス]** を選択します。セットアップ アシスタント構成はデバイスにプッシュされ、[デバイス詳細] ページの [構成] タブには [インストール済み] 状態が表示されます。
9. デバイスにログインします。すべての初期セットアップ画面がスキップされます。

MDM証明書のインストール

iOSデバイスを管理するにはApple MDM証明書を要求し、インストールする必要があります。また、この証明書は年に1回の更新が必要です。(有効期限が近づくと、Appleサイトからの通知が証明書を作成する際に使用されたAppleアカウントに送信されます。)[MDM証明書]ページを使用して、この証明書を追加または更新してください。

MDM証明書の取得とインストール

手順

1. **[MDM証明書]**ページを使用して、Ivanti Neurons for MDMテナントから証明書署名要求(CSR)をダウンロードします。
2. CSRをAppleにアップロードし、新しい証明書を作成します。

   Appleサイトに証明書の用途に関するメモを追加します。このメモは、証明書の更新時に役立ちます。
3. 完成した証明書を保存します。
4. Ivanti Neurons for MDMテナントの証明書をインストールします。

MDM証明書の更新

手順

1. **[証明書を更新]**をクリックします。
2. Ivanti Neurons for MDMテナントから証明書署名要求(CSR)をダウンロードします。
3. CSRをAppleにアップロードし、対応の証明書を更新します。

   Appleサイトで、正しい証明書を更新することを確認します。Ivanti Neurons for MDMへ別の証明書をアップロードすると、登録されているすべてのiOSデバイスが自動的に撤去されます。
4. Ivanti Neurons for MDMテナントの証明書をインストールします。

   誤った証明書をアップロードしようとすると、警告が表示されます。

[MDM証明書のインストール]ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管 理
- 読 み取 り専 用 システム

業務用共有 iPad デバイス

業務用の共有 iPad デバイスは、iOS 13.4以降のサポートされているバージョンが搭載されている場合に、Apple Business Manager で作成された管理対象 Apple ID で使用できます。

- 共有 iPad デバイスでは、パーソナライズされた経験を維持しながら、複数の従業員間でデバイスを共有させることができます。
- 従業員は管理対象 Apple ID でログインし、電子メールアカウント、ファイル、iCloud Photo Library、アプリケーション データなどのデータの読み込みを開始できます。
- このデータは iCloud に保存されるため、従業員は組織に属する任意の共有 iPad デバイスにサインインできます。

共有 iPad デバイスは医療、小売、産業アプリケーションで使用できます。たとえば、医師や看護師は、自分に固有のユーザプロファイルに安全にアクセスできるため、1台の iPad デバイスを共有できます。小売店では、現場の販売担当者が製品情報、資料、専門知識にアクセスすることで、お客様を満足させ、スムーズに買い物をしていただくことができます。

機能の詳細

- iPad デバイスが Apple Business Manager に追加され、共有モードがオンになっている自動登録プロファイルを使用して登録されます。
- 従業員は、会社が提供した管理対象 Apple ID およびパスワードを使用して、共有 iPad デバイスにサインインします。Apple Business Manager 管理者は手動でアカウントを作成するか、Azure Active Directory などの ID プロバイダとフェデレーションしてアカウントを作成することができます。
- 各ユーザは、共有 iPad デバイスにログインしたときにカスタム プロファイルを使用できます。管理者は、ユーザの役割、責任、部署に基づいて、アプリケーションを配布できます。
- ユーザは共有 iPad デバイスにゲスト ユーザとしてログインできます。既定では、ゲスト ユーザのログインが有効です。ゲスト ユーザは管理対象の Apple ID とパスワードでサインインする必要がありません。ゲスト ユーザのログインを無効にするには、iOS 制限構成で **[共有 iPad でゲスト セッションを許可]** オプションを **False** に設定します。
- [Ivanti Neurons for MDM] > **[デバイス]** に移動し、共有 iPad デバイス名をクリックして、**[ユーザ]** タブをクリックします。デバイスと詳細情報 (管理対象 Apple ID、使用可能なデータ (バイト)、使用済みデータ (バイト)、データが Ivanti Neurons for MDM に同期されているかどうか) に関するユーザの一覧が表示されます。

- **[ログ]** タブに移動し、フィルタから **[ユーザ リストの報告]** アクションを選択すると、ユーザ詳細情報が表示されます。
- 共有 iPad デバイスでのゲスト ユーザのログインは、Ivanti Neurons for MDM によるゲスト ユーザの管理とは異なります。Ivanti Neurons for MDMではゲストユーザーアカウントがデフォルトで無効化されています。共有 iPad デバイスでゲスト ユーザを管理するには、ゲスト ユーザ アカウントを有効にします。
- 画面の記録は共有 iPad デバイスのコントロール センターから入手できます。
- Ivanti Neurons for MDM は管理対象AppleIDの代替変数(`${managedAppleID}`)をサポートします。このシステム変数はシステム属性セクションとデバイス属性セクションに表示されます。
- Ivanti Neurons for MDM では、現在ログインしているユーザと過去に共有 iPad デバイスにログインした常駐ユーザの管理対象 Apple ID が、管理者によって変更されないように制限されています。管理対象 Apple ID を変更しようとすると、ユーザが共有 iPad デバイスを使用しているためユーザの管理対象 Apple ID を変更できないというエラー メッセージが表示されます。
- Apple Apps and Books の場合、Apps and Books はデバイスベースのライセンスが選択されているかどうかに関係なく、デバイスベースのライセンスに基づいてインストールされます。

前提条件

以下の前提条件を満たす必要があります。

- 共有 iPad デバイスで管理対象の Apple ID が必要。管理者は手動でアカウントを作成するか、Azure Active Directory などの ID プロバイダとフェデレーションできます。
- 共有 iPad デバイスには、iOS 13.4以降のサポートされているバージョンが搭載されている必要があります。
- デバイスは Apple Business Manager アカウントに関連付けられる必要があります。
- デバイスには32GB 以上のストレージが必要です。

次の点に注意してください。

- Ivanti Neurons for MDM は、パスコードなどの特定の構成を制限します。Apple などの共有 iPad デバイスではサポートされません。このような構成はデバイスにプッシュされません([デバイス] > デバイス名 リンクをクリック > [構成] タブ) 。
- 共有 iPad デバイスでは、パスコードではなくパスワードに関連付けられた管理対象 Apple ID が必要であるため、パスコード構成は共有 iPad デバイスに適用されません。Ivanti Neurons for MDM 管理ポータルのロック解除アクションでは、共有 iPad デバイスのパスワードが消去されません。
- 共有 iPad デバイスに iOS 制限構成を配布しているときには、デバイスチャネルまたはユーザチャネルを選択します。これはそれぞれに異なる構成を配布し、デバイスチャネルまたはユーザーチャネルのみに制約をかける際に有用です。
- Ivanti Neurons for MDM は有効期限切れのアカウントを検証し、アカウントが有効期限切れのデバイスを所有者として除却します。ただし、共有 iPad デバイスの場合、デバイス所有者が最後のログイン ユーザであり、法的な所有者ではない可能性があります。所有者アカウントが有効期限切れの場合、Ivanti Neurons for MDM では共有 iPad デバイスは除却から除外されます。
- iOS クライアント版 Go は共有 iPad デバイスではサポートされていません。
- ユーザは、共有 iPad デバイスでの除却やワイプなどのアクションを実行できません。管理者のみが Ivanti Neurons for MDM 管理ポータルから除却およびワイプ アクションを実行できます。
- 管理者は、Ivanti Neurons for MDM 管理ポータルから共有 iPad デバイスの所有者を変更することはできません。
- ゼロサインオンは共有 iPad デバイスではサポートされていません。
- `ListUsers` コマンドが有効なときには、すべての管理対象ユーザ ID とチェックイン日時が **[管理]** タブのデバイス登録 (Apple Business Manager の一部) に表示されます。

共有 iPad デバイスの構成

共有 iPad デバイスを設定し、設定を構成できます。

手順

1. **[管理]** > **[Apple]** > **[デバイス登録]** を開きます。
2. 自動Device Enrollmentプロファイルを使用してデバイスを登録し、Apple Business Managerにデバイスを追加します。この手順の詳細はDevice Enrollmentを参照してください。
3. Device Enrollmentの設定で以下を有効化します:
   - **監視モード**。
   - **[業務用共有 iPad デバイス]** の **[マルチユーザモード]**。
4. (任意) ローカルユーザーアカウントを作成します。デバイスがそのユーザーに登録されます。このユーザーとしての認証は登録中の1回だけです。
5. 共有 iPad をリセットします。

   登録プロセスはリセットしなければ開始しません。デバイスが登録され、共有 iPad デバイスとして構成されるまでには数分かかります。
6. 法的所有者はデバイスを登録したユーザーのアカウントに割り当てられています。管理者は **[デバイス]** ページで法的な所有者を変更できます。
7. デバイスのログイン画面で、ユーザの管理対象 Apple ID 認証資格情報を入力します。
   - macOS デバイスのように、デバイスとユーザチャネルの両方を使用して、共有 iPad デバイスで構成をプッシュできます。
   - ユーザ代入変数は、デバイスチャネルでプッシュされた構成 (管理されたアプリケーション構成を含む) には代入されません。
   - 共有 iPad デバイスのログインユーザが管理対象ユーザではない場合、管理対象 Apple ID は Ivanti Neurons for MDM 管理ポータルのどのユーザにも属しません。デバイスは誰にも割り当てられません。ユーザは管理されません。管理者は Ivanti Neurons for MDM からユーザチャネル構成をプッシュできません。
   - Ivanti Neurons for MDMが作成するデフォルトのゲストユーザーはデフォルトで無効化されています。ゲスト ユーザがログインするときには、デバイスがどのユーザにも割り当てられてなく、ユーザは管理されていません。ゲスト ユーザを管理する必要がある場合、Ivanti Neurons for MDM によって作成された既定のゲスト ユーザを有効にする必要があります。ゲスト ユーザがログインした後、デバイスが既定のゲスト ユーザに割り当てられます。ユーザを管理できます。
   - デバイス所有者情報は、[Ivanti Neurons for MDM] > **[デバイス]** ページとデバイスログ ([デバイス詳細] ページ > **[ログ]**) に表示されます。

共有iPadの法的所有者の管理

デバイス一覧ページでは、電子メールIDを使用して、共有 iPad の法的な所有者を検索して表示できます。共有 iPad デバイスの法的な所有者を変更するには、既存の法的な所有者を新しい法的な所有者に再割り当てします。共有されていない iPad デバイスの法的な所有者が再割り当てされる場合は、Ivanti Neurons for MDM はその割り当てを無視します。

手順

1. **[デバイス]** を開きます。
2. 歯車アイコンをクリックして、**[法的な所有者]** 列を選択し、デバイス一覧ページに追加します。
3. 共有 iPad デバイスを選択します。
4. **[アクション]** > **[法的所有者に割り当てる]** をクリックします。

共有 iPad デバイスの法的な所有者に電子メールを送信する

共有 iPad デバイスの法的な所有者に電子メールを送信できます。

手順

1. **[デバイス]** を開きます。
2. 共有 iPad デバイスの名前をクリックします。
3. **[メール]** アイコンをクリックします。
4. メールを作成します。
5. **[送信]** をクリックします。

マルチユーザーモード属性の使用

Ivanti Neurons for MDM では、共有 iPad デバイスの [マルチユーザモード] 属性を使用できます。

手順

1. **[デバイス]** ページで **[マルチユーザモード]** 属性を使用します。
2. **[詳細検索]** をクリックして、**[マルチユーザモード]** 属性を使用してデバイスを検索するルールを作成します。

3. **[デバイス > デバイス グループ]** ページで、**[マルチユーザ モード]** 属性を使用して共有 iPad デバイスの動的デバイス グループを作成します。たとえばこのグループを配布フィルターとして構成を配布することが可能です。
4. **[ポリシー]** ページで、**[マルチユーザ モード]** 属性を使用して共有 iPad デバイスのカスタム ポリシーを作成します。
5. **[アプリケーション > 配布]** の **[フィルタ]** で **[マルチユーザ モード]** 属性を使用し、インストール可能なアプリケーションの数を制限します。

- Ivanti Neurons for MDM はApple School Managerデバイスのマルチユーザーモードをサポートしません。この設定を有効にしてDevice Enrollmentプロファイルを Apple School Managerデバイスにプッシュすることは推奨されません。
- iOS のマルチユーザ セキュア サインイン構成は、共有 iPad デバイスに適用されません。

共有 iPad デバイスからのユーザの削除

共有 iPad デバイスから1つ以上のユーザ アカウントを削除できます。現在ログインしているユーザは、[ユーザ] リストタブで **[アクティブ]** ラベルが表示されます。共有 iPad デバイスで現在ログインしているユーザには、[削除] オプションを適用できません。**[デバイス]** または **[ユーザ]** タブからユーザを削除できます。

デバイス タブからのユーザの削除

手順

1. **[デバイス]** タブ > **[デバイス詳細]** に移動します。
2. **[ユーザ]** タブに移動します。ユーザの一覧が表示されます。
3. **[すべてのユーザを削除]** をクリックします。
4. **-** (マイナス記号) をクリックして、特定のユーザを削除します。
   - (任意) **[ユーザの削除]** ウィンドウで **[Ivanti Neurons for MDM とのデータ同期が保留中の場合にも強制的にユーザを削除]** オプションをクリックし、**[はい]** をクリックします。

     [Ivanti Neurons for MDM とのデータ同期が保留中の場合にも強制的にユーザを削除] を選択すると、データがIvanti Neurons for MDM 管理ポータルと同期されていない場合でも、ユーザを強制的に削除します。

ユーザ タブからのユーザの削除

手順

1. **[ユーザ]** タブに移動します。
2. ユーザまたは複数のユーザを選択し、**[アクション]** ドロップダウンメニューで **[削除]** をクリックします。確認メッセージが表示されます。確認した後に、[ユーザの削除] コマンドがデバイスに対して発行されます。
3. デバイス詳細で **[デバイス ログ]** に移動し、[ユーザの削除] コマンドが共有 iPad デバイスの選択したユーザに送信されたことを確認します。

共有 iPad デバイスからユーザをログアウトさせる

管理者は、共有iPadデバイスからユーザーをログアウトできます。

手順

1. **[デバイス]** ページで共有 iPad デバイスを選択します。
2. **[アクション]** メニューから **[強制ログアウト]** を選択します。共有iPadデバイスからのユーザーログアウトに対して、確認のポップアップが表示されます。
3. **[OK]** をクリックして強制ログアウトを承認します。

School Manager

ライセンス：Gold

対象：監視対象のiOS 9.3+

Apple School Managerは、教育機関専用のAppleのクラウドサービスであり、Appleの「Apps and Books」を通じたアプリの購入、Apple Device EnrollmentによるiPadの登録、マネージドApple IDの作成などのサービスを提供します。Apple School Managerとの完全な統合により、Ivanti Neurons for MDM UEMソリューションは、教師や生徒に割り当てられたiPadの完全な管理を容易にし、School ManagerのエコシステムとClassroomなどのアプリを活用します。

Apple Booksはサポートされません。

School Managerの構成

1. **[管理] > [School Manager]** を開きます。
2. **[Educationの設定]** オプションがオフになっている場合はクリックします。
3. 以下のオプションから1つ選択してください：

- **Apple School Managerアカウントと同期し、学校情報をインポートしてください。**

  a. **[管理] > [Apple] > [Device Enrollment]** を開き、組織のキーファイルをダウンロードします。

  b. キーファイルをApple School Managerアカウントにアップロードし、暗号化キーを生成します。

  Apple School Managerから暗号化キーをダウンロードし、Ivanti Neurons for MDM にキーをアップロードします(**[管理] > [Apple] > [Device Enrollment]**) 。

  > Apple Educationには既存のApple Device Enrollmentアカウントを再利用できます。Apple School Managerにアクセスすると、Education機能を含むDevice EnrollmentアカウントにアップグレードするオプションをAppleが提示します。アップグレード方法は、https://support.apple.com/en-in/HT206960をご覧ください。

  c. 暗号キーの承認後、**[今すぐ同期]** ボタンが表示されます。

  d. Apple School Managerとデータ同期を開始するには **[今すぐ同期]** をクリックします。

- **CSVファイルからデータをインポートしてください。**

  a. (任意) **[CSVテンプレートのZIPファイルをダウンロード]** をクリックし、全データタイプのテンプレートを含むzipファイルをダウンロードします。

  b. **[ファイルを選択...]** をクリックします。

  c. 以下の6つのCSVファイルを追加します。

  - 学生データファイル(students.csv)
  - 登録者データファイル(roster.csv)
  - スタッフデータファイル(staff.csv)
  - クラスデータファイル(classes.csv)
  - コースデータファイル(courses.csv)
  - 場所データファイル(locations.csv)

  > アップロードする前に、毎回6つすべてのCSVファイルを一緒に選択する必要があります。

  d. **[アップロード]** をクリックします。

  e. (任意) CSVファイルを変更する必要がある場合は、前にアップロードした6つのファイルの必要データすべてを保存してください。必要な編集を行った後、再び全部一緒にアップロードします。

4. **[クラス]** と **[個人]** タブからデータを検索します。

> 個人 (学生と職員) も Ivanti Neurons for MDM の **[ユーザ]** ページに表示されます。

5. 次のように、学生と職員が教育目的で使用するデバイスで2つのデバイスグループを作成します。

   a. **[管理]** > **[カスタム属性]** を開きます。

   b. 学生とスタッフのカスタム属性を作成します。これらは動的に管理されるデバイスグループの作成に使用します。

   c. **[デバイス]** > **[デバイスグループ]** に進みます。

   d. **[追加 +]** をクリックします。

   e. 前にフィルターとして作成したカスタム属性を使用し、学生用とスタッフ用に1つずつ、動的に管理されるデバイスグループを作成します。

6. **[デバイス]** ページから **[アクション]** > **[ユーザーに割り当てる]** オプションを使用し、登録済みデバイスを学生とスタッフに割り当てます。

7. **[構成]** > **[Education]** ペイロードを追加することにより、リーダー(スタッフ)構成とメンバー(学生)構成を作成します。

8. リーダー(スタッフ)構成とメンバー(学生)構成をスタッフと学生のデバイスグループに配布します。
   この配布によって構成がプッシュされ、各デバイスに証明書がインストールされます。

[管理] > **[School Manager]** ページでクラス名として値が表示されない場合、クラスシステムソース識別子およびコース識別子フィールドから値が作成されます。これらのフィールドはApple School ManagerまたはCSVファイルでは任意です。しかし、クラス名がない場合、これらの組み合わせがデフォルトの識別子として使用されるため、常に値を入力することをお勧めします。

教師へのClassroomアプリのプッシュ

Classroomアプリでは、教師(リーダー)が以下のシナリオを管理できます。

- iPadとアプリをリモートで制御するClassroom管理
- クラスグループの作成
- 教師による対象グループの学生メンバーの閲覧
- 教師による対象グループの学生へのコンテンツ送信
- 学生が閲覧できるアプリやコンテンツの制限

Apple App Store から Classroom アプリケーションをプッシュできます。

手順

1. **[アプリ] > [アプリカタログ]** ページを開きます。
2. **[+追加]** ボタンをクリックします。
3. AppleのClassroomアプリを検索し、選択します。
4. **[次へ]** をクリックします。
5. カテゴリと説明を入力します。
6. **[次へ]** をクリックします。
7. 前に作成した教師デバイスグループにアプリを配布します。
8. [アプリ構成] ページでアプリを設定します。
9. **[完了]** をクリックします。

School Managerの無効化

School Managerを無効化すると、現行のデータがすべてワイプされます。無効化する際は注意してください。

1. **[管理] > [School Manager]** を開きます。
2. **[Education設定]** オプションがオンになっている場合はクリックします。
3. **[はい]** をクリックします。

設定(Apple)

管理者は、Appleデバイスのさまざまな設定を構成、有効化、無効化できます。

サイレント登録(macOSのみ)

macOSデバイスのサイレント登録は「有効」にロックされています。これは、テナント内のすべての新規デバイス登録を対象とし、Mobile@Work 1.4またはサポートされる以降のバージョンで使用できます。

プロファイル設定

管理者は、MDMプロファイルがインストールされていない場合、エンドユーザーへのメール送信、macOSおよびGo for iOSクライアントへの通知の送信を有効化または無効化することができます。MDMプロファイル通知機能はデフォルトで有効になっています。

手順

1. **[管理] > [設定]** を開きます。
2. **[MDMプロファイルがインストールされていない場合、ユーザーにメールを送信し、クライアントに通知を送信する]** オプションを選択または選択解除します。
3. メール/通知の最大回数を1～4の間で選択します。
4. **[保存]** をクリックします。

自動デバイス登録(iOSのみ)のOS更新

管理者は、自動デバイス登録についてiOSオペレーティングシステム更新をオンにすることができます。このオプションが有効化されている場合、Device Enrollmentデバイスは、Device EnrollmentプロファイルのOS更新のスケジュール設定ではなくソフトウェア更新の構成を使用します。

デフォルトではこのオプションがオフになっており、Device EnrollmentプロファイルのOS更新のスケジュール設定が使用されます。この設定をいったんオンにするとオフにはできません。この設定は、すべてのDevice Enrollmentプロファイルの OS更新のスケジュール設定を削除します。

監視対象の非Device Enrollmentデバイスはソフトウェア更新設定を使用します。

手順

1. **[管理] > [設定]** を開きます。
2. **[自動Device Enrollmentにソフトウェア更新構成を使用]** オプションを選択または選択解除します。
3. **[はい]** をクリックして確定します。
4. **[保存]** をクリックします。

マルチユーザーセキュアサインイン

管理者は、ユーザーがiOS共有デバイスでマルチユーザーセキュアサインのWebクリップからログアウトしたときにデバイスパスコードをクリアできます。これには [管理] > [Apple] > [設定] の「**マルチユーザーセキュアサインイン**」セクションにある「**ユーザーのログアウト後にパスコードをクリア**」オプションを選択します。

制約構成の優先度設定

管理者は、**[管理] > [Apple] > [設定]** の **[制約構成の優先度設定]** セクションから **[iOS制約構成]** または **[macOS制約構成]**オプションを選択することにより、複数のiOS/macOS制約構成の優先度を有効にできます。このオプションはデフォルトでは無効化されています。優先度の仕組みについては、「構成の優先度決定」ページ452を参照してください。

手順

1. **[管理] > [Apple] > [設定]** を開きます。
2. **[制約構成の優先度設定]** セクションで **[iOS制約構成]** または **[macOS制約構成]** オプションを選択します。

3. **[保存]** をクリックして優先度を有効化します。「**制約構成の優先度設定(iOSまたはmacOS)が有効です**」バナーが表示されます。優先度が **[承認]** される前の状態:

   - **配布の概要を編集(あれば)**:優先度設定を有効化すると、選択した制約構成の配布の概要が「**他のスペースにあるデバイスに適用**」から「**最高優先度で他のデバイススペースにあるすべてのデバイスに適用**」にデフォルトで変更されます。
   - **作成順にデフォルトの優先度を指定**:選択した制約タイプの構成には、作成順にデフォルトの優先度が指定されます。
   - **構成の管理の一時停止**:選択した制約構成(たとえばiOS制約構成)の管理は優先度の承認まで一時停止されます。

   > 優先度を有効化した後、制約への変更は承認されるまで処理されません。管理者は、承認の前に **[構成]** セクションから制約構成の配布、配布の概要、優先度を編集できます。

4. 優先度を有効にするには **[承認]** オプションを選択します。
5. **[保存]** をクリックします。

   > iOS制約構成オプションの選択を解除するときは**承認**オプションが表示されません。変更は即座に適用されます。

優先度が無効の場合、構成に優先度はありません。すべての制約構成は対象となるデバイスにプッシュされます(次のデバイス同期で)。

- **配布の概要(あれば)**:制約構成の優先度設定が無効の場合、配布の概要は「**最高優先度で他のデバイススペースにあるすべてのデバイスに適用**」または「**最低優先度で他のデバイススペースにあるすべてのデバイスに適用**」から「**他のスペースにあるデバイスに適用**」に変更されます。
- **優先度の指定なし**:選択した制約構成から優先度が削除されます。

Windowsデバイスでの作 業

このセクションは以 下 のトピックを含 みます。

Windows Autopilotプロファイルの構成

Windows Autopilotは、管理者が新しいデバイスを仕事で使えるようにするためのセットアップや事前設定に役立つMicrosoftの機能です。Autopilot機能は、WindowsデスクトップまたはHoloLens2デバイスの迅速で信頼性の高い、シームレスなプロビジョニングを支援します。さらにAutopilot機能は、以下のタスクの実行にも役立ちます。

- Azure Active Directory(AAD) へのデバイスの自動追加
- MDMサービスへのデバイスの自動登録
- デバイスの作成と、デバイスのプロファイルに基づく構成グループへの自動割り当て
- 登録体験のカスタマイズ
- 構成とポリシーの適用
- 必要なアプリケーションのインストール

前提条件

管理者は、Ivanti Neurons for MDM 管理者ポータルのWindows Autopilotページからユーザープロファイルを作成できます。Autopilot機能が期待どおりに機能するには、以下の前提条件を満たす必要があります。

- Autopilot機能(feature.autopilot) が有効化されていること
- Ivanti Neurons for MDM テナントがAAD テナントと統合される
- ダミーユーザfooUser@<aad-domain> が作成され、同期されます

Autopilot登録モード

デバイスを特定のユーザープロファイルグループに関連付けた後、デバイスの使用状況に基づいて、ユーザーがデバイスをすぐに使い始められるように、Autopilot登録モードを設定することができます。Ivanti Neurons for MDM では、以下のAutopilot登録モードが提供されています。

- 自己導入モード
- ユーザ主導 (プリプロビジョニング モード)
- ユーザ主導

自己導入Autopilotモード - 自己導入Autopilotデバイス登録モードでは、デバイスの初期設定を回避し、デバイスが安全に起動するために必要なすべての設定ファイルをプッシュすることで、ユーザー向けに企業のデバイスをシームレスに導入することができます。このモードでは、ハードウェアを保護し、デバイスを企業ネットワークに接続した後、ダミーユーザーIDを使用してAzure Active Directory(AAD) 、MDMサービス、Ivanti Neurons for MDM管理者ポータルにデバイスを登録し、ユーザーがログインする前に必要なすべての設定ファイルをデバイスにプッシュします。必須の設定ファイルがデバイスにプッシュされると、デバイスが再起動し、企業ユーザーが開始できるようにログイン画面が表示されます。キオスクやデジタル署名付きデバイスとして使用できるデバイスには、自己導入モードを使用できます。

ユーザー主導の事前プロビジョニングプロファイルモード – 管理者がユーザー主導の事前プロビジョニングプロファイルを作成し、そのプロファイルをユーザーグループに割り当てると、デバイスのハードウェアIDがアップロードされ、AADグループに割り当てられます。デバイスは、ユーザー主導の事前プロビジョニングプロファイルに関連付けられます。このモードの目的は、管理者がデバイスを企業ユーザーに渡す前にセットアップすることです。手順は以下のとおりです。

手順

1. 新しいハードウェアデバイスをLANに接続し、Windowsボタンを5回押します。
2. デバイスが質問を表示します。[Windows Autopilotプロビジョニング] オプションを選択し、[続行] をクリックします。Intuneがユーザー主導の事前プロビジョニングプロファイルモードを検出し、すべての基本的な構成設定がデバイスに導入されます。Windows Autopilot構成画面が表示されます。
3. [続行] をクリックします。デバイスは処理を進め、ハードウェアを保護し、企業ネットワークに接続した後、ダミーユーザーIDを使用してAzure Active Directory(AAD) 、MDMサービス、Ivanti Neurons for MDM管理者ポータルにデバイスを登録します。必要なすべての構成ファイルがデバイスにプッシュされ、確認メッセージが表示されます。
4. これで、デバイスをユーザーに渡せます。ユーザーがデバイスにログインすると、ユーザーIDがデバイスの詳細とともにIvanti Neurons for MDM管理者ポータルに登録されます。

ユーザーがデバイスにログインする前に、以下の構成が自動的にプッシュされます。

- ID証明書
- Wi-Fi
- Windows Hello for Business
- Windowsの制約

残りの構成は [保留中] 状態であり、ユーザーがメールアドレスを使用してデバイスにログインした後、プッシュされます。

自己配布モードおよびユーザー主導(事前プロビジョニング)モードのAutopilot登録処理中には、割り当てられた.MSIアプリおよび.EXEアプリがデバイスにインストールされ、登録処理が完了します。Autopilot登録処理中に.MSIアプリおよび.EXEアプリをインストールし、インストール中にアプリがレポートするかレポートできない場合、Autopilot処理は完了し、[再封鎖]ボタンが有効になります。

Windows Autopilotユーザープロファイルの作成

Azure Active Directory(AAD)ユーザーソースを設定し、ユーザーとAADユーザーグループをIvanti Neurons for MDMテナントと同期させた後、Autopilotプロファイルを作成します。

手順

1. Ivanti Neurons for MDM管理者ポータルにログインします。
2. **[管理]** > **[Microsoft Azure]** > **[Windows デバイス管理]**をクリックします。

   AADユーザーソースが構成されていない場合、**[追加]**ボタンは無効となります。**[Microsoft Azure]**セクションに表示される**[Windows デバイス管理]**オプションを使用してユーザーソースを構成する必要があります。

3. **[追加]**をクリックします。

   [Windows Autopilotプロファイルを追加]ページが画面に表示されます。

4. **[名前]**ボックスにプロファイル名を入力します。
5. この手順の下のテーブルを使用して**[プロファイル設定]**を完成させます。
6. **[次へ]**をクリックします。

   すべてのAADデバイスグループが入った新しいページが画面に表示されます。

7. Autopilotプロファイルを割り当てるAADデバイスグループを1つ以上選択します。

   AADデバイスグループを作成し、この新たに作成したグループにAutopilotプロファイルを割り当てることもできます。詳細は、「「AADデバイスグループの作成」ページ1206」をご参照ください。

8. Autopilotプロファイルをすべてのグループに割り当てる場合は、**[すべてのAADグループに割り当てる]** オプションを選択します。

> Microsoftからの制約により、「すべてのグループ」に複数のプロファイルを割り当てることはできません。

9. **[完了]** をクリックします。

設定	説明
デバイスの種類	デバイスに応じて以下の2つのオプションから1つを選択します。 • **Windows PC** • **HoloLens** - このオプションを選択する場合は、デフォルトの導入モードを **[自己導入]** モードに設定しておく必要があります。 まれに、Autopilotを使用してHoloLens 2デバイスを登録すると、「仕事用のデバイスのセットアップ」画面で登録が止まることがあります。そのような場合は、電源ボタンを押してデバイスの電源を一旦オフにし、再度オンにします。するとデバイスにログイン画面が表示されるため、ここでAAD認証情報を入力して登録を完了させます。
導入モード	• **自己導入**：このモードでは、ほとんどまたはまったく手動の作業なしにデバイスの導入が行われます。 • **ユーザー主導**：管理者はこのオプションを使用して、ユーザーにデバイスを渡す前に、ユーザー向けに新しいデバイスを構成する登録モードを選択できます。
ユーザーアカウントのタイプ	• **管理者**：デバイスの導入後、ユーザーが完全に制御する必要がある場合は、このオプションを選択します。 • **標準**：デバイスの導入後、ユーザーが基本的なオプションに対する権限を必要とする場合は、このオプションを選択します。
言語	デフォルトでは、言語はオペレーティングシステムによって決まります。リストから別の言語を選択できます。
すべての対象デバイスをAutopilotに変換	割り当てられたグループ内のすべてのデバイスをAutopilotに変換する場合は、このオプションを選択します。

設定	説明
事前プロビジョニングを許可	通常の登録プロセスを使用してAutopilotのデバイスを登録するには、このオプションを選択します。**[自己導入]** オプションが選択されている場合は、このオプションは利用できません。
キーボードの自動構成	**[言語]** オプションがデフォルト値以外の値に設定されている場合、**[はい]** を選択するとキーボード選択がスキップされます。
デバイス名テンプレート	デバイス登録処理中に使用するテンプレート名を入力します。
Microsoft Software ライセンス期間	このオプションは、[ユーザー主導の導入] モードでのみ、表示/非表示を切り替えることができます。
プライバシー設定	このオプションは、[ユーザー主導の導入] モードでのみ、表示/非表示を切り替えることができます。
アカウントオプションの変更	このオプションは、[ユーザー主導の導入] モードで、ユーザーアカウントタイプが [標準] タイプの場合にのみ、表示/非表示を切り替えることができます。

Windows デバイス管理

管理者は、新規オプションである [Windows デバイス管理] を使用して、テナントにAutopilot機能を構成できます。このオプションにより、ユーザが AAD 環境を使用している場合に、Ivanti Neurons for MDM との統合が容易になります。

このオプションを表示するには、**[管理]** > **[Microsoft Azure]** > **[Windows デバイス管理]** をクリックします。

この統合により、Ivanti Neurons for MDM にアクセス権が付与され、Autopilot プロファイルの管理、Windows デバイス準拠の確認、Azure テナントの検証が可能になります。

関連トピック

- TenantLockdown CSP

AADデバイスグループの作成

管理者は、必要に応じていつでも [AADデバイスグループ] セクションからAADデバイスグループを作成できます。AADデバイスグループを作成するには、[デバイスのコンプライアンス] セクションでAADテナント検証が構成されている必要があります。

手順

1. **[管理]** > **[Microsoft Azure]** > **[AADデバイスグループ]** を開きます。

   [Azure Active Directoryデバイスグループ] ページが画面に表示されます。

2. **[追加]** をクリックします。

   [グループ設定] ページが画面に表示されます。

3. 以下の詳細を入力します。

   - グループ名
   - グループの記述
   - メンバーシップタイプ
     - 静的デバイス - 管理者には、利用可能な静的デバイスのリストが **[グループへのメンバーの割り当て]** ウィンドウに示されます。必要なデバイスを選択し、**[保存]** をクリックします。
     - 動的デバイス - 管理者は **[動的クエリ]** ウィンドウから特定の基準を入力する必要があります。

新しいAADデバイスグループが作成され、管理者は、この新たに作成されたグループにデバイスを追加できます。

動的グループを作成後、しばらくすると、特定のデバイスグループの [デバイス] タブにデバイスがリストされます。

Autopilotデバイスの編集

ユーザーは、AutopilotデバイスをIvanti Neurons for MDM管理ポータルから編集できます。

前提条件

以下の前提条件を満たす必要があります。

- ユーザーが割り当てられたMicrosoft Intuneライセンスを持っていること
- ユーザーが設定されている場合のみユーザーに分かりやすい名前を設定できます
- デバイスの名前は、一度設定した後は設定解除できません

手順

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[管理]** > **[Windows]** > **[Autopilot]** を開きます。Autopilotデバイスが、[Autopilot デバイス] タブにリスト表示されます。
3. **[編集]**(鉛筆のアイコン) をクリックします。編集ページが表示されます。
4. 以下の情報を編集します。
   - **ユーザー**
   - **ユーザーに分かりやすい名前**
   - **デバイス名**
   - **グループタグ**
5. **[保存]** をクリックします。デバイスの詳細が更新されます。

Autopilotデバイスの削除

ユーザーは、Ivanti Neurons for MDM 管理ポータルからAutopilotデバイスを削除できます。

1. Ivanti Neurons for MDM 管理者ポータルにログインします。
2. **[管理]** > **[Windows]** > **[Autopilot]** を開きます。Autopilotデバイスが、[Autopilot デバイス] タブにリスト表示されます。
3. **[削除]** をクリックします。デバイスの詳細が削除されます。

Windows Autopilot プロファイルの監査証跡

監査証跡は、Ivanti Neurons for MDM 内のすべてのエンティティで実行されたアクティビティをすべて追跡します。これらのアクティビティには、新しいデバイスの追加、デバイスの削除、更新などがあります。

詳細については、監査証跡をご参照ください。

管理者は、Autopliot モードで登録されたすべての Windows デバイスを使用して、次のアクティビティを実行できます。

Autopilotプロファイル

- 作成
- 編集
- 削除
- プロファイルをグループに割り当てる

Autopliot デバイス

- CSVをアップロード
- 編集
- 削除

TenantLockdown CSP

管理者は、TenantLockdown CSP機能を使用して、すべてのWindowsデバイスをテナントにロックすることができます。この機能を使用するには、Autopilotオプションを使用してデバイスを登録する必要があります。この構成は、デバイスレベルで実行できます。

Autopilot自己導入およびユーザードリブンモードでは、管理者はデバイスをテナントに直接ロックすることができます。これは、デバイスが紛失や盗難にあった場合に便利です。この場合は、デバイスをリセットしてもユーザーは強制的にテナントに接続されます。自己導入モードでローカルアカウントの作成はサポートされません。ただし、ユーザー導入モードでのアカウント作成を防止する必要がある場合、管理者は、Autopilotプロファイル構成中の **[アカウントオプションの変更]** 設定で **[非表示]** オプションを有効化する必要があります。

管理者は、Windows制約構成を作成し、**[その他の制約]** の下の **[ユーザーがデバイス設定中にネットワークに接続する必要があります(Autopilotプロファイルが必要)]** オプションを選択することにより、TenantLockdown CSPを有効化できます。

TenantLockdown CSPからデバイスを削除するには、管理者がデバイスをグループから手動で削除するか、制約を変更する必要があります。

ADMX(GPO)ブラウザ

ADMX(GPO)ブラウザでは、テナント上にあるADMXオブジェクトを踏まえて整理されたGPO設定を確認できます。デフォルトのADMXオブジェクトを検索し、閲覧するほか、XMLベースの構造となるカスタムADMXオブジェクトを追加(アップロード)し、GPO設定の表示を定義することも可能です。

カスタムADMXオブジェクトは、以下の手順でアップロードします。

1. **[管理]** > **[ADMX(GPO)ブラウザ]** を選択します。**[ADMX(GPO)ブラウザ]** ページが表示されます。
2. **[付加]** をクリックします。**[カスタマイズしたADMX(GPO)オブジェクトを付加]** ウィンドウが表示されます。
3. **[ファイルを選択]** をクリックし、アップロードするADMXファイルを選択します。
4. **[付加]** をクリックします。アップロードが成功すると確認メッセージが表示されます。

GPO設定の検索

ADMX(GPO)ブラウザでは、GPOを検索したり、左ペインのGPO階層ツリーで関連コンポーネントをクリックして選択したりできます。GPO階層ツリーは、ポリシー設定のパスを表現しています。また、GPO名やADMXファイル名を検索フィールドに入力すれば、特定のGPO設定を検索することも可能です。選択したGPO設定の詳細は右ペインに表示されます。

アプリインベントリ間隔の構成

複数のアプリソースタイプのインベントリには、Windows 10アプリインベントリコレクション間隔を設定できます。間隔は、デバイスからすべてのアプリを収集するようプライバシー構成が設定されている場合に使用します。

1. **[管理] > [アプリインベントリ間隔]** を開きます。
2. 以下のアプリソースタイプについて、ドロップダウンリストからアプリインベントリを収集する間隔(時間単位)を選択します。
   - **非アプリストアインベントリの間隔**
   - **アプリストアインベントリの間隔**
   - **システムインベントリの間隔**
   - **Win32インベントリの間隔**
     Windowsアプリインベントリの収集間隔は、**24**～**48**時間の範囲で指定できます。デフォルト値は**24**時間です。

ハードウェアインベントリ

Windows 10デバイスからのハードウェア情報の収集を有効化します。ハードウェアインベントリの詳細は、Bridgeを使用して取得します。

1. **[管理] > [ハードウェアインベントリ]** を開きます。
2. **[ハードウェアインベントリの収集を有効化]** オプションを有効化します。
3. **[インベントリ間隔]** では、ハードウェアインベントリを収集する頻度を選択します。選択肢は以下のとおりです。
   - **1日に1回**（デフォルト）
   - **1週間に1回**
   - **30日ごと**

ハードウェアインベントリオプションを有効化すると、[デバイス詳細] ページの **[ハードウェア]** タブにデバイスのハードウェアの詳細が表示されます。

Microsoft Azureでの設定

このセクションは以下のトピックを含みます。

- AADとIvanti Neurons for MDMとの同期
- 「Microsoft Azureの使用」ページ1215
- 「Azure Active Directory Windows 10統合エンドポイント管理設定」ページ1220
- 「AAD UEMアプリの指定」ページ1222
- 「Ivanti Neurons for MDMとAzure Active Directoryユーザーソースとの接続」ページ1223
- 「Azureテナント」ページ1226
- 「[管理] > [Microsoft Azure] > [Office 365アプリ保護]」ページ1249

Microsoft Azureの使用

Microsoft Azureを使用してIvanti Neurons for MDMを設定すると、Windows 10を実行するWindowsデスクトップとタブレットを使用するユーザーをシームレスに登録できます。以下の手順に従い、インスタンスの構成と接続を行ってください。

このセクションは以下のトピックを含みます。

- 「AADアカウントの設定」下
- 「Azure ADでのユーザーの作成」下
- 「Windows 10デバイスにおけるAADとUEMの連携」次のページ
- 「Windowsデバイスにおけるマルチユーザーサポート」ページ1217

AADアカウントの設定

Azure ADを設定するには：

1. https://azure.microsoft.com/en-in/pricing/purchase-options/ を開き、Azureアカウントを購入します。
2. 既存のHotmailまたはOutlook.comアカウントを使用するか、新規アカウントを作成し、新規ユーザーとして登録します。
3. いずれかの支払オプションを使用し、検証手順に従って、Azureアカウントを購入します。
4. Ivanti Neurons for MDM テナントを許可リストに追加するように Microsoft に依頼します。
5. ステップ2と同じHotmailまたはOutlook.comアカウントを使用してADD (https://manage.windowsazure.com/) に管理者としてログインします。
6. **[ドメイン]** タブに進みます。

   お使いのアカウントに対し、デフォルトのドメイン、TestMiBGLRoutlook.onmicrosoft.comが作成され、作成したユーザーはこのドメインに属することになります。必要に応じて、カスタムドメインを作成し直すこともできます。

Azure ADでのユーザーの作成

Azure ADでユーザーを作成するには：

1. [Active Directory] > **[デフォルトディレクトリ] > [ユーザー]** を開きます。
2. [ユーザーオプションを追加] を選択し、組織内の [新規ユーザー] を選択します。
3. ユーザー名を入力します。[次へ]**(->)** をクリックします。

   [ユーザープロフィール] ページが表示されます。
4. 姓名や表示名などのユーザー情報を追加します。
5. ドロップダウンメニューを使用し、ユーザーに適切な役割を割り当てます。
6. 仮パスワードを生成します。

   最初のログイン時にユーザーはこのパスワードの変更を求められます。

Windows 10デバイスにおけるAADとUEMの連携

AADをUEMと連携するには:

1. **[管理] > [Microsoft Azure] > [AADを使用したWindows登録およびコンプライアンス] を開きます。**
2. 「Azure Active Directory Windows 10統合エンドポイント管理設定」ページ1220セクションの手順に従って、UEMをセットアップします。
3. 「AAD UEMアプリの指定」ページ1222 設定をAzureポータルで実行します。
4. Ivanti Neurons for MDM管理ポータルでAADアカウントのドメイン名を入力した後、[Azureポータルを連携] をクリックし、チェックボックスを選択します。
5. サインインした後、MobileIron AD Tenant ValidationアプリがIvanti Neurons for MDM UEMアプリのセットアップを確認することを許可する文章に同意します。連携の完了を示すメッセージが表示されます。

Windows 10デバイス対応Microsoft Passport for Work

Microsoft Passport for WorkはWindows Hello for Businessに変更されました。詳細は「Windows Hello for Business構成」ページ711を参照してください。

WindowsデバイスのAAD登録

前提条件

ユーザをIvanti Neurons for MDMで登録する必要があります。

ドメインに接続し、Windows 10 Mobileデバイス上にユーザーを登録します。

1. **[Azure ADに参加]** をクリックします。
2. ユーザー名とパスワードを入力します。
3. **[サインイン]** をクリックします。
4. EULAを承諾します。
5. **[PINを作成]** をクリックします。
   - Microsoft Passport for WorkのPIN複雑性を有効化している場合は、構成されたポリシーに従って複雑なPINを設定するようプロンプトが表示されます。
   - Azure ADがユーザーを認証し、JWT(JSON Webトークン) をデバイスにダウンロードします。
   - これで、デバイスが登録されました。
   - 確認のためにデバイス経由でユーザーに連絡が届きます。
6. PINを入力し、確認します。
7. **[OK]** をクリックします。

Windowsデバイスにおけるマルチユーザーサポート

Ivanti Neurons for MDM は、Windows 10 Azure ADに登録されたデバイスに対してマルチユーザー機能をサポートしています。これには、VPN、Wi-Fi、デフォルトのメールクライアントプロファイルなどのプロファイルや証明書を、デバイスではなく各ユーザーにプッシュする機能が含まれます。ログインしたユーザーに対する自社開発アプリや市販アプリの配布もサポートします。新規Azure ADユーザーがデバイスにログオンするたびに、Ivanti Neurons for MDMは、デバイスだけでなくユーザーも評価します。新規ユーザーの場合、Ivanti Neurons for MDMはそのユーザー用にデバイスを更新します。ユーザーがそのデバイス上の既存ユーザーである場合、前回のログイン以降にデバイスやユーザー設定の変更があり、更新する必要があるかどうかを判断します。

デバイスにログインしているAzure ADユーザーの詳細が、Ivanti Neurons for MDM 管理ポータルに報告されます。ユーザーがデバイスからログアウトし、次のユーザーがログインすると、デバイス詳細ページに2番目のユーザーが表示されます。

UEMでのビジネス向けMicrosoft Storeの設定

ビジネス向けMicrosoft Storeは、Azureの一環としてMicrosoftが提供するポータルです。管理者は、このポータルにログインし、アプリを購入したり、そのアプリをすべてのマネージドデバイスに配布したりできます。以下の手順を行うことで、ビジネス向けMicrosoft Storeを使用してIvanti Neurons for MDMを設定し、Ivanti Neurons for MDM管理ポータルからアプリケーションを管理できます。

ステップ1：Microsoft AzureポータルでのAADアプリケーション登録

1. 最初のブラウザを開き、Microsoft Azureポータル(https://portal.azure.com/) にログインします。
2. 左ペインの **[アプリ登録]** をクリックします。
3. **[+新規アプリケーションの登録]** をクリックします。
4. 以下の情報を入力し、MobileIronをAzureアプリとして登録します。
    1. **名前**：MobileIronアプリの名前を入力します。(このフィールドは4文字以上で必須です。)
    2. **アプリケーションタイプ**：Webアプリ/APIを選択します。
    3. **サインオンURL**：デバイスユーザーがMobileIronにサインインするためのURLを入力します(必須) 。
5. **[作成]** をクリックし、アプリを追加してAzureホームページに戻ります。
6. [設定] を開き、新しいキーを作成します。

ステップ2：管理ツールとしてのアプリケーション追加

1. ビジネス向けMicrosoft Storeの [設定] から [管理] をクリックします。
2. 配布設定
3. [管理ツールを追加] で、作成したアプリケーションを有効化します。

Admin Portalでのアカウント連携

1. **[管理] > [Microsoft Azure] > [ビジネス向けMicrosoft Store]** を開きます。
2. ステップ1の **[AADアプリケーションを登録]** で、**[はい、この手順を完了しました]** のチェックボックスを選択します。
3. ステップ2の **[管理ツールを追加]** で、**[はい、この手順を完了しました]** のチェックボックスを選択します。
4. ステップ3の [アカウントを連携] で以下のフィールドを更新します。
    1. Azure ADドメイン
    2. アプリケーション識別子
    3. アプリケーションキー
    4. 同期間隔(時間)

5. **[連携]** をクリックします。ビジネス向けMobileIronストアが正常に設定されたという確認メッセージが表示されます。

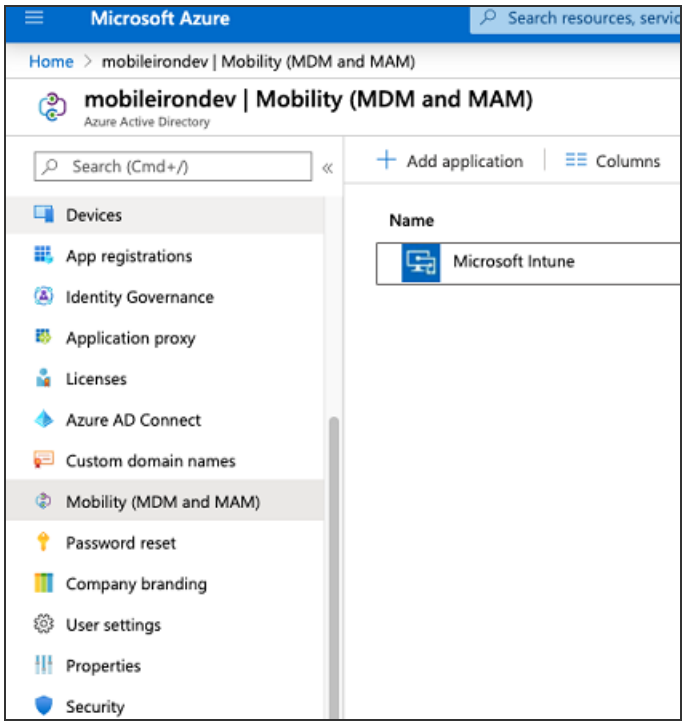
6. **[アプリを同期]** をクリックします。正常に同期されると、**[アプリケーションが正常に同期されました]** というステータスが表示されます。

アプリ用Microsoft Storeがデバイスにプッシュされると、デバイス詳細の **[インストール済みアプリ]** タブにアプリの詳細が表示されます。デバイスから報告されるビジネス向けMicrosoft Storeの各アプリは、**[ソース]** カラムの **[ビジネス向けMicrosoft Store]** で識別できます。

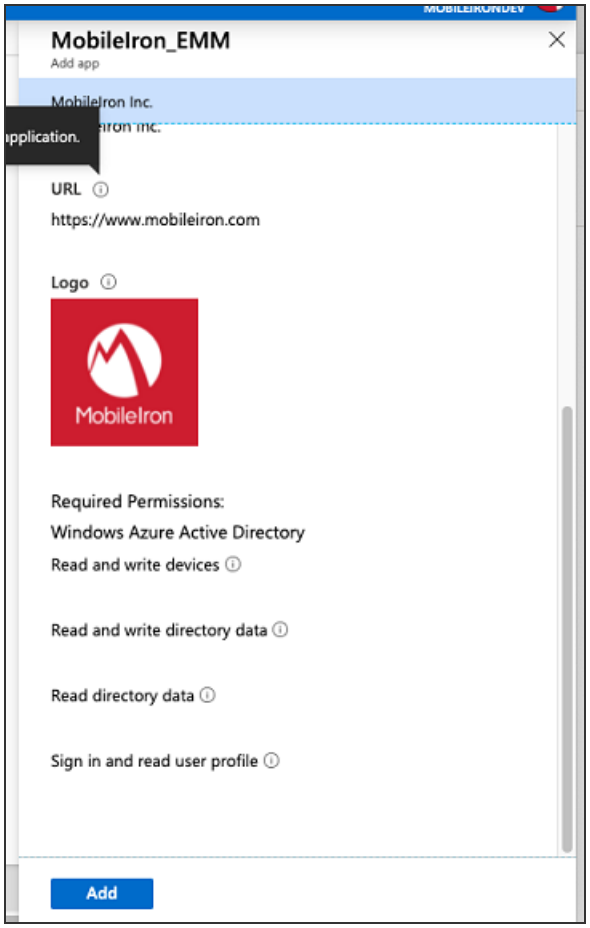
Azure Active Directory Windows 10統合エンドポイント管理設定

Windows 10統合エンドポイント管理(UEM)を設定するには:

1. https://portal.azure.com/から管理者としてログインし、Azure Active Directoryを選択します。
2. 左のパネルで[モビリティ(MDM、MAM)]を選択し、**[+アプリケーションを追加]**をクリックします。



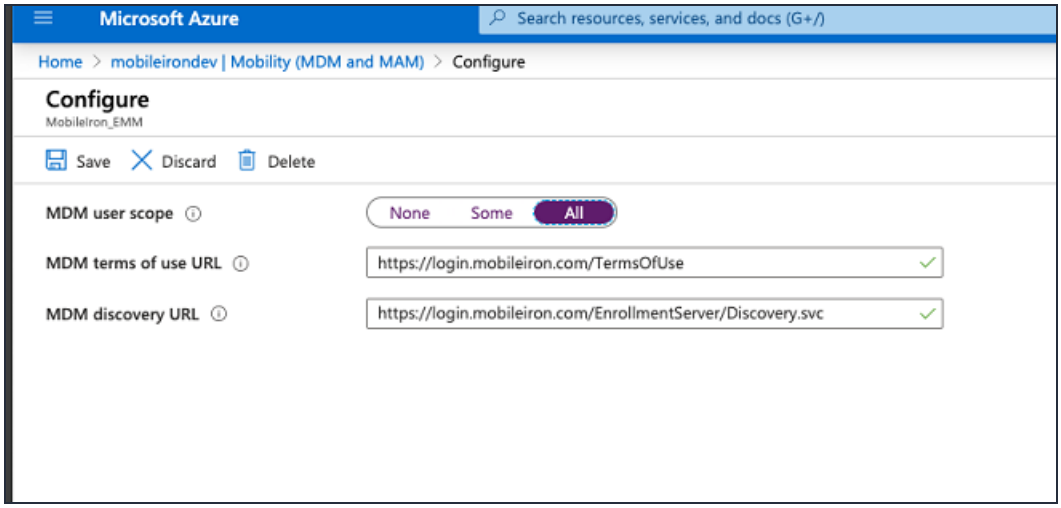
3. アプリギャラリーから [MobileIron_UEM] アプリケーションを選 択し、**[追 加]** をクリックします。



AAD UEMアプリの指定

ユーザー設定の指定を完了するには:

1. 「Azure Active Directory Windows 10統合エンドポイント管理設定」ページ1220の手順2で作成したMobileIron UEM アプリケーションをクリックします。
2. [MDMユーザースコープ] でカスタマイズしたユーザーグループに指定するか、**[すべて]** を選択します。



Ivanti Neurons for MDMとAzure Active Directoryユーザーソースとの接続

Azure Active Directory (AAD) と連携させるには、Microsoft AAD アカウントに関する詳細を使用して Ivanti Neurons for MDM を構成する必要があります。連携には既存の構成済みMicrosoft AADアカウントが必要です。このソリューションにオンプレのConnectorまたはLDAPは不要です。

このセクションは以下のトピックを含みます。

- 「ユースケース」下
- 「Azure Active Directory の使用」次のページ
- 「Azure Active Directory 設定」次のページ

ユースケース

Ivanti Neurons for MDM とAAD は以下のいずれかの場合に連携できます。

- Microsoft Office 365 の操作
- ユーザ認証のため、Microsoft AAD、Microsoft ADFS、別のSAML 2.0 IDプロバイダー(IdP) のいずれかを設定する
- Microsoft AADをユーザーソースに設定する
- Microsoft AADからユーザーを同期して始めましょう。AADドメインのすべてのユーザとグループが Ivanti Neurons for MDM インスタンスに同期されます

  AAD同期に次の理由によるエラーが存在する場合、**[通知]** ページに通知が表示されます。

  - AADサービスに到達できない
  - すべてのユーザー属性がAADと同期されていない
  - 一部のユーザー属性がAADと同期されていない

- 複数のIdPを持つ環境は現在サポートされていません。
- Microsoft AADをユーザーソースとして使用していない場合は、LDAPのローカルアカウントまたはソースユーザーを使用できます。これには、オンプレのLDAPリソースにアクセスするIvanti Neurons for MDM Connectorの設定が必要です。
- 現時点では、Microsoft AADをユーザー認証にのみ使用し、オンプレのLDAPをユーザーディレクトリに使用することできません。

Azure Active Directory の使用

AADを使用するには、以下のいずれかの方法でユーザ認証用のIdPを設定する必要があります。

- ユーザーソースとユーザー認証の両方にMicrosoft AADを使用する場合は、AADをIdPに設定してください。**[管理] > [ID] > [Ivanti Neurons for MDM IdP 設定]** に進み、メニューから **[AAD]** を選択します。
- ユーザーソースにMicrosoft AADを使用し、ユーザー認証にADFSを使用する場合は、ADFSをIdPに設定してください。**[管理] >[ID] >[オンプレミス IdP 設定]** を開き、メニューから [ADFS] を選択します。
- AAD以外のSAML 2.0 IdPを使用し、ADFSをユーザー認証に使用するには、**[管理] > [ID] > [汎用IdP設定]** を開き、ページ上の指示に従います。

詳細については、「IDプロバイダーの構成」ページ1130をご参照ください。

Azure Active Directory 設定

このトピックでは、Azure Active Directory設定の構成について説明します。

手順

1. **[管理] > [Microsoft Azure] > [AAD ユーザソース]** を開きます。
2. 以下の詳細情報を指定します。
   a. **AAD 名**。
   b. **同期間隔** - Ivanti Neurons for MDMがAADからユーザデータを同期する頻度を変更してください。
   c. **このAADを有効化** - このオプションを使用してAADインスタンスを有効化または無効化します。

d. **AAD からインポートしたユーザを自動的に招待** - AAD から Ivanti Neurons for MDM にインポートしたユーザに自動的に登録招待メールを送信するかどうかを管理します。

e. **管理対象 Apple ID** - AADユーザーの管理対象Apple IDを同期する場合に選択します。

- **なし**
- **パターン** -
  - **ユーザーのメールアドレス**
  - **userUPN**
  - (任意) [「appleid」サブドメインを含める] オプションを選択し、既存のApple IDとの競合を避けます。

f. (任意) **カスタム属性の追加** - デバイス管理に適用したいカスタムユーザ属性をディレクトリサービスから指定します。これにより、各属性は、変数をサポートする構成フィールドの${attributeName}によって参照されます。このオプションを使用するには、すべてのAADサーバーにカスタム属性を一貫して実装しておく必要があります。実装に含まれるいずれかのAADサーバーがこの属性を使用していない場合、この属性に依存する機能が意図通りに機能しないことがあります。

3. AAD設定を変更した後、**[保存]** をクリックします。

Azureテナント

このセクションは以 下 のトピックを含 みます。

本セクションではMicrosoft Azureテナントにおける Ivanti Neurons for MDM の設定方法を説明します。

要件

Microsoft

Ivanti Neurons for MDM のお客様は、Microsoft Intuneの有効なサブスクリプションを持ち、デバイスユーザーに Microsoft Intuneライセンスを割り当てる必要があります。

MobileIron

- Ivanti Neurons for MDM - MobileIron でサポートされる Ivanti Neurons for MDM バージョン 75 から最新のバージョン。
- 追加ライセンス - デバイスコンプライアンスはPremiumサービスとしてSecure UEM PremiumおよびPlatinumのユーザーに提供されています。既存のお客様はPlatinumライセンスで十分です。
- Go for iOS(クライアント) またはGo for Android(クライアント) バージョン75.0からMobileIronがサポートする最新版まで。

複数の Ivanti Neurons for MDM サポート

複数の Ivanti Neurons for MDM を同じAzureテナントに連携している場合は、すべての Ivanti Neurons for MDM と連携を解除するか、特定の(1つの) Ivanti Neurons for MDM からAADコンプライアンス統合のコンプライアンスポリシーを無効化することで、デバイスデータがAzureにアップロードされないようにします。

Ivanti Neurons for MDM の連携を解除する前に必ずコンプライアンスポリシーを無効化してください。

Ivanti Neurons for MDM 管理者プロセス

Ivanti Neurons for MDM 管理者の視点から見た手順：

1. 管理者がデバイスユーザーにIntuneライセンスを適用します。「デバイスユーザーへのIntuneライセンス適用」ページ1229を参照してください。
2. 管理者がAzureポータルにログインします。
3. 管理者がAzureコンプライアンスパートナーとしてMobileIronを追加します。「コンプライアンスパートナーとしてのMobileIronの追加」ページ1230を参照してください。

4. 管理者がアプリの条件付きアクセスポリシーを作成します。「Microsoft Endpoint Managerにおける条件付きアクセスポリシーの作成」ページ1234を参照してください。

5. 管理者がMobileIronとAzureの連携を設定します。「Microsoft Azure の接続 Ivanti Neurons for MDM」ページ1239をご参照ください。

6. 管理者が Ivanti Neurons for MDM でデバイスコンプライアンスポリシーを作成します。「パートナーデバイスコンプライアンスポリシーの作成」ページ1241を参照してください。

7. 条件付きアクセスポリシーが有効になります。デバイスのコンプライアンス状況により、アプリへのアクセスが許可または却下されます。

Ivantiは管理者が各Microsoftアプリでテストを実行することを推奨します。

デバイスユーザーへのIntuneライセンス適用

- 以下の場合は使用しないでください：
  - ユーザーを変更する予定がある、またはユーザーが変わる可能性の高い状況を管理している
  - 1台のデバイスが複数のユーザーに所有されている
- Ivantiは、以下のようなマルチユーザーデバイスに **[ユーザーに割り当てる]** を実行したり、デバイスコンプライアンス構成を配布したりしないことを推奨します。
  - セキュアサインインWebクリップのあるデバイス
  - 共有iPadデバイス
  - Androidキオスクモードのデバイス

Ivanti Neurons for MDM ライセンス要件

デバイスコンプライアンスはPremiumサービスとしてSecure UEM PremiumおよびPlatinumのユーザーに提供されています。既存のお客様はPlatinumライセンスで十分です。

デバイスユーザーへのライセンス一括割り当て

既存のデバイスユーザーにライセンスを一括で割り当てるには：

グループベースの割り当て

https://docs.microsoft.com/ja-jp/azure/active-directory/users-groups-roles/licensing-groups-assign

PowerShell ベースの割り当て

https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

コンプライアンスパートナーとしてのMobileIronの追加

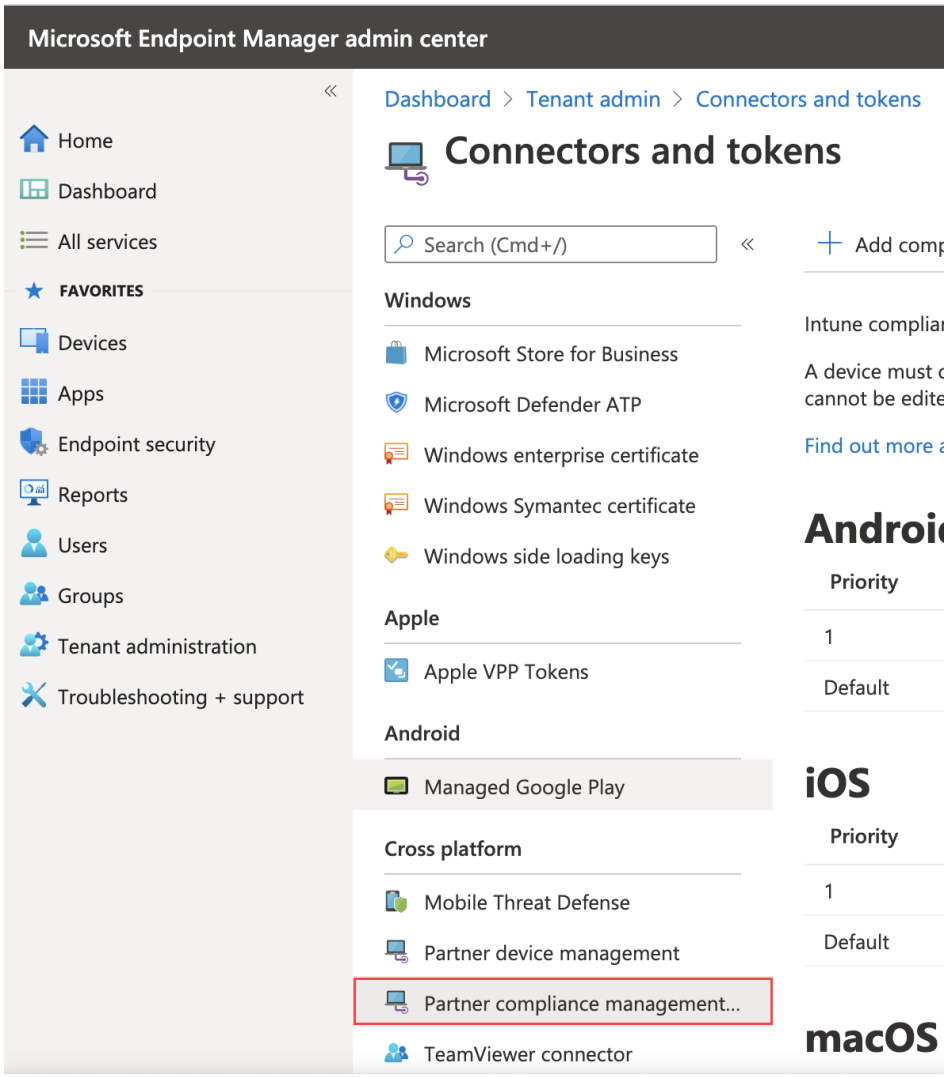
前提条件

- Microsoft Intuneライセンスをインストールしている。「デバイスユーザーへのIntuneライセンス適用」ページ1229を参照してください。
- Microsoft Azureでユーザーを作成している。
- Microsoft Azureでグループを作成している。

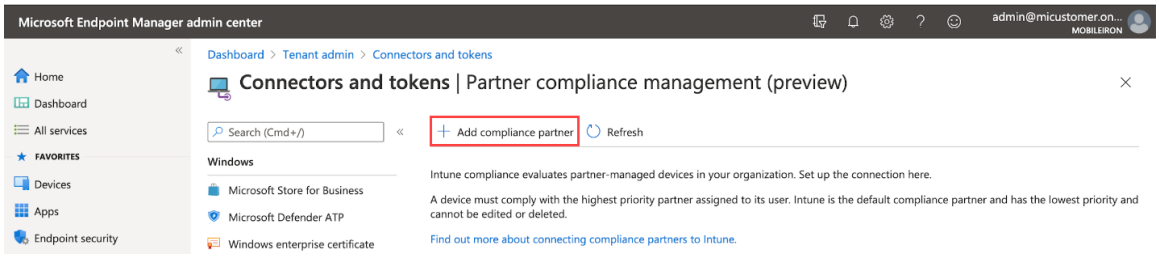
手順

1. ログインします：https://endpoint.microsoft.com

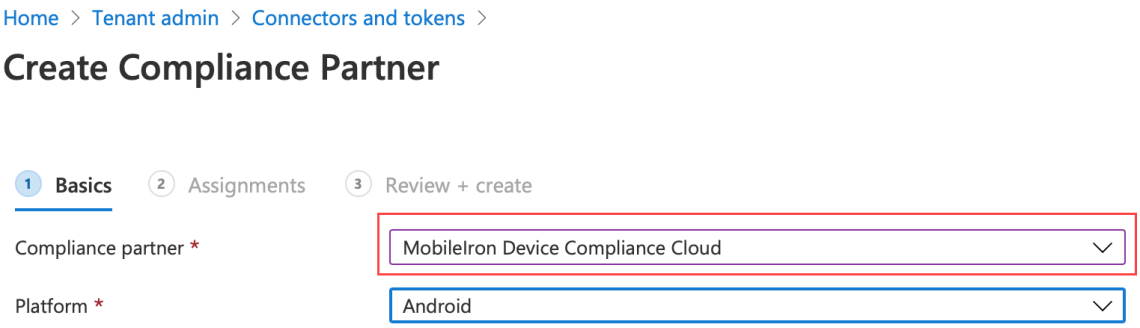
2. Microsoft Endpoint Manager管 理 センターの左 側 のメニューから **[テナント管 理]** をクリックします。**[コネクタとトークン] > [パートナーコンプライアンス管 理]** をクリックします。



3. 検索フィールドの右側にある **[+コンプライアンスパートナーを追加]** をクリックします。

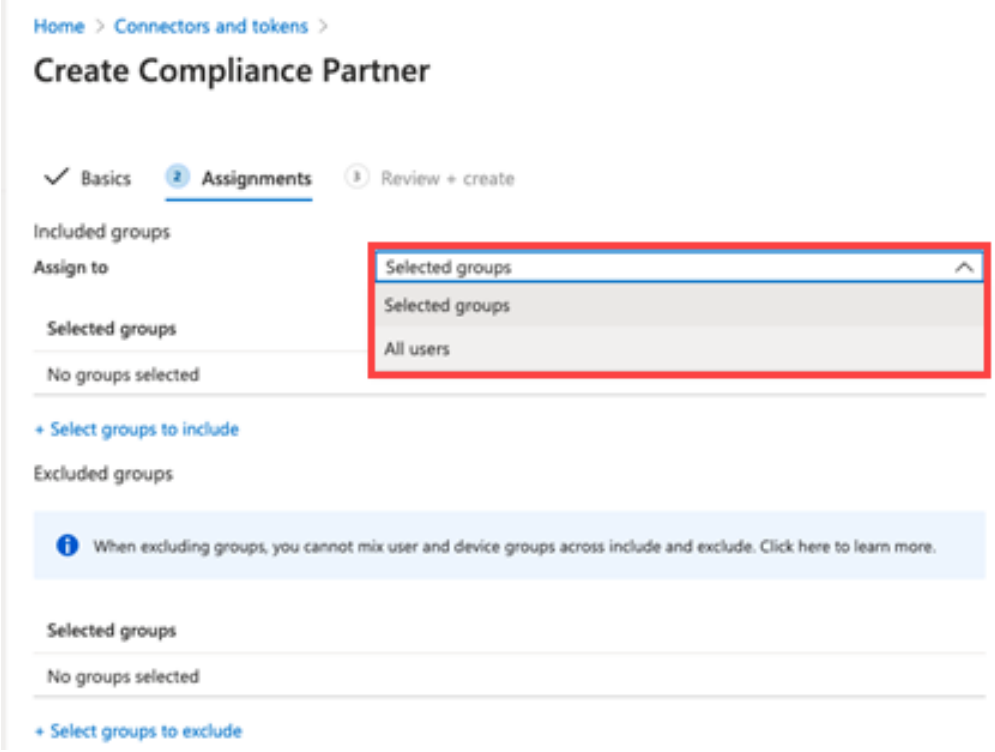


4. [基本] タブで [コンプライアンスパートナー] フィールドのドロップダウンから **[MobileIron Device Compliance Cloud]** を選択します。



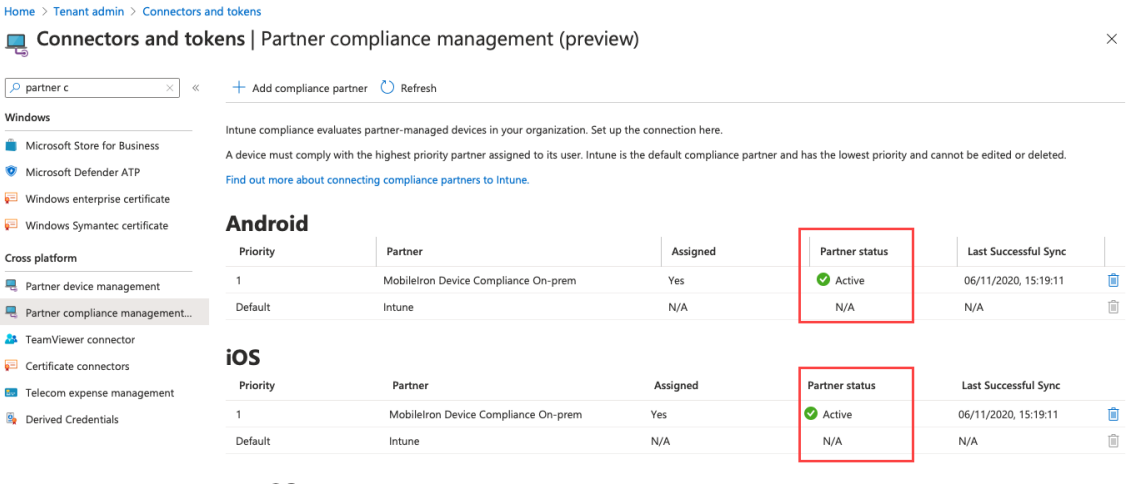
5. [プラットフォーム] フィールドでiOSまたはAndroidを選択し、**[次へ]** をクリックします。

6. **[割り当て]** タブをクリックします。[割り当て先] ドロップダウンでコンプライアンスステータスを指定するユーザーまたはデバイスユーザーグループを選択します。ライセンスを持つユーザー/グループを選択します。



7. **[次へ]** を選択します。

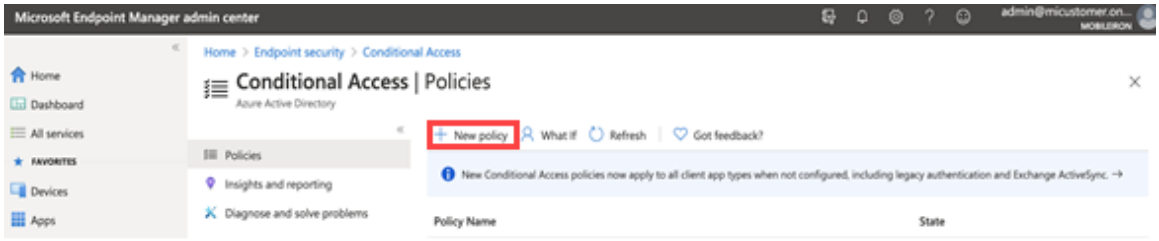
8. **[作成]** をクリックします。新しいコンプライアンスパートナーが [パートナーコンプライアンス管理] ページに表示されます。



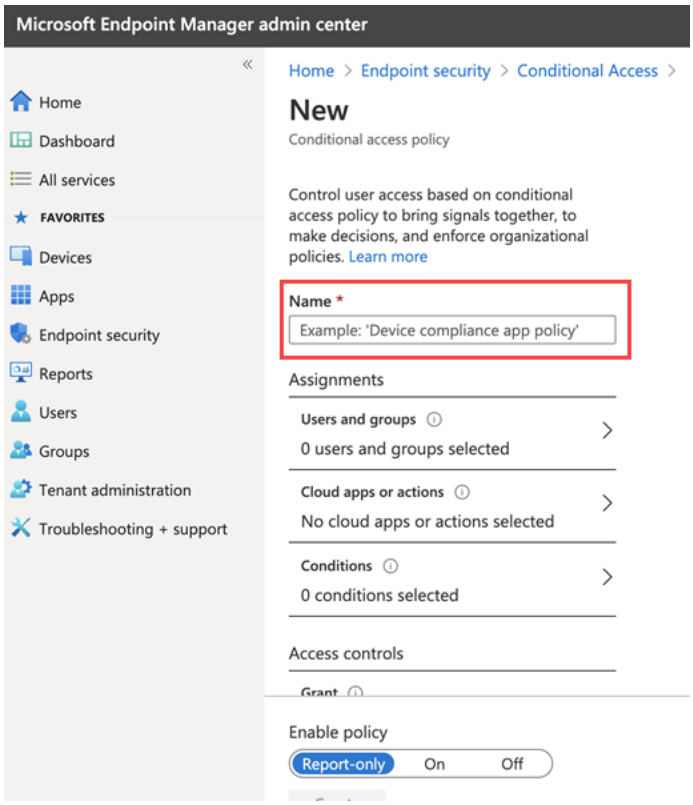
Microsoft Endpoint Managerにおける条 件 付 きアクセスポリシーの作 成

手 順

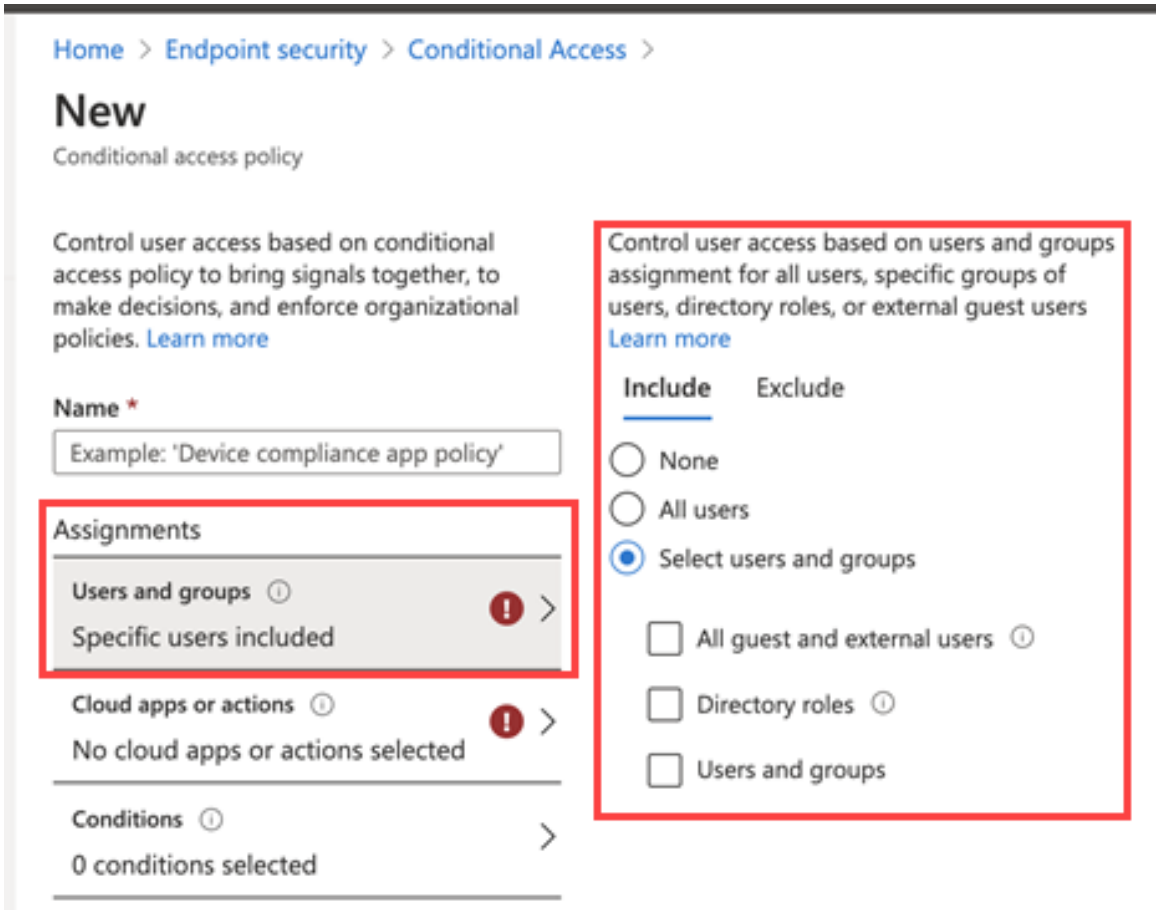
1. Microsoft Endpoint Manager(https://endpoint.microsoft.com) にログインします。
2. Microsoft Endpoint Manager管 理 センターページで **[ホーム]** > **[エンドポイント セキュリティ]** > **[条 件 付 きアクセス]** を開きます。
3. [ポリシー] をクリックし、**[+新しいポリシー]** をクリックします。



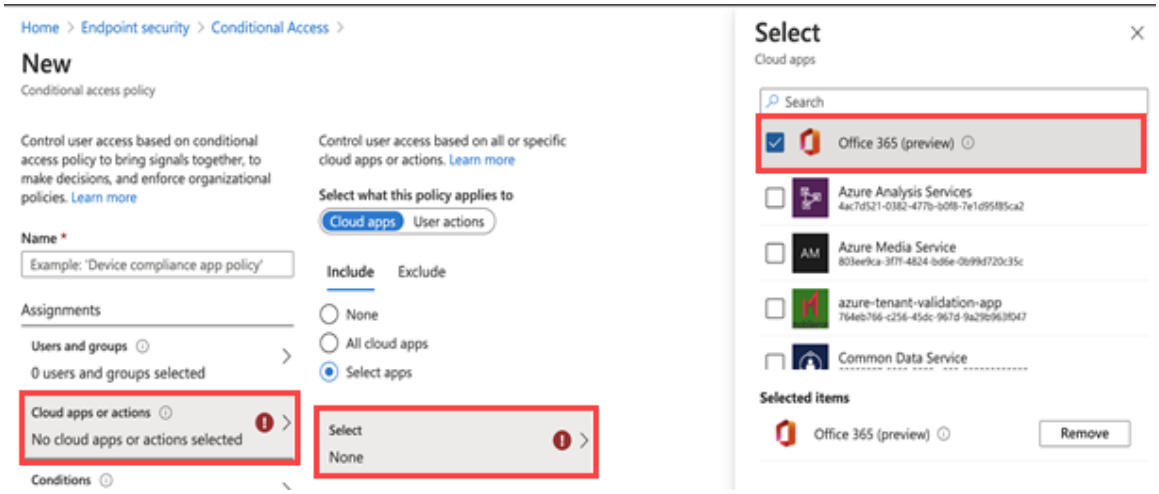
4. 条 件 付 きアクセスポリシーの名 前を入 力します。



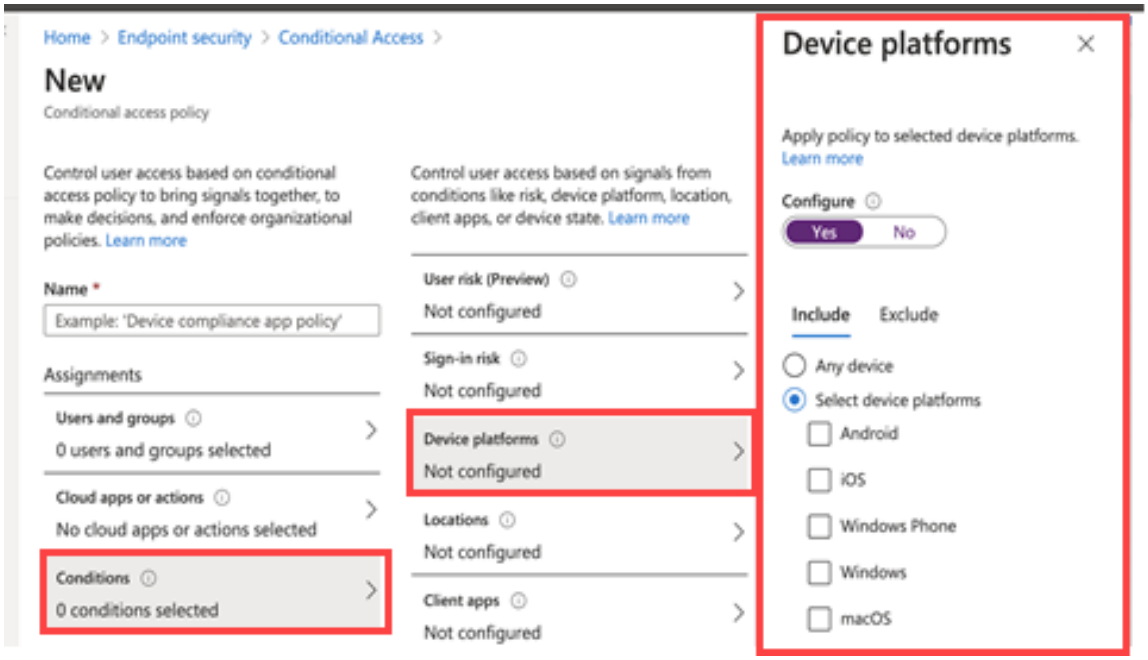
5. [割り当 て] をクリックし、ユーザーやグループにポリシーを割り当 てます。



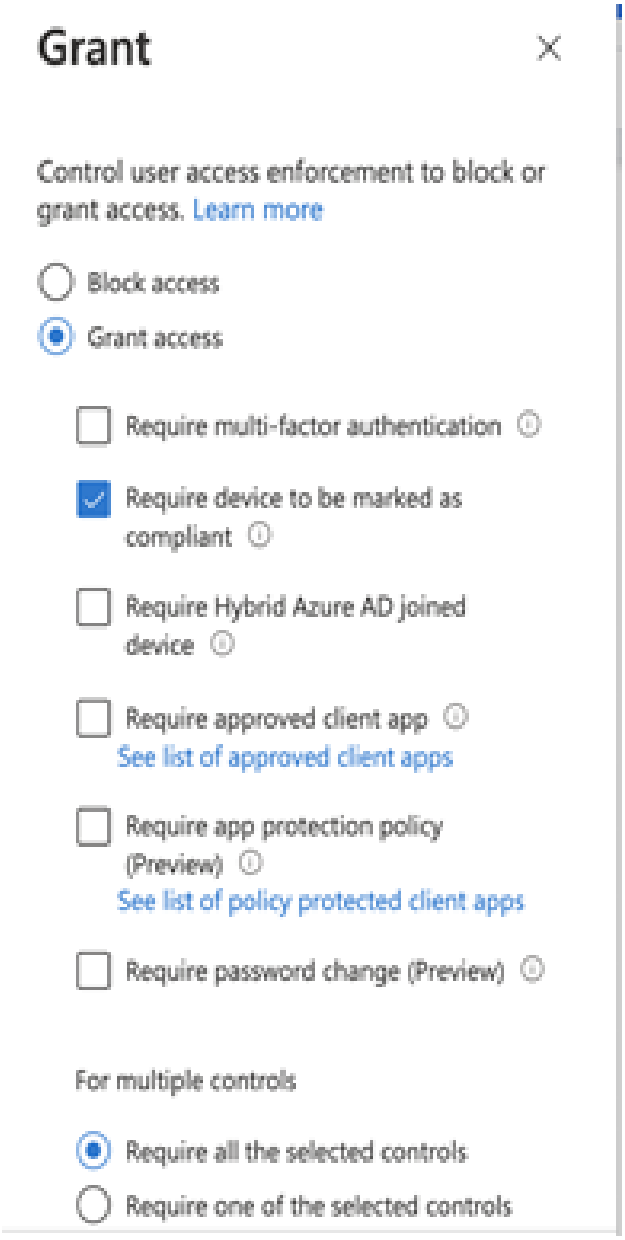
6. **[クラウド アプリまたは操作]** をクリックし、**[選択]** をクリックします。保護する必要のあるアプリを検索し、選択します。



7. 条件をクリックし、**[デバイス プラットフォーム]** をクリックします。適切なデバイスプラットフォームを選択します。



8. **新しい条件付きアクセスポリシーのページから [アクセス制御]** を開き、**[許可]** をクリックして許可またはブロックを選択します。



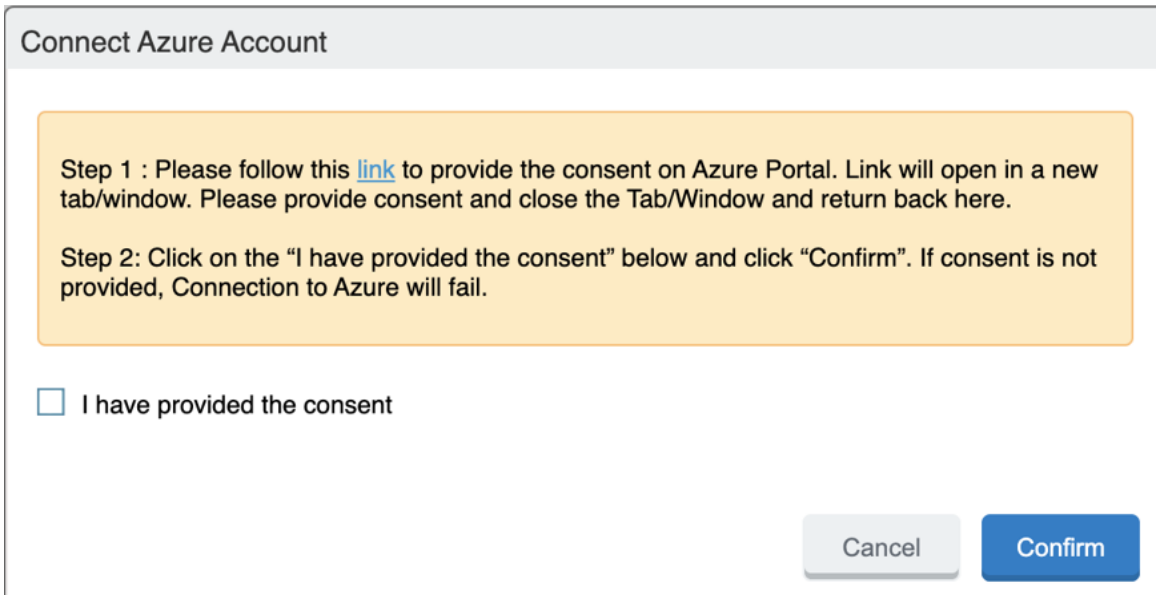
9. 新しいポリシーを有効にするには **[オン]** をクリックします。

10. **[作成]** をクリックします。

Microsoft Azure の接続 Ivanti Neurons for MDM

手順

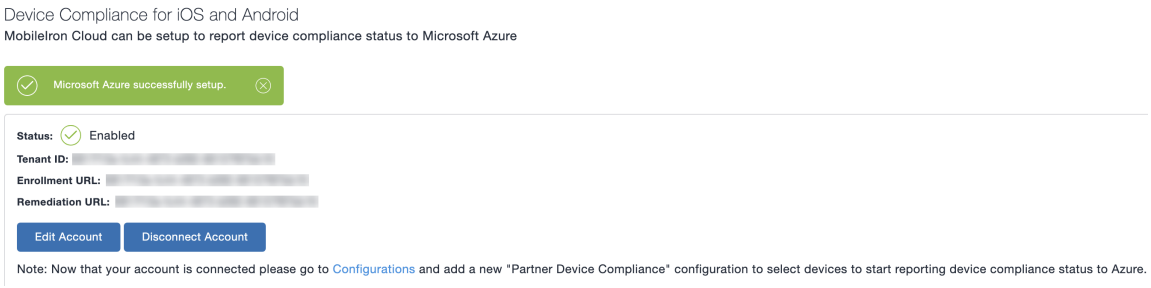
1. Ivanti Neurons for MDM にログインし、**[管理]** > **[Microsoft Azure]** に移動します。
2. 左側のメニューで **[Microsoft Azure]** > **[デバイスコンプライアンス]** をクリックします。
3. **[iOSとAndroidのデバイスコンプライアンス]** セクションまでスクロールします。**[アカウントを設定]** をクリックします。
4. [アカウントを接続] の下で次の詳細情報を入力します。
   - **AzureテナントID** - Microsoft Azureインスタンスを参照します。
   - **登録URL** - (任意) デバイスがMDM登録されていない場合、この登録用URLがデバイスユーザーに表示されます。設定時にはHTTPS形式を使用してください。組織内でページをホストし、デバイスユーザーに登録情報を表示したい場合は、ここにリンクを追加します。
   - **修復URL** - (任意) デバイスがコンプライアンス違反の場合、この修復用URLがデバイスユーザーに表示されます。設定時にはHTTPS形式を使用してください。組織内でページをホストし、デバイスユーザーに修復情報を表示したい場合は、ここにリンクを追加します。
5. **[アカウントを連携]** をクリックします。[Azureアカウントの連携] ダイアログボックスが開きます。



6. [Azure アカウントの接続] ダイアログで**リンク**をクリックします。手順1。
7. **ログイン**します。
8. 許可の内容を読み、**[許可する]** をクリックします。

> ログインした後、再びログインを求めるページが表示された場合はブラウザのタブまたはウィンドウを閉じてください。

9. Ivanti Neurons for MDM に戻ります。[Azureアカウントの連携] ダイアログボックスで **[同意しました]** チェックボックスを選択します。**[確認]** をクリックします。



- アカウントを編集するには **[アカウントを編集]** をクリックします。
- アカウント連携を解除するには **[アカウント連携を解除]** をクリックします。詳しい説明は「Azureテナントのプロビジョニング解除」ページ1247を参照してください。
- アカウントの追加、編集、無効化のすべてのアクティビティはログに記録されます。

パートナーデバイスコンプライアンスポリシーの作成

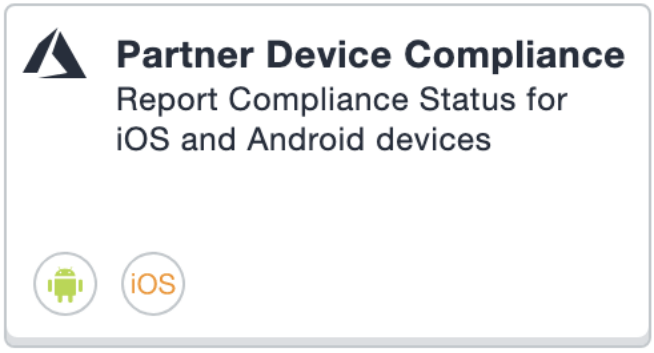
Ivanti Neurons for MDM でパートナー デバイス コンプライアンス ポリシーを作成し、任意のレベルで適用します。パートナーデバイスコンプライアンスポリシーはデバイスのコンプライアンス状態をAzureに報告し、条件付きアクセスに使用します。

前提条件

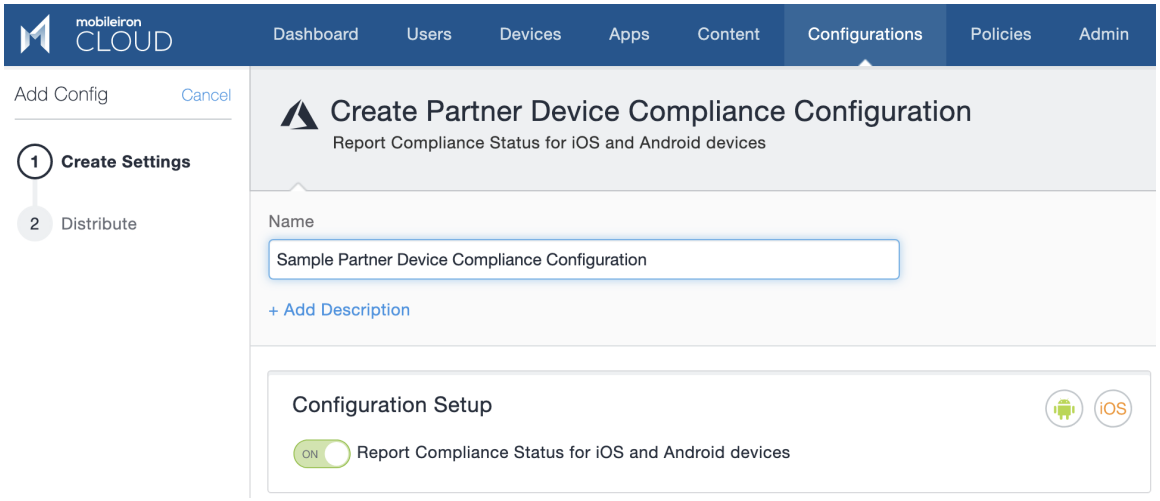
AzureテナントIDを設定する必要があります。「Microsoft Azure の接続 Ivanti Neurons for MDM」ページ1239をご参照ください。

手順

1. Ivanti Neurons for MDM 管理ポータルにログインし、**[構成]** に移動します。
2. **[新規追加]** > **[パートナーデバイスコンプライアンス]** をクリックします。**[構成]** ページで **[パートナーデバイスコンプライアンス]** タイルをクリックしてもかまいません。

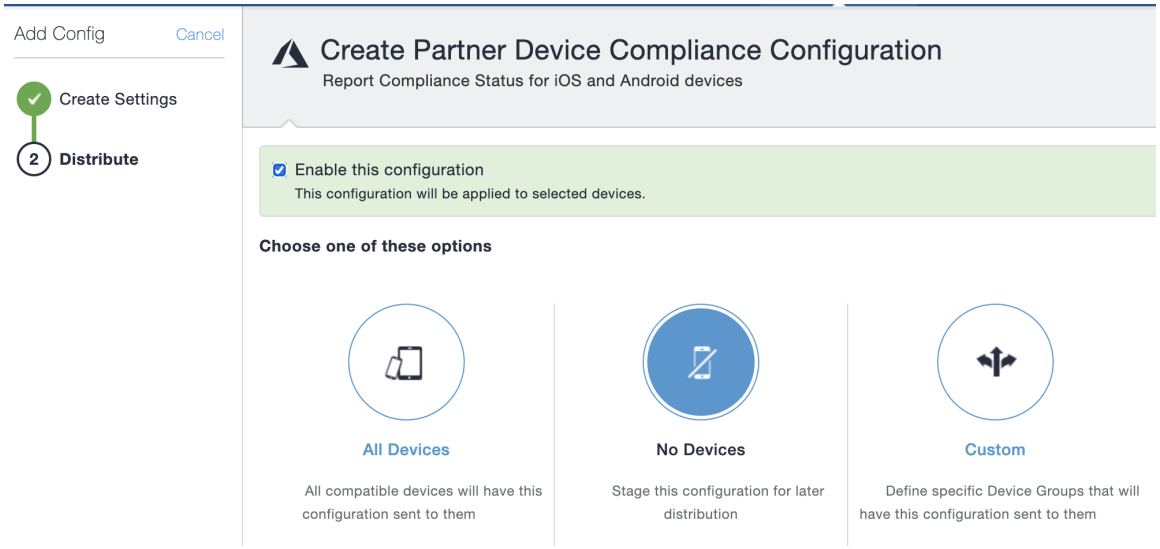


3. **[パートナーデバイスコンプライアンスの作成]** ページで以下のフォームに設定を入力します。



項目	説明
名前	名前を入力します。
+説明を追加	説明を入力します。
iOSおよびAndroidデバイスのコンプライアンス状態をAzureに報告	デフォルトでは [オン] が選択されています。このフィールドが表示されない場合、まずAzureテナントIDを設定する必要があります。「Microsoft Azure の接続 Ivanti Neurons for MDM」ページ1239をご参照ください。 [iOSおよびAndroidデバイスのコンプライアンス状態をAzureに報告] のチェックボックスが有効化されていて、コンプライアンスポリシーがクライアントに適用されている場合、クライアントは [設定] のデバイスに [Microsoft 365 Access] と表示します。デバイスのコンプライアンス状態は以下の場合に報告されます: • デバイスがコンプライアンス違反 • デバイスがコンプライアンス適合 • デバイスがコンプライアンス回復 • 24時間が経過し、状態に変化がない場合は週に1回/7日ごとにレポートが送信されます。

4. **[次へ]** をクリックします。



5. デフォルトでは **[この構成を有効化]** が選択されています。構成の配布レベルを選択します。「構成の追加」ページ426を参照してください。

> AzureテナントはmacOSまたはtvOSに対応しません。

6. **[完了]** をクリックします。

Ivanti Neurons for MDM から Azure へのデバイス ステータスの報告

Ivanti Neurons for MDM は、以下の場合にデバイスインベントリとコンプライアンス状態を報告します。

- オンデバイスのコンプライアンス状態変更
- オンデバイスのインベントリ変更
- 週に1回、Ivanti Neurons for MDM はコンプライアンスとインベントリの状態を報告

コンプライアンスポリシーで選択されたアクションに応じて、以下のデバイス状態が送信されます:

TABLE 2. コンプライアンスポリシーのアクション

アクション (最も厳しいものを適用)	Ivanti Neurons for MDM によって送信される情報
メールとAppConnectアプリをブロックして検疫	コンプライアンス違反デバイス
アラートを送信	Azureにコンプライアンス適合
デバイスの撤去	Azureプラットフォームからデバイスデータを削除

デバイス詳細ページ

デバイスに関するAzure情報は、[デバイス詳細] ページにあります。フィールドの説明と入る可能性のある値は以下のとおりです:

TABLE 3. AZUREデバイス詳細

フィールド	説明
Azureデバイス識別子	MicrosoftがiOS/Androidデバイスに報告するデバイスID。007c8232-9489-4074-9b35-345b16f0a72dなど。Ivanti Neurons for MDM はこのデバイスIDを受信し、デバイスユーザーはMicrosoft Authenticatorアプリケーションに登録してこの機能を使用する必要があります。 デバイスIDを取得できない場合、このフィールドは空白です。
Azureデバイスコンプライアンスステータス	Azure内デバイスのコンプライアンス状態リスト。値は次のいずれか: • 進行中 • 成功 • 失敗
Azureクライアントステータスコード	デバイスがAzureに連携しているかどうかを示します。値は次のいずれか: • Success - デバイスIDを受信可能。 • Internal_Error - クライアント内またはサーバー側に回復可能なエラーが発生。 • Workplace_Join_Required - デバイスの登録が必要。デバイスユーザーがこの状態を修復可能。 • Interaction_Required - 相互作用によるログインが必要。デバイスユーザーがこの状態を修復可能。 • Server_Declined_Scopes - 一部の範囲にはアクセス不可。 • Server_Protection_Policies_Required - 要求されるリソースがIntune条件付きアクセスポリシーの保護対象。 • User_Canceled - デバイスユーザーがWebブラウザで [完了] または [キャンセル] ボタンを押してWeb認証セッションをキャンセル。 • Account_logged_out - アカウントがログアウト済み。

TABLE 3. AZUREデバイス詳細 (CONT.)

フィールド	説明
Azureデバイスコンプライアンスレポート時間	Ivanti Neurons for MDM がデバイスコンプライアンス状態をMicrosoft Intuneに報告する時間。空白は以下のいずれかを意味します: • 機能が無効 • Ivanti Neurons for MDM がデータを受信したが、Microsoft APIをまだ呼び出していない • user_CancelledまたはInternal Errorなどのエラーがある

Azureテナントのプロビジョニング解除

複数のIvanti Neurons for MDMで同じAzureテナントを使用できる場合は、すべてのIvanti Neurons for MDMからプロビジョニング解除します。1つのIvanti Neurons for MDMによるAzure使用を停止する場合は、そのIvanti Neurons for MDM専用のパートナーコンプライアンスポリシーから無効化が可能です。

管理者がIvanti Neurons for MDMで連携解除を実行すると、Ivanti Neurons for MDMはAzureへのデバイスインベントリおよびコンプライアンス状態の報告を停止します。

前提条件

- すべてのデバイスを非マネージドにする
- すべてのデバイスをコンプライアンス違反にする

手順

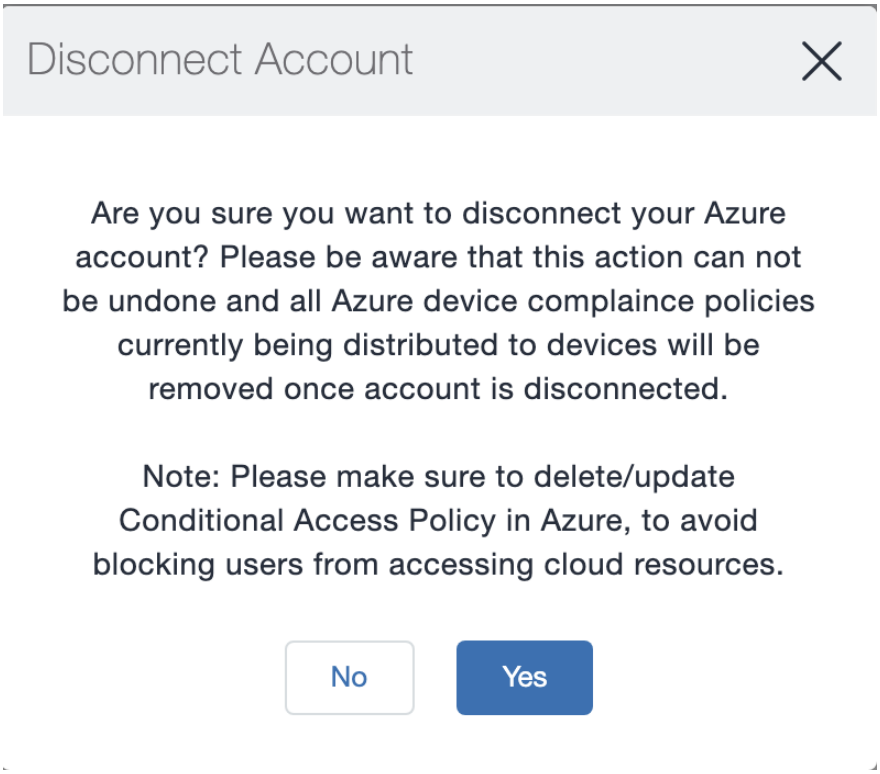
Microsoft

1. Microsoft Azureにログインします。
2. **[Intune] > [条件付きアクセス]**を開きます。条件付きアクセスが無効であることを確認します。

Ivanti Neurons for MDM

1. Ivanti Neurons for MDMにログインし、**[管理]**に移動します。
2. 左側のメニューで**[Microsoft Azure] > [iOS/Androidのデバイスコンプライアンス]**をクリックします。

3. **[アカウントの連携解除]** をクリックします。



4. **[はい]** をクリックします。

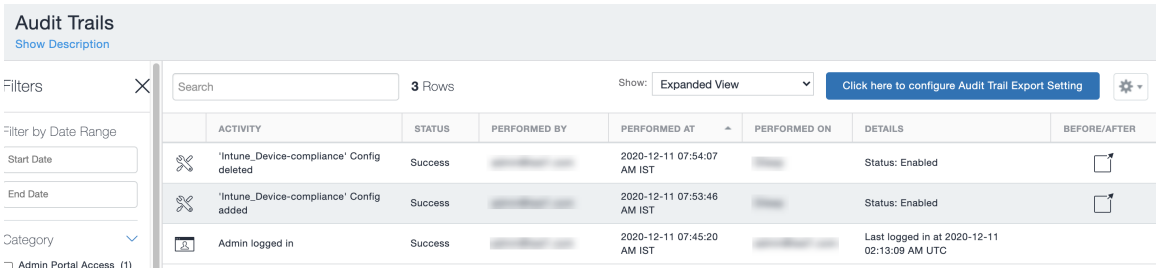
Azureからのデバイス撤去

デバイスを撤去すると、Ivanti Neurons for MDM はAzureにデバイスがもはや管理下になく、コンプライアンスが確保されていないことを報告します。

Azureは撤去済みデバイスの情報を90日後に削除します。

ログに記録されたAzureアカウントアクティビティ

すべてのアクティビティはログに記録されます。



[管理] > [Microsoft Azure] > [Office 365アプリ保護]

ライセンス: Gold

Office 365アプリ保護ポリシーを設定すると、企業データの保護に役立ちます。このポリシーは、Microsoft Graph APIを使用してMicrosoft Office 365アプリに情報漏洩防止(DLP)制御を適用します。これらのGraph APIの一部により管理者は、Graph SDKを利用するiOSとAndroidのネイティブアプリにアプリ保護機能を適用できます。

この機能を使用して以下のようなポリシーを適用してください。

- ユーザーによるOffice 365アプリからの印刷を防止
- Office 365アプリから外部へのデータ共有を防止
- Office 365アプリへのPIN適用
- Office 365アプリからの連絡先同期の無効化

Office 365アプリ保護を使用するための前提条件

Office 365アプリ保護を使用するには、以下が必要です。

- 有効なMobileIronライセンス。
- Ivanti Neurons for MDM で有効化されているOffice 365アプリ保護機能。
- Intuneサブスクリプションまたは Intuneを含むMicrosoft EMSサブスクリプション。
    - ポリシーが適用される使用ごとにライセンスが必要ですが、統合の有効化とテストはライセンス1件のみで実行できます。
- モバイルデバイスでのOffice 365アプリへのアクセス権を含むOffice EnterpriseまたはBusinessの有効なサブスクリプション。
- 1つ以上のOffice 365アプリ。
- Active DirectoryユーザーとAzure Active Directoryの同期。
- Word、Excel、PowerPointのデータを保護するためのOne Drive for Businessのデバイスへのインストール。これは必須ではありません。

- Intuneアプリ保護ポリシーを構成する場合は、Microsoft Azureポータル(https://portal.azure.com/) にアクセスしてください。
- AndroidデバイスへのIntune Company Portalアプリのインストール。
  デバイスユーザーによるサインインは必要ありませんが、デバイス上のデータを保護するためにこのアプリをデバイスにインストールする必要があります。ユーザーがアプリにサインインすれば、保護が自動的に適用されます。

AzureアプリとしてのMobileIronの登録

ここでは、Ivanti Neurons for MDM ソフトウェアでAzureテナント認証情報を登録および保存し、Android および iOS Office 365アプリ対応のMicrosoft Azureクラウドでアプリ保護ポリシーをリモート管理する方法を説明します。必須ではありませんが、2つのブラウザを開いて以下の手順を実行することをお勧めします。最初のブラウザで Microsoft Azureポータルにログインしてください。2番目のブラウザで Ivanti Neurons for MDM 管理ポータルにログインします。

Microsoft Azureポータルの手順

Microsoftは時折、Azureポータルのユーザーインターフェイスを変更する場合があります。この手順はユーザーがMicrosoft Azureポータルの使用に慣れ、AzureアプリとしてMobileIronを登録する際に必要な修正を加えられることを前提とします。

1. 最初のブラウザを開き、Microsoft Azureポータル(https://portal.azure.com/) にログインします。
2. 左ペインの **[アプリ登録]** をクリックします。
3. **[+新規アプリケーションの登録]**をクリックします。
4. 以下の情報を入力し、MobileIronをAzureアプリとして登録します。
   - **名前:** MobileIronアプリの名前を入力します。(このフィールドは4文字以上で必須です。)
   - **アプリケーションタイプ:** Webアプリ/APIを選択します。
   - **サインオンURL:** デバイスユーザーがMobileIronにサインイン(必須) するためのURLを入力します。
5. ペイン最下部の **[作成]** をクリックし、アプリを追加してAzureホームページに戻ります。
6. 新しく作成したMobileIronアプリをAzureホームページでクリックします。
7. Azureホームページに戻り、MobileIron Azureアプリへの許可を割り当てます。

8. 新しく作成されたMobileIronアプリに必要なAPI許可を設定するには、アプリ登録でアプリ名をクリックします。

9. **[API許可]** > **[許可を追加]** をクリックします。

10. **[Microsoft Graph]** > [委譲許可] > [Device Management Apps] セクションを開き、**[DeviceManagementApps.Read.All]** 許可を選択して **[保存]** をクリックします。をクリックします。デフォルトではアプリのuser.Read許可が有効化されています。

11. アクセス権を付与するには **[MobileIronに管理者の同意を付与]** をクリックします。

12. Ivanti Neurons for MDM管理ポータルで次の手順を実行します。

Ivanti Neurons for MDM 管理ポータルの手順

1. 2番目のブラウザを開き、Ivanti Neurons for MDM 管理ポータルにログインします。

2. **[管理]** > **[Microsoft Azure]** > **[Office 365アプリ保護]** を開きます。

3. **アプリケーションID**をIvanti Neurons for MDM管理ポータルに貼り付けます。

   手順

   a. Azureポータルを開きます。

   b. [MobileIronアプリ] > **[プロパティ]** を選択します。

   c. **アプリケーションID**をコピーします。

   d. 管理ポータルで **[管理]** > **[Microsoft Azure]** > **[Office 365アプリ保護]** に戻ります。

   e. **[アプリケーションID]** フィールドに貼り付けます。

4. **アプリケーションシークレット**(クライアントシークレット)をIvanti Neurons for MDM管理ポータルに貼り付けます。

   手順

   a. Azureポータルを開きます。

   b. [MobileIronアプリ] を選択します。

   c. **[キー]** をクリックし、**[キーの説明]** に名前を入力した後、**[時間]** で有効期間を選択します。

d. **[保存]** をクリックし、**[キー]** の値をコピーします。

e. 管理ポータルで **[管理]** > **[Microsoft Azure]** > **[Office 365アプリ保護]** に戻ります。

f. **[アプリケーションシークレット]**(クライアントシークレット) フィールドに貼り付けます。

5. **テナントID**をIvanti Neurons for MDM管理ポータルに貼り付けます。

   手順

   a. Azureポータルを開きます。

   b. **左ペインの** [Azure Active Directory] をクリックし、[プロパティ] をクリックします。

   c. ディレクトリIDをコピーします。

   d. 管理ポータルで **[管理]** > **[Microsoft Azure]** > **[Office 365アプリ保護]** に戻ります。

   e. **[テナントID]** フィールドに貼り付けます。

6. Intune管理者の**ユーザー名**と**パスワード**を入力します。

   - Azureアカウントにはグローバル管理者権限または限定管理者 + Intuneサービス管理権限が必要です。
   - Ivantiは、Intuneサービス管理権限のみのローカルAzureアカウントの作成を推奨しています。IDプロバイダーに連携しているユーザーアカウントはMicrosoftにサポートされていないためGraph APIでの認証ができません。
   - アカウントにMFA要件を指定することはできません。指定した場合は認証が失敗します。

7. **[認証および保存]** をクリックします。

   送信した日付が正しくない場合、エラーメッセージが表示されます。

Office 365アプリ保護のポリシー

Microsoft Graphの認証情報を構成した後、**[アプリ]** > **[Office 365アプリ保護]** を開き、各ユーザーグループについてiOSまたはAndroidデバイスに対応する新しいOffice 365アプリ保護ポリシーを追加します。

ポリシーは **[アプリ]** > **[Office 365アプリ保護]** ページにリスト化されています。ページは **[アプリポリシー]** タブにあります。ポリシーのリストは、最新のタイムスタンプ、プラットフォーム、割り当てられたアプリ、展開されているユーザーグループなど、表形式の詳細情報を提供します。

iOSデバイスに対応するOffice 365アプリ保護ポリシーの追加

手順

1. **[アプリ] > [Office 365アプリ保護]** を開きます。
2. **[アプリポリシー] > [+ 追加]** をクリックします。
3. ポリシーの**名前**と**説明**(任意)を入力します。
4. [OSを選択]で **[iOS]** をクリックします。
5. **[データ再配置]** で以下の設定とオプションを選択します。
   - iTunesおよびiCloudバックアップを防止
   - アプリが他のアプリにデータを転送するのを許可 - すべてのアプリ(デフォルト)、ポリシーマネージドアプリ、なし
   - アプリが他のアプリからデータを受信するのを許可 - すべてのアプリ(デフォルト)、ポリシーマネージドアプリ、なし
   - 「名前を付けて保存」を防止
   - 異なるアプリ間の切り取り、コピー、貼り付けを制限 - 任意のアプリ(デフォルト)、ブロック、ポリシーマネージドアプリ、ペーストインでポリシーを管理
   - マネージドブラウザで表示されるWebコンテンツを制限
   - アプリデータを暗号化 - デバイスがロックされている場合(デフォルト)、デバイスがロックされ、開いたファイルがある場合、デバイスの再起動後、デバイス設定の使用
   - 連絡先同期を無効化
   - 印刷を無効化
6. **[アクセス]** で以下の設定とオプションを選択します。
   - アクセスにPINを要求
   - PINリセットまでの試行回数(デフォルトは5)
   - シンプルなPINを許可

- PINの長さ(デフォルトは4)
- PINの代わりに指紋を許可(iOS 8+)
- デバイスPINが管理されている場合はアプリPINを無効化
- アクセスに企業認証情報を要求
- 脱獄済みのデバイスやルート化したデバイスでマネージドアプリの実行をブロック
- アクセス条件の再チェック間隔(分) :
  - タイムアウト - 1から65535までの値(デフォルトは30)
  - オフライン - 猶予期間は1から65535までの値(デフォルトは720)
  - アプリデータがワイプされるまでのオフライン間隔(日) - 1から65535までの値(デフォルトは90)
- 最小iOSオペレーティングシステムを要求
- 最小iOSオペレーティングシステムを要求(警告のみ)
- 最小アプリバージョンを要求
- 最小アプリバージョンを要求(警告のみ)
- 最小Intuneアプリ保護ポリシーSDKバージョンを要求

7. **[次へ]** をクリックします。
8. このポリシーを適用するアプリを選択し、割り当てます。
9. **[次へ]** をクリックします。
10. このポリシーが適用されるユーザーグループを選択します。
11. **[完了]** をクリックします。

Androidデバイスに対応するOffice 365アプリ保護ポリシーの追加

手順

1. **[アプリ]** > **[Office 365アプリ保護]** を開きます。
2. **[アプリポリシー]** > **[+ 追加]** をクリックします。

3. ポリシーの**名前と説明**(任意)を入力します。
4. [OSを選択]で**[Android]**をクリックします。
5. **[データ再配置]**で以下の設定とオプションを選択します。
   - Androidバックアップを防止
   - アプリが他のアプリにデータを転送するのを許可 - すべてのアプリ(デフォルト)、ポリシーマネージドアプリ、なし
   - アプリが他のアプリからデータを受信するのを許可 - すべてのアプリ(デフォルト)、ポリシーマネージドアプリ、なし
   - 「名前を付けて保存」を防止
   - 異なるアプリ間の切り取り、コピー、貼り付けを制限 - 任意のアプリ(デフォルト)、ブロック、ポリシーマネージドアプリ、ペーストインでポリシーを管理
   - マネージドブラウザで表示されるWebコンテンツを制限
   - アプリデータを暗号化
   - デバイス暗号化が有効化されている場合はアプリ暗号化を無効化
   - 連絡先同期を無効化
   - 印刷を無効化

6. **[アクセス]** で以下の設定とオプションを選択します。
    - アクセスにPINを要求
    - PINリセットまでの試行回数(デフォルトは5)
    - シンプルなPINを許可
    - PINの長さ(デフォルトは4)
    - PINの代わりに指紋を許可(Android 6+)
    - デバイスPINが管理されている場合はアプリPINを無効化
    - アクセスに企業認証情報を要求
    - 脱獄済みのデバイスやルート化したデバイスでマネージドアプリの実行をブロック
    - アクセス条件の再チェック間隔(分):
        - タイムアウト - 1から65535までの値(デフォルトは30)
        - オフライン - 猶予期間は1から65535までの値(デフォルトは720)
        - アプリデータがワイプされるまでのオフライン間隔(日) - 1から65535までの値(デフォルトは90)
    - スクリーンキャプチャとAndroidアシスタントをブロック
    - 最小Androidオペレーティングシステムを要求
    - 最小Androidオペレーティングシステムを要求(警告のみ)
    - 最小アプリバージョンを要求
    - 最小アプリバージョンを要求(警告のみ)
    - 最小Intuneアプリ保護ポリシーSDKバージョンを要求
7. **[次へ]** をクリックします。
8. このポリシーを適用するアプリを選択します。
9. **[次へ]** をクリックします。
10. このポリシーを適用するユーザーグループを選択します。

11. **[完了]** をクリックします。

Office 365アプリ保護ポリシーの変更

手順

1. **[アプリ]** > **[Office 365アプリ保護]** を開きます。
2. **[アプリポリシー]** をクリックします。
3. 変更したいポリシーの名前をクリックします。
4. ポリシーの詳細ページで **[編集]** をクリックします。
5. ポリシーの構成を変更します。
6. **[次へ]** をクリックします。
7. このポリシーを適用するアプリのリストを変更します。
8. **[次へ]** をクリックします。
9. このポリシーを適用するユーザーグループを変更します。
10. **[完了]** をクリックします。

Office 365アプリ保護ポリシーの削除

手順

1. **[アプリ]** > **[Office 365アプリ保護]** を開きます。
2. **[アプリポリシー]** をクリックします。
3. **[アクション]** 列で、削除したいポリシー名に対応する削除アイコンをクリックします。
4. **[はい]** をクリックして確定します。

Office 365アプリ構成

[アプリ] > **[Office 365アプリ保護]** ページを開き、**[アプリ構成]** タブで各ユーザーグループのOffice 365アプリ構成を追加、変更、削除します。このアプリ構成で、管理者はキーと値のペアのリストを追加し、1つ以上のOffice 365アプリに構成を割り当てることができます。[アプリ構成] タブには、最新のタイムスタンプ、割り当てられたアプリ、展開のステータスなど、表形式で詳細情報が記載されています。

Office 365アプリ構成の追加

手順

1. **[アプリ] > [Office 365アプリ保護]** を開きます。
2. **[アプリ構成] > [+ 追加]** をクリックします。
3. 構成の**名前**と**説明**(任意)を入力します。
4. キーと値のペアを入力します。
5. **[次へ]** をクリックします。
6. この構成を適用するアプリを選択します。
7. **[次へ]** をクリックします。
8. この構成を適用するユーザーグループを選択します。
9. **[完了]** をクリックします。

Office 365アプリ構成の変更

手順

1. **[アプリ] > [Office 365アプリ保護]** を開きます。
2. **[アプリ構成]** をクリックします。
3. 変更したい構成の名前をクリックします。
4. 構成の詳細ページで **[編集]** をクリックします。
5. あるいは、**[アプリ配布]** または **[ユーザーグループ配布]** タブをクリックします。**[編集]** をクリックし、それらの設定だけを変更して **[保存]** をクリックします。
6. 構成の設定を変更します。
7. **[次へ]** をクリックします。
8. この構成を適用するアプリのリストを変更します。
9. **[次へ]** をクリックします。

10. この構成を適用するユーザーグループを変更します。

11. **[完了]** をクリックします。

Office 365アプリ構成の削除

手順

1. **[アプリ]** > **[Office 365アプリ保護]** を開きます。
2. **[アプリ構成]** をクリックします。
3. **[アクション]** カラムで、削除したい構成名に対応する削除アイコンをクリックします。
4. **[はい]** をクリックして確定します。

Office 365 アプリを使用するコンプライアンス違反ユーザー

管理者は、コンプライアンス違反のあるユーザーとデバイスのリストを確認できます。このページを使用し、フラグのあるデバイスにOffice 365アプリがある場合はワイプしてください。

Office 365アプリのワイプ

手順

1. **[アプリ]** > **[Office 365アプリ保護]** を開きます。
2. **[コンプライアンス違反ユーザー]** をクリックします。
3. 以下のいずれかのアクションを実行します。
   - リストからユーザーを選択し、**[Office 365アプリをワイプ]** をクリックします。
   - ユーザーの名前をクリックし、コンプライアンス違反のアプリを持つデバイスのリストを表示します。**[アクション]** カラムで、特定のデバイスの **[Office 365アプリをワイプ]** アイコンをクリックします。
   - ユーザーの名前をクリックし、コンプライアンス違反のアプリを持つデバイスのリストを表示します。各デバイスの名前をクリックし、アプリとバンドルID/パッケージ名、フラグの理由を確認します。**[Office 365アプリをワイプ]** をクリックします。
4. **[はい]** をクリックしてアクションを確定します。

または、次の手順を実行します。

1. **[ユーザー]** を開きます。
2. ユーザーの名前をクリックし、ユーザー詳細ページを表示します。
3. **[アクション]** > **[Office 365アプリをワイプ]** をクリックします。
4. Office 365アプリをワイプする必要のあるデバイスを選択します。
5. **[OK]** をクリックしてアクションを確定します。

Office 365アプリのワイプ要求取り消し

手順

1. **[ユーザー]** を開きます。
2. ユーザーの名前をクリックし、ユーザー詳細ページを表示します。
3. **[Office 365保護]** タブをクリックします。
4. **[レポートタイプ選択]** ドロップダウンボックスから **[ワイプ要求]** レポートを選択し、対応する情報を表示します。
5. ワイプ要求を取り消す必要のあるデバイスを選択します。ステータスがワイプ保留のデバイスのみ選択可能です。
6. **[ワイプを取り消す]** をクリックします。
7. **[OK]** をクリックしてアクションを確定します。

Office 365アプリ保護を使用するユーザーのアプリレポート

管理者は、以下のレポートのいずれかを選択し、Office 365アプリ保護を使用しているユーザーのリストと関連情報を確認できます。

- アプリポリシーレポート
- アプリ構成レポート
- ワイプ要求

アプリレポートに記載されている情報には、バンドルID/パッケージ名、デバイス名、デバイスの種類、ポリシーまたは構成(デバイスに適用されている)、ステータス(同期している、同期しているが古い、同期していない)、最後のチェックイン時刻などがあります。アプリレポートの情報はCSVファイルにエクスポートし、後で参照や分析が可能です。

ワイプ要求レポートに記載されている情報には、表示名、ユーザー名、デバイス名、デバイスの種類、ワイプステータス(ワイプ保留中またはワイプ完了)などがあります。

レポートを表示するには、以下の手順を実行してください。

1. **[ユーザー]** を開きます。
2. ユーザーの名前をクリックし、ユーザー詳細ページを表示します。
3. **[Office 365保護]** タブをクリックします。
4. **[レポートタイプ選択]** ドロップダウンボックスから1つレポートを選択し、対応する情報を表示します。
5. (任意) ワイプ要求レポートページからワイプ要求を取り消す必要のあるデバイスを選択し、**[ワイプを取り消す]** をクリックします。ステータスがワイプ保留のデバイスのみ選択可能です。
6. (任意) **[CSVにエクスポート]** をクリックし、後で参照または分析できるようレポートの内容をCSVファイルにダウンロードします。

Googleアプリとの連 携

このセクションは以 下 のトピックを含 みます。

マネージドGoogle Playアカウント(Android Enterpriseアカウント)

ライセンス: Silver

Android Enterpriseデバイスを使用し、構成するには、マネージドGoogle Playアカウントが必要です。Google Apps Directory Sync(GADS)を使用したり、Googleアカウントでデバイスを登録したりする必要はありません。

重要: すでにAndroid Enterpriseを設定している場合、この機能を使用するには、まずデバイスを撤去する必要があります。

Android Enterpriseの構成

手順

1. Ivanti Neurons for MDM ポータルにログインします。
2. **[管理] > [Google] > [Android Enterprise]** に移動します。
3. **[マネージドGoogle Playアカウント]** で **[Googleを認証]** をクリックし、[Google Play for Work] ページを表示します。
4. **[開始]** をクリックします。
   - 会社名を入力します。
   - Android Enterprise契約を承諾します。
5. **[確認]** をクリックします。
6. **[登録を完了]** をクリックします。

マネージドGoogle Playアカウントを使用してAndroid Enterpriseを設定した場合、ユーザー1人に対して登録可能なデバイス数には制限があります。この制限を解除するには、新規ユーザーを作成する際に **[Android Enterpriseデバイスアカウント]** オプションのチェックを選択し、このアカウントに結び付くAndroid Enterprise仕事用マネージドデバイス登録に自動的にGoogleデバイスアカウントが割り当てられるようにします。

デバイスアカウントはCOSU(シングルユース)導入(キオスクモードなど)を想定しています。デバイスアカウントを持つユーザーはGoogle Playへのアクセスを制限される可能性があります。

場合によっては、マネージドGoogle Playアカウントまたはそのトークンが、認証トークンの有効期限切れやアカウントまたは企業の削除など、さまざまな理由で期限切れになることがあります。このような場合、Google Playサービスは、ブロードキャストによってクライアントに通知を出します。そしてクライアントは、既存のアカウントを削除し、UEMサーバーから取得した新しいトークンでアカウントを追加することによって、デバイスを再プロビジョニングします。

古いアカウントを削除できない、または再プロビジョニングの試行回数が多すぎるためにアカウントを再プロビジョニングできない場合、最初からやり直すようユーザーに通知が送られます。ユーザーは、デバイスが仕事用プロファイルモードであれば撤去し、マネージドデバイスモードであれば工場出荷時の状態にデバイスをリセットする必要があります。

Androidデバイスの登録

Androidデバイスの登録中、IMEI、電話番号、その他の電話識別子を報告して登録を完了するためにユーザーからの電話許可が必要な場合は、このオプションを構成します。構成すると、Goクライアントがデバイス識別子にアクセスすることを許可するようデバイスユーザーにプロンプトが表示されます。

この構成は、Androidデバイス(Androidバージョン6.0以降)を新規登録する場合にのみ適用されます。

1. **[管理]** > **[Google]** > **[登録]** を選択します。
2. **[選択登録中にAndroidデバイス識別子を要求(仕事用プロファイルとデバイス管理者)]** のチェックボックスを選択します。
3. **[保存]** をクリックします。

Android Management API

Android Management API(AMAPI) は、GoogleのAndroid UEM機能をIvanti Neurons for MDM に統合するGoogleのクラウドプラットフォームAPIです。デバイスにデバイス管理用のクライアントアプリをインストールせずにAndroid Enterpriseデバイスを管理するには、Android Enterprise設定でAndroid Management APIフレームワークを有効化します。現在、Go app は、MTD などの他の機能に関してはデバイスにプッシュされることができません。

設定時にAndroid Enterpriseアカウントを構成すると、Android Management APIフレームワークの有効化と使用が可能となります。有効化すると以下が可能になります。

- Enrollmentプロファイルを追加してデバイス登録にQRコードを使用する。
- 特定の目的を果たすよう、登録デバイス専用のデバイス構成(会社所有シングルユース: COSU) を作成する。

Android Management APIは現在、Google Playをインストールし、専用モードにプロビジョニングされているAndroidバージョン9以降のデバイスでのみサポートされます。企業専用モードは、COSU(企業所有シングルユース) モードとも呼ばれ、デバイス所有者モードの一種です。この機能は以下のデバイスアクションもサポートします。

- ロック
- 再起動
- サーバーに同期
- ワイプ

デバイスチェックインは一定の間隔(毎時間) でスケジュールされています。ただし即座に実行したい場合は、デバイス詳細ページからデバイスアクション [サーバーに同期] を使用します。AMAPIデバイスは Ivanti Neurons for MDM に強制チェックインを送信しません。インベントリ更新はデバイス上でアクティビティがあった場合のみ実行されます。

Android Management APIの有効化

Android Management APIを有効化するには、**[管理] > [Android Enterprise] > [Googleを認証](有効なGmailアドレスが必要) > [Android Enterprise有効]** に進みます。

Android Management API機能の有効化状態(**[はい]** が有効、**[いいえ]** が無効) はデバイス詳細ページにも表示されます。

GSuiteアカウントは現在COSUではサポートされていません。

Enrollmentプロファイルの追加

QRコードのスキャンまたはトークンの英数字列を使用してAndroidデバイスを登録するには、Enrollmentプロファイルの作成が必要です。EnrollmentプロファイルはAndroid Management APIを有効化している場合のみ作成できます。Enrollmentプロファイルに関連付けるカスタムデバイス属性も作成できます。

1. **[管理] > [Android Enterprise] > [登録プロファイル]** を選択します。
2. **[Enrollmentプロファイル - 会社所有専用デバイス]** ウィンドウで次の項目を設定します。

設定	説明
[名前]	このEnrollmentプロファイルを識別する名前を入力します。
説明	このEnrollmentプロファイルの目的を明示する説明を入力します。
ユーザー名	有効なユーザー名の最初の数文字を入力し、表示された一致結果から選択します。 有効なユーザー名にはローカルユーザー名とLDAPユーザー名が含まれます。 Enrollmentプロファイルはプロファイルのコードを使用して登録デバイスをタグ付けし、Enrollmentプロファイルに対応するユーザーに帰属するデバイスとして表示します。
トークンの有効性	認証トークンQRコードスキャンが有効な日数を入力します。入力可能な数は1～30です。有効日数を過ぎたトークンやEnrollmentプロファイルを使用するとデバイスがリセットされます。
カスタムデバイス属性	[アクション] カラムで **[+新規追加]** をクリックし、Enrollmentプロファイルに関連付けるカスタムデバイス属性を追加します。 a. **[属性名]** カラムのドロップダウンリストからカスタムデバイス属性を選択します。 b. **[値]** カラムでカスタム属性の値を入力します。 c. **[保存]** をクリックします。追加したカスタムデバイス属性が表に表示されます。削除するには [アクション] カラムの **[削除]** オプションをクリックします。

設定	説明
	カスタム属性は、プロファイル作成中にEnrollmentプロファイルに対してのみ追加できます。プロファイル作成後は属性フィールドを編集できません。

3. **[保存]** をクリックします。**[プロファイルの概要]** ウィンドウに以下のトークン情報が表示されます。
   - 名前
   - 説明
   - ユーザー名
   - トークン作成日
   - トークン有効期限
   - トークンの値
   - QRコード
   - カスタムデバイス属性

登録後10分以内にデバイスに適切な構成が取得されない場合、デバイスはリセットされます。このような場合は、登録トークン/QRコードを使用して再登録する必要があります。

Enrollmentプロファイルは作成されると **[Enrollmentプロファイル]** ページに表示されます。**[アクション]** カラムでは以下のいずれかのアクションを実行できます。

- [表示] アイコンをクリックすると、[プロファイルの概要] ウィンドウにEnrollmentプロファイルの詳細が表示されます。このウィンドウにはQRコードも表示されます。
- [編集] アイコンをクリックすると、Enrollmentプロファイルの詳細を編集できます。

  トークンの有効性のみ編集可能です。他の属性は編集できません。

- Enrollmentプロファイルを削除する場合は [削除] をクリックします。

COSU構成の作成

管理者は、Android Enterpriseの専用デバイス(会社所有シングルユース:COSU)構成を使用して、特定の目的に使用する専用デバイスを構成できます。COSU構成は仕事用マネージドデバイス(デバイス所有者モード)に配布され、キオスクモードでユーザーがアプリを1つだけ使用できるようにします。会社所有デバイス上の仕事用プロファイルのデバイスはサポートされません。

この構成では、画面にアプリをピン留めするよう管理者がデバイスを設定します。キオスクモードのユーザーが、このアプリのピン留めを外す、アプリを離れてデバイスの他の画面に移動する、デバイス上の他のアプリを使用することはできません。

[詳細オプションとアプリ構成]から[デバイスにインストール]を選択すれば、他のアプリもAMAデバイスに強制インストールできますが、設定によってキオスクアプリが画面にピン留めされている限り他のアプリにはアクセスできません。マルチアプリキオスクでは、仕事用マネージドデバイス(デバイス所有者モード)のキオスク機能を使用することを推奨します。これにより、アプリやデバイスの設定をより細かく制御し、マルチユーザーモードにも拡張可能になります。

管理者は、ニーズに応じて各種のオプションを検討し、この構成の変更によって、システムのナビゲーションを許可したり、エンドユーザーがGoogle DPC経由でデバイスにプッシュされた他のアプリを使用できるようにしたりできます。

COSU構成は指定された優先度で決まります。Googleにポリシー構成をプッシュする場合は、最も優先度の高い構成が使用されます。COSU構成は所定のスペース内のデバイスに適用されます。デフォルトスペースに定義されていれば、他のスペースに委譲される場合もあります。

構成するには:

1. **[構成] > [+追加]**を開きます。
2. **[ロックダウン& キオスク: Android Enterprise]**で**[専用デバイス(会社所有シングルユース: COSU)]**をクリックします。
3. 構成の名前を入力します。
4. 説明を入力します。

5. 各タブのクリックにより、以下の項目を設定できます。

   - **アプリ設定**
   - **一般的なロックダウン**
   - **キオスクのカスタマイズ**
   - **システム設定**

   構成可能なフィールドの詳細は以下の表のとおりです:

設定	説明
アプリ設定	
アプリ名	デバイスにピン留めするアプリを選択します。アプリ名の最初の数文字を入力し、選びたいアプリがドロップダウンリストに表示されたら選択します。必要なアプリがドロップダウンリストに表示されない場合は、そのアプリがPlayストアで市販/プライベートアプリとして提供され、アプリカタログに追加されていることを確認します。 このフィールドは必須です。このフィールドに追加するアプリを選択しない場合、構成を作成することはできません。追加できるのは市販アプリとプライベートアプリのみです。自社開発アプリとWebアプリ(プライベート)は追加できません。
一般的なロックダウン	
ディスプレイ常時オン	デバイスをオンにするバッテリープラグインモードを構成します。以下のいずれかを選択します。 - **AC** - AC充電器を電源とします。 - **ワイヤレス** - **USB** - USBポートを電源とします。

設定	説明
	• **任意** - AC充電器、USBポート0と、ワイヤレス充電器のいずれかを電源とします。
キオスクのカスタマイズ	
ステータスバーのカスタマイズ	以下のいずれかのオプションを選択し、対象デバイスのステータスバーをカスタマイズします。 • **[通知とシステム情報を有効化]** - システム情報と通知をステータスバーに表示します。 • **[システム情報のみ有効化]** - システム情報のみステータスバーに表示します。
システムナビゲーションのカスタマイズ	以下のいずれかのオプションを選択し、キオスクモードのナビゲーション機能(ホーム、概要ボタン)へのアクセスを指定します。 • **[有効化]** - ホームボタンと概要ボタンによるナビゲーションを有効化します。このオプションを選択した場合、ユーザーは所定のアプリを離れることができます。 • **[無効化]** - ホームボタンと概要ボタンによるナビゲーションを無効化します。 • ***のみ*** - ホームボタン ナビゲーションのみを有効化します。 すべてのオプションで [戻る] ボタンは使用可能です。
グローバルアクションを有効化	キオスクモードでグローバルアクションを有効化する場合に選択します。電源ボタンによる再起動およびシャットダウン機能はこのオプションで制御します。

設定	説明
システムエラーダイアログを有効化	キオスクモードでアプリのクラッシュまたは応答停止のエラーダイアログを有効化する場合に選択します。
システム設定	

システム更新設定	システム更新を管理するには以下の項目を設定します:
	• **[システム更新]** - 必要なシステム更新の種類を選択します。
	  • **自動** - 更新が利用可能になるとすぐに自動的にインストールします。
	  • **[延期]** - 最大30日間、自動インストールを延期します。
	  • **[時間枠]** - 毎日のメンテナンス時間枠内に自動的にインストールします。メンテナンスの開始時間と終了時間を設定してください。
	   デバイスにインストールされる更新は、サポートする機能群、Androidのバージョン、デバイスにインストールされているGoogleのDPCバージョンによって異なる場合があります。
	• **[フリーズ期間]** - デバイスがフリーズ期間にある場合、配布されるシステム更新はすべてブロックされ、インストールされません。**[フリーズ期間の追加]** をクリックし、フリーズ期間の **[開始日]** と **[終了日]** を設定してください。

設定	説明
	デバイスがフリーズ期間外になると、通常の更新動作が適用されます。終了日が開始日の前にある場合、フリーズ期間はその年から翌年まで延長されます。 フリーズ期間は最大90日に設定できます。フリーズ期間と次のフリーズ期間の間は少なくとも60日間空けます。

6. **[次へ]** をクリックします。
7. 以下の配布オプションから1つ選択します。
   - **すべてのデバイス**
   - **デバイスなし**(デフォルト)
   - **カスタム**
8. **[完了]** をクリックします。

AMAPIデバイス上のアプリ管理

COSU構成がデバイスに配布されると、AMAデバイスにアプリがプッシュされ、画面にピン留めされます。プッシュされたCOSU構成に関係なく、AMAデバイスにインストールされたアプリは管理可能です。以下はそのようなデバイス上のアプリ管理の詳細です。

- 市販アプリ、プライベートアプリのみサポートされます。自社開発アプリやWebクリップはサポートされません。
- インストール設定で[デバイスにインストール]または[サイレントインストール]が有効になっている場合のみアプリがプッシュされます。それらが有効化されないままユーザー/デバイスに割り当てられているアプリはデバイス上またはデバイスのPlayストアに表示されず、ユーザーが操作することはできません。
- サポートされるアプリ構成はマネージドGoogle Playおよび仕事用マネージドデバイス(Android for Work)設定です。OEMConfigアプリ用のマネージド構成への対応も含め、アプリ用のマネージド構成がサポートされています。

> 構成のインストールおよびアンインストールの完了時刻は、必要なアクションが実行されたかどうかに関するGoogleからの通知(メッセージングサービス)によって異なる場合があります。

- Go appはデフォルトでAMAデバイス登録の一部としてインストールされます。アプリは、登録プロセス中は画面にピン留めされ、セットアップが完了するとバックグラウンドで実行されます。

> メーカー、OSバージョン、セキュリティパッチレベルに基づくデバイス登録要求強制以外のポリシーはサポートされません。許可リストに入れられたデバイスのみがIvanti Neurons for MDMへの登録を許可される、デバイス許可リスト化がサポートされています。

AMAPIデバイス上でのアプリフィードバックサポートの管理

AMAPI(COSU)デバイス上ではアプリフィードバックへの対応を管理できます。デバイスがAMAPI(COSU)モードで登録されると、マネージドアプリ構成がGoogleからIvanti Neurons for MDMに直接、Go appの介入なしてプッシュされます。マネージドアプリフィードバックの情報は、デバイスレベルでは **[デバイス詳細] > [インストール済みアプリ] > [フィードバックを表示]** で確認できるほか、個々のアプリレベルでは、アプリカタログの[アプリ構成フィードバック]タブで特定のAndroidアプリに移動して、すべてのデバイスにわたる総合的なレポートで確認できます。アプリフィードバックのメカニズムについては、「アプリフィードバックの同期とフェッチ」ページ276を参照してください。

AMAPIの制限

現在、AMAPIには次の制限があります。

- 専用デバイス(COSUモード)のみサポートされます。

対応する構成

AMAPIでは、以下の構成がサポートされています。

- アプリ配布(単一または複数のアプリ)
- デバイスにプッシュされるアプリのマネージドアプリ構成
- Wi-Fi構成
- Android Enterpriseロックダウン専用(COSU)構成
- Always On VPN構成

Google Apps API

シングルサインオン(SSO) を利用してGoogle Appsサービスへのユーザーアクセスを認証しているGoogleのお客様は、デバイスがSSOにトリガーされる外部認証サービスへのリダイレクトを行わないよう定めるプロトコルの制約により、Exchangeを使用してメール、連絡先、カレンダーにアクセスできない場合があります。このサービスは、ActiveSync接続用のアカウントパスワードを作成し、管理することにより、この状態に対処します。

前提条件

Google Apps API機能を構成するには、以下の項目が必要です。

- https://console.developers.google.com/上のアカウントへの管理者アクセス
- https://admin.google.com上のアカウントへの管理者アクセス

Google Apps API機能の有効化

手順

1. **[管理]** > **[Google]** > **[Google Apps API]** を選択します。
2. 左側に1と書かれた長方形の一番下にある **[ステップ1：Google Dev]** をクリックします。

   [ステップ1：Google Dev] ページが表示されます。
3. [ステップ1：Google Dev] ページに表示される指示に従ったあとで、**[完了]** をクリックします。
4. 2と書かれた中央の長方形の一番下にある **[ステップ2：Google管理]** をクリックします。

   [ステップ2：Google管理] ページが表示されます。
5. [ステップ2：Google管理] ページに表示される指示に従ったあとで、**[完了]** をクリックします。
6. 右側に3と書かれた長方形にある **[Google管理ユーザー名を入力]** にGoogle管理ユーザー名を入力します。
7. 同じ長方形の中で、**[ファイルを選択]** をクリックし、ステップ1でダウンロードしたJSONファイルをアップロードします。
8. **[保存]** をクリックします。

[Google Apps API] ページが表示されない場合、必要な権限を持っていない可能性があります。以下のいずれかの役割が必要です。

- システム管理
- システム読み取り専用

[管理] - [Android Enterprise]

ライセンス: Silver

- Android Enterprise 対応の Ivanti, Inc 生産性アプリ (Email+、Docs@Work、Web@Work など) は Gold ライセンスが必要です。
- Tunnel for Android Enterprise には Platinum ライセンスが必要です。

Android Enterprise では、Android Enterprise アプリの使用と構成が可能です。Android Enterprise ユーザは、アプリカタログと Google Play からアプリを表示してインストールできます。

新しいお客様の場合は、アプリ配布がデフォルトで「デバイス単位」に設定されています。この設定は変更できません。アップグレードのお客様の場合は、アプリ配布を「ユーザー単位」と「デバイス単位」からお選びいただけます。デフォルトの選択は「ユーザー単位」です。多くのユーザーは複数のデバイスを持っています。ユーザーが複数のデバイスを持っている場合、アプリ配布を「デバイス単位」にすると、各デバイスに異なるアプリ群を配布できます。

このセクションは以下のトピックを含みます。

- 「Android Enterpriseの構成」下
- 「Android Enterprise仕事用プロファイルの構成」次のページ

Android Enterpriseの構成

1. Ivanti Neurons for MDM ポータルで、**[管理] > [Google] > [Android Enterprise]** をクリックします。
2. 以下のオプションから1つ選択してください。
   - **マネージド Google Play アカウント:** G Suite を利用していない企業の場合、ユーザは個人情報 (Google の電子メールアドレス) を送信せずに、Android Enterprise に登録できます。Ivanti Neurons for MDM はGoogleで自動的にユーザーをプロビジョニングし、管理します。管理者は、管理者用 GoogleアカウントでAndroidエンタープライズを許可するよう求められます。
   - **マネージド Google アカウント:** G Suite を利用している企業の場合、ユーザは Android Enterprise に登録できます。各ユーザは、Android Enterprise を登録するために Google アカウントが必要です。
3. 画面上の指示に従い、構成プロセスを完了します。

   自動方式では以下のようになります。

- UEM APIを有効化し、企業認証情報を作成します。
- 統合の所有者を許可することでGoogleに登録します。これは個人アカウントではなくIT部門のアカウントにしてください。
- サービスアカウント(JSONクライアントID)をドラッグ&ドロップし、認証情報を設定します。

4. オルタネート方式では以下のようになります。
   - 以下のセクションのクライアント IDを参照し、Google 管理に追加します。
   - Google 管理の MDM トークンと、Google Cloud コンソールのサービス アカウントを検索します。
   - Ivanti Neurons for MDM で、MDM トークン、エンタープライズ Google ドメイン、企業管理者の電子メールアドレスを入力し、Google サービスに接続します。
   - Ivanti Neurons for MDM で、サービス アカウント JSON クライアント ID をドラッグアンドドロップします。
   - Ivanti Neurons for MDM で **[認可]** をクリックし、Ivanti Neurons for MDM で Google ユーザを表示、管理することを許可します。

Ivanti Neurons for MDM ユーザーインターフェイスガイドに従って以下の手順を実行します。

Ivanti Neurons for MDM を管理された Google アカウントとバインドするためのクライアント ID

管理コンソールで、クライアント ID「**140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com**」を追加し、Ivanti Neurons for MDM テナントと管理された Google アカウントをバインドします。

Android Enterprise仕事用プロファイルの構成

1. Ivanti Neurons for MDM ポータルで **[構成]** に移動します。
2. **[+追加]** をクリックします。
3. **[ロックダウン& キオスク: Android Enterprise]** 構成を選択します。
4. 構成名と説明を入力します。
5. ロックダウンの種類の **[仕事用プロファイル]** をクリックします。

   対象デバイスに適用したいロックダウン設定を選択します。

重要: ユーザーが [設定] の [アカウント追加] からGoogleアカウントを追加する場合、Google認証サーバーは、アカウントのドメインがUEM管理ドメインとして登録されているかどうかを確認します。**[Androidデバイスに UEMポリシーを適用]** にチェックが入っていることを確認してください。入っている場合、Goクライアントが自動的にインストールまたは更新 (まだデバイスにインストールされていない場合) され、起動します。ユーザーが登録プロセスを終了すると、仕事用プロファイルを作成するよう指示が表示され、Google アカウントが自動的に仕事用プロファイルに移行します。

ChromeOSデバイスの操作

このセクションは以下のトピックを含みます。

- 「ChromeOSとIvanti Neurons for MDM」下
- 「ChromeOSデバイスへのAndroidアプリの配布」次のページ
- 「ChromeOSブループリント構成」ページ1281
- 「デバイスアクション」ページ1282
- 「FAQ」ページ1283
- 「評価の際の推奨手順」ページ1285

ChromeOSとIvanti Neurons for MDM

ChromeOSは、Googleが作成して提供している、Linuxベースのオペレーティングシステムです。Ivanti Neurons for MDM は、Android、Windows、iOS、macOSで動作しているデバイスをサポートしています。このサポートが ChromeOSデバイスにも拡張されました。Ivanti Neurons for MDM により、ChromeOSデバイスを構成、管理するための、統一されたシンプルなモビリティ管理ソリューションが提供されます。Ivantiでは、Ivanti Neurons for MDMでiOS、Android、Windows、Mac向けに提供されている管理ワークフローに類似した、ChromeOSデバイス向けの統一された、シンプルな、豊富な機能を備えたソリューションを提供しています。管理者は、**[管理] > [Google] > [ChromeOS管理]** にある簡易統合を使用することで、簡単にIvanti Neurons for MDMをGoogle Cloud(Google管理コンソールとも呼ばれます) と接続できます。

前提条件

1. 管理対象のGoogle管理者アカウントがあることが必要です。
2. LDAPユーザーとOUを、Google管理コンソールでインポートする必要があります。Ivanti Neurons for MDM は、LDAPソースからインポートされたOUのみをサポートしています。ローカルのOUはサポートされていません。
3. 管理者は、組織ユニット(ユーザーグループ) をIvanti Neurons for MDMと同期させておく必要があります。これは、LDAPサーバーを構成し、組織ユニットを追加することによって行えます。

Googleの許可

Google管理コンソールで選択可能なChromeOSデバイスを、Ivanti Neurons for MDMで直接登録することはできません。代わりに、これらのデバイスを、Googleに登録し、これらのデバイスに関する情報をGoogleとIvanti Neurons for MDMの間で同期させます。Googleがデバイスをインポートし、その他のアクション(アプリや構成の割り当てなど) を実行することを、管理者が許可しなければなりません。

手順

1. **[管理]** > **[Google]** > **[ChromeOS管理]** に進みます。
2. **[Googleを許可]** をクリックします。
3. 許可するGoogle管理アカウントを選択します。
4. **[続行]** をクリックして、必要なサービスを提供する権限を承諾します。

   [ChromeOSの設定に成功しました] という確認のメッセージが、画面に表示されます。確認メッセージの下には、ドメイン情報も記載されています。

GoogleからのChromeOSデバイスの同期

管理者は、Google管理コンソールからChromeOSデバイスを同期させる必要があります。Google管理コンソールを使用してChromeOSデバイスに初めてアクセスする際、管理者は、[ChromeOS管理] ページにある [今すぐ同期] オプションを使用して手動でデバイスを同期させる必要があります。

初めてデバイスを手動で同期させた後、それ以降の同期は、1時間ごとに自動的に行われます。

ChromeOSデバイスへのAndroidアプリの配布

管理者は、アプリカタログ内のAndroidアプリをChromeOSデバイスに配布できます。

前提条件

1. Android Enterpriseが構成されている必要があります。Android Enterpriseの設定については、「Android Enterprise の設定」ページ486を参照してください。
2. Androidアプリがアプリカタログ内に存在している必要があります。
3. AndroidアプリやChromeOSブループリント構成を配布する前に、当該ChromeOSデバイス(Chromebook)ユーザーがユーザーグループ(組織ユニットとも呼ばれます)の一員であることを確認してください。

Androidアプリが識別された場合は、他のアプリを配布するときに従うプロセスと同様のプロセスに従って、そのアプリを配布する必要があります。Androidアプリを配布する際は、必ず、アプリの配布先となるユーザーグループを選択し、デバイス上でサイレントインストールを実行してください。

既存のAndroidアプリ配布が、デバイス/デバイスグループまたはユーザーに配布されるように設定されている場合は、ユーザーグループに基づいた配布になるように変更する必要があります。これは、そのアプリがすでに使用中の場合、既存の配布に影響する可能性があります。設定変更は、まずは完全に新規のアプリに関して行うことをお勧めします。

[インストール設定]により管理者は、最終的なサイレントインストールを制御できます。この設定は、アプリをChromeOSデバイスにプッシュするために必要です。ここでは、ユーザーグループを選択する必要があります。

ChromeOSブループリント構成

ChromeOSブループリント構成には以下の設定があります。

- デバイス設定
- ユーザー設定とブラウザ設定
- マネージドゲストセッション設定

ChromeOS構成を特定のユーザーグループ(組織ユニットとも呼ばれます)に適用できます。ChromeOSブループリント構成を配布しようとすると、[ユーザーグループ]セクションのみが利用可能になり、許可されたGoogle管理コンソールにも関連付けられているLDAPユーザーグループがすべて、このセクションにリストされます。リストされたグループから1つ以上を選択して、構成を適用できます。

手順

1. **[構成]** > **[追加]** を開きます。
2. OSセクションで **[Google ChromeOS]** を選択します。画面に **[ChromeOSブループリント構成]** タブが表示されます。
3. **[ChromeOSブループリント]** をクリックします。画面に **[ChromeOSブループリント構成の作成]** ページが表示されます。
4. **[名前]** ボックスに構成の名前を入力します。
5. [構成設定] で、必要に応じてデバイス設定、ユーザー設定とブラウザ設定、マネージドゲストセッション設定を変更し、[デバイスにプッシュ] ボタンをオンに切り替えることで、変更済みの設定を適用できます。
6. **[次へ]** をクリックします。
7. 配布オプションの **[カスタム]** を選択します。

   構成の配布先として選択できるのは、LDAPユーザーグループのみです。

   構成を全員に配布する場合、これは、Ivanti Neurons for MDMおよびGoogle管理コンソールで選択可能なLDAPユーザーグループに対してのみ行えます。

8. 1つ以上のグループを選択し、**[完了]** をクリックします。

配布済みの設定の配布を取り消した場合、適用済みの設定は元には戻りません。

デバイスアクション

ChromeOSデバイスでは、次のアクションがサポートされています。

- **ワイプ** - 「ワイプ」アクションは、デバイスからすべてのデータを削除します。デバイスは、工場出荷時の設定にリセットされます。詳細については、「デバイスのワイプ」 ページ264を参照してください。
- **ロック** - 「ロック」アクションは、ユーザーがそれ以上のアクションをそのデバイスで実行できないようにします。詳細については、「デバイスのロック」 ページ257を参照してください。
- **ロック解除** - 「ロック解除」アクションは、デバイスのロックを解除して、使用できるようにします。詳細については、「デバイスのロック解除」 ページ267を参照してください。

FAQ

このセクションでは、Ivanti Neurons for MDMでChromeOSデバイスを使用するお客様から寄せられる一般的なFAQをいくつか示します。

- Chromebookの管理は、他のOSとどのような違いがありますか?

  Googleは現在、LDAPユーザーグループベースの構成配布のみを許可しており、管理者は構成やアプリを扱う際に、配布がLDAPユーザーグループに基づいて行われるようにする必要があります。ローカルユーザーグループとデバイスグループは、ChromeOSデバイスの管理ではサポートされていません。

- ChromeOSデバイスを管理するにあたり、Ivantiとはどのようなライセンス契約が必要ですか?

  ChromeOSデバイスには、Chrome Enterprise UpgradeやChrome Education Upgradeなどのライセンスが必要です。これらのライセンスは、ハードウェアライセンスの一部として、またはスタンドアロンライセンスとして、販売代理店から購入できます。詳細については、Googleのドキュメントを参照してください。Chromeデバイス管理を開始するためには、IvantiとのSecure UEM(統合エンドポイント管理)ライセンス契約が必要です。

- Mobile Threat Defense(MTD)、または同様のソリューションを利用できますか? MTDには別のライセンスが必要ですか?

  現在、本製品では利用できません。現在の制限事項を参照してください。今後、機能変更があった場合、詳細についてはFAQやリリース発表資料を通じてお知らせしてまいります。

- なぜ構成とアプリのタブには、他のデバイスの場合のようには詳細が表示されないのですか?

  構成は、ユーザーグループに対して配布されるのであり、ログインしたユーザーに基づいて適用されるわけではないため、現在のところ、構成はデバイスの詳細には表示されません。アプリも同じ配布ロジックに従っているため、同じ制限が課せられます。今後、これらの制限に変更があった場合、詳細についてはFAQやリリース発表資料を通じてお知らせしてまいります。

- ChromeOSの場合、現在サポートされている構成はいくつありますか?

  ChromeOSについては、利用可能な構成タイルの数を減らし、構成に関連する管理タスクの数を削減しています。この構成のことを、「ChromeOSブループリント」と呼んでいます。ChromeOSブループリントでは、ChromeOSデバイス上の700種類近くの構成をサポートしています。構成オプションについては、Googleのドキュメントを参照してください。

- すべてのデバイスに対して1つの構成を管理するのは、どの程度容易ですか?

  管理者は既存の構成を複製し、(必要であれば)それぞれのユーザーグループ用に変更するだけです。ゼロから始める必要はありません。

- ChromeデバイスにVPN構成を追加するには、どうすればいいですか?

  ネイティブVPNを使用するのではなく、Androidアプリを使用して行えます。

- 撤去やワイプなどのデバイスアクションはこれらのデバイスで機能しますか?

  企業内にあるChromebookは常に組織によって管理され、そのようなデバイス上のデータは完全に組織的なものとみなされます。この点を考慮すると、次のようになります。

  - 撤去はブロックされる
  - ワイプは許可される
  - ロックは許可される
  - ロック解除は許可される
  - 他のアクションはサポートされない

- ハードウェアという観点でIvantiでサポートしているChromebookはどれですか?

  Google Cloudデバイス管理ソリューションでサポートされているデバイスは、本質的にIvantiでもサポートされることが予期されます。Ivantiでは現在、Ivantiのソリューションでサポートされている特定のハードウェアのリストは公開していません。

- どのバージョンのChrome OSがサポートされていますか?

  Google Cloudでは、最新の安定したChromeOSバージョンのみをサポートしており、Ivantiのサポートも、バックグラウンド統合という性質により、Googleがサポートしているモデルに準じています。

- この機能を導入するのはまったく初めてなので、現在の制限事項を一覧で示してもらえますか?

新たなChrome OSのサポートに伴ない、当社ではお客様が熱望している機能の提供にむけて、現在懸命に取り組んでいます。管理者が注意すべき制限事項をいくつか以下に示します。

- Chrome OS拡張(ブラウザーアプリ)は、現在のところ配布用には(「アプリ」としては)サポートされていません。
- Androidアプリ用のマネージドアプリ構成は、現在のところサポートされていません。
- Wi-Fi構成APIが最近リリースされましたが、現在のところはサポートされていません。
- 証明書配布は、現在のところサポートされていません。

- Ivanti Go(旧称MobileIron Go) のAndroidアプリの配布は、現在のところサポートされていません。
- Ivanti Tunnel(VPN) アプリは、現在のところサポートされていません。
- 領域および領域委任は、現在のところサポートされていません。
- Mobile Threat Defenseソリューションは、現在のところサポートされていません。
- Ivantiの「ゼロサインオン」ソリューションは、これらのデバイスでサポートされ、管理対象外デバイスとして分類されます。
- ポリシーアクションは完全にはサポートされていません。

評価の際の推奨手順

ソリューションを検証するには、以下の手順をお勧めします。

1. ディレクトリソース(例：Active Directory) 内のユーザーを1人、テストユーザーとして含んだ、別のOU(ユーザーグループ) を作成します。こうすることで、アクティブな組織ユニットへの影響を防止できます。
2. Ivanti、Google、およびディレクトリソース(LDAP) 間でユーザーを同期させます。ユーザーグループとして「test OU」があることを確認します。
3. 上記手順で強調されているようにIvanti Neurons for MDMをGoogleと統合します。
4. ChromeOSブループリント構成を作成し、これを「test OU」ユーザーグループのみに配布します。
5. Chromebook(設定済みまたは事前登録済み) を起動します。[デバイス] リストに表示されていることを確認します。
6. このデバイスでChromeOSブループリント設定が利用可能であることを確認します。
7. Androidアプリ配布についても同様の手順に従います。

ファームウェア管 理

このセクションは以 下 のトピックを含 みます。

- 「Zebra OTAサービスの登 録 」ページ1287
- 「Samsung E-FOTAライセンス管 理 (終 了) 」ページ1289

Zebra OTAサービスの登録

Zebra OTA(Over the Air) サービスに登録すると、Zebra OTA構成を有効にして、Ivanti Neurons for MDMに登録されたZebraデバイスのファームウェアの詳細を受信し、更新できるようになります。

手順

1. **[管理] > [Zebra OTA]** を開きます。**[Zebra OTAサービス]** ページが表示されます。
2. **[開始]** をクリックします。
3. Zebra OTAの認証情報を入力してログインし、手順に従ってZebraサービスの利用許可をリクエストします。
4. **[検証を完了]** をクリックすると、Zebraサービスへの連携の確認が得られます。連携が確認されると、[Zebra OTAサービス] ページに登録完了のステータスが表示されます。

登録を取り消すには、**[アクション]** カラムの **[取り消し]** をクリックします。アクションの取り消しにより、すべてのZebra OTA構成が既存の構成から削除されます。Zebra OTAに再エンロールするには、**[再読み込み]** をクリックします。アクションの再読み込みは既存の構成に影響を与えません。

登録すると、Goクライアントが受信し、デバイス所有者モードでZebraデバイス(Androidバージョン8.0またはサポートされる以降のバージョンを搭載) に適用するZebraファームウェア構成を有効化できます。構成が適用されると、構成のスケジュールに従ってファームウェアがダウンロードされ、デバイスにインストールされます。Zebraファームウェア構成の有効化については、システム更新の構成を参照してください。

ファームウェア更新が完了すると、Zebraデバイスの [デバイス] ページの **[システム更新]** カラムでファームウェア更新ステータスを確認できます。ステータスの種類は以下のとおりです。

- **不明** - クライアントまたはOSに対応していません。
- **最新** - デバイスの更新は最新の状態です。
- **保留中** - システム更新構成は適用されていますが、更新がダウンロードまたは適用されていません。
- **ダウンロード中** - システム更新をクライアントにダウンロード中です。
- **利用可能** - デバイスのシステム更新が提供されています。
- **エラー** - ダウンロードまたはインストールにエラーが発生しました。

[デバイス] ページの **[Zebraパッチバージョン]** カラムには、デバイスのZebraのパッチ情報が表示されます。

Android 11以降のデバイスでは、**[Zebraパッチバージョン]** はサポートされていません。**[Zebraフルアップグレード]** のみサポートされています。

Samsung E-FOTAライセンス管理(終了)

Samsung E-FOTAサービスは、2022年7月に終了します。詳細については、Samsungの発表をご参照ください。

今後、Samsung E-FOTAサービスを構成することはできません。ただし、既存のE-FOTA構成をお持ちの場合、**[管理]** > **[ファームウェア管理]** > **[Samsung E-FOTA]** に移動し、**[無効化]** オプションをクリックすることで、構成を無効化できます。

スクリプトの管理

管理者は、構成に使用したり、デバイスにプッシュしたりするスクリプトを管理できます。

このセクションは以下のトピックを含みます。

「すべてのスクリプト」ページ1291

すべてのスクリプト

対象：macOSデバイス

Ivanti Neurons for MDMでは、システム管理者の役割を持つユーザーが、**[管理] > [すべてのスクリプト]** ページから、構成に使用したりデバイスに配布したりするスクリプトの作成、アップロード、管理を実行できます。カスタム属性をスクリプトに関連付け、結果の値を構成済みのデバイスに割り当てることも可能です。スクリプト変更のログと実行結果を見るには、監査証跡を使用します。

スクリプトの記述により、デバイスの任意の設定を構成することができます。たとえば以下のようなスクリプトも実行できます。

- デバイスユーザーに月1回のパスワード変更を強制する。
- アイドル時間が5分になると画面をロックする。
- セキュリティ付きのWi-Fiネットワークを設定する。

このセクションは以下のトピックを含みます。

スクリプトの追加

bashスクリプトのリポジトリを作成またはアップロードできます。Mobile@Work for macOS Scriptなど、このリポジトリを構成に使用すれば、スクリプトを選択してデバイスに配布し、構成内に指定したスケジュールに応じて実行させることが可能です。

たとえば、シェルスクリプトを作成してデバイス上で実行させます。必要であれば、ラッパーも使用可能です。シェルスクリプト内からのバイナリファイル実行はサポートされません。

Ivantiは、シェルスクリプトをデバイスで実行する前にテストし、安定性やクオリティを確認することを強く推奨します。ローカルでスクリプトを実行し、エラーが発生すれば修正してください。

手順

1. **[管理] > [すべてのスクリプト]** を開きます。
2. **[+追加]** をクリックします。
3. スクリプトの名前と説明を入力します。
4. 次の**スクリプトタイプ**から1つを選択します。
   - **bash**
   - **zsh**
   - **python**
   - **swift**
5. **[ルートとして実行]** チェックボックスを選択し、デバイス上でスクリプトをルートとして実行します。デフォルトではオフです。
6. **スクリプトエディタ**では、スクリプトをテキストボックスに入力、ドラッグ＆ドロップ、コピー＆ペーストできます。
7. **[スクリプトからコードをインポート]** をクリックして既存のスクリプトファイルをドラッグ＆ドロップするか、[ファイルを選択] をクリックしてブラウズし、Ivanti Neurons for MDMにアップロードするスクリプトファイルを選択してもかまいません。これにより、スクリプトエディタ内の既存のスクリプトが上書きされます。このアクションは元に戻せません。**[インポート]** をクリックします。アップロードしたスクリプトのコードがエディタに表示されます。
8. (任意) **[利用可能なカスタム属性]** セクションで、表示されている1つ以上のデバイスカスタム属性を選び、スクリプトに関連付けます。これは、スクリプト実行結果の値を構成済みデバイスのデバイスカスタム属性に割り当てるために使用されます。スクリプト内のカスタム属性を使用したサンプルコードを見るには、**[カスタム属性用のサンプルコード]** をクリックしてください。
9. **[保存]** をクリックします。

スクリプト内のカスタム属性名は必ず小文字です。スクリプト内でカスタム属性が参照されている場合、その属性は削除できません。カスタム属性(名前など)を変更し、それがスクリプトに関連付けられている場合は、そのスクリプトにも対応の変更を加える必要があります。

スクリプトの変更

スクリプトを編集または削除するには:

1. **[管理] > [すべてのスクリプト]** を開きます。
2. スクリプトの **[アクション]** カラムで、編集または削除に対応するアイコンをクリックします。
3. 画面上の指示に従い、アクションを完了させます。

スクリプト(内容、名前、説明)が変更された場合、スクリプトに関連付けられたすべての構成がデバイスに再配布されます。

スクリプト変数の使用

環境変数や置換変数などのスクリプト入力を定義し、スクリプトリポジトリに保存します。macOS対応Mobile@Workスクリプト構成では、どのスクリプトがリンクされているかにより、必要に応じて関連スクリプト変数が使えるようになります。この機能には、macOS対応Mobile@Work 1.71.0以降、Ivanti Neurons for MDMがサポートする最新リリース版までが必要です。

変数を使用してスクリプトを実行し、実行のたびに異なる値を使用してください。たとえば管理者は、${userEmailAddress}環境変数をスクリプト変数として使用するスクリプトを作成し、macOS対応Mobile@Workスクリプト構成と関連付けることができます。構成が配布され、各ユーザーデバイスにインストールされた後、Ivanti Neurons for MDMが異なる登録済みユーザーメールアドレスを各デバイスに送信し、所定のアクションを実行させます。Ivanti Neurons for MDM 管理者ポータルでは、カスタム変数がサポートされます。

スクリプト変数を追加するには:

1. **[管理] > [すべてのスクリプト]** を開きます。
2. [スクリプト入力] セクションで **[+追加]** をクリックします。
3. [スクリプト入力を追加 - 環境変数] ポップアップページで以下の情報を入力します。
   - 表示するラベル - このテキストは、macOS対応Mobile@Workスクリプト構成ページのラベルとして表示されます。「OSフォルダーを入力」、「Apache番号を入力」など。
   - 環境変数名 - JAVA_HOME、OS_VERSIONなど。Ivanti Neurons for MDM は、構成の詳細を対象デバイスに送信すると同時に、データベース内で持続的に使用されるスクリプト変数の値を置換します。
   - 環境変数のデフォルト値 - 1024、bin/java、${PhoneNumber}など。入力変数は、管理者によってアップロードまたは編集されたスクリプトに使用されます。以下の注もお読みください。
4. [プレビュー領域] では、環境変数が構成ページにおいてスクリプト入力としてどのように表示されるかを確認できます。
5. **[保存]** をクリックします。

これにより、環境変数ではなく、ラベルとデフォルト値だけが構成に公開され、抽象化の層ができます。

- 英数字(1024、bin/java、root@localhostなど)やシステム属性(${userFirstName})は環境変数の値として使用できます。
- 環境変数の値は導入中に構成ページで変更や削除が可能です。
- 環境変数の値を提供していない場合は、スクリプト導入中に必ず提供するようにしてください。さもなければ、空値がスクリプトに渡されます。
- スクリプト構成が配布され、デバイスにインストールされた後で、[管理] > [すべてのスクリプト]ページで環境変数を編集しても、スクリプトと関連する既存の構成に影響はありません。macOS対応Mobile@Workスクリプト構成もご覧ください。

スクリプト変数の編集

スクリプト変数を変更するには、変数の編集(鉛筆)アイコンをクリックし、変更を保存してください。

スクリプト構成がスクリプト変数を持つスクリプトを参照している場合、既存のスクリプト変数のラベルを編集するとスクリプト構成にも反映されます。ただし、以下の点に注意してください。

- スクリプト変数のデフォルト値を変更しても既存の構成には反映されません。
- スクリプト変数のデフォルト値の変更は、前のスクリプトを使って作成した新しい構成にのみ反映されます。

スクリプト変数の削除

スクリプト変数を削除するには、変数の削除(マイナス)アイコンをクリックし、確定してください。

新しく作成したスクリプト変数、あるいは既存のスクリプト変数の削除は、既存の構成の中でも反映されます。

スクリプトのテスト

デバイス上でテストする前に、デバッグツールで簡単にスクリプトをテスト実行してください。必ずしもスクリプトを保存する必要はありません。この機能には、macOS対応Mobile@Work 1.67以降、Ivanti Neurons for MDMがサポートする最新リリース版までが必要です。

手順

1. **[管理] > [すべてのスクリプト]**を開きます。
2. スクリプトエディタでスクリプトを追加またはインポートします。
3. テナントに複数のスペースがある場合はスペースを選択します。

4. テストスクリプトのセクションでプラットフォームに **[macOS]** を選択します。
5. **[デバイスの検索]** テキストフィールドで、スクリプトをテストするデバイスを検索し、選択します。デバイスは、シリアル番号、ユーザー名、デバイス名、OSバージョンで検索できます。
6. **[今すぐテスト]** をクリックします。これにより環境変数を追加、編集、削除し、その状態のスクリプト(変更を保存しなくても)をテストできます。
7. スクリプトがデバイスにプッシュされ、実行されるのを待ちます。
8. スクリプト入力(環境変数の詳細を含む)、スクリプト出力、カスタム属性セクションで発行されたテスト結果を確認します。環境変数のデフォルト値も表示されます。

スクリプト実行結果の確認

スクリプト実行結果のログを表示するには:

1. **[デバイス]** を開きます。
2. デバイスの名前をクリックします。
3. **[ログ]** タブをクリックします。
4. スクリプト実行アクションを表示する行では、以下の情報を確認できます。
   - 詳細カラムでスクリプト名
   - ステータスカラムでスクリプト実行ステータス
   - 日付カラムでスクリプト実行の日付と時刻
   - アクションカラムで目のアイコンをクリックしてスクリプト実行ログ(デバイスログのplistファイル)
5. フィルターを使用して **[スクリプト実行]** 行を表示します。これらの行のログには、標準出力の出力(plist)とスクリプトの標準エラーが含まれます。
6. フィルターを使用して **[スクリプト実行結果処理中]** の行を表示します。これらの行のログには、結果の処理方法に関する詳細(plist)が含まれます。
   - スクリプトに関連付けられたカスタム属性がない場合は、処理する結果がありません。そのようなスクリプトはフィルター済みの行のリストに表示されません。

- スクリプトにカスタム属性が関連付けられていて、それらが然るべき形式であれば、結果のカスタム属性がマッピングされてステータスが成功と表示されます。マッピング済みのカスタム属性とその値は、**[属性]** タブで確認できます。
- スクリプトにカスタム属性が関連付けられていて、それらが期待どおりの形式でない場合、結果のカスタム属性はマッピングされず、ステータスはエラーと表示されます。
- 結果の形式が正しいにもかかわらず、関連付けられたカスタム属性すべてが結果に送信されない場合、ステータスはエラーと表示されます。
- スクリプト変数をスクリプトとともに送信すると、[スクリプト実行結果処理中] ログにスクリプト変数の詳細 (plist) が記録されます。

関連トピック:

- macOS対応Mobile@Workのスクリプト構成
- 構成を作成するには

ブランディング

このセクションは以 下 のトピックを含 みます。

[管理] > [Appleアプリカタログ(ブランディング)]

ライセンス: Gold

Apple**アプリカタログ**[1]をブランディングし、iPhone、iPad、Macのエンドユーザーにとって見慣れたデザインにすることができます。Appleアプリカタログ内の次の項目をカスタマイズできます。

- アプリアイコン(PNG、360ピクセル四方)
- アプリ名
- アプリバナー画像(PNG、360x64ピクセル)
- テキストの色

Apple App Catalogには、**スタンドアロンアプリカタログ**と**統合アプリカタログ**の2つのモードでアクセスできます。スタンドアロンアプリカタログはiPhone、iPad、Macデバイスで使用できます。統合アプリカタログを使用できるのは、iOSとMacデバイスのみです。

Appleアプリカタログのブランディング

このページでの変更は、ホーム画面、スプラッシュ画面、アプリのホーム画面に反映されます。手順はスタンドアロンアプリカタログでも統合アプリカタログでも同じです。

手順

1. **[Appleアプリカタログのブランディング]** ページで、**[カスタマイズ]**(右上)をクリックします。
2. **[アプリアイコン]** セクションで、ロゴファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。アプリアイコンはiOSホーム画面に表示されます。
3. **[アプリ名]** セクションで **[アプリカタログ名]** のテキストを編集すると、スプラッシュ画面に表示されるラベルを変更できます。

[1] a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

4. 名前とアイコンはホーム画面のバナーに適用されます。カスタムバナーの画像を変更するには、**[ホーム画面のバナーに名前とアイコンを適用]** の選択を解除します。**[アプリケーション バナー画像]** セクションが表示されます。

5. アプリバナー画像を変更するには、新しいバナー画像ファイルを点線で囲まれたボックスへドラッグアンドドロップするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。アプリバナー画像はアプリのホーム画面のトップバーに表示されます。

6. **[テキストの色]** セクションで16進数のカラーコードボックスをクリックして色を選択するか、16進数のカラーコードを入力してテキストとアイコンに指定します。これでスプラッシュ画面のテキスト、アプリ名、バナー、アクションボタンに適用されます。

7. **[変更の保存]** をクリックします。

入力したアプリカタログ名は、Android、iOS、macOSに適用されます。

Androidアプリカタログのブランディング

ライセンス: Gold

Android**アプリカタログ**[1]をブランディングし、エンドユーザーにとって見慣れたデザインにすることができます。Androidアプリカタログ内の次の項目をカスタマイズできます。

- カタログのロゴ(PNG、360x64)
- カタログ名
- アクションバーの色
- ショートカットアイコン
- ショートカット名

Androidアプリカタログのブランディング

手順

1. **[Androidアプリカタログのブランディング]** 画面で、**[カスタマイズ]**(右上) をクリックします。
2. アプリカタログのロゴを変更するには、ロゴファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。
3. **[アクションバーの色]** フィールドをクリックするとカラーパレットが表示されます。そこから色を選択するか、16進数の値で色を指定します。
4. **[アプリカタログ名]** のテキストを編集すると、カタログのラベルが変更されます。

   入力したアプリカタログ名は、Android、iOS、macOSに適用されます。
5. ショートカットアイコンを変更するには、アイコンファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。

[1]a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

6. **[ショートカット名]** のテキストを編集すると、アプリのショートカットのラベルが変更されます。
7. **[変更の保存]** をクリックします。

[管理] > [Androidキオスクのブランディング]

ライセンス: Silver

Androidキオスクのページをブランディングし、エンドユーザーにとって見慣れたデザインにすることができます。次の項目をカスタマイズできます。

- バナーのロゴ(PNG、840x114) またはテキスト
- バナーボーダーの色
- バナー背景の色
- 画面背景の色
- 画面背景の画像(1280x800)
- 画面背景の形式

Androidキオスク画面のブランディング

手順

1. **[管理]** > **[Androidキオスク]** を開きます。
2. **[キオスクモードのブランディング]** ページを開き、**[ブランディングを作成]** をクリックします。
3. **[名前]** フィールドにキオスクモードのブランディングの名前を入力します。
4. バナーをオフにしたい場合は、**[トップバナーを有効にする]** のチェックを外します。
5. **[バナー背景の色]** フィールドをクリックするとカラーパレットが表示されます。そこから色を選択するか、好きな色の16進数の値を入力します。
6. **[バナーボーダーの色]** フィールドをクリックするとカラーパレットが表示されます。そこから色を選択するか、好きな色の16進数の値を入力します。
7. **[画像/ロゴ]** または **[テキスト]** を選択し、バナーのコンテンツを設定します。
8. **[画像/ロゴ]** を選択した場合は、画像ファイルをドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。
9. **[テキスト]** を選択した場合は、バナーに表示させたいテキストを入力します。

10. **[背景]** タブをクリックします。

11. **[背景の色]** フィールドをクリックするとカラーパレットが表示されます。そこから色を選択するか、好きな色の16進数の値を入力します。

12. 背景画像を変更するには:

    a. 既定の画像を削除します。

    b. 希望の画像をドラッグ＆ドロップするか、**[ファイルを選択]** をクリックして画像を選択します。

    c. 優先レイアウトを選択します。

13. **[変更の保存]** をクリックします。
    作成したキオスクモードのブランディングは、**[キオスクモードのブランディング]** ページに表示されます。カスタマイズ済みのブランディングをさらに編集する場合は、**[アクション]** カラムの編集アイコンをクリックしてください。カスタマイズ済みのブランディングを削除するには、削除アイコンをクリックします。カスタマイズ済みのカスタムブランディングを削除すると、ブランディングを使用した構成はデフォルトのブランディングに戻ります。

メールテンプレートのブランディング

エンドユーザー招待メールをブランディングし、エンドユーザーにとって見慣れたデザインにすることができます。カスタマイズを元に戻すには **[デフォルト設定回復]** をクリックします。

サポートされる全言語で次のメールテンプレートをカスタマイズできます。

- **エンドユーザー招待** - デバイスを接続し、アプリや設定機能へアクセスできるよう招待します。
- **パスワードリセット通知** - ローカルアカウントのパスワード有効期限が切れる7日前と24時間前にシステムがリマインダーメールを送信します。LDAPアカウントには適用されません。
- **登録確認** - ユーザーが登録を完了した後に送信されるメール。ユーザーに登録の御礼を述べ、各種リソースの利用方法を伝えます。
- **ポリシーコンプライアンス通知** - デバイスがコンプライアンス違反になったときに送信されるメール。

このセクションは以下のトピックを含みます。

- 「メールテンプレートのプレビューとテスト」下
- 「メッセージヘッダーのカスタマイズ」次のページ
- 「メールテンプレートのカスタマイズ」次のページ
- 「サポートされるメール変数」ページ1311

メールテンプレートのプレビューとテスト

メールテンプレートのプレビューとテストを実行できます。テストでは、テンプレートを利用したメールを指定のアドレスに送信できます。

メールテンプレートのプレビューとテストを実行するには：

1. **[管理]** をクリックします。
2. [メールテンプレート] で、**[エンドユーザー招待]**、**[パスワードリセット通知]**、**[登録確認]**、**[ポリシーコンプライアンス通知]** のいずれかをクリックします。
3. プレビューとテストを実行したいメールテンプレートの **[プレビューとテスト]** リンクをクリックします。
4. テンプレート表示ペインでテンプレートを閲覧します。
5. テストメールを送信する宛先メールアドレスを指定します。

   指定したメールアドレスがテストを実行する本人である場合、メールのユーザー体験を正確に把握できるよう、テストメールはメールテンプレート変数のほとんどを置換します。ただし、Ivanti Neurons for MDM が実際の招待メールを生成するときに生成する変数の値は置換しません。
6. **[テストメールを送信]** をクリックします。

メッセージヘッダーのカスタマイズ

1. **[管理]** をクリックします。
2. **[メールテンプレート]** をクリックします。
3. 編集したいメールテンプレートに対応する **[編集]** アイコンリンク([アクション] 列) をクリックします。
4. 必要に応じて **[メール表示名]**、**[送信元メールアドレス]**、**[返信用メールアドレス]** を新しく設定してください。

   送信者または返信先メールアドレスをカスタマイズする際は、メールリレーサービスを許可リストに入れ、メールがSPAMフィルタリングサービスによってブロックされないようにすることを推奨します。詳細は、このドキュメントを参照してください。
5. **[保存]** をクリックします。
6. メールテンプレートのプレビューを確認し、**[保存]** をクリックします。

メールテンプレートのカスタマイズ

1. **[管理]** > **[ブランディング]** > **[メールテンプレート]** を選択します。
2. **[エンドユーザー招待]**、**[パスワードリセット通知]**、**[登録確認]**、**[ポリシーコンプライアンス通知]** のいずれかを編集するテンプレートに選択します。

3. カスタマイズしたいメールテンプレートの横にあるペン(編集)のアイコンをクリックします。

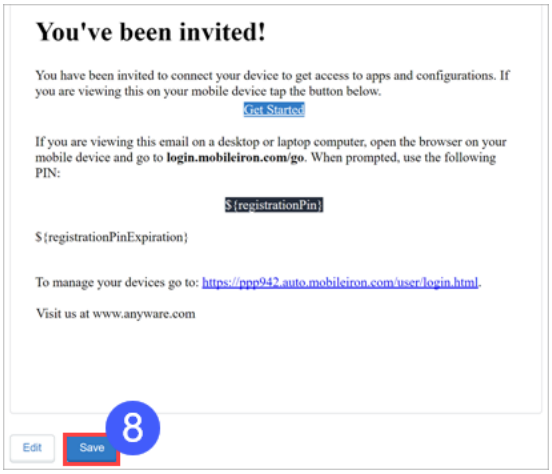
4. 必要に応じて件名を編集します。

5. HTML要素を含むメールテンプレートを本文ペインで編集し、メッセージの内容をカスタマイズします。

   i メール本文の右に表示される変数も使用できます。サポートされるメール変数をご覧ください。

6. **[プレビュー]** をクリックすると、作成中のメールテンプレートをプレビューできます。

7. テンプレートを保存する準備ができたら **[プレビュー]** をクリックします。これでプレビューが表示され、保存が可能となります。



8. プレビューに満足した場合は **[保存]** をクリックします。

カスタマイズされたユーザー招待の許可リスト化されたコンテンツとブロックリスト化されたコンテンツ

[エンドユーザー招待] でユーザー招待メールのテンプレートをカスタマイズする際には、一連の許可リスト化されたHTMLタグと属性を使用できます。また、クロスサイトスクリプティング(XSS)の脆弱性を防ぐために、ユーザー招待で使用できない、ブロックリスト化された文字列のリストもあります。

招待メールには、許可リスト化されたタグと属性のみを使用できます。使用できる許可リスト化されたタグと対応する属性を次の表に示します。

一部の許可リストのタグ(例: <big>)にはAllowlisted属性がないため、空白で表示されます。

許可リスト化されたタグ	許可リスト化された属性
<big>	[]
<img>	["id","label","editable","height","border","src","style","width", "align", "class","cellpadding","alt","title","data-max-width","data-default"]
	[]
<singleline>	["label"]
<tbody>	[]
<!DOCTYPE>	[]
<h1>	["style"]
<h2>	["style"]
<hr>	["noshade","style"]
<h3>	[]
<body>	["style", "class", "bgcolor", "paddingwidth", "paddingheight", "offset", "toppadding", "leftpadding", "lang","link","vlink","border","cellspacing","cellpadding"]
<title>	["id"]
<head>	[]

	["style","class","width","align","id"]
 	[]
<path>	["d"]
	["style"]
<html>	["xmlns","xmlns:mso","xmlns:msdt"]
	["start"]
<table>	["class","width","border","cellspacing","cellpadding","style","height","bgcolor", "align","background"]
<a>	["href","style","target","rel","class","title"]
<b>	[]
<o:p>	[]
<svg>	["xmlns","class","viewbox","width","height","role","aria-labelledby"]
	[]
	[]
<i>	[]
<label>	["style"]

<td>	["valign","width","height","class", "cellpadding", "cellspacing","border","bgcolor","align", "style","colspan","id"]
<p>	["style","class","align"]
<u>	[]
<meta>	["name","content","http-equiv","charset"]
<multiline>	["label"]
<style>	["type","id"]
	["style"]
<tr>	["style"]
	["style","class","lang"]
<font>	["color"]

以下は、カスタマイズされたユーザー招待において使用できないブロックリスト化された文字列のリストです。

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4- ,+ADw-/SCRIPT+AD4-, xml:base
- 特殊文字とjavascriptまたはスクリプトの検索
- 大文字と小文字を区別しない「url =」を含むメタコンテンツ属性
- .svgを含まないimg src
- 「\00」を含む属性値

上述のブロックリスト化された文字列のいずれかがエンドユーザー招待のHTMLコンテンツで使用されていると、**[プレビュー]** をクリックしたときにエラーメッセージが表示されます。このエラーメッセージには、エンドユーザー招待で使用できないHTMLコンテンツが一覧表示されます。使用できないHTMLコンテンツを編集、削除してから、**[プレビュー]** をクリックして先に進みます。

編集したテンプレートにブロックリスト化されたHTMLコンテンツが含まれている場合は、編集済みのテンプレートを保存できません。

サポートされるメール変数

Ivanti Neurons for MDM には、メールテンプレートのカスタマイズに使用できる複数の変数があります。

エンドユーザー招待変数

変数	説明
${userActivationUrl}	ユーザーアクティベーションURL - これは${email.idp.invitation.get.started}テキスト周囲のハイパーリンクです。
${clusterRegistrationUrl}	クラスター登録URL - これはデフォルトテンプレートにはありませんが、間接的に参照されます(${email.idp.invitation.pg4}変数経由で) 。
${productBrandName}	製品ブランド名 - 既定のテンプレートのヘッダーの <title> タグで定義されます。
${companyLogoUrl}	企業ロゴURL - これはデフォルトテンプレート内の画像であり、MobileIron CDN内の画像を参照しています。
${message:${email.idp.invitation.register.your.device}	ユーザーデバイス登録招待メールの件名。
${message:${email.idp.invitation.title}}	招待メールの件名。
${message:${email.idp.invitation.pg1}}	ユーザーがデバイスを使用していることの確認。
${message:${email.idp.invitation.get.started}}	招待メールの説明テキスト。
${message:${email.idp.invitation.pg2}}	ログインと登録の方法。
${message:${email.idp.invitation.pg3}}	デバイスにプッシュされるメールとアプリの情報。
${message:${email.idp.invitation.pg4}}	ユーザーがデバイスを使用していない場合の登録方法(クラスター登録URLを含む) 。
${message:${email.footer}}	企業Webサイトラベルを含む招待メールのフッター。
${companyWebsiteLabel}	企業Webサイトラベル - これはデフォルトテンプレートにはありませんが、間接的に参照されます(${email.footer}変数経由で) 。

パスワード有効期限通知変数

変数	説明
${passwordResetUrl}	パスワードリセットURL。
${productBrandName}	製品ブランド名 - 既定のテンプレートのヘッダーの <title> タグで定義されます。
${companyLogoUrl}	企業ロゴURL - これはデフォルトテンプレート内の画像であり、MobileIron CDN内の画像を参照しています。
${message:${password.expiration.notification.title}}	パスワード有効期限切れ通知のタイトル
${message:${password.expiration.notification.pg1}}	パスワード有効期限切れ通知の冒頭パラグラフ
${message:${email.password.reset.url.name}}	パスワードリセットURL名
${message:${email.footer}}	企業Webサイトラベルを含む招待メールのフッター。
${companyWebsiteLabel}	企業Webサイトラベル - これはデフォルトテンプレートにはありませんが、間接的に参照されます(${email.footer}変数経由で) 。

登録確認変数

変数	説明
${productBrandName}	製品ブランド名 - 既定のテンプレートのヘッダーの <title> タグで定義されます。
${companyLogoUrl}	企業ロゴURL - これはデフォルトテンプレート内の画像であり、MobileIron CDN内の画像を参照しています。
${message:${email.confirmation.title}}	登録確認メール件名。
${message:${email.confirmation.pg1}}	登録確認メール序文。

ポリシーコンプライアンス変数

変数	説明
${policyMessageTitle}	この変数は、ポリシー内でメール送信コンプライアンスアクションの件名に入力されているコンテンツに置換されます。
${policyMessageContent}	この変数は、ポリシー内でメール送信コンプライアンスアクションの本文に入力されているコンテンツに置換されます。
${productBrandName}	製品ブランド名 - 既定のテンプレートのヘッダーの <title> タグで定義されます。
${companyLogoUrl}	企業ロゴURL - これはデフォルトテンプレート内の画像であり、MobileIron CDN内の画像を参照しています。
${message:${email.footer}}	企業Webサイトラベルを含む招待メールのフッター。
${companyWebsiteLabel}	企業Webサイトラベル - これはデフォルトテンプレートにはありませんが、間接的に参照されます(${email.footer}変数経由で) 。

カスタムユーザー属性変数

管理者は、以下の条件下でカスタムユーザー属性をカスタマイズしたメールテンプレート内のメール変数として使用できます。

- カスタムユーザー属性が **[管理] > [属性]** ページにある。
- 管理者がカスタムユーザー属性をユーザーに割り当て、各ユーザーにカスタムユーザー属性の値を与えている。

セルフサービスポータル

登録の招待状にはセルフサービスポータルへのリンクが含まれます。エンドユーザーは、このポータルを利用して以下のタスクを実行できます。

- ロック
- ロックの解除
- 位置情報を表示(プライバシー構成で有効化されている場合)
- ワイプ
- 撤去
- アカウント情報の変更(名前、パスワード、Eメールアドレス)
- 強制チェックイン
- 暗号化証明書と署名証明書を追加

エンドユーザーは、セルフサービスポータルに表示されている登録ポータルリンクをクリックし、追加のデバイスを登録します。

エンドユーザーがセルフサービスポータルのURLを紛失した場合は、https://mydevices.mobileiron.com/user/login.htmlをエンドユーザーに送信してください。iOSユーザーの場合は、セルフサービスポータル用のWebクリップ構成の作成を検討します。

署名証明書と暗号化証明書のアップロード

セルフサービスポータルの[ユーザー提供の証明書]構成では、エンドユーザーにメールの署名証明書と暗号化証明書のアップロードを許可することができます。この設定は[ユーザー提供の証明書]構成で構成します。構成すると、エンドユーザーが署名証明書と暗号化証明書をアップロード可能となります。

1. **[マイ証明書]** タブで **[証明書を追加]** をクリックします。**[証明書を追加]** ウィンドウが表示されます。
2. 次のフィールドを更新します。

フィールド名	説明
証明書の種類	アップロードする証明書の種類を選択します。選択肢は次のとおりです。 • **暗号化証明書** • **署名証明書** これらのオプションはIvanti Neurons for MDM管理ポータルから作成します。詳細は、ID証明書構成をご覧ください。
アップロードする証明書	**[ファイルを選択]** をクリックし、アップロードする証明書を選択します。 ファイルがPKCS12形式であることを確認してください。
パスワード	ファイルに使用するパスワードを入力します。

3. **[アップロード]** をクリックします。

アップロードした後は、以下の詳細を示す表で証明書のリストを確認できます。

フィールド名	説明
証明書名	証明書の種類を **[暗号化]** または **[署名]** に指定します。
発行者：	発行された証明書の詳細。
アップロード日：	証明書がアップロードされた日付。
有効期限	証明書の有効期限。
アクション	以下のアクションを実行できます。 • **証明書の編集** - 証明書の詳細の編集。 • **プライベートキーをクリア** - 証明書パッケージ(PKCS#12) からプライベートキーを削除します。 • **証明書の削除** - Ivanti Neurons for MDMサーバーから証明書を削除します。

ユーザーが証明書の構成をアップロードすると、証明書を使用している構成をサーバーが再プッシュします。

ユーザーがプライベートキーを削除またはクリアした場合は、構成が再プッシュされません。

詳細はセルフサービスポータルブランディングを参照してください。

セルフサービスポータル(ブランディング)

ライセンス: Silver

組織のロゴのついたセルフサービスポータルをカスタマイズできます。ロゴを追加しない場合、セルフサービスポータルにはデフォルトのサービスロゴが表示されます。

セルフサービスポータルのブランディング

手順

1. [セルフサービスポータルのブランディング] 画面で、**[カスタマイズ]**(右上)をクリックします。
2. ロゴファイル(PNG、182x34)を点線で囲まれたボックスへドラッグするか、**[ファイルを選択]**をクリックしてファイルシステムから選択します。
3. **[変更の保存]**をクリックします。

マルチユーザーサインイン(Webクリップ) のブランディング

新しいタイトルとWebクリップアイコンの追加により、iOSのマルチユーザーセキュアサインインをカスタマイズできます。

手順

1. **[管理] > [マルチユーザーサインイン(Webクリップ)]** を開きます。
2. [マルチユーザーサインイン(Webクリップ)] 画面で **[カスタマイズ]** をクリックします。
3. ロゴファイルを点線で囲まれたボックスへドラッグするか、**[ファイルを選択する]** をクリックしてファイルシステムから選択します。
4. ラベルを変更するには **[セキュアサインイン]** テキストを編集します。
5. Webクリップアイコンを変更するには、Webクリップファイルを点線で囲まれたボックスへドラッグアンドドロップするか、**[ファイルを選択]** をクリックしてファイルシステムから選択します。
6. 更新のプレビューを確認し、**[変更を保存]** をクリックします。

iPhoneおよびiPod touchデバイスについては、120 x 120または60 x 60ピクセル(標準解像度) のアイコンを作成してください。

iPadデバイスについては、152 x 152または76 x 76ピクセル(標準解像度) のアイコンを作成してください。

詳細はiOS対応マルチユーザーセキュアサインインを参照してください。

非iOSデバイスの管理追加

ライセンス: Gold

お客様は現在、iOSデバイスに最適化したIvanti Neurons for MDMのバージョンをご利用です。このセクションでは、非iOSデバイスも管理できるようにする方法を説明します。切り替えの後は、以下のデバイスも管理可能となります。

- Android 5.0またはサポートされる以降のバージョン
- Windows 10 Mobileとデスクトップ

非iOSデバイスの管理を可能にする変更は元に戻せません。

非iOSデバイスの管理を可能にするには:

1. **[管理者] > [許可されたプラットフォーム]** をクリックします。
2. **[全プラットフォームを許可]** ボタンをクリックします。
3. **[元に戻せないことを理解します]** にチェックを入れ、この操作を元に戻せないことに対する理解を確認します。
4. **[全プラットフォームを許可]** ボタンをクリックします。

パッケージ

このセクションは以 下 のトピックを含 みます。

Secure UEMパッケージとSecure UEM Premiumパッケージ

Secure UEMパッケージとSecure UEM Premiumパッケージは、以 下 の機 能 を提 供 します。

	Secure UEM	Secure UEM Premium
Device management and security		
Easy on-boarding	✓	✓
Multi-OS security and management	✓	✓
Secure email gateway	✓	✓
App distribution and configuration	✓	✓
Mobile application management (MAM)	✓	✓
Scale IT operations		
Helpdesk tools	✓	✓
Reporting	✓	✓
Secure connectivity		
Per app VPN		✓
Conditional Access		✓
Secure productivity		
Secure email and personal information management (PIM) app		✓
Secure web browsing		✓
Secure content collaboration		✓
Mobile app containerization		✓
Derived Credentials		✓
Zero Sign-On		
Passwordless user authentication (single app)		✓

これらのパッケージは予告なく変更される場合があります。現在の枠組みについては、Ivantiセールスまでお問い合わせください。

レガシーのBronze/Silver/Goldパッケージ

このセクションでは、レガシーのBronze、Silver、およびGoldの各パッケージについて説明します。パッケージングは、Secure UEMおよびSecure UEM Premiumという枠組みに進化しています。

Bronze

Ivanti Neurons for MDM 基本機能は、Bronzeパッケージで提供されています。Bronzeパッケージは、以下の手順で拡張できます。

- より多くのデバイスを追加する
- Silverを追加する
- Goldを追加する
- Platinumを追加する

これらの追加により、モバイルソリューションが基本的なデバイス構成より拡張されます。

管理者は、サポートに問い合わせることにより、テナントでデフォルトで無効化されている1つまたは複数のオンデマンド機能を有効化することができます。

Silver

Silverへアップグレードすると、次の機能が追加されます。

- **LDAPおよびConnector:** 企業ディレクトリおよび認証機関の Ivanti Neurons for MDM への追加をサポートします。
- **Sentry:** メールアクセス制御をサポートします。
- **スペース:** デバイスを指定し、別の管理者に管理させることができます(委譲管理) 。
- **監視モード:** Single-Appモードを含む詳細な設定をデバイスレベルでサポートします。
- **セルフサービスポータルのブランディング:** セルフサービスポータルに御社ロゴを使用します。
- **認証機関:** Ivanti Neurons for MDM を認証機関として使用します。
- **アプリのサイレントインストール/アンインストール:** アプリを自動的にモバイルデバイスに展開したり、モバイルデバイスから消去したりします。
- **アプリの許可リスト/ブロックリスト/必須アプリ:** デバイスにインストールするアプリの監視と制御を行います。
- **Webコンテンツフィルター:** Webサイトの許可リストとブロックリストのポリシーをすべてのWebブラウザに適用します。
- **Apple特有の機能:** AirPlay、AirDrop、iOS壁紙配布、Apple TVの有効化と制限を行います。

- **オープンイン管理：**どのモバイルアプリがどの企業コンテンツを開けるかを制御します。
- **Appleの「Appとブック」：**デバイスにモバイルアプリライセンスを配布し、デバイスを撤去する際にはこのライセンスの回収および再割り当てを行います。
- **Android enterprise(Android for Work)サポート**
- **Device Enrollment：**まとめてデバイスを購入し、起動中にこれらのデバイスを自動的にMDMに登録できます。
- **アプリごとの構成：**構成済みのモバイルアプリが大規模に導入されるため、エンドユーザーによる操作はほとんど必要ありません。
- **サードパーティのPer-App VPN：**VPNセキュリティは、ユーザーに意識されることなく速やかに機能するモバイルアプリ専用のセキュリティです。
- **ポリシーの段階的アクション**
- **アプリ配布フィルター**
- **監査証跡**
- **Androidキオスクモード：**キオスクモードで動作するようAndroidデバイスを構成可能です。
- **Androidキオスクのブランディング：**デバイスがキオスクモードで動作するときのキオスク画面の背景とバナーを変更します。
- **Microsoft Graph APIを使用したOffice 365情報漏洩防止(DLP)対策：**Graph APIを通じてOffice 365アプリにDLP制御機能を適用します。

Gold

Goldへアップグレードすると、Silverの機能に次の機能が追加されます。

- **シングルサインオン：**一度ユーザー認証すると、他の企業のモバイルアプリに自動的にログインします。
- **iOS/Androidアプリカタログのカスタムブランディング：**アプリカタログに企業ロゴを表示します。
- **コンテンツ制限の緩和：**50ファイル、各25MB
- **iOS対応AppConnect：**AppConnect対応アプリのセキュリティ確保と構成を行います。
- **iOS対応AppTunnel：**アプリから企業リソースへのセキュアアクセスを可能にします。

- **iOS対応Docs@Work:** ユーザーがドキュメントを表示、保存、共有できます。
- **iOS 8証明書ベースのシングルサインオン**
- **iOS 8 iBook/ePub管理**
- **macOSサポート**
- **ユーザーのブランディング**
- **AppConnectでのモバイルアプリケーション管理(MAM)**
- **派生認証情報**
- **Windows 10(Bridgeを含む)のサポート**

Platinum

Platinumへアップグレードすると、Goldの機能に次の機能が追加されます。

- **Tunnel:** 企業のデータに対するアプリ固有のアクセスを構成します。
- **Help@Work**
- **モニター**
- **ServiceConnect(ServiceNow、Splunk)**

プレビュー/テスト用サンドボックス

Premium Plusサポートを購入したIvanti Neurons for MDMのお客様には、本番リリースの前に、サンドボックステナントで新しいリリースをプレビューおよびテストしていただけます。

アップグレード

このセクションは以下のトピックを含みます。

- 「ライセンスのアップグレード」下
- 「アップグレードの要求」下
- 「先行リリースからのアップグレード」次のページ

ライセンスのアップグレード

基本的機能は、Bronzeパッケージで提供されています。Bronzeパッケージは、以下の手順で拡張できます。

- より多くのデバイスを追加する
- Silverを追加する
- Goldを追加する
- Platinumを追加する

これらの追加により、モバイルソリューションは基本的なデバイス構成を越えたものに拡張されます。

アップグレードの要求

手順

1. 管理ドロップダウンメニューから **[アップグレードオプション]** を選択します。
2. **[アップグレード/デバイス追加を要求]**(右上)をクリックします。
3. 追加したい項目を選択し、電話番号を入力します。

   担当者が24時間以内に詳しい手順をお知らせいたします。

先行リリースからのアップグレード

先行リリースからアップグレードする際、**[Device Enrollmentプロファイルを編集]** ページの設定は保存されません。アップグレードの前にオプション設定をご確認ください。

- アップグレード前に **[AppleIDおよびiCloudへのサインインをスキップ]** を有効化すると、アップグレード後に **[Apple Pay設定をスキップ]** が有効化されます。
- アップグレード前に **[パスコードの入力をスキップ]** を有効化すると、アップグレード後に **[Touch ID設定をスキップ]** と **[Apple Pay設定をスキップ]** が有効化されます。

手順

1. アップグレード完了後、**[Device Enrollmentプロファイルを編集]** ページに戻り、Device Enrollmentプロファイルを編集して必要な設定を復元してください。
2. **[保存]** をクリックします。

アップグレード後、影響を受ける構成設定がいくつかあります。

プロモーションオプションが **[オフ]** に設定されます。

インストール設定が **[なし]** に設定されます。

[アプリカタログに表示しない] オプションを選択できなくなります。

Android Samsung Knoxでのサイレントインストールが [無効] に設定されます。

[iOS管理フラグ] が次のように設定されます。

- iCloudへバックアップ。
- 登録解除時に削除

これらのiOS管理フラグ設定は、各アプリで個別に選択できます。

アプリ設定：

- アプリ設定が [構成] と呼ばれるようになります。
- その他のすべてのアプリ設定は、アップグレード前と変わりません。

詳細はパッケージを参照してください。

デバイスライセンス

Ivanti Neurons for MDM のデバイスベースのライセンスにより、登 録 できるデバイスの数 、デバイスへの配 布 用 に構 成 できるコンテンツの量 、および利 用 できる機 能 が定 義 されます。デバイスの上 限 に近 付 くと [管 理] ページに赤 い三 角 形 が表 示 されます。コンテンツの上 限 に近 付 くと、サービスでさらなる追 加 が差 し止 められ、上 限 に近 付 いていることを示 すメッセージが表 示 されます。

テナント一時停止

評価ライセンスまたはプロダクションライセンスを使用したテナントへのアクセスがIvanti Neurons for MDMによって一時的に停止される場合があります。評価ライセンスは、評価期間が終了したり、所定の使用量を超えたりすると一時的に停止されます。プロダクションライセンスも、サブスクリプション期間が終了したり、所定の使用量を超えたりすると一時的に停止されます。Ivanti Neurons for MDMは、ライセンスの更新またはライセンスの追加購入(使用量超過の場合)に応じて一時停止中のテナントを回復します。

テナントライセンスが一時停止された場合:

- 既存の登録デバイスは引き続き正常に機能します。
- 管理者は管理ポータルにログインできません。
- 新規デバイスは登録できません。
- テナントへのAPIアクセスはブロックされます。
- エンドユーザーはセルフサービスポータルにログインできなくなります。

テナント一時停止アクションとエラーメッセージ

一時停止アクション	エラー	表示されるエラーメッセージ	場所
エンドカスタマー統合APIアクセスがブロックされる。	API呼び出しに失敗する。	アクセスが拒否されました。評価ライセンスが有効期限切れです。APIアクセスを再有効化するにはライセンスを更新してください。詳細はシステム管理者にお問い合わせください。	APIエラー401。
新規デバイスの登録がブロックされる。	登録画面にエラーメッセージが表示される。	デバイスを登録できません。システムのライセンスが有効期限切れです。詳細はシステム管理者にお問い合わせください。過去に登録したデバイスは引き続き正常に動作します。	パスワード確認後。
管理者による管理ポータルへのログインがブロックされる。	ログイン画面にエラーメッセージが表示される。	ログインできません。ライセンスの有効期限が切れました。管理ポータルへのアクセスを回復し、新しいデバイスを登録するには、ライセンスを更新してください。過去に登録したデバイスは引き続き正常に動作します。ライセンスの更新は営業担当者が承ります。管理パスワードは1年(365日)後に有効期限が切れます。	パスワード確認後。

サポート チケットを登録する

サポート チケットを登録するには、Ivanti サポート ポータルにアクセスします。