HANDS-ON LABS MANUAL - 2022

HOL-2251-09-DWS

デジタル ワークスペースの概要

vmware®

Table of contents

ラボの概要：HOL-2251-09-DWS - Workspace ONE UEM - デジタル ワークスペースの概要

ラボのガイダンス

[2]

注：このラボの所要時間は 90 分以上になる場合があります。いっときに終了するモジュールは 2 ～ 3 個と考えてください。モジュールは相互に独立しているため、どのモジュールから開始してもよく、そこから進めることができます。目次を使用すると、選択したモジュールにアクセスできます。

目次を表示するには、ラボ マニュアルの右上の [目次] をクリックします。

現代の分散した従業員のニーズを満たすために安全なデジタル ワークスペースを提供することに関心がありますが、どこから始めたらいいのか分からないのですか? Workspace ONE UEM（統合エンドポイント管理）の主要な概念と、iOS、macOS、Windows 10、および Android デバイスを登録および管理して、アプリケーション、ポリシー、制限、および強力なワークフローを配布するための基本を学びます。Workspace ONE Intelligence を使用したインサイトに関するレポートや自動化、Unified Access Gateway によるセキュアなアクセスの提供方法など、Anywhere Workspace ソリューション全体について説明します。

ラボのモジュール リスト：

- モジュール 1：Freestyle Orchestrator の概要（30 分）（基本レベル）Freestyle Orchestrator を使用すると、Workspace ONE UEM 管理者は、柔軟性と速度を備えた、特定の要件に適合する複雑なワークフローを作成できます。Freestyle ワークフローを使用して、アプリケーション、プロファイル、センサー、スクリプトなどのリソースを設定できます。これらのワークフローでは、条件を使用して、きめ細かい条件に基づいてリソースをデバイスに適用します。Freestyle Orchestrator でリソースのプロビジョニングプロセスを簡素化し、管理者が非常に効果的な方法で複雑なワークフローを視覚的に定義する方法を直接ご覧ください。
- モジュール 2：Windows 10 管理の概要（30 分）（基本レベル）このラボ モジュールでは、Windows 10 プラットフォームの Workspace ONE を使用した統合エンドポイント管理 (UEM) の概念について説明します。Windows 10 デバイスを Workspace ONE UEM に登録する方法と、制限プロファイルとアプリケーションを構成して登録済みデバイスに展開する方法について説明します。
- モジュール 3：Apple iOS 管理の概要（30 分）（基本レベル）このラボ モジュールでは、iOS プラットフォームの Workspace ONE を使用した統合エンドポイント管理 (UEM) の概念について説明します。iOS デバイスを Workspace ONE UEM に登録し、デバイス プロファイルを展開して制限事項を追加し、iOS デバイスの動作を変更する方法について説明します。
- モジュール 4：Apple macOS 管理の概要（45 分）（中級レベル）macOS プラットフォームで利用可能な、Workspace ONE UEM 管理の主な機能と概念について説明します。このモジュールでは、macOS デバイスの登録方法および使用可能な管理オプションについて確認し、これらのオプションが macOS の構成とアプリケーションの公開を通じてユーザー エクスペリエンスにもたらす改善と影響について理解を深めることができます。
- モジュール 5：Android 管理の概要（30 分）（基本レベル）このラボ モジュールでは、Android プラットフォームの Workspace ONE を使用した統合エンドポイント管理 (UEM) の概念について説明します。Android デバイスを Workspace ONE UEM に登録し、制限を構成してアプリケーションをプッシュすることで、登録済みデバイスを管理する方法など、Android の基礎を学びます。Android Enterprise と Workspace ONE UEM の最新のデバイス管理 API を使用して Android デバイスを保護する方法について説明します。

モジュール 6：Workspace ONE Intelligent Hub と Hub サービスの概要（60 分）（基本レベル）Workspace ONE Intelligent

Hub アプリケーションの基本的な機能と、Workspace ONE UEM の登録を簡素化する方法について学習します。Hub サービスと Workspace ONE Access を確認して構成し、Intelligent Hub アプリケーション機能セットを拡張して、統合アプリケーション カタログ、シングル サインオン (SSO) 機能、People Search などを提供します。

- モジュール 7：Workspace ONE Intelligence - ダッシュボード、自動化、レポートの概要（45 分）（基本レベル）Workspace ONE Intelligence コンソールを確認し、環境についてのより深い洞察とカスタマイズされた検証がダッシュボードとレポートによってどのように一元的に提供されるのかを確認します。自動化タスクを構成して、手動の管理ワークロードの削減、セキュリティの強化、修復の自動化の方法を確認します。
- モジュール 8：Secure Access Service Edge (SASE) による Anywhere Workspace のセキュリティ強化（60 分）(中級レベル) Workspace ONE Tunnel は、モバイル ワーカーとデバイスの安全なアクセスを可能にします。ユーザーの操作はシンプルになり、Tunnel を有効にしたり、操作したりする必要はありません。IT 組織は、エンタープライズ アクセスに対して最小権限のアプローチを取り、定義されたアプリケーションとドメインのみがネットワークにアクセスできるようにすることができます。Tunnel は業界最高のセキュリティを提供し、TLS 1.2 以降のライブラリをベースにしています。また、MITM 攻撃を防止するための SSL ピン留めを実装し、ID の整合性を確保するために許可リストにクライアント証明書を含めます。管理対象アプリケーションの明示的な定義と、Workspace ONE コンプライアンス エンジンとの統合を組み合わせることで、Tunnel はお客様が従業員のゼロトラスト目標を達成するのに役立ちます。

ラボのチーフ：

- EUC テクニカル ストラテジスト（カナダ）、ブレント・マッコーブレー (Brent McCoubrey)
- シニア テクニカル マーケティング アーキテクト（米国）、ジャスティン・シーツ (Justin Sheets)

ラボ責任者：

- EUC スタッフ アーキテクト（米国）、クリスチーナ・ミニハン (Christina Minihan)
- シニア テクニカル マーケティング アーキテクト（オーストラリア）、ダレン・ウェザリー (Darren Weatherly)

アソシエイト ラボ責任者：

- テクニカル スタッフ メンバー（インド）、アシタ・カルナカラン (Asitha Karunakaran)
- シニア コンピティティブ テクニカル マネージャ（米国）、マイク・マークス (Mike Marx)
- コレーグ サポート エンジニア（インド）、パヴィトラ・ナゲンドラッパ (Pavitra Nagendrappa)

Odyssey 責任者：

- シニア ソリューション エンジニア スペシャリスト EUC（ブラジル）、ティアゴ・ヴァルセシア (Thiago Valcesia)

謝辞：

- EUC スタッフ アーキテクト（米国）、アンドレアノ・ラヌース (Andreano Lanusse)
- EUC スタッフ アーキテクト（米国）、ジョシュア・ネグロン (Josue Negron)
- シニア テクニカル マーケティング マネージャ（米国）、カリーム・シェルアティ (Karim Chelouati)
- シニア テクニカル マーケティング アーキテクト（米国）、ロバート・テラケディス (Robert Terakedis II)

・ディレクター、Workspace ONE テクニカル マーケティング（米国）、ロジャー・ディーン (Roger Deane)

この実習ラボ マニュアルは、次のハンズオン ラボ ドキュメント サイトからダウンロードできます。

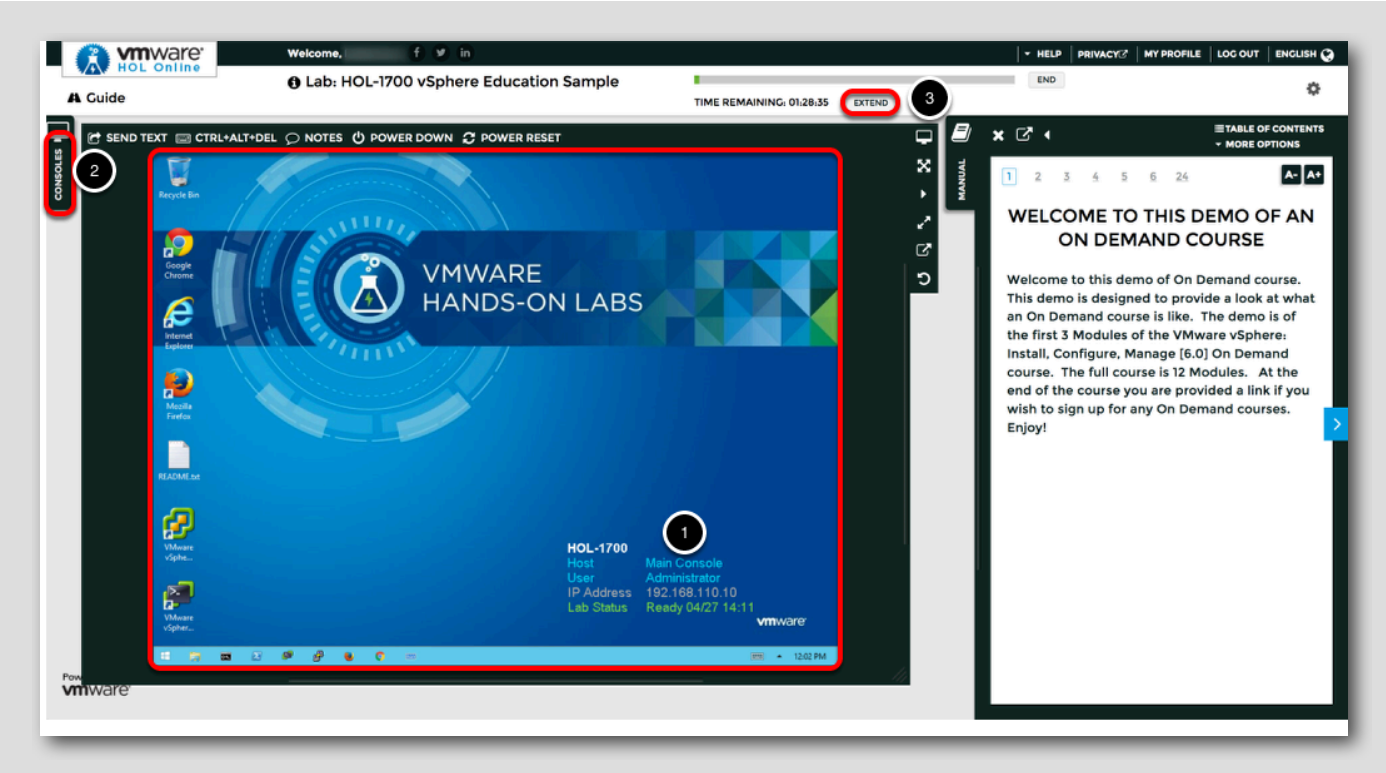
http://docs.hol.vmware.com

このラボは英語以外の言語でも利用できます。言語設定を変更し、翻訳版のマニュアルをラボで使用する手順については、次のドキュメントを参照してください。

http://docs.hol.vmware.com/announcements/nee-default-language.pdf

メイン コンソールの表示位置

[3]



1. 赤の四角形で囲われた領域がメイン コンソールです。ラボ マニュアルは、メイン コンソールの右側のタブに表示されます。
2. ラボによっては、左上のタブにもコンソールが表示されていることがあります。この場合、ラボ マニュアルの説明に従って、指定されたコンソールを開いてください。
3. このラボでは、開始時に 90 分のタイマーが表示されます。このラボは途中経過を保存できません。ラボを開始したら、そのセッション内ですべての作業を完了してください。必要であれば、[EXTEND] をクリックして時間を延長できます。VMware イベントでご使用の場合は、ラボの時間を 2 回まで、最大 30 分延長できます。[EXTEND] を 1 回クリックすると、時間が 15 分間延長されます。VMware イベント以外でご使用の場合はラボの時間を最大 9 時間 30 分延長できます。[EXTEND] を 1 回クリックすると、時間が 1 時間延長されます。

キーボード以外の方法によるデータ入力

[4]

このモジュールでは、メイン コンソールへテキストを入力します。複雑なデータを入力する場合、キーボードから直接入力する以外に、次の 2 つの方法があります。

クリック アンド ドラッグによるコピー

[5]

https://www.youtube.com/watch?v=xS07n6GzGuo

ラボ マニュアルに記載されているテキストやコマンド ライン インターフェイス (CLI) のコマンドは、クリック アンド ドラッグによってメイン コンソールのアクティブ ウィンドウへ直接コピーできます。

オンラインの国際キーボードを使用する

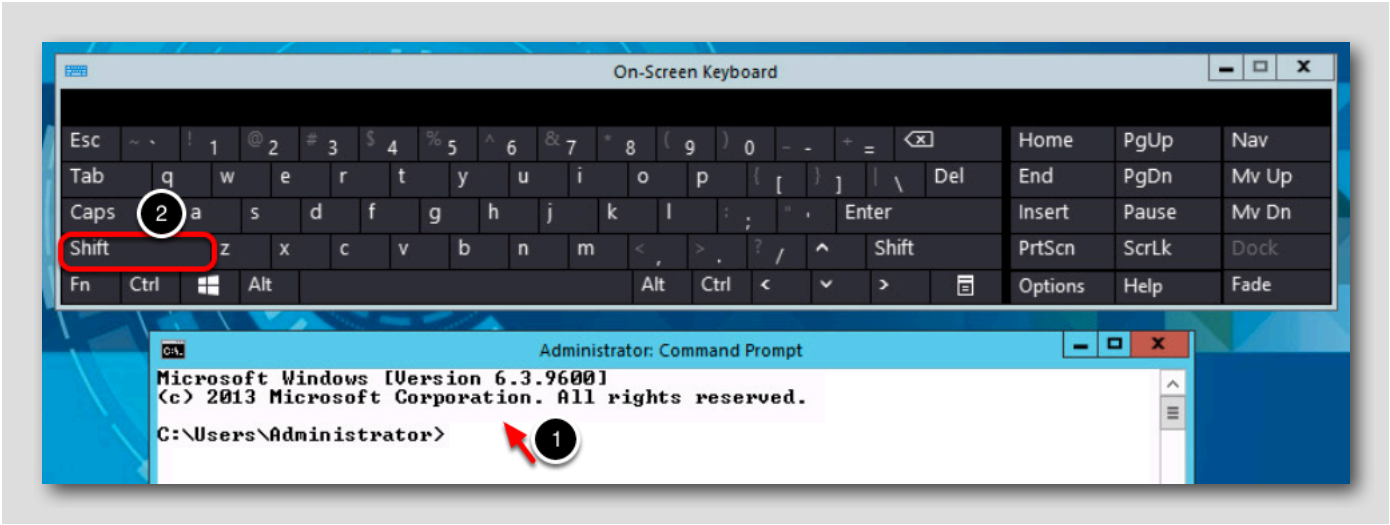
[6]

キーボード配列によっては、特定の文字や記号が入力しにくいことがあります。そのような場合、メイン コンソールに、オンラインの国際キーボードを表示して使用すると便利です。

1. キーボードは、Windows のクイック起動タスク バーで、キーボードのアイコンをクリックして表示します。

アクティブなコンソール ウィンドウをクリック

[7]

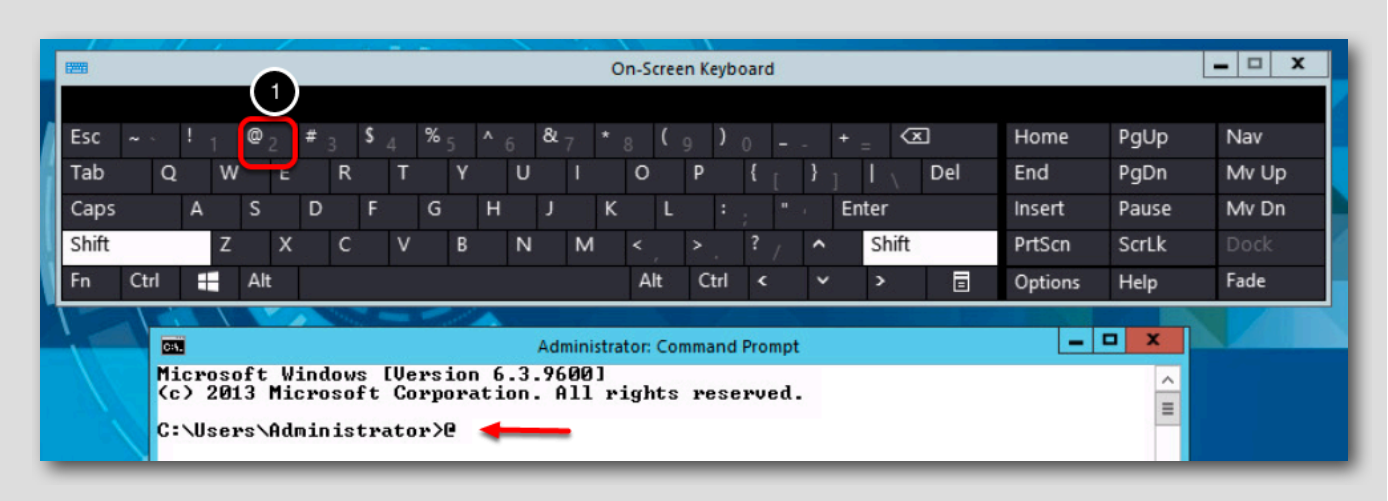


この例では、メール アドレスで使用される「@」記号をオンライン キーボードから入力します。US 配列のキーボードで「@」記号を入力するには、 + <2> キーを押します。

1. アクティブなコンソール ウィンドウを 1 回クリックします。
2. <Shift> キーをクリックします。

<@> キーをクリック

[8]

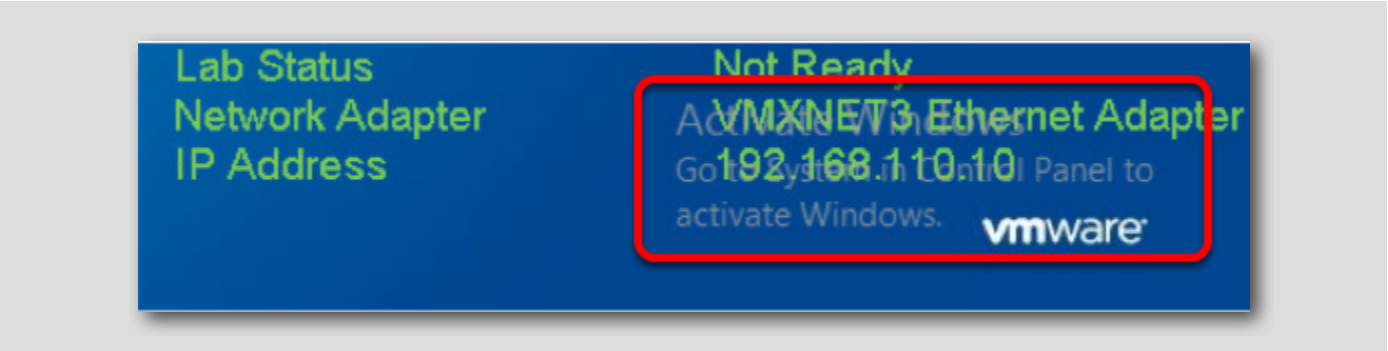


1. キーをクリックします。

アクティブなコンソール ウィンドウに「@」記号が入力されました。

Windows アクティベーションに関するウォーターマーク

[9]



ラボを最初に開始する際、Windows のアクティベーションが完了していないことを知らせるウォーターマークがデスクトップに表示される場合があります。

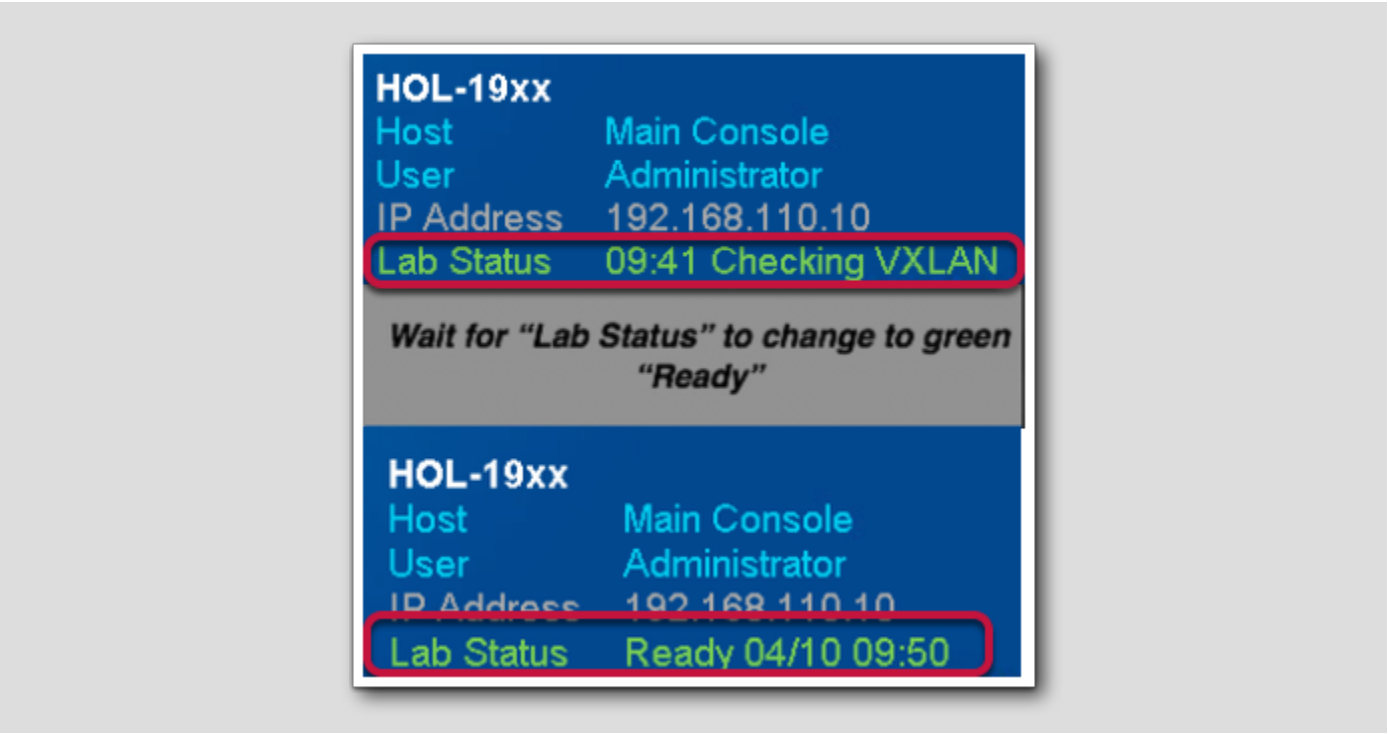
仮想化の大きなメリットの 1 つは、仮想マシンを任意のプラットフォームへ移動して実行できることです。ハンズオン ラボも、このメリットを活用して複数のデータセンターから実行できるようになっています。ただし、データセンターによってプロセッサのタイプが異なることがあり、そのような場合、インターネット経由で Microsoft 社のアクティベーション チェックが行われます。

この場合でも、VMware とハンズオン ラボは Microsoft のライセンス要件に完全に準拠しているため、安心してご利用いただけます。このラボは自己完結型ポッドであり、Windows のアクティベーション チェックに必要なインターネットへのフル アクセス権限がありません。インターネットへのフル アクセス権限がないと、この自動プロセスは失敗し、次のウォーターマークが表示されます。

これは表面上の問題であり、ラボには影響しません。

画面右下でラボの準備完了を確認

[10]



ラボのすべてのスタートアップ ルーチンが完了し、開始する準備ができていることを確認してください。「Ready」以外のステータスが表示される場合は、数分お待ちください。5 分経ってもラボが「Ready」に変更されない場合は、サポートにご連絡ください。

モジュール 1：Freestyle Orchestrator の概要（30 分）

免責事項：VMware のテクニカル プレビュー

[12]

このセッションには、現在開発中の製品機能が含まれている場合があります。

この新しいテクノロジーに関するセッションおよび概要は、VMware が市販製品にこれらの機能を搭載することを確約するものではありません。

機能は変更される場合があり、したがってどのような種類の契約書、発注書、販売契約書にも含まれてはならないものとします。

技術的な問題とマーケットの需要により、最終的に出荷される製品に影響する場合があります。

ここで述べられたり、提示されたりする新しいテクノロジーまたは機能の価格とパッケージングは、決定されたものではありません。

- 「これらの機能は、現在開発中のものです。記述された機能は変更される場合があり、いかなる種類の契約書、発注書、または販売契約書にも含めてはならないものとします。技術面の実現可能性と市場の需要が、最終的に出荷される製品に影響することになります。」

はじめに

[13]

デバイス管理は進化し続けており、この急速な進化は、IT 管理者のエクスペリエンスに直接影響を与えています。*VMware Workspace ONE® UEM* は、あらゆるリリースで進化と革新を続け、管理者がクロスプラットフォーム デバイスを管理して真のデジタル ワークスペース環境を実現できるようにしています。このイノベーションを継続するために、Freestyle Orchestrator を発表します。

Freestyle Orchestrator を使用すると、Workspace ONE UEM 管理者は、柔軟性と速度を備えた、特定の要件に適合する複雑なワークフローを作成できます。Freestyle ワークフローを使用して、アプリケーション、プロファイル、センサー、スクリプトなどのリソースを設定できます。これらのワークフローでは、条件を使用して、きめ細かい条件に基づいてリソースをデバイスに適用します。

Freestyle Orchestrator で解決される問題

[14]

MDM API に基づいてリソース（プロファイル、アプリケーション、コンテンツ、スクリプトなど）をワイヤレスでプロビジョニングする現在の方法は、モバイル プラットフォームで始まり、以降、Windows 10、macOS、Chrome OS などのデスクトップに拡張されました。各プラットフォームでの管理環境には、特定のニーズがあります。全体として、管理者はデバイスにリソースを展開する順序を制御したり、特殊なスクリプトを必要とする現在のリソース状態や外部条件に基づいて条件を定義したりするなど、プロビジョニング プロセスを制御したいと考えています。

デスクトップ プラットフォームで必要な管理環境を提供するには、背後に多くの複雑さがあります。プロビジョニング プロセスには、Workspace ONE とコーディングなどの外部ツールに関する知識が必要です。Freestyle Orchestrator は、このプロセスを簡素化し、管理者が複雑なワークフローを非常に効果的な方法で視覚的に定義できるようにします。

ユースケースの定義

[15]

ユースケースと要件をよりよく理解すると、Workspace ONE UEM のリソースを整理し、ワークフローを定義するのに役立ちます。ワークフローは、ビジネス ニーズから新しいユースケースが生まれるのにつれて進化する目標を達成するための論理的な方法になります。

特定の順序または条件でアプリケーションをプロビジョニングする必要がある Windows 10 デバイスのアプリケーションのユースケースについて考えてみましょう。このユースケースでは、特定のアプリケーションを他のアプリケーションの前に最初に展開する必要があります。

ビジネス要件は単純に見えますが、それらを技術要件に変換すると、さまざまなタイプのペイロード（制限、証明書、カスタム設定など）、アプリケーション、特殊なスクリプト、リソースの状態を検証するための条件などを備えたプロファイルにマッピングされます。

この例のユースケースは、次の機能要件に変換されます。

- Zoom Client for Meetings を展開します（ユーザーに対して自動）。
- Zoom Plugin for Microsoft Outlook を展開します（オプション）。
- Microsoft Office および Zoom Client がインストールされている場合にのみ、Zoom Meetings などの Outlook プラグインを展開して構成します。

ワークフローの一部として使用するには、次のリストに従って、事前にプロファイルとアプリケーションのリソースを構成する必要があります。

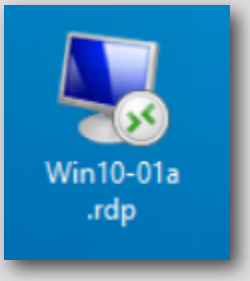
- アプリケーションを *オンデマンド*展開に設定します。*自動*に設定されたリソースは、ワークフローの外部でプロビジョニングされます。
- アプリケーション リソースには、デフォルト ポリシーの割り当てルールを少なくとも 1 つ含める必要があります。ただし、ワークフローによってプロビジョニングされたリソースは、ワークフローに割り当てられたスマート グループを使用します。

アプリケーションやプロファイルなどのリソースがデバイスに割り当てられ、自動展開用に構成されている場合、ワークフローの一部としてデバイスに割り当てられるだけでなく、デバイスが処理するコマンドに基づいてリソースがインストールされます。

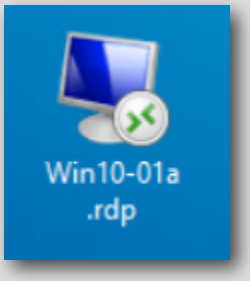
管理者は、Workspace ONE UEM Console から Freestyle Orchestrator Designer にアクセスします。

Windows 10 仮想マシンへの接続

[16]



メイン コンソール デスクトップにある [Win10-01a.rdp] ショートカットをダブルクリックして、Windows 10 仮想マシンに接続します。



Workspace ONE UEM Console へのログイン

[17]

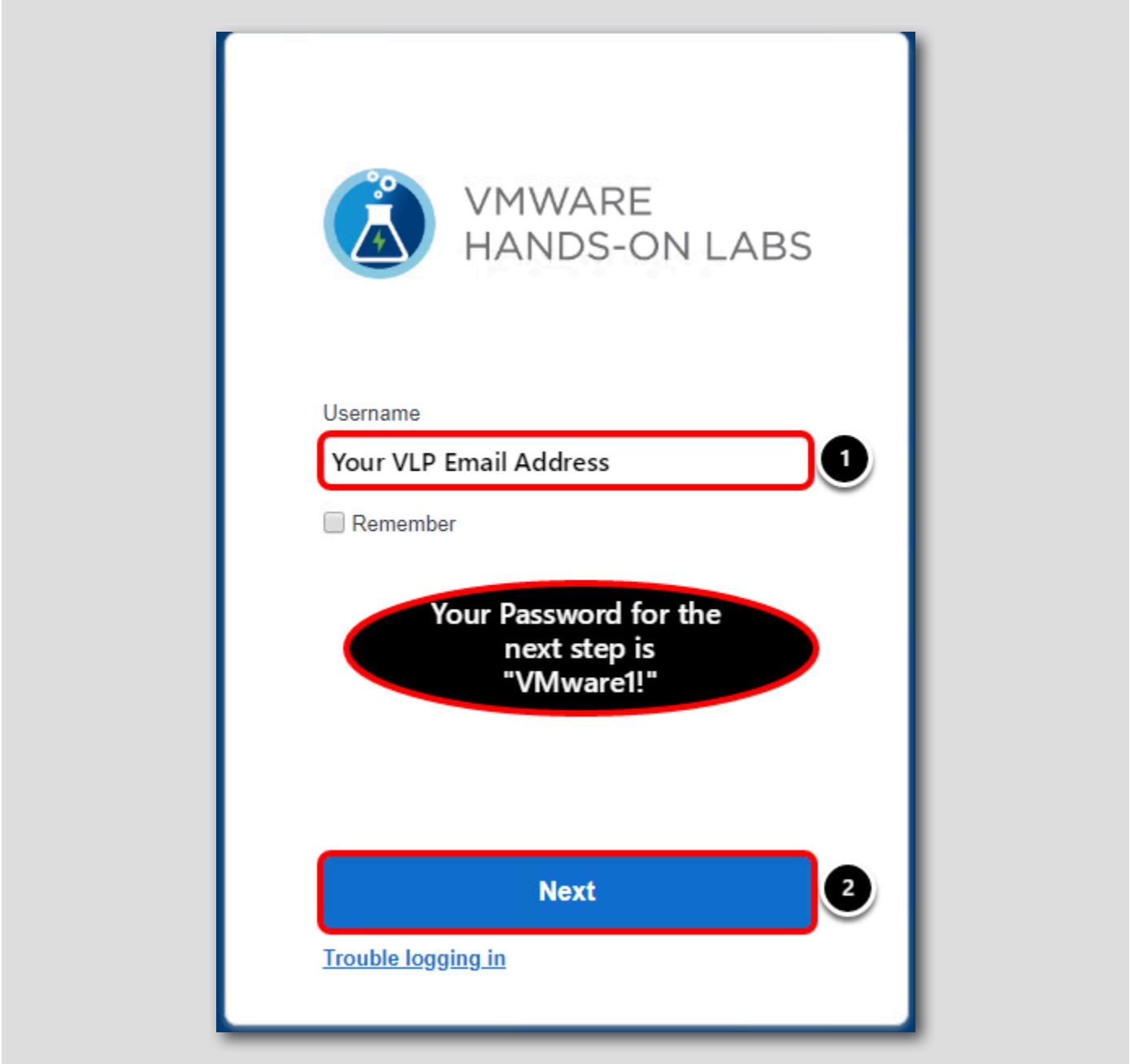
このラボでは、ほとんどの場合、Workspace ONE UEM 管理コンソールにログインします。

Chrome ブラウザの起動

[18]

現在接続している仮想マシンのデスクトップにある [Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールでの管理者ユーザー名の入力 [19]

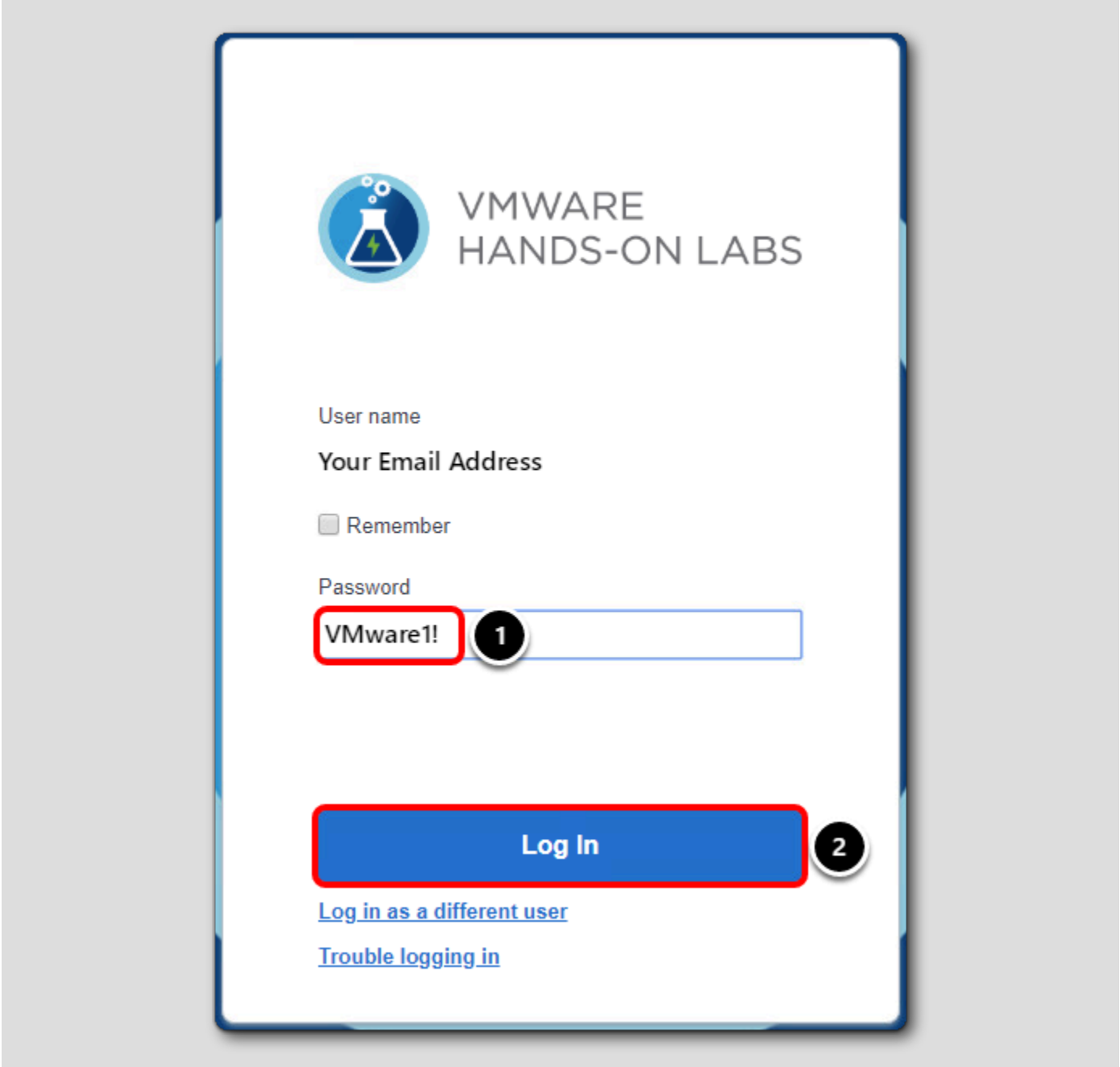


ブラウザのデフォルトのホーム ページは https://hol.awmdm.com です。Workspace ONE UEM 管理者アカウント情報を入力し、[Login] ボタンをクリックします。

1. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。
2. [Next] をクリックして、ラボ マニュアルの次の手順に進み、パスワードを入力します。これは常に **`VMware1!`** です。

注：Captcha による入力を求められた場合は、大文字と小文字を区別して入力してください。

Workspace ONE UEM Console の認証情報の入力 [20]



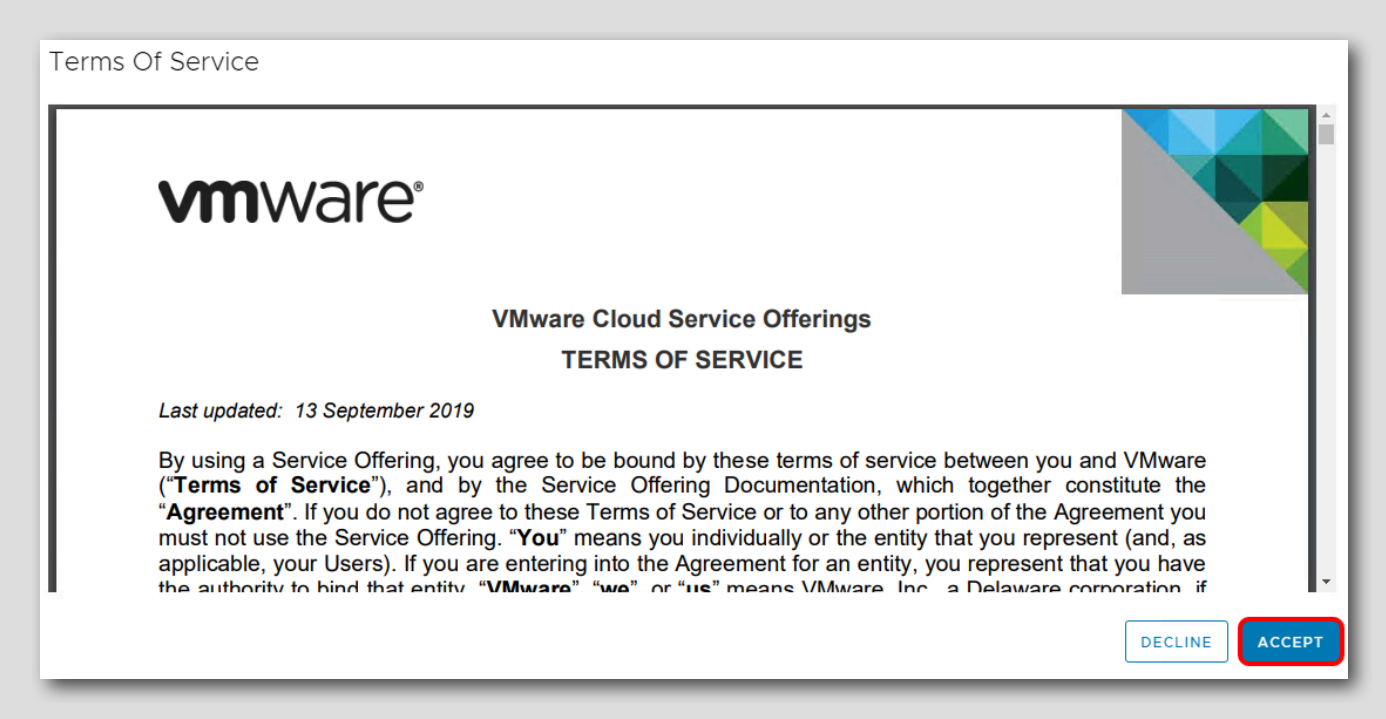
ユーザー名を入力すると、パスワード フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ラボの制限により、ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

エンド ユーザー使用許諾契約書に同意

[21]



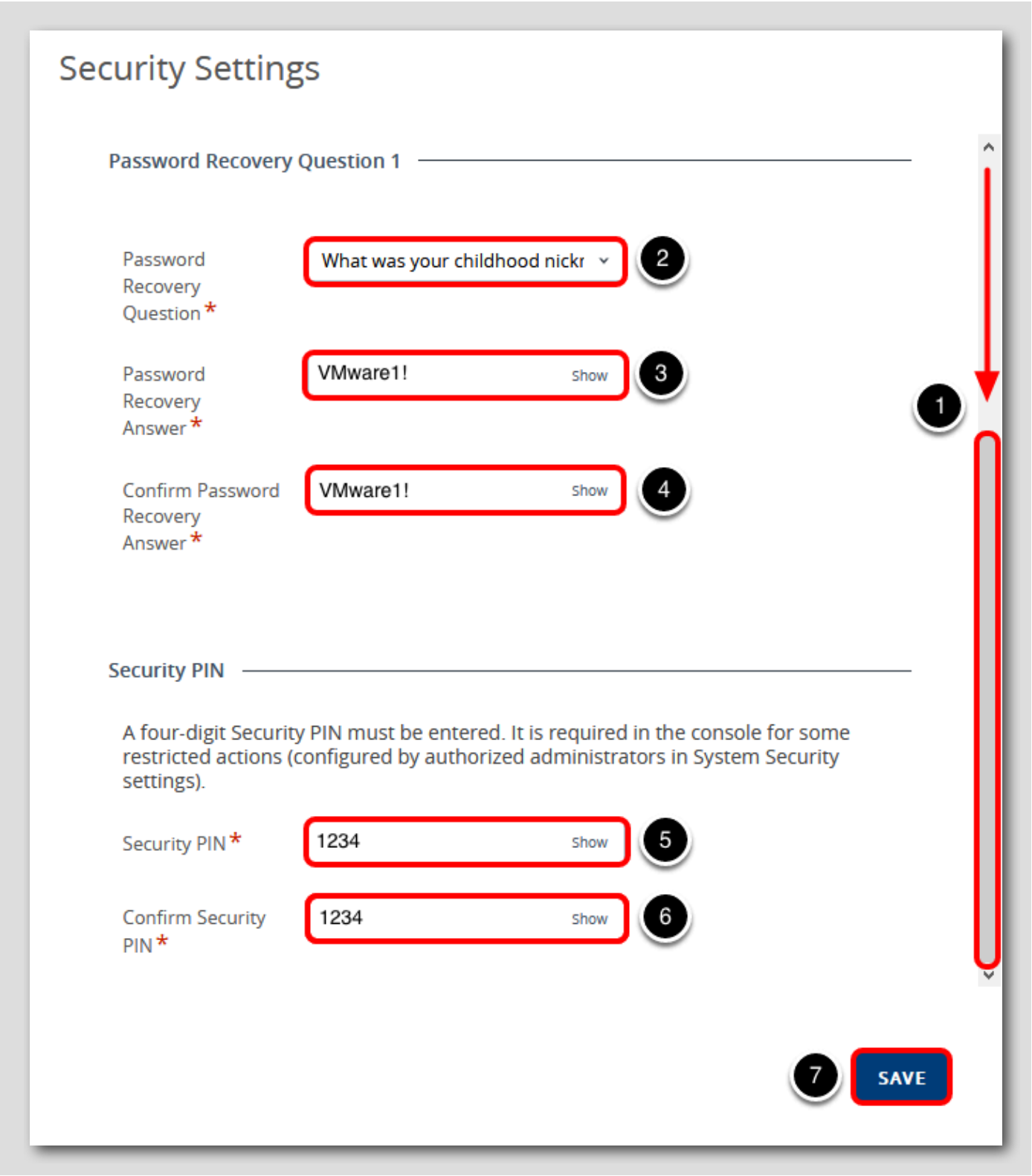
Workspace ONE UEM の「利用規約」が表示されたら、[Accept] ボタンをクリックします。

注：管理コンソールに初めてログインする場合のみ、次の手順に従ってログインしてください。

初期セキュリティ設定の完了

[22]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

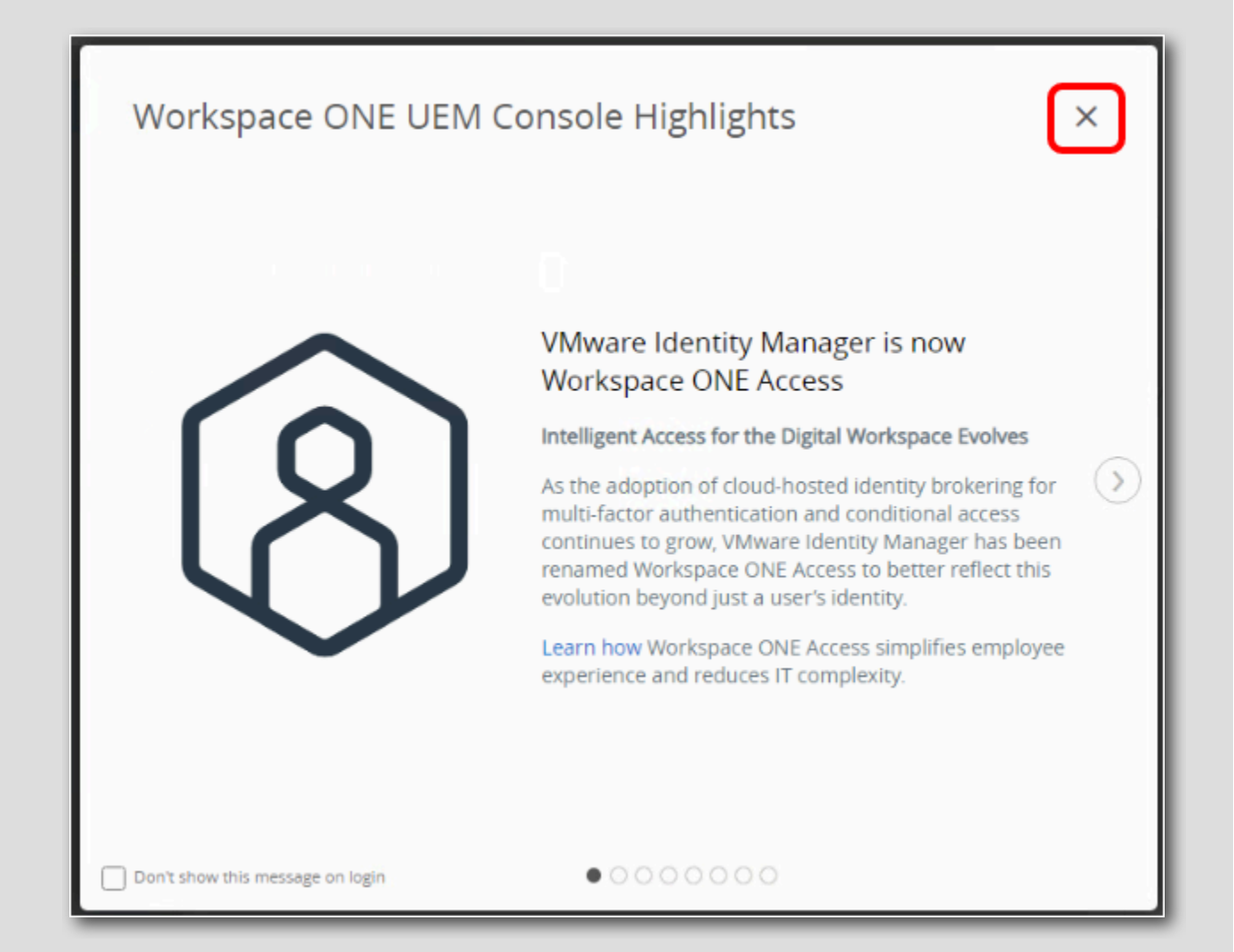

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 必要に応じて画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示してください。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[23]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

個人の Windows 10 デバイスを登録しないこと

[24]

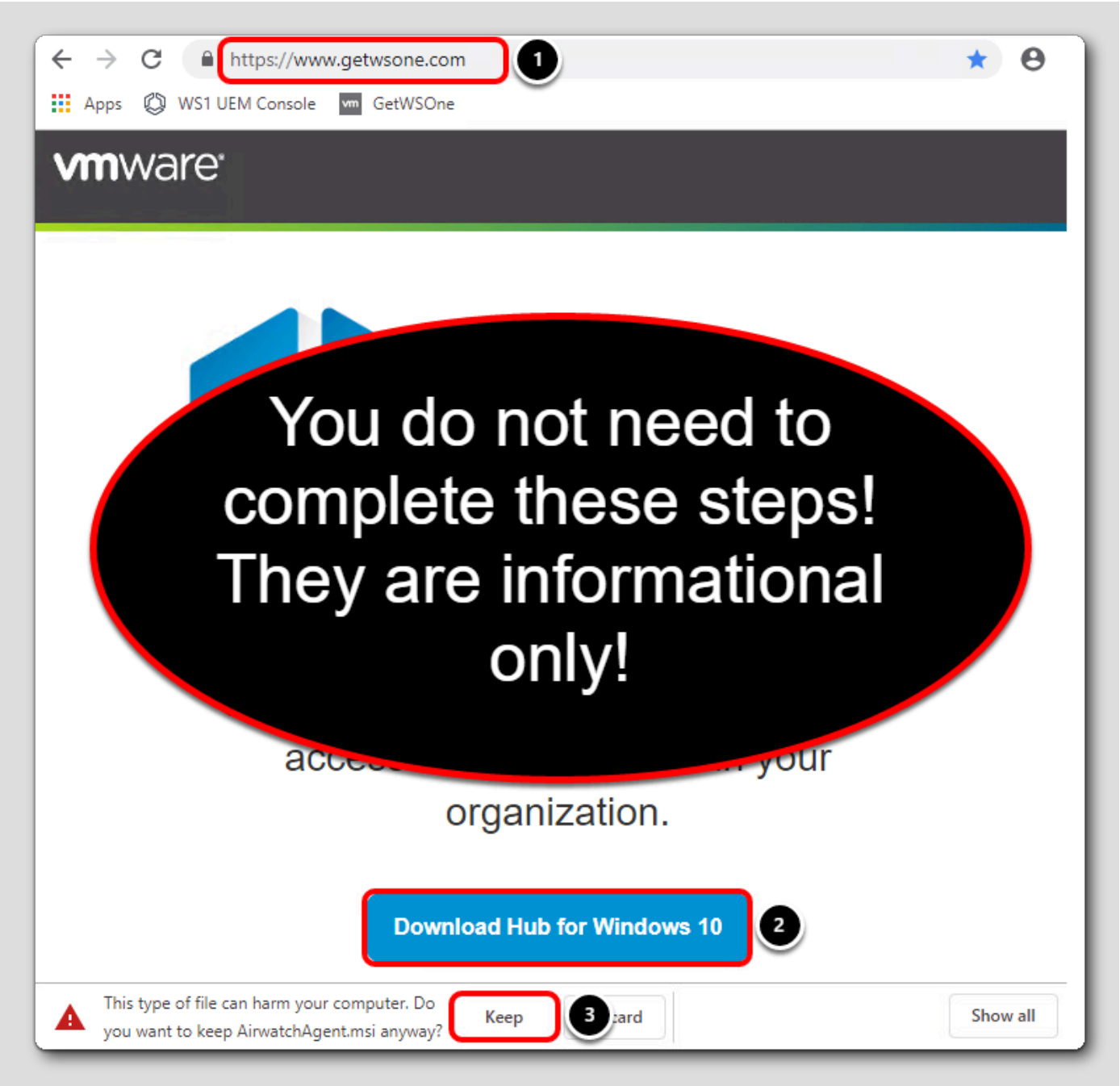
重要：今後の演習で、個人の Windows 10 デバイスを登録しないでください。個人デバイスが他の EMM プロバイダに加入している場合、望ましくない競合や問題が発生する可能性があります。

以降の手順に従って、このハンズオン ラボ用に提供されている Win10-01a 仮想マシンを登録して使用してください。

基本アカウントを使用した Windows 10 デバイスの登録 [25]

次に、Workspace ONE Intelligent Hub アプリケーションを使用して、Workspace ONE UEM に Windows 10 デバイスを登録します。

Workspace ONE Intelligent Hub アプリケーションのダウンロード [26]



注：これらの手順を実行する必要はありません。Workspace ONE Intelligent Hub はすでにダウンロードされています。この手順は単なる情報です。

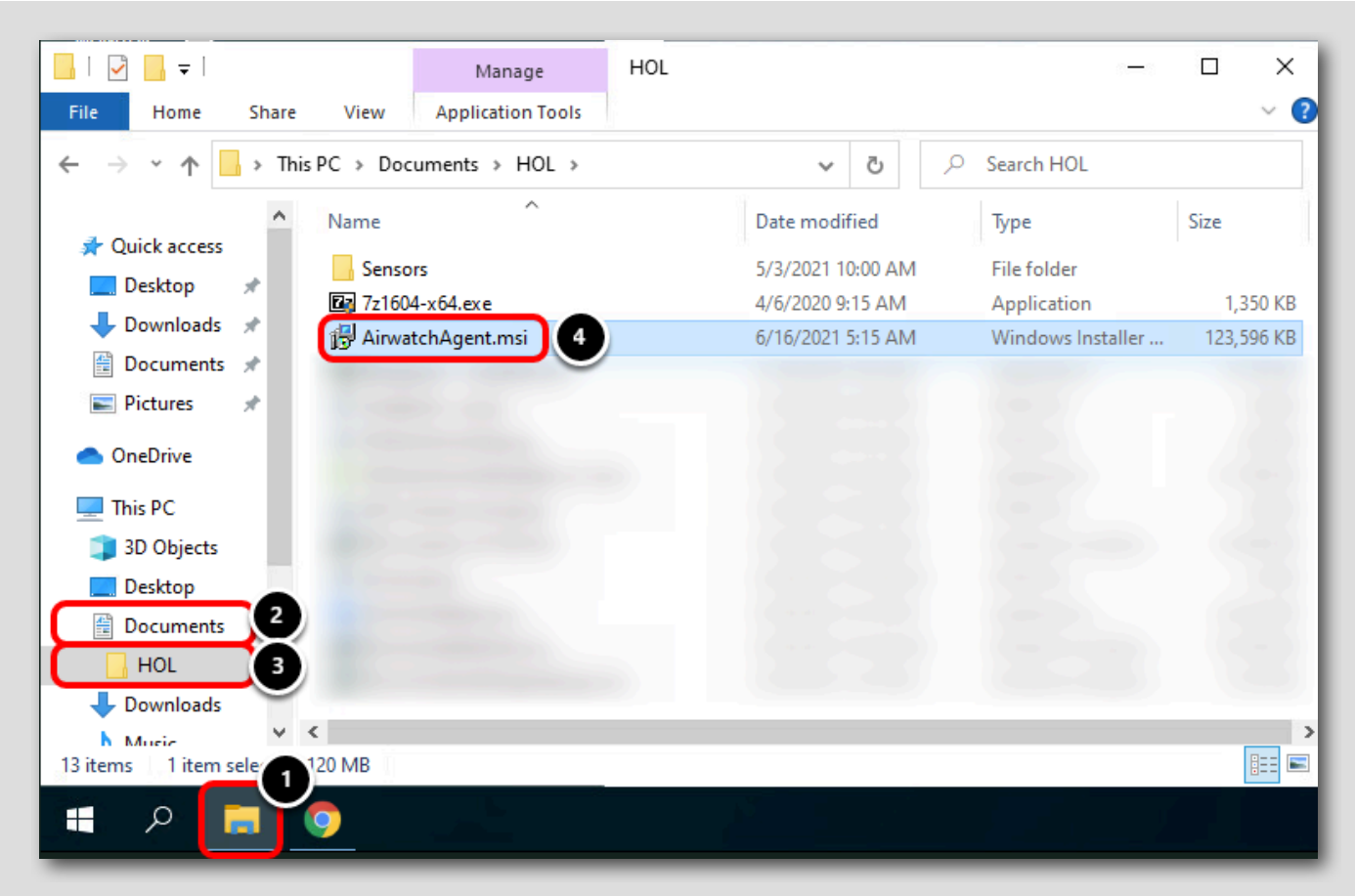
次の手順に従って、現在のプラットフォーム用の最新の Workspace ONE Intelligent Hub アプリケーションをダウンロードできます。

1. ブラウザで **`https://www.getwsone.com`** に移動します。
2. [Download Hub for Windows 10] をクリックします。
3. AirWatchAgent.msi のダウンロードについて警告が表示されたら、[Keep] をクリックします。

便宜上、Workspace ONE Intelligent Hub アプリケーションはすでにダウンロードされています。次の手順に進んで、インストーラを起動します。

Workspace ONE Intelligent Hub インストーラの起動

[27]

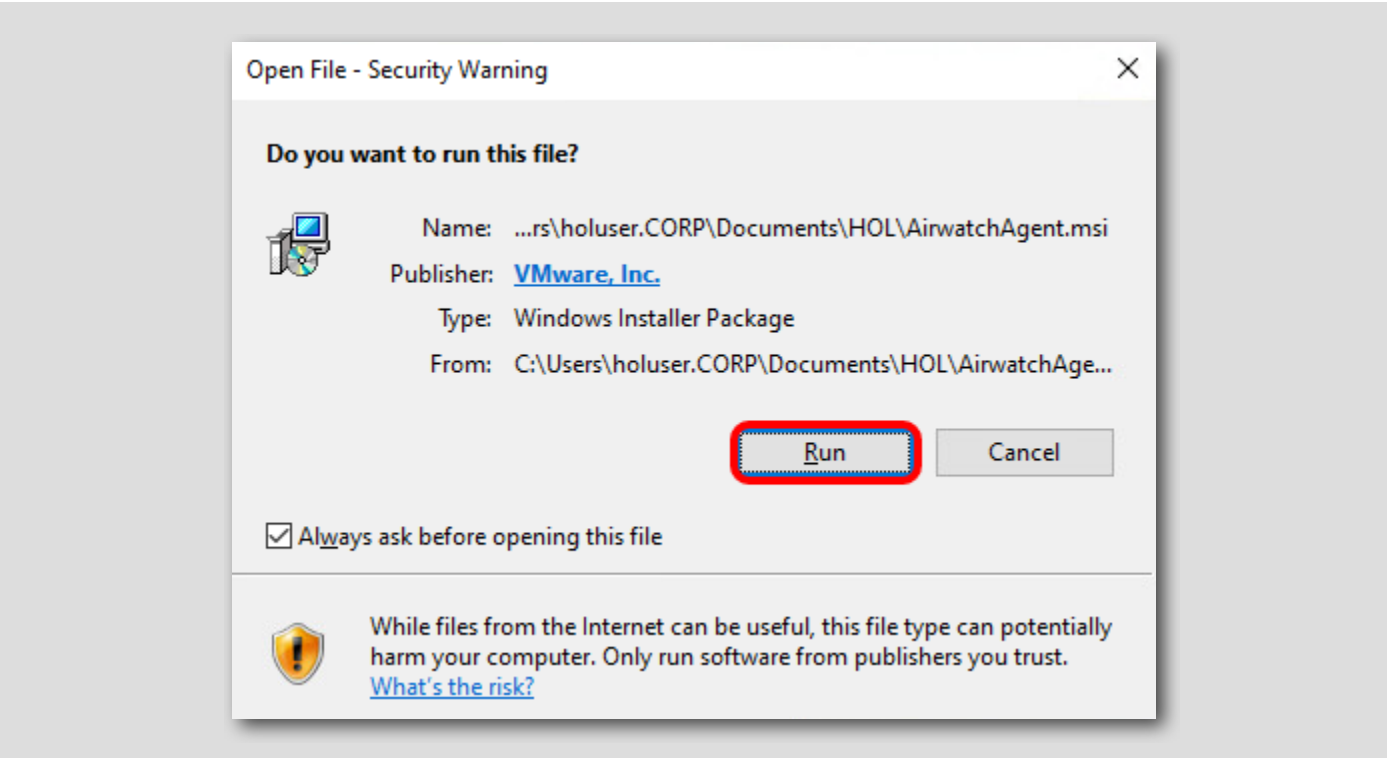


1. タスクバーの [File Explorer] アイコンをクリックします。
2. [Documents] をクリックします。
3. [HOL] をクリックします。
4. AirwatchAgent.msi ファイルをダブルクリックして、インストーラを起動します。

注：インストーラが起動するまでに数秒かかる場合があります。AirwatchAgent.msi ファイルをクリックして、しばらくお待ちください。

[Run] のクリック

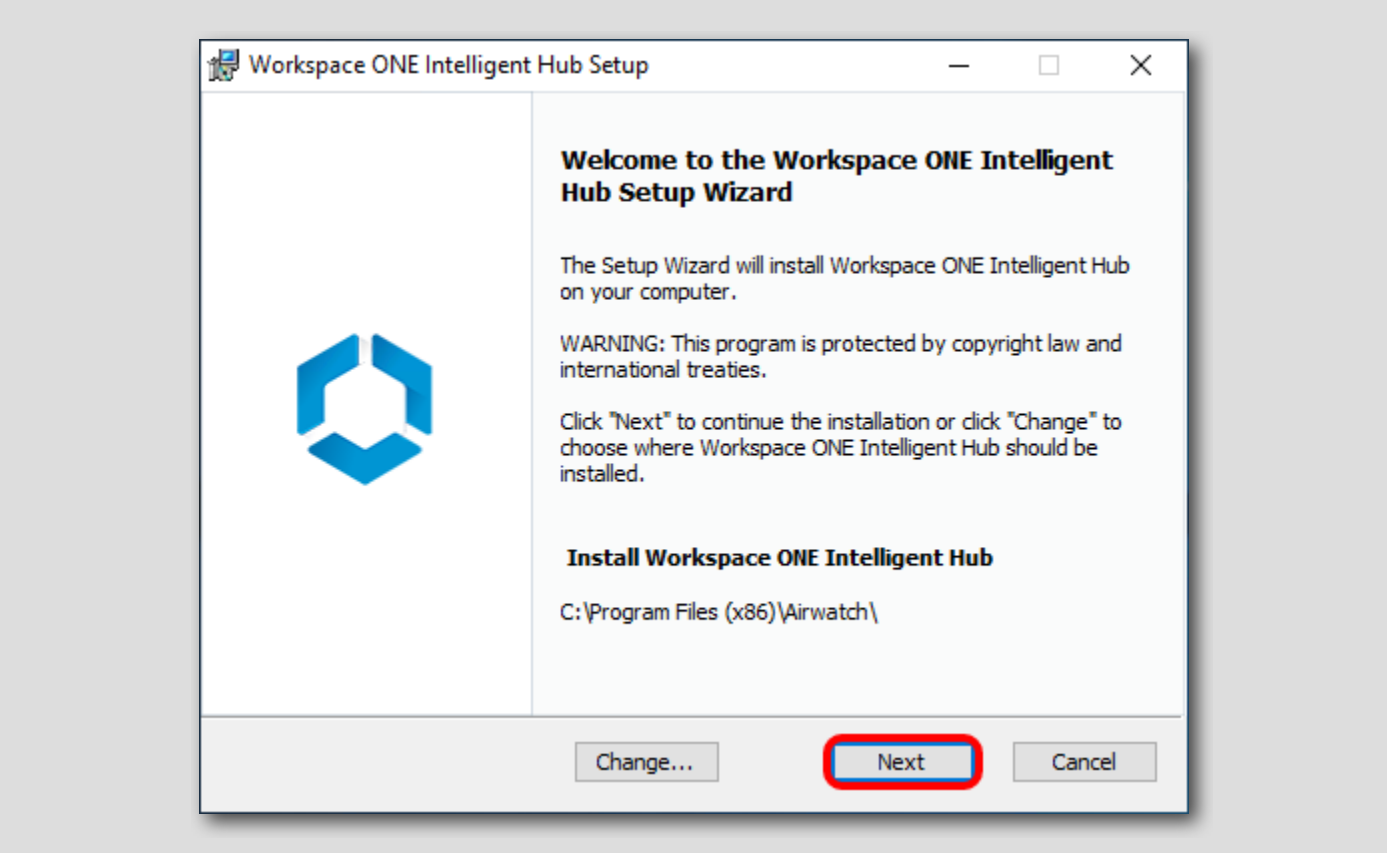
[28]



[Run] をクリックして、インストールを続行します。

デフォルトのインストール場所の受け入れ

[29]

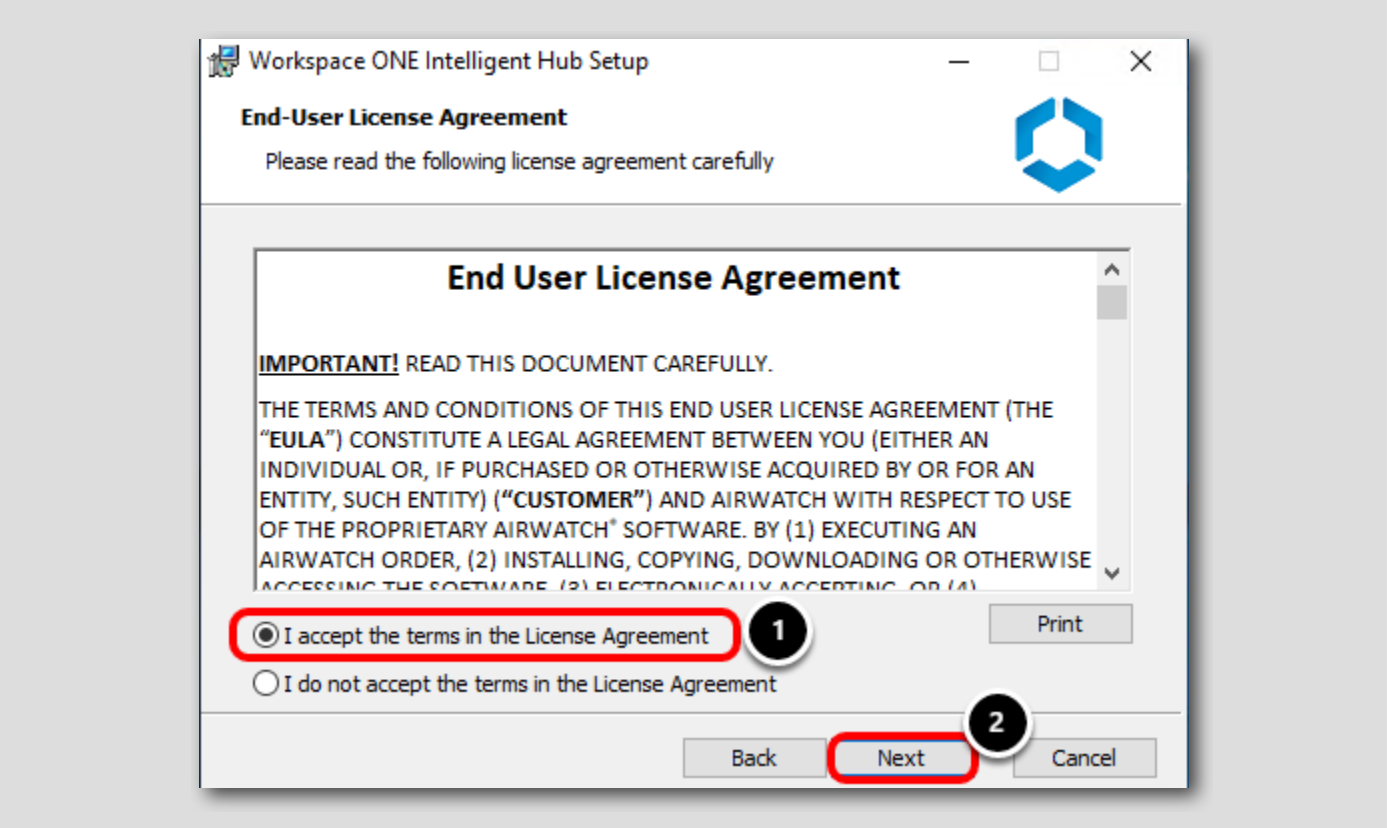


インストール場所はデフォルトのまま、[Next] をクリックします。

注：必要な追加機能がインストールされ、[Next] ボタンが有効になるまで数秒かかる場合があります。

使用許諾契約書への同意

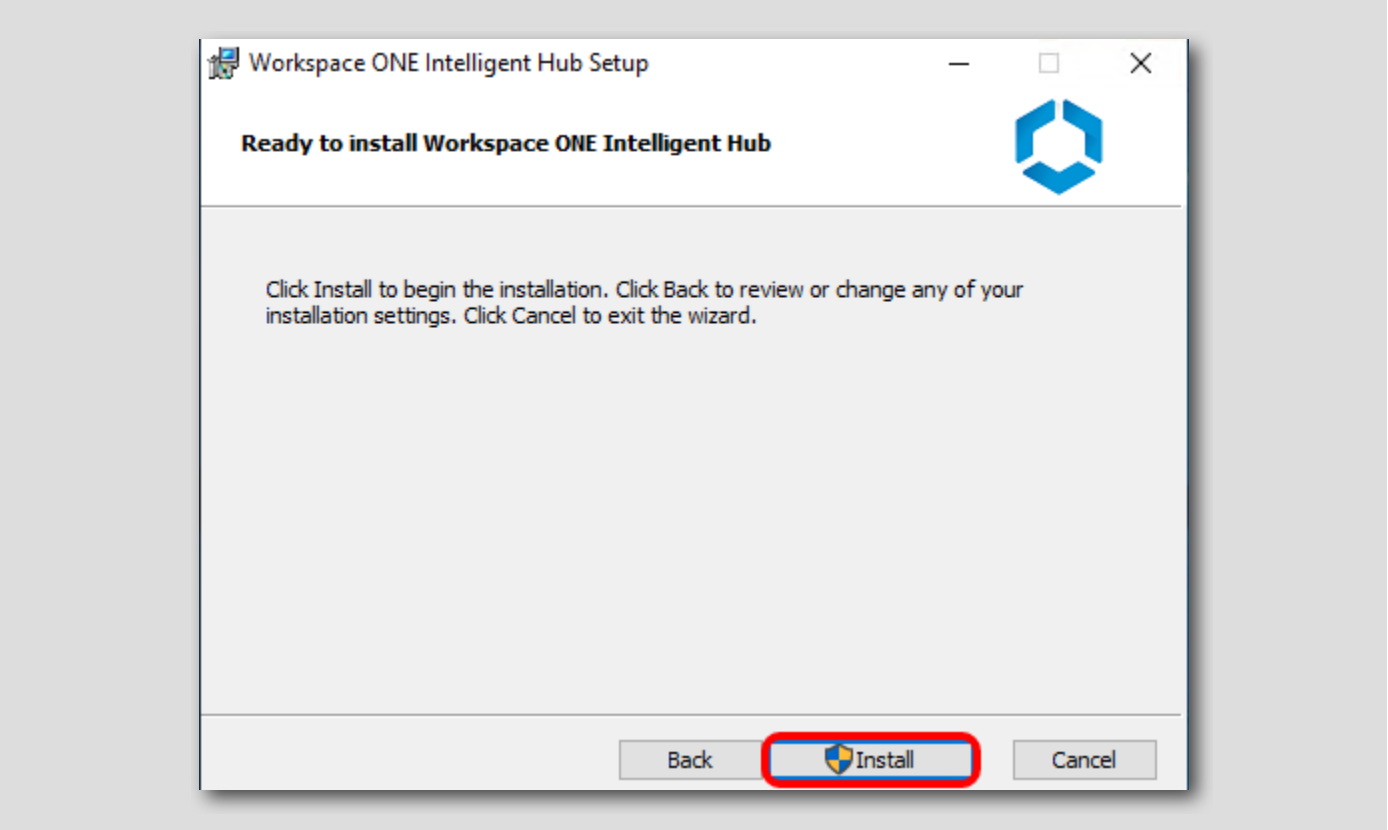
[30]



1. [I accept the terms of the License Agreement] を選択します。
2. [Next] をクリックします。

Workspace ONE Intelligent Hub のインストールの開始

[31]

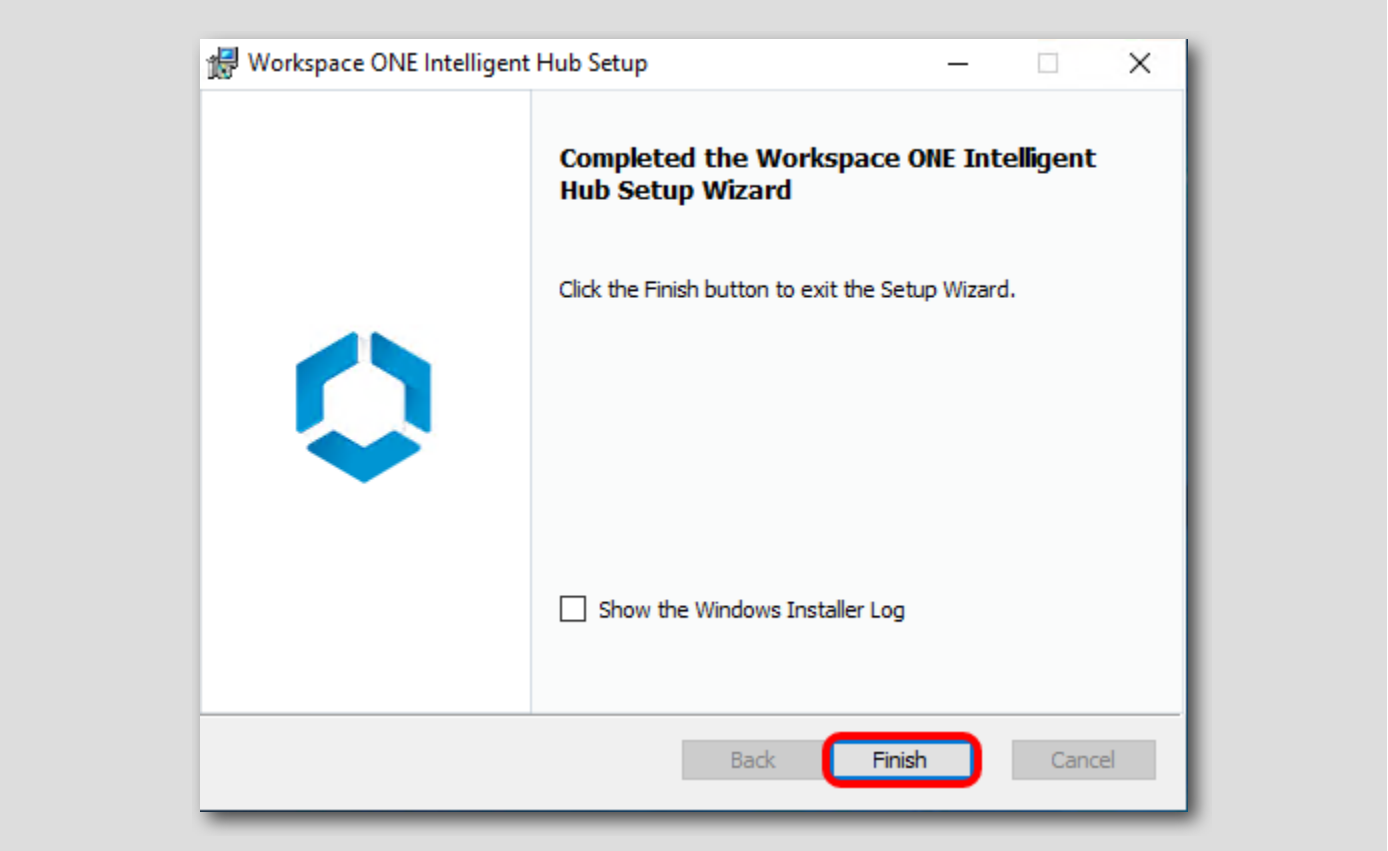


[Install] をクリックして、インストーラを開始します。

注：VMware Workspace ONE Intelligent Hub のインストールは完了までに数分かかる場合があります。インストーラを中断しないようにしてください。

Workspace ONE Intelligent Hub インストーラの完了

[32]



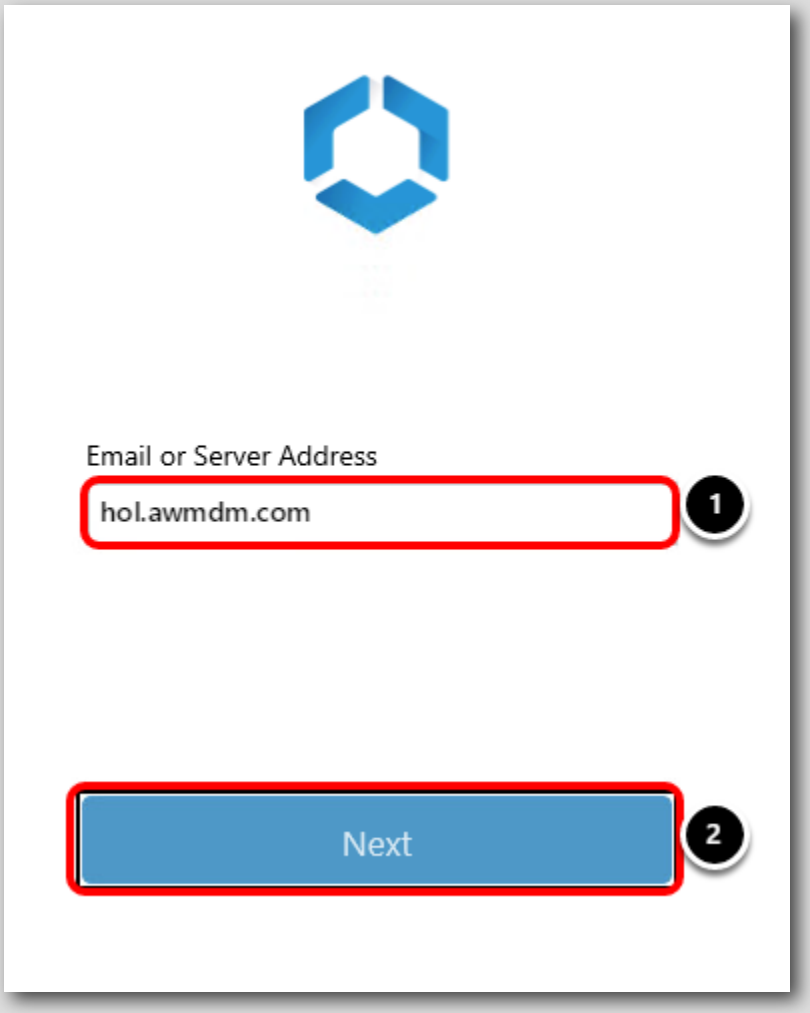
注：インストーラの完了には数分かかる場合があります。続行する前に、インストールの完了画面が表示されるまでお待ちください。

[Finish] をクリックして、Workspace ONE Intelligent Hub インストーラを完了します。

注：[Finish] をクリックすると Native Enrollment アプリケーションが起動し、Workspace ONE UEM への登録手順が表示されます。Intelligent Hub の起動には、約 2 ～ 3 分かかります。

Workspace ONE Intelligent Hub を使用した Windows 10 デバイスの登録

[33]

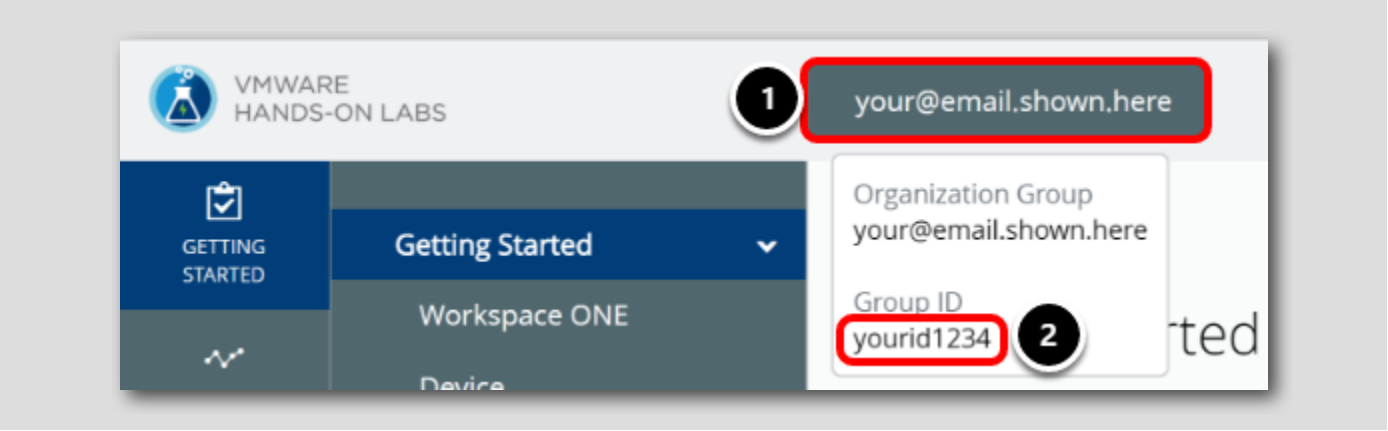


注：前の手順で [Finish] をクリックした後、上記の画面が表示されるまでに 2 ～ 3 分かかることがあります。

1. [Server Address] に **`hol.awmdm.com`** と入力します。
2. [Next] をクリックします。

Workspace ONE UEM Console からのグループ ID の特定

[34]

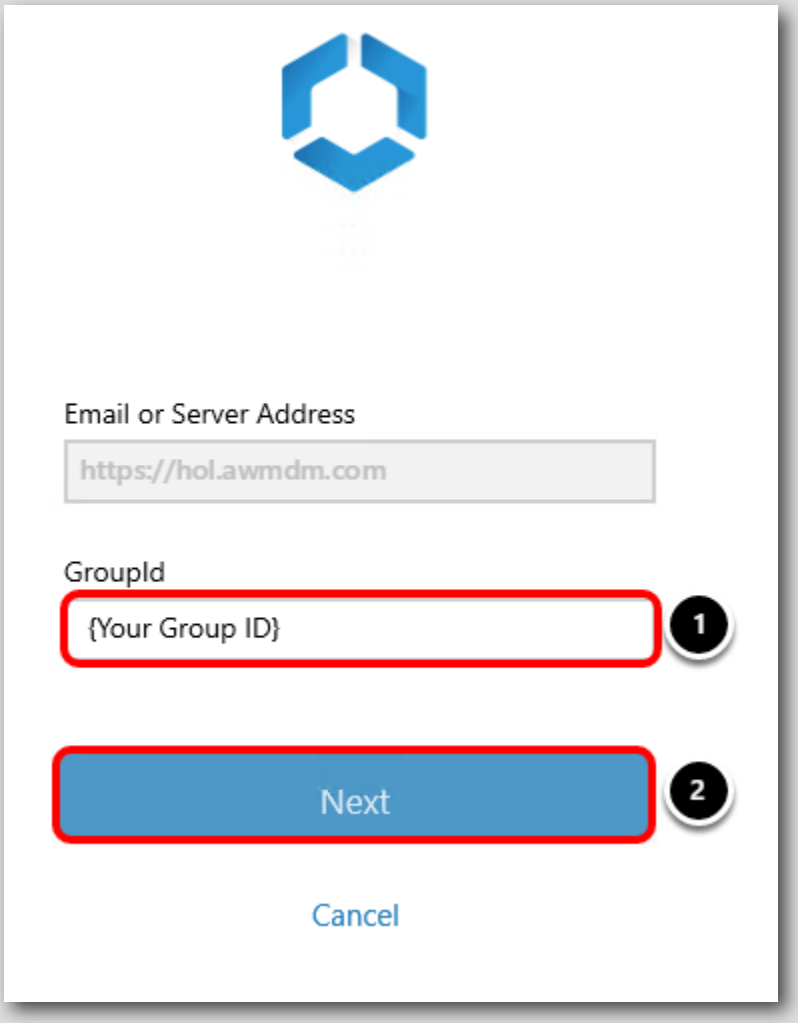


次の手順では、[Organization Group ID] を取得します。

1. グループ ID を確認するには、Workspace ONE UEM 管理コンソールに戻って、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. グループ ID は [Organization Group] ポップアップの最下部に表示されます。この値をコピーします。

グループ ID の入力

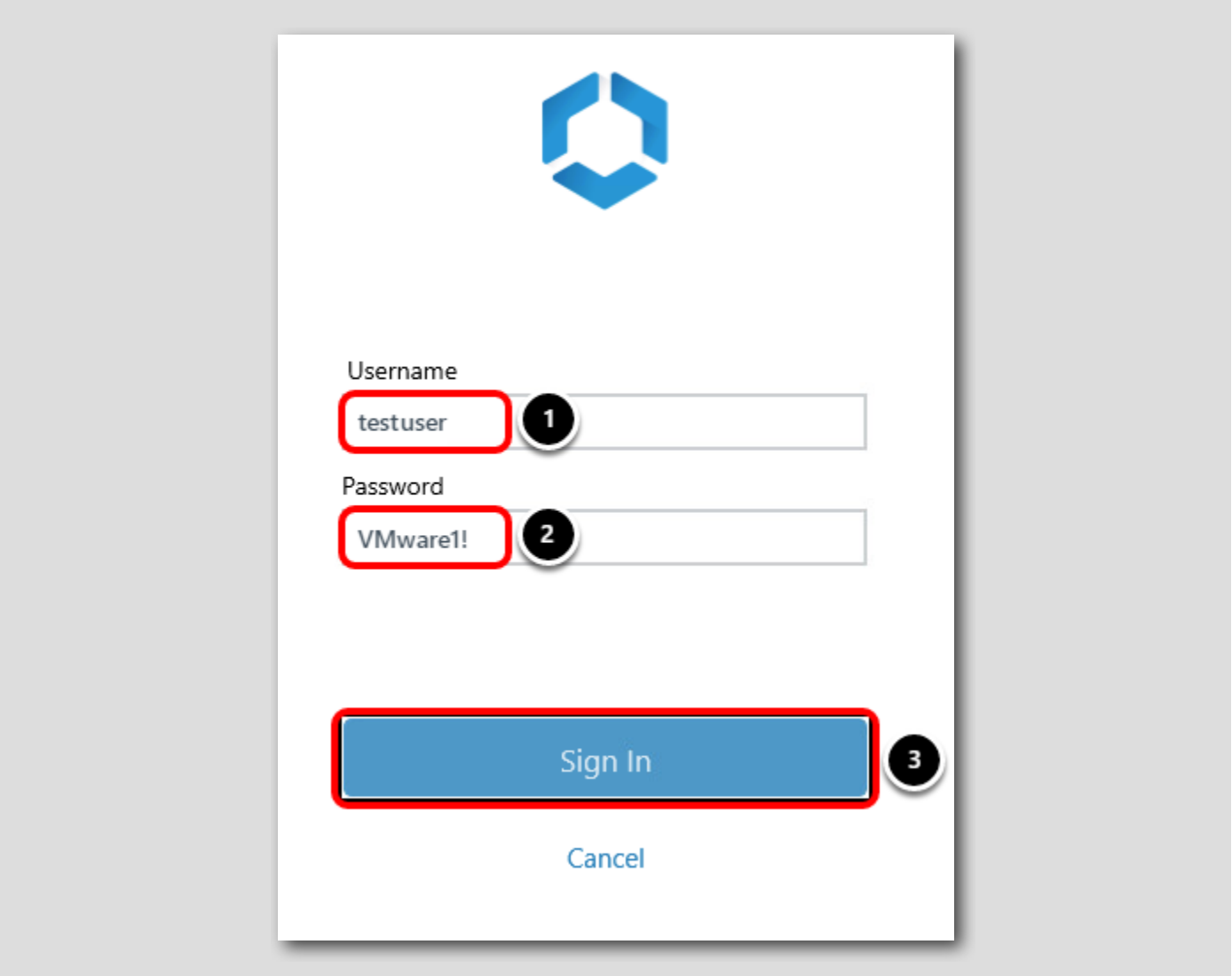
[35]



1. [Group ID] フィールドにグループ ID を入力します。グループ ID を忘れた場合は、前の手順で取得方法を確認してください。
2. [Next] をクリックします。

ユーザー認証情報の入力

[36]

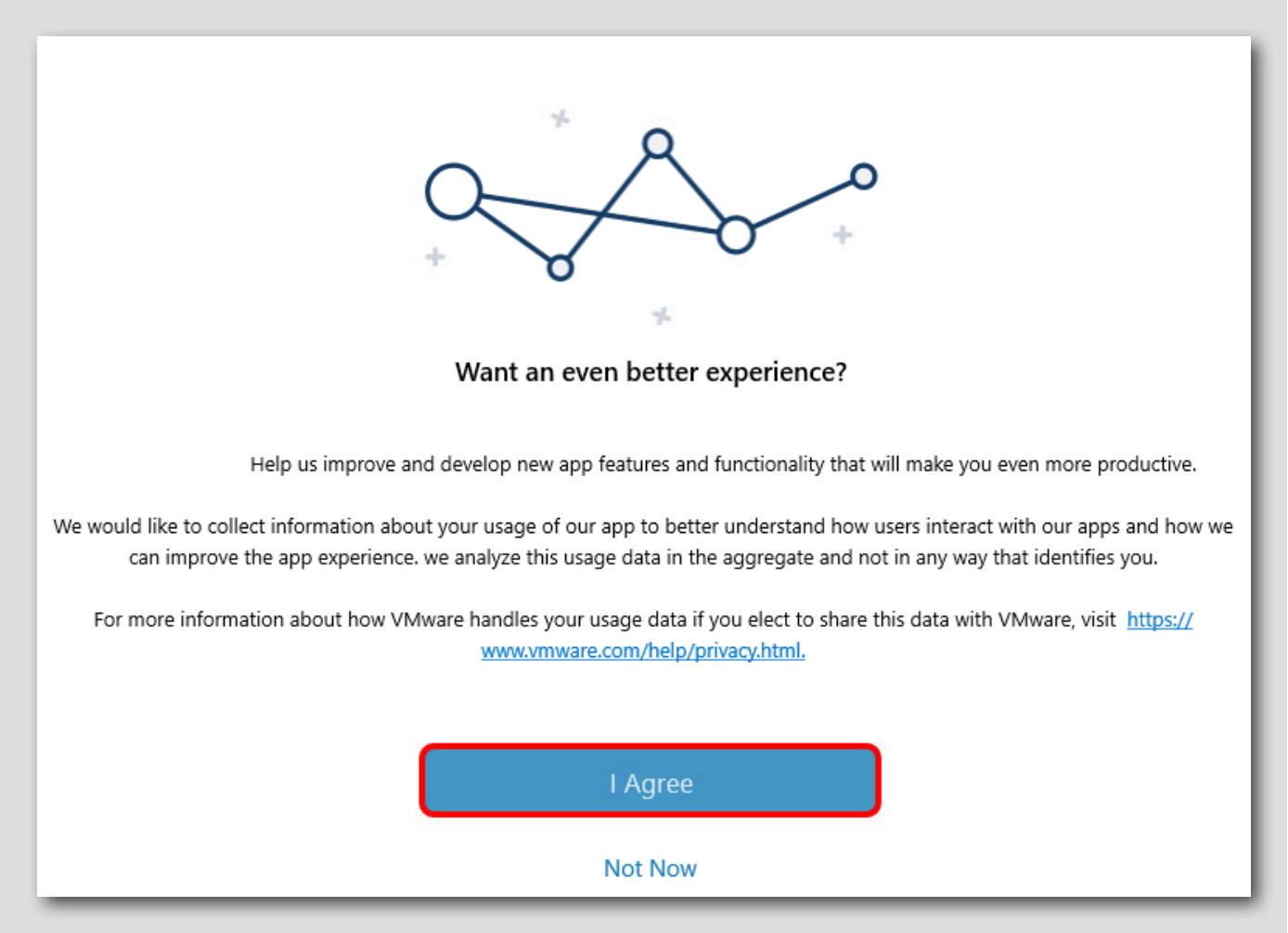


1. [Username] フィールドに **testuser** と入力します。
2. [Password] フィールドに **VMware1!** と入力します。
3. [Sign In] をクリックします。

注：サーバが登録の詳細を確認するまでしばらくお待ちください。これには数分かかる場合があります。

データ ポリシーの承諾

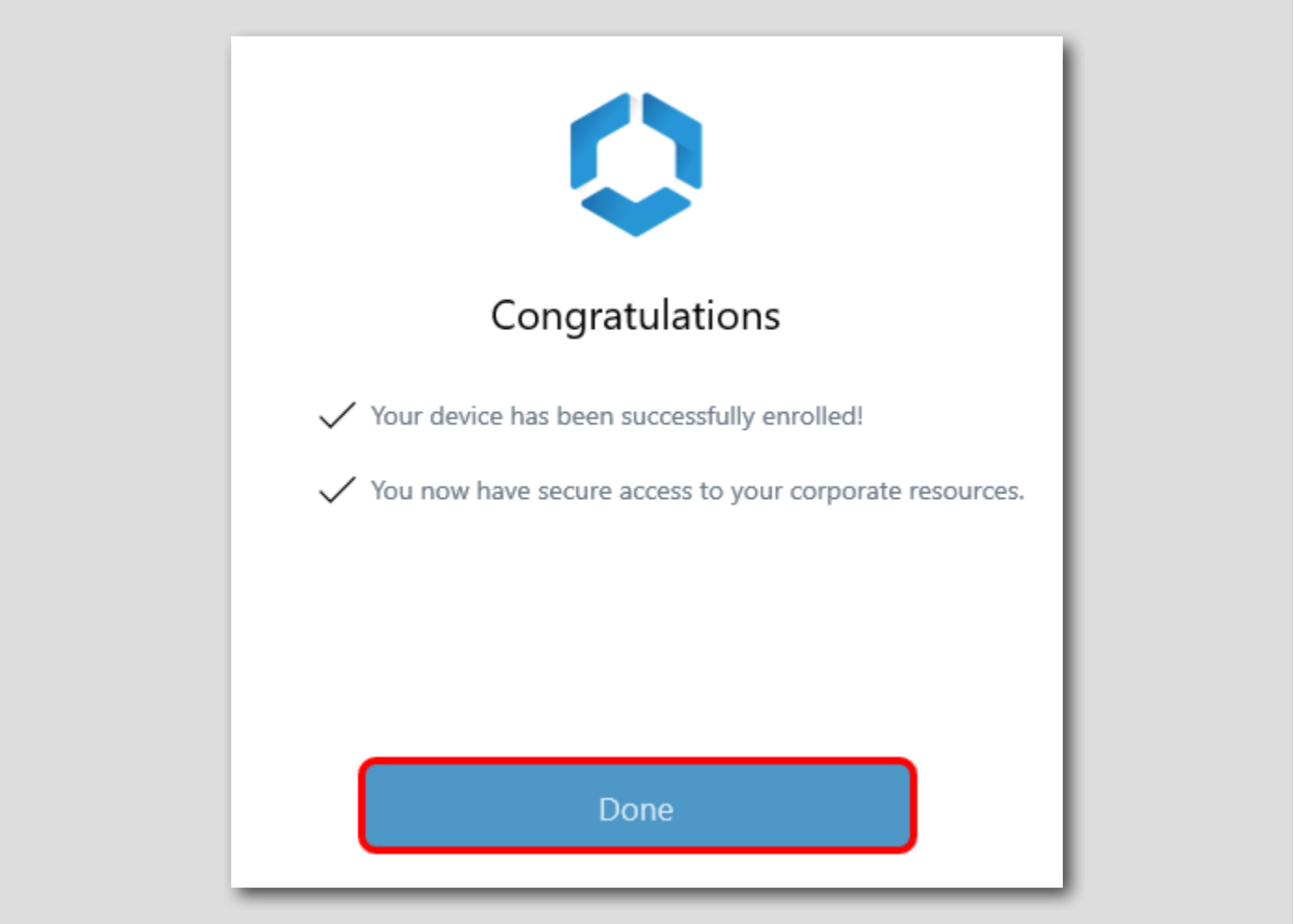
[37]



[I Agree] をクリックします。

Workspace ONE UEM 登録プロセスの終了

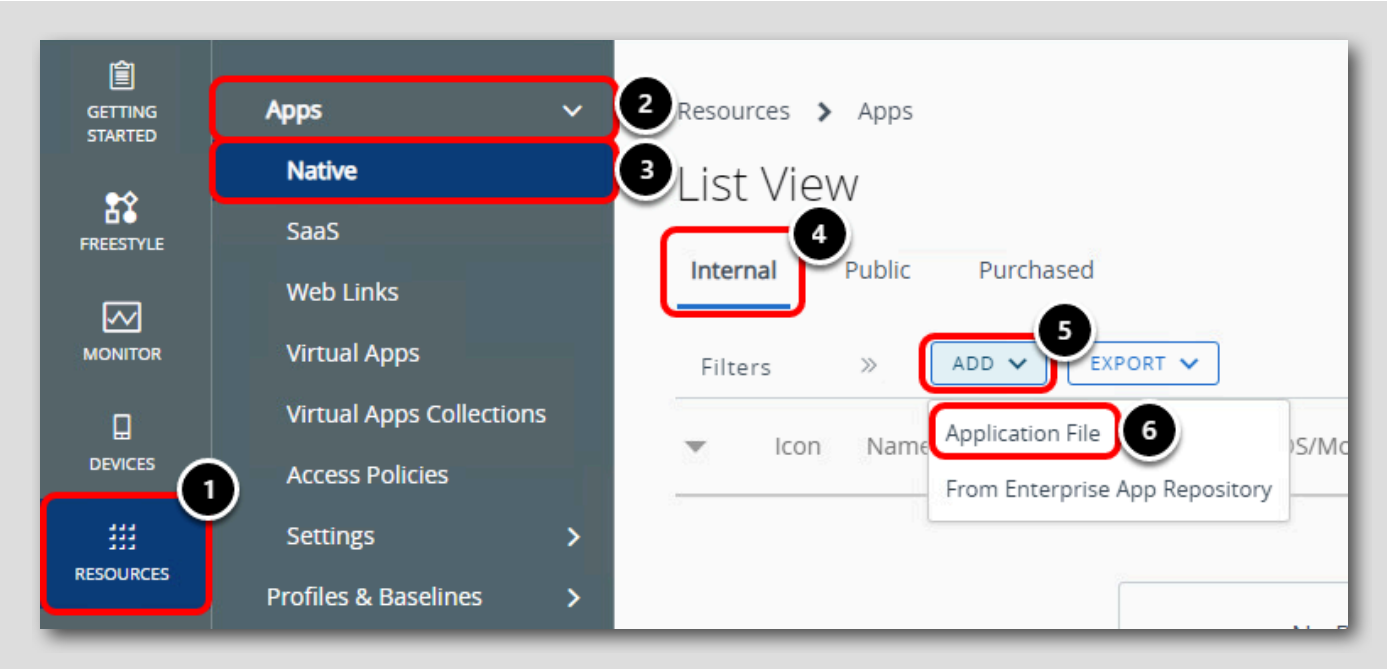
[38]



[Done] をクリックして登録プロセスを終了します。これで、Windows 10 デバイスは Workspace ONE UEM に正常に登録されました。

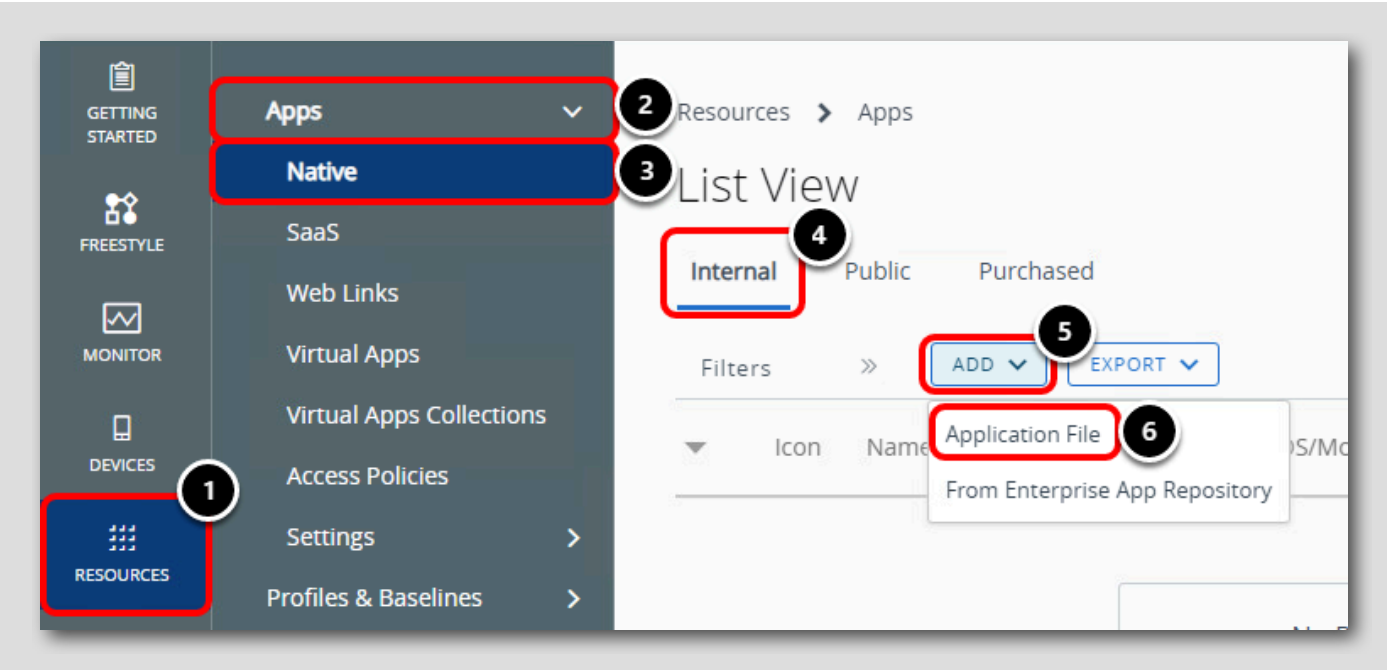
Zoom Client for Meetings アプリケーション（社内アプリケーション）の構成

[39]

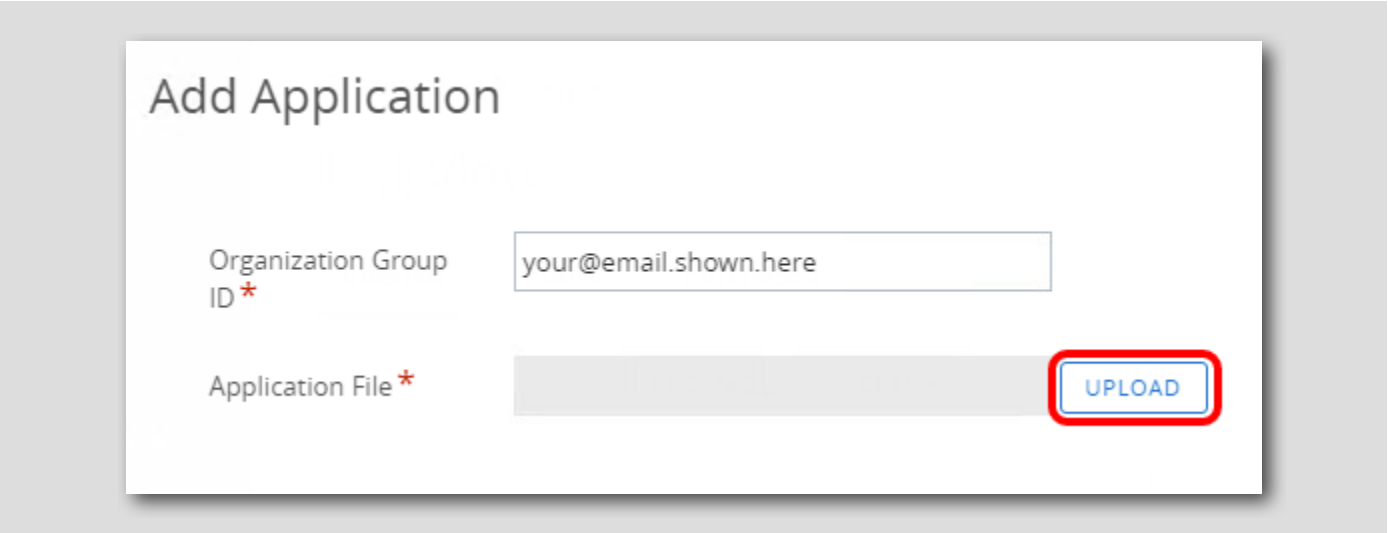


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Apps] を展開します。
3. [Native] をクリックします。
4. [Internal] タブを選択します。
5. [Add] をクリックします。
6. [Application File] をクリックします。

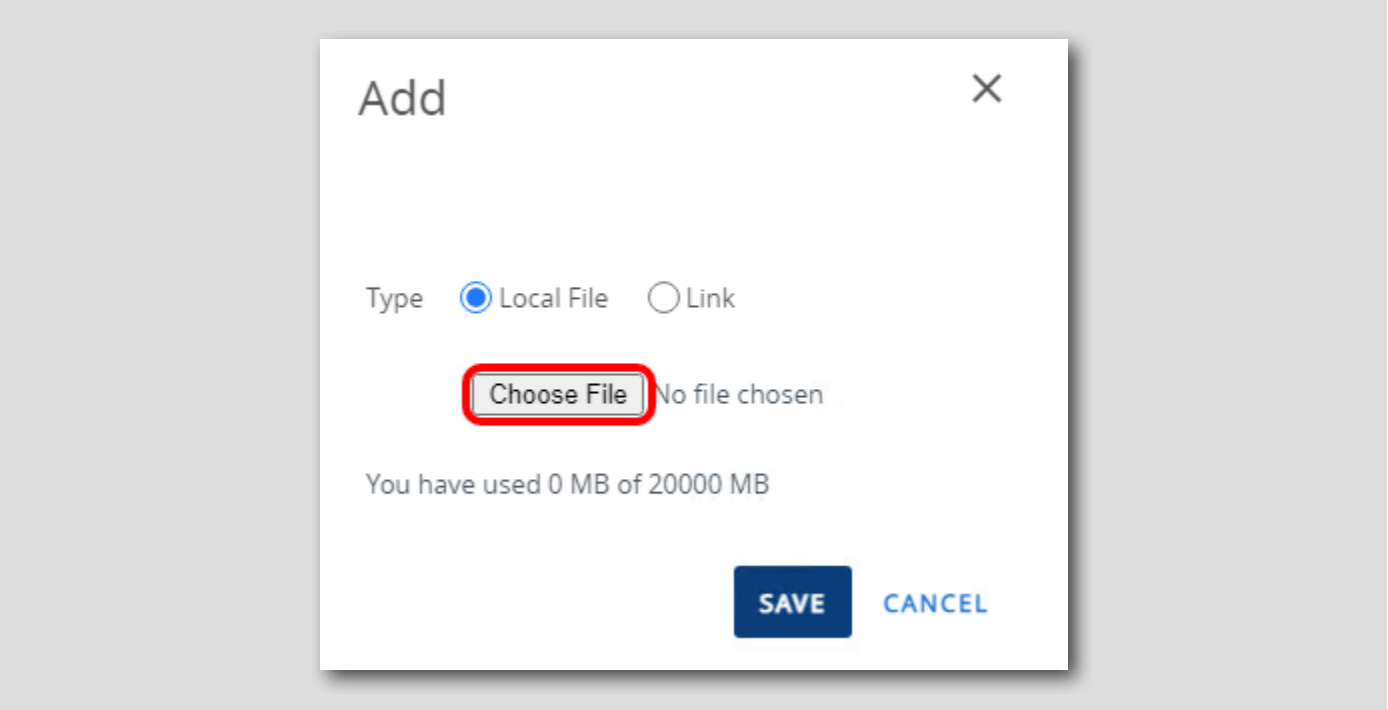


Zoom Client for Meetings アプリケーションのアップロード [40]



[Upload] をクリックします。

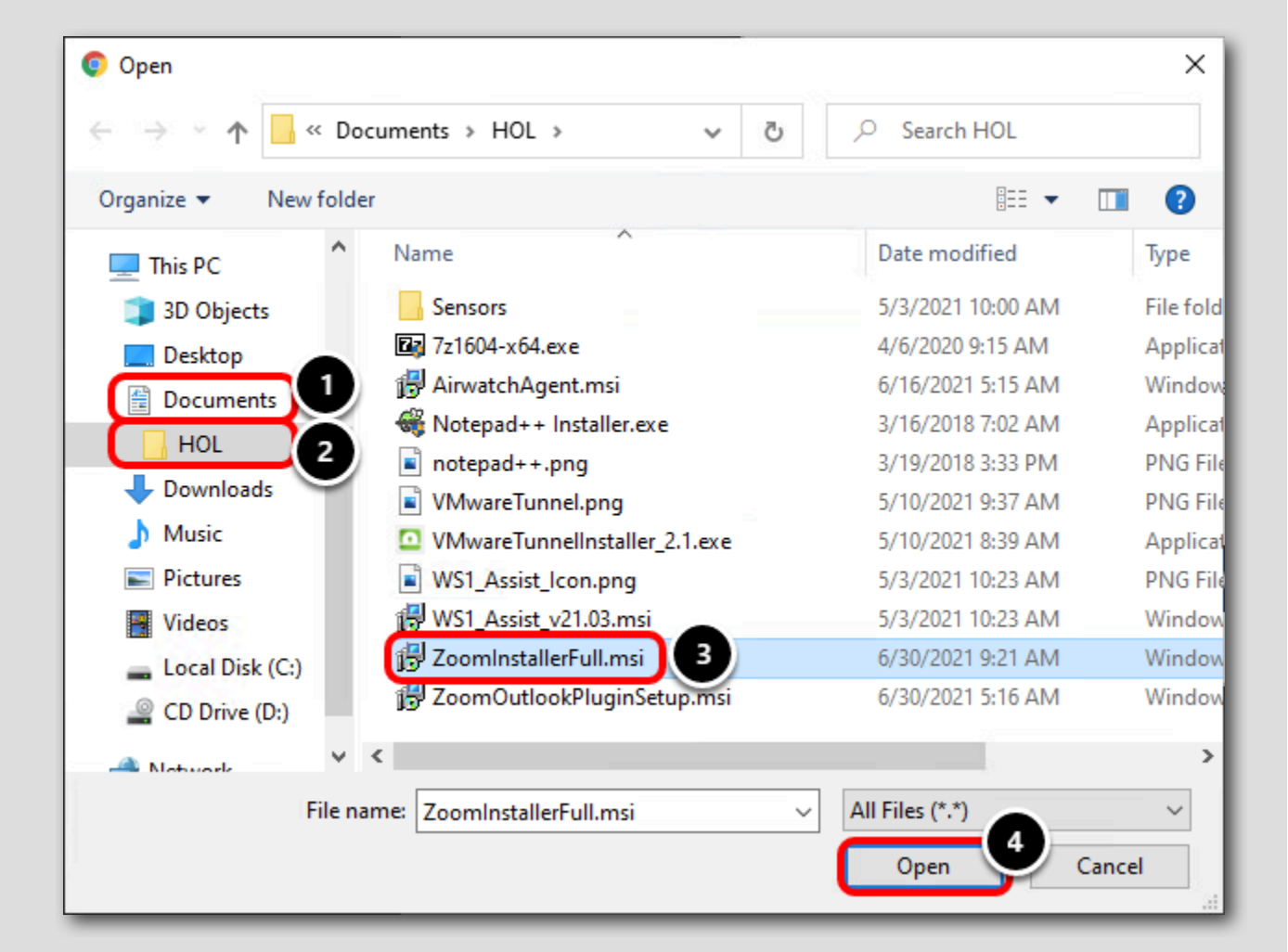
アップロードするファイルの選択 [41]



[Choose File] をクリックします。

ZoomInstallerFull.msi ファイルの選択

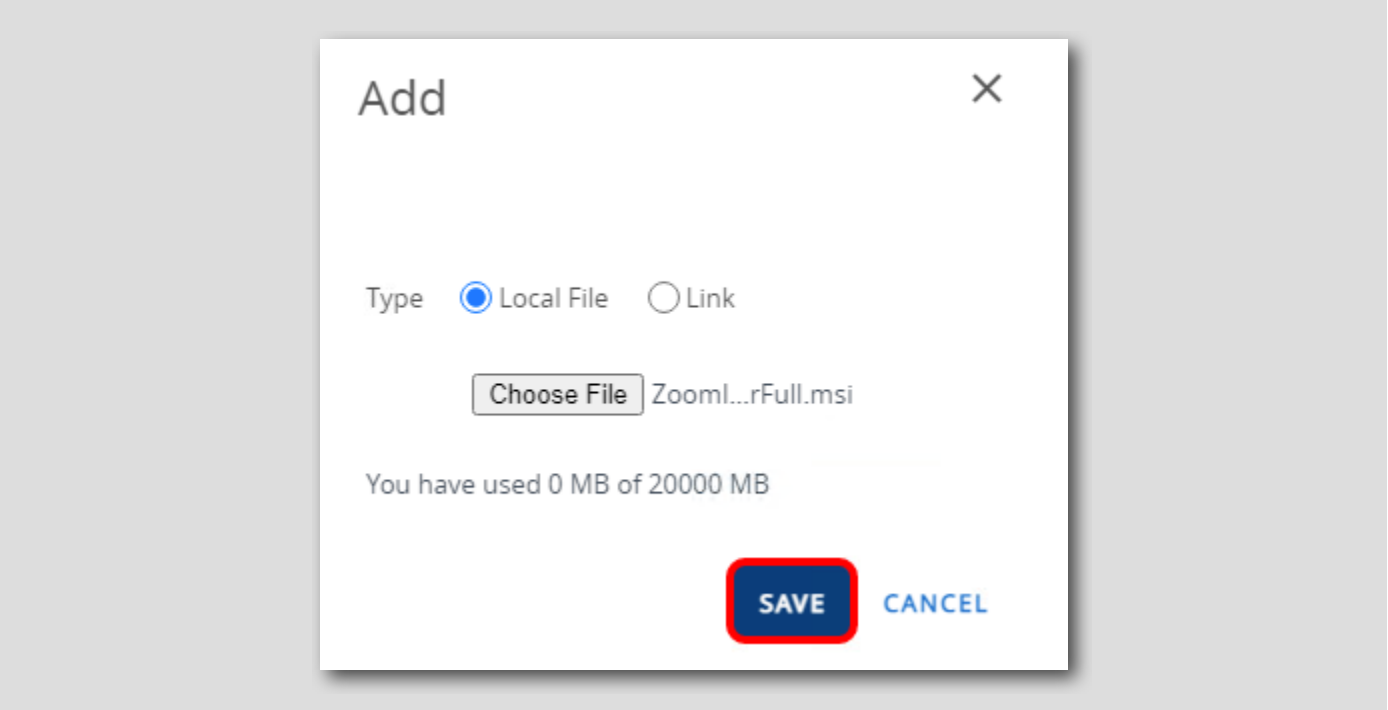
[42]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [ZoomInstallerFull.msi] をクリックします。
4. [Open] をクリックします。

ZoomInstallerFull.msi ファイルの保存

[43]

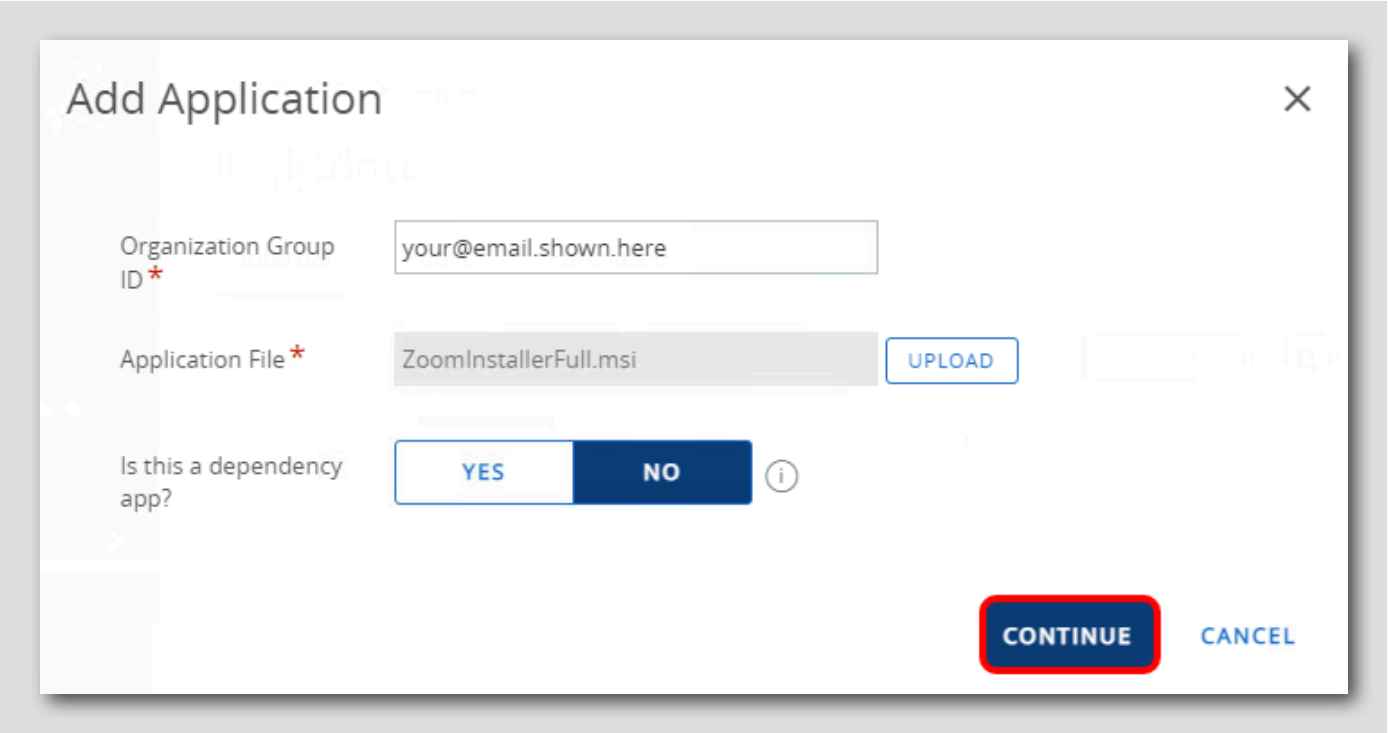


[Save] をクリックして、選択した ZoomInstallerFull.msi ファイルをアップロードします。

注：アプリケーションのアップロードが完了するまで数分かかる場合があります。アップロードが完了したら、次の手順に進みます。

Zoom Client for Meetings アプリケーションの追加（続き）

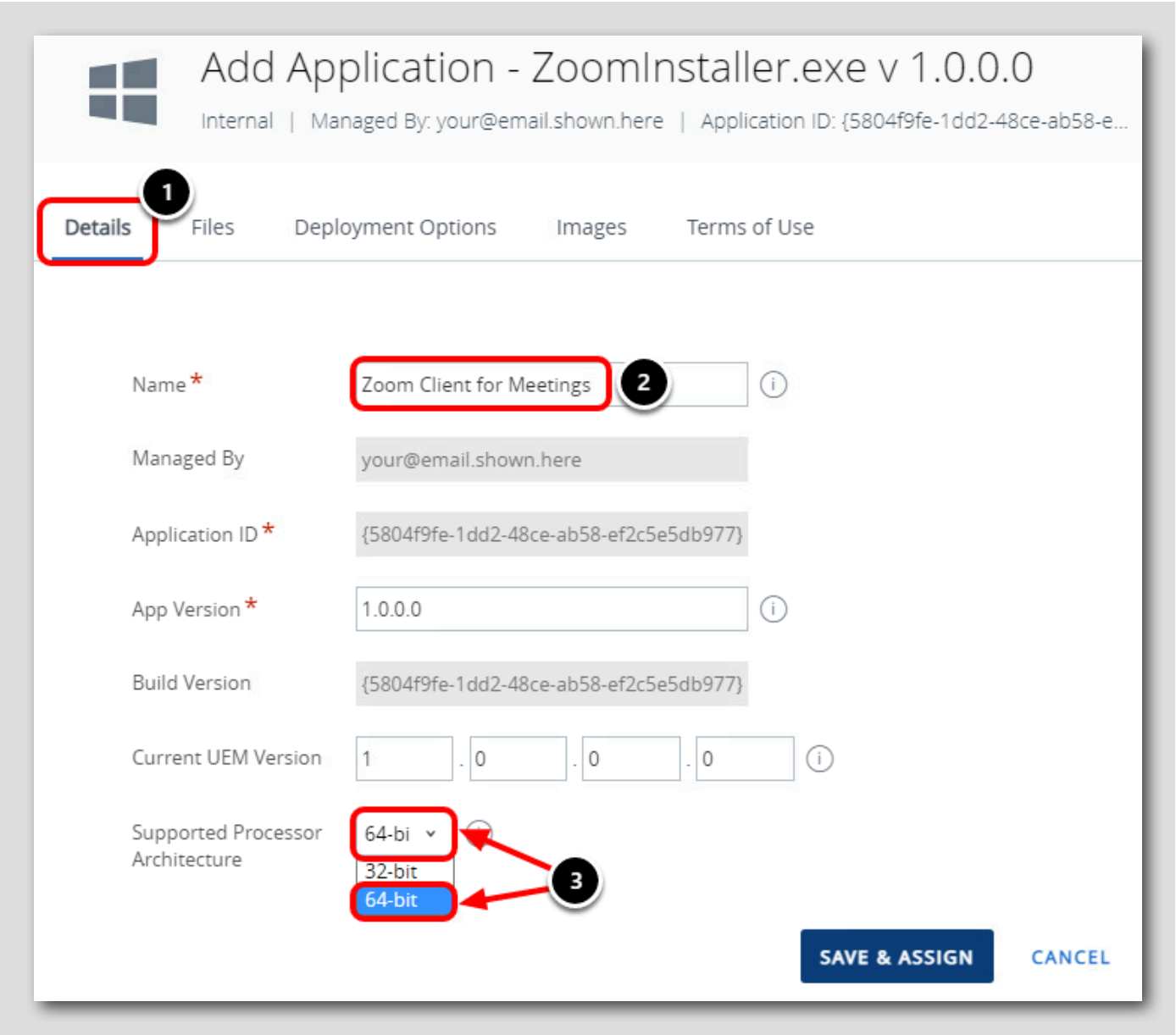
[44]



[Continue] をクリックします。

Zoom Client for Meetings アプリケーションの構成

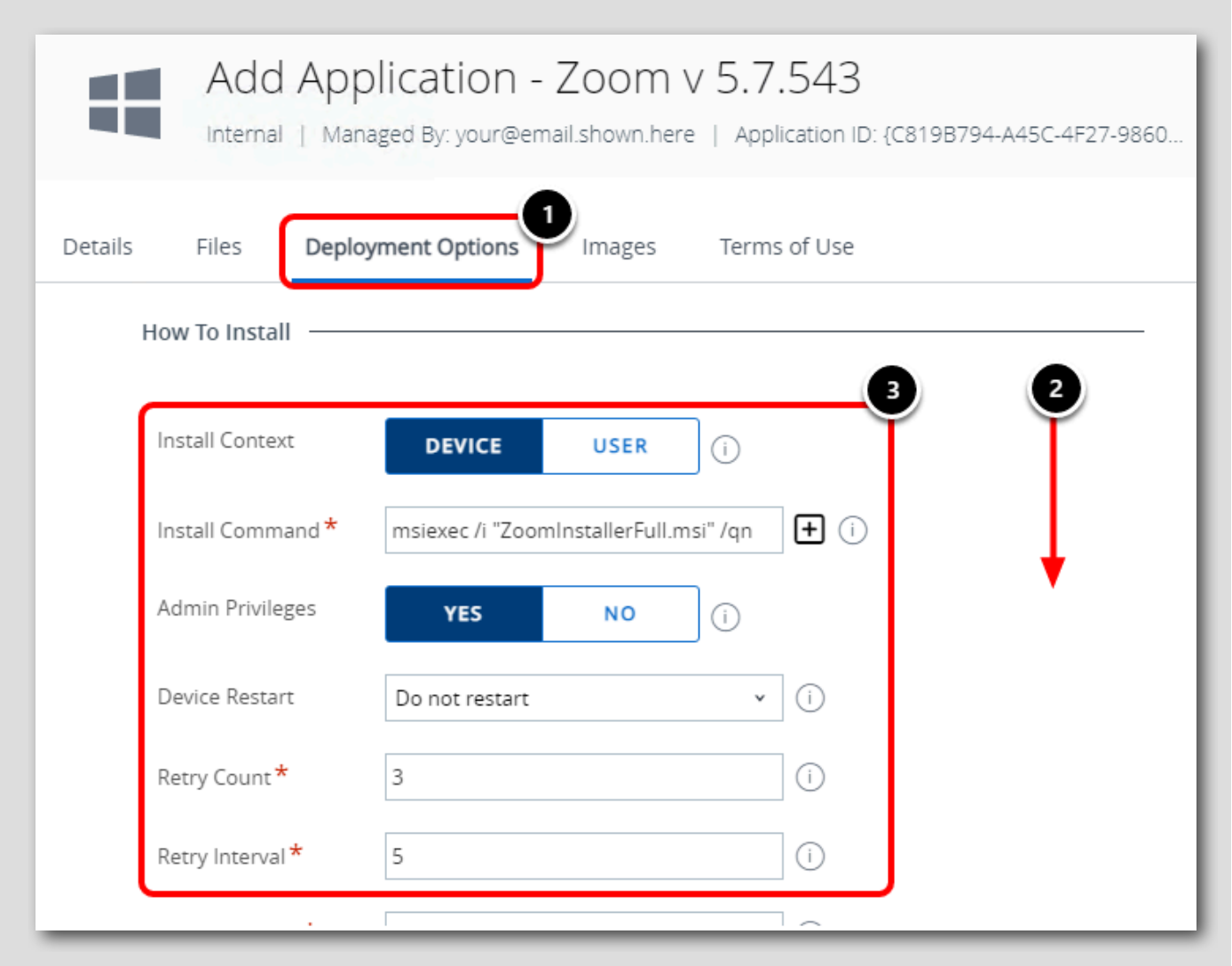
[45]



1. [Details] タブをクリックします。
2. 名前を **`Zoom Client for Meetings`** に更新します。この名前は、エンド ユーザーのデバイスおよびアプリケーション カタログのアプリケーション名になります。
3. サポートされているプロセス アーキテクチャを [64-bit] に更新します。

展開オプションの確認

[46]

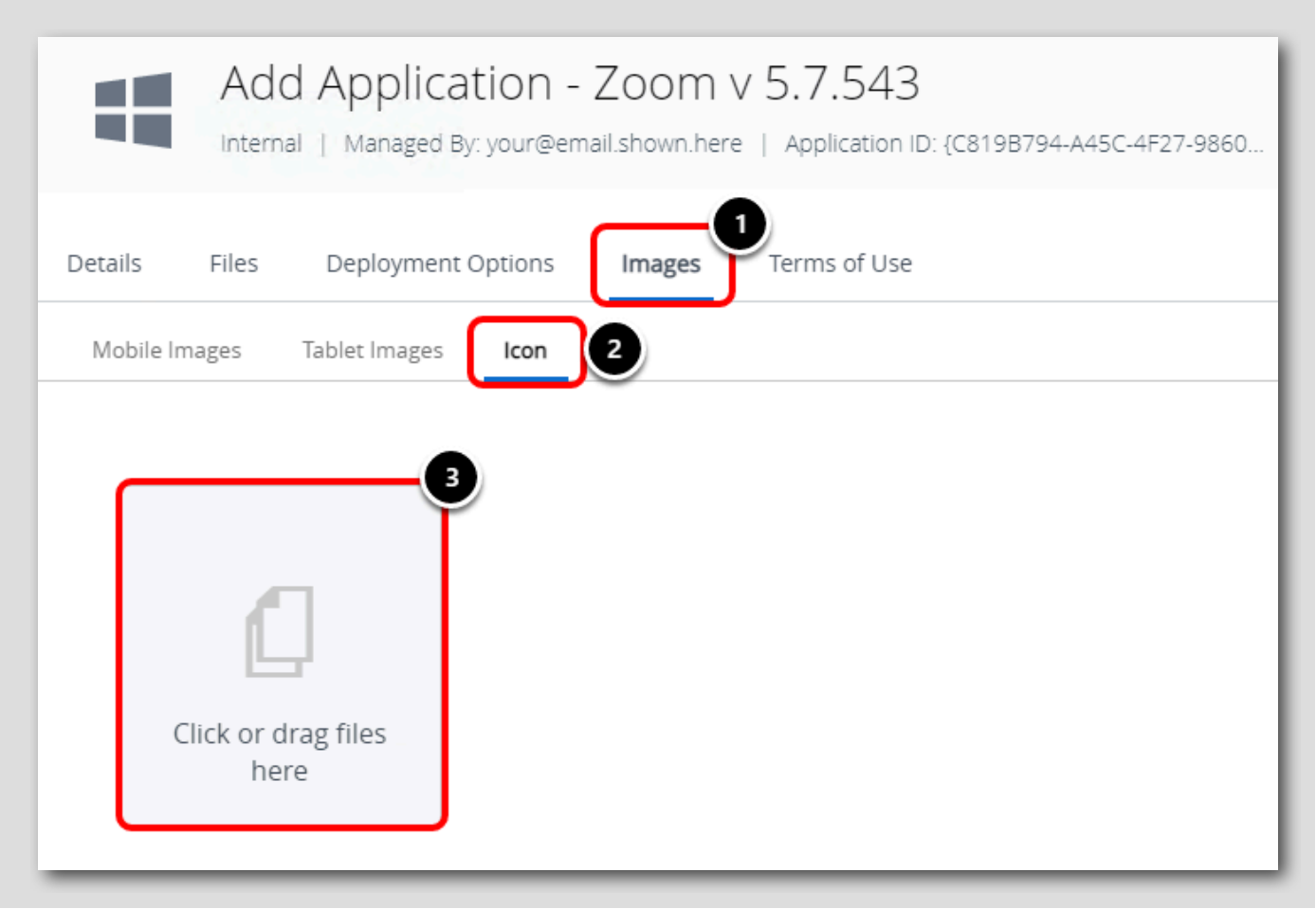


1. [Deployment Options] タブをクリックします。
2. [How To Install] 設定まで下にスクロールします。
3. [Install Command] などの [How To Install] 設定はすでに完了しています。これらの詳細は、アップロードされた MSI から抽出されました。

次の手順に進んでください。

アイコンの構成

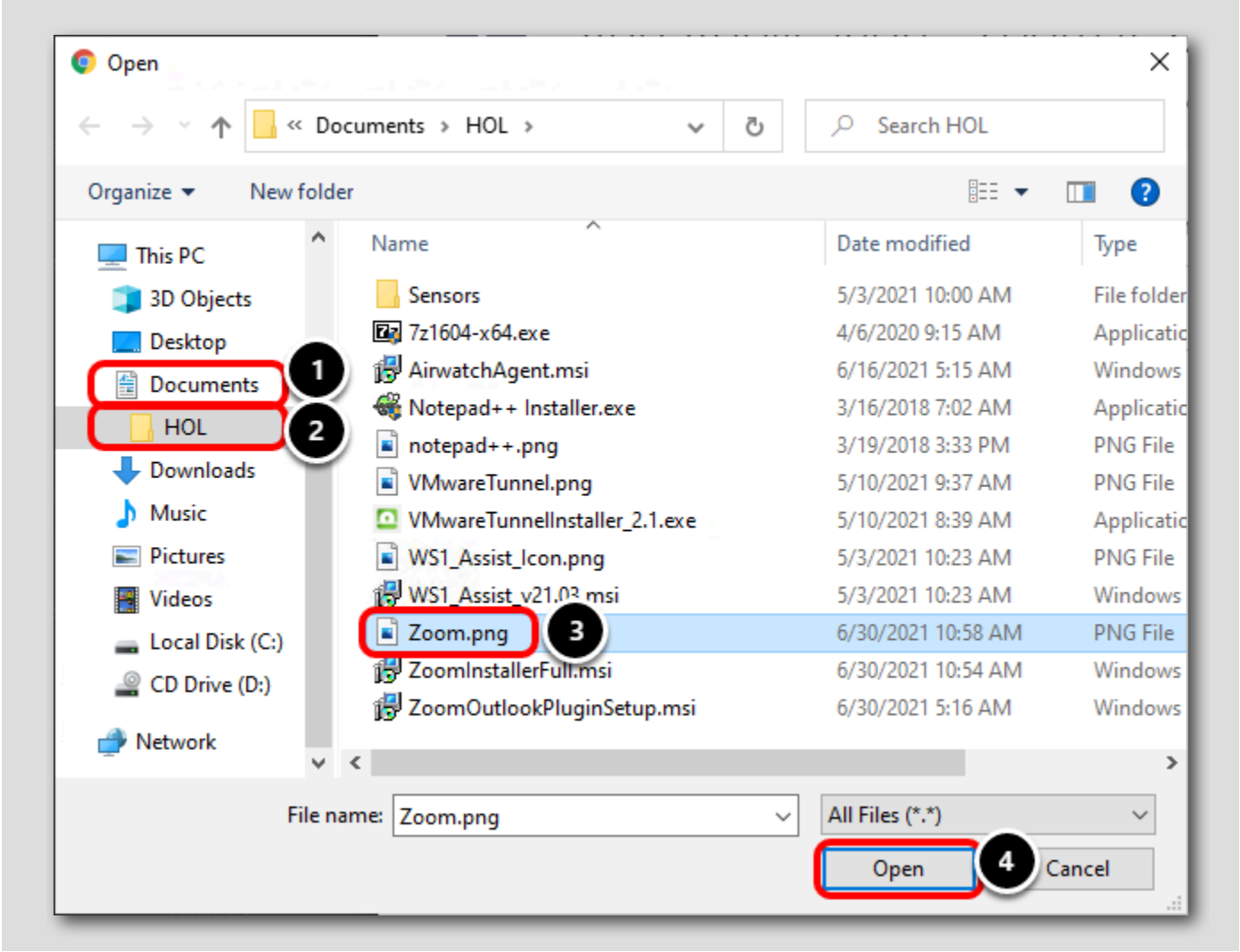
[47]



1. [Images] タブをクリックします。
2. [Icon] タブをクリックします。
3. [Click or drag files here] というラベルの付いた領域をクリックします。

Zoom.png ファイルの選択

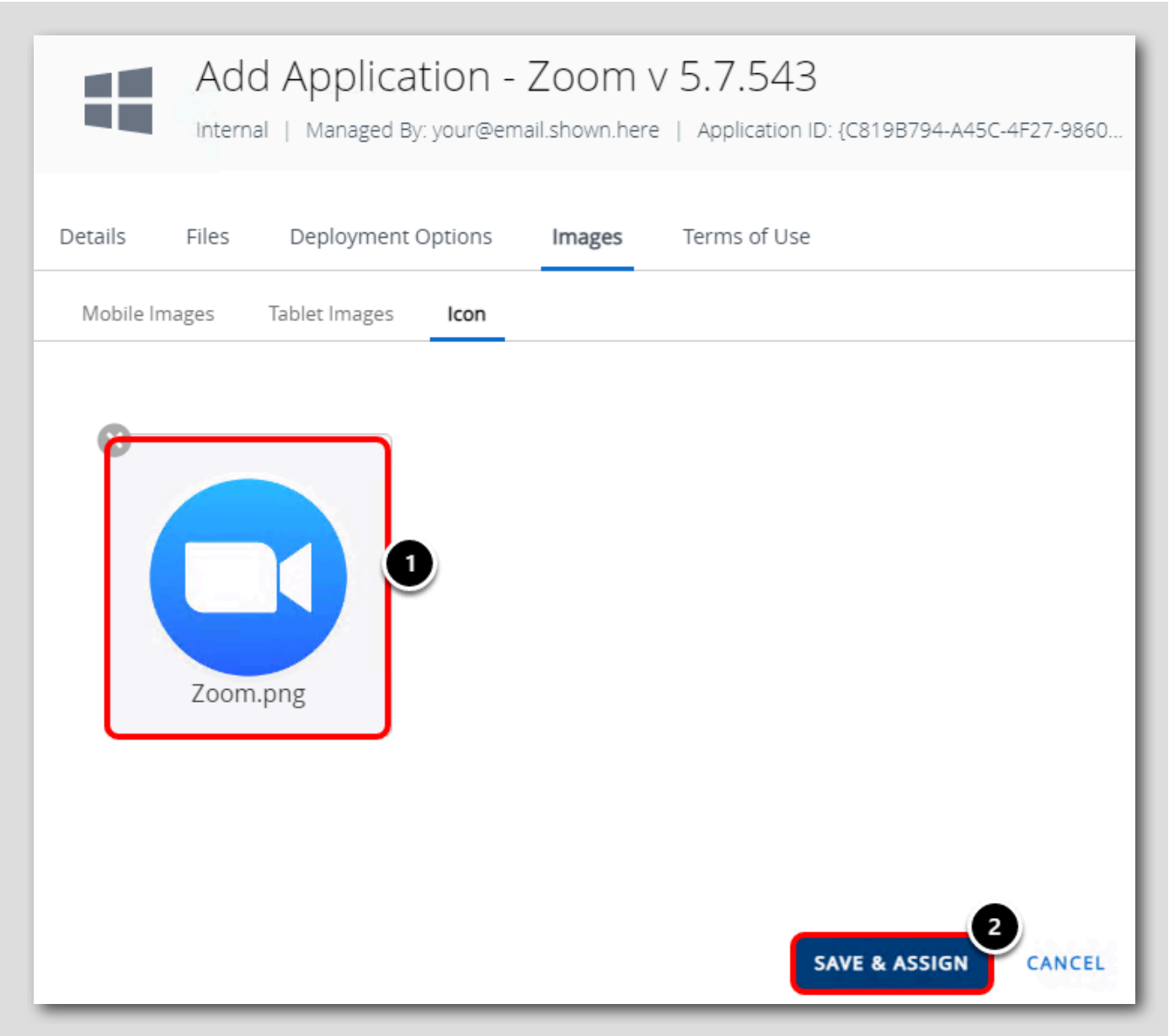
[48]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [Zoom.png] をクリックします。
4. [Open] をクリックします。

Zoom Client for Meetings を保存して割り当てる

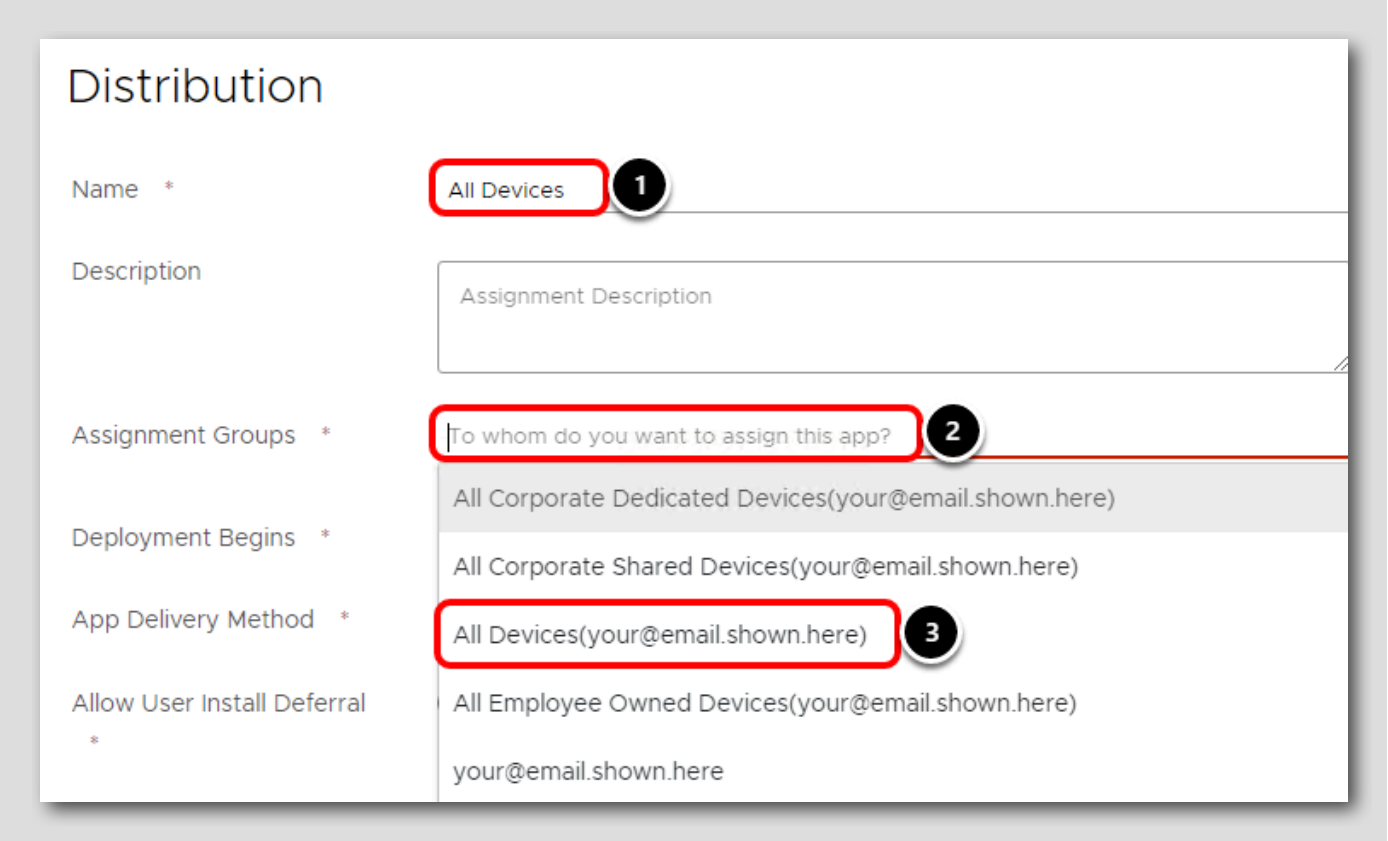
[49]



1. Zoom.png アイコンがアップロードされていることを確認します。
2. [Save & Assign] をクリックします。

配布割り当ての作成

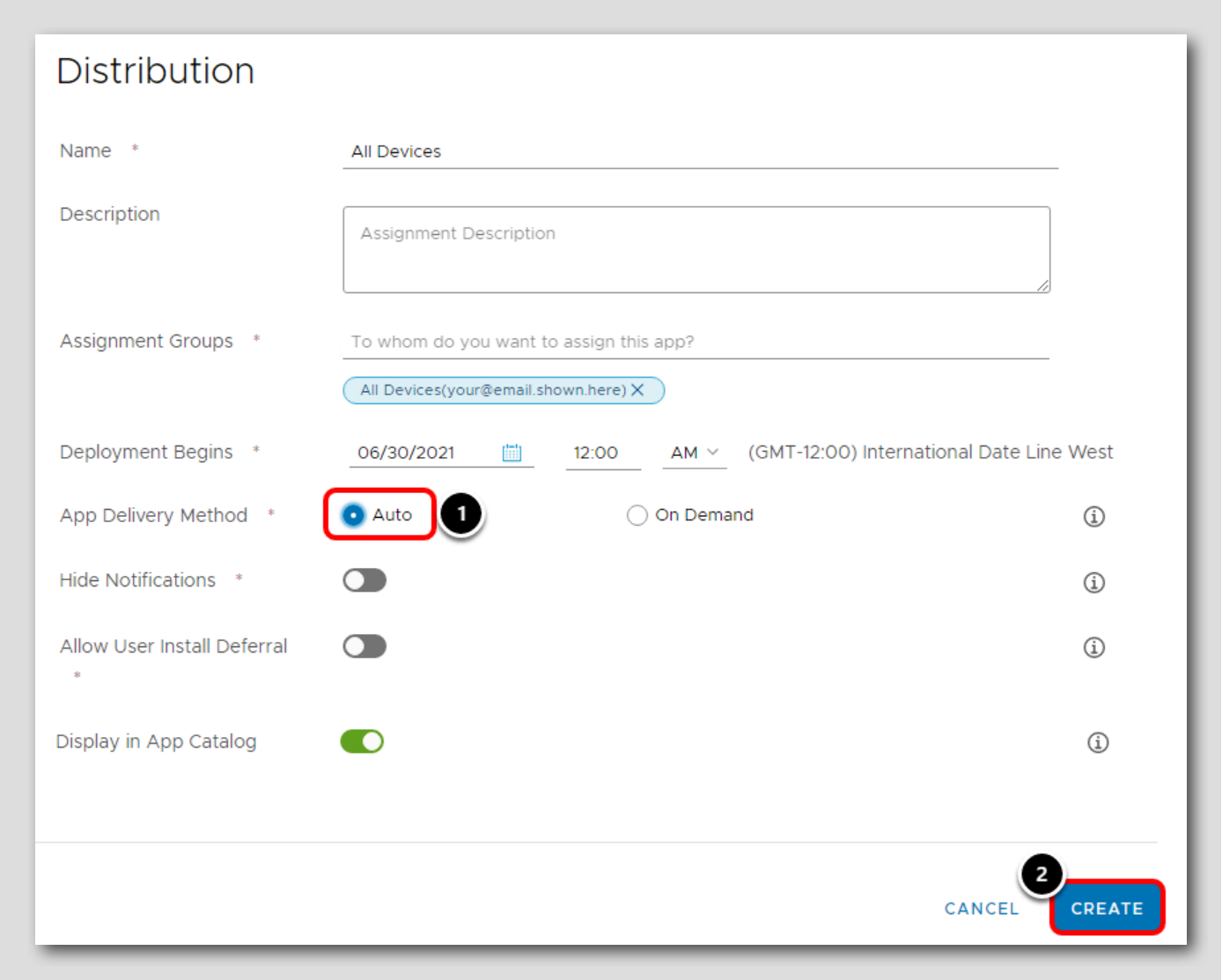
[50]



1. [Name] に **`All Devices`** と入力します。
2. **[Assignment Groups]** フィールドをクリックして、対象となるグループのリストを表示します。
3. **[All Devices (your@email.shown.here)]** グループを選択します。これにより、貴社組織に登録されているすべての Windows 10 デバイスにアプリケーションが公開されます。

アプリケーション配信方法の更新

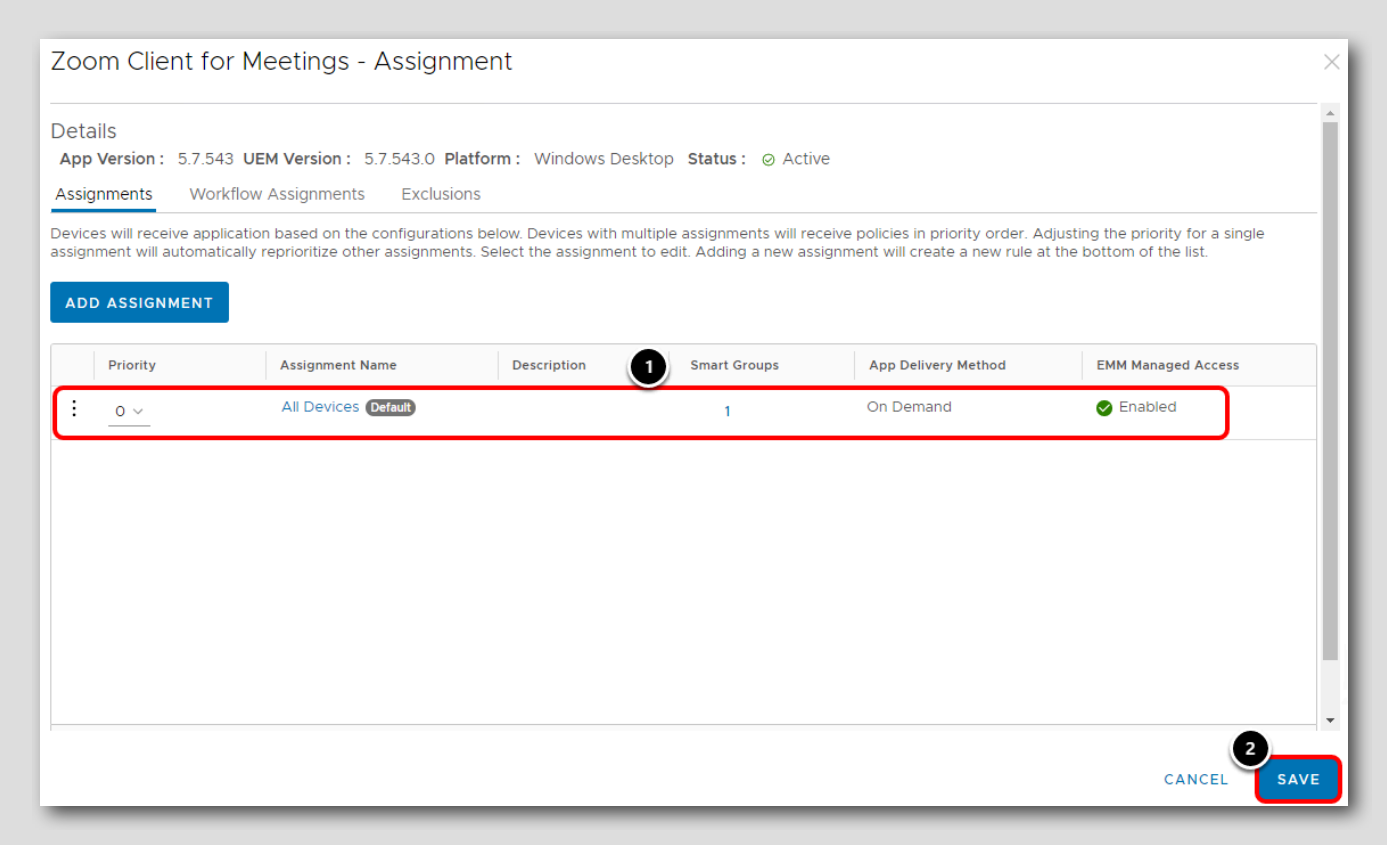
[51]



1. アプリケーション配信方法を **[Auto]** に変更します。[Auto] では、割り当てられた Windows 10 デバイスが Workspace ONE UEM にチェックインするときに、Zoom アプリケーションが自動的にインストールされます。これに対して、[On Demand] では、アプリケーションはカタログで利用可能になりますが、自動的にインストールされません。
2. **[Create]** をクリックします。

Zoom Client for Meetings アプリケーションの保存

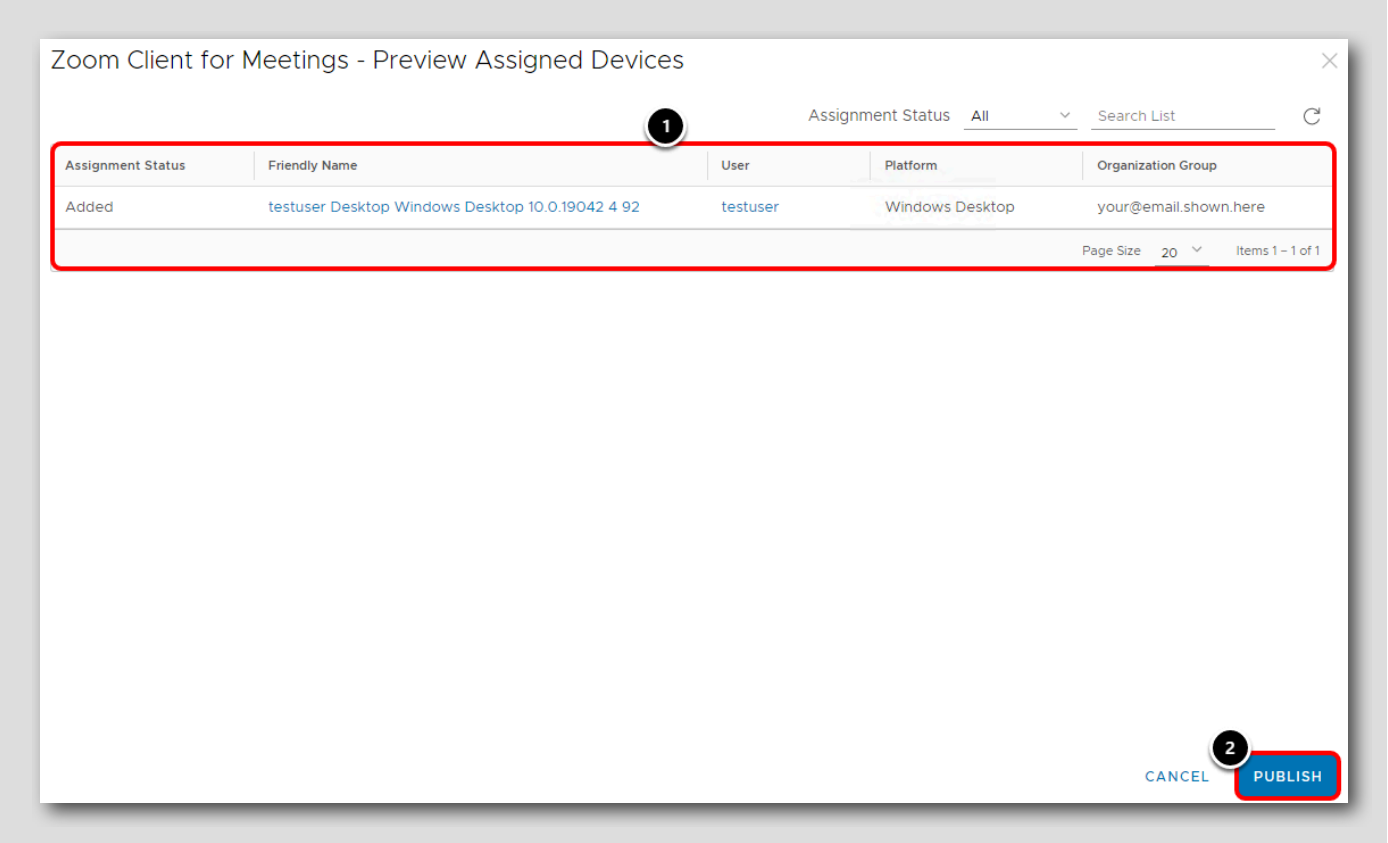
[52]



1. 割り当てのリストがここに表示されます。作成した All Devices 割り当てが表示されていることを確認します。
2. [Save] をクリックします。

Zoom Client for Meetings アプリケーションの公開

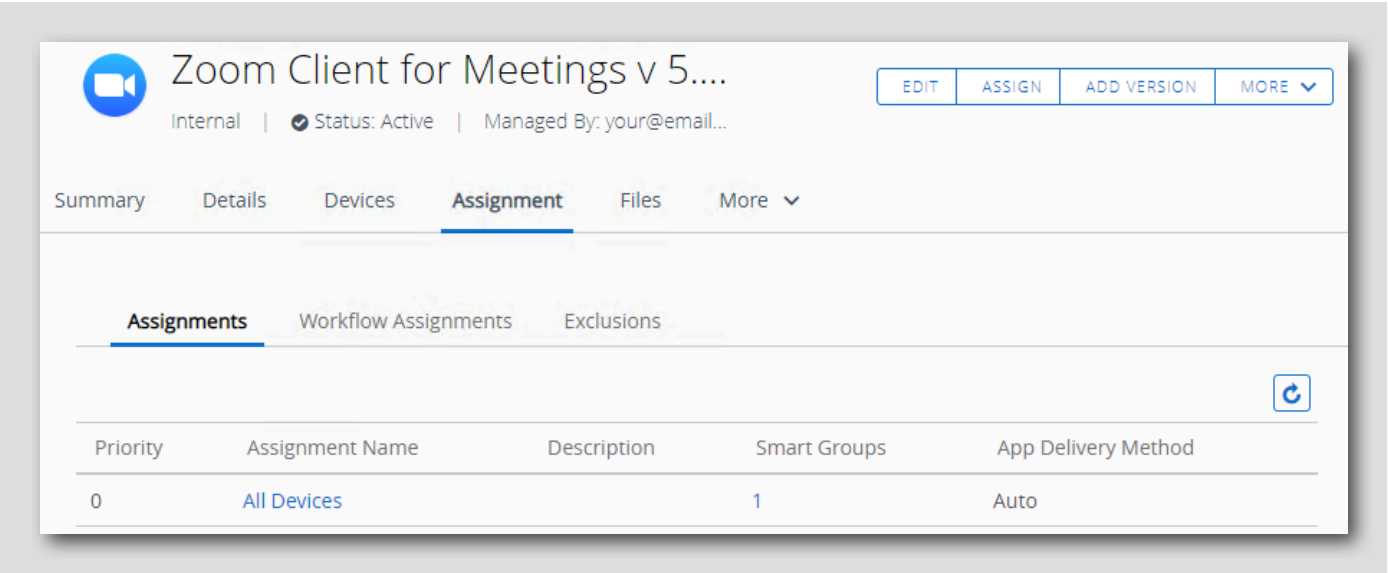
[53]



1. このアプリケーションを受信するデバイスのプレビューがここに表示されます。組織に 1 台のデバイスしか登録していないので、1 つのデバイス レコードが表示されます。
2. [Publish] をクリックします。

アプリケーション作成の確認

[54]

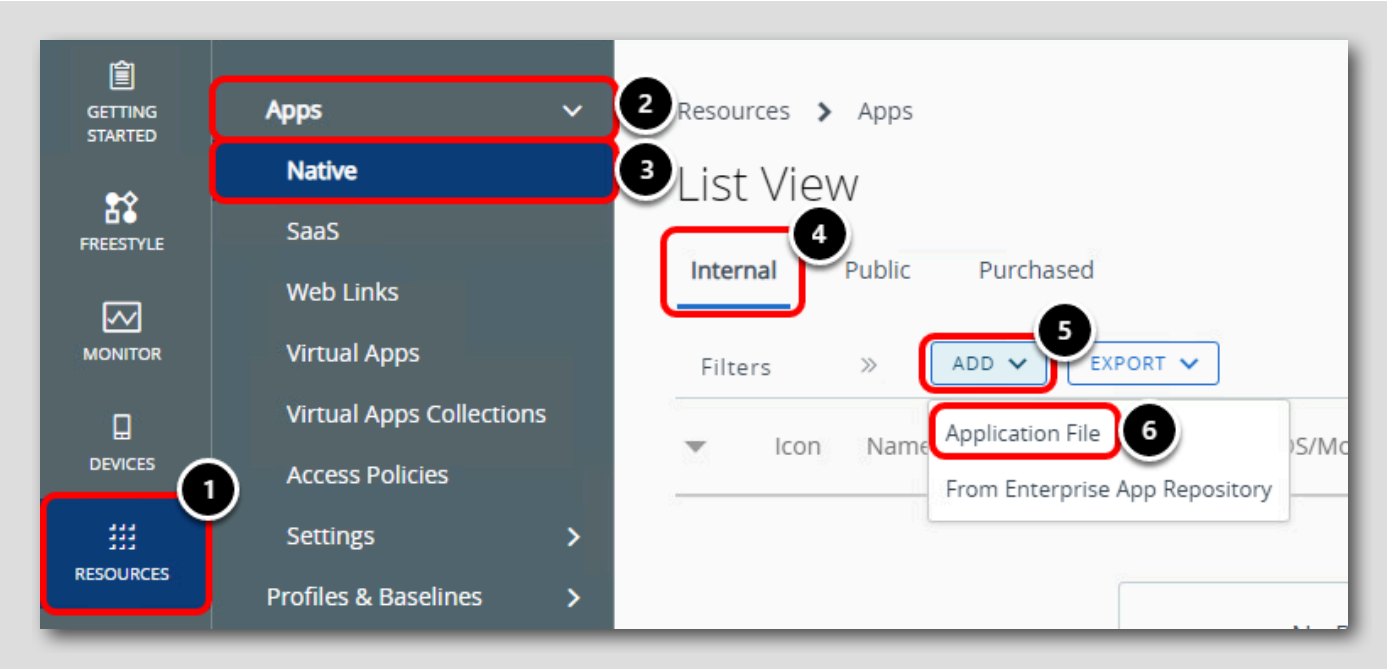


Zoom Client for Meetings アプリケーションが作成され、自動展開されたアプリケーションとして作成した All Devices 割り当てに割り当てられていることを確認します。

次の手順に進んでください。

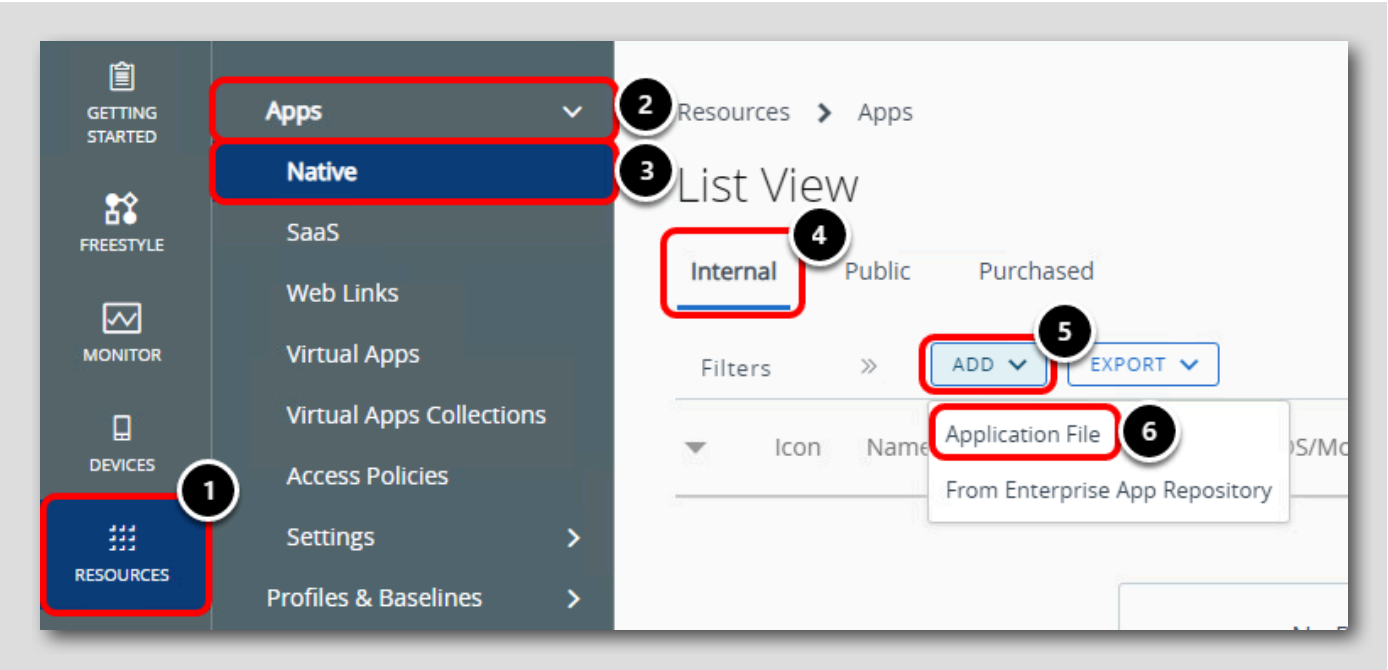
Zoom Plugin for Microsoft Outlook（社内アプリケーション）の構成

[55]

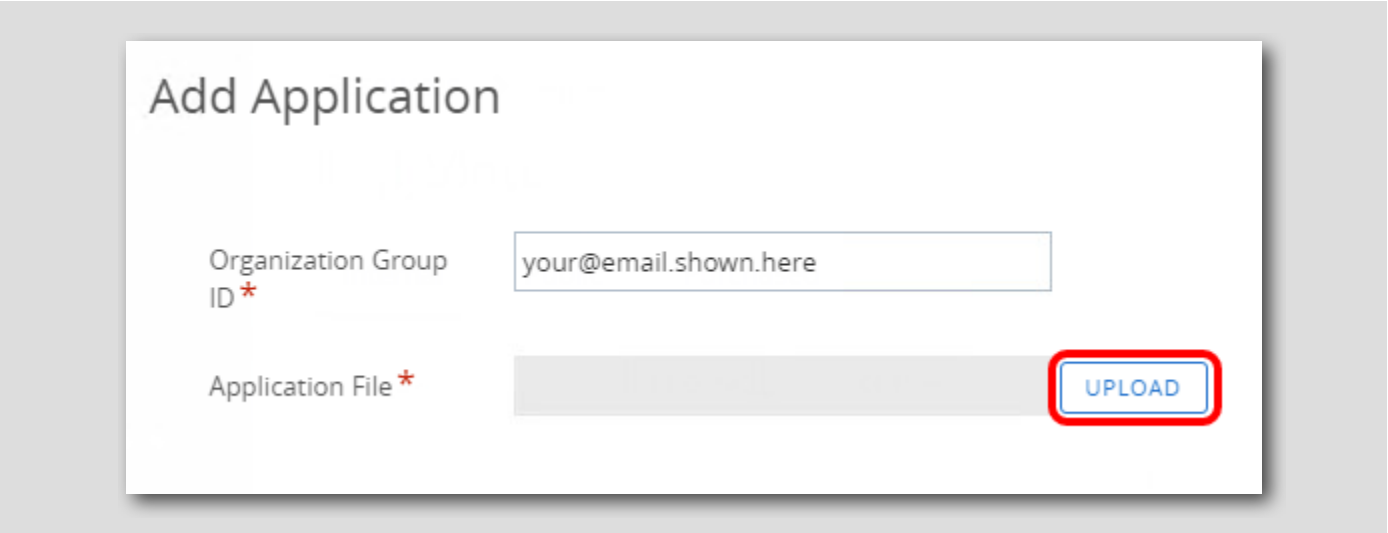


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Apps] を展開します。
3. [Native] をクリックします。
4. [Internal] タブを選択します。
5. [Add] をクリックします。
6. [Application File] をクリックします。

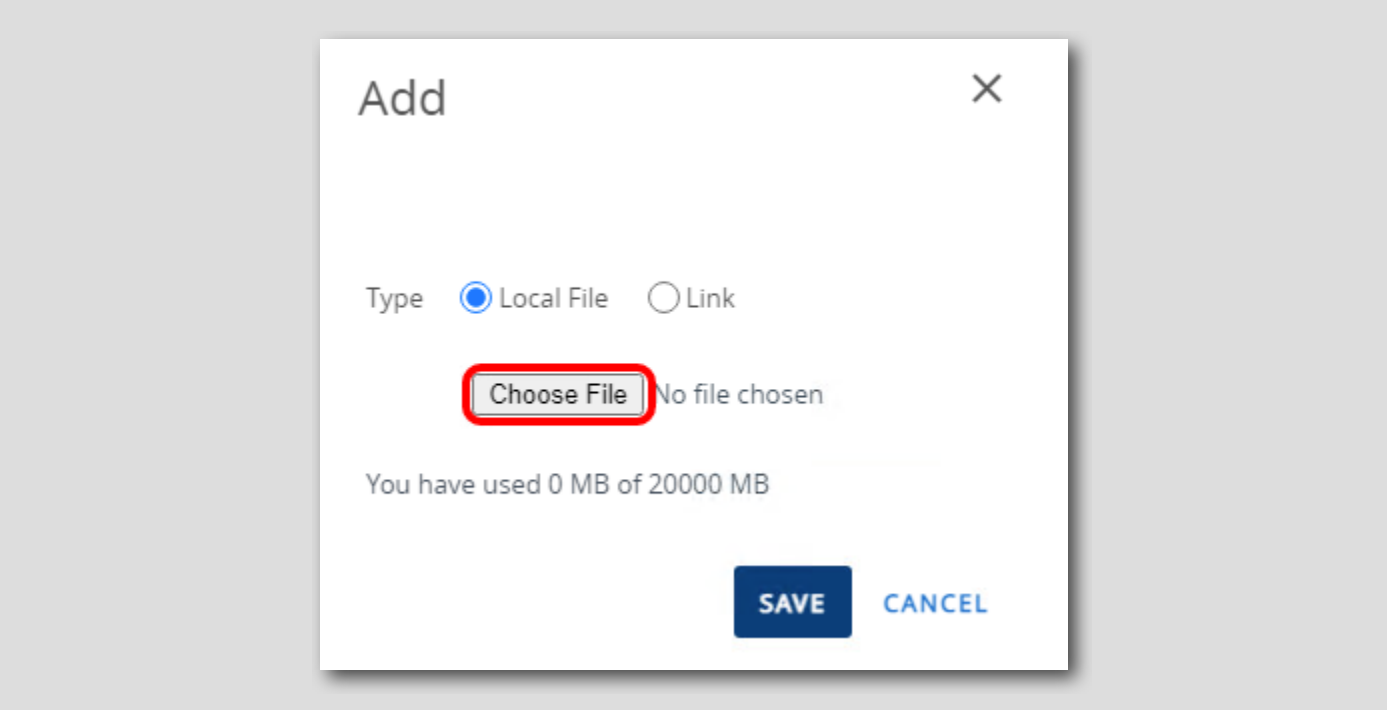


Zoom Plugin for Microsoft Outlook アプリケーションの更新 [56]



[Upload] をクリックします。

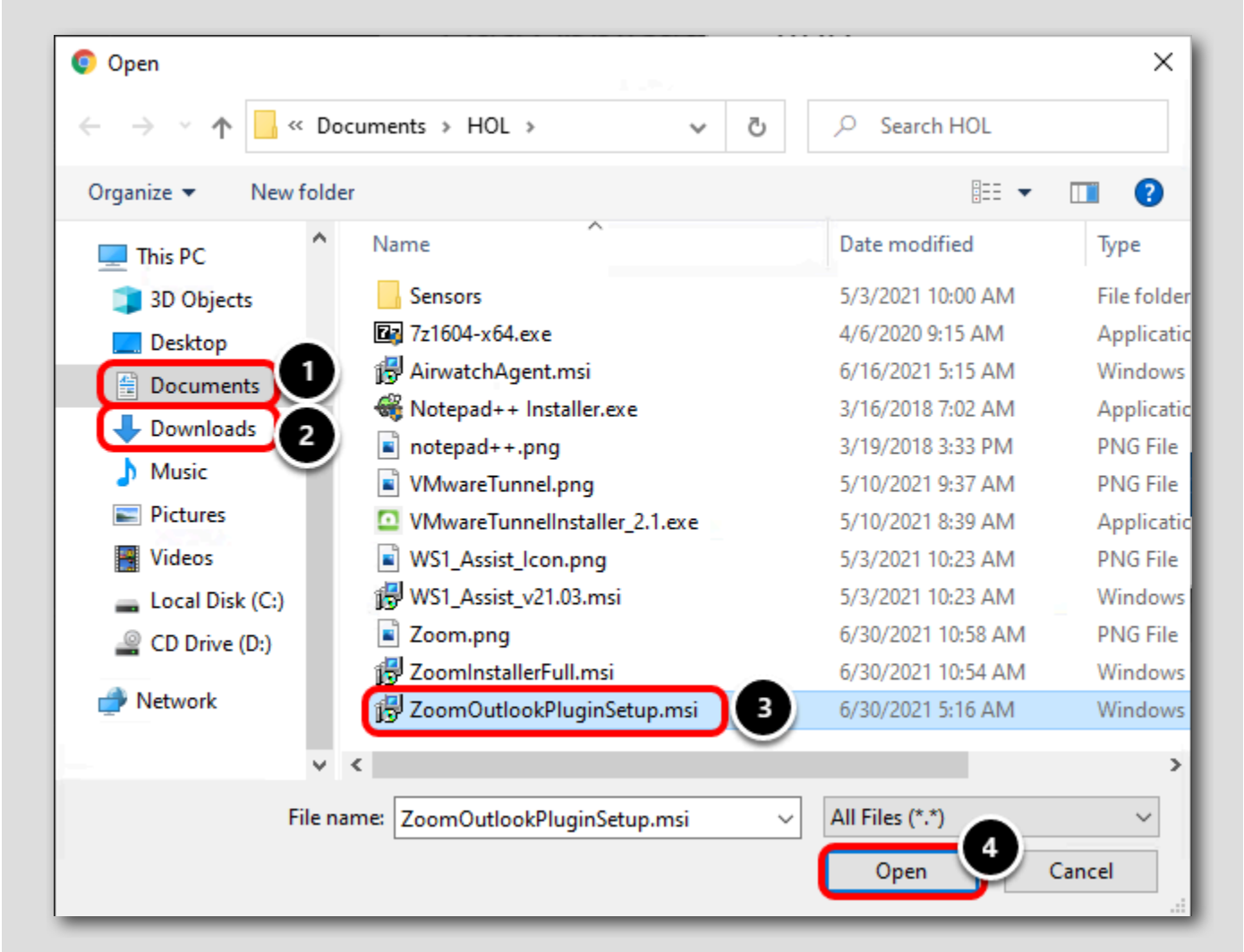
アップロードするファイルの選択 [57]



[Choose File] をクリックします。

ZoomOutlookPluginSetup.msi ファイルの選択

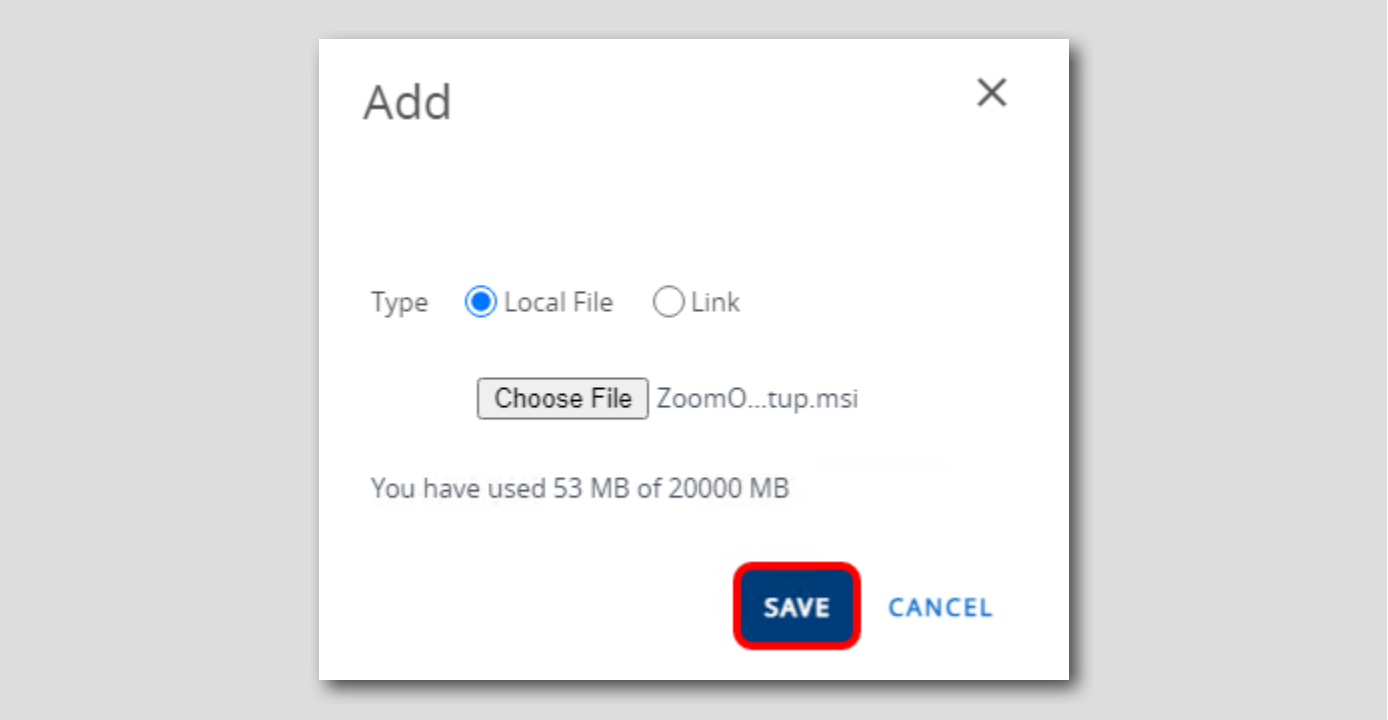
[58]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [ZoomOutlookPluginSetup.msi] をクリックします。
4. [Open] をクリックします。

[59]

ZoomOutlookPluginSetup.msi ファイルの保存

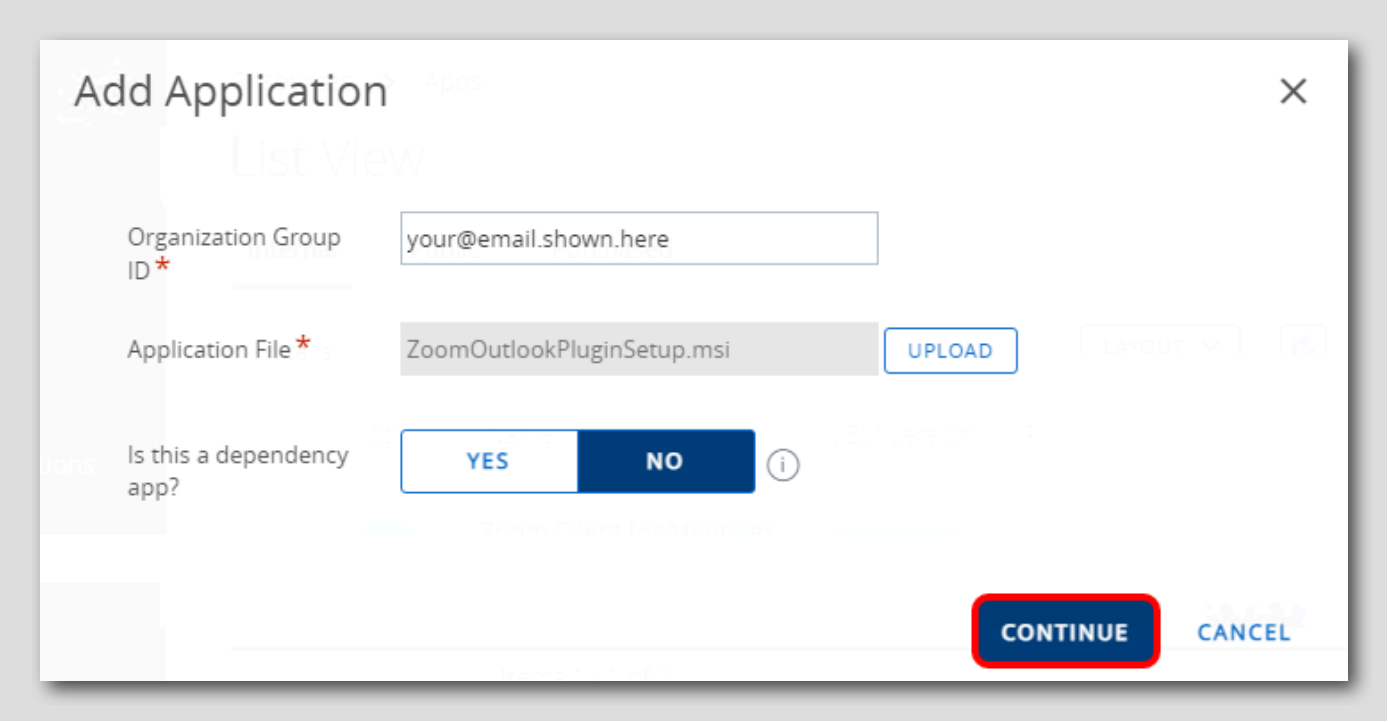


[Save] をクリックして、選択した ZoomOutlookPluginSetup.msi ファイルをアップロードします。

注：アプリケーションのアップロードが完了するまで数分かかる場合があります。アップロードが完了したら、次の手順に進みます。

[60]

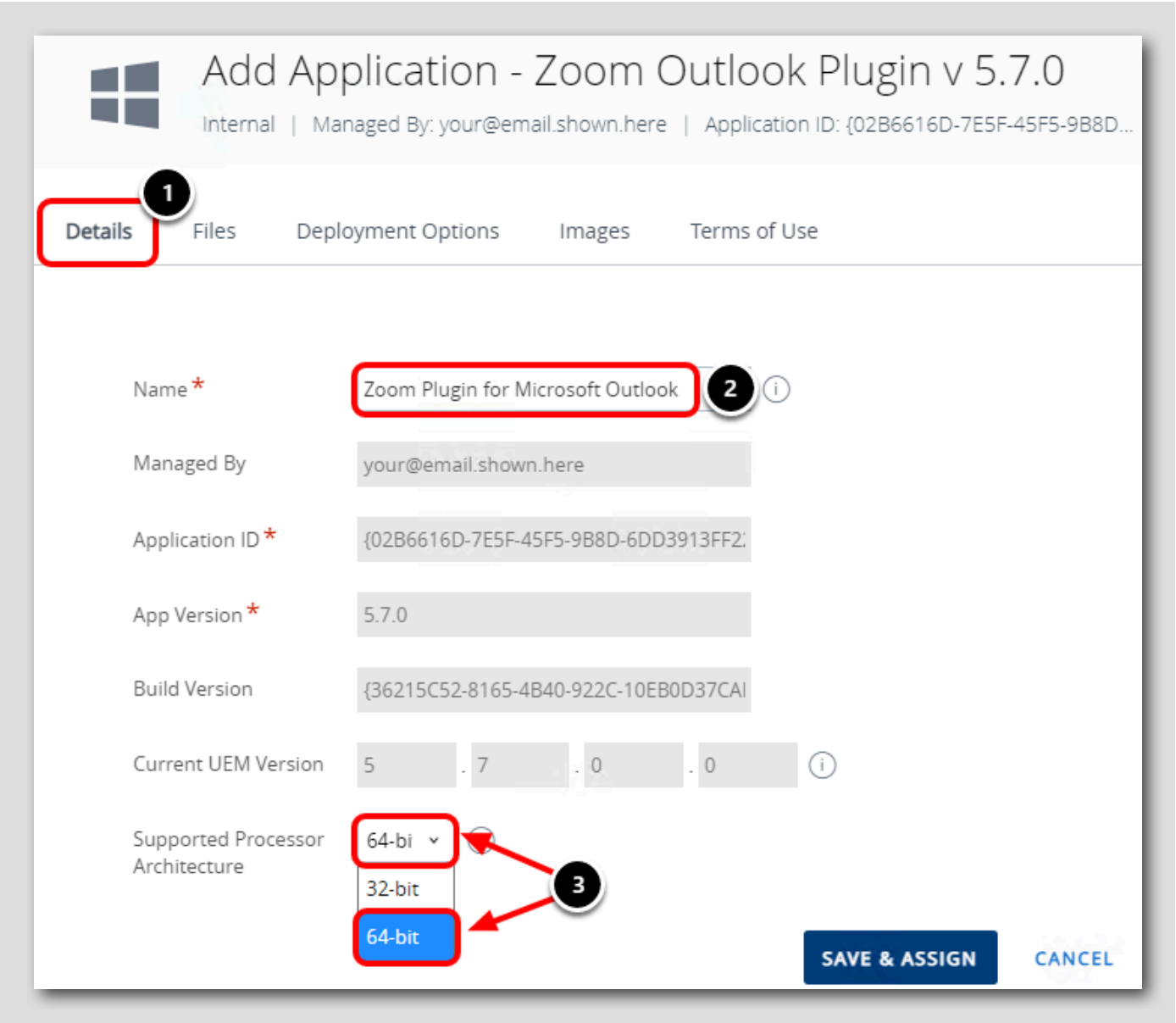
Zoom Plugin for Microsoft Outlook アプリケーションの追加（続き）



[Continue] をクリックします。

Zoom Plugin for Microsoft Outlook アプリケーションの構成

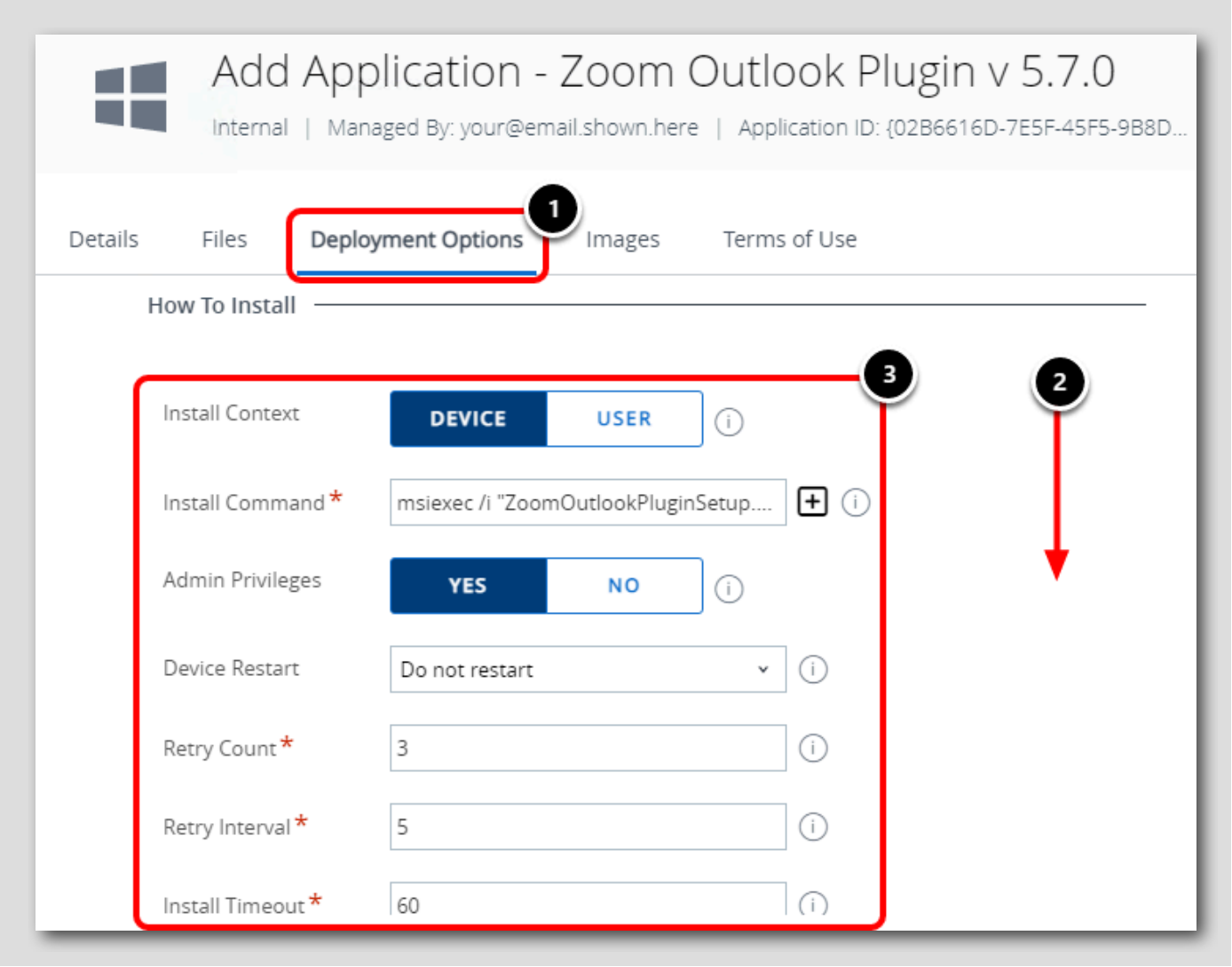
[61]



1. [Details] タブをクリックします。
2. 名前を **`Zoom Plugin for Microsoft Outlook`** に更新します。この名前は、エンド ユーザーのデバイスおよびアプリケーション カタログのアプリケーション名になります。
3. サポートされているプロセス アーキテクチャを [64-bit] に更新します。

展開オプションの確認

[62]

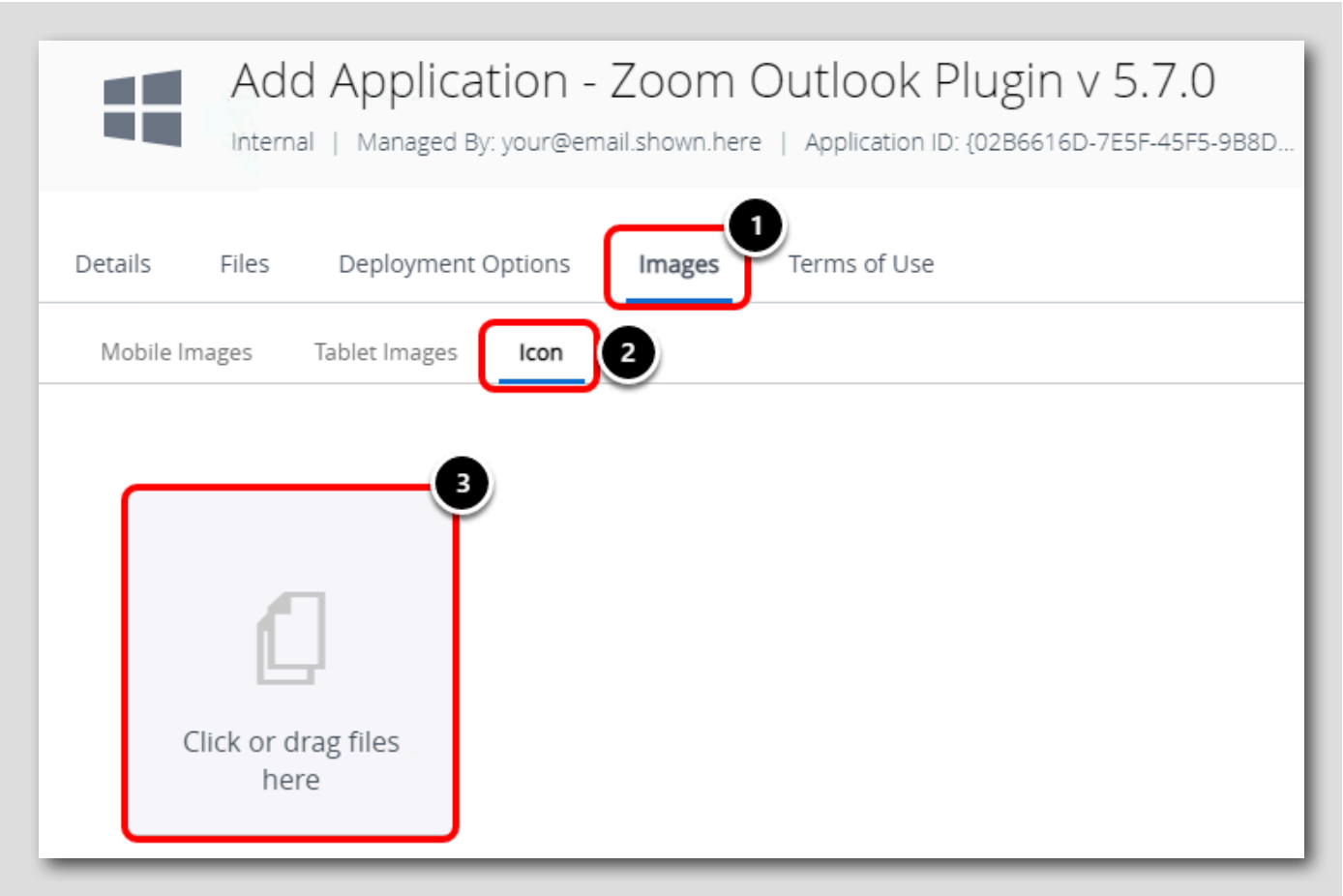


1. [Deployment Options] タブをクリックします。
2. [How To Install] 設定まで下にスクロールします。
3. [Install Command] などの [How To Install] 設定はすでに完了しています。これらの詳細は、アップロードされた MSI から抽出されました。

次の手順に進んでください。

アイコンの構成

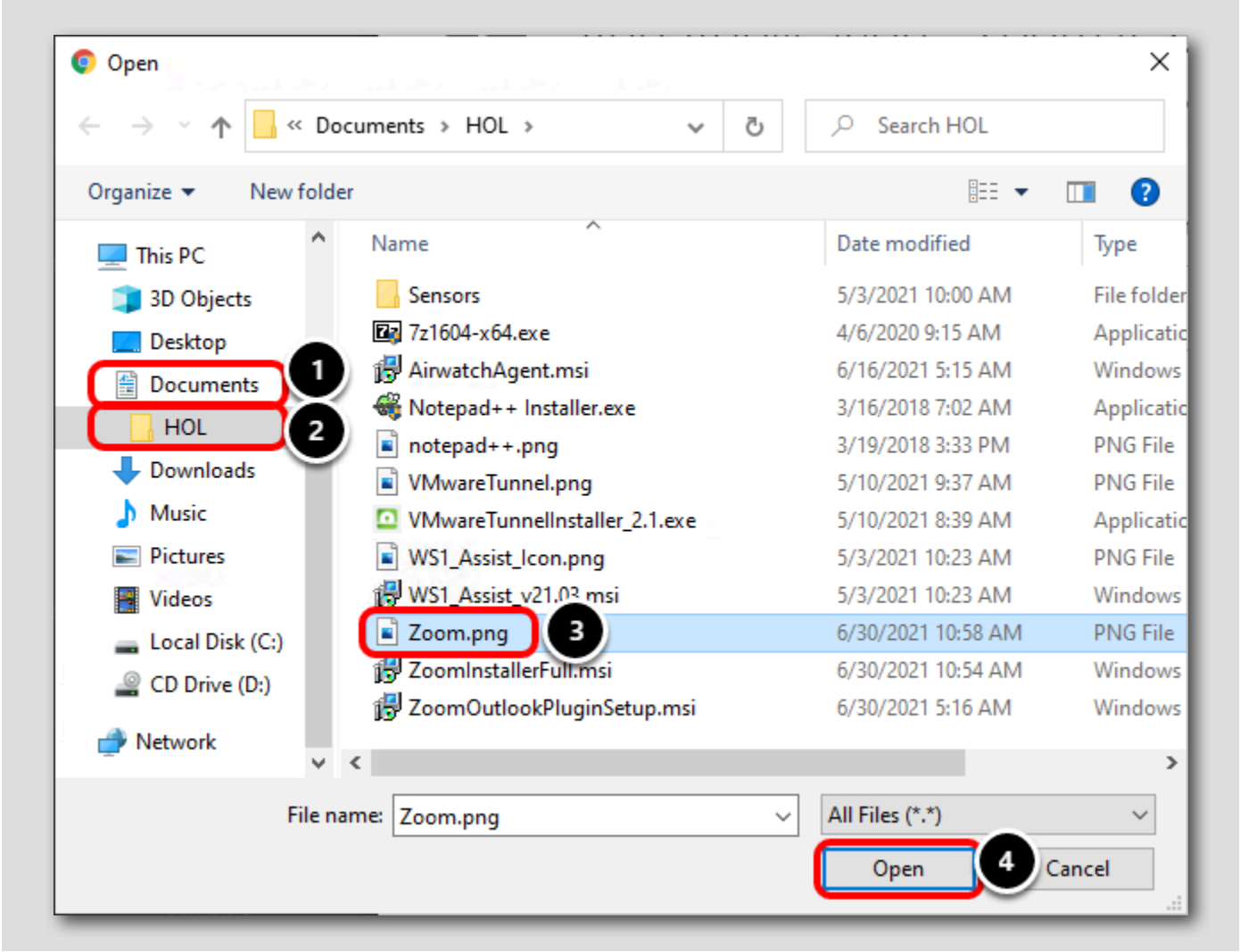
[63]



1. [Images] タブをクリックします。
2. [Icon] タブをクリックします。
3. [Click or drag files here] というラベルの付いた領域をクリックします。

Zoom.png ファイルの選択

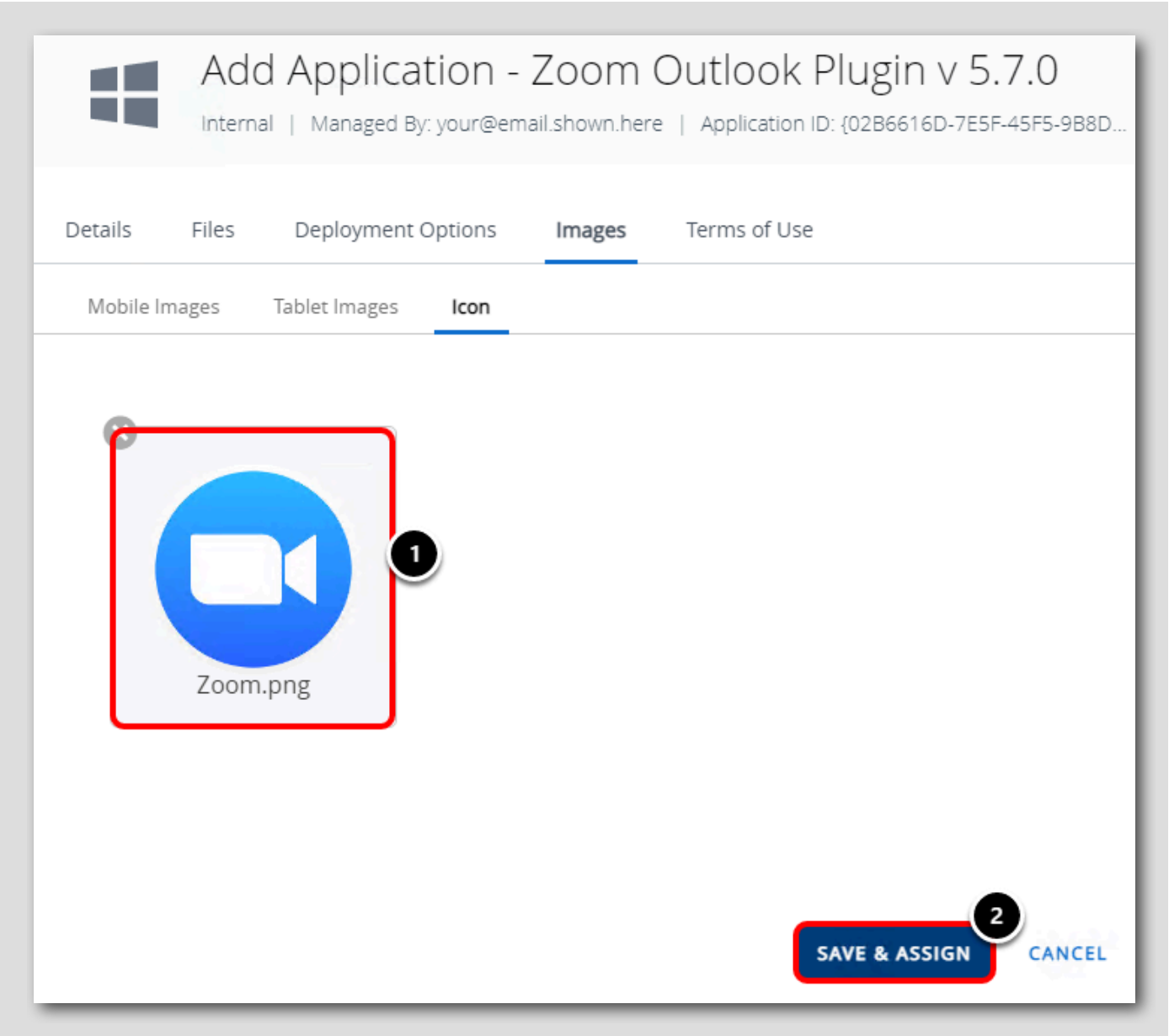
[64]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [Zoom.png] をクリックします。
4. [Open] をクリックします。

Zoom Plugin for Microsoft Outlook の保存と割り当て

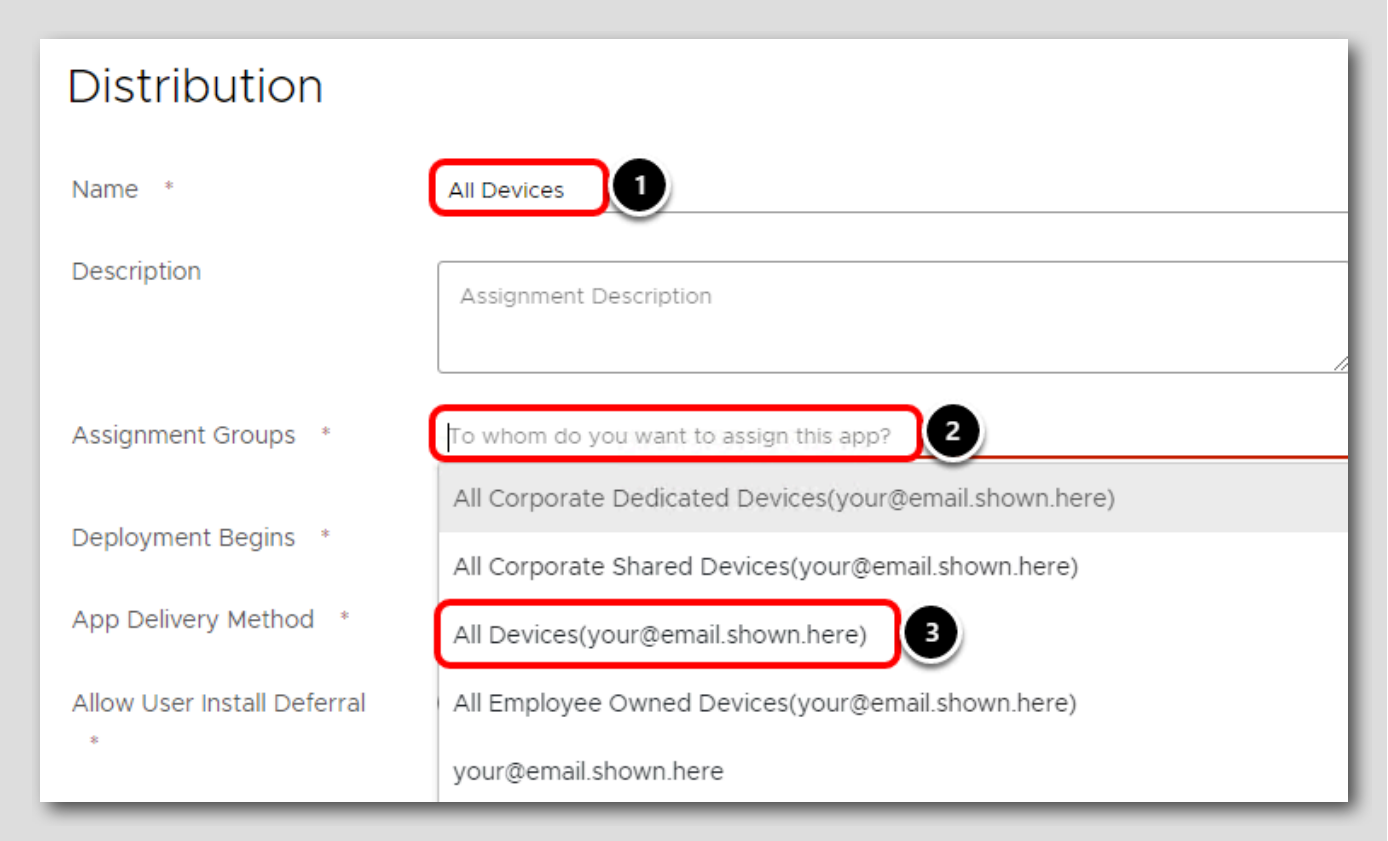
[65]



1. Zoom.png アイコンがアップロードされていることを確認します。
2. [Save & Assign] をクリックします。

配布割り当ての作成

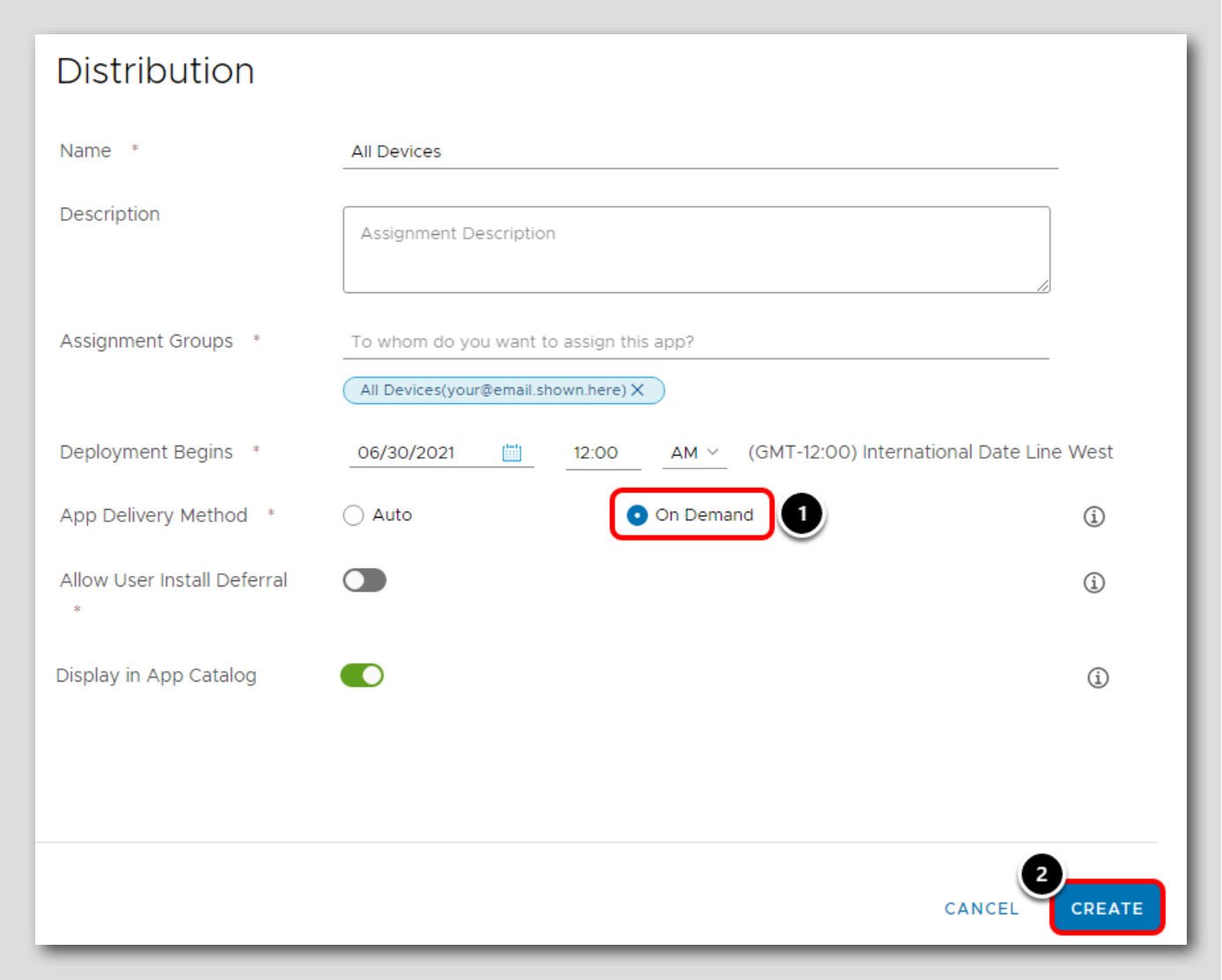
[66]



1. [Name] に **`All Devices`** と入力します。
2. **[Assignment Groups]** フィールドをクリックして、対象となるグループのリストを表示します。
3. **[All Devices (your@email.shown.here)]** グループを選択します。これにより、貴社組織に登録されているすべての Windows 10 デバイスにアプリケーションが公開されます。

アプリケーション配信方法の更新

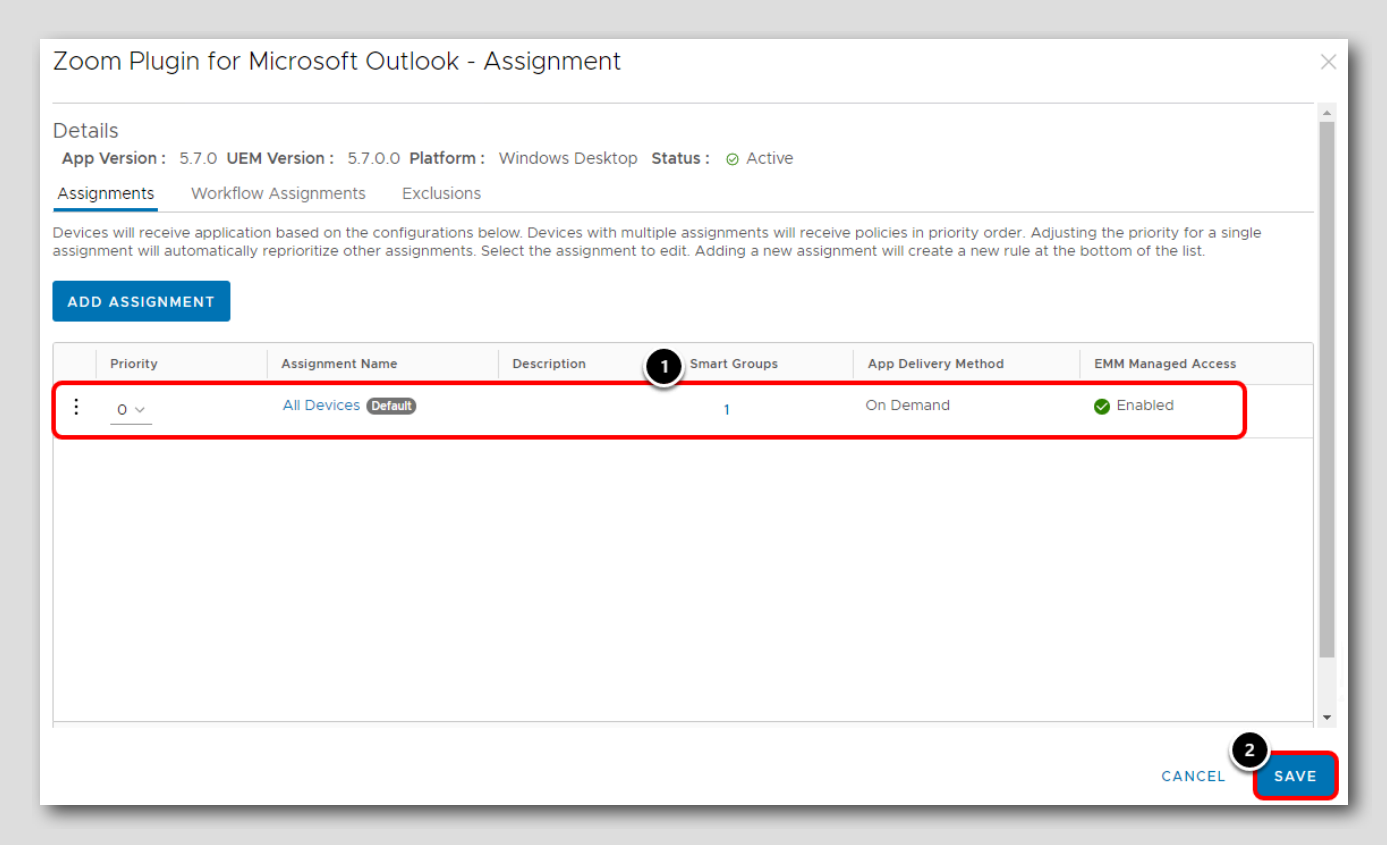
[67]



1. アプリケーション配信方法は **[On Demand]** のままにします。[Auto] では、割り当てられた Windows 10 デバイスが Workspace ONE UEM にチェックインするときに、アプリケーションが自動的にインストールされます。これに対して、[On Demand] では、アプリケーションはカタログで利用可能になりますが、自動的にインストールされません。Freestyle Orchestrator を介してアプリケーションを配布する場合、アプリケーションはオンデマンドのままにしておく必要があります。そうしないと、ワークフローで指定されたとおりにインストールされず、できるだけ早くインストールされます。
2. **[Create]** をクリックします。

Zoom Plugin for Microsoft Outlook アプリケーションの保存

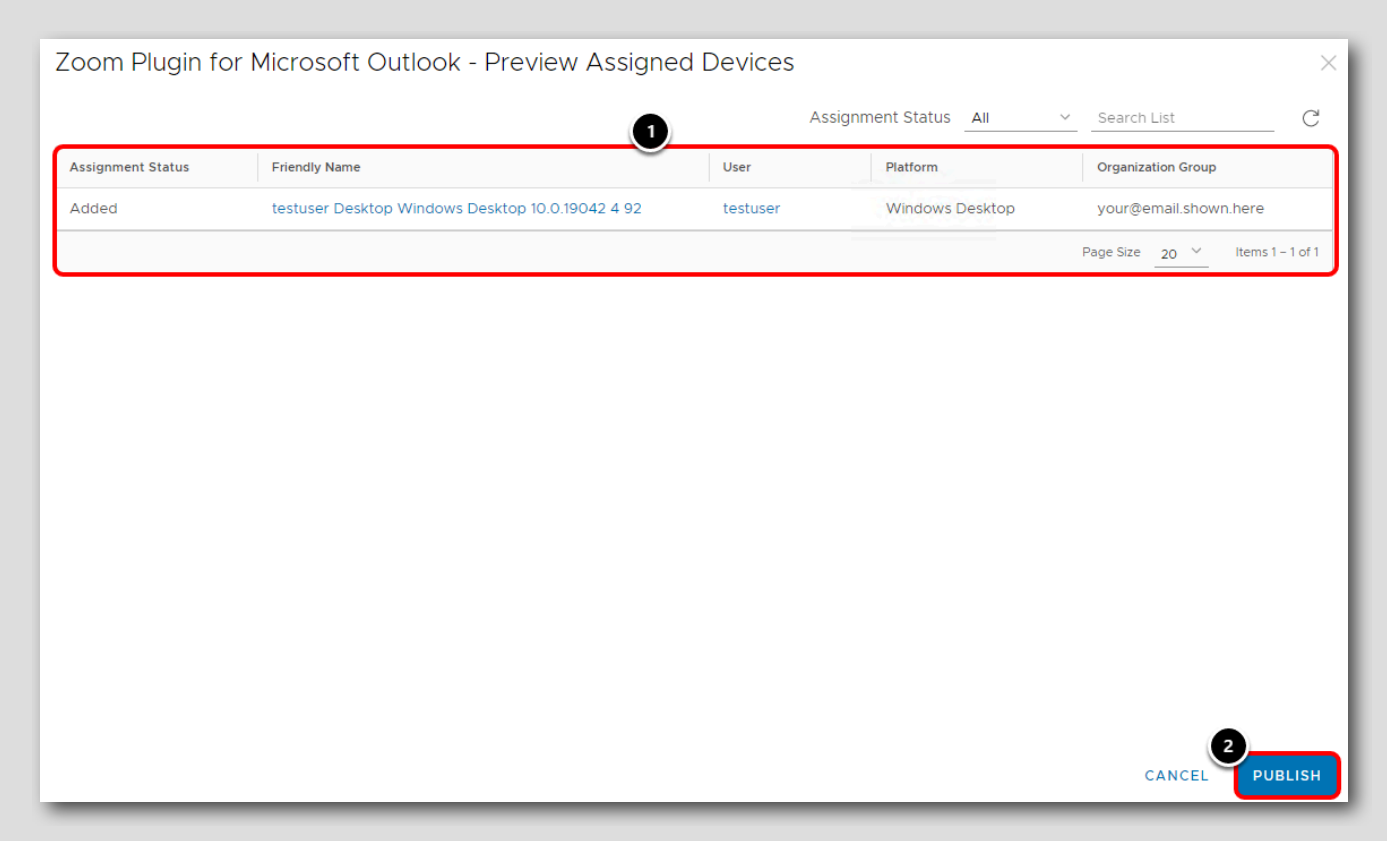
[68]



1. 割り当てのリストがここに表示されます。作成した All Devices 割り当てが表示されていることを確認します。
2. [Save] をクリックします。

Zoom Plugin for Microsoft Outlook アプリケーションの公開

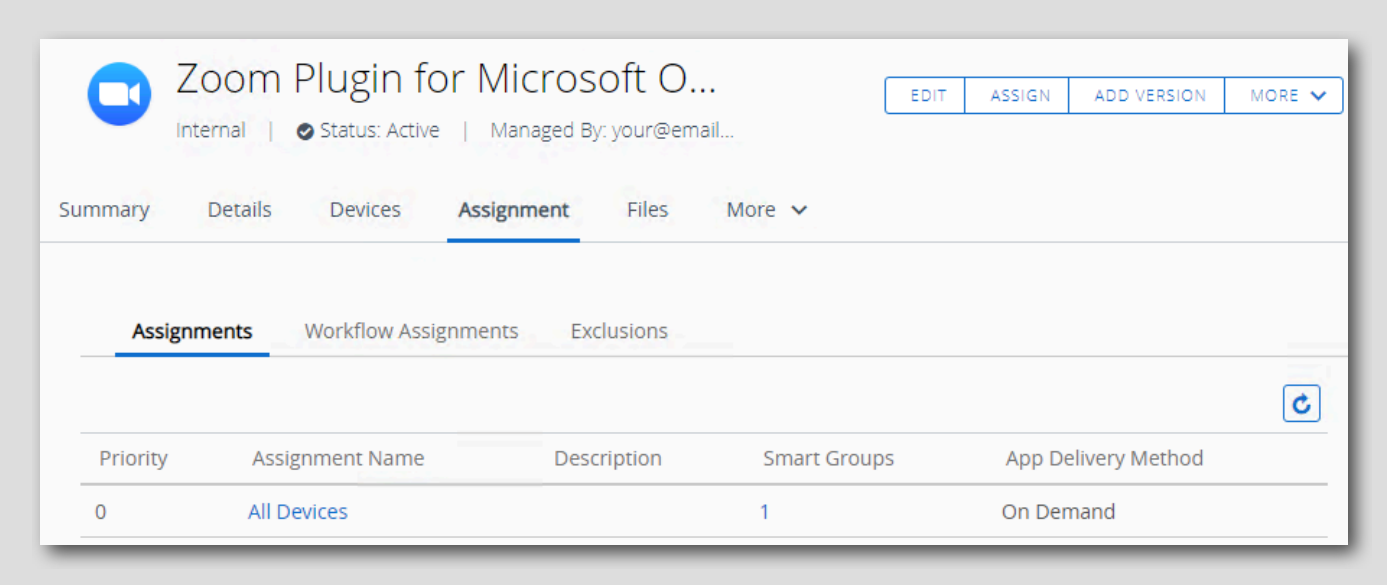
[69]



1. このアプリケーションを受信するデバイスのプレビューがここに表示されます。組織に 1 台のデバイスしか登録していないので、1 つのデバイス レコードが表示されます。
2. [Publish] をクリックします。

アプリケーション作成の確認

[70]

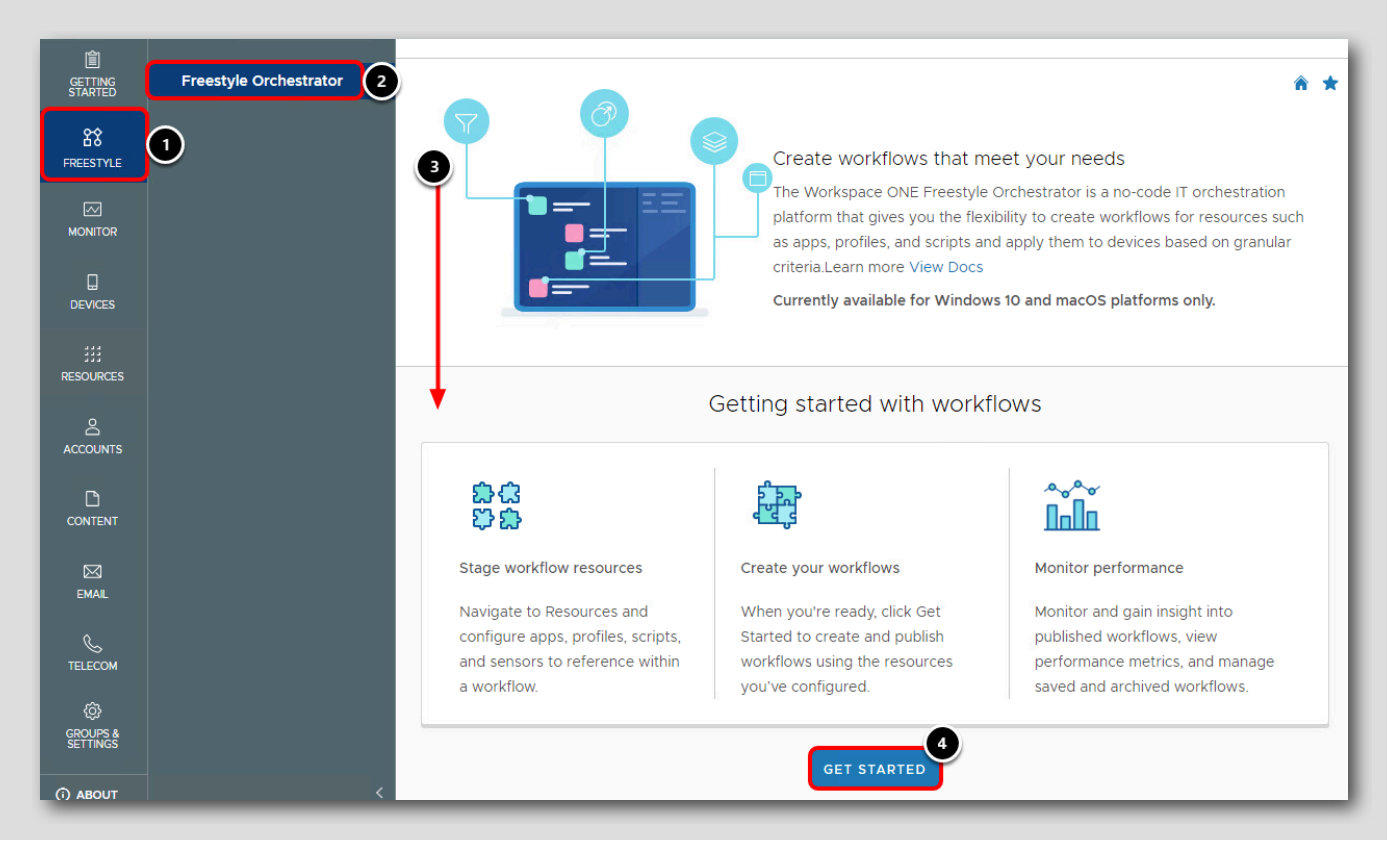


Zoom Plugin for Microsoft Outlook アプリケーションが作成され、オンデマンド アプリケーションとして作成した All Devices 割り当てに割り当てられていることを確認します。

次の手順に進んでください。

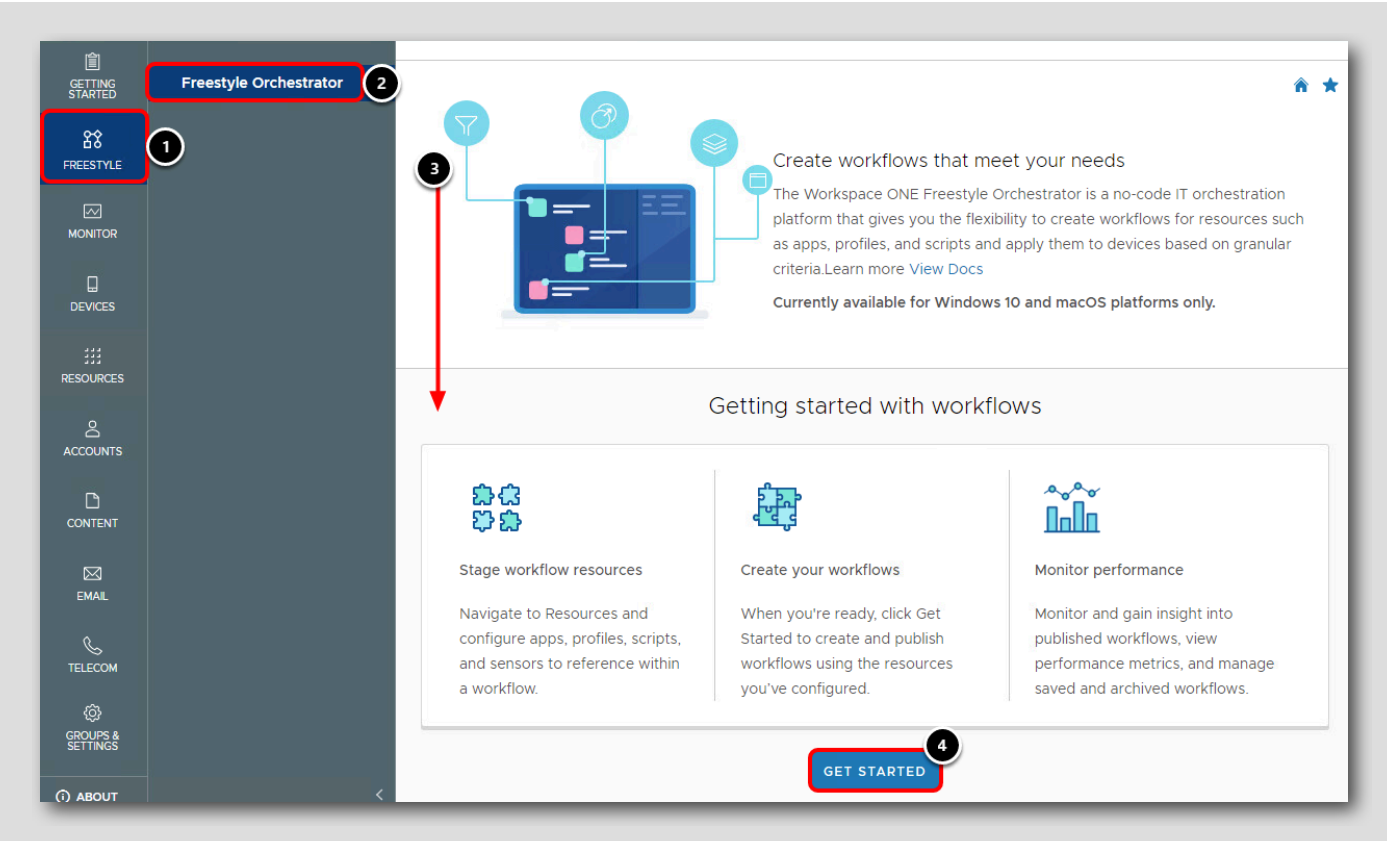
Freestyle Orchestrator を使用したワークフローの作成

[71]



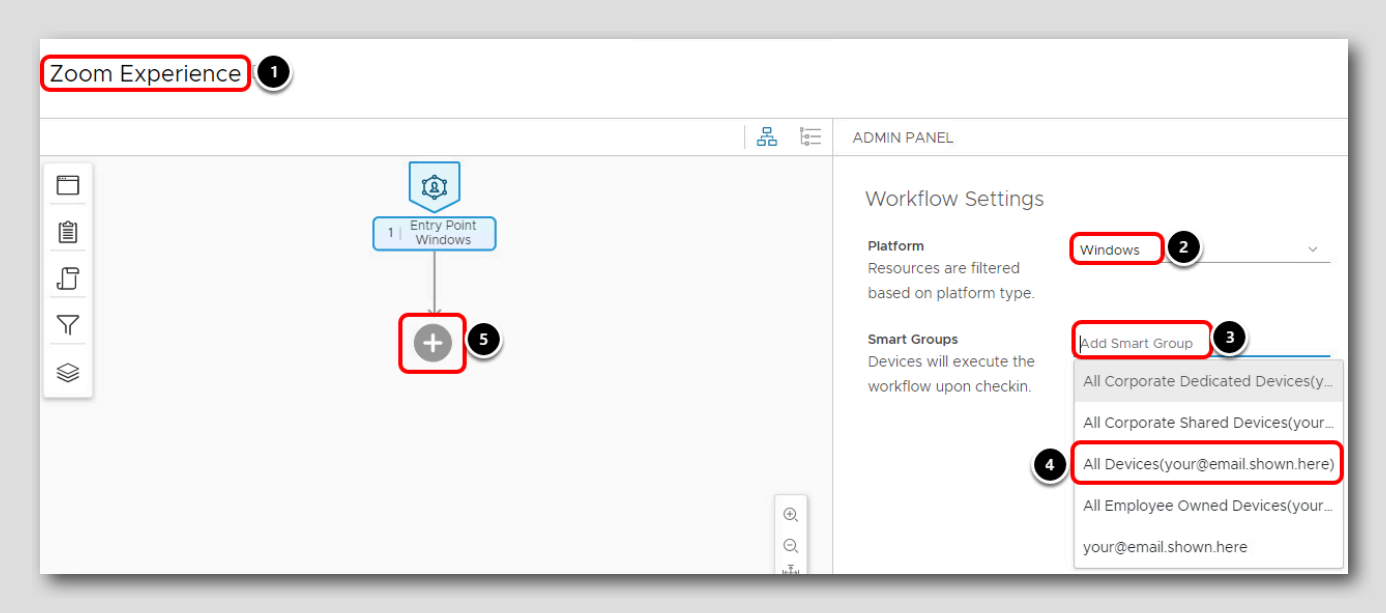
ここで、必要な Zoom アプリケーションがインストールされている場合にのみ、Zoom Plugin for Microsoft Outlook をデバイスに配布するワークフローを Freestyle Orchestrator で構築します。ワークフローの条件付きチェックとステップ ロジックにより、必要なリソースをインテリジェントに配布できます。

1. [Freestyle] をクリックします。
2. [Freestyle Orchestrator] をクリックします。
3. Freestyle Orchestrator の [Getting Started] 情報を過ぎて、下にスクロールします。
4. [Get Started] をクリックします。


GETTING STARTED
FREESTYLE
MONITOR
DEVICES
RESOURCES
ACCOUNTS
CONTENT
EMAIL
TELECOM
GROUPS & SETTINGS
ABOUT
Freestyle Orchestrator
1
2
3
4
Create workflows that meet your needs
The Workspace ONE Freestyle Orchestrator is a no-code IT orchestration platform that gives you the flexibility to create workflows for resources such as apps, profiles, and scripts and apply them to devices based on granular criteria.Learn more View Docs
Currently available for Windows 10 and macOS platforms only.
Getting started with workflows
Stage workflow resources
Navigate to Resources and configure apps, profiles, scripts, and sensors to reference within a workflow.
Create your workflows
When you're ready, click Get Started to create and publish workflows using the resources you've configured.
Monitor performance
Monitor and gain insight into published workflows, view performance metrics, and manage saved and archived workflows.
GET STARTED

ワークフローの設定

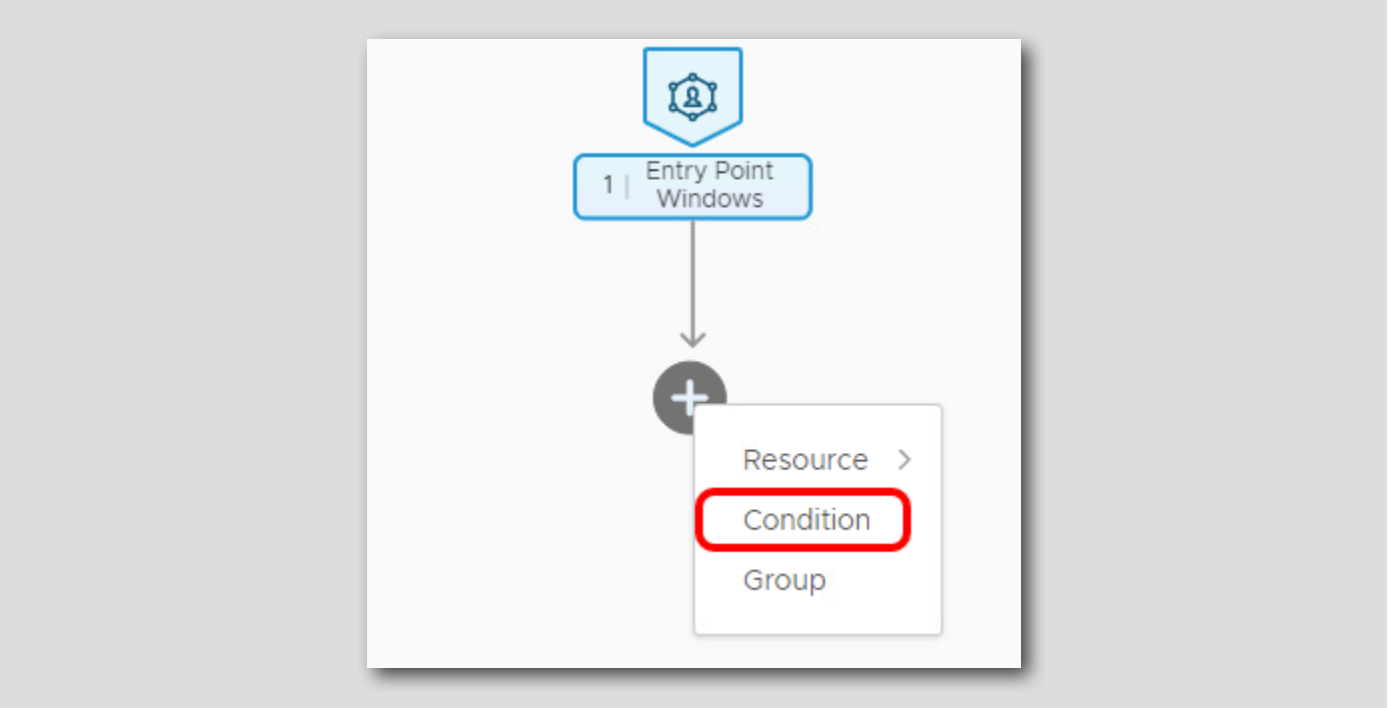
[72]



1. ワークフローに **`Zoom Experience`** という名前を付けます。
2. [Platform] で [Windows] を選択します。
3. [Smart Groups] フィールドをクリックして、対象となるスマート グループのリストを表示します。
4. リストから [All Devices (your@email.shown.here)] を選択します
5. [Add] ボタンをクリックして、次の手順をビルドします。

ワークフロー条件の追加

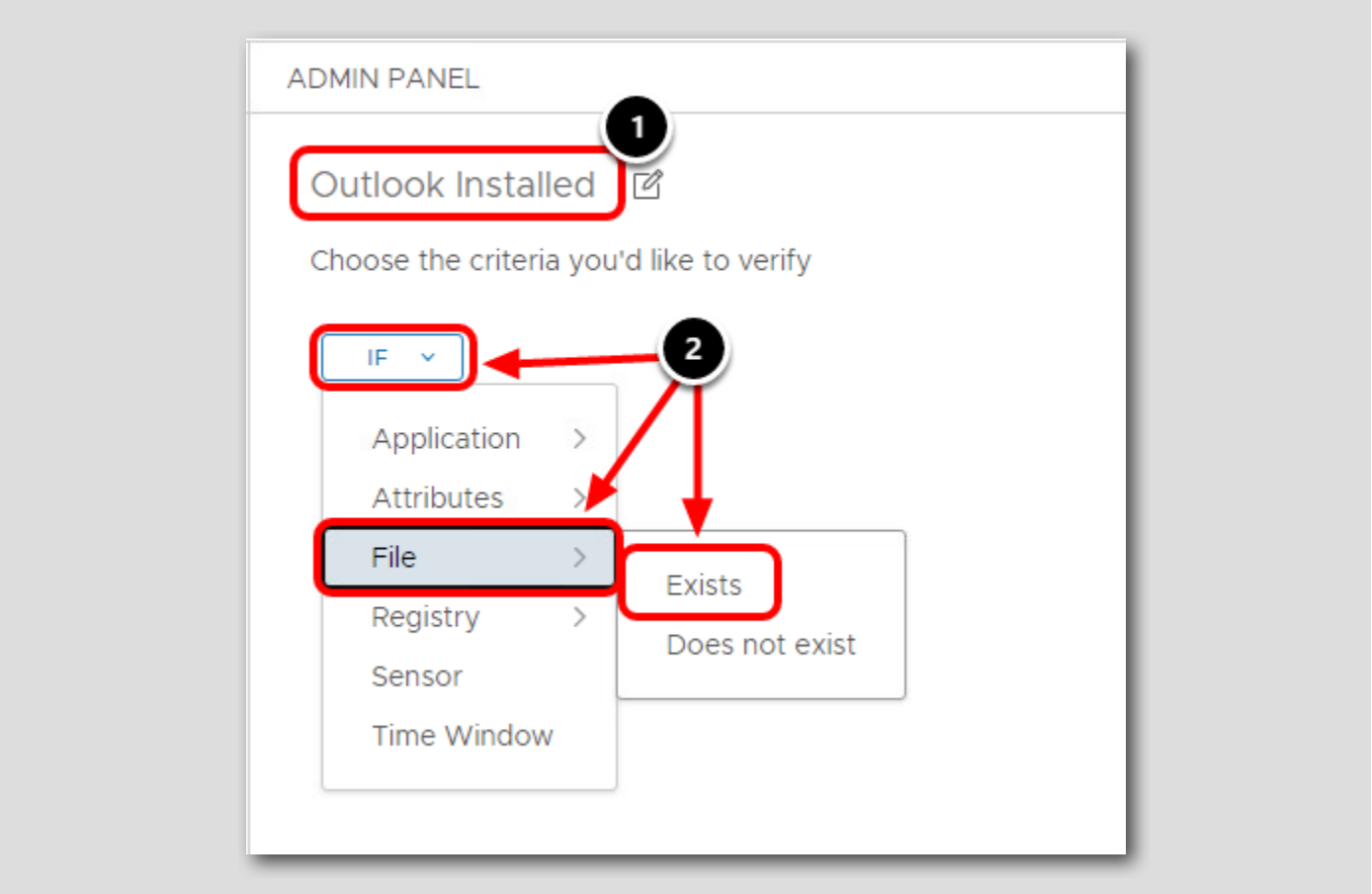
[73]



[Condition] をクリックします。これにより、ワークフローの条件 (If/Else) を作成および構成できます。

[File Exists] 条件の追加

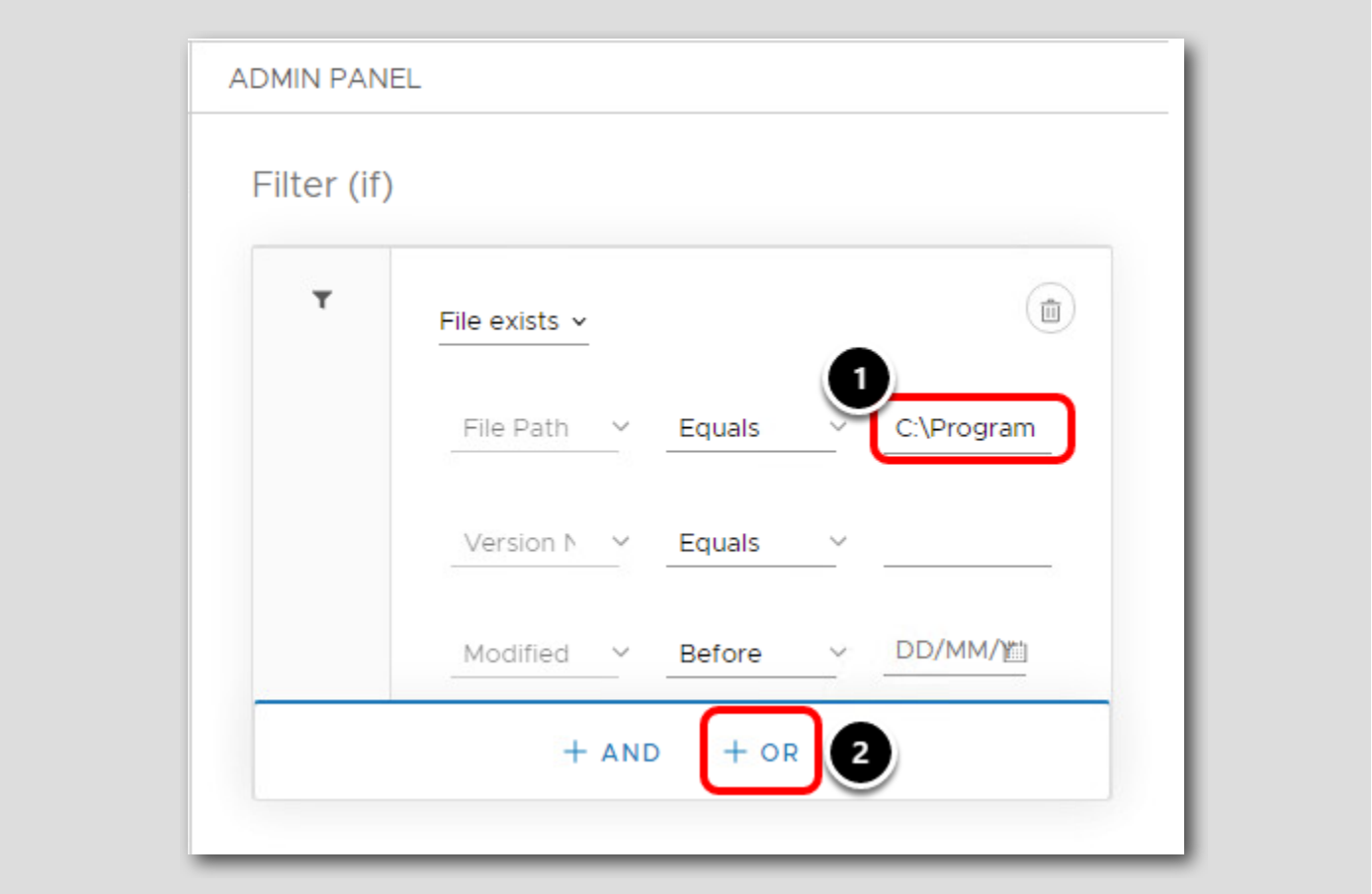
[74]



1. 条件に **`Outlook Installed`** という名前を付けます。
2. [IF] ボタンをクリックして条件を追加し、ドロップダウン リストから [File]、次に [Exists] を選択します。

[75]

[File Condition] 値の追加



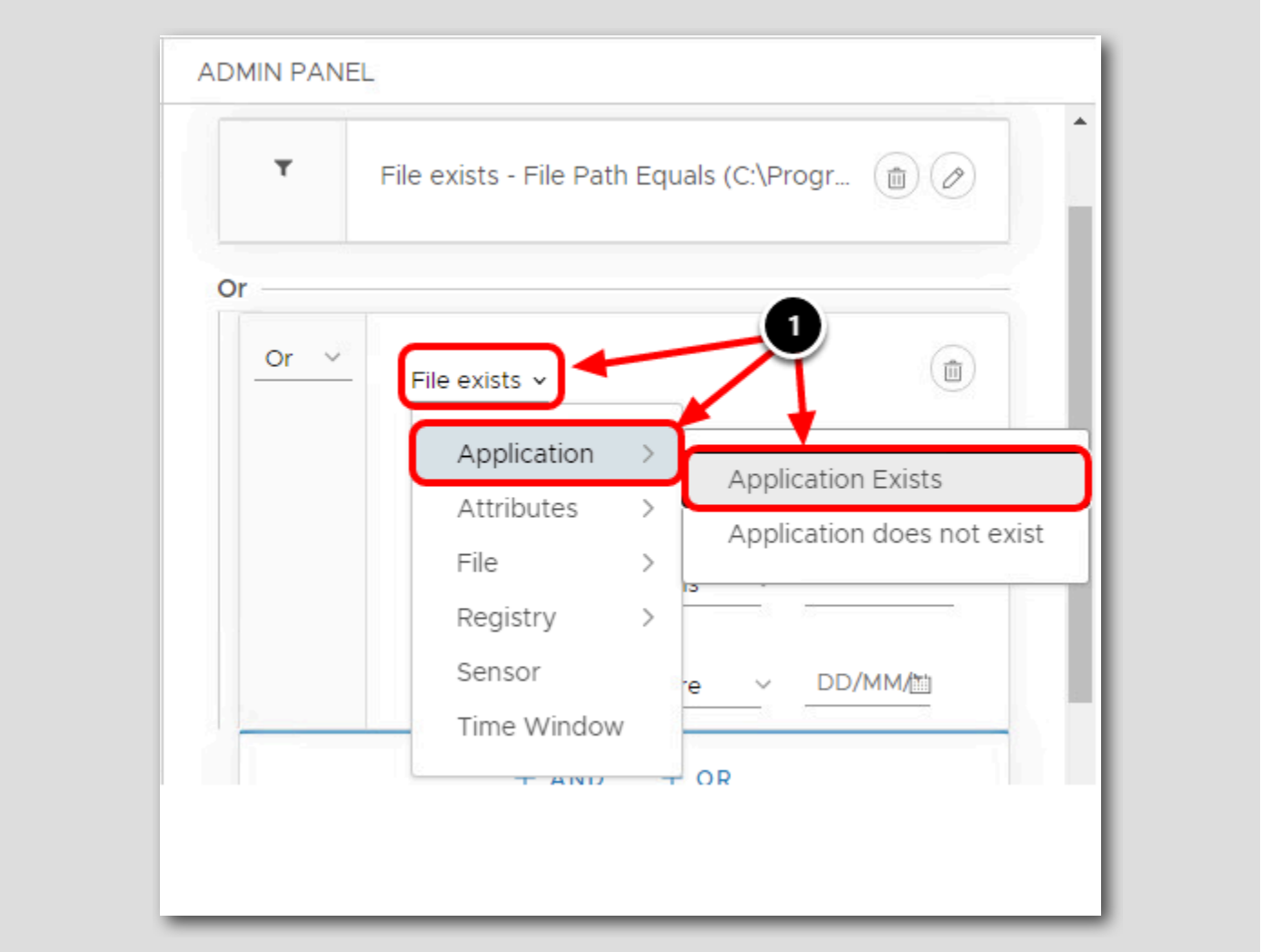
1. [File Path equals] セクションで、`C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE` と入力します。

   注： エラーを回避するために、コピーして貼り付けるか、クリックしてテキストを強調表示し、マニュアルからドラッグアンドドロップできることを忘れないでください。

2. [OR] を選択します。

[76]

[Application Exists] 条件値の追加

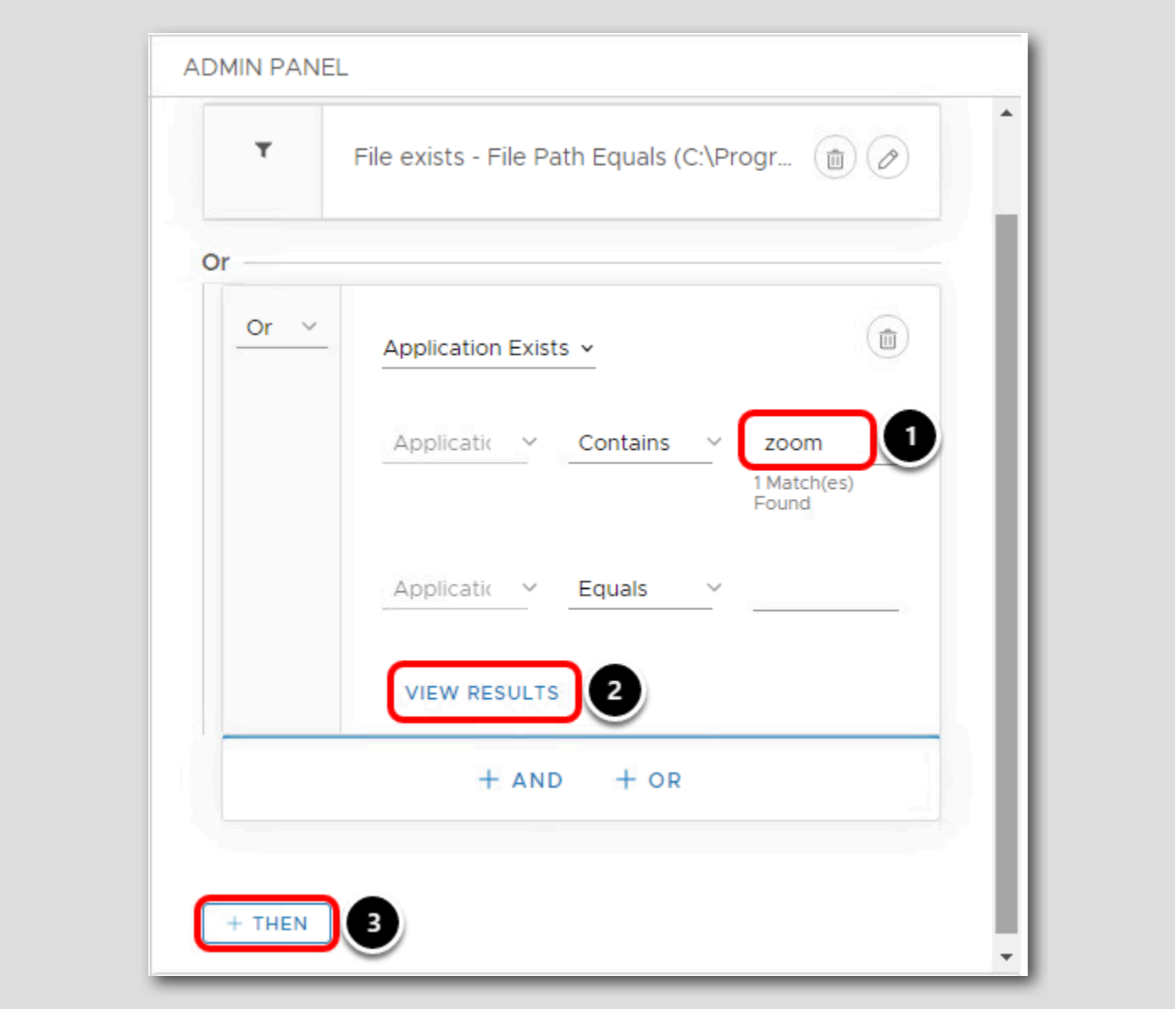


新しい [Or] セクションで、次の手順を実行します。

1. [File Exists] 条件をクリックし、[Application > Application Exists] を選択します。

[Or] 条件の追加

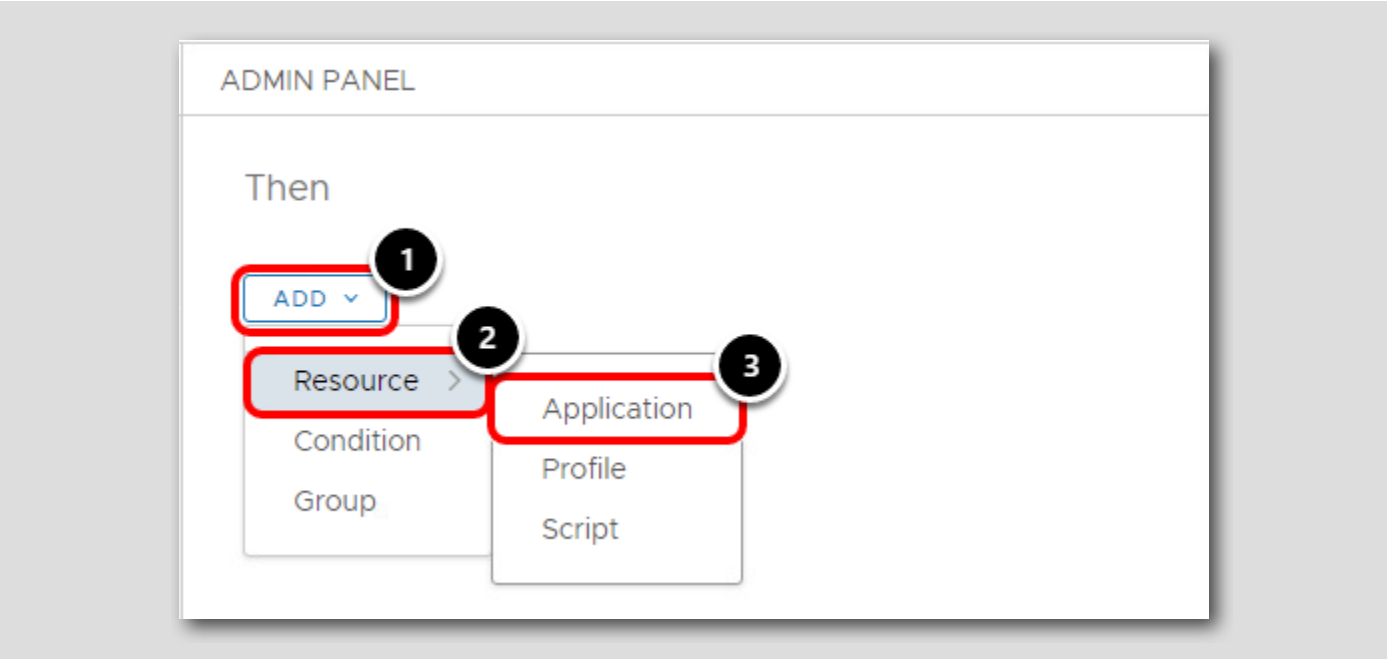
[77]



1. [Application Name Contains] フィールドに **Zoom** と入力します。フィールドの下に一致するアプリケーションの数が表示されていることを確認します。
2. これらの結果を表示するには、[View Results] をクリックします。ページの [< Back] ボタンをクリックして、[Or] アクションの構成に戻ります。
3. この If ステートメントのアクションを構成するには、[Then] を選択します。

[78]

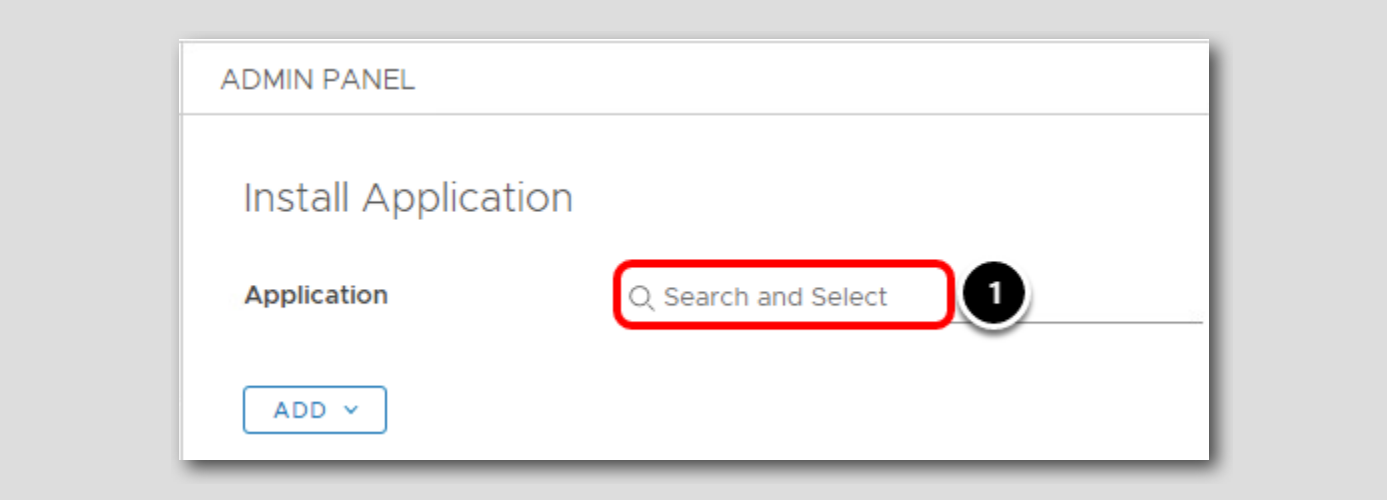
次のアクション：Zoom Plugin for Microsoft Outlook のインストール

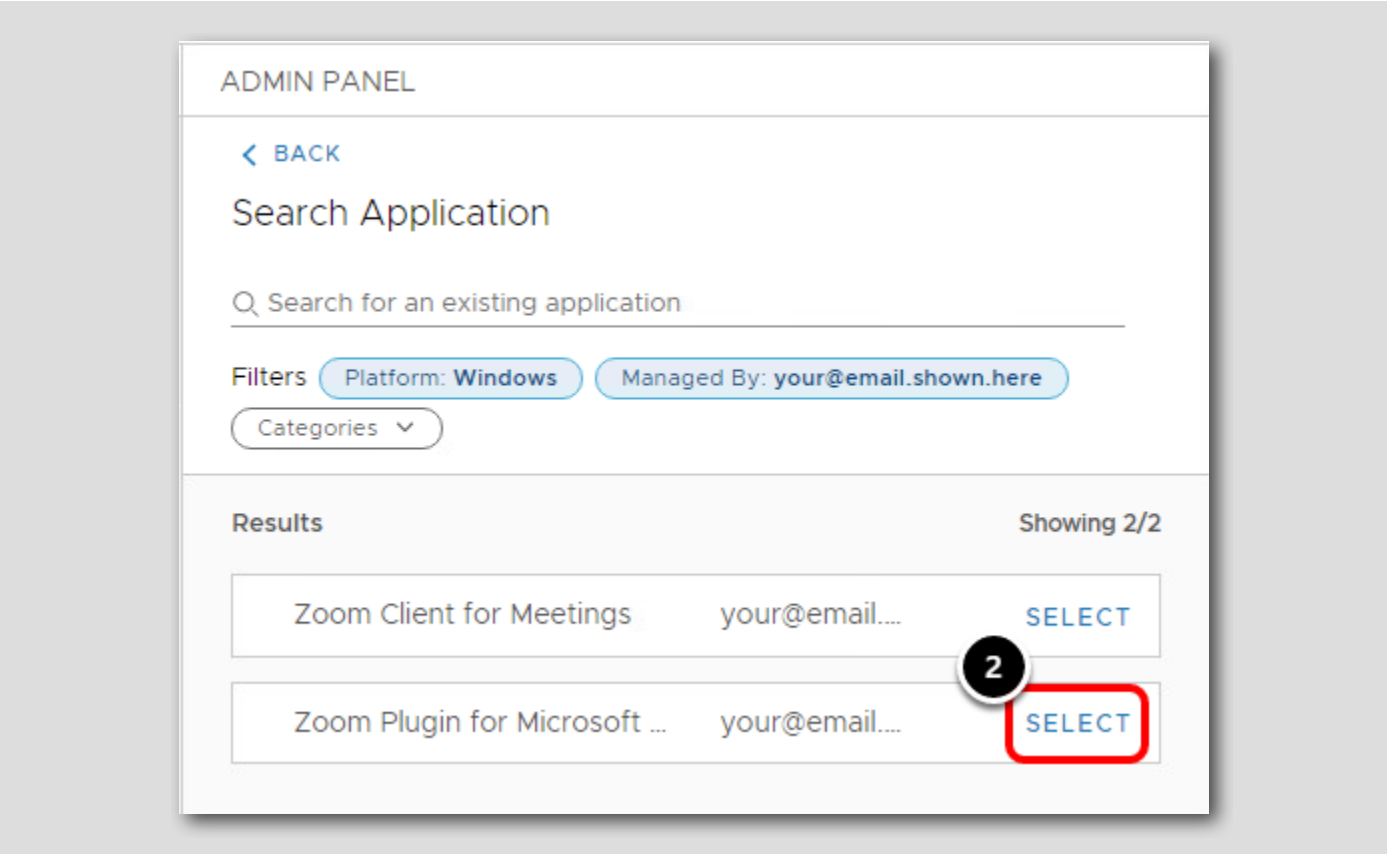


1. [Add] ドロップダウンをクリックします。
2. [Resources] を選択します。
3. [Application] をクリックします。

[79]

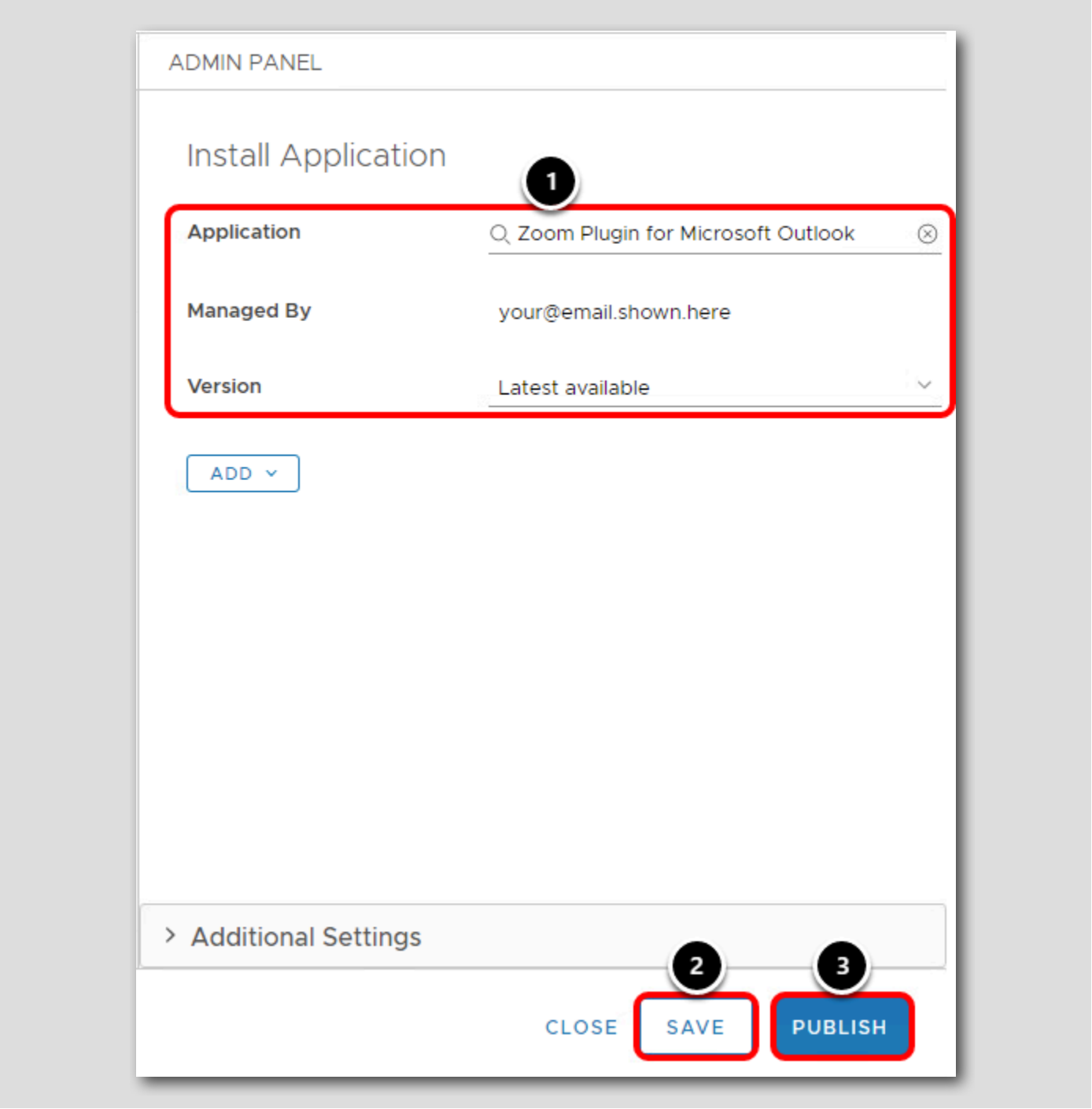
Zoom Plugin for Microsoft Outlook の選択





1. [Application] 検索フィールドをクリックします。
2. [Zoom Plugin for Microsoft Outlook] アプリケーションを選択します。

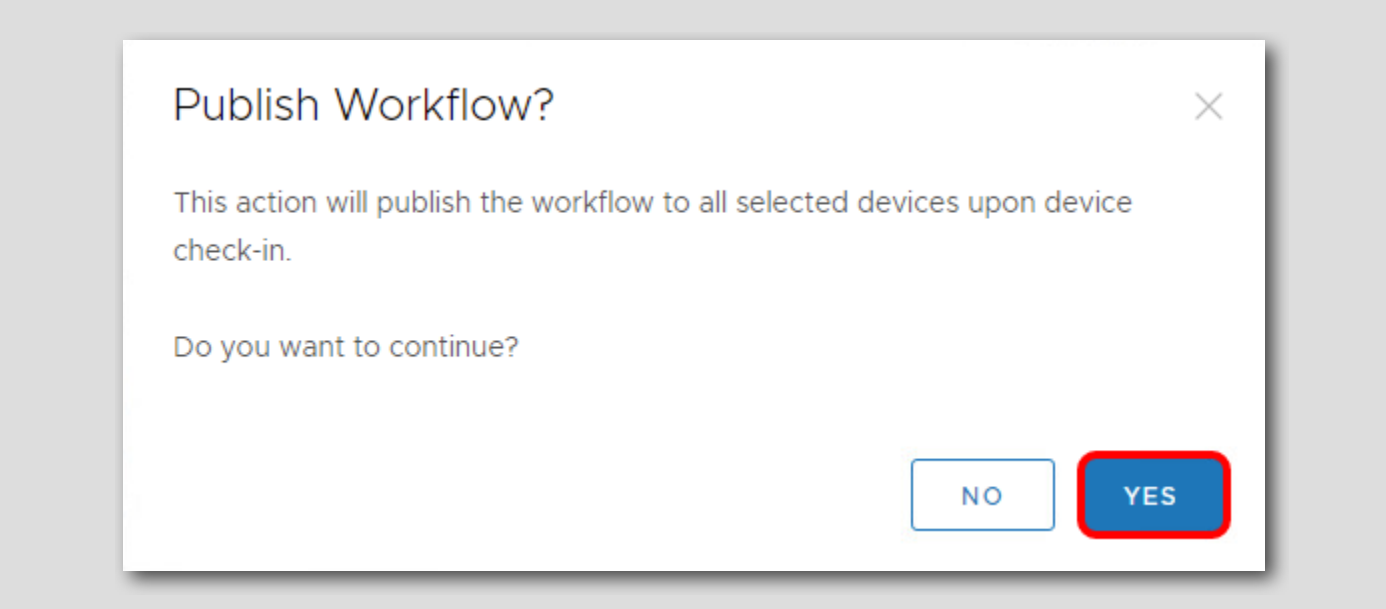
アプリケーション インストール設定の確認



1. アプリケーションの詳細を確認します。[Version] は [Latest available] を使用しています。つまり、Zoom Plugin for Microsoft Outlook アプリケーションの複数のバージョンがアップロードされると、最新のアプリケーションが使用されます。また、このユースケースで使用するバージョンを指定することもできます。
2. [Save] をクリックします。
3. [Publish] をクリックします。

ワークフローの公開

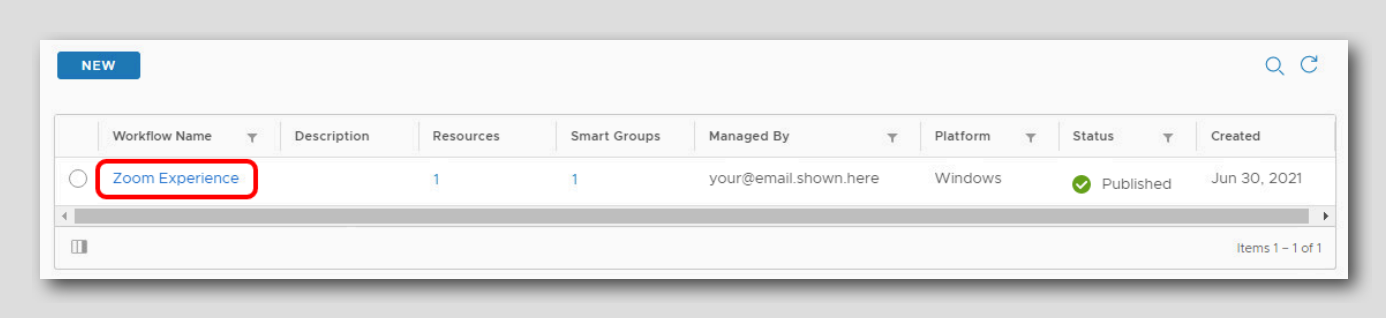
[81]



[Yes] を選択してワークフローを公開します。

ワークフローの確認

[82]

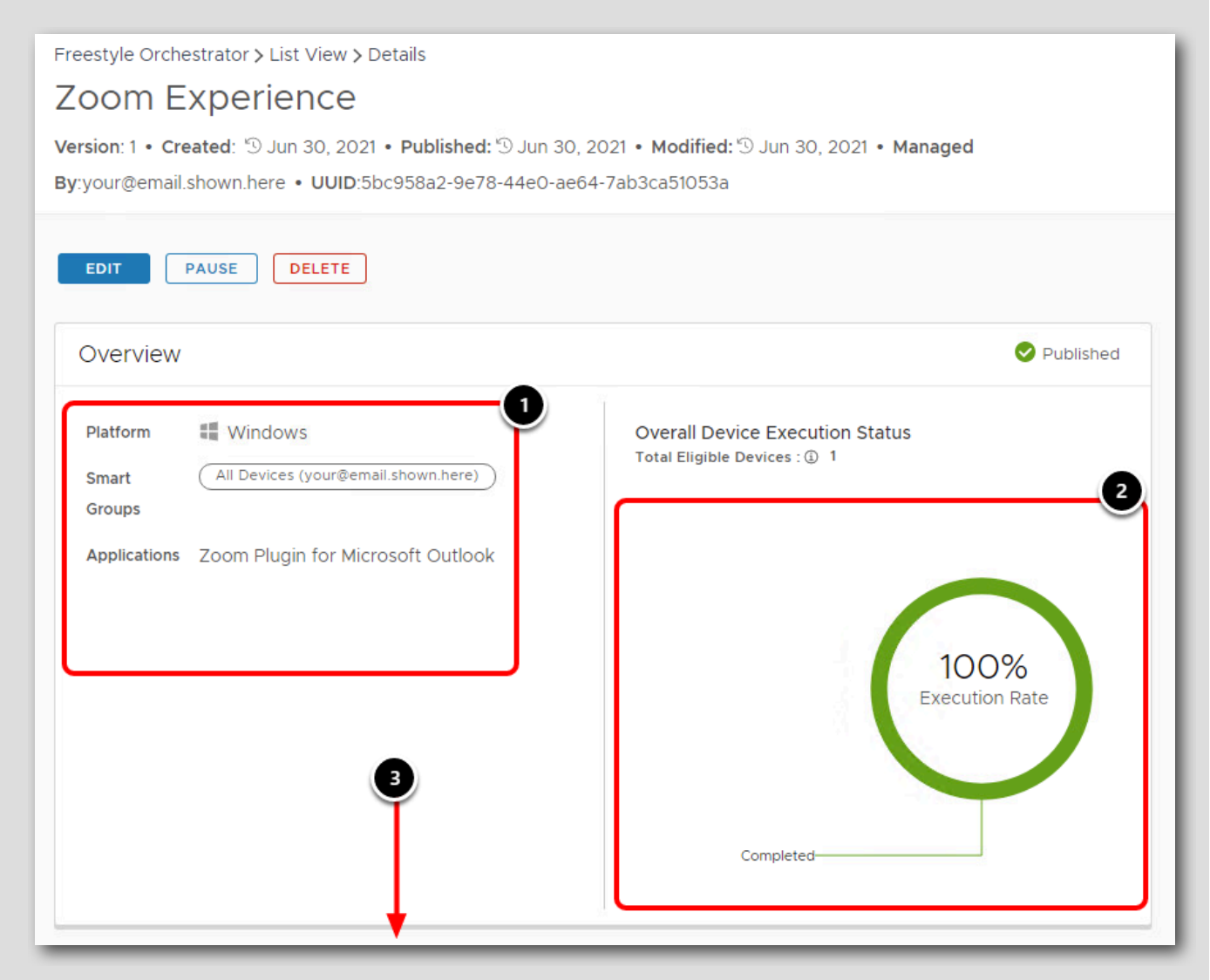


作成したワークフローのリストがこのページに表示され、名前、リソース、割り当てられたスマート グループ、ターゲット プラットフォーム、およびステータスが表示されます。

[Zoom Experience] ワークフローをクリックして、先ほど作成したワークフローを選択します。

ワークフローの概要の確認

[83]



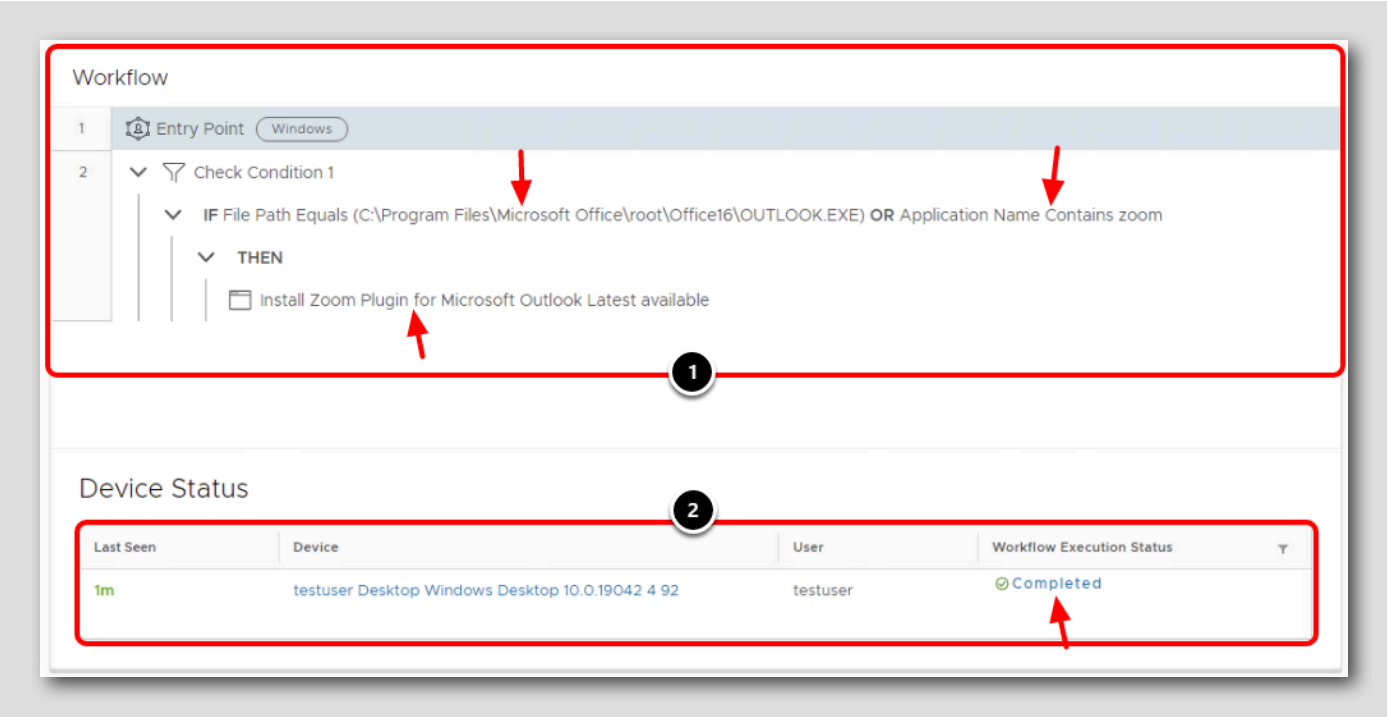
1. ワークフロー構成を確認します。ターゲット プラットフォーム、割り当てられたスマート グループ、およびこのワークフローに属するアプリケーションが表示されます。
2. ワークフロー デバイスの実行状態を確認します。割り当てられたデバイスの数とワークフローを受信したデバイスの数が表示されます。

   注：[Overall Device Execution Status] の下に「Device distribution is unavailable」と表示される場合があります。これに対処するには、以降の手順を実行します。

   注：デバイスのチェックイン時間に基づいて、データの更新に最大 4 時間かかる場合があります。ワークフローをデバイスに強制同期するには、[Device Details] ページを使用してデバイスのワークフローをクエリするか、ハブ/デバイスから強制同期します。
3. 下にスクロールします。

ワークフローの詳細とデバイスの確認

[84]



1. [Workflow details] を確認します。
   - 構成した条件を確認します：ファイルが存在する場合、またはアプリケーション名に Zoom が含まれている場合、「Install Zoom Plug in for Microsoft Outlook」コマンドを実行します。
2. ワークフローの [Device Status] を確認します。

   注：ワークフローがまだ実行されていない場合、[Device Status] にデバイスが表示されないことがあります。これに対処するには、以降の手順を実行します。

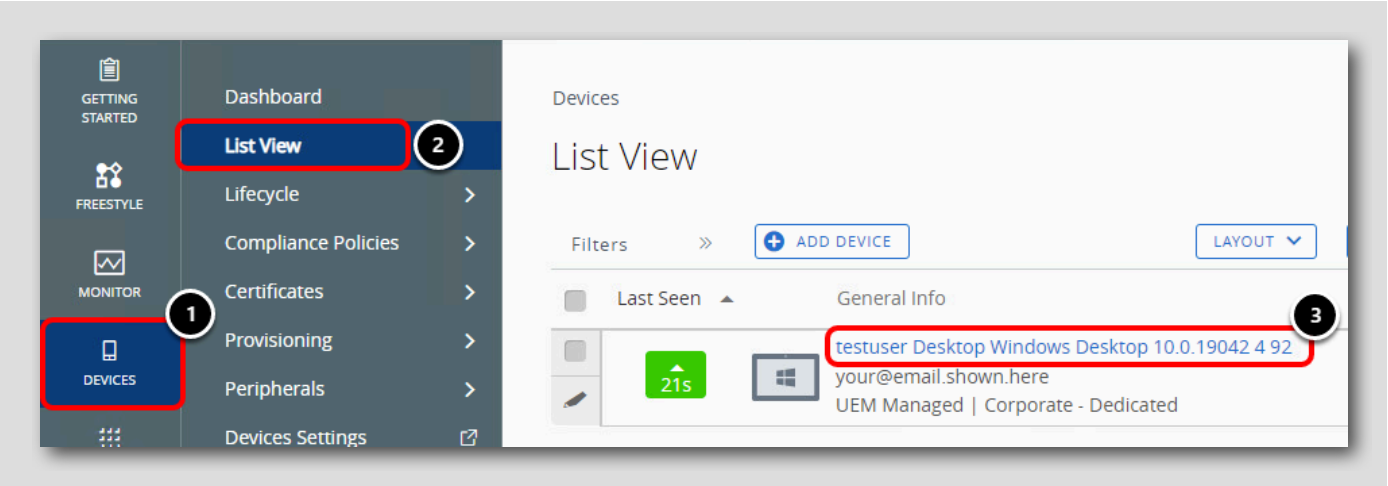
Workspace ONE UEM でのワークフロー実行の確認

[85]

ここで、Workspace ONE UEM 管理者コンソールからデバイスにクエリを実行して、ワークフローの実行を確認し、必要に応じて強制的に実行します。ワークフローは、実行してデータをコンソールに報告するのに時間がかかる場合があるため、これを使用して実行を高速化します。

デバイスへの移動

[86]

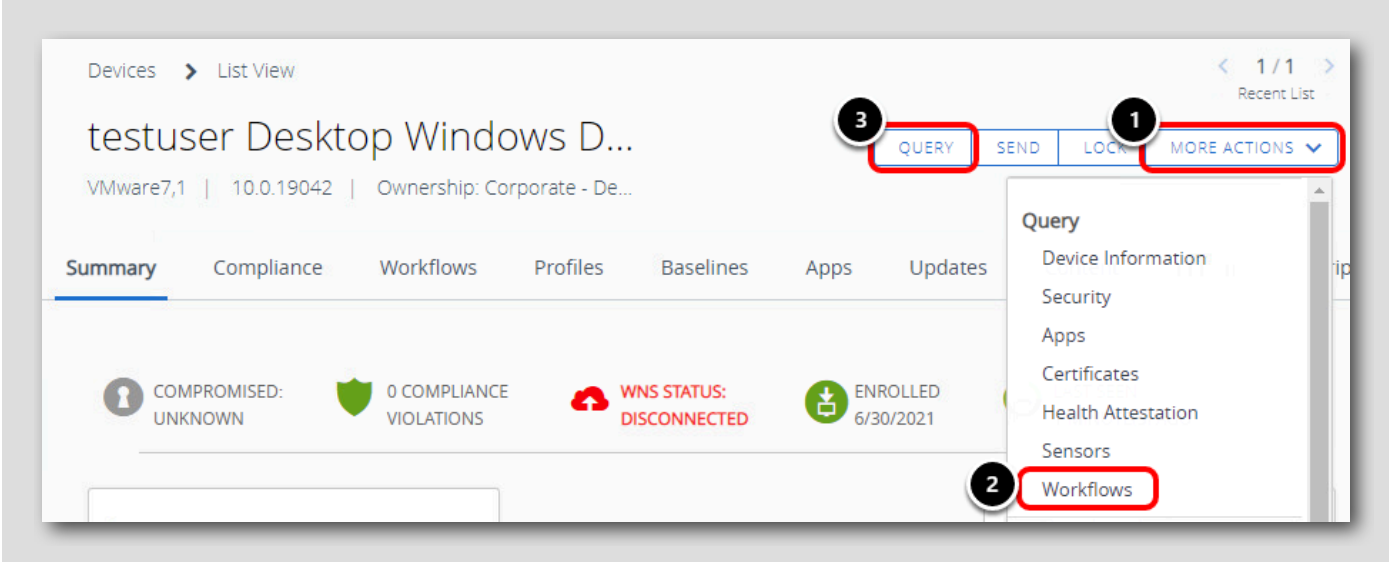


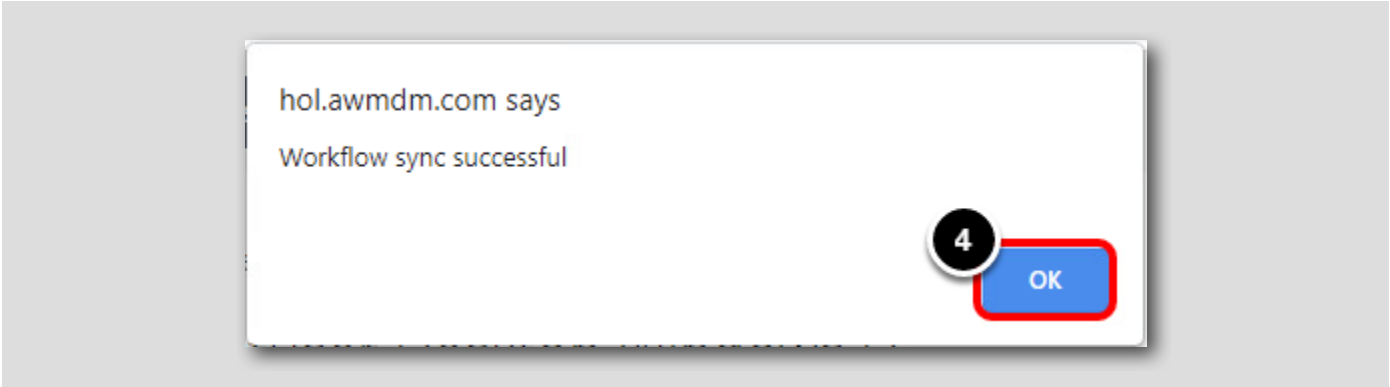
Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. [enrolled device name] をクリックすると、デバイスの詳細が表示されます。

デバイスの詳細のクエリ

[87]

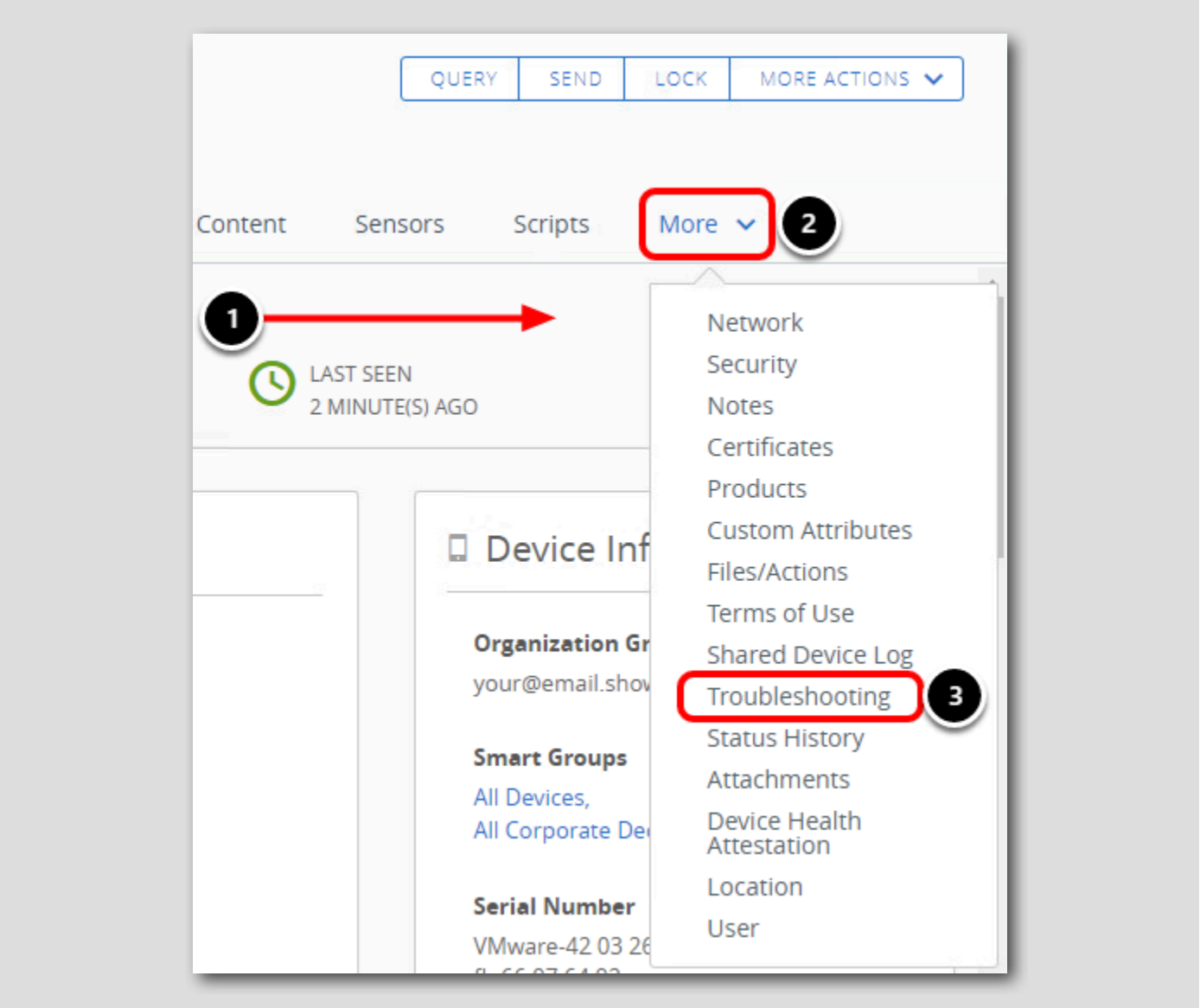




1. [More Actions] ドロップダウンをクリックします。
2. [Workflows] をクリックします。これにより、デバイスでワークフロー クエリがトリガされ、公開済みのワークフローがまだ処理されていない場合は処理されます。
3. または、[Query] をクリックして、デバイスに対して完全なクエリを実行することもできます。これにより、他のクエリ（デバイス サンプル、アプリケーション、証明書など）に加えてワークフロー クエリがトリガされ、公開されたワークフローも処理されます。
4. 同期が成功したことを示すメッセージが表示されたら、[OK] をクリックします。

デバイス クエリの確認

[88]

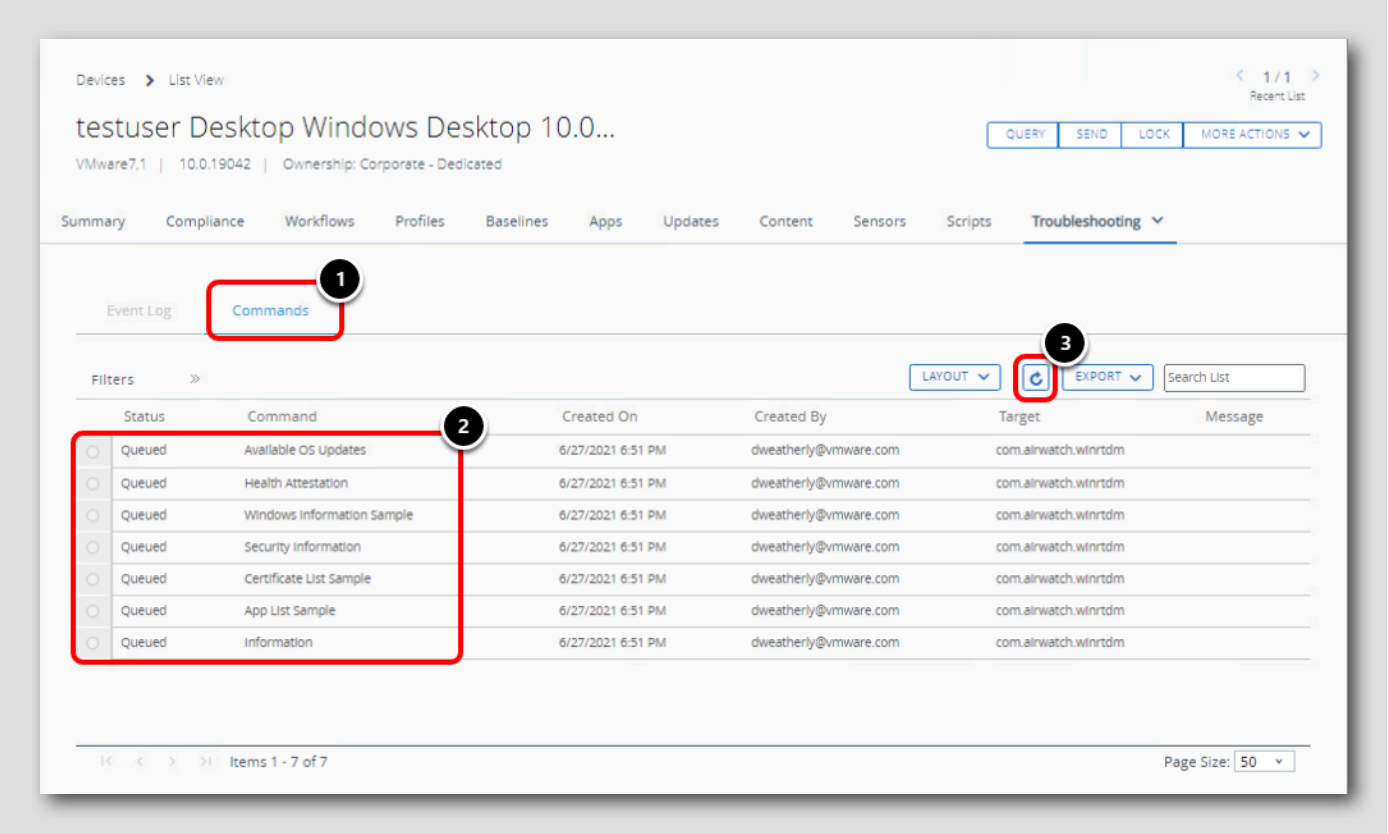


[Device Details] ページから、次の手順を実行します。

1. 必要に応じて右にスクロールして、[More] ドロップダウンを見つけます。
2. [More] を選択します。
3. [Troubleshooting] をクリックします。

コマンド キューの確認

[89]



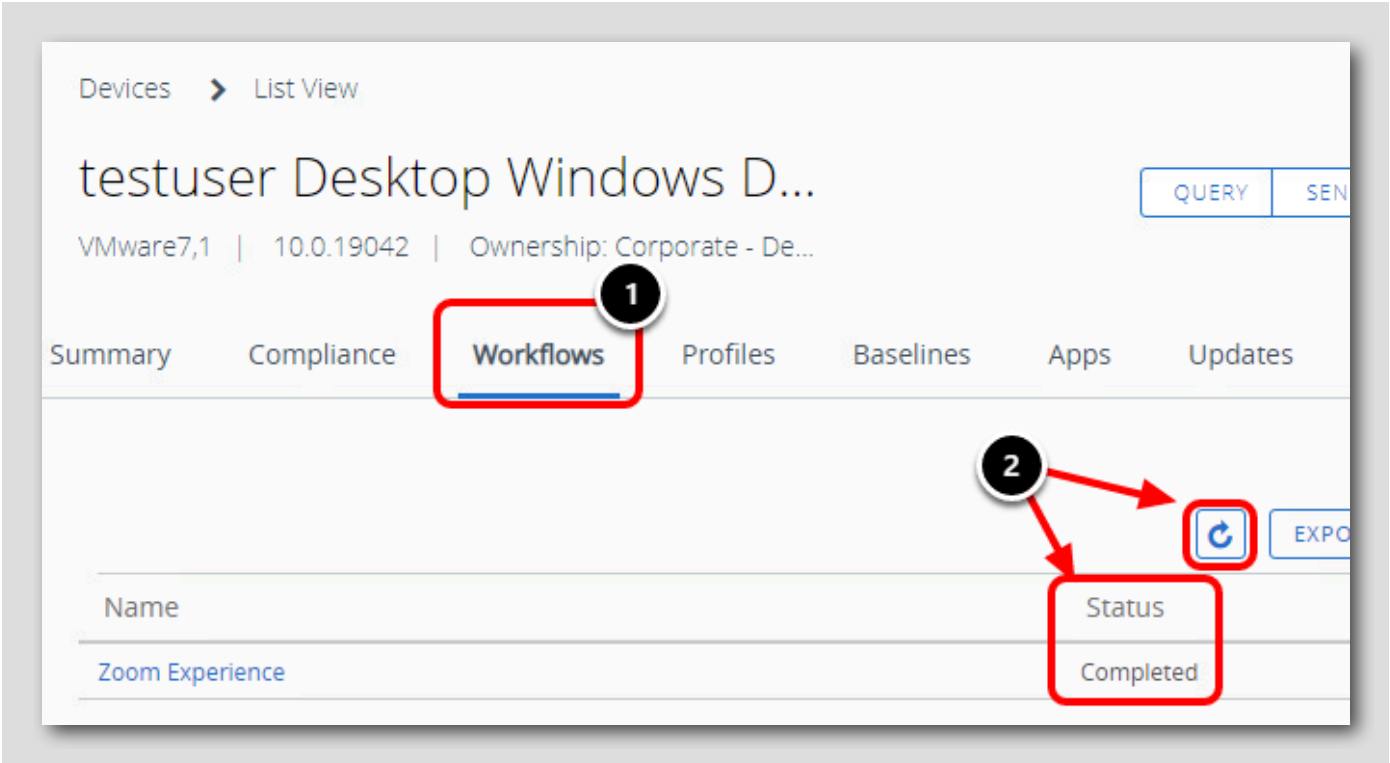
1. [Commands] タブを選択します。
2. キューにあるコマンドを確認します。
3. 数分ごと、またはコマンドがクリアされるまでページの更新ボタンをクリックします。

注: キューにコマンドが表示されない場合は、すでに処理されている可能性があります。

次の手順に進んでください。

デバイスでのワークフロー実行の確認

[90]



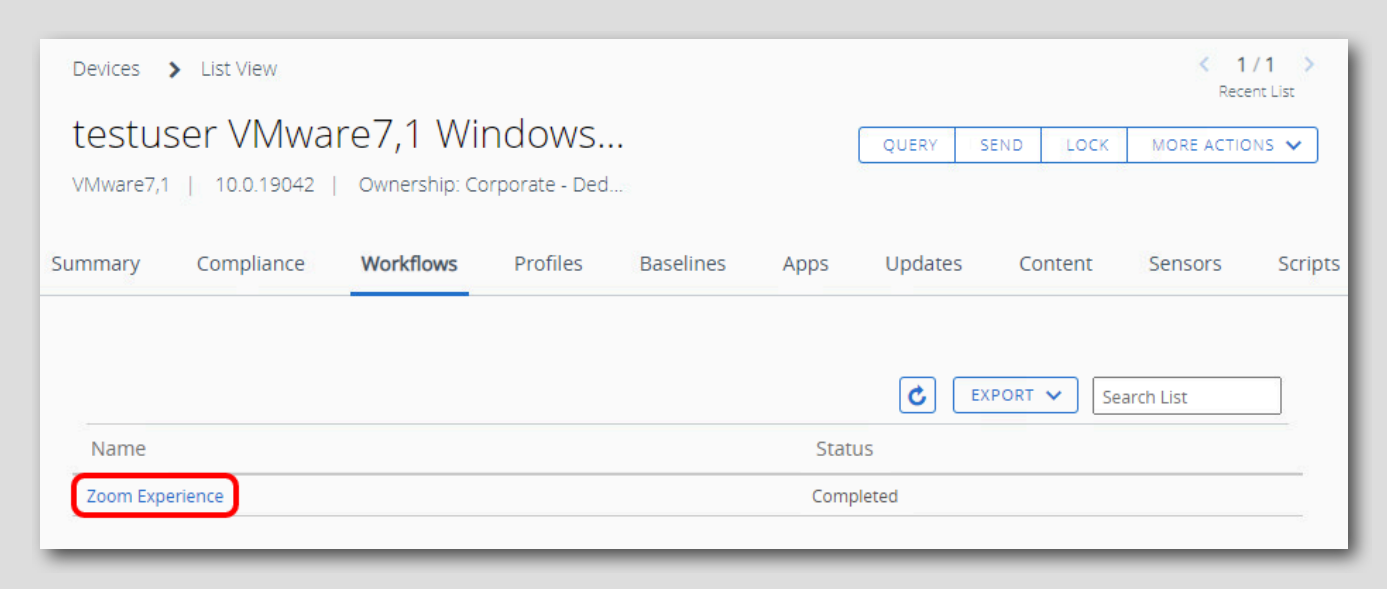
1. [Workflows] タブをクリックします。
2. Zoom Experience ワークフローのステータスが [Completed] かどうかを確認します。完了していない場合は、ステータスが [Completed] に変わるまで [Refresh] ボタンを定期的にクリックします。

   注：ワークフローが完了し、[Completed] と報告されるまで数分かかる場合があります。

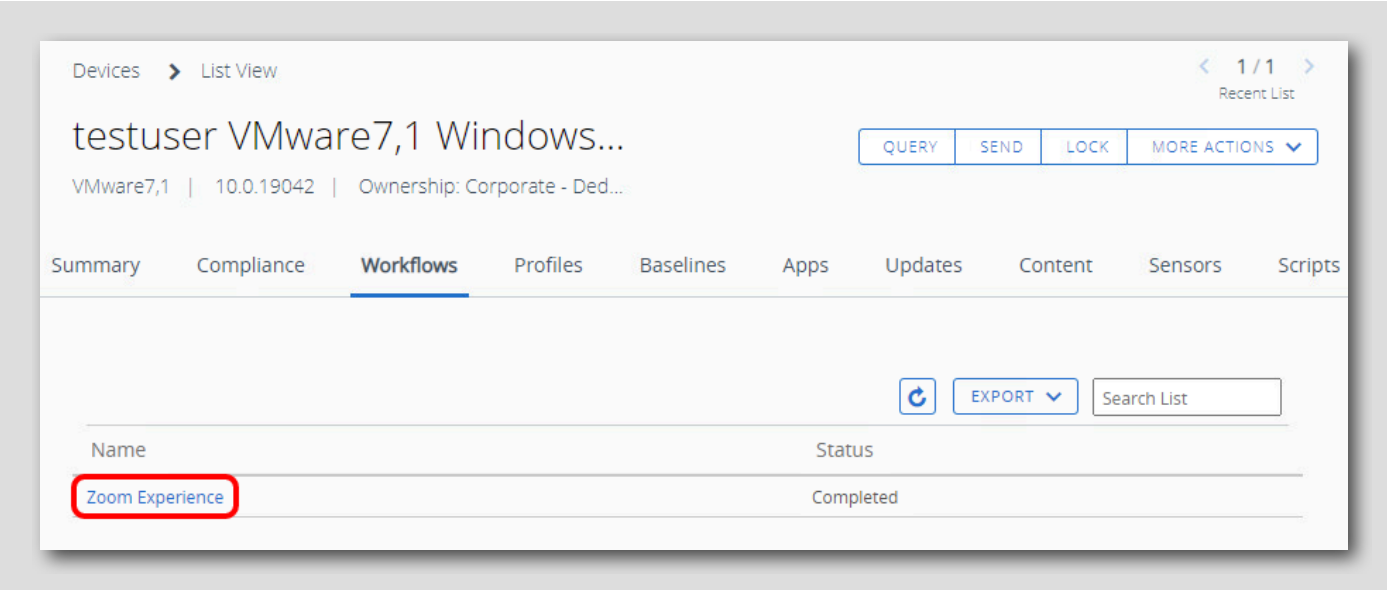
ワークフローのステータスが [Completed] になったら、次の手順に進みます。

デバイスでのワークフロー実行の確認

[91]

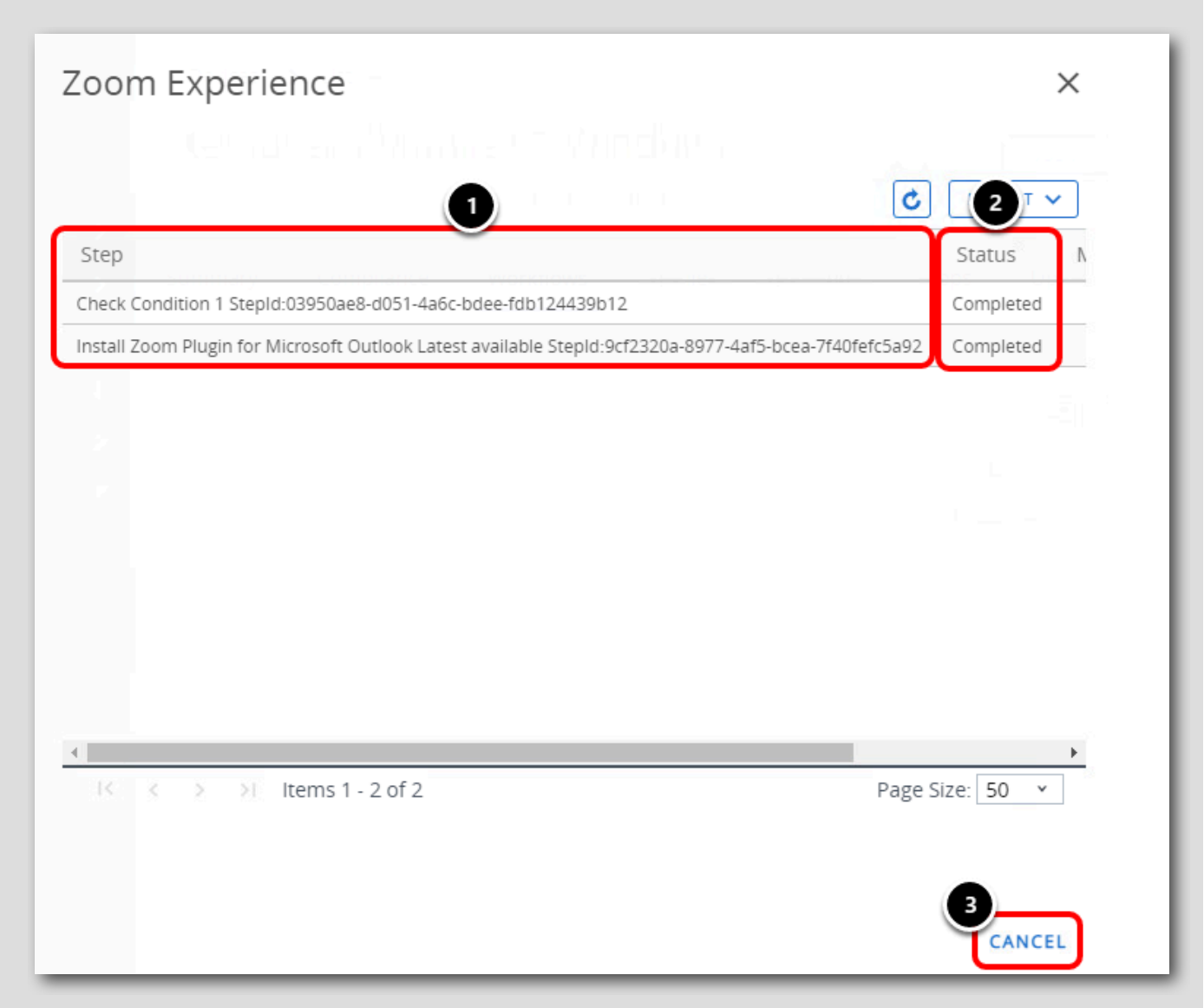


[Zoom Experience] ワークフローをクリックします。



デバイスで実行されたワークフローの確認

[92]



1. [Workflow Steps] を確認して、ワークフローで発生したアクションを確認します。
2. [Workflow Status] を確認して、各手順が完了したことを確認します。
3. [Cancel] をクリックしてワークフローを終了します。

Outlook プラグインがインストールされていることの確認

[93]

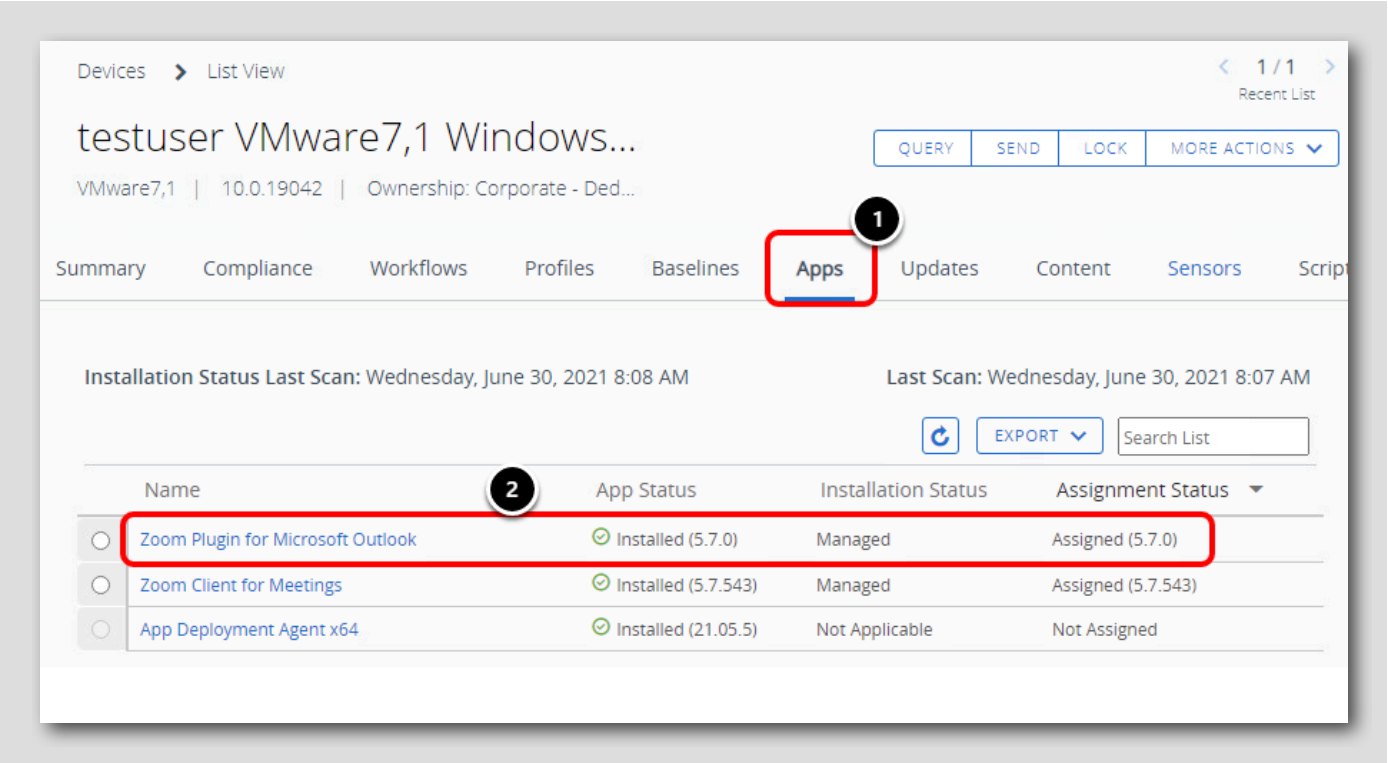
最後に、ワークフローが完了したことを確認するために、Zoom Outlook Plugin がデバイスにインストールされていることを確認します。

次の 2 つの方法で確認できます。

1. Workspace ONE UEM Console を使用して Zoom Outlook Plugin がインストールされていることを確認する
2. 直接デバイスで Zoom Outlook Plugin がインストールされていることを確認する

Workspace ONE UEM Console を使用して Zoom Outlook Plugin がインストールされていることを確認する

[94]

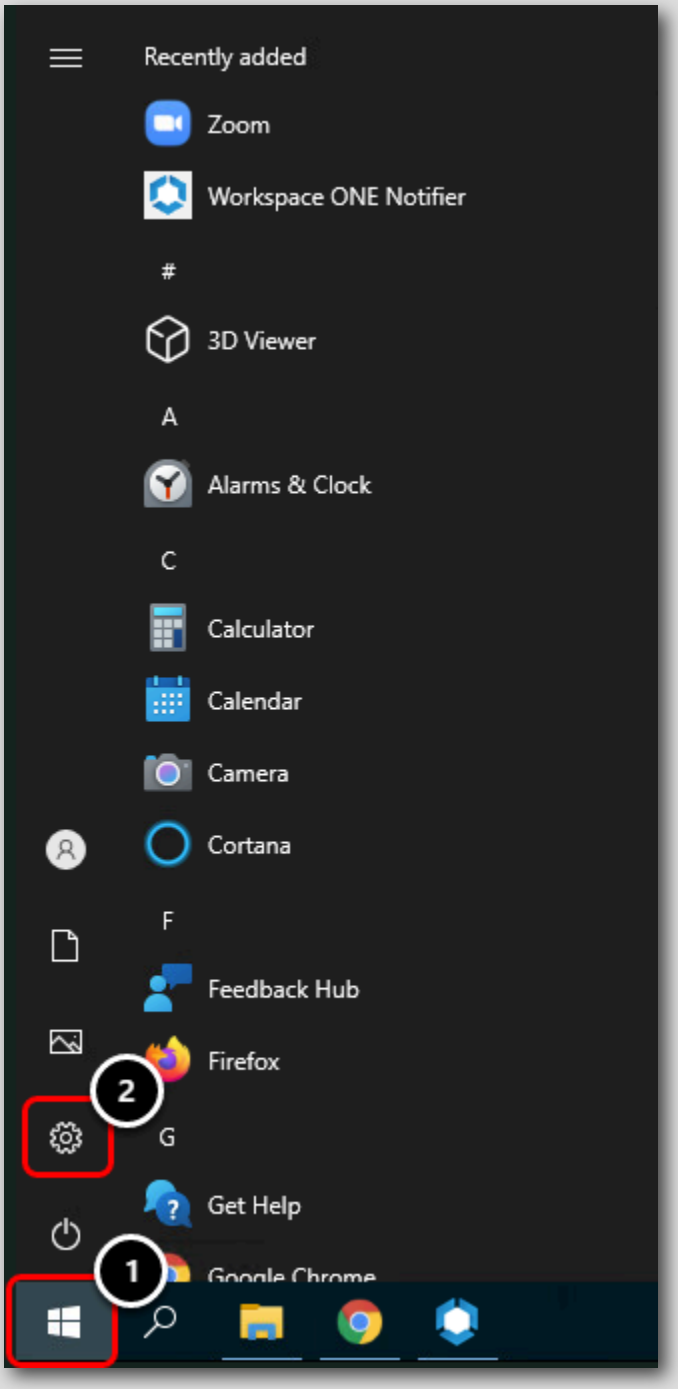


Workspace ONE UEM Console で、[Device Details] ページが開いていることを確認します。

1. **[Apps]** タブを選択します。
2. **[Zoom Plugin for Microsoft Outlook]** の [App Status] に [Installed] と表示されていることを確認します。

直接デバイスで Zoom Outlook Plugin がインストールされていることを確認する

[95]

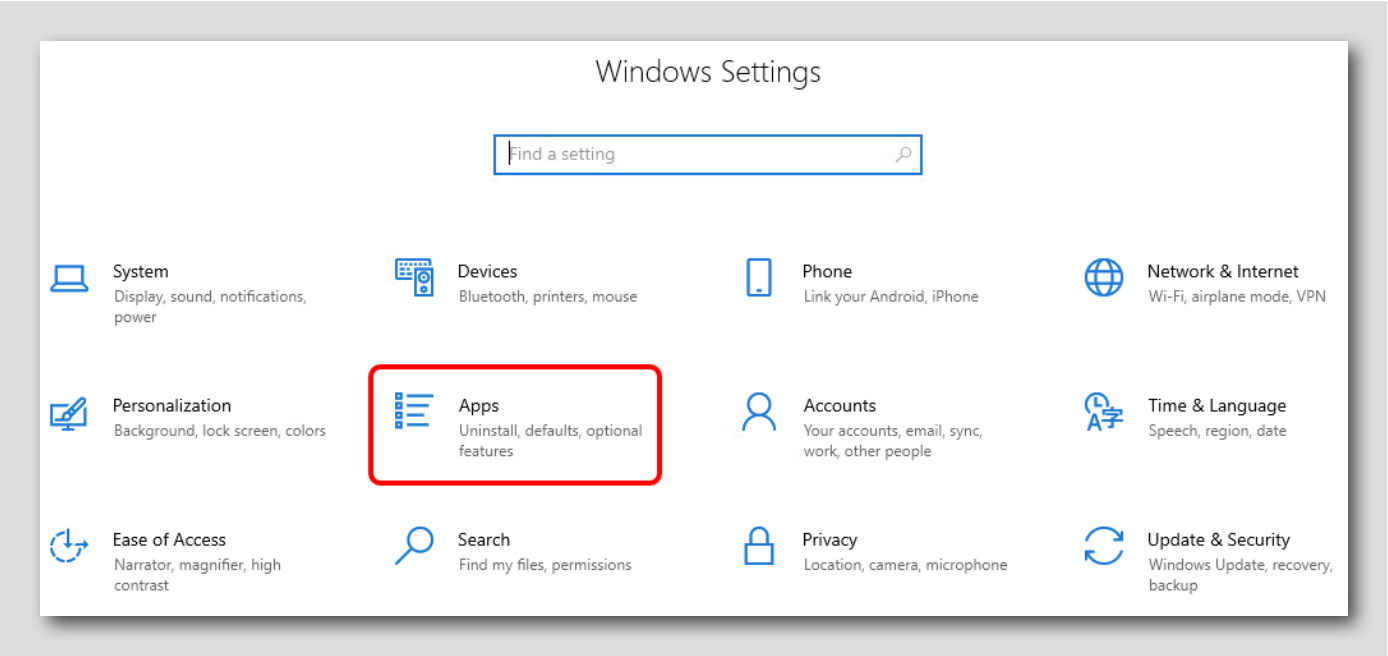


リモート デスクトップ経由で接続している Win10-01a 仮想マシンで、次の手順を実行します。

1. Windows ボタンをクリックします。
2. [Settings] を選択します。

[Applications] を選択します。

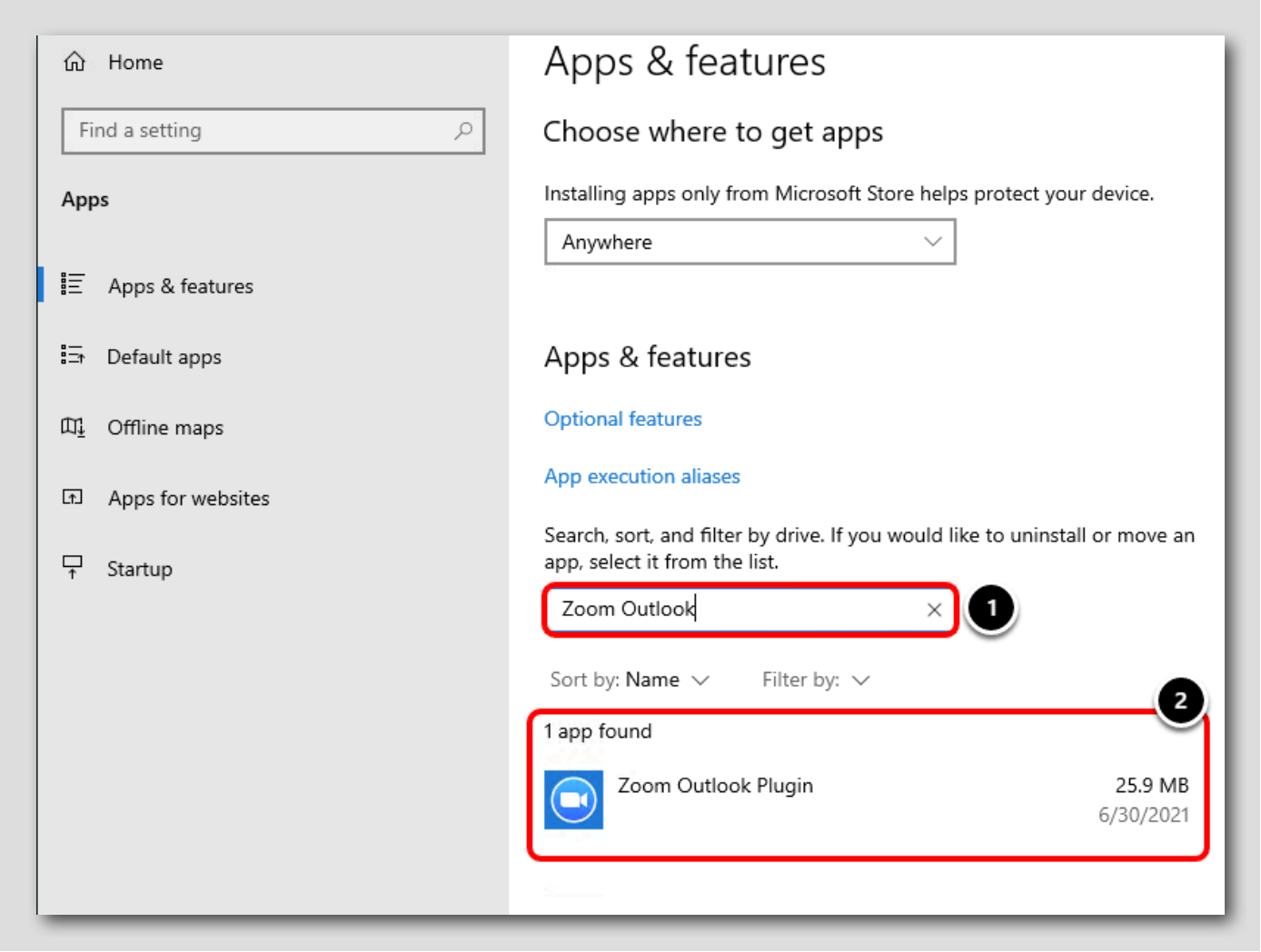
[96]



[Apps] をクリックします。

Zoom Outlook の検索

[97]



1. 検索バーに **`Zoom Outlook`** と入力します。
2. [Zoom Outlook Plugin] がインストール済みアプリケーション リストに表示されていることを確認します。

これで、Freestyle Orchestrator によって構築されたワークフローの一部として Zoom Outlook Plugin がインストールされていることを確認しました。Zoom Outlook Plugin は、Zoom インストール パスが入力され、アプリケーションがデバイスに存在していることを確認して、アプリケーションに Zoom アプリケーションがインストールされていることを確認した後にのみインストールされました。

Windows 10 デバイスの登録解除

[98]

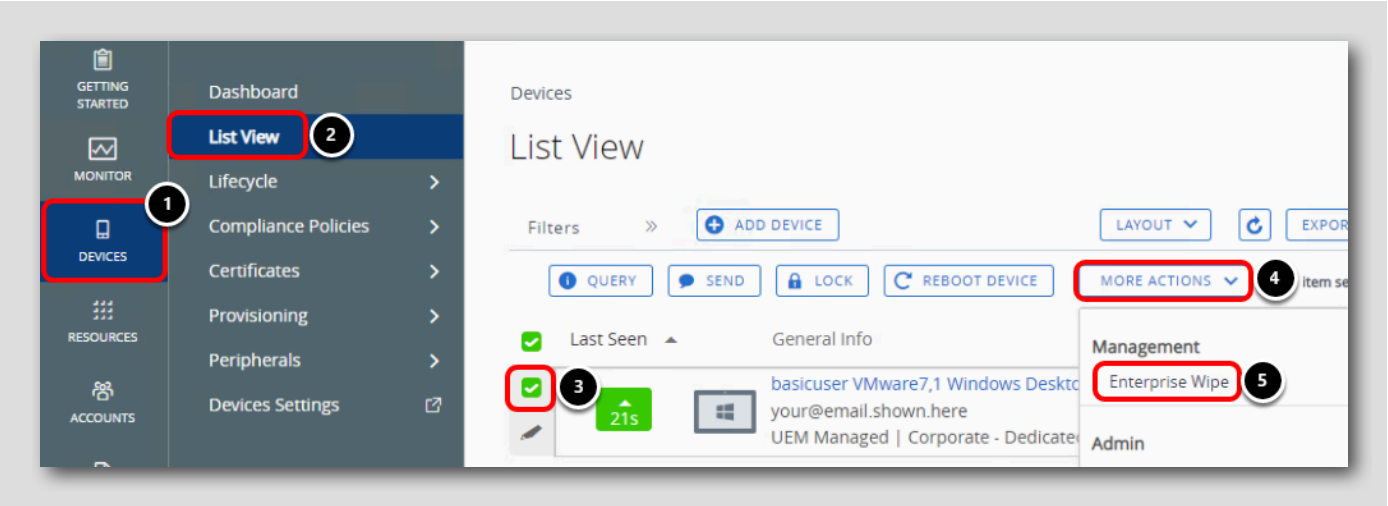
このセクションでは、Windows 10 仮想マシンの登録を解除して、他のラボ モジュールで使用できるようにします。

Enterprise Wipe ワイプ コマンドを使用して、Workspace ONE によってデバイスにプッシュされたすべての管理対象コンテンツ（プロファ

イルやアプリケーションなど）を削除しますが、デバイス上の個人的なコンテンツやデータは変更しません。

Workspace ONE UEM Console からの企業情報ワイプ

[99]

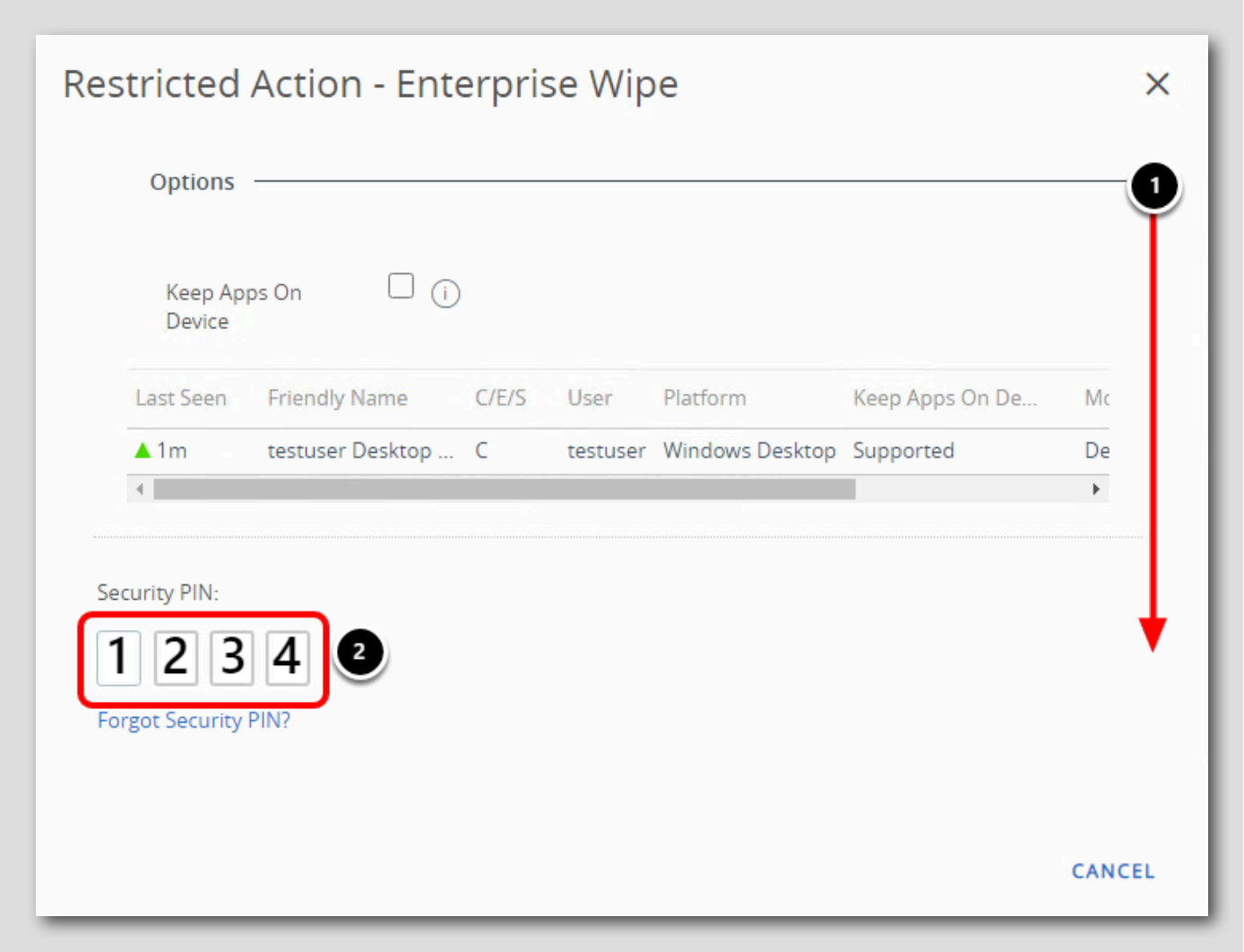


Google Chrome で Workspace ONE UEM 管理者コンソールに戻ります。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. デバイスのフレンドリ名の横にあるチェックボックスを選択します。
4. [More Actions] をクリックします。
5. [Enterprise Wipe] をクリックします。

PIN の入力とデバイスの企業情報ワイプ

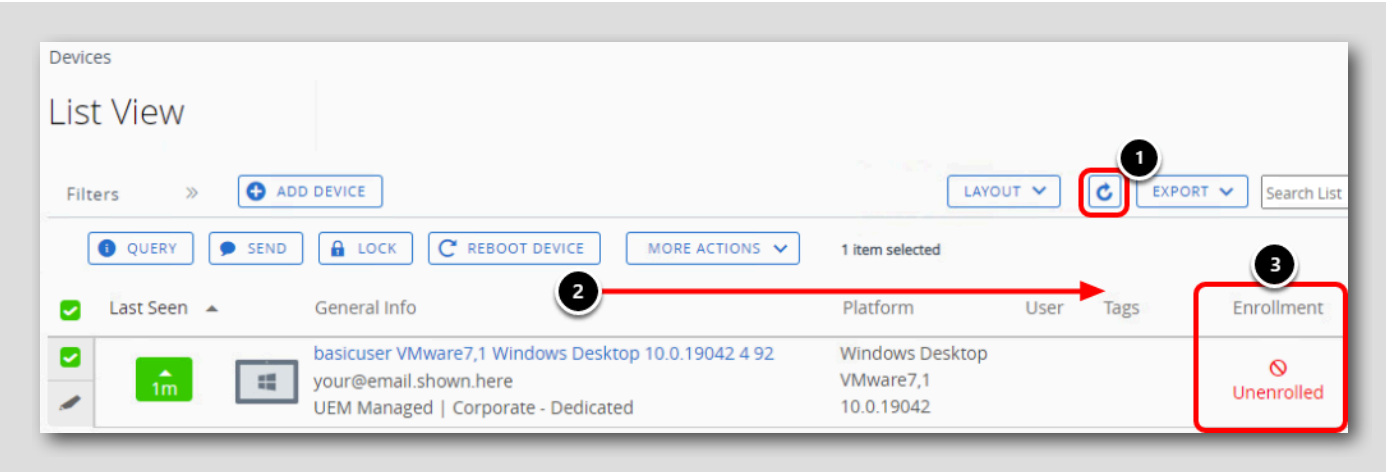
[100]



1. [Security PIN] 入力を見つけるために、下にスクロールする必要がある場合があります。
2. Workspace ONE UEM 管理コンソールに初めてログインしたときに作成したセキュリティ PIN (**1234**) を入力します。別の PIN を使用した場合は、代わりにその PIN を入力します。
3. **[Delete]** をクリックします。

企業情報ワイプの検証

[101]

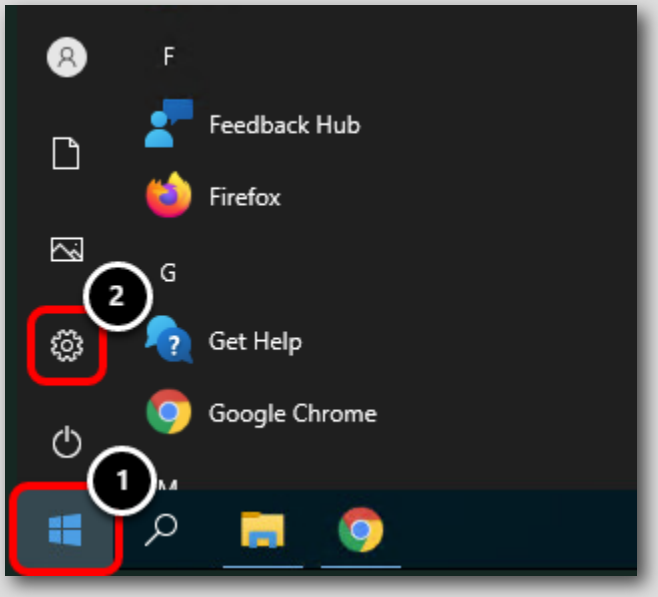


注：企業情報ワイプの処理には、数分かかる場合があります。

1. 更新アイコンを定期的にクリックしてページを更新し、企業情報ワイプが処理されたかどうかを確認します。
2. 必要に応じて、右にスクロールして [Enrollment] 列を見つけます。
3. 企業情報ワイプ コマンドが処理されると、デバイスの登録状態が [Unenrolled] に変わります。

[Windows 10 Settings] への移動

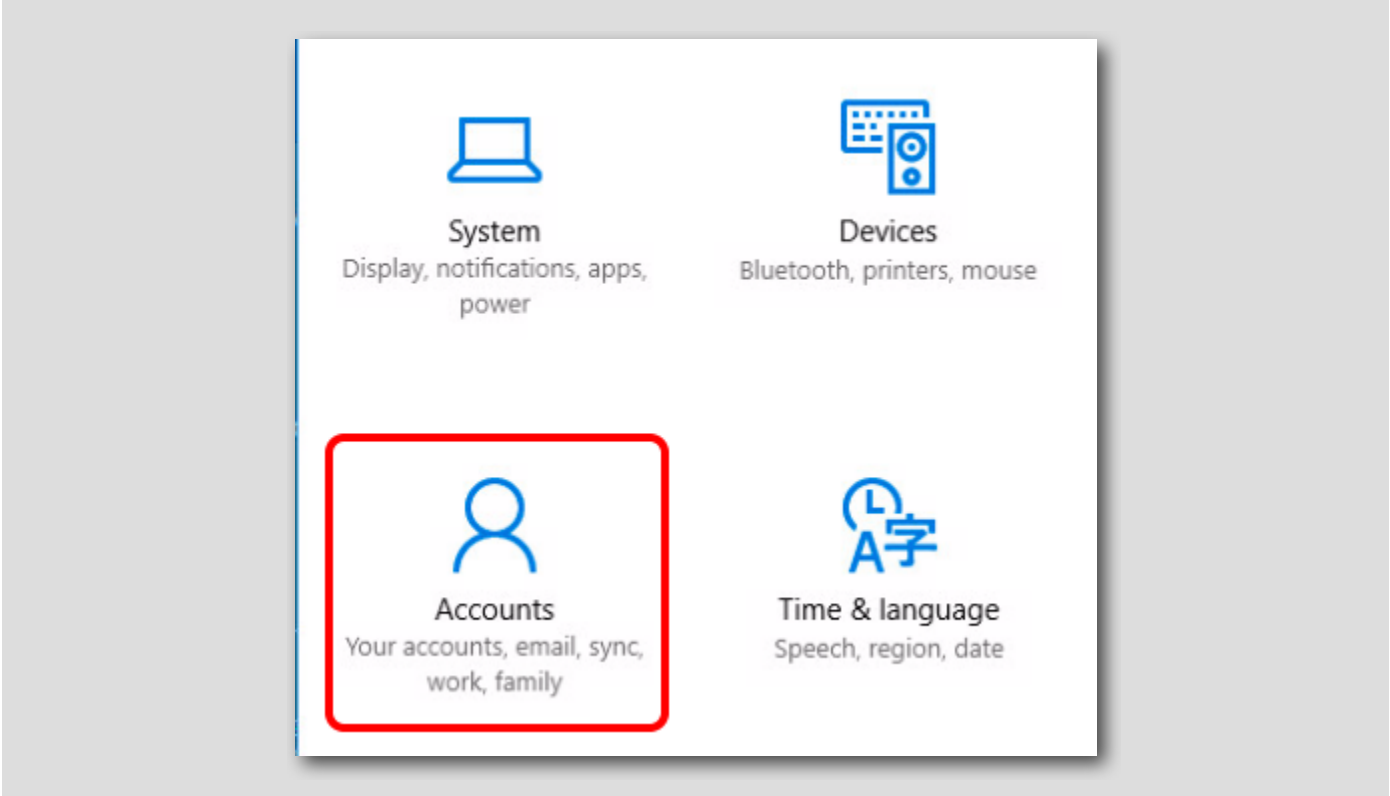
[102]



1. Windows アイコンをクリックします。
2. 歯車アイコンをクリックして、[Windows 10 Settings] にアクセスします。

[Accounts] 設定へのアクセス

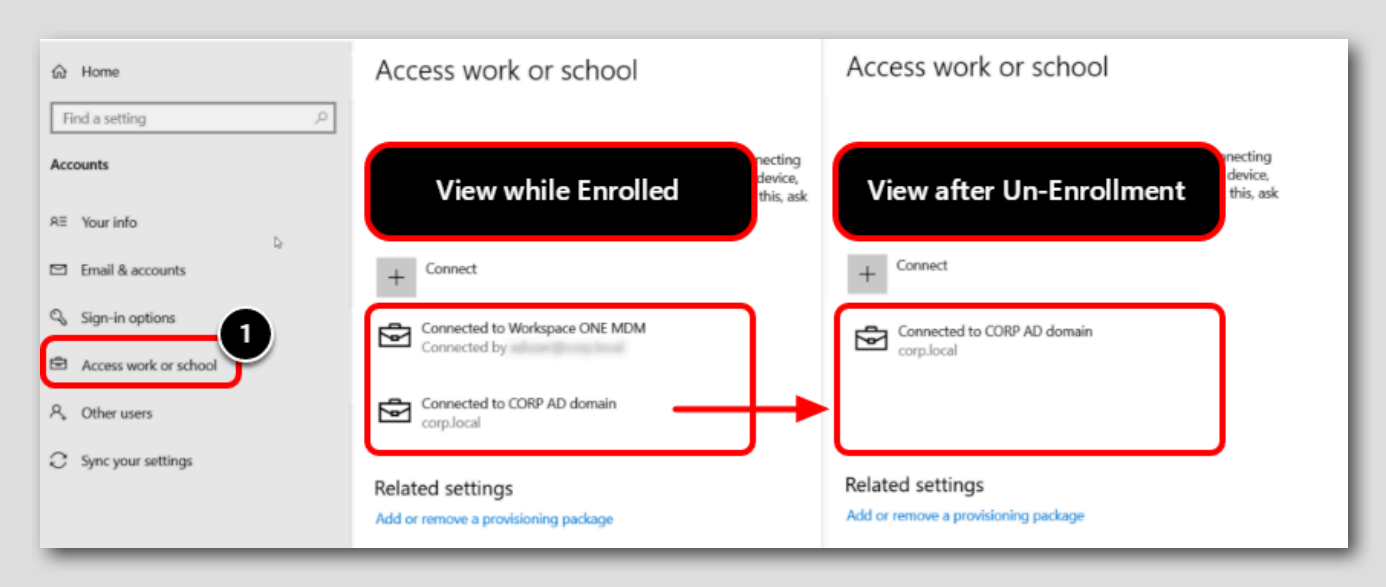
[103]



[Settings] メニューから **[Accounts]** にアクセスします。

管理アカウントが存在しないことの検証

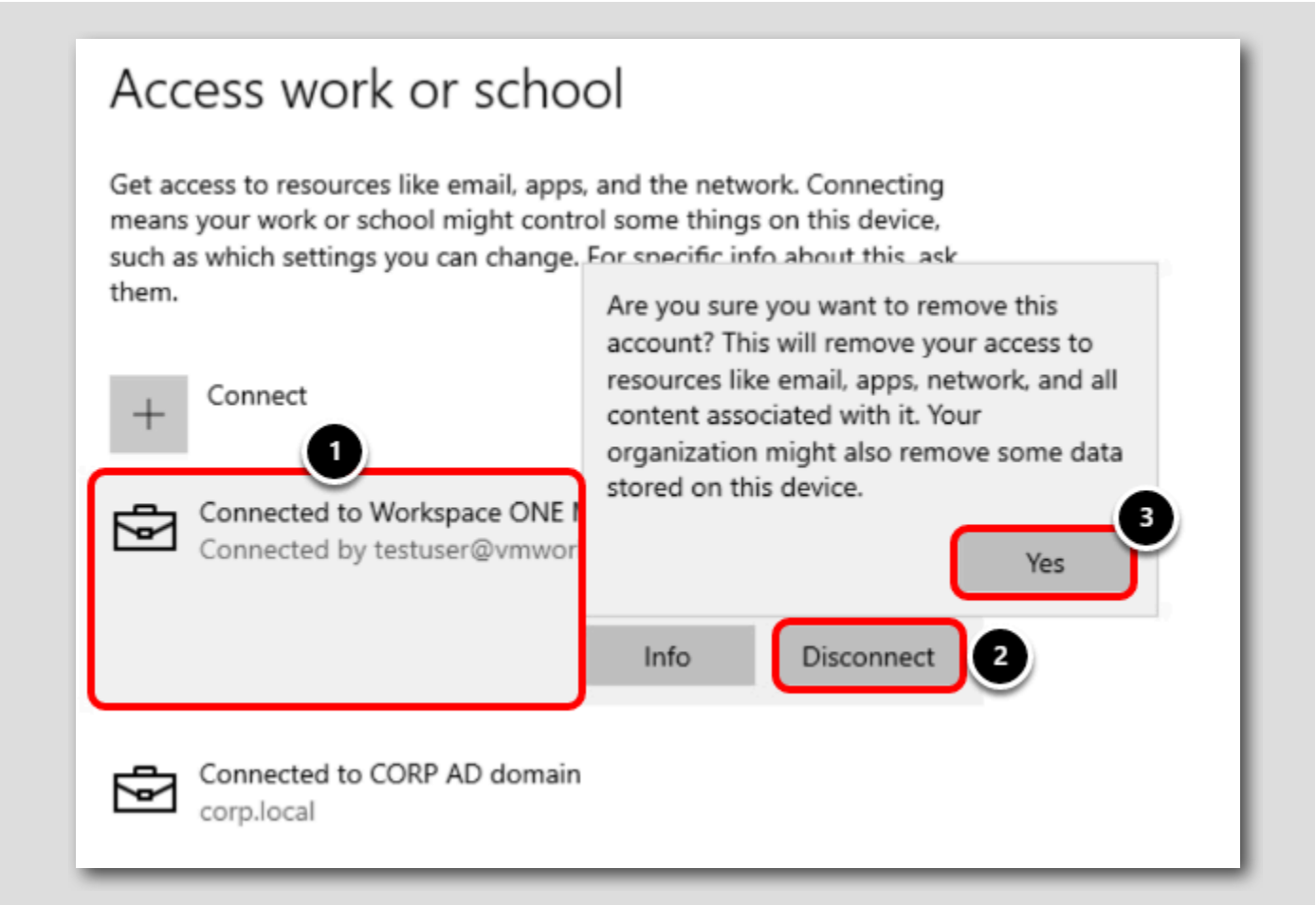
[104]



1. [Access work or school] をクリックします。
2. Workspace ONE MDM に接続されているアカウントがないことを確認します。

注：このラボでは、CORP AD ドメインはローカル ドメインであり、Workspace ONE UEM 登録によって管理されていないため、デバイスの登録時または登録解除時にこの接続が表示されます。

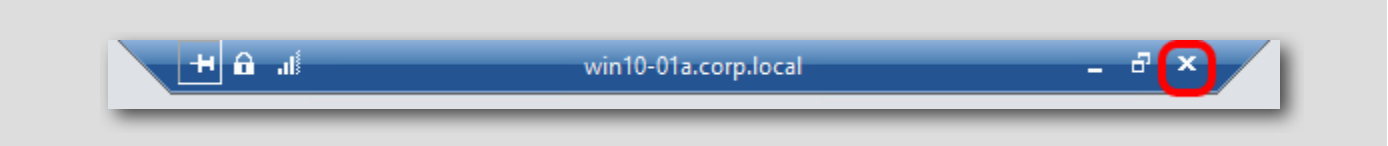
注：[Access Work or School] ページが以前に開かれていた場合は、ページを更新するか、ページから移動してから戻り、変更を確認する必要がある場合があります。



1. [Connected to Workspace ONE UEM] アカウントをクリックします。
2. [Disconnect] をクリックします。
3. [Yes] をクリックします。

メイン コンソールに戻る

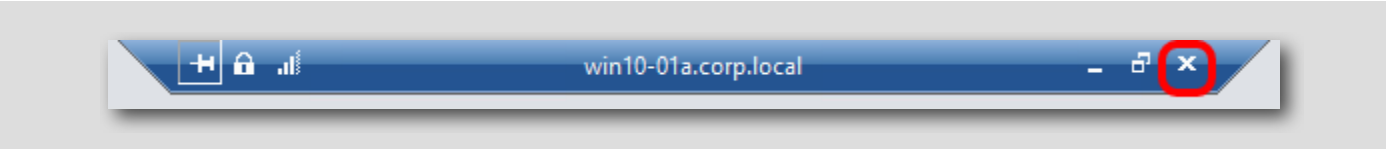
[105]



画面上部の [Remote Desktop Connection] バーで [Close (X)] をクリックしてメイン コンソールに戻り、Workspace ONE UEM Console 内での構成を完了します。

注：[Remote Desktop Connection] バーが表示されない場合は、固定が解除されている可能性があります。画面の上部にカーソルを置くと、

[Remote Desktop Connection] バーが再度表示されるので、[Close] をクリックします。



まとめ

[106]

おめでとうございます。Freestyle Orchestrator の概要モジュールが完了しました。

また、特定のアプリケーションまたはファイルが最初に存在する必要がある場合に条件に基づいてアプリケーションをインストールする Windows 10 デバイスのユースケースについて説明しました。

このモジュールでは、次の事項について学習しました。

- エンタープライズ アプリケーション リポジトリ
  経由のアプリケーションの割り当て
  - Zoom Client for Meetings アプリケーションの構成（自動インストール）
  - Zoom Plugin for Microsoft Outlook の構成（オンデマンドで利用可能）
- Freestyle Orchestrator を使用したワークフローの作成
- Workspace ONE UEM でのワークフロー実行の確認
- デバイスでのワークフロー実行の確認

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[107]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。

モジュール 2：Windows 10 管理の概要（30 分）

はじめに

[109]

Windows 10 デバイスを Workspace ONE UEM に登録する方法と、制限事項プロファイルとアプリケーションを構成して登録済みデバイスに展開する方法について説明します。

前提条件

[110]

このハンズオン ラボを修了するには、次のものが必要となります。

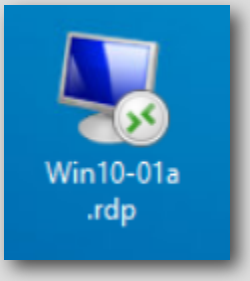
- 最新の更新プログラムがインストールされた Windows10（Home Edition を除く）が実行されている仮想マシンまたはスペアの Windows デバイス。管理対象にするマシンからハンズオン ラボにアクセスしないでください。

  注：このラボの前提条件がすべて設定済みの Windows 10 仮想マシンが用意されています。このラボのマニュアルに従って、この仮想マシンを利用されることをおすすめします。
- ハンズオン ラボを実施するために使用する仮想マシンまたはスペア Windows デバイスに対する管理者権限。
- 7-Zip などの Windows 10 デスクトップ アプリケーション (*.msi)。実習用マシンに Windows 10 アプリケーションのサンプルが用意されています。

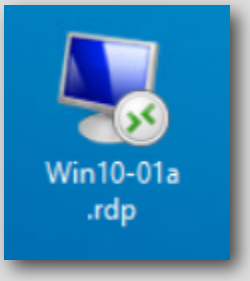
繰り返しますが、このハンズオン ラボで登録して管理する予定のマシンからハンズオン ラボにアクセスしないでください。このハンズオン ラボでは登録するマシンを再起動するため、同じマシンからラボを実行していると、ラボのマニュアルに一時的にアクセスできなくなります。

Windows 10 仮想マシンへの接続

[111]



メイン コンソール デスクトップにある [Win10-01a.rdp] ショートカットをダブルクリックして、Windows 10 仮想マシンに接続します。



Workspace ONE UEM Console へのログイン

[112]

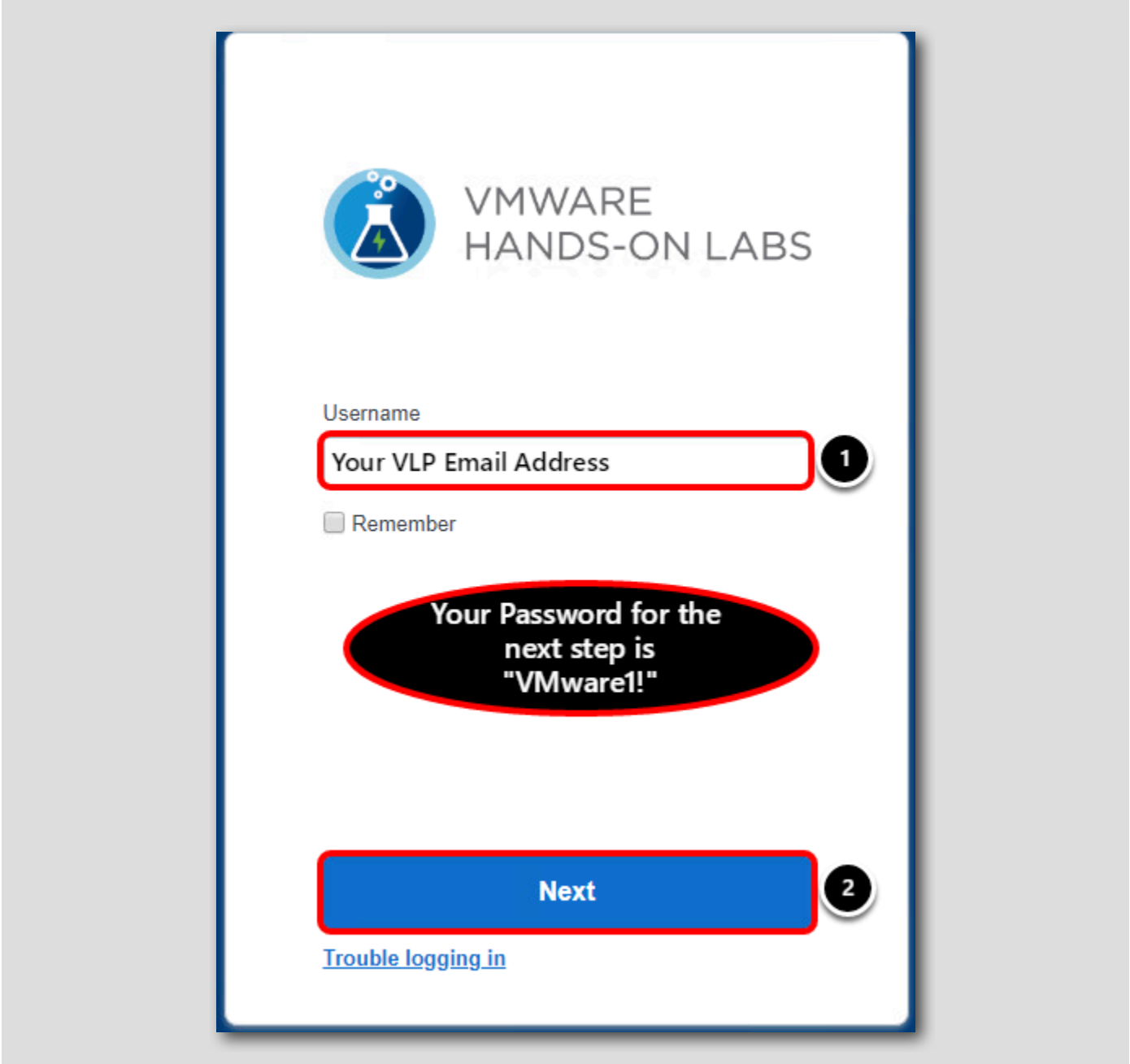
このラボでは、ほとんどの場合、Workspace ONE UEM 管理コンソールにログインします。

Chrome ブラウザの起動

[113]

現在接続している仮想マシンのデスクトップにある [Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールでの管理者ユーザー名の入力 [114]



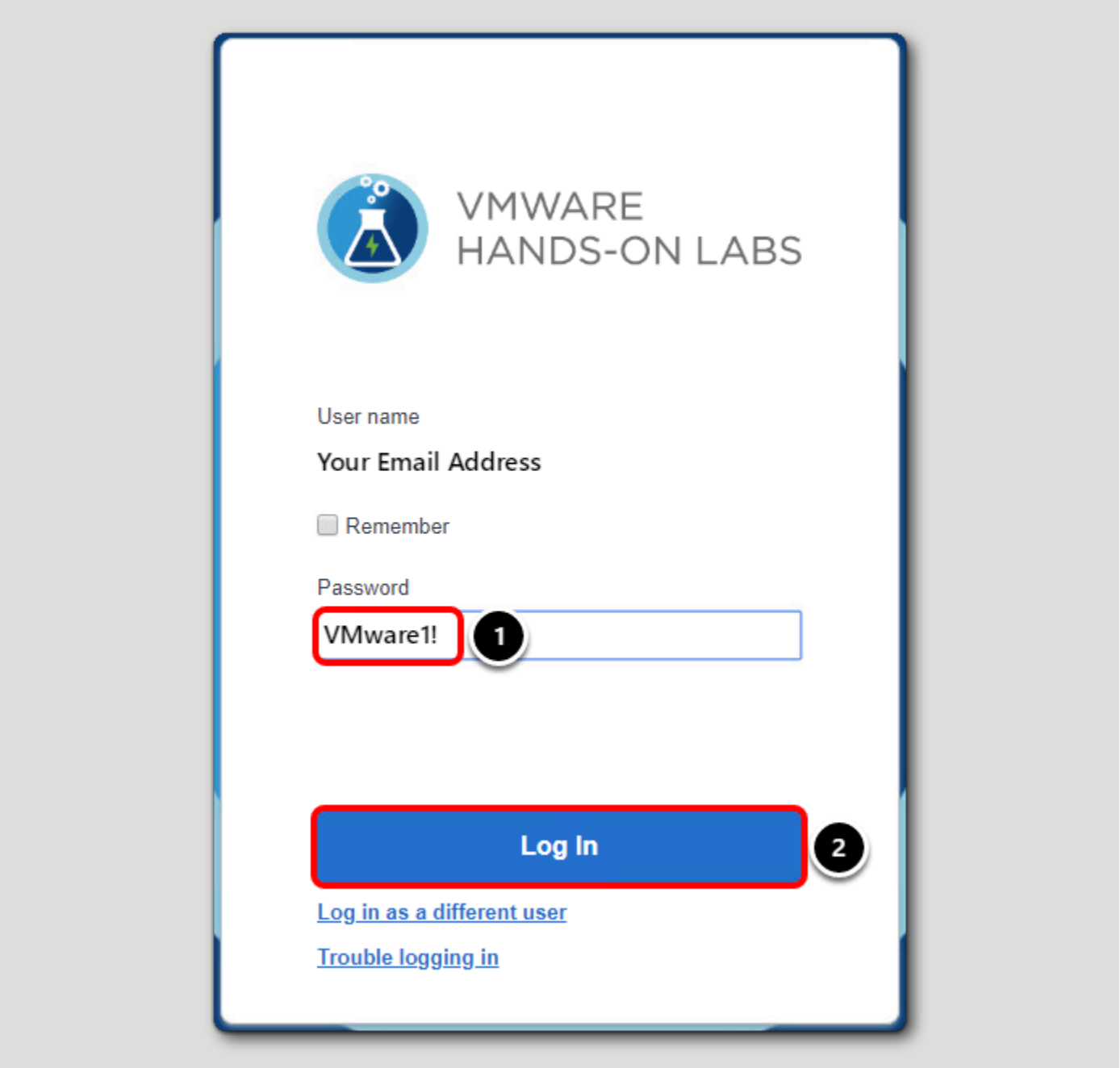
ブラウザのデフォルトのホーム ページは https://hol.awmdm.com です。Workspace ONE UEM 管理者アカウント情報を入力し、[Login] ボタンをクリックします。

1. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。
2. [Next] をクリックして、ラボ マニュアルの次の手順に進み、パスワードを入力します。これは常に **`VMware1!`** です。

注：Captcha による入力を求められた場合は、大文字と小文字を区別して入力してください。

Workspace ONE UEM Console の認証情報の入力

[115]



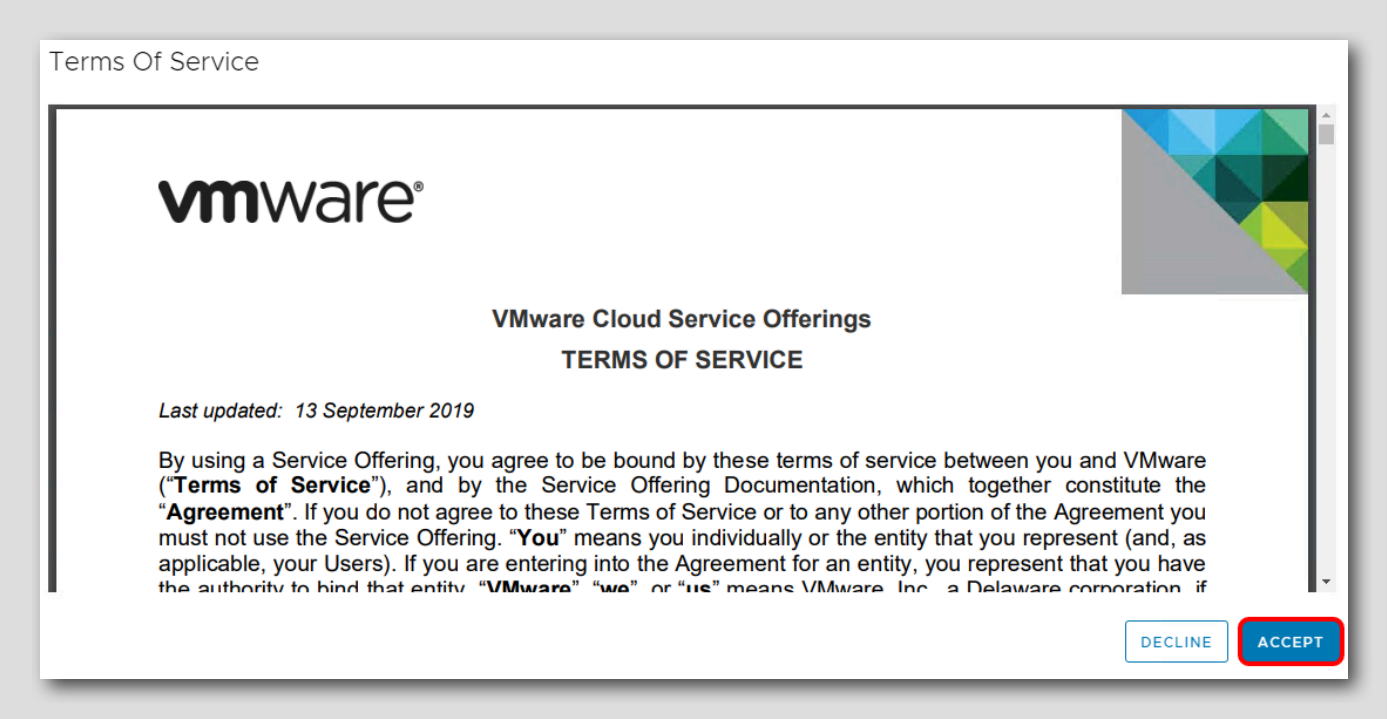
ユーザー名を入力すると、パスワード フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ラボの制限により、ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

エンド ユーザー使用許諾契約書に同意

[116]



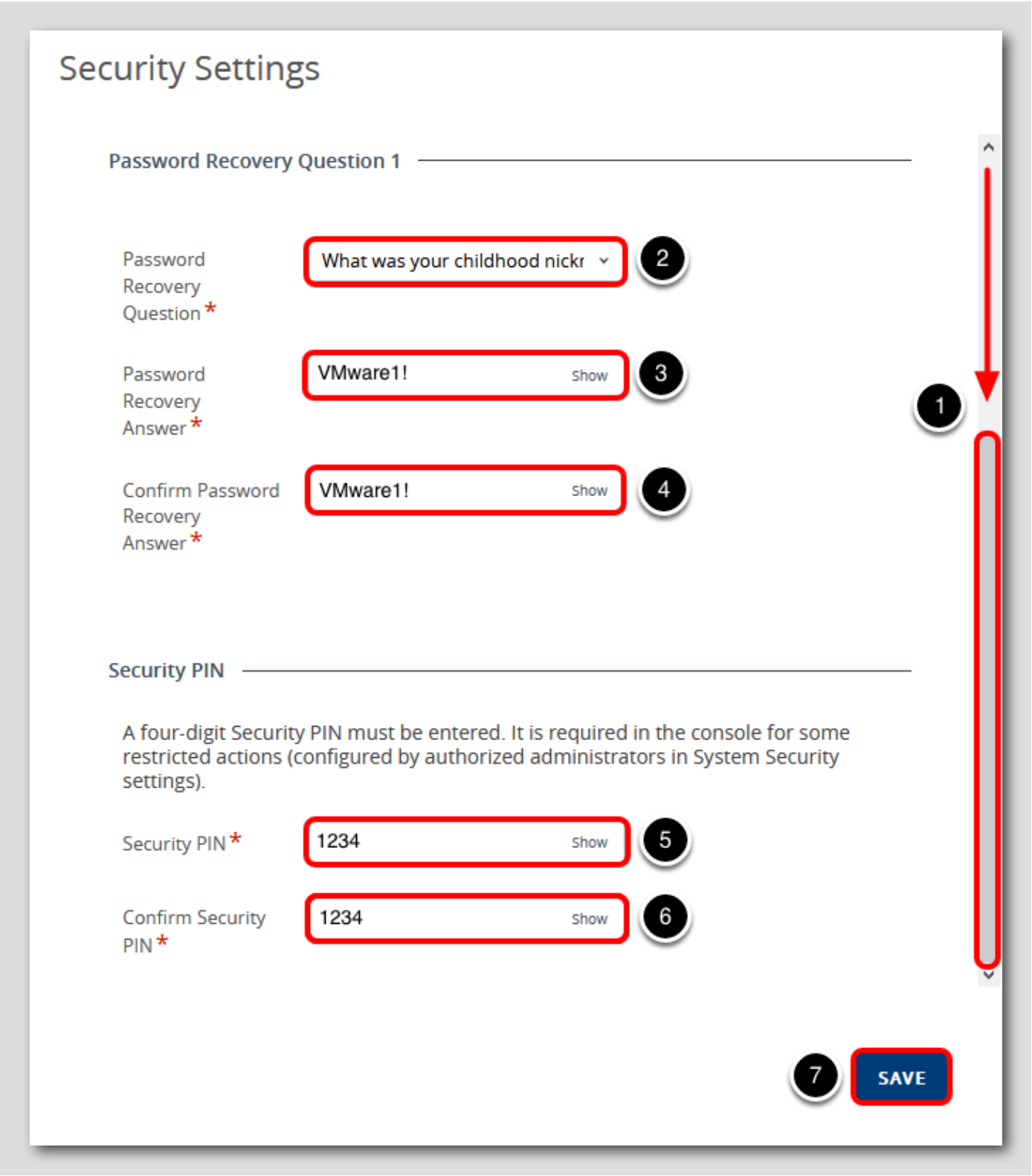
Workspace ONE UEM の「利用規約」が表示されたら、[Accept] ボタンをクリックします。

注：管理コンソールに初めてログインする場合のみ、次の手順に従ってログインしてください。

初期セキュリティ設定の完了

[117]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

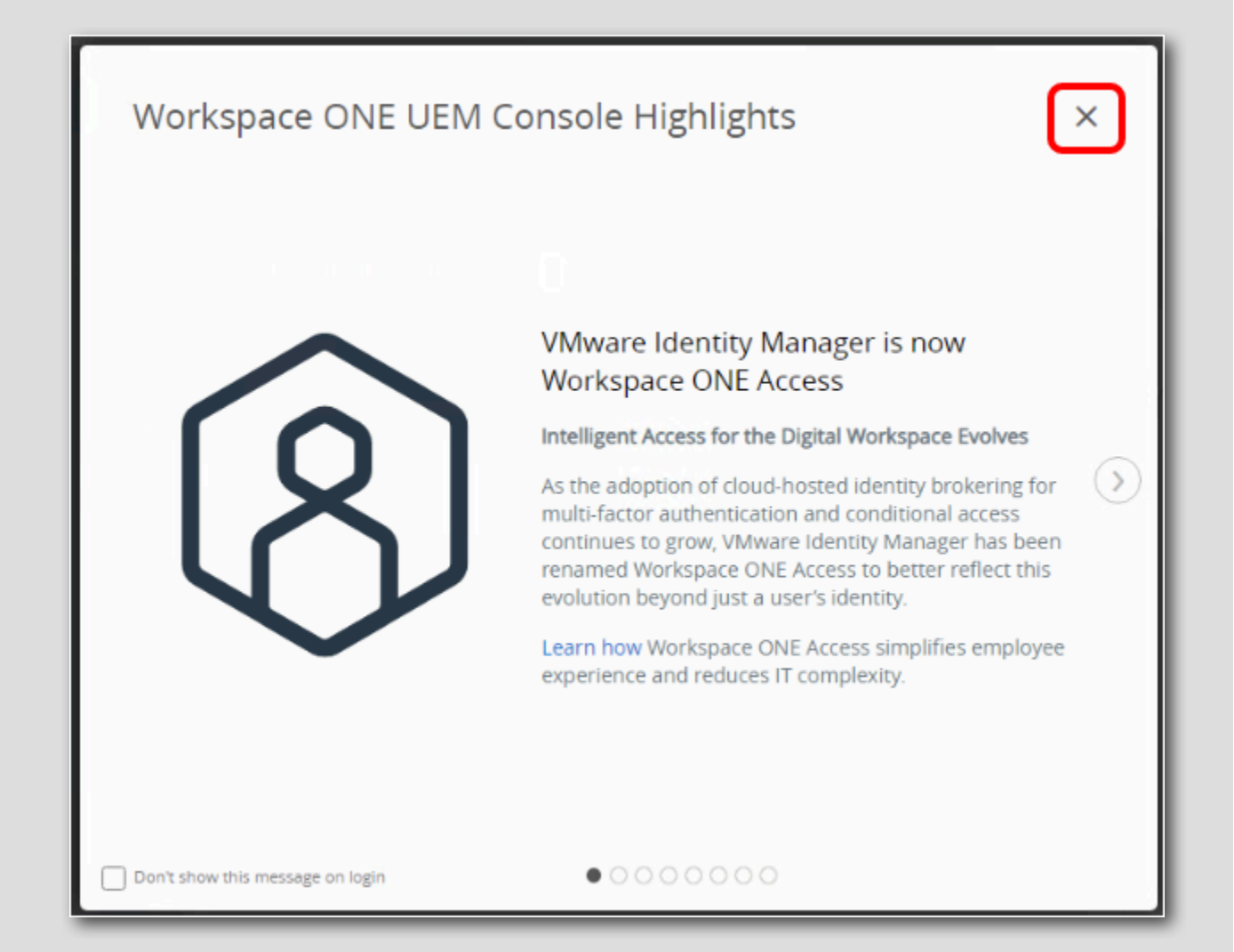

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 必要に応じて画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示してください。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[118]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

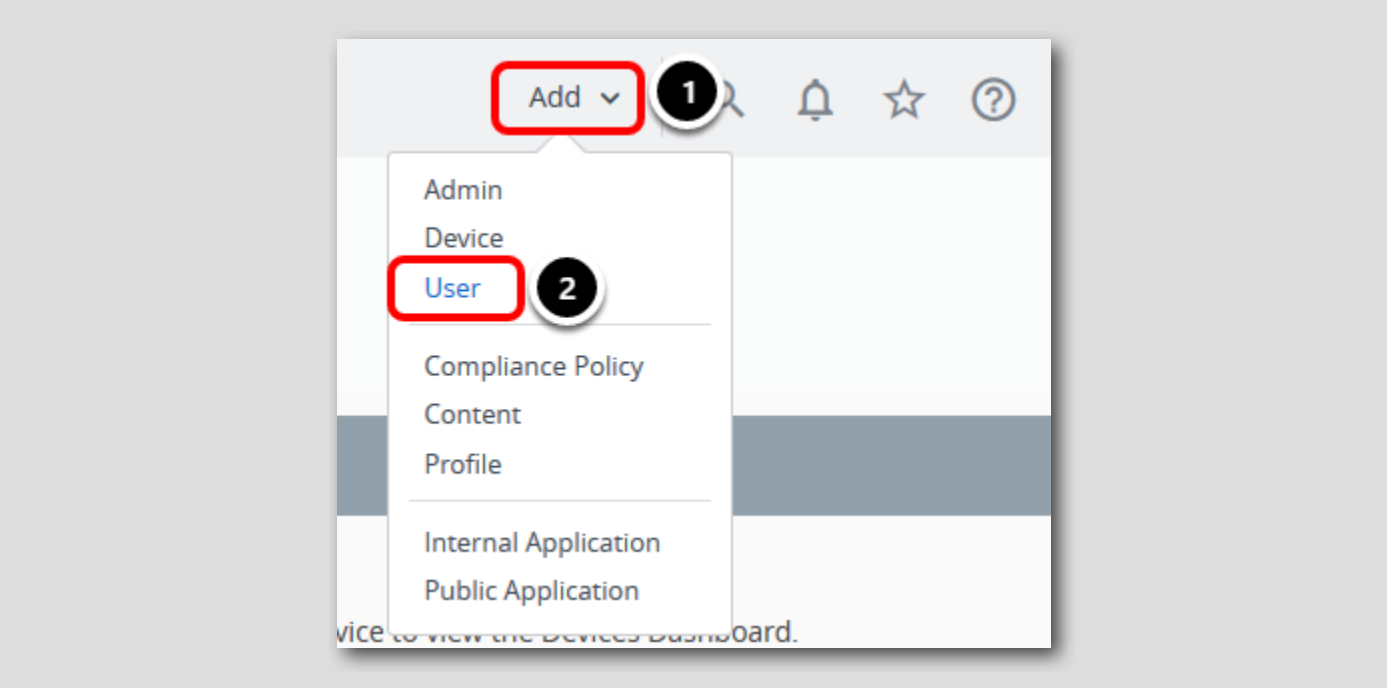
基本ユーザー アカウントの作成

[119]

基本アカウントは、Active Directory からインポートされるアカウントではなく、Workspace ONE UEM 管理コンソールで作成されるローカル アカウントです。このセクションでは、基本ユーザー アカウントを作成します。このアカウントは、次のセクションでデバイスを登録するときに使用します。

[Add] > [User] のクリック

[120]

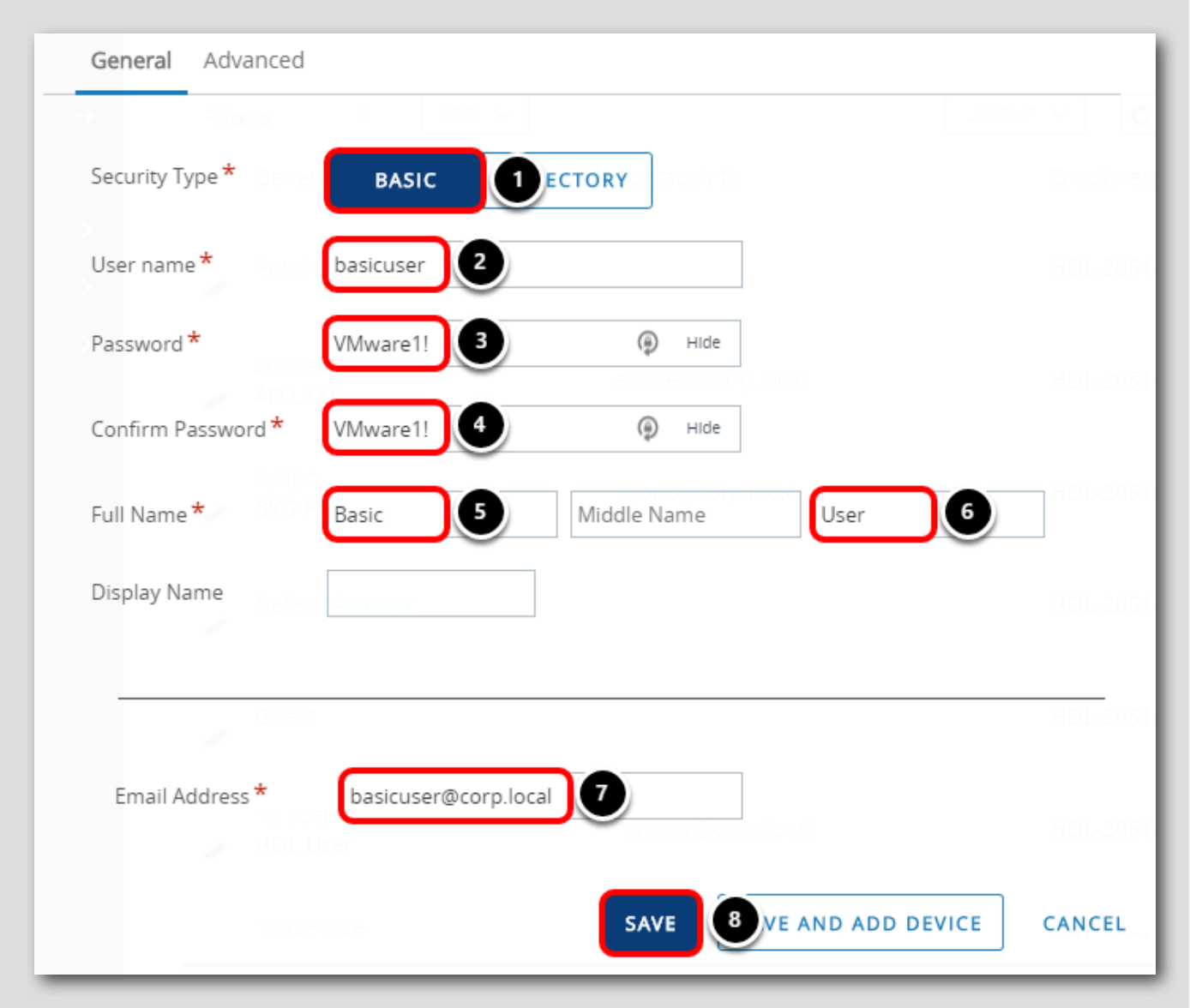


Workspace ONE UEM Console の右上で、次のように操作します。

1. [Add] をクリックします。
2. [User] をクリックします。

ユーザー情報の追加

[121]



ポップアップ ウィンドウで、次のように操作します。

1. セキュリティ タイプとして [Basic] が選択されていることを確認します。
2. ユーザー名として **basicuser** と入力します。
3. パスワードとして **VMware1!** と入力します。
4. 確認のため、同じパスワード (**VMware1!**) をもう一度入力します。
5. 名として **Basic** と入力します。
6. 姓として **User** と入力します。
7. メール アドレスとして **basicuser@corp.local** と入力します。

   注: 必要に応じてスクロール バーを使用して、メール アドレスを入力するフィールドを表示します。
8. [Save]

   をクリックします。

ユーザーが正しく作成されたことを知らせる確認メッセージが表示されます。同じ名前のユーザーがすでに作成されている場合は、そのユーザーを次のセクションで使用できます。

Hub サービスの有効化

[122]

Hub サービスの有効化フローは、新規のお客様であるか、既存のお客様であるかによって異なります。

Workspace ONE の新しいお客様

[123]

2019 年 1 月以降に Workspace ONE を購入した新しいクラウドのお客様の場合、インスタンス プロビジョニング プロセスの一環として Hub サービスが自動的に有効化されます。Workspace ONE UEM、Workspace ONE Access、および Hub サービス コンソールは相互に接続されており、Intelligent Hub アプリケーションで Hub カタログが有効になっています。

既存のクラウド Workspace ONE UEM のお客様

[124]

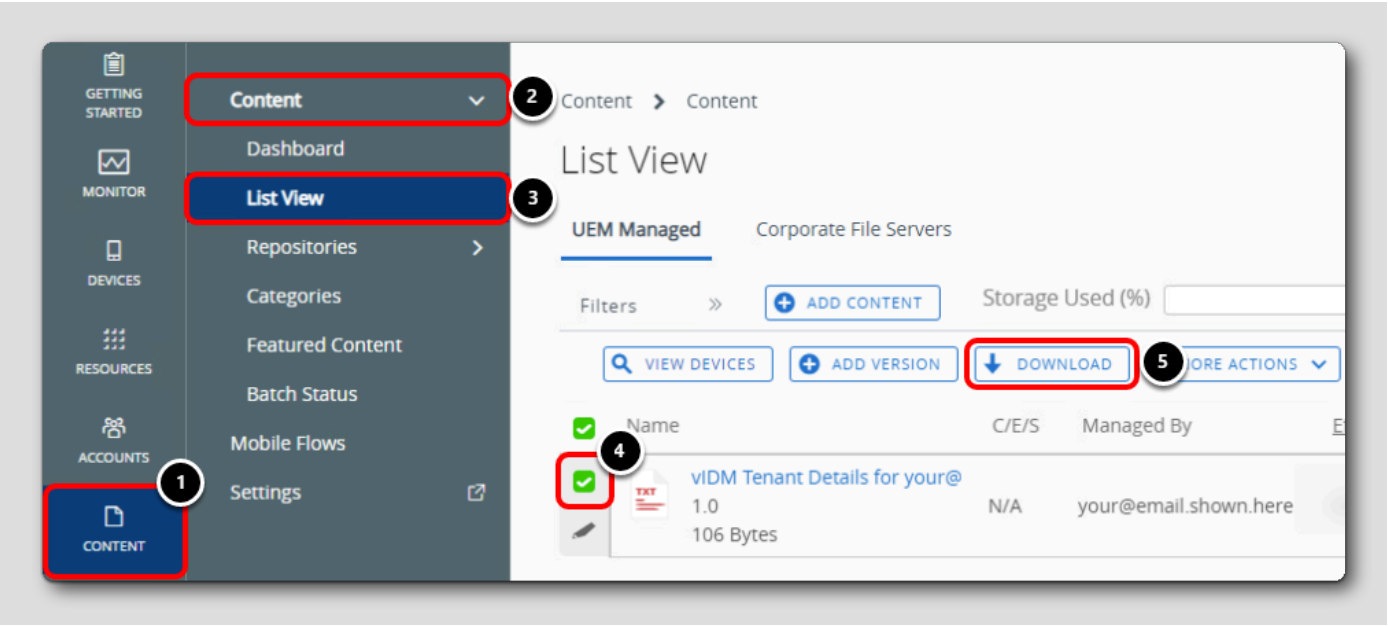
既存のお客様は、Hub サービスを有効化するために、Workspace ONE Access テナント URL、テナント管理者ユーザー名およびパスワードを構成できます。Workspace ONE Access テナントがない場合は、[Request a Cloud Tenant] ボタンを使用して、Workspace ONE UEM 管理者コンソールから要求できます。

このラボでは、次の手順で Hub サービスを有効化するために使用する Workspace ONE Access テナントがすでに提供されています。

Workspace ONE UEM Console のテナントの詳細へのアクセス

[125]

このラボ全体を通じて使用するために、一時的な Workspace ONE Access テナントが生成されています。Workspace ONE Access のテナント URL とログインの詳細が、ラボの最初に Workspace ONE UEM Console の [Content] セクションにアップロードされました。

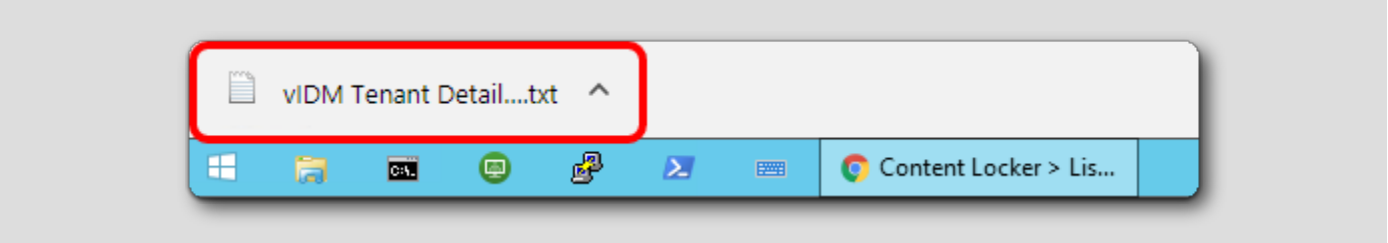


Workspace ONE UEM Console で、次のように操作します。

1. [Content] をクリックします。
2. [Content] を展開します。
3. [List View] をクリックします。
4. **`vIDM Tenant Details for your@email.shown.here.txt`** という名前のテキスト ファイルを見つけ、その横にあるチェックボックスをクリックしてファイルを選択します。
5. [Download] をクリックします。

ダウンロードしたテキスト ファイルを開く

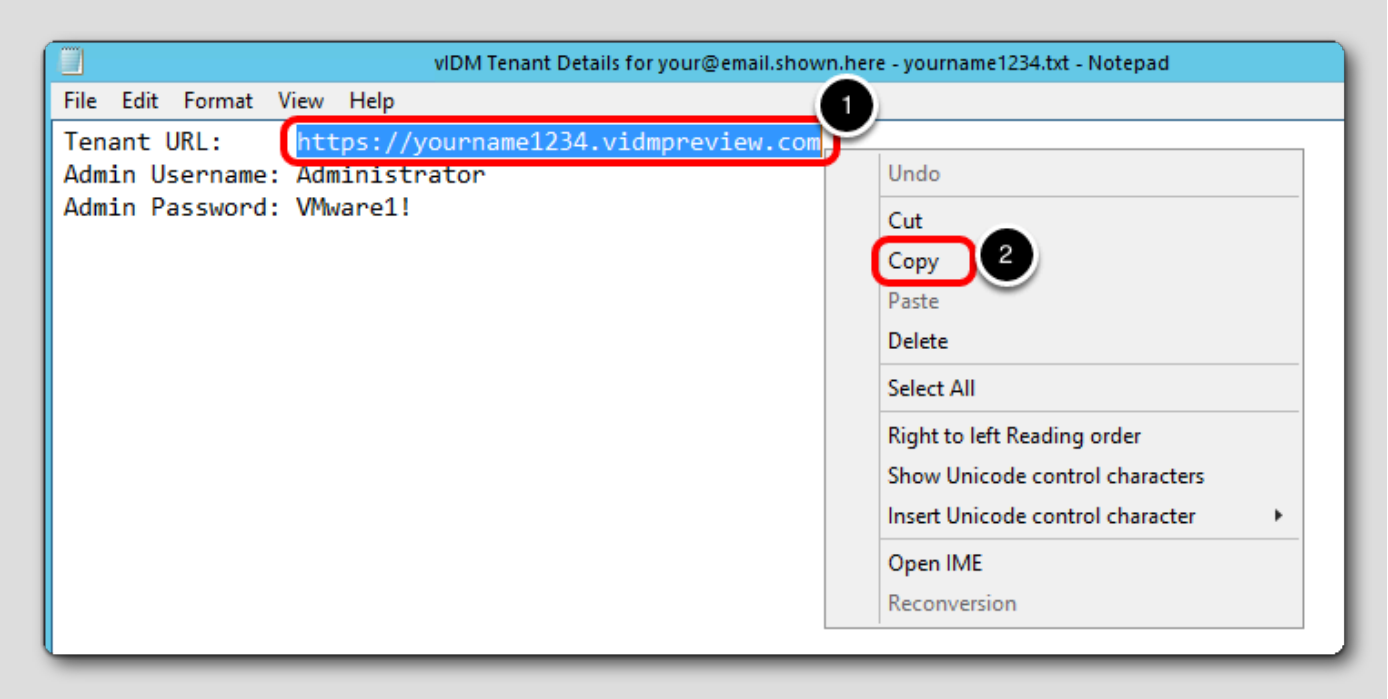
[126]



ファイルのダウンロード後、ダウンロード バーから「vIDM Tenant Details for your@email.shown.here.txt」ファイルをクリックして開きます。

テナント URL のコピー

[127]

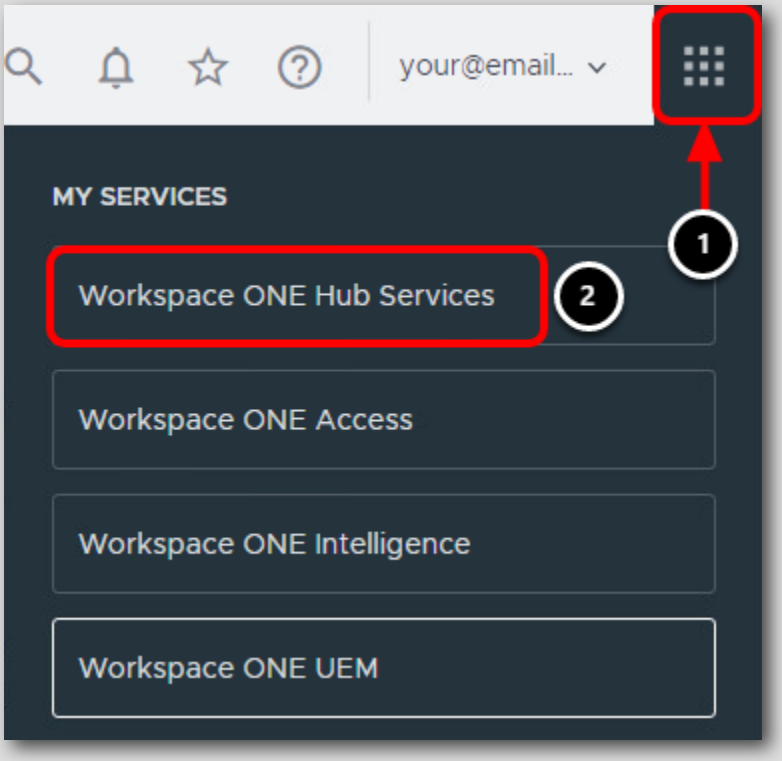


1. [Tenant URL] テキストを選択して右クリックします。
2. [Copy] をクリックします。

注：テナント名は Workspace ONE UEM Console のグループ ID と一致します。

Workspace ONE Hub サービスへの移動

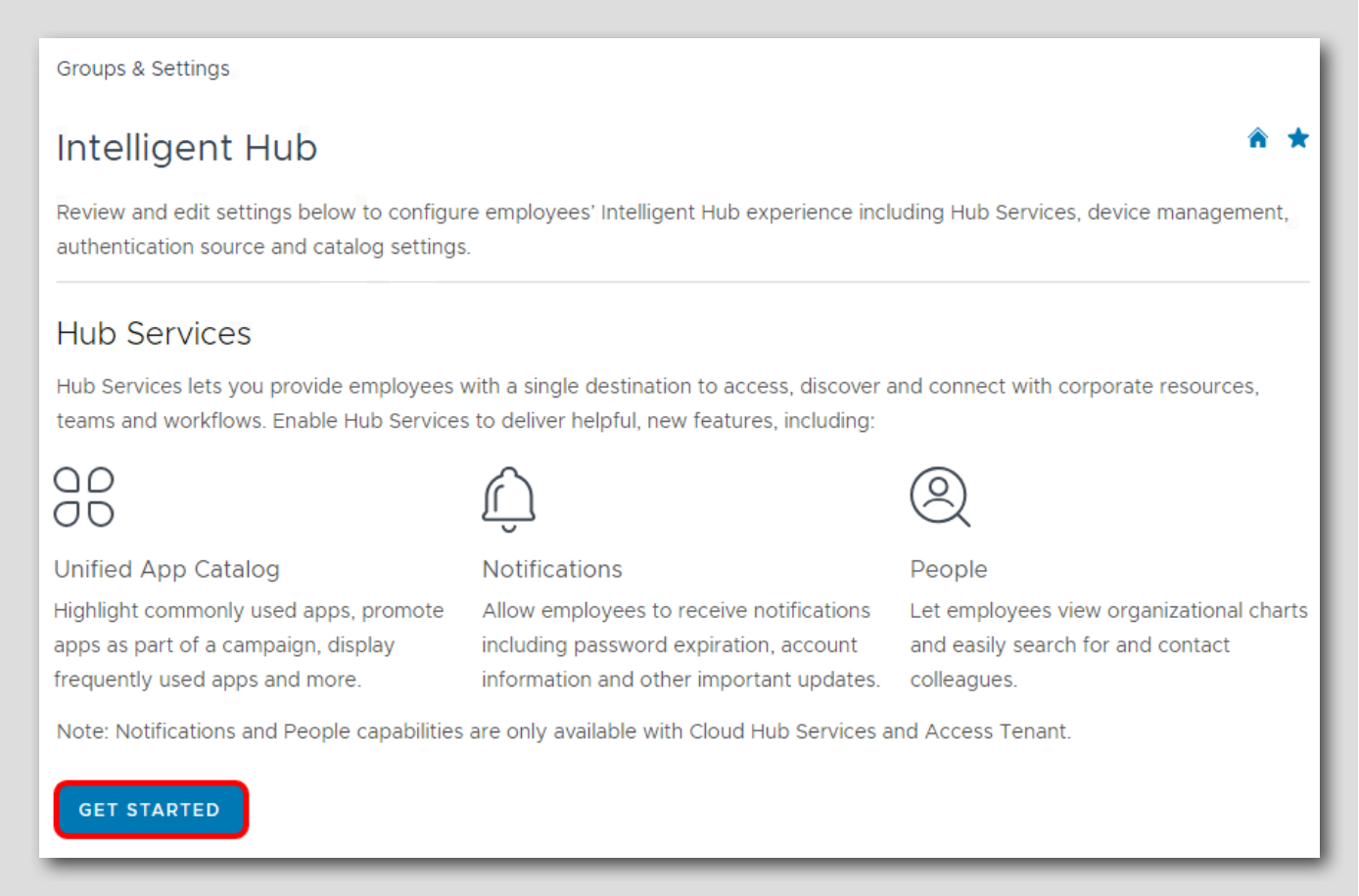
[128]



1. 右上にある [My Services] ボタンをクリックします。
2. [Workspace ONE Hub Services] をクリックします。

はじめに

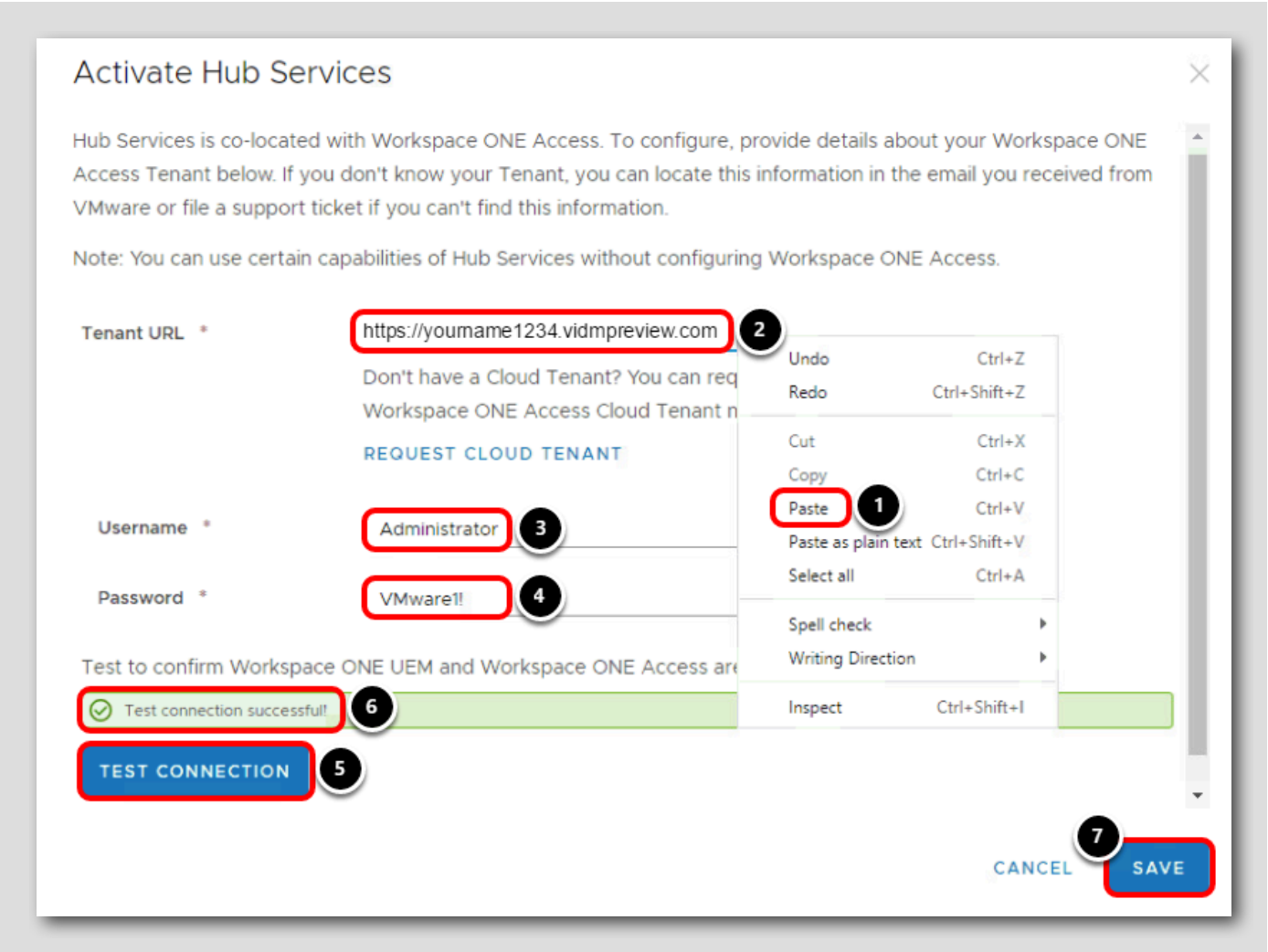
[129]



[Get Started] クリックして、Hub サービスの有効化プロセスを開始します。

Hub サービスの有効化

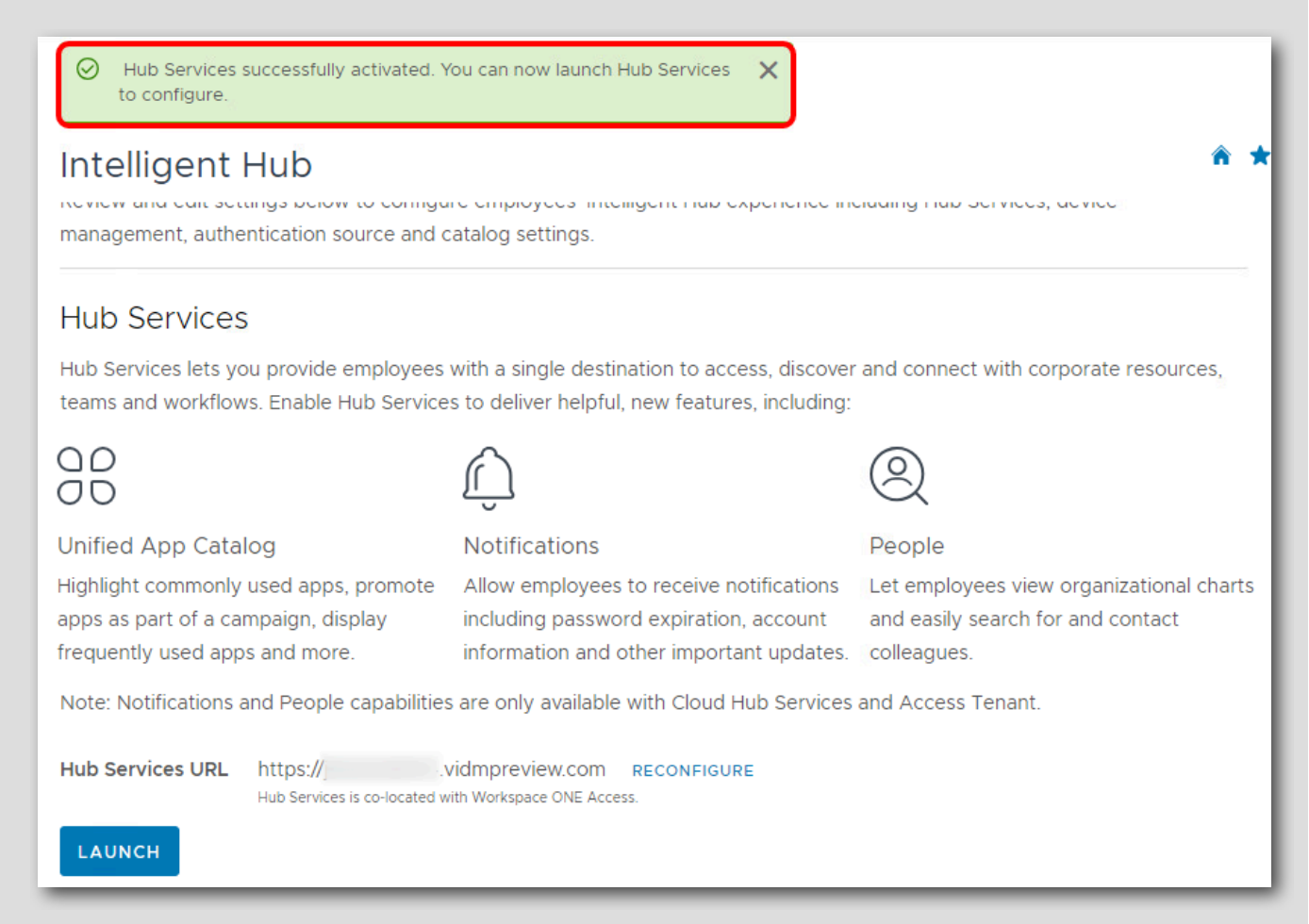
[130]



1. [Tenant URL] フィールドを右クリックし、[Paste] をクリックします。
2. 前の手順でダウンロードしたメモ帳ファイルの URL を入力していることを確認します。クリップボードが空白であるか、他の値が保存されている場合は、前の手順に戻って、ダウンロードしたメモ帳ファイルからテナントの URL をコピーします。
3. [Username] に **`Administrator`** と入力します。
4. [Password] に **`VMware1!`** と入力します。
5. [Test Connection] をクリックします。
6. 成功メッセージ「Test Connection Successful!」が表示されることを確認します。
7. [Save] をクリックして続行します。

Hub サービスの起動

[131]



Hub サービスが正常に有効化されたことを確認するメッセージが表示されていることを確認します。これで、テナントの Hub サービスの有効化が正常に完了しました。

個人の Windows 10 デバイスを登録しないこと

[132]

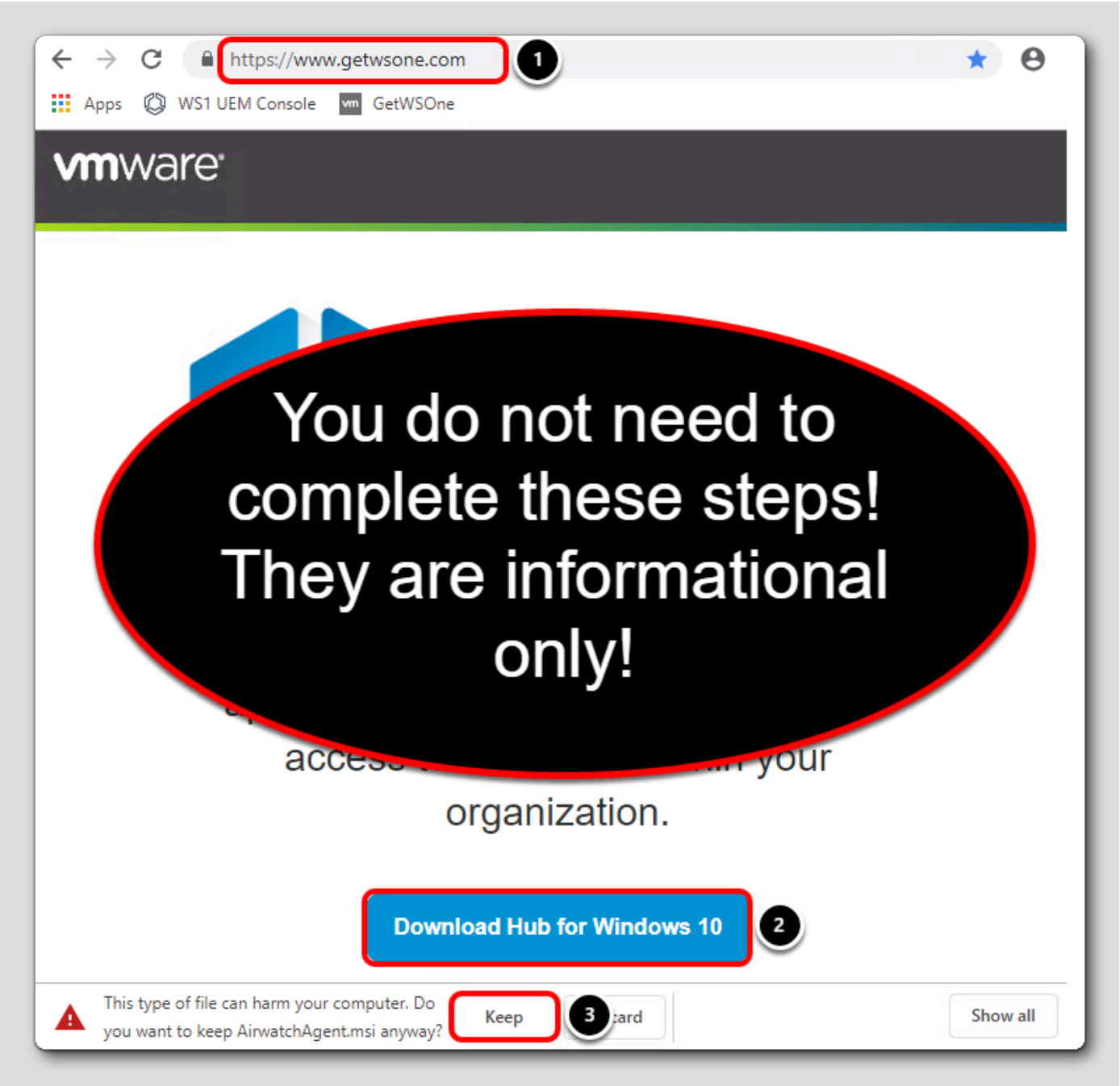
重要：今後の演習で、個人の Windows 10 デバイスを登録しないでください。個人デバイスが他の EMM プロバイダに加入している場合、望ましくない競合や問題が発生する可能性があります。

以降の手順に従って、このハンズオン ラボ用に提供されている Win10-01a 仮想マシンを登録して使用してください。

作成した基本アカウントを使用した Windows 10 デバイスの登録 [133]

次に、Workspace ONE Intelligent Hub アプリケーションを使用して、Workspace ONE UEM に Windows 10 デバイスを登録します。

Workspace ONE Intelligent Hub アプリケーションのダウンロード [134]



注：これらの手順を実行する必要はありません。Workspace ONE Intelligent Hub はすでにダウンロードされています。この手順は単なる情報です。

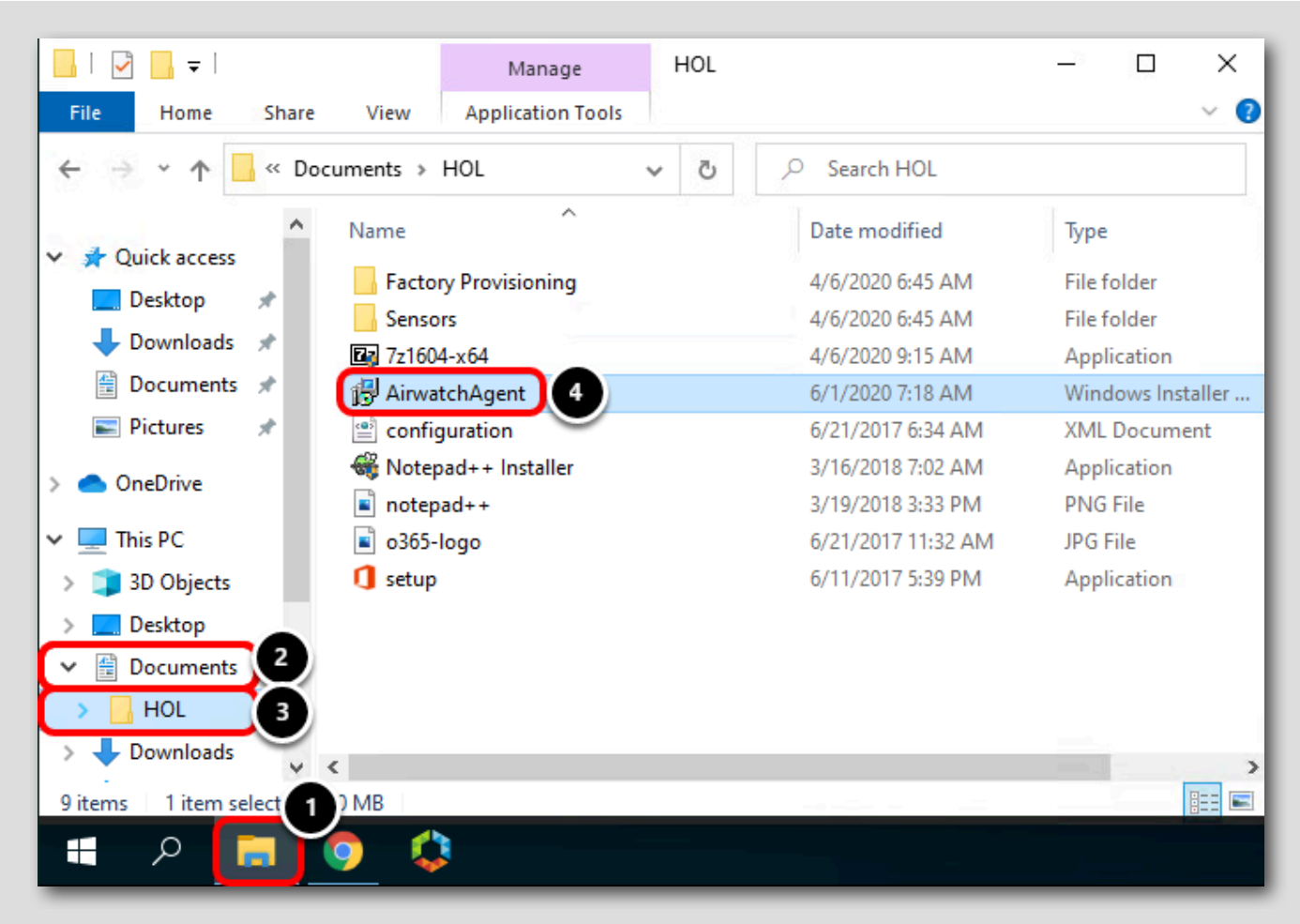
次の手順に従って、現在のプラットフォーム用の最新の Workspace ONE Intelligent Hub アプリケーションをダウンロードできます。

1. ブラウザで **`https://www.getwsone.com`** に移動します。
2. [Download Hub for Windows 10] をクリックします。
3. AirWatchAgent.msi のダウンロードについて警告が表示されたら、[Keep] をクリックします。

便宜上、Workspace ONE Intelligent Hub アプリケーションはすでにダウンロードされています。次の手順に進んで、インストーラを起動します。

Workspace ONE Intelligent Hub インストーラの起動

[135]

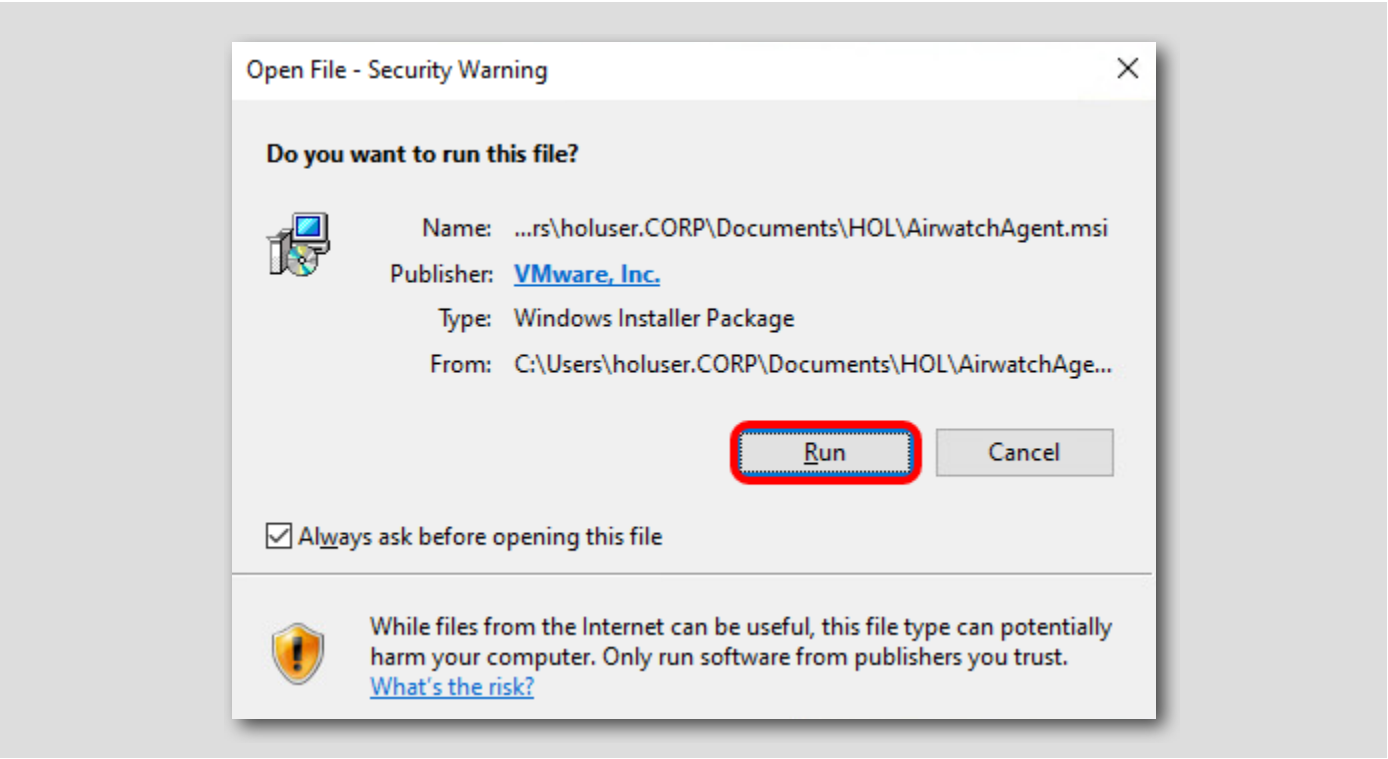


1. タスクバーの [File Explorer] アイコンをクリックします。
2. [Documents] をクリックします。
3. [HOL] をクリックします。
4. AirwatchAgent.msi ファイルをダブルクリックして、インストーラを起動します。

注：インストーラが起動するまでに数秒かかる場合があります。AirwatchAgent.msi ファイルをクリックして、しばらくお待ちください。

[Run] のクリック

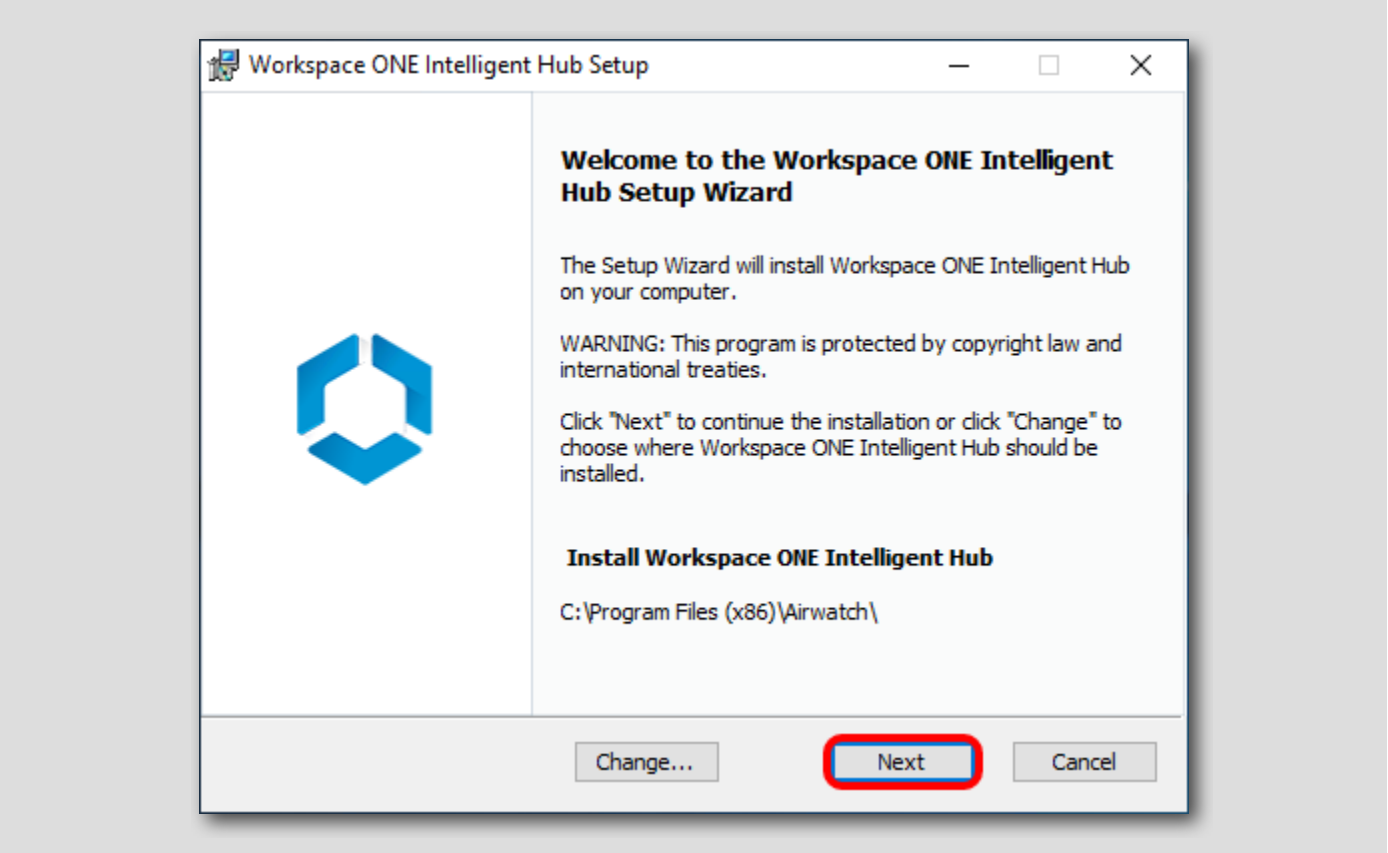
[136]



[Run] をクリックして、インストールを続行します。

デフォルトのインストール場所の受け入れ

[137]

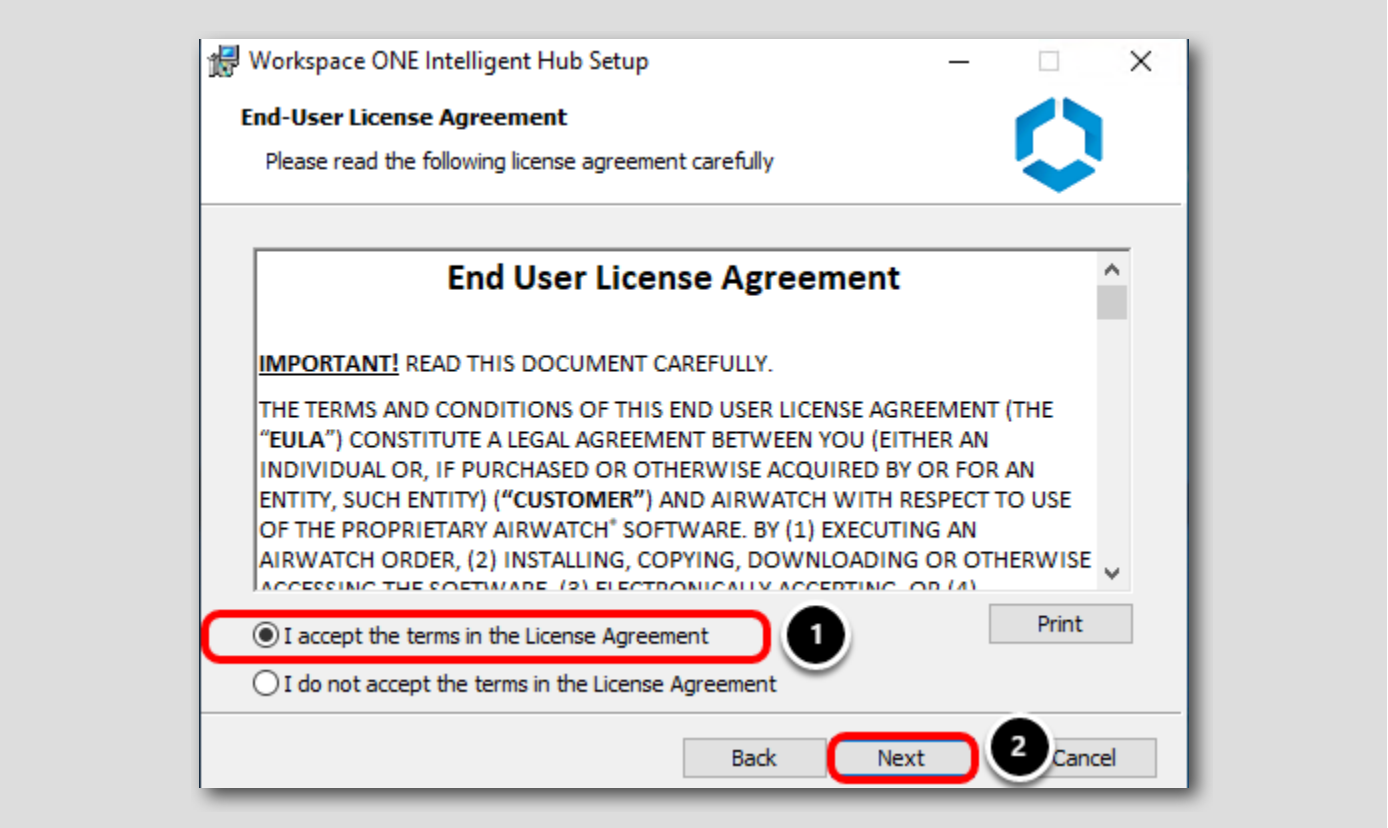


インストール場所はデフォルトのまま、[Next] をクリックします。

注：必要な追加機能がインストールされ、[Next] ボタンが有効になるまで数秒かかる場合があります。

使用許諾契約書への同意

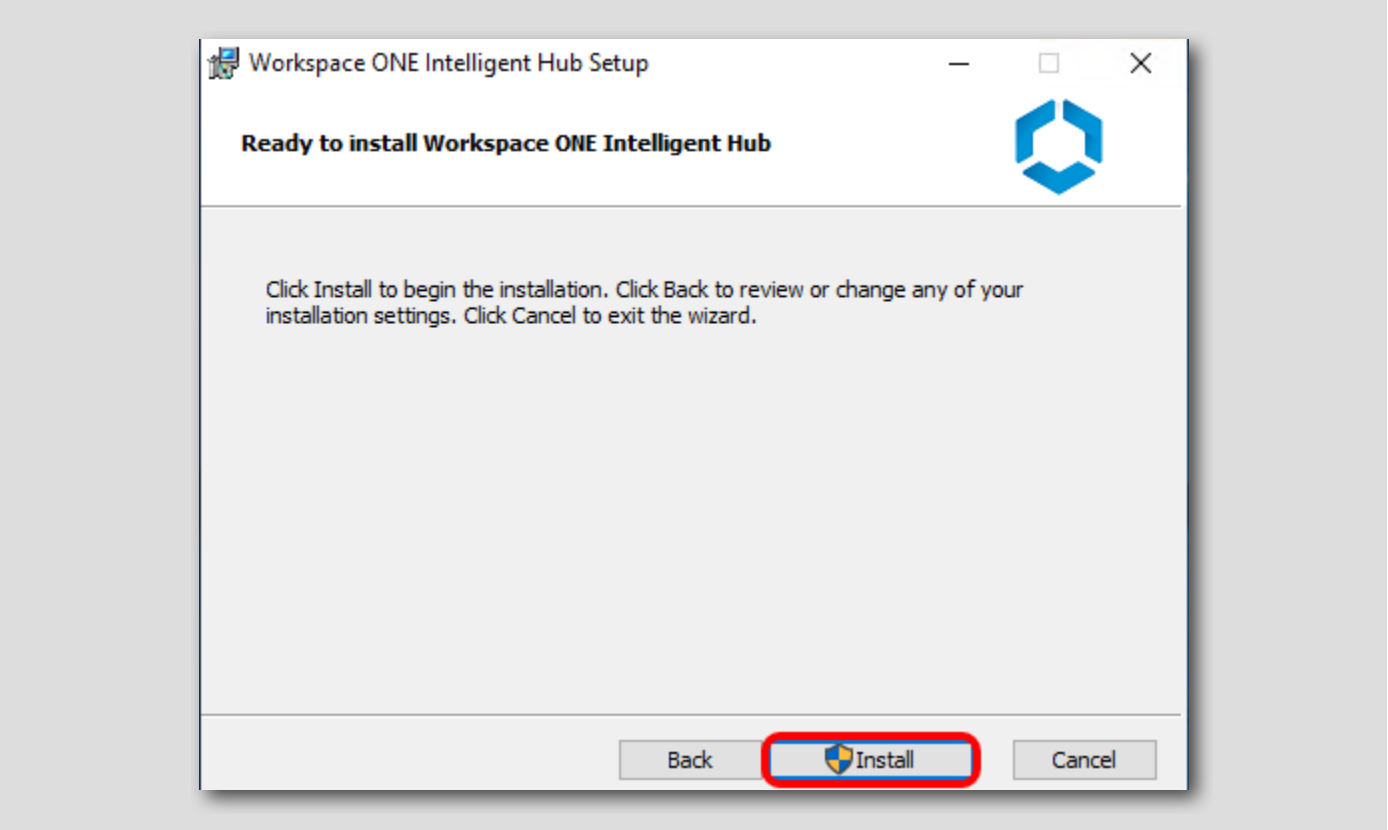
[138]



1. [I accept the terms of the License Agreement] を選択します。
2. [Next] をクリックします。

Workspace ONE Intelligent Hub のインストールの開始

[139]

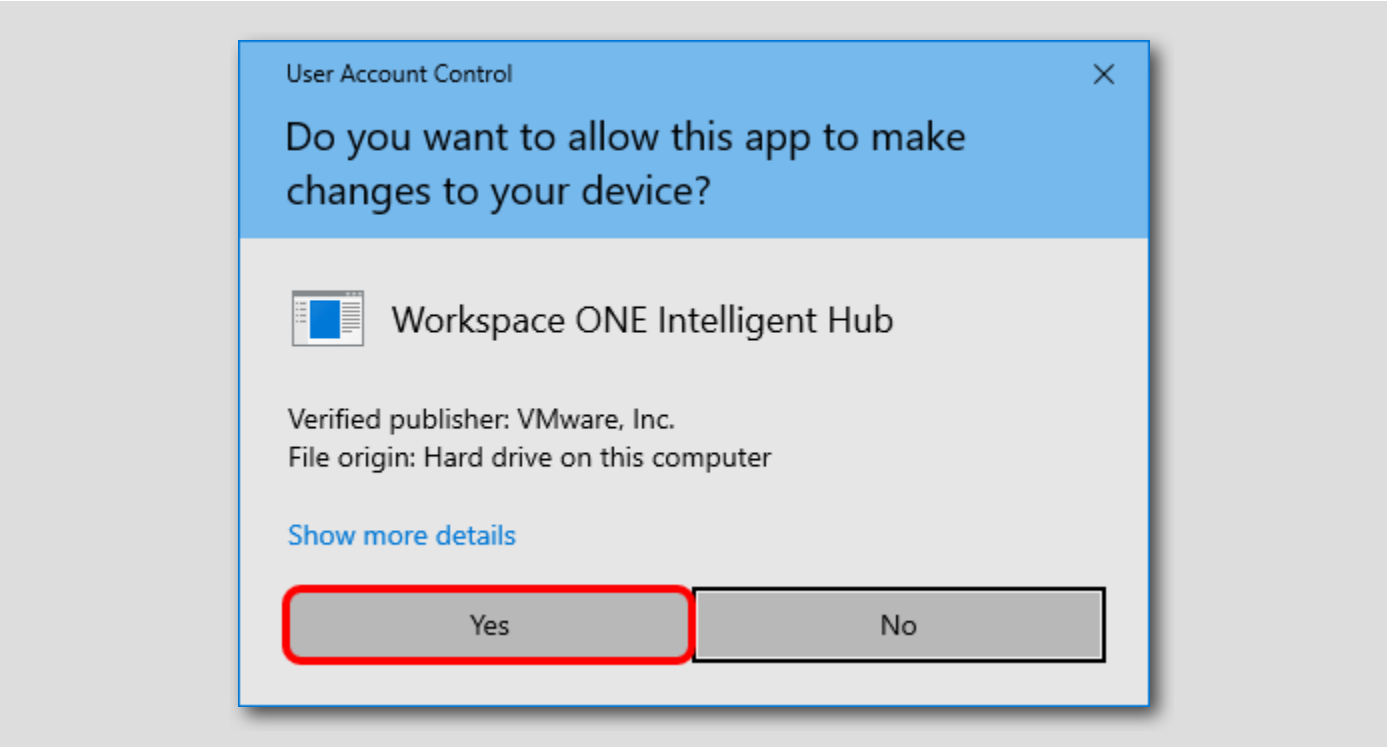


[Install] をクリックして、インストーラを開始します。

注：Hub のユーザー インターフェイス コンポーネントのインストール手順は完了までに数分かかる場合があります。インストールを中断しないようにしてください。

Workspace ONE Intelligent Hub インストーラを実行できるようにする（必要な場合）

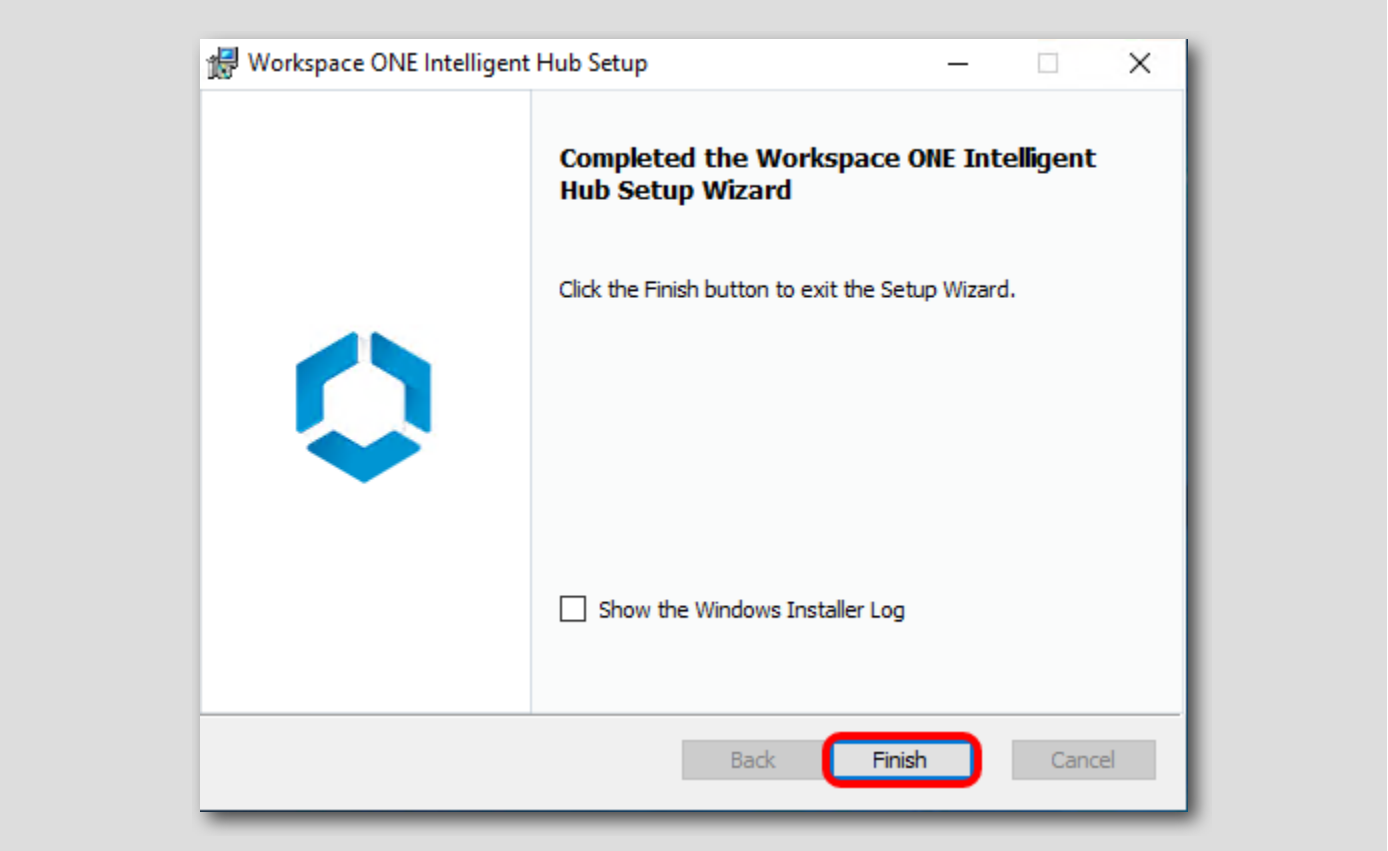
[140]



デバイスでアプリケーションが変更を実行することを許可するように求められた場合は、[Yes] をクリックします。それ以外の場合は、次の手順に進みます。

Workspace ONE Intelligent Hub インストーラの完了

[141]



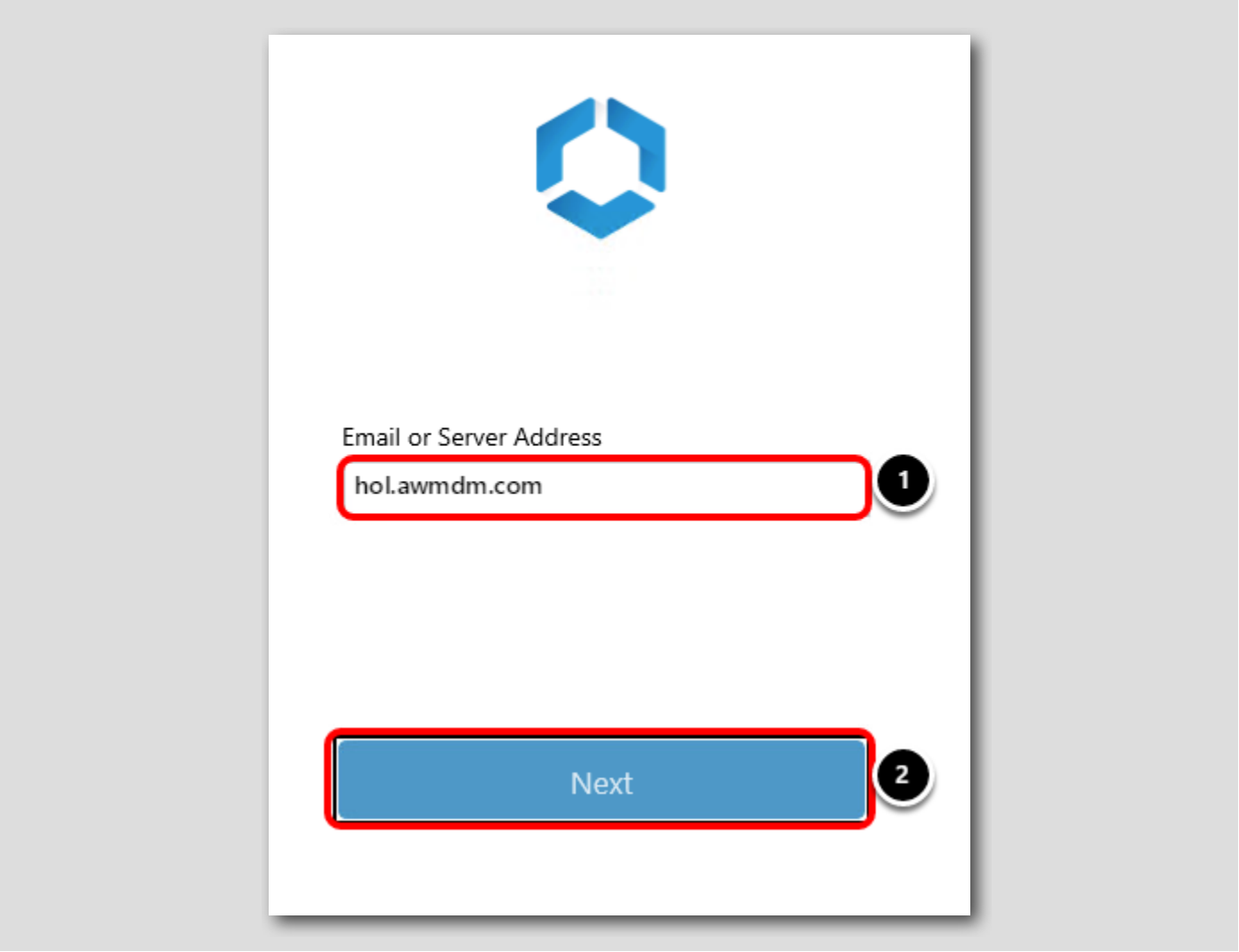
注：インストーラの完了には数分かかる場合があります。続行する前に、インストールの完了画面が表示されるまでお待ちください。

[Finish] をクリックして、Workspace ONE Intelligent Hub インストーラを完了します。

注：[Finish] をクリックすると Native Enrollment アプリケーションが起動し、Workspace ONE UEM への登録手順が表示されます。エージェントの起動には、約 45 ～ 60 秒かかります。

Workspace ONE Intelligent Hub を使用した Windows 10 デバイスの登録

[142]

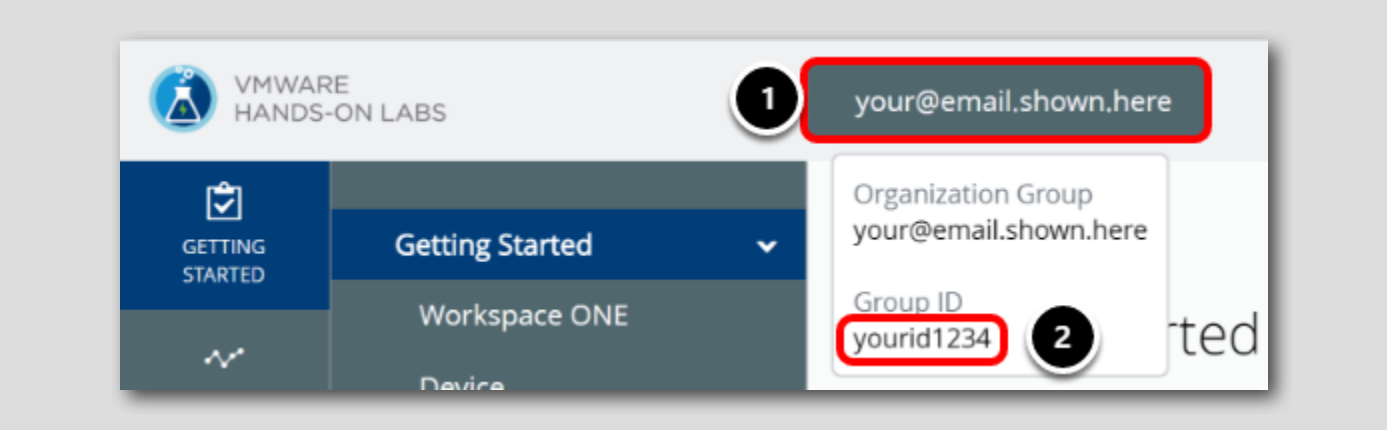


注：前の手順で [Finish] をクリックした後、上記の画面が表示されるまでに 2 ～ 3 分かかることがあります。

1. [Server Address] に **`hol.awmdm.com`** と入力します。
2. [Next] をクリックします。

Workspace ONE UEM Console からのグループ ID の検索

[143]

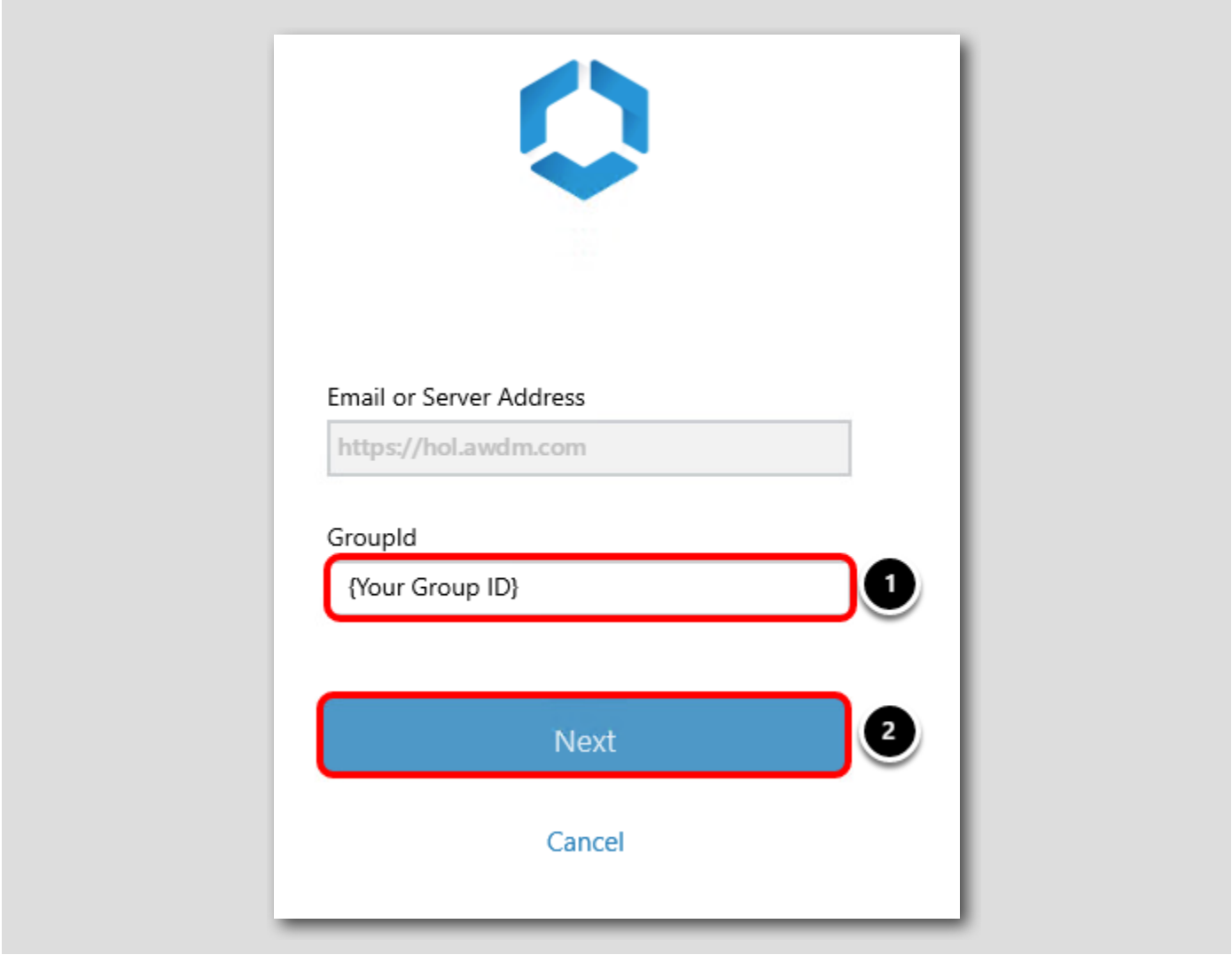


次に、**組織グループ ID** を確認します。

1. グループ ID を確認するには、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. **グループ ID** は [Organization Group] ポップアップの最下部に表示されます。

グループ ID の入力

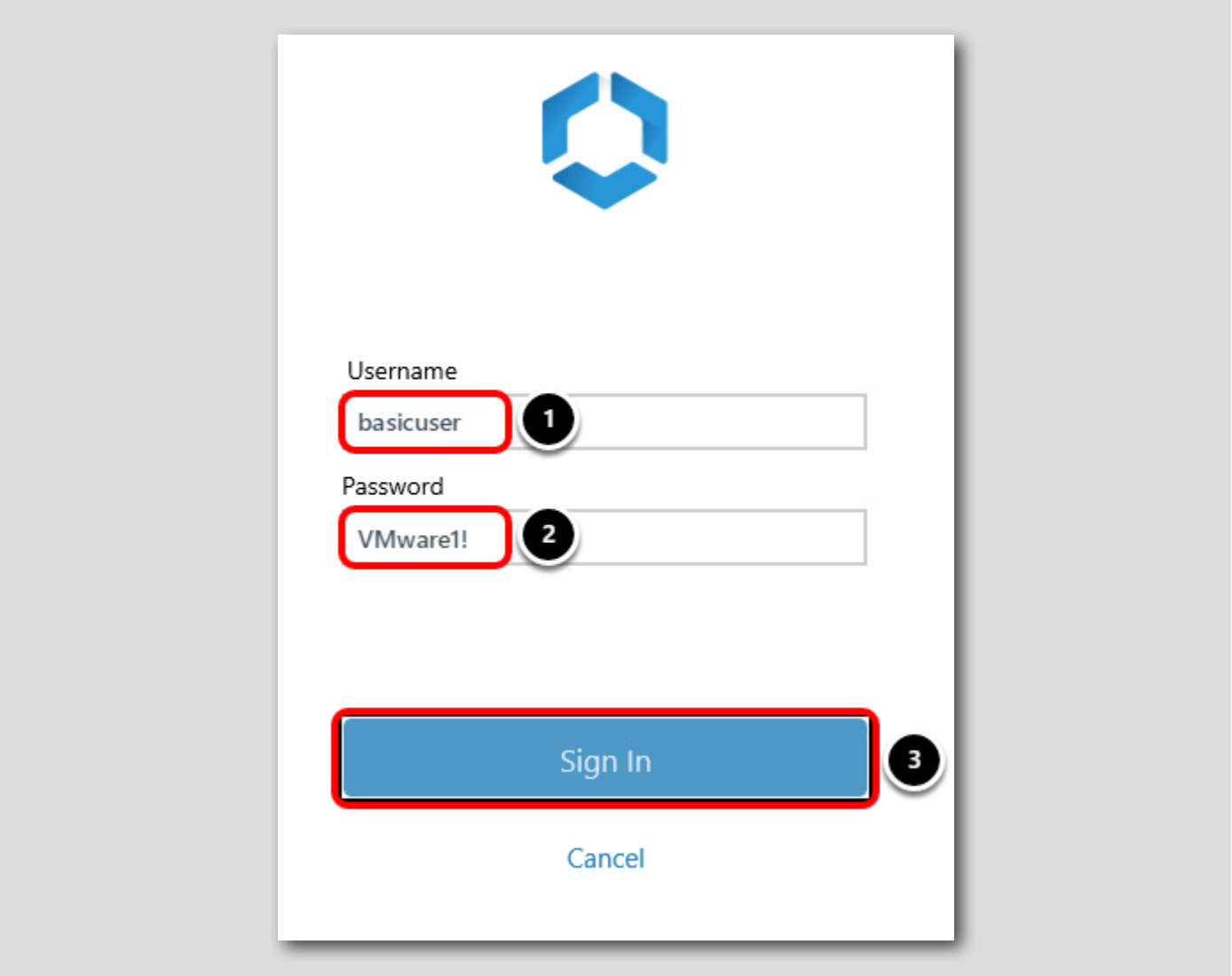
[144]



1. [Group ID] フィールドにグループ ID を入力します。グループ ID を忘れた場合は、前の手順で取得方法を確認してください。
2. [Next] をクリックします。

ユーザー認証情報の入力

[145]



1. [Username] フィールドに **basicuser** と入力します。

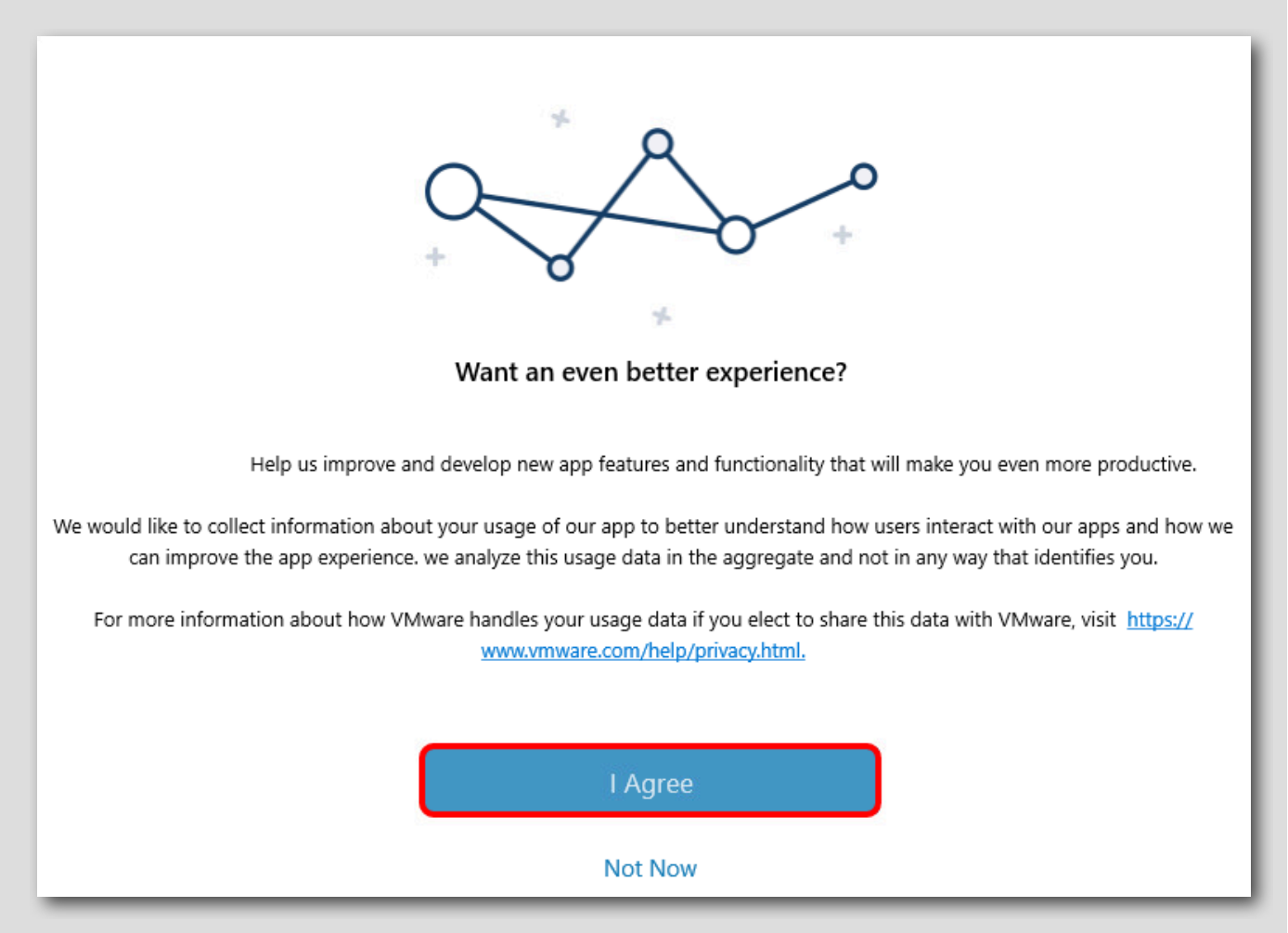
   注：これは、前の手順で Workspace ONE UEM Console で作成した基本ユーザー アカウントのユーザー名です。

2. [Password] フィールドに **VMware1!** と入力します。
3. [Sign In] をクリックします。

注：サーバが登録の詳細を確認するまでしばらくお待ちください。これには数分かかる場合があります。

データ ポリシーの承諾

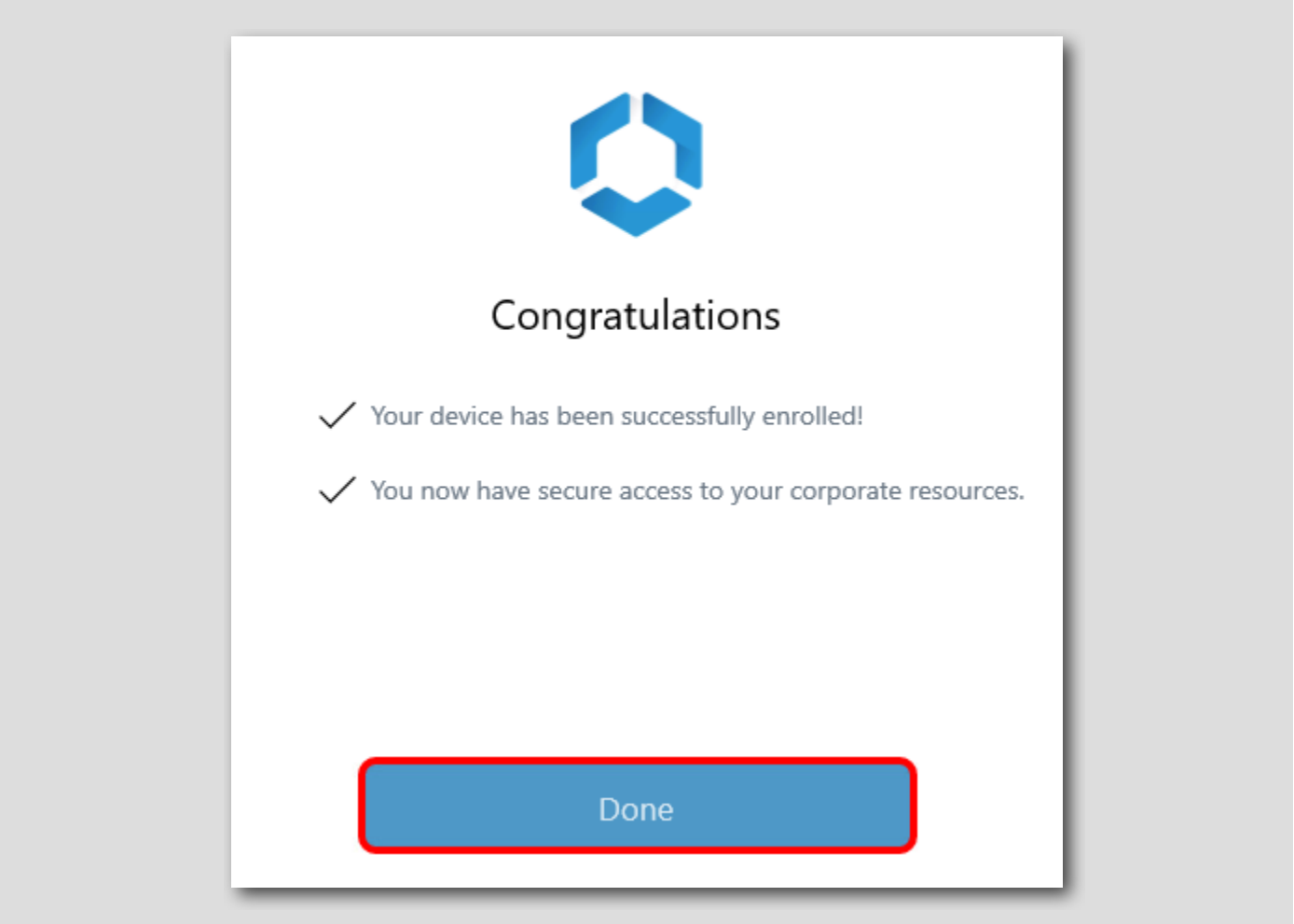
[146]



[I Agree] をクリックします。

Workspace ONE UEM 登録プロセスの終了

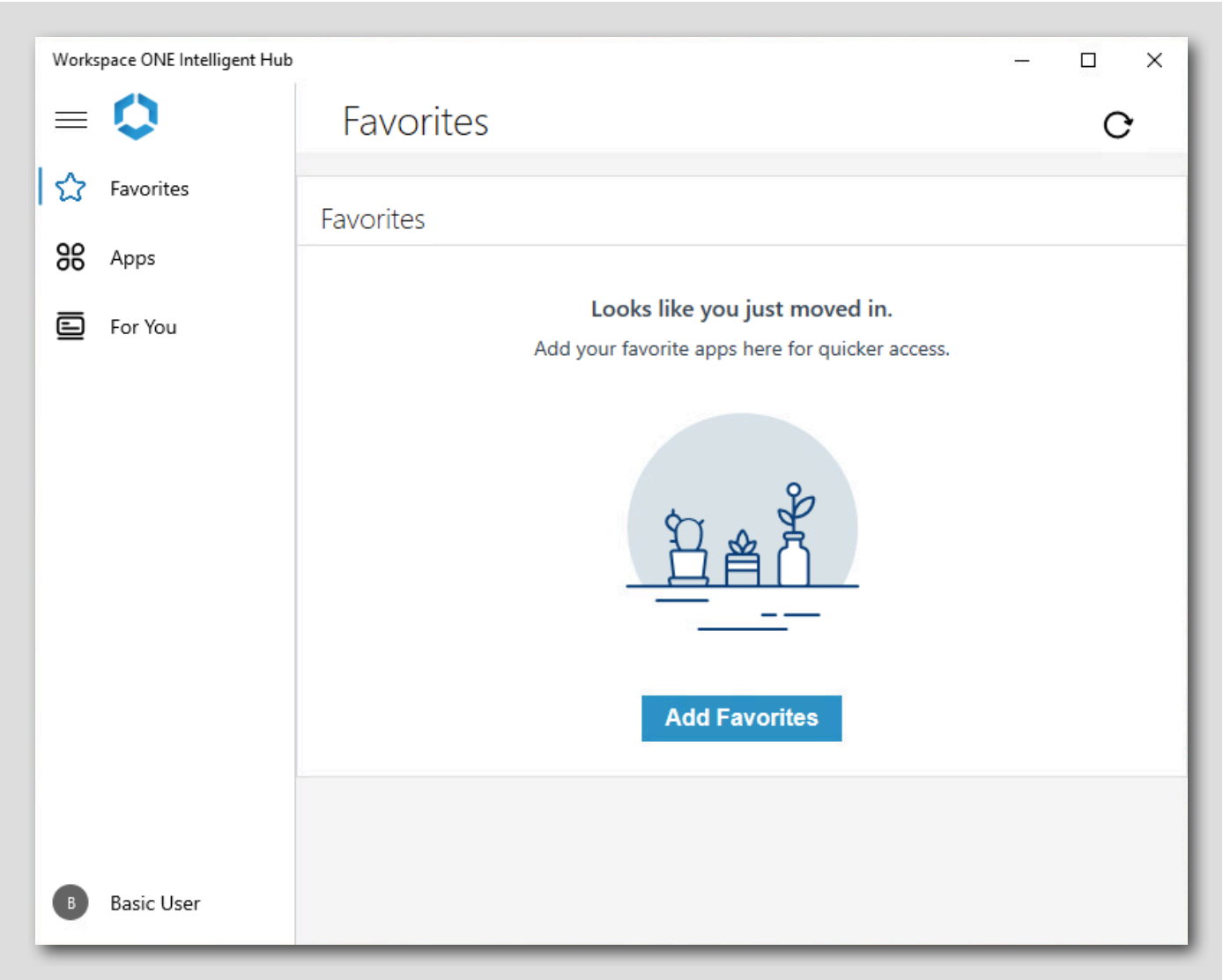
[147]



[Done] をクリックして登録プロセスを終了します。これで、Windows 10 デバイスは Workspace ONE UEM に正常に登録されました。

Intelligent Hub アプリケーションの表示

[148]



登録が完了すると、Workspace ONE Intelligent Hub アプリケーションが表示されます。ユーザーとデバイスにアプリケーションがまだ展開されていないため、[Favorites] および [Apps] タブは空になります。

次の手順では、2 つのアプリケーション（Workspace ONE Assist と 7-Zip）を展開します。Workspace ONE Assist はエンド ユーザーのデバイスに自動的に展開されてインストールされますが、7-Zip は「オンデマンド」アプリケーションとなります。これは、7-Zip へのアクセスが必要になったときに、アプリケーション カタログからアプリケーションのダウンロードとインストールを開始できることを意味します。

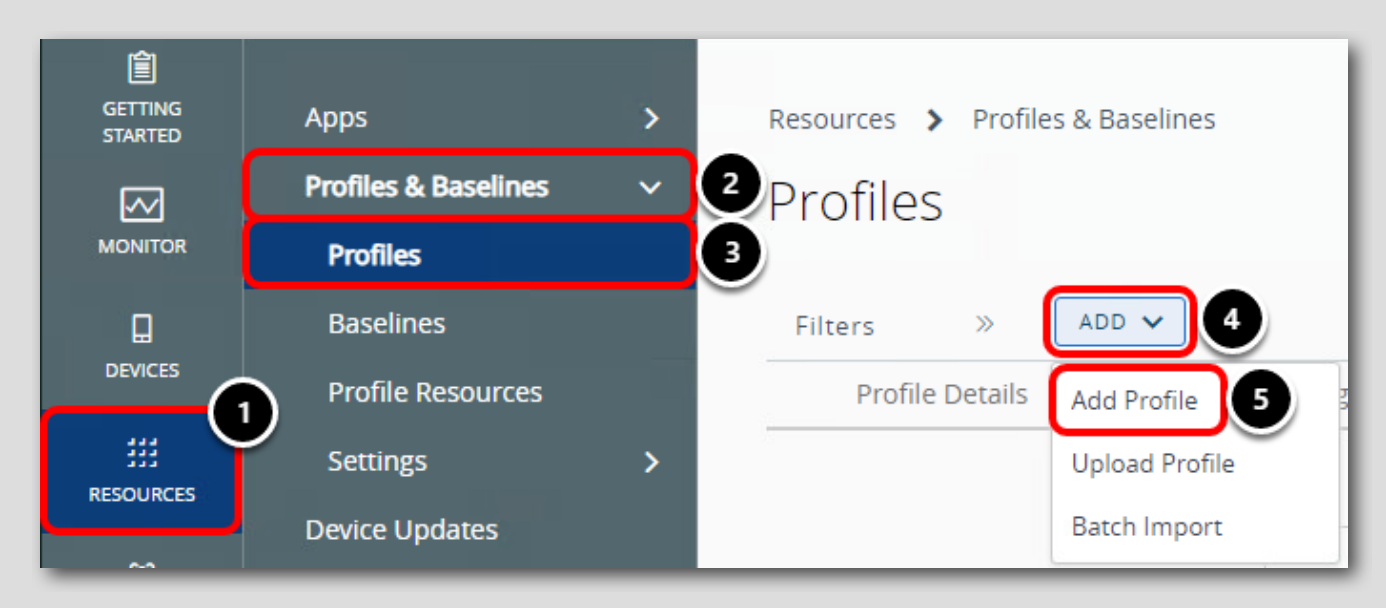
Windows 10 のデバイス プロファイルの構成

[149]

プロファイルを使用して、登録済みデバイスの動作を変更できます。この演習は、セクションの後半でデバイスに適用されていることを確認できる制限事項プロファイルを構成および展開します。

プロファイルの追加

[150]

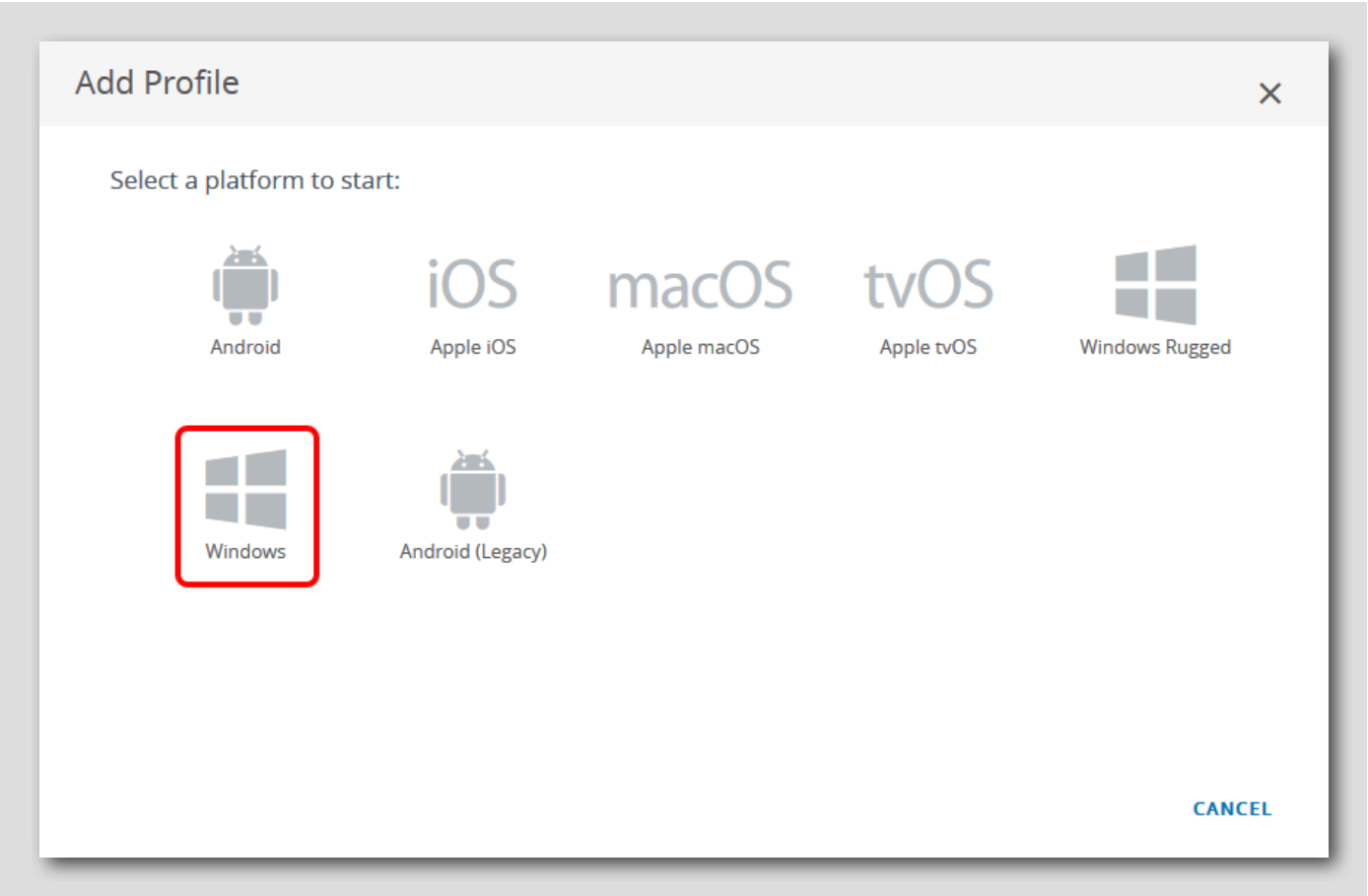


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Profiles & Baselines] セクションを展開します。
3. [Profiles] をクリックします。
4. [Add] をクリックします。
5. [Add Profile] をクリックします。

Windows プロファイルの追加

[151]

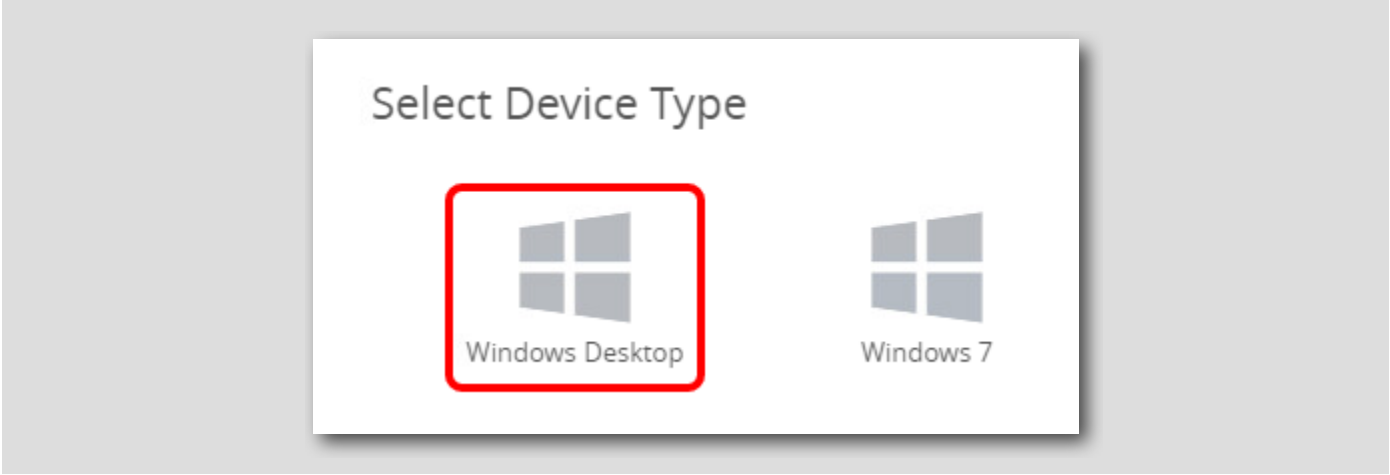


[Windows] アイコンを選択します。

注：[Windows Rugged] ではなく [Windows] を選択してください。

Windows デスクトップ プロファイルの追加

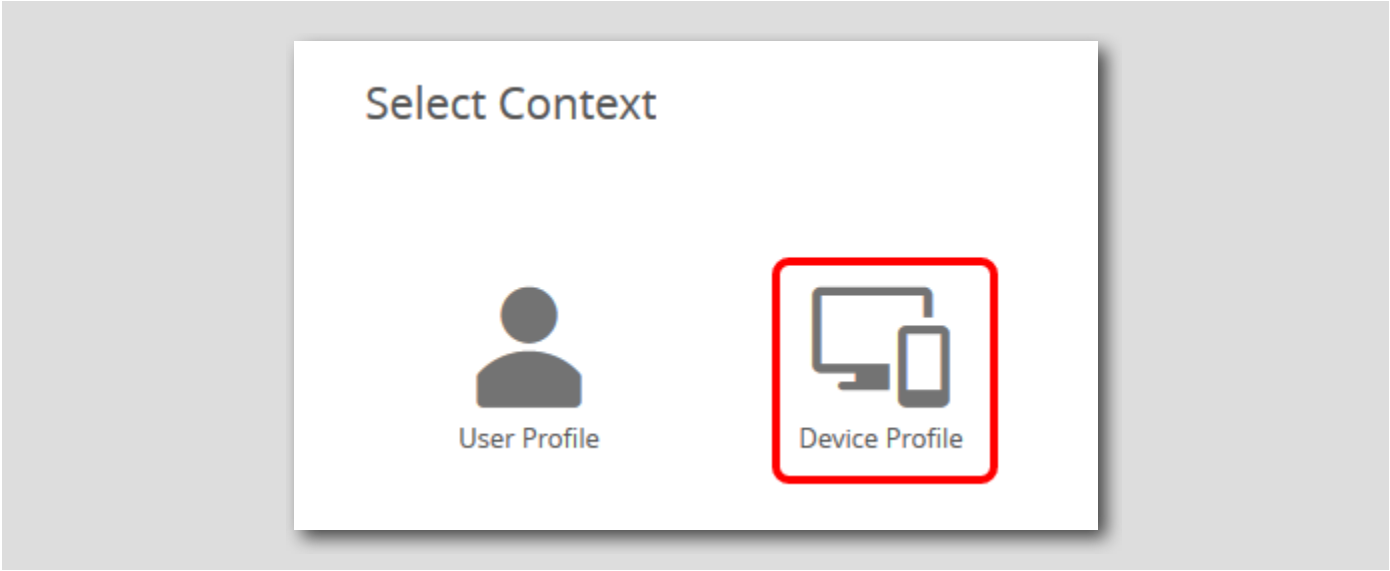
[152]



[Windows Desktop] を選択します。

[Context] > [Device Profile] の選択

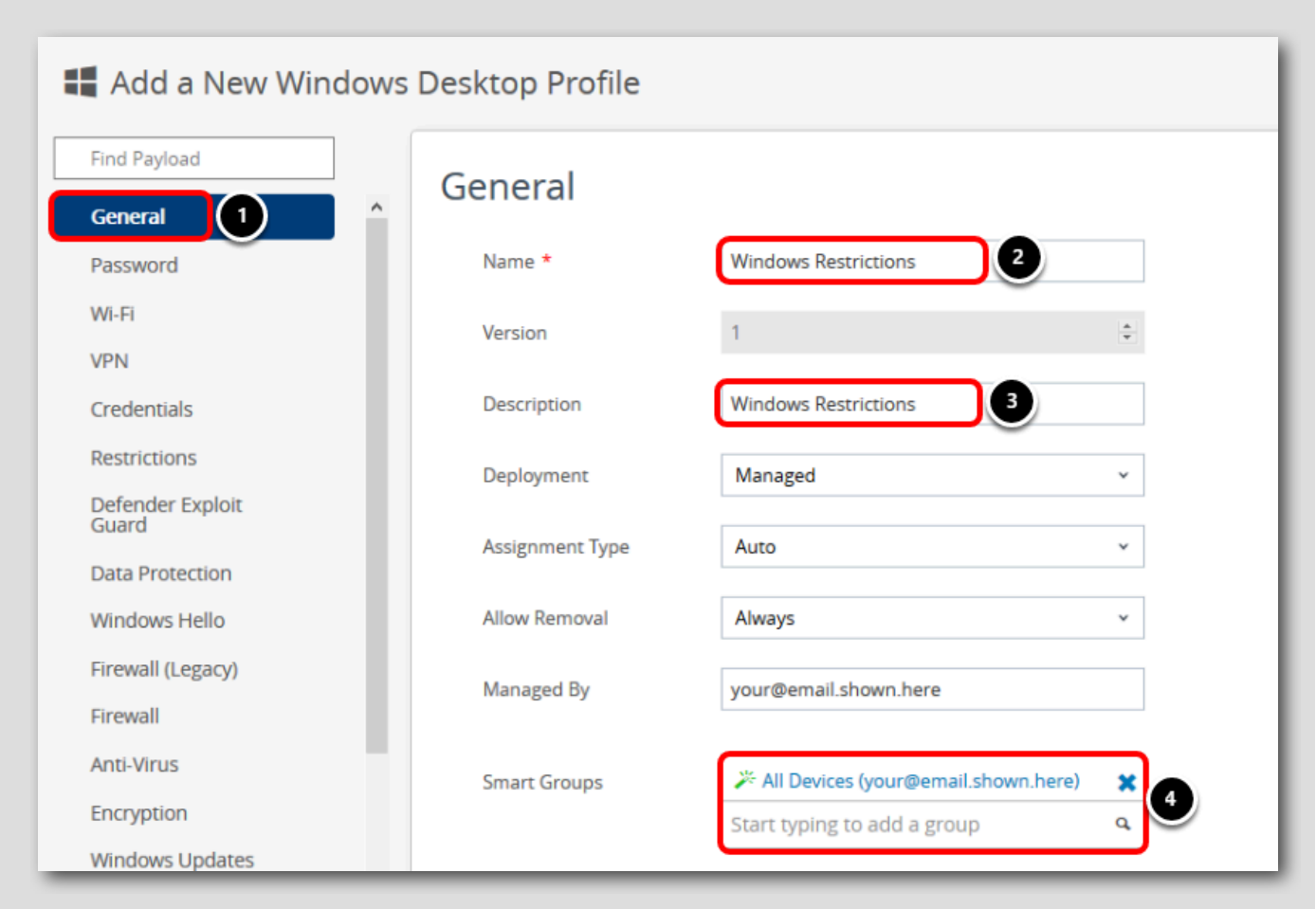
[153]



[Device Profile] を選択します。

全般設定の定義

[154]



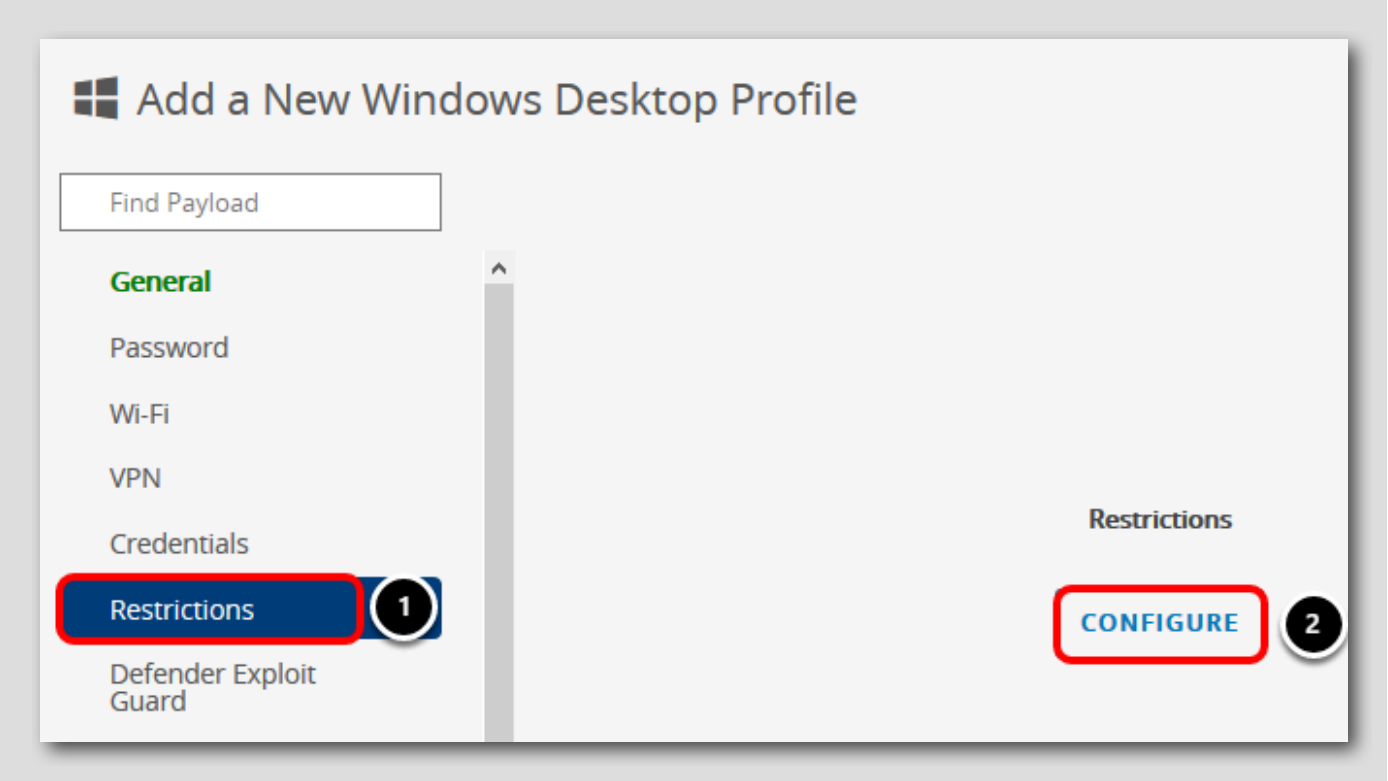
1. 選択されていない場合は、[General] を選択します。
2. [Name] テキスト ボックスに **`Windows Restrictions`** などのプロファイル名を入力します。
3. 必要に応じて、[Description] フィールドに **`Windows Restrictions`** と入力します。
4. [Smart Groups] フィールドをクリックします。作成されたスマート グループのリストがポップアップ表示されます。[All Devices] スマート グループを選択します。

   注：[Smart Groups] フィールドを表示するために、下にスクロールする必要がある場合があります。

注：この時点では、[Save & Publish] をクリックする必要はありません。このインターフェイスでは、保存する前に、さまざまなペイロード構成画面に移動できます。

制限事項ペイロードの選択

[155]

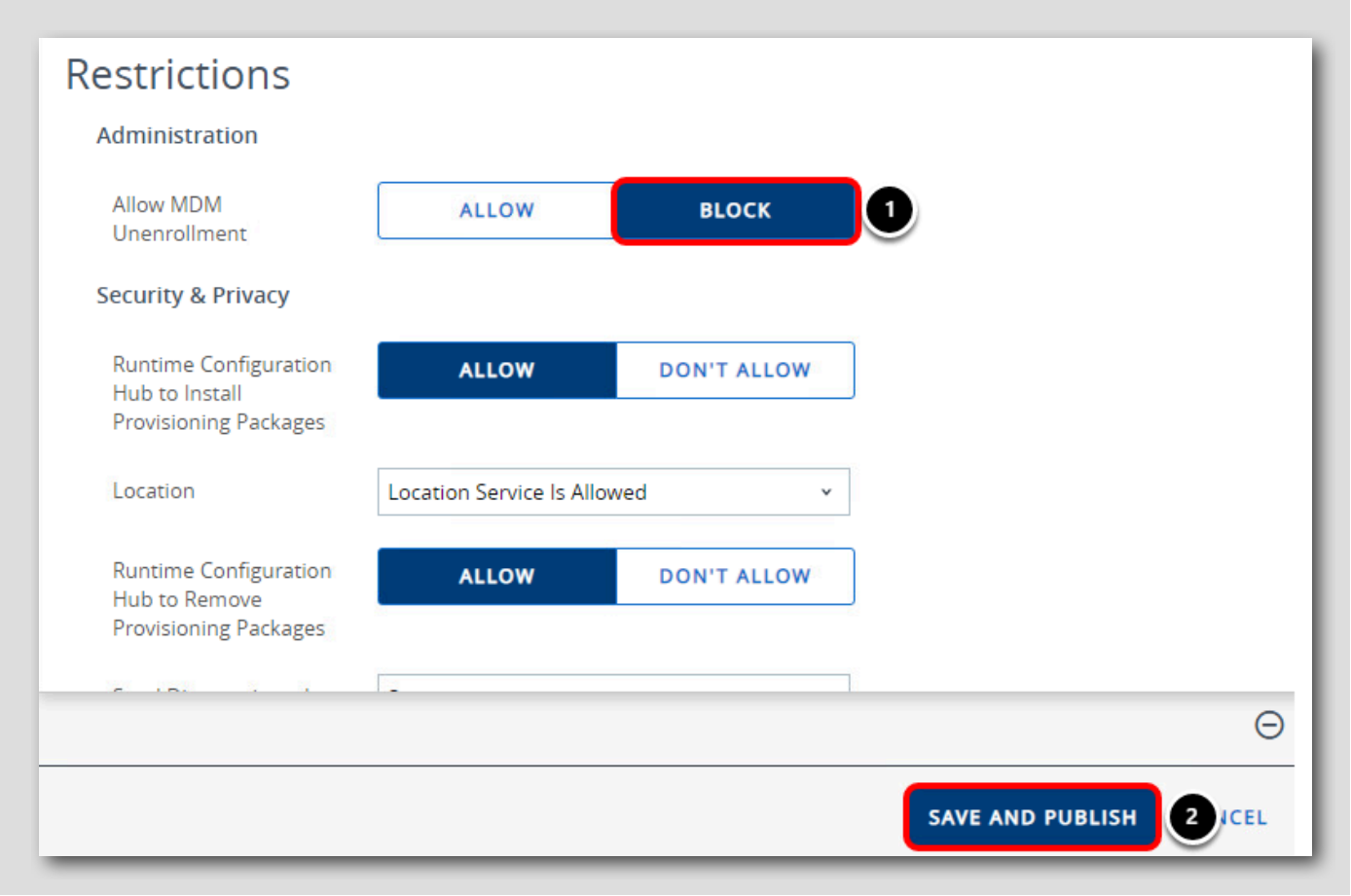


注：ペイロードを最初に設定するときには、ペイロード構成を誤って設定しないよう [Configure] ボタンが表示されます。

1. 左側の [Payload] セクションで [Restrictions] ペイロードを選択します。
2. [Configure] ボタンをクリックして、[Restrictions] ペイロードの設定を続行します。

制限の追加 - エンド ユーザー登録解除を無効にする

[156]



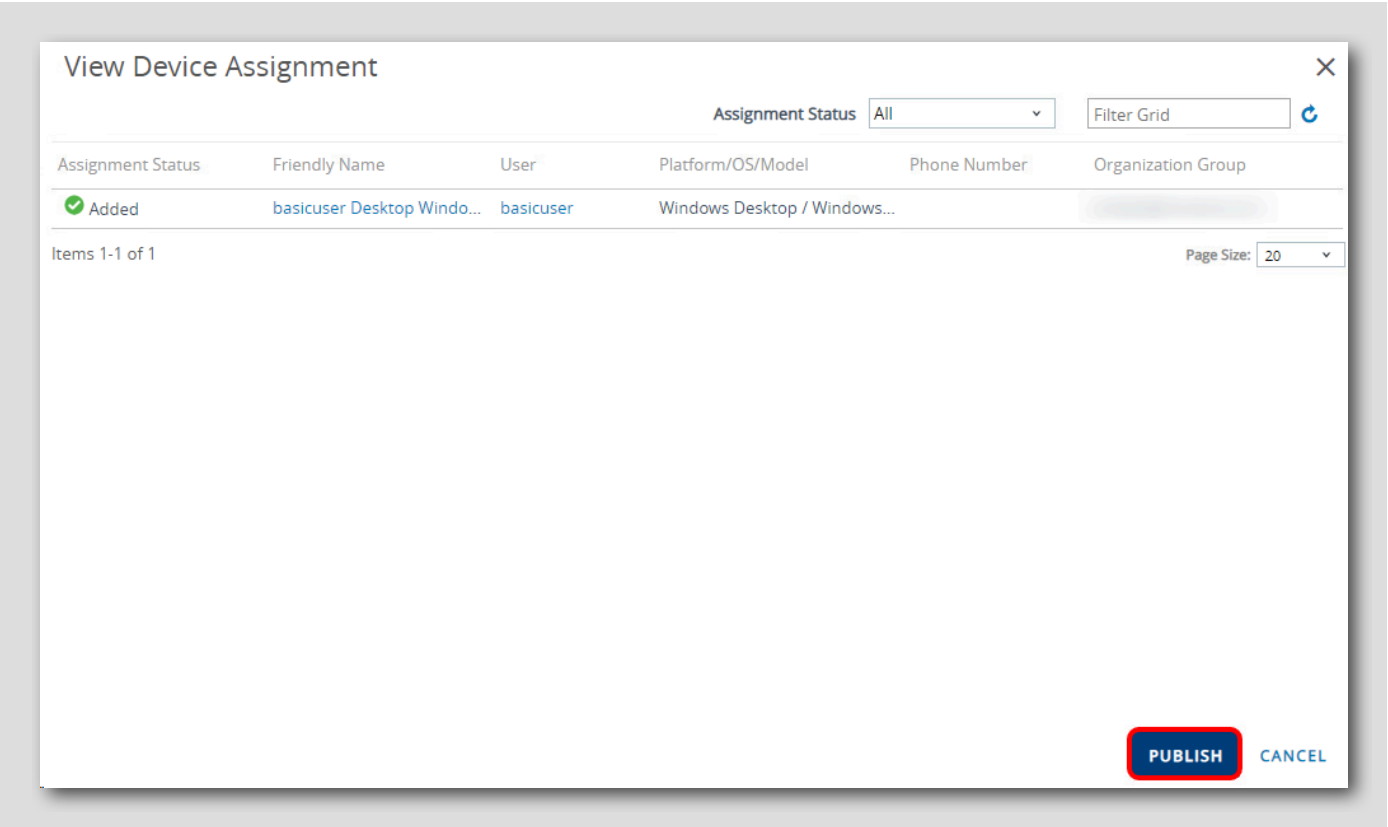
1. [Allow MDM Unenrollment] に対して [Block] を選択します。
2. [Save & Publish] をクリックします。

注：一部の制限事項では、特定のバージョン以降の Windows をデバイスに適用する必要があります。どのバージョンの Windows が必要かを判断するために、次のようないくつかの参考資料が用意されています。

- VMware Policy Builder：`https://www.vmwarepolicybuilder.com`
- 構成サービス プロバイダ (CSP) リファレンス：`http://aka.ms/CSPList`
- MDM の登録と管理の新機能：`https://docs.microsoft.com/ja-jp/windows/client-management/mdm/new-in-windows-mdm-enrollment-management`

制限事項プロファイルの公開

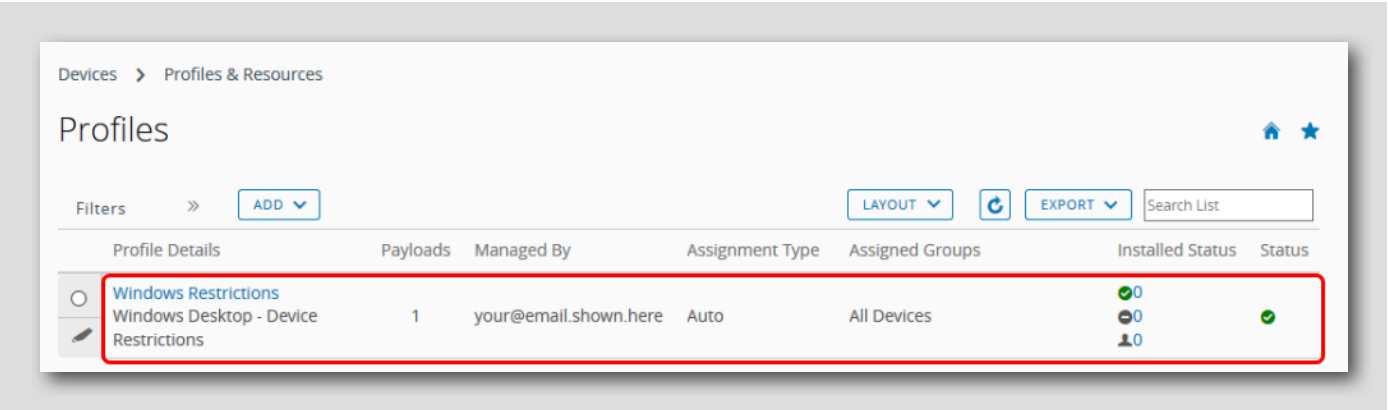
[157]



割り当てられたスマート グループに基づいて、このプロファイルを受信するデバイスのプレビューが表示されます。[Publish] をクリックします。

制限事項プロファイルが追加されたことの確認

[158]



現在、[Devices Profiles] ウィンドウのリスト表示に制限事項プロファイルが表示されているはずです。

注：制限事項プロファイルを編集する必要がある場合は、ここで実行します。プロファイルを編集するには、プロファイル名をクリックし、[Add Version] を選択します。プロファイルを更新し、[Save & Publish] をクリックして、新しい設定を割り当てられたデバイスにプッシュします。

Windows 10 でのオンデマンド アプリケーションの提供

[159]

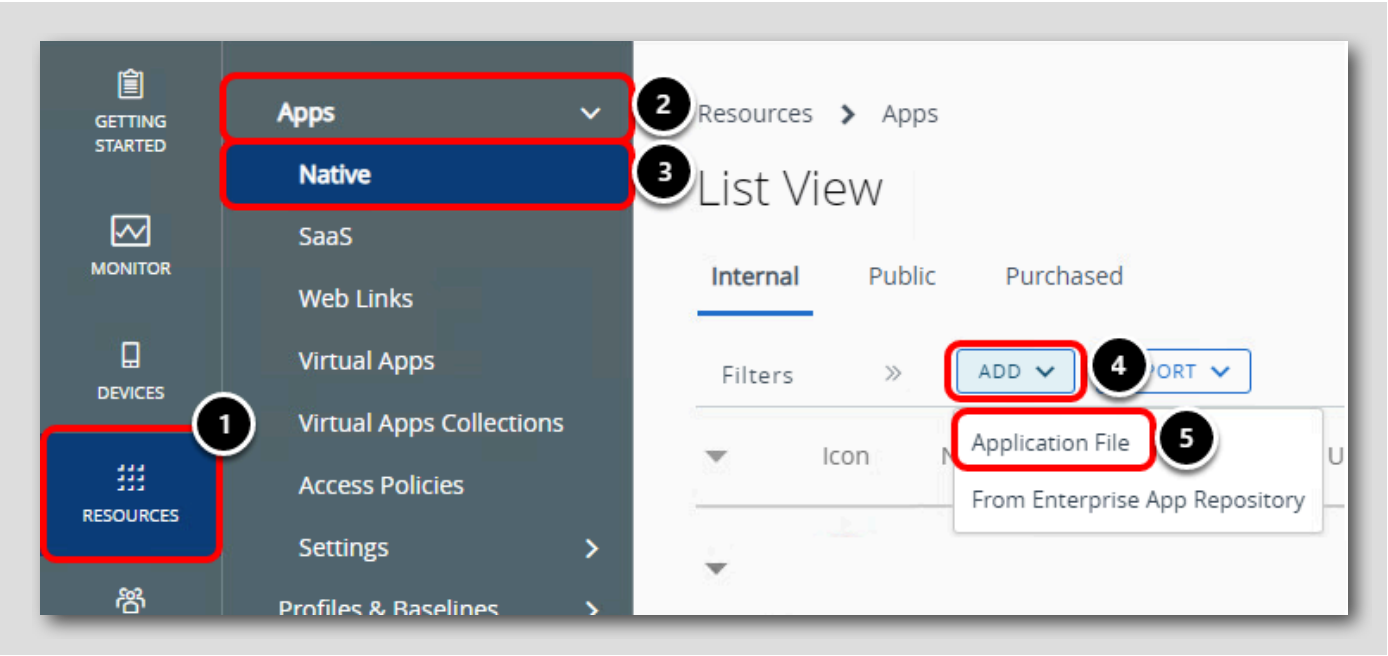
アプリケーションを配布するには、[On Demand] と [Auto] の 2 つの方法があります。

- [On Demand] では、ユーザーがアプリケーションにアクセスする必要があると判断したときに、Intelligent Hub アプリケーション カタログに表示されているアプリケーションのダウンロードとインストールを開始できます。
- [Auto] では、ユーザーが Intelligent Hub アプリケーション カタログからアプリケーションを操作する必要なく、自動的にアプリケーションをダウンロードしてデバイスにインストールします。

この演習では、オンデマンド アプリケーションとして、7-Zip 実行ファイルを展開する方法について説明します。

内部アプリケーションの追加

[160]

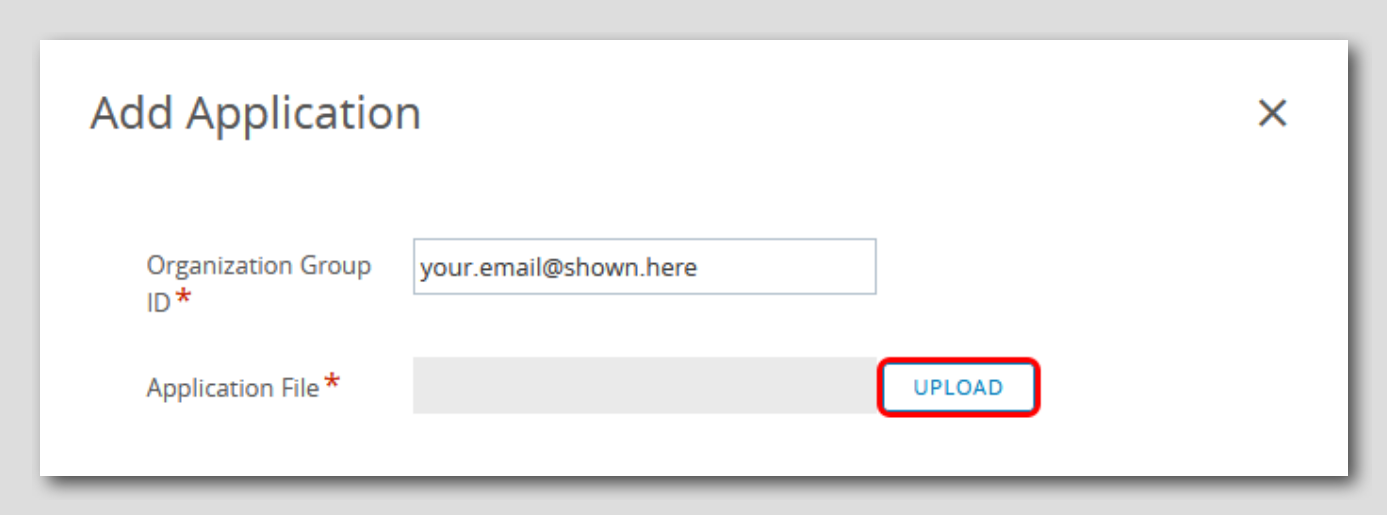


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Apps] セクションを展開します。
3. [Native] をクリックします。
4. [Add] をクリックします。
5. [Application File] をクリックします。

アプリケーションのアップロード

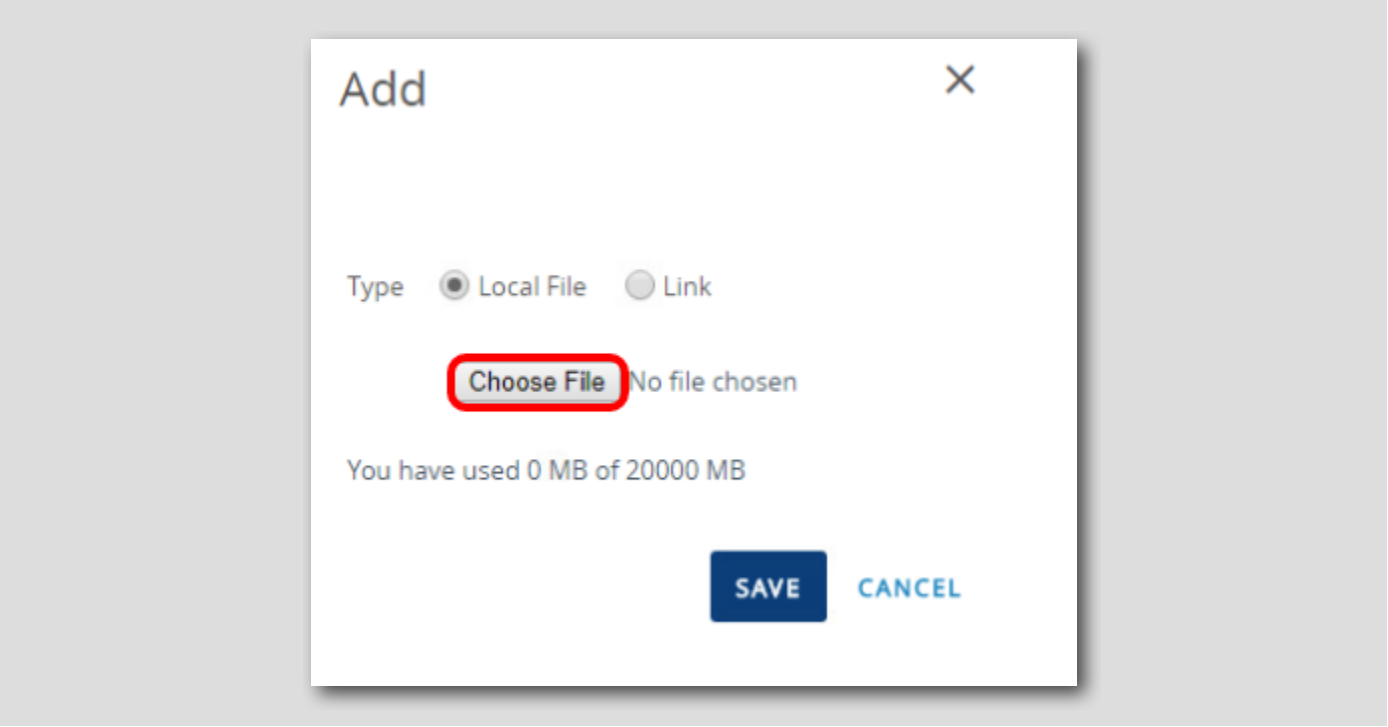
[161]



[Upload] をクリックします。

アプリケーション インストーラの検索

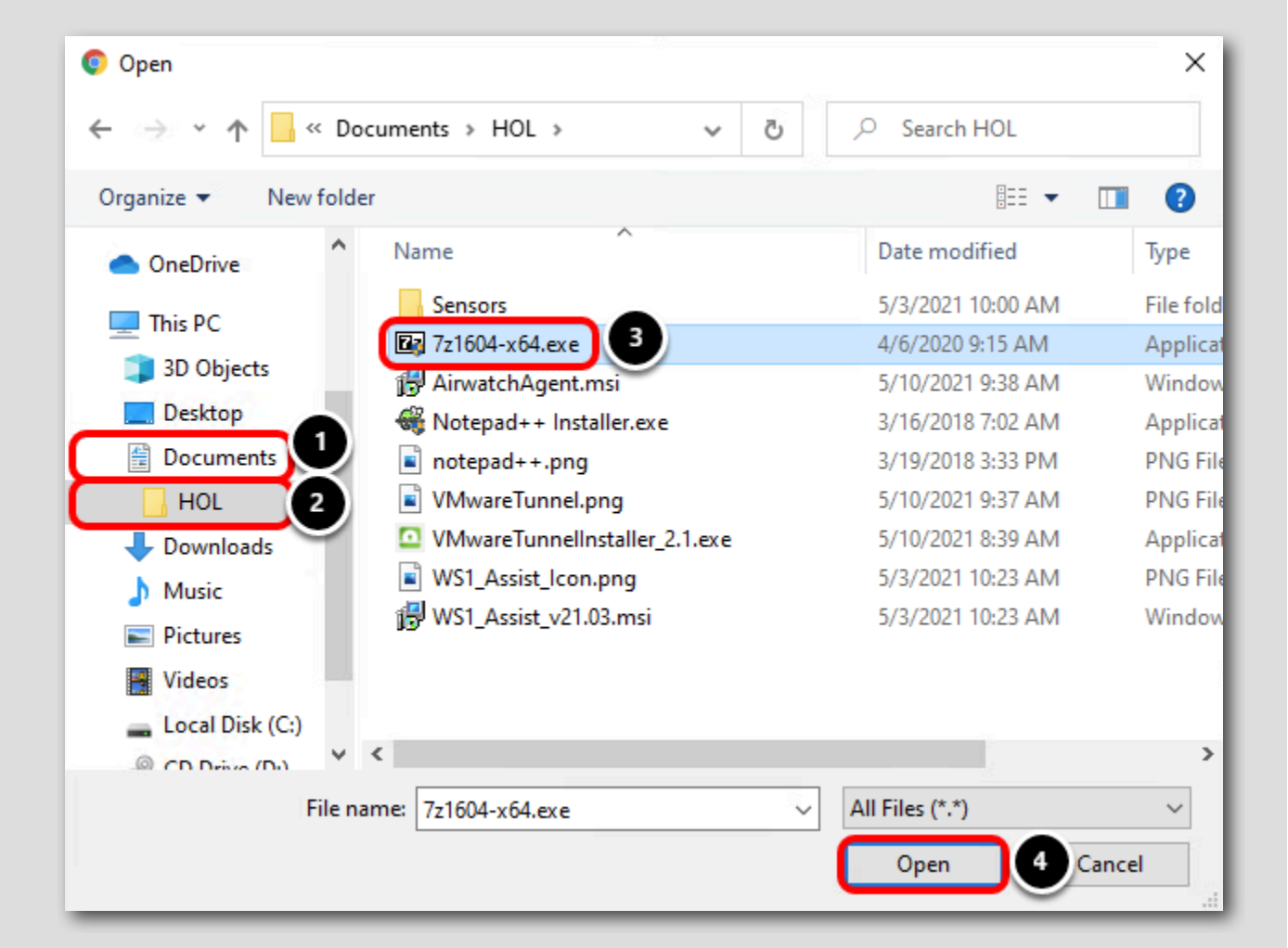
[162]



[Choose File] ボタンをクリックします。

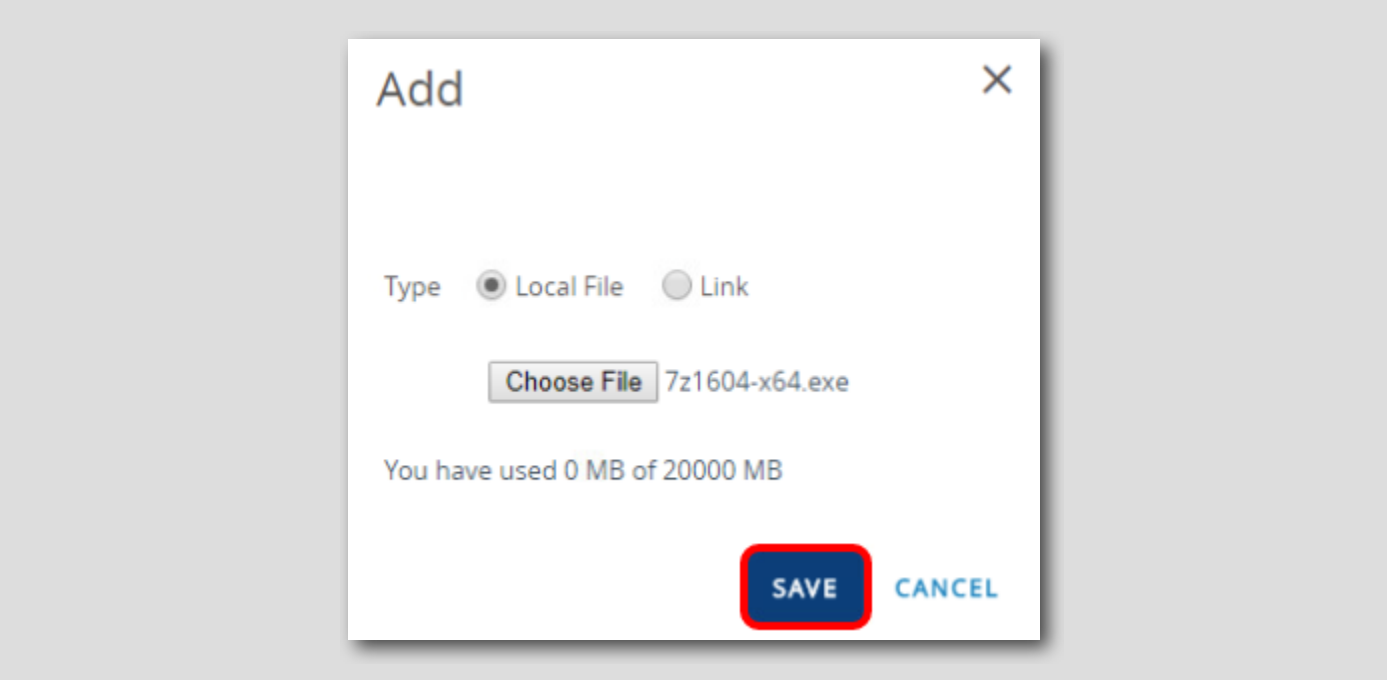
7-Zip EXE ファイルのアップロード

[163]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. 7z1604-x64 実行ファイルを選択します。
4. [Open] をクリックします。

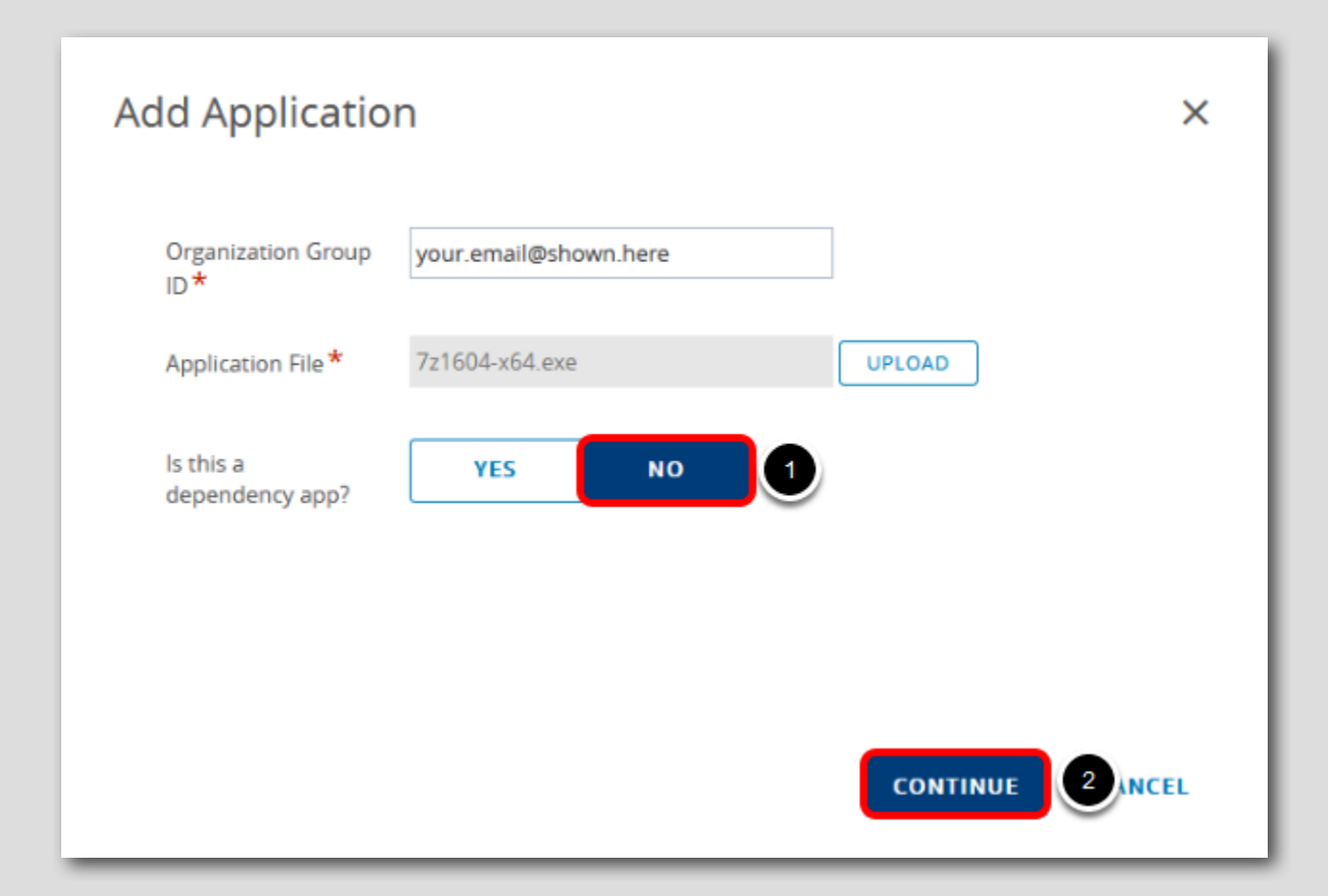
EXE ファイルの保存 [164]



[Save] をクリックします。

アプリケーションの設定に進む

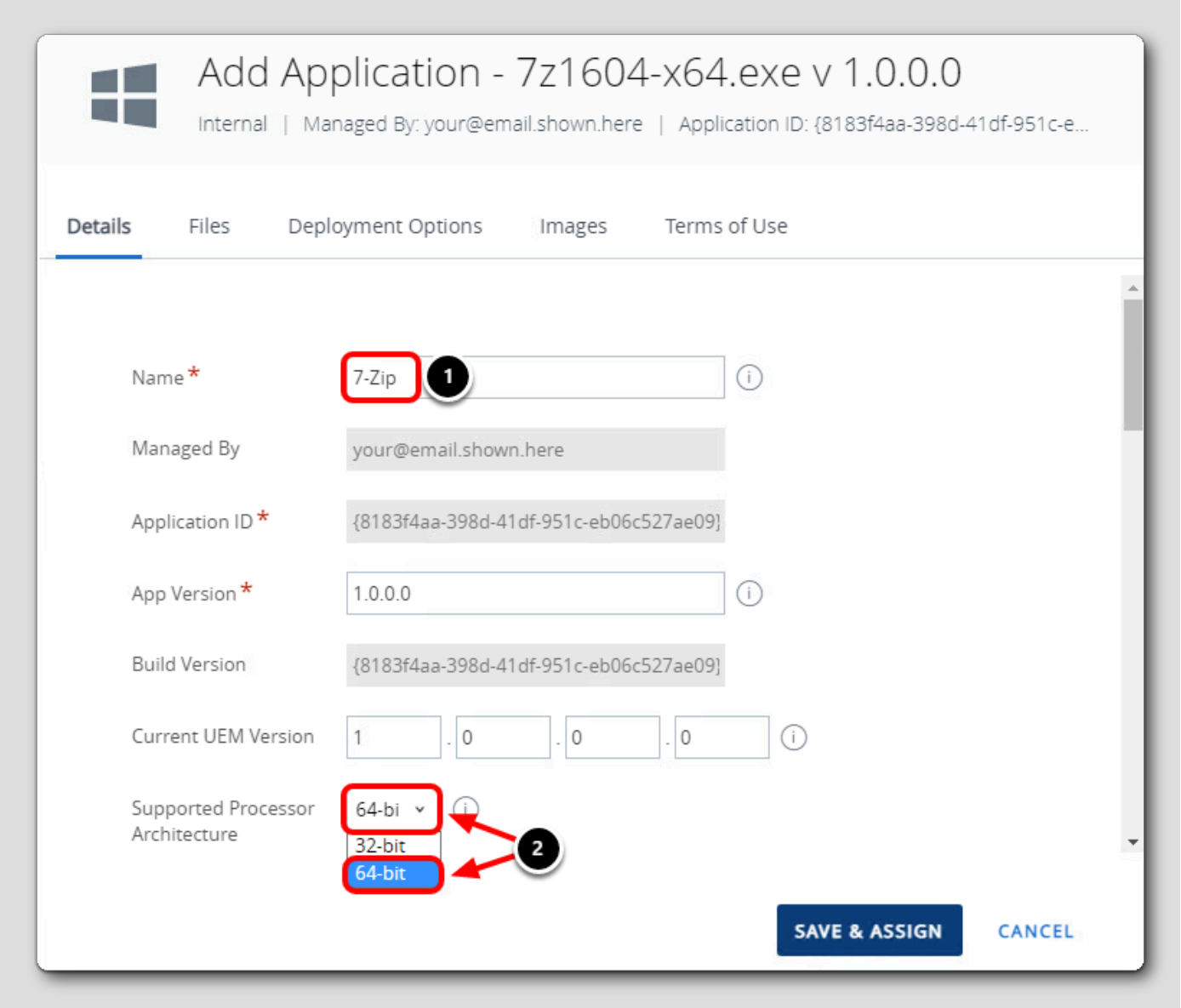
[165]



1. [Is this a dependency app?] に対して [No] をクリックします。
2. [Continue] をクリックします。

アプリケーションの詳細の設定

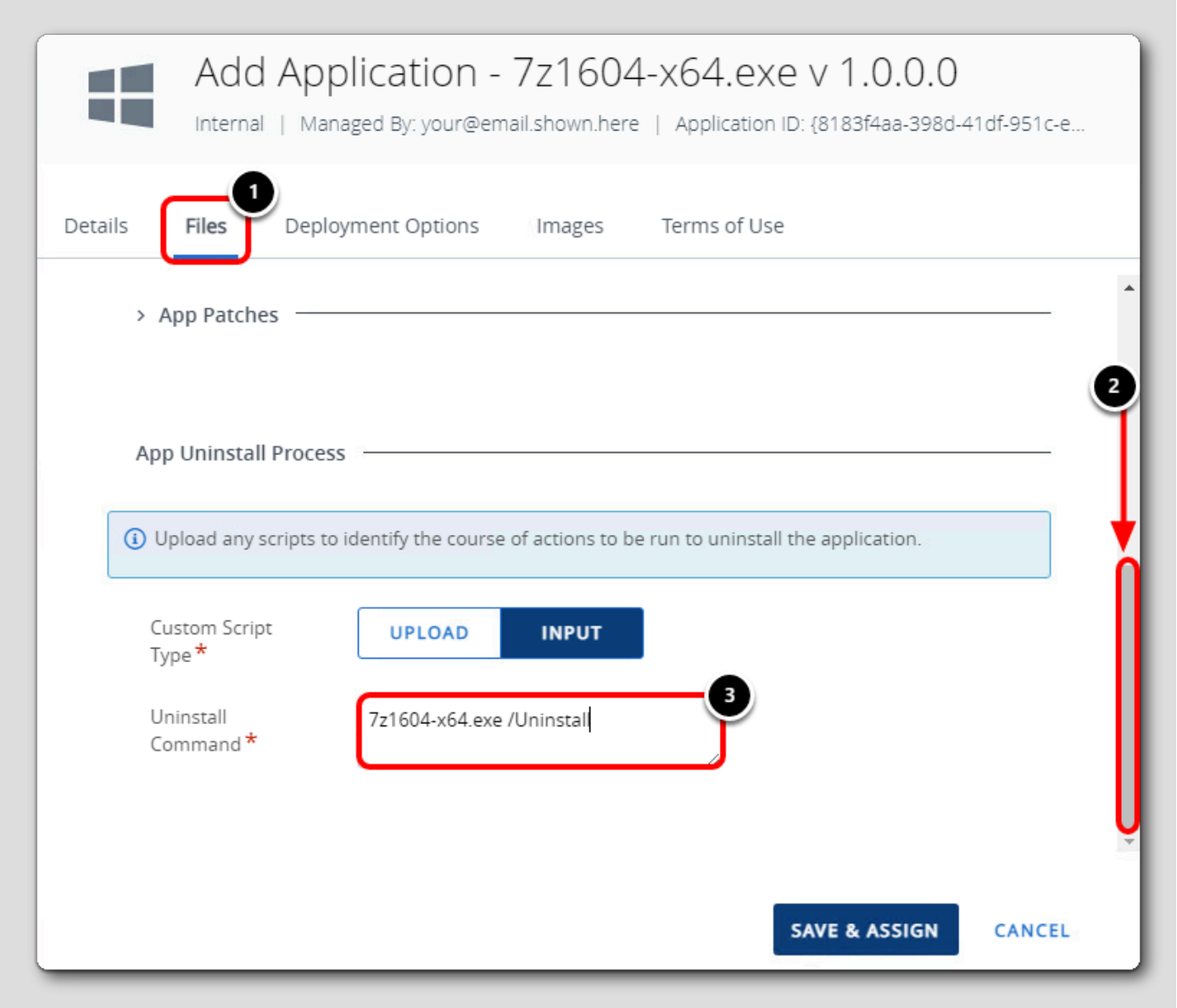
[166]



1. アプリケーションの名前に **7-Zip** と入力します。この名前は、ユーザー向けのアプリケーション カタログに表示されます。
2. [Supported Processor Architecture] に対して [64-bit] を選択します。

アプリケーション ファイルの構成

[167]



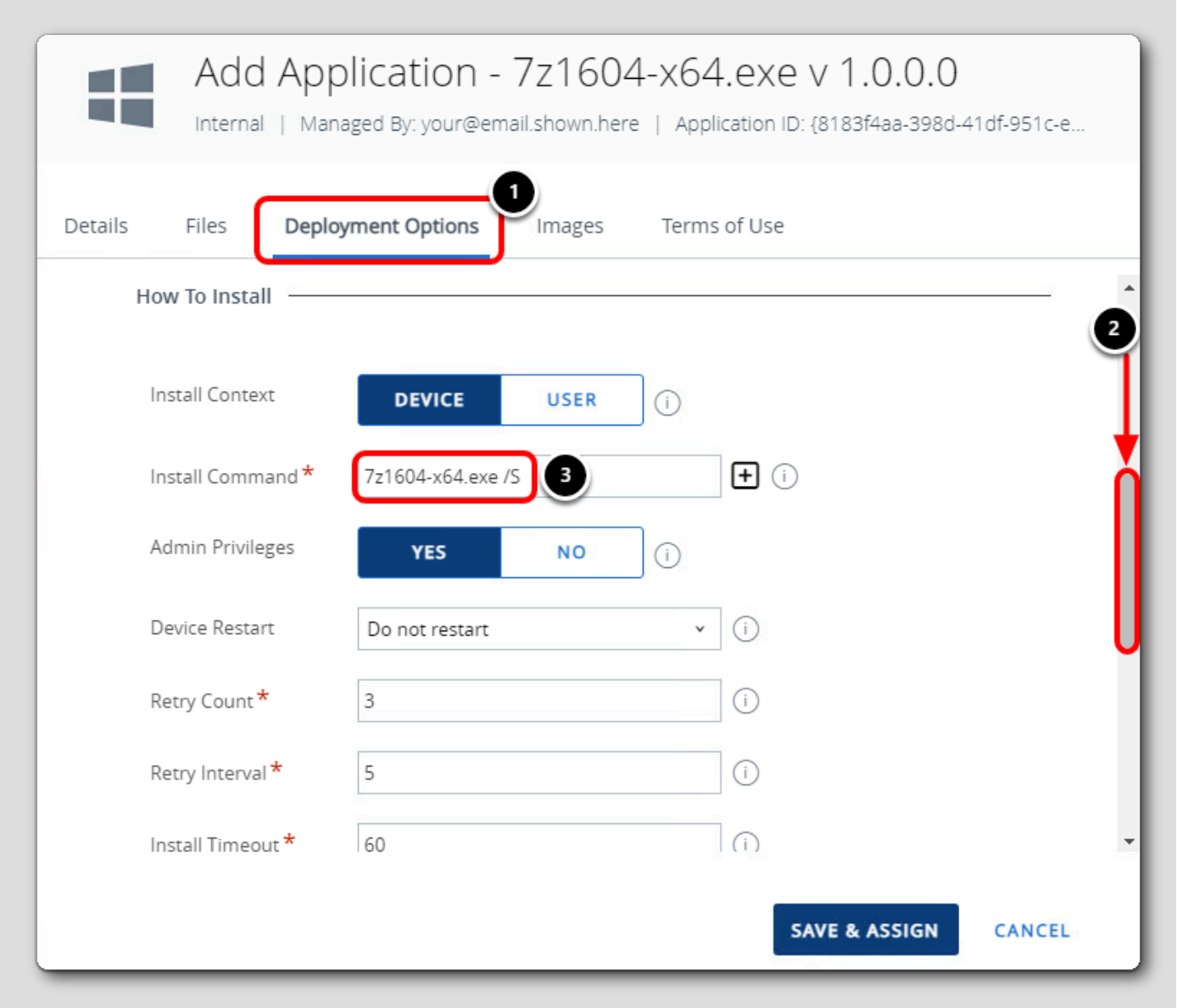
1. [Files] タブを選択します。
2. 下にスクロールして、[App Uninstall Process] セクションを見つけます。
3. [Uninstall Command] に `7z1604-x64.exe /Uninstall` と入力します。

注：マニュアルのテキストをコピーしてラボに貼り付け、入力ミスを回避できることを忘れないでください。

注：マニュアルからテキストをコピーする方法については、「ガイダンス」セクションを参照してください。

展開オプションの選択

[168]



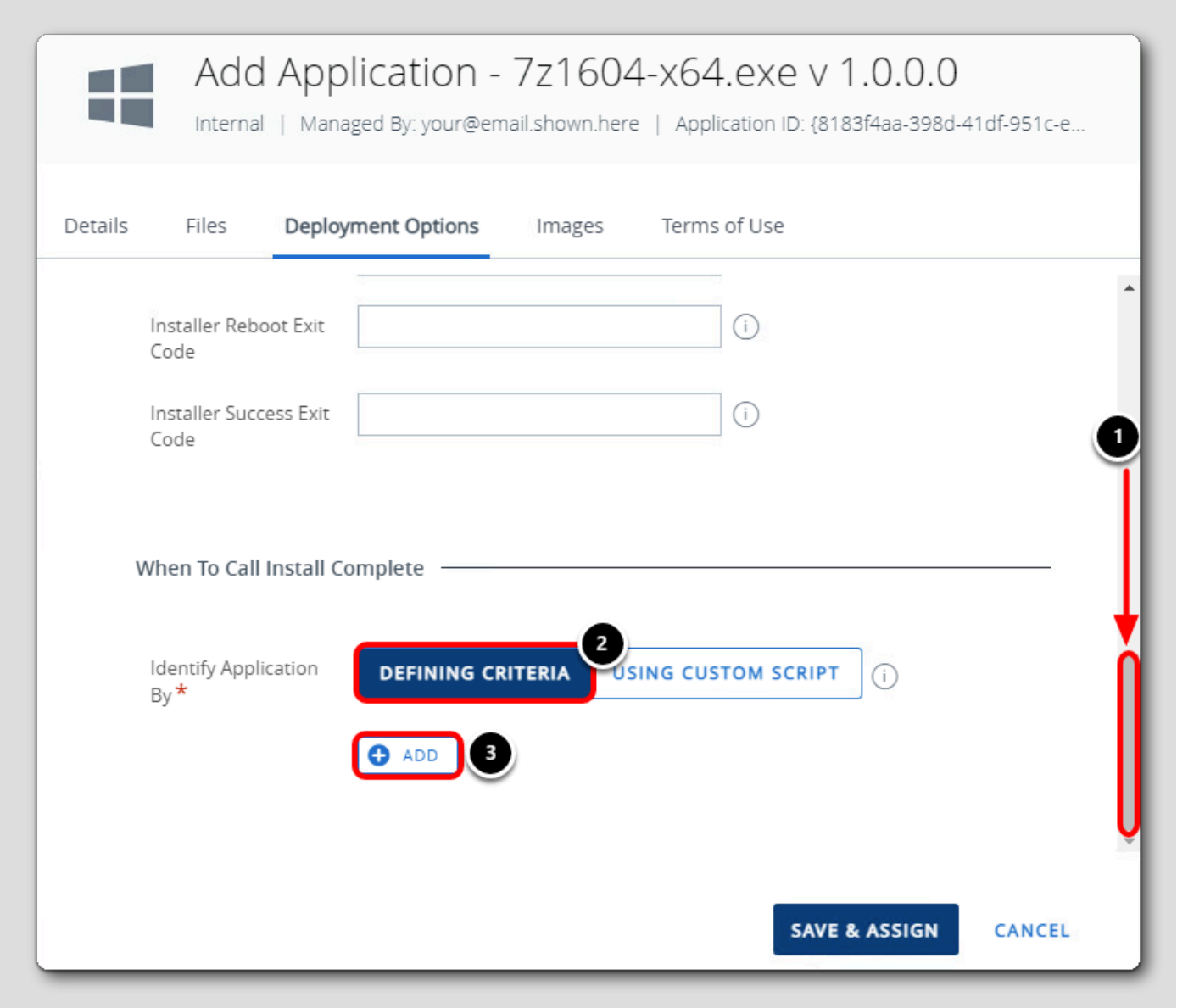
1. [Deployment Options] を選択します。
2. 下にスクロールして、[Install Command] オプションを表示します。
3. [Install Command] に `7z1604-x64.exe /S` と入力します。

注：マニュアルのテキストをコピーしてラボに貼り付け、入力ミスを回避できることを忘れないでください。

注：マニュアルからテキストをコピーする方法については、「ガイダンス」セクションを参照してください。

アプリケーションの識別条件の追加

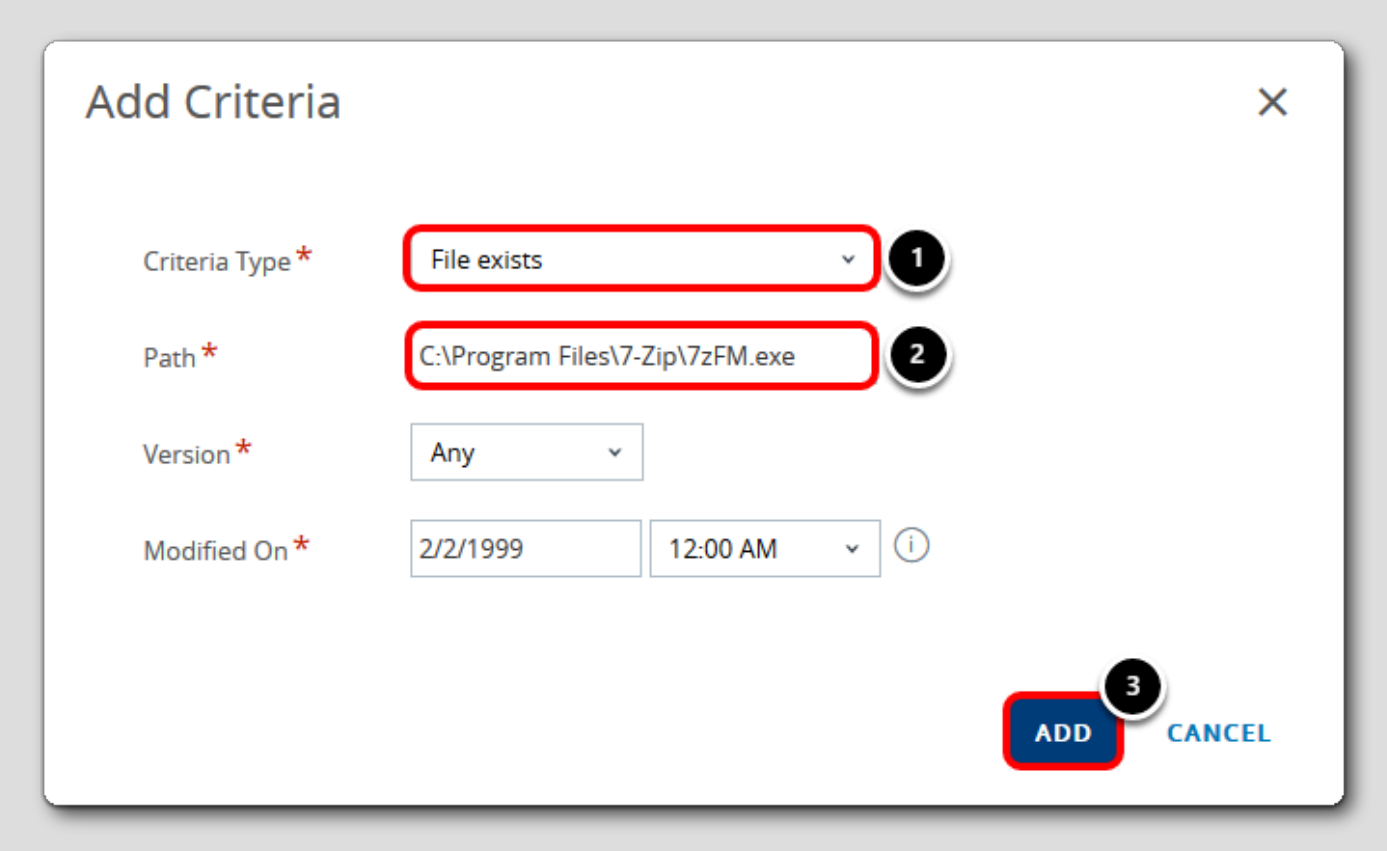
[169]



1. 下にスクロールして、[When To Call Install Complete] セクションを見つけます。
2. [Identity Application By] に対して [Defining Criteria] を選択します。
3. [Add] をクリックします。

インストール完了を判断する条件の設定

[170]



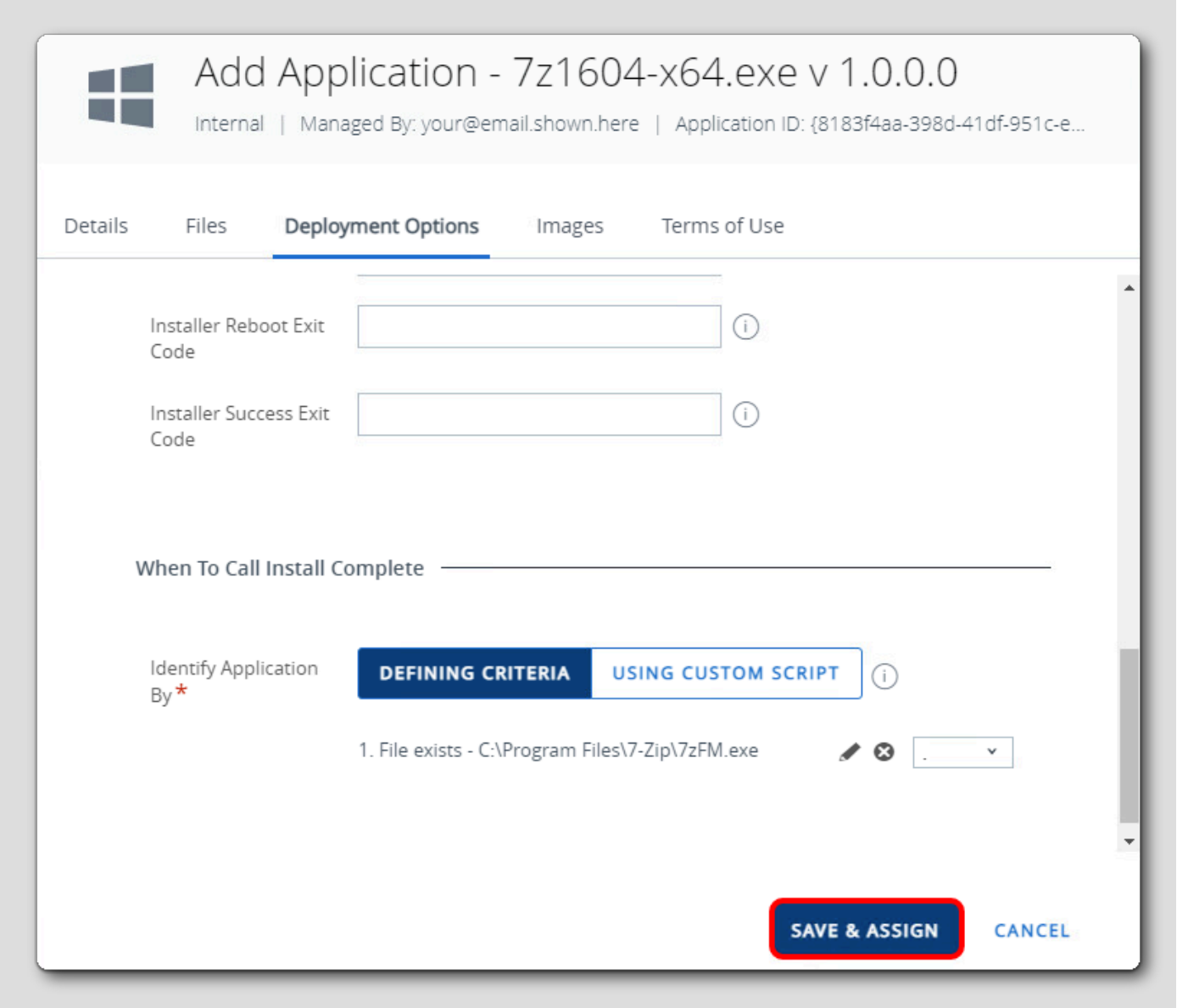
1. [Criteria Type] で [File Exists] を選択します。
2. [Path] に `C:\Program Files\7-Zip\7zFM.exe` と入力します。
3. [Add] をクリックします。

注：マニュアルのテキストをコピーしてラボに貼り付け、入力ミスを回避できることを忘れないでください。

注：マニュアルからテキストをコピーする方法については、「ガイダンス」セクションを参照してください。

アプリケーションの保存と割り当て

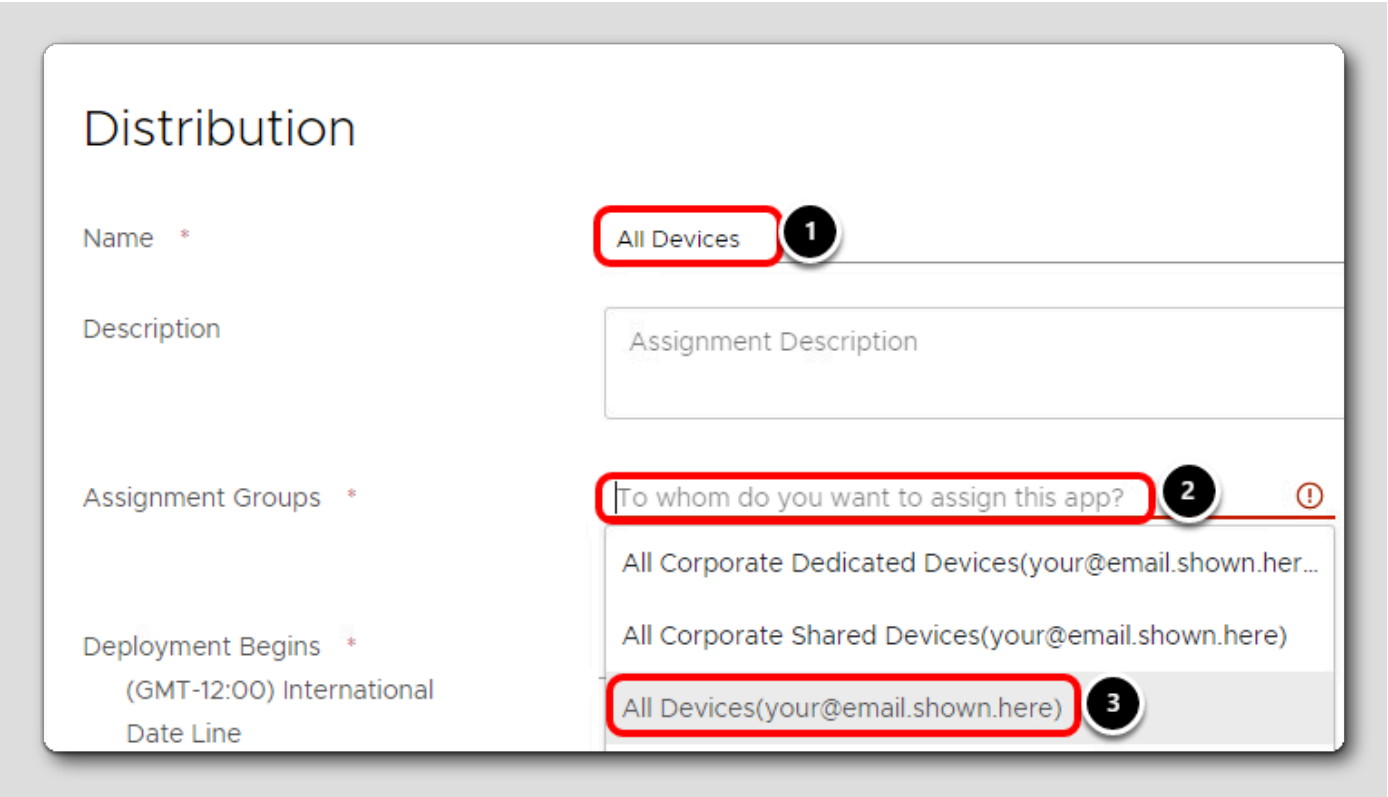
[171]



[Save & Assign] をクリックします。

割り当て配布の構成

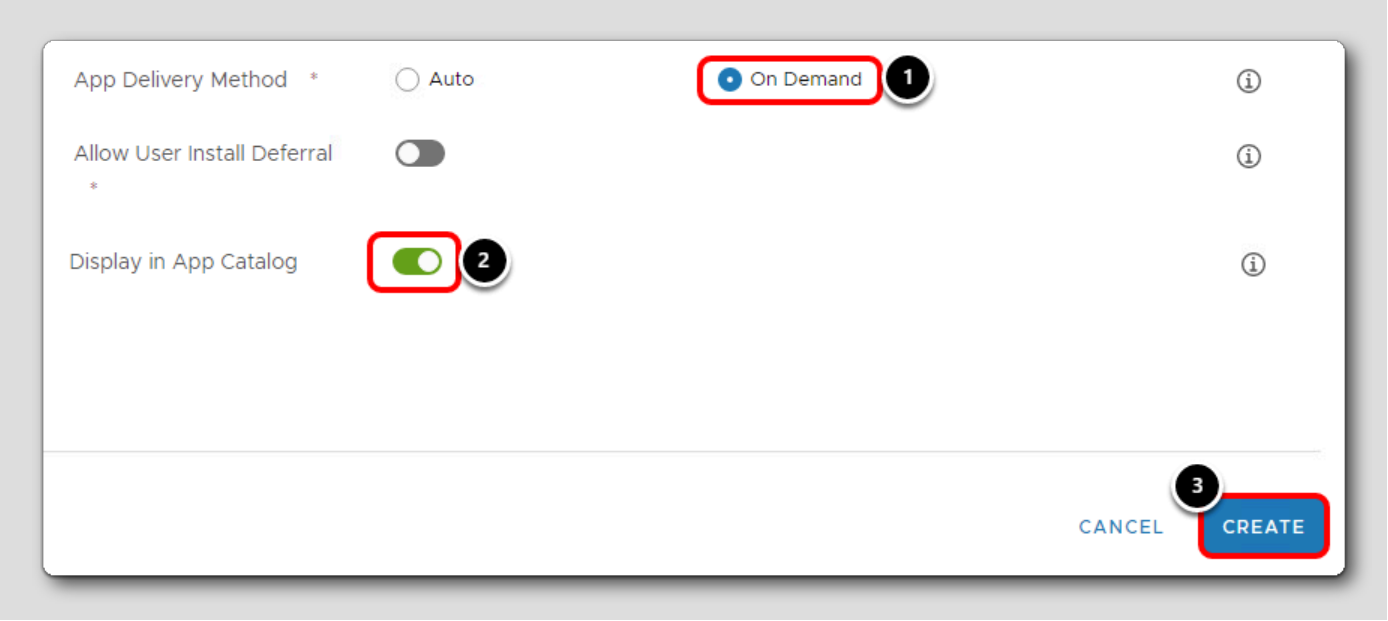
[172]



1. [Name] に **`All Devices`** と入力します。
2. [Assignment Groups] フィールドをクリックします。
3. リストから [All Devices (your@email.shown.here)] を選択します。

割り当てグループとプッシュ モードの追加

[173]

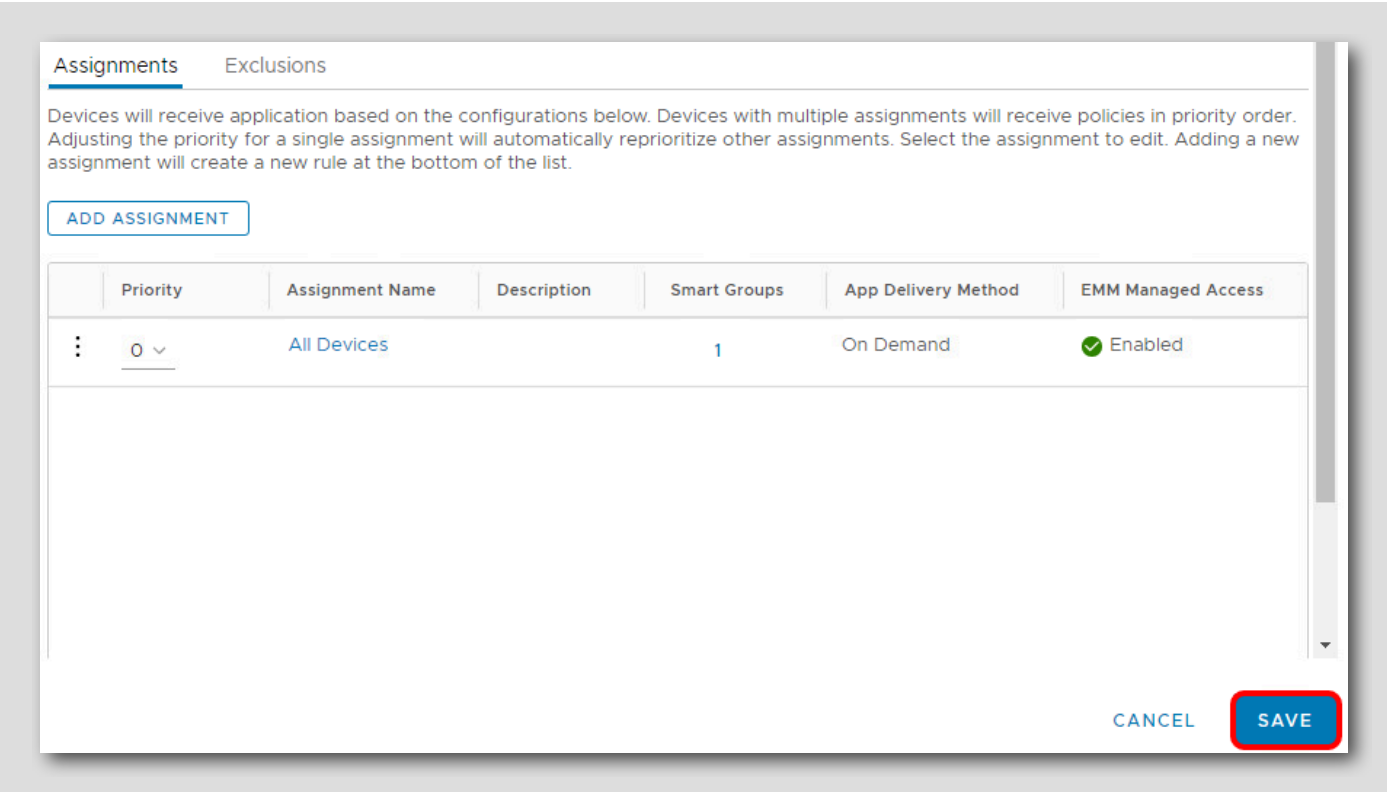


1. [App Delivery Method] に対して [On Demand] を選択します。これにより、アプリケーション カタログ内の割り当てられたユーザーがアプリケーションを利用できるようになります。
2. [Display in App Catalog] 設定を有効にします。
3. [Create] をクリックします。

注：アプリケーション カタログにアプリケーションを表示するかどうかを選択できるようになりました。これは、ドライバの更新またはスクリプト化されたアクションを展開し、エンド ユーザーがカタログでこれを表示できないようにする場合に役立ちます。

割り当ての保存

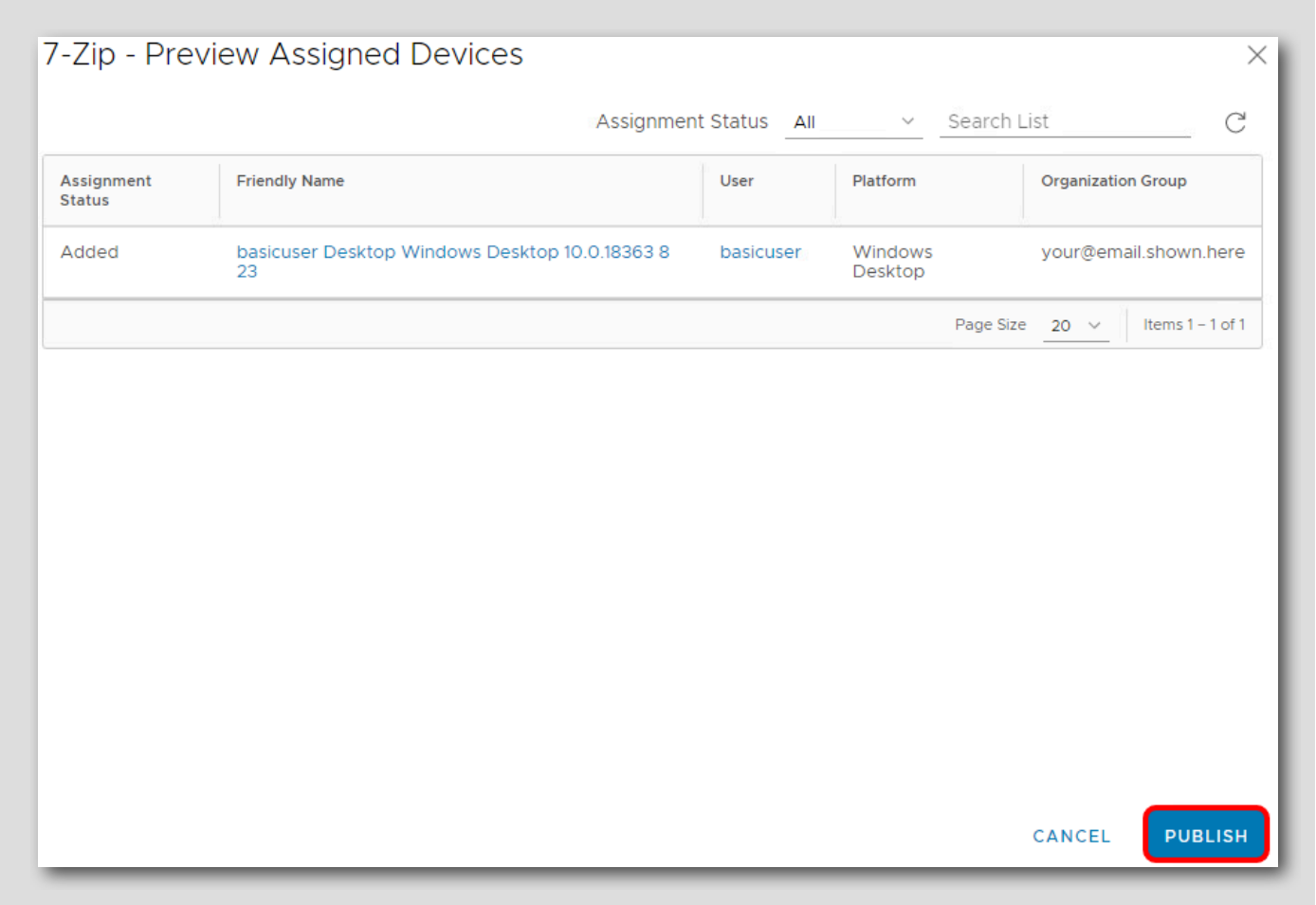
[174]



[Save] をクリックしてアプリケーションの割り当てを保存します。

アプリケーションの公開

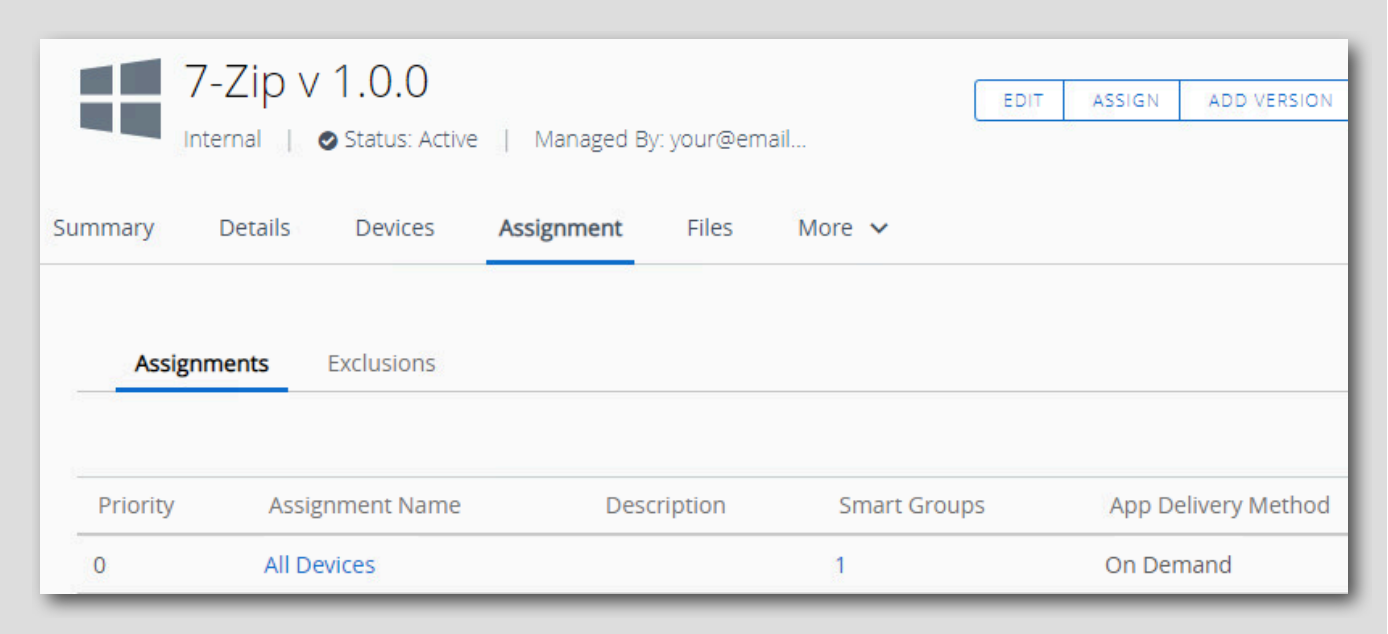
[175]



[Publish] をクリックして、表示されているデバイスのリストにアプリケーションを公開します。

アプリケーション作成の確認

[176]



7-Zip アプリケーションが作成され、[All Devices] スマート グループにオンデマンド アプリケーションとして割り当てられています。つまり、登録時にエンド ユーザーのデバイスに自動的にインストールされることはありません。これにより、エンド ユーザーがアプリケーション カタログを介して、または管理者が Workspace ONE UEM 管理者コンソールを介してアプリケーションをインストールできるようになります。

次の手順に進んでください。

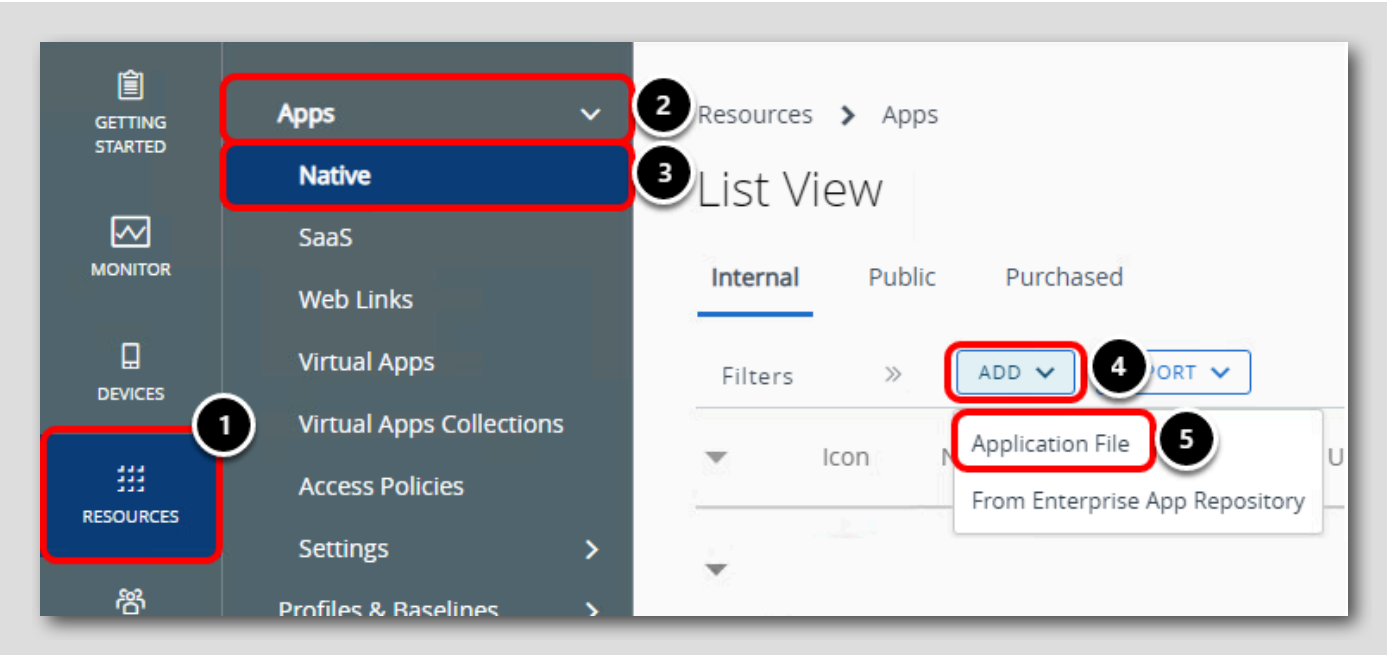
Windows 10 での自動アプリケーションの配布

[177]

次に、自動アプリケーションを配布します。これにより、ユーザーは Intelligent Hub アプリケーション カタログ内のアプリケーションを操作しなくても、アプリケーションを自動的にダウンロードしてユーザーのデバイスにインストールできます。

内部アプリケーションの追加

[178]

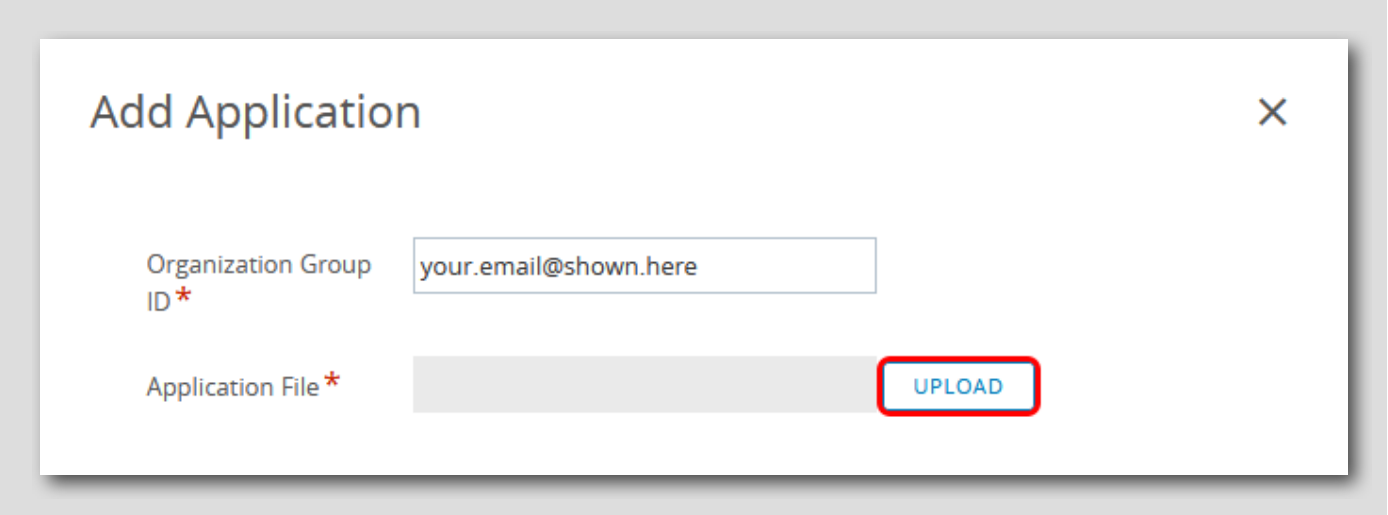


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Apps] セクションを展開します。
3. [Native] をクリックします。
4. [Add] をクリックします。
5. [Application File] をクリックします。

アプリケーションのアップロード

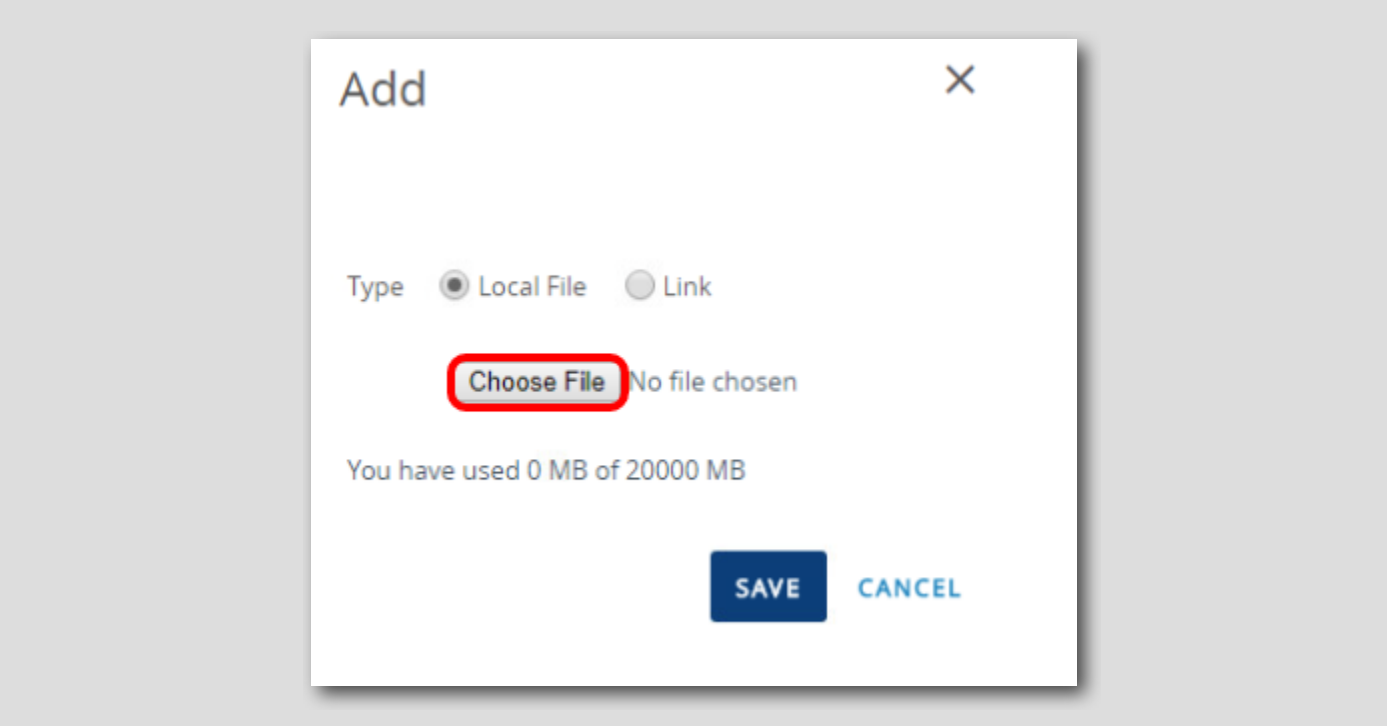
[179]



[Upload] をクリックします。

アプリケーション MSI の選択

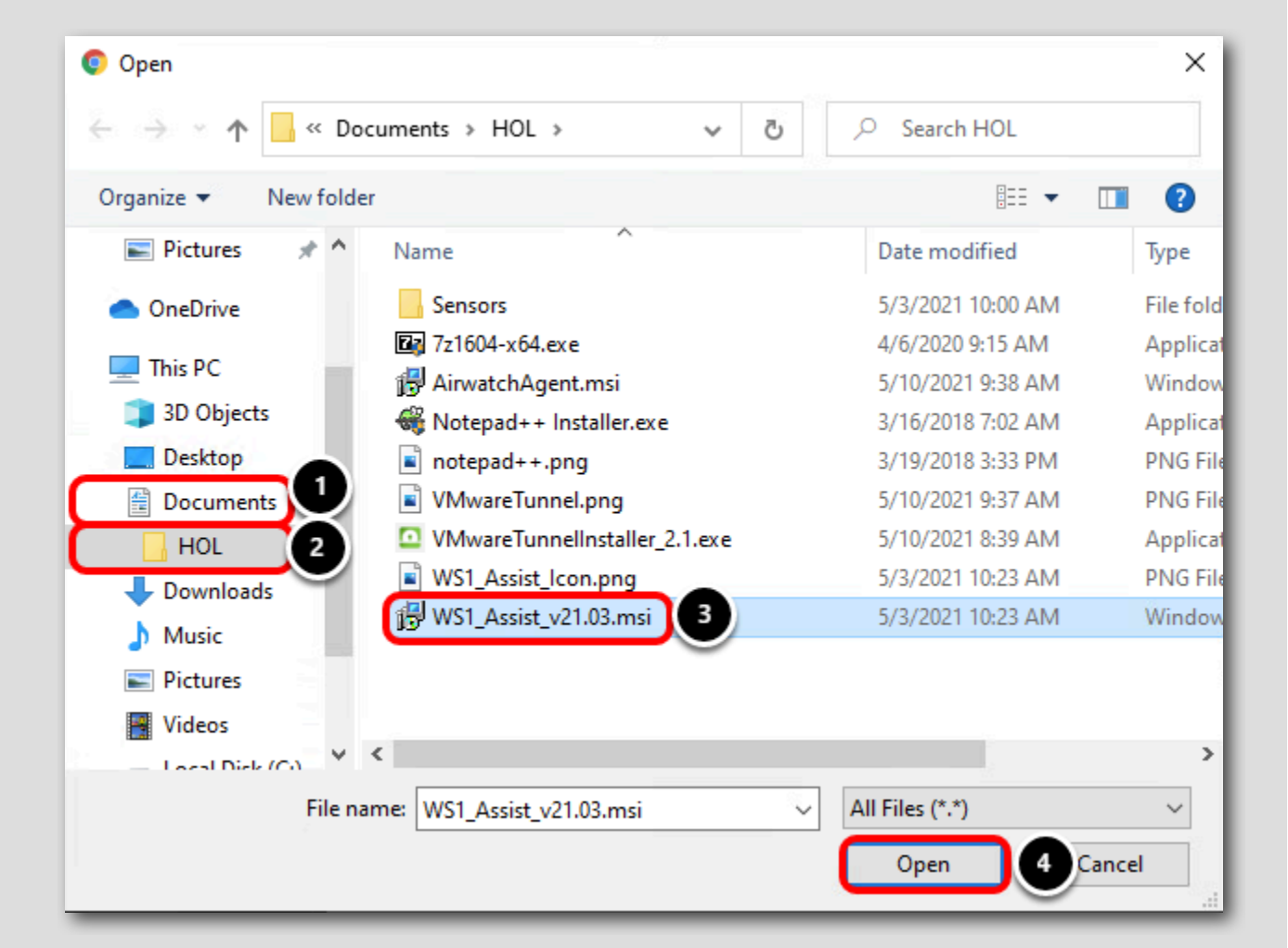
[180]



[Choose File] ボタンをクリックします。

Workspace ONE Assist MSI ファイルのアップロード

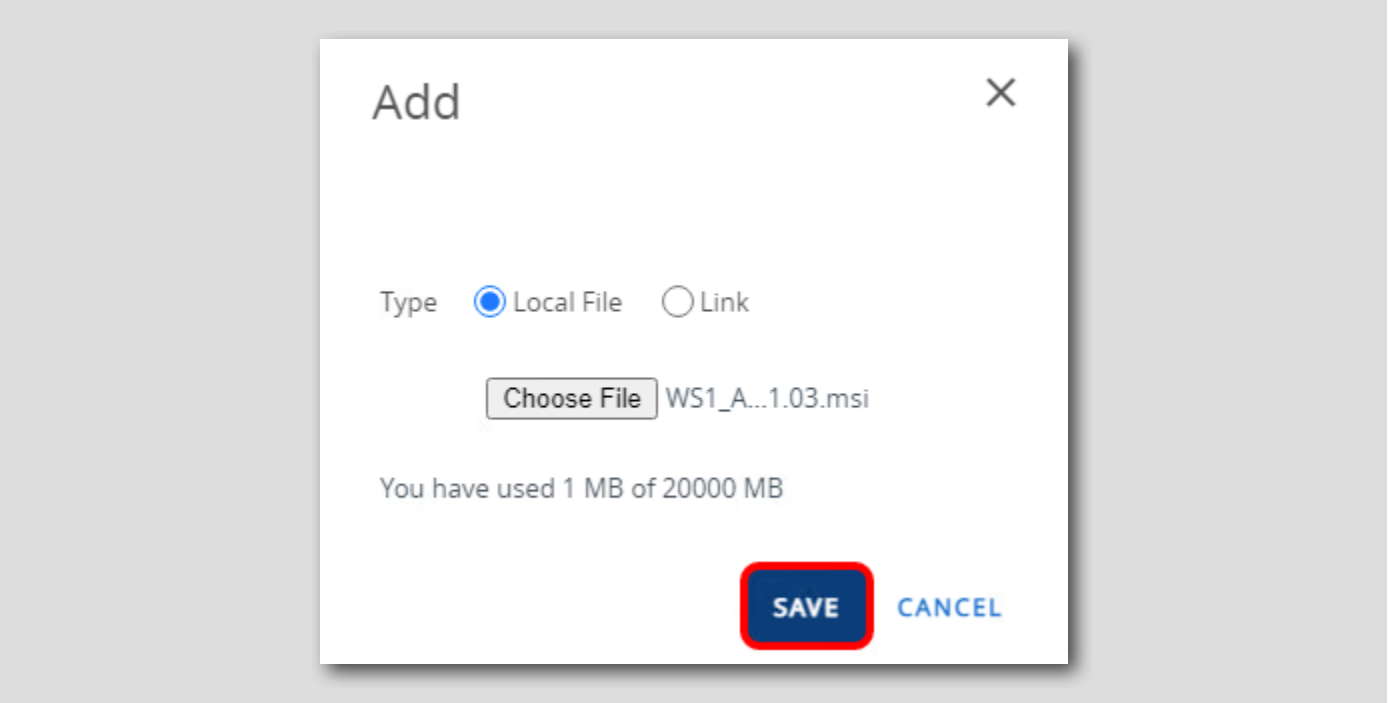
[181]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [WS1_Assist_v21.03.msi] ファイルを選択します。
4. [Open] をクリックします。

MSI ファイルの保存

[182]

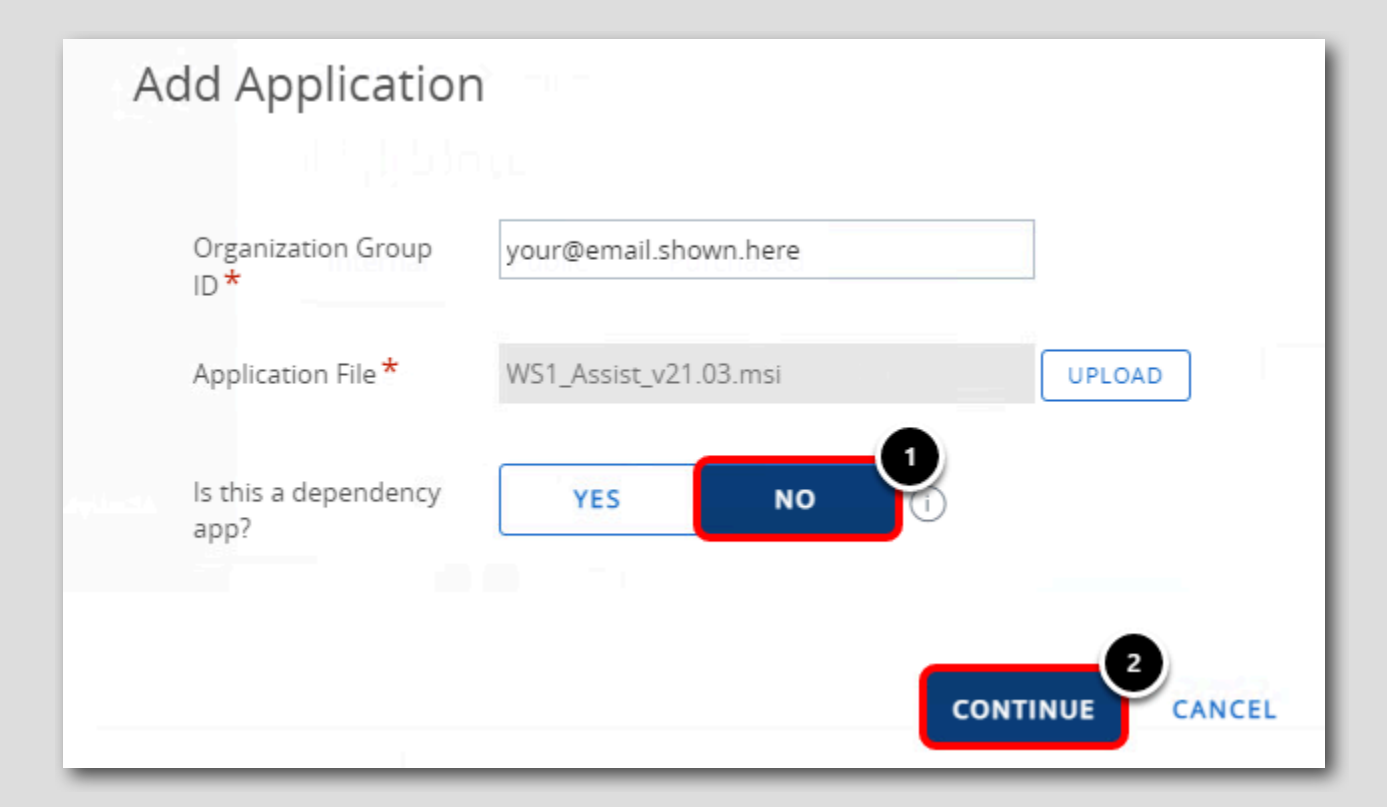


[Save] をクリックします。

注： MSI のアップロードには 1 ～ 2 分かかることがあります。

アプリケーションの設定に進む

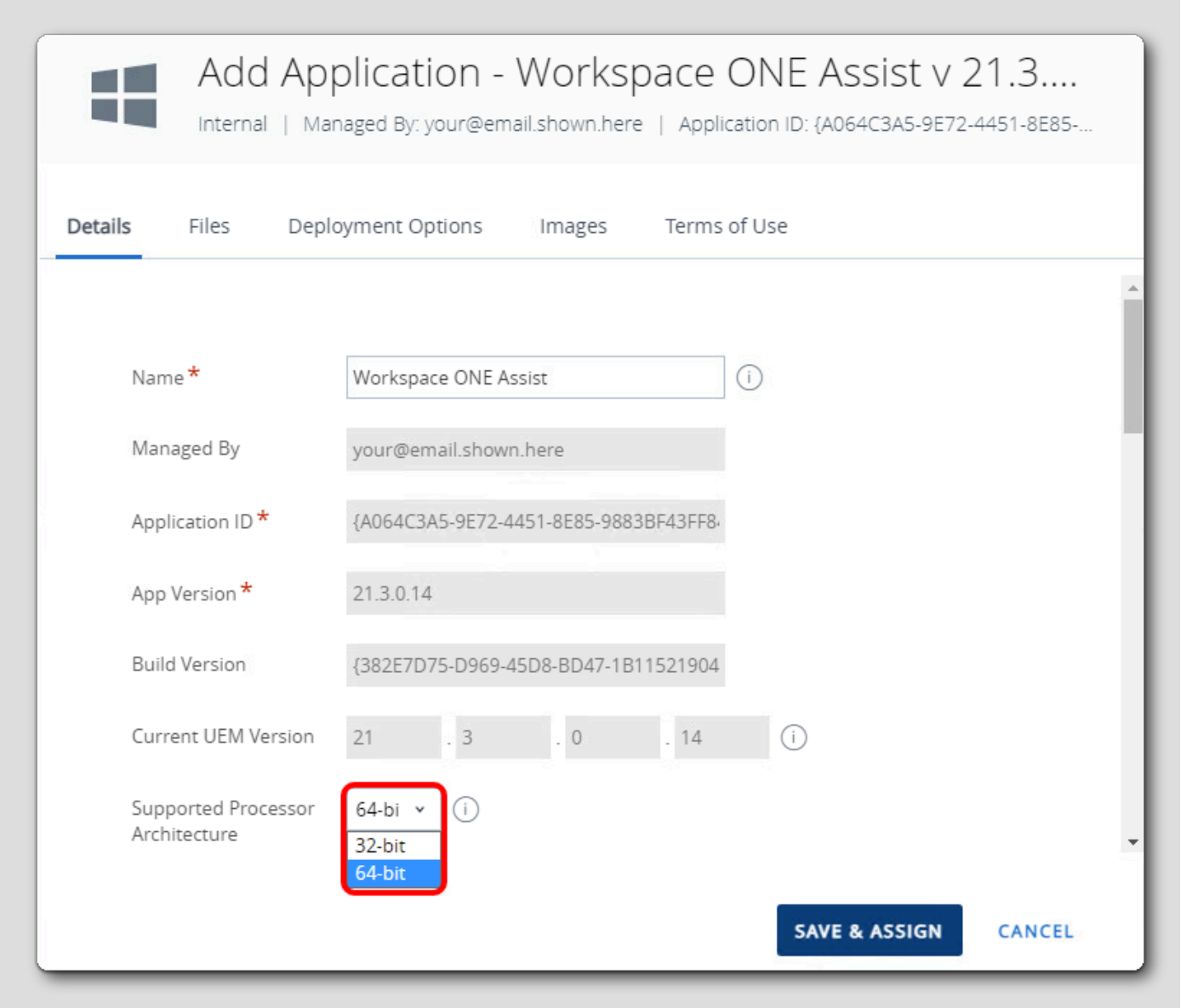
[183]



1. [Is this a dependency app?] に対して [No] をクリックします。
2. [Continue] をクリックします。

アプリケーションの詳細の設定

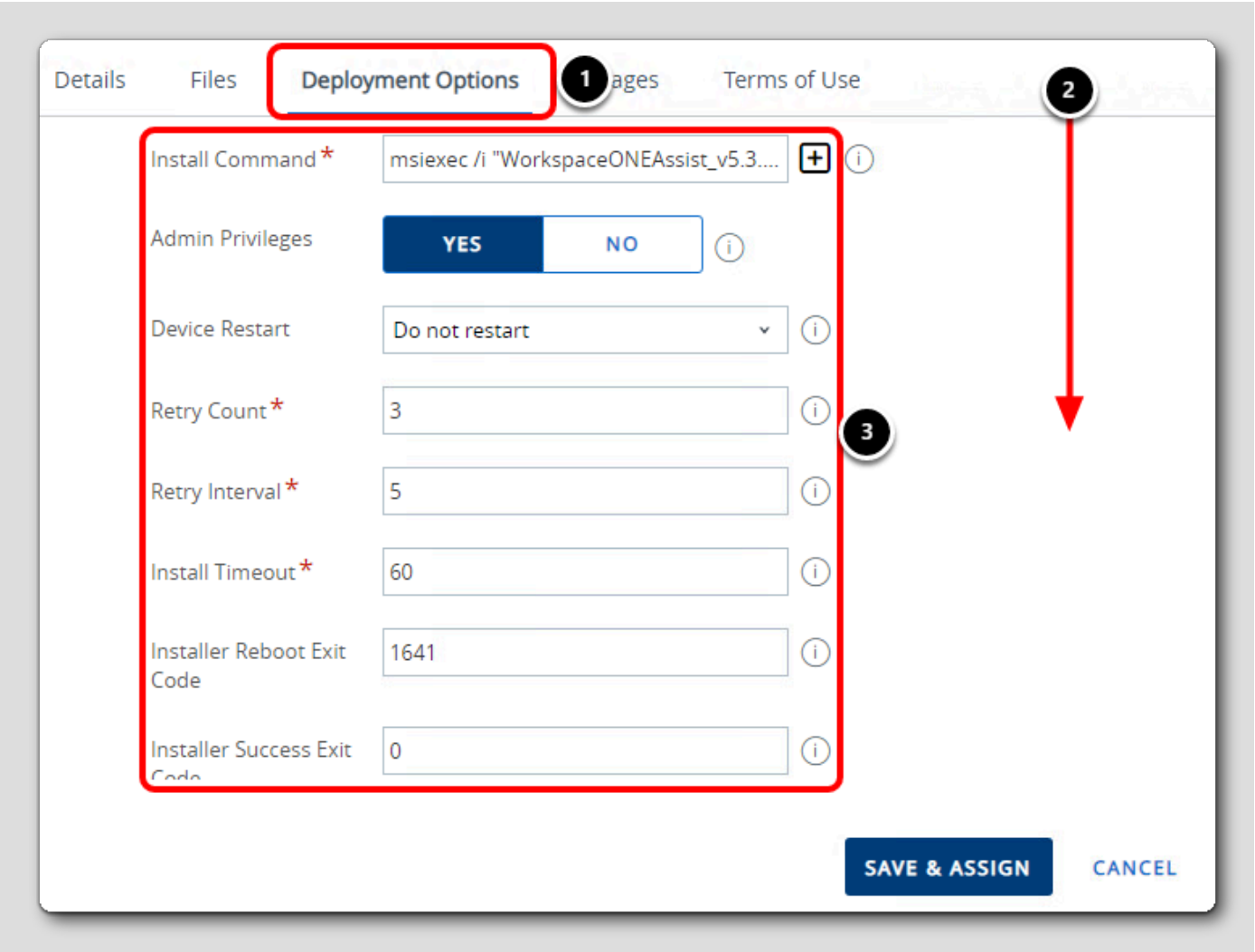
[184]



[Supported Processor Architecture] に対して [64-bit] を選択します。

展開オプションの確認

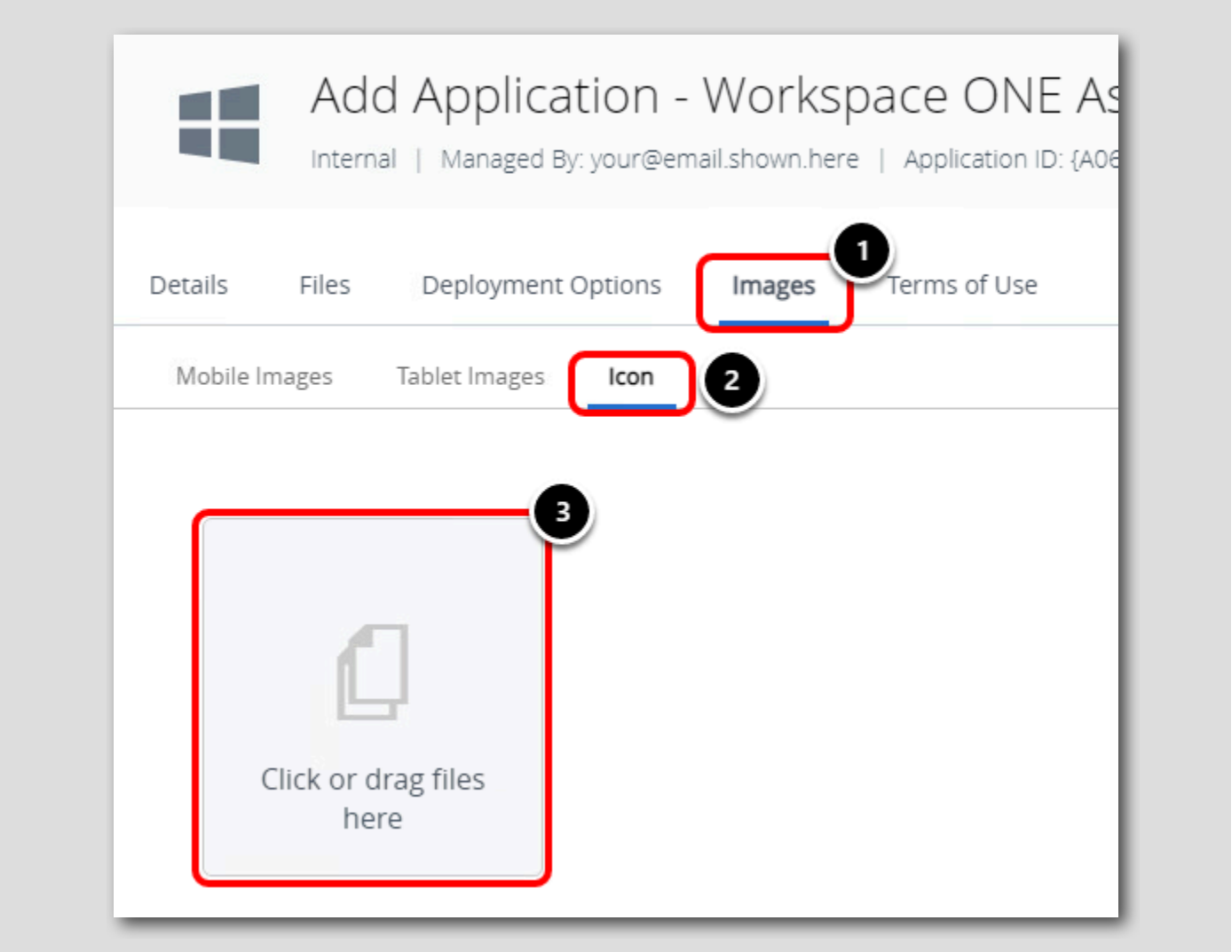
[185]



1. [Deployment Options] タブを選択します。
2. 下にスクロールして、[How To Install] セクションを見つけます。
3. 前の EXE ファイルを使用する場合と異なり、[Install Command] およびインストーラ コードが MSI 内の詳細から自動的に入力されたことに注意してください。

アプリケーション イメージの追加

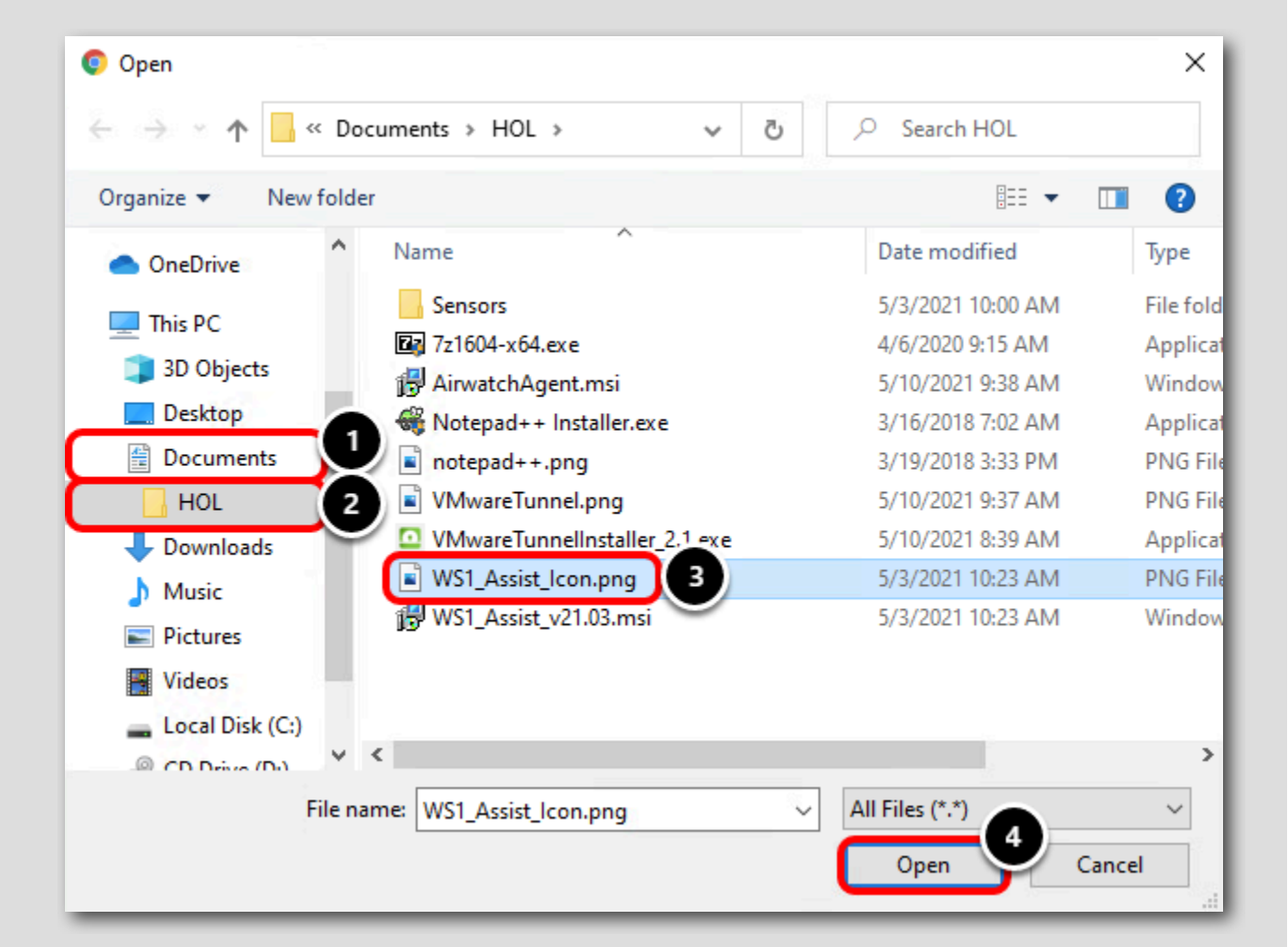
[186]



1. [Images] タブをクリックします。
2. [Icon] タブをクリックします。
3. [Click or drag files here] というラベルの付いた領域をクリックします。

Workspace ONE Assist アイコンのアップロード

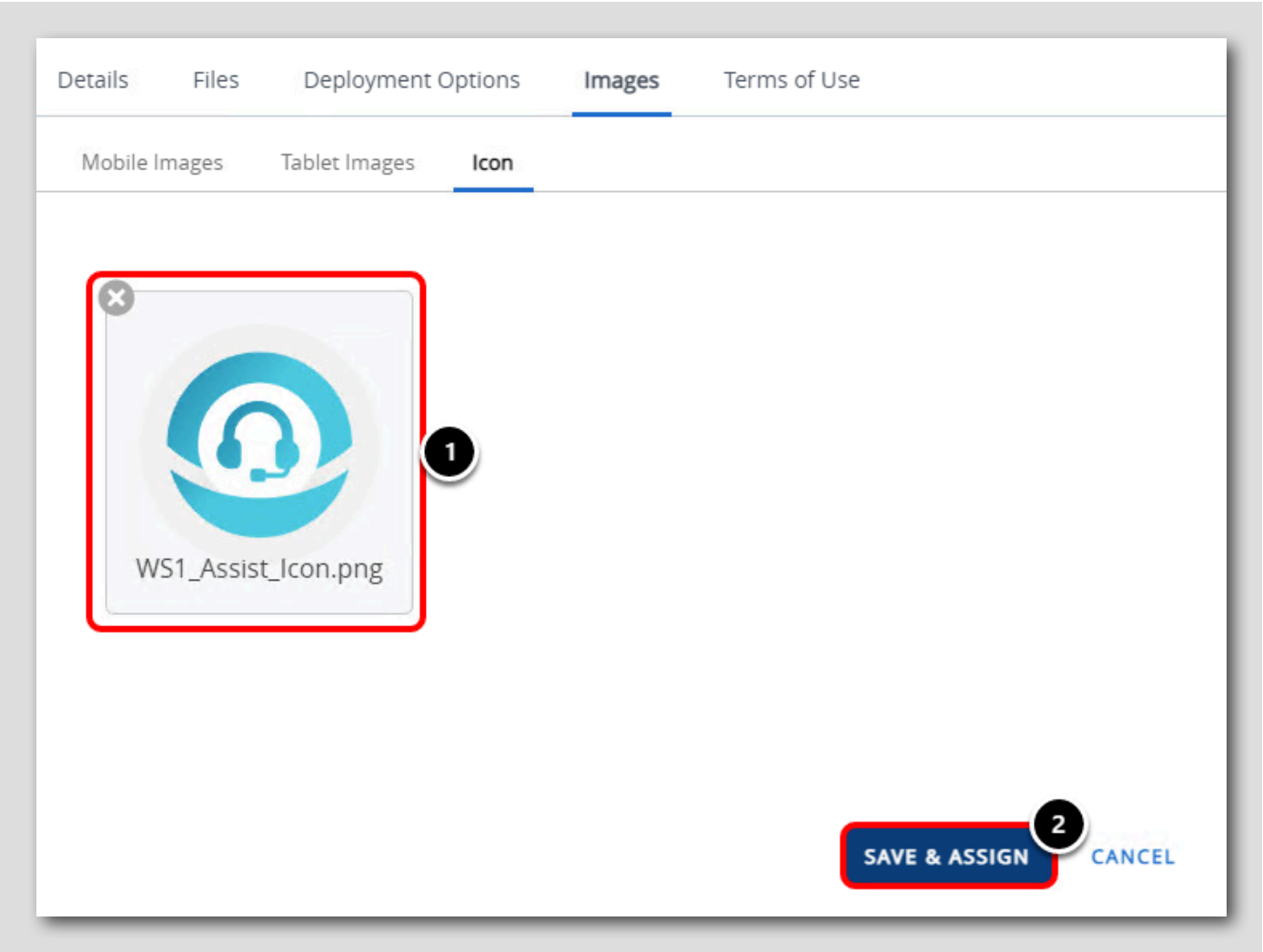
[187]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [WS1_Assist_Icon.png] をクリックして選択します。
4. [Open] をクリックします。

[Save and Assign] に進む

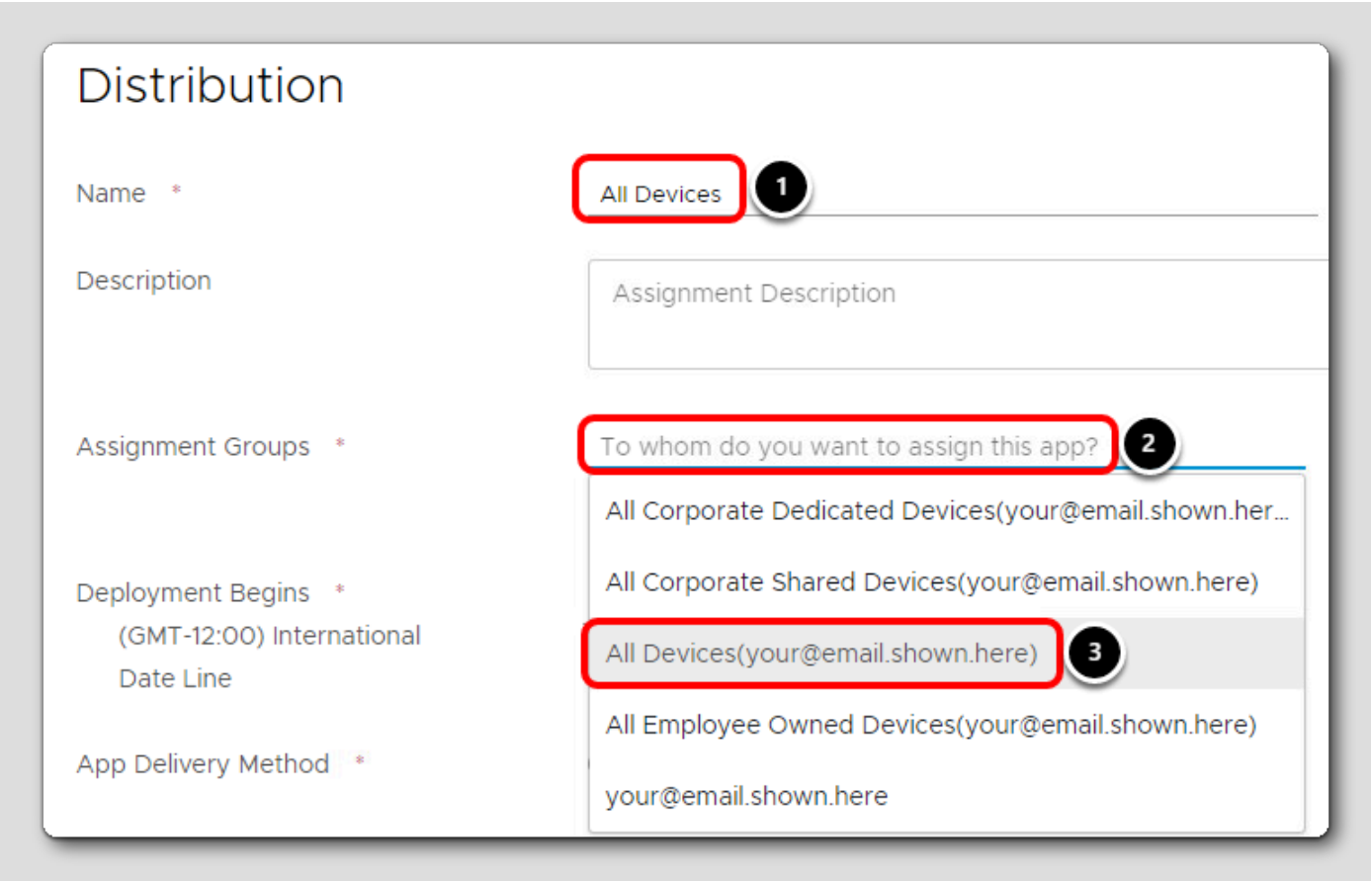
[188]



1. Workspace ONE Assist アイコンが正常にアップロードされたことを確認します。
2. [Save & Assign] をクリックします。

アプリケーションの保存と割り当て

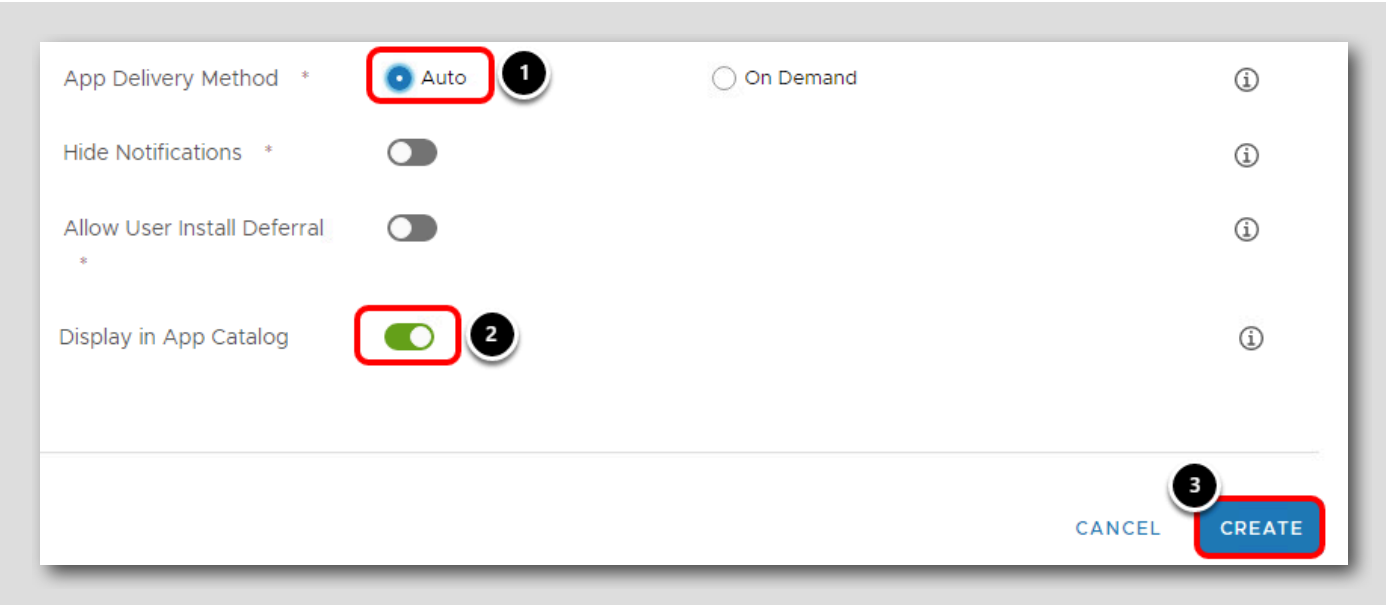
[189]



1. 配布名に **`All Devices`** と入力します。
2. [Assignment Groups] フィールドをクリックします。
3. [All Devices (your@email.shown.here)] グループを選択します。

アプリケーション配信方法の構成

[190]

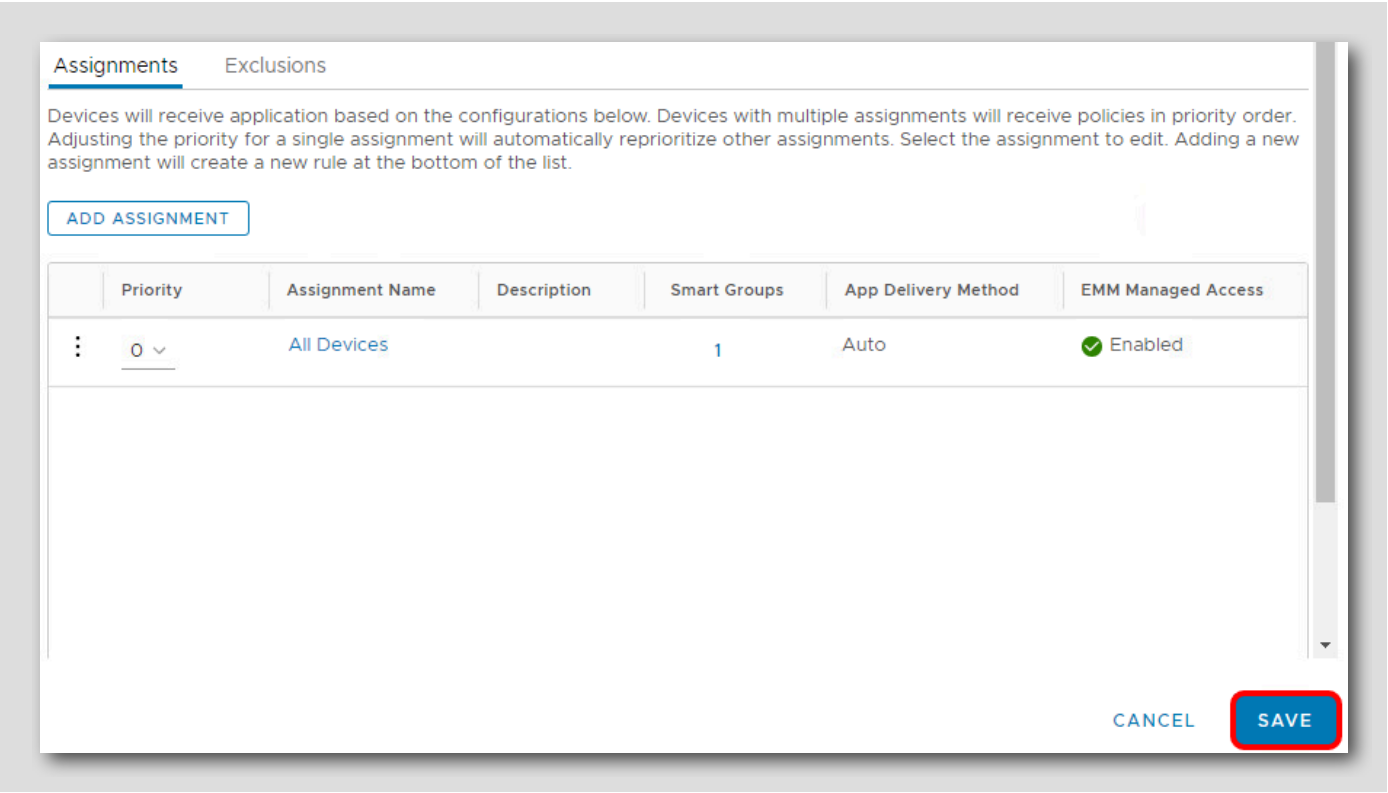


1. [App Delivery Method] に対して [Auto] を選択します。これにより、ユーザーのアプリケーションが自動的に展開されてインストールされるので、アプリケーション カタログを使用せずにすぐに利用できるようになります。
2. [Display in App Catalog] 設定を有効にします。
3. [Create] をクリックします。

注：アプリケーション カタログにアプリケーションを表示するかどうかを選択できるようになりました。これは、ドライバの更新またはスクリプト化されたアクションを展開し、エンド ユーザーがカタログでこれを表示できないようにする場合に役立ちます。

割り当ての保存

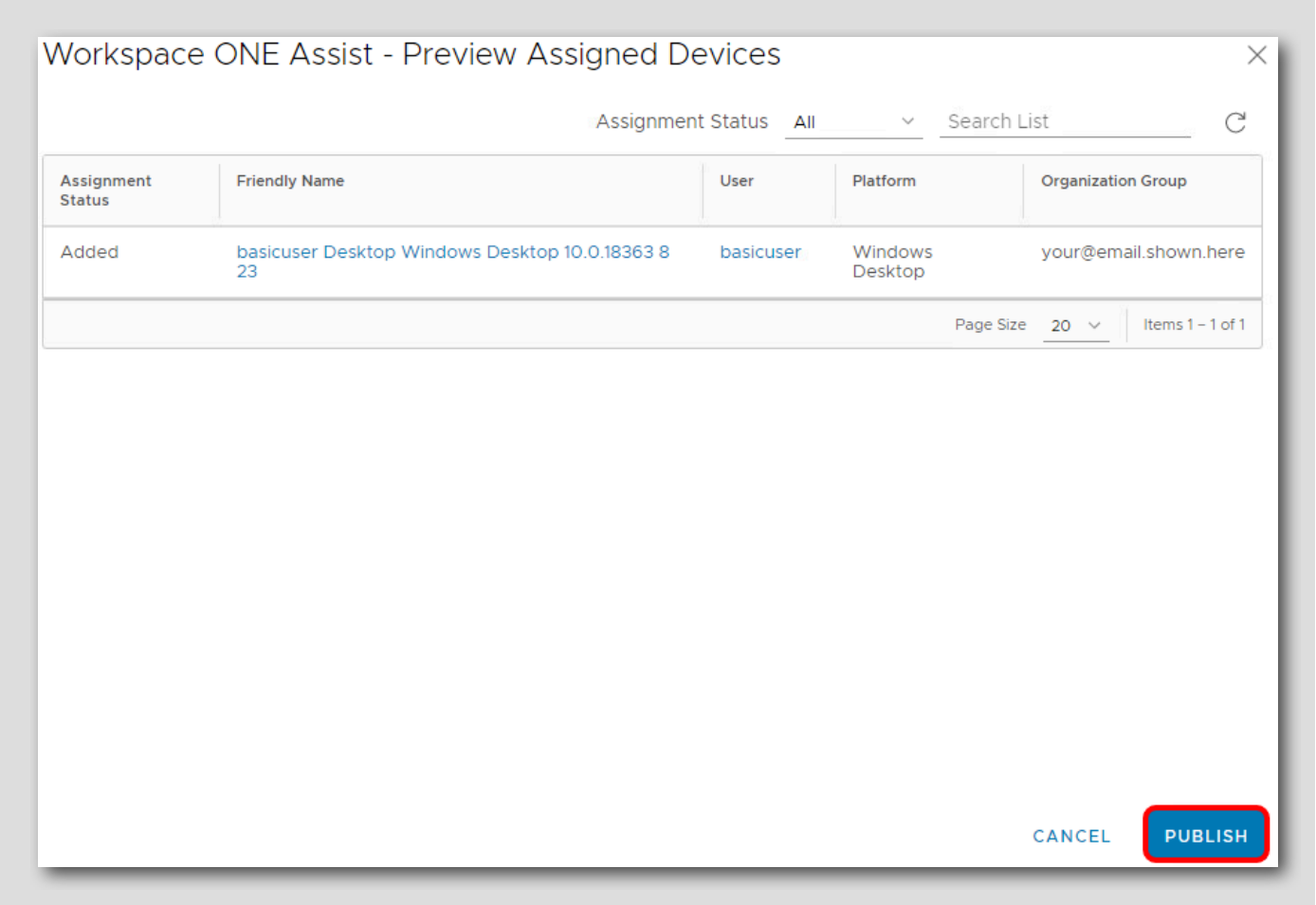
[191]



[Save] をクリックしてアプリケーションの割り当てを保存します。

アプリケーションの公開

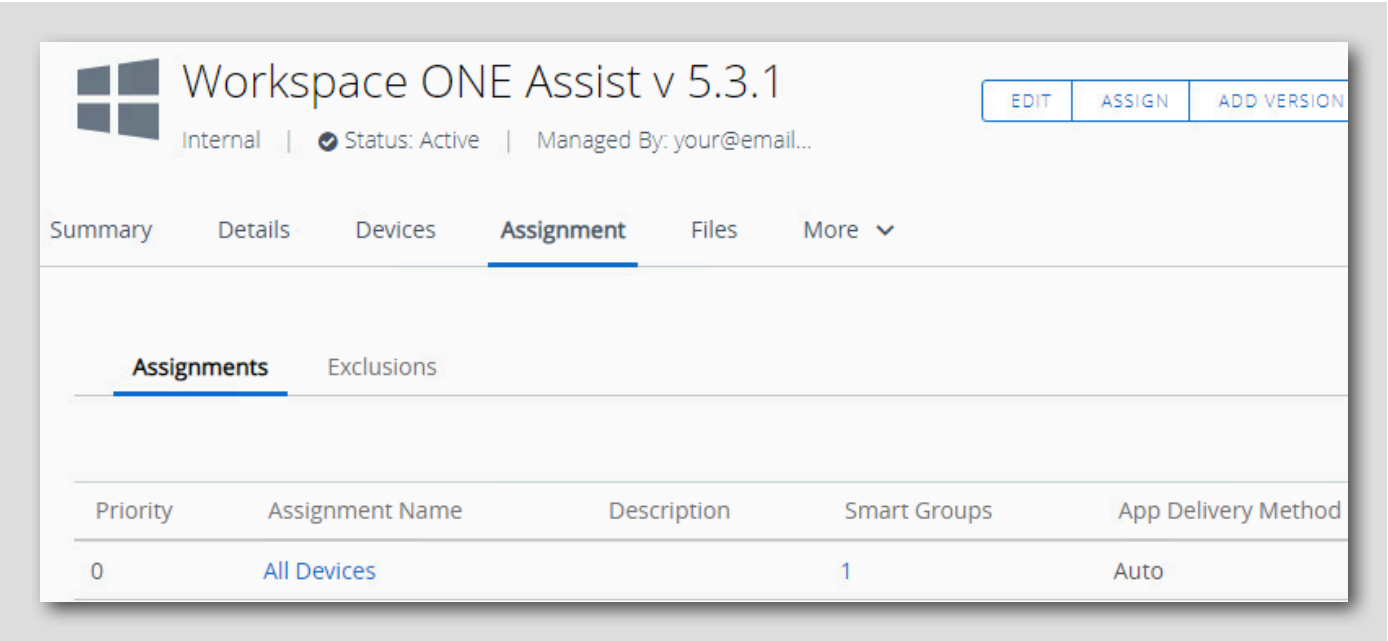
[192]



[Publish] をクリックして、表示されているデバイスのリストにアプリケーションを公開します。

アプリケーション作成の確認

[193]



Workspace ONE Assist アプリケーションが作成され、[All Devices] スマート グループに割り当てられ、[App Delivery Method] が [Auto] に設定されています。つまり、Windows 10 デバイスが組織に登録されている場合、ユーザーの操作を必要とせずに、アプリケーションが自動的にダウンロードおよびインストールされます。

次の手順に進んでください。

デバイス登録の確認

[194]

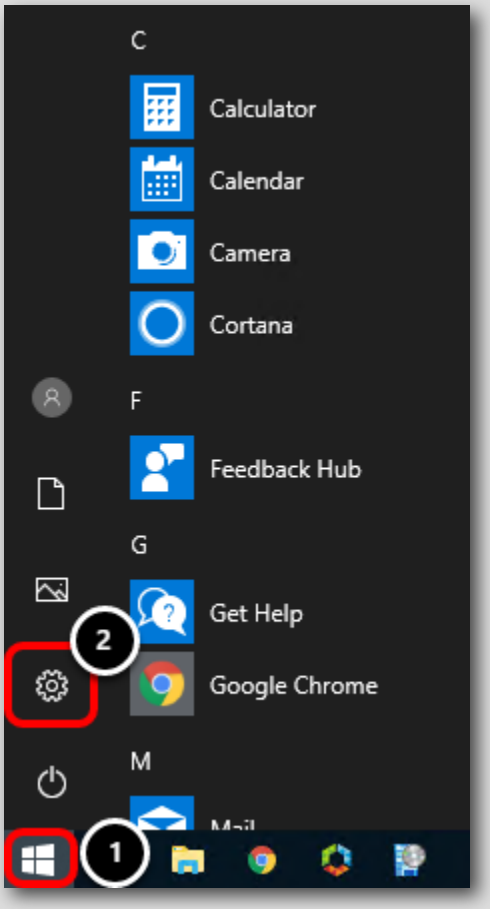
デバイスが登録済みで、次の 3 つの構成を受け取りました。

1. エンド ユーザーが Windows 10 デバイスを登録解除できないようにする制限事項プロファイル
2. 7-Zip アプリケーションが On Demand アプリケーションとして展開されました
3. Workspace ONE Assist アプリケーションが Auto アプリケーションとして展開されました

ここで、制限事項がデバイスに適用されていること、および 2 つのアプリケーションが展開の種類（「On Demand」と「Auto」）に応じて利用可能であることを確認することで、制限事項プロファイルがインストールされたことを確認します。

新しい登録解除設定の確認

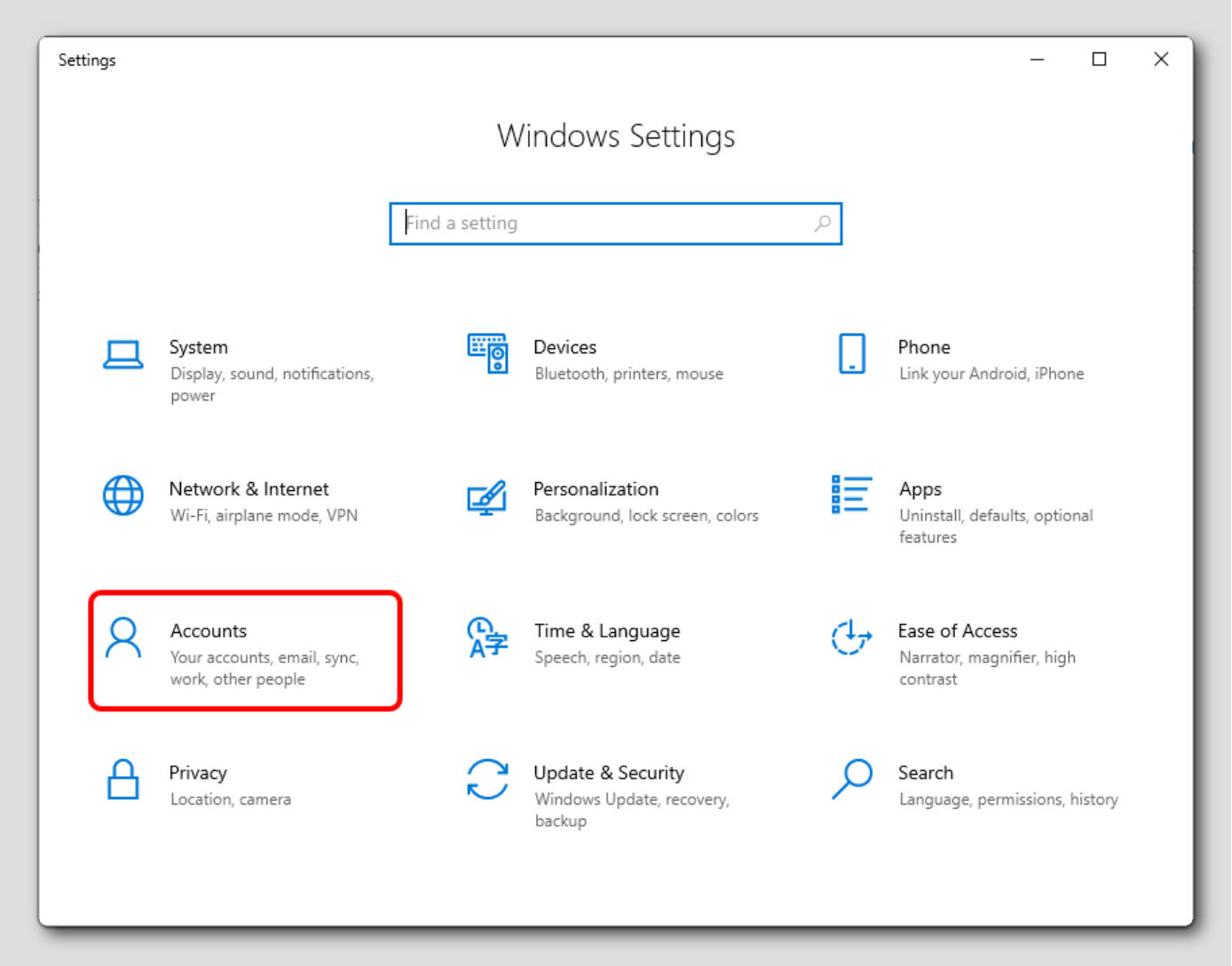
[195]



1. Windows の [Start] ボタンをクリックします。
2. Windows の [Settings] ボタンをクリックします。

アカウント

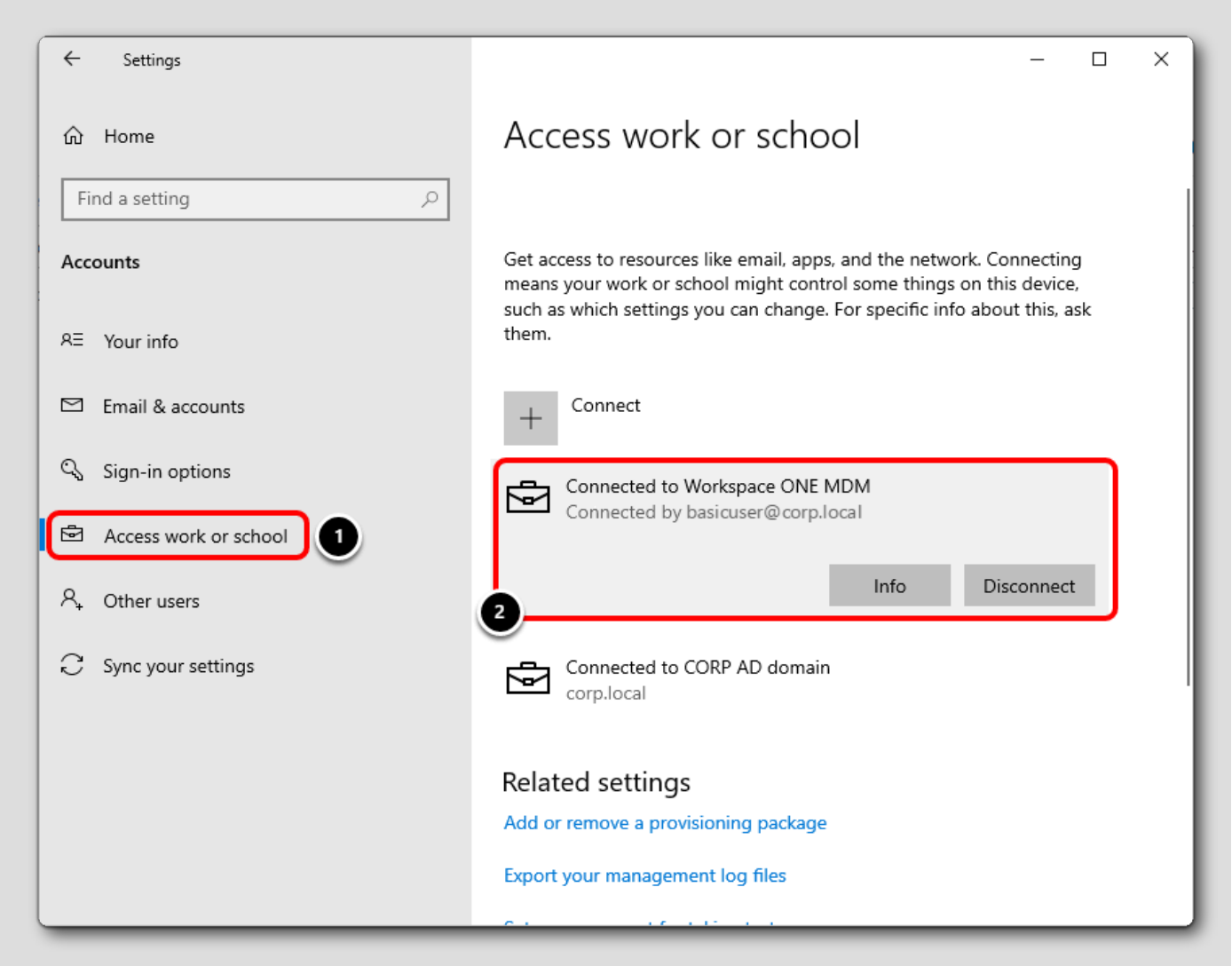
[196]



[Accounts] をクリックします。

職場または学校にアクセス

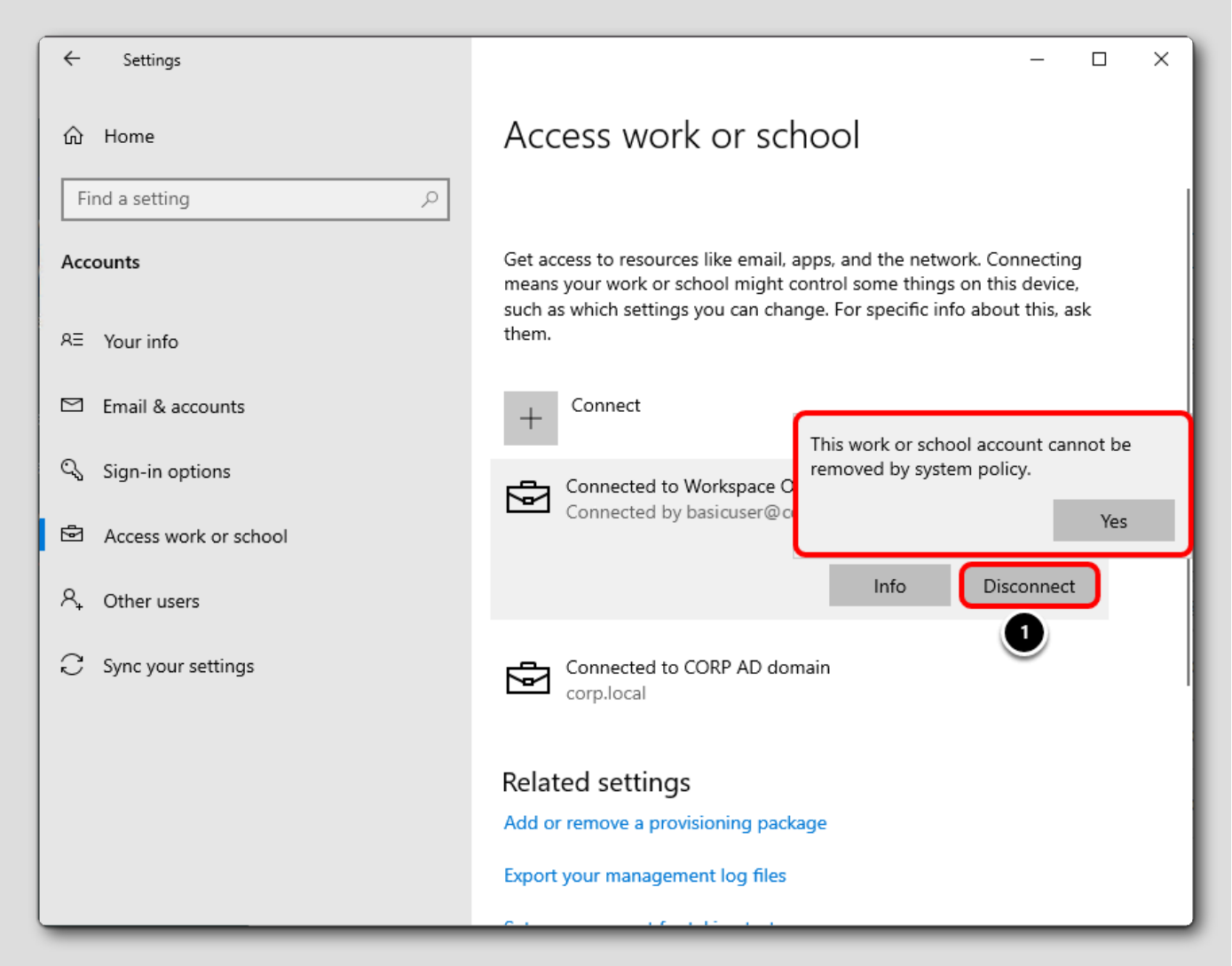
[197]



1. [Access work or school] をクリックします。
2. [Connected to Workspace ONE MDM] をクリックします。

エンドユーザーは登録解除できません

[198]

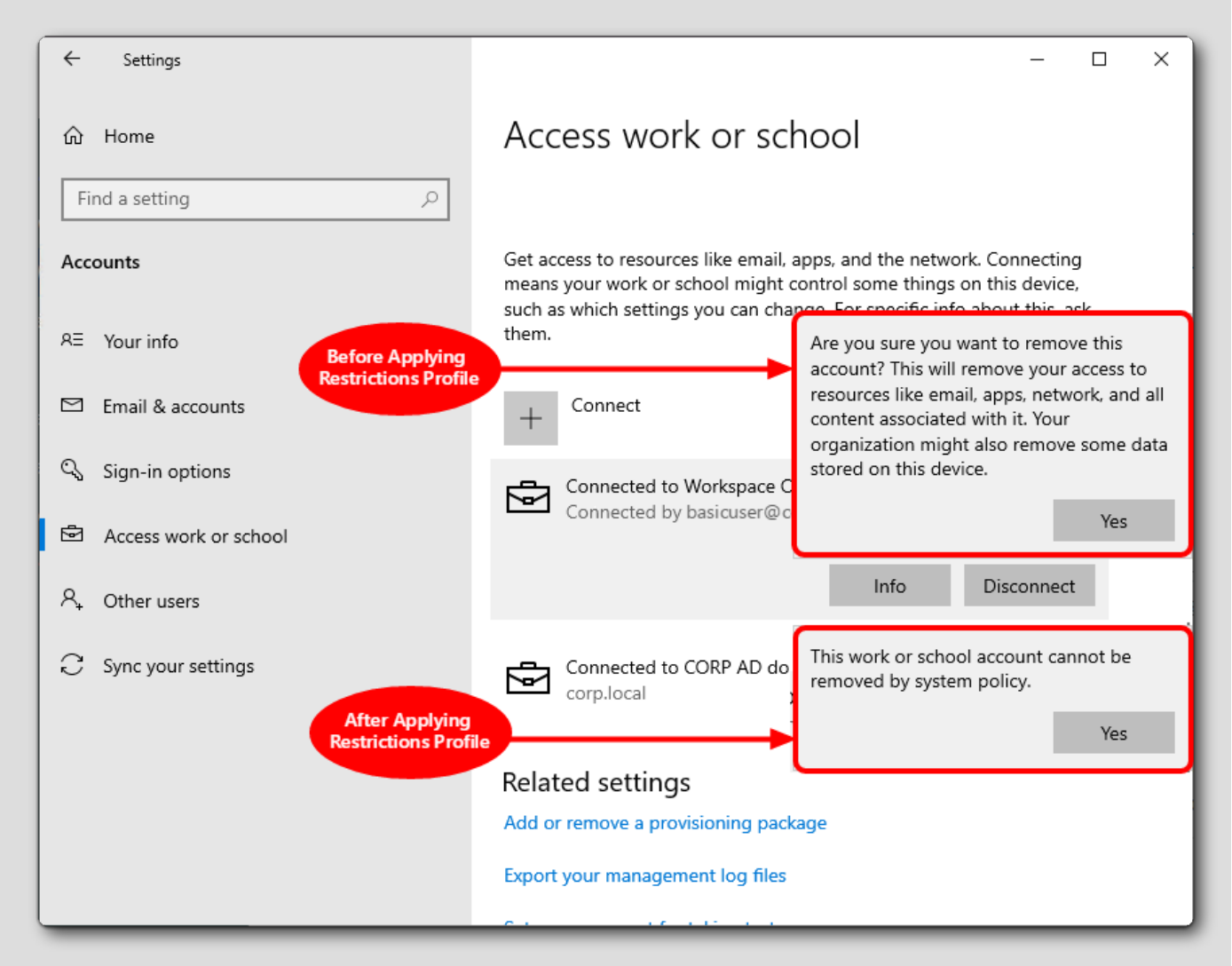


1. [Disconnect] をクリックします。

エンド ユーザーが Workspace ONE UEM 管理からデバイスを登録解除できないことを確認します。

制限事項の適用の前と後

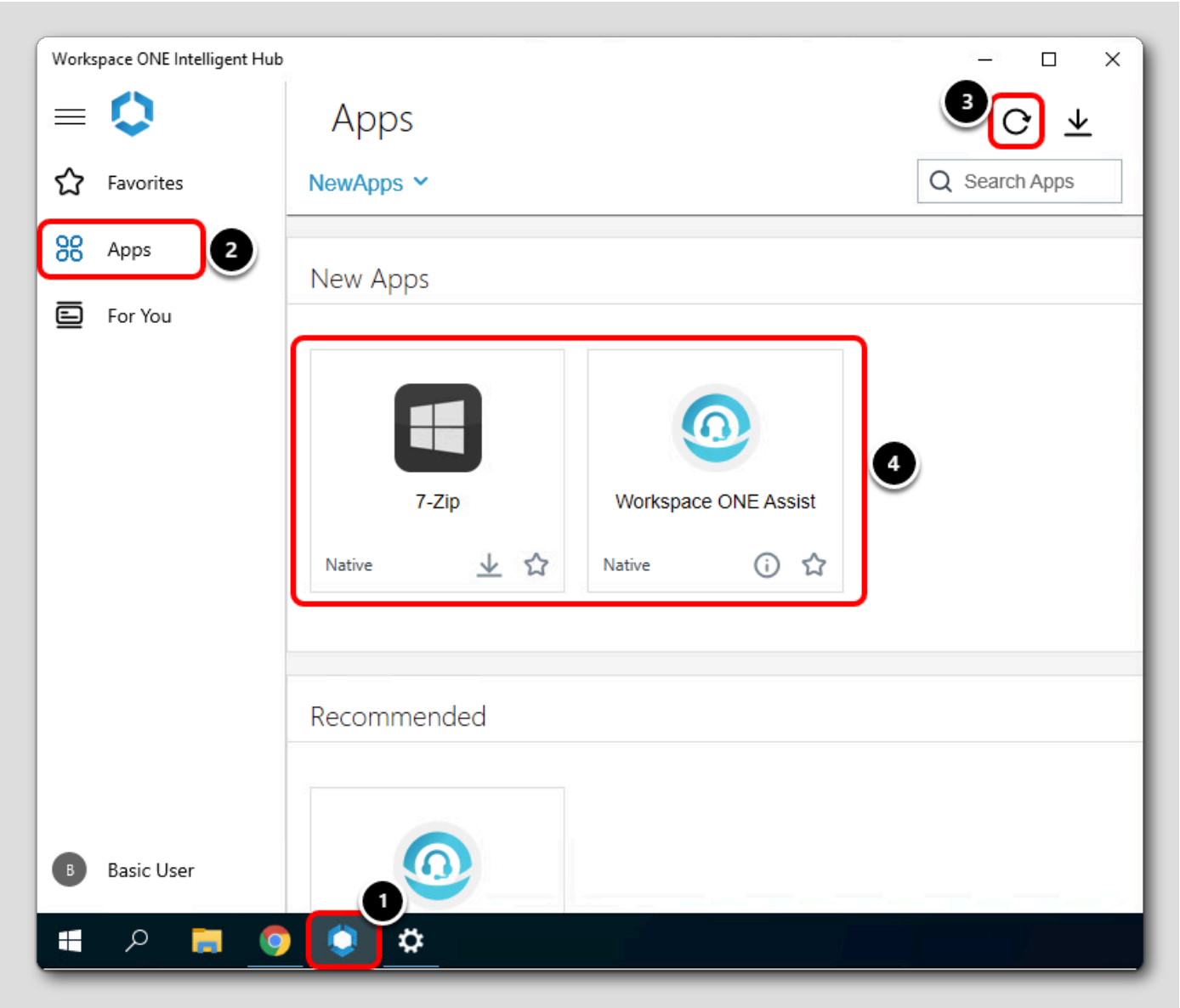
[199]



ここでは、Windows 10 デバイスで [Allow MDM Unenrollment] または [Don't Allow MDM Unenrollment] ポリシーを適用する前と後の結果を確認できます。

アプリケーションの確認

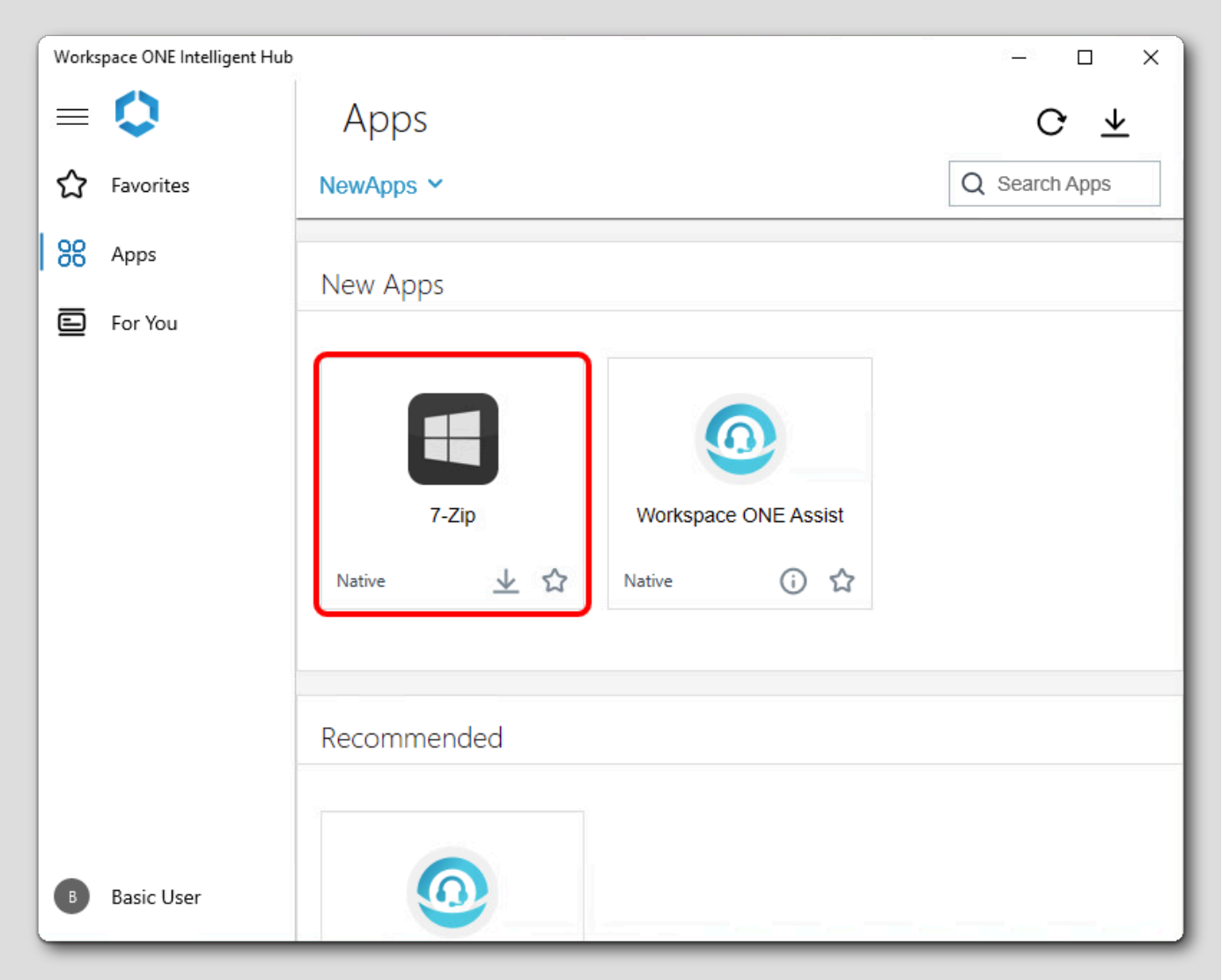
[200]



1. タスク バーから [Workspace ONE Intelligent Hub app] をクリックします。
2. [Apps] タブをクリックして、アプリケーション カタログを表示します。
3. [Refresh] をクリックして、利用可能になった新しいアプリケーションを表示します。
4. [7-Zip] と [Workspace ONE Assist] アプリケーションの両方が [New Apps] セクションに表示されていることを確認します。

7-Zip アプリケーションのインストール

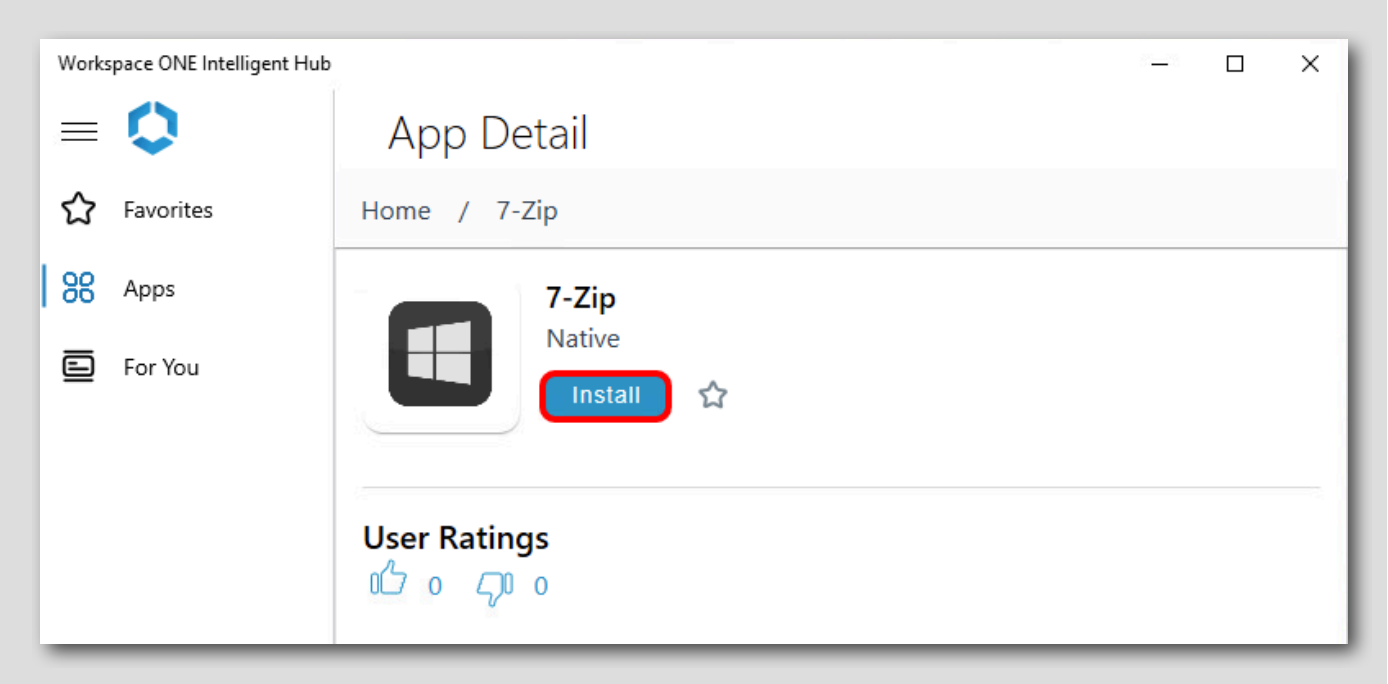
[201]



[7-Zip] アプリケーションをクリックします。

7-Zip インストールの開始

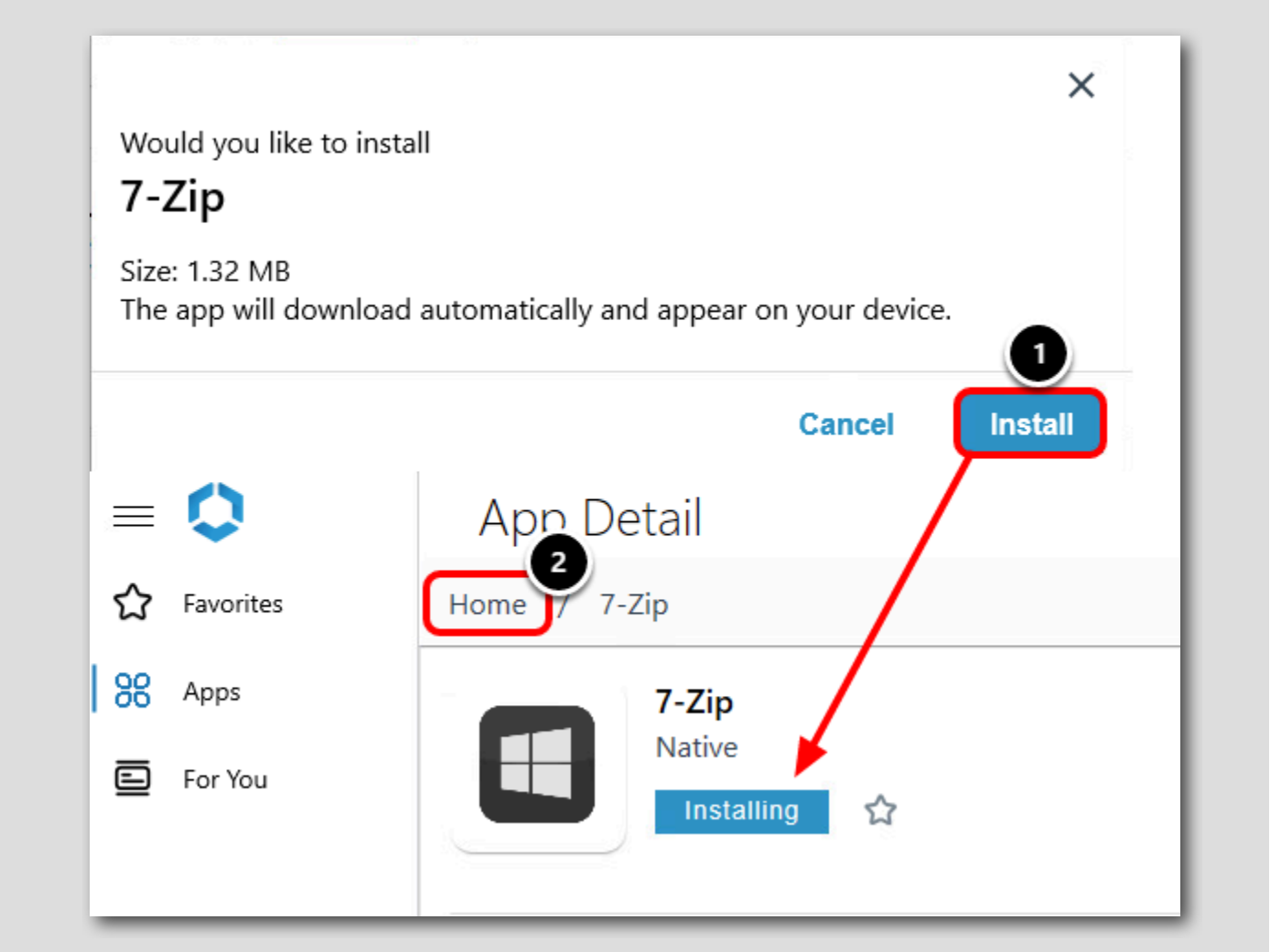
[202]



[Install] をクリックします。

インストールの確認

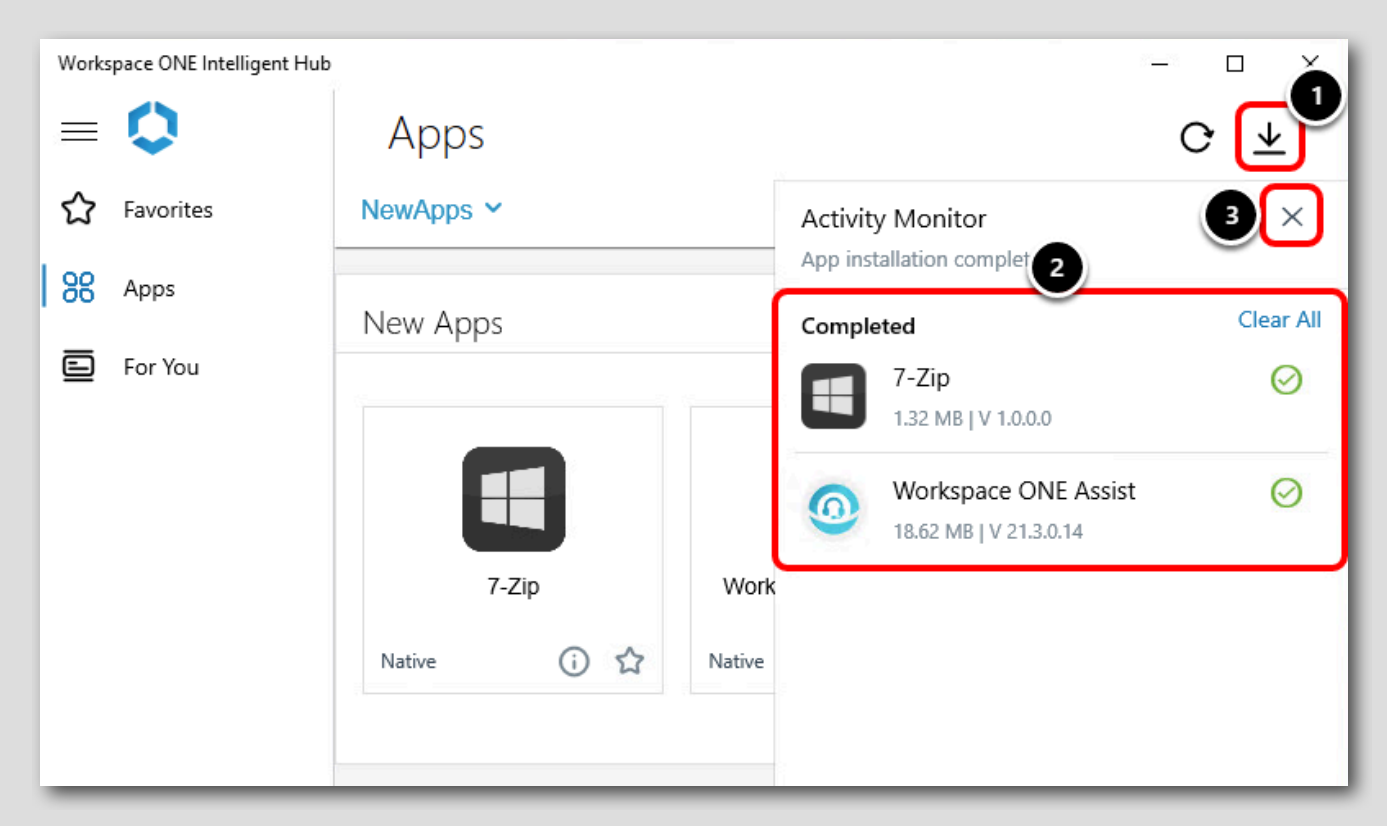
[203]



1. ポップアップに対して [Install] をクリックします。7-Zip アプリケーションのステータスが [Installing] に変わります。
2. [Home] をクリックして、アプリケーション カタログに戻ります。

インストールの監視

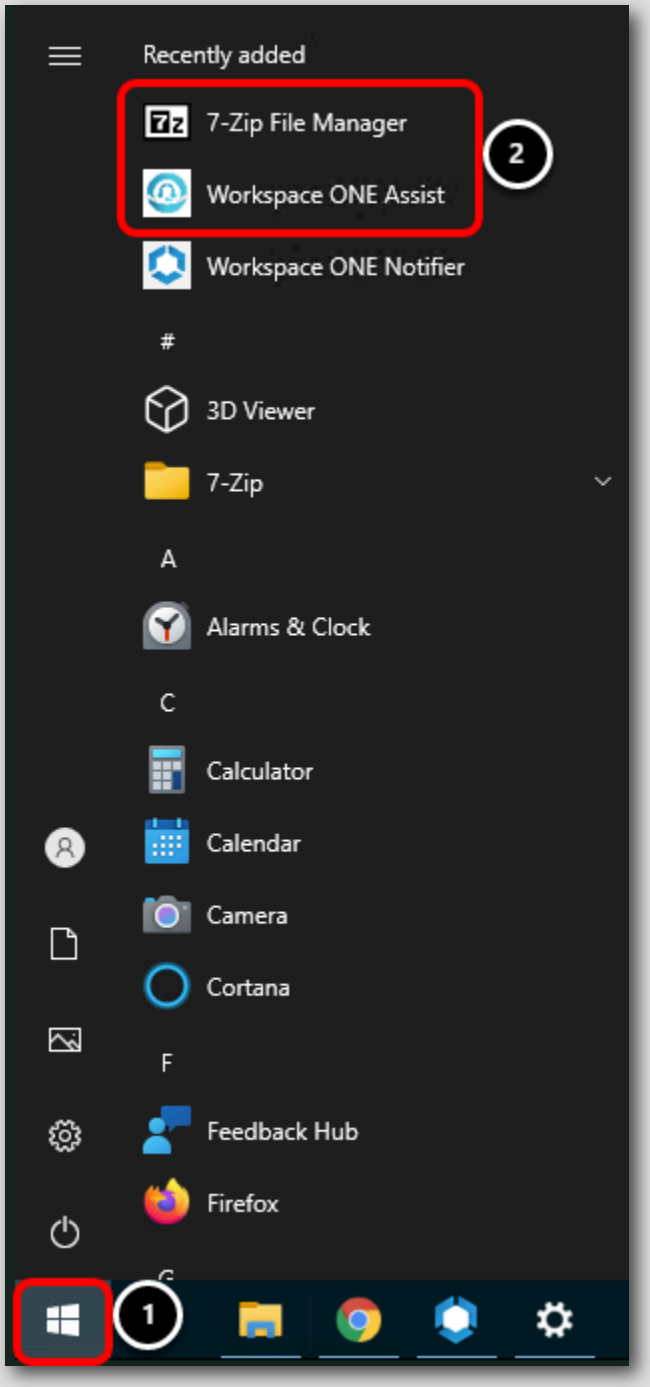
[204]



1. **[Downloads]** ボタンをクリックして、[Activity Monitor] を開きます。
2. [Activity Monitor] を使用すると、アプリケーションのダウンロードの進行状況と完了したかどうかを確認できます。7-Zip と Workspace ONE Assist の両方のインストールが完了するまで待ってから、次の手順に進みます。
3. **[X]** をクリックして [Activity Monitor] を閉じます。

アプリケーション インストールの確認

[205]



1. [Windows] ボタンをクリックします。
2. [Recently Added] セクションに [7-Zip] と [Workspace ONE Assist] の両方が表示されていることを確認します。必要に応じてアプリケーションを起動してから、次の手順に進みます。

検証のまとめ

[206]

制限事項プロファイルが意図したとおりにデバイスに適用されたこと、また、使用可能になった 2 つのアプリケーション（Workspace ONE Assist と 7-Zip）がアプリケーション カタログからユーザーに提示され、正常にインストールされたことを確認できました。

Windows 10 デバイスの登録解除

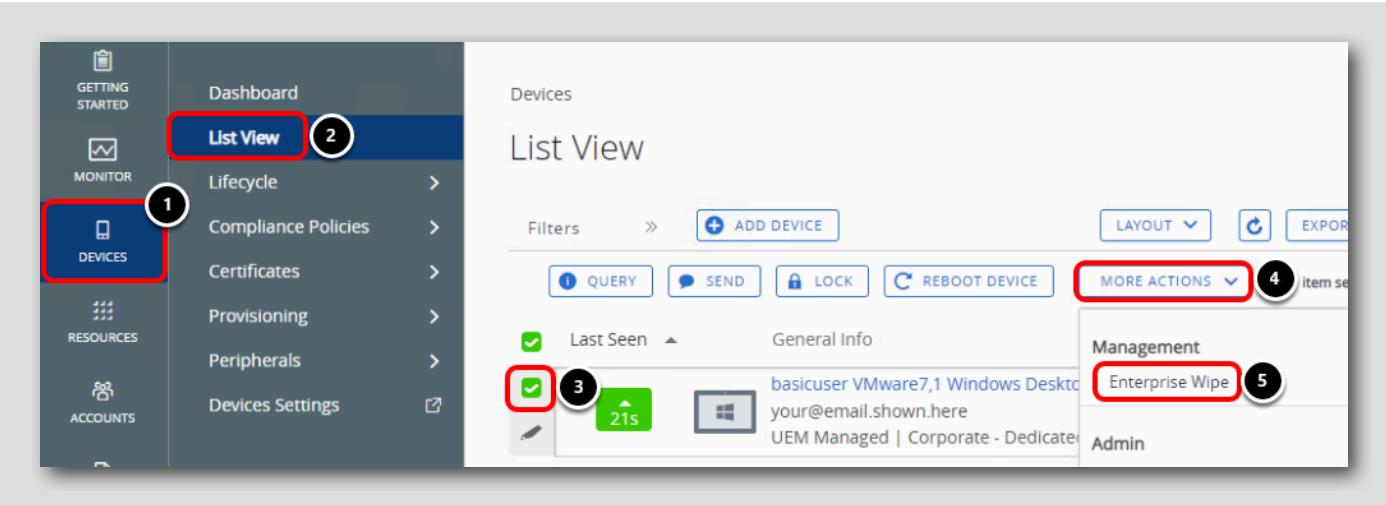
[207]

このセクションでは、Windows 10 仮想マシンの登録を解除して、他のラボ モジュールで使用できるようにします。

Enterprise Wipe ワイプ コマンドを使用して、Workspace ONE によってデバイスにプッシュされたすべての管理対象コンテンツ（プロファイルやアプリケーションなど）を削除しますが、デバイス上の個人的なコンテンツやデータは変更しません。

Workspace ONE UEM Console からの企業情報ワイプ

[208]

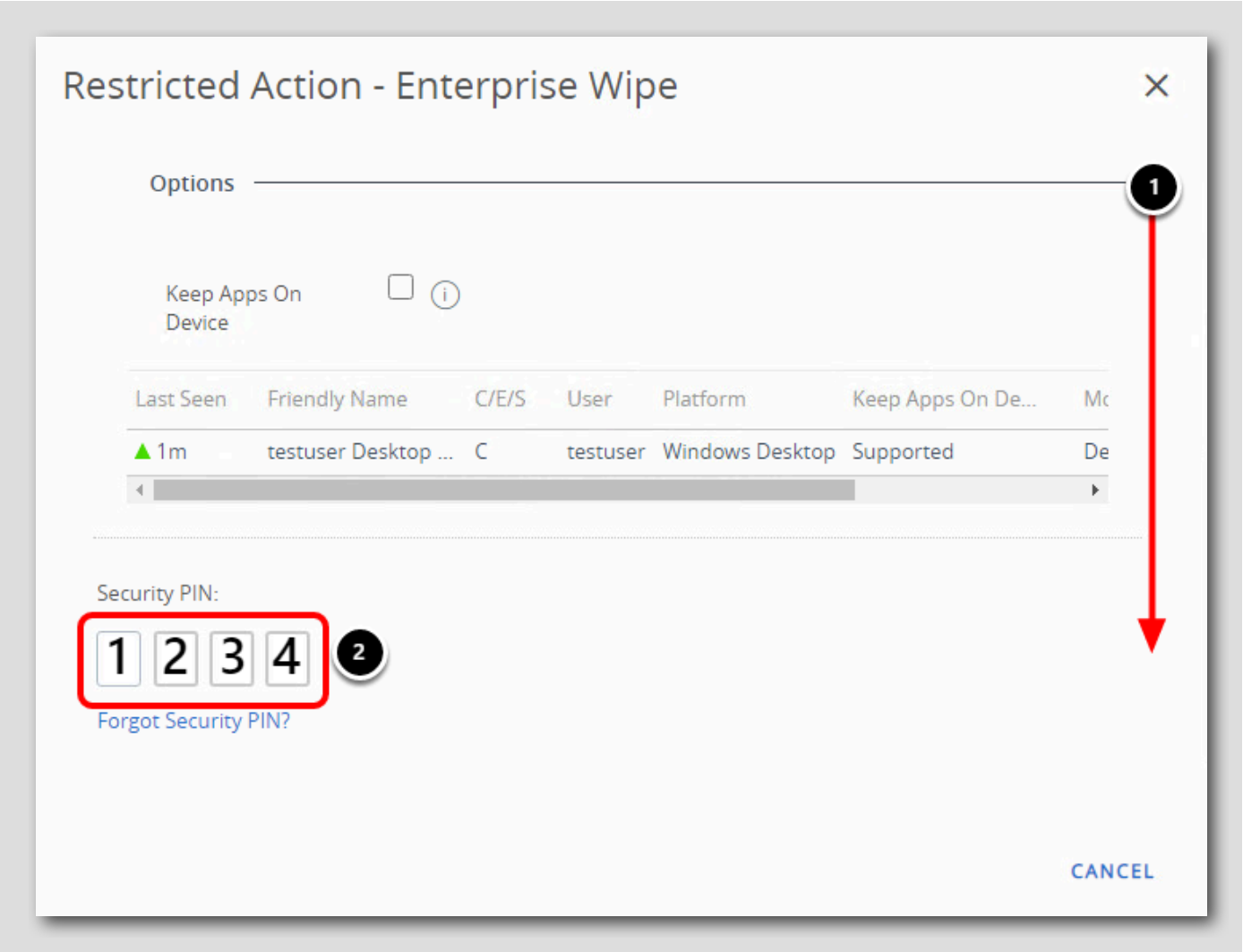


Google Chrome で Workspace ONE UEM 管理者コンソールに戻ります。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. デバイスのフレンドリ名の横にあるチェックボックスを選択します。
4. [More Actions] をクリックします。
5. [Enterprise Wipe] をクリックします。

PIN の入力とデバイスの企業情報ワイプ

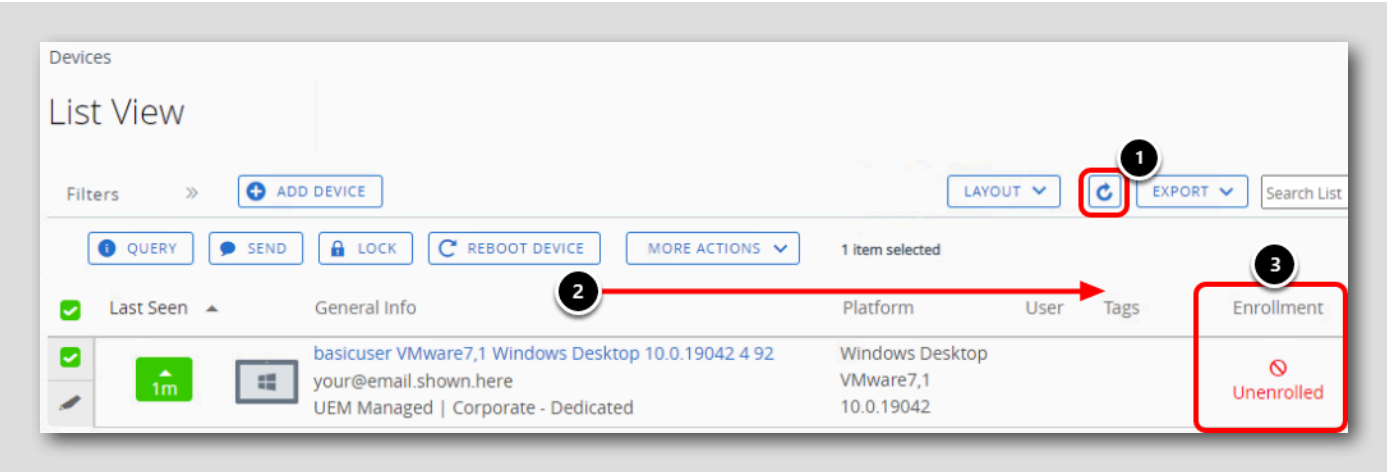
[209]



1. [Security PIN] 入力を見つけるために、下にスクロールする必要がある場合があります。
2. Workspace ONE UEM 管理コンソールに初めてログインしたときに作成したセキュリティ PIN (**1234**) を入力します。別の PIN を使用した場合は、代わりにその PIN を入力します。
3. **[Delete]** をクリックします。

企業情報ワイプの検証

[210]

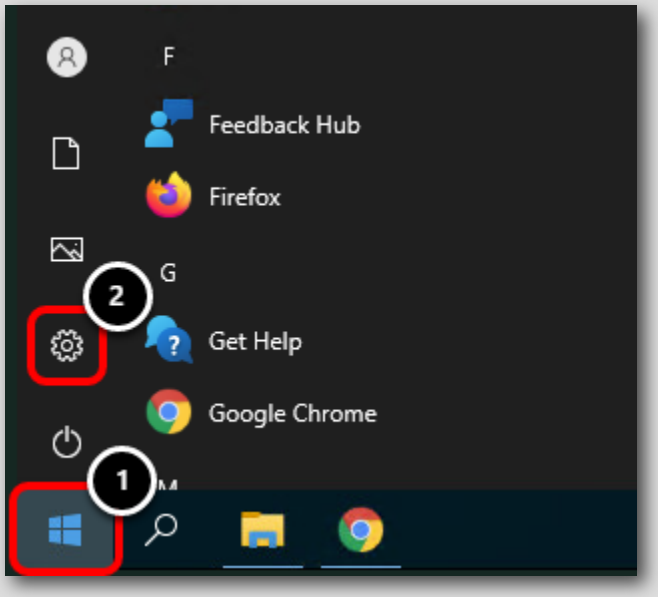


注：企業情報ワイプの処理には、数分かかる場合があります。

1. 更新アイコンを定期的にクリックしてページを更新し、企業情報ワイプが処理されたかどうかを確認します。
2. 必要に応じて、右にスクロールして [Enrollment] 列を見つけます。
3. 企業情報ワイプ コマンドが処理されると、デバイスの登録状態が [Unenrolled] に変わります。

[Windows 10 Settings] への移動

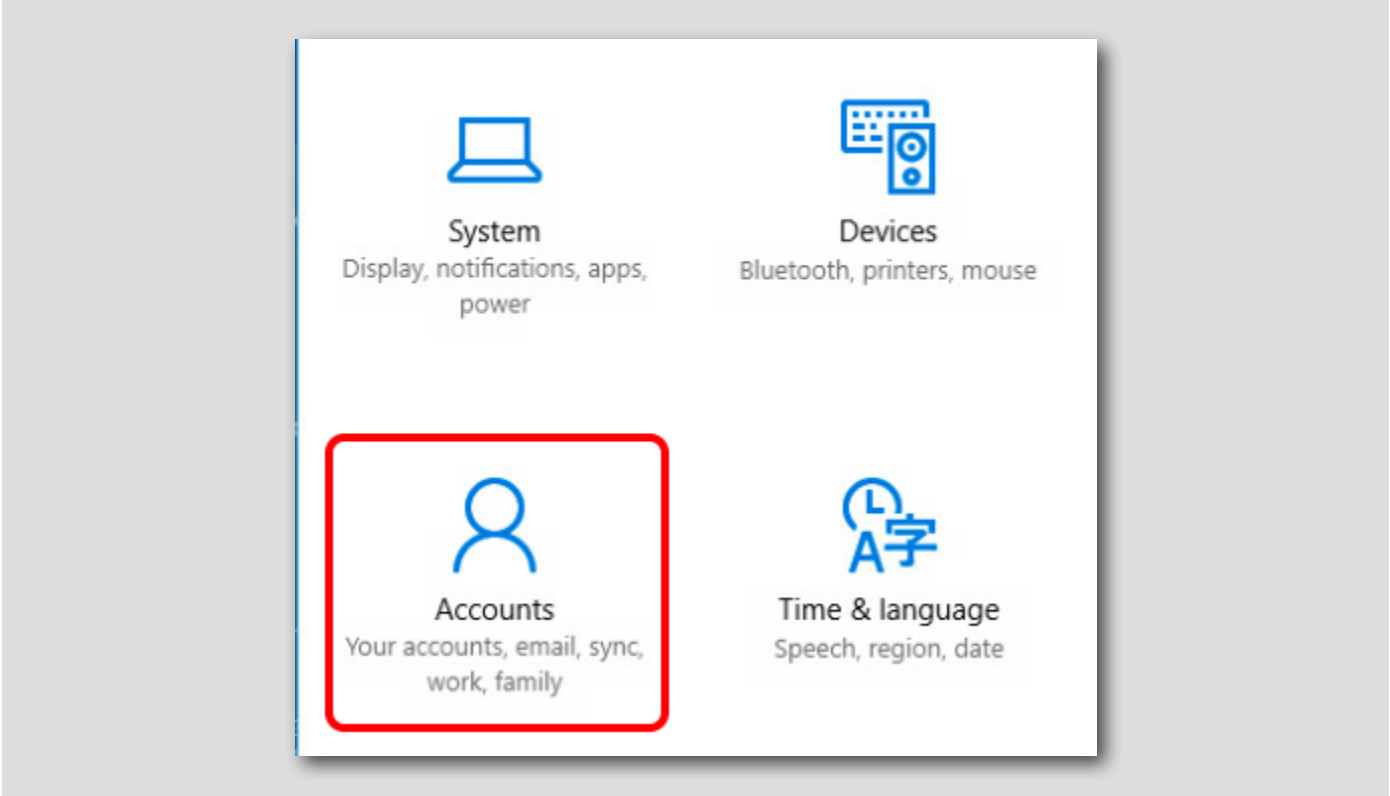
[211]



1. Windows アイコンをクリックします。
2. 歯車アイコンをクリックして、[Windows 10 Settings] にアクセスします。

[212]

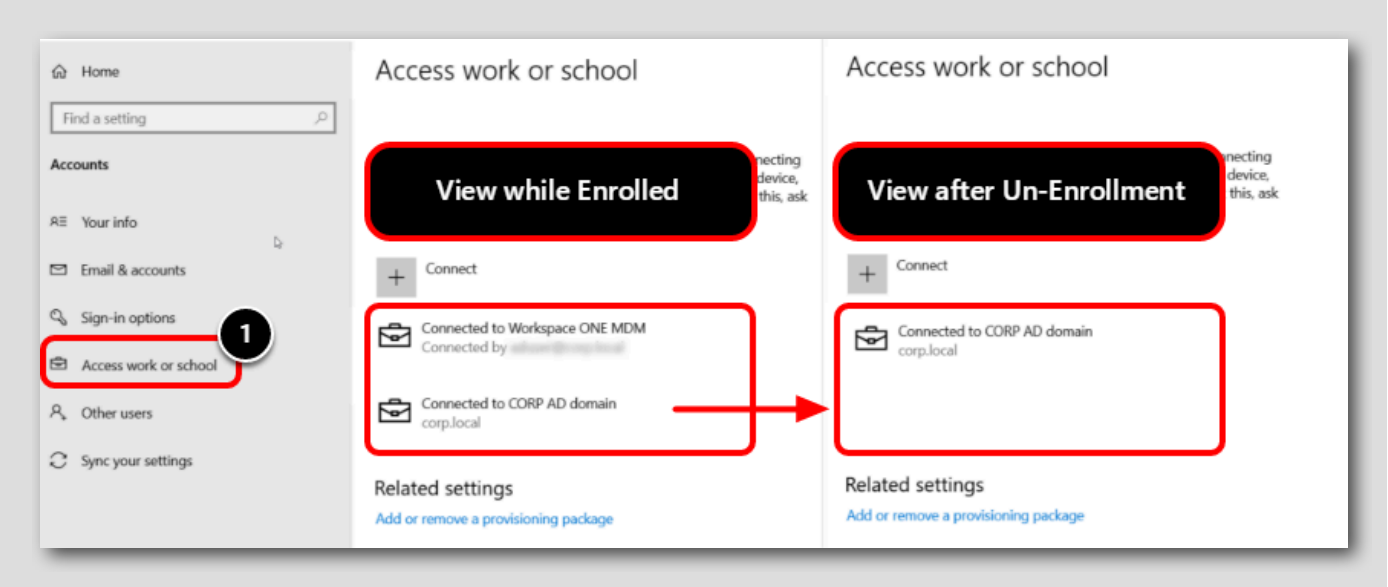
[Accounts] 設定へのアクセス



[Settings] メニューから **[Accounts]** にアクセスします。

管理アカウントが存在しないことの検証

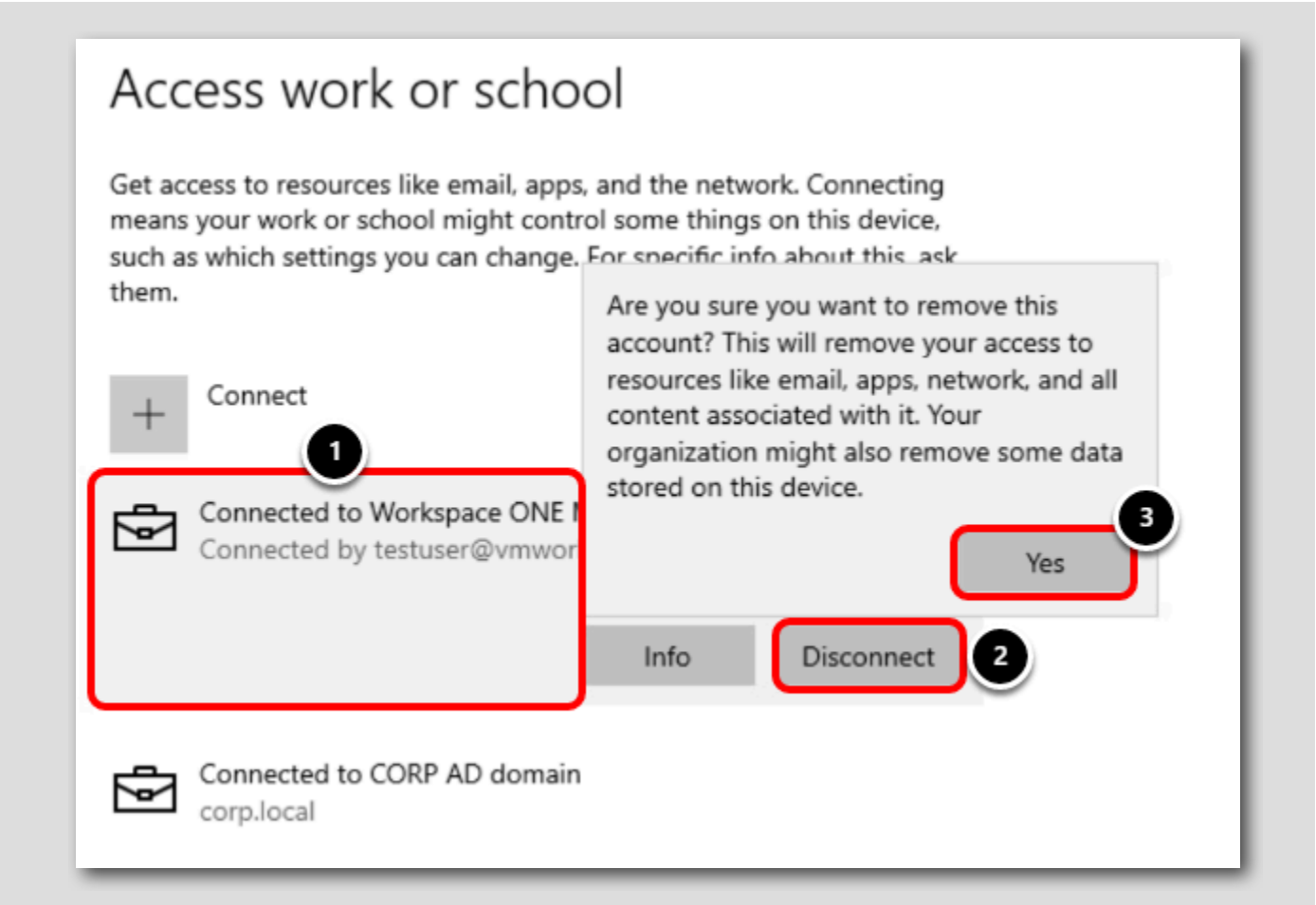
[213]



1. [Access work or school] をクリックします。
2. Workspace ONE MDM に接続されているアカウントがないことを確認します。

注：このラボでは、CORP AD ドメインはローカル ドメインであり、Workspace ONE UEM 登録によって管理されていないため、デバイスの登録時または登録解除時にこの接続が表示されます。

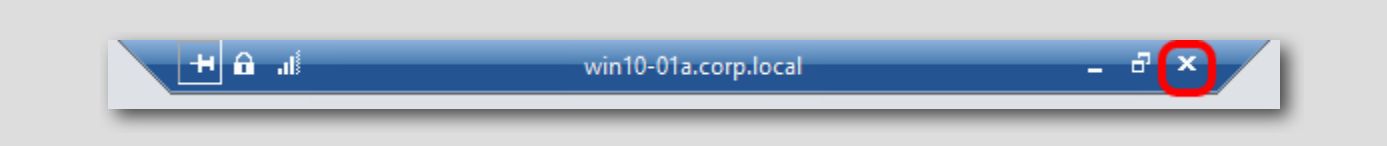
注：[Access Work or School] ページが以前に開かれていた場合は、ページを更新するか、ページから移動してから戻り、変更を確認する必要がある場合があります。



1. [Connected to Workspace ONE UEM] アカウントをクリックします。
2. [Disconnect] をクリックします。
3. [Yes] をクリックします。

メイン コンソールに戻る

[214]



画面上部の [Remote Desktop Connection] バーで [Close (X)] をクリックしてメイン コンソールに戻り、Workspace ONE UEM Console 内での構成を完了します。

まとめ

[215]

モバイル デバイスの管理に加えて、Workspace ONE UEM は Windows 10 デバイスを管理できます。この Windows 10 管理の概要を通じて、制限事項とプロファイルを構成し、モバイル ユーザーにアプリケーションを展開することで、Windows 10 デバイスを管理する方法をより明確に把握できます。

これで、「Windows 10 管理の基本」モジュールは終了です。

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[216]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。


Your Personal journey from zero to IT Superhero
TECH ZONE
Hands on Labs, Tools and Best Practices
How the products work – beginner to expert
Guide to production deployments & operations
Quick start for your first proof of concept
Latest product information

モジュール 3：Apple iOS 管理の概要（30 分）

はじめに

[218]

このラボ モジュールでは、Unified Endpoint Management (UEM) と Workspace ONE の概念について説明します。このラボでは、iOS デバイスを登録し、デバイス プロファイルを展開して、UEM 機能を利用できるように iOS デバイスを構成する方法について説明します。

個人の iOS デバイスを登録しないでください

[219]

重要: 今後の演習のために個人のデバイスを登録しないでください。

個人のデバイスが他の UEM プロバイダーに登録されると、望ましくない競合や問題が発生する可能性があります。

このラボを完了するには、テスト デバイスのみを使用し、個人のデバイスをラボに登録しないことをお勧めします。

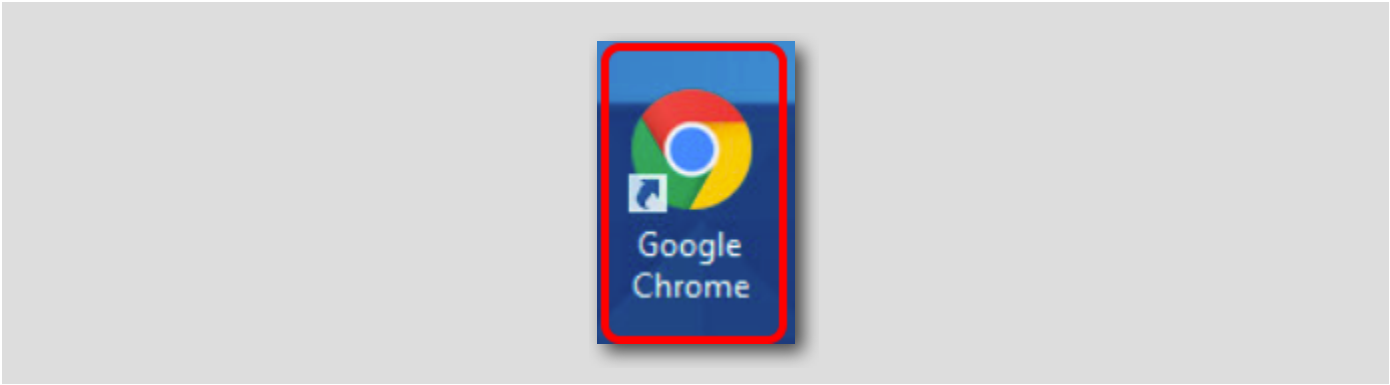
Workspace ONE UEM Console へのログイン

[220]

このラボを開始するには、Workspace ONE UEM 管理コンソールにログインする必要があります。

Chrome ブラウザの起動

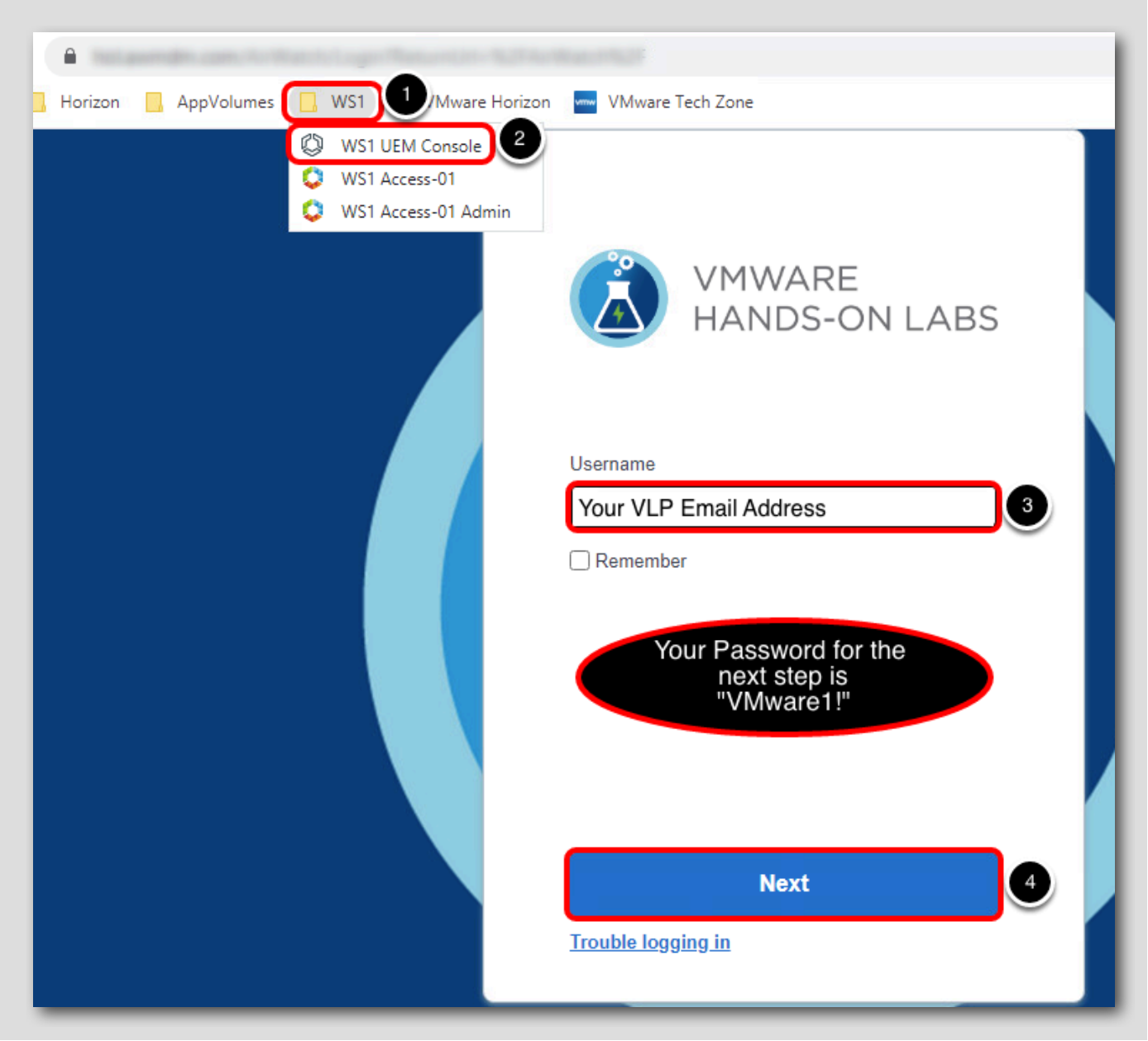
[221]



現在接続している仮想マシンのデスクトップから、[Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールへのログイン

[222]

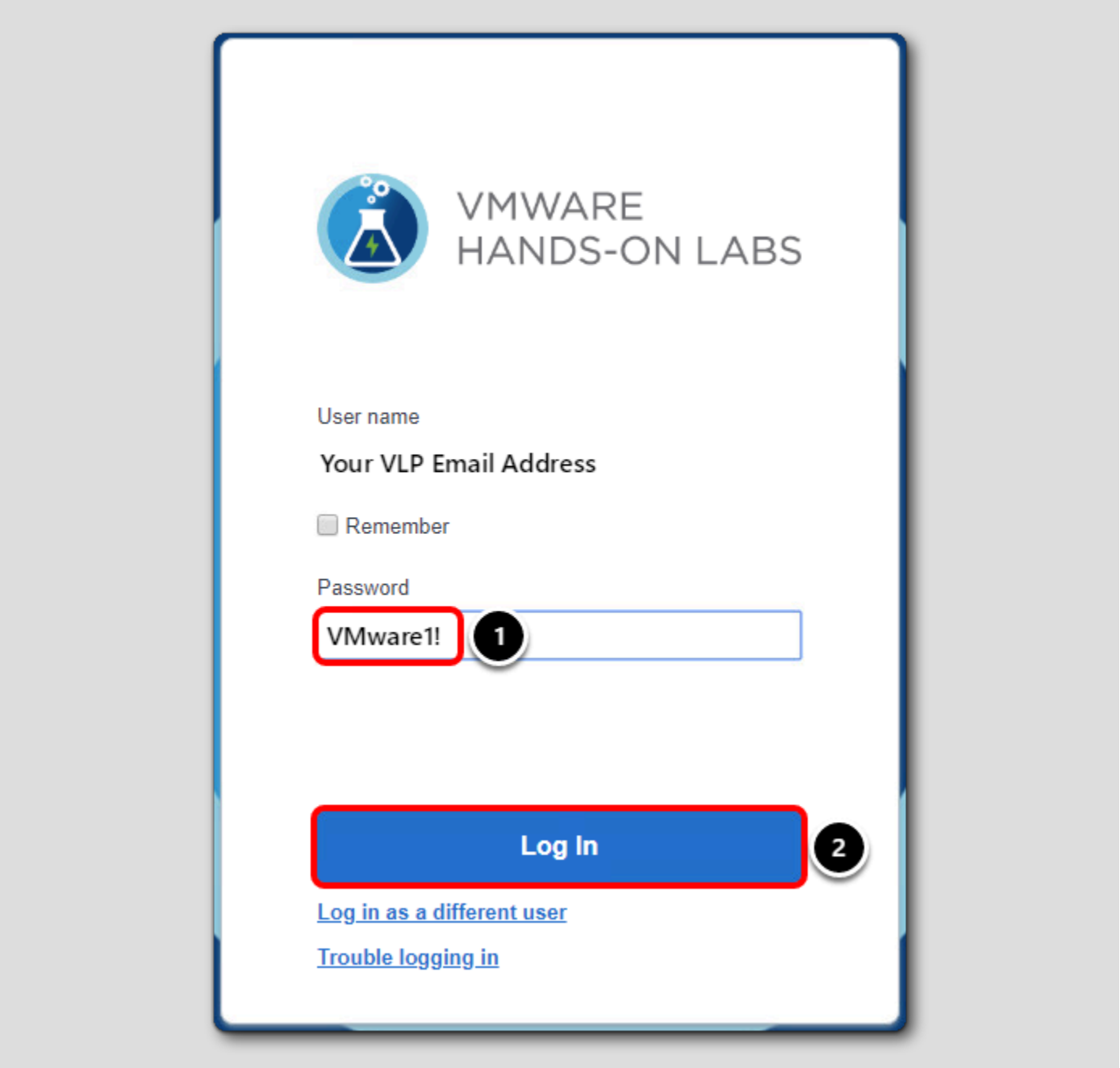


1. [WS1] ブックマーク フォルダをクリックします。
2. [WS1 UEM Console] リンクをクリックします。
3. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。

   注： 次の手順のパスワードは、**`VMware1!`** になります。

4. [Next] をクリックします。

Workspace ONE UEM Console の認証情報の入力 [223]



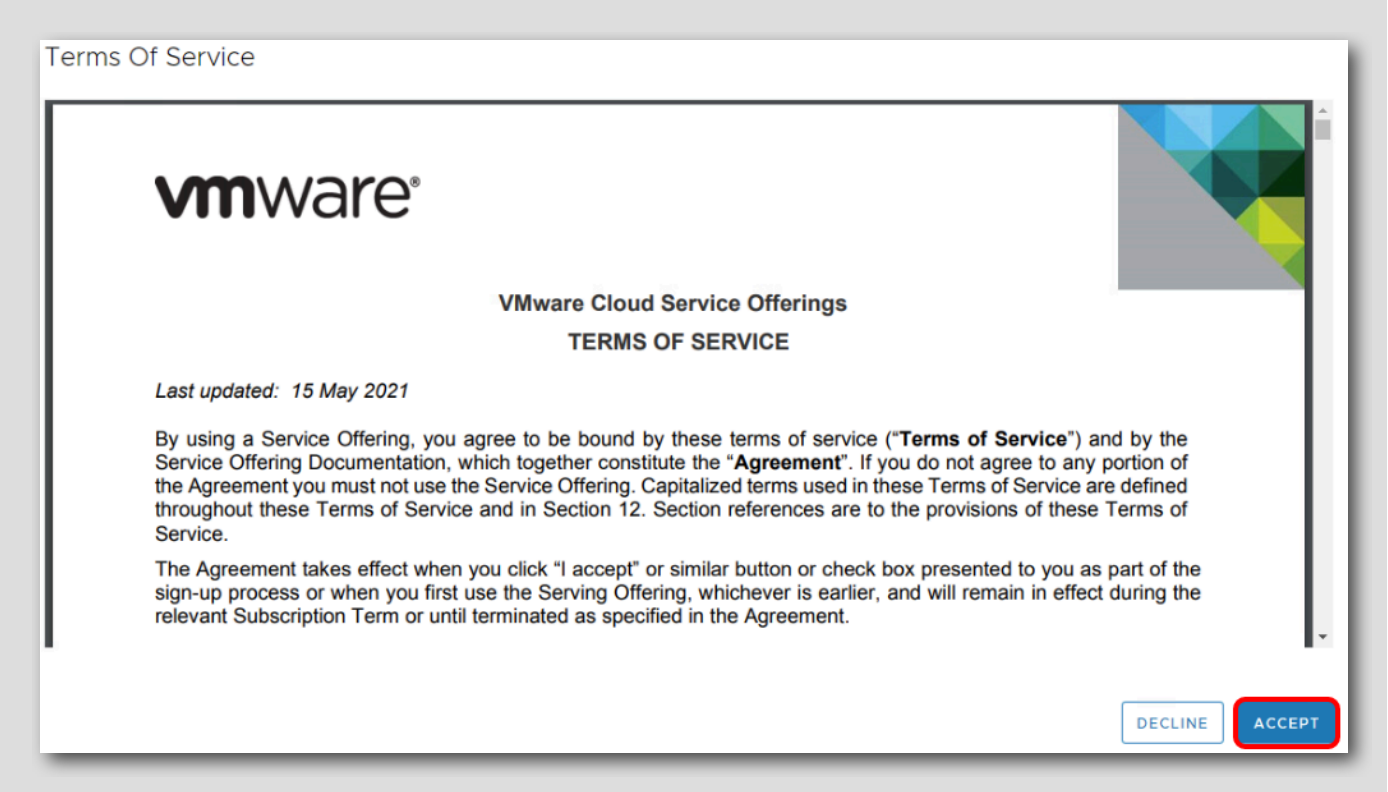
[Password] フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

利用規約の承諾

[224]



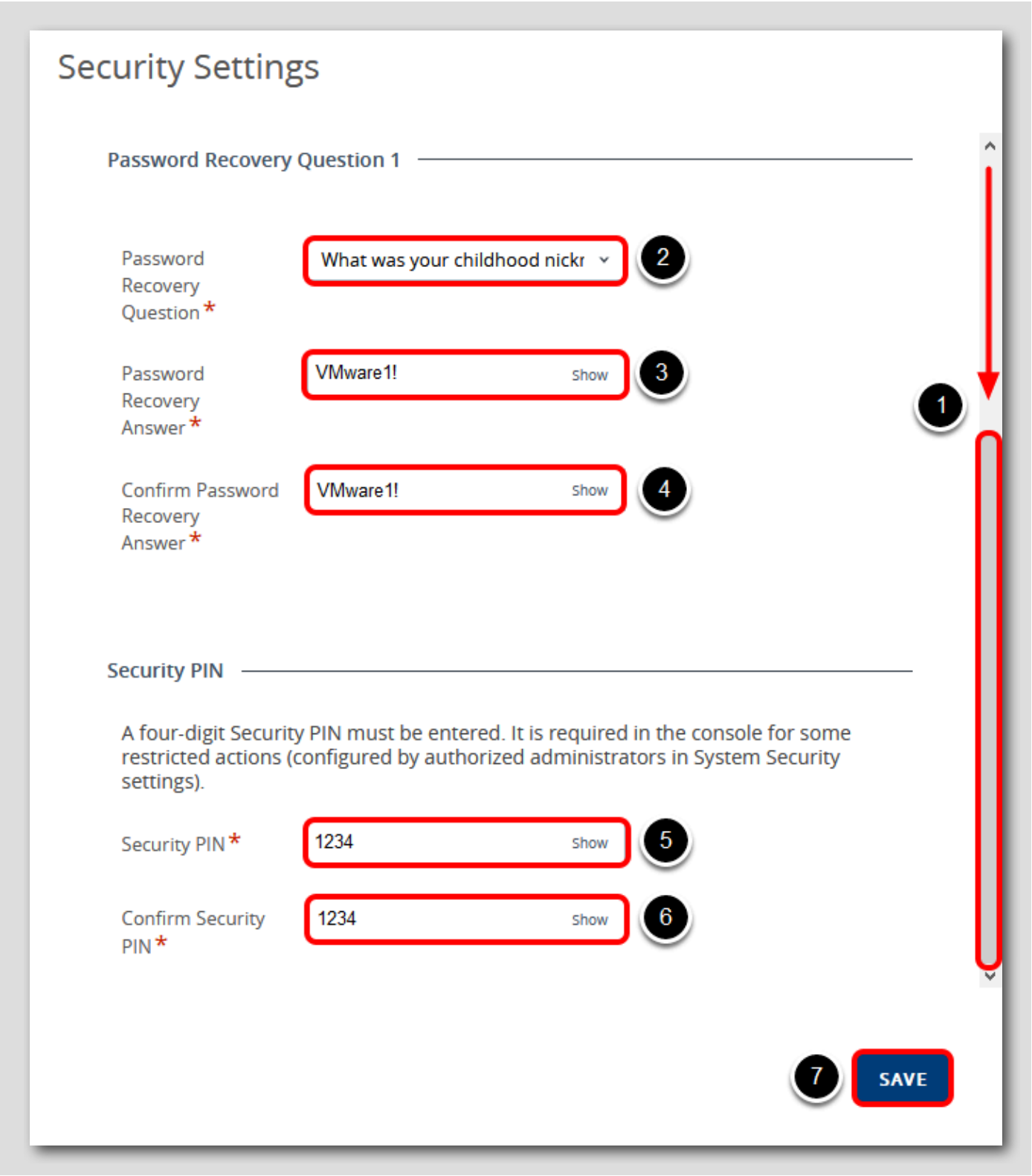
[Workspace ONE UEM Terms of Service] が表示されたら、[Accept] ボタンをクリックします。

注：以降の手順は、管理コンソールへの初回ログイン時にのみ実行されます。

初期セキュリティ設定の完了

[225]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

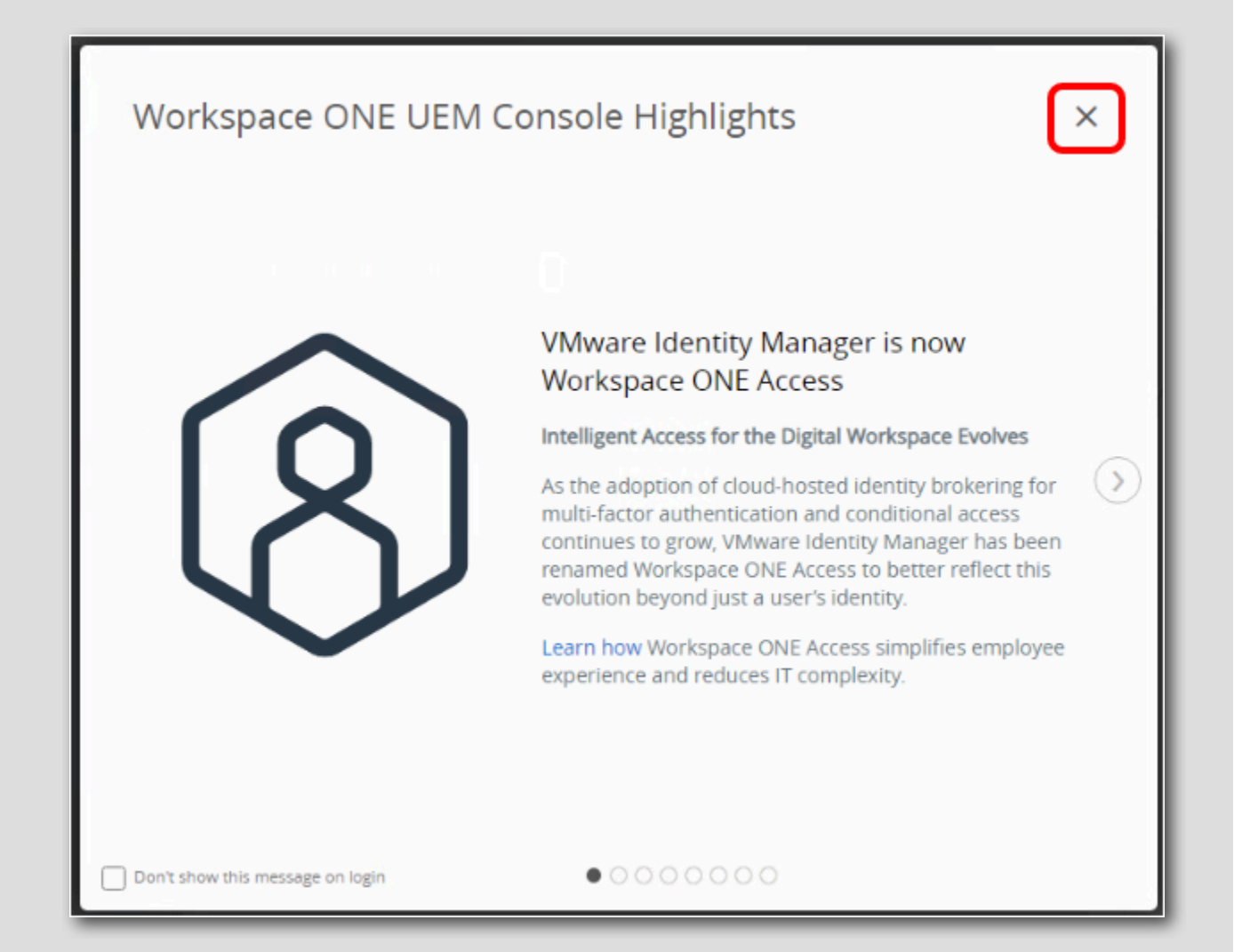

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示します。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[226]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

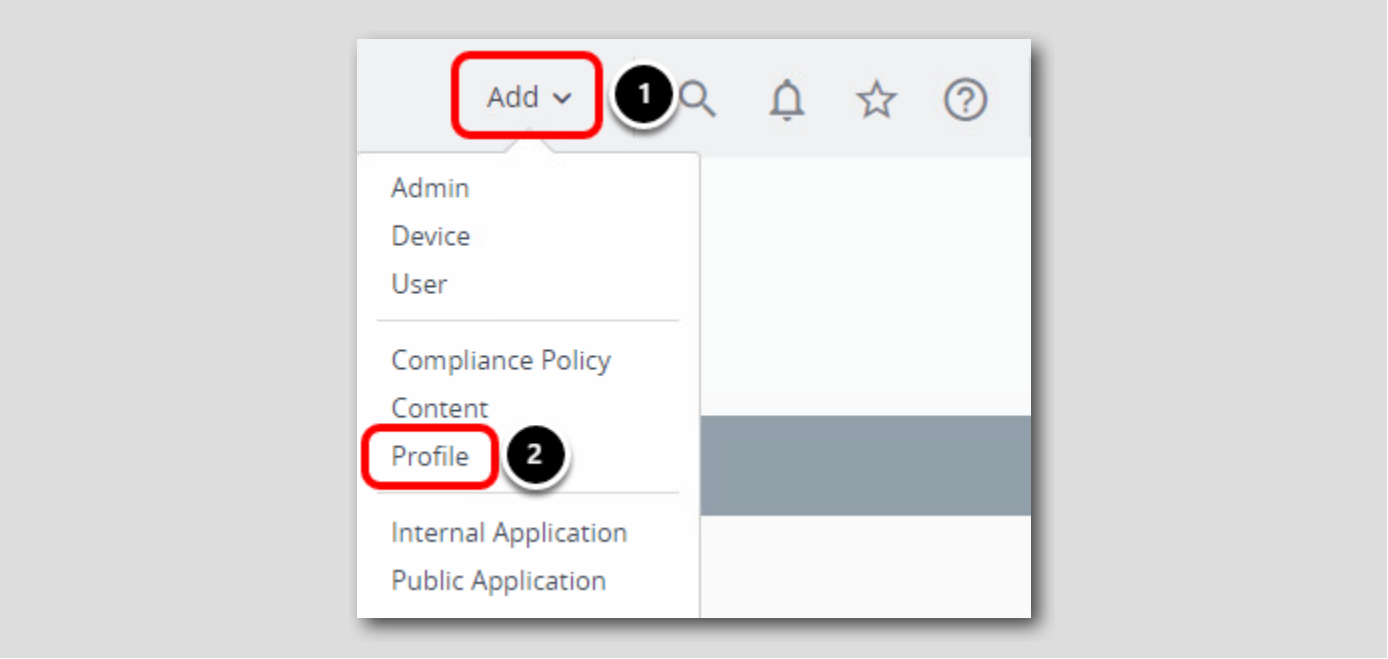
デバイス制限事項プロファイルの作成

[227]

このセクションでは、デバイス上のカメラおよび Siri を無効にする制限事項プロファイルを作成します。自動展開用にプロファイルを設定します。これにより、デバイスの登録時にプロファイルが自動的にインストールされるようになります。

プロファイルの追加

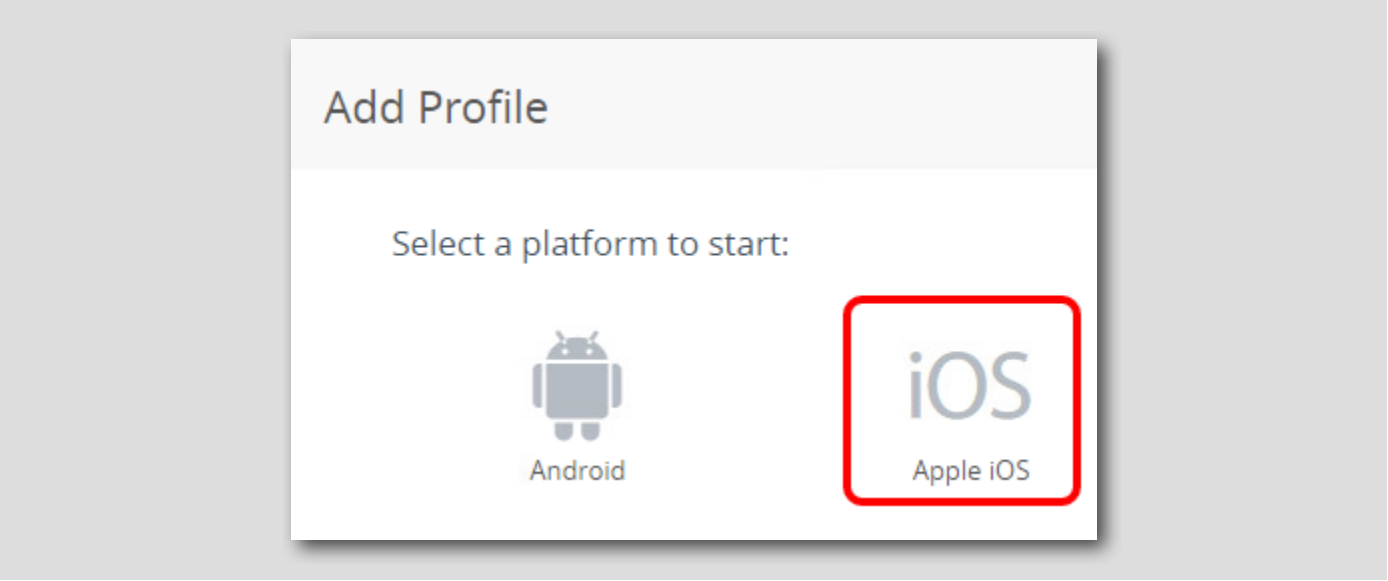
[228]



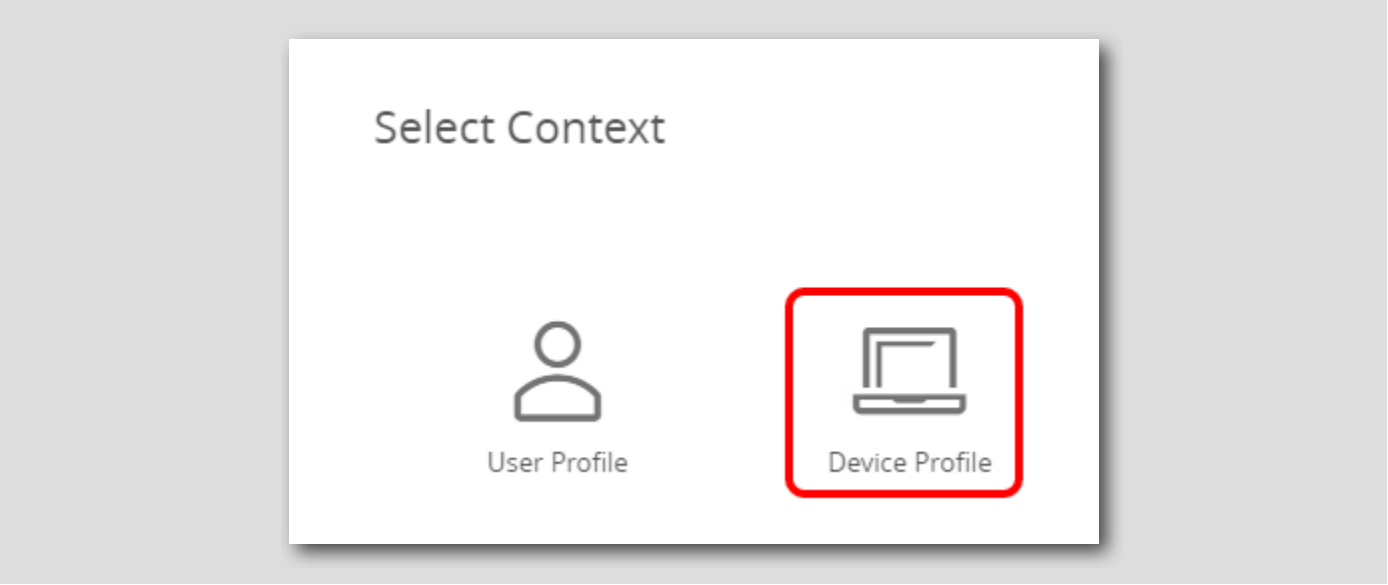
Workspace ONE UEM Console の右上で、次のように操作します。

1. [Add] をクリックします。
2. [Profile] をクリックします。

プラットフォームの選択 [229]



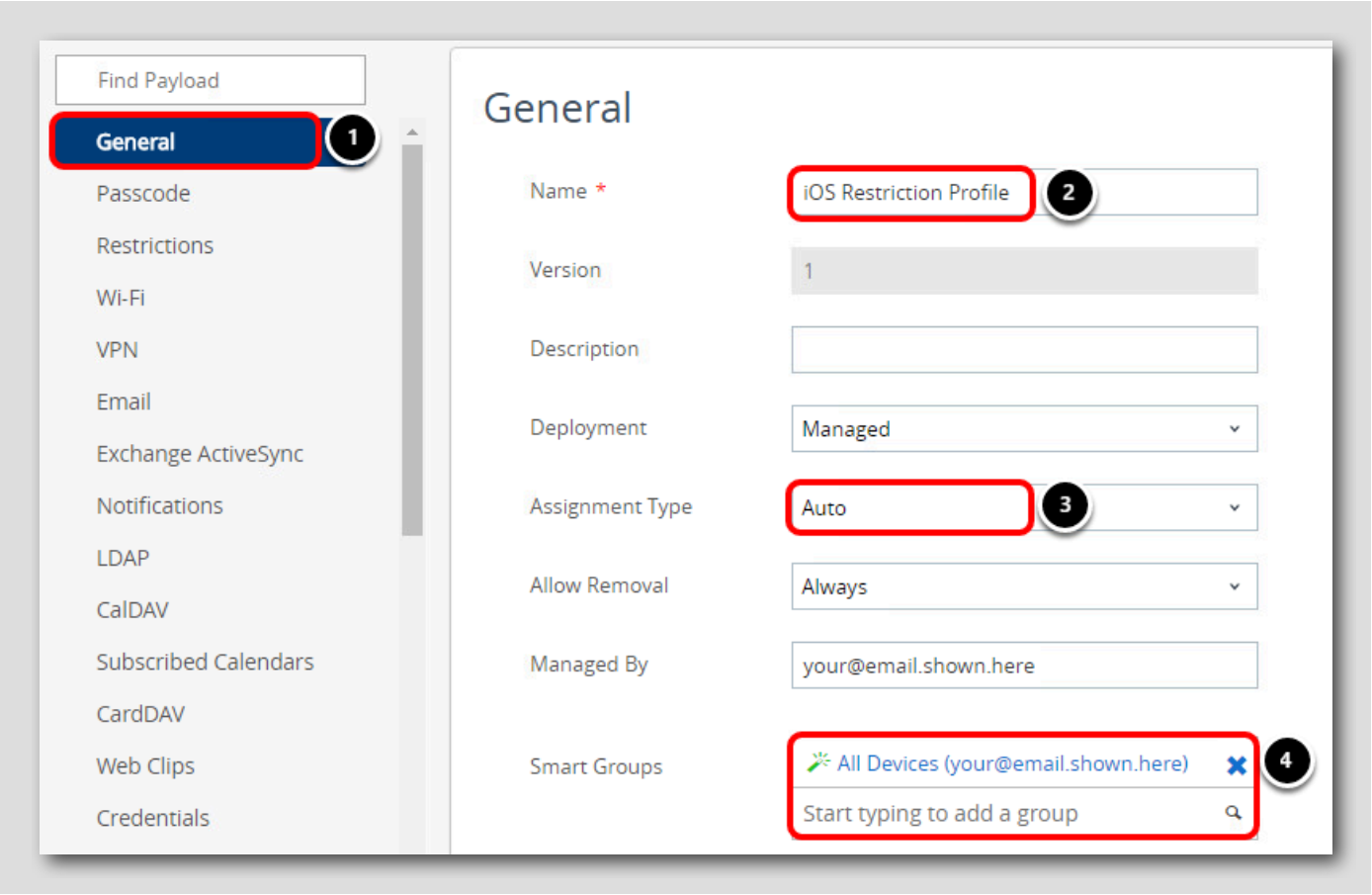
コンテキストの選択 [230]



[Device Profile] コンテキスト オプションをクリックします。

全般ペイロードの構成

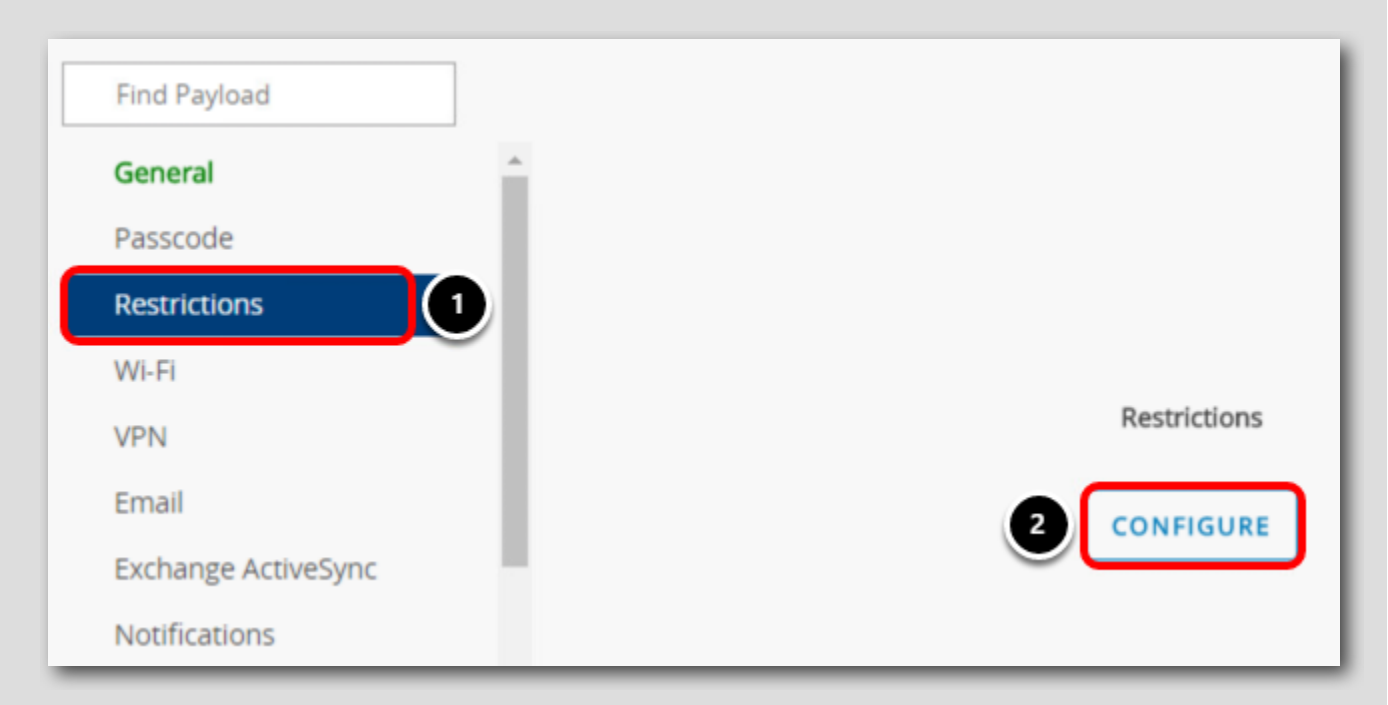
[231]



1. 選択されていない場合は、[General] をクリックします。
2. [Name] フィールドに **`iOS Restriction Profile`** と入力します。
3. [Assignment Type] が [Auto] に設定されていることを確認します。
4. [Smart Groups] ドロップダウン フィールドをクリックして、[All Devices (your@email.shown.here)] を選択します。

制限事項ペイロードの構成

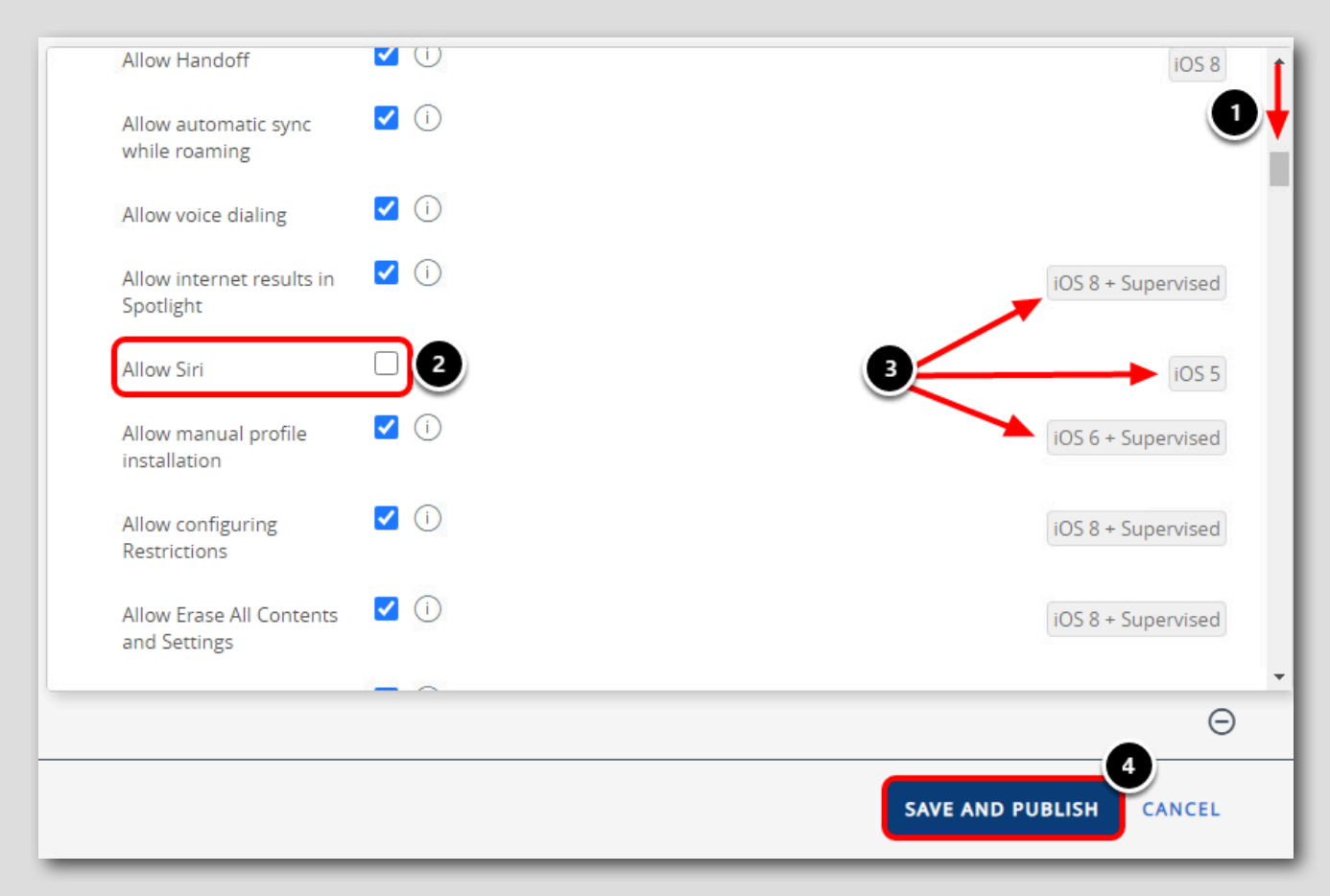
[232]



1. 左側のパネルで [Restrictions] ペイロードをクリックします。
2. [Configure] をクリックします。

カメラと Siri を無効にする

[233]

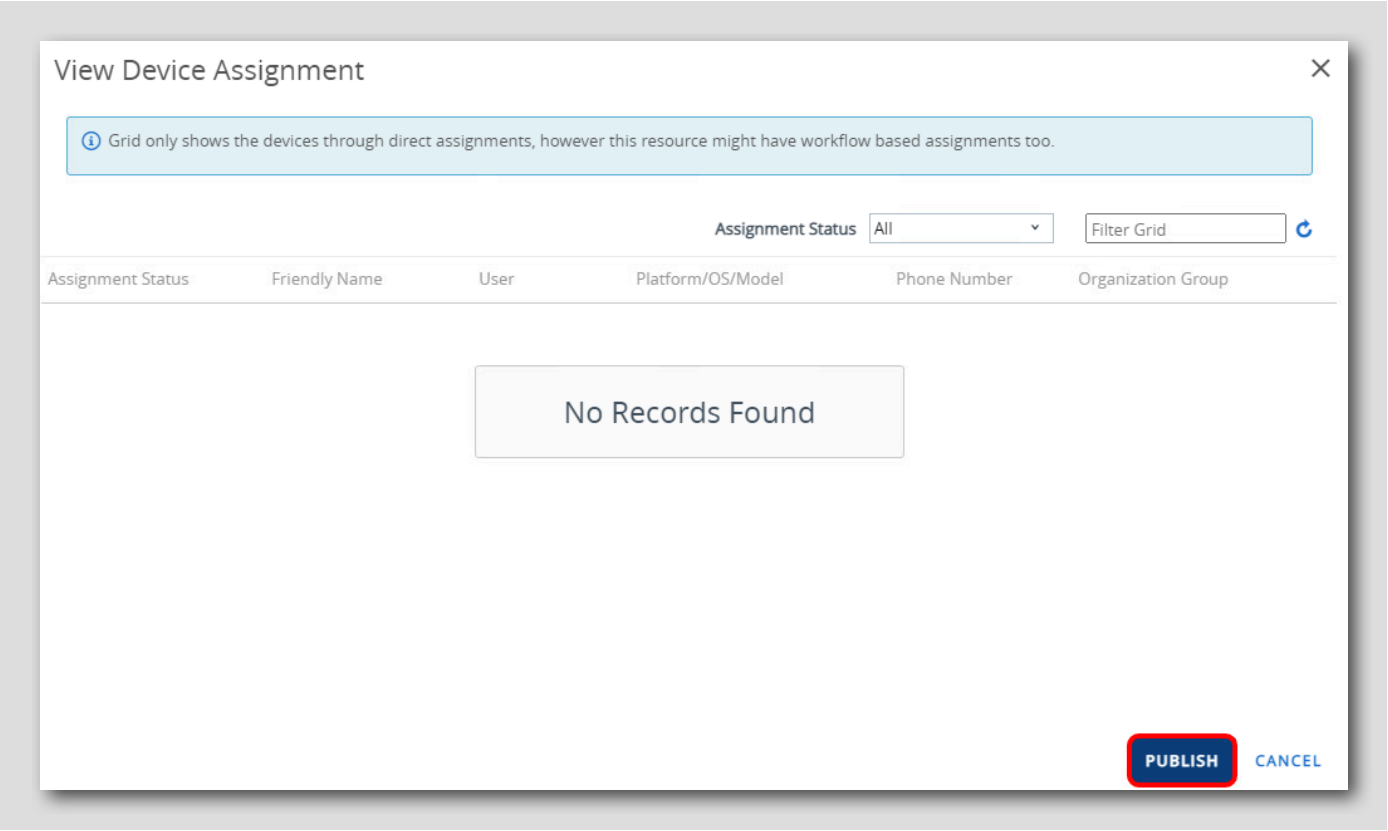


1. 約 1 ページ下へスクロールして、[Allow Siri] オプションを見つけます。
2. [Device Functionality] セクションの下に表示されている [Allow Siri] チェックボックスをオフにします。これにより、デバイス上の Siri が無効になります。
3. 各制限事項に対する [iOS version] と [Supervised] の要件に注意してください。この制限を受けるターゲット デバイスは、リストされている iOS バージョン（つまり iOS 5）以降で、[Supervised] タグも表示されている場合は監視対象である必要があります。例：[Allow Siri] 制限ではデバイスを監視する必要はありませんが、[Allow Manual Profile Installation] 制限では監視する必要があります。これらの要件に注意し、制限プロファイルを公開するときに表示されるすべての要件をデバイスが満たしていることを確認してください。
4. [Save & Publish] をクリックします。

注：監視対象デバイスにより、学校および企業は所有する iOS デバイスをより細かく制御できます。デバイスの監視により、管理者は、Bring Your Own Device (BYOD) シナリオでは不可能な追加のデバイス制限事項を使用して、エンド ユーザーのプライバシーを尊重できます。

プロファイルの公開

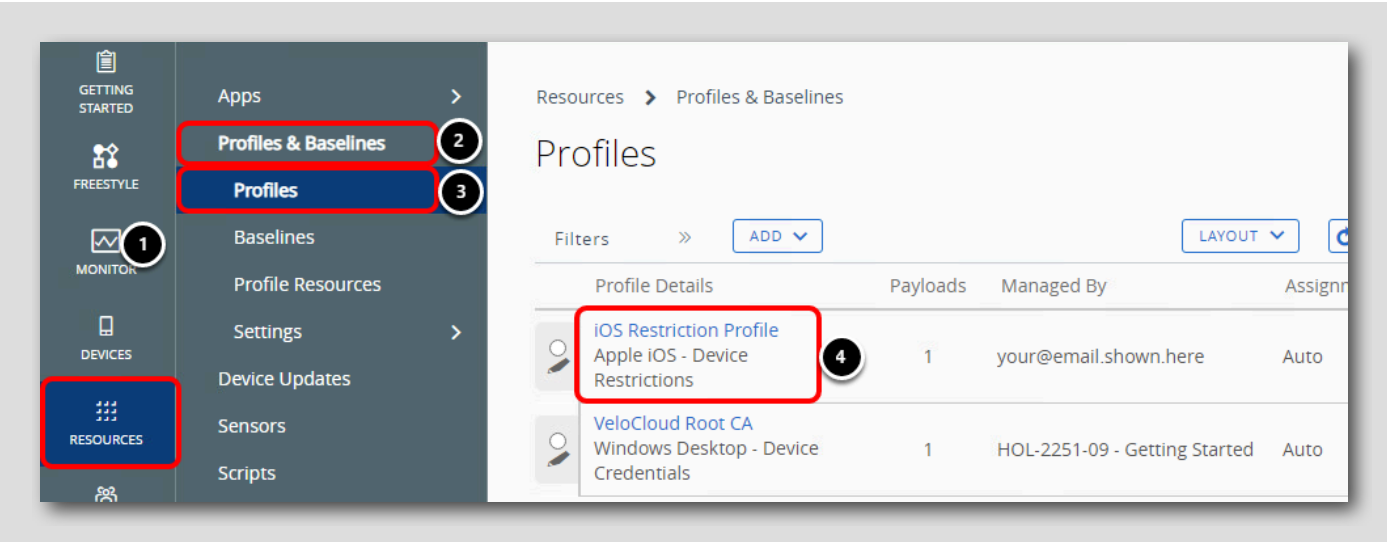
[234]



[Publish] をクリックします。

プロファイルが作成されたことの確認

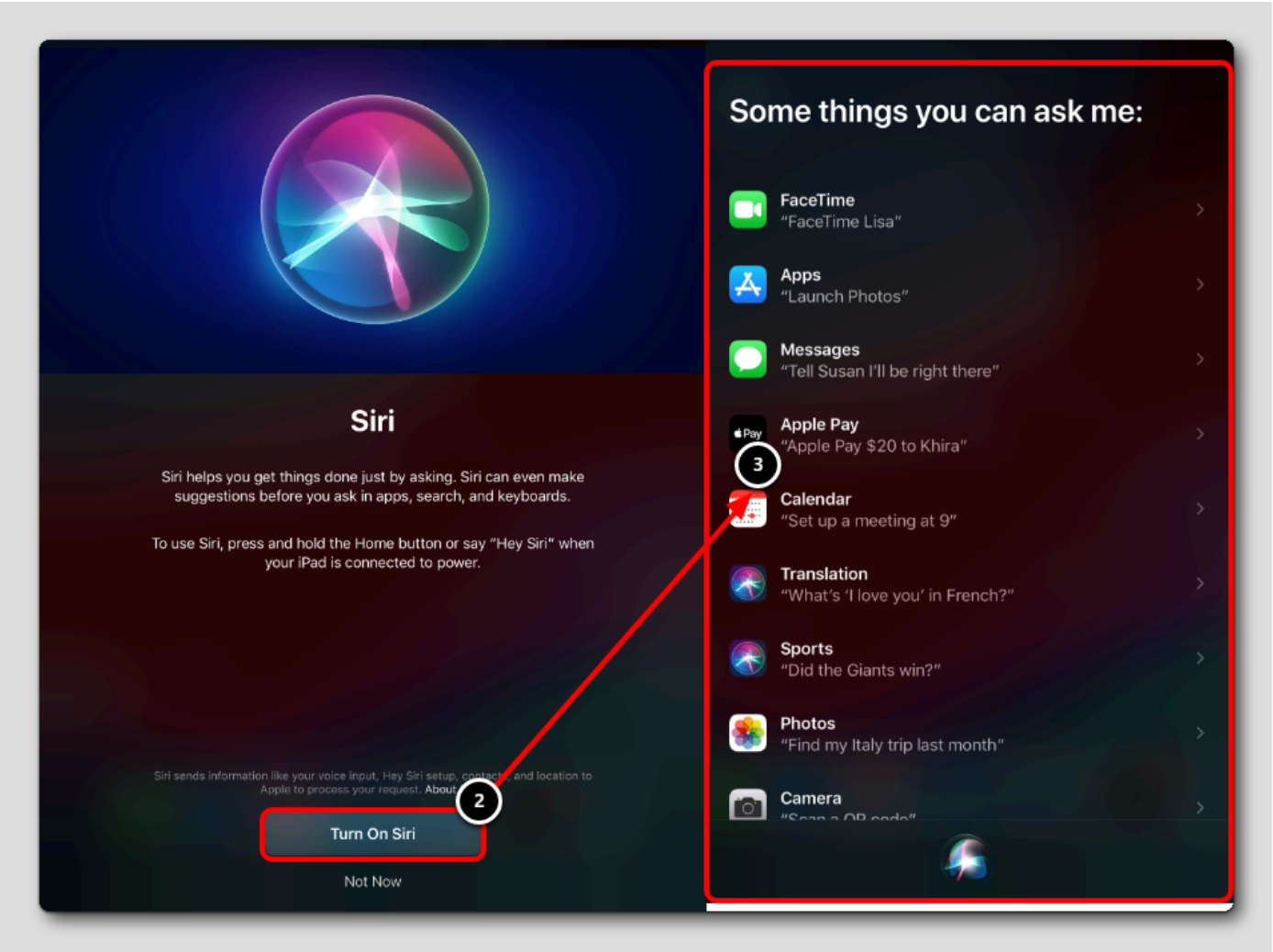
[235]



1. [Resources] をクリックします。
2. [Profiles & Baselines] を展開します。
3. [Profiles] をクリックします。
4. [Profiles] のリストに [iOS Restriction Profile] が表示されていることを確認します。

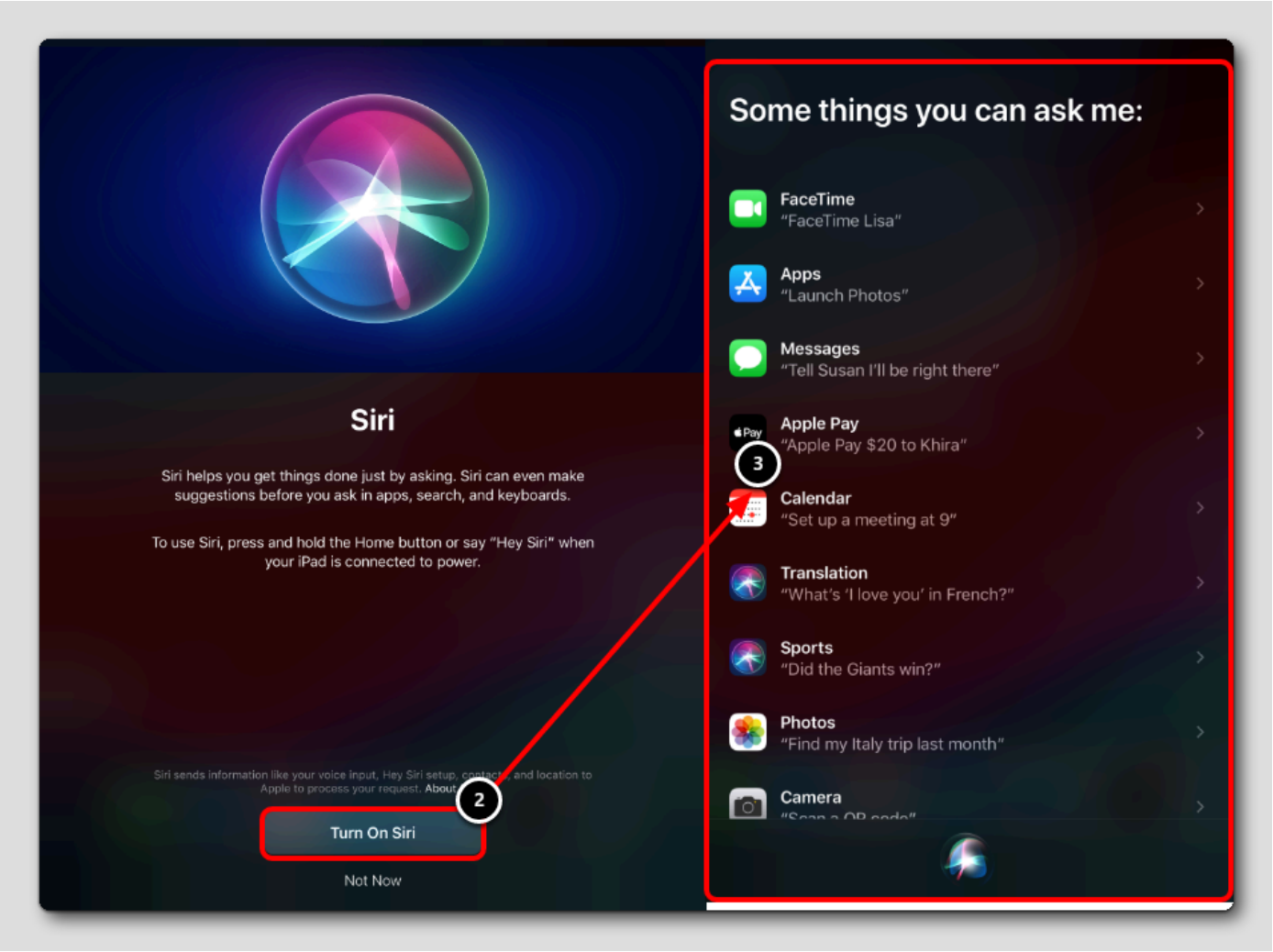
登録前のデバイス構成の確認

[236]



デバイスを登録する前に、Siri が iOS アプリケーションで使用できることを確認します。これにより、デバイスが次回以降の手順で登録されたときに、iOS の制限事項プロファイルで Siri が正しく無効になることを確認できます。

1. デバイスで Siri を有効にします（デバイスに応じて [Home] または [Side] ボタンを押したままにします）。
2. Siri が無効な場合は、[Turn On Siri] をタップします。
3. デバイスで Siri が有効になっていることを確認し、Siri が入力を待機していることを確認します。



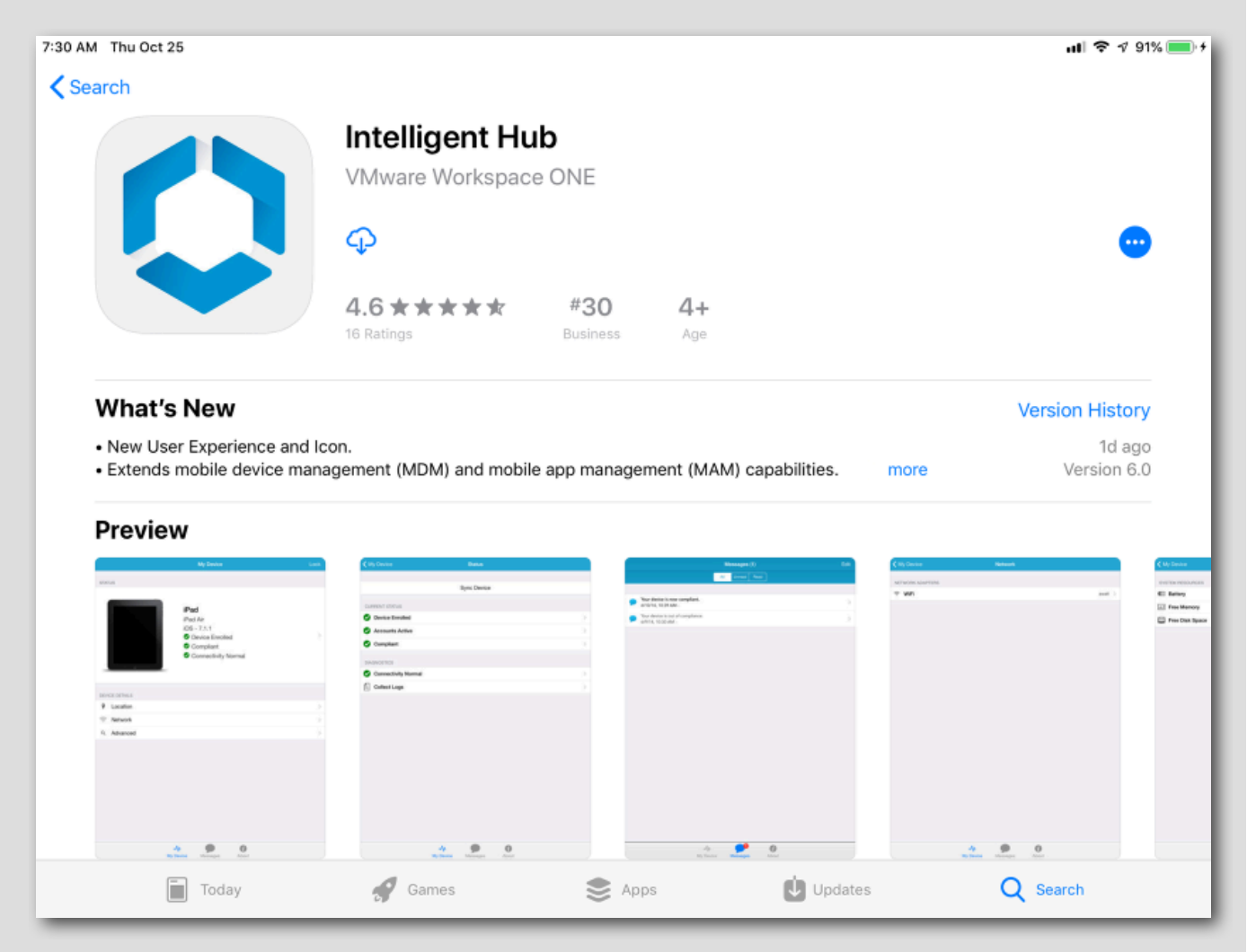
testuser を使用した iOS デバイスの登録

[237]

このセクションでは、iOS デバイスを登録します。以降の手順は、iOS デバイスから完了する必要があります。

App Store から Workspace ONE Intelligent Hub をダウンロードしてインストール（必要な場合）

[238]



注：チェックアウトされたデバイスには、Workspace ONE Intelligent Hub がすでにインストールされている可能性があります。デバイスに Workspace ONE Intelligent Hub がインストールされている場合は、この手順をスキップできます。

この時点で、ご自身の iOS デバイスを使用している場合、またはご使用のデバイスに Workspace ONE Intelligent Hub アプリケーションがインストールされていない場合は、App Store からアプリケーションをインストールしてください。

App Store から Workspace ONE Intelligent Hub アプリケーションをインストールするには、App Store アプリケーションを開き、無料の Workspace ONE Intelligent Hub アプリケーションをダウンロードします。

Workspace ONE Intelligent Hub の起動

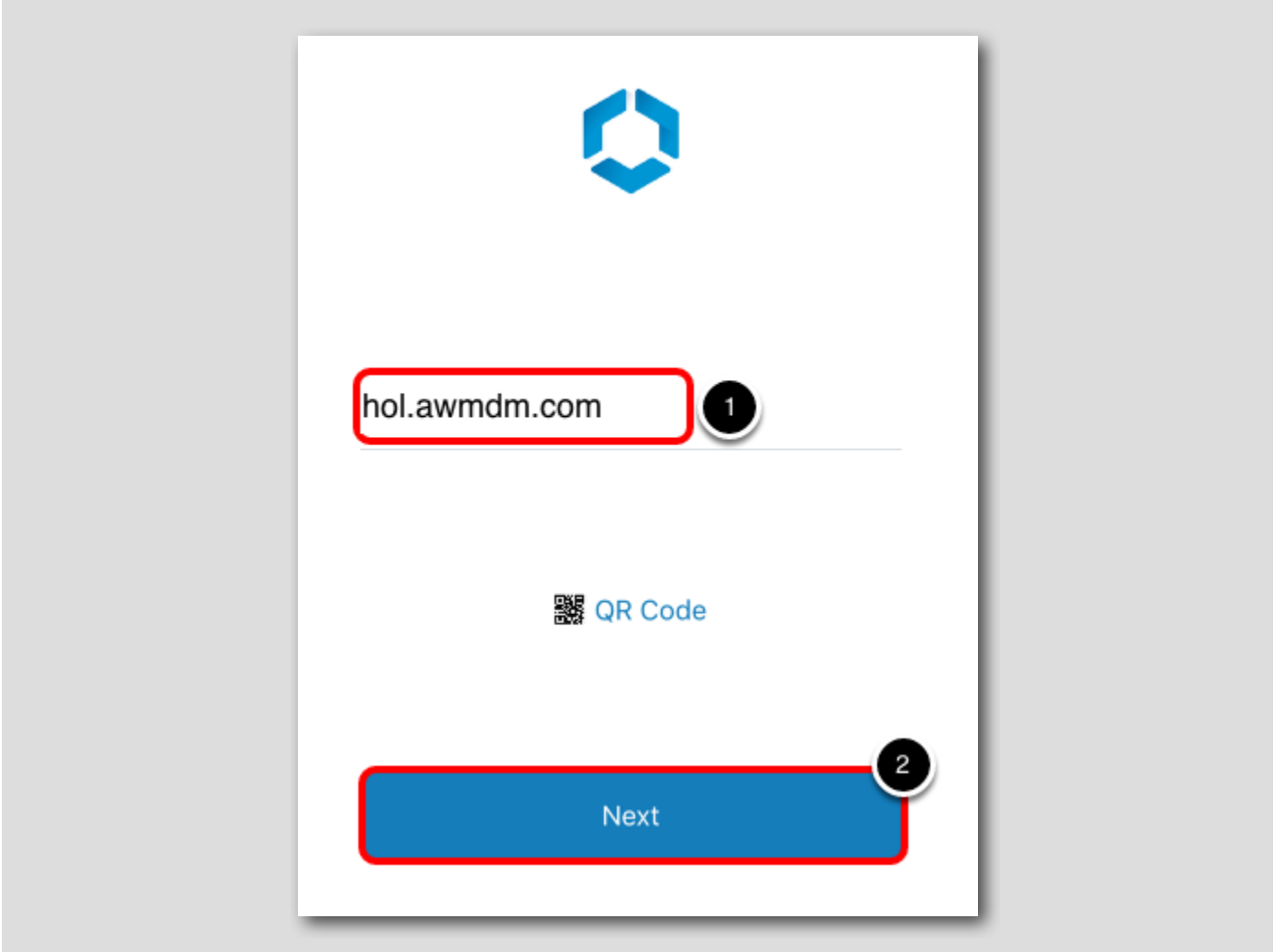
[239]

デバイス上で Hub アプリケーションを起動します。

注：ご自身の iOS デバイスでテストをご希望の場合は、まず Workspace ONE Intelligent Hub アプリケーションをダウンロードしてください。

サーバ URL の入力

[240]



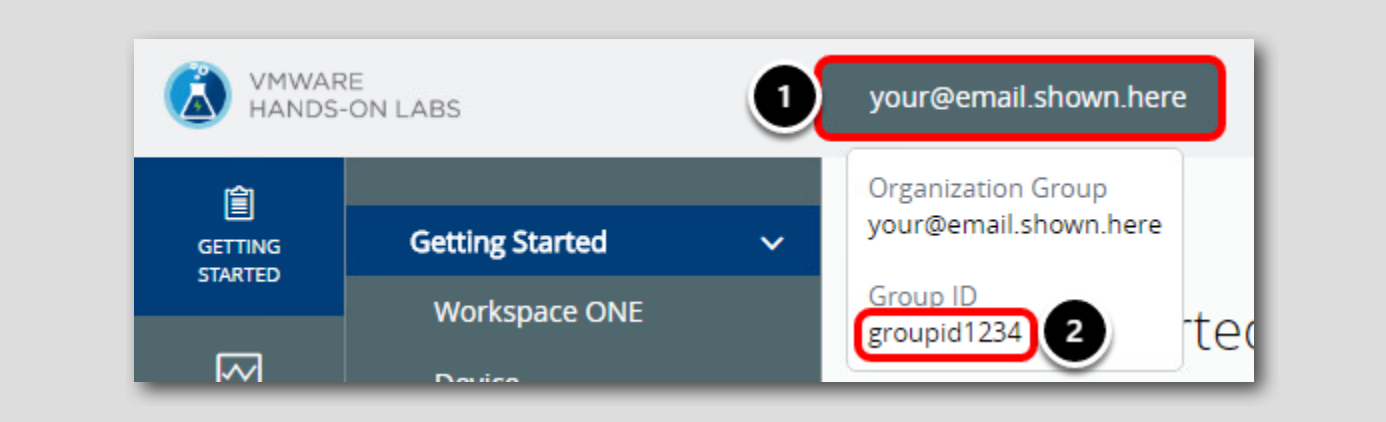
Hub が起動したら、デバイスを登録することができます。これを行うには、次の手順を実行します。

1. [Server] フィールドに **`hol.awmdm.com`** と入力します。
2. [Next] ボタンをクリックします。

注：iPhone をご使用の場合は、必要に応じて [Done] をタップしてキーボードを閉じた後、[Continue] ボタンをタップします。

Workspace ONE UEM Console でのグループ ID の検索

[241]



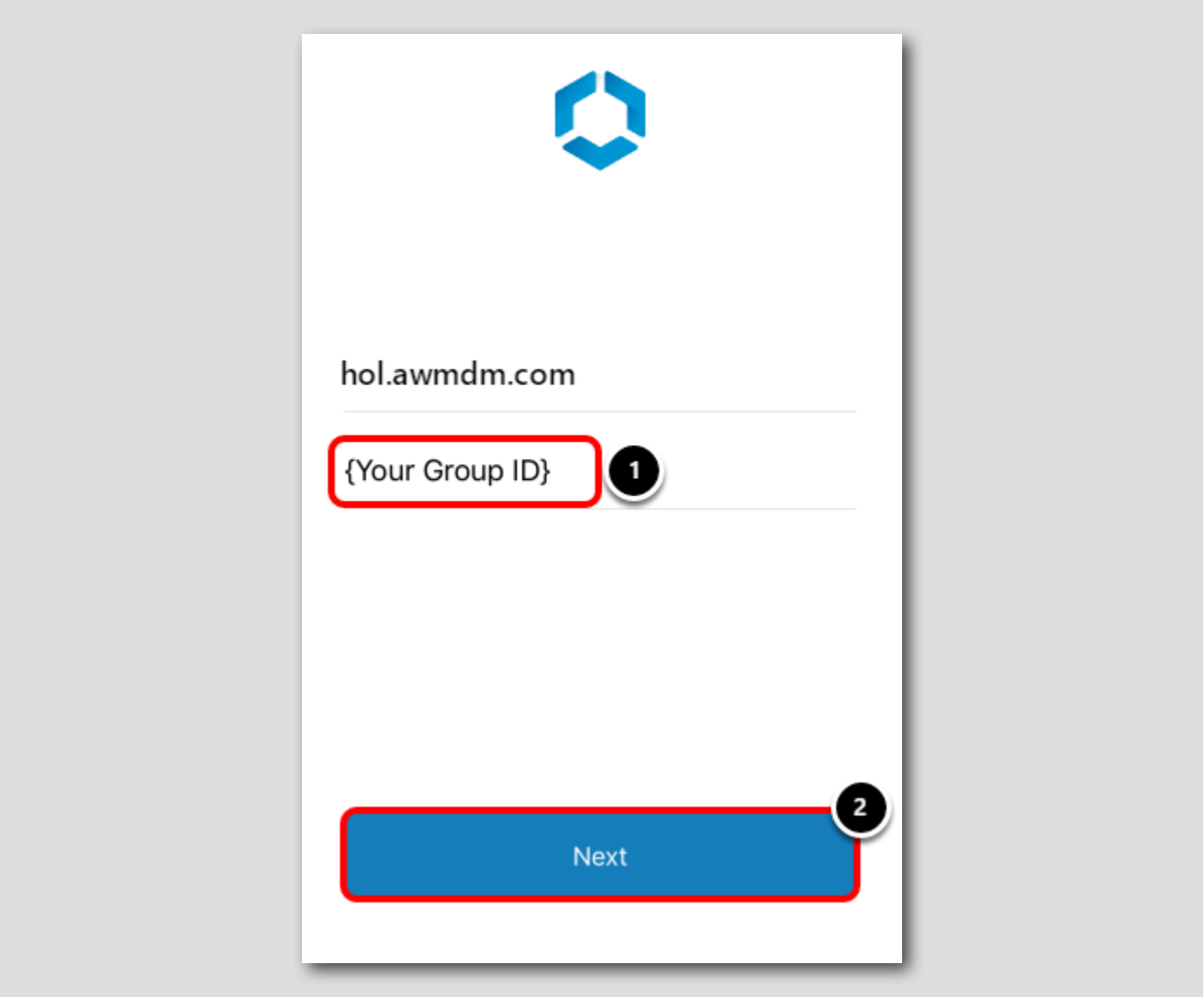
Workspace ONE UEM Console に戻ります。

1. グループ ID を確認するには、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. グループ ID は [Organization Group] ポップアップの最下部に表示されます。

注：このグループ ID は、以降の手順でデバイスを登録するときに必要です。

サンドボックスへの Workspace ONE Intelligent Hub の接続

[242]



iOS デバイスの Workspace ONE Intelligent Hub アプリケーションに戻ります。

1. [Group ID] フィールドに、組織グループの**グループ ID** を入力します。グループ ID は、前に「**グループ ID の確認**」手順で確認しました。
2. [Next] ボタンをクリックします。

注： iPhone をご使用の場合は、必要に応じて [Done] をタップしてキーボードを閉じた後、[Next] ボタンをタップします。

ユーザー認証情報の入力

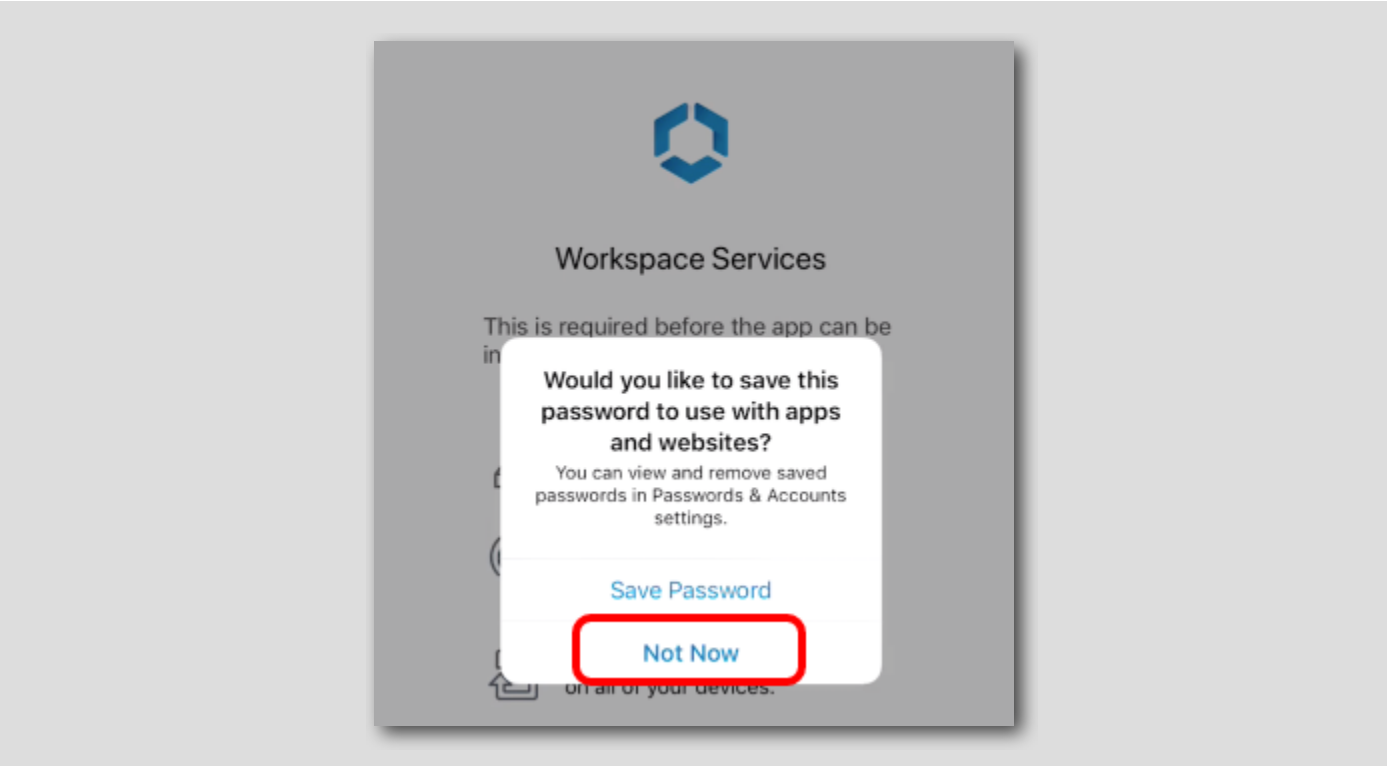
[243]

Workspace ONE UEM の認証に使用するユーザー認証情報を入力します。

1. [Username] フィールドに **testuser** と入力します。
2. [Password] フィールドに **VMware1!** と入力します。
3. [Next] ボタンをクリックします。

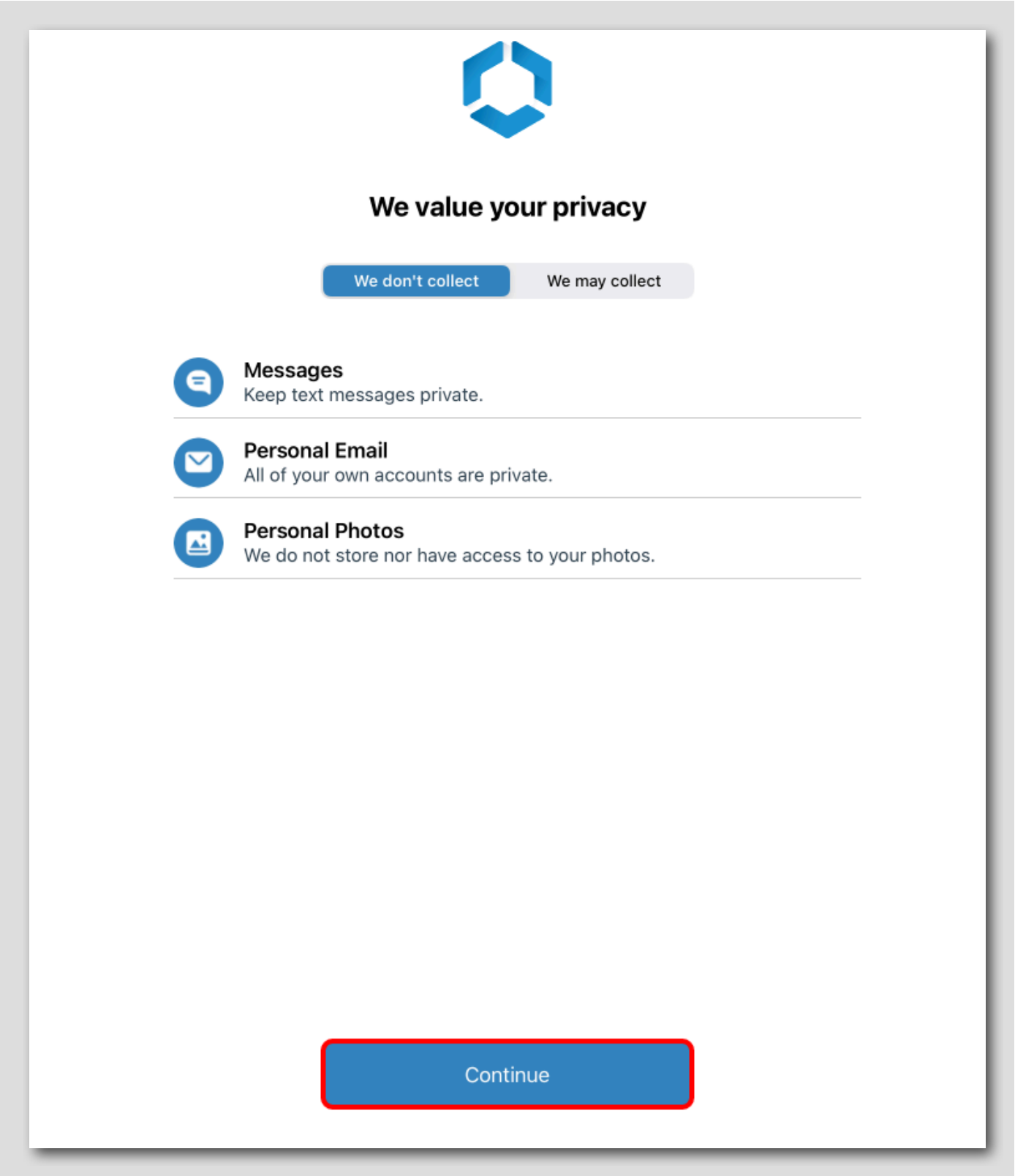
パスワードを保存しない

[244]



パスワードを保存するように求めるメッセージが表示された場合は、[Not Now] をクリックします。

プライバシー通知の確認


We value your privacy
We don't collect
We may collect
Messages
Keep text messages private.
Personal Email
All of your own accounts are private.
Personal Photos
We do not store nor have access to your photos.
Continue

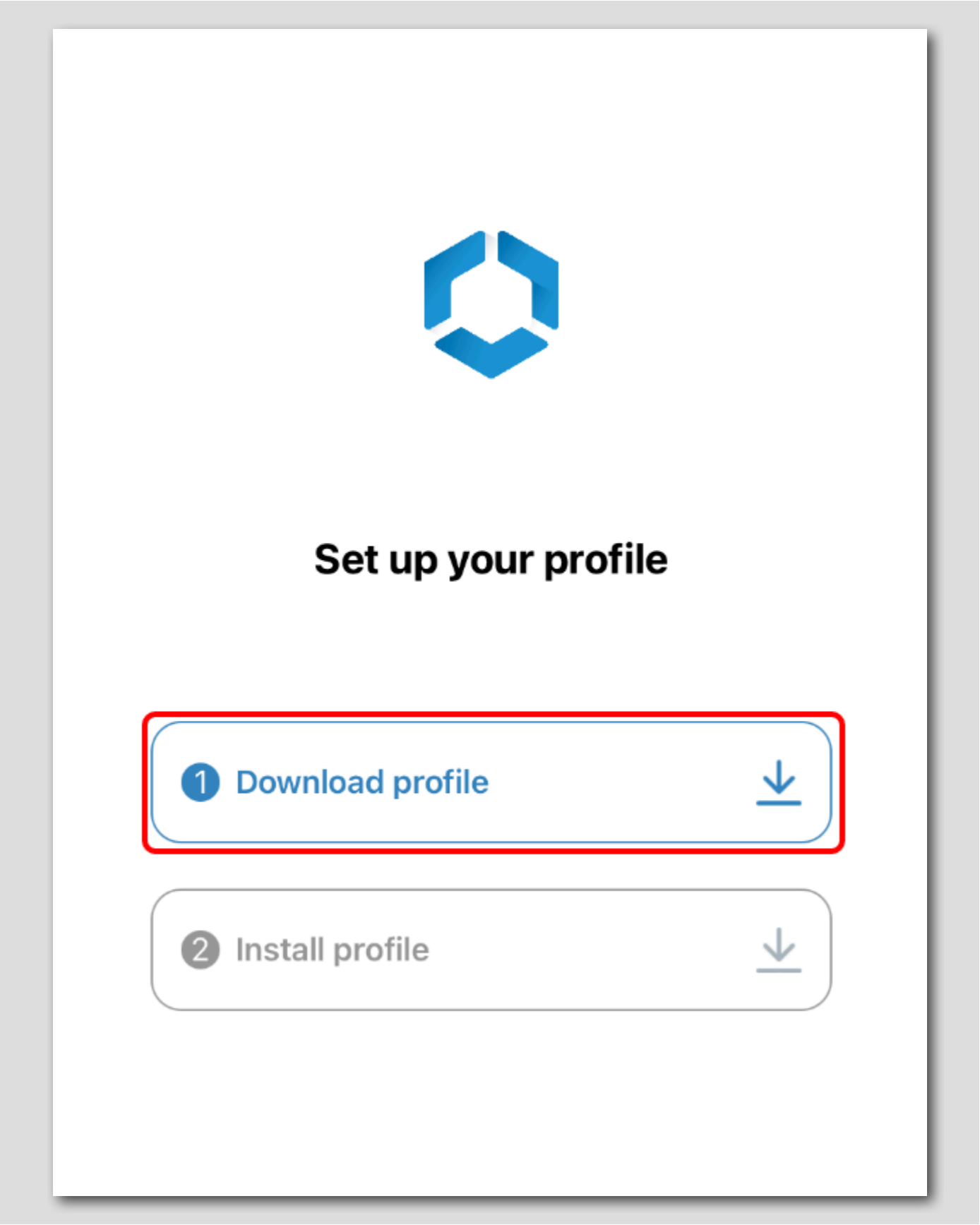
Workspace ONE Intelligent Hub には、デバイスから収集される内容と収集されない内容の詳細を示すプライバシー メッセージが表示されます。

次の手順では、デバイスを Workspace ONE UEM に登録する構成プロファイルをダウンロードします。

[Continue] をタップして開始します。

デバイス プロファイルのセットアップ

[246]

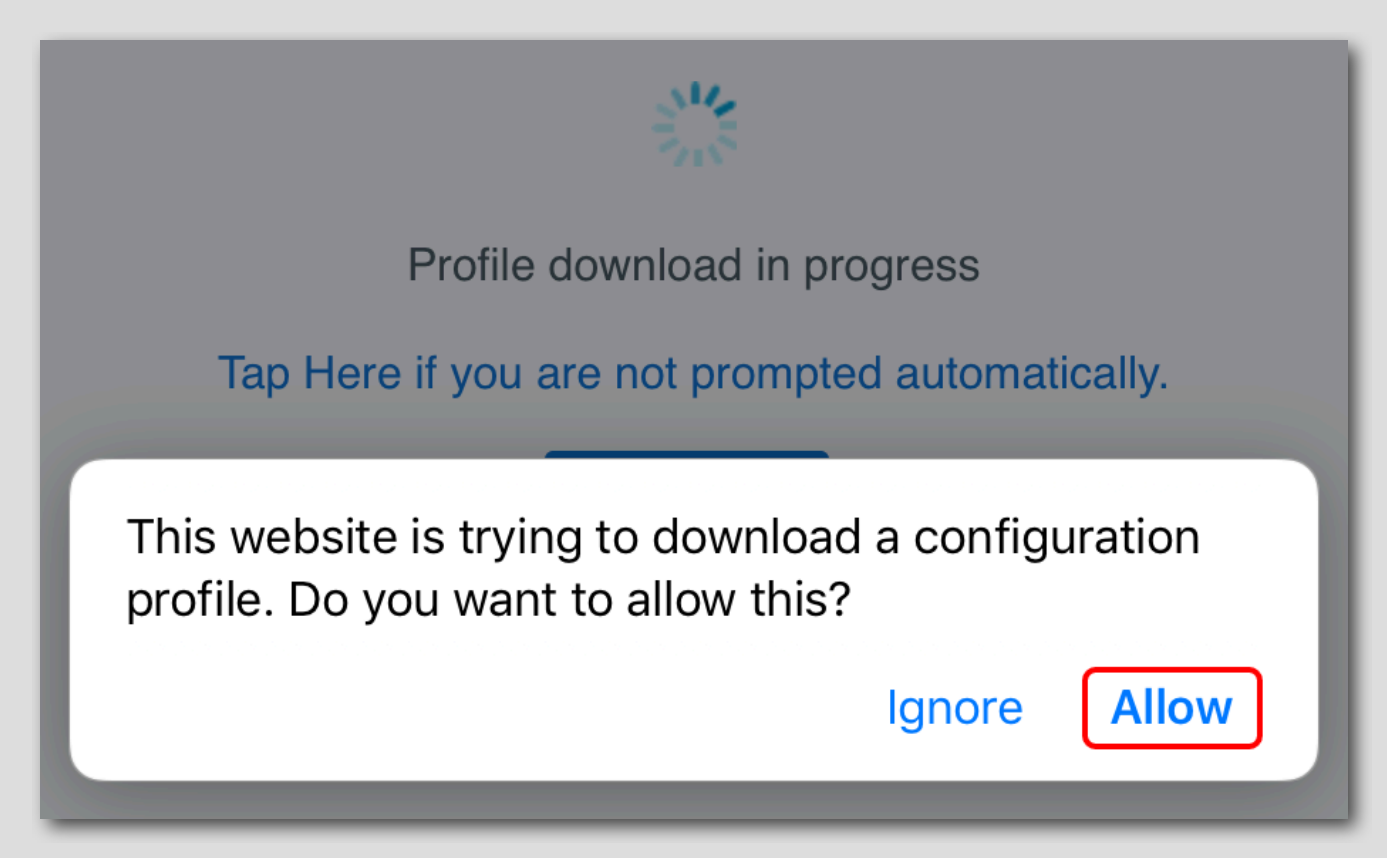

Set up your profile
1 Download profile
2 Install profile

次の手順では、デバイスを Workspace ONE UEM に登録する構成プロファイルをダウンロードします。

[Download profile] をタップして開始します。

Web サイトで設定を開くことを許可する

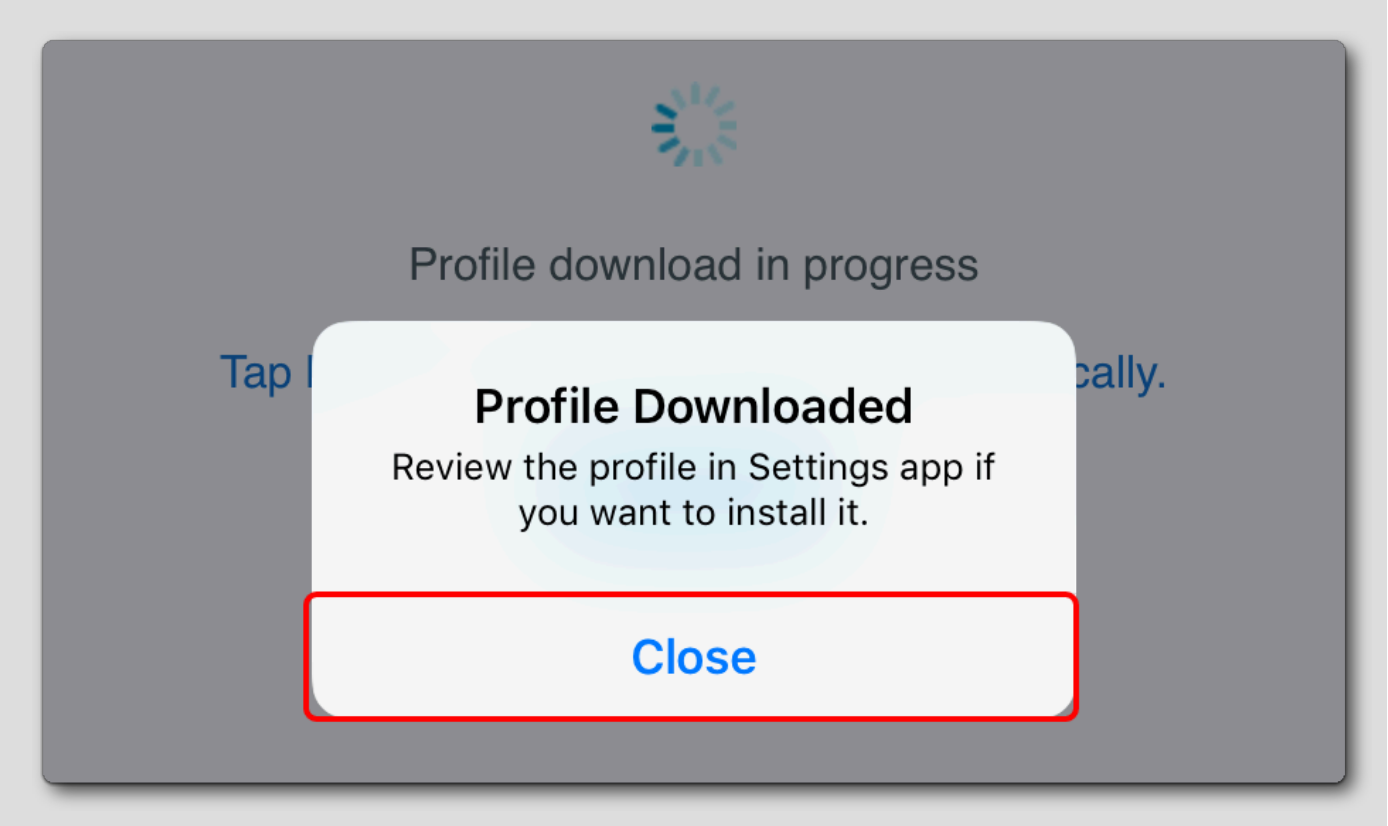
[247]



Web サイトで構成プロファイルをダウンロードしようとしていることを示すメッセージが表示されたら、[Allow] をタップします。

[Profile Downloaded] 通知を閉じる

[248]



プロファイルがダウンロードされたという通知が表示されたら、[Close] をクリックします。

VMWARE
HANDS-ON LABS

Steps to download profile

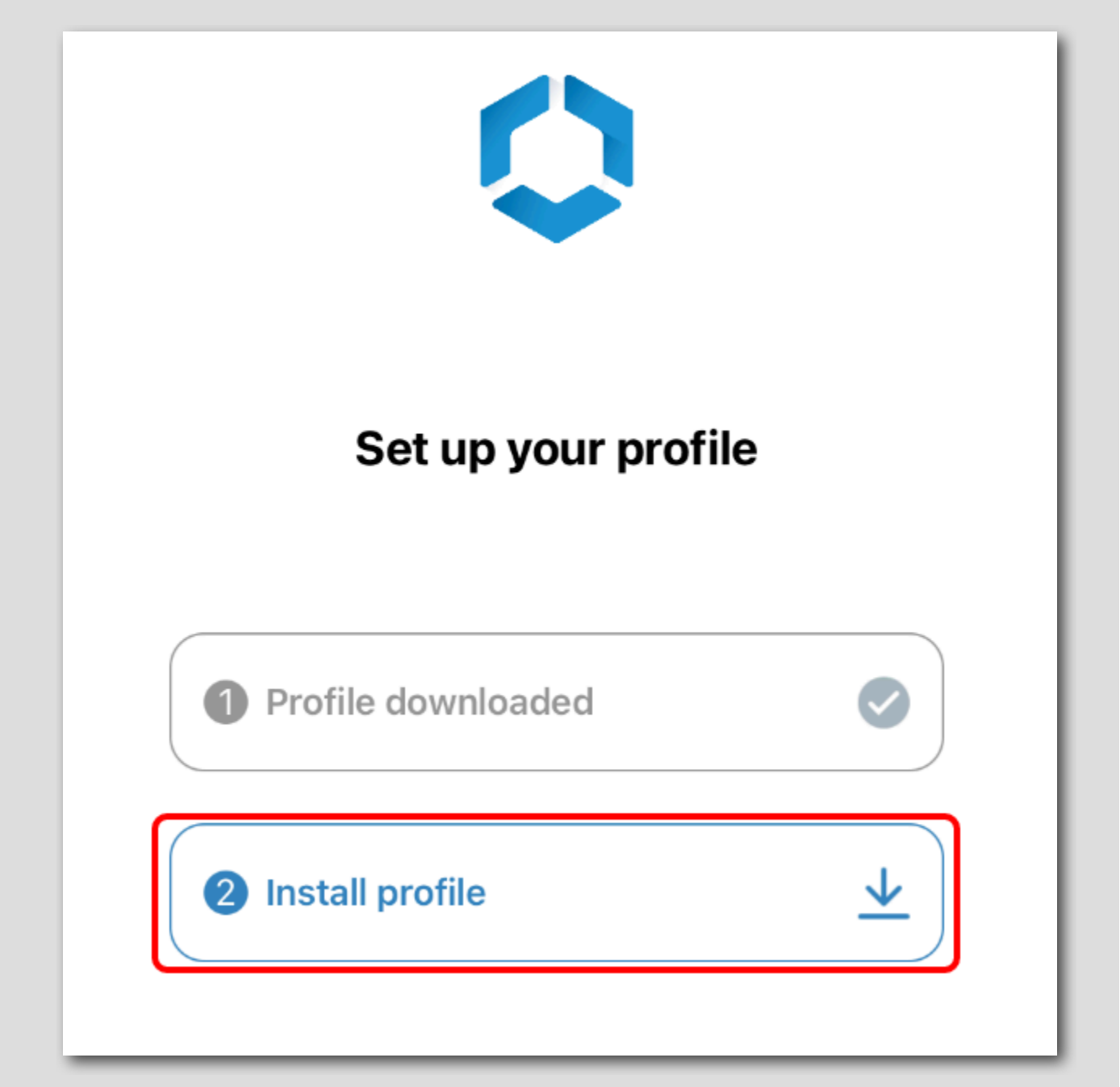
1. When prompted to download the profile, tap on **Allow**

2. After the download is complete, tap on

プロファイルがダウンロードされたら、[Tap here when download finishes] をタップします。これにより、プロファイルをインストールする Intelligent Hub アプリケーションに戻ります。

デバイス プロファイルのインストール

[249]

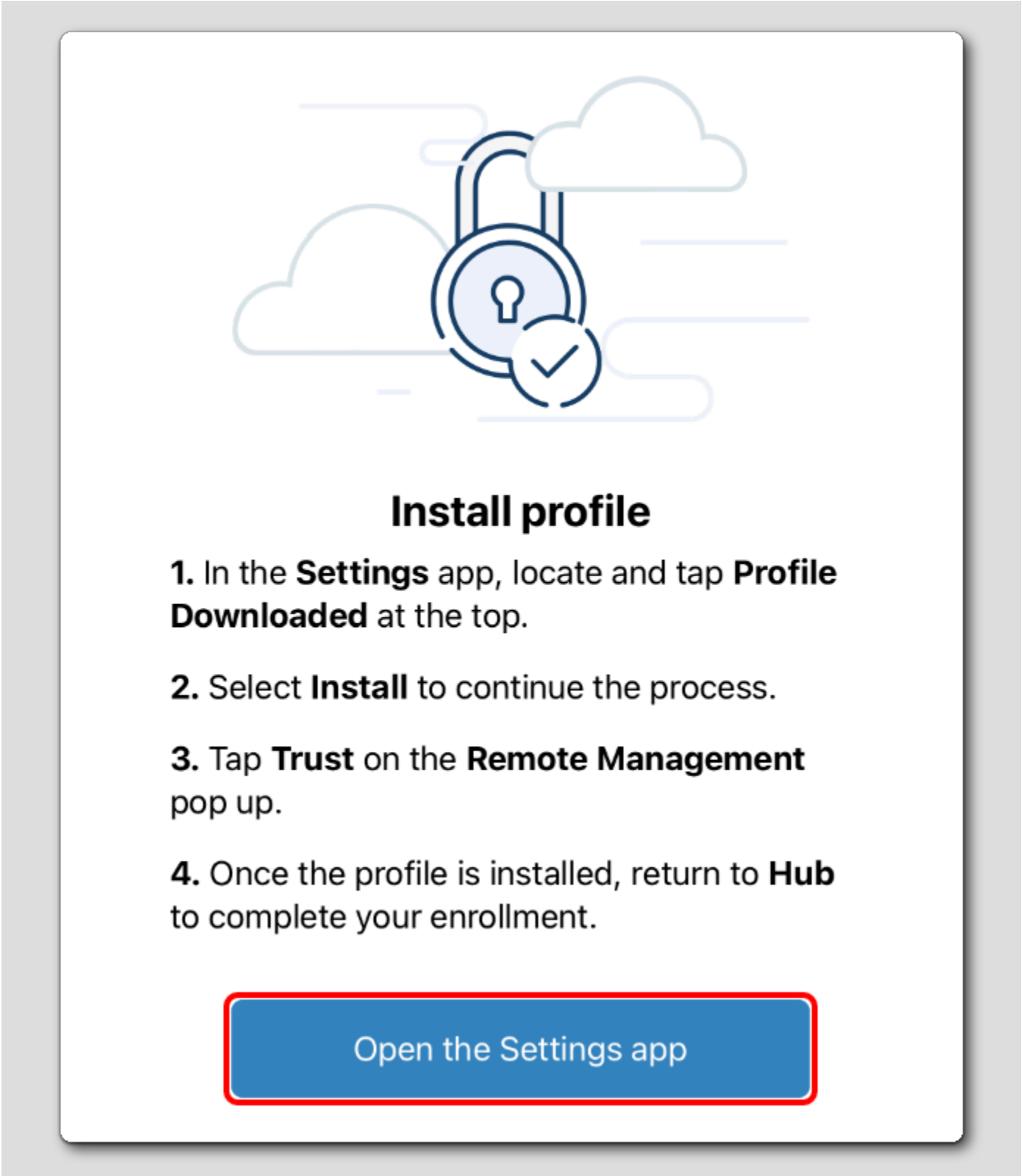


次の手順では、構成プロファイルをインストールしてデバイスを Workspace ONE UEM に登録します。

[Install profile] をタップして開始します。

Settings アプリケーションを開く

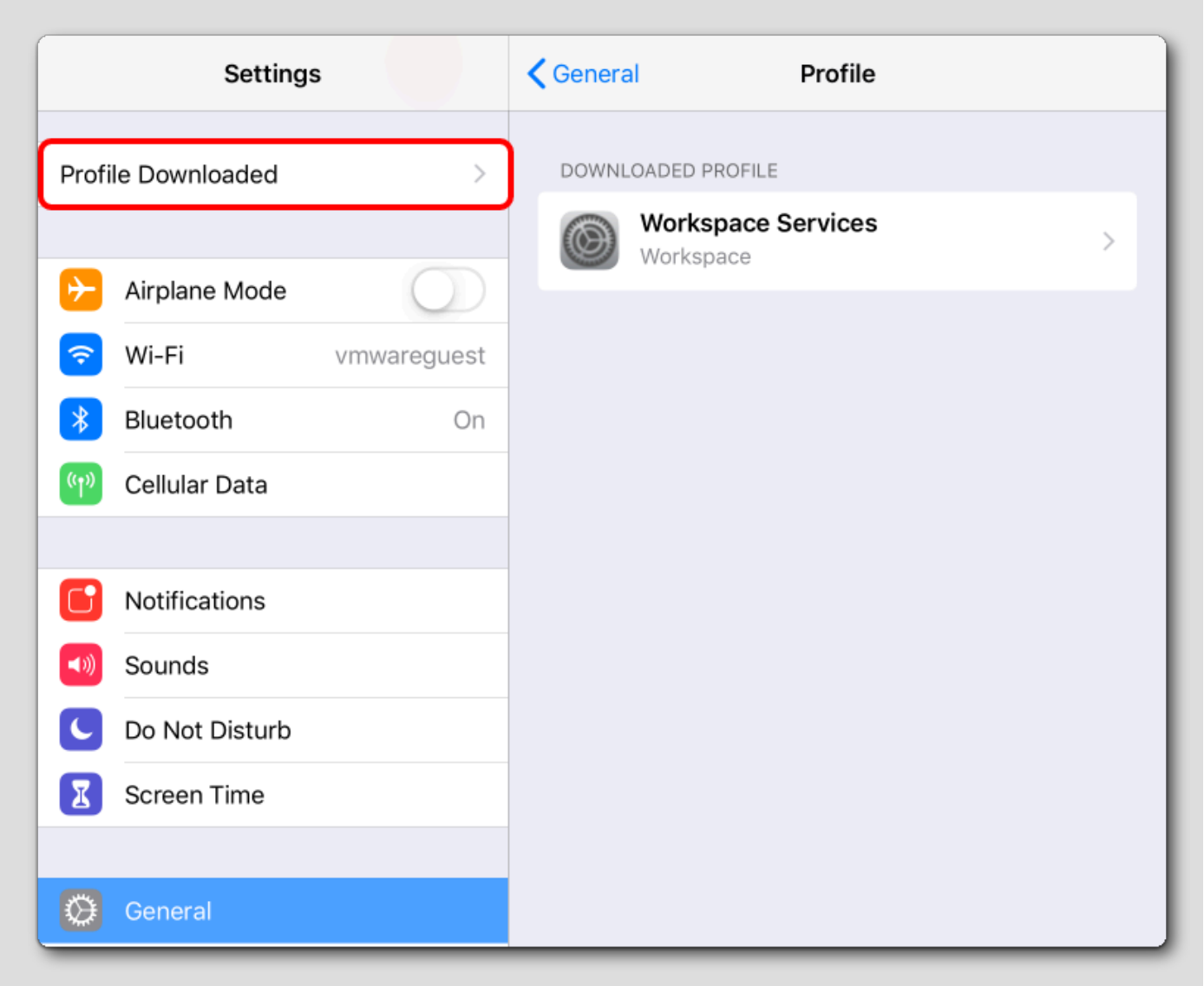
[250]


Install profile
1. In the Settings app, locate and tap Profile Downloaded at the top.
2. Select Install to continue the process.
3. Tap Trust on the Remote Management pop up.
4. Once the profile is installed, return to Hub to complete your enrollment.
Open the Settings app

Settings アプリケーションで登録プロファイルのインストールを完了する方法を説明するプロンプトが表示されます。[Open the Settings app] をタップして続行します。

ダウンロードされたプロファイルを開く

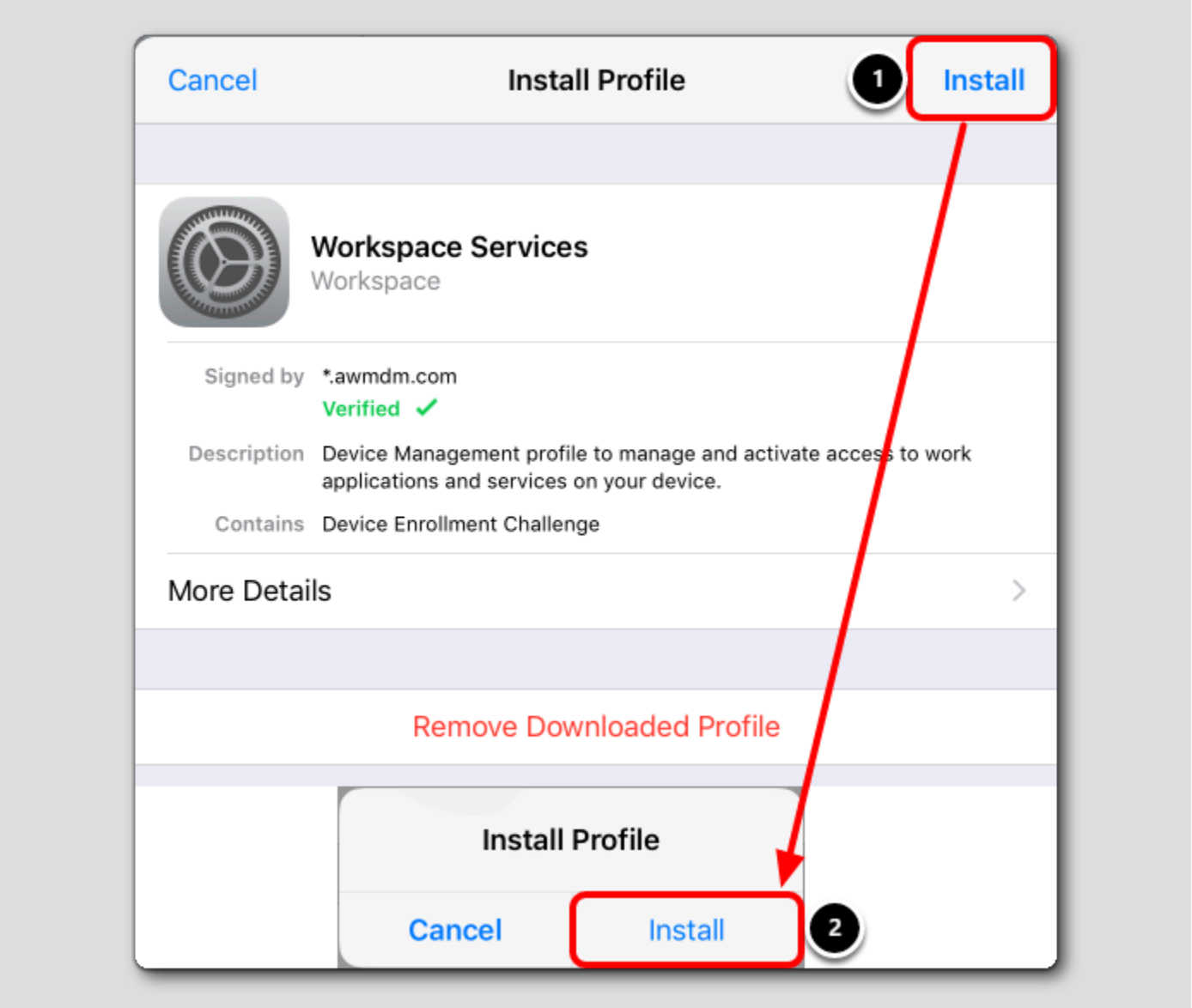
[251]



Settings アプリケーションで、[Settings] メニューの [Profile Downloaded] タブをタップします。

Workspace ONE MDM プロファイルのインストール

[252]



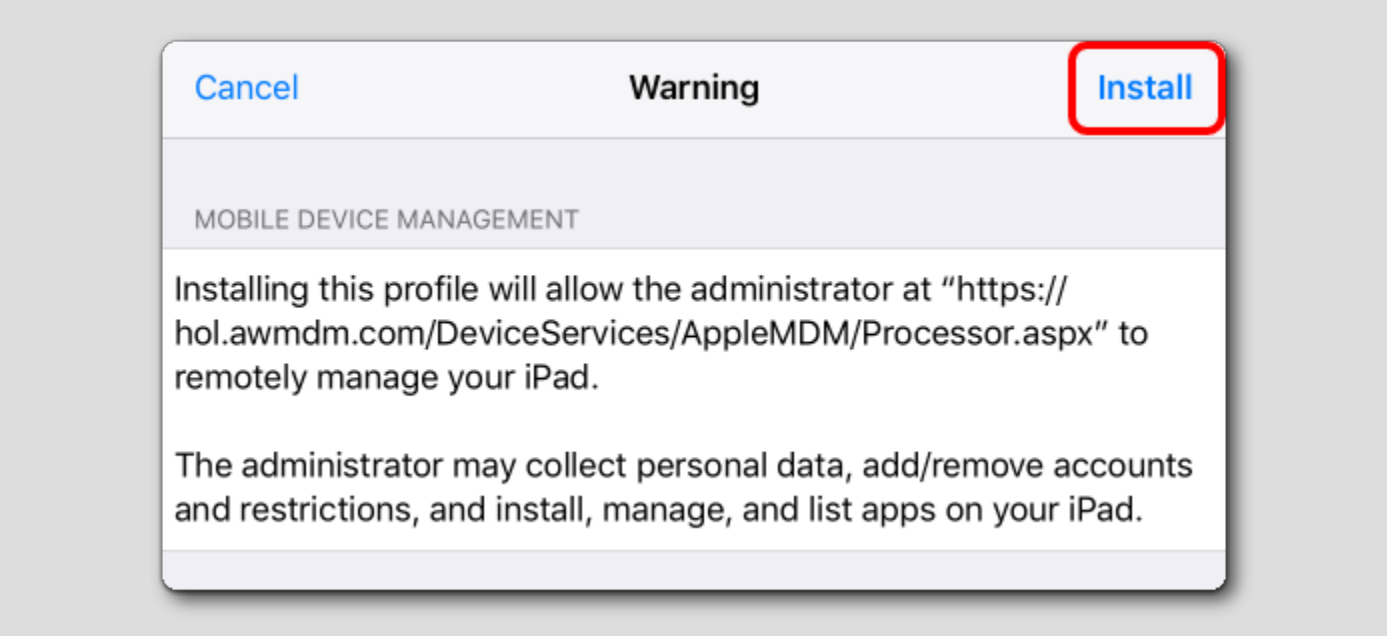
1. [Install Profile] ダイアログ ボックスの右上隅にある [Install] をタップします。

   注：デバイスにパスコードがある場合は、パスコードを入力して続行するように求められます。

2. ポップアップのプロンプトが表示されたら、[Install] をタップして確認します。

iOS MDM プロファイルの警告

[253]

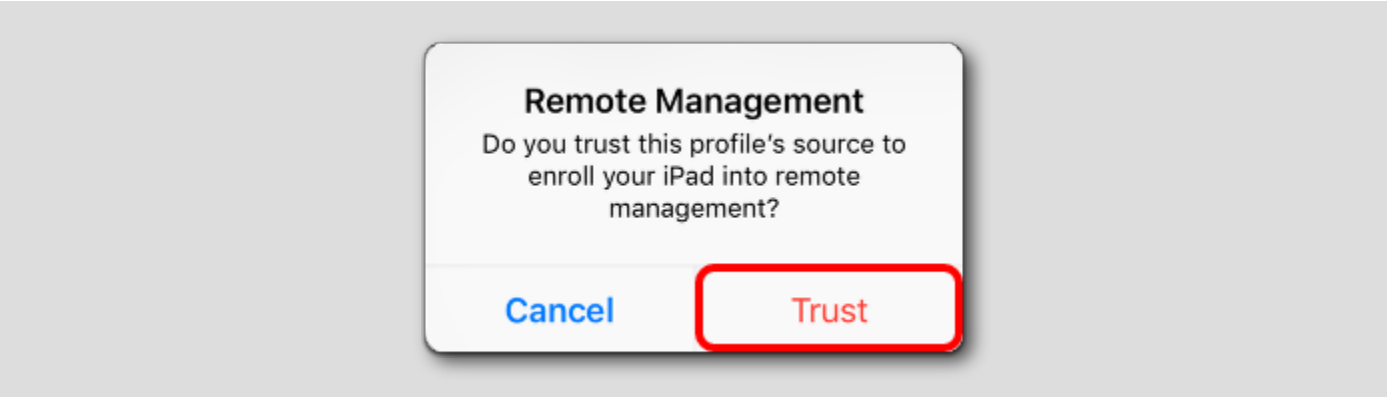


ここで、iOS プロファイルのインストールに関する警告が表示され、このプロファイルをインストールすることにより iOS デバイスで許可される内容が説明されます。

画面右上にある [Install] をタップします。

リモート管理プロファイルの信頼

[254]

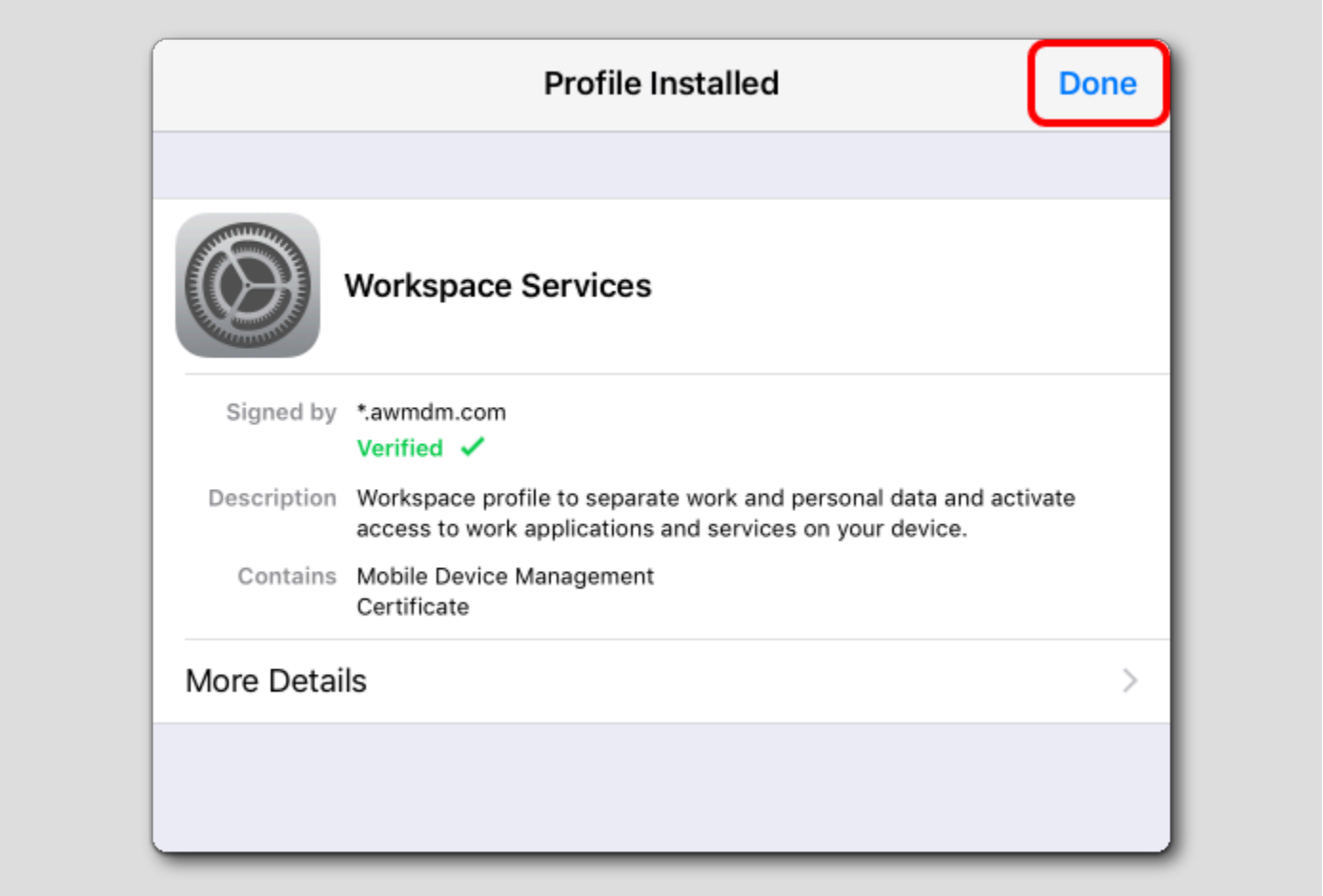


次に、iOS のリクエストで MDM プロファイルのソースを信頼する必要があります。

[Remote Management] ダイアログが表示されたら [Trust] をタップします。

iOS プロファイルのインストールが完了

[255]



iOS プロファイルが正常にインストールされたことを示す画面が表示されます。

プロンプトの右上にある [Done] をタップします。

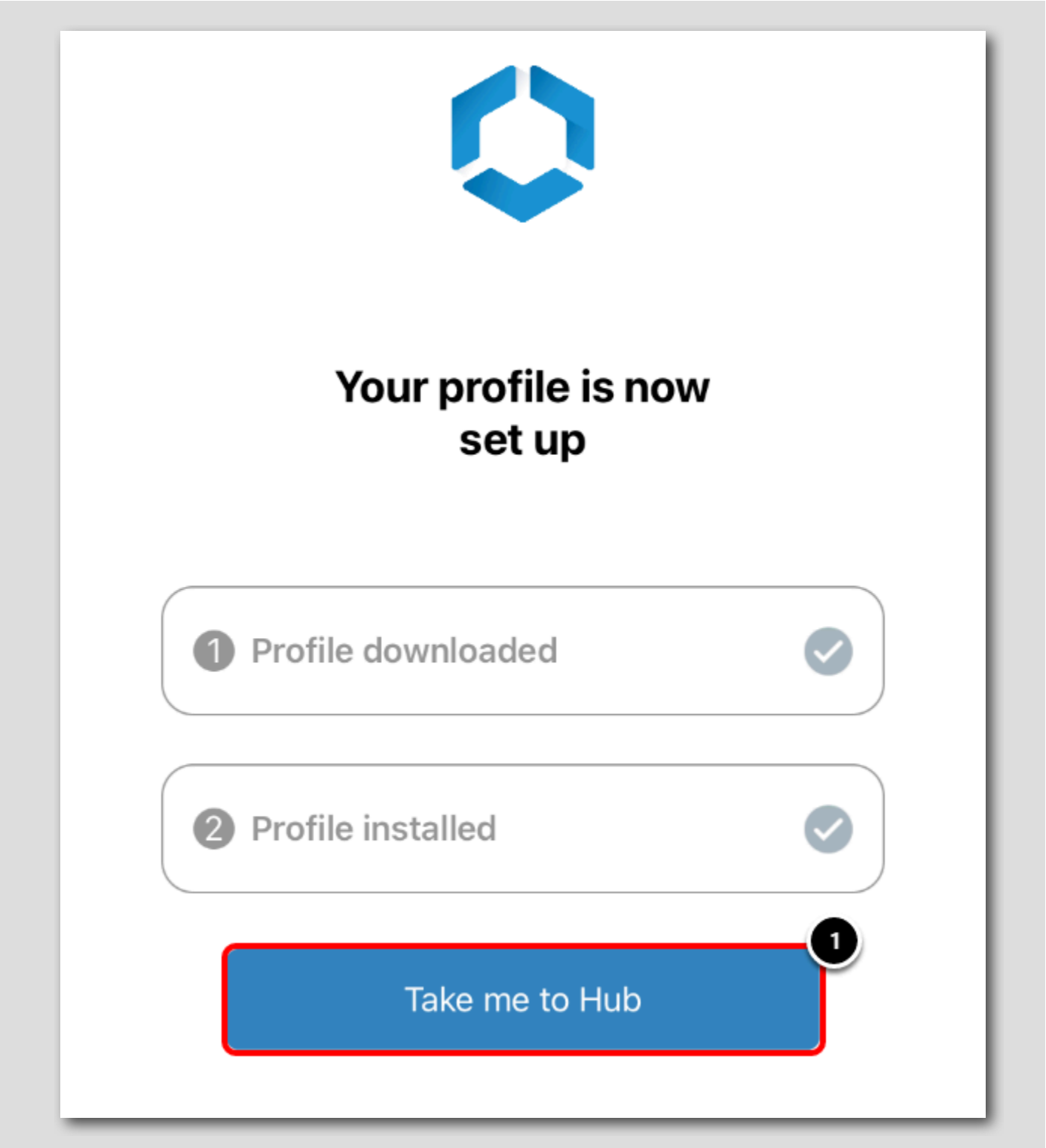
Workspace ONE Intelligent Hub への移動

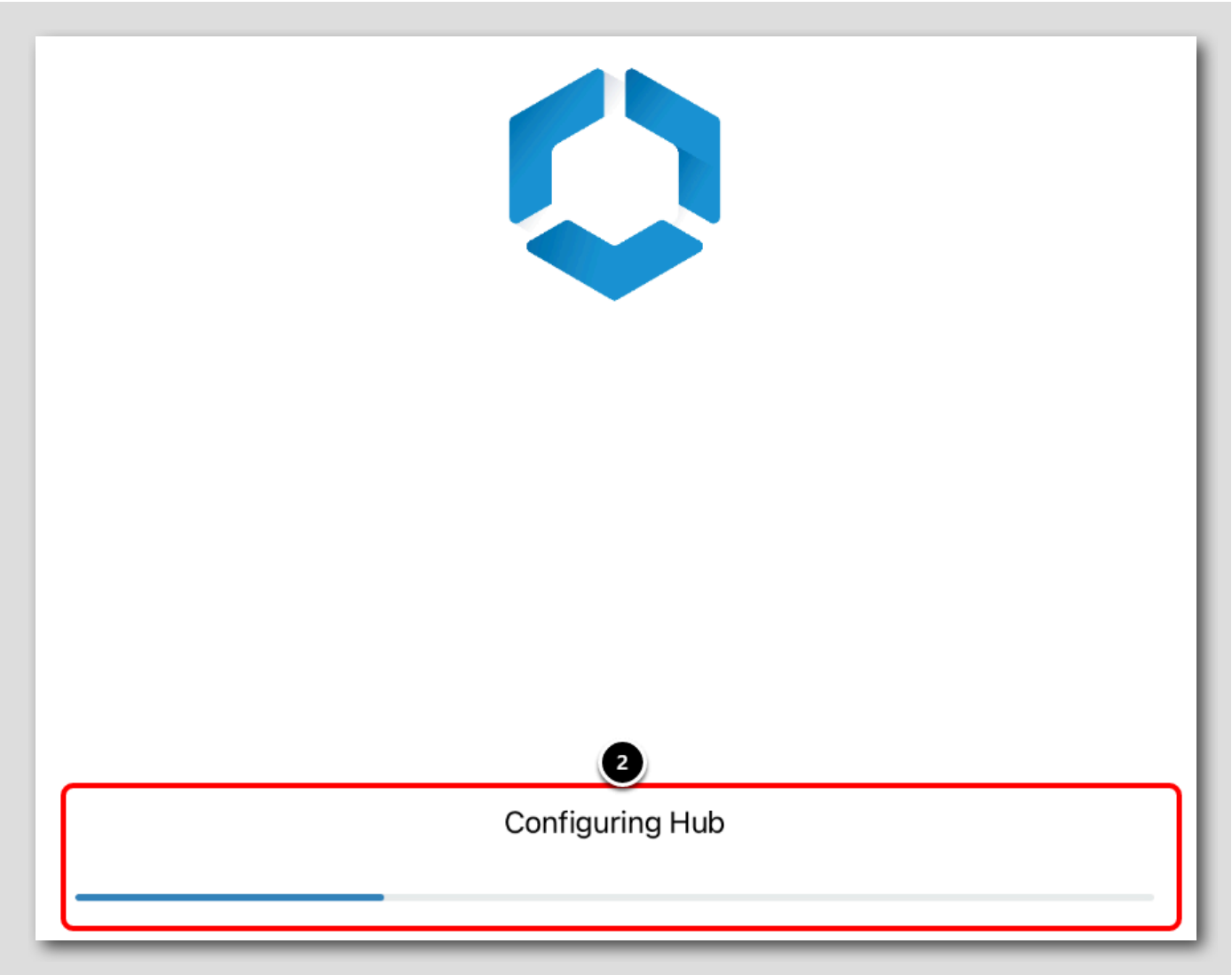
[256]

これで登録が完了しました。[Workspace ONE Intelligent Hub] アプリケーションに戻ります。

[257]

Hub に進む


Your profile is now set up
1 Profile downloaded
2 Profile installed
1
Take me to Hub

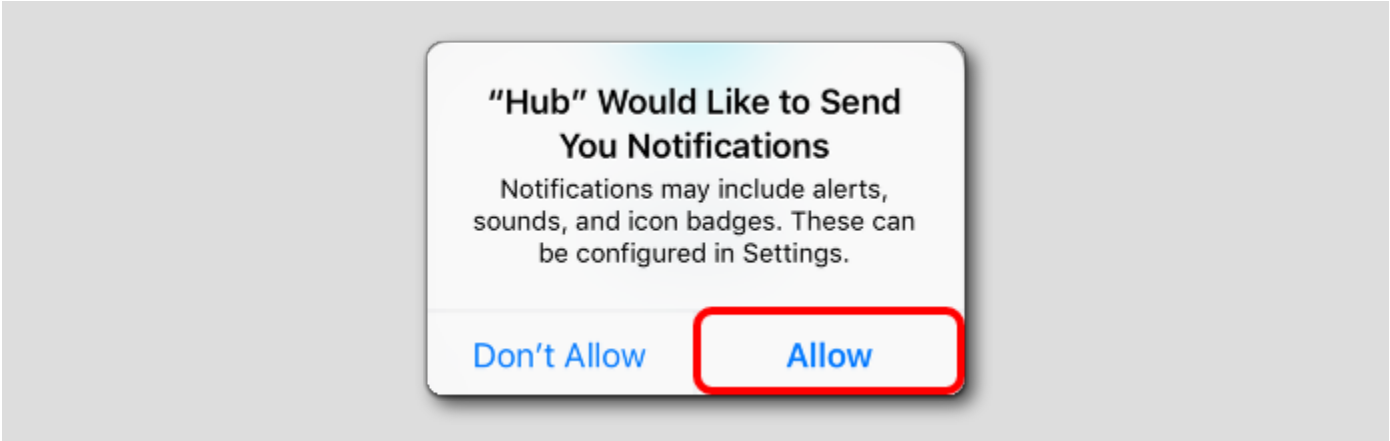


プロファイルが正常に構成されていないことが表示されます。

1. [Take me to Hub] をタップして続行します。
2. [Configuring Hub] ロード バーが表示されます。これが完了するまで待ってから、次の手順に進みます。

Hub の通知を承諾（必要な場合）

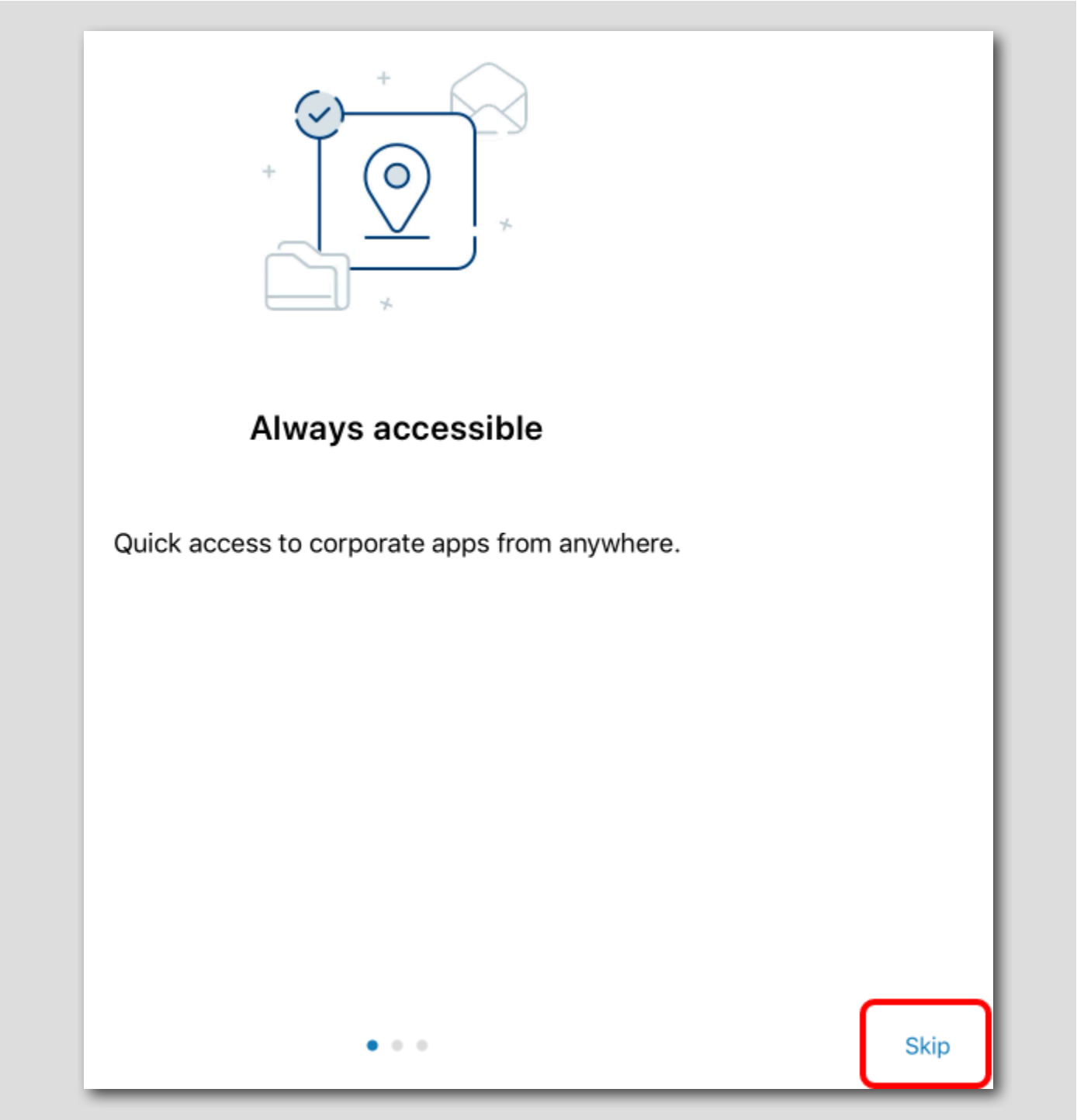
[258]



Hub アプリケーションの通知を許可するように求めるメッセージが表示されたら、[Allow] をタップします。

概要のスキップ（表示された場合）

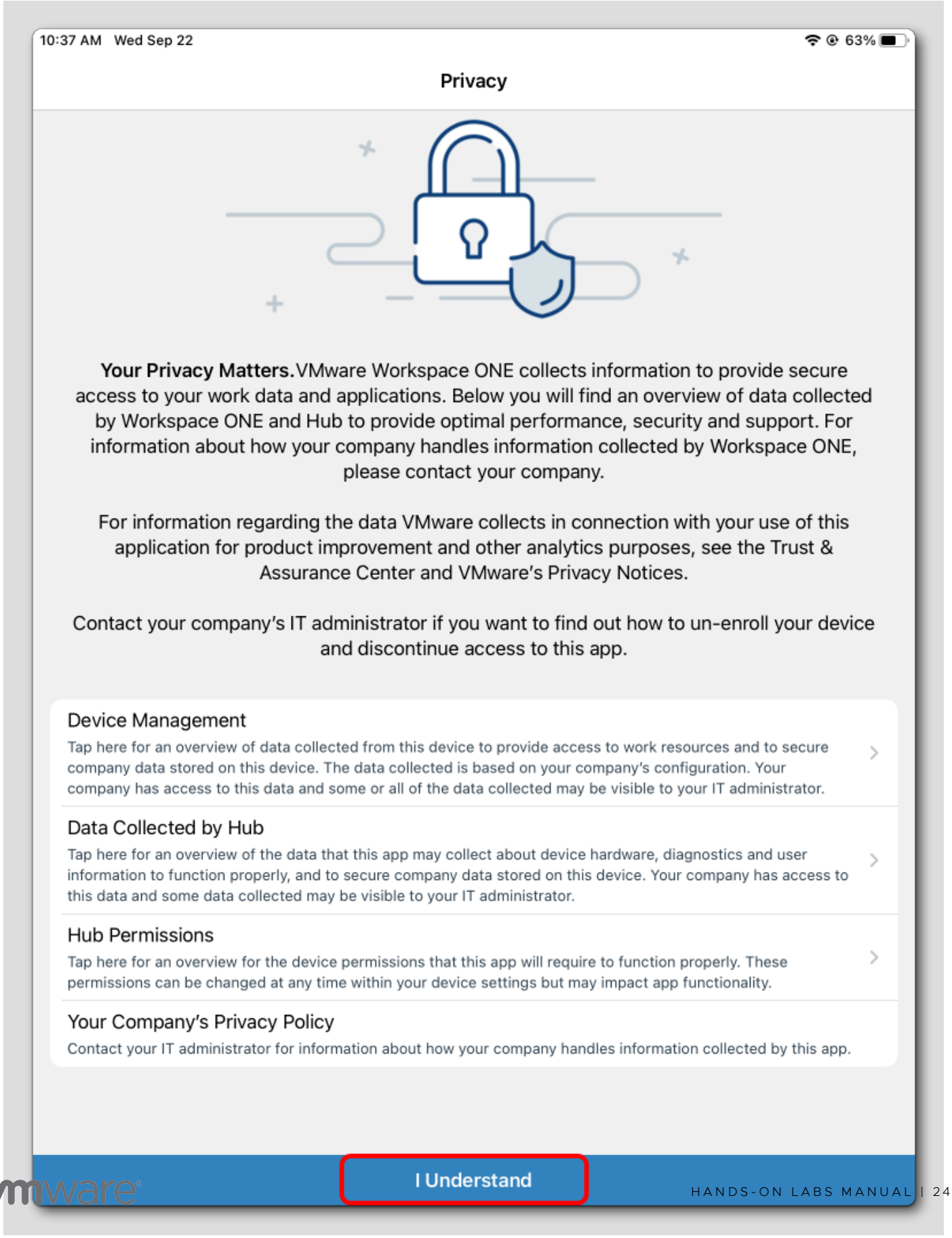
[259]



[Skip] をクリックします。

[260]

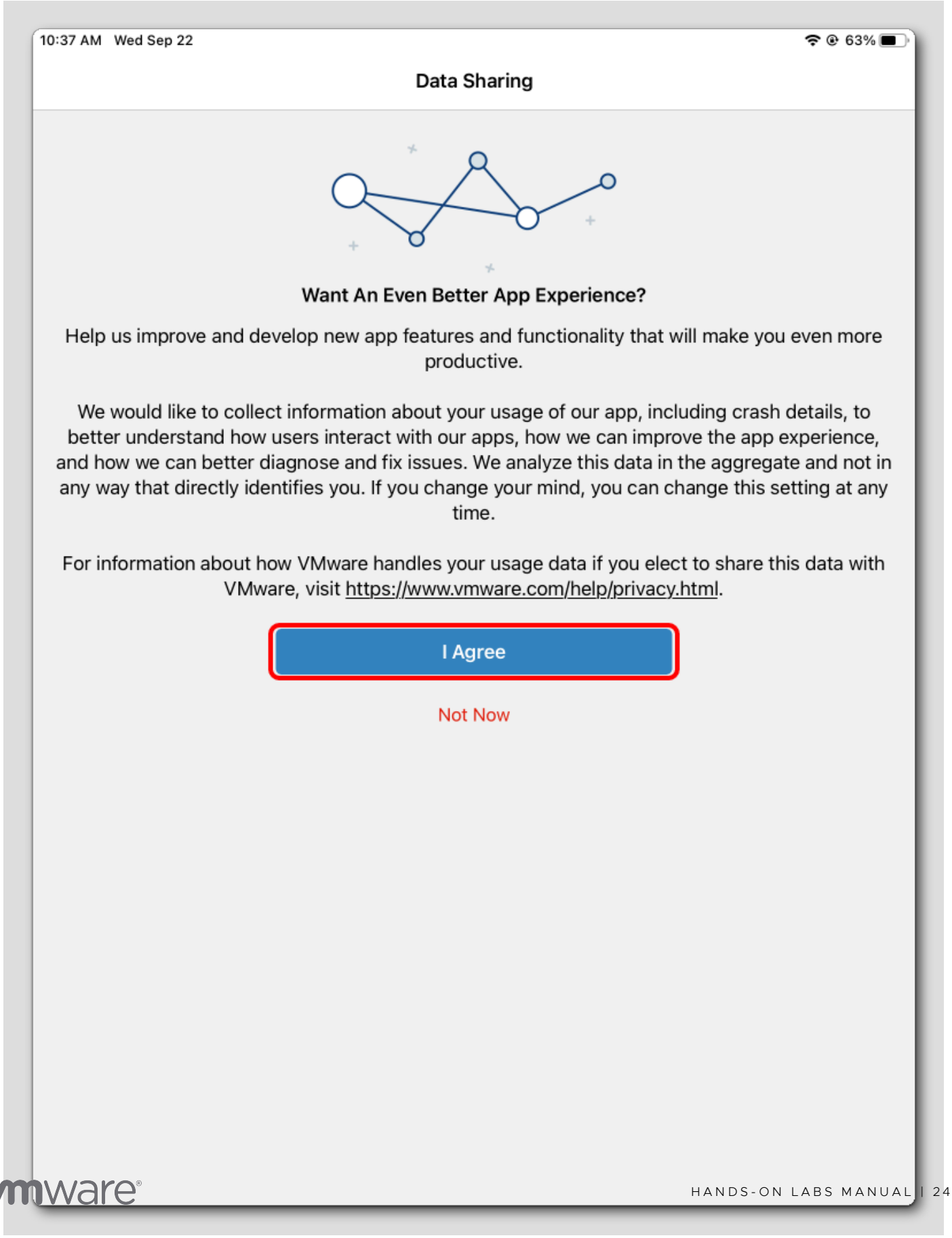
プライバシー ポリシーの確認


10:37 AM Wed Sep 22
63%
Privacy
Your Privacy Matters. VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.
For information regarding the data VMware collects in connection with your use of this application for product improvement and other analytics purposes, see the Trust & Assurance Center and VMware's Privacy Notices.
Contact your company's IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.
Device Management
Tap here for an overview of data collected from this device to provide access to work resources and to secure company data stored on this device. The data collected is based on your company's configuration. Your company has access to this data and some or all of the data collected may be visible to your IT administrator.
Data Collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.
Hub Permissions
Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.
Your Company's Privacy Policy
Contact your IT administrator for information about how your company handles information collected by this app.
I Understand

プライバシー ポリシーが表示されたら、[I Understand] をタップします。

データ共有ポリシーの承諾

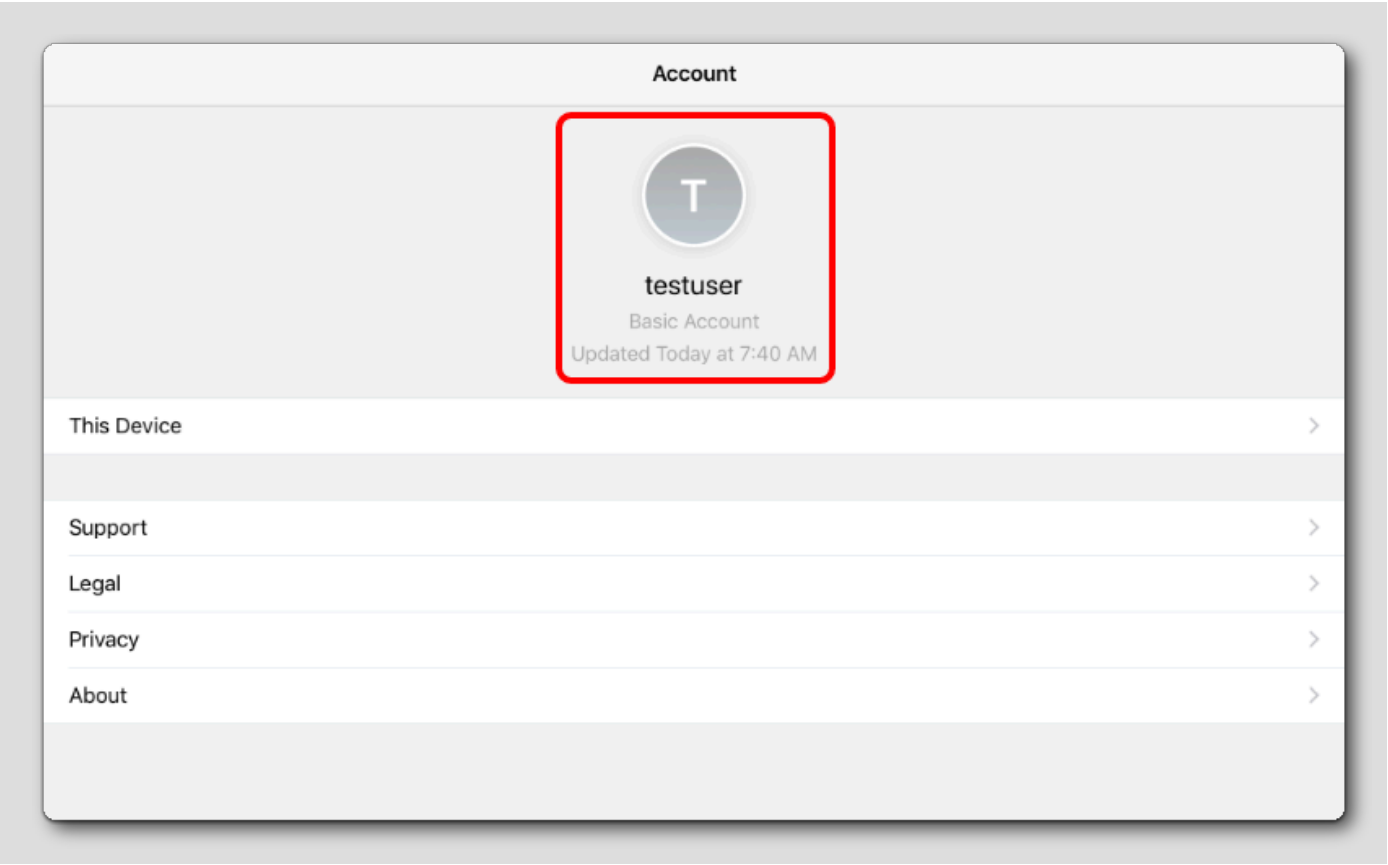
[261]


10:37 AM Wed Sep 22
63%
Data Sharing
Want An Even Better App Experience?
Help us improve and develop new app features and functionality that will make you even more productive.
We would like to collect information about your usage of our app, including crash details, to better understand how users interact with our apps, how we can improve the app experience, and how we can better diagnose and fix issues. We analyze this data in the aggregate and not in any way that directly identifies you. If you change your mind, you can change this setting at any time.
For information about how VMware handles your usage data if you elect to share this data with VMware, visit https://www.vmware.com/help/privacy.html.
I Agree
Not Now

データ共有ポリシーに対して [I Agree] をタップします。

Hub アプリケーションでのデバイス登録の確認

[262]



Hub アプリケーションに、登録に使用したユーザー アカウント (testuser) が表示されていることを確認します。

これで、Workspace ONE UEM に iOS デバイスが正常に登録されました。次の手順に進みます。

制限事項プロファイル適用後のデバイスの確認

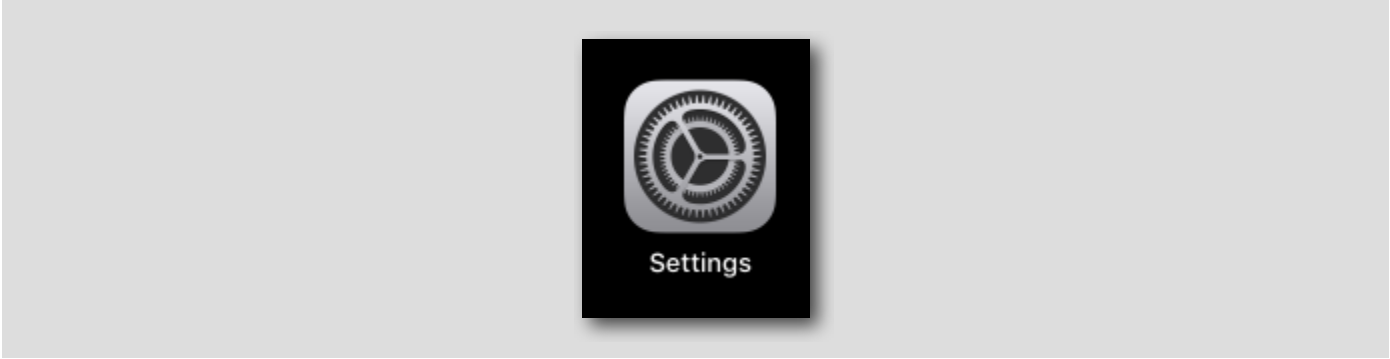
[263]

ここでは、デバイスで Siri を無効にするための制限事項プロファイルが期待どおりに適用されることを確認します。制限事項プロファイルを確認するには、次の 2 つの方法があります。

1. 前の手順でデバイスにインストールされたモバイル デバイス管理プロファイルを検査し、制限事項が存在することを確認する。
2. デバイス上で Siri の操作を試みる。

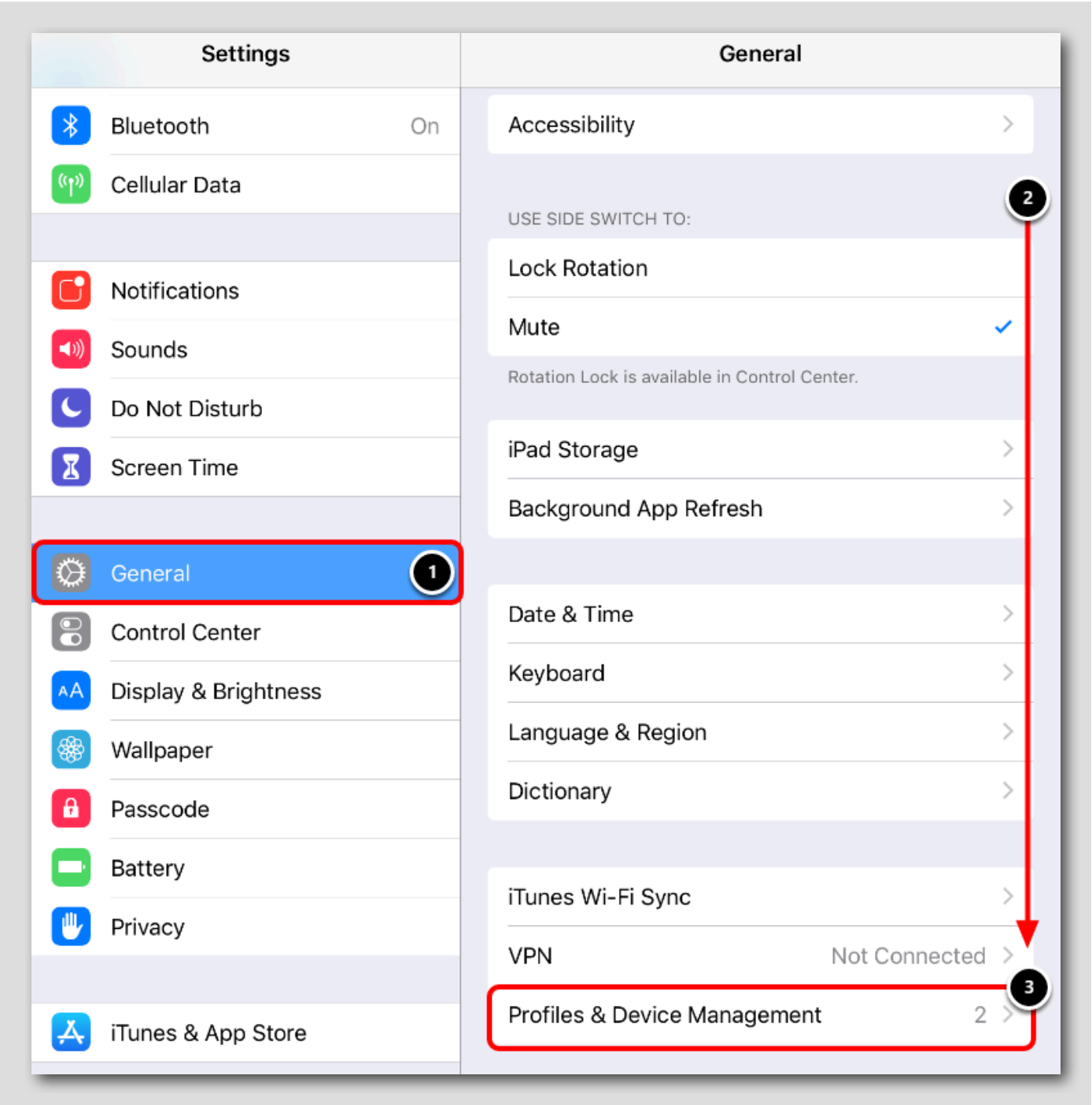
[Settings] での制限事項プロファイルの確認

[264]



Settings アプリケーションをタップします。

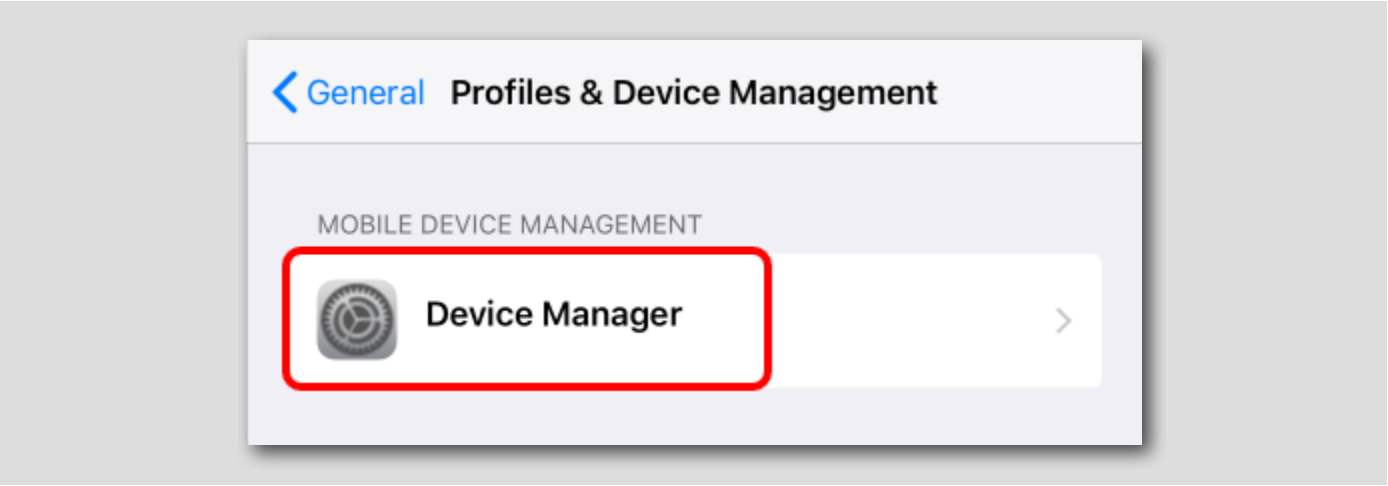
[Profiles & Device Management] への移動 [265]



1. [General] をタップします。
2. 下にスクロールして [Profiles & Device Management] オプションを見つけます。
3. [Profiles & Device Management] をタップします。

[Device Manager] プロファイルを開く

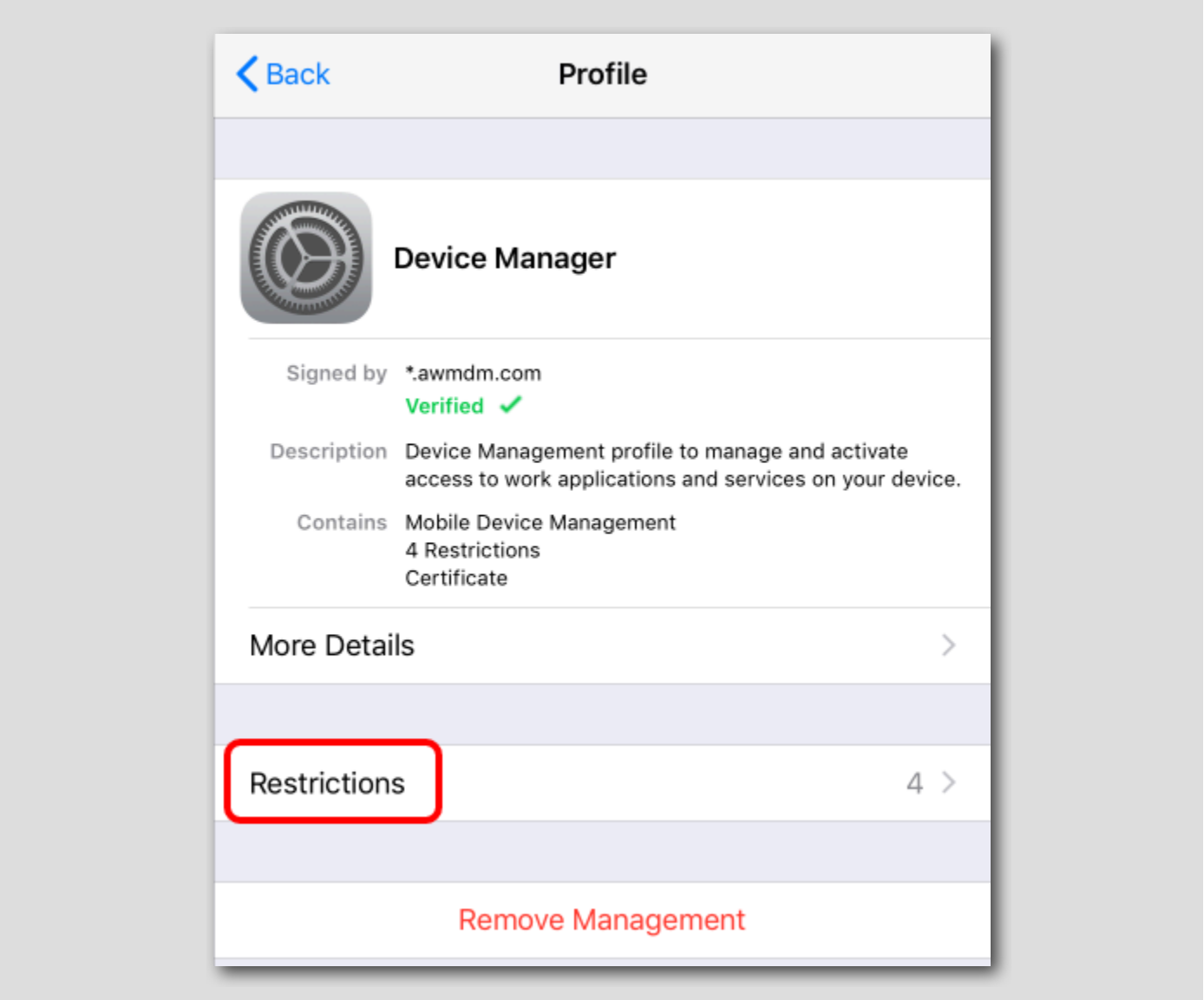
[266]



[Mobile Device Management] の下の [Device Manager] プロファイルをタップします。

制限事項の検査

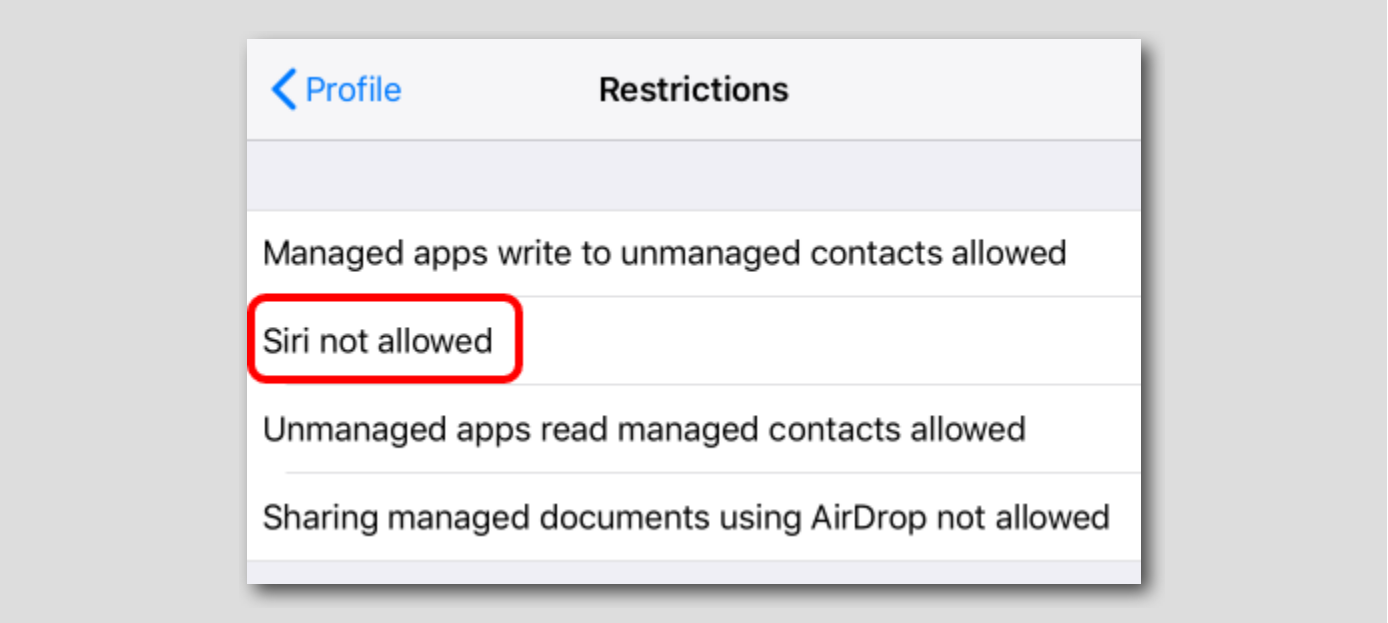
[267]



このプロファイルに関連する制限事項を調べるには、[Restrictions] をタップします。

[Siri not allowed] 制限事項の確認

[268]



[Siri not allowed] 制限事項がリストに含まれていることを確認します。

デバイスで Siri が無効になっていることの確認

[269]

ホーム ボタンを押したままにして、デバイス上の Siri を再度アクティブ化してみると、Siri が応答しなくなったことを確認できます。

Settings アプリケーションに移動すると、[Siri & Search] 設定もデバイスで使用できなくなっていることがわかります。

iOS デバイスの登録解除

[270]

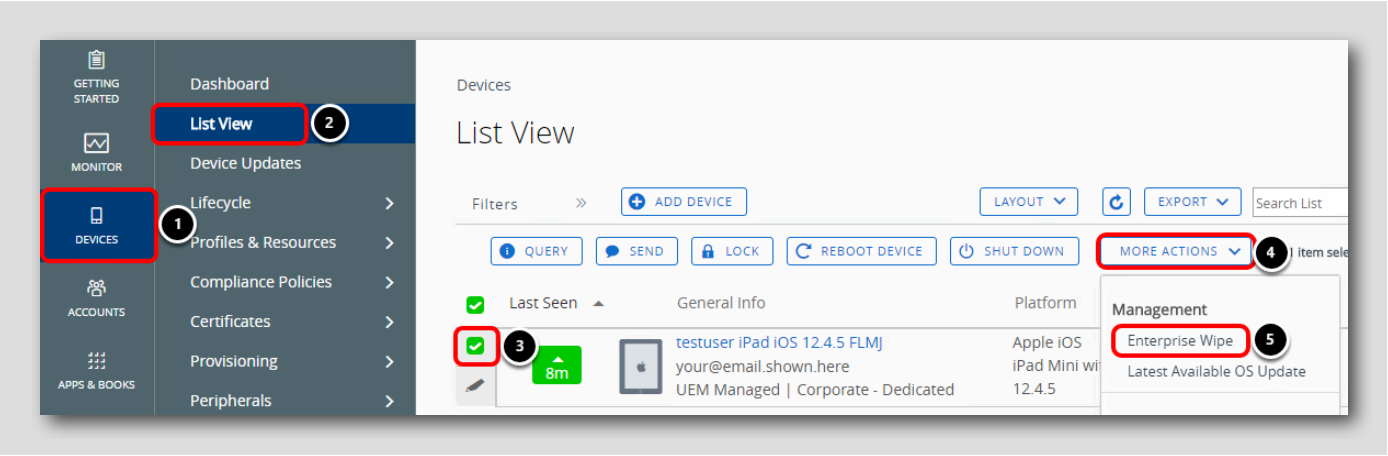
次に、Workspace ONE UEM から iOS デバイスの登録を解除します。

注: 「企業情報ワイプ」という用語は、デバイスのリセットまたは完全なワイプを意味するものではありません。これは、Workspace ONE Intelligent Hub が制御する MDM プロファイル、ポリシー、およびコンテンツのみを削除します。

Workspace ONE Intelligent Hub アプリケーションは、ユーザーが Workspace ONE UEM に登録される前に手動でダウンロードされたため、デバイスから削除されません。

iOS デバイスの企業情報ワイプ（登録解除）

[271]



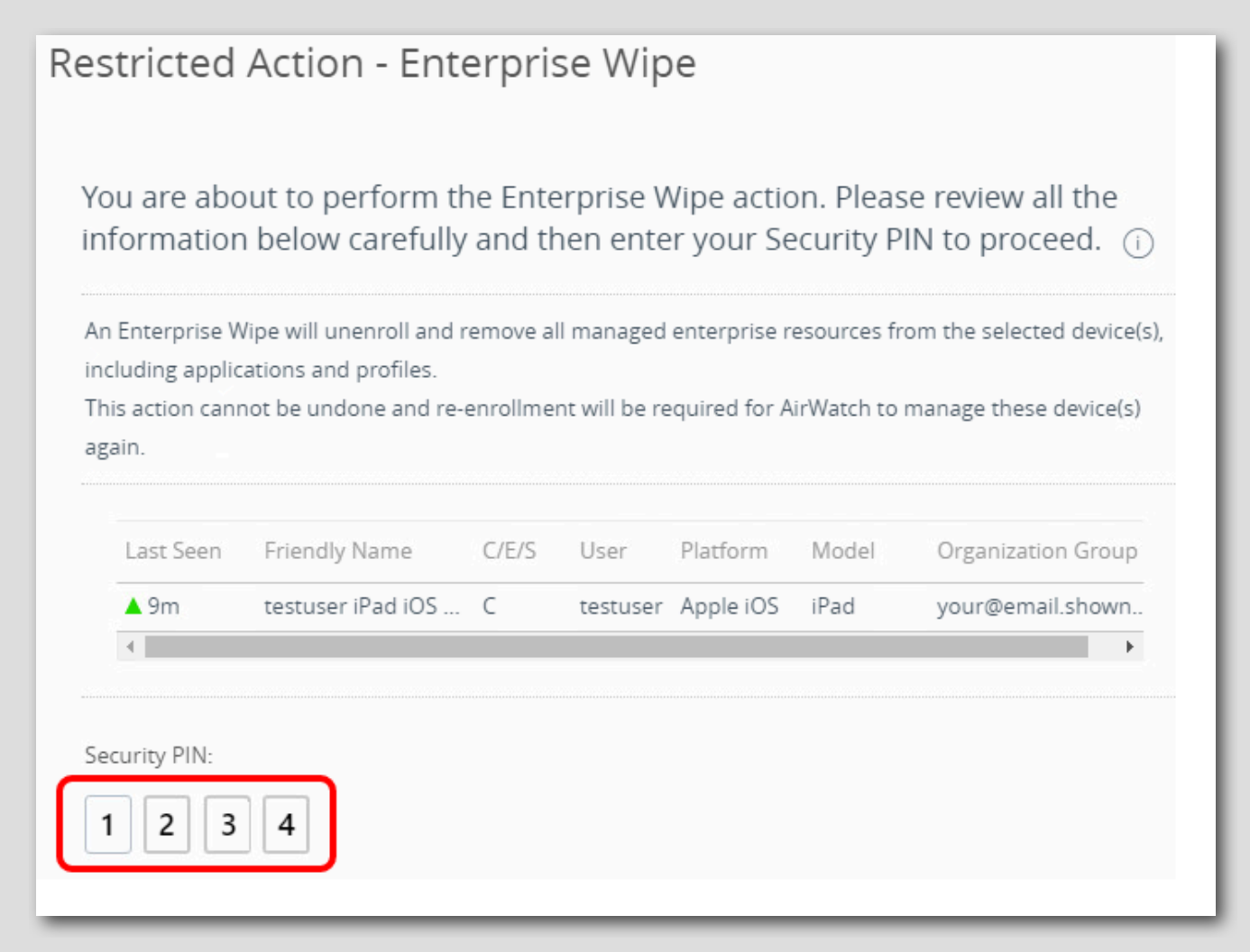
「企業情報ワイプ」では、登録後にデバイスにプッシュされたすべての設定とコンテンツが削除されます。登録前にすでにデバイス上にあった設定とコンテンツには影響しません。

Workspace ONE UEM Console に戻ります。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. 企業情報ワイプを行うデバイスの横のチェックボックスをクリックします。
4. [More Actions] をクリックします。
5. [Enterprise Wipe] をクリックします。

セキュリティ PIN の入力

[272]



[Enterprise Wipe] を選択すると、Workspace ONE UEM Console へのログイン後に設定したセキュリティ PIN (**1234**) を入力するよう求められます。

[Security PIN] に **1234** と入力します。Enter キーや [Continue] を押さなくても、PIN が正しいことを確認する「Successful」というメッセージがセキュリティ PIN 入力フィールドの下に表示されて、企業情報ワイプが要求されたことが示されます。

注：**1234** が機能しない場合は、Workspace ONE UEM Console に最初にログインしたときに別のセキュリティ PIN が指定されています。セキュリティ PIN に指定した値を使用します。

注：企業情報ワイプがすぐに実行されない場合は、次の手順に従って強制的にデバイスの同期を実行します。

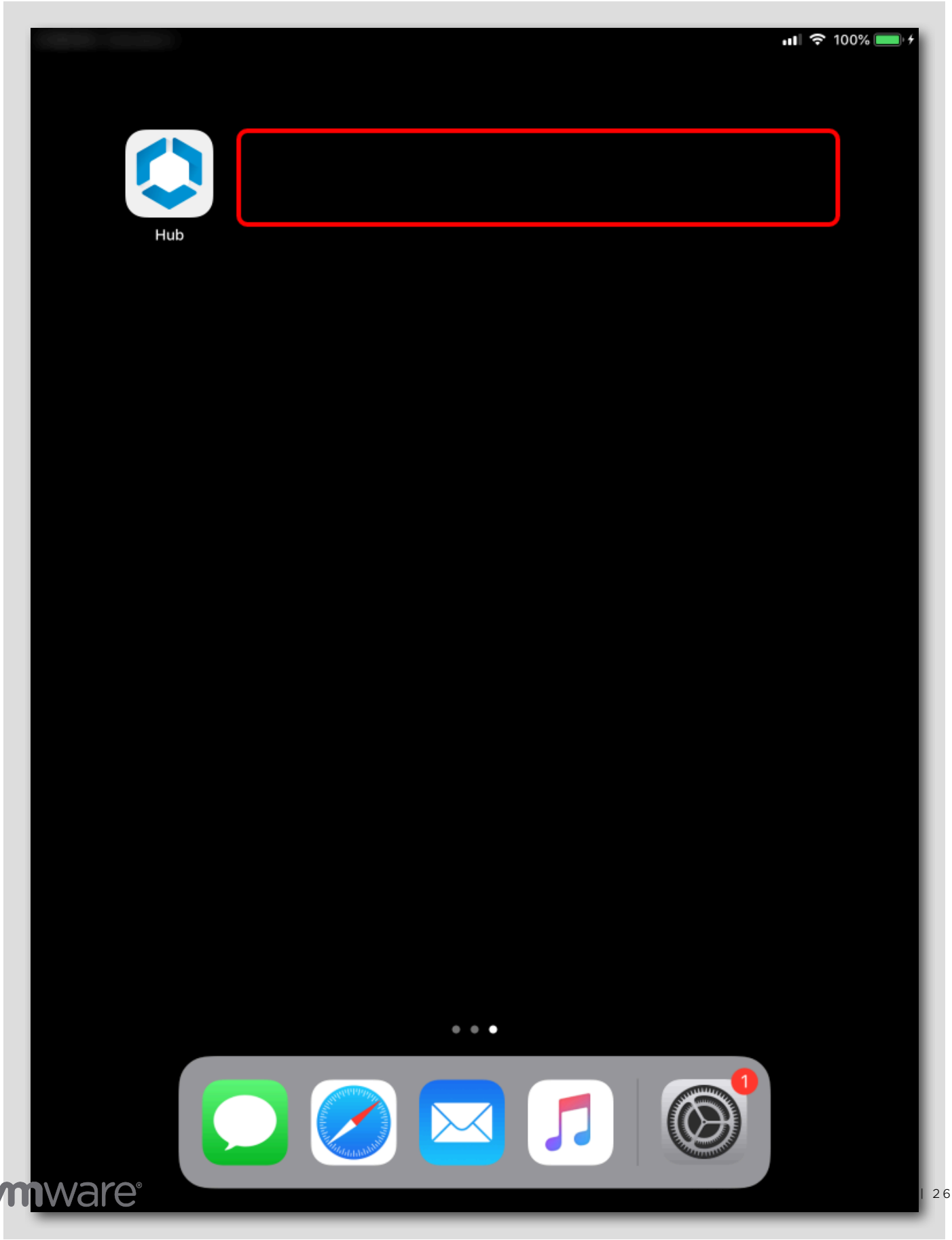
1. デバイスで [Workspace ONE Intelligent Hub] アプリケーションをタップします。
2. [This Device] をタップします。
3. 画面上部の近くにある [Send Data] をタップします。これによってデバイスのチェックインが行われず、すぐに登録解除されない場合は、手順 #4 に進みます。
4. 上記の操作で登録がすぐに解除されない場合は、[Diagnostics] で [Connectivity [Status]] をタップします。
5. 画面上部にある [Test Connectivity] をタップします。

注：ハンズオン ラボ環境内で大量のトラフィックが発生している場合、デバイスのインターネット接続やラボのインフラストラクチャの即応性によっては、この処理に 2 ～ 3 分以上かかることがあります。

ネットワークに接続できない場合は、「ワイプの強制実行」の手順に進んで、手動で Workspace ONE UEM サービスをデバイスからアンインストールできます。

登録解除の確認

[273]

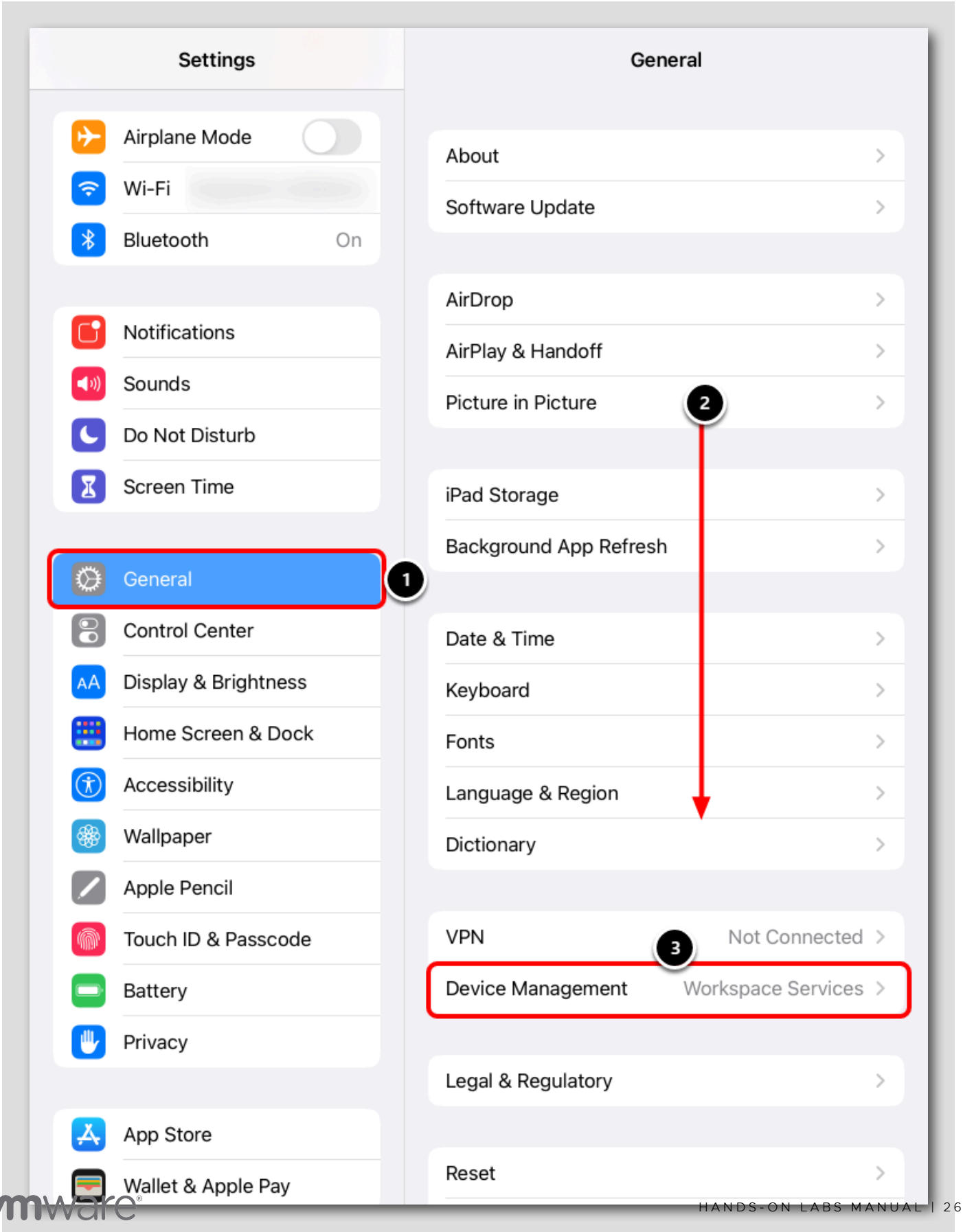

100%
Hub

デバイスのスプリングボードに戻ります。Workspace ONE UEM によってプッシュされたアプリケーションがデバイスから削除されていることを確認します。さらに、[Settings] > [General] > [Profiles] の順に移動すると、デバイスから Workspace Services プロファイルが削除され、プッシュされた構成が元に戻ります。

注：Workspace ONE Intelligent Hub は、App Store から手動でダウンロードされたため、デバイス上に残っています。ラボの環境設定によっては、信号がさまざまなネットワークを経由してデバイスに戻ってくるまでに、ある程度の時間がかかる場合があります。必要な場合は、次の手順に進み、強制的にワイプを実行します。

[274]

ワイプの強制実行（必要な場合）

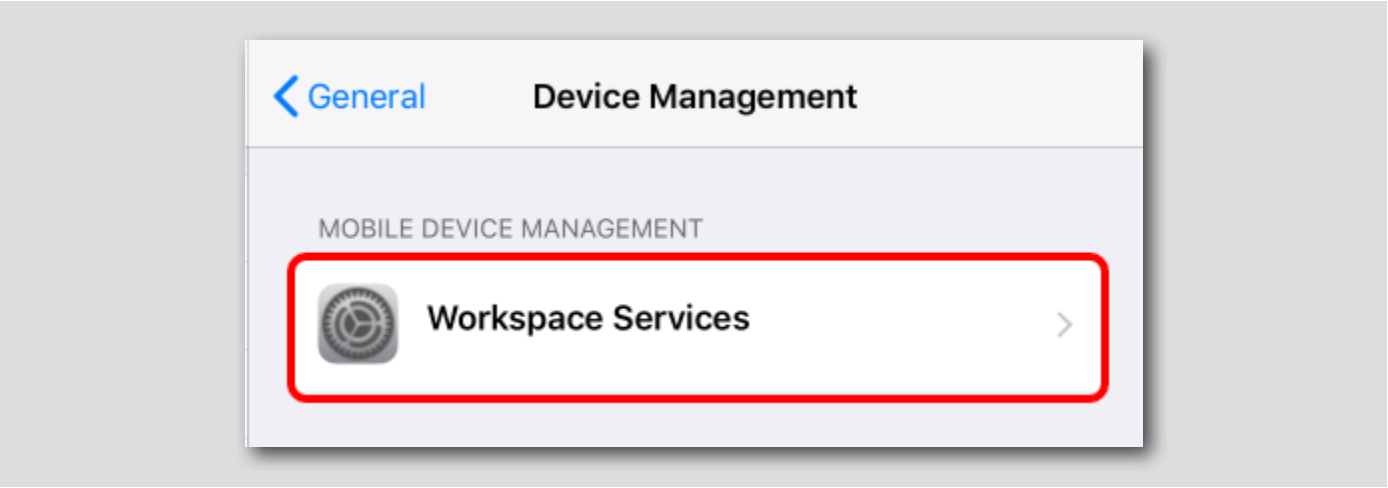

Settings
Airplane Mode
Wi-Fi
Bluetooth
On
Notifications
Sounds
Do Not Disturb
Screen Time
General
1
Control Center
Display & Brightness
Home Screen & Dock
Accessibility
Wallpaper
Apple Pencil
Touch ID & Passcode
Battery
Privacy
App Store
Wallet & Apple Pay
General
About
Software Update
AirDrop
AirPlay & Handoff
Picture in Picture
2
iPad Storage
Background App Refresh
Date & Time
Keyboard
Fonts
Language & Region
Dictionary
VPN
Not Connected
3
Device Management
Workspace Services
Legal & Regulatory
Reset

デバイスでワイプが実行されなかった場合は、次の手順で直ちにワイプを強制実行します。まず、iOS Settings アプリケーションを開きます。

1. 左側の列で [一般] を選択します。
2. 下にスクロールして [Device Management] オプションを表示します。
3. [General] 設定のリストの一番下にある [Device Management] をタップします。

ワイプの強制実行（必要な場合）

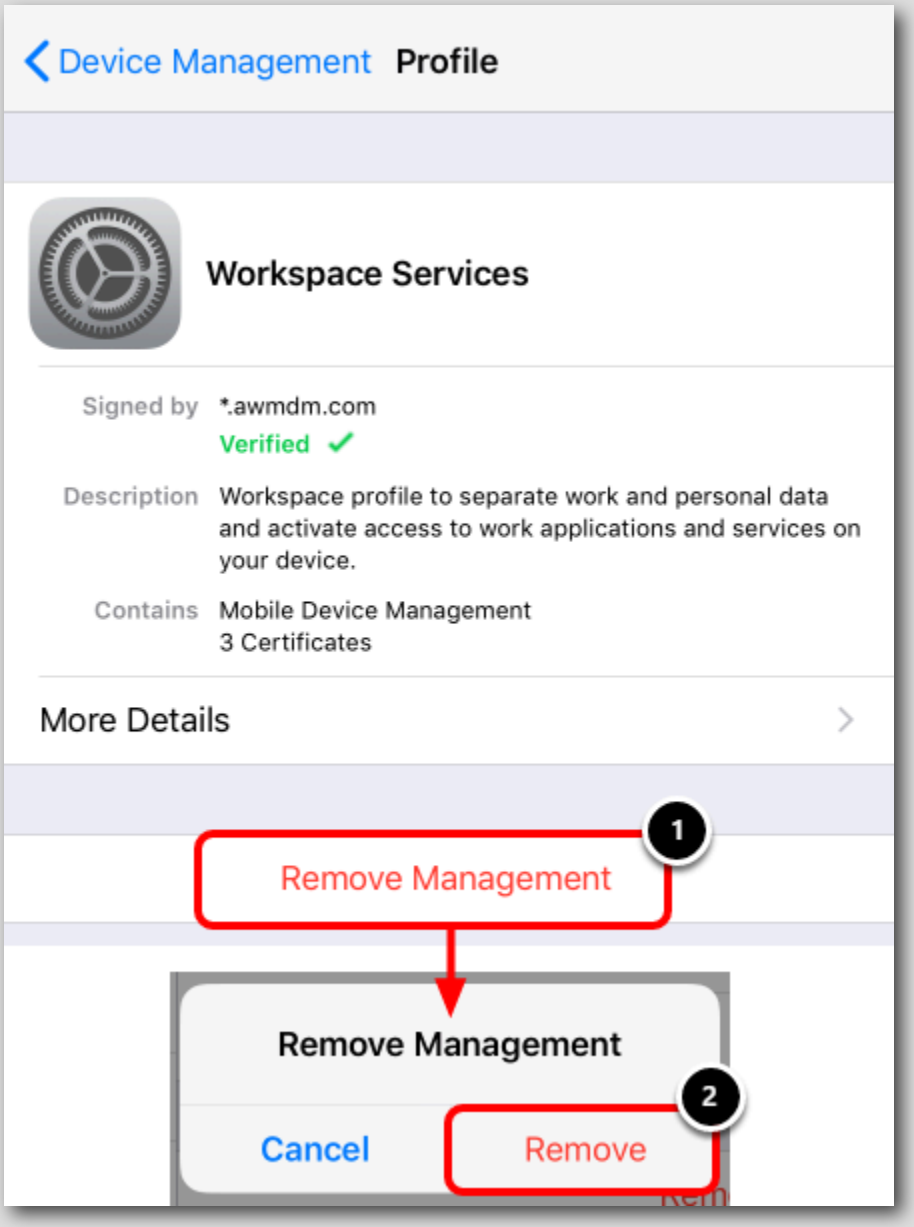
[275]



デバイスに適用した [Device Manager] プロファイルをタップします。

ワイプの強制実行（必要な場合）

[276]



1. [Workspace Services] プロファイルで **[Remove Management]** をタップします。

   注：デバイス PIN の入力を求められたら、入力して続行します。

2. [Remove Management] プロンプトで **[Remove]** をタップします。

[Device Manager] プロファイルを削除すると、デバイスの登録が解除されます。いつでも「**登録解除の確認**」の手順に戻って、デバイスの登録解除が正常に完了したことを確認できます。

登録解除後のデバイスの確認

[277]

デバイスの登録が解除されると、Siri を無効にするためにプッシュした制限事項は削除されますが、デバイスの他の要素は変更されません。Siri を再度アクティブ化し、Siri が機能するようになったことを確認します。

まとめ

[278]

管理者は、Workspace ONE UEM を使用してデバイスを管理することで、ユーザーのプライバシーに違反することなく、デバイスが正常に動作し、企業リソースにアクセスしていることを確認できます。デバイスを登録し、プロファイルをプッシュする方法を確認したので、次に、このモジュールで説明している他のラボ トピックを確認して Workspace ONE UEM の知識をさらに広げましょう。

これで、「Apple iOS 管理の概要」モジュールは終了です。

このハンズオン ラボでは、Workspace ONE で iOS と tvOS を管理するためのすべての機能を網羅していないことに注意してください。iOS/tvOS 管理の高度なトピックに役立つビデオ、ブログ、およびドキュメントについては、次のような VMware の TechZone を参照してください。

- Apple Business Manager と自動デバイス登録
- デバイスのステージングと代理登録
- Volume 購入済みアプリケーションの展開
- キオスク モード
- 証明書と ID/ディレクトリの統合
- 生産性向上アプリケーション
- チェックイン、チェックアウト
- Hub サービスと VMware Access による統合されたアプリケーション カタログとシングル サインオン
- Apple Education との連携（例：Apple School Manager）
- その他

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[279]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。

モジュール 4：Apple macOS 管理の概要（45 分）

はじめに

[281]

このラボ モジュールでは、macOS プラットフォームで利用可能な、いくつかの Workspace ONE 管理機能と概念について説明します。このラボでは、macOS デバイスの登録方法および使用可能な管理オプションについて確認し、これらのオプションが macOS の構成とアプリケーションの公開を通じてユーザー エクスペリエンスにもたらす改善と影響について理解を深めることができます。

このラボを修了するには、あらかじめ次のページを確認しておく必要があります。

前提条件

[282]

このハンズオン ラボを修了するには、次のものが必要となります。

- macOS バージョン 10.14.0 (Mojave) 以降を実行している Apple デバイス。

個人の macOS デバイスを登録しないでください

[283]

重要: 今後の演習のために個人のデバイスを登録しないでください。

個人のデバイスが他の UEM プロバイダーに登録されると、望ましくない競合や問題が発生する可能性があります。

このラボを完了するには、テスト デバイスのみを使用し、個人のデバイスをラボに登録しないことをお勧めします。

Workspace ONE UEM Console へのログイン

[284]

このラボを開始するには、Workspace ONE UEM 管理コンソールにログインする必要があります。

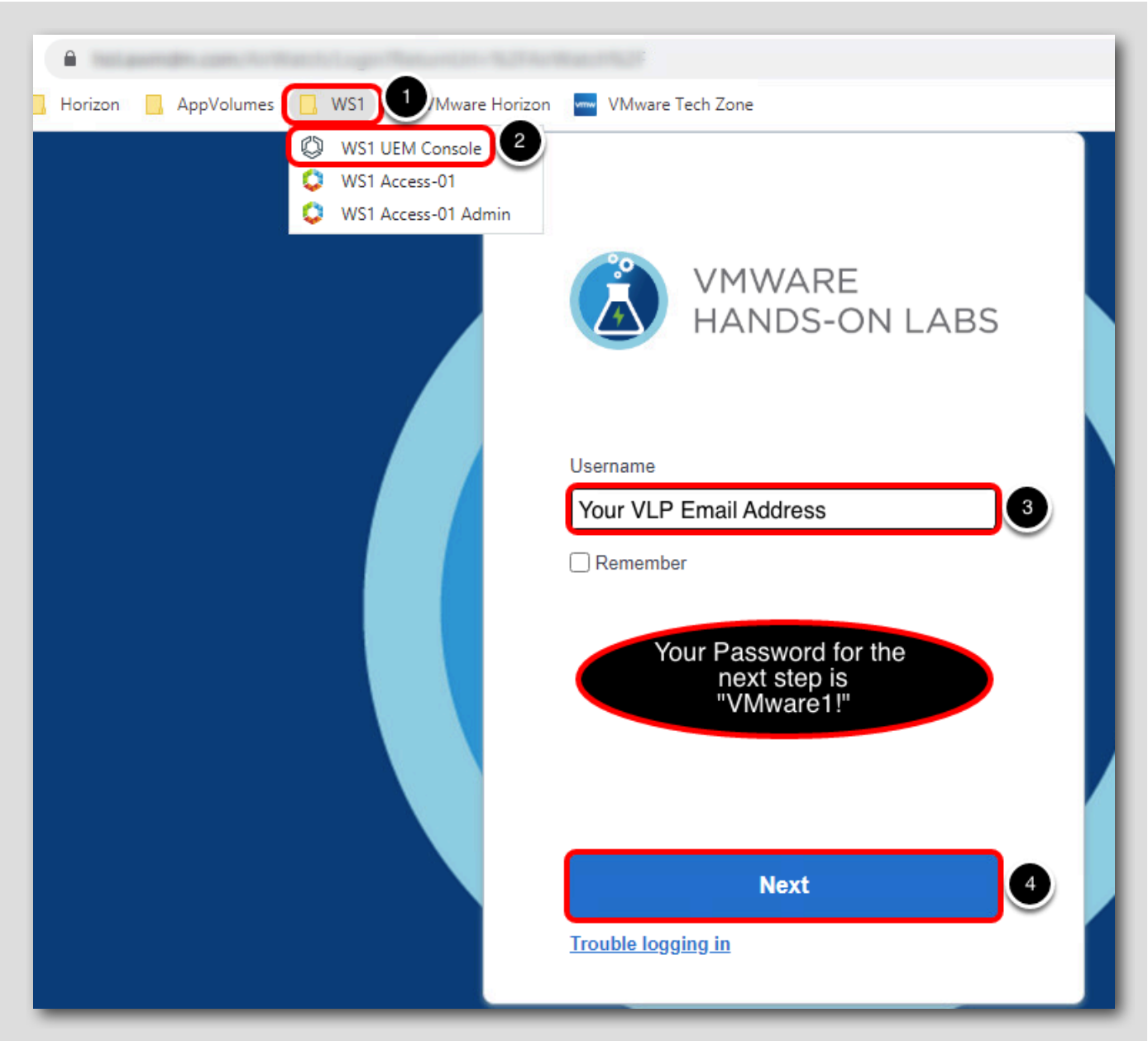
Chrome ブラウザの起動

[285]

現在接続している仮想マシンのデスクトップから、[Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールへのログイン

[286]



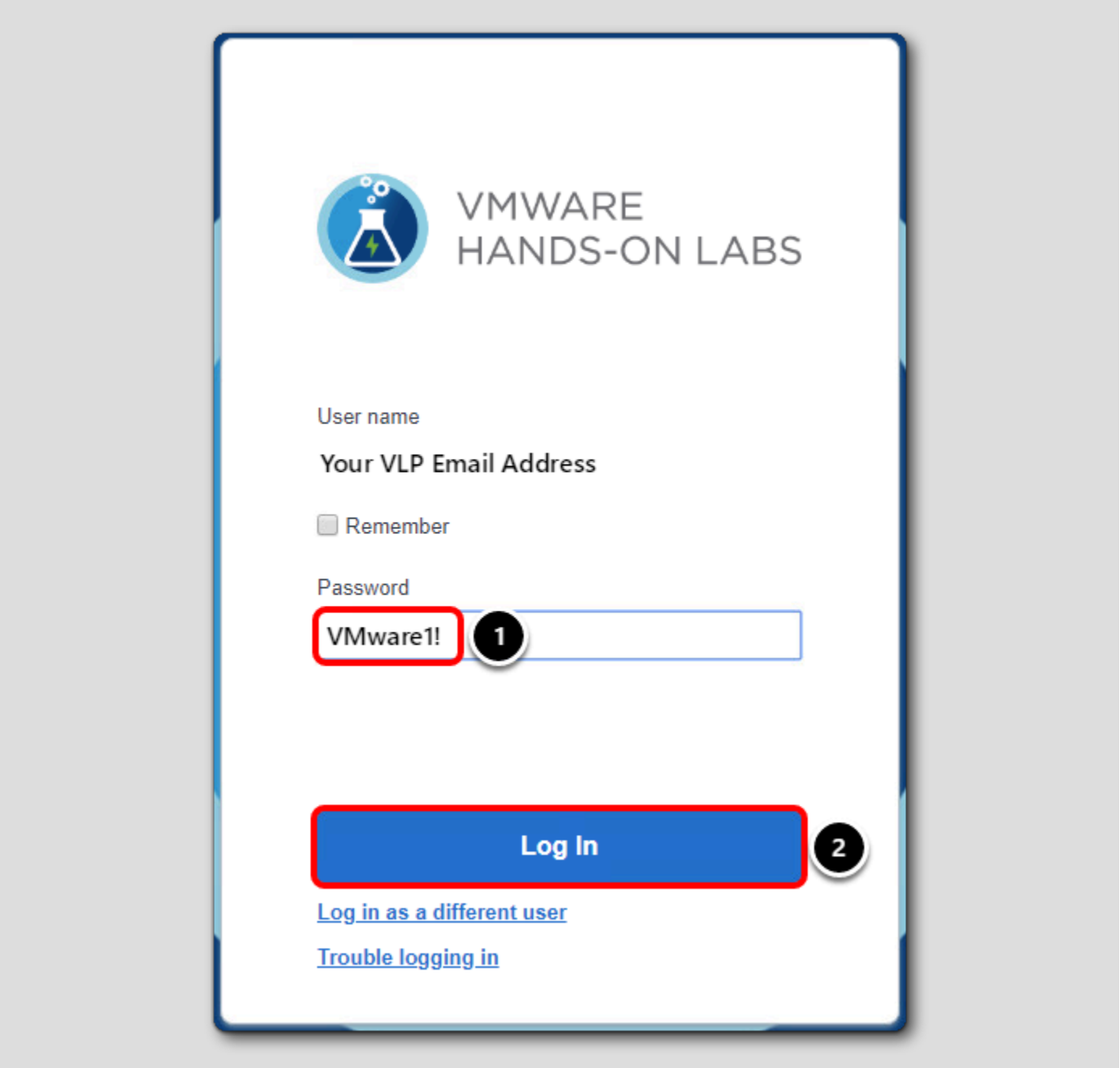
1. [WS1] ブックマーク フォルダをクリックします。
2. [WS1 UEM Console] リンクをクリックします。
3. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。

   注： 次の手順のパスワードは、**`VMware1!`** になります。

4. [Next] をクリックします。

Workspace ONE UEM Console の認証情報の入力

[287]



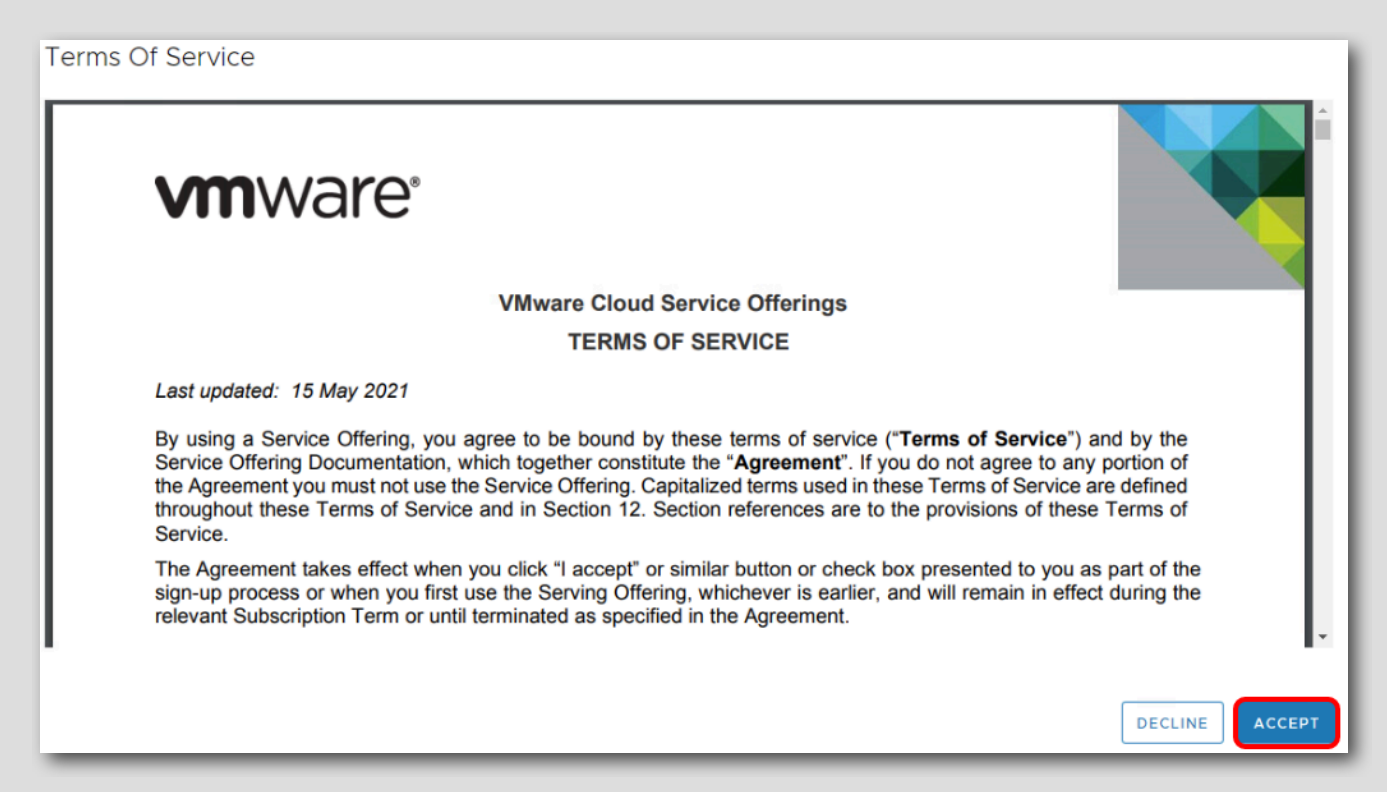
[Password] フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

利用規約の承諾

[288]



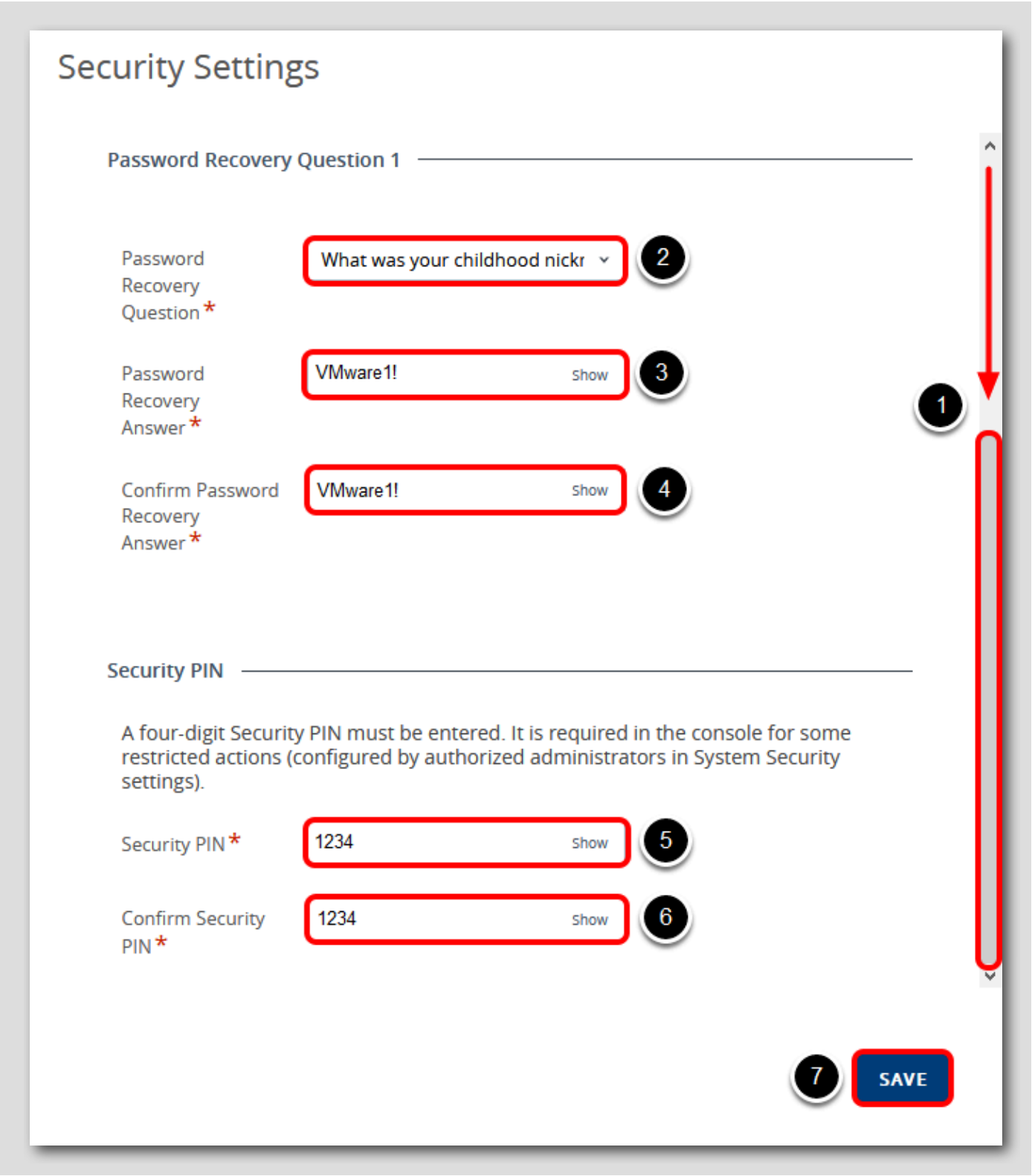
[Workspace ONE UEM Terms of Service] が表示されたら、[Accept] ボタンをクリックします。

注：以降の手順は、管理コンソールへの初回ログイン時にのみ実行されます。

初期セキュリティ設定の完了

[289]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

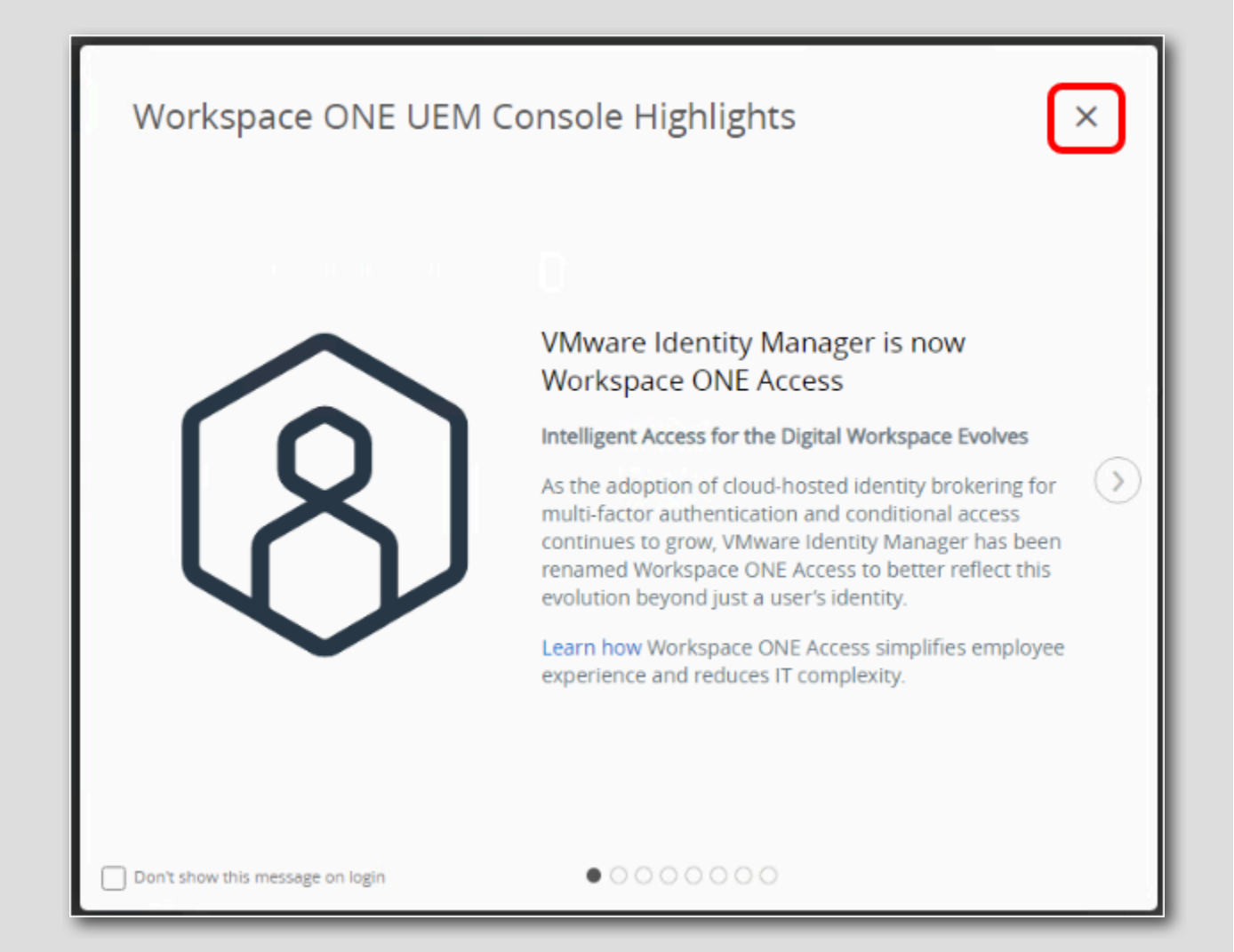

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示します。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[290]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

Hub サービスの有効化

[291]

Hub サービスの有効化フローは、新規のお客様であるか、既存のお客様であるかによって異なります。

Workspace ONE の新しいお客様

[292]

2019 年 1 月以降に Workspace ONE を購入した新しいクラウドのお客様の場合、インスタンス プロビジョニング プロセスの一環として Hub サービスが自動的に有効化されます。Workspace ONE UEM、Workspace ONE Access、および Hub サービス コンソールは相互に接続されており、Intelligent Hub アプリケーションで Hub カタログが有効になっています。

既存のクラウド Workspace ONE UEM のお客様

[293]

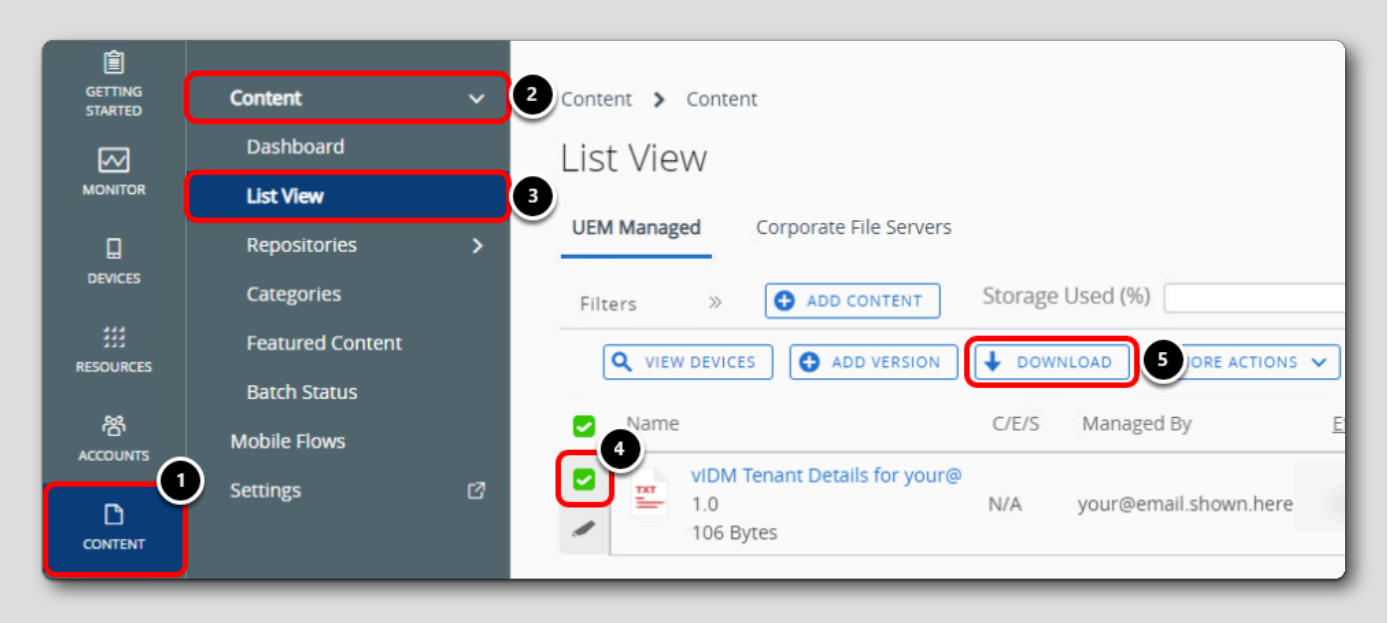
既存のお客様は、Hub サービスを有効化するために、Workspace ONE Access テナント URL、テナント管理者ユーザー名およびパスワードを構成できます。Workspace ONE Access テナントがない場合は、[Request a Cloud Tenant] ボタンを使用して、Workspace ONE UEM 管理者コンソールから要求できます。

このラボでは、次の手順で Hub サービスを有効化するために使用する Workspace ONE Access テナントがすでに提供されています。

Workspace ONE UEM Console のテナントの詳細へのアクセス

[294]

このラボ全体を通じて使用するために、一時的な Workspace ONE Access テナントが生成されています。Workspace ONE Access のテナント URL とログインの詳細が、ラボの最初に Workspace ONE UEM Console の [Content] セクションにアップロードされました。

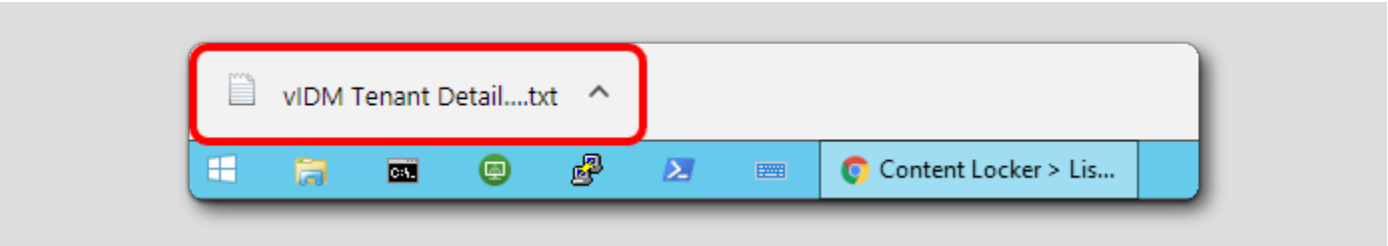


Workspace ONE UEM Console で、次のように操作します。

1. [Content] をクリックします。
2. [Content] を展開します。
3. [List View] をクリックします。
4. **`vIDM Tenant Details for your@email.shown.here.txt`** という名前のテキスト ファイルを見つけ、その横にあるチェックボックスをクリックしてファイルを選択します。
5. [Download] をクリックします。

ダウンロードしたテキスト ファイルを開く

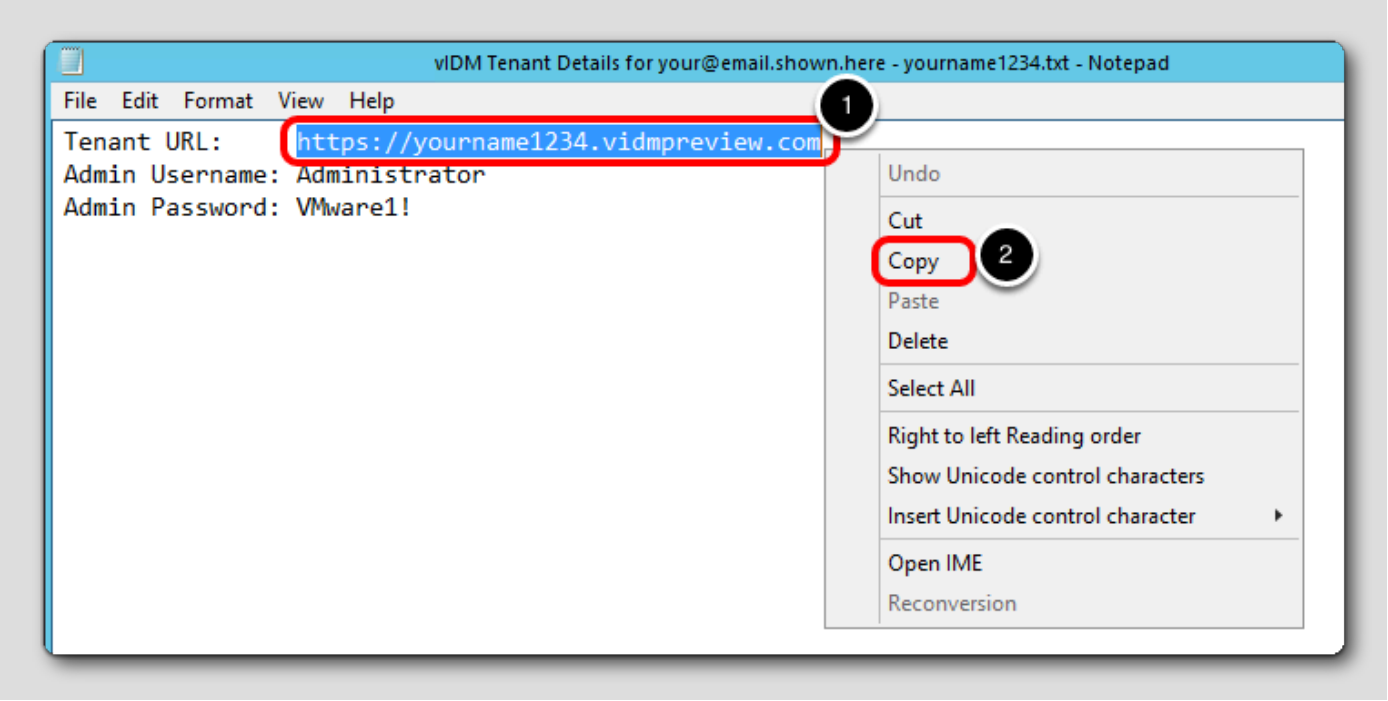
[295]



ファイルのダウンロード後、ダウンロード バーから「vIDM Tenant Details for your@email.shown.here.txt」ファイルをクリックして開きます。

テナント URL のコピー

[296]

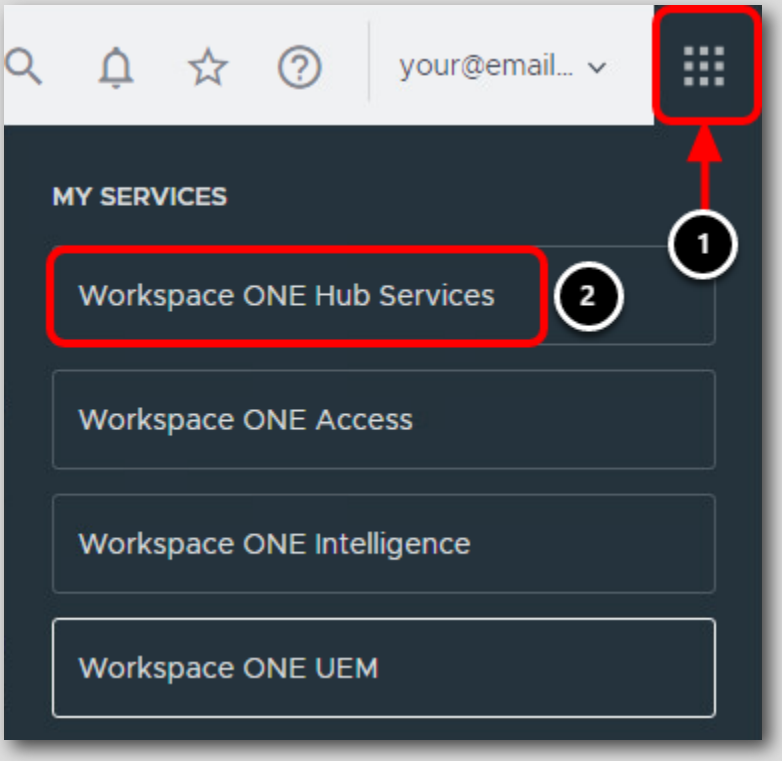


1. [Tenant URL] テキストを選択して右クリックします。
2. [Copy] をクリックします。

注：テナント名は Workspace ONE UEM Console のグループ ID と一致します。

Workspace ONE Hub サービスへの移動

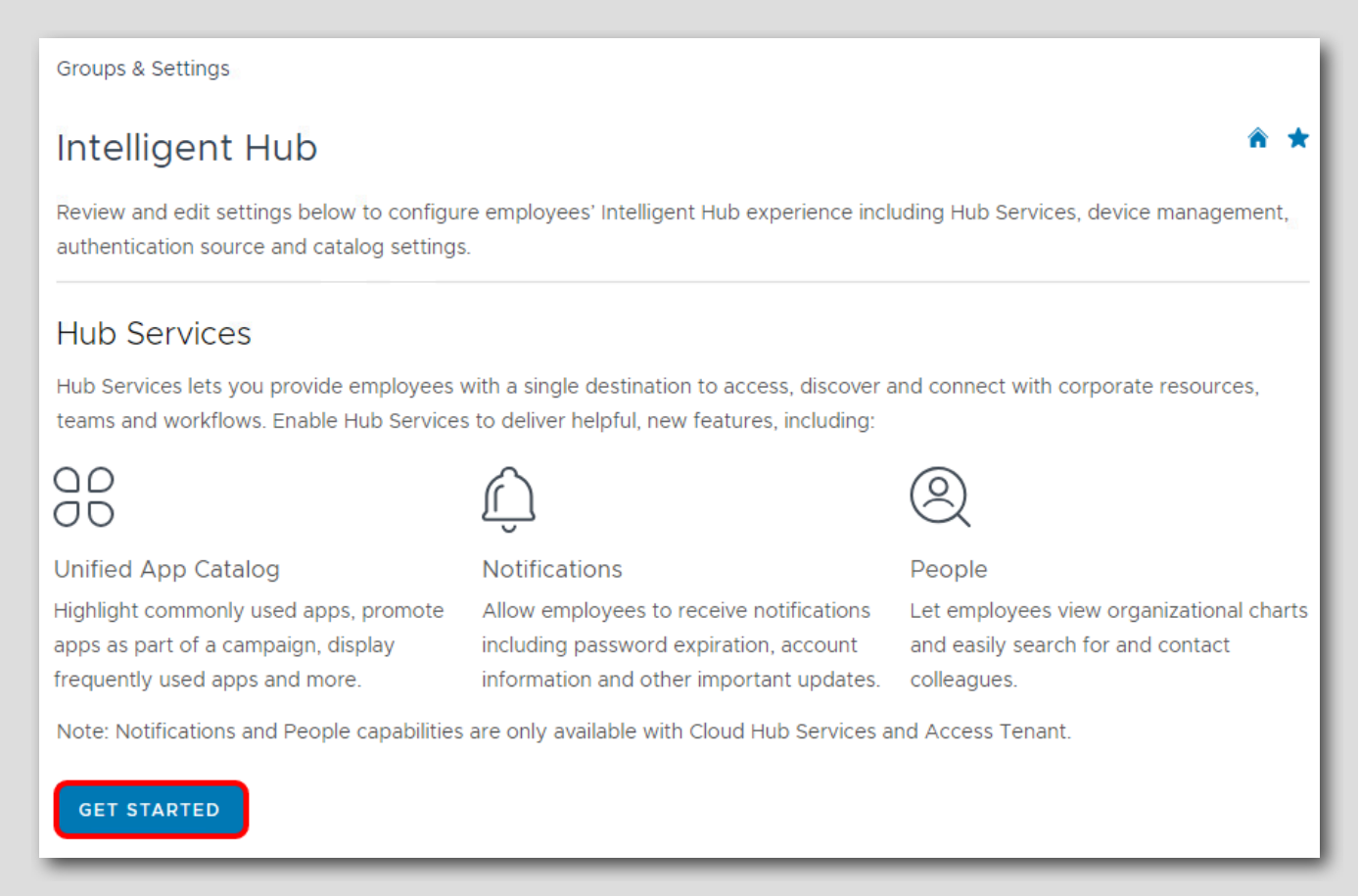
[297]



1. 右上にある [My Services] ボタンをクリックします。
2. [Workspace ONE Hub Services] をクリックします。

はじめに

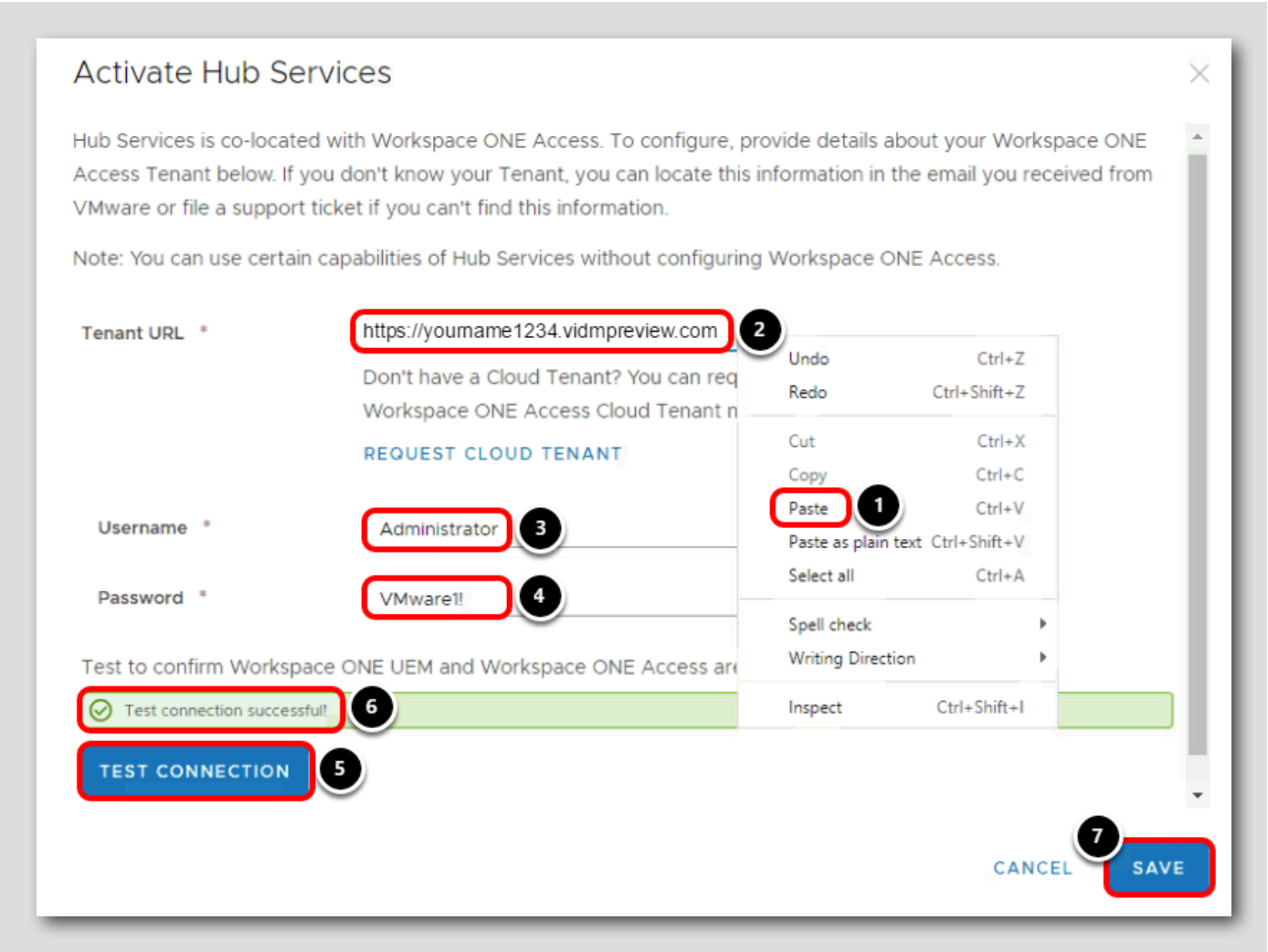
[298]



[Get Started] クリックして、Hub サービスの有効化プロセスを開始します。

Hub サービスの有効化

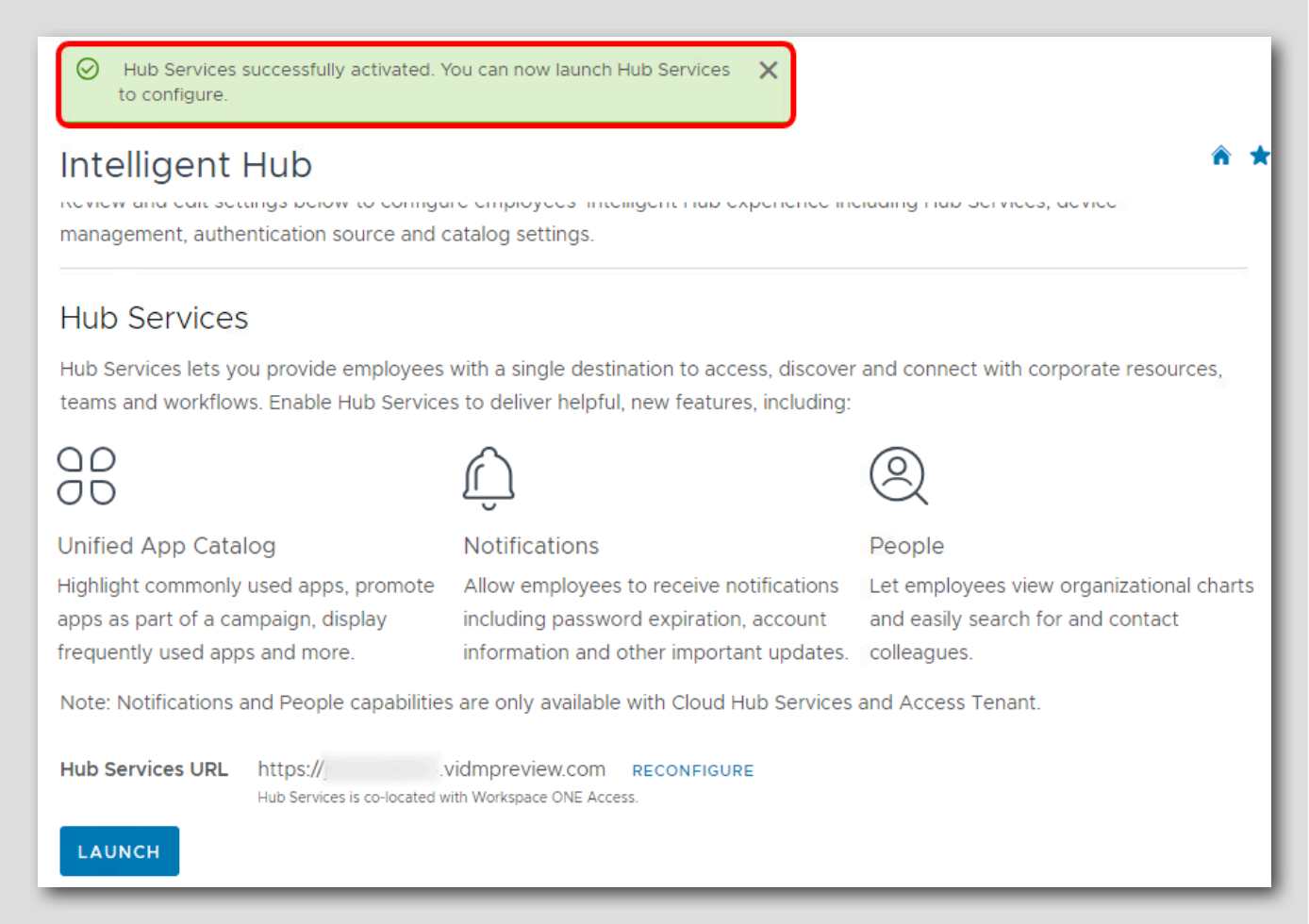
[299]



1. [Tenant URL] フィールドを右クリックし、[Paste] をクリックします。
2. 前の手順でダウンロードしたメモ帳ファイルの URL を入力していることを確認します。クリップボードが空白であるか、他の値が保存されている場合は、前の手順に戻って、ダウンロードしたメモ帳ファイルからテナントの URL をコピーします。
3. [Username] に **`Administrator`** と入力します。
4. [Password] に **`VMware1!`** と入力します。
5. [Test Connection] をクリックします。
6. 成功メッセージ「Test Connection Successful!」が表示されることを確認します。
7. [Save] をクリックして続行します。

Hub サービスの起動

[300]



Hub サービスが正常に有効化されたことを確認するメッセージが表示されていることを確認します。これで、テナントの Hub サービスの有効化が正常に完了しました。

macOS Hub アプリケーション カタログの有効化

[301]

Workspace ONE UEM テナントで Hub サービスを有効にすると、Hub サービスで使用可能な統合アプリケーション カタログが、登録済みデバイスの Intelligent Hub アプリケーションで使用されます。Hub サービスで最新の統合アプリケーション カタログを有効にするには、追加の設定が必要です。macOS のレガシー カタログを無効にする必要があります。

このセクションでは、macOS の Hub アプリケーション カタログを有効化します。

[Catalog Settings] への移動

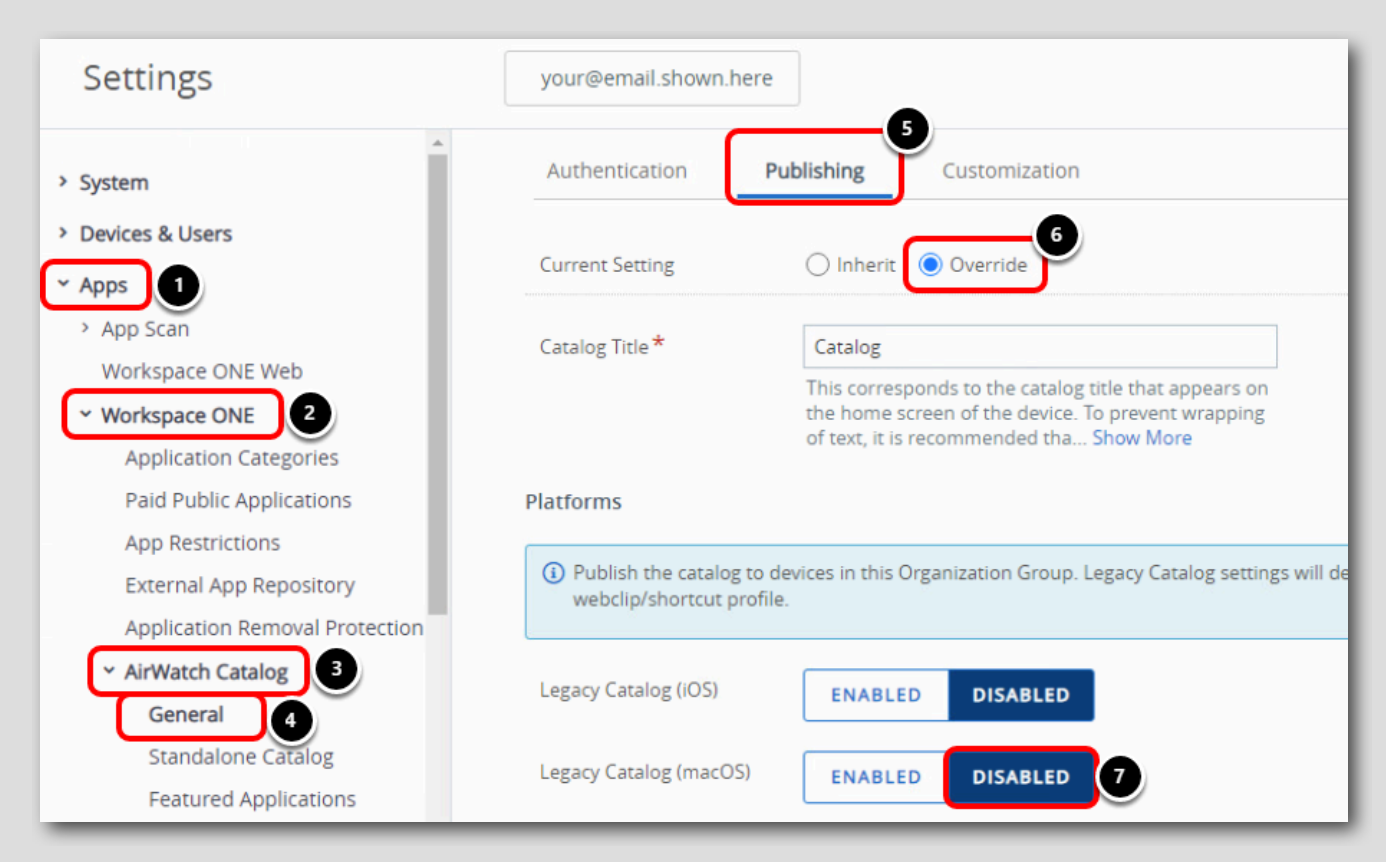
[302]

Workspace ONE UEM Console で次のように操作します。

1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

レガシー カタログ設定のオーバーライド

[303]

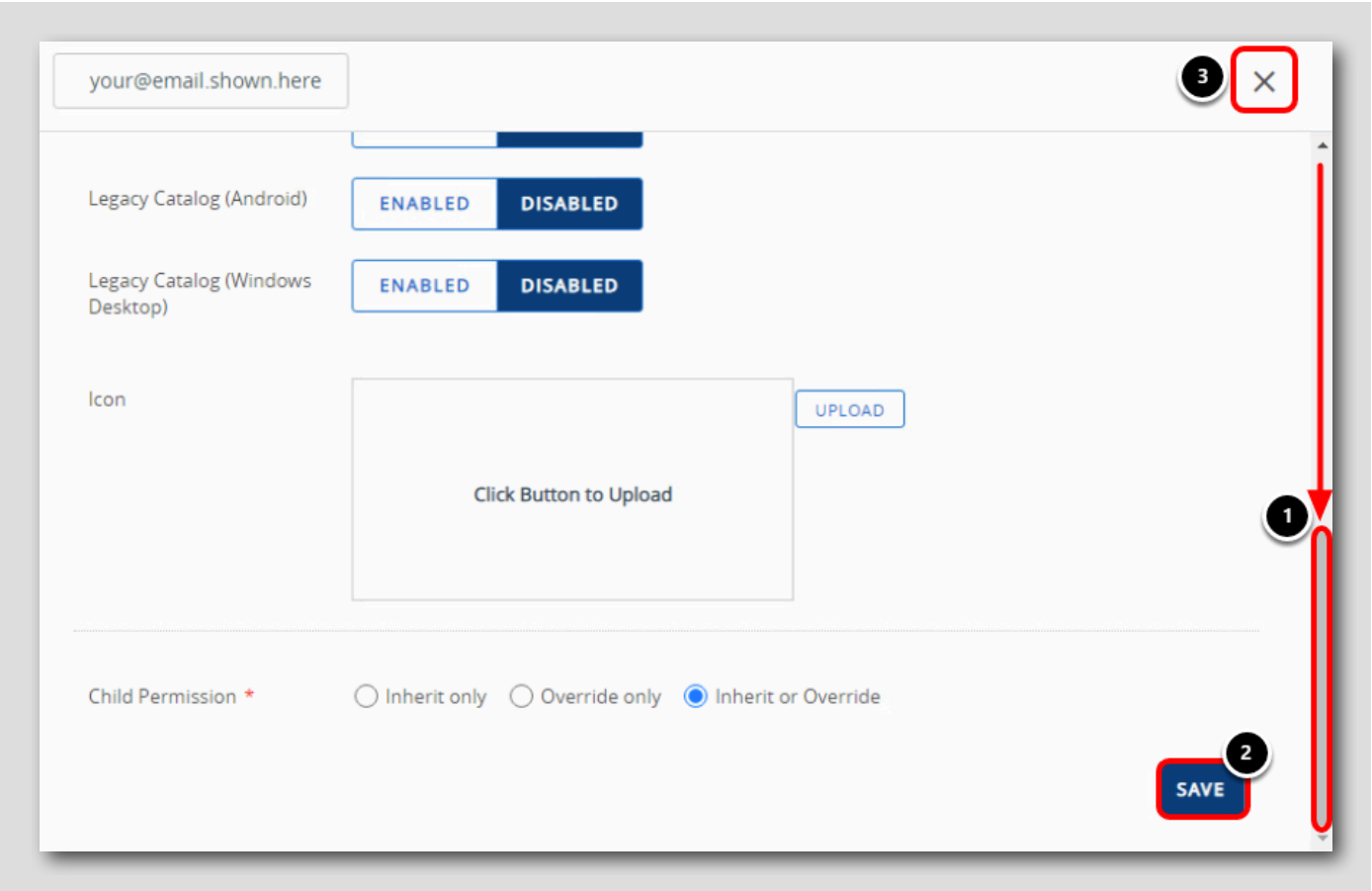


1. [Apps] をクリックします。
2. [Workspace ONE] をクリックします。
3. [AirWatch Catalog] をクリックします。
4. [General] をクリックします。
5. [Publishing] をクリックします。
6. [Current Setting] で [Override] を選択します。
7. [Legacy Catalog (macOS)] に対して [Disabled] を選択します。

これにより、macOS プラットフォームの古い Web クリップ ベースのカタログが無効になります。代わりに、ユーザーは新しい Hub アプリケーション カタログを受け取ります。これにより、より豊富な機能を備えながらも、通知、People Search、カスタム ホーム ページなどの機能を含む更新されたアプリケーション カタログが提供されます。

変更の保存

[304]



1. 一番下までスクロールします。
2. [Save] をクリックします。
3. [X] をクリックして [Settings] ウィンドウを閉じます。

プロファイルの作成

[305]

この実習では、プロファイルを使用して macOS デバイスの動作を変更する方法について説明します。

プロファイルは、Workspace ONE UEM が macOS デバイスの設定を管理するためのメカニズムです。macOS プロファイル管理は、デバイス レベルと登録ユーザー レベルの 2 つの方法で実行されます。ログインしているユーザーに関係なく、適切な制限を設定し、適切な設定を適用できます。また、デバイスにログインしているユーザーに固有の設定を適用することもできます。

どのプロファイルにも [General] セクションと [Payload] セクションがあります。

- [General] セクションには、プロファイルの情報と名前、そのプロファイルを適用するデバイスを指定するためのフィルタがあります。
- [Payload] セクションでは、デバイスで実行されるアクションを定義します。

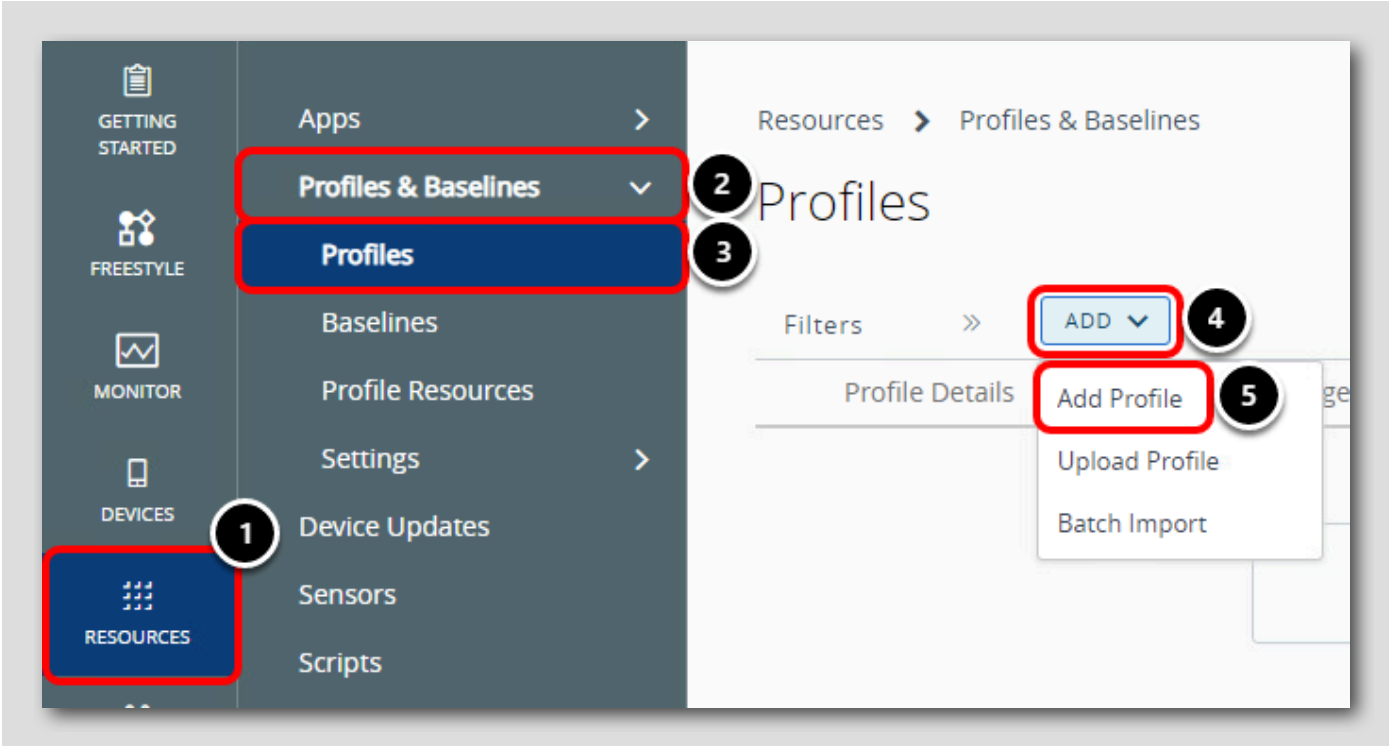
すべてのプロファイルについて、[General] セクションの必須フィールドに適切な情報を入力し、ペイロードを 1 つ以上構成してください。

デバイス プロファイルは、通常、システム全体に適用される設定を管理するときに使用します。デバイス プロファイルには、VPN と Wi-Fi の構成、グローバル HTTP プロキシ、ディスク暗号化、ディレクトリ (LDAP) 統合などの項目を含めることができます。

この演習では、エンド ユーザーがさまざまな macOS システム環境設定を変更できないようにするプロファイルを作成します。

macOS プロファイルの追加

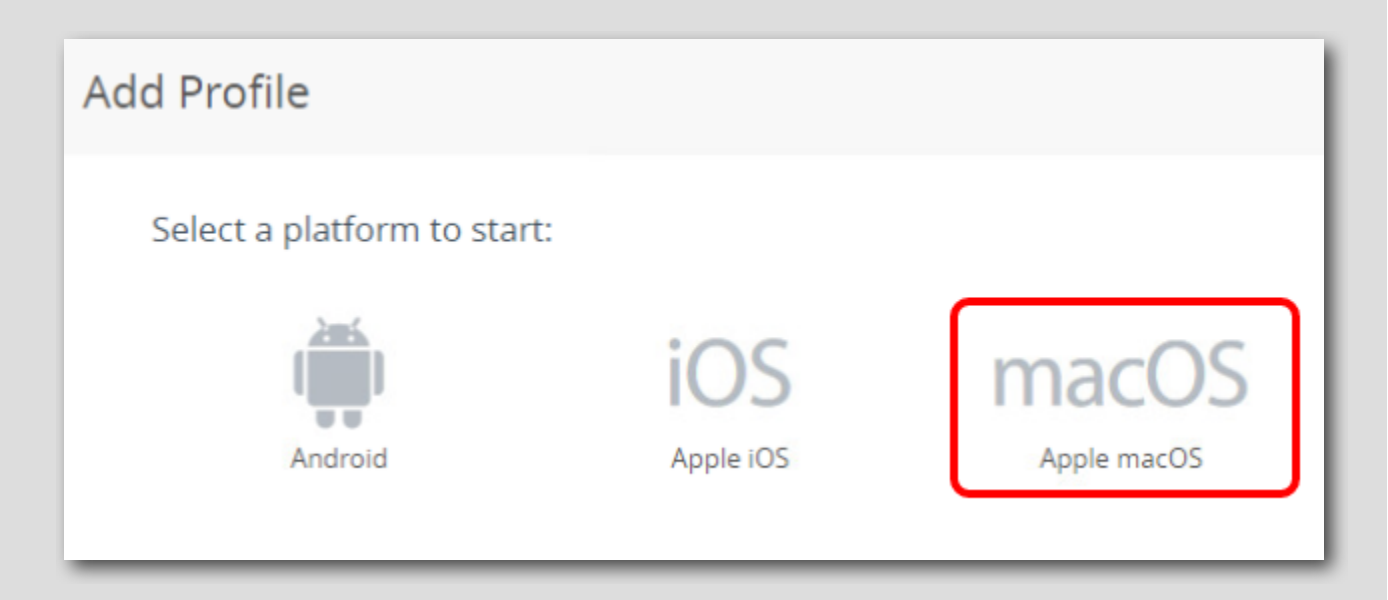
[306]



Google Chrome で Workspace ONE UEM 管理コンソールに戻ります。

1. [Resources] をクリックします。
2. [Profiles & Baselines] を展開します。
3. [Profiles] をクリックします。
4. [Add] をクリックします。
5. [Add Profile] をクリックします。

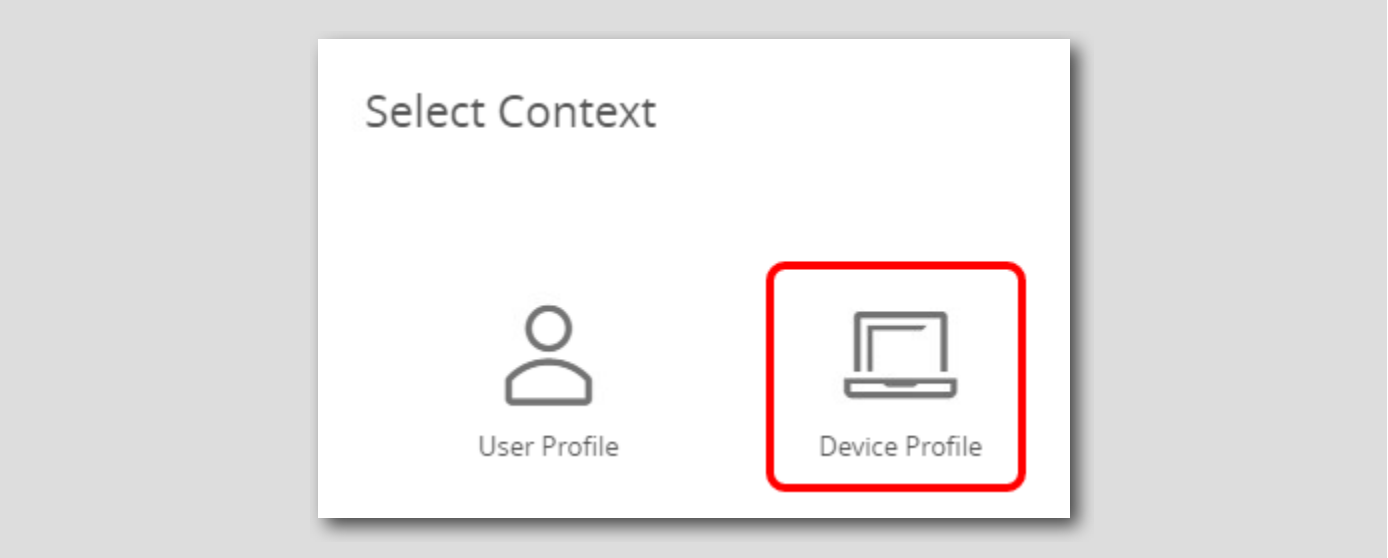
プロファイル プラットフォームの選択 [307]



[macOS] をクリックします。

プロファイル コンテキストの選択

[308]

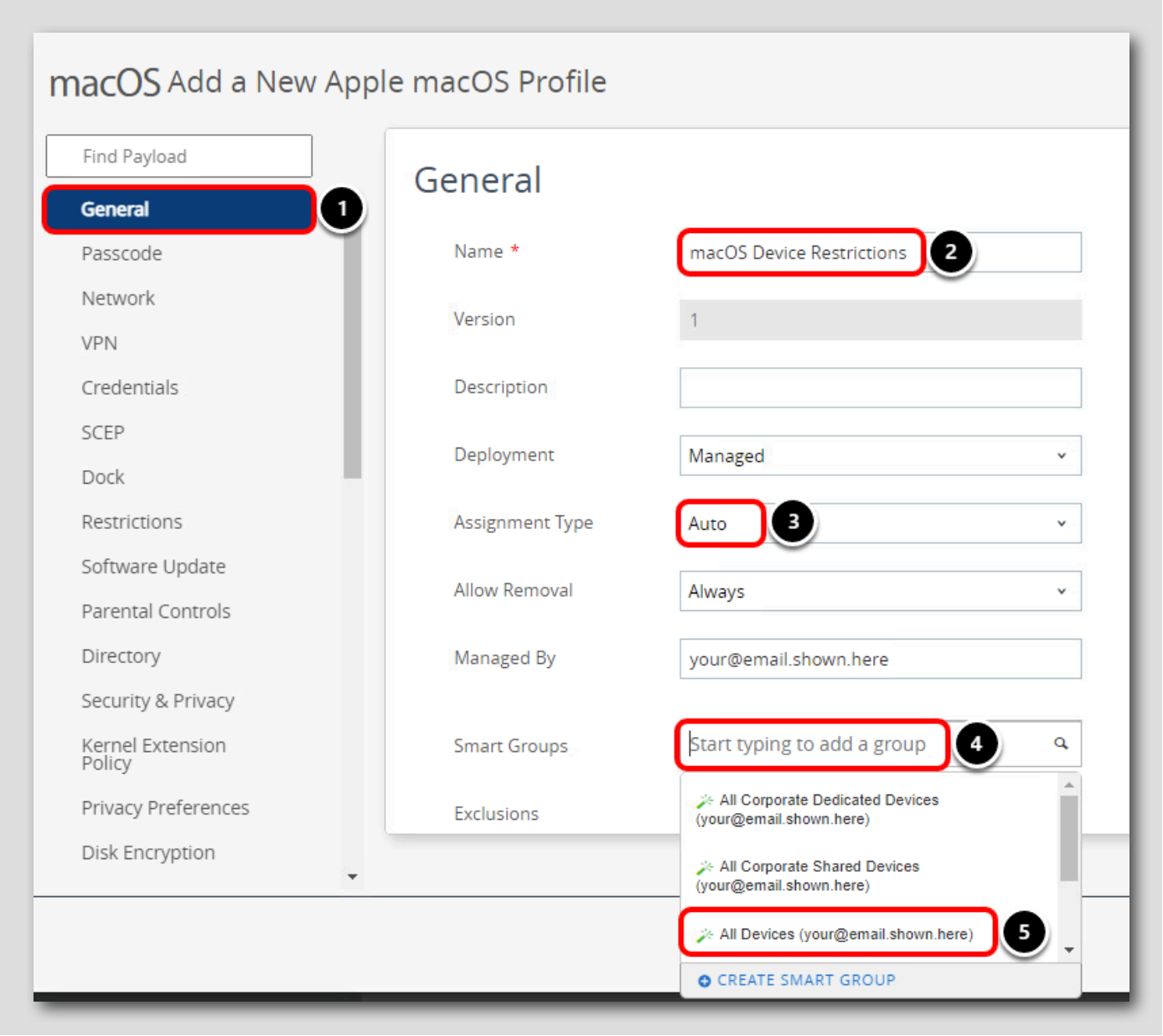


プロファイルには、ユーザーとデバイスの 2 つのコンテキストがあります。ユーザー プロファイルは、デバイスにログインしているユーザーにのみ構成を適用します。デバイス プロファイルは、デバイス全体に構成を適用します。

[Device Profile] をクリックします。

[309]

全般ペイロードの構成



デバイス プロファイルを次のように構成します。

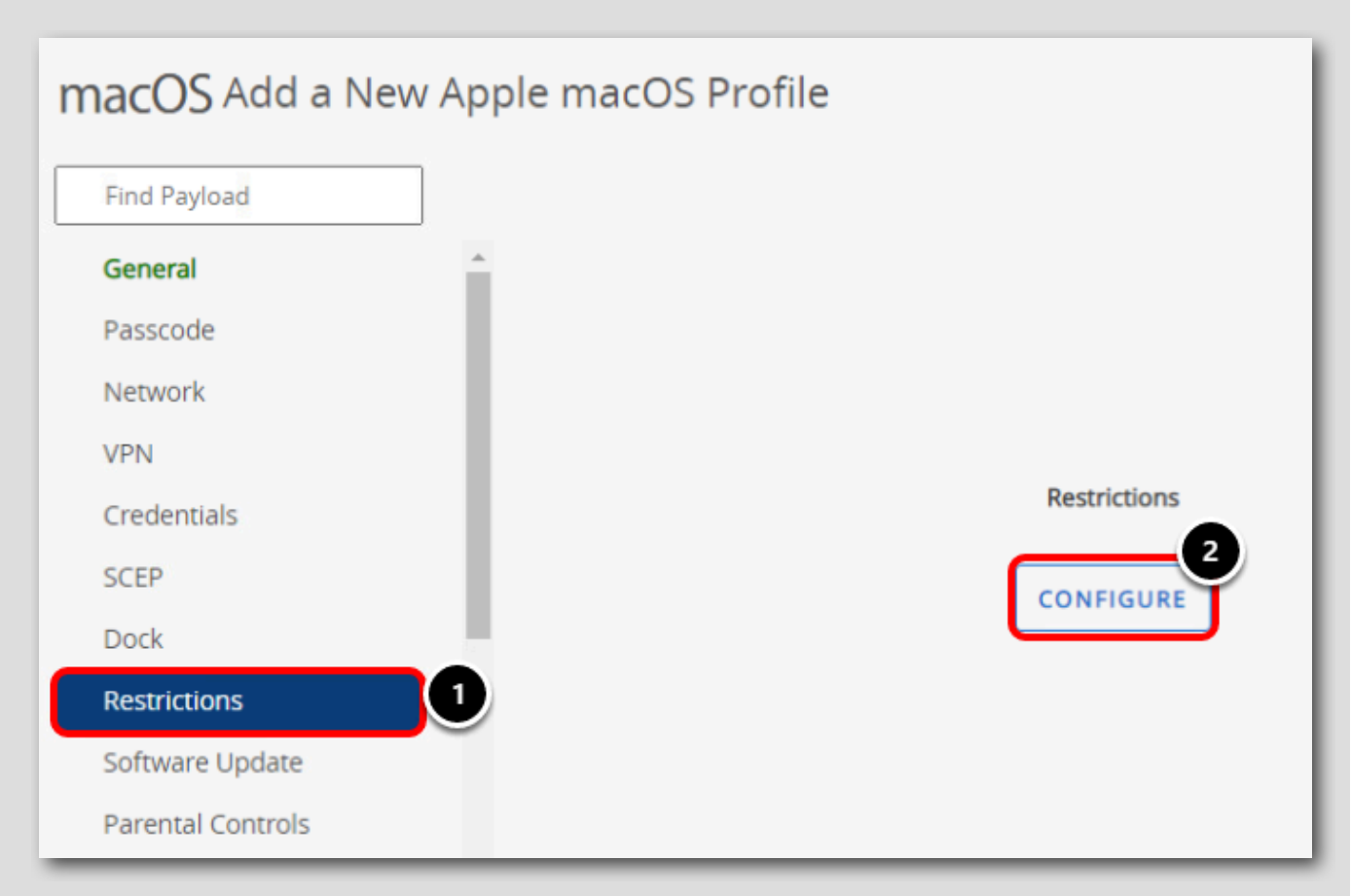
1. [General] ペイロードを選択します（選択されていない場合）。
2. プロファイル名に **`macOS Device Restrictions`** と入力します。
3. [Assignment Type] に対して [Auto] を選択します。
4. 下にスクロールして [Smart Groups] フィールドを表示し、検索ボックスをクリックします。
5. リストから [All Devices (your@email.shown.here)] グループを選択します。

左側の各タブは「Payload」です。これらは、選択したプラットフォームとプロファイルのコンテキストでデバイス上で構成できるさまざまな機能または制限を表します。プロファイルごとに複数のペイロードがある場合がありますが、一般的にプロファイルごとに 1 つのペイロードを保持することをお勧めします（全般ペイロードは除きます。これは必須です）。

行った構成により、macOS デバイス コンテキスト プロファイルが作成されます。このプロファイルは、組織グループに登録するすべての macOS デバイスに自動的に割り当てられ、適用されます。

制限事項ペイロードの追加

[310]

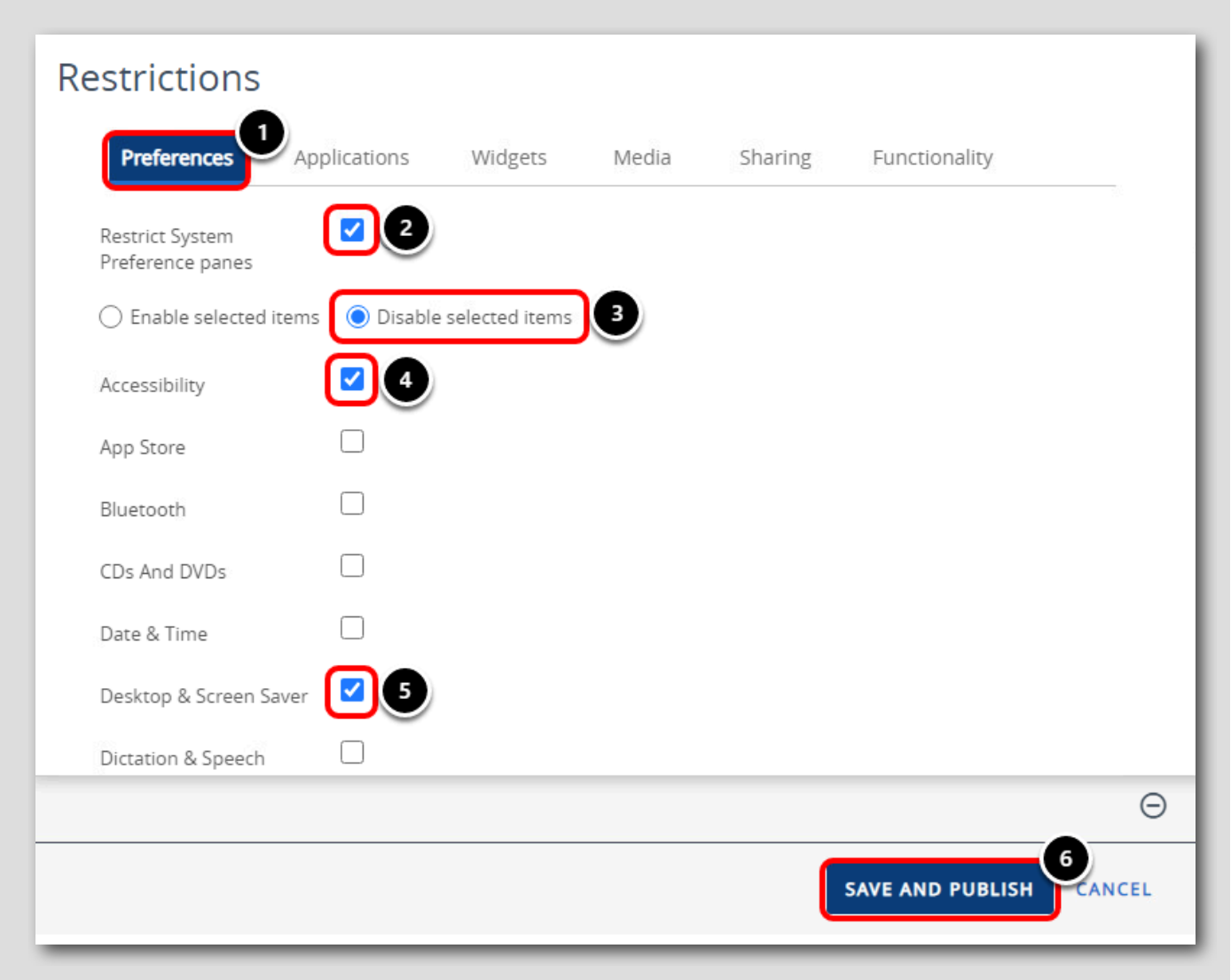


1. [Restrictions] ペイロードをクリックします。
2. [Configure] をクリックします。

[Configure] をクリックすると、[Restrictions] ペイロードがプロファイルに追加され、このプロファイルを持つ macOS デバイスに適用される制限を決定できます。

制限事項ペイロードの構成

[311]

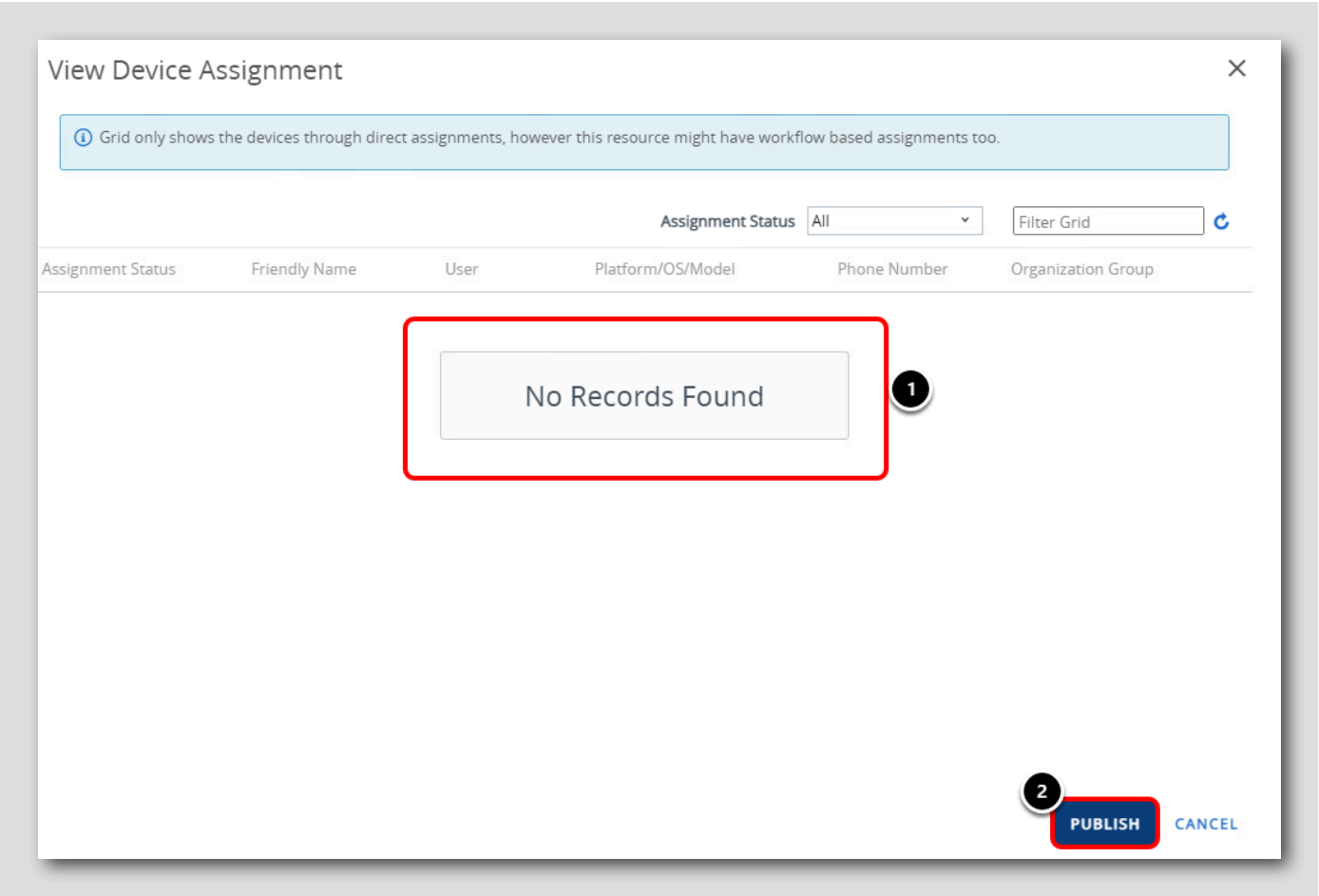


1. [Preferences] タブをクリックします。
2. [Restrict System Preference Panes] チェックボックスを [Enable] にします。
3. [Disable Selected Items] を選択します。
4. [Accessibility] チェックボックスを有効にします。
5. [Desktop & Screen Saver] チェックボックスを有効にします。
6. [Save & Publish] をクリックします。

これにより、エンド ユーザーが [System Preferences] の [Accessibility] および [Desktop] > [Screen Saver] 設定にアクセスしたり、変更したりすることができなくなります。

プロファイルのプレビューと公開

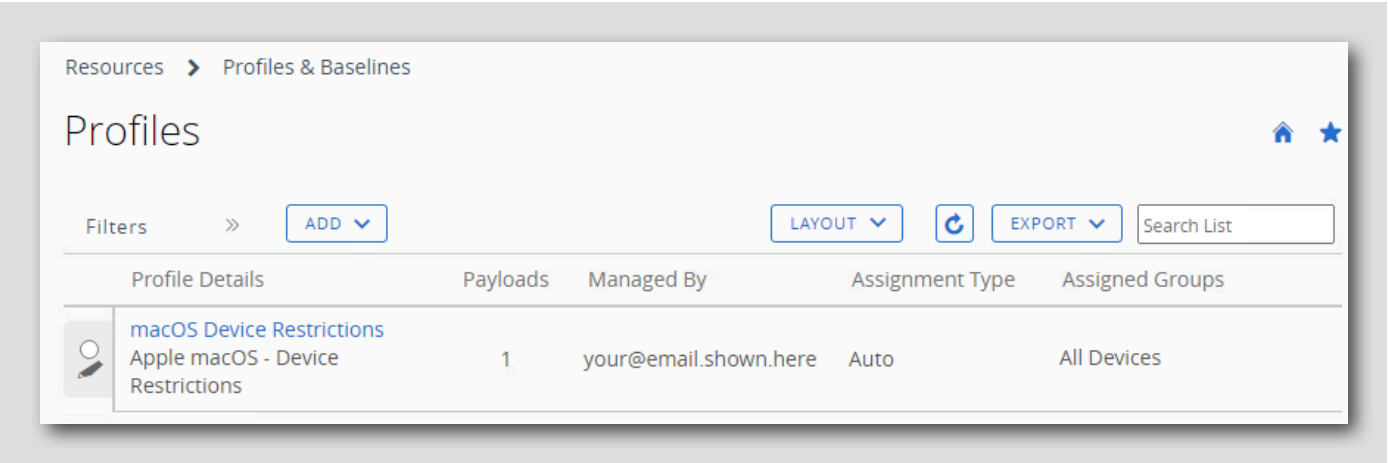
[312]



1. 通常、この構成を受信するデバイスのリストがここに表示されます。macOS デバイスをまだ登録していないため、デバイスは表示されません。
2. [Publish] をクリックします。

プロファイルが作成されたことの確認

[313]



これで、macOS デバイス制限事項プロファイルが組織グループのプロファイルのリストに追加されました。構成されているペイロード（[General] を除く）の数、割り当てのタイプ、割り当てられたグループを確認できます。プロファイルを編集する必要がある場合は、このビューに戻って変更を加えます。

この制限事項プロファイルが公開され、組織グループに登録するすべての macOS デバイスに自動的に割り当てられます。後の手順でデバイスを登録した後、この制限事項プロファイルがデバイスに適用されることを確認します。

センサーの作成

[314]

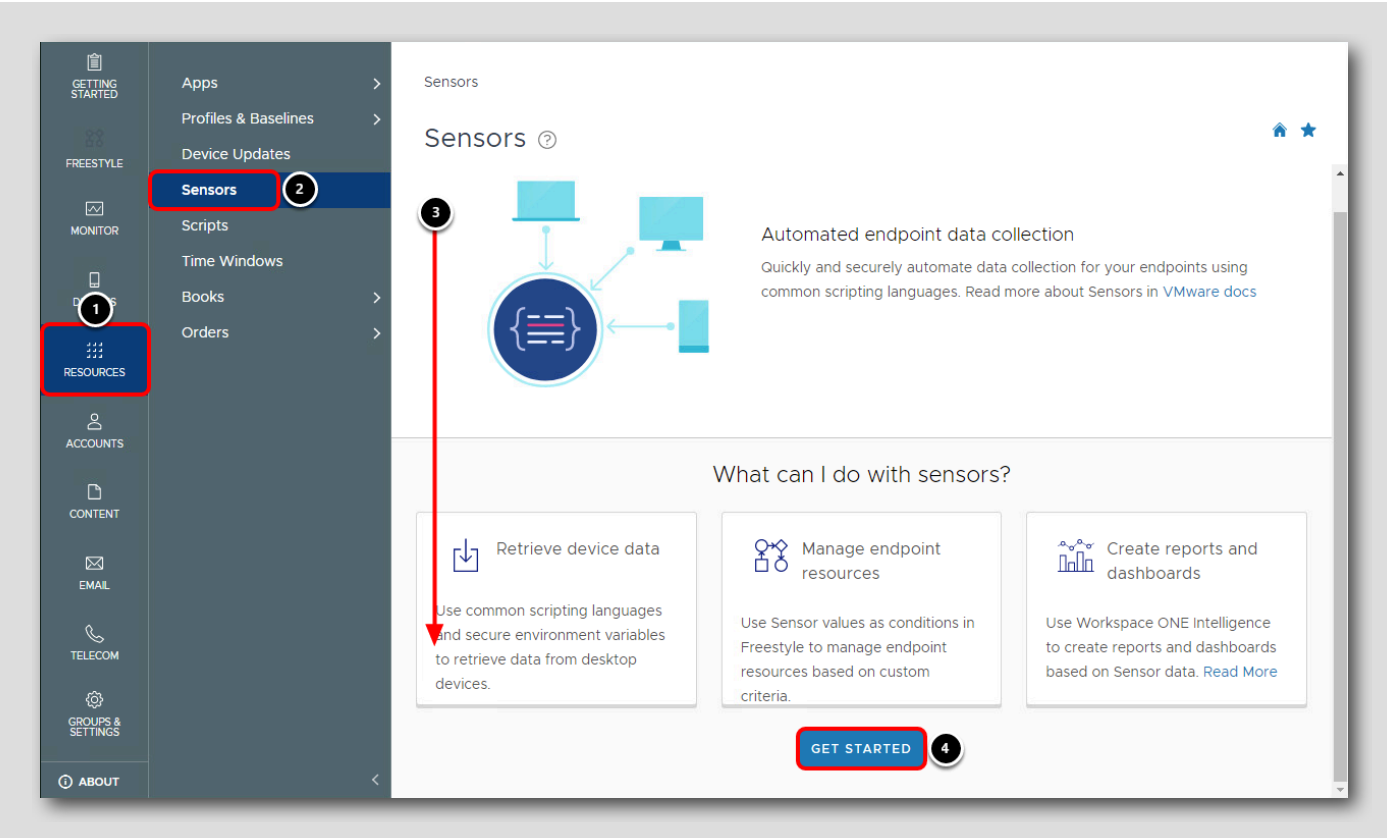
センサーを使用すると、一般的なスクリプト言語を使用して、エンドポイントからのデータ収集を迅速かつ安全に自動化できます。macOS センサーは Bash、Python 3、Zsh をサポートし、Windows デスクトップは PowerShell をサポートします。

この収集されたデータを Freestyle Orchestrator 機能の条件として使用し、このデータの条件と値に基づいてアクションを実行できます。Freestyle Orchestrator の詳細については、「*モジュール 1: Freestyle Orchestrator の概要*」を参照してください。Workspace ONE Intelligence を使用して、センサー データに基づいてレポートとダッシュボードを作成することもできます。

このセクションでは、デバイスで使用されているプロセッサのタイプをクエリする macOS のセンサーを作成します。

[Sensors] への移動

[315]

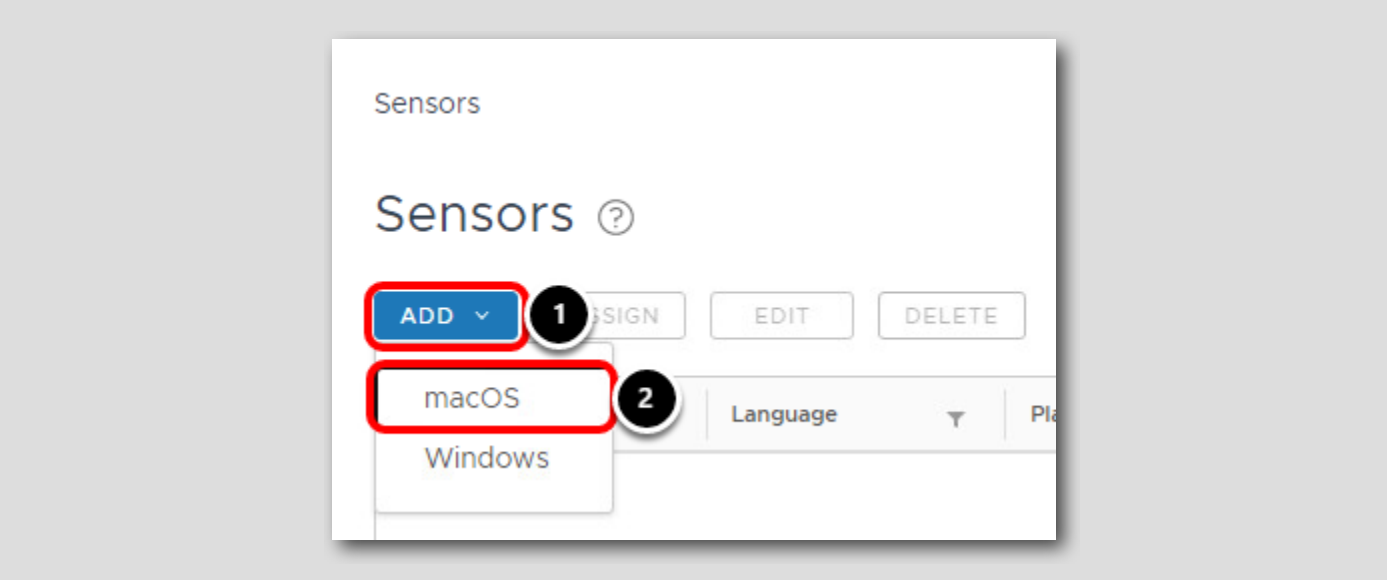


[Sensors] ページに初めてアクセスすると、概要に、「*macOS センサー*」および「*Windows デスクトップ センサー*」に関する VMware ドキュメントの記事へのリンクが表示されます。センサーに関するその他のドキュメントについては、これらのリンクを参照してください。

1. [Resources] をクリックします。
2. [Sensors] をクリックします。
3. ページの一番下までスクロールします。
4. [Get Started] をクリックします。

macOS センサーの追加

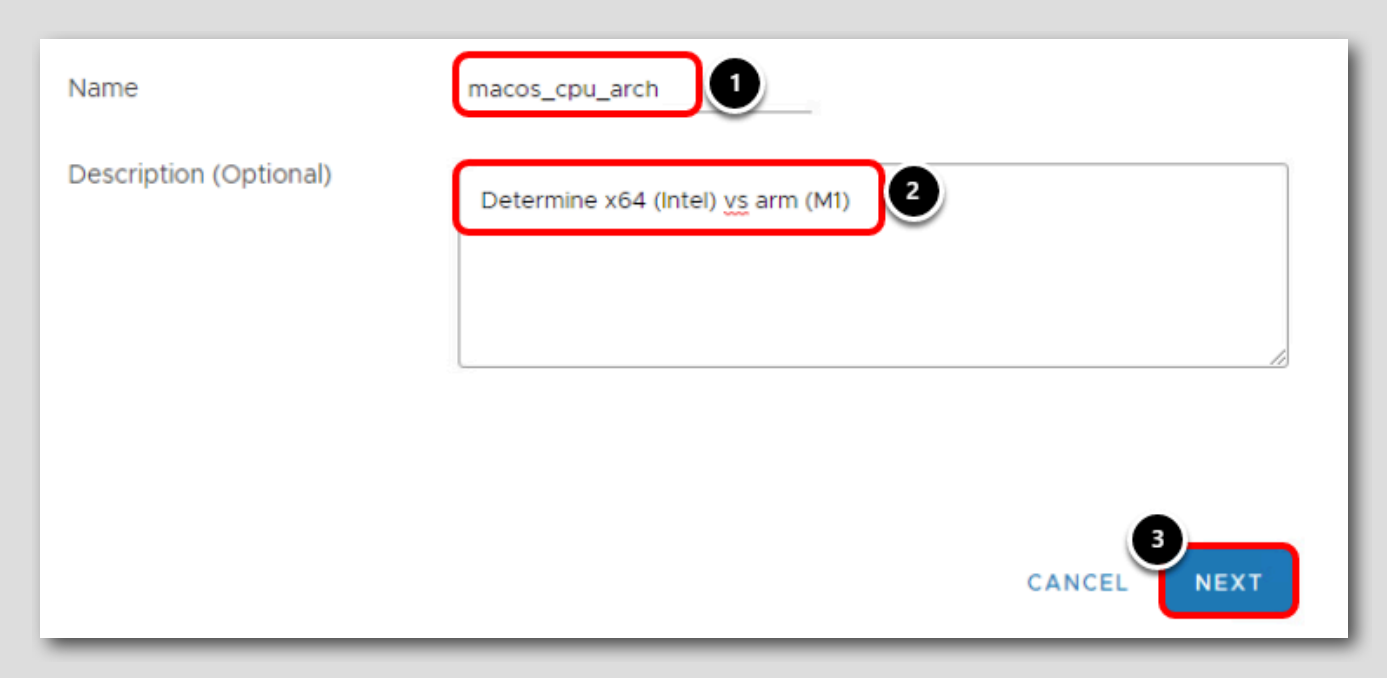
[316]



1. [Add] をクリックします。
2. [macOS] をクリックします。

全般情報の追加

[317]

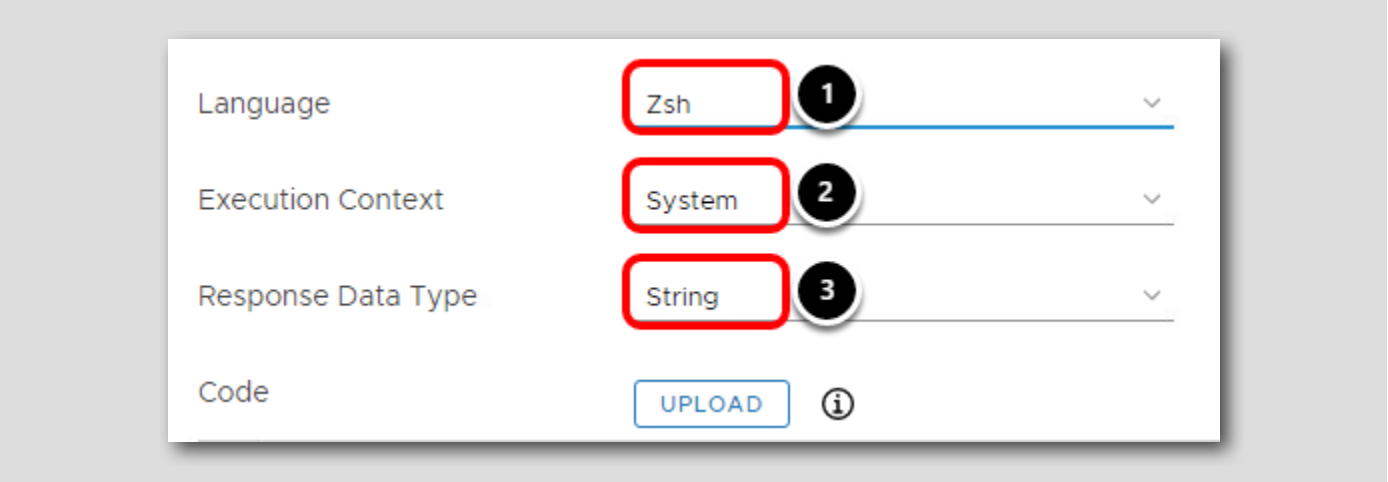


1. [Name] に **macos_cpu_arch** と入力します。
2. 必要に応じて、説明に **Determine x64 (Intel) vs arm (M1)** と入力します。
3. **[Next]** をクリックします。

このセンサーは、デバイスの CPU アーキテクチャが x64（Intel チップを使用）または arm（M1 チップを使用）のどちらであるかを報告するために使用されます。

センサーの詳細の入力

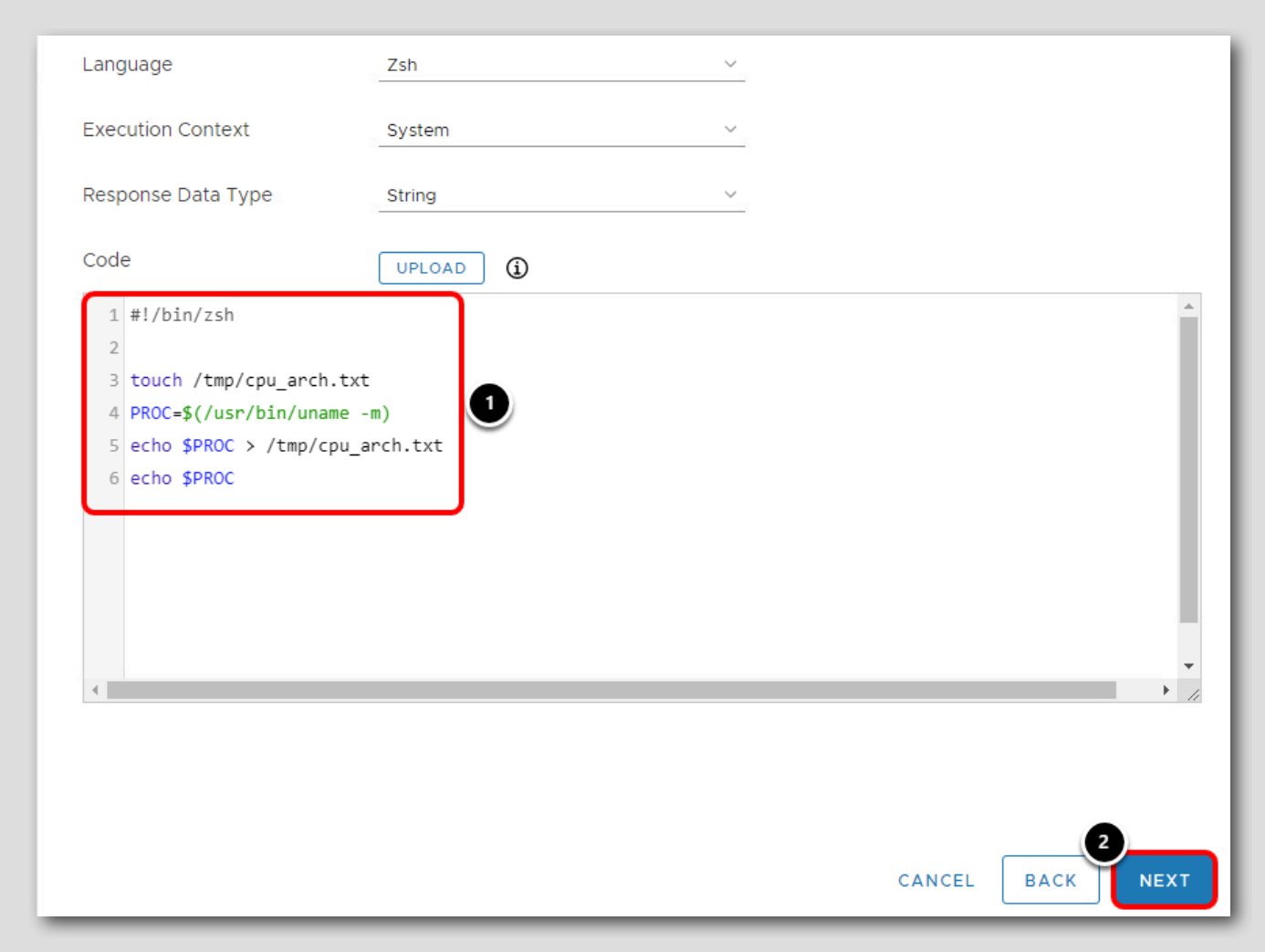
[318]



1. [Language] で **[Zsh]** を選択します。
2. [Execution Context] で **[System]** を選択します。
3. [Response Data Type] で **[String]** を選択します。

センサー コードをコピーして貼り付ける

[319]



このセンサーは Zsh 言語を使用するように設定され、デバイスの現在ログインしているユーザーに対して実行される Current User コンテキスト設定ではなく、システム（デバイス全体）の実行コンテキストをターゲットにしています。[Response Data Type] には、スクリプトから返される値（文字列（テキスト）、整数（数値）、ブール値 (true/false)、または日時）が示されます。

この場合、センサーは CPU アーキテクチャ（「x64」または「M1」）を読み取り、値を文字列として返します。

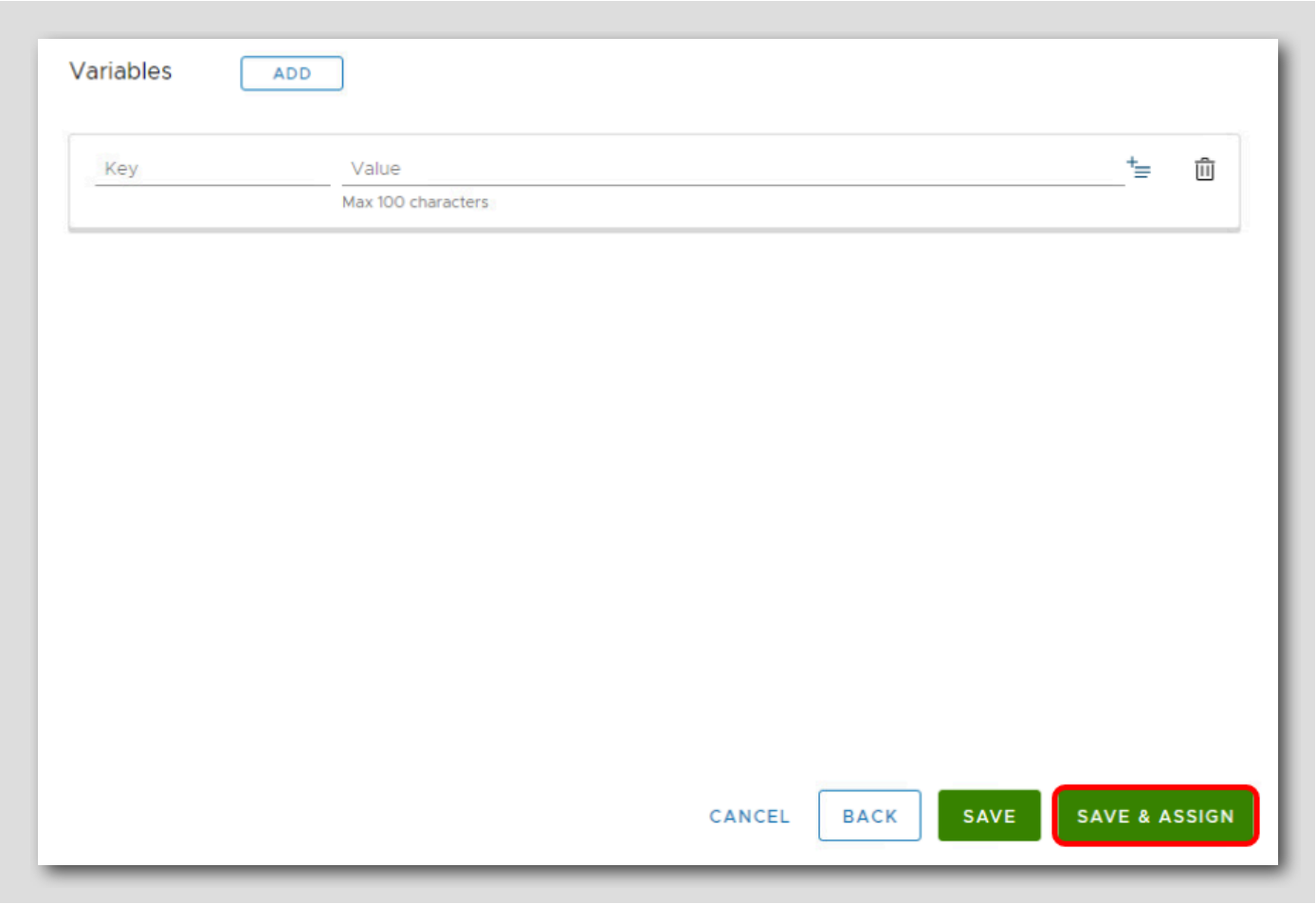
1. 下の **`#!/bin/zsh`** から **`echo $PROC`** までのコード ブロックをクリックアンドドラッグし、強調表示して、[Code] セクションにドラッグアンドドロップして、必要なセンサー コードを貼り付けます。
2. [Next] をクリックします。

```
#!/bin/zsh

touch /tmp/cpu_arch.txt
PROC=$(/usr/bin/uname -m)
echo $PROC > /tmp/cpu_arch.txt
echo $PROC
```

センサーの保存と割り当て

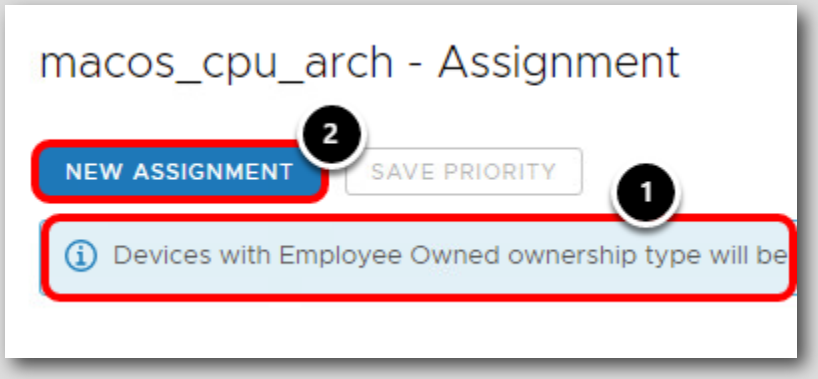
[320]



オプションで、このスクリプトで使用する変数を作成できますが、このユースケースでは必要ありません。[Save & Assign] をクリックして続行します。

macOS センサーの割り当て

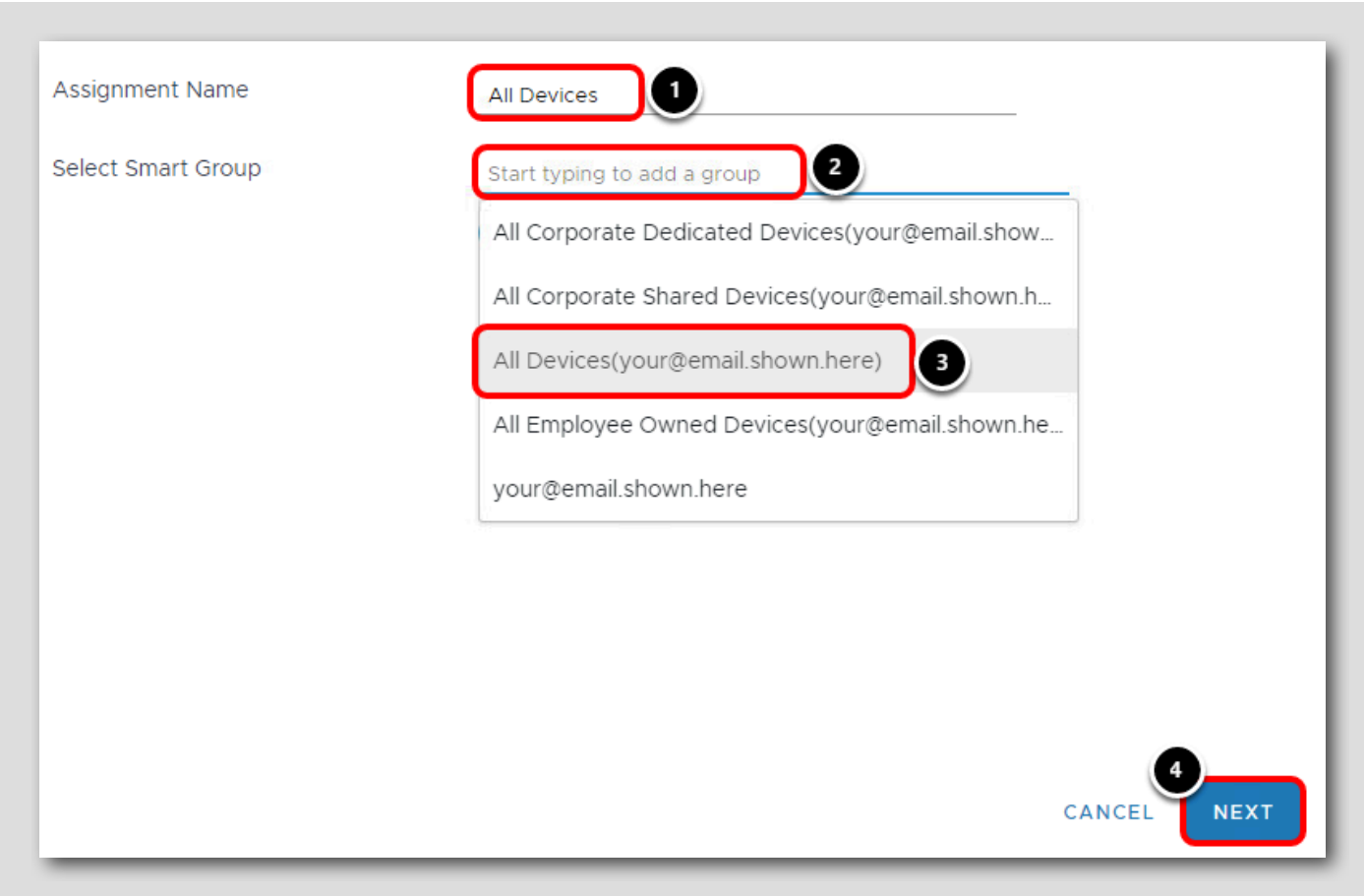
[321]



1. センサーはデバイスから機密情報を照会できるため、プライバシー上の理由から、従業員が所有するデバイスはセンサーの割り当てから自動的に除外されるという警告を確認します。
2. [New Assignment] をクリックします。

All Devices への割り当て

[322]

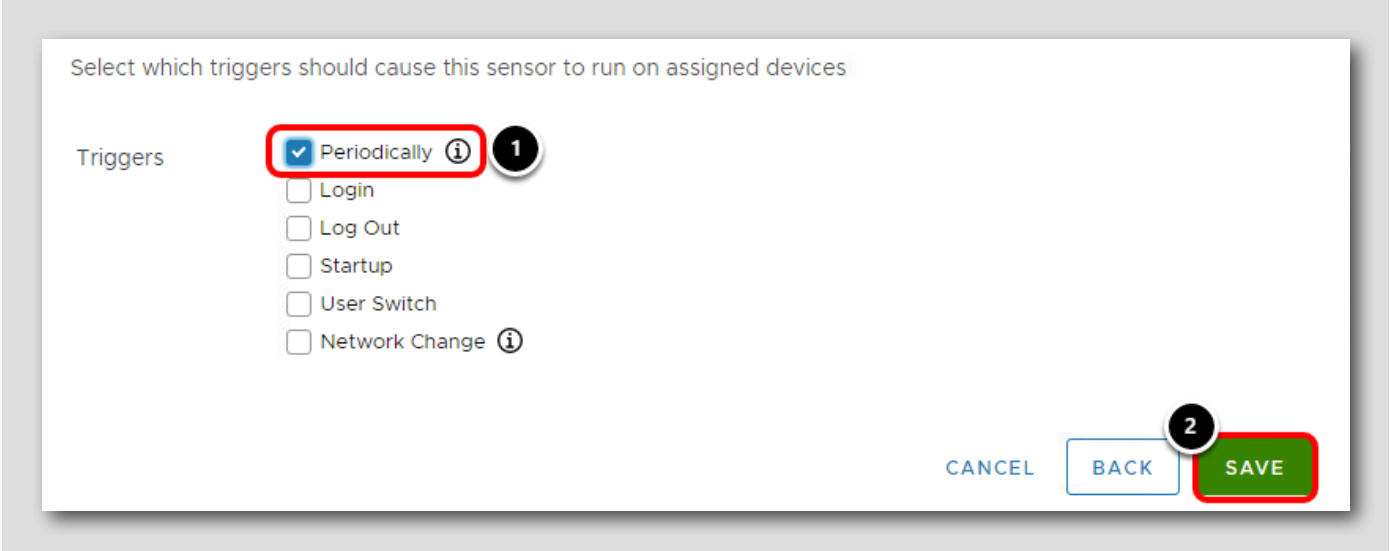


1. [Assignment Name] に **`All Devices`** と入力します。
2. [Select Smart Group] フィールドをクリックします。
3. [All Devices (your@email.shown.here)] グループを選択します。
4. [Next] をクリックします。

簡単にするために、このセンサーを、組織に登録している従業員が所有していないすべてのデバイスに展開します。実際の展開では、このセンサーを展開する特定のスマート グループをターゲットにすることができます。

展開トリガの構成

[323]

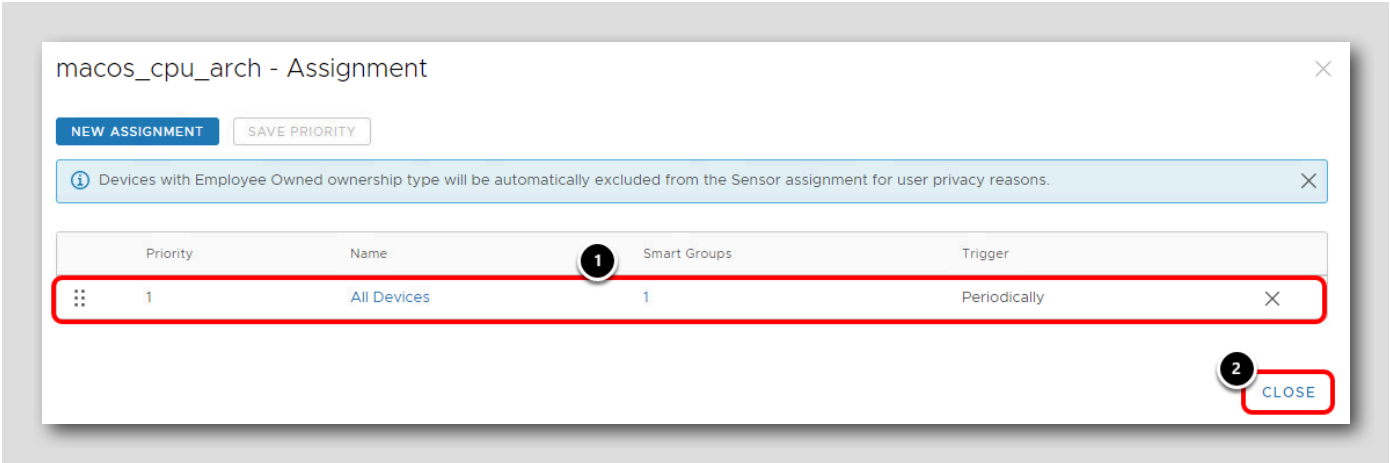


1. [Triggers] で **[Periodically]** を選択します。
2. **[Save]** をクリックします。

複数のトリガを選択できるため、組織内でセンサーを作成する際に、ユーザーのケースに最も適しているものを検討してください。

センサー作成の確認

[324]



1. これで、All Devices センサーが作成されました。複数の割り当てが作成されている場合、それらはすべてここに表示され、左側のハンドル バーを使用して、必要に応じて優先順位を再調整できます。
2. [Close] をクリックして、[Resources] ページに戻ります。

これで、デバイスの CPU アーキテクチャが「x64」(Intel) または「arm」(M1) のどちらであるかを報告する macOS センサーが正常に作成され、割り当てられました。今後の手順でデバイスを登録すると、このセンサーが表示され、値が確認されます。

センサーは、エンドポイントのデータ収集を安全に自動化するための強力なオプションです。センサーを使用して達成できる他のユースケースを検討し、ドキュメントの「*macOS センサーの例*」でアイデアを確認してください。

サードパーティ製 macOS アプリケーション（社内アプリケーション）の展開

[325]

VMware は、登録済みの macOS デバイス上のサードパーティ製アプリケーション管理のために、*オープンソースの「munki」プロジェクト*と統合します。管理者は、Workspace ONE UEM の*社内アプリケーション*ビューを使用して、サードパーティ製の（AppStore 以外の）ソフトウェアを管理できます。この統合により、管理者は munki の内部作業と構成を十分に理解する必要なく、グローバル CDN を使用して、ソフトウェアを配信することができます。

この演習では、アプリケーション カタログを有効にして、デバイスにアプリケーションを展開します。

注：Workspace ONE UEM は、ソフトウェア/構成を提供し、macOS デバイスでスクリプト/コマンドを実行するための 2 つ目の機能も提供します。プロダクト プロビジョニングと呼ばれるこの方法は、この演習の範囲外です。詳細については、VMware TechZone の「*Deploying Third-Party macOS Applications: VMware Workspace ONE Operational Tutorial*」を参照してください。

ソフトウェア提供の推奨方法

[326]

管理者は、複数の方法でソフトウェアを macOS に提供できます。クイック リファレンスとして、VMware は、次の方法を使用して macOS デバイスにソフトウェアを提供することを推奨しています。

- Mac App Store アプリケーション：VMware は、Mac App Store で入手できる可能性のあるアプリケーションを、Apple Business Manager からボリューム購入アプリケーションとして提供することを推奨します。アプリケーションがビジネスクリティカルでない場合は、デバイスベースのライセンスを使用してアプリケーションを割り当て、自動更新に設定する必要があります。
- ストア以外のアプリケーション：可能な限り、App Store から入手できないサードパーティ製アプリケーションは、内部アプリケーションとして提供する必要があります（基盤となる munki 統合を活用します）。

MacOS ソフトウェア管理の有効化

[327]

注：このセクションの手順は、ハンズオン ラボですでに完了しています。すでに完了しているため、ソフトウェア管理を有効にする必要はありません。

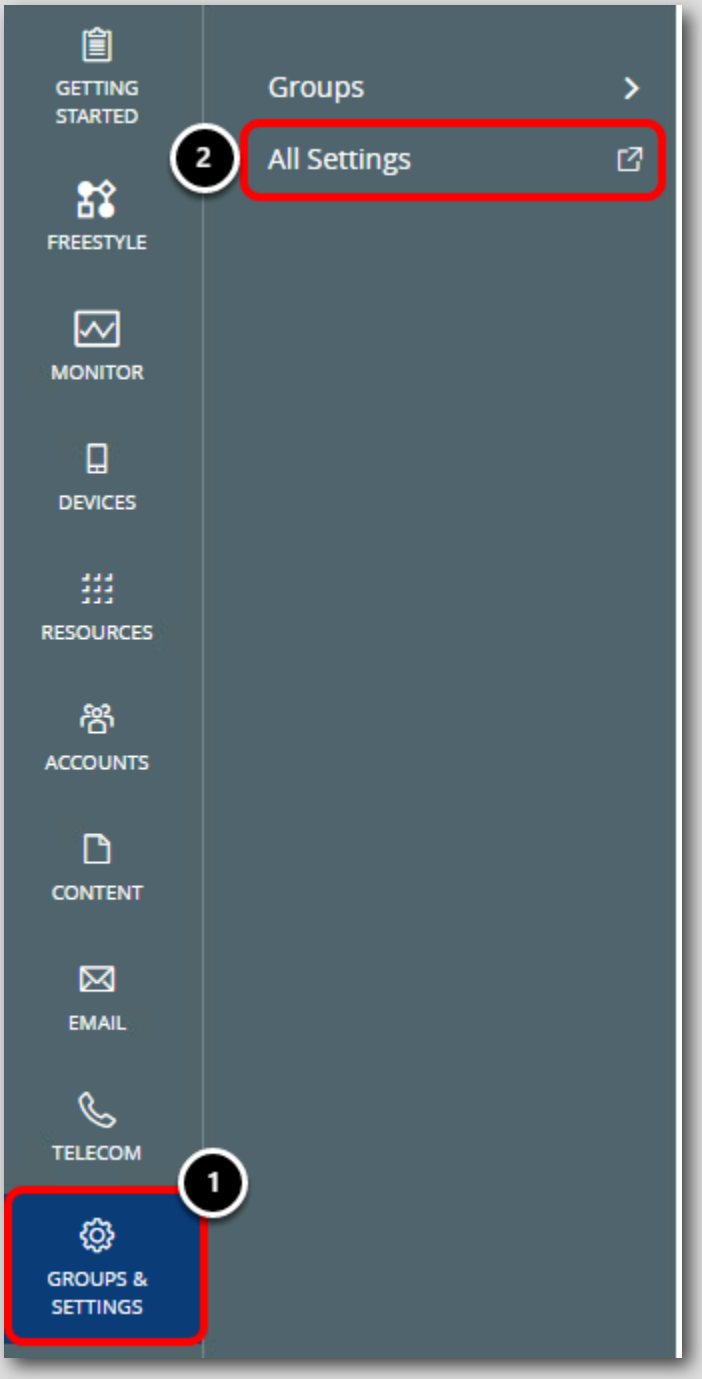
macOS アプリケーションを展開する前に、VMware Workspace ONE UEM 管理者はソフトウェア管理のための環境を有効にする必要があります。以下の項目は、macOS ソフトウェア管理の前提条件です。

1. オンプレミス インストールの場合は、[File Storage] を有効にする必要があります（[Settings] > [Installation] > [File Path]）。
2. [Software Management] を有効にする必要があります（[Settings] > [Devices & Users] > [Apple] > [Apple macOS] > [Software Management]）。
3. macOS バージョン 3.0（以降）の VMware AirWatch Agent。最適なエクスペリエンスは macOS Intelligent Hub によって提供されます。

次の手順に進んでください。

[328]

すべての設定にアクセス（参照用）

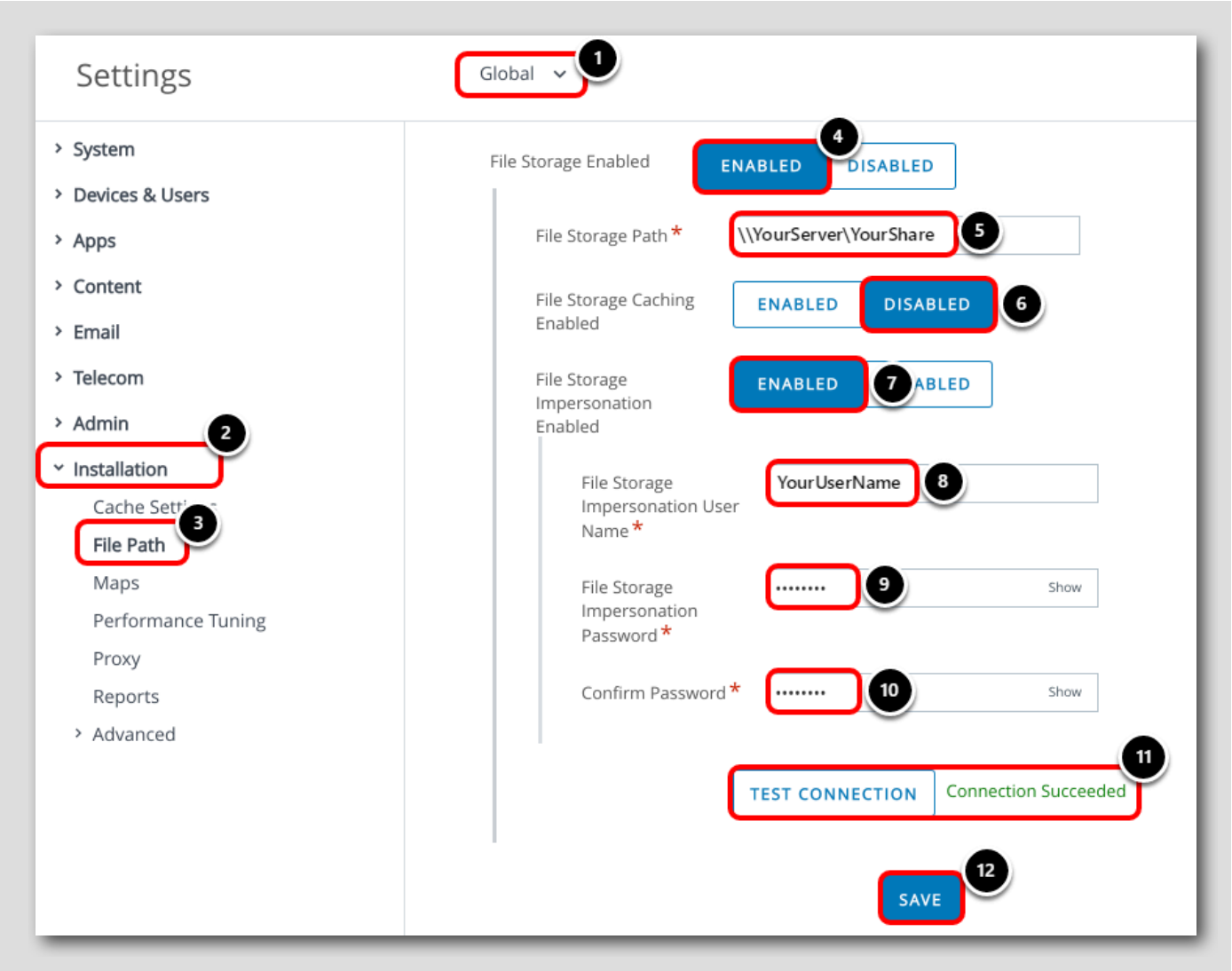


注: このセクションの手順は、ハンズオン ラボですでに完了しています。すでに完了しているため、ソフトウェア管理を有効にする必要はありません。

1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

ファイル ストレージの有効化（参照用）

[329]

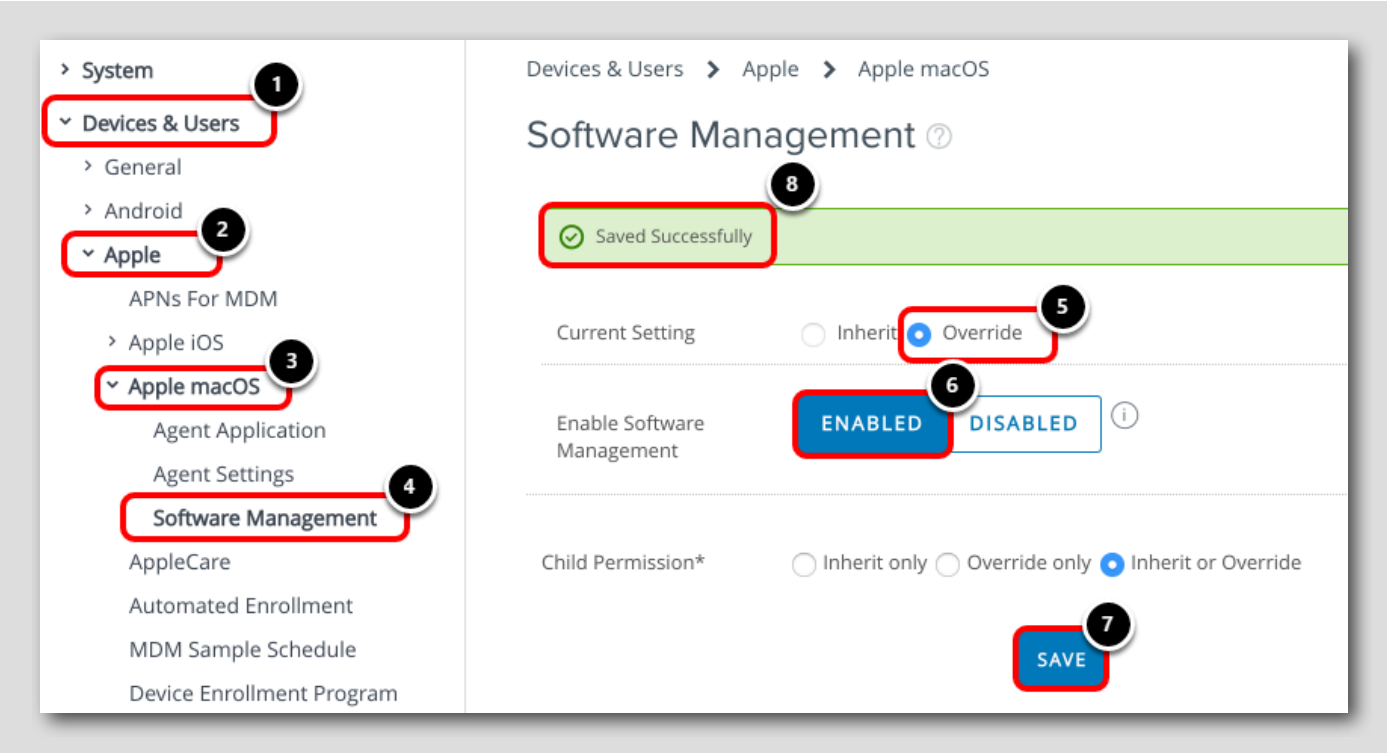


注: このセクションの手順は、ハンズオン ラボですでに完了しています。すでに完了しているため、ソフトウェア管理を有効にする必要はありません。

1. 特定のセットアップで子組織グループを構成する必要がある場合を除き、グローバル組織グループに所属していることを確認します。
2. [Installation] を展開します。
3. [File Path] をクリックします。
4. ファイル パス画面をスクロールし、*[File Storage Enabled]* に対して [Enabled] をクリックします。
5. デバイス サービスおよびコンソール サーバからアクセス可能なファイル共有のパスを入力します。
6. デバイス サービス サーバを計画し、計画に応じてサイズ設定している場合を除き、*[File Storage Caching Enabled]* に対して [Disabled] をクリックします。
7. *[File Storage Impersonation Enabled]* に対して [Enabled] をクリックします。
8. ファイル ストレージ パスにアクセスするためになりすますユーザー名の認証情報を入力します。
9. なりすましユーザーのパスワードを入力します。
10. なりすましユーザーのパスワードを確認します。
11. [Test Connection] をクリックして、「*Connection Succeeded*」と表示されることを確認します。
12. [Save] をクリックします。

ソフトウェア管理の有効化（参照用）

[330]



注: このセクションの手順は、ハンズオン ラボですでに完了しています。すでに完了しているため、ソフトウェア管理を有効にする必要はありません。

1. [Devices & Users] を展開します。
2. [Apple] を展開します。
3. [Apple macOS] を展開します。
4. [Software Management] をクリックします。
5. [Override] をクリックします。
6. *[Enable Software Management]* に対して [Enabled] をクリックします。
7. [Save] をクリックします。
8. 設定が*正常に保存されたことを*確認します。

macOS アプリケーションを展開するための準備

[331]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。

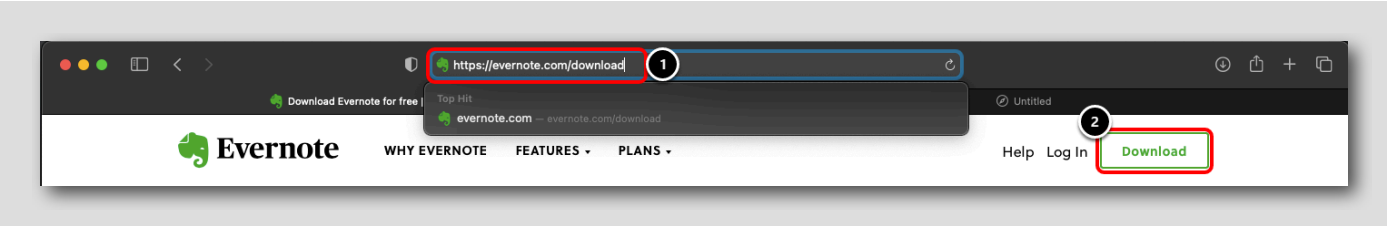
このセクションでは、Workspace ONE Admin Assistant ツールをダウンロードし、別のサードパーティ製アプリケーションを展開するための準備作業に使用します。

Evernote のダウンロード

[332]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



macOS デバイスで、Safari または選択した Web ブラウザを開きます。

1. URL バーに **`https://evernote.com/download`** と入力し、**ENTER** キーを押します。
2. [Download] をクリックします。

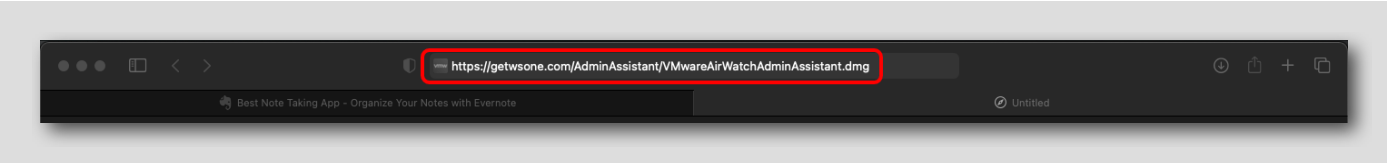
Evernote の DMG ファイルが [Downloads] フォルダにダウンロードされます。

Workspace ONE Admin Assistant ツールのダウンロード

[333]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



Skitch をダウンロードしたときと同じタブで、Safari に次のリンクを貼り付けて Workspace ONE Admin Assistant ツールをダウンロードし、キーボードの **ENTER** キーを押します: **`https://getwsone.com/AdminAssistant/VMwareAirWatchAdminAssistant.dmg`**

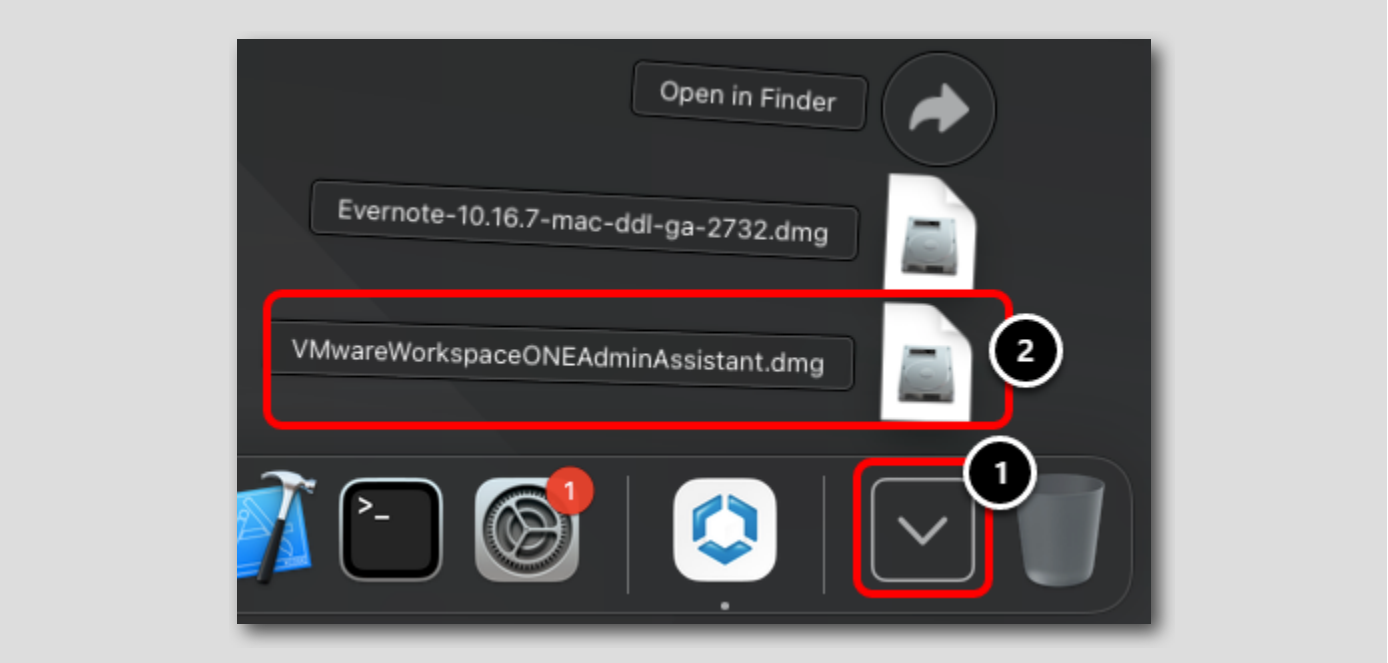
DMG ファイルが [Downloads] フォルダにダウンロードされます。

Workspace ONE Admin Assistant ツールのインストールの開始

[334]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



Dock で、次のように操作します。

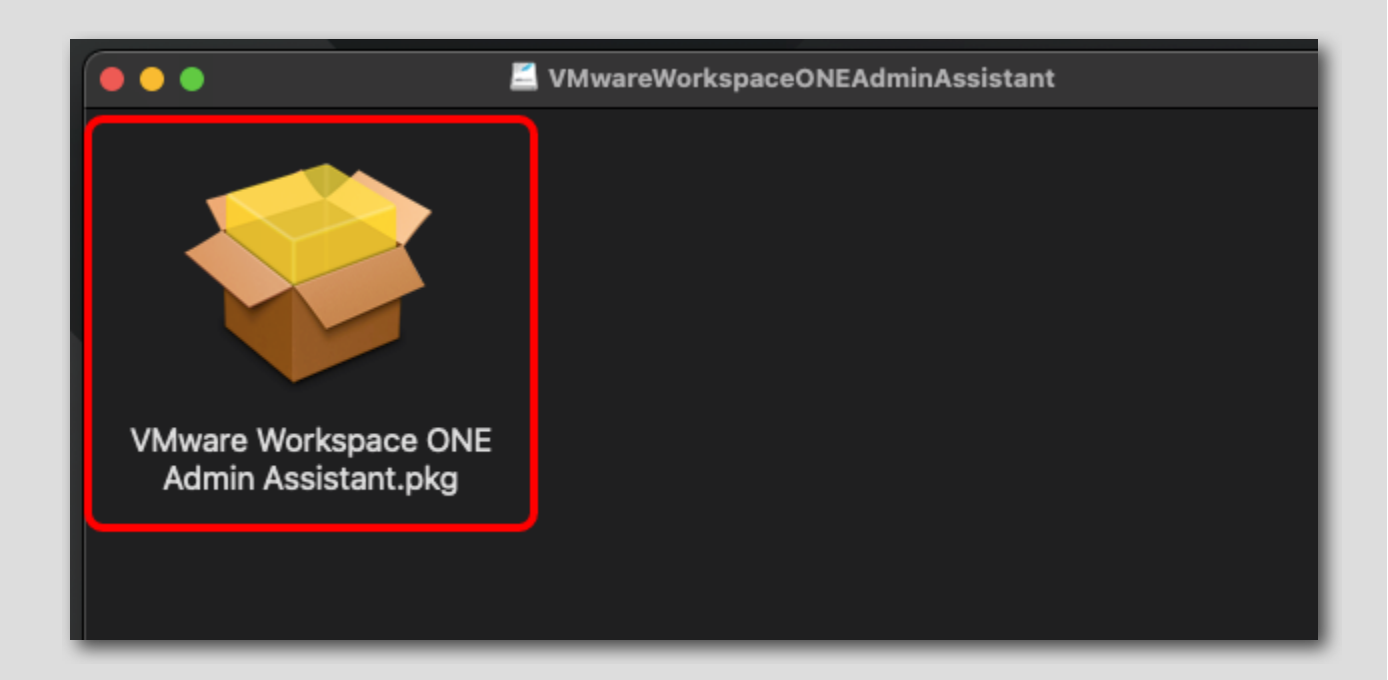
1. [Downloads] フォルダをクリックします。
2. [VMwareWorkspaceONEAdminAssistant.dmg] をクリックします。

インストーラ パッケージの起動

[335]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



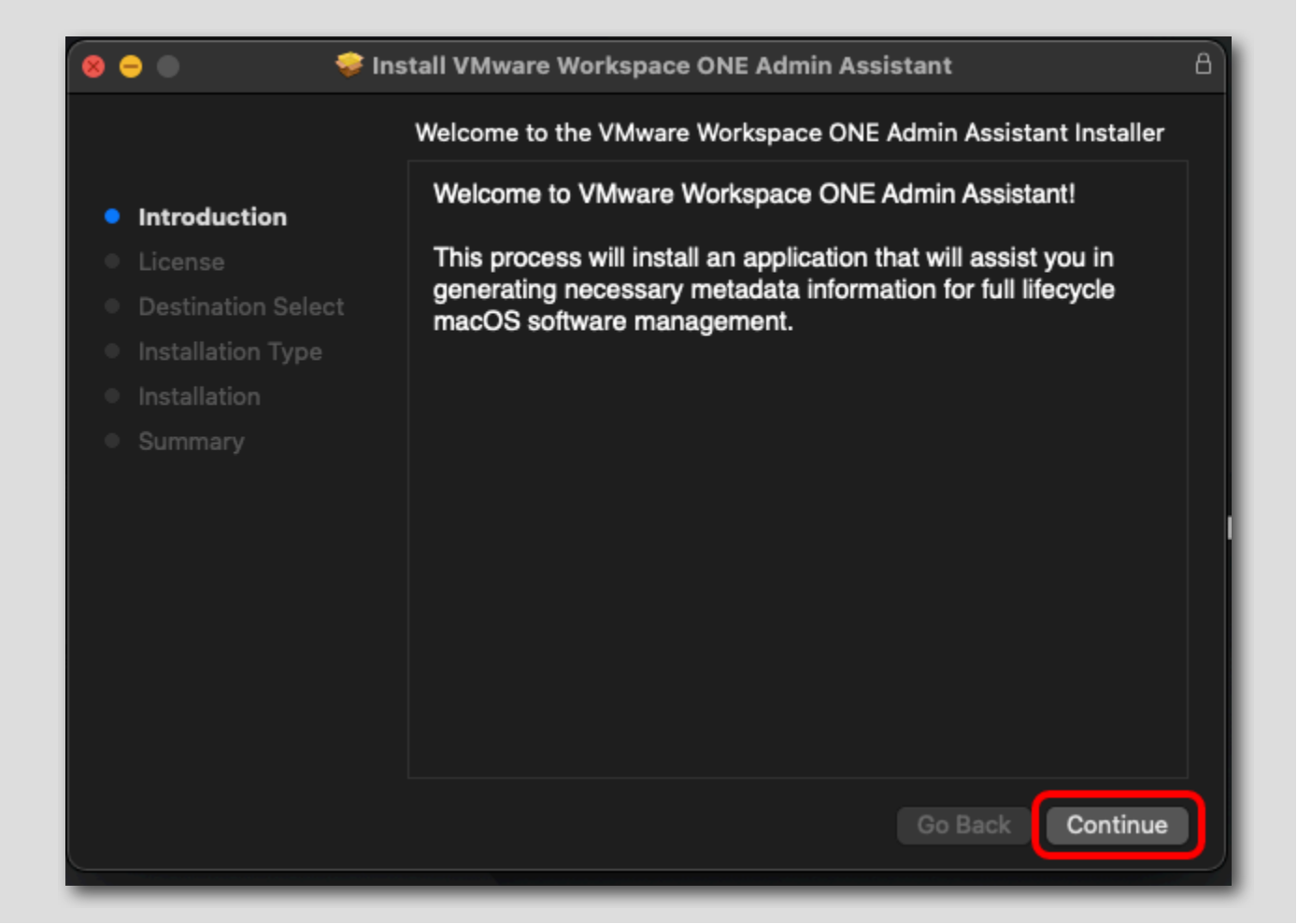
VMware Workspace ONE Admin Assistant.pkg ファイルをダブルクリックします。

インストーラの続行

[336]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



[Continue] をクリックします。

インストーラの確認と続行

[337]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。

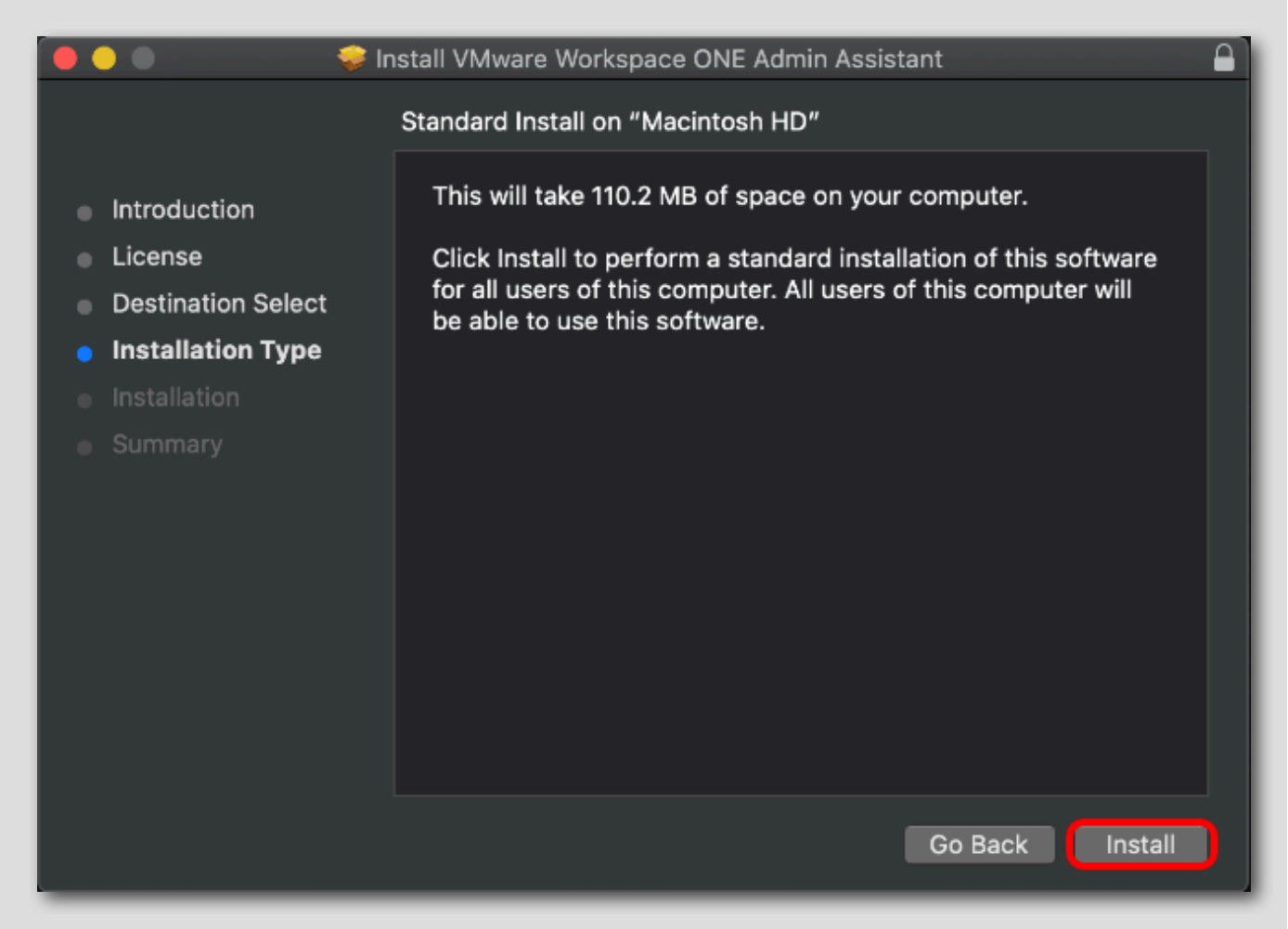
1. 使用許諾契約書を確認し、[Continue] をクリックします。
2. [Agree] をクリックします。

Admin Assistant ツールのインストール

[338]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



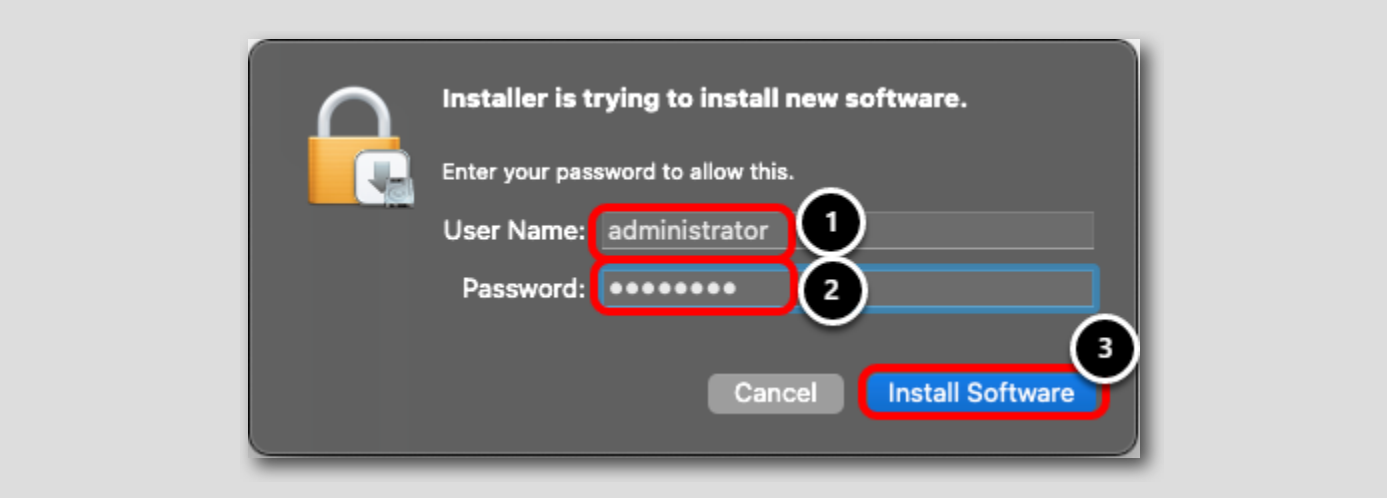
[Install] をクリックします。

管理者認証情報の入力

[339]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



管理者認証情報の入力を求められた場合は、インストールに必要な認証情報を入力します。

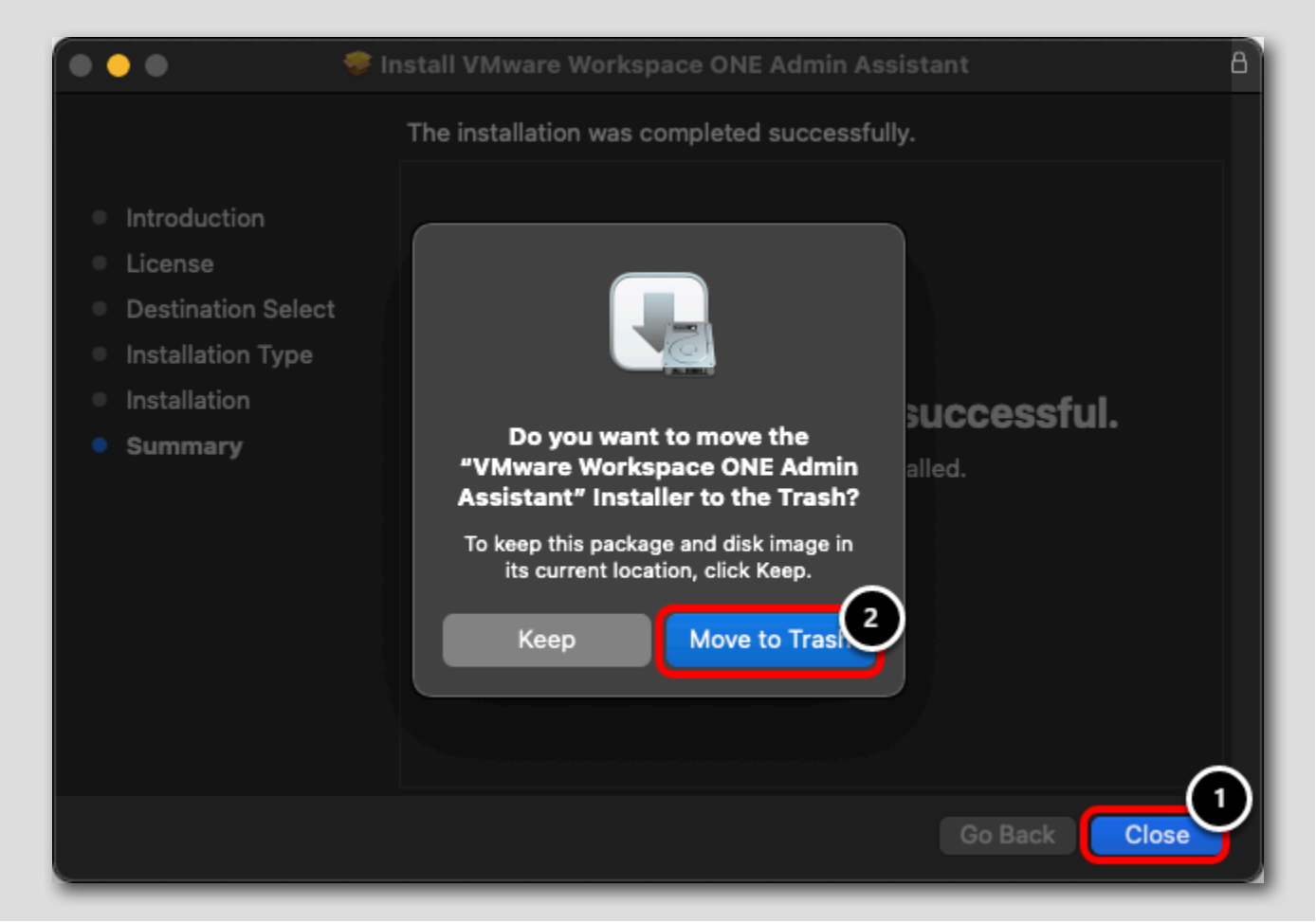
1. デバイスのユーザー名を入力します。
2. デバイスのパスワードを入力します。
3. [Install Software] をクリックします。

インストーラを閉じる

[340]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



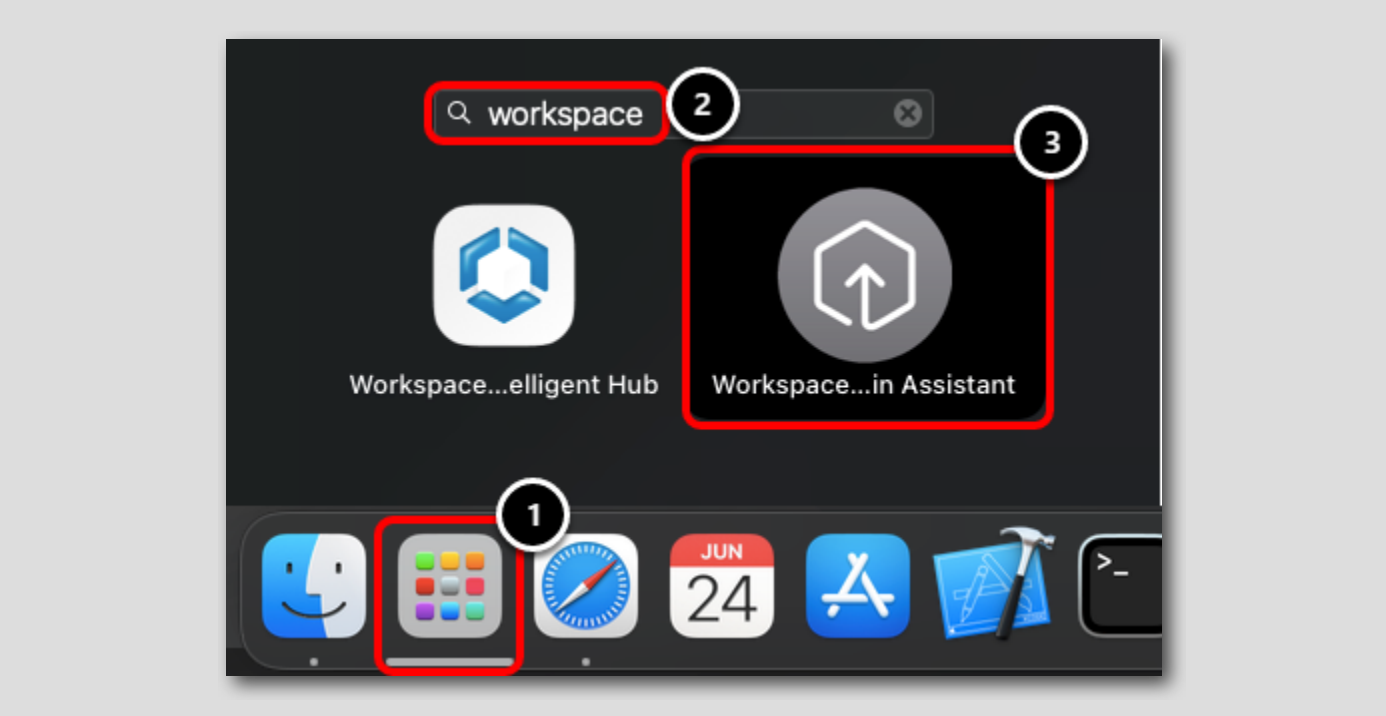
1. インストーラが完了したら、[Close] をクリックします。
2. [Move to Trash] をクリックして、インストーラをクリーンアップします。

VMware Admin Assistant ツールの起動

[341]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



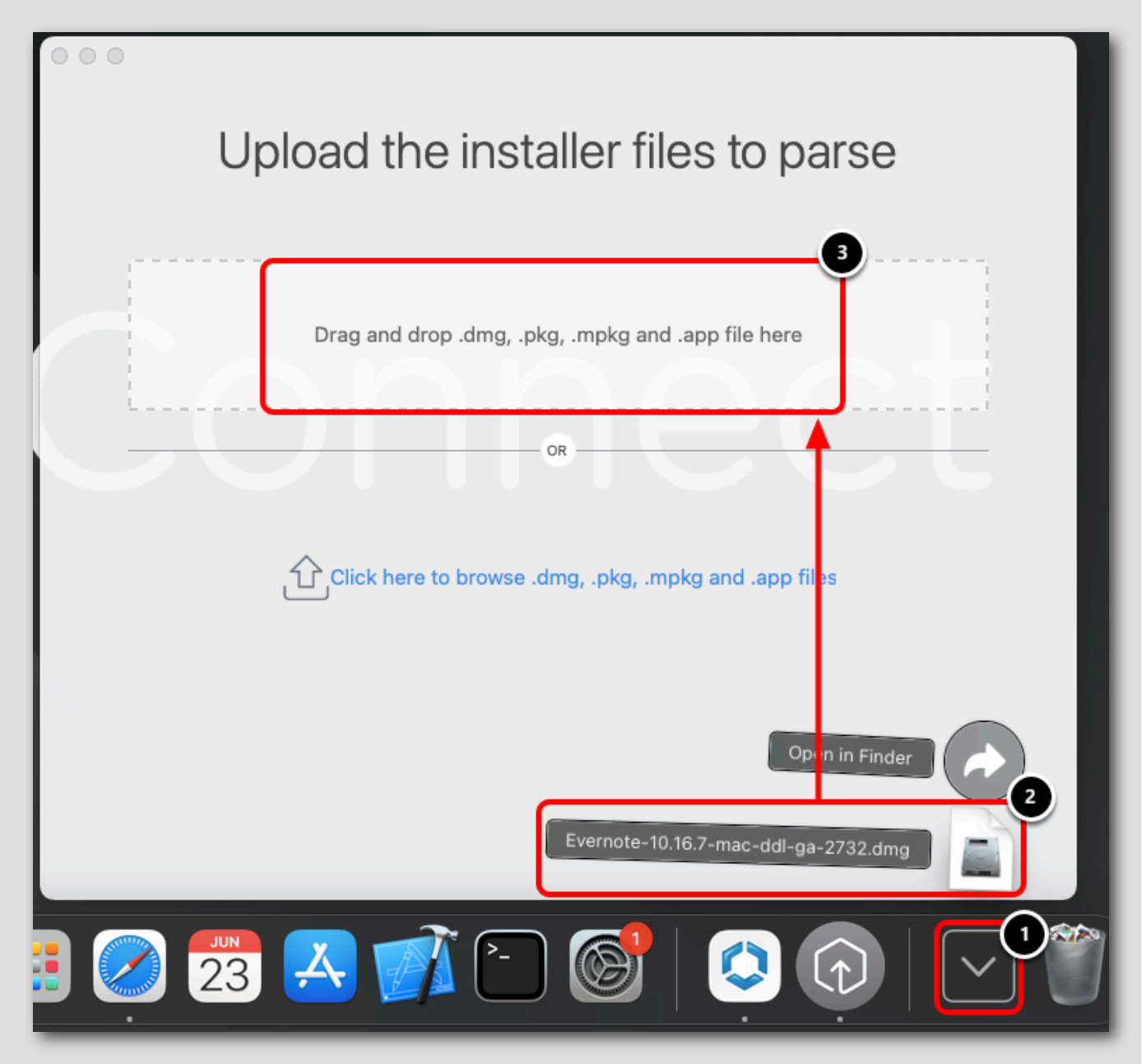
1. Launchpad の起動
2. 検索バーに **`Workspace`** と入力します。
3. Workspace ONE Admin Assistant をクリックします。

Evernote のドラッグアンドドロップ

[342]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



1. Workspace ONE Admin Assistant が開いている状態で、Dock の [Downloads] フォルダをクリックします。
2. [Evernote DMG] をクリックしてドラッグします。
3. [Evernote DMG] を Workspace ONE Admin Assistant アプリケーション ファイルのアップロード セクションにドラッグアンドドロップします。

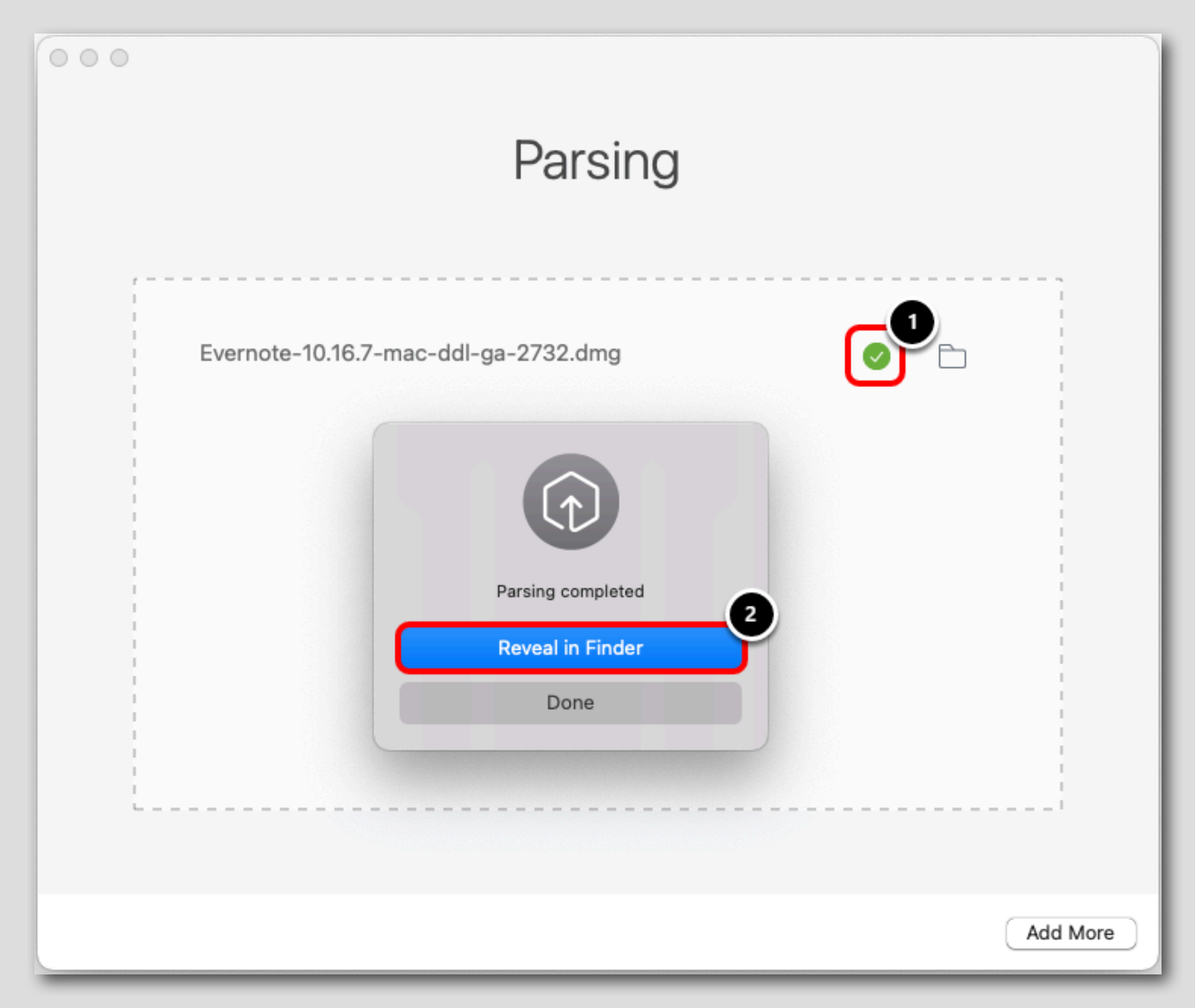
Workspace ONE Admin Assistant ツールは、ソフトウェアの展開に必要な情報を抽出するためにファイルの解析を開始します。

プロセスの監視とファイルの表示

[343]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



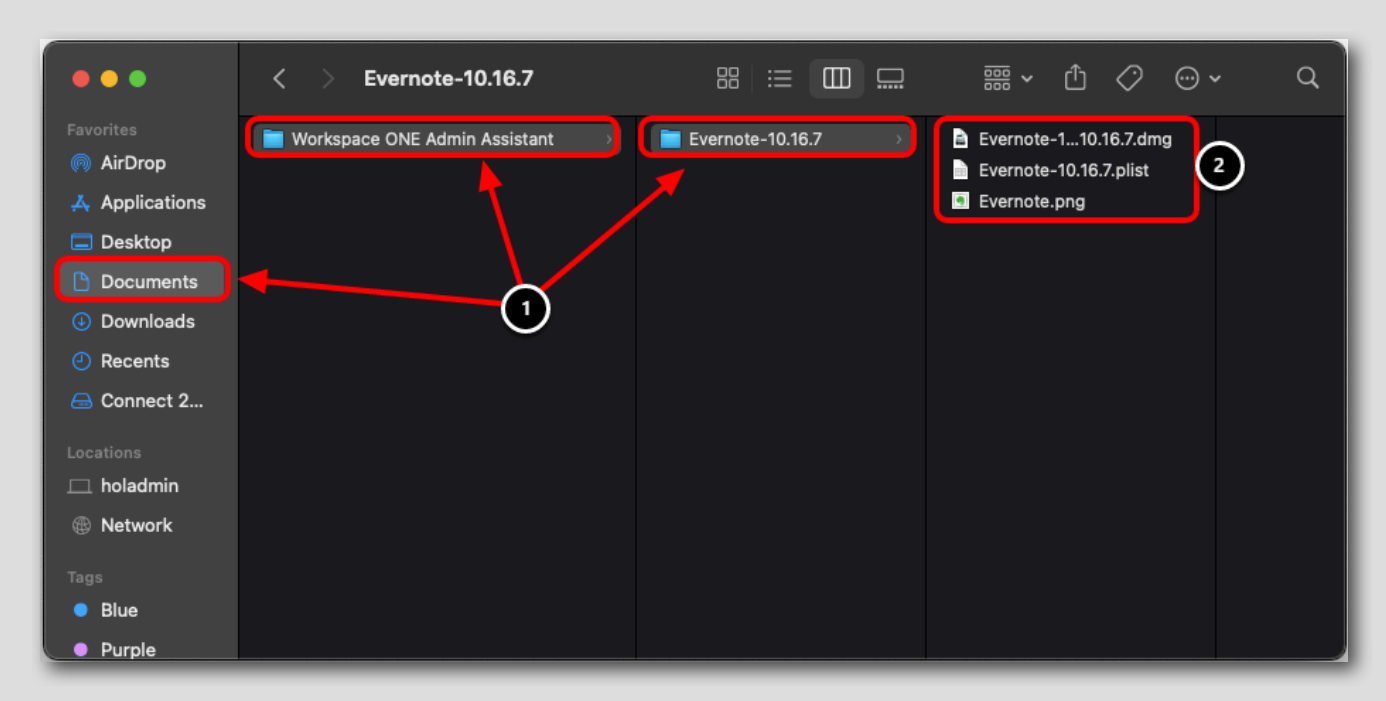
1. 解析の進行状況を監視します。完了すると、結果は緑色のチェックマークに変わります。これには 15 ～ 30 秒かかる場合があります。
2. ポップアップ ウィンドウで、[Reveal in Finder] をクリックします。

生成されたファイルの確認

[344]

注: ハンズオン ラボには必要なアプリケーション ファイルが含まれるため、これらの手順はオプションです。macOS でのアプリケーション展開に必要なファイルを抽出する方法を確認したい場合は、これらの手順に進んでください。そうでない場合は、ここをクリックして、アプリケーション ファイルのアップロードを続行します。

注: これらの手順には macOS デバイスが必要です。



[Finder] ウィンドウで、次のように操作します。

1. Evernote ファイルの出力パスを確認します: ~/Documents/Workspace ONE Admin Assistant/Evernote-##.##.##
2. Assistant ツールの出力が次のように表示されることを確認します。

```
Evernote-##.##.##.dmg -- The Application has been packaged into a DMG file. (Note: MPKG and PKG files
Evernote-##.##.##.plist -- A metadata file (referenced as the pkginfo.plist in munki documentation)
Evernote.png -- An icon image extracted from the app used for user-friendly display in the console
```

Admin Assistant ツールのすべての出力は、「~/Documents/Workspace ONE Admin Assistant/{AppName-Version}」の規則に従います。このラボが作成された時点での Evernote のバージョンは 10.16.7 ですが、このラボに参加するタイミングによって異なる場合があります。

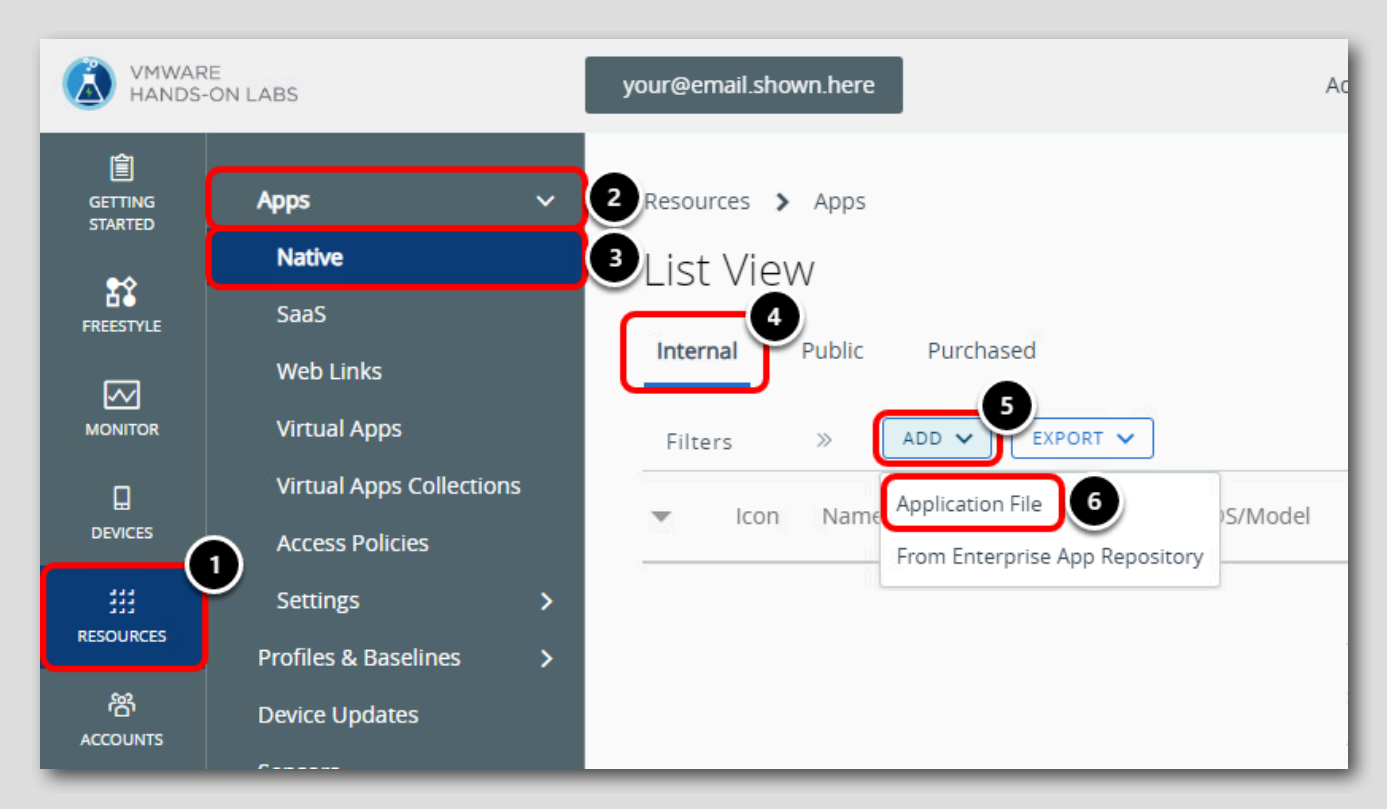
サードパーティ製 macOS アプリケーションの展開

[345]

提供されている Workspace ONE Assist dmg ファイルと plist ファイルを使用して、Workspace ONE Assist をサードパーティの macOS アプリケーションとして Workspace ONE UEM にアップロードします。

アプリケーション ファイルの追加

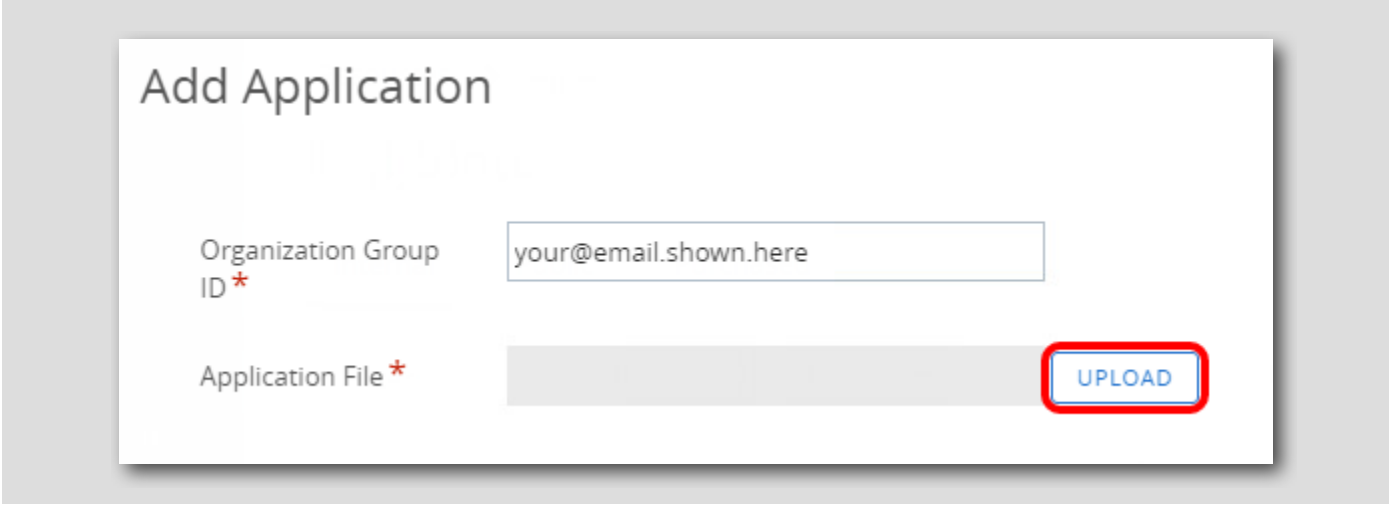
[346]



ハンズオン ラボのインターフェイスで、Workspace ONE UEM 管理者コンソールに戻ります。

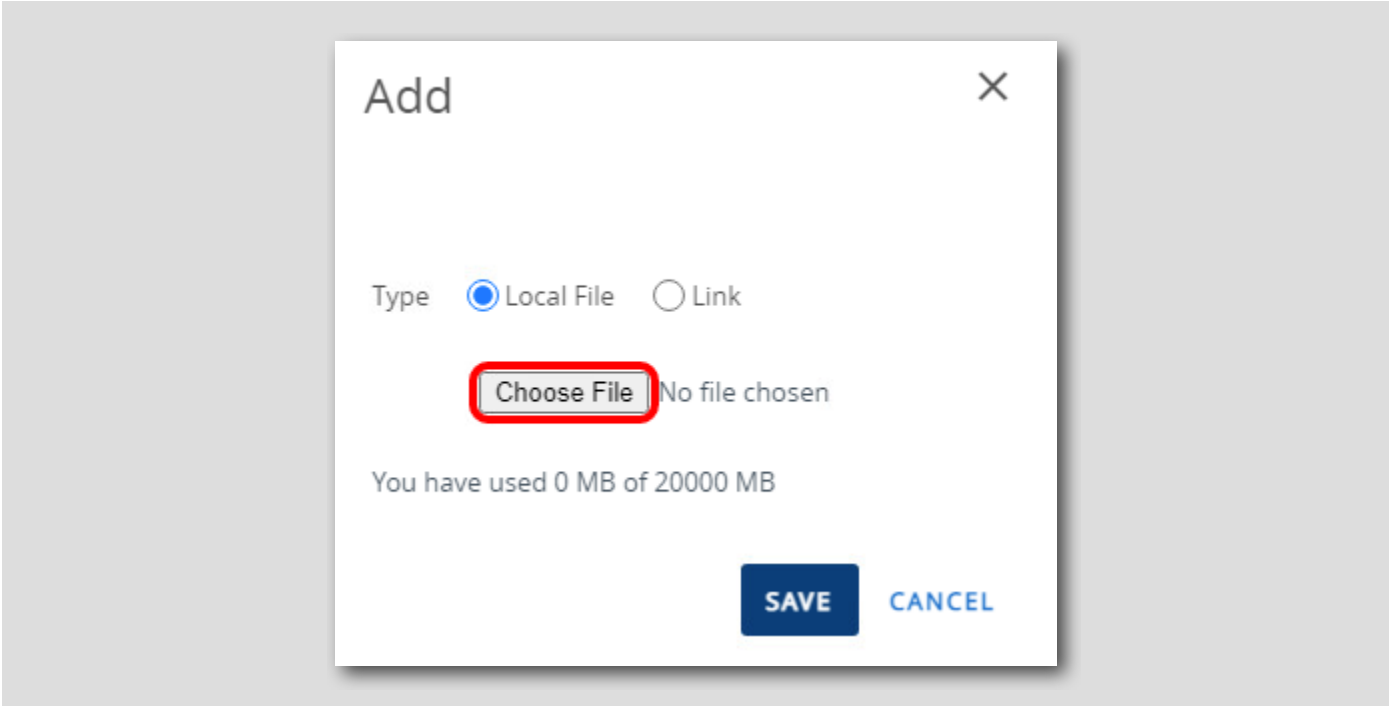
1. [Resources] をクリックします。
2. [Apps] を展開します。
3. [Native] をクリックします。
4. [Internal] タブをクリックします。
5. [Add] をクリックします。
6. [Application File] をクリックします。

アプリケーション ファイルのアップロード [347]



[Upload] をクリックします。

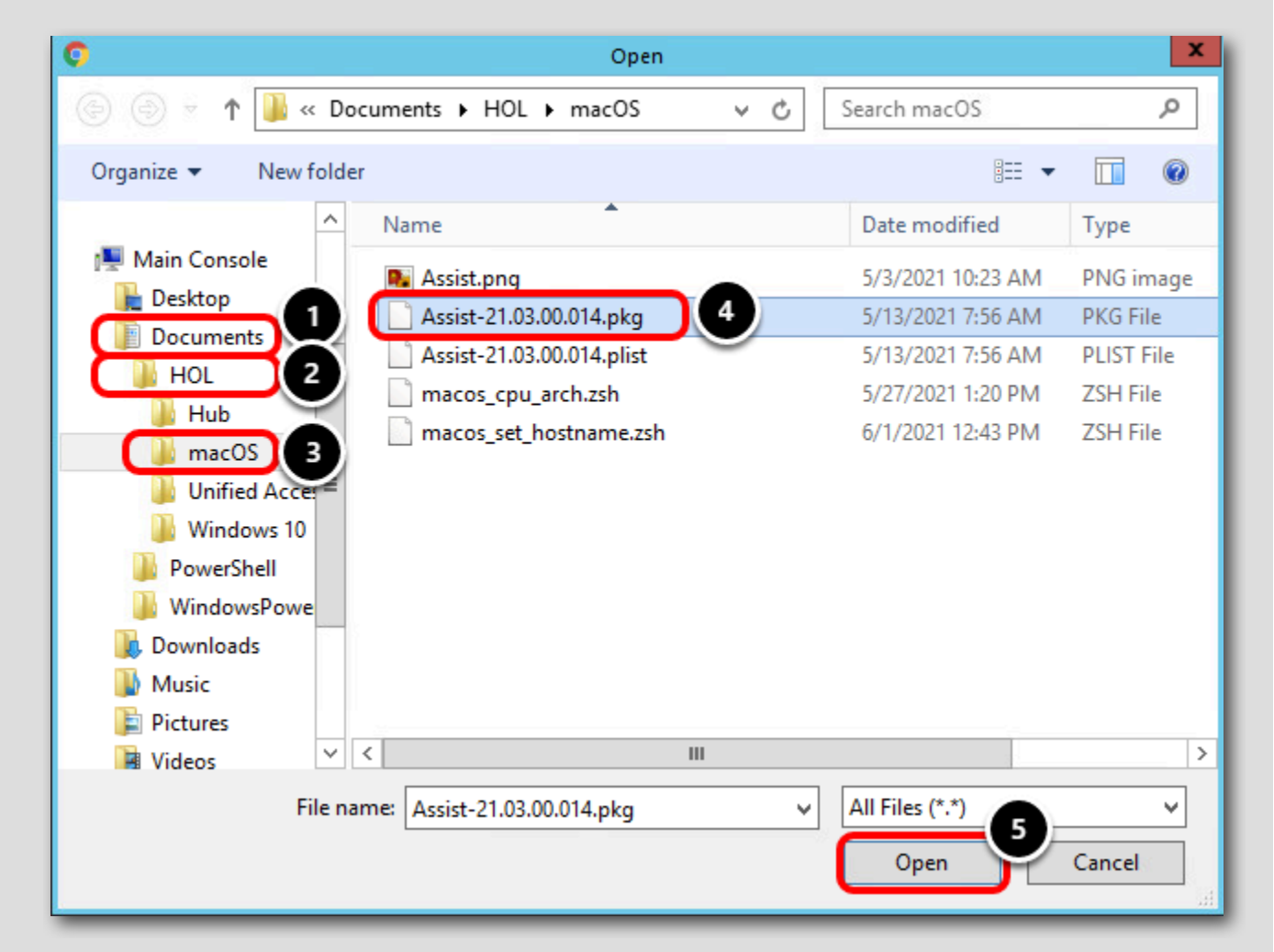
アップロードするファイルの選択 [348]



[Choose File] をクリックします。

Assist PKG ファイルの選択

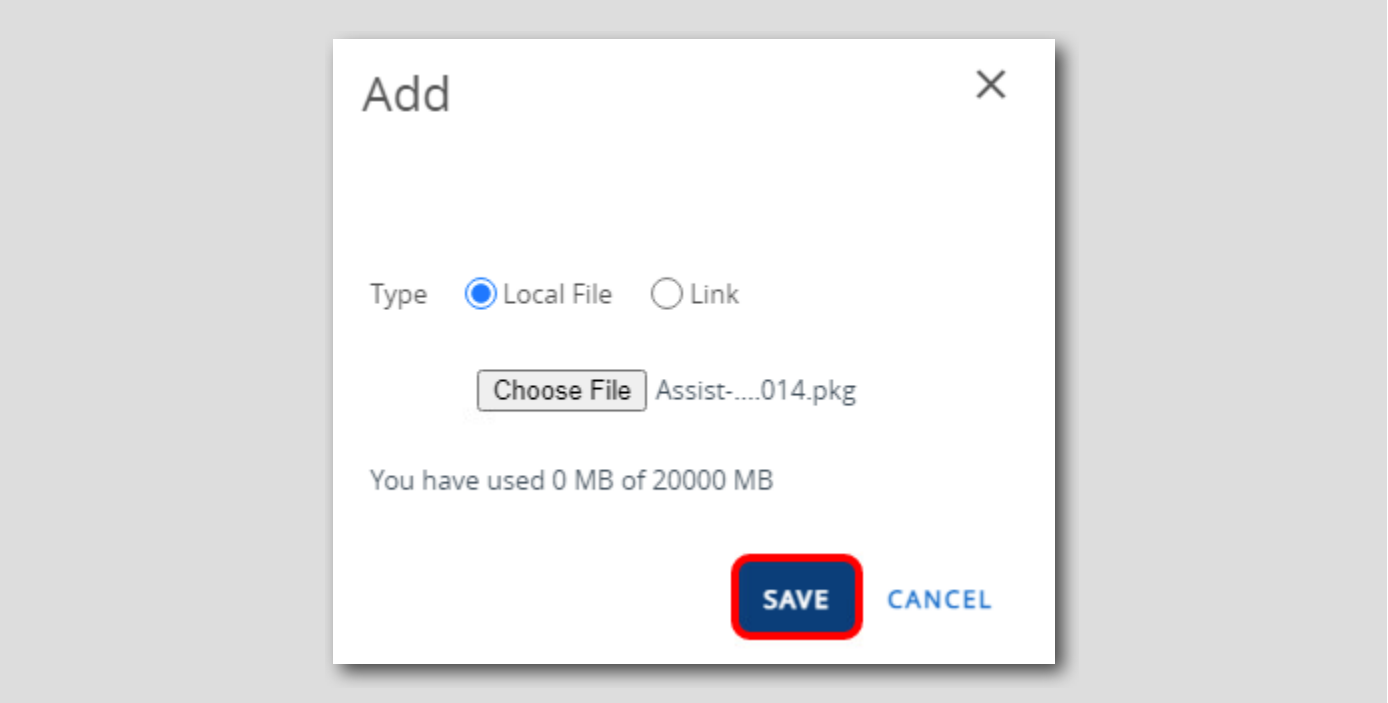
[349]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [macOS] をクリックします。
4. [Assist-21.03.00.014.pkg] をクリックします。
5. [Open] をクリックします。

Assist PKG ファイルのアップロード

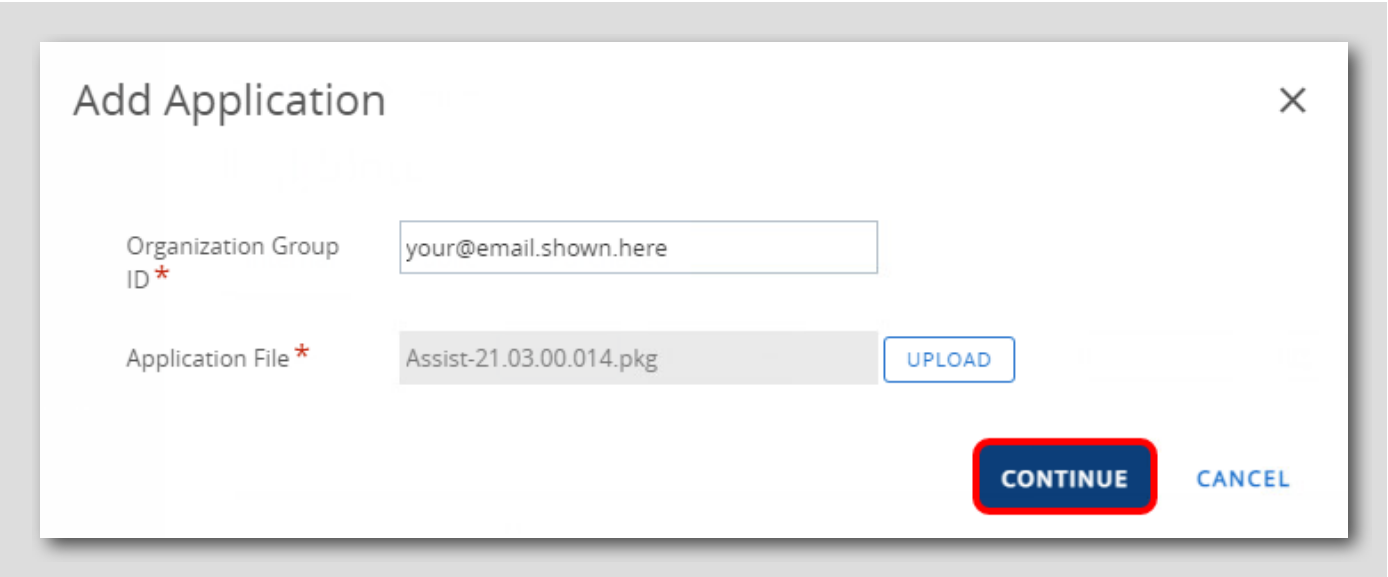
[350]



[Save] をクリックして、選択した Assist-21.03.00.014.pkg ファイルをアップロードします。

注：pkg ファイルのアップロードには 1 ～ 2 分かかることがあります。アップロードが完了したら、次の手順に進みます。

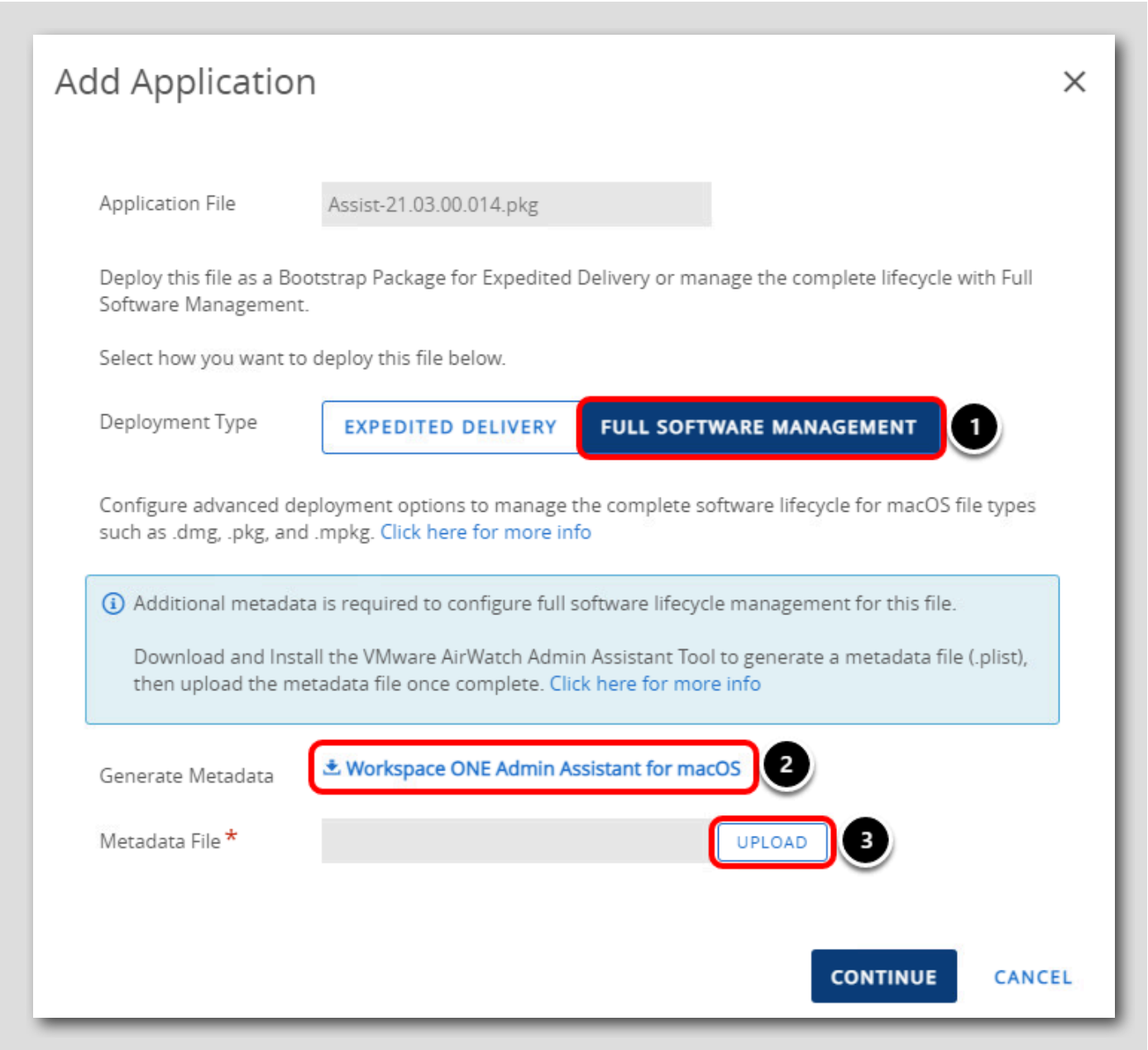
アプリケーションのアップロード後の続行 [351]



[Continue] をクリックします。

展開タイプの構成

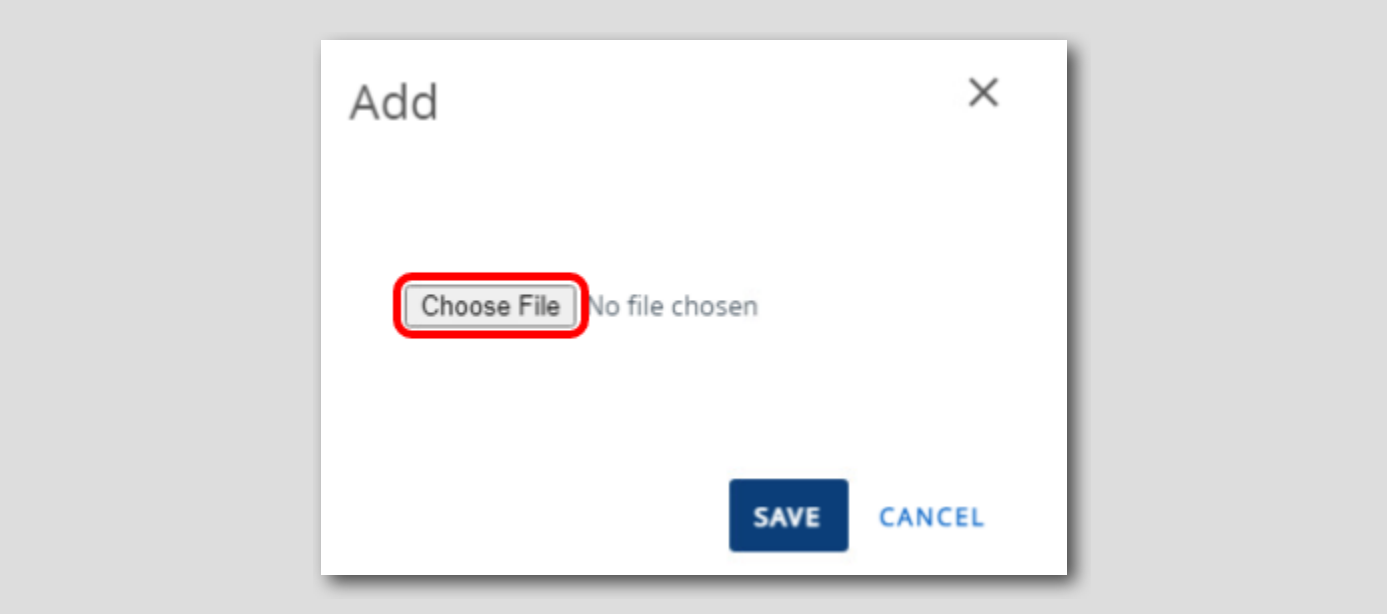
[352]



1. [Deployment Type] で **[Full Software Management]** を選択します。
2. macOS の Workspace ONE Admin Assistant は、必要に応じてこのページからダウンロードできます。これは情報提供のみを目的としたもので、前の手順で macOS デバイスでアプリケーションを使用する方法をすでに確認しているため、Workspace ONE Admin Assistant をダウンロードする必要はありません。
3. **[Upload]** をクリックして、このアプリケーションのメタデータ ファイルを指定します。

メタデータ ファイルの選択

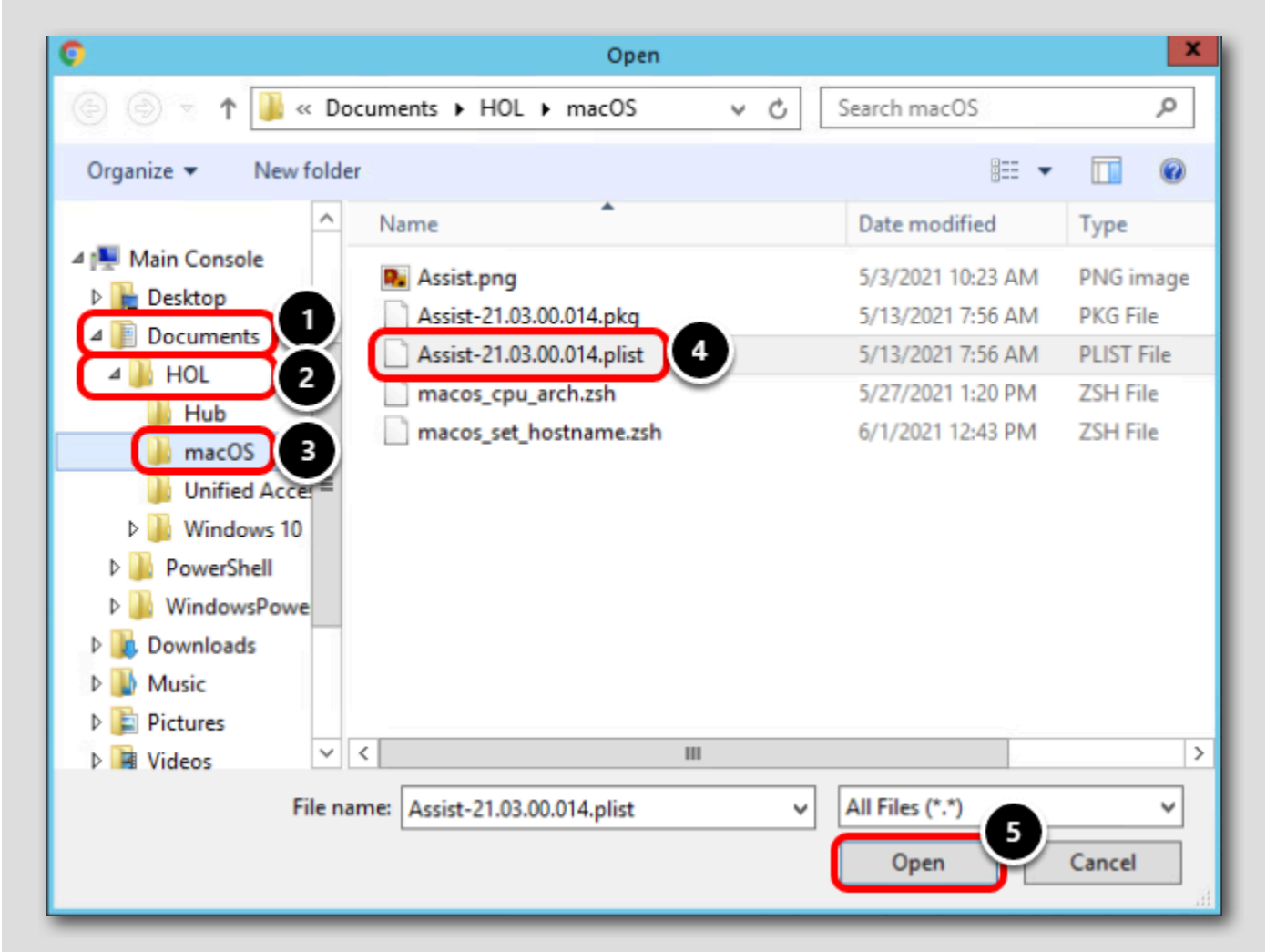
[353]



[Choose File] をクリックします。

Workspace ONE Assist plist ファイルの選択

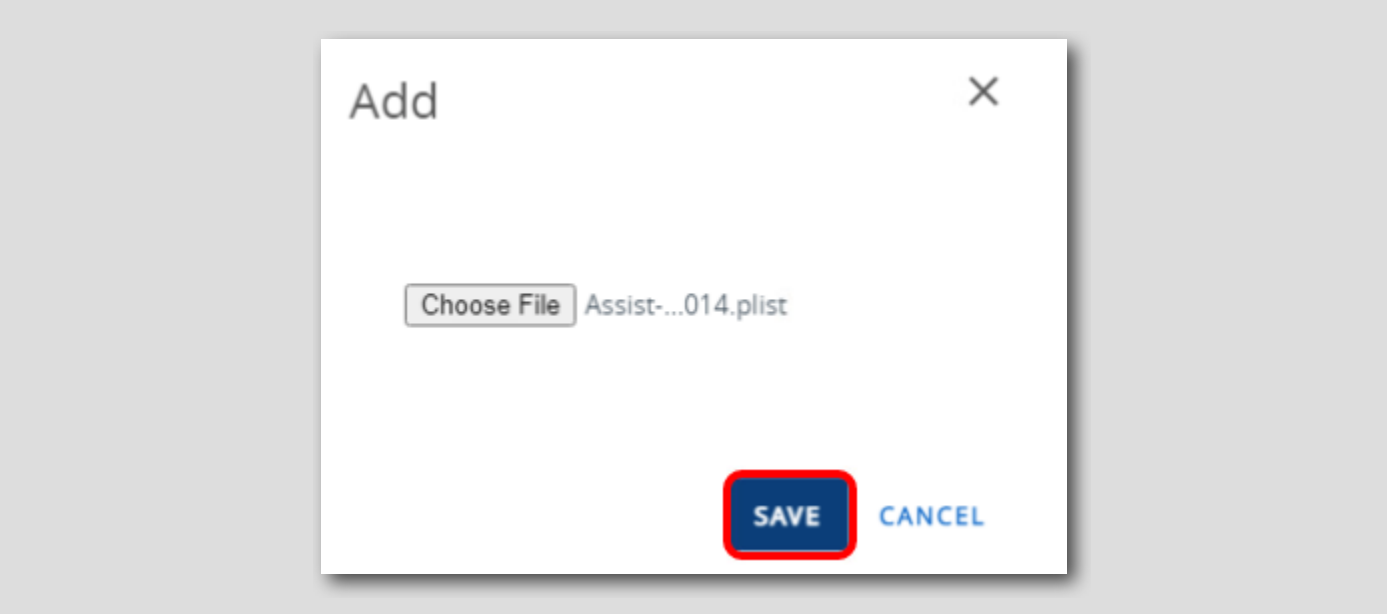
[354]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [macOS] をクリックします。
4. [Assist-21.03.00.014.plist] をクリックします。
5. [Open] をクリックします。

Assist plist ファイルのアップロード

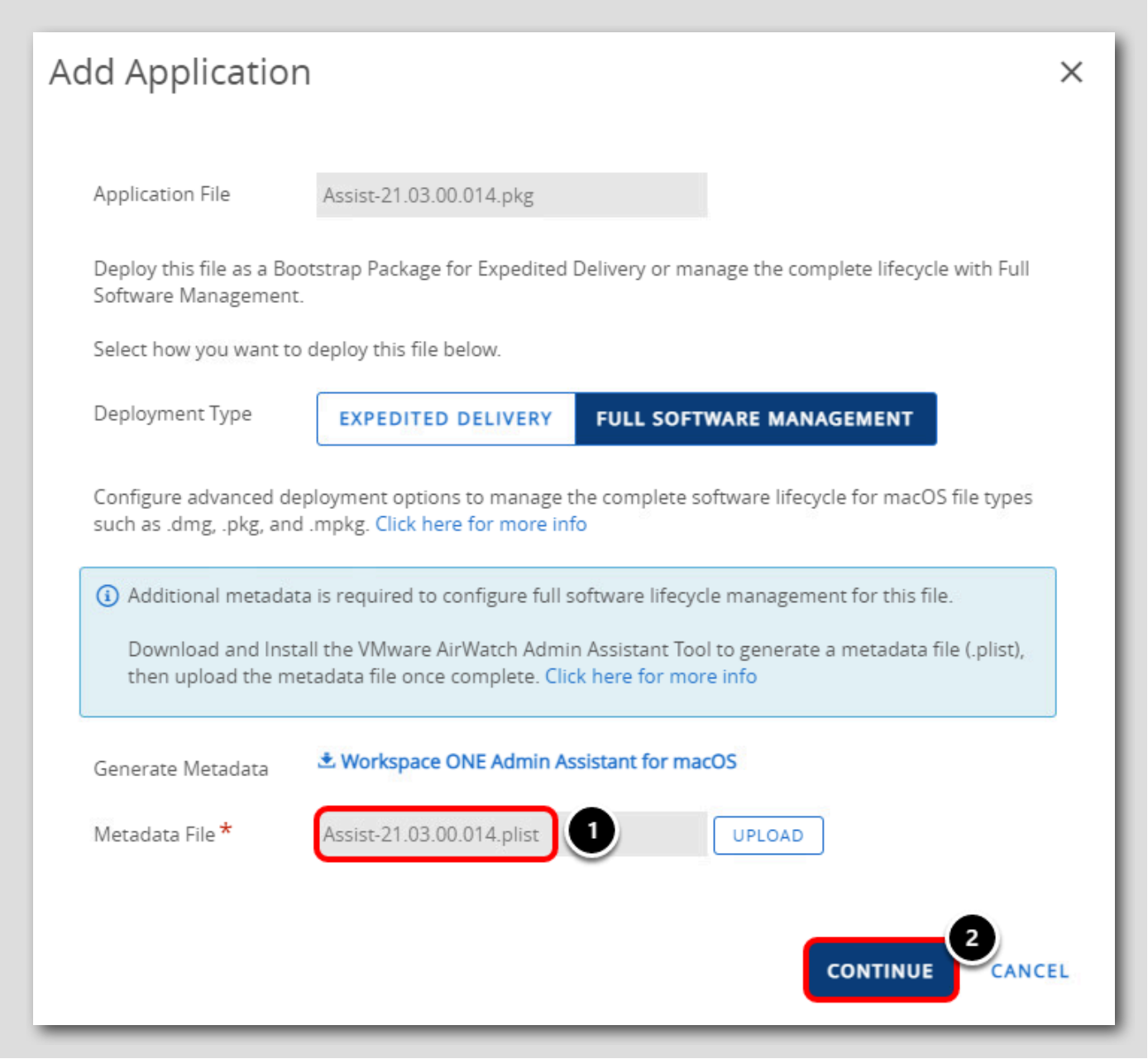
[355]



[Save] をクリックして、選択した Assist-21.03.00.014 plist ファイルをアップロードします。

メタデータ ファイルのアップロード後の続行

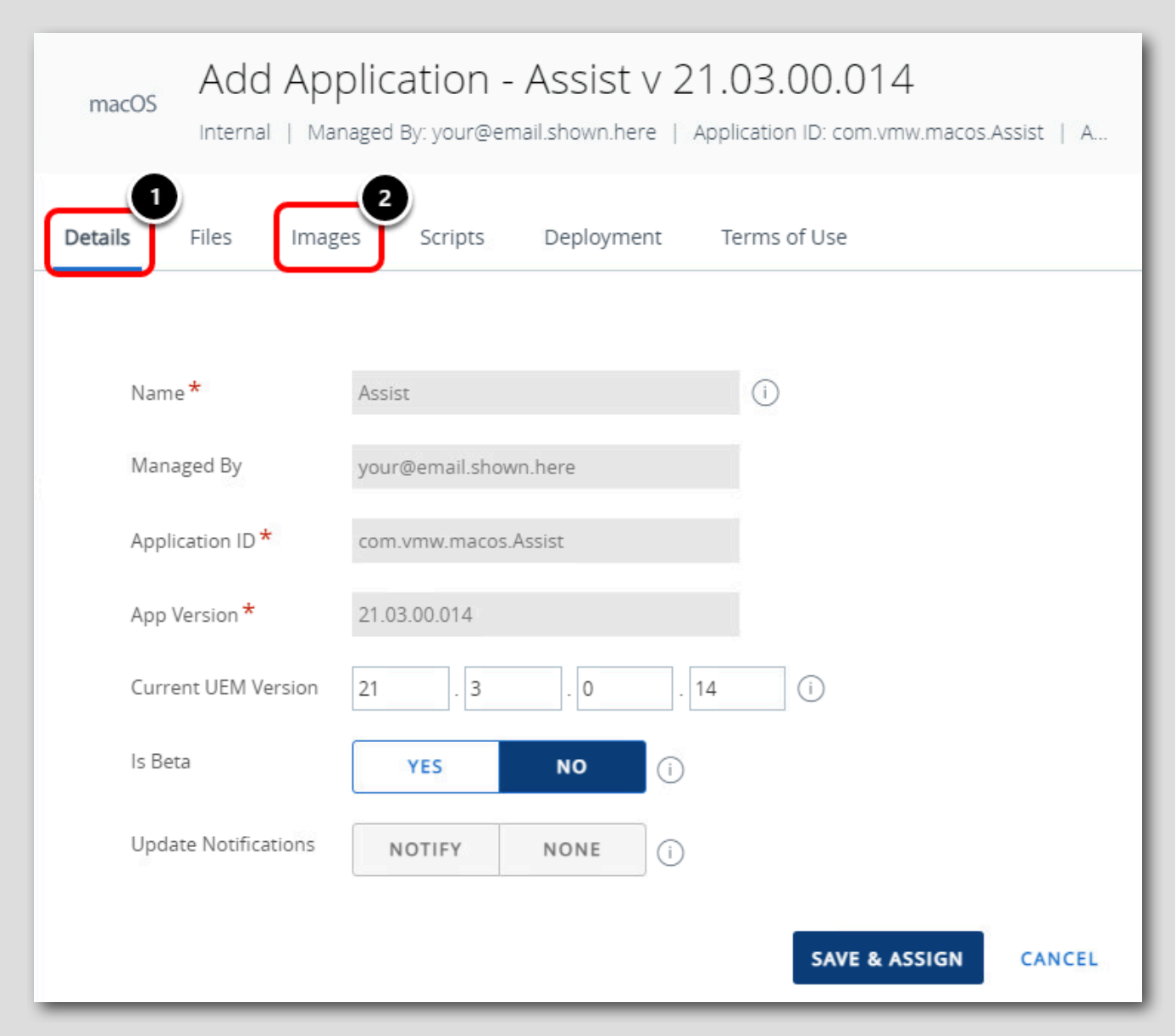
[356]



1. Assist メタデータ ファイルがアップロードされました。
2. [Continue] をクリックします。

アプリケーションの構成

[357]

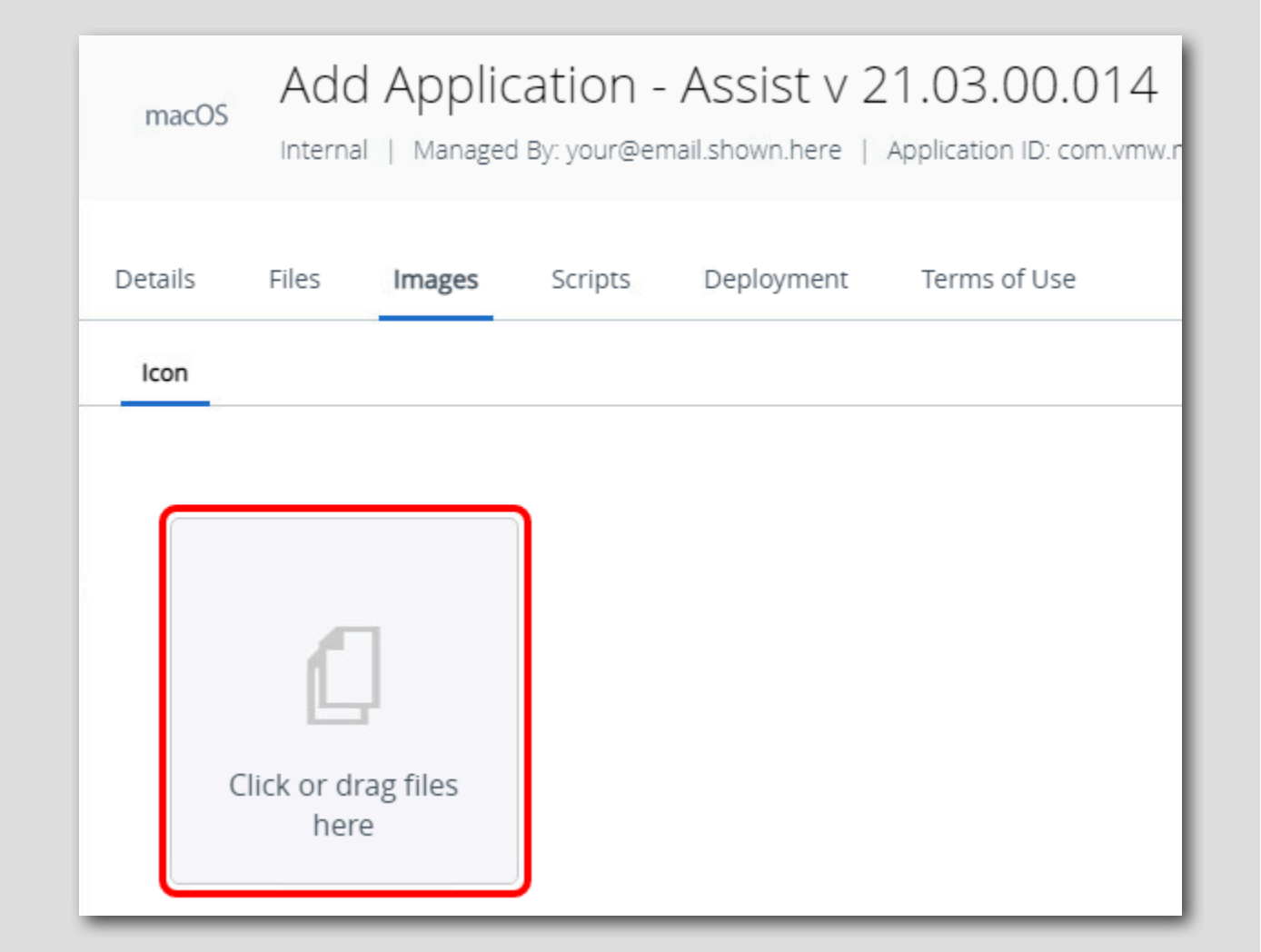


Workspace ONE Assist アプリケーションと対応するメタデータが Workspace ONE UEM にアップロードされました。

1. [Details] タブには、アプリケーション ID、バージョン、サポートされているデバイス モデルなどが表示されます。この情報は、提供された plist メタデータから収集されます。必要に応じて [Details] タブやその他のタブを自由に確認できますが、変更は行わないでください。
2. [Images] タブをクリックします。

アプリケーション アイコンの構成

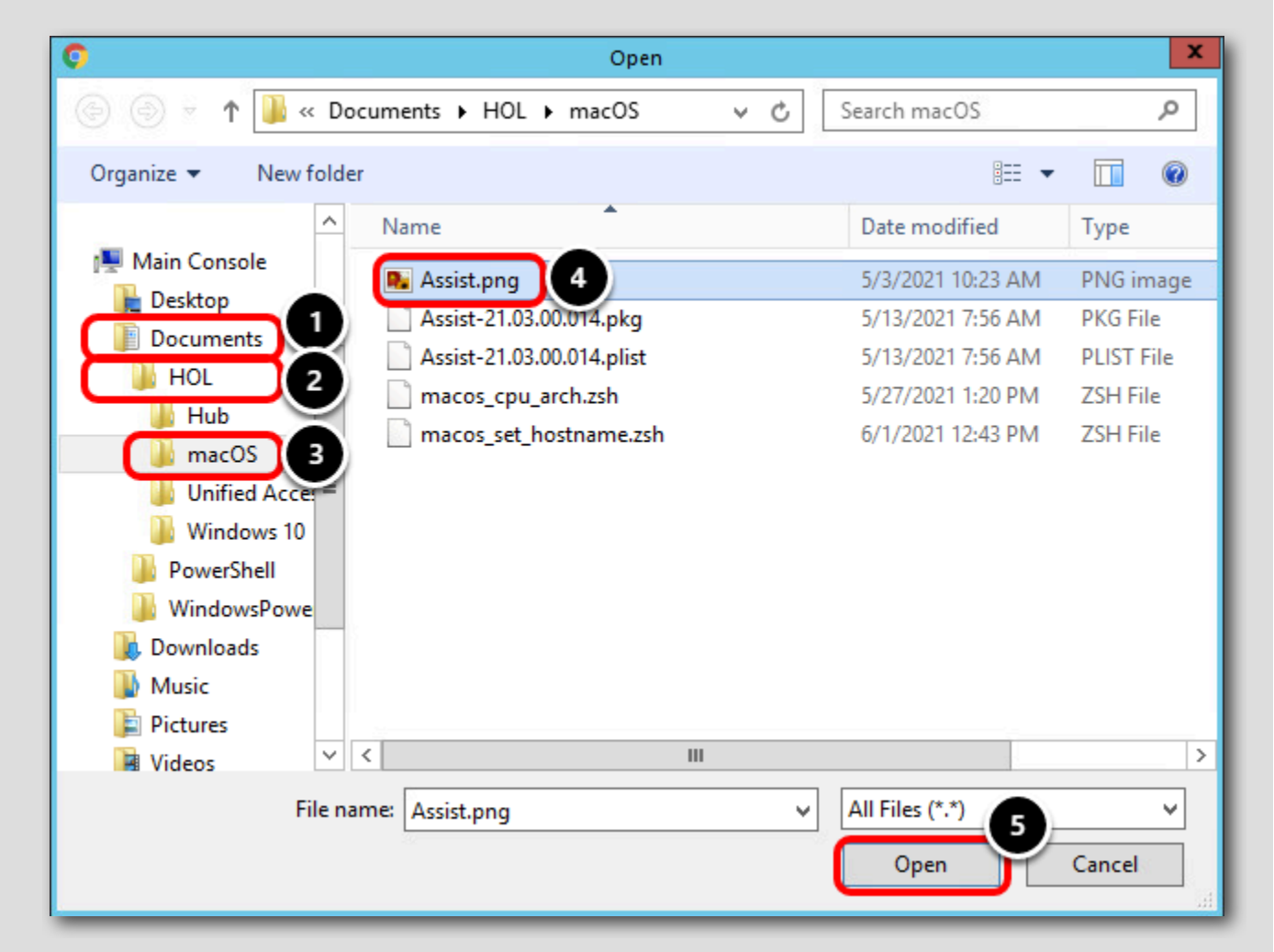
[358]



アプリケーションのアイコンを追加する必要があります。このアイコンは、インストール後にアプリケーション カタログとユーザーのデバイスに表示されます。[click or drag files here] 領域をクリックして、画像をアップロードします。

[Assist] アイコンの選択

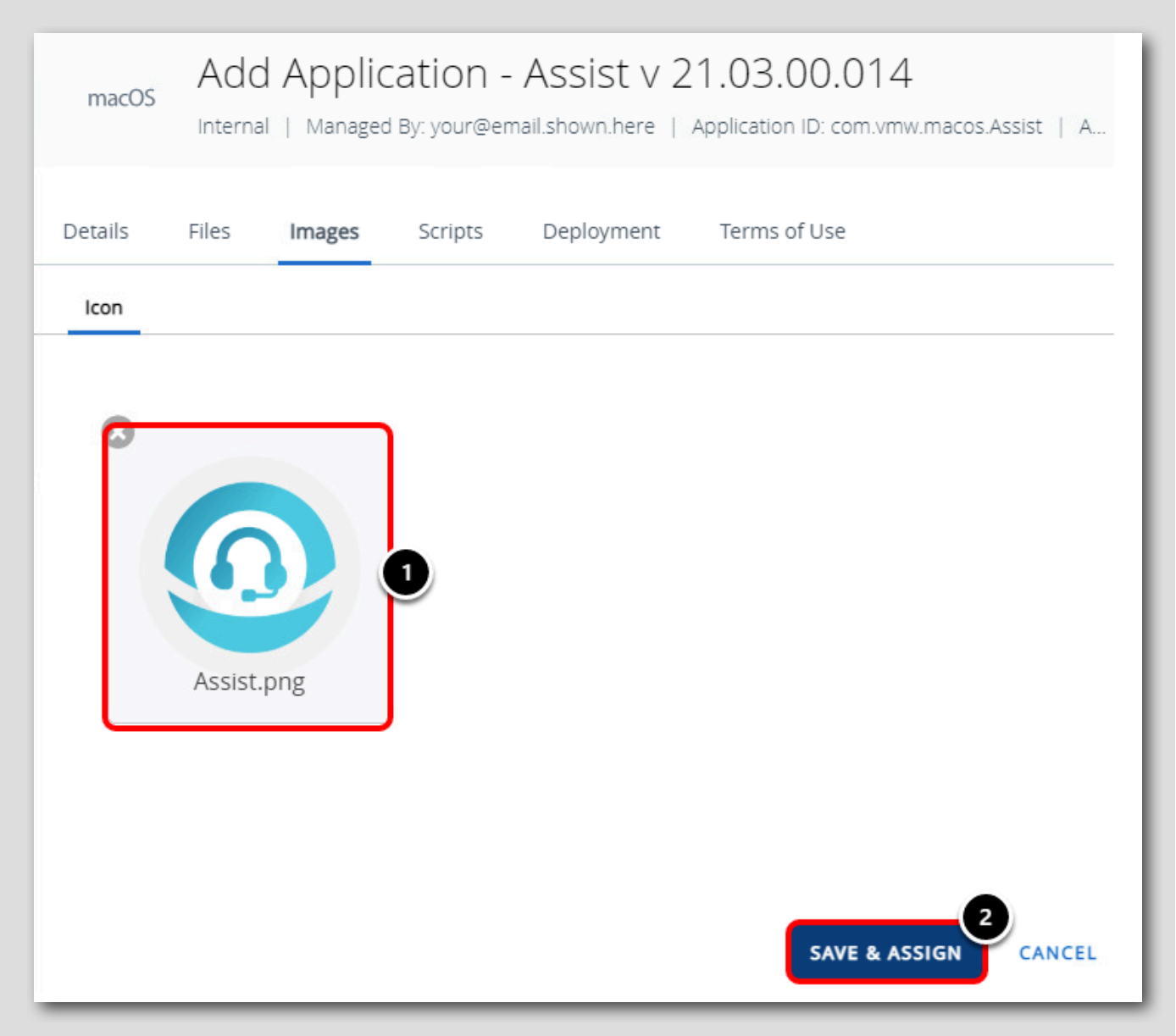
[359]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [macOS] をクリックします。
4. Workspace ONE Admin Assistant ツールも、使用する画像を抽出して提供します。この画像は Assist.png として使用できます。[Assist.png] をクリックします。
5. [Open] をクリックします。

アイコンを確認して保存

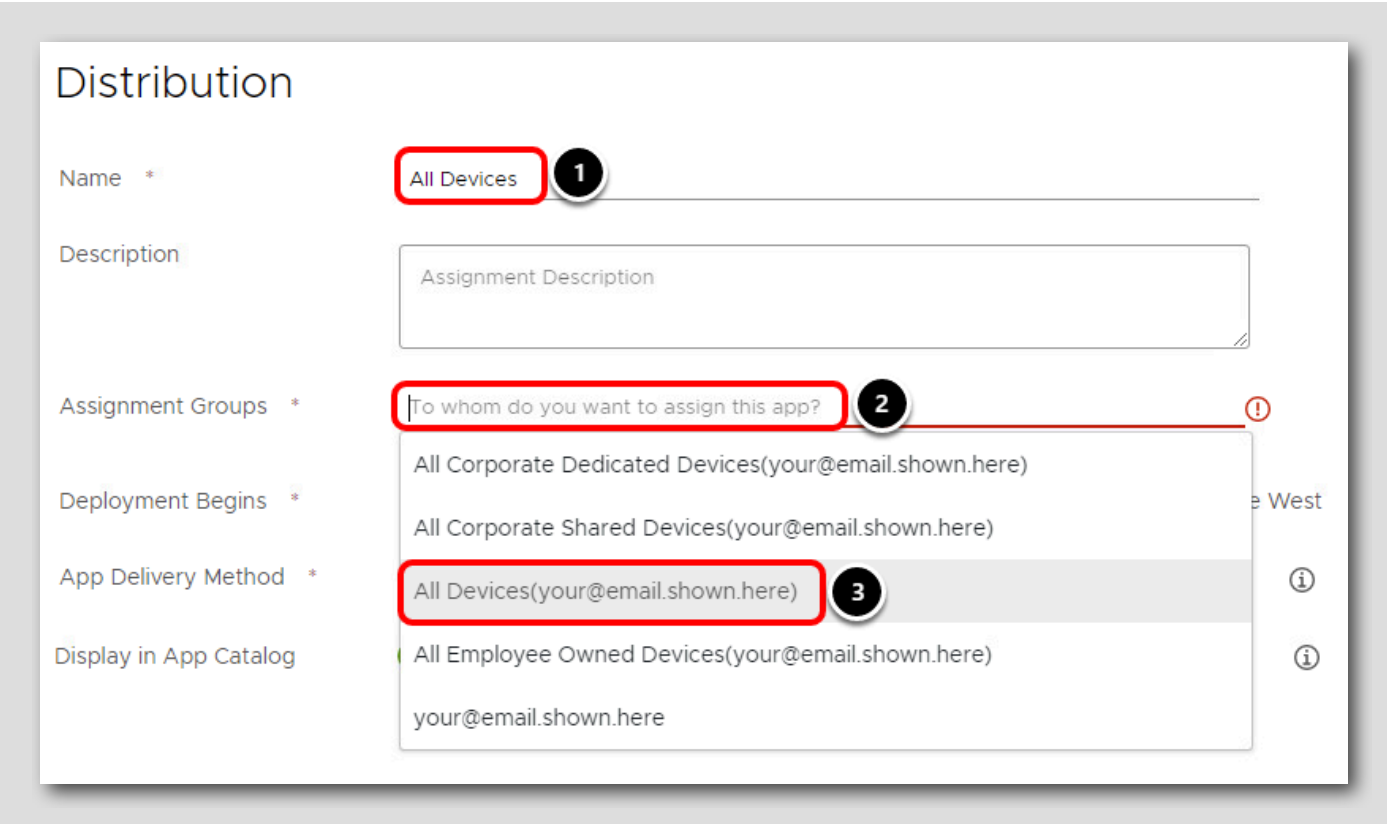
[360]



1. アップロードされたアイコンはここでプレビューできます。
2. [Save & Assign] をクリックして、アップロードされた Workspace ONE Assist アプリケーションを受信するデバイスとユーザーを構成します。

アプリケーション割り当ての構成

[361]

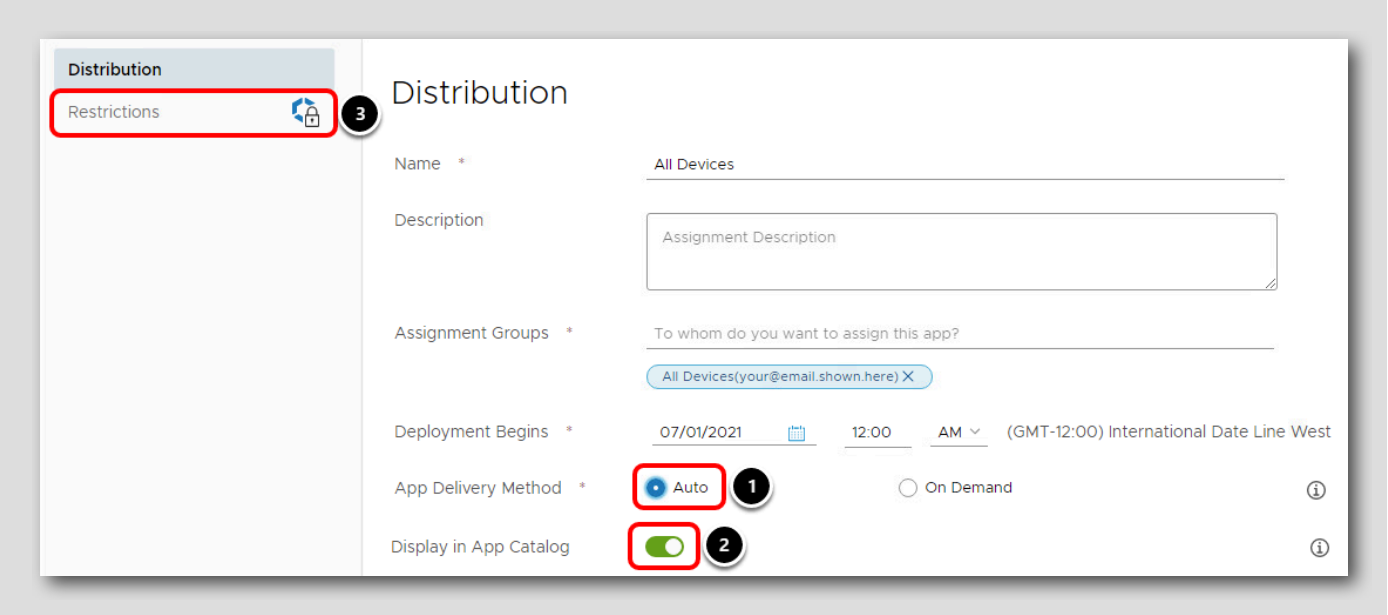


アプリケーション割り当てにより、Workspace ONE Assist を受信するユーザーとデバイス、およびアプリケーションの配信方法が決まります。組織内のすべてのデバイスにアプリケーションを自動的に公開する（ユーザー入力を必要とせずにアプリケーションをインストールする）割り当てルールを作成します。

1. 割り当てのわかりやすい名前を入力します（`All Devices` など）。
2. [Assignment Groups] セクションをクリックして、使用可能な割り当てグループのリストを表示します。
3. [All Devices (your@email.shown.here)] を選択します。これにより、組織に登録されているすべての適格なデバイスにアプリケーションが配布されます。

アプリケーション配信方法の更新

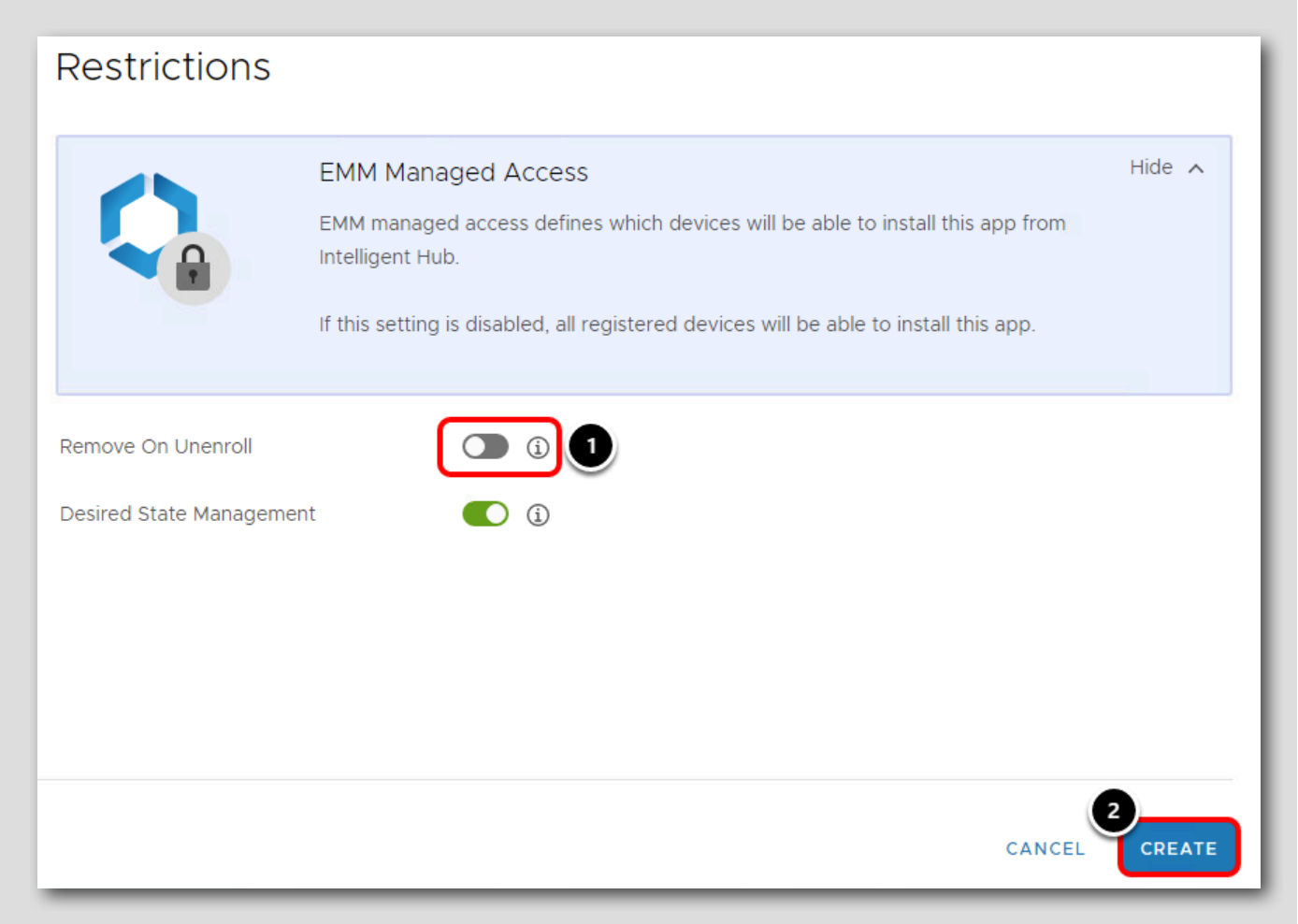
[362]



1. [App Delivery Method] で **[Auto]** を選択します。
   [Auto] は、ユーザーの操作を必要とせずに、アプリケーションができるだけ早く公開され、デバイスにインストールされることを意味します。[On Demand] では、アプリケーションはデバイスで使用できるようになりますが、インストールは開始されません。インストールは、ユーザーがアプリケーション カタログまたはセルフ サービス ポータルを介してトリガするか、管理者が Workspace ONE UEM 管理コンソールを介してトリガすることができます。
2. [Display in App Catalog] オプションは **[Enabled]** のままにします。
   これにより、Workspace ONE Assist アプリケーションがアプリケーション カタログでユーザーに表示され、必要に応じてアプリケーションをインストールまたは再インストールできます。
3. **[Restrictions]** をクリックします。

アプリケーション制限の有効化

[363]

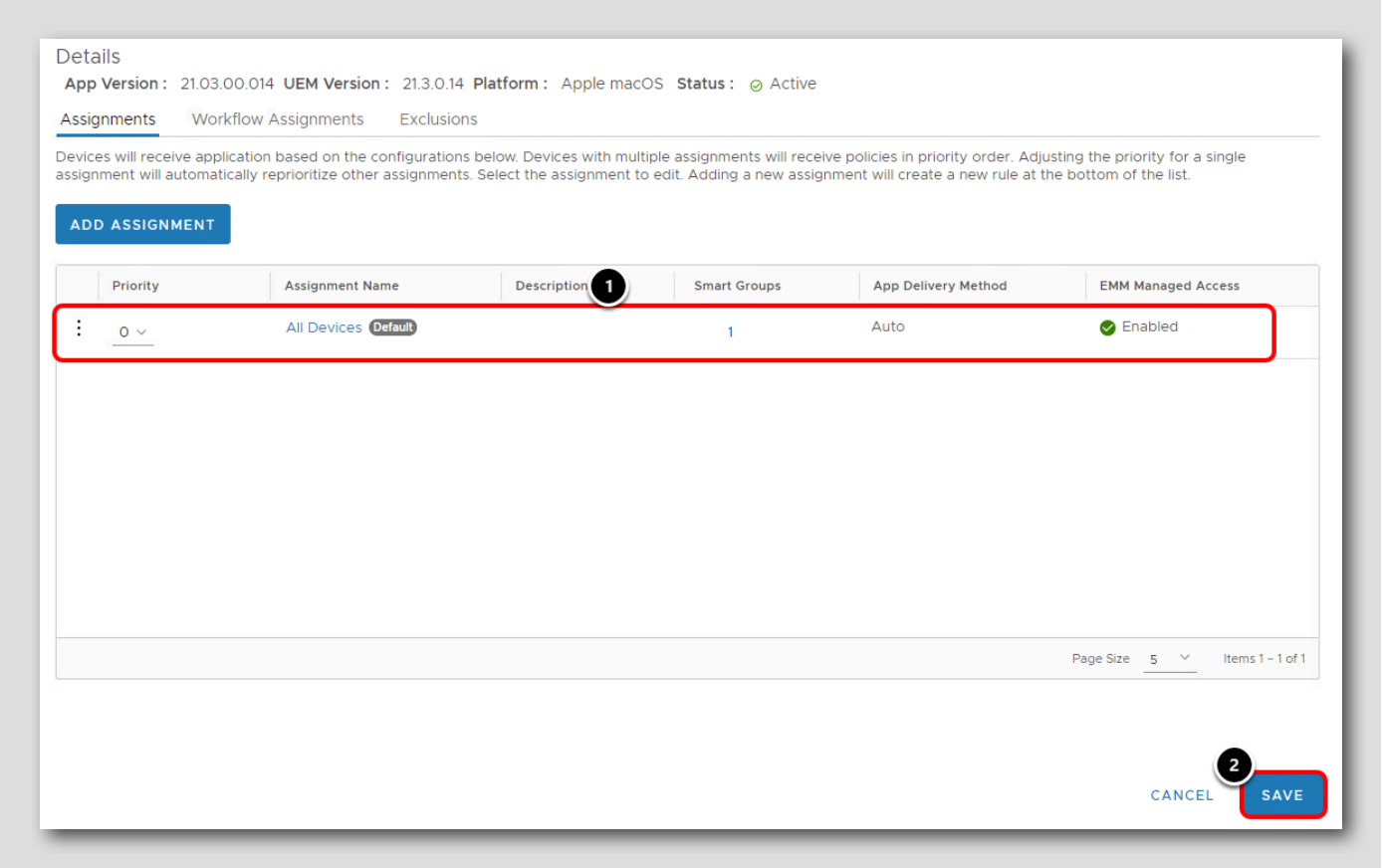


制限を割り当てに適用して、アプリケーションの動作を変更できます。

1. [Remove on Unenroll] 制限事項をクリックして、**有効**にします。これにより、デバイスが登録解除される（つまり、Workspace ONE UEM によって管理されなくなります）と、Workspace ONE Assist アプリケーションはユーザーのデバイスから自動的に削除されます。
2. **[Create]** をクリックします。

アプリケーション割り当ての保存

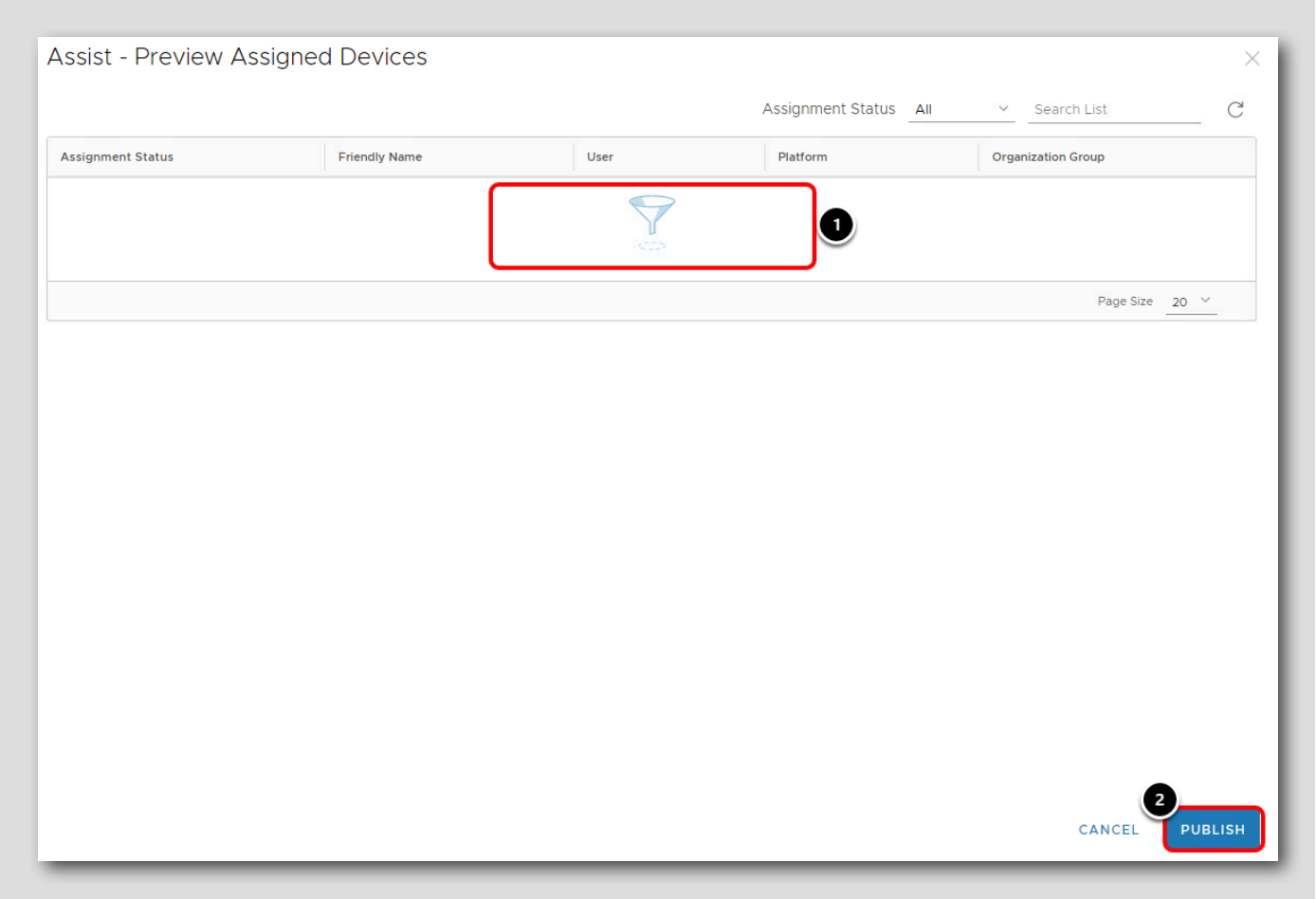
[364]



1. このビューから割り当てを確認および編集できます。複数の割り当てを優先順位で並べ、複数の割り当てタイプが重複するデバイスに適用する割り当てを決定できます。このシンプルなユースケースでは、単一の割り当てを活用して、組織内のすべての macOS デバイスに適用します。
2. [Save] をクリックします。

アプリケーションの公開

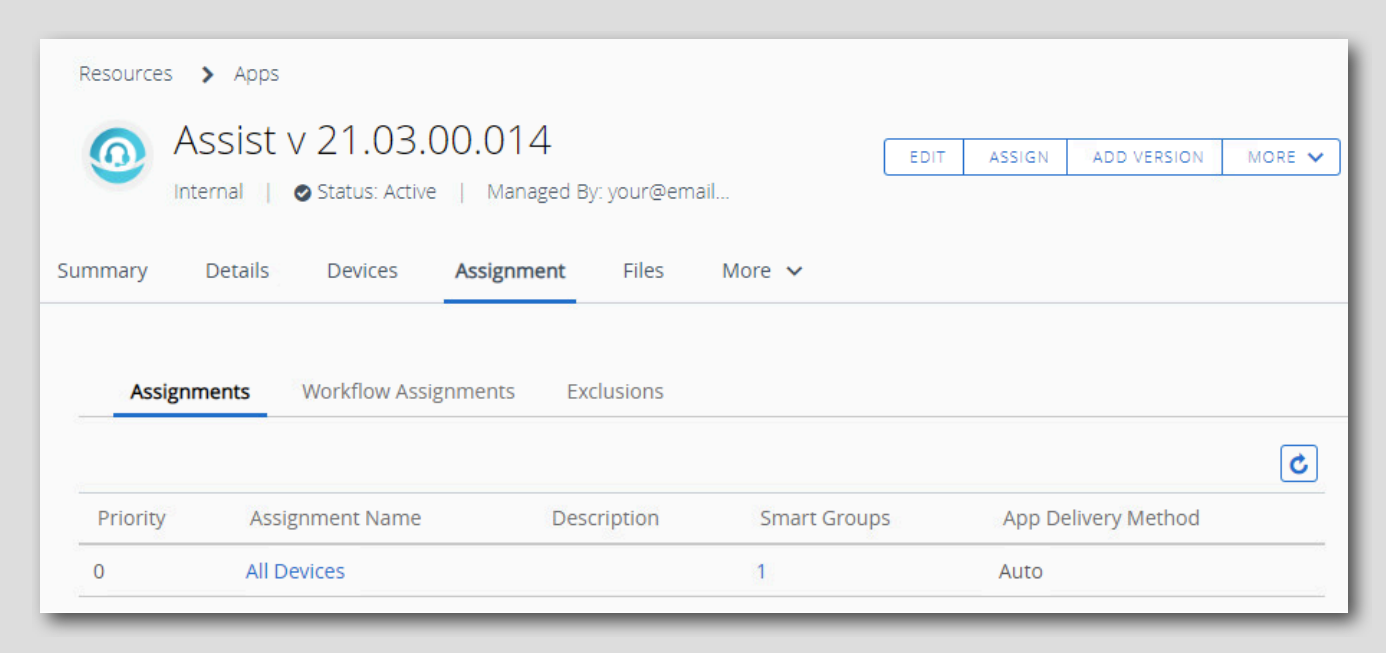
[365]



1. このアプリケーションを受信するデバイスのリストがここに表示されます。macOS デバイスはまだ登録していないため、リストは空です。
2. [Publish] をクリックします。

アプリケーションが公開されたことの確認

[366]



Workspace ONE Assist アプリケーションが公開されました。組織に登録されている macOS デバイスには、Workspace ONE Assist アプリケーションが自動的に割り当てられ、ユーザーの操作なしでインストールされます。デバイスの登録が解除されると、アプリケーションはデバイスから自動的に削除されます。

今後必要に応じてこのビュー（[Resources] > [Native] > [Internal]）に戻り、Workspace ONE Assist アプリケーションをクリックして、割り当ての更新、新しいアプリケーション バージョンの追加など、変更を加えることができます。

次の手順に進んでください。

登録後のオンボーディング エクスペリエンスの構成

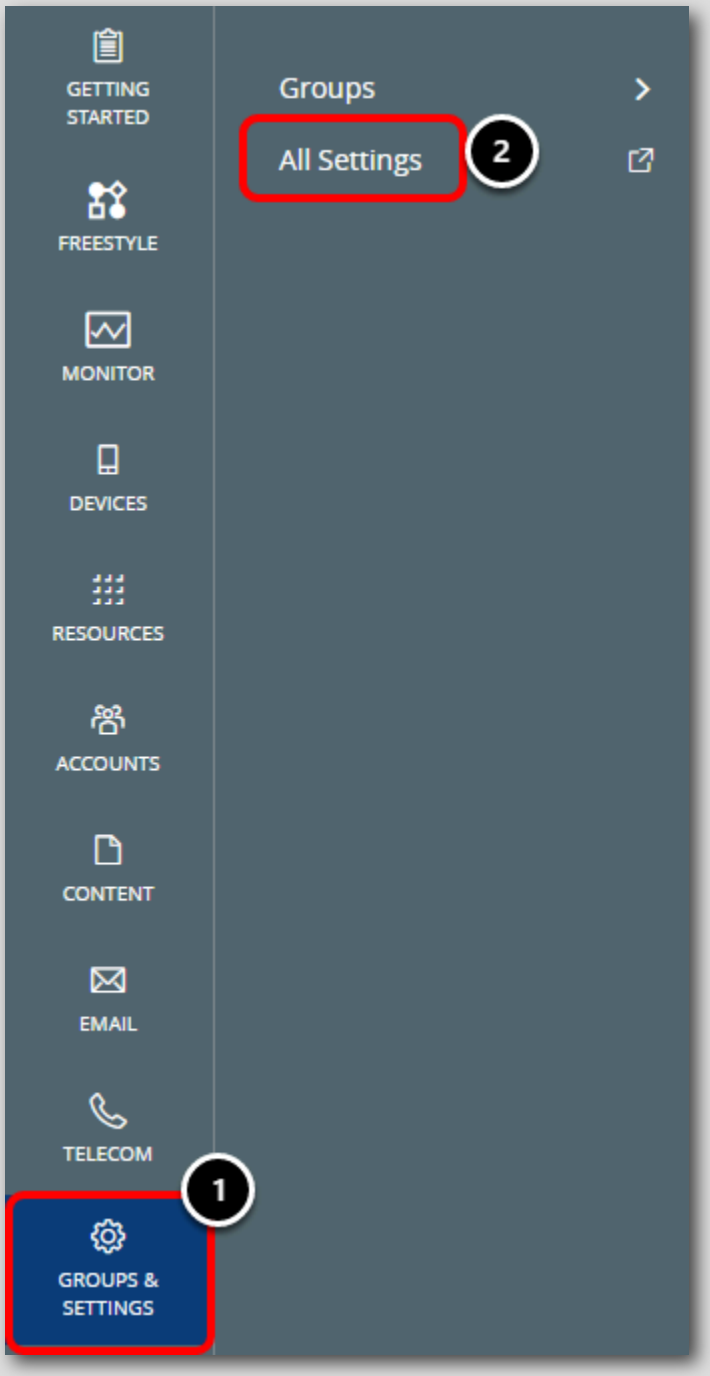
[367]

管理者は、Workspace ONE UEM Intelligent Hub で登録後のオンボーディング エクスペリエンスを有効にすることで、登録が完了した後もデバイスのプロビジョニング プロセスについてユーザーに通知できるようになりました。登録が完了すると、Intelligent Hub には、受信するすべてのアプリケーションのインストールを追跡する新しいウィンドウが表示されます。管理者は、Workspace ONE UEM 管理者コンソールでエクスペリエンスを有効にしてカスタマイズできます。

この機能を使用するには、Workspace ONE UEM 21.05 以降および Workspace ONE Intelligent Hub 21.04 以降が必要です。

登録後のオンボーディング エクスペリエンスの有効化

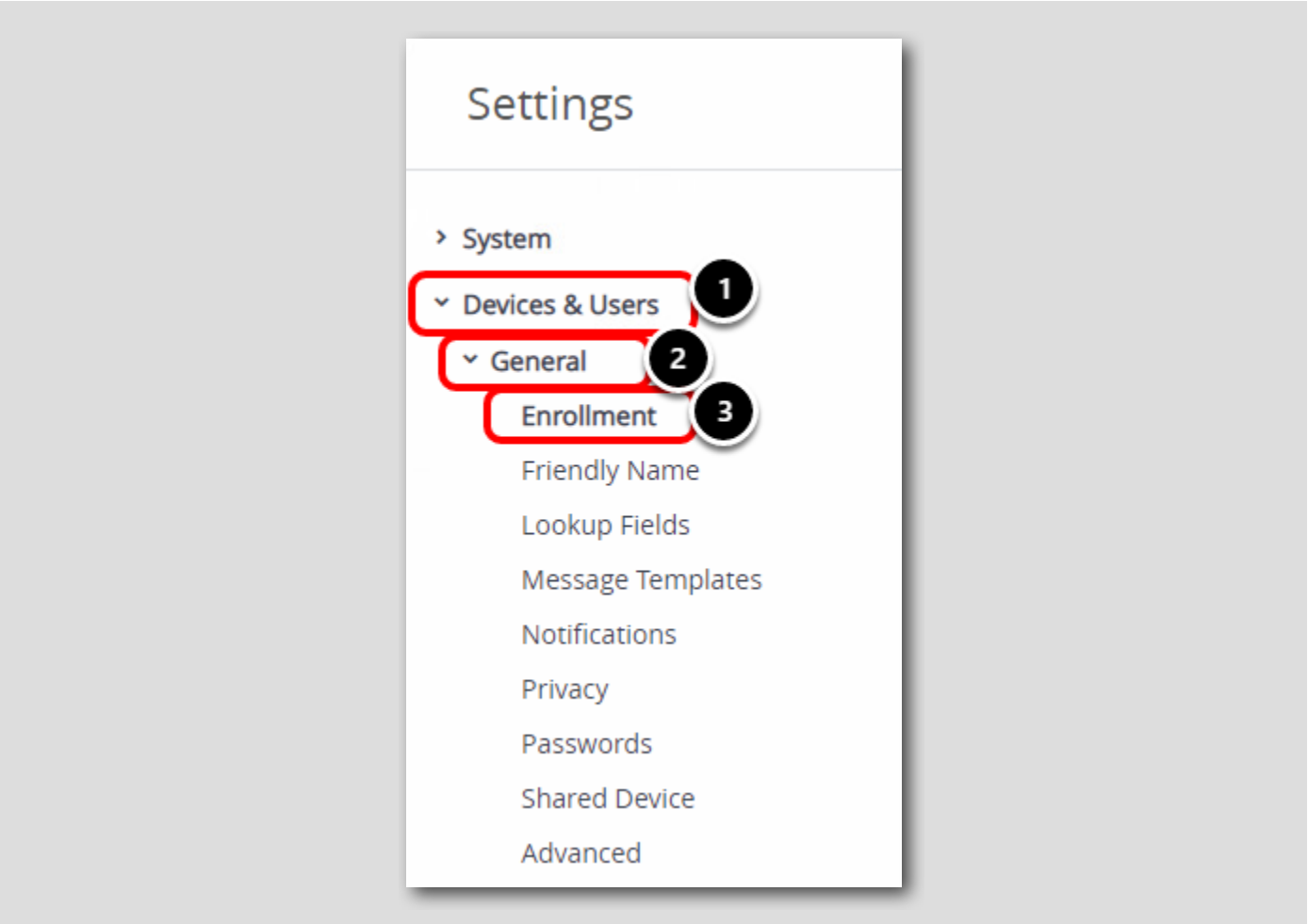
[368]



1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

[Enrollment Settings] への移動

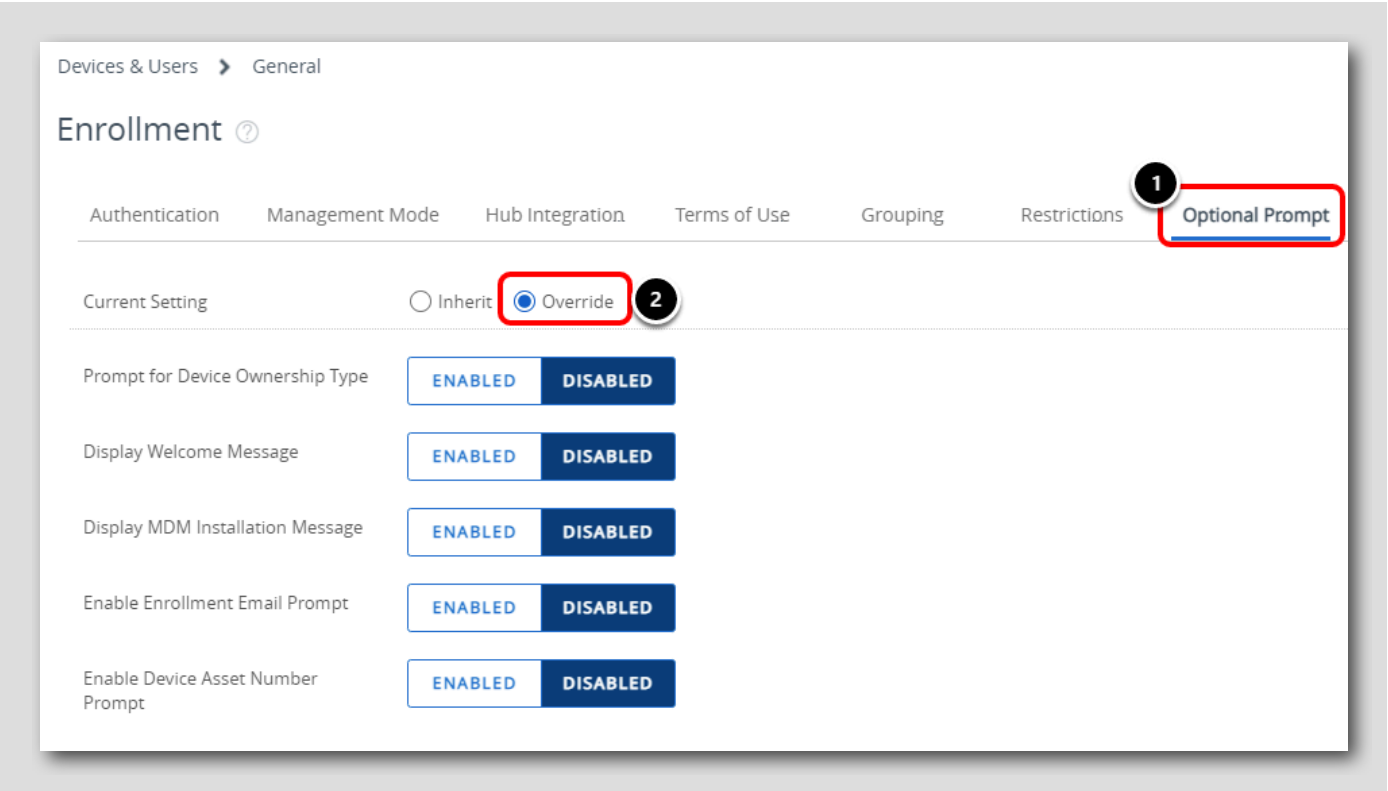
[369]



1. [Devices & Users] を展開します。
2. [General] を展開します。
3. [Enrollment] をクリックします。

[Optional Prompt] の構成

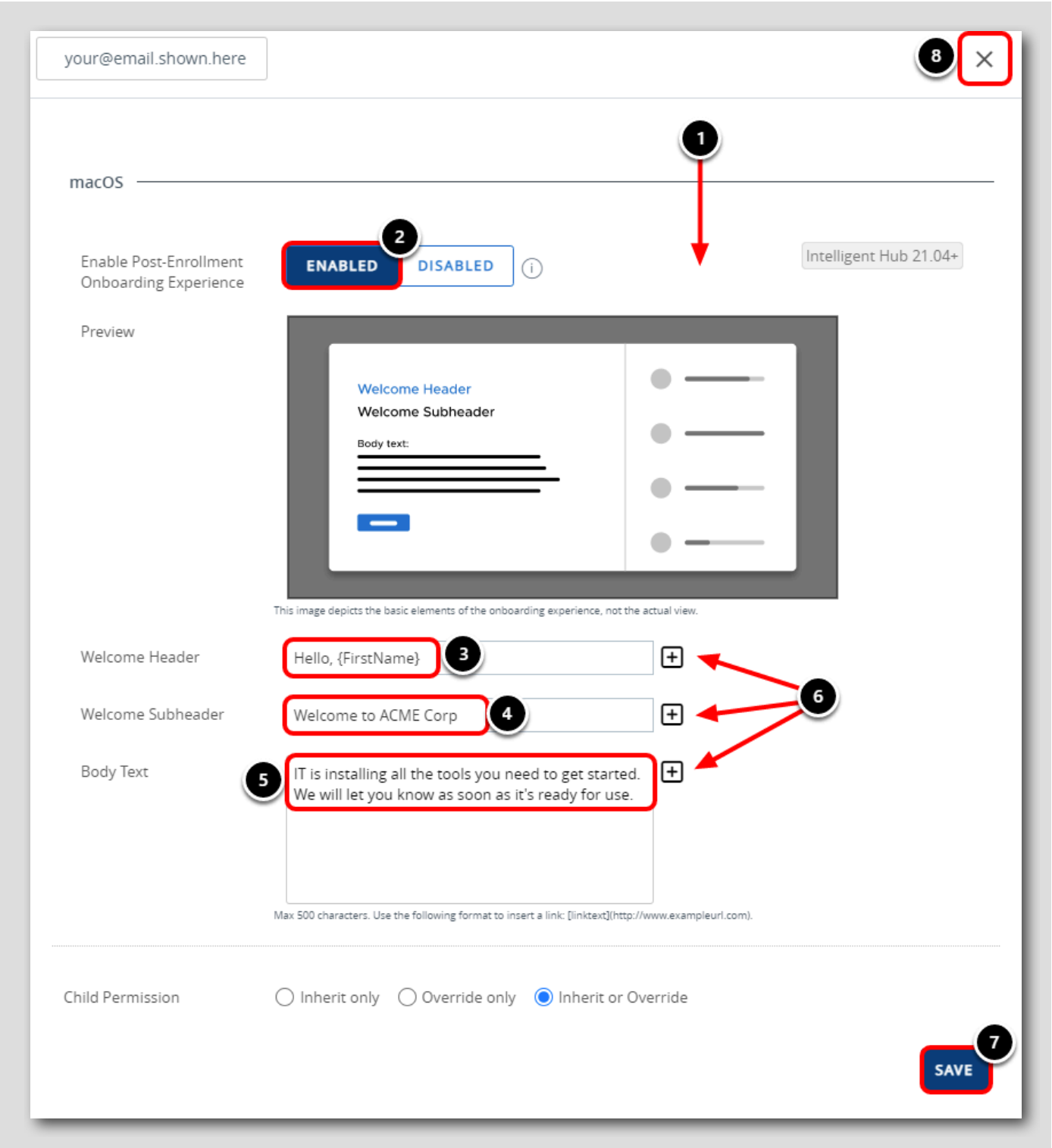
[370]



1. **[Optional Prompt]** タブをクリックします。
2. [Current Setting] で **[Override]** を選択して変更します。

登録後のオンボーディング エクスペリエンスの構成

[371]


your@email.shown.here
8
1
macOS
2
Enable Post-Enrollment Onboarding Experience
ENABLED
DISABLED
Intelligent Hub 21.04+
Preview
Welcome Header
Welcome Subheader
Body text:
This image depicts the basic elements of the onboarding experience, not the actual view.
Welcome Header
Hello, {FirstName}
3
Welcome Subheader
Welcome to ACME Corp
4
6
Body Text
5
IT is installing all the tools you need to get started.
We will let you know as soon as it's ready for use.
Max 500 characters. Use the following format to insert a link: [linktext](http://www.exampleurl.com).
Child Permission
Inherit only
Override only
Inherit or Override
7
SAVE

1. 一番下までスクロールして、macOS の設定を見つけます。
2. [Enable Post-Enrollment Onboarding Experience] オプションで [Enabled] を選択し、下へスクロールします。
3. 初期画面のヘッダーはデフォルトの **`Hello`**、**`{FirstName}`** のままにします。このヘッダーは、ユーザーの名前で挨拶をするものです。
4. 初期画面のサブヘッダーを **`Welcome to ACME Corp`** に更新します。
5. デフォルトの本文テキストを使用するか、独自の本文を入力します。文字数には 500 文字の制限があることに注意してください。
6. フィールドを構成するときに、プラス (+) ボタンを使用して、このフィールドでサポートされている参照値を表示できます。

   `{FirstName}` などの参照値は、ランタイム時に値を取得し、現在の値に置き換え、動的変数の取得を容易にします。
7. [Save] をクリックします。
8. [Close] をクリックします。

これで、登録後のオンボーディング エクスペリエンスが有効になり、構成されました。これにより、ユーザーはダウンロードおよびインストールしているアプリケーションの進行状況を簡単に追跡できるため、ユーザーのオンボーディング エクスペリエンスが向上します。

macOS の Workspace ONE Intelligent Hub のインストール

[372]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

この演習では、Workspace ONE Intelligent Hub をダウンロードして macOS デバイスにインストールします。

macOS デバイスへのログイン

[373]

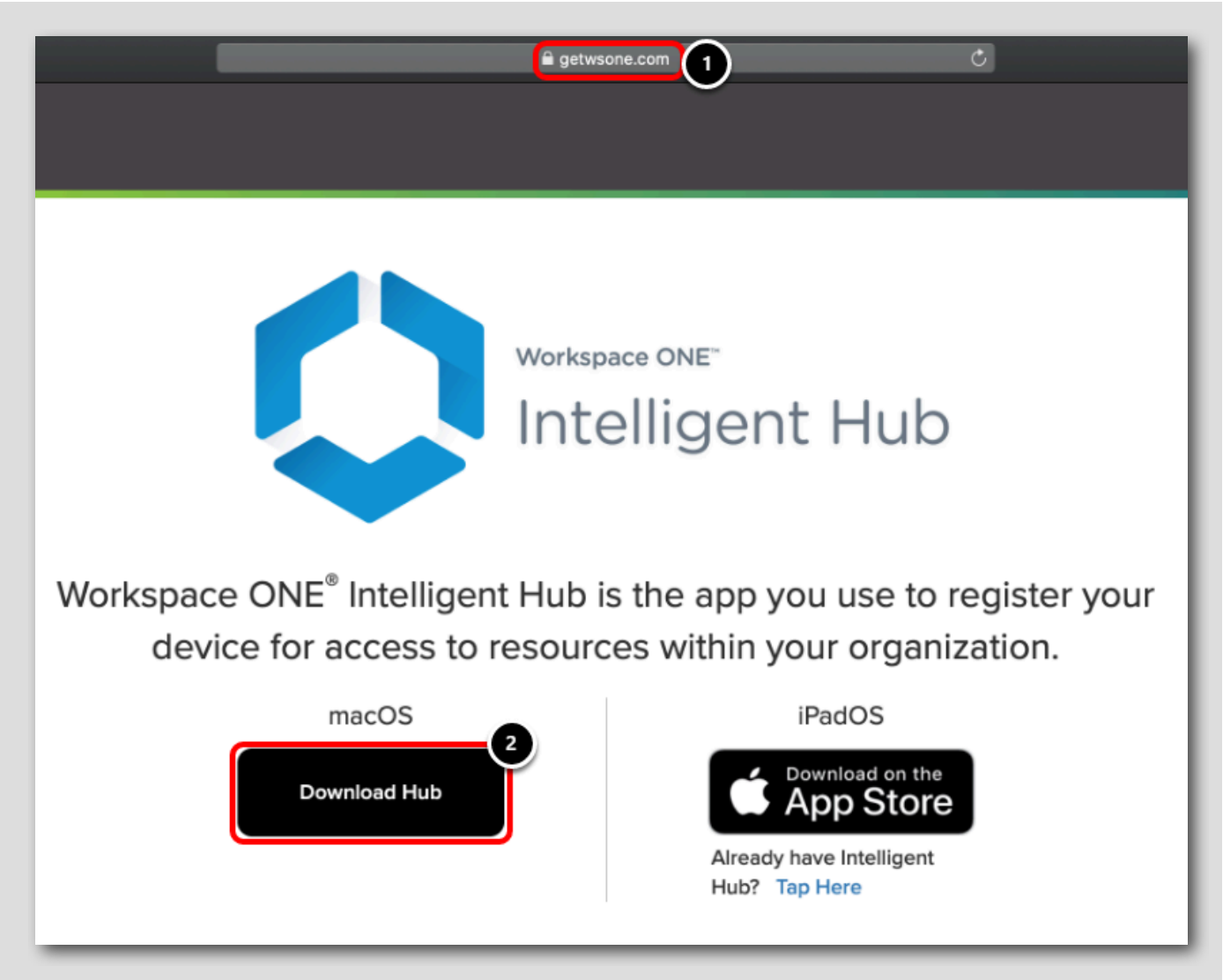
注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

macOS デバイスに管理者アカウントでログインします。

Workspace ONE Intelligent Hub のダウンロード

[374]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。



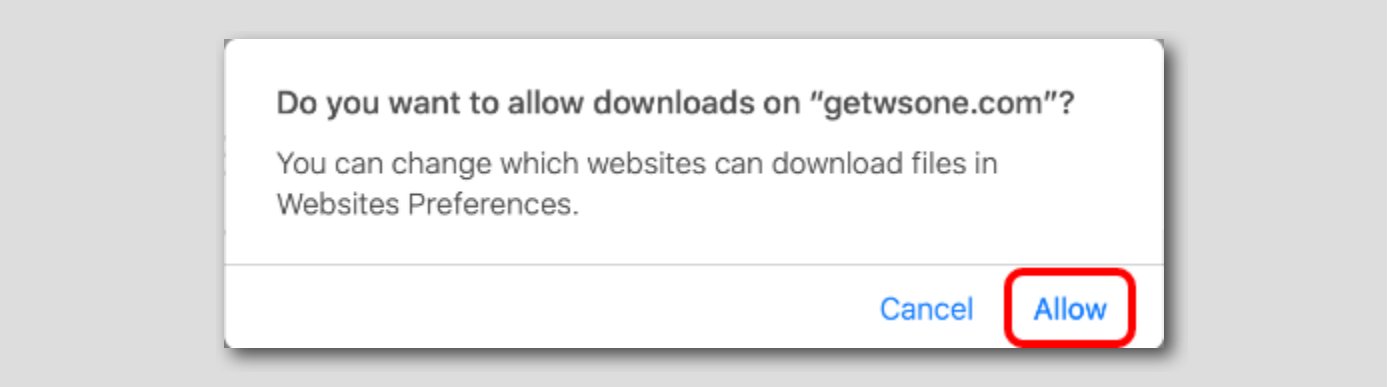
Safari またはお好みの Web ブラウザを開きます。

1. URL フィールドに `https://www.getwsone.com` と入力し、`ENTER` キーを押します。
2. [macOS] セクションの下の [Download Hub] をクリックします。Workspace ONE Intelligent Hub インストーラのダウンロードが開始され、デフォルトでダウンロード フォルダに保存されます。

ダウンロードを許可（必要な場合）

[375]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

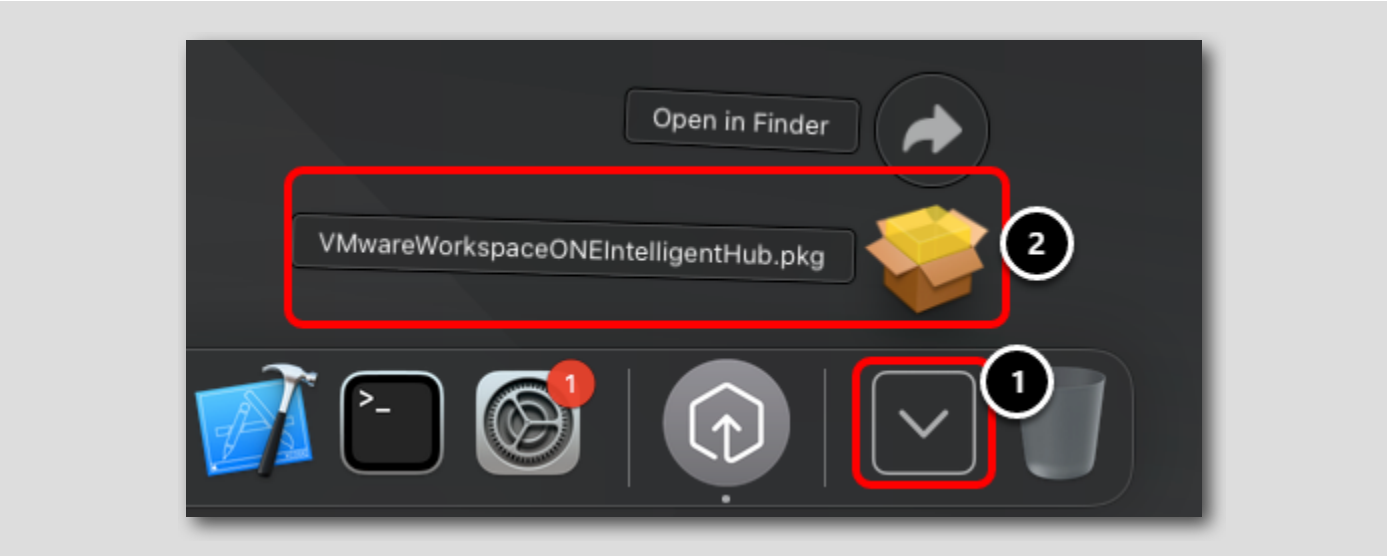


getwsone.com からのダウンロードを許可するように求められた場合は、[Allow] をクリックします。それ以外の場合は、次の手順に進みます。

Workspace ONE Intelligent Hub のインストール

[376]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

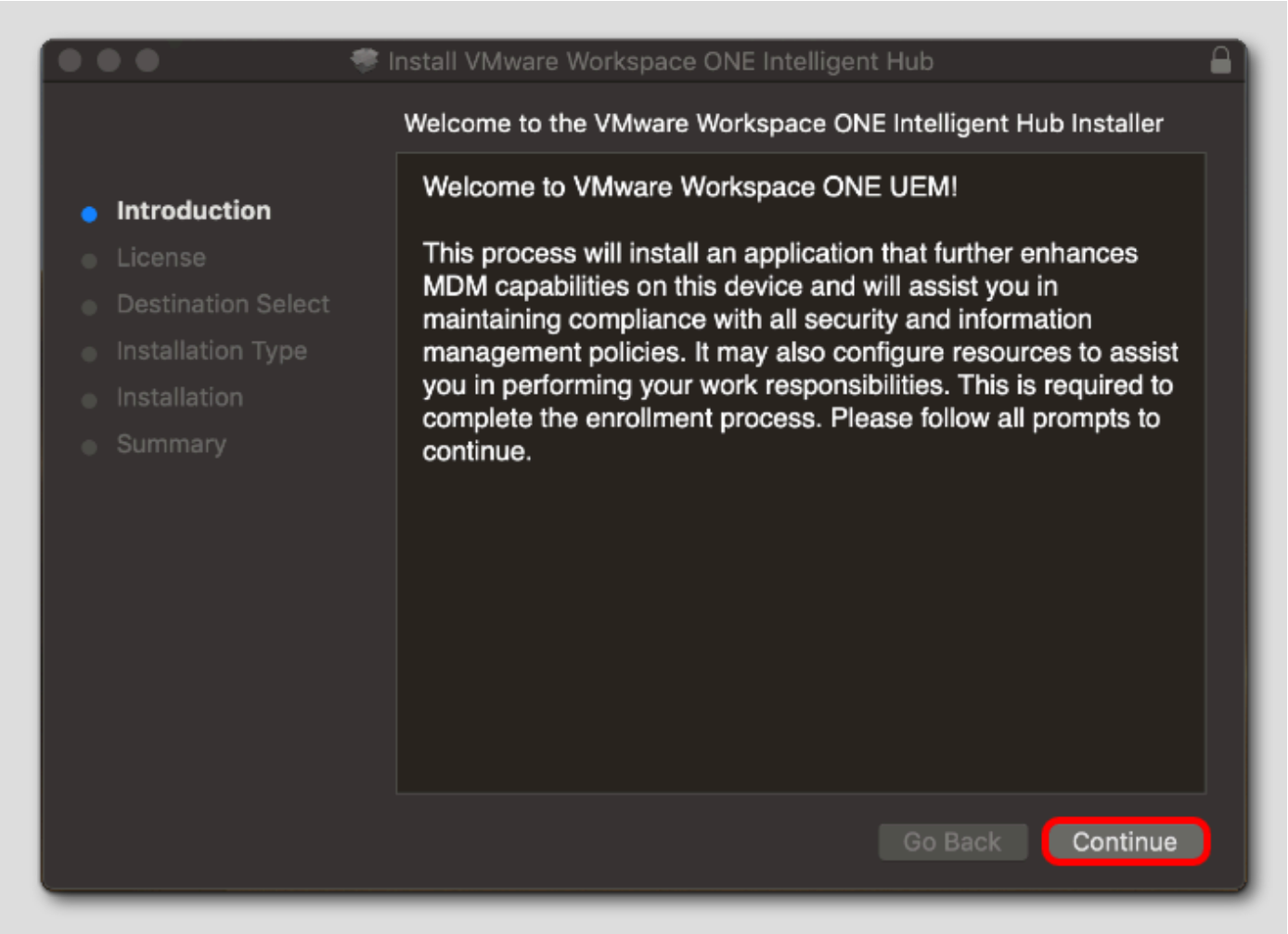


1. Dock 内の [Downloads] フォルダ（ゴミ箱の横）をクリックします。
2. VMwareWorkspaceONEIntelligentHub.pkg ファイルをクリックして、インストーラを起動します。

[Introduction] 画面で続行

[377]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

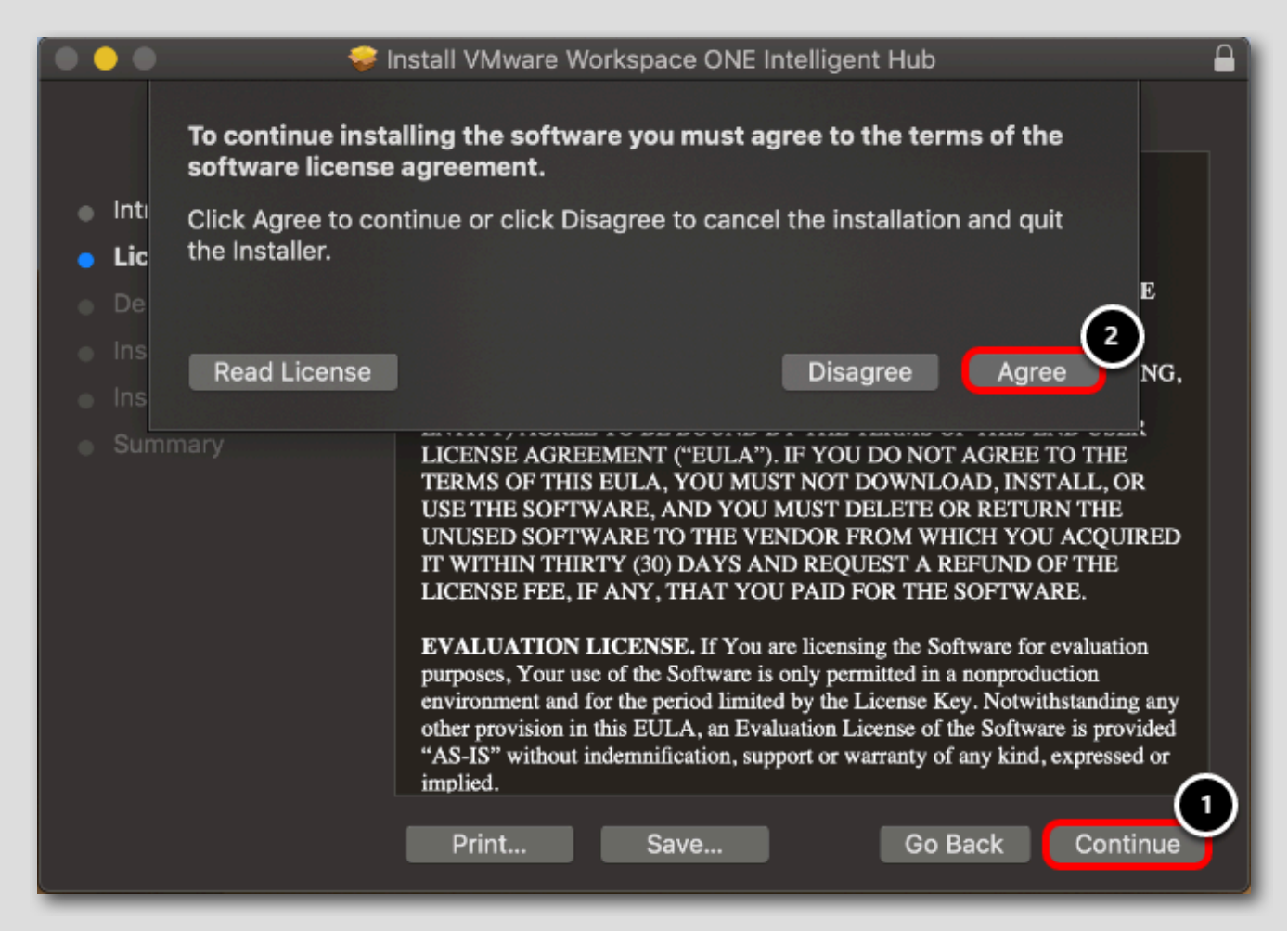


[Continue] をクリックします。

続行して利用規約に同意

[378]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。

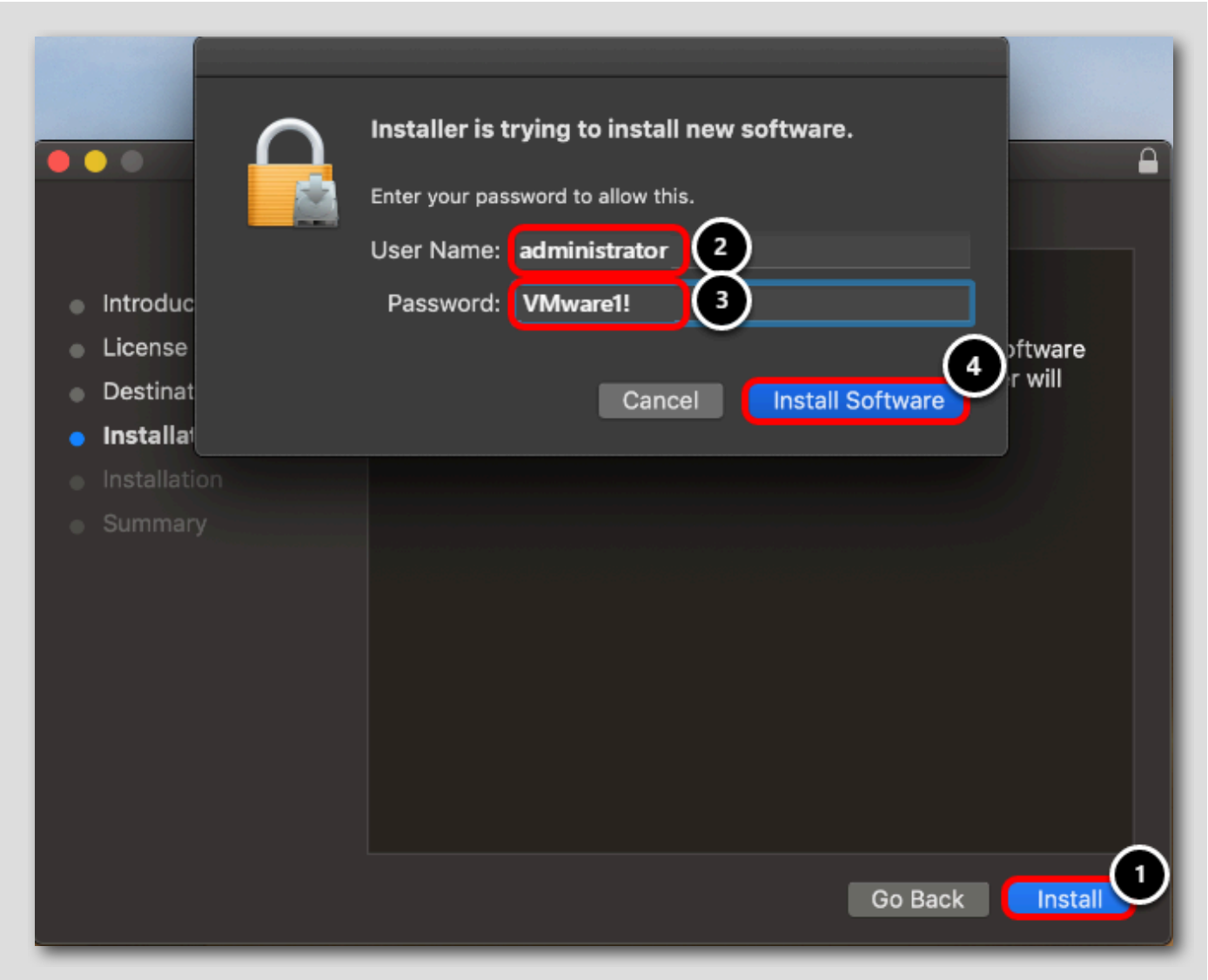


1. [License] ページで、[Continue] をクリックします。
2. [Agree] をクリックして、使用許諾契約書に同意します。

インストールの開始

[379]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。



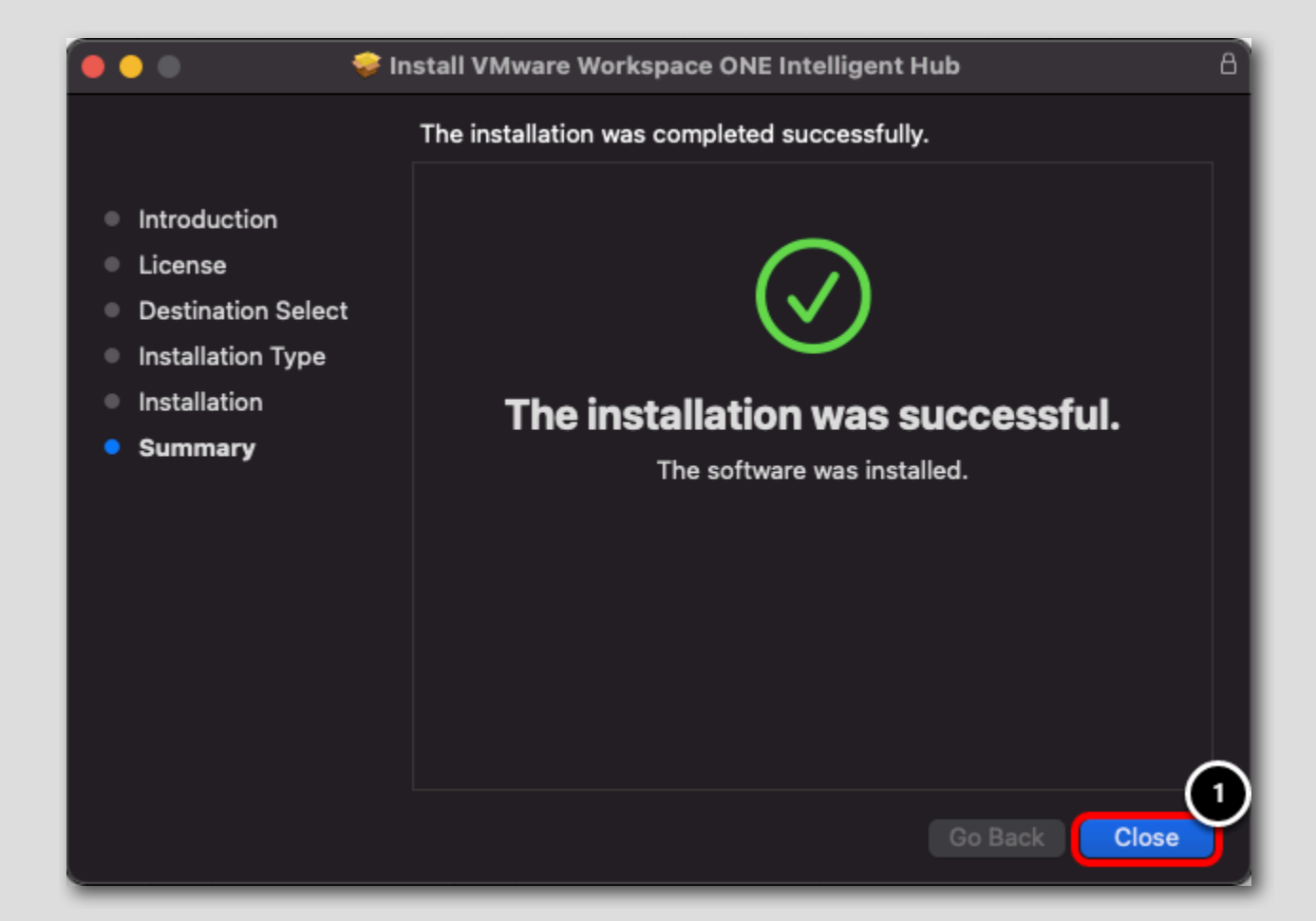
1. [Install] をクリックします。コンピュータ管理者の認証情報の入力を求められます。
2. デバイスのユーザー名を入力します。
3. デバイスのパスワードを入力します。
4. [Install Software] ボタンをクリックします。

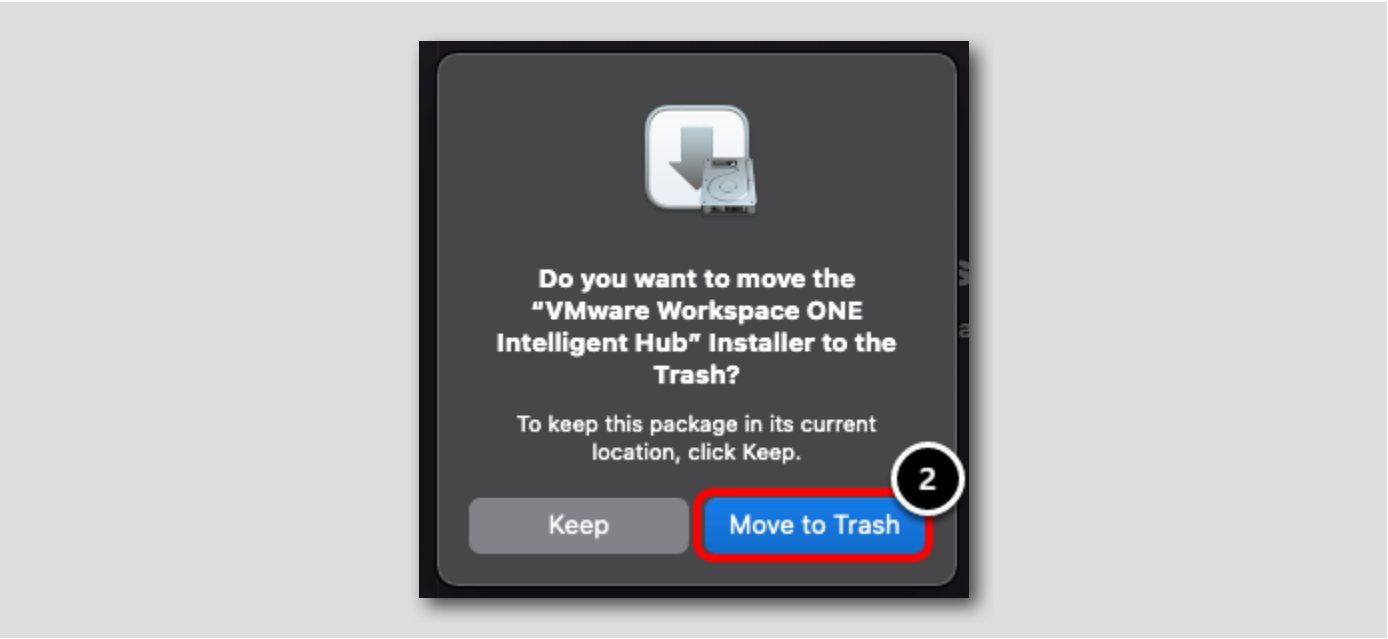
注: インストールには数分かかる場合があります。インストールが完了するまでしばらくお待ちください。

ファイルを閉じてゴミ箱に移動

[380]

注: これらの手順には macOS デバイスが必要です。macOS デバイスがない場合は、マニュアルの手順に従って、最終的な結果を確認できます。





1. インストールが終了したら [Close] をクリックします。
2. [Move to Trash] をクリックして、インストーラをゴミ箱に移動します。

macOS デバイスの登録

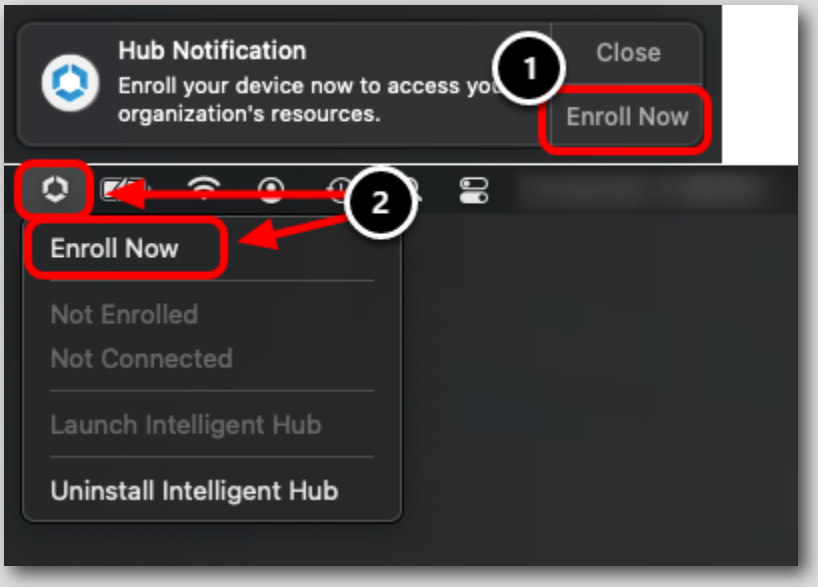
[381]

この実習では、macOS デバイスを Workspace ONE UEM に登録します。登録とは、デバイスを Workspace ONE UEM によって管理および制御される状態にする操作のことです。さまざまなプラットフォーム（macOS を含む）を登録するにはいくつかの方法がありますが、この実習では、基本的な登録シナリオについて説明します。

この登録フローは、macOS High Sierra で導入された機能に従って*ユーザー承認済み*と見なされます。

macOS 登録プロセスの開始

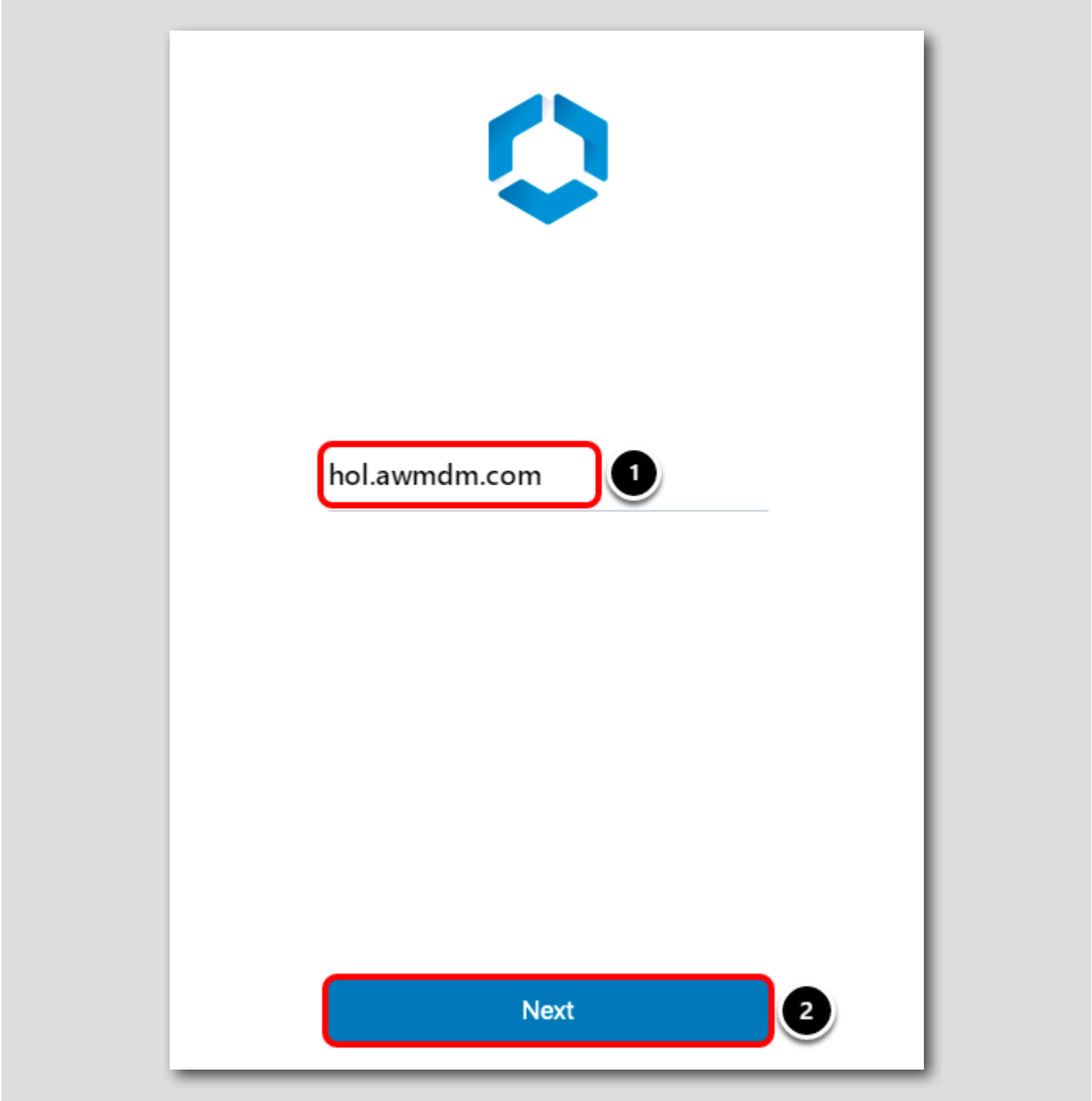
[382]



1. Hub 通知が表示されたら、[Enroll Now] をクリックして登録プロセスを開始します。
2. または、上部のバーで Hub アイコンをクリックし、[Enroll Now] をクリックして登録プロセスを開始することもできます。

登録サーバ URL の入力

[383]

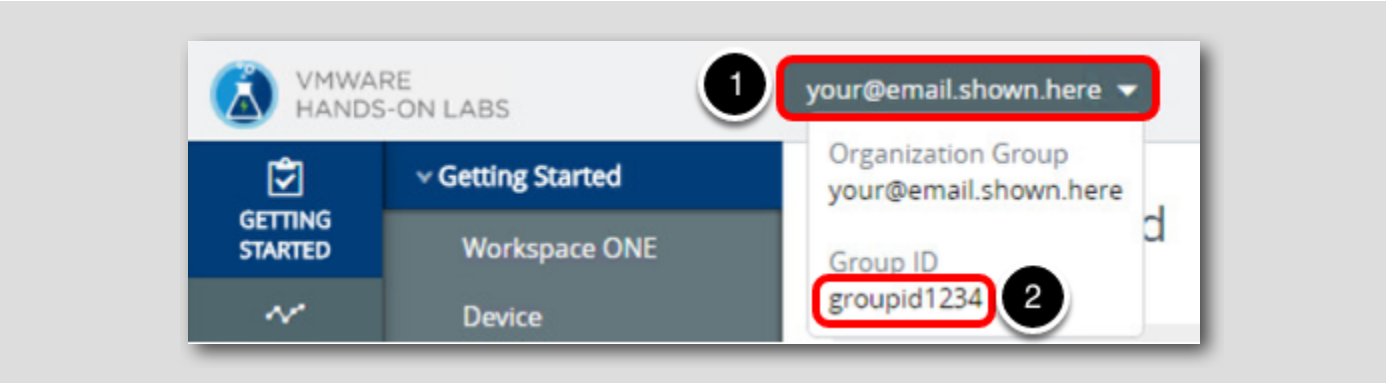


1. [Email or Server Address] フィールドに **`hol.awmdm.com`** と入力します。
2. [Next] をクリックします。

注：登録ウィザードは、ハードウェアまたは仮想マシンの機能に基づいて、起動に少し時間がかかる場合があります。登録ウィザードがすぐに表示されない場合は、表示されるまでしばらくお待ちください。

Workspace ONE UEM Console でのグループ ID の検索

[384]



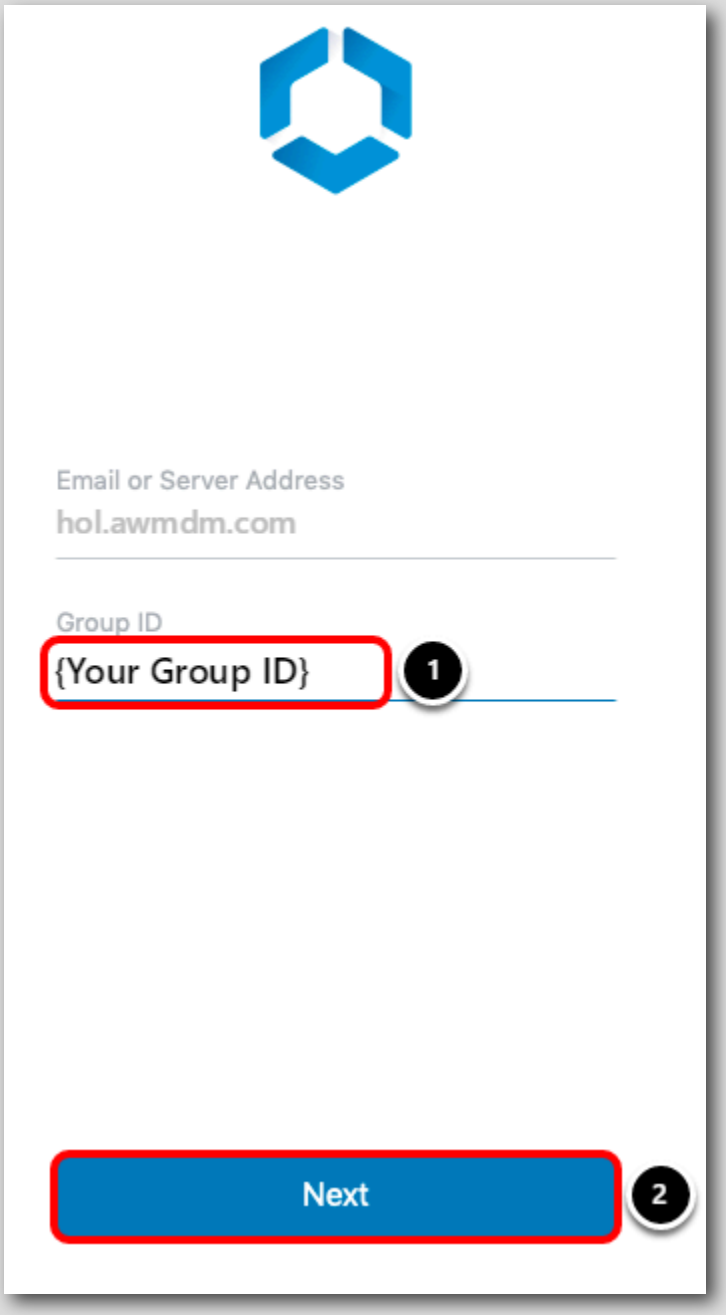
Workspace ONE UEM Console に戻ります。

1. グループ ID を確認するには、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. グループ ID は [Organization Group] ポップアップの最下部に表示されます。

注：このグループ ID は、以降の手順でデバイスを登録するときに必要です。

登録サーバの詳細情報の入力

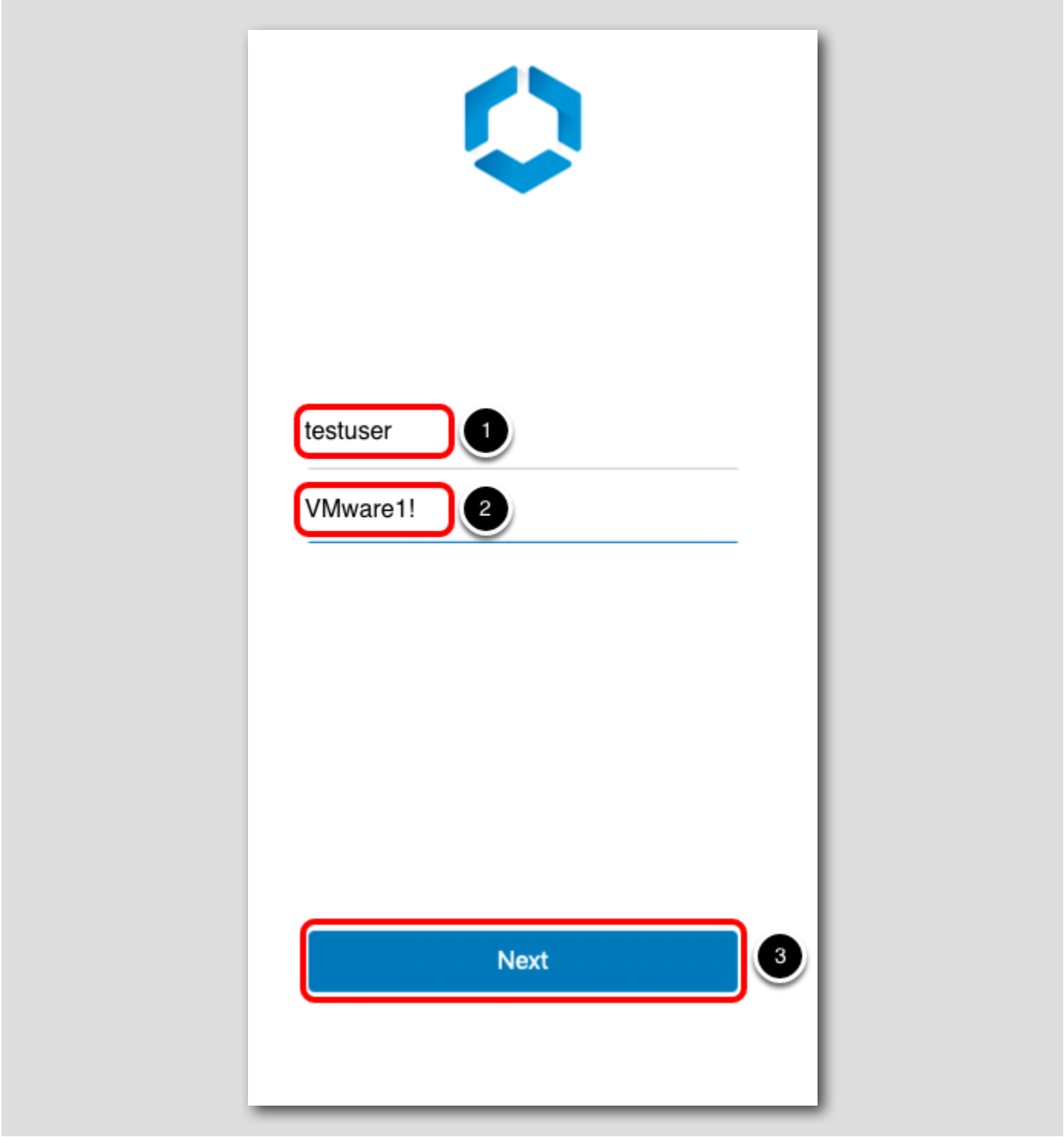
[385]



1. [Group ID] を入力します。これは、前の「グループ ID の取得」の手順で説明されています。
2. [Next] をクリックします。

登録の認証情報の入力

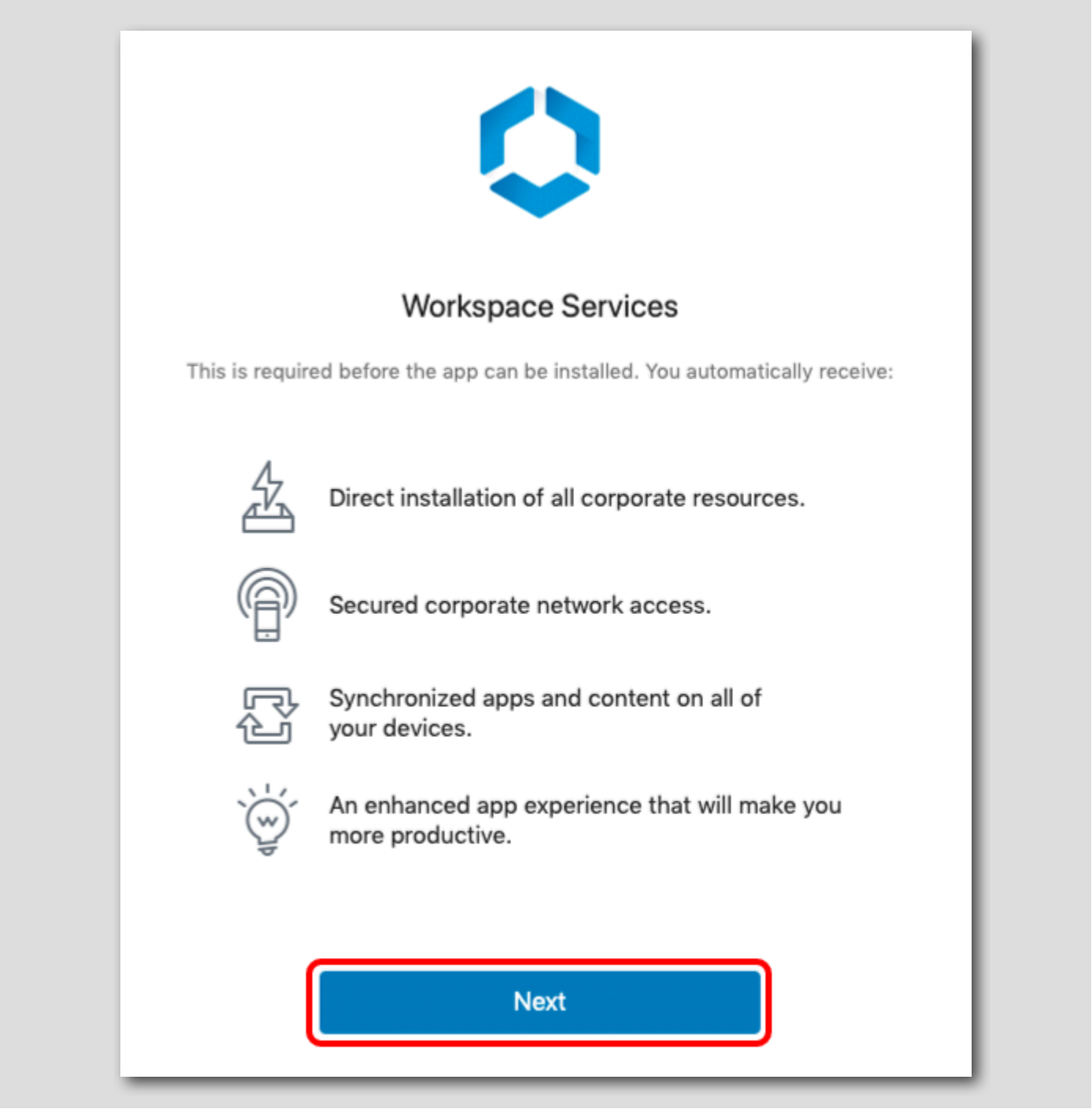
[386]



1. 登録ユーザー名に **`testuser`** と入力します。
2. パスワードに **`VMware1!`** と入力します。
3. [Next] をクリックします。

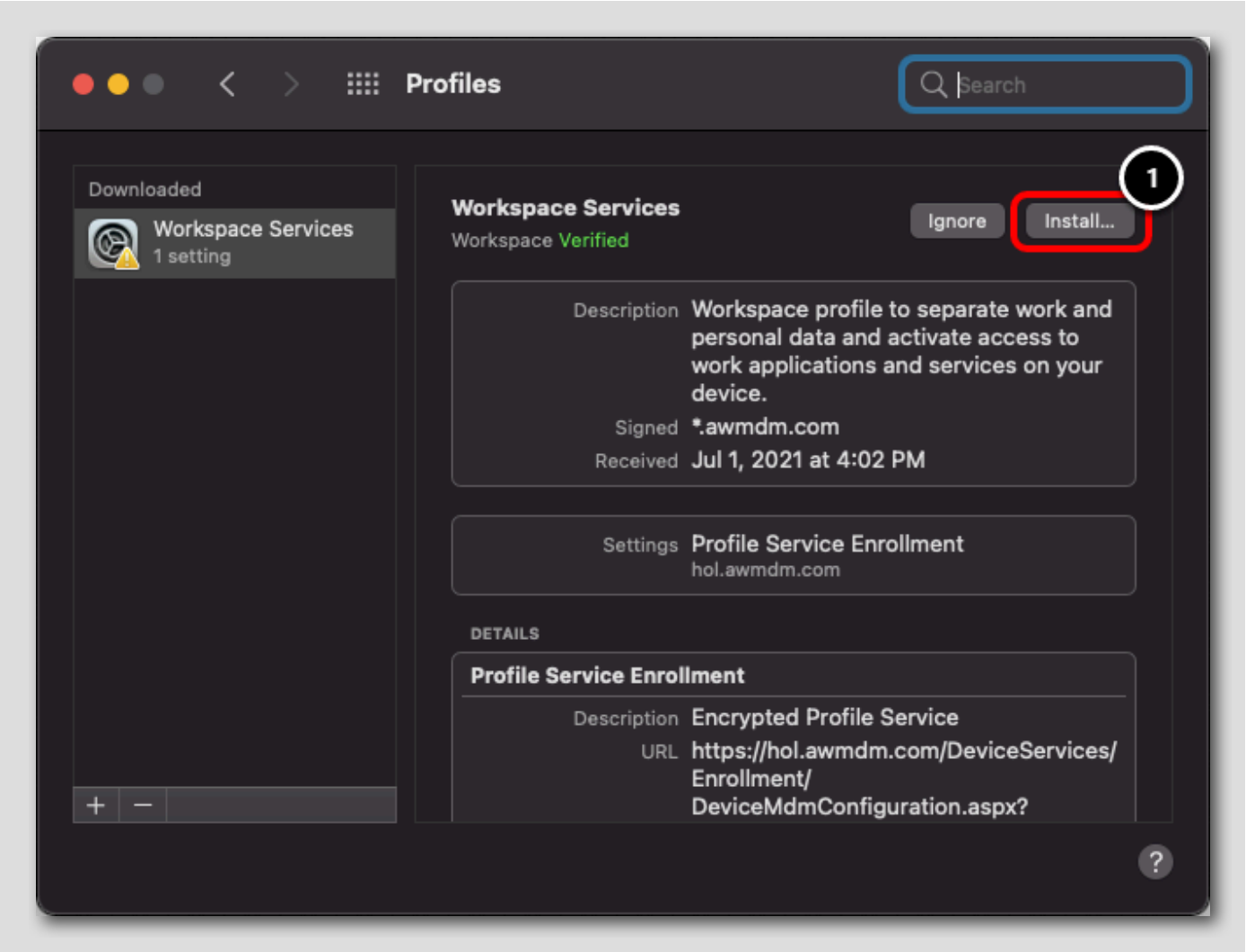
デバイス管理の有効化

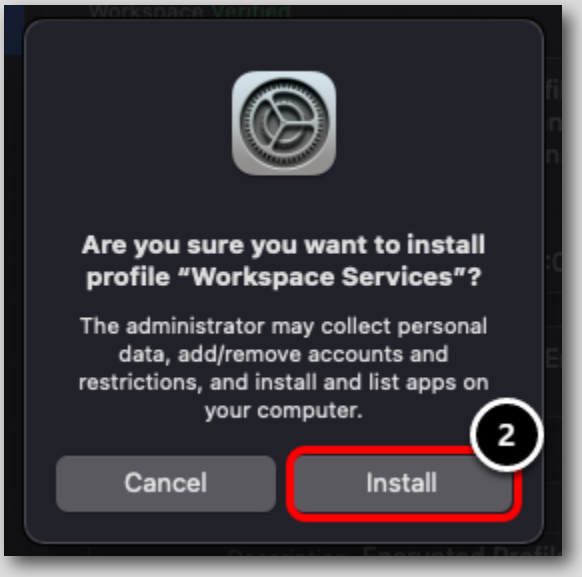
[387]

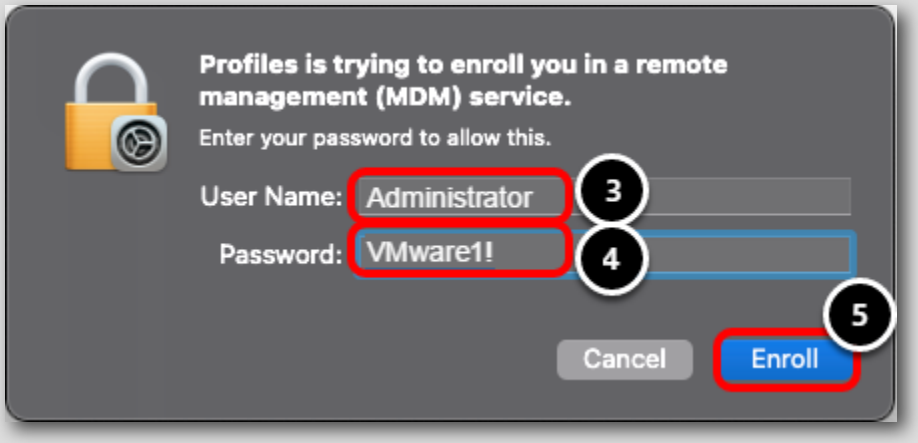


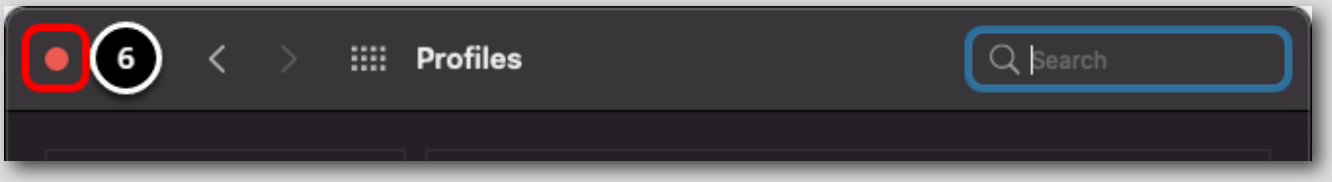
[Next] をクリックして、デバイス管理を有効にします。

Workspace Services プロファイルのインストール [388]




Are you sure you want to install profile "Workspace Services"?
The administrator may collect personal data, add/remove accounts and restrictions, and install and list apps on your computer.
2
Cancel
Install


Profiles is trying to enroll you in a remote management (MDM) service.
Enter your password to allow this.
User Name:
Administrator
3
Password:
VMware1!
4
5
Cancel
Enroll

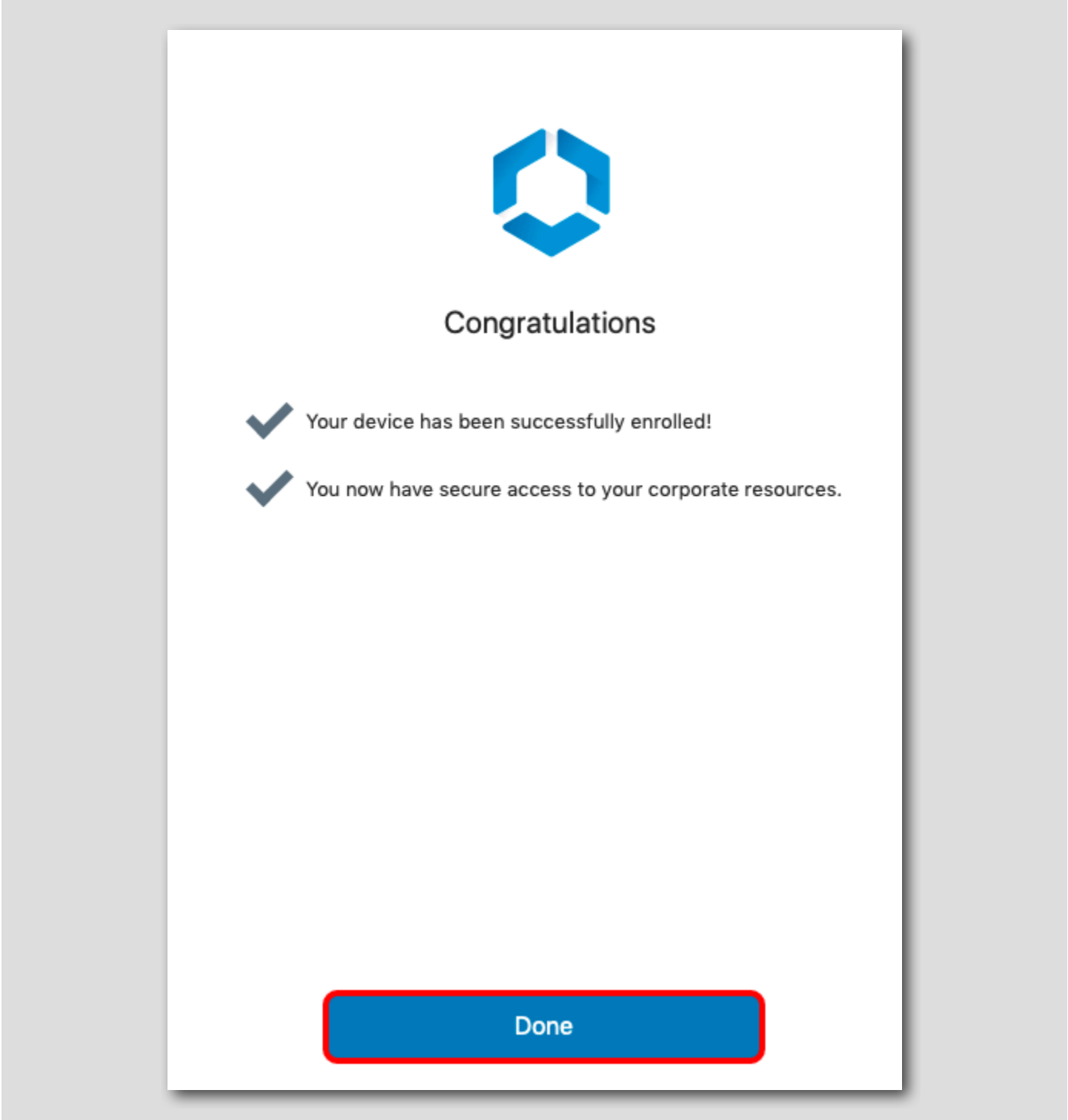

6
Profiles
Search

数秒後、[Profiles System Preferences] ページが表示され、Workspace Services プロファイルをインストールするように求められます。これにより、Workspace ONE UEM を使用してデバイスをモバイル デバイス管理 (MDM) に登録します。

1. Workspace Services プロファイルの [Install] をクリックします。
2. プロンプトが表示されたら、[Install] をクリックします。
3. デバイス ユーザーの**ユーザー名**を入力します。
4. デバイス ユーザーの**パスワード**を入力します。
5. [Enroll] をクリックします。
6. [System Preferences] ウィンドウで [Close] をクリックして閉じます。

デバイス登録後の操作の続行

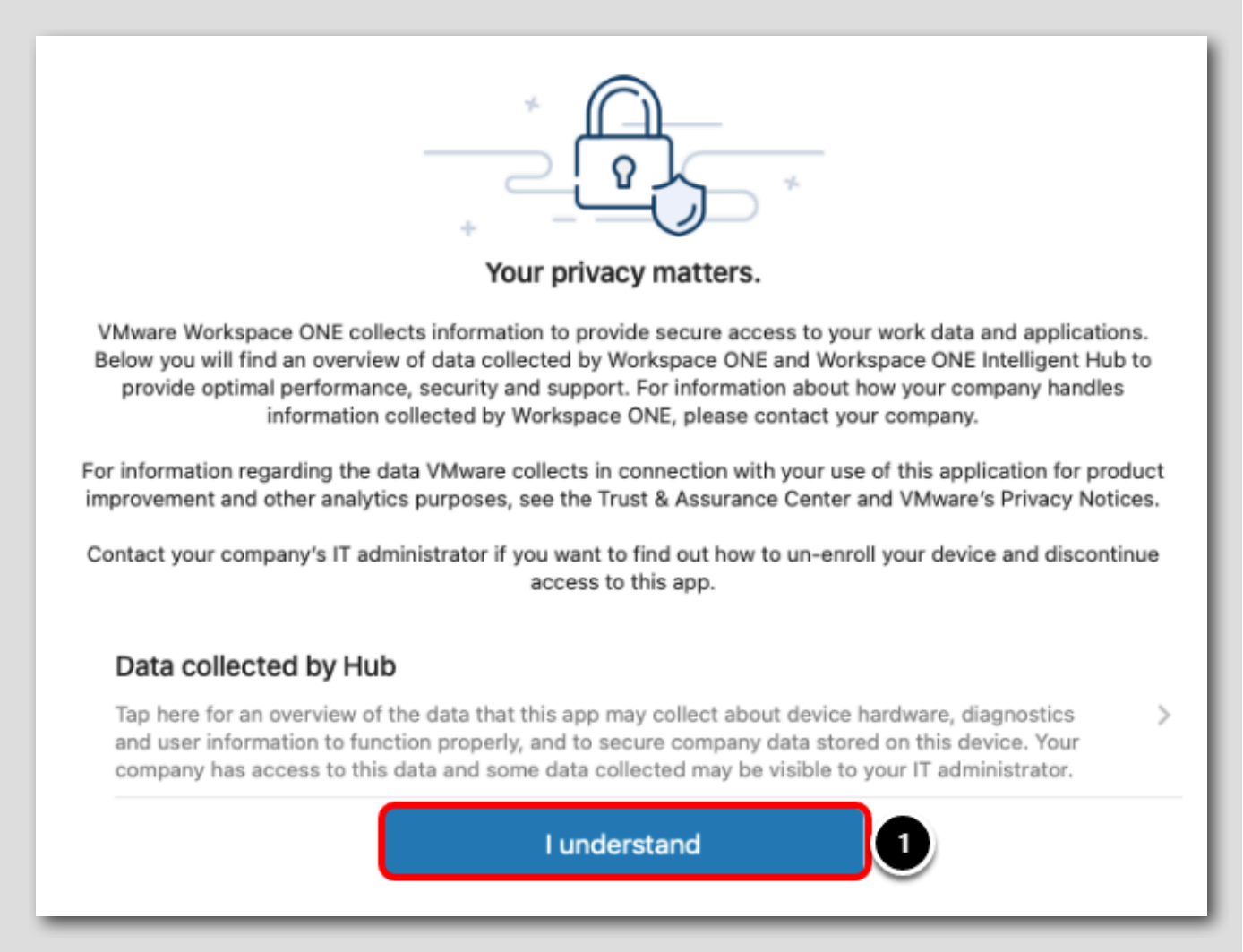
[389]

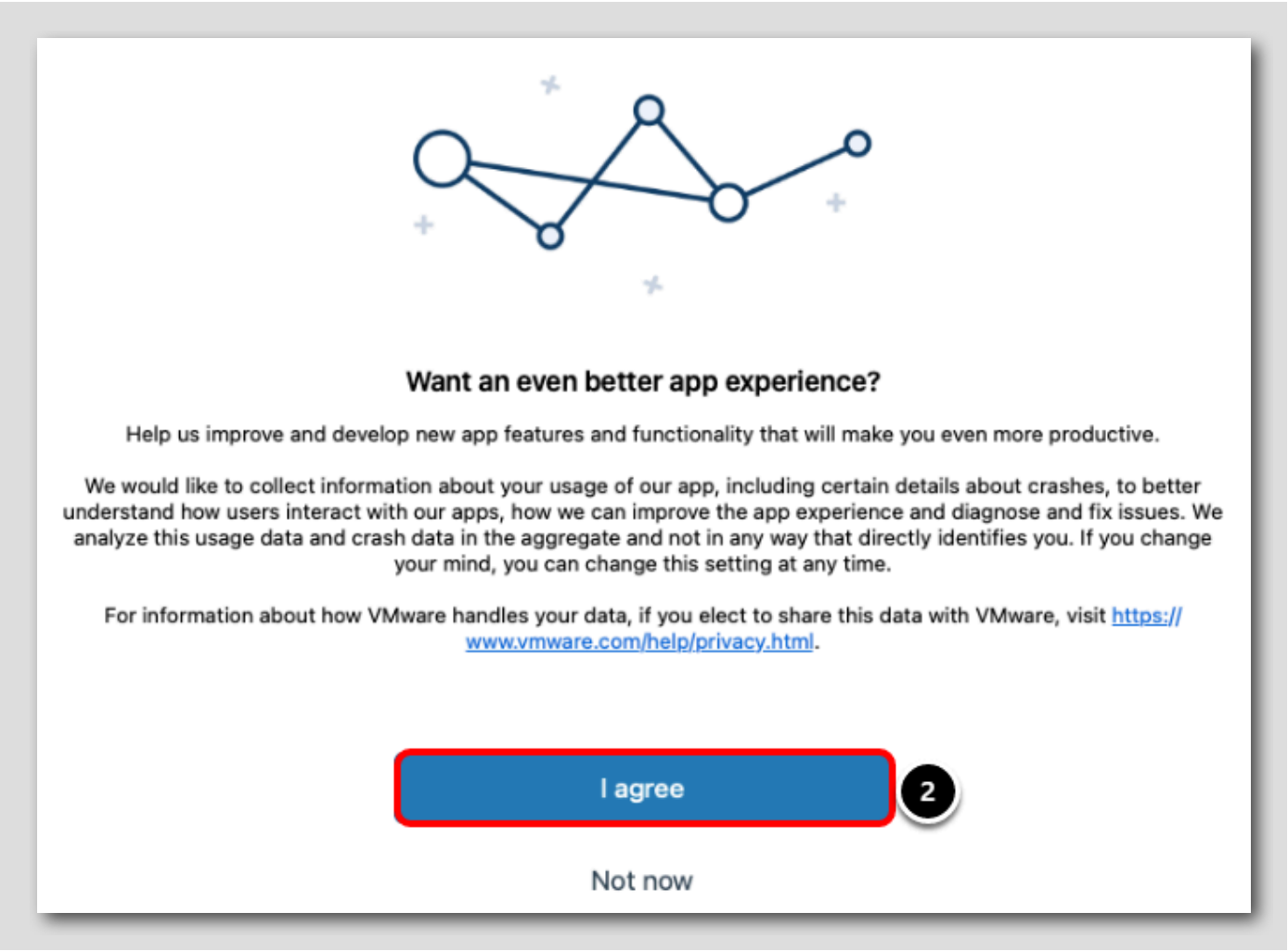


インストールが完了したら、Workspace ONE Intelligent Hub アプリケーションに戻り、[Done] をクリックします。

プライバシーとデータ共有のプロンプトに同意する

[390]





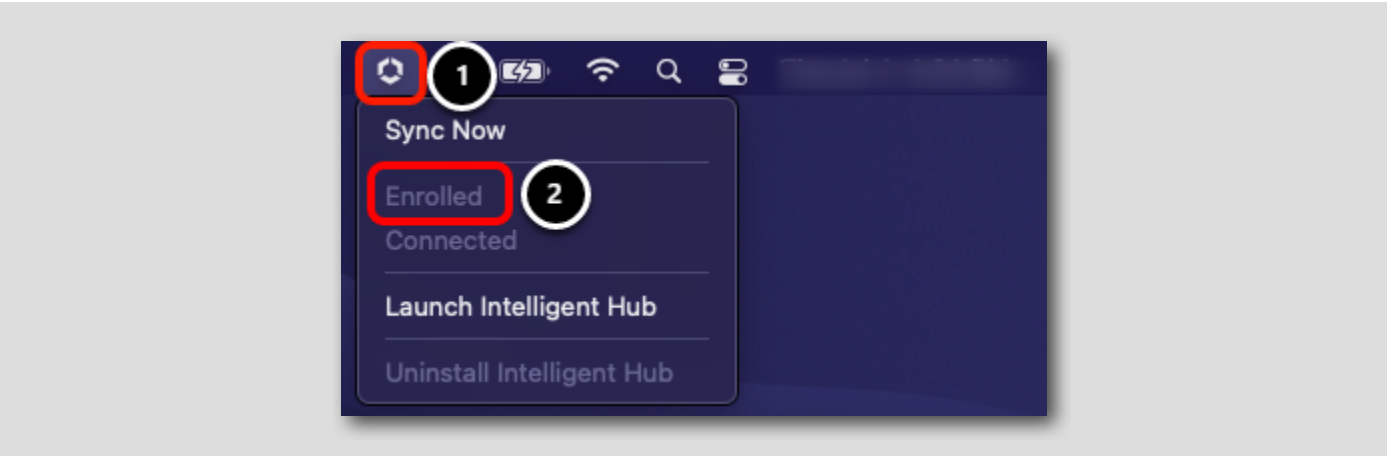
プロンプトが表示されたら、次の手順を実行します。

1. プライバシー ポリシーに対して [I Understand] をクリックします。
2. データ共有ポリシーに対して [I Agree] をクリックします。

Mac 登録の確認

[391]

次の手順に進み、Mac が正常に登録されたことを確認します。



右上隅で、次のように操作します。

1. メニュー バーの Workspace ONE アイコンに注意してください。アイコンをクリックすると、メニューが表示されます。
2. メニューにデバイスが「Enrolled」として表示されます。

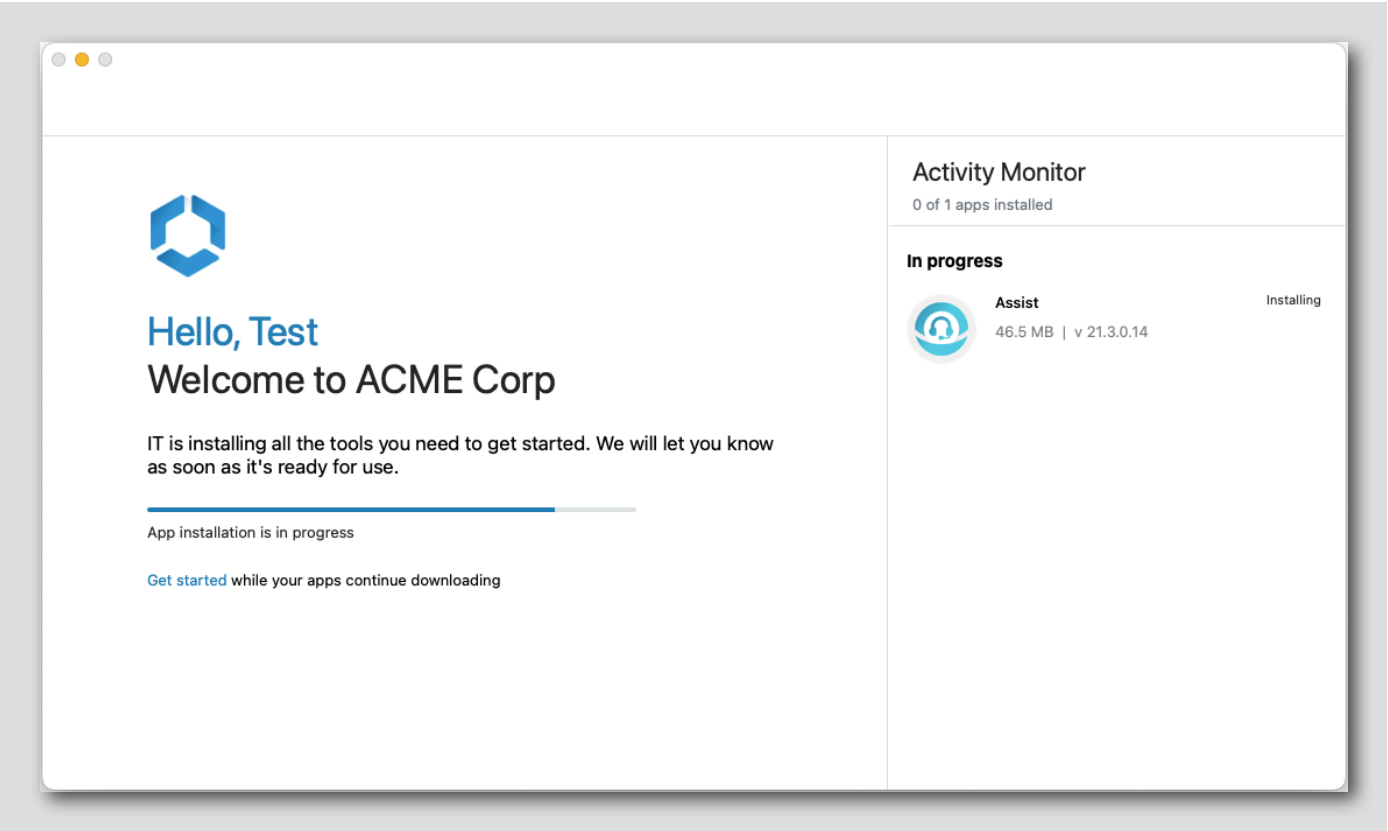
重要なポイント

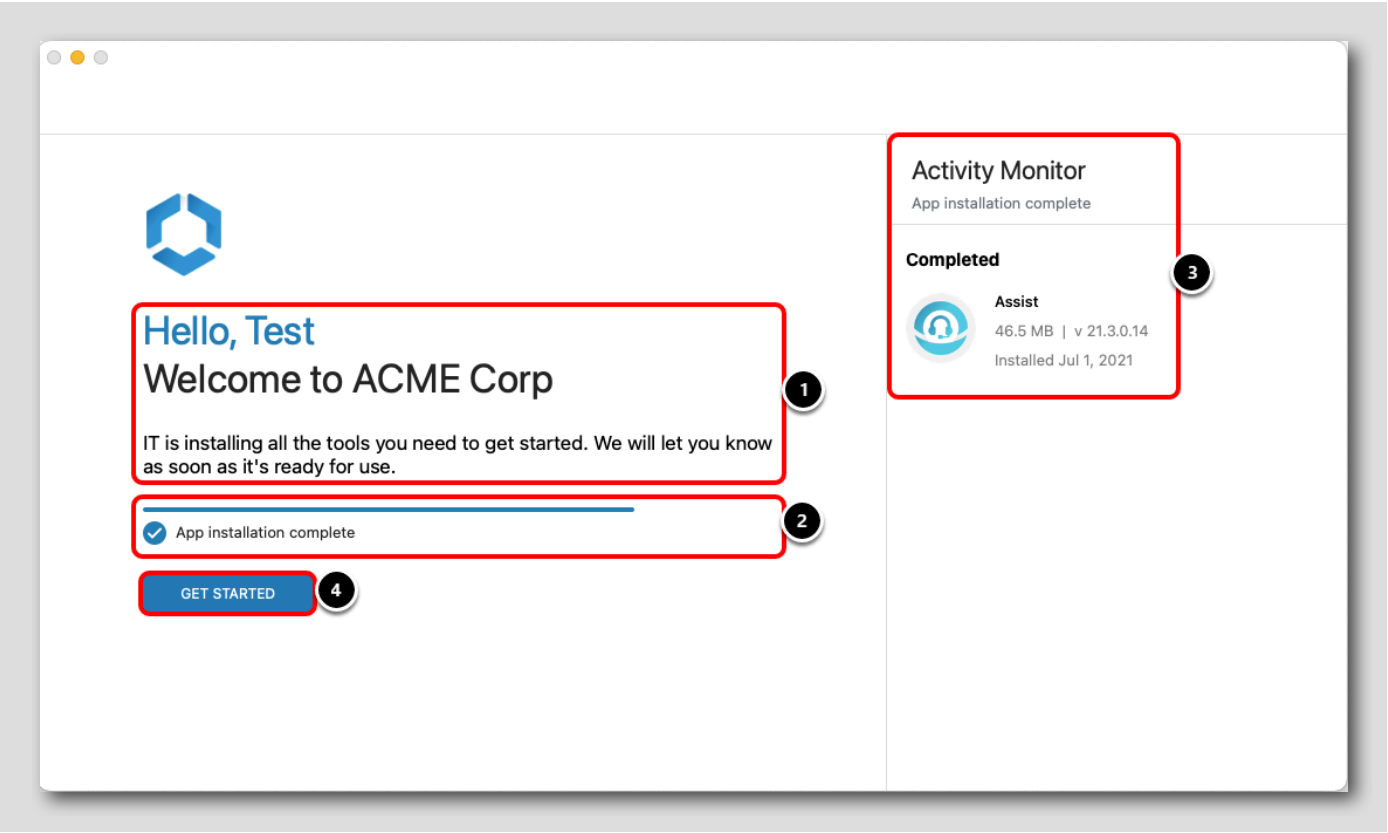
[392]

- エージェント ベースの macOS の登録は、効率的かつ直感的に行えます。
- Workspace ONE UEM では、Web ベースの登録、エージェント ベースの登録に加えて、ステージング（事前にインストールされたエージェント）による登録、代理登録、Apple デバイス登録プログラムによる登録など、さまざまな方法で macOS を登録することができます。
- エージェント ログは、Workspace ONE Intelligent Hub から直接収集できます。これにより、エンド ユーザーがヘルプデスクまたは管理者ユーザーに診断情報を迅速に送信できるようになり、ヘルプデスクのトラブルシューティングが容易になります。

登録済み macOS デバイスの構成の検証

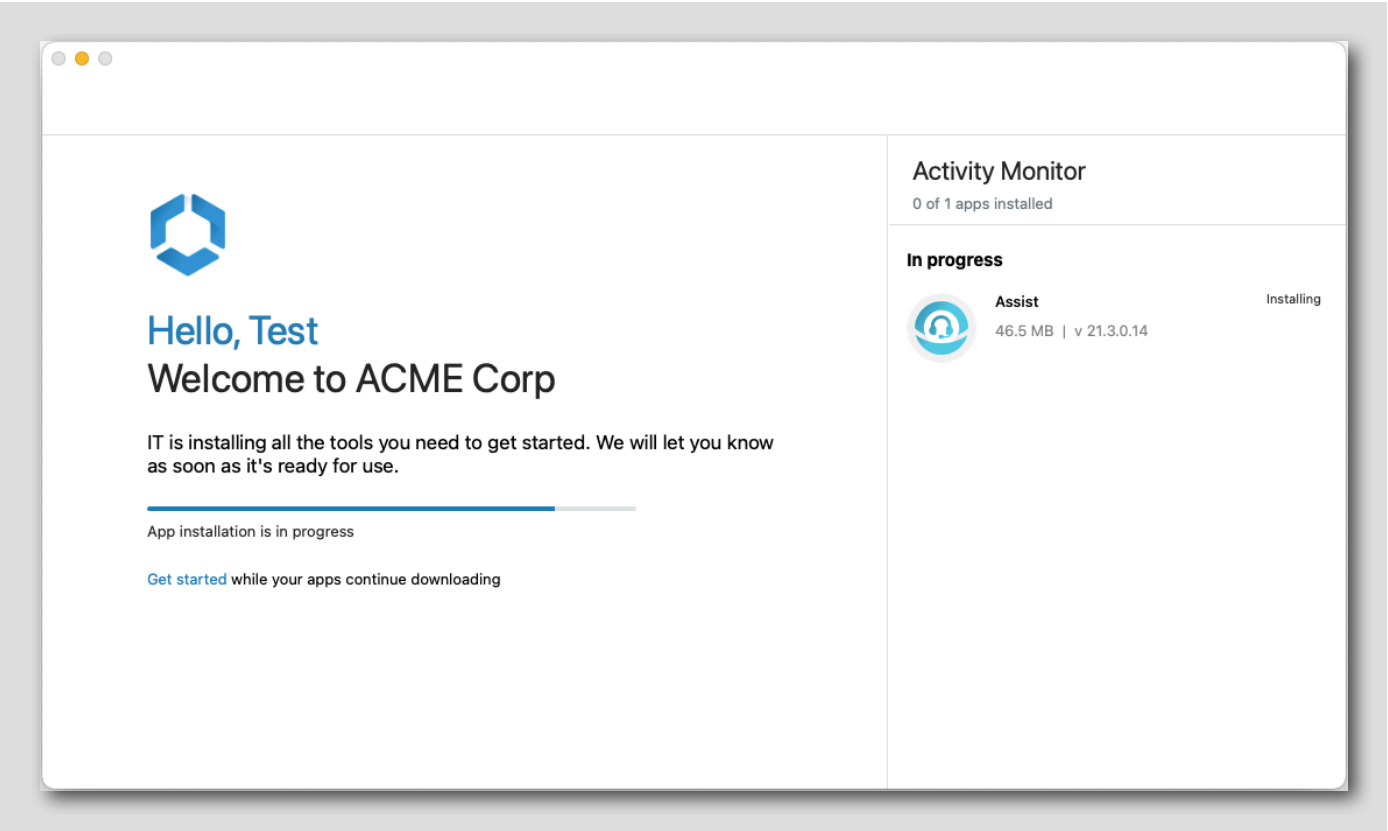
[393]

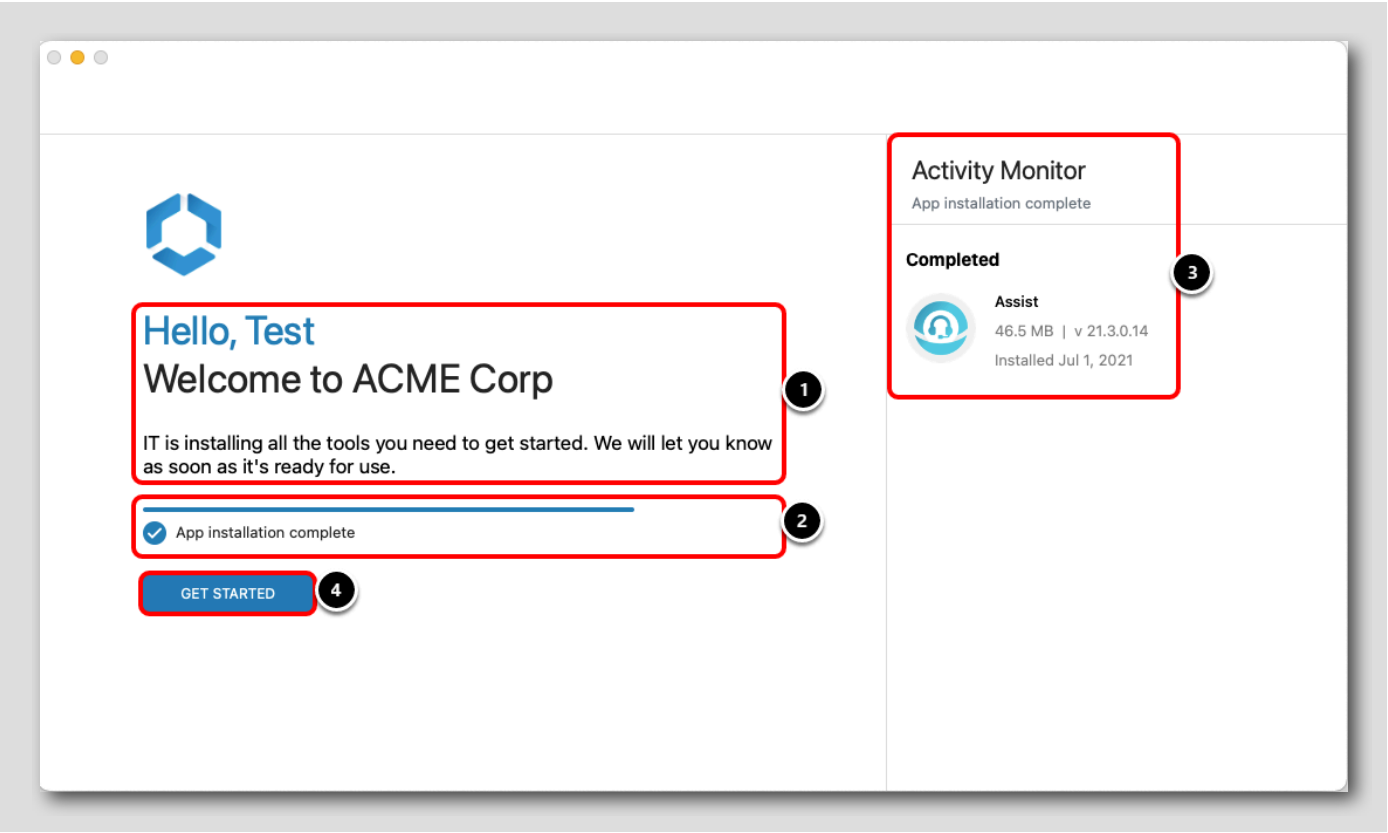




Workspace ONE Intelligent Hub には、Workspace ONE UEM 管理者コンソールで以前に構成したオンボーディング設定が表示されます。

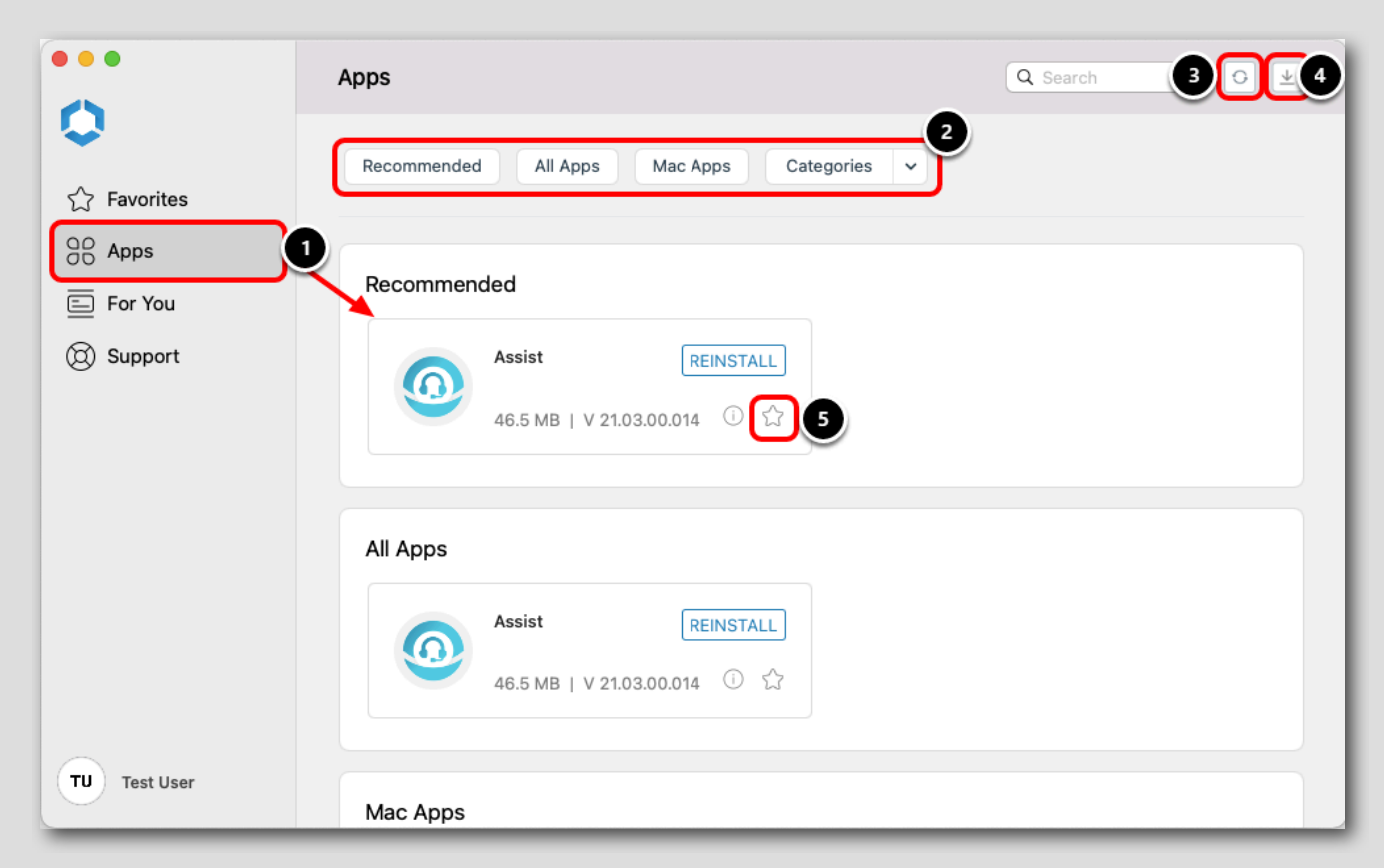
1. ヘッダー (**`Hello, {FirstName}`**)、サブヘッダー (**`Welcome to ACME Corp`**)、および本文にカスタマイズされたオンボーディング エクスペリエンスのために構成されたメッセージが表示されることを確認します。
2. アプリケーションのインストールの進行状況がここに表示されます。
3. 登録時にインストールするように構成されたすべてのアプリケーションが [Activity Monitor] に表示され、監視が簡単かつ明確になります。
4. Workspace ONE Assist アプリケーションのインストールが完了したら、[Get Started] をクリックします。ユーザーはいつでも [Get Started] をクリックして、すべてが完了する前に Hub アプリケーション カタログに進むことができますが、デバイスが完全に構成されているかどうかを、使用する前に監視する明確な方法が提供されます。


Hello, Test
Welcome to ACME Corp
IT is installing all the tools you need to get started. We will let you know as soon as it's ready for use.
App installation is in progress
Get started while your apps continue downloading
Activity Monitor
0 of 1 apps installed
In progress
Assist
Installing
46.5 MB | v 21.3.0.14


Hello, Test
Welcome to ACME Corp
IT is installing all the tools you need to get started. We will let you know as soon as it's ready for use.
1
App installation complete
2
GET STARTED
4
Activity Monitor
App installation complete
Completed
3
Assist
46.5 MB | v 21.3.0.14
Installed Jul 1, 2021

Intelligent Hub アプリケーションの表示

[394]



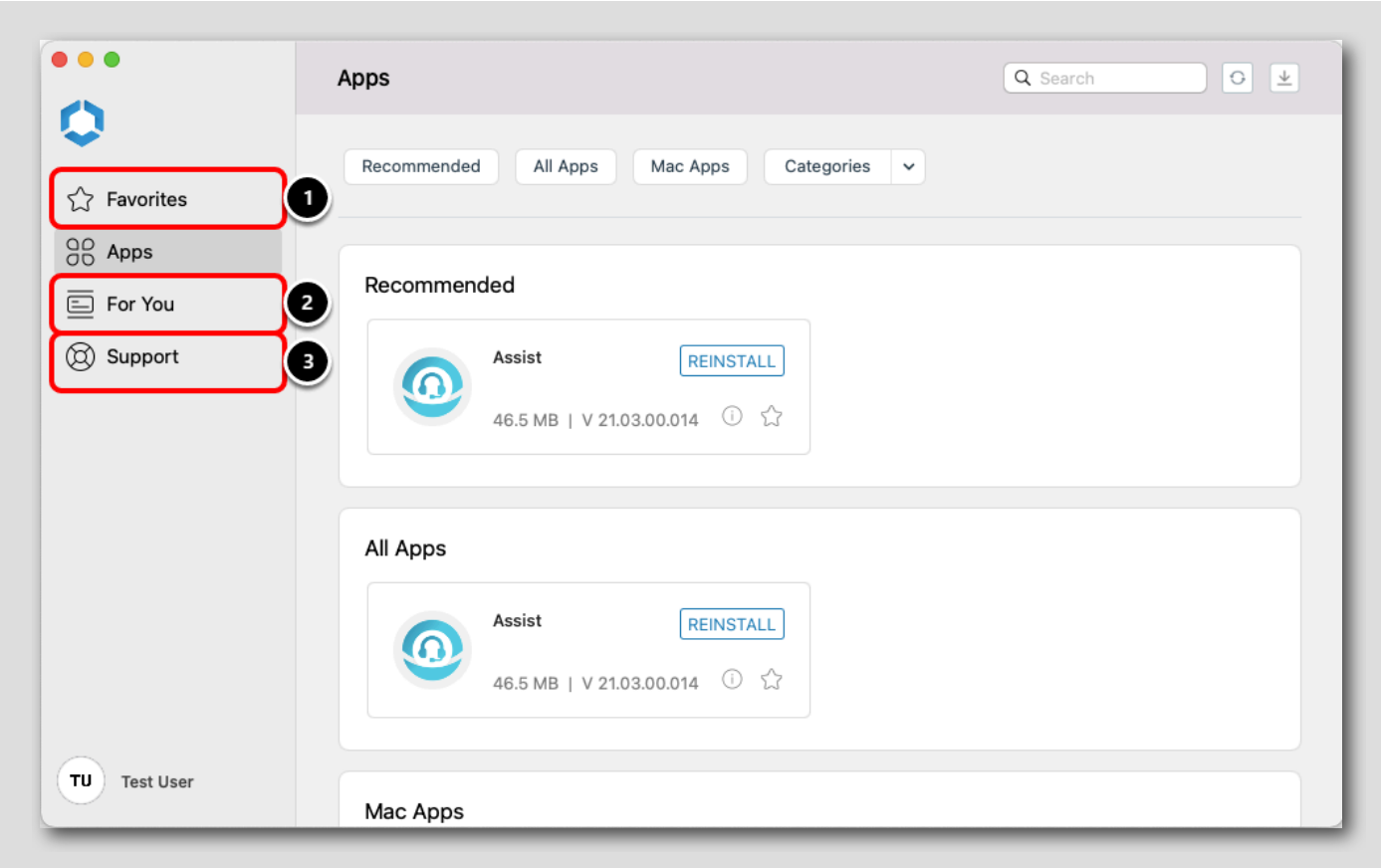
ユーザーが行った構成により、Hub サービスが提供する最新の統合アプリケーション カタログが表示されます。これにより、次の機能が有効になります。

- Favorites
- Apps
- For You（通知）
- Support

1. [Apps] タブをクリックします。ユーザーが操作に使用できるアプリケーションのリストがこのページに表示されます。これには、ネイティブ アプリケーションに加えて、Horizon を介して利用可能になった仮想アプリケーションが含まれる場合があります。
2. 公開したアプリケーションに基づいてフィルタのリストを利用できるため、ユーザーは必要なものを見つけることができます。
3. [Refresh] ボタンをクリックすると、アプリケーション カタログが再ロードされます。
4. [Activity Monitor] を表示して、ユーザーまたは管理者がデバイスに対してトリガした新しいアプリケーションのインストールの進行状況を追跡できます。
5. アプリケーションをお気に入りに追加すると、簡単にアクセスできます。[Assist] をお気に入りアプリケーションとして追加するには星アイコンをクリックします。

その他の Intelligent Hub 機能（オプション）

[395]



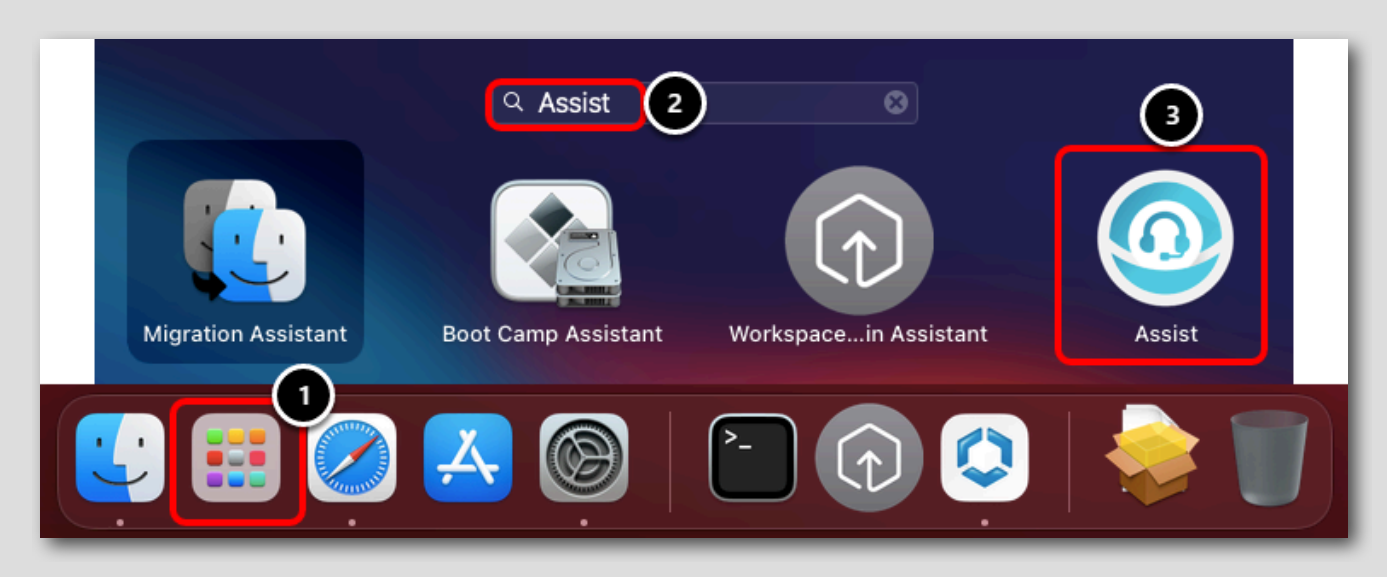
必要に応じて、Intelligent Hub のその他の機能を確認してから、次の手順に進み、デバイスに公開した他の構成を確認します。

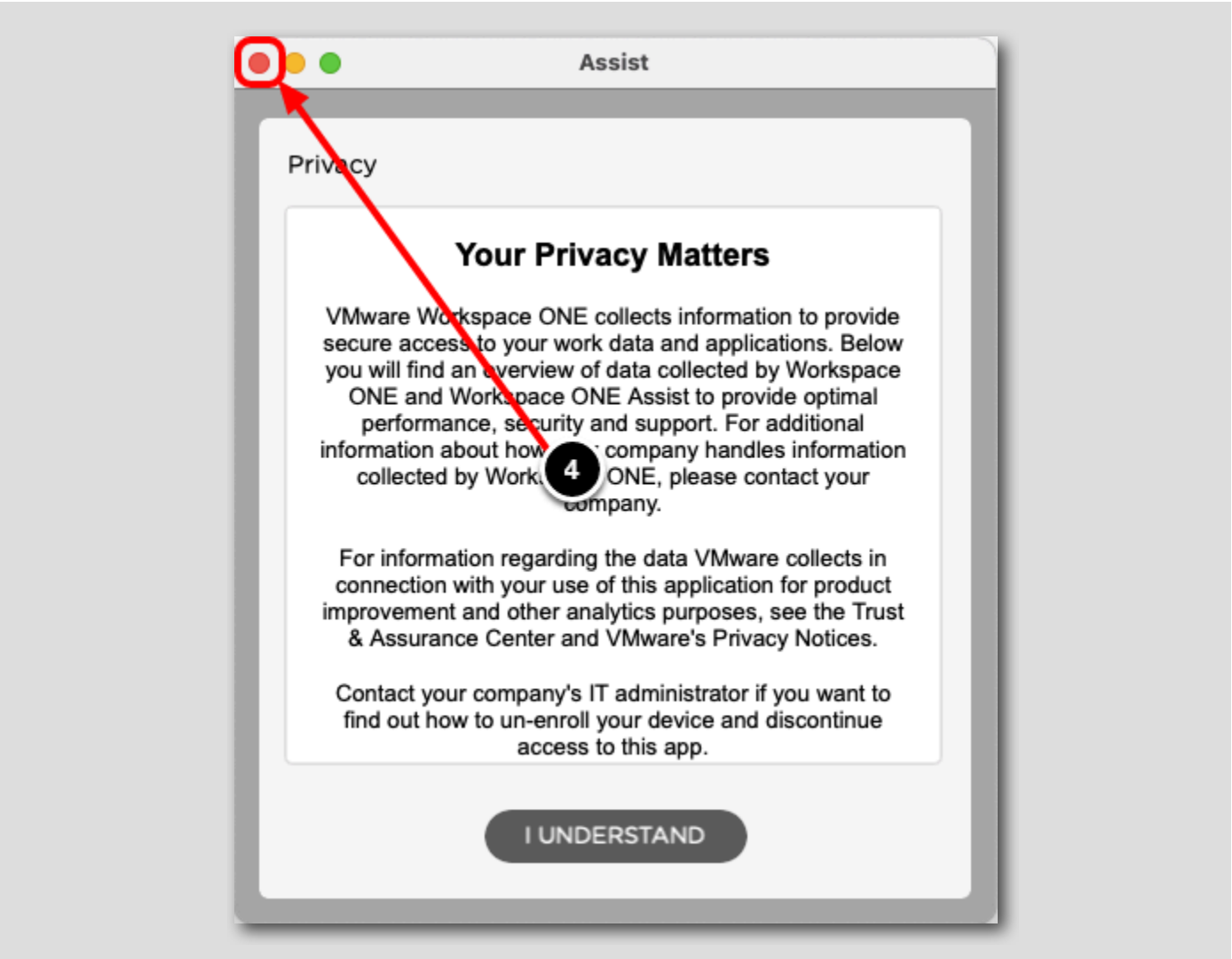
1. [Favorites] タブには、すぐにアクセスできるお気に入りにマークしたアプリケーションのリストが表示されます。
2. [For You] タブには、管理者から送信された通知のリストが表示されます。このリッチ通知は Hub サービスで構成できます。これらの通知の詳細については、「Workspace ONE Intelligent Hub および Hub サービスの概要」モジュールを参照してください。
3. [Support] タブには、ユーザー アカウントに登録されているデバイスのリスト、ログを収集する方法、および管理者に連絡するための構成可能な連絡先の詳細が表示されます。

準備ができたら、次の手順に進んでください。

Workspace ONE Assist のインストールの検証

[396]





1. [Launchpad] を開きます。
2. `Assist` を検索します。
3. Workspace ONE UEM によってインストールされた [Assist] アプリケーションをクリックします。
4. アプリケーションが起動したことを確認したら、[Close] ボタンをクリックしてアプリケーションを閉じます。

これにより、Workspace ONE Assist アプリケーションが正常にダウンロードされ、デバイスにインストールされたことが確認されます。

制限事項プロファイルの確認

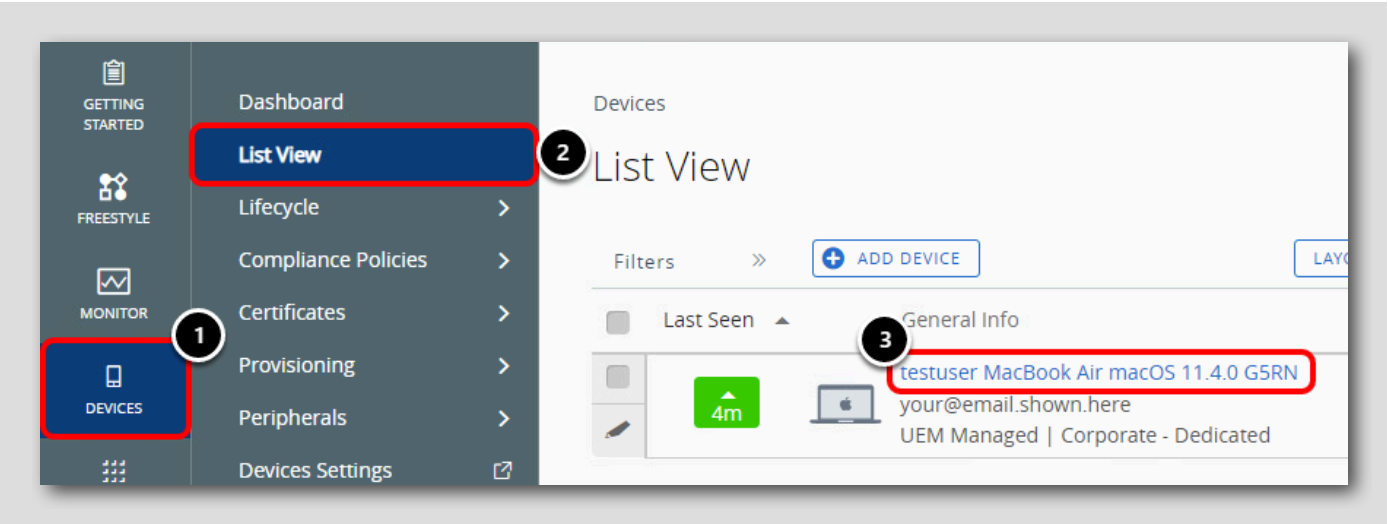
[397]

1. [System Preferences] を開きます。
2. [Desktop & Screen Saver] および [Accessibility] オプションが無効になっていることを確認します。これにより、[System Preferences] でこれらの構成をブロックするために作成した制限事項プロファイルがデバイスに正常に適用されたことが確認されます。

注: これらのオプションに引き続きアクセスできる場合は、[System Preferences] を閉じてから再度開く必要がある場合があります。

デバイス センサーの確認

[398]

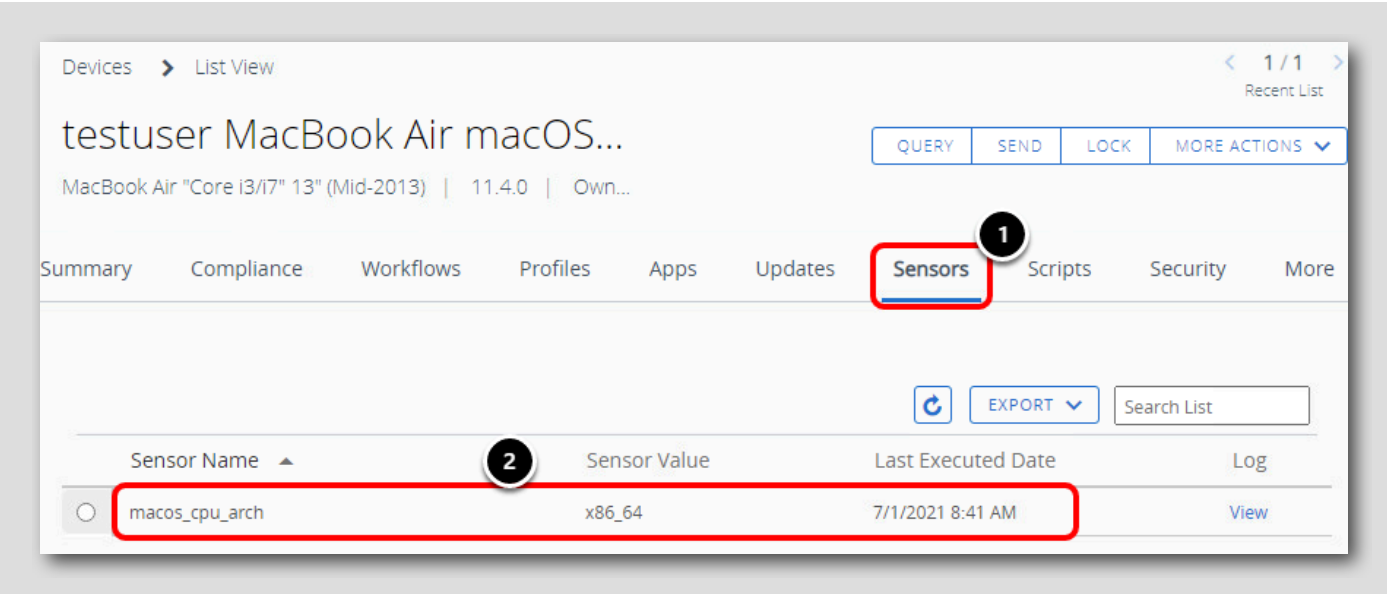


Workspace ONE UEM 管理者コンソールに戻ります。

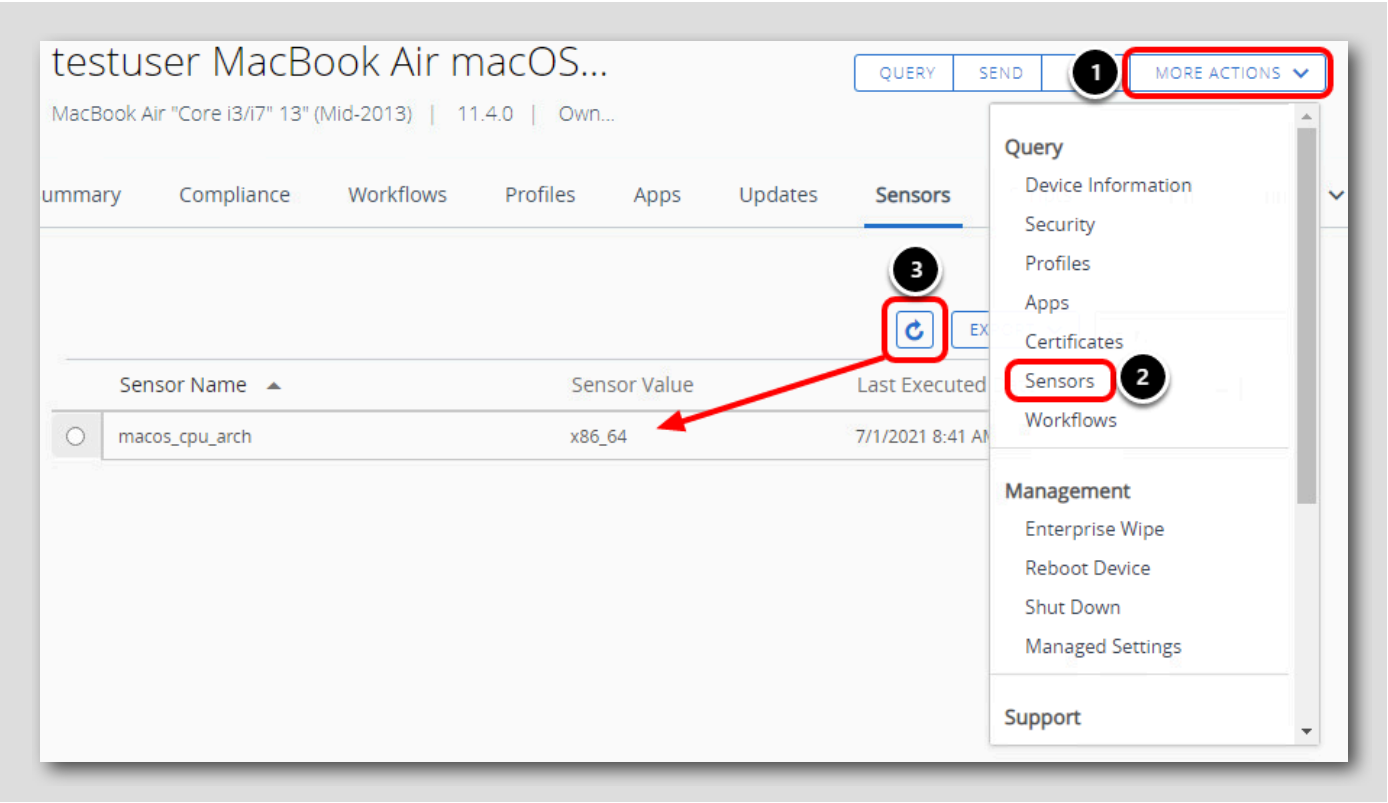
1. [Devices] をクリックします。
2. [List View] をクリックします。
3. [enrolled macOS device] をクリックして、[Device Details] ページを表示します。

デバイス センサーの表示

[399]



1. [Sensors] タブをクリックします。
2. 作成された「macos_cpu_arch」センサーが表示されていることを確認します。デバイスのプロセッサに基づいて、**x86_64**（Intel チップの場合）または **ARM**（M1 チップの場合）のいずれかのセンサー値が表示されます。



センサーがデバイスでまだ処理されていない場合は、デバイスのセンサーを照会してセンサーに処理を強制できます。センサーがすでに実行されている場合は、これをスキップして次の手順に進むことができます。

1. [More Actions] をクリックします。
2. [Sensors] をクリックします。
3. [Refresh] を定期的にクリックし、実行後に macos_cpu_arch センサーがデータを報告しているかどうかを確認します。

重要なポイント

[400]

これで、macOS デバイスに対して行った構成の検証が完了しました。つまり、次の構成と確認が行われました。

1. Hub サービスの統合アプリケーション カタログおよびその他の機能は、Intelligent Hub アプリケーションを介してデバイスで使用できました。
2. [System Preferences] で [Desktop & Screen Saver] および [Accessibility] 設定をブロックする制限事項プロファイルが正常に適用されました。
3. デバイスのプロセッサを検出するセンサーがデバイスに展開され、Workspace ONE UEM 管理者コンソールからアクセスできました。
4. Workspace ONE Assist アプリケーションが正常にアップロードされ、デバイスに展開されました。
5. オンボーディング プロセスが完了したかどうか、およびオンボーディングに含まれていた資産をユーザーが理解するのに役立つ、カスタムの登録後のオンボーディング エクスペリエンスがデバイスで利用可能でした。

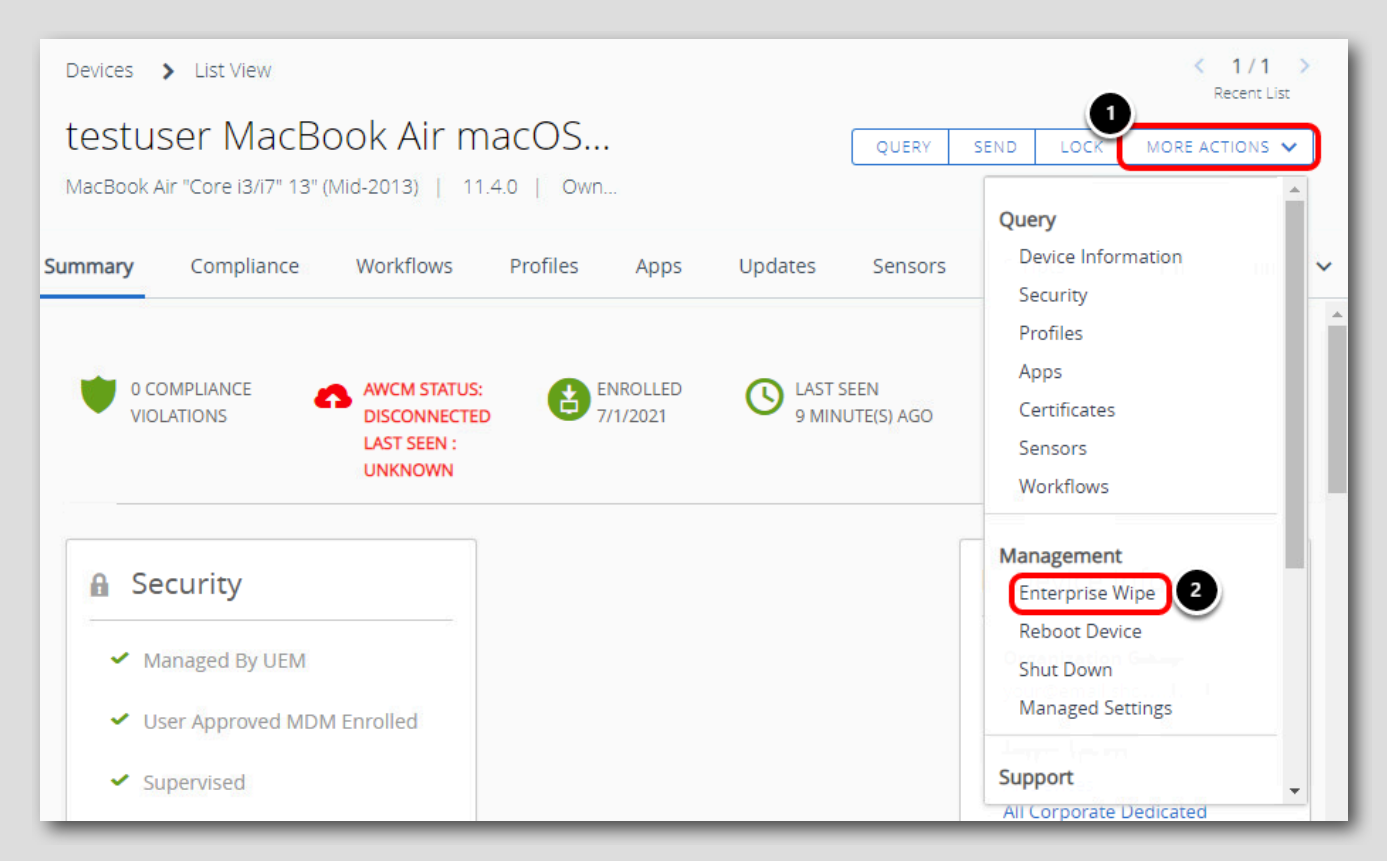
macOS デバイスの企業情報ワイプ

[401]

企業情報ワイプを実行すると、デバイスに追加した企業データが削除されます。個人データはそのまま保持されます。これを使用して、組織からデバイスを廃棄したり、紛失したデバイスをワイプしたりして、企業アプリケーションとデータが確実に削除されるようにすることができます。

企業情報ワイプの開始

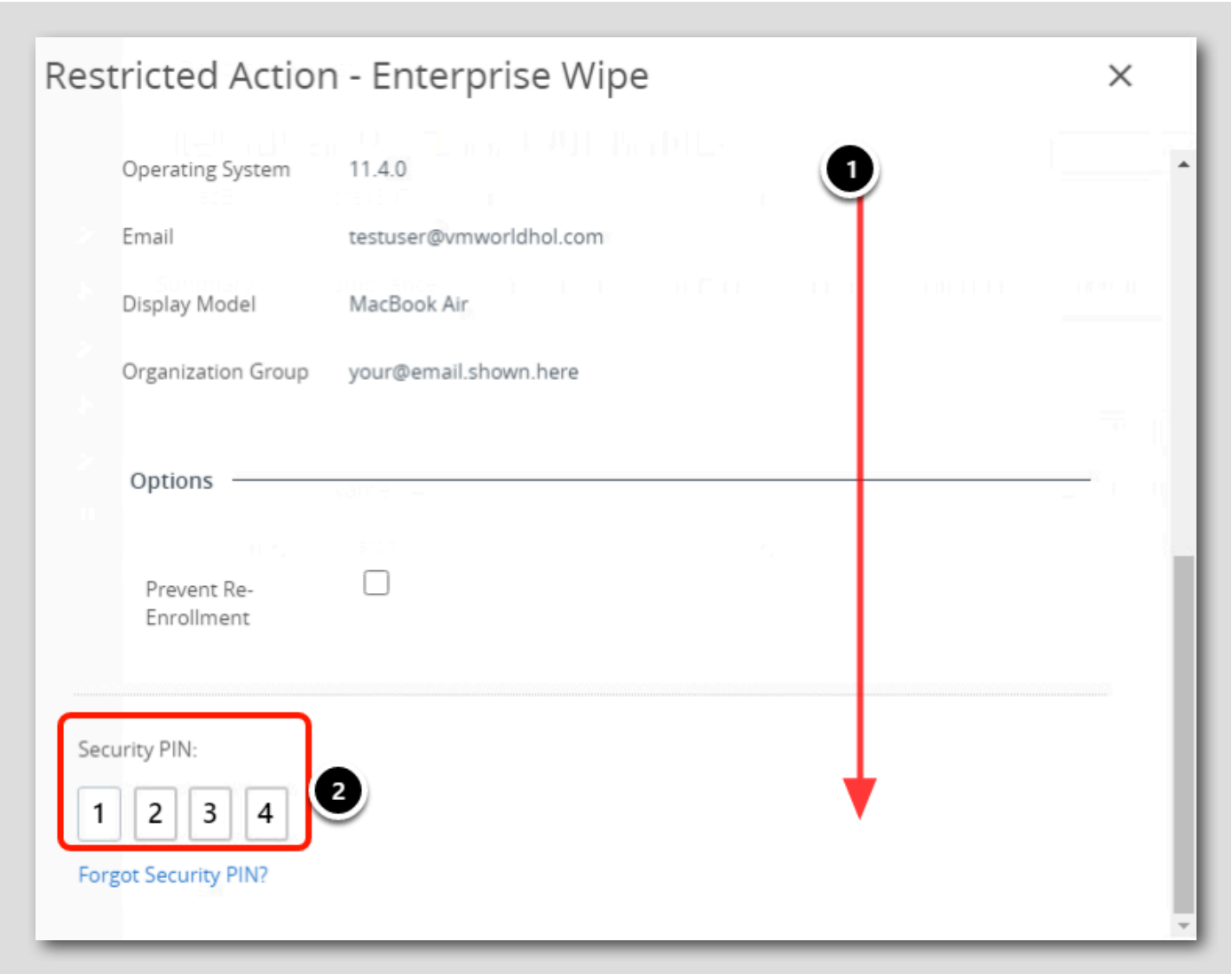
[402]



1. デバイスの詳細ヘッダーのツールバーで、[More Actions] を選択します。
2. ドロップダウン メニューの [Management] ヘッダーの下の [Enterprise Wipe] を選択します。

セキュリティ PIN を入力してワイプを開始

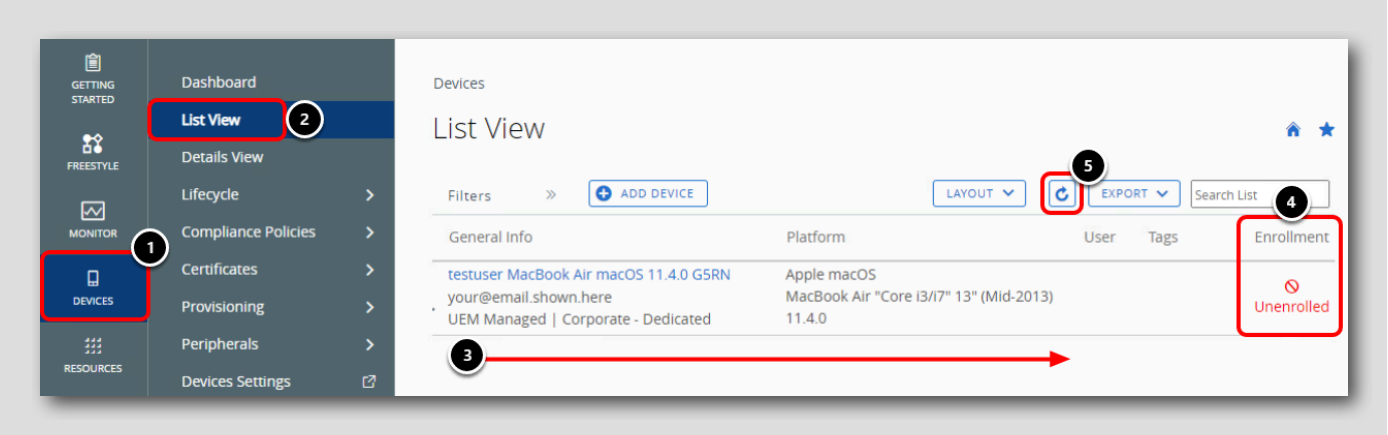
[403]



1. セキュリティ PIN を入力するセクションが表示されるまで下にスクロールします。
2. セキュリティ PIN (**1234**) を入力して、企業情報ワイプを開始します。ラボの最初に別の PIN を入力した場合は、代わりにそのセキュリティ PIN を入力します。

企業情報ワイプの確認

[404]



1. [Devices] をクリックします。
2. [List View] をクリックします。
3. 右にスクロールして、macOS デバイスの [Enrollment] 列を見つけます。
4. [Enrollment] 列に [Unenrolled] と表示されていることを確認します。
5. デバイスがまだ登録解除されていない場合は、[Refresh] ボタンを定期的にクリックして状態を確認します。

企業情報ワイプが完了するまでに数分かかる場合があります。完了すると、デバイスにプッシュされた企業データとアプリケーションは削除されますが、個人データをそのまま残ります。

[Enrollment] 列に [Unenrolled] と表示されたら、次の手順に進みます。

macOS デバイスでの企業情報ワイプの確認

[405]

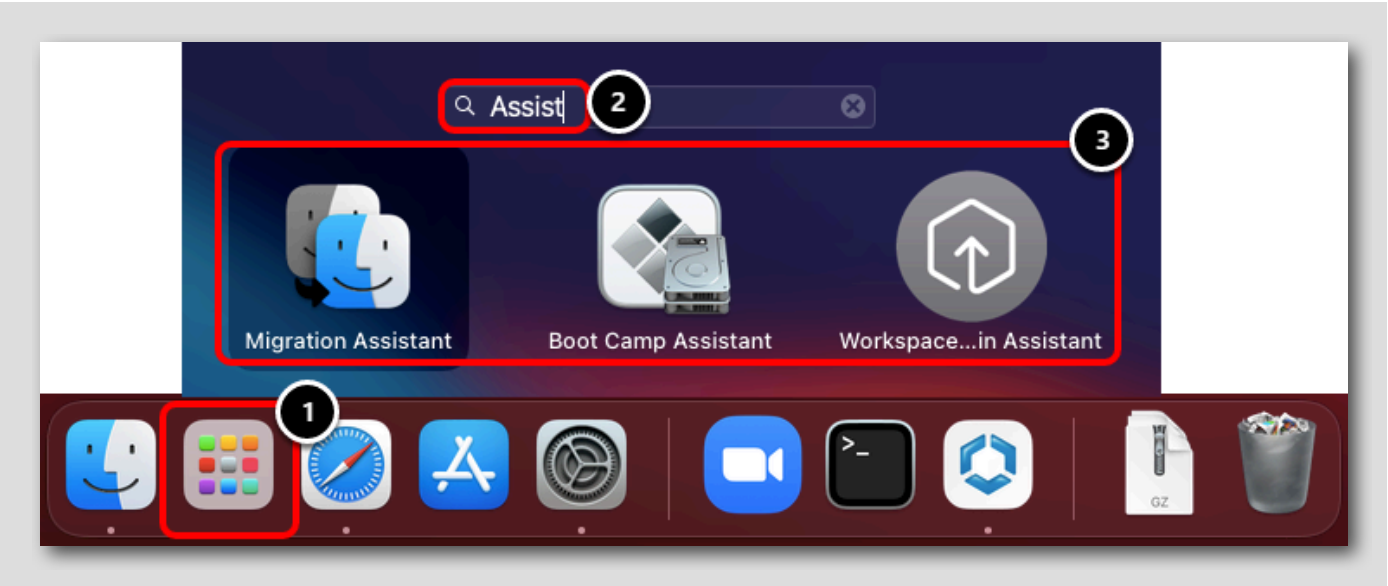
1. [System Preferences] を開きます。
2. [Desktop & Screen Saver] および [Accessibility] の設定を再度構成できることを確認します。

これにより、デバイスが登録解除されたときに制限事項プロファイルが削除されたことを確認できます。


System Preferences
Search
Apple ID
Family Sharing
2
General
Desktop & Screen Saver
Dock & Menu Bar
Mission Control
Siri
Spotlight
Language & Region
Notifications
Internet Accounts
Users & Groups
Accessibility
Screen Time
Extensions
Security & Privacy
Software Update
Network
Bluetooth
Sound
Printers & Scanners
Keyboard
Trackpad
Mouse
Displays
Battery
Date & Time
Sharing
Time Machine
Startup Disk
1

Workspace ONE Assist が削除されたことの確認

[406]



1. [Launchpad] を開きます。
2. 検索バーに **`Assist`** と入力します。
3. 返されるアプリケーションのリストに Workspace ONE Assist が含まれていないことを確認します。

Workspace ONE Assist アプリケーションは [Remove On Unenroll] 制限事項を適用してプッシュされたため、Workspace ONE Assist は登録が解除されるとデバイスから削除されます。

まとめ

[407]

このラボでは、VMware Workspace ONE UEM とユーザーにより開始された登録ワークフローを使用した macOS の基本的な管理について学習しました。実習した内容は、macOS デバイスの登録、プロファイルの作成、アプリケーションの展開、デバイスのロック、カスタム属性の使用、企業情報ワイプによるデバイスからのコンテンツや設定の削除です。

このハンズオン ラボでは、Workspace ONE で macOS を管理するためのすべての機能を網羅*していない*ことに注意してください。macOS 管理の高度なトピックに役立つビデオ、ブログ、およびドキュメントについては、次のような VMware の TechZone を参照してください。

- Apple Business Manager と自動デバイス登録
- デバイスのステージングと代理登録
- Volume 購入済みアプリケーション
- キオスク モード
- 証明書と ID/ディレクトリの統合
- メール統合

・その他

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[408]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。


Your Personal journey from zero to IT Superhero
TECH ZONE
Hands on Labs, Tools and Best Practices
How the products work – beginner to expert
Guide to production deployments & operations
Quick start for your first proof of concept
Latest product information

モジュール 5：Android 管理の概要（30 分）

はじめに

[410]

Android デバイスを Workspace ONE UEM に登録し、制限事項を構成してアプリケーションをプッシュすることで登録済みデバイスを管理する方法など、Android Enterprise の基礎を学びます。Android Enterprise と Workspace ONE UEM が、最新のデバイス管理 API を使用して Android デバイスをどのように保護するかを学びます。

Android Enterprise とは

[411]

Android Enterprise とは

Android Enterprise は、デバイス管理とエンタープライズ モビリティ管理 (EMM) API の共通セットを統合するために、メーカーが自社の OS イメージに追加できるオプションのソリューションとして、2014 年に 5.0 Lollipop でデビューしました。6.0 Marshmallow 以降はオプションではなくなり、Google Mobile Service (GMS) 認定のすべてのメーカーにとって必須のコンポーネントになりました。

Android Enterprise のメリット

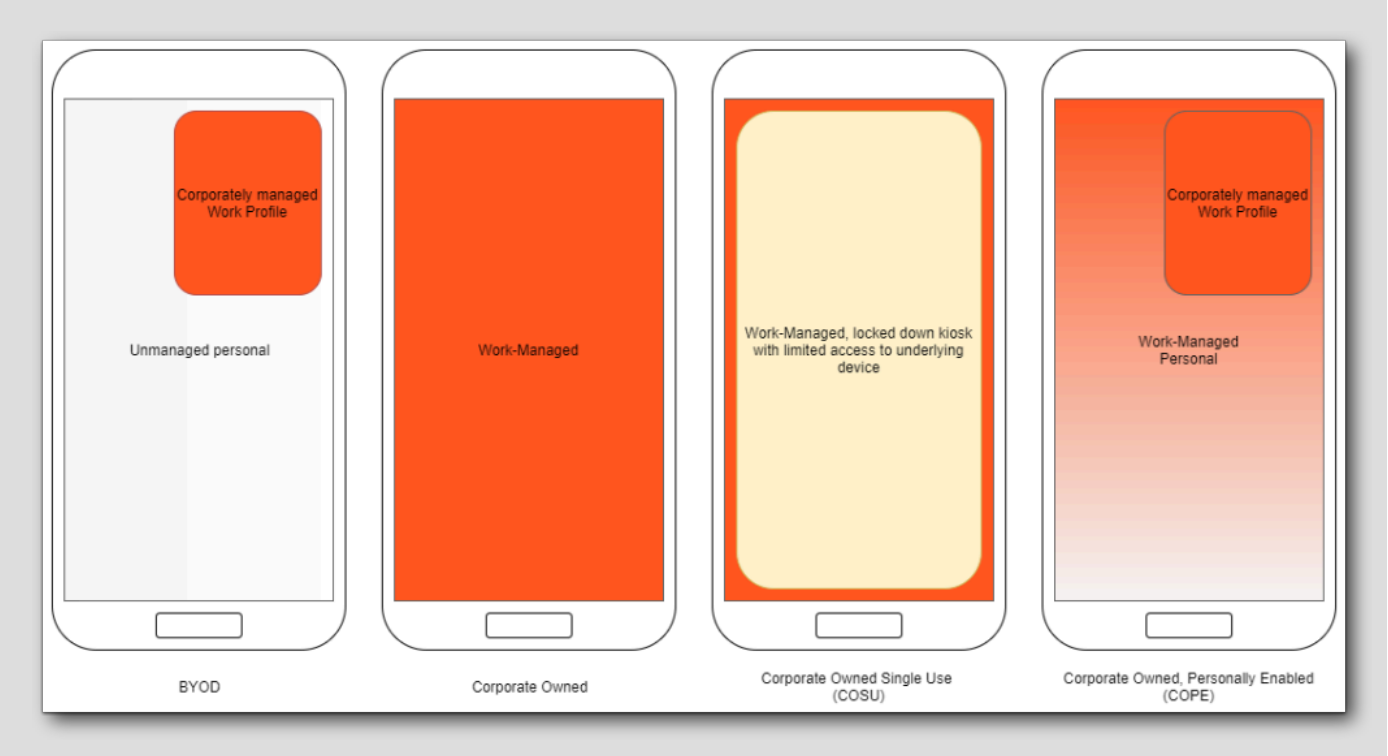
[412]

Android Enterprise には、デバイス管理のさまざまなシナリオに対応するさまざまな豊富な機能が用意されています。

- **Enterprise Mobility Management (EMM)** の豊富なエクスペリエンス。これにより、デバイス管理者は構成、アプリケーション、ポリシーを任意の Android Enterprise (AE) デバイスに送信できます。デバイスの場所を問わず、デバイスおよび企業データを安全に管理することができます。
- BYOD (Bring Your Own Device) シナリオの**Work Profile** モード。これにより、デバイスに個人のアプリケーションやデータとは別の作業コンテナを持たせることができます。
- **Work-Managed** モード（以前の**デバイス所有者**）。これは、個人使用を目的としていない企業所有のデバイスを保護するためのより多くのオプションを企業に提供します。
- **Corporate Owned Single Use** (COSU) モード。これはキオスクライクのエクスペリエンスを企業に提供します。Work-Managed デバイスは、キオスクライクな状態でロックダウンされ、基盤となるデバイス オペレーティング システム全体ではなく、いくつかのアプリケーションまたはリソースへのアクセスを許可します。
- **Corporate Owned Personally Enabled** (COPE) は、Work Profile と Work-Managed モードを統合し、個人スペースを備えた完全に管理されたデバイスを提供します。
- 特別な設定なしで使用できる Android 8.0 以降のデバイスの**ゼロタッチ登録**。エンド ユーザーに合理化された登録エクスペリエンスを提供します。
- 企業が管理する **Managed Google Play ポータル**。これにより、管理者は、エンド ユーザーがアクセスできるアプリケーション ストアへのアプリケーションを明示的に承認できます。
- ユーザーがデバイス上で Google アカウントを指定する必要のない**アプリケーションのサイレント インストール**。
- **アプリケーション構成**。これにより、デバイス管理者がキーと値のペアを管理対象アプリケーションに展開し、エンド ユーザーのエクスペリエンスを変更できるようにします。
- 企業のリソースがデバイス上で保護されていることを確認するための**必須のデバイス暗号化**。

デバイス管理のシナリオについて

[413]



上記の図は、さまざまなデバイス管理シナリオ間の全体像の違いを示しています。

Bring Your Own Device (BYOD):

- 通常、従業員やエンド ユーザーが企業リソースへのアクセスを必要とする個人所有のデバイスを使用する場合に使用されます。
- エンド ユーザーの個人データまたはアプリケーションを管理しないようにするために、**仕事用プロファイル**を展開して、個人アプリケーションおよびデータとは別に企業アプリケーションとデータを保持することができます。
- これにより、デバイス管理者は、個人用デバイスを完全に管理することなく、個人デバイスから企業リソースへのアクセスを安全に制御することができます。

Corporate Owned:

- 通常、各自のロールやタスクを遂行できるように従業員またはエンド ユーザーに配備するデバイスを企業が所有している場合に使用されます。
- Work-Managed モードでは、デバイス全体の管理と制御が可能になり、幅広い構成が可能になります。
- Work-Managed モードでは、管理対象外の個人スペースは提供されません。企業所有のデバイスにのみ使用する必要があります。

Corporate Owned Single Use (COSU):

- 通常、キオスクとして使用されるデバイス、またはキオスクライクなアプリケーションが実行されているデバイスを企業が所有している場合に使用されます。
- Corporate Owned Single Use は Work-Managed モードを利用してデバイス全体を管理しますが、基盤となるデバイス オペレーティング システムへのアクセスをエンド ユーザーに付与することはありません。

Corporate Owned Personally Enabled (COPE):

- 通常、従業員またはエンド ユーザーに配備され、一定レベルの個人使用を許可する一方で、企業による制御が実施されるデバイスを企業が所有している場合に使用されます。
- Corporate Owned Personally Enabled の場合は、Work Profile を利用して企業のリソース、データ、およびアプリケーションを管理しながら、さまざまな量の個人使用に対して Work-Managed 個人スペースを利用します。
- これにより、Work Profile モードと Work-Managed モードのアイデアが 1 つのデバイスに統合されます。

さまざまな登録方法

[414]

さまざまなデバイス管理シナリオを提供することに加えて、複数の方法でデバイスを Android Enterprise に登録することもできます。

Near-Field Communication (NFC) の登録

[415]

Near-Field Communication (NFC) のバンプ方式を使用すると、指定されたプログラマ デバイス上に NFC プログラマ アプリケーションがセットアップされます。後続のデバイスはプログラマ デバイスに「バンプ」され、必要な初期ポリシー（Wi-Fi、デバイス構成など）を NFC 経由でバンプされたデバイスに渡します。

プロセスは、事前に適用された設定、関連するプラットフォームにデバイスを登録するためにダウンロードされるエージェントなどの点で、多少異なります。Workspace ONE UEM では、デバイスを直接登録するための名前付きアカウントの追加構成が可能です。

ハッシュタグ (#) 登録またはデバイス ポリシー コントローラ (DPC) ID の登録

[416]

この方法は、Android 6.0 Marshmallow で導入されました。新しくワイプされた（または購入した新しい）デバイスでアカウントを追加または作成するように求められた場合、管理者は Google アカウントを入力するのではなく、**afw#hub** と入力するだけで、デバイスが Workspace ONE Intelligent Hub アプリケーションをダウンロードして、正しい構成で登録プロセスを開始します。

QR 登録

[417]

デバイスでセットアップ ウィザードが起動するときに [Welcome] を 6 回タップすると、デバイスを Wi-Fi に接続して QR 登録を開始するように求められます。

Android 9.0 P では、QR ペイロードはシステムにバンドルされているため、ダウンロードする必要はありません。これにより、デバイスが QR パッケージをダウンロードするためにインターネットに接続する必要がなくなり、QR コードに Wi-Fi 認証情報を追加できるため、プロビジョニングが高速になります。

ゼロタッチ登録

[418]

デバイスは、認定リセラーを通じて購入され、Workspace ONE UEM に割り当てられます。その後、エンド ユーザーが初めてデバイスを使用すると、すぐに Work-Managed デバイスとして登録できるようになります。ゼロタッチ登録では、管理者は登録および構成済みのデバイスをエンド ユーザーに直接送り、認証を受けることができます。

個人の Android デバイスを登録しないでください

[419]

重要: 今後の演習のために個人のデバイスを登録しないでください。

個人のデバイスが他の UEM プロバイダーに登録されると、望ましくない競合や問題が発生する可能性があります。

このラボを完了するには、テスト デバイスのみを使用し、個人のデバイスをラボに登録しないことをお勧めします。

Workspace ONE UEM Console へのログイン

[420]

このラボを開始するには、Workspace ONE UEM 管理コンソールにログインする必要があります。

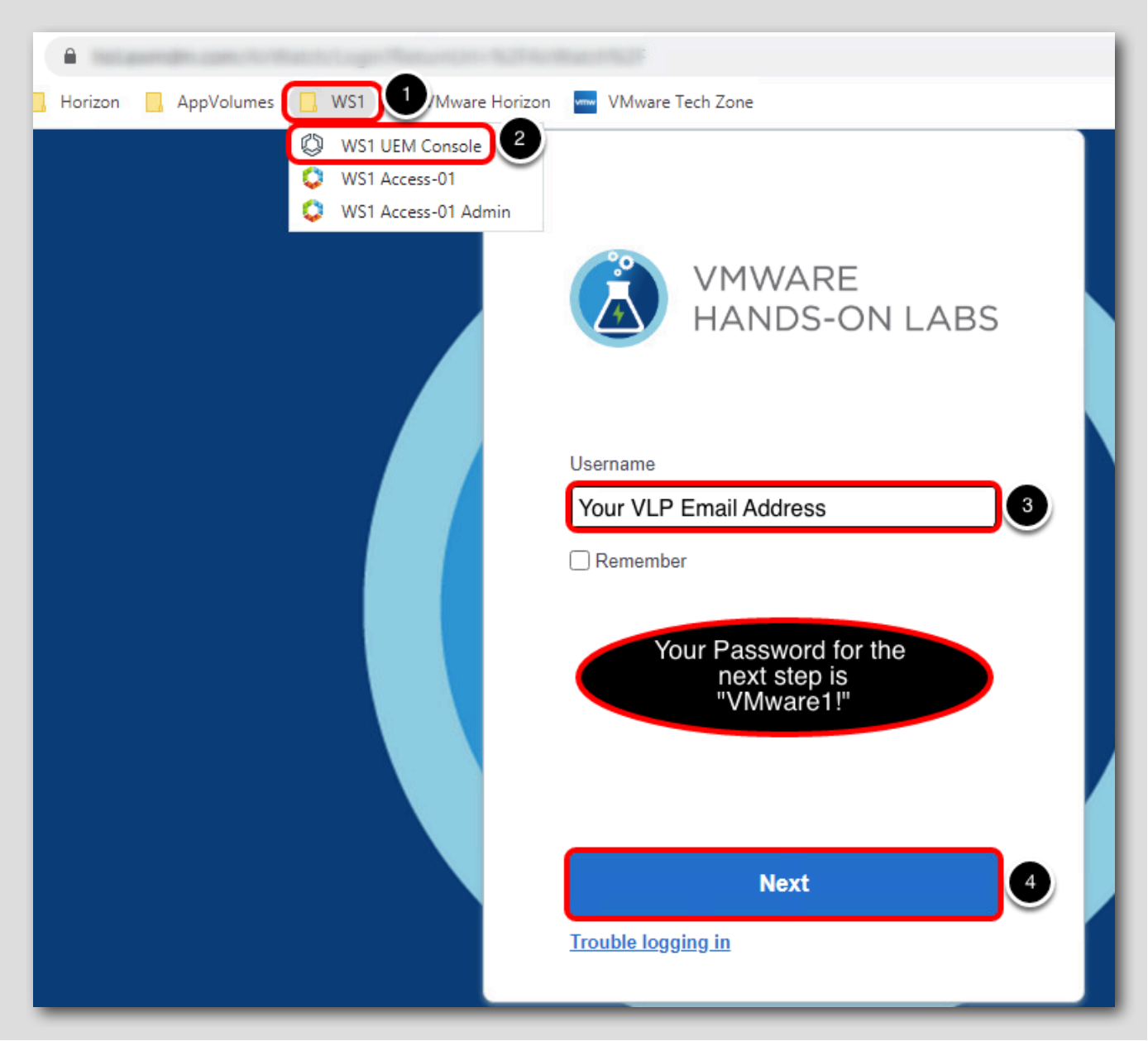
Chrome ブラウザの起動

[421]

現在接続している仮想マシンのデスクトップから、[Google Chrome] ショートカットをダブルクリックします。

[422]

Workspace ONE UEM 管理コンソールへのログイン



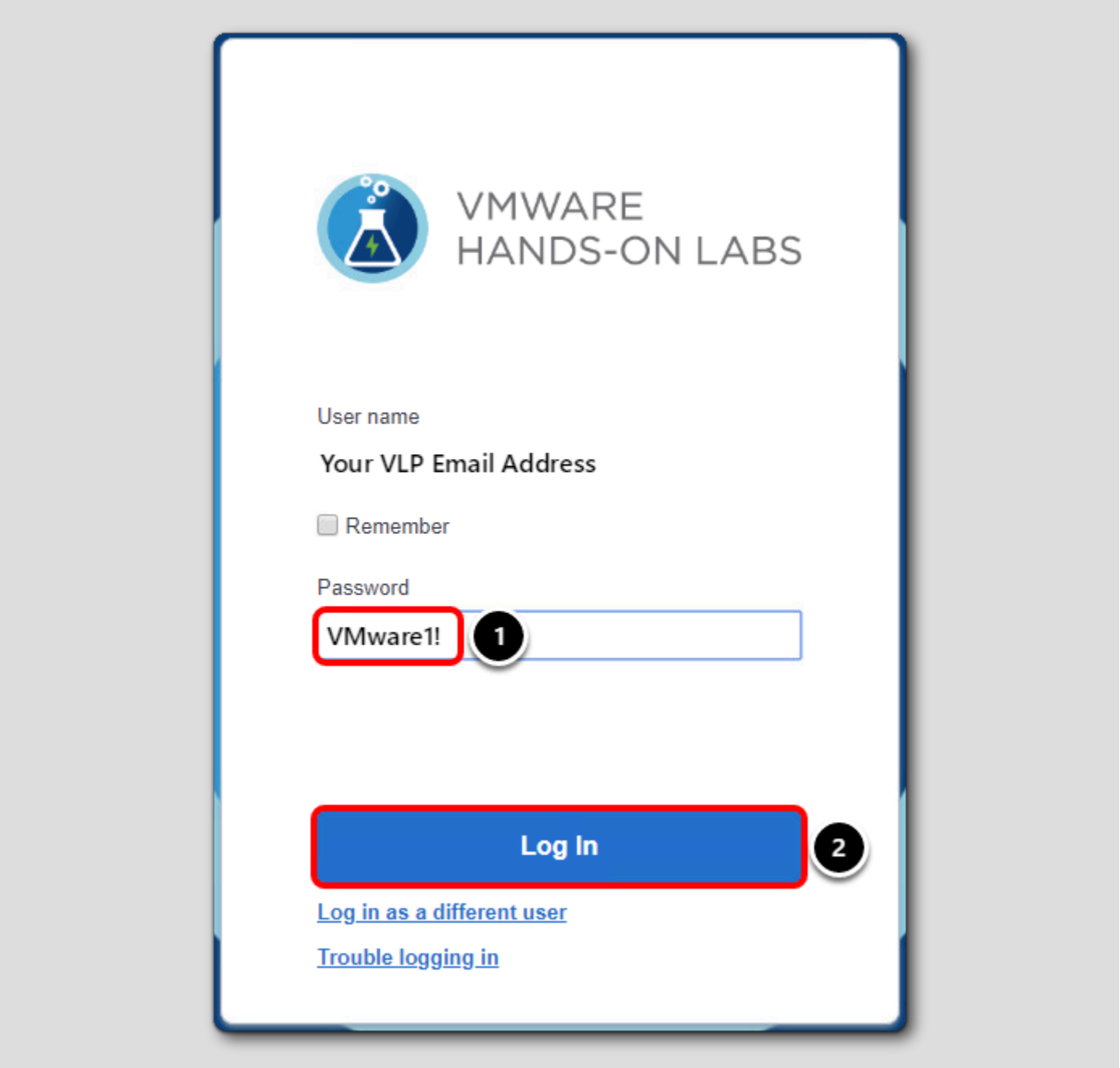
1. [WS1] ブックマーク フォルダをクリックします。
2. [WS1 UEM Console] リンクをクリックします。
3. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。

   注： 次の手順のパスワードは、**`VMware1!`** になります。

4. [Next] をクリックします。

Workspace ONE UEM Console の認証情報の入力

[423]



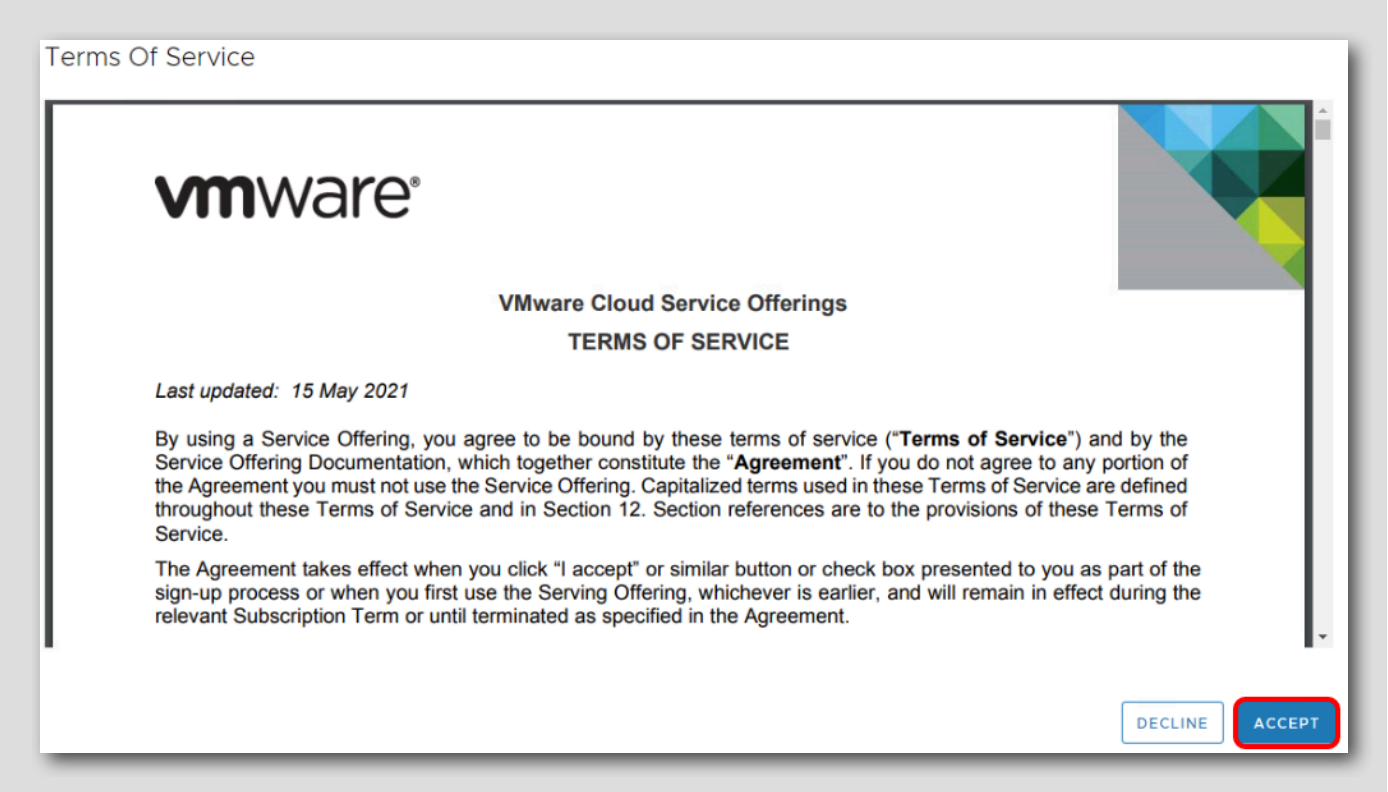
[Password] フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

利用規約の承諾

[424]



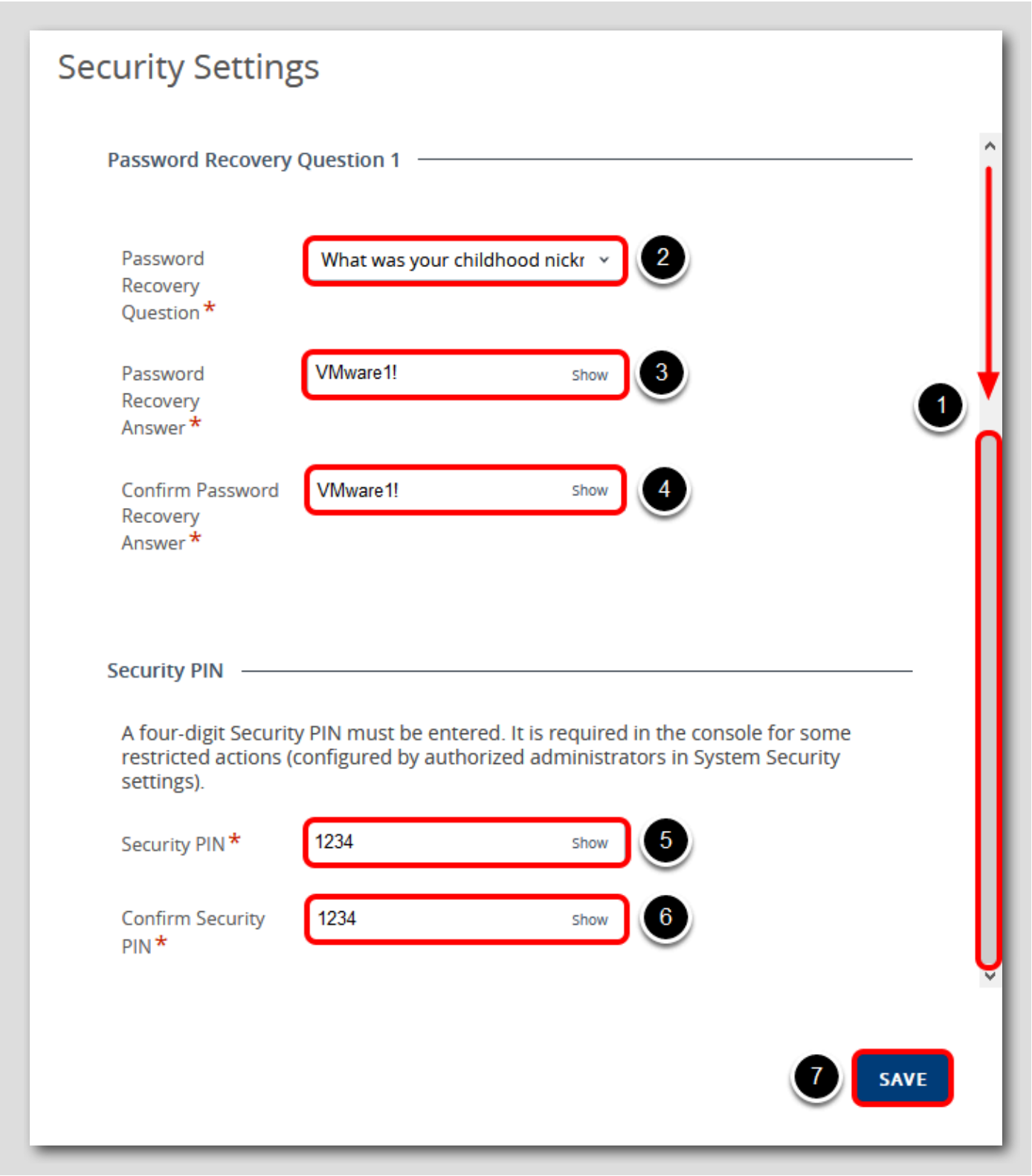
[Workspace ONE UEM Terms of Service] が表示されたら、[Accept] ボタンをクリックします。

注：以降の手順は、管理コンソールへの初回ログイン時にのみ実行されます。

初期セキュリティ設定の完了

[425]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

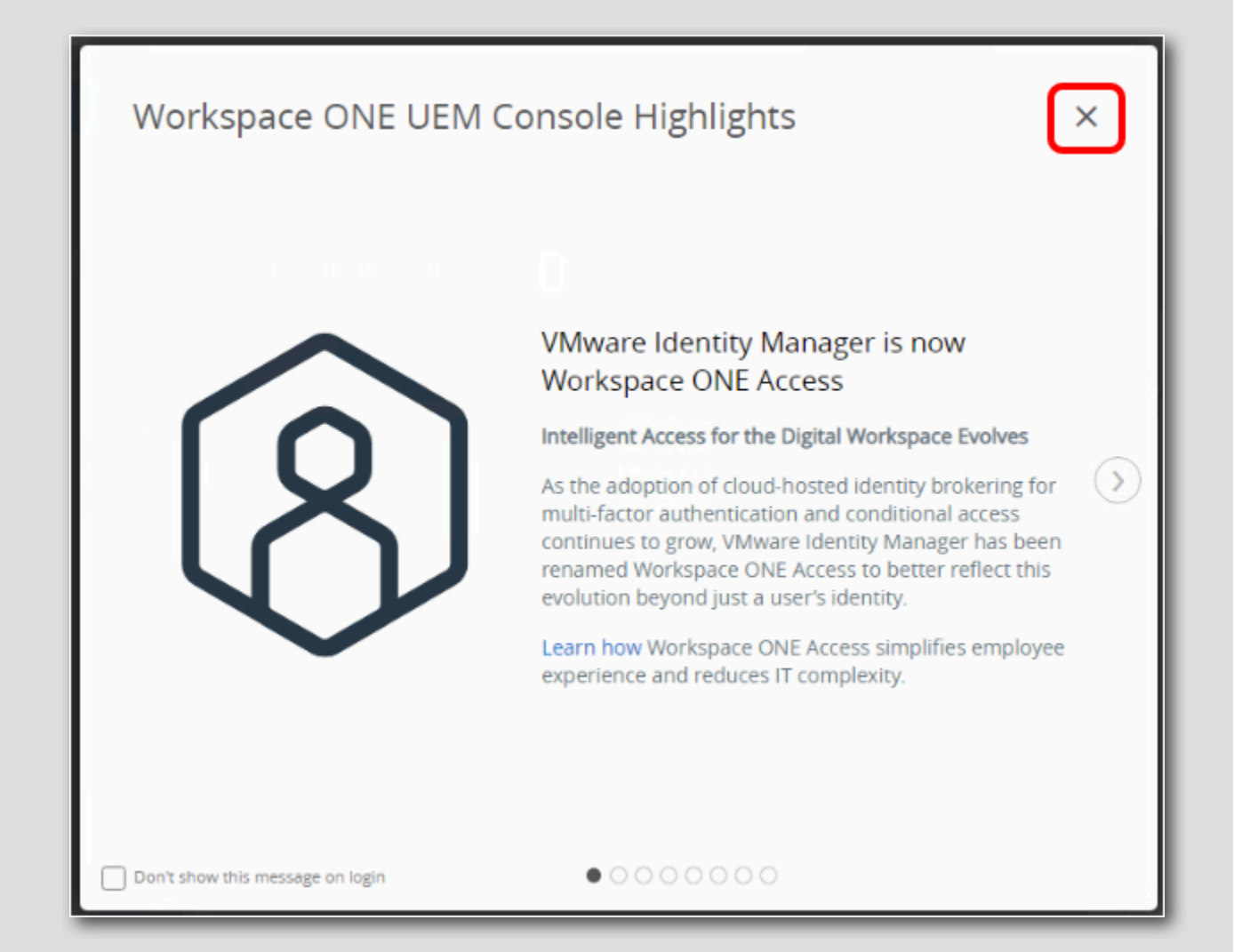

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示します。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[426]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

Workspace ONE UEM のための Android Enterprise の構成

[427]

Android のいくつかの基本機能について説明します。

Android 5.0 Lollipop デバイスで実行している場合、Android Enterprise はオペレーティング システムに組み込まれており、追加のアプリケーションは必要ありません。

Workspace ONE UEM Console 内で Android Enterprise を使用するには、会社を Google に登録しておく必要があります。これにより、Workspace ONE UEM に接続してエンタープライズ デバイスを管理する Android Enterprise 管理者アカウントが作成されます。ユーザーは、Workspace ONE UEM に登録するまで、デバイスから Android Enterprise の機能を使用できません。Android Enterprise セットアップ ウィザードは、プロセスを簡素化します。エクスペリエンスを単純化するために、この最初のプロセスはすでに実行済みです。このプロセスの詳細に関心がある場合は、Workspace ONE UEM セールス エンジニアまたは担当者に問い合わせてください。

注：Google 管理者アカウントが Workspace ONE UEM にバインドされた後は、別の組織に対してこの Google 管理者を再利用することはできません。この制限により、このラボで Workspace ONE UEM にすでにバインドされている Google 管理者アカウントを使用することはできません。

設定を開く（手順に沿って）

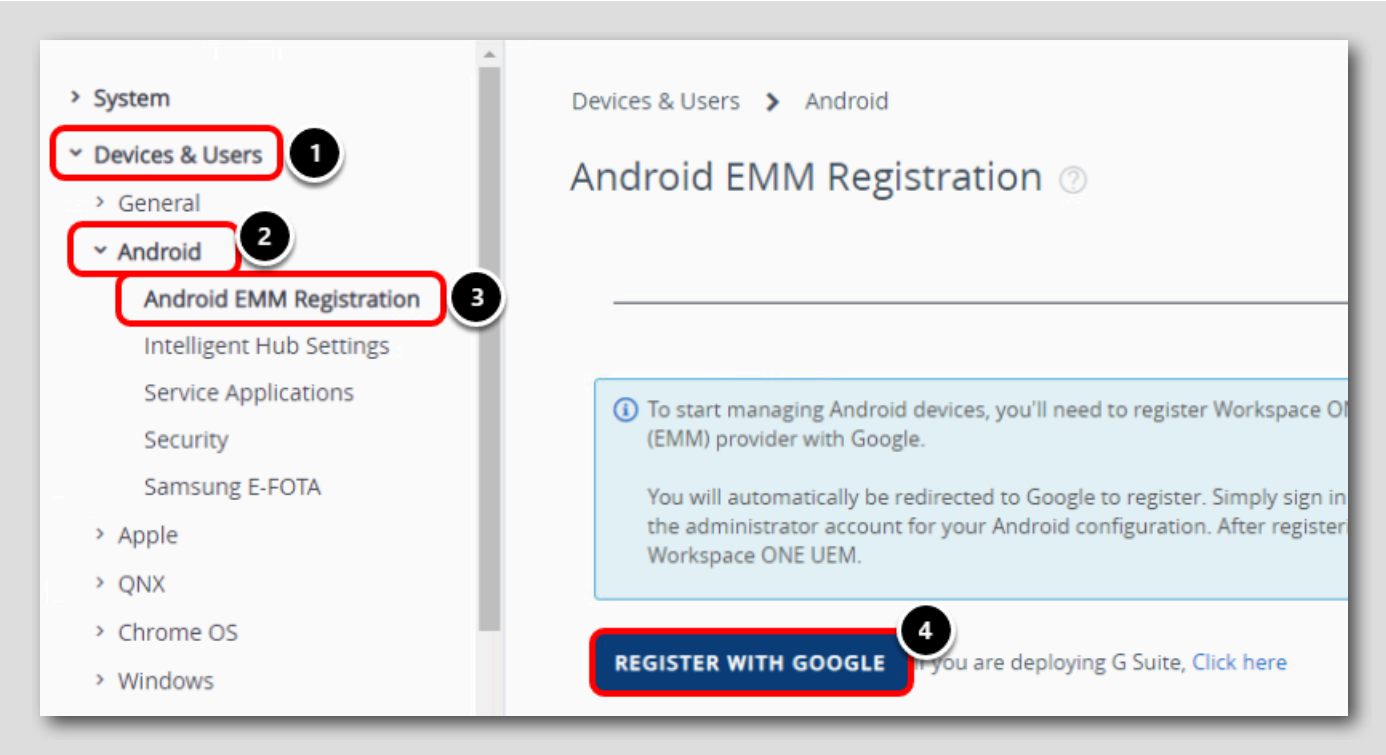
[428]

注：次の変更は、ラボの一環としてすでに構成されています。

1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

Android Enterprise 構成を開く（手順に沿って）

[429]

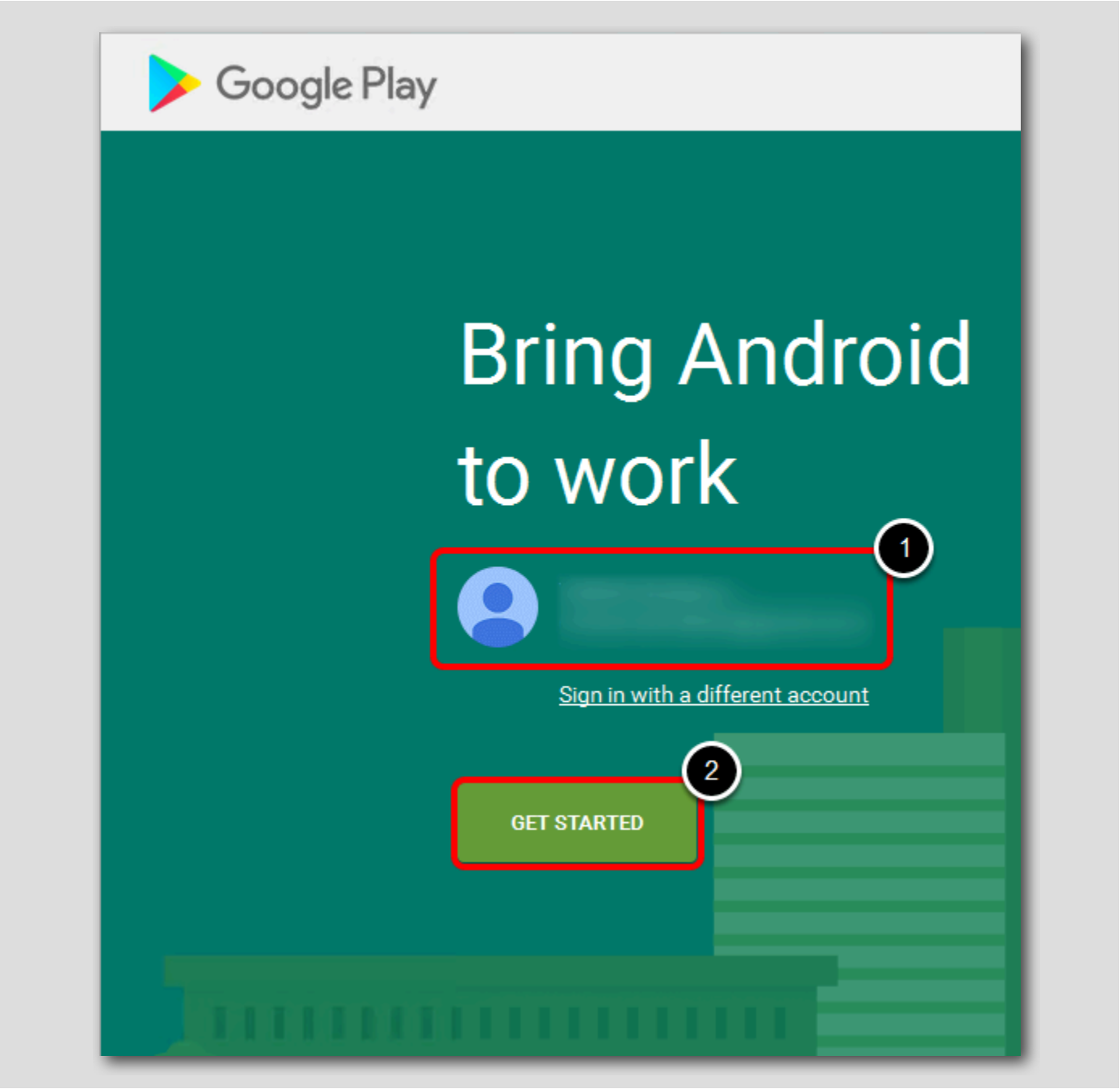


注：次の変更は、ラボの一環としてすでに構成されています。

1. [Devices & Users] をクリックします。
2. [Android] を展開します。
3. [Android EMM Enterprise] をクリックします。
4. [Register with Google] をクリックします。

Google 管理者アカウントの指定（手順に沿って）

[430]



注：次の変更は、ラボの一環としてすでに構成されています。

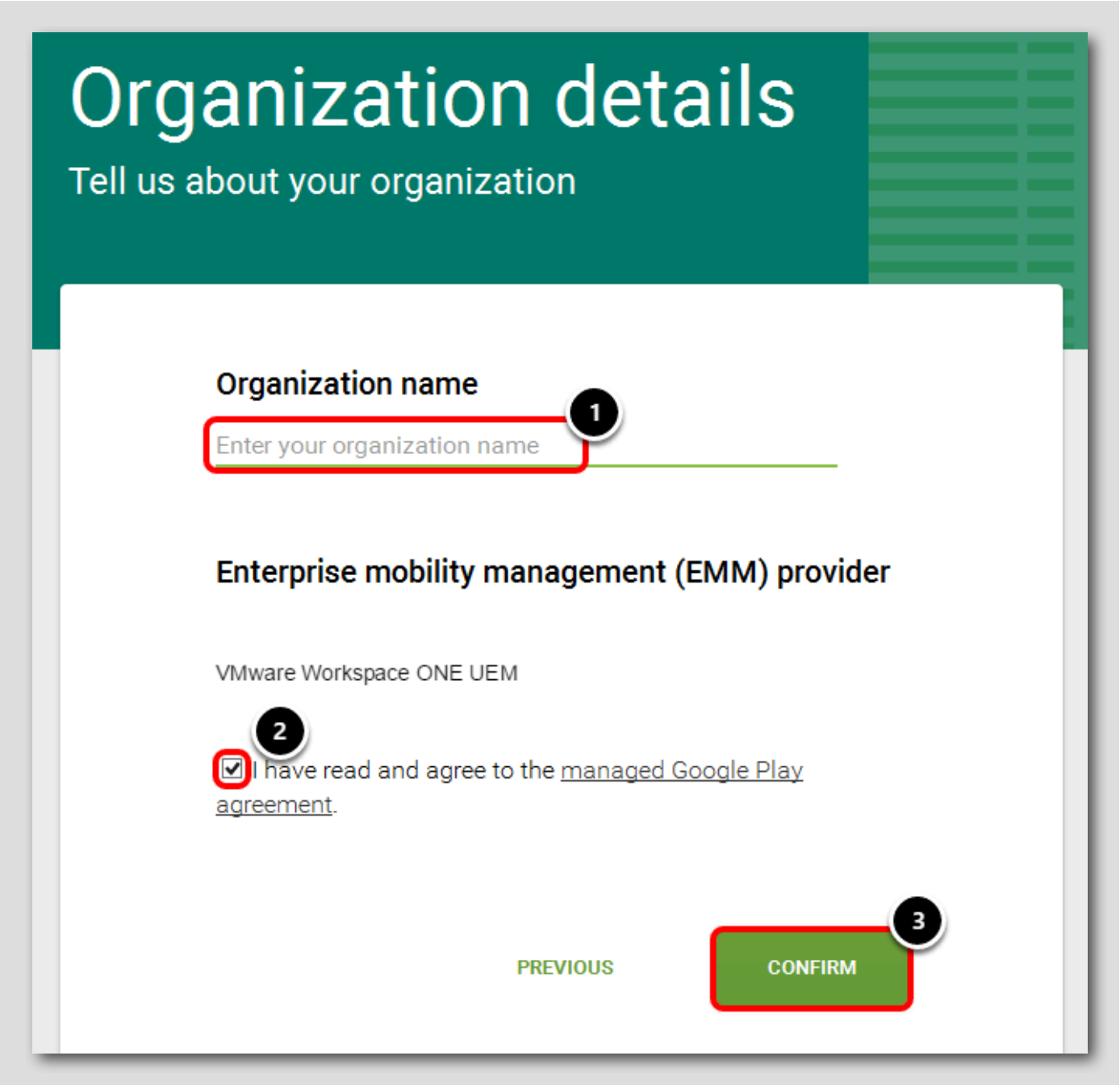
1. Android Enterprise 構成に関連付ける Google 管理者アカウントにログインしていることを確認します。

   注：Google 管理者アカウントを Android Enterprise に登録すると、その組織から Google 管理者アカウントの関連付けを解除することはできません。表示されている Google 管理者アカウントが、組織に関連付けるアカウントであることを確認します。

2. [Get Started] をクリックします。

[431]

組織の詳細の指定（手順に沿って）

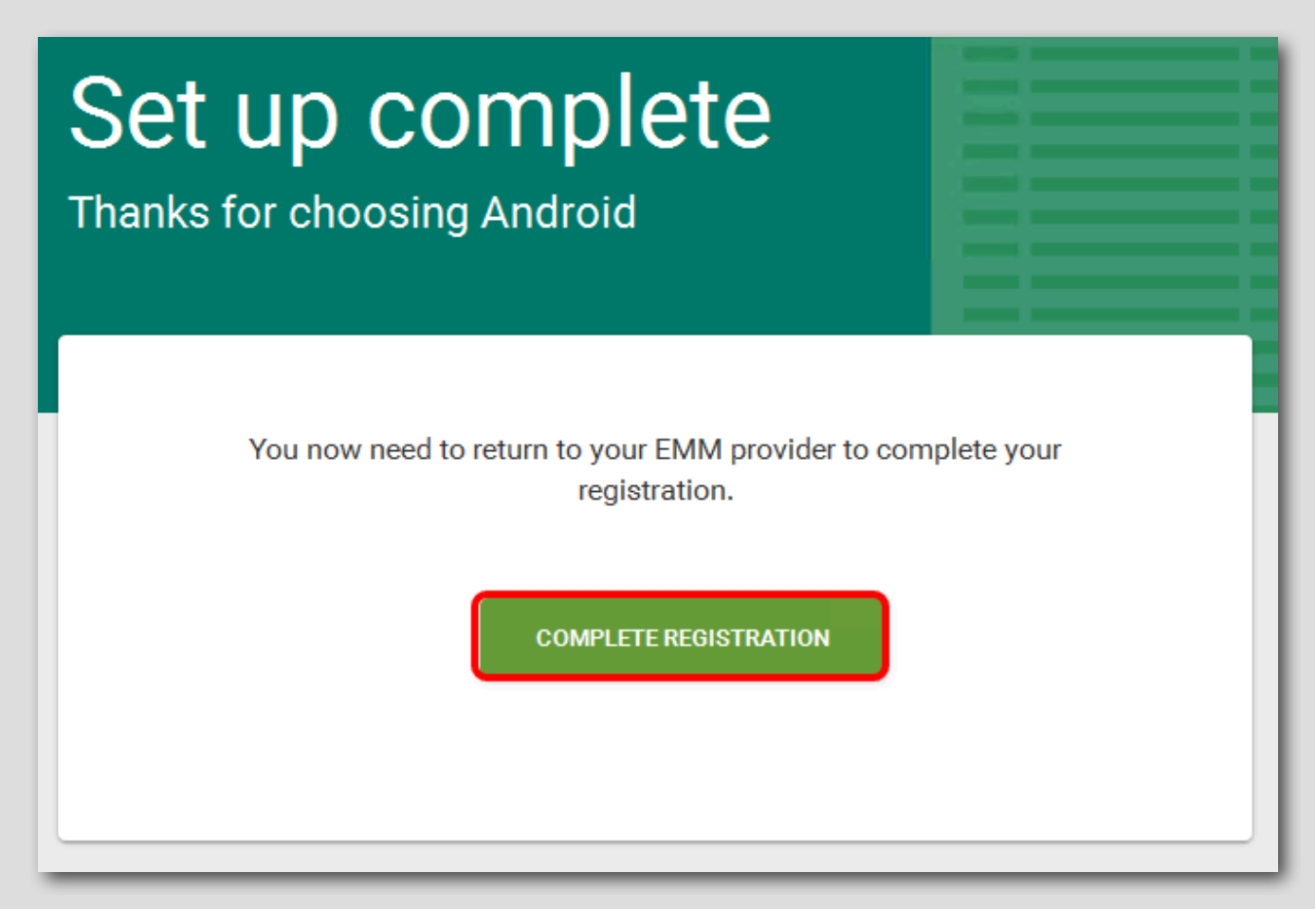


注：次の変更は、ラボの一環としてすでに構成されています。

1. [Organization Name] を入力します。
2. [Google Play Agreement] チェックボックスをオンにします。
3. [Confirm] をクリックします。

登録の完了（手順に沿って）

[432]

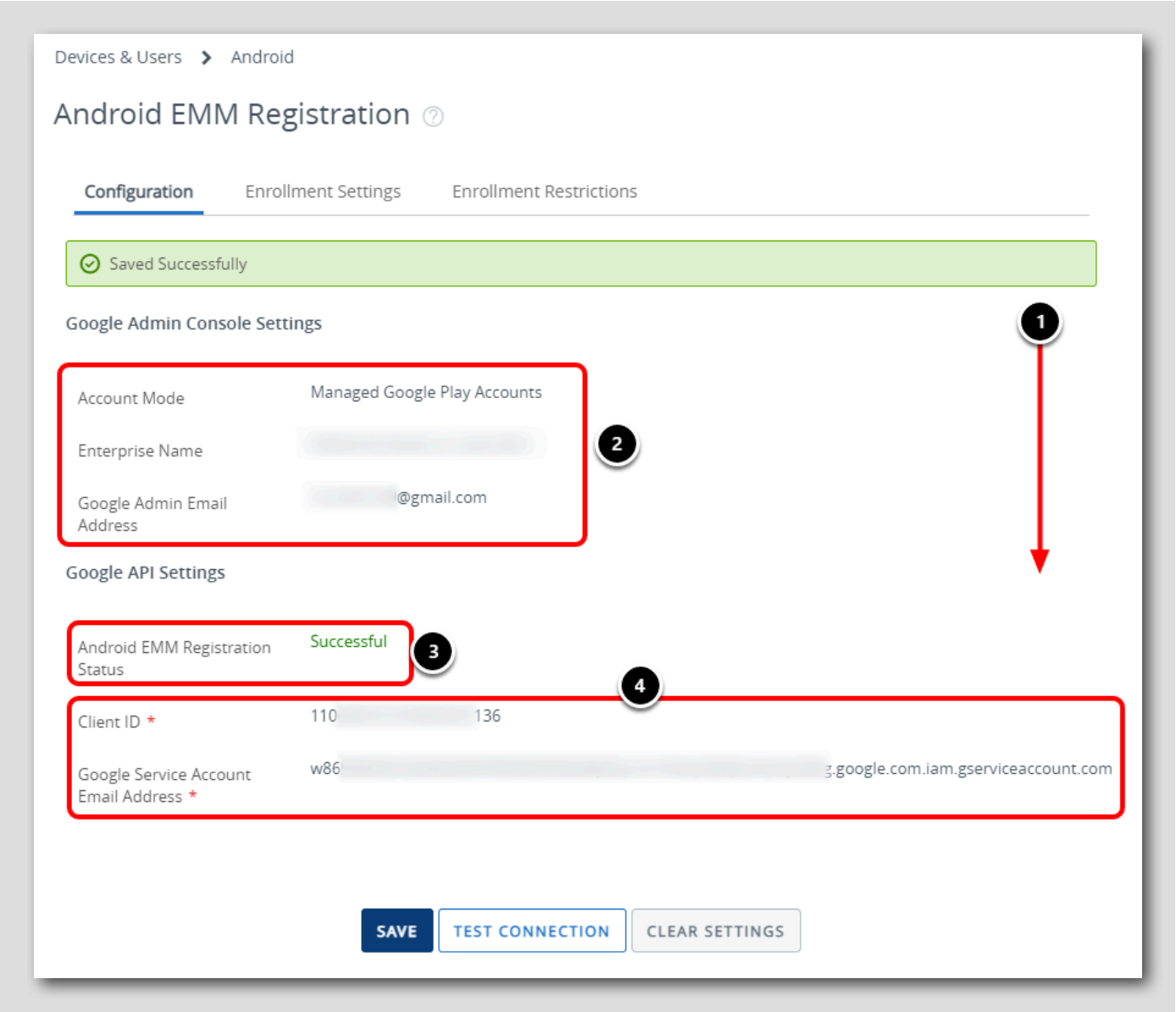


注：次の変更は、ラボの一環としてすでに構成されています。

[Complete Registration] をクリックして、Workspace ONE UEM の Android Enterprise 構成に戻ります。

[433]

Android Enterprise との統合の確認（手順に沿って）



注：次の変更は、ラボの一環としてすでに構成されています。

Workspace ONE UEM Console に戻り、次のように操作します。

1. [Android Enterprise Configuration] ページで、[Google Admin Console Settings] と [Google API Settings] のセクションが表示されるまで下にスクロールします。
2. [Google Admin Console Settings] で、Android Enterprise の構成手順で指定したアカウント情報がここに表示されていることを確認します。
3. [Android Enterprise Registration Status] に [Successful] と表示されることを確認します。
4. [Client ID] と [Google Service Account Email Address] が自動的に作成され、構成されていることを確認します。Android Enterprise または Google Developers Console では、追加の構成は必要ありません。

これで、組織グループが Android Enterprise で正常に構成されました。

Android Enterprise (Work Profile) を使用したデバイス登録

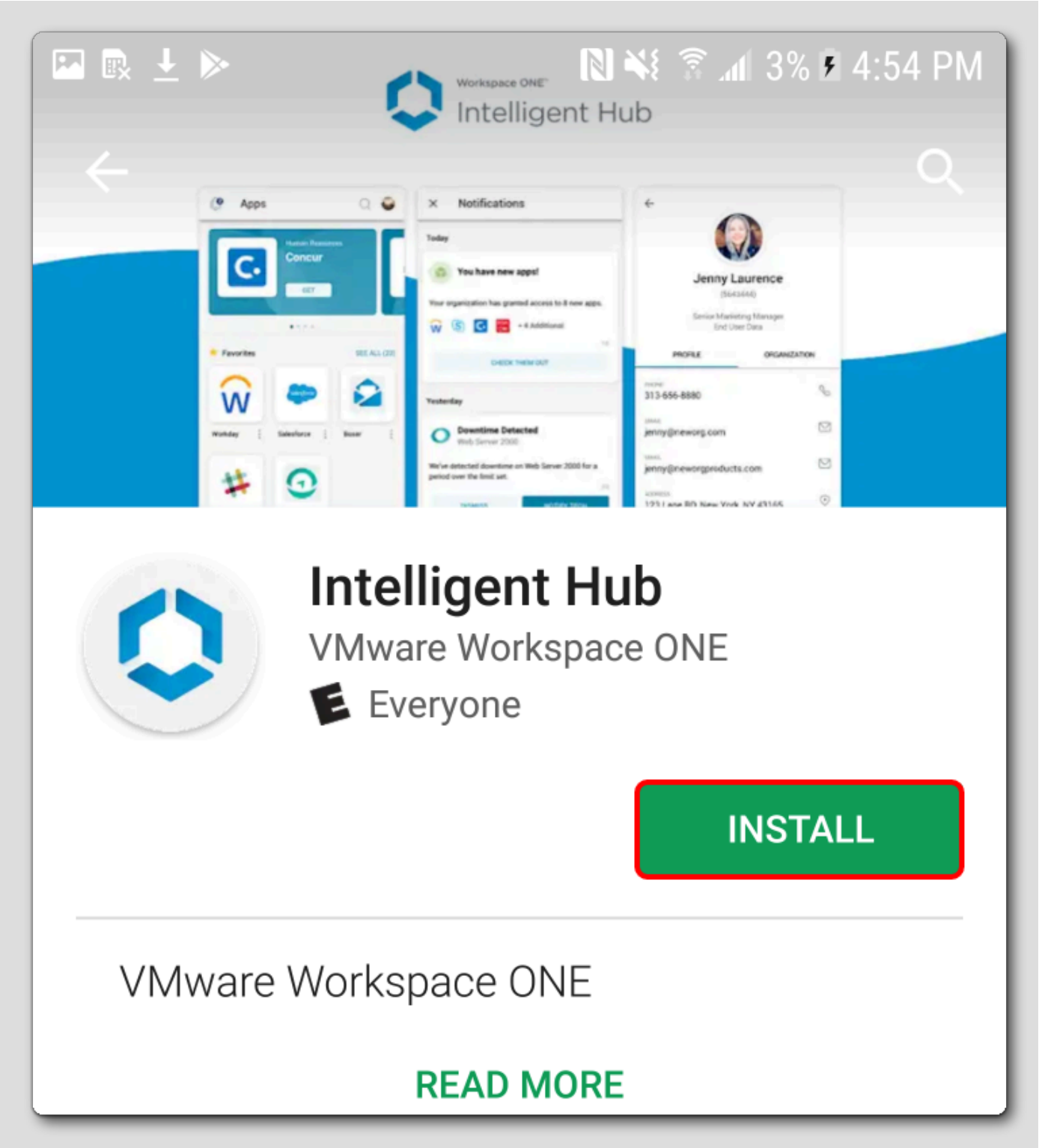
[434]

このセクションでは、デバイスを Workspace ONE UEM に登録し、Android Enterprise でセットアップします。

注：この記事のスクリーンショットは、使用している Android デバイスのメーカーとモデルによって実際とは異なる場合があります。

Workspace ONE Intelligent Hub のダウンロード（必要な場合）

[435]


3% 4:54 PM
Workspace ONE
Intelligent Hub
Apps
Notifications
Concur
Favorites
Today
You have new apps!
Yesterday
Downtime Detected
Jenny Laurence
PROFILE
ORGANIZATION
313-656-8880
jenny@neworg.com
jenny@neworgproducts.com
Intelligent Hub
VMware Workspace ONE
Everyone
INSTALL
VMware Workspace ONE
READ MORE

デバイスに Workspace ONE Intelligent Hub アプリケーションがない場合は、続行する前にアプリケーションをダウンロードする必要があります。

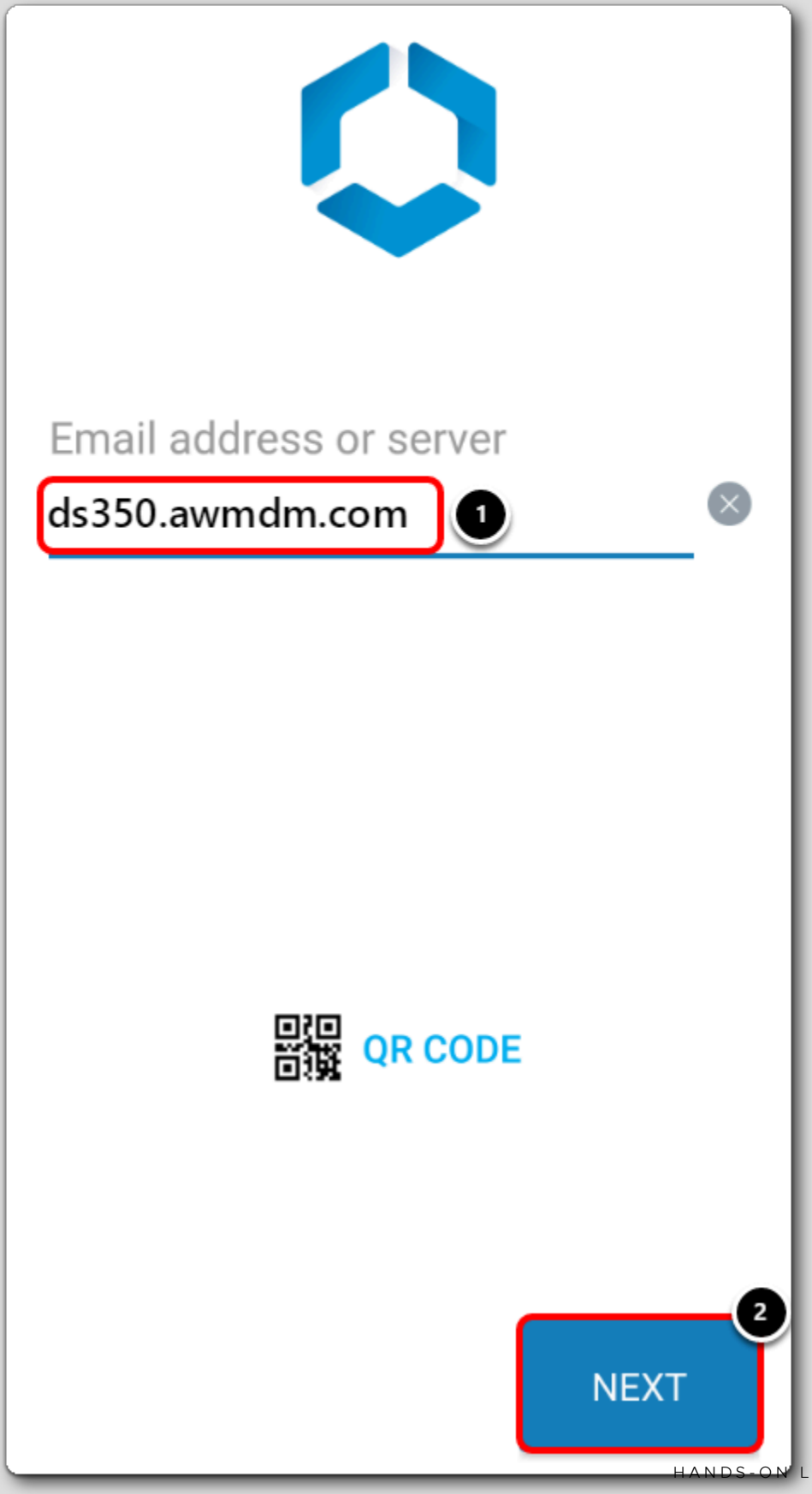
Workspace ONE Intelligent Hub アプリケーションをインストールするには、Google Play Store アプリケーションを開いて、無料の Workspace ONE Intelligent Hub アプリケーションをダウンロードします。または、デバイスのブラウザで `https://www.getwsone.com` に移動し、「Get it on Google Play」リンクに従って Google Play Store の [Workspace ONE Intelligent Hub] ページに移動します。

Workspace ONE Intelligent Hub アプリケーションの起動

[436]

デバイス上で Hub アプリケーションを起動します。

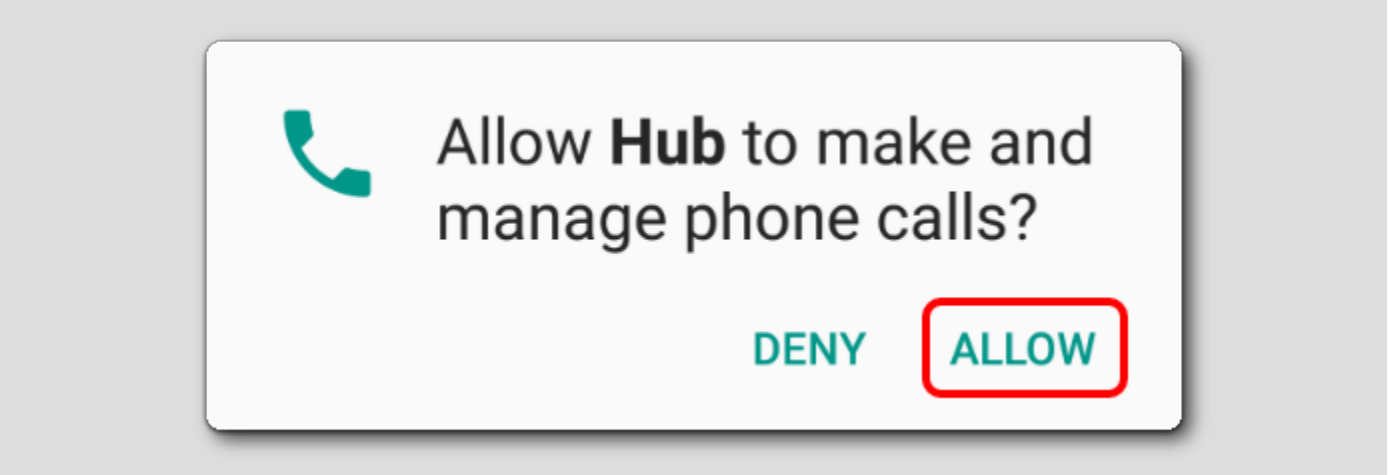
Workspace ONE UEM サーバ URL の指定


Email address or server
ds350.awmdm.com
1
QR CODE
2
NEXT

1. [Server URL] に **`ds350.awmdm.com`** と入力します。
2. [NEXT] をタップします。

Hub の通話権限を許可（必要な場合）

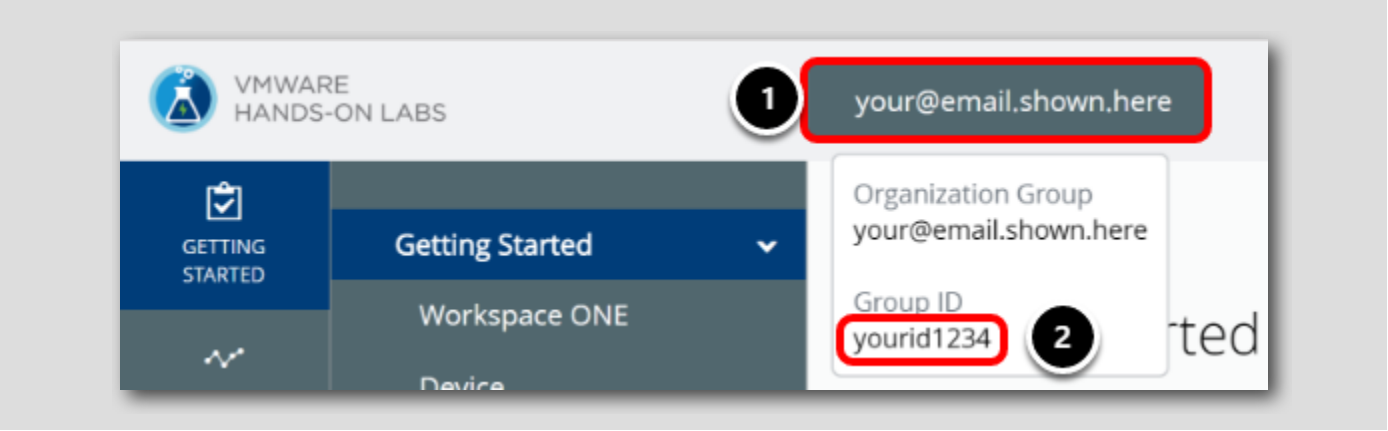
[438]



[Allow] をタップします。

Workspace ONE UEM Console からのグループ ID の検索

[439]

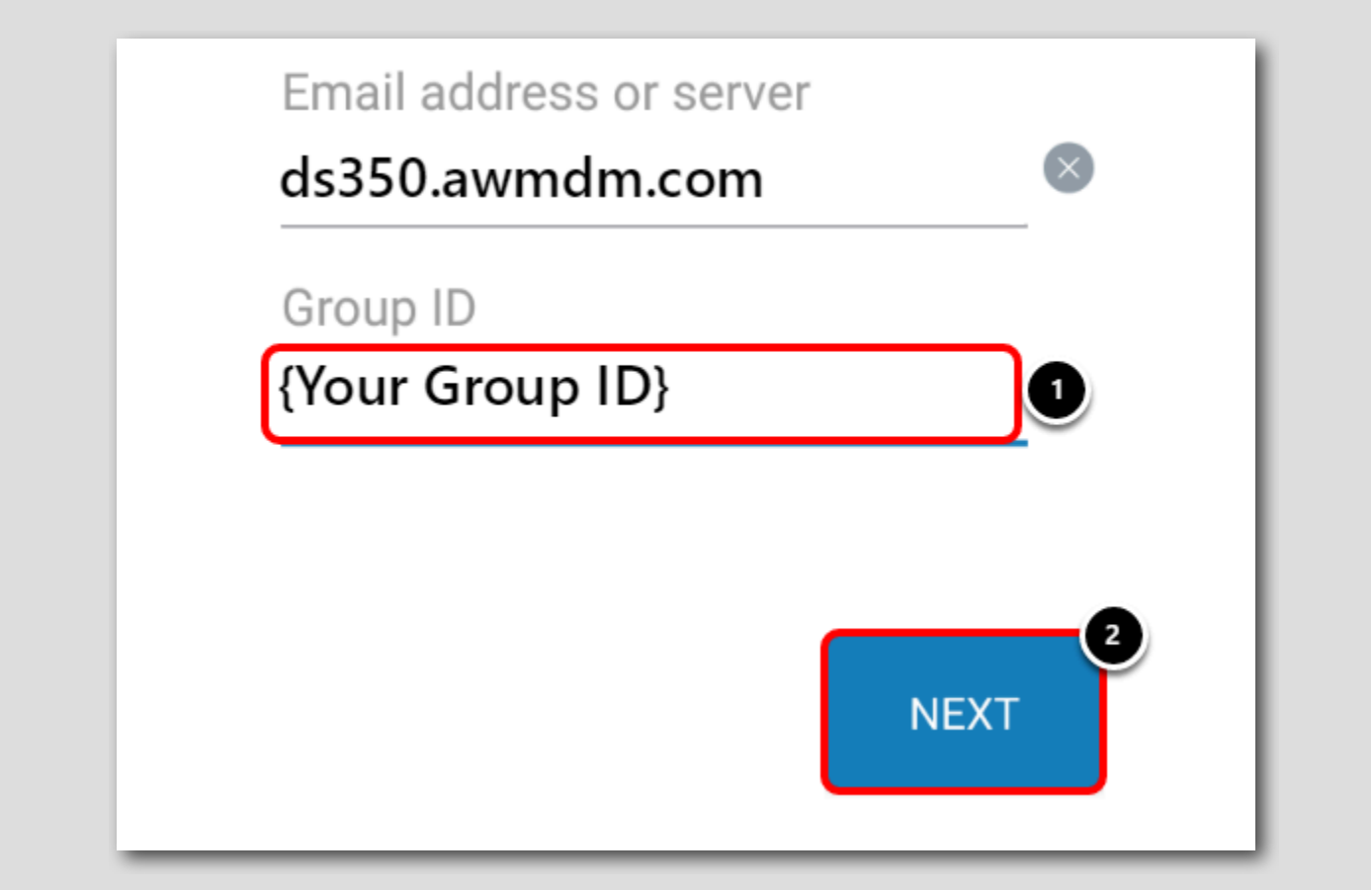


次に、**組織グループ ID** を確認します。

1. グループ ID を確認するには、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. **グループ ID** は [Organization Group] ポップアップの最下部に表示されます。

HOL サンドボックスへの Workspace ONE Intelligent Hub の接続

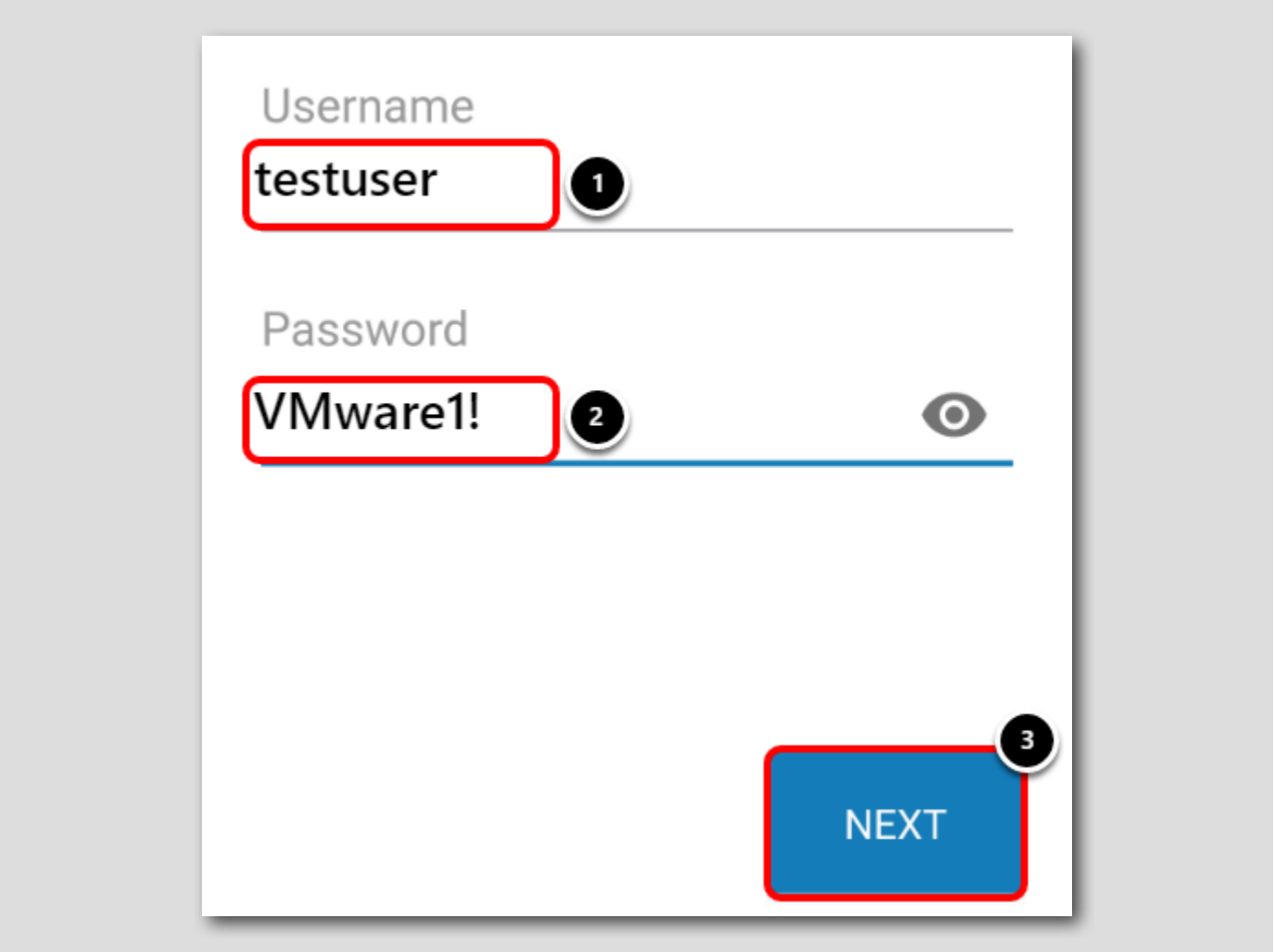
[440]



1. [Group ID] フィールドにグループ ID を入力します。これは、前述の「グループ ID の確認」の手順に記載されています。
2. [NEXT] をタップします。

ユーザー認証情報の指定

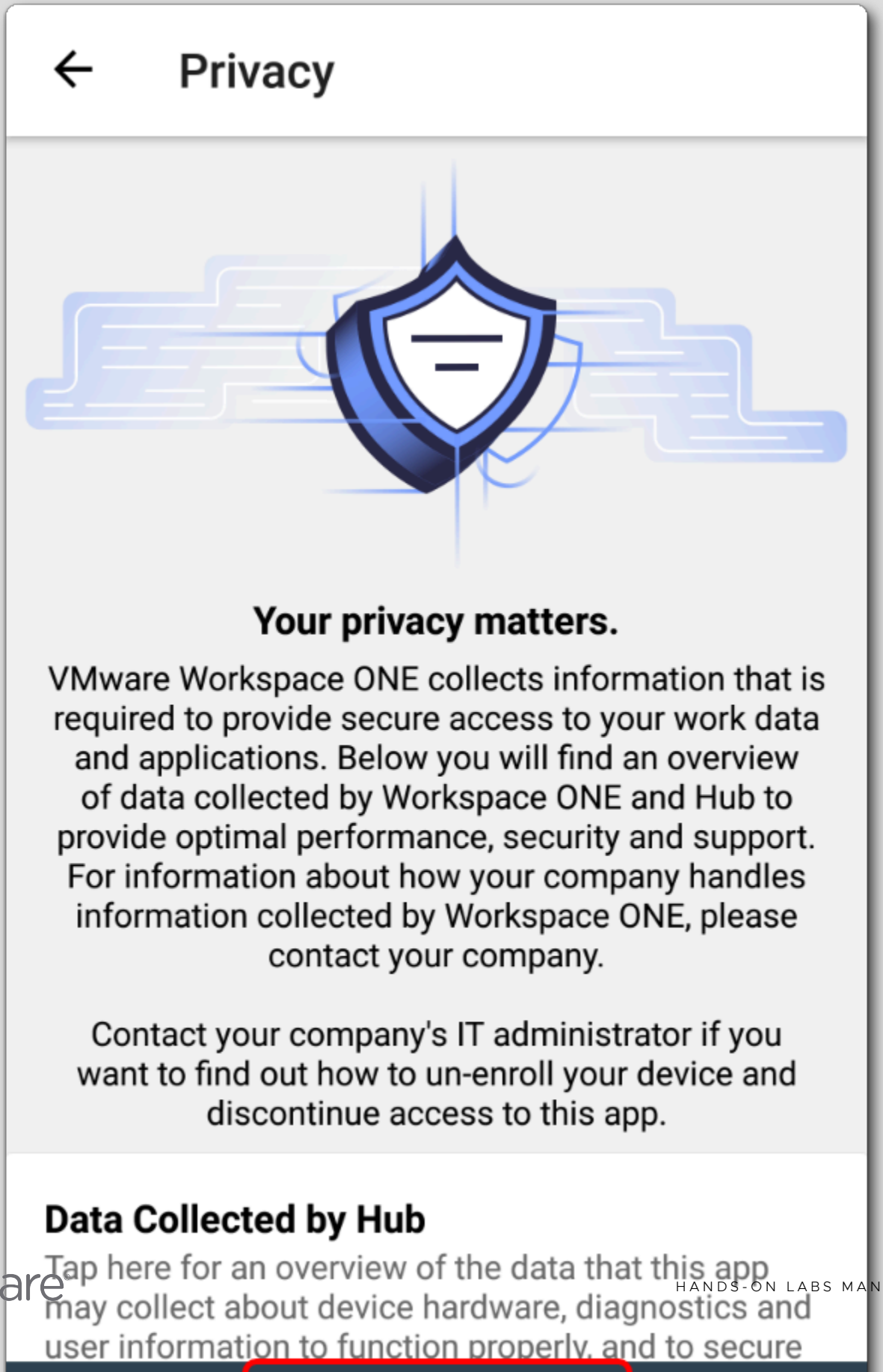
[441]



1. [Username] フィールドに **testuser** と入力します。
2. [Password] フィールドに **VMware1!** と入力します。
3. [Continue] をタップします。

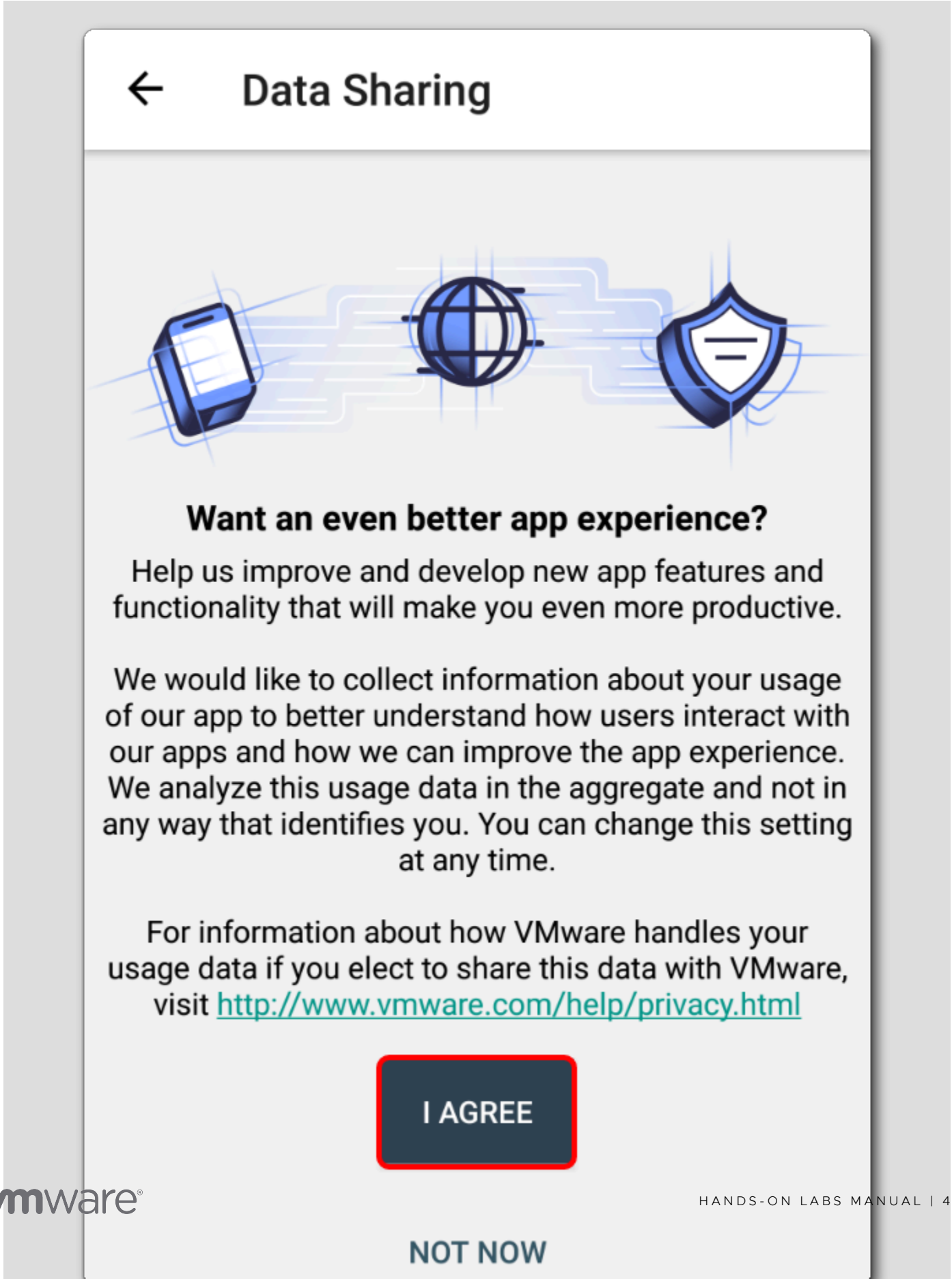
[442]

プライバシー ポリシーの確認


Privacy
Your privacy matters.
VMware Workspace ONE collects information that is required to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.
Contact your company's IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.
Data Collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure

プライバシー ポリシーを読み、[I Understand] をタップします。

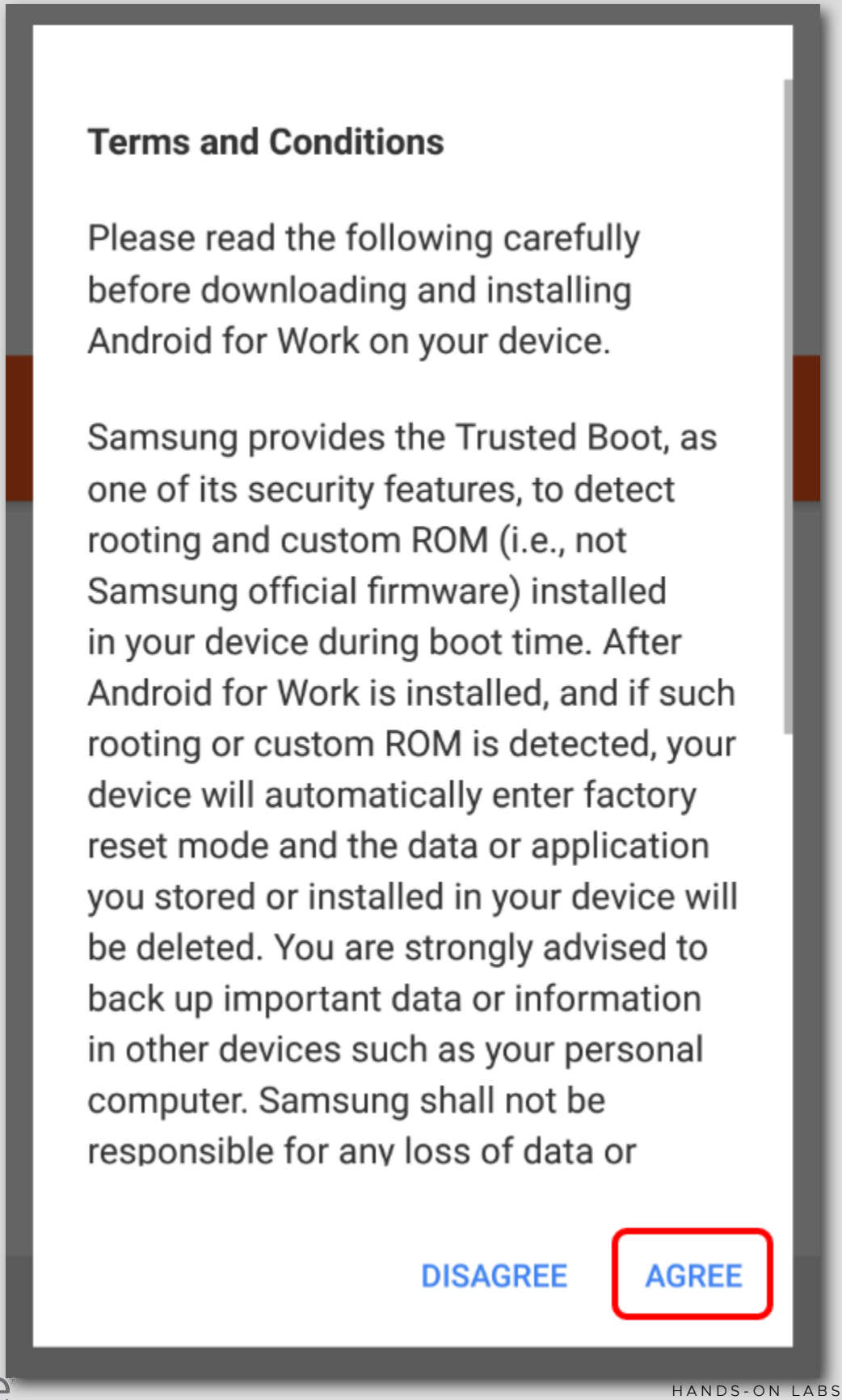
データ共有ポリシーの承諾


Data Sharing
Want an even better app experience?
Help us improve and develop new app features and functionality that will make you even more productive.
We would like to collect information about your usage of our app to better understand how users interact with our apps and how we can improve the app experience. We analyze this usage data in the aggregate and not in any way that identifies you. You can change this setting at any time.
For information about how VMware handles your usage data if you elect to share this data with VMware, visit http://www.vmware.com/help/privacy.html
I AGREE
NOT NOW

データ共有ポリシーに対して **[I Agree]** をタップします。

[444]

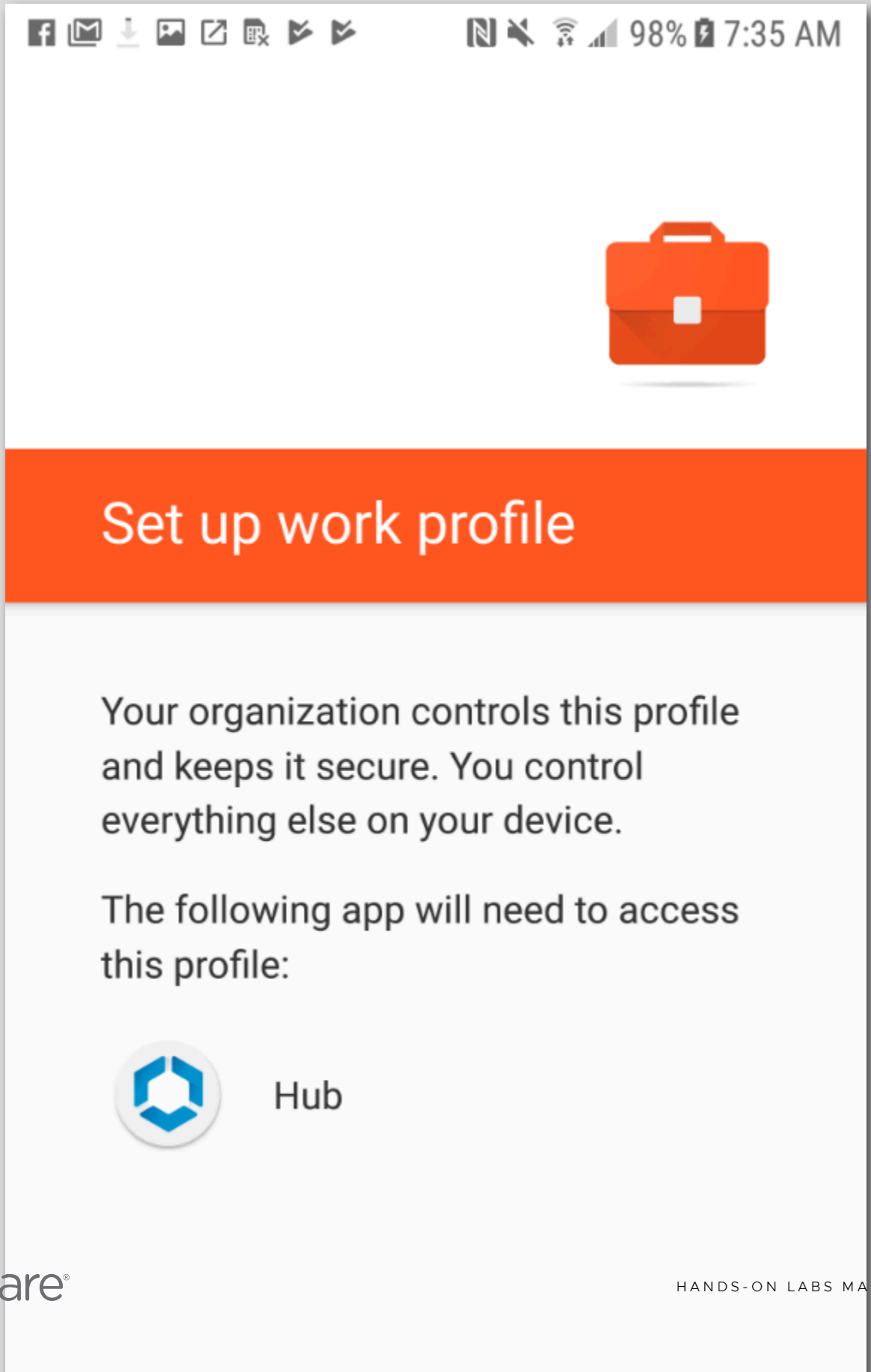
利用条件への同意


Terms and Conditions
Please read the following carefully before downloading and installing Android for Work on your device.
Samsung provides the Trusted Boot, as one of its security features, to detect rooting and custom ROM (i.e., not Samsung official firmware) installed in your device during boot time. After Android for Work is installed, and if such rooting or custom ROM is detected, your device will automatically enter factory reset mode and the data or application you stored or installed in your device will be deleted. You are strongly advised to back up important data or information in other devices such as your personal computer. Samsung shall not be responsible for any loss of data or
DISAGREE
AGREE

[Agree] をタップします。

Android Enterprise 仕事用プロファイルの設定

[445]

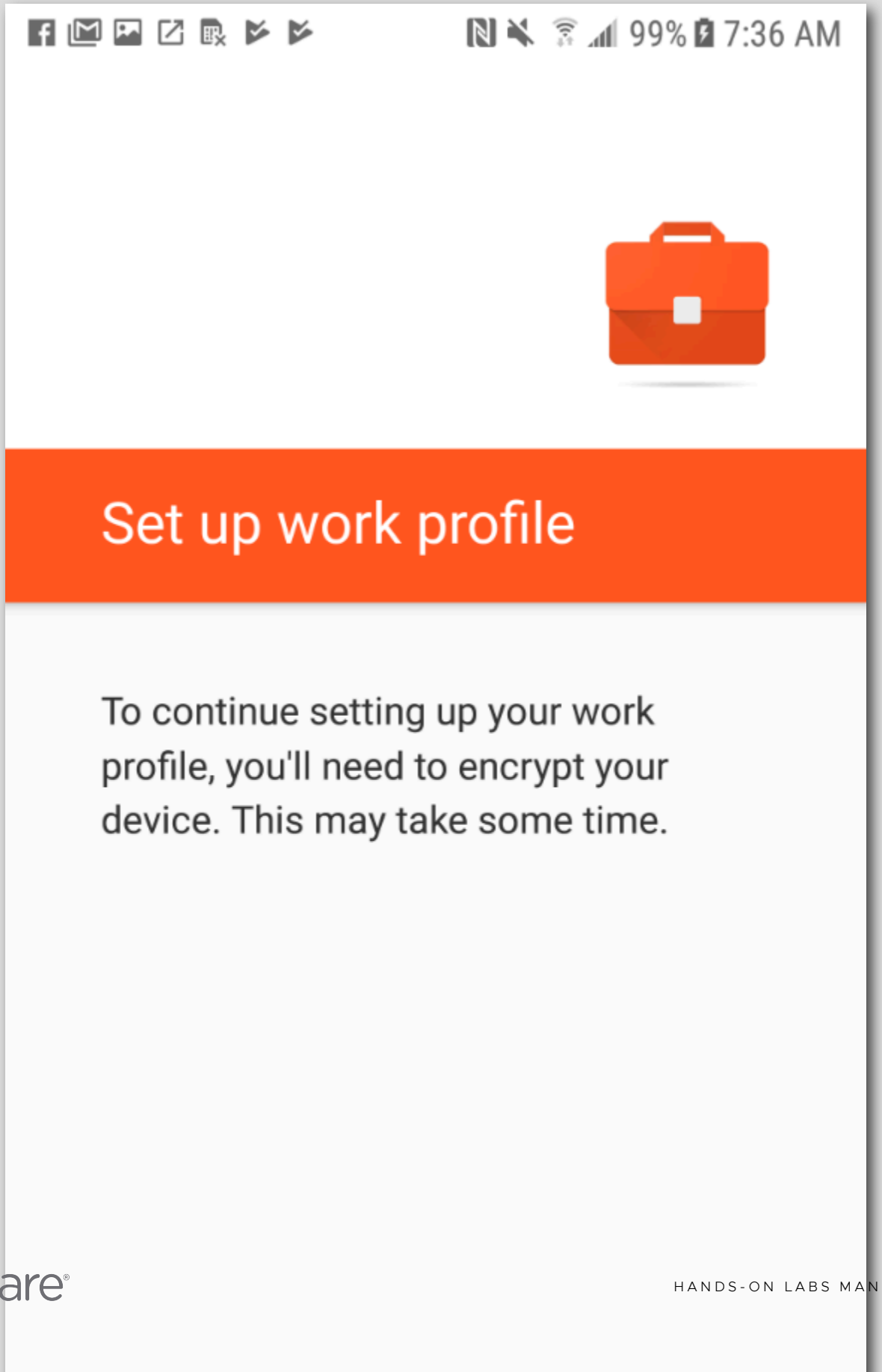

98% 7:35 AM
Set up work profile
Your organization controls this profile and keeps it secure. You control everything else on your device.
The following app will need to access this profile:
Hub

[NEXT] をタップします。

注：これには時間がかかることがあります。セットアップ プロセスが完了するまでしばらくお待ちください。

[446]

（オプション）デバイス暗号化

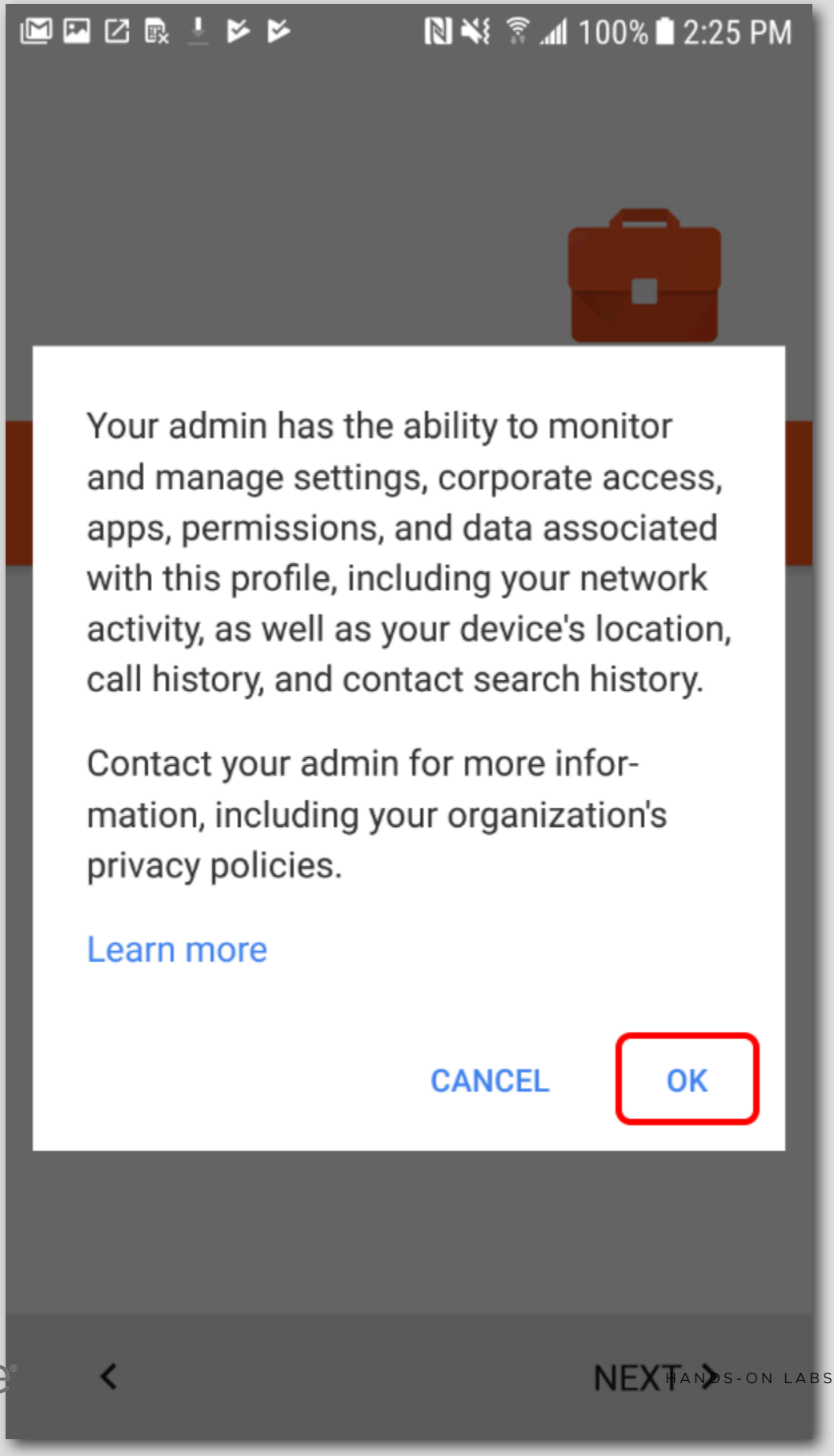

99% 7:36 AM
Set up work profile
To continue setting up your work profile, you'll need to encrypt your device. This may take some time.

デバイスが暗号化されている場合、このページは表示されず、次の手順に進むことができます。

デバイスが暗号化されていない場合は、暗号化を求めるプロンプトが表示されます。続行するには、[ENCRYPT] をタップする必要があります。デバイス上のデータ量によっては、デバイスの暗号化に数分またはそれ以上長くかかる場合があります。

[447]

管理者権限


100% 2:25 PM
Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, and data associated with this profile, including your network activity, as well as your device's location, call history, and contact search history.
Contact your admin for more information, including your organization's privacy policies.
Learn more
CANCEL
OK
NEXT

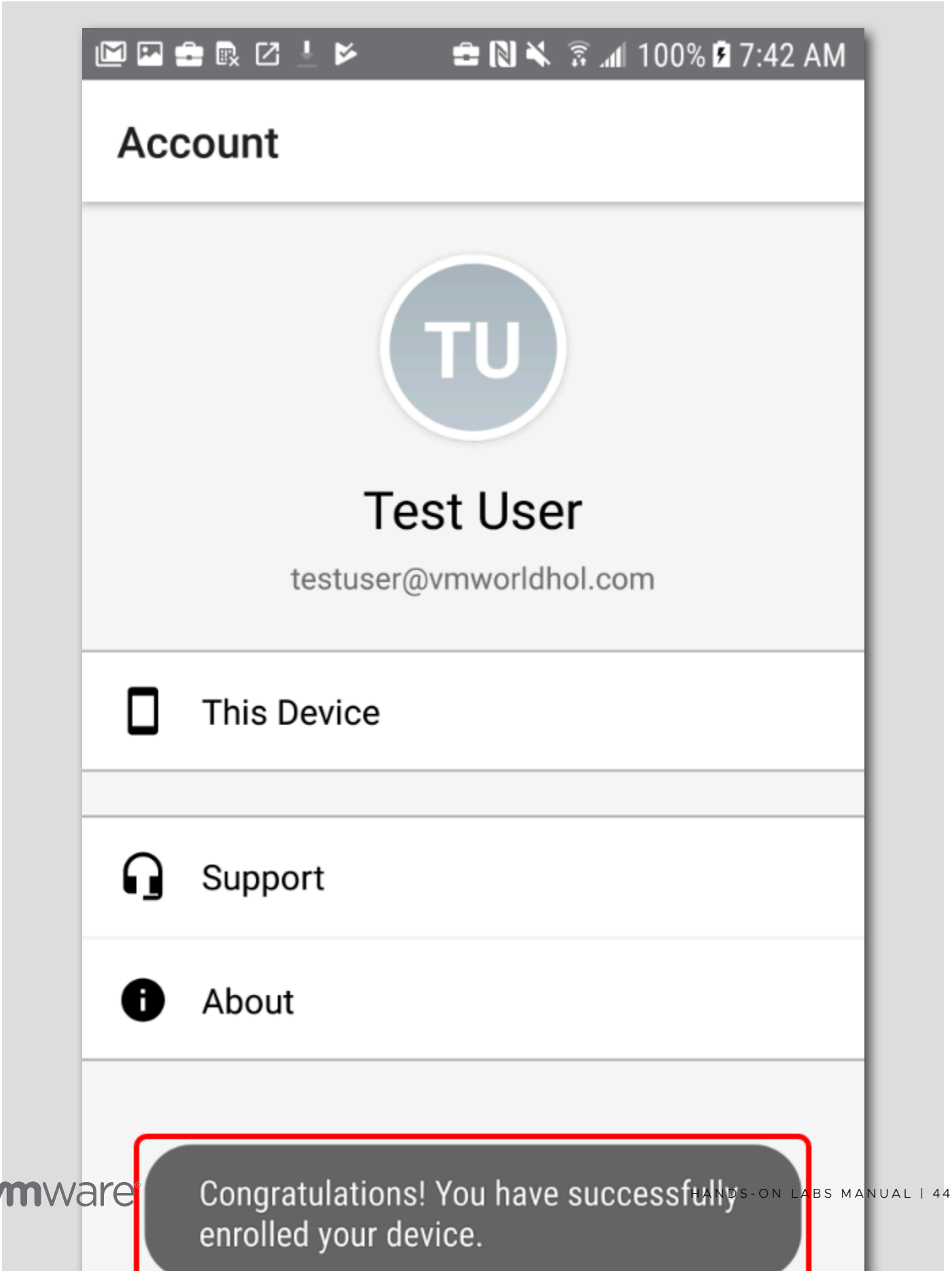
[OK] をタップして、プライバシー ポリシーを確認します。

注：登録時間は、ネットワーク接続によって異なります。通常は、完了までに約 1 分かかります。このプロセスが完了するまでしばらくお待ちください。

重要：登録プロセス中には、いくつかの処理画面が表示されます。Workspace ONE Intelligent Hub アプリケーションが登録を確認する（次のページ）まで、デバイスを操作する必要はありません。

デバイス登録の確認

[448]

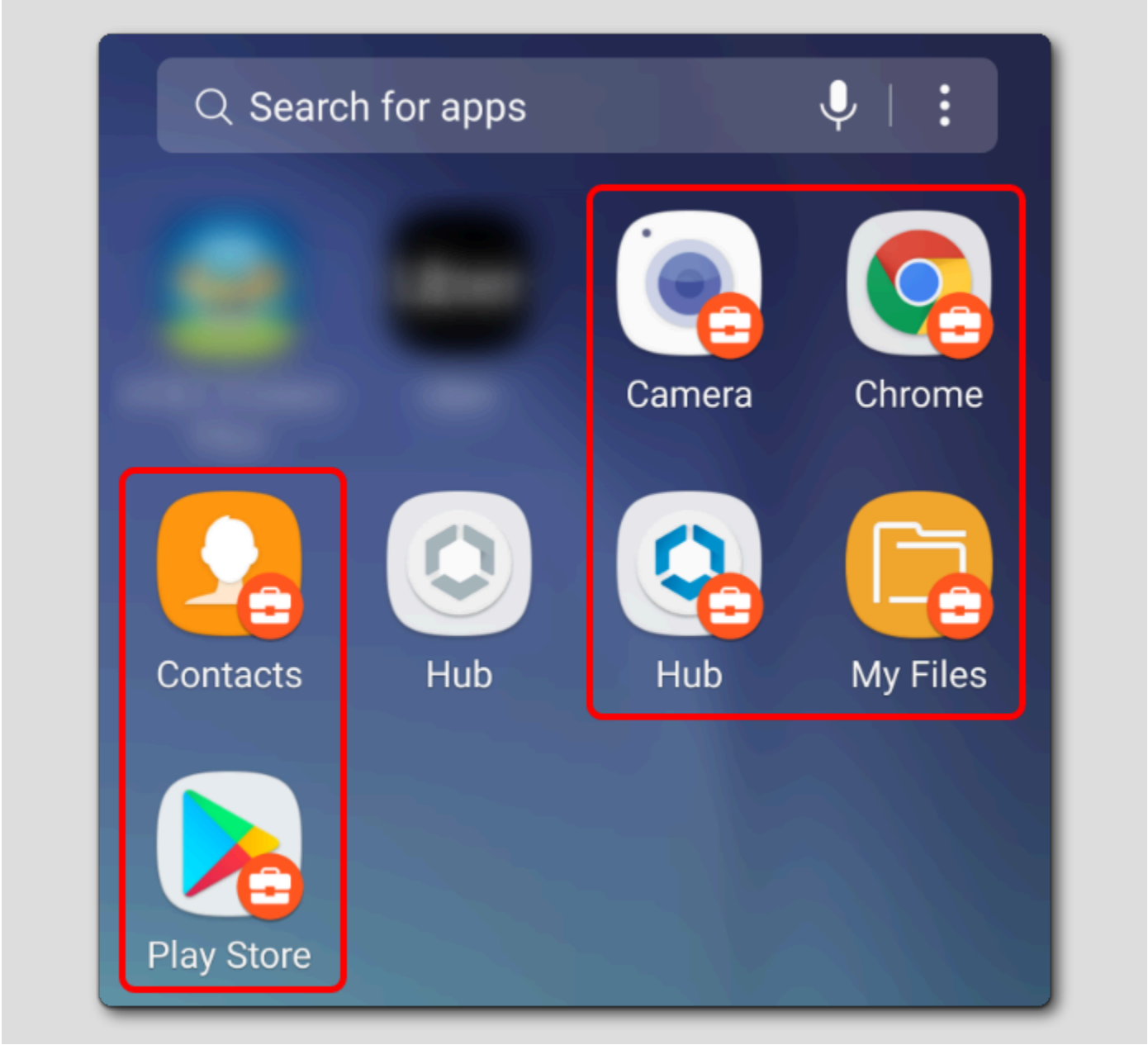

100% 7:42 AM
Account
TU
Test User
testuser@vmworldhol.com
This Device
Support
About
Congratulations! You have successfully enrolled your device.

これで、Workspace ONE Intelligent Hub を使用したデバイスの登録が完了しました。登録プロセスが完了すると、Workspace ONE Intelligent Hub アプリケーションに「Congratulations! You have successfully enrolled your device.」という通知が表示されます。

これで、Workspace ONE Intelligent Hub アプリケーションを終了できるようになりました。

バッジ付きアプリケーション

[449]



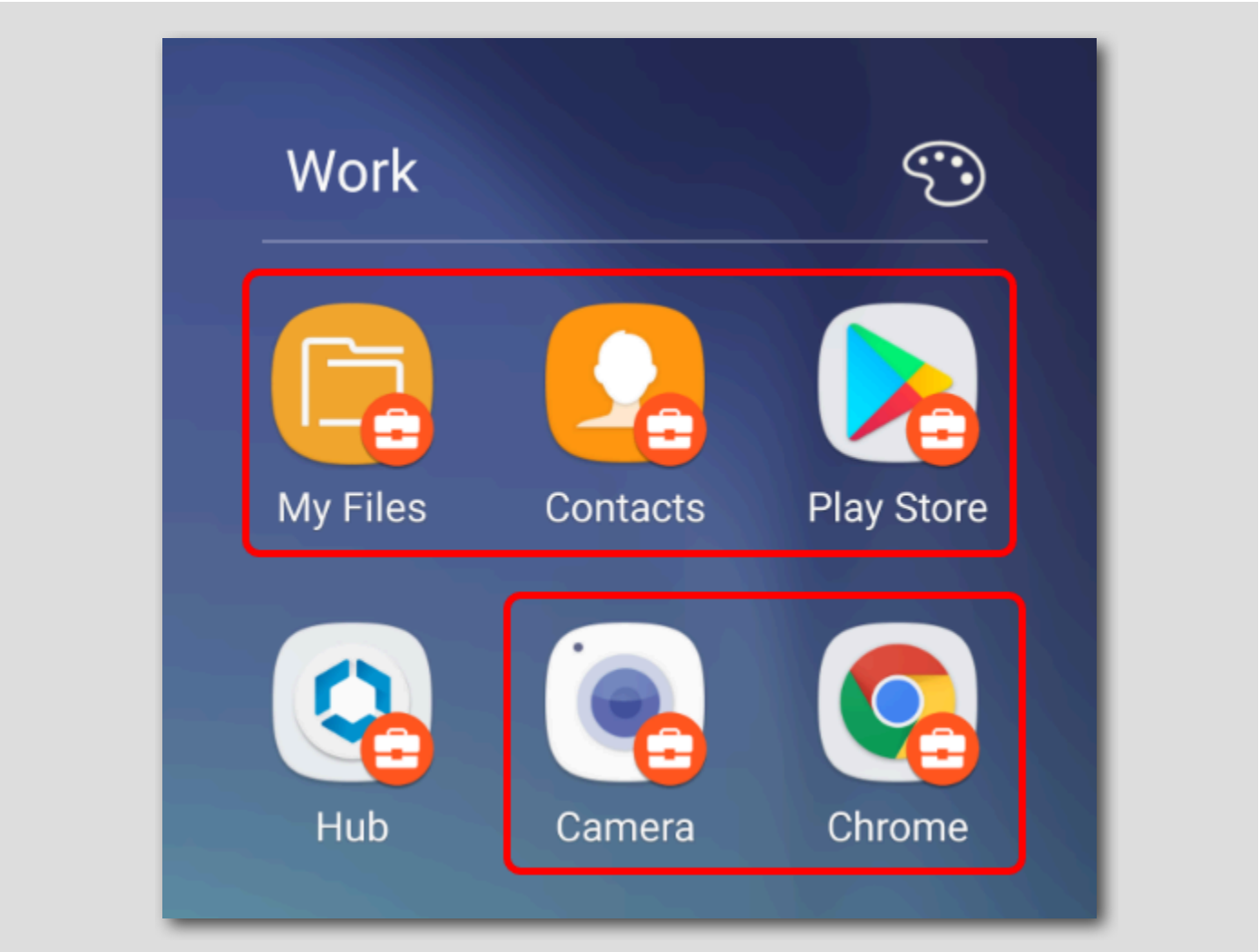
現在、Android デバイスに新しい仕事用アプリケーションが表示されているはずです。Android Enterprise アプリケーションは、バッジ付きアプリケーションとも呼ばれ、オレンジ色のブリーフケース アイコンによって区別されます。

[Applications] ビューでは、仕事用アプリケーションと個人用アプリケーションが統合されたランチャーで表示されます。たとえば、Google Chrome の個人アイコンと、バッジで示される Work Chrome の個別のアイコンの両方がデバイスに表示されます。Workspace ONE Intelligent Hub はバッジ付きで、仕事用プロファイル データ領域内のみに存在します。

重要：個人用アプリケーションに対する制御はなく、Hub アプリケーションは個人情報にアクセスできません。「Work Chrome」、「Google Play」、「Google 設定」、「連絡先」、「カメラ」など、デフォルトで仕事用プロファイルに含まれているいくつかのシステム アプリケーションがあります。

Work コンテナ

[450]



OS のバージョンによっては、一部のデバイスに Work コンテナが表示されることがあります。この Work コンテナを使用して、仕事用（バッジ付き）アプリケーションに素早くアクセスできます。

Android Enterprise プロファイル

[451]

このセクションでは、Android Enterprise プロファイルを作成して、デバイスの制限を変更し、機密データの保護を支援します。プロファイルは、企業のルールや手順を適用することから、Android Enterprise 対応デバイスを使用方法に合わせて調整および準備することまで、さまざまな目的に役立ちます。

重要：デバイスが Android Enterprise に登録されている場合、デバイスでは Android Enterprise プロファイルのみが有効になり、Android デバイス プロファイルは有効になりません。

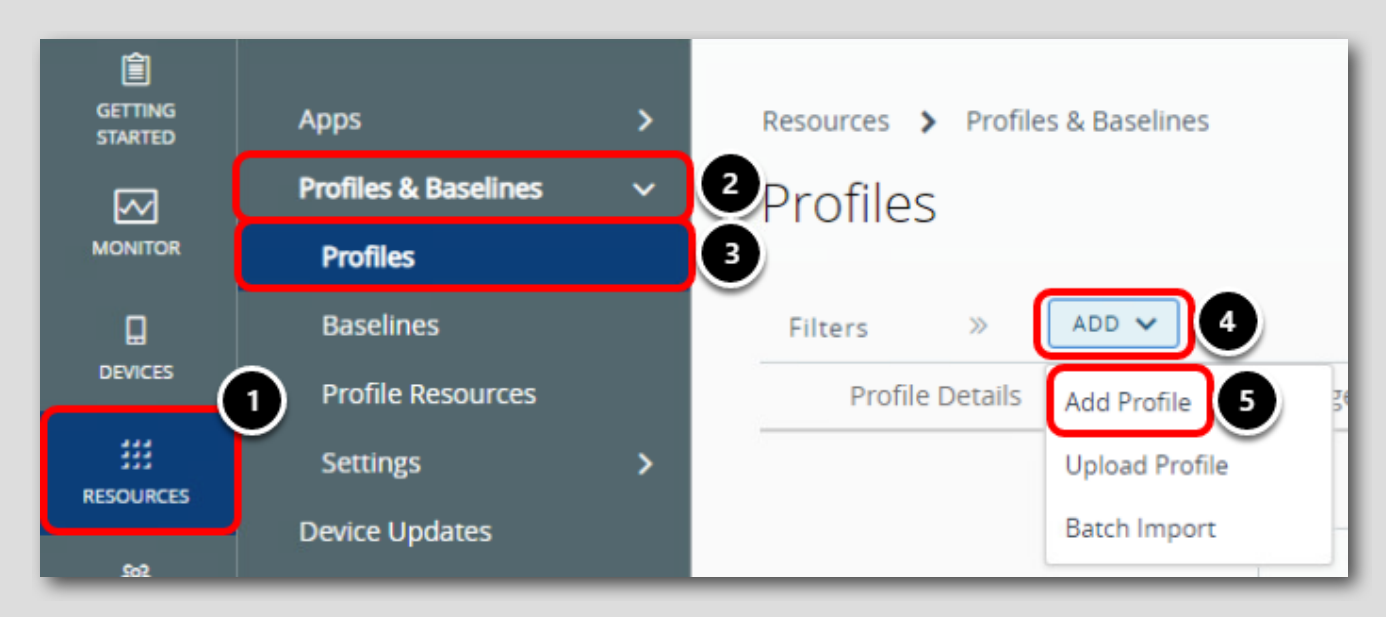
制限事項プロファイルの概要

[452]

制限事項プロファイルを使用すると、従業員がいつどこで、どのようにデバイスを使用するかを指定して制御できるようになり、デバイスのデータを保護する 2 つ目のレイヤーが提供されます。制限事項プロファイルは Android Enterprise デバイスのネイティブ機能をロックします。これはデバイスの登録によって異なります。

新しいプロファイルの作成

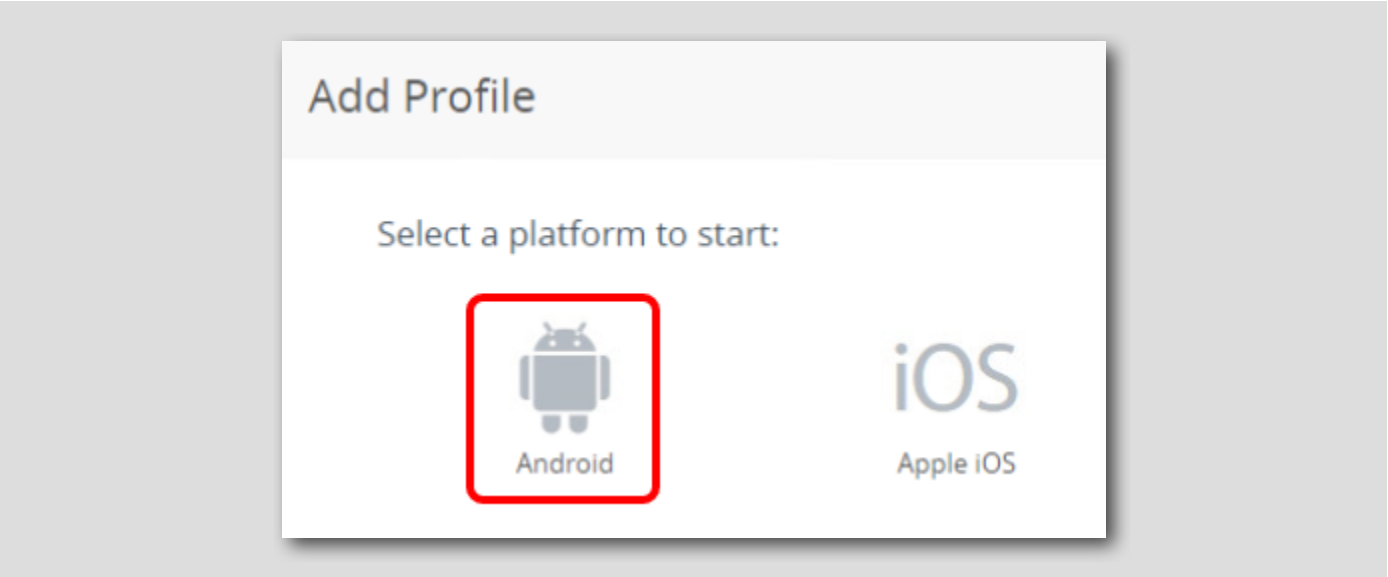
[453]



Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Profiles & Baselines] セクションを展開します。
3. [Profiles] をクリックします。
4. [Add] をクリックします。
5. [Add Profile] をクリックします。

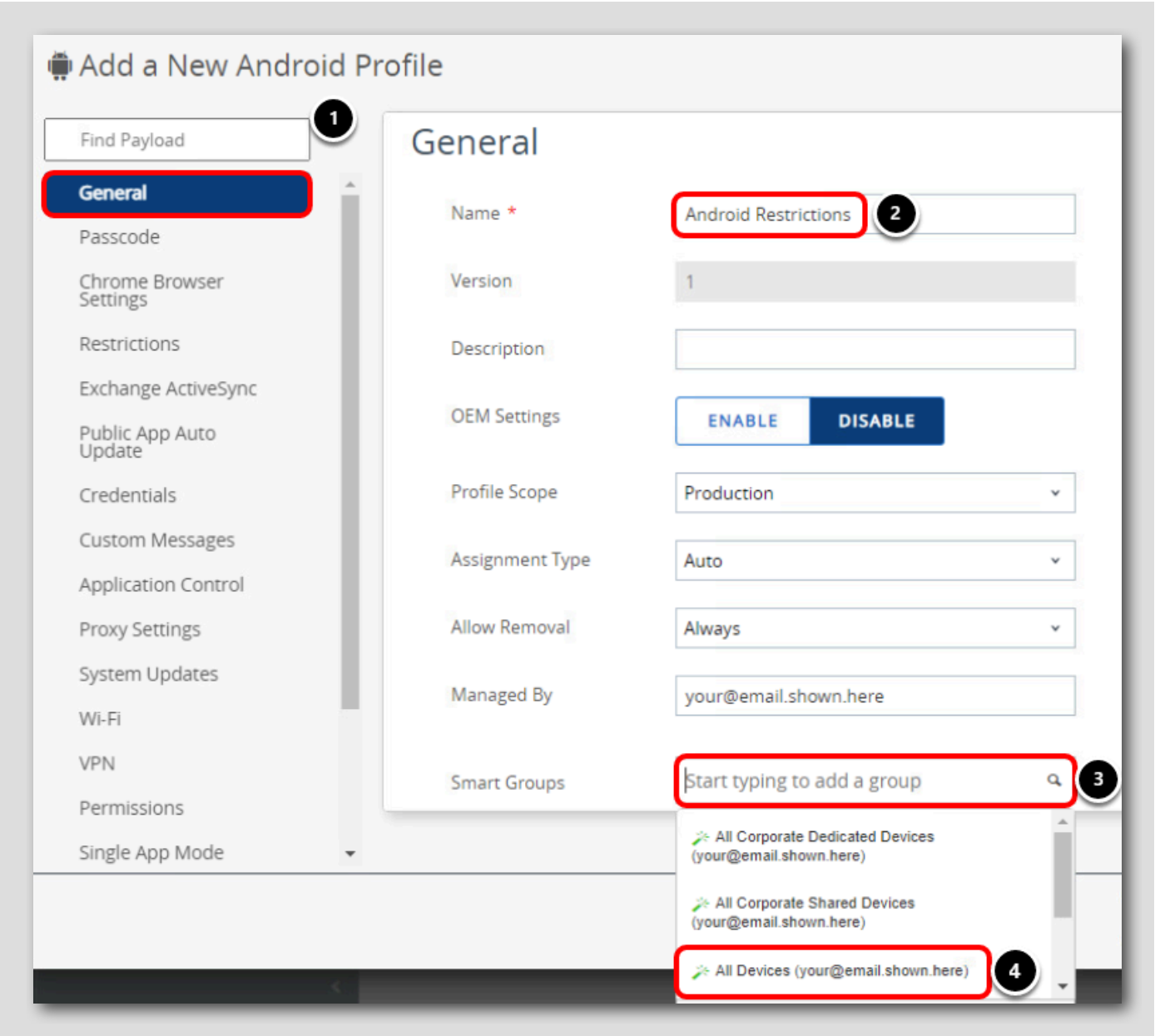
Android プラットフォームの選択 [454]



[Android] をクリックします。

全般設定の構成

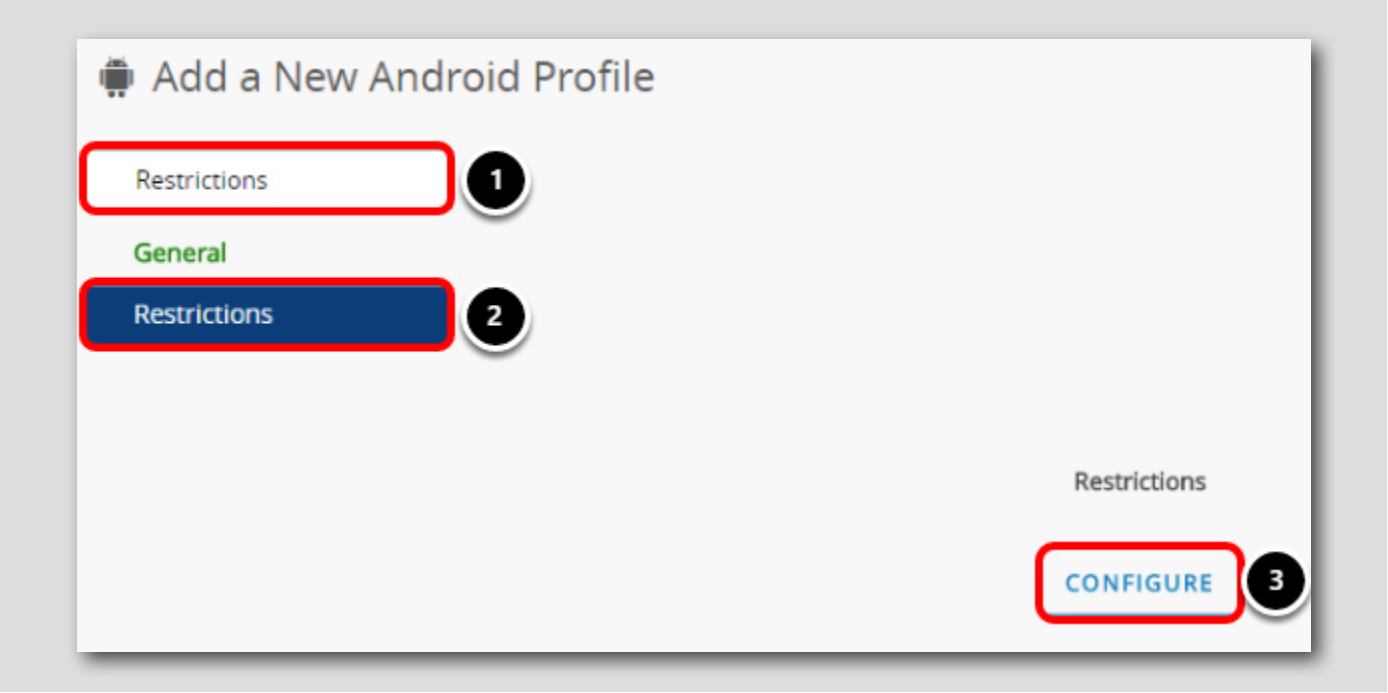
[455]



1. [General] ペイロードが選択されていることを確認します。
2. [Name] フィールドに **`Android Restrictions`** と入力します。
3. [Smart Groups] をクリックして、使用可能な割り当てのリストを表示します。
4. [All Devices (your@email.shown.here)] グループを選択します。

制限事項の構成

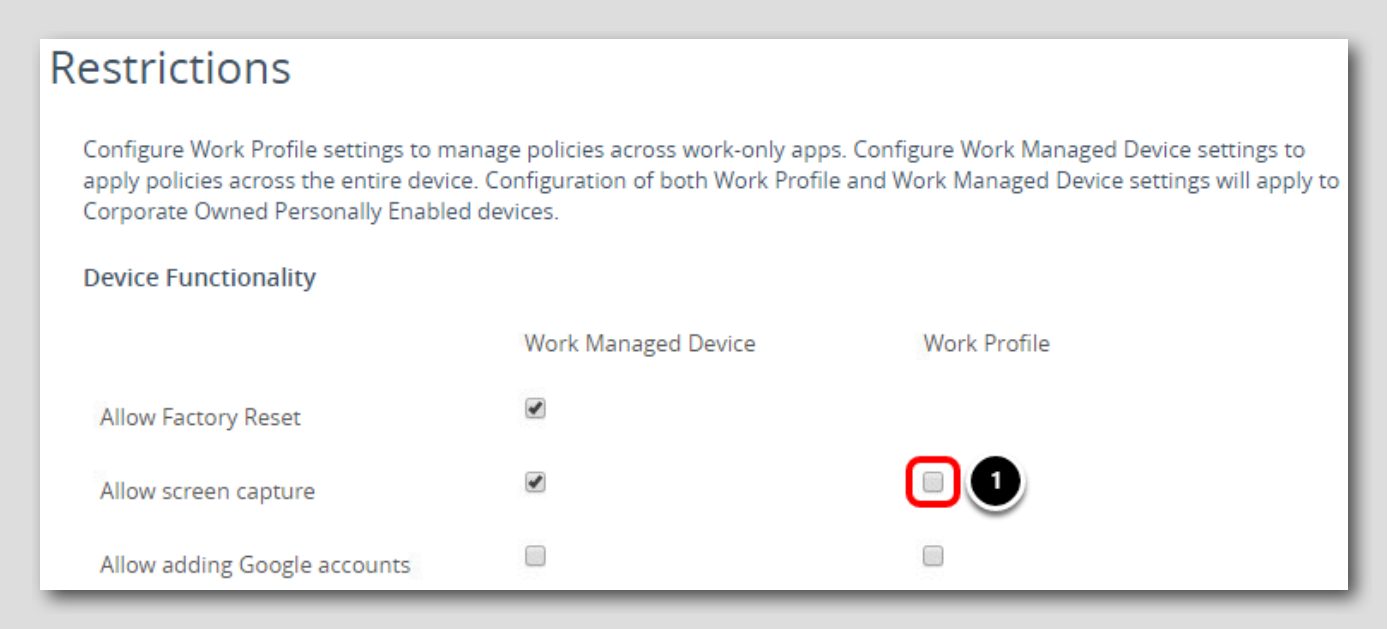
[456]



1. ペイロードの検索ボックスに **Restrictions** と入力します。
2. [Restrictions] ペイロードをクリックします。
3. [Configure] をクリックします。

スクリーン キャプチャの制限事項の構成

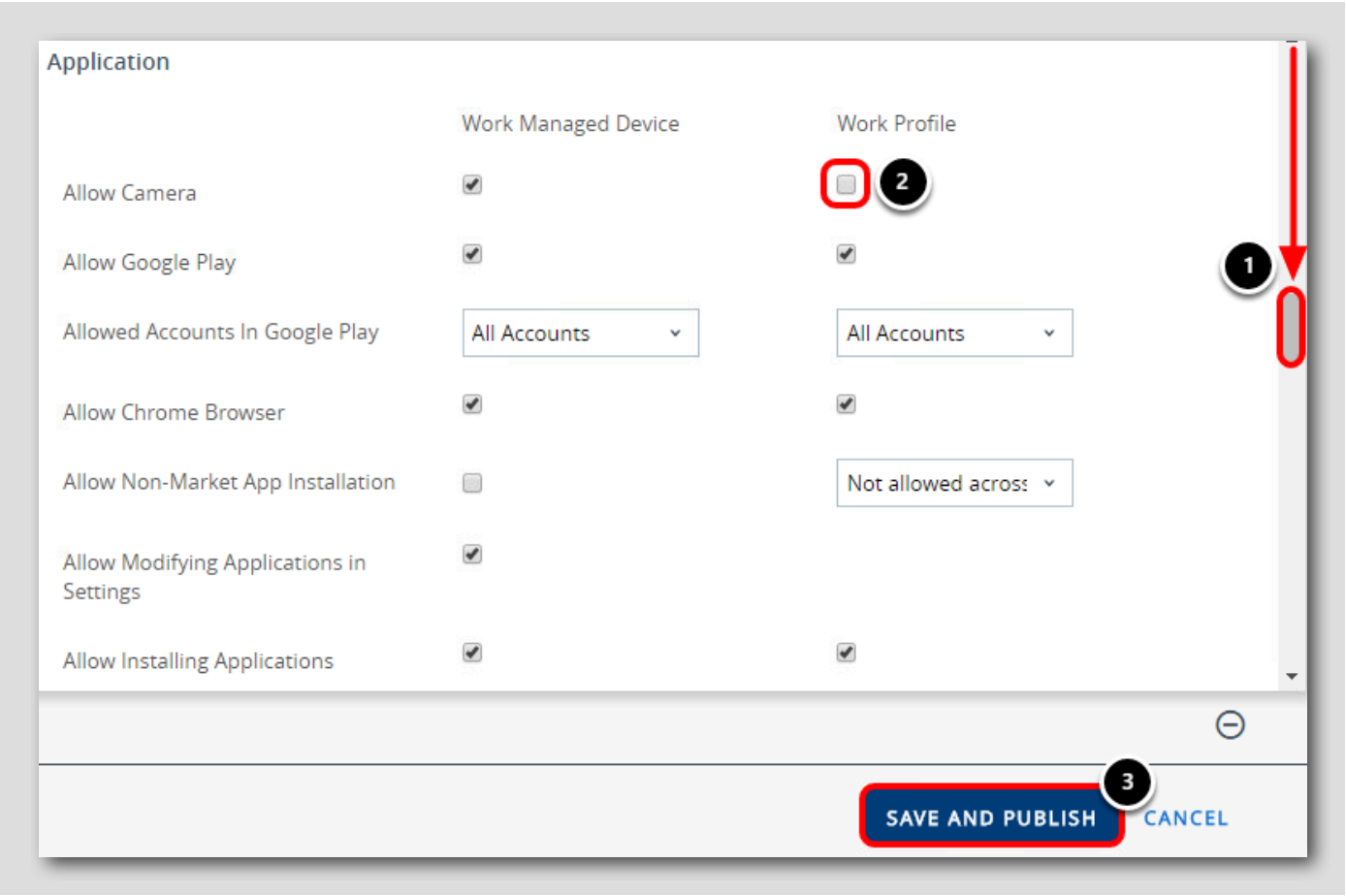
[457]



[Work Profile] 列の [Allow Screen Capture] チェックボックスをオフにします。

カメラの制限事項の構成

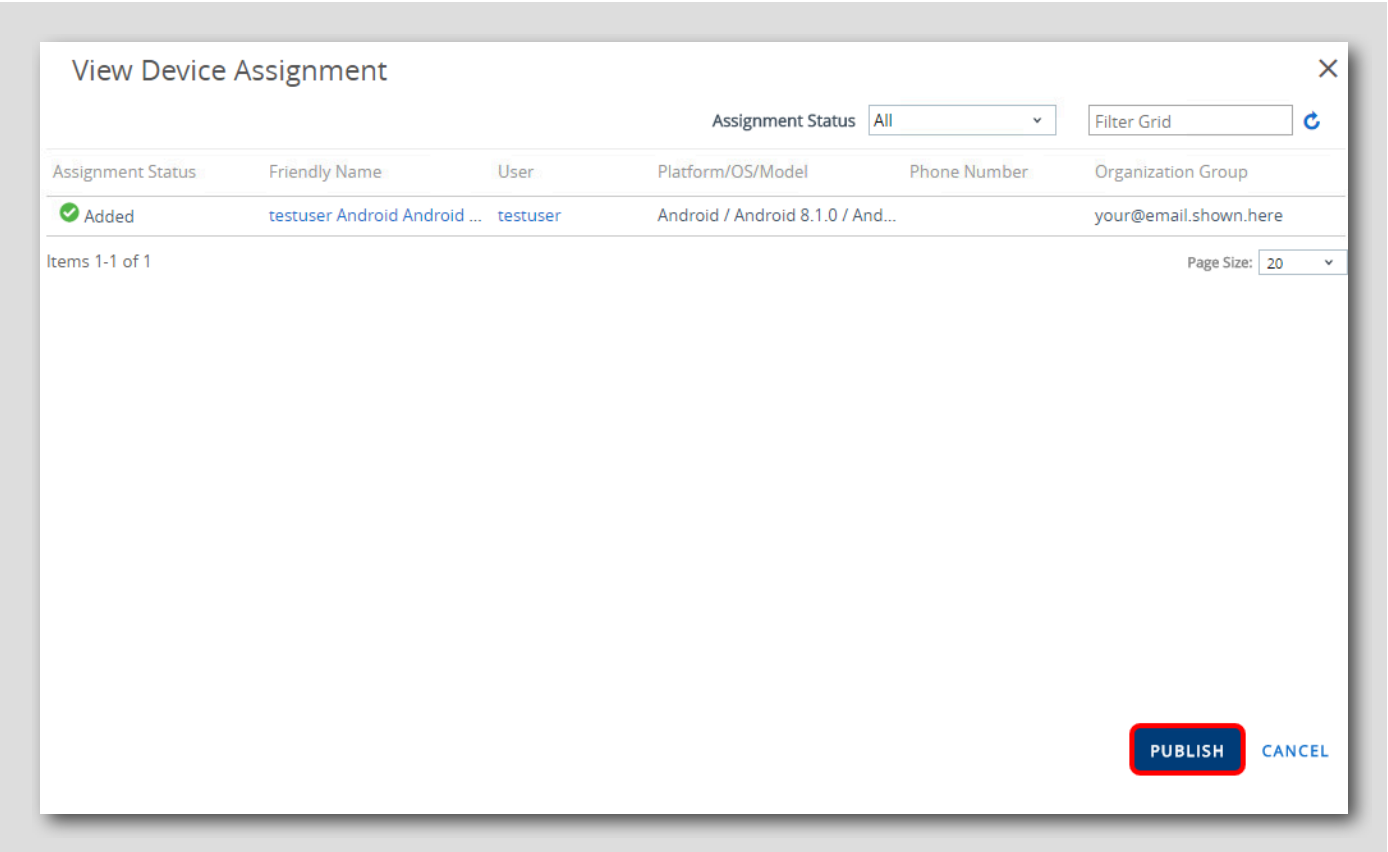
[458]



1. 下にスクロールして、[Applications] セクションを見つけます。
2. [Work Profile] 列の [Allow Camera] チェックボックスをオフにします。
3. [Save And Publish] をクリックします。

プロファイルの公開

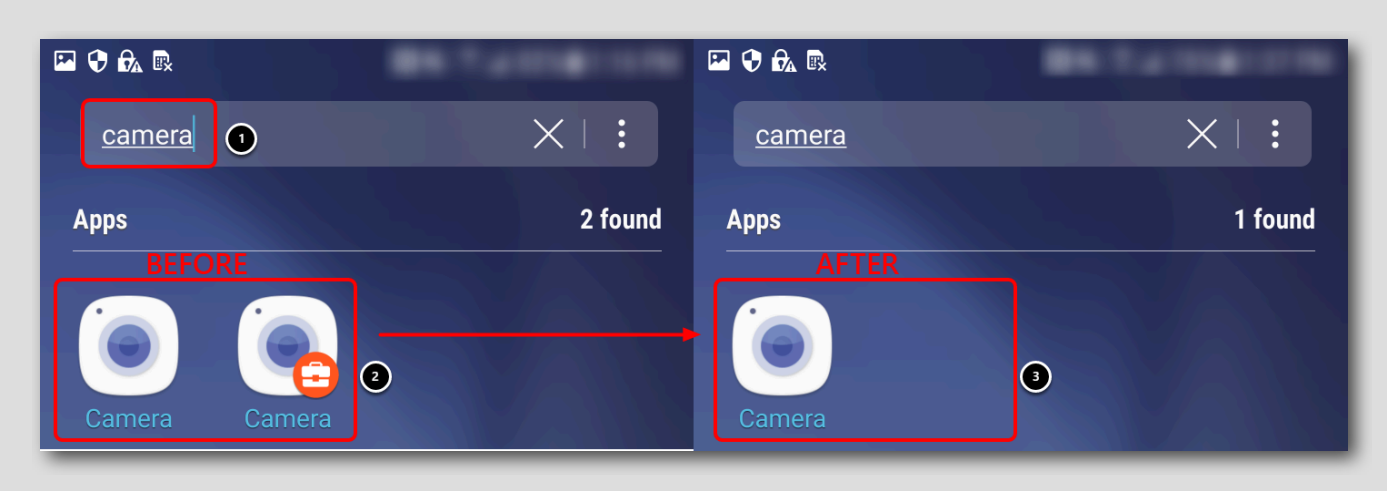
[459]



[Publish] をクリックします。

Android Enterprise カメラの制限事項の確認

[460]



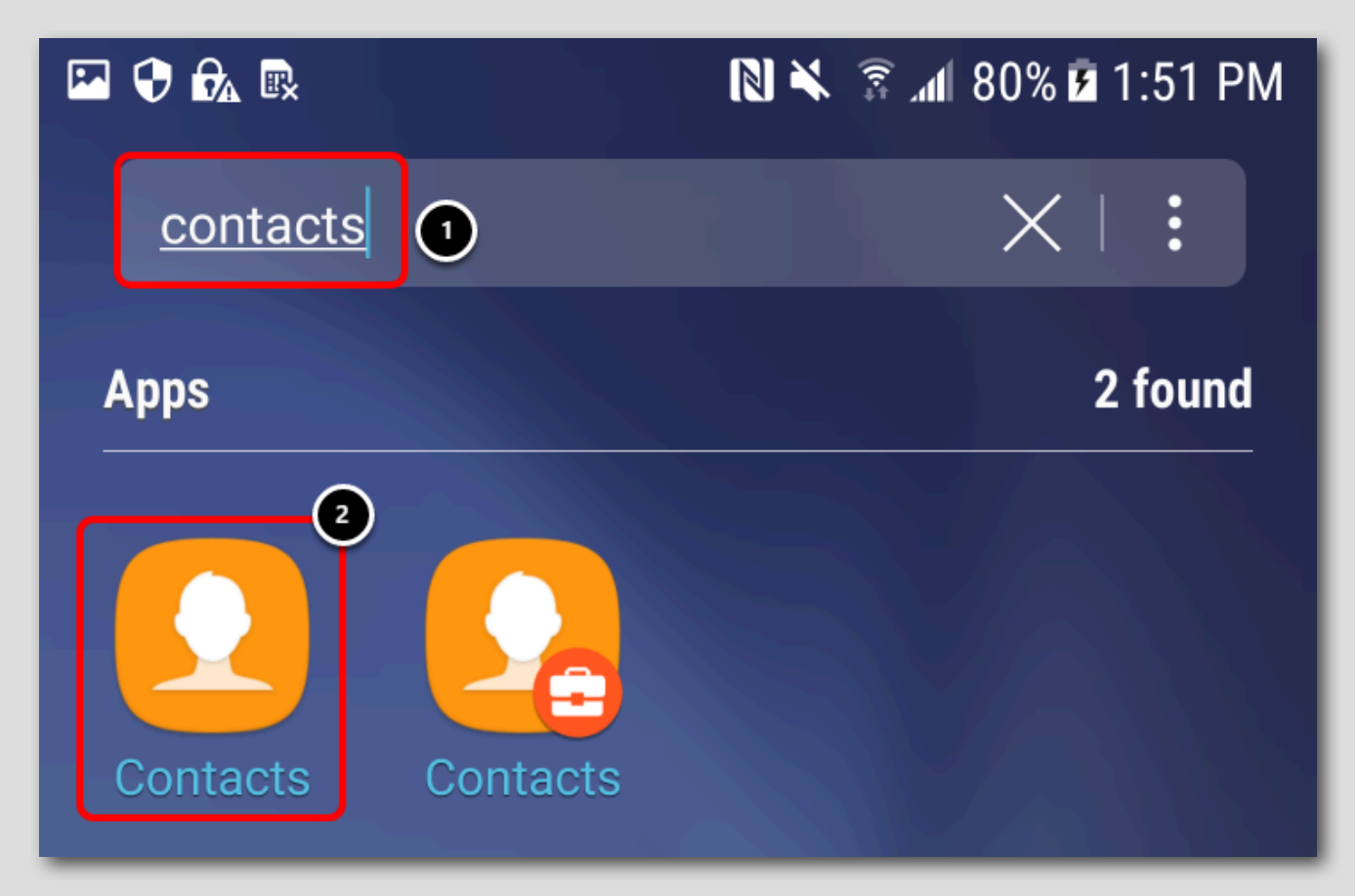
デバイスにプロファイルをプッシュした後に、デバイスではバッジ付きカメラ アプリケーションが利用できなくなりますが、個人側（バッジなし）のカメラは使用可能な状態のままです。これにより、以前に作成された Workspace ONE UEM Android プロファイルで設定したカメラの制限事項を確認できます。

1. デバイスで **`camera`** を検索します。
2. プロファイルが有効になる前に、Camera 仕事用（バッジ付き）アプリケーションが個人用（バッジなし）アプリケーションの横に存在することに注意してください。
3. プロファイルが有効になった後、Camera 仕事用（バッジ付き）アプリケーションが削除されました。

注：ラボのネットワーク制限により、バッジ付き Camera アプリケーションが削除されるまでに数分かかる場合があります。まだデバイス上に表示されている場合は、アプリケーションが正常に削除されるまでお待ちください。

バッジなしアプリケーションのスクリーンショット

[461]

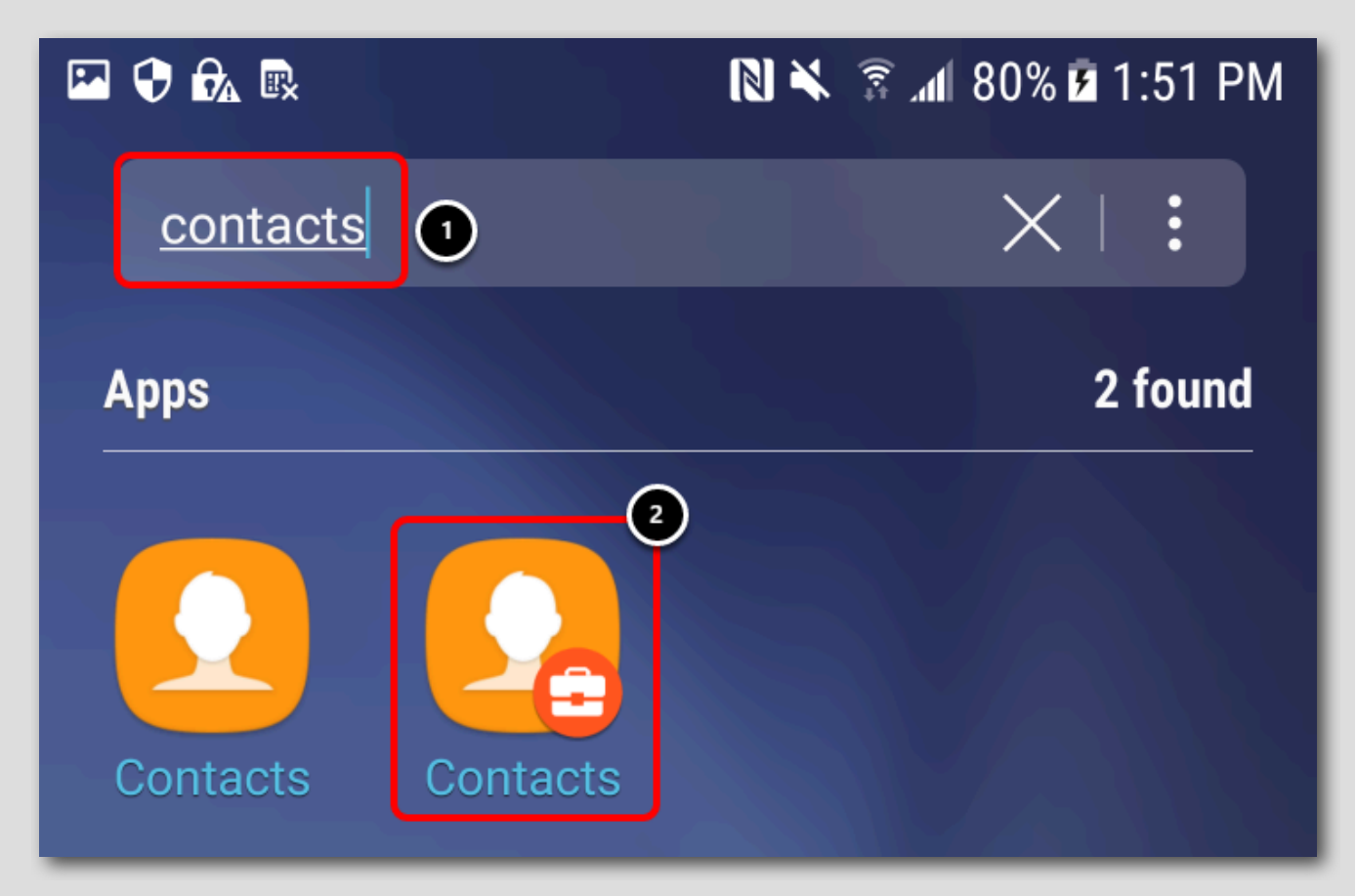


1. デバイスで **contacts** を検索します。
2. 個人用（バッジなし） の Contacts アプリケーションを開きます。
3. スクリーンショットを作成します（電源ボタンとボリューム ダウン/電源ボタン + ホーム ボタンを同時に 2 秒間押します）。スクリーンショットが正常に作成されたことを確認します。

注：スクリーンショットを変更するためのショートカットは、デバイス モデルによって異なる場合があります。サポートが必要な場合は、ラボのアシスタントに問い合わせてください。

Android Enterprise のスクリーンショットの制限を確認

[462]



1. デバイスで **contacts** を検索します。
2. **仕事用（バッジ付き）** の Contacts アプリケーションを開きます。
3. スクリーンショットを作成します（電源ボタンとボリューム ダウン/電源ボタン + ホーム ボタンを同時に 2 秒間押します）。スクリーンショットが正常に作成されなかったことを確認します。

これは、以前に作成された Workspace ONE UEM Android プロファイルで適用されたスクリーンショットの制限を示しています。

アプリケーションの承認

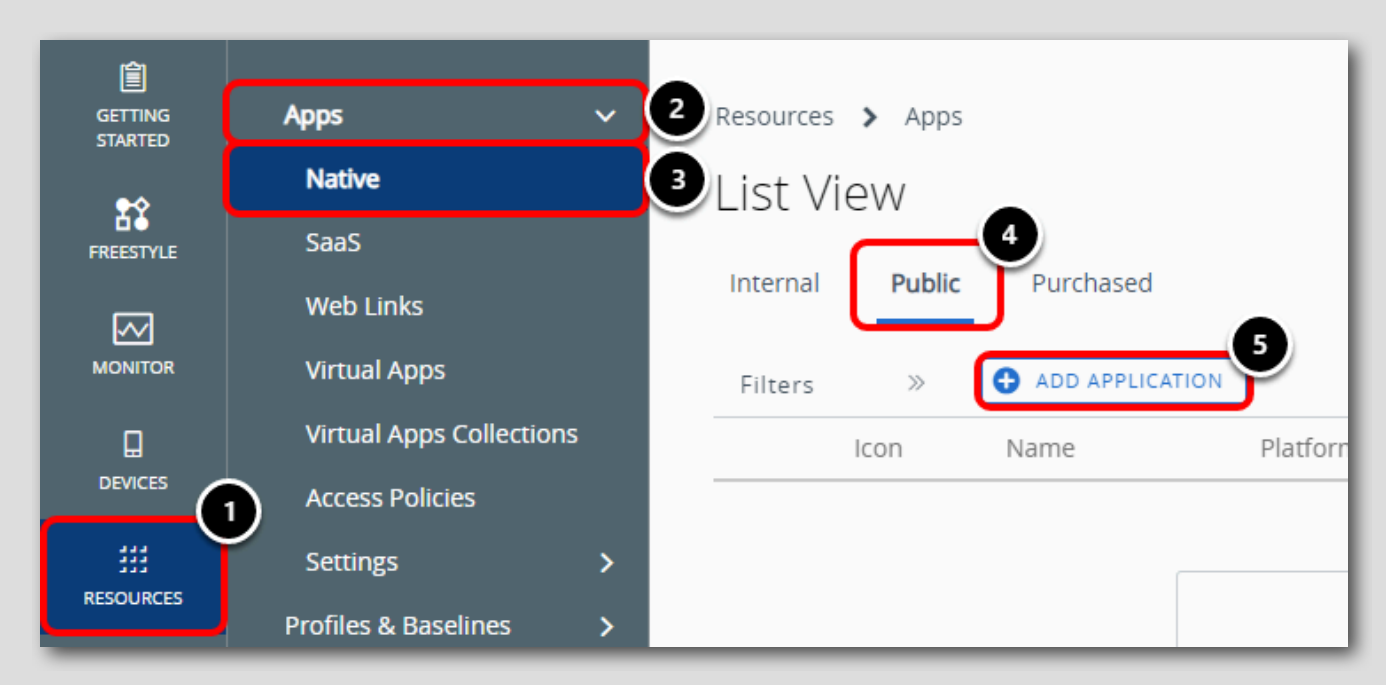
[463]

このセクションでは、Workspace ONE UEM と Android Enterprise の連携のためにアプリケーションを承認するプロセスについて説明します。Workspace ONE UEM と Android Enterprise の連携を通じてプッシュするアプリケーションは、Google Play Store の対応するアプリケーションと同じ機能を備えています。ただし、Workspace ONE UEM 機能を使用すると、これらのアプリケーションに機能とセキュリティを追加できます。

- 使いやすくするため、[Send Application Configuration] オプションを構成します。アプリケーション構成を使用すると、サポートされているキーと値のペアを事前構成し、アプリケーションと一緒にデバイスにプッシュすることができます。サポートされている値の例としては、ユーザー名、パスワード、VPN 設定などがあります。サポート値はアプリケーションによって異なります。
- 安全な機能を追加するには、Android Enterprise に Workspace ONE UEM プロファイルを使用します。プロファイルを使用すると、パスコードを設定し、制限事項を適用し、認証に証明書を使用できます。

パブリック アプリケーションの追加

[464]

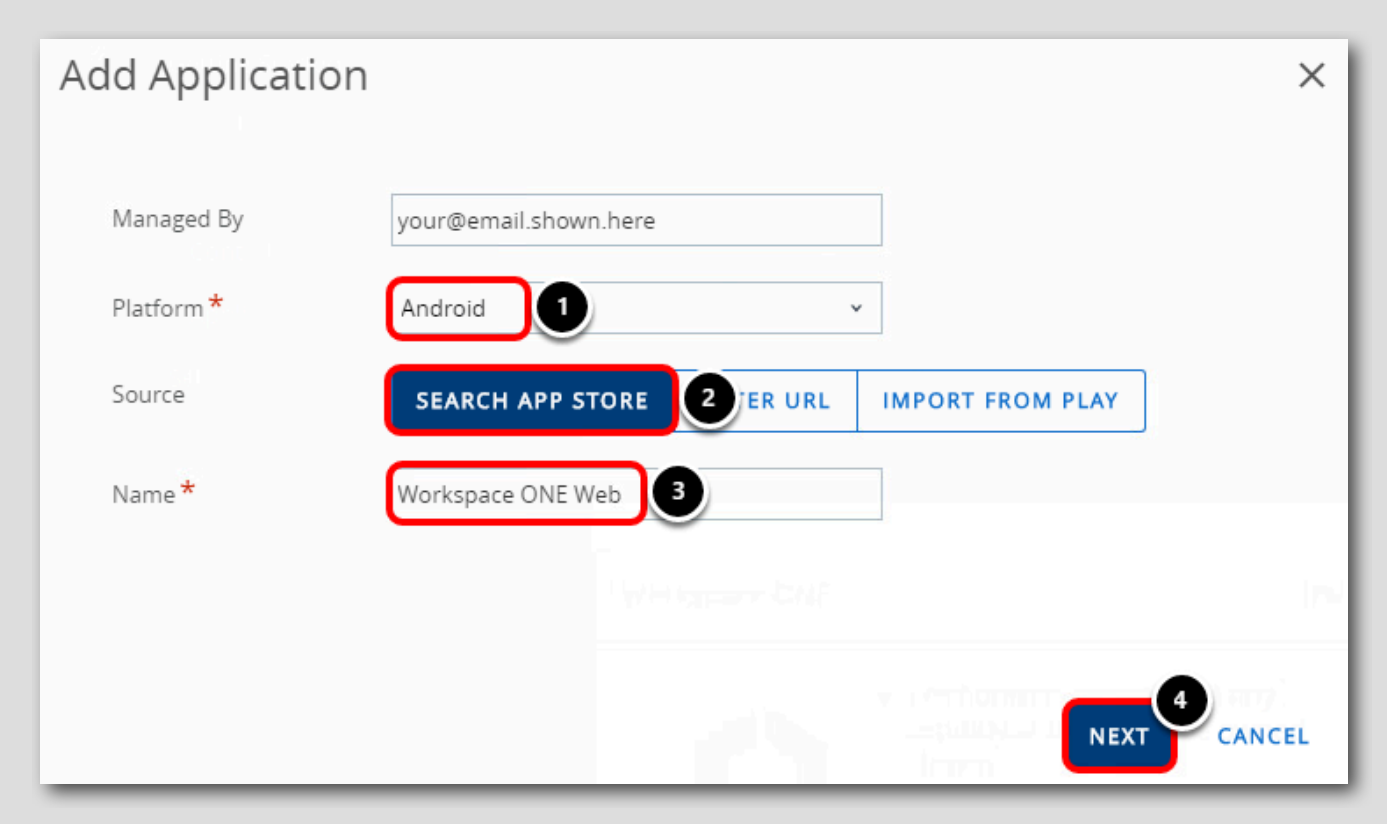


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Resources] をクリックします。
2. [Apps] を展開します。
3. [Native] をクリックします。
4. [Public] タブをクリックします。
5. [Add Application] をクリックします。

パブリック アプリケーションの検索

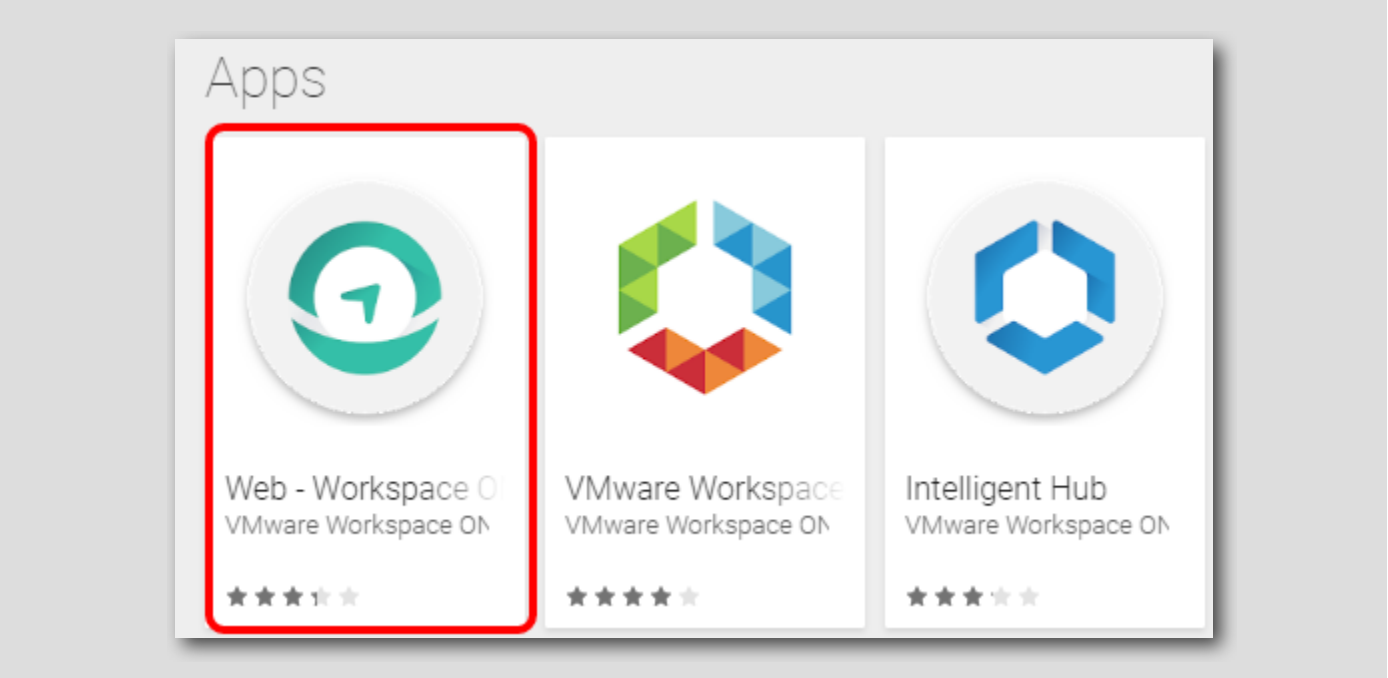
[465]



1. [Platform] ドロップダウン メニューから [Android] を選択します。
2. [Source] に対して [Search App Store] を選択します。
3. [Name] テキスト ボックスに **`Workspace ONE Web`** と入力します。
4. [Next] をクリックします。

Workspace ONE Web アプリケーションの選択

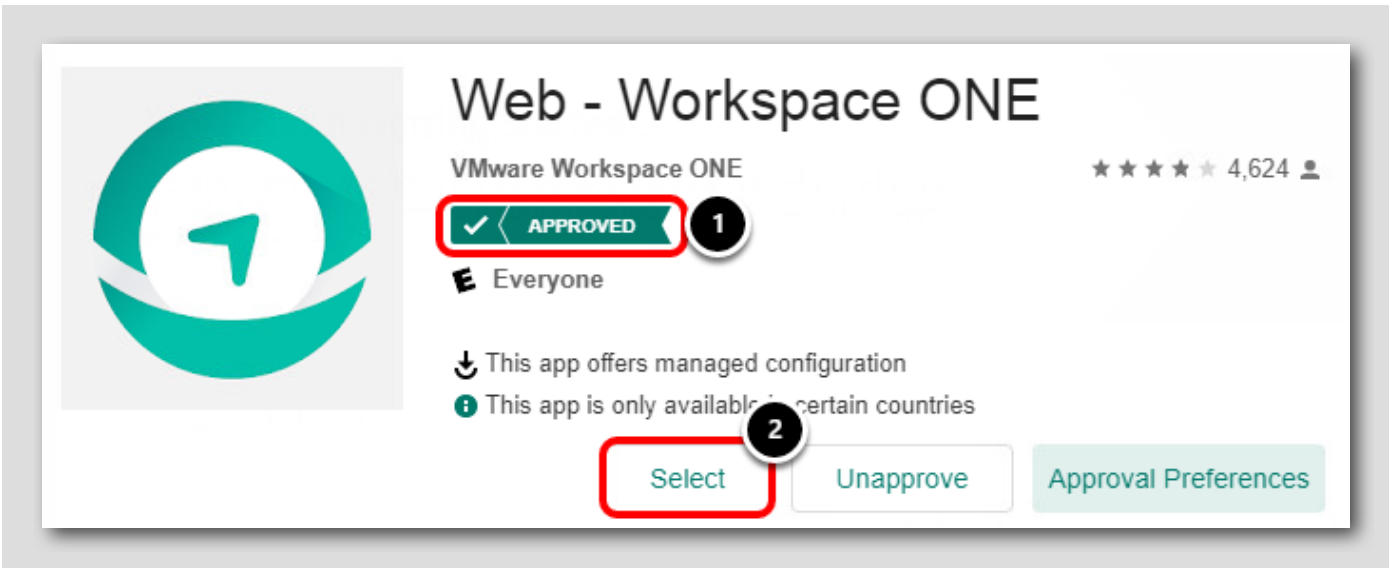
[466]



[Web - Workspace ONE] アプリケーションをクリックします。

アプリケーションを選択して承認

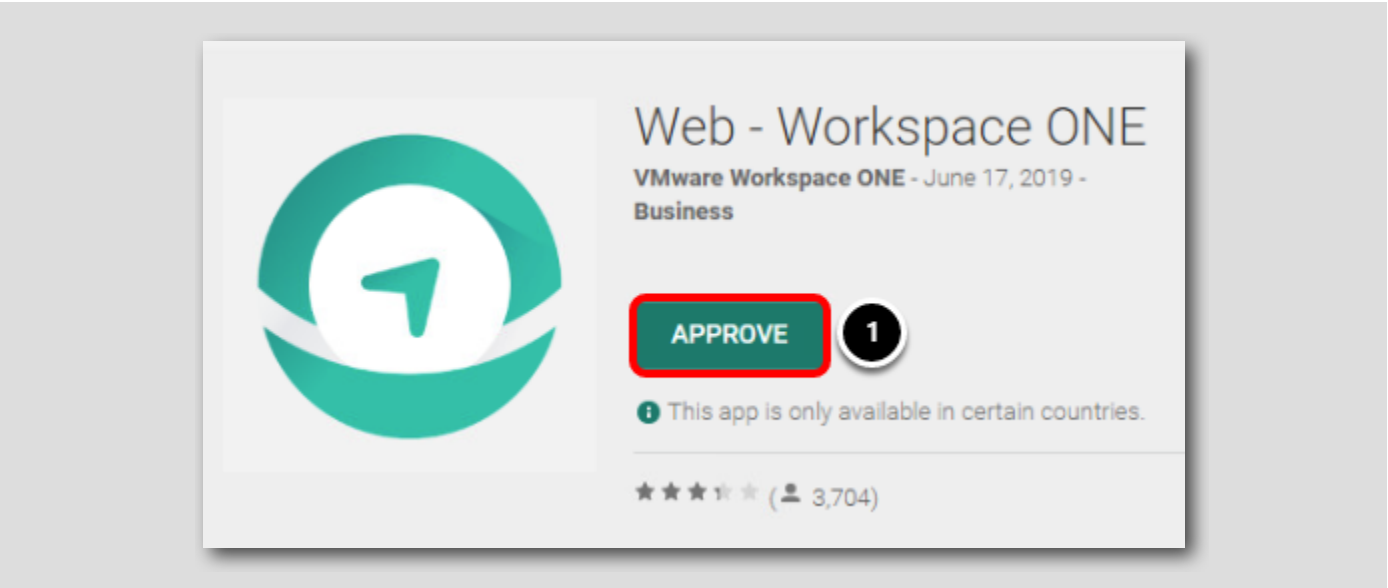
[467]

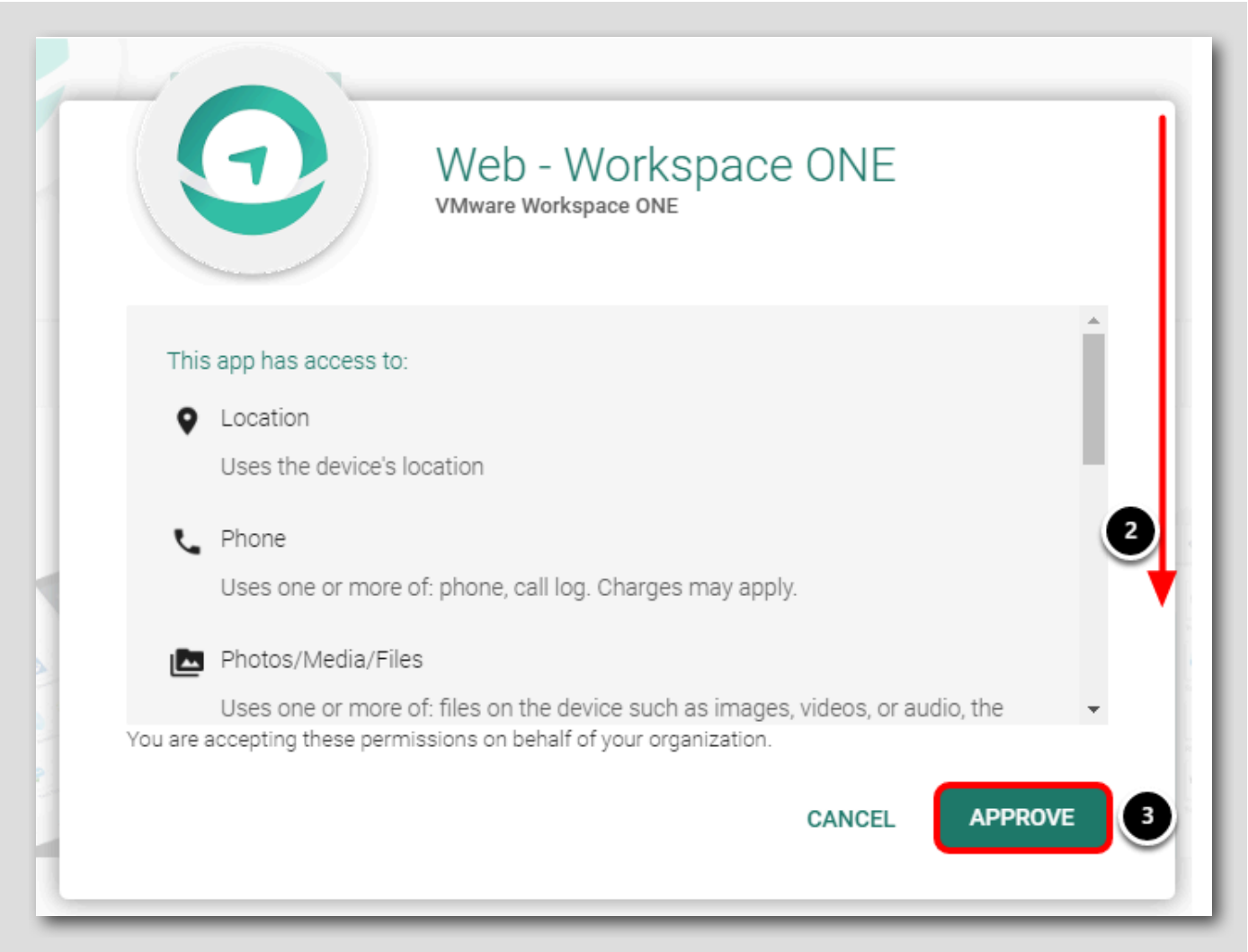


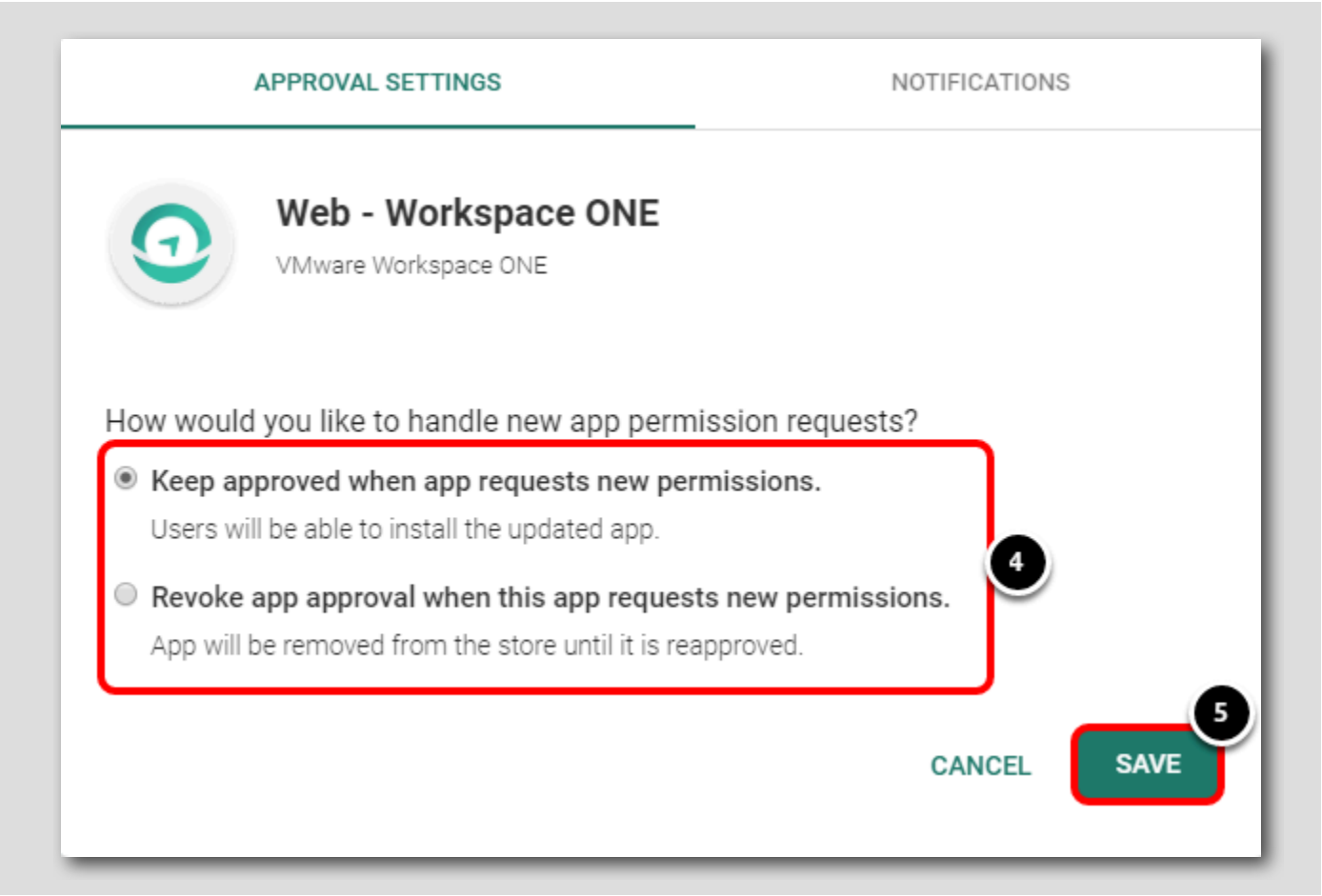
1. アプリケーションがすでに「Approved」としてマークされていることを確認します。これは、Android EMM 登録設定が親レベルの組織グループで構成されており、組織グループがこれらの設定を継承しているためです。アプリケーションの承認が必要になるのは一度だけです。これはすでに実行済みです。
2. [Select] をクリックして進みます。

次の手順に進むか、以降の手順を確認して、新しいアプリケーションに必要な承認手順を確認します。

重要：以降の手順は単なる情報であり、必要に応じてスキップできます。これらは、新しいアプリケーションの承認プロセスを示すために含まれています。


Web - Workspace ONE
VMware Workspace ONE - June 17, 2019 - Business
APPROVE
1
This app is only available in certain countries.
(3,704)


Web - Workspace ONE
VMware Workspace ONE
This app has access to:
Location
Uses the device's location
Phone
Uses one or more of: phone, call log. Charges may apply.
Photos/Media/Files
Uses one or more of: files on the device such as images, videos, or audio, the
You are accepting these permissions on behalf of your organization.
CANCEL
APPROVE
2
3

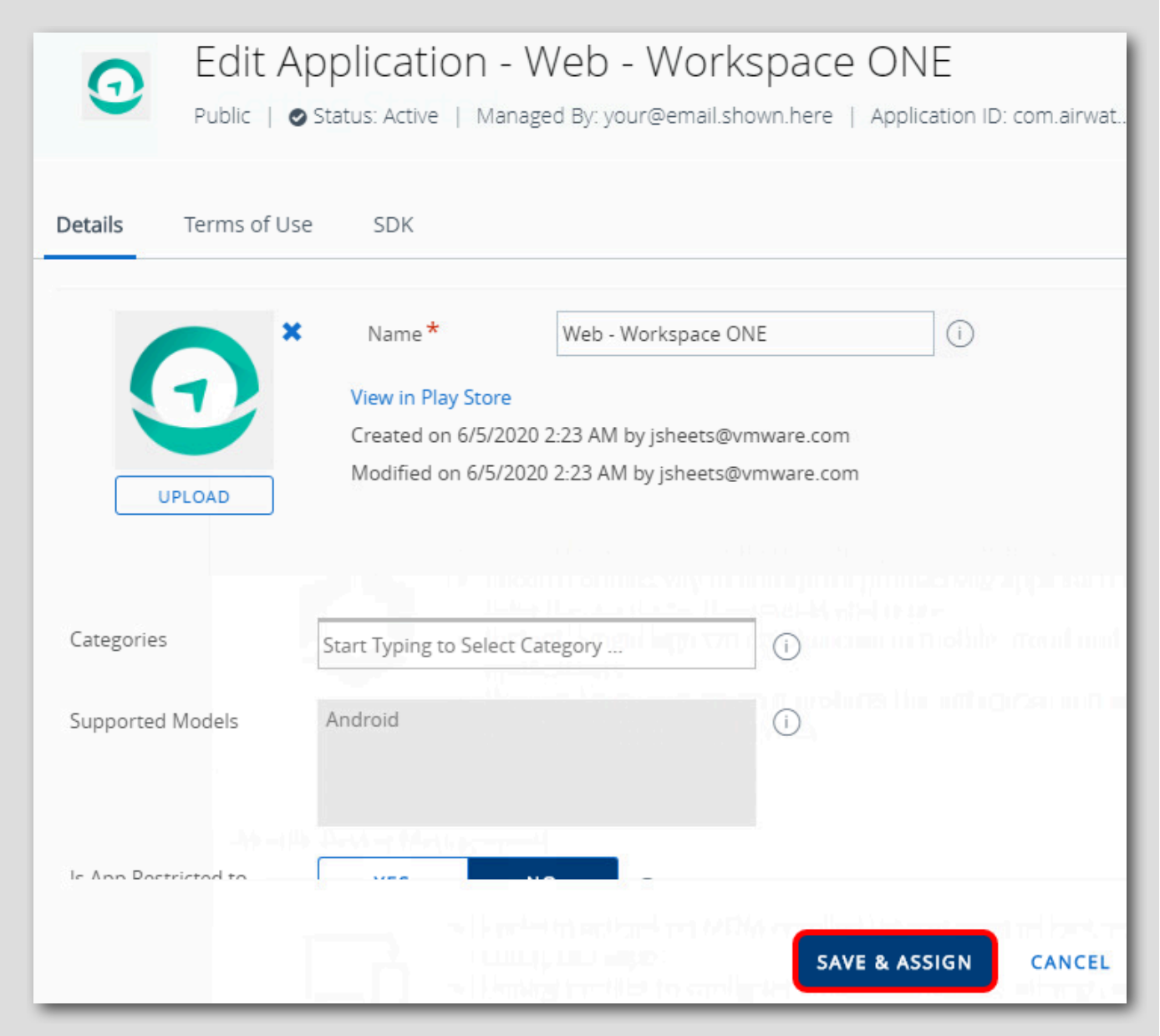


1. 目的のアプリケーションに対して [Approve] をクリックします。
2. アプリケーションがアクセスできる項目のリストをスクロールします。
3. [Approve] をクリックします。
4. 新しいアプリケーションの権限要求をどのように処理するかを確認して選択します。これにより、アプリケーションが将来、前の画面に表示されていたものではない新しい権限を要求した場合に、手動で承認するか自動で承認するかを選択できます。
5. [Save] をクリックします。

その後、管理者はこのプロセスの最初の手順に戻ります。そこで、[Select] をクリックして、さらに必要なアプリケーションを追加することができます。

パブリック アプリケーションの公開

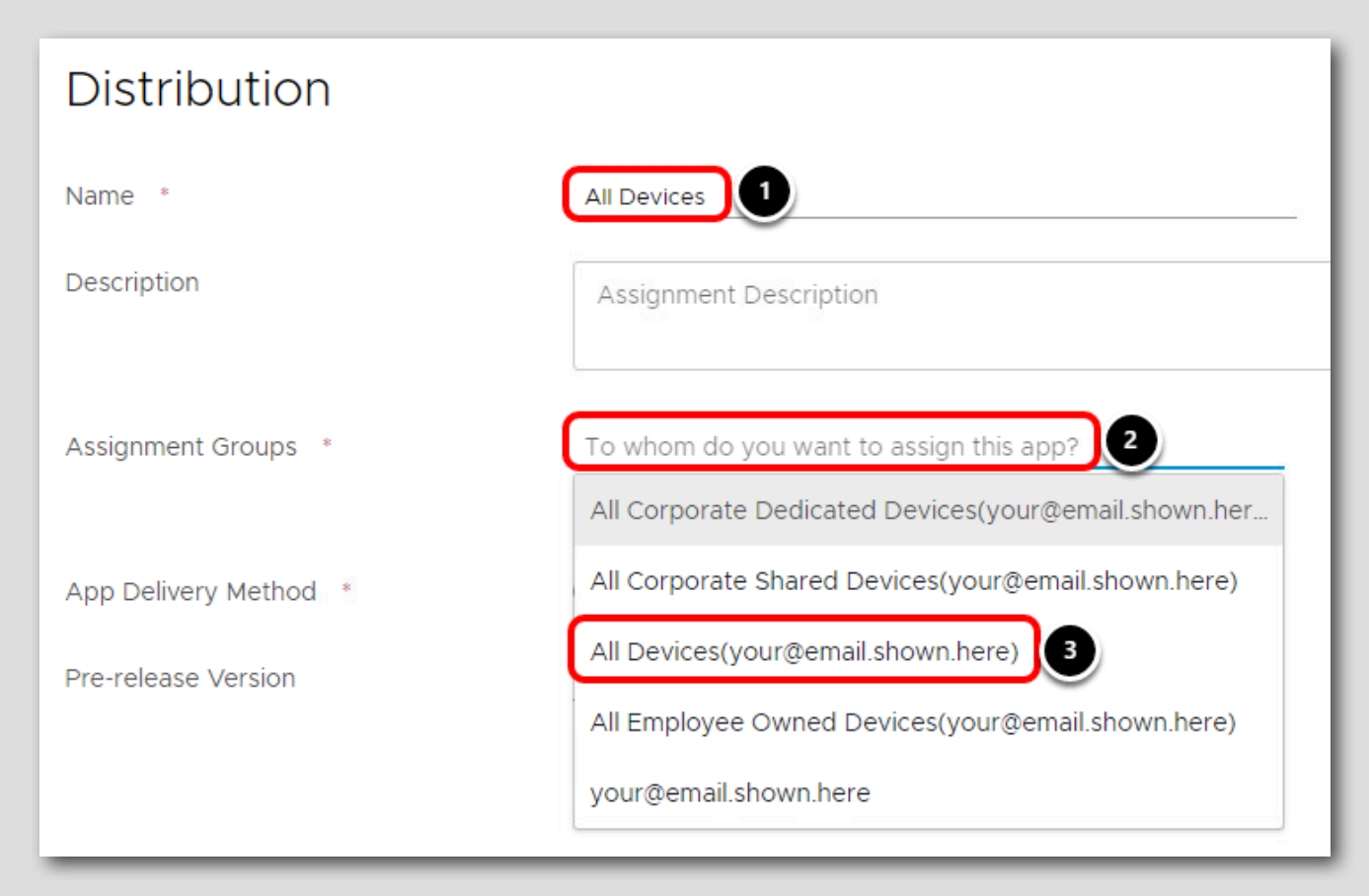
[468]



[Save & Assign] をクリックします。

割り当て配布の追加

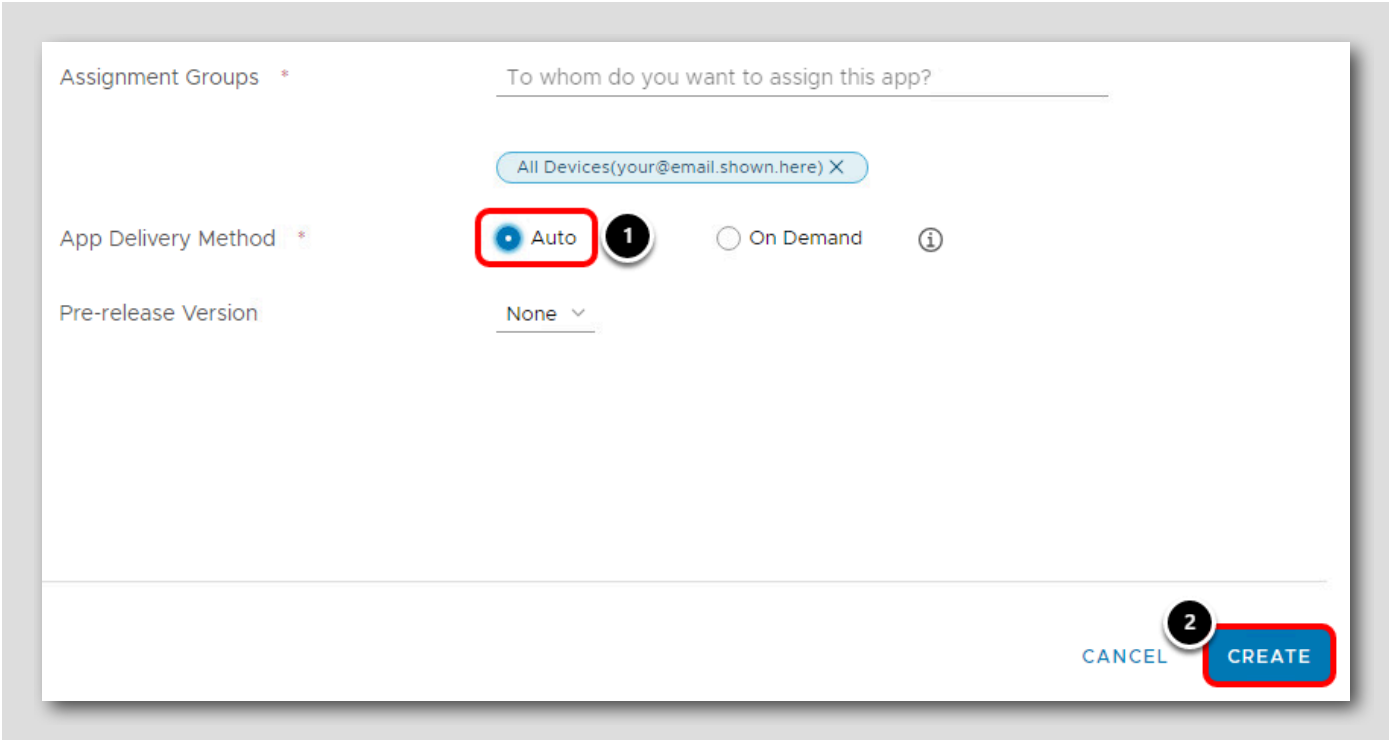
[469]



1. 配布名に **`All Devices`** と入力します。
2. [Assignment Groups] フィールドをクリックします。
3. [All Devices (your@email.shown.here)] グループを選択します。

割り当ての構成

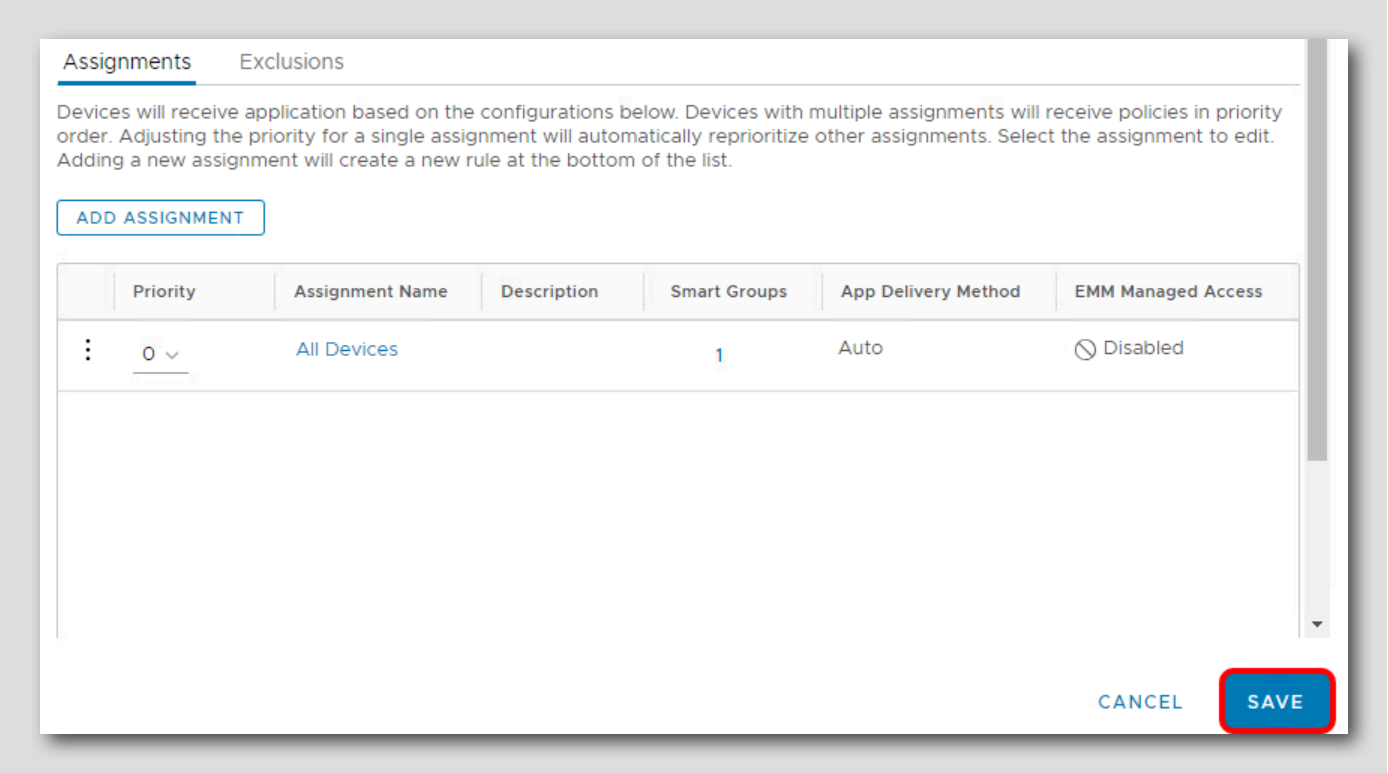
[470]



1. [App Delivery Method] に対して **[Auto]** を選択します。
2. **[Create]** をクリックします。

Workspace ONE Web を保存して公開

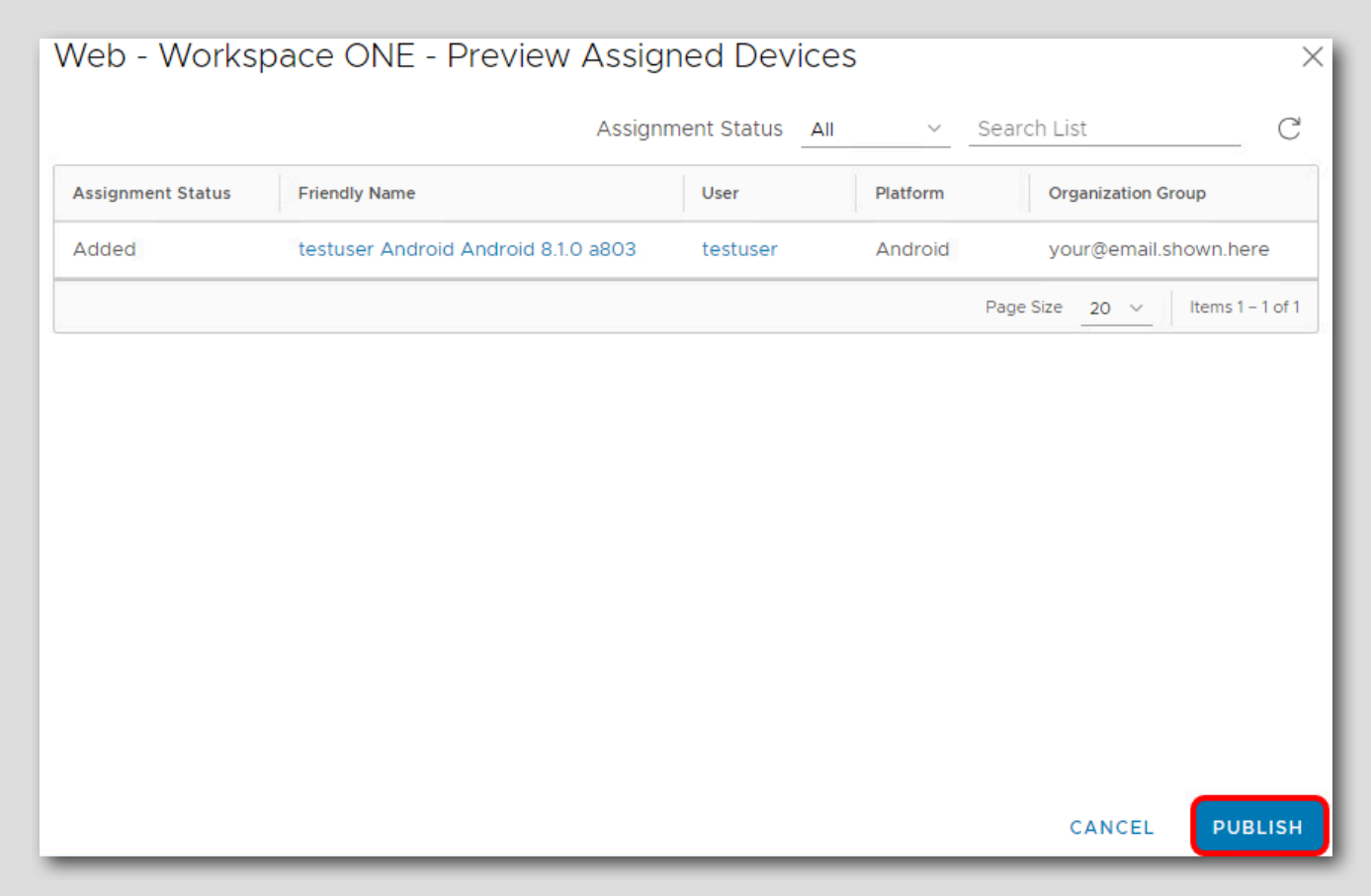
[471]



[Save] をクリックします。

割り当てられたデバイスをプレビューして公開

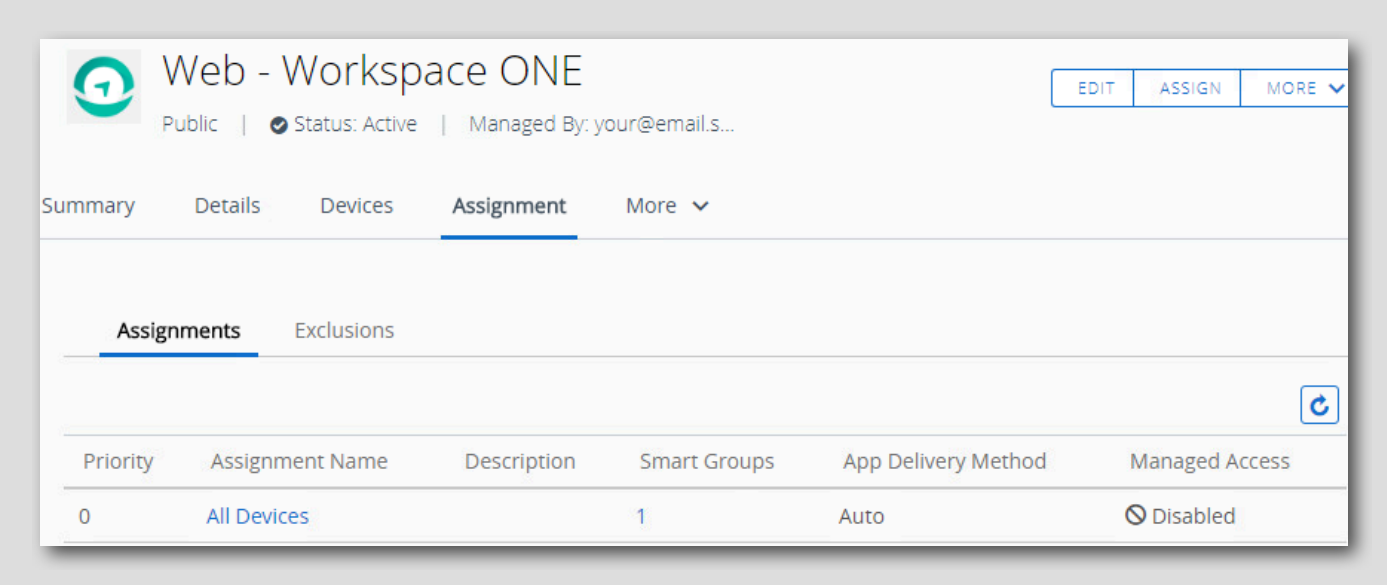
[472]



[Publish] をクリックします。

アプリケーション作成の確認

[473]



Workspace ONE Web アプリケーションが承認、作成され、[All Devices] グループに割り当てられたことを確認します。

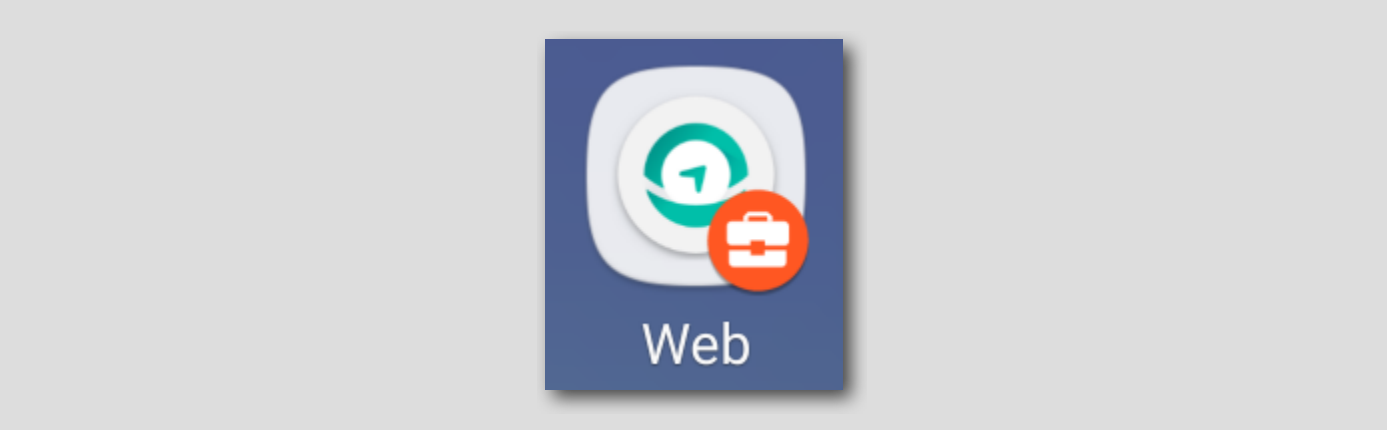
仕事用アプリケーションの確認

[474]

前のセクションでは、Workspace ONE UEM Console から Android アプリケーションを承認してプッシュする方法について学習しました。このセクションでは、登録済みの Android デバイスに仕事用アプリケーションが正しくインストールされていることを確認します。

公開された Workspace ONE Web アプリケーションがダウンロードされたことの確認

[475]



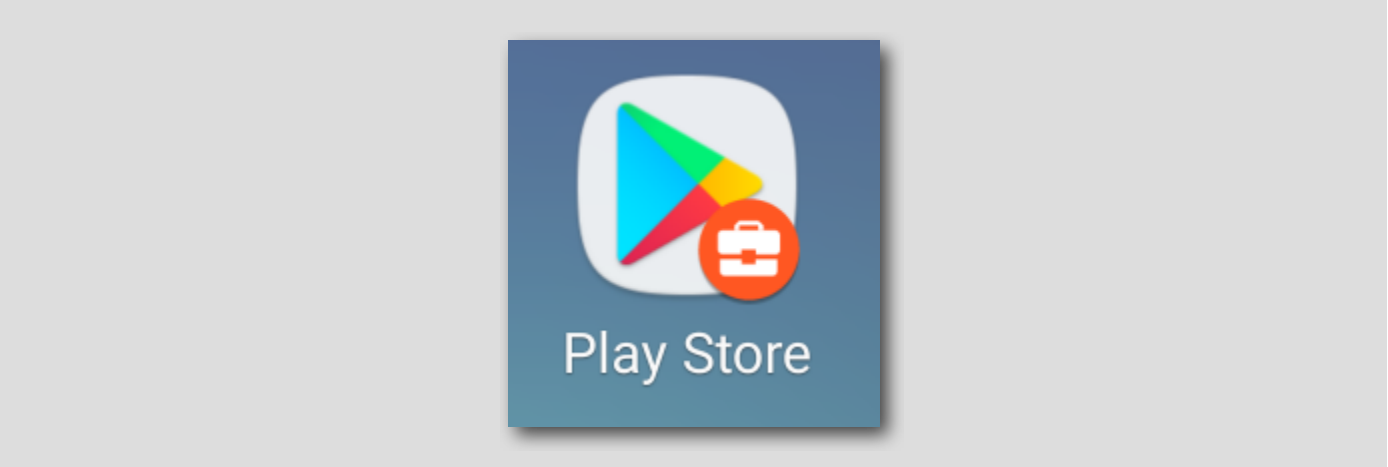
テスト用の Android デバイスに戻り、Workspace ONE Web アプリケーションがダウンロードされ、仕事用アプリケーションとして表示されていることを確認します。

注：ラボのネットワーク トラフィックによっては、ダウンロードが完了するまで数分かかる場合があります。

このプロセスを使用して、新しいアプリケーションを迅速に承認し、ユーザーに展開できます。

バッジ付きの Android Enterprise Play Store アプリケーションを開く

[476]

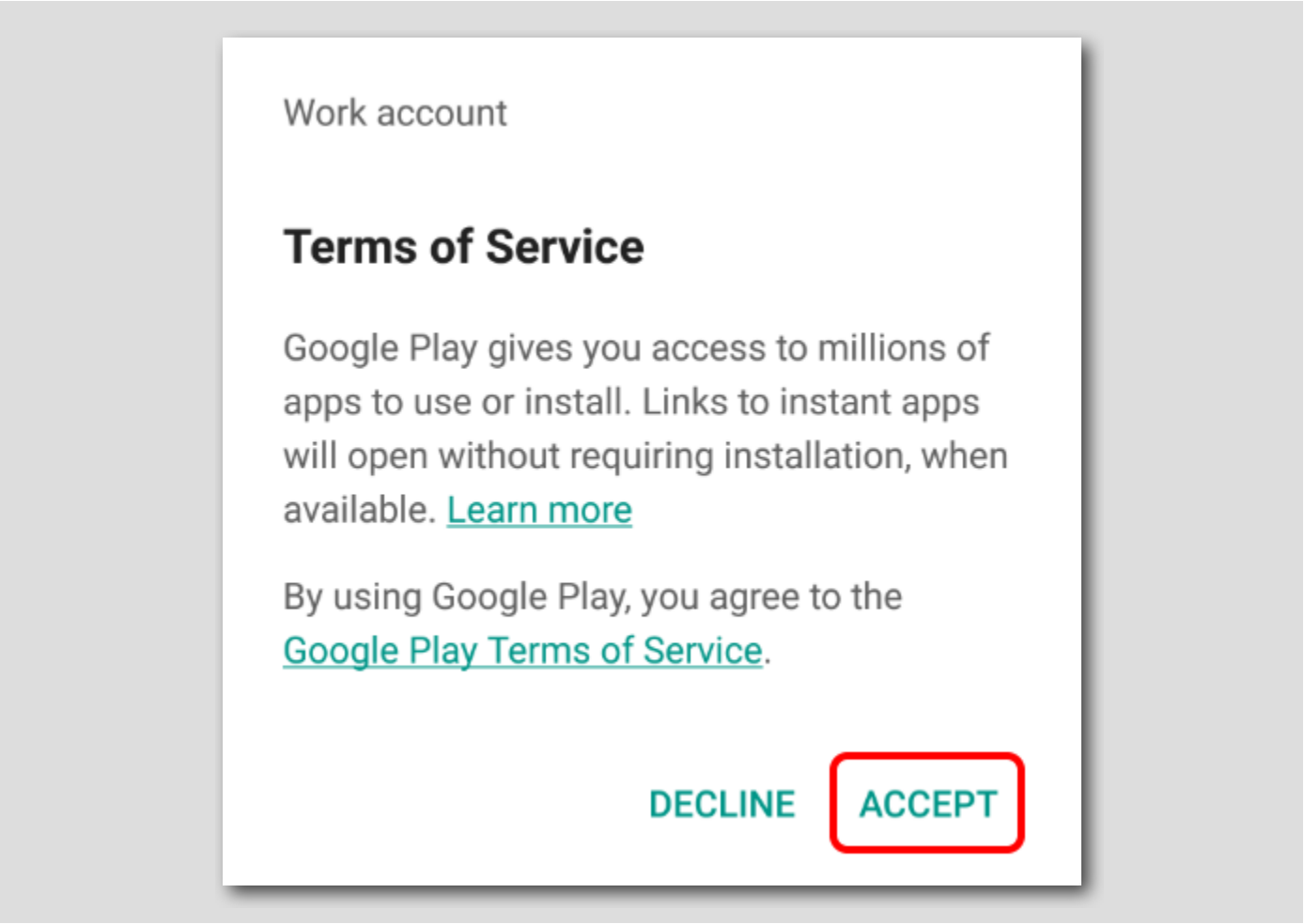


Android デバイスで仕事用 Play Store アプリケーションを開きます。

注：スクリーンショットは、デバイス モデルと OS によって異なる場合があります。

Google Play 利用規約の承諾（必要な場合）

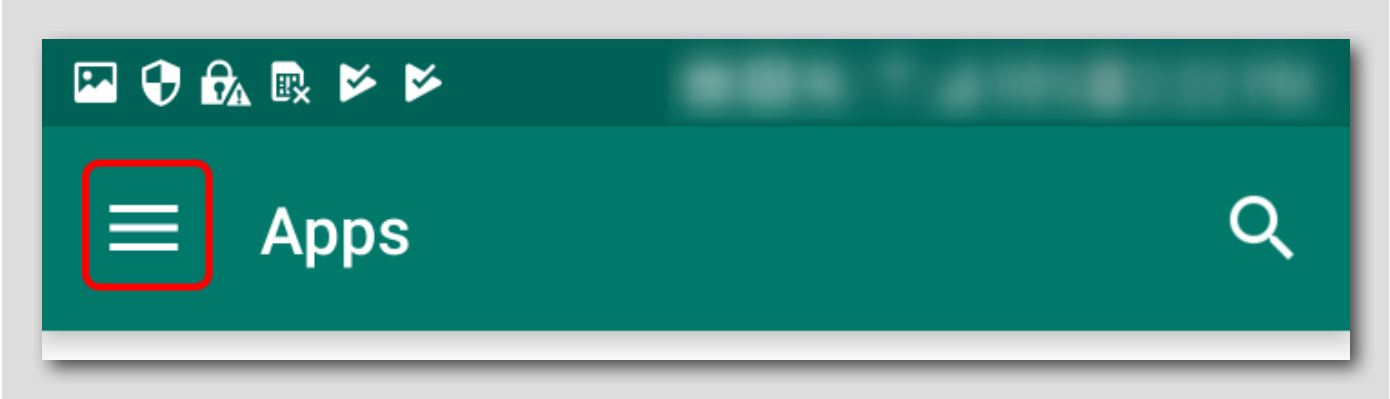
[477]



Google Play 利用規約に同意するよう求めるメッセージが表示されたら、[Accept] をタップします。それ以外の場合は、次の手順に進みます。

Play Store メニューを開く

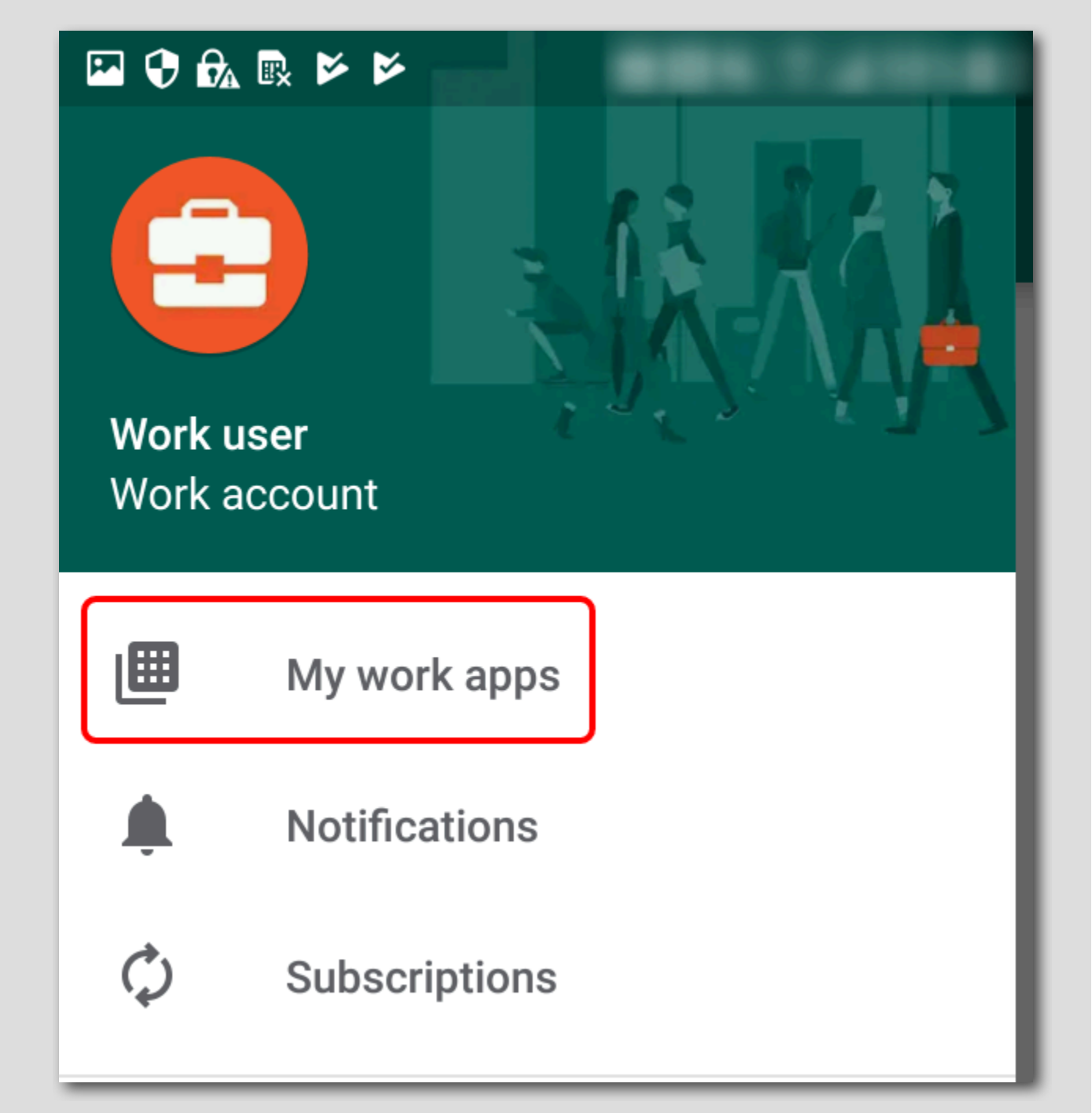
[478]



左上にある [Menu] ボタンをタップします。

注：スクリーンショットは、デバイス モデルと OS によって異なる場合があります。

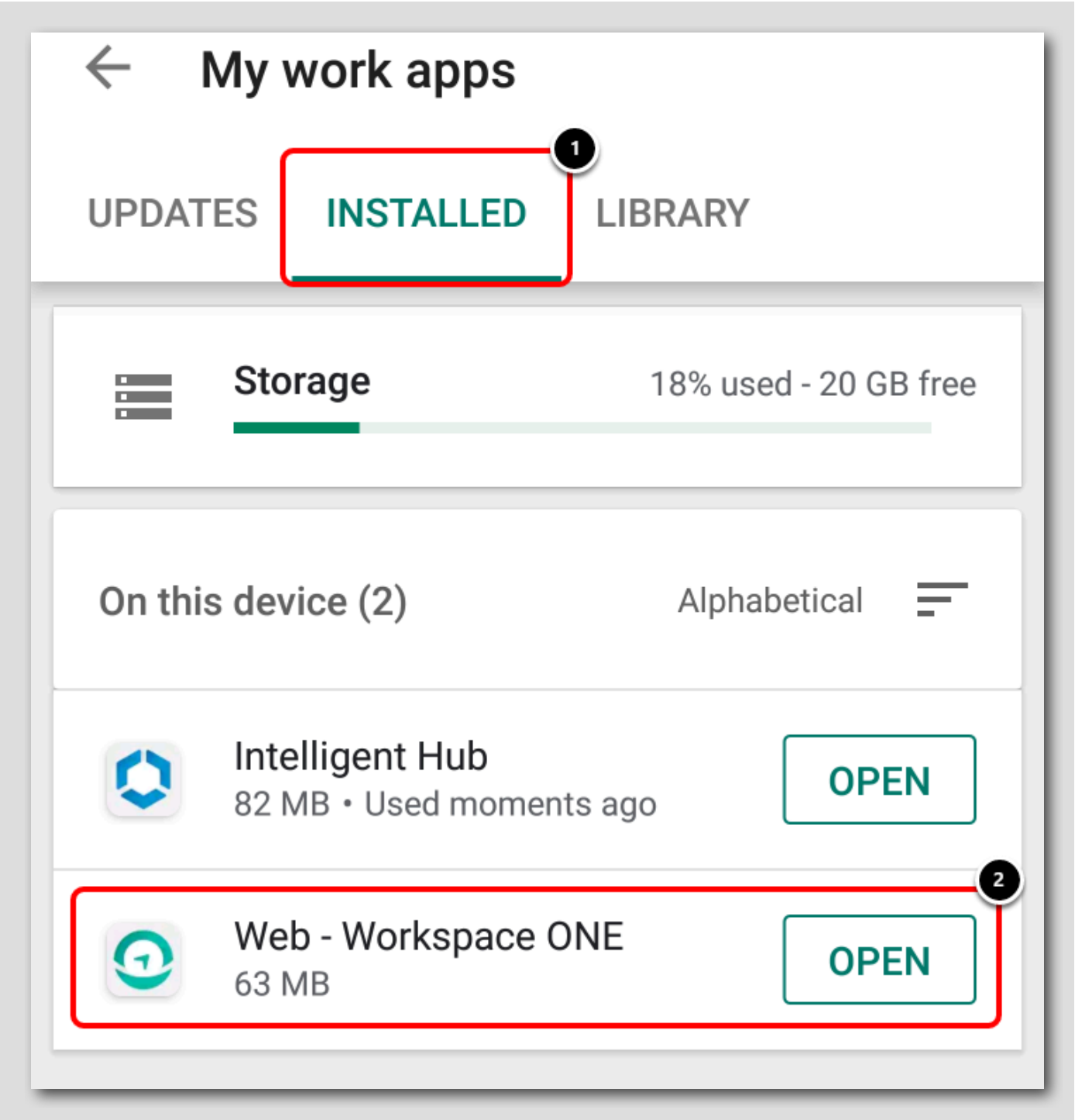
Play Store の仕事用アプリケーションの表示 [479]



メニューから [My Work Apps] をタップします。

注：スクリーンショットは、デバイス モデルと OS によって異なる場合があります。

Workspace ONE Web が仕事用アプリケーションとして利用可能であることの確認 [480]



1. [Installed] をタップします。
2. Workspace ONE Web アプリケーションが仕事用アプリケーションのリストに含まれていることを確認します。アプリケーションが見つからない場合は、下にスクロールします。

注：スクリーンショットは、デバイス モデルと OS によって異なる場合があります。

Workspace ONE Web アプリケーションは仕事用アプリケーションとしてリストされています。これは、アプリケーションをユーザーに追加および割り当てているときに、Workspace ONE UEM Console を介して仕事用アプリケーションとして承認されたためです。これにより、仕事用アプリケーションの承認と Android デバイスへの展開のプロセスが効率化され、急速に改善されます。

Android デバイスの登録解除

[481]

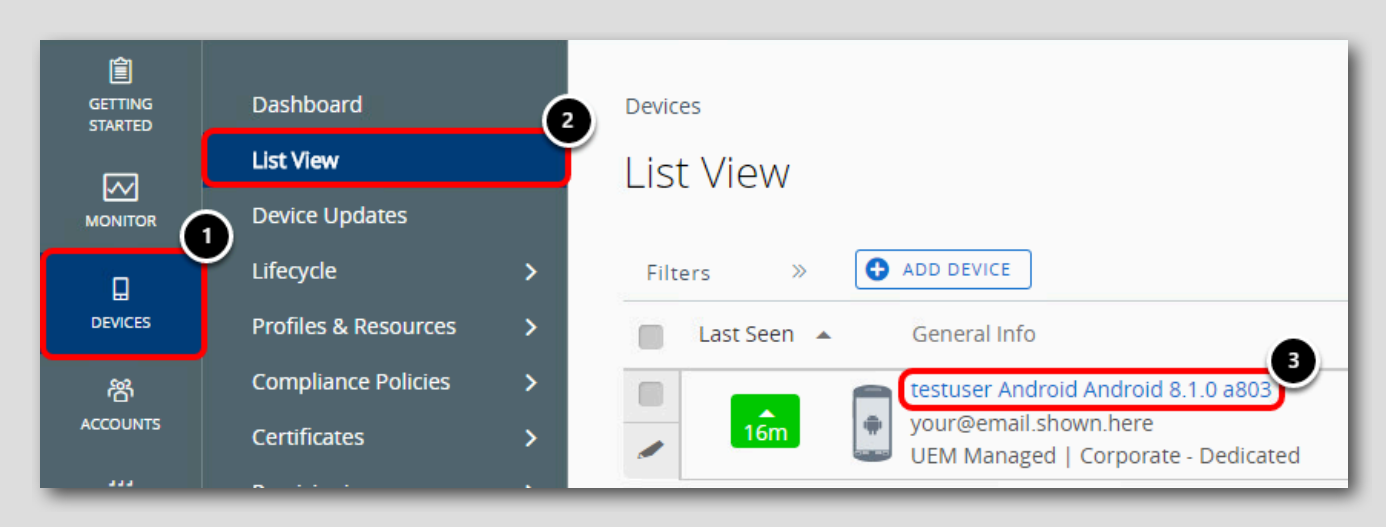
次に、Workspace ONE UEM から Android デバイスの登録を解除します。

注：「企業情報ワイプ」という用語は、デバイスのリセットまたは完全なワイプを意味するものではありません。これは、Workspace ONE Intelligent Hub アプリケーションが制御する MDM プロファイル、ポリシー、およびコンテンツのみを削除します。

注：企業情報ワイプを実行しても、デバイスから Workspace ONE Intelligent Hub アプリケーションが削除されることはありません。このアプリケーションは、Workspace ONE UEM がデバイスを制御する前に手動でダウンロードされたためです。

Android デバイスの企業情報ワイプ（登録解除）

[482]



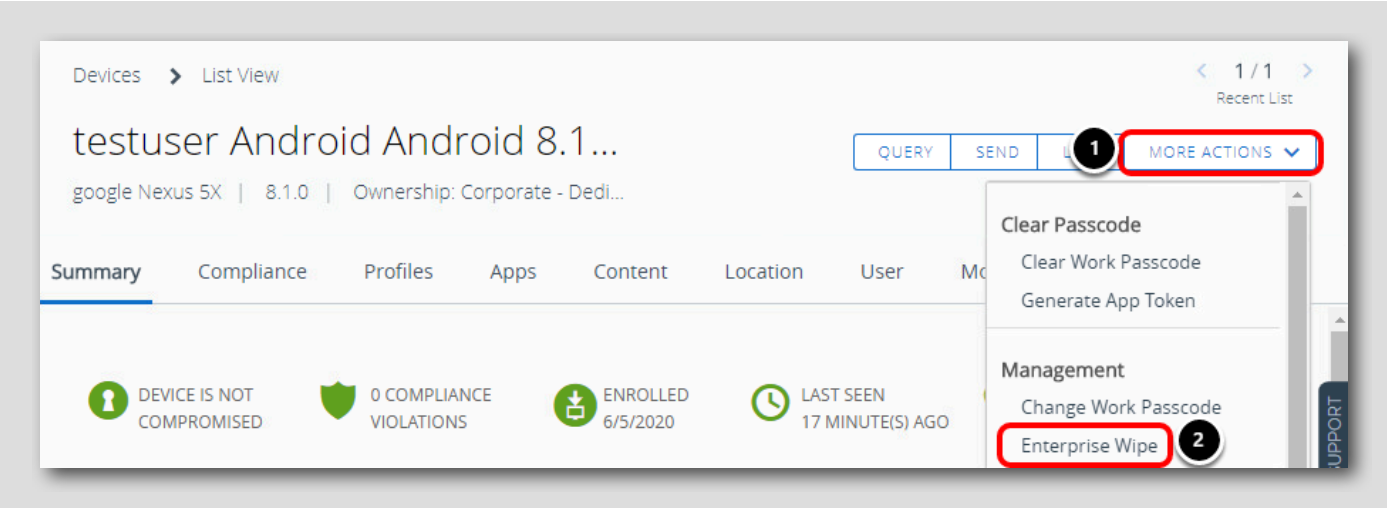
「企業情報ワイプ」では、登録時にデバイスにプッシュされたすべての設定とコンテンツが削除されます。登録前にすでにデバイス上にあった設定とコンテンツには影響しません。

デバイスに対して企業情報ワイプを実行するには、Workspace ONE UEM 管理コンソールに戻ります。

1. 左側の列で [Devices] をクリックします。
2. [List View] をクリックします。
3. 登録したデバイスのリンクをクリックします。

企業情報ワイプ オプションを見つける

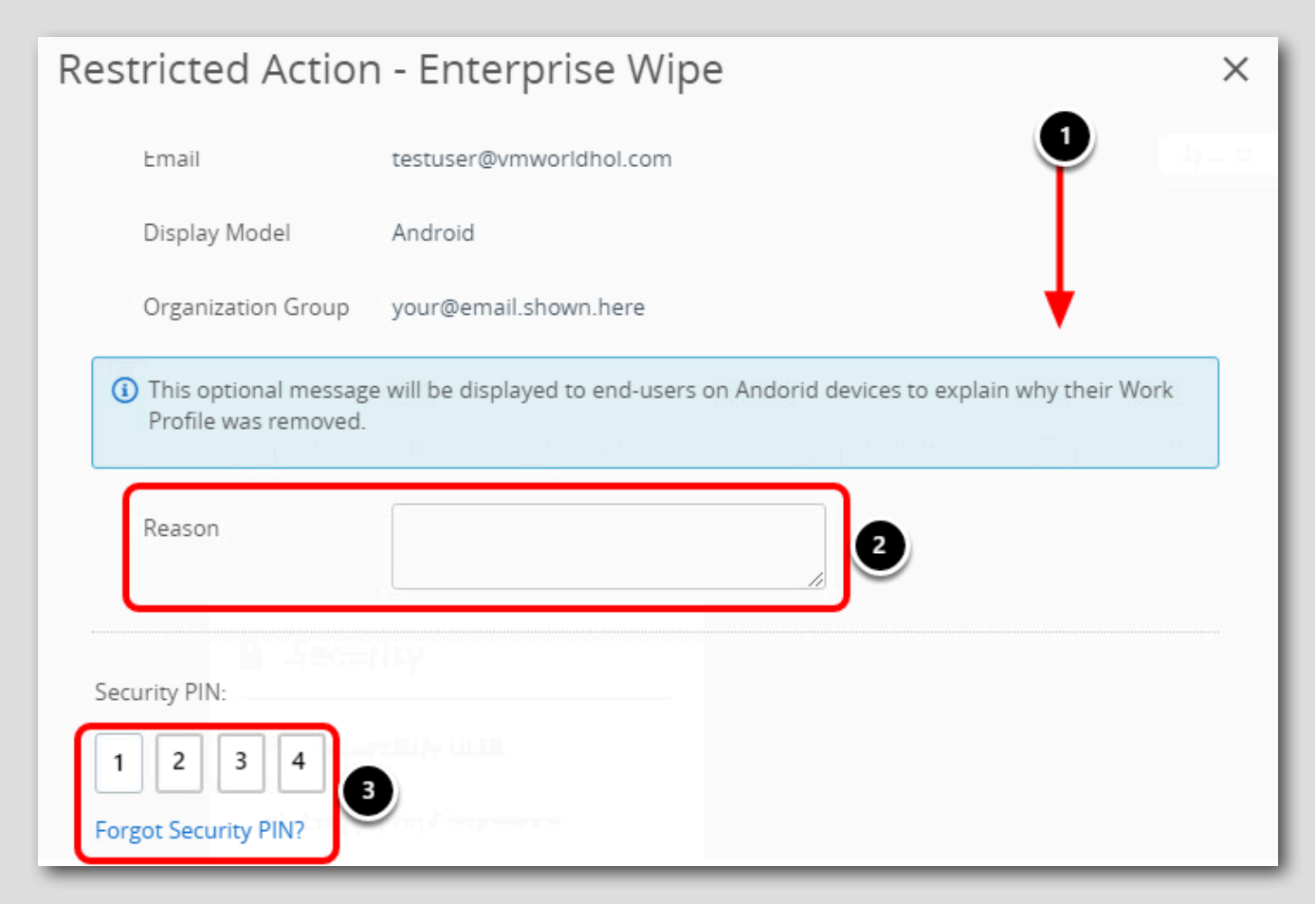
[483]



1. [More Actions] をクリックします。
2. [Management] の [Enterprise Wipe] をクリックします。

[484]

セキュリティ PIN の入力



[Enterprise Wipe] を選択すると、コンソールへのログイン後に設定したセキュリティ PIN（**1234**）を入力するよう求められます。

1. 企業情報ワイプ プロンプトの最下部までスクロールします。
2. 仕事用プロファイルが削除された理由をエンド ユーザーに送信するためのオプションのフィールドを確認します。
3. [Security PIN] に **1234** と入力します。Enter キーや [Continue] を押さなくても、PIN が正しいことを確認する「Successful」というメッセージがセキュリティ PIN 入力フィールドの下に表示されて、企業情報ワイプが要求されたことが示されます。

   注： **1234** が機能しない場合は、Workspace ONE UEM Console に最初にログインしたときに別のセキュリティ PIN が指定されています。セキュリティ PIN に指定した値を使用します。

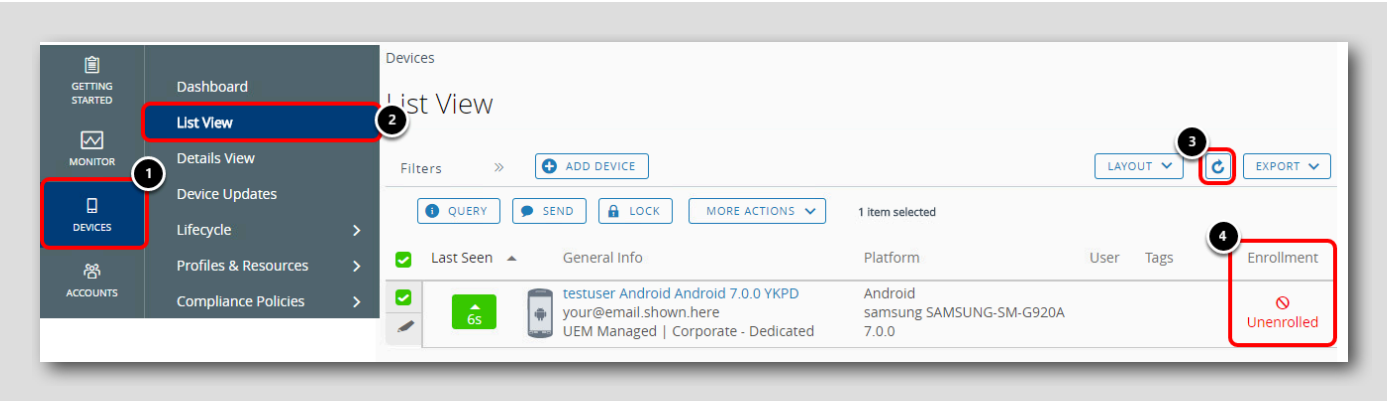
注：企業情報ワイプがすぐに実行されない場合は、次の手順に従って強制的にデバイスの同期を実行します。

1. デバイスで [Workspace ONE Intelligent Hub] アプリケーションを開きます。
2. [This Device] をタップします。
3. 一番下までスクロールして、[Sync Device] をクリックします。これによりデバイスを Workspace ONE UEM に強制的にチェックインし、登録解除が必要であることを通知します。しばらく待って、コマンドが処理されているかどうかを確認します。処理されていない場合は、手順 #4 に進みます。
4. [Enrollment] をタップします。
5. [Unenroll Device] をタップします。これにより、デバイスから登録解除コマンドを手動で処理できます。

注：ハンズオン ラボ環境内で大量のトラフィックが発生している場合、デバイスのインターネット接続やラボのインフラストラクチャの即応性によっては、この処理に 2 ～ 3 分以上かかることがあります。

デバイスが登録解除されたことの確認（コンソール）

[485]

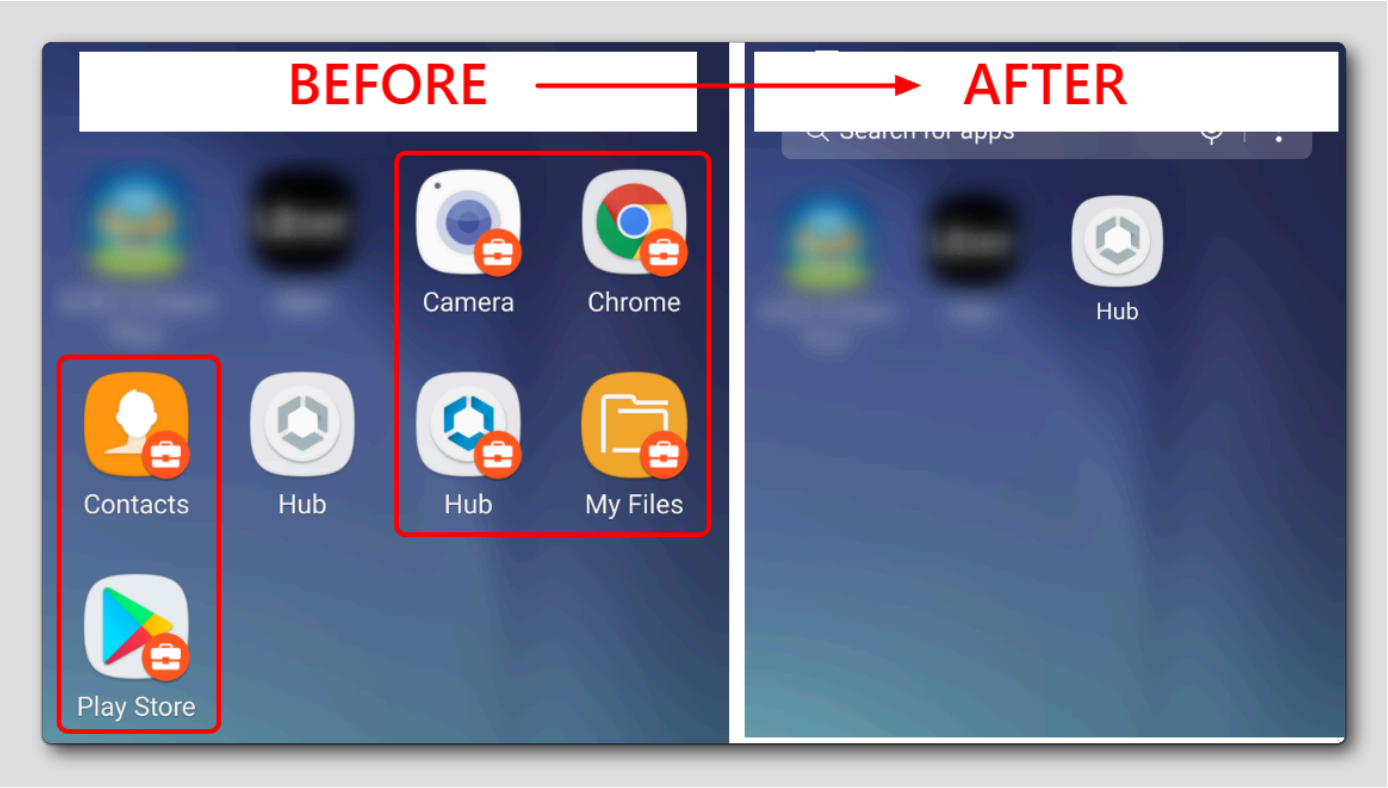


1. [Devices] をクリックします。
2. [List View] をクリックします。
3. [Device List View] 画面の [Refresh] ボタンをクリックします。
4. デバイスの登録ステータスが [Unenrolled] と表示されているかどうかを確認します。表示されていない場合は、デバイスに「Unenrolled」と表示されるまでページを更新し続けます。

注：デバイスのインターネット接続によっては、この処理には数分かかることがあります。

デバイスが登録解除されたことの確認（デバイス）

[486]



デバイスで、デバイスの登録解除後にバッジ付きアプリケーションが削除され、登録後にデバイスにプッシュされた構成が削除されたことを確認します。

Android Enterprise の詳細情報

[487]

これは、Workspace ONE UEM と統合された Android Enterprise で表示される機能の一例です。機能の詳細については、VMware End User Computing 担当者にお問い合わせいただくか、当社の Web サイト (*http://www.workspaceone.com/*) または Android Enterprise の Web

サイト (*https://www.android.com/enterprise*) を参照してください。

まとめ

[488]

仕事用プロファイルは、個人用 (BYOD) デバイス専用に設計されています。企業で Android を使用している場合、Workspace ONE UEM は、デバイスの個人スペースと企業スペースを分離するコンテナである「仕事用プロファイル」を作成します。Workspace ONE UEM は、仕事用プロファイルを完全に制御できますが、個人用プロファイルを制御することはできません。

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[489]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。

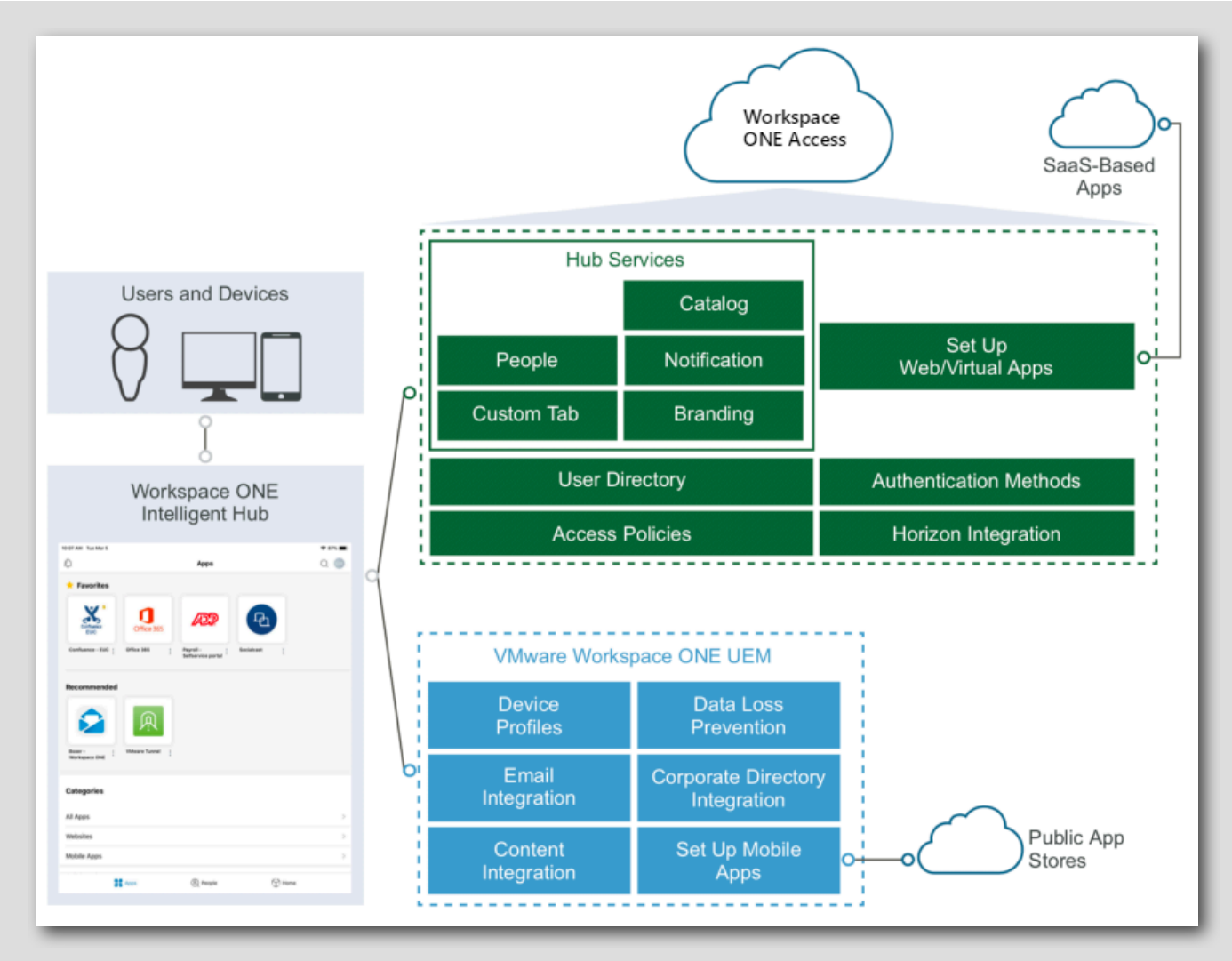

Your Personal journey from zero to IT Superhero
TECH ZONE
Hands on Labs, Tools and Best Practices
How the products work – beginner to expert
Guide to production deployments & operations
Quick start for your first proof of concept
Latest product information

モジュール 6：Workspace ONE Intelligent Hub と Hub サービスの概要（60 分）

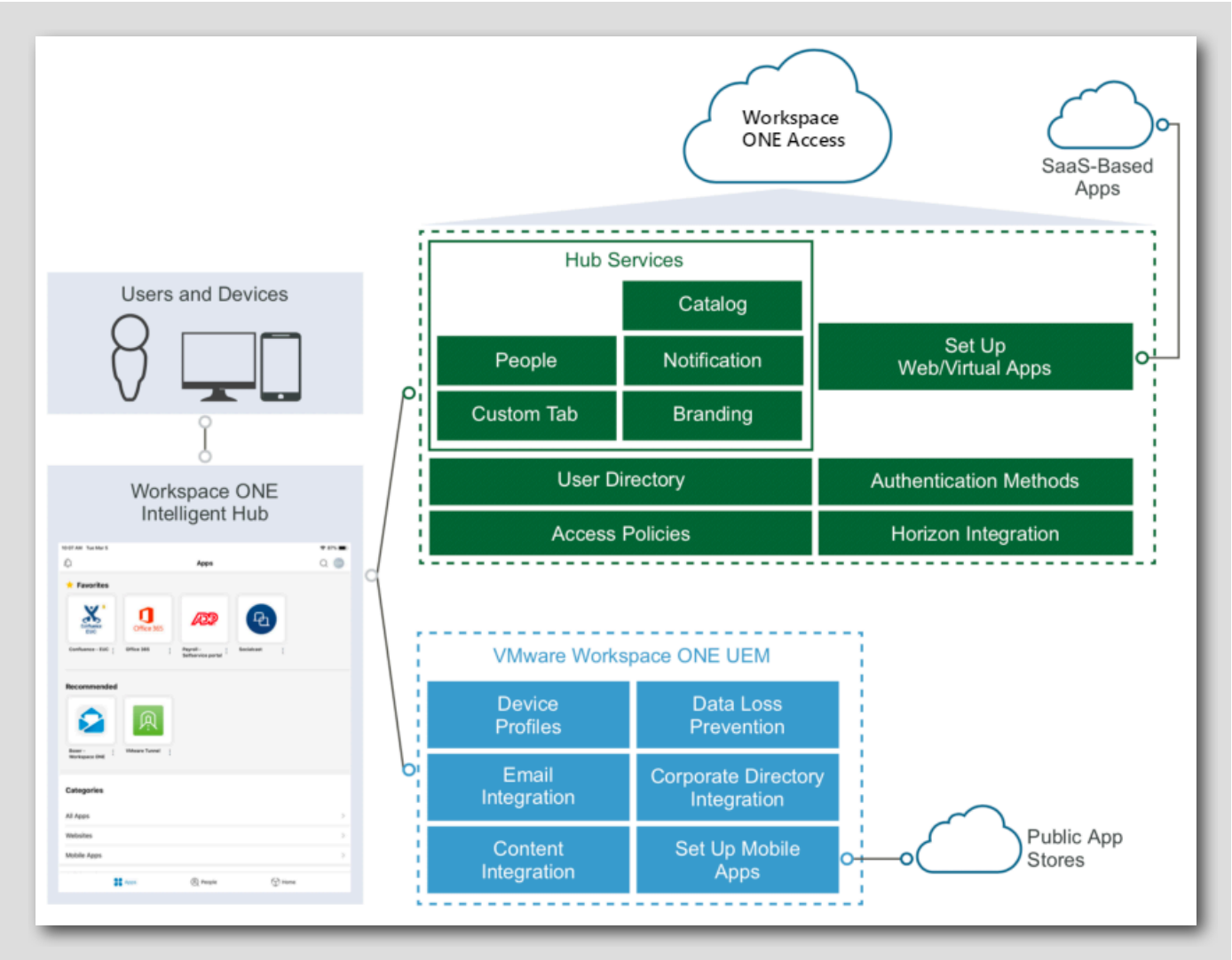
はじめに

[491]

Workspace ONE Intelligent Hub は、場所を問わず、セキュアなアクセス、検出、常時接続、生産性の向上を実現する、VMware の次世代の従業員エンゲージメント アプリケーションです。レガシーのエージェント アプリケーションに代わるものであり、Hub サービスとの組み合わせにより、Workspace ONE によって提供される ID、アプリケーション、エンタープライズ モビリティ管理機能を強化します。



Intelligent Hub は、ブラウザを介して iOS、Android、macOS、Windows 10 上の統合アプリケーション カタログ、アクセス コントロール、およびアプリケーション管理を統合します。多くの Intelligent Hub 機能の前提条件は、Workspace ONE Access 内で Hub サービス コンポーネントを有効にすることにあります。Hub サービスの有効化後、展開が Workspace ONE Access と統合されているかどうかに基づいて、Intelligent Hub 機能をカスタマイズできます。



Workspace ONE Access なしの Hub サービス

[492]

Workspace ONE Access と統合されていない場合、Hub カタログを構成してネイティブ モバイル アプリケーションおよび Web アプリケーションへのアクセスを許可したり、カスタム タブを作成したりすることができます。また、Workspace ONE Intelligent Hub アプリケーションをブランディングして会社のロゴと色のプロファイルを追加することもできます。

Workspace ONE Access ありの Hub サービス

[493]

Workspace ONE Access が Workspace ONE UEM と統合されている場合、People Search や通知などの追加の Hub 機能および認証とシングル サインオンなどの ID 関連機能を使用して、ユーザーのために完全なデジタル ワークスペース環境を作成できます。

このラボでは、Hub サービス内のいくつかの機能を構成し、ブラウザ バージョンの Intelligent Hub で結果を表示します。

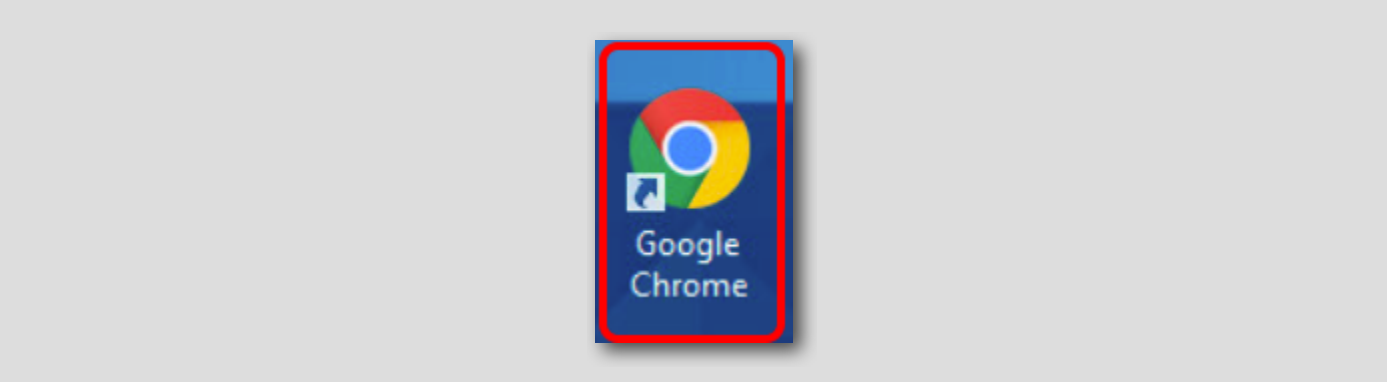
Workspace ONE UEM Console へのログイン

[494]

このラボを開始するには、Workspace ONE UEM 管理コンソールにログインする必要があります。

Chrome ブラウザの起動

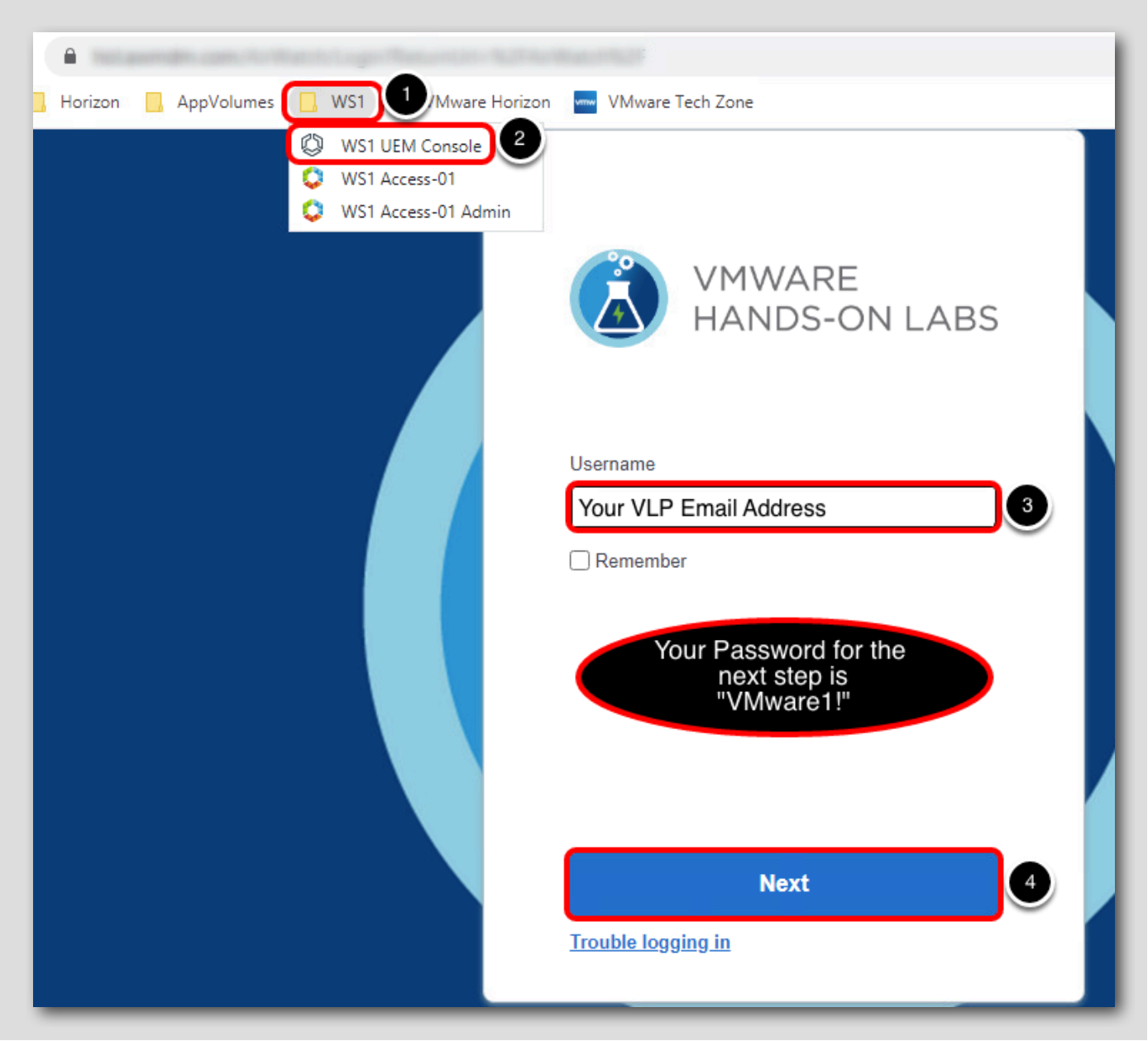
[495]



現在接続している仮想マシンのデスクトップから、[Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールへのログイン

[496]

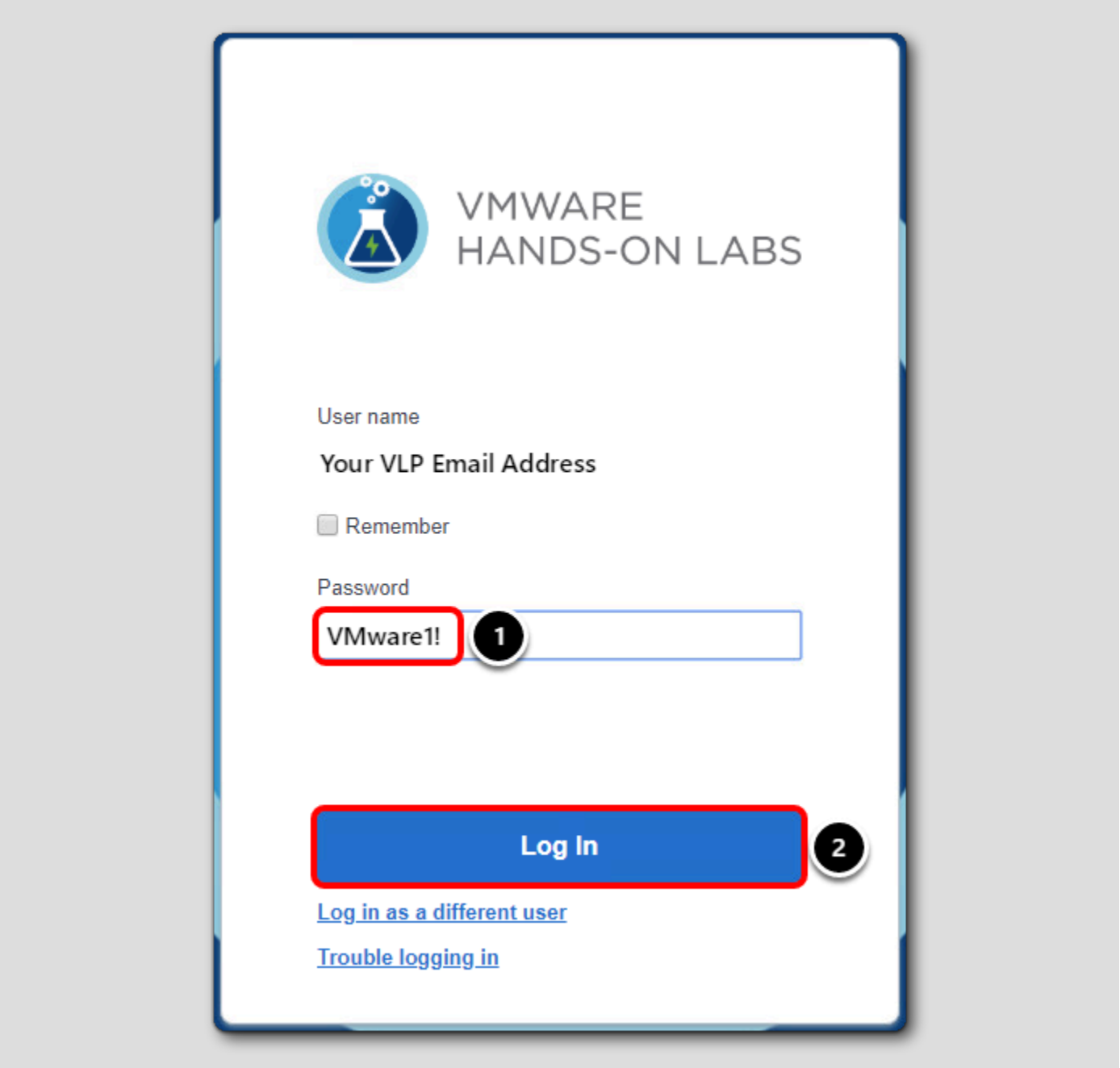


1. [WS1] ブックマーク フォルダをクリックします。
2. [WS1 UEM Console] リンクをクリックします。
3. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。

   注： 次の手順のパスワードは、**`VMware1!`** になります。

4. [Next] をクリックします。

Workspace ONE UEM Console の認証情報の入力 [497]



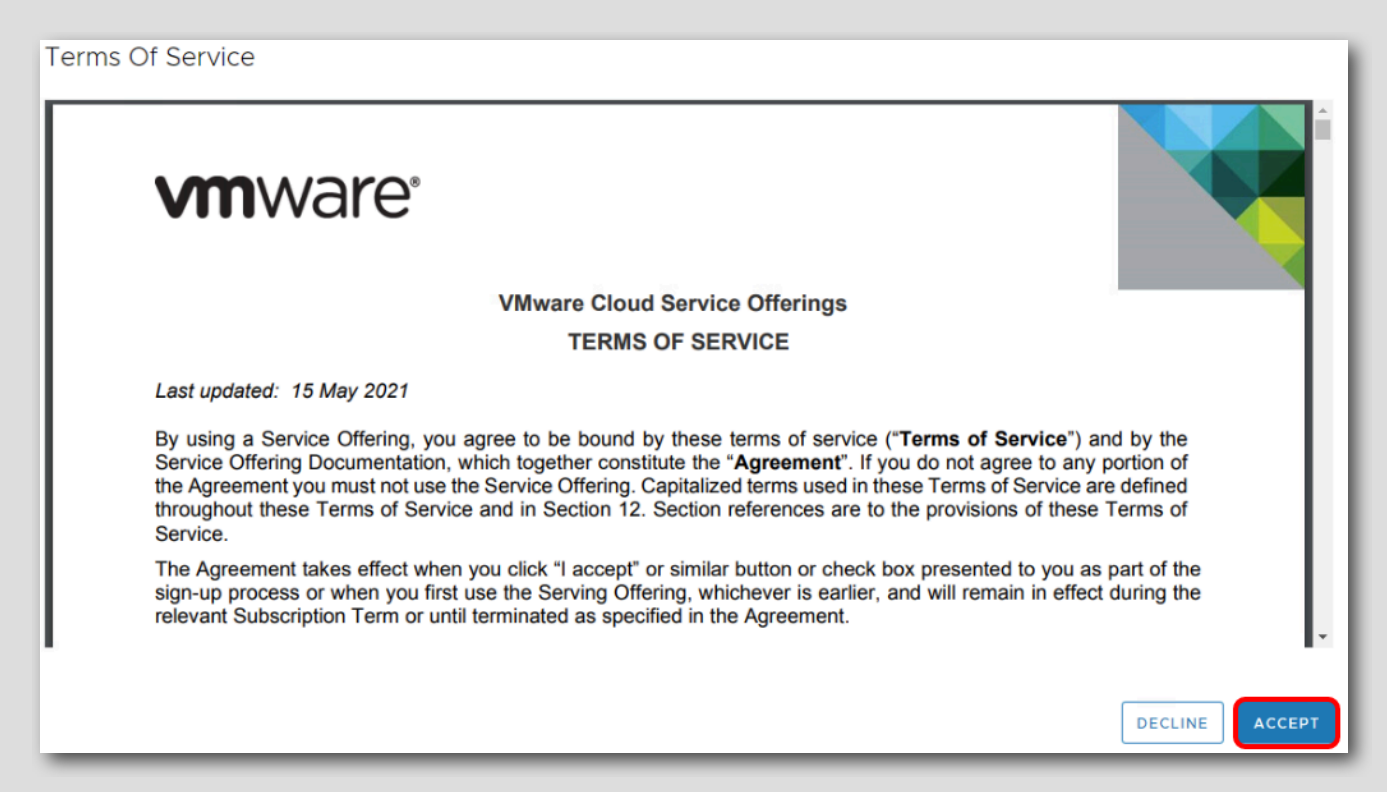
[Password] フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

利用規約の承諾

[498]



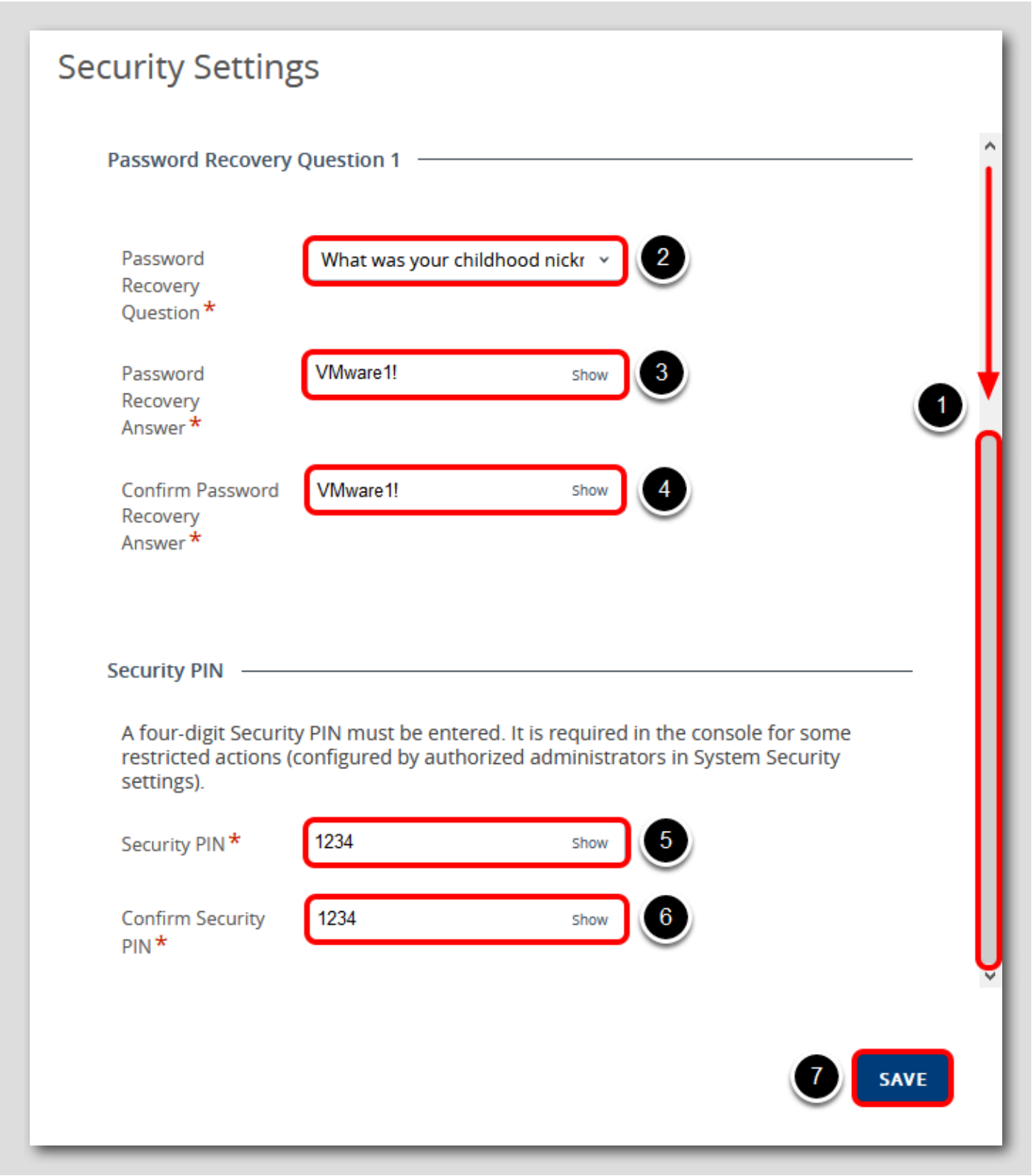
[Workspace ONE UEM Terms of Service] が表示されたら、[Accept] ボタンをクリックします。

注：以降の手順は、管理コンソールへの初回ログイン時にのみ実行されます。

初期セキュリティ設定の完了

[499]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

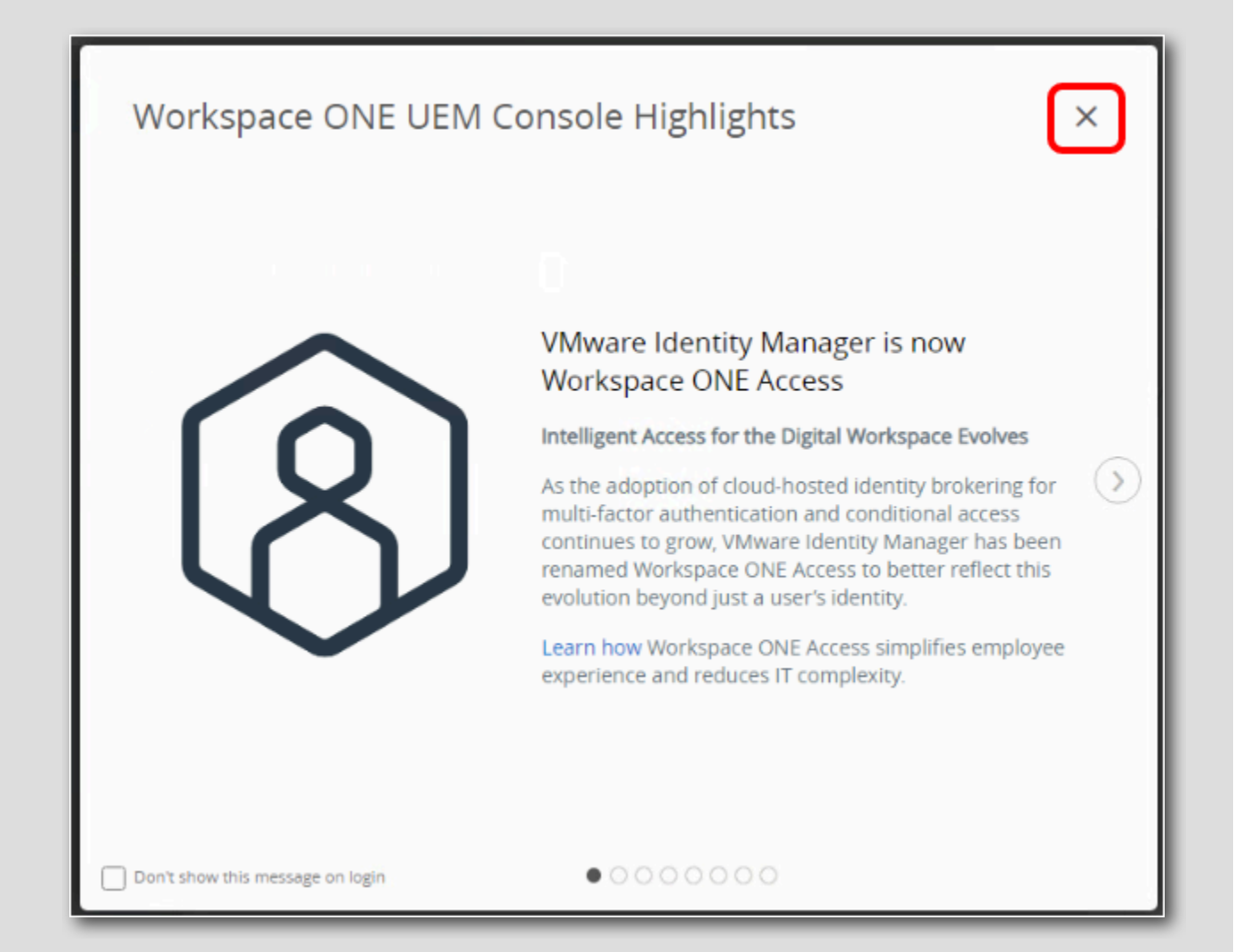

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示します。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[500]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

Workspace ONE Access テナントの詳細へのアクセス

[501]

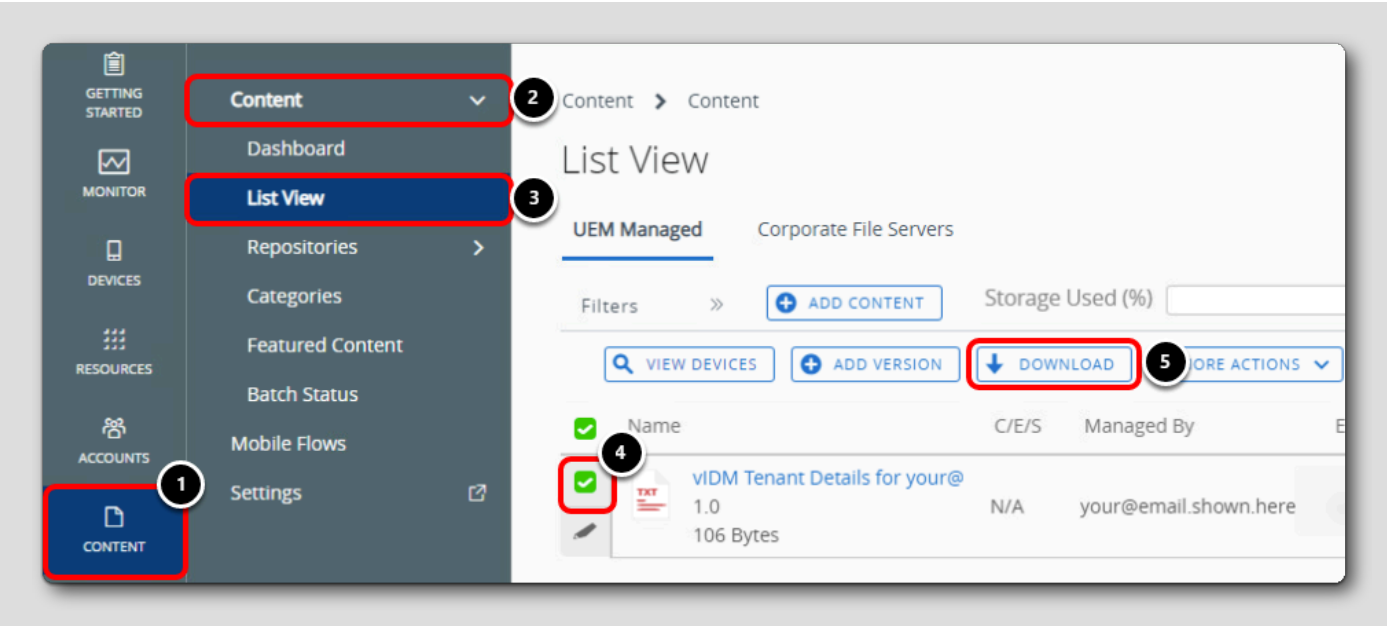
Workspace ONE Intelligent Hub エンドユーザー サービスは、Hub サービス管理コンソールを介して構成されます。Hub サービスは、Workspace ONE Access と同じ場所にあります。Hub サービスはサーバ側のコンポーネントであり、Intelligent Hub はエンドユーザー クライアントと考えてください。

以降のセクションでは、Workspace ONE Access テナントへのアクセス、ログイン、Hub サービス管理コンソールへのアクセスについて説明します。

UEM Console での Workspace ONE Access テナントの詳細へのアクセス

[502]

このラボ全体を通じて使用するために、一時的な Workspace ONE Access テナントが生成されています。Workspace ONE Access のテナント URL とログインの詳細が、ラボの最初に Workspace ONE UEM Console の [Content] セクションにアップロードされました。

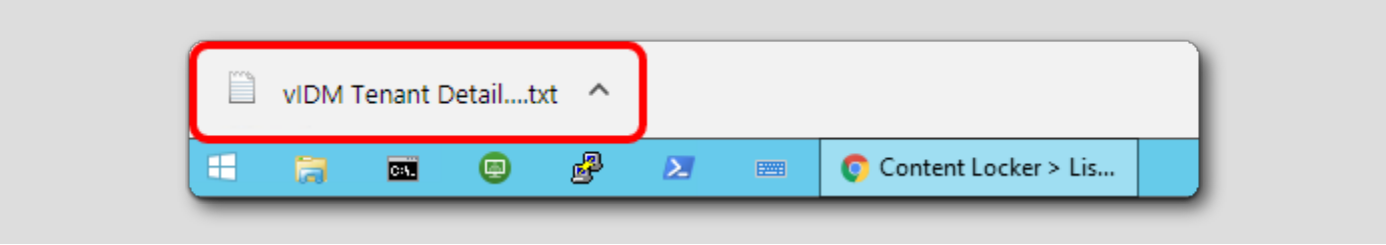


Workspace ONE UEM Console で、次のように操作します。

1. 左端の [Content] をクリックします。
2. 上部の [Content] を展開します。
3. [List View] をクリックします。
4. `vIDM Tenant Details for your@email.shown.here.txt` という名前のテキスト ファイルを見つけ、その横にあるチェックボックスをクリックしてファイルを選択します。
5. [Download] をクリックします。

ダウンロードしたテキスト ファイルを開く

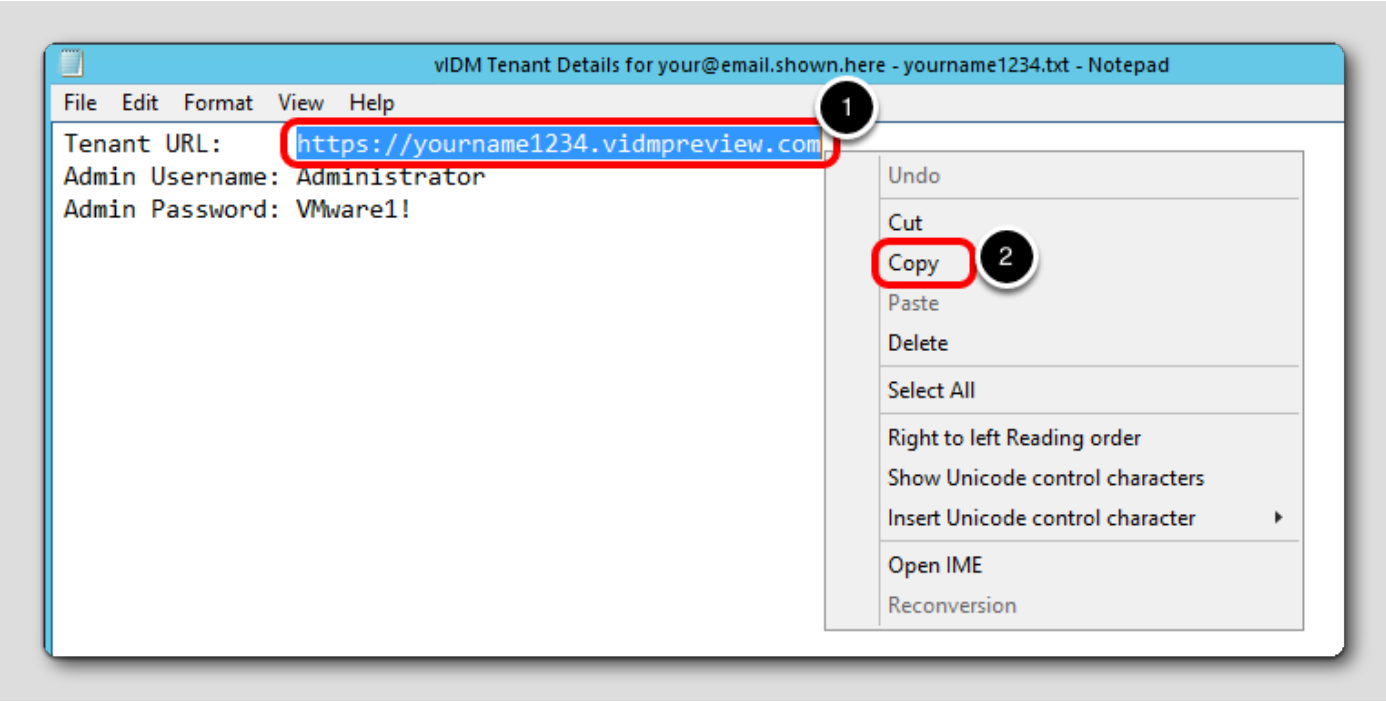
[503]



ファイルのダウンロード後、ダウンロード バーから「vIDM Tenant Details for your@email.shown.here.txt」ファイルをクリックして開きます。

テナント URL のコピー

[504]



1. [Tenant URL] テキストを選択して右クリックします。
2. [Copy] をクリックします。

注：テナント名は Workspace ONE UEM Console のグループ ID と一致します。

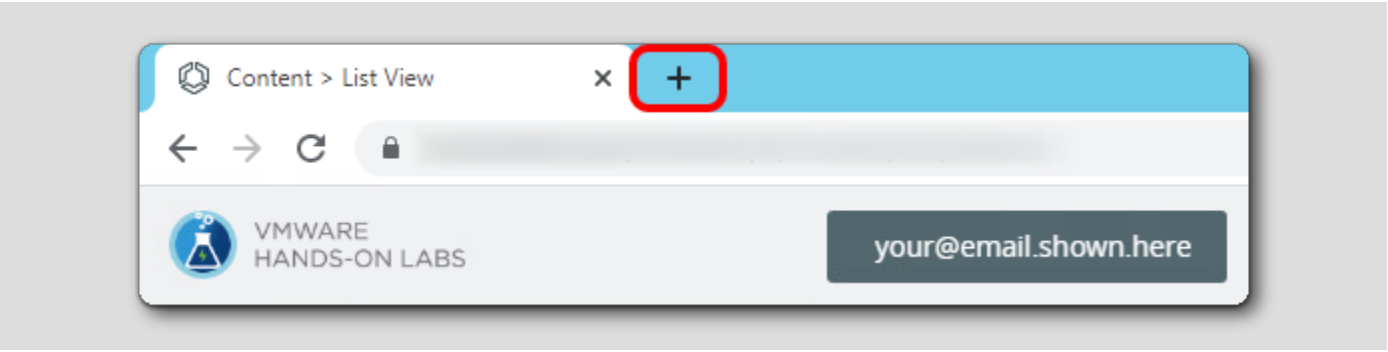
Workspace ONE Access 管理コンソールへのログイン

[505]

このセクションでは、Workspace ONE Access 管理コンソールにログインし、Hub サービス管理コンソールにアクセスします。

新しいブラウザ タブを開く

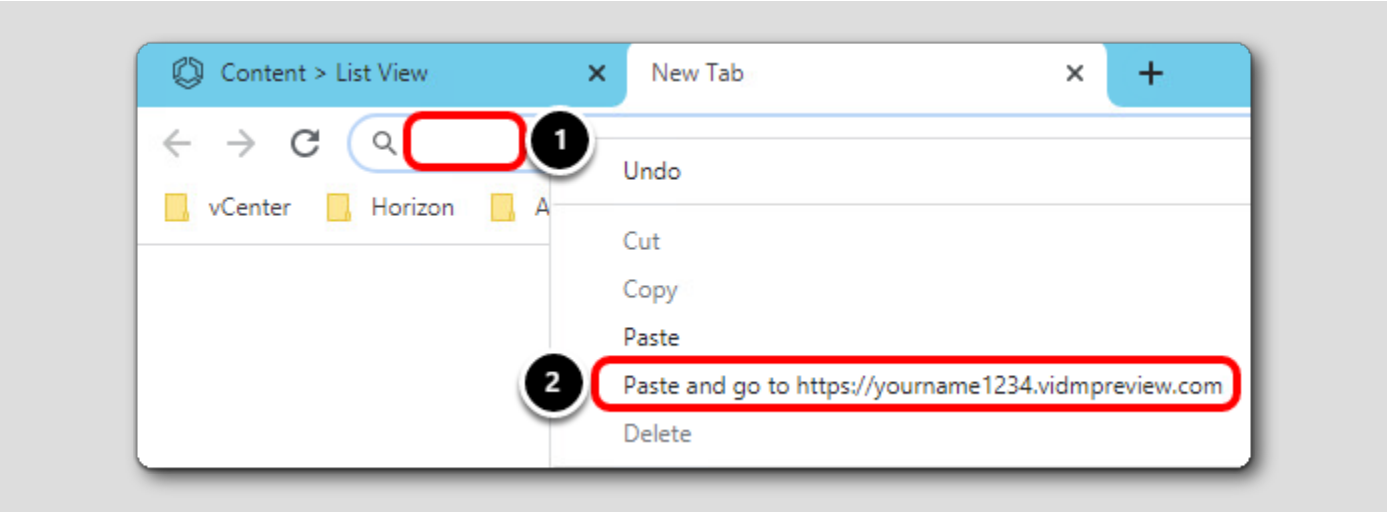
[506]



ブラウザで [Add Tab] ボタンをクリックして、新しいタブを開きます。

Workspace ONE Access テナント URL への移動

[507]

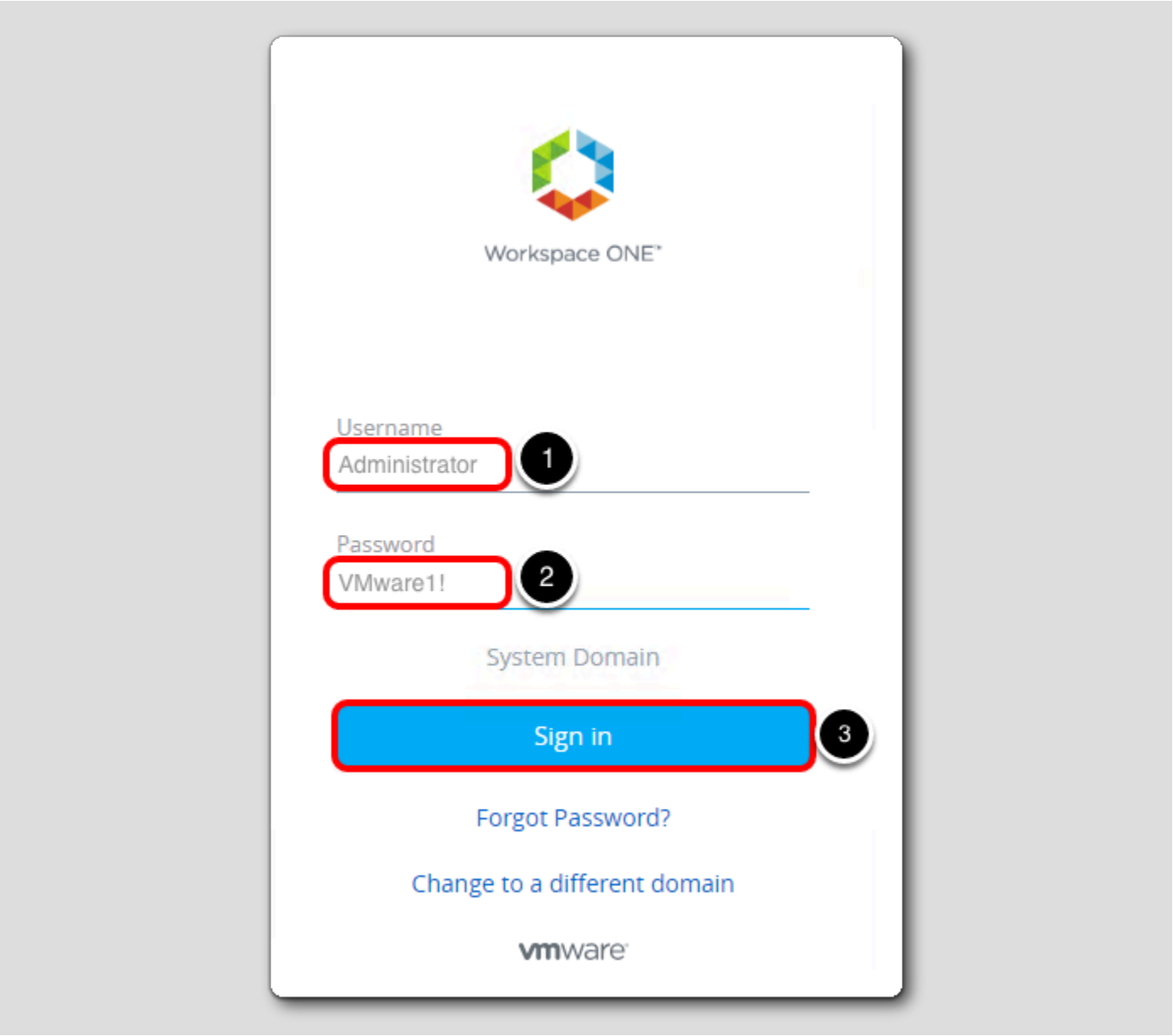


1. 新しいタブのアドレス バーの内側を右クリックします。
2. [Paste] をクリックして、URL に移動します。

注：これは、前の手順で取得した Workspace ONE Access テナント URL です。前の手順でこの情報をコピーまたはメモしていない場合は、前の手順に戻り、テナント URL をメモしておきます。

Workspace ONE Access テナントへのログイン

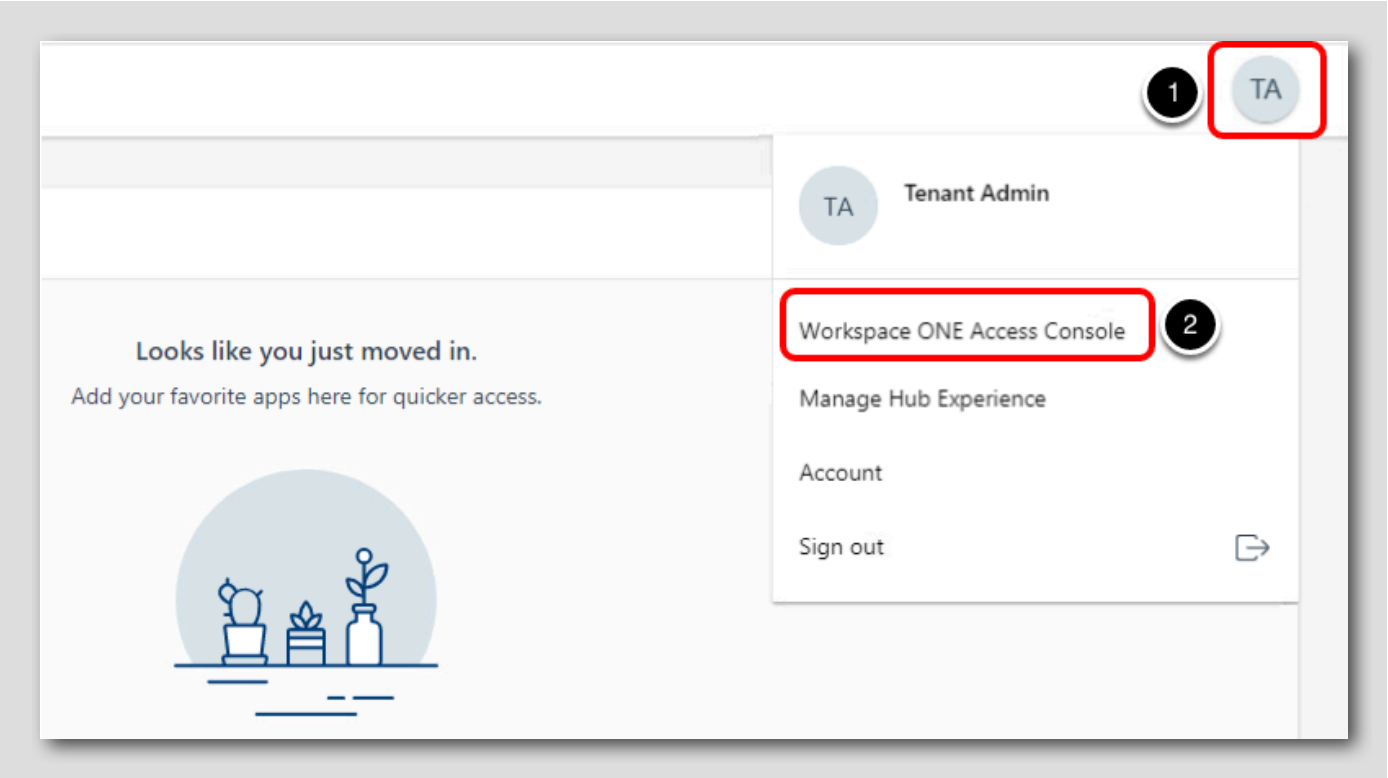
[508]



1. [Username] に **Administrator** と入力します。
2. [Password] に **VMware1!** と入力します。
3. [Sign In] をクリックします。

管理コンソールへの移動

[509]



ログイン後、上の図のように Intelligent Hub ユーザー ポータルが表示されます。管理コンソールに移動する必要があります。

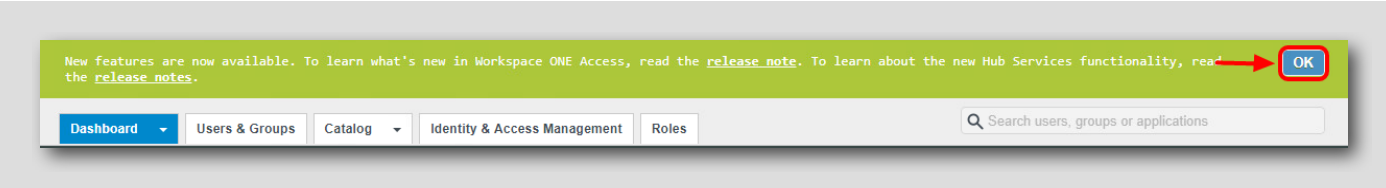
1. 右上にある**円形のユーザー ドロップダウン メニュー**をクリックします。
2. **[Workspace ONE Access Console]** をクリックします。

これにより、管理コンソールがブラウザの別のタブで開きます。

注：上記のビューが表示されていない場合は、すでに管理コンソールが表示されているので、この手順をスキップできます。

（オプション）リリース ノートのバナーを閉じる

[510]



リリース ノートの詳細についてのバナーが表示されている場合は、右端の [OK] をクリックして閉じます。

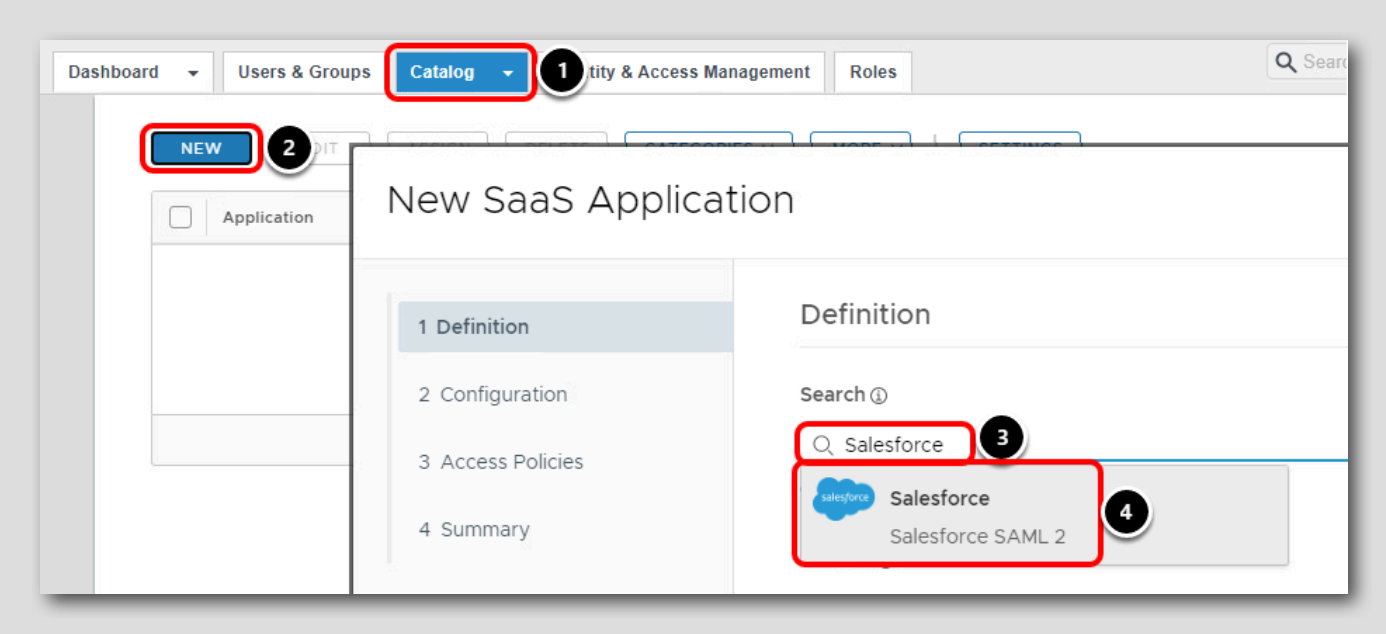
アプリケーション カタログへの SaaS アプリケーションの追加

[511]

後のセクションで使用するサンプルの SaaS アプリケーションをアプリケーション カタログに追加します。

Workspace ONE Access の [App Catalog] への移動と SaaS アプリケーションの追加

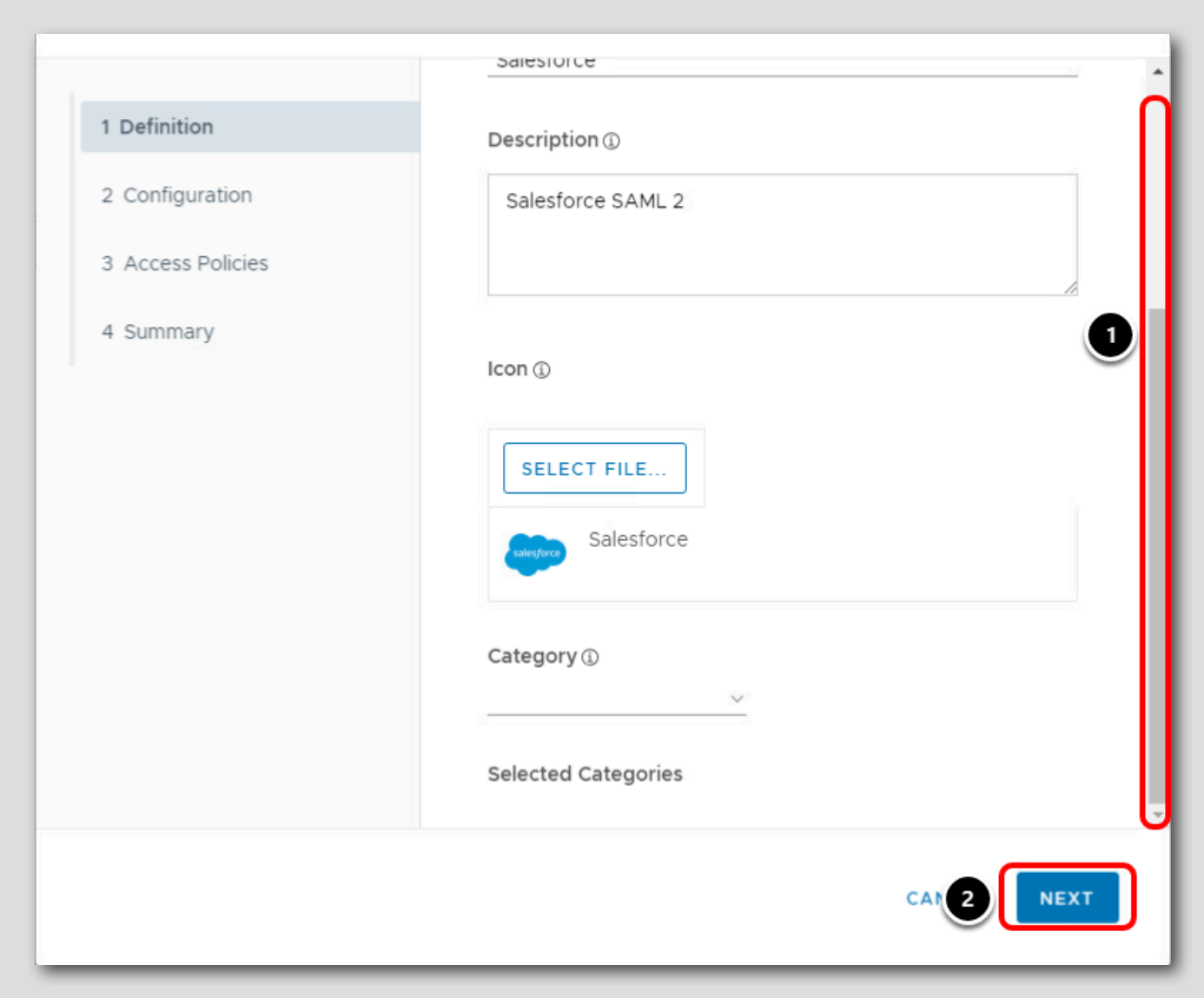
[512]



1. [Catalog] タブをクリックします（注：[Catalog] タブの下矢印はクリックしないでください。代わりに、[Catalog] をクリックします）。
2. [NEW] ボタンをクリックします。
3. 検索フィールドに **Salesforce** と入力します。
4. 検索結果で Salesforce をクリックします。

新しい SaaS アプリケーションの [Definition] セクション

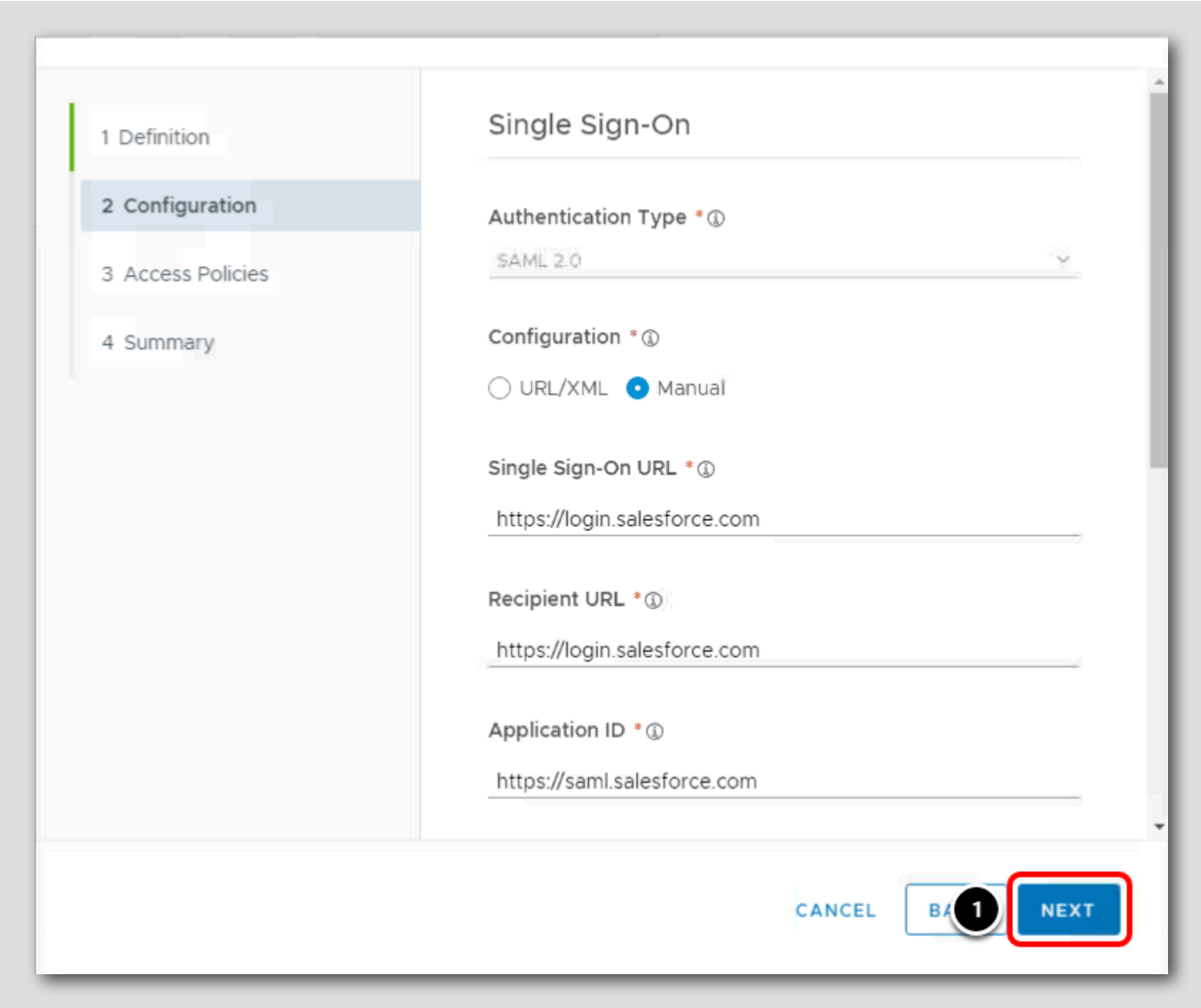
[513]



1. 下にスクロールします。
2. [NEXT] ボタンをクリックします。

新しい SaaS アプリケーションの [Configuration] セクション

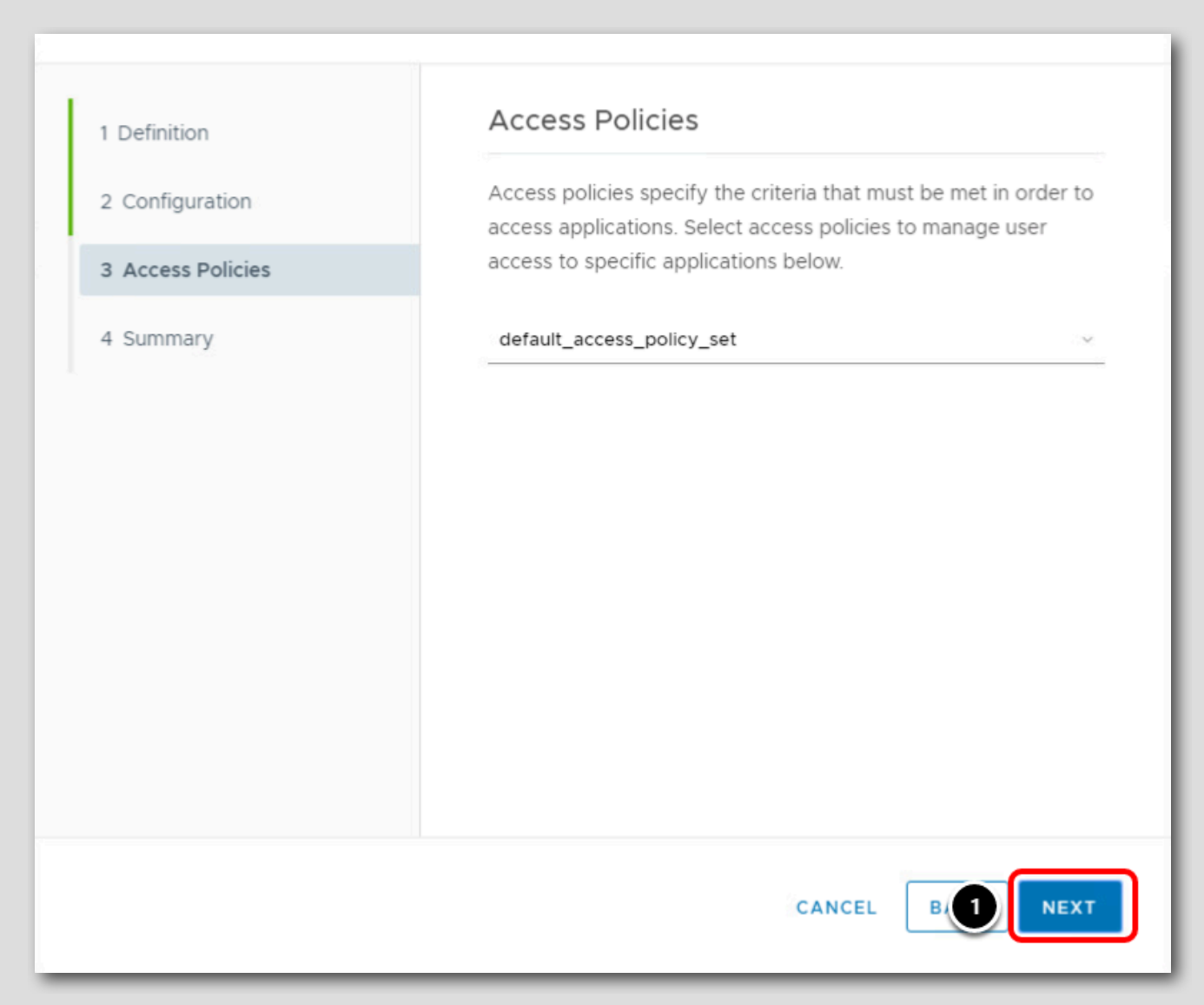
[514]



1. デフォルト設定のまま、[NEXT] をクリックします。

新しい SaaS アプリケーションの [Access Policies] セクション

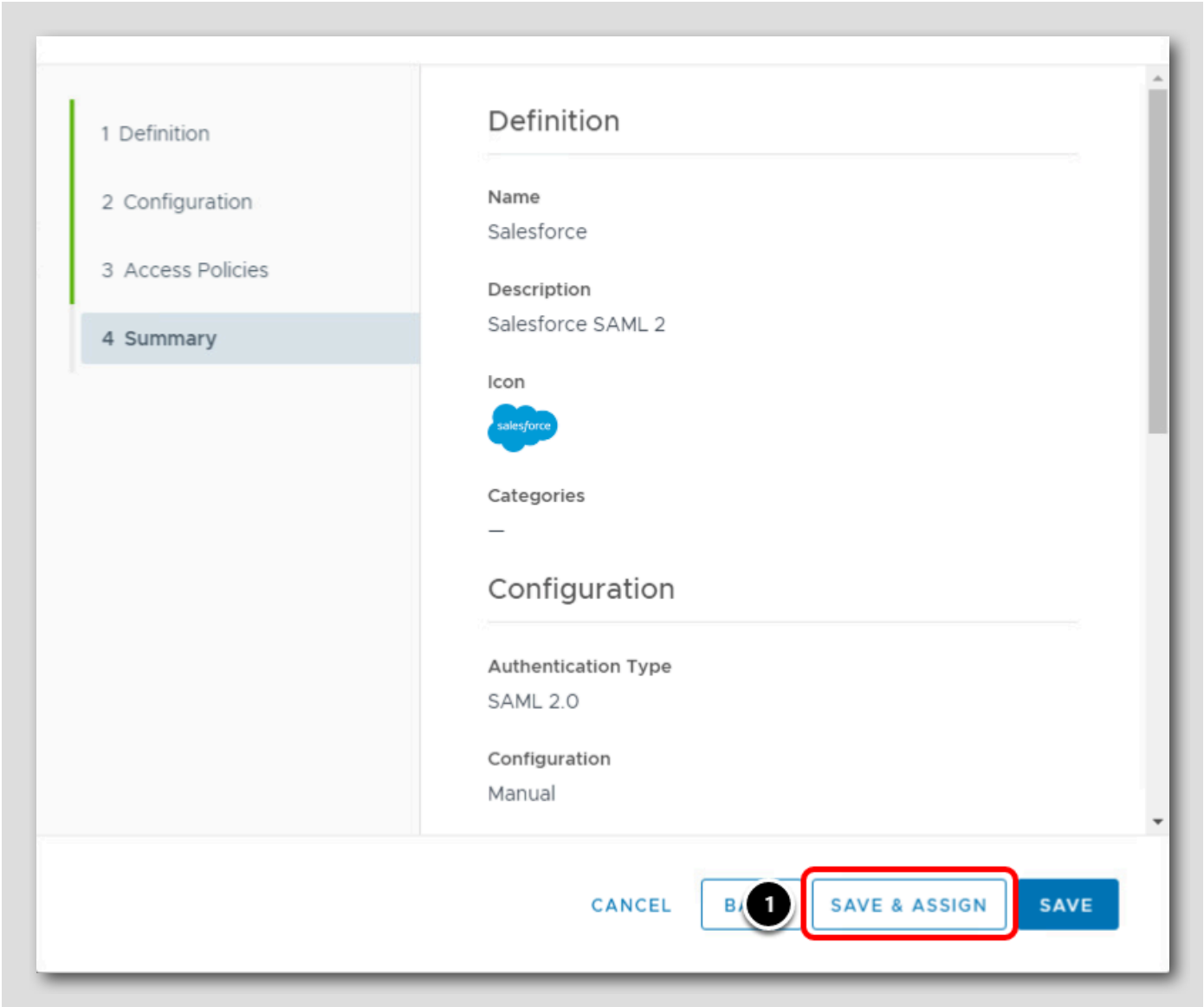
[515]



1. デフォルトのアクセス ポリシーを保持し、[NEXT] をクリックします。

新しい SaaS アプリケーションの [Summary] セクション

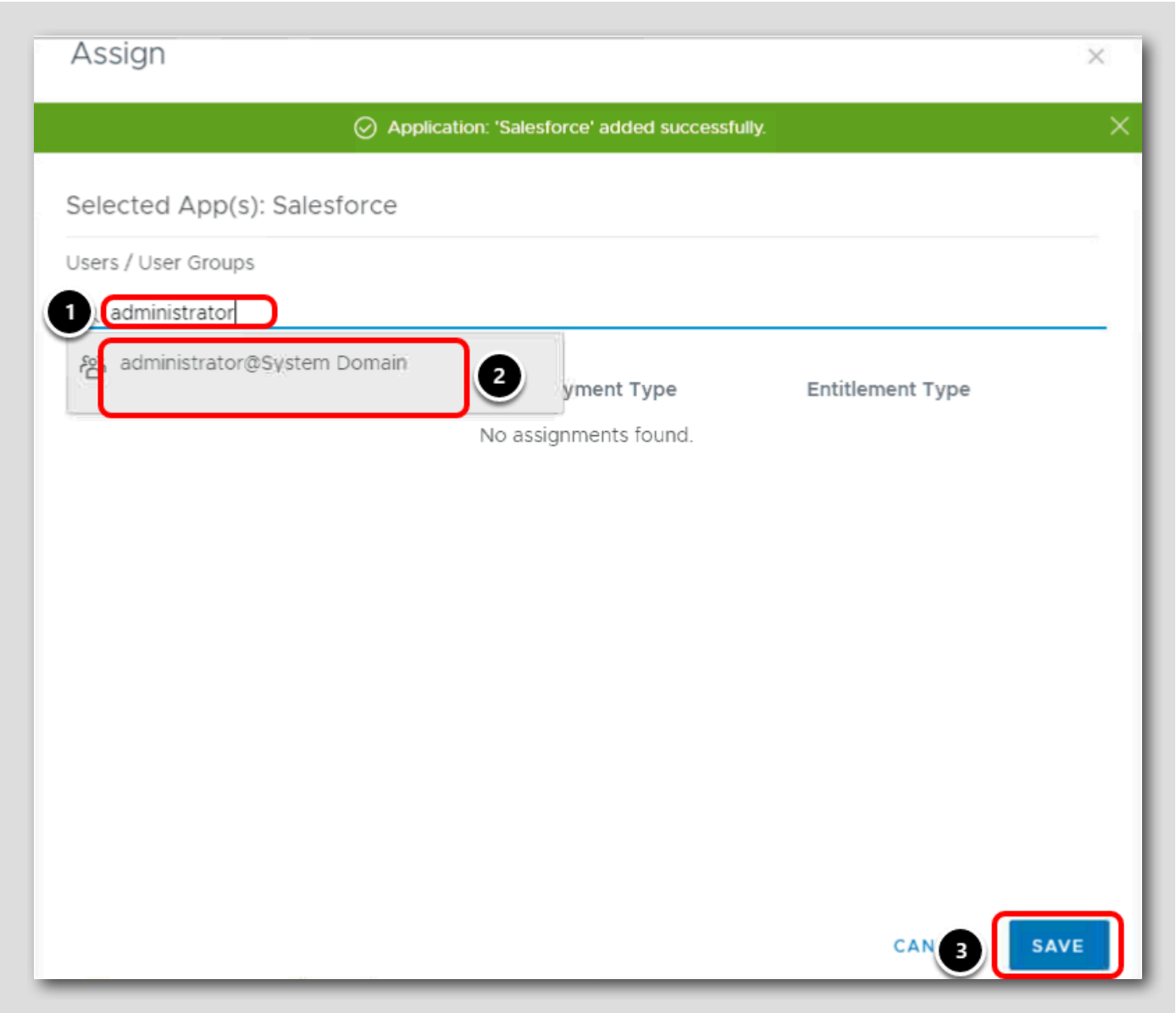
[516]



1. [SAVE & ASSIGN] をクリックします。

新しい SaaS アプリケーションをユーザーに割り当てる

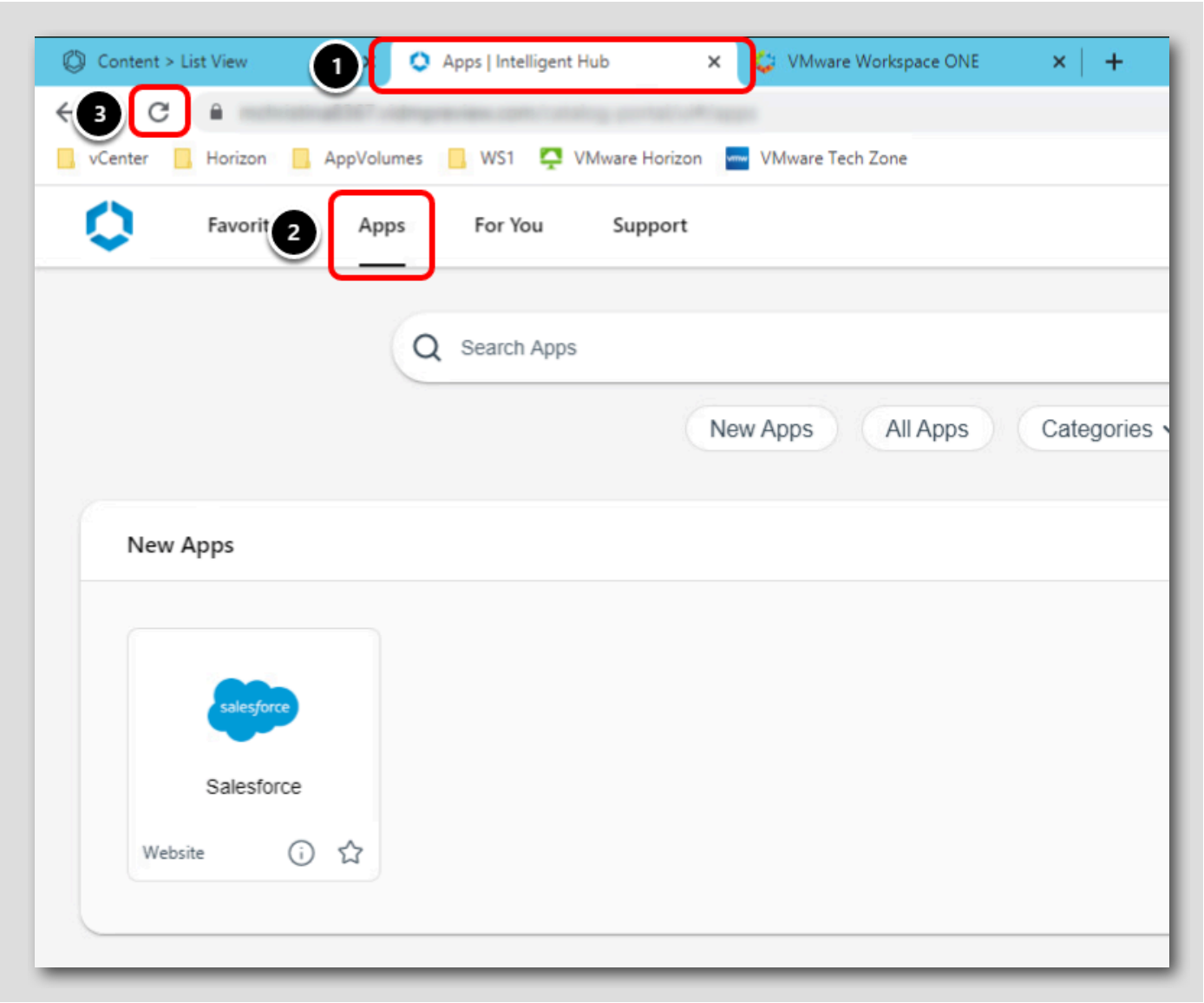
[517]



1. [Users/ User Groups] 検索フィールドに **administrator** と入力します。
2. 検索結果で administrator@System Domain をクリックします。
3. [SAVE] をクリックします。

SaaS アプリケーションがユーザーのカタログに追加されたことの確認

[518]

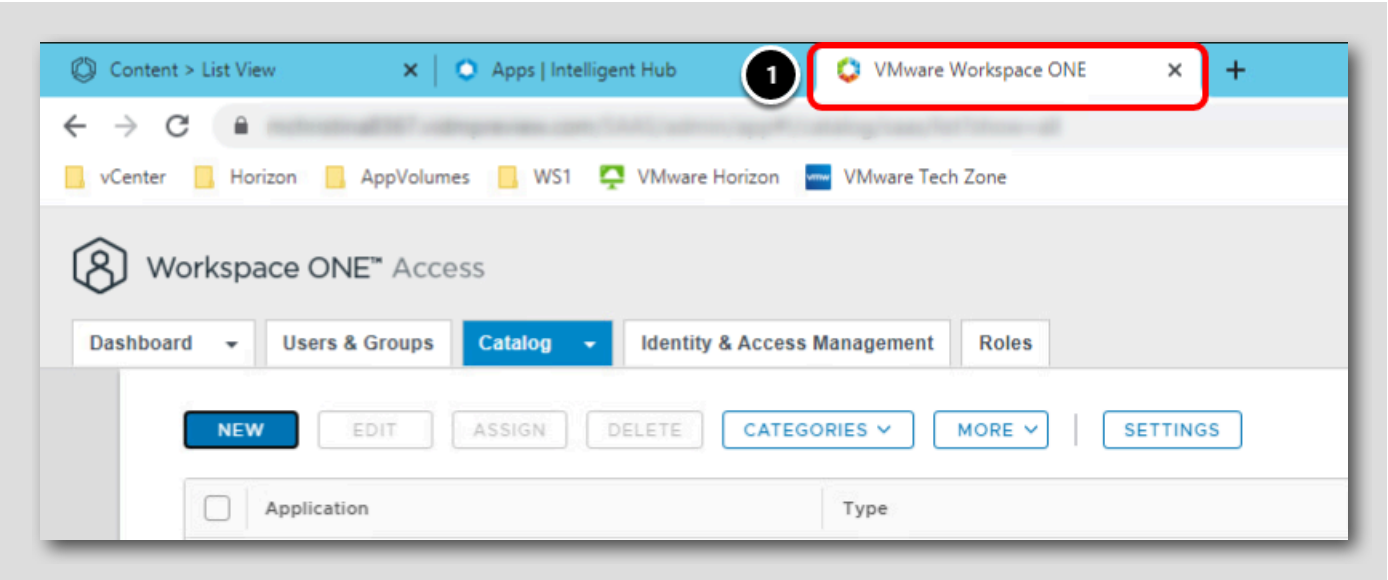


1. クリックして、**ブラウザの 2 番目のタブ**に戻ります。これは、Intelligent Hub ユーザー ポータルです。
2. **[Apps]** タブをクリックして、アプリケーション カタログを表示します。
3. ブラウザの **[Refresh]** ボタンをクリックして、カタログを更新します。アプリケーション カタログに Salesforce が表示されます。

Hub サービス管理コンソールへの移動と Hub テンプレート ウィザードの完了 [519]

次のセクションでは、Hub サービス管理コンソールで始めて、Hub テンプレートについて説明します。

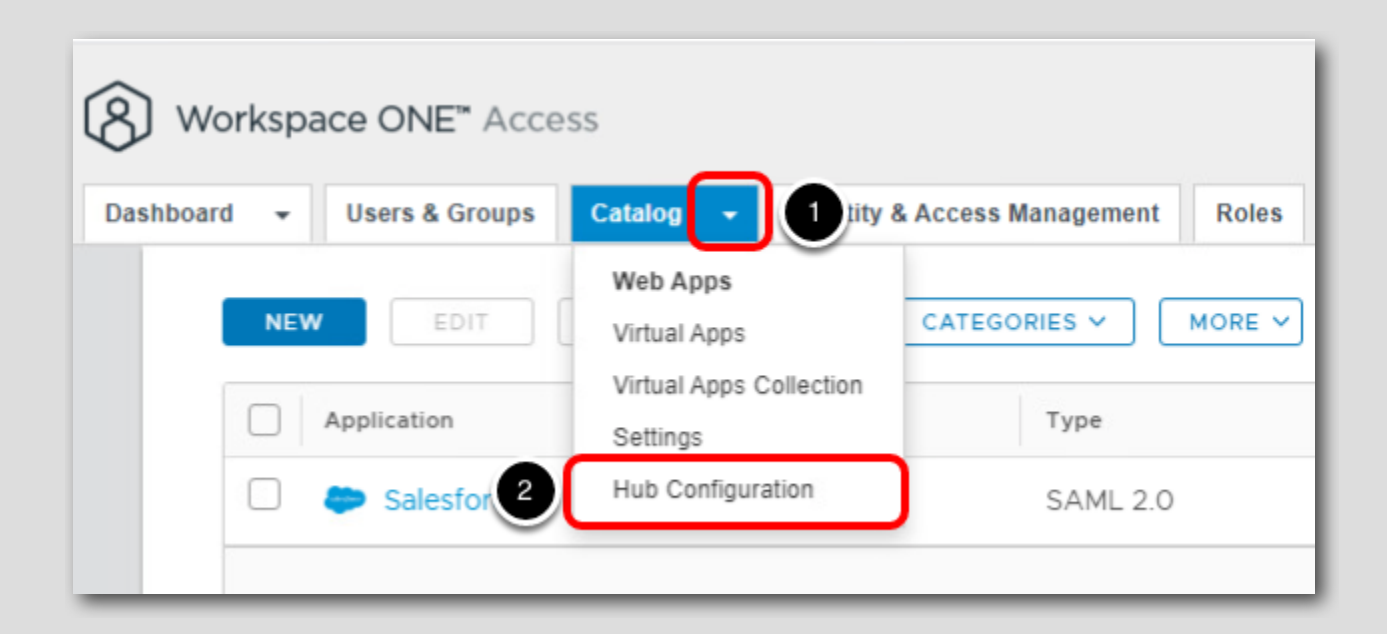
Workspace ONE Access 管理コンソールに戻る [520]



1. ブラウザの 3 番目のタブをクリックして、Workspace ONE Access 管理コンソールに戻ります。

Hub サービス管理コンソールへの移動

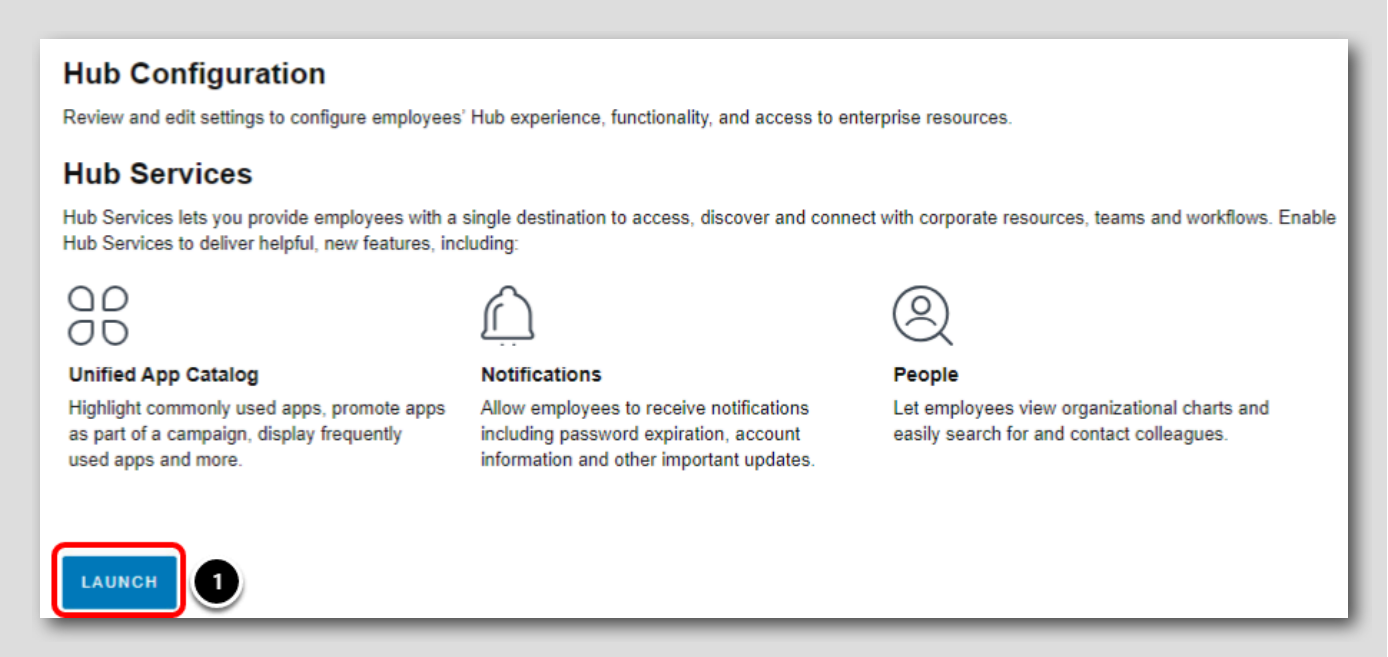
[521]



1. [Catalog] タブを見つけて,下矢印をクリックします。
2. [Hub Configuration] をクリックします。

Hub サービスの起動

[522]



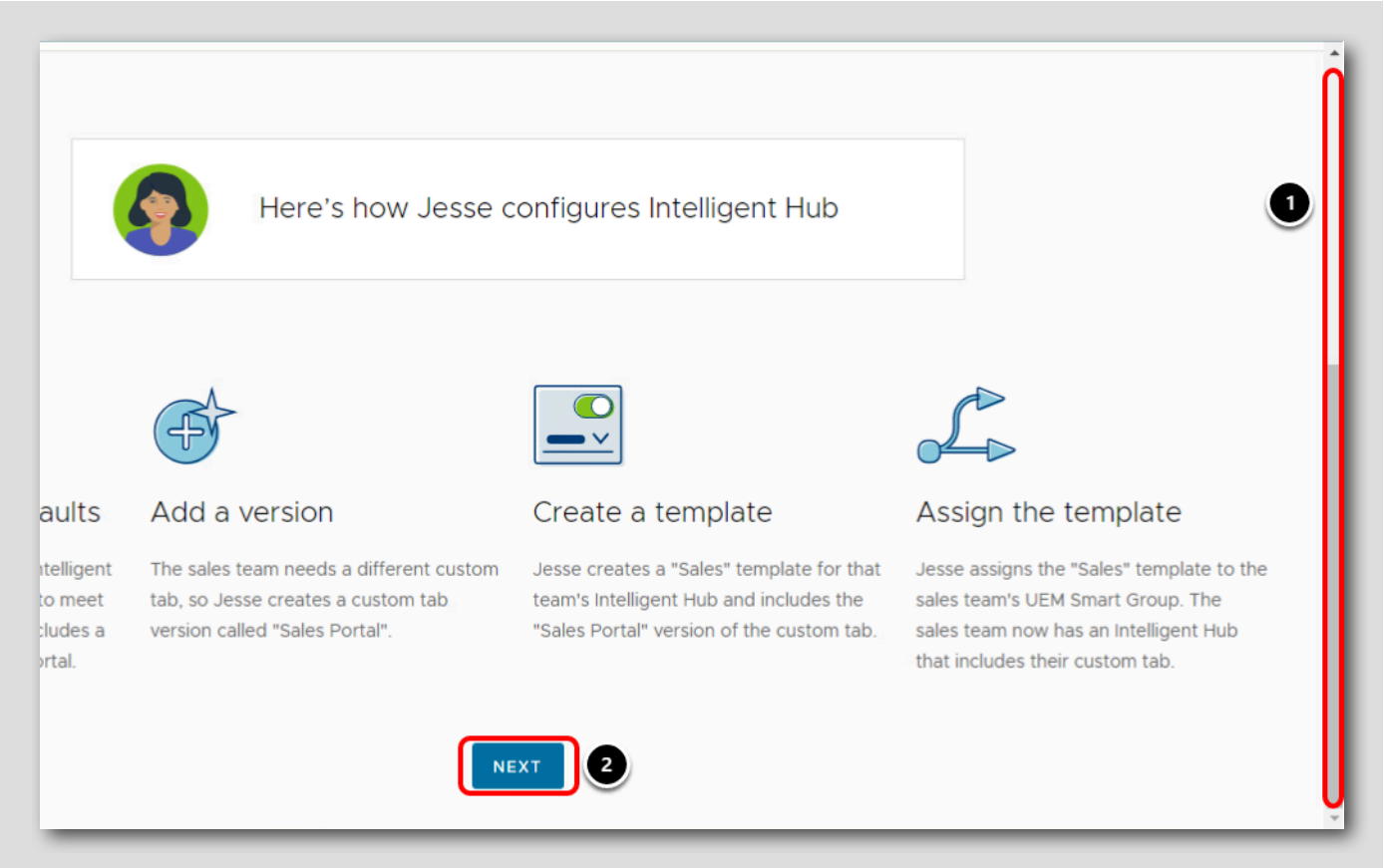
1. [LAUNCH] ボタンをクリックします。

Hub テンプレート ウィザード

[523]

Hub サービスの 20.08 リリースには、Hub サービスと Hub テンプレートと呼ばれる Intelligent Hub 機能の幅広い導入をサポートするための大幅な追加機能が含まれています。20.08 より前のリリースでは、Intelligent Hub のすべての Hub サービス構成はオールオアナッシングで、すべての従業員が同じ構成を受け取りました。このため、管理者が機能を段階的に展開したり、さまざまなチームや部門に対応したりすることが制限されていました。現在、管理者は独自の Hub サービス機能を持つ 1 つ以上のテンプレートを作成し、UEM スマート グループまたは Workspace ONE Access ユーザー グループに割り当てて、従業員の Intelligent Hub エクスペリエンスを制御できるようになりました。Hub テンプレートは Hub サービス 20.08 SaaS リリース以降で利用でき、UEM 20.08 以降および 20.08 バージョン以降の Intelligent Hub クライアントが必要です。

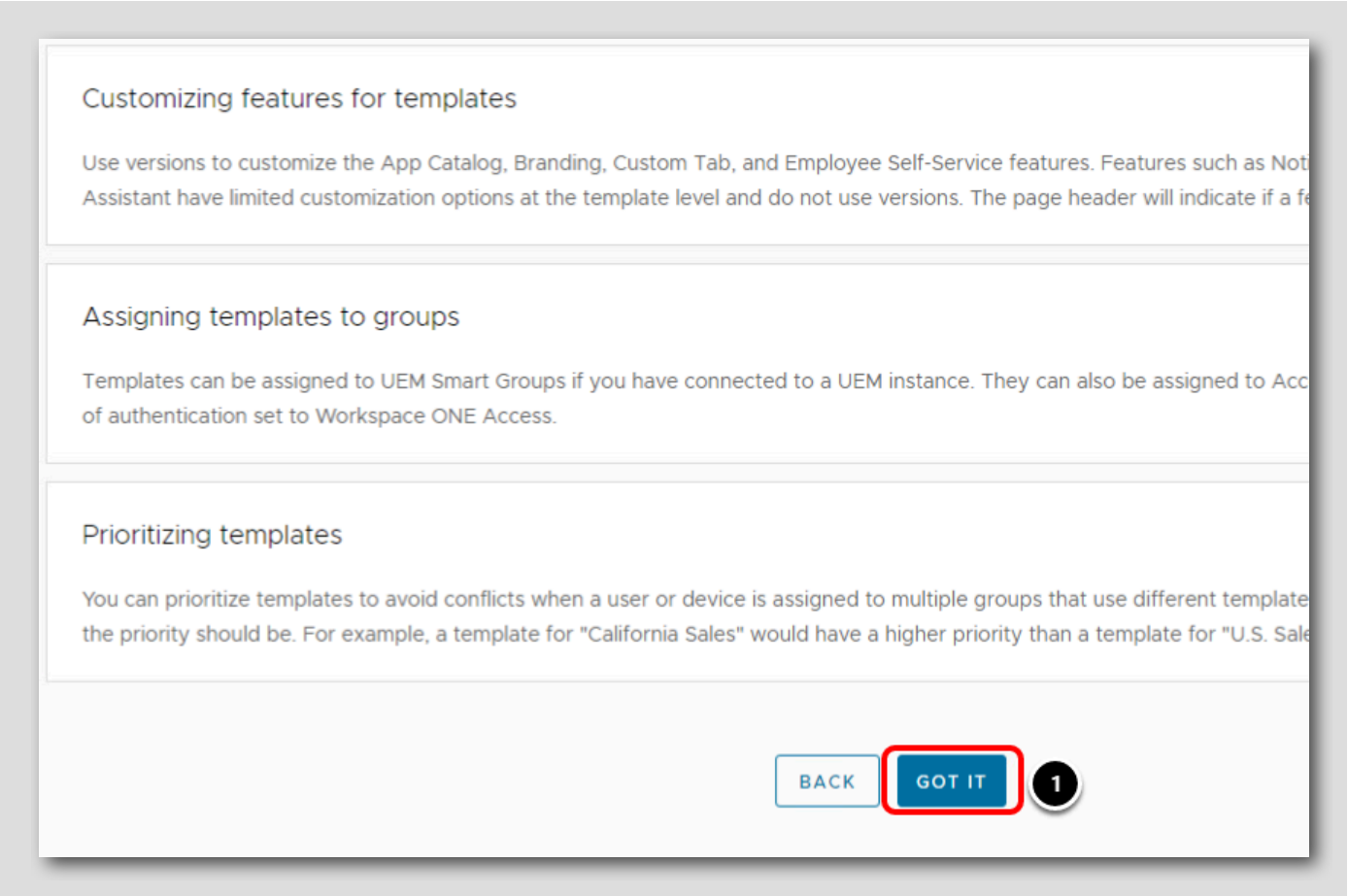
Hub サービスがすでに有効になっている環境では、20.08 へのアップグレード後に移行ウィザードが表示されます。管理者は、UEM Console からアプリケーション カタログ設定を移行するか、新しいグローバル設定を作成するかを選択できます。



1. この画面には、Hub テンプレートの概要が表示されます。下にスクロールして、[Next] ボタンを見つけます。
2. [Next] ボタンをクリックします。

Hub テンプレート ウィザード（続き）

[524]

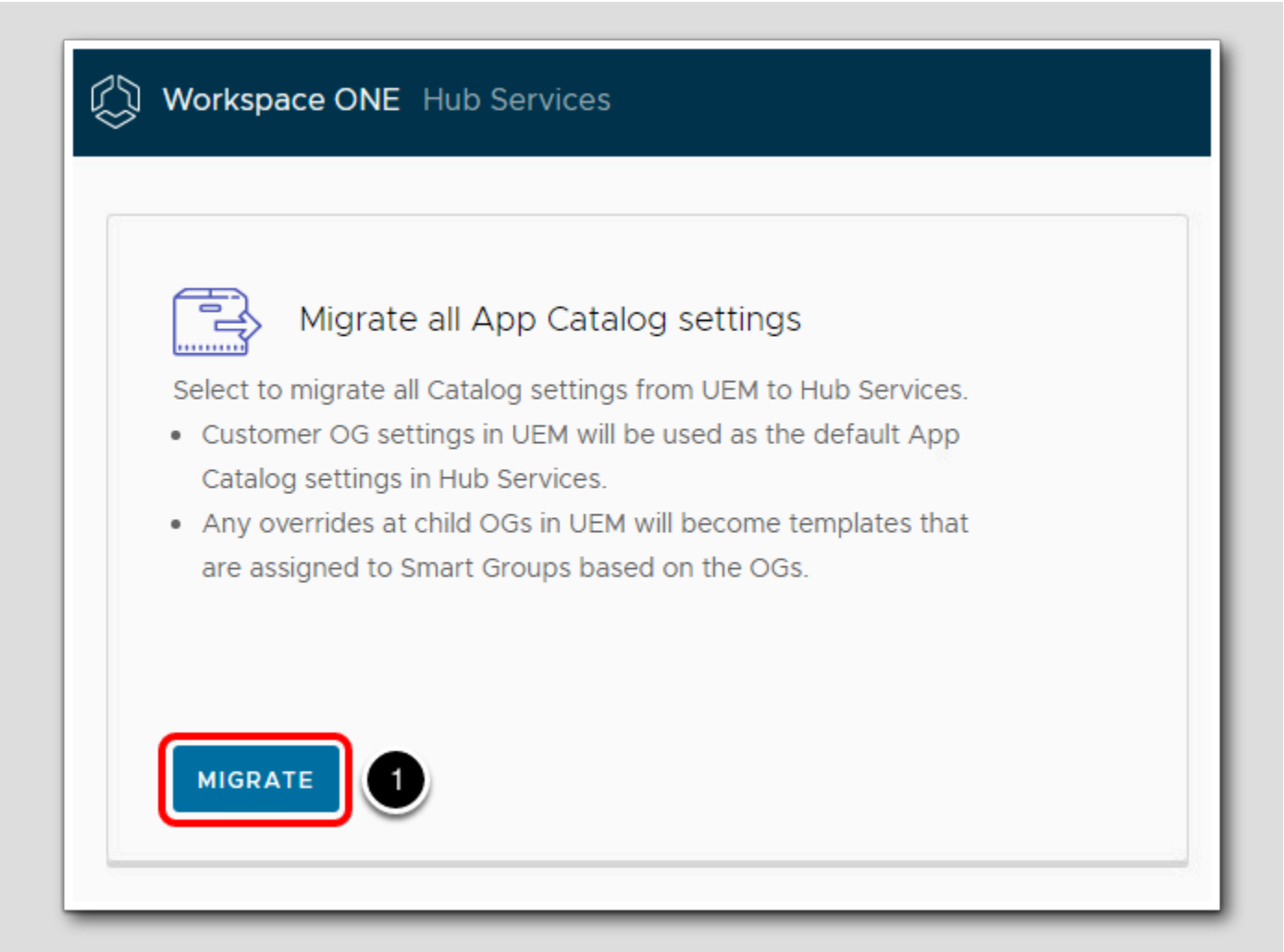


1. Hub テンプレートの構成手順の詳細を参照できます。次に、[GOT IT] ボタンをクリックします。

アプリ カタログ設定の移行

[525]

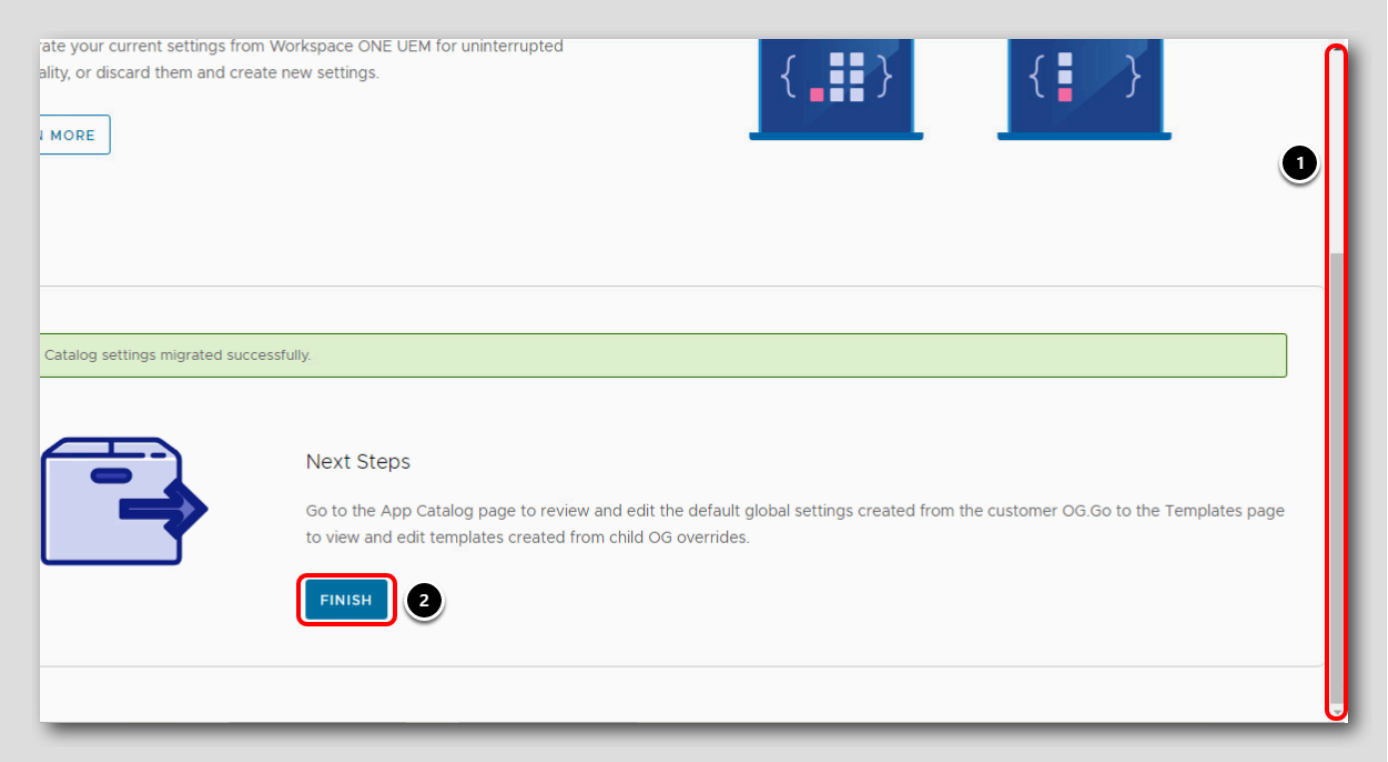
20.08 UEM リリース以降、すべての Intelligent Hub アプリケーション カタログ設定が Hub サービス コンソールに表示されるようになりました。Hub サービスがすでに構成されている環境では、管理者はアプリケーション カタログ設定を Workspace ONE UEM から移行することを選択できます。


Workspace ONE Hub Services
Migrate all App Catalog settings
Select to migrate all Catalog settings from UEM to Hub Services.
Customer OG settings in UEM will be used as the default App Catalog settings in Hub Services.
Any overrides at child OGs in UEM will become templates that are assigned to Smart Groups based on the OGs.
MIGRATE
1

1. 単击迁移按钮。

アプリケーション カタログ設定の移行

[526]



1. 下にスクロールして、[FINISH] ボタンを見つけます。
2. [FINISH] ボタンをクリックします。

アプリケーション カタログとカスタム タブのバージョンの追加

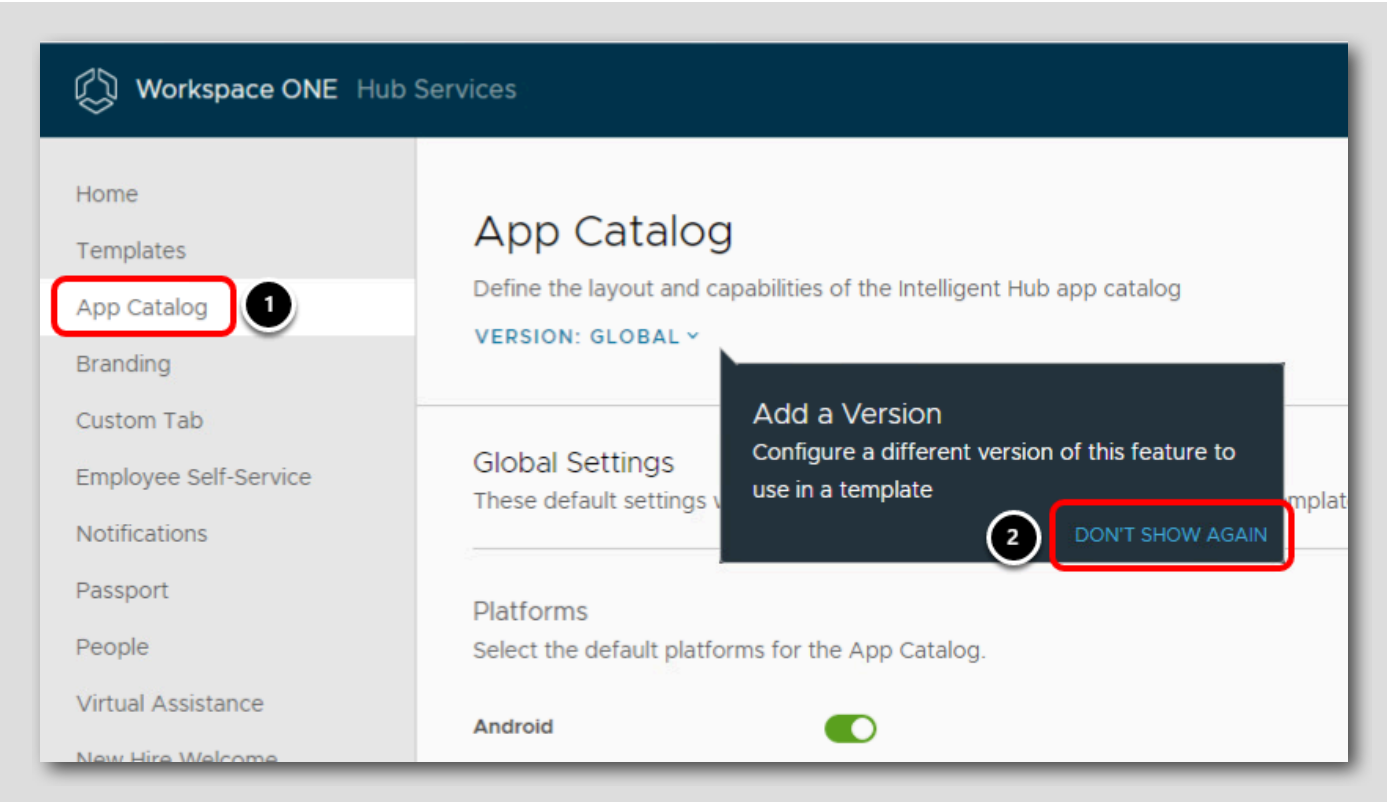
[527]

Intelligent Hub 設定用のテンプレートを作成する前に、まずエンド ユーザーが使用できる機能をいくつか構成する必要があります。

アプリケーション カタログ設定へのアクセス

[528]

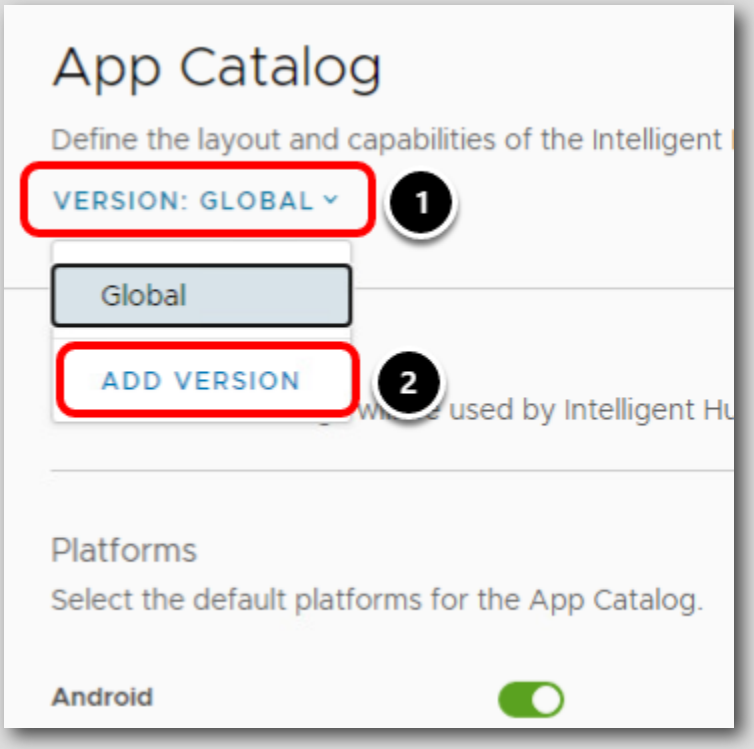
[App Catalog] タブでは、ユーザーに表示される Intelligent Hub アプリケーション カタログのレイアウトと機能を定義できます。Salesforce アプリケーションのプロモーションを追加してカタログを変更し、このアプリケーションをカタログで強調表示してから、モバイル デバイスでの仮想アプリケーションの使用を無効にします。



1. 左側の [App Catalog] メニュー項目をクリックします。
2. ユーザーのグループごとに異なるバージョンのアプリケーション カタログを作成できることを示す [Add a Version] の通知が表示される場合があります。[DON'T SHOW AGAIN] をクリックします。

アプリケーション カタログのバージョンの追加

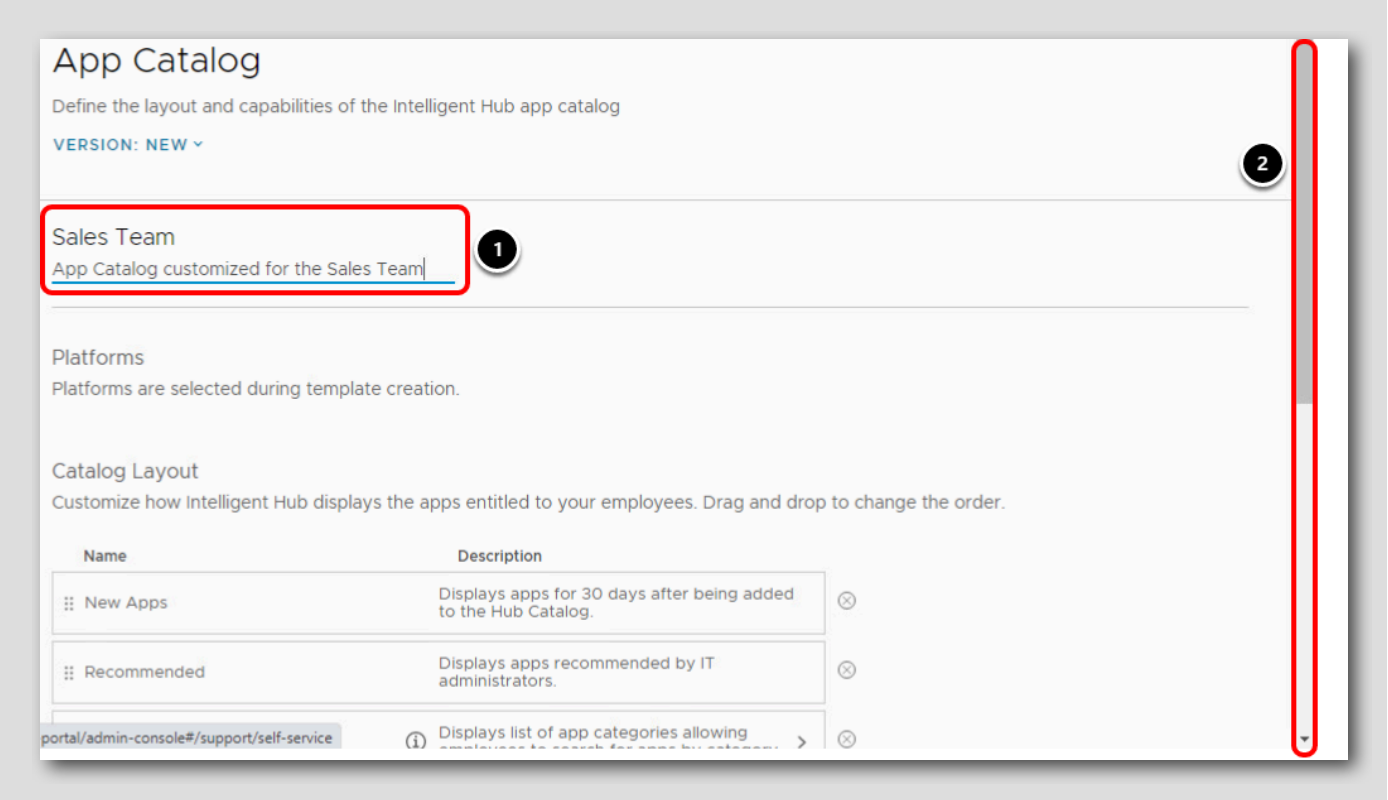
[529]



1. [VERSION: GLOBAL] ドロップダウンをクリックします。
2. [ADD VERSION] をクリックします。

セールス チームのアプリケーション カタログ バージョンに名前を付ける

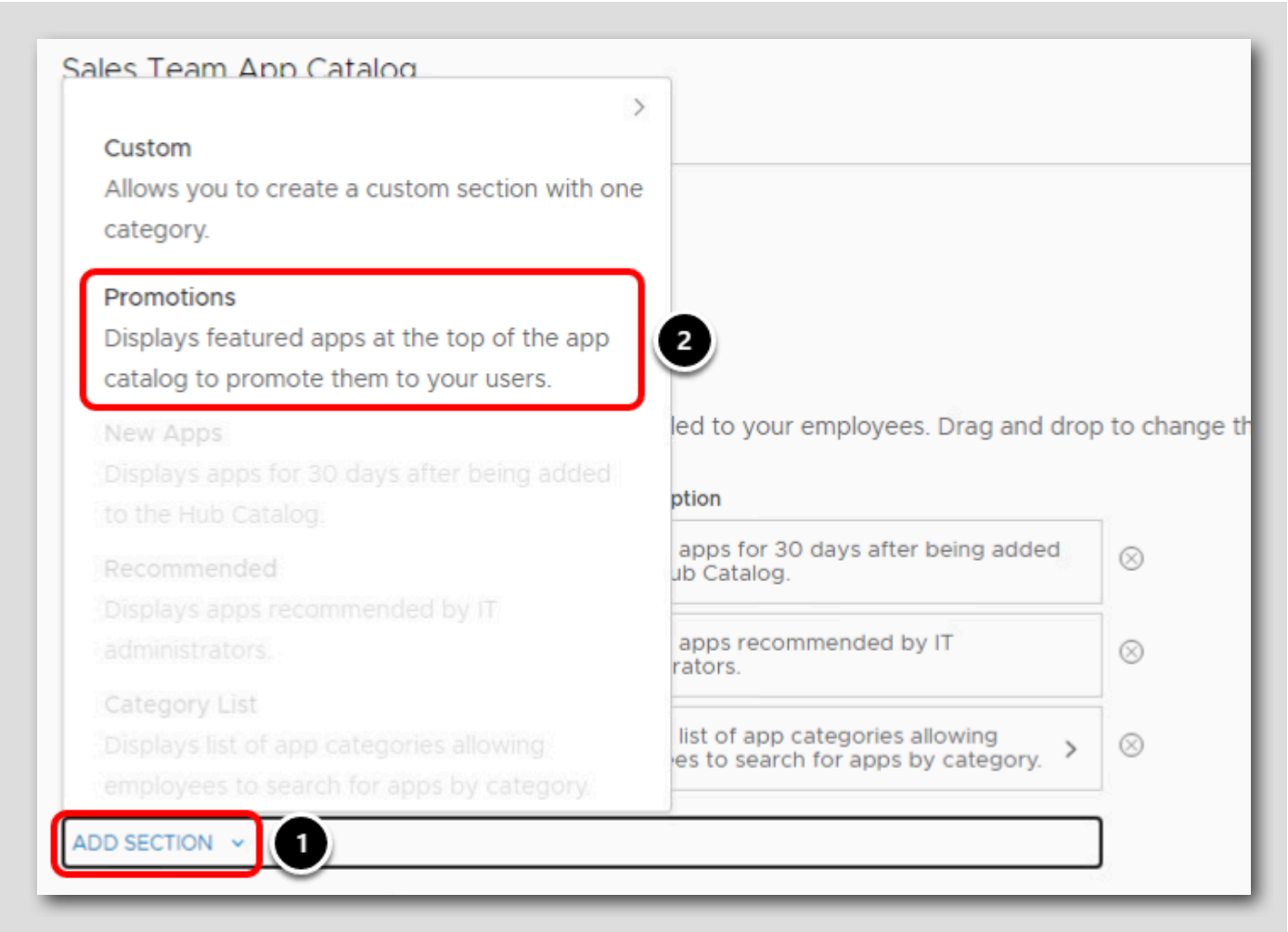
[530]



1. バージョン名に **Sales Team** を入力し、**App Catalog customized for the Sales Team** という説明を追加します。
2. 下にスクロールして、[Catalog Layout] セクションの下の [ADD SECTION] ドロップダウンを探します。

セールス チームのアプリケーション カタログ レイアウトのカスタマイズ

[531]

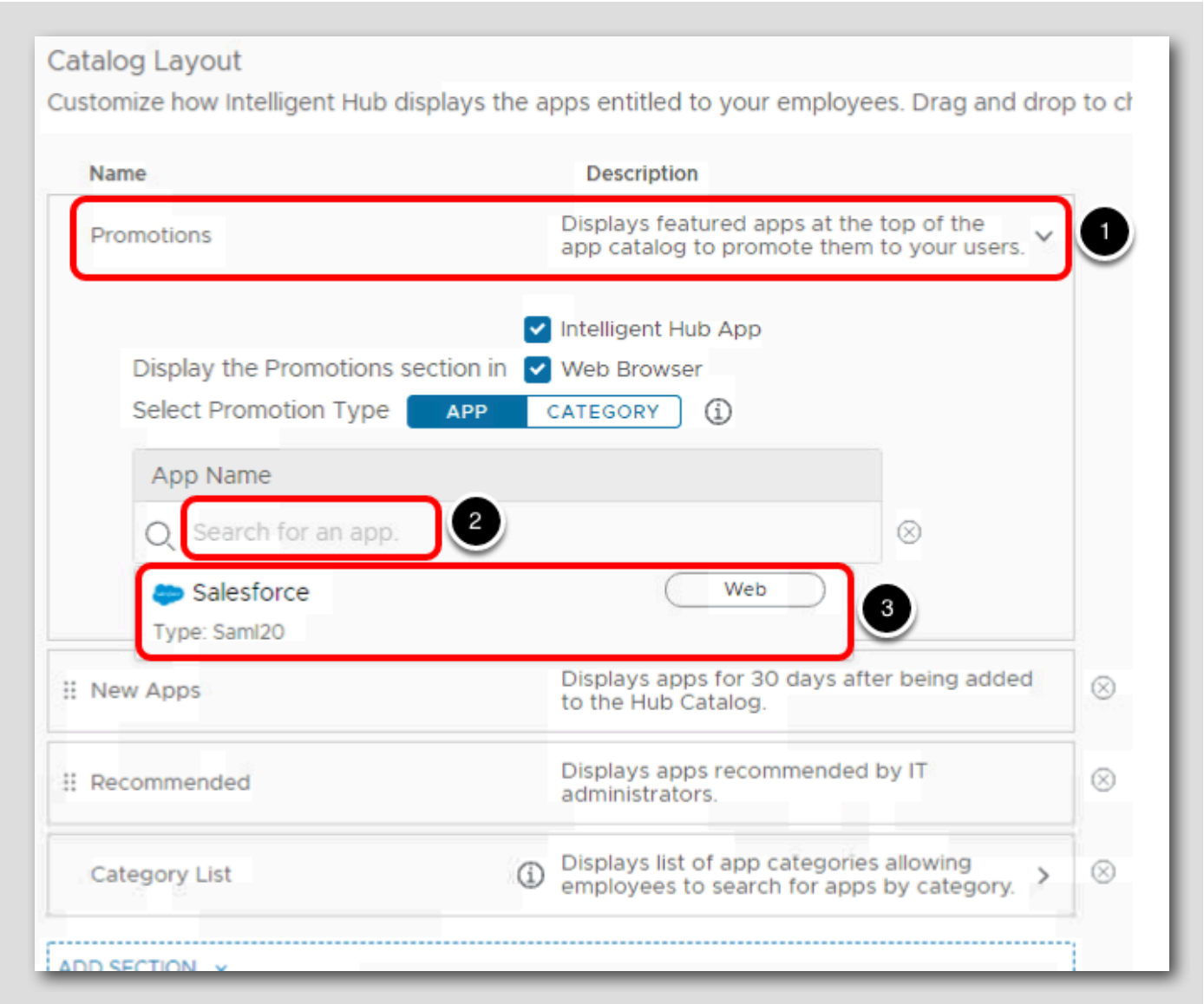


1. [ADD SECTION] をクリックします。
2. [Promotions] をクリックします。

Sales Team アプリケーション カタログの上部に [Promotions] セクションが表示され、その後に [New Apps]、[Recommended]、[Category List] のセクションが表示されます。

[Promotions] セクションのカスタマイズ

[532]

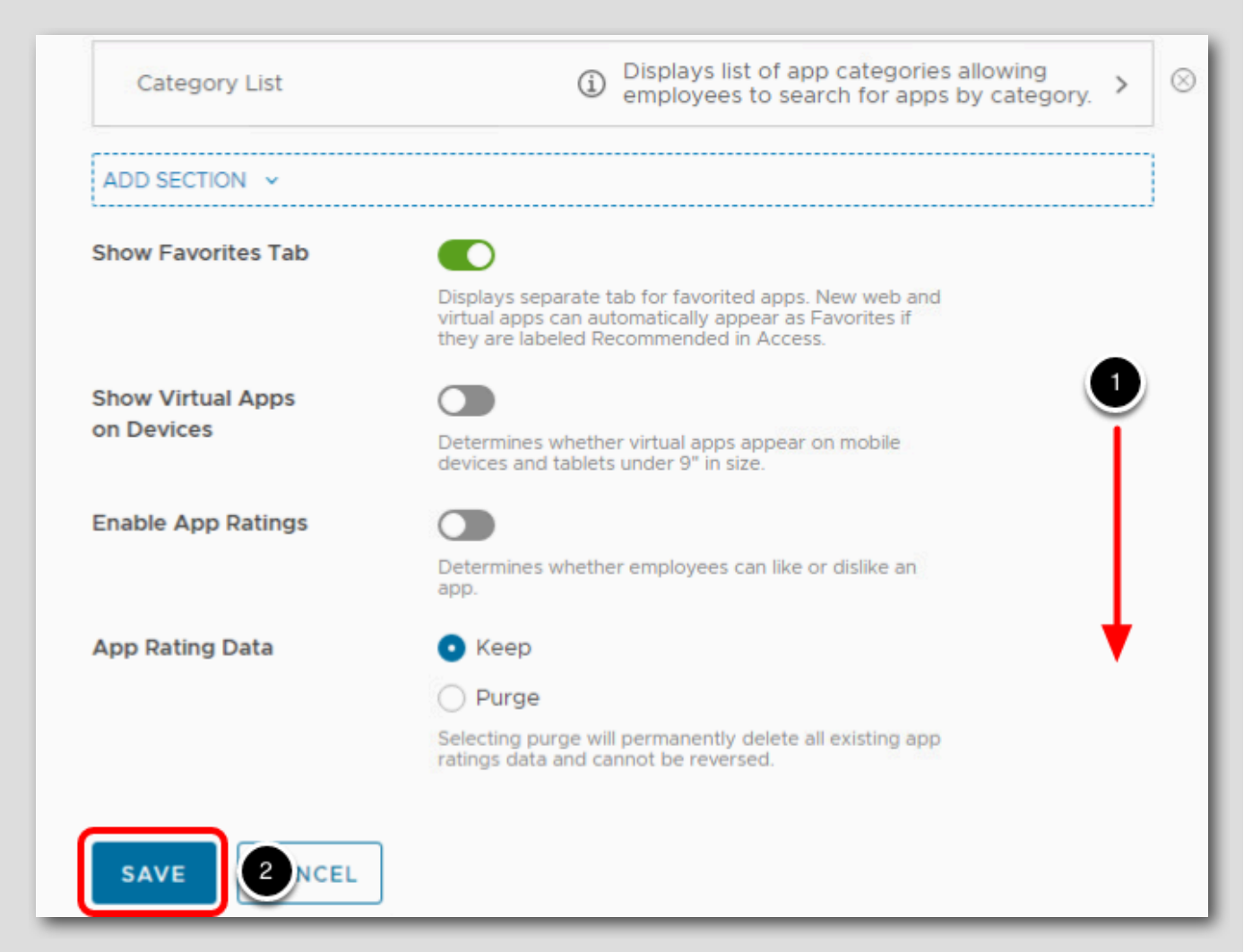


1. [Promotions] セクションをクリックして展開します。
2. [App Name] 検索ボックス内をクリックします。複数のアプリケーションがある場合は、ここに入力して表示される結果を絞り込むことができます。
3. リストから [Salesforce] の結果を選択します。

これにより、Salesforce アプリケーションがエンド ユーザーに推奨されます。重要なアプリケーションや使用頻度の高いアプリケーションを推奨して、エンド ユーザーの利用を促進することを検討してください。

セールス チームのカタログ レイアウトの保存

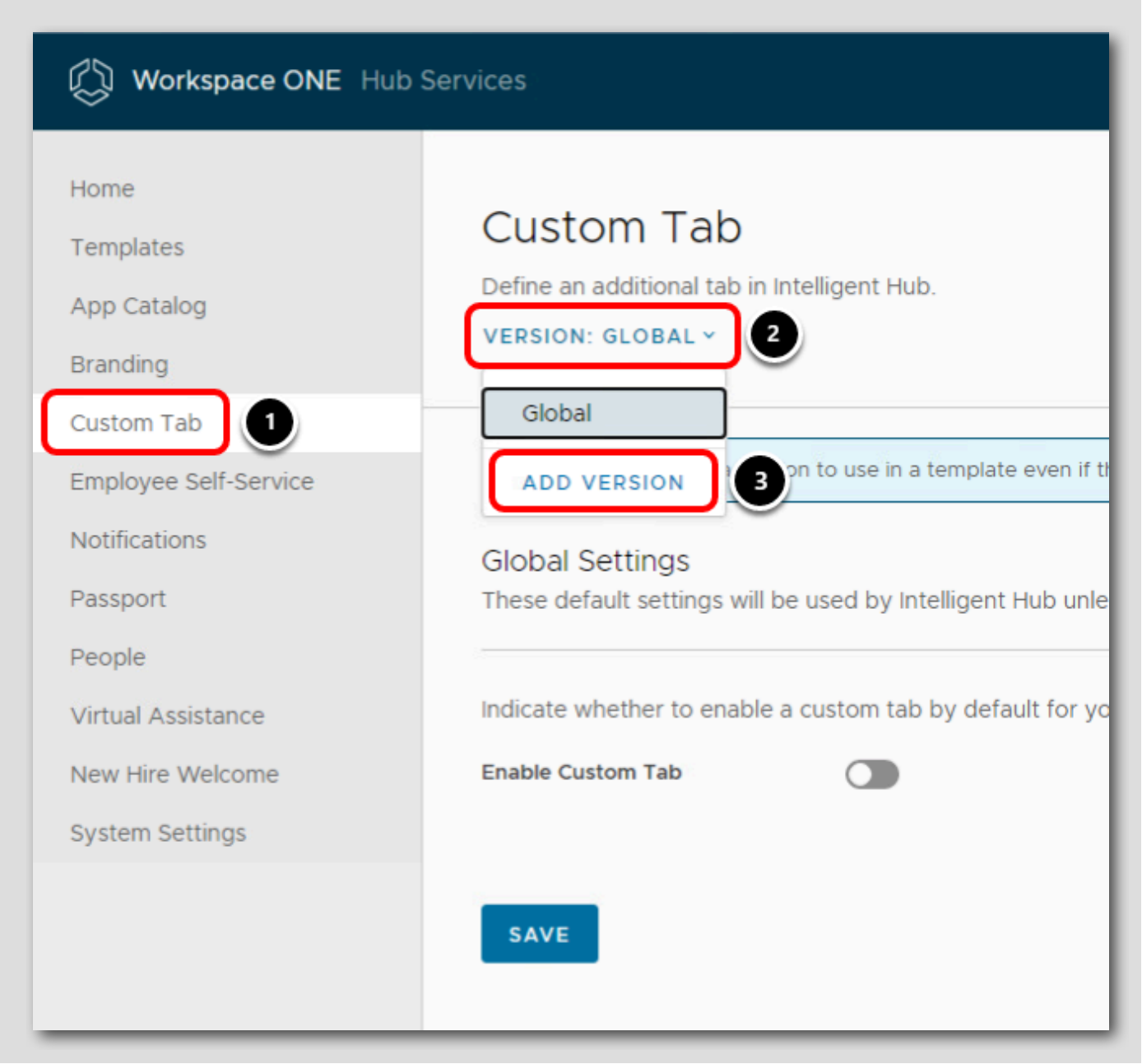
[533]



1. [Catalog Layout] セクションを下にスクロールして、[Save] ボタンを見つけます。
2. [SAVE] をクリックします。

カスタム タブの構成

[534]

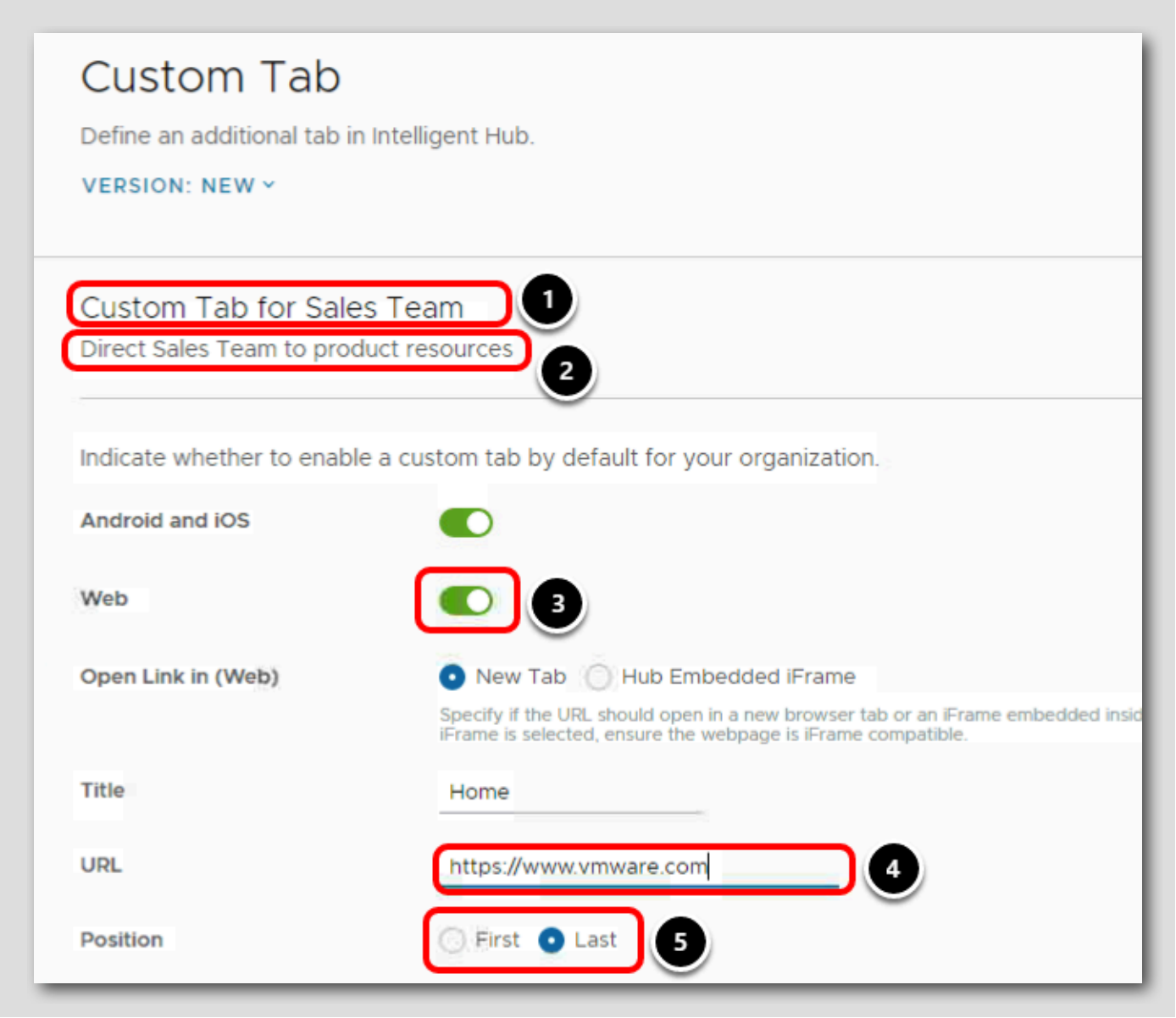


カスタム タブは、会社のイントラネット サイトやユーザーと簡単に共有する別のリソースにリンクする URL です。

1. 左側の [Custom Tab] メニュー項目を選択します。
2. [VERSION: GLOBAL] ドロップダウンをクリックします。
3. [ADD VERSION] をクリックします。

カスタム タブの設定

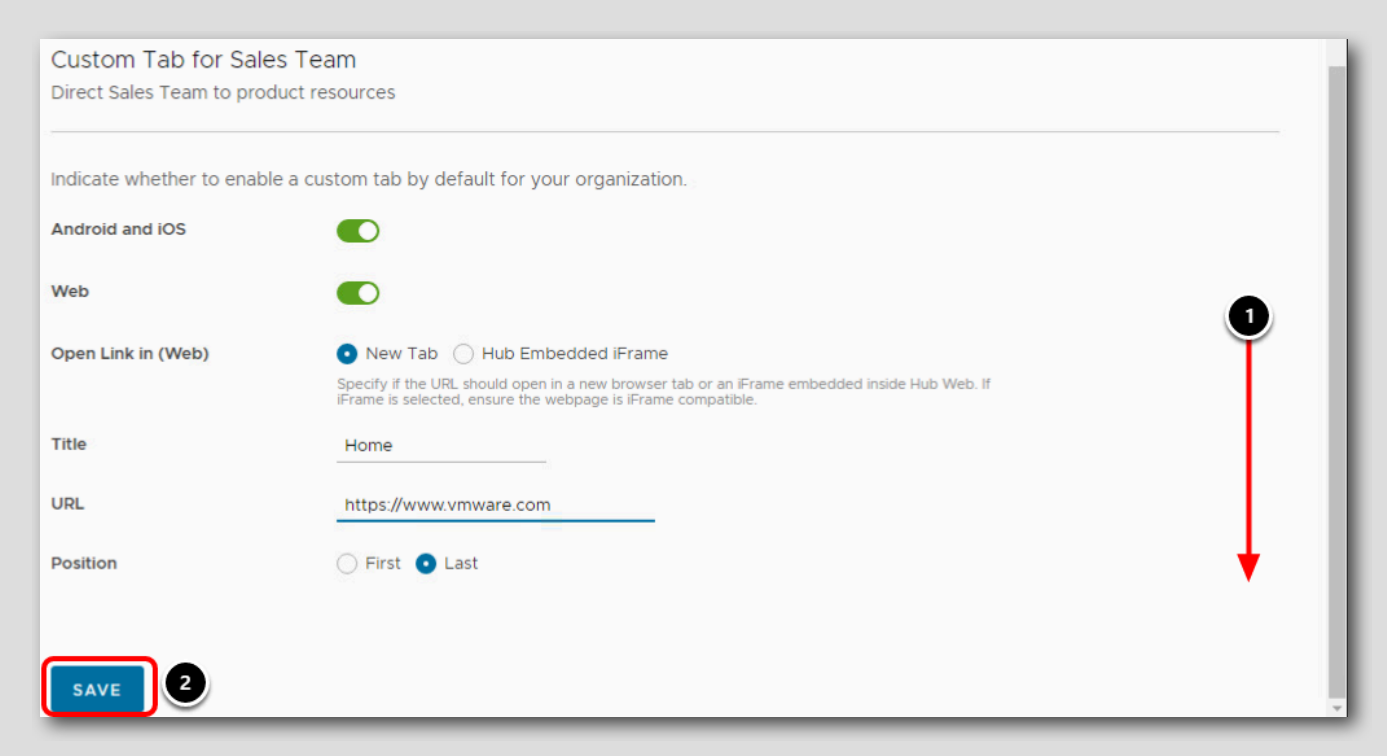
[535]



1. [Version Name] に **`Custom Tab for Sales Team`** と入力します。
2. [Description] に **`Direct Sales Team to product resources`** と入力します。
3. [Web] トグルをオンにして、このカスタム タブが Intelligent Hub のブラウザ バージョンに表示されるようにします。
4. [URL] に **`https://www.vmware.com`** と入力します。
5. [Position] で [Last] を選択します。

カスタム タブの設定の保存

[536]



1. 下にスクロールして、[Save] ボタンを見つけます。
2. [SAVE] をクリックします。

Intelligent Hub のブランディングの構成

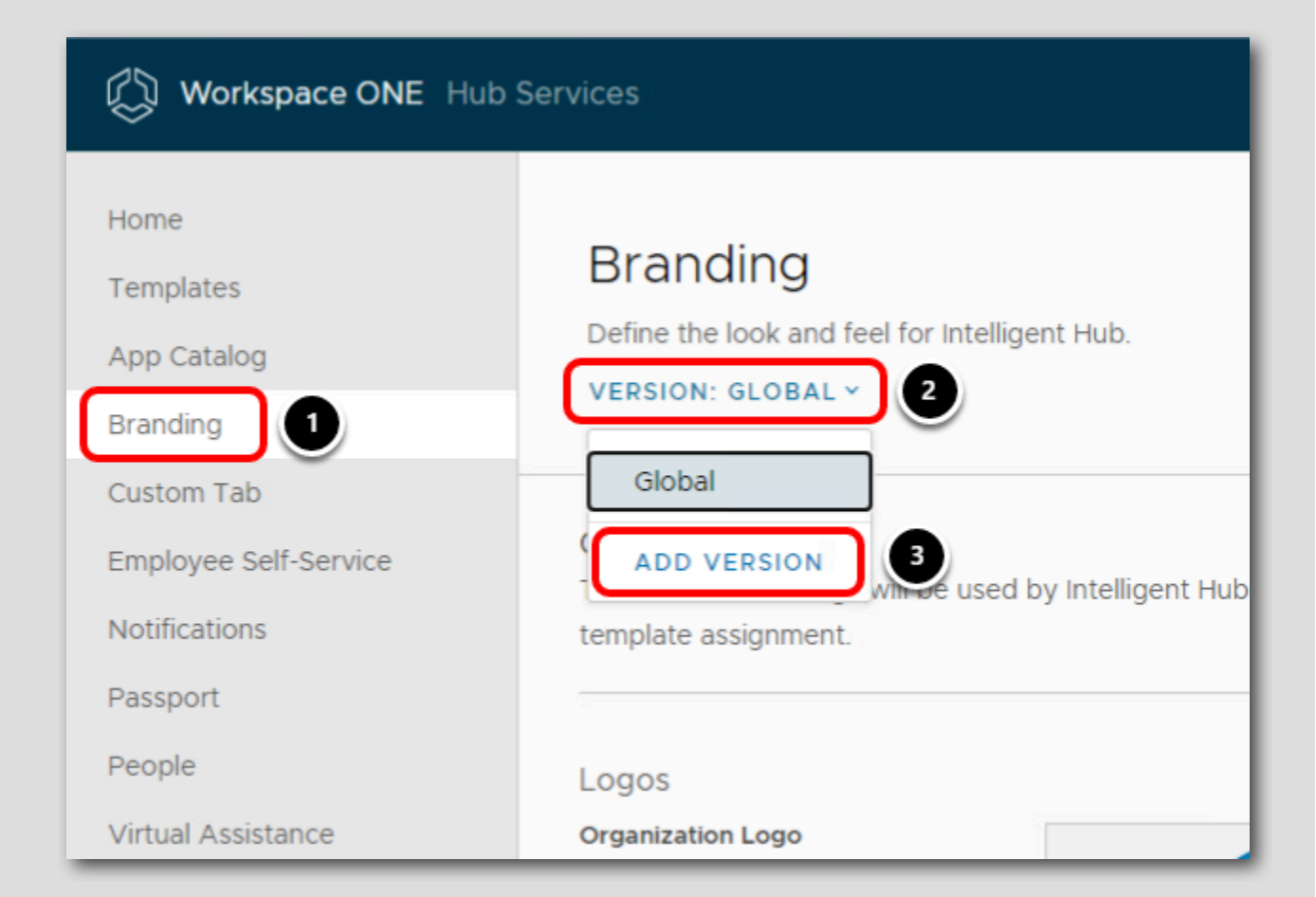
[537]

デフォルトでは、Intelligent Hub 内で VMware のブランディングが使用されますが、Intelligent Hub アプリケーションおよびブラウザ ビューに表示されるロゴ、テキストの色、および背景色をカスタマイズできます。

このセクションでは、Intelligent Hub のブランディング設定で会社のロゴと組織名を変更します。

ブランディング バージョンの追加

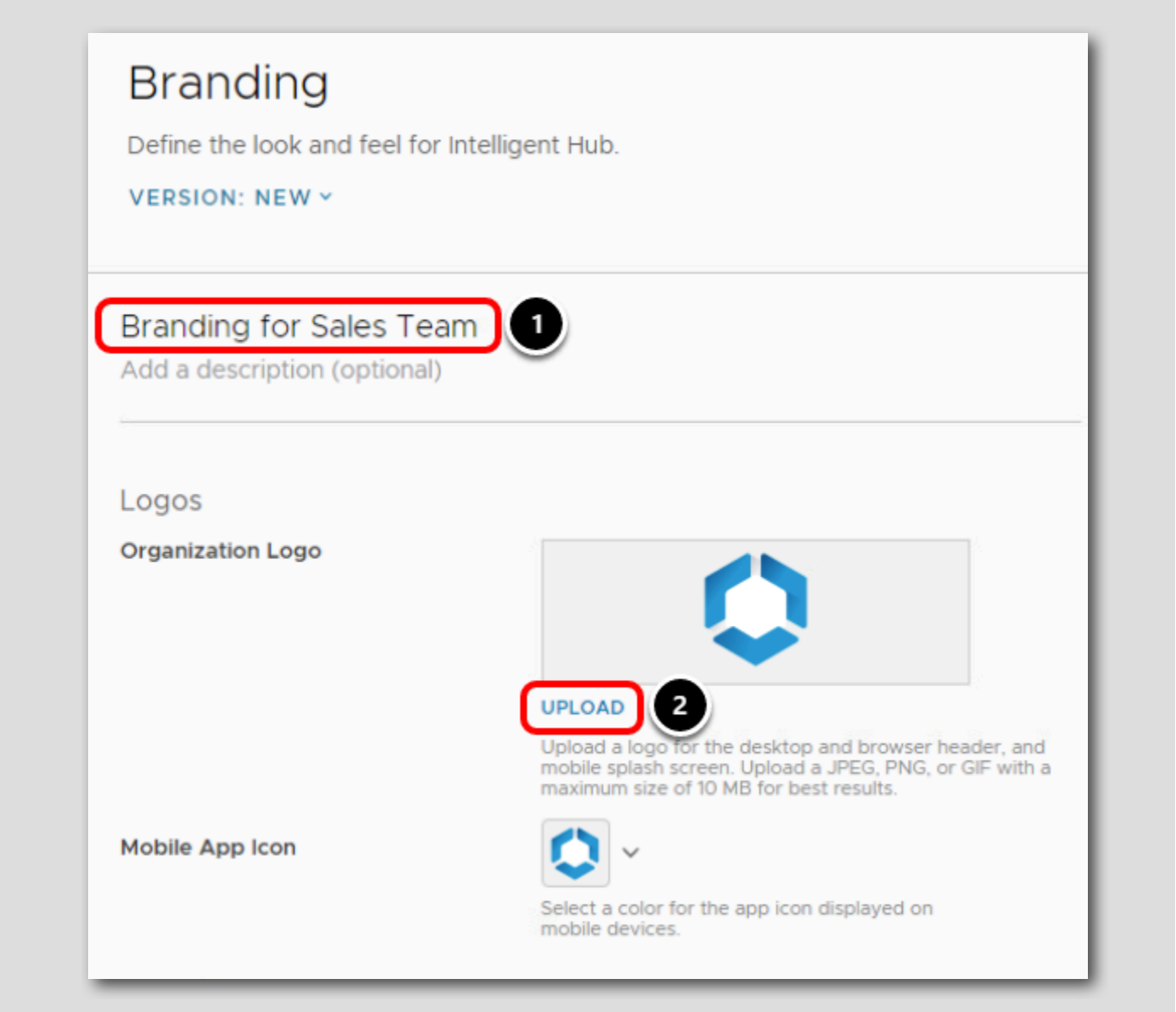
[538]



1. 左側の [Branding] メニュー項目をクリックして、Intelligent Hub のブランディングをカスタマイズします。
2. [VERSION: GLOBAL] ドロップダウンをクリックします。
3. [ADD VERSION] をクリックします。

ブランディング バージョンの名前付けとロゴのアップロード

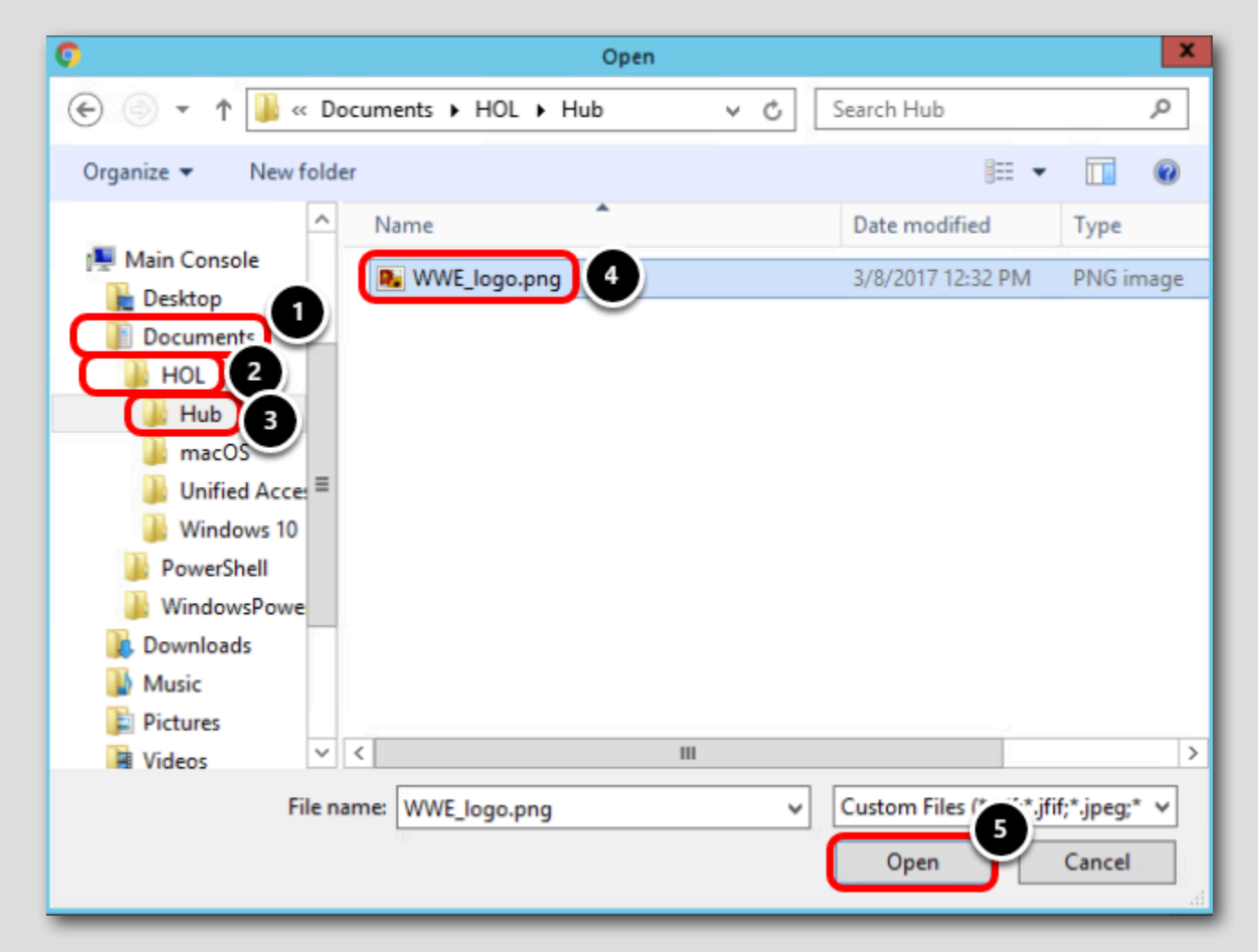
[539]



1. バージョンに **`Branding for Sales Team`** という名前を付けます。
2. 組織ロゴの [UPLOAD] リンクをクリックします。

会社のロゴ ファイルへの移動

[540]

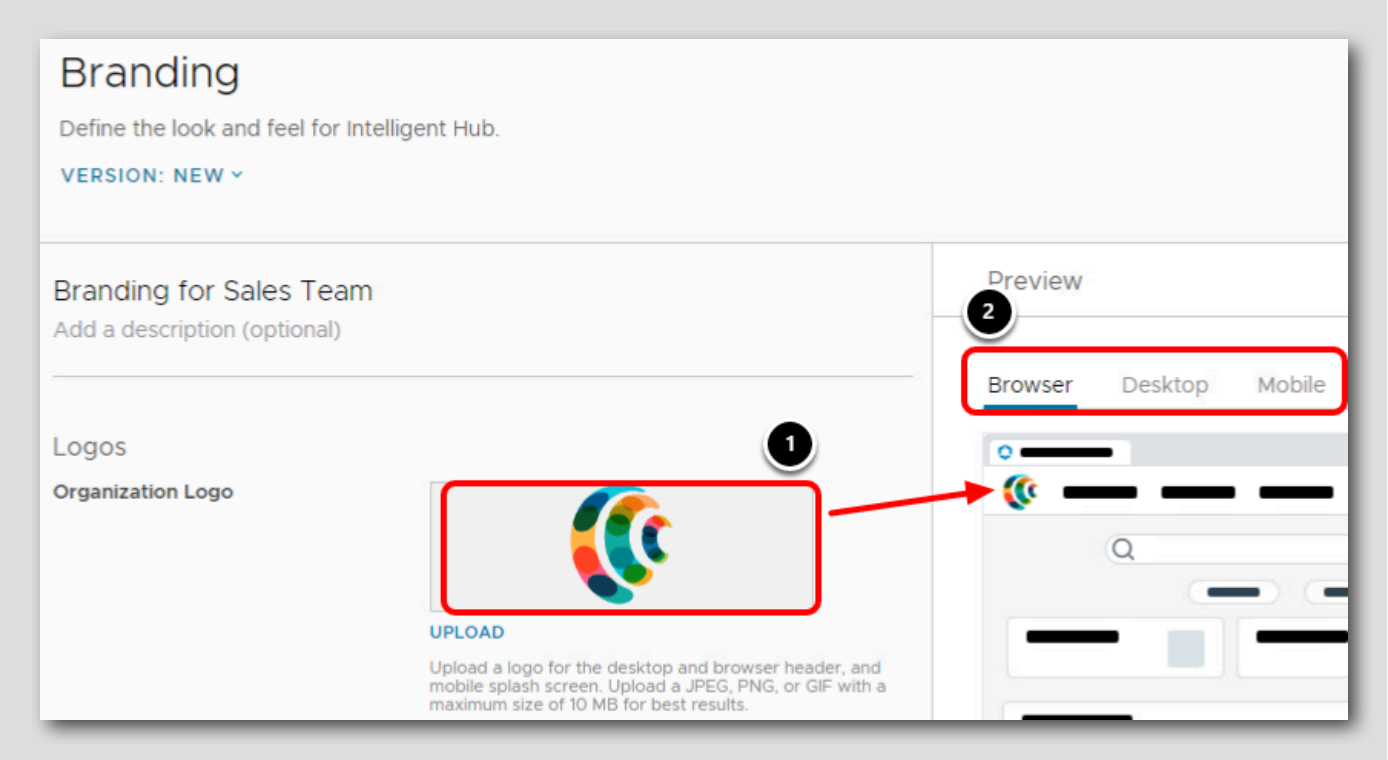


ポップアップ ウィンドウで、次のように操作します。

1. [Documents] を展開します。
2. [HOL] を展開します。
3. [Hub] フォルダをクリックします。
4. [WWE_logo.png] を選択します。
5. [Open] をクリックします。

ブランディングの変更のプレビュー

[541]



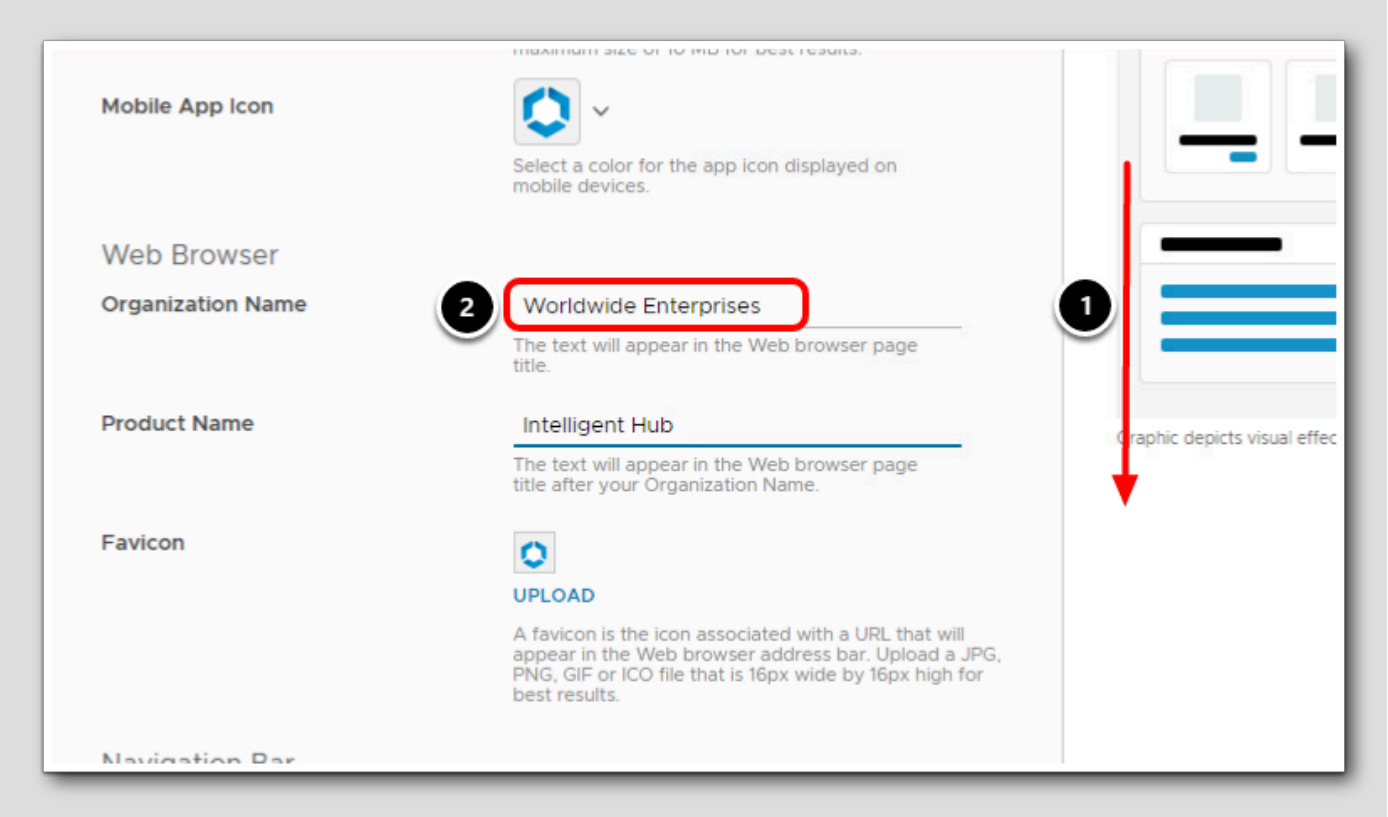
1. [Company Logo] 設定を更新した後、[Preview] ペインが更新され、ユーザーに表示される内容が反映されていることを確認します。
2. [Preview] ペインでは、ブラウザ、デスクトップ、モバイルの各ビューを切り替えて、変更が各プラットフォームにどのように反映されるかを確認できます。

ユーザーに変更を公開する前に、このページのその他の設定がここに反映され、クイック プレビューが表示されます。

次の手順に進んでください。

組織名の変更

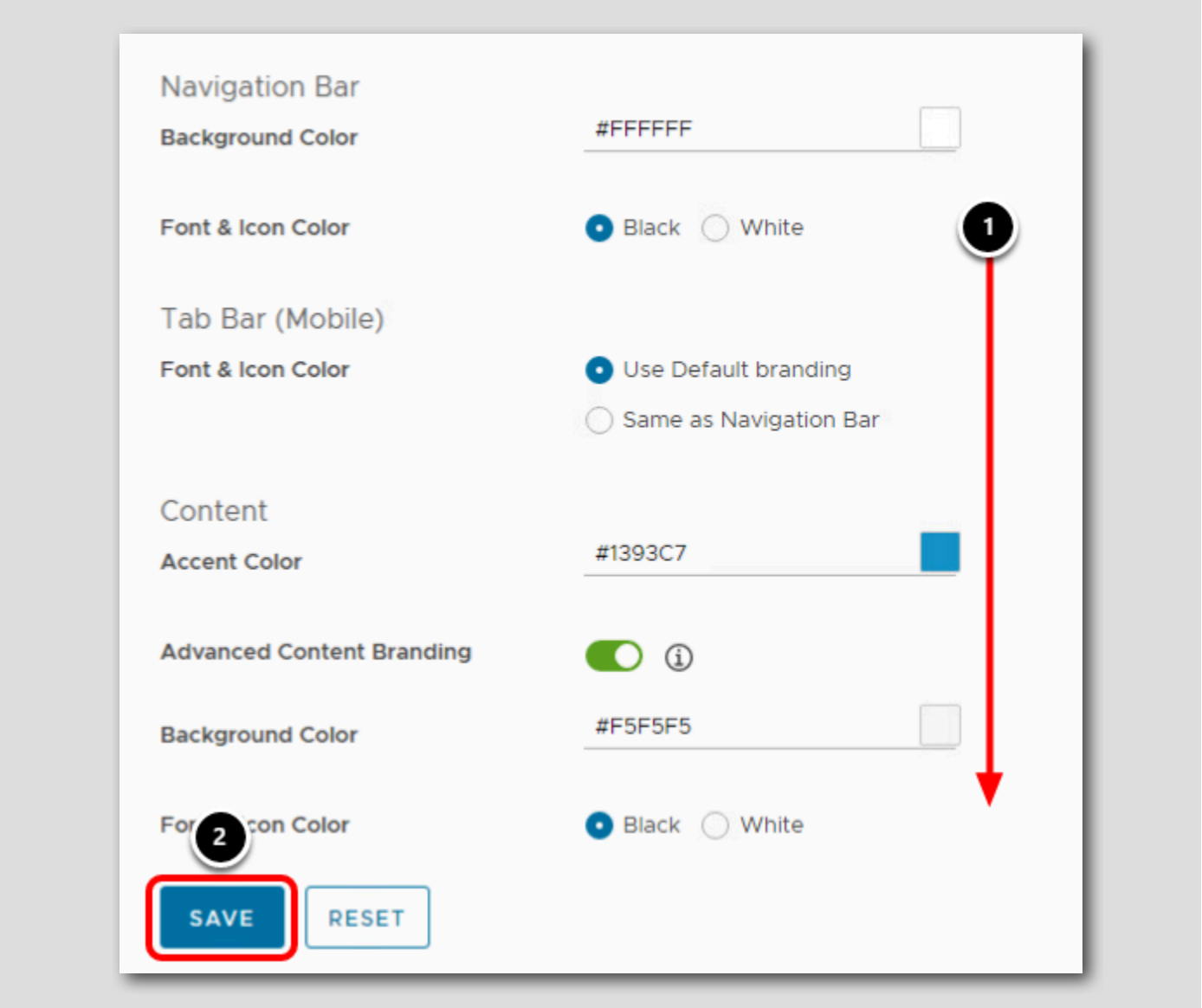
[542]



1. 下にスクロールして、[Web Browser] セクションに移動します。
2. [Organization Name] を VMware から **`Worldwide Enterprises`** に変更します。

ブランディングの変更の保存

[543]



1. [Branding] セクションの一番下までスクロールします。
2. [Save] をクリックして、ブランディングの構成を保存します。

注：背景色やアイコンの色などのブランディング オプションもありますが、このラボの対象範囲を制限するため、デモの目的で組織名と会社ロゴのみを変更します。後でその他の構成を自由に実行して、結果を確認することができます。

Hub サービスの通知

[544]

Intelligent Hub 通知フレームワークは、従業員に対して実用的なリアルタイム通知を生成して提供するために設計された、堅牢で柔軟性のあるクラウドホスト型サービスです。ユーザーは、ブラウザの Hub ポータルとデバイスの Intelligent Hub アプリケーションで通知を受け取ることができます。

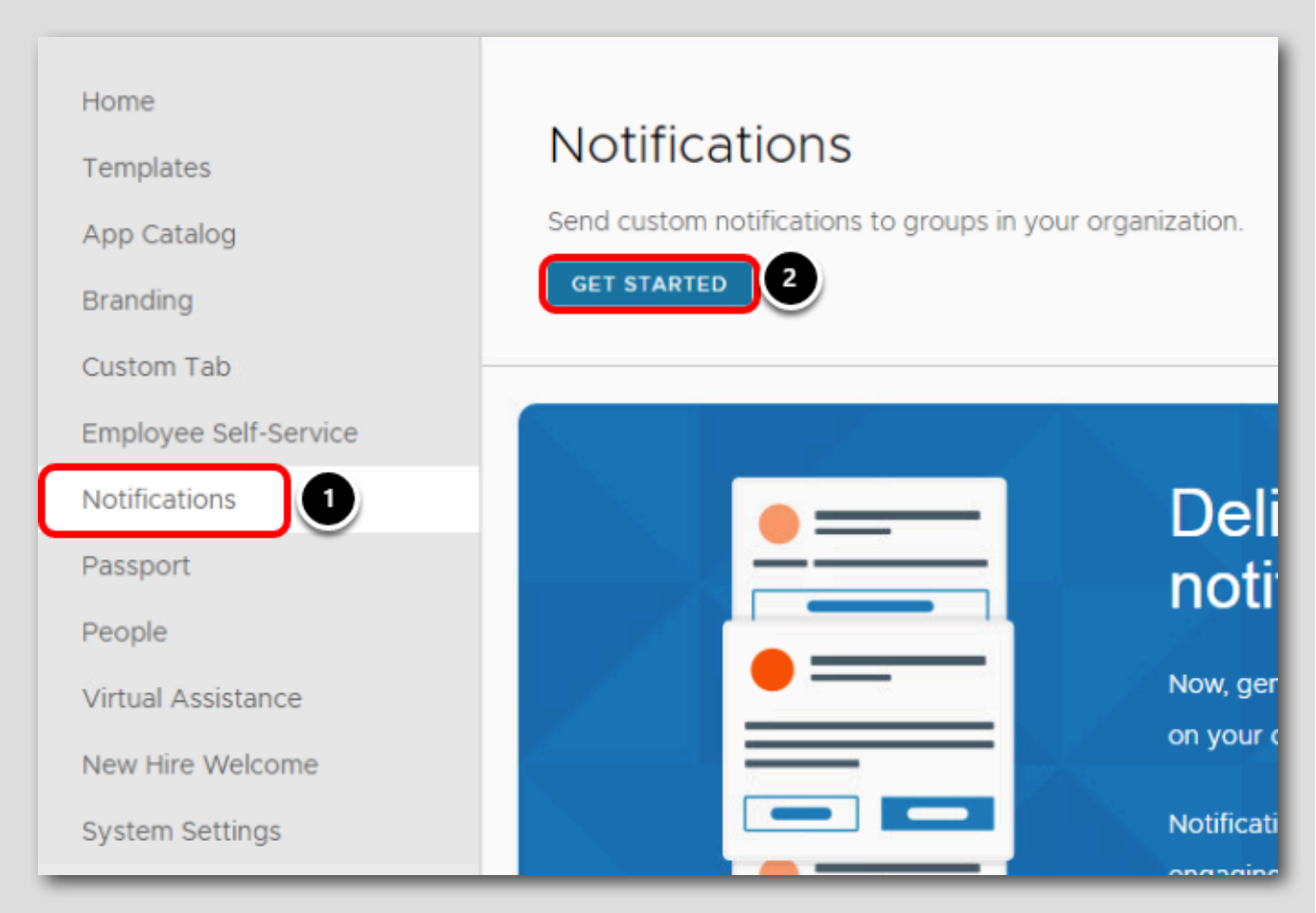
利用可能な通知のタイプについて見てみましょう。

1. 新しいアプリケーションが利用可能：新しいアプリケーションがカタログで利用可能であることを通知するために、Hub サービスで自動的に生成される通知です。ユーザーは、通知メッセージから新しいアプリケーションを選択し、自分のデバイスに保存できます。
2. カスタム通知：Hub サービス管理コンソールの通知ウィザードのテンプレートを使用するか、通知 API を使用して通知を自動化できます。これらの通知により、ユーザー デバイスでリマインダーおよび重要な情報の送信、またはアクションの呼び出しを行うことができます。
3. Workspace ONE Mobile Flows 経由の通知：Mobile Flows サービスが Workspace ONE UEM 環境で構成されている場合、Mobile Flows と Hub サービスの統合を有効にして、Mobile Flows で構成されたビジネス アプリケーションからの通知（Salesforce、Concur、Coupa からの承認通知など）を Intelligent Hub で直接受信できます。

このセクションでは、Hub サービス管理コンソール内のウィザードを使用してカスタム通知を作成します。

通知の開始

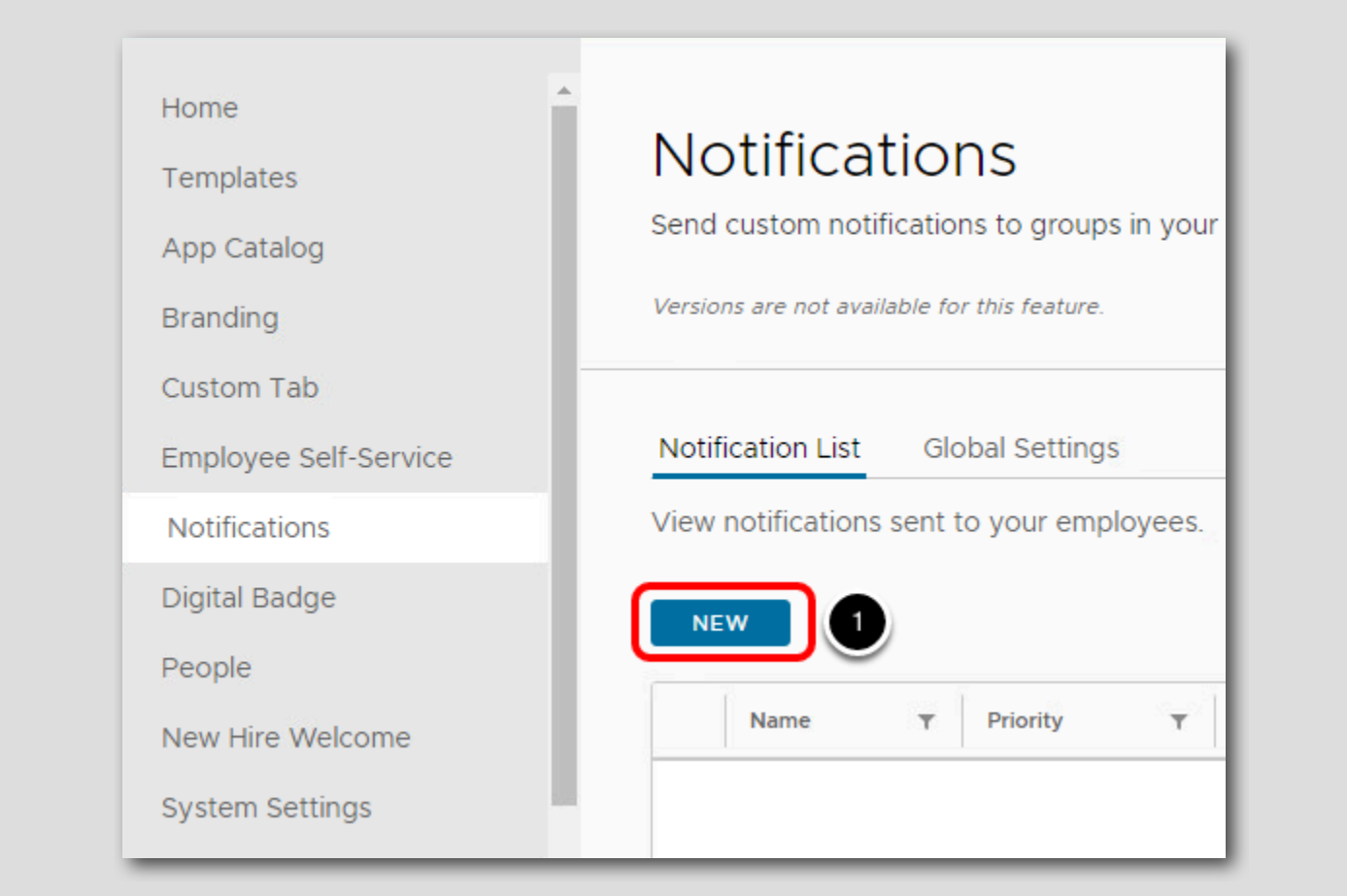
[545]



1. 左側の [Notifications] メニュー項目をクリックします。
2. [GET STARTED] をクリックして続行します。

Hub サービスの [通知] タブ

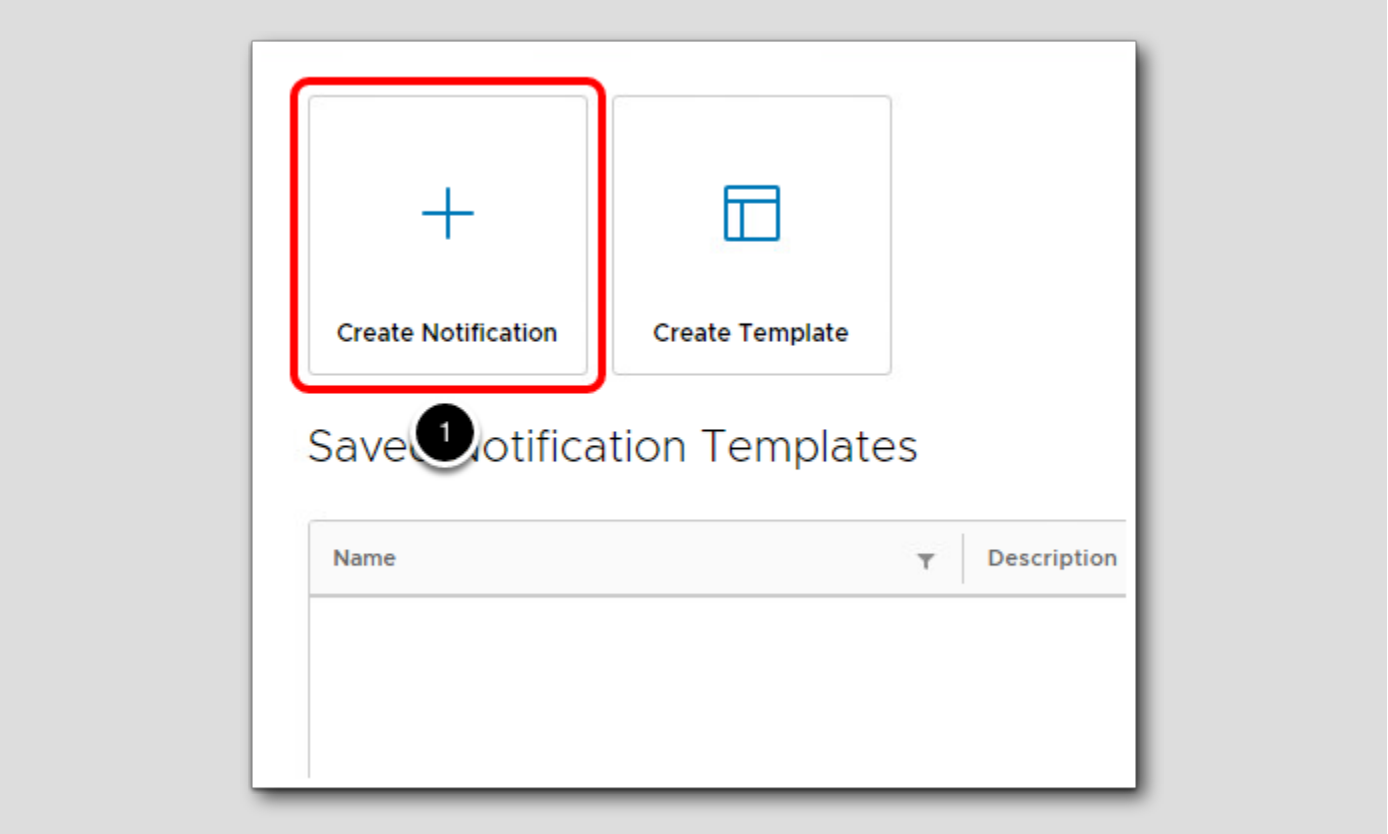
[546]



1. 「NEW」ボタンをクリックします。

通知アクションの選択

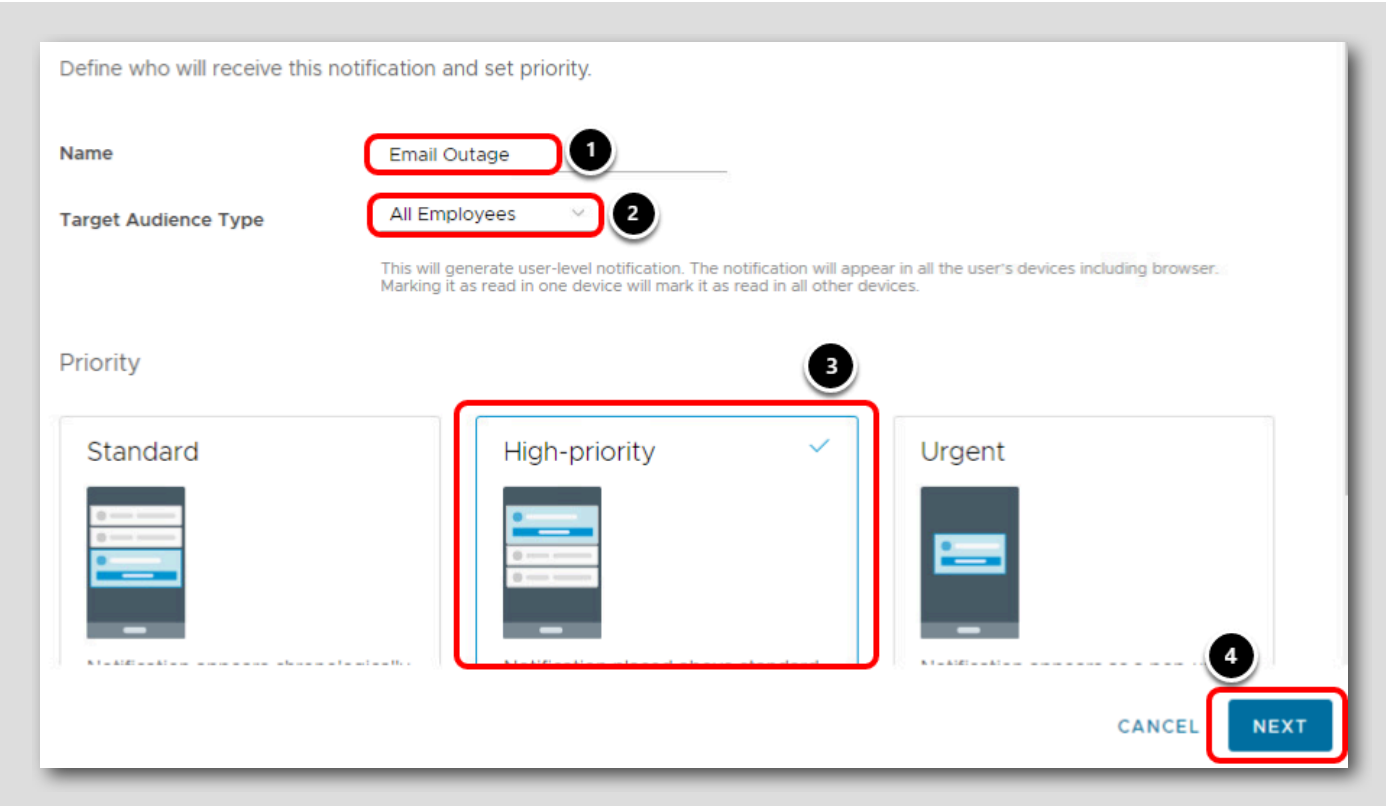
[547]



1. 「通知の作成」を選択します。

通知定義の設定

[548]

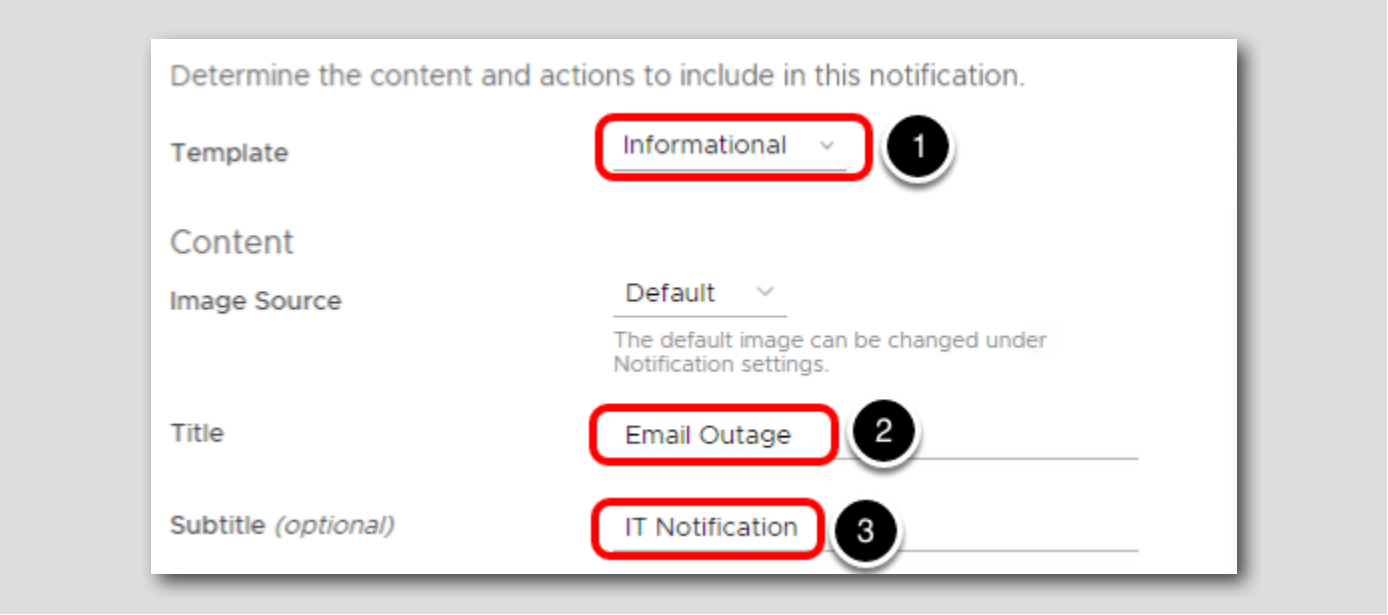


1. [Name] に **`Email Outage`** と入力します。
2. [Target Audience] ドロップダウンから [All Employees] を選択します。
3. 優先順位の種類に [High-priority] を選択します。
4. [NEXT] をクリックします。

通知は、[Standard]、[High-priority]、または [Urgent] の優先度レベルに設定できます。優先度の高い通知は、Intelligent Hub 内の [For You] タブの上部に表示されます。緊急通知は、Intelligent Hub 内にポップアップ ウィンドウとして表示され、ユーザーが閉じる必要があります。

通知コンテンツの設定

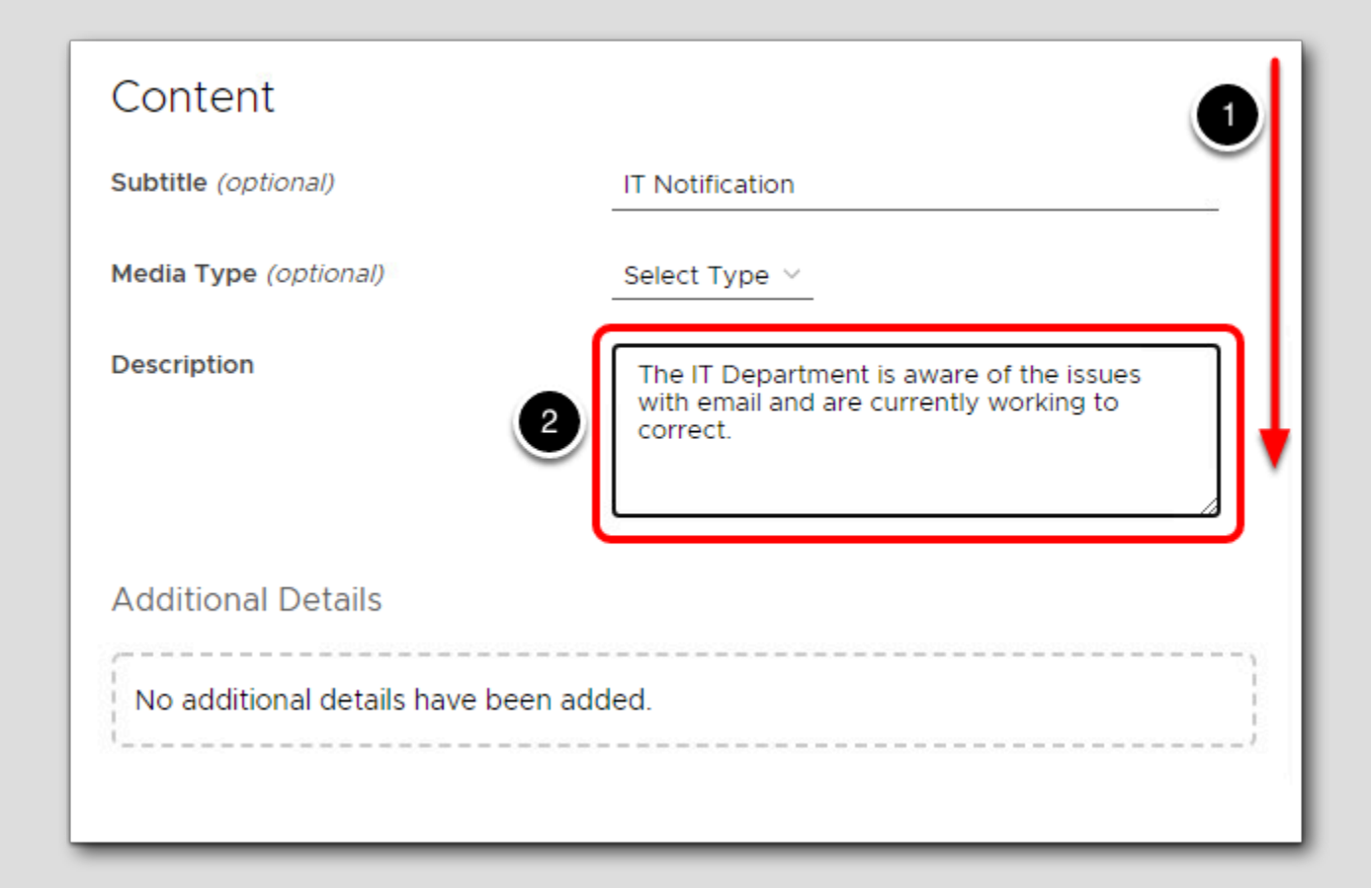
[549]



1. 通知は、[Informational] または [Actionable] のいずれかです。[Actionable] 通知には、ユーザーがクリックして通知を受け入れる、拒否する、許可する、承認する、またはアクションを実行するボタンが含まれています。[Informational] 通知は、ユーザーが読む情報を通知するだけです。テンプレートは [Informational] のままにします。
2. [Title] に **`Email Outage`** と入力します。
3. [Subtitle] に **`IT Notification`** と入力します。

通知内容を続ける

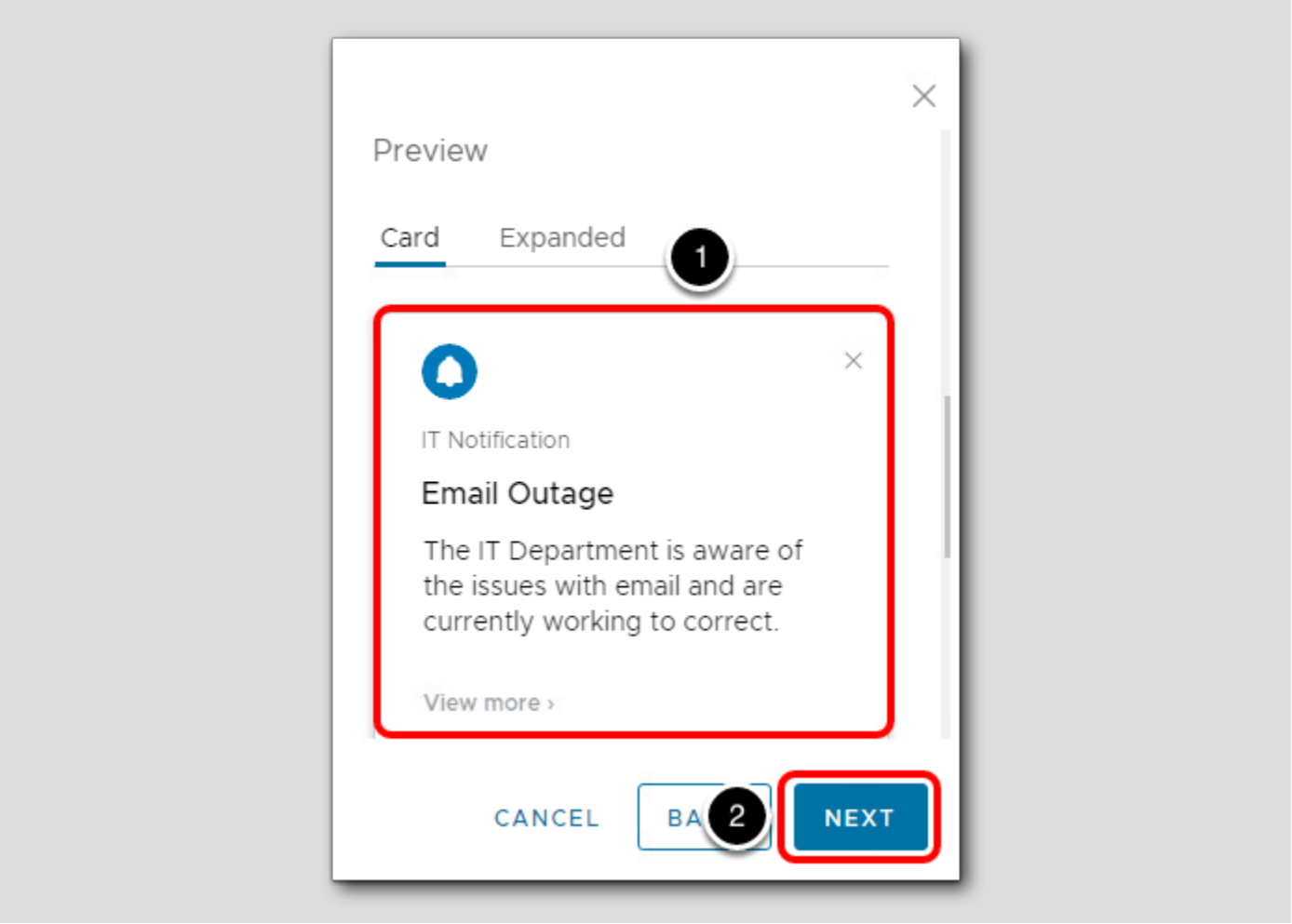
[550]



1. 1. 下にスクロールして [説明] フィールドを見つけます。
2. 2. [説明] に「`The IT Department is aware of the issues with email and are currently working to correct.`」と入力します。

通知のサマリの確認

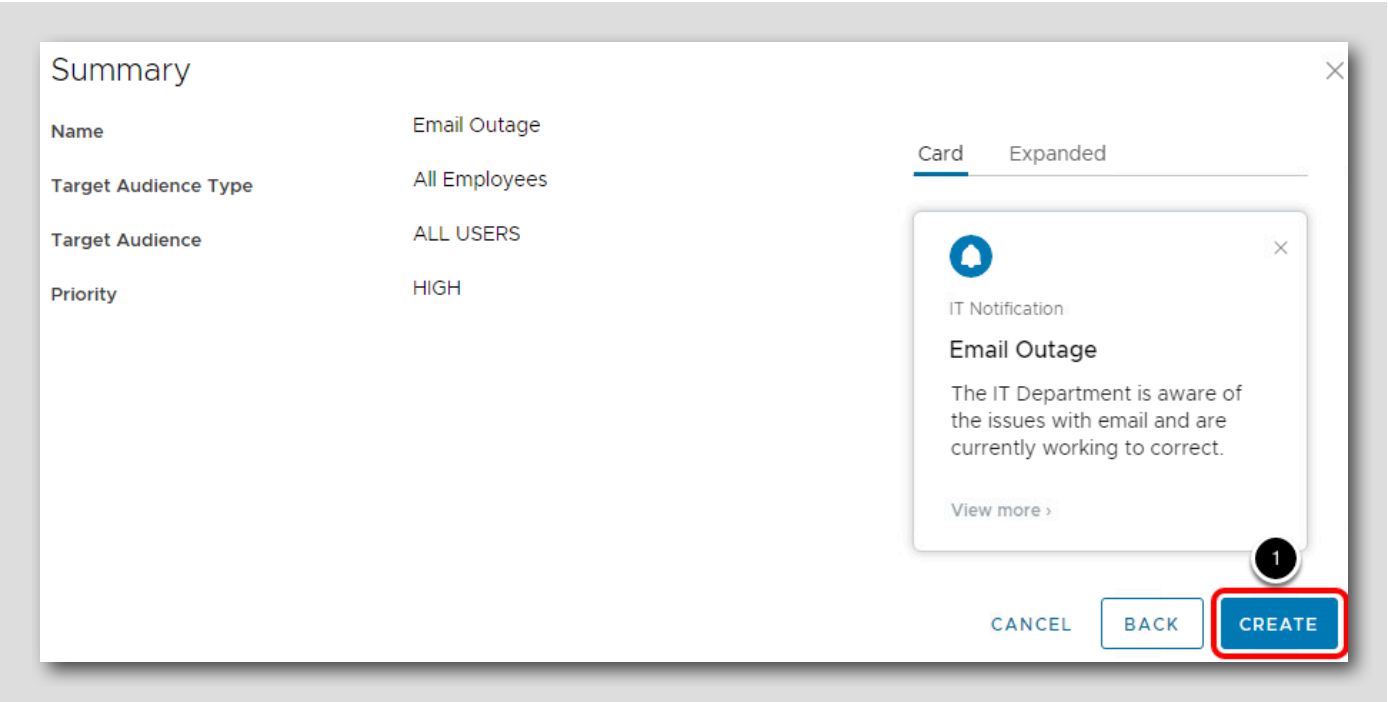
[551]



1. コンテンツを変更すると、画面の右側にある Hub サービス コンソール内で通知のプレビューを表示できます。
2. [NEXT] をクリックします。

通知の概要の確認

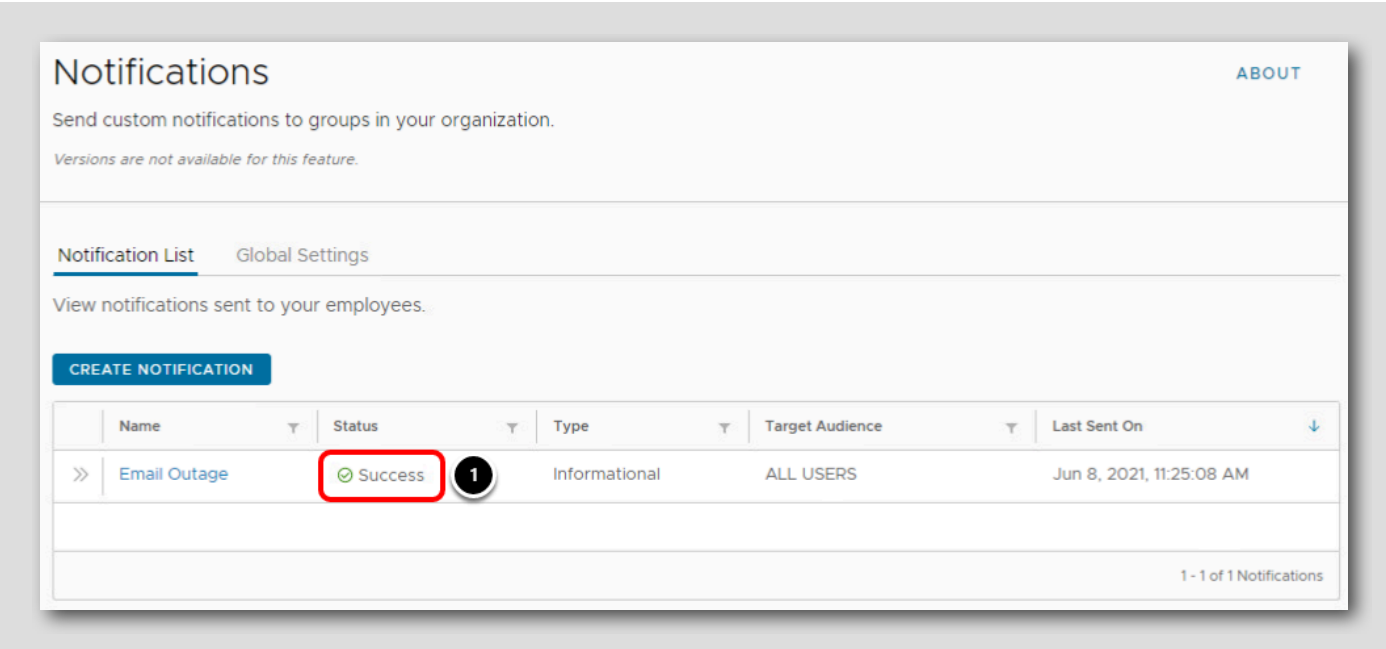
[552]



1. 1. 通知設定を確認し、「CREATE」をクリックします。
2. これはこの実習ラボのシナリオ例にすぎませんが、Hub サービス通知フレームワークは、電子メールやその他の通信媒体が利用できない場合に特に役立ちます。

通知ステータスの確認

[553]

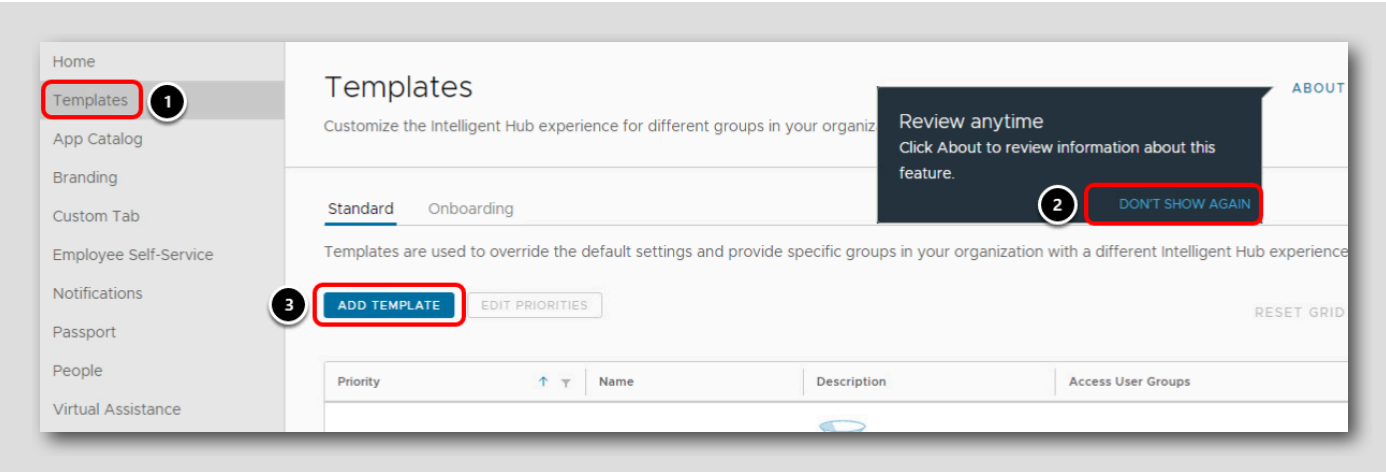


通知の送信には約 10 ～ 15 秒かかります。

1. このセクションで作成した [Email Outage] の通知に「Success」のステータスが表示されることを確認します。

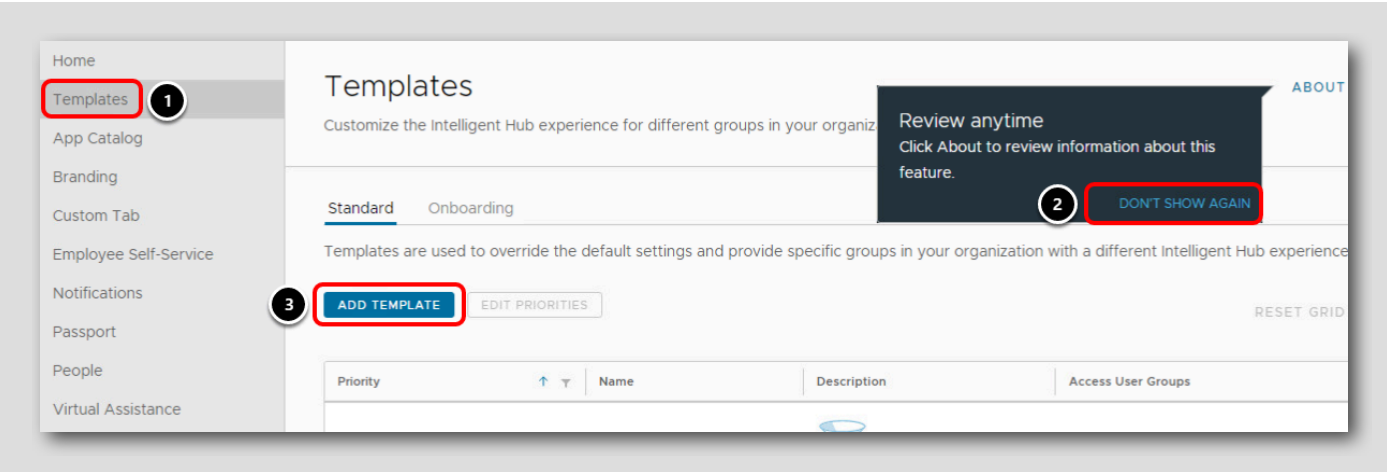
新しいテンプレートへの Hub 設定の割り当て

[554]



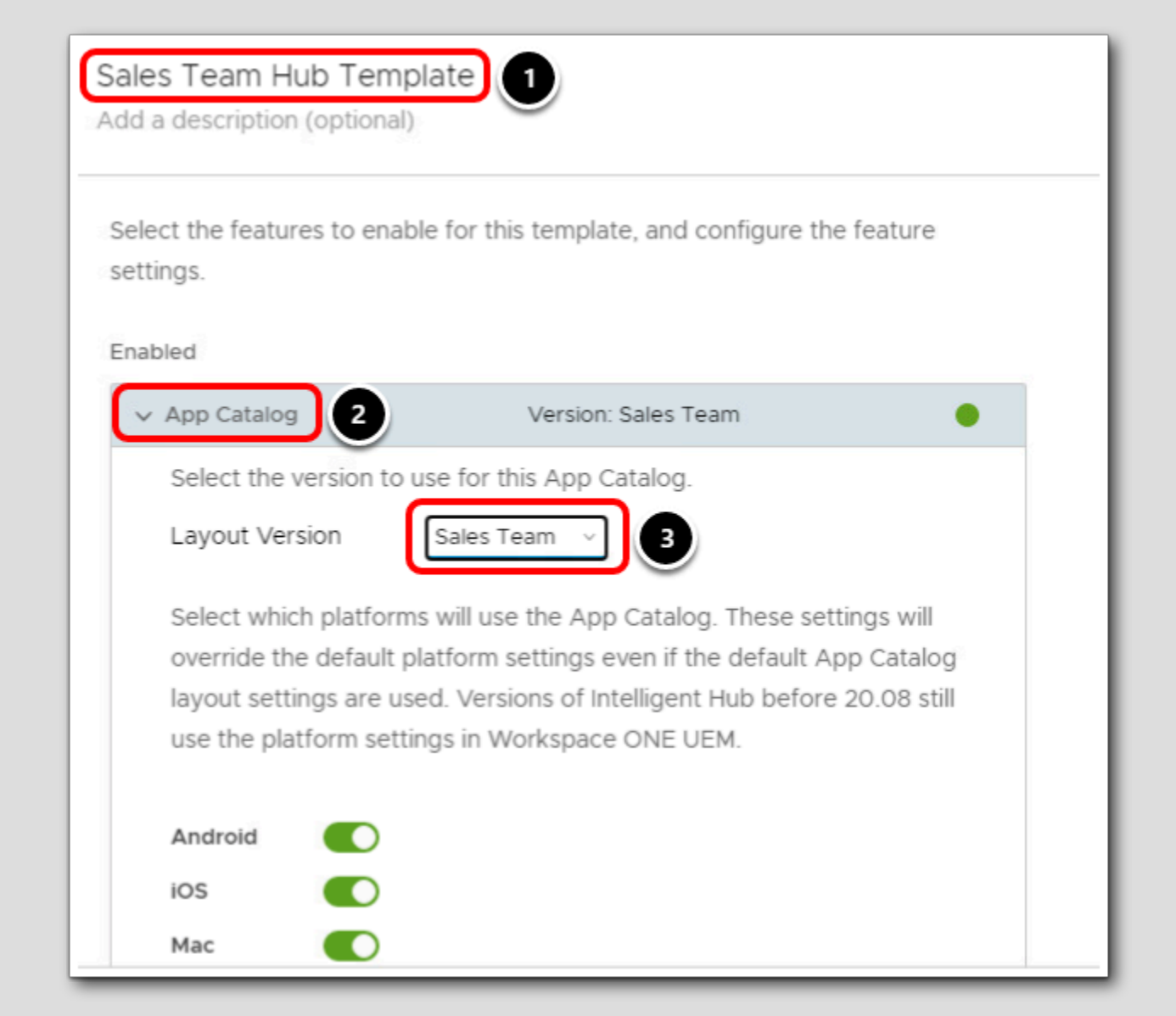
1. 左側の [Templates] メニュー項目をクリックします。

2. [Review anytime] ポップアップが表示されたら、**[DON'T SHOW AGAIN]** をクリックして閉じます。
3. **[ADD TEMPLATE]** をクリックして、セールス チームの新しい Intelligent Hub テンプレートを作成します。



セールス チームの新しい Hub テンプレートの変更

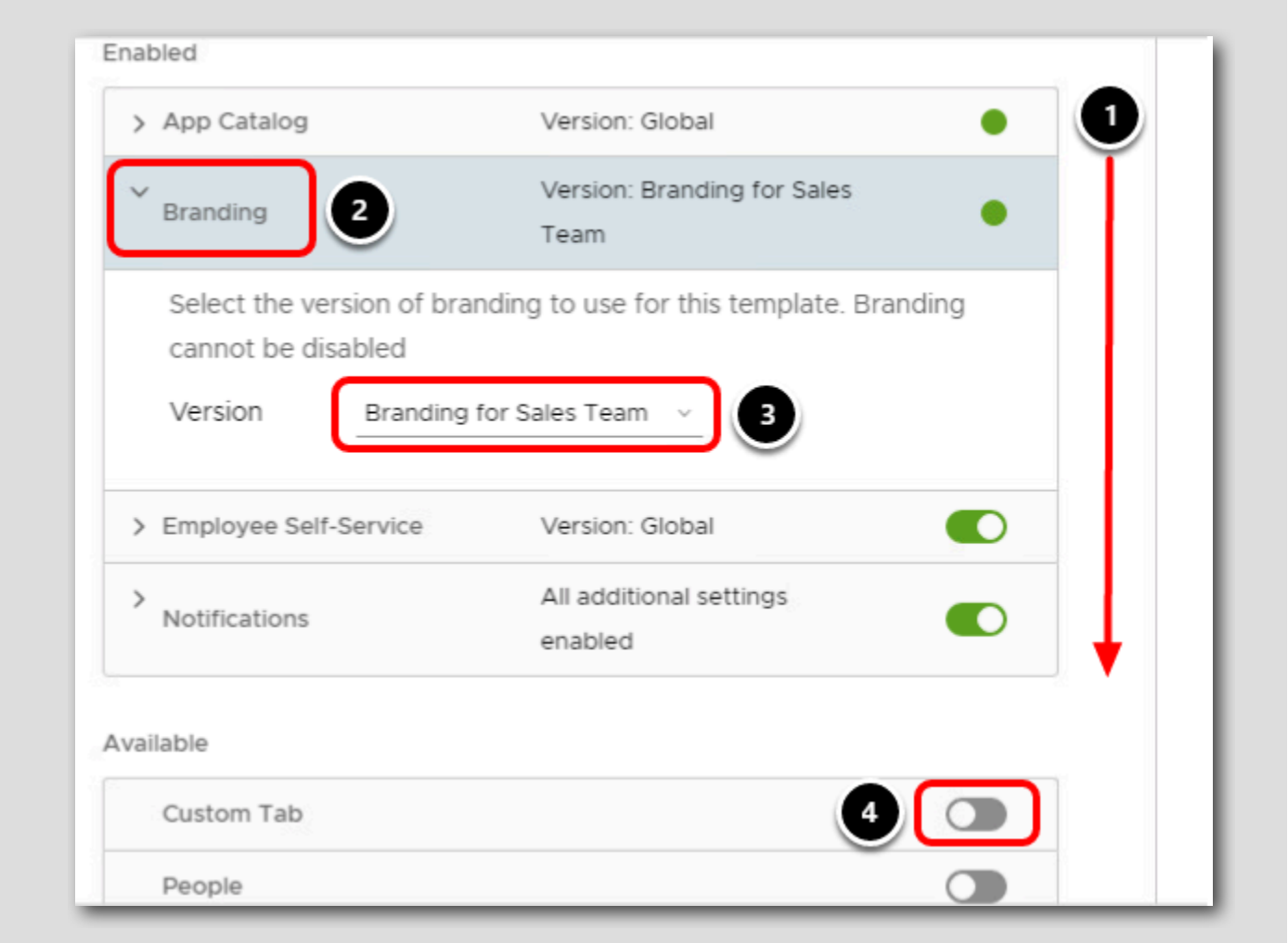
[555]



1. `Sales Team Hub Templete` と入力して、新しいテンプレートに名前を付けます。
2. [App Catalog] をクリックして、このセクションを展開します。
3. [Layout Version] ドロップダウンから [Sales Team] を選択します。これは、このモジュールで以前に作成したカタログ レイアウトのバージョンです。

セールス チームの Hub テンプレートの変更を完了する

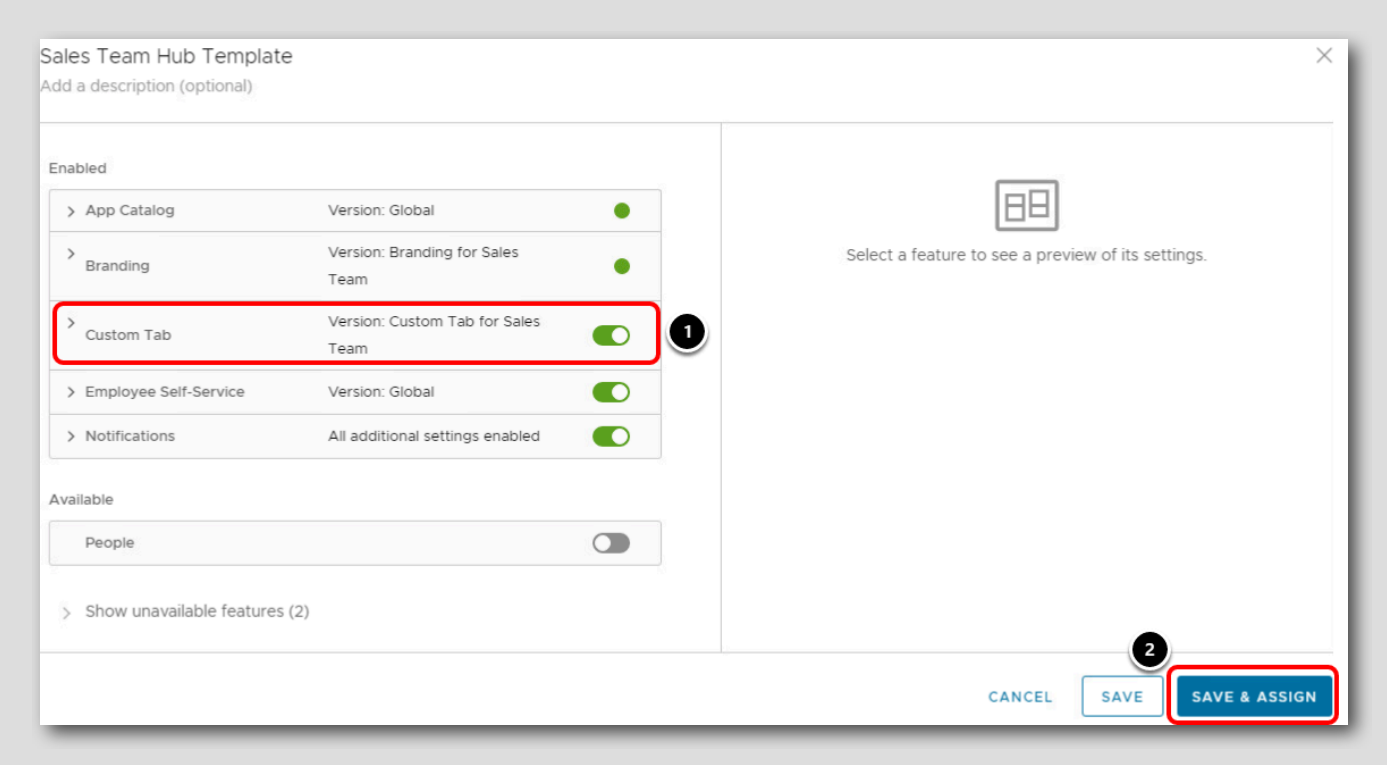
[556]



1. 下にスクロールして、ブランディング設定を見つけます。
2. [Branding] セクションを展開します。
3. ドロップダウンで **[Branding for Sales Team]** バージョンを選択します。
4. **[Custom Tab]** をオンにして、緑色にします。オンにすると、[Custom Tab] は有効なサービスのリストに移動し、[Available services] セクションから削除されます。

新しい Hub テンプレートの保存

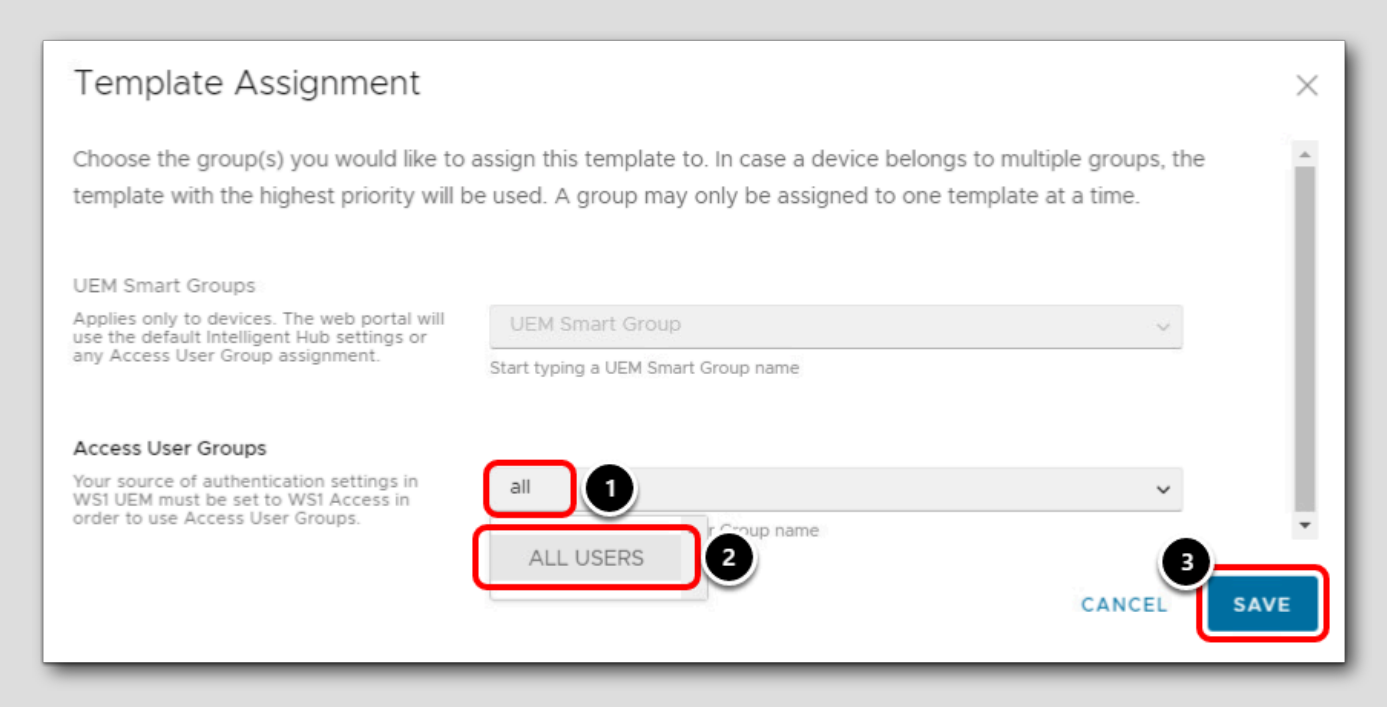
[557]



1. [Custom Tab] 設定が [Available services] から [Enabled] セクションに移動したことを確認します。
2. [SAVE & ASSIGN] をクリックします。

ユーザー グループへの Hub テンプレートの割り当て

[558]

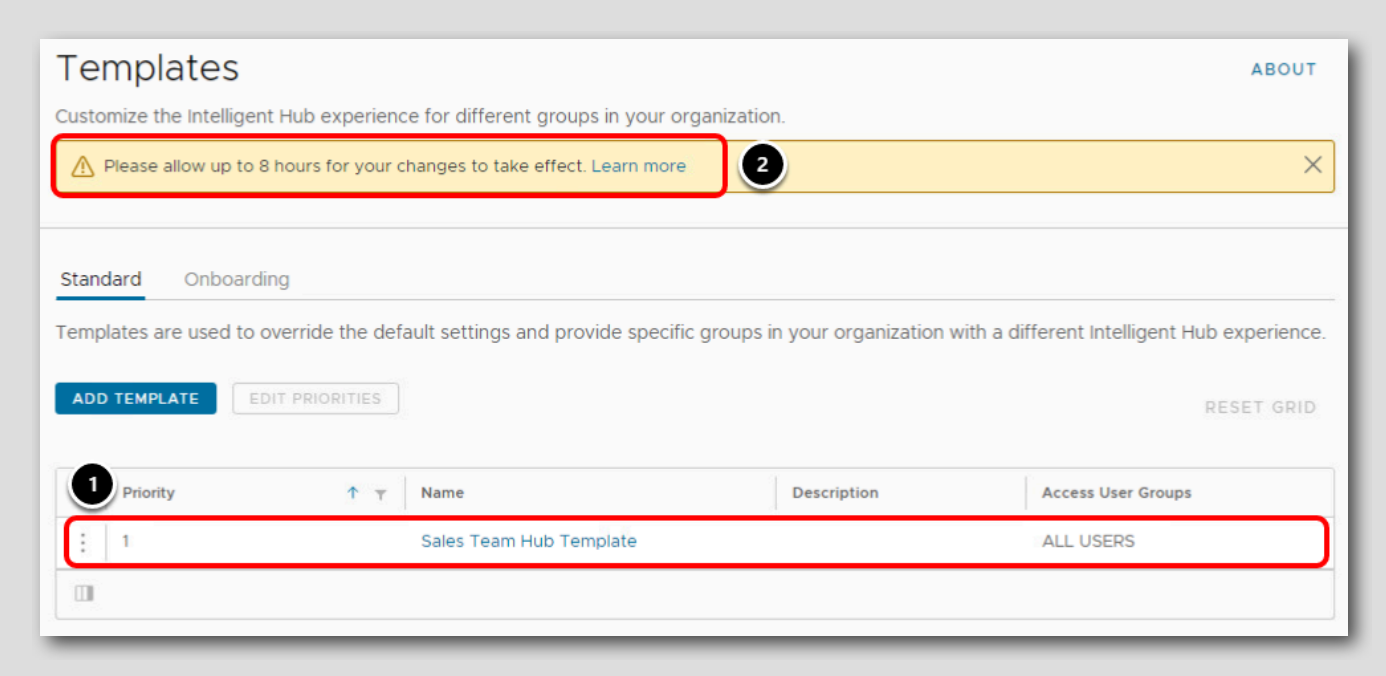


ポップアップ表示される [Template Assignment] ダイアログ ボックスで、次の手順を実行します。

1. [Access User Groups] 検索バーに **`all`** と入力します。
2. [ALL USERS] 検索結果をクリックします。
3. [SAVE] ボタンをクリックします。

Hub テンプレートの割り当ての確認

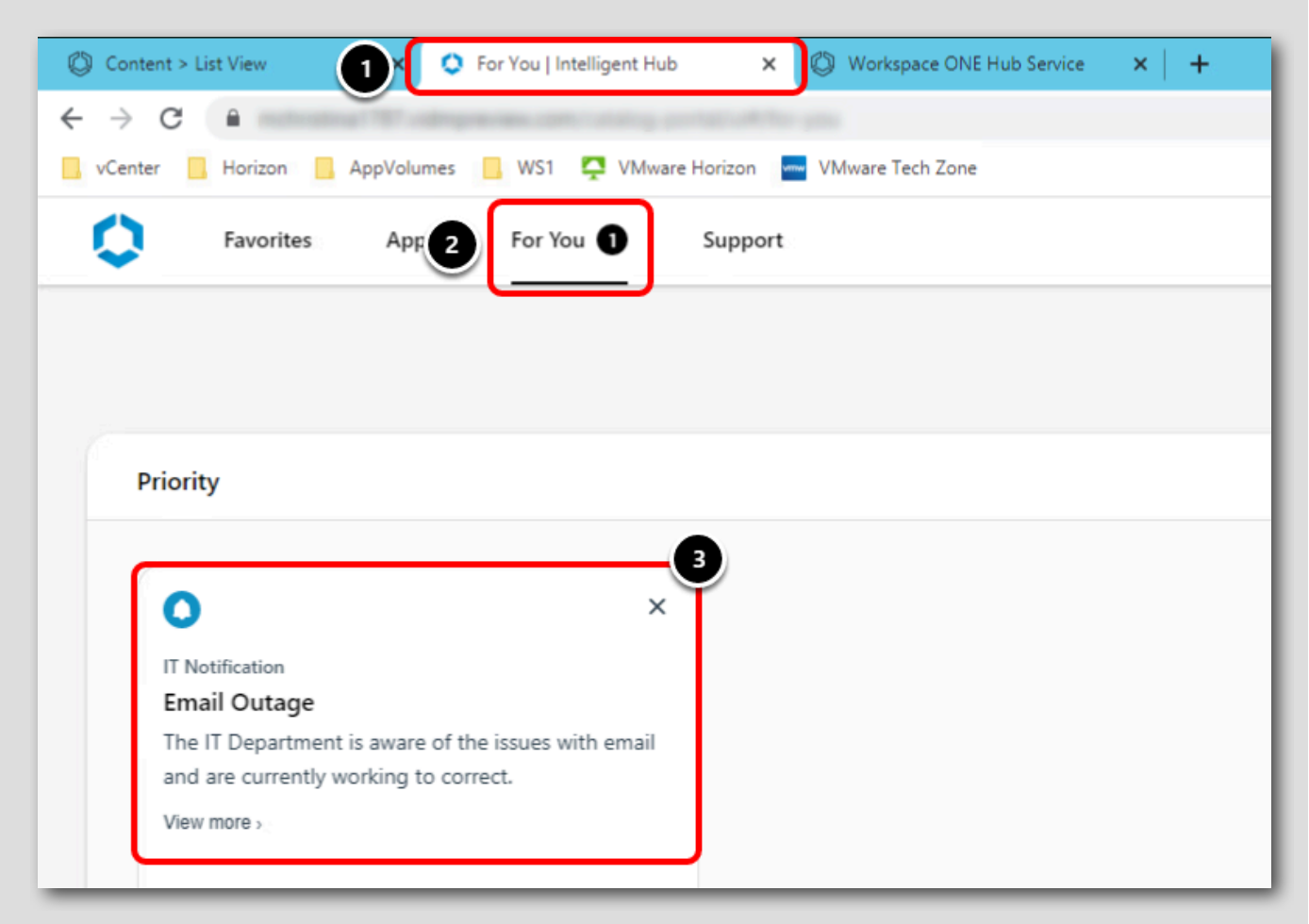
[559]



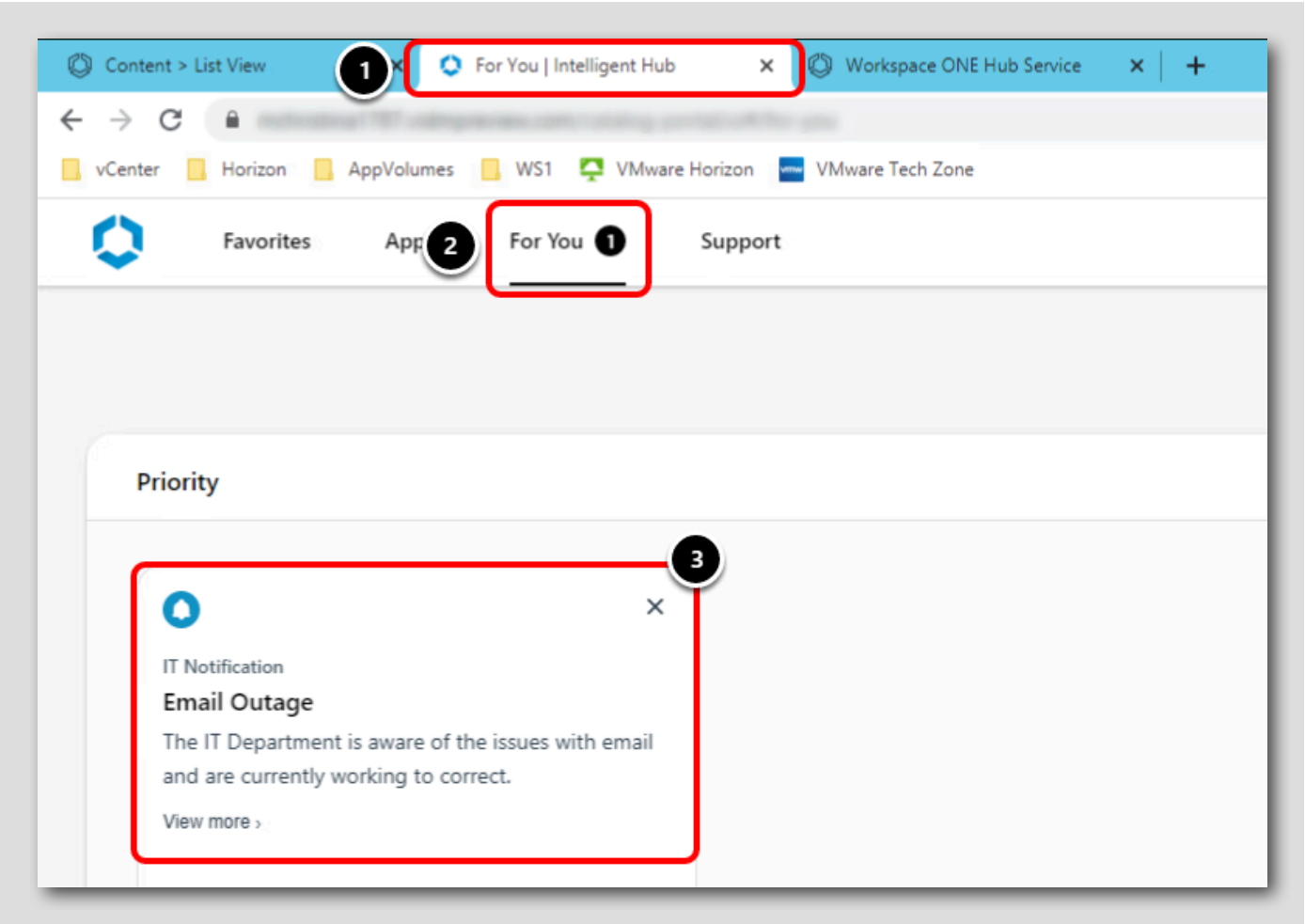
1. セールス チームの Hub テンプレートが ALL USERS に割り当てられていることがわかります。優先順位は、複数のユーザー グループに存在するユーザーの競合を管理するために使用できます。
2. 画面上部の通知は気にしないでください。遅延を回避するために、ブラウザでログアウトしてから Intelligent Hub に再度ログインします。

Intelligent Hub でのカスタマイズの確認

[560]

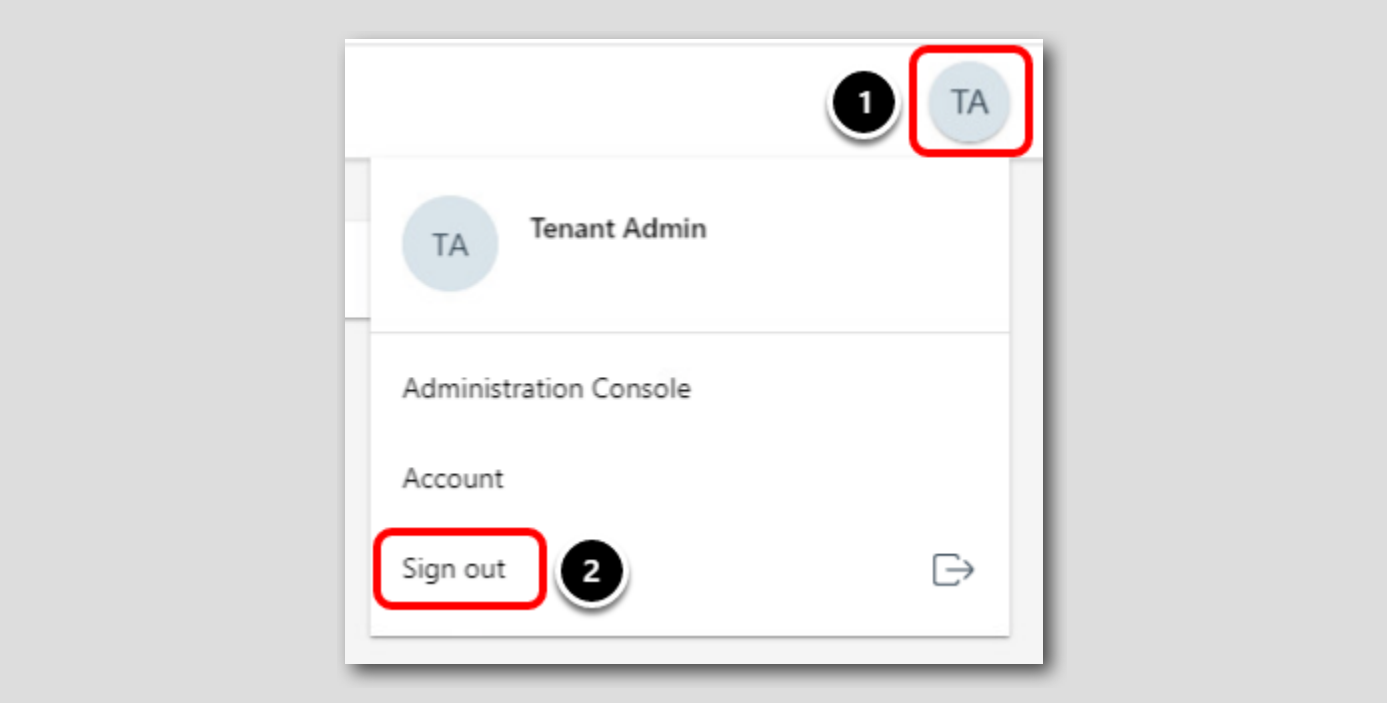


1. ブラウザの 2 番目のタブをクリックします。これは、Intelligent Hub ユーザー ポータルです。
2. Intelligent Hub で [For You] タブをクリックします。タブの通知数が 1 で、新しい通知が 1 つあることを示します。
3. 作成した IT 通知が [For You] タブの [Priority] セクションにすぐに表示されます。ブラウザの表示を更新する必要はありません。通知カードの右上にある X をクリックして、通知の表示を消し、通知を履歴に移動します。


Content > List View
1
For You | Intelligent Hub
Workspace ONE Hub Service
vCenter
Horizon
AppVolumes
WS1
VMware Horizon
VMware Tech Zone
Favorites
App
2
For You
1
Support
Priority
3
IT Notification
Email Outage
The IT Department is aware of the issues with email and are currently working to correct.
View more ›

Intelligent Hub からのログアウト

[561]

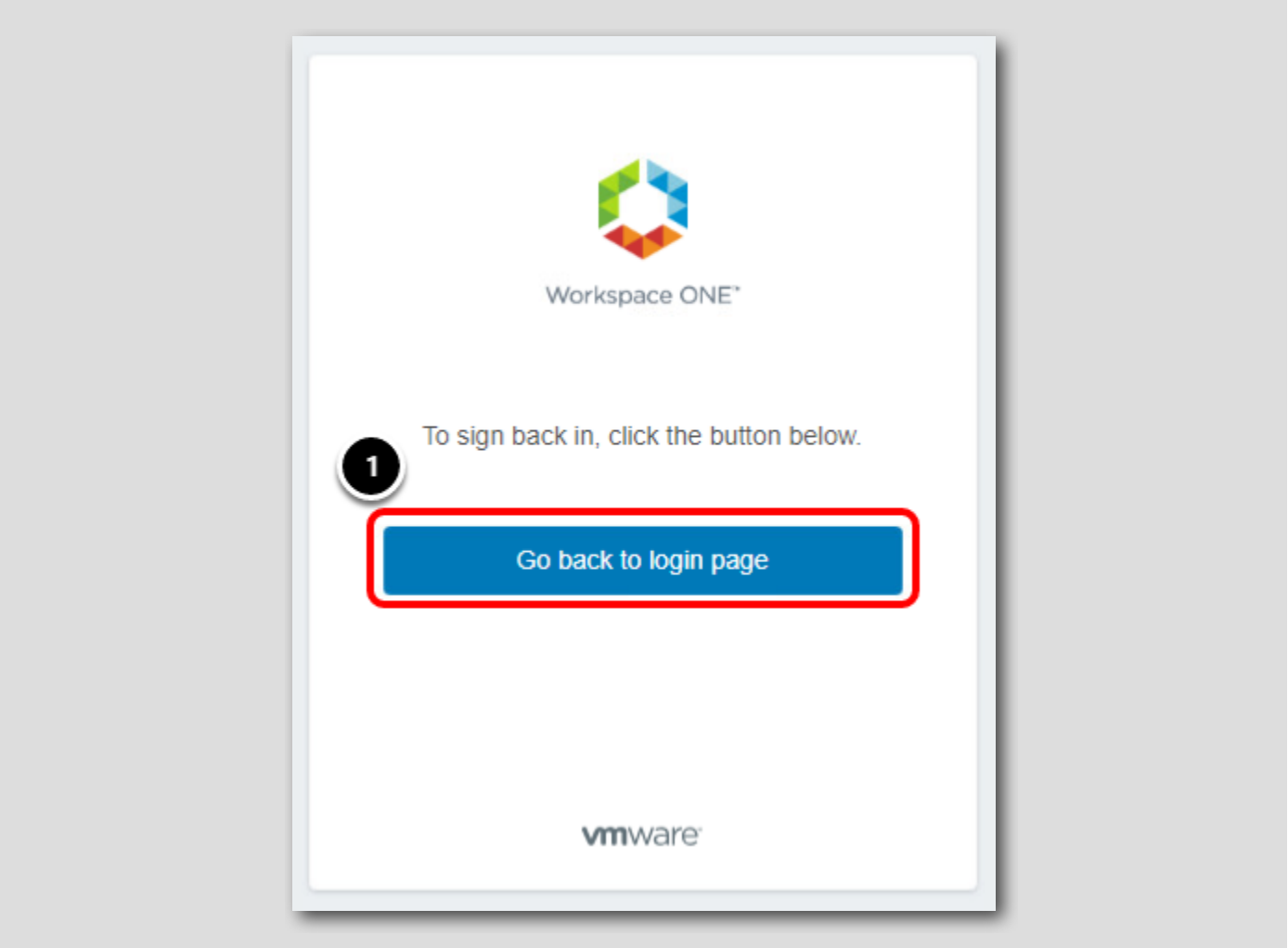


以前に行った [App Catalog]、[Branding]、および [Custom Tab] の変更を表示するには、Intelligent Hub からログアウトして再度ログインする必要があります。

1. Intelligent Hub の右上にある円形のユーザー ドロップダウン メニューをクリックします。
2. [Sign out] をクリックして、Intelligent Hub からログアウトします。

Intelligent Hub ログイン ページに戻る

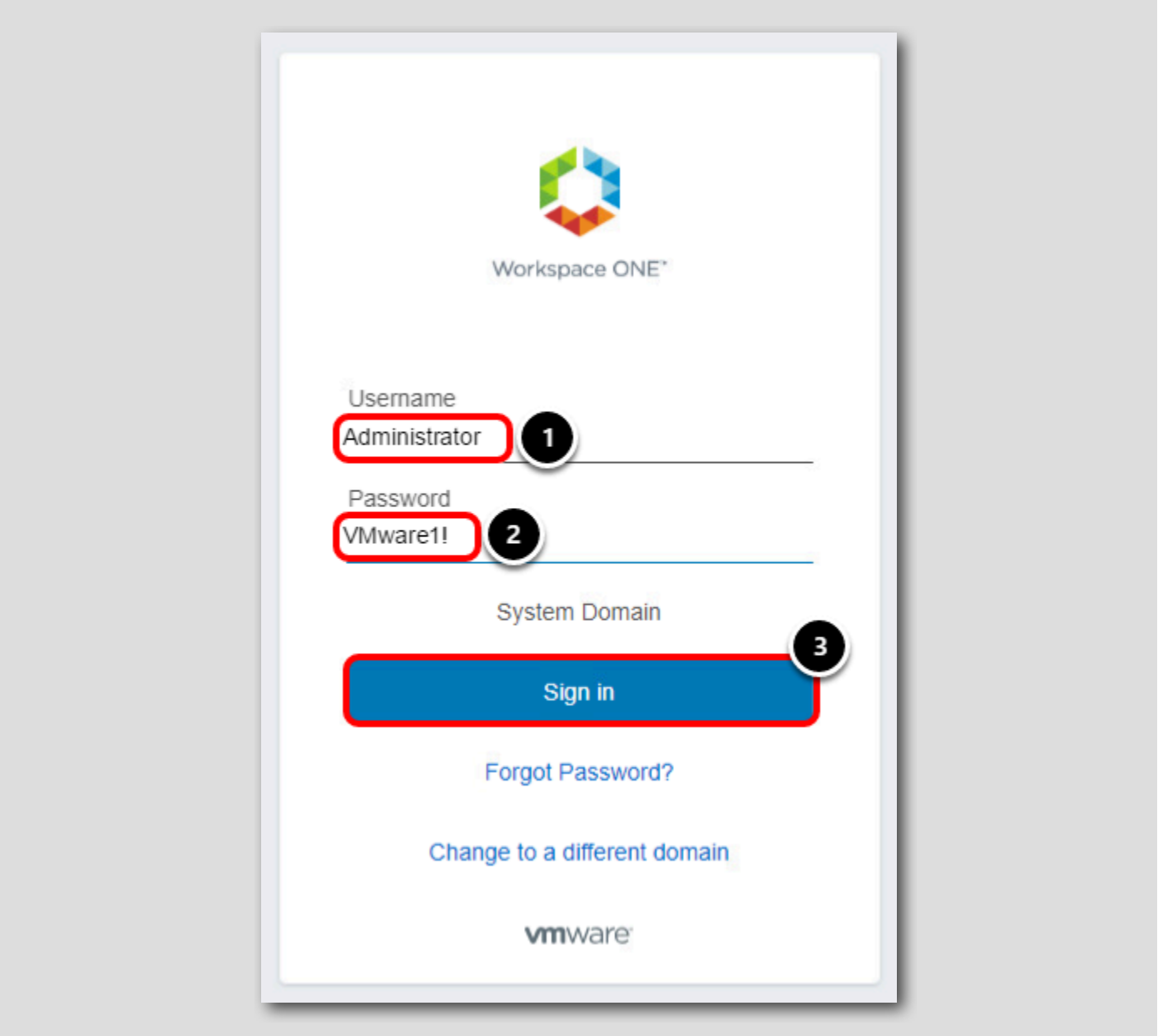
[562]



1. [Go back to login page] ボタンをクリックします。

Intelligent Hub にログインし直す

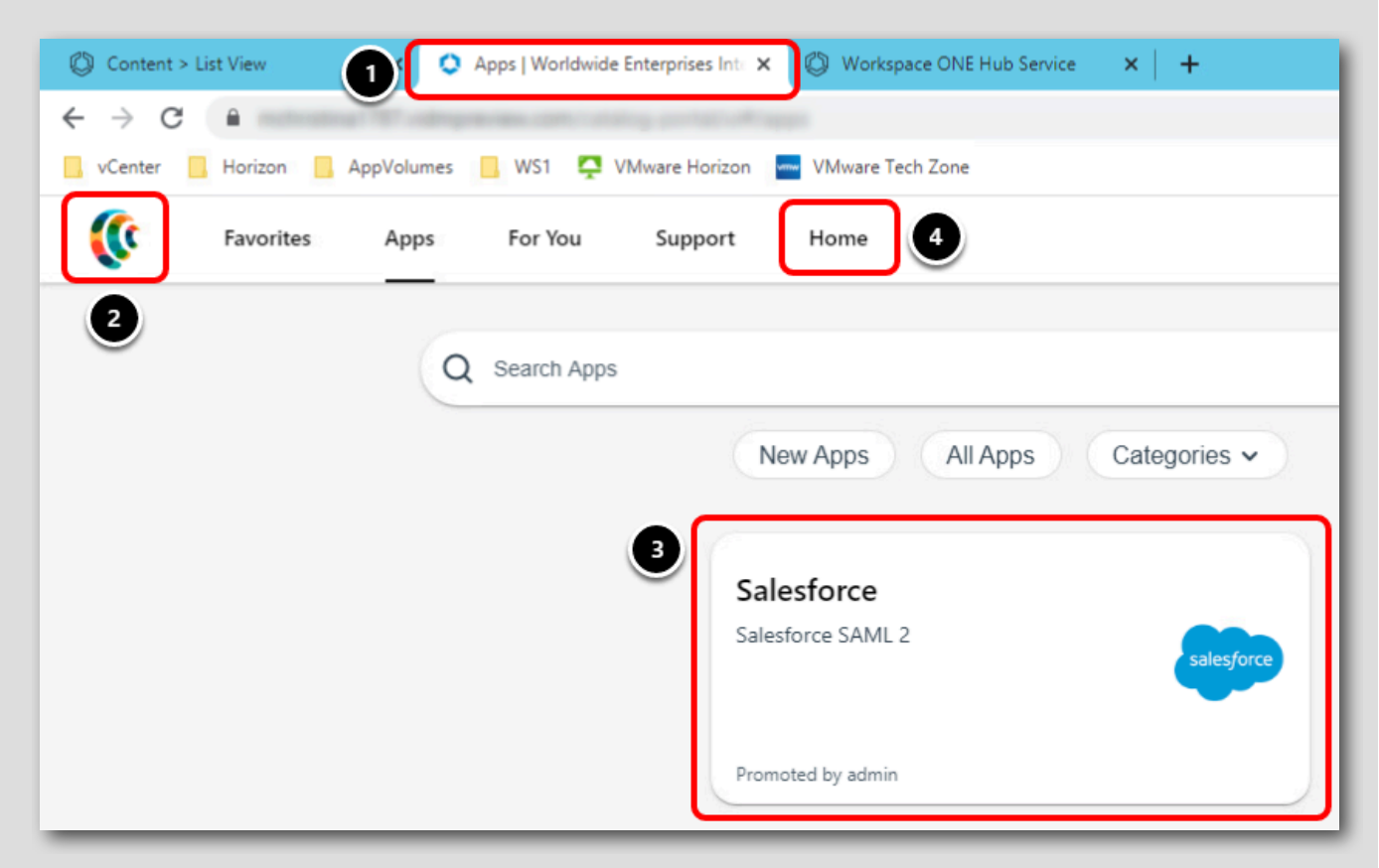
[563]



1. [Username] に **`administrator`** と入力します。
2. [Password] に **`VMware1!`** と入力します。
3. [Sign in] ボタンをクリックします。

[Branding]、[App Catalog]、[Custom Tab] の変更の確認

[564]



1. ブラウザのタブの会社名が「Worldwide Enterprises」に変更されていることを確認します。
2. 会社のロゴがアップロードしたロゴに変更されていることを確認します。
3. Salesforce アプリケーションがアプリケーション カタログの最上部に昇格したことを確認します。
4. **[Home]** タブをクリックすると、前に入力した URL で新しいブラウザ タブが開きます。

まとめ

[565]

おめでとうございます。これで、Workspace ONE Intelligent Hub と Hub サービスのモジュールは終了です。このモジュールでは、次の方法について学習しました。

- Workspace ONE Hub サービスを構成し、Intelligent Hub内でカスタマイズを表示します。
- Intelligent Hub カタログに SaaS アプリケーションを追加します。
- さまざまなバージョンの Intelligent Hub 設定を作成し、Hub テンプレートに割り当てます。

- Intelligent Hub アプリケーション カタログのレイアウトをカスタマイズします。
- Workspace ONE Intelligent Hub アプリケーションのブランディングをカスタマイズします。
- Intelligent Hub のカスタム タブを作成します。
- カスタム通知を作成して Intelligent Hub アプリケーションに送信します。

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[566]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。


Your Personal journey from zero to IT Superhero
TECH ZONE
Hands on Labs, Tools and Best Practices
How the products work – beginner to expert
Guide to production deployments & operations
Quick start for your first proof of concept
Latest product information

モジュール 7：Workspace ONE Intelligence - ダッシュボード、自動化、レポートの概要（45 分）

はじめに

[568]

IT 管理者が最新のモバイル ワーク スタイルを管理するために利用できるデータが非常に多く、それを理解するための単一のツールがないため、IT 部門はデジタル ワークスペースを管理するという大きな課題に直面しています。デバイス、アプリケーション、およびユーザー間で可視性に一貫性がないため、データ主導の意思決定を行うことは特に困難です。その結果、手動でのプロセスが標準になり、IT 部門は、プロアクティブに対応するのではなく、従業員の要求や外部イベントに対してリアクティブに対応するように追い詰められています。

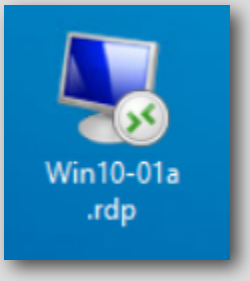
深い洞察により、IT 管理者は、ネットワークのパフォーマンス、リソースの権限、展開のリスクに基づいて、アプリケーションとポリシーの展開をより適切に計画および最適化できるようになります。また、プロセスを自動化する機能により、IT 管理者は、ユーザーのエクスペリエンスを向上させながら、セキュリティの健全性をプロアクティブに高め、コンプライアンス要件を満たすことができます。

Workspace ONE Intelligence の中心に新しい*ルール エンジン*を配置することで、IT 管理者は、豊富なパラメータ セットに基づいてアクションを実行するルールを定義することにより環境全体のプロセスを自動化できます。これにより IT 部門は、セキュリティの脅威に基づいて自動化された修復アクションを実行し、自動化されたアクセス制御を通じてコンプライアンス要件を満たす*コンテキスト ワークフロー*を作成できます。また、Workspace ONE Intelligence は、サードパーティ向けの API レイヤーに*拡張性*を提供するため、IT 管理者は独自の環境を活用するワークフローを構築してニーズを満たすことができます。

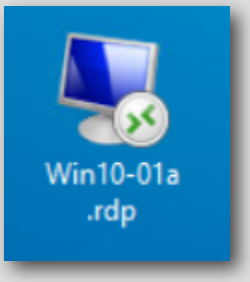
自動化を備えた Workspace ONE Intelligence は、IT 部門がコンプライアンス要件を満たし、自動修復を通じてセキュリティを強化するのに役立ちます。

Windows 10 仮想マシンへの接続

[569]



メイン コンソール デスクトップにある **[Win10-01a.rdp]** ショートカットをダブルクリックして、Windows 10 仮想マシンに接続します。



Workspace ONE UEM Console へのログイン

[570]

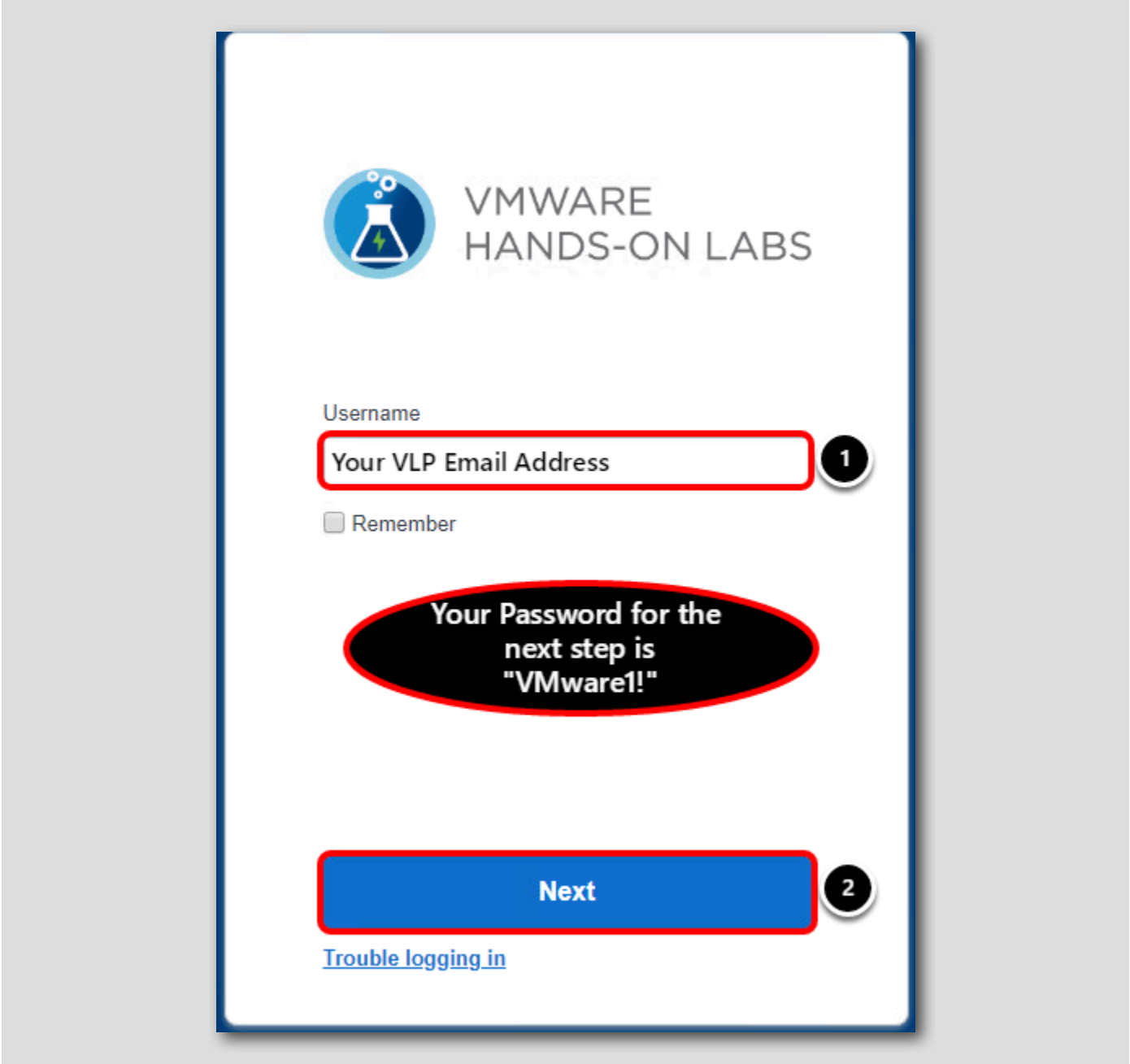
このラボでは、ほとんどの場合、Workspace ONE UEM 管理コンソールにログインします。

Chrome ブラウザの起動

[571]

現在接続している仮想マシンのデスクトップにある [Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールでの管理者ユーザー名の入力 [572]

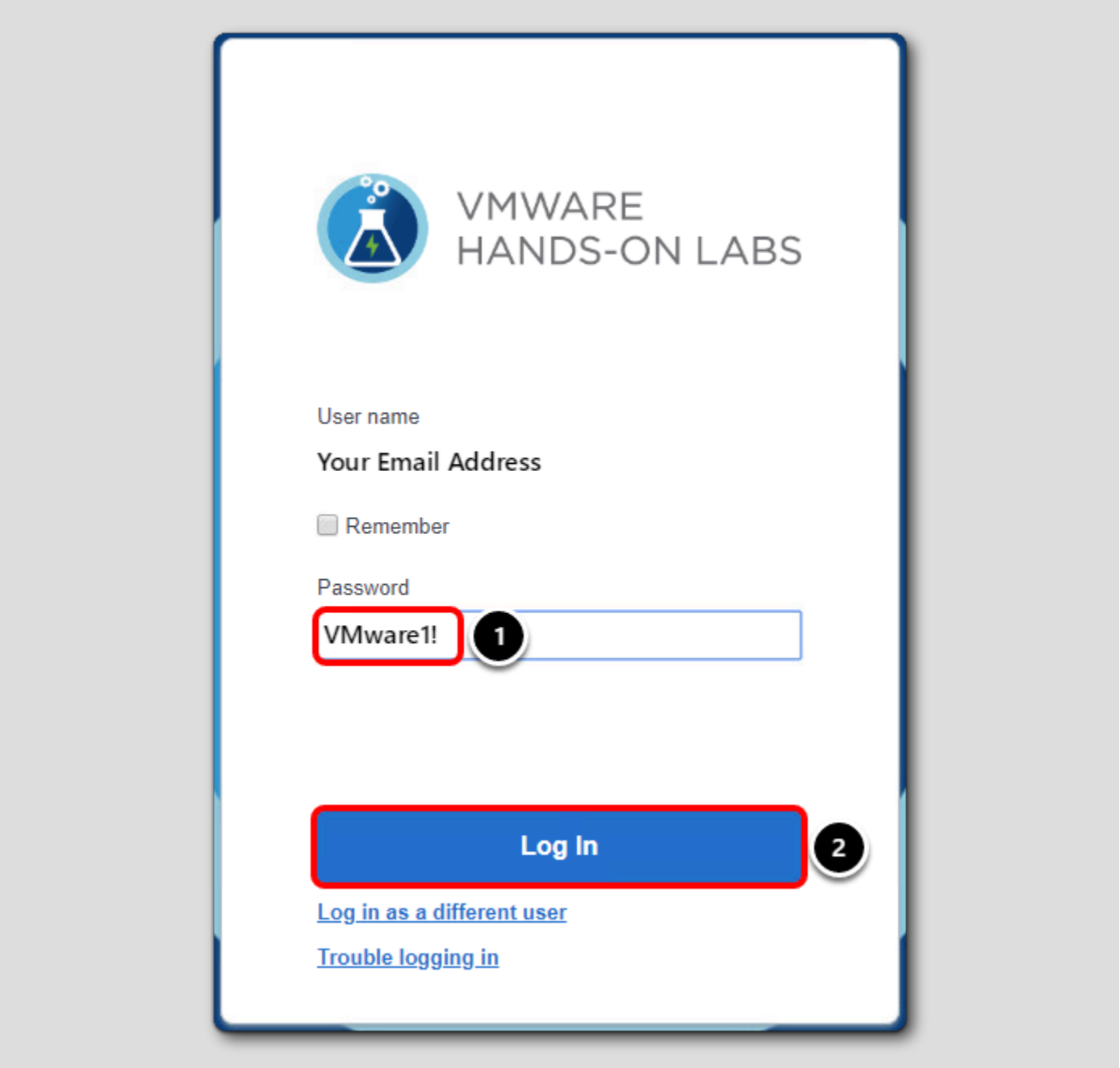


ブラウザのデフォルトのホーム ページは https://hol.awmdm.com です。Workspace ONE UEM 管理者アカウント情報を入力し、[Login] ボタンをクリックします。

1. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。
2. [Next] をクリックして、ラボ マニュアルの次の手順に進み、パスワードを入力します。これは常に **`VMware1!`** です。

注：Captcha による入力を求められた場合は、大文字と小文字を区別して入力してください。

Workspace ONE UEM Console の認証情報の入力 [573]



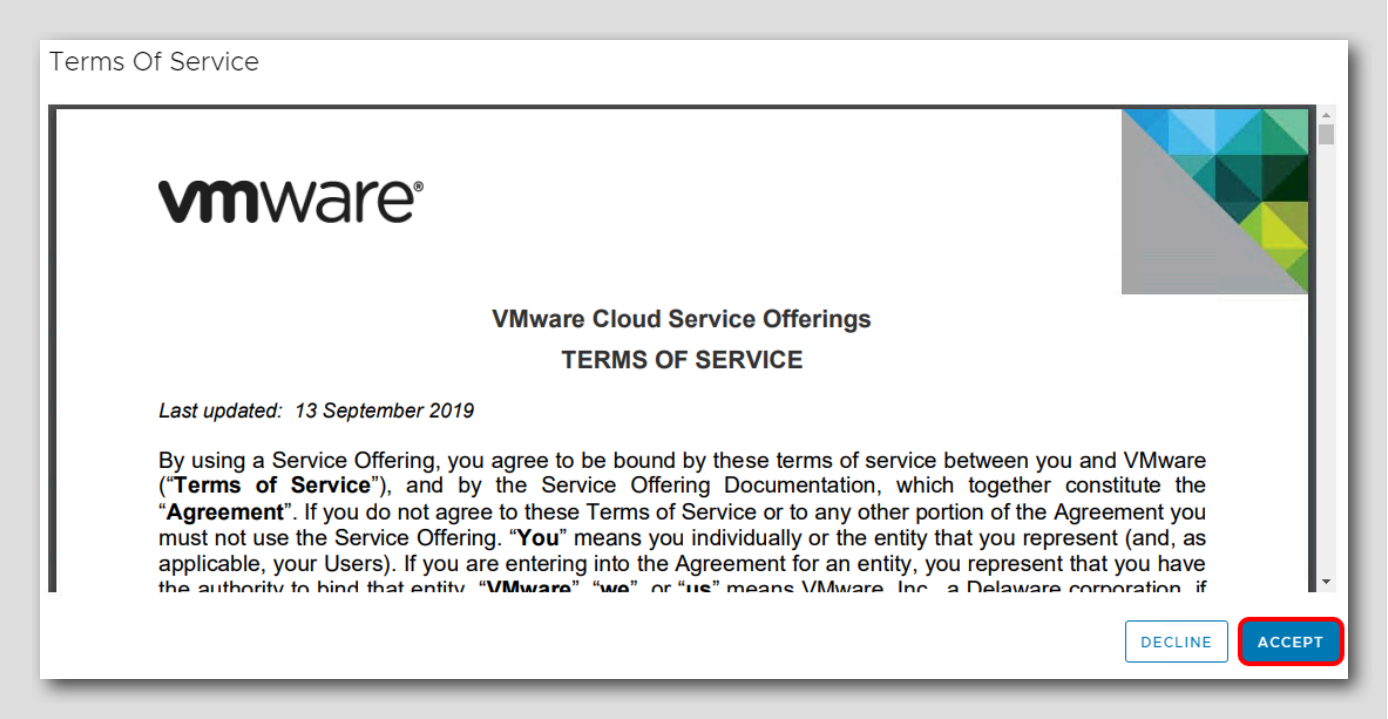
ユーザー名を入力すると、パスワード フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ラボの制限により、ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

エンド ユーザー使用許諾契約書に同意

[574]



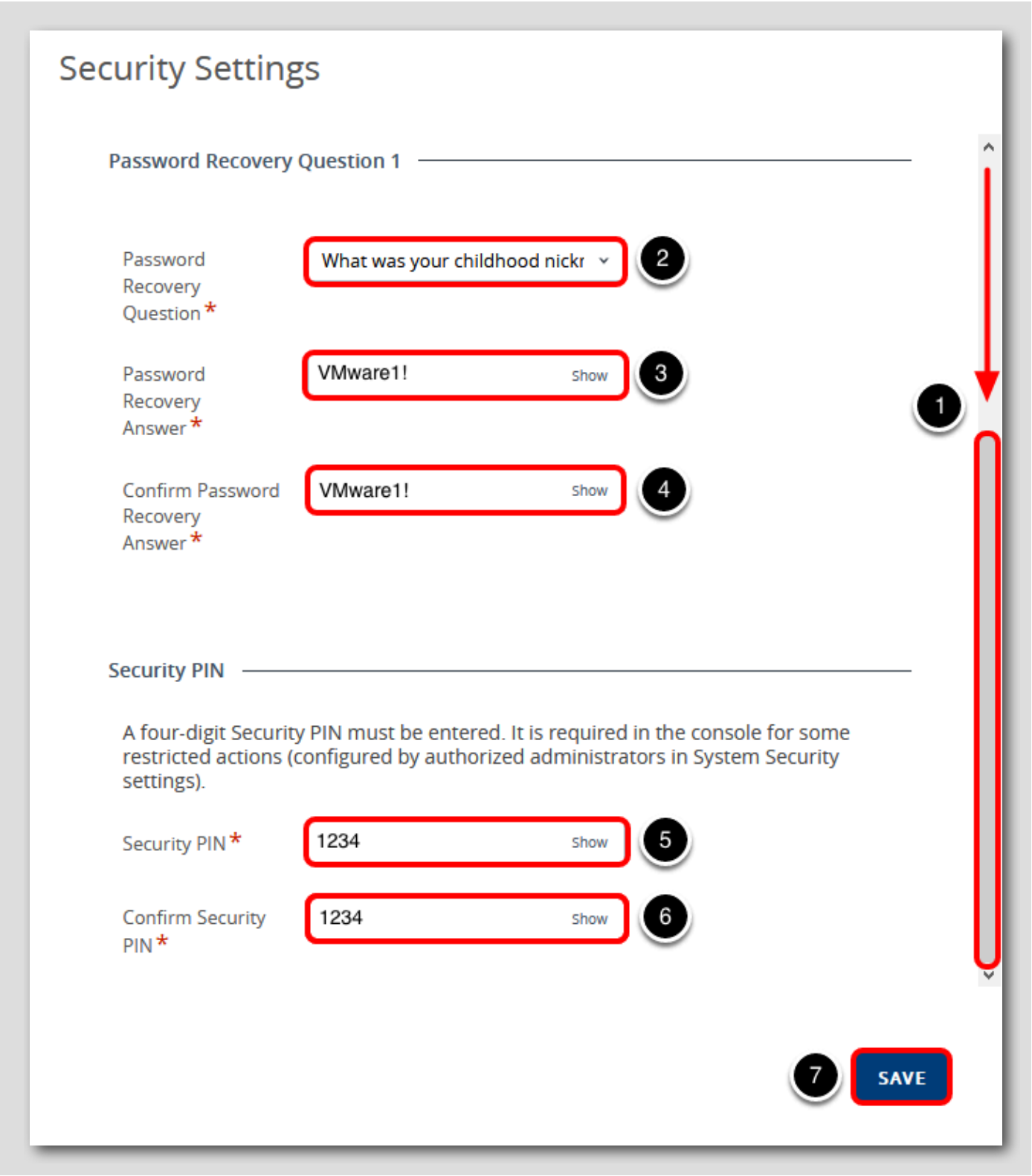
Workspace ONE UEM の「利用規約」が表示されたら、[Accept] ボタンをクリックします。

注：管理コンソールに初めてログインする場合のみ、次の手順に従ってログインしてください。

初期セキュリティ設定の完了

[575]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

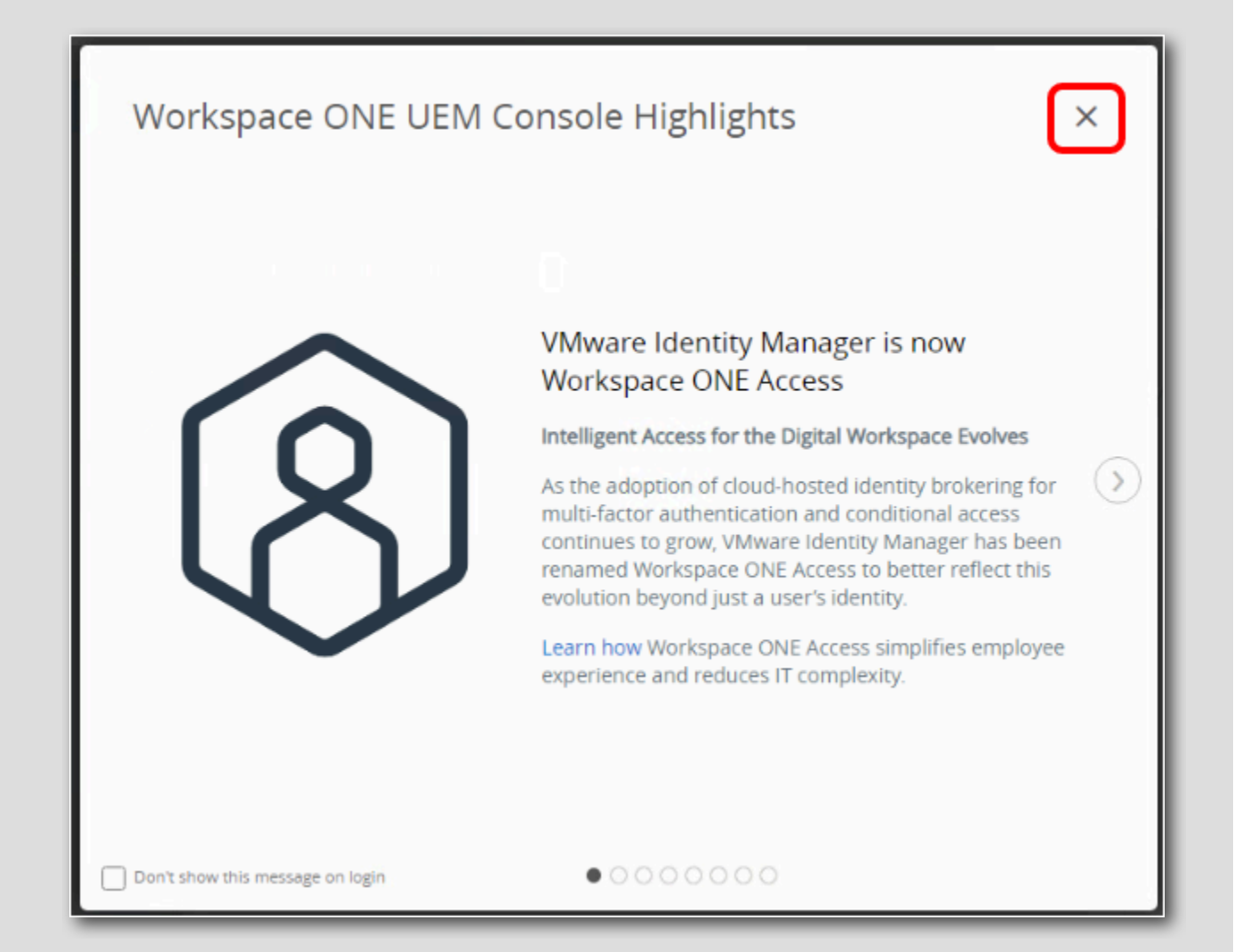

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 必要に応じて画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示してください。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[576]



セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

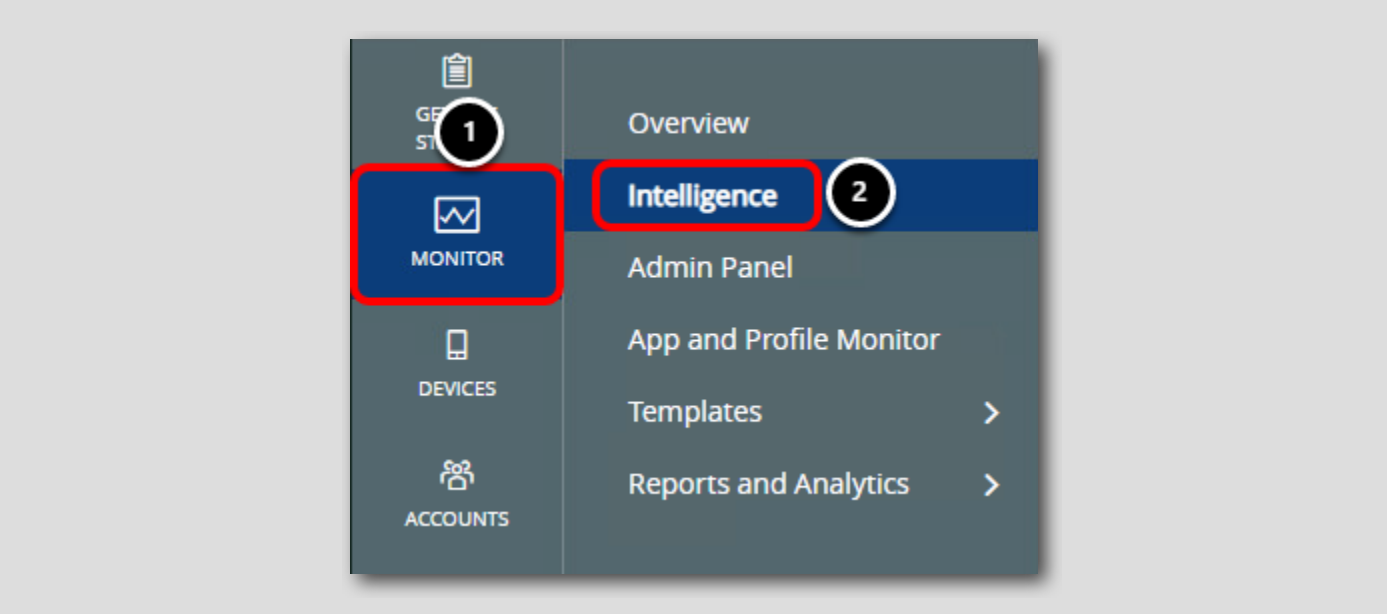
Intelligence のオプトイン プロセス

[577]

Workspace ONE Intelligence の使用を開始する最初の手順は Workspace ONE UEM とインテリジェンス クラウド サービス間のデータ同期を許可することです。これは、Workspace ONE UEM Console に管理者権限を持つユーザーが実行する必要のあるオプトイン プロセスを通じて行われます。

Intelligence へのアクセス

[578]

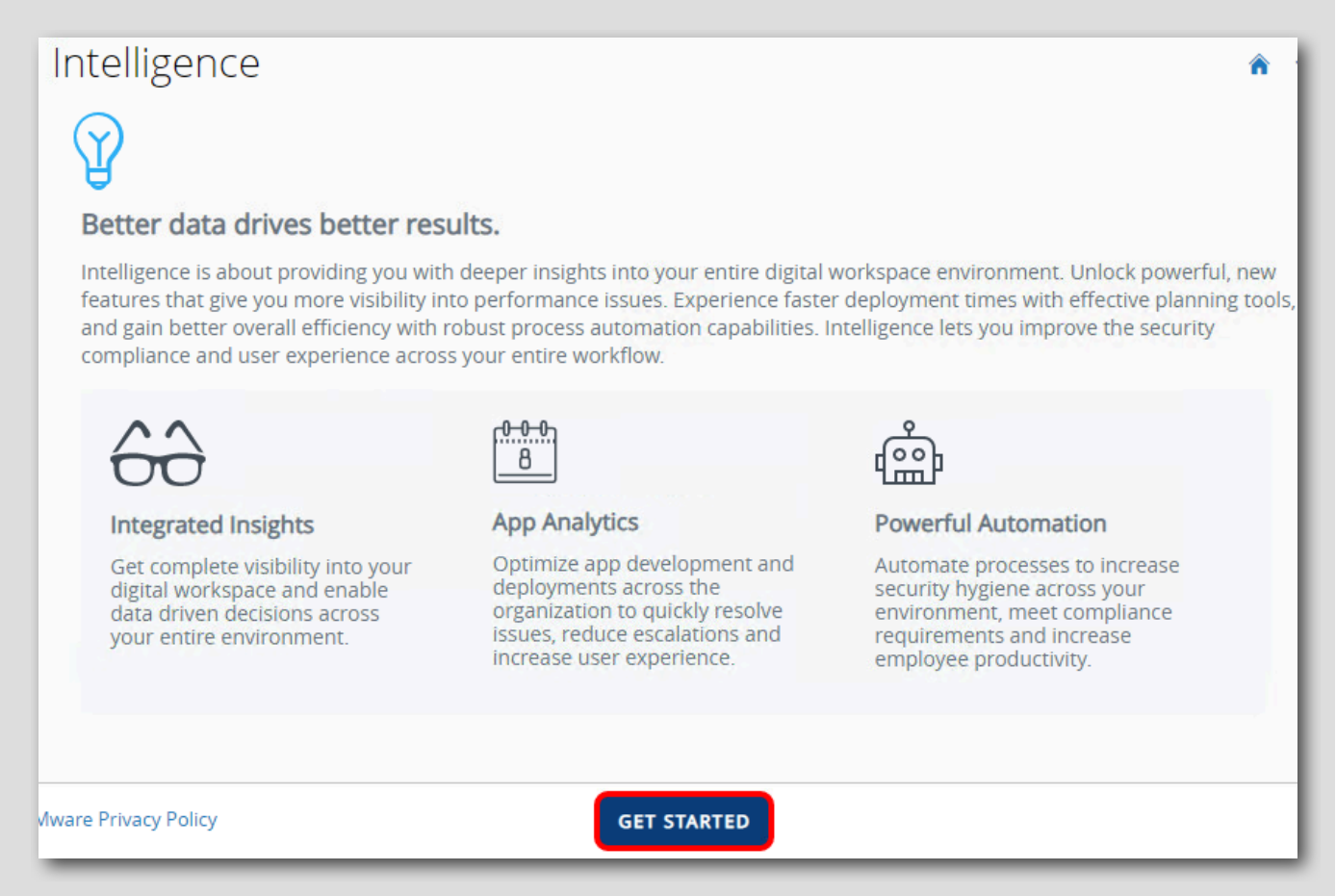


Workspace ONE UEM Console で、次のように操作します。

1. [Monitor] をクリックします。
2. [Intelligence] をクリックします。

最初のステップ

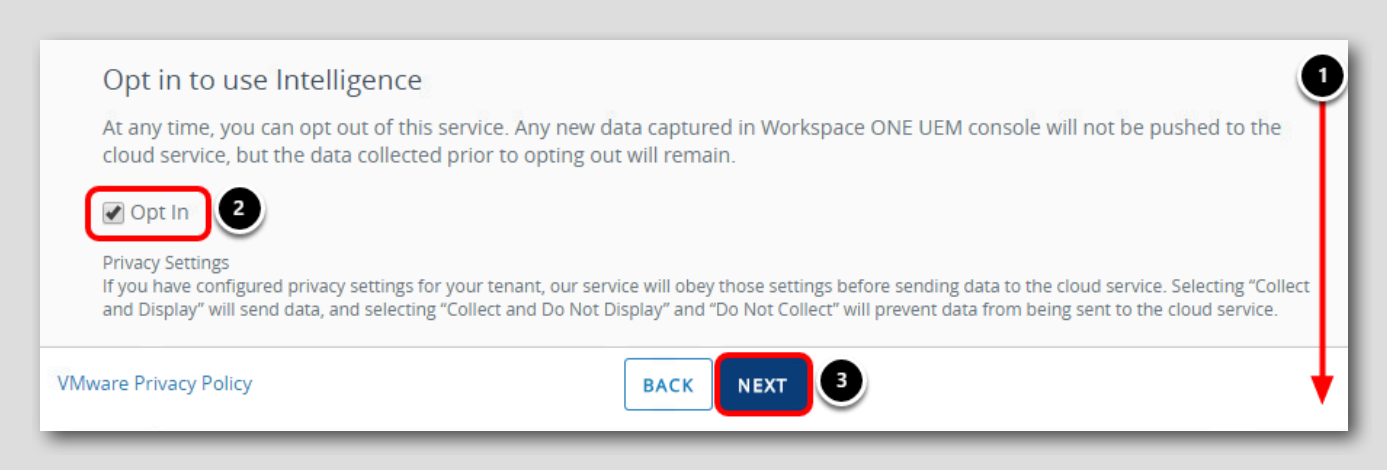
[579]



[GET STARTED] をクリックして、オプトイン プロセスを開始します。

データを収集してレプリケートするための Intelligence の認証（オプトイン）

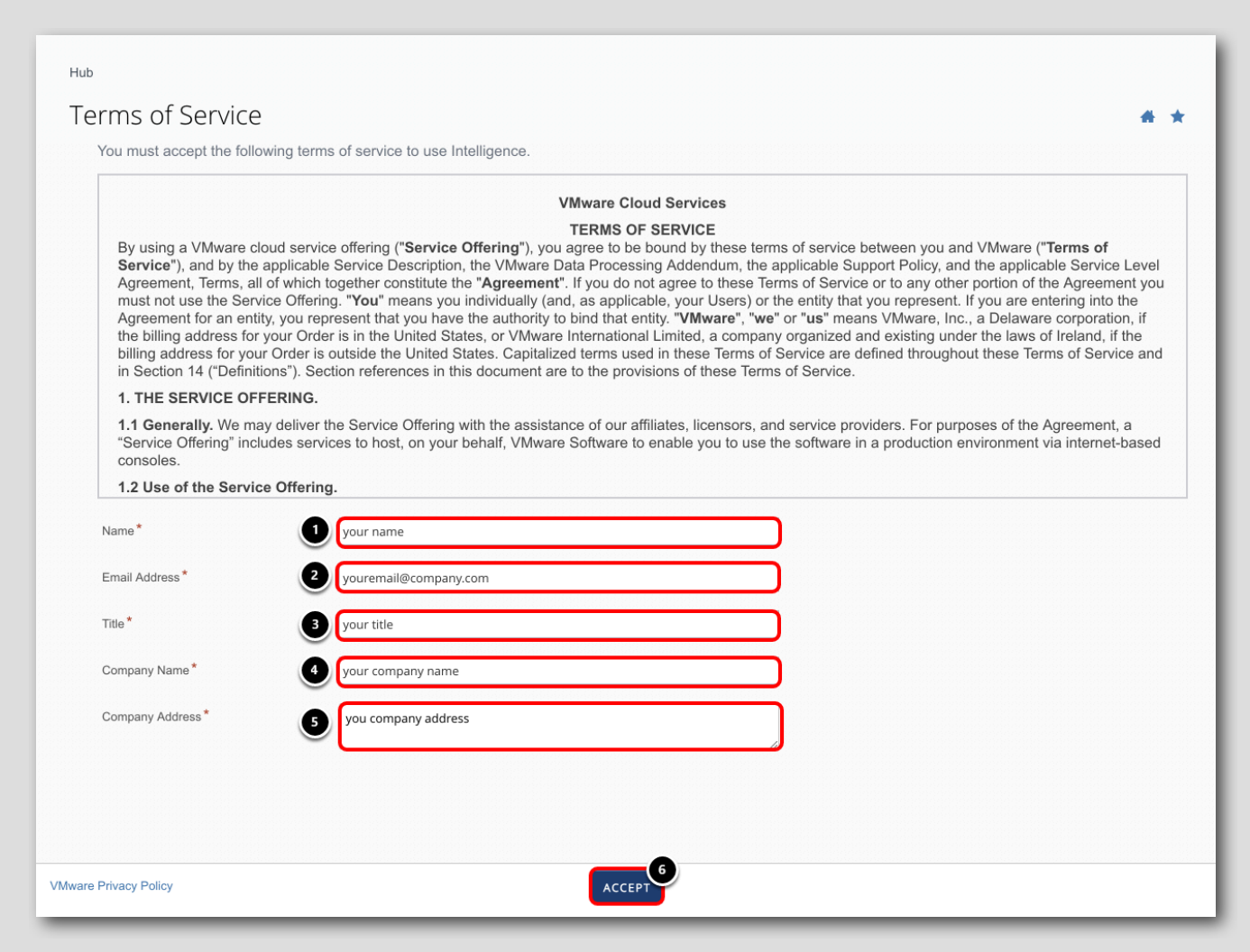
[580]



1. 下にスクロールして [Opt In] チェックボックスを確認します。
2. [Opt In] チェックボックスを有効にします。
3. [Next] をクリックします。

利用規約の完了

[581]



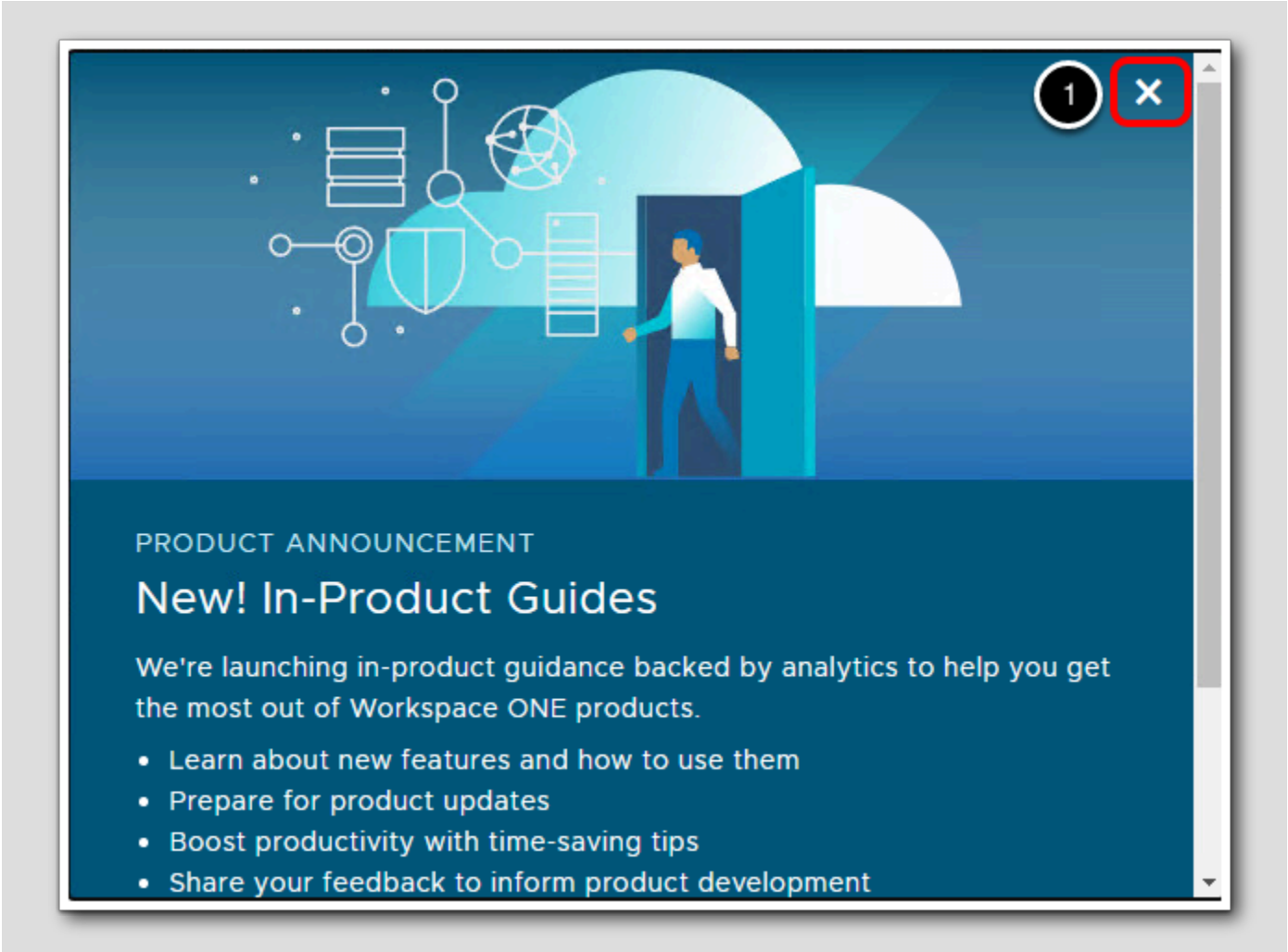
これはオプトイン プロセスの最後のステップであり、ここで情報を提供し、VMware Cloud Services 利用規約に同意します。

1. 名前を入力します。
2. メール アドレスを入力します。
3. 肩書を入力します。
4. 会社名を入力ます。
5. 会社の住所を入力します。
6. [Accept] をクリックします。

承諾すると、Workspace ONE Intelligence コンソールにリダイレクトされます。

製品発表を閉じる

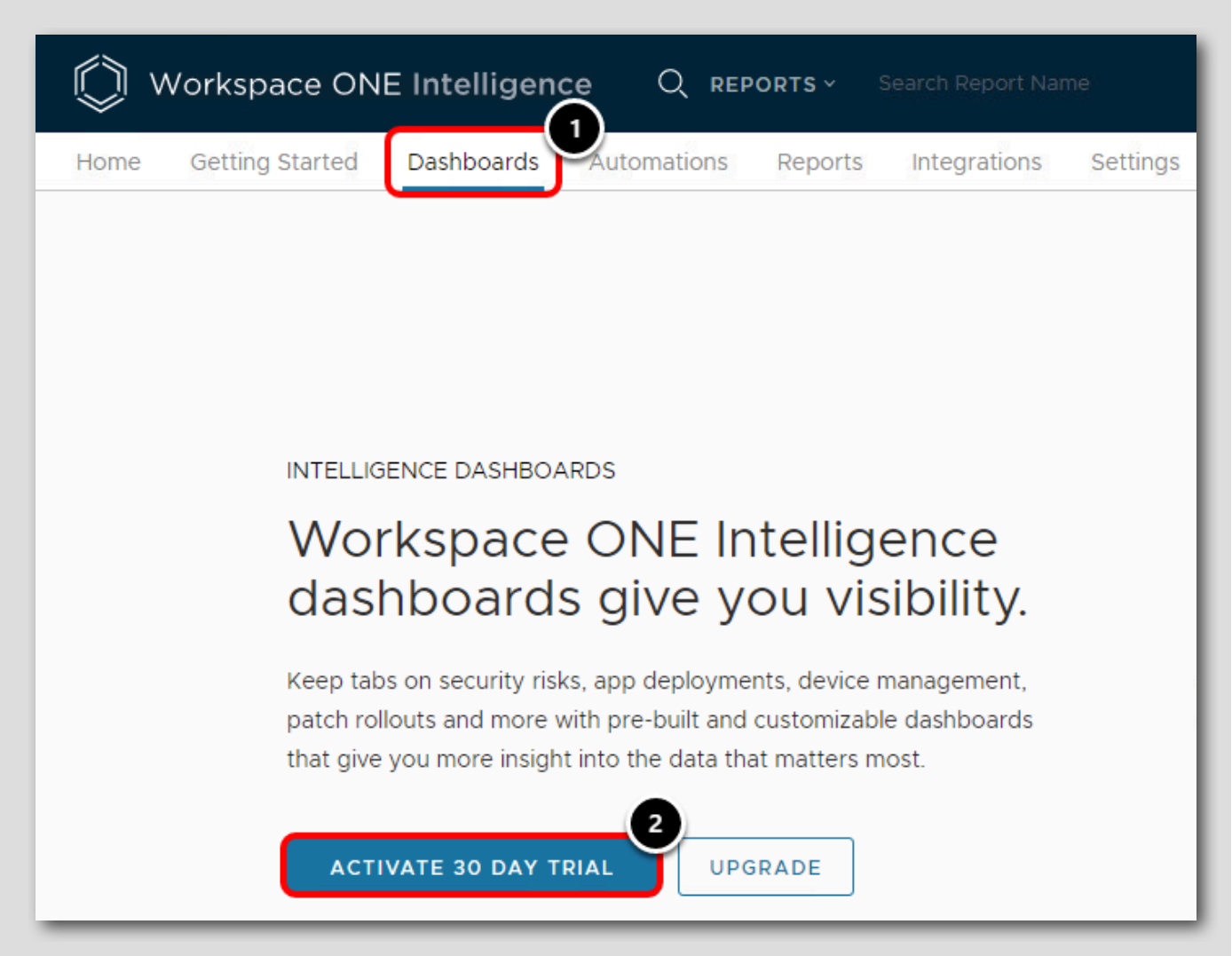
[582]



1. 1. 製品発表のポップアップ ウィンドウが表示される場合があります。 ウィンドウを閉じるには、右上の [X] をクリックします。

30 日間のトライアルのアクティブ化

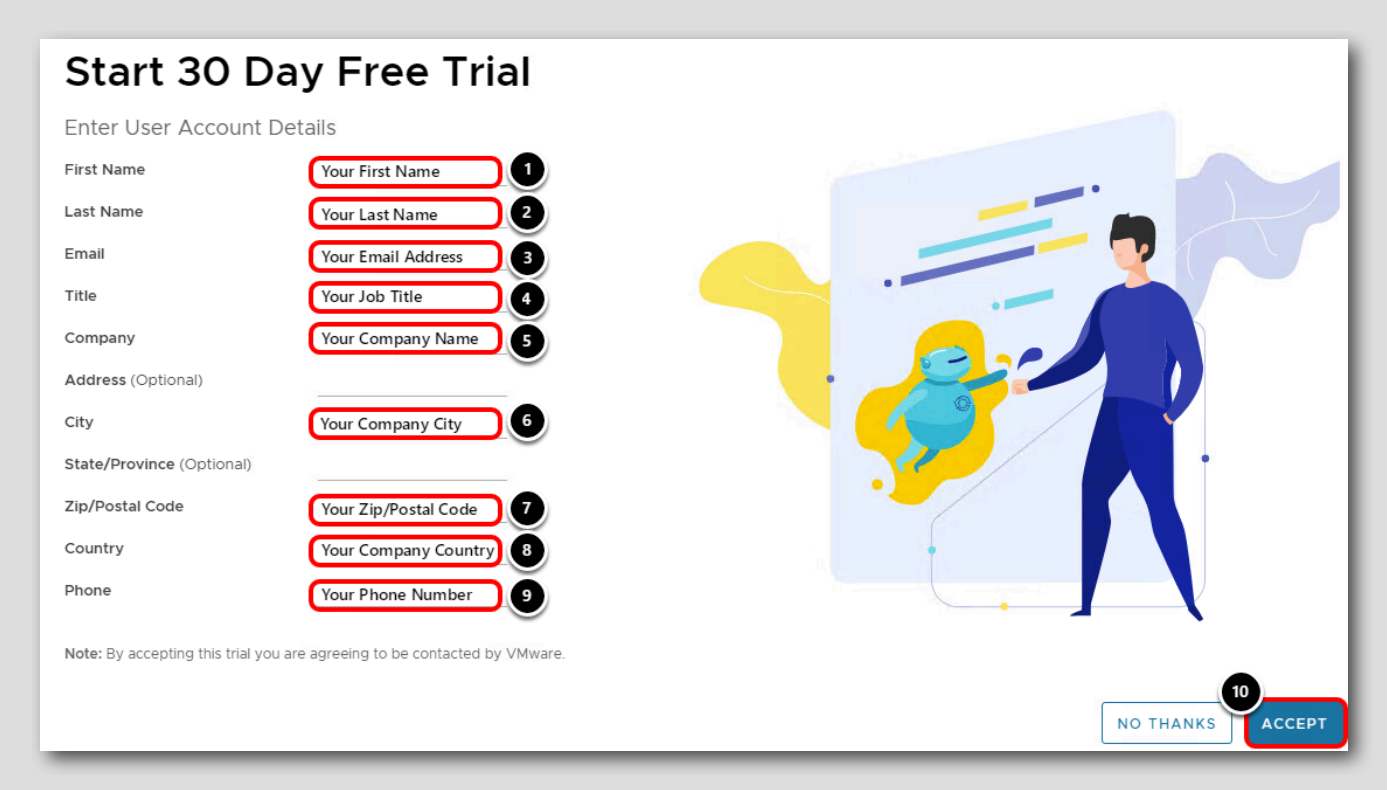
[583]



1. [Dashboards] をクリックします。
2. [Activate 30 Day Trial] をクリックします。

30 日間トライアルの詳細の入力

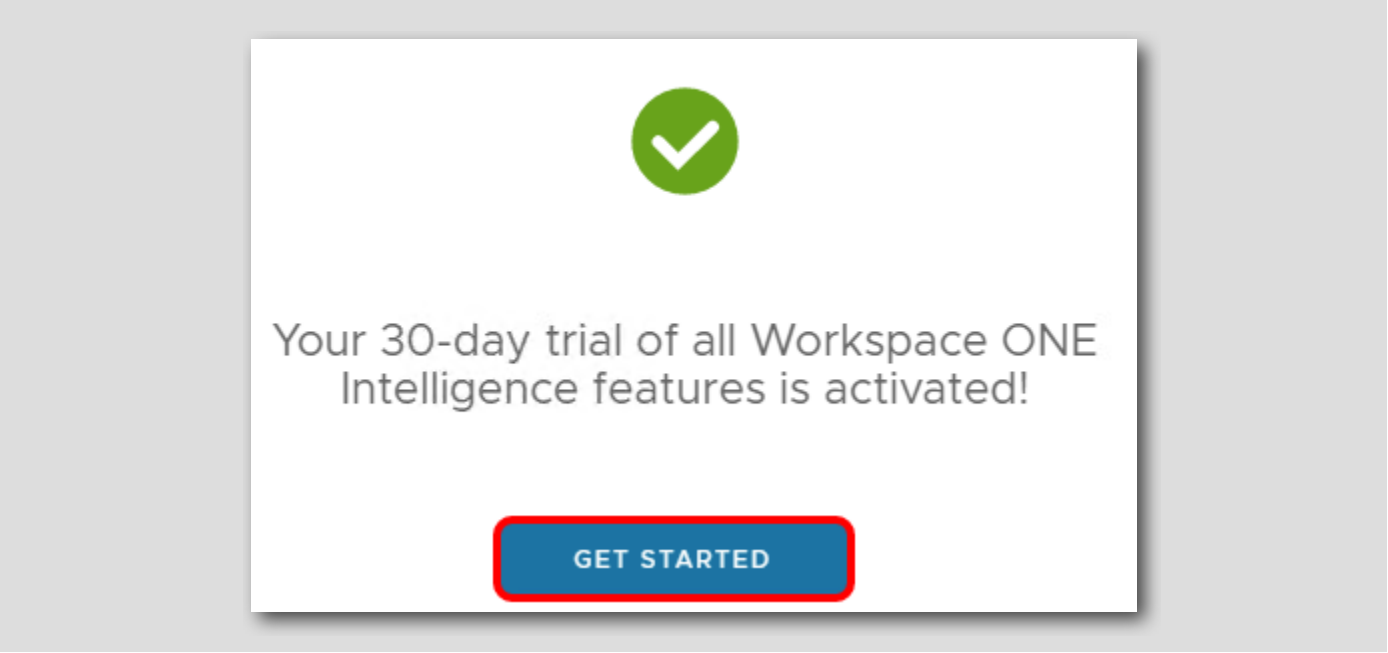
[584]



1. 名を入力します。
2. 姓を入力します。
3. メール アドレスを入力します。
4. 役職名を入力します。
5. 会社名を入力ます。
6. 会社の市区町村を入力します。
7. 郵便番号を入力します。
8. 会社の国を入力します。
9. 電話番号を入力します。
10. [Accept] をクリックします。

トライアルのアクティブ化の確認

[585]

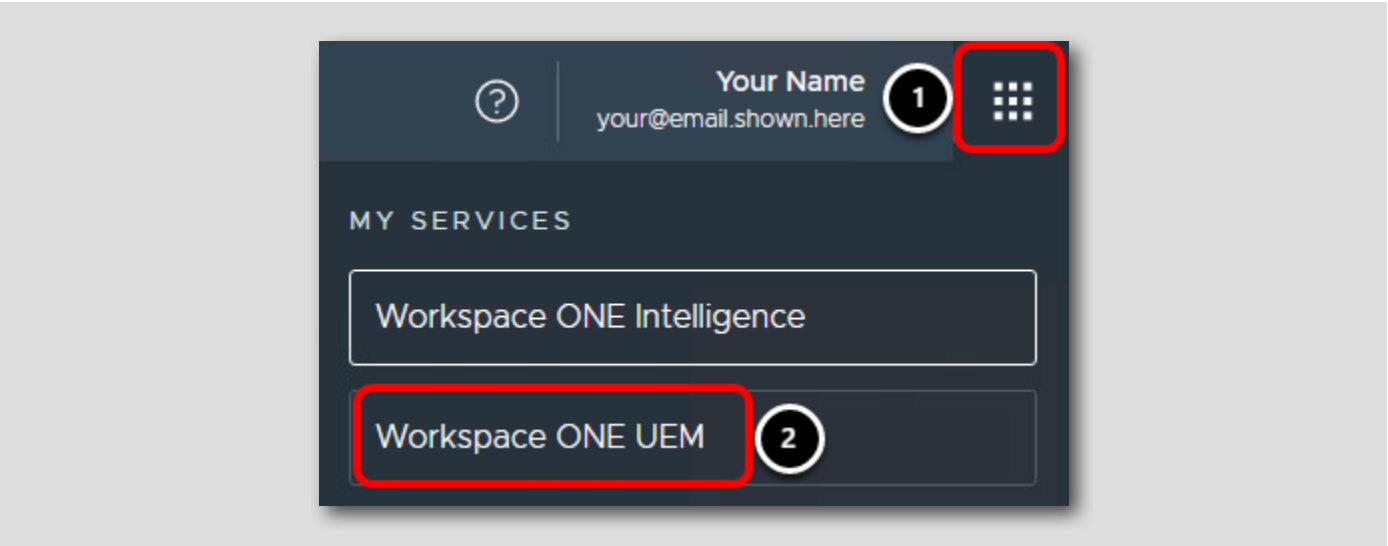


[Get Started] をクリックします。

Workspace ONE UEM Console に戻る

[586]

次に、提供された Windows 10 仮想マシンを Workspace ONE UEM に登録します。この Windows 10 仮想マシンをラボ全体で使用して、Workspace ONE UEM と Workspace ONE Intelligence の両方でデバイスを操作する方法を確認します。



1. [Services] ボタンをクリックします。
2. [Workspace ONE UEM] をクリックします。

個人の Windows 10 デバイスを登録しないこと

[587]

重要：今後の演習で、個人の Windows 10 デバイスを登録しないでください。個人デバイスが他の EMM プロバイダに加入している場合、望ましくない競合や問題が発生する可能性があります。

以降の手順に従って、このハンズオン ラボ用に提供されている Win10-01a 仮想マシンを登録して使用してください。

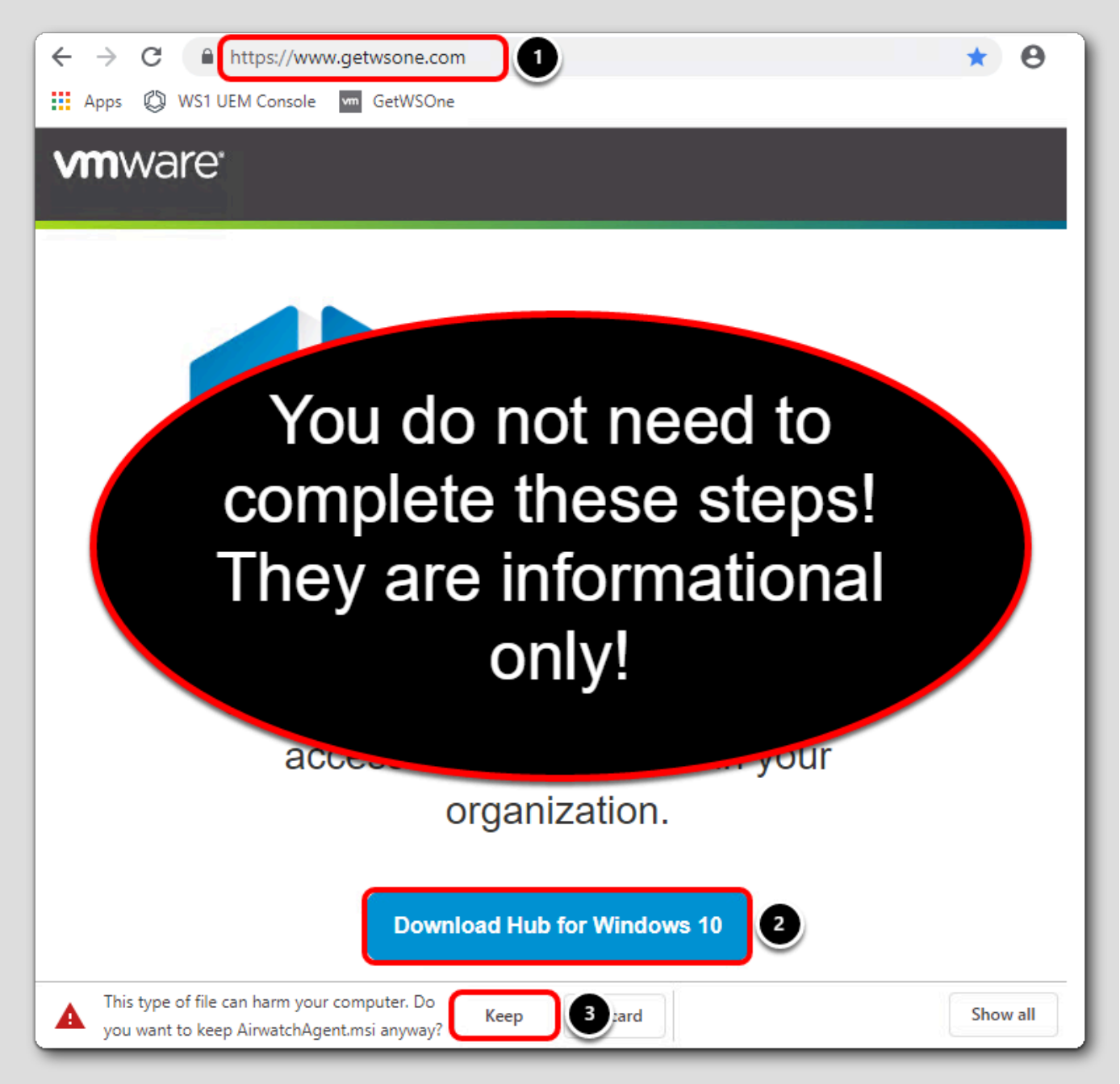
基本アカウントを使用した Windows 10 デバイスの登録

[588]

次に、Workspace ONE Intelligent Hub アプリケーションを使用して、Workspace ONE UEM に Windows 10 デバイスを登録します。

Workspace ONE Intelligent Hub アプリケーションのダウンロード

[589]



注：これらの手順を実行する必要はありません。Workspace ONE Intelligent Hub はすでにダウンロードされています。この手順は単なる情報です。

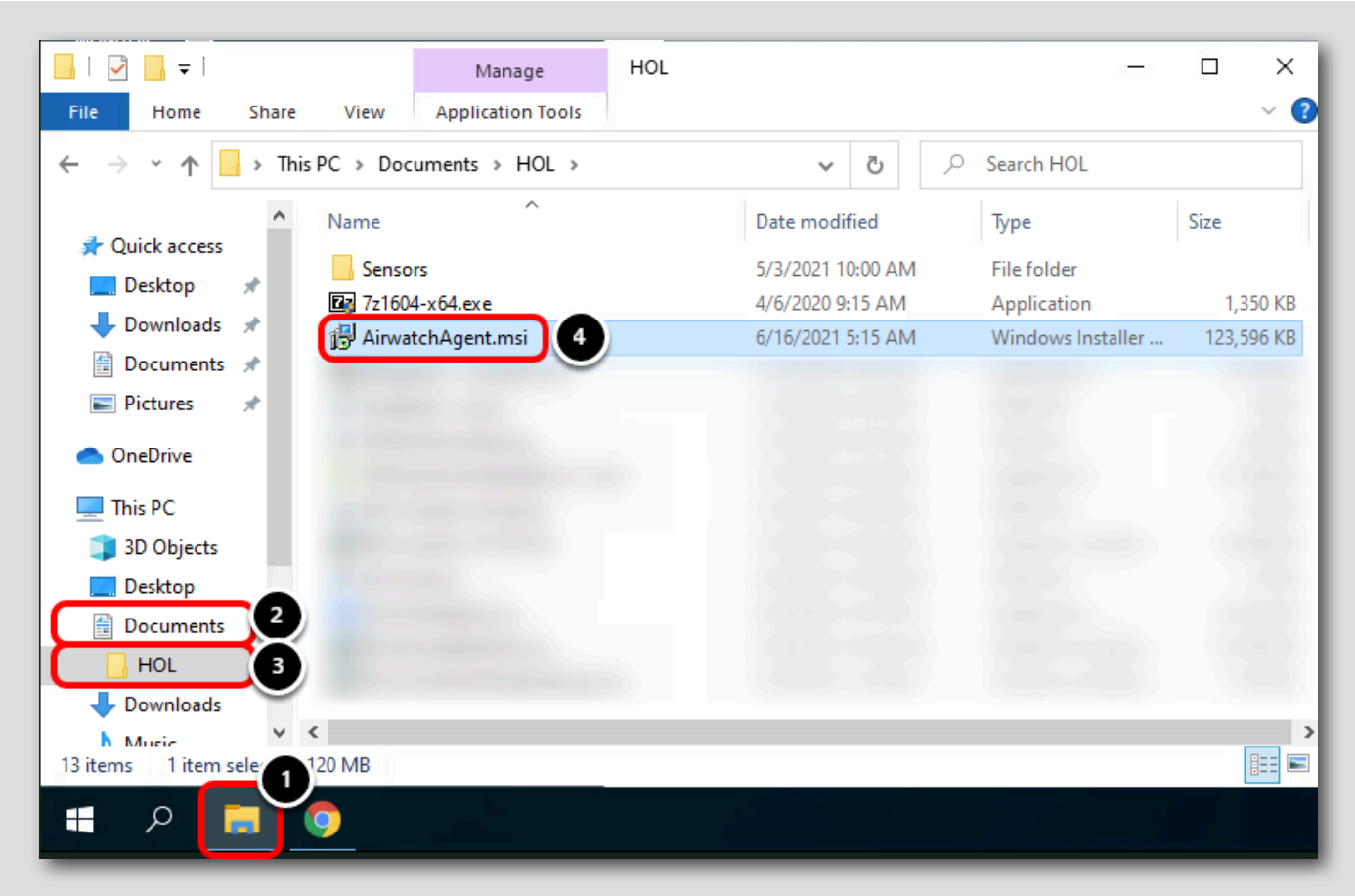
次の手順に従って、現在のプラットフォーム用の最新の Workspace ONE Intelligent Hub アプリケーションをダウンロードできます。

1. ブラウザで **`https://www.getwsone.com`** に移動します。
2. [Download Hub for Windows 10] をクリックします。
3. AirWatchAgent.msi のダウンロードについて警告が表示されたら、[Keep] をクリックします。

便宜上、Workspace ONE Intelligent Hub アプリケーションはすでにダウンロードされています。次の手順に進んで、インストーラを起動します。

Workspace ONE Intelligent Hub インストーラの起動

[590]

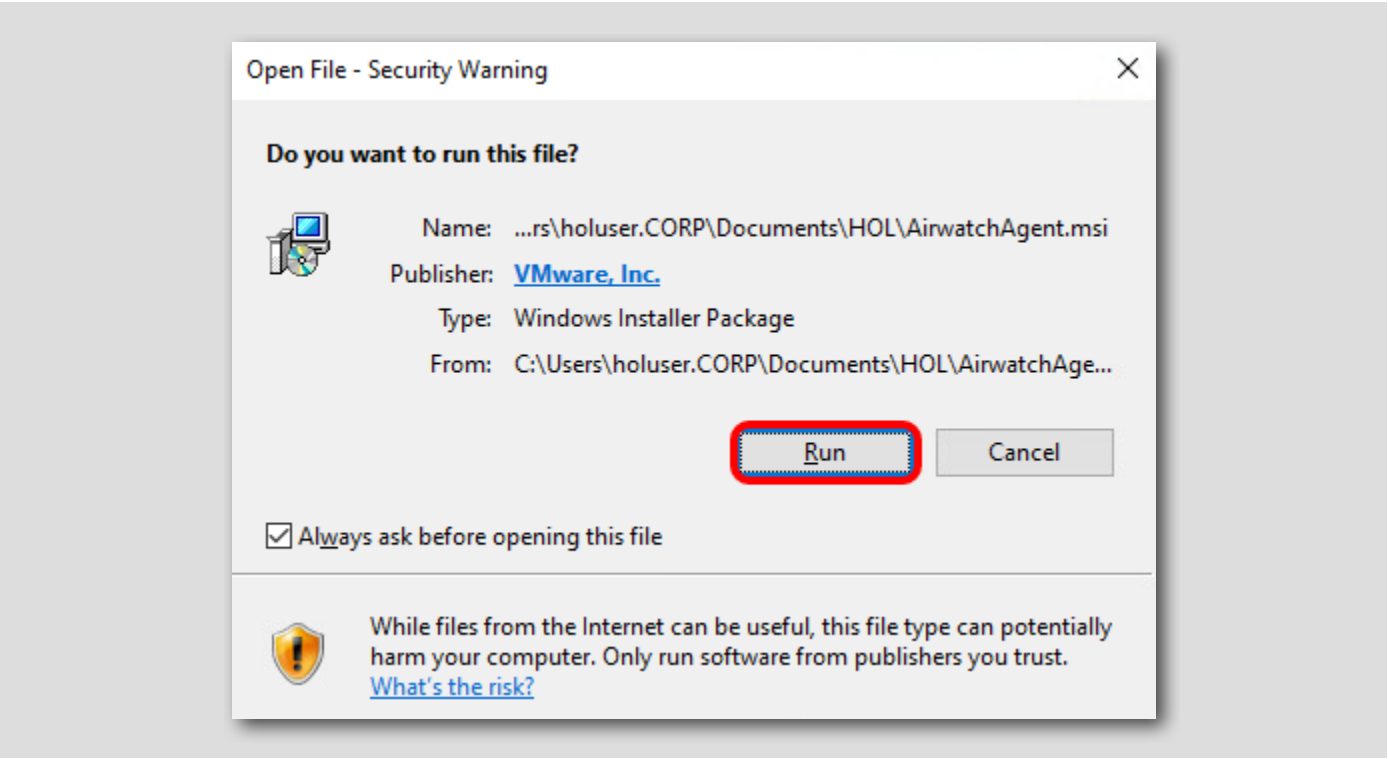


1. タスクバーの [File Explorer] アイコンをクリックします。
2. [Documents] をクリックします。
3. [HOL] をクリックします。
4. AirwatchAgent.msi ファイルをダブルクリックして、インストーラを起動します。

注：インストーラが起動するまでに数秒かかる場合があります。AirwatchAgent.msi ファイルをクリックして、しばらくお待ちください。

[Run] のクリック

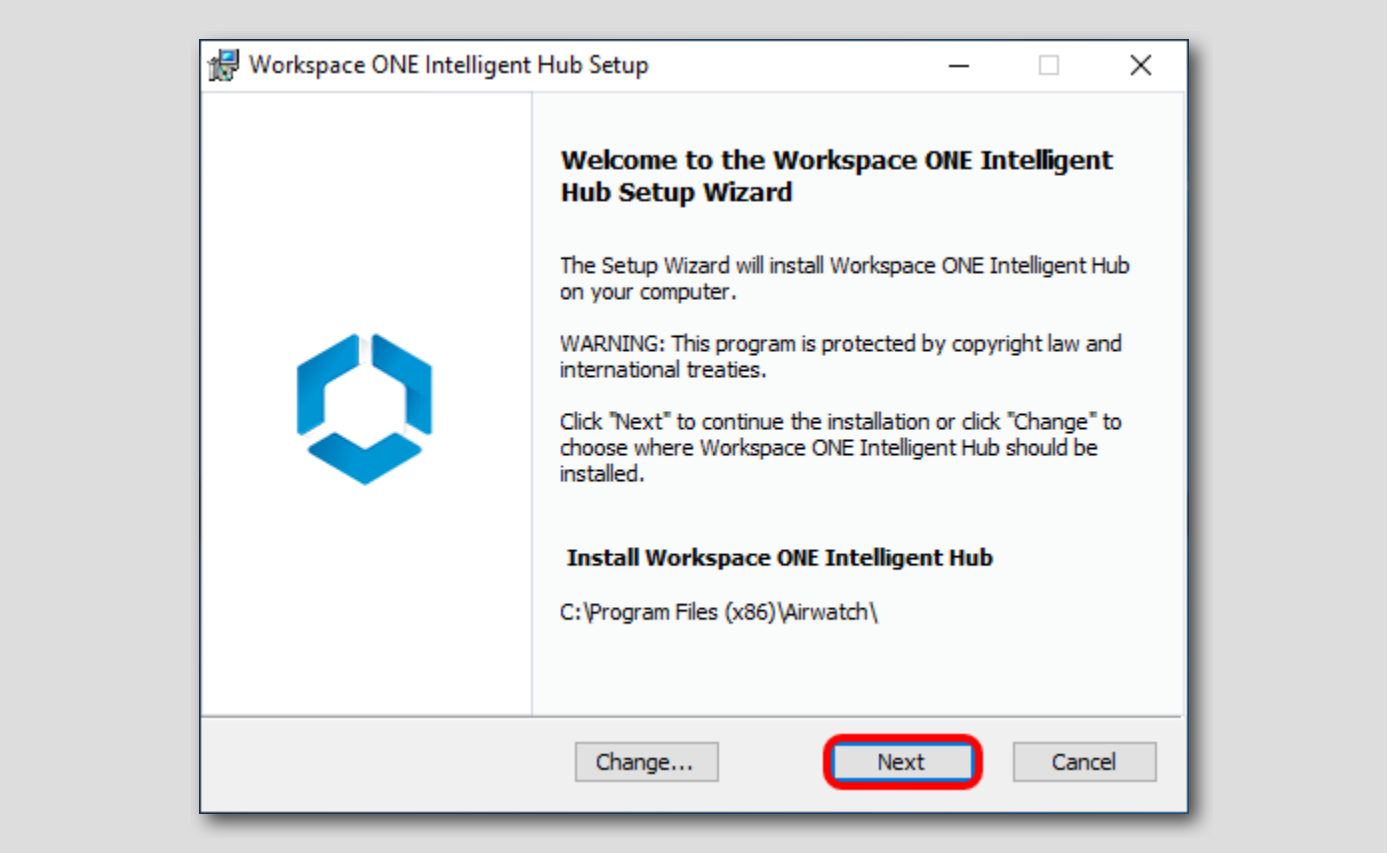
[591]



[Run] をクリックして、インストールを続行します。

デフォルトのインストール場所の受け入れ

[592]

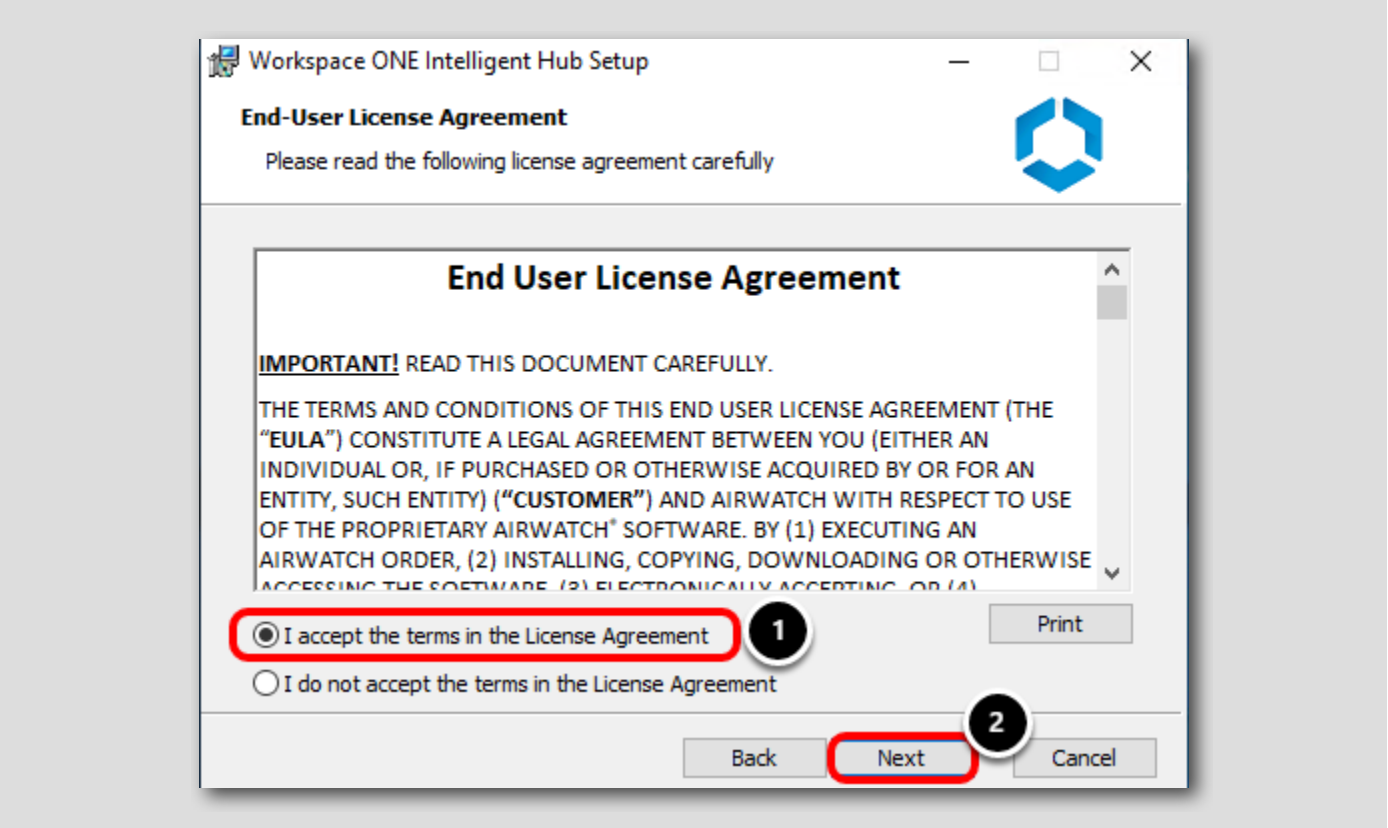


インストール場所はデフォルトのまま、[Next] をクリックします。

注：必要な追加機能がインストールされ、[Next] ボタンが有効になるまで数秒かかる場合があります。

使用許諾契約書への同意

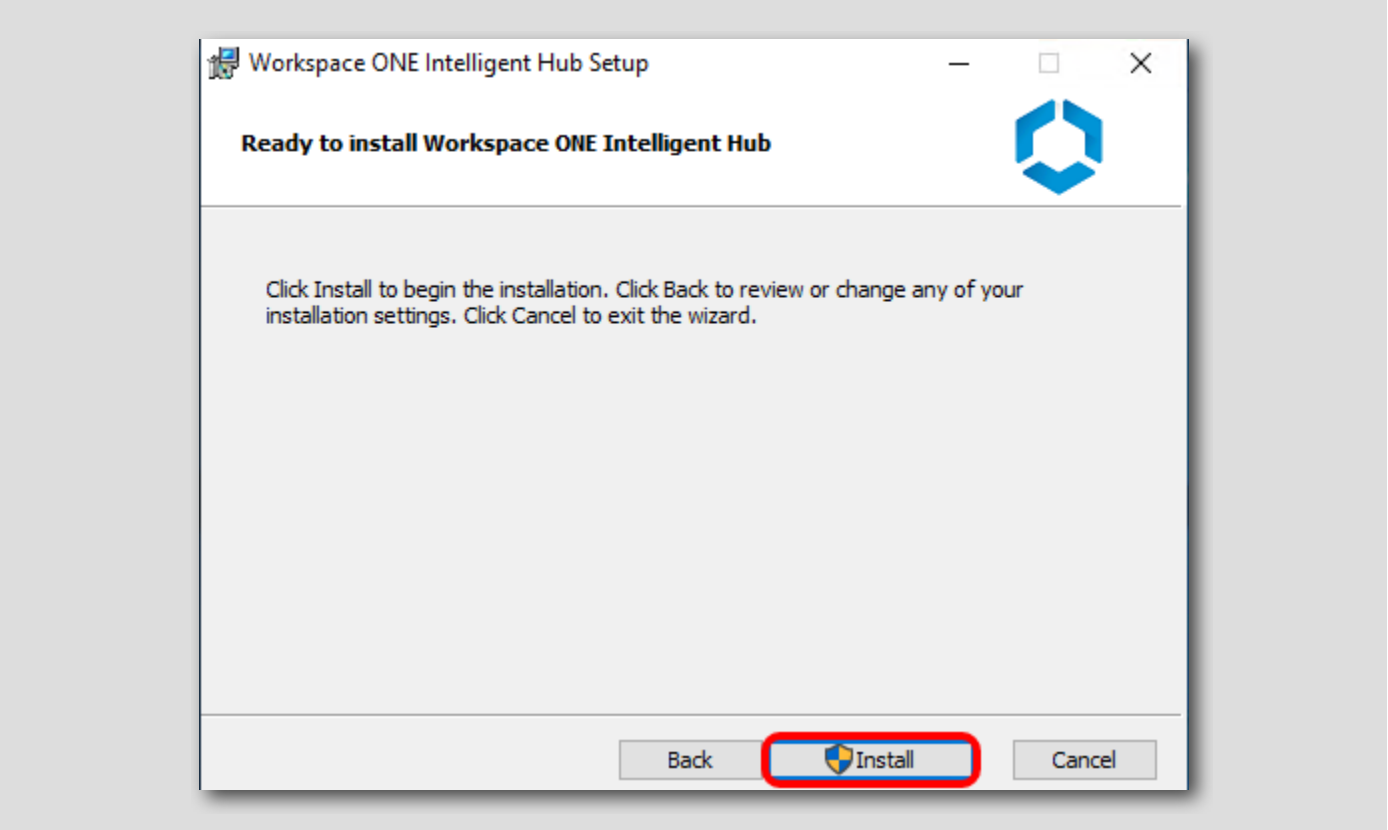
[593]



1. [I accept the terms of the License Agreement] を選択します。
2. [Next] をクリックします。

Workspace ONE Intelligent Hub のインストールの開始

[594]

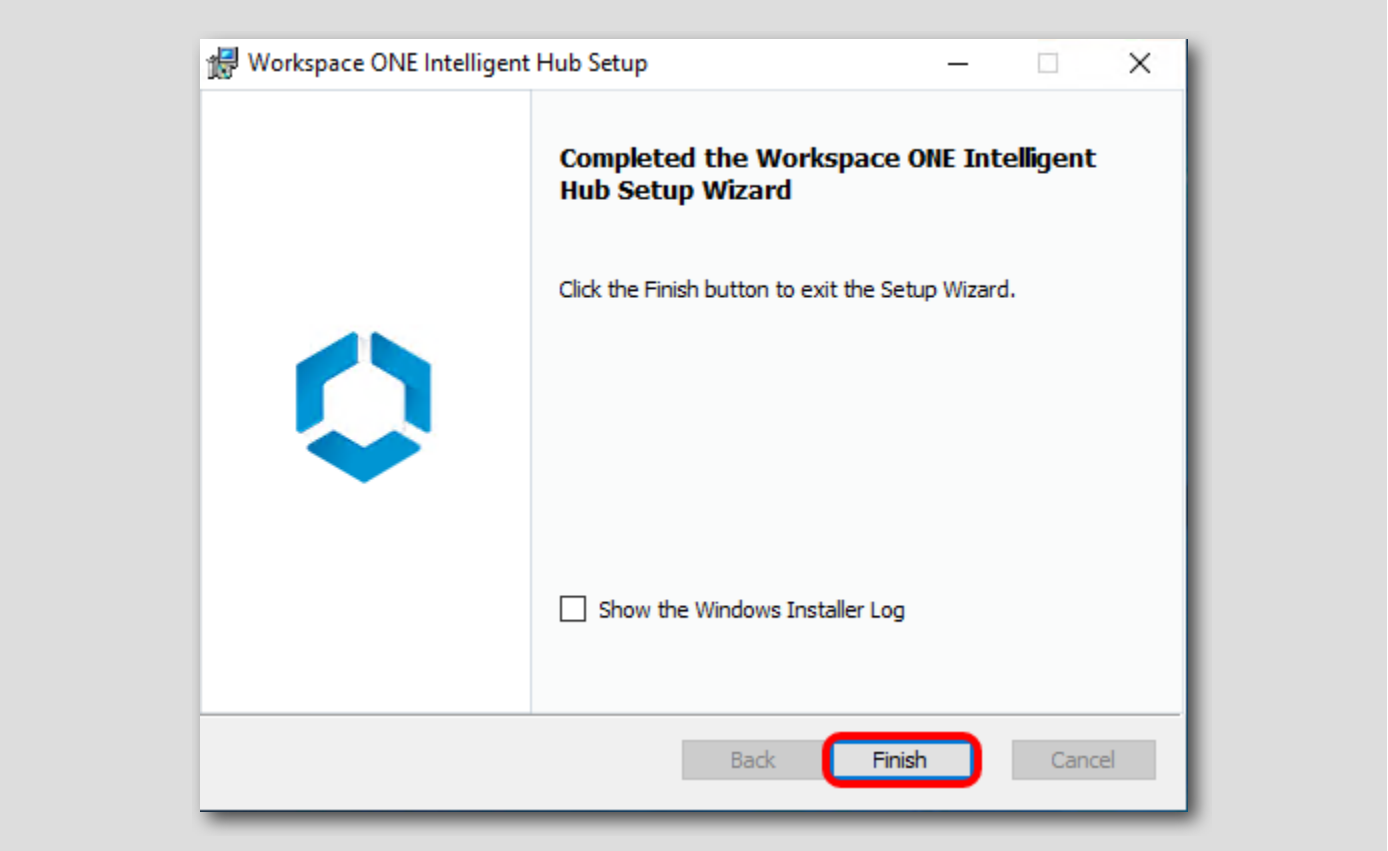


[Install] をクリックして、インストーラを開始します。

注：VMware Workspace ONE Intelligent Hub のインストールは完了までに数分かかる場合があります。インストーラを中断しないようにしてください。

Workspace ONE Intelligent Hub インストーラの完了

[595]



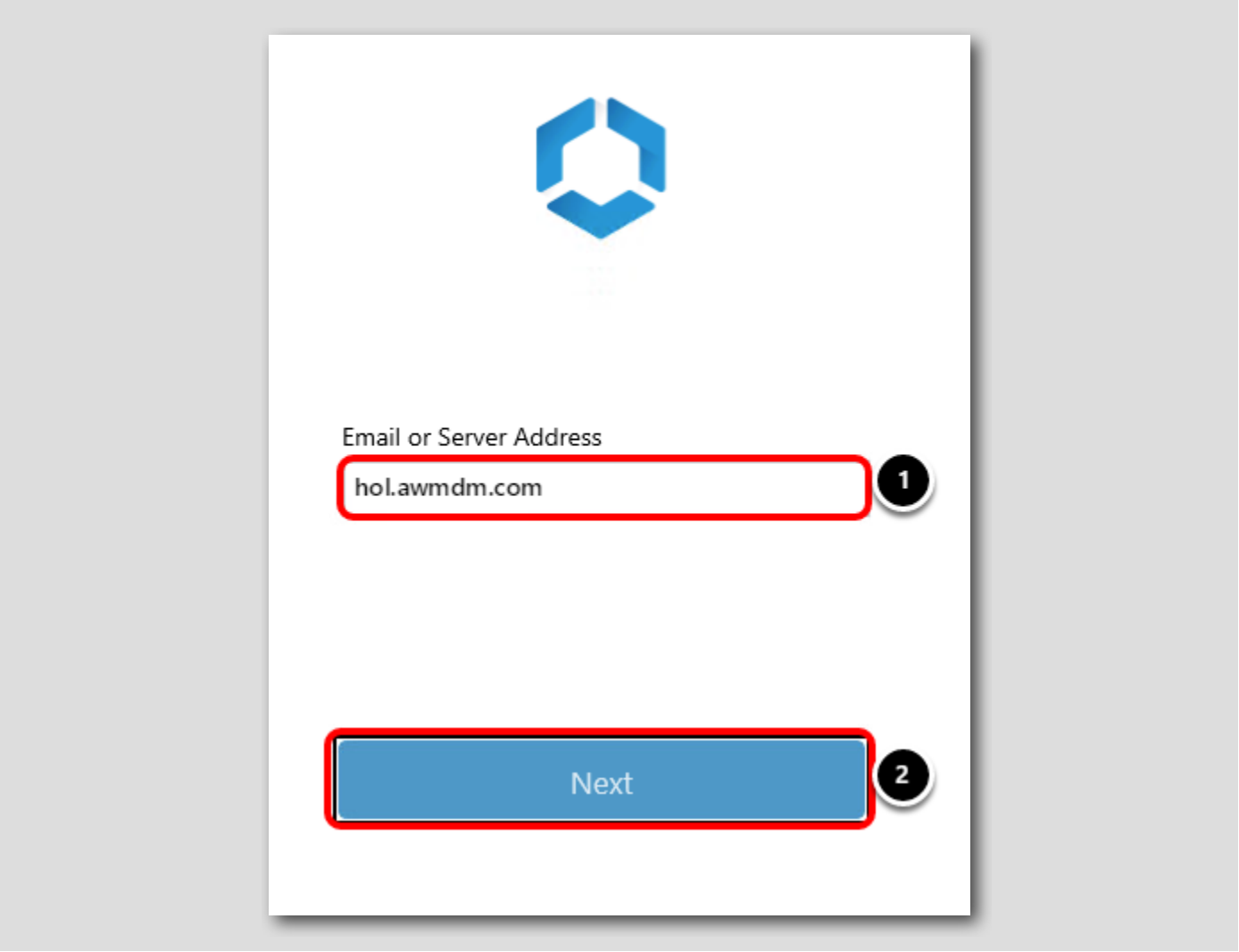
注：インストーラの完了には数分かかる場合があります。続行する前に、インストールの完了画面が表示されるまでお待ちください。

[Finish] をクリックして、Workspace ONE Intelligent Hub インストーラを完了します。

注：[Finish] をクリックすると Native Enrollment アプリケーションが起動し、Workspace ONE UEM への登録手順が表示されます。Intelligent Hub の起動には、約 2 ～ 3 分かかります。

Workspace ONE Intelligent Hub を使用した Windows 10 デバイスの登録

[596]

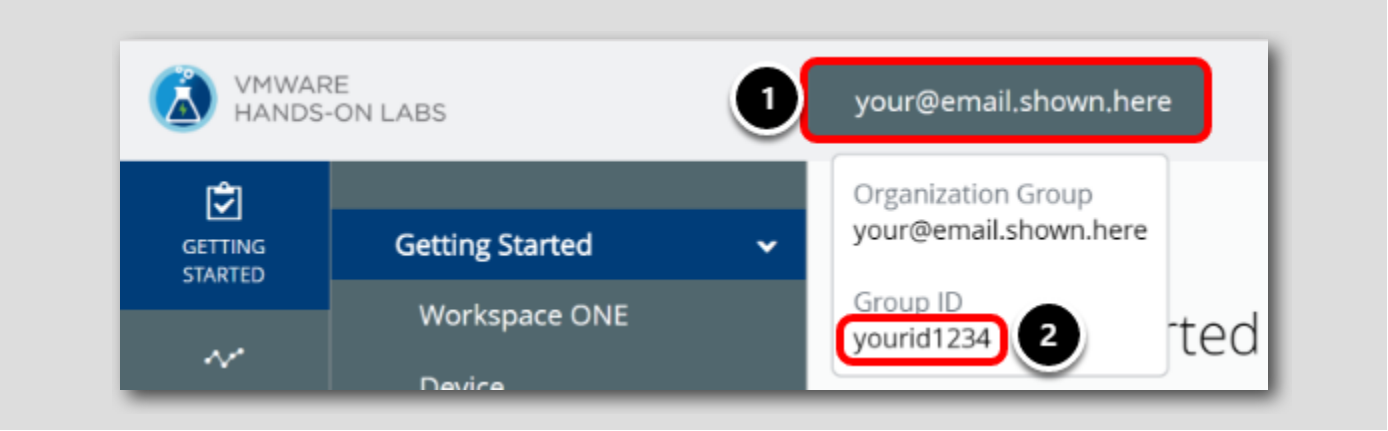


注：前の手順で [Finish] をクリックした後、上記の画面が表示されるまでに 2 ～ 3 分かかることがあります。

1. [Server Address] に **`hol.awmdm.com`** と入力します。
2. [Next] をクリックします。

Workspace ONE UEM Console からのグループ ID の特定

[597]

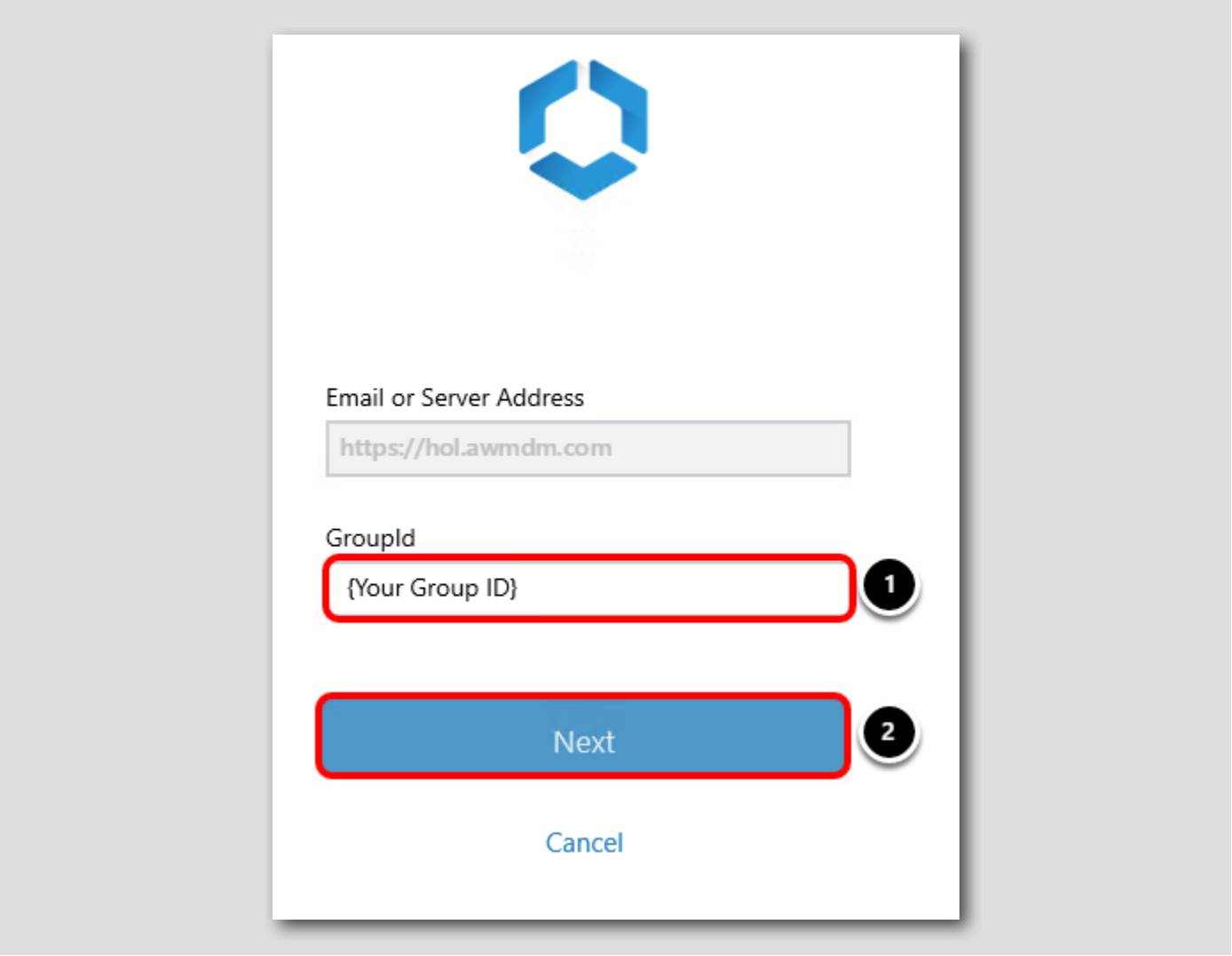


次の手順では、[Organization Group ID] を取得します。

1. グループ ID を確認するには、Workspace ONE UEM 管理コンソールに戻って、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. グループ ID は [Organization Group] ポップアップの最下部に表示されます。この値をコピーします。

グループ ID の入力

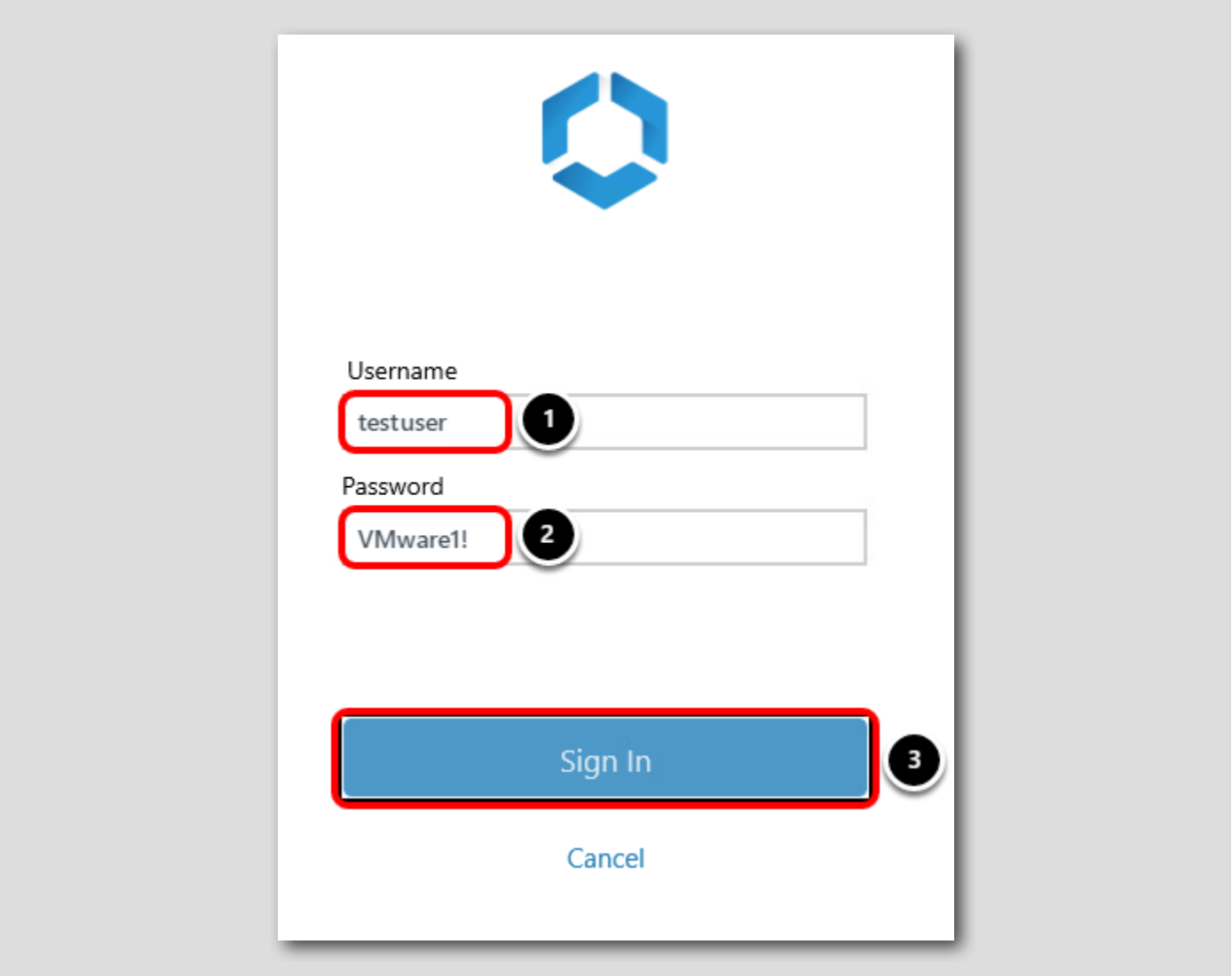
[598]



1. [Group ID] フィールドにグループ ID を入力します。グループ ID を忘れた場合は、前の手順で取得方法を確認してください。
2. [Next] をクリックします。

ユーザー認証情報の入力

[599]

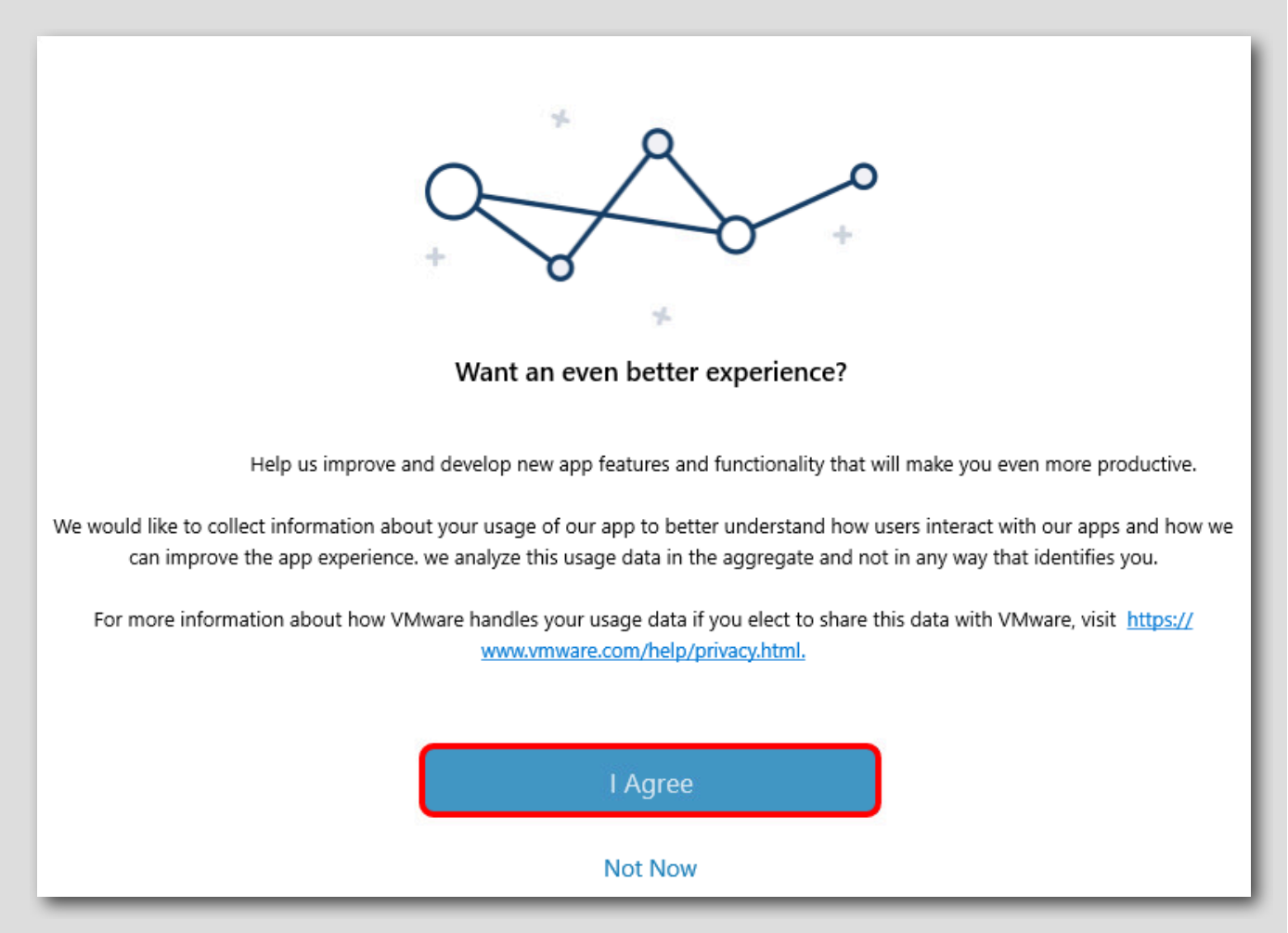


1. [Username] フィールドに **testuser** と入力します。
2. [Password] フィールドに **VMware1!** と入力します。
3. [Sign In] をクリックします。

注：サーバが登録の詳細を確認するまでしばらくお待ちください。これには数分かかる場合があります。

データ ポリシーの承諾

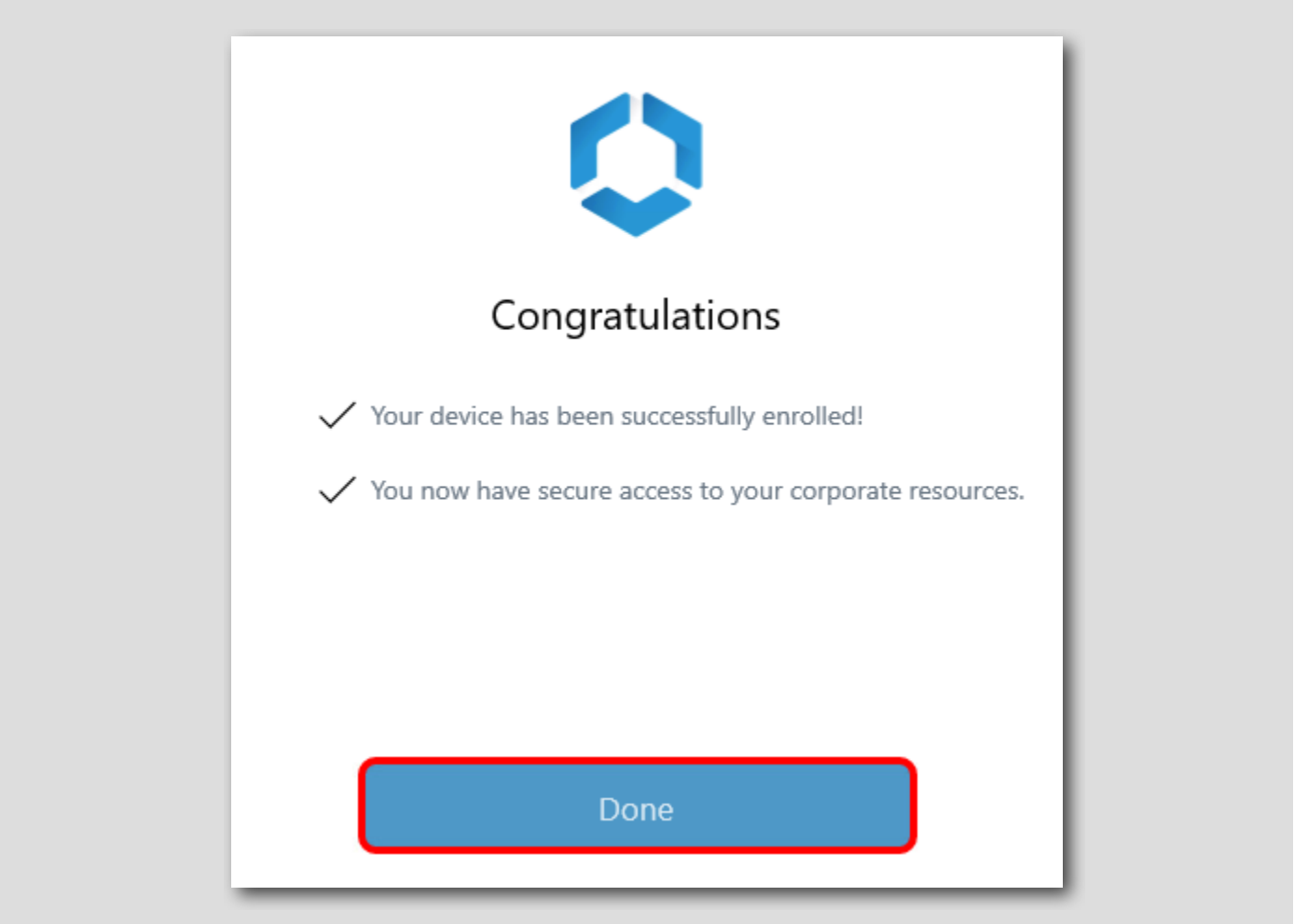
[600]



[I Agree] をクリックします。

Workspace ONE UEM 登録プロセスの終了

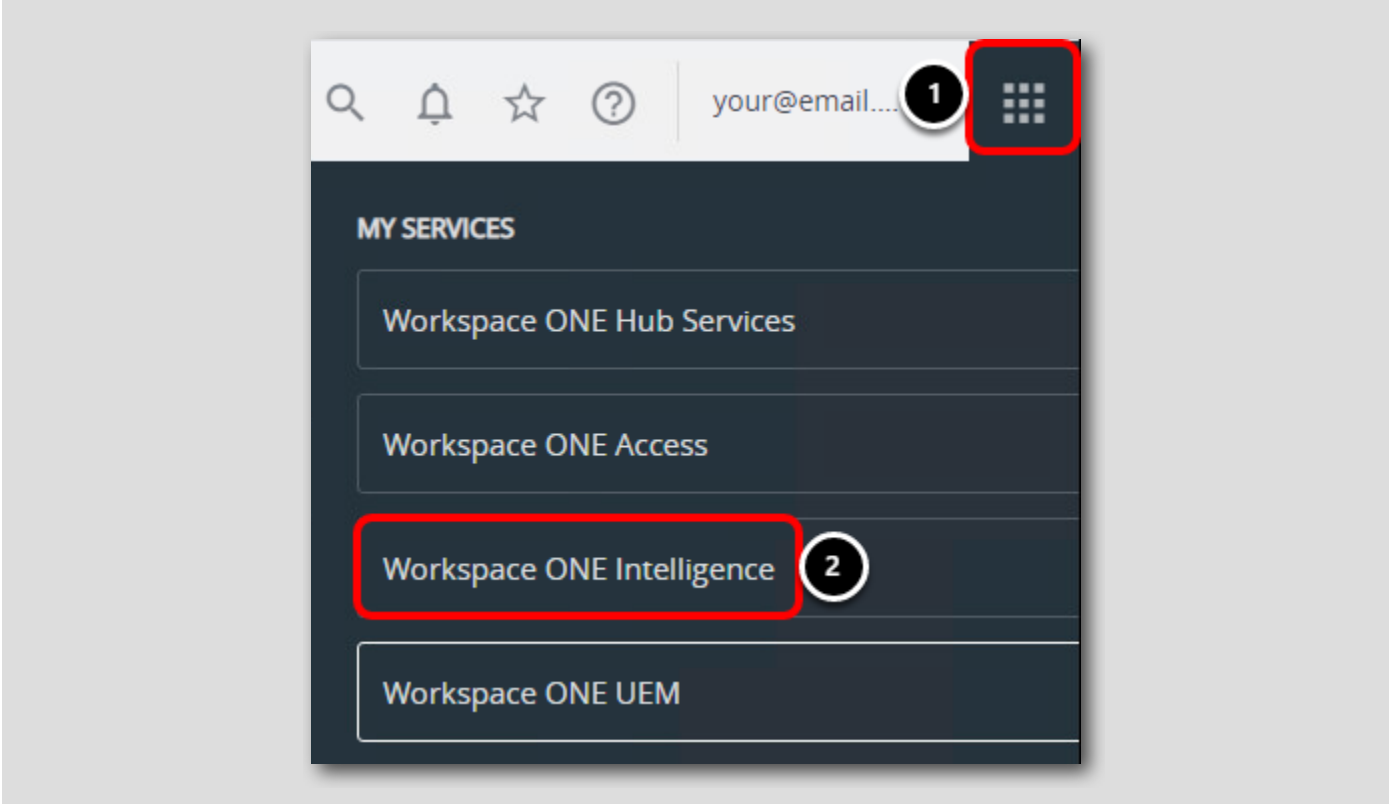
[601]



[Done] をクリックして登録プロセスを終了します。これで、Windows 10 デバイスは Workspace ONE UEM に正常に登録されました。

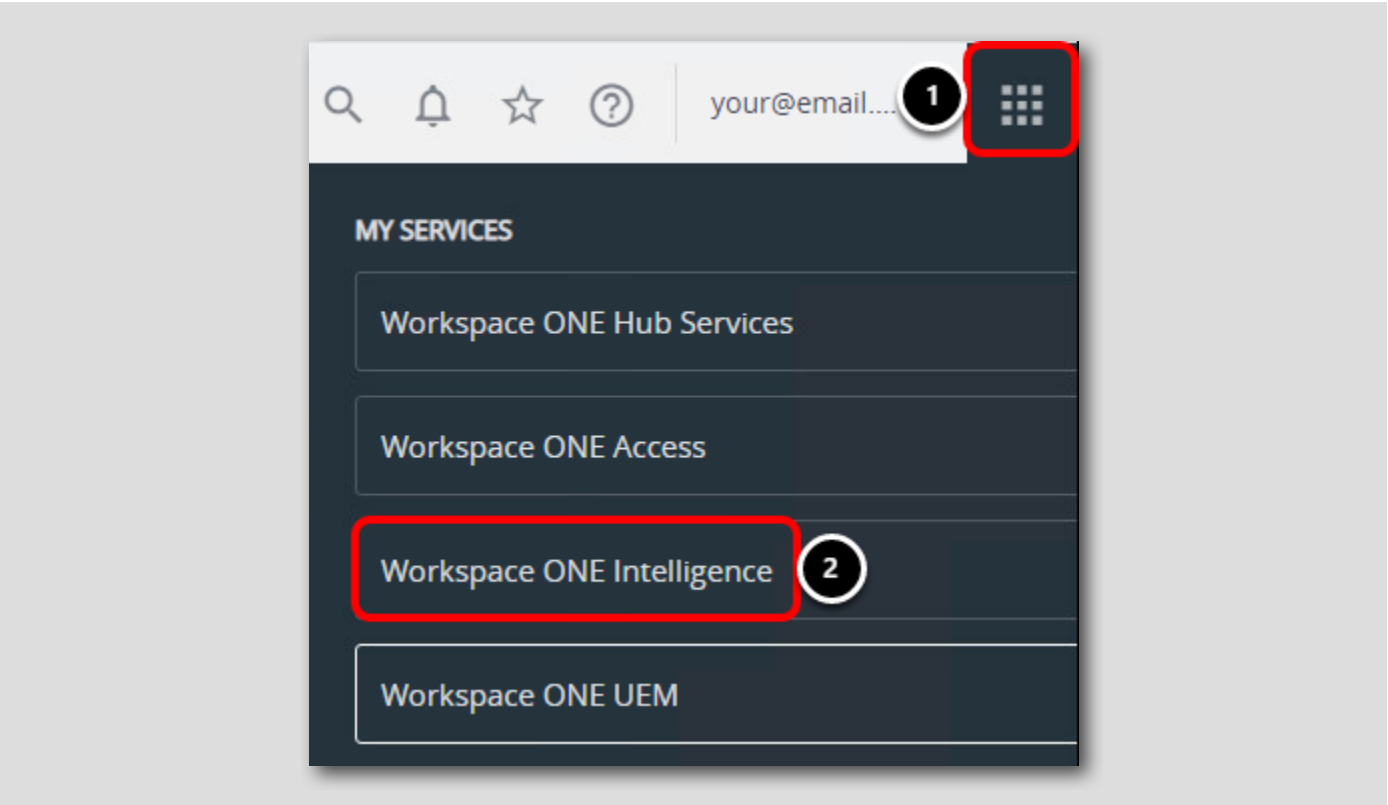
Workspace ONE Intelligence コンソールに戻る

[602]



ブラウザで Workspace ONE UEM 管理コンソールに戻ります。

1. 右上の [My Services] ボタンをクリックします。
2. Workspace ONE Intelligence をクリックします。



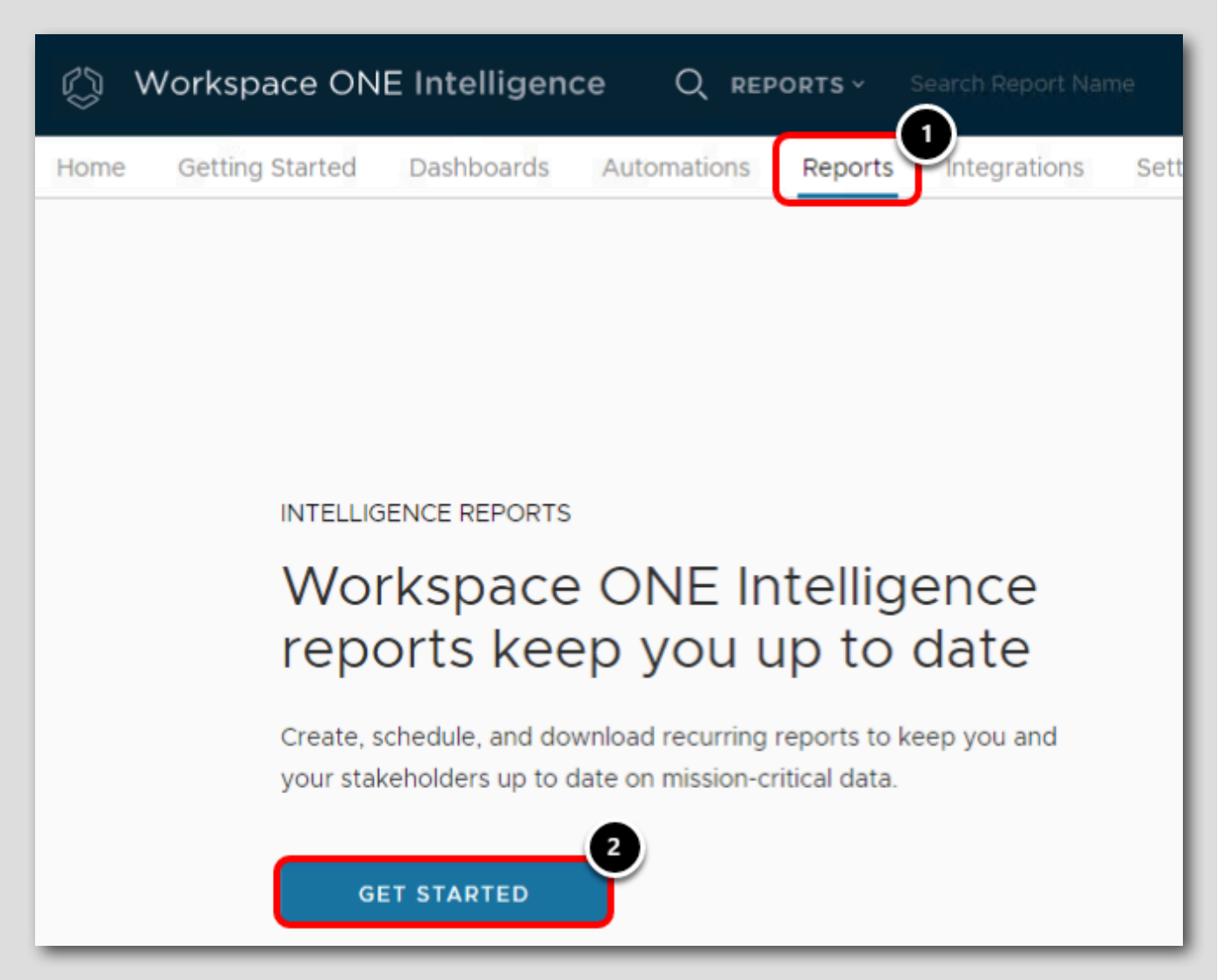
レポートの作成

[603]

このアクティビティでは、登録済みデバイスのレポートを作成して、レポート機能を確認します。

レポート設定を開く

[604]

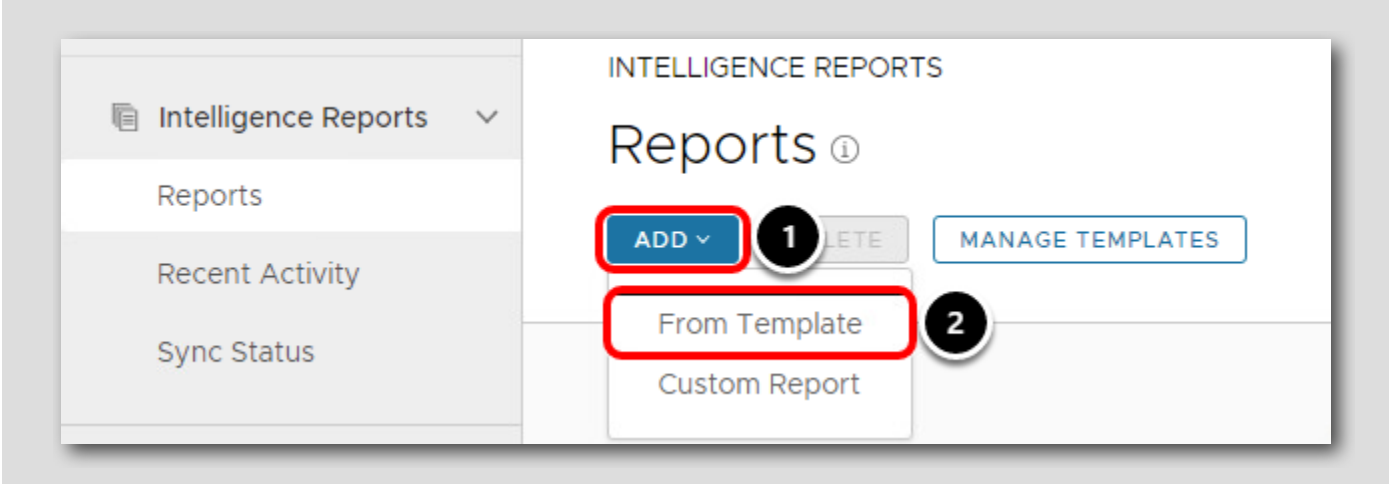


Workspace ONE Intelligence コンソールで、次のように操作します。

1. **[Reports]** をクリックします。
2. [Reports] セクションに初めてアクセスする場合は、[Get Started] ページが表示されます。その場合は、**[Get Started]** をクリックします。

レポートの追加

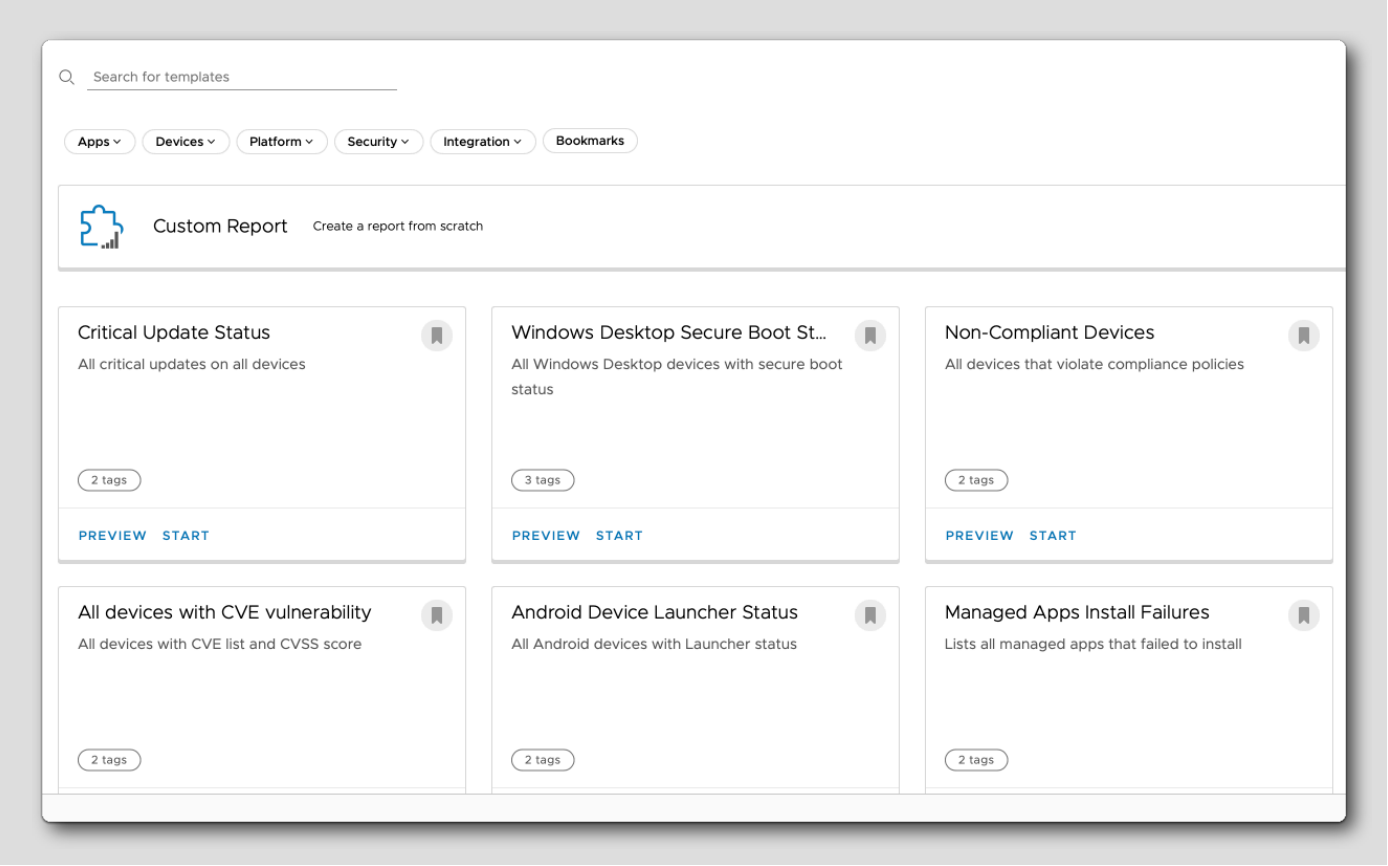
[605]



1. [Add] をクリックします。
2. [From Template] をクリックします。

レポート カテゴリとテンプレートの確認

[606]



レポートの作成を開始するには、取得するデータのカテゴリを選択します。使用可能なカテゴリは次のとおりです。

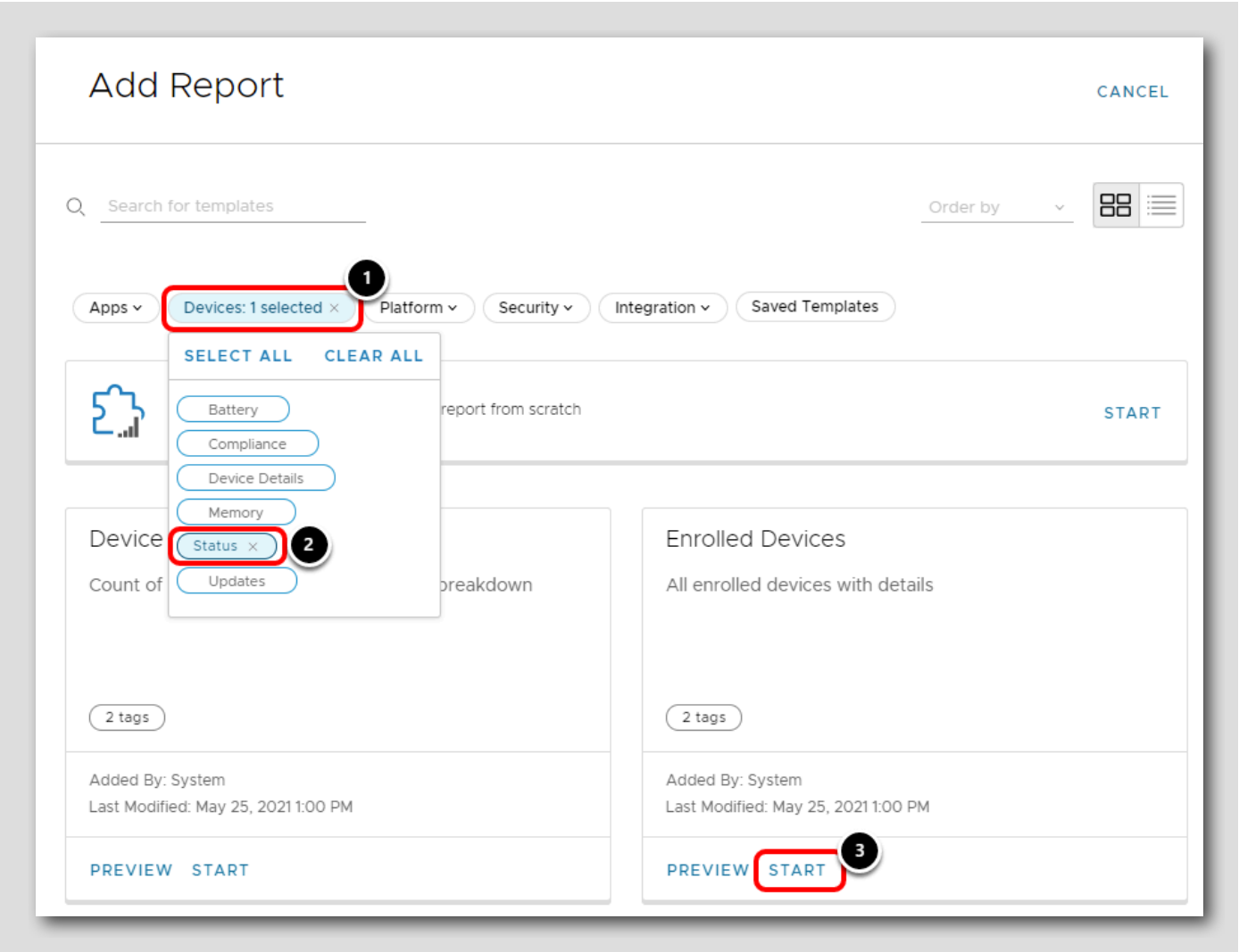
- Apps
- Devices
- Platform
- セキュリティ
- Integration

次に、各カテゴリのタグを使用して、カテゴリのカスタマイズ可能なテンプレートをフィルタリングし、レポートが収集するコンテンツを定義します。レポートのコンテンツを完全に制御するには、Custom Report テンプレートを使用して独自の条件を定義します。

各カテゴリをクリックすると、対応するテンプレートを表示できます。

Enrolled Devices テンプレートの選択

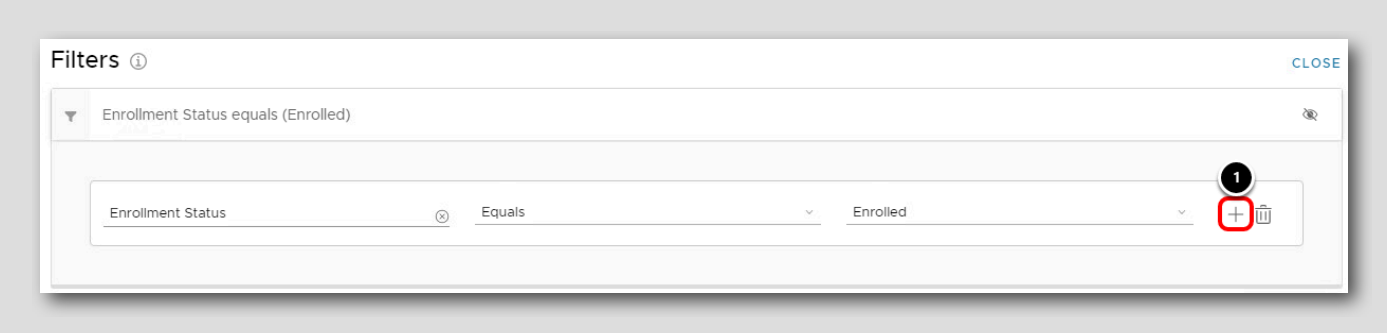
[607]

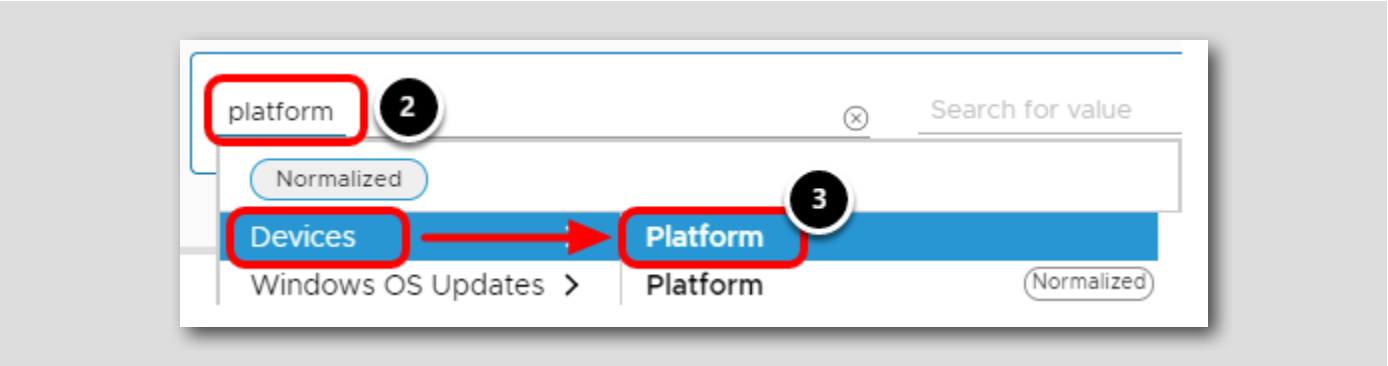


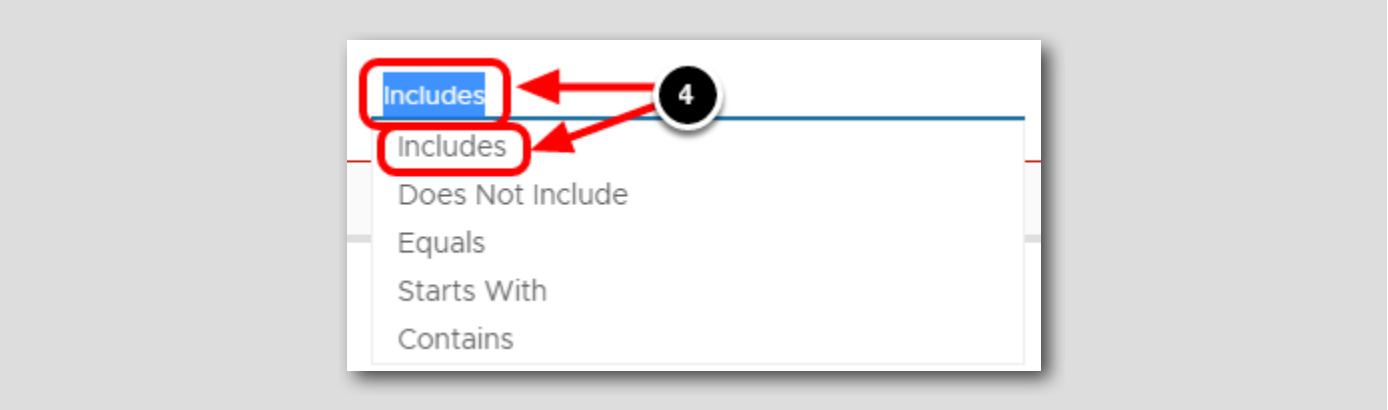
1. [Devices] カテゴリを選択します。
2. [Status] タグを選択して、関連するテンプレートをフィルタリングします。
3. Enrolled Devices テンプレートに対して [Start] をクリックします。このテンプレートを選択すると、事前定義された列にデータを表示する登録済みデバイスに関するレポートが作成されます。

レポート フィルタの追加

[608]







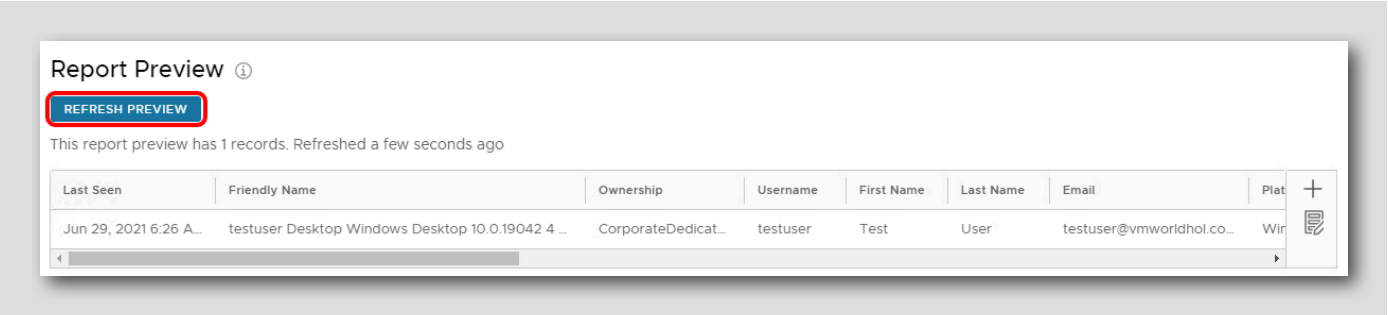
1. フィルタで、[+] アイコンをクリックして新しいフィルタを追加します。
2. 最初の検索フィールドに **platform** と入力します。
3. 表示されるドロップダウン メニューから [Devices] の [Platform] を選択します。
4. [Search for value] ドロップダウン メニューから [Includes] を選択します。
5. 最後のドロップダウン メニューから [Apple]、[Android] および [WinRT] を選択します。

   注：ドロップダウン メニューに上記のオプションが表示されない場合は、組織内にそのタイプの登録済みデバイスがないことを意味します。各プラットフォーム名を手動で入力し、それぞれの後に **ENTER** キーを押してリストに追加できます。

注：プラットフォーム リストは環境内で使用可能なデバイスに基づいているため、このアクティビティには 3 つのすべてのプラットフォームが表示されない場合があります。

レポートのプレビュー

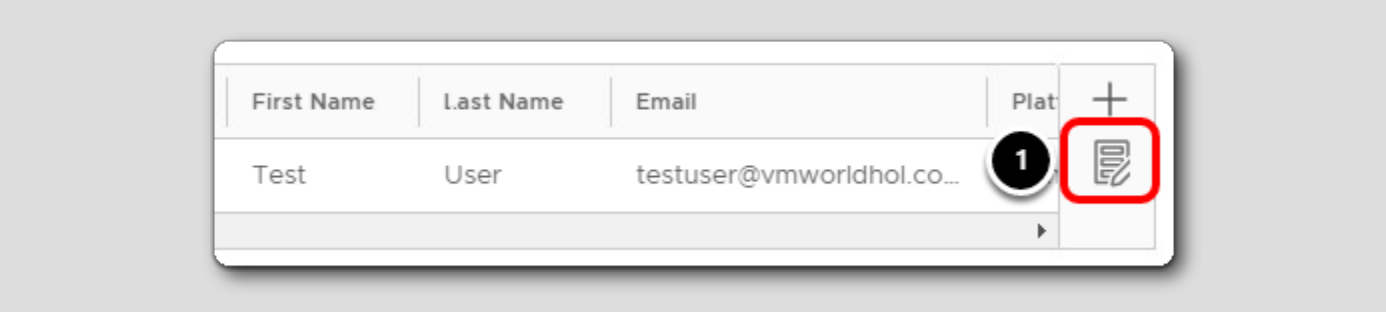
[609]

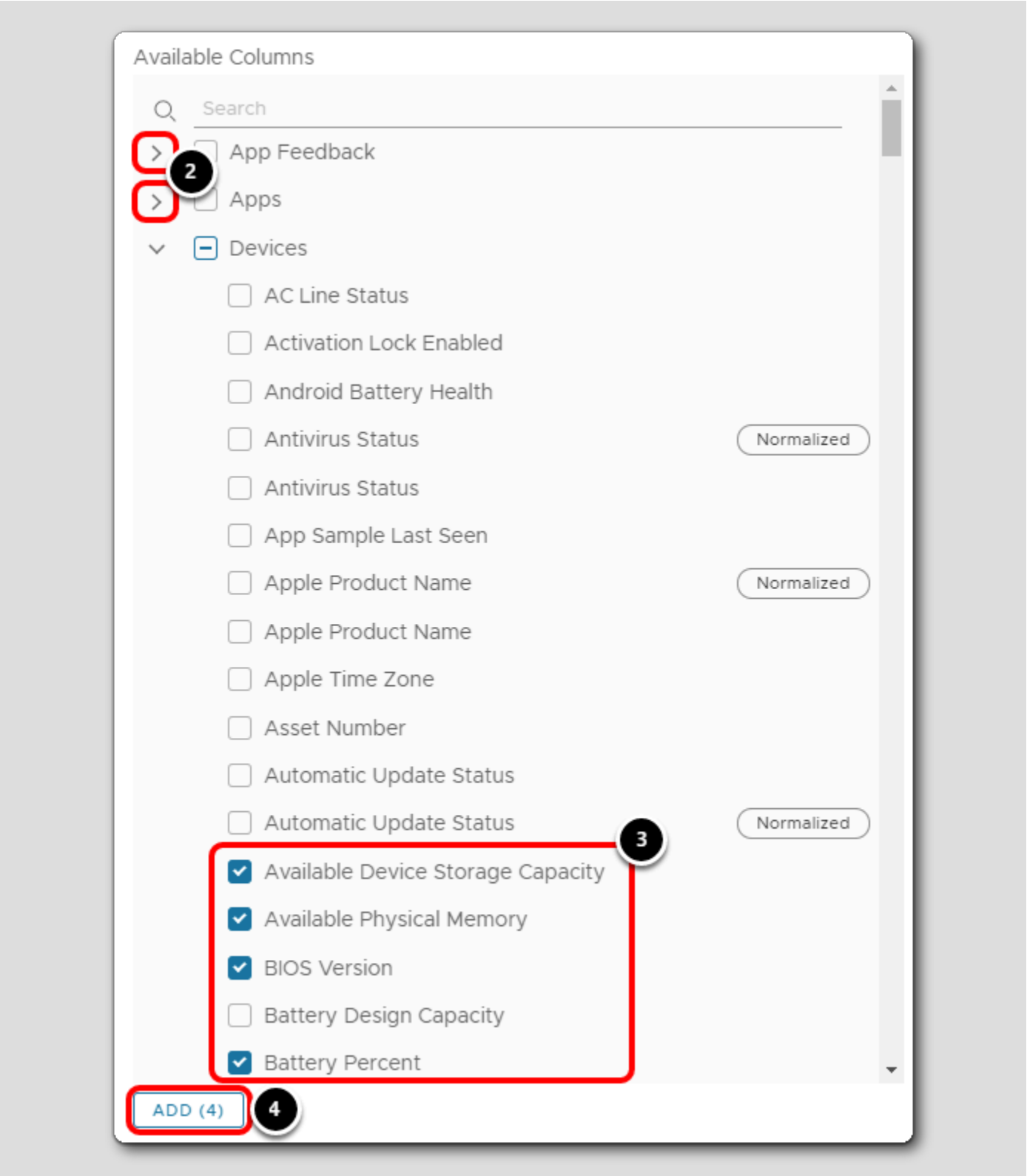


[Report Preview] セクションまで下にスクロールして [Refresh Preview] をクリックします。現在登録しているデバイスが自動的にプレビューに表示される様子を確認します。

[610]

レポートの列の追加

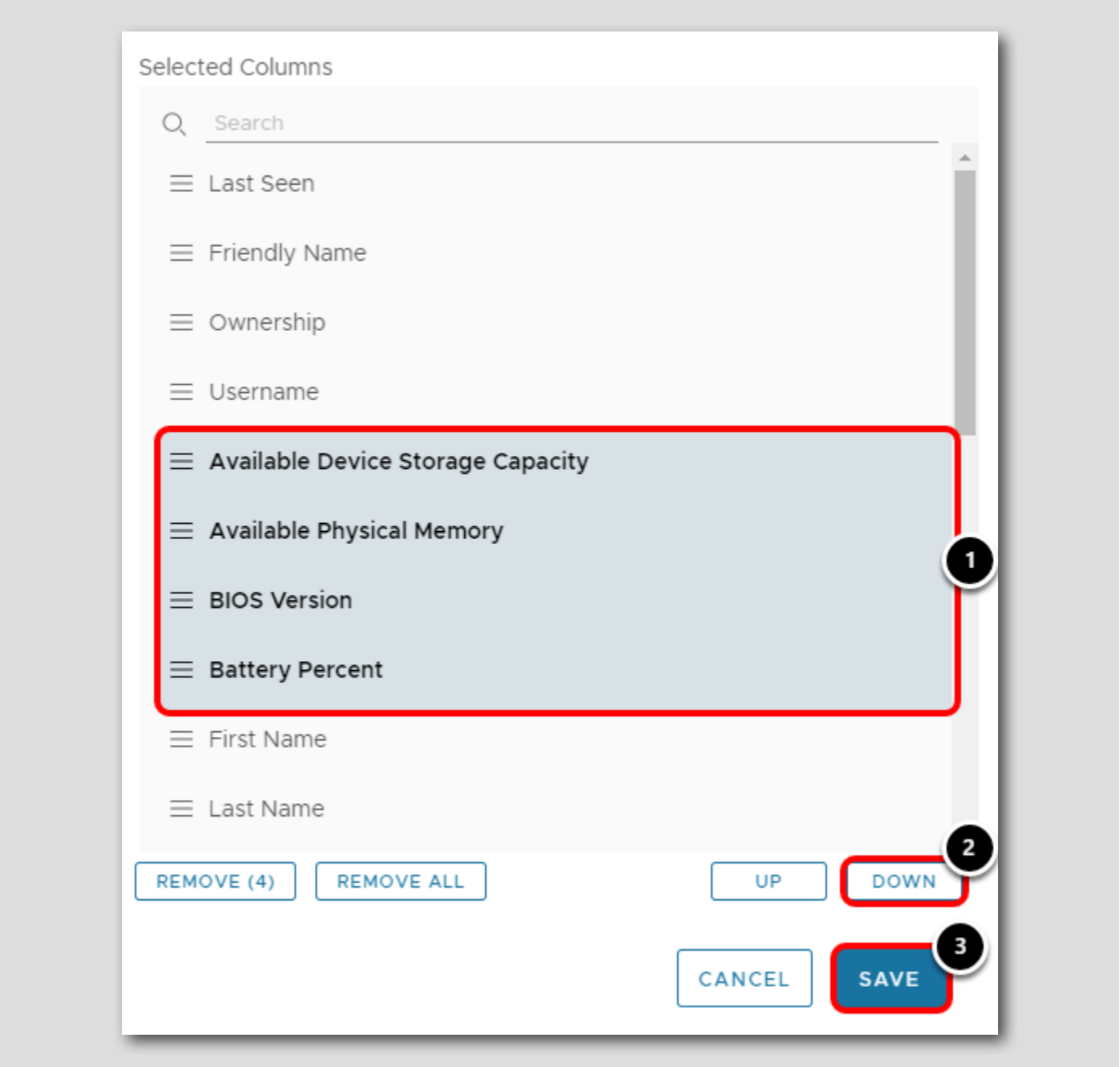



Available Columns
Search
App Feedback
Apps
Devices
AC Line Status
Activation Lock Enabled
Android Battery Health
Antivirus Status
Normalized
Antivirus Status
App Sample Last Seen
Apple Product Name
Normalized
Apple Product Name
Apple Time Zone
Asset Number
Automatic Update Status
Automatic Update Status
Normalized
Available Device Storage Capacity
Available Physical Memory
BIOS Version
Battery Design Capacity
Battery Percent
ADD (4)
2
3
4

1. [Report Preview] で、**[Edit Columns]** ボタンをクリックします。
2. 下にスクロールして [Devices] セクションを見つけます。**[App Feedback]** および **[Apps]** の横にある矢印をクリックすると、これらのセクションを折りたたむことができます。
3. [Available Columns] で、次の項目を選択します。
    - Available Device Storage Capacity
    - Available Physical Memory
    - BIOS Version
    - Battery Percent
4. **[Add]** をクリックします。

列の順序の変更

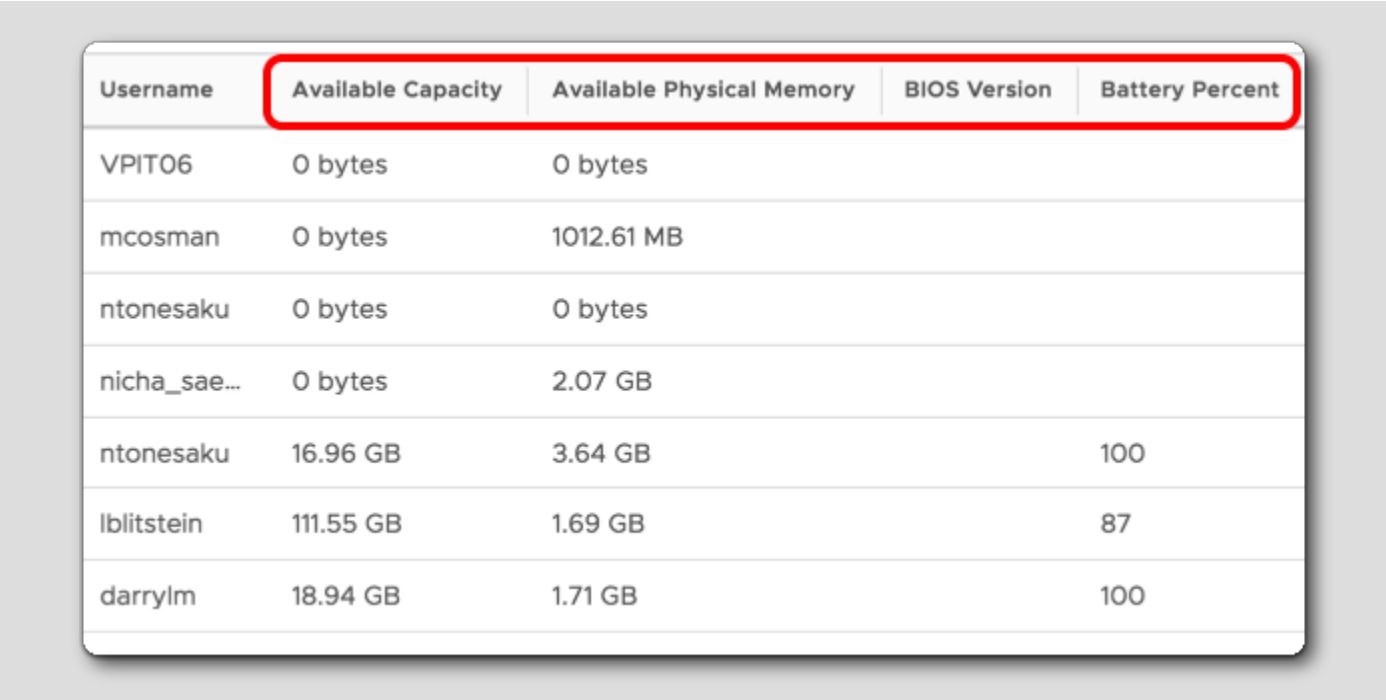
[611]


Selected Columns
Search
Last Seen
Friendly Name
Ownership
Username
Available Device Storage Capacity
Available Physical Memory
BIOS Version
Battery Percent
First Name
Last Name
1
2
3
REMOVE (4)
REMOVE ALL
UP
DOWN
CANCEL
SAVE

1. [Selected Columns] の下で、[Available Device Storage Capacity]、[Available Physical Memory]、[BIOS Version]、および [Battery Percent] を選択します。これらの新しく追加された列は、リストの一番上に表示されます。一度に複数の列を選択するには、Shift キーを押しながら各列をクリックする必要があります。
2. 列を並べ替えるには、[Down] を 4 回クリックします。選択した項目をドラッグアンドドロップして値を上下に移動することもできます。
3. [Save] をクリックします。

新しい列の確認

[612]



Username	Available Capacity	Available Physical Memory	BIOS Version	Battery Percent
VPIT06	0 bytes	0 bytes		
mcosman	0 bytes	1012.61 MB		
ntonesaku	0 bytes	0 bytes		
nicha_sae...	0 bytes	2.07 GB		
ntonesaku	16.96 GB	3.64 GB		100
lblitstein	111.55 GB	1.69 GB		87
darrylm	18.94 GB	1.71 GB		100

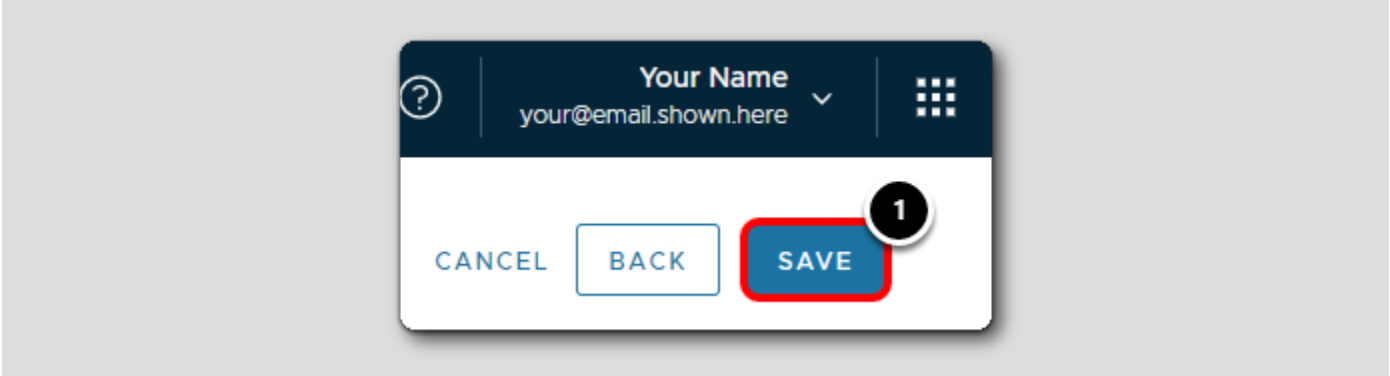
[Report Preview] で、レポートに新しい列が表示されていることを確認します。

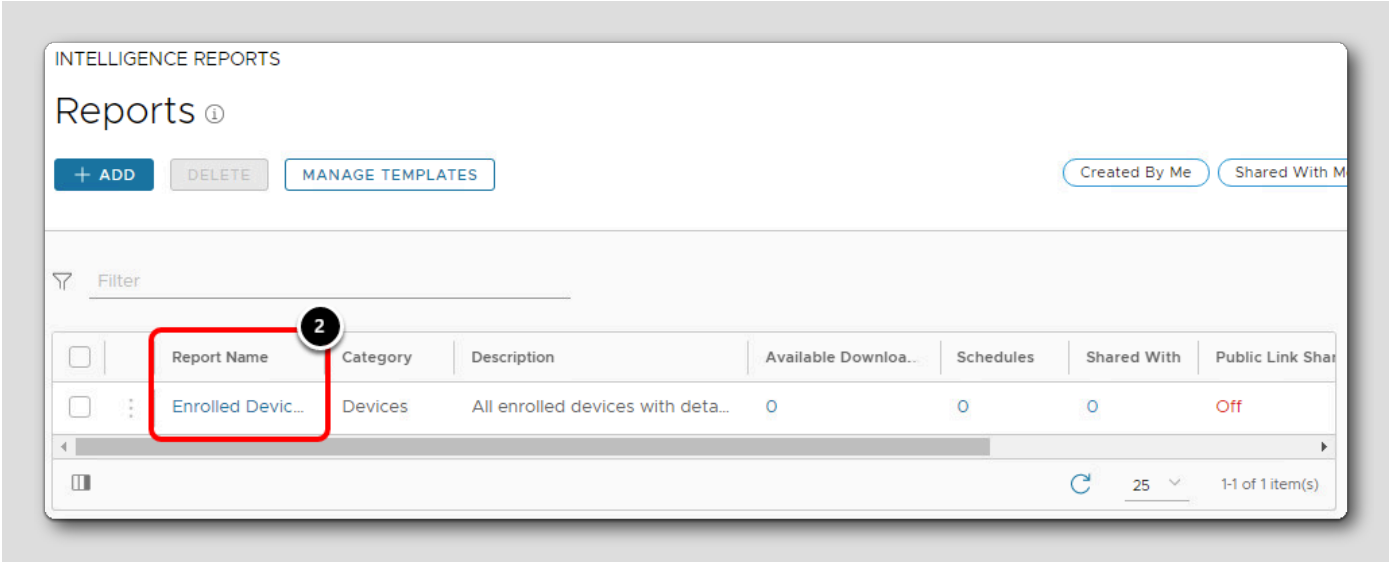
注：列データが空の場合は、デバイス サンプルがまだ取得されていないか、列が特定のデバイスに適用されないためです（例：デスクトップデバイスのバッテリ残量）。

注：上記のスクリーンショットは、複数のデバイスを含むデモ環境の例を示したものです。ご利用の環境では見た目が異なります。

レポートの保存

[613]

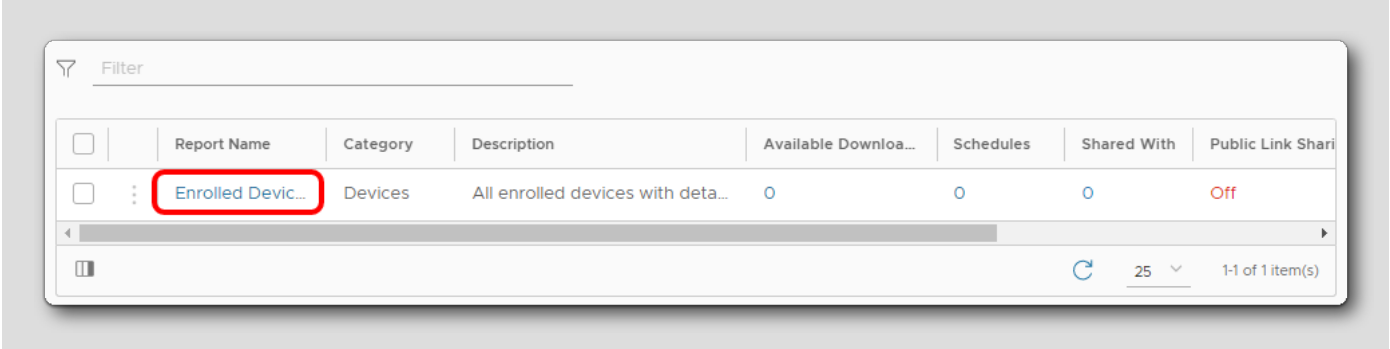




1. 右上隅にある [Save] をクリックして、レポートを保存します。
2. 「Enrolled Devices」レポートが正常に保存されたことを確認します。

レポートの管理

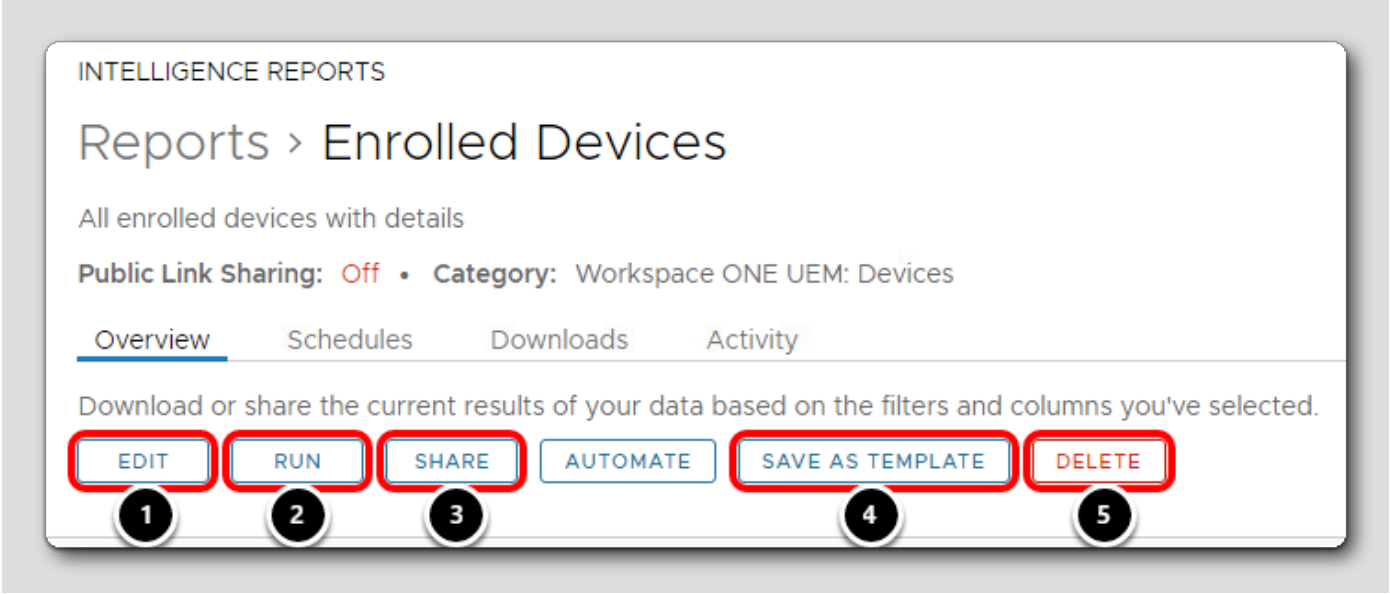
[614]



レポートが保存されると、使用可能なレポートのリストに追加されます。レポートを管理するには、[Report Name (Enrolled Devices)] をクリックします。

レポートの概要の確認

[615]



このビューから、追加の管理設定を構成できます。

注：次のボタンはクリックしないでください。これらの詳細は情報提供のみを目的としています。

1. [Edit]：レポートを作成したときに構成した設定を変更できます。
2. [Run]：手動でデータ同期をトリガできます。
3. [Share]：レポートを E メールで送信できます。
4. [Save As Template]：このレポートからテンプレートを作成できます。
5. [Delete]：レポートを削除できます。

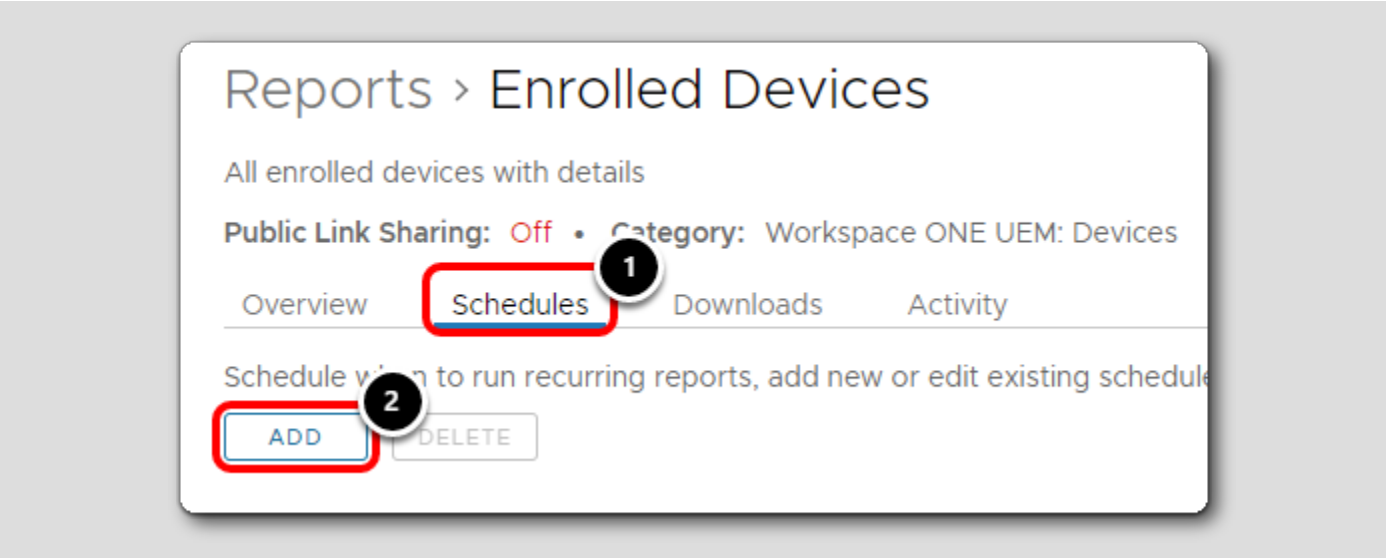
レポートのスケジュール設定

[616]

レポートを保存した後、スケジュール設定を使用して、データの収集と共同作業を自動化できます。このアクティビティでは、「*Enrolled Devices*」レポートを月ごとに実行するようにスケジュール設定します。

レポート スケジュールの追加

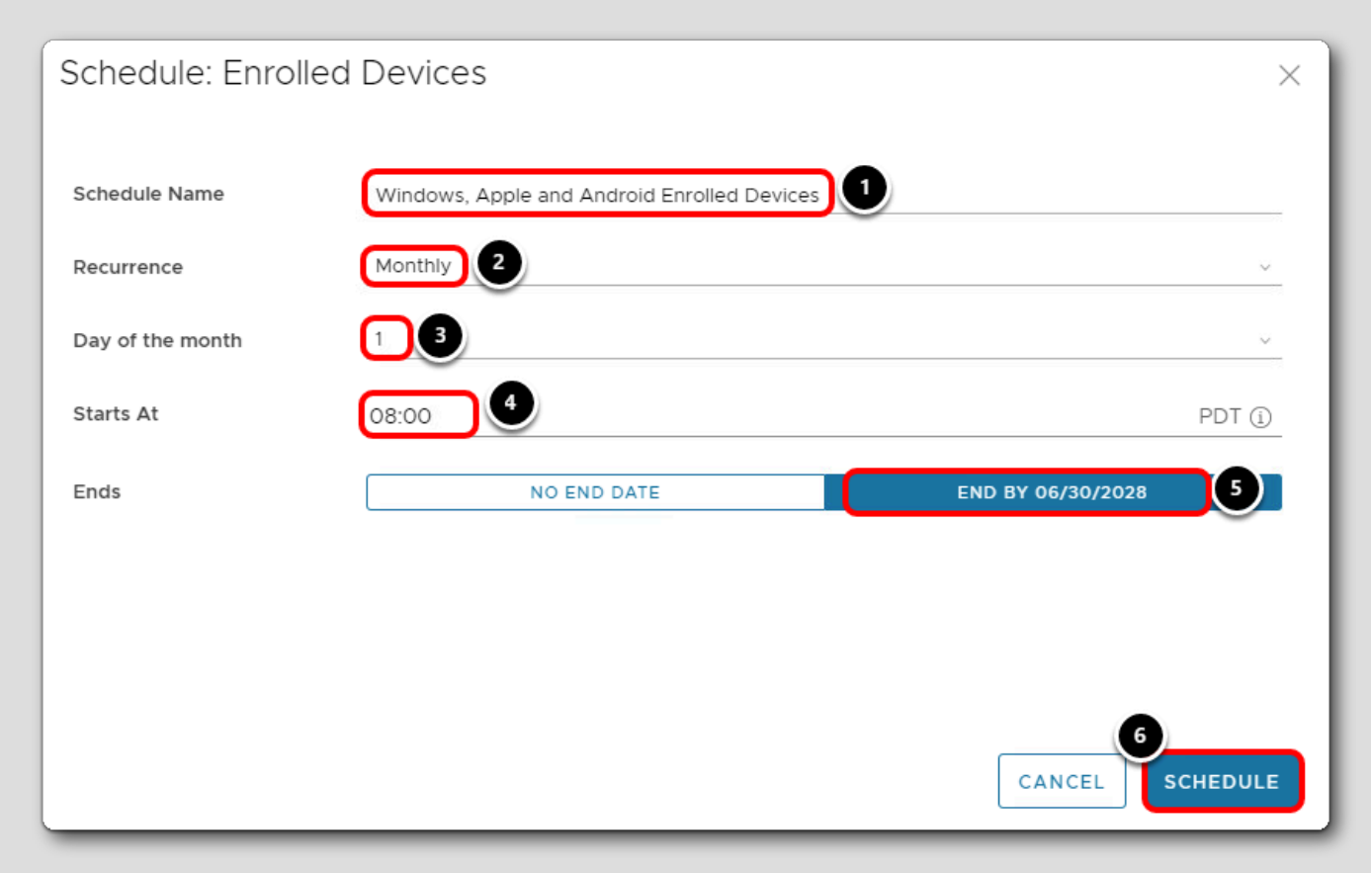
[617]



1. [Schedules] をクリックします。
2. [Add] をクリックします。

レポート スケジュールの構成

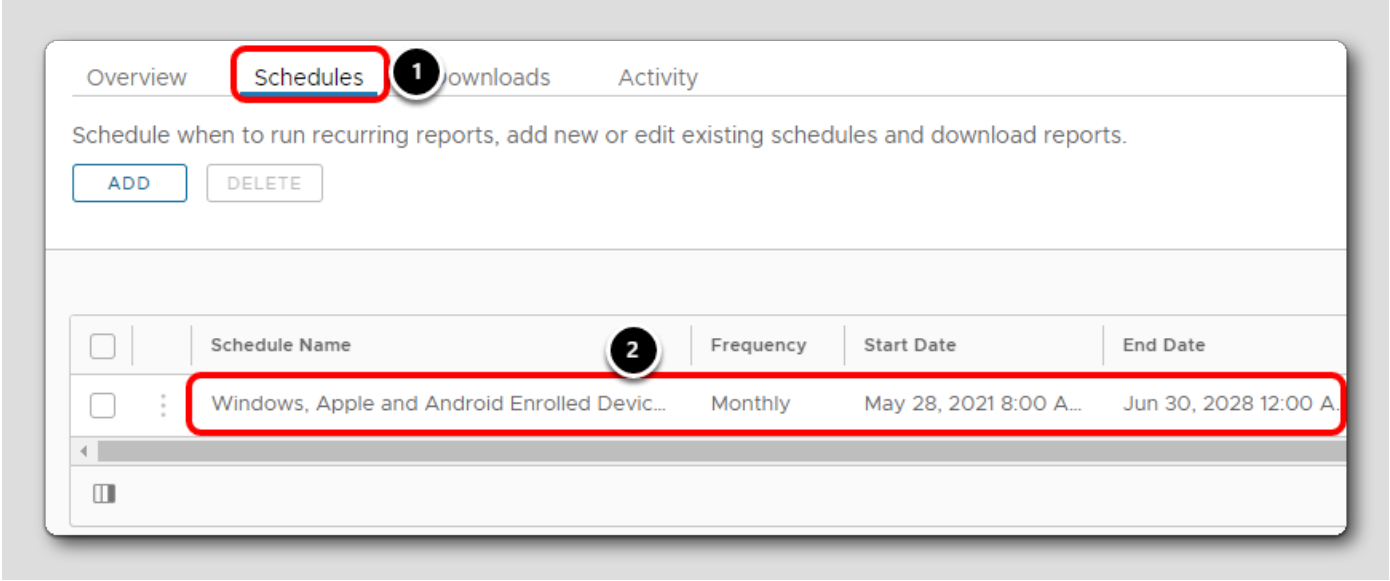
[618]



1. スケジュール名を入力します。たとえば、**Windows, Apple and Android Enrolled Devices** のように入力します。
2. [Recurrence] に対して **[Monthly]** を選択します。
3. [Day of the Month] に対して **[1]** を選択します。
4. [Start AT] で、時刻を **08:00** に変更します。
5. [Ends] で、**06/30/2028** などの未来の日付を選択します。ポップアウトの年の横にあるドロップダウン矢印をクリックすると、現在選択されている年を変更できます。
6. **[Schedule]** をクリックします。

レポート スケジュールの確認

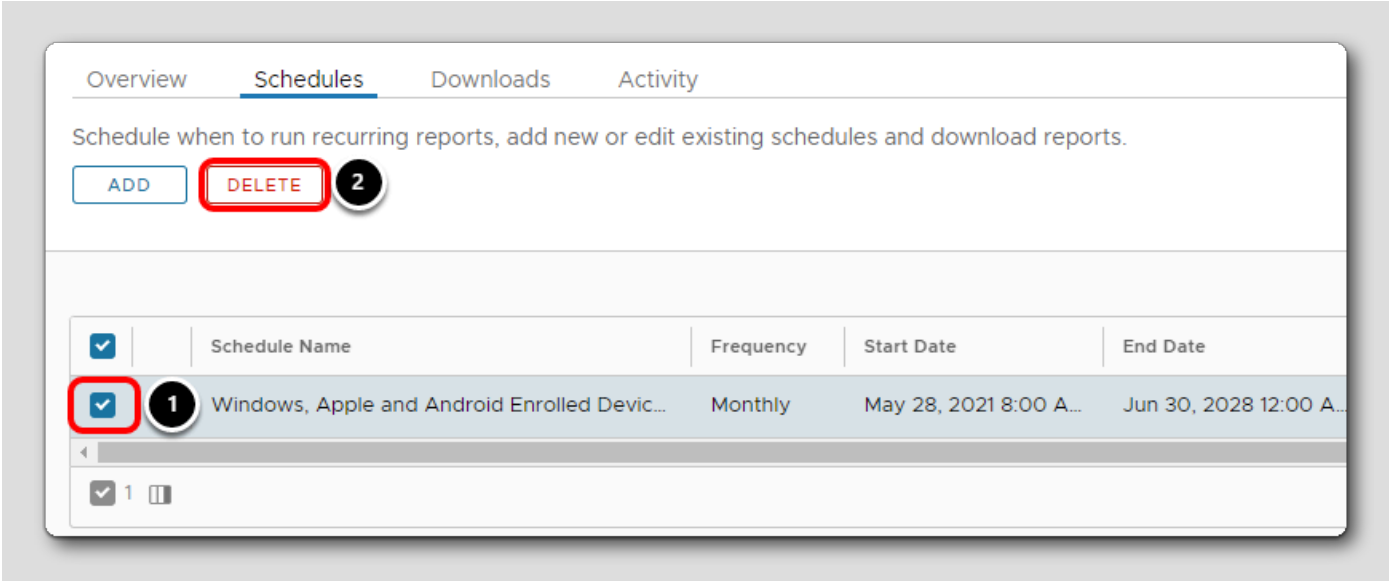
[619]

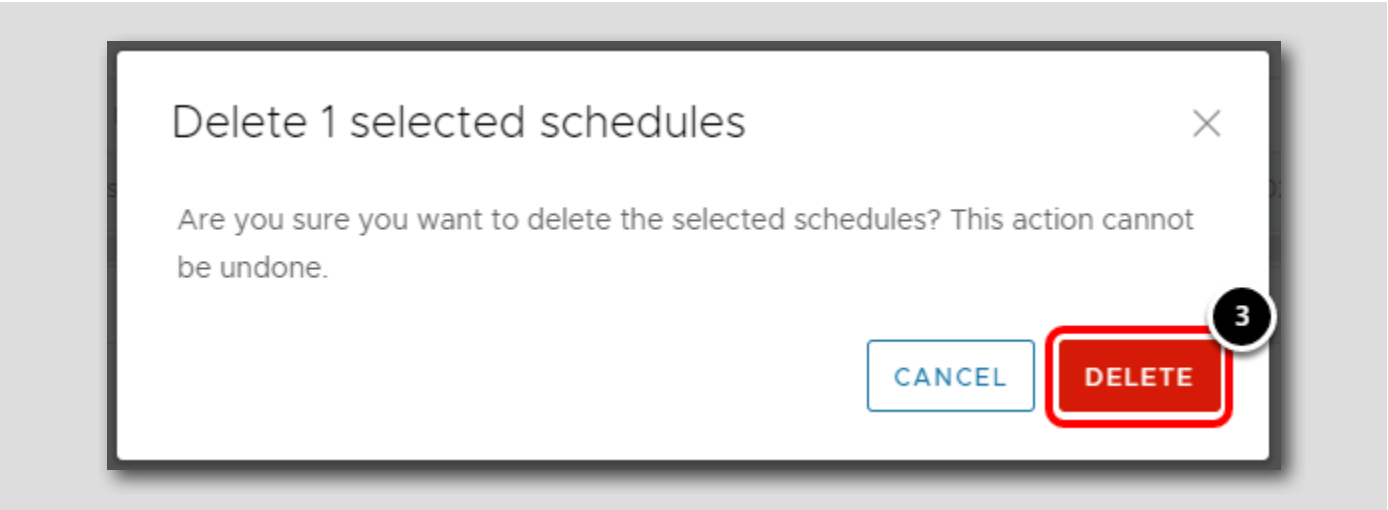


1. [Schedules] をクリックします。
2. 定義したパラメータとスケジュールが一致していることを確認します。

レポート スケジュールの削除

[620]





スケジュール レポートを削除するには、次のように操作します。

1. 削除するレポートを選択します。この場合は、先ほど作成した「Windows, Apple and Android Enrolled Devices」レポートを選択します。
2. [Delete] をクリックします。
3. ポップアップで [Delete] をクリックして、アクションを確認します。

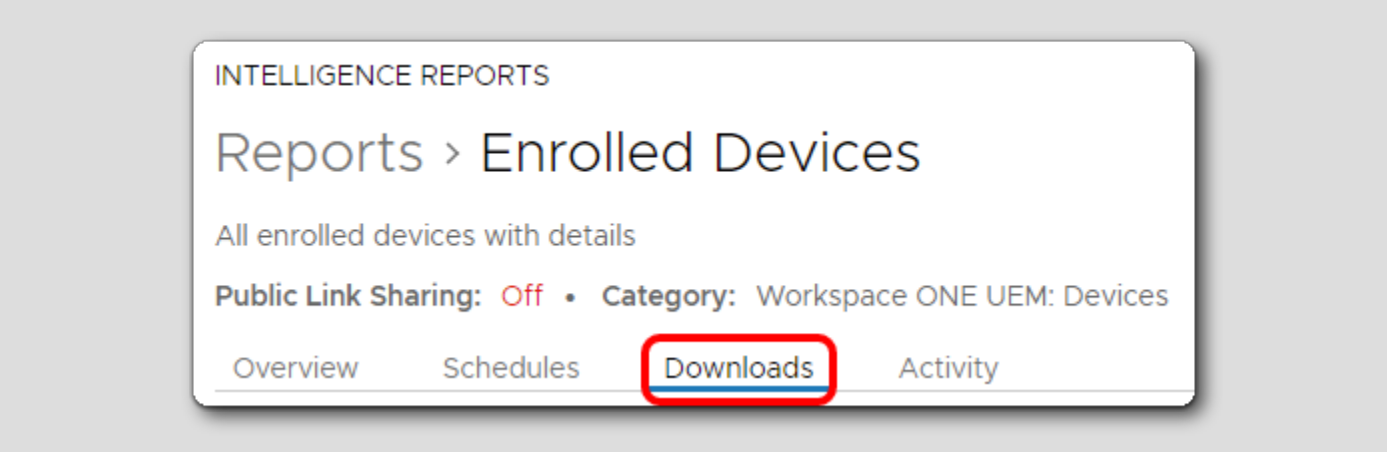
レポートのダウンロード

[621]

レポートを保存した後、すぐに CSV ファイルとしてダウンロードできます。このアクティビティでは、作成した「*Enrolled Devices*」レポートの CSV ファイルをダウンロードします。

レポートのダウンロードへのアクセス

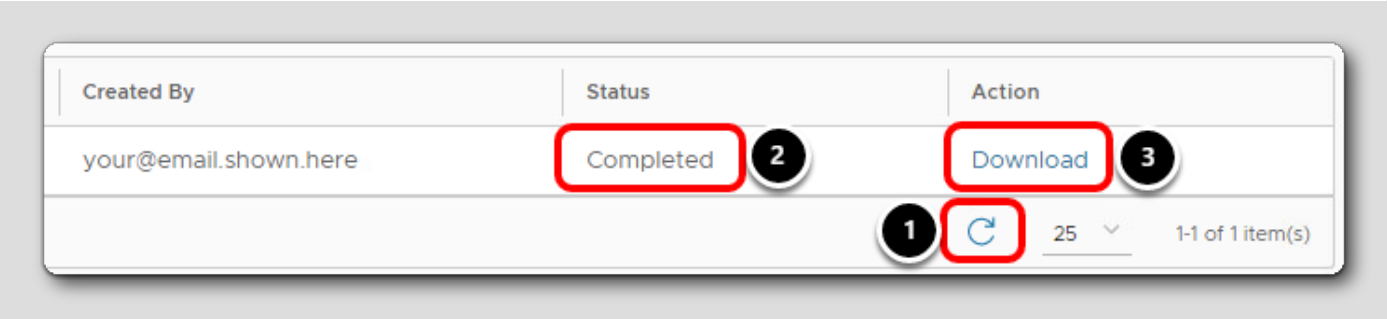
[622]

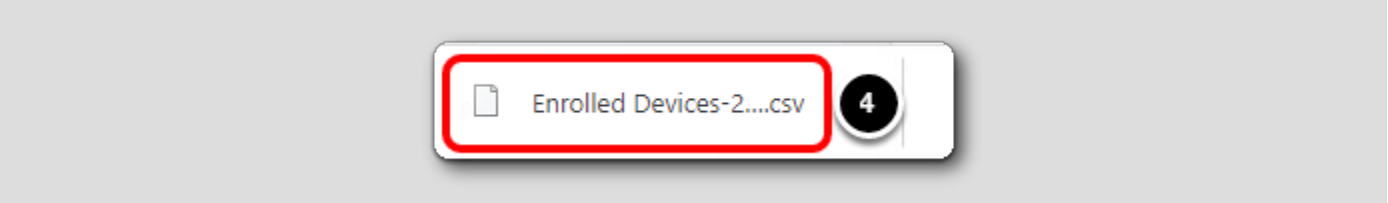


レポートで利用可能なダウンロードにアクセスするには、[Downloads] タブを選択します。

レポートのダウンロード

[623]



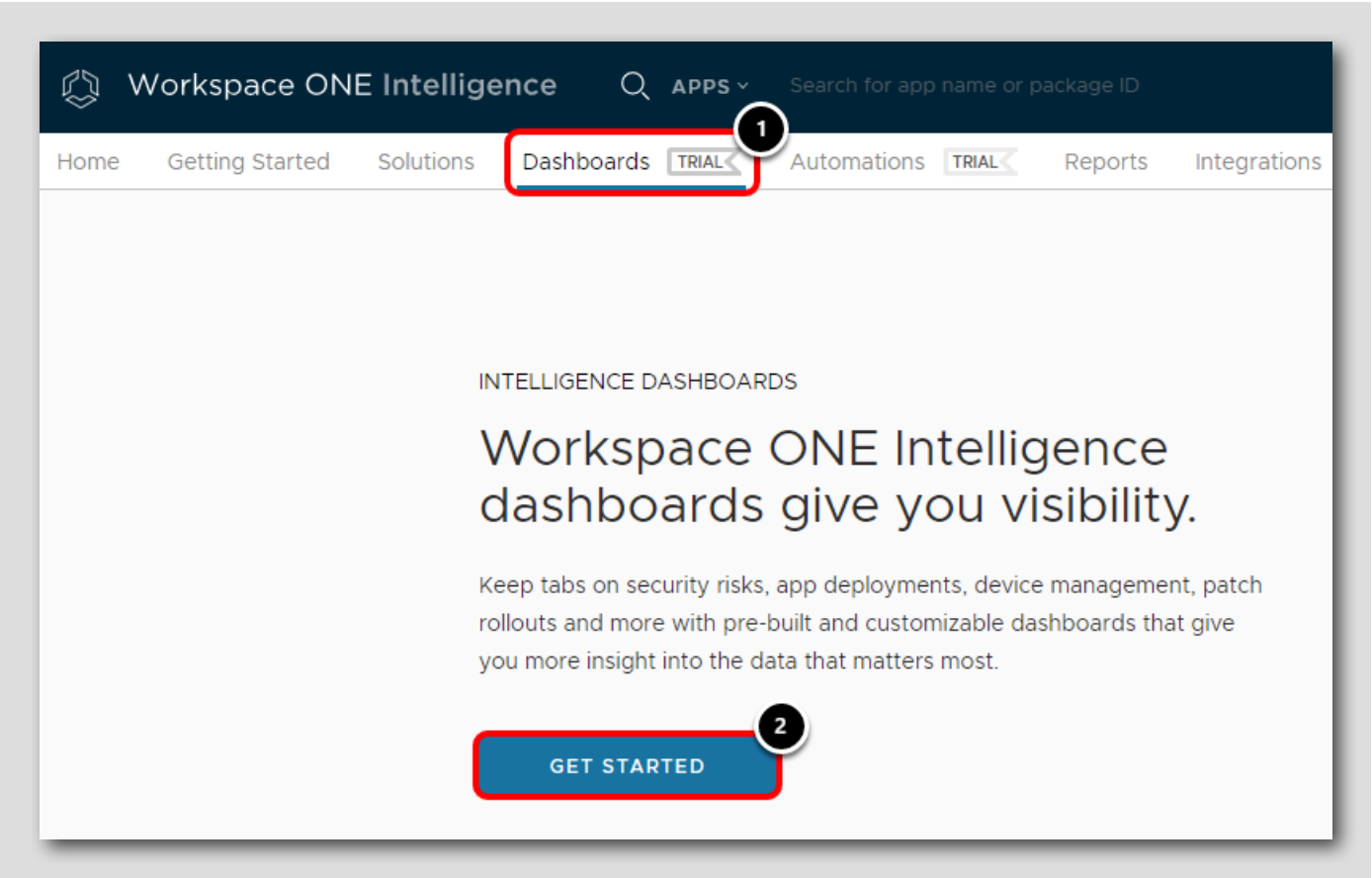


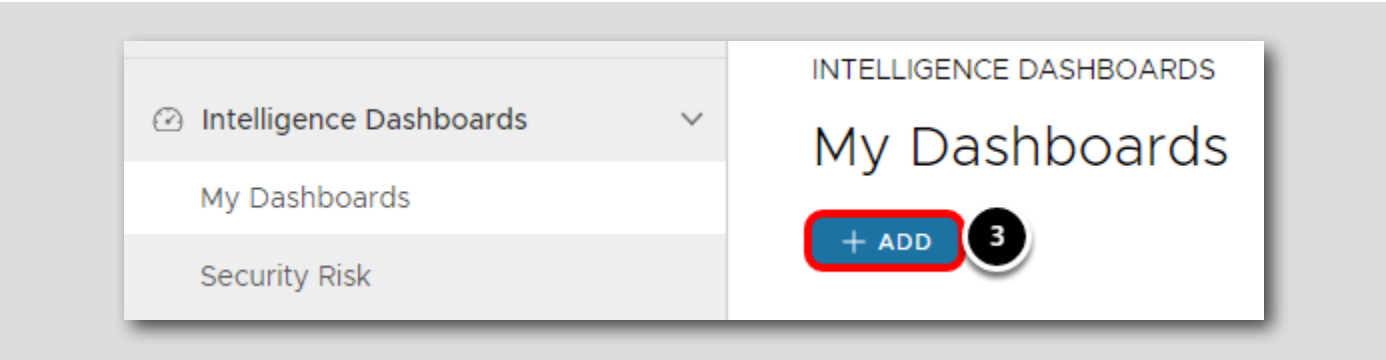
[Downloads] タブで、次のように操作します。

1. レポートが表示されない場合は、**[Refresh]** アイコンをクリックしてリストを更新します。
2. ステータスが **[Completed]** になっていることを確認します。
3. **[Download]** をクリックします。
4. 「*Enrolled Devices*」レポートの CSV がダウンロードされていることを確認します。

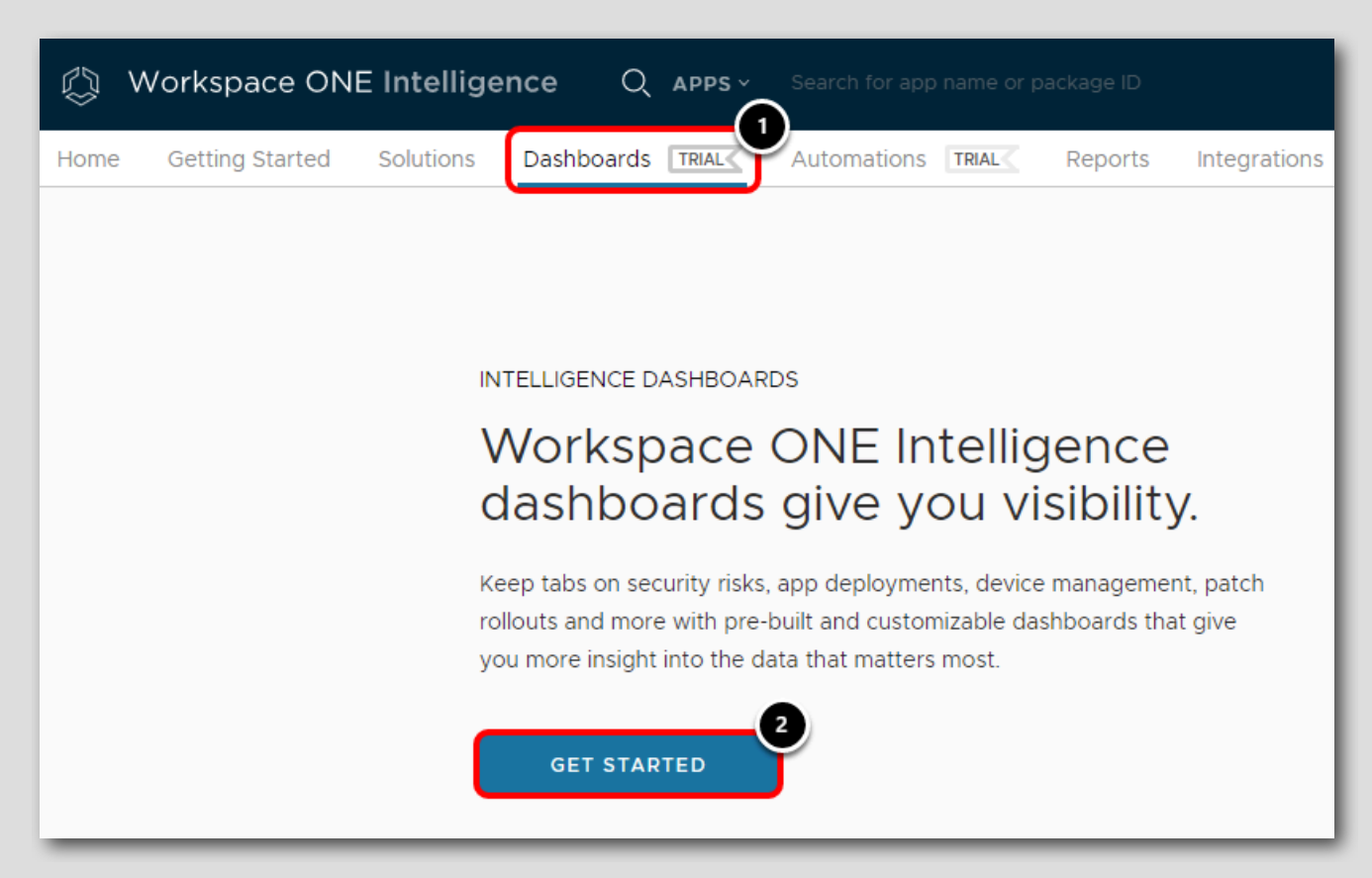
ダッシュボード ビューのカスタマイズ

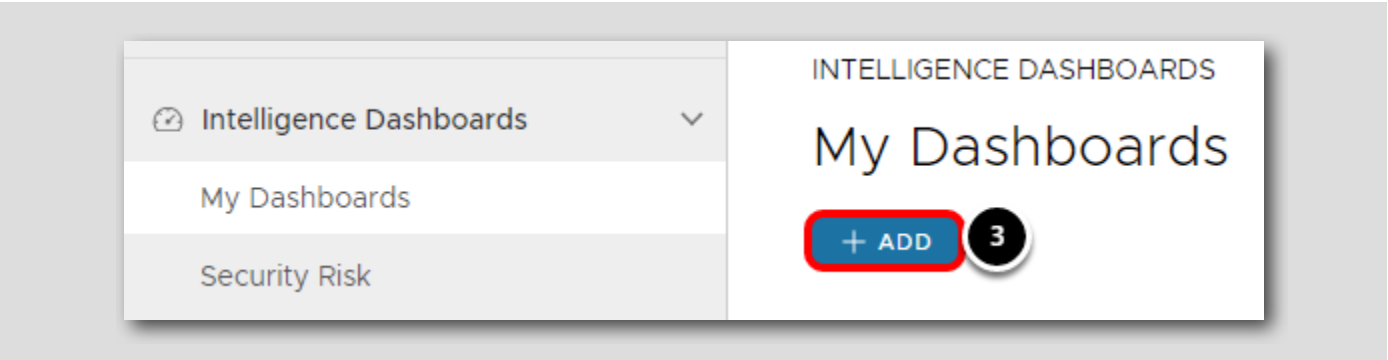
[624]





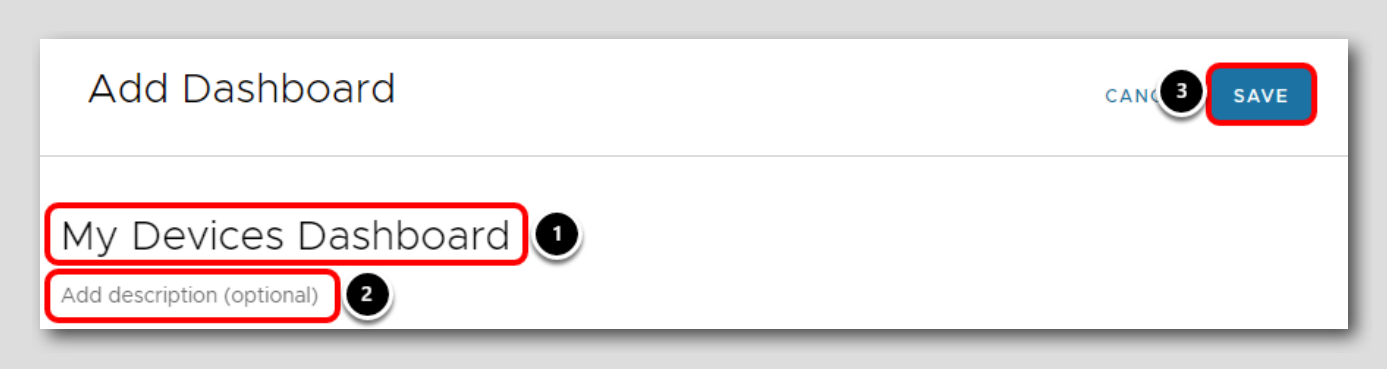
1. [Dashboards] タブをクリックします。
2. [Dashboards] ページに初めてアクセスする場合は、[Get Started] ページが表示されます。その場合は、[Get Started] をクリックします。
3. [Add] をクリックして、新しいダッシュボードを作成します。





ダッシュボードの追加

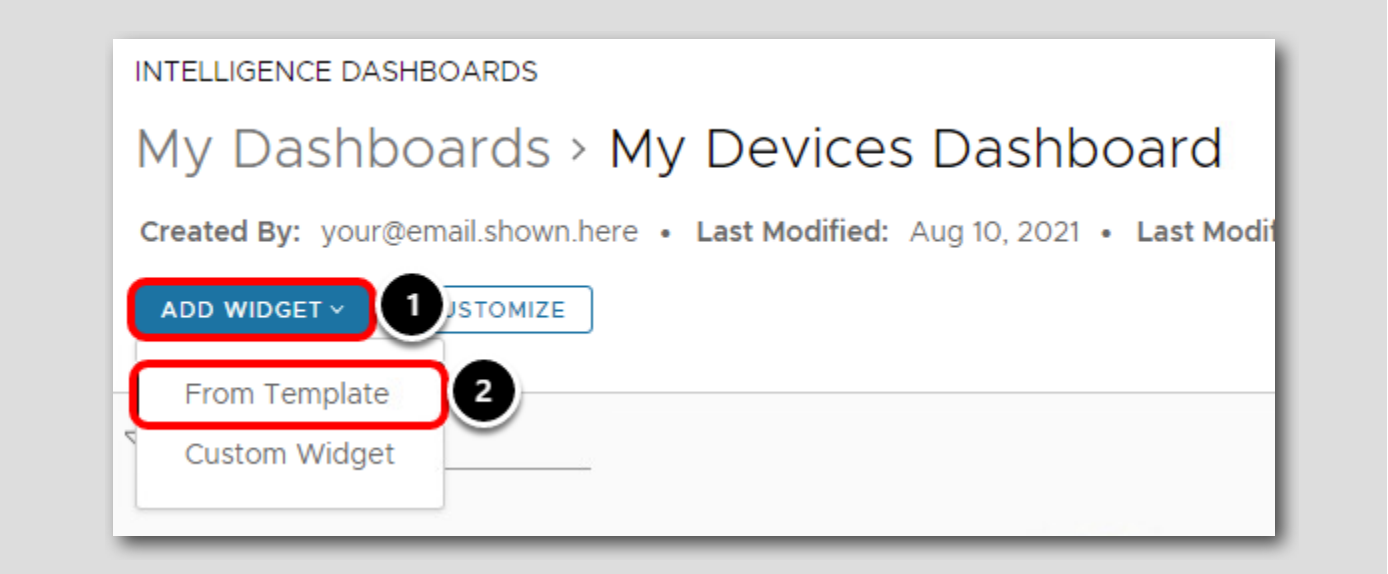
[625]



1. ダッシュボード名（**`My Devices Dashboard`** など）を入力します。
2. 必要に応じてダッシュボードの説明を入力します。
3. [Save] をクリックします。

ウィジェットの追加

[626]

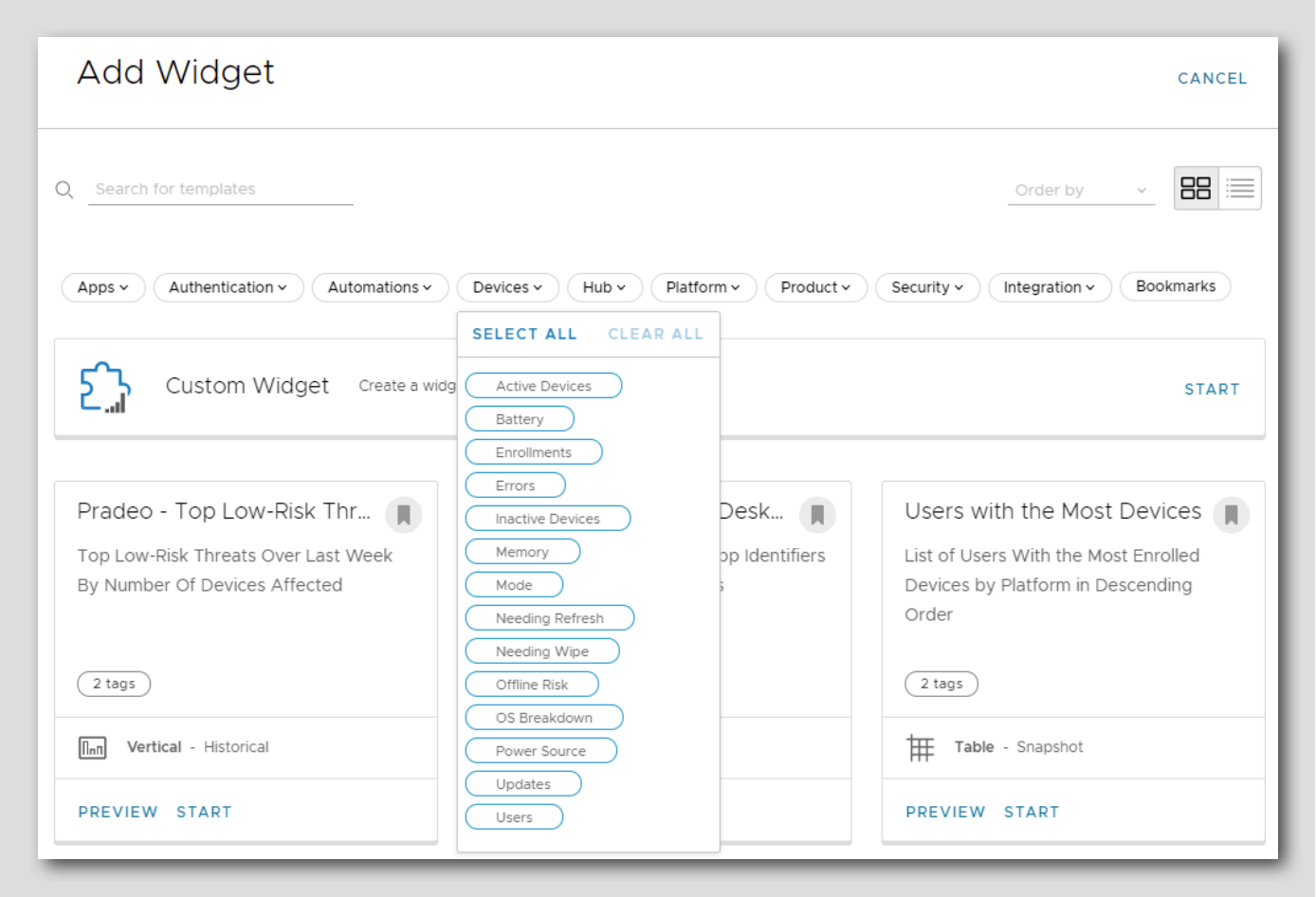


デフォルトでは、新しく作成されたダッシュボードには情報がありません。これらのダッシュボードにウィジェットを追加し、ビジネス ニーズに合わせてカスタム ダッシュボードを作成できます。

1. [Add Widget] をクリックします。
2. [From Template] をクリックします。

ウィジェット カテゴリとテンプレートの確認

[627]



ウィジェットの作成を開始するには、カスタム ウィジェットを選択するか、カテゴリとタグを選択して組み込みのウィジェットの 1 つを選択します。カテゴリのリストは、Workspace ONE Intelligence に構成された統合に基づいており、このアクティビティで表示されるイメージとは異なる場合があります。

使用可能なカテゴリは以下の通りです。

- Apps
- Authentication
- Automations
- Devices
- Hub
- Platform
- Product
- Security
- Integration

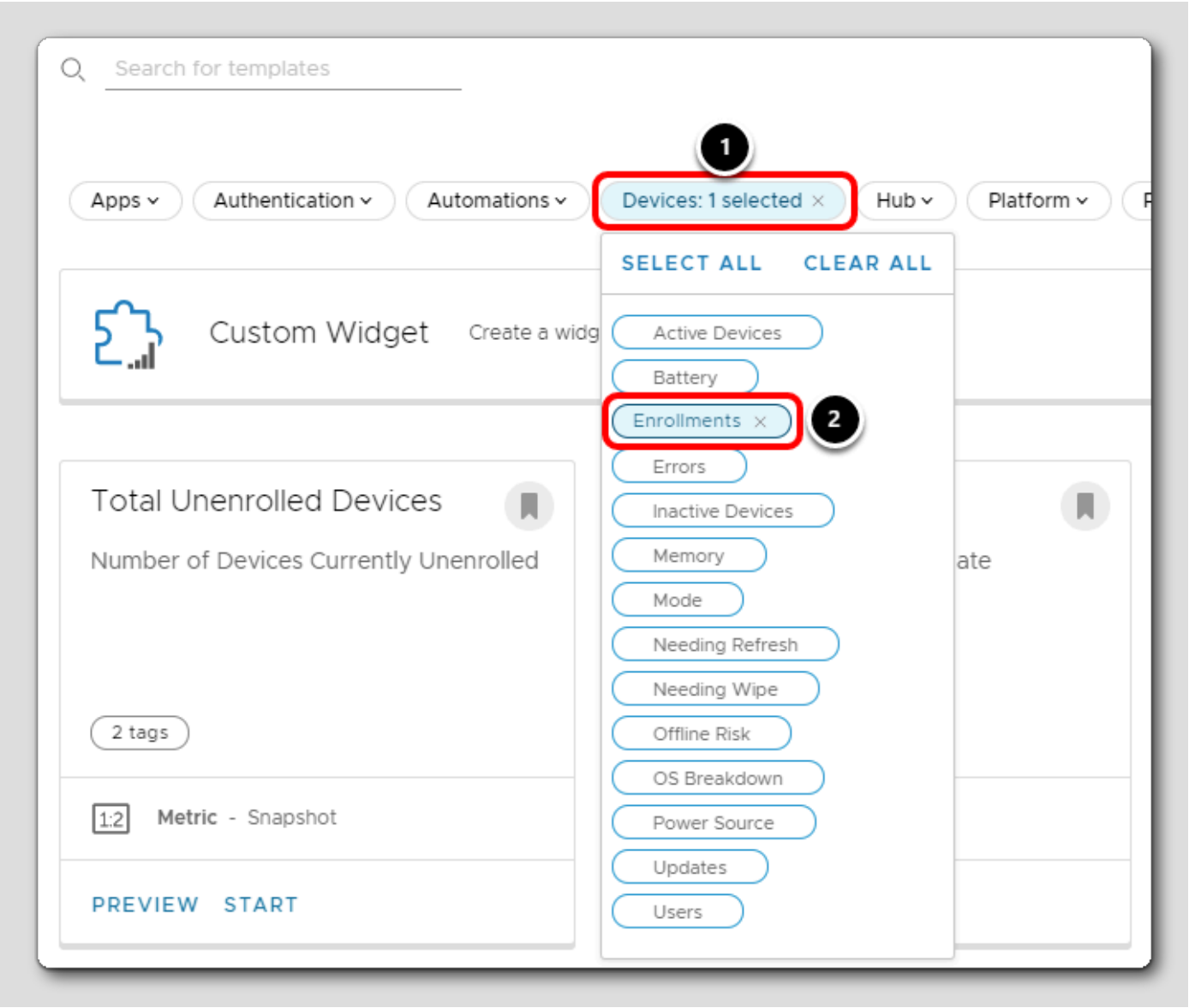
初めて Workspace ONE Intelligence を開始すると、複数のカテゴリが表示されます。

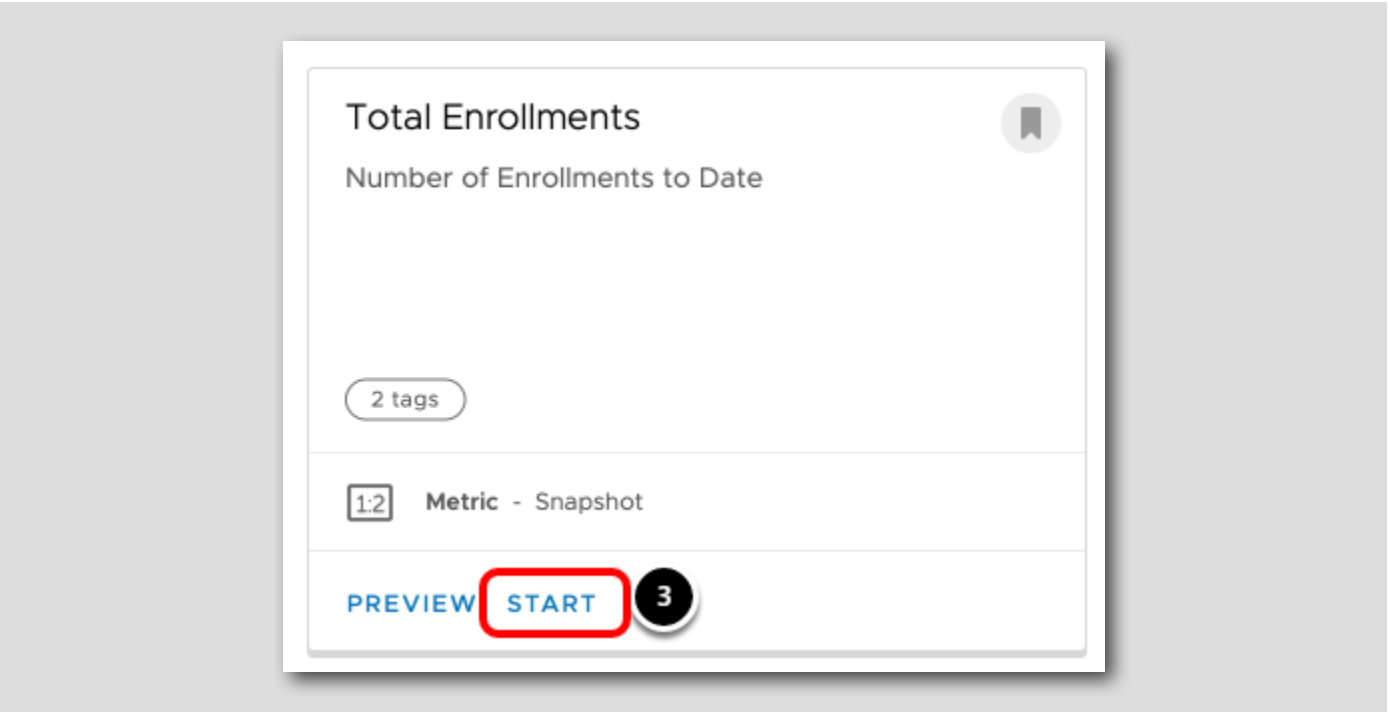
次に、各カテゴリのタグを使用して、カスタマイズ可能なテンプレートをフィルタリングし、ウィジェットに表示されるコンテンツを定義します。ウィジェットのコンテンツを完全に制御するには、Custom Widget テンプレートを使用して独自の条件を定義します。

各カテゴリをクリックすると、対応するテンプレートを表示できます。

テンプレートの選択

[628]



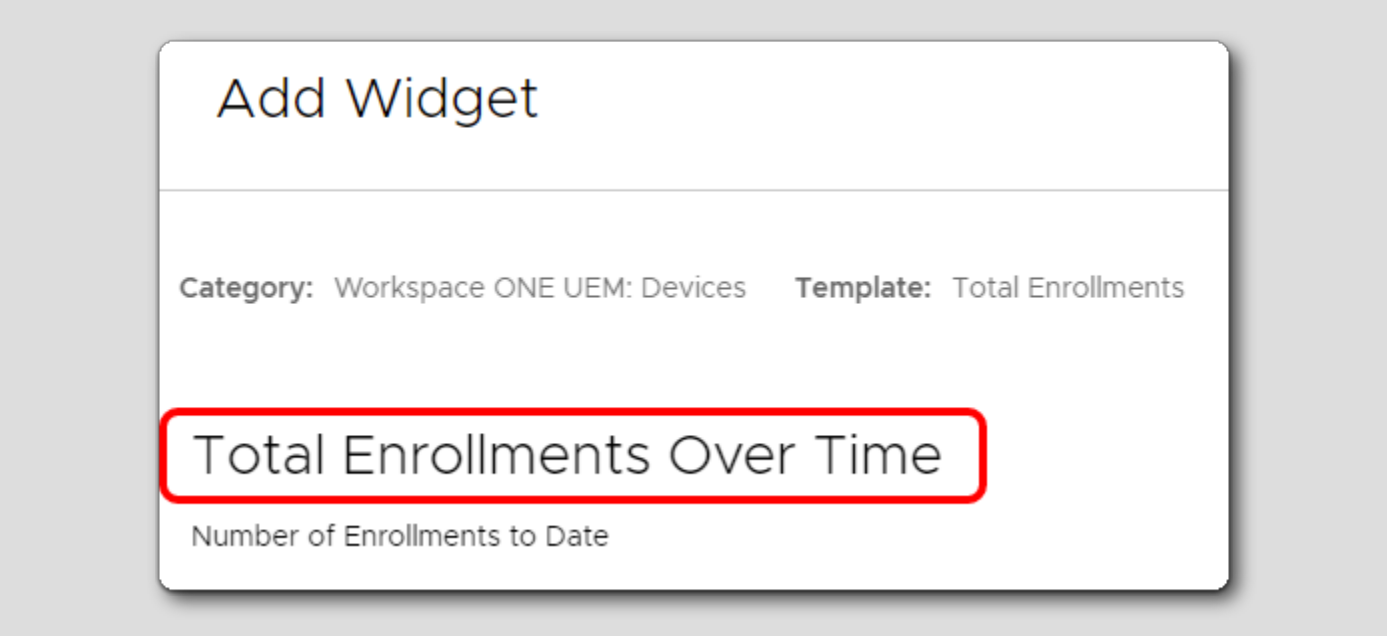


1. [Devices] カテゴリを選択します。

   注：クリックしてもドロップダウンがロードされない場合は、[Devices] カテゴリをクリックする前に下にスクロールする必要がある場合があります。小さい解像度でドロップダウンを描画するのに十分なユーザー インターフェイス領域がない場合、リストはロードされません。
2. [Enrollments] タグを選択します。
3. [Total Enrollments] テンプレートに対して [Start] をクリックします。

デフォルトのテンプレートに名前を付ける

[629]

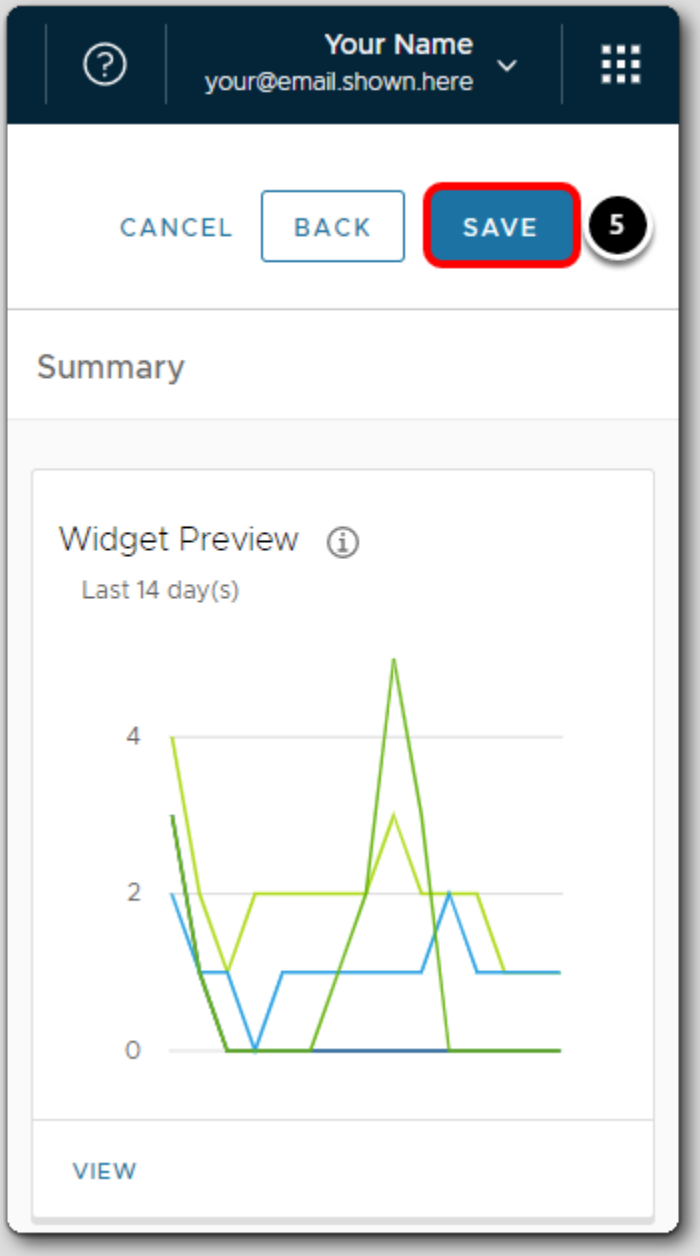


[Data Visualization] で、デフォルトの Total Enrollments テンプレートを確認します。初期のデフォルト設定では、現在のデバイス登録のスナップショットが提供されます。設定を変更すると、スナップショットの結果もそれに応じて変更されます。

ウィジェットの名前を **`Total Enrollments Over Time`** に変更します。

テンプレートの構成

[630]


Your Name
your@email.shown.here
CANCEL
BACK
SAVE
5
Summary
Widget Preview
Last 14 day(s)
4
2
0
VIEW

時間の経過に伴う登録総数のスナップショットを作成するには、デフォルトの Total Enrollments テンプレートを変更します。

1. [Historical] を選択します。
2. [Chart Type] に対して [Line] を選択します。
3. [Group by] に **`Platform`** と入力し、リストから最初の結果を選択します。
4. [Date Range] を **`Last 14 Days`** に設定します。
5. 右上隅にある [Save] をクリックして、ウィジェットを保存します。

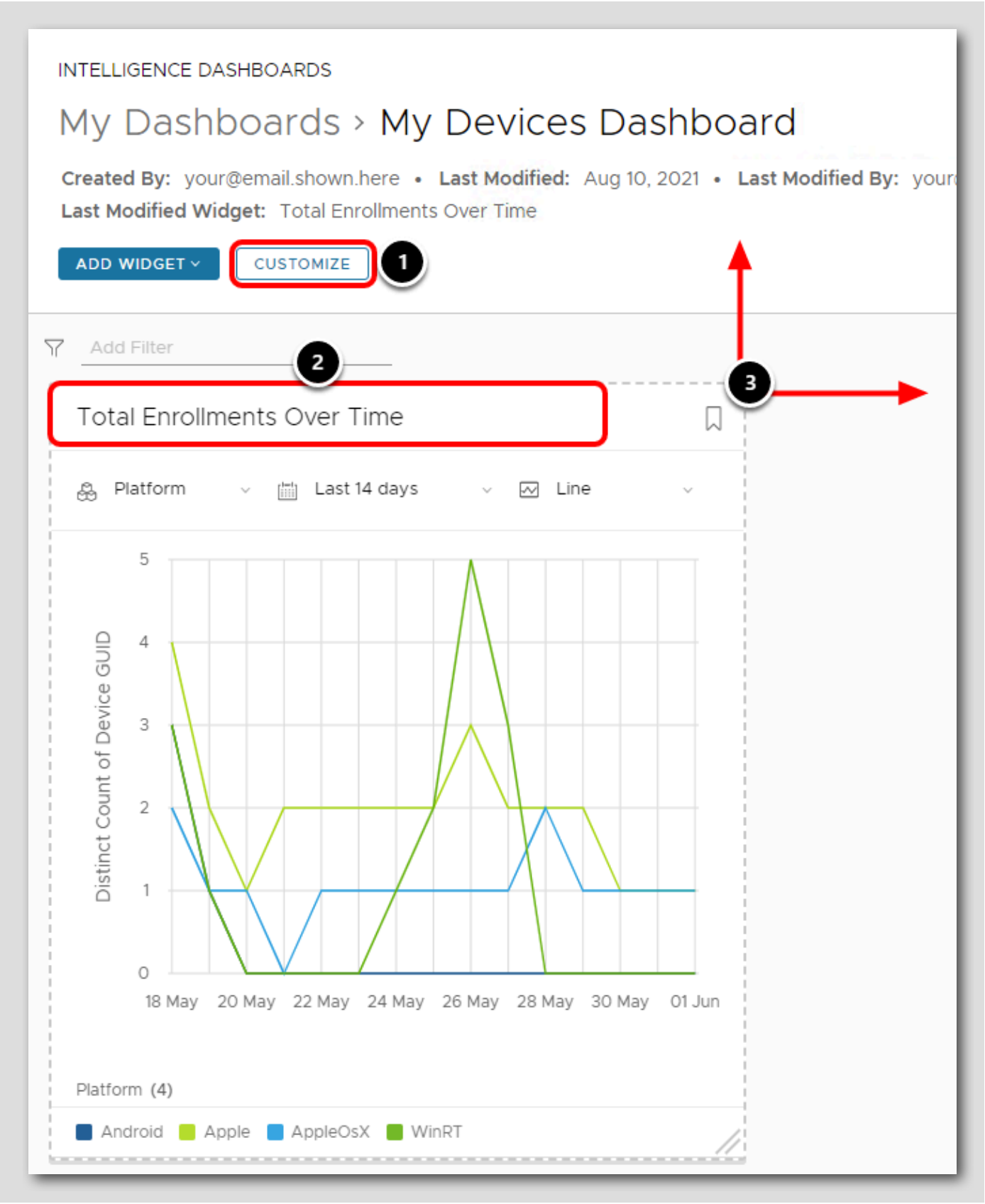
注：表示されているスクリーンショットはテスト環境のものです。プレビューはお使いの環境に基づいており、スクリーンショットに表示されているプレビューとは異なります。

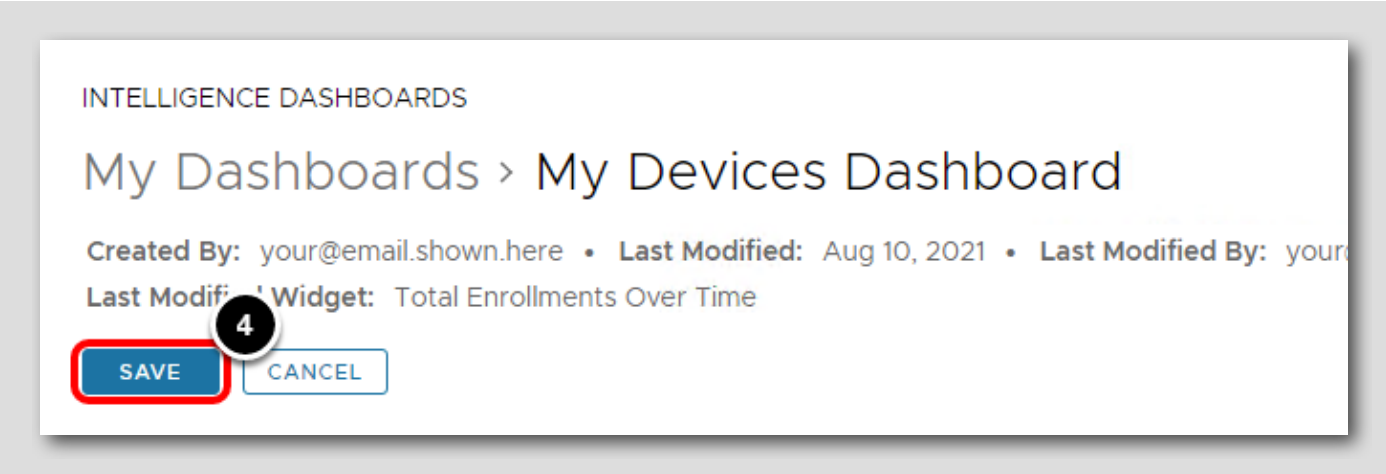
レポート機能の補足として、Workspace ONE Intelligence ダッシュボードには、使用しやすい視覚的なサマリに重要なビジネス データが表示されます。ダッシュボード内で、構成可能なウィジェットを使用して、表示されるデータをカスタマイズできます。

[Total Enrollment Over Time] ウィジェットを構成した後、ダッシュボードでの表示方法を管理できます。このアクティビティでは、[Total Enrollment Over Time] ウィジェットを再配置して展開することで、ダッシュボードのビューを変更します。

ダッシュボードのカスタマイズ

[631]


INTELLIGENCE DASHBOARDS
My Dashboards › My Devices Dashboard
Created By: your@email.shown.here • Last Modified: Aug 10, 2021 • Last Modified By: your
Last Modified Widget: Total Enrollments Over Time
ADD WIDGET
CUSTOMIZE
1
Add Filter
2
3
Total Enrollments Over Time
Platform
Last 14 days
Line
Distinct Count of Device GUID
5
4
3
2
1
0
18 May
20 May
22 May
24 May
26 May
28 May
30 May
01 Jun
Platform (4)
Android
Apple
AppleOsX
WinRT

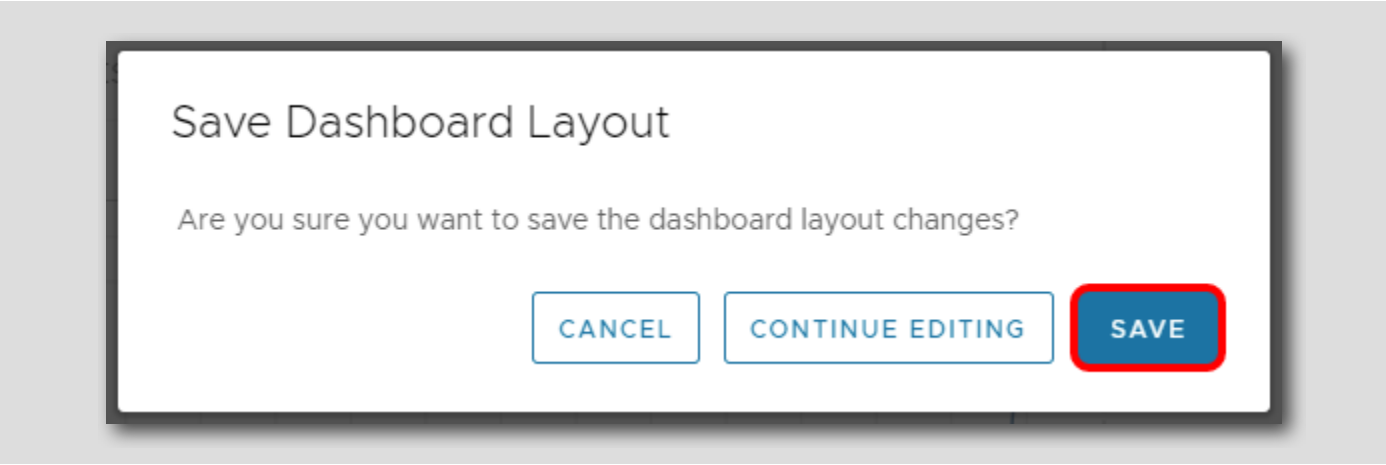


デフォルトでは、新しいウィジェットはダッシュボードの下部に表示されます。これはこのダッシュボードの最初のウィジェットであるため、最上部に表示されます。

1. [Customize] をクリックし、ダッシュボード ウィジェットのロックを解除します。
2. [Total Enrollments Over Time]（グラフのタイトル）をクリックして、ウィジェットをダッシュボードの新しい位置にドラッグできます。
3. ウィジェットの端をクリックしてドラッグすると、[Total Enrollments over Time] ウィジェットの幅または高さを変更できます。
4. ウィジェットの位置とサイズに問題がなければ、[Dashboards] ページの上部にある [Save] をクリックします。

ダッシュボード レイアウトの保存

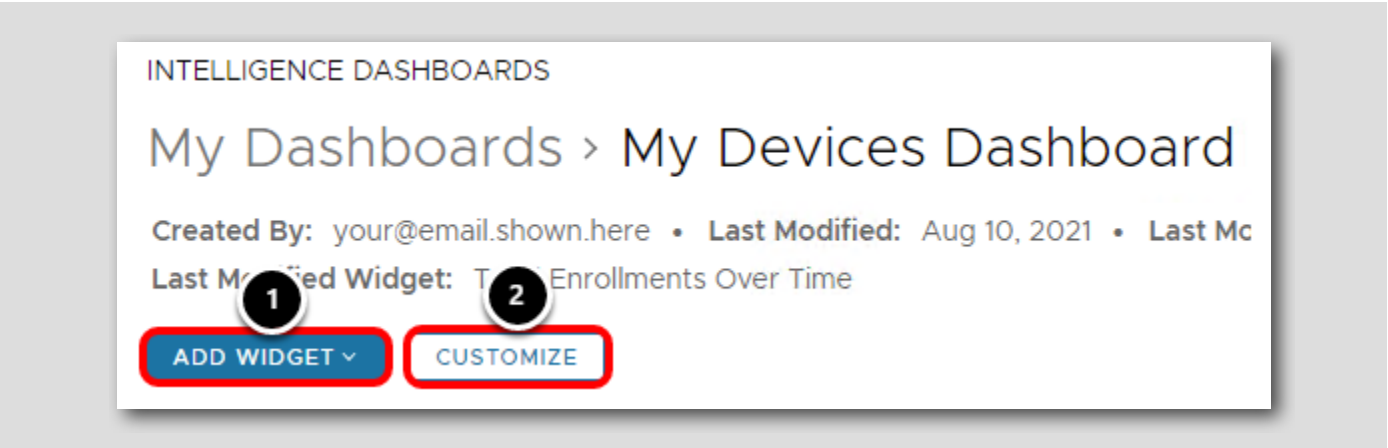
[632]



[Save] をクリックして、ダッシュボード レイアウトを保存します。

ダッシュボードの今後の更新

[633]



今後ダッシュボードを変更する場合は、次の操作を行うことができます。

1. [Add Widget]：ダッシュボードにウィジェットを追加できます。
2. [Customize]：ダッシュボード上の既存のウィジェットのレイアウトを変更できます。

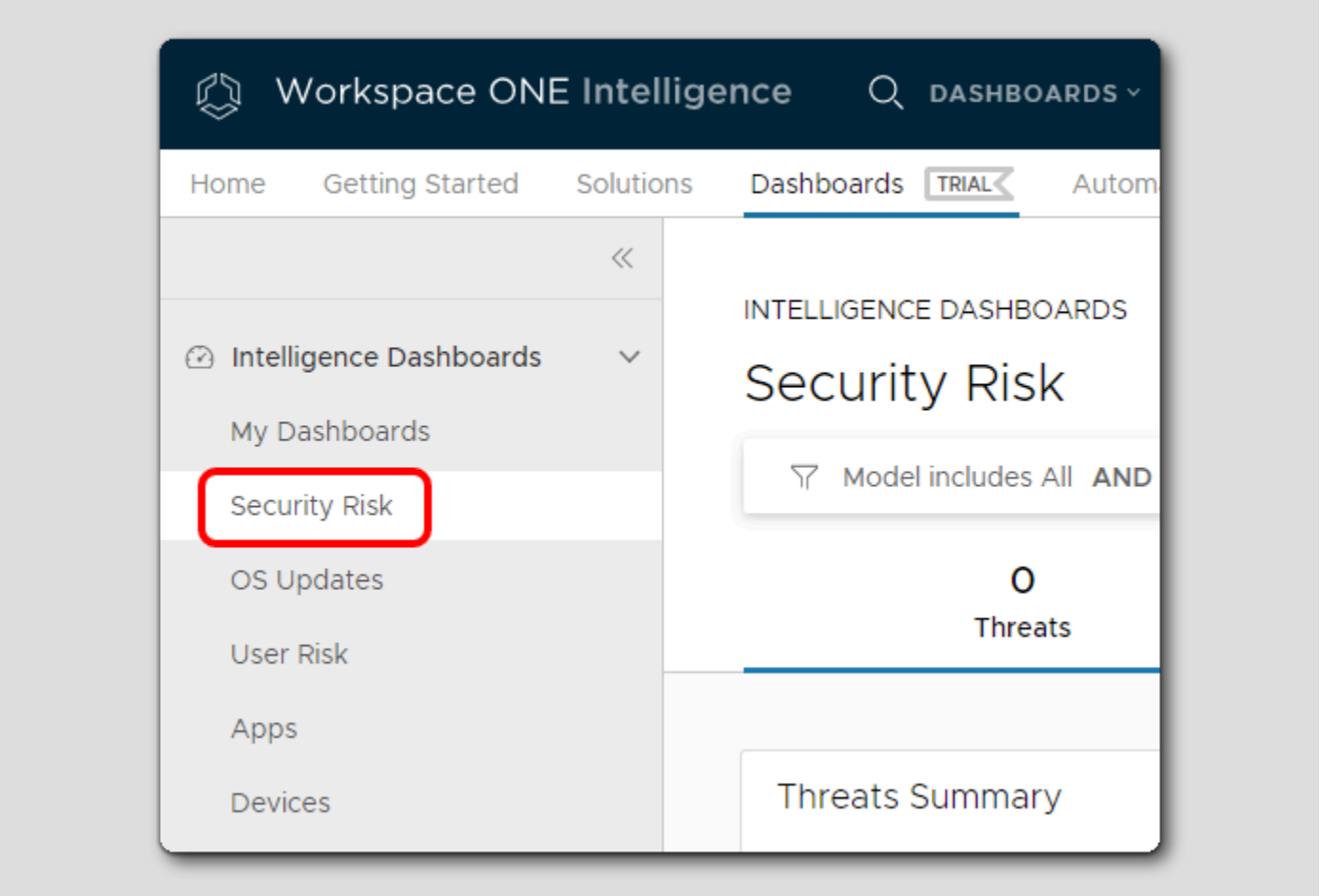
デバイス間のコンプライアンスの強化

[634]

Workspace ONE Intelligence のセキュリティ リスク ダッシュボードでは、さまざまなデバイス状態に関するレポートを収集し、ハイリスクのデバイスをすばやく特定できます。このアクティビティでは、次の Workspace ONE Intelligence セキュリティ リスク ダッシュボードを検討します：Threats Summary、Compromised Devices、Policy Risks、Vulnerabilities。

セキュリティ リスク ダッシュボードへのアクセス

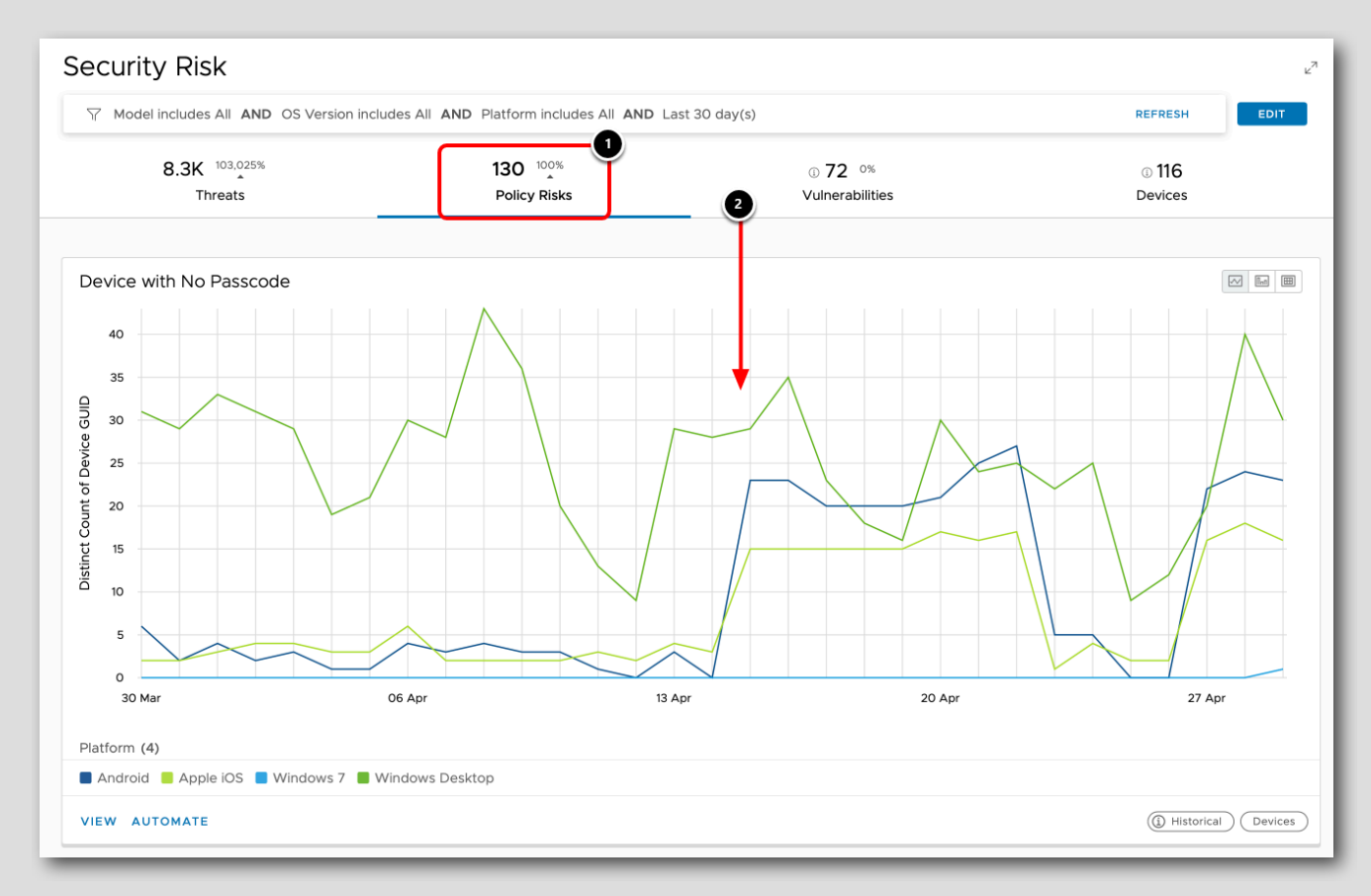
[635]



Workspace ONE Intelligence コンソールの [Dashboards] で、[Security Risk] をクリックします。

パスコードなしのデバイスの特定

[636]

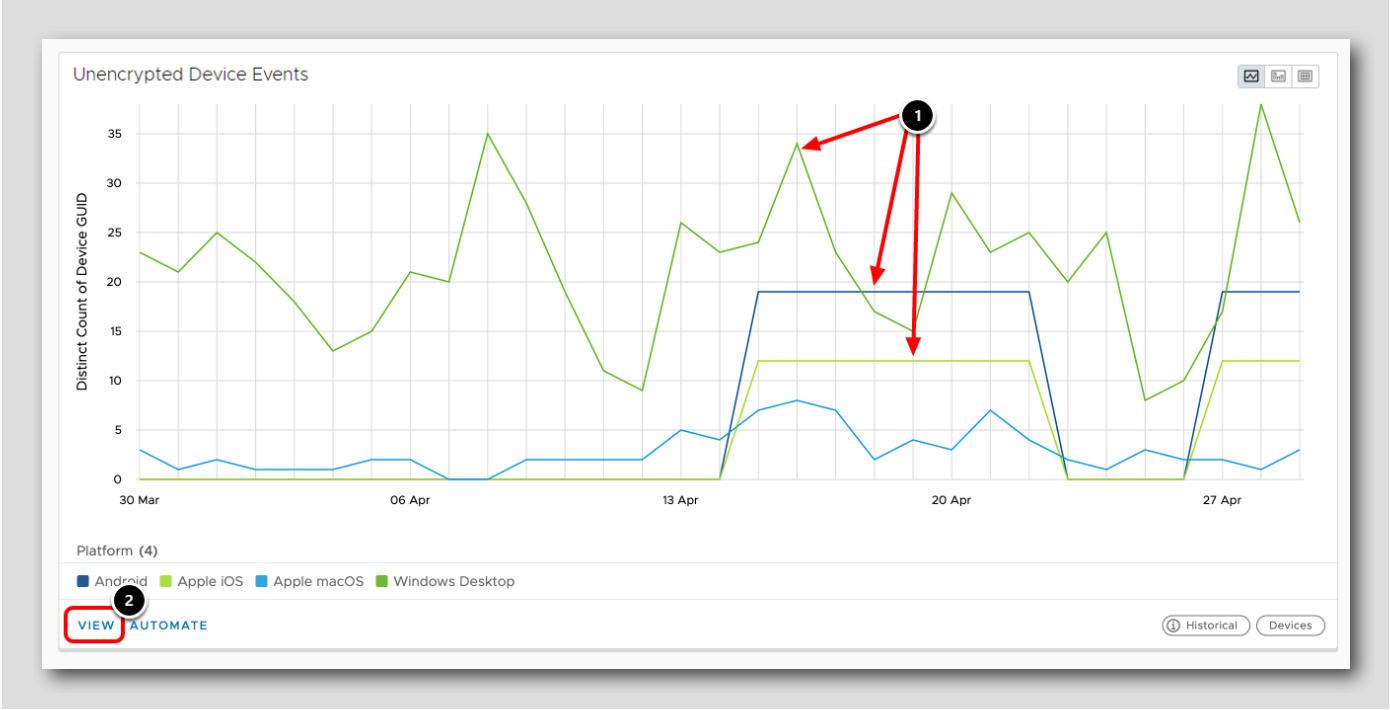


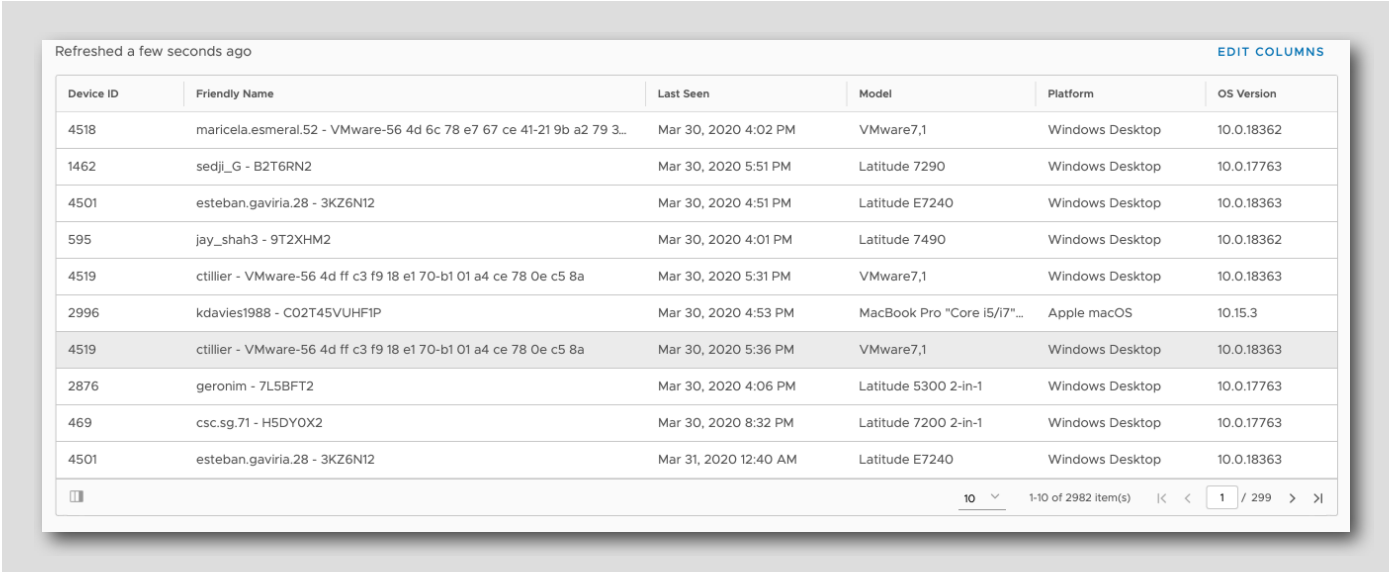
注：スクリーンショットはデモ環境から取得されたため、実際のビューは上記の例と一致することはありません。

1. [Policy Risks] タブを選択すると、過去 30 日間に検出されたパスコードなしのデバイスの数が表示されます。
   次に、問題の範囲を理解したら、自動化を使用してリスクを軽減します。たとえば、パスコードなしのデバイスを自動的に移動して隔離するか、そのデバイスから企業データへのアクセスを削除するルールを作成できます。
2. 下にスクロールします。

暗号化されていないデバイスの特定

[637]



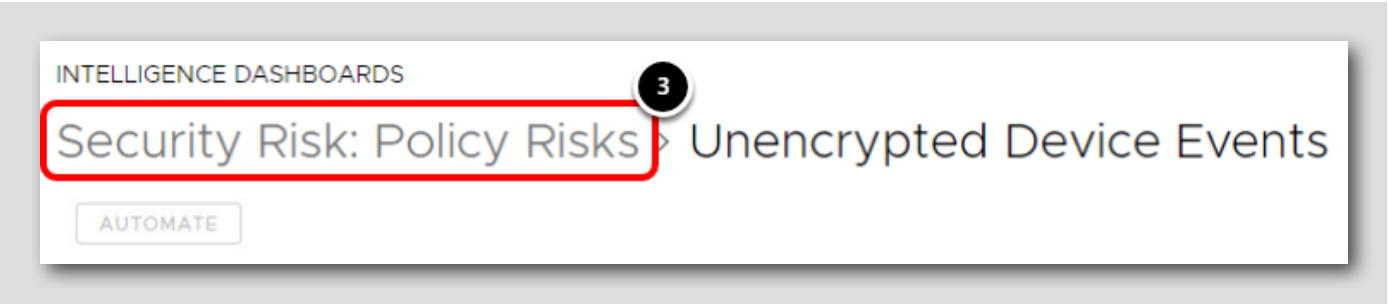


Refreshed a few seconds ago

EDIT COLUMNS

Device ID	Friendly Name	Last Seen	Model	Platform	OS Version
4518	maricela.esmeral.52 - VMware-56 4d 6c 78 e7 67 ce 41-21 9b a2 79 3...	Mar 30, 2020 4:02 PM	VMware7,1	Windows Desktop	10.0.18362
1462	sedji_G - B2T6RN2	Mar 30, 2020 5:51 PM	Latitude 7290	Windows Desktop	10.0.17763
4501	esteban.gaviria.28 - 3KZ6N12	Mar 30, 2020 4:51 PM	Latitude E7240	Windows Desktop	10.0.18363
595	jay_shah3 - 9T2XHM2	Mar 30, 2020 4:01 PM	Latitude 7490	Windows Desktop	10.0.18362
4519	ctillier - VMware-56 4d ff c3 f9 18 e1 70-b1 01 a4 ce 78 0e c5 8a	Mar 30, 2020 5:31 PM	VMware7,1	Windows Desktop	10.0.18363
2996	kdavies1988 - C02T45VUHF1P	Mar 30, 2020 4:53 PM	MacBook Pro "Core i5/i7"...	Apple macOS	10.15.3
4519	ctillier - VMware-56 4d ff c3 f9 18 e1 70-b1 01 a4 ce 78 0e c5 8a	Mar 30, 2020 5:36 PM	VMware7,1	Windows Desktop	10.0.18363
2876	geronim - 7L5BFT2	Mar 30, 2020 4:06 PM	Latitude 5300 2-in-1	Windows Desktop	10.0.17763
469	csc.sg.71 - H5DY0X2	Mar 30, 2020 8:32 PM	Latitude 7200 2-in-1	Windows Desktop	10.0.17763
4501	esteban.gaviria.28 - 3KZ6N12	Mar 31, 2020 12:40 AM	Latitude E7240	Windows Desktop	10.0.18363

10 1-10 of 2982 item(s) 1 / 299



注：スクリーンショットはデモ環境から取得されたため、実際のビューは上記の例と一致することはありません。

下にスクロールして、[Unencrypted Device Events] ダッシュボードを見つけます。このチャートは、Workspace ONE Intelligence によって日単位で特定された、暗号化されていないデバイスの合計数を示しています。

1. プラットフォームごとのデバイス数の詳細については、データ ポイントの上にカーソルを合わせます。
2. [View] をクリックして、デバイスの詳細なリストを取得します。
3. [Security Risk: Policy Risks] をクリックして戻ります。

脆弱なデバイスの特定

[638]

注：スクリーンショットはデモ環境から取得されたため、実際のビューは上記の例と一致することはありません。

[Vulnerabilities] タブを選択して、過去 30 日間に特定された脆弱なデバイスの数を表示します。

暗号化しない場合、機密情報は保護されず、悪意のある人が簡単に手に入れることができます。このリスクを軽減するには、ポリシーを作成してデバイスの暗号化を強制します。たとえば、デバイスが Workspace ONE UEM 経由で暗号化されるまで企業へのアクセスをブロックするポリシーを作成できます。

Workspace ONE Intelligence Automation Connector の構成

[639]

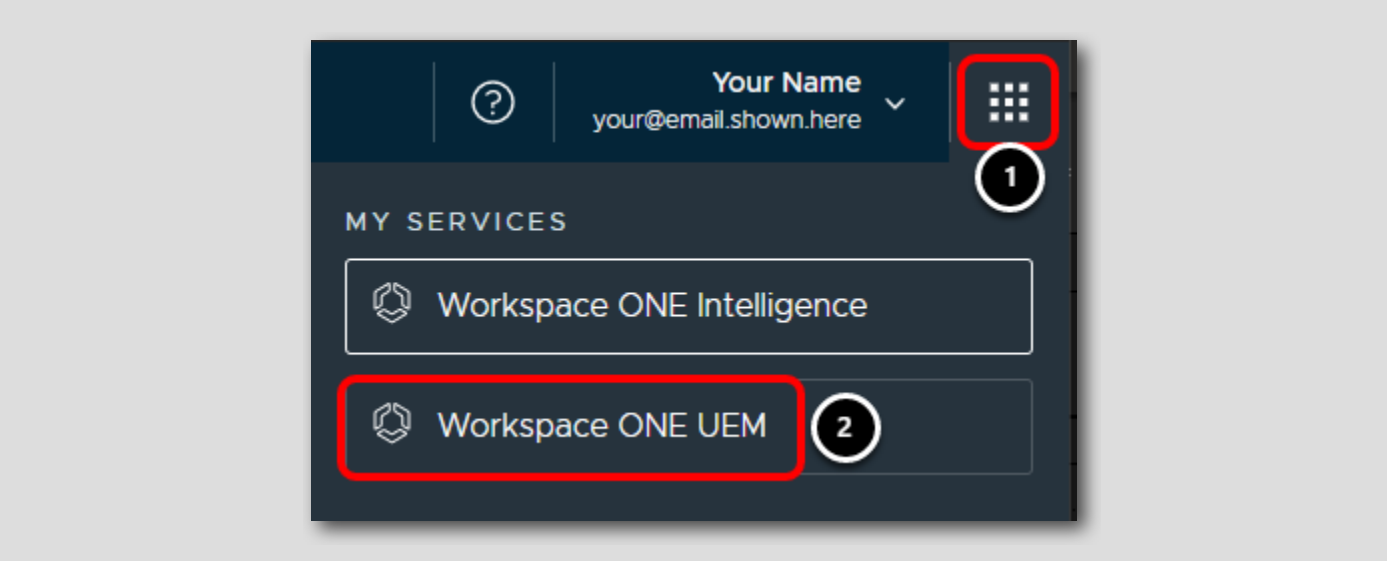
Workspace ONE Intelligence を最大限に活用するには、少なくとも 1 つの Automation Connector を構成して、環境内で自動化アクションを有効にする必要があります。

利用可能なコネクタの中で重要なのが、Workspace ONE UEM Connector です。これにより、Intelligence Automation は、組織のデバイス、アプリケーション、デバイス センサー、および OS の更新に対してアクションを実行できます。

このアクティビティでは、Workspace ONE Intelligence と Workspace ONE UEM 間の API 通信を許可するように Workspace ONE UEM Connector を構成します。

Workspace ONE UEM Console への切り替え

[640]

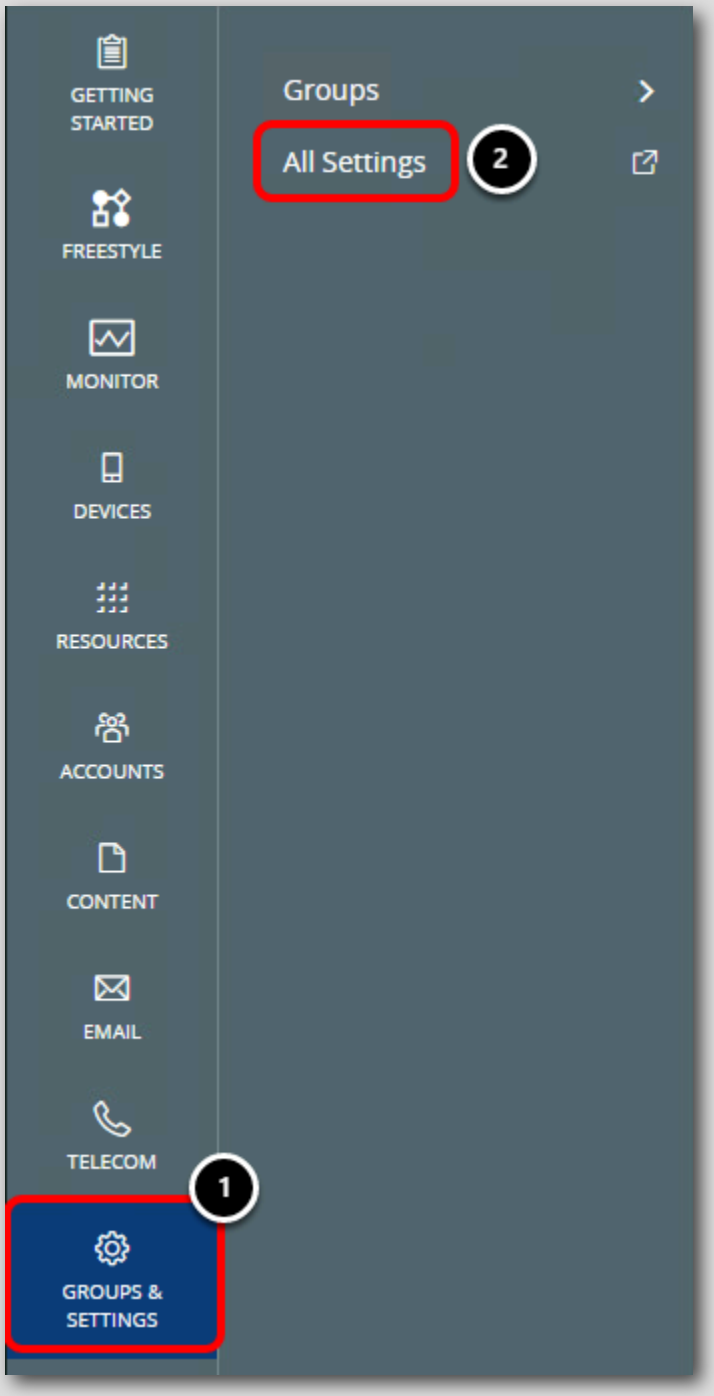


Workspace ONE Intelligence コンソールで、次のように操作します。

1. [Services] メニュー アイコンをクリックします。
2. [Workspace ONE UEM] を選択します。

[All Settings] への移動

[641]

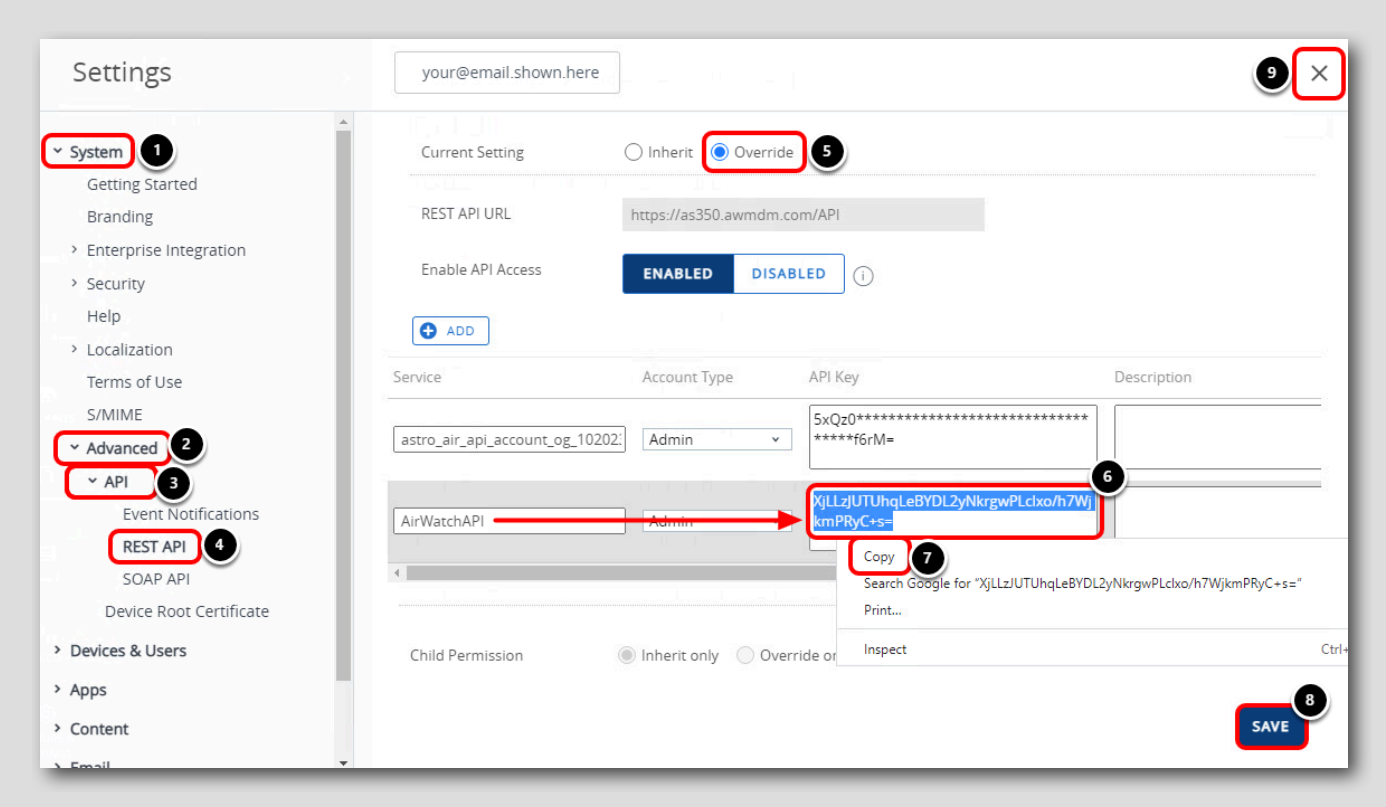


Workspace ONE UEM 管理者コンソールで次のように操作します。

1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

API キーの再生成

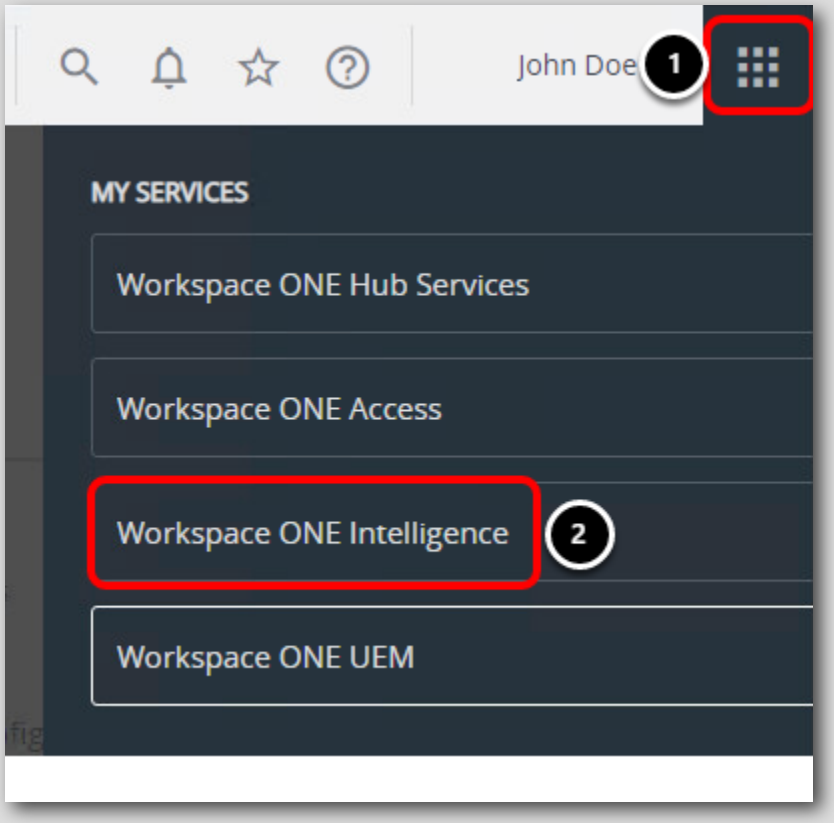
[642]



1. [System] をクリックします。
2. [Advanced] をクリックします。
3. [API] をクリックします。
4. [REST API] をクリックします。
5. [Override] をクリックして、Workspace ONE Intelligence との統合に使用する新しい API キーを生成します。
6. [AirWatchAPI Service] に対して、[API Key] フィールドの内容をすべて選択して**右クリック**します。
7. [Copy] をクリックして、次の手順に備えて API キーを保存します。
8. [Save] をクリックします。
9. [Close] をクリックします。

Workspace ONE Intelligence コンソールに戻る

[643]

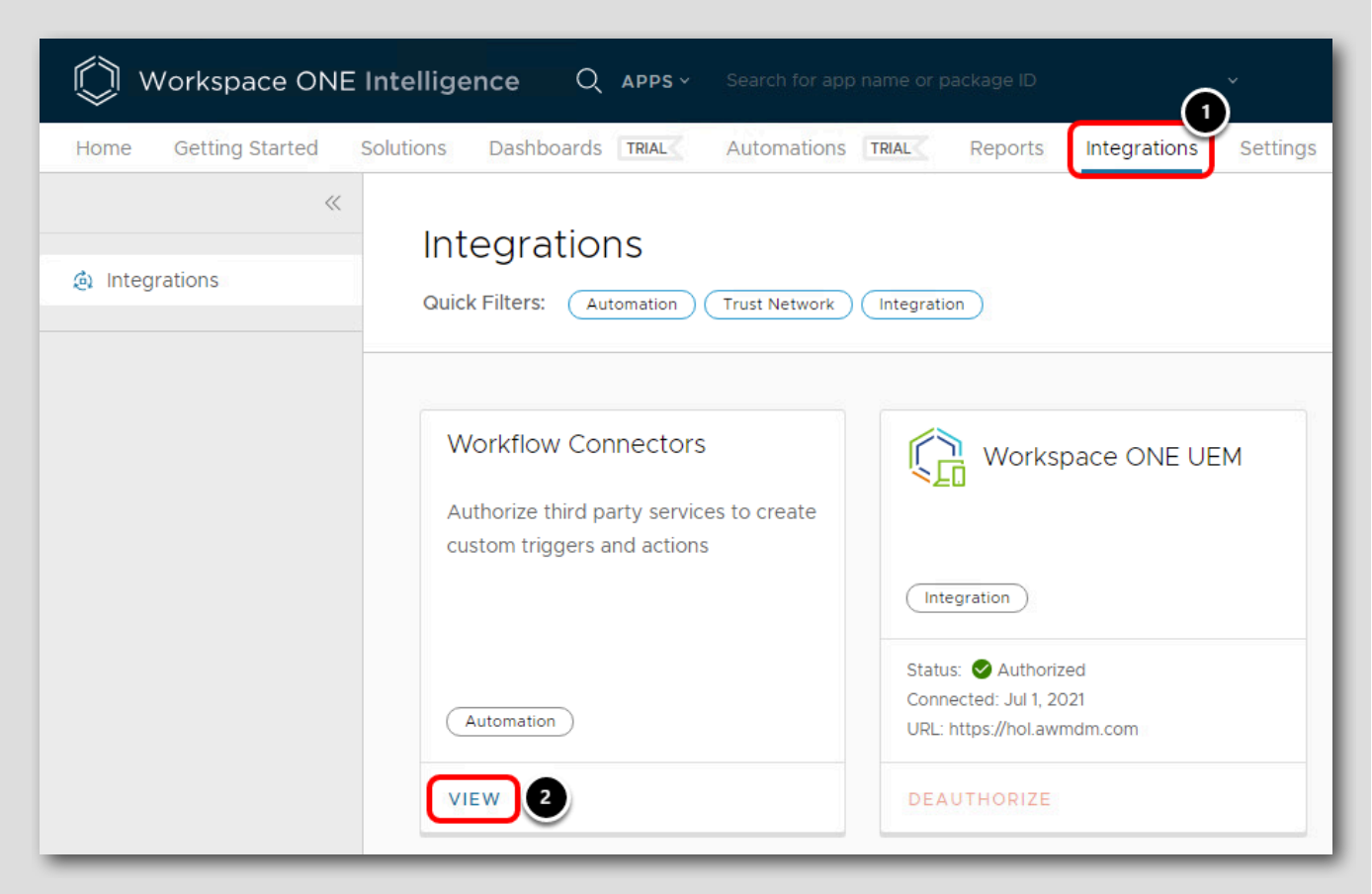


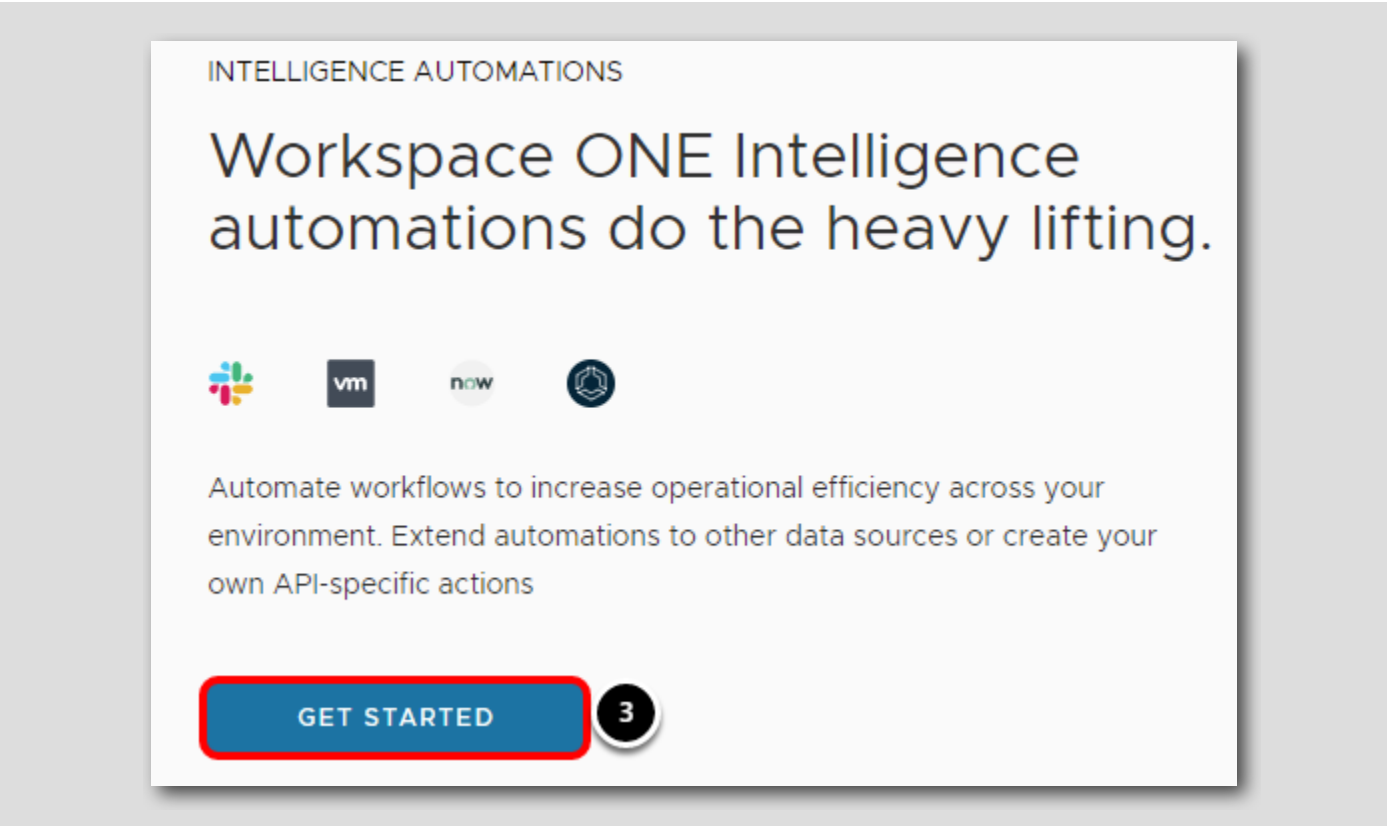
Workspace ONE UEM 管理者コンソールから、次のように操作します。

1. [Services] メニュー アイコンをクリックします。
2. [Workspace ONE Intelligence] を選択します。

[Automation Connections] を開く

[644]

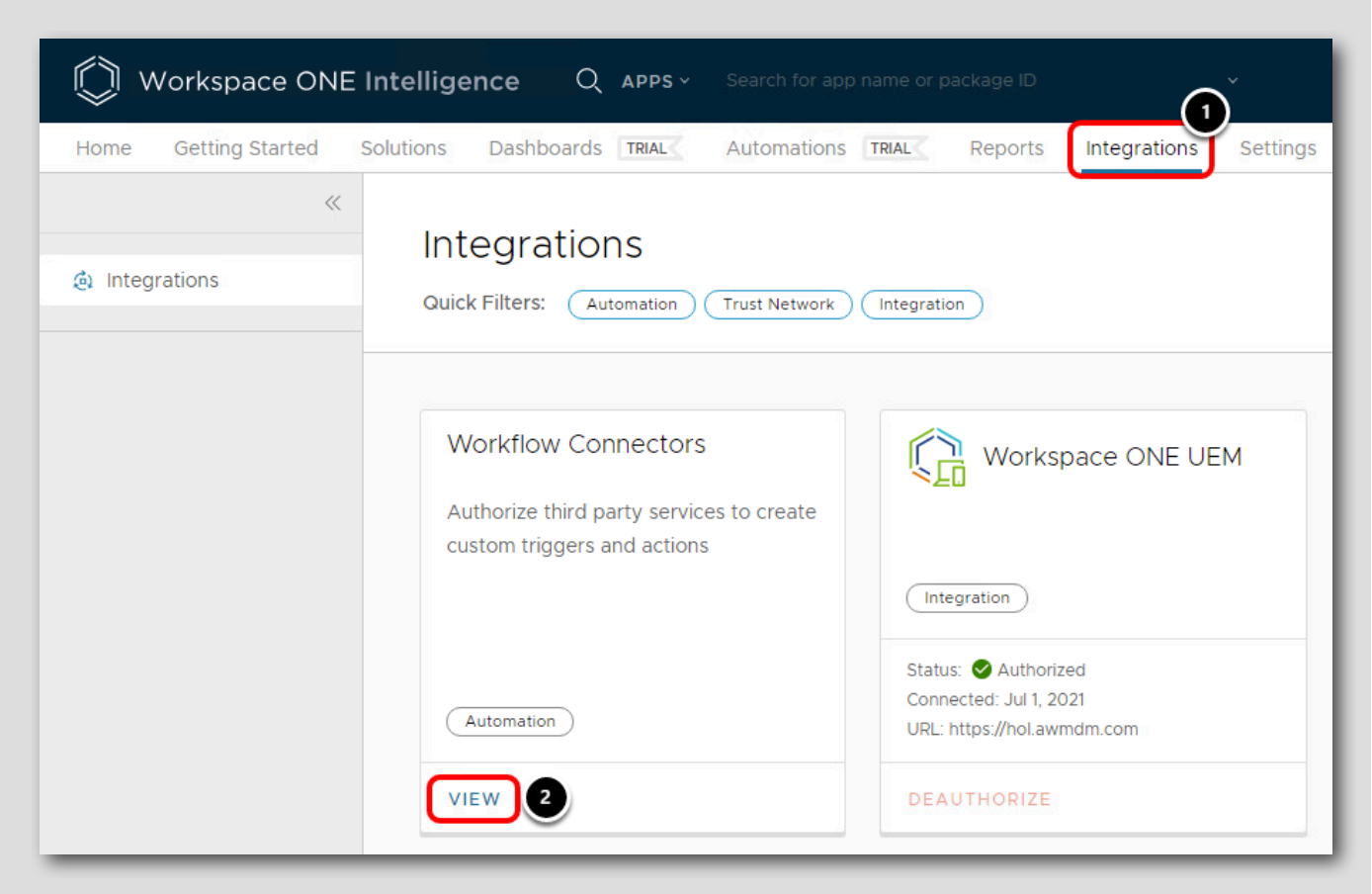


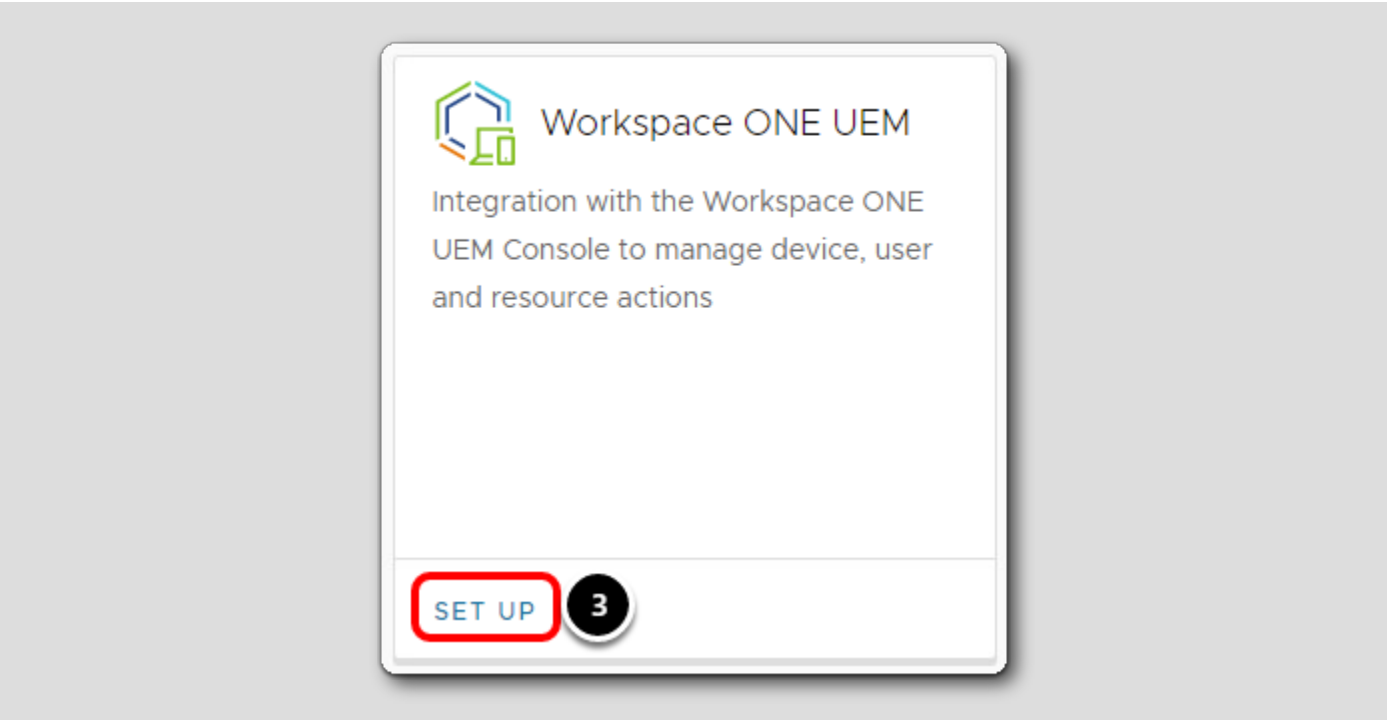


1. [Integrations] をクリックします。
2. [Workflow Connectors] で [View] をクリックします。
3. [Get Started] をクリックします。

Workspace ONE UEM 統合のセットアップ

[645]



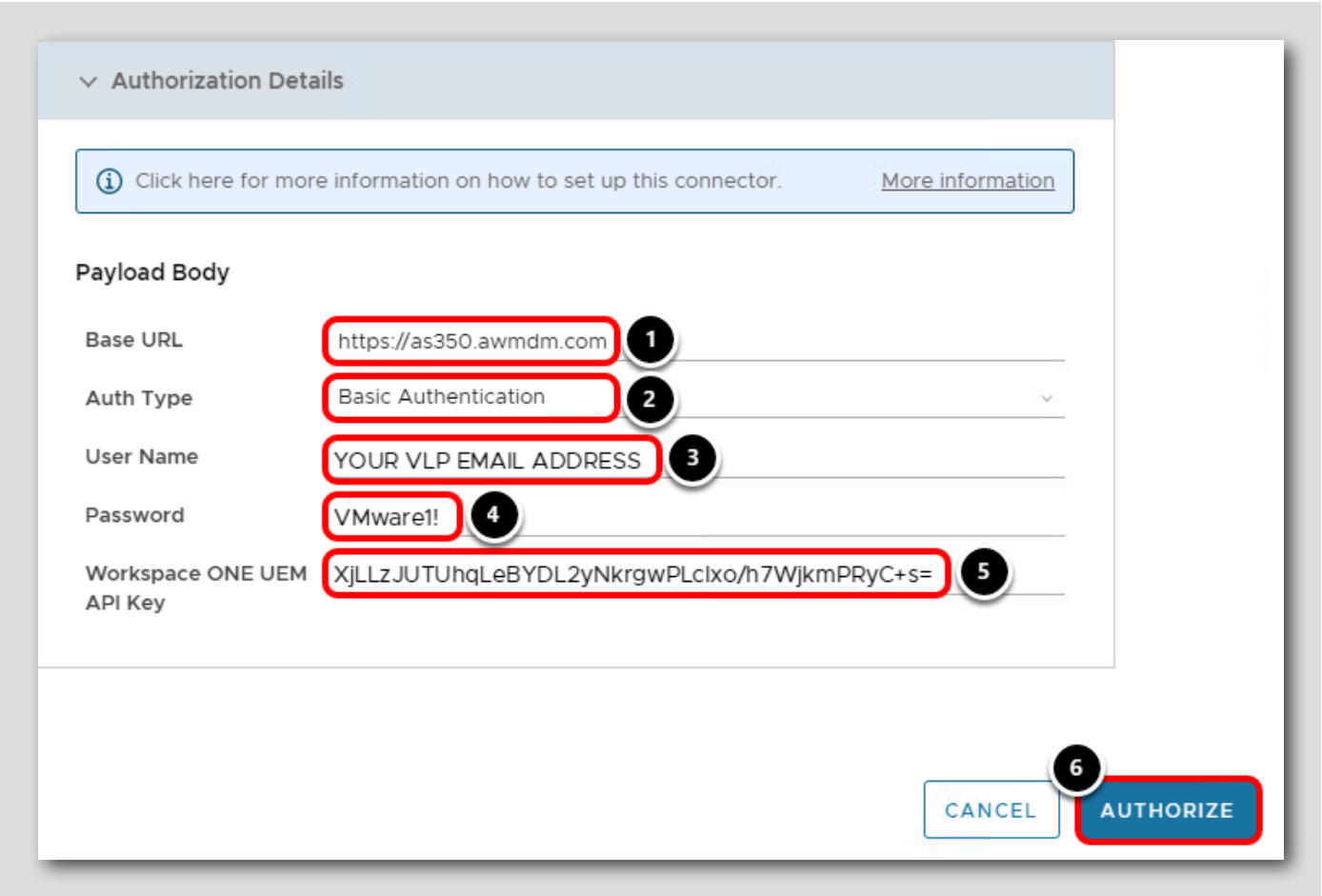


1. [Get Started] をクリックした後に [Integrations] タブから移動した場合は、**[Integrations]** タブをもう一度クリックします。
2. [Workflow Connections] カードで **[View]** をクリックします。
3. [Workspace ONE UEM] カードで **[Setup]** をクリックします。

[Workspace ONE UEM] カードで、**[Set Up]** をクリックします。

認証の構成

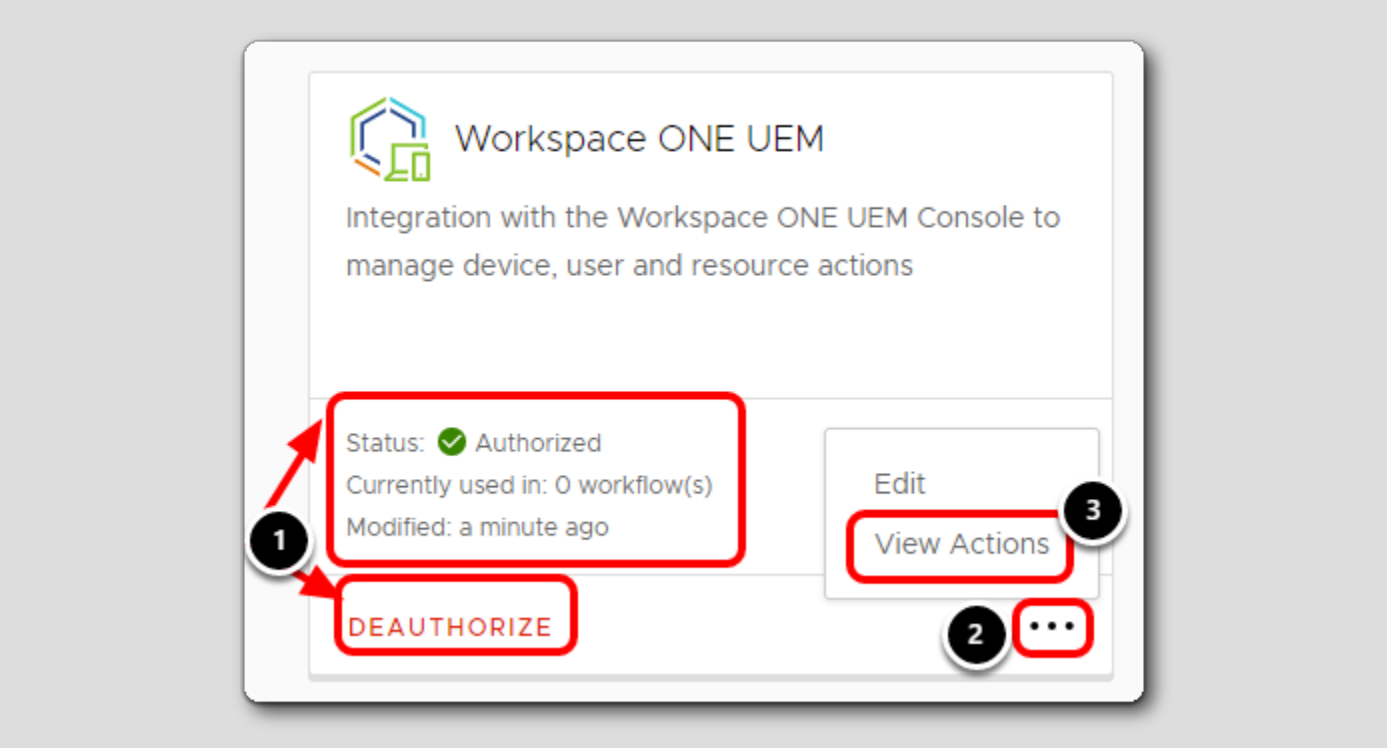
[646]



1. Workspace ONE UEM 環境のベース URL を入力します。この場合、**`https://as350.awmdm.com`** と入力します。
2. [Auth Type] で [Basic Authentication] を選択します。
3. 以前にコピーした REST API キーにアクセスできる Workspace ONE UEM 管理者の API ユーザー名を入力します。これは、Workspace ONE UEM Console へのログインに使用した VLP メール アドレスです。
4. API ユーザー パスワード **`VMware1!`** を入力します。
5. Workspace ONE UEM API キーを貼り付けます。これは、前のアクティビティで Workspace ONE UEM Console からコピーした AirWatchAPI サービス キーです。
6. [Authorize] をクリックします。

認証の検証

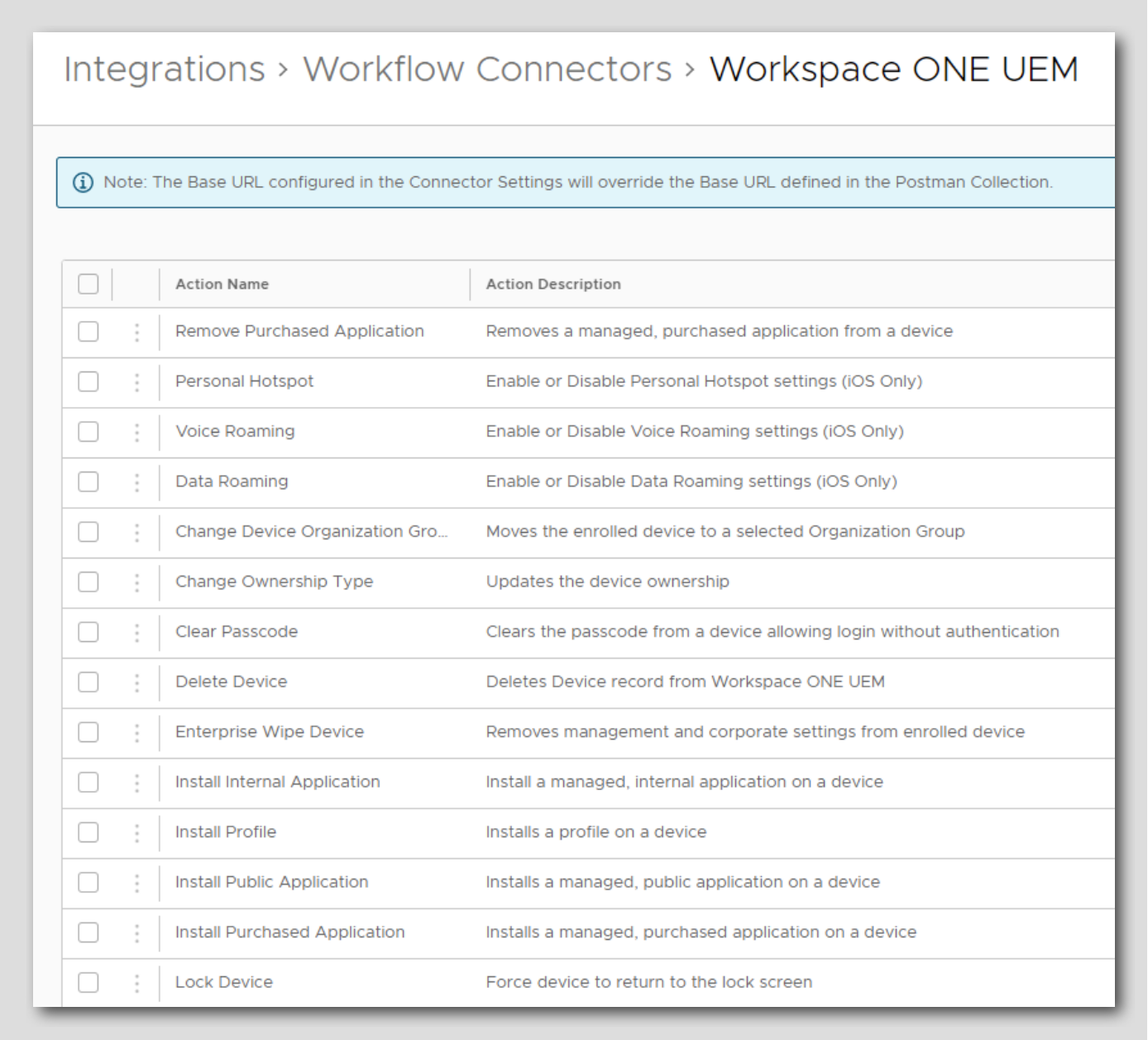
[647]



1. Workspace ONE UEM カードのステータスが [Authorized] と表示されるようになったことを確認し、カードのアクションが [Deauthorize] に変更されたことを確認します。これは統合が成功したことを示しています。
2. [...] ボタンをクリックします。
3. [View Actions] をクリックします。

Workspace ONE UEM に対する自動化アクションの確認

[648]



Action Name	Action Description
Remove Purchased Application	Removes a managed, purchased application from a device
Personal Hotspot	Enable or Disable Personal Hotspot settings (iOS Only)
Voice Roaming	Enable or Disable Voice Roaming settings (iOS Only)
Data Roaming	Enable or Disable Data Roaming settings (iOS Only)
Change Device Organization Gro...	Moves the enrolled device to a selected Organization Group
Change Ownership Type	Updates the device ownership
Clear Passcode	Clears the passcode from a device allowing login without authentication
Delete Device	Deletes Device record from Workspace ONE UEM
Enterprise Wipe Device	Removes management and corporate settings from enrolled device
Install Internal Application	Install a managed, internal application on a device
Install Profile	Installs a profile on a device
Install Public Application	Installs a managed, public application on a device
Install Purchased Application	Installs a managed, purchased application on a device
Lock Device	Force device to return to the lock screen

これで、自動化されたフローを定義できるようになりました。これにより、デバイス、アプリケーション、OS の更新に対して、25 以上の異なるアクションを実行できます。このスクリーンショットは、デバイスに対して使用できるアクションの一部を示しています。

次の手順に進んでください。

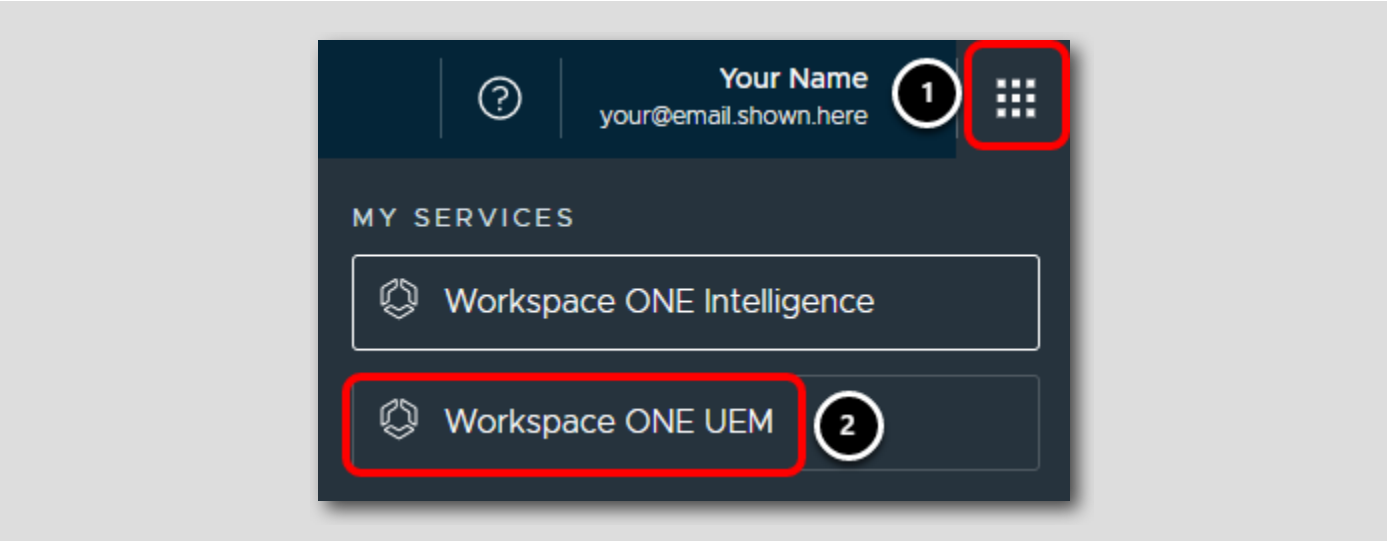
自動化を使用して、バッテリ残量低下状態のデバイスにタグを付ける

[649]

このアクティビティでは、Workspace ONE Intelligence の自動化機能を使用して、Workspace ONE UEM のバッテリ残量低下状態のデバイスにタグを付けます。

Workspace ONE UEM Console に戻る

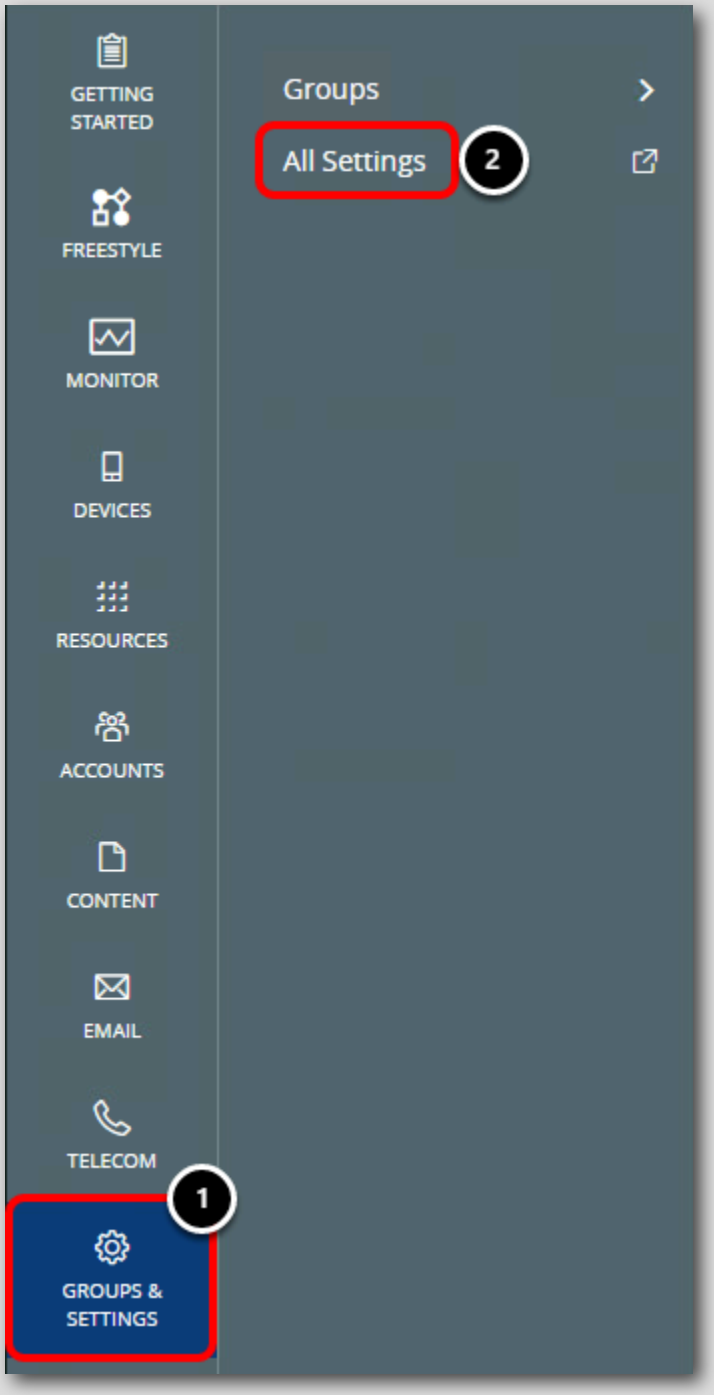
[650]



Workspace ONE Intelligence コンソールで、次のように操作します。

1. [Services] メニューをクリックします。
2. [Workspace ONE UEM] をクリックします。

Workspace ONE UEM Console の [All Settings] への移動 [651]

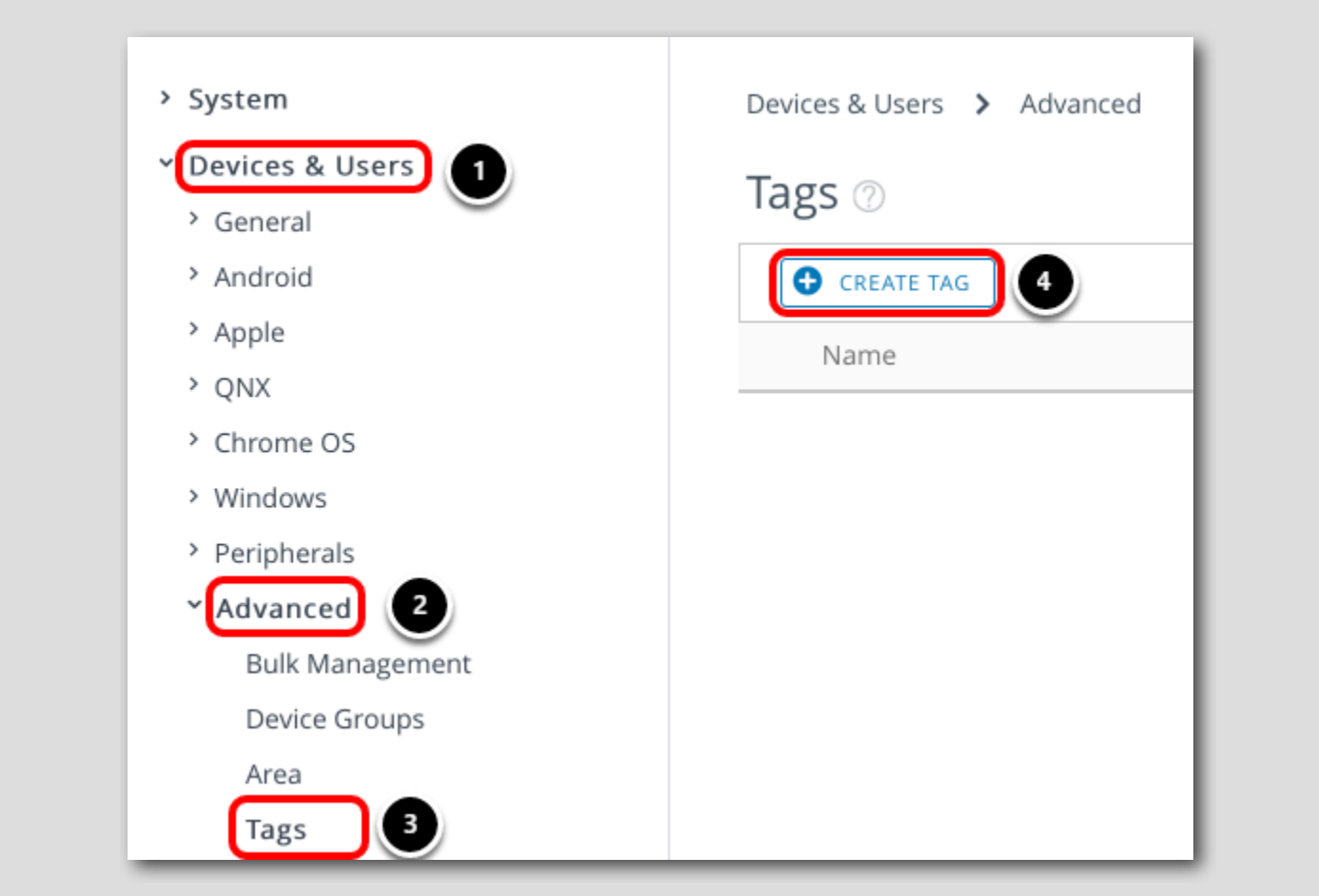


Workspace ONE UEM Console で、次のように操作します。

1. [Groups & Settings] をクリックします。
2. [All Settings] をクリックします。

「Low Battery Health」タグの作成

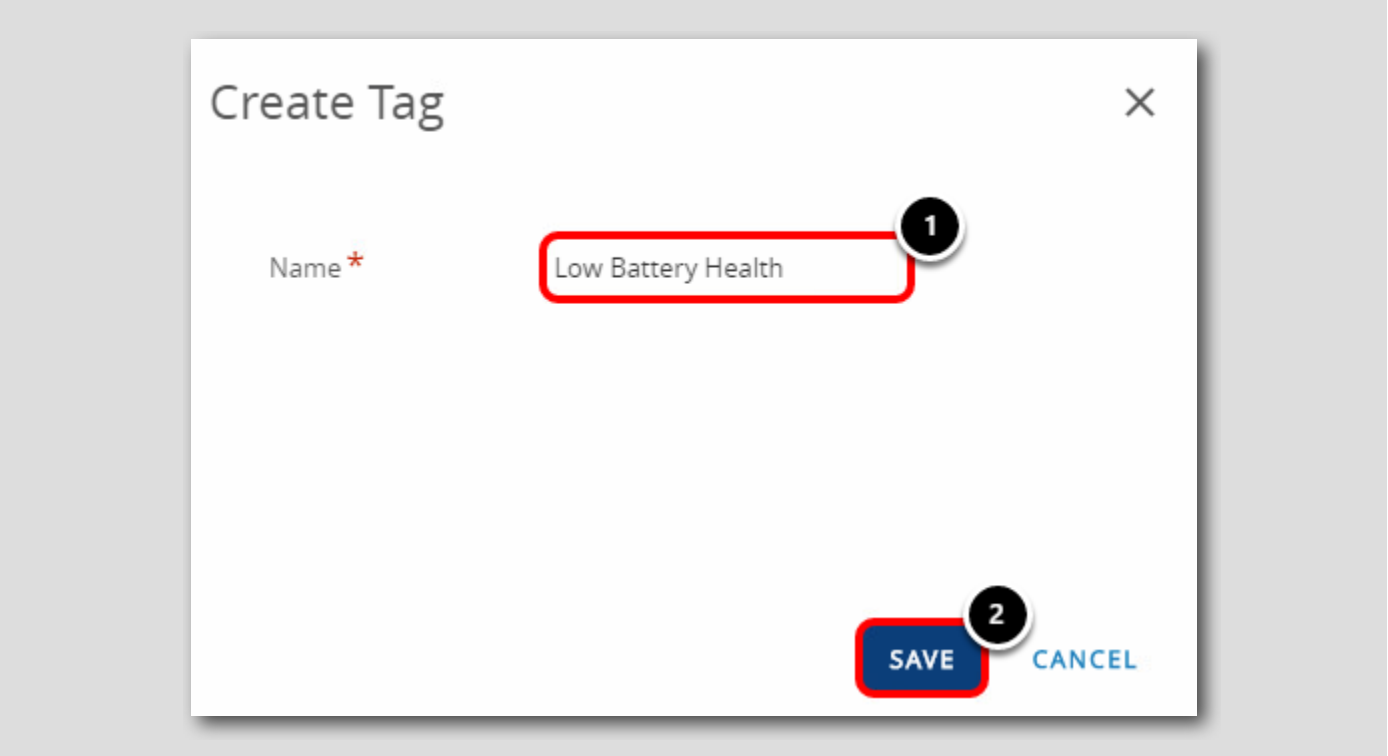
[652]



1. [Device & Users] をクリックします。
2. [Advanced] をクリックします。
3. [Tags] をクリックします。
4. [Create Tag] をクリックします。

「Low Battery Health」タグの保存

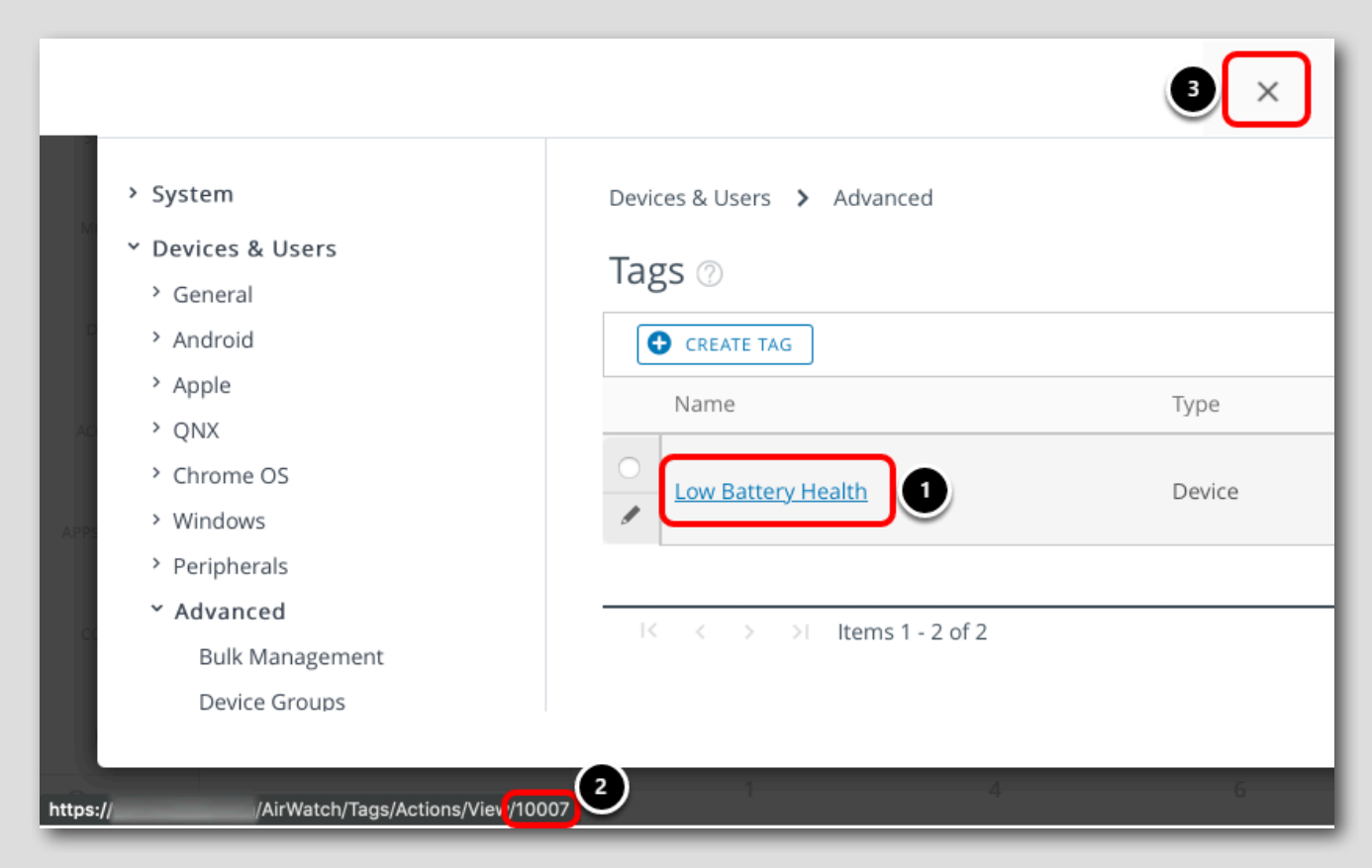
[653]



1. [Tag Name] に **`Low Battery Health`** と入力します。
2. [Save] をクリックします。

タグ ID の取得

[654]

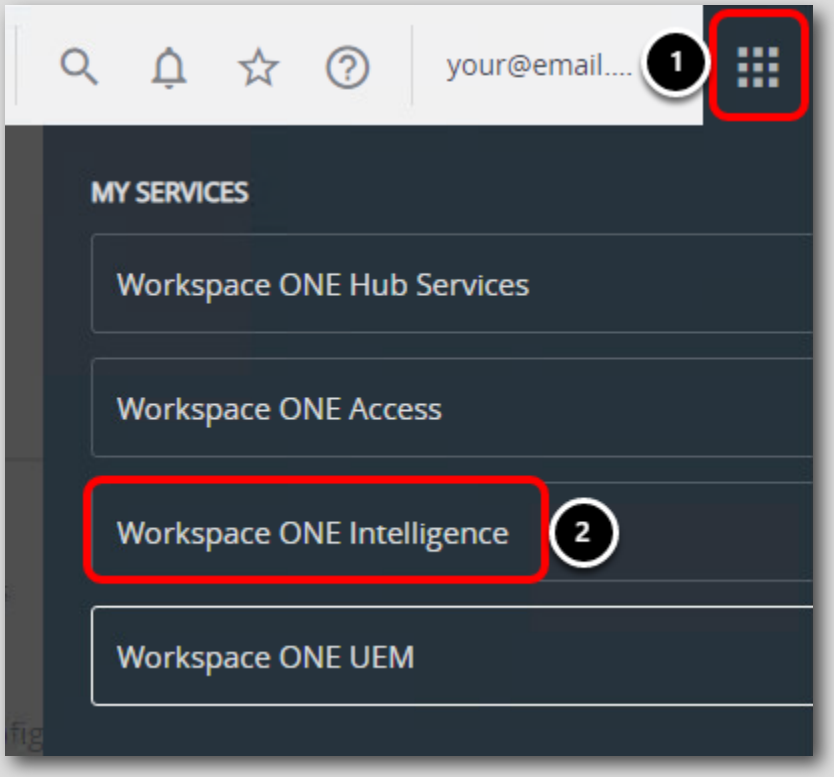


1. 作成した [Low Battery Health] タグの上にカーソルを合わせます。
2. タグの URL はブラウザのステータス バーに表示されます。タグ ID は、URL の末尾の番号です。この番号をメモ帳に手動で入力するか、どこか参照できる場所にコピーします。このタグ ID は、以降の手順で自動化アクションの一部として使用されます。
3. [Close] をクリックします。

注：サンプル イメージでは、タグ ID は **10007** です。ID は異なります。

Workspace ONE Intelligence コンソールに戻る

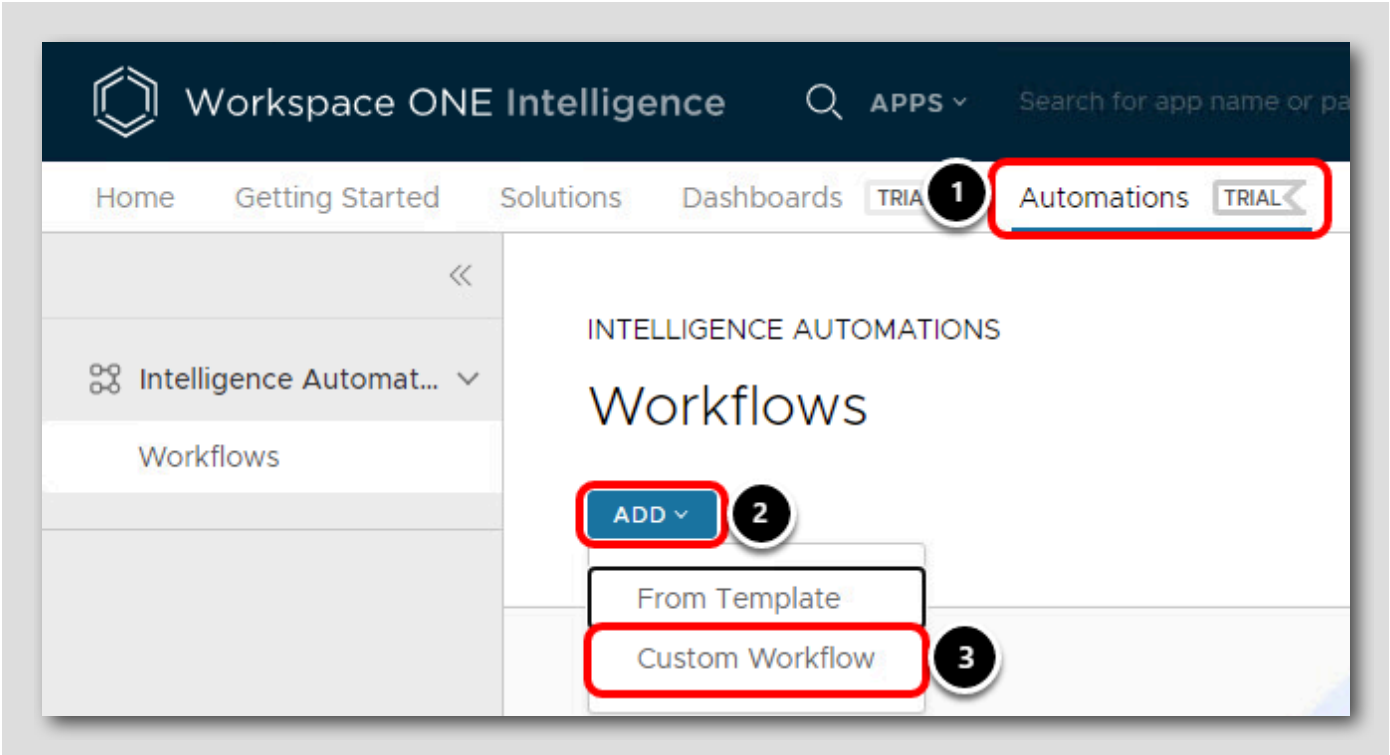
[655]



1. [My Services] ボタンをクリックします。
2. [Workspace ONE Intelligence] をクリックします。

自動化設定を開く

[656]

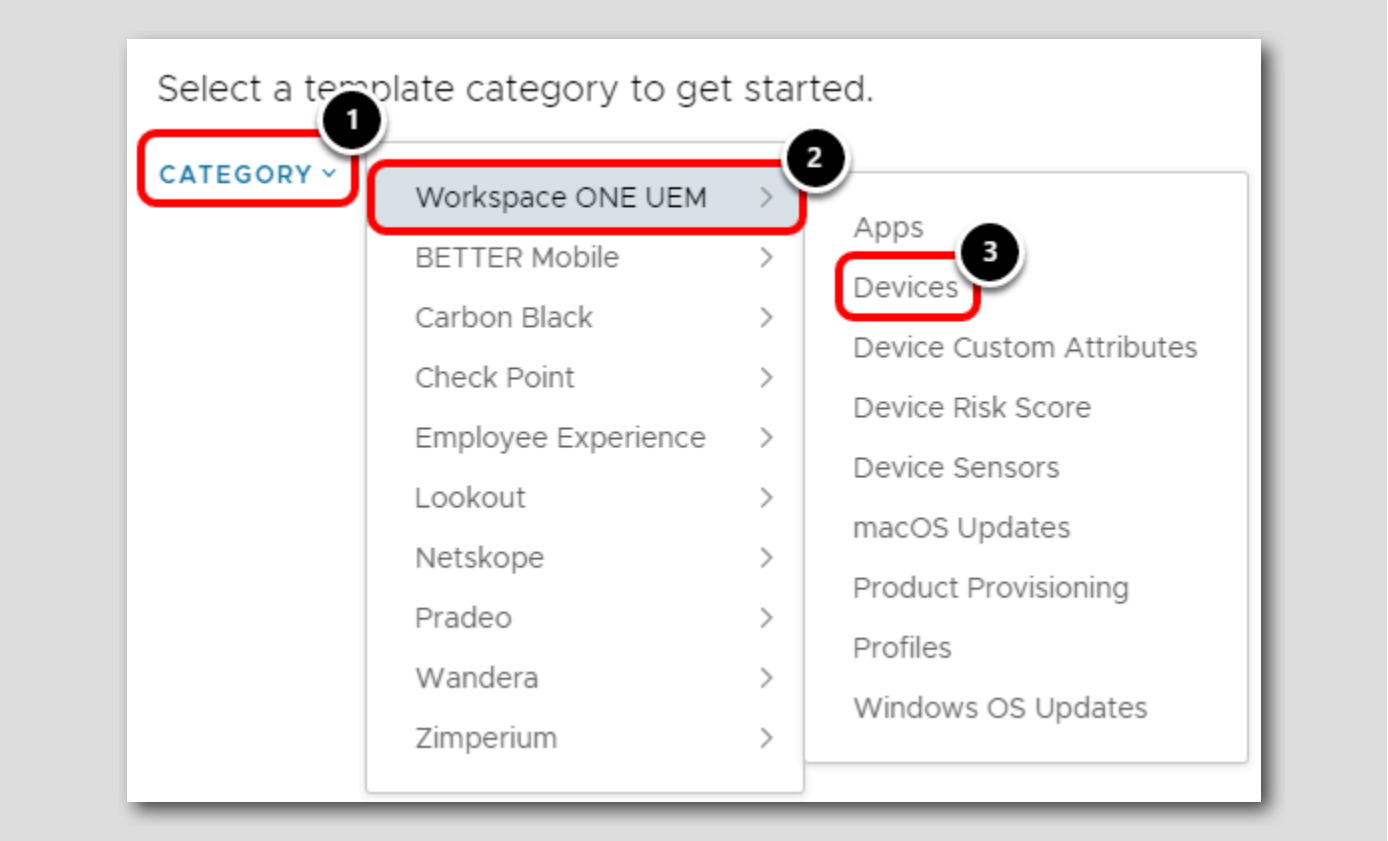


Workspace ONE Intelligence コンソールで、次のように操作します。

1. [Automations] タブをクリックします。
2. [Add] をクリックします。
3. [Custom Workflow] をクリックします。

テンプレートの選択

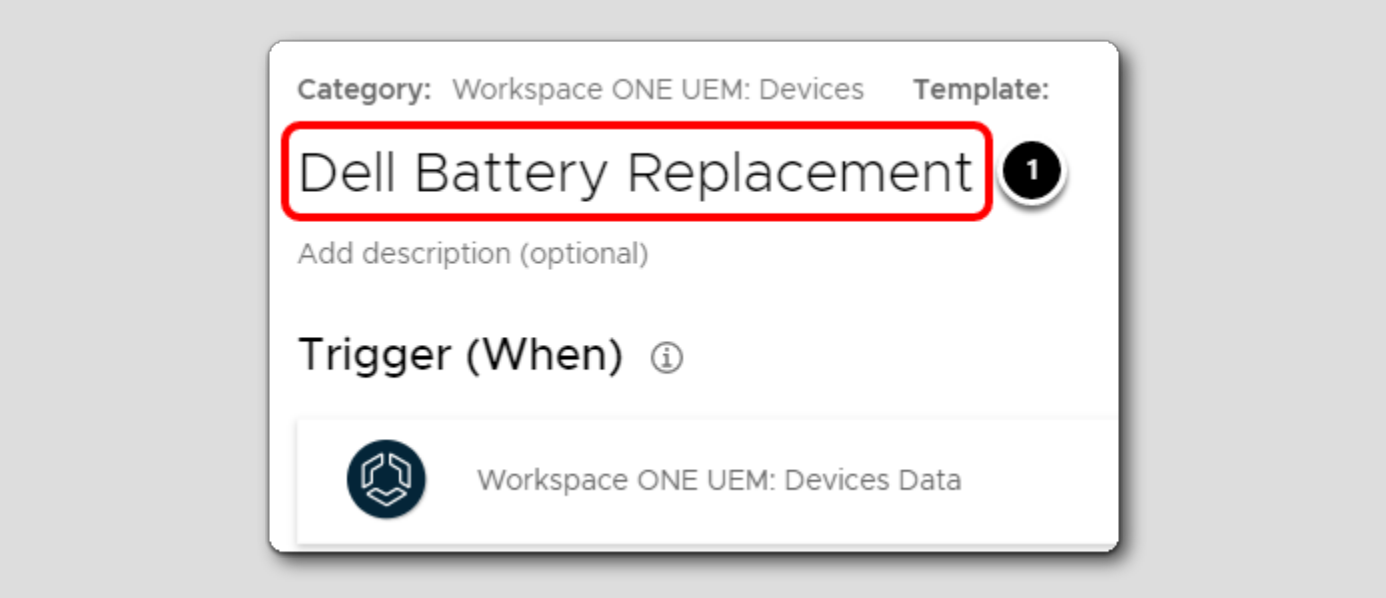
[657]



1. [Category] に移動します。
2. Workspace ONE UEM に移動します。
3. [Devices] をクリックします。

自動化設定の定義

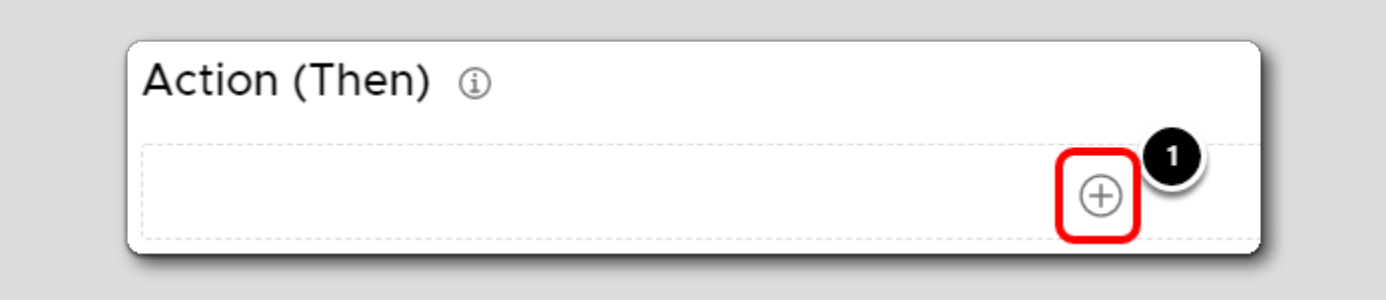
[658]

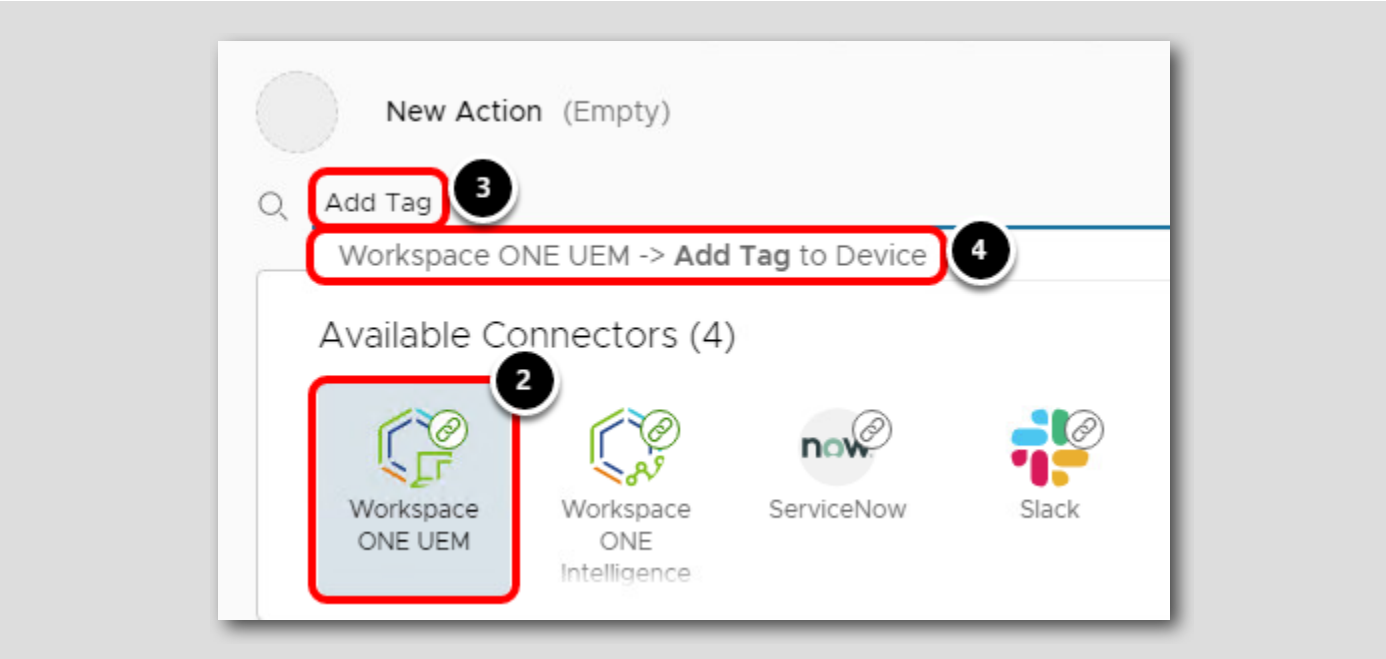


1. [Name] フィールドに **`Dell Battery Replacement`** と入力します。
2. [Filter (If)] で、[Dell Battery Health] を選択します。
3. [Less Than] を選択します。
4. **25** と入力します。

アクションの追加

[659]

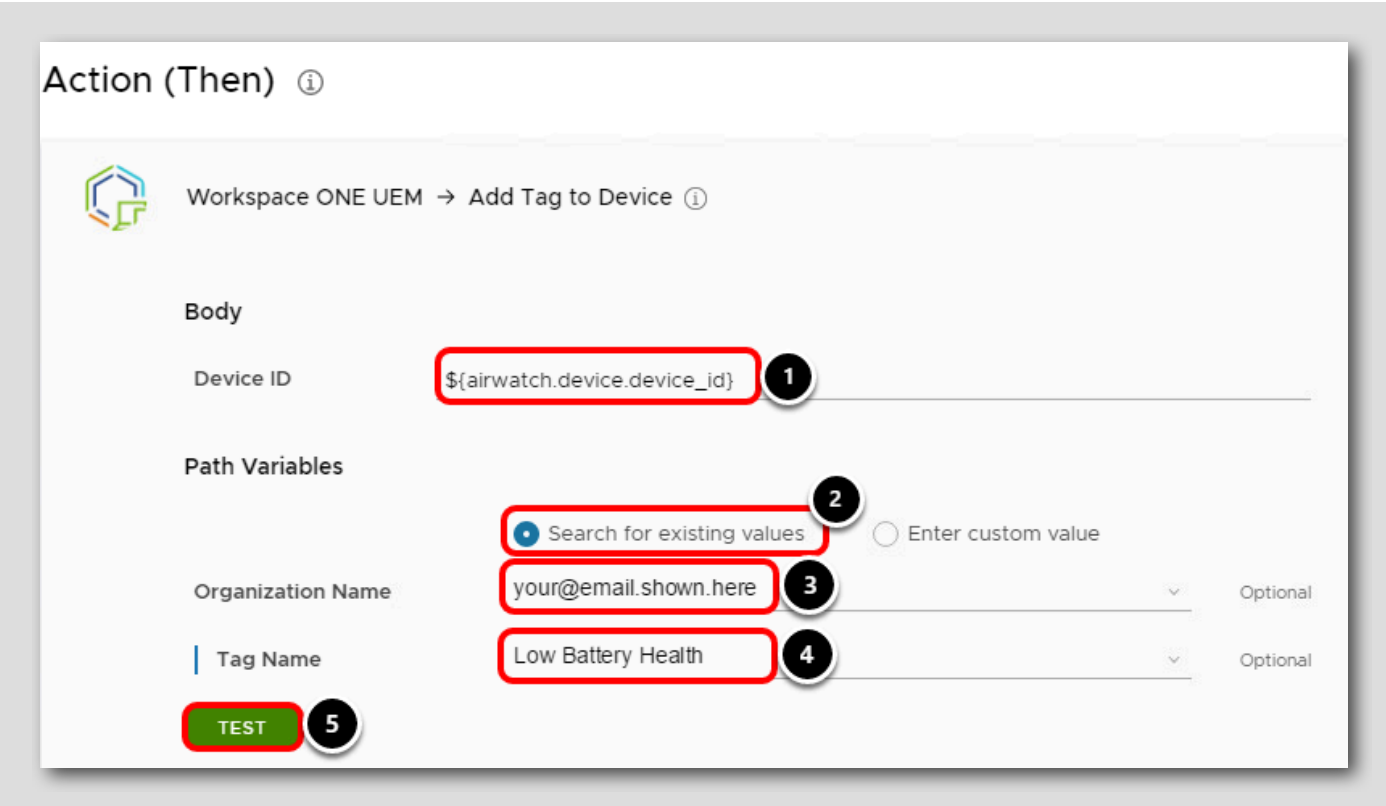




1. [Action (Then)] セクションで、[+] アイコンをクリックしてオプションを展開します。
2. [Workspace ONE UEM] をクリックします。
3. 検索フィールドに **Add tag** と入力します。
4. [Workspace ONE UEM -> Add Tag to Device] 結果を選択します。

アクション設定の構成

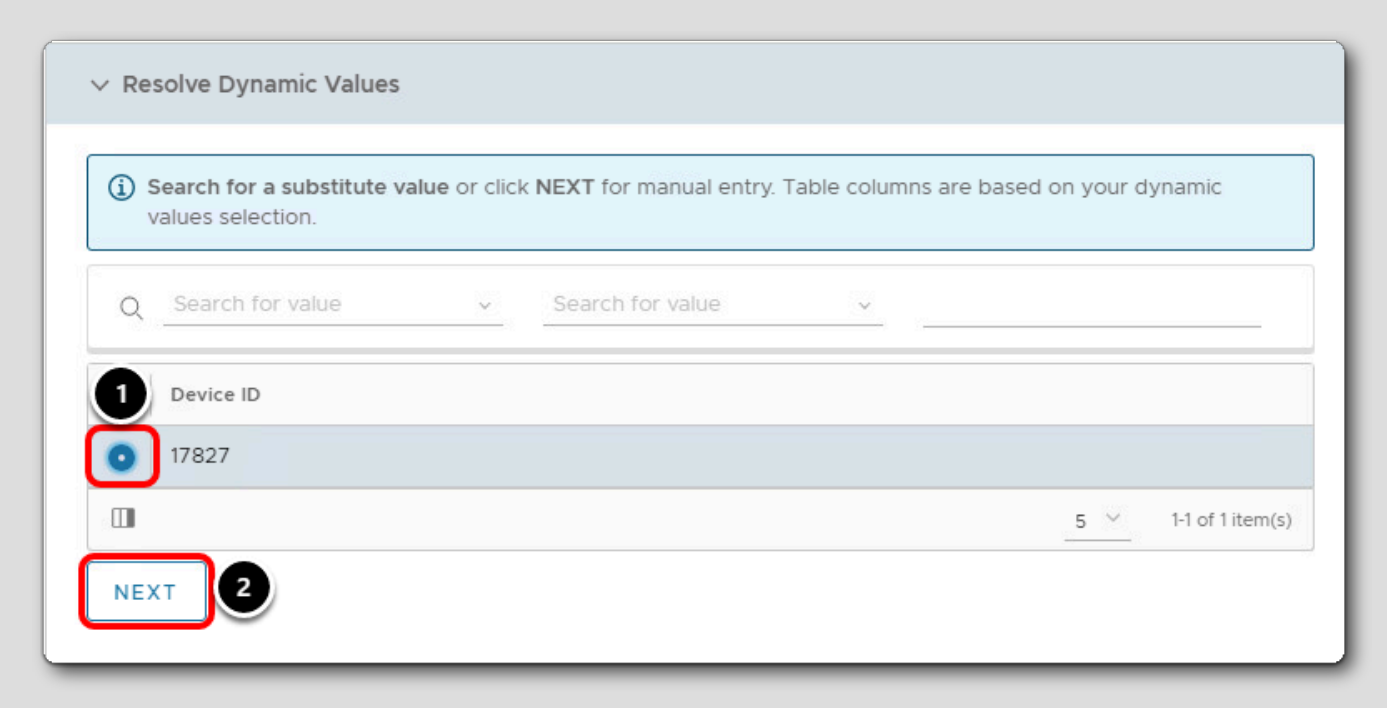
[660]



1. [Device ID] フィールドは **`${device_id}`** のままにします。
2. [Path Variables] の選択を [Search for existing values] に変更します。
3. [Organization Name] フィールドをクリックし、リストから組織名を選択します。グループの組織名はメール アドレスと一致します。
4. [Tag Name] フィールドをクリックし、リストから [Low Battery Health] タグを選択します。
5. [Test] をクリックします。

[Add Tag to Device] 自動化のテスト

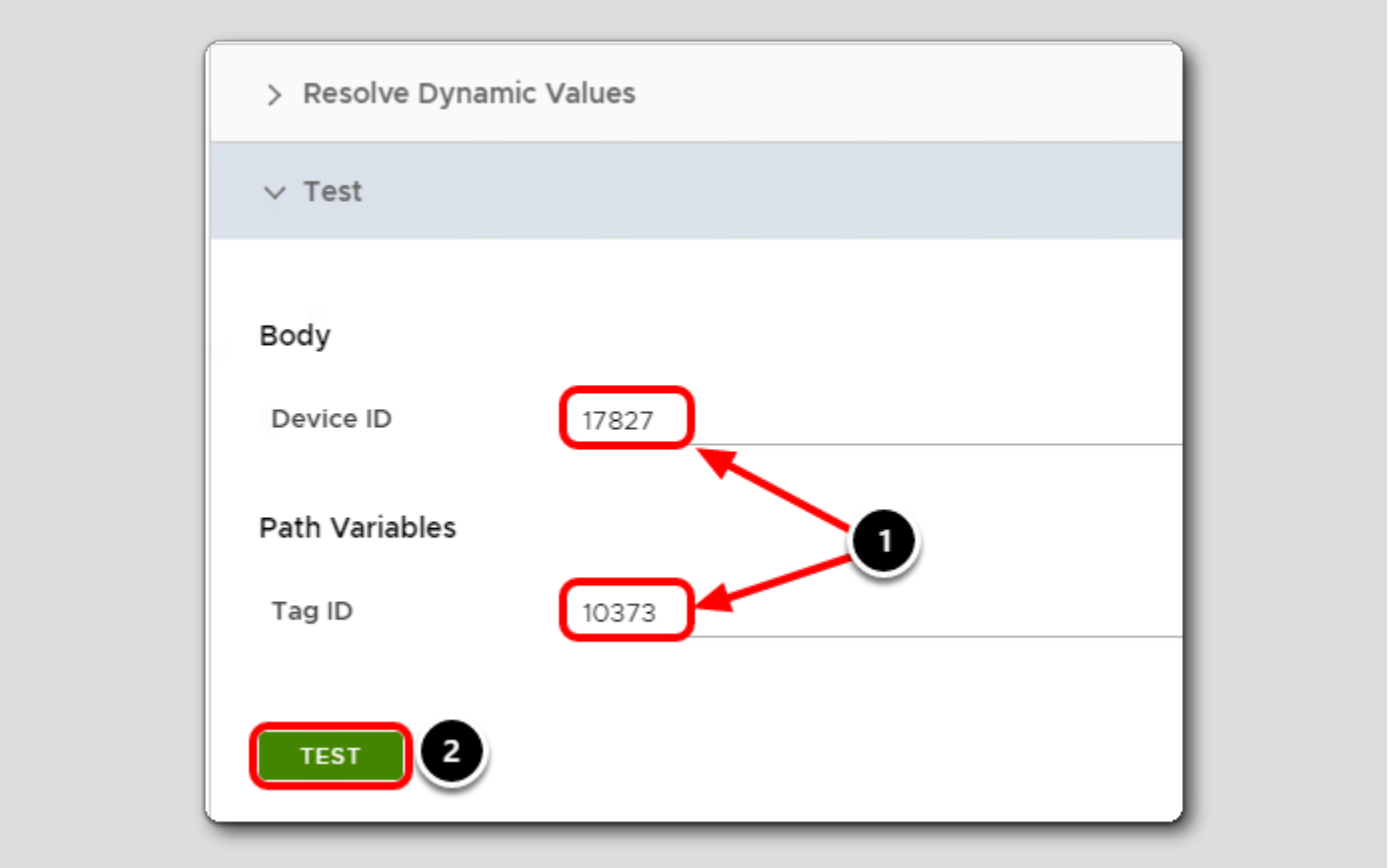
[661]



1. 前の手順の動的な値 **`${device_id}`** を置き換えるには、デバイス ID を選択する必要があります。単一のデバイス ID レコードは、以前に登録した Windows 10 デバイスに関連付けられます。クリックして選択します。
   注：ここに表示されているデバイス ID は実際の環境によって異なります。
2. [Next] をクリックします。

テストの実行

[662]



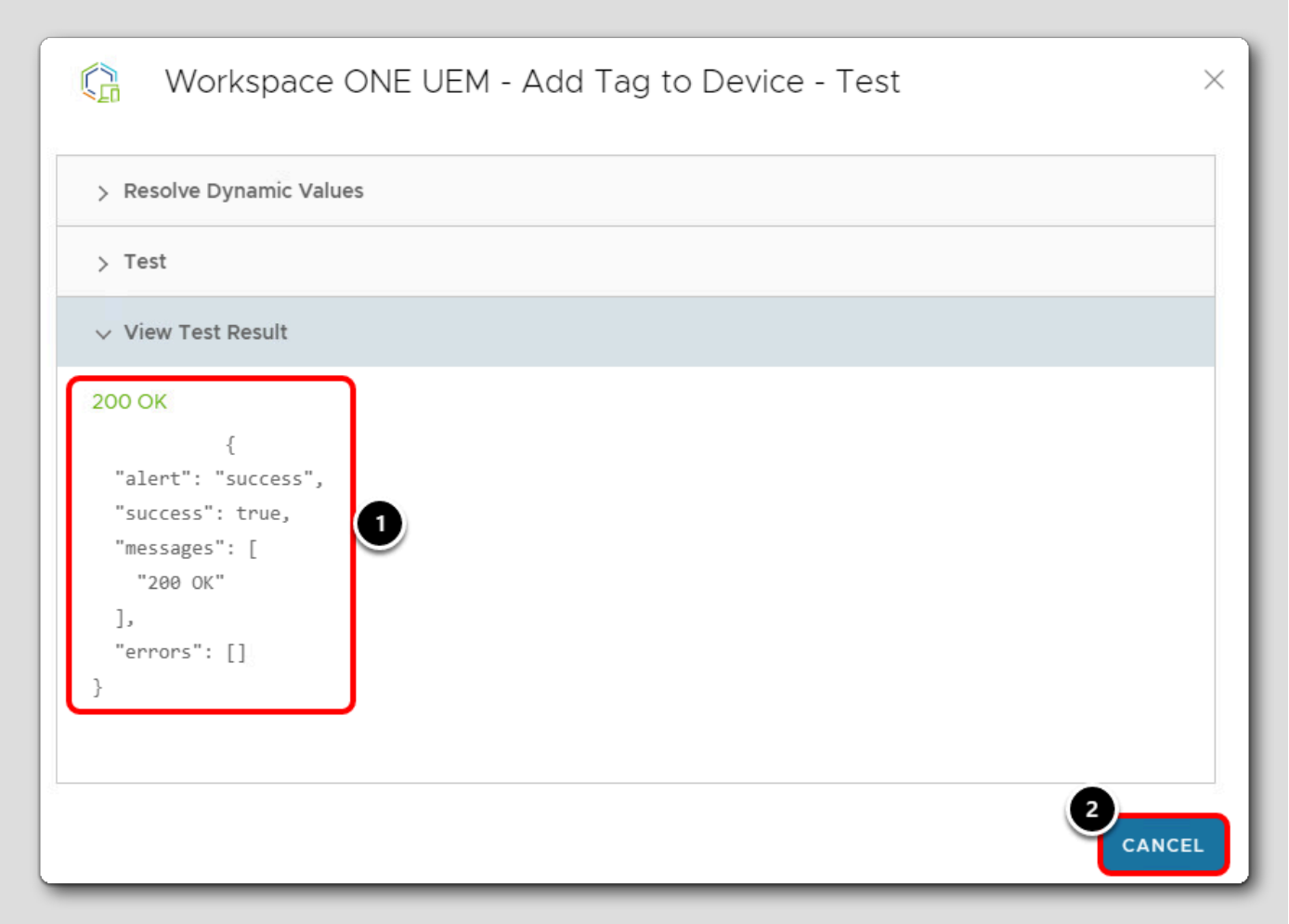
1. デバイス ID とタグ ID の値が、Workspace ONE UEM 環境の値に置き換えられていることを確認します。

   注：ここに表示されているデバイス ID は実際の環境によって異なります。

2. [Test] をクリックします。

テストが成功したことの確認

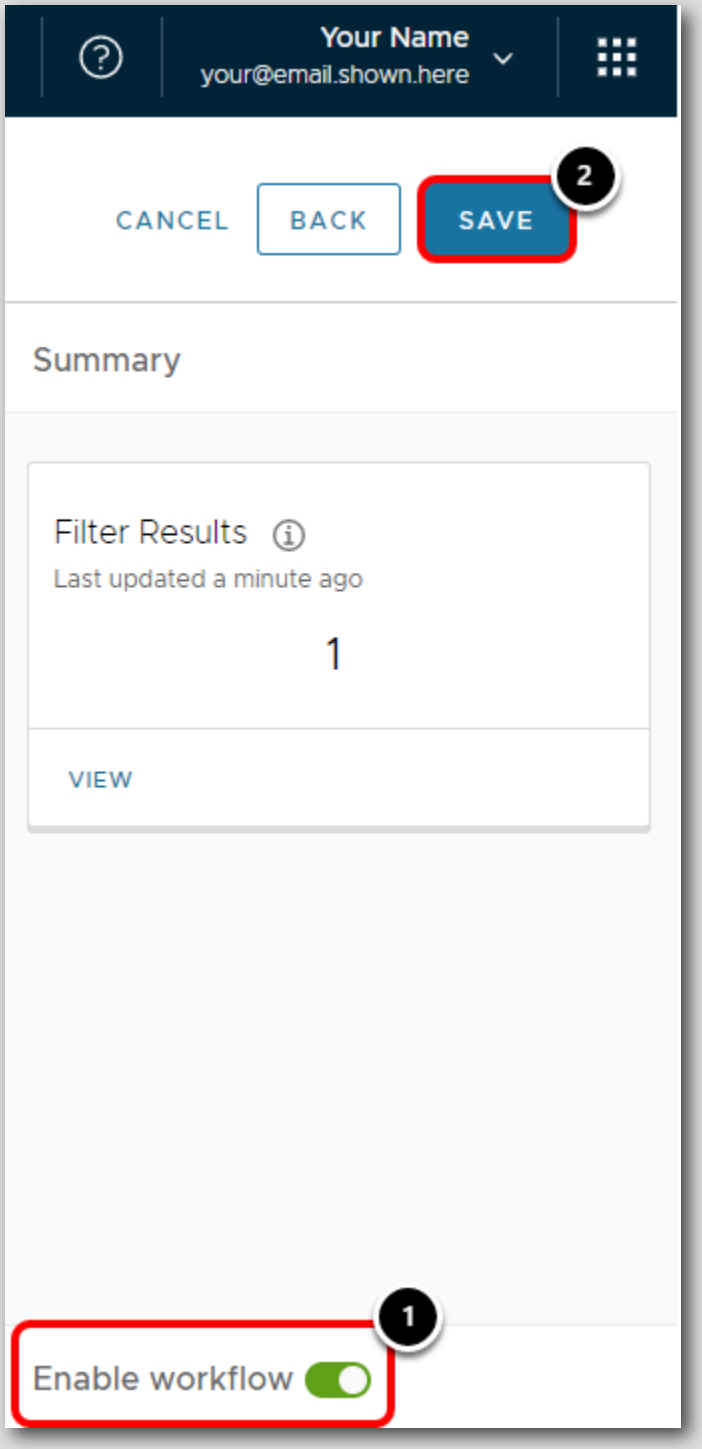
[663]



1. テスト結果に「200 OK」と表示されていることを確認します。
2. [Cancel] をクリックして、自動化テストを終了します。

ワークフローの保存

[664]

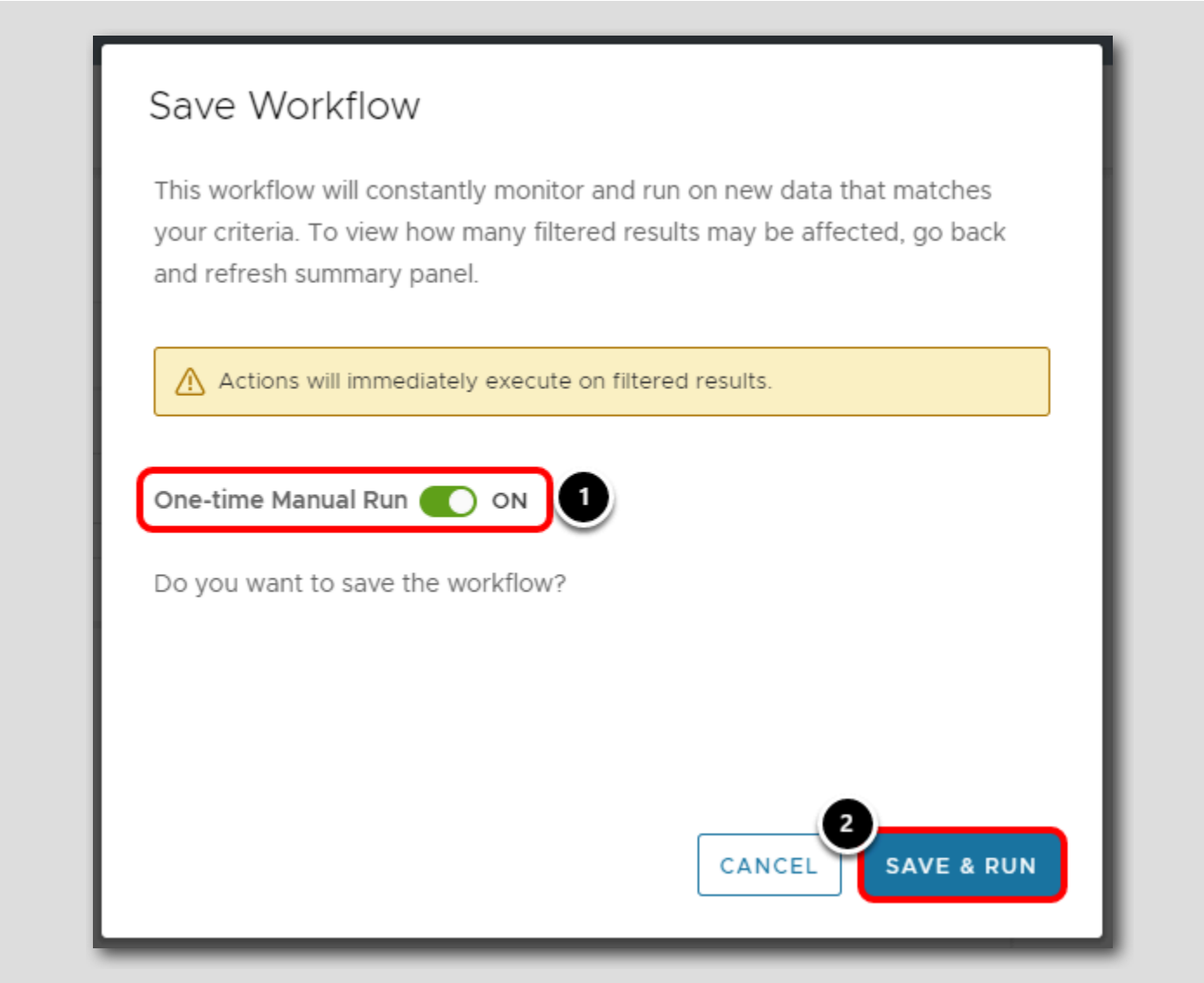


1. 右下隅で、[Enable Workflow] をオンに切り替えます。
2. [Save] をクリックします。

注：このスクリーンショットはサンプル環境から取得したものです。Dell Battery Health イベントが登録済みの Windows 10 仮想マシンに適用されないため、フィルタ結果には 0 と表示されます。物理 Dell デバイスに同じ自動化を展開すると、影響を受けるデバイスがここに表示されます。

ワークフローの保存と実行

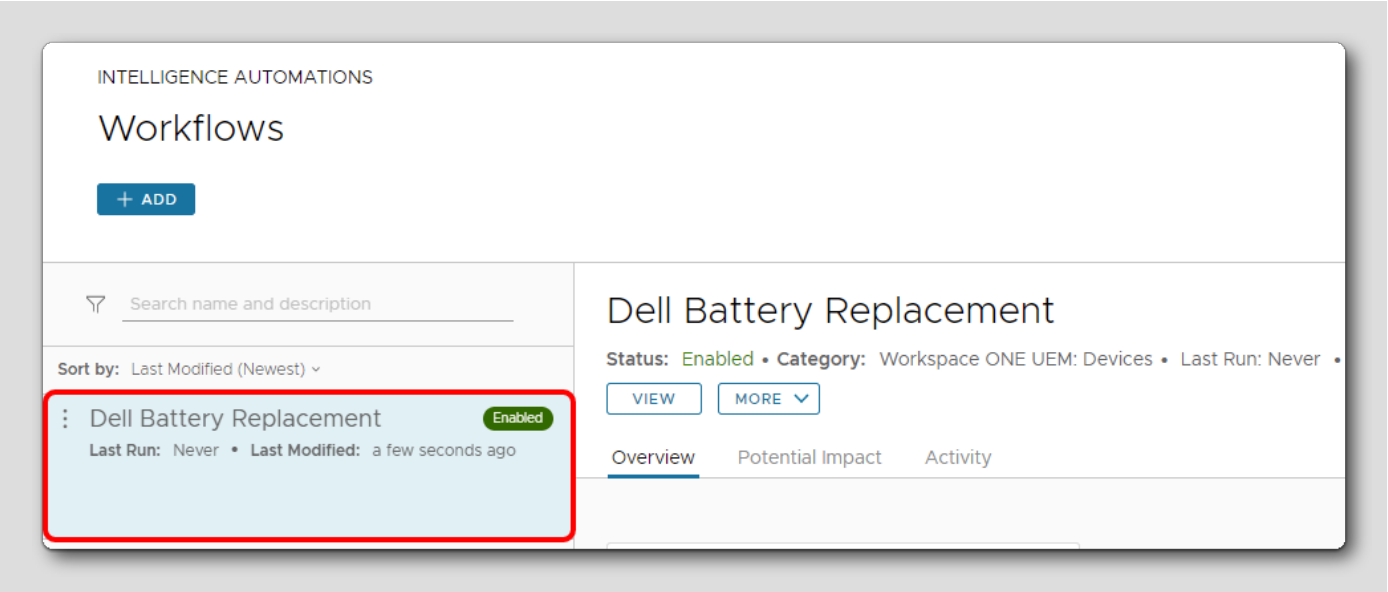
[665]



1. [One-time Manual Run] オプションをオンに切り替えます。これにより、ターゲット デバイスに対してワークフローがすぐに実行されます。
2. [Save & Run] をクリックします。

自動化が作成されたことの確認

[666]



ダッシュボードで、[Dell Battery Replacement] 自動化に [Enabled] のステータスが表示されることを確認します。

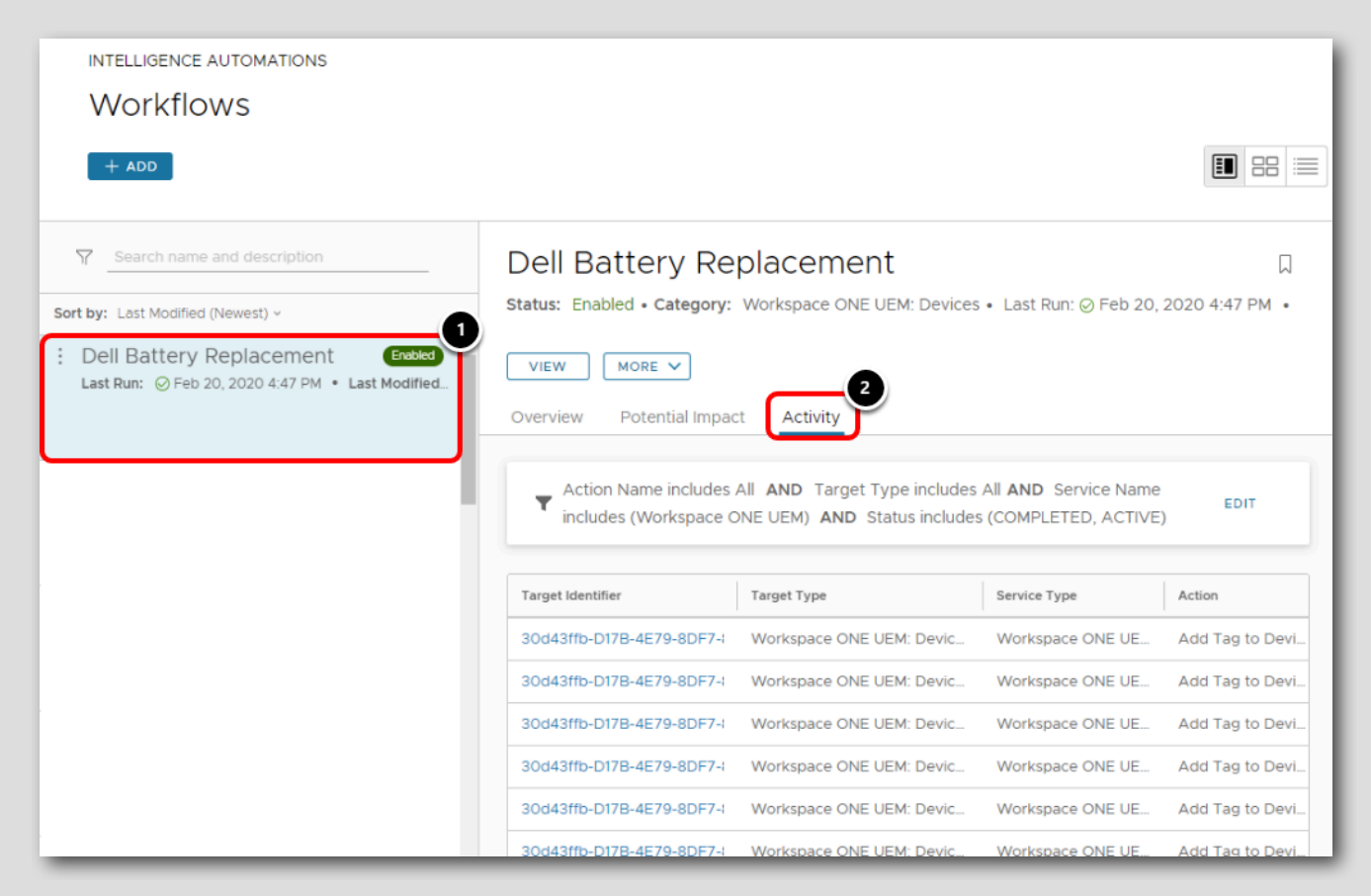
自動化イベントの確認

[667]

Workspace ONE Intelligence コンソールで自動化を作成すると、構成済みのアクションが有効になり、ログに記録されます。このアクティビティでは、自動化ログを使用して、バッテリ交換が必要な Dell デバイスの自動化イベントを確認します。

ログを開く

[668]



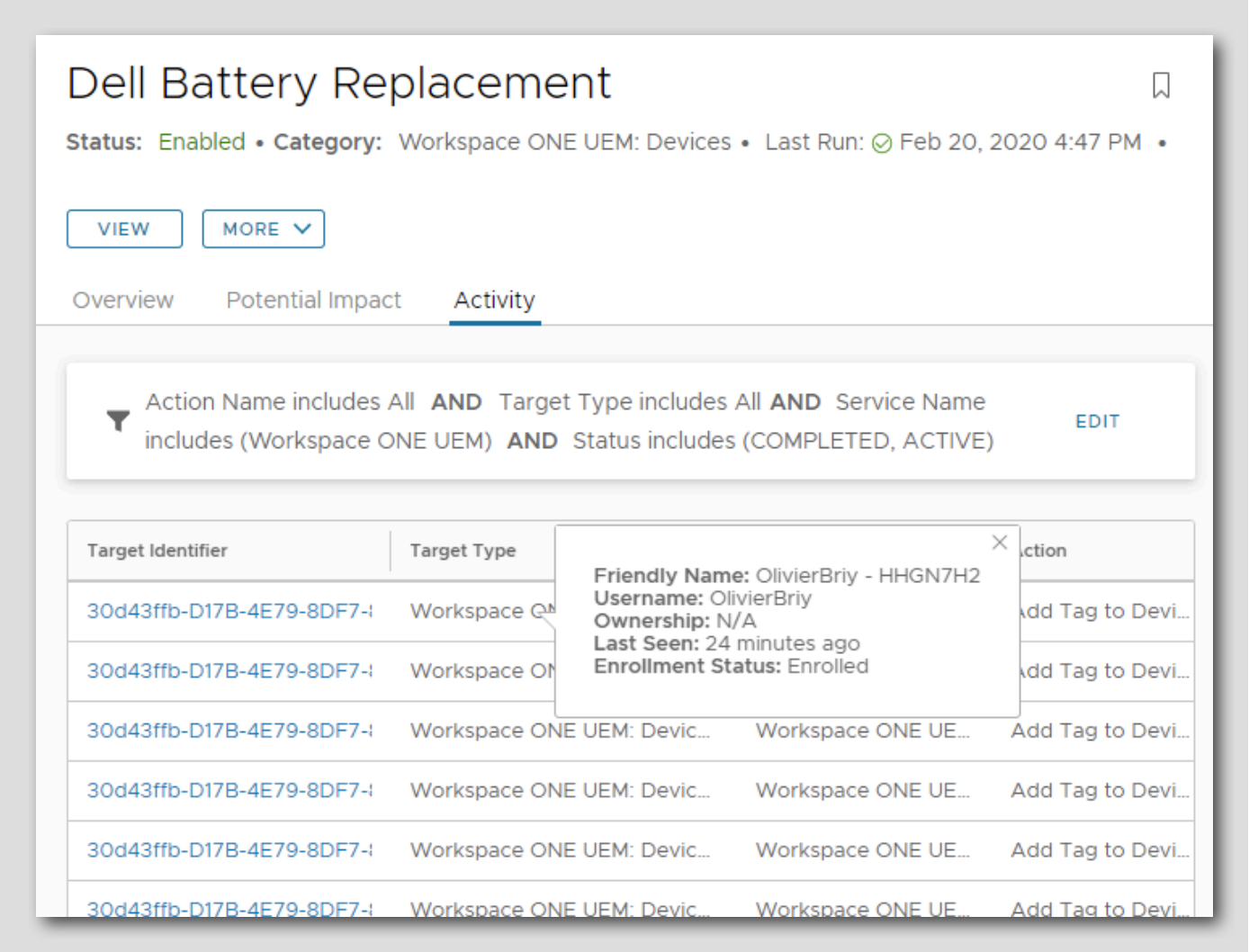
注：物理的な Dell デバイスではないため、登録された Windows 10 仮想マシンに対して Dell Battery Health イベントがトリガされません。このため、スクリーンショットはご利用の環境とは異なります。実際の環境でどのように表示されるかの例として、スクリーンショットを参照してください。

[Automations] ダッシュボードで、次のように操作します。

1. [Dell Battery Replacement] ワークフローをクリックします。
2. [Activity] を選択します。

ログの確認

[669]

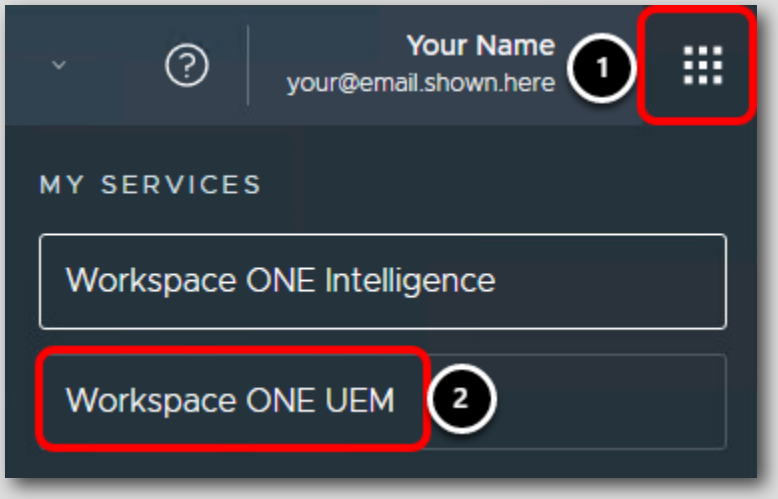


注：物理的な Dell デバイスではないため、登録された Windows 10 仮想マシンに対して Dell Battery Health イベントがトリガされません。このため、スクリーンショットはご利用の環境とは異なります。実際の環境でどのように表示されるかの例として、スクリーンショットを参照してください。

登録したデバイスのバッテリの健全性に応じて、このアクティビティで構成した自動化イベントがトリガされるかどうかが決まります。そのため、次のスクリーンショットは、関連性のないログのサンプルです。さまざまなサービスに対して実行される複数のアクションの例を示しています。

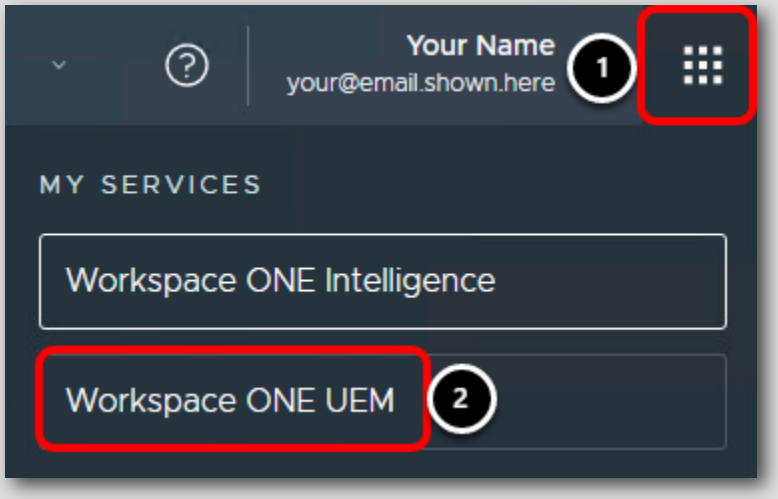
Workspace ONE UEM Console に戻る

[670]



Workspace ONE Intelligence コンソールの右上で、次のように操作します。

1. [My Services] ボタンをクリックします。
2. [Workspace ONE UEM] ボタンをクリックします。



Windows 10 デバイスの登録解除

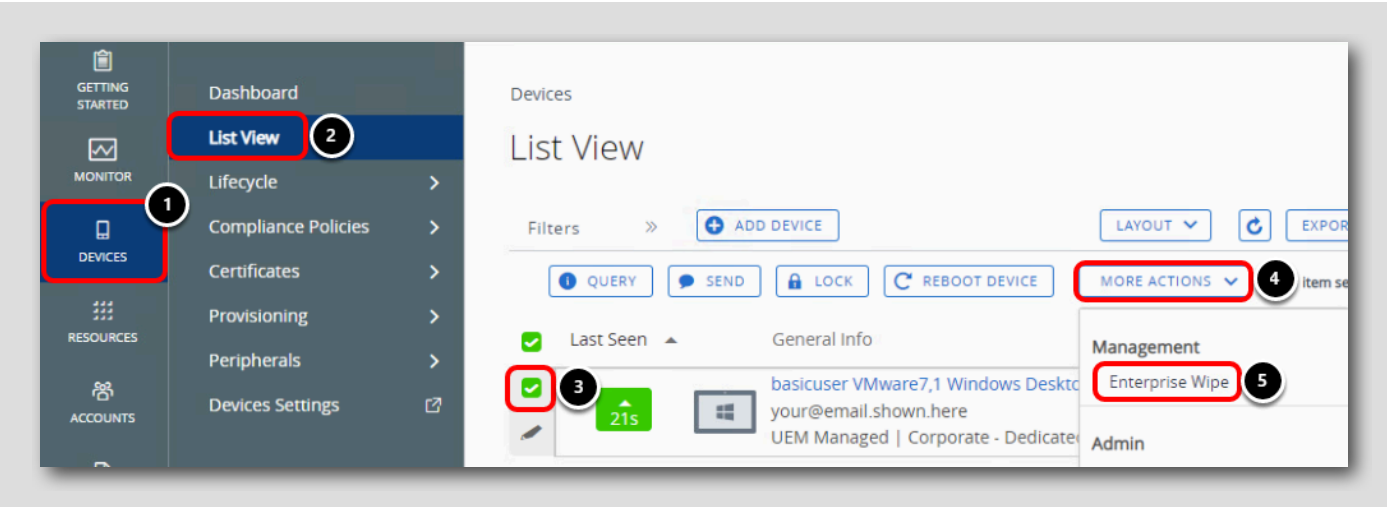
[671]

このセクションでは、Windows 10 仮想マシンの登録を解除して、他のラボ モジュールで使用できるようにします。

Enterprise Wipe ワイプ コマンドを使用して、Workspace ONE によってデバイスにプッシュされたすべての管理対象コンテンツ（プロファイルやアプリケーションなど）を削除しますが、デバイス上の個人的なコンテンツやデータは変更しません。

Workspace ONE UEM Console からの企業情報ワイプ

[672]

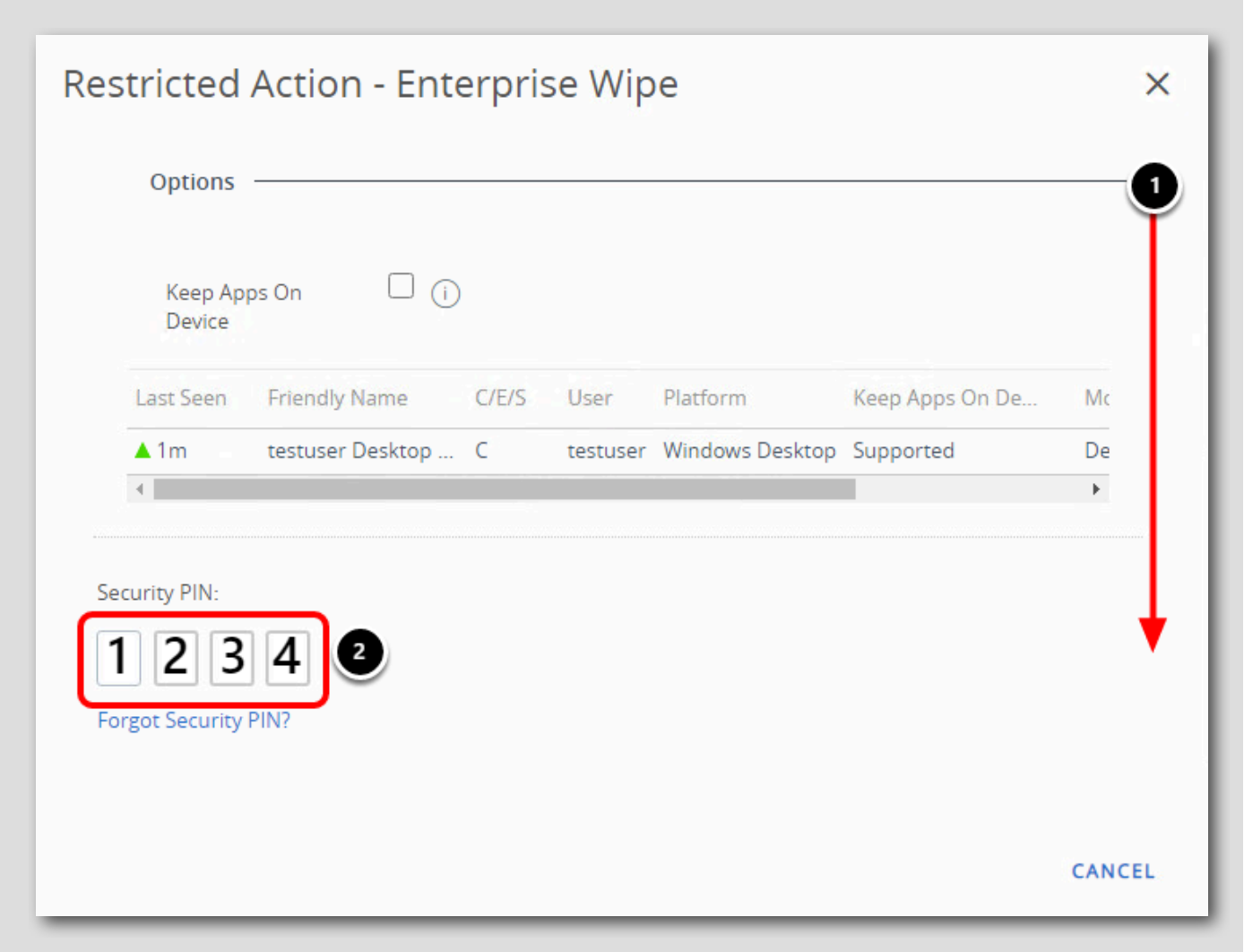


Google Chrome で Workspace ONE UEM 管理者コンソールに戻ります。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. デバイスのフレンドリ名の横にあるチェックボックスを選択します。
4. [More Actions] をクリックします。
5. [Enterprise Wipe] をクリックします。

PIN の入力とデバイスの企業情報ワイプ

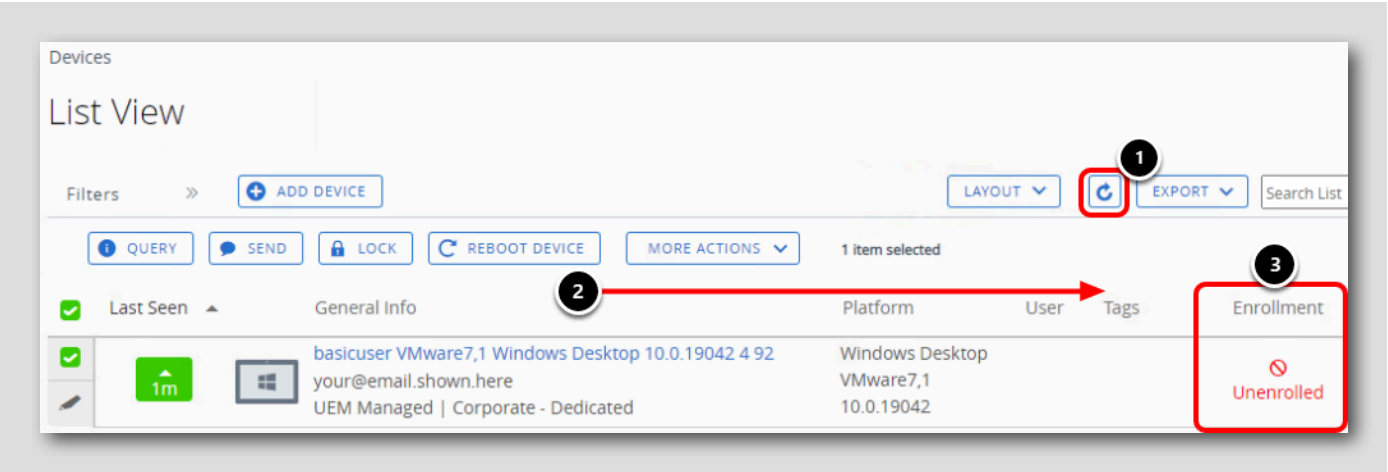
[673]



1. [Security PIN] 入力を見つけるために、下にスクロールする必要がある場合があります。
2. Workspace ONE UEM 管理コンソールに初めてログインしたときに作成したセキュリティ PIN (**1234**) を入力します。別の PIN を使用した場合は、代わりにその PIN を入力します。
3. **[Delete]** をクリックします。

企業情報ワイプの検証

[674]

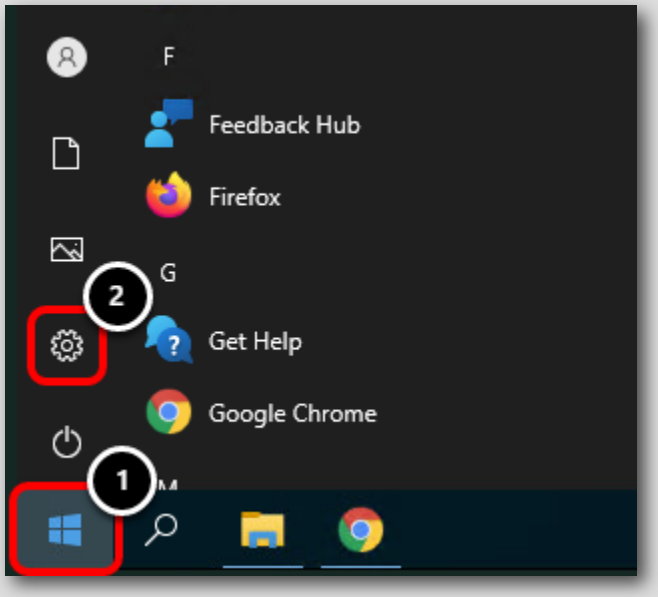


注：企業情報ワイプの処理には、数分かかる場合があります。

1. 更新アイコンを定期的にクリックしてページを更新し、企業情報ワイプが処理されたかどうかを確認します。
2. 必要に応じて、右にスクロールして [Enrollment] 列を見つけます。
3. 企業情報ワイプ コマンドが処理されると、デバイスの登録状態が [Unenrolled] に変わります。

[Windows 10 Settings] への移動

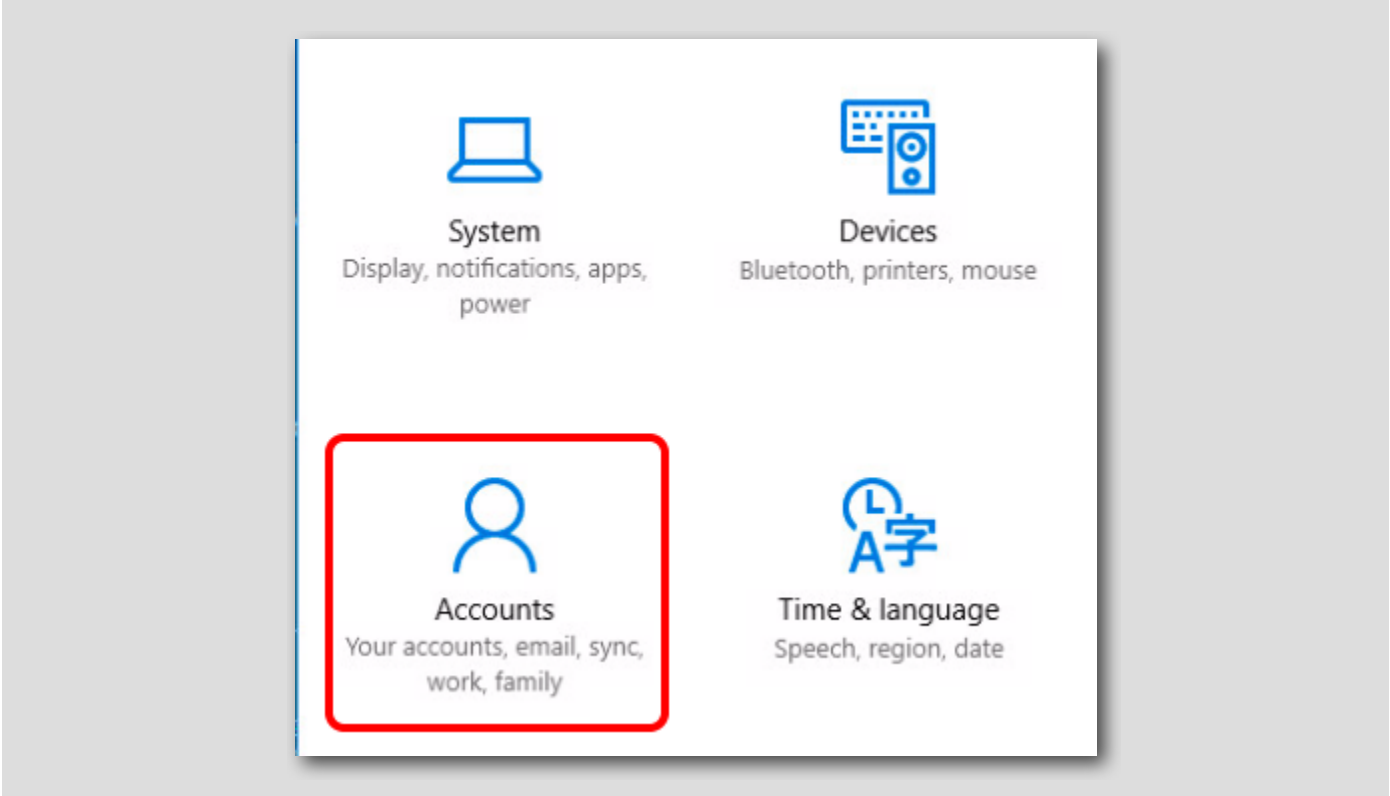
[675]



1. Windows アイコンをクリックします。
2. 歯車アイコンをクリックして、[Windows 10 Settings] にアクセスします。

[Accounts] 設定へのアクセス

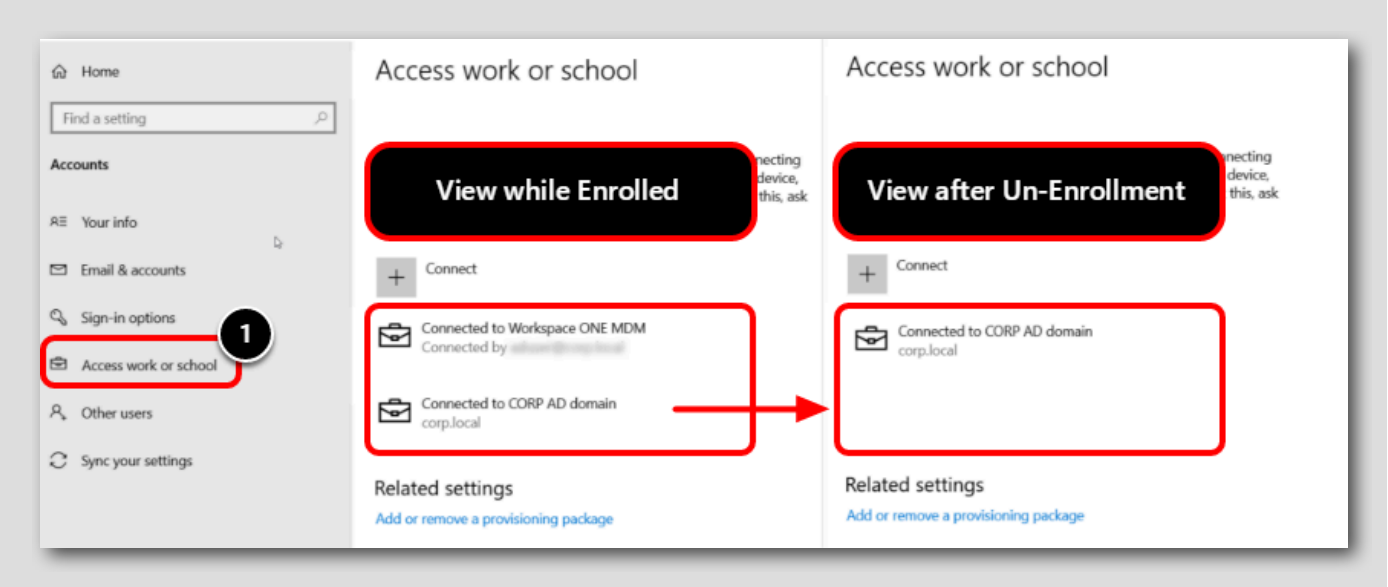
[676]



[Settings] メニューから **[Accounts]** にアクセスします。

管理アカウントが存在しないことの検証

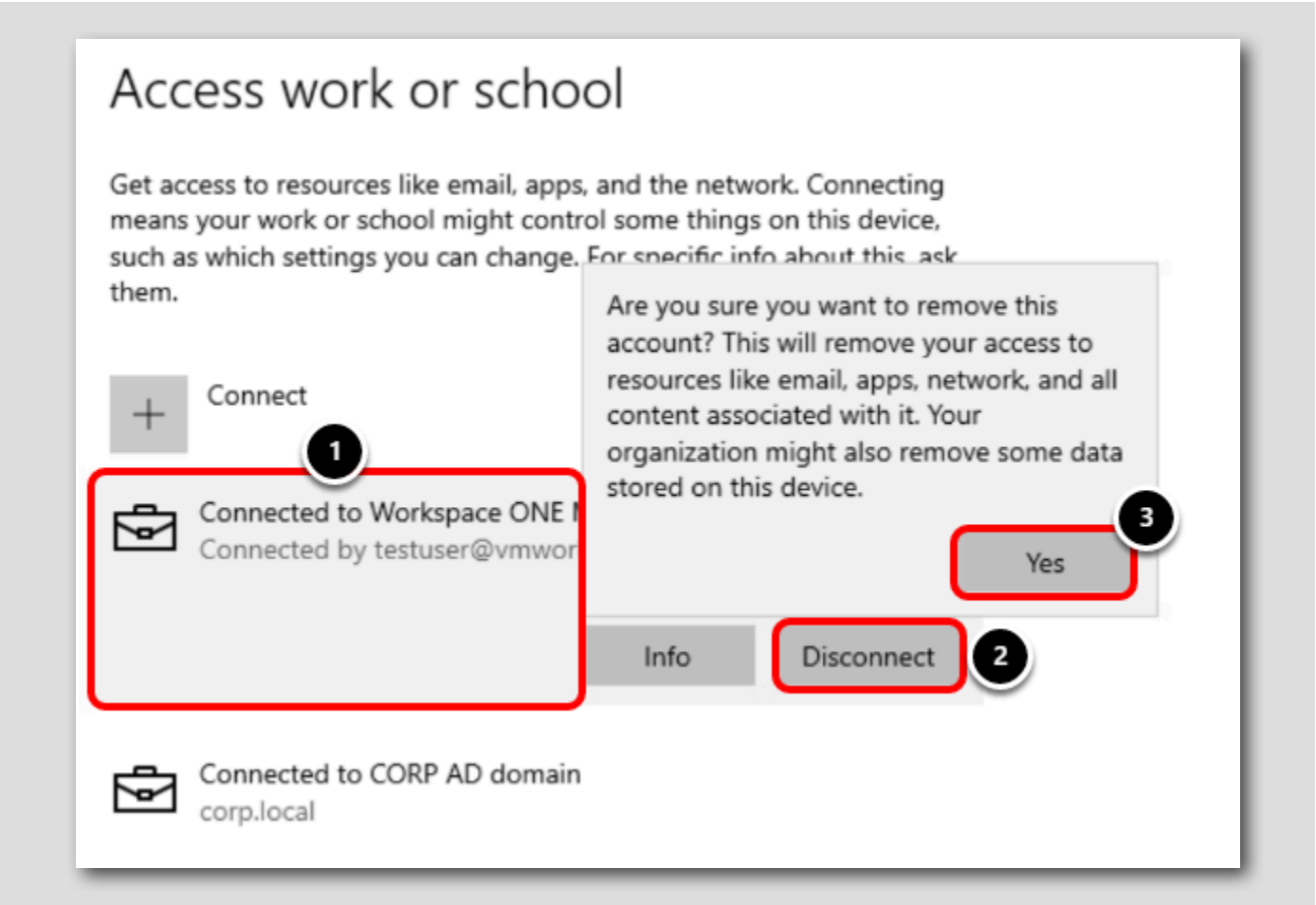
[677]



1. [Access work or school] をクリックします。
2. Workspace ONE MDM に接続されているアカウントがないことを確認します。

注：このラボでは、CORP AD ドメインはローカル ドメインであり、Workspace ONE UEM 登録によって管理されていないため、デバイスの登録時または登録解除時にこの接続が表示されます。

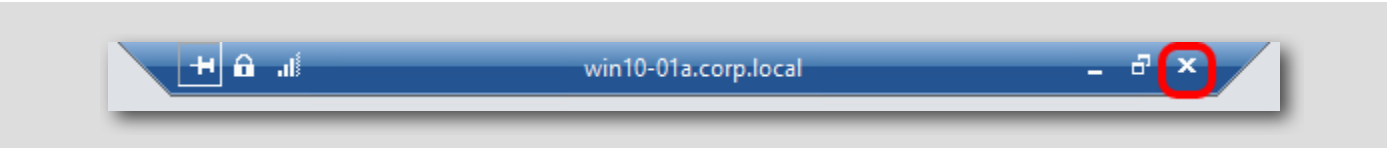
注：[Access Work or School] ページが以前に開かれていた場合は、ページを更新するか、ページから移動してから戻り、変更を確認する必要がある場合があります。



1. [Connected to Workspace ONE UEM] アカウントをクリックします。
2. [Disconnect] をクリックします。
3. [Yes] をクリックします。

メイン コンソールに戻る

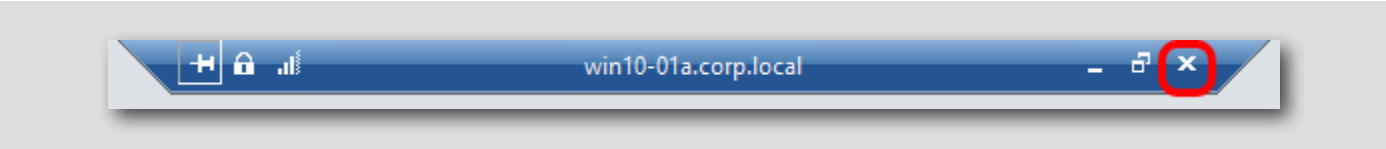
[678]



画面上部の [Remote Desktop Connection] バーで [Close (X)] をクリックしてメイン コンソールに戻り、Workspace ONE UEM Console 内での構成を完了します。

注：[Remote Desktop Connection] バーが表示されない場合は、固定が解除されている可能性があります。画面の上部にカーソルを置くと、

[Remote Desktop Connection] バーが再度表示されるので、[Close] をクリックします。



まとめ

[679]

このモジュールでは、次の事項について学習しました。

- 関連する情報を関心のある関係者と共有する自動レポートを作成し、IT チームの手動での作業を排除する。
- 時間の経過に伴う登録総数を示すウィジェットをダッシュボードに追加する。
- Windows 10 Dell デバイスのバッテリ障害を予測し、交換用のタグ付けを自動化する。
- Service Now などのサードパーティ サービスとの統合を活用して、自動化に関するアクションをトリガする。

Workspace ONE Intelligence を利用できるその他のユースケースの詳細については、次の Tech Zone ビデオをご覧ください。

- Workspace ONE Intelligence と VMware Carbon Black：デバイス隔離の自動化 - 機能の詳細説明
- VMware Workspace ONE Intelligence：コネクタ - 機能の詳細説明
- Workspace ONE Intelligence：リスク分析の理解 - 詳細な説明
- VMware の IT 部門が Workspace ONE Intelligence をどのように活用するか - VMware on VMware

Workspace ONE Intelligence のその他のリソースや情報については、VMware Workspace ONE Intelligence のページ (*https://www.vmware.com/products/workspace-one/intelligence.html*) を確認してください。

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[680]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。

モジュール 8：Secure Access Service Edge (SASE) を使用した Anywhere Workspace のセキュリティ強化（60 分）

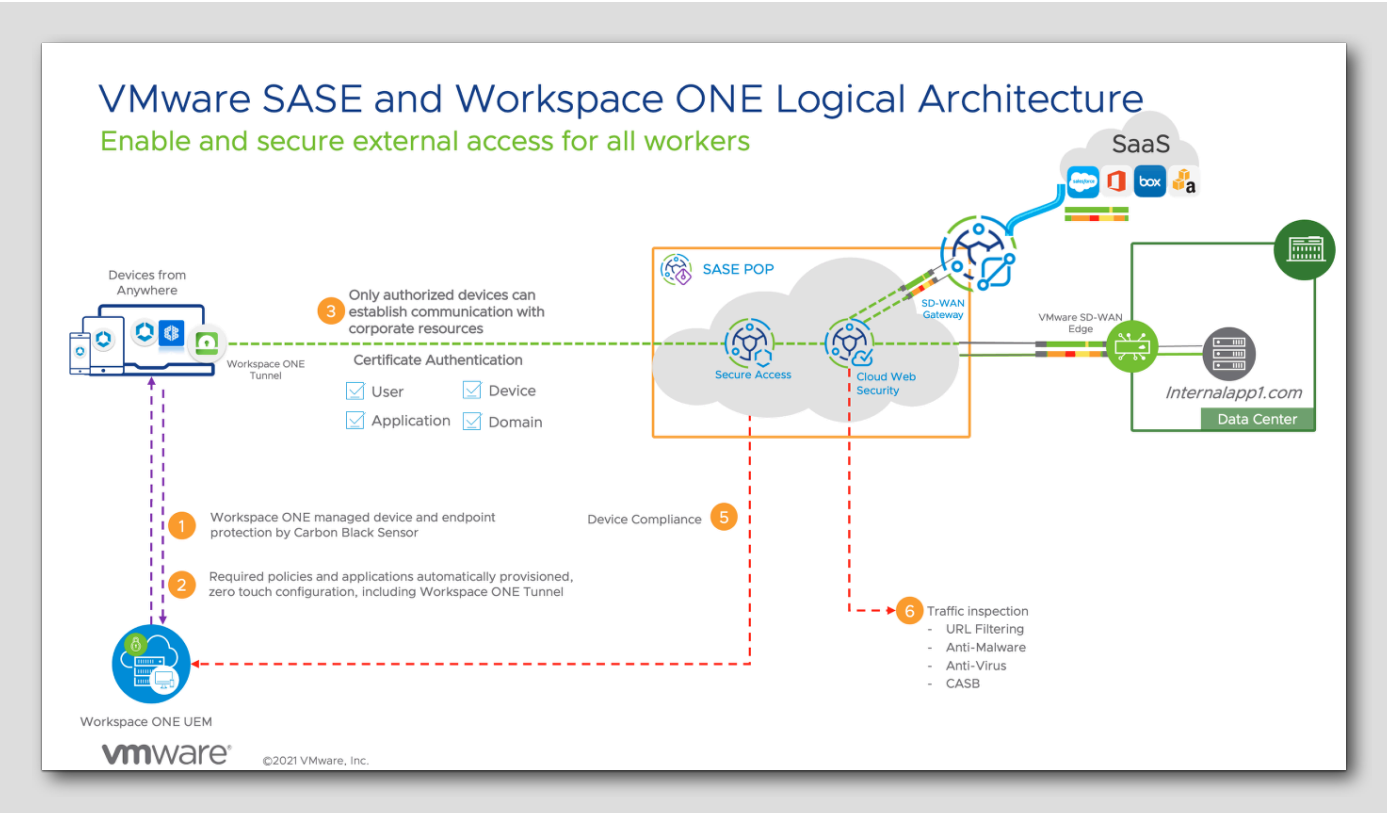
はじめに

[682]

Workspace ONE Tunnel と Secure Access Service Edge は、Anywhere Workspace の 2 つのコンポーネントで、アプリケーション単位およびフル デバイス トンネル接続を提供することで、従業員がオンプレミスおよびクラウド内のリソースに安全にアクセスできるようにします。これにより、アプリケーションはターゲット ドメインに基づいてトラフィックをトンネリング、ブロック、またはバイパスできます。

論理アーキテクチャ

[683]



VMware Secure Access により、VMware は、VMware SD-WAN の一貫性のあるセキュアなクラウド アプリケーション アクセス機能と、Workspace ONE の機能を組み合わせて、信頼できるデバイスとユーザーのみがオンプレミスまたはクラウドでホストされているアプリケーションにアクセスできるようにしました。

Workspace ONE の場合:

- Workspace ONE Tunnel は、オフィス外でインターネット接続を使用するすべてのワーカーとデバイスが任意の場所から安全にアクセスできるようにします。
- 認証レイヤーも複数あります。ユーザーとデバイスは Workspace ONE に登録されている必要があります。その後、Tunnel クライアントはアプリケーションとドメイン固有のルーティングを提供できます。
- ユーザーは「ノータッチ」の Tunnel 体験をすることはありません。セットアップと構成は、Workspace ONE UEM によって 100% 管理されます。
- IT 組織は、エンタープライズ アクセスに対して最小限の権限を持つアプローチを取り、管理対象デバイス、定義済みアプリケーションとドメインのみが内部ネットワークにアクセスできるようにします。
- 管理対象アプリケーションの明示的な定義と、Workspace ONE コンプライアンス エンジンとの統合を組み合わせることで、ゼロトラスト目標を達成できます。

SASE の場合:

- VMware SD-WAN は、VMware SASE の不可欠な要素であり、リモート モバイル ユーザーがデバイス上でアクセスするアプリケーションを可視化します。
- トラフィックが SD-WAN オーバーレイに統合されると、動的マルチパス最適化 (DMPO) のメリットが適用され、遅延、パケットロス、ジッターが削減され、帯域幅の使用率が向上します。
- Secure Access は、Workspace ONE Tunnel アプリケーションを介してデバイスから接続を受け取り、管理対象デバイスとコンプライアンス デバイスのみが接続できるようにします。
- Cloud Web Security は、Secure Access から受信する Web トラフィックを検査します。セキュリティ保護されていないトラフィックは、最終宛先にルーティングされる前にドロップされます。

このラボで学習する内容

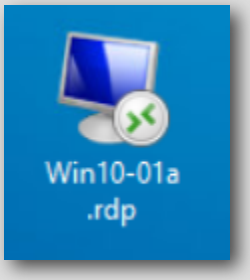
[684]

このラボでは、次の事項について学習します。

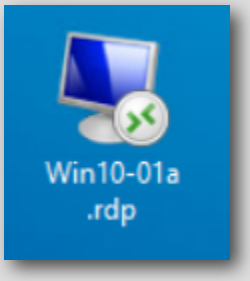
- Workspace ONE Tunnel と Workspace ONE UEM の統合
- Workspace ONE Tunnel へのトラフィックをトンネリング、ブロック、またはバイパスするためのトンネル トラフィック ルールの構成
- Workspace ONE Tunnel アプリケーションのインポートとエンド ユーザーへの公開
- Workspace ONE Tunnel の VPN ペイロードを使用したプロファイルの作成と公開
- Windows 10 仮想マシンの登録
- Workspace ONE Tunnel アプリケーションを使用した、プライベート ネットワークでホストされているイントラネット Web サイトへのアクセス
- 不要なアクションや悪意のあるアクションをブロックするための Secure Access での Cloud Web Security ポリシーの構成
- SD-WAN Network Orchestrator のトラフィックの詳細とメトリックの調査

Windows 10 仮想マシンへの接続

[685]



メイン コンソール デスクトップにある **[Win10-01a.rdp]** ショートカットをダブルクリックして、Windows 10 仮想マシンに接続します。



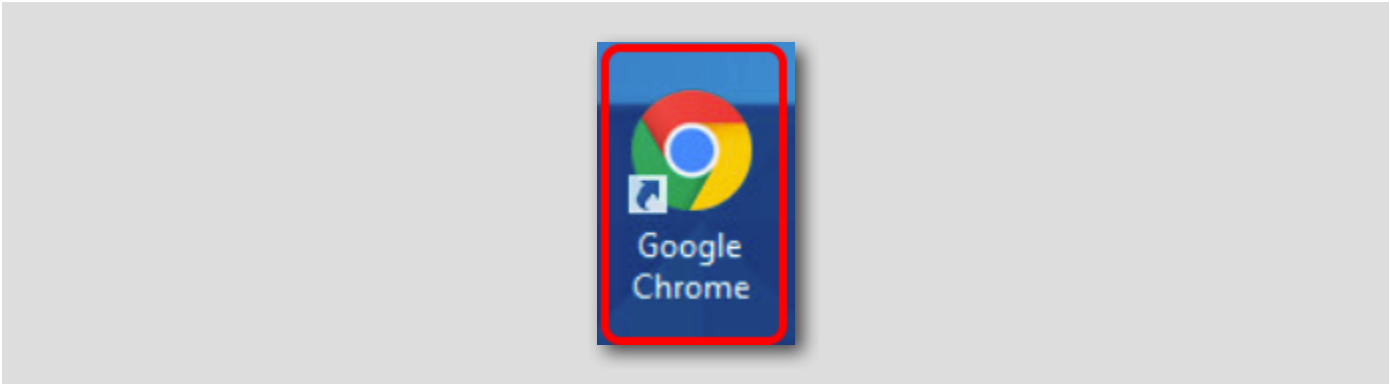
Workspace ONE UEM Console へのログイン

[686]

このラボでは、ほとんどの場合、Workspace ONE UEM 管理コンソールにログインします。

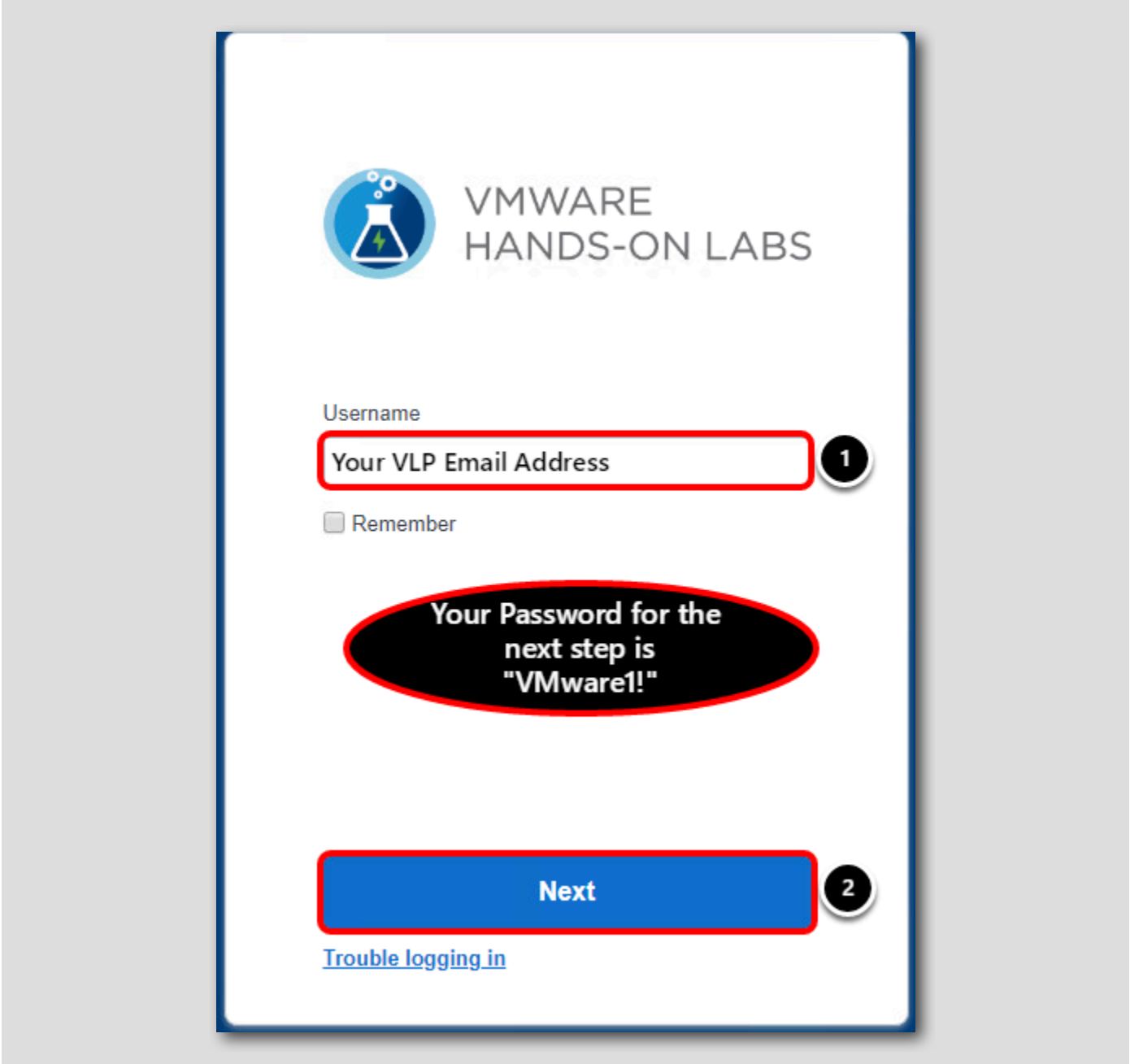
Chrome ブラウザの起動

[687]



現在接続している仮想マシンのデスクトップにある [Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールでの管理者ユーザー名の入力 [688]

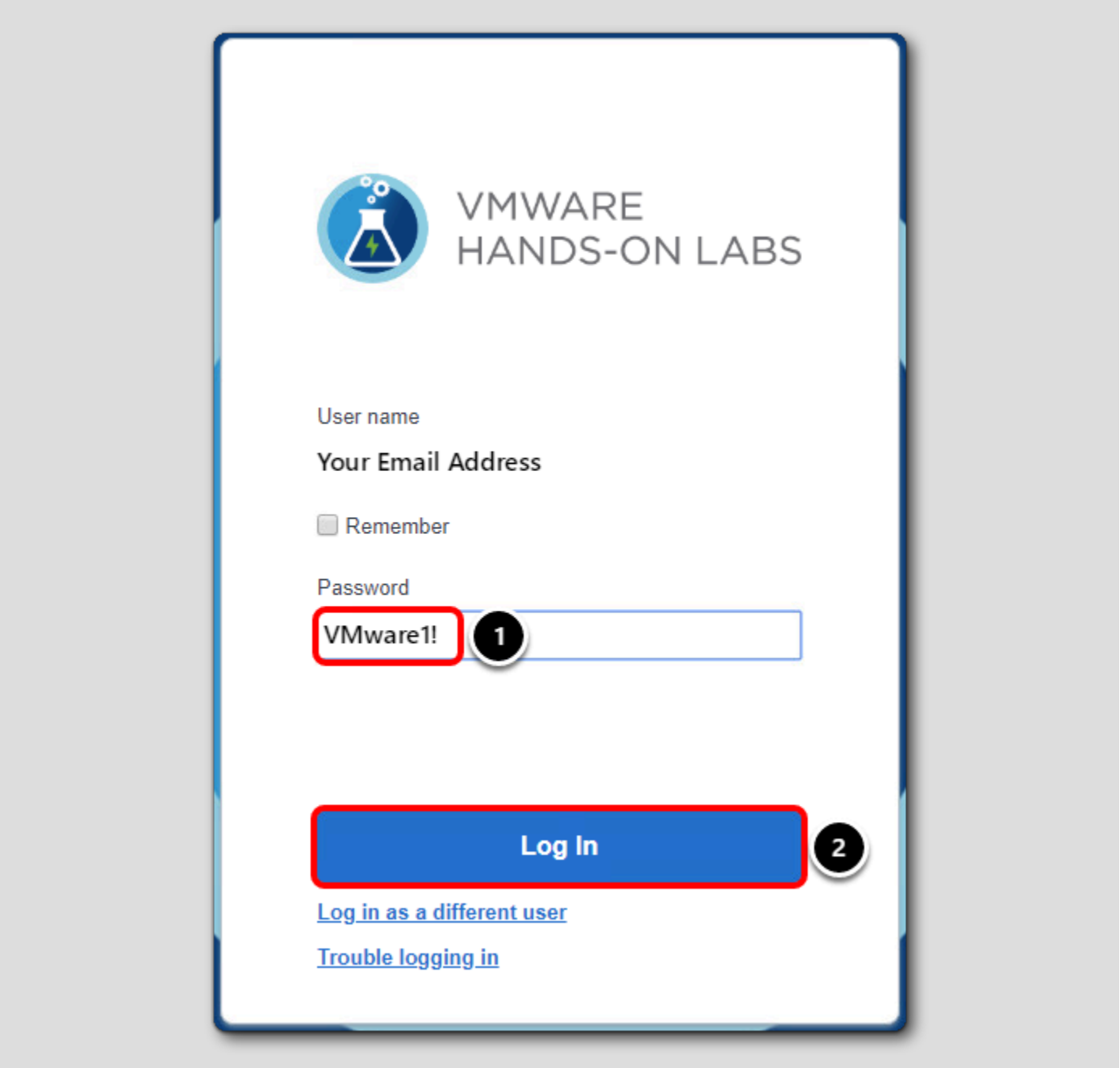


ブラウザのデフォルトのホーム ページは https://hol.awmdm.com です。Workspace ONE UEM 管理者アカウント情報を入力し、[Login] ボタンをクリックします。

1. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。
2. [Next] をクリックして、ラボ マニュアルの次の手順に進み、パスワードを入力します。これは常に **`VMware1!`** です。

注：Captcha による入力を求められた場合は、大文字と小文字を区別して入力してください。

Workspace ONE UEM Console の認証情報の入力 [689]



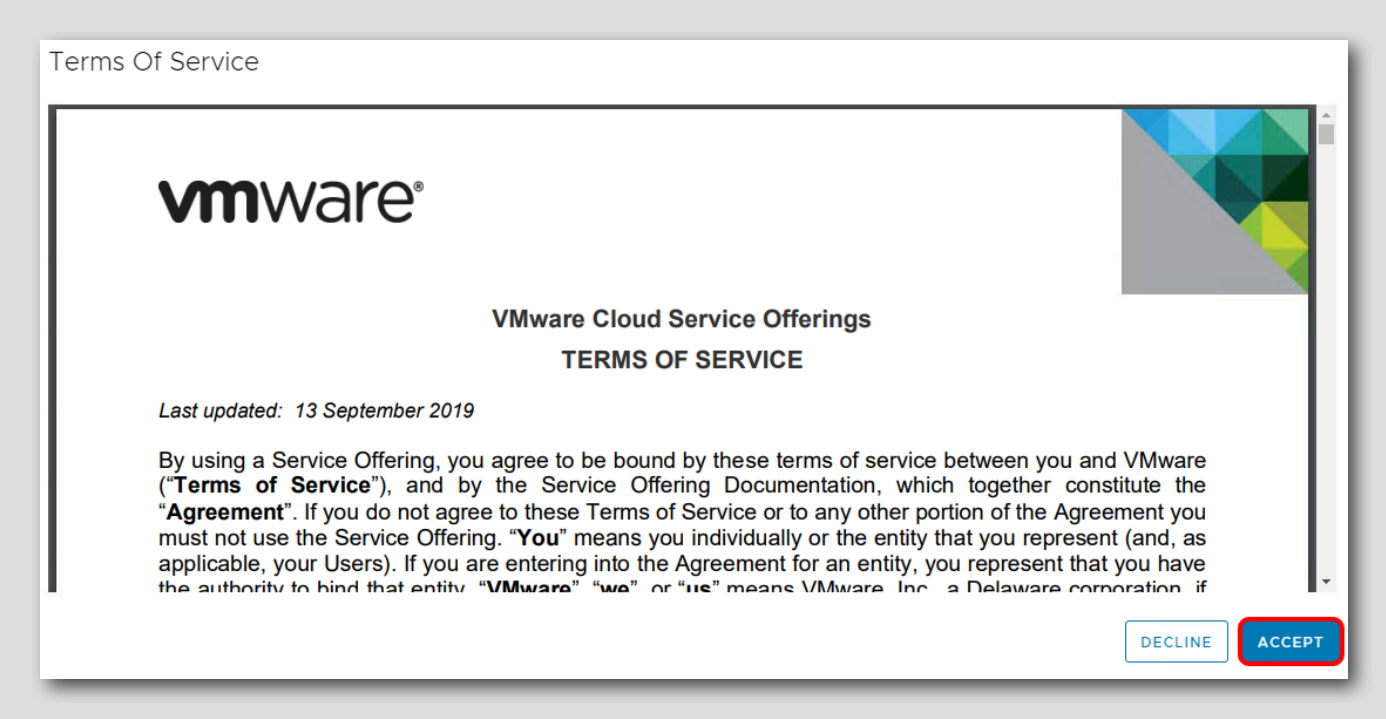
ユーザー名を入力すると、パスワード フィールドが表示されます。

1. [Password] フィールドに **`VMware1!`** と入力します。
2. [Log in] ボタンをクリックします。

注：ラボの制限により、ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

エンド ユーザー使用許諾契約書に同意

[690]



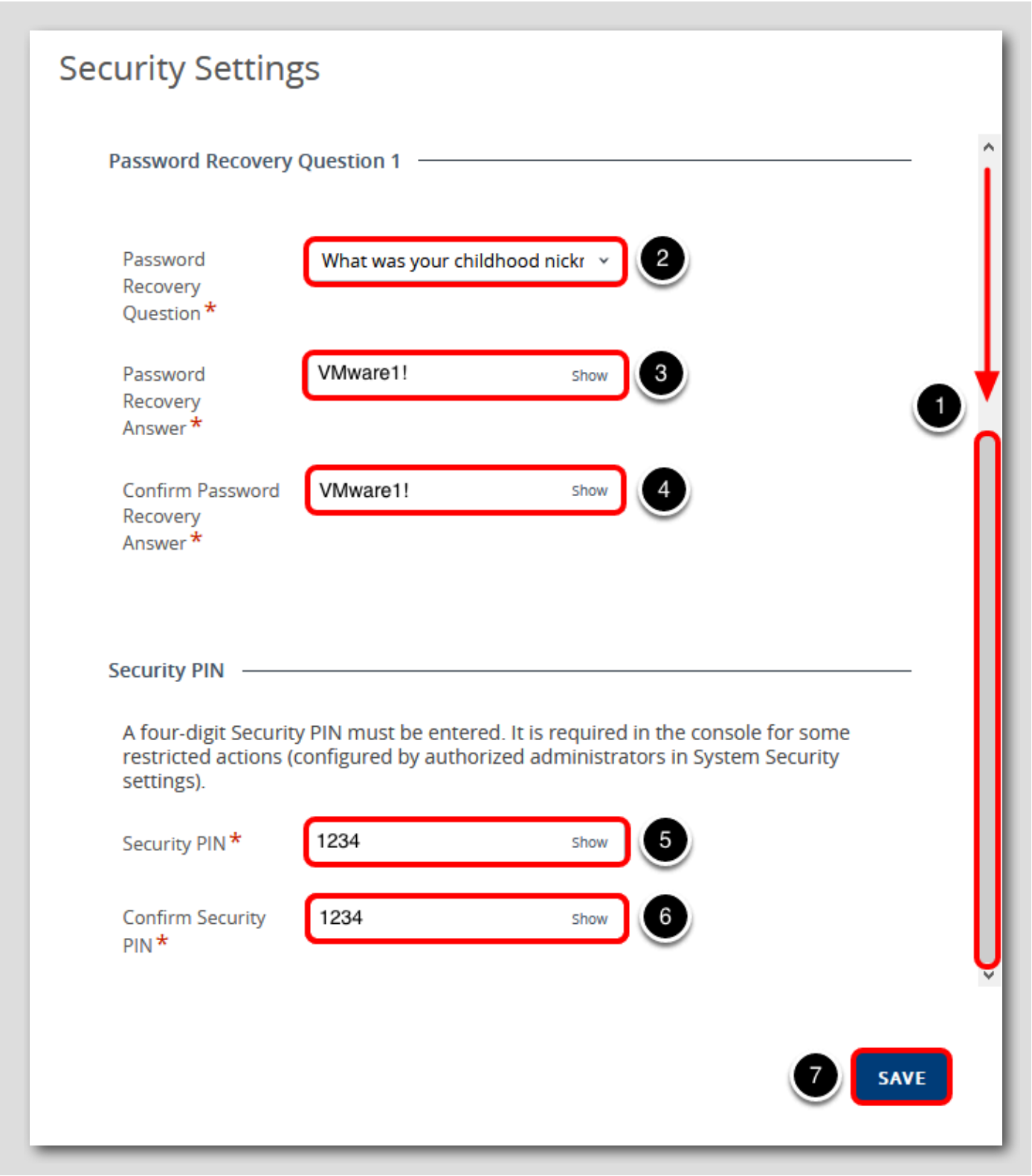
Workspace ONE UEM の「利用規約」が表示されたら、[Accept] ボタンをクリックします。

注：管理コンソールに初めてログインする場合のみ、次の手順に従ってログインしてください。

初期セキュリティ設定の完了

[691]

利用規約に同意すると、次の [Security Settings] ポップアップ画面が表示されます。

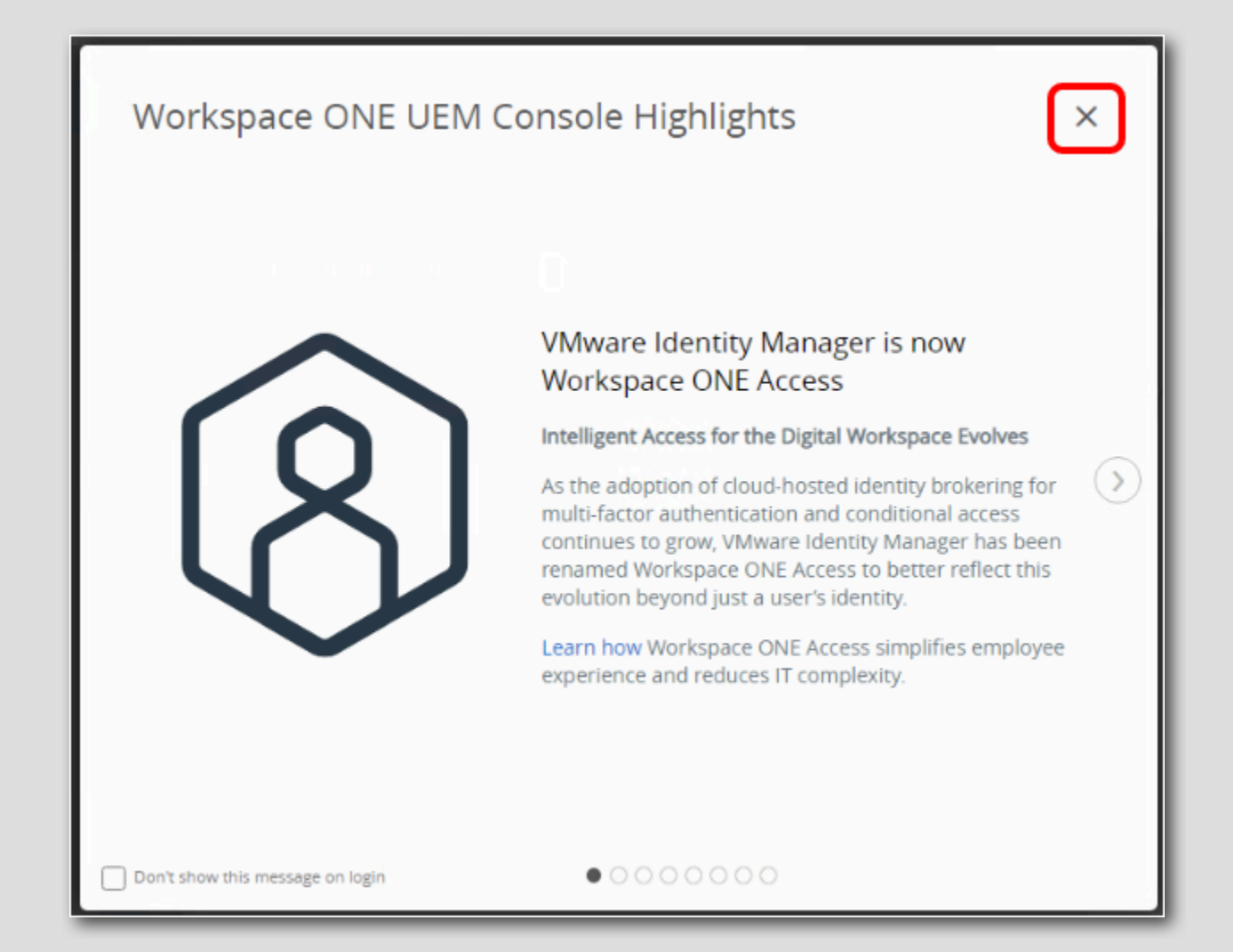

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

[Password Recovery Question] は、管理パスワードを忘れた場合に備えて設定します。また、[Security PIN] は、コンソールで特定の管理機能を保護するために使用します。

1. 必要に応じて画面を下方向にスクロールして、[Password Recovery Questions] および [Security PIN] セクションを表示してください。
2. [Password Recovery Question] ドロップダウンから**質問**を選択します （ここでは、デフォルトで表示されている質問をそのまま選択します）。
3. [Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
4. [Confirm Password Recovery Answer] フィールドに **`VMware1!`** と入力します。
5. [Security PIN] フィールドに **1234** と入力します。
6. [Confirm Security PIN] フィールドに **1234** と入力します。
7. 完了すると [Save] ボタンをクリックします。

コンソールのハイライト

[692]

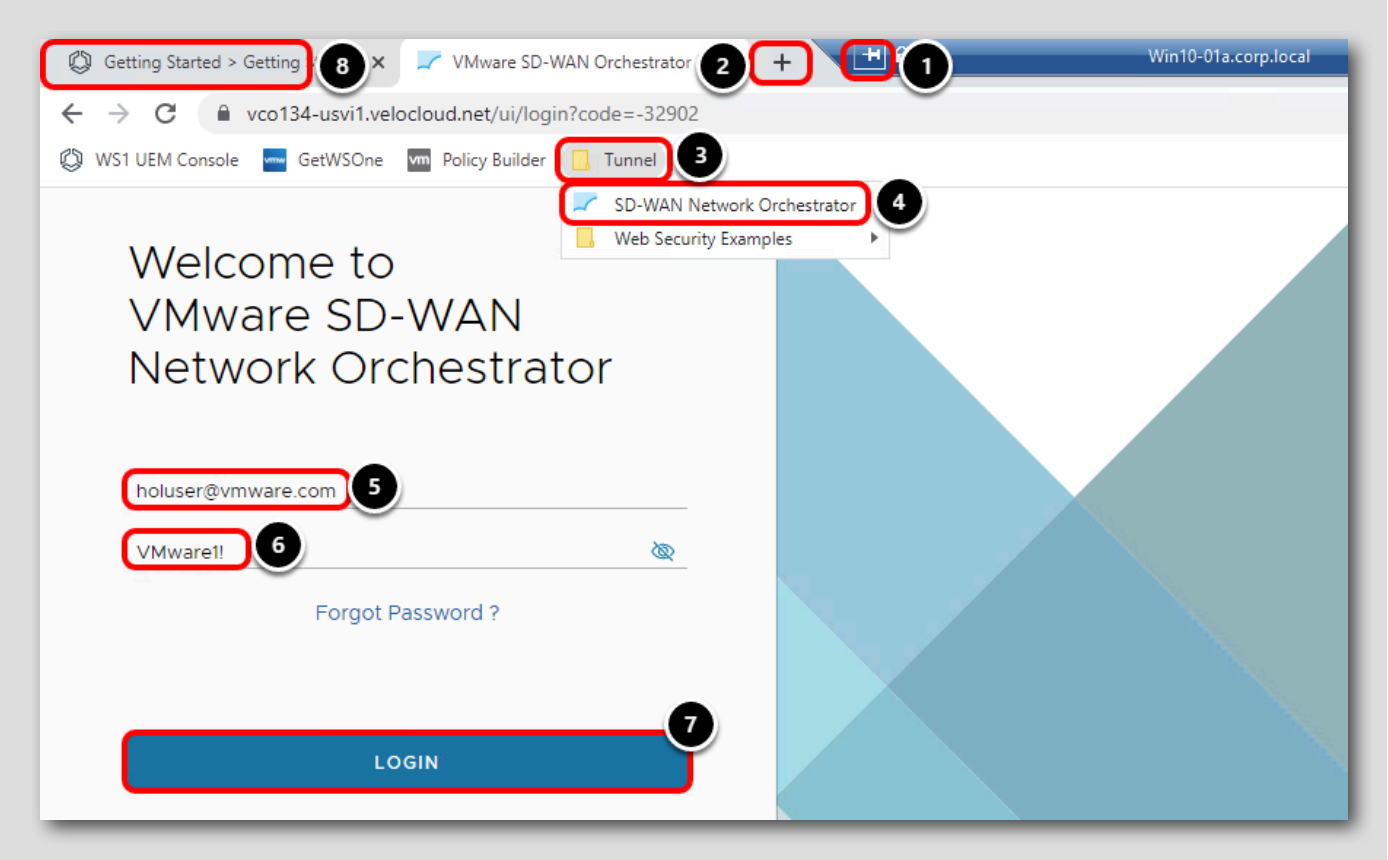


セキュリティの質問を完了すると、ポップアップ ウィンドウが表示されます。

右上隅の [X] をクリックして、[Workspace ONE UEM Console Highlights] ウィンドウを閉じます。

SD-WAN Network Orchestrator へのログイン

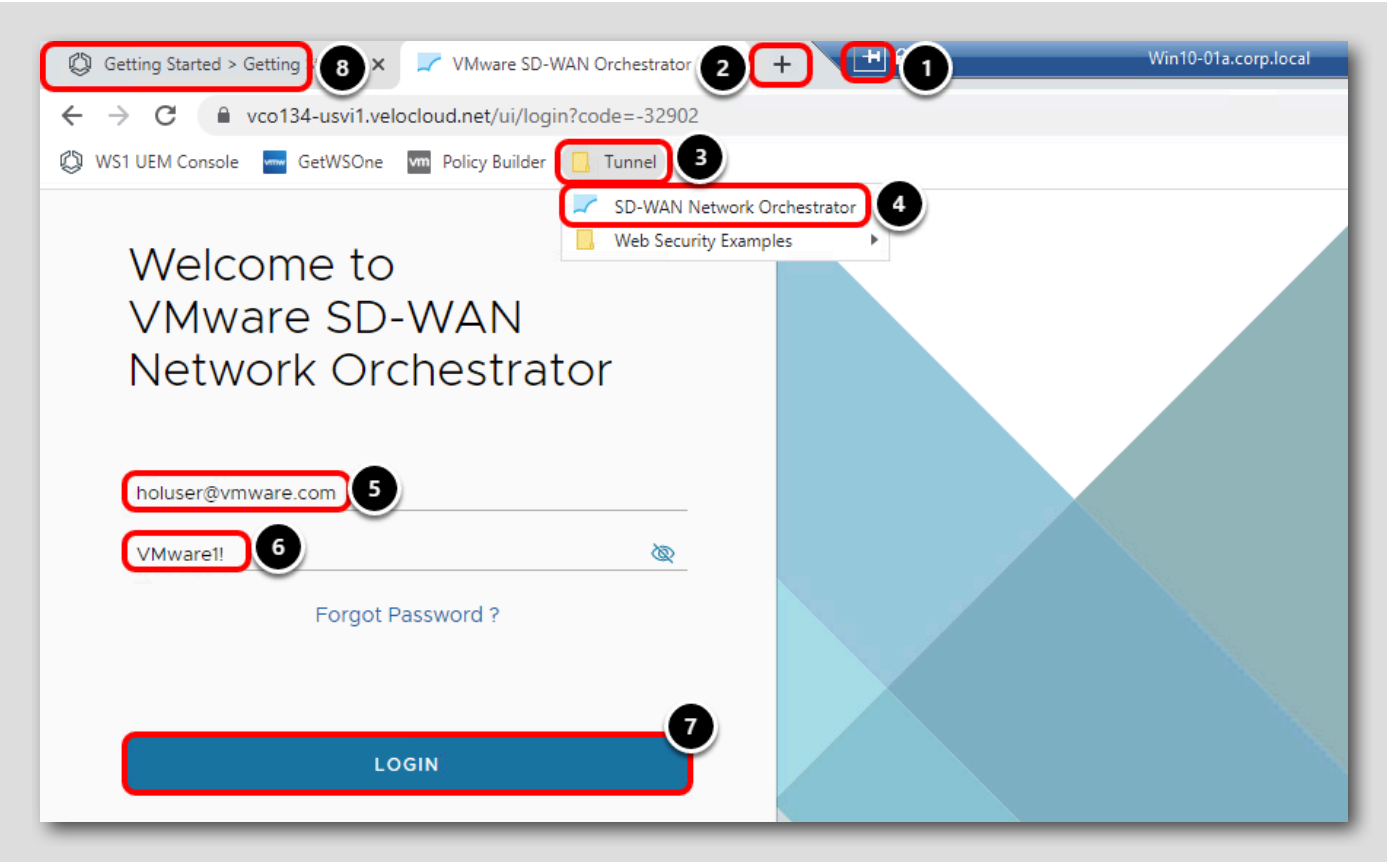
[693]



Workspace ONE UEM 管理者コンソールに加えて、このハンズオン ラボの SD-WAN Network Orchestrator コンソールに読み取り専用ユーザーとしてログインし、Workspace ONE Tunnel サービス ホスティング、Secure Access 設定、および Cloud Web Security ポリシーに関連するさまざまな設定を表示および確認します。

1. リモート デスクトップ タブの**ピン ボタン**をクリックすると、ブラウザのさまざまなタブに簡単にアクセスできるようになります。
2. **[New Tab]** ボタンをクリックして、新しいタブを開きます。
3. **[Tunnel]** ブックマーク フォルダをクリックします。
4. **[SD-WAN Network Orchestrator]** ブックマークをクリックします。
5. [Username] に **`holuser@vmware.com`** と入力します。
6. [Password] に **`VMware1!`** と入力します。
7. **[Login]** をクリックします。
8. **最初のタブ**をクリックして、Workspace ONE UEM に戻ります。

ラボ全体を通じて [SD-WAN Network Orchestrator] タブに定期的に戻る予定なので、このタブは開いたままにします。



イントラネット サイトへの接続に失敗した場合の検証

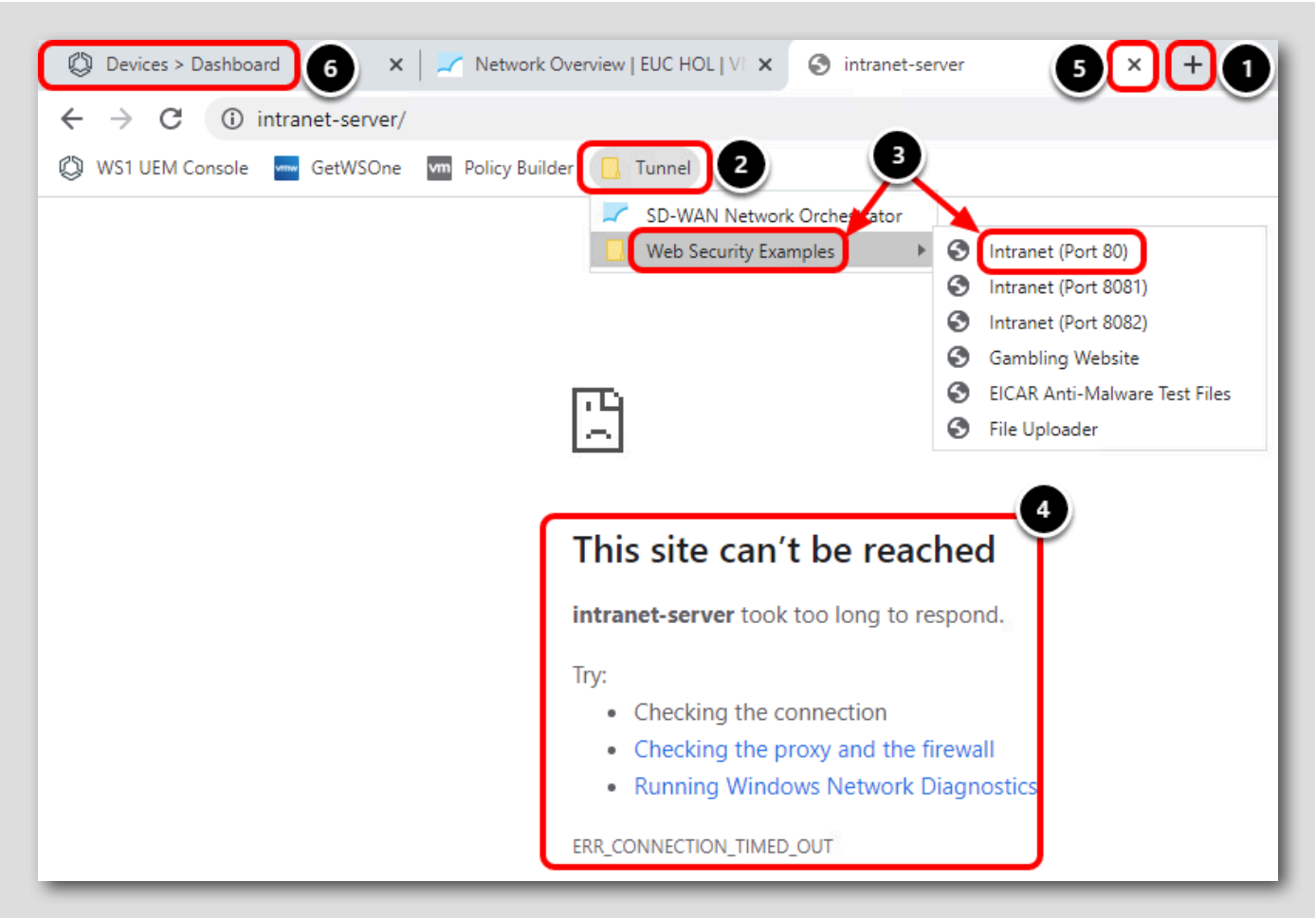
[694]

イントラネット Web サイトは、ハンズオン ラボ ネットワークからアクセスできない外部プライベート ネットワーク上でホストされています。このイントラネット Web サイトでは、ポート 80、8081、および 8082 を介した接続を受け入れます。

Workspace ONE Tunnel および VPN ポリシーを Windows 10 仮想マシンに公開する前に、このイントラネット Web サイトを参照して、アクセス不能であることを確認します。Workspace ONE Tunnel アプリケーションとポリシーが構成され、登録された仮想マシンに配布されたら、このイントラネット Web サイトを参照して、デバイスが Workspace ONE Tunnel サービスを介してトラフィックをトンネリングして、保護されたネットワーク上のイントラネット Web サイトにアクセスできることを確認します。

アクセスできないイントラネット サイトの参照

[695]



Google Chrome で、次のように操作します。

1. [New Tab] ボタンをクリックします。
2. [Tunnel] ブックマーク フォルダをクリックします。
3. [Web Security Examples] にカーソルを合わせて、フォルダから [Intranet (Port 80)] をクリックします。
4. http://intranet-server サイトにアクセスできないことを確認します。

   注：要求はタイムアウトになり、エラー ページが表示されます。タイムアウトが発生するまで 30 ～ 60 秒待機する必要がある場合があります。
5. [intranet-server] タブで [Close] ボタンをクリックして閉じます。
6. 最初のタブをクリックして、Workspace ONE UEM 管理者コンソールに戻ります。

http://intranet-server はパブリック インターネット経由でアクセスできないため、仮想マシンは Web ページを表示できません。イントラネット サイトはプライベート ネットワーク上でホストされており、デバイスが同じプライベート ネットワークでホストされている Workspace ONE Tunnel サービスに接続されている場合にのみアクセスできます。

デバイスがサンノゼの SASE PoP (Point of Presence) でホストされている Tunnel サービスへの接続を確立できるようにするには、Workspace ONE Tunnel アプリケーションと VPN プロファイルを展開して構成する必要があります。これらの構成が完了すると、デバイスは http：// intranet-server サイトのトラフィックをイントラネット サイトがホストされているプライベート ネットワークにトンネリングします。

必要なアプリケーションとプロファイルをデバイスにプッシュする前に、まずデバイスを登録する必要があります。これにより、Workspace ONE UEM がデバイスを管理し、アプリケーションとプロファイルをワイヤレスで公開できるようになります。

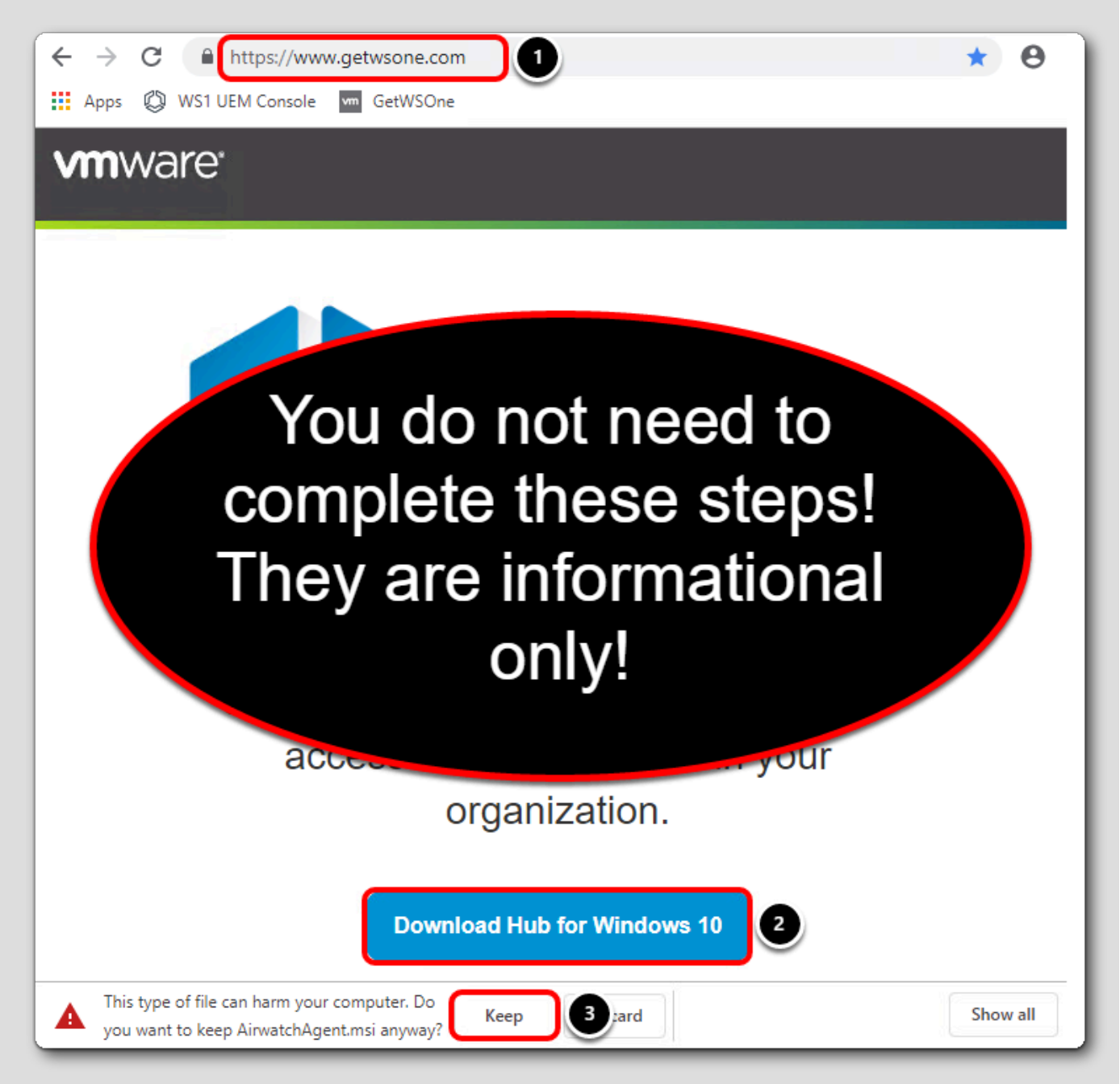
基本アカウントを使用した Windows 10 デバイスの登録

[696]

次に、Workspace ONE Intelligent Hub アプリケーションを使用して、Workspace ONE UEM に Windows 10 デバイスを登録します。

Workspace ONE Intelligent Hub アプリケーションのダウンロード

[697]



注：これらの手順を実行する必要はありません。Workspace ONE Intelligent Hub はすでにダウンロードされています。この手順は単なる情報です。

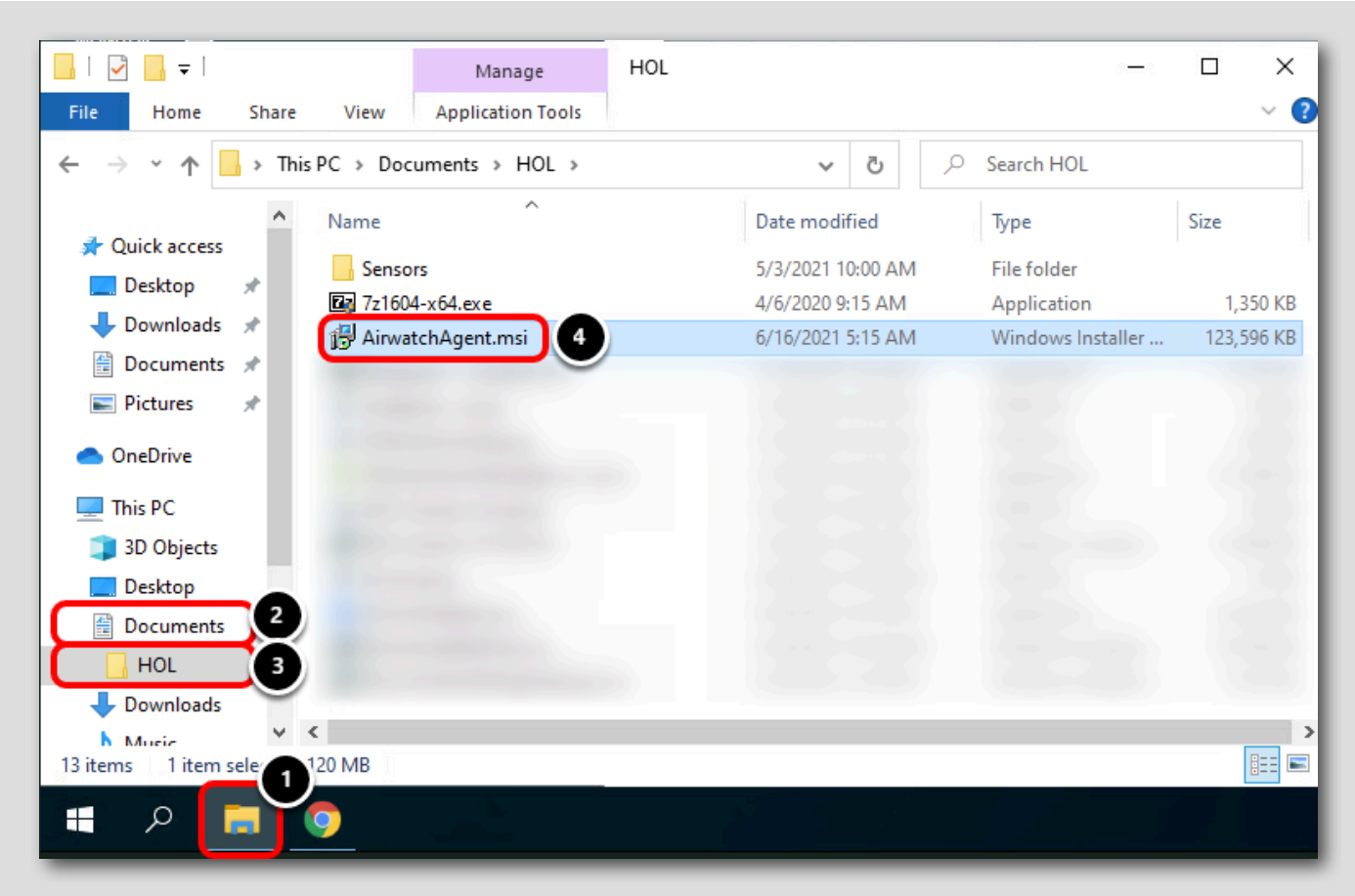
次の手順に従って、現在のプラットフォーム用の最新の Workspace ONE Intelligent Hub アプリケーションをダウンロードできます。

1. ブラウザで **`https://www.getwsone.com`** に移動します。
2. [Download Hub for Windows 10] をクリックします。
3. AirWatchAgent.msi のダウンロードについて警告が表示されたら、[Keep] をクリックします。

便宜上、Workspace ONE Intelligent Hub アプリケーションはすでにダウンロードされています。次の手順に進んで、インストーラを起動します。

Workspace ONE Intelligent Hub インストーラの起動

[698]

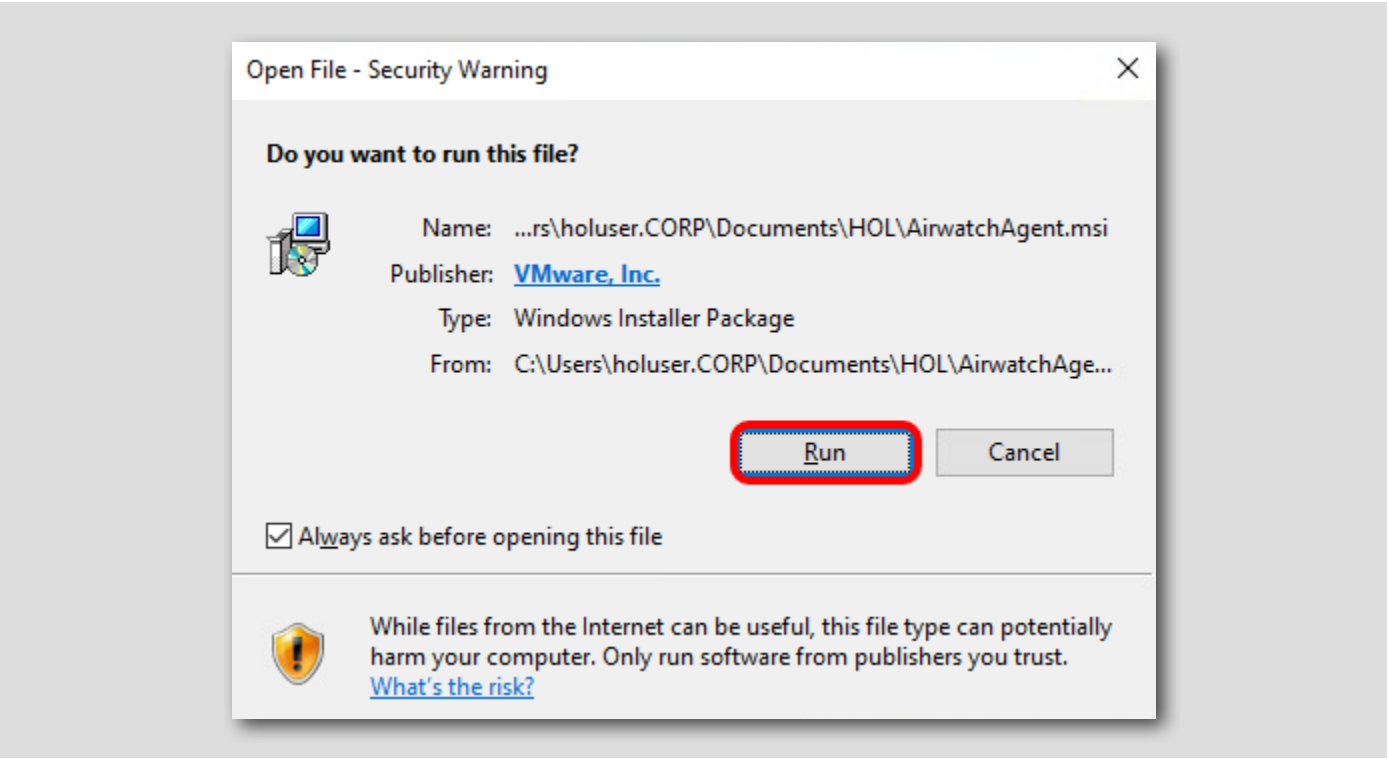


1. タスクバーの [File Explorer] アイコンをクリックします。
2. [Documents] をクリックします。
3. [HOL] をクリックします。
4. AirwatchAgent.msi ファイルをダブルクリックして、インストーラを起動します。

注：インストーラが起動するまでに数秒かかる場合があります。AirwatchAgent.msi ファイルをクリックして、しばらくお待ちください。

[Run] のクリック

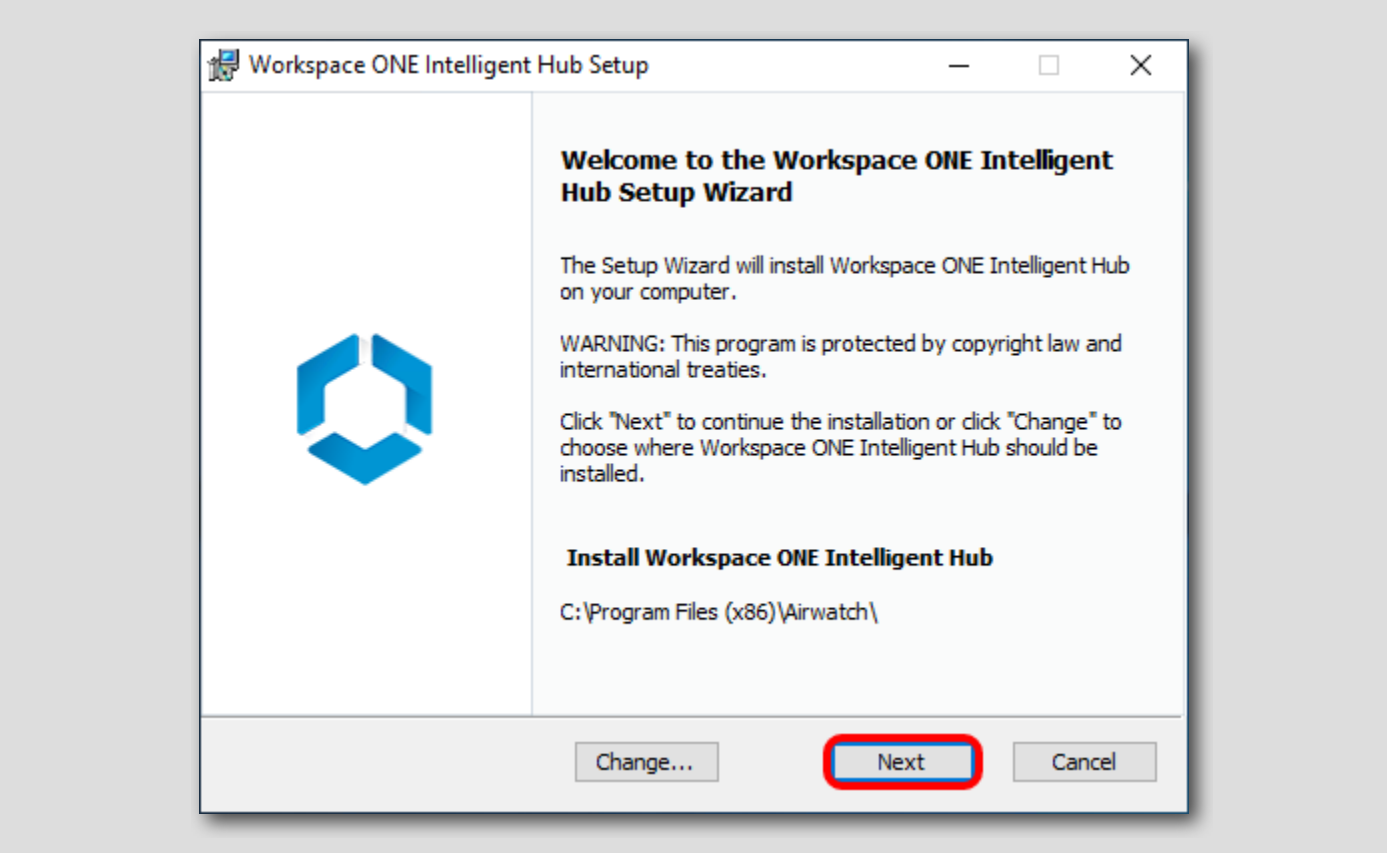
[699]



[Run] をクリックして、インストールを続行します。

デフォルトのインストール場所の受け入れ

[700]

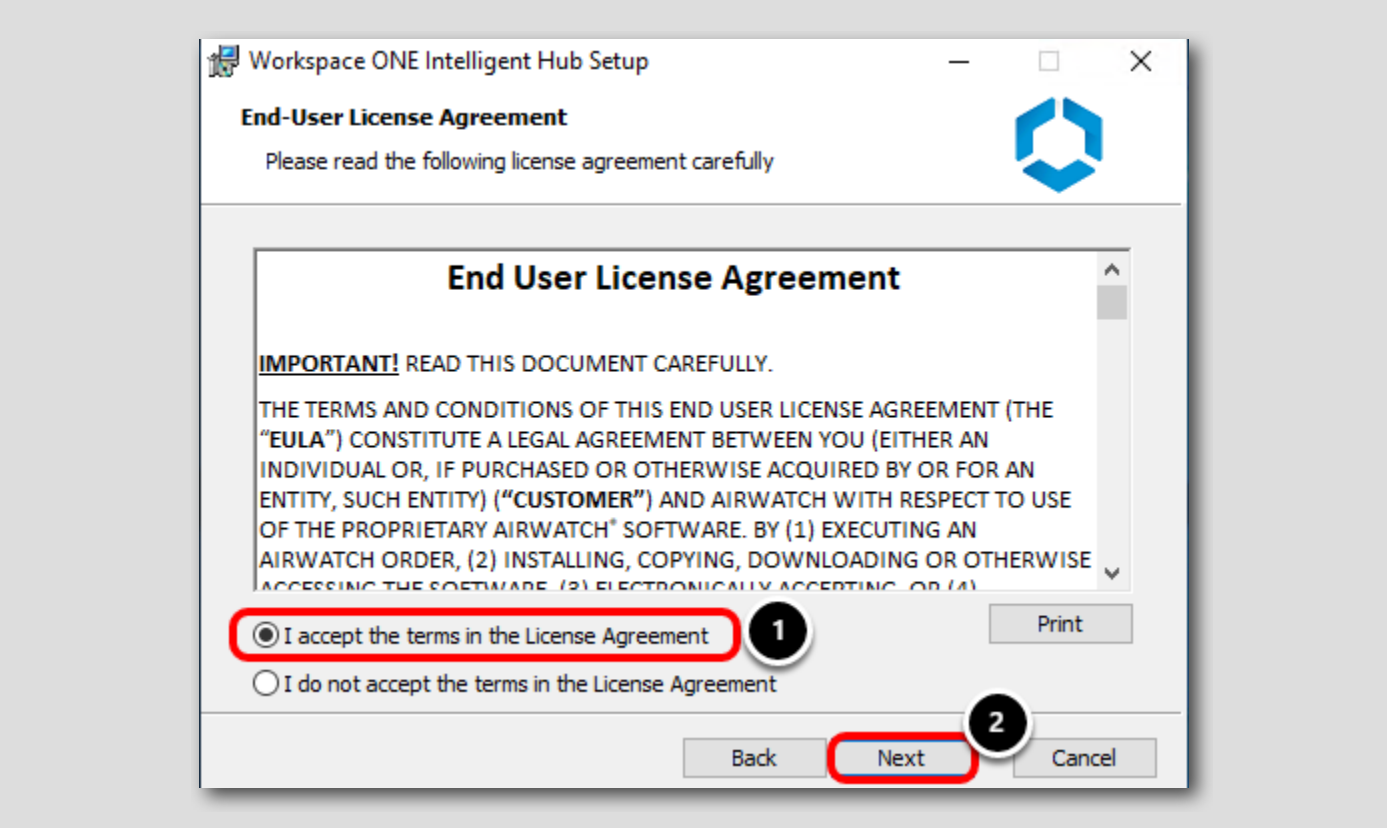


インストール場所はデフォルトのまま、[Next] をクリックします。

注：必要な追加機能がインストールされ、[Next] ボタンが有効になるまで数秒かかる場合があります。

使用許諾契約書への同意

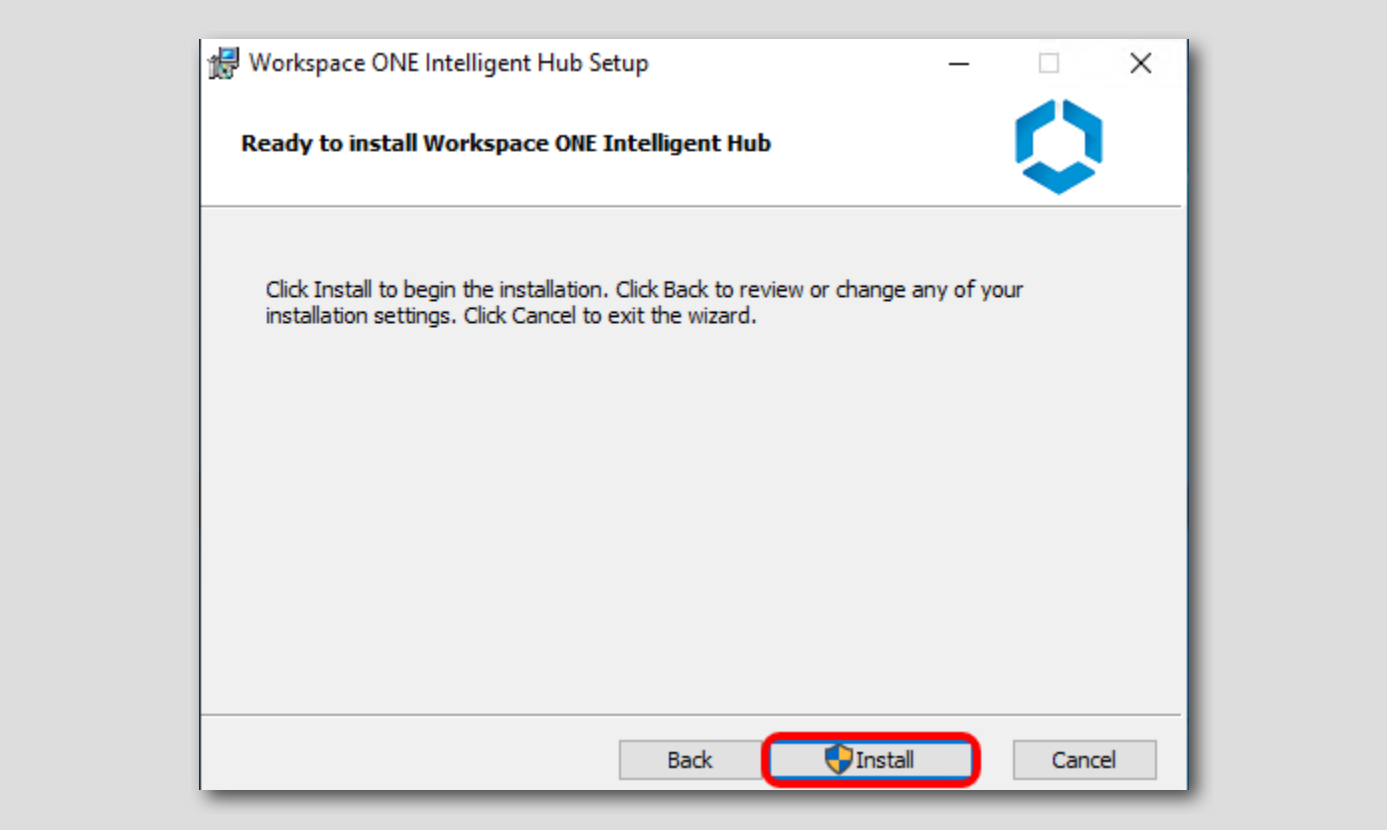
[701]



1. [I accept the terms of the License Agreement] を選択します。
2. [Next] をクリックします。

Workspace ONE Intelligent Hub のインストールの開始

[702]

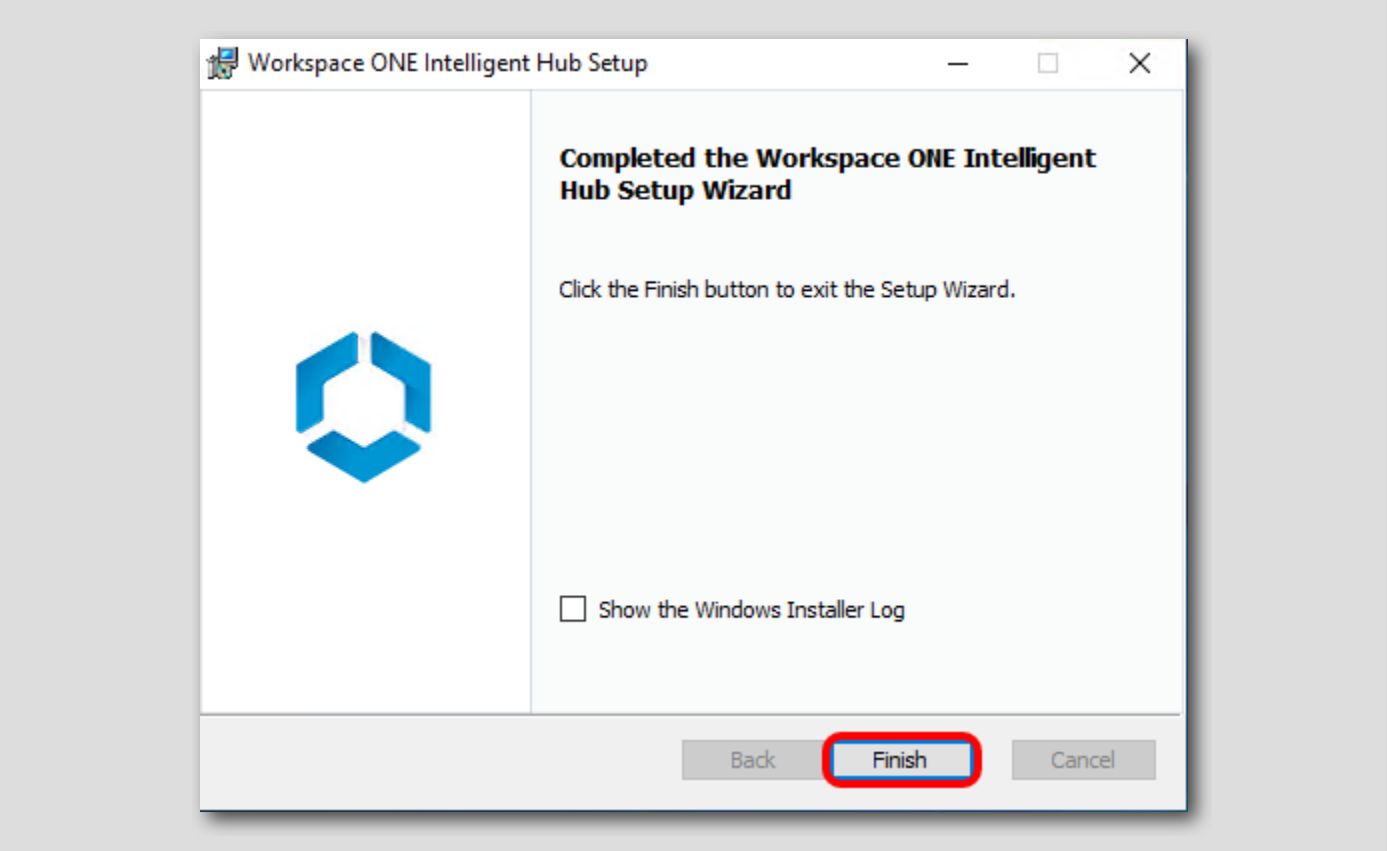


[Install] をクリックして、インストーラを開始します。

注：VMware Workspace ONE Intelligent Hub のインストールは完了までに数分かかる場合があります。インストーラを中断しないようにしてください。

Workspace ONE Intelligent Hub インストーラの完了

[703]



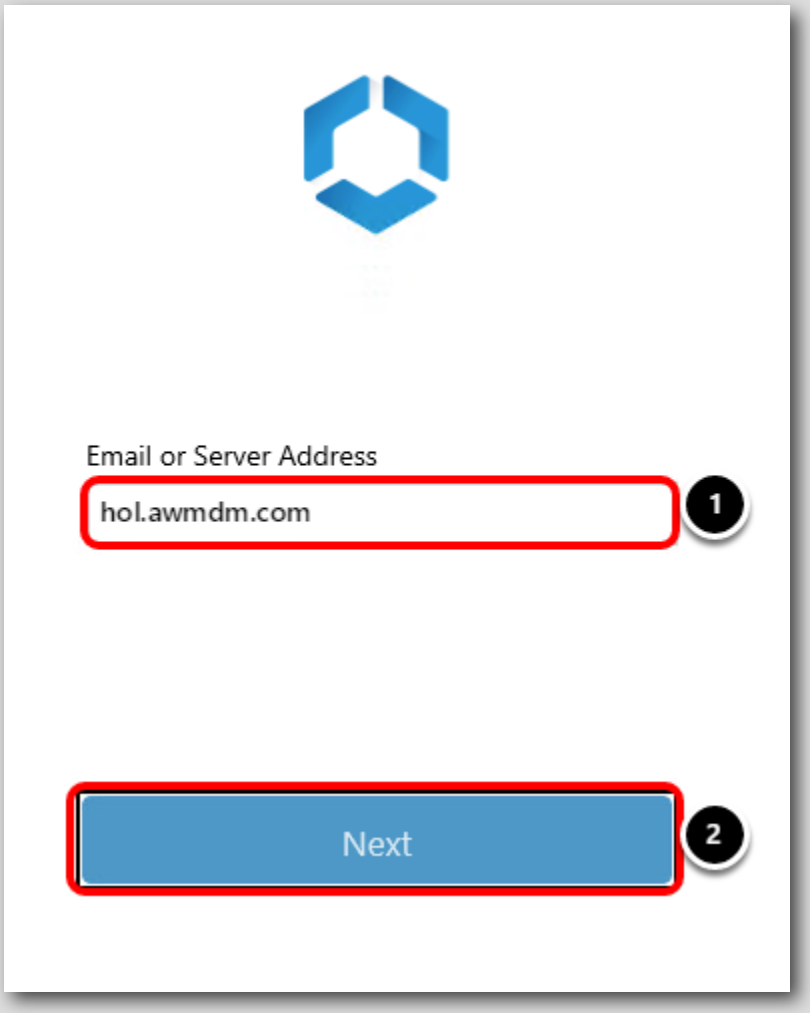
注：インストーラの完了には数分かかる場合があります。続行する前に、インストールの完了画面が表示されるまでお待ちください。

[Finish] をクリックして、Workspace ONE Intelligent Hub インストーラを完了します。

注：[Finish] をクリックすると Native Enrollment アプリケーションが起動し、Workspace ONE UEM への登録手順が表示されます。Intelligent Hub の起動には、約 2 ～ 3 分かかります。

Workspace ONE Intelligent Hub を使用した Windows 10 デバイスの登録

[704]

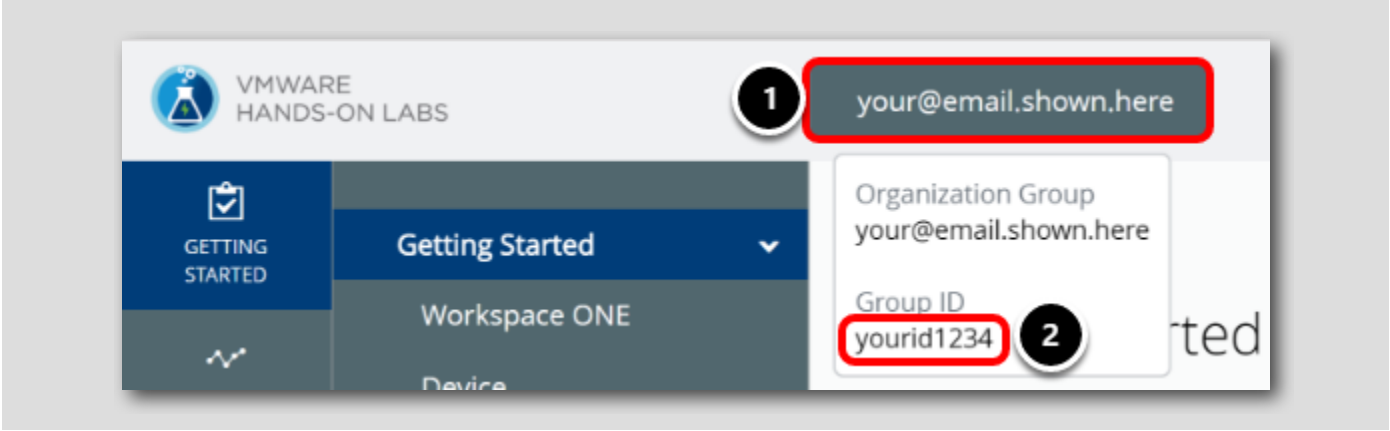


注：前の手順で [Finish] をクリックした後、上記の画面が表示されるまでに 2 ～ 3 分かかることがあります。

1. [Server Address] に **`hol.awmdm.com`** と入力します。
2. [Next] をクリックします。

Workspace ONE UEM Console からのグループ ID の特定

[705]

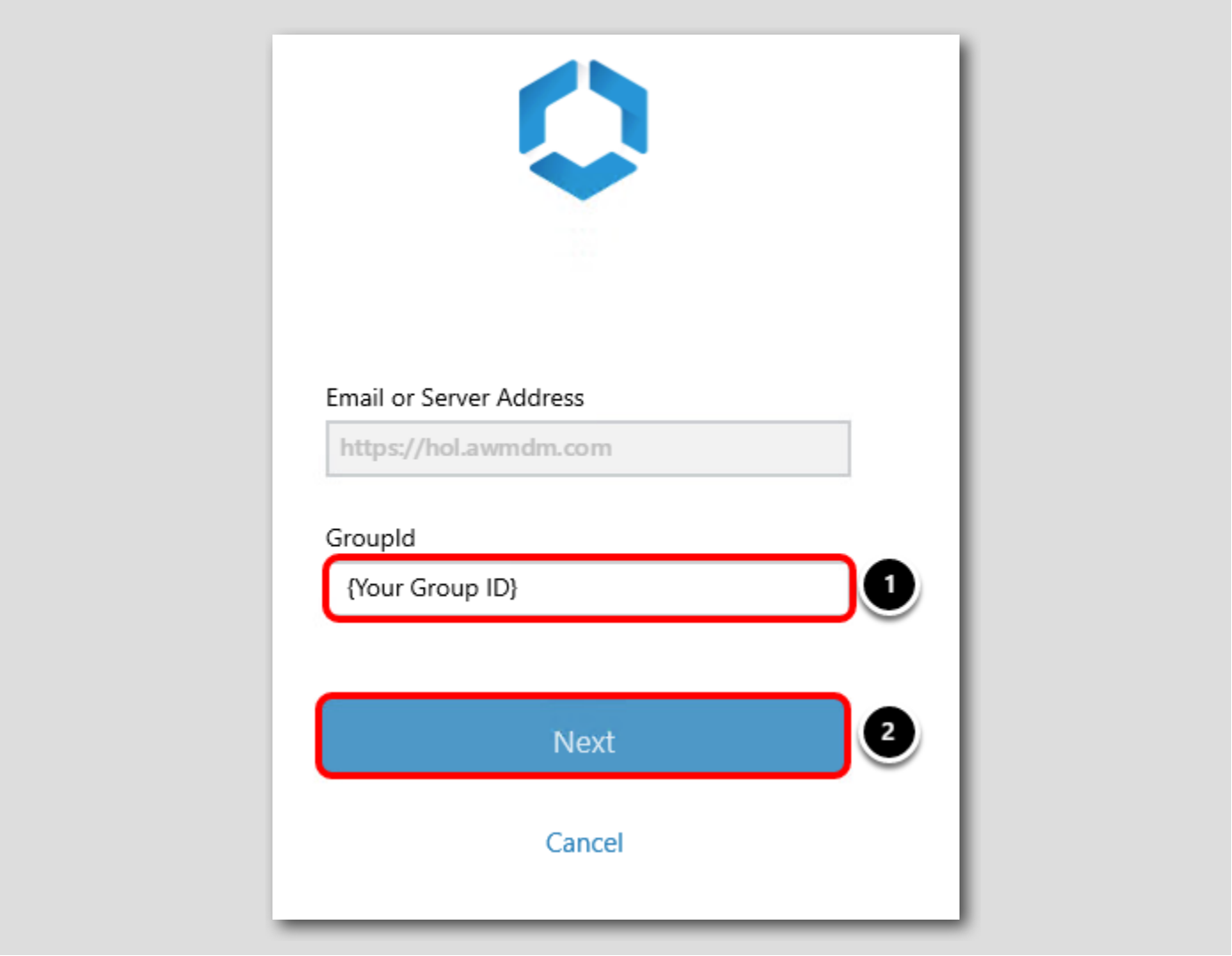


次の手順では、[Organization Group ID] を取得します。

1. グループ ID を確認するには、Workspace ONE UEM 管理コンソールに戻って、画面上部の [Organization Group] タブにカーソルを合わせます。ラボ ポータルへのログインに使用したメール アドレスを探します。
2. グループ ID は [Organization Group] ポップアップの最下部に表示されます。この値をコピーします。

グループ ID の入力

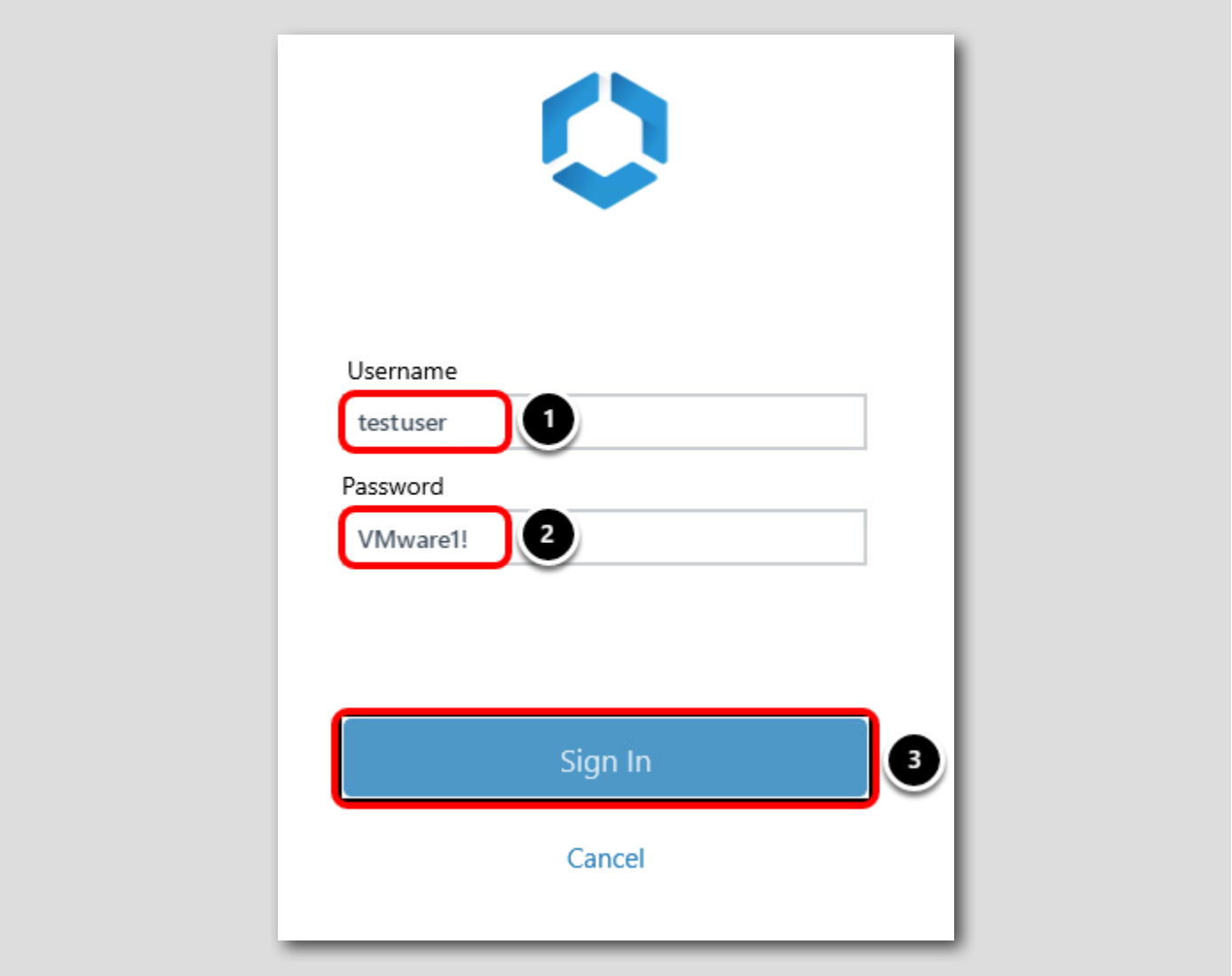
[706]



1. [Group ID] フィールドにグループ ID を入力します。グループ ID を忘れた場合は、前の手順で取得方法を確認してください。
2. [Next] をクリックします。

ユーザー認証情報の入力

[707]

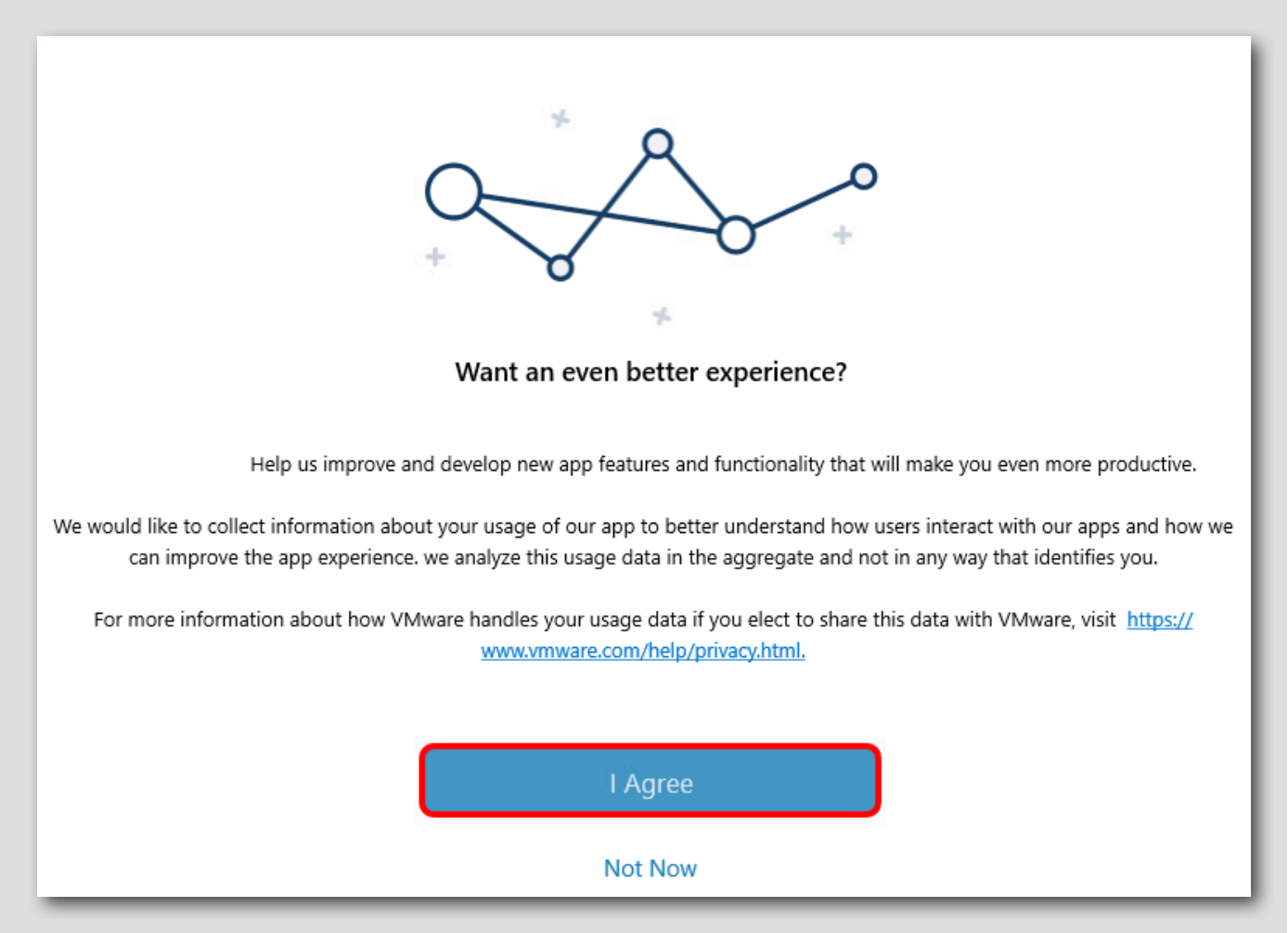


1. [Username] フィールドに **testuser** と入力します。
2. [Password] フィールドに **VMware1!** と入力します。
3. [Sign In] をクリックします。

注：サーバが登録の詳細を確認するまでしばらくお待ちください。これには数分かかる場合があります。

データ ポリシーの承諾

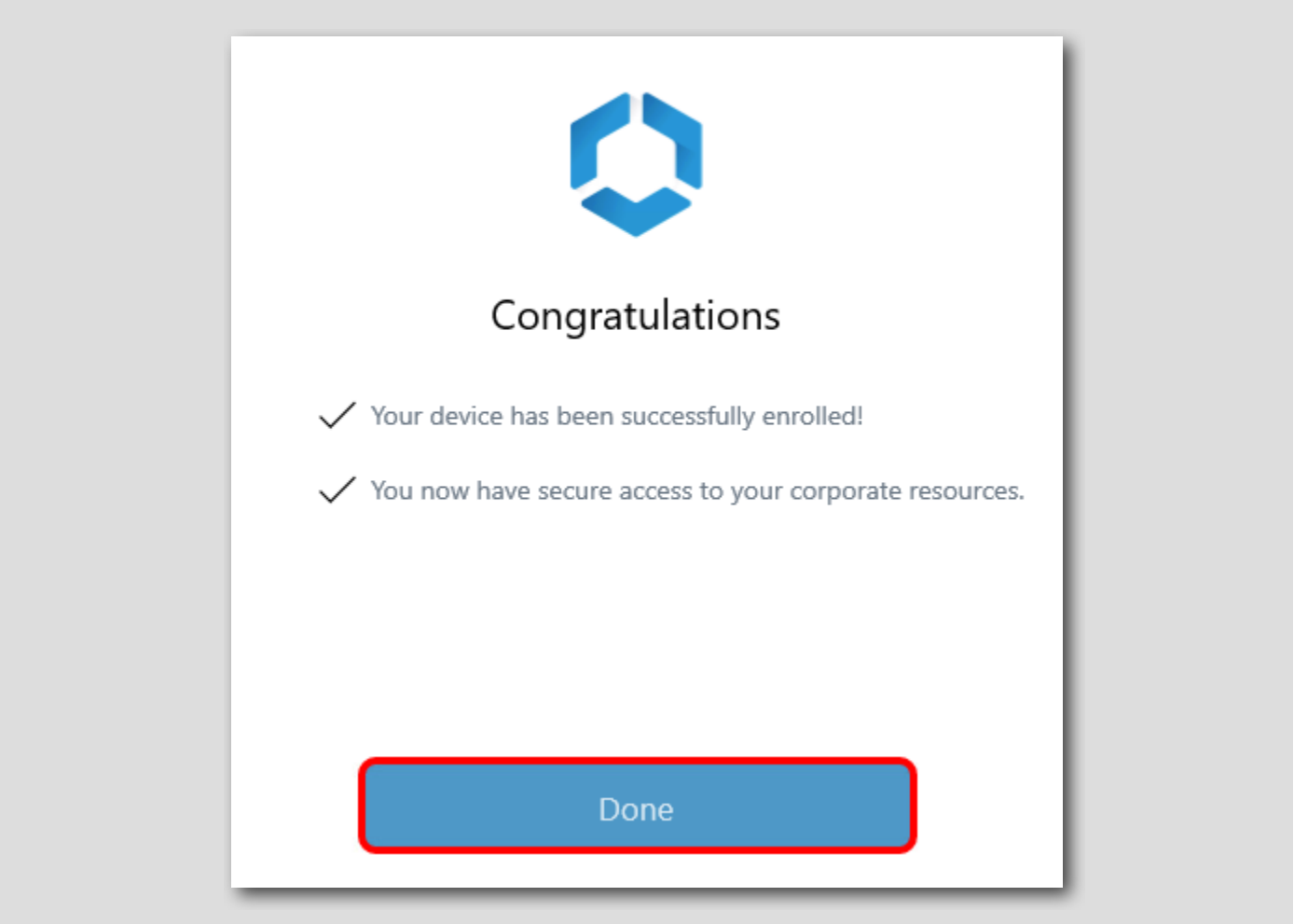
[708]



[I Agree] をクリックします。

Workspace ONE UEM 登録プロセスの終了

[709]



[Done] をクリックして登録プロセスを終了します。これで、Windows 10 デバイスは Workspace ONE UEM に正常に登録されました。

Tunnel トラフィック ルールの構成

[710]

管理者が SASE PoP からホストされている Workspace ONE Tunnel サービスを Workspace ONE UEM に統合する場合、次の手順を実行します。

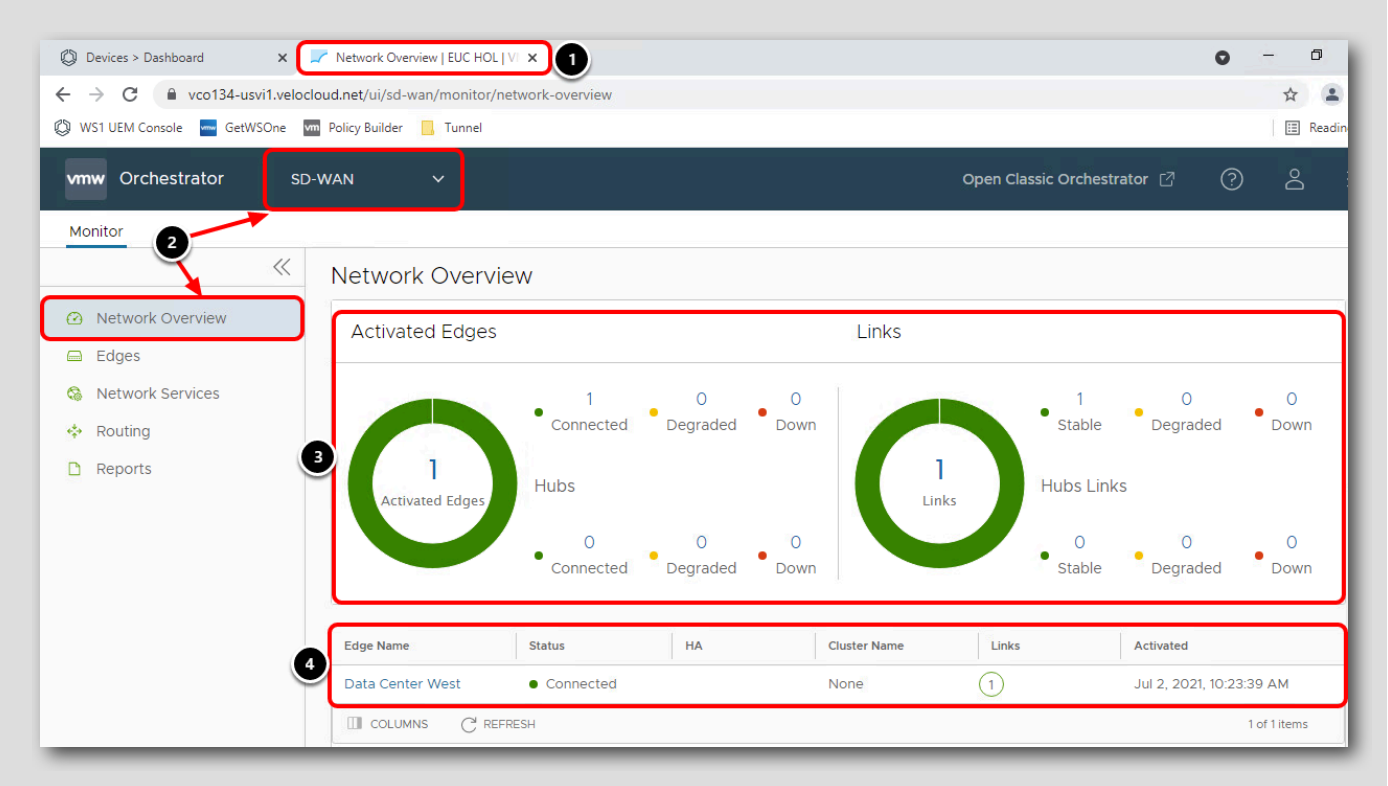
1. SD-WAN Network Orchestrator にログインします。
2. Secure Access に移動し、Secure Access ポリシーを構成し、Tunnel サービスの DNS 名、Workspace ONE UEM 統合の詳細、および Tunnel サービスが使用する DNS サーバを指定します。
3. Workspace ONE UEM 管理者コンソールにログインします。
4. Tunnel 統合画面に移動し、SASE PoP でホストされる Tunnel サービスと同じ DNS 名と適切なポートを構成します。

5. トンネル トラフィック ルールを構成して、デバイス上で Tunnel サービスをトンネリング、プロキシ、またはバイパスするトラフィックを決定します。

このラボでは、時間の都合で、Secure Access ポリシーと Workspace ONE Tunnel の統合が行われました。SD-WAN Network Orchestrator コンソールと Workspace ONE UEM の Workspace ONE Tunnel 設定の両方に**読み取り専用アクセス権**が付与されます。このプロセスの手順を実行して、構成について理解し、セットアップ内容を確認します。

SD-WAN Network Orchestrator での Secure Access 設定の確認

[711]

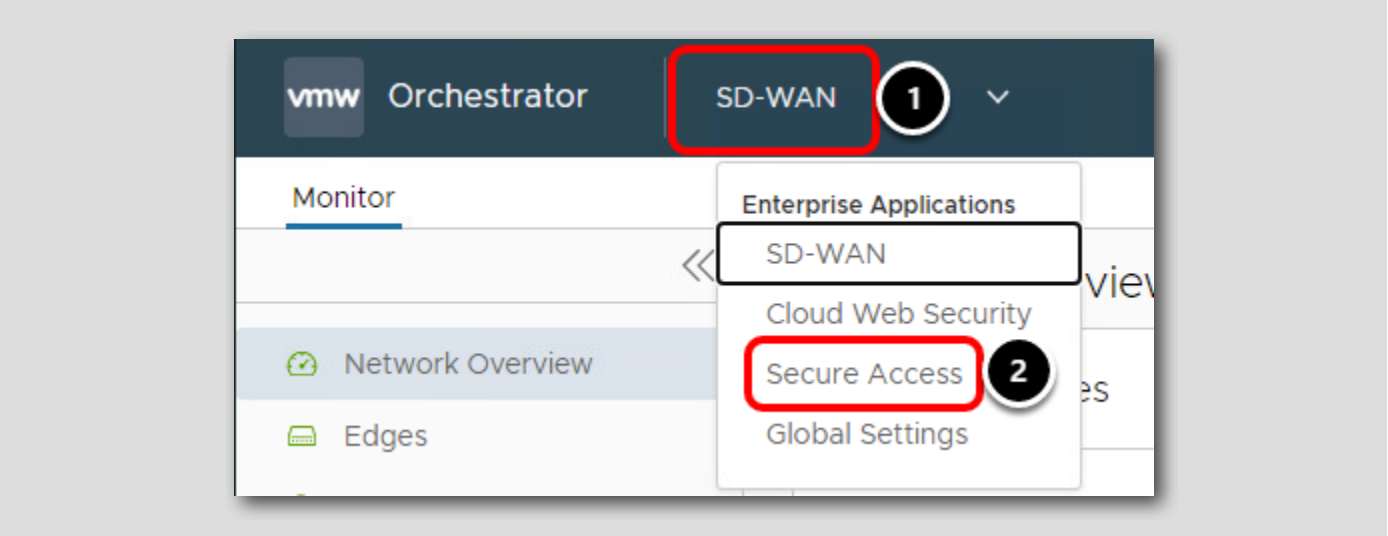


Google Chrome で、次のように操作します。

1. [SD-WAN Network Orchestrator] タブをクリックします。
2. デフォルトのランディング ページは、[SD-WAN] > [Network Overview] ページです。
3. このページには、アクティベーションされた Edge とリンクの数とそれぞれの健全性ステータスが表示されます。
4. Edge の詳細については、ここで参照できます。このラボでは、Edge をオンプレミス データセンターに展開して、SD-WAN 経由でイントラネット Web サイトにアクセスできるようにします。

[Secure Access] ページへの移動

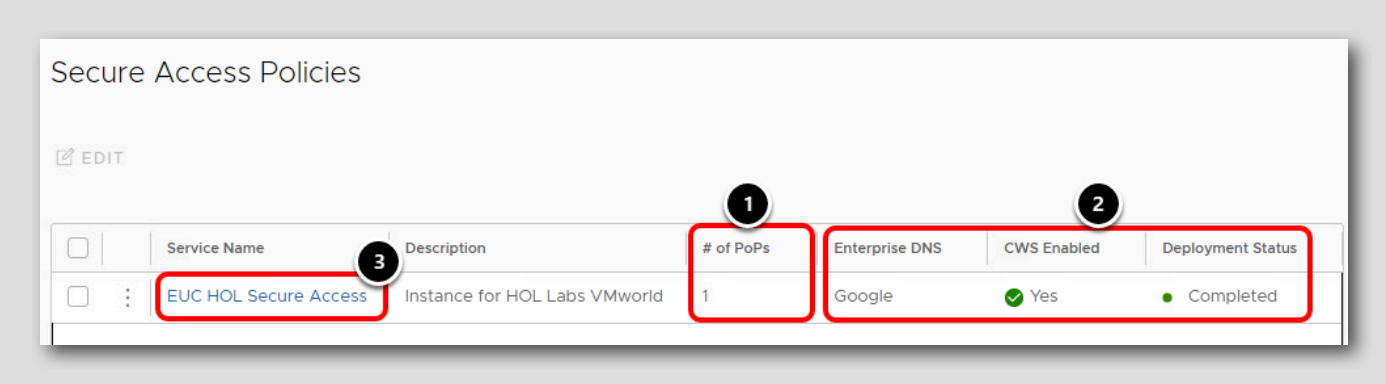
[712]



1. 現在 SD-WAN が表示されている [Enterprise Applications] ドロップダウンをクリックします。
2. [Secure Access] をクリックします。

Secure Access 設定の表示

[713]

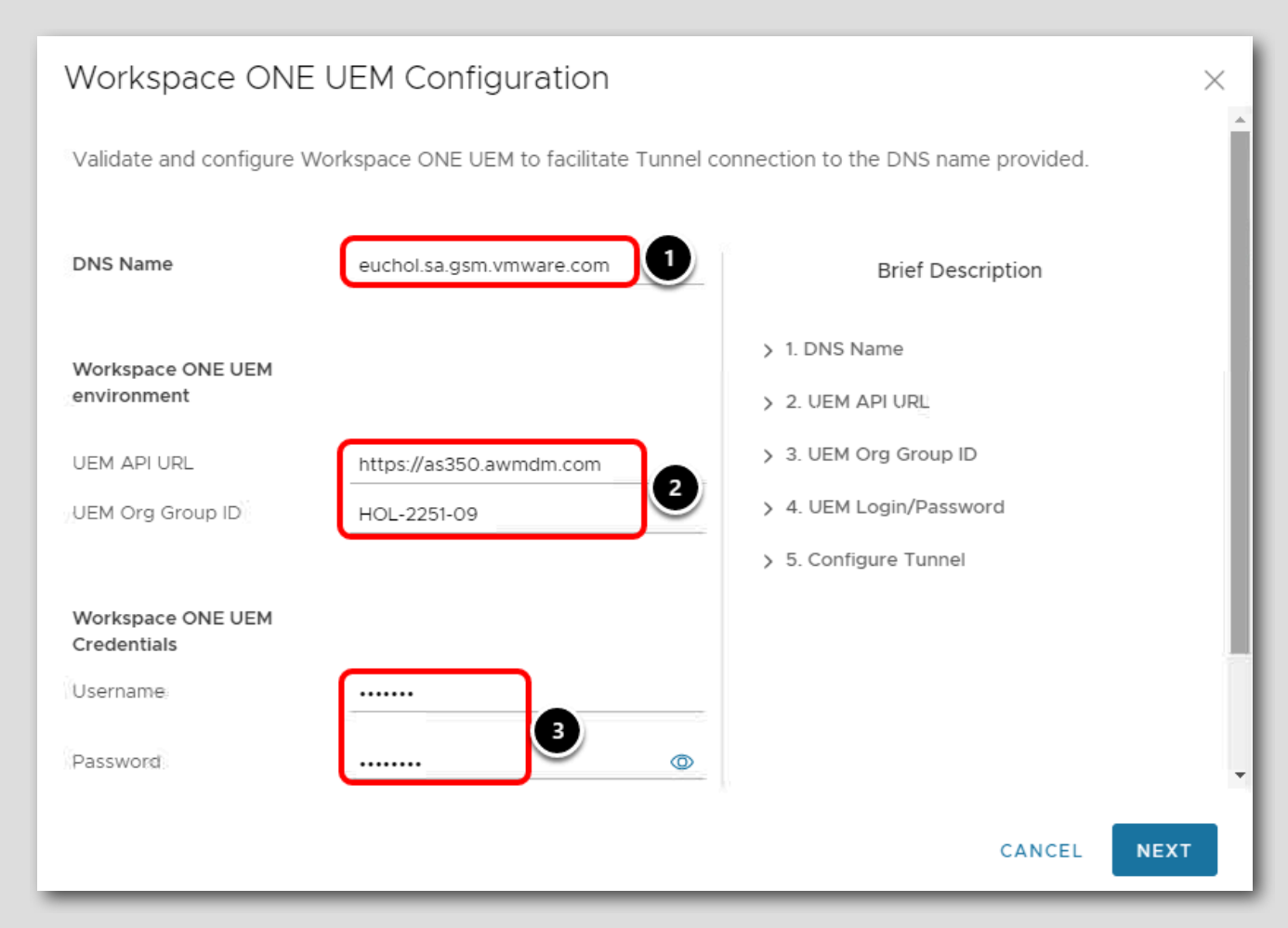


[Secure Access Policies] ページには、Secure Access クライアントのリストが表示されます。

1. [EUC HOL Secure Access] サービスの [# of PoPs] が 1 であることを確認します。SD-WAN には 1 つ以上の PoP を設定できます。
2. CWS (Cloud Web Security) ポリシーが有効になっている場合のエンタープライズ DNS 設定、展開ステータスなど、Secure Access クライアントに関する追加情報はここで確認できます。
3. [EUC HOL Secure Access] リンクをクリックします。

Workspace ONE UEM 構成

[714]

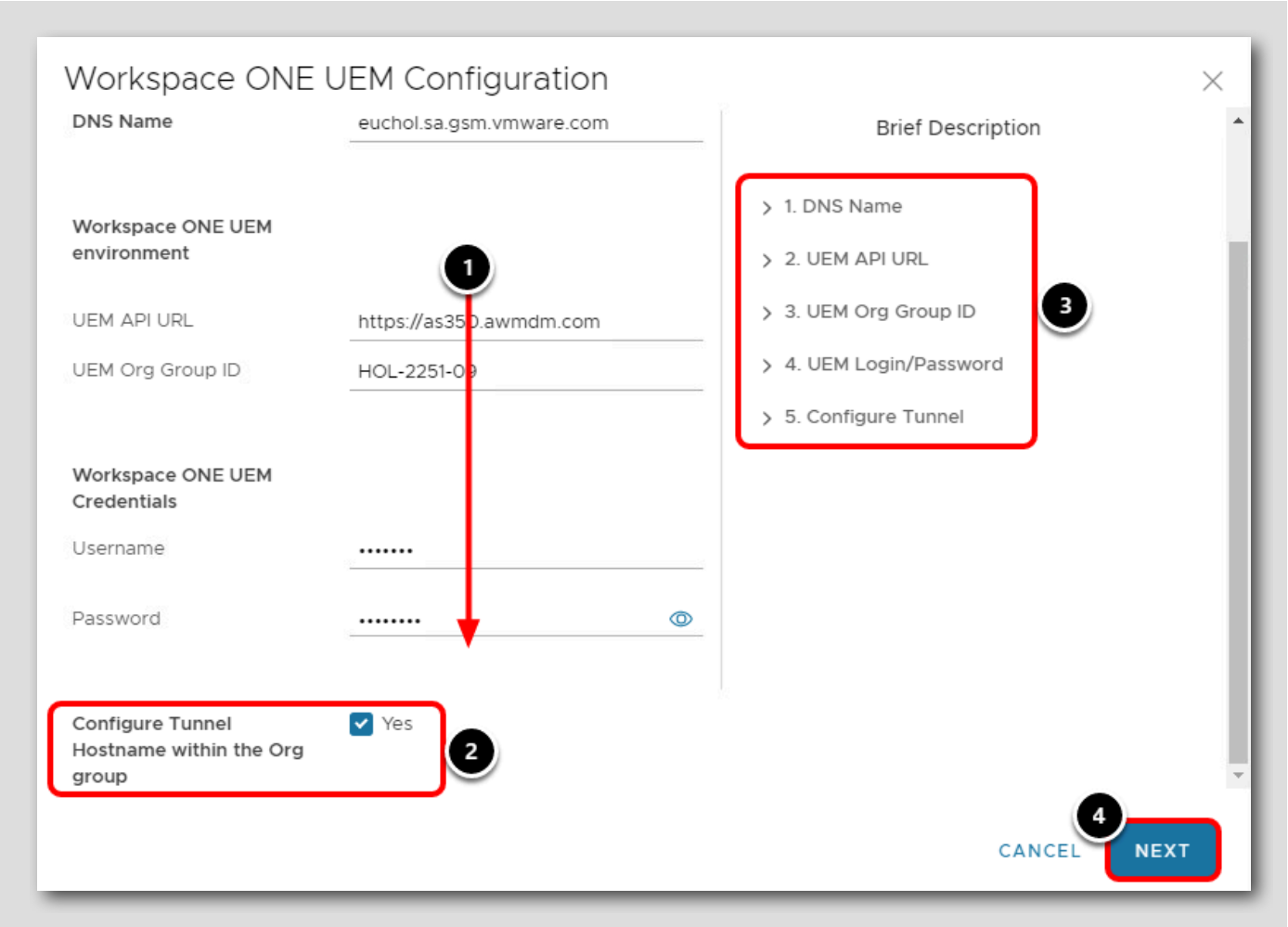


1. [DNS Name] フィールドは、Workspace ONE Tunnel サービスがホストされているエンドポイントを示します。
2. Workspace ONE Tunnel を統合する Workspace ONE UEM API URL と組織グループ ID はここで指定できます。

   注：このセットアップでは、Workspace ONE Tunnel はすでに親組織グループの Workspace ONE UEM と統合されており、設定は子グループによって継承されています。
3. Workspace ONE UEM REST API を認証できる Workspace ONE UEM 管理者認証情報はここで指定できます。

Workspace ONE UEM 構成（続き）

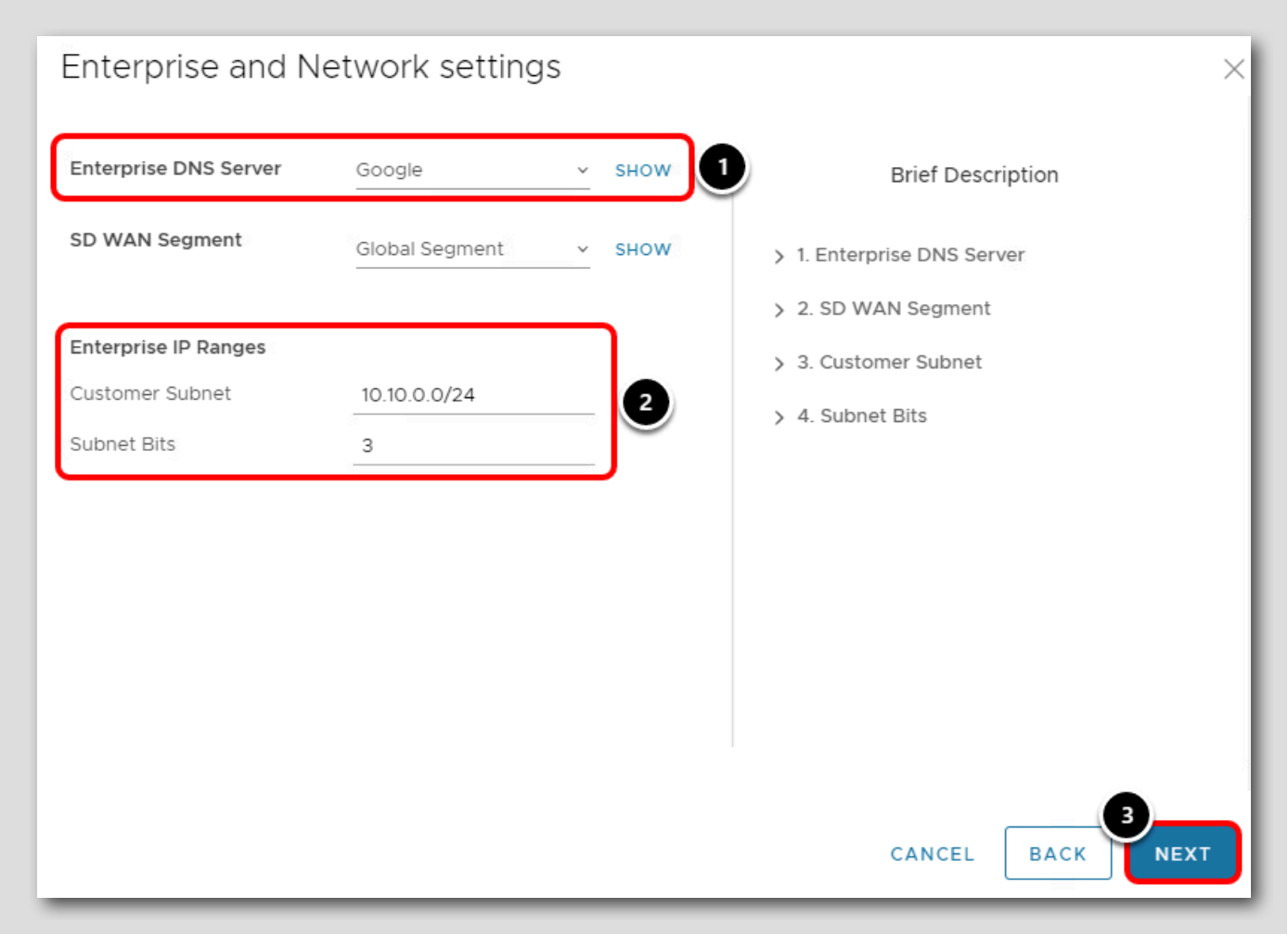
[715]



1. [Workspace ONE UEM Configuration] セクションの一番下までスクロールします。
2. [Configure Tunnel Hostname within the Org Group] トグルを使用すると、指定された API URL、グループ ID、および管理者認証情報を使用して Workspace ONE UEM で Workspace ONE Tunnel ホスト名が自動的に設定されるため、管理者は Tunnel 接続の詳細を手動で構成する必要はありません。
3. [Brief Description] タブを展開して、各セットアップ手順の詳細を確認できます。
4. [Next] をクリックします。

エンタープライズとネットワークの設定

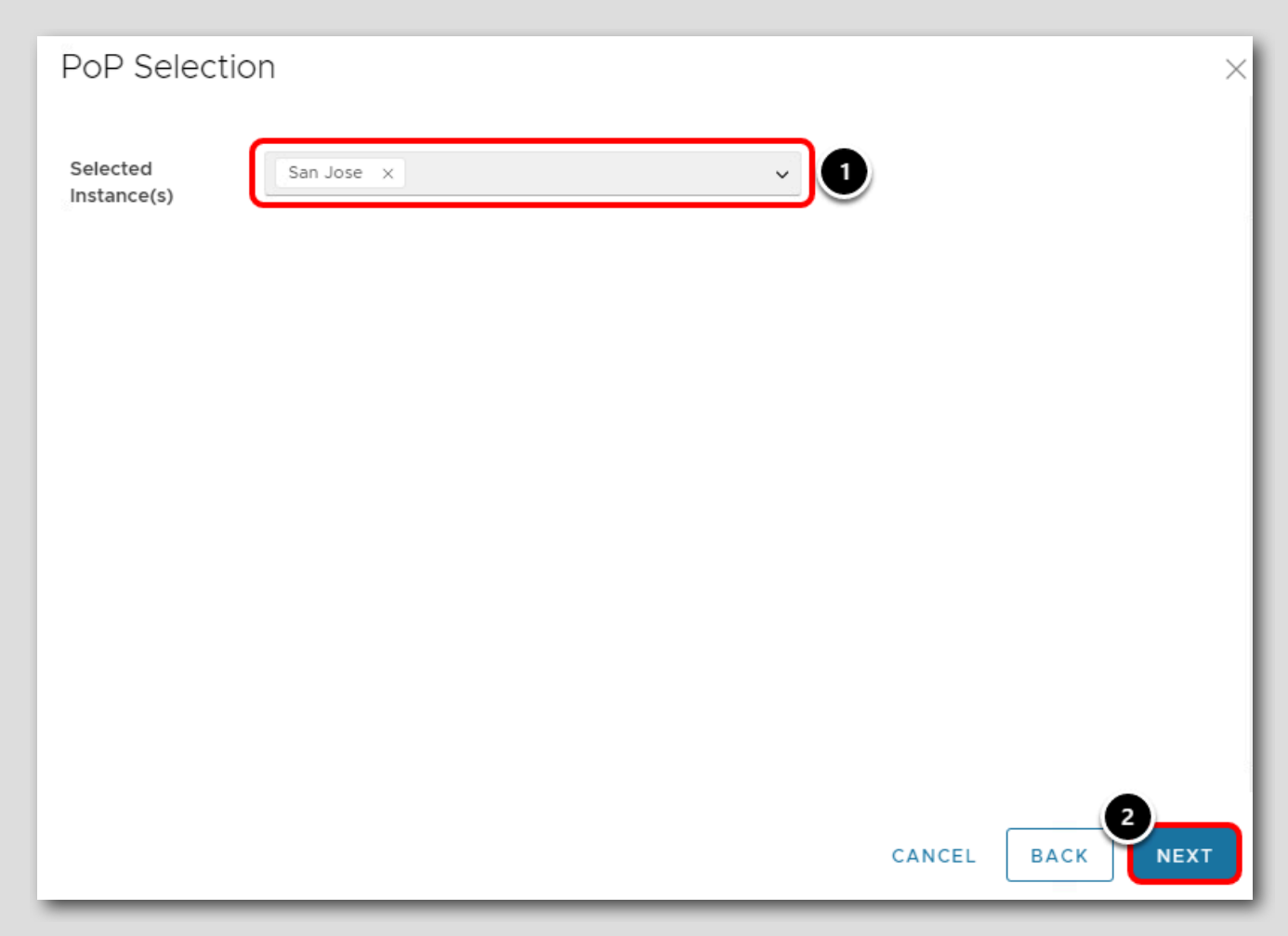
[716]



1. Secure Access クライアントが使用する [Enterprise DNS Server] は Google に設定されます（DNS 8.8.8.8、8.8.4.4 を使用）。ネットワークのニーズに合わせて、他のパブリックまたはプライベート DNS サーバを構成し、ここに指定することができます。
2. [Enterprise IP Ranges] は、すべての PoP のすべての Secure Access ユーザーに適用されるスーパーネットを示します。
3. [Next] をクリックします。

PoP (Point of Presence) の選択

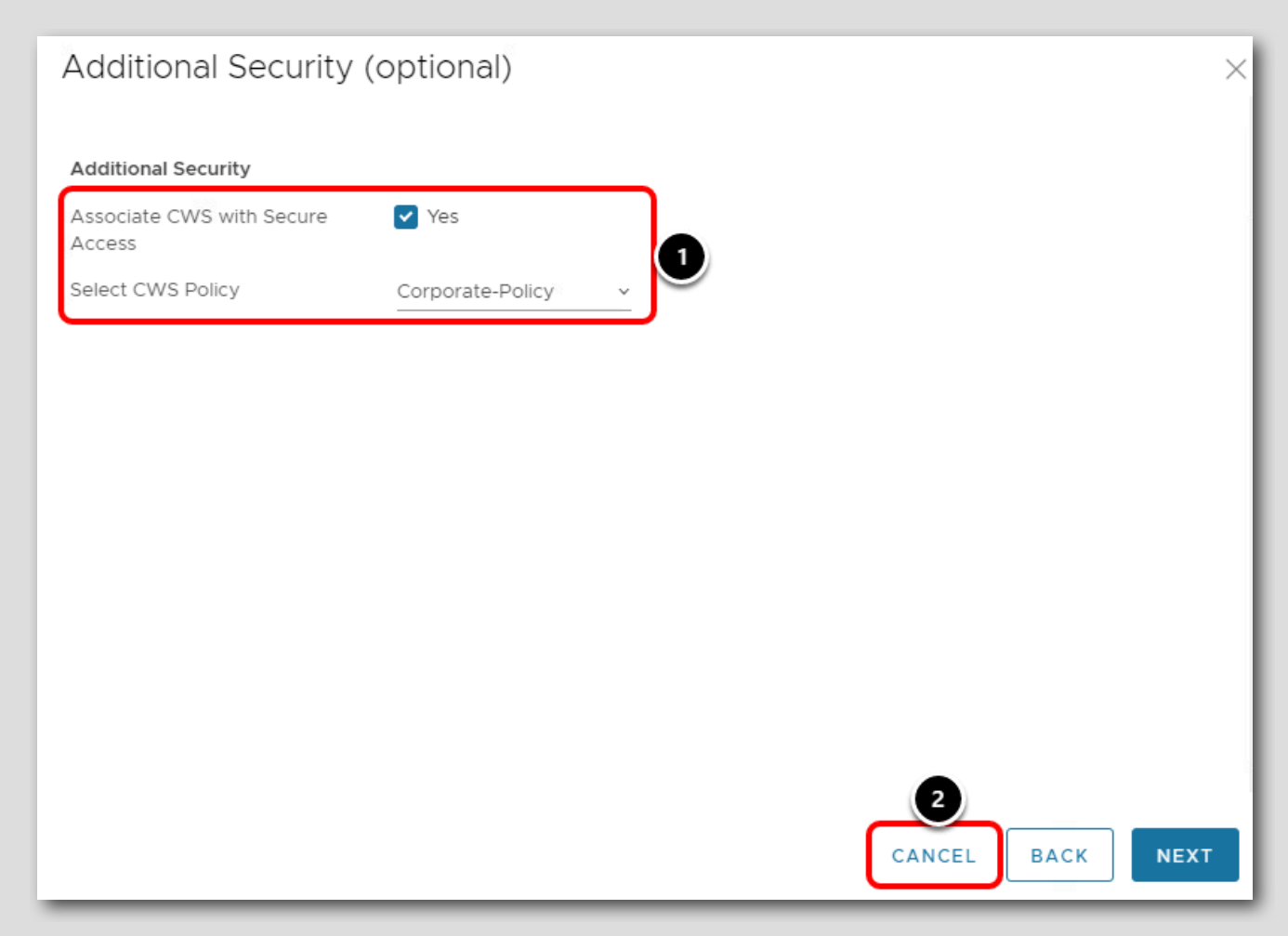
[717]



1. [Selected Instances] には、この Secure Access 展開に参加している PoP が表示されます。この場合、サンノゼの PoP が 1 つ提供されています。
2. [Next] をクリックします。

追加のセキュリティ設定

[718]

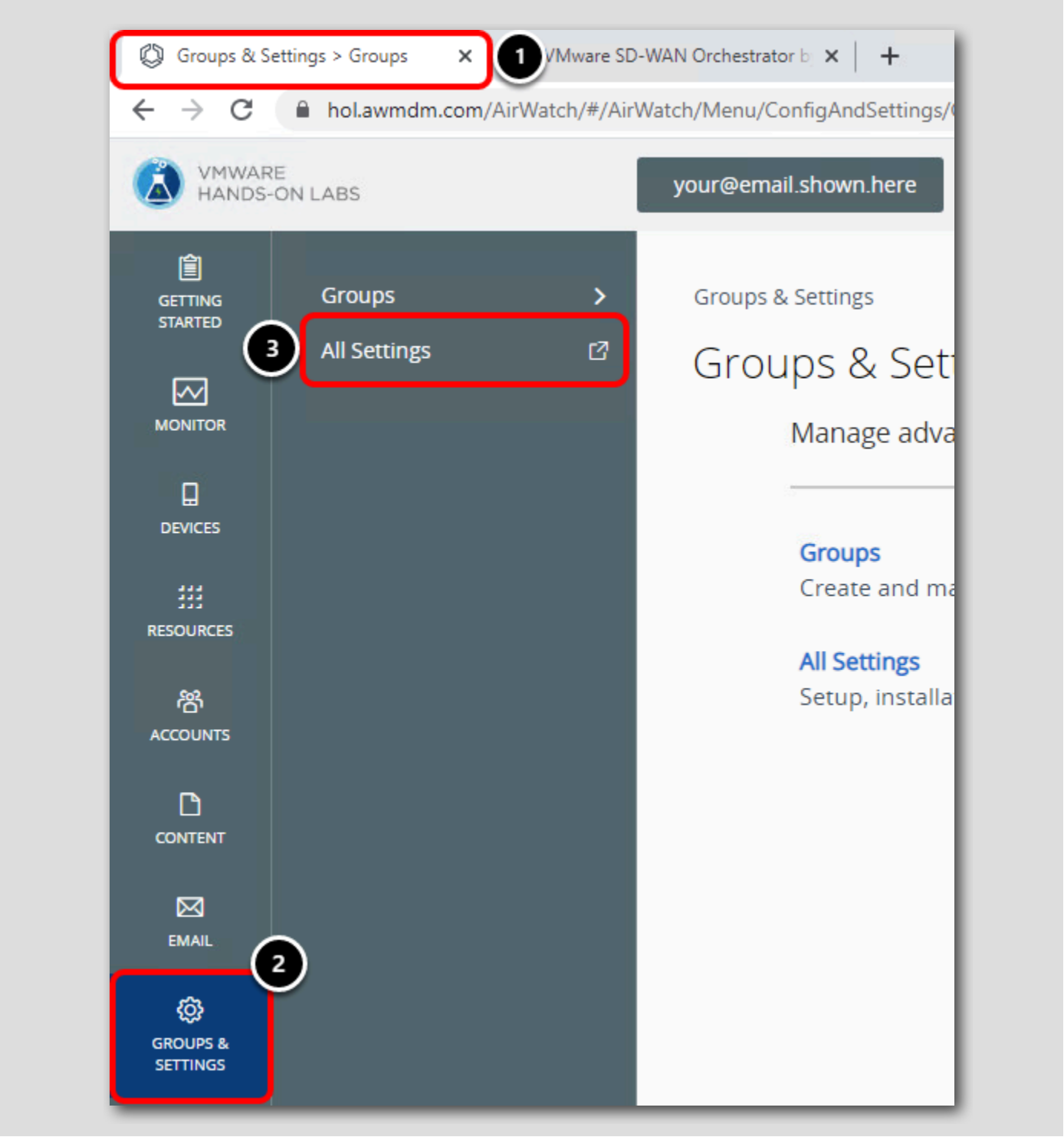


1. [Additional Security] 設定を使用すると、この Secure Access 展開に適用される Cloud Web Security (CWS) ポリシーを指定できます。このセットアップでは、Corporate-Policy CWS ポリシーが関連付けられます。次のステップでは、これらの設定を調べて、Cloud Web Security ポリシーについて詳しく学習します。
2. [Cancel] をクリックして、[Secure Access] 構成を閉じます。

Secure Access 展開と単一の PoP がどのように構成されているかを確認したので、Workspace ONE UEM 管理者コンソールに戻り、Workspace ONE Tunnel 統合設定を確認します。

[719]

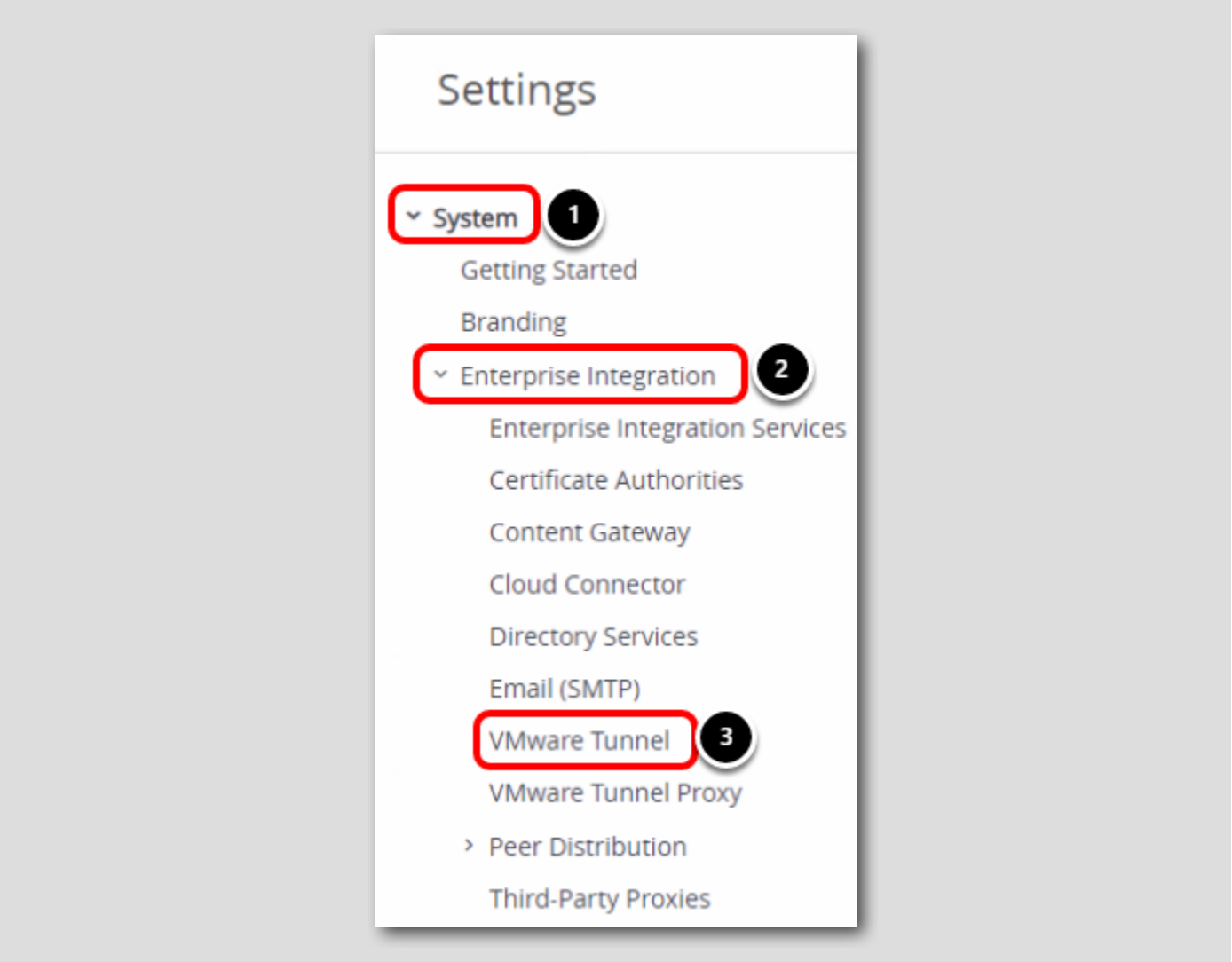
Tunnel 構成を開く



1. 最初のタブをクリックして、Workspace ONE UEM 管理者コンソールに戻ります。
2. [Groups & Settings] をクリックします。
3. [All Settings] をクリックします。

Tunnel 構成への移動

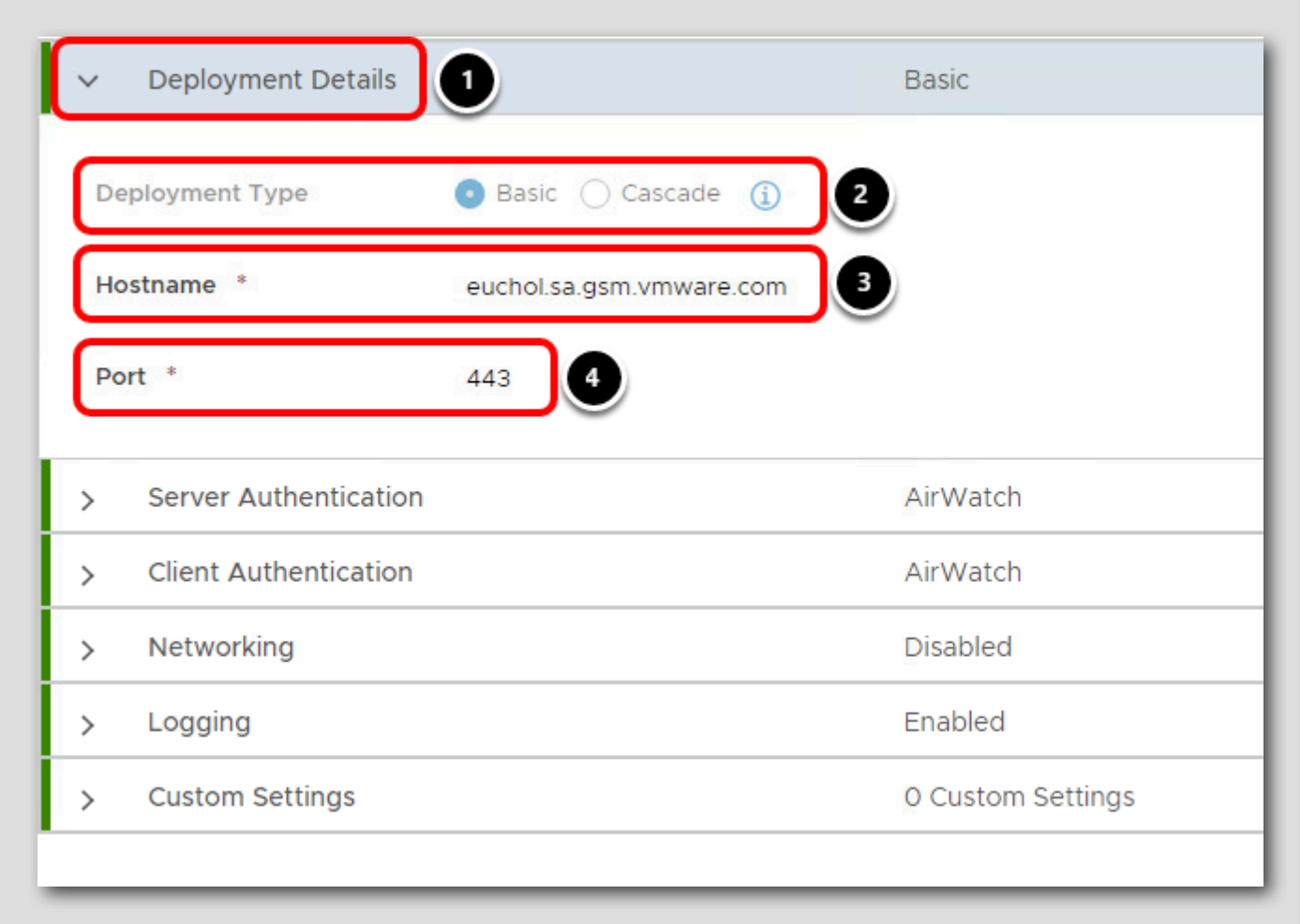
[720]



1. [System] をクリックします。
2. [Enterprise Integration] をクリックします。
3. [VMware Tunnel] をクリックします。

Tunnel 構成の参照

[721]



注：SASE PoP テナントへの Tunnel 構成は、時間の都合ですでにセットアップされています。構成済みの変更を確認して、この実装で使用された設定を理解します。

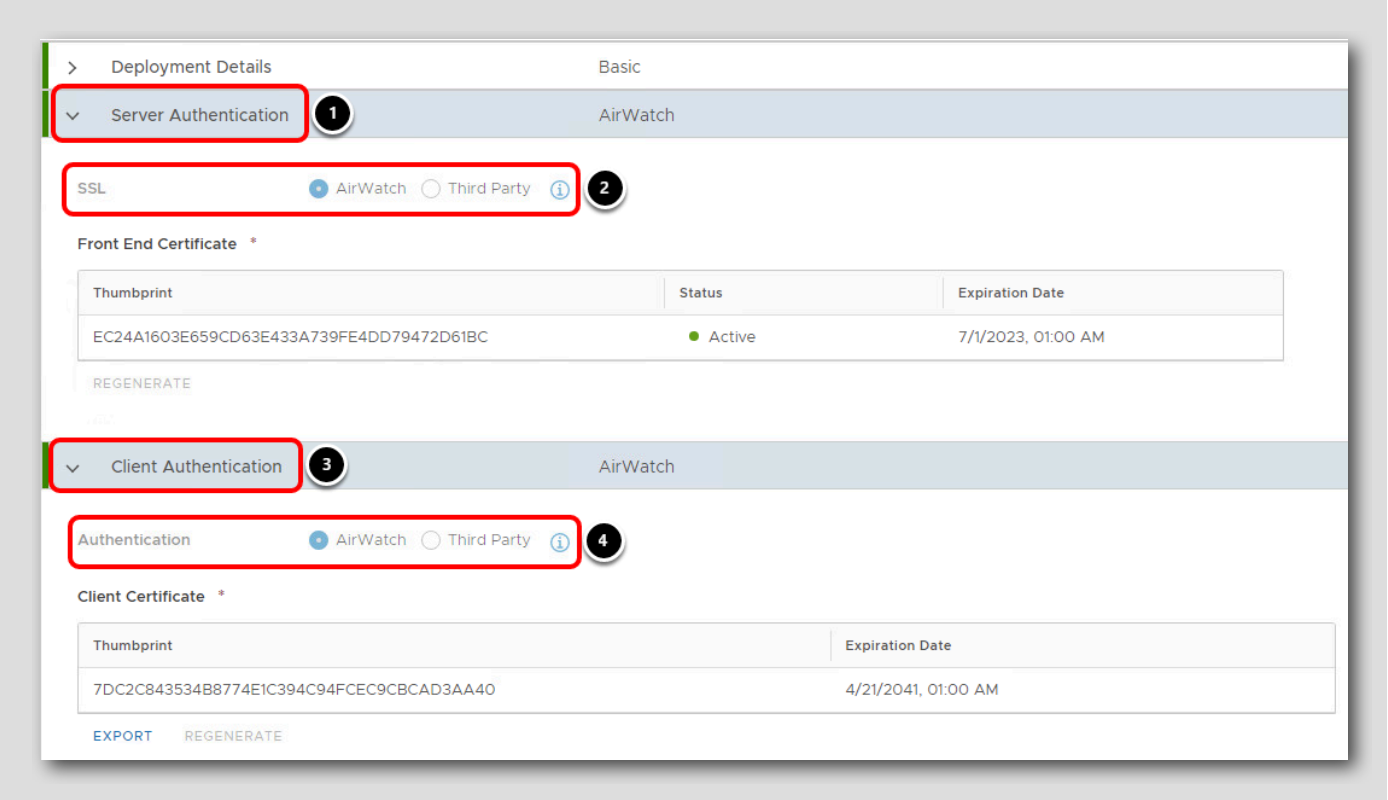
1. [Deployment Details] をクリックして、このセクションを展開します。
2. [Deployment Type] は [Basic] に設定されています。これは、VMware SASE でサポートされている展開タイプです。SASE PoP でカスケード モードを実行する必要はありません。
3. Secure Access サービスの DNS 名は euchol.sa.gsm.vmware.com で、Workspace ONE Tunnel クライアントが Tunnel サービスがホストされている場所を知るために使用されることを思い出してください。[Hostname] は、Tunnel サービスにアクセスできるエンドポイントでなければならず、これは、展開内では euchol.sa.gsm.vmware.com になります。
4. Tunnel サービスをホストする SASE PoP の [Port] は 443 であり、SASE ホスティング ソリューションの一部として提供されます。

このセクションでは、Tunnel サービスへの接続方法を定義します。ラボの Windows 10 仮想マシンは、これらの設定を使用して、ポート 443 の euchol.sa.gsm.vmware.com でホストされている SASE PoP でホストされている Tunnel サービスへの接続を確立します。

次の手順に進んでください。

認証設定の確認

[722]



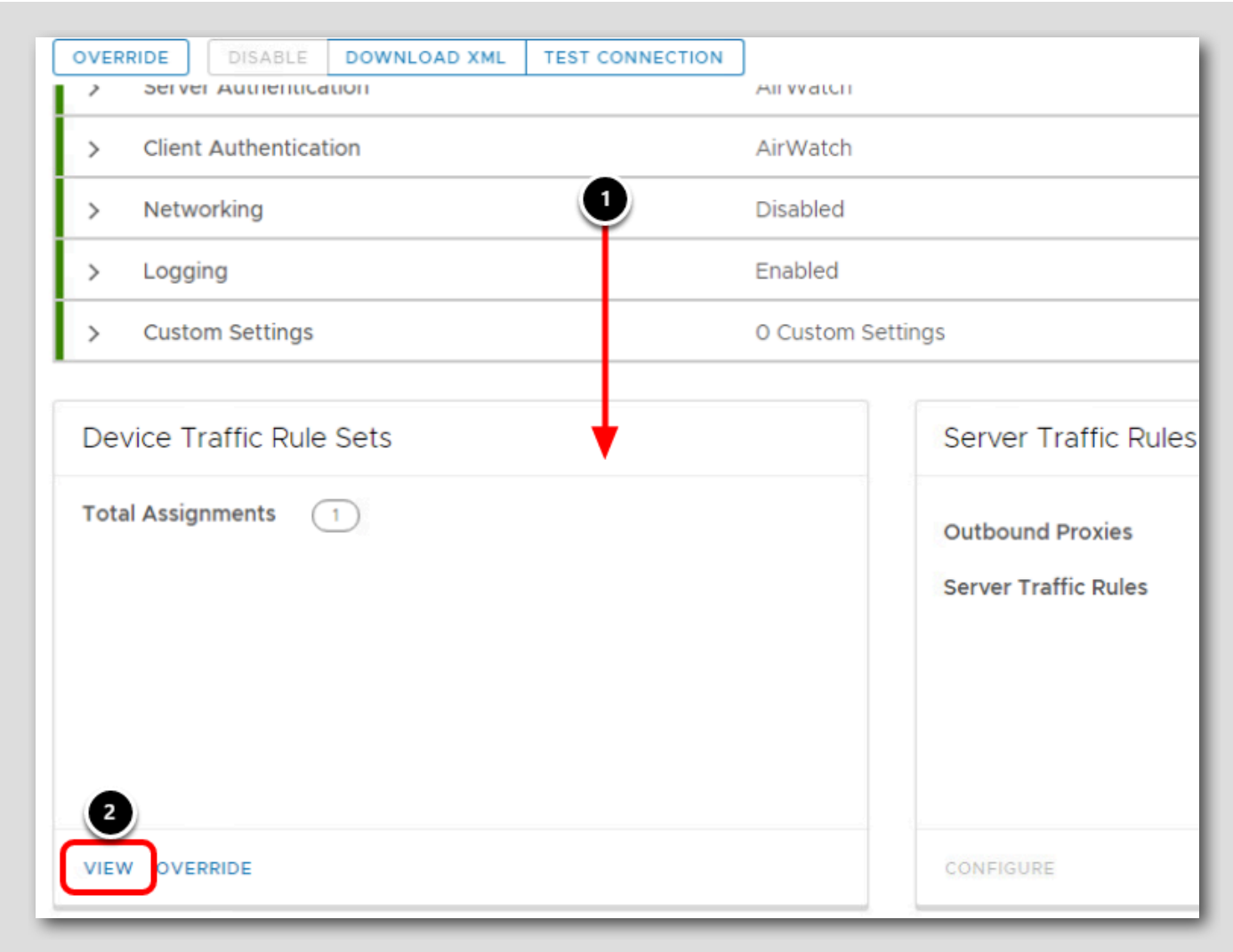
1. [Server Authentication] をクリックして、セクションを展開します。
2. [SSL] 設定が [AirWatch] であることを確認します。
3. [Client Authentication] をクリックして、セクションを展開します。
4. [Authentication] 設定が [AirWatch] であることを確認します。

証明書は、クライアントと Tunnel サービス間のトラフィックを保護するために使用されます。AirWatch 認証局を使用して、Tunnel サービスのクライアント証明書やサーバ証明書を生成できます。必要に応じて、[Third Party] を選択して証明書をアップロードすることで、独自の証明書を提供できます。

このユースケースでは、証明書に AirWatch 認証局を使用します。

トラフィック ルール セットの確認

[723]



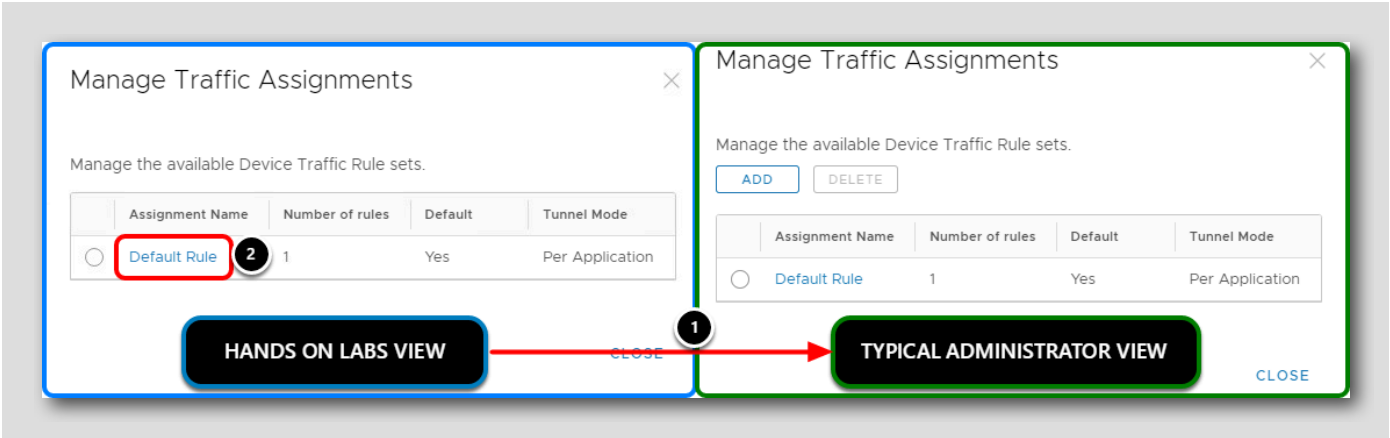
1. 下にスクロールして、[Device Traffic Rule Sets] セクションを見つけます。
2. [View] をクリックします。

[Device Traffic Rule Sets] でどのデバイスのどのアプリケーションが Tunnel サービスを使用して宛先に到達できるか、どの宛先がブロックされるか、どの宛先がバイパスできるか（Tunnel 経由で送信しない）を定義します。

詳細については、TechZone で「*Understanding Device Traffic Rules*」を参照してください。

トラフィック割り当ての表示

[724]

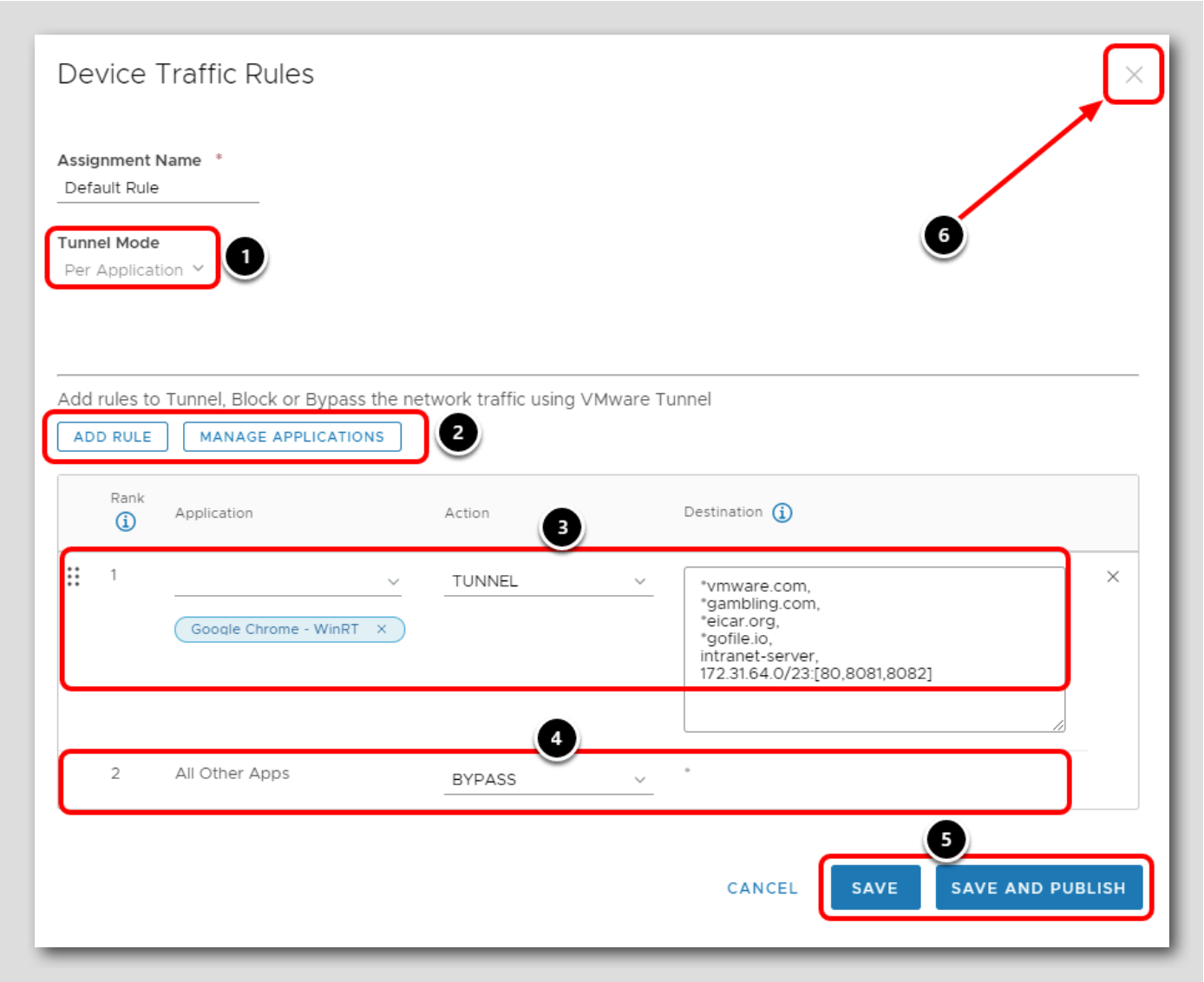


1. デバイス トラフィック ルール セットは、Workspace ONE UEM の親組織グループで構成されているため、アカウントにルールを追加または削除する権限はありません。自分のビュー（左側）を Tunnel 権限を持つ管理者（右側）と比較します。
2. [Default Rule] をクリックします。

デバイス トラフィック ルールの確認

[725]

このハンズオン ラボでは、デバイス トラフィック ルールは親組織グループで構成されているため、デバイス トラフィック ルールを表示する権限はありません。ラボ用の構成内容を確認するために、以下の構成のスクリーンショットを参照してください。



注：上記のページにアクセスしたり、これらの設定を変更したりすることはできません。スクリーンショットは情報提供を目的としているため、このラボの Tunnel の構成を確認できます。

この構成では、Windows 10 デバイスで Google Chrome を使用場合に宛先の小さなサブセットがトンネルを通過できるようにし、他のすべてのユースケースでトンネルをバイパスするようにします。この構成は、ハンズオン ラボ ネットワークの特定のユースケースを示すために使用されます。次のステップでは、比較のために、より一般的な実際の構成について説明します。

1. ルールを作成するときに、管理者は Tunnel モードを [Per Application] または [Full Device] に設定できます。アプリケーション単位では、以下のルールにリストされているアプリケーションが使用され、TUNNEL アクション ルールの宛先に接続する必要がある場合に Tunnel が有効になり、特定のトラフィックを選択的にトンネリングできます。[Full Device] を選択すると、デバイス上のすべてのトラフィックがトンネル経由でルーティングされます。
2. 管理者は、新しいルールを追加したり、Workspace ONE Tunnel の利用を許可するアプリケーションを管理したりできます。ルールは以下に表示され、ランク順に処理されます。
3. 最もランクの高いルールは、Windows デバイス (WinRT) 上の Google Chrome が Tunnel サービスを介して [Destination] フィールドの値に一致するドメインまたは IP アドレスをトンネリングできるように設定されています。ユーザーが Windows 10 で Chrome を開き、これらの宛先のいずれかに移動すると、トラフィックは SASE PoP テナントでホストされている Secure Access サービスにトンネリングされます。

   注：宛先ドメインのワイルドカードと IP アドレスを構成する方法の詳細については、「Device Traffic Rules Wildcard Guidelines」を参照してください。
4. 最後のルールは BYPASS です。他のすべてのアプリケーションと宛先が Tunnel サービスを完全にバイパスします。
5. 管理者は、[Save] または [Save and Publish] ボタンを使用して構成を保存できます。構成を公開すると、最新の変更がデバイスにプッシュされます。保存すると、変更のみが書き込まれます。
6. 終了したら、[Close] をクリックして前のページに戻ります。

トンネル トラフィック ルールの例

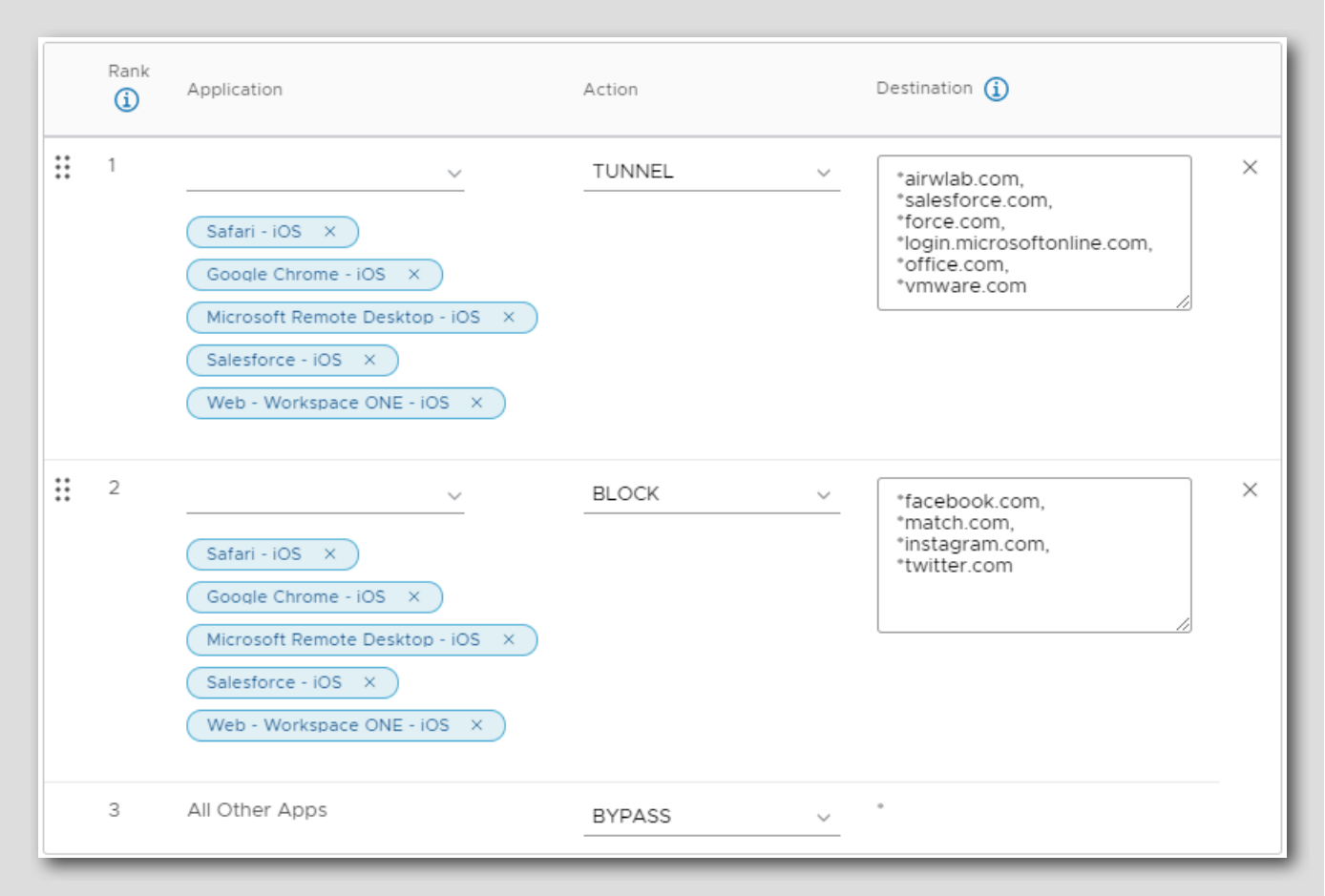
[726]

注：この手順は情報提供のみを目的としたものであり、望ましい結果を達成するためのトンネル トラフィック ルールの実際の応用について説明します。この手順で表示される構成を行うことはできません。

前の手順では、使用しているデバイス トラフィック ルールが一般的な展開を反映していないことを示しました。

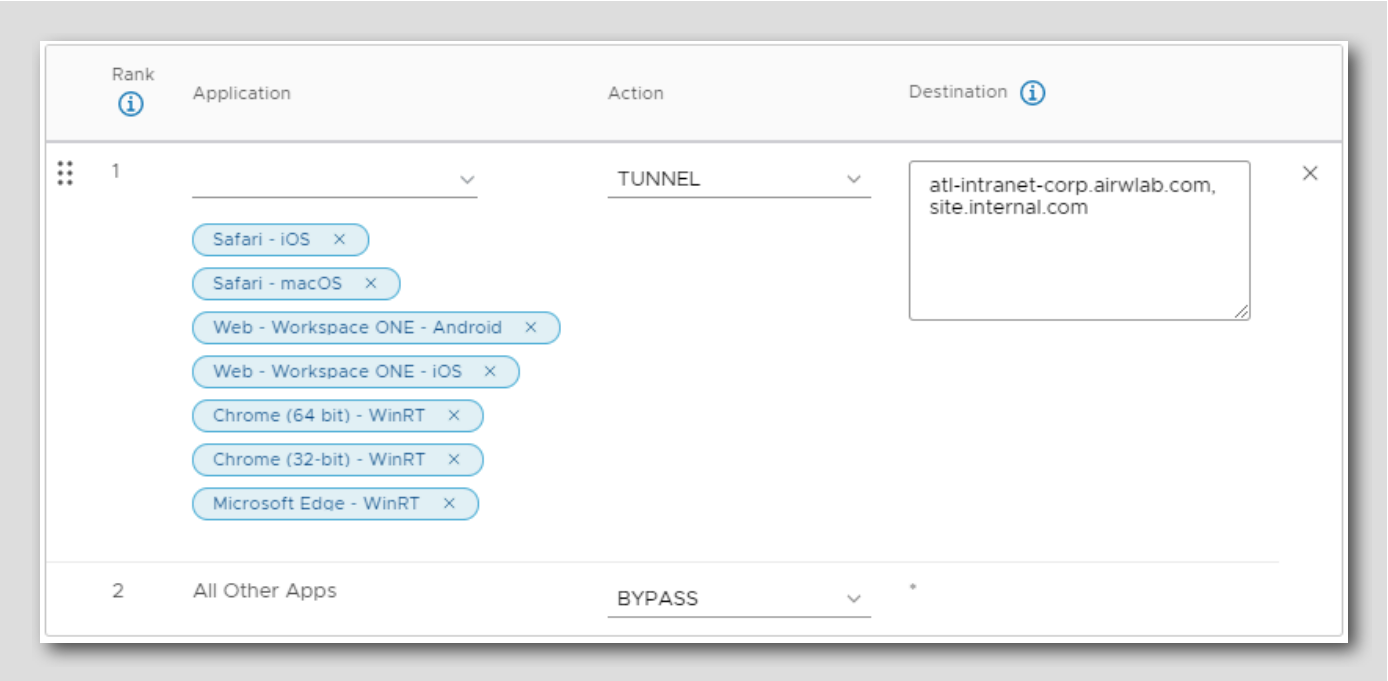
ユースケース：企業所有の iOS デバイス

次の例では、デバイス トラフィック ルールにより、iOS 用のいくつかの特定のブラウザで、必要な企業トラフィック（SalesForce や Microsoft Office など）をトンネリングしながら、企業が所有するデバイスで許可したくない一部のソーシャル メディア サイトをブロックしています。



ユースケース：契約社員での制限された Tunnel トラフィック

契約社員が自分のデバイスから一連のイントラネット サイトにアクセスする必要があり、常にオンサイトで企業ネットワークにアクセスするとは限らないユースケースを考えてみましょう。この例では、iOS、macOS、Android、および Windows 全体の一連のブラウザで 2 つのイントラネット サイトへのトラフィックをトンネリングできますが、他のすべてのトラフィックは Tunnel をバイパスします。これにより、Tunnel サービスを介して個人トラフィックをトンネリングせず、悪意のあるサイトや望ましくないサイトが Tunnel サービスを経由してルーティングされないようにすることで、エンドユーザーのプライバシーを尊重できます。

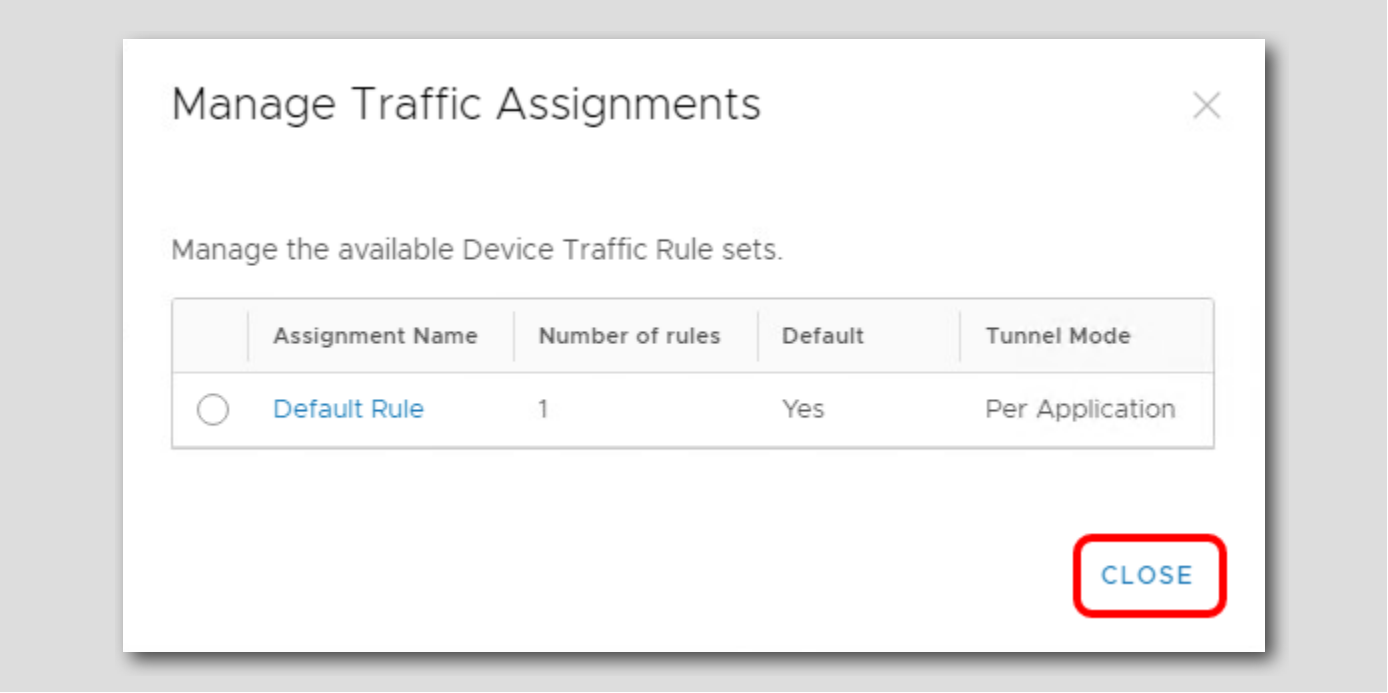


Per Application ルールと Full Device ルールを TUNNEL、BYPASS、BLOCK、および PROXY アクションと組み合わせて使用し、さまざまなビジネス ユースケースに対して望ましい結果を達成する方法を検討してください。

次の手順に進んでください。

[Traffic Assignments] ページを閉じる

[727]



[Manage Traffic Assignments] ポップアップで **[Close]** をクリックして、トンネル構成ページに戻ります。

まとめ

[728]

これで、登録済み Windows 10 デバイスの Google Chrome が一致するすべてのドメインと IP アドレスを SASE PoP によってホストされている Tunnel サービスにトンネリングできるようにするために、完了した Tunnel 構成を確認しました。この構成により、http://intranet-server 宛先へのトラフィックはプライベート ネットワークにトンネリングし、イントラネット サイトにアクセスできます。また、トラフィックをトンネリングして悪意のある、または望ましくないネットワーク動作を検査し、構成済みの Cloud Web Security (CWS) ポリシーを使用してユーザーを保護できます。

次に、VPN ペイロードを含むプロファイルを作成します。このプロファイルは、組織に登録されているデバイスに Workspace ONE Tunnel 構成を送信します。

VPN プロファイルの作成と公開

[729]

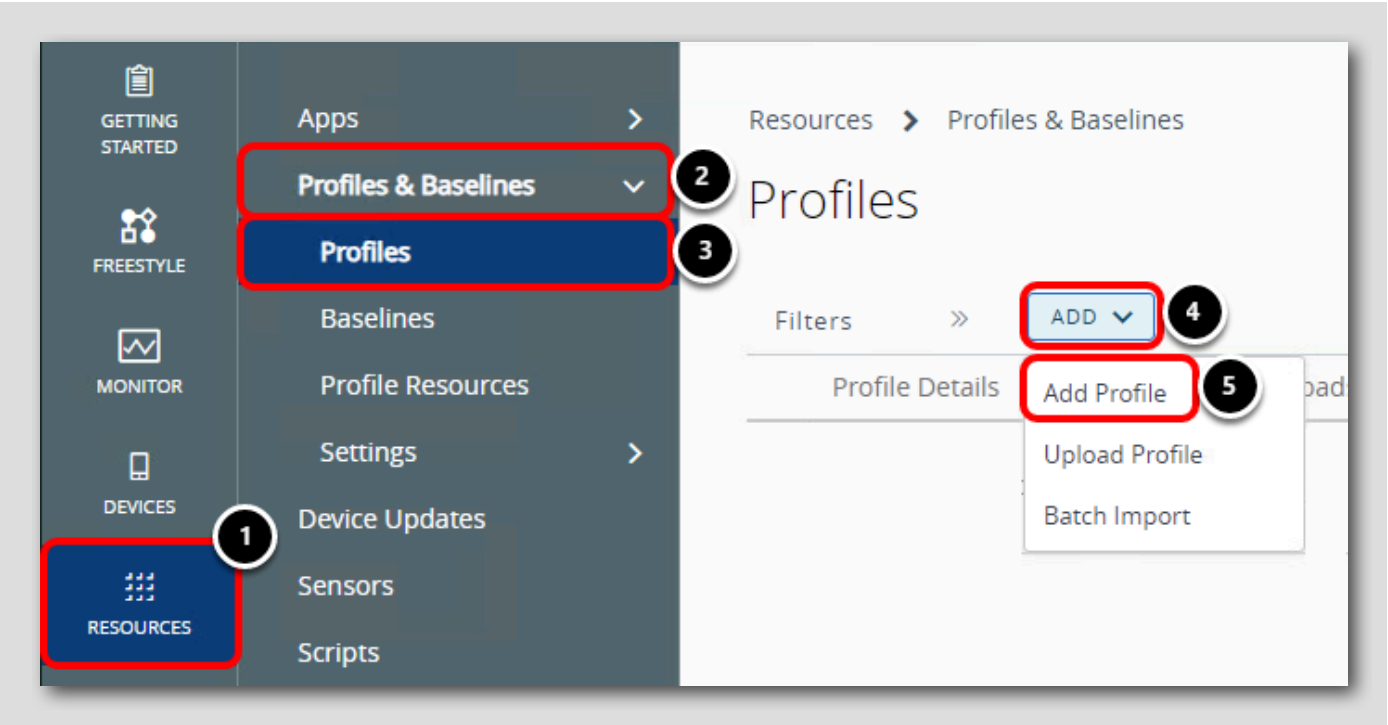
Workspace ONE UEM と統合された Workspace ONE Tunnel を使用すると、VPN ペイロードを含むプロファイルを作成する準備が整いました。後の手順で展開する Workspace ONE Tunnel アプリケーションでは、デバイスで VPN ペイロードを含むプロファイルが必要です。これにより、トンネル デバイス トラフィック ルールを解析して適用できます。

これにより、さまざまなトンネル デバイス トラフィック ルールを、組織内のさまざまなユーザーまたはデバイスに配信し、それぞれのニーズを満たすことができます。

詳細については、TechZone の Workspace ONE Tunnel 運用チュートリアルで、*iOS*、*macOS*、*Windows 10*、*Android* 用のアプリケーションごとの VPN プロファイルの作成を参照してください。

VPN ペイロードを含むプロファイルの作成

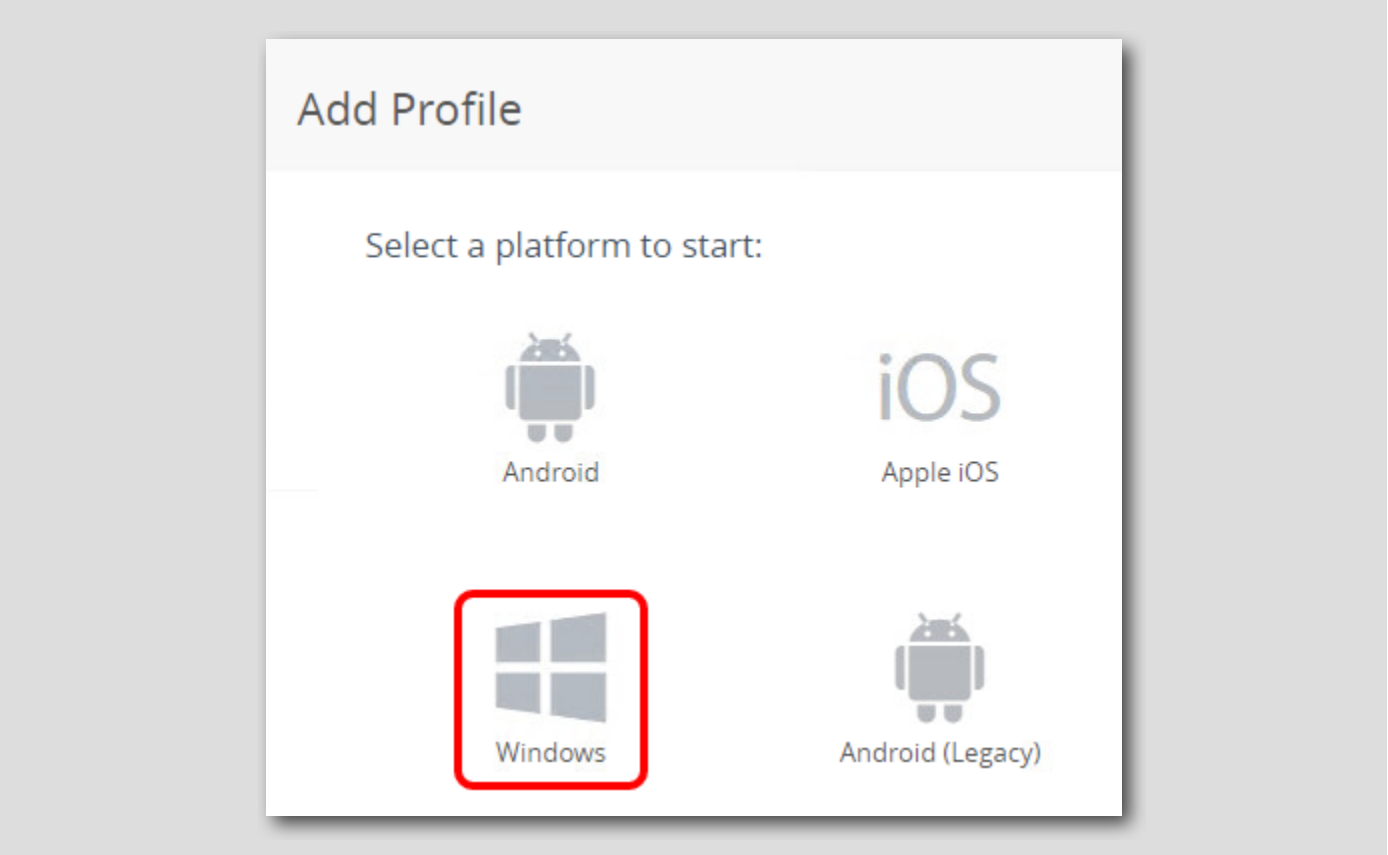
[730]



1. [Resources] をクリックします。
2. [Profiles & Baselines] をクリックします。
3. [Profiles] をクリックします。
4. [Add] をクリックします。
5. [Add Profile] をクリックします。

Windows プラットフォームの選択

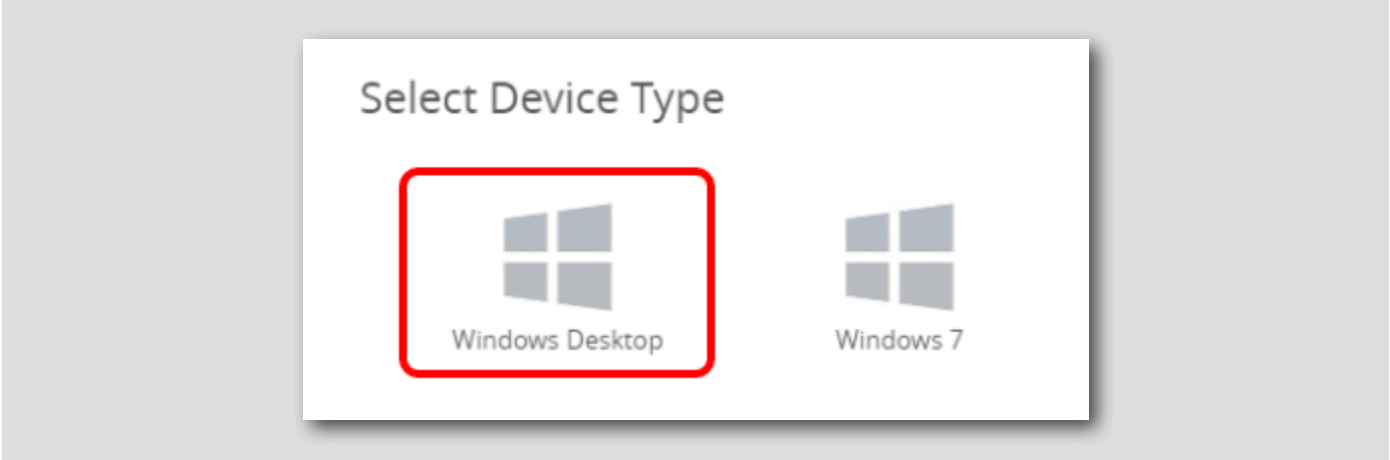
[731]



[Windows] をクリックします。

Windows デスクトップ デバイス タイプの選択

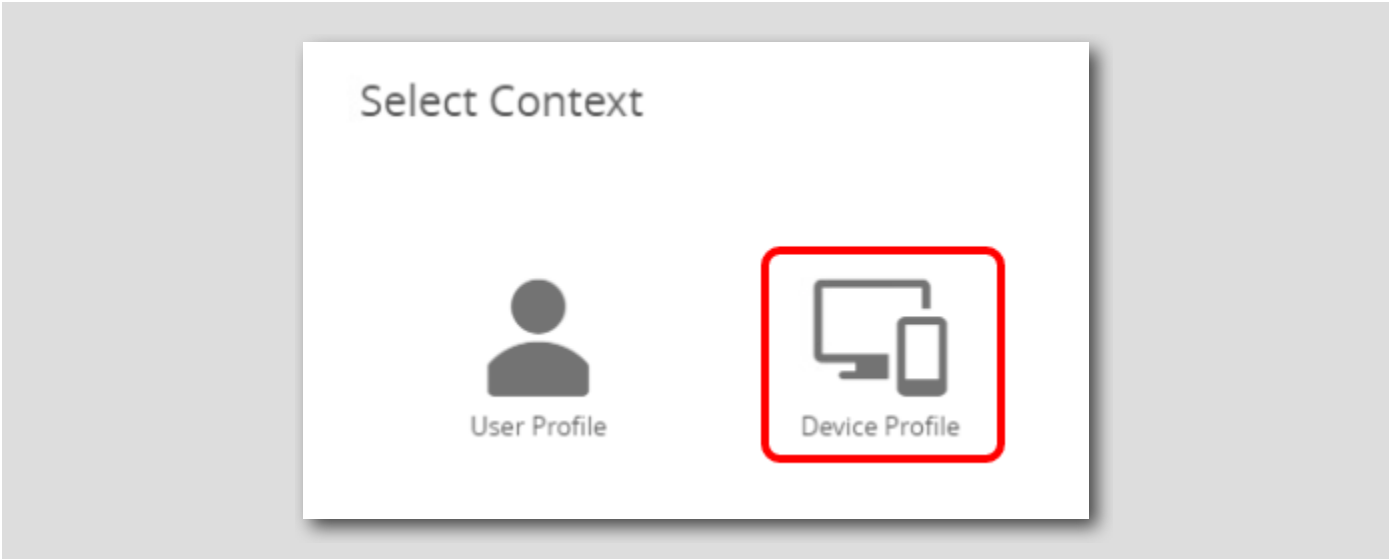
[732]



[Windows Desktop] デバイス タイプをクリックします。これにより、Windows 10 デバイスに対して行う次の構成が適用されます。

デバイス プロファイル コンテキストの選択

[733]

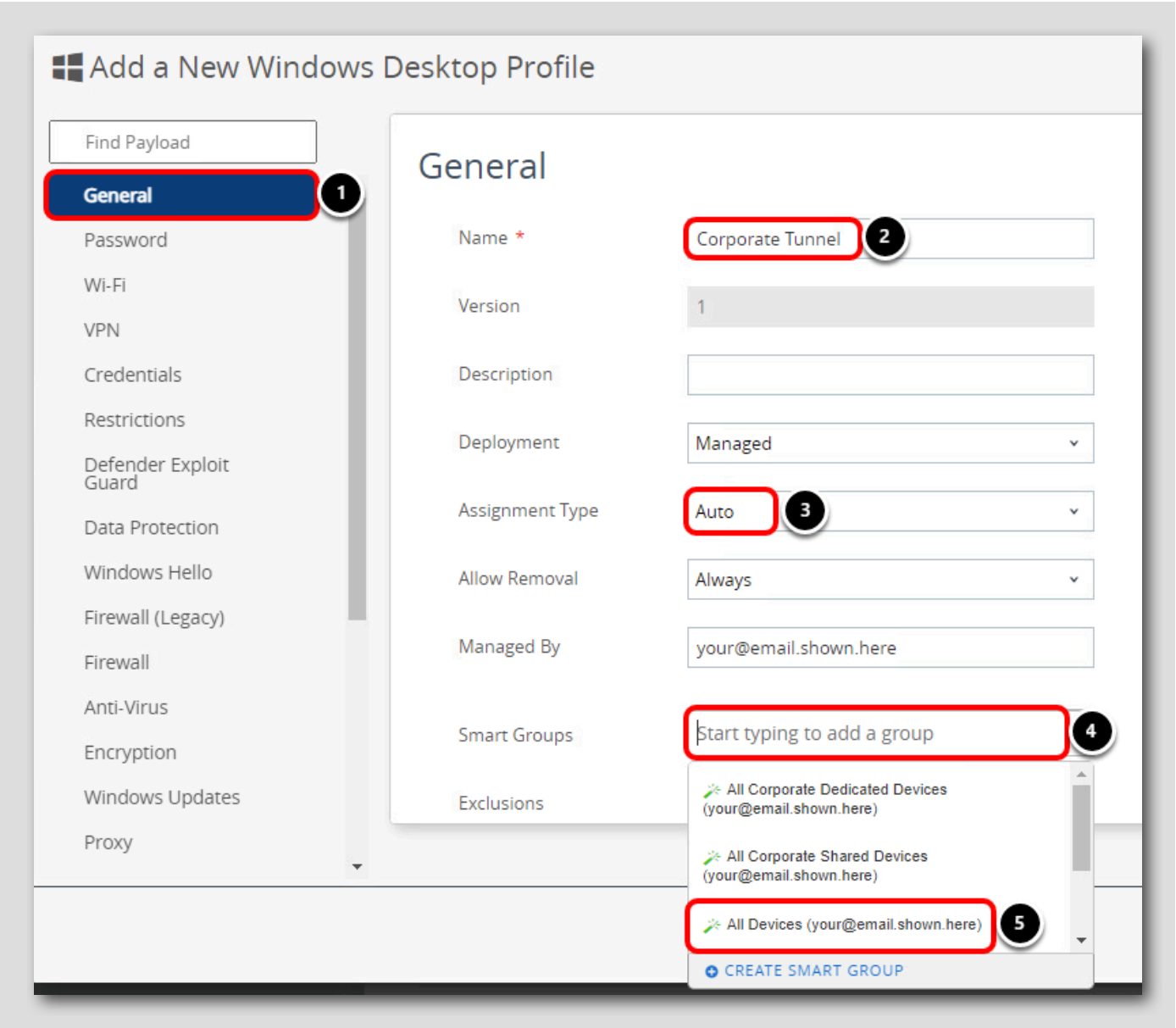


[Device Profile] コンテキストをクリックします。

これにより、ユーザーに関係なく、Windows 10 デバイス全体に対して行う構成が適用されます。ユーザー固有の構成を展開する場合は、代わりにユーザー プロファイルを使用します。

全般ペイロード設定の構成

[734]

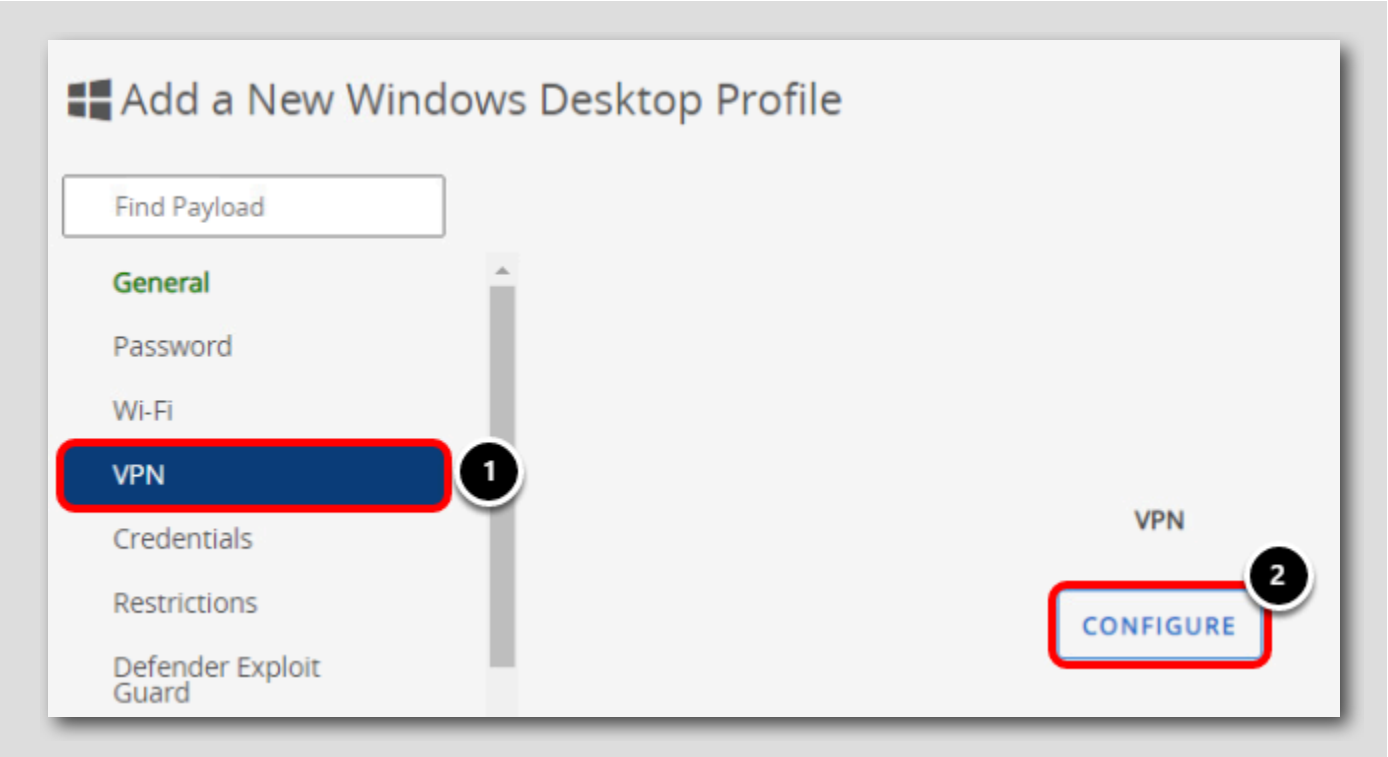


1. [General] ペイロード タブをクリックします（選択されていない場合）。
2. [Name] に **`Corporate Tunnel`** と入力します。このプロファイルは、管理者コンソールおよびデバイス上でこの名前で識別されます。
3. [Assignment Type] で [Auto] を選択します。これにより、指定されたデバイスにプロファイルが自動的に公開され、設定を取得するためにエンド ユーザーが入力する必要はありません。
4. [Smart Groups] 入力フィールドをクリックすると、割り当てに使用できるスマート グループのリストが表示されます。
5. [All Devices (your@email.shown.here)] の結果を選択します。

これにより、「Corporate Tunnel」という名前のプロファイルが、組織に登録されている Windows 10 デバイスに自動的に公開されるように構成されます。

VPN ペイロードの追加

[735]

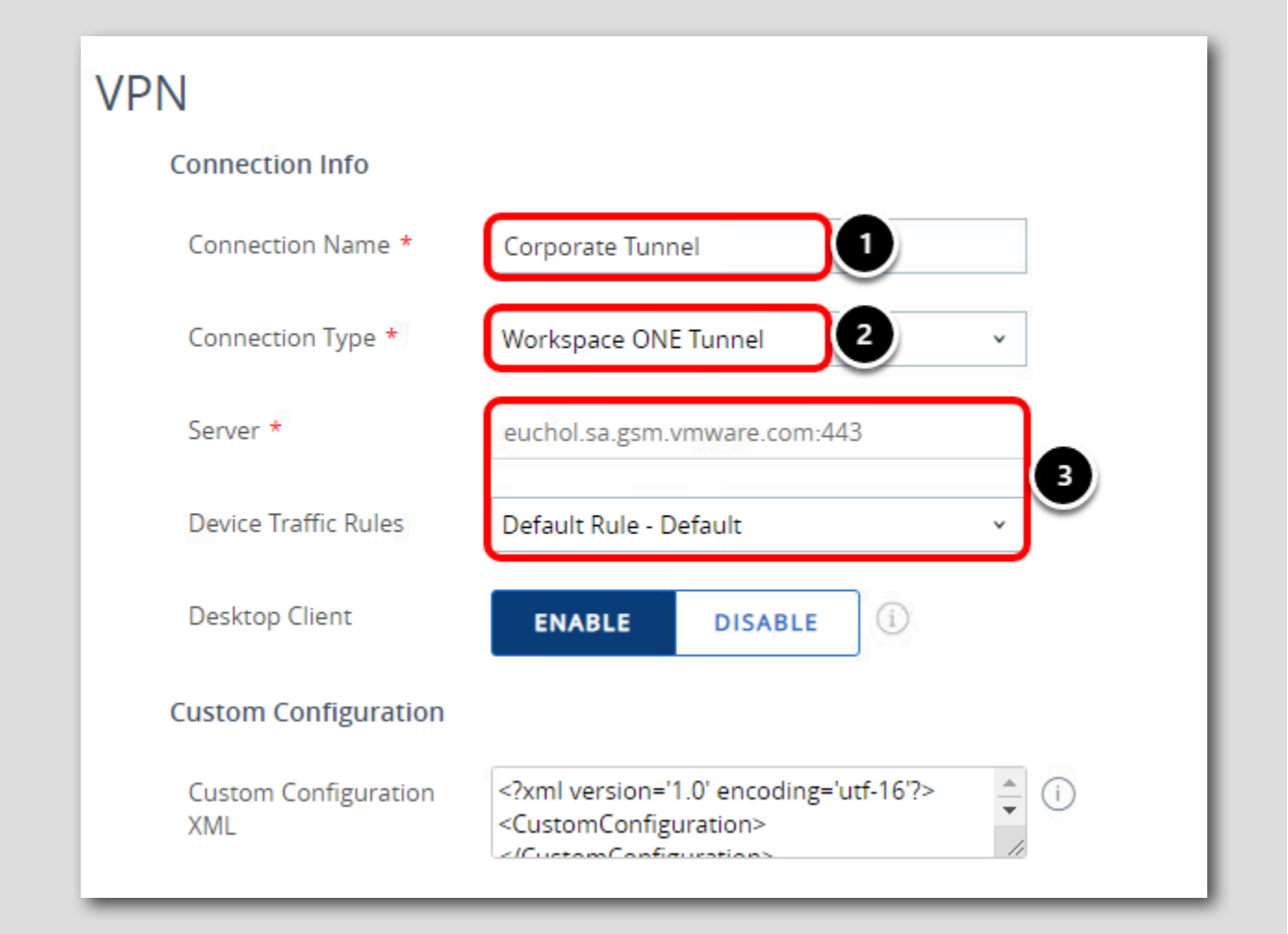


1. [VPN] ペイロード タブをクリックします。
2. [Configure] をクリックして VPN ペイロードを有効にします。

プロファイルには複数のペイロードを関連付けることができます。そのため、追加するペイロードごとに [Configure] をクリックする必要があります。ただし、一般的に、簡素化のため、プロファイルごとにペイロードを 1 つだけ含めるのがベスト プラクティスです。

VPN ペイロードの構成

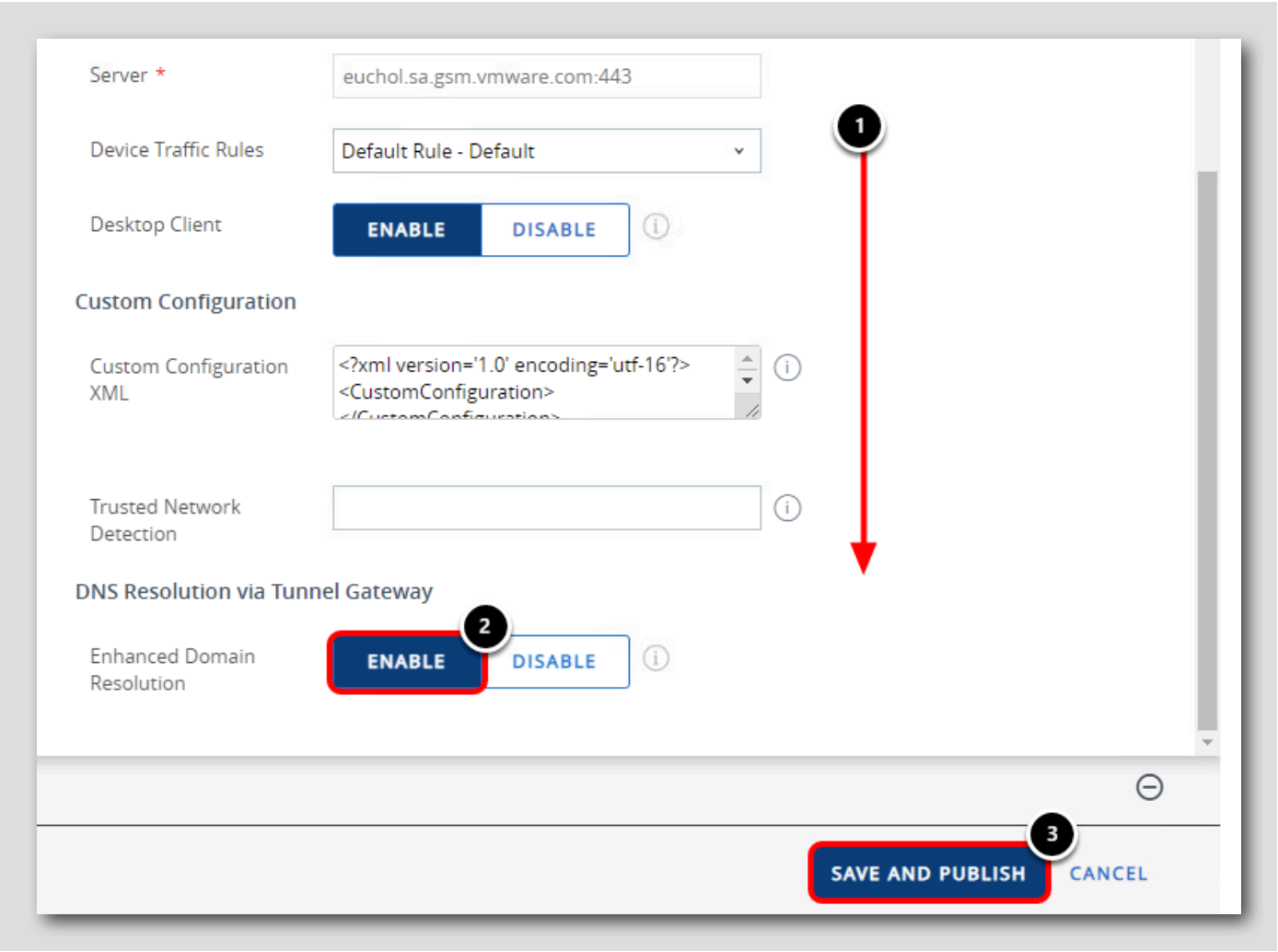
[736]



1. 接続名に **`Corporate Tunnel`** と入力します。
2. 接続タイプに [Workspace ONE Tunnel] を選択します。
3. [Server] とその他のオプションが自動的に入力されていることを確認します。デバイス トラフィック ルールが複数ある場合は、このプロファイルに適用するルール セットを選択できますが、作成したのは 1 つのみです（デフォルト - デフォルト）。他のデフォルトは、このラボではそのまま残すことができます。

DNS 解決用ドメインの追加

[737]

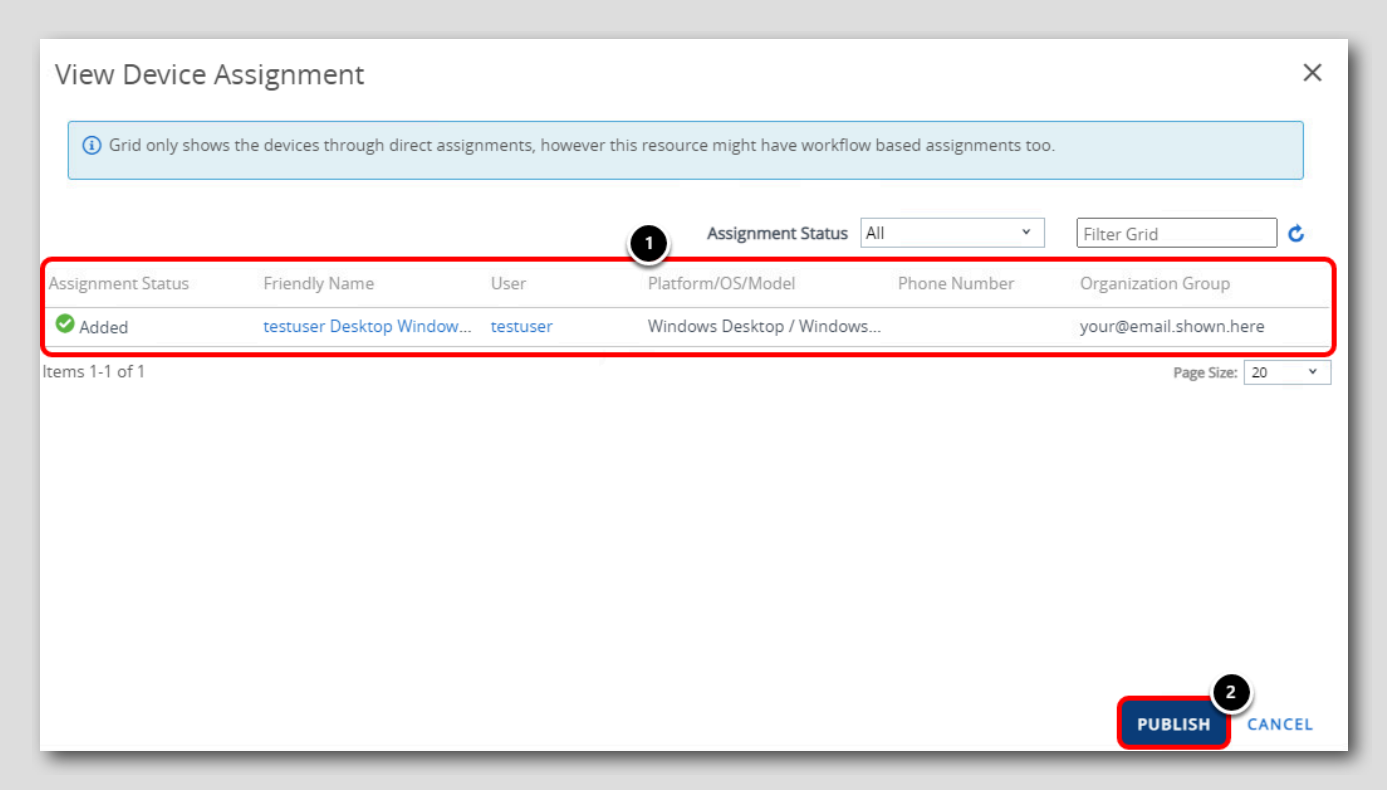


1. 下にスクロールして、[DNS Resolution] 設定を見つけます。
2. [Enhanced Domain Resolution] 設定で [Enabled] を選択します。
3. [Save and Publish] をクリックします。

この VPN プロファイルはデバイスにプッシュされます。このプロファイルは、Workspace ONE Tunnel アプリケーションで Tunnel サービスがホストされる場所 (euchol.sa.gsm.vmware.com:443) と使用されるデバイス トラフィック ルールを決定するために使用します。

VPN プロファイルの公開

[738]

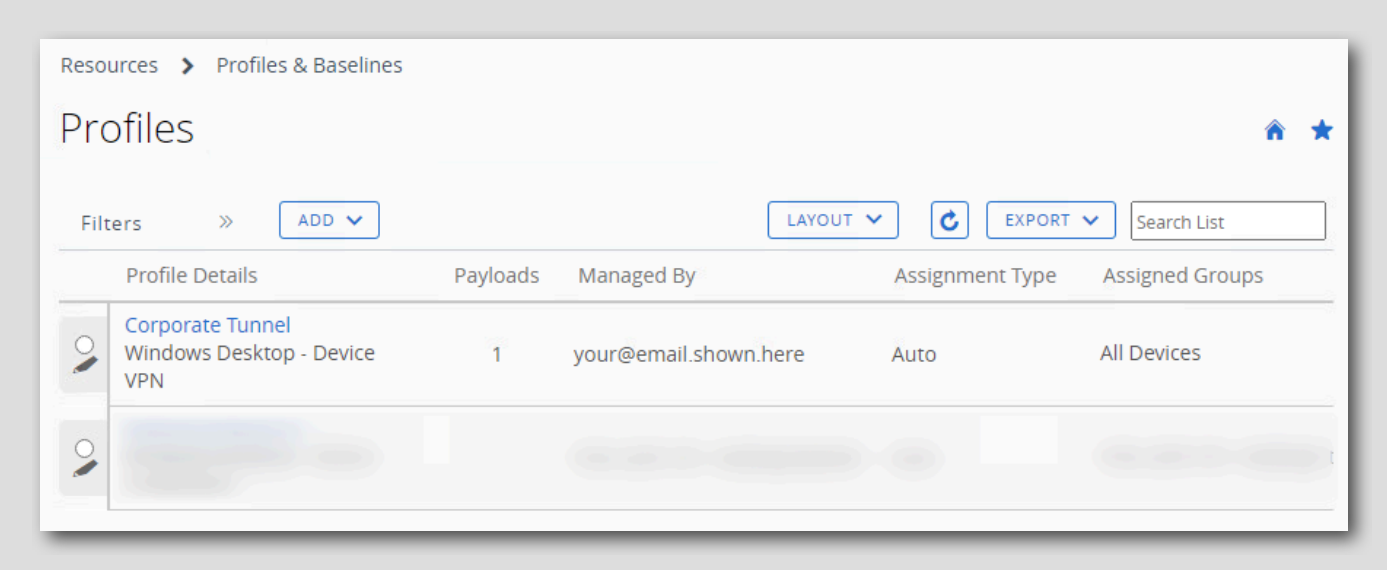


1. 選択した割り当てに基づいてこのプロファイルを受信するデバイスのプレビューがここに表示されます。登録された単一の仮想マシンが現在表示されています。
2. [Publish] をクリックします。

VPN ペイロードを含むプロファイルが、必要な Workspace ONE Tunnel 構成を使用してデバイスに公開されるようになりました。割り当てタイプが [Auto] に設定されているため、登録されたデバイスはこの構成を自動的に受け取ります。

プロファイルが作成されたことの確認

[739]



作成されると、Workspace ONE UEM 管理者コンソールのプロファイルのリストに Corporate Tunnel プロファイルが表示されます。プロファイルを編集または更新する必要がある場合は、このビューを使用して行います。

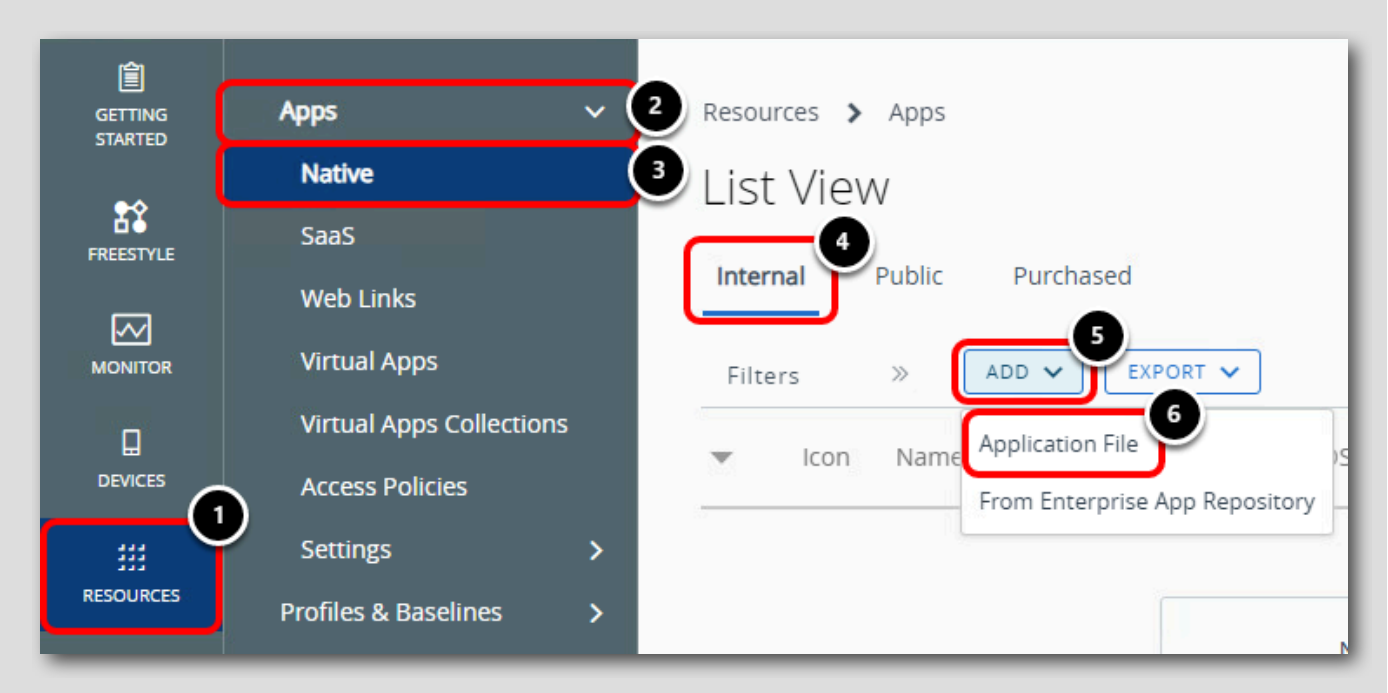
Workspace ONE Tunnel アプリケーションの公開

[740]

次に、Workspace ONE Tunnel アプリケーションをアップロードして展開の準備を行います。Workspace ONE Tunnel アプリケーションは、VPN ペイロードを含むプロファイルの詳細を利用して、SASE PoP でホストされている Workspace ONE Tunnel サービスへの接続を確立します。

Workspace ONE Tunnel アプリケーションのアップロード

[741]

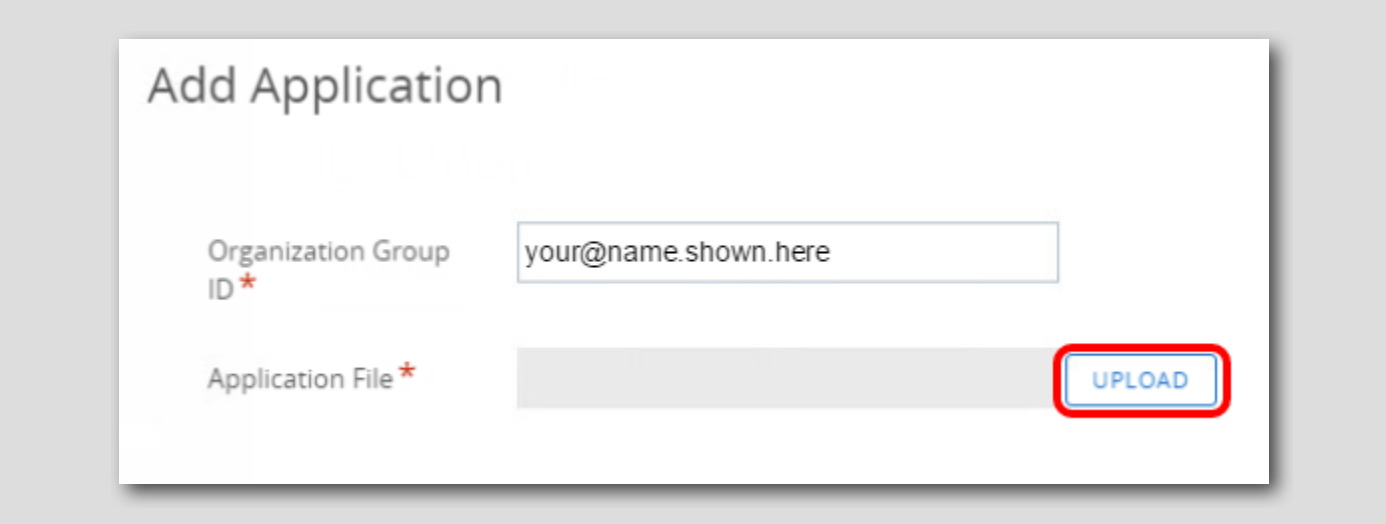


1. 左側のメニューで、[Resources] をクリックします。
2. 必要に応じて、[Apps] をクリックしてセクションを展開します。
3. 必要に応じて、[Native] をクリックします。
4. [Internal] タブをクリックします。
5. [Add] ドロップダウンをクリックします。
6. [Application File] をクリックします。

Workspace ONE Tunnel バイナリが仮想マシンでホストされています。通常は、https://my.workspaceone.com に移動し、認証情報を使用してログインし、[Products] セクションから目的のプラットフォームの Workspace ONE Tunnel バイナリをダウンロードします。

アプリケーションの追加

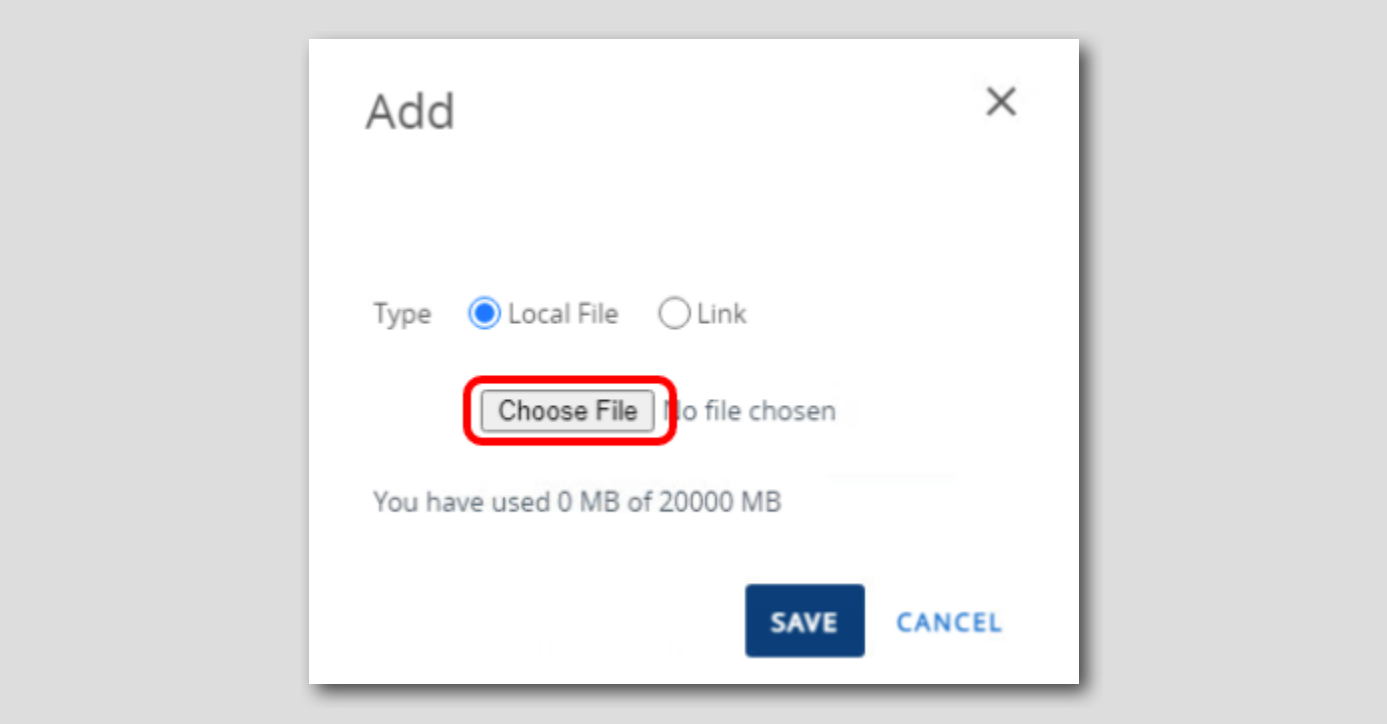
[742]



[Upload] をクリックします。

アプリケーション ファイルの選択

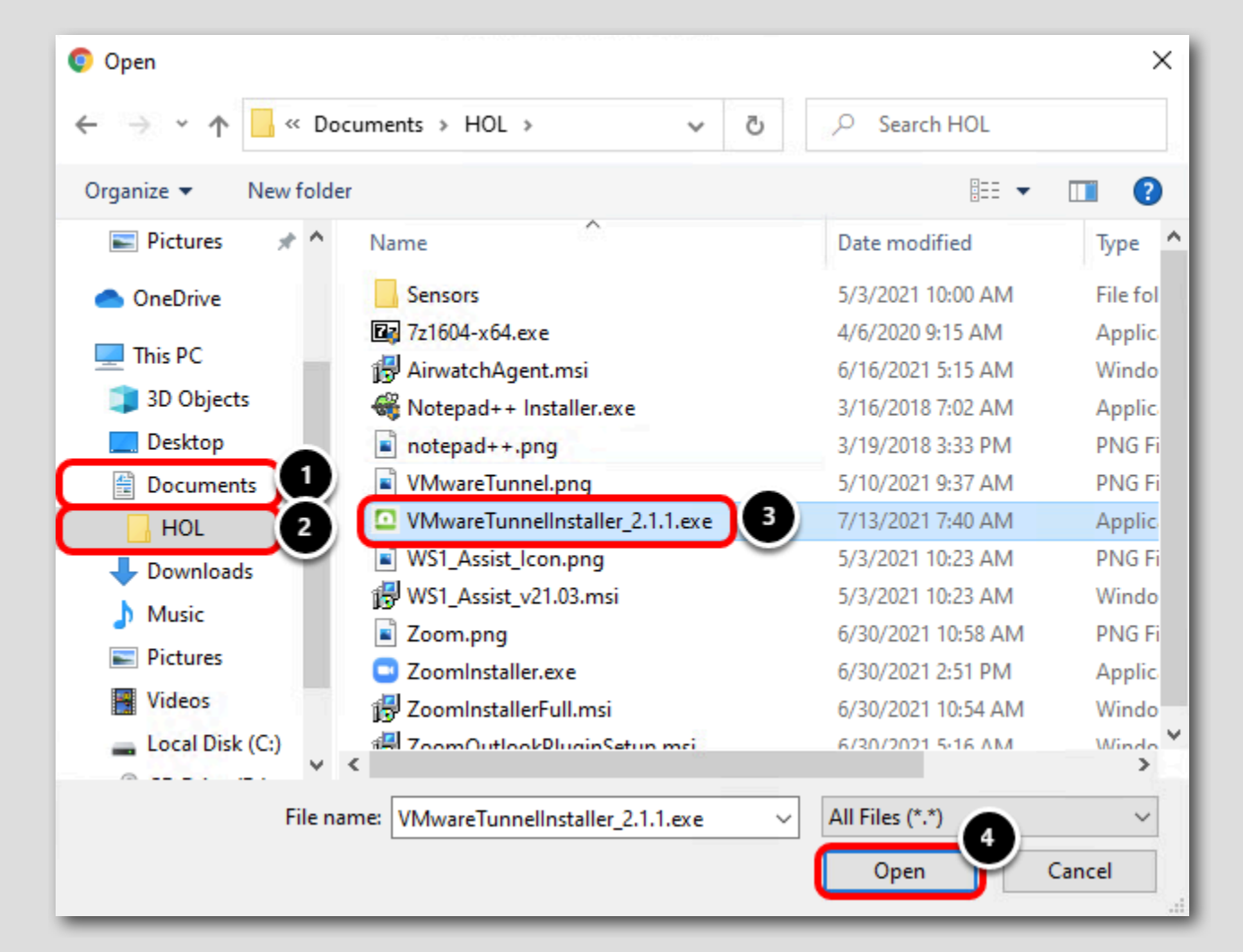
[743]



[Choose File] をクリックします。

VMwareTunnelInstaller_2.1.1.exe ファイルの選択

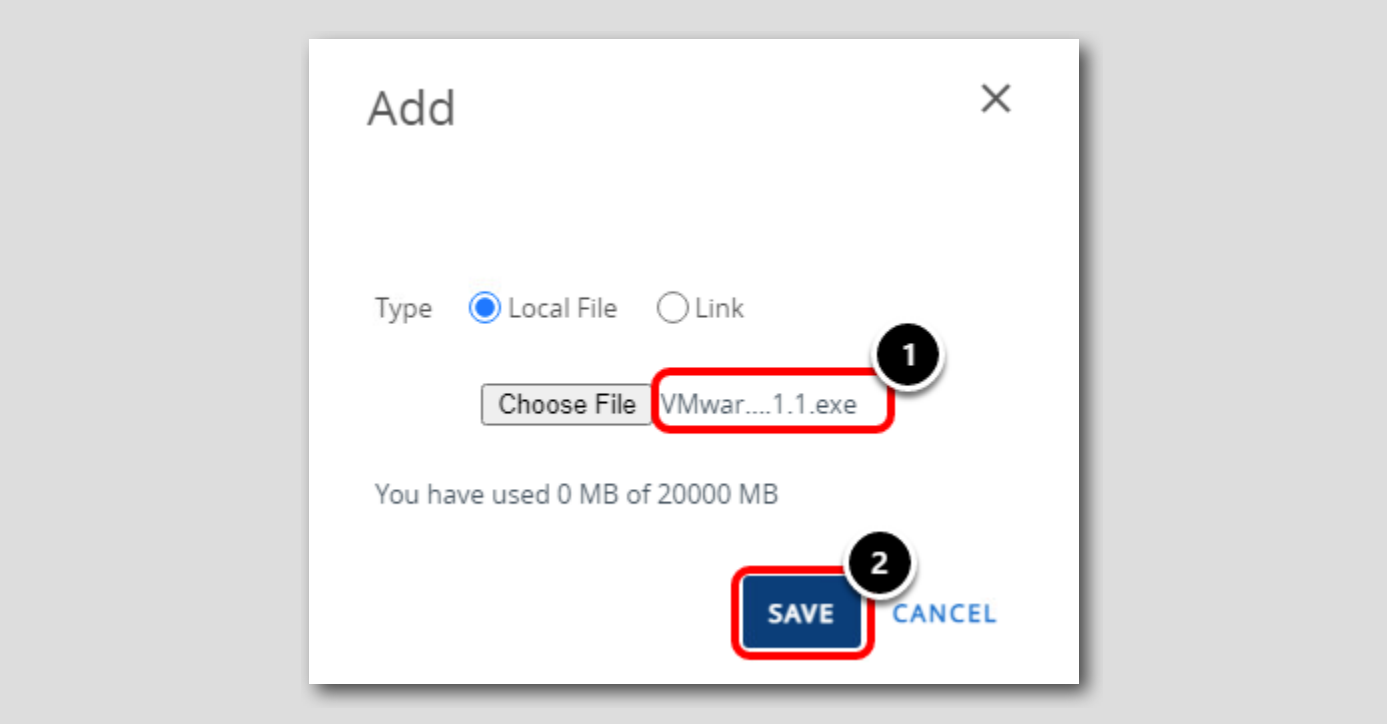
[744]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. VMwareTunnelInstall_2.1.1.exe ファイルをクリックして、選択します。
4. [Open] をクリックします。

アプリケーション アップロードの保存

[745]

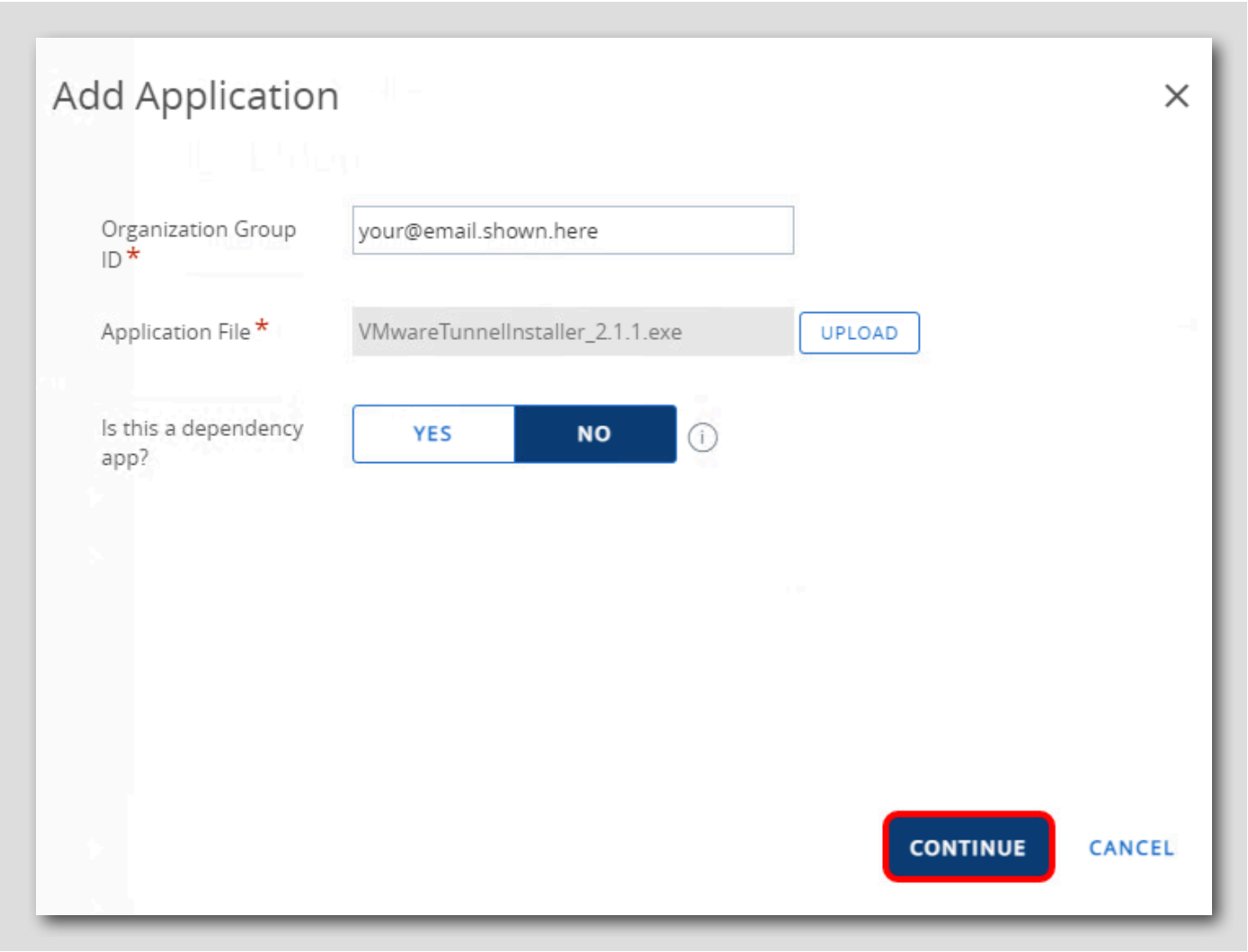


1. Workspace ONE Tunnel インストーラが選択されたことを確認します。
2. [Save] をクリックして、アプリケーション ファイルをアップロードします。

注：ハンズオン ラボ環境では、アプリケーションのアップロードに 1 ～ 2 分かかる場合があります。アップロードが完了するまでしばらくお待ちください。アップロードが完了すると、ページは自動的に進行します。

Workspace ONE Tunnel アプリケーションの構成

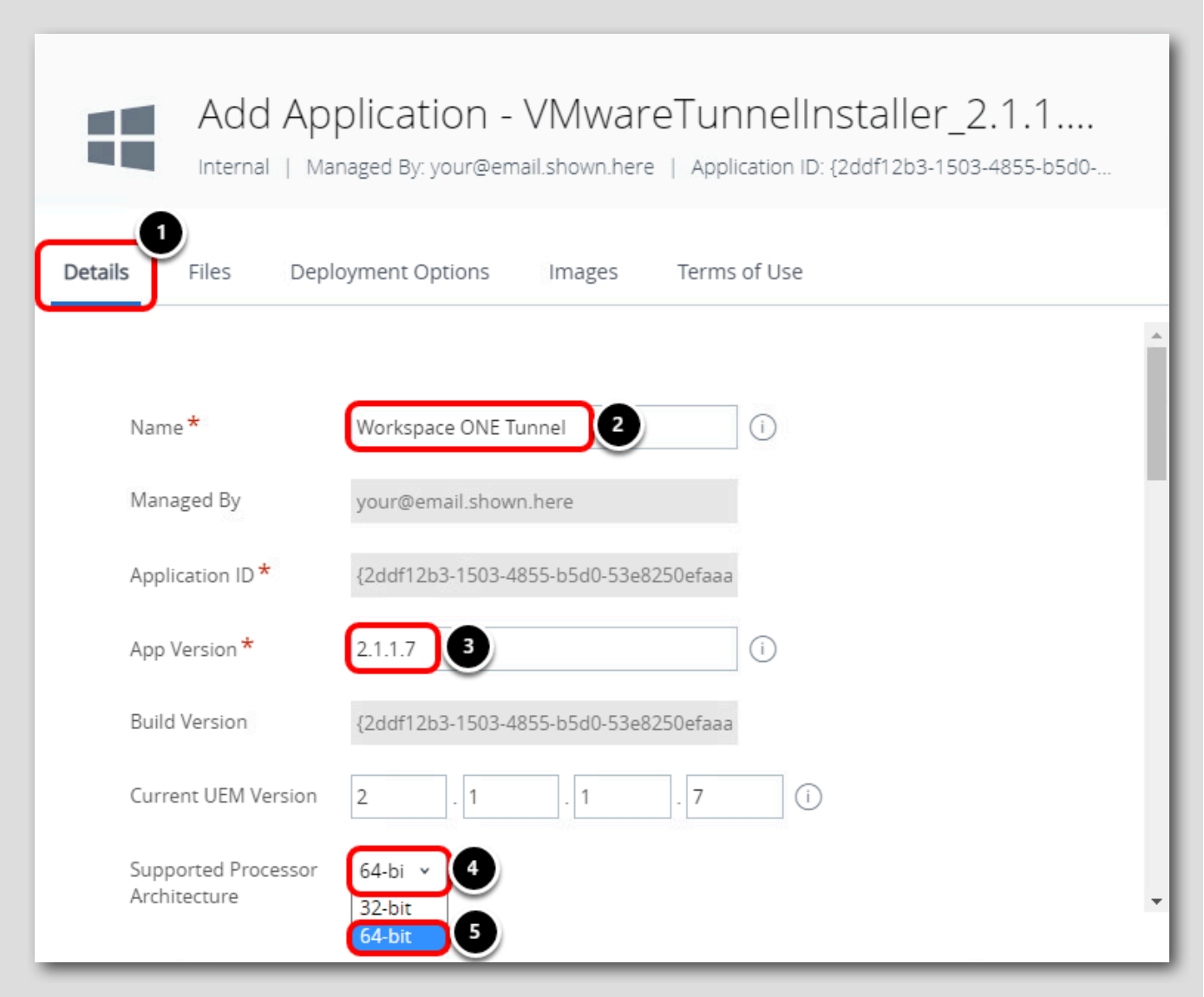
[746]



[Continue] をクリックします。

アプリケーションの詳細の編集

[747]

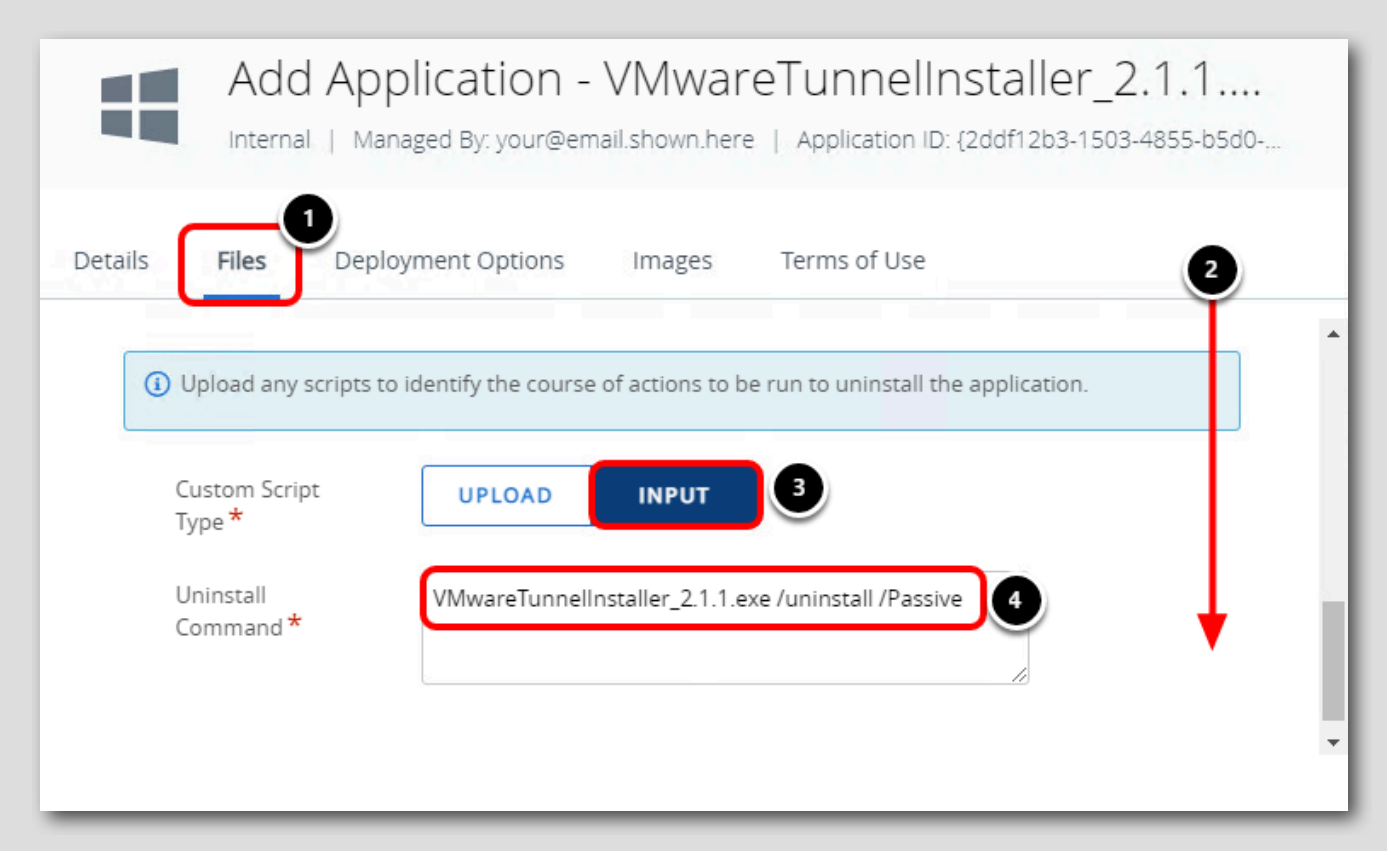


1. [Details] タブをクリックします。
2. [Name] フィールドに **`Workspace ONE Tunnel`** と入力します。
3. [App Version] フィールドに **`2.1.1.7`** と入力します。
4. [Supported Processor Architecture] ドロップダウンをクリックします。
5. [64-bit] をクリックします。

[Save & Assign] はまだクリックしないで、次の手順に進みます。

アンインストール コマンドの構成

[748]

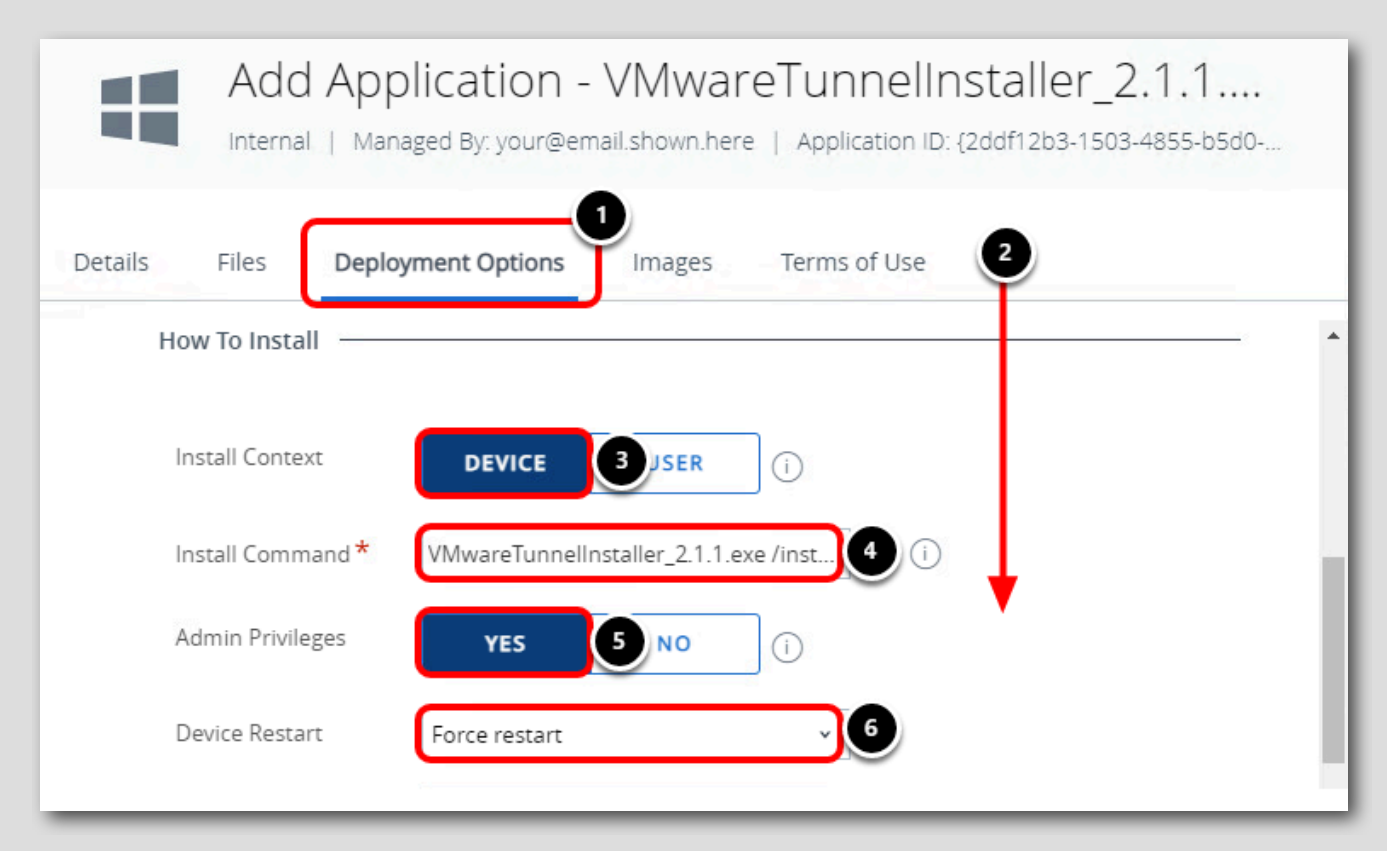


注:キーボード ショートカットを使用するか、テキストをクリックアンドドラッグして強調表示してから、テキスト フィールドにドラッグすることにより、テキストをマニュアルからコピーしてコンソールに貼り付けることができます。

1. [Files] タブをクリックします。
2. 一番下までスクロールします。
3. [Custom Script Type] で [Input] を選択します。
4. [Uninstall Command] では、次のコマンドを入力して、UEM がデバイスからアプリケーションを削除する必要がある場合に、Workspace ONE Tunnel アプリケーションをアンインストールする方法を通知します。`VMwareTunnelInstaller_2.1.1.exe /uninstall /Passive`

[How to Install] 設定の構成

[749]

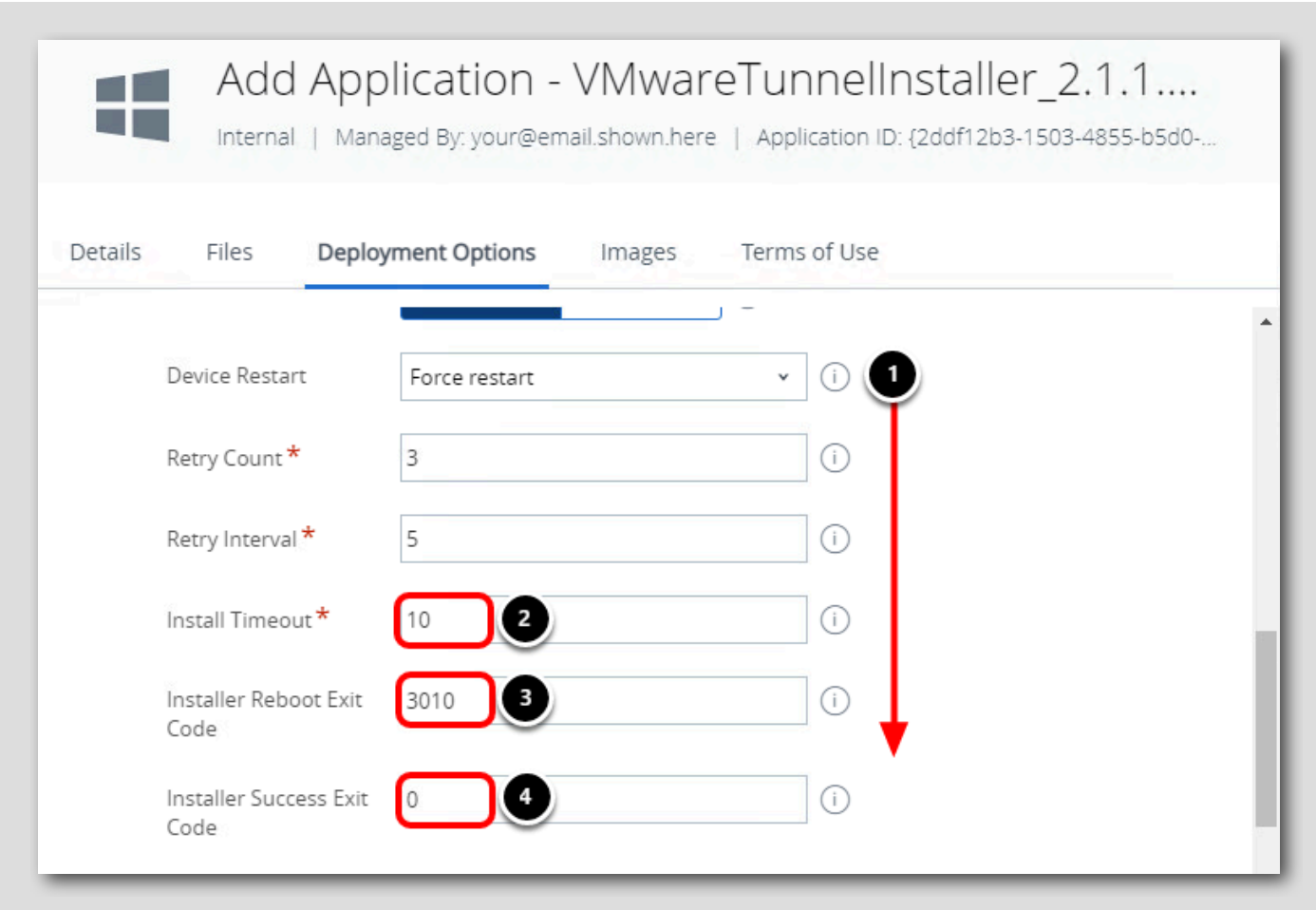


注:キーボード ショートカットを使用するか、テキストをクリックアンドドラッグして強調表示してから、テキスト フィールドにドラッグすることにより、テキストをマニュアルからコピーしてコンソールに貼り付けることができます。

1. [Deployment Options] タブをクリックします。
2. 下にスクロールして、[How To Install] セクションを見つけます。
3. [Install Context] で [Device] をクリックします。
4. [Install Command] で **`VMwareTunnelInstaller_2.1.1.exe /install /Passive`** と入力します。これにより、アプリケーションがデバイスに公開されたときにそれをサイレント インストールする方法が UEM に通知されます。
5. [Admin Privileges] で [Yes] をクリックします。
6. [Device Restart] で [Force restart] を選択します。

インストーラ コードの構成

[750]



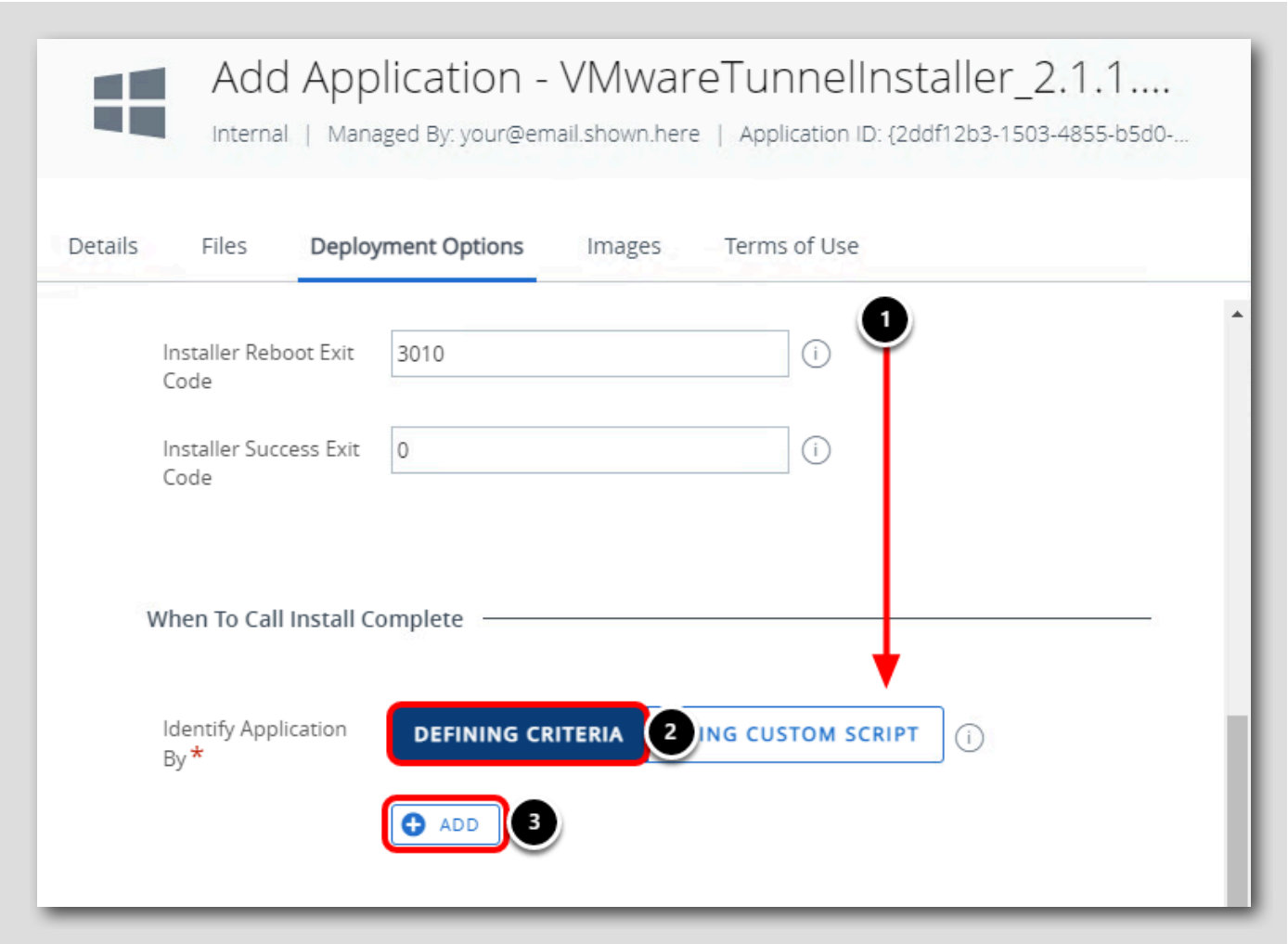
1. 下にスクロールして、[Install Timeout]、[Installer Reboot Exit Code]、および [Installer Success Exit Codes] を見つけます。
2. [Installer Timeout] に **10** と入力します。
3. [Installer Reboot Exit Code] に **3010** と入力します。
4. [Installer Success Exit Code] に **0** と入力します。

[Install Timeout] フィールドは、コマンドを再試行する前に実行ファイルのインストールを試行する時間（分単位）を UEM に通知します。

[Exit Codes] は、インストール プロセスへの応答方法をデバイスに通知します。3010 は、インストールを完了するために再起動が必要であることを示します。0 は、アクションが正常に完了したことを示します。

[751]

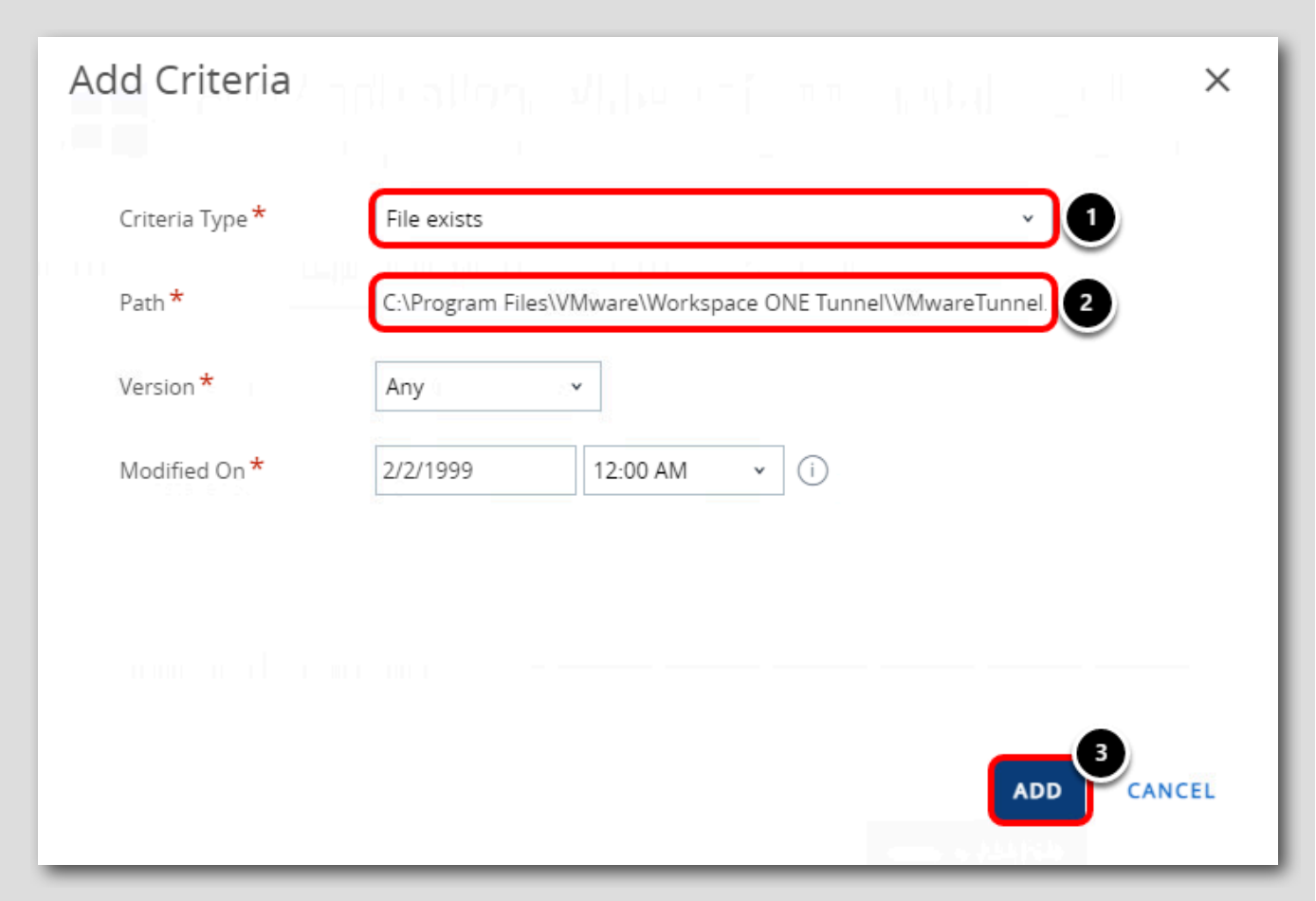
[When to Call Install Complete] への条件の追加



1. 一番下までスクロールして、[When to Call Install Complete] 設定を見つけます。
2. [Defining Criteria] を選択します。
3. [Add] をクリックします。

[File Exists] 条件の追加

[752]



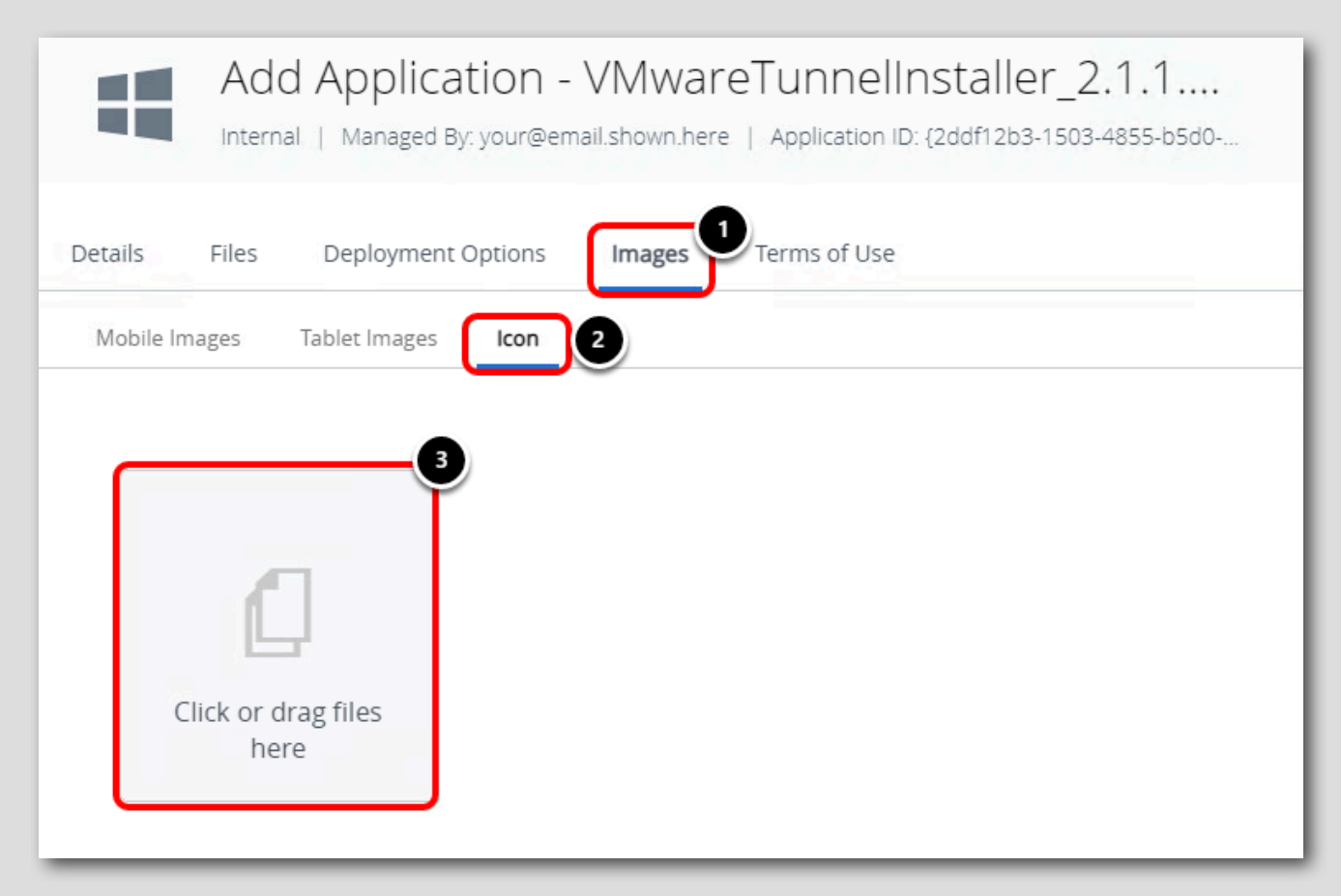
注:キーボード ショートカットを使用するか、テキストをクリックアンドドラッグして強調表示してから、テキスト フィールドにドラッグすることにより、テキストをマニュアルからコピーしてコンソールに貼り付けることができます。

1. [Criteria Type] で [File exists] を選択します。
2. パスに `C:\Program Files\VMware\Workspace ONE Tunnel\VMwareTunnel.exe` と入力します。
3. [Add] をクリックします。

[File exists] 条件は、構成されたパスに VMwareTunnel.exe ファイルが存在すると、Workspace ONE Tunnel アプリケーションが正常にインストールされたことを UEM に通知します。

アプリケーション アイコンの追加

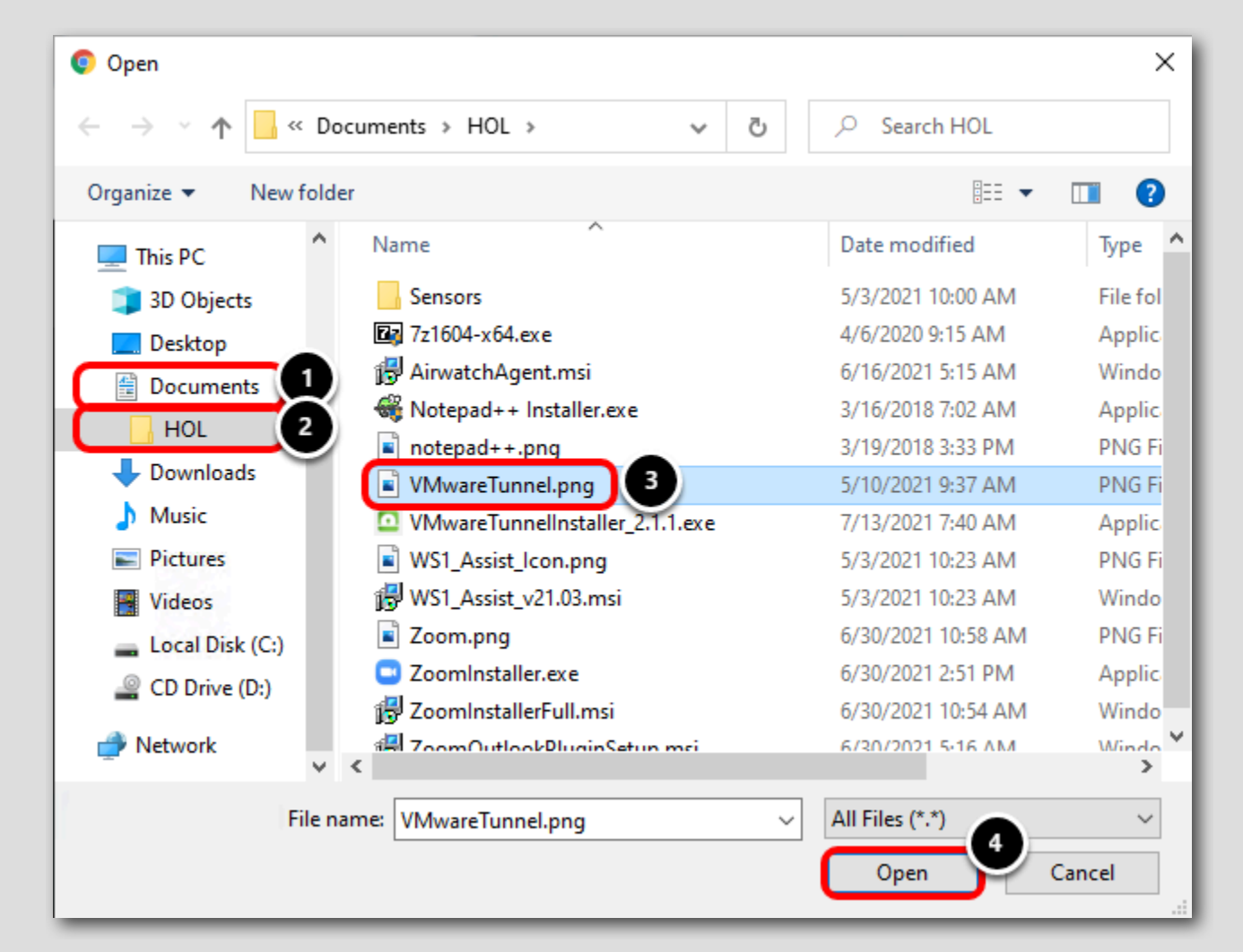
[753]



1. [Images] タブをクリックします。
2. [Icon] タブをクリックします。
3. 現在空のイメージ ボックスをクリックします。

VMwareTunnel.png ファイルの選択

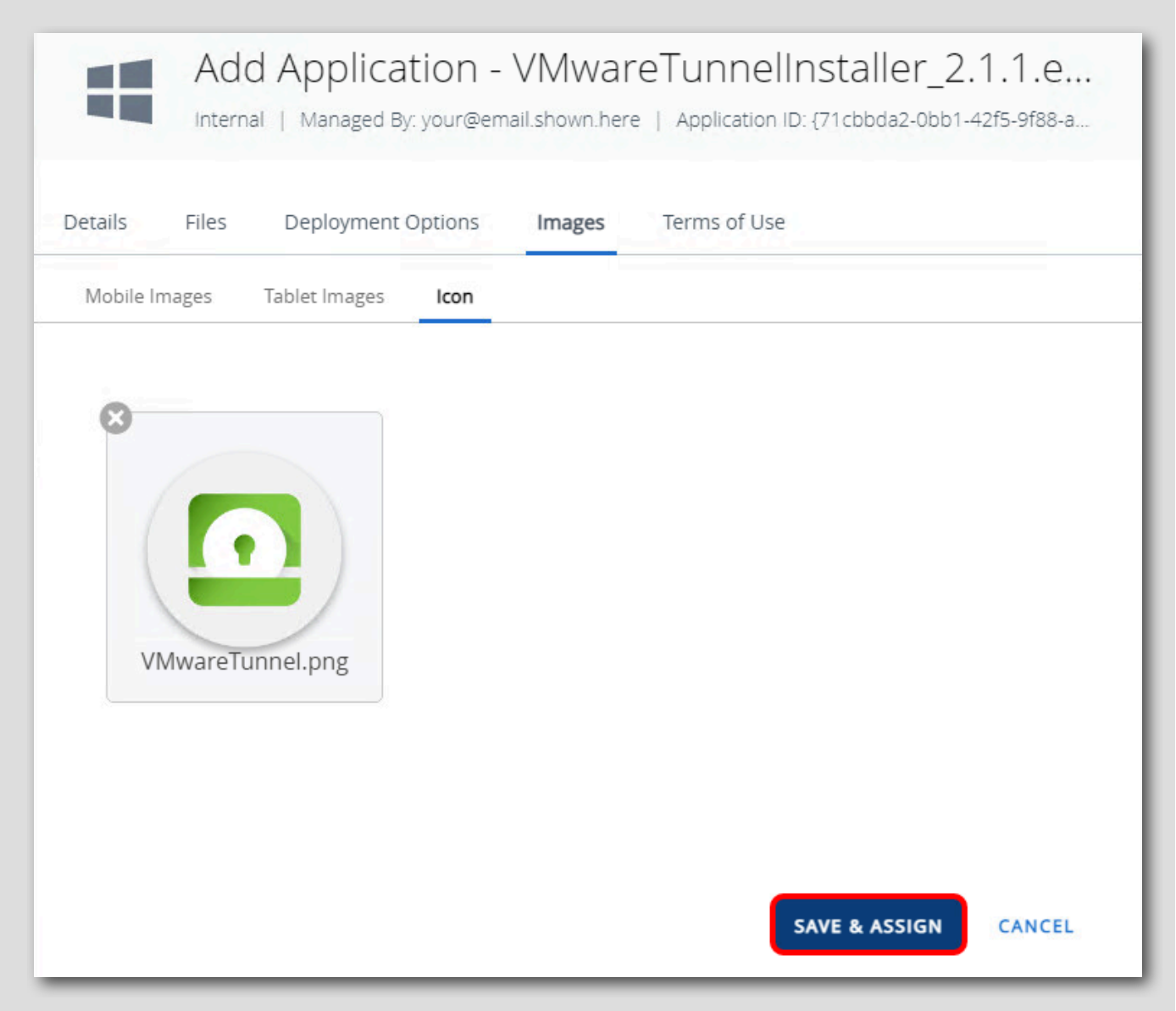
[754]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [VMwareTunnel.png] ファイルを選択します。
4. [Open] をクリックします。

保存して割り当て

[755]

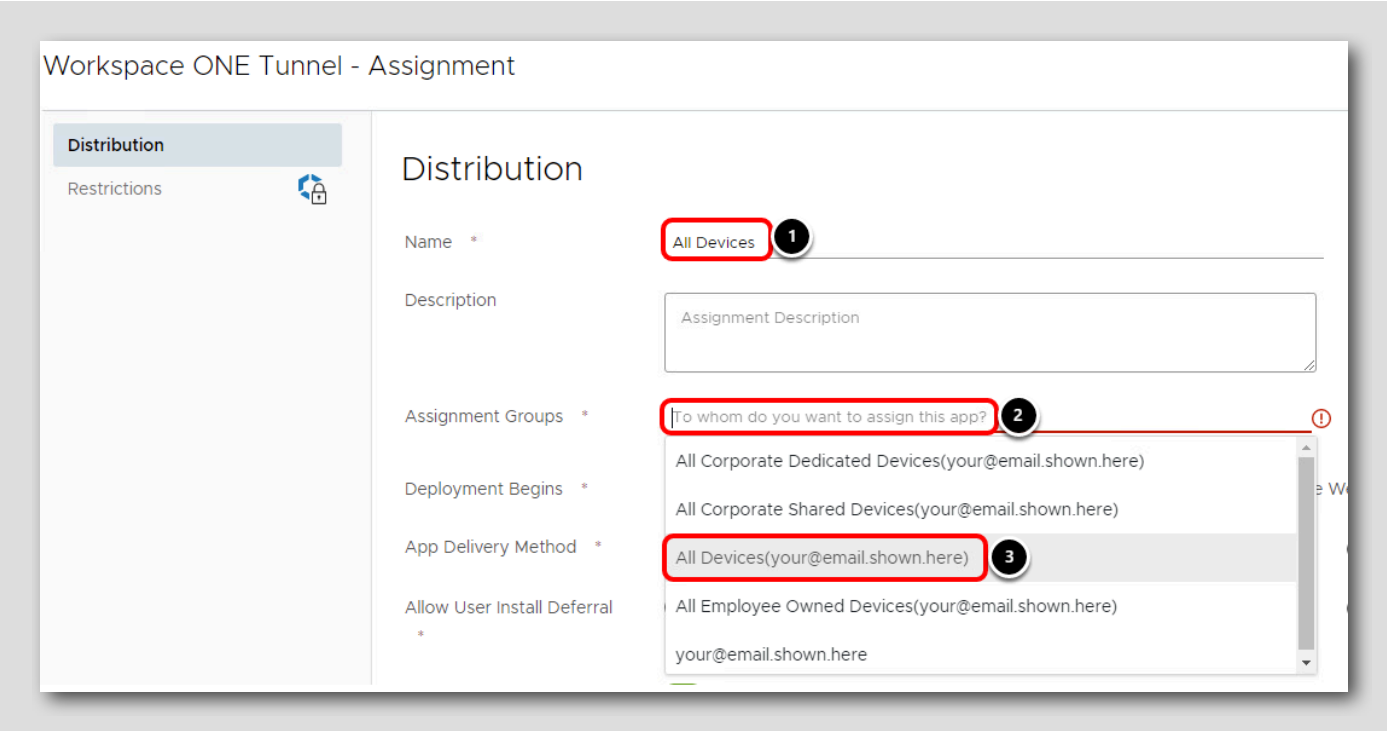


アプリケーションの構成が完了しました。[Save & Assign] をクリックします。

アプリケーション割り当ての作成

[756]

Workspace ONE UEM がアプリケーションのインストールとアンインストールの方法を認識できるように、アプリケーションと入力の詳細をアップロードしたので、組織内のどのユーザーまたはデバイスがこのアプリケーションを受け取るかを割り当てる必要があります。

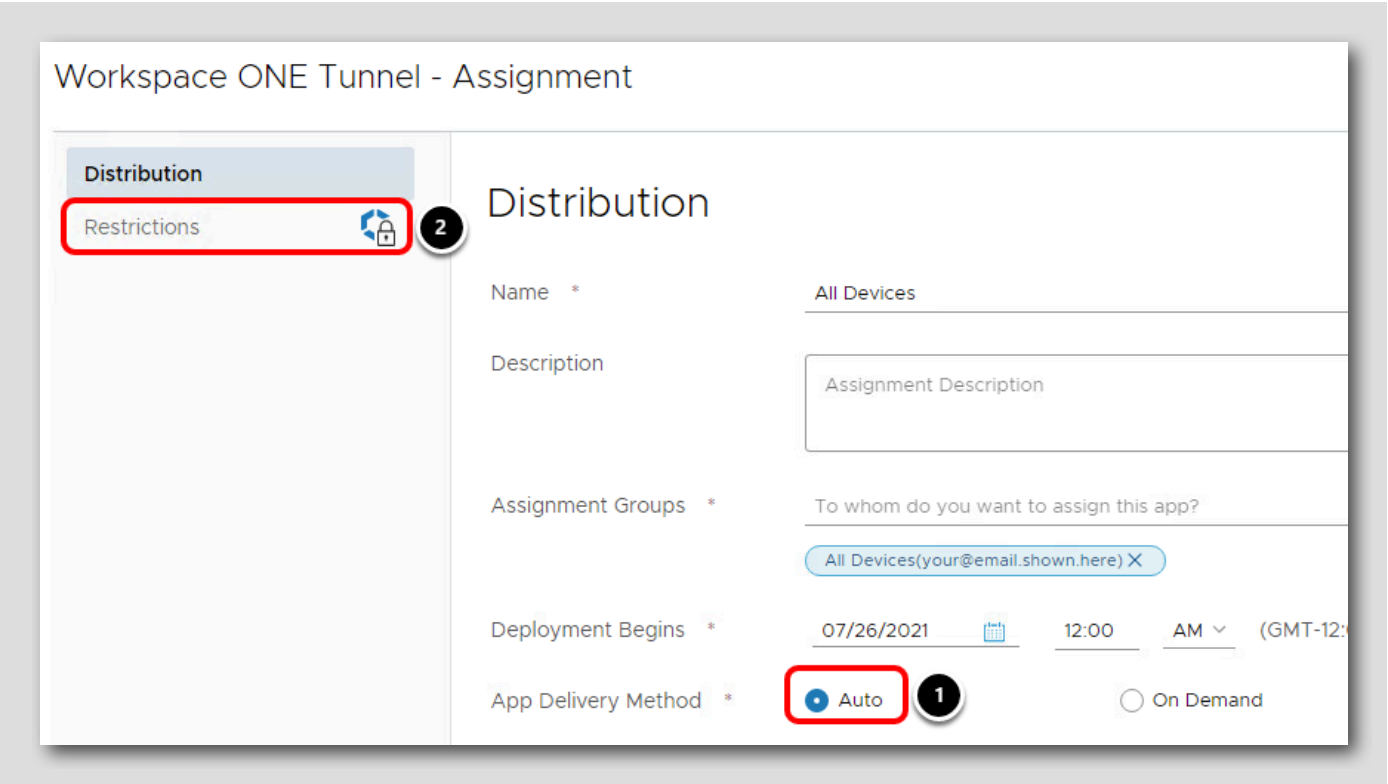


1. [Assignment Name] に **`All Devices`** と入力します。
2. **[Assignment Groups]** 入力フィールドをクリックします。
3. **[All Devices (your@email.shown.here)]** オプションをクリックします。

[All Devices] グループへのこの割り当ては、ユーザーまたはタイプ（従業員所有、企業所有など）に関係なく、組織に登録するすべての Windows 10 デバイスがアプリケーションを受信することを示します。

配信方法の更新

[757]

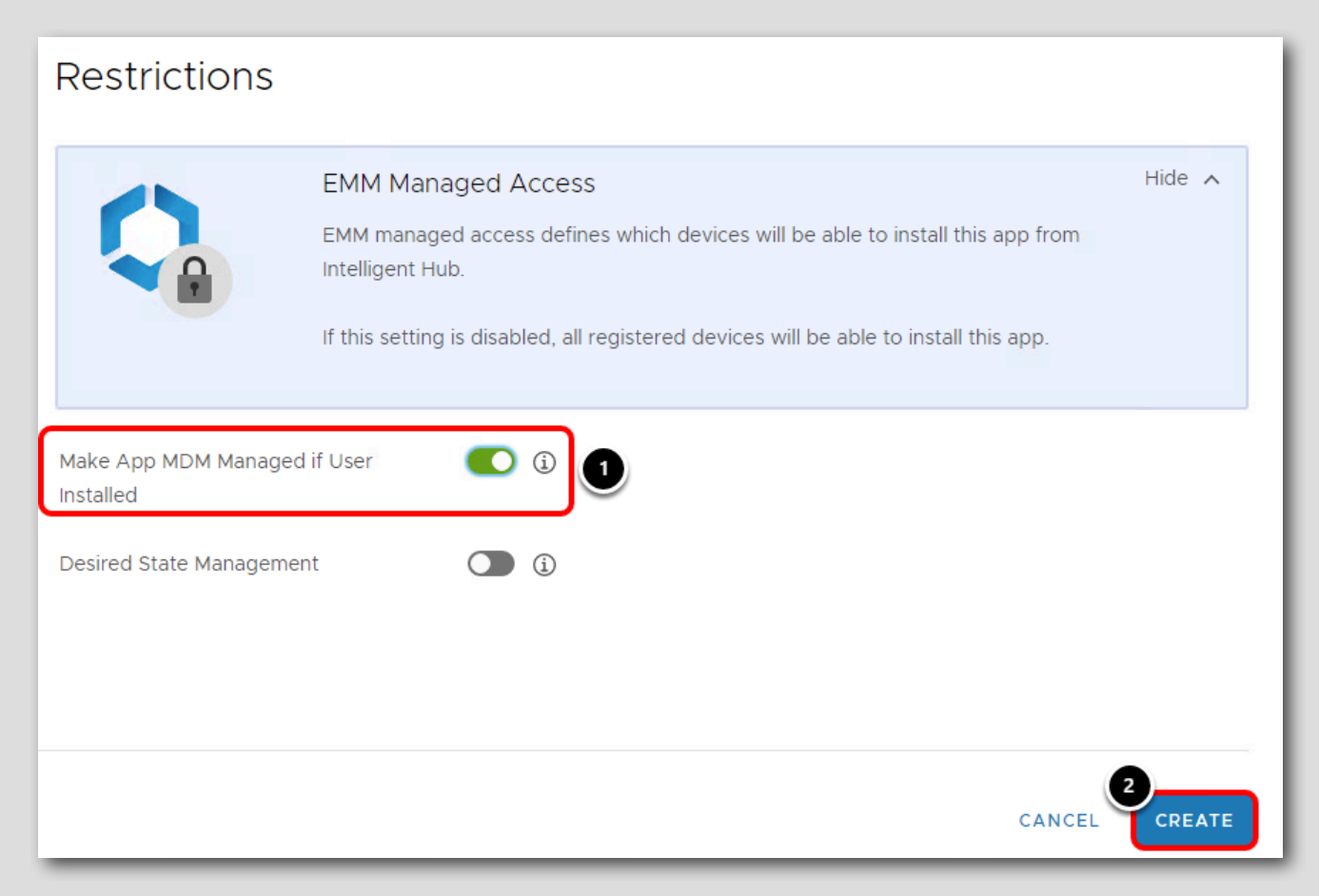


1. [App Delivery Method] に対して **[Auto]** を選択します。
2. **[Restrictions]** をクリックします。

[App Delivery Method] を [Auto] に構成すると、組織内に登録されている Windows 10 デバイスにアプリケーションが自動的に配信されます。必要に応じてユーザーがアプリケーションをダウンロードできるようにするには、[On Demand] を選択してください。

制限事項の更新

[758]

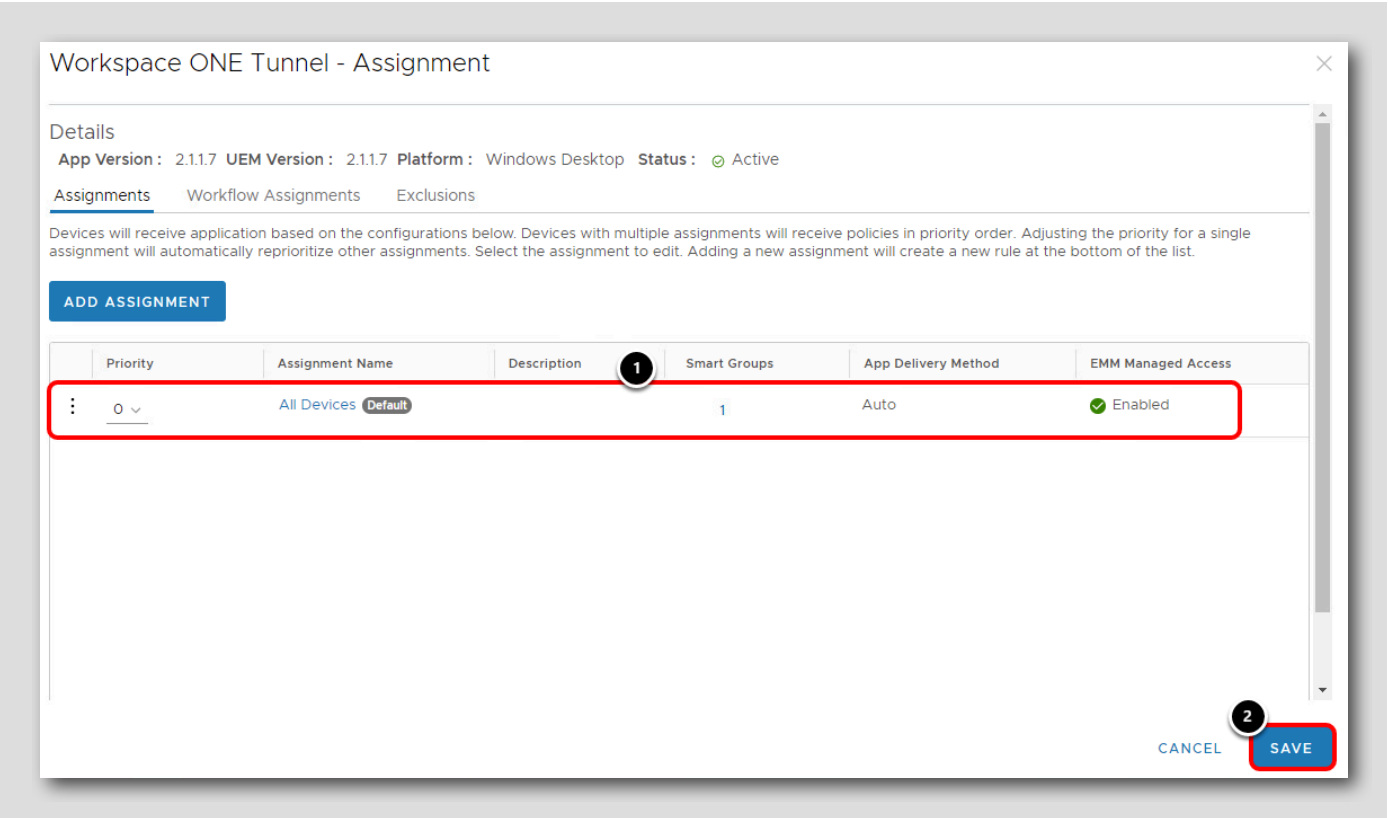


1. [Make App MDM Managed if User Installed] オプションを有効にします。
2. [Create] をクリックします。

[Make App MDM Managed if User Installed] オプションは、デバイスにインストールされる Workspace ONE Tunnel アプリケーションがすでに存在する場合は上書きします。デバイスが MDM (Workspace ONE UEM) によって管理されていない場合は、構成をデバイスにプッシュダウンできないため、これは構成をデバイスにプッシュダウンする必要がある場合に重要になる可能性があります。このオプションを有効にすると、デバイスにインストールされているすべての Workspace ONE Tunnel アプリケーションが MDM で管理されるようになります。

アプリケーション割り当ての保存

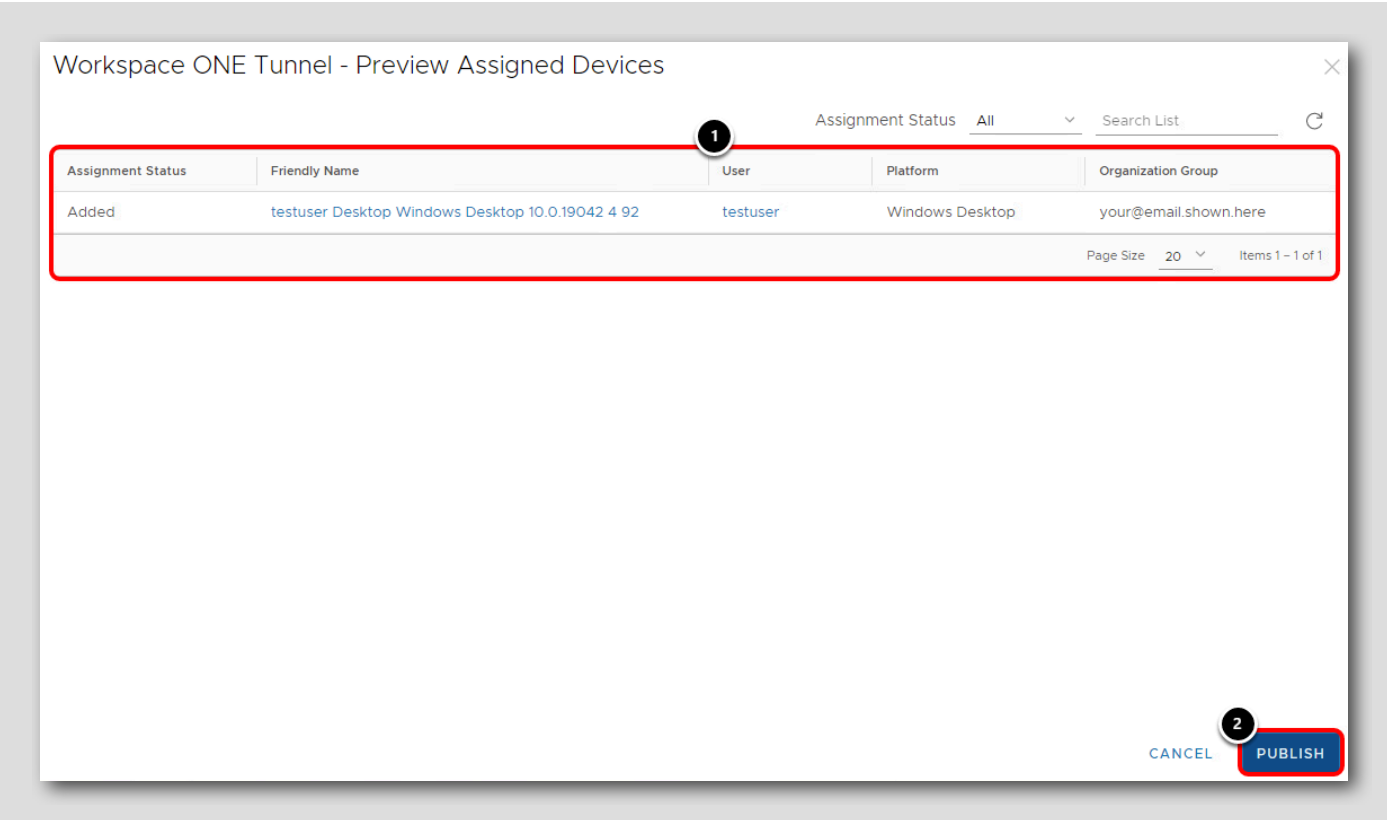
[759]



1. 作成した [All Devices] 割り当てが表示されることを確認します。
2. [Save] をクリックします。

アプリケーションの公開

[760]



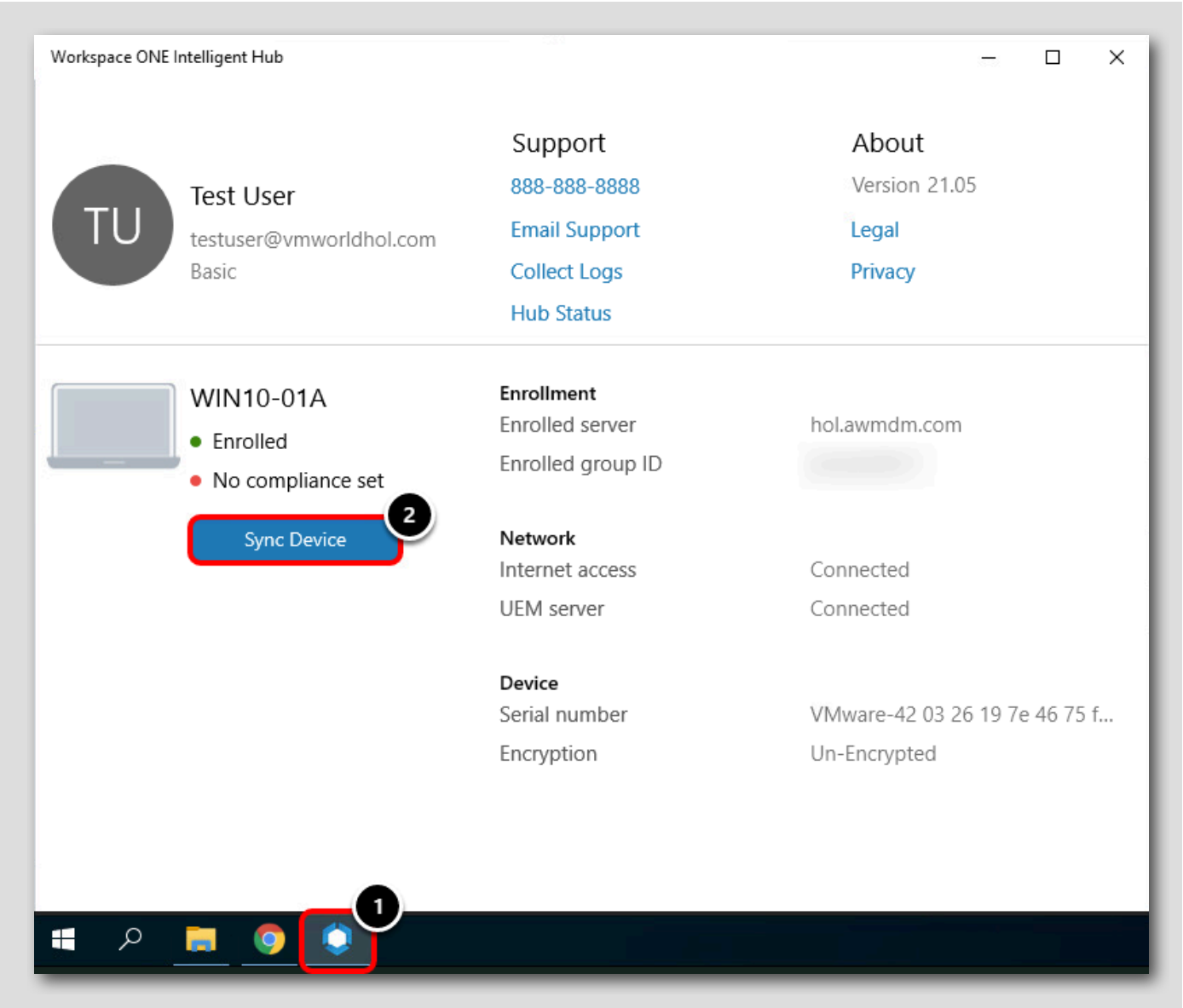
これでアプリケーションが構成され、割り当てられ、公開の準備が整いました。公開すると、ユーザーがアプリケーションとその構成を使用できるようになります。

1. このアプリケーション割り当てを受信するデバイスのプレビューがここに表示されます。Windows 10 仮想マシンはすでに登録されているため、このプレビューに表示されます。
2. [Publish] をクリックします。

Workspace ONE Tunnel インストールの検証

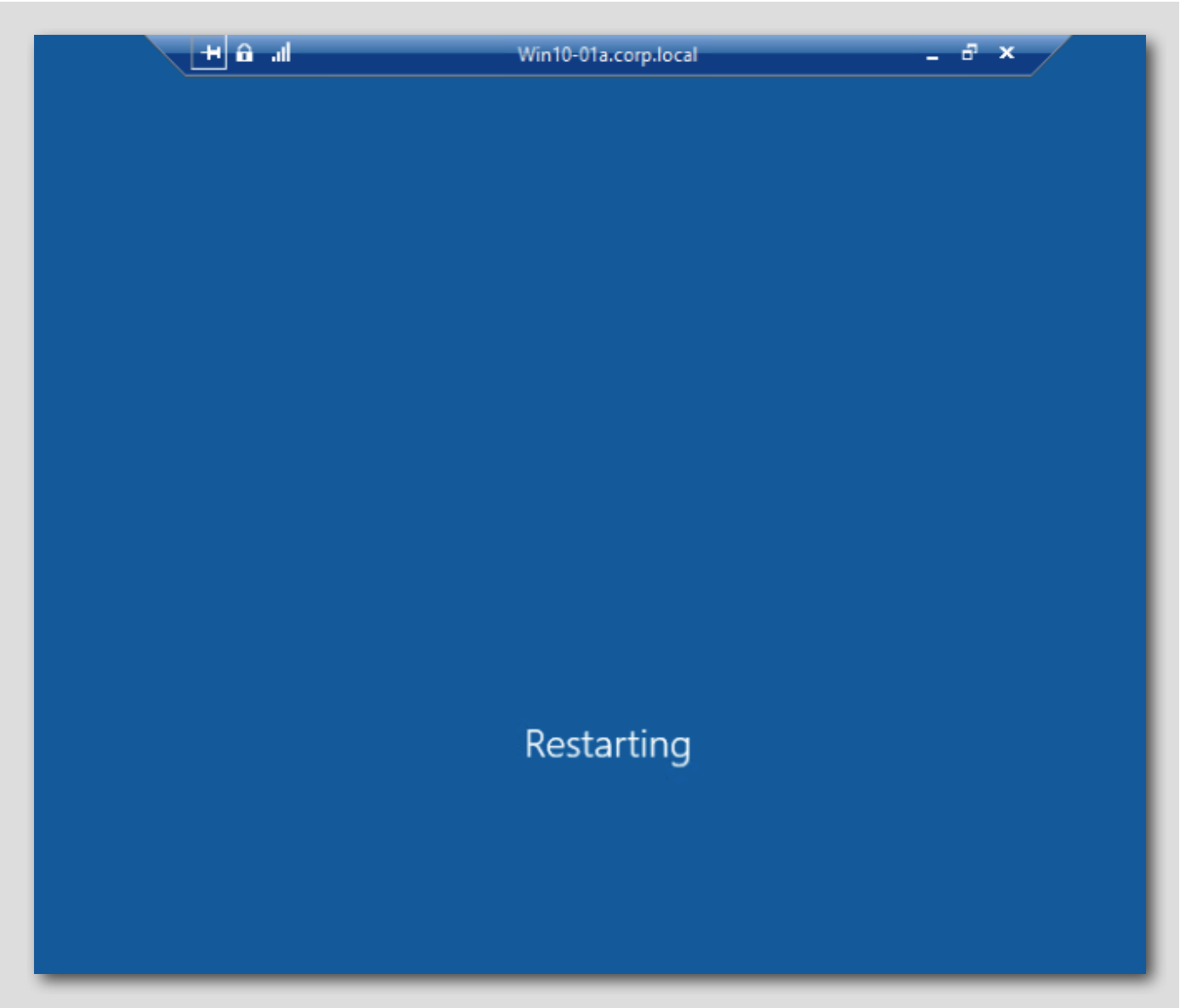
[761]

デバイスに公開された Workspace ONE Tunnel アプリケーションは、インストールを完了するために再起動する必要があります。セットアップされたアプリケーション構成は、アプリケーションのインストールが完了すると、デバイスを自動的に再起動します。



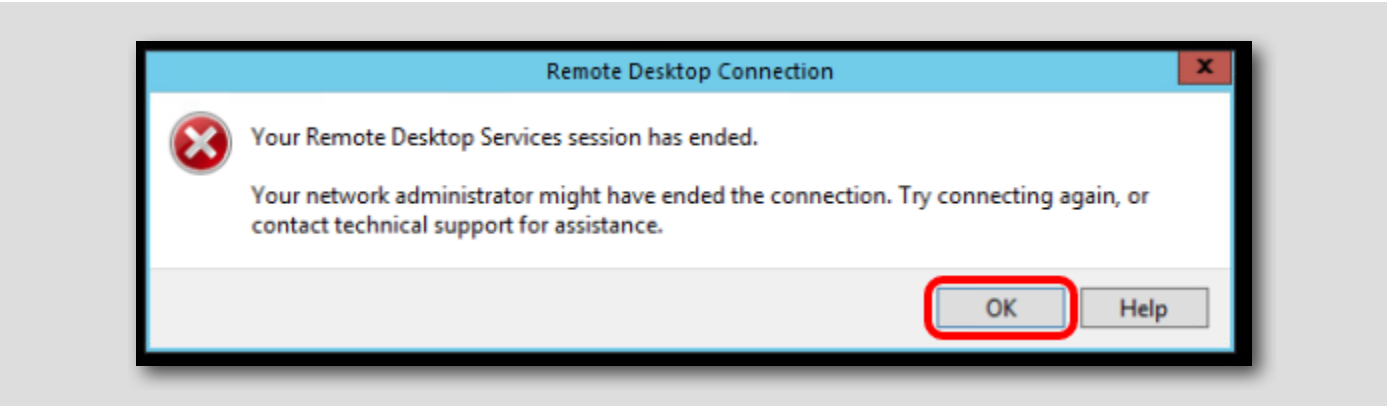
アプリケーションのインストールをトリガする同期プロセスを迅速化するには、次の手順を実行します。

1. タスク バーの [Workspace ONE Intelligent Hub app] をクリックします。
2. [Sync Device] をクリックします。

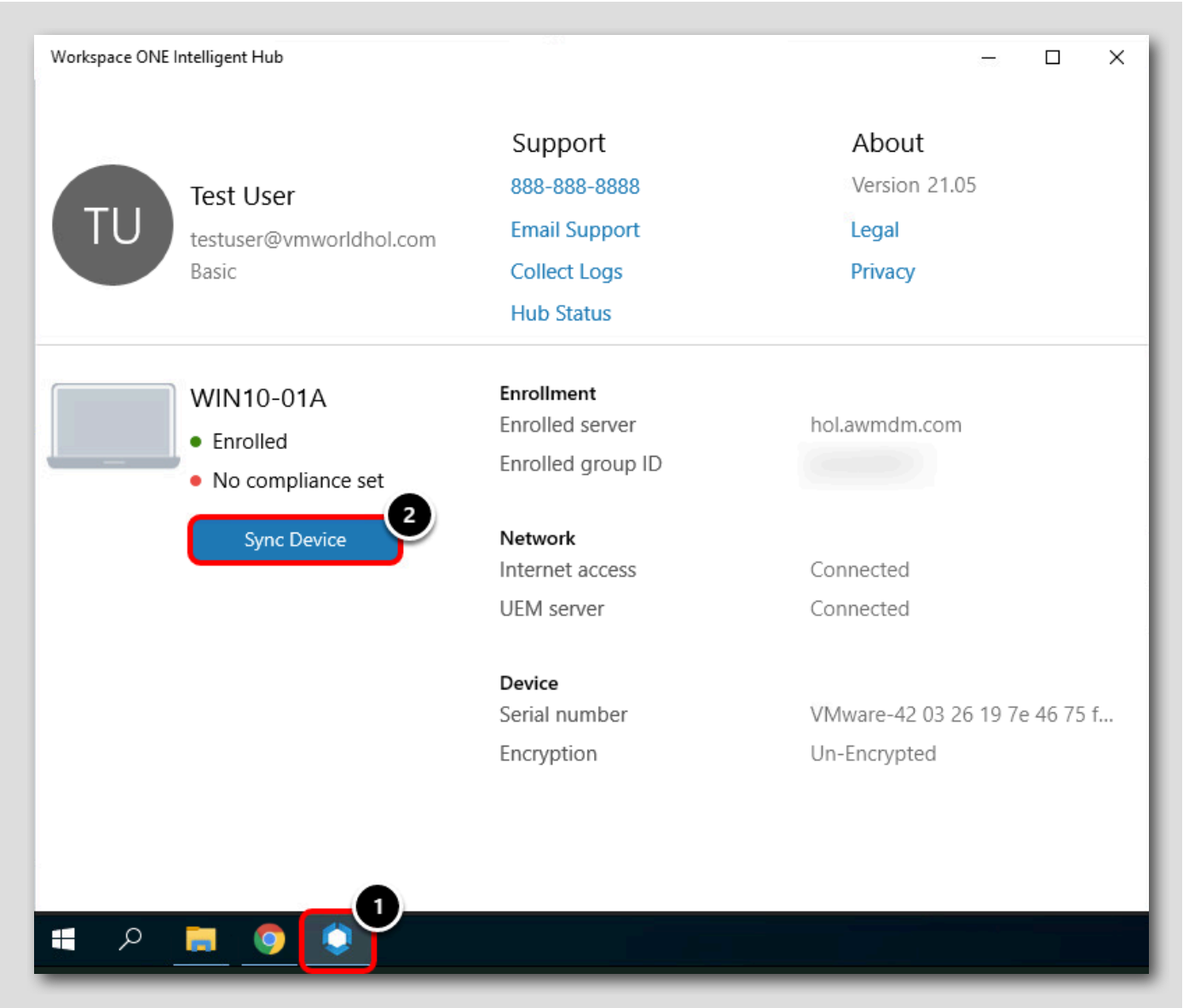


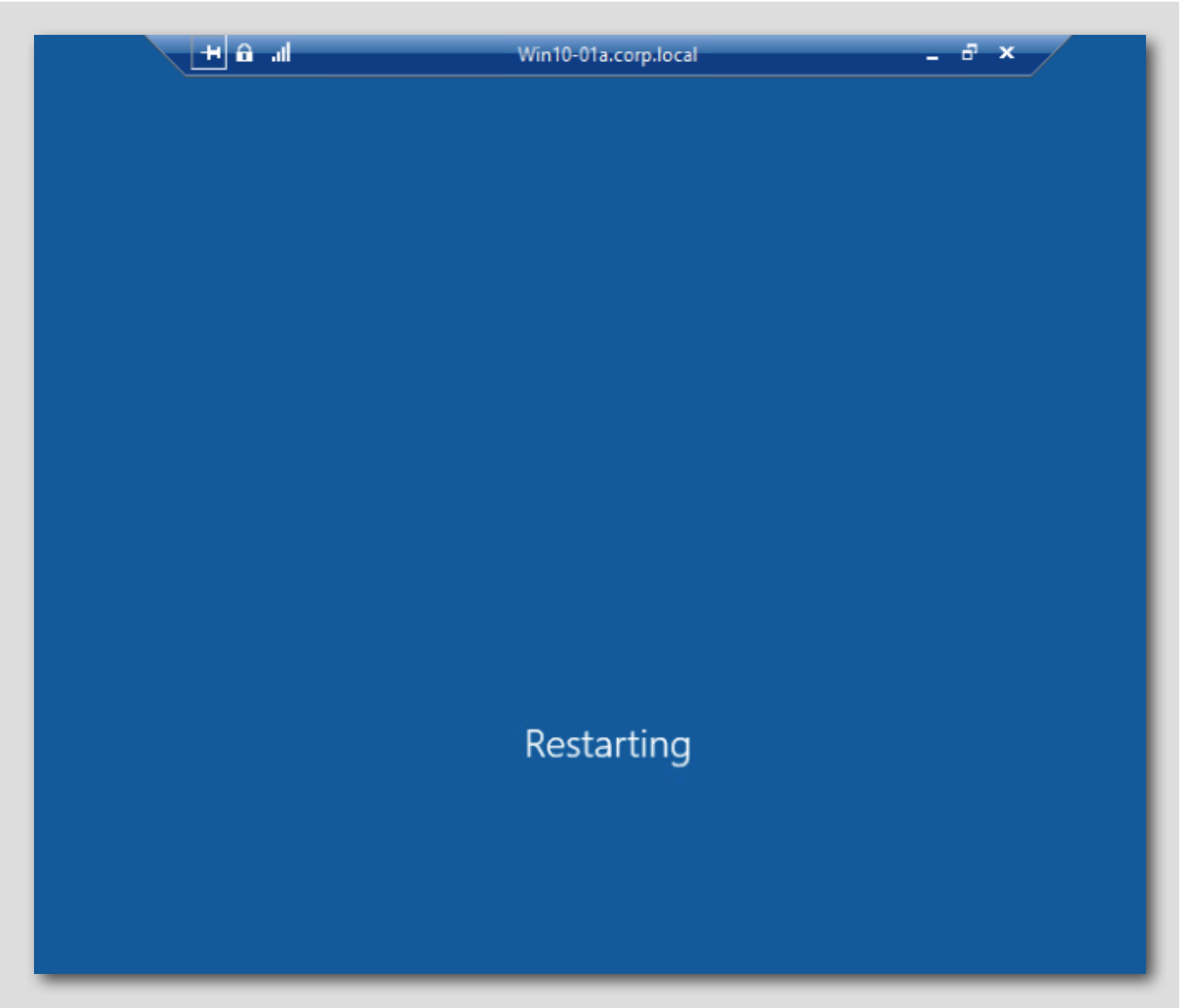
デバイスに公開された Workspace ONE Tunnel アプリケーションは、インストールを完了するために再起動する必要があります。セットアップされたアプリケーション構成は、アプリケーションのインストールが完了すると、デバイスを自動的に再起動します。

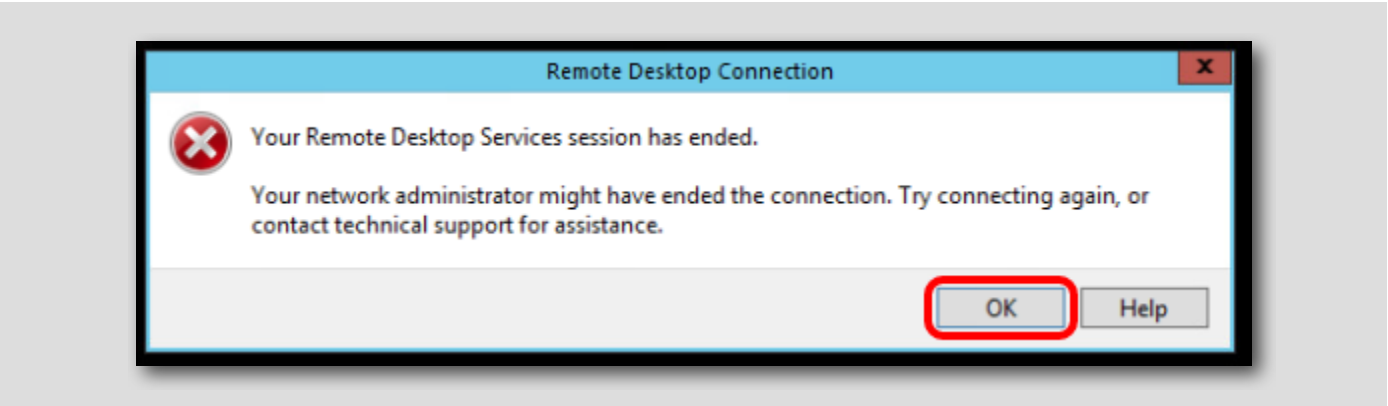
重要：Workspace ONE Tunnel アプリケーションのインストールには数分かかる場合があるため、自動再起動がすぐにトリガされないことがあります。デバイスが自動的に再起動されるまでお待ちください。手動で再起動をトリガしないでください。



デバイスの再起動がトリガされると、リモート デスクトップ接続が終了したという通知が表示されます。[OK] をクリックします。

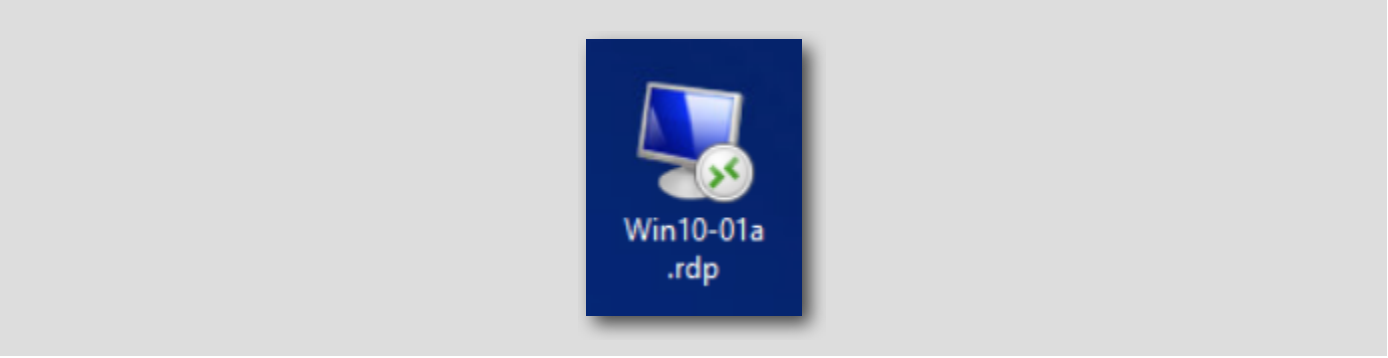

Workspace ONE Intelligent Hub
TU
Test User
testuser@vmworldhol.com
Basic
Support
888-888-8888
Email Support
Collect Logs
Hub Status
About
Version 21.05
Legal
Privacy
WIN10-01A
Enrolled
No compliance set
Sync Device
2
Enrollment
Enrolled server
hol.awmdm.com
Enrolled group ID
Network
Internet access
Connected
UEM server
Connected
Device
Serial number
VMware-42 03 26 19 7e 46 75 f...
Encryption
Un-Encrypted
1


Win10-01a.corp.local
Restarting



Win10-01a 仮想マシンへの再接続

[762]



メイン コンソール デスクトップで、[Win10-01a.rdp] ショートカットをダブルクリックして仮想マシンに再接続します。

注: デバイスの再起動が完了するまでに数分かかる場合があります。接続に失敗した場合は、1 分間待ってから再試行してください。

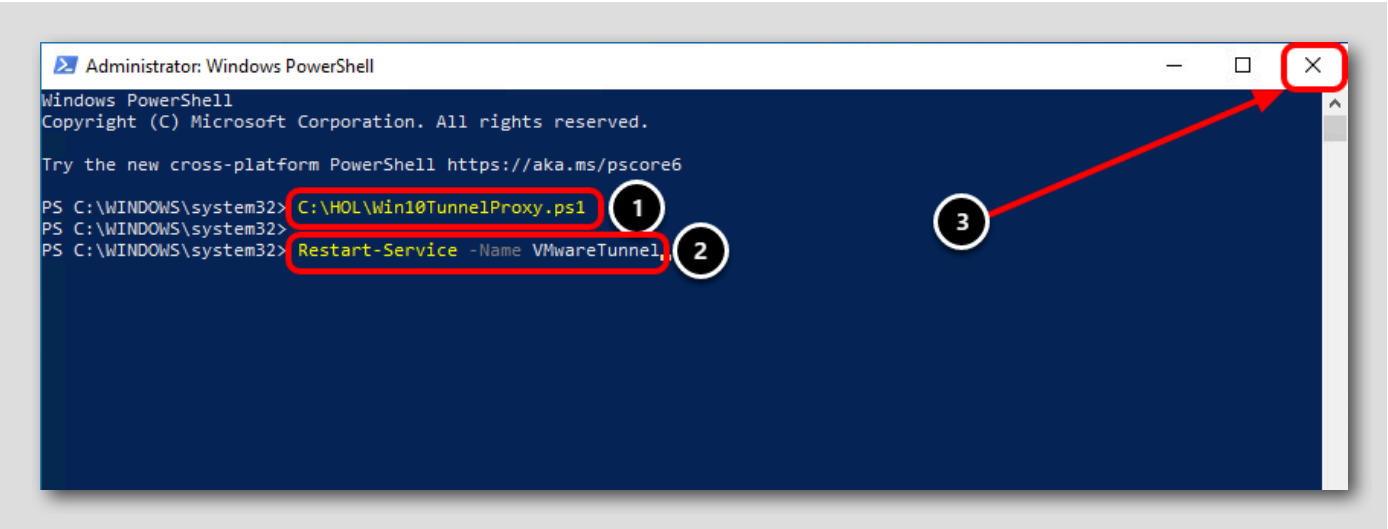
Microsoft PowerShell の起動

[763]

1. Windows の [Start] ボタンを右クリックします。
2. [Windows PowerShell (Admin)] をクリックします。

プロキシ セットアップ スクリプトの実行

[764]



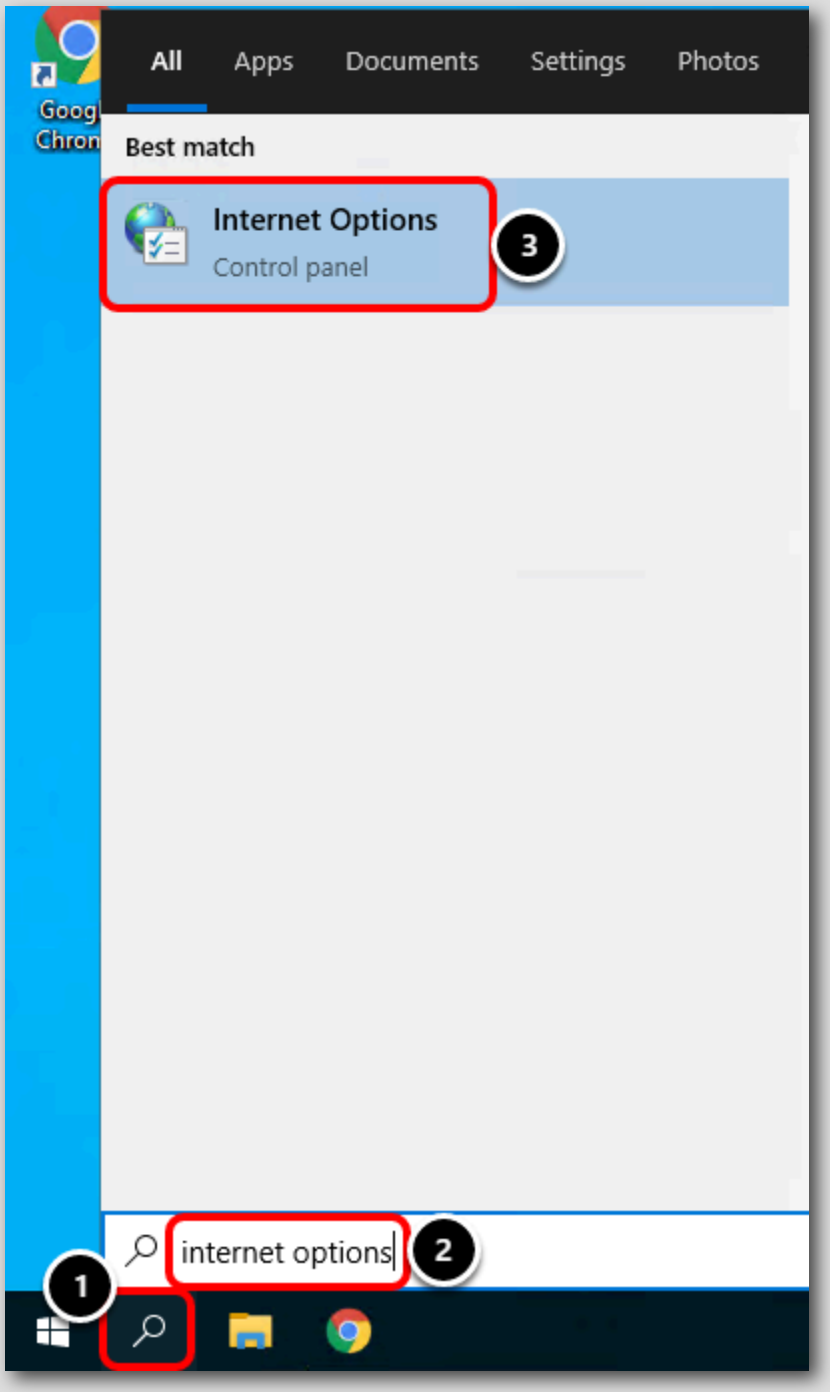
注: 入力ミスを避けるために、上のテキストをクリックして強調表示し、HOL コンソールにドラッグアンドドロップして貼り付けることができます。

1. **`C:\HOL\Win10TunnelProxy.ps1`** コマンドを入力し、**ENTER** キーを押します。
2. **`Restart-Service -Name VMwareTunnel`** コマンドを入力し、**ENTER** キーを押します。
3. **[X]** をクリックして、PowerShell を閉じます。

ハンズオン ラボ環境のネットワークにより、送信トラフィックがネットワークから離れるようにするには、プロキシ設定にエントリを入力する必要があります。このスクリプトは、この更新を自動的に行います。

プロキシ設定の確認

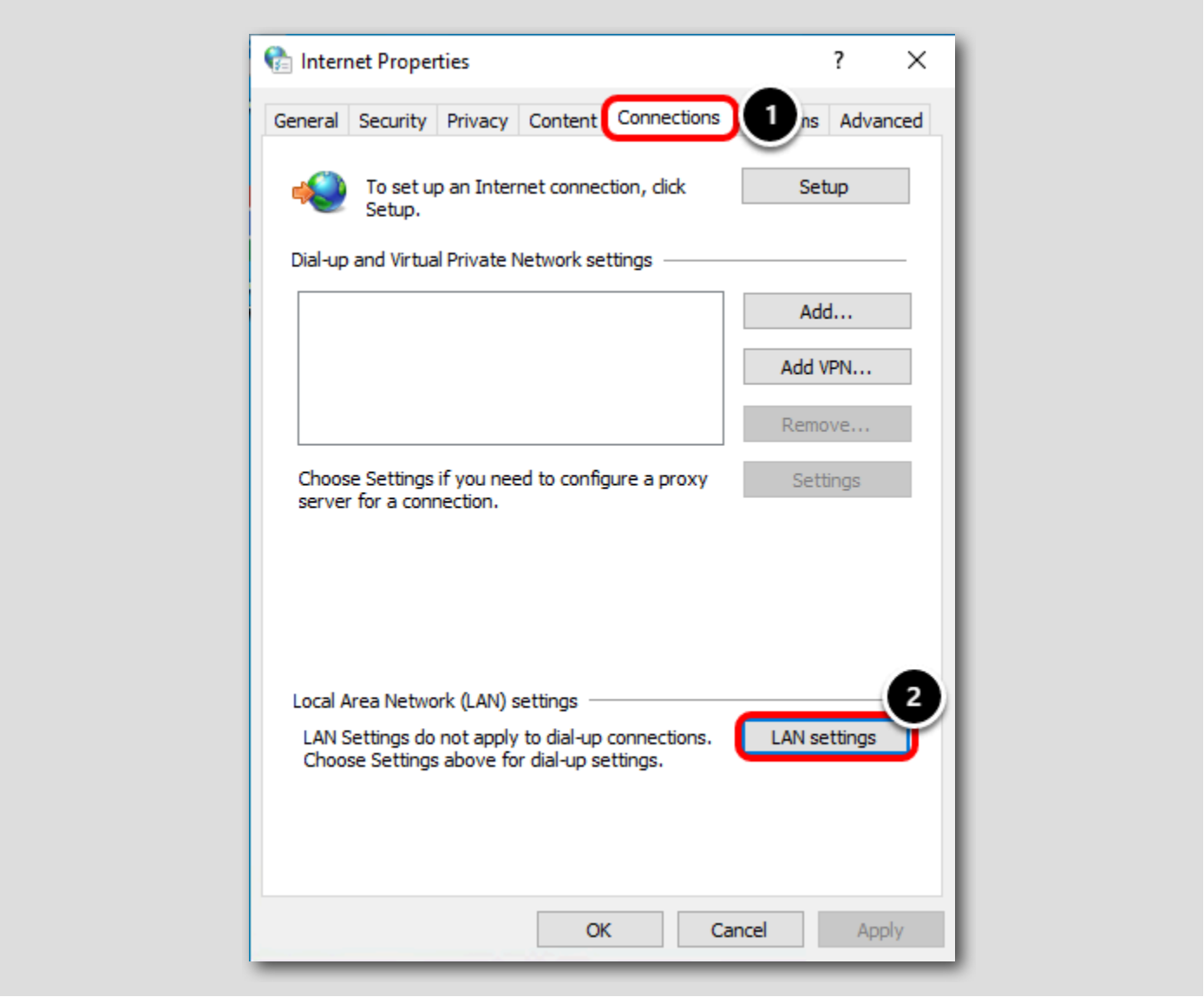
[765]

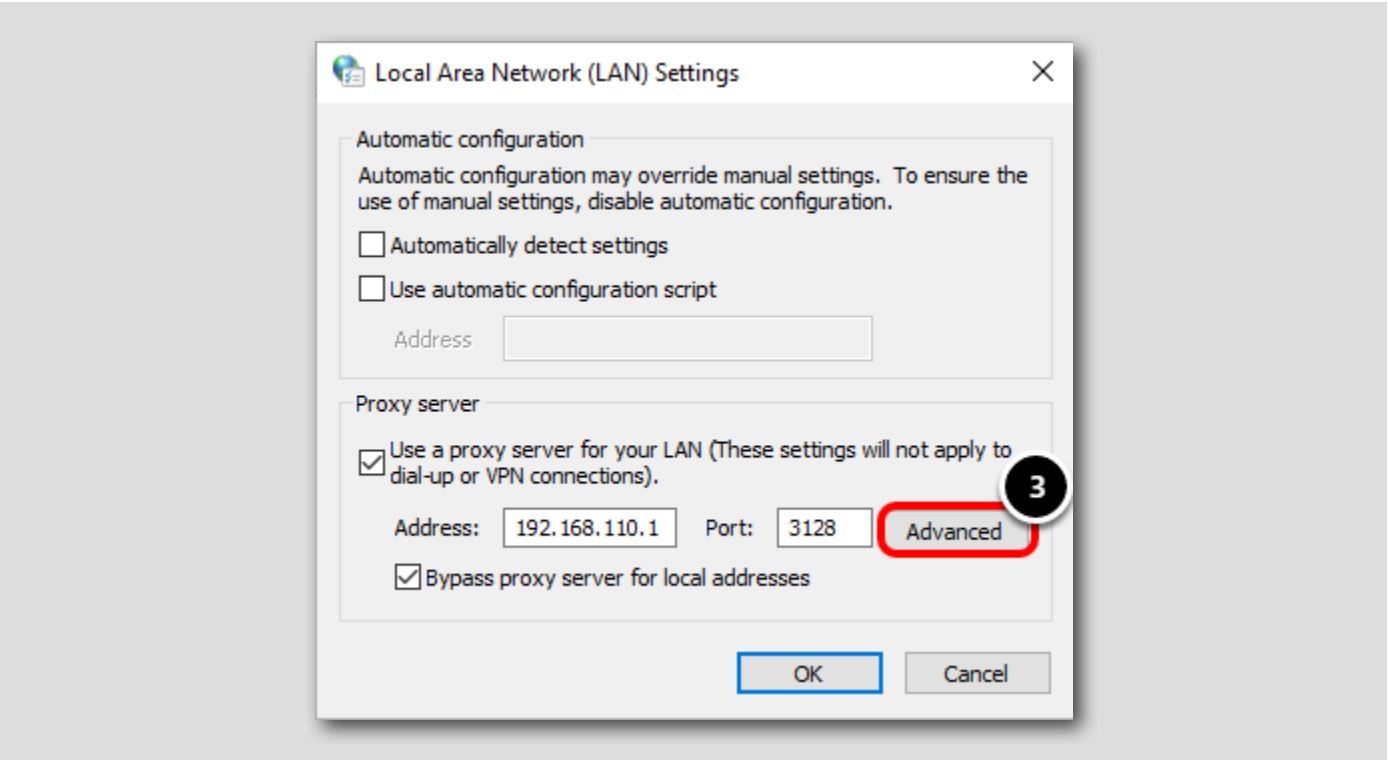


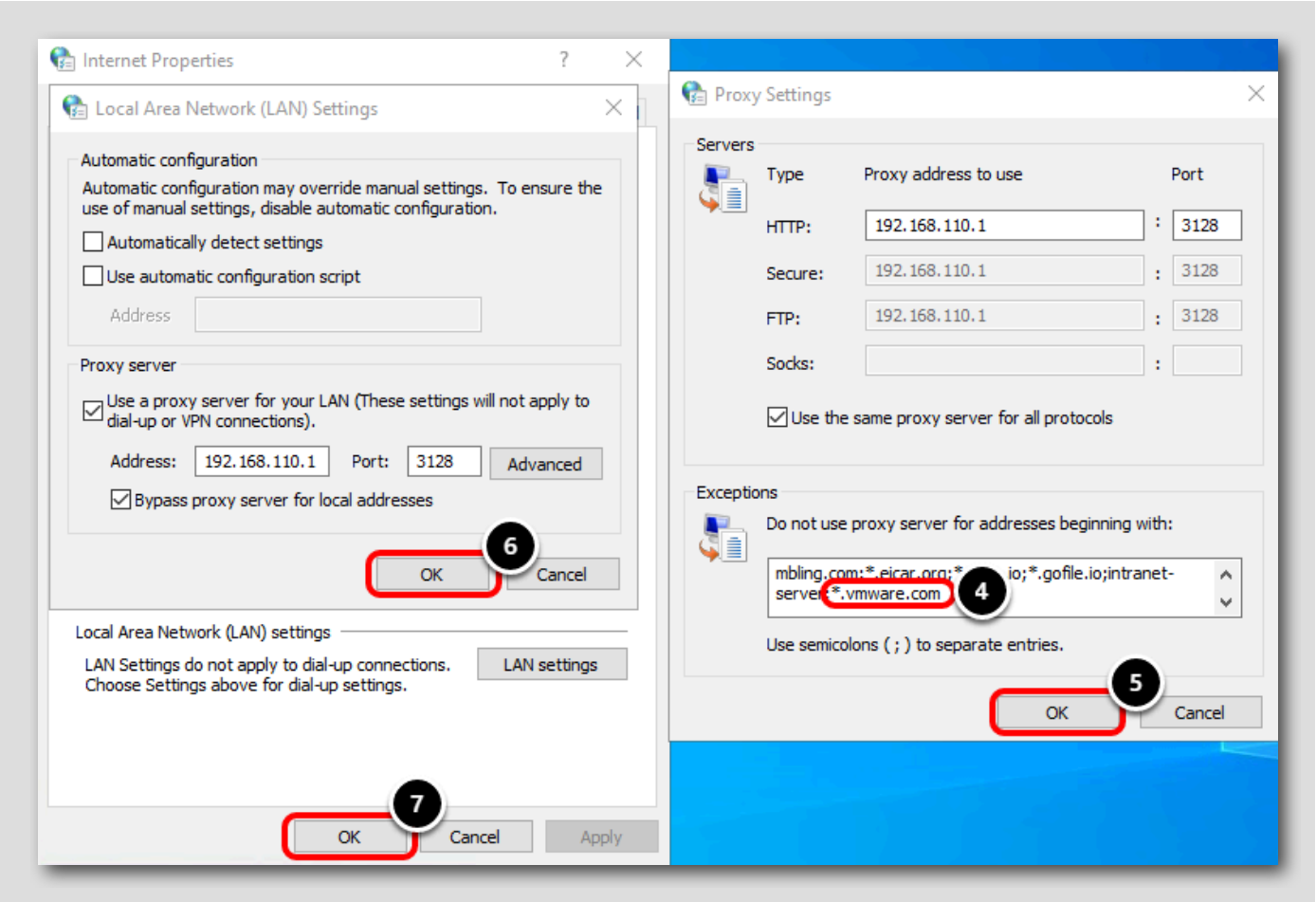
1. タスク バーの [Search] アイコン をクリックします。
2. **`internet options`** と入力します。
3. [Internet Options] をクリックします。

プロキシ例外の確認

[766]



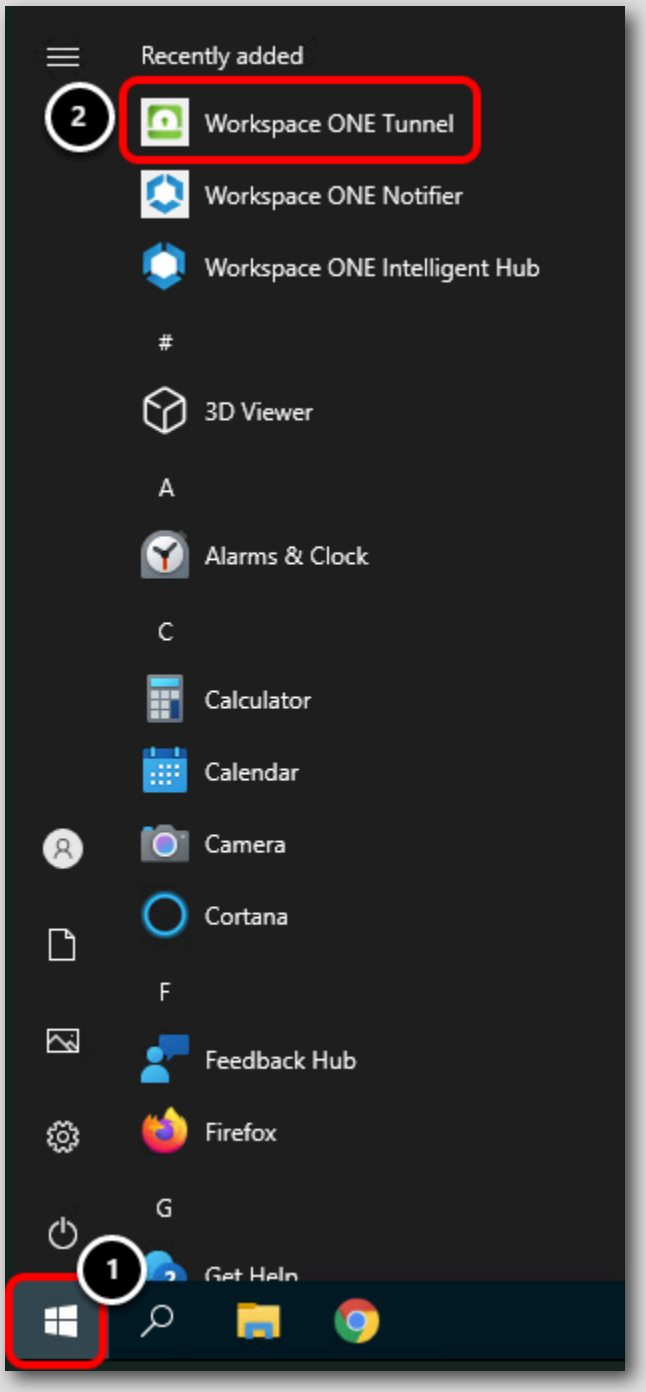

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
192.168.110.1
Port:
3128
Advanced
3
Bypass proxy server for local addresses
OK
Cancel



1. [Internet Options] で、**[Connections]** タブをクリックします。
2. **[LAN Settings]** をクリックします。
3. **[Advanced]** をクリックします。
4. [Exceptions] リストに `*.vmware.com` エントリが含まれていることを確認します。
5. [Proxy Settings] で **[OK]** をクリックして、ページを閉じます。
6. [Local Area Network (LAN) Settings] で **[OK]** をクリックして、ページを閉じます。
7. [Internet Properties] で **[OK]** をクリックして、ページを閉じます。

Workspace ONE Tunnel アプリケーションの起動

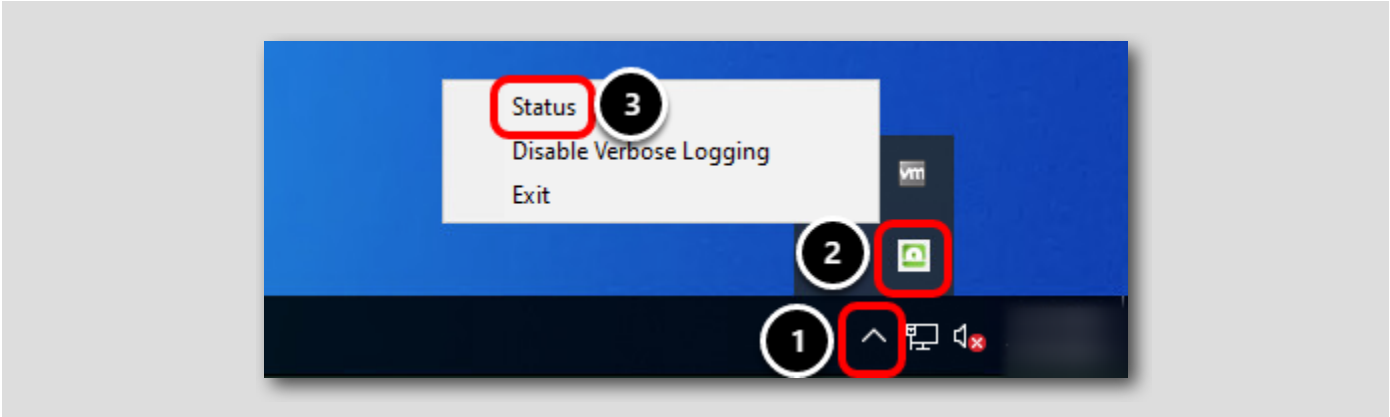
[767]



1. Windows の [Start] ボタンをクリックします。
2. [Recently added] の下にある [Workspace ONE Tunnel] アプリケーションをクリックします。

[Workspace ONE Tunnel Status] ページを開く

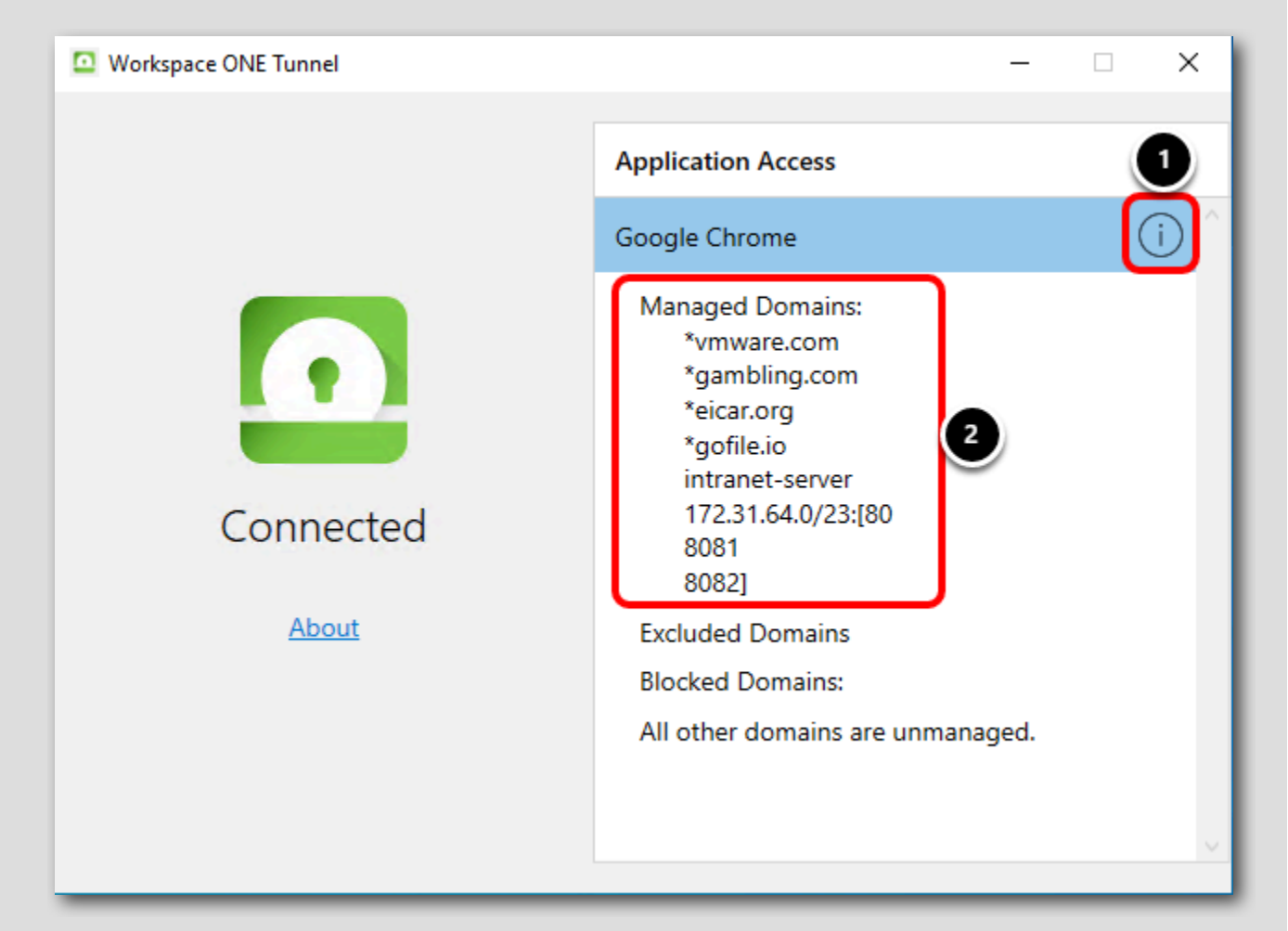
[768]



1. タスク バーのドロップダウン ボタンをクリックして、他のアプリケーションを表示します。
2. システム ツールバーから Workspace ONE Tunnel アプリケーションのアイコンを右クリックします。
3. [Status] をクリックします。

Tunnel のステータスの確認

[769]



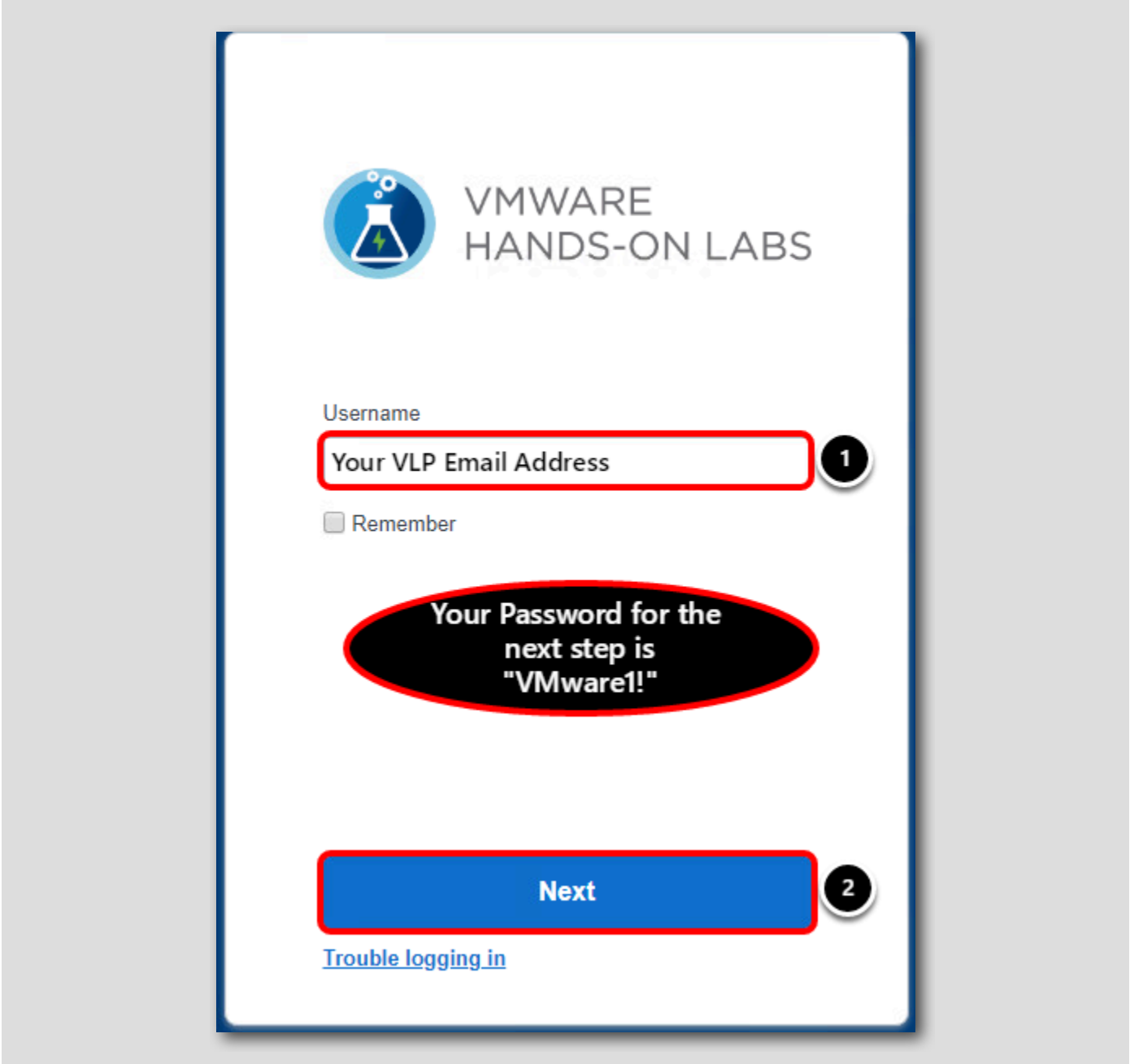
1. Google Chrome の横にある (i) アイコンクリックして構成を表示します。
2. Google Chrome アプリケーションが一連のドメイン（*vmware.com、*gambling.com など）と IP アドレス CIDR ブロックおよびポート（172.31.64.0/23 ポート 80、8081、8082 など）を Tunnel サービスを介して送信するように構成されていることを確認できます。

Workspace ONE UEM Console へのログイン

[770]

現在接続している仮想マシンのデスクトップにある [Google Chrome] ショートカットをダブルクリックします。

Workspace ONE UEM 管理コンソールでの管理者ユーザー名の入力 [771]

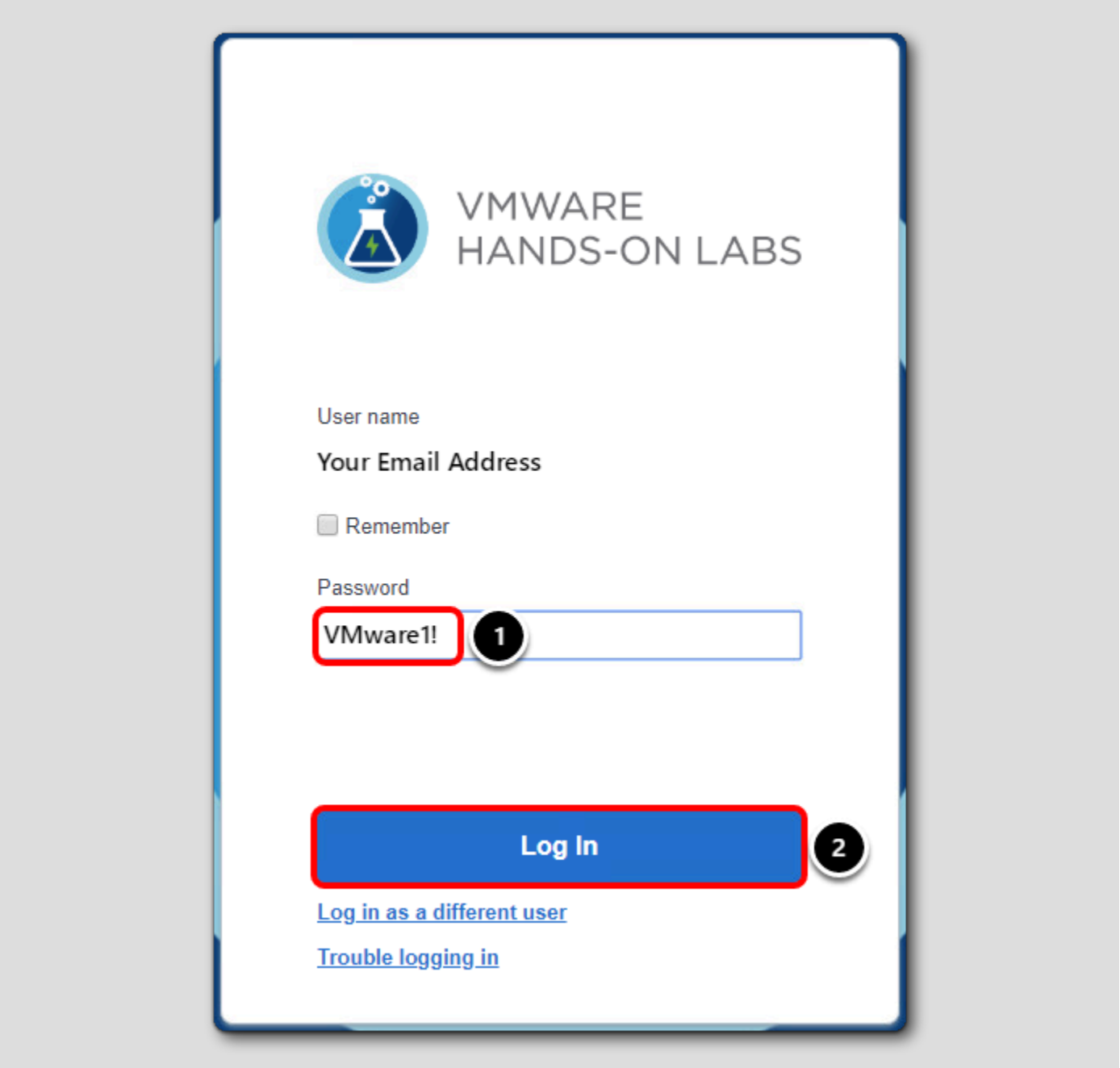


ブラウザのデフォルトのホーム ページは https://hol.awmdm.com です。Workspace ONE UEM 管理者アカウント情報を入力し、[Login] ボタンをクリックします。

1. [Username] を入力します。これは、ハンズオン ラボを受講するために以前に利用した VMware Learning Platform (VLP) アカウントに関連付けたメール アドレスです。
2. [Next] をクリックして、ラボ マニュアルの次の手順に進み、パスワードを入力します。これは常に **`VMware1!`** です。

注：Captcha による入力を求められた場合は、大文字と小文字を区別して入力してください。

Workspace ONE UEM Console の認証情報の入力 [772]



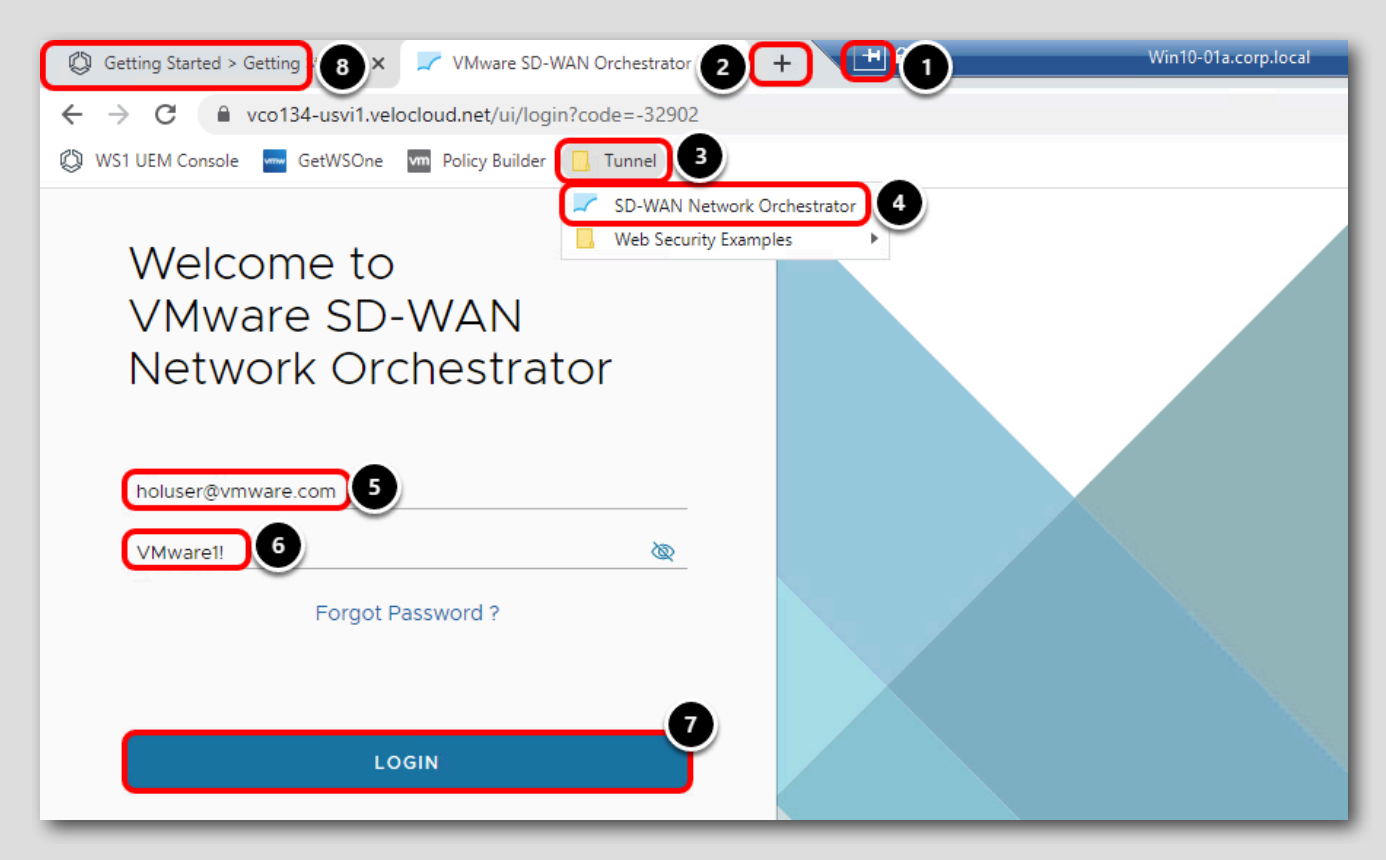
ユーザー名を入力すると、パスワード フィールドが表示されます。

1. [Password] フィールドに **VMware1!** と入力します。
2. [Log in] ボタンをクリックします。

注：ラボの制限により、ハンズオン ラボが Workspace ONE UEM ハンズオン ラボ サーバに接続するまでに、1～2 分かかる場合があります。

SD-WAN Network Orchestrator へのログイン

[773]

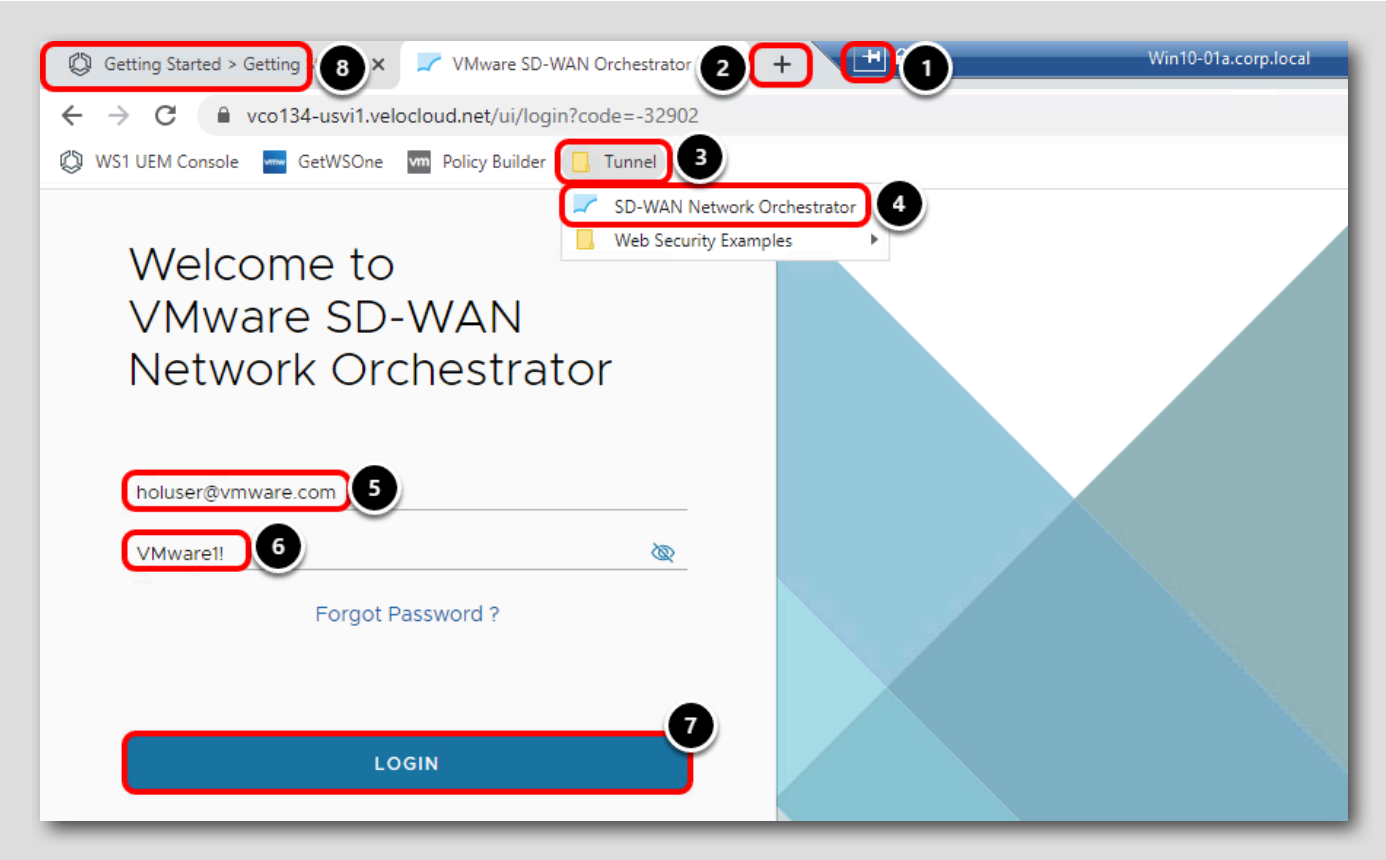


Workspace ONE UEM 管理者コンソールに加えて、このハンズオン ラボの SD-WAN Network Orchestrator コンソールに読み取り専用ユーザーとしてログインし、Workspace ONE Tunnel サービス ホスティング、Secure Access 設定、および Cloud Web Security ポリシーに関連するさまざまな設定を表示および確認します。

1. リモート デスクトップ タブの**ピン ボタン**をクリックすると、ブラウザのさまざまなタブに簡単にアクセスできるようになります。
2. [New Tab] ボタンをクリックして、新しいタブを開きます。
3. [Tunnel] ブックマーク フォルダをクリックします。
4. [SD-WAN Network Orchestrator] ブックマークをクリックします。
5. [Username] に **holuser@vmware.com** と入力します。

6. [Password] に **VMware1!** と入力します。
7. **[Login]** をクリックします。
8. **最初のタブ**をクリックして、Workspace ONE UEM に戻ります。

ラボ全体を通じて [SD-WAN Network Orchestrator] タブに定期的に戻る予定なので、このタブは開いたままにします。



イントラネット サイトへの正常な接続の検証

[774]

これで、次の構成が行われました。

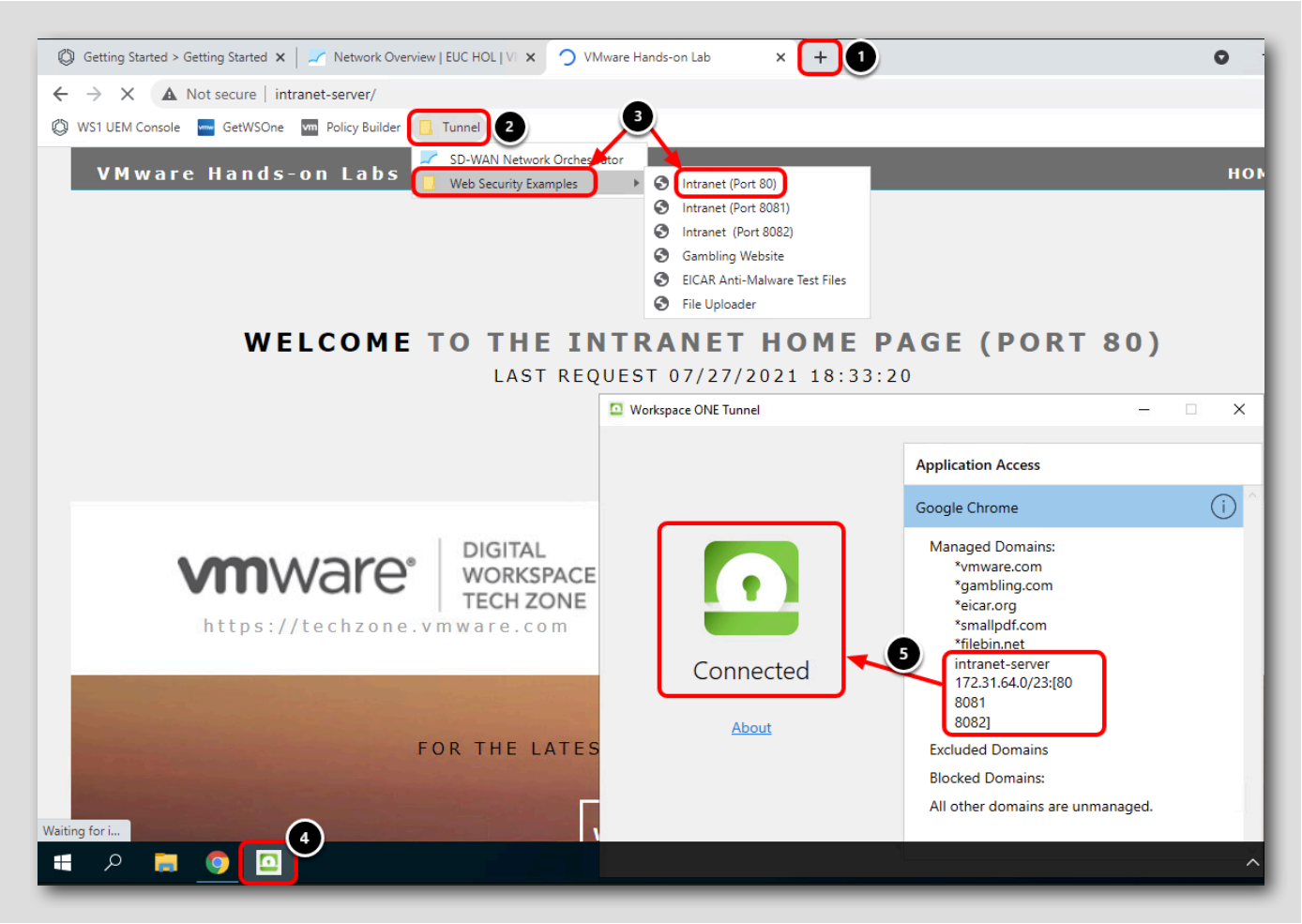
- Workspace ONE UEM テナントの Workspace ONE Tunnel 構成が、SASE PoP によってホストされている Tunnel サービスと統合されていることを確認しました。
- トンネル、プロキシ、またはバイパスするドメインと IP アドレスを指定するデバイス トンネル トラフィック ルールを確認しました。
- VPN ペイロードを含むプロファイルを作成し、デバイスに展開しました。
- Workspace ONE Tunnel アプリケーションをデバイスにインポート、構成、および展開しました。
- Workspace ONE Tunnel のインストール後にデバイスの再起動が必要な Windows 10 仮想マシンに再接続しました。

Workspace ONE Tunnel アプリケーションを展開して構成することで、イントラネット サイトへのアクセスを再度テストする準備が整いました。

今回は、Tunnel は同じプライベート ネットワークでホストされているため、Workspace ONE Tunnel デバイス トンネル トラフィック ルールで、ポート 80、8081、および 8082 の 172.31.64.0/23 範囲（イントラネット サーバがホストされている場所）の IP アドレスへの要求が Tunnel を通過するように指定されています。

ポート 80 のイントラネット Web サイトへの移動

[775]

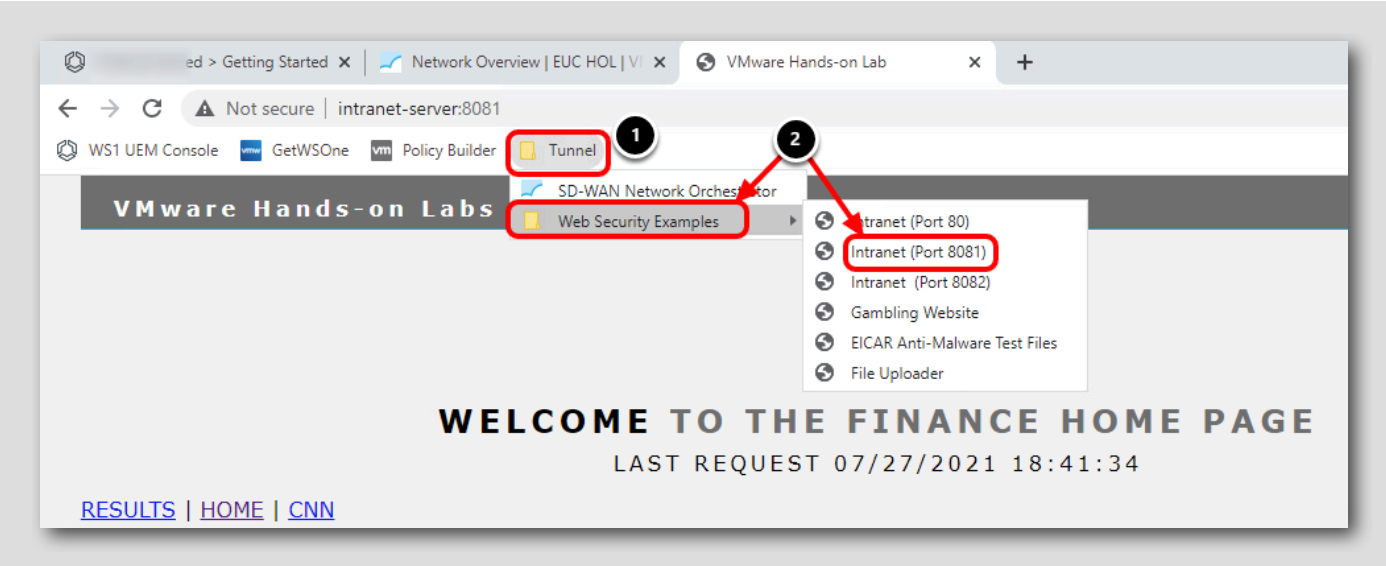


1. [New Tab] ボタンをクリックします。
2. [Tunnel] ブックマーク フォルダをクリックします。
3. [Web Security Examples] フォルダにカーソルを合わせ、[Intranet (Port 80)] ブックマーク リンクをクリックします。デバイスがローカル ホスト レコードを介して http://intranet-server サイトを解決できる Tunnel への正常な接続を確立できたため、イントラネット ホーム ページがロードされます。
4. タスク バーから Workspace ONE Tunnel アプリケーションをクリックします。
5. [Status] に [Connected] と表示されていることを確認します。これは、管理対象アプリケーションである Google Chrome が、デバイス トラフィック ルールから管理対象ドメインに接続し、SASE PoP によってホストされている Tunnel サービスに接続してエンドポイントに到達しようとしたために発生しました。

重要：サイトへの接続時にホスト名が解決できないというエラーが表示された場合は、Tunnel サービスが接続を確立している可能性があります。数秒待ってからページを更新してください。

ポート 8081 のイントラネット Web サイトへの移動

[776]

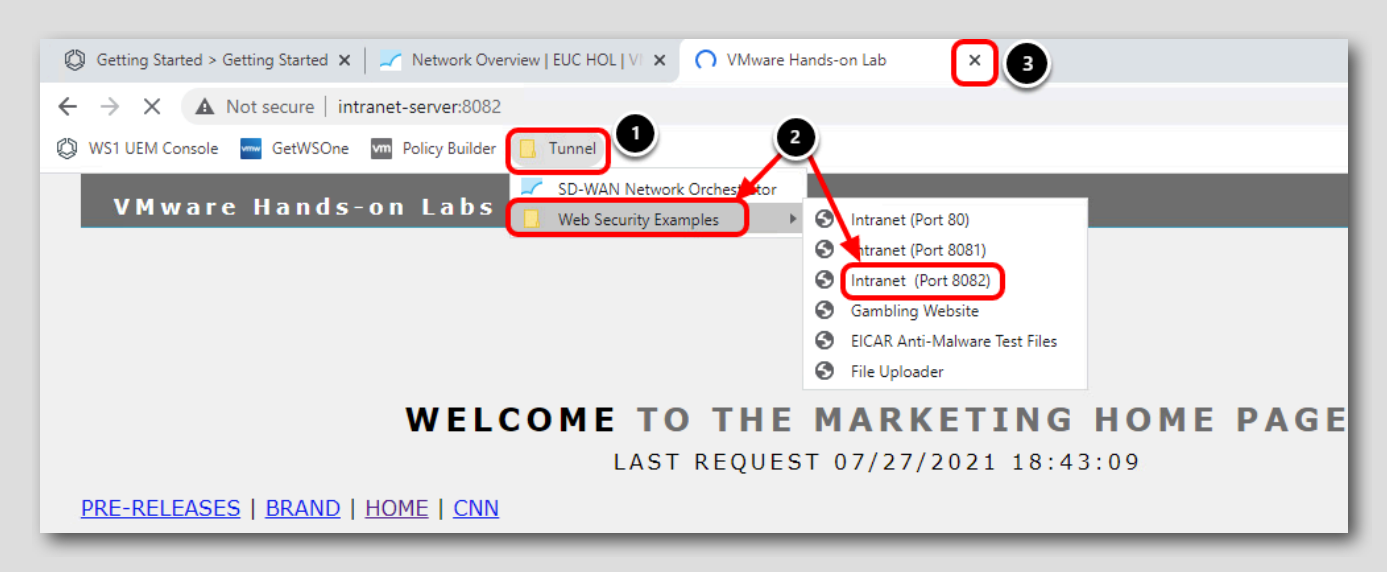


1. [Tunnel] ブックマーク フォルダをクリックします。
2. [Web Security Examples] フォルダにカーソルを合わせ、[Intranet (Port 8081)] ブックマーク リンクをクリックします。

デバイス トラフィック ルールでは、イントラネット サーバが存在する 172.31.64.0/23 ネットワークへのポート 8081 および 8082 も許可されていたことを思い出してください。これにより、Tunnel を介して http://intranet-server:8081 エンドポイントに正常にアクセスできることも確認されています。

ポート 8082 のイントラネット Web サイトへの移動

[777]



1. [Tunnel] ブックマーク フォルダをクリックします。
2. [Web Security Examples] フォルダにカーソルを合わせ、[Intranet (Port 8082)] ブックマーク リンクをクリックします。
3. このタブの [Close] ボタンをクリックします。

デバイス トラフィック ルールでは、イントラネット サーバが存在する 172.31.64.0/23 ネットワークへのポート 8081 および 8082 も許可されていたことを思い出してください。これにより、Tunnel を介して http://intranet-server:8082 エンドポイントに正常にアクセスできることも確認されています。

Cloud Web Security ポリシーの検証

[778]

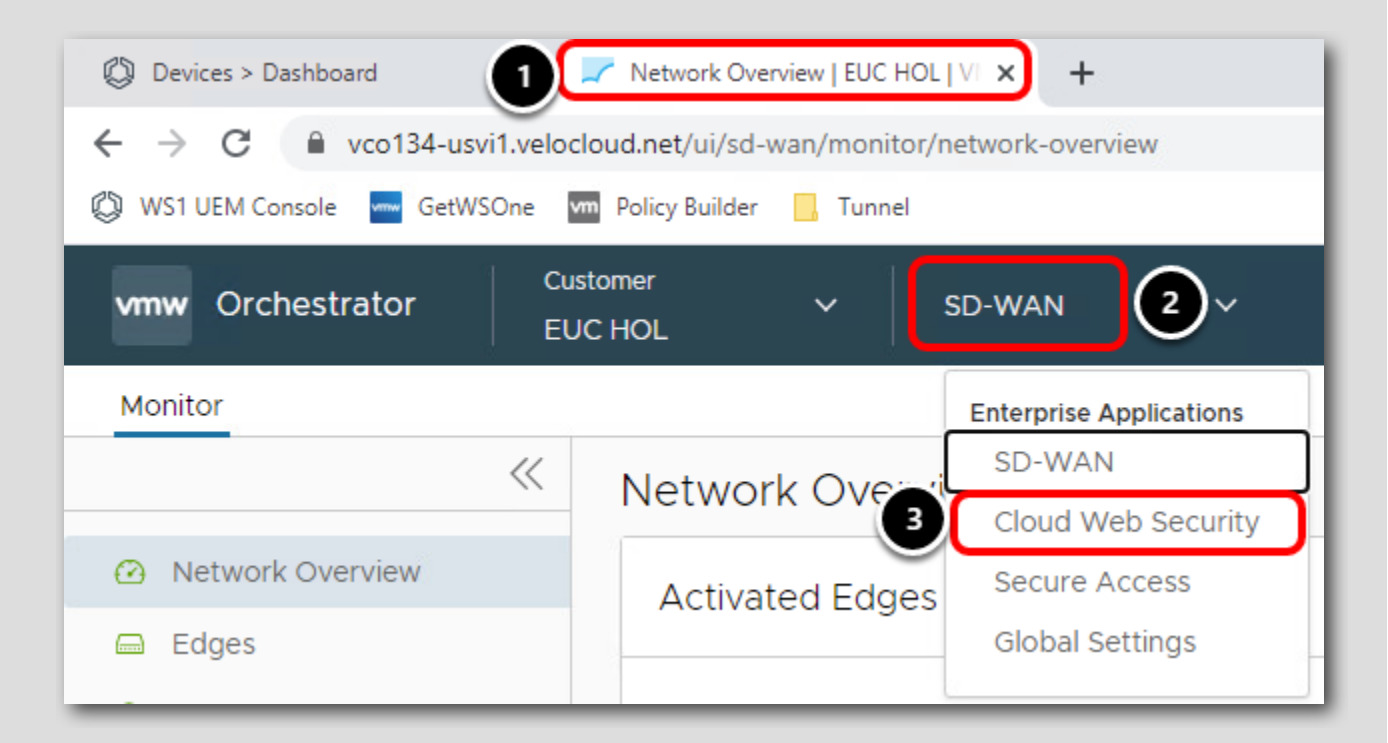
SD-WAN Network Orchestrator の Secure Access 設定を調べたときに、Corporate-Policy という名前の Cloud Web Security (CWS) ポリシーが有効になっていたことを思い出してください。Cloud Web Security ポリシーにより、Secure Access ユーザーのネットワーク トラフィックを検査およびブロックして、ユーザーと企業リソースを悪意のある望ましくないサイトから保護することができます。

Cloud Web Security ポリシー「Corporate-Policy」は、次の目的で構成されています。

- 登録済みデバイスが、ギャンブリング Web サイトの閲覧など、カテゴリに基づいて望ましくない Web サイトを閲覧できないようにする
- パスワードで暗号化されていないファイルをユーザーがダウンロードできないようにする

Cloud Web Security ポリシーの表示

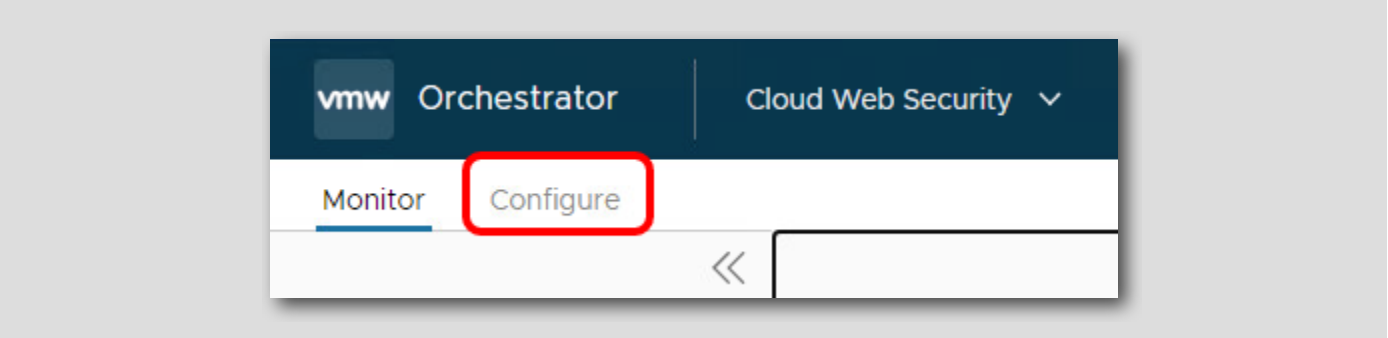
[779]



1. 2 つ目のタブをクリックして、SD-WAN Network Orchestrator に戻ります。
2. [Enterprise Applications] ドロップダウンをクリックします。
3. [Cloud Web Security] をクリックします。

[Configure] タブへの移動

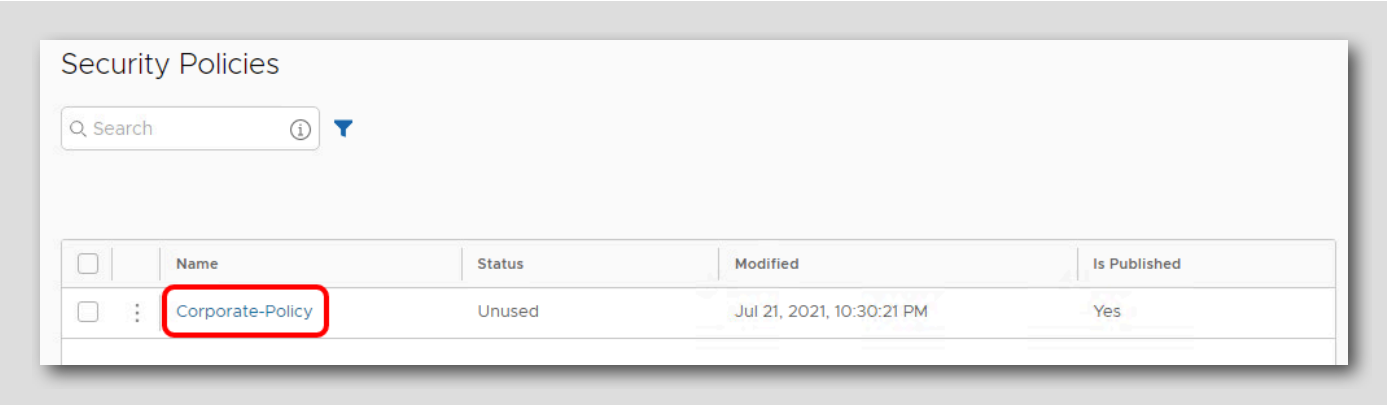
[780]



[Configure] タブをクリックします。

セキュリティ ポリシーの確認

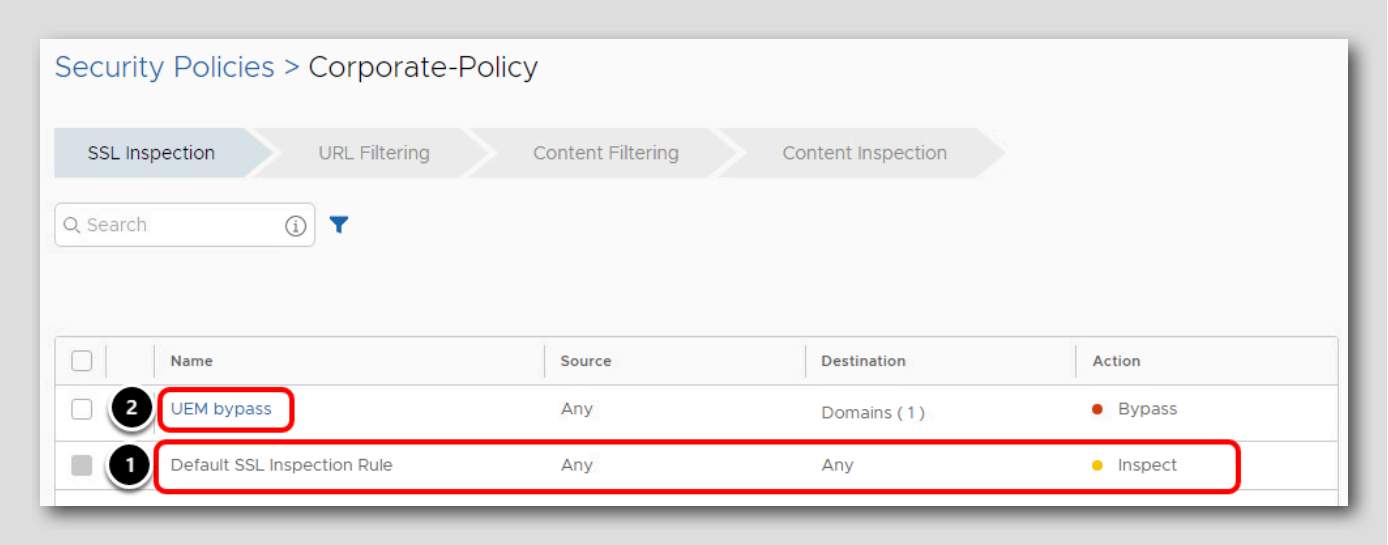
[781]

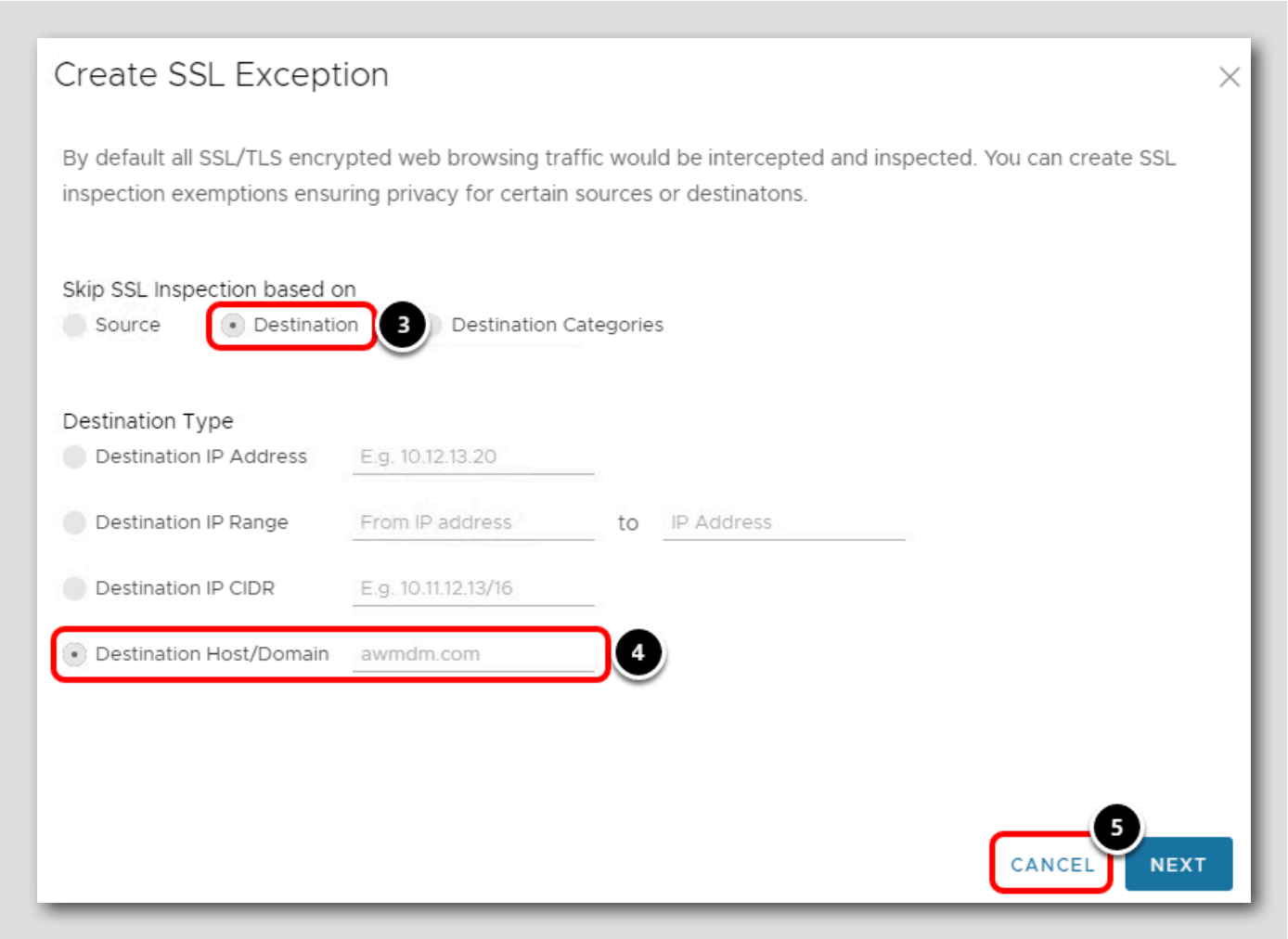


Secure Access 展開のセキュリティ ポリシーのリストについては、ここで参照できます。[Corporate-Policy] リンクをクリックします。

SSL 検査ポリシー

[782]



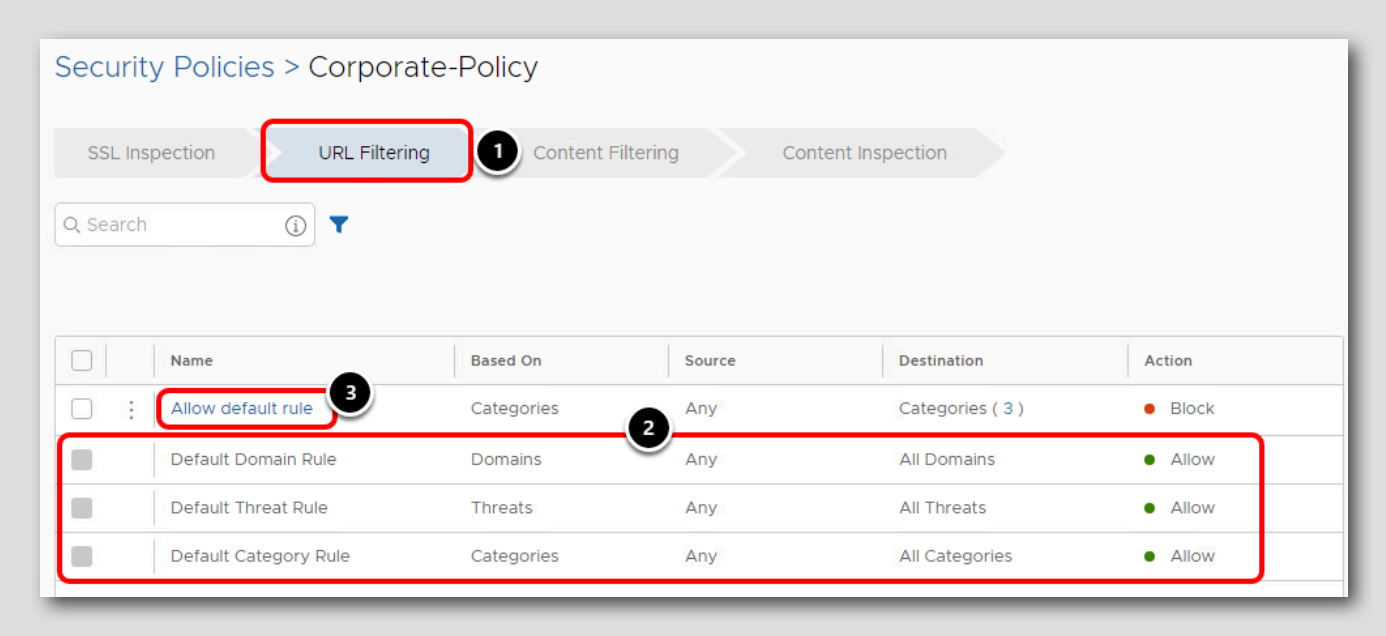


[SSL Inspection] タブは、デフォルトのランディング タブです。すべてのポリシーは、ネットワーク アクセス コントロール リスト (NACL) と同様に、上から下に順番に処理されます。

1. [Default SSL Inspection Rule] は任意の送信元または宛先に適用され、ログおよびメトリックの目的でのみトラフィックを検査します。これは初期およびデフォルトの SSL 検査ルールであり、編集または削除できません。
2. [UEM bypass] という名前のバイパス ルールが追加されました。[UEM bypass] ルールをクリックして、詳細を表示します。
3. [Skip SSL Inspection] が [Destination] に設定されているため、バイパスする IP アドレス、範囲、CIDR ブロック、またはホスト/ドメイン レコードを指定できます。
4. [Destination Host/Domain] フィールドを **`awmdm.com`** に構成しました。つまり、hol.awmdm.com への Workspace ONE UEM トラフィックは検査されません。
5. [Cancel] をクリックして SSL 例外を閉じます。

URL フィルタリング ポリシー

[783]

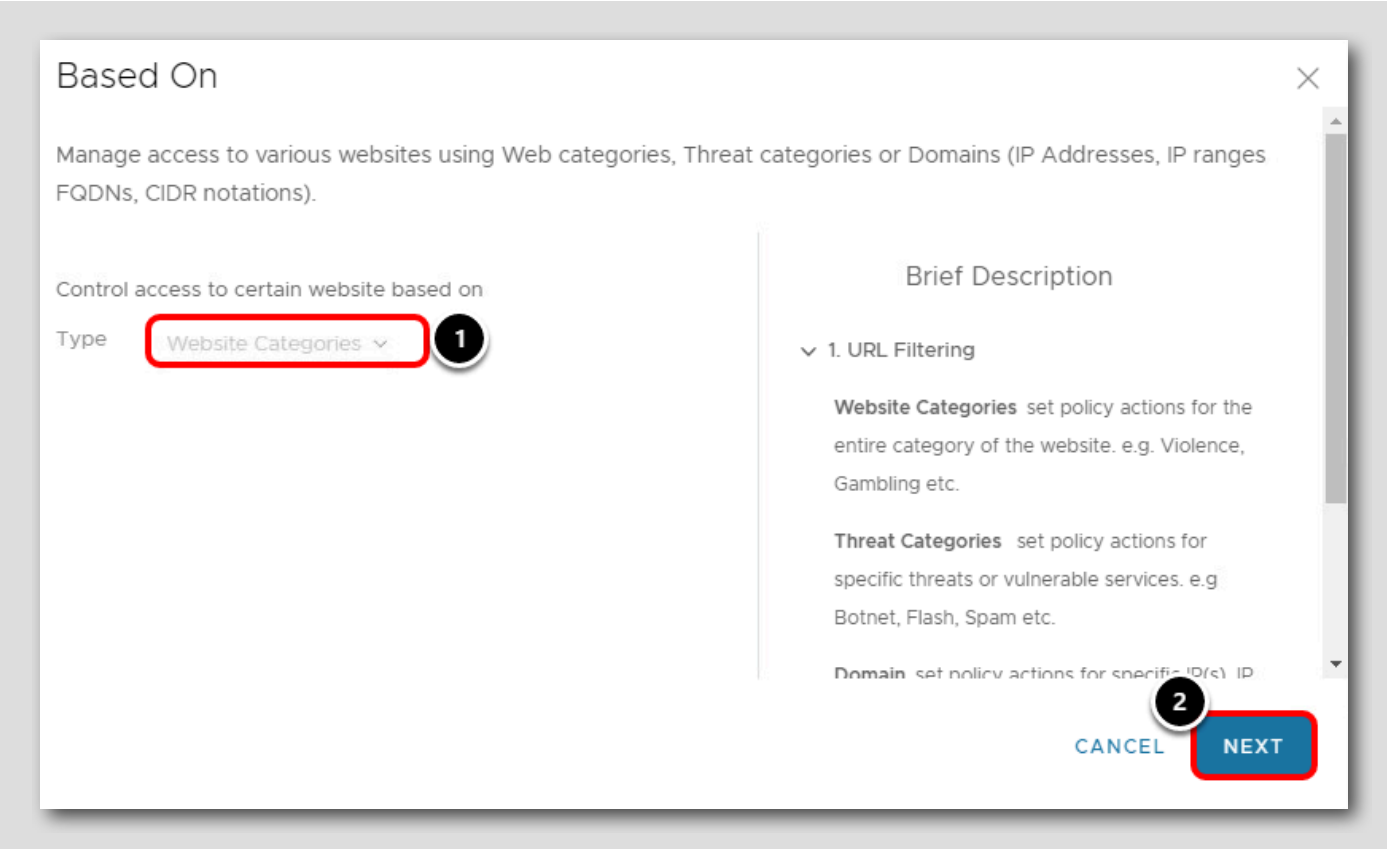


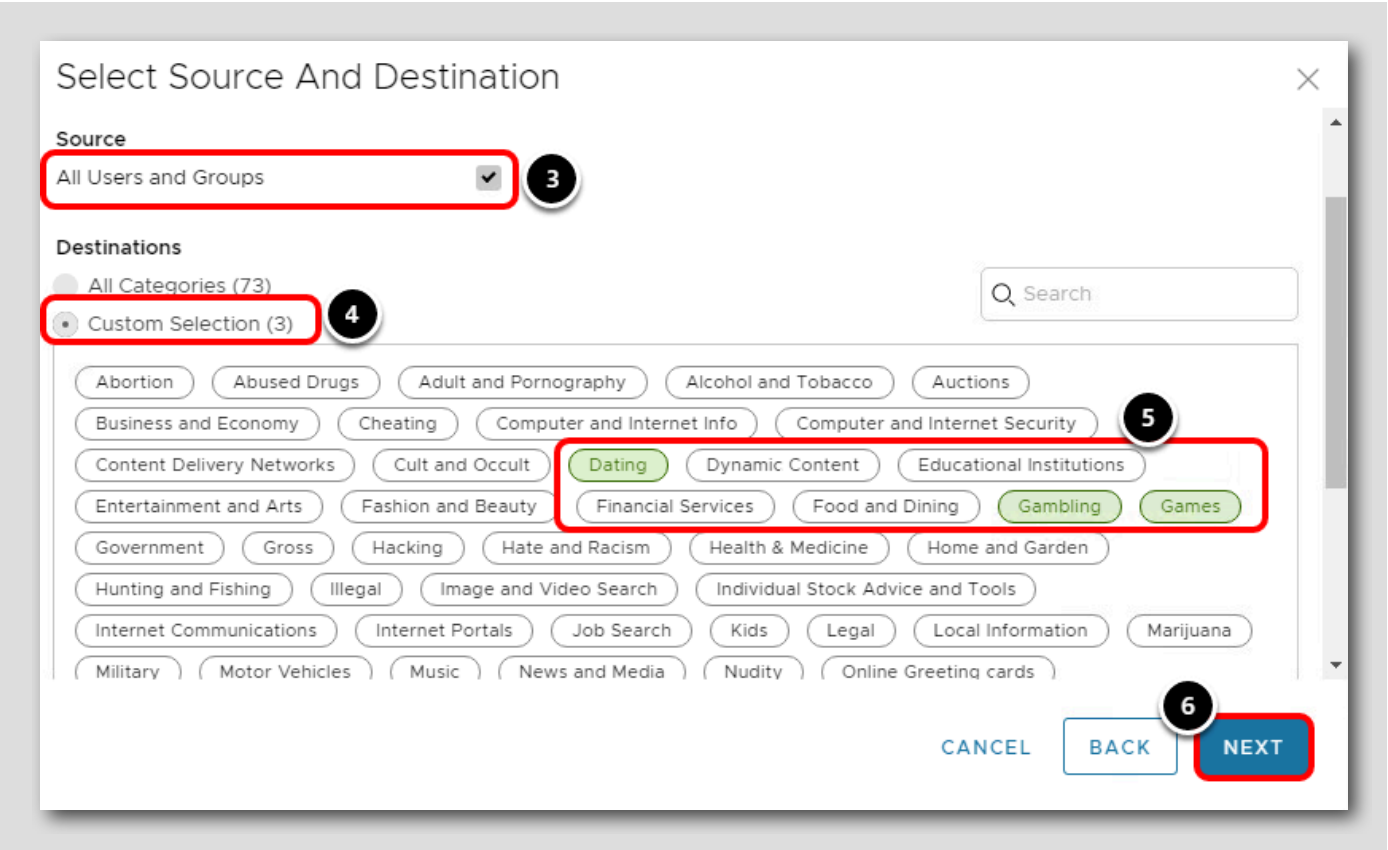
1. [URL Filtering] タブをクリックします。
2. catch-all ルールとして機能し、すべてのドメイン、脅威、およびカテゴリを許可する、削除または編集できない 3 つのデフォルトの URL フィルタリング ルールを確認します。
3. 一部のカテゴリをブロックするために作成された [Allow default rule] をクリックします。

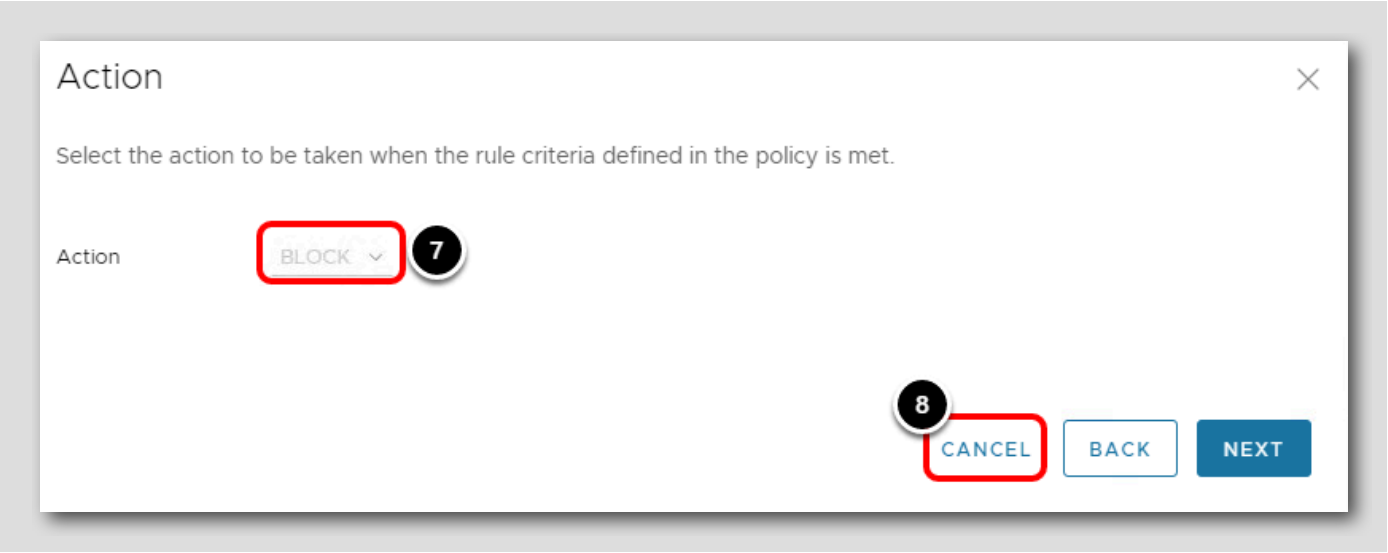
ルールは上から下に順番に処理されるため、3 つのデフォルトの許可ルールは、先行するルールが適用されない場合にのみ処理されます。

URL フィルタリング ポリシー（続き）

[784]



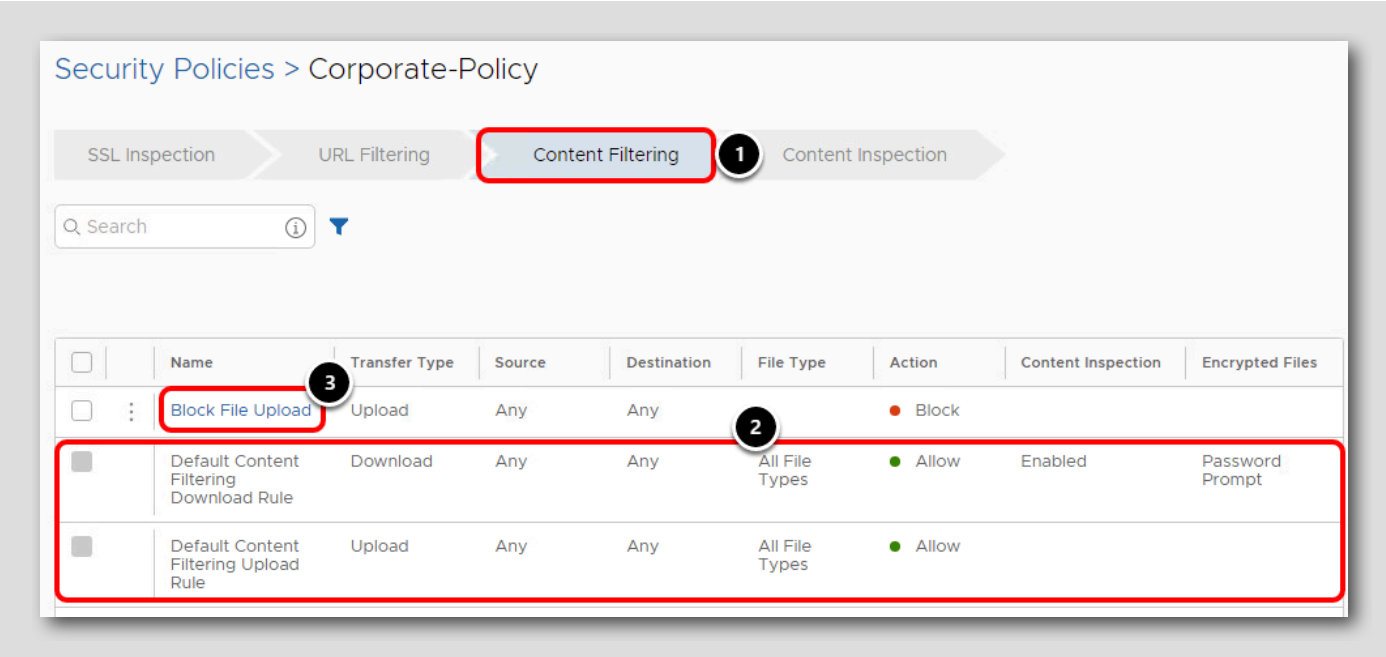

Select Source And Destination
Source
All Users and Groups
3
Destinations
All Categories (73)
Custom Selection (3)
4
Search
Abortion
Abused Drugs
Adult and Pornography
Alcohol and Tobacco
Auctions
Business and Economy
Cheating
Computer and Internet Info
Computer and Internet Security
5
Content Delivery Networks
Cult and Occult
Dating
Dynamic Content
Educational Institutions
Entertainment and Arts
Fashion and Beauty
Financial Services
Food and Dining
Gambling
Games
Government
Gross
Hacking
Hate and Racism
Health & Medicine
Home and Garden
Hunting and Fishing
Illegal
Image and Video Search
Individual Stock Advice and Tools
Internet Communications
Internet Portals
Job Search
Kids
Legal
Local Information
Marijuana
Military
Motor Vehicles
Music
News and Media
Nudity
Online Greeting cards
6
CANCEL
BACK
NEXT


Action
Select the action to be taken when the rule criteria defined in the policy is met.
Action
BLOCK
7
8
CANCEL
BACK
NEXT

1. [Based On] 設定が最初に表示されます。これにより、Web サイトのカテゴリ、脅威のカテゴリ、またはドメインをターゲットにできます。デバイスの特定のカテゴリをブロックしたいので、[Website Categories] を選択しました。
2. [Next] をクリックして、[Source] と [Destination] の設定に進みます。
3. [All Users and Groups] ソースが選択され、すべてのユーザーにこのルールが適用されました。
4. ターゲットにするカテゴリを選択するために、[Destinations] に [Custom Selection] オプションが選択されました。
5. [Dating, Gambling, and Games] カテゴリが選択されました。
6. [Next] をクリックして、[Action] 設定に進みます。
7. [Action] 設定では、このルールを選択したカテゴリを [Allow] または [Block] に設定できます。[Block] を選択して、ユーザーがターゲット カテゴリを閲覧できないようにしました。
8. [Cancel] をクリックして、URL フィルタリング ルールを閉じます。

コンテンツ フィルタリング ポリシー

[785]

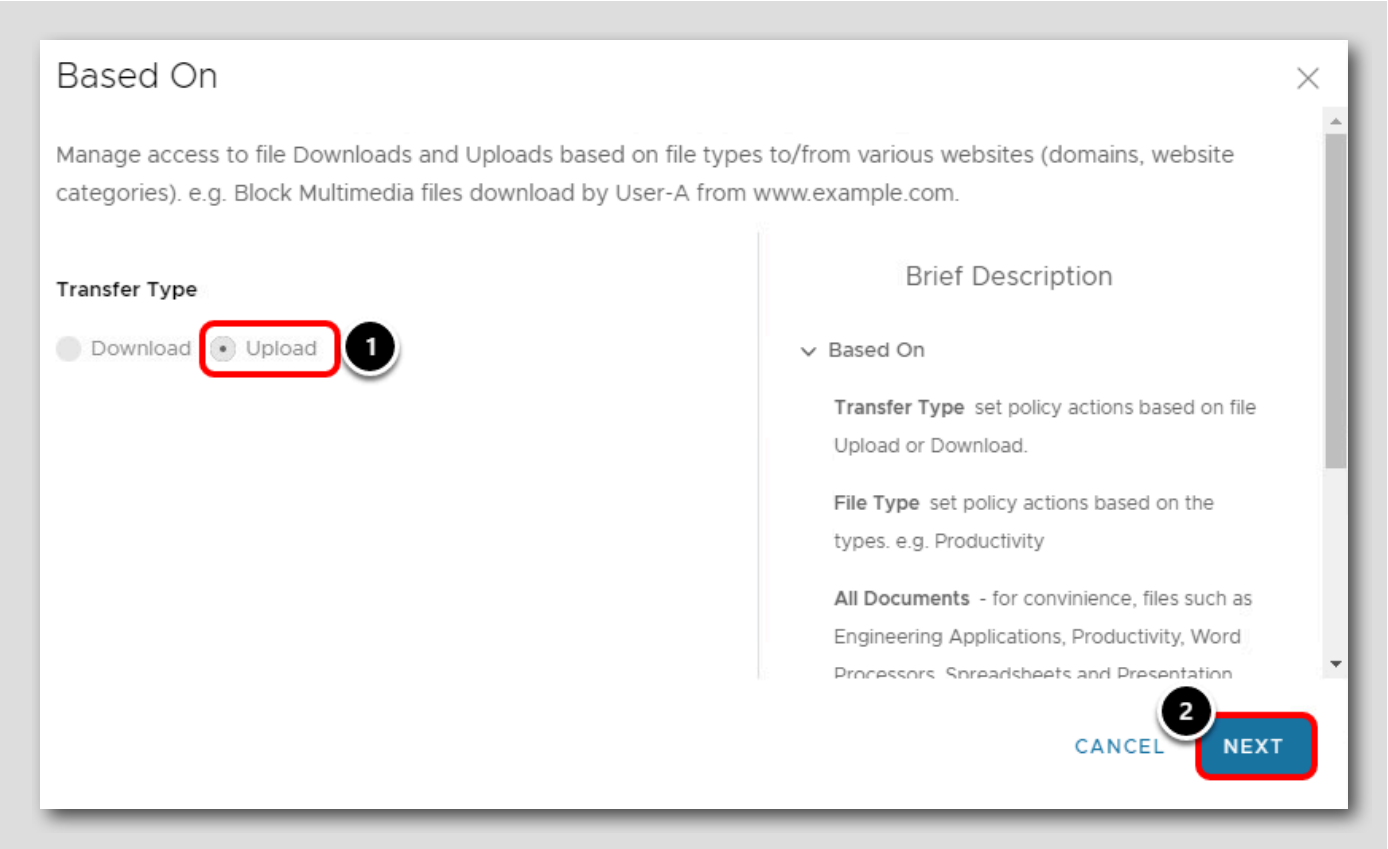


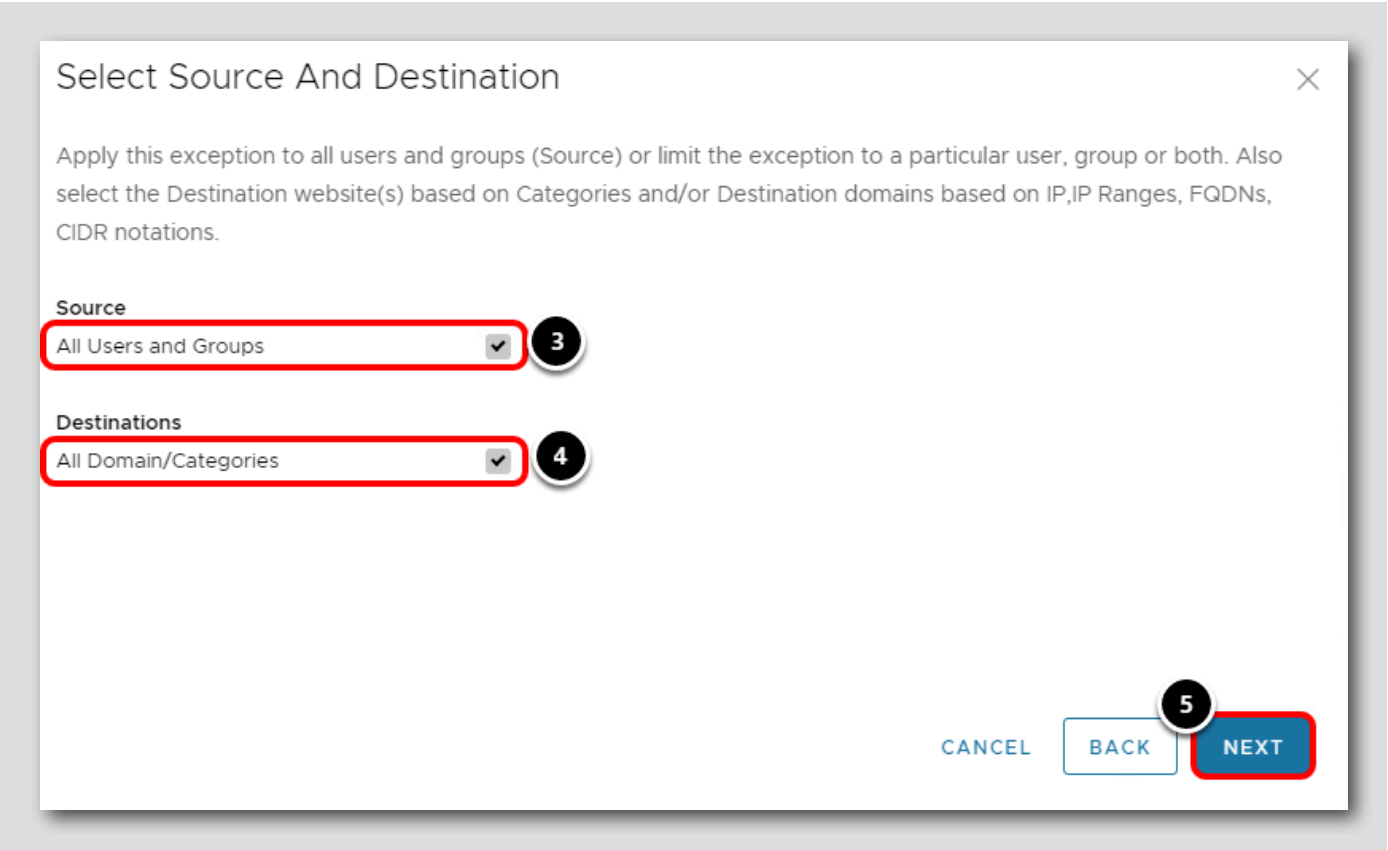
1. [Content Filtering] タブをクリックします。
2. ファイルのダウンロード（ファイルがパスワード プロンプトを使用して暗号化されている場合）およびファイルのアップロードを許可する 2 つのデフォルトのコンテンツ フィルタリング ルールを確認します。
3. 作成した [Block File Upload] ルールをクリックします。

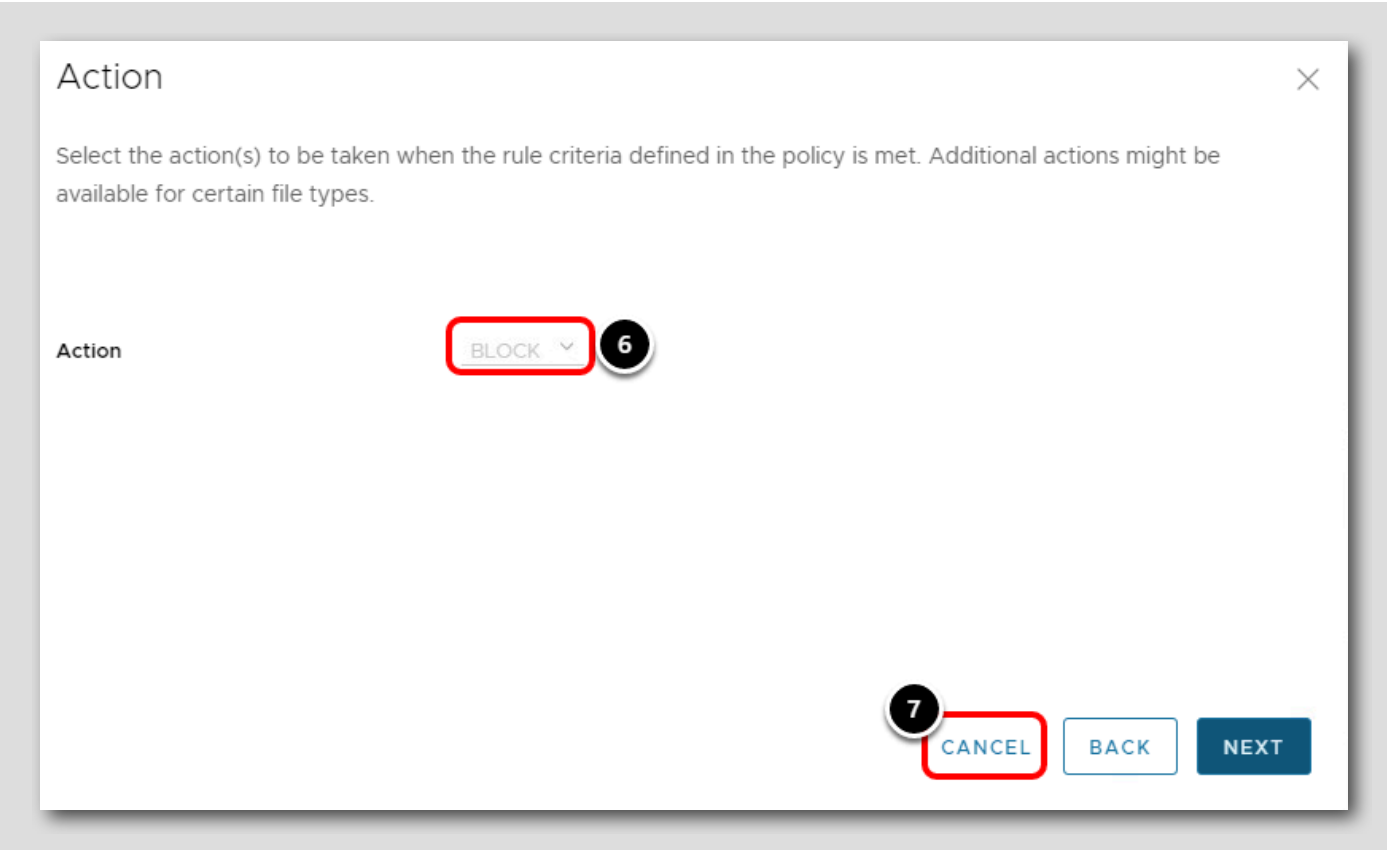
ルールは上から下に順番に処理されるため、2 つのデフォルトの許可ルールは、先行するルールが適用されない場合にのみ処理されます。

[786]

コンテンツ フィルタリング ポリシー（続き）




Select Source And Destination
Apply this exception to all users and groups (Source) or limit the exception to a particular user, group or both. Also select the Destination website(s) based on Categories and/or Destination domains based on IP,IP Ranges, FQDNs, CIDR notations.
Source
All Users and Groups
3
Destinations
All Domain/Categories
4
5
CANCEL
BACK
NEXT

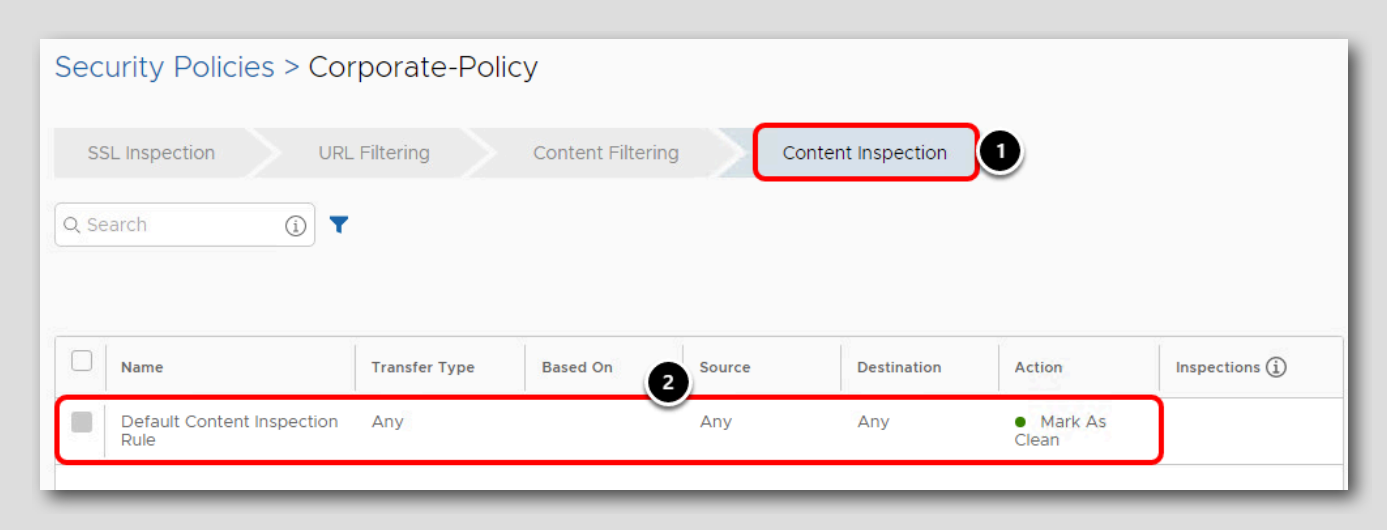


注：以下は情報提供のみを目的としています。これは実稼働環境であり、変更を加えることはできません。「Cancel」ボタンをクリックして続行します。

1. [Transfer Type] では、[Uploads] または [Downloads] のどちらをターゲットにするかを決定します。このルールでは、[Upload] を選択しました。
2. [Next] をクリックして、[Source] と [Destination] の設定に進みます。
3. すべてのユーザーにルールを適用するために、[Source] が [All Users and Groups] に設定されました。
4. すべての宛先に適用するために、[Destinations] が [All Domains/Categories] に設定されました。
5. [Next] をクリックして、[Action] 設定に進みます。
6. [Action] 設定では、このルールを選択したコンテンツを [Allow] または [Block] に設定できます。[Block] を選択して、ユーザーがファイルをアップロードできないようにしました。
7. [Cancel] をクリックして、このコンテンツ フィルタリング ルールを閉じます。

コンテンツ検査ポリシー

[787]

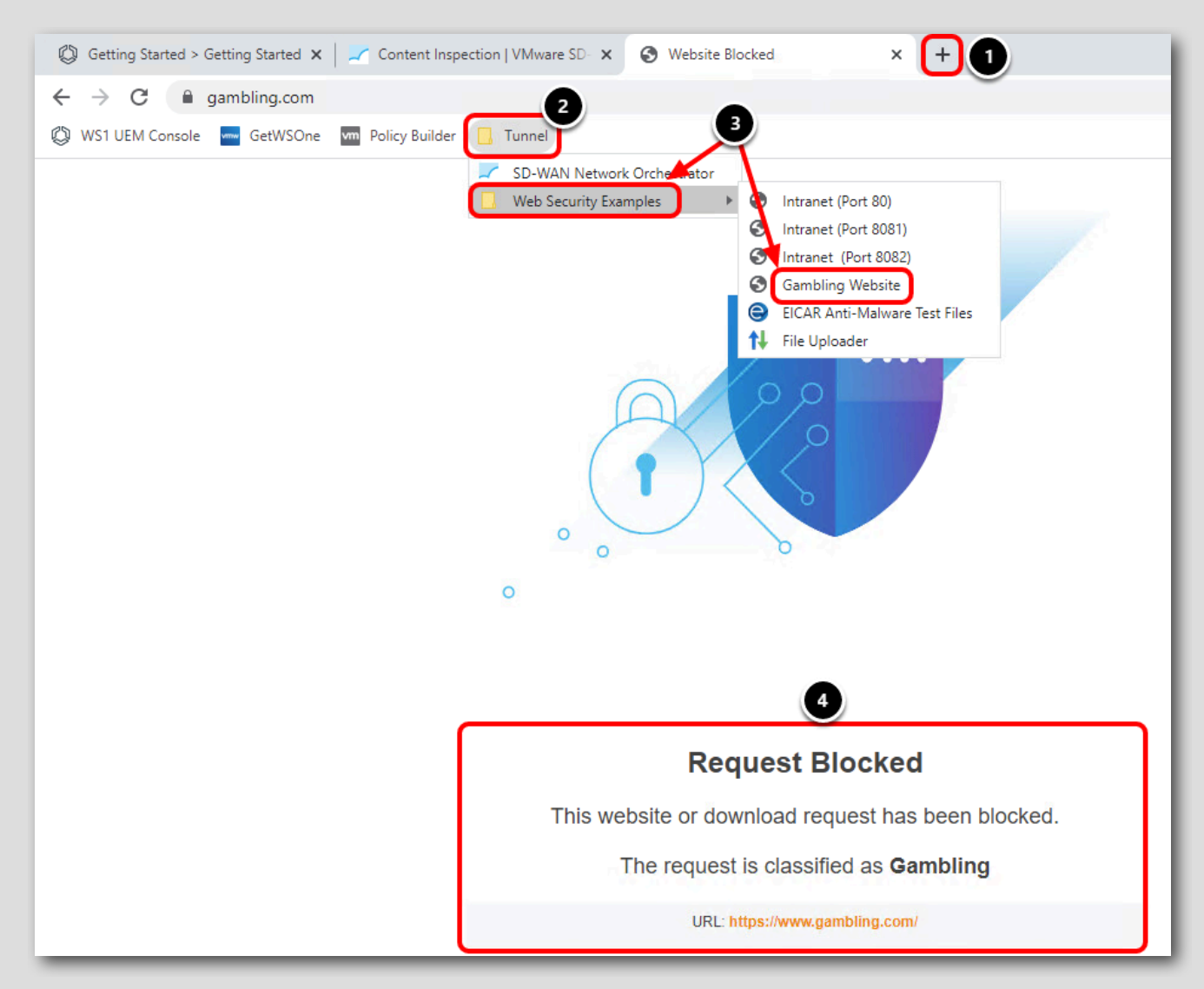


1. [Content Inspection] タブをクリックします。
2. 送信元または宛先の検査をクリーンとしてマークするデフォルトのコンテンツ検査ルールは、何も実行されないことを意味します。

この展開に対して追加のコンテンツ検査ルールが作成されませんでした。

カテゴリ フィルタリング ルールの検証

[788]

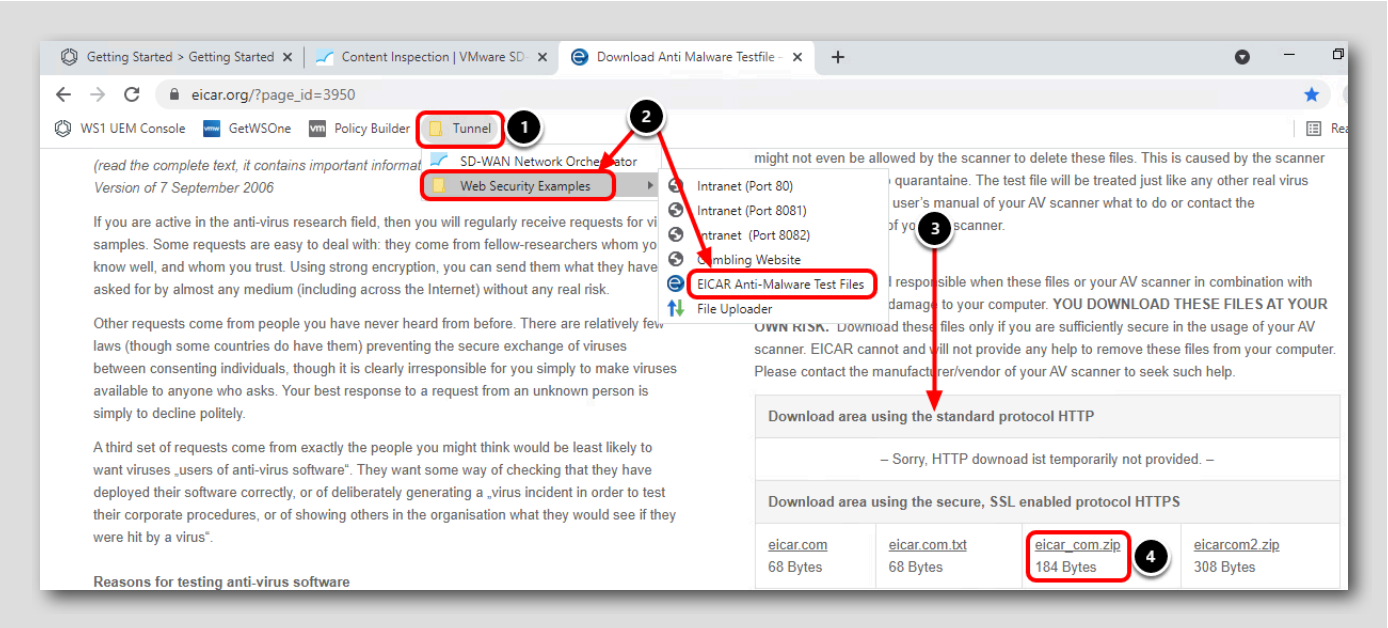


1. [New Tab] ボタンをクリックします。
2. [Tunnel] ブックマーク フォルダをクリックします。
3. [Web Security Examples] フォルダにカーソルを合わせ、[Gambling Website] ブックマーク リンクをクリックします。
4. Web サイトがギャンブル サイトとして分類されたため、要求がブロックされたことを確認します。

URL フィルタリング ポリシーには、いくつかのカテゴリの Web サイトへのアクセスをブロックするルールがあり、そのうちの 1 つにギャンブリング Web サイトが含まれていました。これにより、Tunnel サービスを通過するトラフィックが検査され、カテゴリがポリシーでブロックする必要があると指定されている「ギャンブリング Web サイト」であると判断されたことが確認されます。

コンテンツ フィルタリング ルールの検証

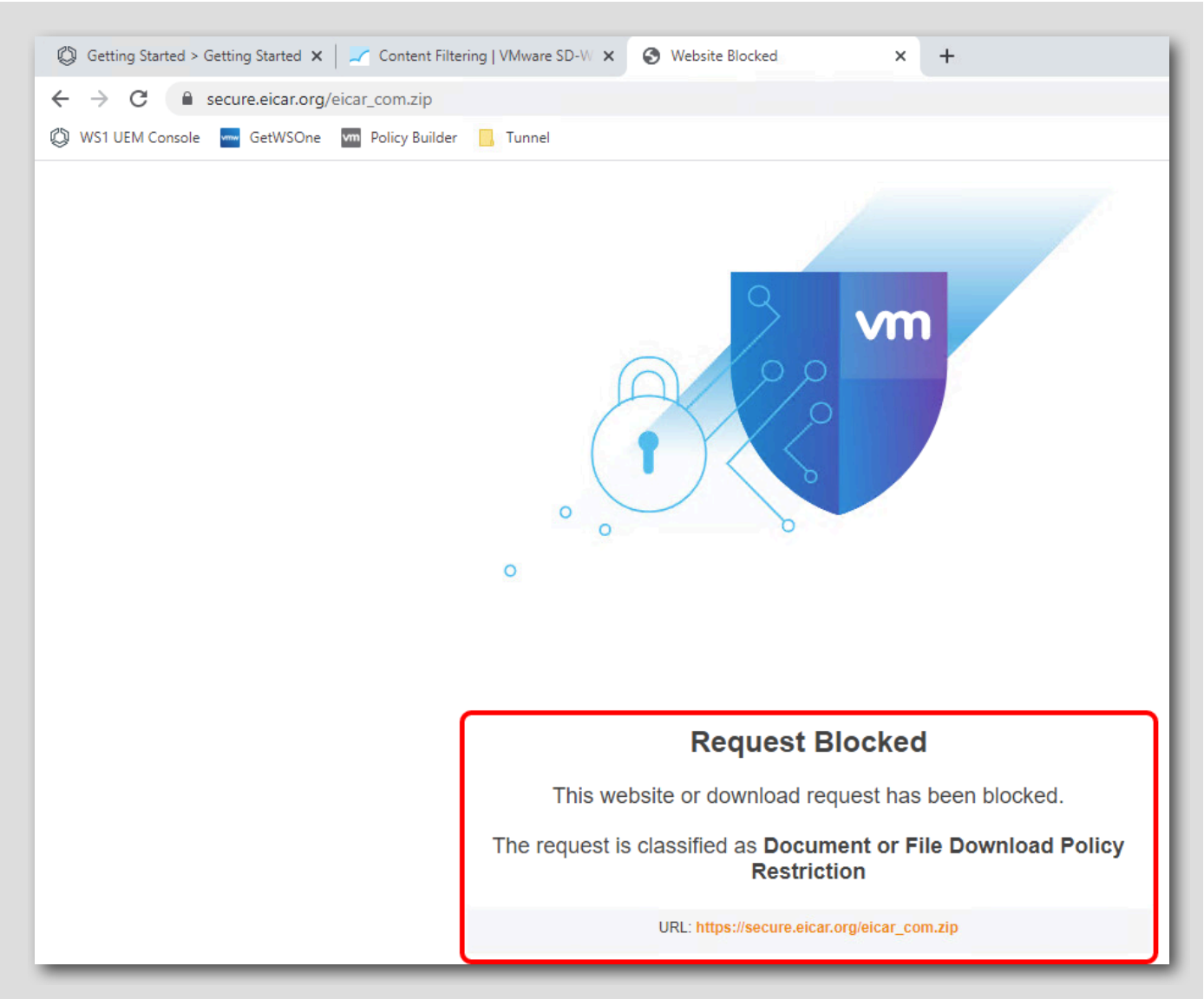
[789]



1. [Tunnel] ブックマーク フォルダをクリックします。
2. [Web Security Examples] フォルダにカーソルを合わせ、[EICAR Anti-Maleware Test File] ブックマーク リンクをクリックします。
3. 下にスクロールして、ダウンロード領域を見つけます。
4. eicar_com.zip ファイルをクリックします。

ファイル ダウンロード ポリシーによる要求の制限

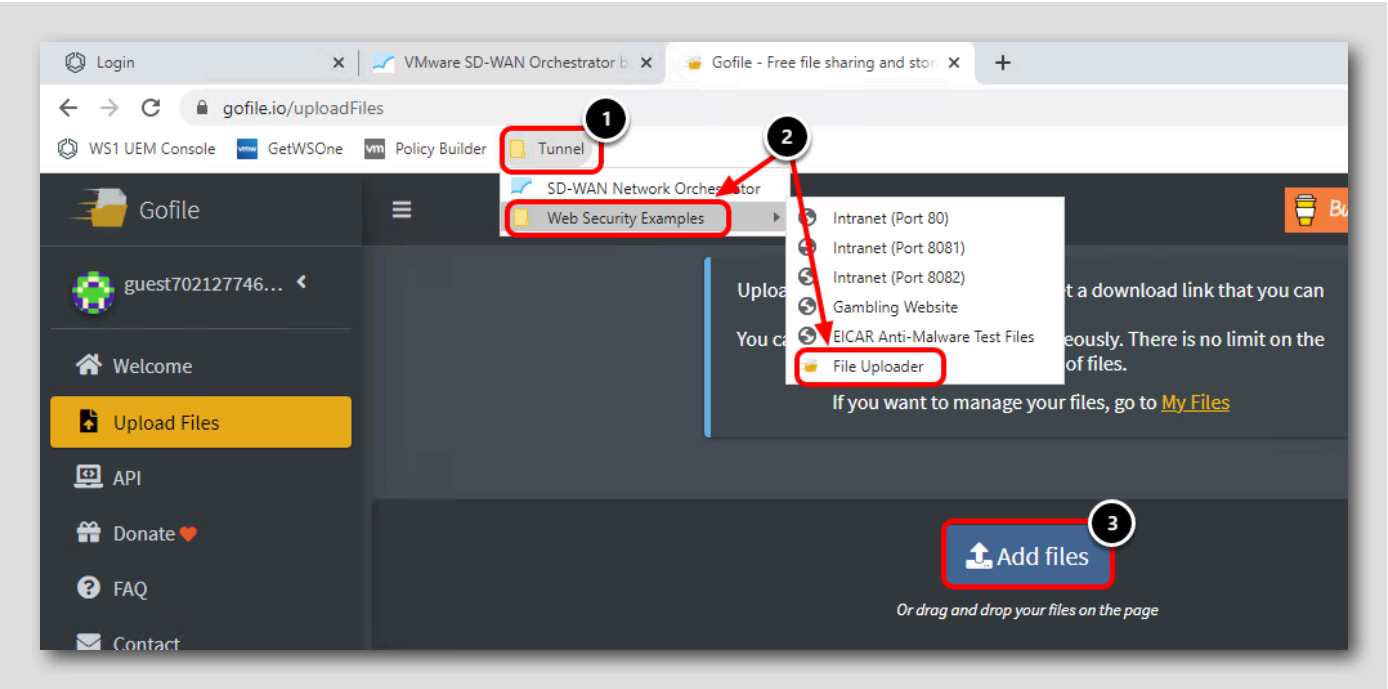
[790]



.zip ファイルをダウンロードしようとすると、構成されているドキュメントまたはファイル ダウンロード ポリシーの制限に違反しているため、要求がブロックされます。デフォルトのコンテンツ フィルタリング ルールでファイルのダウンロードが許可されるのは、暗号化されていてパスワードの入力が必要な場合のみですが、このファイルは暗号化されていません。他の構成済みルールでは、暗号化されていないファイルのダウンロードを明示的に許可していないため、ファイルはブロックされます。

ファイルのアップロード ブロック ルールの検証

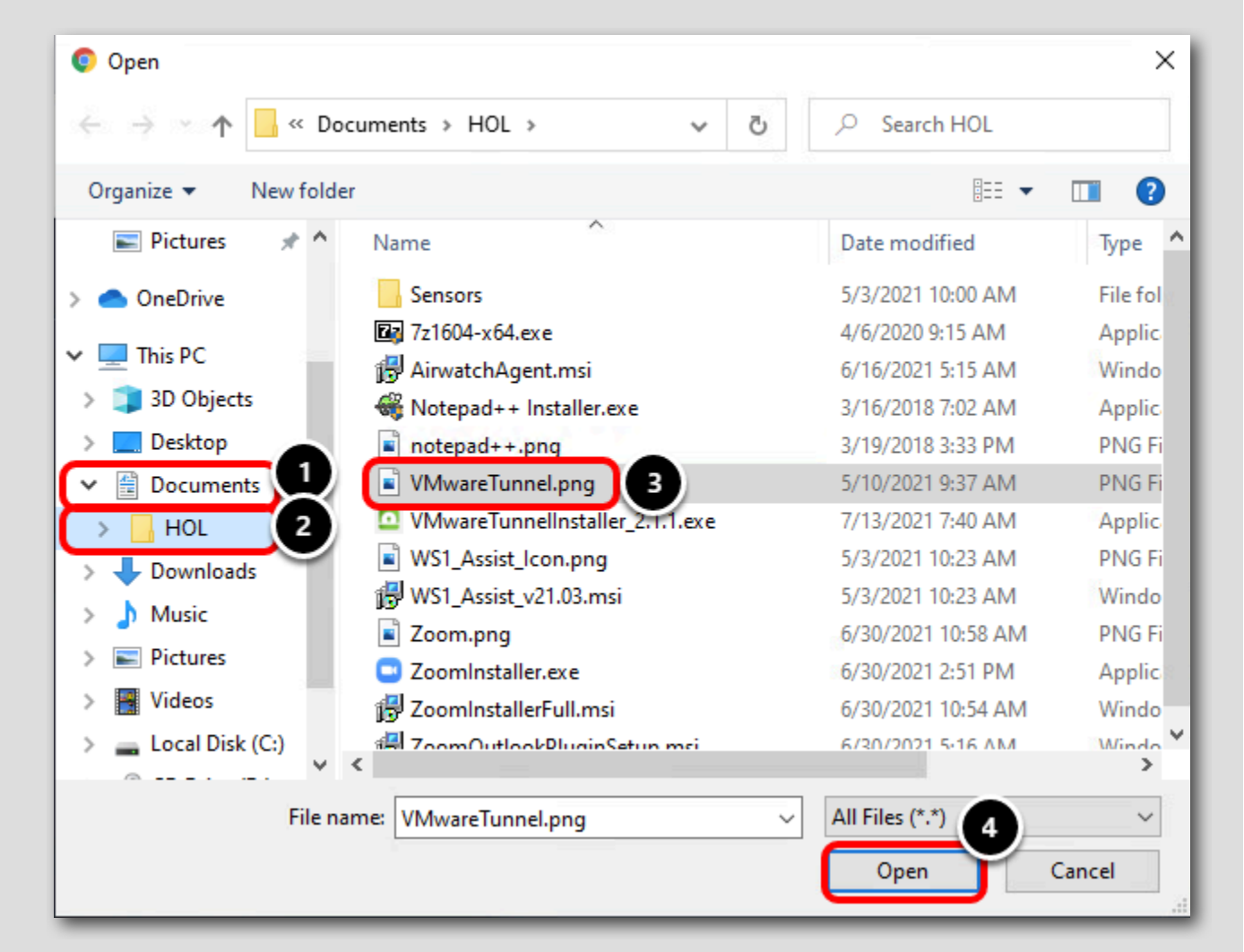
[791]



1. [Tunnel] ブックマーク フォルダをクリックします。
2. [Web Security Examples] フォルダにカーソルを合わせ、[File Uploader] ブックマーク リンクをクリックします。
3. [Add Files] をクリックします。

アップロードするファイルの選択

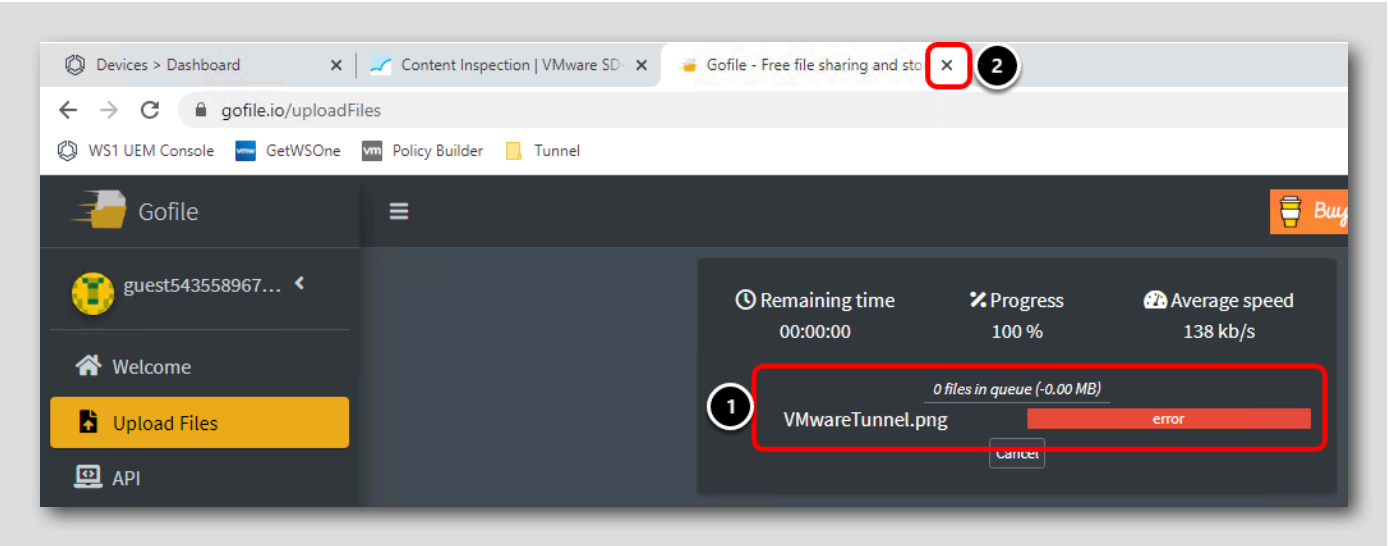
[792]



1. [Documents] をクリックします。
2. [HOL] をクリックします。
3. [VMwareTunnel.png] をクリックします。
4. [Open] をクリックします。

ファイルがアップロードできないことを確認

[793]



1. ファイルのアップロード プロセスが開始された後、[VMwareTunnel.png] アップロードの進行状況バーが [error] に変わります。
2. このブラウザ タブで [Close] をクリックします。

Cloud Web Security ポリシーに、すべてのユーザーのすべてのファイル アップロードをブロックするコンテンツ フィルタリング ルールがあることを思い出してください。これにより、Cloud Web Security ポリシーによってプロセスがブロックされたため、ユーザーがファイルをアップロードできなかったことが確認されます。

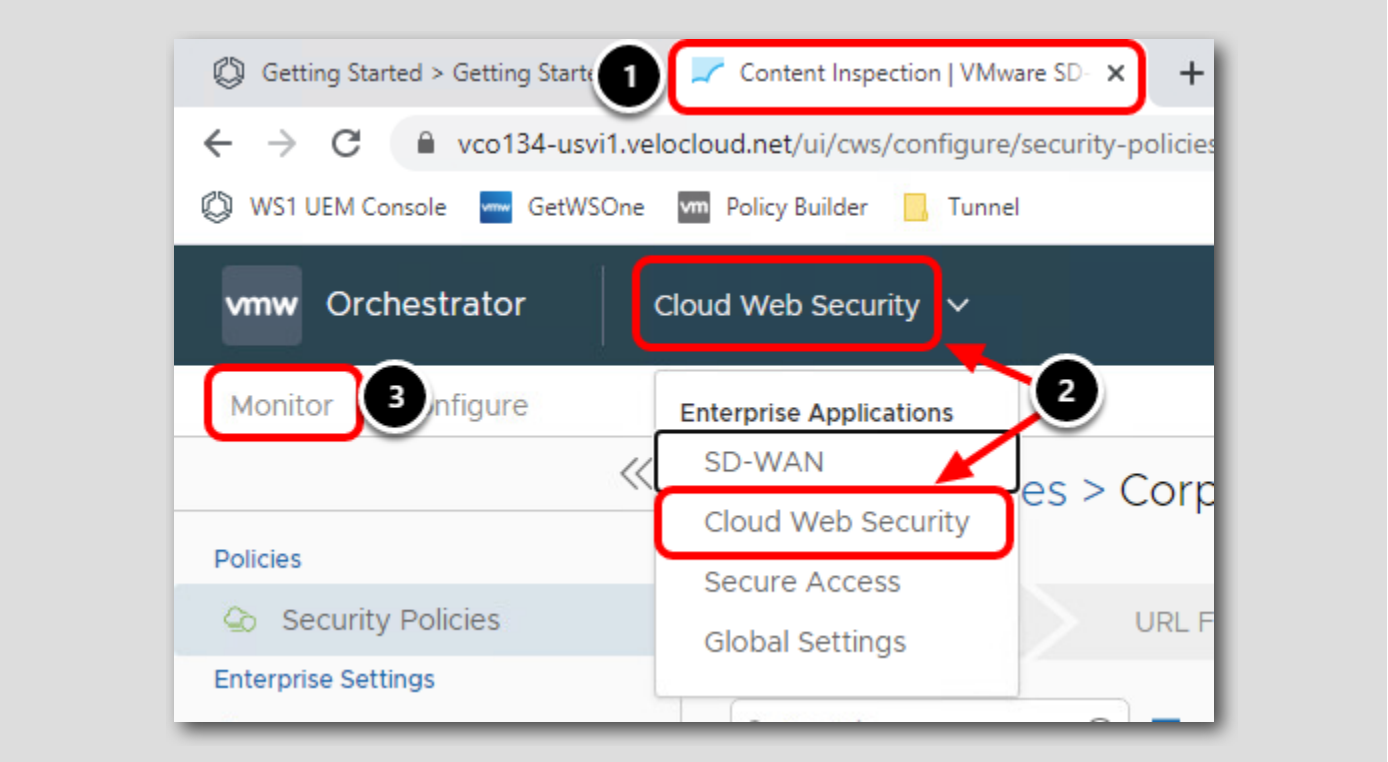
Cloud Web Security 分析

[794]

エンド ユーザーのアクションを防止するために Cloud Web Security ポリシーがどのように構成されたかを確認しました。次に、SD-WAN Network Orchestrator ユーザー インターフェイスの [Cloud Web Security] セクションの [Monitoring] セクションで、システムの管理者が利用できる詳細を確認します。

Cloud Web Security の [Monitor] ページへの移動

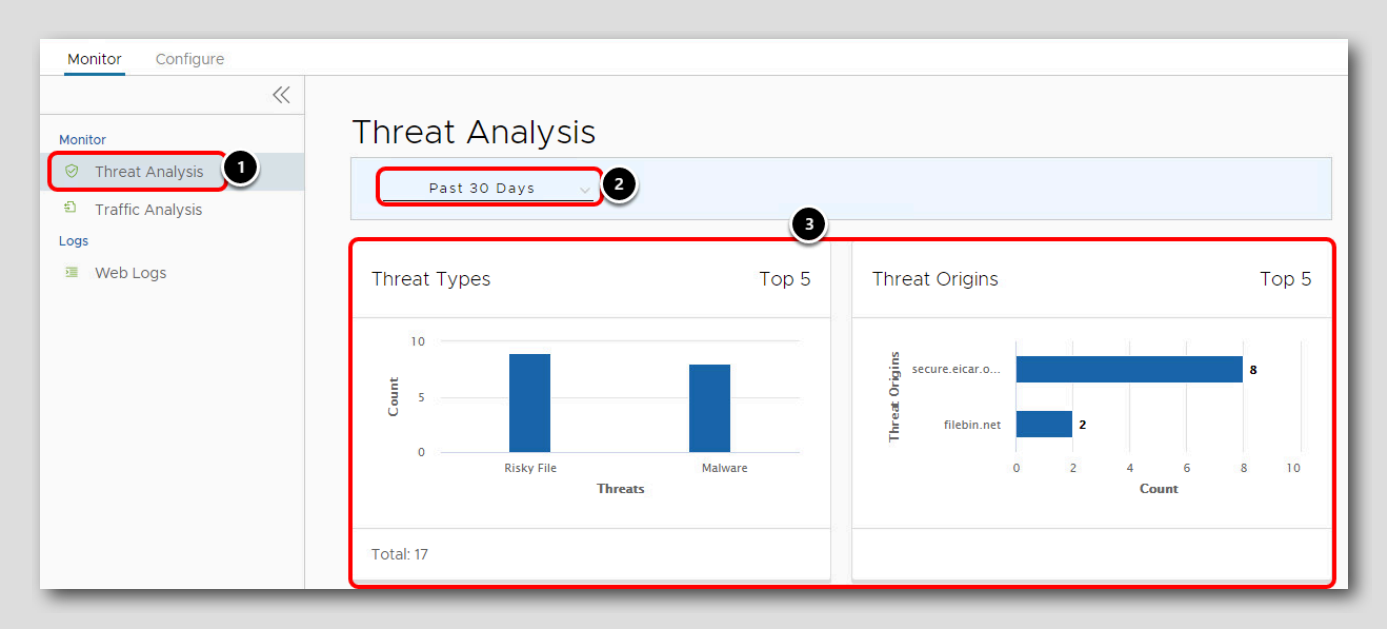
[795]



1. SD-WAN Network Orchestrator タブから移動した場合は、2 つ目のタブをクリックして戻ります。
2. Cloud Web Security ページから移動した場合は、[Enterprise Applications] ドロップダウンをクリックして、[Cloud Web Security] を選択します。
3. [Cloud Web Security] ページで [Monitor] タブをクリックします。

脅威分析の表示

[796]

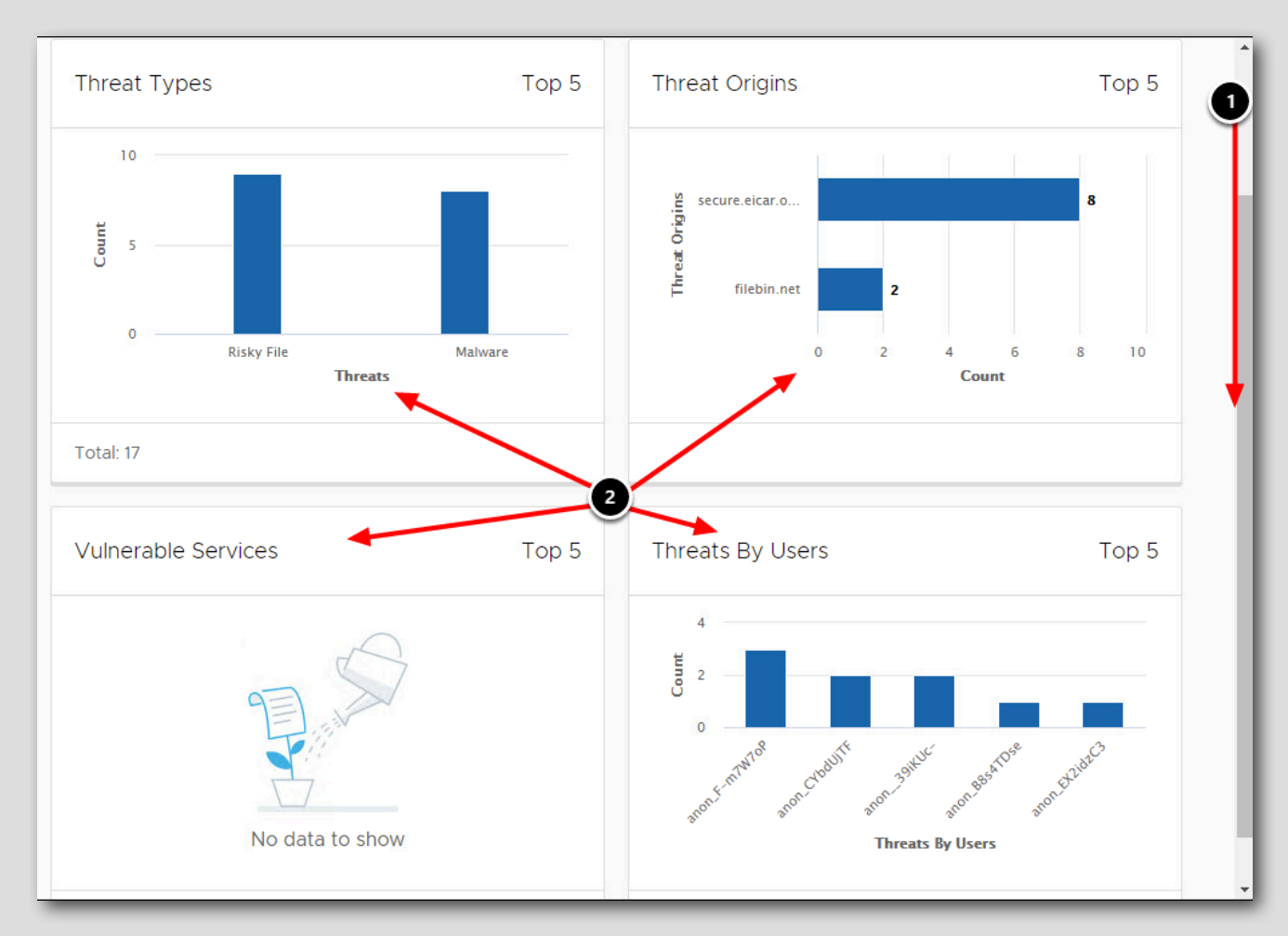


注：ダッシュボードは、ハンズオン ラボから収集した実際のメトリックを表示しているため、上記の表示とは異なります。

1. [Threat Analysis] をクリックします。
2. 時間フィルタをクリックし、[Past 30 Days] に変更します。
3. ダッシュボードが更新され、過去 30 日間のデータが表示されます。

[Threat Analysis] ダッシュボード

[797]

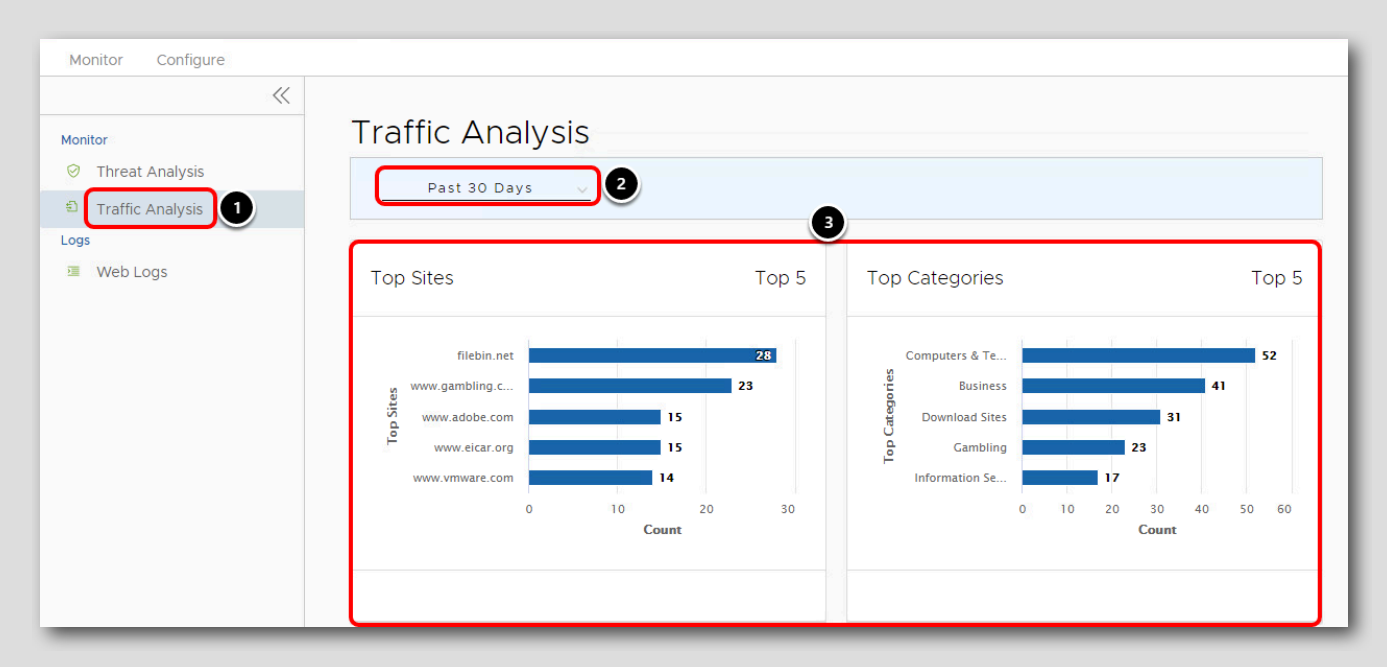


注：ダッシュボードは、ハンズオン ラボから収集した実際のメトリックを表示しているため、上記の表示とは異なります。

1. 下にスクロールして、[Threat Analysis] ダッシュボードを見つけます。
2. 上位 5 つの脅威タイプ、脅威の発生元、脆弱なサービス、ユーザー別の脅威には、Secure Access 展開の実際のメトリックが表示されます。ここで詳細を確認して、Secure Access 展開への変更に関する情報に基づいた決定を行うことができます。

トラフィック分析の表示

[798]

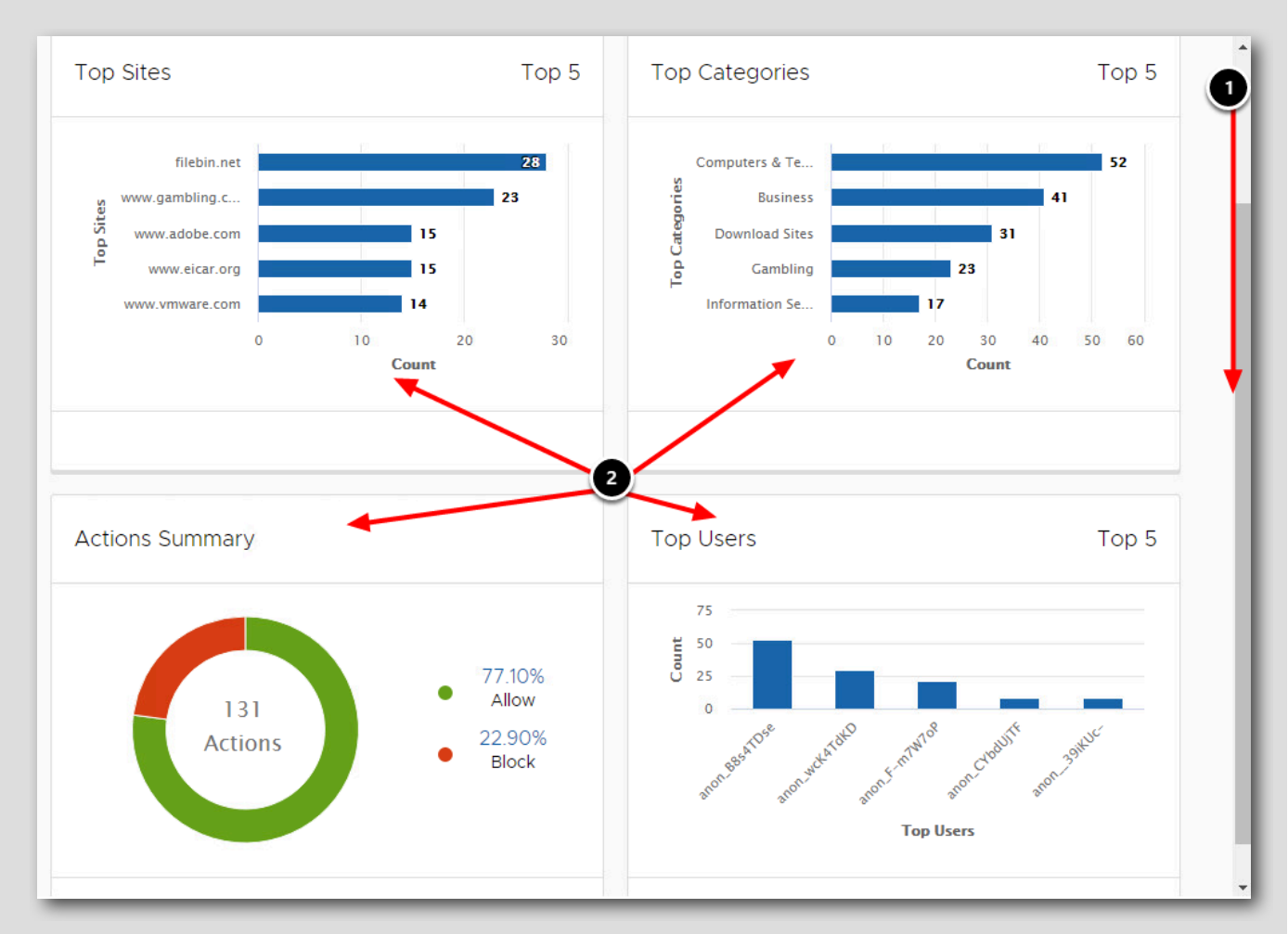


注：ダッシュボードは、ハンズオン ラボから収集した実際のメトリックを表示しているため、上記の表示とは異なります。

1. [Traffic Analysis] をクリックします。
2. 時間フィルタをクリックし、[Past 30 Days] に変更します。
3. ダッシュボードが更新され、過去 30 日間のデータが表示されます。

[Traffic Analysis] ダッシュボード

[799]

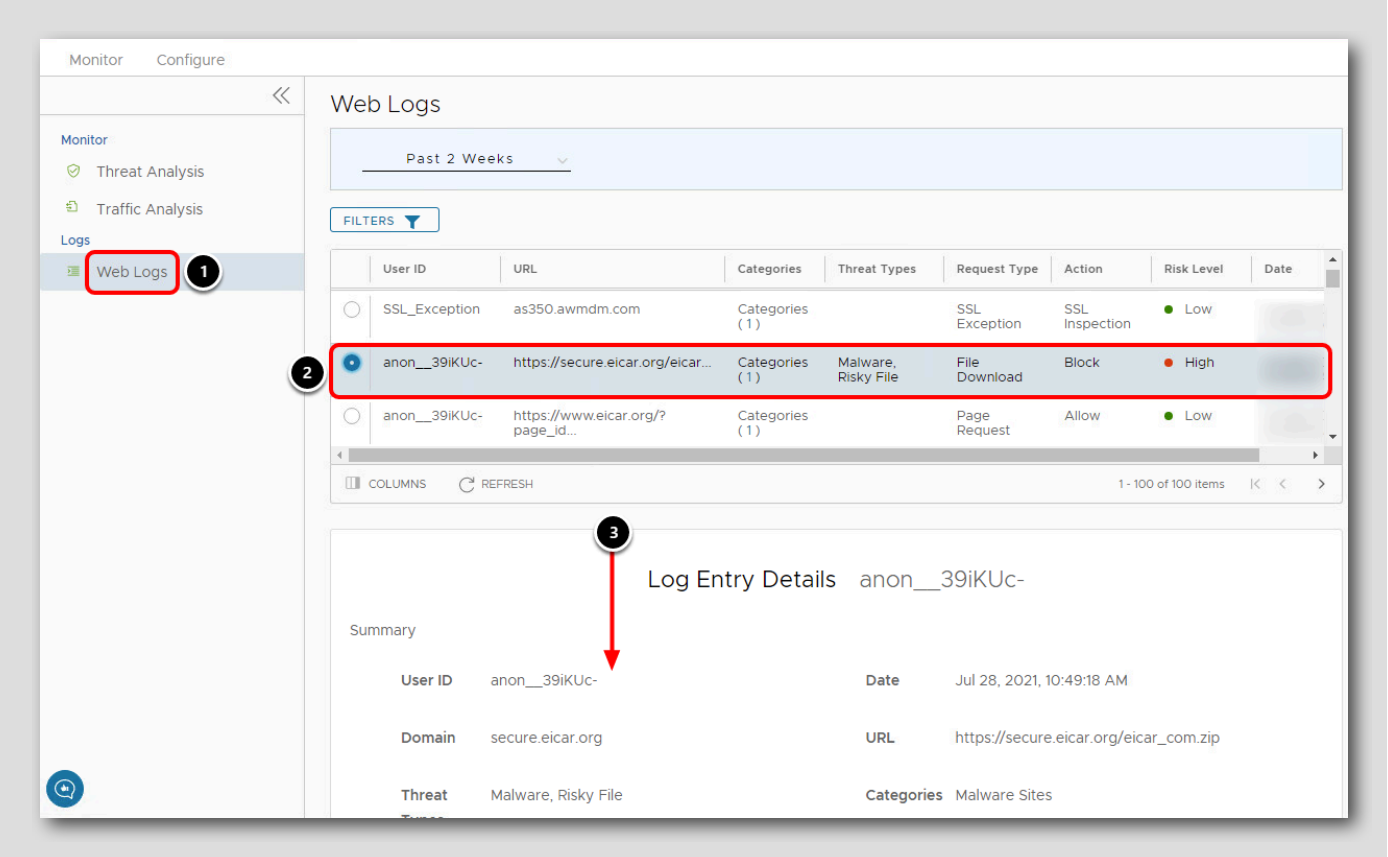


注: ダッシュボードは、ハンズオン ラボから収集した実際のメトリックを表示しているため、上記の表示とは異なります。

1. 下にスクロールして、[Traffic Analysis] ダッシュボードを見つけます。
2. 上位 5 つのサイト、カテゴリ、アクション、およびユーザーのダッシュボードには、Secure Access 展開の実際のメトリックが表示されます。ここで詳細を確認して、Secure Access 展開への変更に関する情報に基づいた決定を行うことができます。

Web ログの表示

[800]

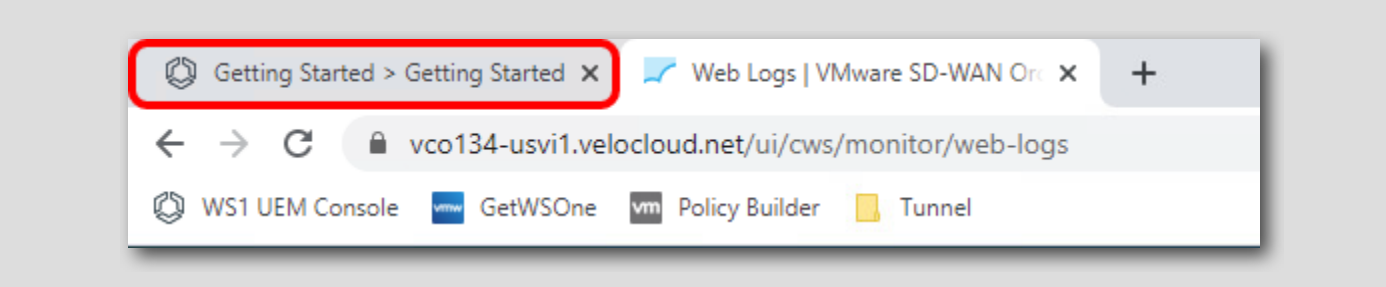


トラフィックのログ、トラフィックの分類方法、ポリシーによる処理方法は、[Web Logs] セクションで確認できます。

1. [Web Logs] をクリックします。
2. Web ログのいずれかの結果をクリックして、トラフィックの詳細を表示します。
3. 下にスクロールして、[Log Entry Details] セクションに詳細を表示します。

Workspace ONE UEM 管理者コンソールに戻る

[801]



最初のタブをクリックして Workspace ONE UEM 管理者コンソールに戻り、次の手順を完了します。

Windows 10 デバイスの登録解除

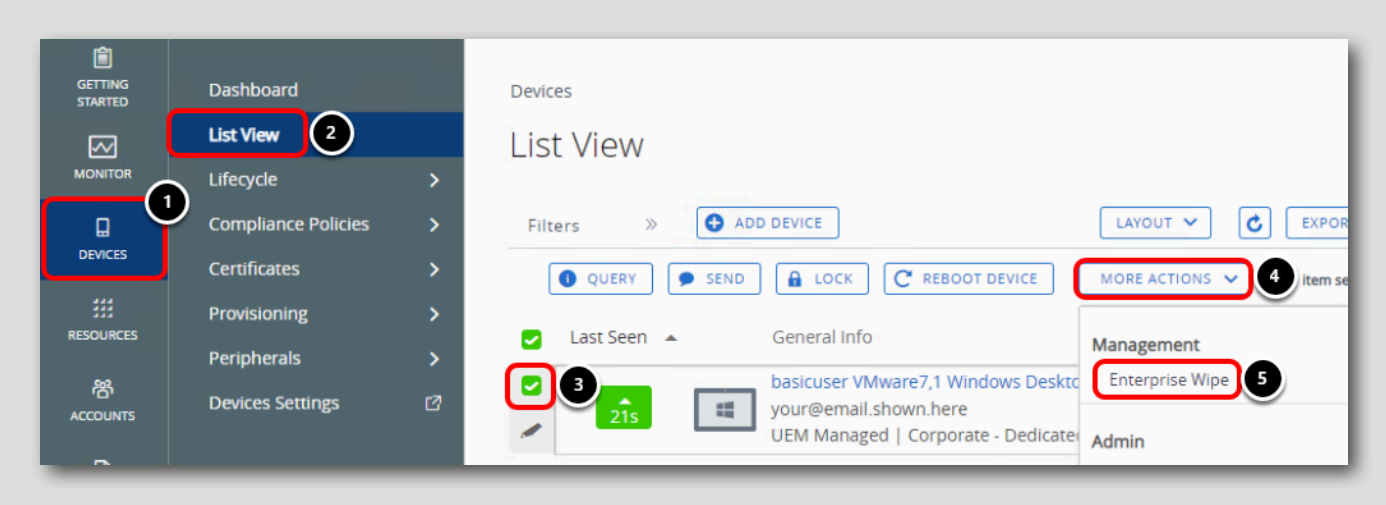
[802]

このセクションでは、Windows 10 仮想マシンの登録を解除して、他のラボ モジュールで使用できるようにします。

Enterprise Wipe ワイプ コマンドを使用して、Workspace ONE によってデバイスにプッシュされたすべての管理対象コンテンツ（プロファイルやアプリケーションなど）を削除しますが、デバイス上の個人的なコンテンツやデータは変更しません。

Workspace ONE UEM Console からの企業情報ワイプ

[803]

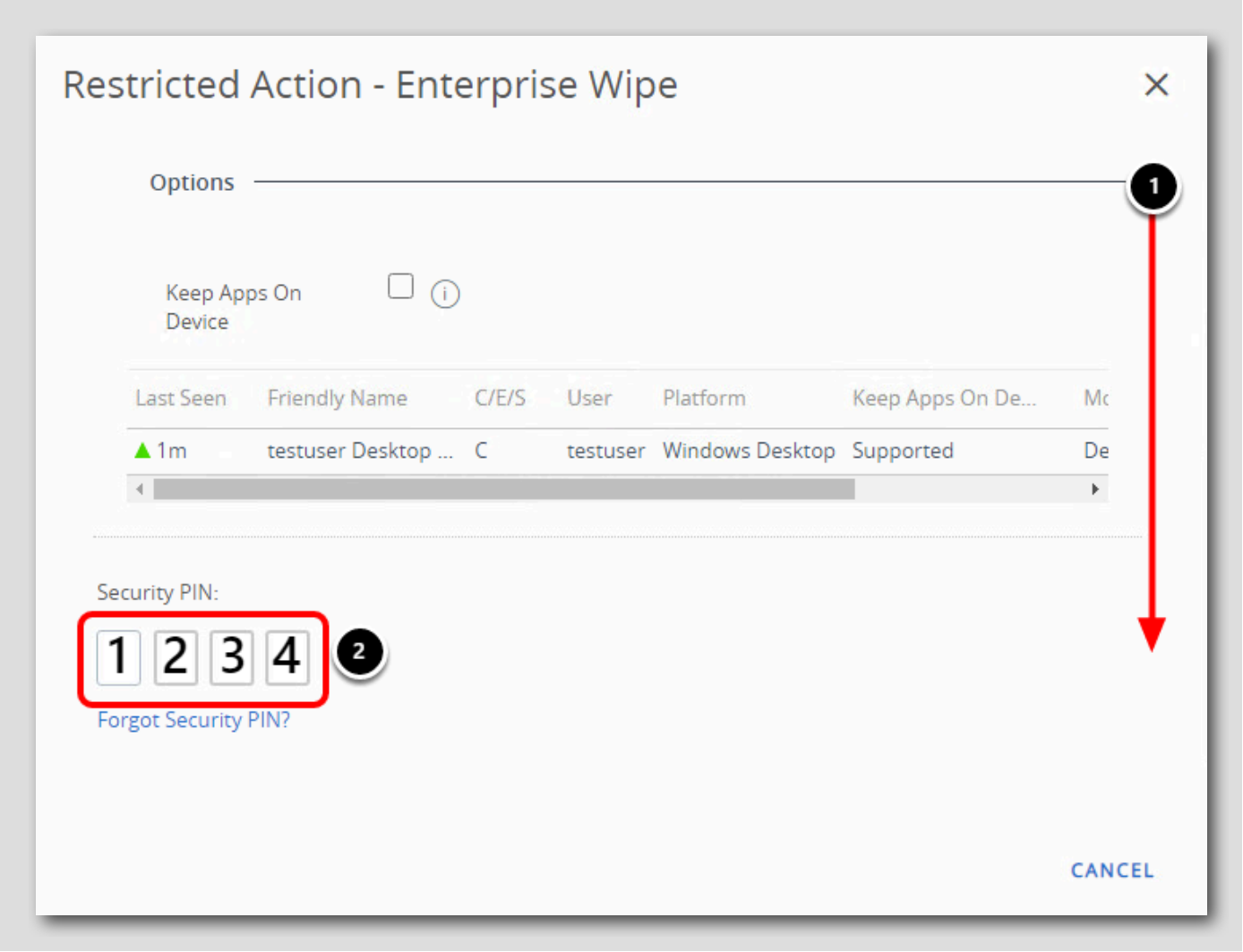


Google Chrome で Workspace ONE UEM 管理者コンソールに戻ります。

1. [Devices] をクリックします。
2. [List View] をクリックします。
3. デバイスのフレンドリ名の横にあるチェックボックスを選択します。
4. [More Actions] をクリックします。
5. [Enterprise Wipe] をクリックします。

PIN の入力とデバイスの企業情報ワイプ

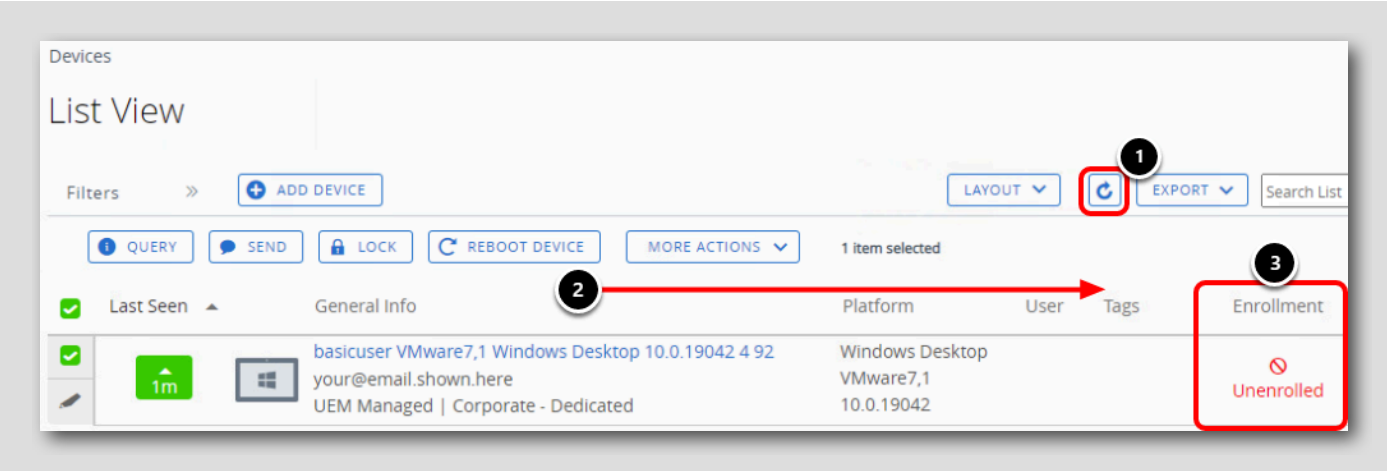
[804]



1. [Security PIN] 入力を見つけるために、下にスクロールする必要がある場合があります。
2. Workspace ONE UEM 管理コンソールに初めてログインしたときに作成したセキュリティ PIN (**1234**) を入力します。別の PIN を使用した場合は、代わりにその PIN を入力します。
3. **[Delete]** をクリックします。

企業情報ワイプの検証

[805]

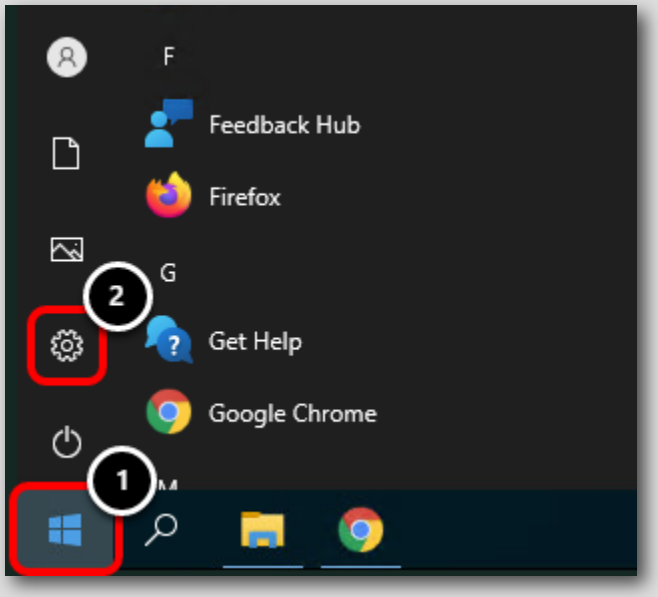


注：企業情報ワイプの処理には、数分かかる場合があります。

1. **更新**アイコンを定期的にクリックしてページを更新し、企業情報ワイプが処理されたかどうかを確認します。
2. 必要に応じて、右にスクロールして [Enrollment] 列を見つけます。
3. 企業情報ワイプ コマンドが処理されると、デバイスの登録状態が **[Unenrolled]** に変わります。

[Windows 10 Settings] への移動

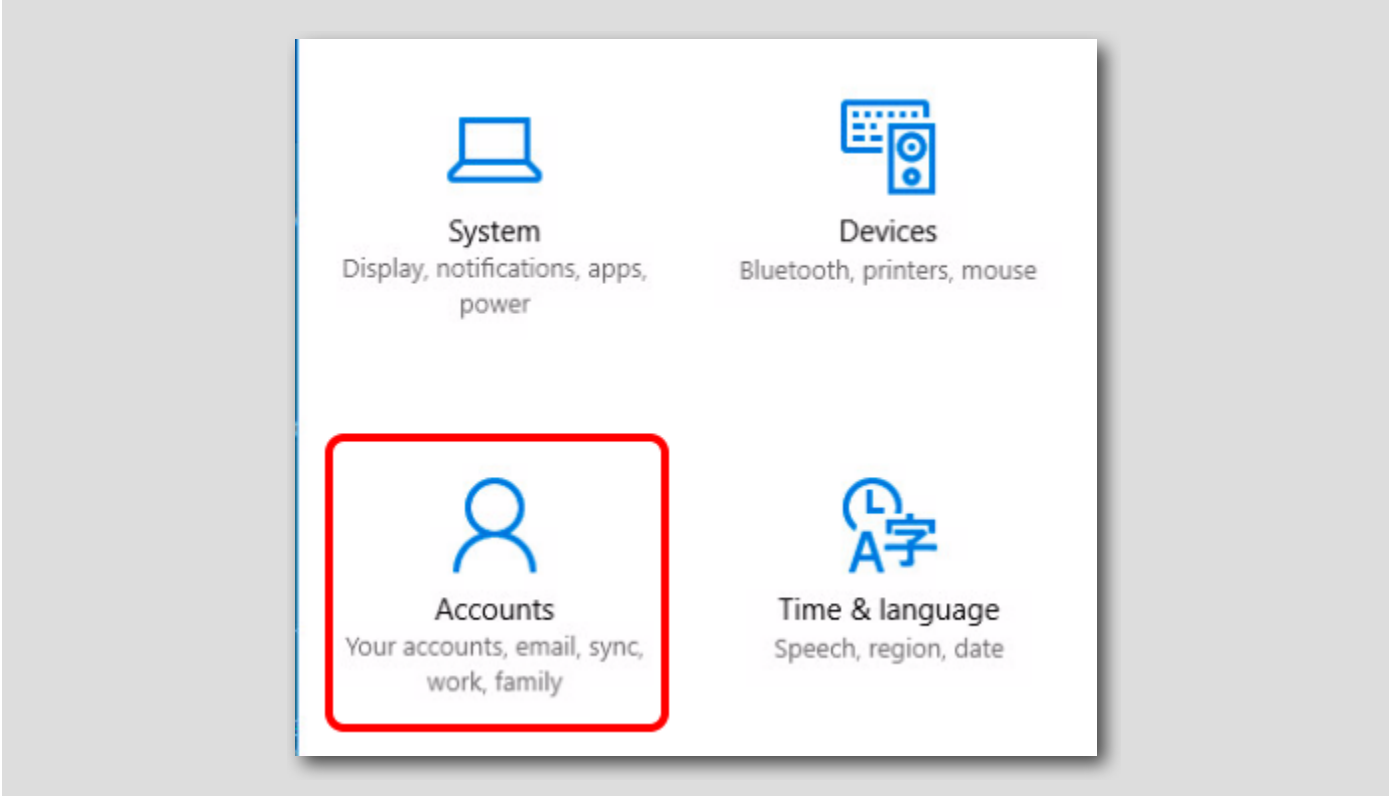
[806]



1. Windows アイコンをクリックします。
2. 歯車アイコンをクリックして、[Windows 10 Settings] にアクセスします。

[Accounts] 設定へのアクセス

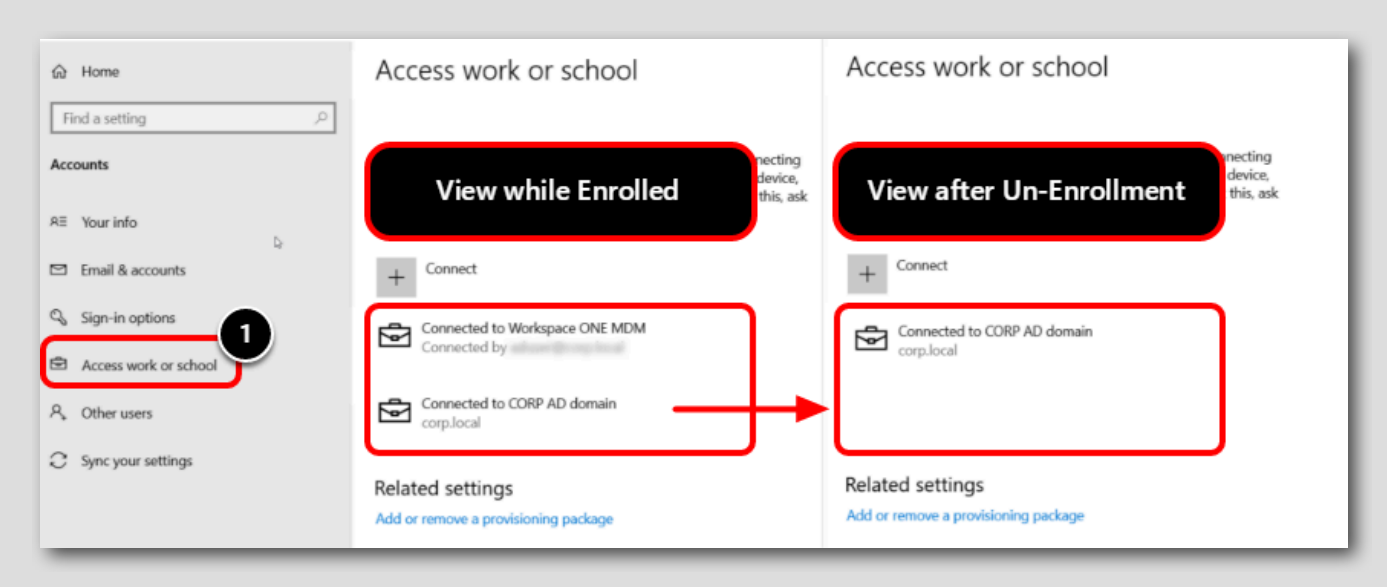
[807]



[Settings] メニューから **[Accounts]** にアクセスします。

管理アカウントが存在しないことの検証

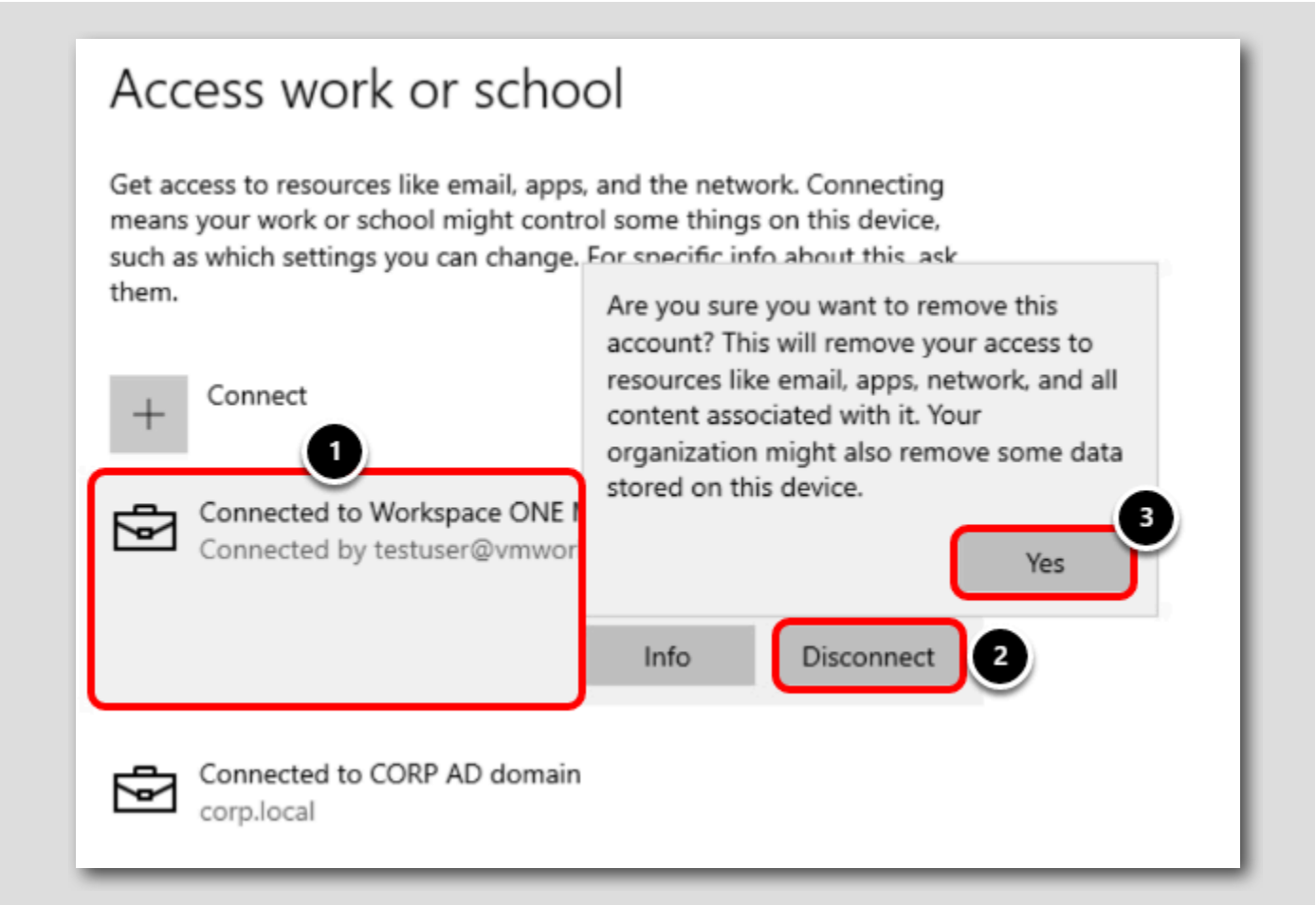
[808]



1. [Access work or school] をクリックします。
2. Workspace ONE MDM に接続されているアカウントがないことを確認します。

注：このラボでは、CORP AD ドメインはローカル ドメインであり、Workspace ONE UEM 登録によって管理されていないため、デバイスの登録時または登録解除時にこの接続が表示されます。

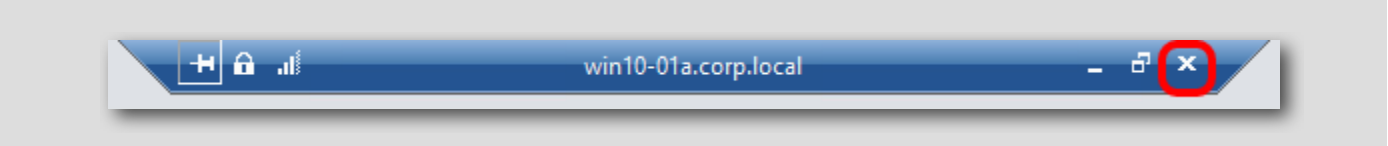
注：[Access Work or School] ページが以前に開かれていた場合は、ページを更新するか、ページから移動してから戻り、変更を確認する必要がある場合があります。



1. [Connected to Workspace ONE UEM] アカウントをクリックします。
2. [Disconnect] をクリックします。
3. [Yes] をクリックします。

メイン コンソールに戻る

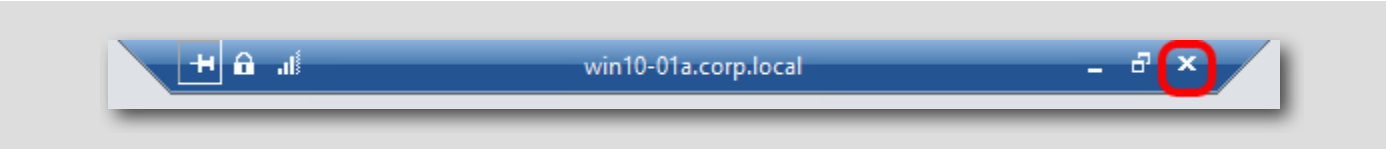
[809]



画面上部の [Remote Desktop Connection] バーで [Close (X)] をクリックしてメイン コンソールに戻り、Workspace ONE UEM Console 内での構成を完了します。

注：[Remote Desktop Connection] バーが表示されない場合は、固定が解除されている可能性があります。画面の上部にカーソルを置くと、

[Remote Desktop Connection] バーが再度表示されるので、[Close] をクリックします。



まとめ

[810]

Secure Access Service Edge (SASE) を使用した Anywhere Workspace のセキュリティ強化のハンズオン ラボはこれで終了です。ここで学んだ原則を踏まえて、従業員がどこにいても、Anywhere Workspace でクラウド アプリケーションと企業データセンターへのリモートからの安全なアクセスを可能にする方法を検討してください。

レビューでは、次の方法について学習しました。

- Workspace ONE Tunnel と Workspace ONE UEM の統合
- Workspace ONE Tunnel へのトラフィックをトンネリング、ブロック、またはバイパスするためのトンネル トラフィック ルールの構成
- Workspace ONE Tunnel アプリケーションのインポートとエンド ユーザーへの公開
- Workspace ONE Tunnel の VPN ペイロードを使用したプロファイルの作成と公開
- Windows 10 仮想マシンの登録
- Workspace ONE Tunnel アプリケーションを使用した、プライベート ネットワークでホストされているイントラネット Web サイトへのアクセス
- 不要なアクションや悪意のあるアクションをブロックするための Secure Access での Cloud Web Security ポリシーの構成
- SD-WAN Network Orchestrator のトラフィックの詳細とメトリックの調査

VMware Tech Zone を使用して VMware End User Computing に関する知識を高める

[811]

VMware End User Computing (EUC) について詳しく知りたいのですが、どこから始めればよいかわからないこともあると思います。この場合は、*https://techzone.vmware.com* を参照すれば十分です。ここでは、VMware End User Computing 製品を理解、評価、展開するための情報をすぐに見つけることができます。

Tech Zone は、実用的な製品ガイダンス、厳選されたアクティビティ パス、技術的なコンテンツを提供して、初心者をエキスパートへと成長させることに重点を置いています。Tech Zone の使命は、デジタル ワークスペースへの移行のあらゆる過程において、ユーザーの知識を深めるために必要なリソースを提供することです。

興味をお持ちの場合は、*https://techzone.vmware.com* をご確認ください。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.
 Lab SKU: HOL-2251-09-DWS Version: 20221025-143140