GUIDE – APRIL 2019

PRINTED 5 APRIL 2019

MANAGING CHROME OS DEVICES: VMWARE WORKSPACE ONE OPERATIONAL TUTORIAL

VMware Workspace ONE

vmware®

Table of Contents

Configuring Basic Chrome OS Management in Workspace ONE UEM

Overview

Introduction

VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. This exercise introduces you to managing Chrome OS devices in Workspace ONE.

Audience

This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM (unified endpoint management), powered by VMware AirWatch, is also helpful.

Getting Started with Chrome OS Management

Introduction

This exercise introduces you to managing Chrome OS devices in Workspace ONE. This exercise walks through creating a profile and enrolling your device to test the results. The procedures are sequential and build upon one another, so make sure that you complete each procedure in this section before going to the next procedure.

Prerequisites

Before you can perform the procedures in this exercise, you must complete the following tutorials:

- Installation and Setup
- Initial Configuration

This exercise requires an admin user to authenticate into G-Suite and enroll device into Workspace ONE UEM. Note the user account information in the following table. The details provided in this table are based on a test environment. Your user account details will differ.

User Account Information	
User name	`admin`
Password	`VMware1!`
Email	`admin@quickstarttest.com`

You must also satisfy the following requirements:

- Chrome Enterprise license
- Google Admin Console Service Account
- Google Cloud Directory Sync Enabled
- Supported Chrome OS device
- Factory reset device in out of the box mode

For more information, see Requirements for Deploying Chrome OS.

Caution: *Do not* factory reset your personal device to complete these exercises.

Logging in to the Google Admin Console

To perform most of the steps in this exercise, you must first log in to the Google Admin Console.

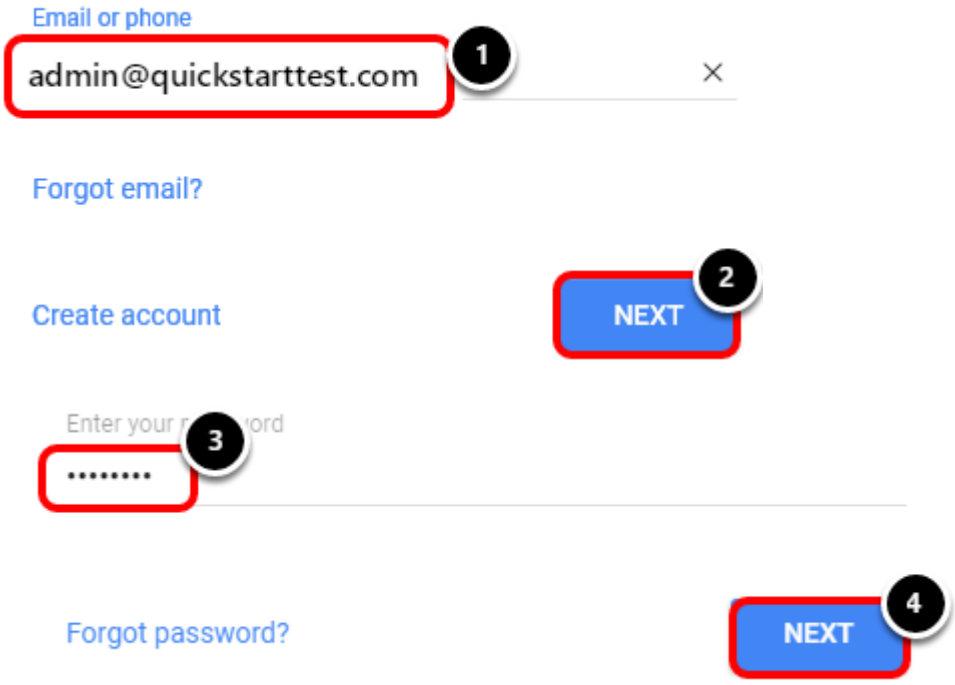
1. Launch Chrome Browser

On your desktop, double-click the **Google Chrome** icon.

2. Open the Google Admin Console

Navigate to http://admin.google.com/.

3. Authenticate

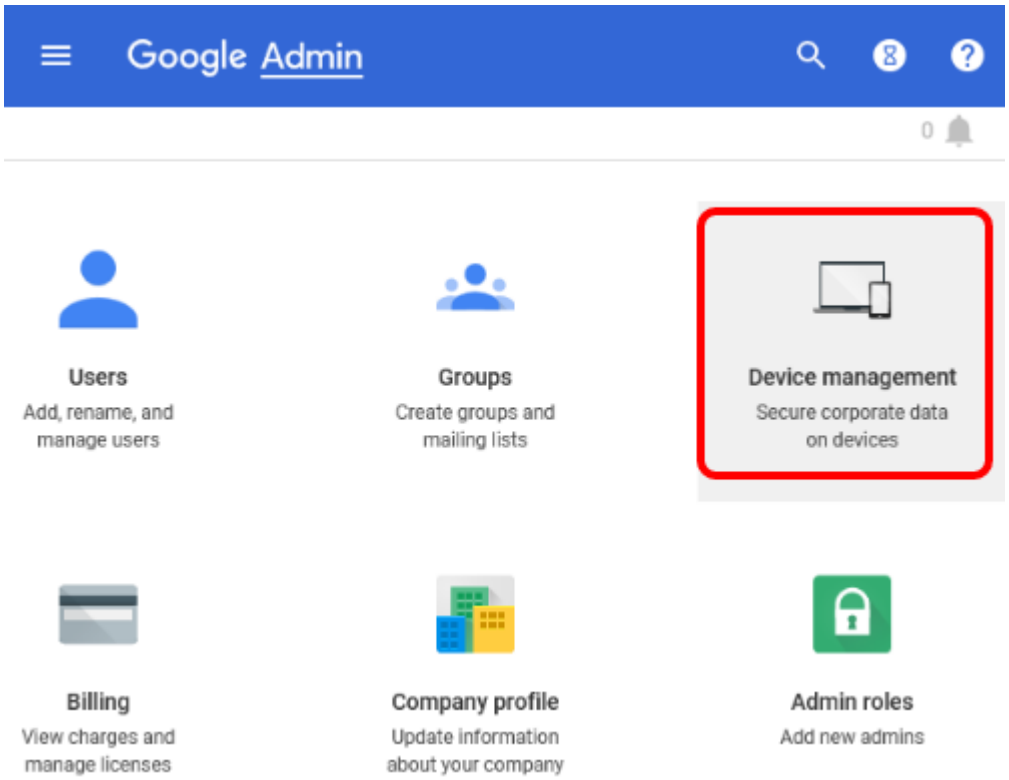


1. Enter your email address or phone number. For example, `admin@quickstarttest.com`.
2. Click **Next**.
3. Enter your **Password**. For example, `VMware1!`.
4. Click **Next**.

Enabling Chrome Device Management

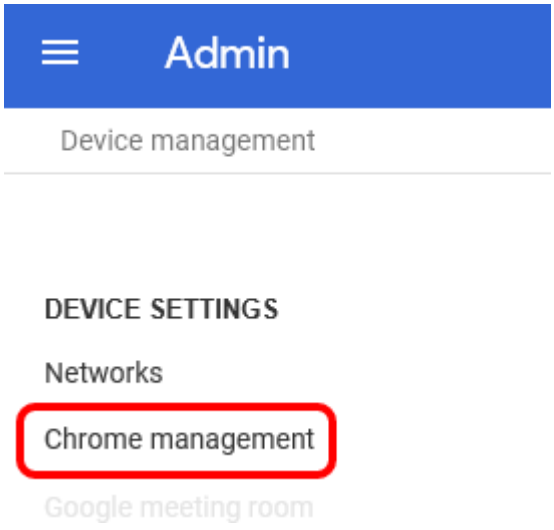
In this activity, enable Chrome device management from the Google Admin page.

1. Open Device Management Settings



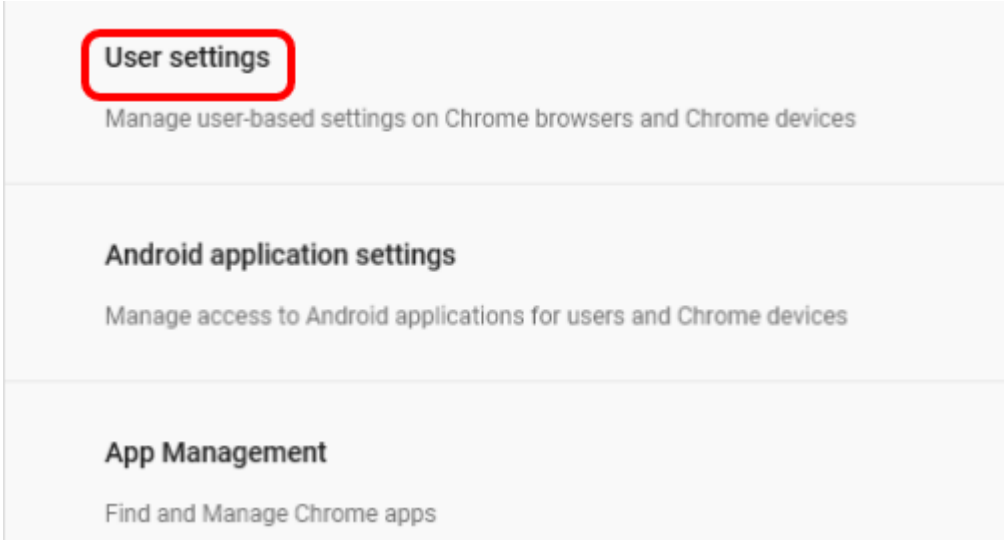
From the home page of the Google Admin Console, click **Device Management**.

2. Open Chrome Management Settings



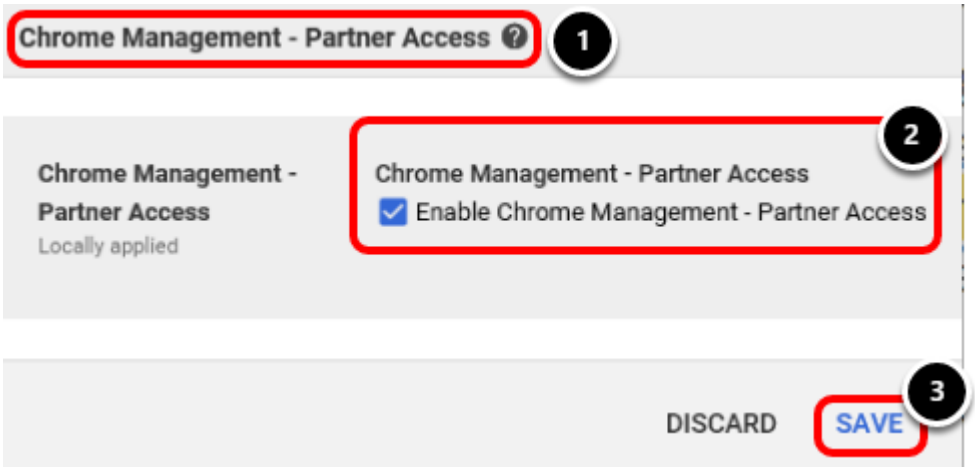
Click **Chrome management**.

3. Open User Settings



Click **User Settings**.

4. Enable Partner Access



1. Scroll to the **Chrome Management - Partner Access** section.
2. Select the **Enable Chrome Management-Partner Access** check box.
3. Click **Save**.

Integrating Google Management with Workspace ONE UEM

Introduction

In this activity, you integrate Workspace ONE UEM with Google management. The procedures are sequential and build upon one another, so make sure that you complete each procedure in this section before going to the next procedure.

Prerequisites

Before you can perform the procedures in this exercise, you must first complete the steps in Getting Started with Google Management.

Logging In to the Workspace ONE UEM Console

To perform most of the steps in this exercise, you must first log in to the Workspace ONE UEM Console.

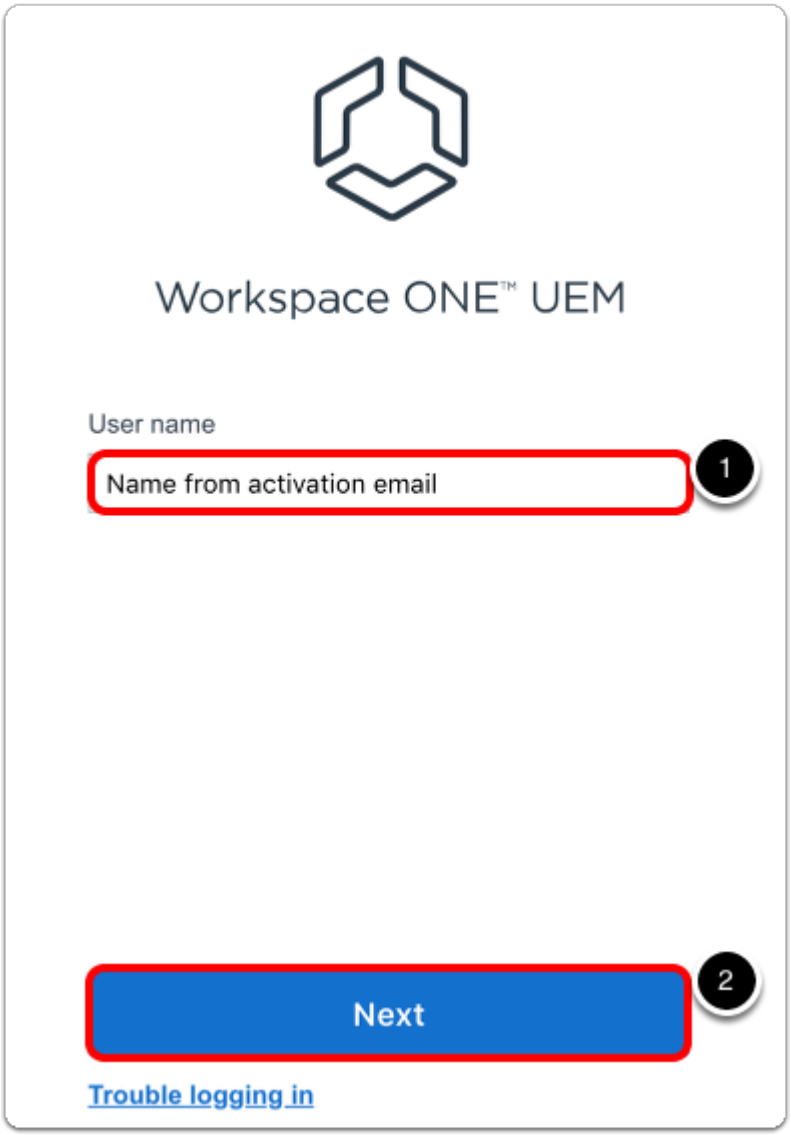
1. Launch Chrome Browser

On your desktop, double-click the **Google Chrome** icon.

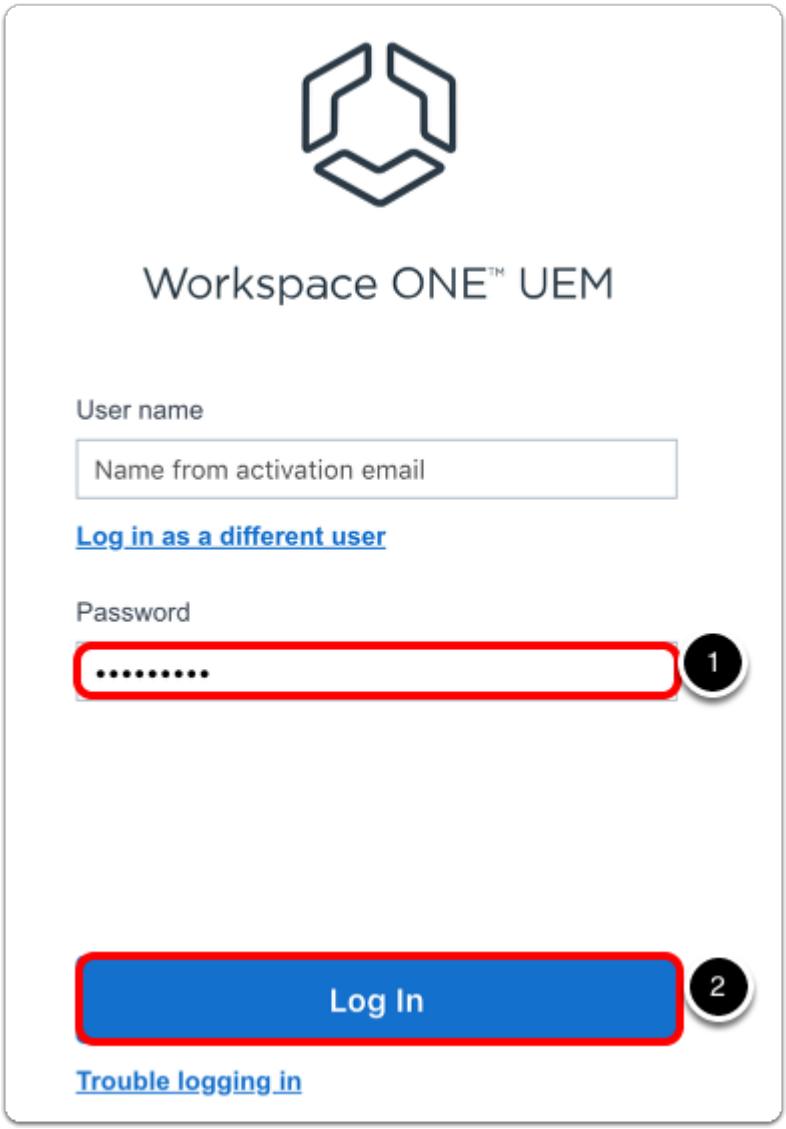
2. Navigate to the VMware Workspace ONE UEM Console

For example, navigate to `https://<WorkspaceONEUEMHostname>` where *`WorkspaceONEUEMHostname`* is the host name of the Workspace ONE UEM console.

3. Authenticate In to the Workspace ONE UEM Console



1. Enter your **Username**. This is the name provided in the activation email.
2. Click **Next**. After you click Next, the Password text box is displayed.



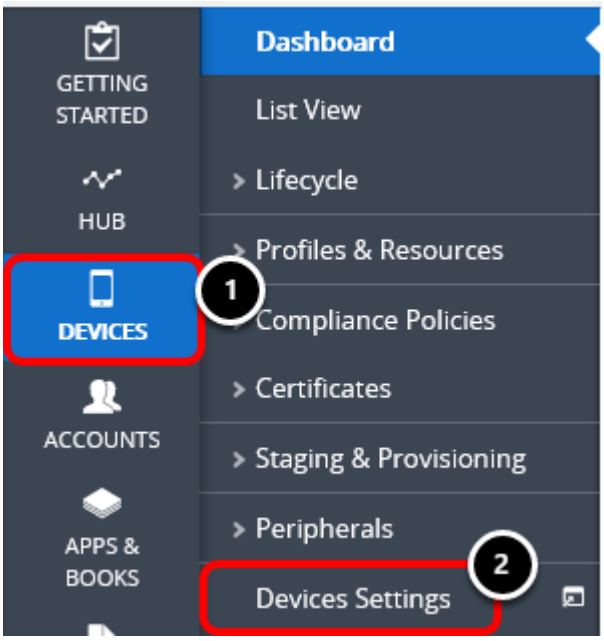
1. Enter your **Password**. This is the password provided in the activation email.
2. Click the **Login** button.

Note: If you see a Captcha, be aware that it is case sensitive.

Configuring Google Integration with Workspace ONE UEM

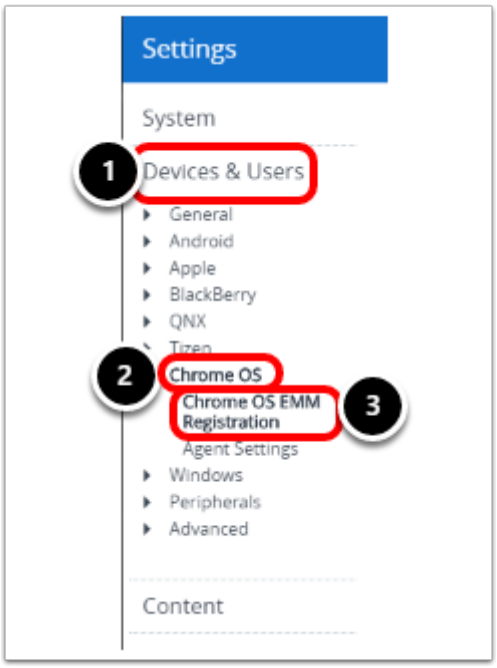
Begin integrating Workspace ONE with Google by entering your Chrome admin email on the Workspace ONE Console setup page. This redirects you to a Google authorization page to grant permissions.

1. Navigate to Device Settings



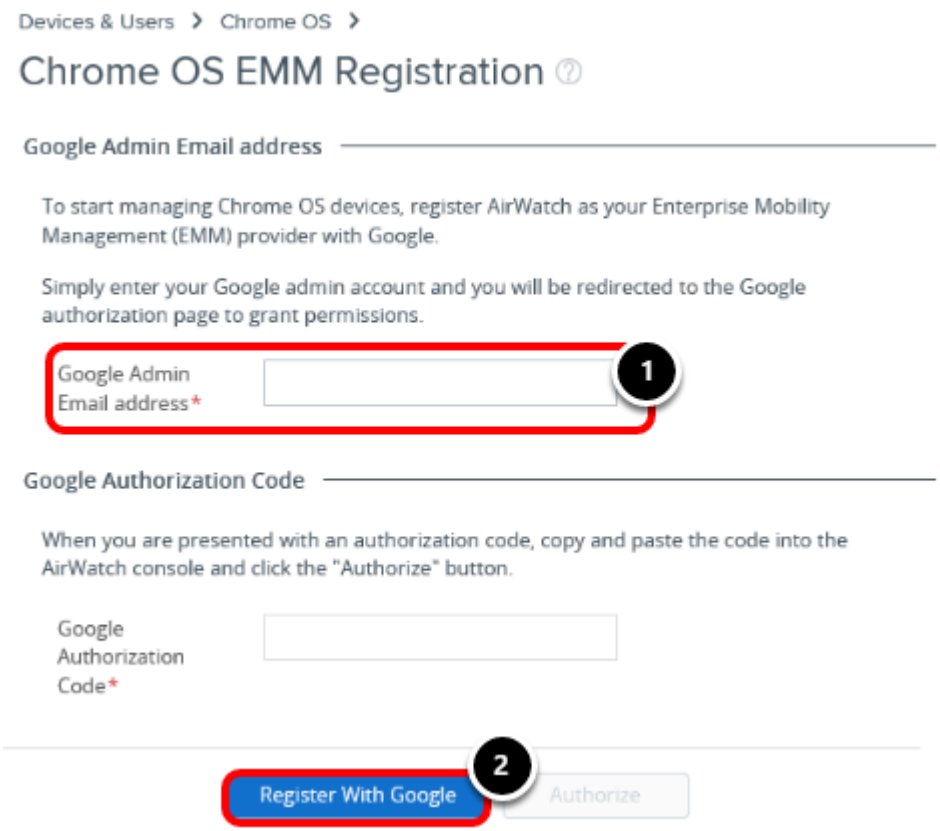
1. In the Workspace ONE Console, click **Devices**.
2. Click **Device Settings**.

2. Navigate to EMM Registration Settings



1. Click **Devices & Users**.
2. Click **Chrome OS**.
3. Click **Chrome OS EMM Registration.**

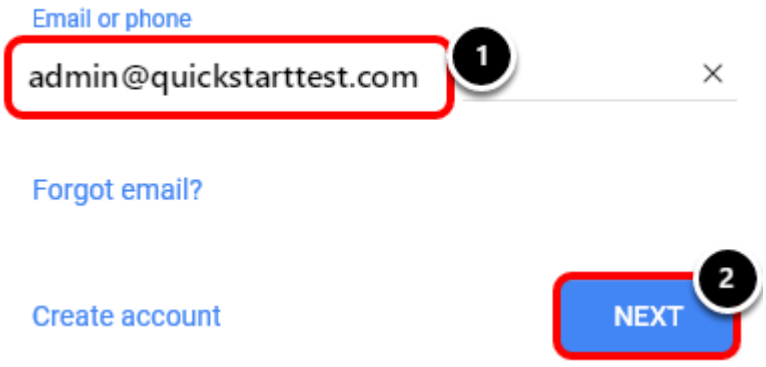
3. Initiate Google Registration

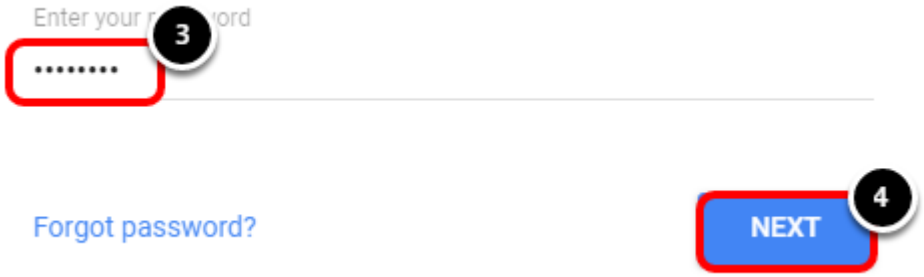


1. Enter the **Google Admin Email Address**. For example, `admin@quickstarttest.com`.
2. Select **Register with Google** which redirects you to Google.

Caution: Please make sure you have pop-ups enabled otherwise the Google authorization page will not open.

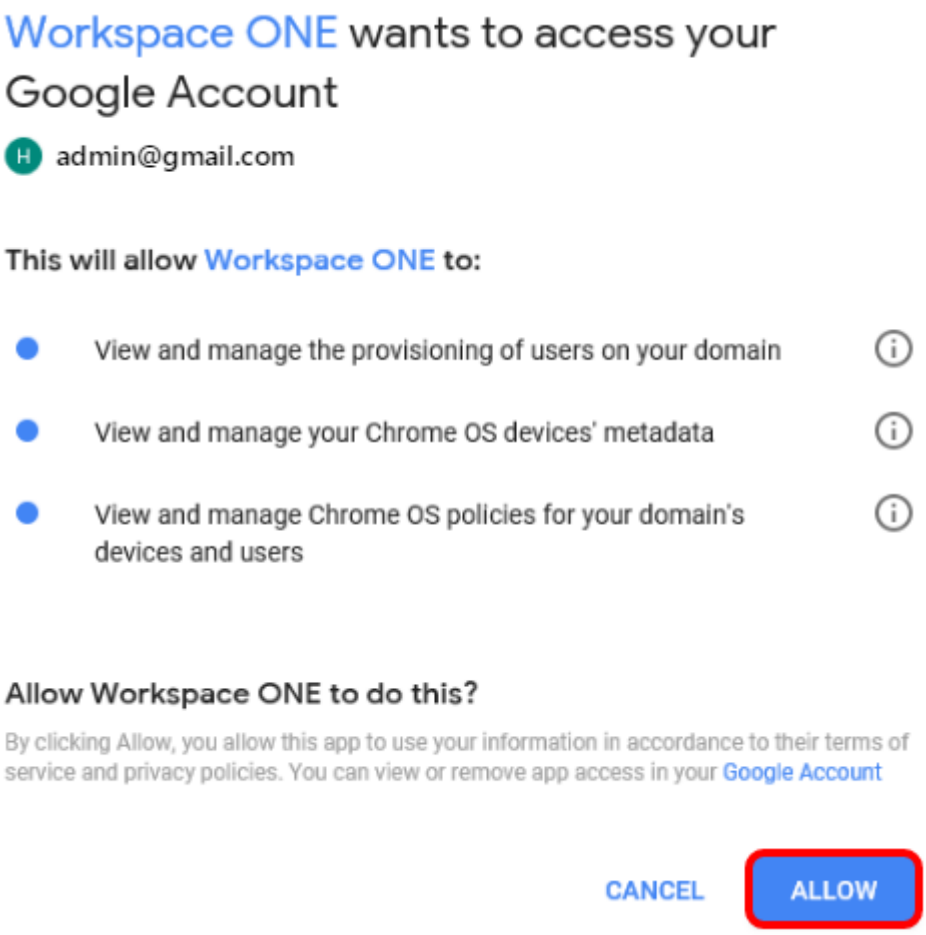
4. Log In to Google





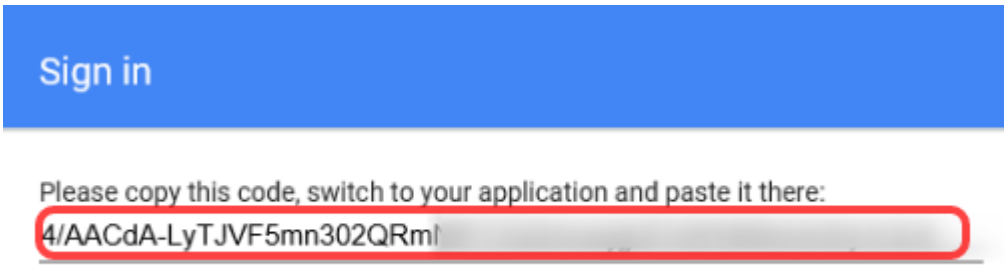
1. Enter your email address or phone number. For example, `admin@quickstarttest.com`.
2. Click **Next**.
3. Enter your **Password**. For example, `VMware1!`.
4. Click **Next**.

5. Allow Workspace One to Access Your Google Account



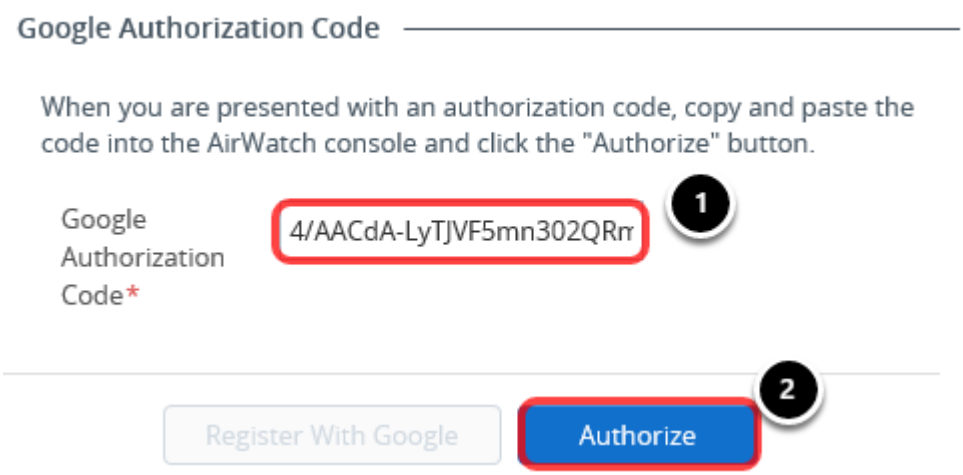
Review the screen and click **Allow**.

6. Copy the Google Authorization Code



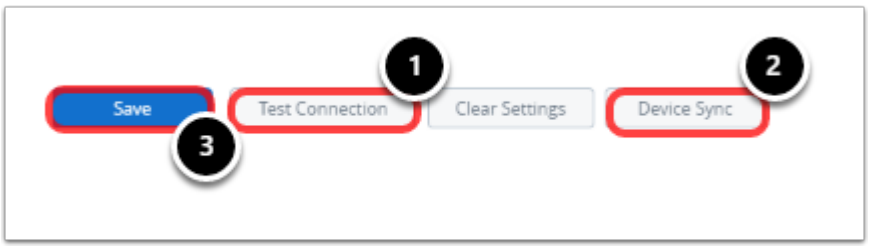
Copy the Google Authorization Code.

7. Register Google with Workspace ONE



1. Return to the Workspace ONE Console and paste the code copied from Google into the **Google Authorization Code** field.
2. Select **Authorize**.

8. Verify Connectivity & Save



1. Click **Test Connection** to ensure the connection between AirWatch and Google is established. If successful, a green `Test Connection Successful` message displays.
2. Click **Device Sync** to manually sync new Chrome OS enrollments into the Workspace ONE UEM Console.
3. Click **Save**.

Enrolling Chrome OS Devices

Introduction

Device enrollment establishes communication with the Workspace ONE UEM console and allows devices to access internal resources. In this exercise, generate a QR code in the Workspace ONE UEM console, and use it to enroll your Android COPE device.

While this exercise walks through QR code enrollment, there are several additional enrollment options for Android COPE devices:

- AirWatch Relay
- Unique Identifier
- Zero Touch

Prerequisites

Before you can perform the activities in this exercise, you must meet the following requirements:

- Successfully complete directory integration
- Retrieve the Group ID from Workspace ONE UEM Console
- Android device 8.0 or later
- Factory reset device in out of the box mode

Warning: *Do not* factory reset your personal device to complete these exercises.

This exercise requires a user to enroll their device into Workspace ONE UEM. Gather the required account information, and record it in the following table. The account information used in this exercise is based on a test environment. Your account details will differ.

User Account Information	
User name	
Password	
Email	

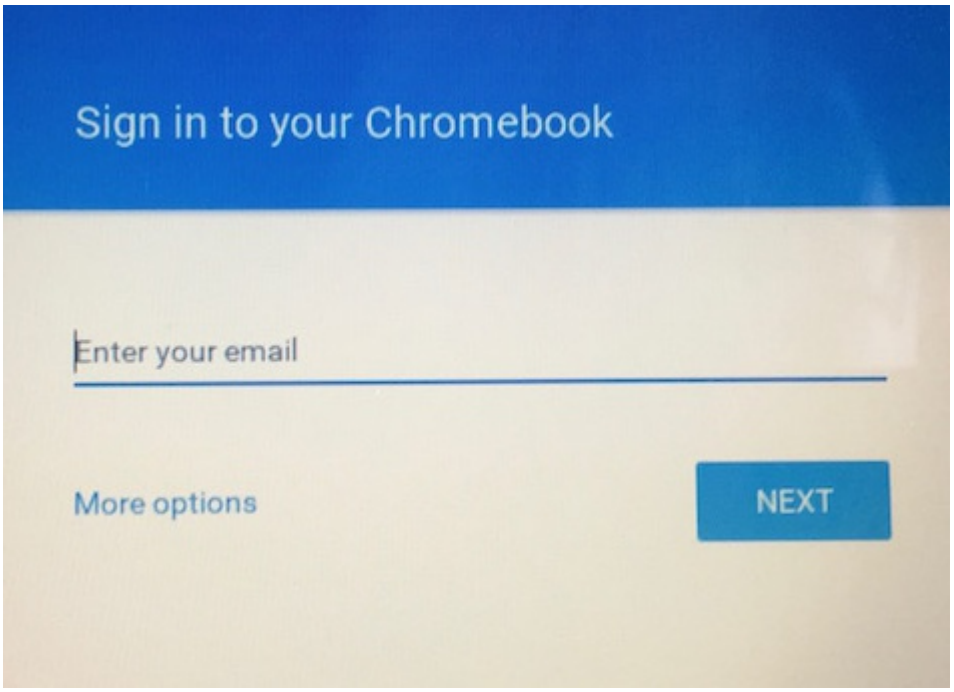
Enrolling a Chrome OS Device

Enrollment is facilitated from the Chrome OS device using the Google admin credentials or existing G Suite user credentials. After you select done, the Chromebook automatically applies any pre-configured device policies and is ready for a user to sign in. Once a user signs in, all applicable user profiles are pushed to the Chrome device. Once devices are enrolled, they display in the Device List View in the Workspace ONE UEM console.

1. Power On the Device

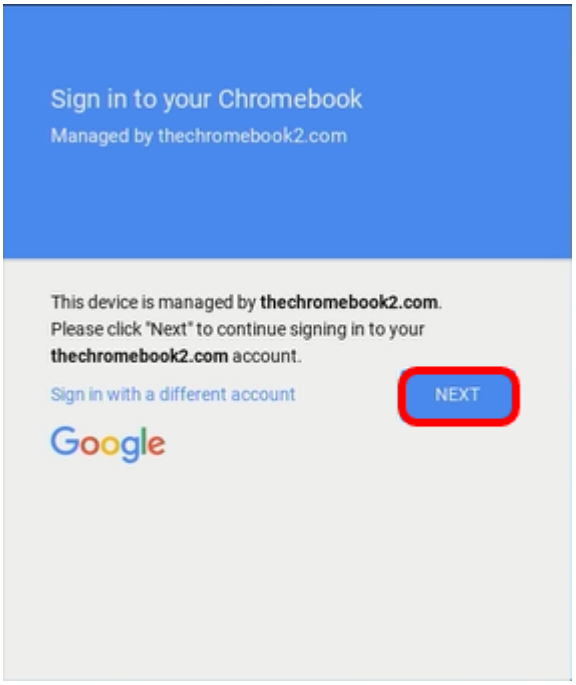
Boot up a factory-reset Chrome OS device that's connected to the internet.

2. Go to Enterprise Enrollment



At the Sign into the Chromebook page, press **CTRL+ALT+E** to bypass the sign-in screen and go straight to enterprise enrollment.

3. Authenticate



Enter the user name and password from your Google Admin welcome letter or use your existing G Suite user credentials, and click **Next**.

4. Finish Enrollment

Click **Done**.

Configuring Chrome OS Profiles

Introduction

In this exercise, set up and configure a restrictions profile in Workspace ONE UEM to explore how enterprise profile settings apply on an Android COPE device.

Prerequisites

Before you can complete this exercise, you must successfully enroll an Android device in COPE mode.

Understanding Configuration Options for Chrome OS Profiles

Profiles are the mechanism by which Workspace ONE UEM manages settings on a device. All profiles are broken down into two basic sections; the *General* section and the *Payload* section.

- The General section defines the profile's name and assignment settings.
- The Payload sections define actions to be taken on the device.

Every profile must have all *required* fields in the General section properly filled out and at least one payload configured.

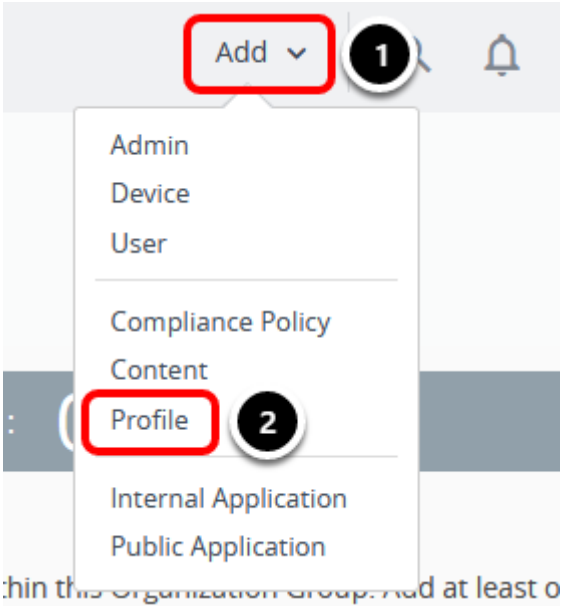
While all Workspace ONE UEM profiles manage device settings, Chrome OS profiles can apply at the device level or the enrollment-user level.

- **Device Profiles** - Apply to Chrome OS devices regardless of the user logged into the device. Device polices are applied through Smart Groups.
- **User Profiles** - Apply to Chrome OS devices at the user level, and do not apply to users signed in as guest or with a Google Account outside of your organization (such as a personal Gmail account). User polices are applied through User Groups.

Configuring a User Profile for Chrome OS

In this procedure, configure a Security & Privacy user profile for Chrome OS to disable incognito mode.

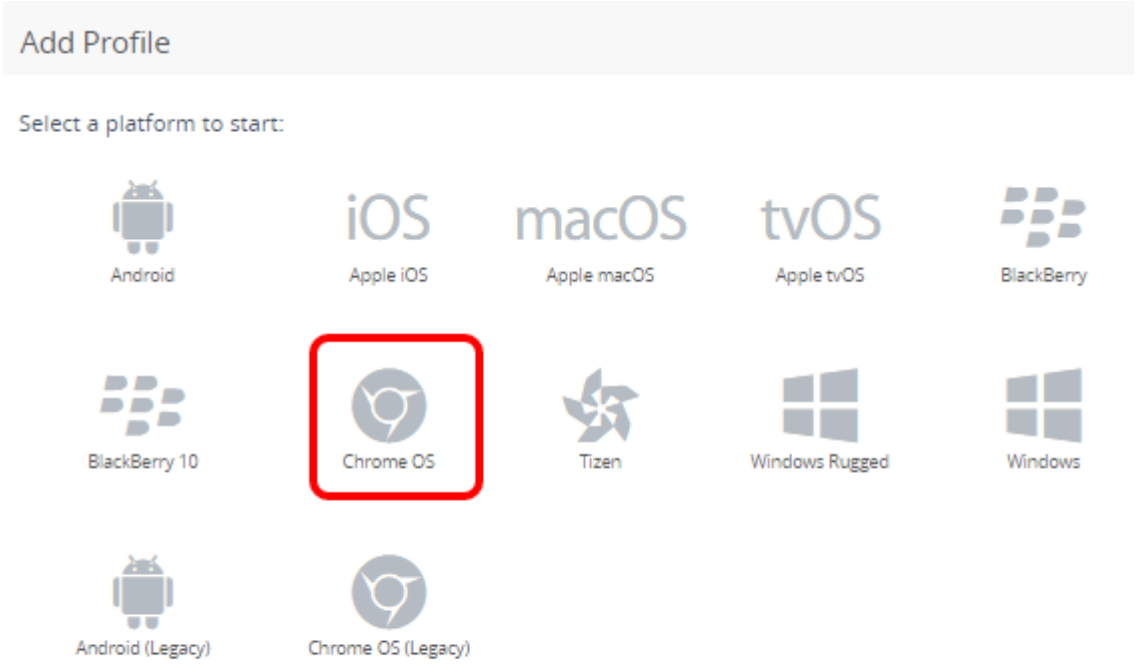
1. Navigate to Profile Settings



In the upper-right corner of Workspace ONE UEM Console:

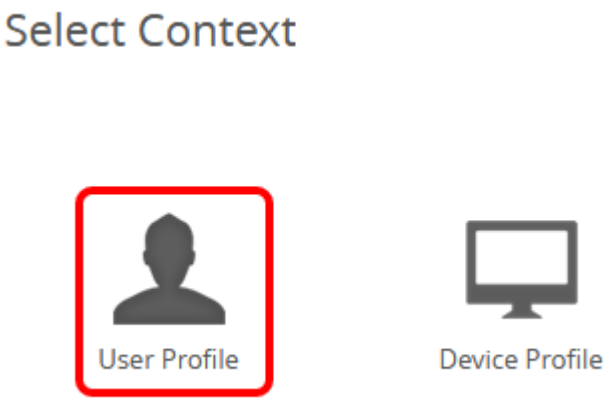
1. Select **Add**.
2. Select **Profile**.

1.1. Select the Platform



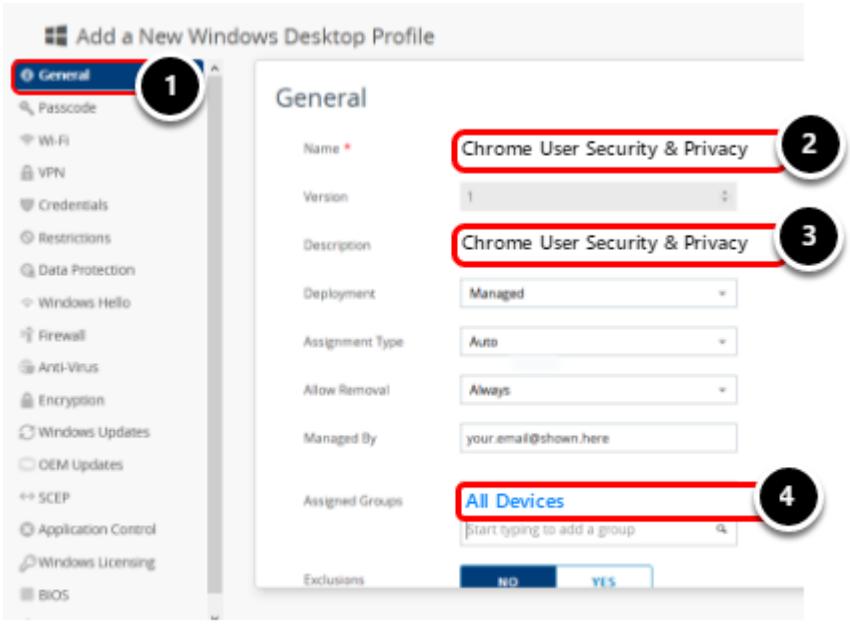
Select the **Chrome OS** icon.

1.2. Select Profile Context



Select **User Profile**.

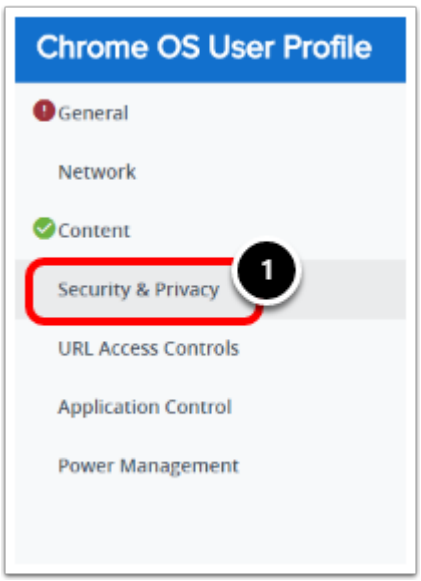
2. Define the General Settings



1. Select **General** if it is not already selected.
2. Enter a profile name such as `Chrome User Security & Privacy` in the Name text box.
3. Copy the profile name into the Description field.
4. If necessary, scroll down to **Assigned Groups.** Click the field and select **All Devices** from the list of Assignment Groups that populate.

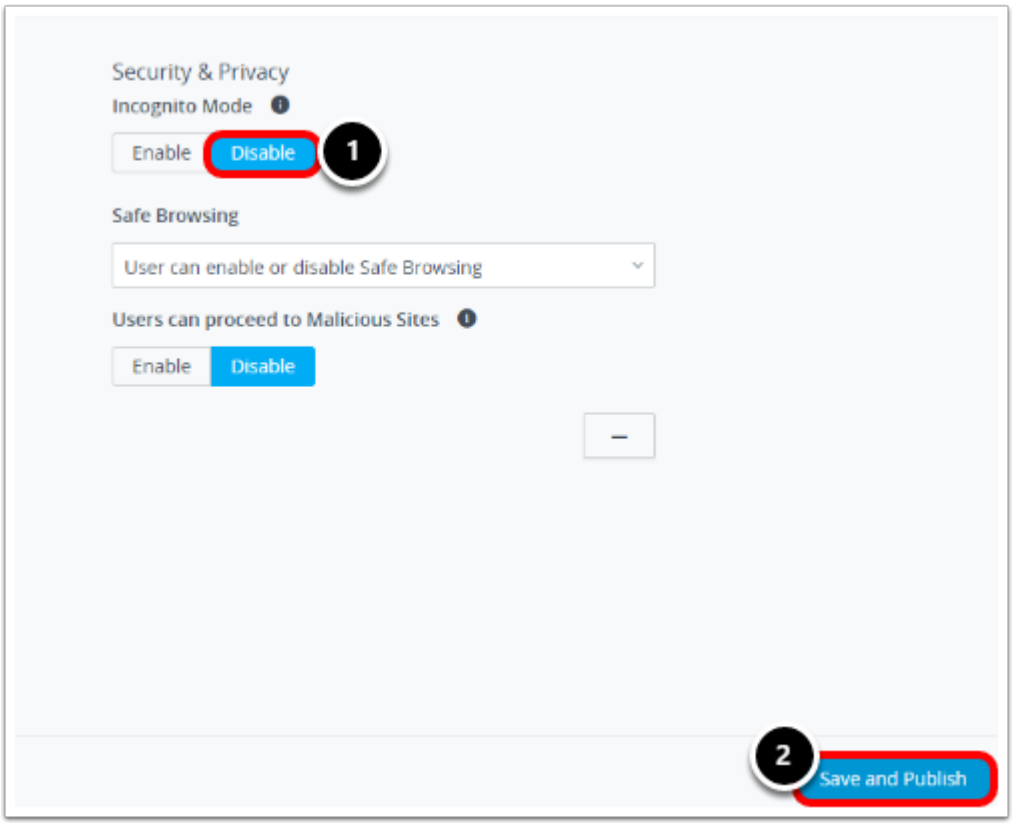
Note: Do *not* click Save & Publish at this point. This interface allows you to move around to different payload configuration screens before saving.

3. Open the Security & Privacy Payload



1. Select the **Security & Privacy** payload from the menu on the left.
2. Click the **Configure** button to begin configuring payload settings.

4. Configure Security & Privacy Settings



1. **Disable** Incognito Mode to keep users from browsing the web without storing local data.
2. Click **Save and Publish**.

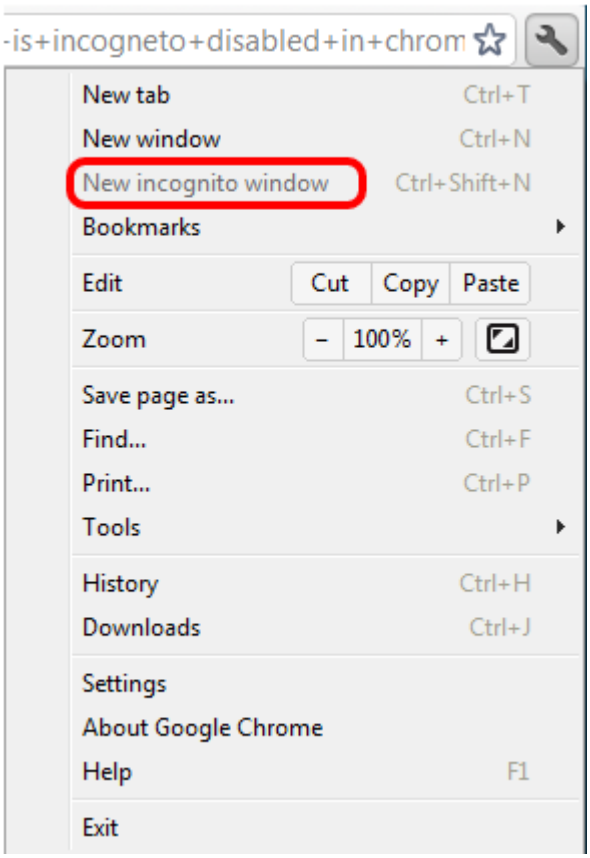
5. Publish the Profile

Click **Publish**.

6. Verify the Profile Applied

Profiles for Chrome OS are deployed using API calls, which are a different solution than is used with other platforms, in which the profile is sent directly to the Workspace ONE Intelligent Hub on the device. For Chrome OS devices, the Workspace ONE UEM console relies on API responses to the Google Cloud to push new polices. The console displays a green check mark to show that the policy has been updated to the Google cloud.

7. Test the Incognito Mode Restriction



Try to open a tab in incognito mode. Notice how the option is disabled.

Summary and Additional Resources

Conclusion

This operational tutorial provided steps to deploy corporate owned personally-enabled Android devices.

Procedures included:

- Registering Android EMM
- Configuring Corporate Owned Personally-Enabled Devices
- Configuring the Enrollment QR Code
- Enrolling Using the QR Code
- Configuring Camera Restrictions

Terminology Used in This Tutorial

The following terms are used in this tutorial:

application store	A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.
auto-enrollment	Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.
catalog	A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.
cloud	Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.
device enrollment	The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.
identity provider (IdP)	A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.
mobile device management (MDM) agent	Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the VMware Glossary.

Additional Resources

For more information about Workspace ONE, you can explore the following resources:

- VMware Workspace ONE Action Path
- VMware Workspace ONE product page
- VMware Workspace ONE Documentation
- VMware Identity Manager product page
- VMware Identity Manager Documentation
- VMware Workspace ONE UEM, powered by VMware AirWatch product page
- VMware AirWatch Documentation
- VMware Workspace ONE free trial
- VMware Workspace ONE Enterprise Edition Reference Architecture
- VMware End-User-Computing Blogs
- Workspace ONE UEM Hands-On Lab

About the Authors

This exercise was written by:

- Karim Chelouati, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware
- Hannah Jernigan, Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Feedback

The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com