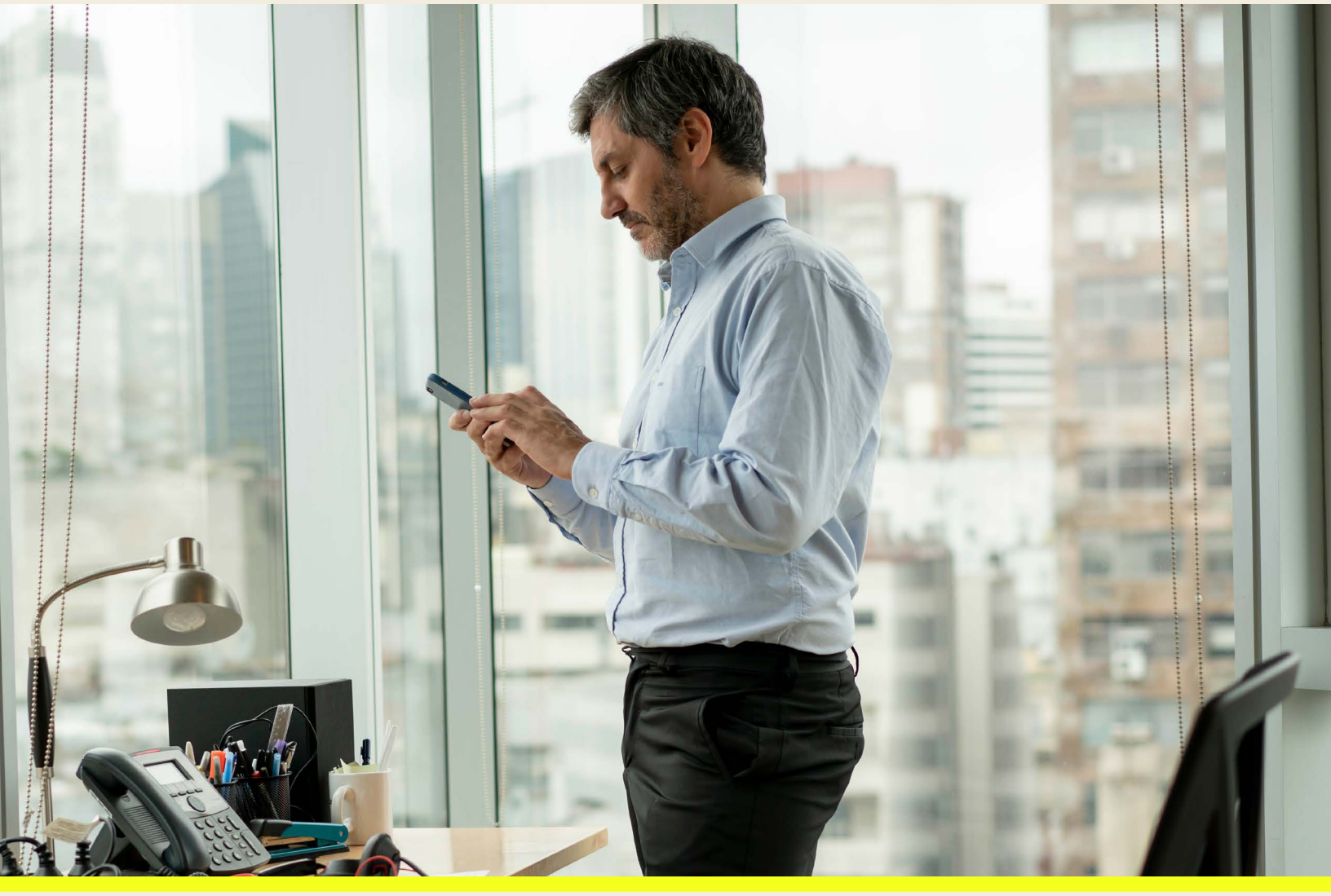


Jamf Now MDM: Trusted Connection customer, administrator and end-user setup steps

April, 2025

verizon business

Contents

Summary

This document covers the Jamf Now customer setup steps required to deploy Trusted Connection.

Trusted Connection is supported on the following 4 operating systems: iOS, Android, macOS and Windows. Please note that Jamf Now only supports Apple specific devices (iOS and macOS).

Steps for Customer Admins

1. Purchase Trusted Connection Client Licenses in Apple Business Manager.
2. Sync Trusted Connection Licenses from Apple Business Manager to Jamf Now.
3. Assign Trusted Connection to a Blueprint.

Steps for Customer End-Users

4. Install the “Versa Network Root Certificate Authority”.
5. Set the Hostname, Enterprise Name and User ID.
6. Connected the device to Verizon’s Trusted Connection service.

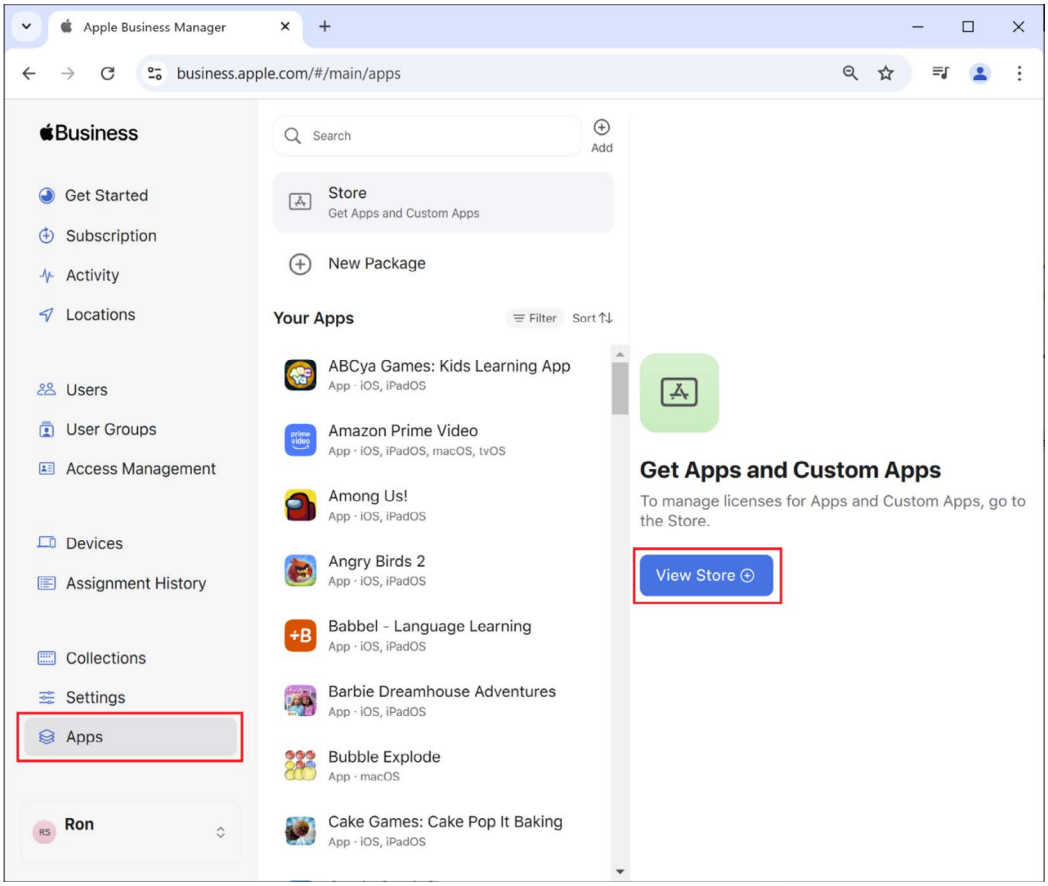
Steps to deploy Trusted Connection on Jamf Now Managed devices

Jamf Now requires the use of volume purchasing to deploy paid iPad or iPhone apps.

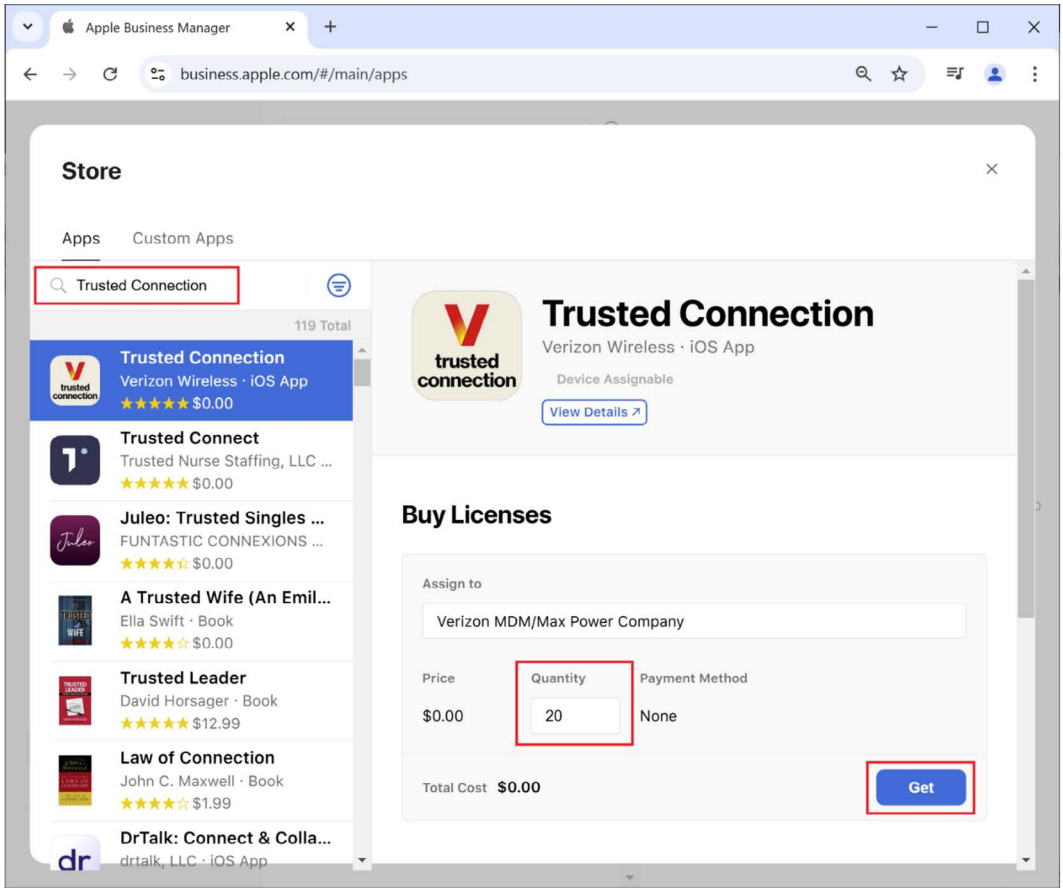
- Purchased licenses are required to install the application silently and prevent user uninstallation.
- Non-supervised devices will prompt users to permit the installation of apps regardless of whether app licenses are used. Verizon and Jamf recommend supervising your devices when deploying licensed apps to install apps without end user interaction.

Purchase Trusted Connection client licenses in Apple Business Manager

- **Step 1:** Log on to your Apple Business Manager account: https://business.apple.com
- **Step 2:** Click on **Apps**, then click on **View Store**.



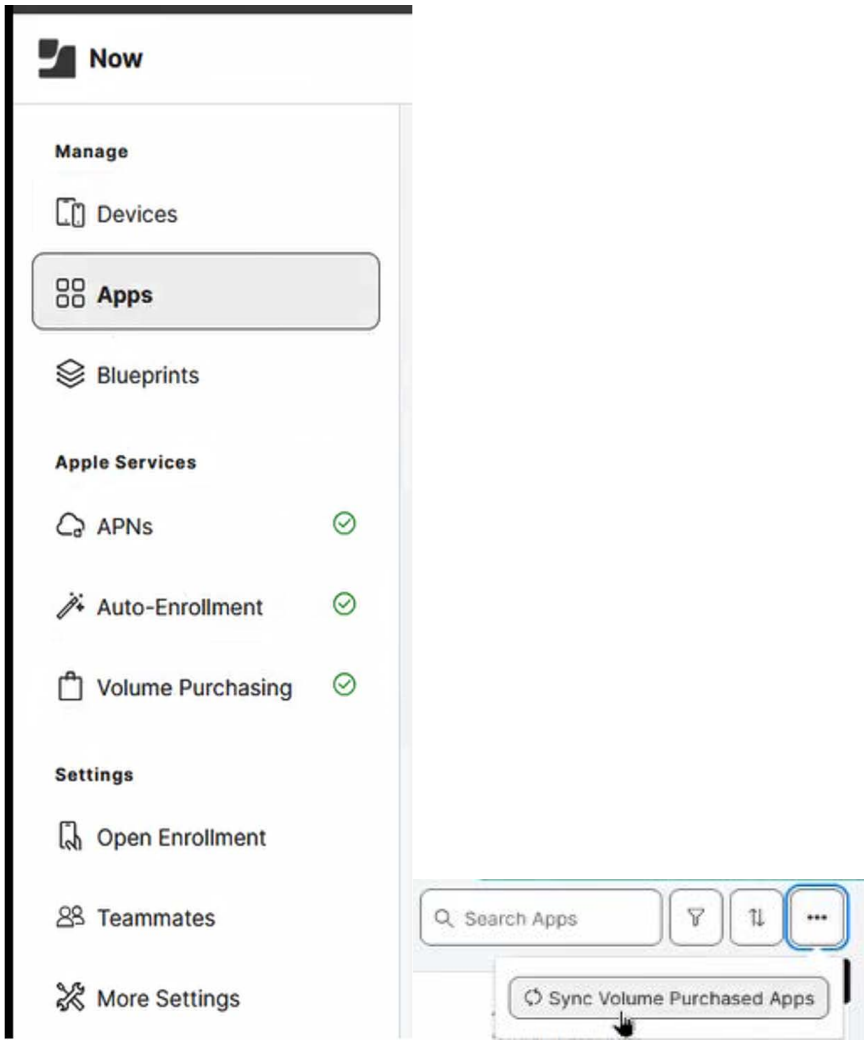
- **Step 3:** Enter “Trusted Connection” in the search field, then select the Trusted Connection application from the search results.
- **Step 4:** Enter the **Quantity** of licenses purchased in Verizon systems, then click **Get** to complete the purchase.



Sync Trusted Connection licenses from Apple Business Manager to Jamf Now

Integrating Jamf Now with Apple’s volume purchasing allows you to distribute Trusted Connection directly to devices for managed distribution.

- **Step 1:** Log in to Jamf Now.
- **Step 2:** Click **More Settings**.
- **Step 3:** Click **Apps**.
- **Step 4:** Select **device-based** app assignment under App License Assignment Type.
- **Step 5:** Click **Save Settings**.
- **Step 6:** Click on **Apps** under the main “Manage” heading and click on the (...) in the top right-hand side of the screen and select “Sync Volume Purchased Apps”.



After updating your license assignment type, it may affect the number of licenses needed for your devices. Jamf Now will display the number of licenses needed for Trusted Connection. If you do not have enough licenses, you will need to purchase additional licenses from Apple and Trusted Connection subscriptions from Verizon.

Assign Trusted Connection to a blueprint

After configuring a blueprint with Trusted Connection, you can assign devices to that blueprint to deploy Trusted Connection Client to those devices. Any time you assign a device to this blueprint, the device will receive all the applications including Trusted Connection from that blueprint. Any time you update the settings in a blueprint, the changes will be applied to all devices linked to that blueprint.

As a reminder, a device will always be associated with only one blueprint. If you have more than one blueprint, you can use a blueprint's unique URL to navigate directly to that configuration. Blueprints can also be preassigned to devices enrolled with Automated Device Enrolment associated with your Jamf Now account. This can be completed before a device enrolled with Automated Device Enrolment is turned on. If users manually remove these apps including Trusted Connection, then the apps will automatically be reinstalled on devices when devices sync with Jamf Now.

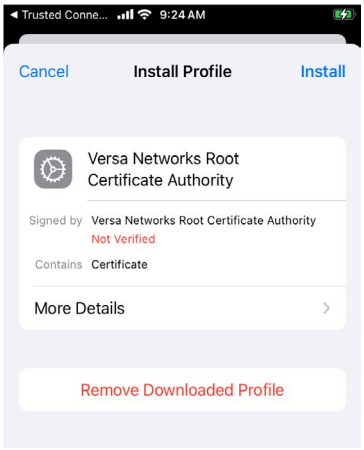
- **Step 1:** Log in to Jamf Now.
- **Step 2:** Click on **Blueprints**.
- **Step 3:** Select the blueprint you want to add Trusted Connection to.
- **Step 4:** Click on **Apps** inside the blueprint.
- **Step 5:** Click **Edit Apps**.
- **Step 6:** Find the Trusted Connection app you want to add to the blueprint by searching, filtering, or sorting apps. You can filter by device type, and sort alphabetically by app name, seller, or platform.
- **Step 7:** To automatically install apps on devices, select the **Install Automatically** checkbox next to Trusted Connection, or select all apps by selecting the **Install All Filtered Apps Automatically** or **Install All Apps Automatically** checkbox.
- **Step 8:** Click **Save Changes**.

Please note that deselecting Install Automatically removes installed apps on devices in the blueprint via Remove Application commands in Jamf Now, and removes associated app data saved locally on devices.

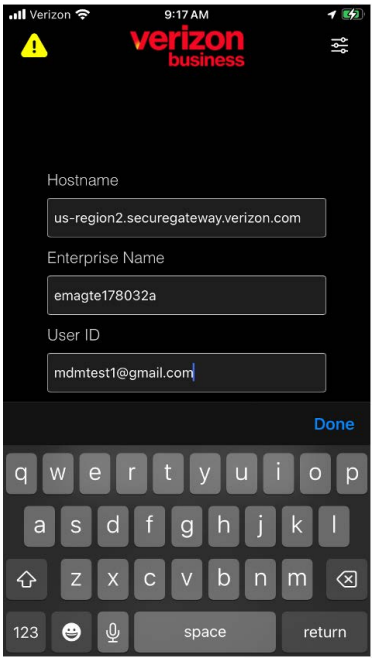
Steps for customer end-users

Jamf Now can push out the Trusted Connection Clients to devices, but it doesn't support a managed configuration. This means that end-users will need to complete the configuration of the Client to work with the Trusted Connection service. Here are the instructions for an end-user:

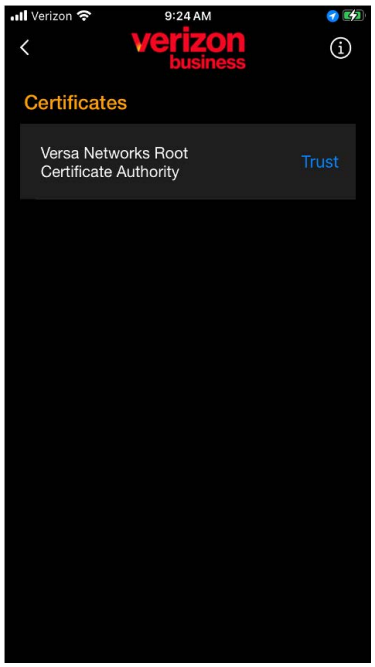
- **Step 1:** Open the Trusted Connection Client on your device. You will be presented with a "**Privacy Policy**" screen. Please select "**Agree**".
- **Step 2:** You will then be presented with "Trusted Connection would like to find and connect to devices on your local network". Please select "Allow".
- **Step 3:** You will now be presented with the following notice "**This website is trying to download a configuration profile. Do you want to allow this?**" Please select "**Allow**". Once downloaded, you will see a screen saying "**Kindly install the certificates to continue**." You will then be automatically taken to settings, where you will see the "**Profile Downloaded**."
- **Step 4:** Please click on "**Profile Downloaded**" and click install the "**Versa Network Root Certificate Authority**". Please click on "**Install**" and once completed "**Done**".



- **Step 5:** Please go back to the Trusted Connection Client and click on the yellow warning triangle in the top left-hand corner.



- **Step 6:** Please select "**Trust**" for the "**Versa Network Root Certificate Authority**" and hit the back button.



- **Step 7:** Set the Hostname, Enterprise Name and input your User ID and click "**Done**" followed by "**Submit**". The Hostname and Enterprise name will be provided to you by your company Admin e.g.:

  Hostname: us-region2.securegateway.verizon.com (please do not use, this is an example only).
  Enterprise Name: emagte178032a (please do not use, this is an example only).

  You will now be taken to your companies Identify Platform (IdP) where you'll be asked for your Username and Password.

- **Step 8:** Once you've successfully logged into your company's IdP platform, please click "**Allow"** to enable Trusted Connection to send you notifications and select "Allow" to permit Trusted Connection to "**Add a VPN Configuration**". Finally, turn on "Location Services" using the "Settings" link.
- **Step 9:** Please go back to the Trusted Connection Client and finally click the "**big red power button**" and you will now be connected to Verizon's Trusted Connection service.