Quick reference guide

Jamf Pro MDM: Trusted Connection Customer Admin and End-user Setup Steps

verizon business

Contents

Summary

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

- Trusted Connection is supported on the following four operating systems: iOS, Android, macOS and Windows. Please note that Jamf Pro 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 Pro.

3. App Configuration for Mobile Devices.

Steps for Customer End-Users:

4. Install the "Versa Network Root Certificate Authority".

5. Login to your company's IdP.

6. Connect the device to Verizon's Trusted Connection service.

Steps to Deploy Trusted Connection on Jamf Pro Managed Devices

Jamf Pro 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

To install apps and books on devices, Jamf Pro includes two distribution methods:

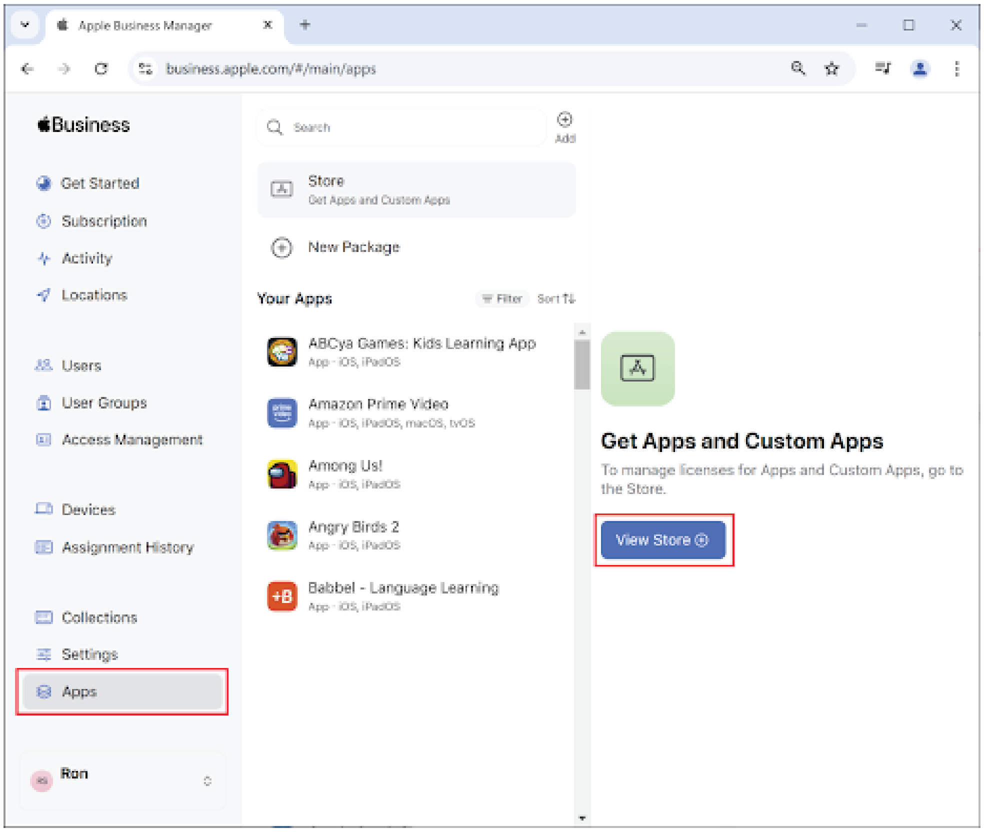
- Make Available in Jamf Self Service
- Install automatically/prompt users to install

Given the nature and purpose of Trusted Connection, Verizon strongly recommends that Administrators use the second option to install the Trusted Connection Client automatically. Automatic installation of the Trusted Connection Client can only occur if the endpoint device is supervised, and a license has been assigned to the device.

Trusted Connection supports a number of key-values that can be used in Jamf-managed apps so it can be configured specifically for your organization. This way you can use Jamf Pro to configure Trusted Connection before distributing it to mobile devices. In this document, we have provided you with the instructions needed to achieve this.

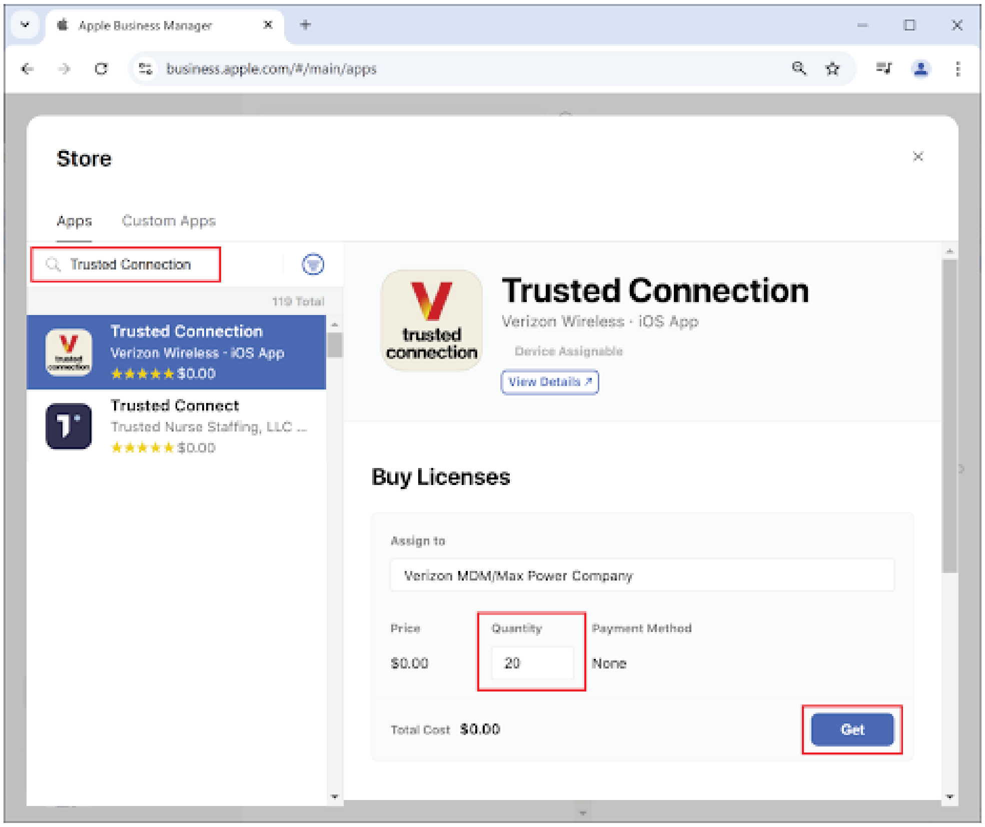
Purchase Trusted Connection Client Licenses in Apple Business Manager

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



To manage licenses for Apps and Custom Apps, go to the 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



Trusted Connection

Verizon Wireless · iOS App

Buy Licenses

Assign to: Verizon MDM/Max Power Company

Price: $0.00

Quantity: 20

Payment Method: None

Total Cost: $0.00

Sync Trusted Connection Licenses from Apple Business Manager to Jamf Pro

Apps you purchase in Apple Business Manager sync with Jamf Pro. You can then configure the app's distribution settings, and add devices to the app scope. Keep the following in mind about device-assigned managed distribution:

- If the Trusted Connection Client is assigned directly to a device, it does do not require the use of an end-user Apple Account.
- End-users with multiple managed devices require multiple licenses.

Jamf Pro allows you to distribute the Trusted Connection Client purchased in volume to computers and mobile devices. After the Client has been distributed, you can use Jamf Pro to manage future updates.

To distribute the Trusted Connection Client, add the app to Jamf Pro and then configure app settings and scope to distribute it to target devices.

- **Step 1:** In Jamf Pro, click **Computers** or **Devices** in the sidebar.
- **Step 2:** Click **Mac Apps** or **Mobile Device Apps** in the sidebar.
- **Step 3:** Click **New**.
- **Step 4:** For mobile devices only - **select apps purchased in volume** and click **Next**.
- **Step 5:** Enter Trusted Connection, and choose the U.S. App Store or region and click **Next**. Then click **Add**.
- **Step 6:** Use the **General pane** to configure settings for the app, including the distribution method. Select distributing the Trusted Connection to mobile devices, and **select to make the app managed**.
- **Step 7:** Click the Scope tab and configure the scope for Trusted Connection. Scope gives you granular control over which computers and mobile devices will receive the Trusted Connection Client.
- **Step 8:** To distribute the Trusted Connection Client directly to computers or mobile devices via managed distribution click the Managed Distribution tab, and then click the Device Assignments tab then:
  - Computers only - Select the **Assign Volume Content** checkbox.
  - Mobile devices only - Select the **Assign Content Purchased in Volume** checkbox.
  - Then choose the location that has purchased the app.

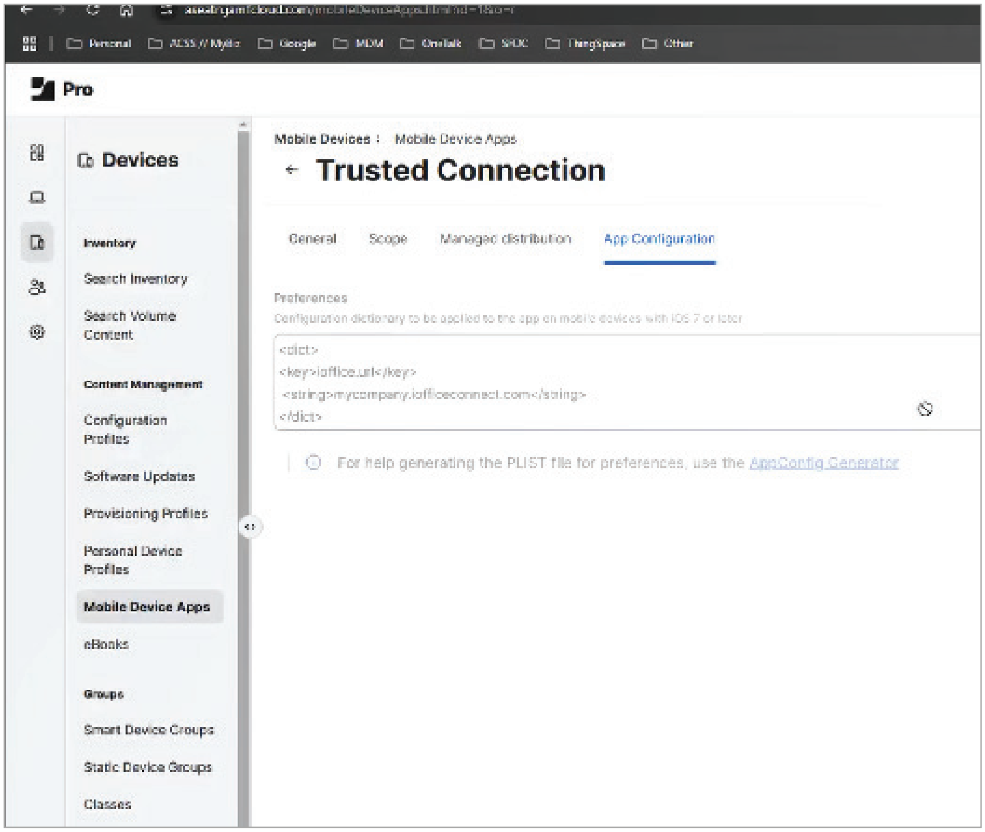
App Configuration for Mobile Devices

Device assigned managed distribution assigns apps directly to managed devices using Jamf Pro. This method is recommended for institutionally owned devices enrolled via Automated Device Enrollment or Device Enrollment. Please note, that the **App Configuration** tab is only displayed if the **Make App Managed when possible**, checkbox is selected.

- **Step 1:** In Jamf Pro, click **Computers** or **Devices** in the sidebar.
- **Step 2:** Click **Mac Apps** or **Mobile Device Apps** in the sidebar.
- **Step 3:** Click on **Trusted Connection** and select the **App Configuration** tab.
- **Step 4:** Find the **Fully Qualified Domain Name** (FQDN) and **Enterprise Name** details from your Trusted Connection portal.
- **Step 5:** Then in the Preferences box, please copy and paste the following managed configuration text replacing **%CustomToken_TC_fqdn%** with your **fqdn** details and **%CustomToken_TC_enterprise_name%** with the enterprise name as list in the Trusted Connection portal.

```
<dict>
<key>fqdn</key>
<string>%CustomToken_TC_fqdn%</string>
<key>enterprise_name</key>
<string>%CustomToken_TC_enterprise_name%</string>
<key>managed_device</key>
<true/>
</dict>
```

- **Step 6:** Then click **Save**.



← Trusted Connection

Preferences

Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

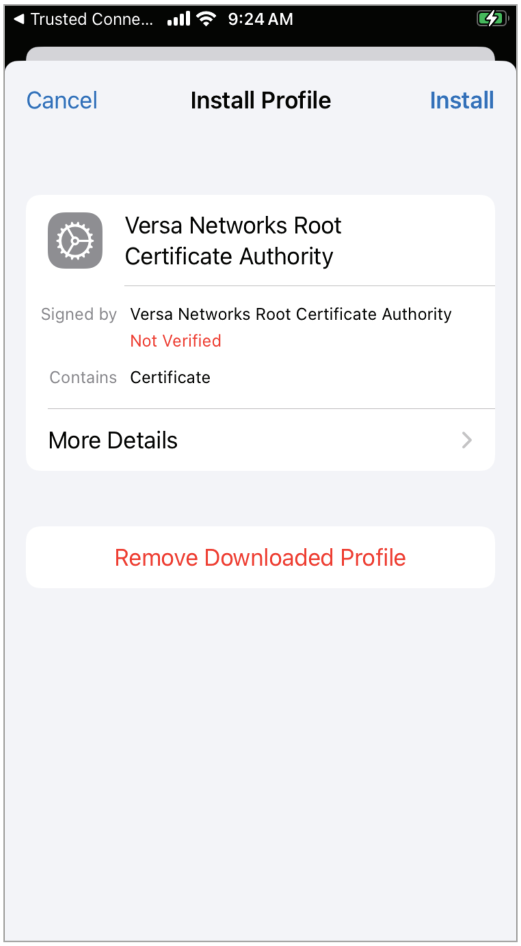
```
<dict>
<key>iofflice.url</key>
<string>mycompany.iofficeconnect.com</string>
</dict>
```

For help generating the PLIST file for preferences, use the AppConfig Generator

Steps for Customer End-Users

Jamf Pro can push out a preconfigured Trusted Connection Client to devices. However, 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.
- **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"**.
- **Step 4:** Please exit the App and go to settings, where you will see the **"Profile Downloaded."**
- **Step 5:** Please click on **"Profile Downloaded"** and click install the **"Versa Network Root Certificate Authority"**. Please click on **"Install"** and **"Install"** again, once completed click on **"Done"**.

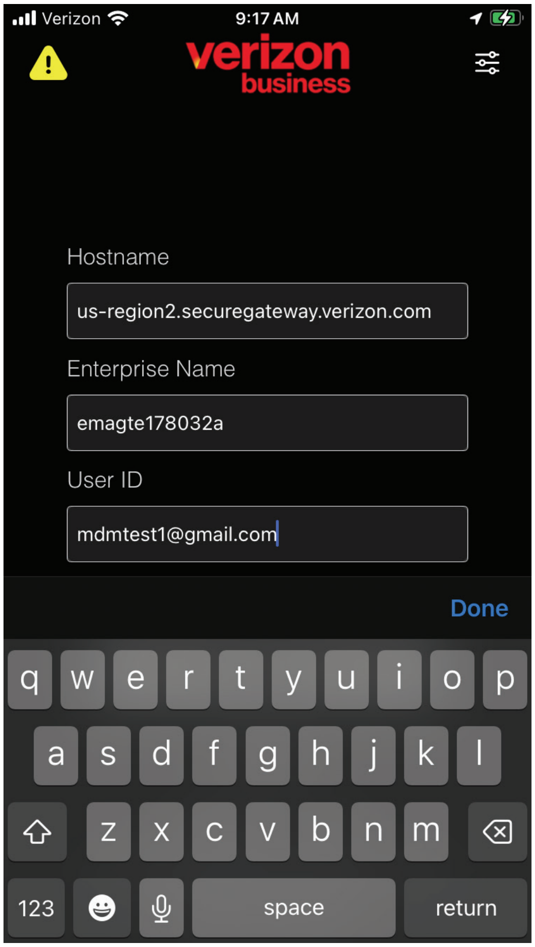


Versa Networks Root Certificate Authority

Signed by Versa Networks Root Certificate Authority
Not Verified

Contains Certificate

- **Step 6:** Please go back to the Trusted Connection Client and if you're presented with a bank screen, click **"Done"**, then click on the yellow warning triangle in the top left-hand corner.



Hostname

us-region2.securegateway.verizon.com

Enterprise Name

emagte178032a

User ID

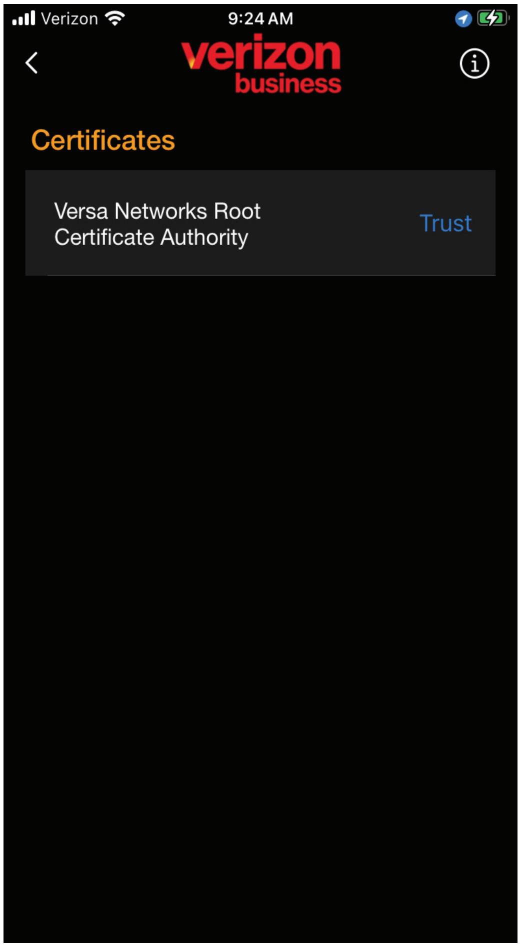
mdmtest1@gmail.com

- **Step 7:** Please select "Trust" for the "Versa Network Root Certificate Authority" and move the slider to the right, and then select "Continue". Please then go back to the Trusted Connection Client.

- **Step 8:** Put in your User ID (username) into the field and click **“Submit”**. You will now be taken to your companies Identify Platform (IdP) where you’ll be asked for your Username and Password.

- **Step 9:** 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 10:** 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.



Verizon 9:24 AM

Certificates

Versa Networks Root Certificate Authority Trust