MAGTEK®
SECURITY FROM THE INSIDE

DYNAPRO GO TLS CERTIFICATE

PIN Encryption Devices
Installation Manual

September 2018

Document Number:
D998200279-10

REGISTERED TO ISO 9001:2015

MagTek I 1710 Apollo Court I Seal Beach, CA 90740 I Phone: (562) 546-6400 I Technical Support: (888) 624-8350
www.magtek.com

Table 0-1 - Revisions

Rev Number	Date	Notes
10	September 2018	Initial Release

SOFTWARE LICENSE AGREEMENT

IMPORTANT: YOU SHOULD CAREFULLY READ ALL THE TERMS, CONDITIONS AND RESTRICTIONS OF THIS LICENSE AGREEMENT BEFORE INSTALLING THE SOFTWARE PACKAGE. YOUR INSTALLATION OF THE SOFTWARE PACKAGE PRESUMES YOUR ACCEPTANCE OF THE TERMS, CONDITIONS, AND RESTRICTIONS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, CONDITIONS, AND RESTRICTIONS, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ASSOCIATED DOCUMENTATION TO THE ADDRESS ON THE FRONT PAGE OF THIS DOCUMENT, ATTENTION: CUSTOMER SUPPORT.

TERMS, CONDITIONS, AND RESTRICTIONS

MagTek, Incorporated (the "Licensor") owns and has the right to distribute the described software and documentation, collectively referred to as the "Software."

LICENSE: Licensor grants you (the "Licensee") the right to use the Software in conjunction with MagTek products. LICENSEE MAY NOT COPY, MODIFY, OR TRANSFER THE SOFTWARE IN WHOLE OR IN PART EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. Licensee may not decompile, disassemble, or in any other manner attempt to reverse engineer the Software. Licensee shall not tamper with, bypass, or alter any security features of the software or attempt to do so.

TRANSFER: Licensee may not transfer the Software or license to the Software to another party without the prior written authorization of the Licensor. If Licensee transfers the Software without authorization, all rights granted under this Agreement are automatically terminated.

COPYRIGHT: The Software is copyrighted. Licensee may not copy the Software except for archival purposes or to load for execution purposes. All other copies of the Software are in violation of this Agreement.

TERM: This Agreement is in effect as long as Licensee continues the use of the Software. The Licensor also reserves the right to terminate this Agreement if Licensee fails to comply with any of the terms, conditions, or restrictions contained herein. Should Licensor terminate this Agreement due to Licensee's failure to comply, Licensee agrees to return the Software to Licensor. Receipt of returned Software by the Licensor shall mark the termination.

LIMITED WARRANTY: Licensor warrants to the Licensee that the disk(s) or other media on which the Software is recorded are free from defects in material or workmanship under normal use.

THE SOFTWARE IS PROVIDED AS IS. LICENSOR MAKES NO OTHER WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Because of the diversity of conditions and PC hardware under which the Software may be used, Licensor does not warrant that the Software will meet Licensee specifications or that the operation of the Software will be uninterrupted or free of errors.

IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, OR INABILITY TO USE, THE SOFTWARE. Licensee's sole remedy in the event of a defect in material or workmanship is expressly limited to replacement of the Software disk(s) if applicable.

GOVERNING LAW: If any provision of this Agreement is found to be unlawful, void, or unenforceable, that provision shall be removed from consideration under this Agreement and will not affect the enforceability of any of the remaining provisions. This Agreement shall be governed by the laws of the State of California and shall inure to the benefit of MagTek, Incorporated, its successors or assigns.

ACKNOWLEDGMENT: LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS, AND RESTRICTIONS, AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL VERBAL AND WRITTEN COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

QUESTIONS REGARDING THIS AGREEMENT SHOULD BE ADDRESSED IN WRITING TO MAGTEK, INCORPORATED, ATTENTION: CUSTOMER SUPPORT, AT THE ADDRESS LISTED IN THIS DOCUMENT, OR E-MAILED TO SUPPORT@MAGTEK.COM.

Table of Contents

1 Introduction

This document provides instructions for downloading and installing DynaPro Go TLS certificates.

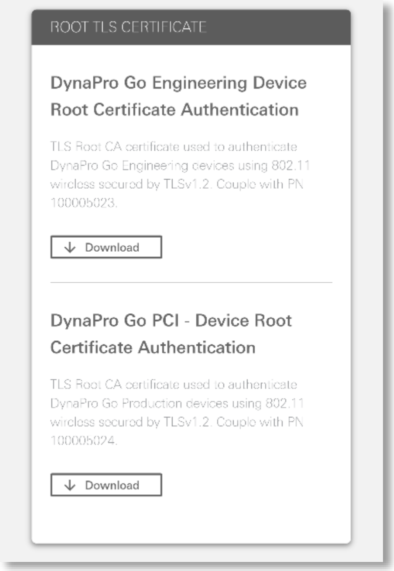
The TLS Root and TLS Client certificates provided from the download links are the same for different operating systems, but this document instructions are partitioned into respective operating systems for clarity. Further, the instructions are segmented for two types of MagTek devices, Demo and Production.

2 Android Instructions

2.1 Download and Install Root TLS Certificate

This section details the steps to download and install the Root TLS certificate. The Root TLS certificate is categorized into either Demo or Production. The Demo Root TLS certificate is valid for Demo devices, whereas the Production Root TLS certificates is valid for Production devices.

1) On the target Android device, launch the Chrome browser and navigate to: https://www.magtek.com/support/dynapro-go?tab=software
2) Scroll down to the **Root TLS Certificate** section.



ROOT TLS CERTIFICATE

DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

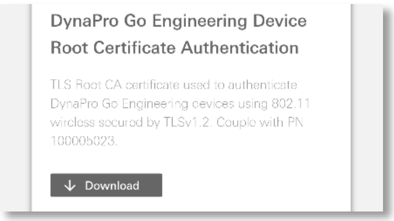
DynaPro Go PCI - Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Production devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005024.

2.1.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

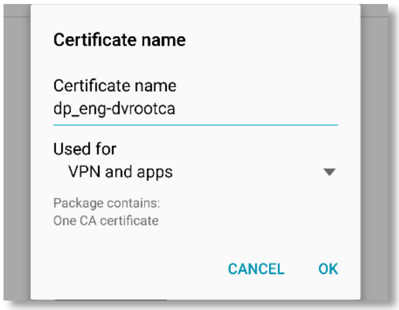
1) Touch download button under **Root TLS Certificate -> DynaPro Go Engineering Device Root Certificate Authentication**.



DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

2) Enter passcode or set up passcode if you don't have one, then press Next button.
3) Enter prefer certificate name, then select VPN and apps under Used for, then press OK button.



Certificate name

Certificate name
dp_eng-dvrootca

Used for
VPN and apps

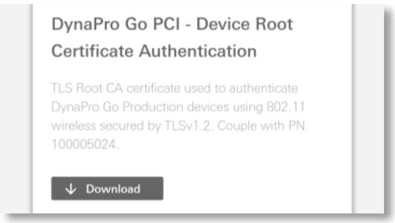
Package contains:
One CA certificate

4) The device will display message that the certificate installed.

2.1.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

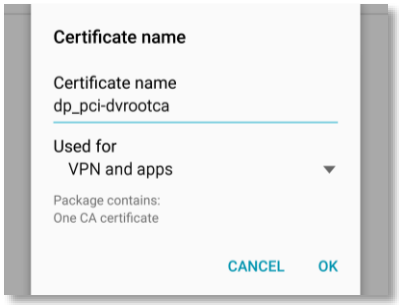
1) Touch download button under **Root TLS Certificate → DynaPro Go PCI - Device Root Certificate Authentication**



DynaPro Go PCI - Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Production devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005024.

2) Enter passcode or set up passcode if you don't have one, then press Next button.
3) Enter prefer certificate name, then select VPN and apps under Used for, then press OK button.



Certificate name

Certificate name
dp_pci-dvrootca

Used for
VPN and apps

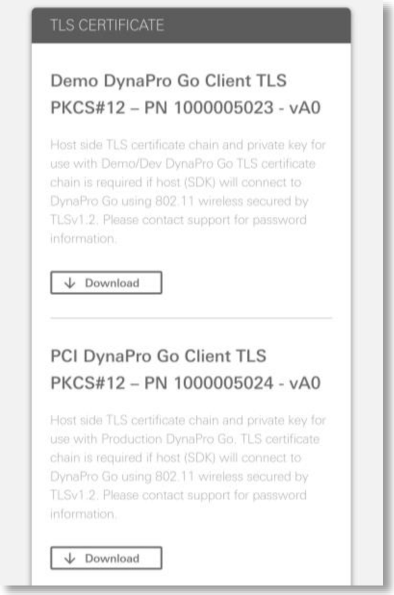
Package contains:
One CA certificate

4) The device will display message that the certificate installed.

2.2 Download Client TLS Certificate

This section details the steps to download and install the Client TLS certificate. The Client TLS certificate is categorized into either Demo or Production. The Demo Client TLS certificate is valid for Demo devices, whereas the Production Client TLS certificates is valid for Production devices.

1) Launch the browser and navigate to https://www.magtek.com/support/dynapro-go?tab=software
2) Scroll down to the TLS Certificate section.



TLS CERTIFICATE

Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

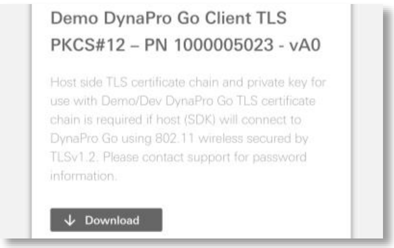
PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2.2.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

1) Touch the download button under **Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023.** The certificate password is “`password`” without the quotes.



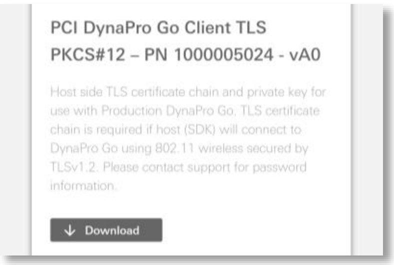
Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2.2.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

1) Touch the download button the **Production DynaPro Go Client TLS PKCS#12 – PN 1000005024**



PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2) Contact MagTek Support at support@magtek.com to obtain client certificate password from MagTek customer service if you have Production DynaPro Go.
3) Copy the certificate file you downloaded to your project and use the password you got from MagTek support to build your application.

2.3 Using the TLS Client Certificate

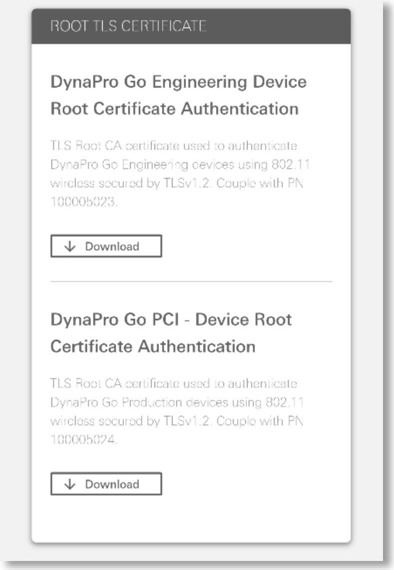
1) Put the client certificate in to the Android Studio Project. Before connecting to the device in wireless mode, load the TLS client certificate for the device instance by calling the SDK function loadClientCertificate().

3 iOS Instructions

3.1 Download and Install Root TLS Certificate

This section details the steps to download and install the Root TLS certificate. The Root TLS certificate is categorized into either Demo or Production. The Demo Root TLS certificate is valid for Demo devices, whereas the Production Root TLS certificates is valid for Production devices.

1) On the target iOS device, launch the Safari browser and navigate to: https://www.magtek.com/support/dynapro-go?tab=software
2) Scroll down to the **Root TLS Certificate** section.



ROOT TLS CERTIFICATE

DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

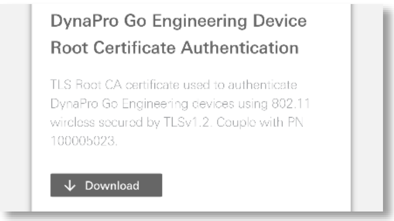
DynaPro Go PCI - Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Production devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005024.

3.1.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

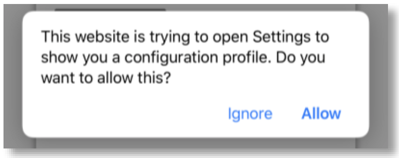
1) Touch the download button under **Root TLS Certificate → DynaPro Go Engineering Device Root Certificate Authentication**



DynaPro Go Engineering Device Root Certificate Authentication

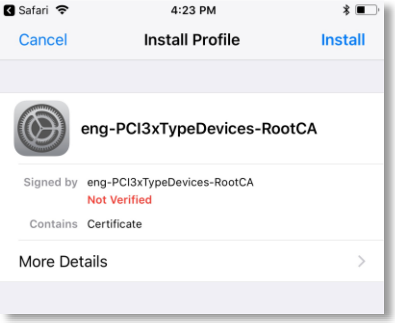
TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

2) Press on Allow if prompted.



This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

3) Press Install and enter the passcode.

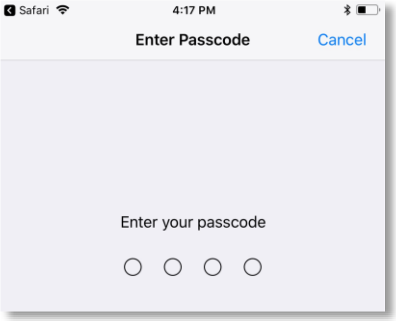


eng-PCI3xTypeDevices-RootCA

Signed by eng-PCI3xTypeDevices-RootCA

Not Verified

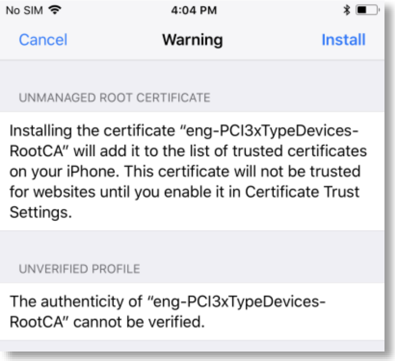
Contains Certificate



Enter your passcode

○ ○ ○ ○

4) At the Warning prompt, press Install 2 times to install the Demo root certificate into the iOS device.

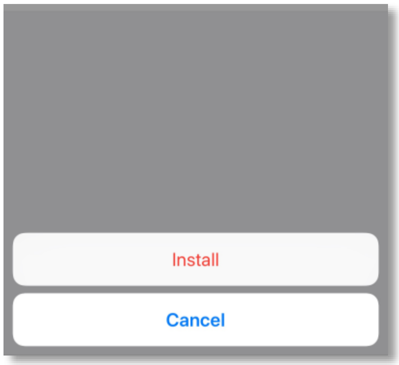


UNMANAGED ROOT CERTIFICATE

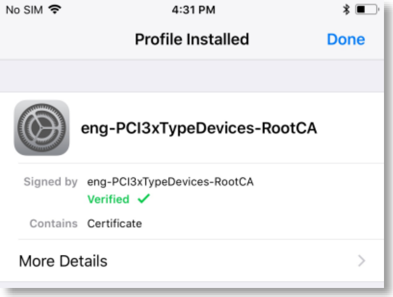
Installing the certificate "eng-PCI3xTypeDevices-RootCA" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

UNVERIFIED PROFILE

The authenticity of "eng-PCI3xTypeDevices-RootCA" cannot be verified.



5) Press Done to complete the installation.



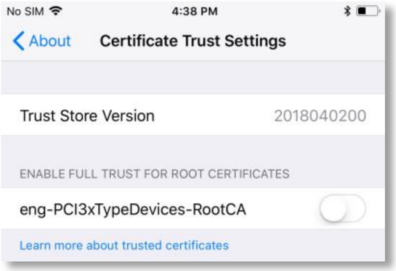
eng-PCI3xTypeDevices-RootCA

Signed by eng-PCI3xTypeDevices-RootCA

Verified ✓

Contains Certificate

6) Go to Settings → General → About → Certificate Trust Settings → ENALBE FULL TRUST FOR ROOT CERTIFICATES.



No SIM 4:38 PM

About Certificate Trust Settings

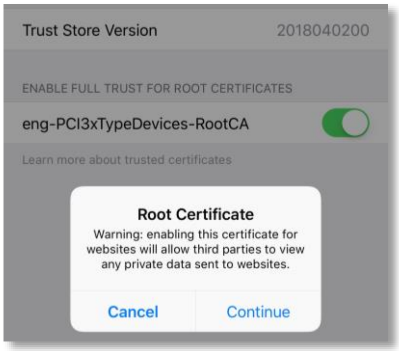
Trust Store Version 2018040200

ENABLE FULL TRUST FOR ROOT CERTIFICATES

eng-PCI3xTypeDevices-RootCA

Learn more about trusted certificates

7) Enable the trust for **eng-PCI3xTypeDevice-RootCA**, then press on Continue.



Trust Store Version 2018040200

ENABLE FULL TRUST FOR ROOT CERTIFICATES

eng-PCI3xTypeDevices-RootCA

Learn more about trusted certificates

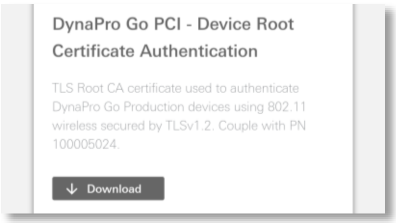
Root Certificate

Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

3.1.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

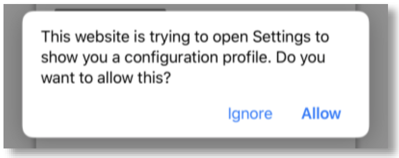
1) Touch the download button under **Root TLS Certificate** → **DynaPro Go PCI - Device Root Certificate Authentication**



DynaPro Go PCI - Device Root Certificate Authentication

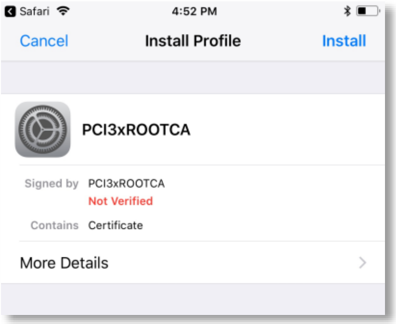
TLS Root CA certificate used to authenticate DynaPro Go Production devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005024.

2) Press on Allow if prompted.



This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

3) Press Install and enter the passcode.



Safari 4:52 PM

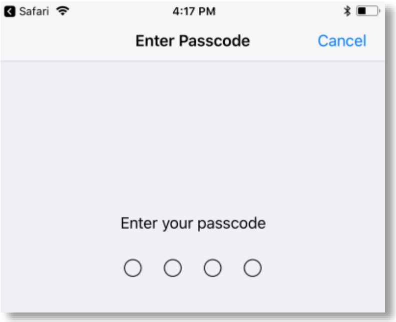
Cancel Install Profile Install

PCI3xROOTCA

Signed by PCI3xROOTCA
Not Verified

Contains Certificate

More Details



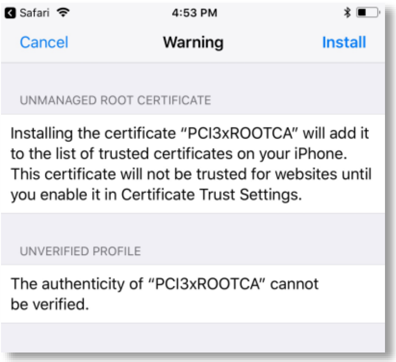
Safari 4:17 PM

Enter Passcode Cancel

Enter your passcode

○ ○ ○ ○

4) At the Warning prompt, press Install 2 times to install the Demo root certificate into the iOS device.



Safari 4:53 PM

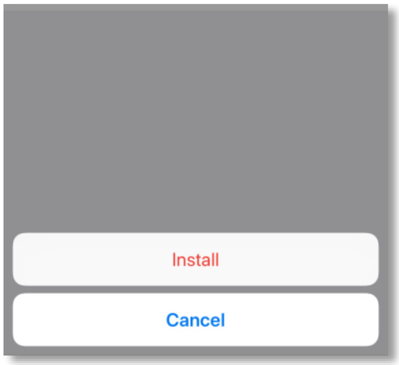
Cancel Warning Install

UNMANAGED ROOT CERTIFICATE

Installing the certificate "PCI3xROOTCA" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

UNVERIFIED PROFILE

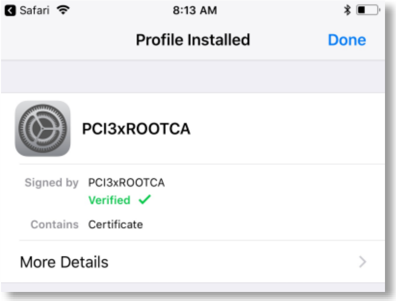
The authenticity of "PCI3xROOTCA" cannot be verified.



Install

Cancel

5) Press Done to complete the installation.



Safari 8:13 AM

Profile Installed Done

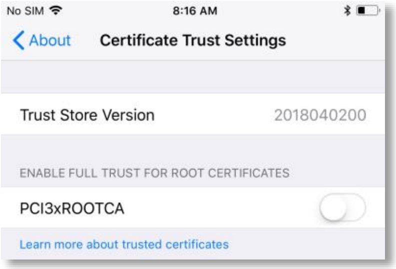
PCI3xROOTCA

Signed by PCI3xROOTCA
Verified ✓

Contains Certificate

More Details

6) Go to **Settings → General → About → Certificate Trust Settings →** ENALBE FULL TRUST FOR ROOT CERTIFICATES.



No SIM 8:16 AM

About Certificate Trust Settings

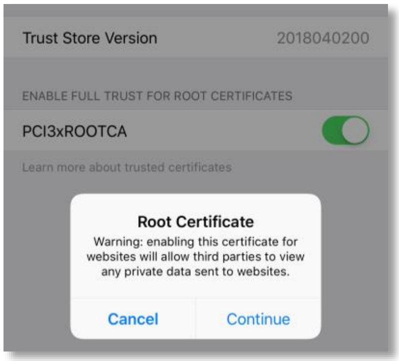
Trust Store Version 2018040200

ENABLE FULL TRUST FOR ROOT CERTIFICATES

PCI3xROOTCA

Learn more about trusted certificates

7) Enable the trust for **PCI3xRootCA**, then press on Continue.



Trust Store Version 2018040200

ENABLE FULL TRUST FOR ROOT CERTIFICATES

PCI3xROOTCA

Learn more about trusted certificates

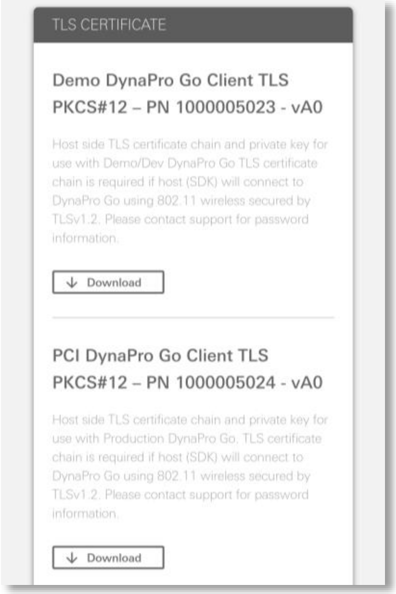
Root Certificate

Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

3.2 Download and Install TLS Client Certificate

This section details the steps to download and install the Client TLS certificate. The Client TLS certificate is categorized into either Demo or Production. The Demo Client TLS certificate is valid for Demo devices, whereas the Production Client TLS certificates is valid for Production devices.

1) Launch the browser and navigate to https://www.magtek.com/support/dynapro-go?tab=software
2) Scroll down to the **TLS Certificate** section.



TLS CERTIFICATE

Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

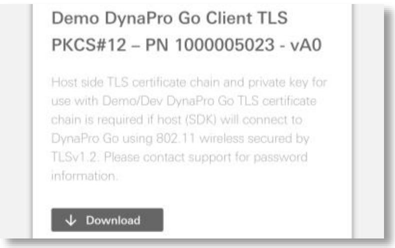
PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

3.2.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

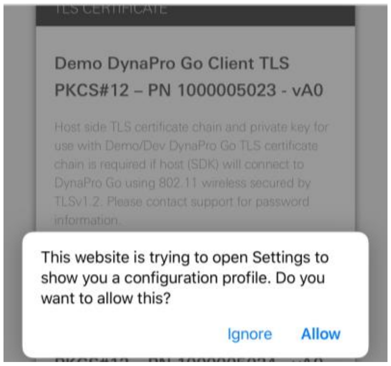
1) Touch the download button under **Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023.**



Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2) Press on Allow if prompted.

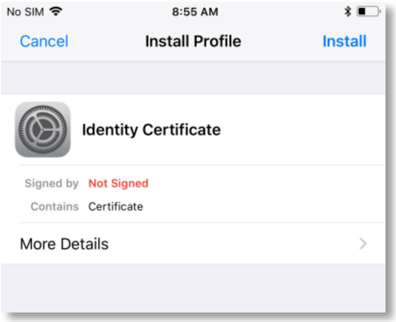


Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

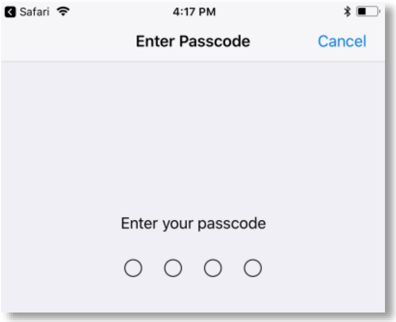
3) At the Install Profile screen, press Install and enter the passcode.



Identity Certificate

Signed by Not Signed

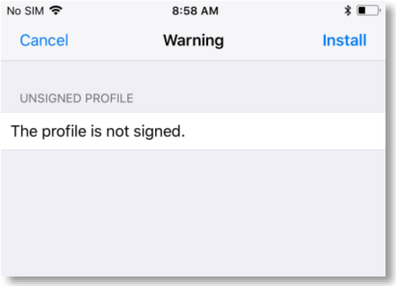
Contains Certificate



Enter your passcode

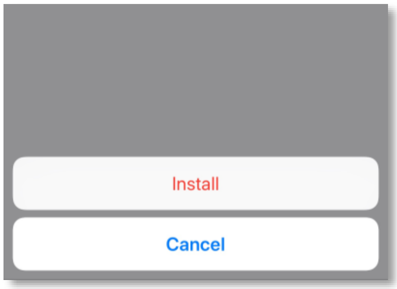
○ ○ ○ ○

4) At the Warning screen, press Install 2 times.

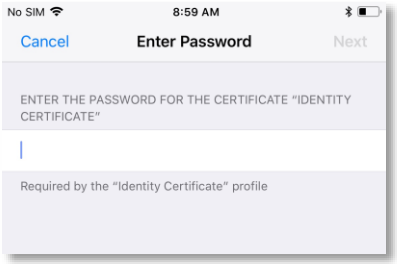


UNSIGNED PROFILE

The profile is not signed.

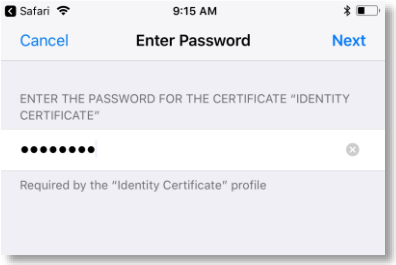


5) Enter the password “`password`” without the quotes for the certificate, press Next, and then press Done.



ENTER THE PASSWORD FOR THE CERTIFICATE "IDENTITY CERTIFICATE"

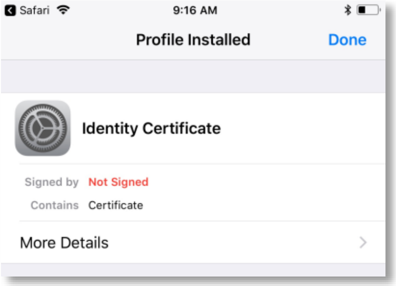
Required by the "Identity Certificate" profile



ENTER THE PASSWORD FOR THE CERTIFICATE "IDENTITY CERTIFICATE"

••••••••

Required by the "Identity Certificate" profile



Identity Certificate

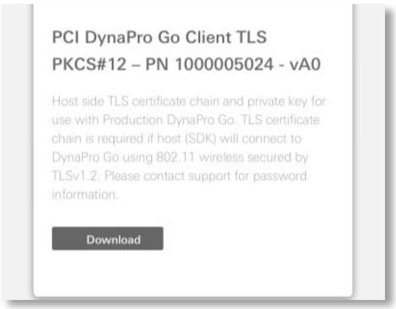
Signed by Not Signed

Contains Certificate

3.2.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

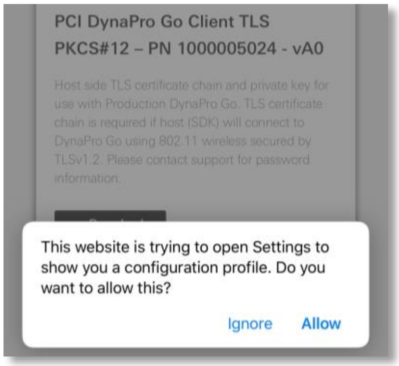
1) Touch the download button under **Production DynaPro Go Client TLS PKCS#12 – PN 1000005024.**



PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2) Press on Allow if prompted.

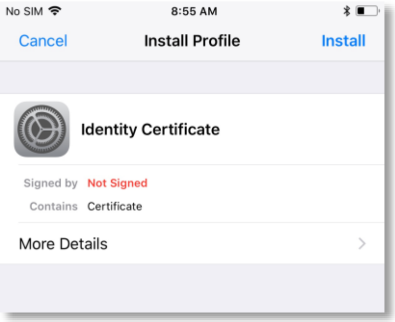


PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

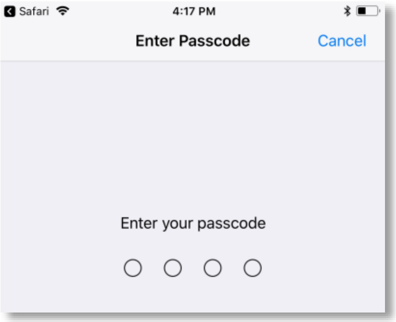
3) At the Install Profile screen, press Install and enter the passcode.



Identity Certificate

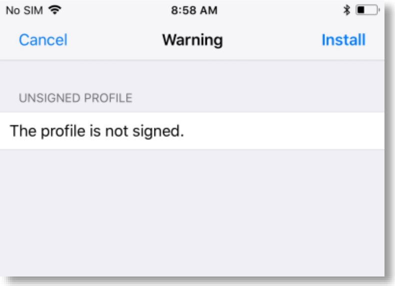
Signed by Not Signed

Contains Certificate



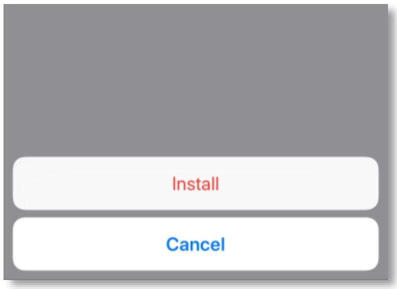
Enter your passcode

4) At the Warning screen, press Install 2 times.



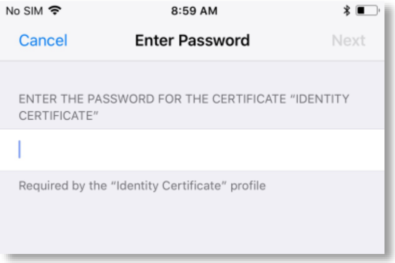
UNSIGNED PROFILE

The profile is not signed.



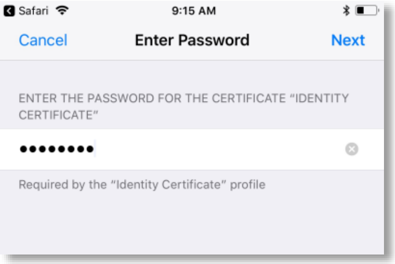
5) Contact MagTek Support at support@magtek.com to obtain client certificate password from MagTek customer service if you have Production DynaPro Go.

6) Enter the password for the certificate, press Next, and then press Done.



ENTER THE PASSWORD FOR THE CERTIFICATE "IDENTITY CERTIFICATE"

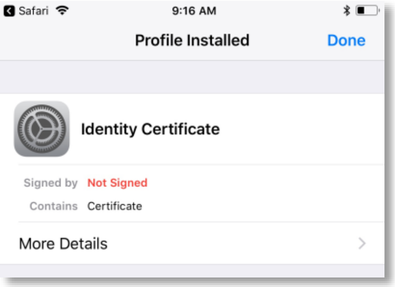
Required by the "Identity Certificate" profile



ENTER THE PASSWORD FOR THE CERTIFICATE "IDENTITY CERTIFICATE"

••••••••

Required by the "Identity Certificate" profile



Identity Certificate

Signed by Not Signed

Contains Certificate

3.3 Using the TLS Client Certificate

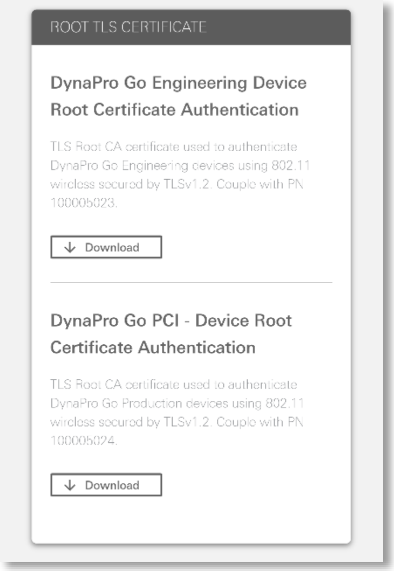
1) Put the client certificate in to the XCode Project. Before connecting to the device in wireless mode, load the TLS client certificate for the device instance by calling the SDK function loadClientCertificate().

4 Windows Instructions

4.1 Download and Install Root TLS Certificate

This section details the steps to download and install the Root TLS certificate. The Root TLS certificate is categorized into either Demo or Production. The Demo Root TLS certificate is valid for Demo devices, whereas the Production Root TLS certificates is valid for Production devices.

1) On the target Windows machine, launch a browser and navigate to: https://www.magtek.com/support/dynapro-go?tab=software
2) Scroll down to the **Root TLS Certificate** section.



ROOT TLS CERTIFICATE

DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

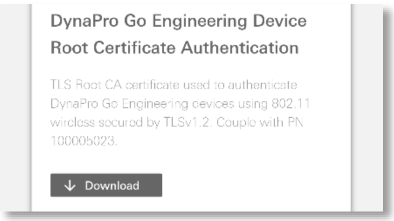
DynaPro Go PCI - Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Production devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005024.

4.1.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

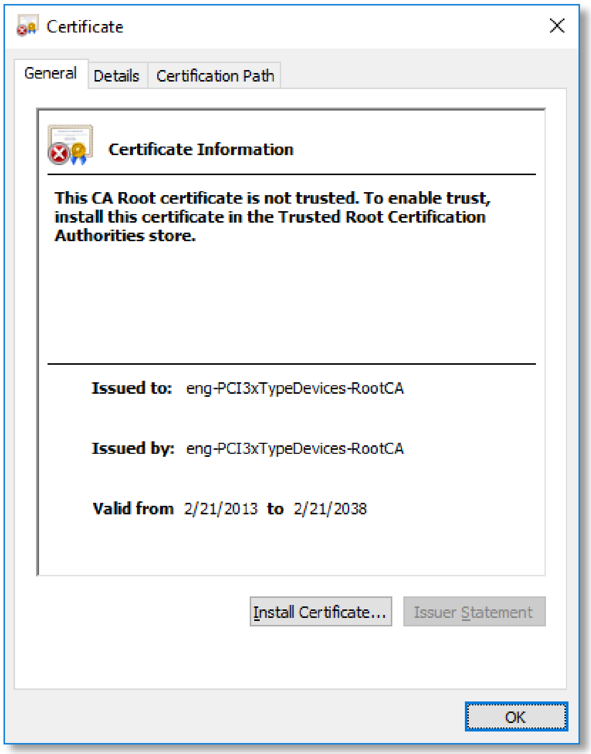
1) Touch the download button under **Root TLS Certificate** → **DynaPro Go Engineering Device Root Certificate Authentication**



DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

2) Save the downloaded file `dp_eng-dvrootca.cer` to the local computer.
3) Double click on the file `dp_eng-dvrootca.cer` to install the certificate, and then click the **Install Certificate** button.



Certificate

Certificate Information

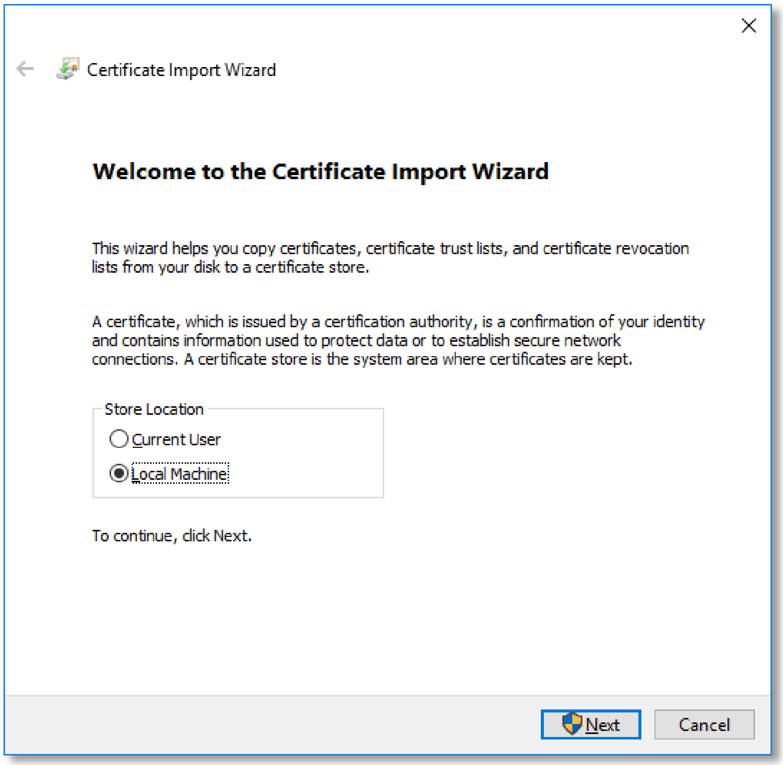
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: eng-PCI3xTypeDevices-RootCA

Issued by: eng-PCI3xTypeDevices-RootCA

Valid from 2/21/2013 to 2/21/2038

4) At the Certificate Import Wizard window, under Store Location, select **Local Machine**, and then click the **Next** button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

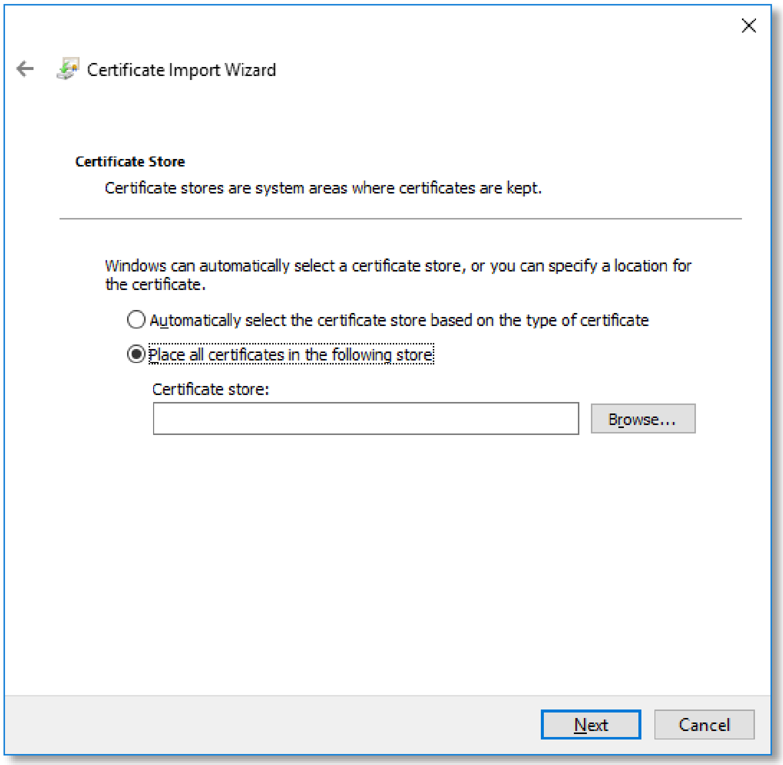
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

5) Select **Place all certificates in the follow store**, then click the **Browse** button.



Certificate Store

Certificate stores are system areas where certificates are kept.

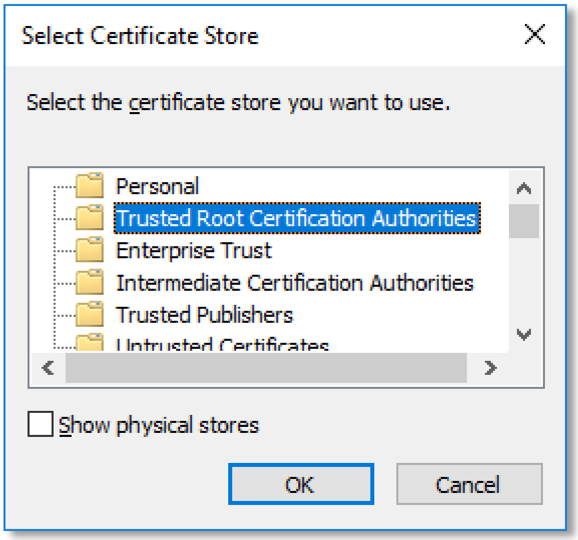
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

6) Select the store **Trusted Root Certification Authorities**., then click the **OK** button.

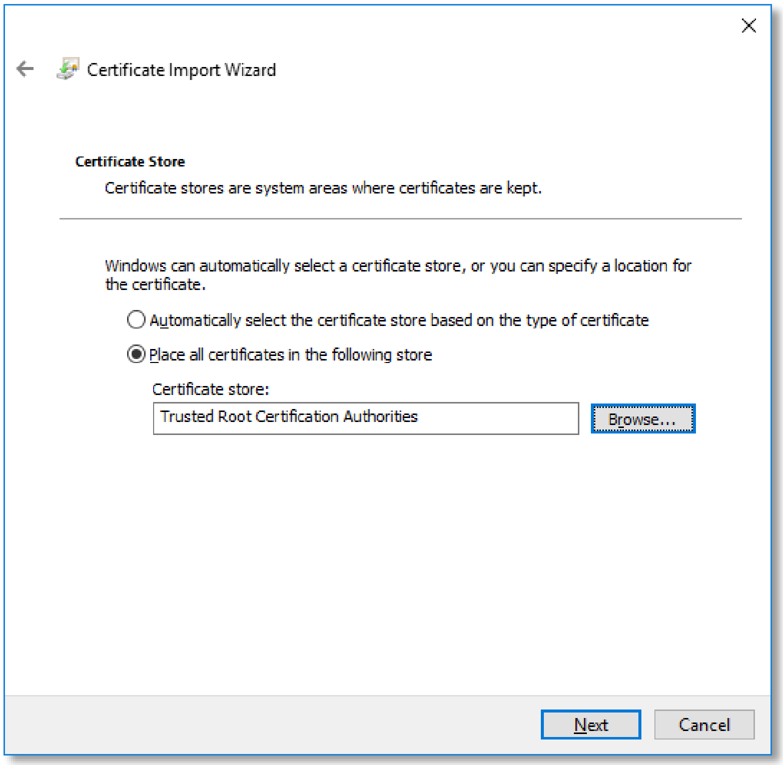


Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

□ Show physical stores

7) Click the **Next** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

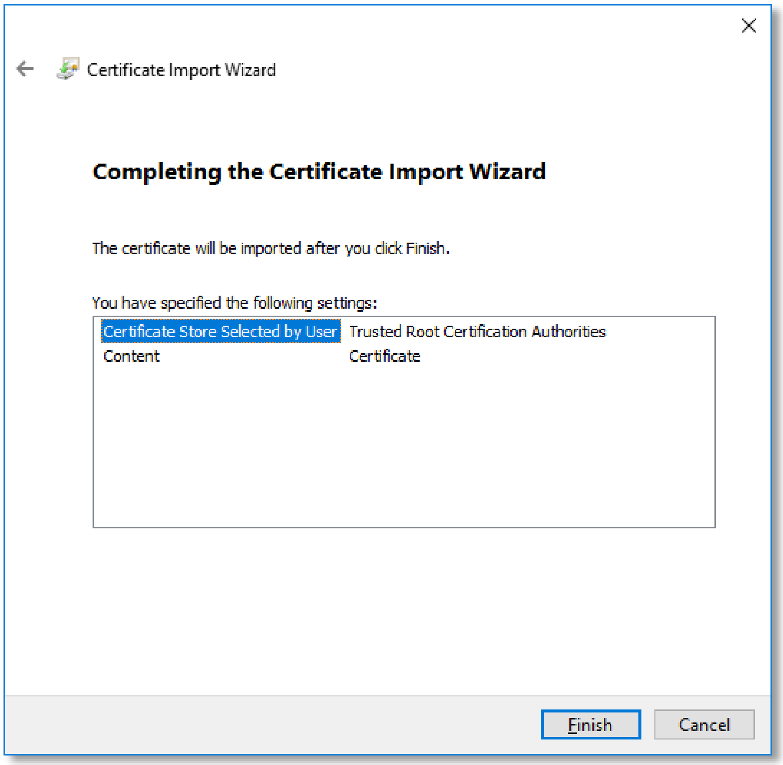
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

8) Click the **Finish** button and OK button to complete the certificate import.



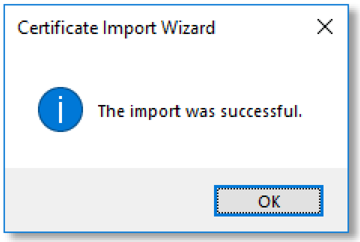
Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate



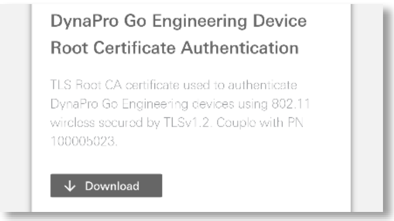
Certificate Import Wizard

The import was successful.

4.1.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

1) Touch the download button under **Root TLS Certificate** → **DynaPro Go PCI - Device Root Certificate Authentication**

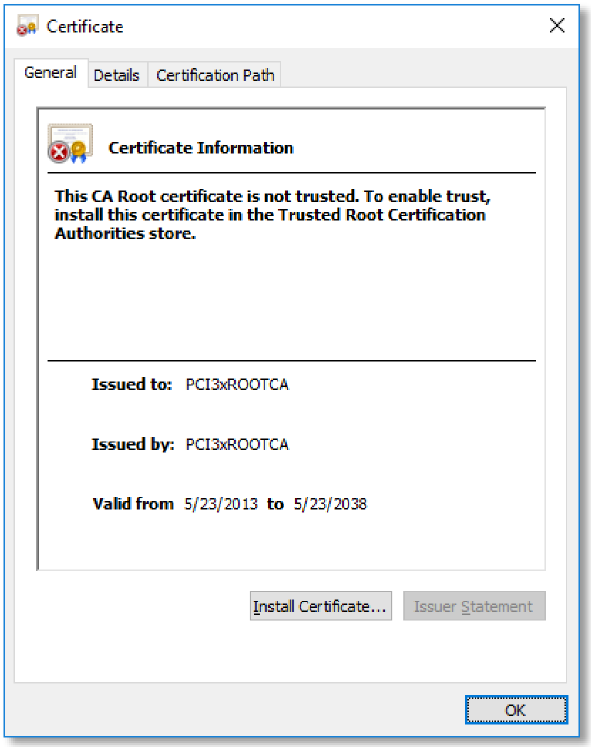


DynaPro Go Engineering Device Root Certificate Authentication

TLS Root CA certificate used to authenticate DynaPro Go Engineering devices using 802.11 wireless secured by TLSv1.2. Couple with PN 100005023.

2) Save the downloaded file `dp_pci-dvrootca.cer` to the local computer.

3) Double click on the file `dp_pci-dvrootca.cer` to install the certificate, and then click the **Install Certificate** button.



Certificate Information

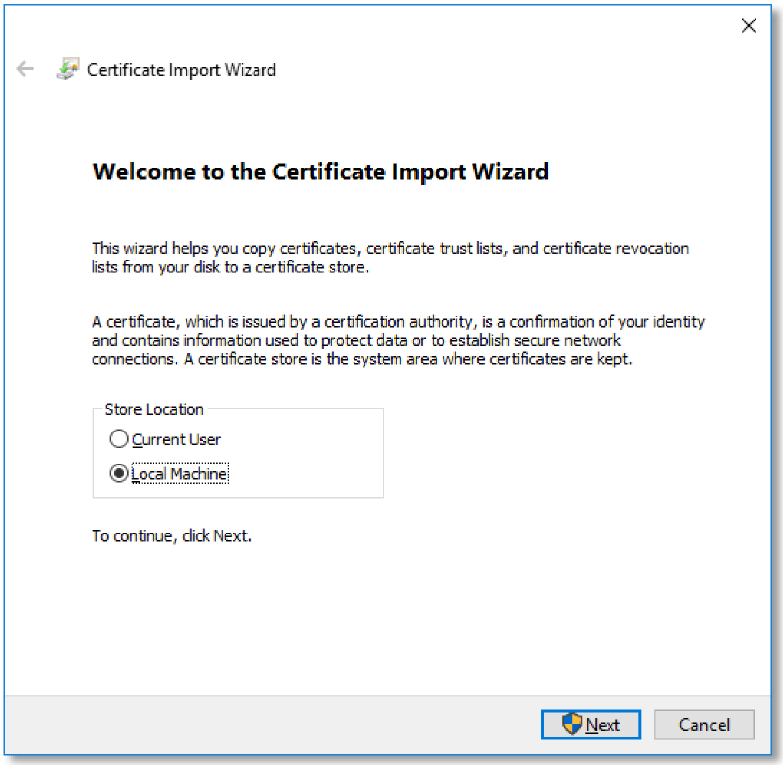
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: PCI3xROOTCA

Issued by: PCI3xROOTCA

Valid from 5/23/2013 to 5/23/2038

4) At the Certificate Import Wizard window, under Store Location, select **Local Machine**, and then click the **Next** button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

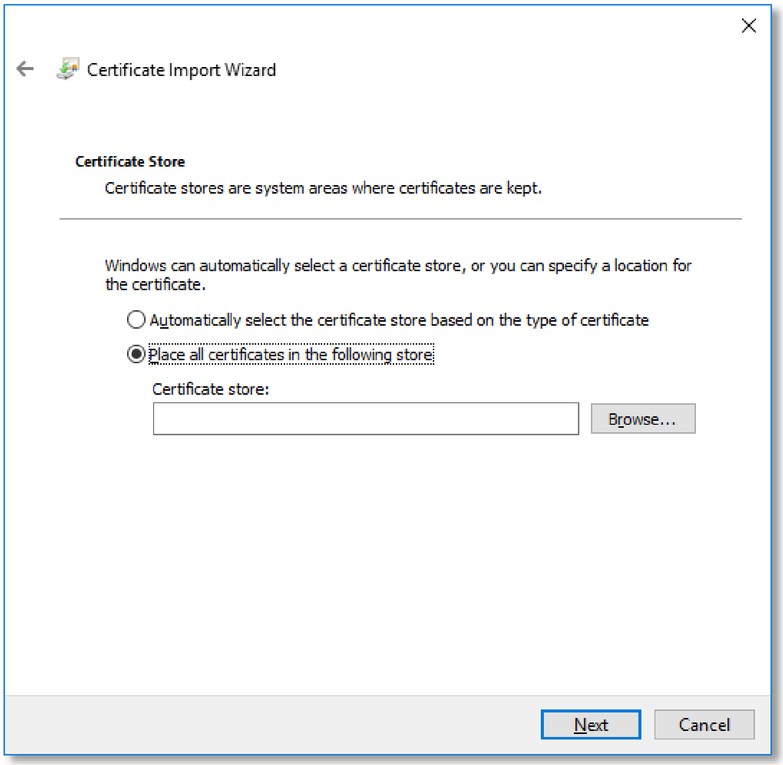
Store Location

○ Current User

● Local Machine

To continue, click Next.

5) Select **Place all certificates in the follow store**, then click the **Browse** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

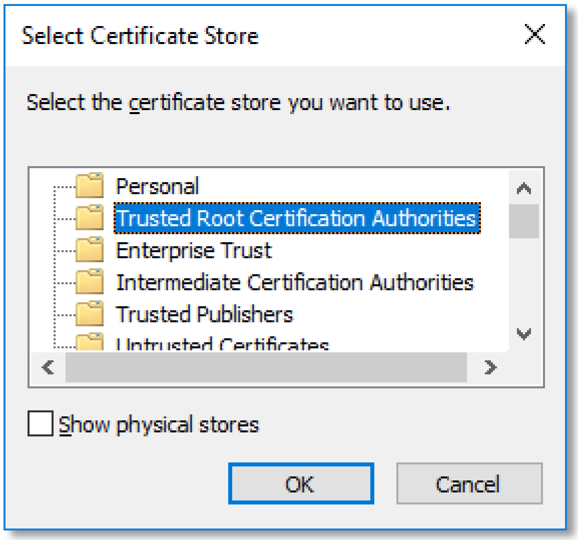
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

6) Select the store **Trusted Root Certification Authorities**., then click the **OK** button.



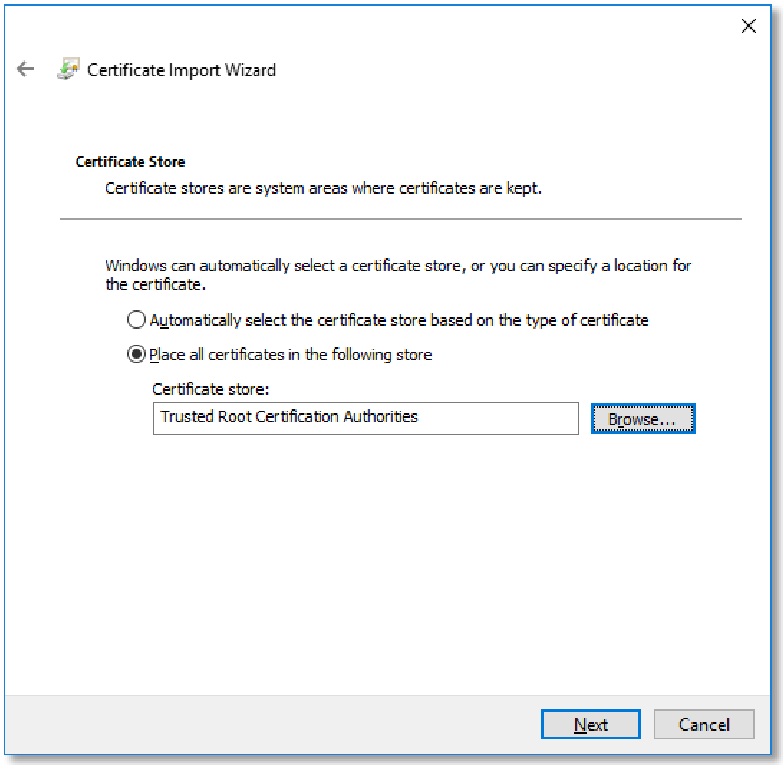
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

7) Click the **Next** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

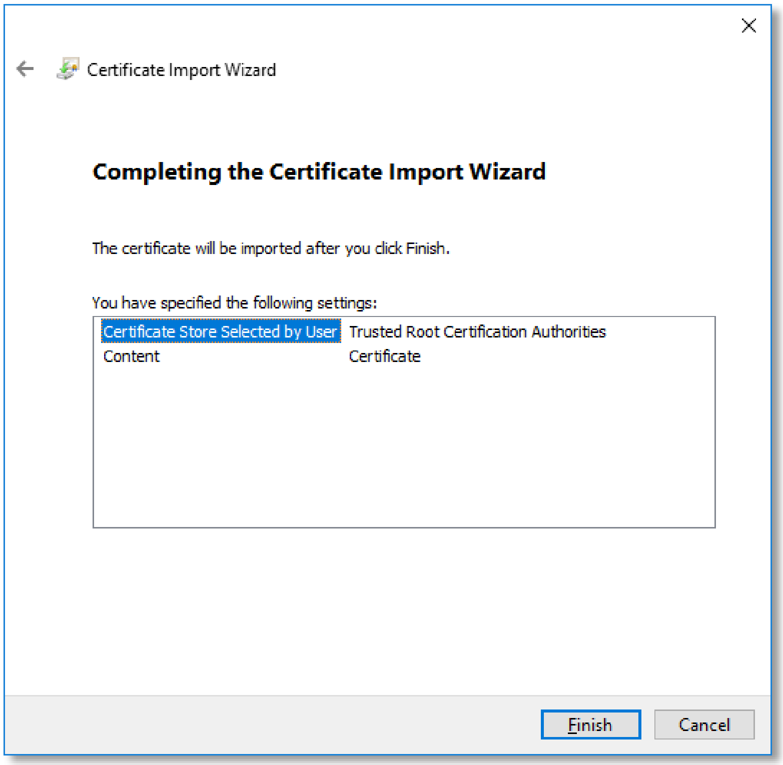
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

8) Click the **Finish** button and OK button to complete the certificate import.

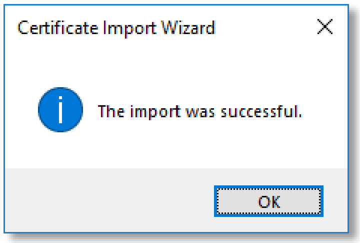


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

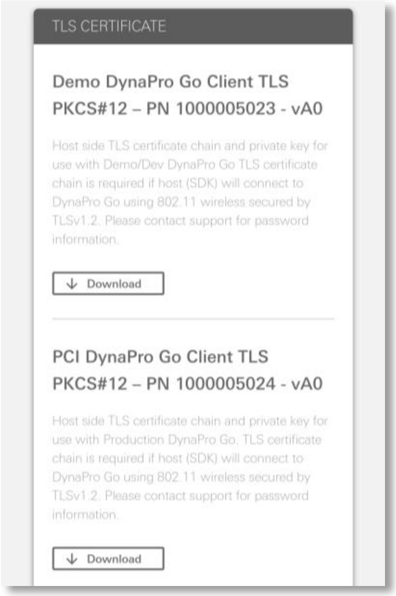


The import was successful.

4.2 Download and Install TLS Client Certificate

This section details the steps to download and install the Client TLS certificate. The Client TLS certificate is categorized into either Demo or Production. The Demo Client TLS certificate is valid for Demo devices, whereas the Production Client TLS certificates is valid for Production devices.

3) Launch the browser and navigate to https://www.magtek.com/support/dynapro-go?tab=software
4) Scroll down to the TLS Certificate section.



Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

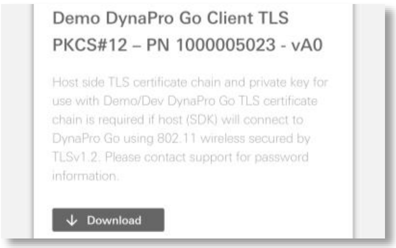
PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

4.2.1 Demo (Engineering)

Follow the instructions of this sub section only for Demo devices. If not using Demo devices, skip this subsection.

1) Touch the download button under **Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023.**



Demo DynaPro Go Client TLS PKCS#12 – PN 1000005023 - vA0

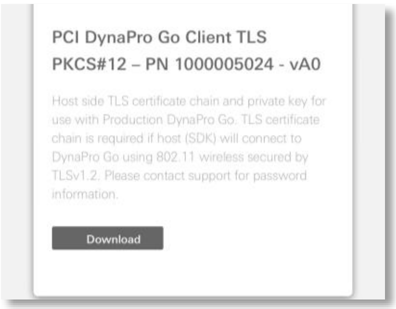
Host side TLS certificate chain and private key for use with Demo/Dev DynaPro Go TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2) Save the downloaded file `1000005023.p12` to the local computer.

4.2.2 Production (PCI)

Follow the instructions of this sub section only for Production devices. If not using Production devices, skip this subsection.

1) Touch the download button under **Production DynaPro Go Client TLS PKCS#12 – PN 1000005024.**



PCI DynaPro Go Client TLS PKCS#12 – PN 1000005024 - vA0

Host side TLS certificate chain and private key for use with Production DynaPro Go. TLS certificate chain is required if host (SDK) will connect to DynaPro Go using 802.11 wireless secured by TLSv1.2. Please contact support for password information.

2) Save the downloaded file `1000005024.p12` to the local computer.

4.3 Using the TLS Client Certificate

1) Put the client certificate in to the Visual Studio Project. Before connecting to the device in wireless mode, load the TLS client certificate for the device instance by calling the SDK function loadClientCertificate().