

## NIST SPECIAL PUBLICATION 1800-12C

---

# Derived Personal Identity Verification (PIV) Credentials

---

**Volume C:**  
How-to Guides

**William Newhouse**  
National Cybersecurity Center of Excellence  
Information Technology Laboratory

**Michael Bartock**  
**Jeffrey Cichonski**  
**Hildegard Ferraiolo**  
**Murugiah Souppaya**  
National Institute of Standards and Technology  
Information Technology Laboratory

**Christopher Brown**  
**Spike E. Dog**  
**Susan Prince**  
The MITRE Corporation  
McLean, VA

September 2017

DRAFT

This publication is available free of charge from:  
<https://nccoe.nist.gov/projects/building-blocks/piv-credentials>



## DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-12C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-12C, 59 pages, (September 2017), CODEN: NSPUE2

## FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: [piv-nccoe@nist.gov](mailto:piv-nccoe@nist.gov).

Public comment period: September 29, 2017 through November 29, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology  
100 Bureau Drive  
Mailstop 2002  
Gaithersburg, MD 20899  
Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards  
3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and  
4 academic institutions work together to address businesses' most pressing cybersecurity issues. This  
5 public-private partnership enables the creation of practical cybersecurity solutions for specific  
6 industries, as well as for broad, cross-sector technology challenges. Through consortia under  
7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from  
8 Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards  
9 and best practices to develop modular, easily adaptable example cybersecurity solutions using  
10 commercially available technology. The NCCoE documents these example solutions in the NIST Special  
11 Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the  
12 steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by  
13 NIST in partnership with the State of Maryland and Montgomery County, Md.

14 To learn more about the NCCoE, visit <https://nccoe.nist.gov>. To learn more about NIST, visit  
15 <https://www.nist.gov>.

## 16 **NIST CYBERSECURITY PRACTICE GUIDES**

17 NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity  
18 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the  
19 adoption of standards-based approaches to cybersecurity. They show members of the information  
20 security community how to implement example solutions that help them align more easily with relevant  
21 standards and best practices and provide users with the materials lists, configuration files, and other  
22 information they need to implement a similar approach.

23 The documents in this series describe example implementations of cybersecurity practices that  
24 businesses and other organizations may voluntarily adopt. These documents do not describe regulations  
25 or mandatory practices, nor do they carry statutory authority.

## 26 **ABSTRACT**

27 Federal Information Processing Standards (FIPS) Publication 201-2, "Personal Identity Verification (PIV)  
28 of Federal Employees and Contractors," establishes a standard for a PIV system based on secure and  
29 reliable forms of identity credentials issued by the federal government to its employees and contractors.  
30 These credentials are intended to authenticate individuals who require access to federally controlled  
31 facilities, information systems, and applications. In 2005, when FIPS 201 was published, logical access  
32 was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV  
33 card provides common multifactor authentication mechanisms through integrated smart card readers  
34 across the federal government. With the emergence of computing devices such as tablets, convertible

35 computers, and in particular mobile devices, the use of PIV cards has proved challenging. Mobile devices  
36 lack the integrated smart card readers found in laptop and desktop computers and require separate  
37 card readers attached to devices to provide authentication services. To extend the value of PIV systems  
38 into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the  
39 implementation and lifecycle of identity credentials that are issued by federal departments and agencies  
40 to individuals who possess and prove control over a valid PIV card. These NIST guidelines, published in  
41 2014, describe Derived PIV Credentials (DPCs) which leverage identity proofing and vetting results of  
42 current and valid PIV credentials.

43 To demonstrate the DPCs guidelines, the National Cybersecurity Center of Excellence (NCCoE) at NIST  
44 built in its laboratory a security architecture using commercial technology to manage the lifecycle of  
45 DPCs demonstrating the process that enables a PIV Card holder to establish DPCs in a mobile device  
46 which then can be used to allow the PIV Card holder to access websites that require PIV authentication.

47 This project resulted in a freely available NIST Cybersecurity Practice Guide which demonstrates how an  
48 organization can continue to provide two-factor authentication for users with a mobile device that  
49 leverages the strengths of the PIV standard. Although this project is primarily aimed at the Federal  
50 sector's needs, it is also relevant to mobile device users with smart card based credentials in the private  
51 sector.

## 52 **KEYWORDS**

53 *Cybersecurity; derived PIV credential (DPC); enterprise mobility management (EMM); identity; mobile  
54 device; mobile threat; (multifactor) authentication; network/software vulnerability; Personal Identity  
55 Verification (PIV); PIV card; smart card*

## 56 **ACKNOWLEDGMENTS**

57 We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Walter Holda	MobileIron
Loay Oweis	MobileIron
Sean Frazier	MobileIron
Dan Miller	Entrust Datacard

Name	Organization
Bryan Rosensteel	Entrust Datacard
Emmanuel Bello-Ogunu	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Poornima Koka	The MITRE Corporation
Matthew Steele	The MITRE Corporation

58 The technology vendors who participated in this build submitted their capabilities in response to a  
 59 notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative  
 60 Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium  
 61 to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
<a href="#">Entrust Datacard</a>	Entrust IdentityGuard, Entrust Managed Services PKI
<a href="#">MobileIron</a>	MobileIron Enterprise Mobility Management Platform

62 The NCCoE also wishes to acknowledge the special contributions of [Intercede](#) for providing us with  
 63 feedback on the risk assessment section of this practice guide, including risk mitigation and residual risk  
 64 association with a Derived PIV Credential system.

## 65 **Contents**

66	<b>1 Introduction.....</b>	<b>1</b>
67	1.1 Practice Guide Structure .....	1
68	1.2 Build Overview .....	2
69	1.3 Typographical Conventions.....	4
70	<b>2 Product Installation Guides .....</b>	<b>4</b>
71	2.1 Entrust Datacard IdentityGuard (IDG).....	5
72	2.1.1 Identity Management Profiles .....	6
73	2.2 MobileIron Core .....	6
74	2.2.1 Installation .....	6
75	2.2.2 General MobileIron Core Set Up.....	7
76	2.2.3 Configuration of MobileIron Core for DPC .....	7
77	2.3 DPC Lifecycle Workflows.....	17
78	2.3.1 DPC Initial Issuance .....	17
79	2.3.2 DPC Maintenance .....	50
80	2.3.3 DPC Termination .....	50

## 81 **List of Figures**

82	<b>Figure 1-1 Lab Network Diagram .....</b>	<b>3</b>
83	<b>Figure 2-1 Build 1 Architecture .....</b>	<b>5</b>
84	<b>Figure 2-2 MobileIron Registration Confirmation Page .....</b>	<b>23</b>
85	<b>Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page .....</b>	<b>47</b>

## 1 Introduction

The following guides show IT professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not recreate the product manufacturers' documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

*Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.*

### 1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate Derived Personal Identity Verification (PIV) Credential (DPC) lifecycle solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-12a: *Executive Summary*
- NIST SP 1800-12b: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-12c: *How-To Guides* – instructions for building the example solution (**you are here**)

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief security and technology officers** will be interested in the *Executive Summary* (NIST SP 1800-12a), which describes the:

- challenges enterprises face in issuing strong, two-factor credentials to mobile devices
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-12b*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.3, Risk, provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary*, *NIST SP 1800-12a*, with your leadership team members to help them understand the importance of adopting a standards-based Derived PIV Credential lifecycle solution.

117 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.  
118 You can use the How-To portion of the guide, *NIST SP 1800-12c*, to replicate all or parts of the build  
119 created in our lab. The How-To guide provides specific product installation, configuration, and  
120 integration instructions for implementing the example solution. We do not recreate the product  
121 manufacturers' documentation, which is generally widely available. Rather, we show how we  
122 incorporated the products together in our environment to create an example solution.

123 This guide assumes that IT professionals have experience implementing security products within the  
124 enterprise. While we have used a suite of commercial products to address this challenge, this guide  
125 does not endorse these particular products. Your organization can adopt this solution or one that  
126 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
127 implementing parts of a Derived PIV Credential lifecycle solution. Your organization's security experts  
128 should identify the products that will best integrate with your existing tools and IT system  
129 infrastructure. We hope you will seek products that are congruent with applicable standards and best  
130 practices. Volume B, Section 4.2, Technologies, lists the products we used and maps them to the  
131 cybersecurity controls provided by this reference solution.

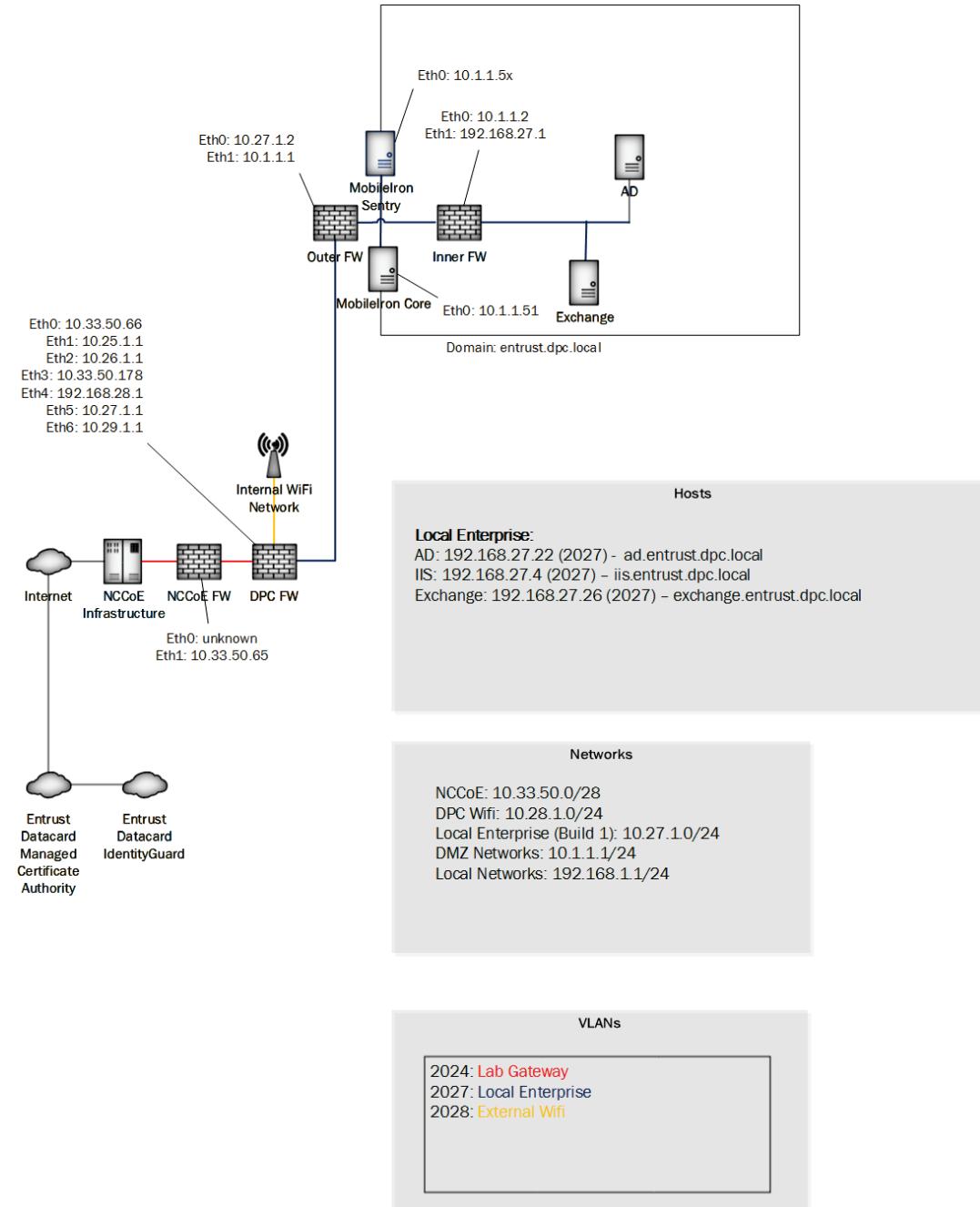
132 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a  
133 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and  
134 success stories will improve subsequent versions of this guide. Please contribute your thoughts to  
135 [piv-nccoe@nist.gov](mailto:piv-nccoe@nist.gov).

## 136 1.2 Build Overview

137 Unlike desktop computers and laptops that have built-in readers to facilitate the use of PIV Cards,  
138 mobile devices pose usability and portability issues because of the lack of a smart card reader.  
  
139 NIST sought to address this issue with the introduction of the general concept of Derived PIV Credentials  
140 in SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials.  
141 Published in 2014, SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*  
142 defined requirements for initial issuance and maintenance of Derived PIV Credentials. NIST's Applied  
143 Cybersecurity Division then created a NCCoE project to provide an example solution for federal agencies  
144 and private entities that follows the requirements in SP 800-157.

145 In the NCCoE lab, the team built an environment that resembles an enterprise network using  
146 commonplace components such as identity repositories, supporting certificate authorities (CA), and  
147 web servers. In addition, products and capabilities were identified that, when linked together, provide  
148 an example solution that demonstrate lifecycle functions outlined in SP 800-157. Figure 1-1 depicts the  
149 final lab environment.

150 Figure 1-1 Lab Network Diagram



151

## 152 1.3 Typographical Conventions

153 The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
<b>Bold</b>	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output, sample code examples, sta- tus codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b>service sshd start</b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

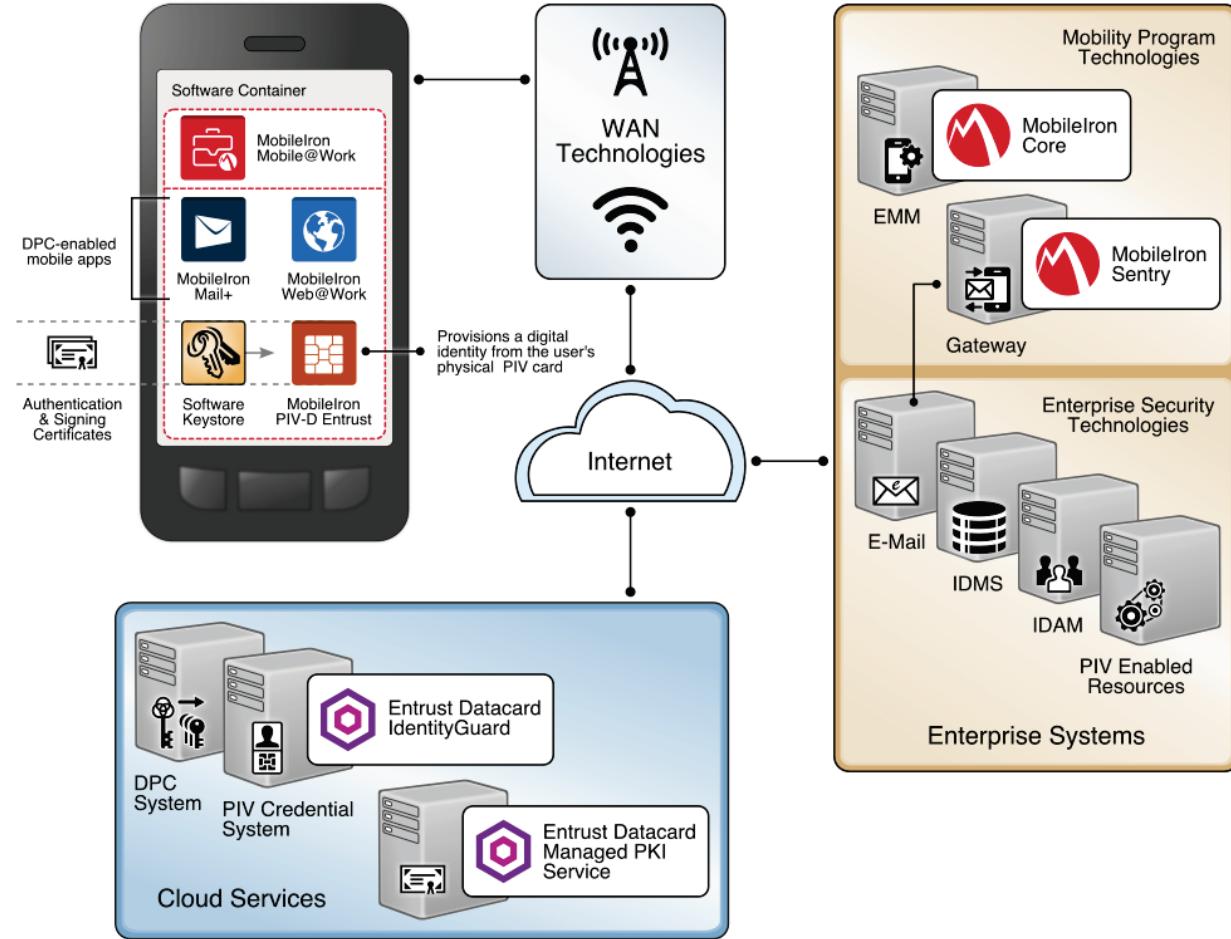
## 154 2 Product Installation Guides

155 This section of the practice guide contains detailed instructions for installing and configuring of key  
156 products used for the depicted architecture illustrated below, as well as demonstration of the DPC  
157 lifecycle management activities of initial issuance and termination.

158 In our lab environment, the example solution was logically separated by a Virtual Local Area Network  
159 (VLAN) wherein each VLAN represented a mock enterprise environment. The network topology consists  
160 of an edge router connected to a Demilitarized Zone (DMZ). An internal firewall separates the DMZ from  
161 internal systems that support the enterprise. All routers and firewalls used in the example solution were  
162 virtual [pfSense](#) appliances.

163 As a basis, the enterprise network had an instance of Active Directory (AD) to serve as a repository for  
164 identities to support DPC vendors.

165 Figure 2-1 Build 1 Architecture



166

## 167 2.1 Entrust Datacard IdentityGuard (IDG)

168 Entrust Datacard contributed test instances of their managed Public Key Infrastructure (PKI) service and  
 169 IdentityGuard products, the latter of which directly integrates with MobileIron to support the use of  
 170 Derived PIV Credentials with MobileIron Mobile@Work apps. Contact Entrust Datacard  
 171 (<https://www.entrust.com/contact/>) to establish service instances in support of a Derived PIV  
 172 Credentials with MobileIron (<https://www.mobileiron.com/>).

173 **2.1.1 Identity Management Profiles**

174 To configure services and issue certificates for Derived PIV Credentials that will work with your  
 175 organization's user identity profiles, Entrust Datacard will need information on how identities are  
 176 structured and which users will use PKI services. For this lab instance, Entrust Datacard issued PIV  
 177 Authentication, Digital Signature, and Encryption certificates for PIV Cards and Derived PIV Credentials  
 178 for two test identities, as represented below.

User Name	Email Address	User Principal Name (UPN)
Patel, Asha	asha@entrust.dpc.nccoe.org	asha@entrust.dpc.nccoe.org
Tucker, Matteo	matteo@entrust.dpc.nccoe.org	matteo@entrust.dpc.nccoe.org

179 **2.2 MobileIron Core**

180 MobileIron Core is the central product in the MobileIron suite. The following sections describe the steps  
 181 for installation, configuration, and integration with Active Directory and the Entrust Datacard  
 182 IdentityGuard cloud service. Key configuration files used in this build are listed below and are available  
 183 from the NCCoE DPC project website.

Filename	Description
core.dpc.nccoe.org-Default AppConnect Global Policy-2017-08-14 16-48-36.json	Configures policies such as password strength for the container
core.dpc.nccoe.org-Default Privacy Policy-2017-08-14 16-52-33.json	Configures privacy settings for each enrolled device
core.dpc.nccoe.org-DPC Security Policy-2017-08-14 16-51-07.json	Configures device level security management settings
shared_mdm_profile.mobileconfig	iOS MDM profile used when issuing DPCs to devices

184 **2.2.1 Installation**

185 Follow the steps below to install MobileIron Core:

- 186 1. Obtain a copy of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* from the MobileIron support portal.
- 187 2. Follow the MobileIron Core pre-deployment and installation steps in Chapter 1 of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* for the version of MobileIron being deployed in your environment. In our lab implementation, we deployed MobileIron Core 9.2.0.0 as a Virtual Core running on VMware 6.0.

192    **2.2.2 General MobileIron Core Set Up**

193    The following steps are necessary for mobile device administrators or users to register devices with  
194    MobileIron, which is a prerequisite to issuing Derived PIV Credentials.

- 195    1. Obtain a copy of *MobileIron Core Device Management Guide for iOS Devices* from the MobileIron-  
196    support portal.  
  
197    2. Complete all instructions provided in Chapter 1, Setup Tasks.

198    **2.2.3 Configuration of MobileIron Core for DPC**

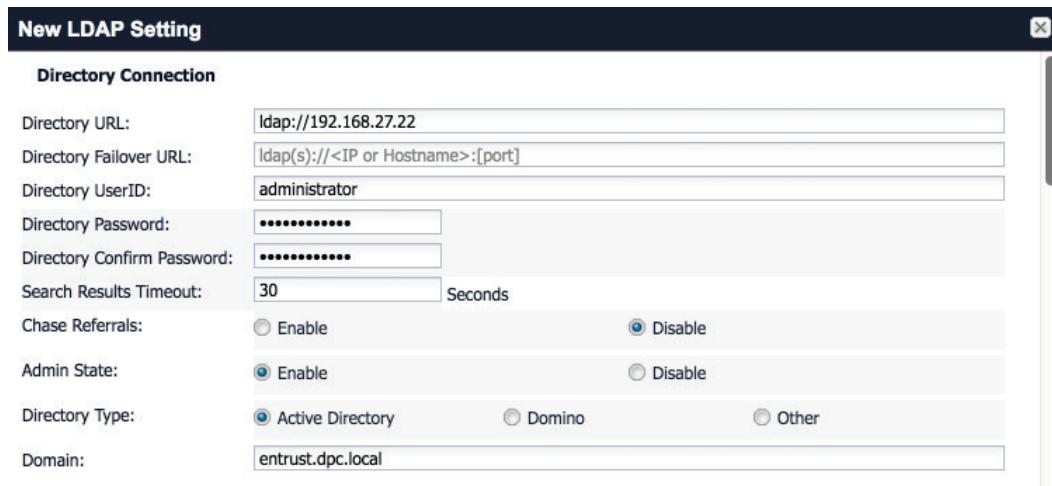
199    The following steps will reproduce this configuration of MobileIron Core.

200    **2.2.3.1 Integration with Active Directory**

201    In our implementation, we chose to integrate MobileIron Core with Active Directory using LDAP. This is  
202    optional. General instructions for this process are covered in the *Configuring LDAP Servers* section in  
203    Chapter 2 of *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector*. The  
204    configuration details used during our completion of selected steps (retaining original numbering) from  
205    that guide are given below:

- 206    1. From Step 4 in the MobileIron guide, in the **New LDAP Server** dialog:  
  
207        a. Directory Connection:

208



The screenshot shows the 'New LDAP Setting' dialog box with the title 'New LDAP Setting'. The 'Directory Connection' tab is selected. The configuration includes:

- Directory URL: ldap://192.168.27.22
- Directory Failover URL: ldap(s)://<IP or Hostname>:[port]
- Directory UserID: administrator
- Directory Password: [REDACTED]
- Directory Confirm Password: [REDACTED]
- Search Results Timeout: 30 Seconds
- Chase Referrals:  Enable  Disable
- Admin State:  Enable  Disable
- Directory Type:  Active Directory  Domino  Other
- Domain: entrust.dpc.local

209

## b. Directory Configuration - OUs:

**New LDAP Setting**

**Directory Configuration - OUs**

OU Base DN:	dc=entrust,dc=dpc,dc=local
OU Search Filter:	( (objectClass=organizationalUnit)(objectClass=container))

210

211

## c. Directory Configuration - Users:

**New LDAP Setting**

**Directory Configuration - Users**

User Base DN:	dc=entrust,dc=dpc,dc=local
Search Filter:	(&(objectClass=user)(objectClass=person))
Search Scope:	All Levels
First Name:	givenName
Last Name:	sn
User ID:	sAMAccountName
Email:	mail
Display Name:	displayName
Distinguished Name:	distinguishedName
User Principal Name:	userPrincipalName
Locale:	c

212

213

## d. Directory Configuration - Groups:

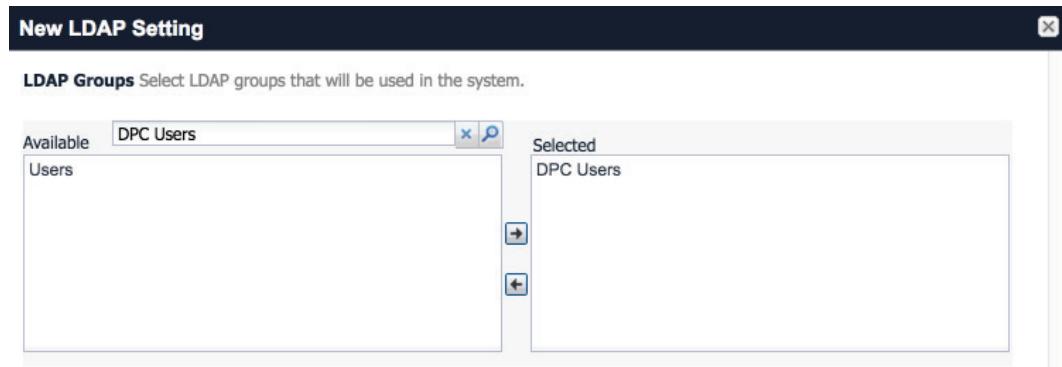
**New LDAP Setting**

**Directory Configuration - Groups**

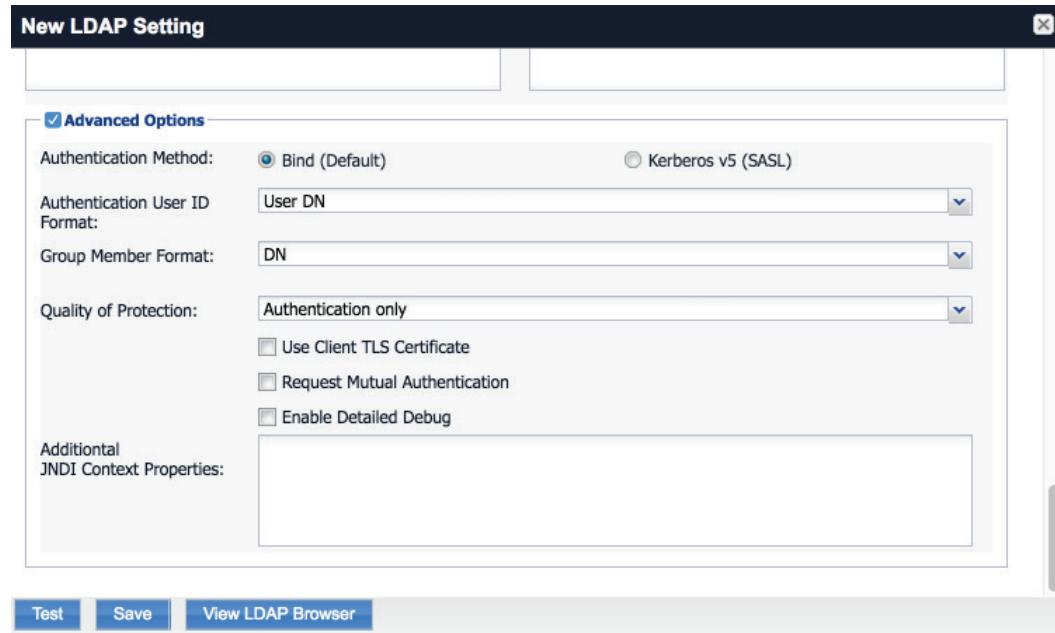
User Group Base DN:	dc=entrust,dc=dpc,dc=local
Search Filter:	(objectClass=group)
Search Scope :	All Levels
User Group Name:	cn
Membership Attribute:	member
Member Of Attribute:	memberOf
Custom Attribute-1:	
Custom Attribute-2:	
Custom Attribute-3:	
Custom Attribute-4:	

214

- 215                   e. LDAP Groups:
- 216                    i. As a prerequisite step, we used Active Directory Users and Computers to create  
217                    a new security group for DPC-authorized users on the Domain Controller for the  
218                    entrust.dpc.local domain. In our example, this group is named **DPC Users**.
- 219                    ii. In the search bar, enter the name of the LDAP group for DPC-authorized users  
220                    and click the **magnifying glass** button; the group name should be added to the  
221                    **Available** list.
- 222                    iii. In the **Available** list, select **DPC Users** and click the **right-arrow** button to move  
223                    it to the **Selected** list.
- 224                    iv. In the **Selected** list, select the default **Users** group and click the **left-arrow** but-  
225                    ton to move it to the **Available** list.



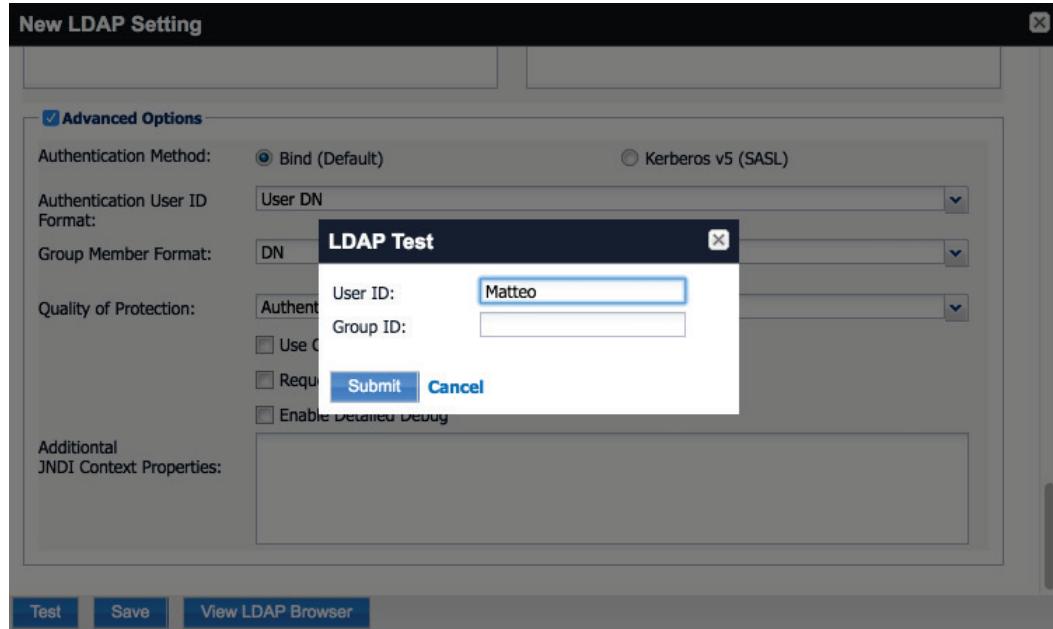
- 226
- 227                   f. Custom Settings: custom settings were not specified.
- 228                   g. Advanced Options:



229

230    **Note:** In our lab environment, we did not enable stronger Quality of Protection or enable the Use of  
 231    Client TLS Certificate or Request Mutual Authentication features. However, we recommend  
 232    implementers consider using those additional security mechanisms to secure communication with the  
 233    LDAP server.

- 234    2. From Steps 19-21 from the MobileIron guide, we tested that MobileIron can successfully query  
 235    LDAP for DPC Users.
- 236        a. In the **New LDAP Setting** dialog, click the **Test** button to open the **LDAP Test** dialog.  
 237        b. In the **LDAP Test dialog**, enter a **User ID** for a member of the DPC Users group then click  
 238           the **Submit** button. A member of the DPC Users group in our environment is **Matteo**.



239

240

- c. The **LDAP Test** dialog indicates the query was successful:



241

242 **2.2.3.2 Create a DPC Users Label**

243 MobileIron uses labels to link policies and device configurations with users and mobile devices. Creating  
 244 a unique label for DPC users allows mobile device administrators to apply controls applicable to mobile  
 245 devices provisioned with a derived credential specifically to those devices. We recommend applying  
 246 DPC-specific policies and configurations to this label, in addition to any others appropriate to your  
 247 organization's mobile device security policy.

248 1. In the **MobileIron Core Admin Portal**, navigate to **Devices & Users > Devices**.

249 2. Select **Advanced Search** (far right).

DISPLAY NAME	CURRENT PHONE NU...	MODEL	MANUFACT...	PLATFORM ...	STATUS	REGISTRATION...	LAST CHEC...	OWNER
Asha Patel	PDA 10			iOS	Pending			Company
Matteo Tucker	PDA 2	iPad Air 2	Apple	iOS 10.2	Active	2017-08-04 11:0...	6 d 23h	Company
Selina Kyle	PDA 2			Android	Pending			Company

250

251 3. In the **Advanced Search** pane:

252 a. In the blank rule:

253 i. In the **Field** drop-down menu, select **User > LDAP > Groups > Name**.

254 ii. In the **Value** drop-down menu, select the Active Directory group created to support DPC-specific MobileIron policies (named **DPC User** in this example).

256 b. Select the **plus sign icon** to add a blank rule.

257 c. In the newly created blank rule:

258 i. In the **Field** drop-down menu, select **Common > Platform**.

259 ii. In the **Value** drop-down menu, select **iOS**.

260 d. Optionally, select **Search** to view matching devices.

261 e. Select **Save to Label**.

All    Any    of the following rules are true

Name Equals DPC User  
Platform Equals iOS

"user.ldap.groups.name" = "DPC Users" AND "common.platform" = "iOS"

Exclude retired devices from search results

**Search** **Save to Label** **Clear**

	DISPLAY NAME	CURRENT...	MODEL	MANUFACT...	PLATFORM...	STATUS	LAST...	OWNER
<input type="checkbox"/>	Asha Patel	PDA 10		iOS	Pending	Company		
<input type="checkbox"/>	Matteo Tucker	PDA 2	iPad Air 2	Apple	iOS 10.2	Active	6 d 18h	Company

262

263 f. In the Save to Label dialog:

- 264 i. In the **Name** field, enter a descriptive name for this label (**DPC Users** in this example).
- 265 ii. In the **Description** field, provide additional information to convey the purpose of this label.
- 266 iii. Click **Save**.
- 267

Save to Label

Name	DPC Users
Description	Used for iOS users that are permitted to have a DPC provisioned to their mobile device.

**Cancel** **Save**

269

- 270     4. **Navigate to Devices & Users > Labels** to confirm the label was successfully created. It can be  
 271       applied to Derived PIV Credential-specific MobileIron policies and configurations in future steps.

	NAME	DESCRIPTION	TYPE	CRITERIA	SPACE	VIEW DE...
<input type="checkbox"/>	Android	Label for all ...	Filter	"common.platform"="Android" ...	Global	<u>1</u>
<input type="checkbox"/>	Company-O...	Label for all ...	Filter	"common.owner"="COMPANY..."	Global	<u>3</u>
<input type="checkbox"/>	DPC Users	Used for iO...	Filter	("common.platform" = "iOS" A...	Global	<u>2</u>

272

### 2.2.3.3 Implement MobileIron Guidance

- 273     The following provides the sections from the *MobileIron Derived Credentials with Entrust Guide* that  
 274       were used in configuring this instance of MobileIron Derived PIV Credentials. Sections for which there  
 275       may be configuration items tailored to a given instance (e.g., local system hostnames), this  
 276       configuration is provided only as a reference. We noted any sections in which the steps performed to  
 277       configure our systems varies from those in the *MobileIron Derived Credentials with Entrust Guide*.

- 279 Complete these sections in Chapter 2 of the *MobileIron Derived Credentials with Entrust Guide*:
- 280     1. Before beginning:
- 281         a. Configuring certificate authentication to the user portal.
- 282             Note: The root CA certificate or trust chain file can be obtained from Entrust Datacard.
- 283         b. Configuring the Entrust IdentityGuard Self-Service Module (SSM) Module Universal Re-
- 284             source Locator (URL).
- 285             Note: The URL will be specific to your organization's instance of the IDG service and can
- 286             be obtained from Entrust Datacard.
- 287     2. Configuring PIN-based registration.
- 288     3. Configuring user portal roles.
- 289     4. Adding the PIV-D Entrust app to the App Catalog.
- 290         a. Adding Web@Work for iOS.
- 291     5. Configuring Apps@Work.
- 292         a. Setting authentication options.
- 293         b. Sending the Apps@Work web clip to devices.
- 294     6. Configuring AppConnect.
- 295         a. Configuring AppConnect licenses.
- 296         b. Configuring the AppConnect global policy. The **AppConnect Passcode** policy settings for
- 297             our implementation are presented below.

**Modify AppConnect Global Policy**

**AppConnect Passcode**

Passcode Type:  Numeric  Alphanumeric  Don't Specify

Minimum Passcode Length:

Minimum Number of Complex Characters:

Maximum Passcode Age:  1-730 days, or none

Auto-Lock Time:

Passcode History:

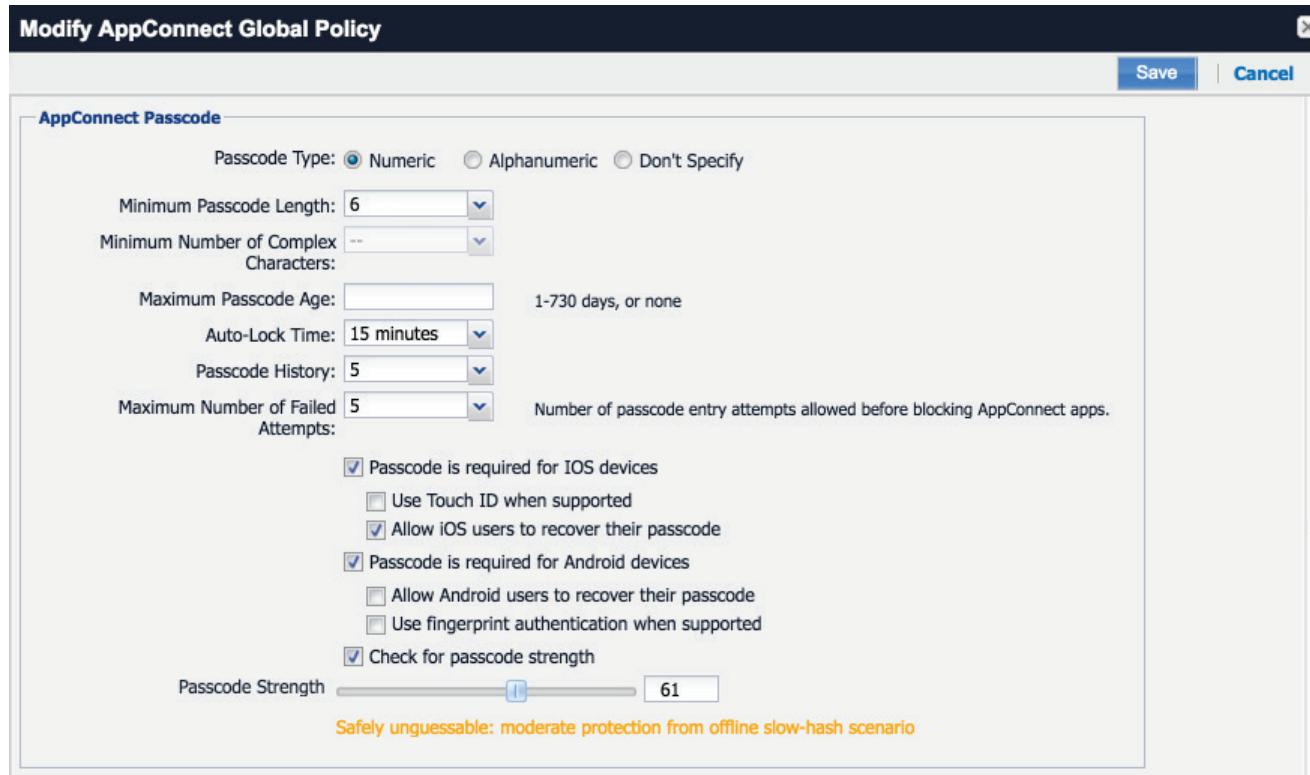
Maximum Number of Failed Attempts:  Number of passcode entry attempts allowed before blocking AppConnect apps.

Passcode is required for iOS devices  
 Use Touch ID when supported  
 Allow iOS users to recover their passcode  
 Passcode is required for Android devices  
 Allow Android users to recover their passcode  
 Use fingerprint authentication when supported  
 Check for passcode strength

Passcode Strength  61

Safely unguessable: moderate protection from offline slow-hash scenario

**Save** | **Cancel**



298

299

300

Note that based on our testing, a **Passcode Strength** of 61/100 or higher prevents easily guessable derived credential passcode combinations (e.g., abc123) from being set by a DPC Applicant.

- 301        7. Configuring the PIV-D Entrust app.
- 302        8. Configuring client-provided certificate enrollment settings. Note that the configuration items  
 303        created by completing this section will be used in the following section. Replace **Step 2** in this  
 304        section of the *MobileIron Derived Credentials with Entrust Guide* with the following:
- 305            a. Select **Add New > Certificate Enrollment > SCEP**.
- 306        9. Configuring Web@Work to use Derived PIV Credentials.
- 307            a. Require a device password.
- 308            b. Configure a Web@Work setting. The **Custom Configurations** key-value pairs set for our  
 309        instance in Step 4 are presented below.
- 310            Note: The value for `idCertificate_1` is the descriptive name we applied to the Simple  
 311        Certificate Enrollment Protocol (SCEP) certificate enrollment configuration for derived  
 312        credential authentication created in the *MobileIron Derived Credentials with Entrust*  
 313        *Guide* section referenced in **Step 8**.

KEY	VALUE	
<code>IdCertificate_1_host</code>	*	
<code>IdCertificate_1</code>	DC Authentication	

314

## 315 2.3 DPC Lifecycle Workflows

316 The following sections describe how to perform the DPC lifecycle activities of issuance, maintenance,  
 317 and termination.

### 318 2.3.1 DPC Initial Issuance

319 The following sections provide the steps necessary to issue a Derived PIV Credential onto a target  
 320 mobile device.

#### 321 2.3.1.1 Register Target Device with MobileIron

322 The following steps will register the target mobile device with MobileIron, which will create the secure  
 323 Mobile@Work container into which a Derived PIV Credential is later provisioned.

- 324        1. Insert your valid PIV Card into the card reader attached to, or integrated into, your laptop or  
 325        computer workstation.
- 326        2. Using a web browser, visit the MobileIron Self-Service Portal URL provided by your administra-  
 327        tor.

328

3. In the MobileIron Self-Service Portal, click **Sign in with certificate**.

MobileIron seamlessly secures your device and provides easy access to your email, applications and content.



**SIGN IN WITH CERTIFICATE**



**Instant Access**

Receive instant access to your corporate email, calendar and contacts.



**Apps**

Utilize your favorite corporate apps whenever and wherever you want.



**Secure Content**

Easily access corporate documents, presentations and more.

329

330

4. In the certificate selection dialog:

331

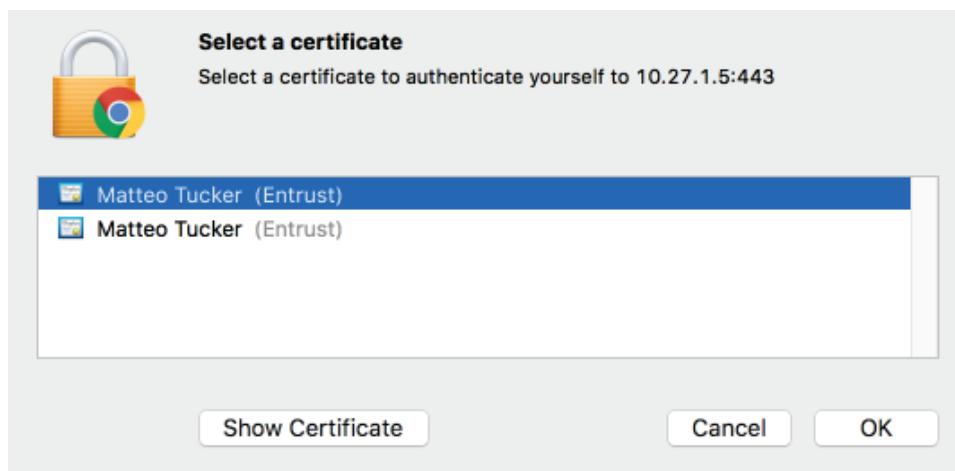
- a. If necessary, identify your PIV Authentication certificate:

332

- i. Highlight a certificate.

333

- ii. Select **Show Certificate**.

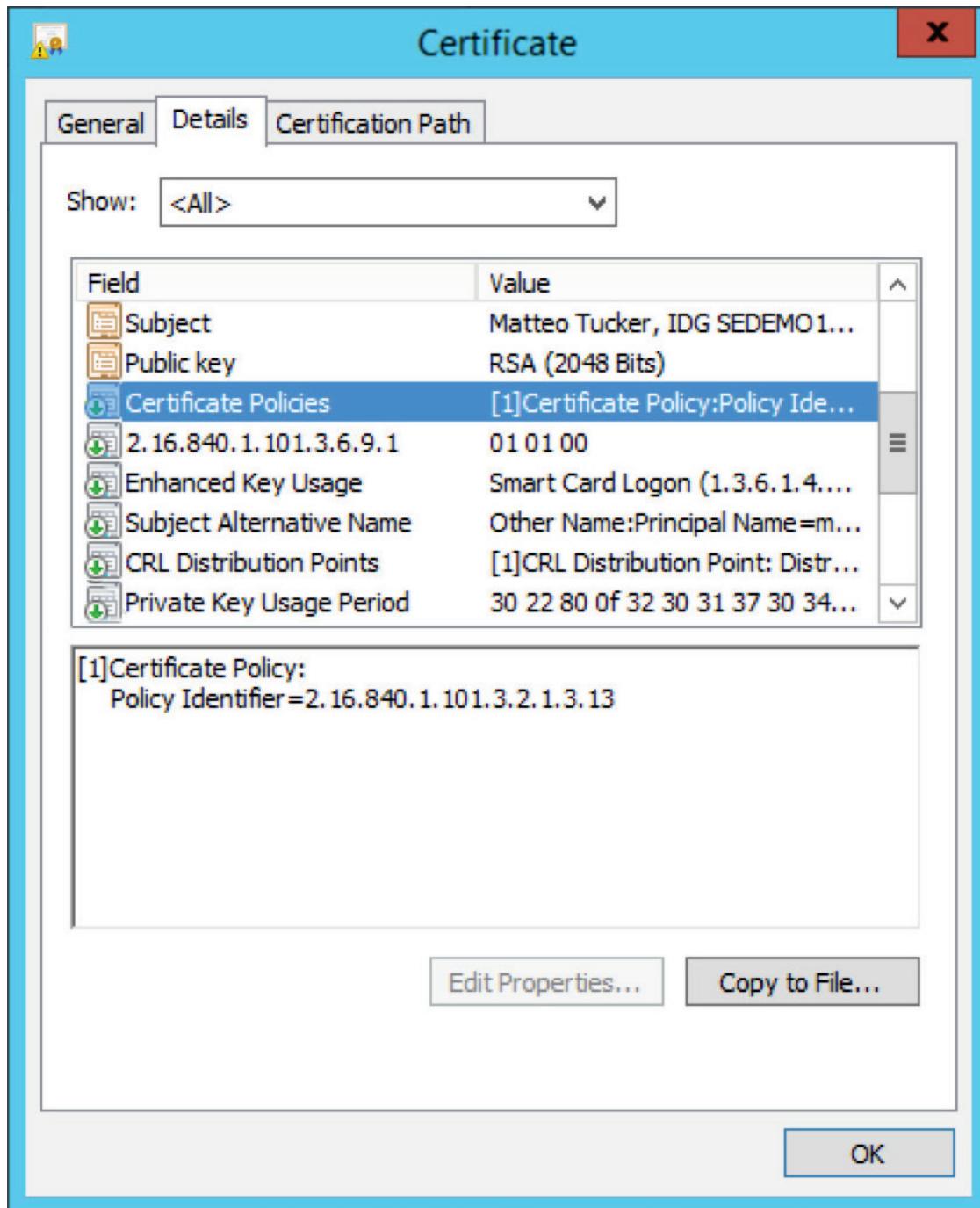


334

335

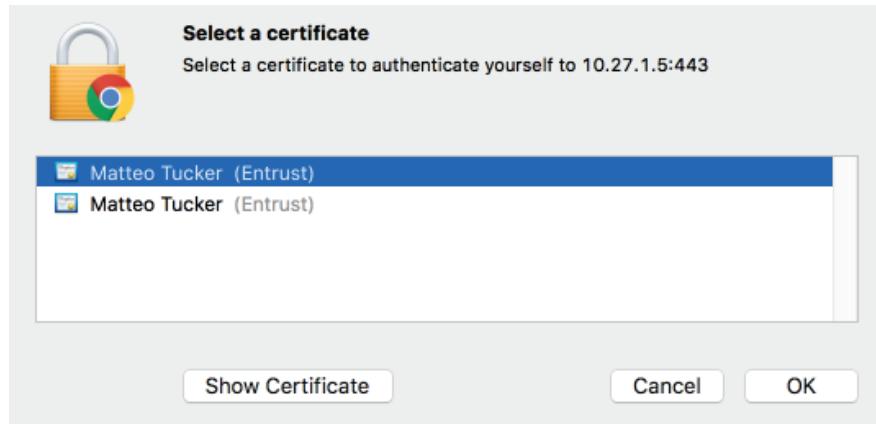
- iii. Navigate to the **Details** tab.

- 336                  iv. The PIV Authentication certificate contains a **Field** named **Certificate Policies**  
337                  with a **Value** that contains **Policy Identifier=2.16.840.1.101.3.2.1.3.13**.  
338                  v. Repeat **Steps i-iii** above as necessary.



339

- 340            b. Select your PIV Authentication certificate in the list of available certificates.
- 341            c. Click **OK**.



- 342
- 343        5. In the authentication dialog:
- 344            a. In the **PIN** field, enter your PIV Card PIN.
- 345            b. Click **OK**.

MobileIron seamlessly secures your device and provides easy access to your email, applications and content.



[SIGN IN WITH CERTIFICATE](#)

**Instant Access**  
Receive instant access to your corporate email, calendar and contacts.

**Apps**  
Utilize your favorite corporate apps whenever and wherever you want.

**Secure Content**  
Easily access corporate documents, presentations and more.

"Google Chrome" is trying to authenticate user.  
Enter PIN to allow this.  
PIN:

Cancel      OK

346

- 347 6. In the right-hand sidebar of the device summary screen, click **Request Registration PIN**.

The screenshot shows the MobileIron Device Management interface. On the left, there are two device cards: "SAMSUNG-SM-G925A" (Company Owned) and "iPhone 6" (Company Owned). Each card displays the device name, ownership status, a thumbnail icon, the word "Active", the last seen time, a "No Phone Number" message, and detailed technical information like Version, Carrier, IMEI, Manufacturer, and Registration Date. Below each card are three circular buttons: "Lock", "Unlock", and "More". On the right, a vertical sidebar is titled "Need to register another device?". It features a diagram of two phones showing a login screen with fields for "user@example.com" and "password", and a "Sign In" button. Below the diagram, a message states: "Your organization requires you to have a valid PIN to register a device." A large blue button labeled "Request Registration PIN" is prominently displayed. At the bottom of the sidebar, another message says: "On your mobile device, visit <https://core.dpc.nccoe.org/go>".

348

- 349 7. In the **Request Registration PIN** page:
- 350 a. Select **iOS** from the **Platform** drop-down menu.
- 351 b. If your device does not have a phone number, check **My device has no phone number**.
- 352 c. If your device has a phone number, enter it in the **Phone Number** field.

353

- d. Click **Request PIN**.

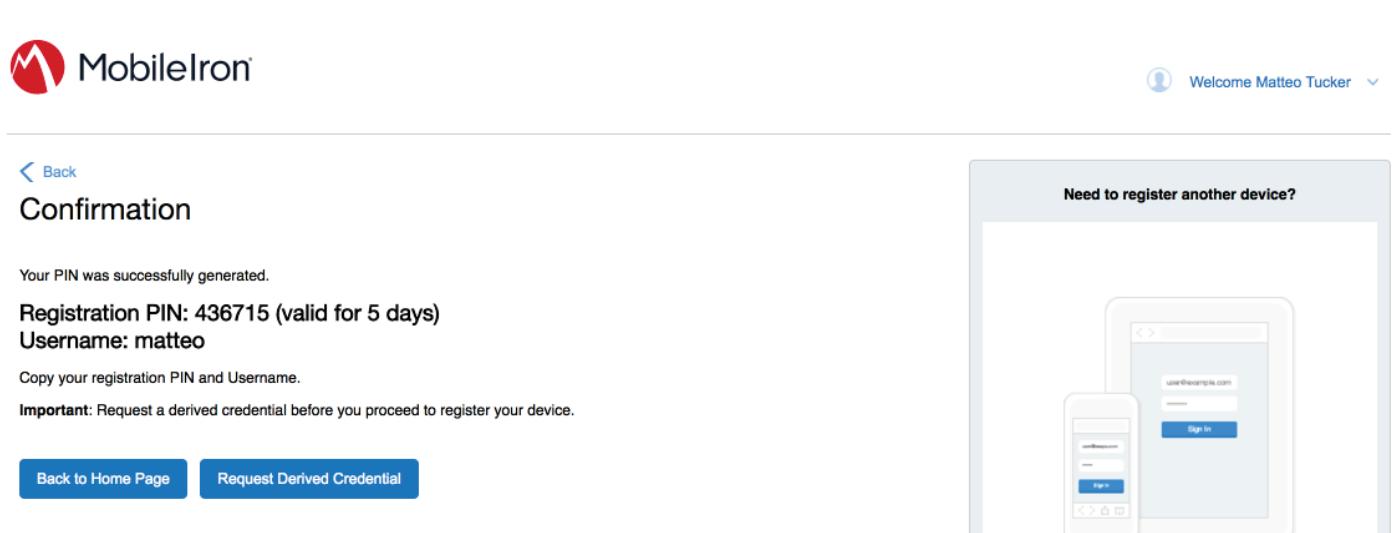
The screenshot shows the MobileIron web interface for requesting a registration PIN. The main panel is titled "Request Registration PIN" and contains fields for Platform (selected as iOS), Device Language (English), and a checked checkbox for "My device has no phone number". It also includes fields for Country (United States), Phone Number (No space or leading zero) with a placeholder "+1", Operator (Operator Name dropdown), and a checked checkbox for "Notify User By SMS". At the bottom are "Cancel" and "Request PIN" buttons. To the right, a sidebar titled "Need to register another device?" displays a diagram of two mobile devices showing a login screen with "Sign In" buttons. Below the diagram, text states "Your organization requires you to have a valid PIN to register a device." and a large blue "Request Registration PIN" button. Further down, it says "On your mobile device, visit <https://core.dpc.nccoe.org/go>".

354

- 355        e. The **Confirmation** page, shown in Figure 2-2 displays a unique device **Registration PIN**. Leave this page open while additional  
356        registration steps are performed on the target mobile device.

357            Note: This page may also facilitate the workflow for initial DPC issuance, covered in [Section 2.3.1.2](#).

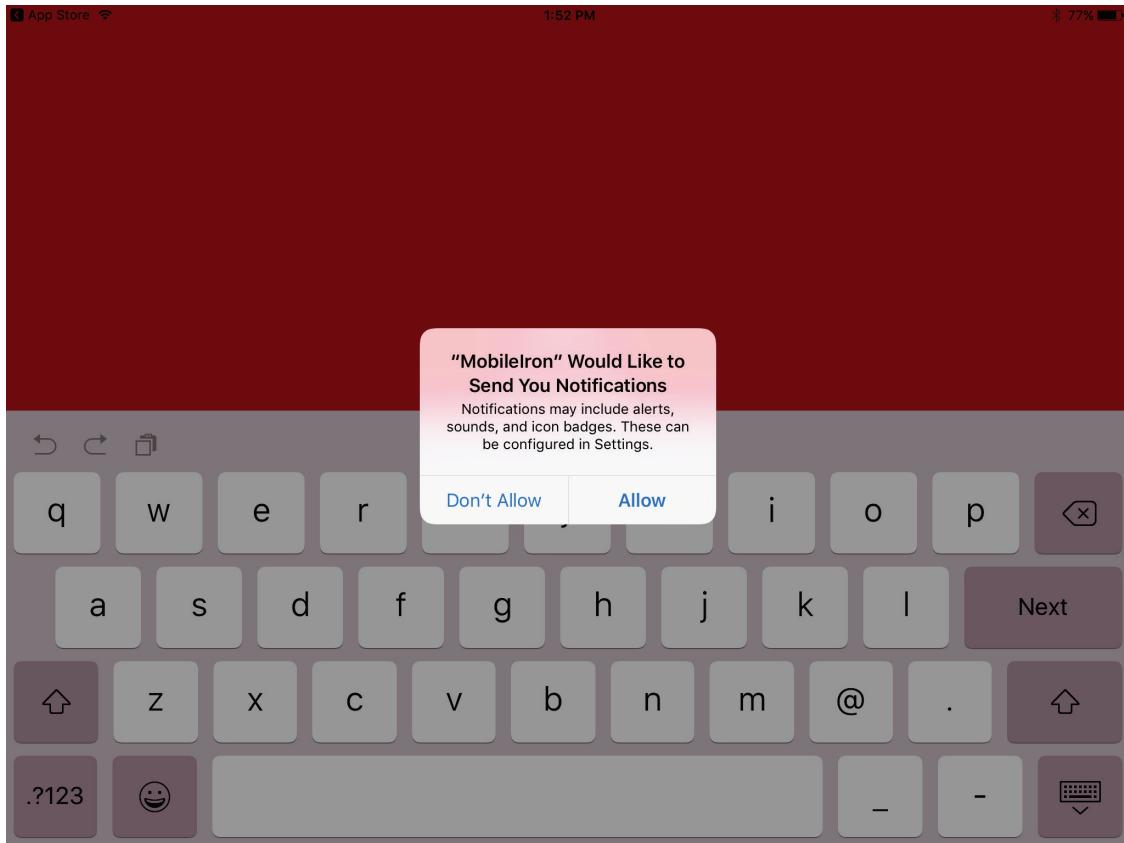
358        **Figure 2-2 MobileIron Registration Confirmation Page**



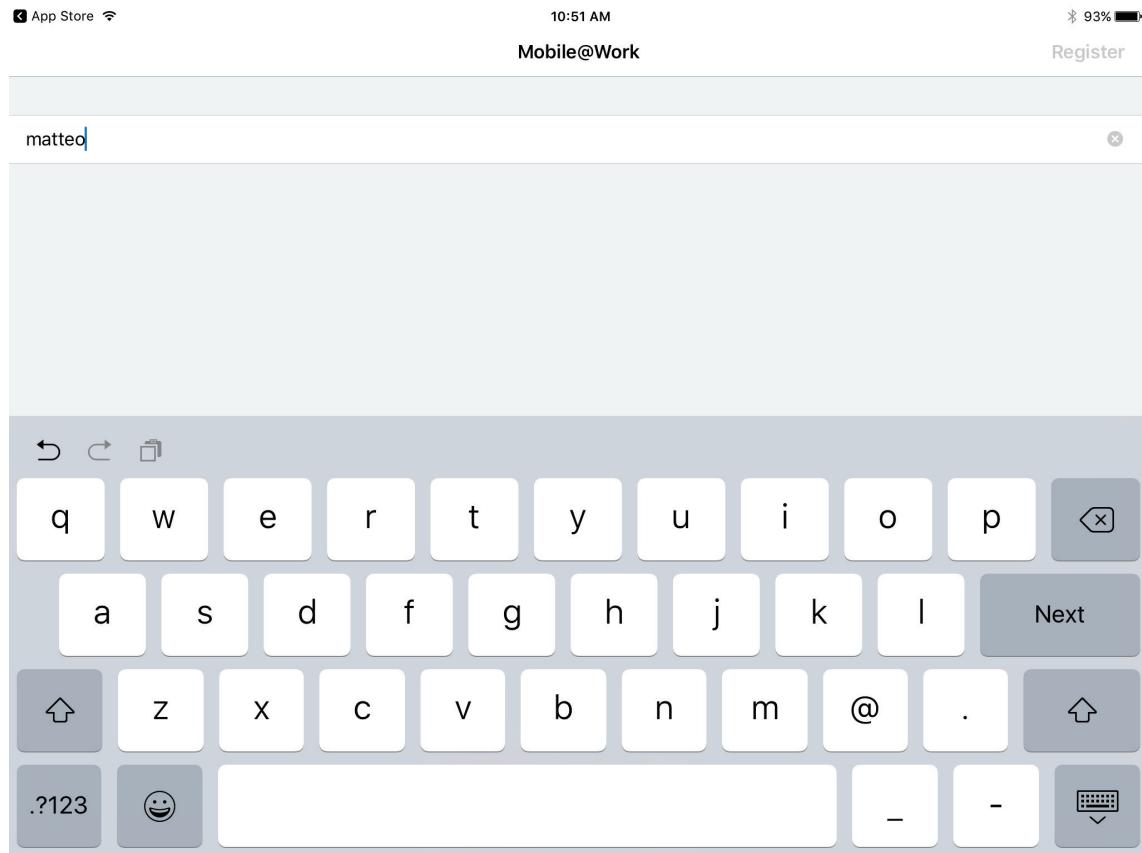
The screenshot shows the MobileIron Registration Confirmation Page. At the top left is the MobileIron logo. At the top right is a user profile icon and the text "Welcome Matteo Tucker". Below the header, there's a "Back" button and the word "Confirmation". The main content area displays a success message: "Your PIN was successfully generated." followed by the "Registration PIN: 436715 (valid for 5 days)" and "Username: matteo". Below this, instructions say "Copy your registration PIN and Username." and "Important: Request a derived credential before you proceed to register your device." At the bottom are two buttons: "Back to Home Page" and "Request Derived Credential". To the right of the main content is a modal window titled "Need to register another device?". The modal shows icons of a laptop, tablet, and smartphone, each displaying a login screen with a "Sign In" button.

359

- 360        8. Using the target mobile device, launch the MobileIron **Mobile@Work** app.
- 361        9. In the request to grant MobileIron permission to receive push notifications, tap **Allow**.

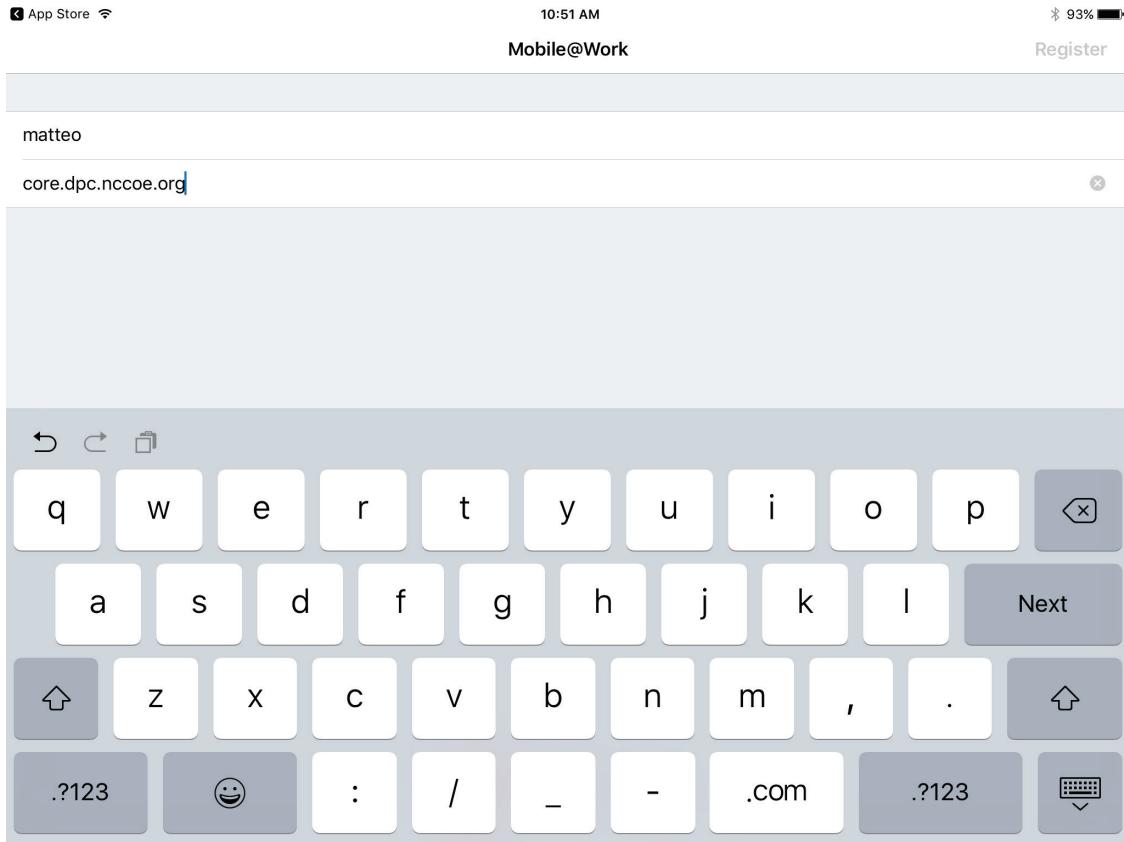


- 362
- 363        10. In **Mobile@Work**:
- 364            a. In the **User Name** field, enter your LDAP or MobileIron user ID.
- 365            b. Tap **Next**.



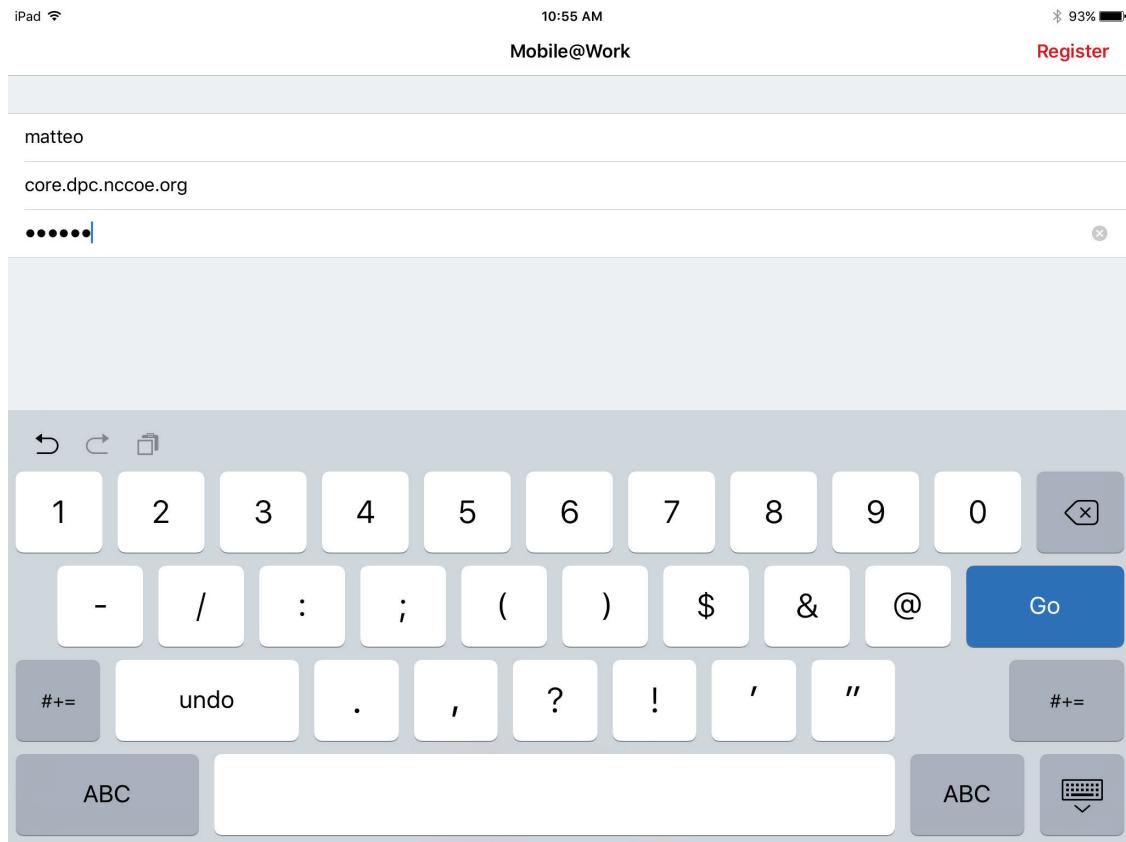
366

- 367       c. In the **Server** field, enter the URL for your organization's instance of MobileIron Core as  
368                   provided by a MobileIron Core administrator.  
369       d. Tap **Next**.



370

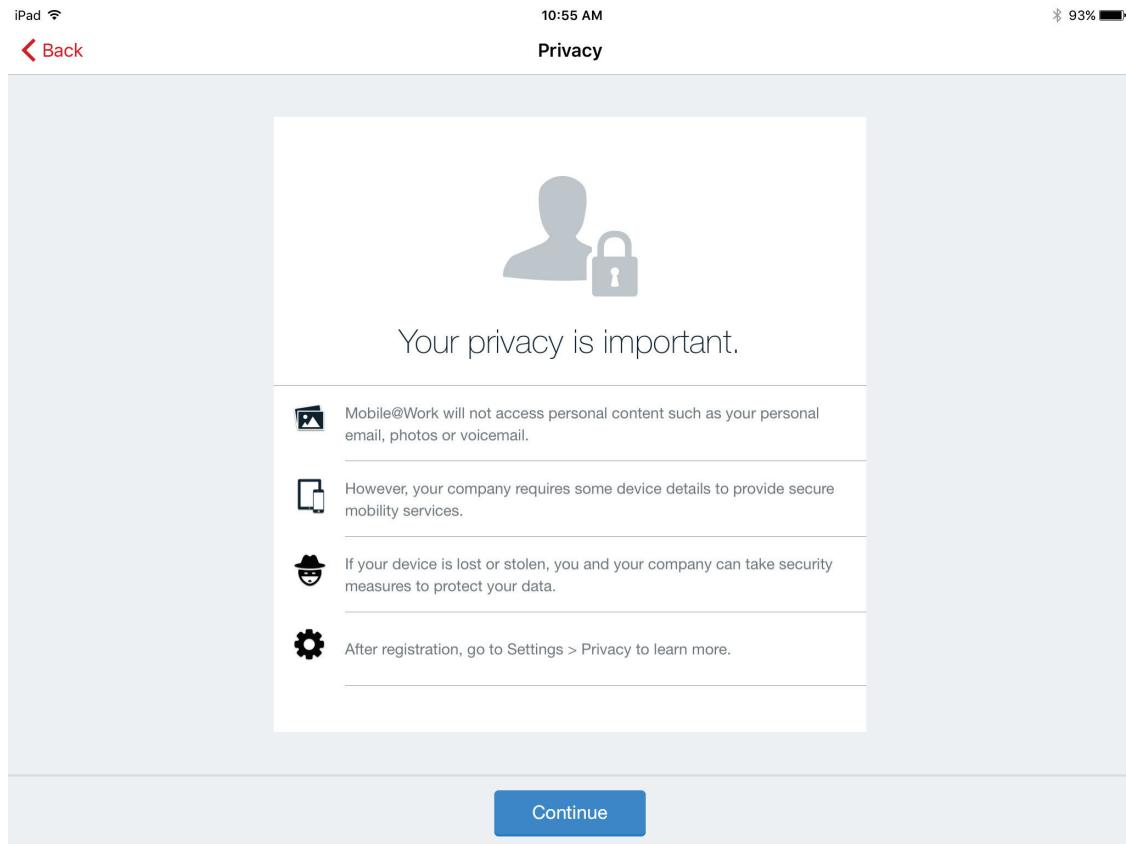
- 371       e. In the **PIN** field, enter the **Registration PIN** displayed in the **Confirmation** page (see  
372                          Figure 2-2) of the MobileIron Self-Service Portal at the completion of **Step 7e**.  
373       f. Tap **Go** on keyboard or **Register** in Mobile@Work.



374

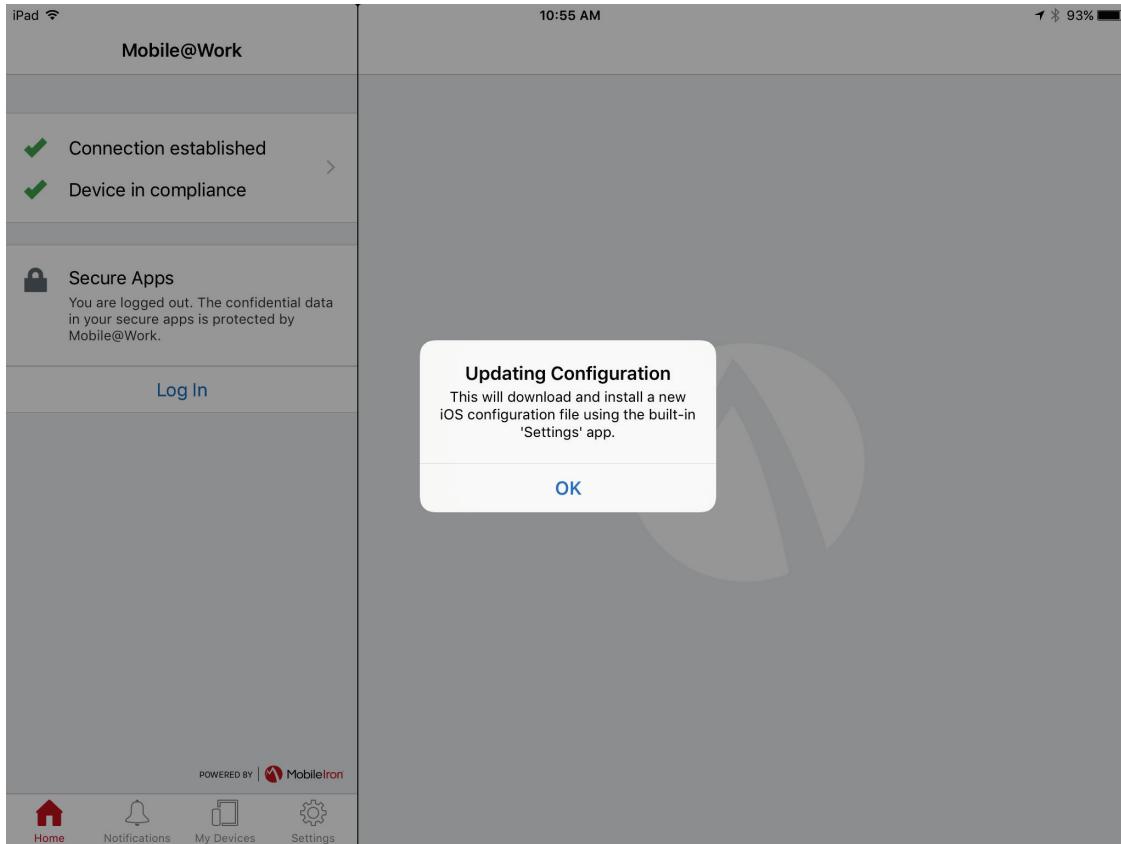
375

- g. In the Privacy screen, tap **Continue**.



376

377 11. In the **Updating Configuration** dialog, tap **OK**; this will launch the built-in iOS **Settings** app.



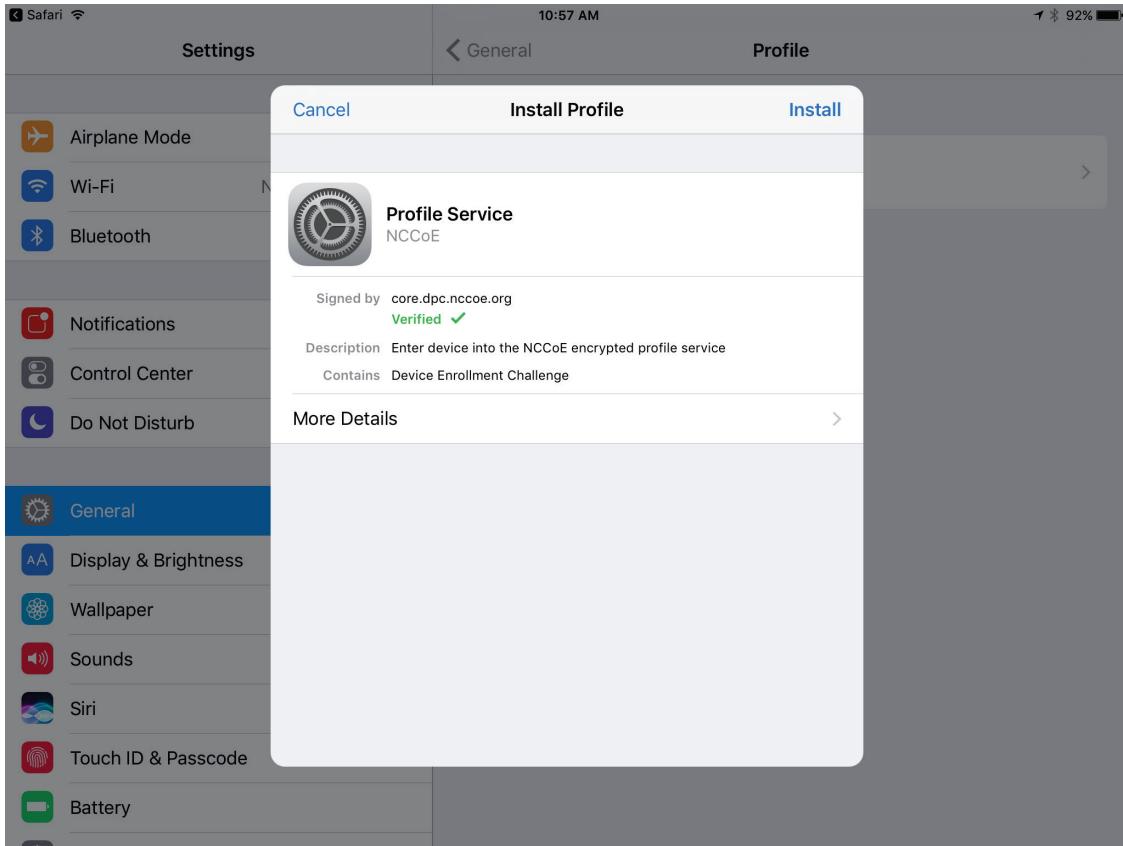
378

379     12. In the **Settings** app, in the **Install Profile** dialog:

380       a. In the **Signed By** field, confirm the originating server identity shows as **Verified**.

381           **Note:** If verification of the originating server fails, contact your MobileIron administrator  
382           before resuming registration.

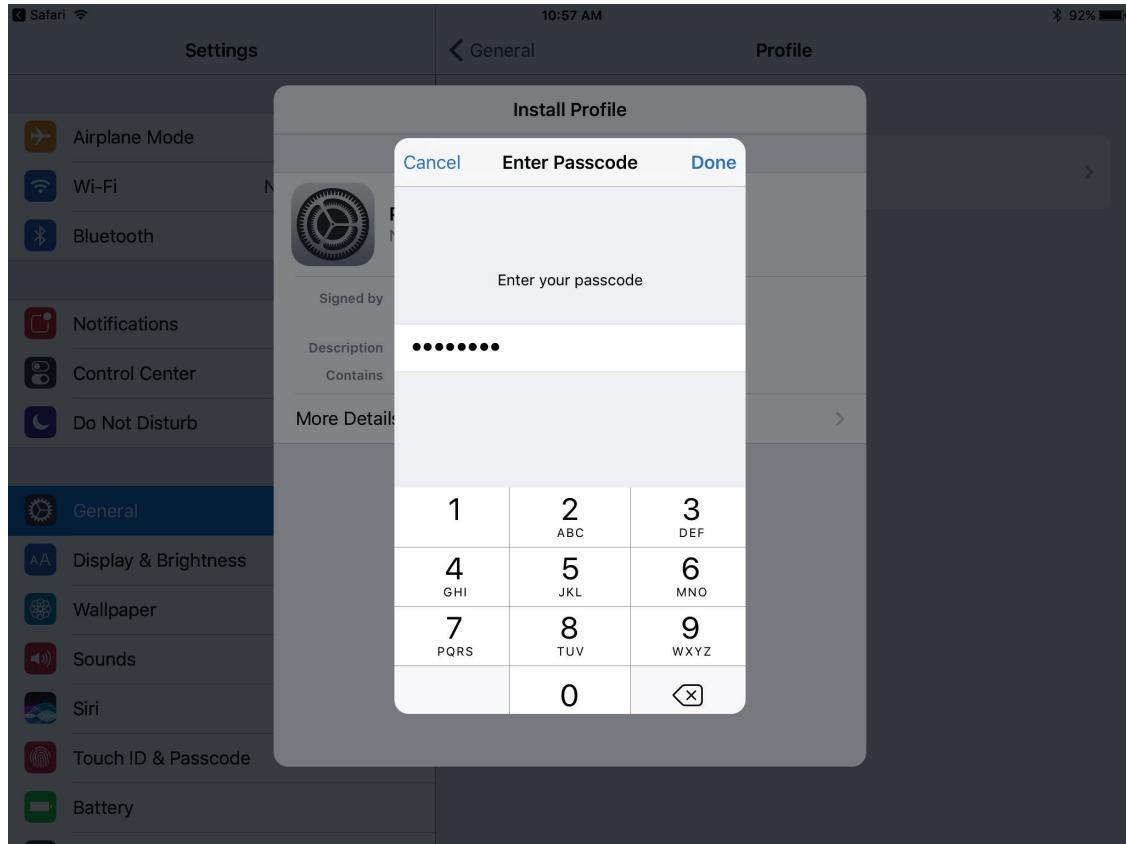
383       b. Tap **Install**.



384

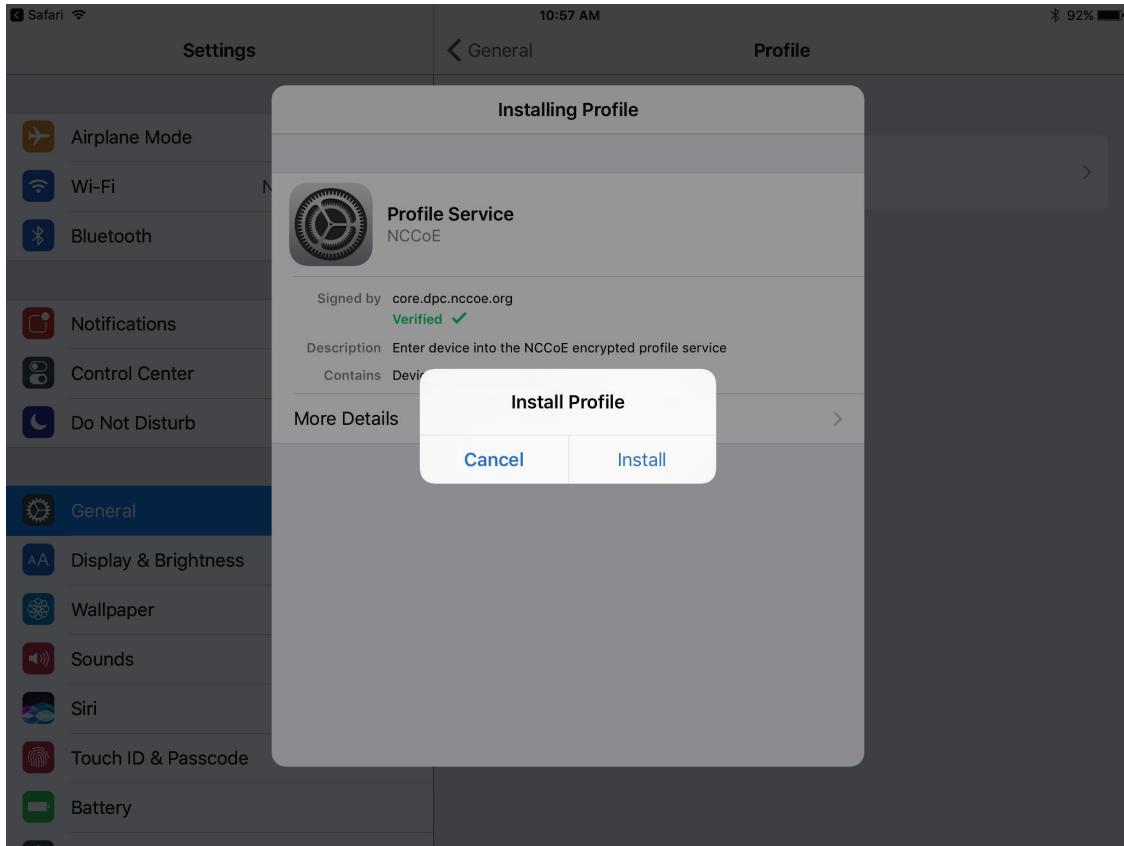
385     13. In the Enter **Passcode** dialog:

- 386       a. Enter your device unlock code.  
387       b. Tap **Done**.



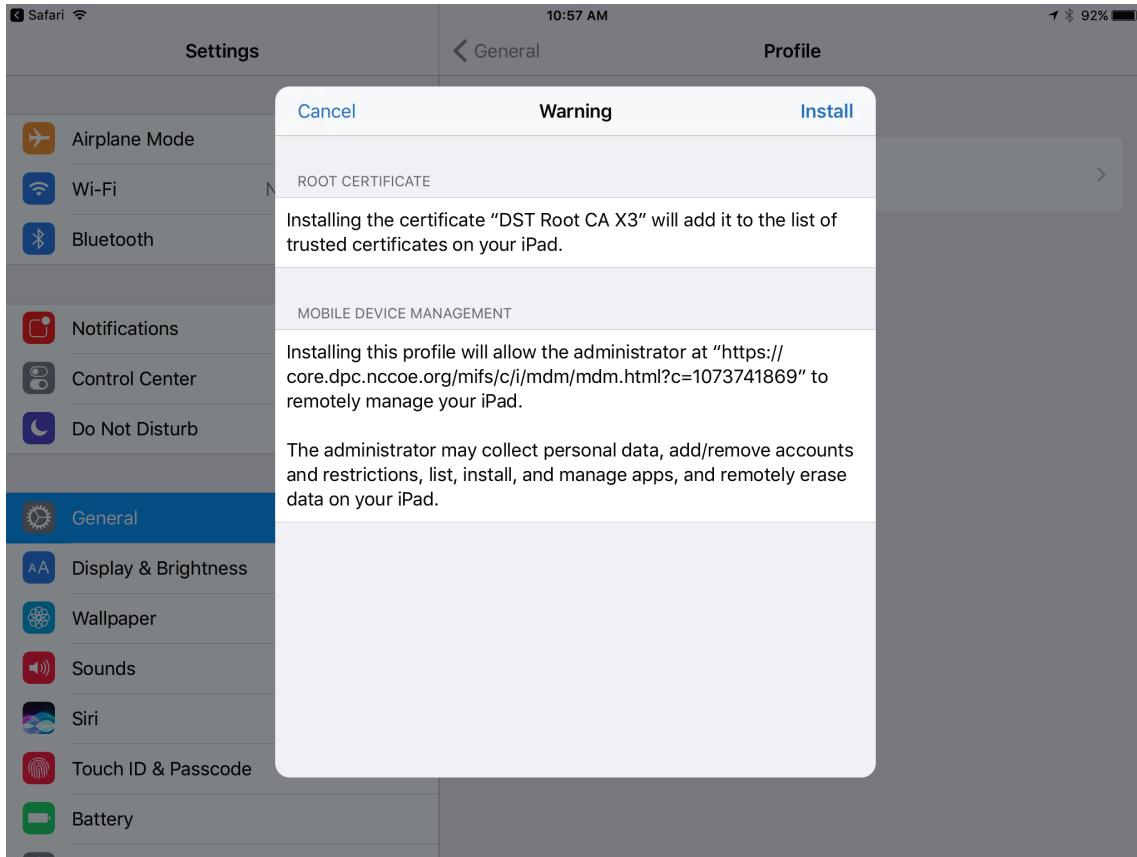
388

389     14. In the **Install Profile** dialog, tap **Install**.



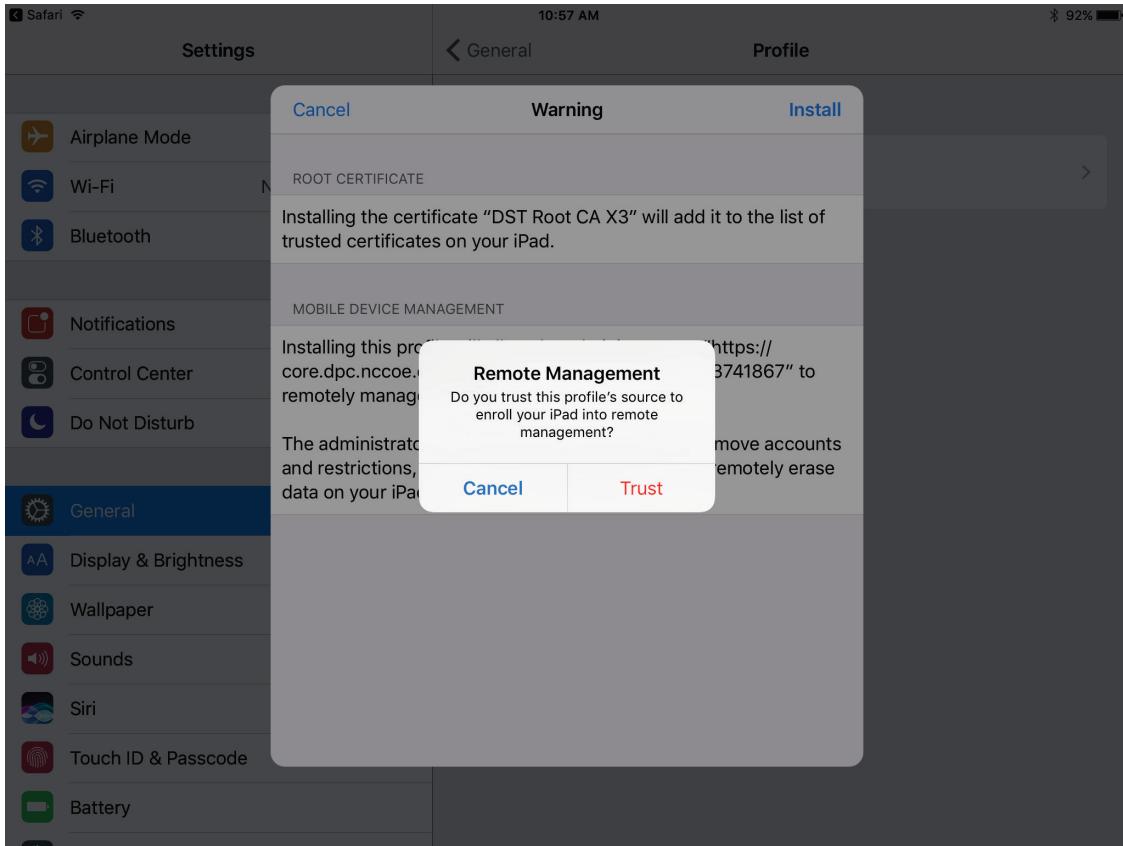
390

391     15. In the **Warning** dialog, tap **Install**.



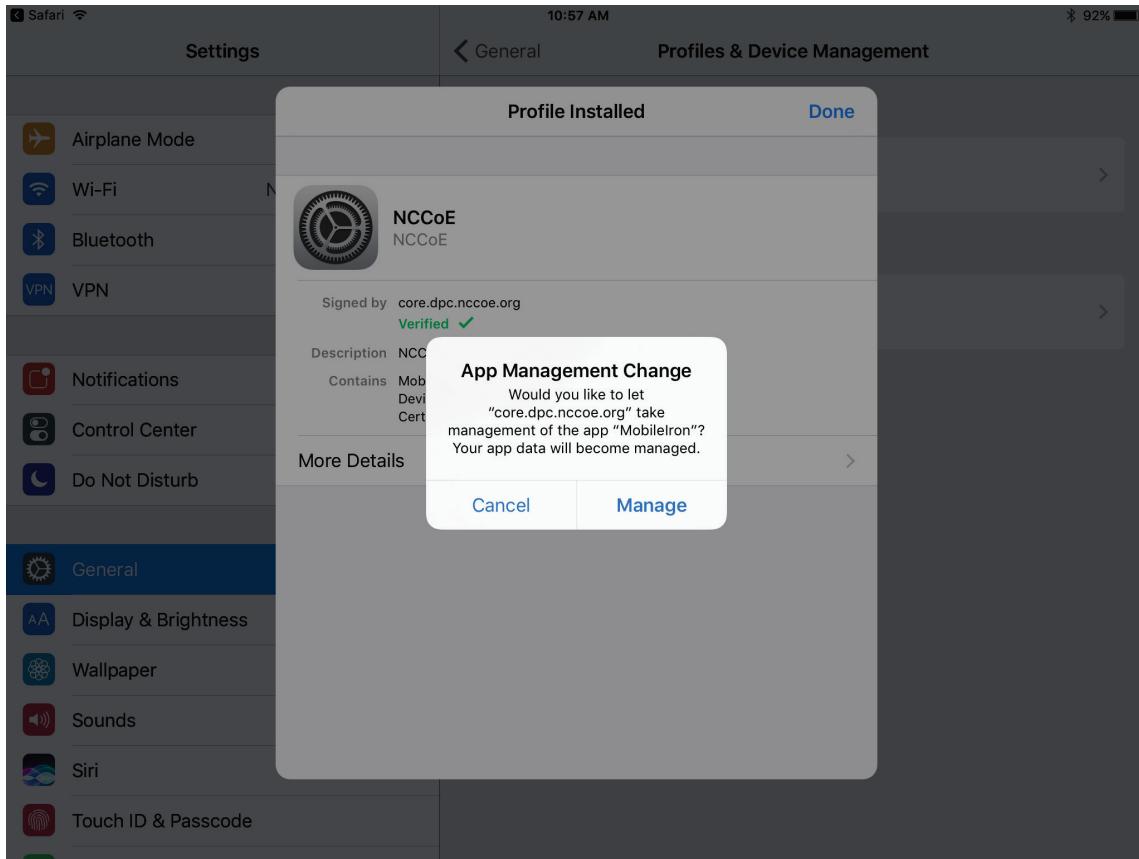
392

393     16. In the **Remote Management** dialog, tap **Trust**.



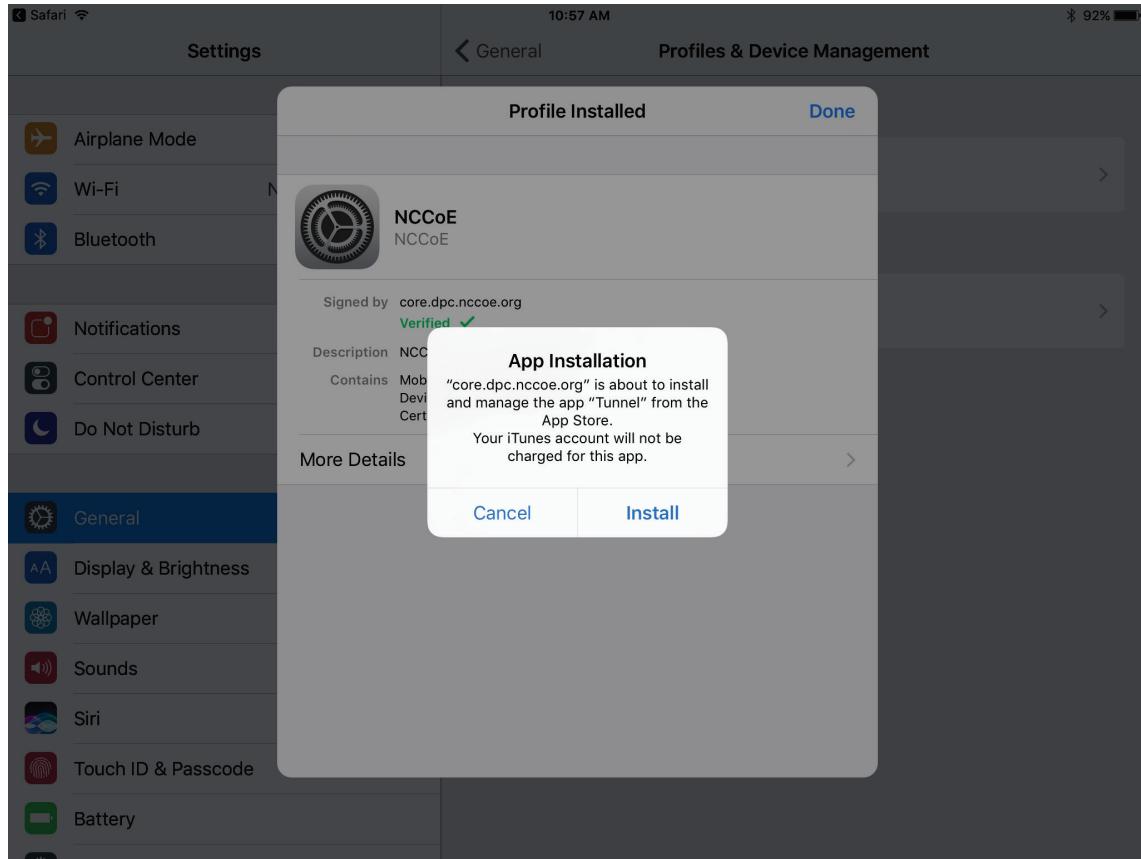
394

- 395     17. In the **Profile Installed** dialog, tap **Done**.
- 396     18. In the **App Management Change** dialog, tap **Manage**.



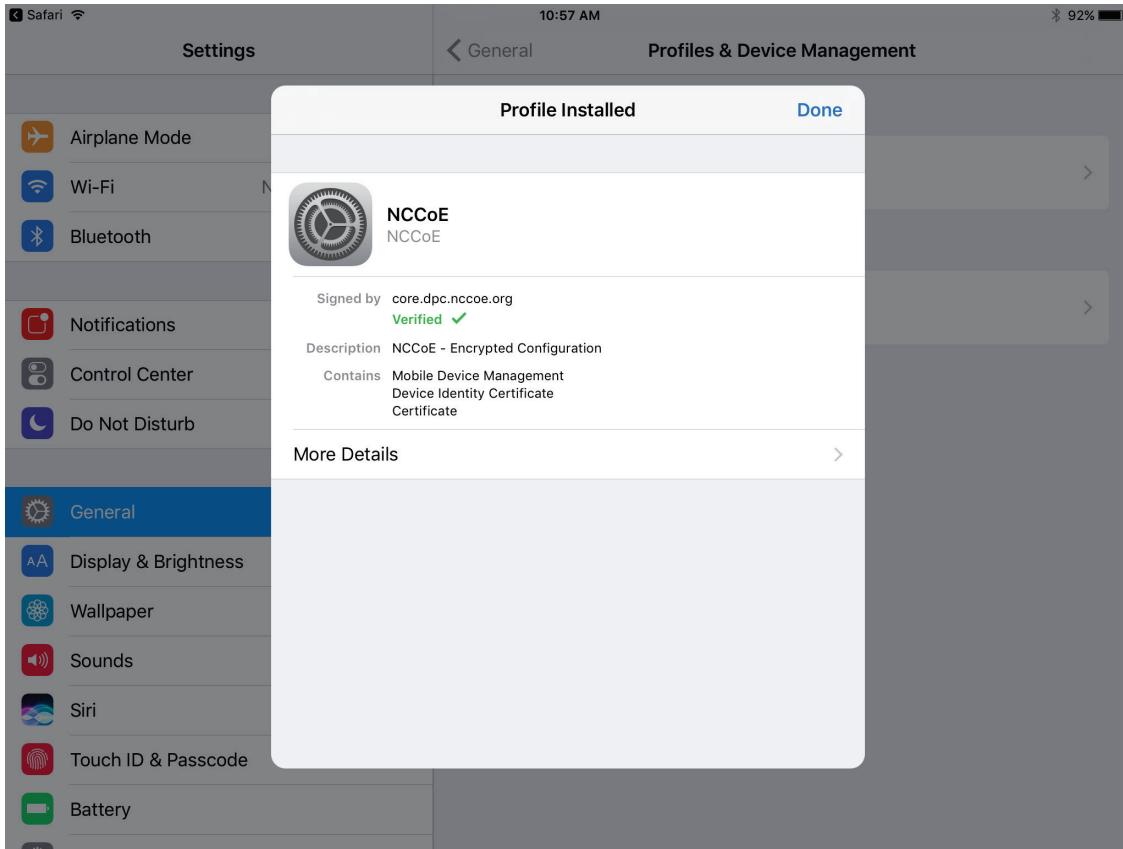
397

- 398     19. If additional Mobile@Work apps (e.g., Email+) are installed as part of the MobileIron management profile (based on your organization's use case), an **App Installation** dialog will appear for  
399       each app. To confirm, tap **Install**.  
400



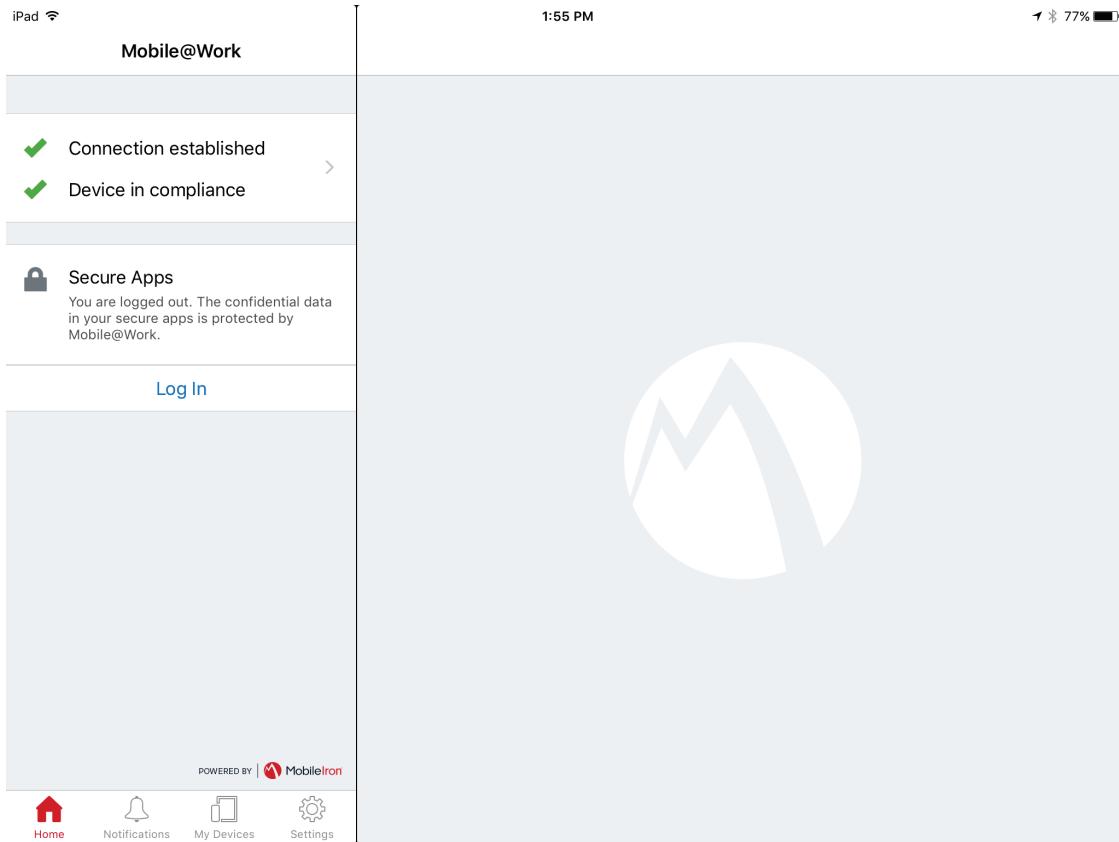
401

20. In the **Profile Installed** dialog, tap **Done**.



403

- 404 21. The **Mobile@Work > Home** screen should now display checkmarks for both status indicators of  
405 **Connection established** (with MobileIron Core) and **Device in compliance** (with the MobileIron  
406 policies that apply to your device).



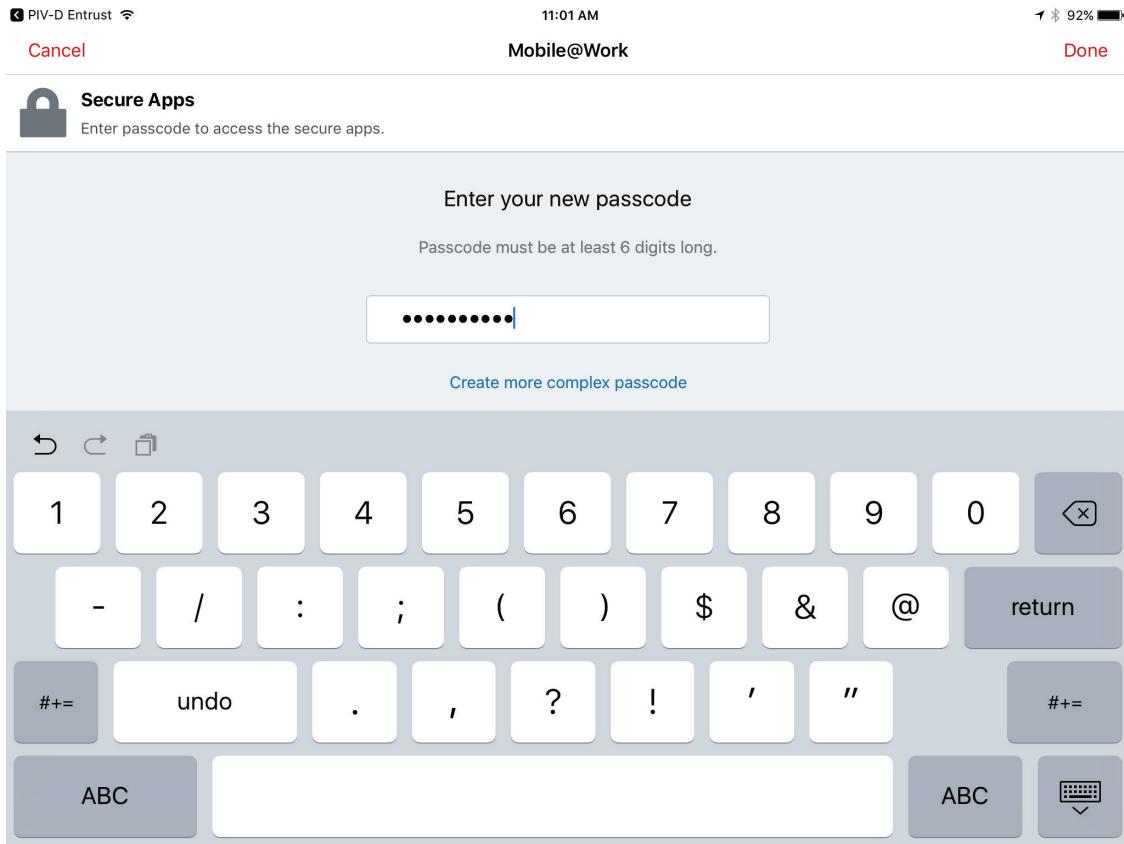
407

### 408 2.3.1.2 DPC Initial Issuance

409 The following steps demonstrate how a DPC is issued to an applicant's mobile device. It assumes the  
 410 target mobile device is registered with MobileIron (see Register Target Device with MobileIron) and the  
 411 MobileIron PIV-D Entrust app is installed (see Implement MobileIron Guidance). These steps are  
 412 completed by the mobile device user who is receiving a DPC.

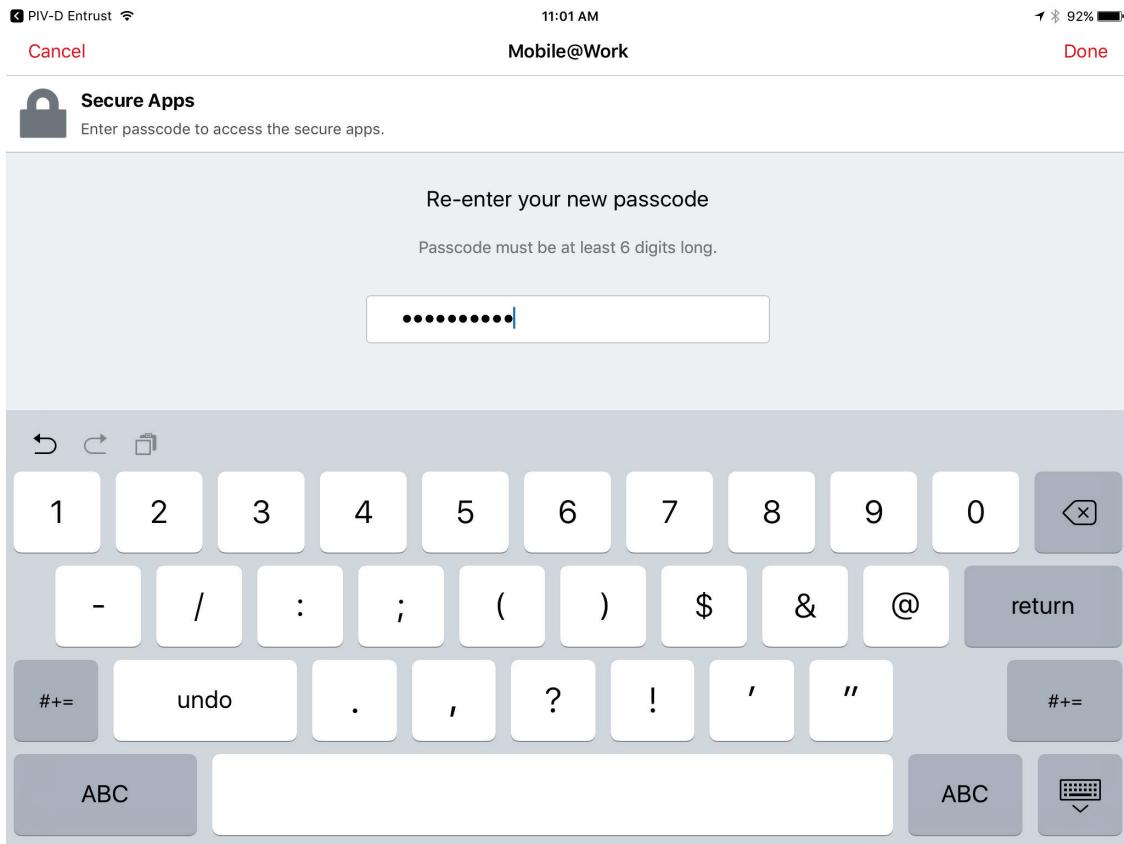
- 413 1. Launch the **MobileIron PIV-D Entrust** app on the target mobile device.
- 414 2. If a Mobile@Work Secure Apps passcode has not been set, you will be prompted to create one.  
 415 In the **Mobile@Work Secure Apps** screen:
  - 416 a. In the **Enter your new passcode** field, enter a password consistent with your organiza-  
 417 tion's DPC password policy. This password will be used to activate your DPC (password-  
 418 based Subscriber authentication) for use by Mobile@Work secure apps.

419 Note: NIST SP 800-63-3 increased the minimum DPC password length to eight characters.



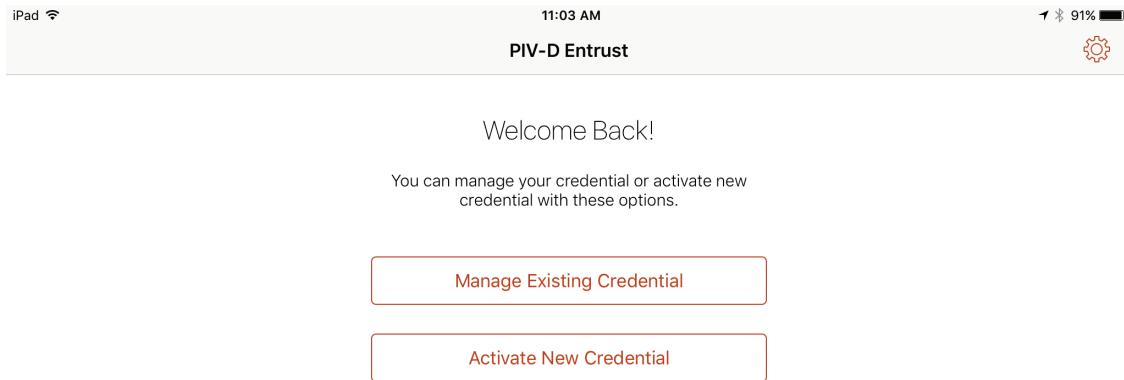
420

- 421      b. In the **Re-Enter your new passcode** field, re-enter the password you entered in **Step 2b**.  
422      c. Tap **Done**.



423

- 424     3. Following registration with MobileIron Core and when no Derived PIV Credential is associated  
425       with Mobile@Work, **PIV-D Entrust** displays a screen for managing your DPC. You will return to  
426       this app in a later step.

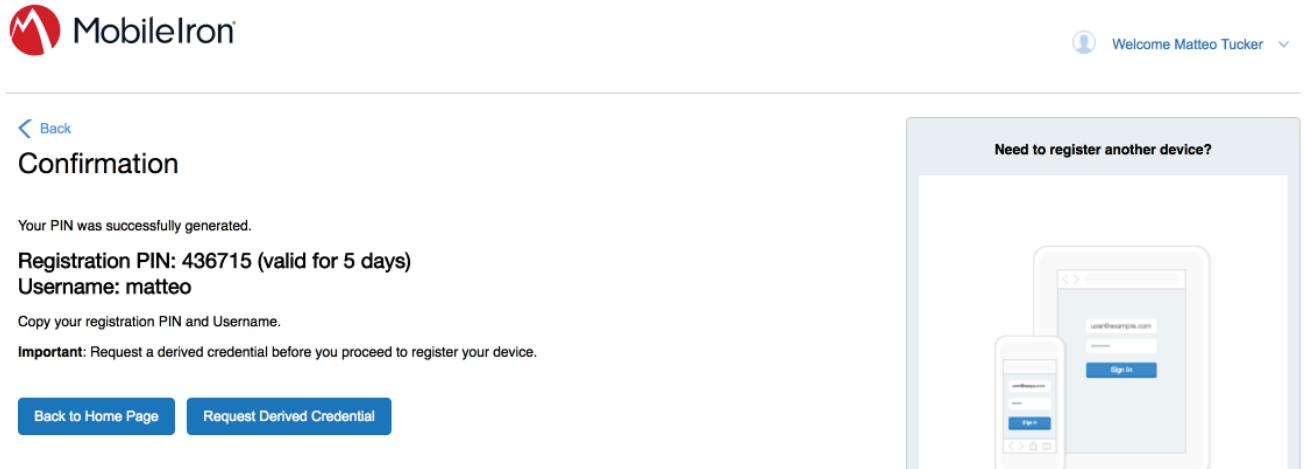


427

428     4. Insert your valid PIV Card into the reader attached to your laptop or computer workstation.

429        5. To request a Derived PIV Credential during the same session as registration with MobileIron:

430            a. In the MobileIron Self-Service Portal **Confirmation** page (see Figure 2-2), click **Request Derived Credential**.



The screenshot shows the MobileIron Self-Service Portal Confirmation page. At the top, there is a logo and a welcome message: "Welcome Matteo Tucker". Below the header, the page title is "Confirmation". A success message states "Your PIN was successfully generated." followed by "Registration PIN: 436715 (valid for 5 days)" and "Username: matteo". There is a note to "Copy your registration PIN and Username." and an important instruction: "Important: Request a derived credential before you proceed to register your device." At the bottom, there are two buttons: "Back to Home Page" and "Request Derived Credential". To the right of the main content, a modal window titled "Need to register another device?" displays an illustration of two mobile devices showing a login screen with the URL "usethesample.com".

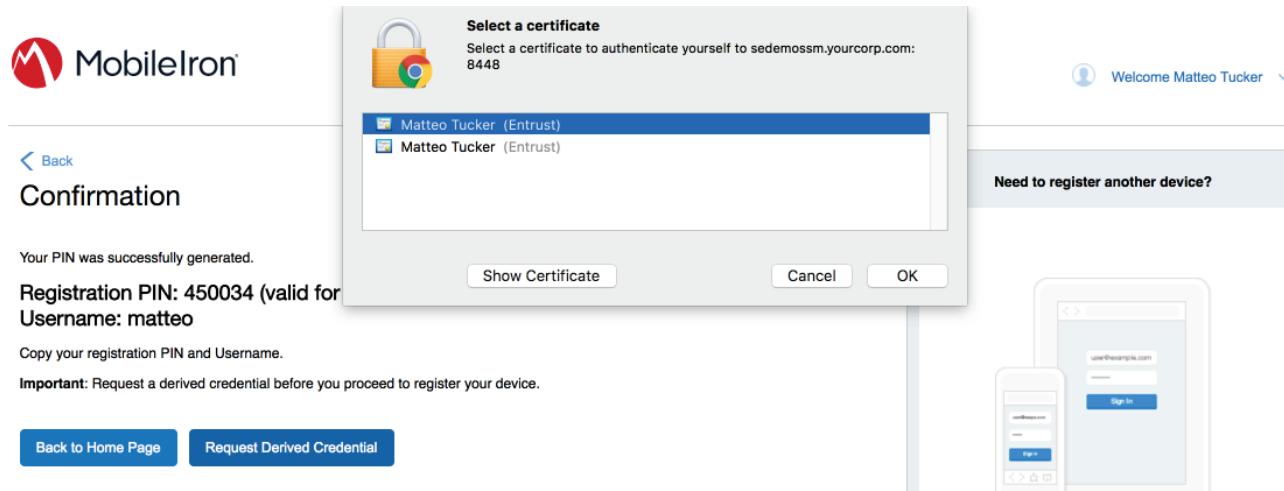
431

432            b. In the certificate selection dialog:

433              i. Select your PIV Authentication certificate from the list of available certificates. See **Step 4** of  
434              [Section 2.3.1.1](#) for additional steps to identify this certificate, as necessary.

435              ii. Click **OK**.

436              iii. Continue with **Step 7**.

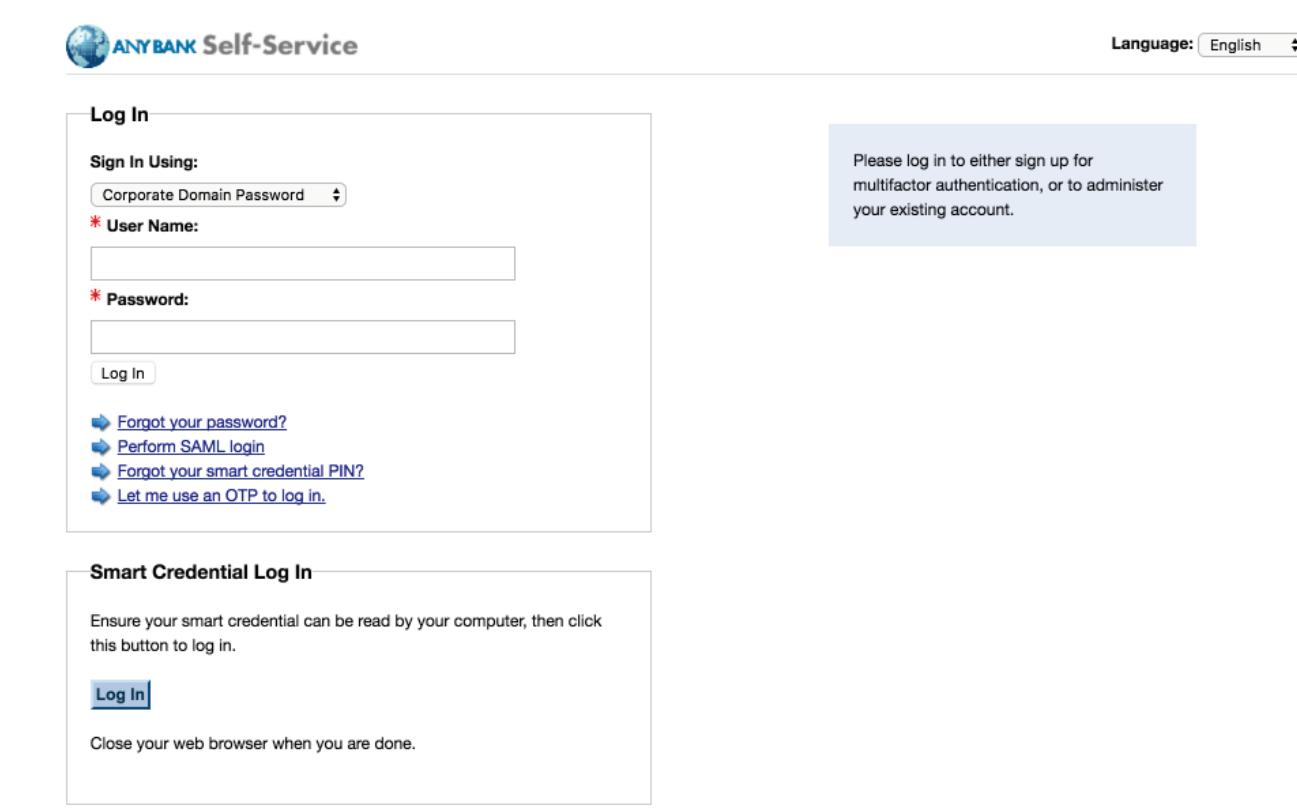


437

438     6. To request a Derived PIV Credential in a new session:

- 439         a. Using a web browser, visit the Entrust IDG Self-Service Portal URL provided by an administrator.
- 440         b. In the Entrust IDG Self-Service portal, under **Smart Credential Log In**, click **Log In**.

441         Note: The portal used in our test environment is branded as a fictitious company, AnyBank Self-Service.



The screenshot shows the ANYBANK Self-Service Log In page. At the top right, there is a language selection dropdown set to English. The main form area has a title "Log In" and a sub-section "Sign In Using:" with a dropdown menu showing "Corporate Domain Password". Below this are fields for "User Name" and "Password", both marked with red asterisks. A "Log In" button is located below the password field. To the right of the main form is a light gray sidebar containing the text: "Please log in to either sign up for multifactor authentication, or to administer your existing account." At the bottom of the main form, there is a "Smart Credential Log In" section with instructions to ensure a smart credential is readable by the computer and then click a "Log In" button. It also includes a note to close the browser after use.

442

443

c. In the **Select a certificate** dialog:

444

445

i. Select your PIV Authentication certificate from the list of available certificates. See **Step 4 of Section 2.1.3.1** for additional steps to identify this certificate, as necessary.

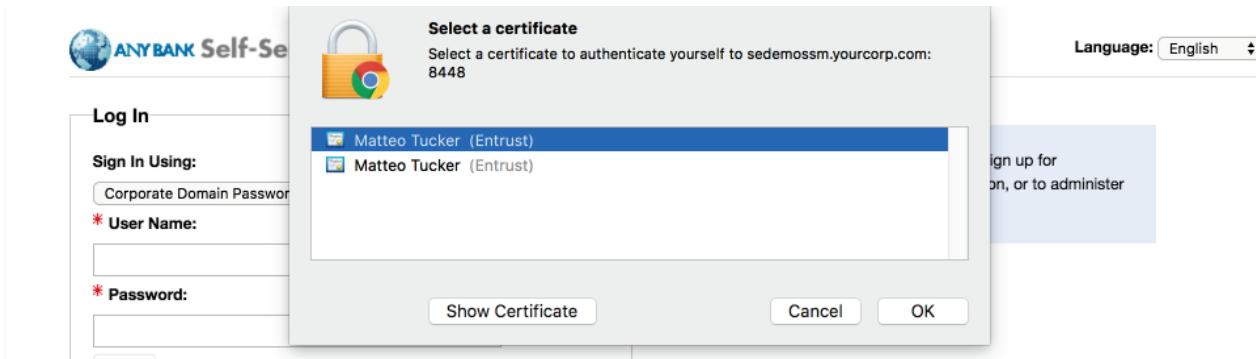
446

ii. Click **OK**.

447

448

- d. In the authentication dialog:
- In the **PIN** field, enter the password to activate your PIV Card.
  - Click **OK**.



449

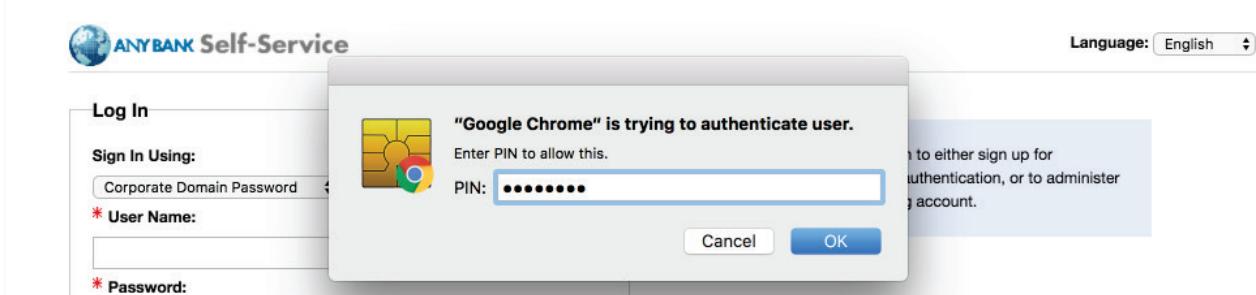
450

451

452

453

7. On the **Self-Administration Actions** page, follow the **I'd like to enroll for a derived mobile smart credential link** (displayed below as the last item; this may vary based on which self-administration actions your Entrust IDG administrator enabled).





**ANYBANK Self-Service**

Language: English

**Self-Administration Actions**

Please select one of the actions below or click Done if you're finished:

- [I'd like to update my personal information.](#)
- [I'd like to request a grid.](#)
- [I'd like to change my Entrust IdentityGuard password.](#)
- [I've forgotten my Entrust IdentityGuard password.](#)
- [I'd like to request a soft token.](#)
- [I'd like to unblock my smart credential.](#)
- [I've permanently lost my smart credential or it has been compromised.](#)
- [I've temporarily forgotten or misplaced my smart credential.](#)
- [I'd like to enroll for a derived mobile smart credential.](#)

454

- 455     8. On the **Smart Credential enabled Application** page, select **Option 2: I've successfully down-**  
 456       **loaded and installed the Smart Credential enabled application.**



**ANYBANK Self-Service**

Language: English

**Smart Credential enabled Application**

Please select the option that best matches your current situation:

1.  I haven't attempted to download the Smart Credential enabled application yet.
2.  I've successfully downloaded and installed the Smart Credential enabled application.
3.  I want to cancel my request for the Smart Credential enabled application.

457

- 458     9. On the **Derived Mobile Smart Credential** page:
- 459       a. In the **Identity Name** field, enter your LDAP or MobileIron user ID.  
 460       b. Click **OK**.

 ANYBANK Self-Service

Language: English

Derived Mobile Smart Credential

Enter any name you would like to use to identify your new derived mobile smart credential identity.

\* Identity Name:

On the next page, a QR code will be displayed that contains the data required to activate your derived mobile smart credential. You should open the derived mobile smart credential app on your mobile device and scan the QR code.

In addition to the QR code, the next page will also display a password that is required to unlock the activation data contained in the QR code.

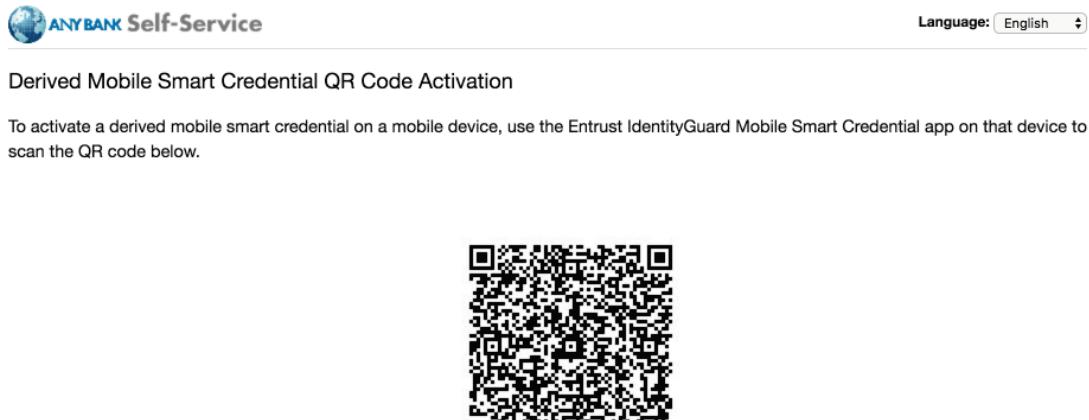
Your derived mobile smart credential will be associated with the email address associated with the account named Email.

461

462 10. The **Derived Mobile Smart Credential QR Code Activation** page displays information used in  
 463 future steps; keep this page displayed. The workflow resumes using the MobileIron PIV-D En-  
 464 trust app open on the target mobile device.

465 Note: **Steps 11-13** must be completed using the target mobile device within approximately  
 466 three minutes or **Steps 7-10** must be repeated to generate new activation codes.

467 **Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page**



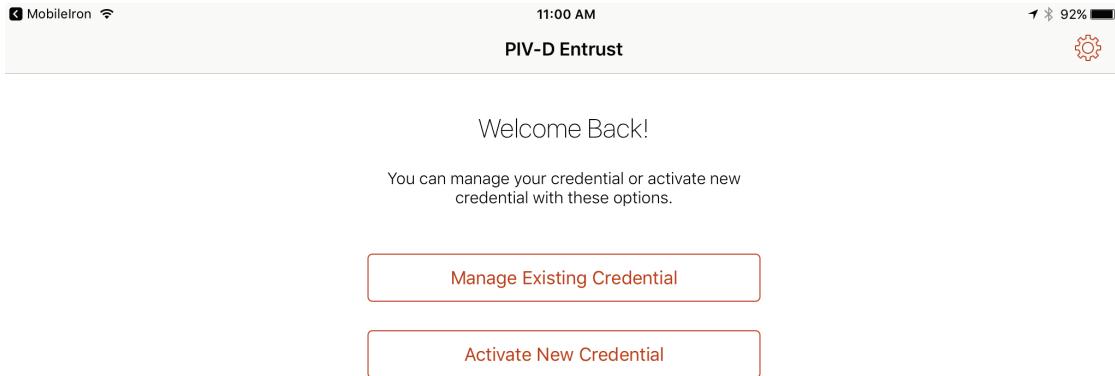
**82291766**

To complete activation, you must provide the Entrust IdentityGuard Mobile Smart Credential app with the password displayed above.

You will have approximately 3 minutes to complete the activation of your derived mobile smart credential.

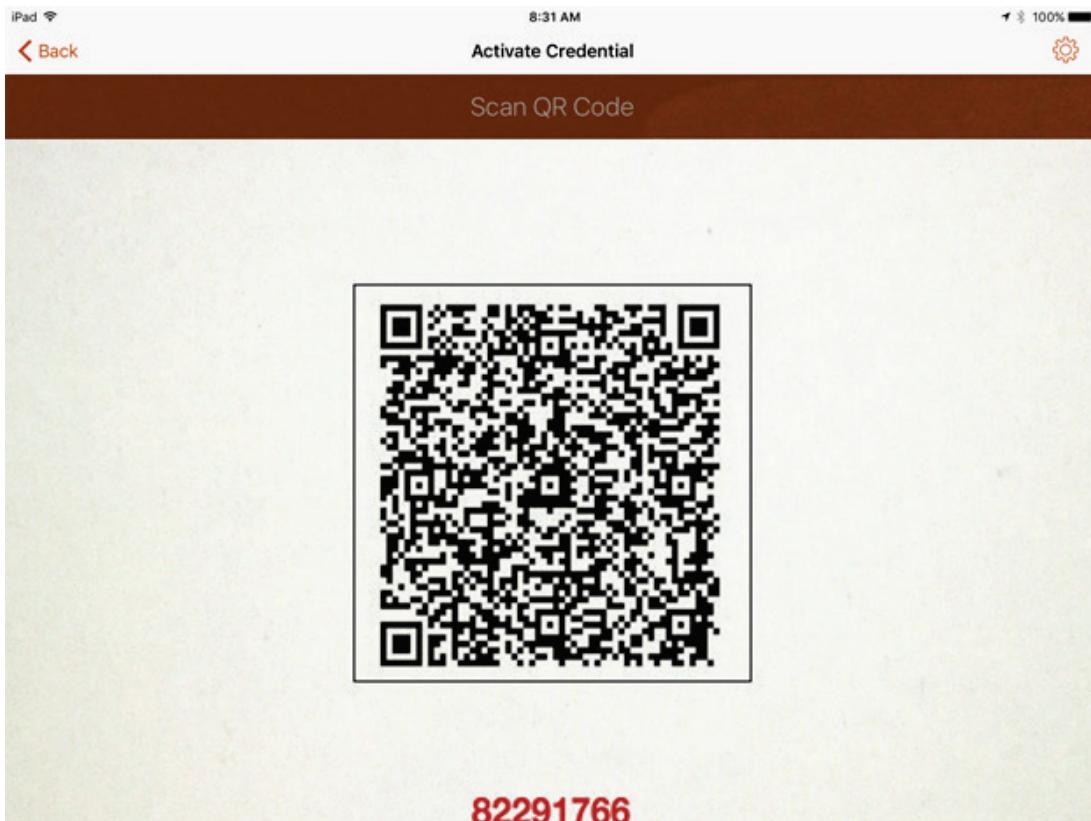
468

469 11. In the **PIV-D Entrust** app running on the target mobile device, tap **Activate New Credential**.



470

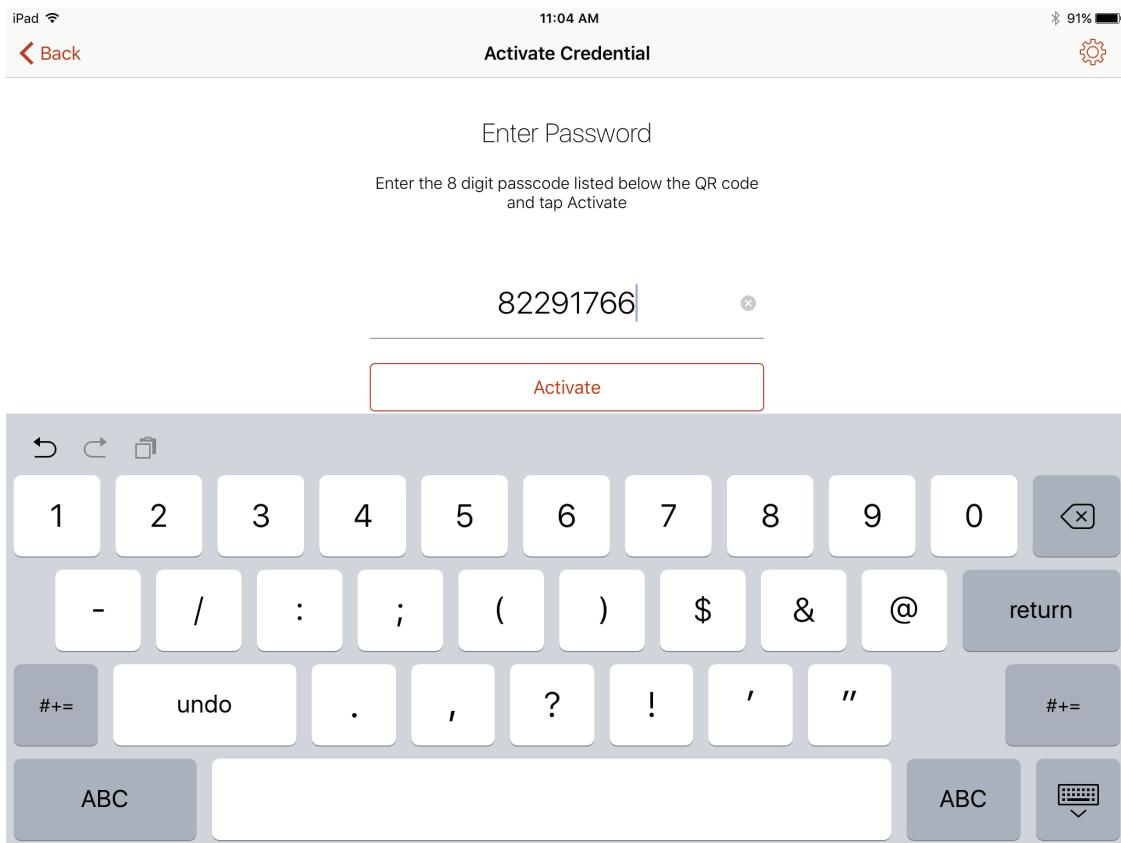
- 471    12. Use the device camera to capture the QR code displayed on the **Derived Mobile Smart Credential QR Code Activation** page as represented in Figure 2-3.
- 472



473

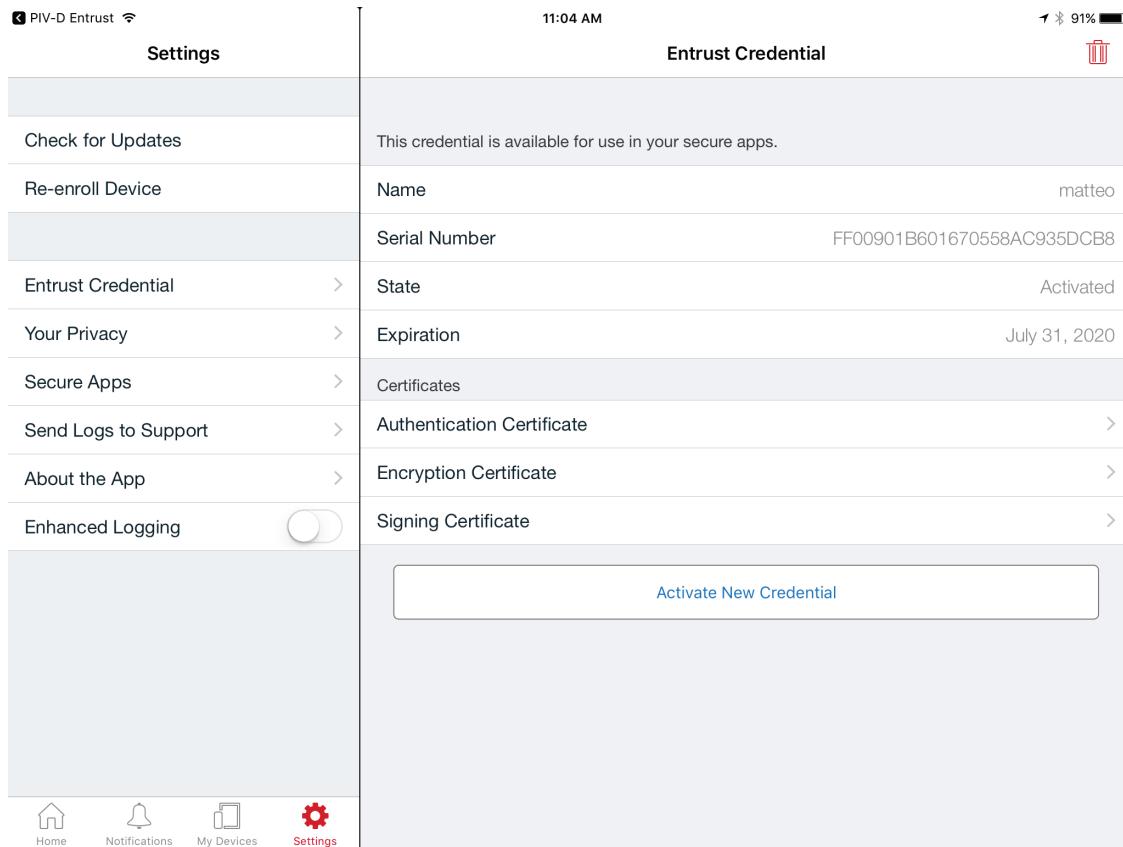
474        13. On the **Activate Credential** screen:

- 475        a. Enter the **password** below the QR code displayed on the **Derived Mobile Smart Creden-**  
476        **tial QR Code Activation** page (displayed by the same device used to perform **Steps 4-**  
477        **10**) as represented in Figure 2-3.
- 478        b. Tap **Activate**.



479

- 480        14. If issuance was successful, the PIV-D Entrust app should automatically launch MobileIron. Go to  
481        **Mobile@Work > Settings > Entrust Credential** to view its details.



482

### 483 2.3.2 DPC Maintenance

484 Changes to a DPC Subscriber's PIV Card that result in a re-key or reissuance (e.g., official name change)  
 485 require the subscriber to repeat the initial issuance workflow as described in the previous section. The  
 486 issued DPC will replace any existing DPC in the MobileIron Apps@Work container.

### 487 2.3.3 DPC Termination

488 Termination of a DPC can be initiated from the MobileIron Admin Console. Upon completion of this  
 489 workflow, the DPC stored in the MobileIron Apps@Work container will be cryptographically wiped  
 490 (destroyed). These steps are performed by a MobileIron Core administrator.

- 491 1. In the MobileIron Admin Console, navigate to **Devices & Users > Devices**.

	DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
<input type="checkbox"/>	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
<input type="checkbox"/>	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32
<input type="checkbox"/>	Matteo Tucker	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03

492

- 493 2. Select the **checkbox** in the row identifying the mobile device to be retired.

	DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
<input type="checkbox"/>	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
<input type="checkbox"/>	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32
<input checked="" type="checkbox"/>	Matteo Tucker	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03

494

- 495 3. Select **Actions > Retire**.

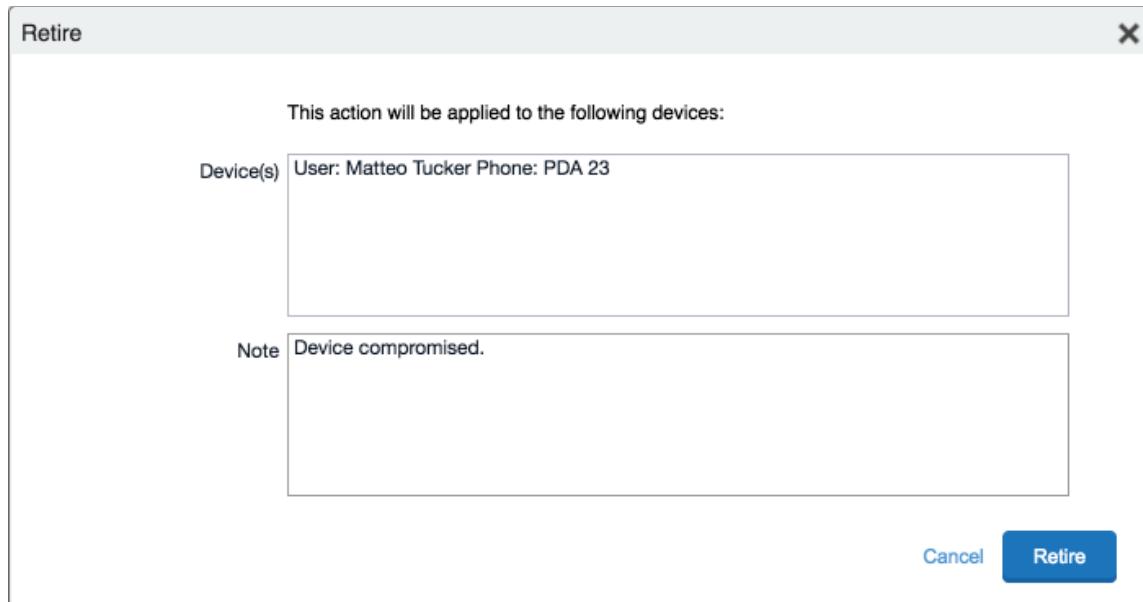
- Force Device Check-In
- Check Compliance
- Set Custom Attributes
- Apply to Label
- Remove from Label
- Lock
- Unlock Device
- Change Language
- Change Ownership
- Send Message
- More Actions... ▾
- Android Only ▾
- iOS Only ▾
- Windows Only ▾
- Wipe
- Cancel Wipe
- Retire**

496

497        4. In the **Retire** dialog that appears:

498            a. In the **Note** textbox, enter the reason(s) the device is being retired from MobileIron.

499            b. Select **Retire**.



500

501        5. The **Devices** tab no longer displays the retired mobile device in the list of the devices.

	DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
<input type="checkbox"/>	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3	Active	2017-06-09 09:29:38	
<input type="checkbox"/>	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0	Active	2017-06-05 10:14:32	

502

503        The MobileIron PIV-D Entrust app now no longer reflects management by MobileIron. As a result, the  
504        Derived PIV Credential has been cryptographically wiped (destroyed) and its recovery is computationally  
505        infeasible.

## Appendix A List of Acronyms

<b>AD</b>	Active Directory
<b>API</b>	Application Programming Interface
<b>CA</b>	Certificate Authority
<b>CAPI</b>	Cryptographic Application Programming Interface
<b>CMS</b>	Credential Management System
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>DMZ</b>	Demilitarized Zone
<b>DN</b>	Distinguished Name
<b>DPC</b>	Derived PIV Credential
<b>EEM</b>	Enterprise Mobility Management
<b>FASC-N</b>	Federal Agency Smart Card Number
<b>FIPS</b>	Federal Information Processing Standards
<b>IDG</b>	Identity Guard
<b>IT</b>	Information Technology
<b>JCE</b>	Java Cryptography Extension
<b>JTK</b>	Java Tool Kit
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>OU</b>	Organizational Unit
<b>PFX</b>	Personal Exchange Format
<b>PIN</b>	Personal Identification Number
<b>PIV</b>	Personal Identity Verification
<b>PKI</b>	Public Key Infrastructure
<b>QR</b>	Quick Response [code]
<b>RSA</b>	Rivest-Shamir-Adleman
<b>SCEP</b>	Simple Certificate Enrollment Protocol
<b>SP</b>	Special Publication
<b>SQL</b>	Structured Query Language
<b>SSM</b>	Self-Service Module
<b>TLS</b>	Transport Layer Security

<b>UPN</b>	User Principal Name
<b>URL</b>	Universal Resource Locator
<b>UUID</b>	Universal Unique Identifier
<b>VLAN</b>	Virtual Local Area Network