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
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

SECOND DRAFT

This publication is available free of charge from:
https://www.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, 151 pages, (August 2018), 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

Public comment period: August 1, 2018 through October 1, 2018

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Federal Information Processing Standards (FIPS) Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals to federally controlled facilities, information systems, and applications, as part of access management. In 2005, when FIPS 201 was published, authentication of individuals was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV Card provides common multifactor authentication mechanisms through integrated or external smart card readers, where available. With the emergence of computing devices, such as tablets, hybrid computers, and, in particular, mobile devices, the use of PIV Cards has proved to be challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers, and require separate card readers attached to devices to provide authentication services. To extend the value of PIV systems into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the implementation and life cycle of identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. These NIST guidelines, published in 2014, describe Derived PIV Credentials (DPC) that leverage identity proofing and vetting results of current and valid PIV credentials.

To demonstrate the DPC guidelines, the NCCoE at NIST built two security architectures using commercial technology to enable the issuance of a Derived PIV Credential to mobile devices using ICAM shared services One option uses a software-only solution while the other leverages hardware built into many computing devices used today.

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

KEYWORDS

cybersecurity; Derived PIV Credential (DPC); enterprise mobility management (EMM); identity; mobile device; mobile threat; multifactor authentication; personal identity verification (PIV); PIV Card; smart card

ACKNOWLEDGMENTS

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
Dror Shilo	Intel Corporation
Simy Cohen	Intel Corporation
Abhilasha Bhargav-Spantzel	Intel Corporation
Carlton Ashley	Intel Corporation
Alfonso Villasenor	Intel Corporation
Won Jun	Intercede
Alan Parker	Intercede
Allen Storey	Intercede
Iain Wotherspoon	Intercede
Andre Varacka	Verizon
Russ Weiser	Verizon
Emmanuel Bello-Ogunu	The MITRE Corporation
Lorrayne Auld	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Poornima Koka	The MITRE Corporation

Name	Organization
Matthew Steele	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Entrust Datacard	Entrust IdentityGuard, Entrust Managed Services Public Key Infrastructure (PKI)
Intel Corporation	Intel Authenticate Solution
Intercede	MyID Credential Management System
MobileIron	MobileIron Enterprise Mobility Management (EMM) Platform
Verizon	Verizon Shared Service Provider (SSP) PKI

Contents

List of Figures

List of Tables

1 Introduction

This guide shows information technology (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, this guide shows 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 National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a Derived Personal Identity Verification (PIV) Credential (DPC) life-cycle solution. This reference design is modular and can be deployed in whole or in part.

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 following topics:

- challenges enterprises face in issuing strong, multifactor credentials to mobile devices
- the 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 *NIST SP 1800-12B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5.3, Risk, provides a description of the risk analysis we performed
- Section 3.5.4, 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 DPC solution.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-12C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the DPC example solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Vol B, Section 3.6, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

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

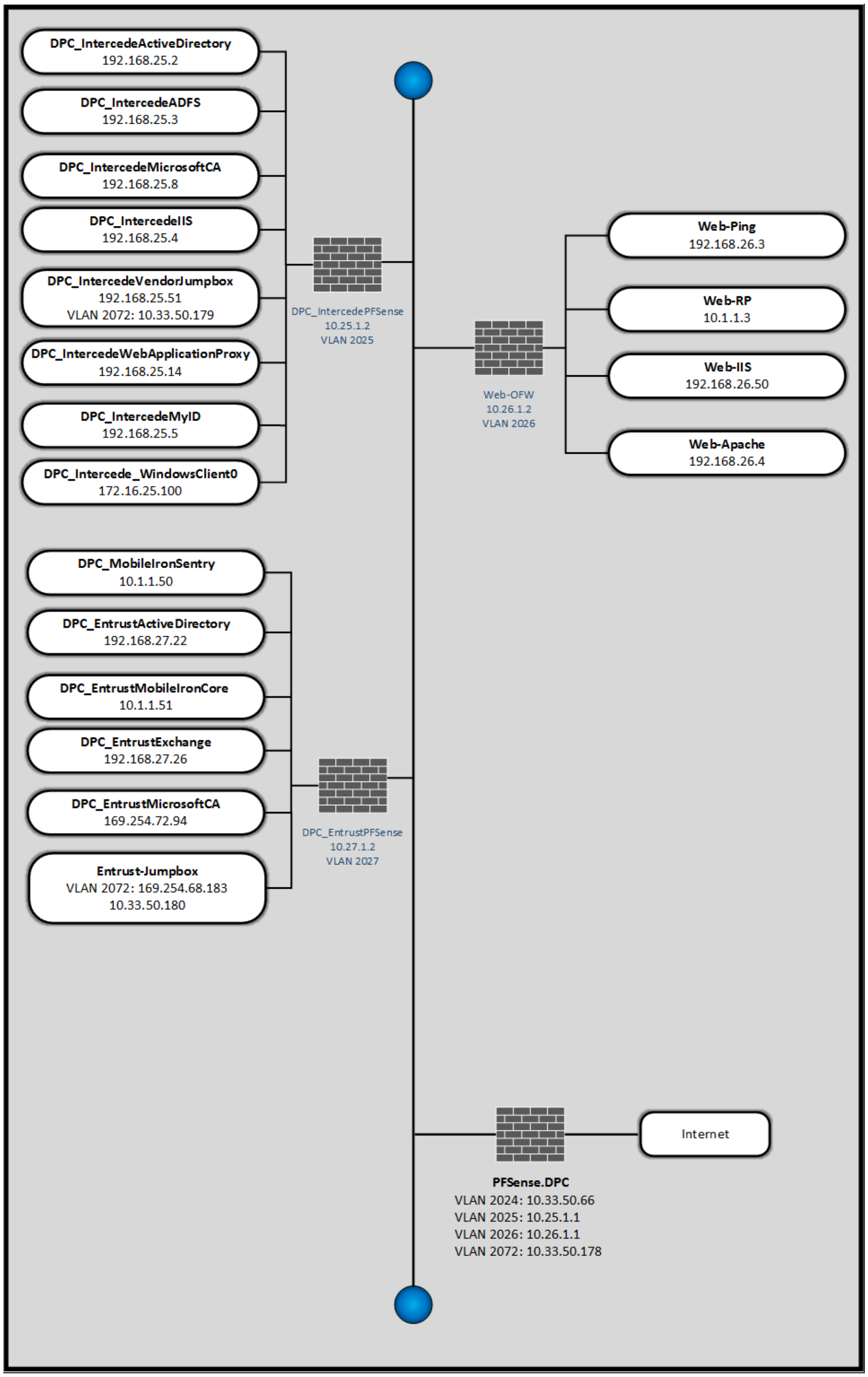
1.2 Build Overview

Unlike desktop computers and laptops that have built-in readers to facilitate the use of PIV Cards, mobile devices pose usability and portability issues because of the lack of a smart card reader.

NIST sought to address this issue with the introduction of the general concept of DPC in Special Publication (SP) 800-63-2, which leverages identity proofing and vetting results of current and valid credentials. Published in 2014, SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* defined requirements for initial issuance and maintenance of DPC. NIST's Applied Cybersecurity Division then created a National Cybersecurity Center of Excellence (NCCoE) project to provide an example implementation for federal agencies and private entities that follows the requirements in SP 800-157.

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

Figure 1-1 Lab Network Diagram



1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

2 Product Installation Guides

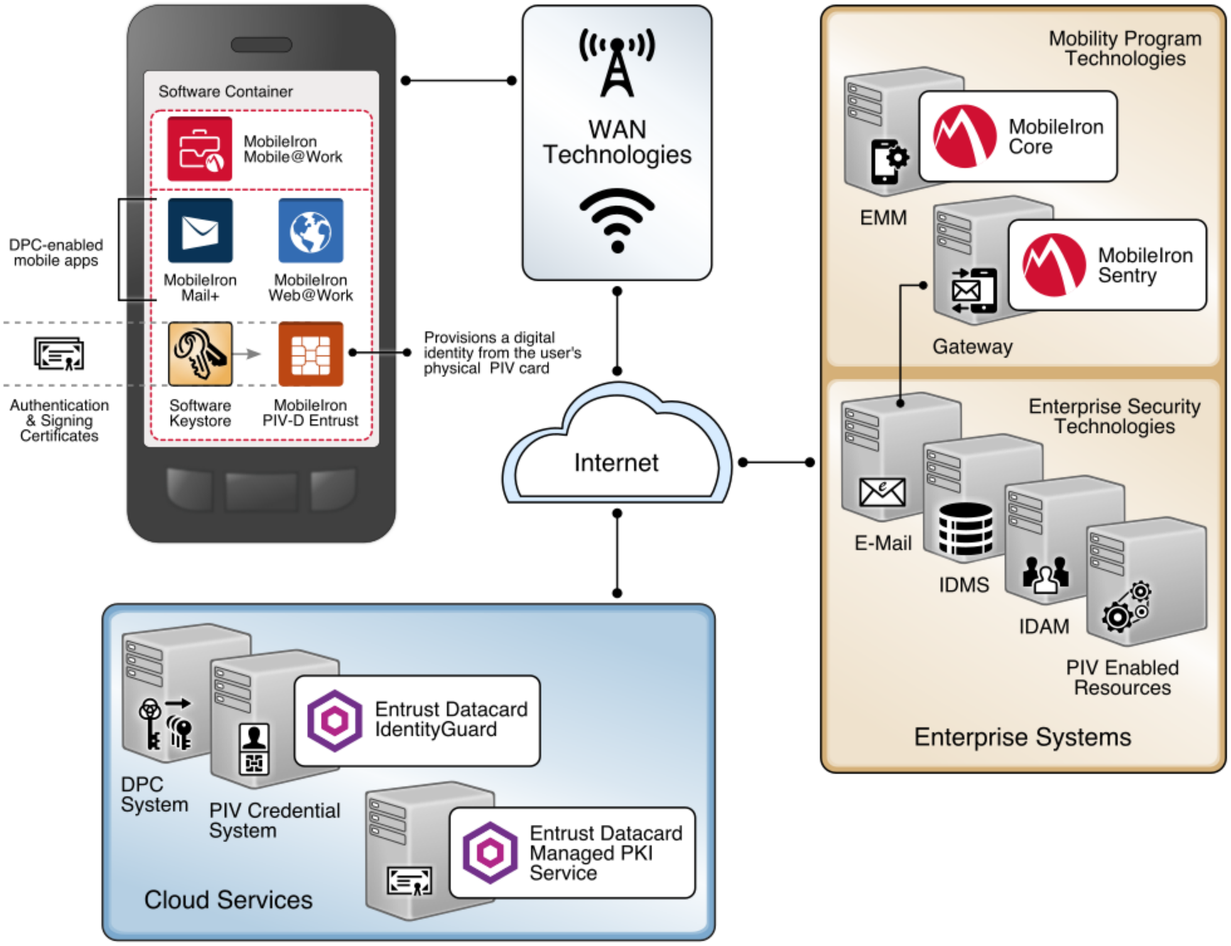
This section of the practice guide contains detailed instructions for installing and configuring key products used for the depicted architectures documented below, as well as demonstration of the DPC lifecycle management activities of initial issuance and termination.

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

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

2.1 Managed Service Architecture with Enterprise Mobility Management (EMM) Integration

Figure 2-1 Architecture



2.1.1 Entrust Datacard IdentityGuard (IDG)

Entrust Datacard contributed test instances of its managed public key infrastructure (PKI) service and IdentityGuard products, the latter of which directly integrates with MobileIron to support the use of DPC with MobileIron Mobile@Work applications. Contact Entrust Datacard (https://www.entrust.com/contact/) to establish service instances in support of DPC with MobileIron (https://www.mobileiron.com/).

2.1.1.1 Identity Management Profiles

To configure services and issue certificates for DPC that will work with your organization's user identity profiles, Entrust Datacard will need information on how identities are structured and which users will use PKI services. For this lab instance, Entrust Datacard issued PIV Authentication, Digital Signature, and Encryption certificates for PIV Cards and DPC for two test identities, as represented in Table 2-1.

Table 2-1 Identity Management Profiles

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

2.1.2 MobileIron Core

MobileIron Core is the central product in the MobileIron suite. The following sections describe the steps for installation, configuration, and integration with Active Directory and the Entrust Datacard IdentityGuard managed service. Key configuration files used in this build are listed in Table 2-2 and are available from the NCCoE DPC project website.

Table 2-2 MobileIron Core Settings

File Name	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 DPC to devices

2.1.2.1 Installation

Follow the steps below to install MobileIron Core:

1. Obtain a copy of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* from the MobileIron support portal.

2. Follow the MobileIron Core pre-deployment and installation steps in Chapter 1 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.

2.1.2.2 General MobileIron Core Setup

The following steps are necessary for mobile device administrators or users to register devices with MobileIron, which is a prerequisite to issuing DPC.

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

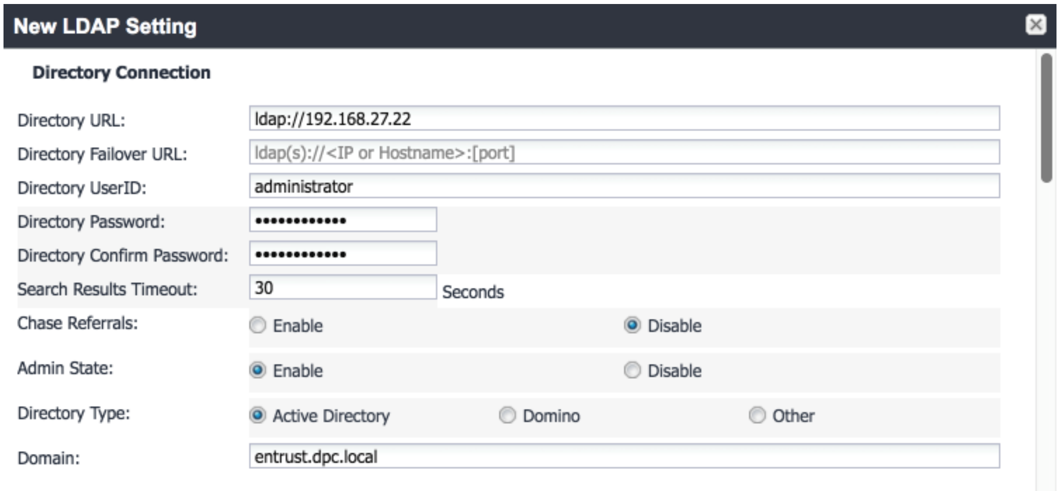
2.1.2.3 Configuration of MobileIron Core for DPC

The following steps will reproduce this configuration of MobileIron Core.

2.1.2.3.1 Integration with Active Directory

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

1. From Step 4 in the MobileIron guide, in the **New LDAP Server** dialogue:
   a. Directory Connection:

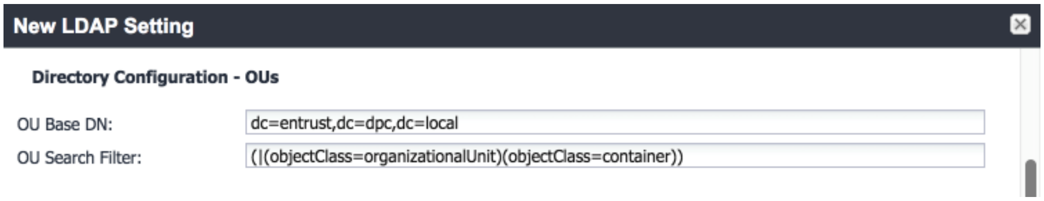


New LDAP Setting

Directory Connection

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

b. Directory Configuration—OUs:

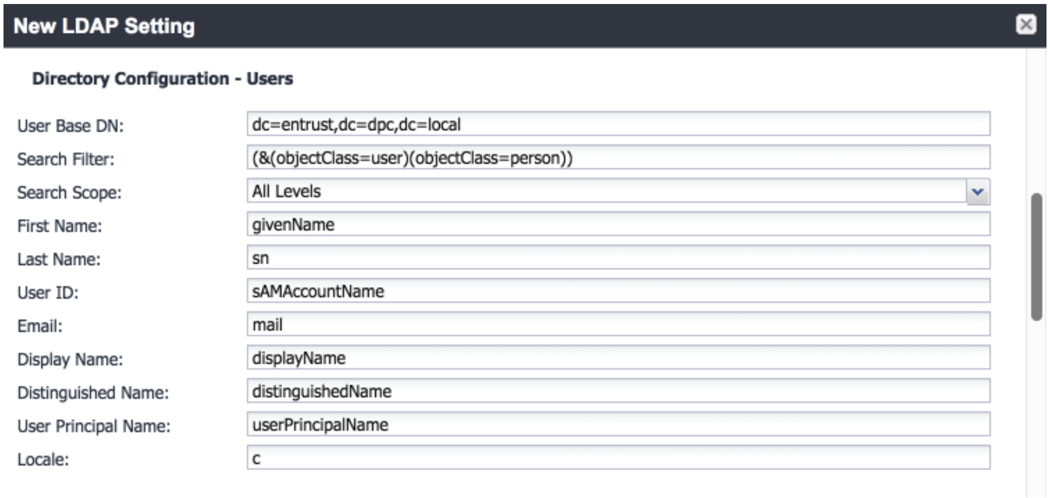


Directory Configuration - OUs

OU Base DN: dc=entrust,dc=dpc,dc=local

OU Search Filter: (|(objectClass=organizationalUnit)(objectClass=container))

c. Directory Configuration—Users:



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

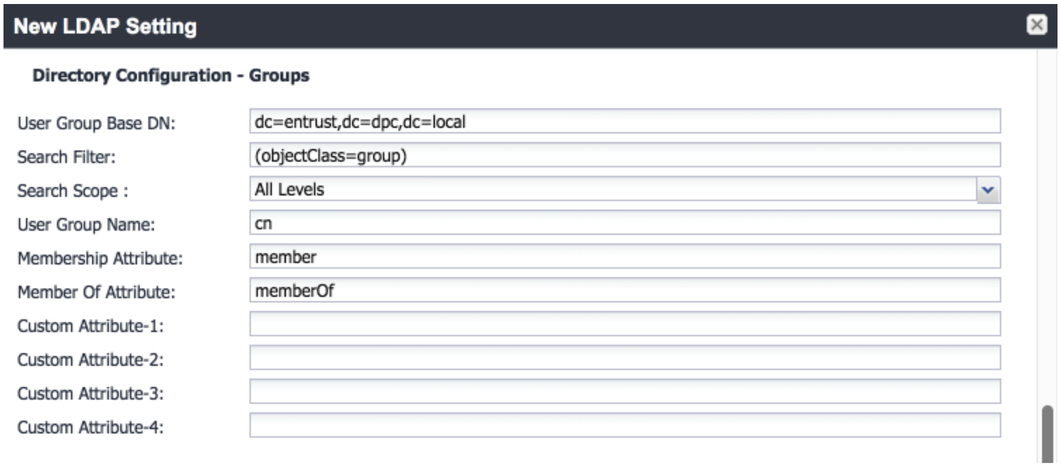
Display Name: displayName

Distinguished Name: distinguishedName

User Principal Name: userPrincipalName

Locale: c

d. Directory Configuration—Groups:



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:

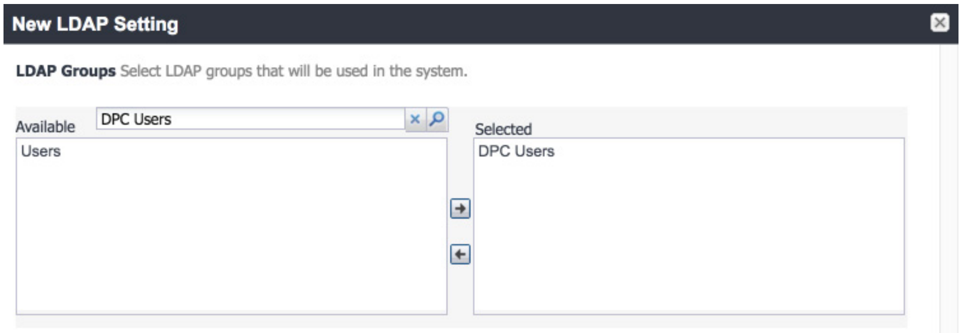
e. LDAP Groups:

   i. As a prerequisite step, we used Active Directory Users and Computers to create a new security group for DPC-authorized users on the Domain Controller for the entrust.dpc.local domain. In our example, this group is named **DPC Users.**

   ii. In the search bar, enter the name of the LDAP group for DPC-authorized users and click the **magnifying glass** button; the group name should be added to the **Available** list.

   iii. In the **Available** list, select **DPC Users** and click the **right-arrow** button to move it to the **Selected** list.

   iv. In the **Selected** list, select the default **Users** group and click the **left-arrow** button to move it to the **Available** list.



New LDAP Setting

LDAP Groups Select LDAP groups that will be used in the system.

Available: DPC Users

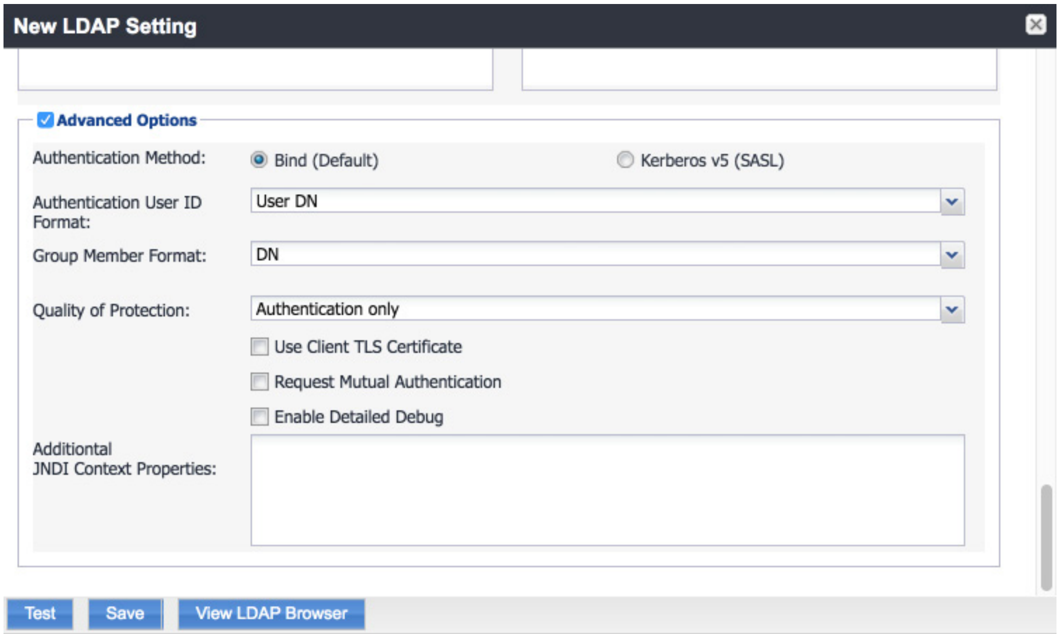
Users

Selected

DPC Users

f. Custom Settings: Custom settings were not specified.

g. Advanced Options:



New LDAP Setting

☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authentication only

□ Use Client TLS Certificate

□ Request Mutual Authentication

□ Enable Detailed Debug

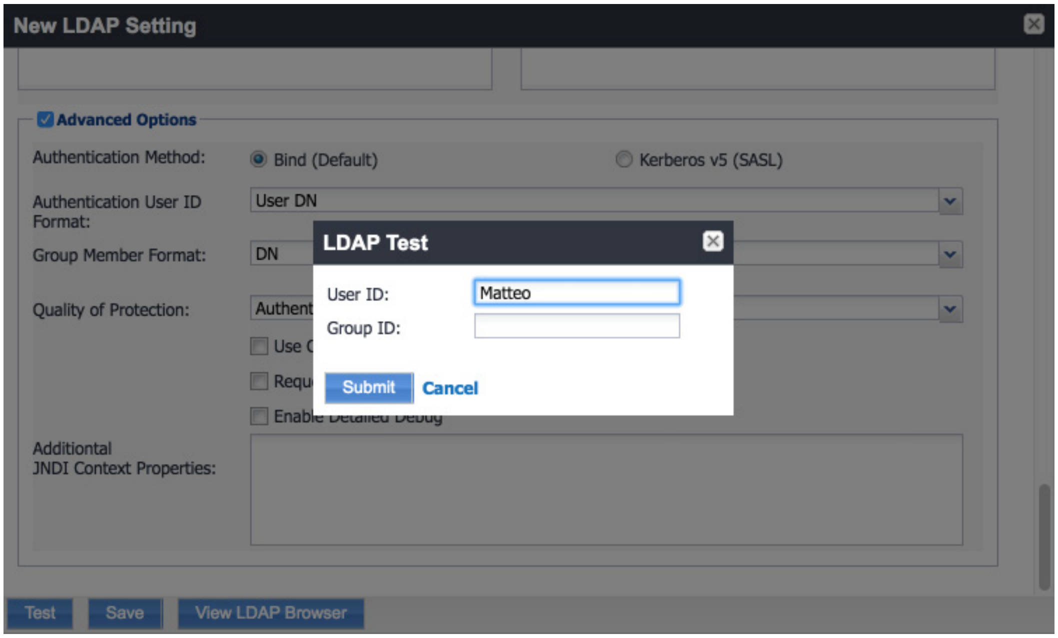
Additiontal JNDI Context Properties:

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

2. From Steps 19–21 from the MobileIron guide, we tested that MobileIron can successfully query LDAP for DPC Users.

   a. In the **New LDAP Setting** dialogue, click the **Test** button to open the **LDAP Test** dialogue.

   b. In the **LDAP Test** dialogue, enter a **User ID** for a member of the DPC Users group, then click the **Submit** button. A member of the DPC Users group in our environment is **Matteo**.



New LDAP Setting

☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authent

□ Use C

□ Requ

□ Enable Detailed Debug

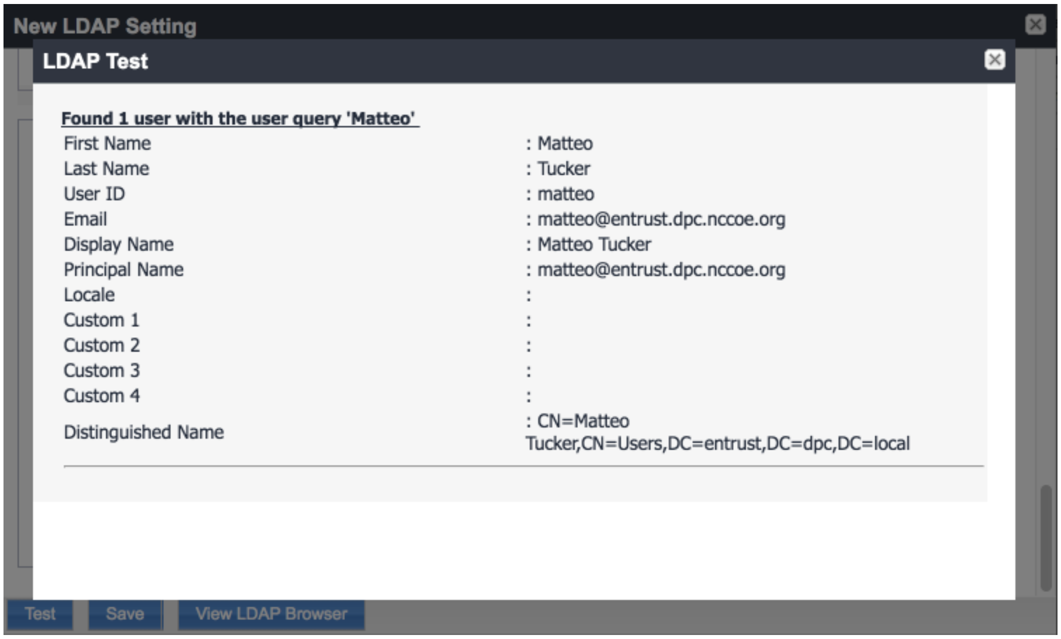
Additiontal JNDI Context Properties:

LDAP Test

User ID: Matteo

Group ID:

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



New LDAP Setting

LDAP Test

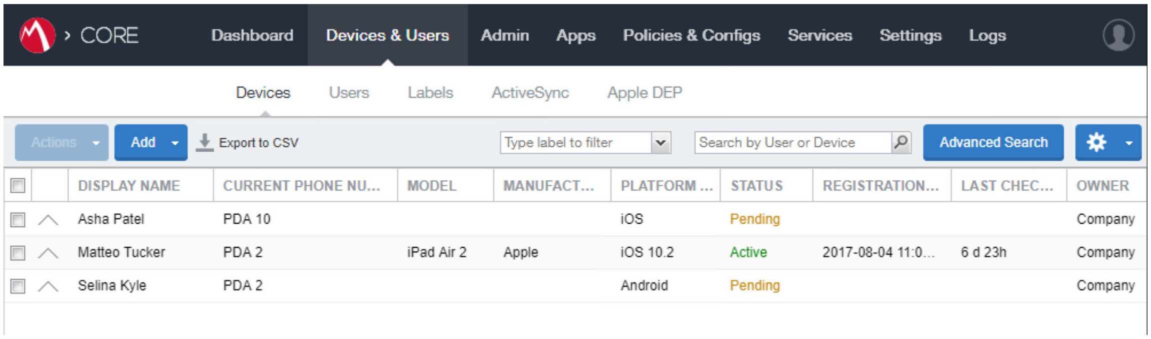
Found 1 user with the user query 'Matteo'

```
First Name               : Matteo
Last Name                : Tucker
User ID                  : matteo
Email                    : matteo@entrust.dpc.nccoe.org
Display Name             : Matteo Tucker
Principal Name           : matteo@entrust.dpc.nccoe.org
Locale                   :
Custom 1                 :
Custom 2                 :
Custom 3                 :
Custom 4                 :
Distinguished Name       : CN=Matteo
                           Tucker,CN=Users,DC=entrust,DC=dpc,DC=local
```

2.1.2.3.2 Create a DPC Users Label

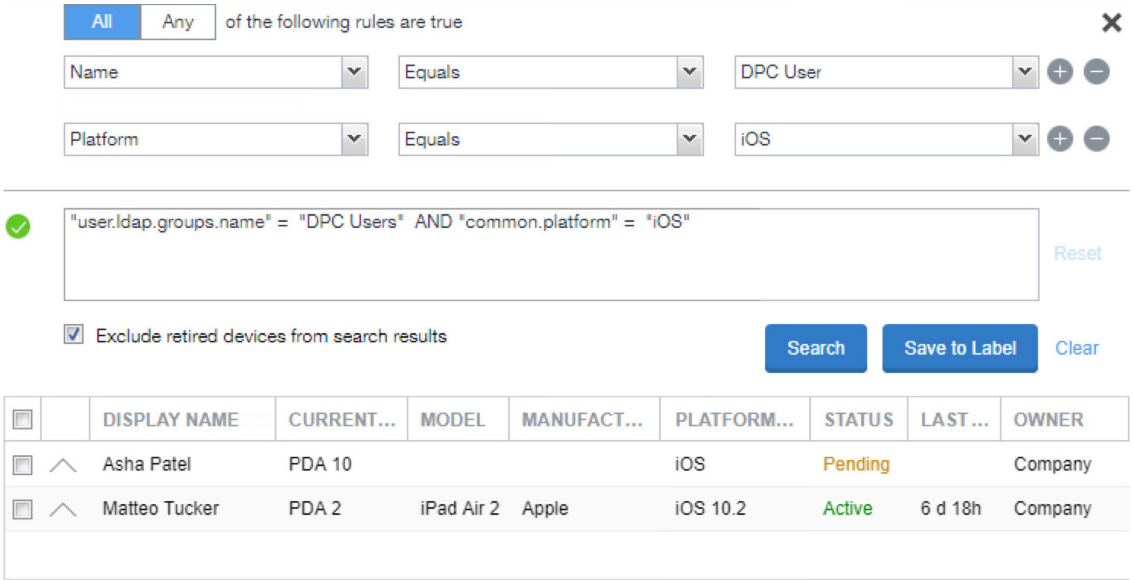
MobileIron uses labels to link policies and device configurations with users and mobile devices. Creating a unique label for DPC users allows mobile device administrators to apply controls relevant for mobile devices provisioned with a derived credential specifically to those devices. We recommend applying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

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

3. In the **Advanced Search** pane:
   a. In the blank rule:
      i. In the **Field** drop-down menu, select **User > LDAP > Groups > Name**.
      ii. In the **Value** drop-down menu, select the Active Directory group created to support DPC-specific MobileIron policies (named **DPC Users** in this example).
   b. Select the **plus sign icon** to add a blank rule.
   c. In the newly created blank rule:
      i. In the **Field** drop-down menu, select **Common > Platform**.
      ii. In the **Value** drop-down menu, select **iOS**.
   d. Optionally, select **Search** to view matching devices.
   e. Select **Save to Label**.



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

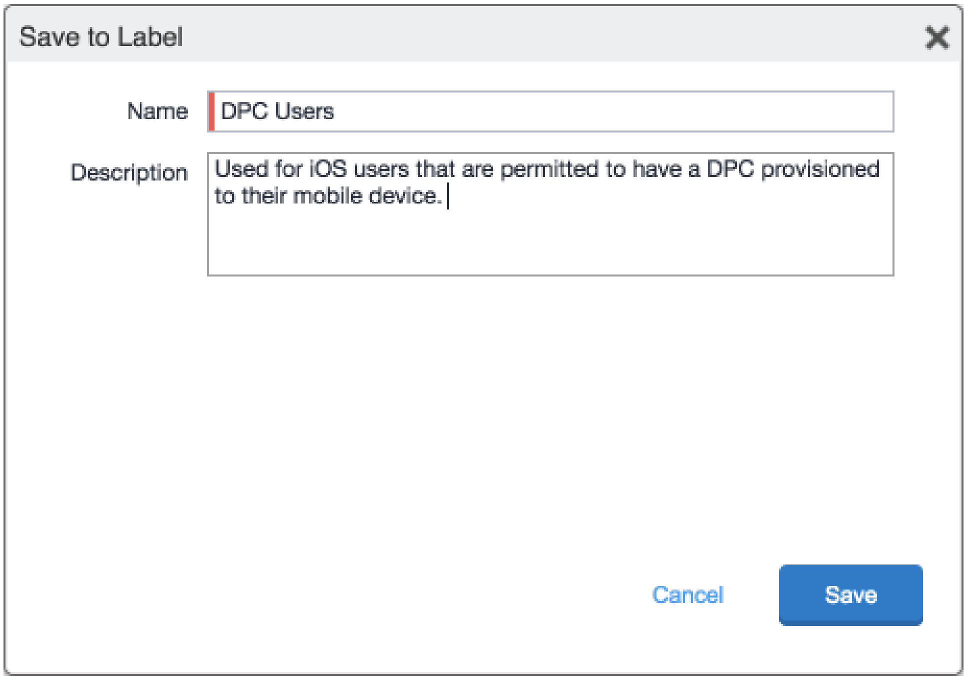
□		DISPLAY NAME	CURRENT...	MODEL	MANUFACT...	PLATFORM...	STATUS	LAST ...	OWNER
□		Asha Patel	PDA 10			iOS	Pending		Company
□		Matteo Tucker	PDA 2	iPad Air 2	Apple	iOS 10.2	Active	6 d 18h	Company

f. In the **Save to Label** dialogue:

   i. In the **Name** field, enter a descriptive name for this label (**DPC Users** in this example).

   ii. In the **Description** field, provide additional information to convey the purpose of this label.

   iii. Click **Save**.

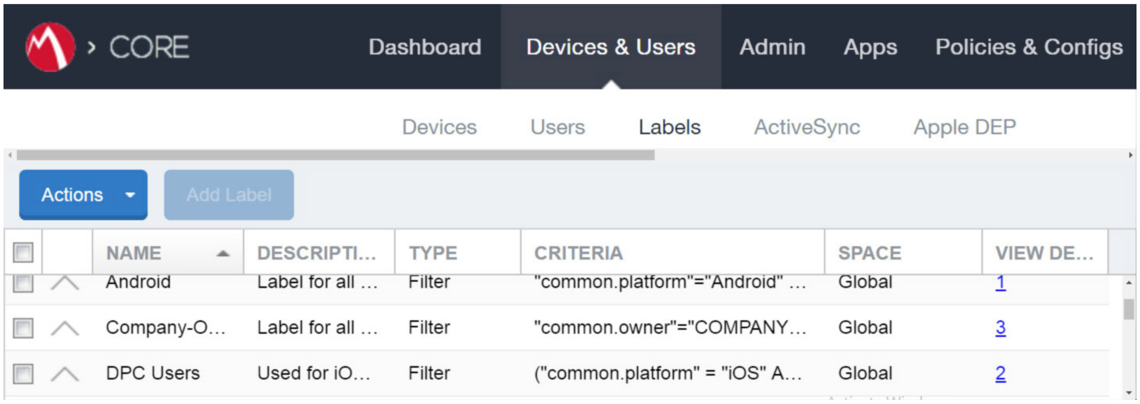


Save to Label

Name: DPC Users

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

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



NAME	DESCRIPTI…	TYPE	CRITERIA	SPACE	VIEW DE…
Android	Label for all …	Filter	"common.platform"="Android" …	Global	1
Company-O…	Label for all …	Filter	"common.owner"="COMPANY…	Global	3
DPC Users	Used for iO…	Filter	("common.platform" = "iOS" A…	Global	2

2.1.2.3.3 Implement MobileIron Guidance

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

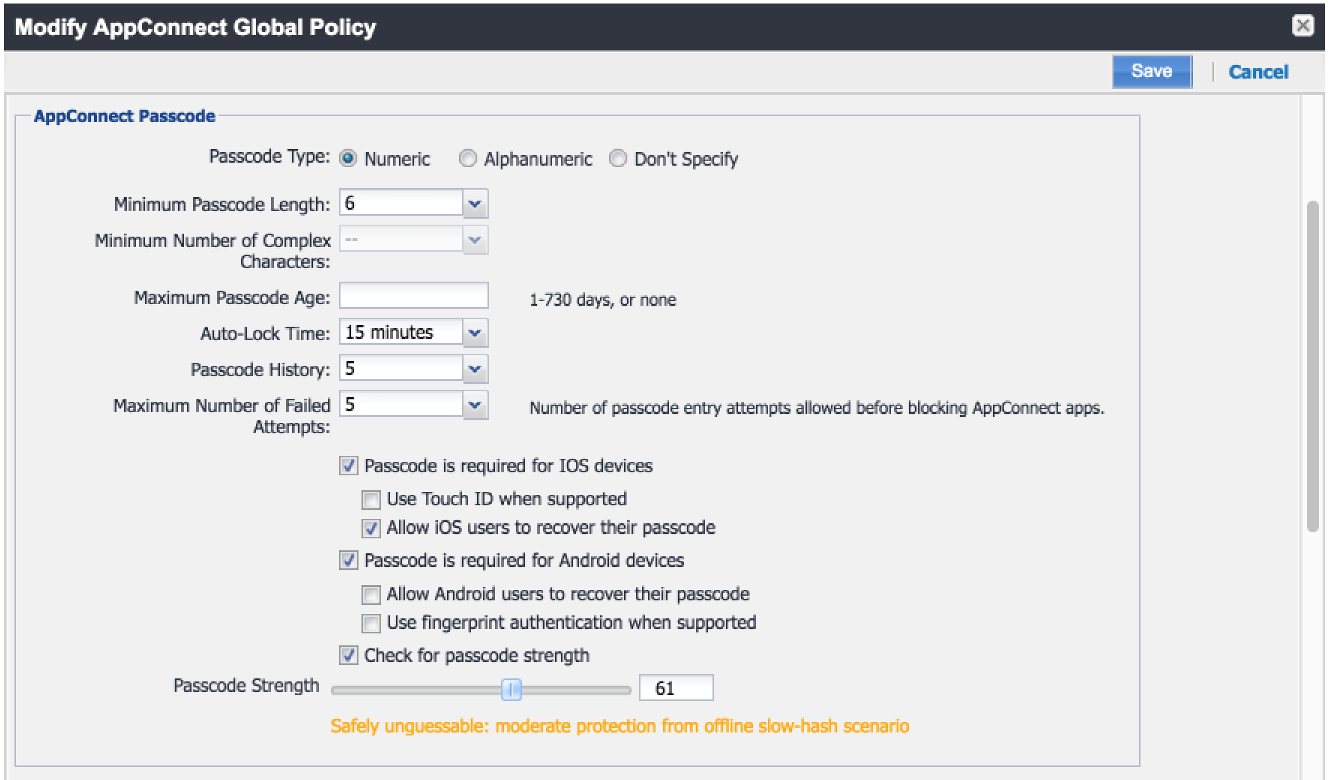
Complete these sections in Chapter 2 of the *MobileIron Derived Credentials with Entrust Guide:*

1. Before beginning:
    a. Configuring certificate authentication to the user portal

       Note: The root CA certificate or trust chain file can be obtained from Entrust Datacard.

    b. Configuring the Entrust IdentityGuard Self-Service Module (SSM) Universal Resource Locator (URL).

       Note: The URL will be specific to your organization's instance of the IDG service and can be obtained from Entrust Datacard.
2. Configuring PIN-based registration
3. Configuring user portal roles
4. Adding the PIV-D Entrust app to the App Catalog
    a. Adding Web@Work for iOS
5. Configuring Apps@Work
    a. Setting authentication options
    b. Sending the Apps@Work web clip to devices
6. Configuring AppConnect
    a. Configuring AppConnect licenses
    b. Configuring the AppConnect global policy. The **AppConnect Passcode** policy settings for our implementation are presented below.



Modify AppConnect Global Policy

AppConnect Passcode

Passcode Type: ● Numeric ○ Alphanumeric ○ Don't Specify

Minimum Passcode Length: 6

Minimum Number of Complex Characters: --

Maximum Passcode Age: 1-730 days, or none

Auto-Lock Time: 15 minutes

Passcode History: 5

Maximum Number of Failed Attempts: 5 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

Note: 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.

7. Configuring the PIV-D Entrust app

8. Configuring client-provided certificate enrollment settings. Note that the configuration items created by completing this section will be used in the following section. Replace Step 2 in this section of the *MobileIron Derived Credentials with Entrust Guide* with the following step:

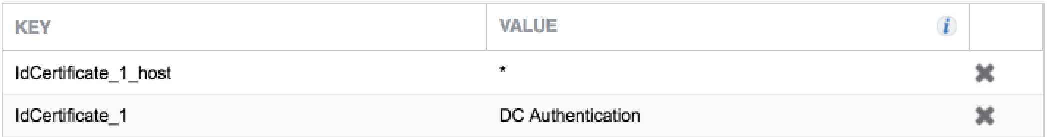
   a. Select **Add New > Certificate Enrollment > SCEP**.

9. Configuring Web@Work to use DPC:

   a. Require a device password.

   b. Configure a Web@Work setting. The **Custom Configurations** key-value pairs set for our instance in Step 4 are presented below.

      Note: The value for `idCertificate_1` is the descriptive name we applied to the Simple Certificate Enrollment Protocol (SCEP) certificate enrollment configuration for derived credential authentication created in the *MobileIron Derived Credentials with Entrust Guide* section referenced in Step 8.



KEY	VALUE	
IdCertificate_1_host	*	✖
IdCertificate_1	DC Authentication	✖

2.1.3 DPC Lifecycle Workflows

This section describes how to perform the DPC lifecycle activities of initial issuance, maintenance, and termination.

2.1.3.1 DPC Initial Issuance

This section provides the steps necessary to issue a DPC onto a target mobile device.

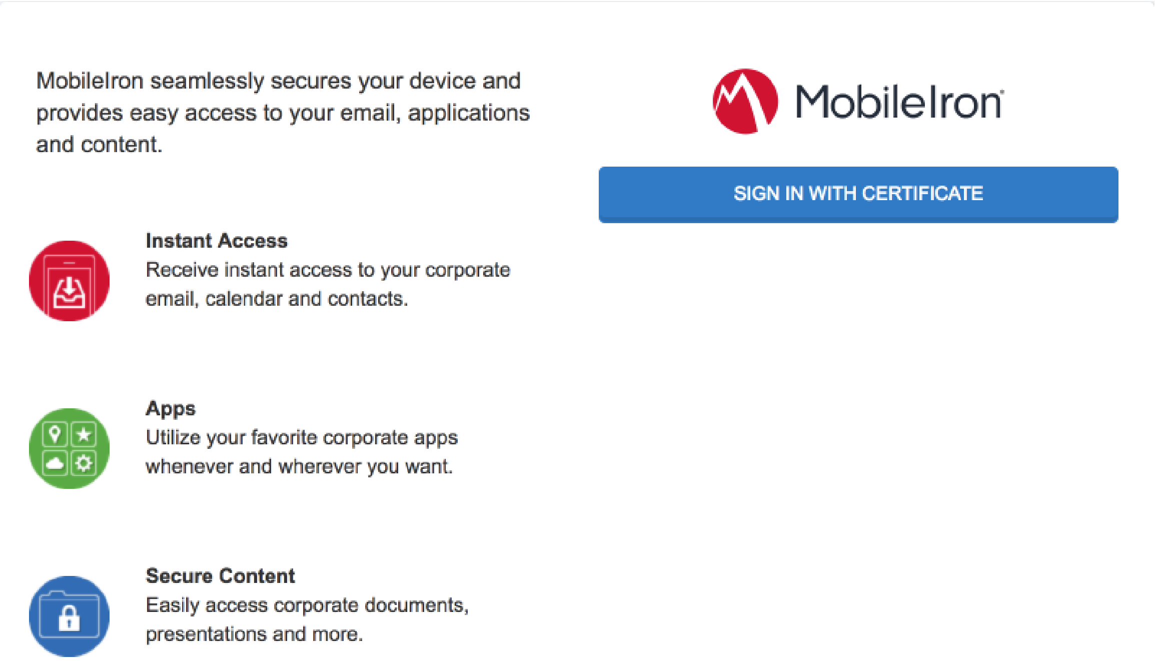
2.1.3.1.1 Register Target Device with MobileIron

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

1. Insert your valid PIV Card into the card reader attached to, or integrated into, your laptop or computer workstation.

2. Using a web browser, visit the MobileIron Self-Service Portal URL provided by your administrator.

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



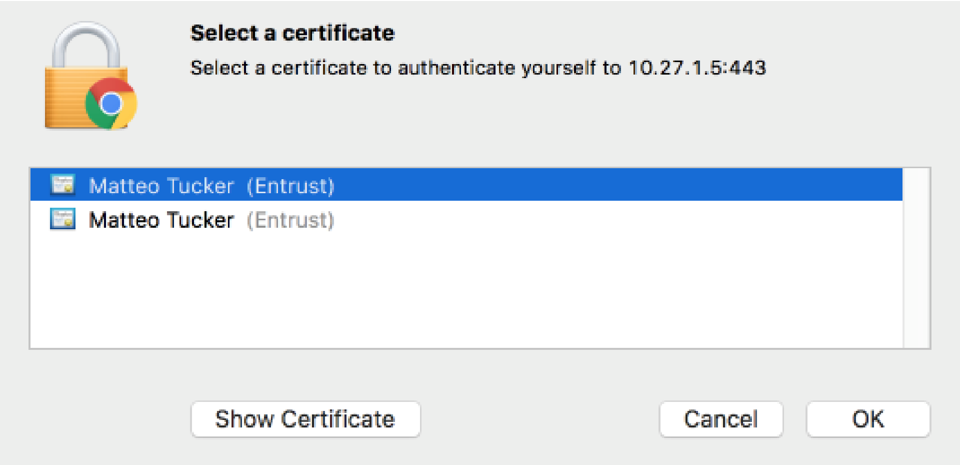
MobileIron seamlessly secures your device and provides easy access to your email, applications and content.

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.

4. In the certificate selection dialogue:
   a. If necessary, identify your PIV Authentication certificate:
      i. Highlight a certificate.
      ii. Select **Show Certificate**.



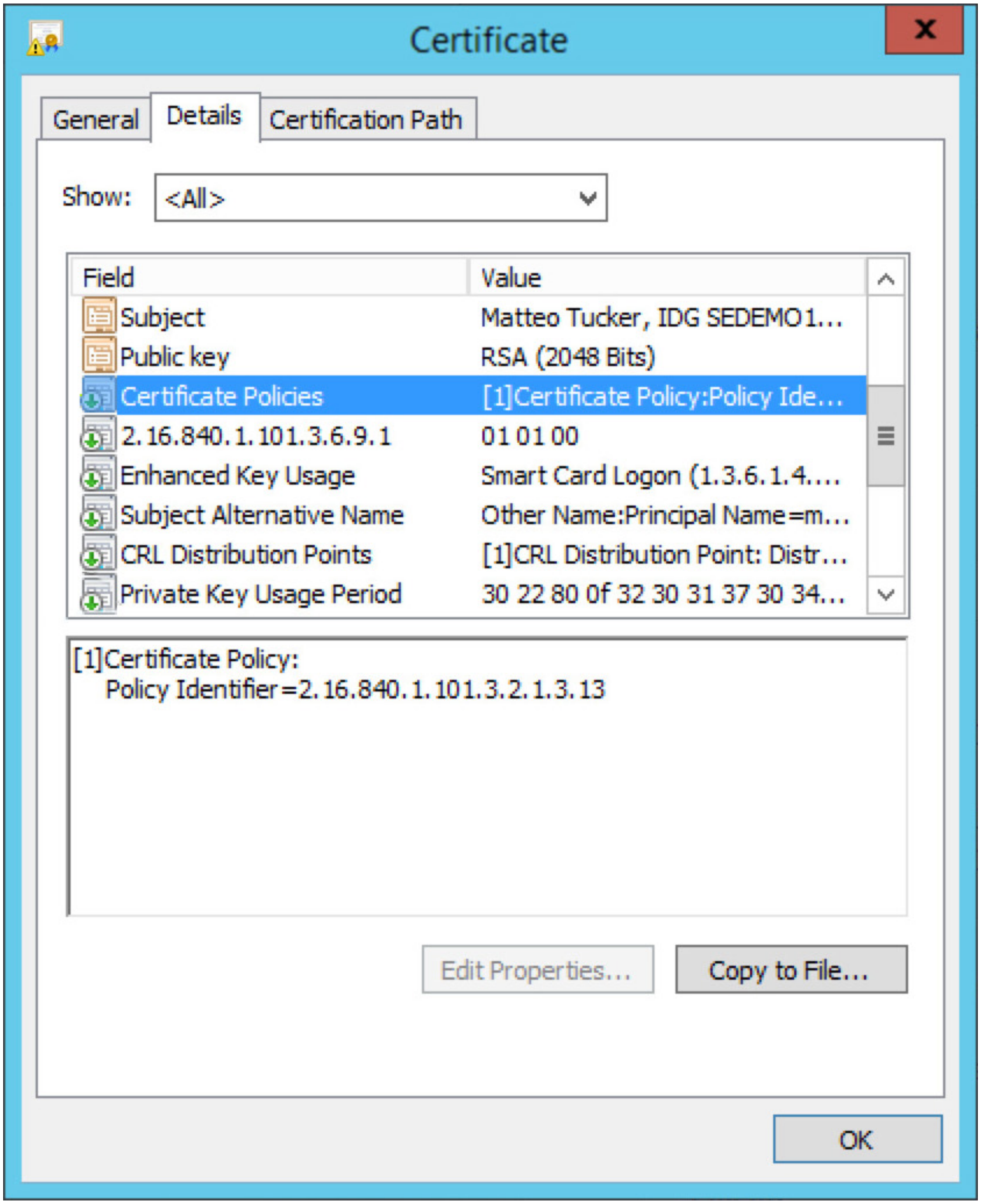
Select a certificate
Select a certificate to authenticate yourself to 10.27.1.5:443

Matteo Tucker (Entrust)
Matteo Tucker (Entrust)

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

iv. The PIV Authentication certificate contains a **Field** named **Certificate Policies** with a **Value** that contains **Policy Identifier=2.16.840.1.101.3.2.1.3.13**.

v. Repeat Steps i–iii above as necessary.



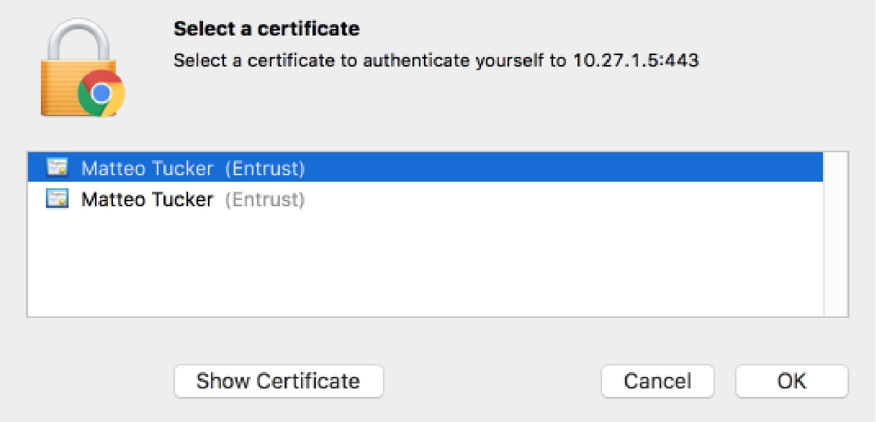
Show: <All>

Field	Value
Subject	Matteo Tucker, IDG SEDEMO1...
Public key	RSA (2048 Bits)
Certificate Policies	[1]Certificate Policy:Policy Ide...
2.16.840.1.101.3.6.9.1	01 01 00
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4....
Subject Alternative Name	Other Name:Principal Name=m...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Private Key Usage Period	30 22 80 0f 32 30 31 37 30 34...

[1]Certificate Policy:
    Policy Identifier=2.16.840.1.101.3.2.1.3.13

b. Select your PIV Authentication certificate in the list of available certificates.

c. Click **OK**.



Select a certificate

Select a certificate to authenticate yourself to 10.27.1.5:443

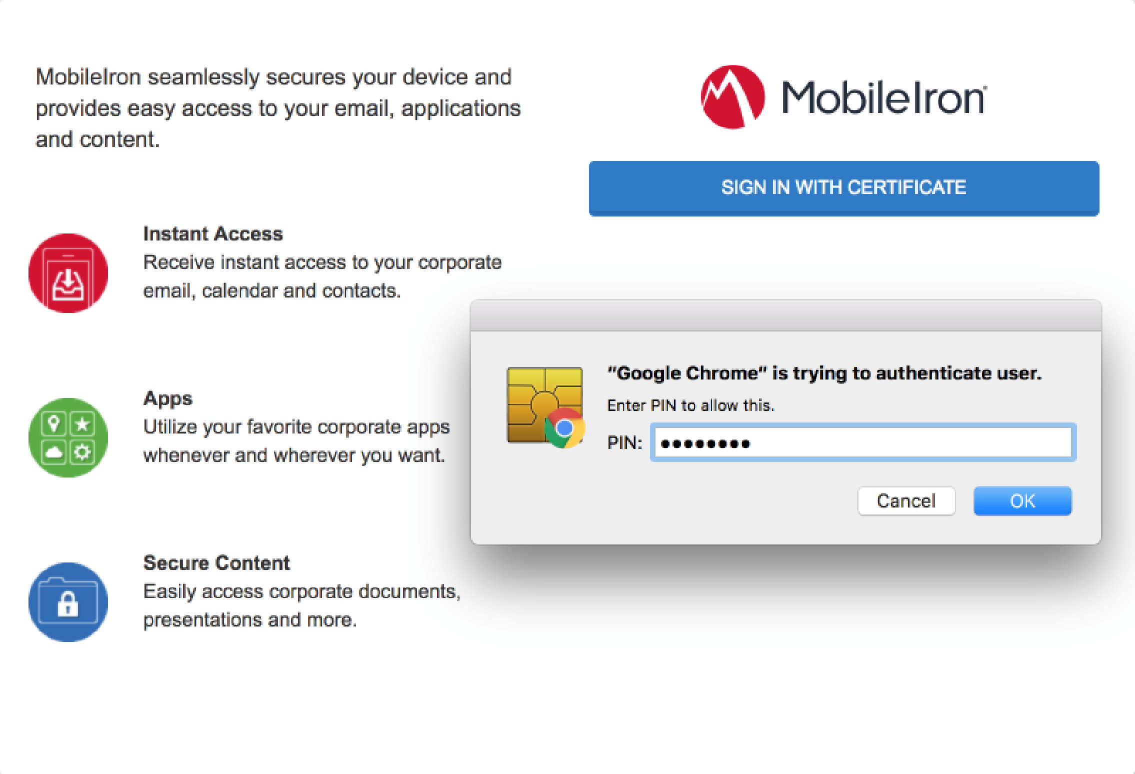
Matteo Tucker (Entrust)

Matteo Tucker (Entrust)

5. In the authentication dialogue:

   a. In the **PIN** field, enter your PIV Card PIN.

   b. Click **OK**.



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

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

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

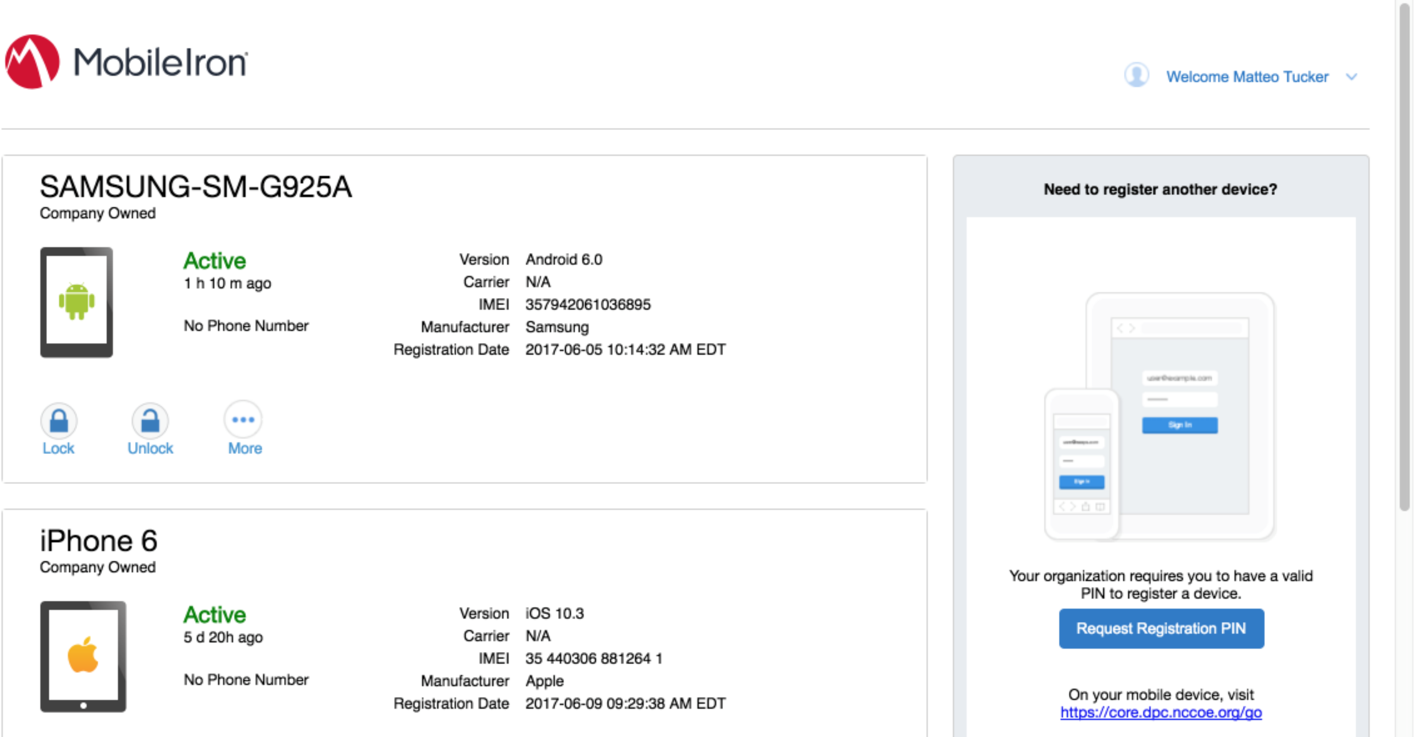
Secure Content
Easily access corporate documents, presentations and more.

"Google Chrome" is trying to authenticate user.

Enter PIN to allow this.

PIN: •••••••••

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



MobileIron

Welcome Matteo Tucker

SAMSUNG-SM-G925A
Company Owned

Active
1 h 10 m ago

No Phone Number

Version	Android 6.0
Carrier	N/A
IMEI	357942061036895
Manufacturer	Samsung
Registration Date	2017-06-05 10:14:32 AM EDT

iPhone 6
Company Owned

Active
5 d 20h ago

No Phone Number

Version	iOS 10.3
Carrier	N/A
IMEI	35 440306 881264 1
Manufacturer	Apple
Registration Date	2017-06-09 09:29:38 AM EDT

Need to register another device?

Your organization requires you to have a valid PIN to register a device.

On your mobile device, visit https://core.dpc.nccoe.org/go

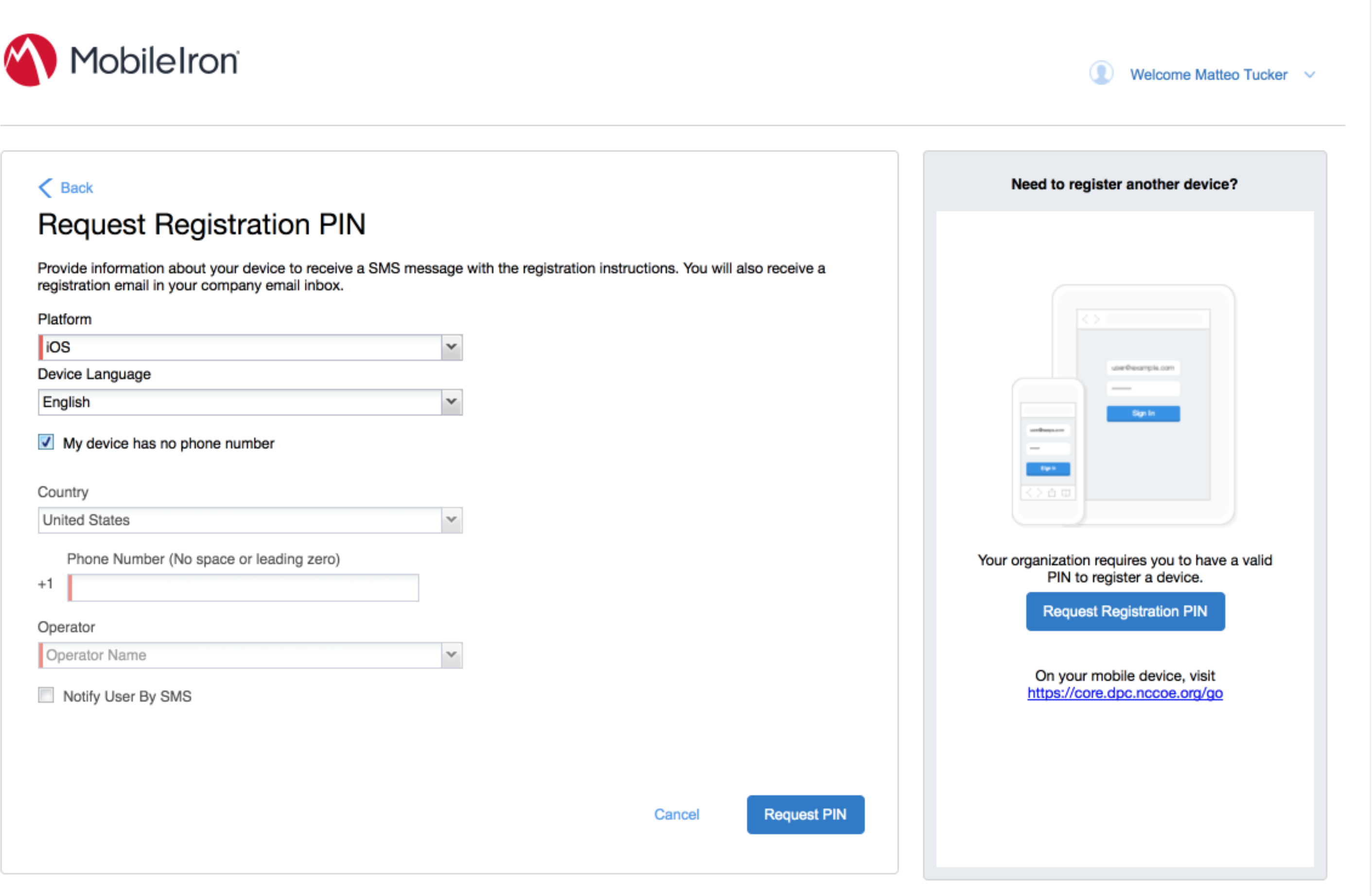
7. In the **Request Registration PIN** page:

   a. Select **iOS** from the **Platform** drop-down menu.

   b. If your device does not have a phone number, check **My device has no phone number**.

   c. If your device has a phone number, enter it in the **Phone Number** field.

304 d. Click **Request PIN**.



Request Registration PIN

Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.

Platform: iOS

Device Language: English

☑ My device has no phone number

Country: United States

Phone Number (No space or leading zero)

+1

Operator: Operator Name

□ Notify User By SMS

Your organization requires you to have a valid PIN to register a device.

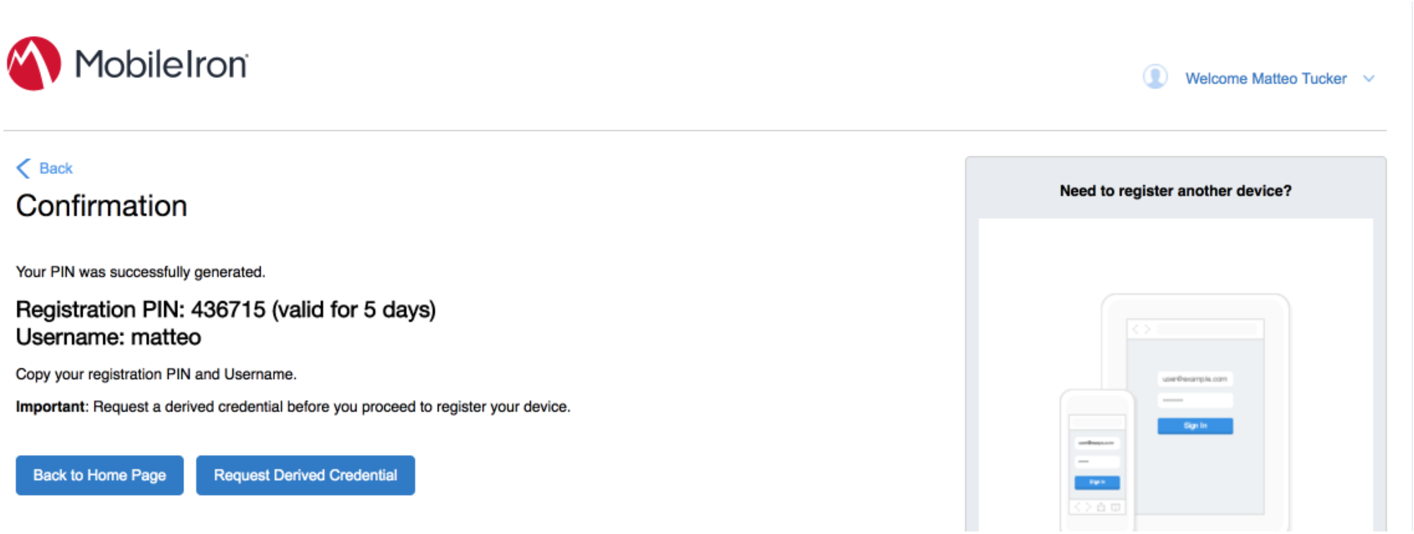
On your mobile device, visit https://core.dpc.nccoe.org/go

305

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

Note: This page may also facilitate the workflow for initial DPC issuance, covered in Section 2.1.3.1.2.

Figure 2-2 MobileIron Registration Confirmation Page



Confirmation

Your PIN was successfully generated.

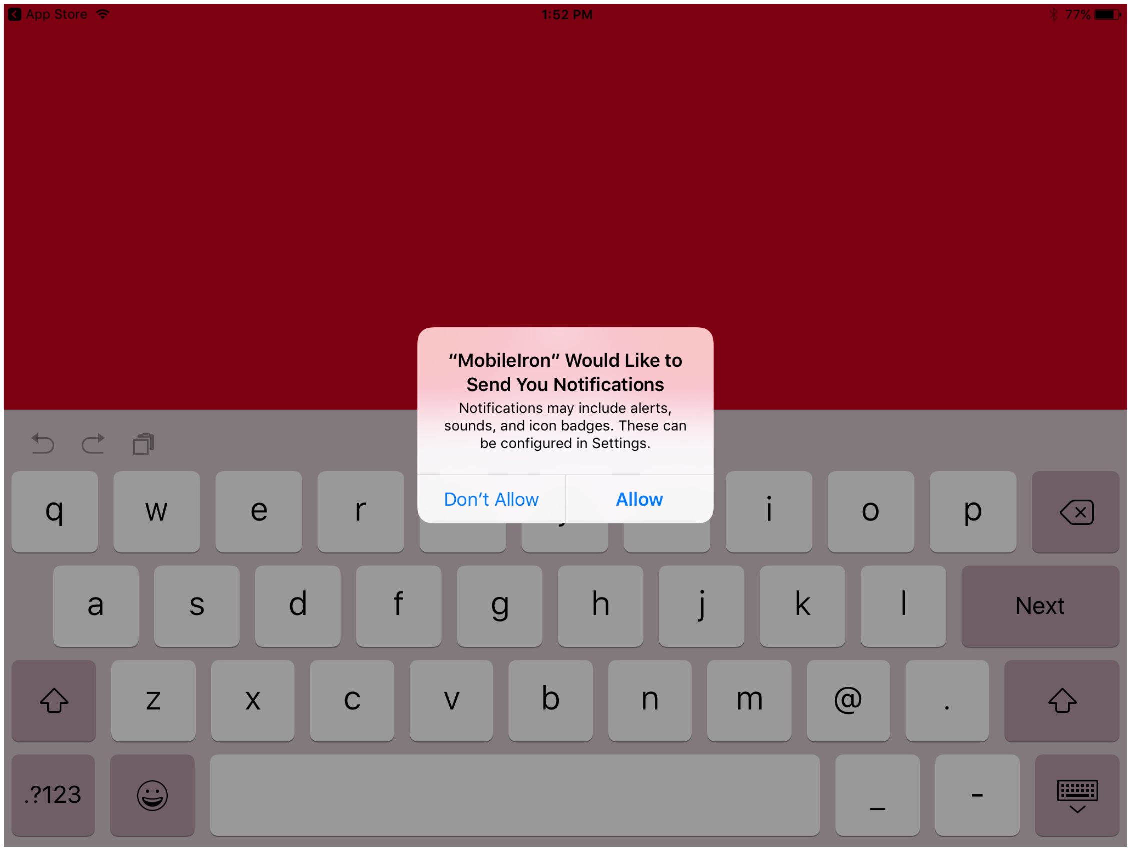
Registration PIN: 436715 (valid for 5 days)
Username: matteo

Copy your registration PIN and Username.

Important: Request a derived credential before you proceed to register your device.

8. Using the target mobile device, launch the MobileIron **Mobile@Work** application.

9. In the request to grant MobileIron permission to receive push notifications, tap **Allow**.



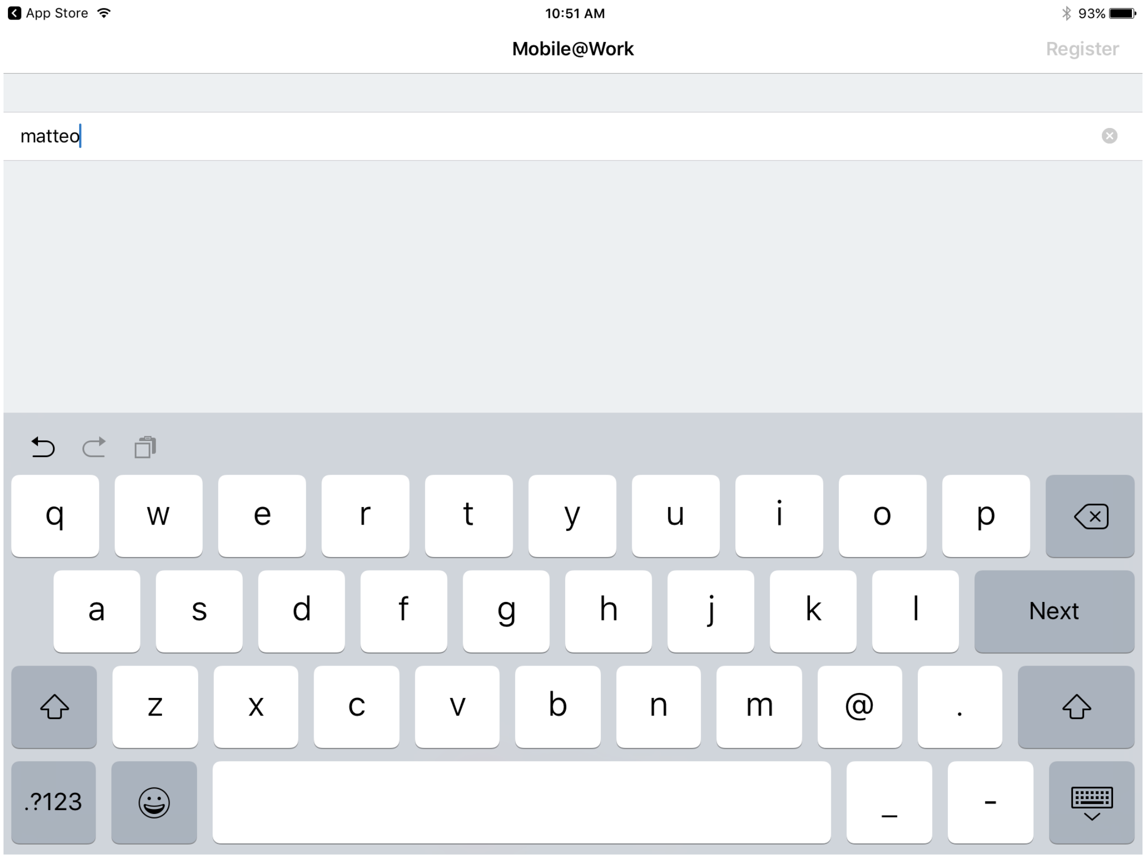
“MobileIron” Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

10. In **Mobile@Work**:

    a. In the **User Name** field, enter your LDAP or MobileIron user ID.

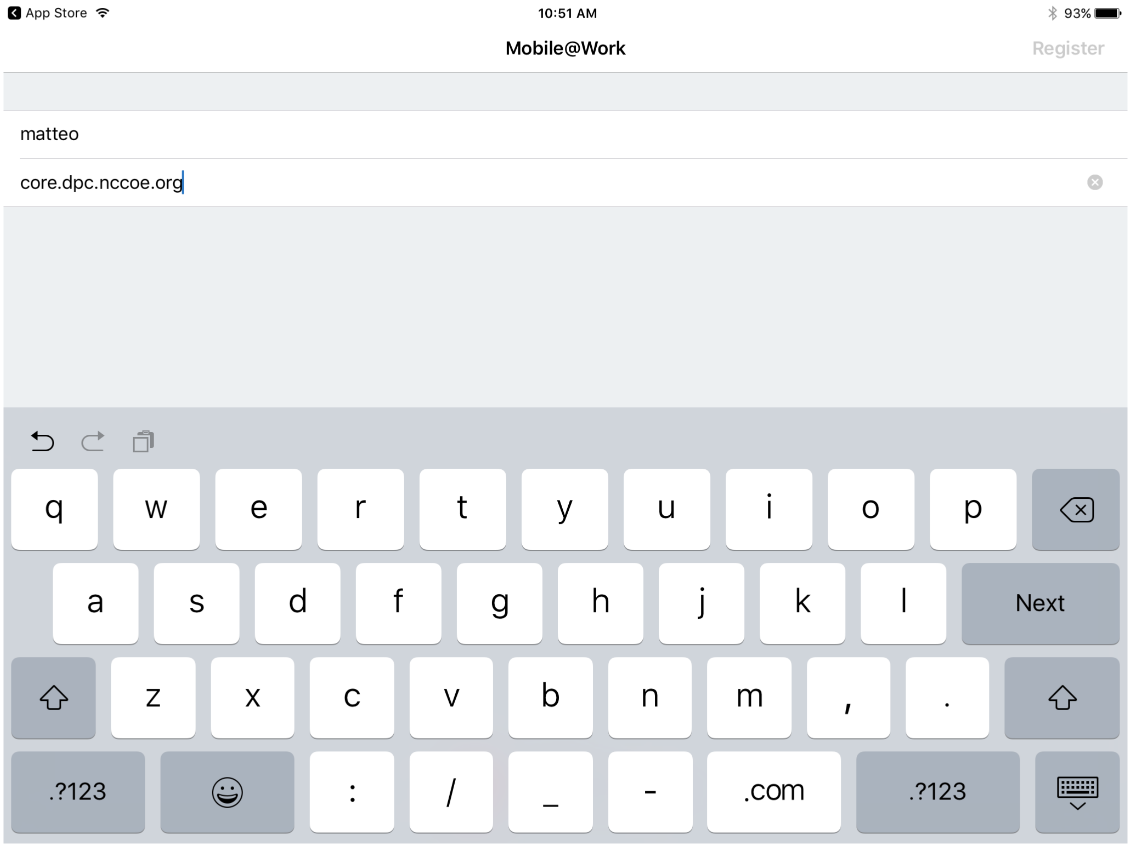
    b. Tap **Next**.



matteo

c. In the **Server** field, enter the URL for your organization's instance of MobileIron Core as provided by a MobileIron Core administrator.

d. Tap **Next**.

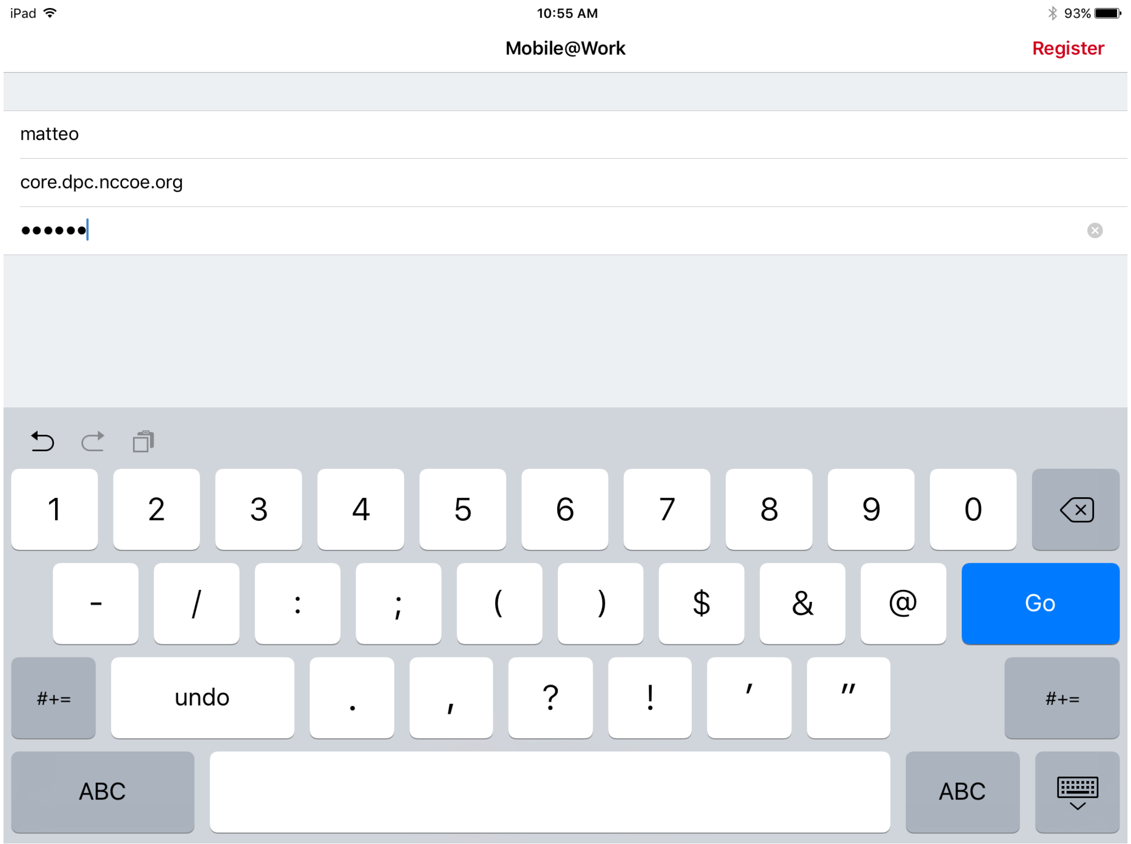


matteo

core.dpc.nccoe.org

e. In the **PIN** field, enter the **Registration PIN** displayed in the **Confirmation** page (see Figure 2-2) of the MobileIron Self-Service Portal at the completion of Step 7e.

f. Tap **Go** on keyboard or **Register** in Mobile@Work.

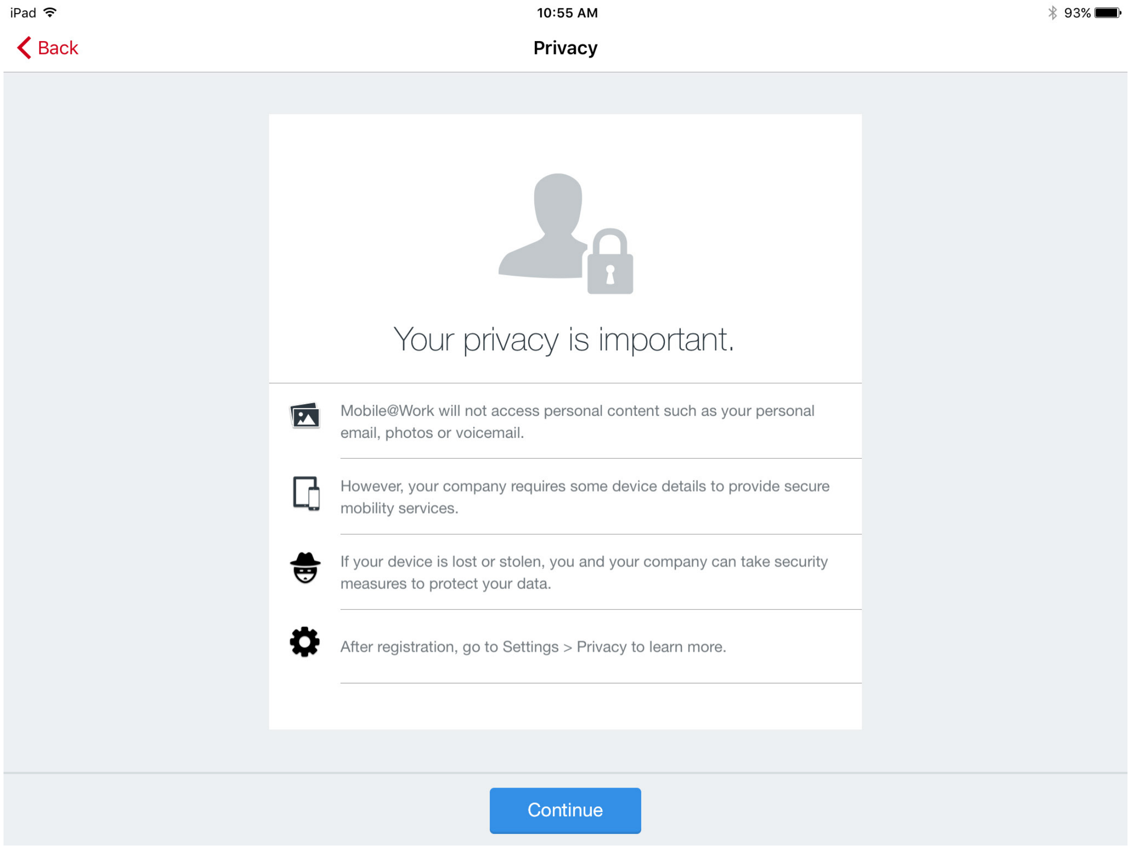


matteo

core.dpc.nccoe.org

••••••

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



iPad 10:55 AM 93%

Back

Privacy

Your privacy is important.

Mobile@Work will not access personal content such as your personal email, photos or voicemail.

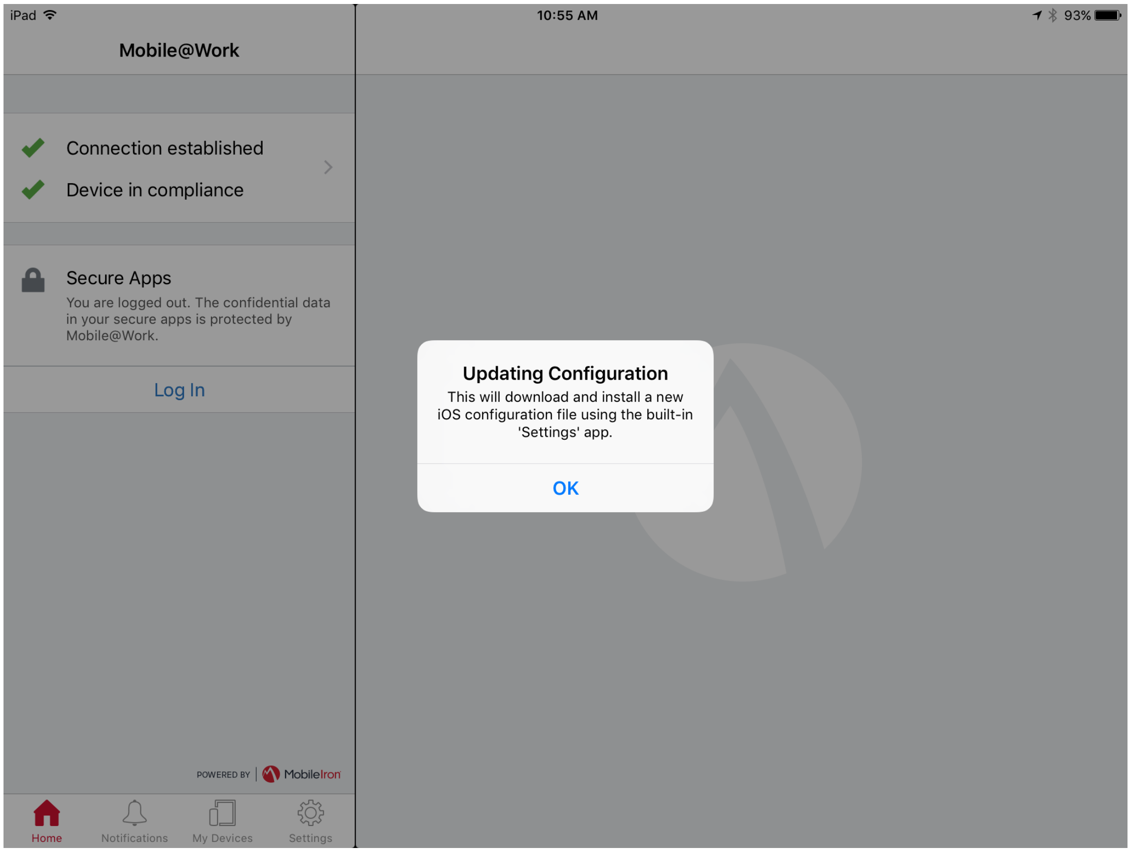
However, your company requires some device details to provide secure mobility services.

If your device is lost or stolen, you and your company can take security measures to protect your data.

After registration, go to Settings > Privacy to learn more.

Continue

11. In the **Updating Configuration** dialogue, tap **OK**; this will launch the built-in iOS **Settings** application.



Connection established

Device in compliance

Secure Apps

You are logged out. The confidential data in your secure apps is protected by Mobile@Work.

Log In

Updating Configuration

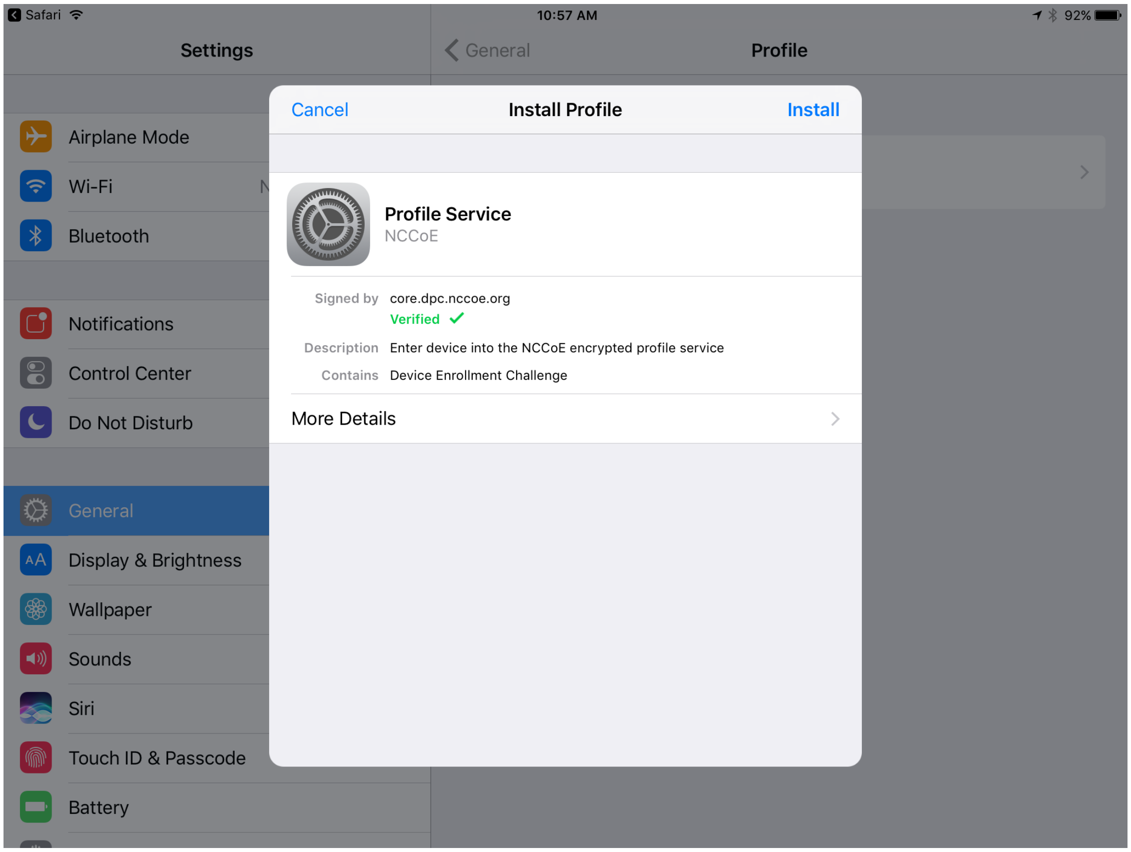
This will download and install a new iOS configuration file using the built-in 'Settings' app.

OK

12. In the **Settings** application, in the **Install Profile** dialogue:
    a. In the **Signed B**y field, confirm that the originating server identity shows as **Verified**.

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

    b. Tap **Install**.



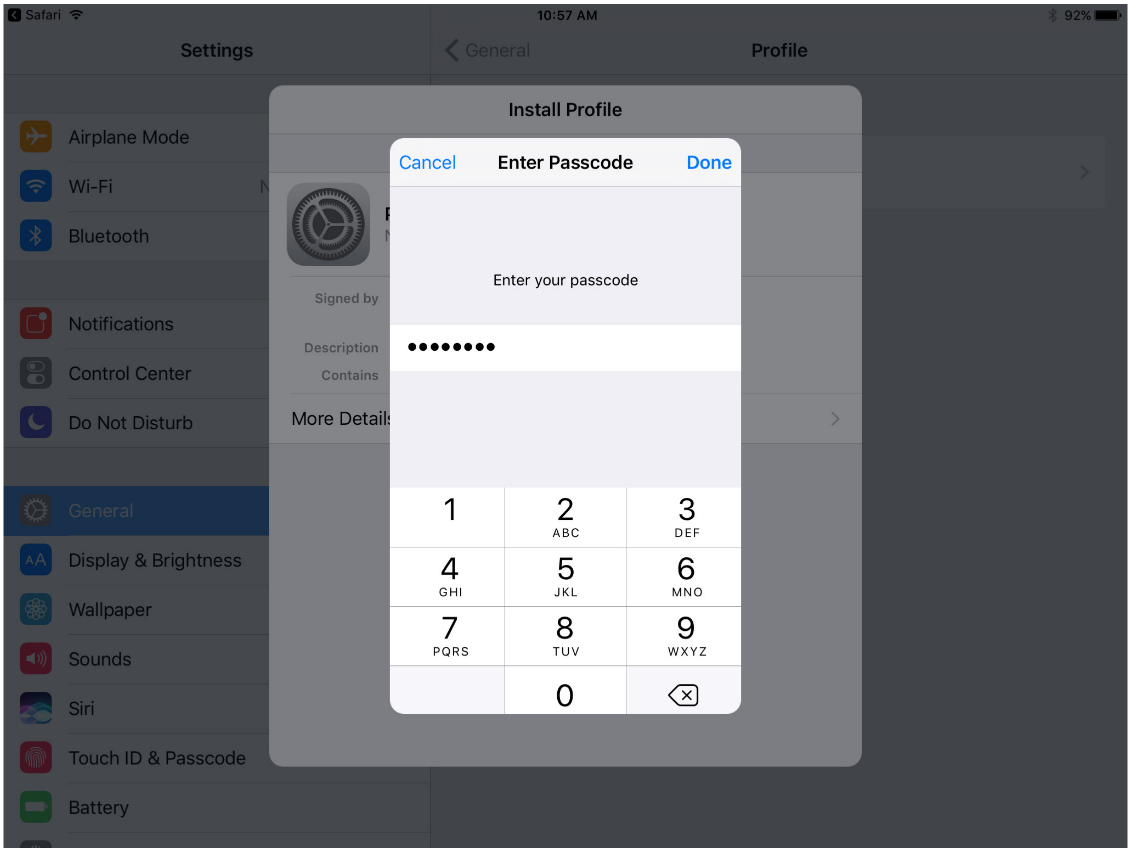
Profile Service
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

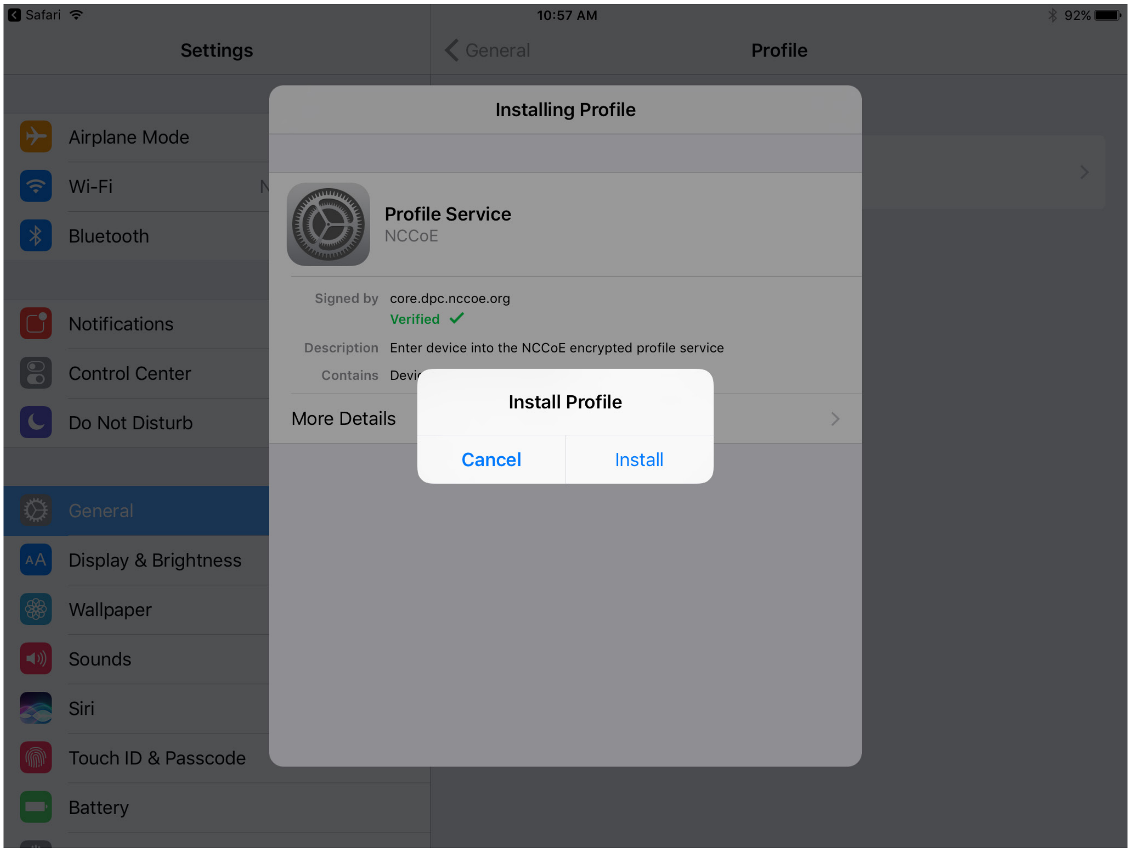
Description Enter device into the NCCoE encrypted profile service

Contains Device Enrollment Challenge

13. In the Enter **Passcode** dialogue:
    a. Enter your device unlock code.
    b. Tap **Done**.



14. In the **Install Profile** dialogue, tap **Install**.



Installing Profile

Profile Service
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

Description Enter device into the NCCoE encrypted profile service

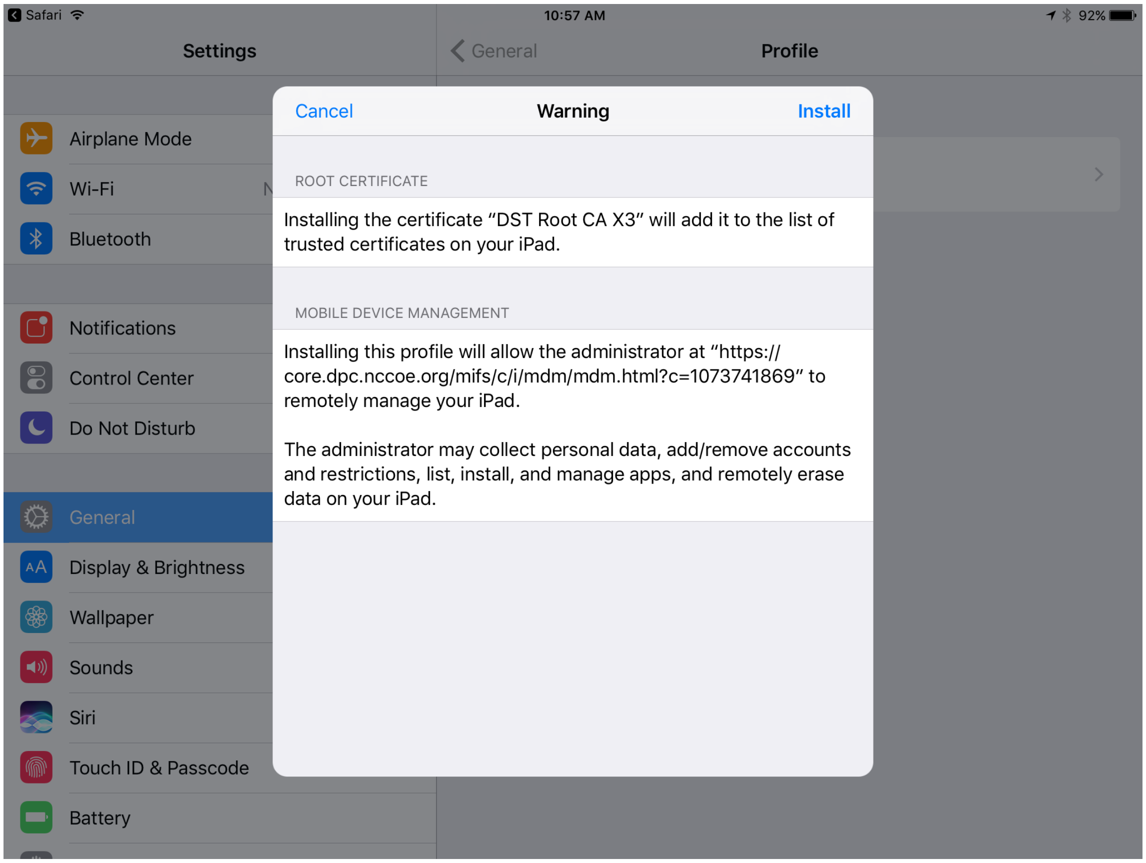
Contains Devi

More Details

Install Profile

Cancel Install

15. In the **Warning** dialogue, tap **Install**.



ROOT CERTIFICATE

Installing the certificate "DST Root CA X3" will add it to the list of trusted certificates on your iPad.

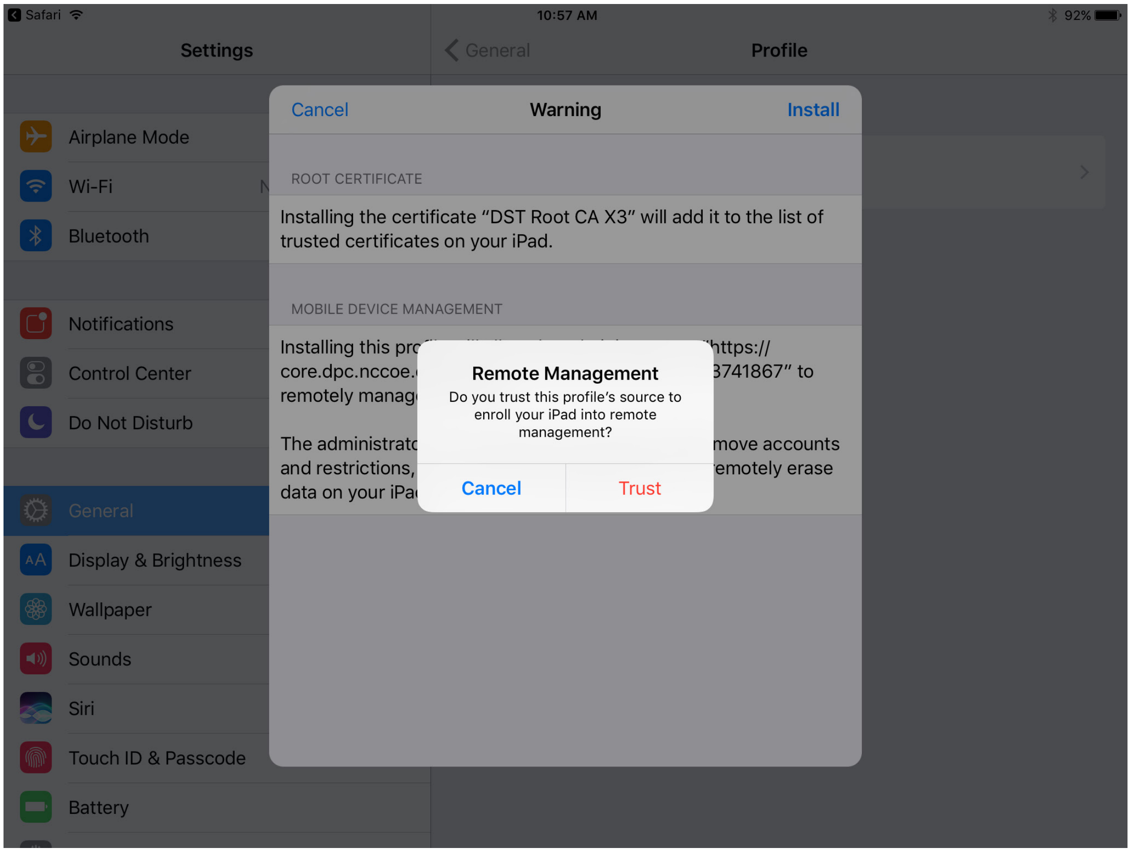
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://core.dpc.nccoe.org/mifs/c/i/mdm/mdm.html?c=1073741869" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.

16. In the **Remote Management** dialogue, tap **Trust**.

    Note: The root certificate presented in this step may vary based on the CA used to sign the MDM profile. This build uses the Let's Encrypt certificate authority.



ROOT CERTIFICATE

Installing the certificate "DST Root CA X3" will add it to the list of trusted certificates on your iPad.

MOBILE DEVICE MANAGEMENT

Installing this pro… "https:// core.dpc.nccoe.… 3741867" to remotely manag…

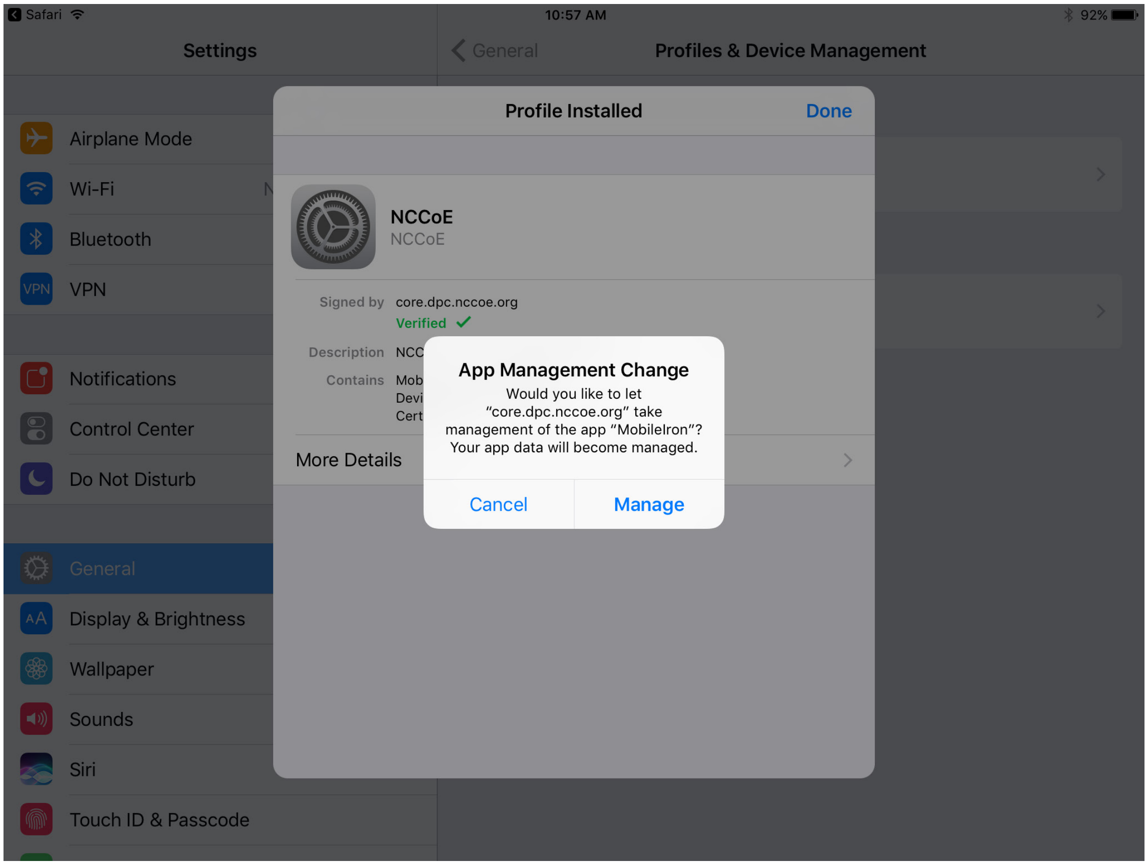
The administrat… move accounts and restrictions, … emotely erase data on your iPa…

Remote Management

Do you trust this profile's source to enroll your iPad into remote management?

17. In the **Profile Installed** dialogue, tap **Done**.

18. In the **App Management Change** dialogue, tap **Manage**.



NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

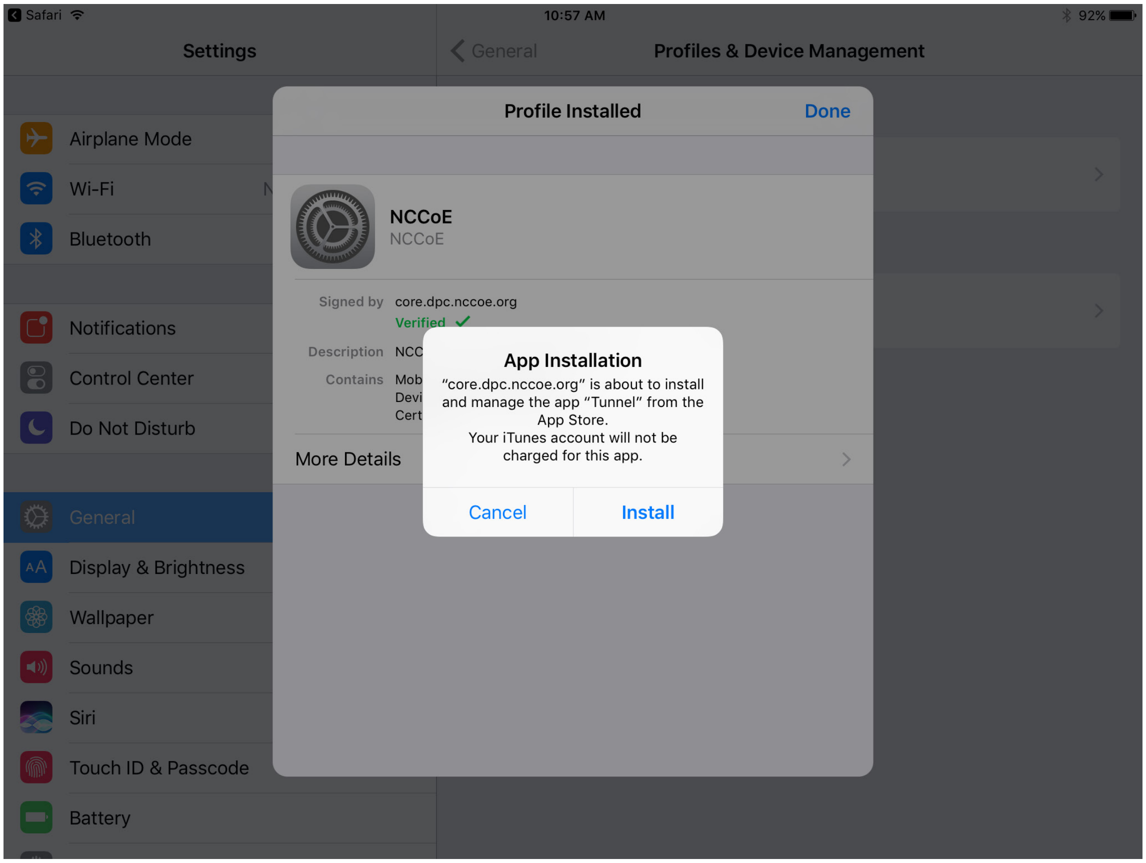
Description NCC

Contains Mob
Devi
Cert

App Management Change

Would you like to let "core.dpc.nccoe.org" take management of the app "MobileIron"? Your app data will become managed.

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



Profile Installed Done

NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

Description NCC

Contains Mob Devi Cert

More Details

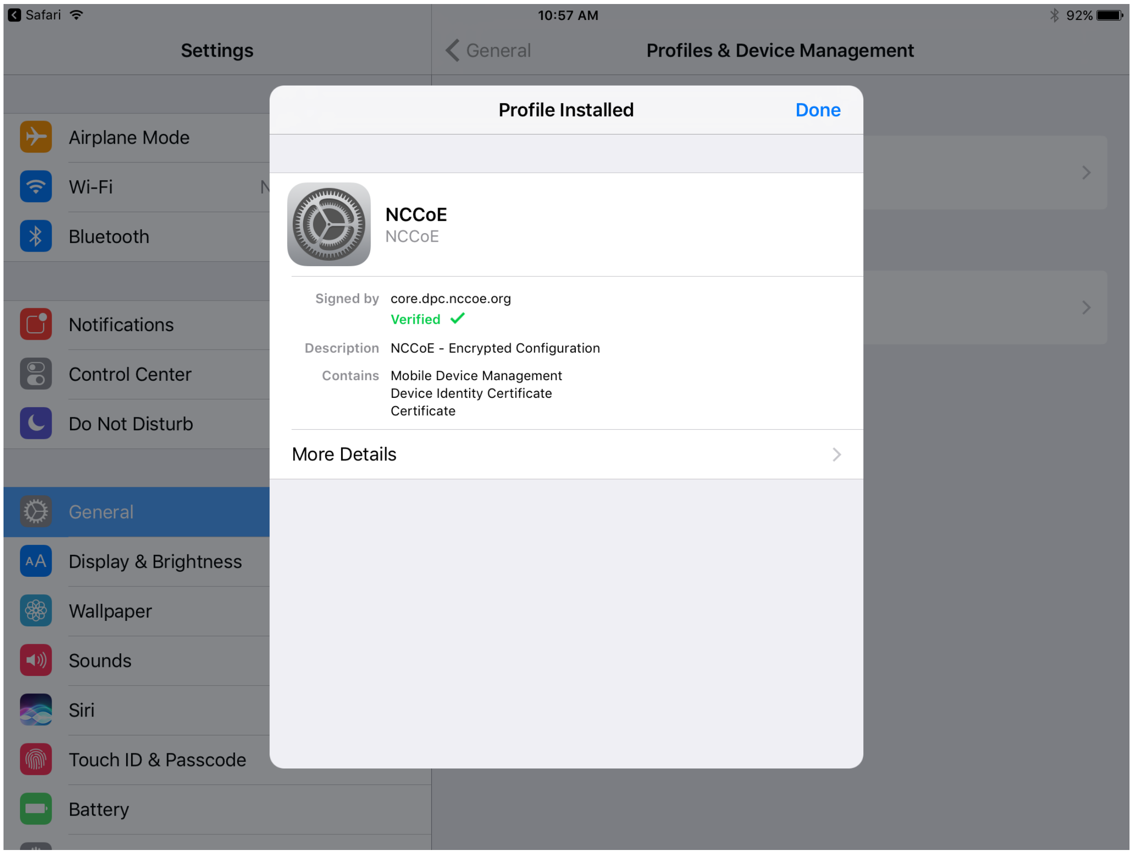
App Installation

“core.dpc.nccoe.org” is about to install and manage the app “Tunnel” from the App Store.
Your iTunes account will not be charged for this app.

Cancel Install

355

356 20. In the **Profile Installed** dialogue, tap **Done**.



Profile Installed

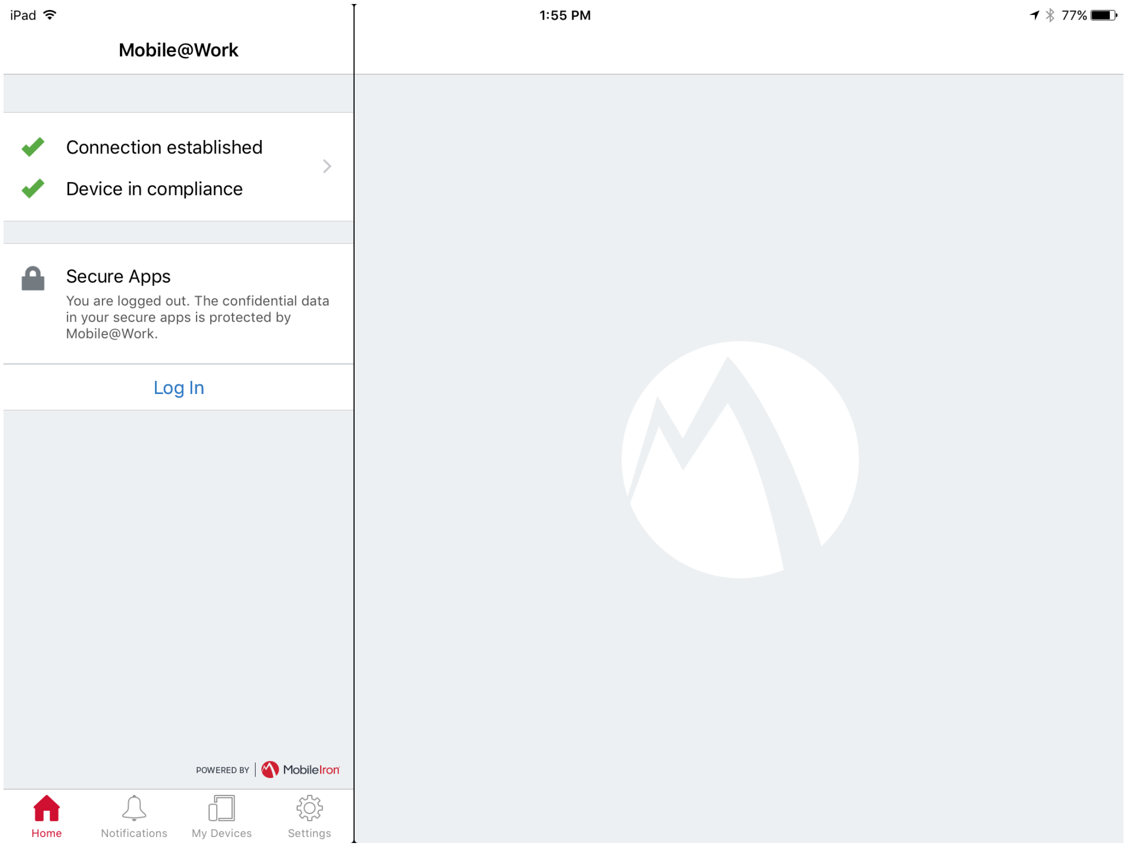
NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

Description NCCoE - Encrypted Configuration

Contains Mobile Device Management
Device Identity Certificate
Certificate

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



iPad 1:55 PM 77%

Mobile@Work

✓ Connection established

✓ Device in compliance

Secure Apps

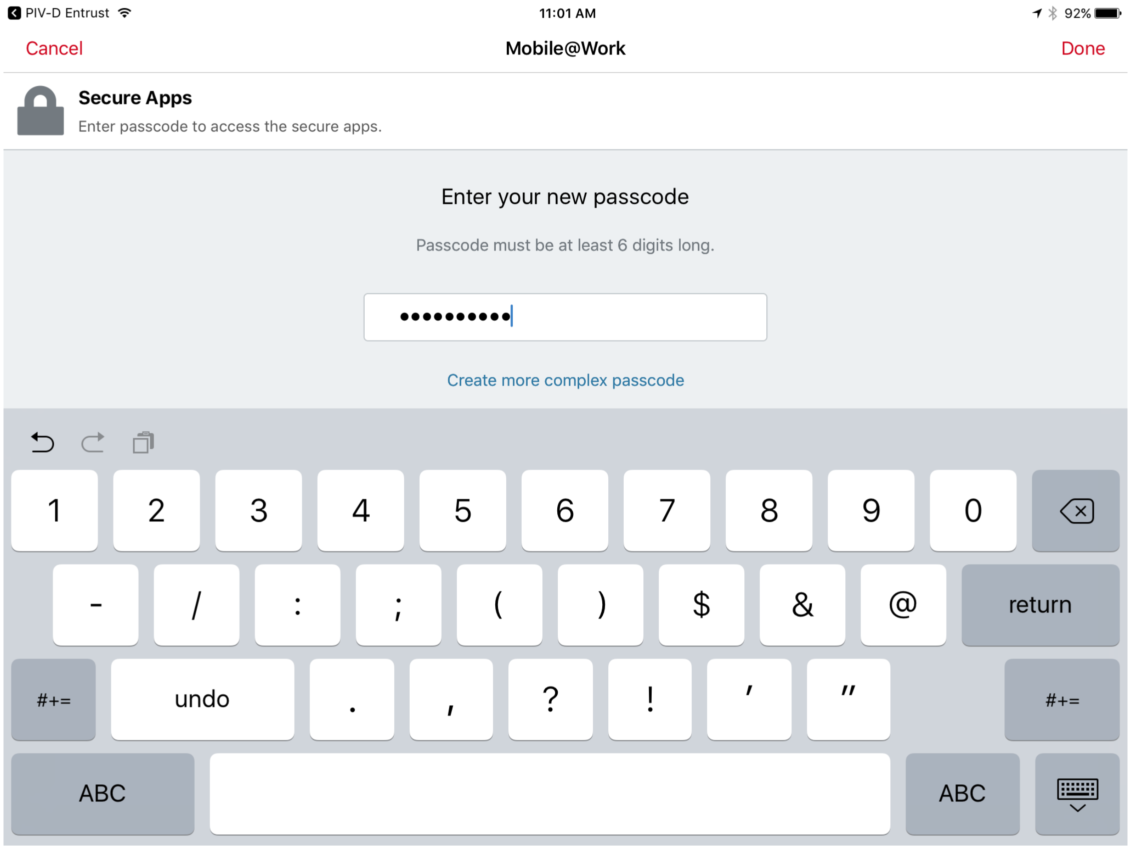
You are logged out. The confidential data in your secure apps is protected by Mobile@Work.

2.1.3.1.2 DPC Initial Issuance

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

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

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



Secure Apps

Enter passcode to access the secure apps.

Enter your new passcode

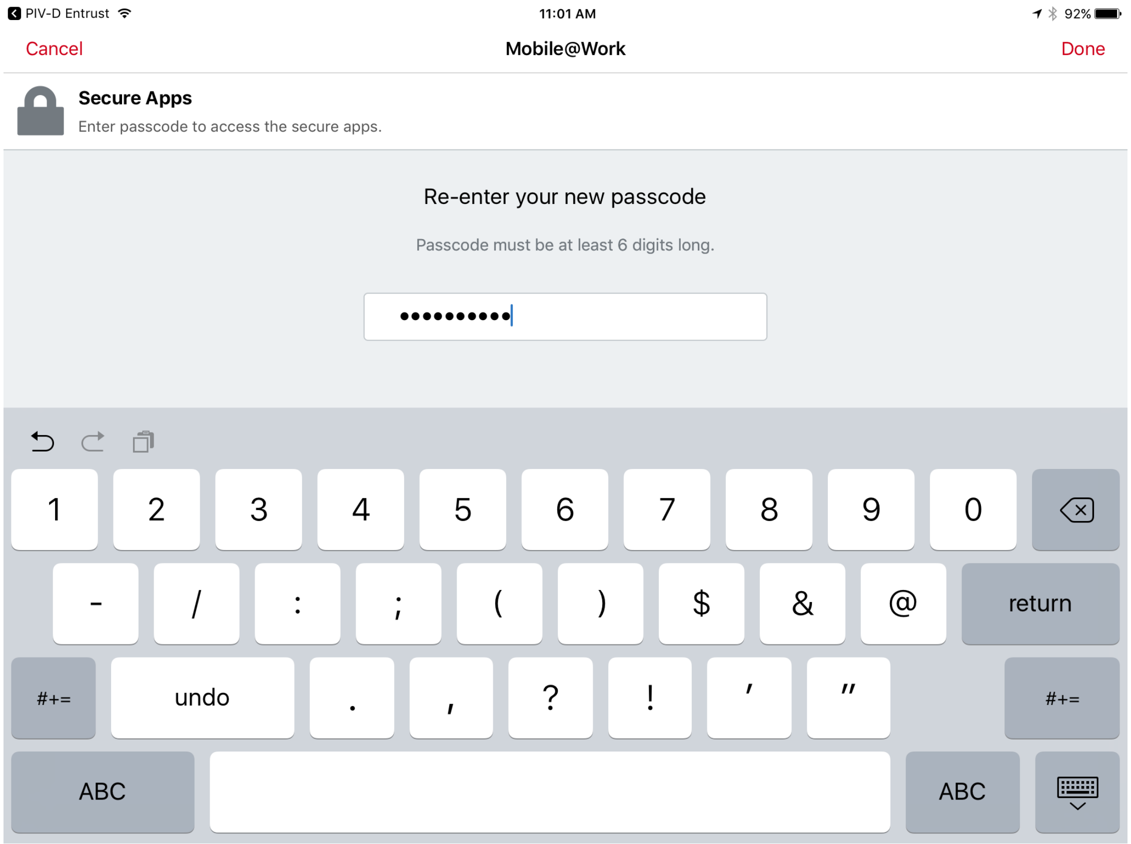
Passcode must be at least 6 digits long.

•••••••••••

Create more complex passcode

b. In the **Re-enter your new passcode** field, re-enter the password you entered in Step 2b.

c. Tap **Done**.



Secure Apps

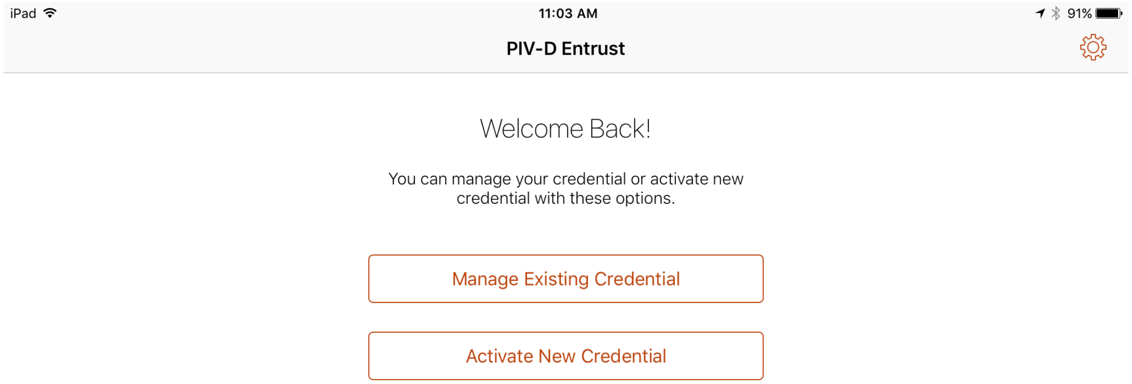
Enter passcode to access the secure apps.

Re-enter your new passcode

Passcode must be at least 6 digits long.

•••••••••••

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



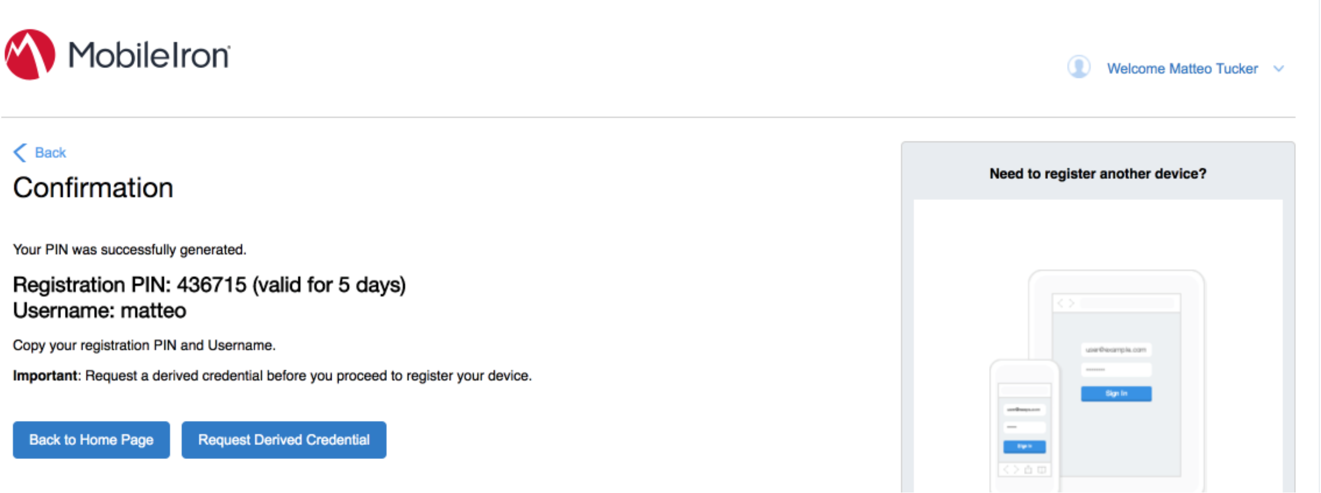
Welcome Back!

You can manage your credential or activate new credential with these options.

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

5. To request a DPC during the same session as registration with MobileIron:

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



Confirmation

Your PIN was successfully generated.

Registration PIN: 436715 (valid for 5 days)
Username: matteo

Copy your registration PIN and Username.

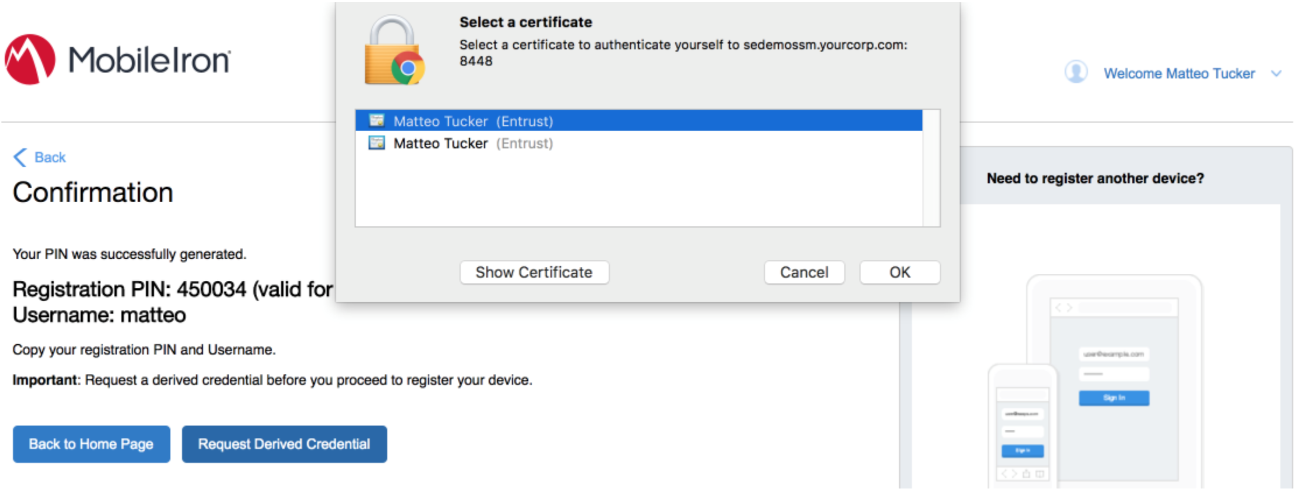
Important: Request a derived credential before you proceed to register your device.

   b. In the certificate selection dialogue:

      i. Select your PIV Authentication certificate from the list of available certificates. See Step 4 of Section 2.1.3.1.1 for additional steps to identify this certificate, as necessary.

      ii. Click **OK**.

      iii. Continue with Step 6.



Select a certificate

Select a certificate to authenticate yourself to sedemossm.yourcorp.com:8448

Matteo Tucker (Entrust)

Matteo Tucker (Entrust)

Confirmation

Your PIN was successfully generated.

Registration PIN: 450034 (valid for

Username: matteo

Copy your registration PIN and Username.

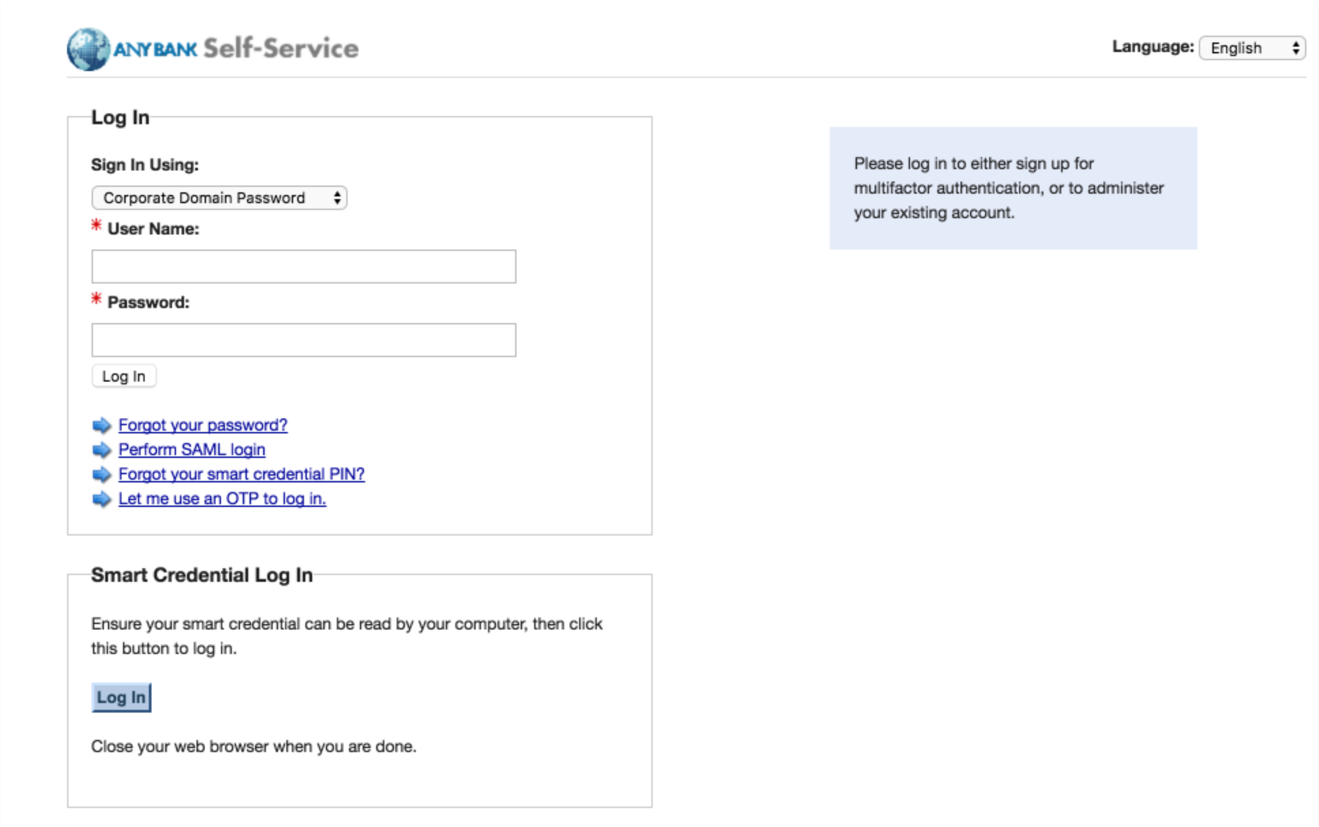
Important: Request a derived credential before you proceed to register your device.

6. To request a DPC in a new session:

    a. Using a web browser, visit the Entrust IDG Self-Service Portal URL provided by an administrator.

    b. In the Entrust IDG Self-Service Portal, under **Smart Credential Log In**, click **Log In**.

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



ANYBANK Self-Service

Language: English

Log In

Sign In Using:

Corporate Domain Password

* User Name:

* Password:

Log In

- Forgot your password?
- Perform SAML login
- Forgot your smart credential PIN?
- Let me use an OTP to log in.

Smart Credential Log In

Ensure your smart credential can be read by your computer, then click this button to log in.

Log In

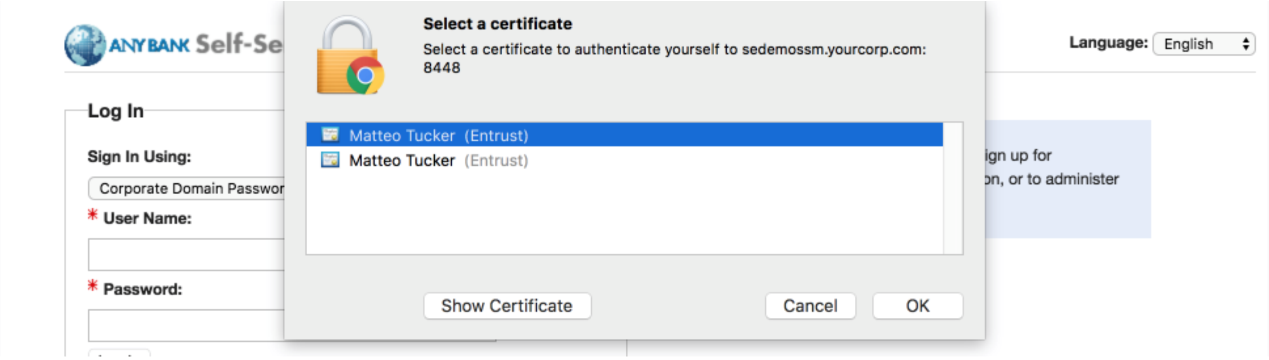
Close your web browser when you are done.

Please log in to either sign up for multifactor authentication, or to administer your existing account.

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

i. Select your PIV Authentication certificate from the list of available certificates. See Step 4 of Section 2.1.3.1.1 for additional steps to identify this certificate, as necessary.

ii. Click **OK**.



Select a certificate

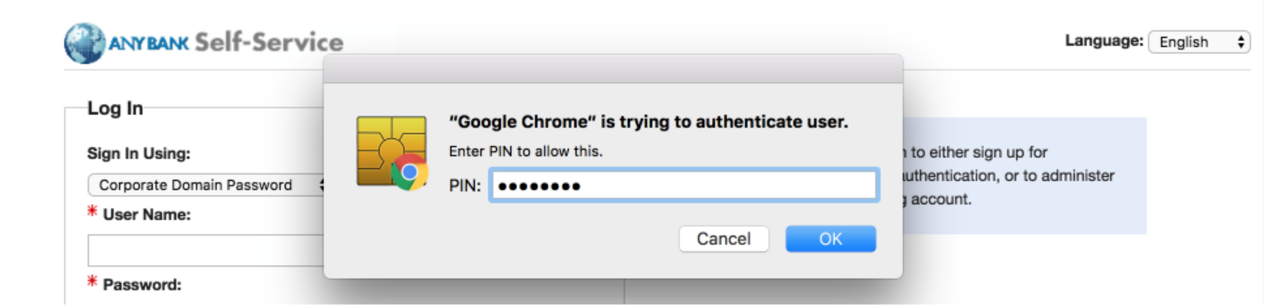
Select a certificate to authenticate yourself to sedemossm.yourcorp.com:8448

- Matteo Tucker (Entrust)
- Matteo Tucker (Entrust)

d. In the authentication dialogue:

   i. In the **PIN** field, enter the password to activate your PIV Card.

   ii. Click **OK**.

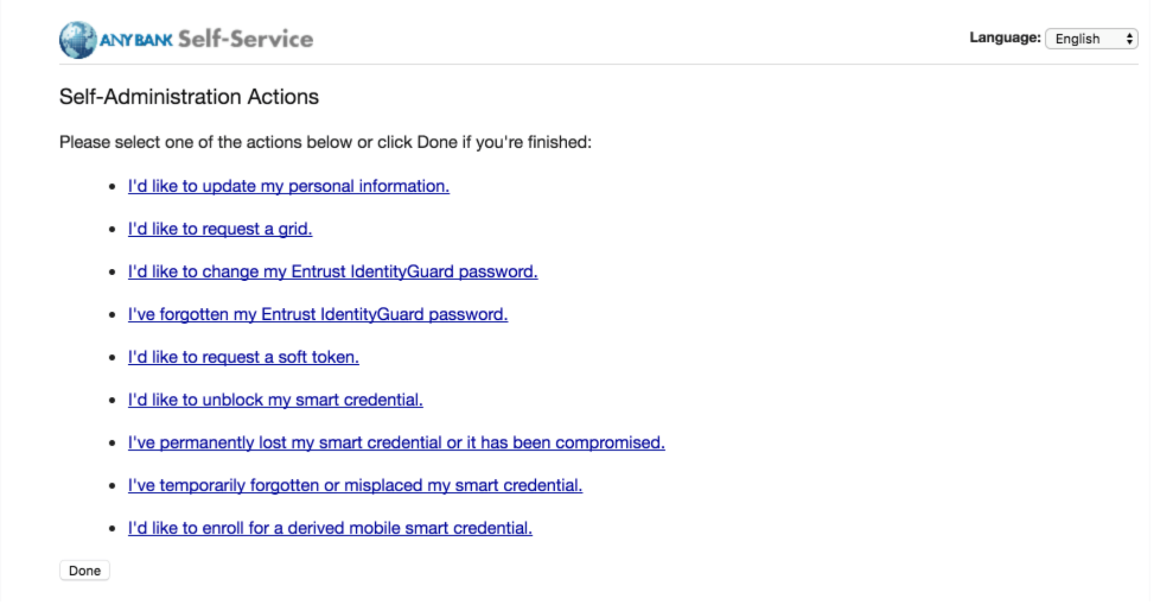


"Google Chrome" is trying to authenticate user.

Enter PIN to allow this.

PIN: •••••••••

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).



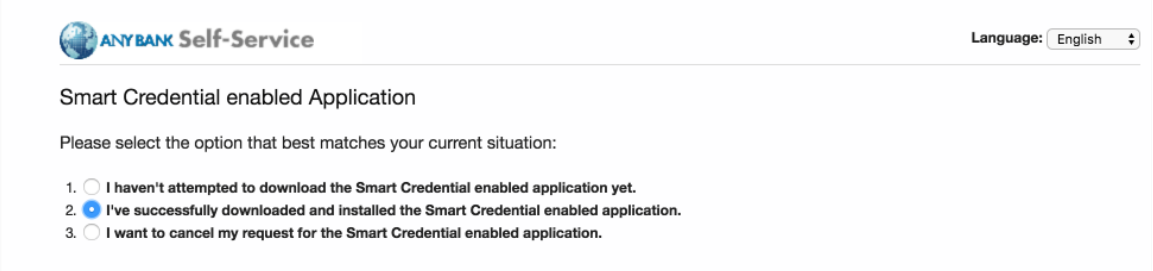
Language: English

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.

8. On the **Smart Credential enabled Application** page, select **Option 2: I've successfully downloaded and installed the Smart Credential enabled application**.



Language: English

Smart Credential enabled Application

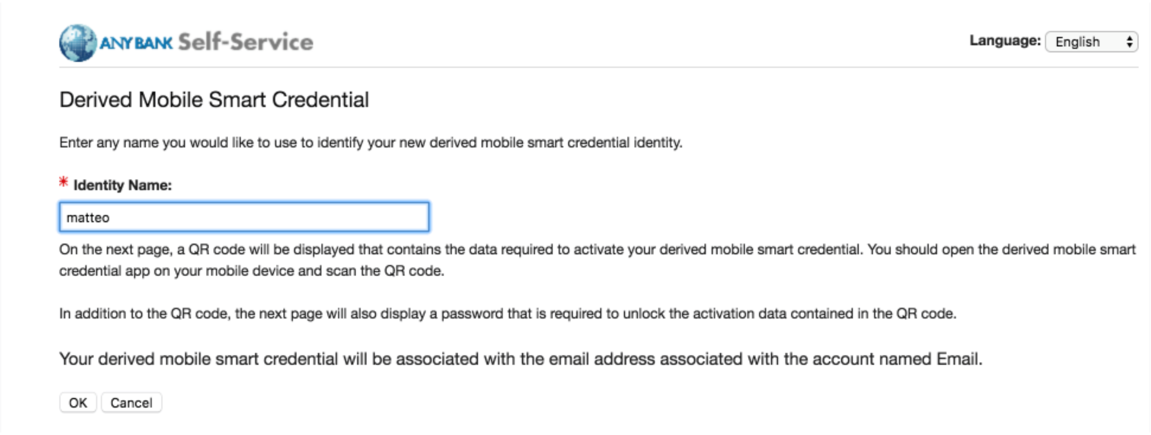
Please select the option that best matches your current situation:

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.**

9. On the **Derived Mobile Smart Credential** page:

    a. In the **Identity Name** field, enter your LDAP or MobileIron user ID.

    b. Click **OK**.



Derived Mobile Smart Credential

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

* Identity Name: matteo

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.

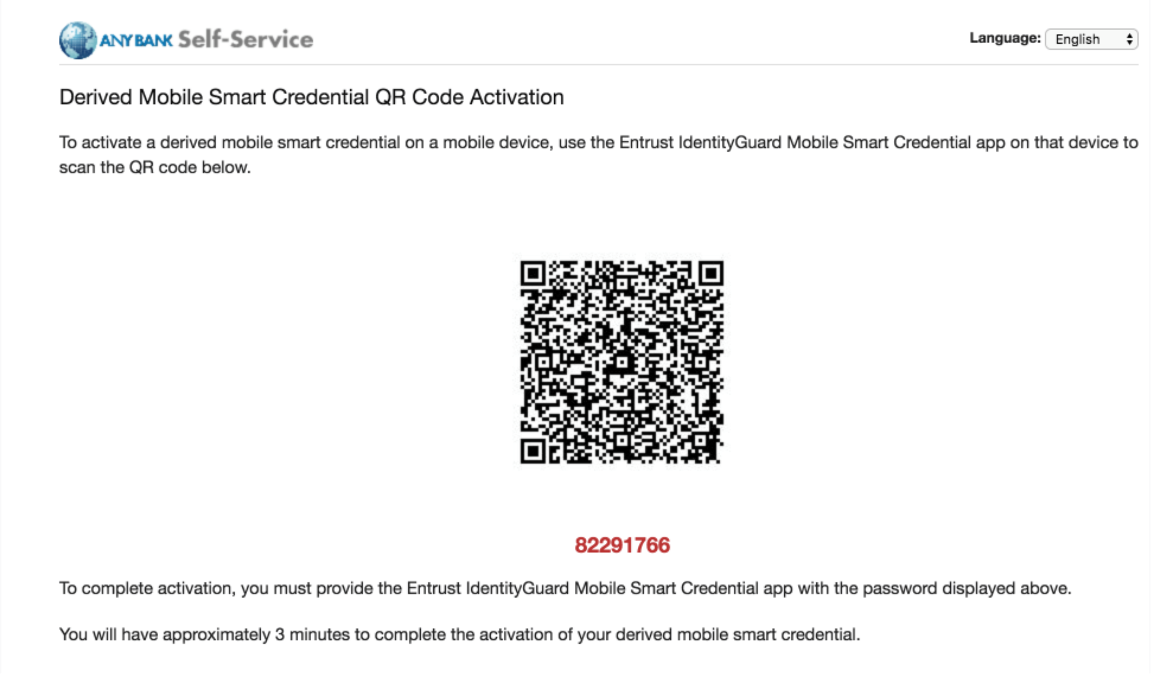
In addition to the QR code, the next page will also display a password that is required to unlock the activation data contained in the QR code.

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

10. The **Derived Mobile Smart Credential QR Code Activation** page displays information used in future steps; keep this page displayed. The workflow resumes using the MobileIron PIV-D Entrust application that is open on the target mobile device.

    Note: Steps 11–13 must be completed by using the target mobile device within approximately three minutes, otherwise Steps 7–10 must be repeated to generate new activation codes.

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



Derived Mobile Smart Credential QR Code Activation

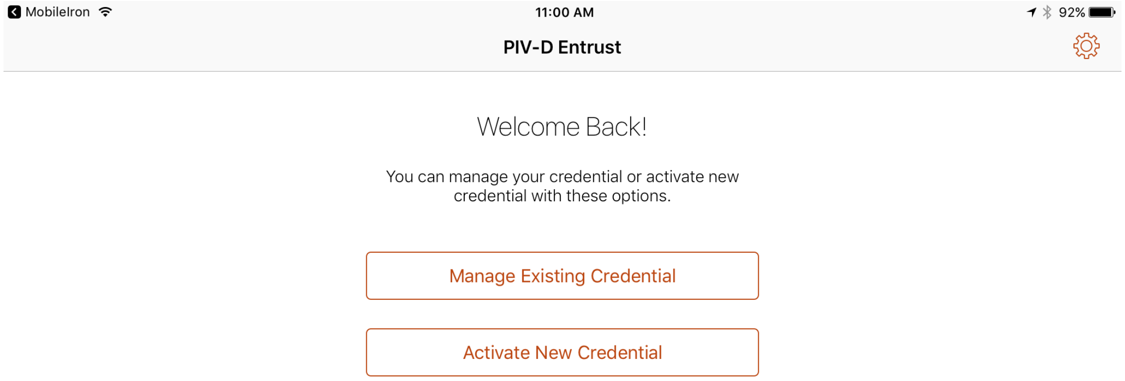
To activate a derived mobile smart credential on a mobile device, use the Entrust IdentityGuard Mobile Smart Credential app on that device to scan the QR code below.

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.

11. In the **PIV-D Entrust** application that is running on the target mobile device, tap **Activate New Credential**.

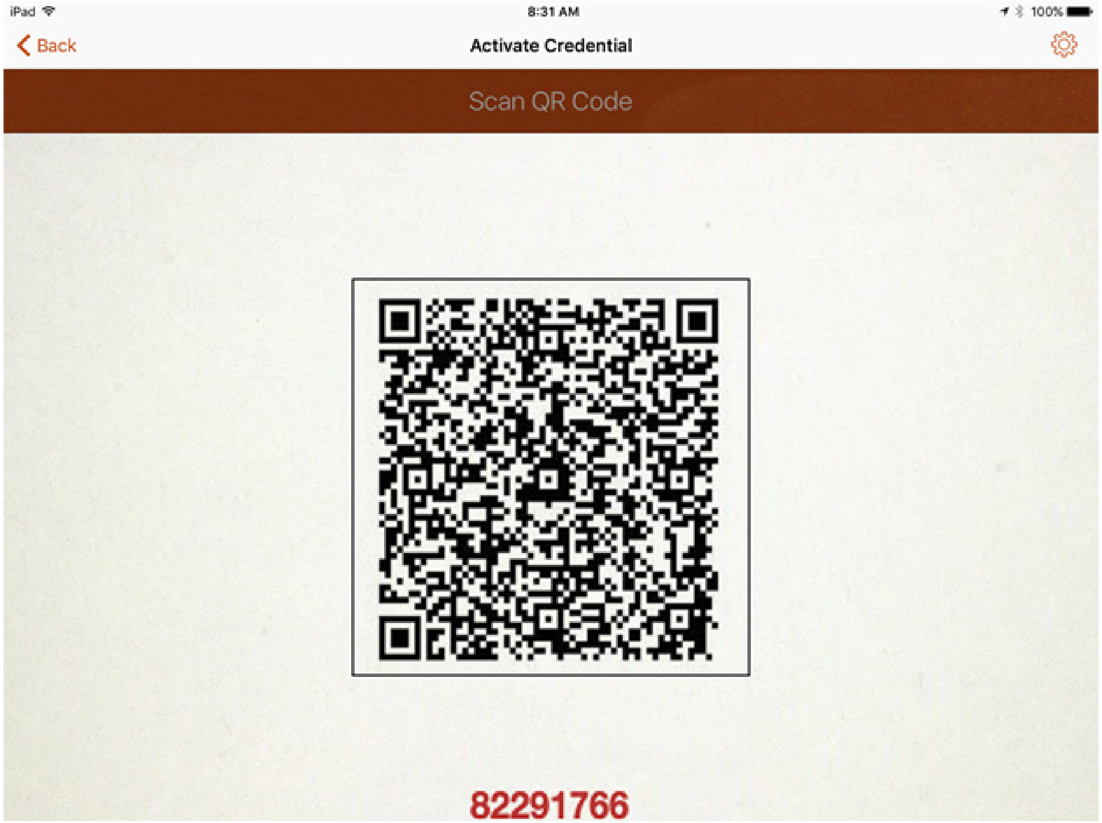


PIV-D Entrust

Welcome Back!

You can manage your credential or activate new credential with these options.

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.



Activate Credential

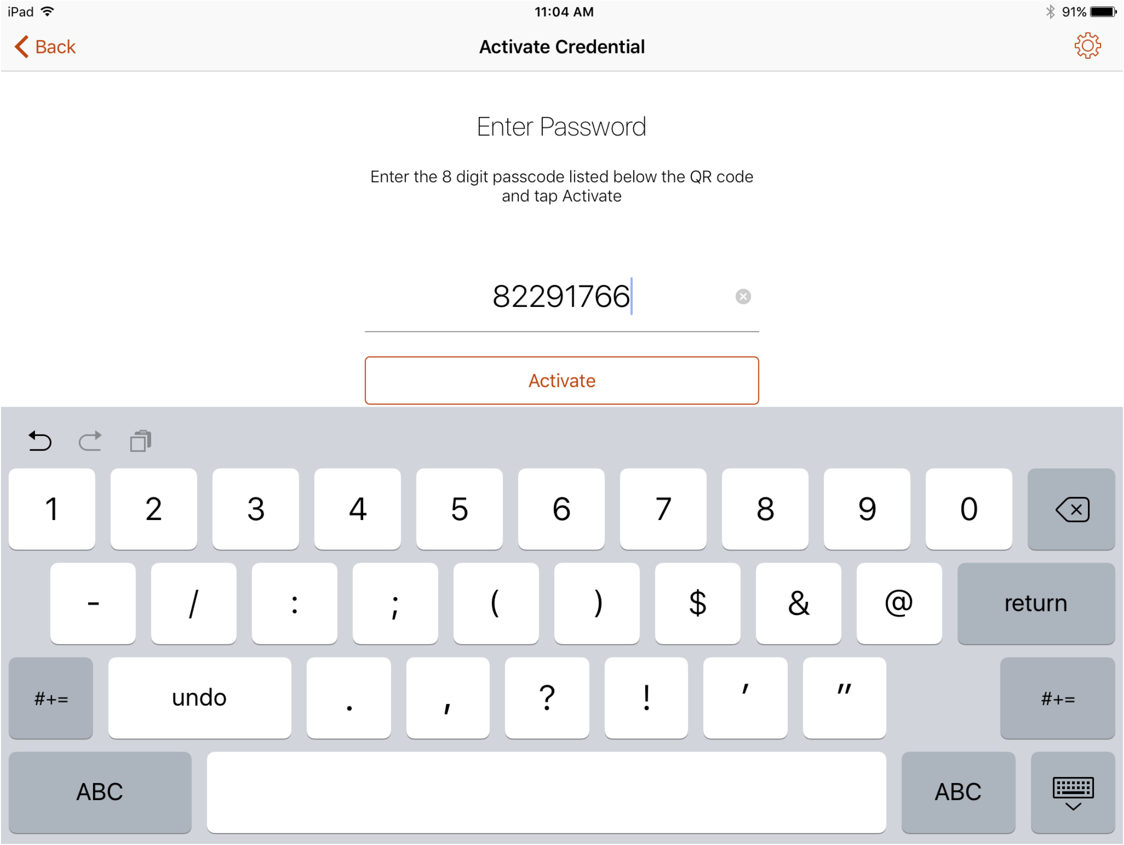
Scan QR Code

82291766

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

    a. Enter the **password** below the QR code that is displayed on the **Derived Mobile Smart Credential QR Code Activation** page (displayed by the same device used to perform Steps 4–10) as represented in Figure 2-3.

    b. Tap **Activate**.

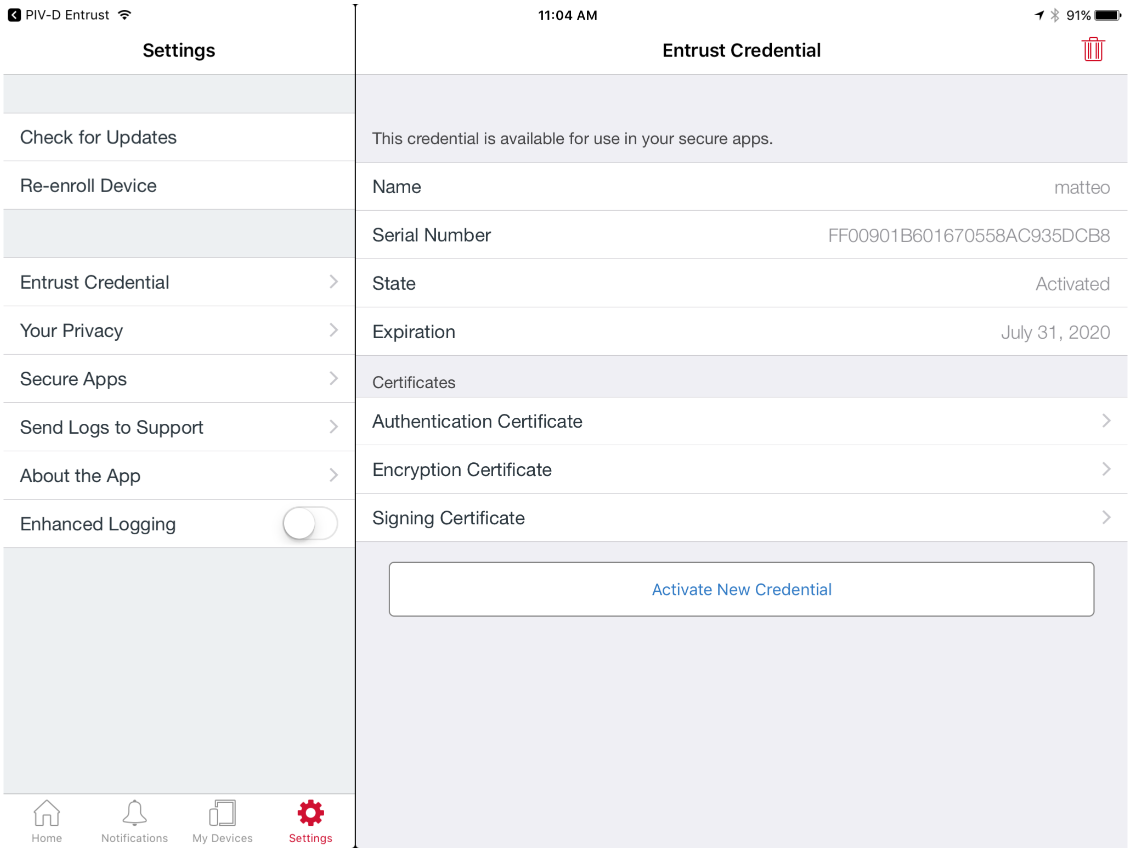


Enter Password

Enter the 8 digit passcode listed below the QR code and tap Activate

82291766

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



Check for Updates

Re-enroll Device

Entrust Credential

Your Privacy

Secure Apps

Send Logs to Support

About the App

Enhanced Logging

This credential is available for use in your secure apps.

Name	matteo
Serial Number	FF00901B601670558AC935DCB8
State	Activated
Expiration	July 31, 2020

Certificates

Authentication Certificate

Encryption Certificate

Signing Certificate

Activate New Credential

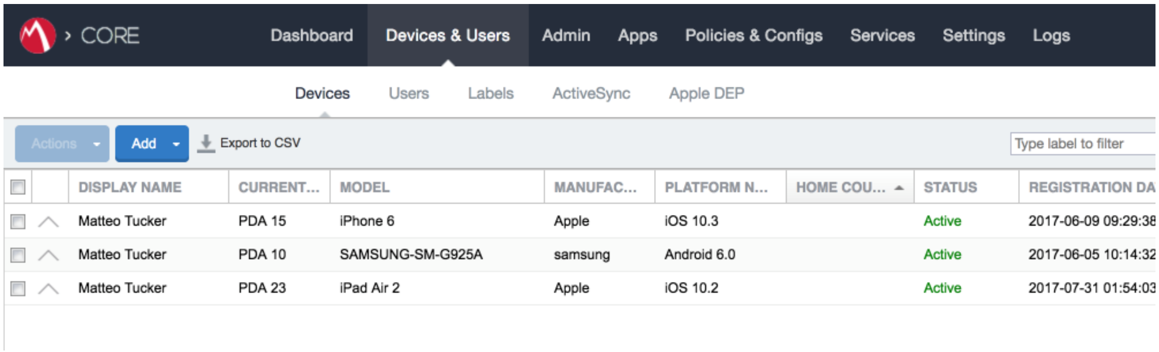
2.1.3.2 DPC Maintenance

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

2.1.3.3 DPC Termination

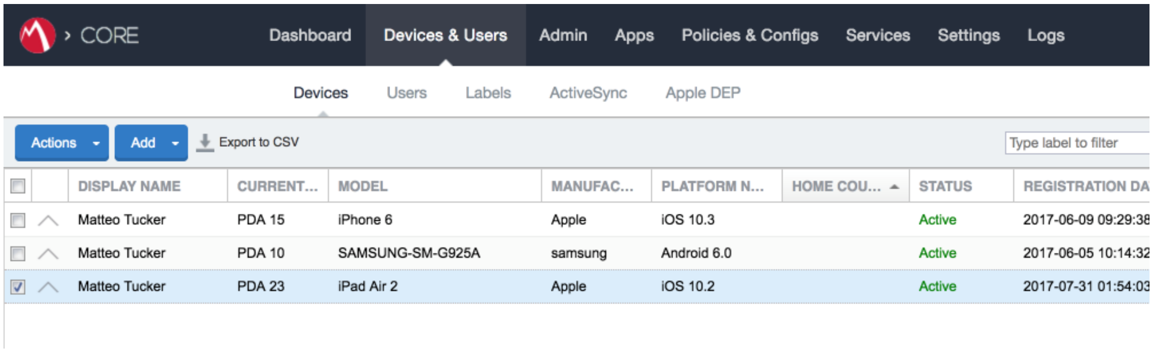
Termination of a DPC can be initiated from the MobileIron Admin Console. Upon completion of this workflow, the DPC stored in the MobileIron Apps@Work container will be cryptographically wiped (destroyed). These steps are performed by a MobileIron Core administrator.

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



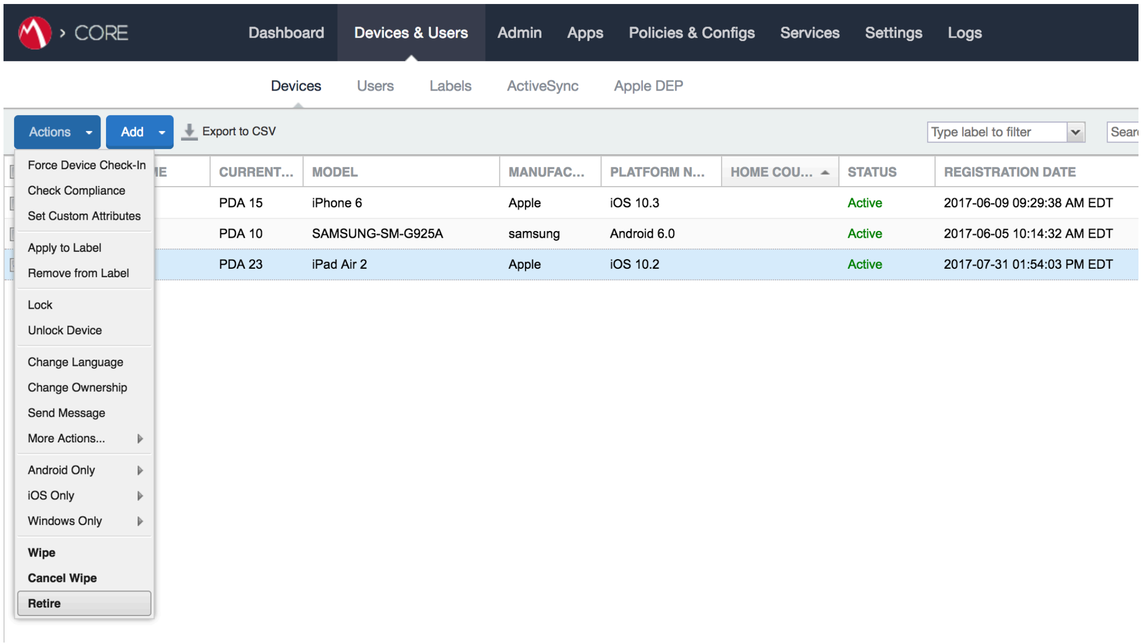
□		DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
□	︿	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
□	︿	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32
□	︿	Matteo Tucker	PDA 23	iPad Air 2	Apple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

2. Select the check box in the row identifying the mobile device to be retired.



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

3. Select **Actions > Retire**.

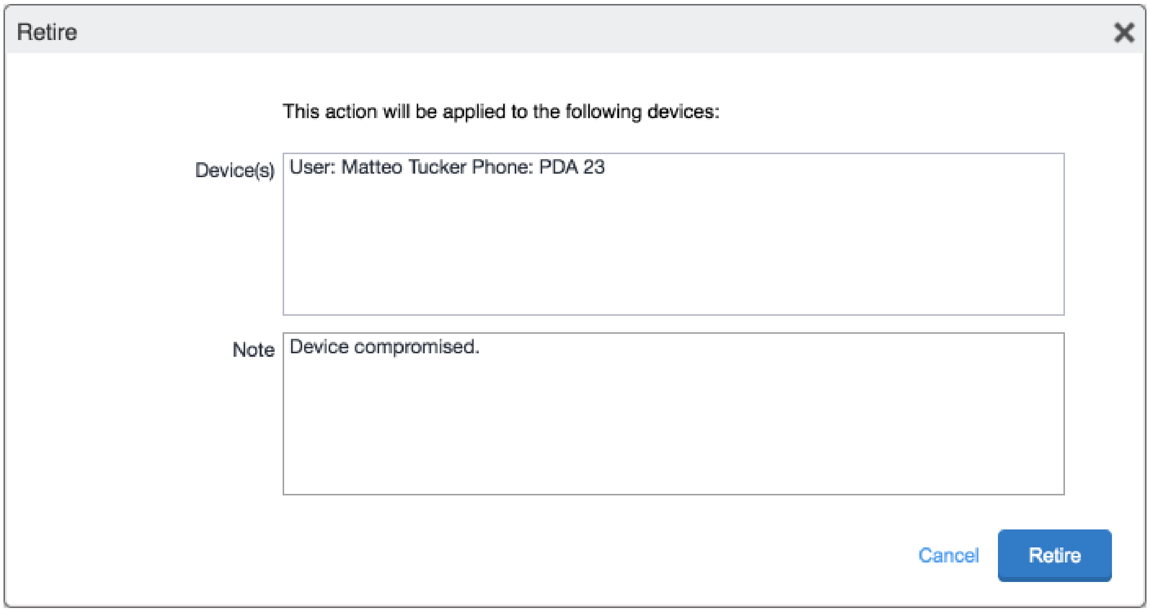


E	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DATE
	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38 AM EDT
	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32 AM EDT
	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03 PM EDT

4. In the **Retire** dialogue that appears:

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

   b. Select **Retire**.

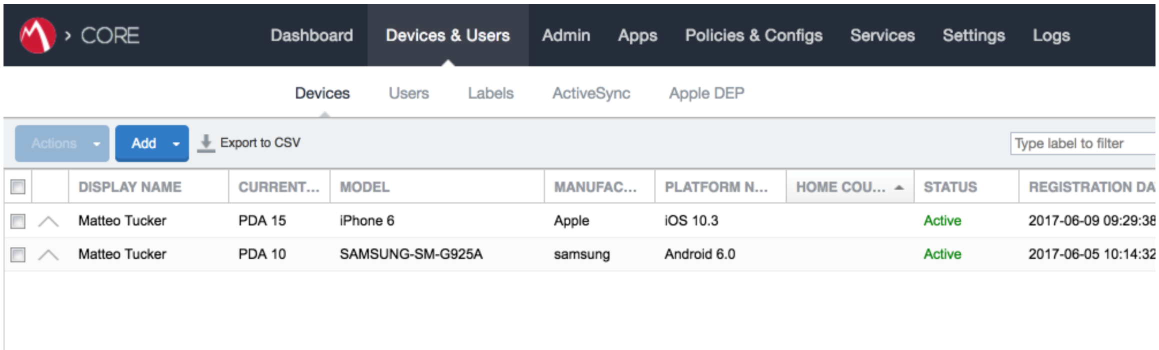


This action will be applied to the following devices:

Device(s): User: Matteo Tucker Phone: PDA 23

Note: Device compromised.

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
☐	︿	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
☐	︿	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32

The MobileIron PIV-D Entrust application now no longer reflects management by MobileIron. As a result, the DPC has been cryptographically wiped (destroyed) and its recovery is computationally infeasible.

2.2 Hybrid Architecture for PIV and DPC Life-Cycle Management

This section describes the installation and configuration of key products for the architecture depicted in Figure 2-4 and Figure 2-5, as well as demonstration of the DPC lifecycle management activities of initial issuance and termination. Figure 2-4 focuses on the mobile device implementation. Here, the Identity Agent application is used to manage the DPC. The DPC authentication key is stored in a software keystore within the secure container. The supporting cloud and enterprise systems as described above are also shown. Figure 2-5**Error! Reference source not found.** depicts the architecture when an Intel-based device that supports Intel Authenticate is used to store the DPC.

Figure 2-4 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Software Keystore)

Figure 2-5 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Intel Authenticate)

2.2.1 Intercede MyID CMS

Intercede offers its identity and credential management system (CMS) product, MyID, as a software solution that can be hosted in the cloud or deployed on premises. The MyID server platform is composed of an application server, database, and web server. It provides connectors to infrastructure components such as directories and PKIs, and application programming interfaces to enable integration with the organization’s identity and access management system. The MyID CMS is the core component for the architecture; as such, it should be fully configured and operational before other components.

2.2.1.1 Installation

Detailed instructions to install an instance of the MyID CMS are in the Intercede document *MyID Version 10.8 Installation and Configuration Guide*. Here, we document specific installation instructions for our environment.

The MyID system is modularly designed with web, application, and database tiers. In a production environment, it is likely that these tiers are separated onto multiple systems depending on performance and disaster recovery requirements. However, in our architecture, all tiers were installed on a Windows Server 2012 system due to resource constraints. Finally, role separation within the MyID system is not addressed here but should be considered before any deployment.

1. Install a supported version of Microsoft Structured Query Language (SQL) Server on the target MyID server. Our environment uses SQL Server 2012 with the SQL Server Database Engine and SQL Server Management Tools. See Components for specific component versions. A full settings document *(Exported-2017-07-27.vssettings)* is available from the NCCoE DPC project website. Refer to Microsoft's online documentation for specific installation procedures.

Table 2-3 SQL Server Components

Microsoft SQL Server Management Studio	11.0.5058.0
Microsoft Analysis Services Client Tools	11.0.5058.0
Microsoft Data Access Components (MDAC)	6.3.9600.17415
Microsoft Extensible Markup Language (MSXML)	3.0 6.0
Microsoft Internet Explorer	9.11.9600.18739
Microsoft .NET Framework	4.0.30319.42000
Operating System (OS)	6.3.9600

2.2.1.2 Verizon Shared Service Provider (SSP) PKI Integration

Detailed instructions to integrate Verizon SSP with MyID are in Intercede's *UniCERT UPI Certificate Authority Integration Guide*. Here, we document the specific configurations used within our builds.

1. Install the following prerequisites on the MyID server:

Component	Comment
Java Runtime Environment 8.0	Download and install the latest update from the Oracle website. This build uses 8u121.
Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8	Download and install from the Oracle website.

2. Obtain the following configuration settings from your managed PKI instance:

Setting	Comment
Verizon SSP CA Path	Distinguished name to directory instance supplied by Verizon
Verizon SSP Enrollment Agent	Distinguished name for the Registration Authority supplied by Verizon
Verizon SSP Service Point	URI endpoint of the Verizon SSP web service supplied by Verizon
Verizon SSP Registration Authority Operator PKCS#12	Credentials are supplied by Verizon SSP
Verizon SSP Registration Authority Operator PKCS#12 Password	

3. Create a CA configuration by using the following procedures:

    a. In **MyID Desktop,** select the **Configuration** category.

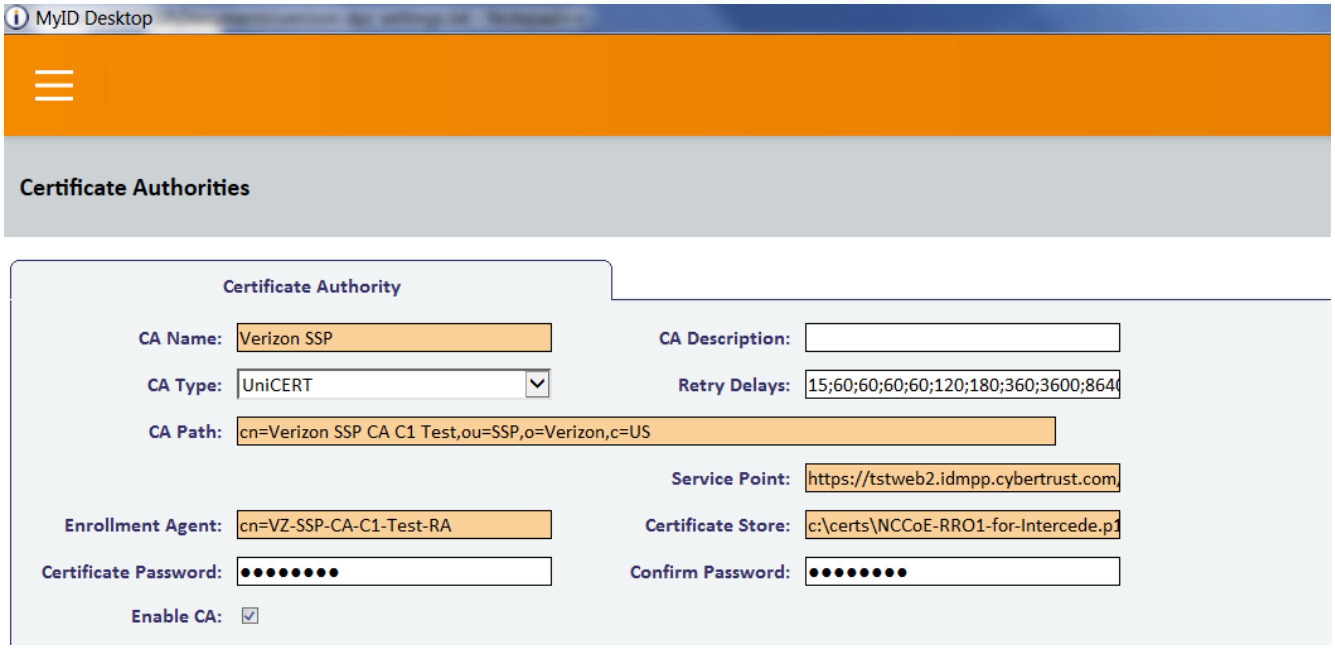
    b. Select **Certificate Authorities** from the **Configuration** menu.

    c. Select **New** from the **Select a CA** drop-down menu.

    d. From the **CA Type** drop-down menu, select **Entrust JTK**. A form with a setting specifically for the Entrust Datacard CA will appear.

    e. Fill in the **Certificate Authority** form with the following settings from Step 2:

CA Name	Enter a short name to identify the Verizon SSP
CA Description	Optional long description
CA Type	Leave this setting **UniCERT**
Retry Delays	Leave the defaults
CA Path	Retrieve setting from Step 2
Service Point	Retrieve setting from Step 2
Enrollment Agent	Retrieve setting from Step 2
Directory	Select the Entrust directory configured from Step **Error! Reference source not found.**
Certificate Store	Retrieve setting from Step 2 – enter fully qualified file path
Certificate Password	Retrieve setting from Step 2
Enable CA	Select this option



Certificate Authorities

Certificate Authority

CA Name:	Verizon SSP	CA Description:	
CA Type:	UniCERT	Retry Delays:	15;60;60;60;120;180;360;3600;864(
CA Path:	cn=Verizon SSP CA C1 Test,ou=SSP,o=Verizon,c=US		
		Service Point:	https://tstweb2.idmpp.cybertrust.com/
Enrollment Agent:	cn=VZ-SSP-CA-C1-Test-RA	Certificate Store:	c:\certs\NCCoE-RRO1-for-Intercede.p1
Certificate Password:	••••••••	Confirm Password:	••••••••
Enable CA:	☑		

f. Click **Save**.

4. Enable Verizon SSP CA policies by using the following procedures.

   a. Within **MyID Desktop**, click the **Configuration** category and choose **Certificate Authorities**.

   b. From the **CA Name** drop-down, select the **Verizon SSP CA** configured in Step 3.

   c. Click **Edit**.

   d. In the **Available Certificates** list, select **PIV-SSP-Derived-Auth-sw-1yr-v3** to enable it for DPC issuance.

   e. Click the **Enabled (Allow Issuance)** check box.

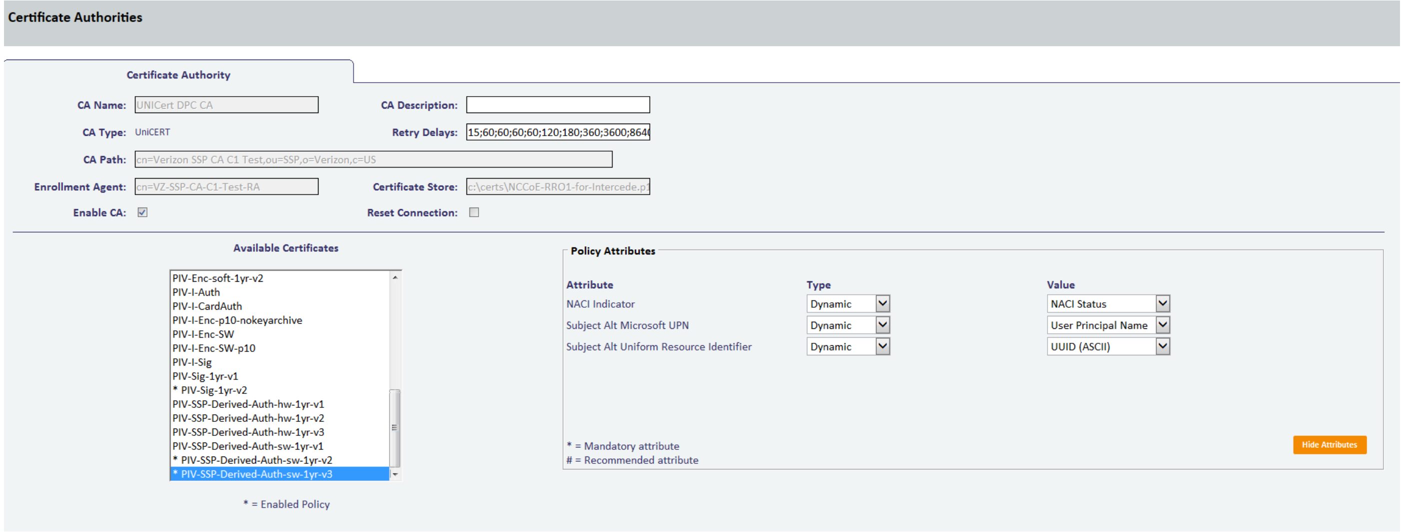
f. Set the following options for the policy.

Setting	Value
Display Name	Arbitrary name for this policy
Description	Optional description for this policy
Allow Identity Mapping	Unchecked
Reverse DN	Checked
Archive Keys	Unchecked
Certificate Lifetime	365
Automatic Renewal	Unchecked
Certificate Storage	Both
Recovery Storage	Both
CSP Name	Microsoft Enhanced Cryptographic Provider 1.0
Requires Validation	Unchecked
Private Key Exportable	Unchecked
User Protected	Unchecked
Key Algorithm	RSA 2048
Key Purpose	Signature

g. Click **Edit Attributes** and set the following values:

Attribute	Type	Value
NACI Indicator	Dynamic	NACI Status
Subject Alt Microsoft UPN	Dynamic	User Principal Name
Subject Alt Uniform Resource Identifier	Dynamic	UUID

Figure 2-6 Certificate Profile Attributes



Certificate Authorities

Certificate Authority

CA Name:	UNICert DPC CA	CA Description:	
CA Type:	UniCERT	Retry Delays:	15;60;60;60;60;120;180;360;3600;864(
CA Path:	cn=Verizon SSP CA C1 Test,ou=SSP,o=Verizon,c=US		
Enrollment Agent:	cn=VZ-SSP-CA-C1-Test-RA	Certificate Store:	c:\certs\NCCoE-RRO1-for-Intercede.p1
Enable CA:	☑	Reset Connection:	□

Available Certificates

PIV-Enc-soft-1yr-v2
PIV-I-Auth
PIV-I-CardAuth
PIV-I-Enc-p10-nokeyarchive
PIV-I-Enc-SW
PIV-I-Enc-SW-p10
PIV-I-Sig
PIV-Sig-1yr-v1
* PIV-Sig-1yr-v2
PIV-SSP-Derived-Auth-hw-1yr-v1
PIV-SSP-Derived-Auth-hw-1yr-v2
PIV-SSP-Derived-Auth-hw-1yr-v3
PIV-SSP-Derived-Auth-sw-1yr-v1
* PIV-SSP-Derived-Auth-sw-1yr-v2
* PIV-SSP-Derived-Auth-sw-1yr-v3

* = Enabled Policy

Policy Attributes

Attribute	Type	Value
NACI Indicator	Dynamic	NACI Status
Subject Alt Microsoft UPN	Dynamic	User Principal Name
Subject Alt Uniform Resource Identifier	Dynamic	UUID (ASCII)

* = Mandatory attribute
= Recommended attribute

5. Repeat Step 4 for the **PIV-Auth-1-yr-v2**, **PIV-CardAuth-1yr-v1**, and **PIV-Sig-1yr-v1** certificate profiles.

2.2.1.3 Configuration for DPC

Detailed instructions to configure an instance of the MyID CMS for DPC are in Intercede's *Derived Credentials Installation and Configuration Guide*. Here, we document the specific configurations used within our builds. Before you begin, you need the *Test Federal Common Policy CA* root certificate file, which can be downloaded from the Federal PKI test repository. Also obtain the intermediate certificates for the Verizon SSP certificate chain (Verizon SSP CA A2 Test and Verizon SSP CA C1 Test) from the Verizon certificate test repositories.

The first step in configuration is to create a content signing certificate that is used to sign data stored on the DPC mobile container. This certificate (and associated private key) must be made available to MyID through the Windows Cryptographic Application Interface (CAPI) store on the same server where the MyID server is installed. There are various ways to generate a certificate; in our environment we chose to create a certificate authority on a separate instance of Windows Server 2012.

1. Install Microsoft Certificate Services. There are a few online resources that can assist in the installation process. We suggest the Adding Active Directory Certificate Services to a Lab Environment tutorial from the Microsoft Developer Network.

    a. Add a certificate template. For reference, we have exported the certificate template (PIVContentSigning) that we used for the content signing certificate. The configuration file (CertificateTemplates.xml) is available for download from the NCCoE DPC project website. A script to import the certificate template can be found at the Microsoft Script Center.

2. Request a content signing certificate from the MyID system by using the procedures noted in the "Request a Certificate" TechNet article.

3. Save the content signing certificate in binary format to the **Components** folder of the MyID installation folder.

4. Edit the system registry with the following procedures:

    a. From the **Start** menu:

        i. Select **Run**.

        ii. Type `regedit` in the dialogue displayed.

        iii. Click **OK**.

    b. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\ContentSigning**.

    c. Check that the value of the following string is set:

       Active – set to **WebService**.

    d. Set the value of the following string to the full path of the certificate on the application server:

       For example: *C:\Program Files (x86)\Intercede\MyID\Components\contentcert.cer*

5. Set the location of the MyID web service that allows a mobile device to collect the DPC by using the following procedures within MyID Desktop:

    a. From the **Configuration** category, select the **Operation Settings** workflow.

    b. Click the **Certificates** tab.

    c. Set the **Mobile Certificate Recovery Service URL** option to the location of the MyID Process Driver web service host.

       For example: https://<replace-with-your-hostname>

    d. Click **Save Changes**.

6. Set which PIV Cards are available for DPC by using the following procedures within MyID Desktop:

    a. From the **Configuration** category, select the **Operation Settings** workflow.

    b. Click the **Certificates** tab.

    c. To allow eligibility for all PIV Federal Agency Smart Card Number (FASC-N) values, set **Cards allowed for derivation** to **.+** (dot plus).

    d. Click **Save Changes**.

7. Configure the system to check the revocation status of the PIV Authentication certificate to seven days by using the following procedures within MyID Desktop:

    a. From the **Configuration** category, select **Operation Settings**.

    b. On the **Certificates** tab, set **Derived credential revocation check offset** to **7**.

    c. Click **Save Changes**.

8. Grant access to the following workflows by using the MyID Desktop: Request Derived Credentials, Cancel Credential, Enable/Disable ID, Request Replacement ID, Unlock Credential, Collect My Updates.

    a. From the **Configuration** category, select the **Edit Roles** workflow.

    b. Select the check box for each of the roles to which you want to grant access. In our environment, **Startup User** was selected for all workflows.

    c. Click **Save Changes**.

9. Edit the workflows from Step 8 with the appropriate permissions.

    a. From the **Configuration** category, select the **Edit Roles** workflow.

    b. Click **Show/Hide Roles**.

    c. Select the check boxes for **Mobile User, Derived Credential Owner,** and **PIV Applicant**.

    d. Click **Close**.

    e. Select the corresponding roles:

Role	Permission
Mobile User	Console Logon, Request Derived Credentials (part 1), Mobile Certificate Recovery, Collect My Updates, Issue Device
Derived Credential Owner	Console Logon, Request Derived Credentials (part 2), Collect My Updates, Issue Device
PIV Applicant	Request Derived Credentials (part 2), Collect My Updates

10. Import the Test Federal Common Policy CA certificate into the MyID application server by using the following command as an administrator. This enables the administrator to control the PKI hierarchy that is trusted when verifying PIV cards:

```
certutil -addstore -f -Enterprise DerivedCredentialTrustedRoots RootCA.cer
```

11. Configure the MyID system with the PIV Authentication and Digital Signature certificate policy Object Identifiers (OIDs) by using the following procedures. The values shown below are production values, so they may need to be changed for your organization:

    a. From the MyID Desktop **Configuration** category, select **Operation Settings.**

b. On the **Certificates** tab, set the following values:

Setting	Value
Derived credential certificate OID	2.16.840.1.101.3.2.1.3.13

Derived credential signing certificate OID	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.16

12. Create an Identity Agent credential profile for the DPC by using the following procedures:

a. From the MyID Desktop **Configuration** category, select **Credential Profiles.**

b. Click **New.**

c. In the **Name** field, enter a descriptive name for the profile.

d. In **Card Encoding,** select **Identity Agent (Only)** and **Derived Credential.**

e. In **Services,** leave default selections **MyID Logon** and **MyID Encryption.**

f. In **Issuance Settings,** in the **Mobile Device Restrictions** drop-down, select **Any.**

g. In **Issuance Settings, Require Facial Biometrics,** select **Never Required.**

h. In **PIN Settings,** configure the following settings:

Setting	Value
Authentication Mode	PIN
Maximum PIN Length	12
Minimum PIN Length	6
Repeated Characters Allowed	1
Sequential Characters Allowed	1
Logon Attempts	5
PIN Inactivity Time	180
PIN History	0
Issue With	User specified PIN (default)
Email PIN	Unselect
Length	0

i. In **Device Profiles,** select **PIVDerivedCredential.xml** from the **Card Format** drop-down.

j. Click **Next.**

k. In the **Select Certificates** tab, check **PIV-SSP-Derived-Auth-sw-1yr-v3** along with **Signing** under **Certificate Policy Description.** Choose **Authentication Certificate** in the **Container** drop-down.

l. Click **Next.**

m. Select the roles that receive, issue, and validate DPC. **All** was chosen in this example.

n. Click **Next.**

o. Select **PIV_CON** in the **Select Card Layout** tab.

p. Click **Next.**

q. Enter text into the **Comments** and click **Next,** then **Finish.**

2.2.2 Intercede MyID Identity Agent

The MyID Identity Agent runs as an application and interfaces with the MyID CMS and supports a wide range of mobile devices and credential stores, including the device native key store, software key store, and microSD. The MyID Identity Agent mobile application is required to issue and manage DPC. No special configuration is necessary after installing the application; scanning the QR code during the initial enrollment directs the Identity Agent to your instance of MyID CMS. MyID Identity Agent is supported for both iOS and Android platforms.

2.2.2.1 Installation

MyID Identity Agent is available on the Google Play Store and the Apple App Store. Detailed installation procedures are found on the Google Play Store and Apple App Store support sites.

2.2.3 Intercede Desktop Client

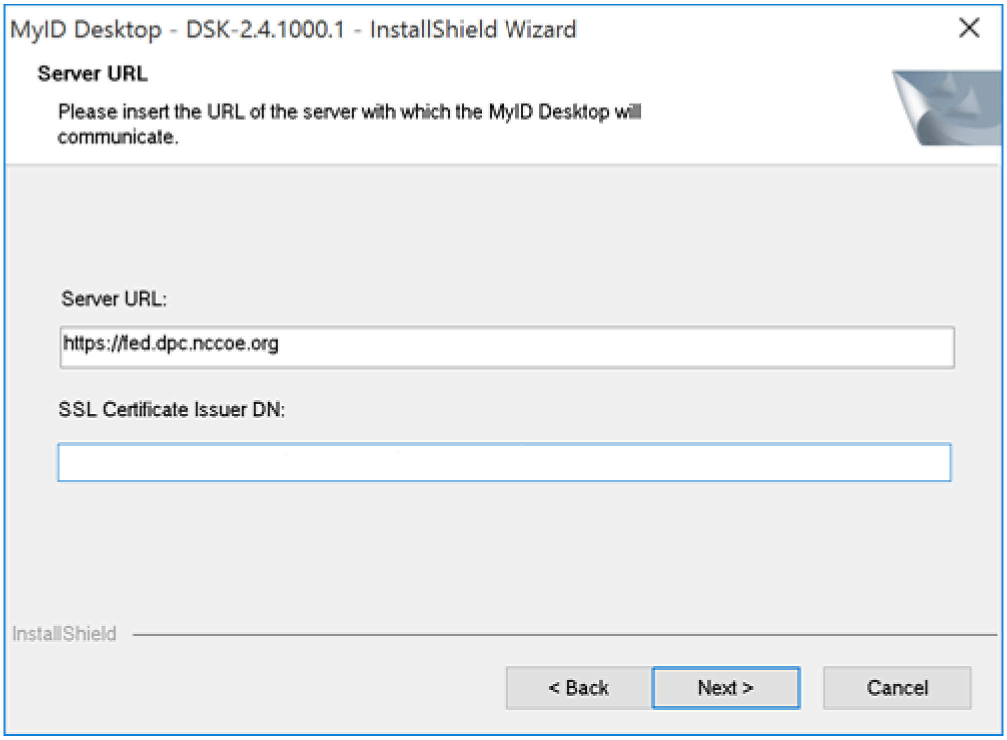
The Intercede Desktop component of this example solution serves as the main point of administration of the MyID CMS. It was installed on a Dell Latitude E6540 laptop running Windows 7. The procedures below are adapted from the *Installation and Configuration Guide Version 10.8,* Section 7.4.

2.2.3.1 Installation

Before installation, have available the hostname and the Distinguished Name (DN) of the issuer of the Transport Layer Security (TLS) certificate used to communicate with the MyID application server.

1. Run the provided *.msi* file as an administrator.
2. Select the destination location, then click **Next.**

3. Select the desired shortcuts to be installed.
4. Click **Next.**
5. In the **MyID Desktop InstallShield Wizard:**
    a. In the **Server URL** field, enter the **URL** for your instance of MyID Server.
    b. In the **SSL Certificate Issuer DN** field, leave empty as this prompt is applicable only when mutual TLS is implemented.
    c. Click **Next.**
    d. Click **Install.**


MyID Desktop - DSK-2.4.1000.1 - InstallShield Wizard

Server URL

Please insert the URL of the server with which the MyID Desktop will communicate.

Server URL:

https://fed.dpc.nccoe.org

SSL Certificate Issuer DN:

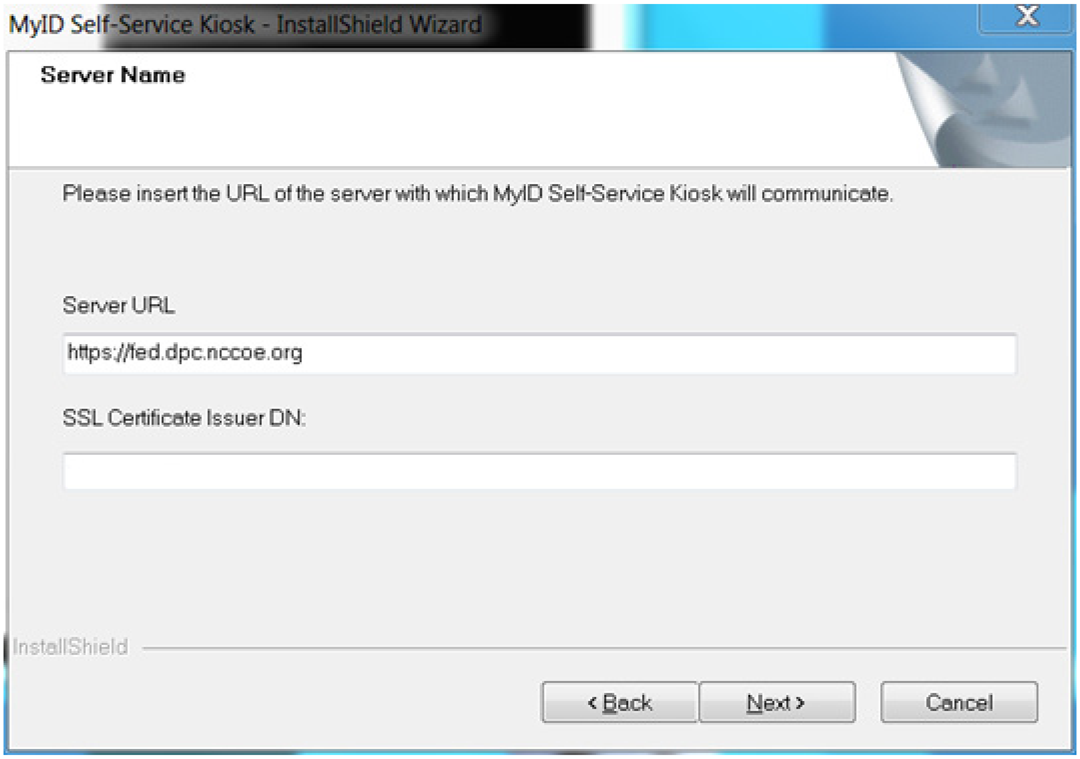
2.2.4 Intercede Self-Service Kiosk

The MyID Self-Service Kiosk serves as a DPC issuance station for eligible PIV holders. While the software is designed to run on a shared Windows system as a kiosk in public space, in this example it is installed on a Dell Latitude E6540 laptop running Windows 7. The procedures below are adapted from *Self-Service Kiosk Installation and Configuration* and *Derived Credentials Installation and Configuration Guide*.

2.2.4.1 Installation

Before installation, have available the hostname and the issuer distinguished name of the TLS certificate used to communicate with the MyID application server.

1. Click **Next.**
2. Accept default and click **Next.**
3. In the **MyID Self-Service Kiosk InstallShield Wizard:**
    a. In the **Server URL** field, enter the **URL** of your instance of MyID Server.
    b. In the **SSL Certificate Issuer DN** field, leave empty as this prompt is applicable only when mutual TLS is implemented.
    c. Select **Next.**
    d. Select **Install.**
    e. Select **Finish.**



MyID Self-Service Kiosk - InstallShield Wizard

Server Name

Please insert the URL of the server with which MyID Self-Service Kiosk will communicate.

Server URL

https://fed.dpc.nccoe.org

SSL Certificate Issuer DN:

2.2.4.2 Configuration

Use the following procedures to configure the MyID Self-Service Kiosk for DPC issuance:

1. Set the timeout for the PIN entry screen by using the following procedures:
   a. Open C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\MyIDKiosk.exe.config by using a text editor.
   b. Edit the **value** parameter in the following line:

   ```
   <add key="DerivedCredentialsPageTimeoutSeconds" value="120"/>
   ```

   c. Edit the **value** parameter in the following line with the MyID application server address:

   ```
   <add key="Server" value="http://myserver.example.com/"></add>
   ```

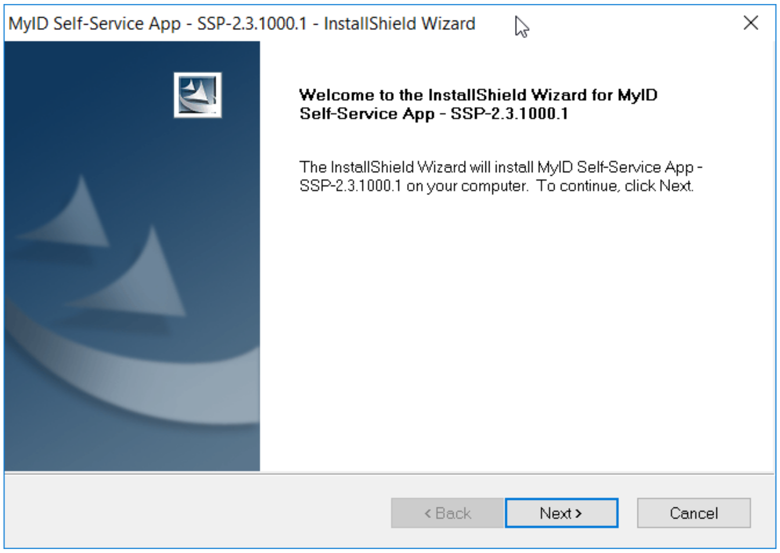
   d. Save changes to the file.

2.2.5 Windows Client Installation for MyID and Intel Authenticate

The *Intel Authenticate Integration Guide for Active Directory Policy Objects* provides instructions on how to set up Group Policy Objects for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the *Intel Authenticate Integration Guide*.

2.2.5.1 Installing the MyID Self-Service Application

1. Run **SSP-2.3.1000.1_E.msi** on the client computer.
2. Click **Next**.

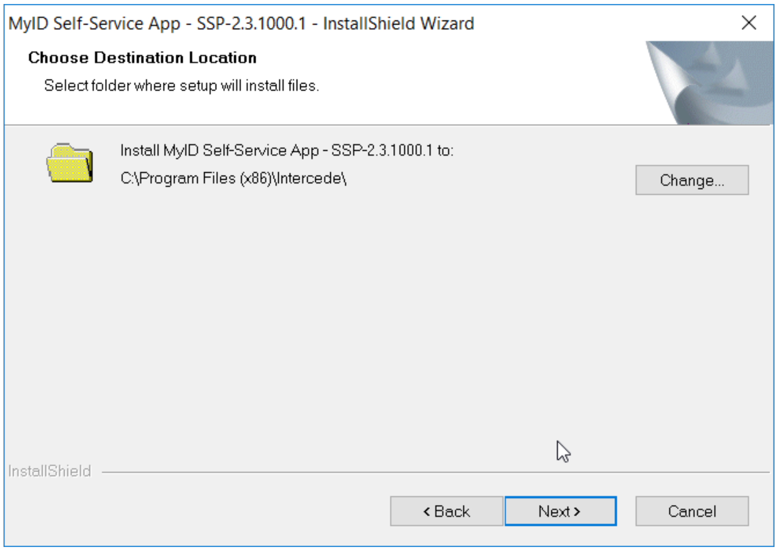


MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for MyID Self-Service App - SSP-2.3.1000.1

The InstallShield Wizard will install MyID Self-Service App - SSP-2.3.1000.1 on your computer. To continue, click Next.

3. Click **Next**.



MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

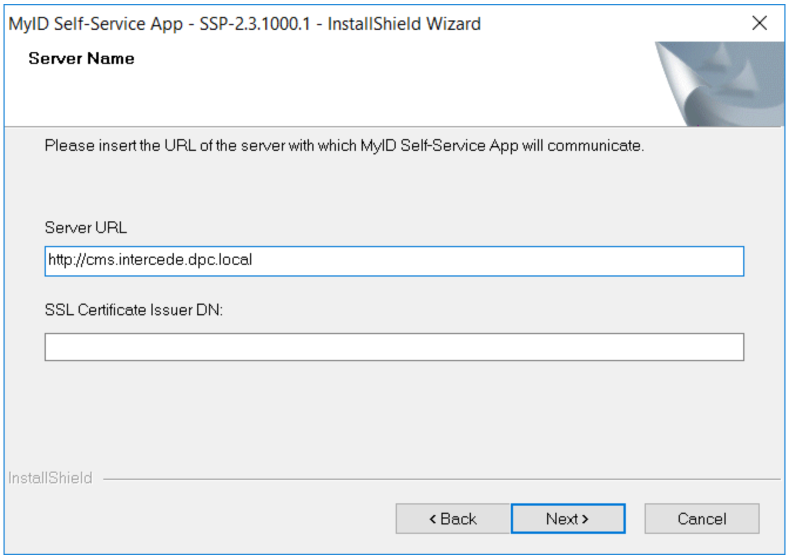
Choose Destination Location

Select folder where setup will install files.

Install MyID Self-Service App - SSP-2.3.1000.1 to:
C:\Program Files (x86)\Intercede\

4. Enter the **Server URL** for your organization's MyID server. Leave the **SSL Certificate Issuer DN** field empty, as this prompt is applicable only when mutual TLS is implemented.

5. Click **Next**.



MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

Server Name

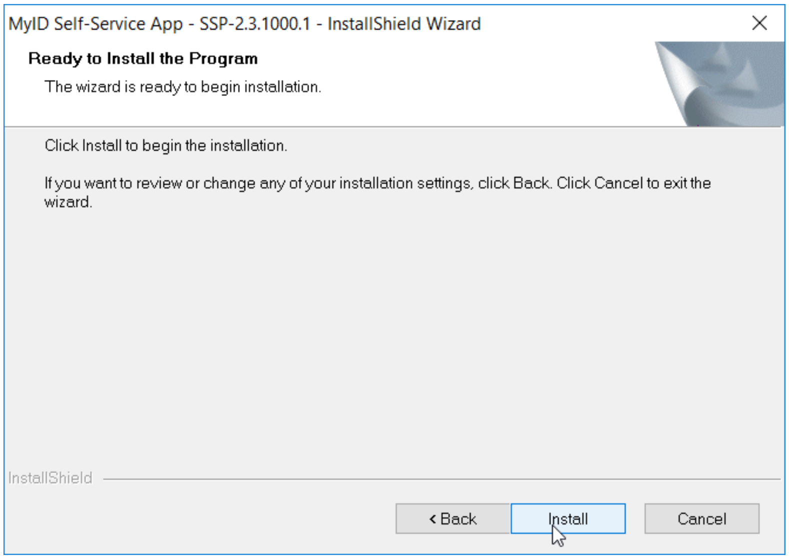
Please insert the URL of the server with which MyID Self-Service App will communicate.

Server URL

http://cms.intercede.dpc.local

SSL Certificate Issuer DN:

6. Click **Install**.



MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

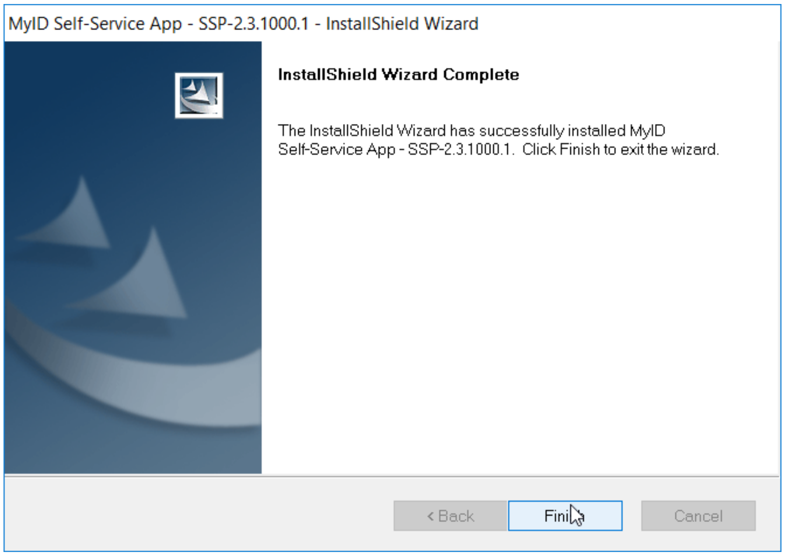
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click **Finish**.

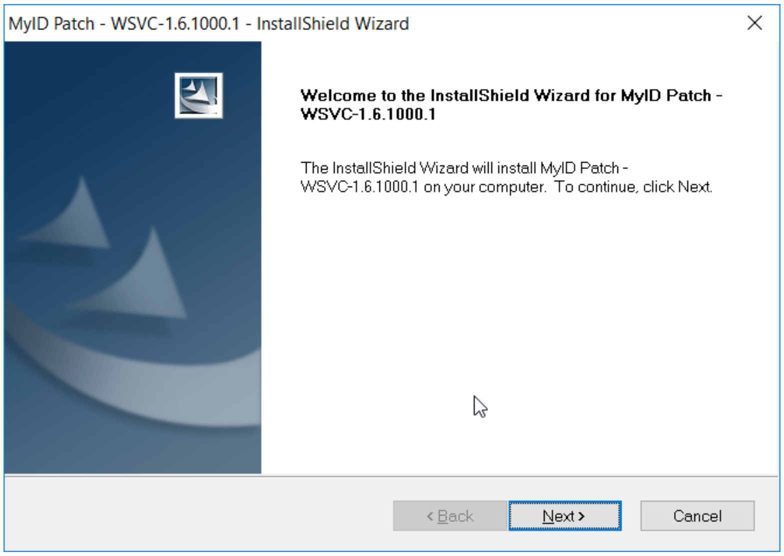

MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed MyID Self-Service App - SSP-2.3.1000.1. Click Finish to exit the wizard.

2.2.5.2 Installing the WSVC Service

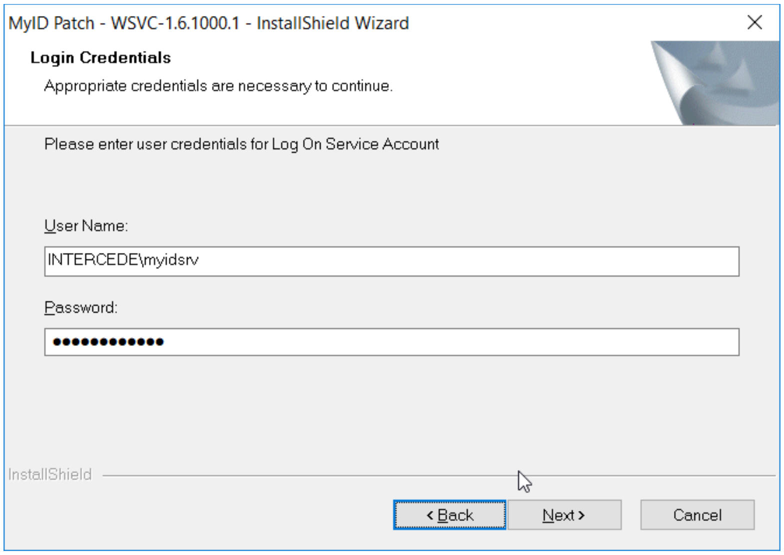
1. Run **WSVC-1.6.1000.1_B.msi.**
2. Click **Next.**


MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for MyID Patch - WSVC-1.6.1000.1

The InstallShield Wizard will install MyID Patch - WSVC-1.6.1000.1 on your computer. To continue, click Next.

3. Enter the username and password for the account that will install the service.
4. Click **Next.**



MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Login Credentials

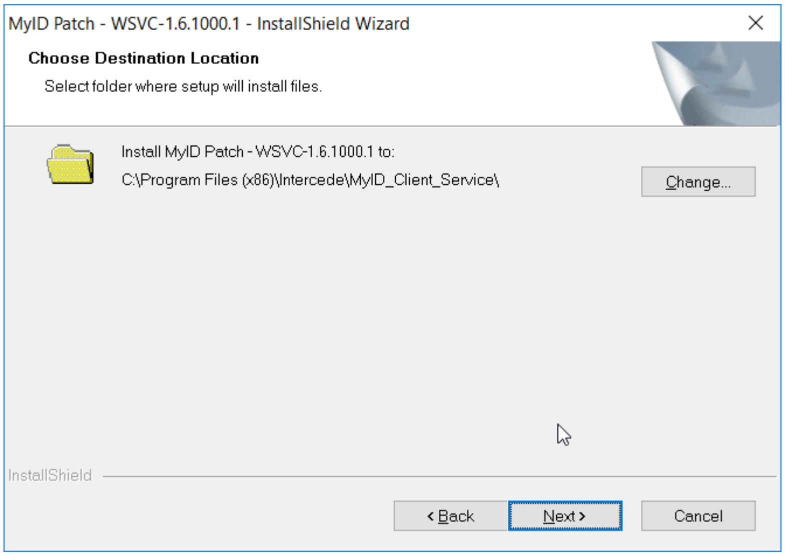
Appropriate credentials are necessary to continue.

Please enter user credentials for Log On Service Account

User Name: INTERCEDE\myidsrv

Password: ●●●●●●●●●●●●●

5. Click **Next.**



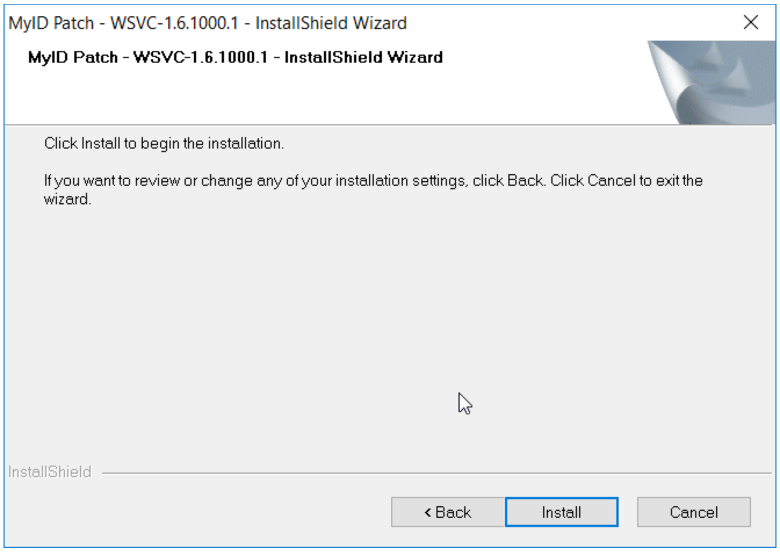
MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Install MyID Patch - WSVC-1.6.1000.1 to:
C:\Program Files (x86)\Intercede\MyID_Client_Service\

6. Click **Install.**



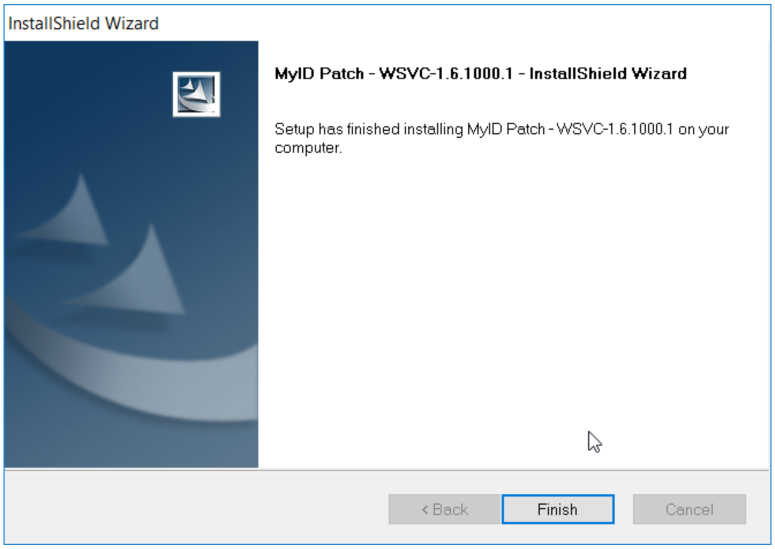
MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click **Finish.**



InstallShield Wizard

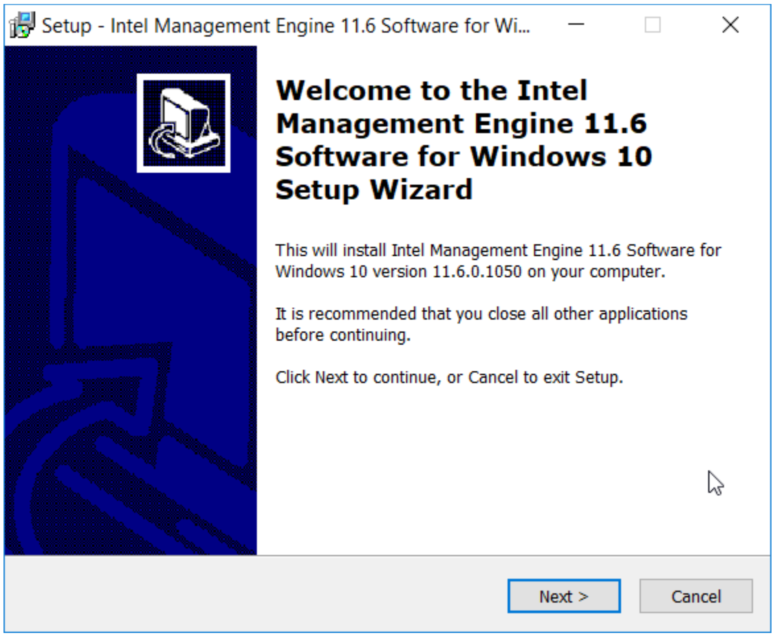
MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Setup has finished installing MyID Patch - WSVC-1.6.1000.1 on your computer.

2.2.5.3 Installing Prerequisites for Intel Authenticate

This process may differ depending on the client system. Primarily, it is important that the Intel Management Engine is installed and that any Intel drivers are up-to-date so that the Intel Authenticate Precheck is successful.

1. Run **n1cra26w.exe.** (The name may differ based on your system—this is the Intel Management Engine.)
2. Click **Next.**



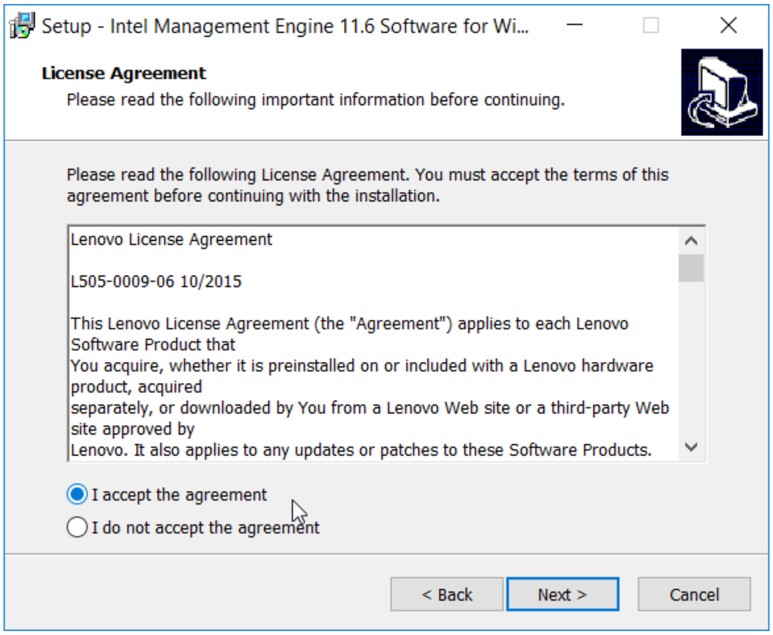
Welcome to the Intel Management Engine 11.6 Software for Windows 10 Setup Wizard

This will install Intel Management Engine 11.6 Software for Windows 10 version 11.6.0.1050 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

3. Select **I accept the agreement.**
4. Click **Next.**



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

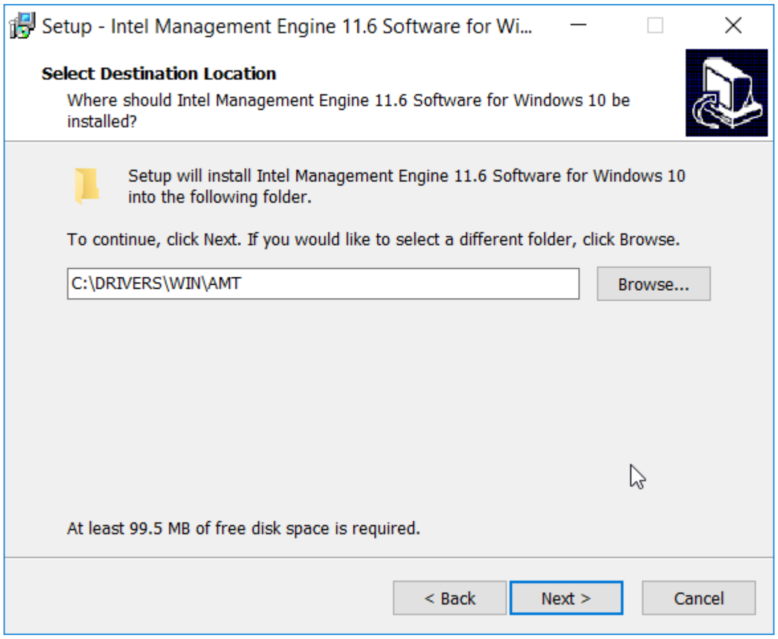
Lenovo License Agreement

L505-0009-06 10/2015

This Lenovo License Agreement (the "Agreement") applies to each Lenovo Software Product that
You acquire, whether it is preinstalled on or included with a Lenovo hardware product, acquired
separately, or downloaded by You from a Lenovo Web site or a third-party Web site approved by
Lenovo. It also applies to any updates or patches to these Software Products.

● I accept the agreement
○ I do not accept the agreement

5. Click **Next.**



Select Destination Location

Where should Intel Management Engine 11.6 Software for Windows 10 be installed?

Setup will install Intel Management Engine 11.6 Software for Windows 10 into the following folder.

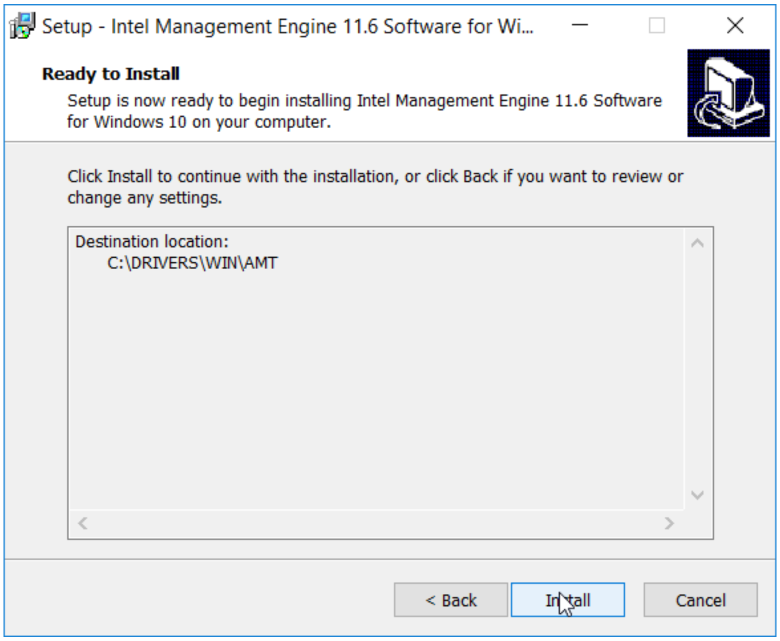
To continue, click Next. If you would like to select a different folder, click Browse.

C:\DRIVERS\WIN\AMT

At least 99.5 MB of free disk space is required.

729

730 6. Click **Install.**



Ready to Install

Setup is now ready to begin installing Intel Management Engine 11.6 Software for Windows 10 on your computer.

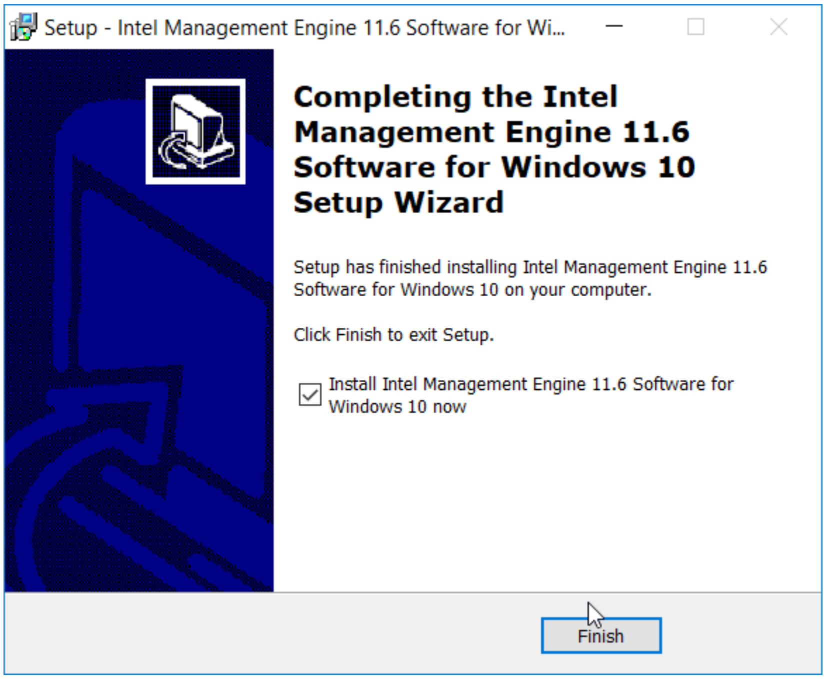
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
    C:\DRIVERS\WIN\AMT

731

732 7. Check the box next to **Install Intel Management Engine 11.6 Software for Windows 10 now.**

733 8. Click **Finish.**



Completing the Intel Management Engine 11.6 Software for Windows 10 Setup Wizard

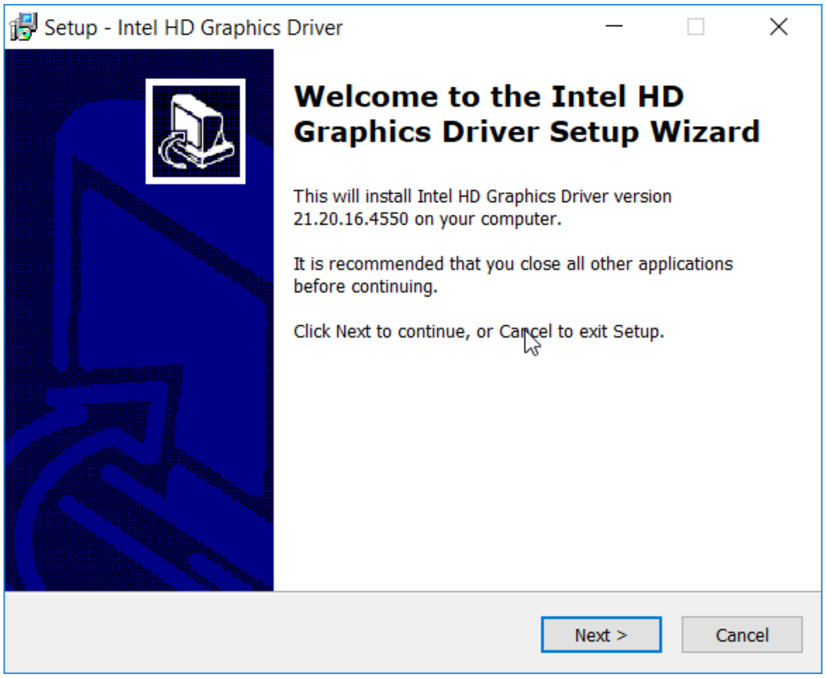
Setup has finished installing Intel Management Engine 11.6 Software for Windows 10 on your computer.

Click Finish to exit Setup.

☑ Install Intel Management Engine 11.6 Software for Windows 10 now

9. Run **u2vdo22us14avc.exe.** (The name may differ based on your system—this is the graphics driver update.)

10. Click **Next.**



Welcome to the Intel HD Graphics Driver Setup Wizard

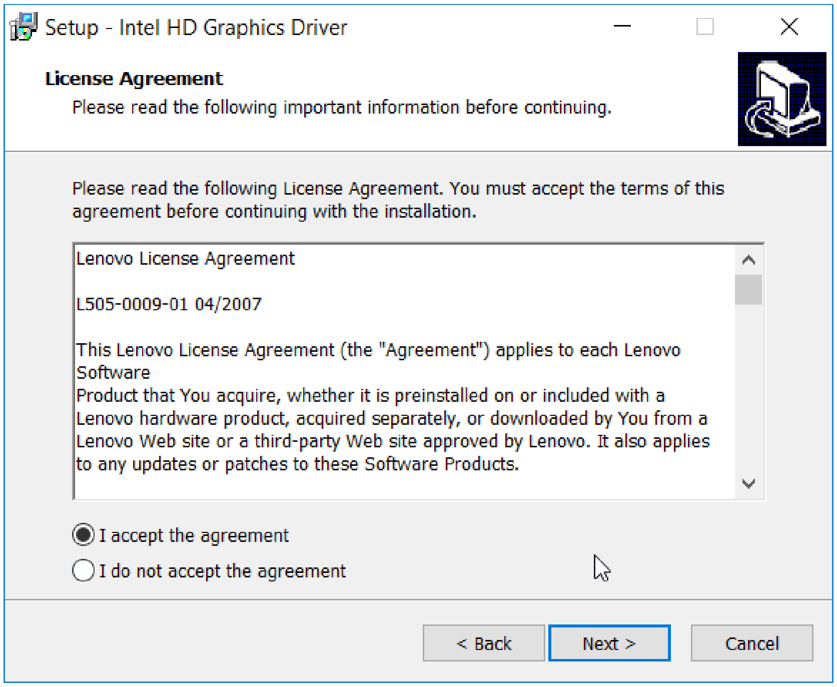
This will install Intel HD Graphics Driver version 21.20.16.4550 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

11. Select **I accept the agreement.**

12. Click **Next.**



Setup - Intel HD Graphics Driver

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Lenovo License Agreement

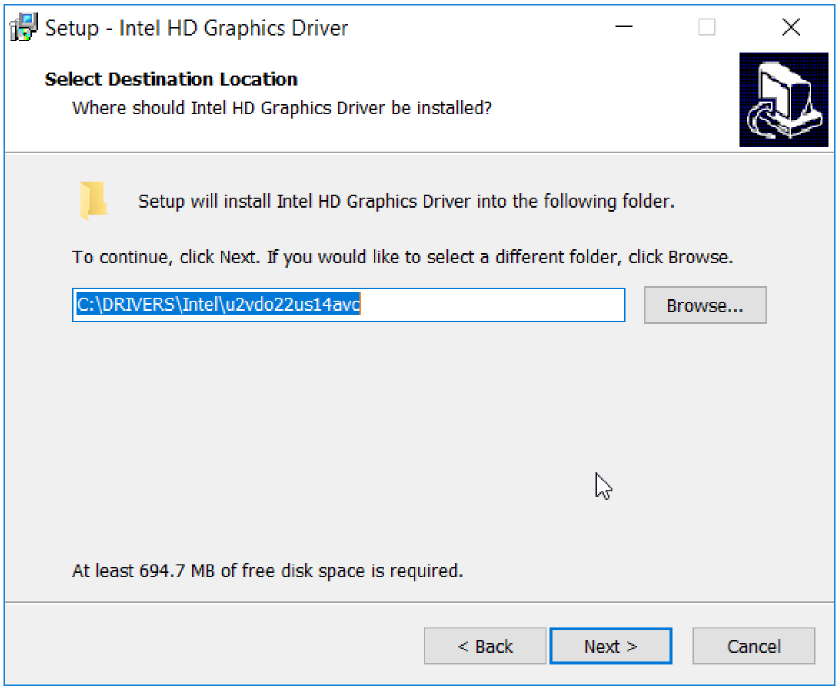
L505-0009-01 04/2007

This Lenovo License Agreement (the "Agreement") applies to each Lenovo Software
Product that You acquire, whether it is preinstalled on or included with a Lenovo hardware product, acquired separately, or downloaded by You from a Lenovo Web site or a third-party Web site approved by Lenovo. It also applies to any updates or patches to these Software Products.

● I accept the agreement

○ I do not accept the agreement

13. Click **Next.**



Select Destination Location

Where should Intel HD Graphics Driver be installed?

Setup will install Intel HD Graphics Driver into the following folder.

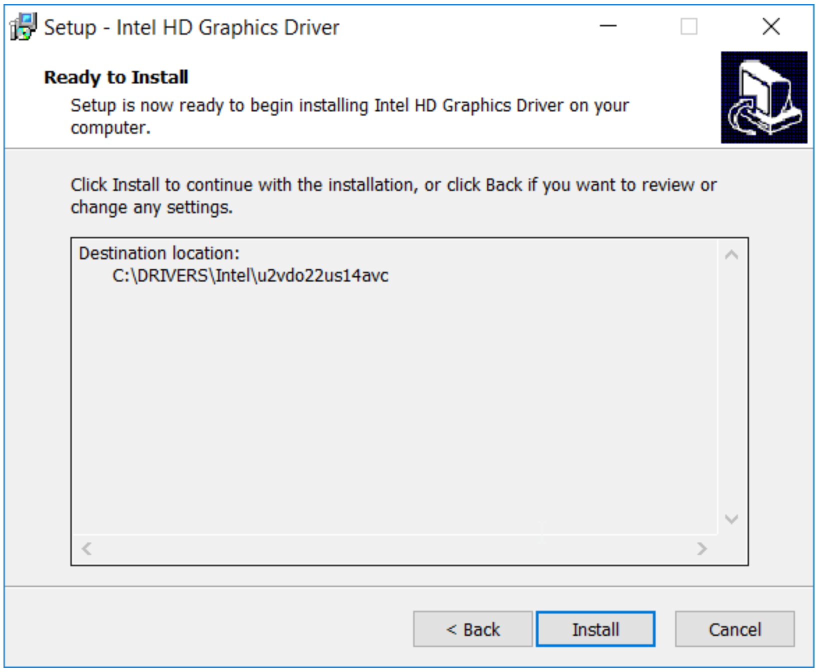
To continue, click Next. If you would like to select a different folder, click Browse.

C:\DRIVERS\Intel\u2vdo22us14avc

At least 694.7 MB of free disk space is required.

743

744 14. Click **Install.**



Ready to Install

Setup is now ready to begin installing Intel HD Graphics Driver on your computer.

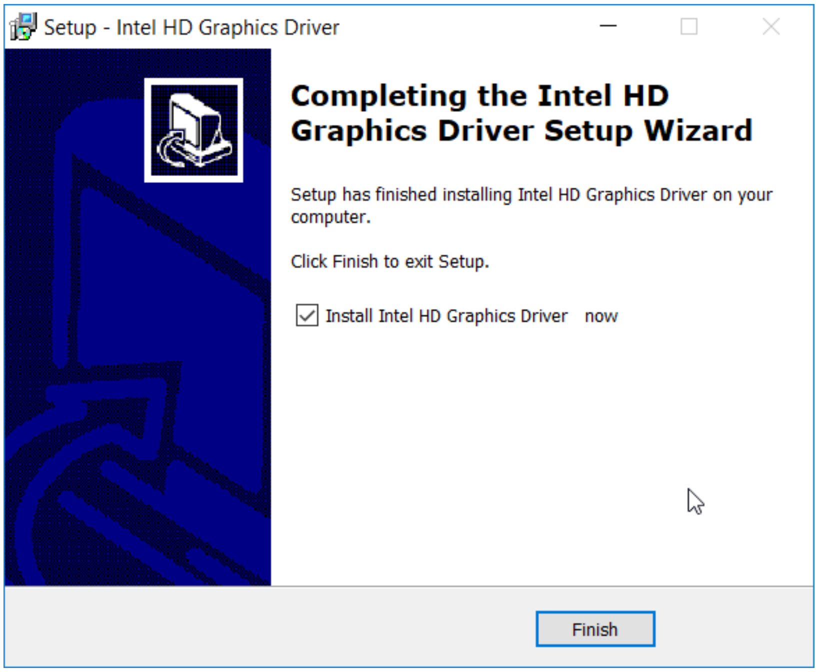
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\DRIVERS\Intel\u2vdo22us14avc

745

746 15. Check the box next to **Install Intel HD Graphics Driver now.**

16. Click **Finish.**



Completing the Intel HD Graphics Driver Setup Wizard

Setup has finished installing Intel HD Graphics Driver on your computer.

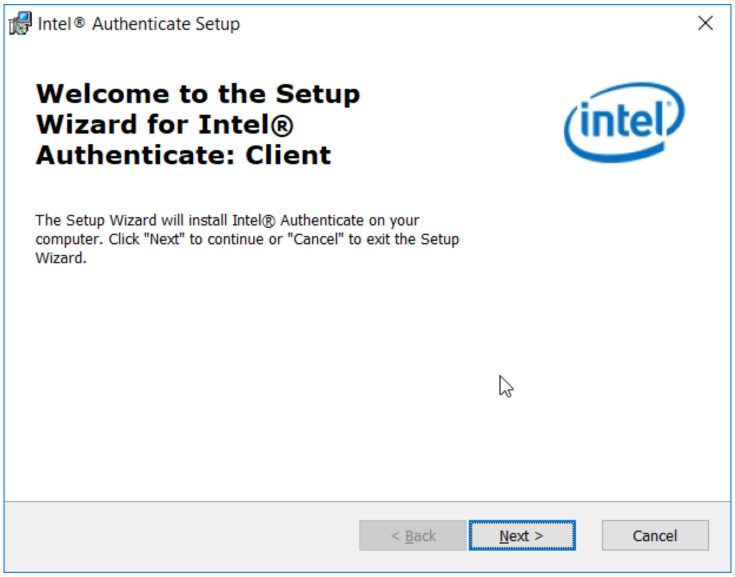
Click Finish to exit Setup.

☑ Install Intel HD Graphics Driver now

2.2.5.4 Installing the Intel Authenticate Client

The Intel Authenticate Client should be installed automatically by the Group Policy Object (GPO), but it can also be installed manually by running IAx64-2.5.0.68.msi.

1. Run **IAx64-2.5.0.68.msi**.
2. Click **Next.**



Intel® Authenticate Setup

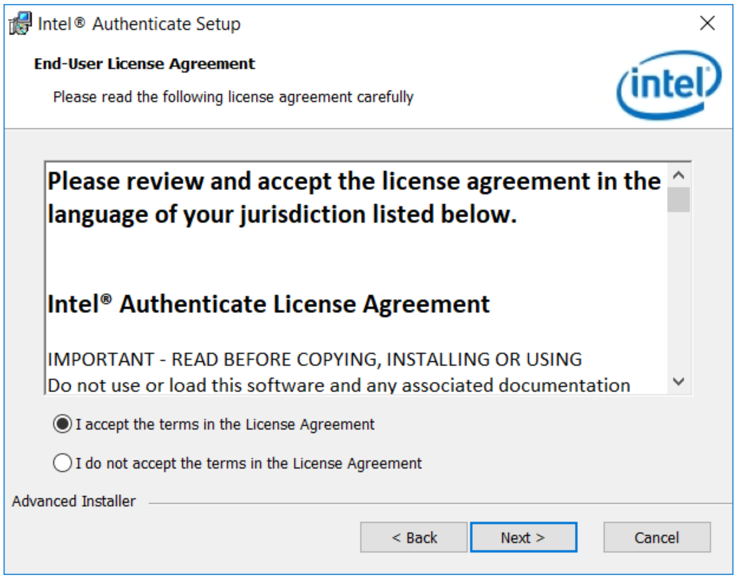
Welcome to the Setup Wizard for Intel® Authenticate: Client

The Setup Wizard will install Intel® Authenticate on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

754

755 3. Select **I accept the terms in the License Agreement.**

756 4. Click **Next.**



Intel® Authenticate Setup

End-User License Agreement

Please read the following license agreement carefully

Please review and accept the license agreement in the language of your jurisdiction listed below.

Intel® Authenticate License Agreement

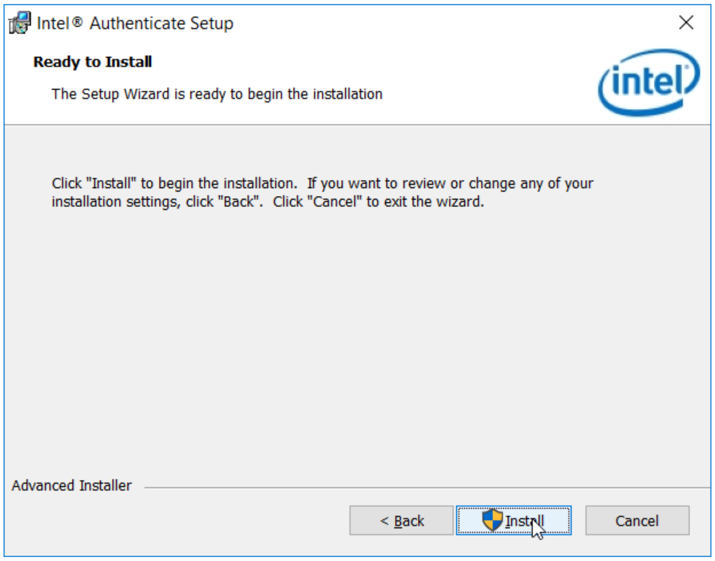
IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING
Do not use or load this software and any associated documentation

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

757

758 5. Click **Install.**



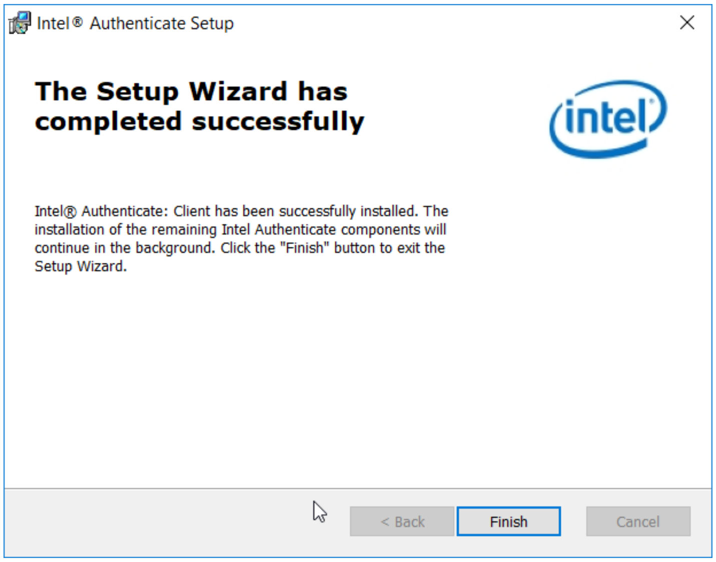
Intel® Authenticate Setup

Ready to Install

The Setup Wizard is ready to begin the installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

6. Click **Finish.**



Intel® Authenticate Setup

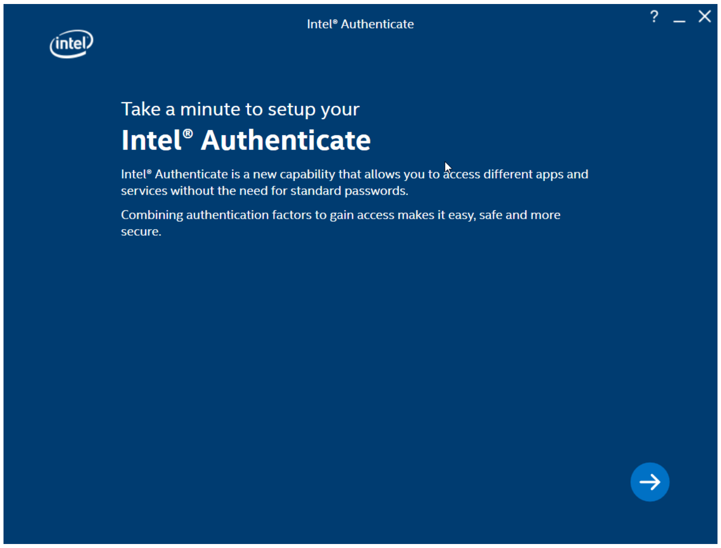
The Setup Wizard has completed successfully

Intel® Authenticate: Client has been successfully installed. The installation of the remaining Intel Authenticate components will continue in the background. Click the "Finish" button to exit the Setup Wizard.

2.2.5.5 Configuring Intel Authenticate

1. Once the Enforce Policy GPO is run, the window for configuring Intel Authenticate will open on the client machine. You can also open this manually by searching for Intel Authenticate in the Start Menu.

2. Click the **right arrow button.**



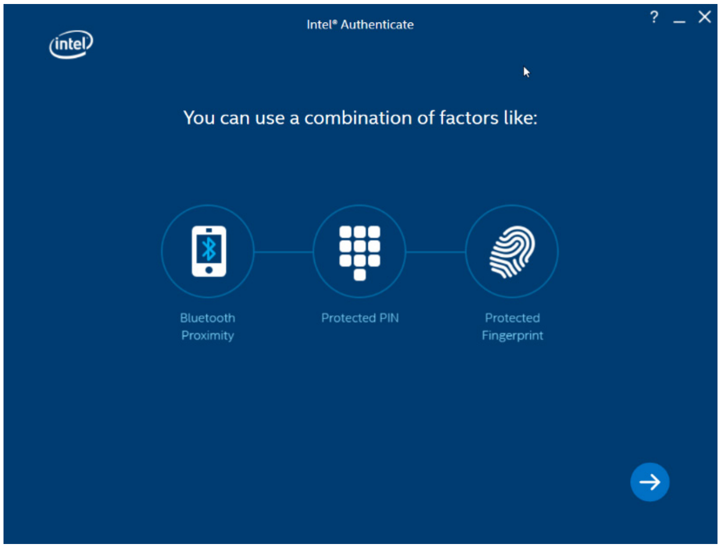
Take a minute to setup your

Intel® Authenticate

Intel® Authenticate is a new capability that allows you to access different apps and services without the need for standard passwords.

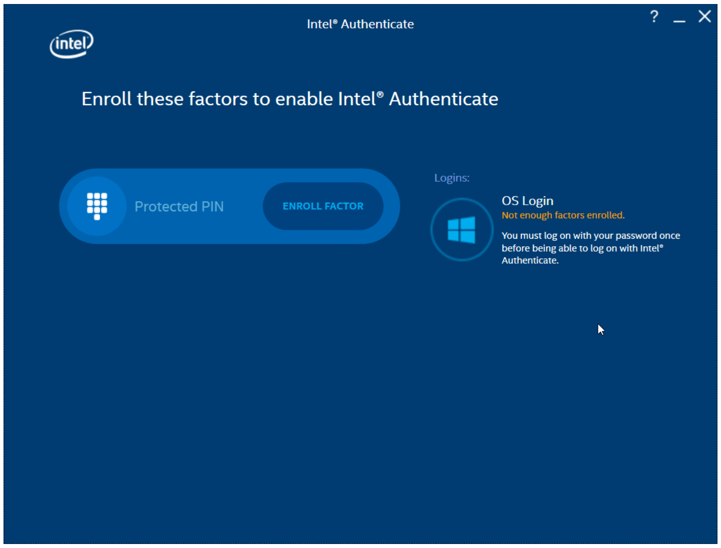
Combining authentication factors to gain access makes it easy, safe and more secure.

3. Click the **right arrow button.**



You can use a combination of factors like:

4. Click **Enroll Factor.**

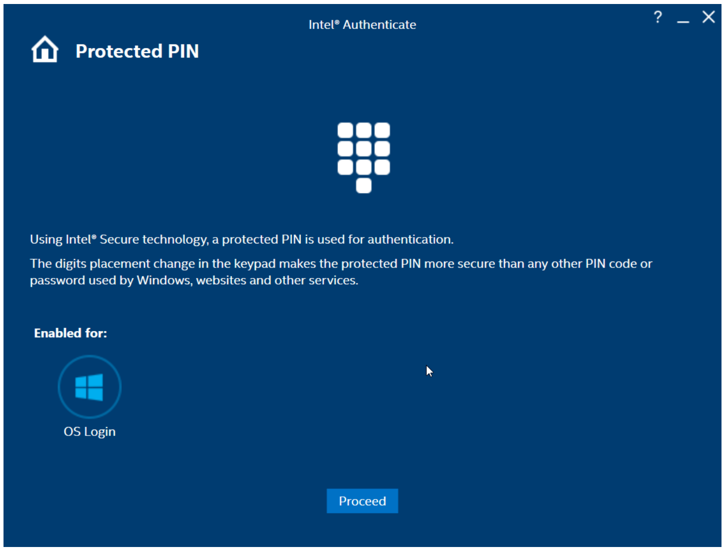


Enroll these factors to enable Intel® Authenticate

Not enough factors enrolled.

You must log on with your password once before being able to log on with Intel® Authenticate.

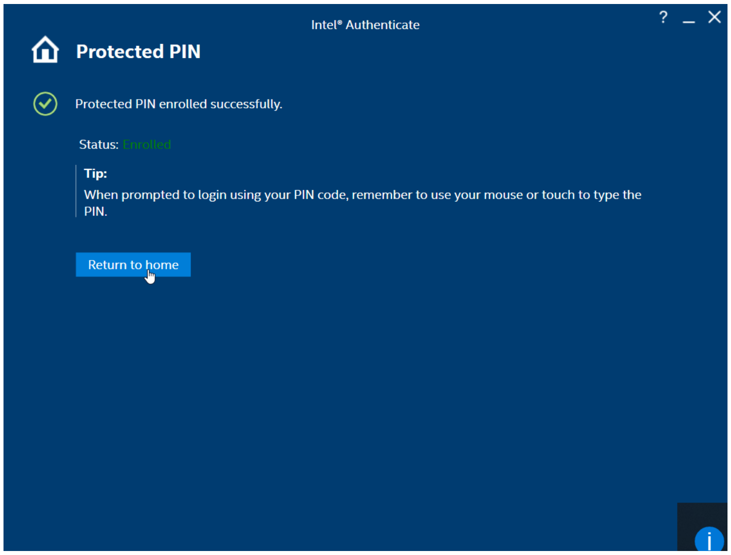
5. Click **Proceed.**



Using Intel® Secure technology, a protected PIN is used for authentication.

The digits placement change in the keypad makes the protected PIN more secure than any other PIN code or password used by Windows, websites and other services.

6. Enter a PIN for Intel Authenticate, which will be used for any certificates issued to the device.
7. Re-enter the PIN.
8. Click **Return to home.**

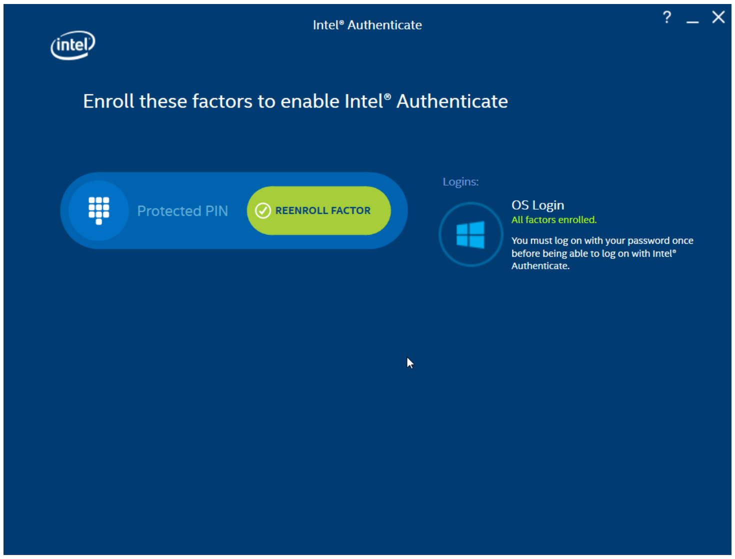


Protected PIN

Protected PIN enrolled successfully.

Status: Enrolled

Tip:
When prompted to login using your PIN code, remember to use your mouse or touch to type the PIN.



Enroll these factors to enable Intel® Authenticate

OS Login
All factors enrolled.
You must log on with your password once before being able to log on with Intel® Authenticate.

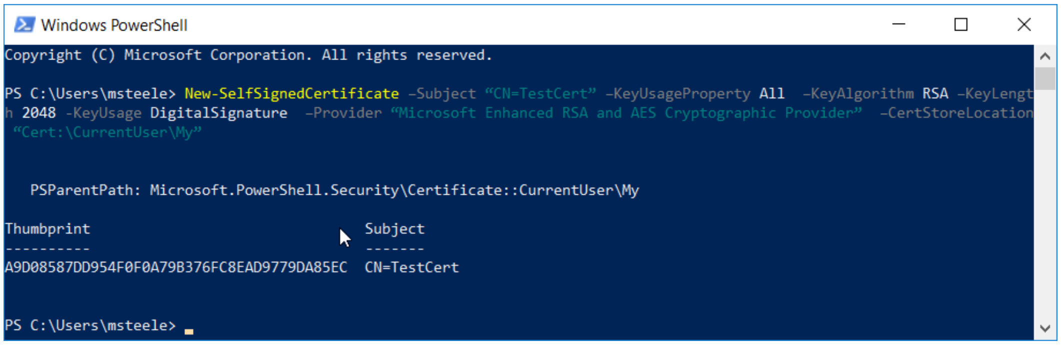
2.2.6 Intel Authenticate GPO

The *Intel Authenticate Integration Guide for Active Directory Policy Objects* provides instructions on how to set up GPOs for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the *Intel Authenticate Integration Guide*.

2.2.6.1 Preparing a Digital Signing Certificate

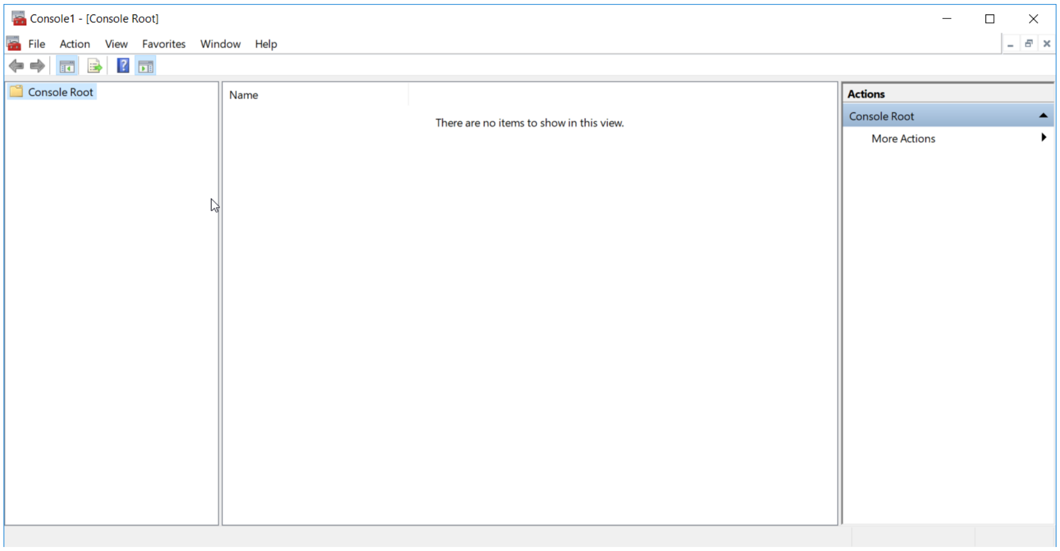
1. In a new PowerShell window, generate a new self-signed certificate to sign the Intel Policy. Enter the command:

```
New-SelfSignedCertificate -Subject “CN=TestCert” -KeyUsageProperty All -KeyAlgorithm RSA -KeyLength 2048 -KeyUsage DigitalSignature -Provider “Microsoft Enhanced RSA and AES Cryptographic Provider” -CertStoreLocation “Cert:\CurrentUser\My”
```



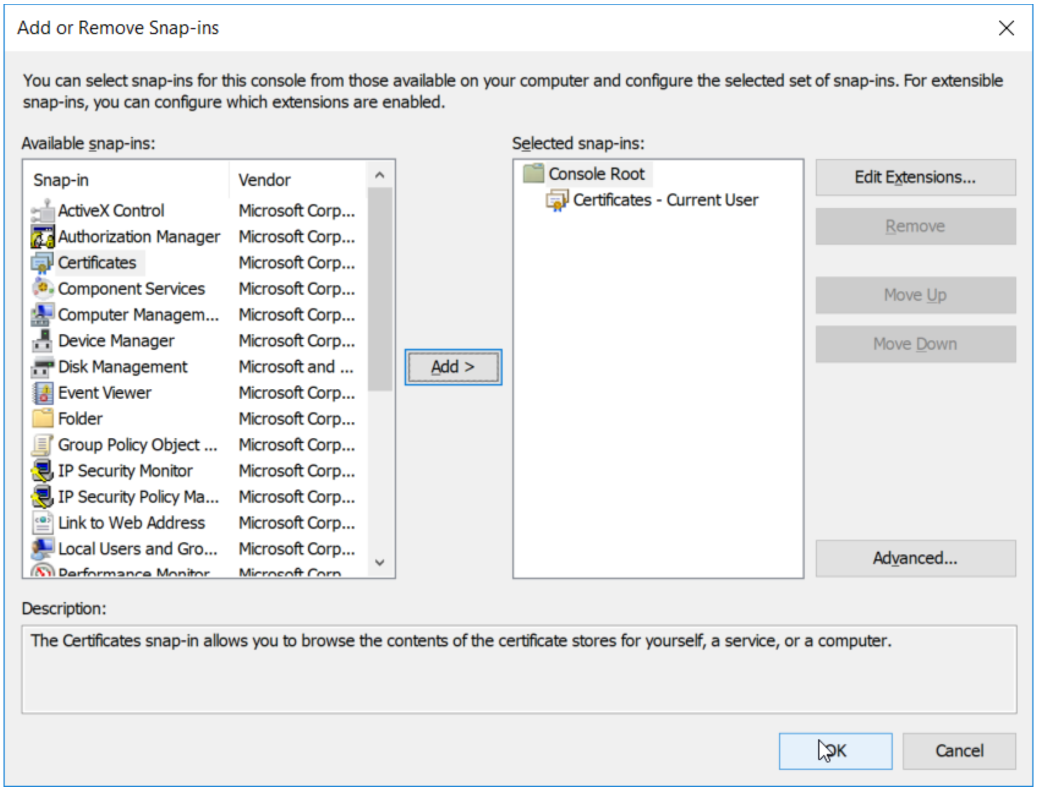
```
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\msteele> New-SelfSignedCertificate -Subject “CN=TestCert” -KeyUsageProperty All  -KeyAlgorithm RSA -KeyLengt
h 2048 -KeyUsage DigitalSignature  -Provider “Microsoft Enhanced RSA and AES Cryptographic Provider”  -CertStoreLocation
 “Cert:\CurrentUser\My”


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
A9D08587DD954F0F0A79B376FC8EAD9779DA85EC  CN=TestCert


PS C:\Users\msteele> _
```

2. Run **mmc.exe** from the Start menu to open the **Microsoft Management Console** window.



There are no items to show in this view.

3. Select **File > Add/Remove Snap-In.** Add the **Certificates** snap-in.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Corp...
Authorization Manager	Microsoft Corp...
Certificates	Microsoft Corp...
Component Services	Microsoft Corp...
Computer Managem...	Microsoft Corp...
Device Manager	Microsoft Corp...
Disk Management	Microsoft and ...
Event Viewer	Microsoft Corp...
Folder	Microsoft Corp...
Group Policy Object ...	Microsoft Corp...
IP Security Monitor	Microsoft Corp...
IP Security Policy Ma...	Microsoft Corp...
Link to Web Address	Microsoft Corp...
Local Users and Gro...	Microsoft Corp...
Performance Monitor	Microsoft Corp

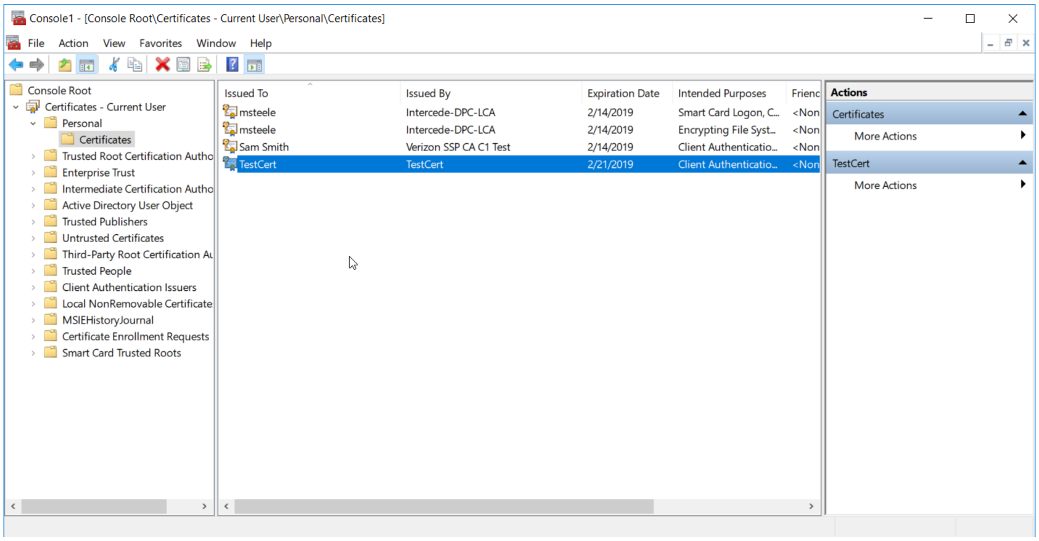
Selected snap-ins:

Console Root
Certificates - Current User

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. The newly created certificate should be in the **Certificates – Current User > Personal > Certificates** store.



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

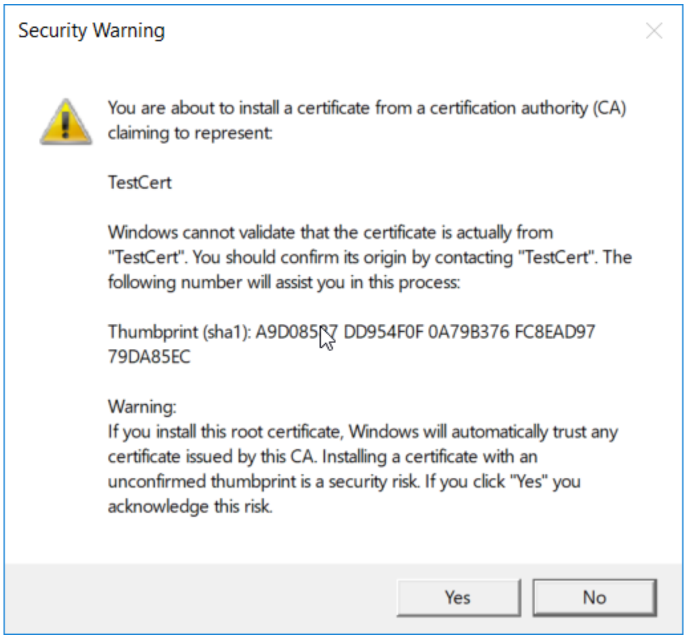
Console Root
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification Autho
  - Enterprise Trust
  - Intermediate Certification Autho
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Au
  - Trusted People
  - Client Authentication Issuers
  - Local NonRemovable Certificate
  - MSIEHistoryJournal
  - Certificate Enrollment Requests
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Frienc
msteele	Intercede-DPC-LCA	2/14/2019	Smart Card Logon, C...	<Non
msteele	Intercede-DPC-LCA	2/14/2019	Encrypting File Syst...	<Non
Sam Smith	Verizon SSP CA C1 Test	2/14/2019	Client Authenticatio...	<Non
TestCert	TestCert	2/21/2019	Client Authenticatio...	<Non

5. Right-click the newly created certificate and select **Copy.**

6. Navigate to **Certificates – Current User > Trusted Root Certification Authorities > Certificates** and paste the certificate there.

7. Click **Yes** when a warning message appears.



Security Warning

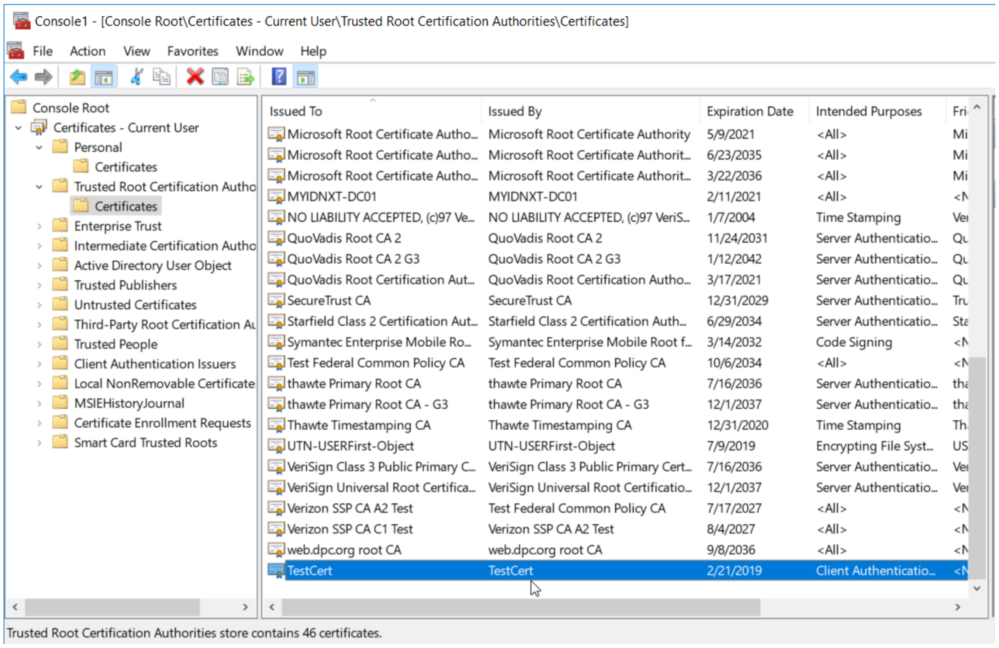
You are about to install a certificate from a certification authority (CA) claiming to represent:

TestCert

Windows cannot validate that the certificate is actually from "TestCert". You should confirm its origin by contacting "TestCert". The following number will assist you in this process:

Thumbprint (sha1): A9D0857 DD954F0F 0A79B376 FC8EAD97 79DA85EC

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

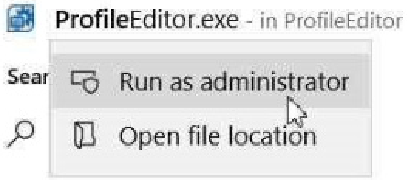
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Certificates
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Local NonRemovable Certificate
MSIEHistoryJournal
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Fri
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Mi
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Mi
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Mi
MYIDNXT-DC01	MYIDNXT-DC01	2/11/2021	<All>	<N
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	Ve
QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticatio...	Qu
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticatio...	Qu
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Server Authenticatio...	Qu
SecureTrust CA	SecureTrust CA	12/31/2029	Server Authenticatio...	Tru
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticatio...	Sta
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<N
Test Federal Common Policy CA	Test Federal Common Policy CA	10/6/2034	<All>	<N
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	tha
thawte Primary Root CA - G3	thawte Primary Root CA - G3	12/1/2037	Server Authenticatio...	tha
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Th
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	US
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Server Authenticatio...	Ve
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	Server Authenticatio...	Ve
Verizon SSP CA A2 Test	Test Federal Common Policy CA	7/17/2027	<All>	<N
Verizon SSP CA C1 Test	Verizon SSP CA A2 Test	8/4/2027	<All>	<N
web.dpc.org root CA	web.dpc.org root CA	9/8/2036	<All>	<N
TestCert	TestCert	2/21/2019	Client Authenticatio...	<N

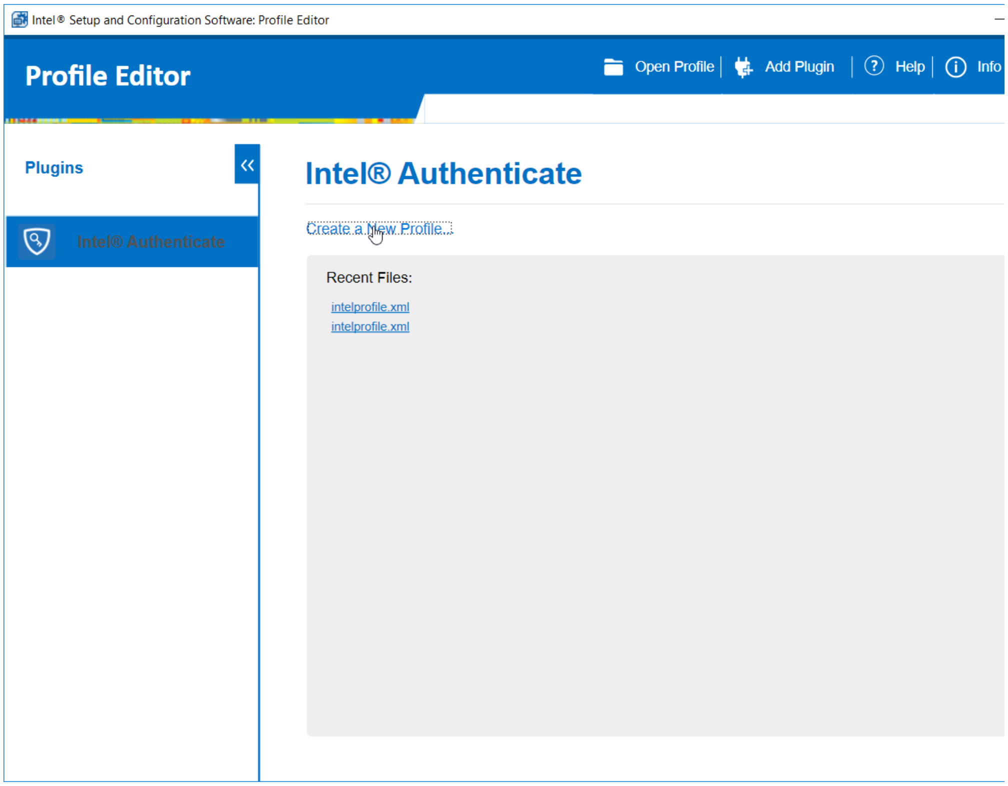
Trusted Root Certification Authorities store contains 46 certificates.

2.2.6.2 Creating a Profile

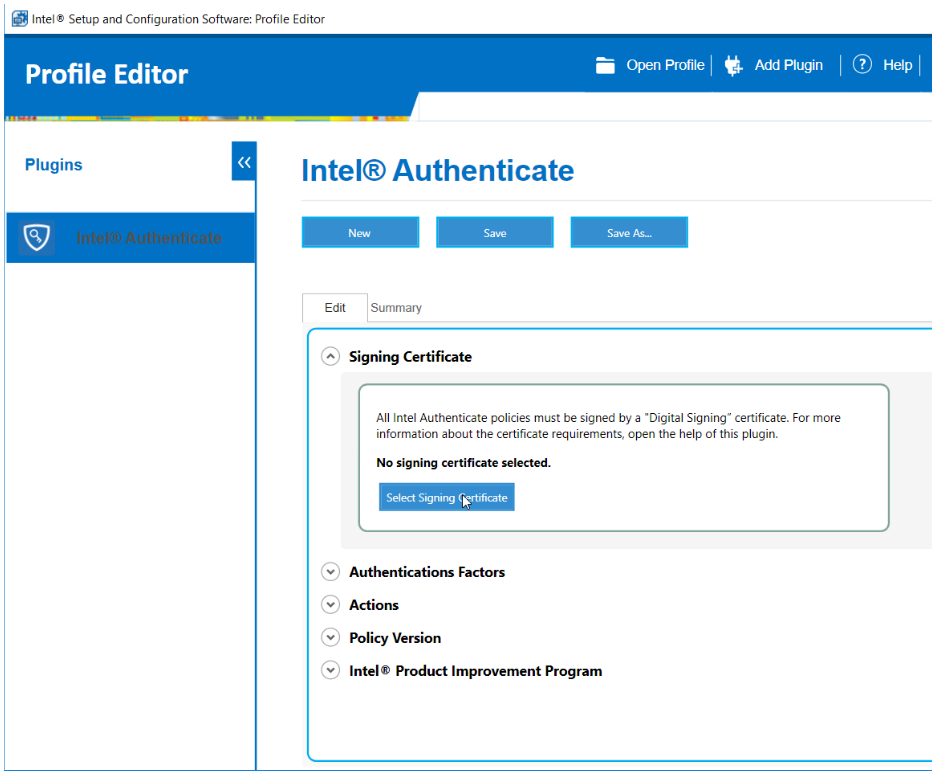
1. Run the **ProfileEditor.exe** file as an administrator.



2. Click **Create a New Profile…**.



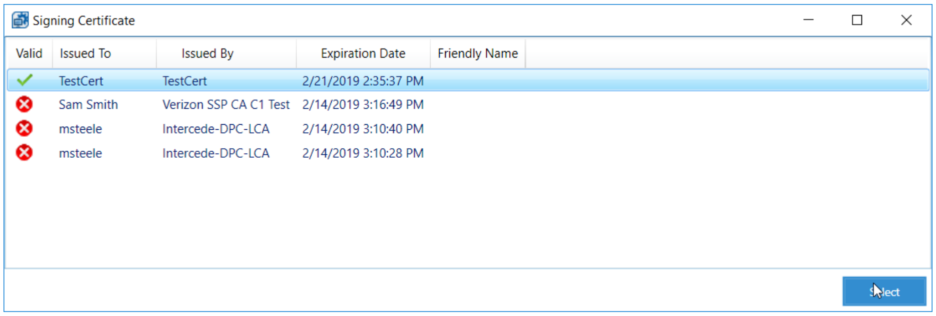
3. Click **Select Signing Certificate**.



All Intel Authenticate policies must be signed by a "Digital Signing" certificate. For more information about the certificate requirements, open the help of this plugin.

No signing certificate selected.

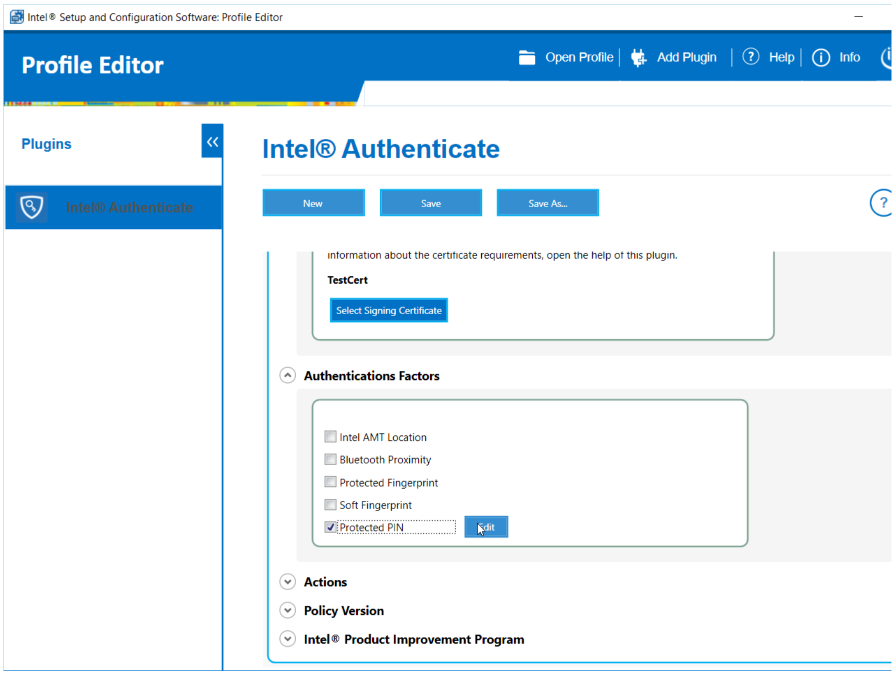
4. Select the newly created certificate and click **Select**.



Valid	Issued To	Issued By	Expiration Date	Friendly Name
✓	TestCert	TestCert	2/21/2019 2:35:37 PM	
☒	Sam Smith	Verizon SSP CA C1 Test	2/14/2019 3:16:49 PM	
☒	msteele	Intercede-DPC-LCA	2/14/2019 3:10:40 PM	
☒	msteele	Intercede-DPC-LCA	2/14/2019 3:10:28 PM	

5. Under **Authentications Factors**, check the box next to **Protected PIN**.

6. Click the **Edit** button.



Intel® Authenticate

information about the certificate requirements, open the help of this plugin.

TestCert

Select Signing Certificate

Authentications Factors

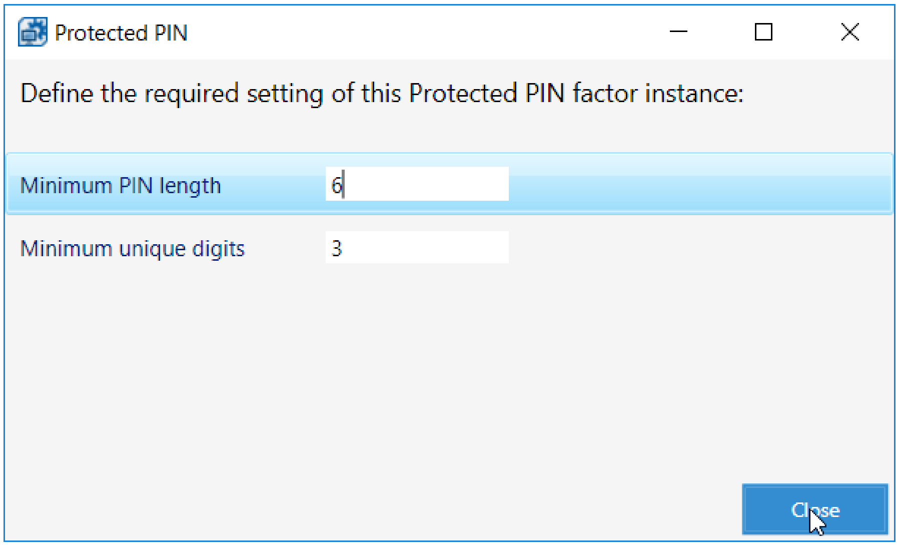
□ Intel AMT Location
□ Bluetooth Proximity
□ Protected Fingerprint
□ Soft Fingerprint
☑ Protected PIN Edit

Actions

Policy Version

Intel® Product Improvement Program

7. Set the PIN length and the minimum number of unique digits.
8. Click **Close**.



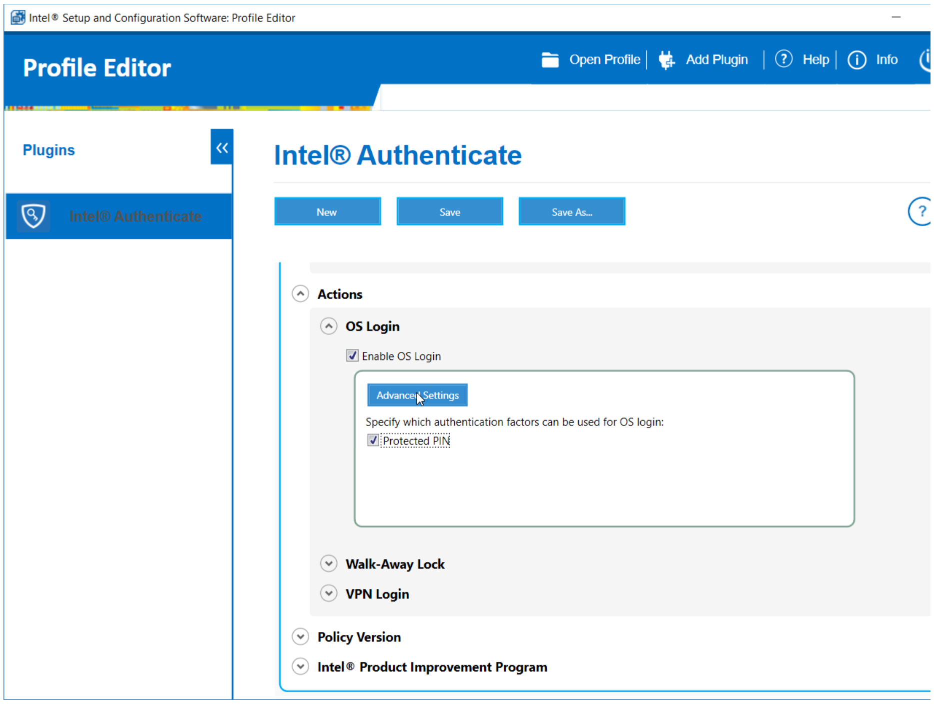
Protected PIN

Define the required setting of this Protected PIN factor instance:

Minimum PIN length	6
Minimum unique digits	3

Close

9. Under **Actions > OS Login**, check the box next to **Enable OS Login**.
10. Check the box next to **Protected PIN**.
11. Click **Advanced Settings**.



Intel® Authenticate

Actions

OS Login

☑ Enable OS Login

Specify which authentication factors can be used for OS login:

☑ Protected PIN

Walk-Away Lock

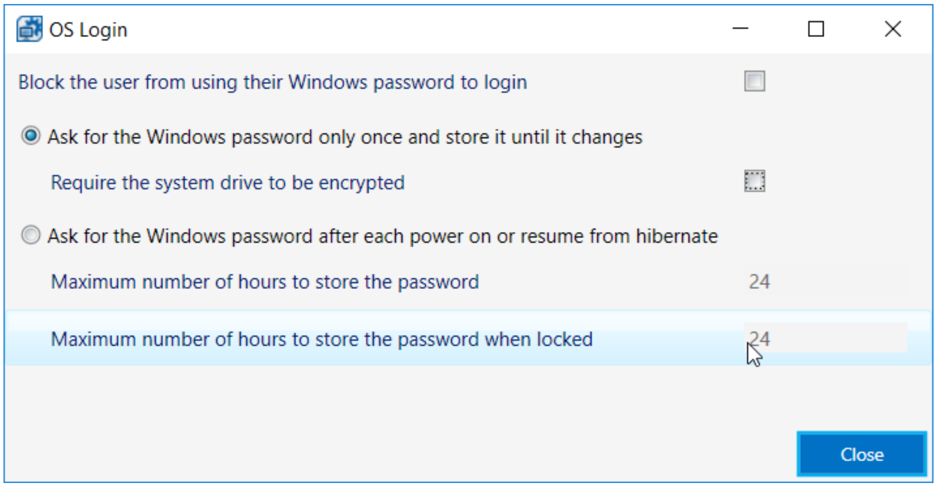
VPN Login

Policy Version

Intel® Product Improvement Program

12. Uncheck the box next to **Require the system drive to be encrypted**.

13. Click **Close**.

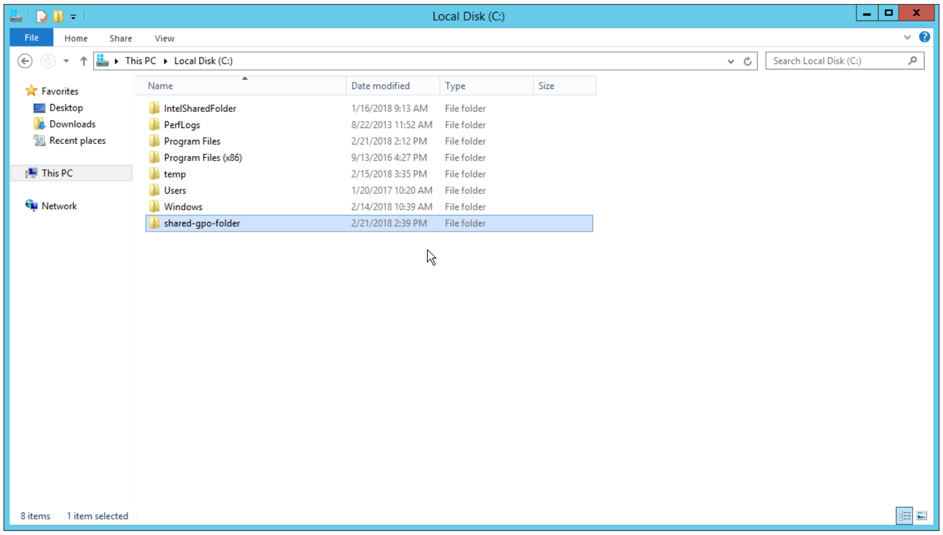


Block the user from using their Windows password to login	□
● Ask for the Windows password only once and store it until it changes	
Require the system drive to be encrypted	□
○ Ask for the Windows password after each power on or resume from hibernate	
Maximum number of hours to store the password	24
Maximum number of hours to store the password when locked	24

14. Click the **Save As…** button and save the profile.

2.2.6.3 Creating a Shared Folder

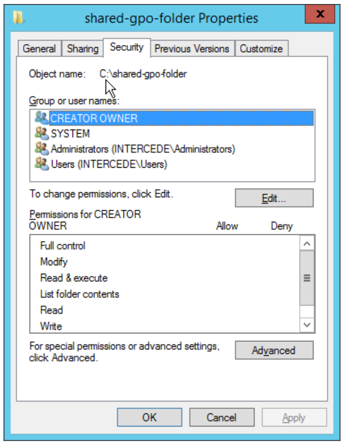
1. Create a new folder on the network.
2. Give it a name such as *shared-gpo-folder*.



Name	Date modified	Type	Size
IntelSharedFolder	1/16/2018 9:13 AM	File folder	
PerfLogs	8/22/2013 11:52 AM	File folder	
Program Files	2/21/2018 2:12 PM	File folder	
Program Files (x86)	9/13/2016 4:27 PM	File folder	
temp	2/15/2018 3:35 PM	File folder	
Users	1/20/2017 10:20 AM	File folder	
Windows	2/14/2018 10:39 AM	File folder	
shared-gpo-folder	2/21/2018 2:39 PM	File folder	

8 items 1 item selected

3. Right-click the folder and select **Properties**.
4. Go to the **Security** Tab.
5. Click **Edit**.



Object name: C:\shared-gpo-folder

Group or user names:

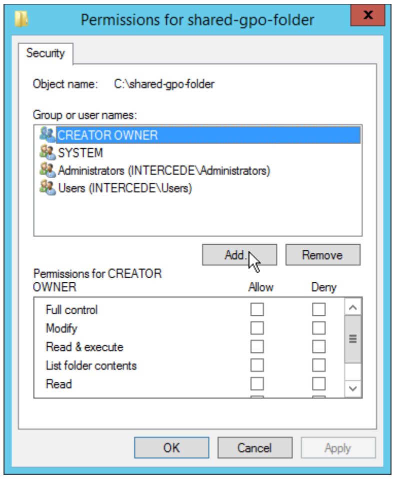
- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Users (INTERCEDE\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

6. Click **Add**.



Permissions for shared-gpo-folder

Security

Object name: C:\shared-gpo-folder

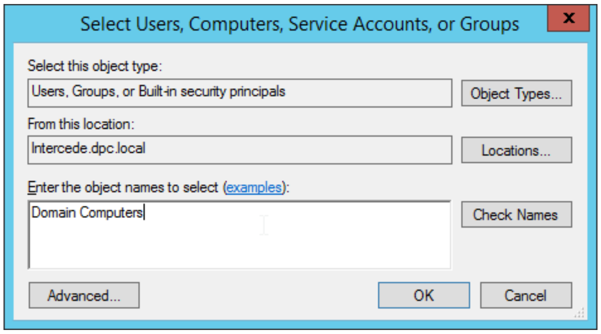
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Users (INTERCEDE\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

7. Enter **Domain Computers** in the text box.

8. Click **OK**.



Select Users, Computers, Service Accounts, or Groups

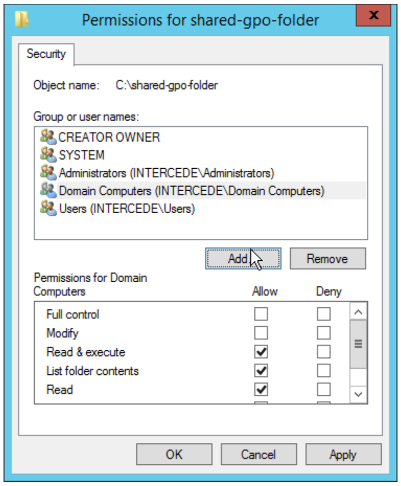
Select this object type:
Users, Groups, or Built-in security principals

From this location:
Intercede.dpc.local

Enter the object names to select (examples):
Domain Computers

9. Ensure that the Domain Computers have read permissions on this folder.

10. Click **OK.**



Object name: C:\shared-gpo-folder

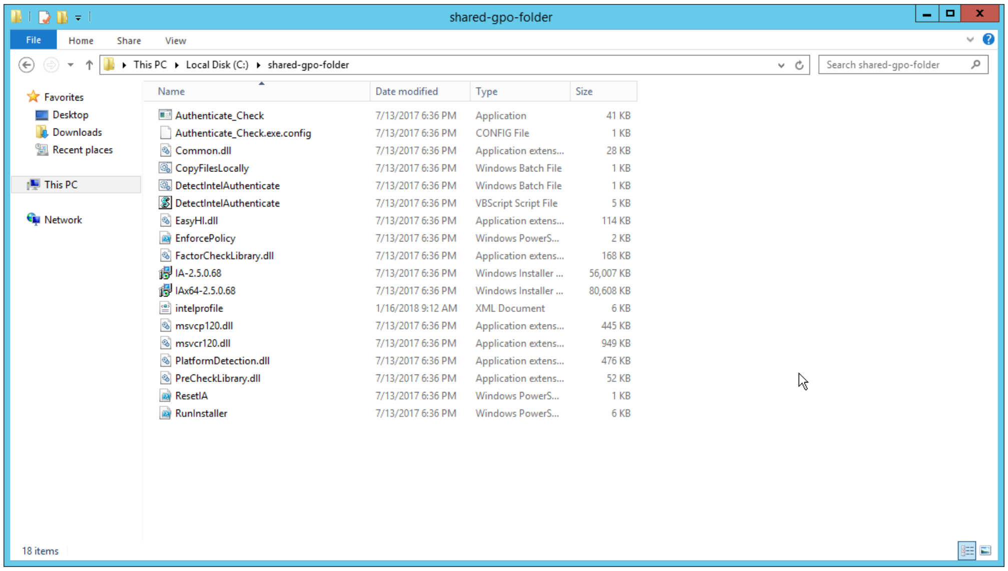
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Domain Computers (INTERCEDE\Domain Computers)
- Users (INTERCEDE\Users)

Permissions for Domain Computers	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

11. Click **OK.**

12. Copy all the files from the HostFiles folder, as well as the Intel Profile you created, into this shared folder.

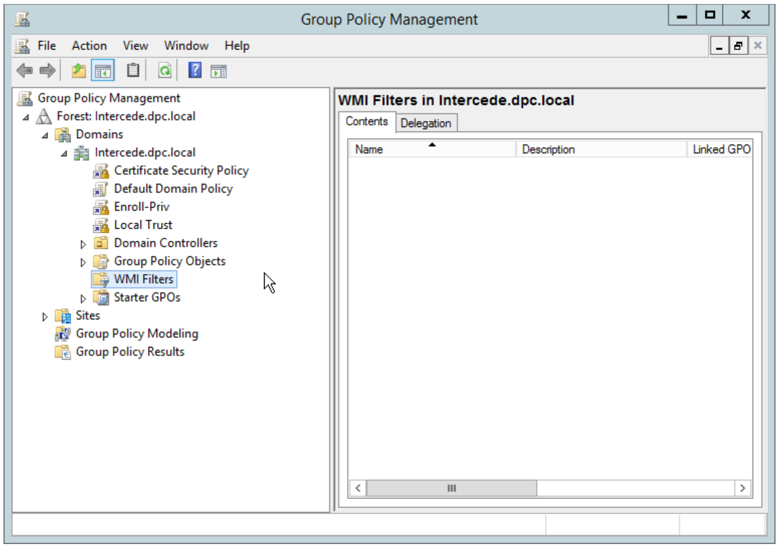


Name	Date modified	Type	Size
Authenticate_Check	7/13/2017 6:36 PM	Application	41 KB
Authenticate_Check.exe.config	7/13/2017 6:36 PM	CONFIG File	1 KB
Common.dll	7/13/2017 6:36 PM	Application extens...	28 KB
CopyFilesLocally	7/13/2017 6:36 PM	Windows Batch File	1 KB
DetectIntelAuthenticate	7/13/2017 6:36 PM	Windows Batch File	1 KB
DetectIntelAuthenticate	7/13/2017 6:36 PM	VBScript Script File	5 KB
EasyHI.dll	7/13/2017 6:36 PM	Application extens...	114 KB
EnforcePolicy	7/13/2017 6:36 PM	Windows PowerS...	2 KB
FactorCheckLibrary.dll	7/13/2017 6:36 PM	Application extens...	168 KB
IA-2.5.0.68	7/13/2017 6:36 PM	Windows Installer ...	56,007 KB
IAx64-2.5.0.68	7/13/2017 6:36 PM	Windows Installer ...	80,608 KB
intelprofile	1/16/2018 9:12 AM	XML Document	6 KB
msvcp120.dll	7/13/2017 6:36 PM	Application extens...	445 KB
msvcr120.dll	7/13/2017 6:36 PM	Application extens...	949 KB
PlatformDetection.dll	7/13/2017 6:36 PM	Application extens...	476 KB
PreCheckLibrary.dll	7/13/2017 6:36 PM	Application extens...	52 KB
ResetIA	7/13/2017 6:36 PM	Windows PowerS...	1 KB
RunInstaller	7/13/2017 6:36 PM	Windows PowerS...	6 KB

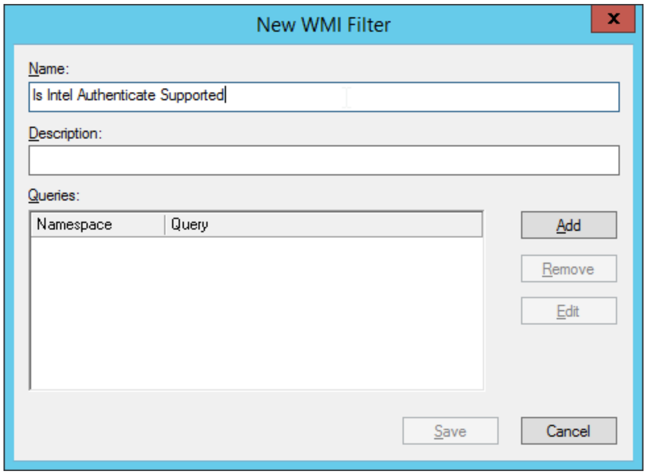
2.2.6.4 Creating WMI Filters for the GPOs

1. Open the **Group Policy Management** window by running **gpmc.msc** from the **Start** menu.

2. Right-click **WMI Filters** and select **New…**.



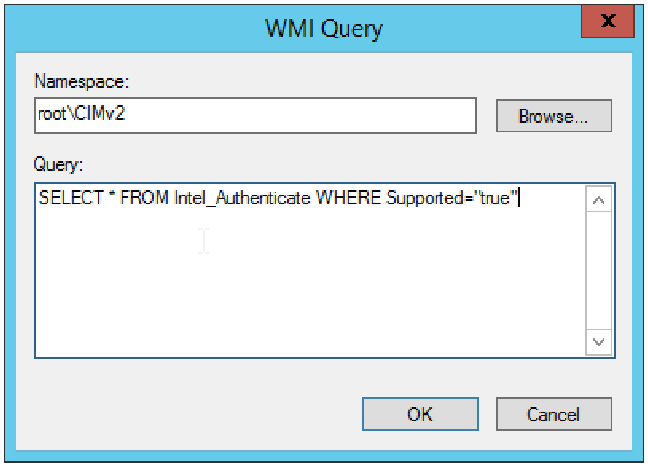
3. Enter a name such as *Is Intel Authenticate Supported* and click **Add**.



Name: Is Intel Authenticate Supported

4. In the **Query** field, enter *SELECT * FROM Intel_Authenticate WHERE Supported="true"*.

5. Click **OK**.

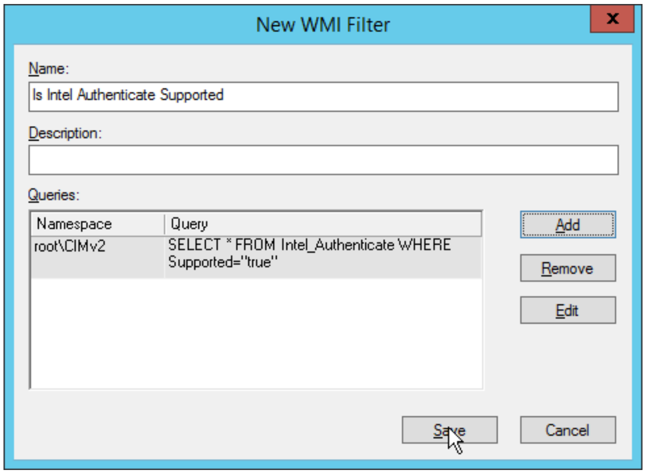


Namespace: root\CIMv2

Query:

```
SELECT * FROM Intel_Authenticate WHERE Supported="true"
```

6. Click **Save**.



Name: Is Intel Authenticate Supported

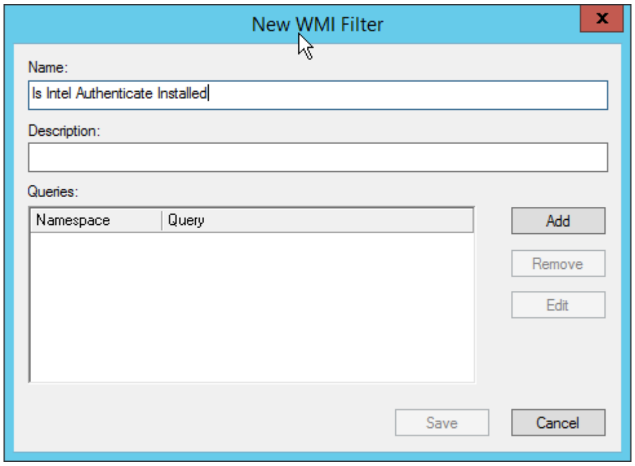
Description:

Queries:

Namespace	Query
root\CIMv2	SELECT * FROM Intel_Authenticate WHERE Supported="true"

7. Right-click **WMI Filters** and select **New…**.

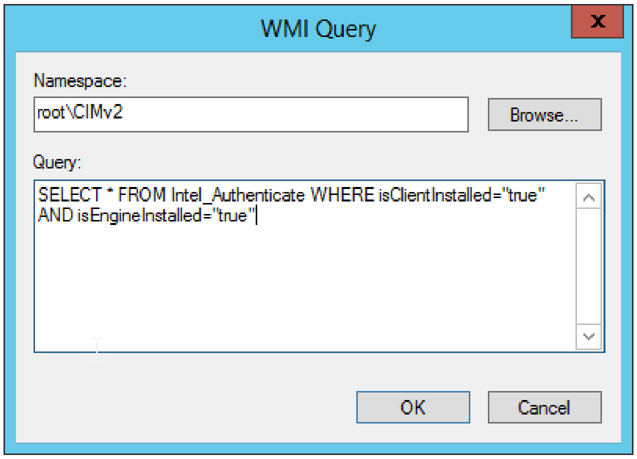
8. Enter a name such as *Is Intel Authenticate Installed* and click **Add**.



Name: Is Intel Authenticate Installed

9. In the **Query** field, enter *SELECT * FROM Intel_Authenticate WHERE isClientInstalled=“true” AND isEngineInstalled=“true”*.

10. Click **OK**.

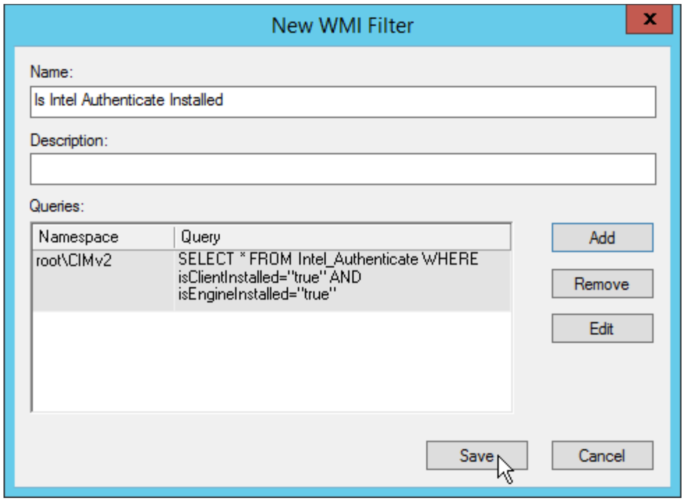


Namespace: root\CIMv2

Query:

```
SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true"
AND isEngineInstalled="true"
```

11. Click **Save**.

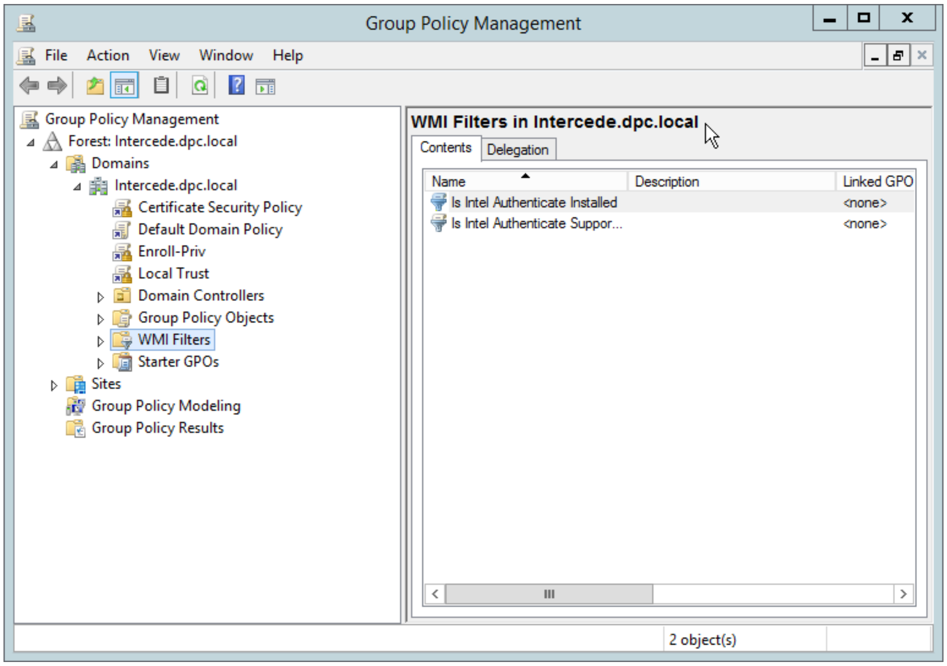


Name: Is Intel Authenticate Installed

Description:

Queries:

Namespace	Query
root\CIMv2	SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true" AND isEngineInstalled="true"



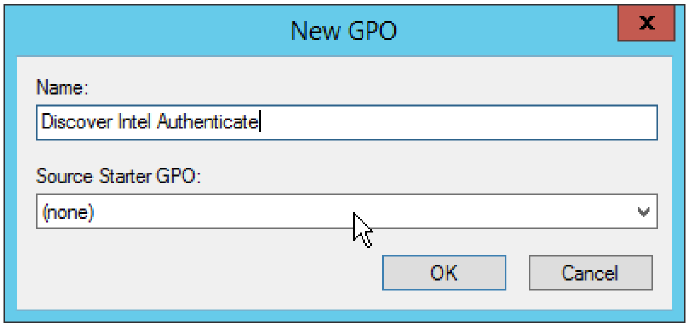
WMI Filters in Intercede.dpc.local

Name	Description	Linked GPO
Is Intel Authenticate Installed		<none>
Is Intel Authenticate Suppor...		<none>

2 object(s)

2.2.6.5 Creating a GPO to Discover Intel Authenticate

1. Open **Group Policy Management**.
2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.
3. Enter a **name** for this GPO.

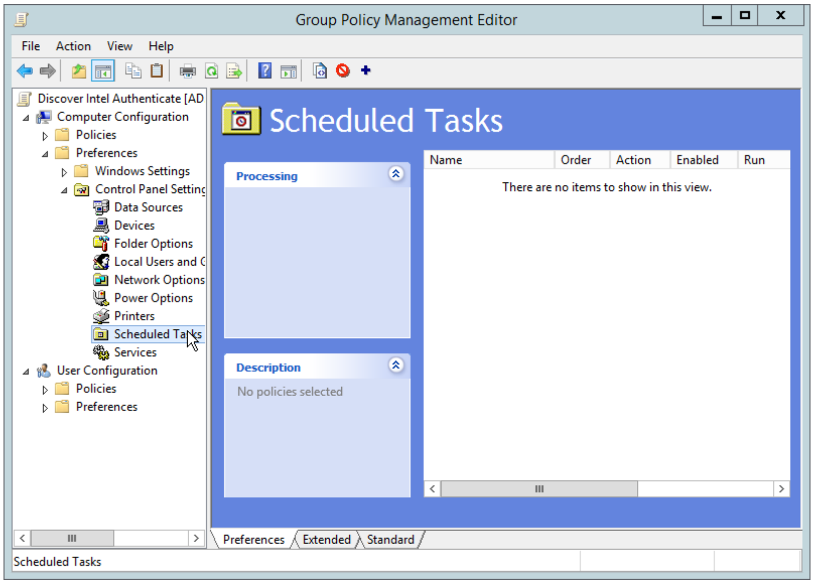


Name: Discover Intel Authenticate

Source Starter GPO: (none)

4. Right-click the GPO just created and select **Edit**.

5. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.



No policies selected

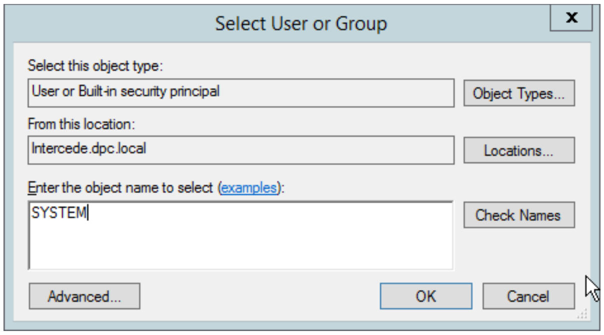
There are no items to show in this view.

6. Select **Replace** from the drop-down list for **Action**.

7. Enter a descriptive name.

8. Click **Change User or Group**.

9. Enter *SYSTEM* and click **OK**.



Select User or Group

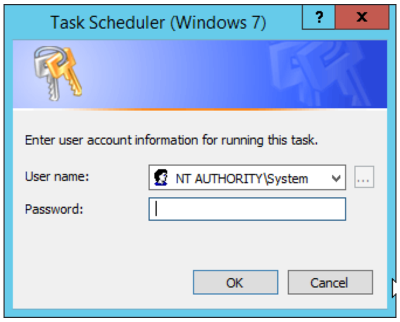
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

10. Check the box next to **Run whether user is logged on or not**.

11. A window will open asking for a password. Click **Cancel**.



Task Scheduler (Windows 7)

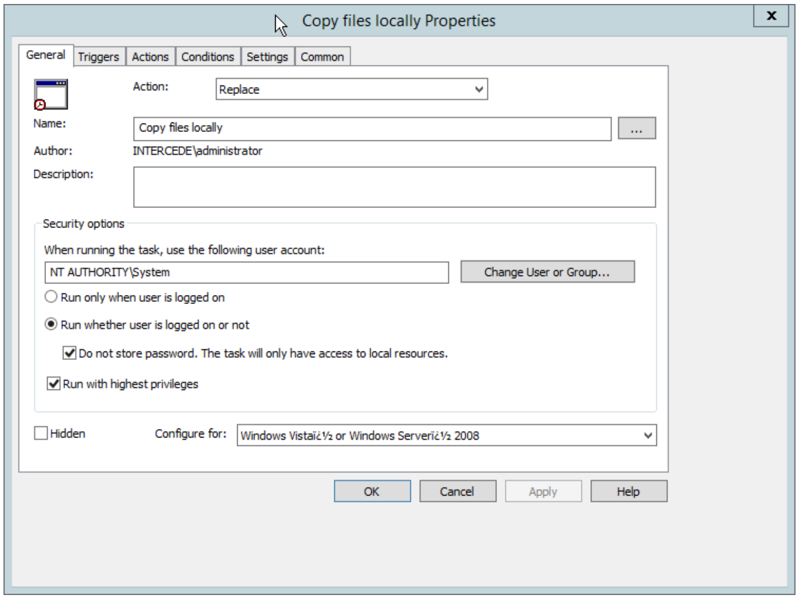
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

12. Check the box next to **Do not store password. The task will only have access to local resources**.

13. Check the box next to **Run with highest privileges**.



Copy files locally Properties

Action: Replace

Name: Copy files locally

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:
NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

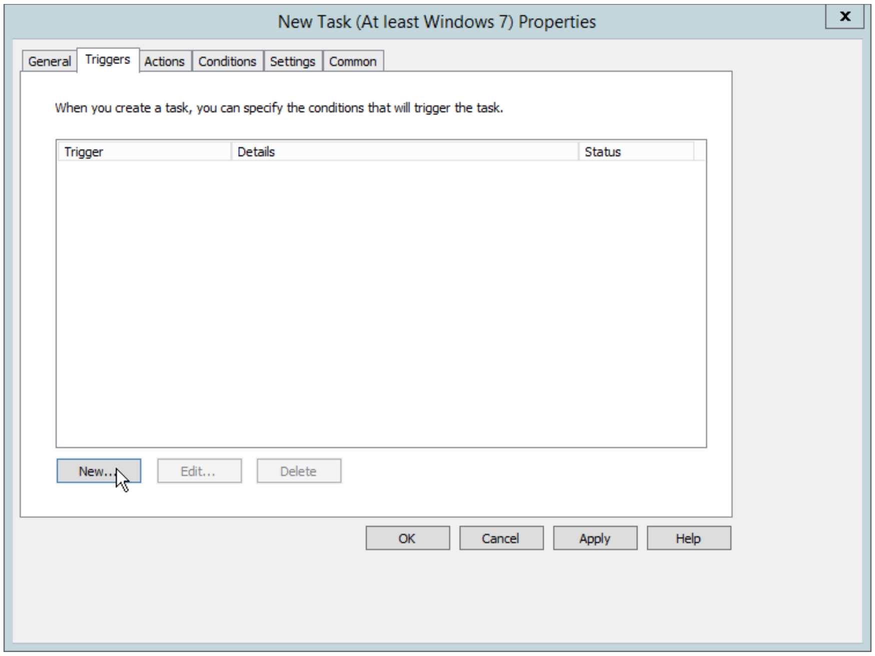
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

14. Select the **Triggers** tab.

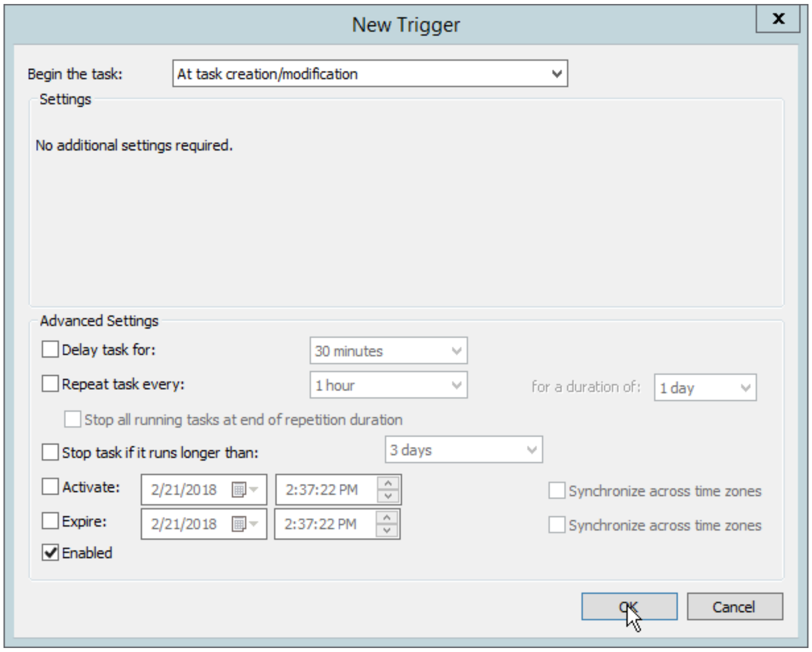
15. Click **New…**.



When you create a task, you can specify the conditions that will trigger the task.

16. Select **At task creation/modification** for **Begin the task**.

17. Click **OK**.



Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

□ Delay task for: 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

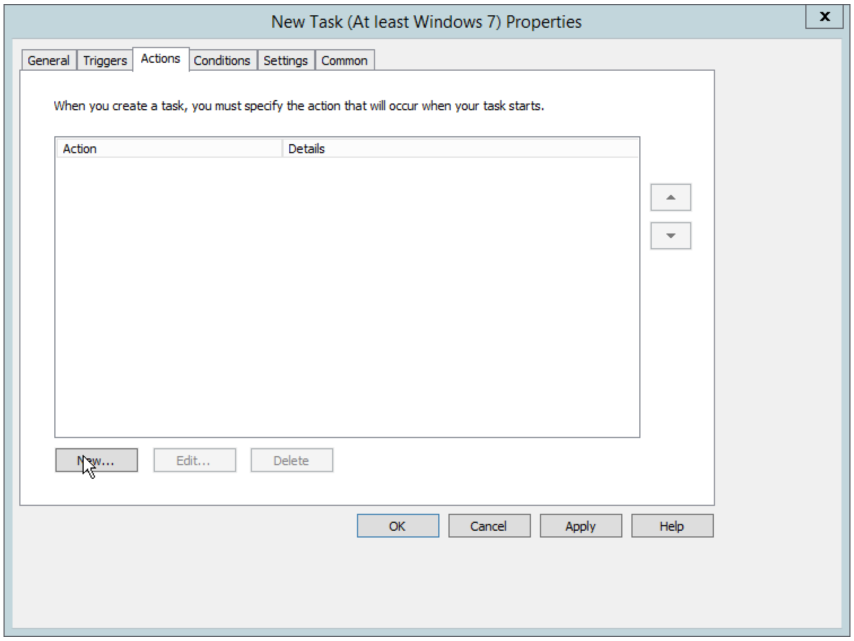
□ Activate: 2/21/2018 2:37:22 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:37:22 PM □ Synchronize across time zones

☑ Enabled

18. Select the **Actions** tab.

19. Click **New…**.

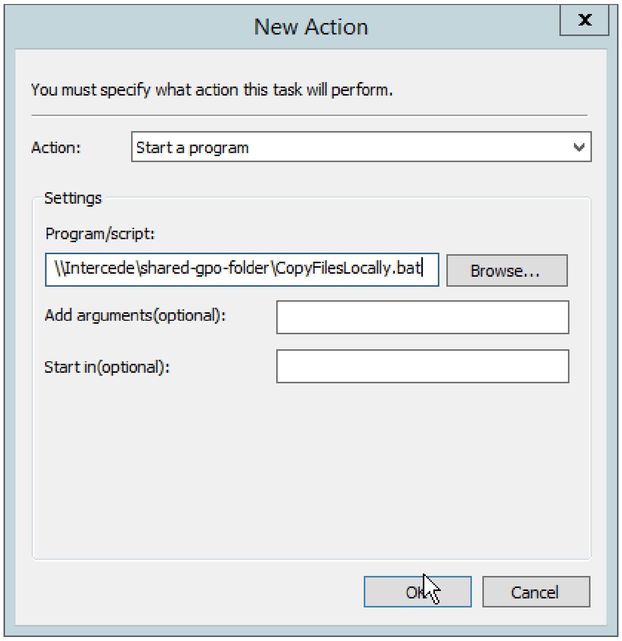


When you create a task, you must specify the action that will occur when your task starts.

20. Select **Start a program**.

21. For **Program/script,** enter the network location of the **CopyFilesLocally.bat** file.

22. Click **OK**.



You must specify what action this task will perform.

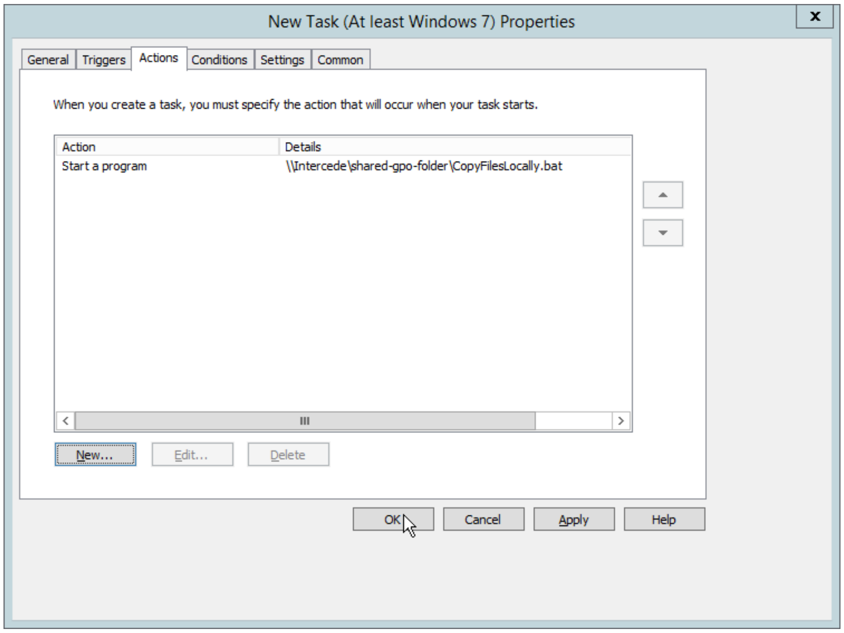
Action: Start a program

Program/script: \\Intercede\shared-gpo-folder\CopyFilesLocally.bat

Add arguments(optional):

Start in(optional):

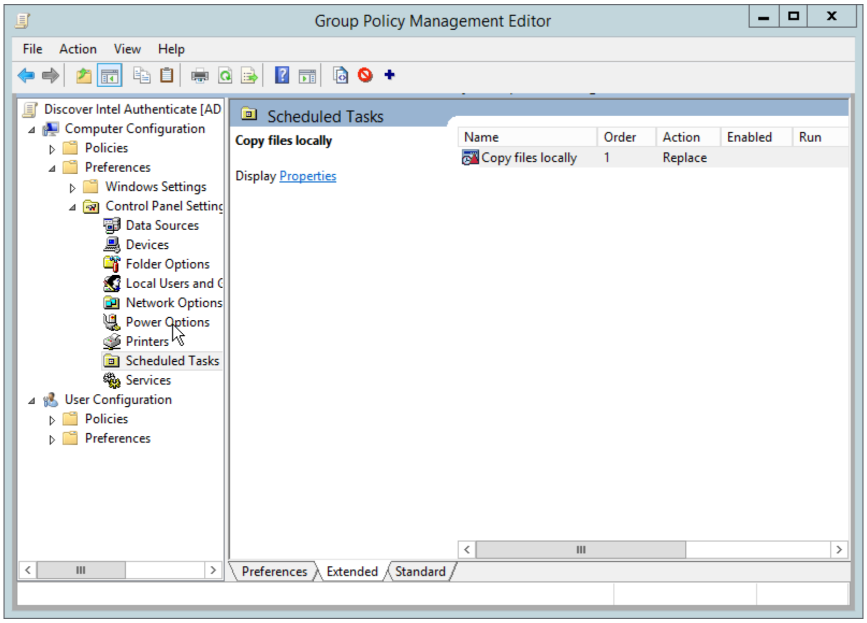
23. Click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	\\Intercede\shared-gpo-folder\CopyFilesLocally.bat

24. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.



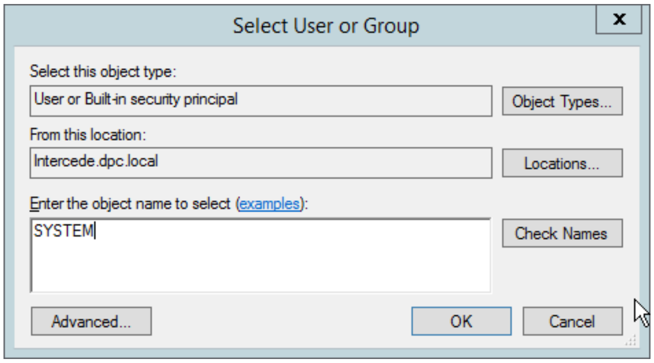
Name	Order	Action	Enabled	Run
Copy files locally	1	Replace		

25. Select **Replace** from the drop-down list for **Action**.

26. Enter a descriptive name.

27. Click **Change User or Group**.

28. Enter *SYSTEM* and click **OK**.



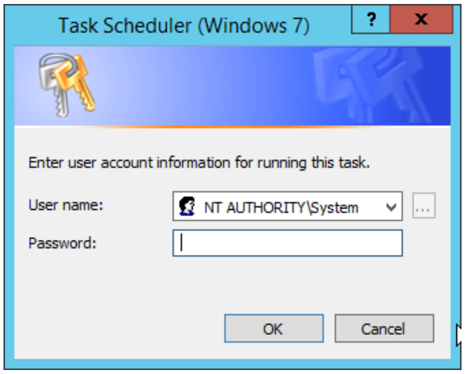
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

29. Check the box next to **Run whether user is logged on or not**.

30. A window will open asking for a password. Click **Cancel**.

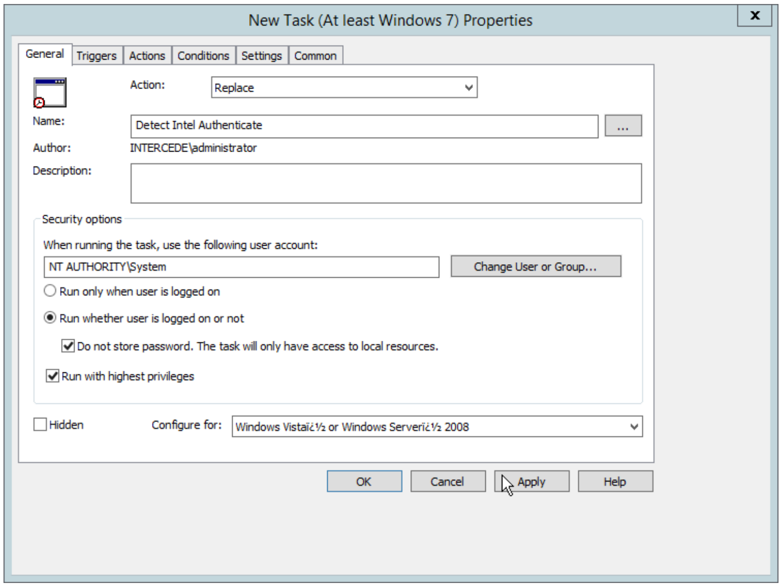

Task Scheduler (Windows 7)

Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

31. Check the box next to **Do not store password. The task will only have access to local resources**.
32. Check the box next to **Run with highest privileges**.


New Task (At least Windows 7) Properties

Action: Replace

Name: Detect Intel Authenticate

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

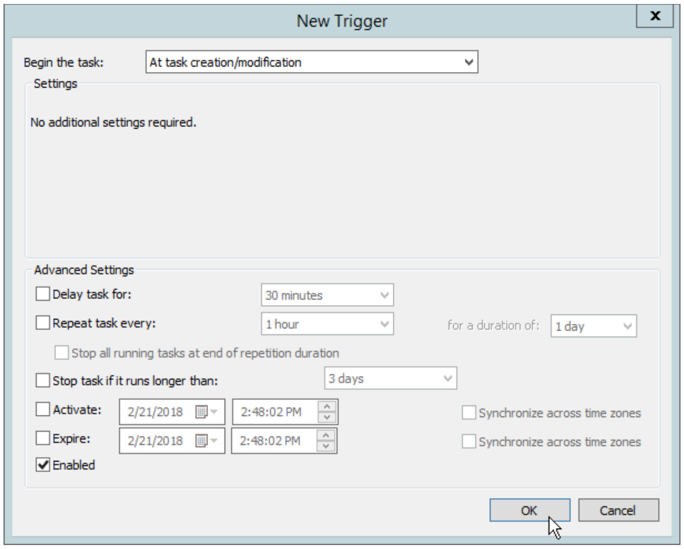
☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

33. Select the **Triggers** tab.
34. Click **New…**.
35. Select **At task creation/modification** for **Begin the task**.
36. Click **OK**.



New Trigger

Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

□ Delay task for: 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

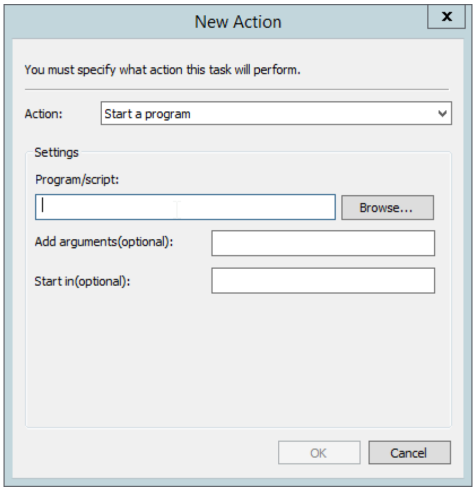
□ Stop task if it runs longer than: 3 days

□ Activate: 2/21/2018 2:48:02 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:48:02 PM □ Synchronize across time zones

☑ Enabled

37. Select the **Actions** tab.
38. Click **New….**
39. Select **Start a program**.



New Action

You must specify what action this task will perform.

Action: Start a program

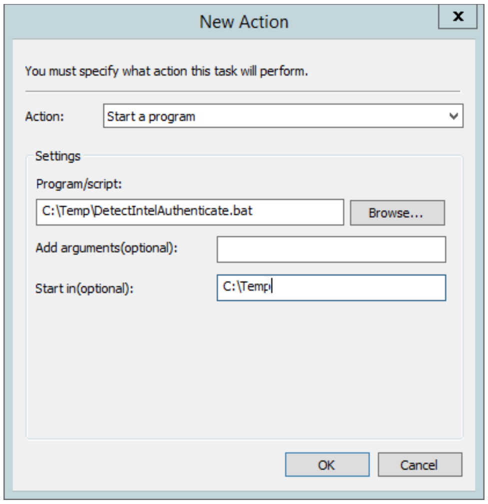
Settings

Program/script:

Add arguments(optional):

Start in(optional):

40. For **Program/script**, enter *C:\Temp\DetectIntelAuthenticate.bat*.
41. For **Start In**, enter *C:\Temp*.
42. Click **OK**.



You must specify what action this task will perform.

Action: Start a program

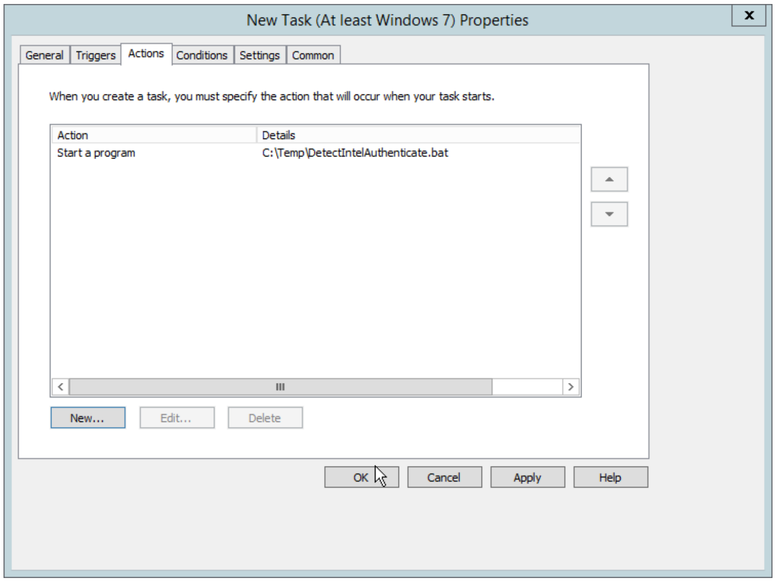
Program/script: C:\Temp\DetectIntelAuthenticate.bat

Add arguments(optional):

Start in(optional): C:\Temp

930

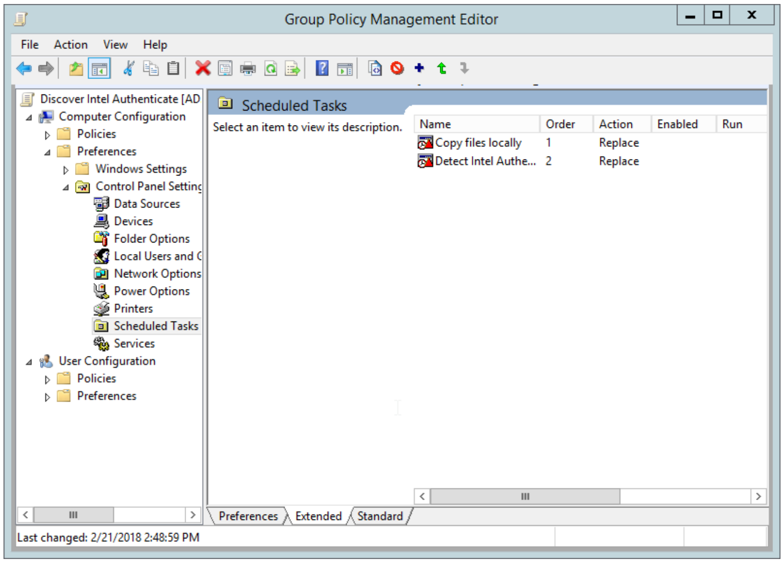
931 43. Click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Temp\DetectIntelAuthenticate.bat

932

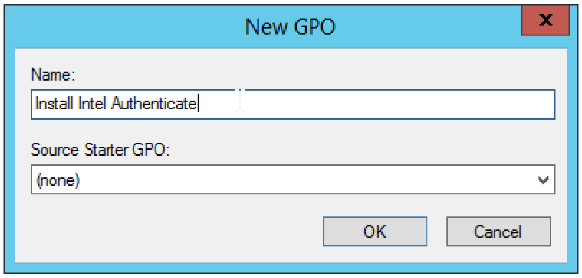


Name	Order	Action	Enabled	Run
Copy files locally	1	Replace		
Detect Intel Authe...	2	Replace		

Last changed: 2/21/2018 2:48:59 PM

2.2.6.6 Creating a GPO to Install Intel Authenticate

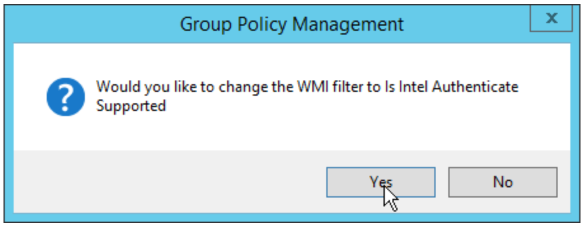
1. Open **Group Policy Management**.
2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.
3. Enter a **name** for this GPO.
4. Click **OK**.



Name:
Install Intel Authenticate

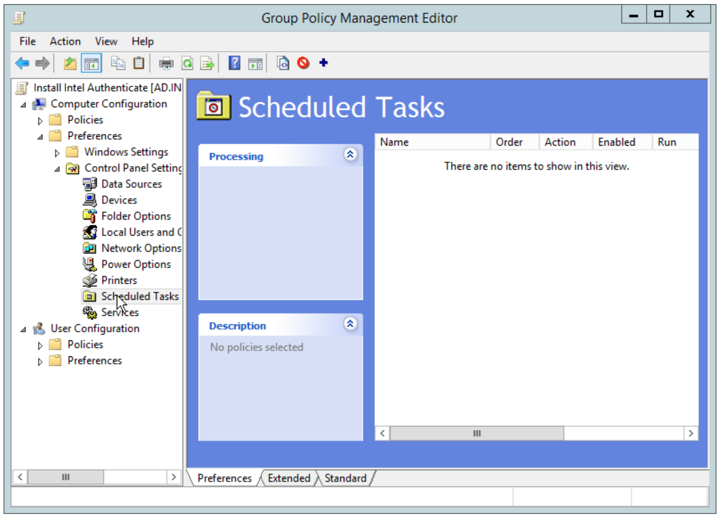
Source Starter GPO:
(none)

5. Select the GPO you just created and select **Is Intel Authenticate Supported** in the **WMI Filtering** section.
6. Click **Yes**.



Would you like to change the WMI filter to Is Intel Authenticate Supported

7. Right-click the GPO just created and select **Edit**.



There are no items to show in this view.

No policies selected

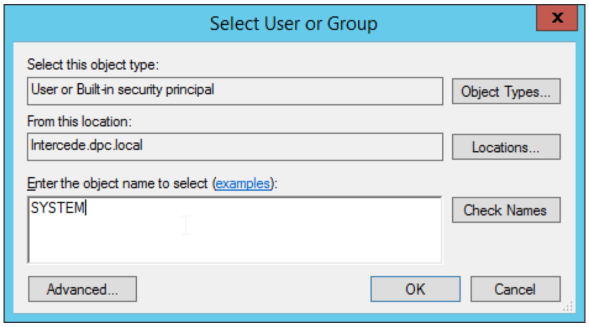
8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

9. Select **Replace** from the drop-down list for **Action**.

10. Enter a descriptive name.

11. Click **Change User or Group**.

12. Enter *SYSTEM* and click **OK**.



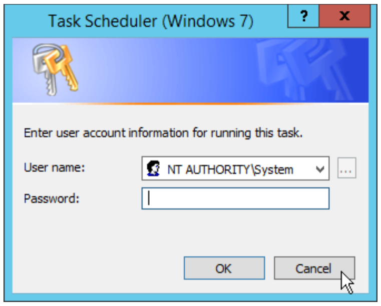
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

13. Check the box next to **Run whether user is logged on or not**.

14. A window will open asking for a password. Click **Cancel**.



Task Scheduler (Windows 7)

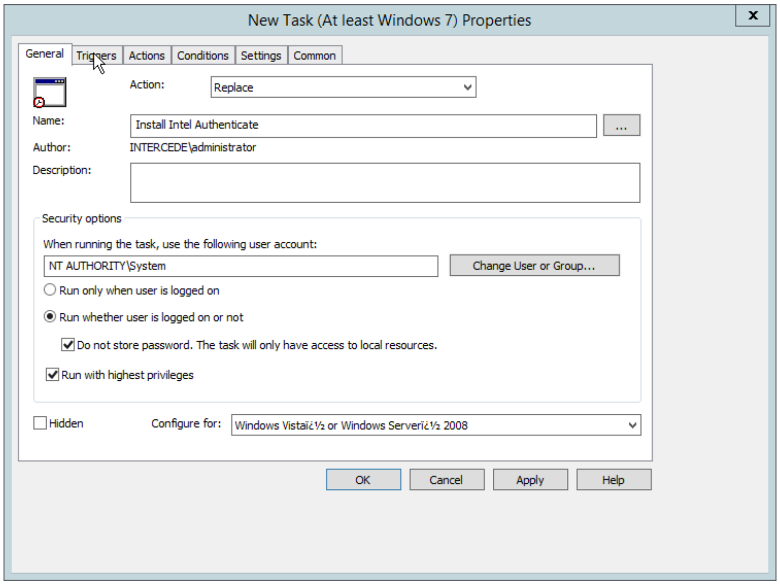
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

15. Check the box next to **Do not store password. The task will only have access to local resources**.

16. Check the box next to **Run with highest privileges**.



New Task (At least Windows 7) Properties

Action: Replace

Name: Install Intel Authenticate

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

17. Select the **Triggers** tab.

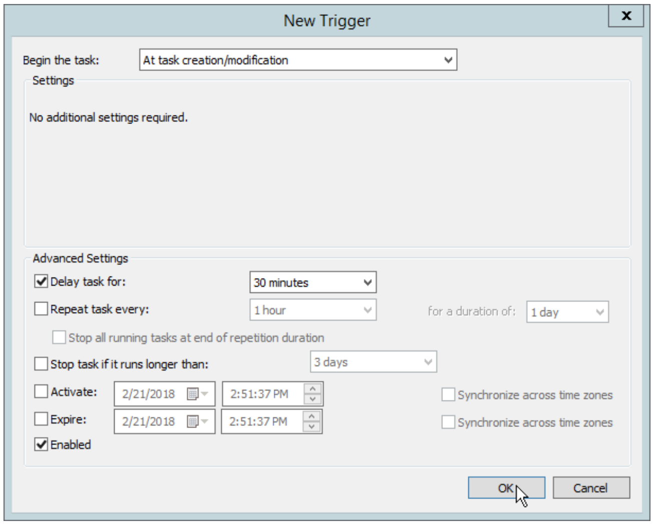
18. Click **New…**.

19. Select **At task creation/modification** for **Begin the task**.

20. Check the box next to **Delay task for**.

21. Select **30 minutes**.

22. Ensure **Enabled** is selected and Click **OK**.



New Trigger

Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

☑ Delay task for: 30 minutes

☐ Repeat task every: 1 hour for a duration of: 1 day

☐ Stop all running tasks at end of repetition duration

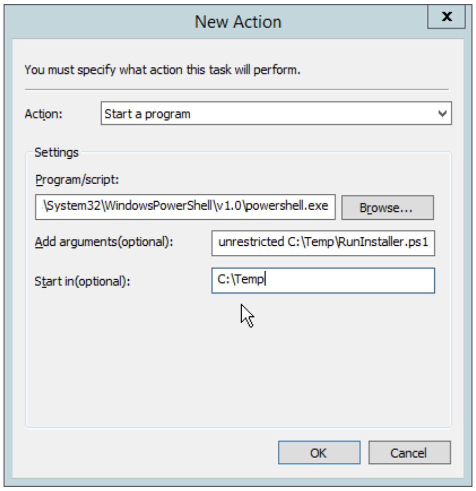
☐ Stop task if it runs longer than: 3 days

☐ Activate: 2/21/2018 2:51:37 PM ☐ Synchronize across time zones

☐ Expire: 2/21/2018 2:51:37 PM ☐ Synchronize across time zones

☑ Enabled

23. Select the **Actions** tab.
24. Click **New…**.
25. Select **Start a program**.
26. For **Program/script**, enter *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*.
27. For **Add arguments**, enter *-executionpolicy unrestricted C:\Temp\RunInstaller.ps1*.
28. For **Start In**, enter *C:\Temp*.
29. Click **OK**.



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: \System32\WindowsPowerShell\v1.0\powershell.exe

Add arguments(optional): unrestricted C:\Temp\RunInstaller.ps1

Start in(optional): C:\Temp

30. Click **OK**.

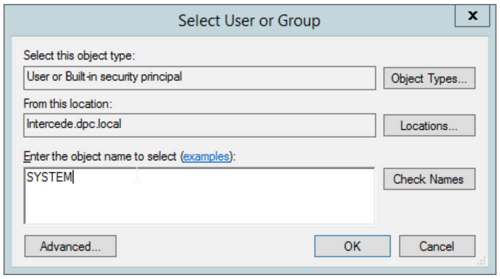
31. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

32. Select **Replace** from the drop-down list for **Action**.

33. Enter a descriptive name.

34. Click **Change User or Group**.

35. Enter *SYSTEM* and click **OK**.



Select User or Group

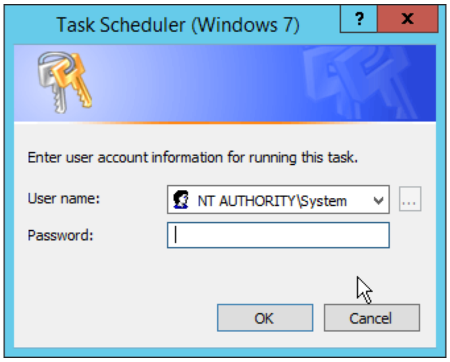
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

36. Check the box next to **Run whether user is logged on or not**.

37. A window will open asking for a password. Click **Cancel**.



Task Scheduler (Windows 7)

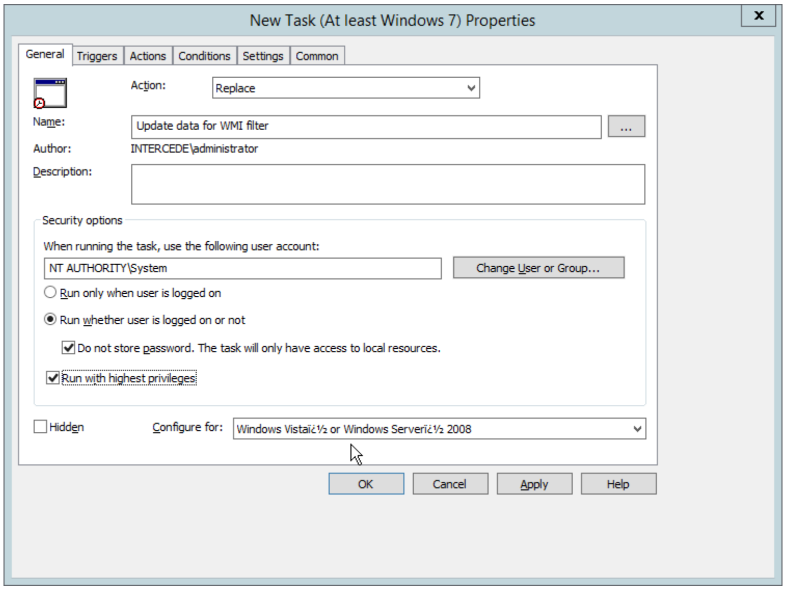
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

38. Check the box next to **Do not store password. The task will only have access to local resources**.

39. Check the box next to **Run with highest privileges**.



New Task (At least Windows 7) Properties

Action: Replace

Name: Update data for WMI filter

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

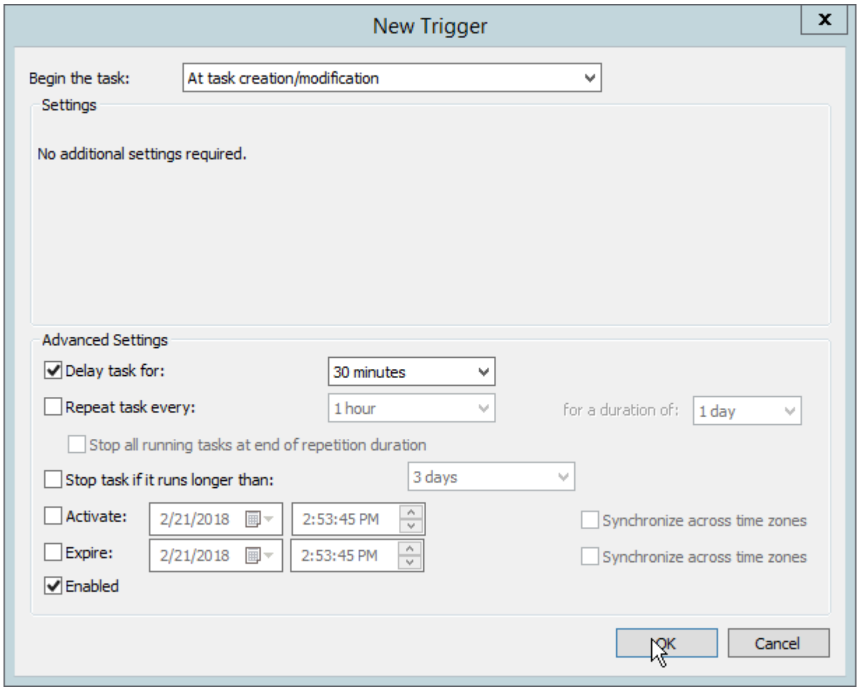
☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

40. Select the **Triggers** tab.
41. Click **New….**
42. Select **At task creation/modification** for **Begin the task**.
43. Check the box next to **Delay task for**.
44. Select **30 minutes**.
45. Ensure **Enabled** is selected and Click **OK**.



New Trigger

Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

☑ Delay task for: 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

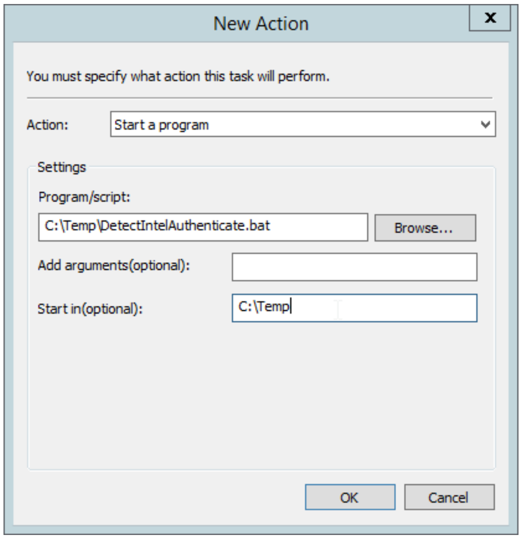
□ Stop task if it runs longer than: 3 days

□ Activate: 2/21/2018 2:53:45 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:53:45 PM □ Synchronize across time zones

☑ Enabled

46. Select the **Actions** tab.
47. Click **New…**.
48. Select **Start a program**.
49. For **Program/script**, enter *C:\Temp\DetectIntelAuthenticate.bat*.
50. For **Start In**, enter *C:\Temp*.
51. Click **OK**.



Action: Start a program

Settings

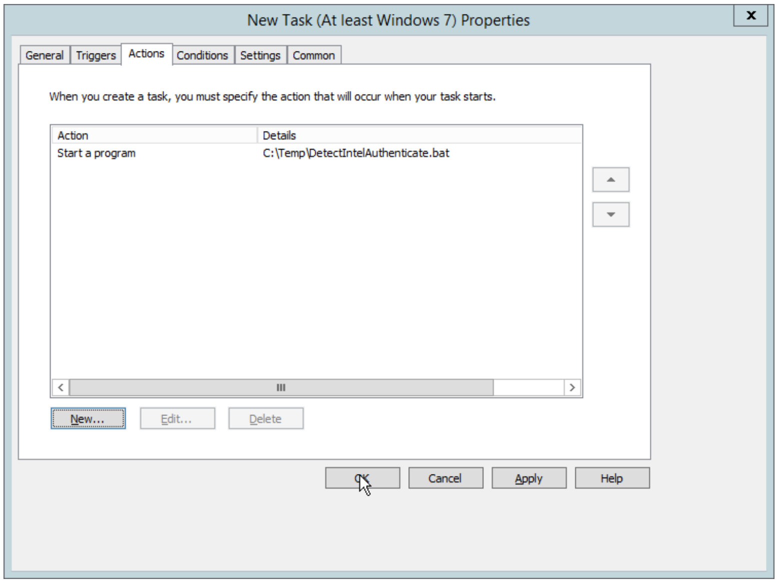
Program/script: C:\Temp\DetectIntelAuthenticate.bat

Add arguments(optional):

Start in(optional): C:\Temp

1002

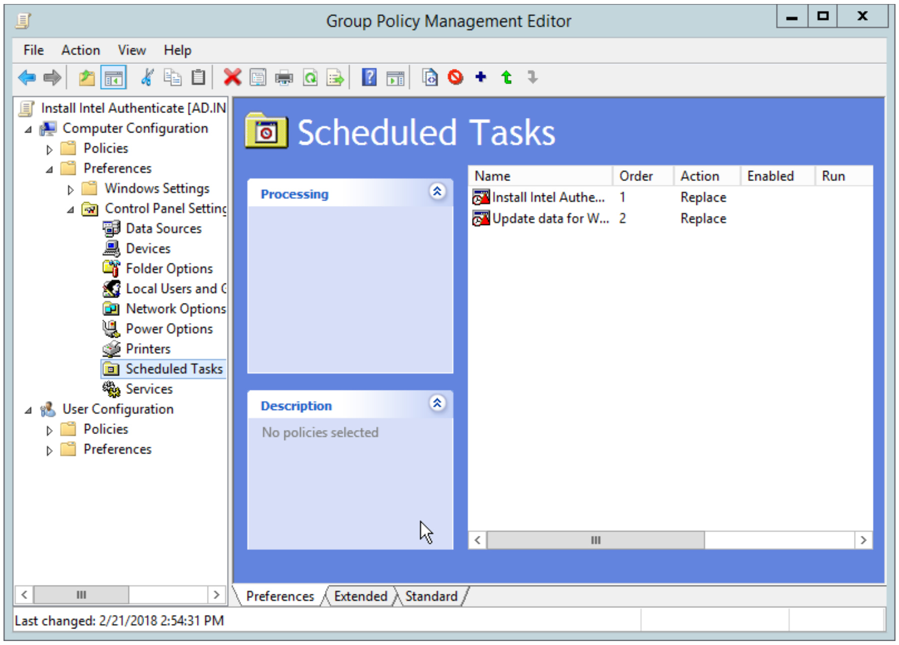
1003 52. Click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Temp\DetectIntelAuthenticate.bat

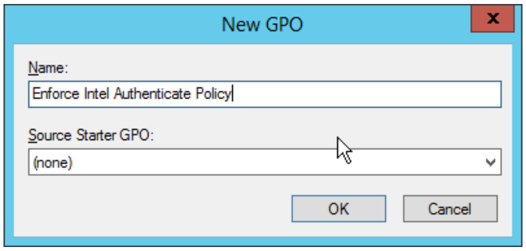
1004



Name	Order	Action	Enabled	Run
Install Intel Authe...	1	Replace		
Update data for W...	2	Replace		

2.2.6.7 Creating a GPO to Enforce the Policy

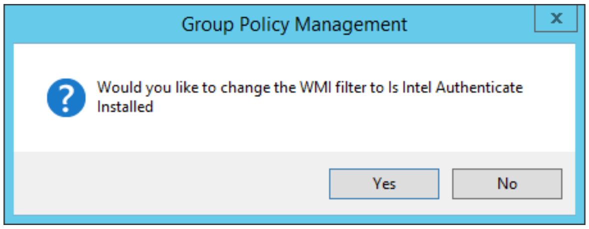
1. Open **Group Policy Management**.
2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.
3. Enter a name for this GPO
4. Click **OK**.



Name: Enforce Intel Authenticate Policy

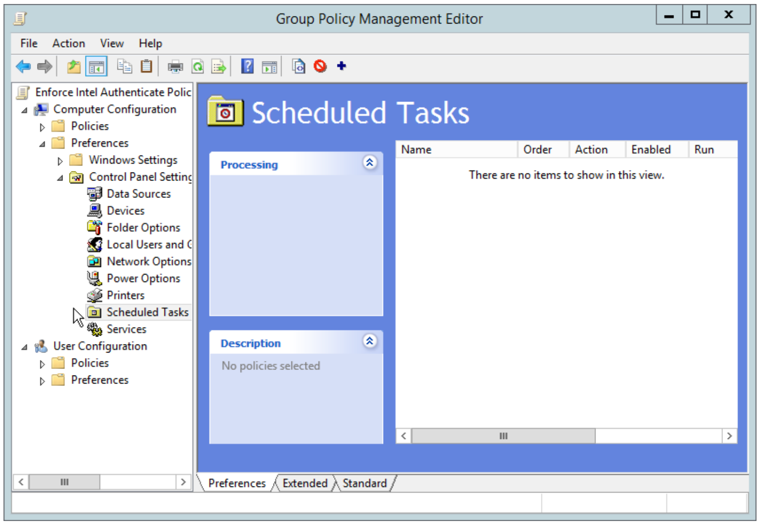
Source Starter GPO: (none)

5. Select the GPO you just created and select **Is Intel Authenticate Installed** in the **WMI Filtering** section.
6. Click **Yes**.



Would you like to change the WMI filter to Is Intel Authenticate Installed

7. Right-click the GPO just created and select **Edit**.



No policies selected

There are no items to show in this view.

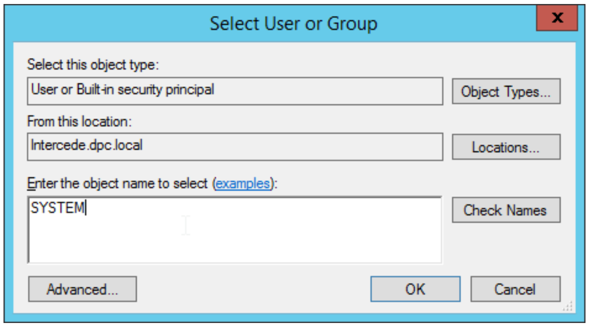
8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

9. Select **Replace** from the drop-down list for **Action**.

10. Enter a descriptive name.

11. Click **Change User or Group**.

12. Enter *SYSTEM* and click **OK**.



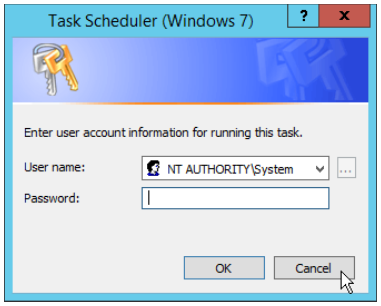
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

13. Check the box next to **Run whether user is logged on or not**.

14. A window will open asking for a password. Click **Cancel**.



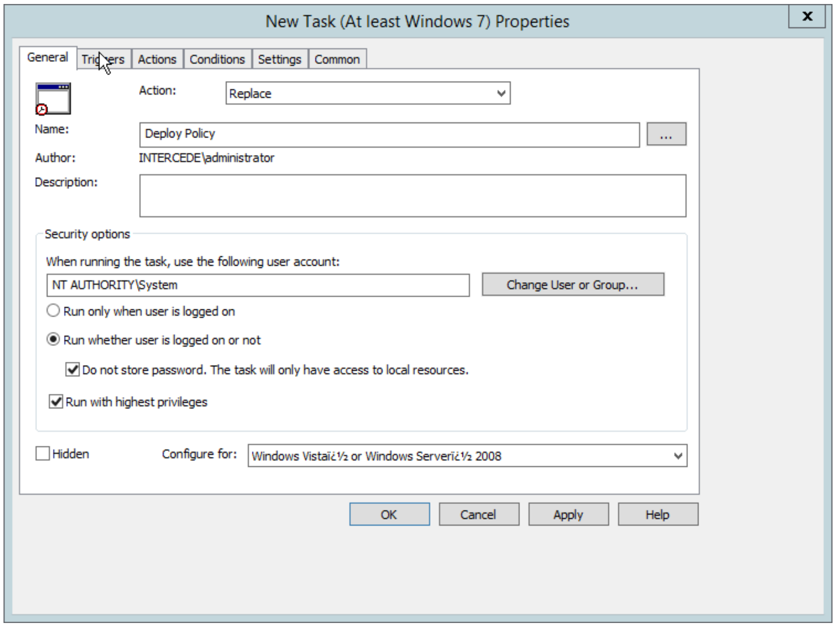
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

15. Check the box next to **Do not store password. The task will only have access to local resources**.

16. Check the box next to **Run with highest privileges**.



Action: Replace

Name: Deploy Policy

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

17. Select the **Triggers** tab.

18. Click **New…**.

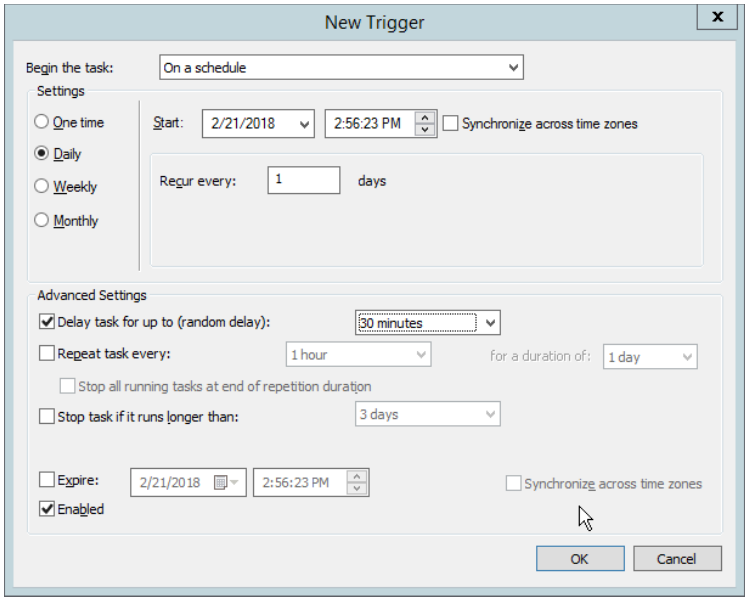
19. Select **On a schedule** for **Begin the task**.

20. Select **Daily**.

21. Check the box next to **Delay task for**.

22. Select **30 minutes**.

23. Ensure **Enabled** is selected and Click **OK**.



New Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 2/21/2018 2:56:23 PM □ Synchronize across time zones

Recur every: 1 days

Advanced Settings

☑ Delay task for up to (random delay): 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 2/21/2018 2:56:23 PM □ Synchronize across time zones

☑ Enabled

24. Select the **Actions** tab.

25. Click **New…**.

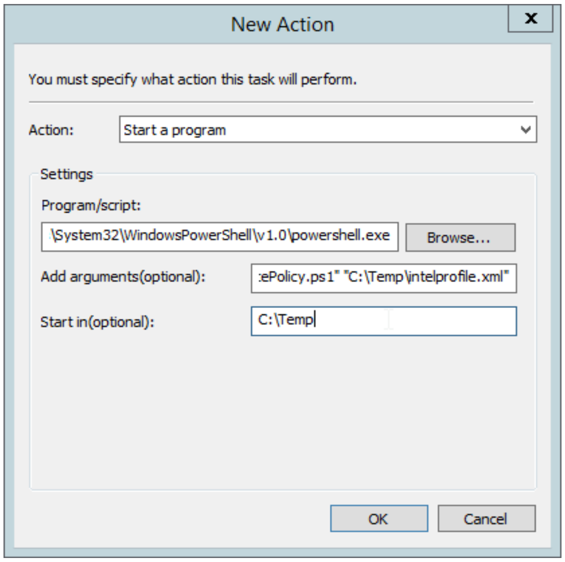
26. Select **Start a program**.

27. For **Program/script**, enter *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*.

28. For **Add arguments**, enter *-executionpolicy unrestricted "C:\Temp\EnforcePolicy.ps1" "C:\Temp\intelprofile.xml".*

29. For **Start In**, enter *C:\Temp*.

30. Click **OK**.



You must specify what action this task will perform.

Action: Start a program

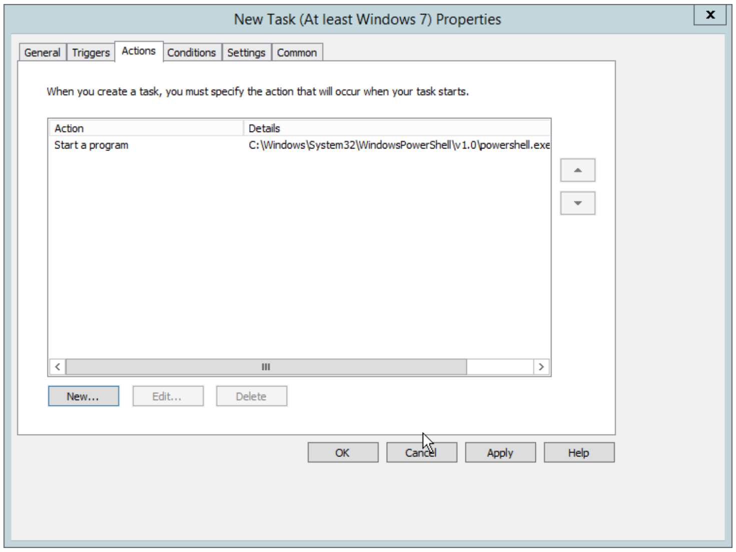
Settings

Program/script: \System32\WindowsPowerShell\v1.0\powershell.exe

Add arguments(optional): :ePolicy.ps1" "C:\Temp\intelprofile.xml"

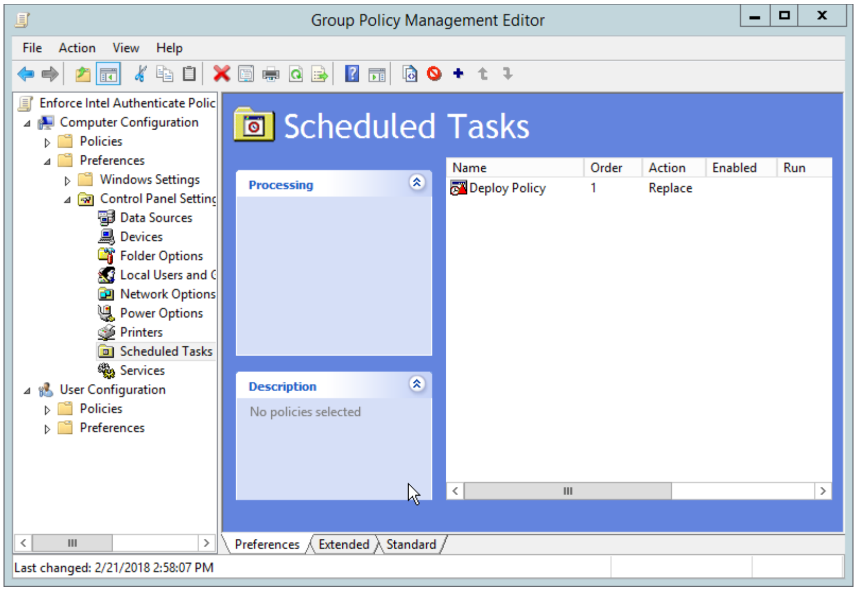
Start in(optional): C:\Temp

31. Click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe



Name	Order	Action	Enabled	Run
Deploy Policy	1	Replace		

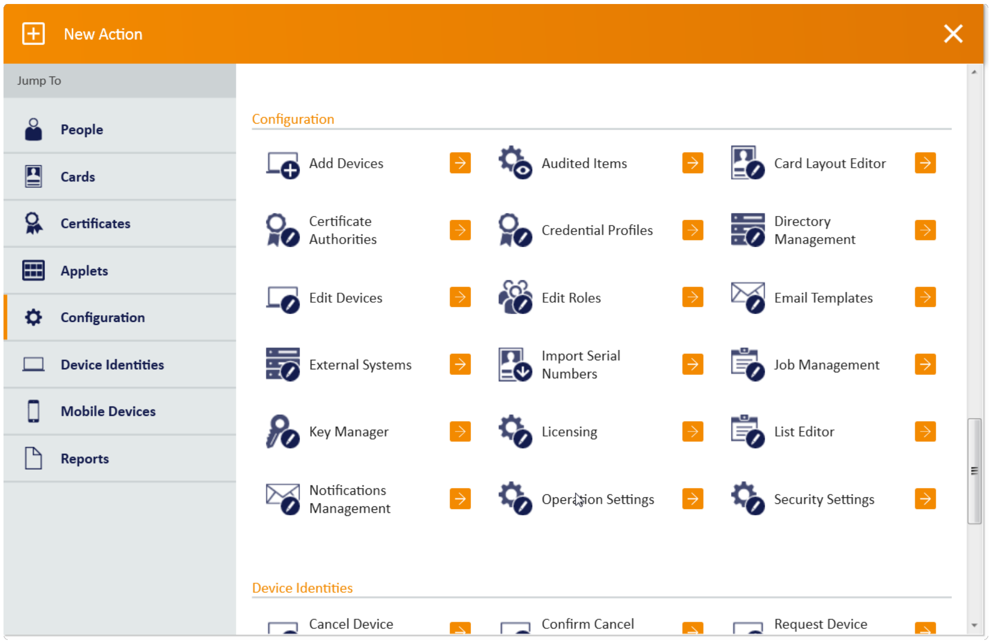
Last changed: 2/21/2018 2:58:07 PM

2.2.7 Intel VSC Configuration

The *Intel Authenticate Integration Guide for Active Directory Policy Objects* provides instructions on how to set up GPOs for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the *Intel Authenticate Integration Guide*.

2.2.7.1 Configuring MyID for Intel VSC

1. Open **MyID Desktop**.
2. Click **New Action**.
3. Click **Configuration > Operation Settings**.

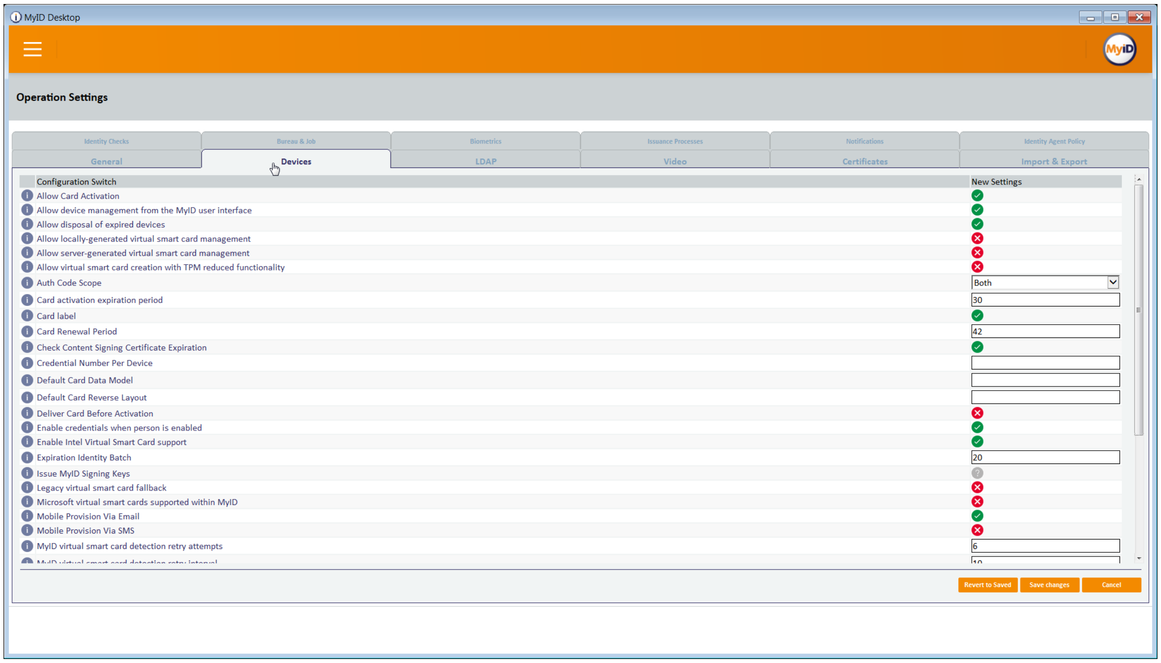


4. Go to the **Devices** tab.

5. Delete the value in **Default Card Data Model**.

6. Set **Enable Intel Virtual Smart Card support** to **Yes**.

7. Click **Save changes**.



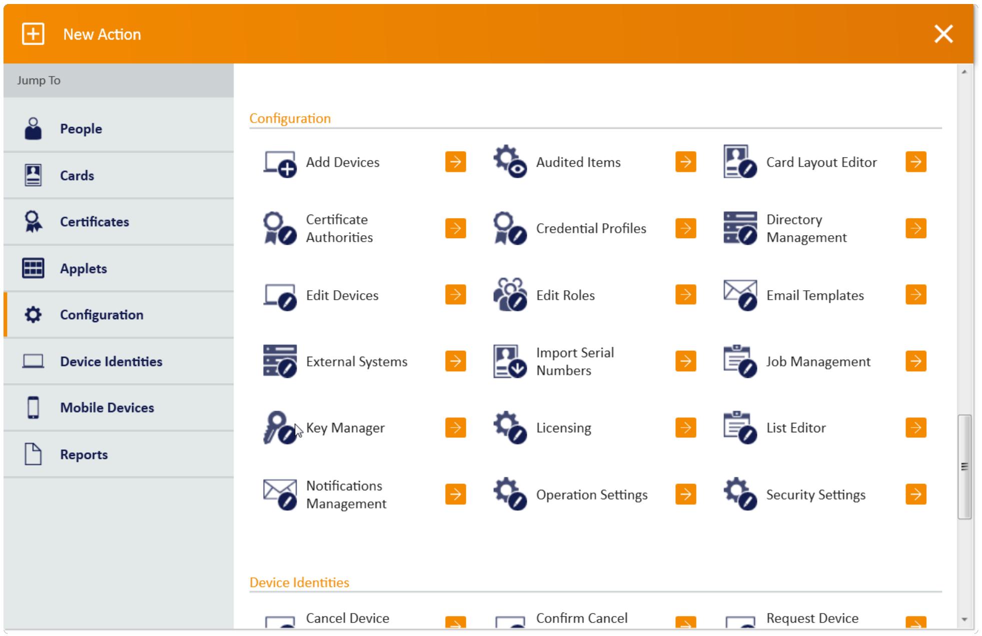
Operation Settings

Configuration Switch	New Settings
Allow Card Activation	✓
Allow device management from the MyID user interface	✓
Allow disposal of expired devices	✓
Allow locally-generated virtual smart card management	☒
Allow server-generated virtual smart card management	☒
Allow virtual smart card creation with TPM reduced functionality	☒
Auth Code Scope	Both
Card activation expiration period	30
Card label	✓
Card Renewal Period	42
Check Content Signing Certificate Expiration	✓
Credential Number Per Device	
Default Card Data Model	
Default Card Reverse Layout	
Deliver Card Before Activation	☒
Enable credentials when person is enabled	✓
Enable Intel Virtual Smart Card support	✓
Expiration Identity Batch	20
Issue MyID Signing Keys	?
Legacy virtual smart card fallback	☒
Microsoft virtual smart cards supported within MyID	☒
Mobile Provision Via Email	✓
Mobile Provision Via SMS	☒
MyID virtual smart card detection retry attempts	6
MyID virtual smart card detection retry interval	10

2.2.7.2 Setting Up a PIN Protection Key

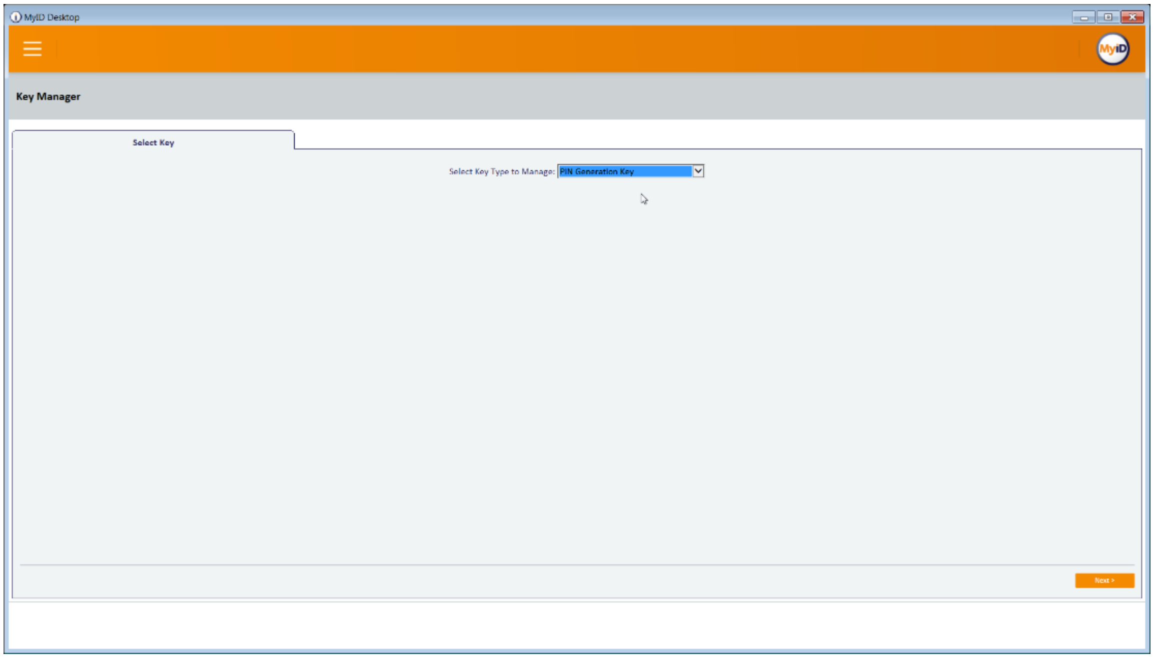
1. Click **New Action**.

2. Click **Configuration > Key Manager**.



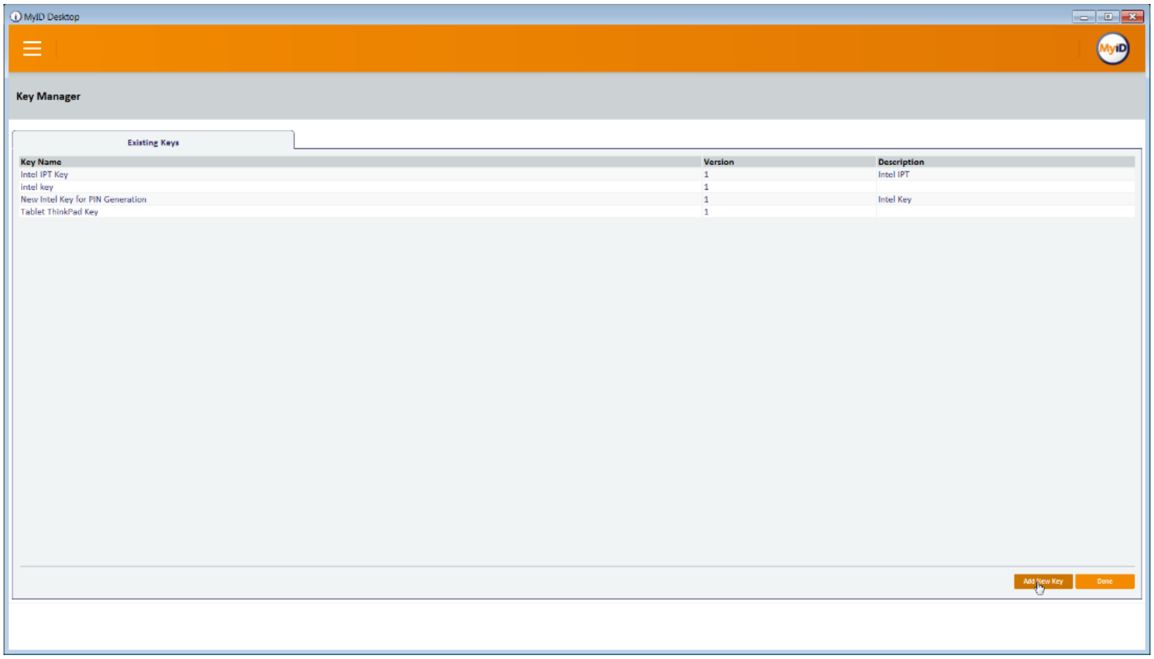
3. For **Select Key Type to Manage,** select **PIN Generation Key**.

4. Click **Next**.



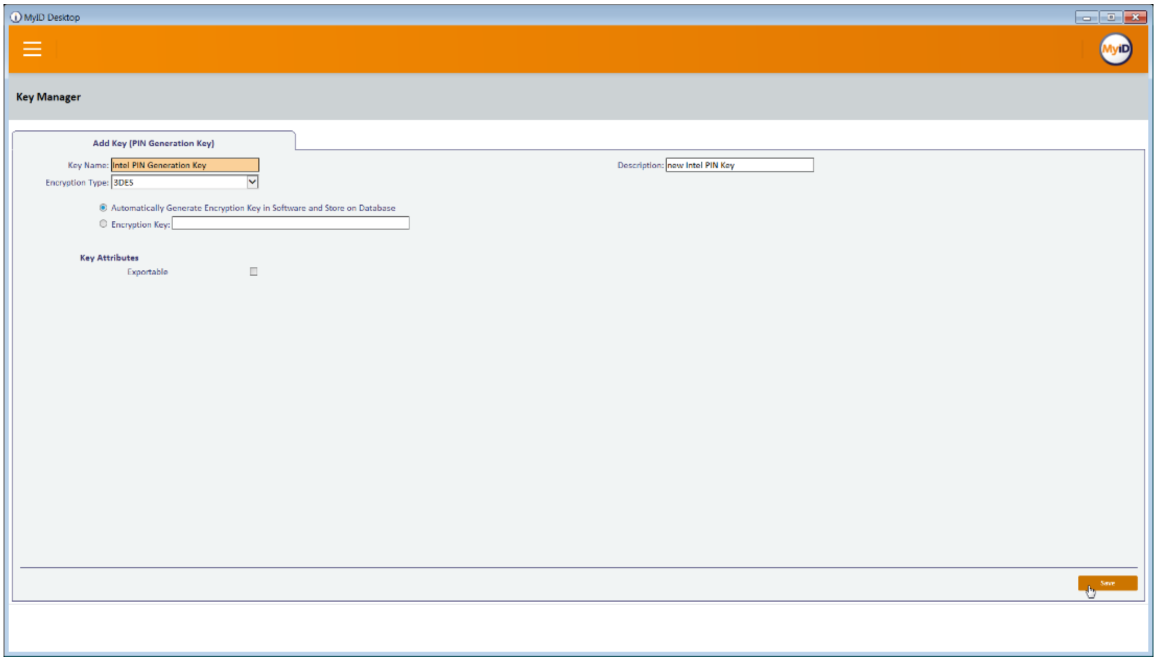
Select Key Type to Manage: PIN Generation Key

5. Click **Add New Key**.



Key Name	Version	Description
Intel IPT Key	1	Intel IPT
intel key	1	
New Intel Key for PIN Generation	1	Intel Key
Tablet ThinkPad Key	1	

6. Enter a **name** and a **description**.
7. For **Encryption Type,** select **3DES**.
8. Select **Automatically Generate Encryption Key in Software and Store on Database**.
9. Click **Save**.



Key Name: Intel PIN Generation Key

Description: new Intel PIN Key

Encryption Type: 3DES

● Automatically Generate Encryption Key in Software and Store on Database

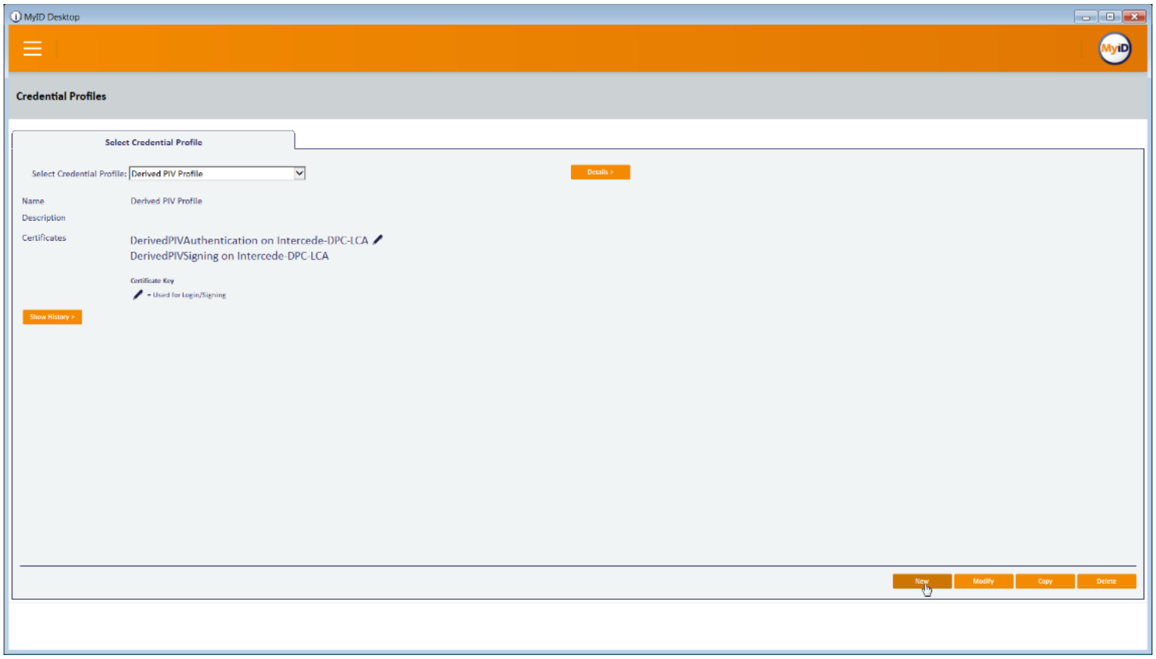
○ Encryption Key:

Key Attributes

Exportable □

2.2.7.3 Creating a Credential Profile

1. Click **New Action**.
2. Click **Configuration > Credential Profiles**.
3. Click **New**.



Credential Profiles

Select Credential Profile

Select Credential Profile: Derived PIV Profile

Name Derived PIV Profile

Description

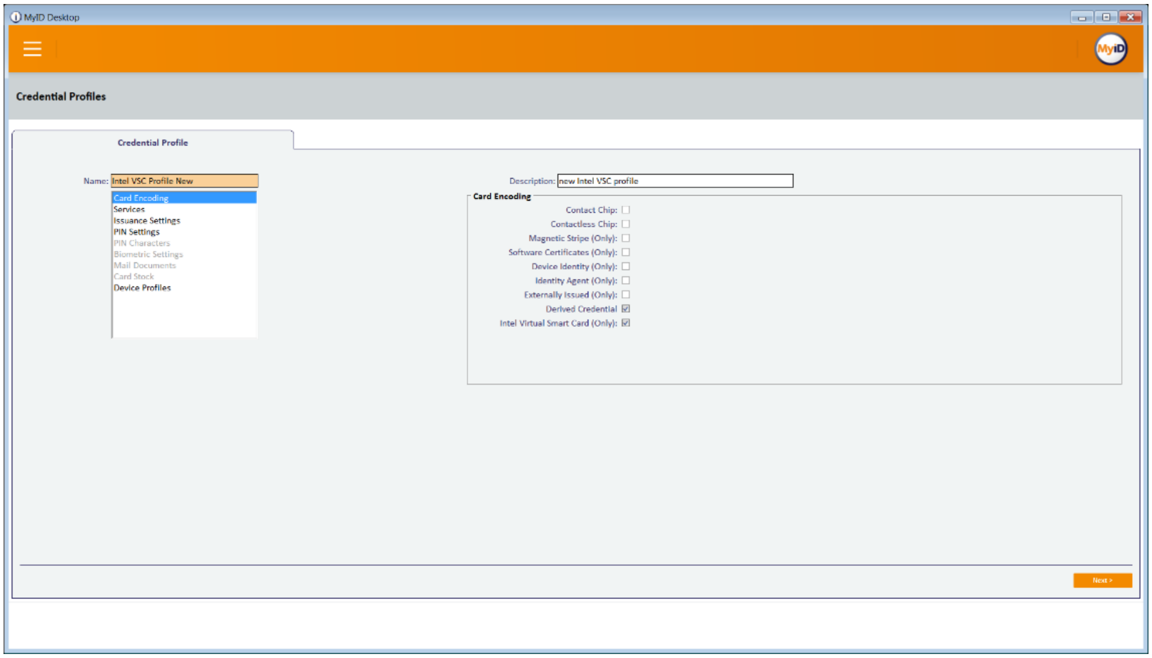
Certificates DerivedPIVAuthentication on Intercede-DPC-LCA
DerivedPIVSigning on Intercede-DPC-LCA

Certificate Key
= Used for Login/Signing

4. Enter a name and a description.

5. Check the box next to **Derived Credential**.

6. Check the box next to **Intel Virtual Smart Card (Only)**.



Credential Profiles

Credential Profile

Name: Intel VSC Profile New

Description: new Intel VSC profile

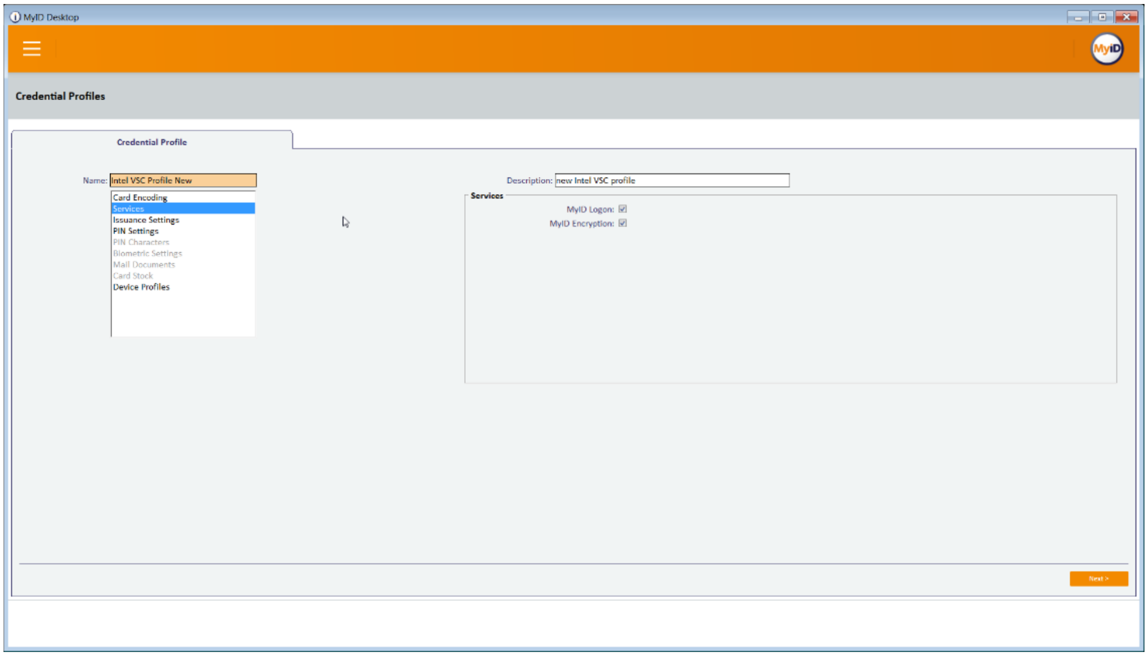
Card Encoding

Contact Chip: □
Contactless Chip: □
Magnetic Stripe (Only): □
Software Certificates (Only): □
Device Identity (Only): □
Identity Agent (Only): □
Externally Issued (Only): □
Derived Credential ☑
Intel Virtual Smart Card (Only): ☑

7. Select the **Services** tab.

8. Check the box next to **MyID Logon**.

9. Check the box next to **MyID Encryption**.



Name: Intel VSC Profile New

Description: new Intel VSC profile

Services

MyID Logon: ☑

MyID Encryption: ☑

10. Select the **Issuance Settings** tab.

11. Set **Require Activation** to **No**.

12. Set **Pre-encode Card** to **None**.

13. Set **Require Fingerprints at Issuance** to **Never Required**.

14. Set **Require Facial Biometrics** to **Never Required**.

15. Set **Additional Authentication** to **None**.

16. Set **Terms and Conditions** to **None**.

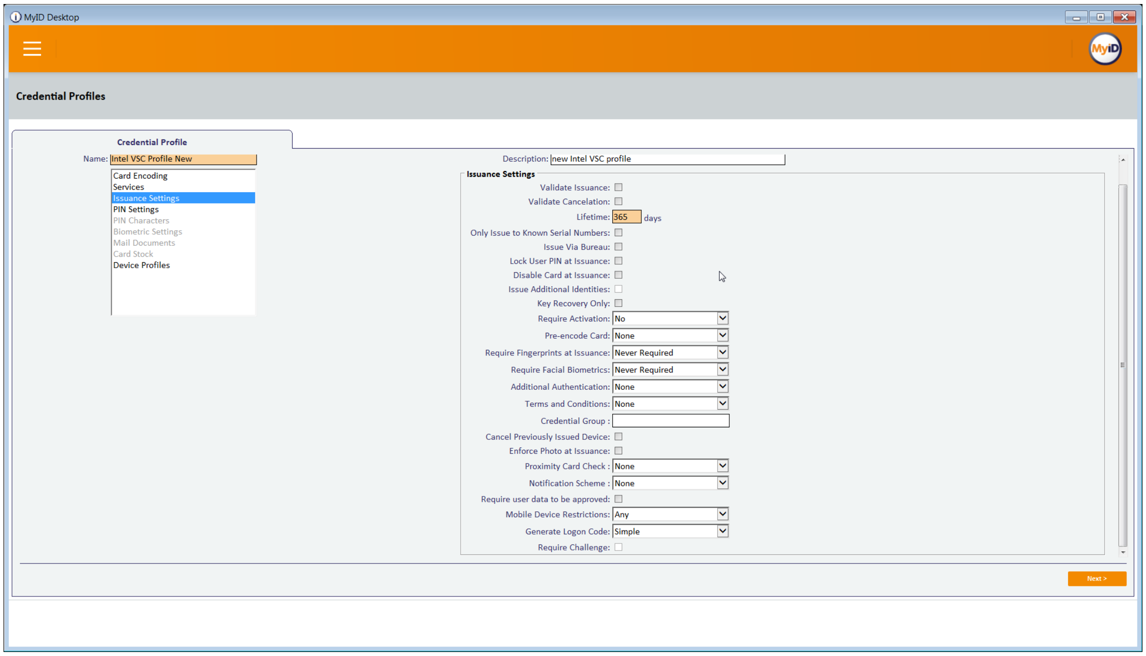
17. Set **Proximity Card Check** to **None**.

18. Set **Notification Scheme** to **None**.

19. Uncheck all boxes.

20. Set **Mobile Device Restrictions** to **Any**.

21. Set **Generate Logon Code** to **Simple**.



Name: Intel VSC Profile New

Description: new Intel VSC profile

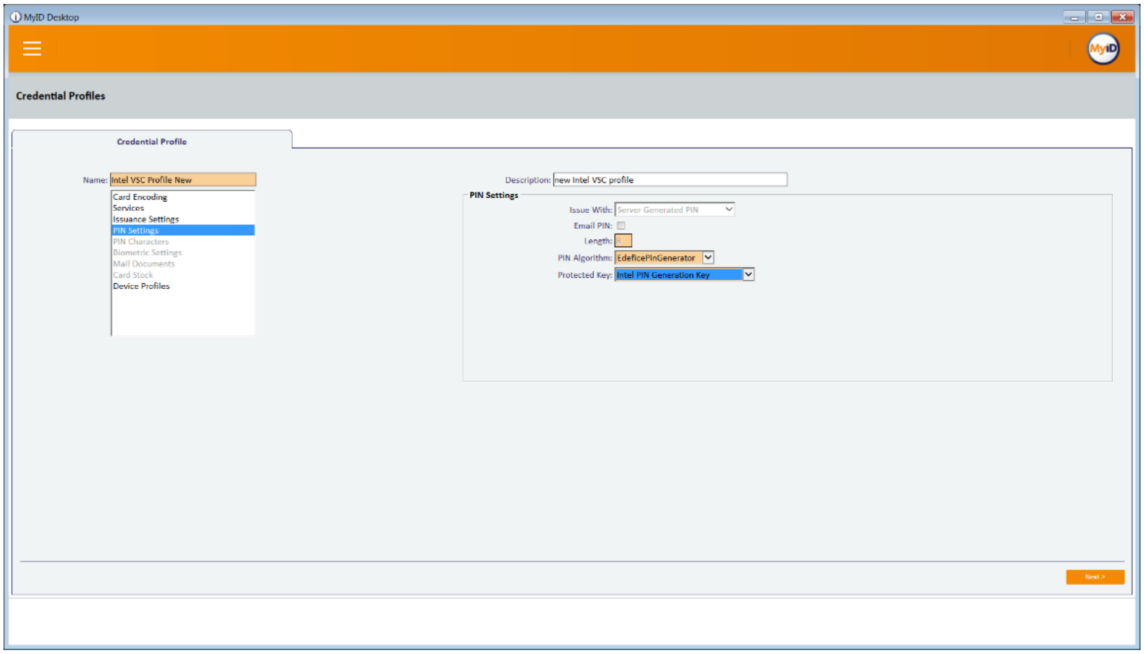
Issuance Settings

Validate Issuance: □
Validate Cancelation: □
Lifetime: 365 days
Only Issue to Known Serial Numbers: □
Issue Via Bureau: □
Lock User PIN at Issuance: □
Disable Card at Issuance: □
Issue Additional Identities: □
Key Recovery Only: □
Require Activation: No
Pre-encode Card: None
Require Fingerprints at Issuance: Never Required
Require Facial Biometrics: Never Required
Additional Authentication: None
Terms and Conditions: None
Credential Group :
Cancel Previously Issued Device: □
Enforce Photo at Issuance: □
Proximity Card Check : None
Notification Scheme : None
Require user data to be approved: □
Mobile Device Restrictions: Any
Generate Logon Code: Simple
Require Challenge: □

22. Select the **PIN Settings** tab.

23. For **PIN Algorithm**, select **EdeficePinGenerator**.

24. For **Protected Key**, select the PIN generation key created earlier.



Name: Intel VSC Profile New

Description: new Intel VSC profile

PIN Settings

Issue With: Server Generated PIN

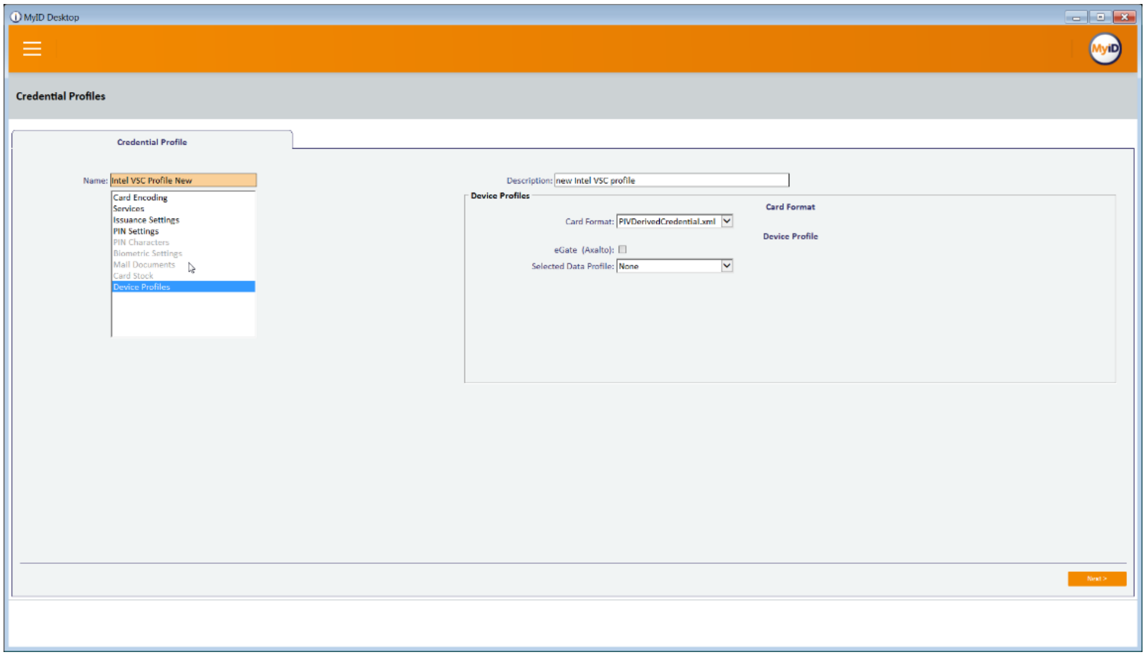
Email PIN: ☐

Length:

PIN Algorithm: EdeficePINGenerator

Protected Key: Intel PIN Generation Key

25. Select the **Device Profiles** tab.
26. For **Card Format**, select **PIVDerivedCredential.xml**.
27. Click **Next**.



Name: Intel VSC Profile New

Description: new Intel VSC profile

Device Profiles

Card Format

Card Format: PIVDerivedCredential.xml

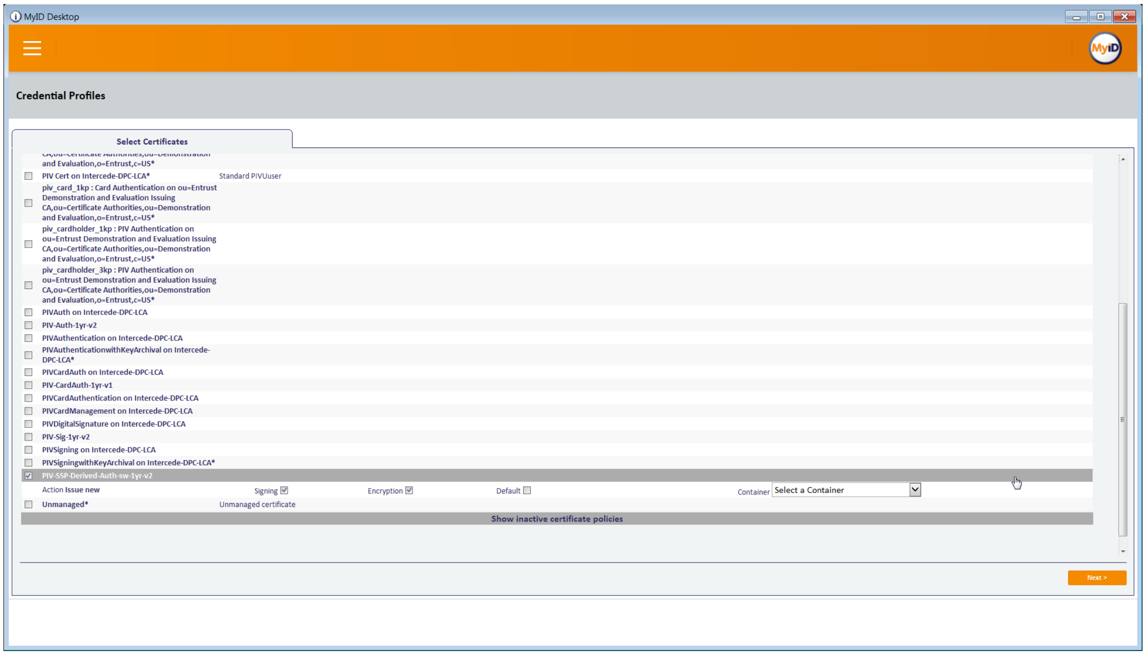
Device Profile

eGate (Axalto): ☐

Selected Data Profile: None

28. Select the certificates to be issued with the VSC.

29. Click **Next**.



Credential Profiles

Select Certificates

CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*

□	PIV Cert on Intercede-DPC-LCA*	Standard PIVUuser
□	piv_card_1kp : Card Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*	
□	piv_cardholder_1kp : PIV Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*	
□	piv_cardholder_3kp : PIV Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*	
□	PIVAuth on Intercede-DPC-LCA	
□	PIV-Auth-1yr-v2	
□	PIVAuthentication on Intercede-DPC-LCA	
□	PIVAuthenticationwithKeyArchival on Intercede-DPC-LCA*	
□	PIVCardAuth on Intercede-DPC-LCA	
□	PIV-CardAuth-1yr-v1	
□	PIVCardAuthentication on Intercede-DPC-LCA	
□	PIVCardManagement on Intercede-DPC-LCA	
□	PIVDigitalSignature on Intercede-DPC-LCA	
□	PIV-Sig-1yr-v2	
□	PIVSigning on Intercede-DPC-LCA	
□	PIVSigningwithKeyArchival on Intercede-DPC-LCA*	
☑	PIV-SSP-Derived-Auth-sw-1yr-v2	

Action **Issue new** Signing ☑ Encryption ☑ Default □ Container Select a Container

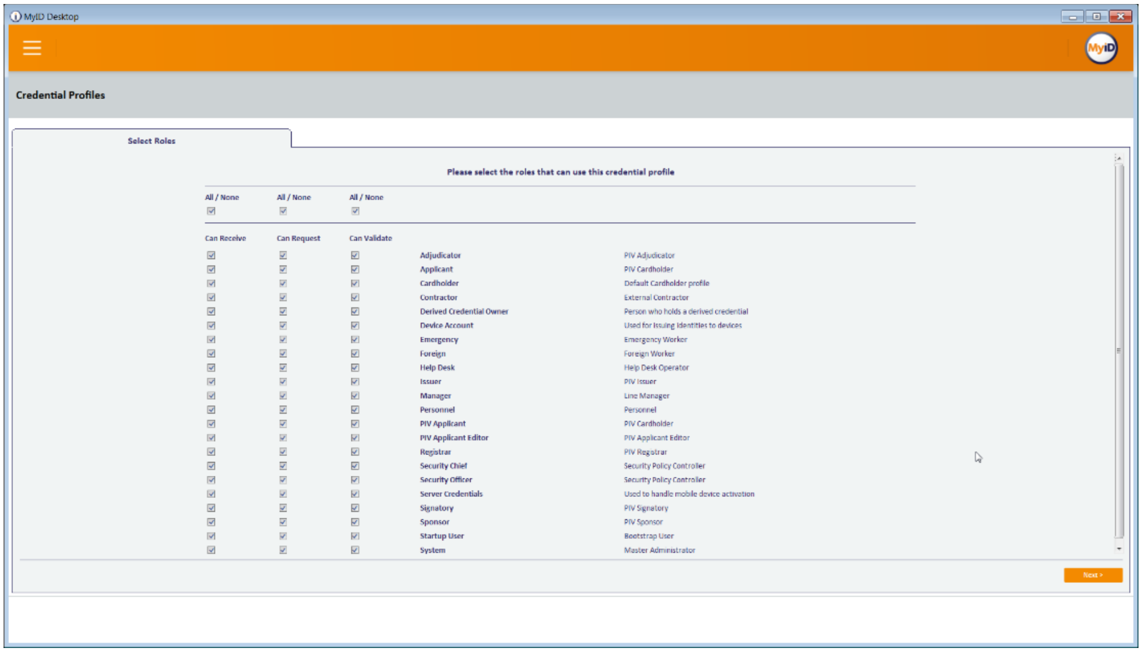
□	**Unmanaged***	Unmanaged certificate

Show inactive certificate policies

Next >

30. Select the roles that are allowed to use this profile.

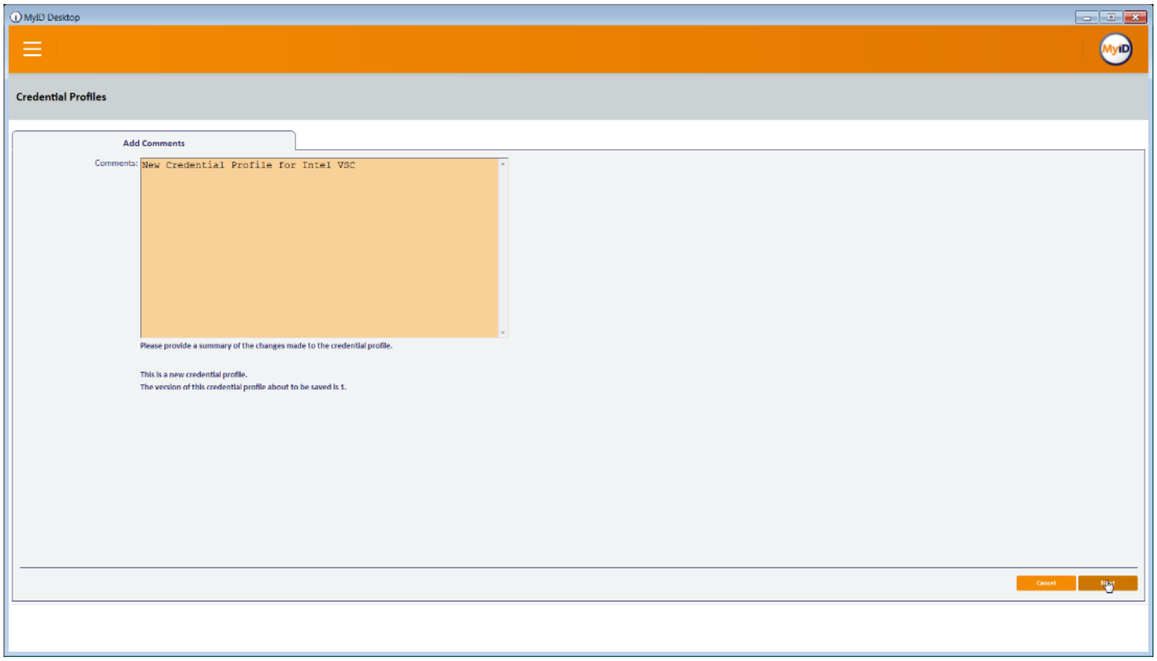
31. Click **Next**.



Please select the roles that can use this credential profile

All / None	All / None	All / None		
☑	☑	☑		
Can Receive	Can Request	Can Validate		
☑	☑	☑	Adjudicator	PIV Adjudicator
☑	☑	☑	Applicant	PIV Cardholder
☑	☑	☑	Cardholder	Default Cardholder profile
☑	☑	☑	Contractor	External Contractor
☑	☑	☑	Derived Credential Owner	Person who holds a derived credential
☑	☑	☑	Device Account	Used for issuing identities to devices
☑	☑	☑	Emergency	Emergency Worker
☑	☑	☑	Foreign	Foreign Worker
☑	☑	☑	Help Desk	Help Desk Operator
☑	☑	☑	Issuer	PIV Issuer
☑	☑	☑	Manager	Line Manager
☑	☑	☑	Personnel	Personnel
☑	☑	☑	PIV Applicant	PIV Cardholder
☑	☑	☑	PIV Applicant Editor	PIV Applicant Editor
☑	☑	☑	Registrar	PIV Registrar
☑	☑	☑	Security Chief	Security Policy Controller
☑	☑	☑	Security Officer	Security Policy Controller
☑	☑	☑	Server Credentials	Used to handle mobile device activation
☑	☑	☑	Signatory	PIV Signatory
☑	☑	☑	Sponsor	PIV Sponsor
☑	☑	☑	Startup User	Bootstrap User
☑	☑	☑	System	Master Administrator

32. Enter a description and click **Next**.



Comments: New Credential Profile for Intel VSC

Please provide a summary of the changes made to the credential profile.

This is a new credential profile.
The version of this credential profile about to be saved is 1.

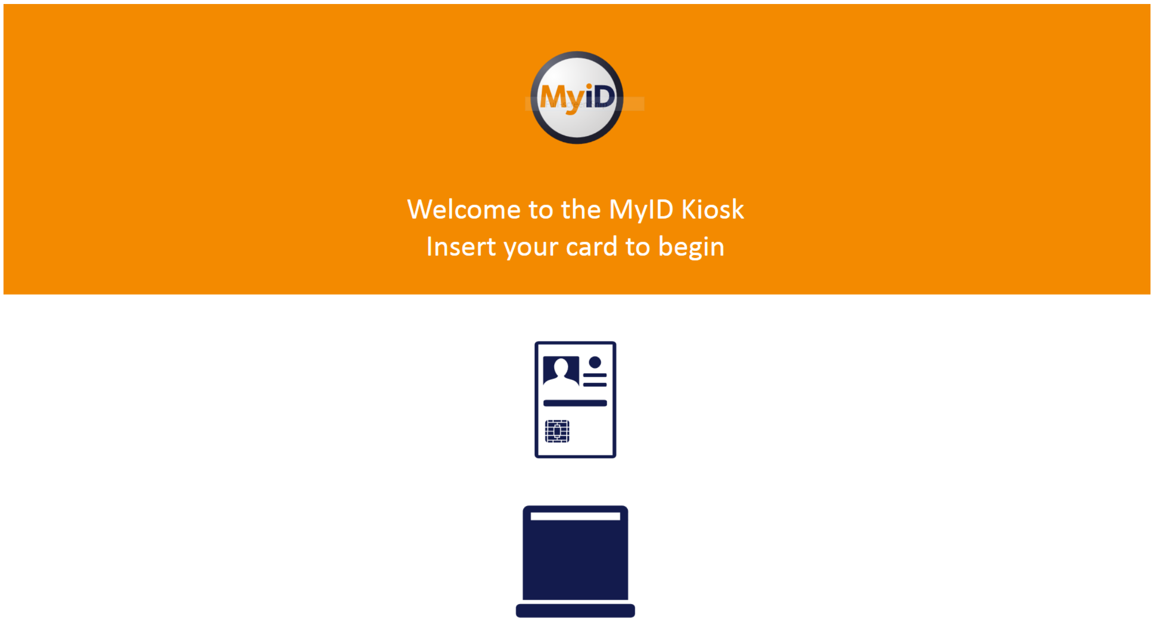
2.2.8 DPC Lifecycle Workflows

This section details the steps to perform issuance and termination of the DPC by using the MyID CMS. Issuance is started from the MyID Self-Service Kiosk application, while termination uses the MyID Desktop administration application.

2.2.8.1 Mobile Device Issuance Workflow

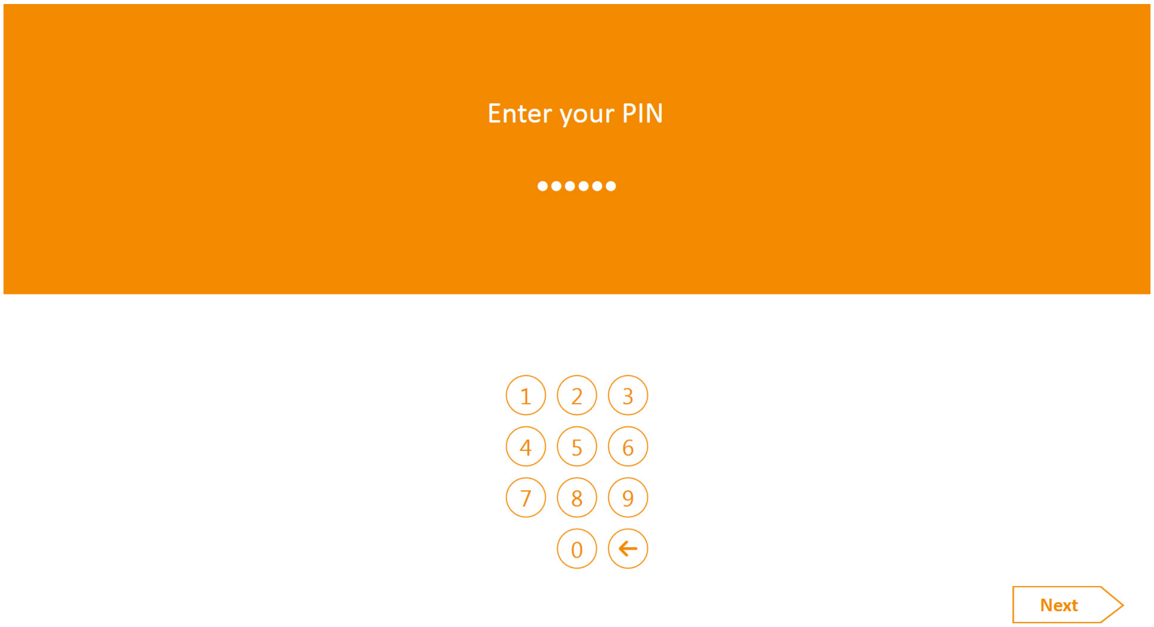
The following steps are performed by the DPC Applicant by using the MyID Self-Service Kiosk and the MyID Identity Agent application on the target mobile device.

1. At the Welcome screen of the MyID Self-Service Kiosk, insert your PIV Card into the card reader.

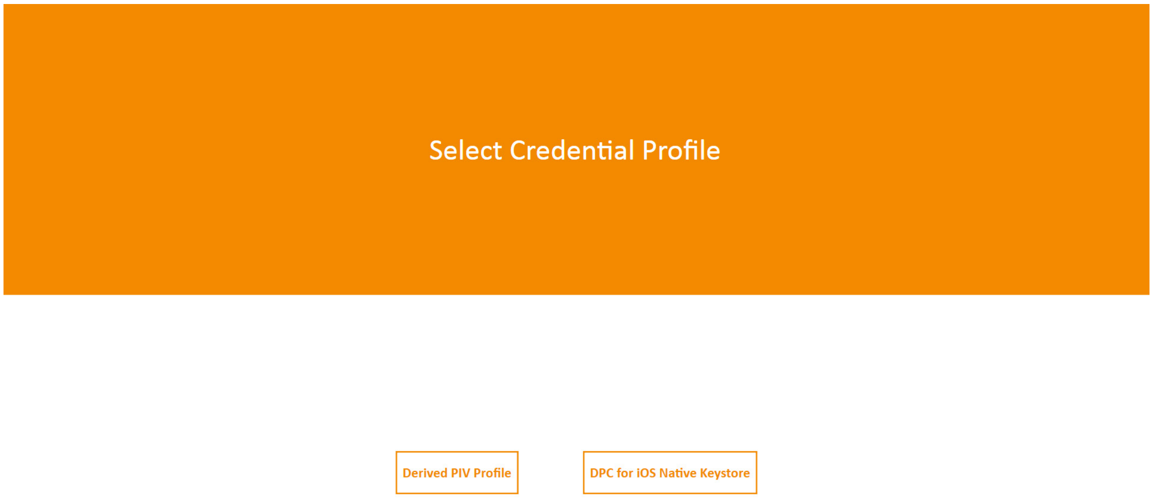


Welcome to the MyID Kiosk
Insert your card to begin

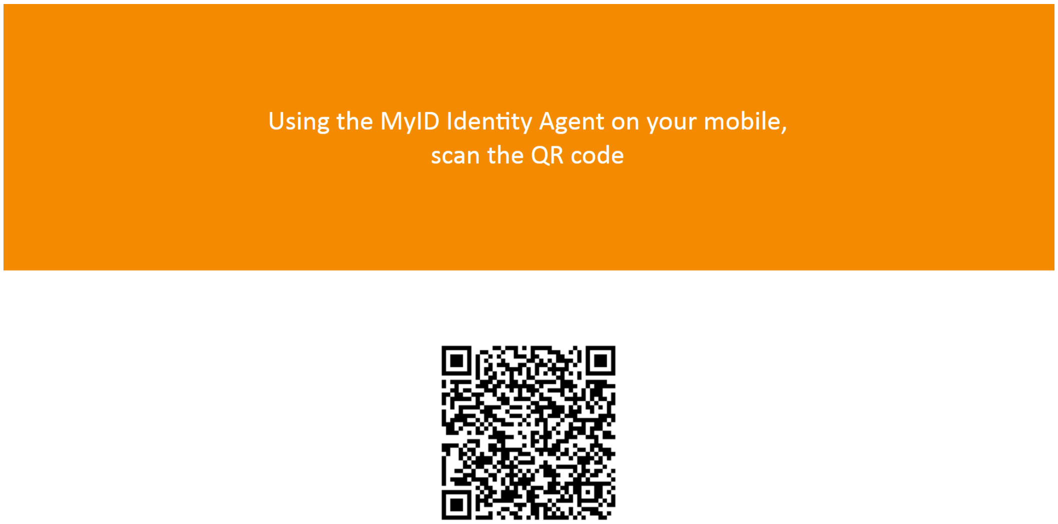
2. On the **Enter your PIN** screen:
    a. Enter the PIN used to activate the inserted PIV Card.
    b. Select **Next**.



3. On the **Select Credential Profile** screen:
    a. To provision the DPC to the MyID software token, select **Derived PIV Profile**.
    b. To provision the DPC to the iOS Secure Enclave hardware-backed token, select **DPC for Native iOS Keystore**.

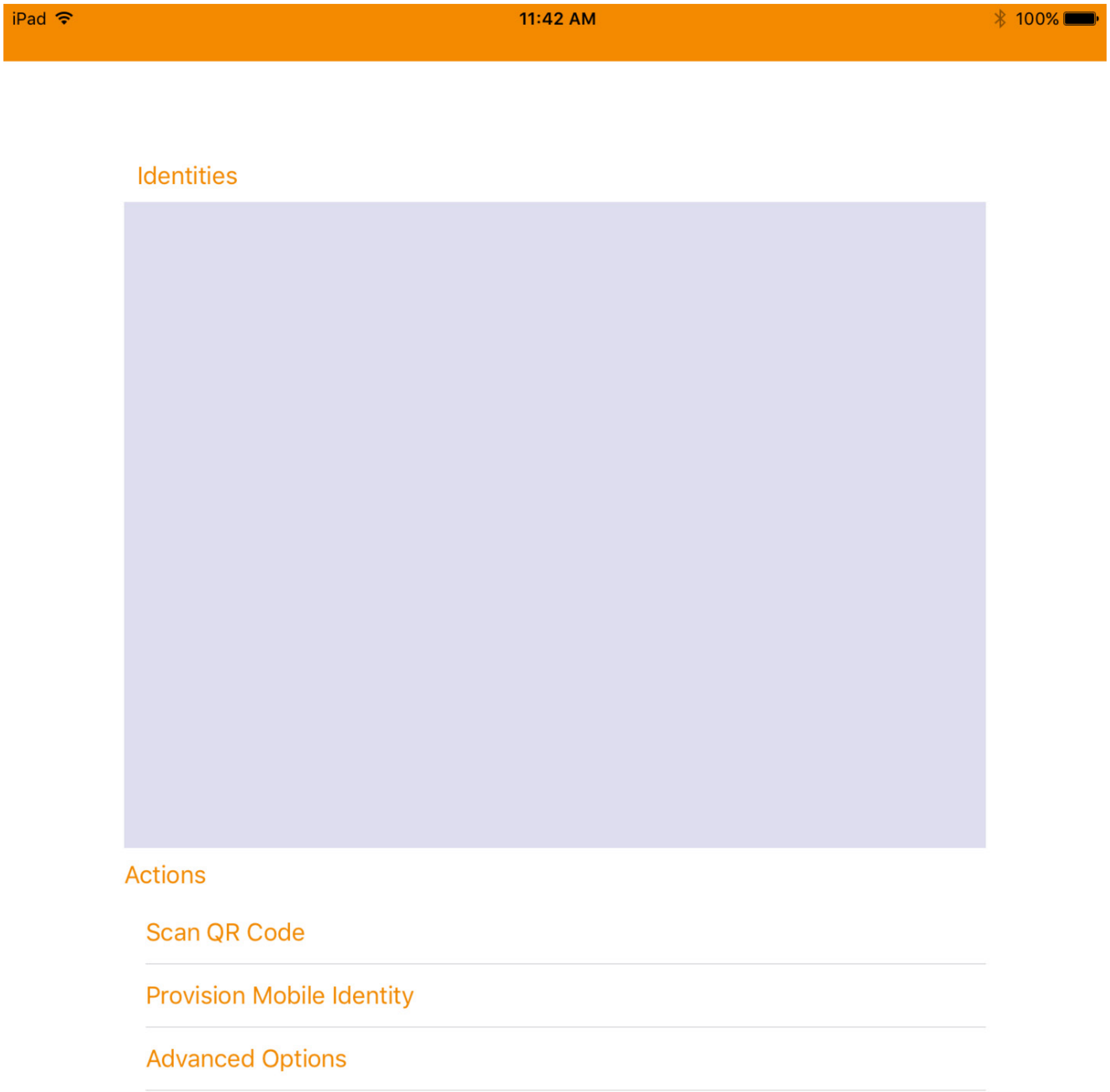


    c. The MyID Self-Service Kiosk will display a QR code; the remaining steps are completed by using the MyID Identity Agent application on the target mobile device.

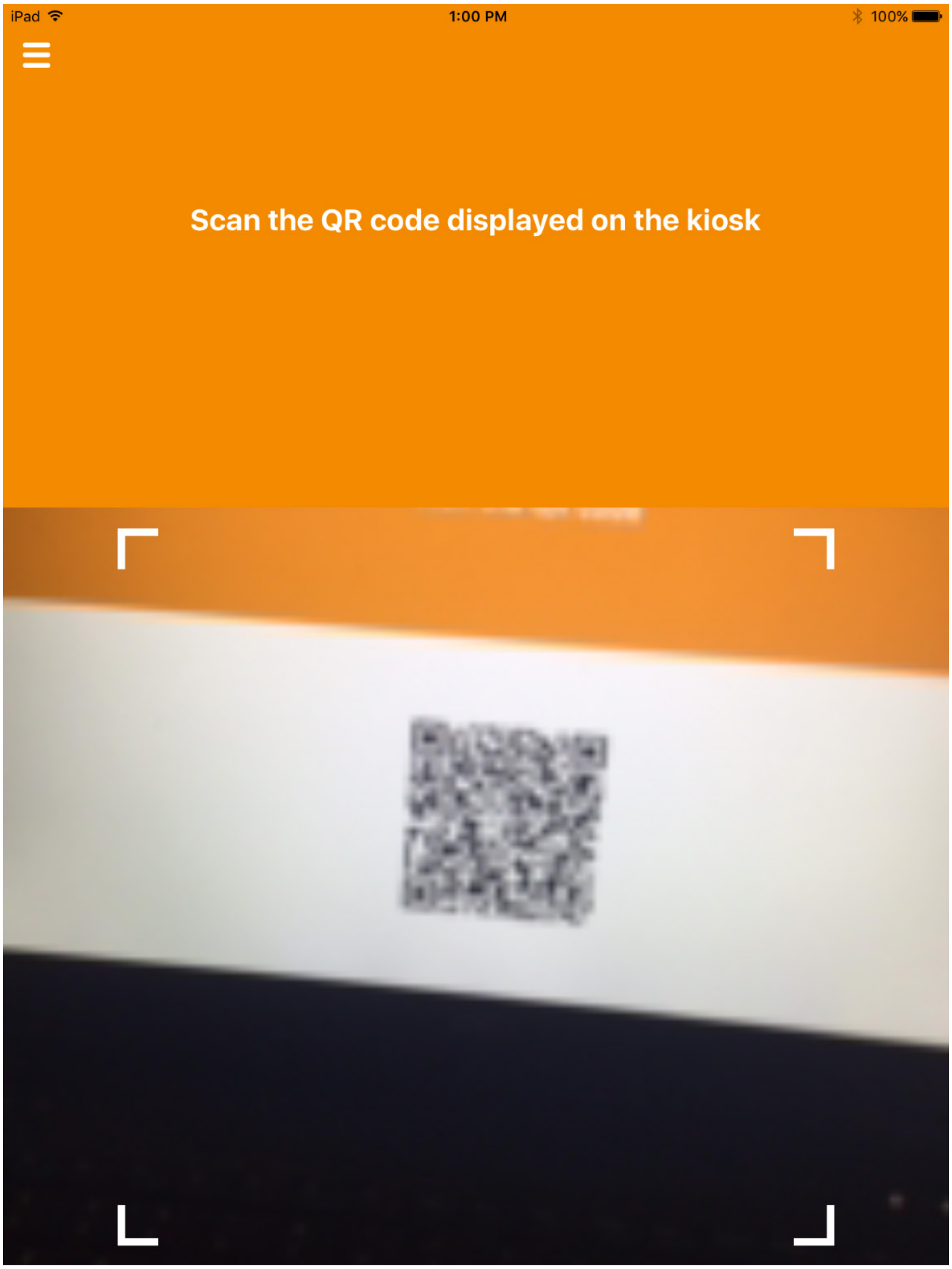


Using the MyID Identity Agent on your mobile, scan the QR code

4. Launch MyID Identity Agent.
5. On the initial screen, under **Actions**, tap **Scan QR Code**.



6. Use the device camera to capture the QR code displayed by the MyID Self-Service Kiosk.

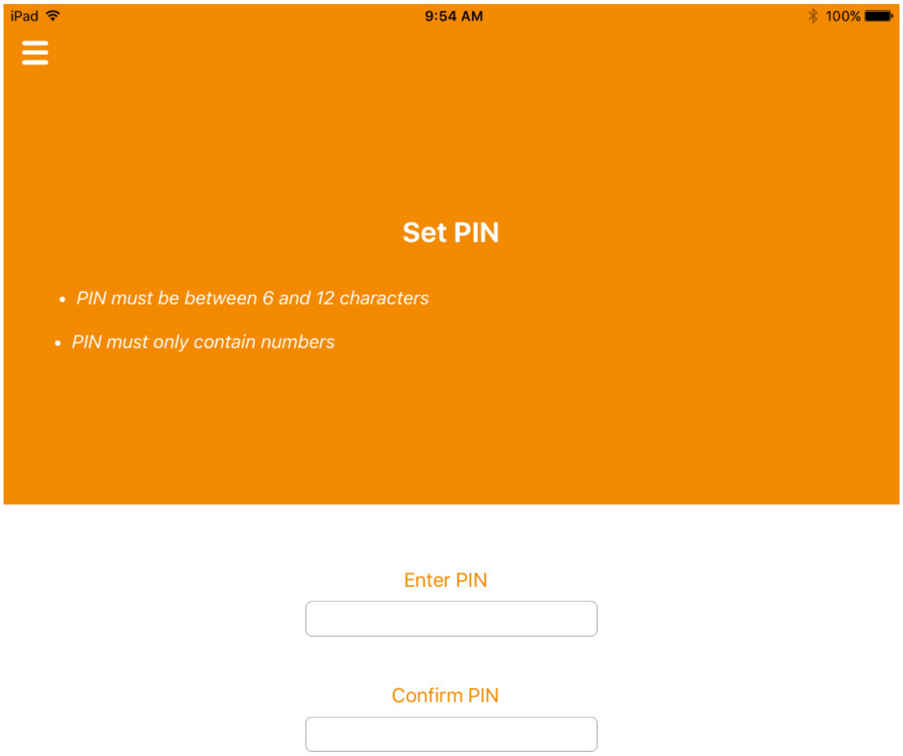


Scan the QR code displayed on the kiosk

7. On the **Set PIN** screen:

    a. In the **Enter PIN** field, enter a numeric PIN that will be used to activate the DPC.

b. In the **Confirm PIN** field, enter the same numeric PIN.



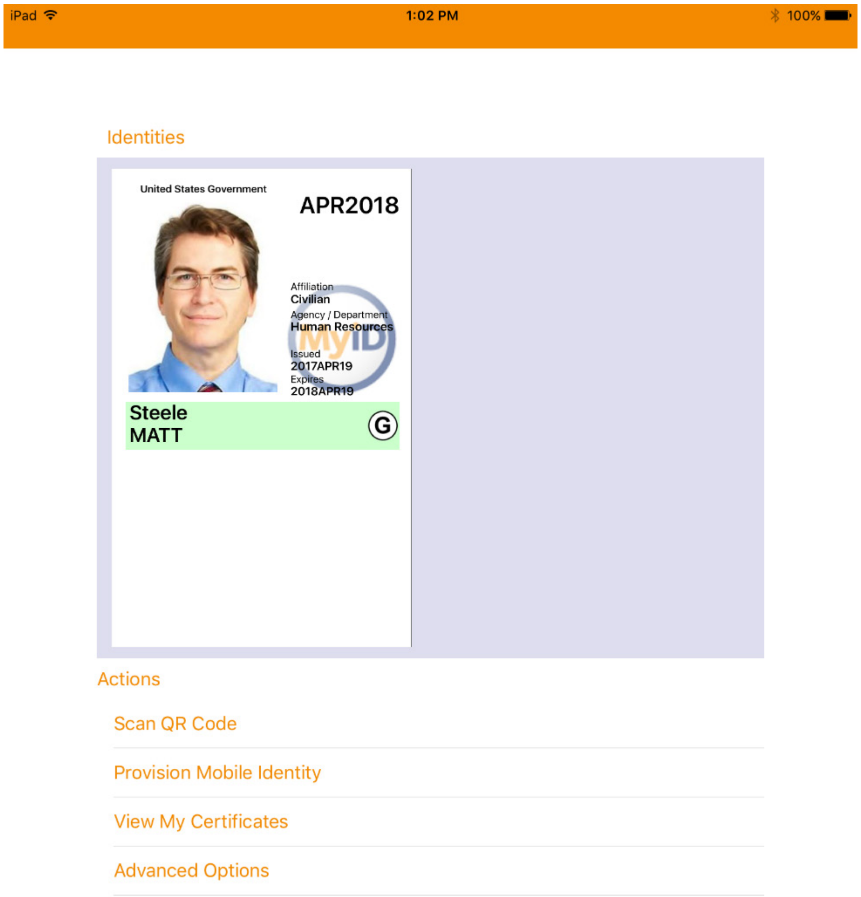
Set PIN

- *PIN must be between 6 and 12 characters*
- *PIN must only contain numbers*

Enter PIN

Confirm PIN

8. If DPC provisioning was successful, the Identities screen will provide a visual representation of information for the DPC Subscriber's linked PIV Card.



United States Government

APR2018

Affiliation
Civilian

Agency / Department
Human Resources

Issued
2017APR19

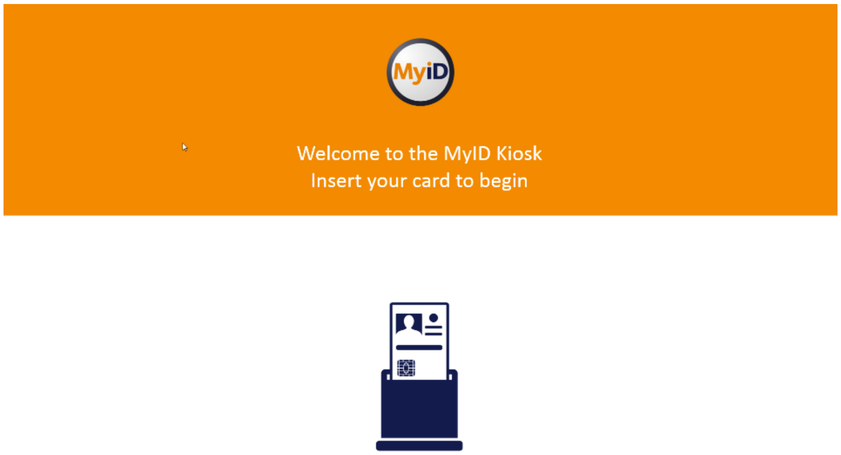
Expires
2018APR19

Steele
MATT

2.2.8.2 Intel Authenticate Issuance Workflow

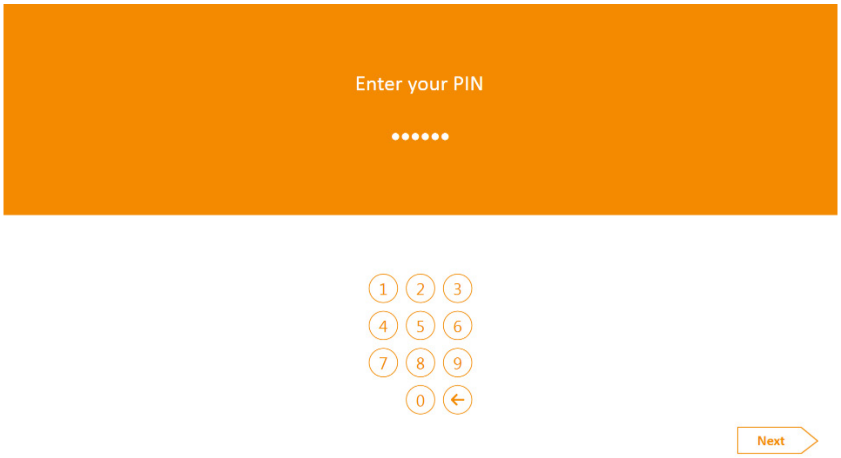
2.2.8.2.1 Requesting a DPC for Intel VSC

1. Go to a **MyID Kiosk**.



Welcome to the MyID Kiosk
Insert your card to begin

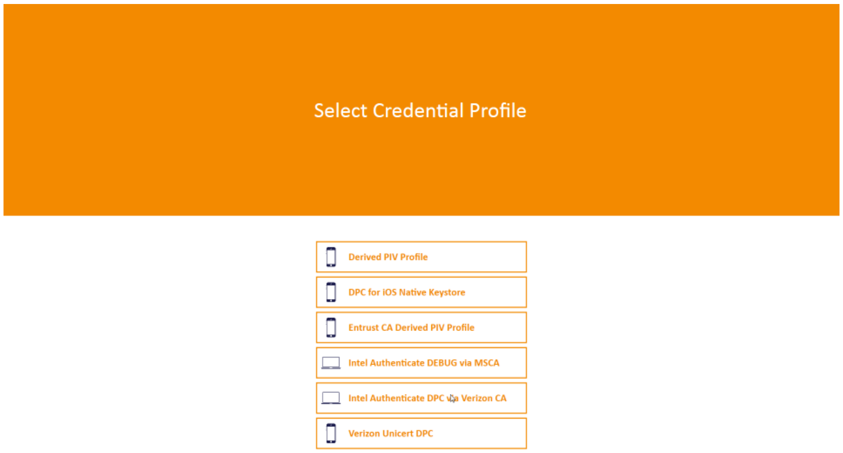
2. Insert a PIV Card.
3. Enter the PIN for the PIV Card.



Enter your PIN

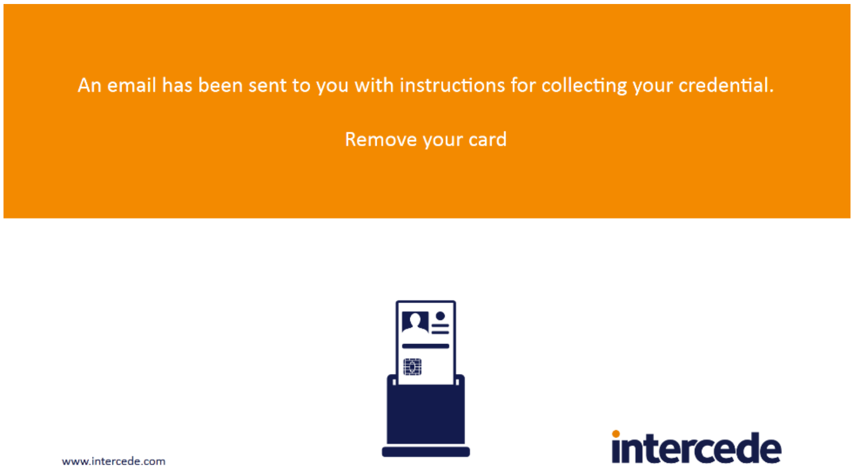
••••••

4. Select the profile created for Derived PIV. An email will be sent to the user with a one-time code for collection.



Select Credential Profile

- Derived PIV Profile
- DPC for iOS Native Keystore
- Entrust CA Derived PIV Profile
- Intel Authenticate DEBUG via MSCA
- Intel Authenticate DPC via Verizon CA
- Verizon Unicert DPC



An email has been sent to you with instructions for collecting your credential.

Remove your card

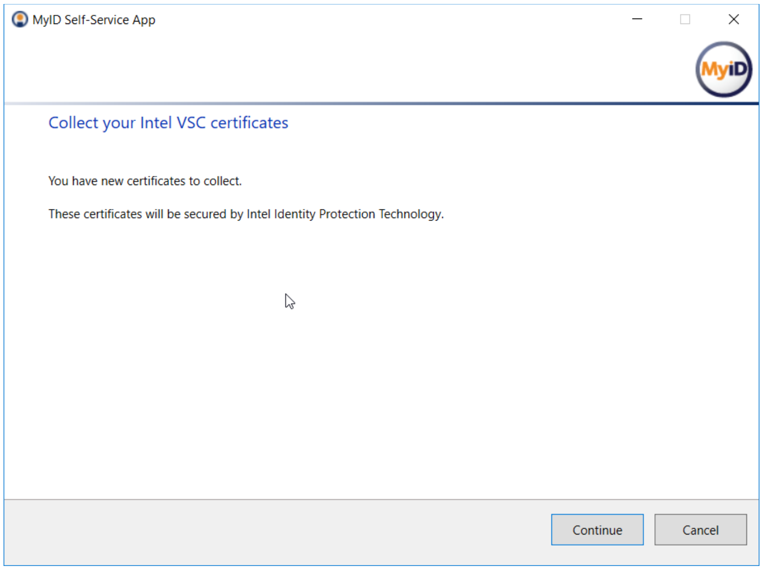
2.2.8.2.2 Collecting the DPC

The following procedures will request and install the DPC in the Intel Authenticate protected token. Note that the DPC will be protected by the enrollment factors set in Section 2.2.5.5.

1. On the client machine, open the MyID Self-Service App with the parameters `/nopopup` and `/iptonly`.

   ```
   $ MyIDApp.exe /nopopup /iptonly
   ```

2. Click **Continue**.

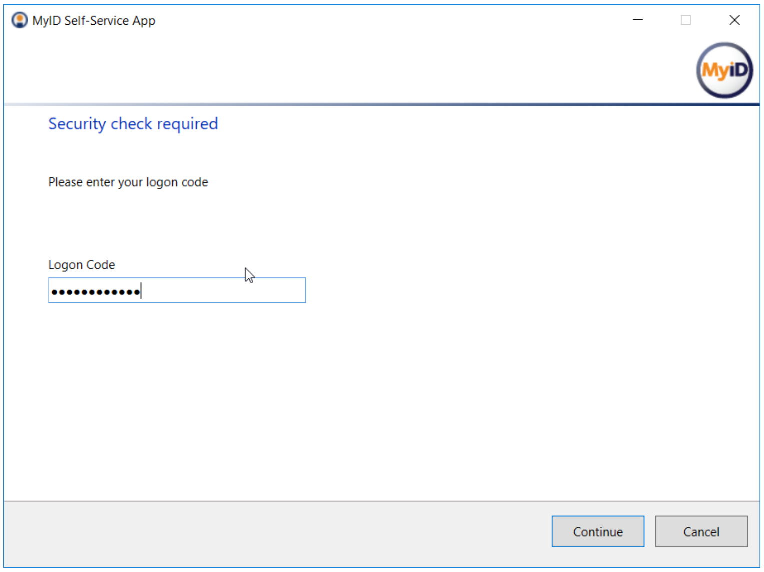

MyID Self-Service App

Collect your Intel VSC certificates

You have new certificates to collect.

These certificates will be secured by Intel Identity Protection Technology.

3. Enter the **Logon Code** from the email.
4. Click **Continue**.

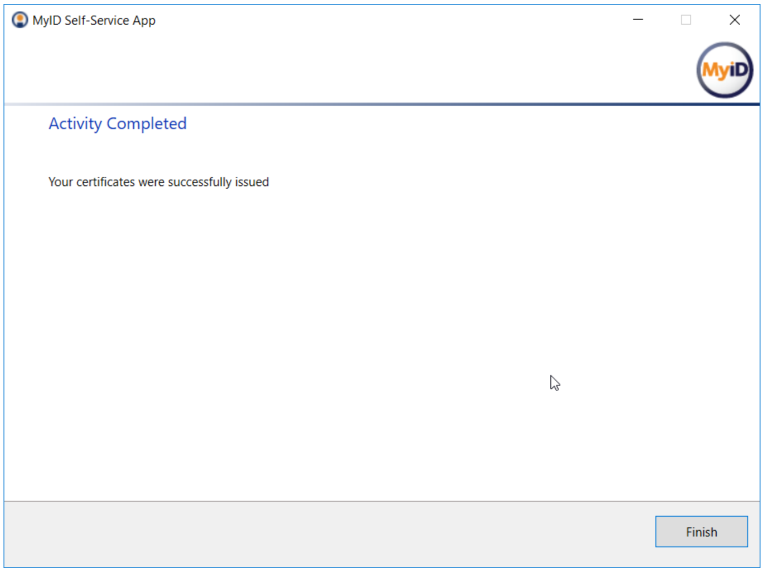

MyID Self-Service App

Security check required

Please enter your logon code

Logon Code: ••••••••••••

5. Click **Finish** after the certificates are successfully collected.



Activity Completed

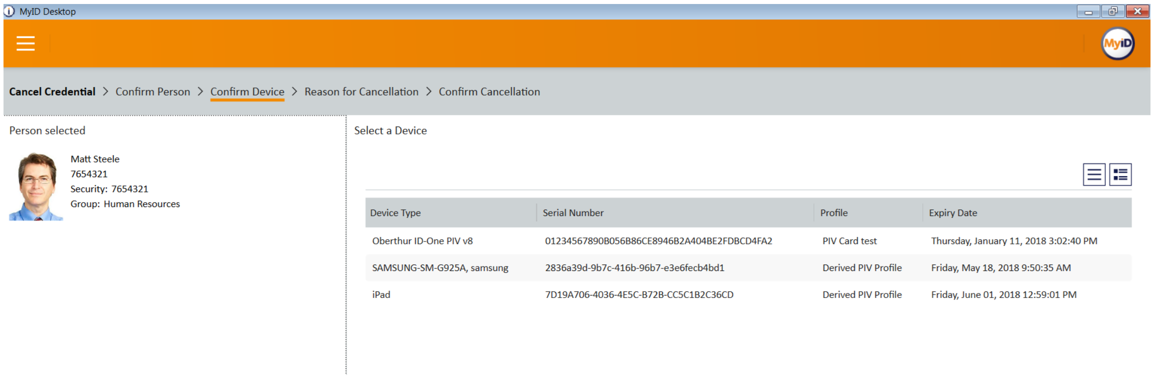
Your certificates were successfully issued

2.2.8.3 Maintenance Workflow

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

2.2.8.4 Termination Workflow

1. Select the target device associated with the DPC subscriber that will be terminated.


MyID Desktop
Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation

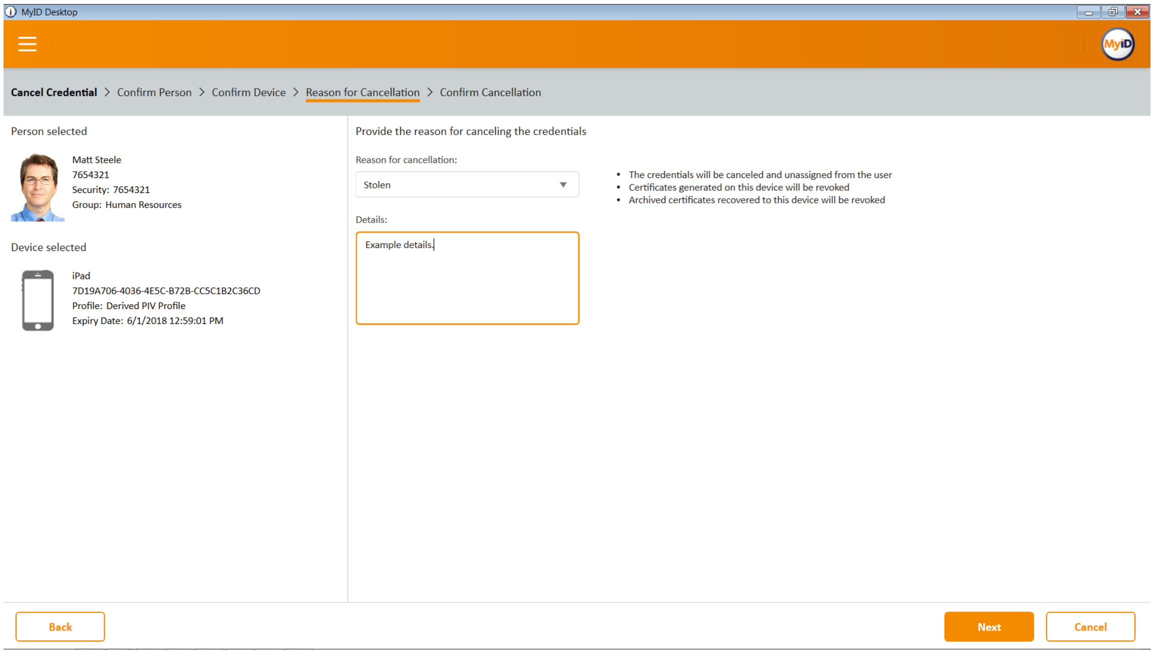
Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Select a Device

Device Type	Serial Number	Profile	Expiry Date
Oberthur ID-One PIV v8	01234567890B056B86CE8946B2A404BE2FDBCD4FA2	PIV Card test	Thursday, January 11, 2018 3:02:40 PM
SAMSUNG-SM-G925A, samsung	2836a39d-9b7c-416b-96b7-e3e6fecb4bd1	Derived PIV Profile	Friday, May 18, 2018 9:50:35 AM
iPad	7D19A706-4036-4E5C-B72B-CC5C1B2C36CD	Derived PIV Profile	Friday, June 01, 2018 12:59:01 PM

2. Select a reason for termination and enter any other required information for policy compliance.


MyID Desktop
Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation
Back
Next
Cancel

Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Device selected

iPad
7D19A706-4036-4E5C-B72B-CC5C1B2C36CD
Profile: Derived PIV Profile
Expiry Date: 6/1/2018 12:59:01 PM

Provide the reason for canceling the credentials

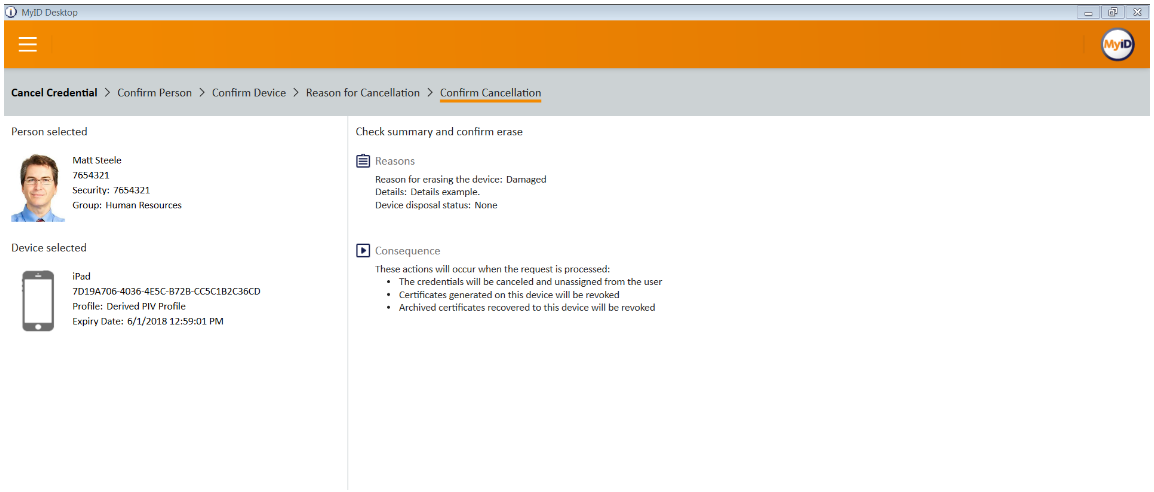
Reason for cancellation: Stolen

Details: Example details.

- The credentials will be canceled and unassigned from the user
- Certificates generated on this device will be revoked
- Archived certificates recovered to this device will be revoked

3. Click **Next**

4. Confirm the termination of the DPC.


MyID Desktop
Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation

Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Device selected

iPad
7D19A706-4036-4E5C-B72B-CC5C1B2C36CD
Profile: Derived PIV Profile
Expiry Date: 6/1/2018 12:59:01 PM

Check summary and confirm erase

Reasons

Reason for erasing the device: Damaged
Details: Details example.
Device disposal status: None

Consequence

These actions will occur when the request is processed:

- The credentials will be canceled and unassigned from the user
- Certificates generated on this device will be revoked
- Archived certificates recovered to this device will be revoked

Appendix A List of Acronyms

AD	Active Directory
CA	Certificate Authority
CAPI	Cryptographic Application Interface
CMS	Credential Management System
CPS	Cryptographic Service Provider
DMZ	Demilitarized Zone
DN	Distinguished Name
DPC	Derived PIV Credential
EMM	Enterprise Mobility Management
FASC-N	Federal Agency Smart Card Number
GPO	Group Policy Object
IDG	Identity Guard
IT	Information Technology
JCE	Java Cryptography Extension
JTK	Java Tool Kit
LDAP	Lightweight Directory Access Protocol
MDAC	Microsoft Data Access Components
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OID	Object Identifier
OS	Operating System
OU	Organizational Unit
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QR	Quick Response [code]
RSA	Rivest-Shamir-Adleman
SCEP	Simple Certificate Enrollment Protocol
SP	Special Publication
SQL	Structured Query Language

SSL	Secure Sockets Layer
SSM	Self-Service Module
SSP	Shared Service Provider
TLS	Transport Layer Security
UPI	UniCERT Programmatic Interface
UPN	User Principal Name
URL	Universal Resource Locator
UUID	Universal Unique Identifier
VLAN	Virtual Local Area Network
VSC	Virtual Smart Card
WMI	Windows Management Instrumentation
WSVC	World Wide Web Publishing Service