

Profile Manager

Workforce Connect



ZEBRA

Imprivata Integration Guide

2023/03/10

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal.

COPYRIGHTS: zebra.com/copyright.

PATENTS: ip.zebra.com.

WARRANTY: zebra.com/warranty.

END USER LICENSE AGREEMENT: zebra.com/eula.

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Imprivata WFC Integration with Active Directory

Workforce Connect uses Active Directory (AD) to authenticate users at sign-on time.

The Imprivata NFC tap-and-go authentication can be integrated with the Profile Manager.

This guide describes configuring Imprivata with the Profile Manager and PTT Pro.

Component Versions

The device and server versions used in this guide are described below. The components can change as software versions are updated.

- Imprivata Mobile Device Access (IMDA) version: Imprivata provides updates on the Google Play Store:
 - Enterprise Customers and Partners may also retrieve the MDA ADB Installation kit from their support site
 - IMDA version 7.9
- Workforce Connect Profile Client version 2.0.20406 or later
- Workforce Connect PTT Pro version 3.3.10166 or later
- Imprivata Server:
 - The Zebra Engineering server is kept up to date with the latest Imprivata images
 - Version 7.7 build 7.7.001.12
- Workforce Connect Profile Manager server version 1.19.37 or later
- Workforce Connect PTT Pro server version 4.9 or later

NFC Card Specifications

The Imprivata system supports tap-and-go NFC card technology. Use Imprivata cards when available.

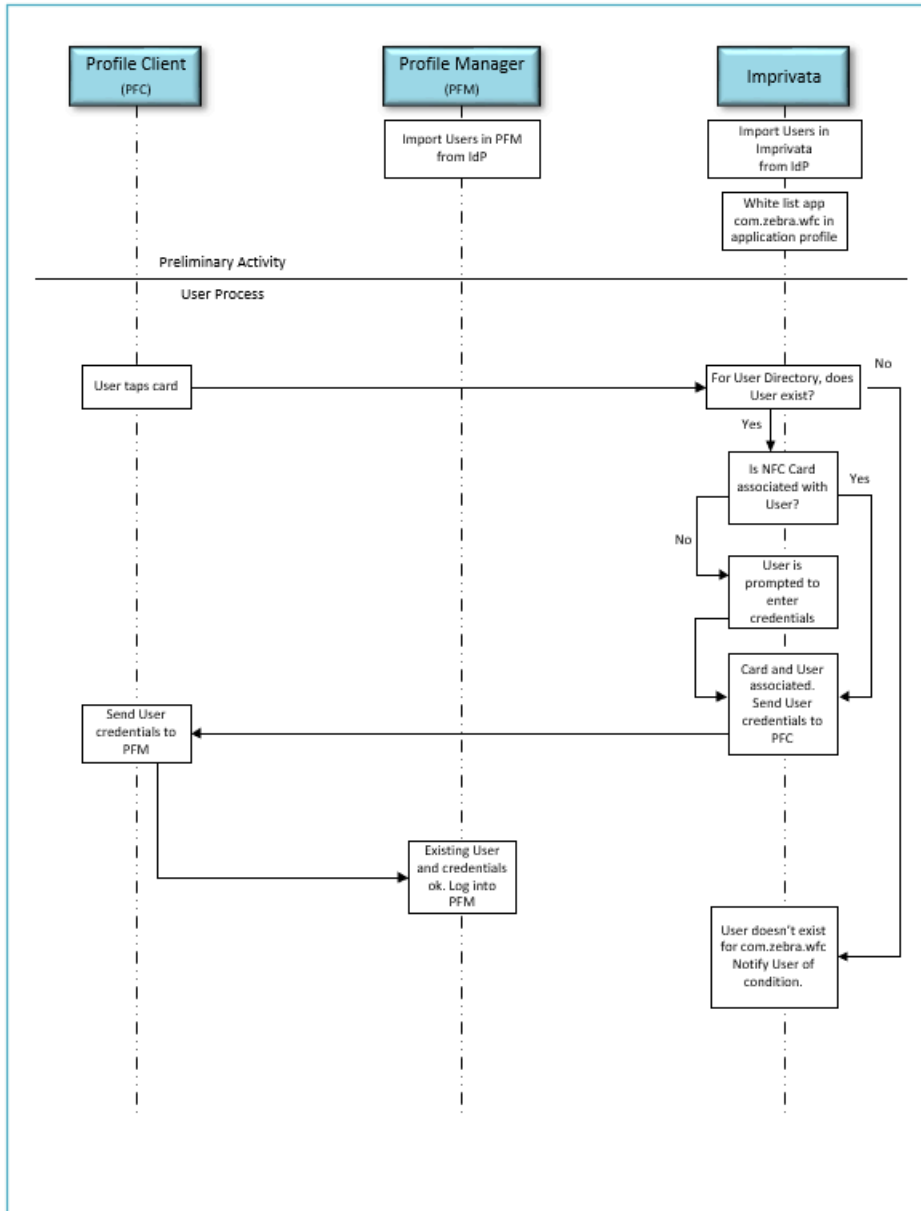
The following cards work successfully:

- Card Type: Mifare / NXP Mifare Ultralight
- Model: 13.56 MHz
- ISO: 14443-3A, or 15693

NFC Card Activation and User Association

The diagram illustrates the sequence of events and interaction of the Profile Client, Profile Manager, and Imprivata server for associating the NFC Card to the user and standard user login.

Figure 1 NFC Card Activation and User Association



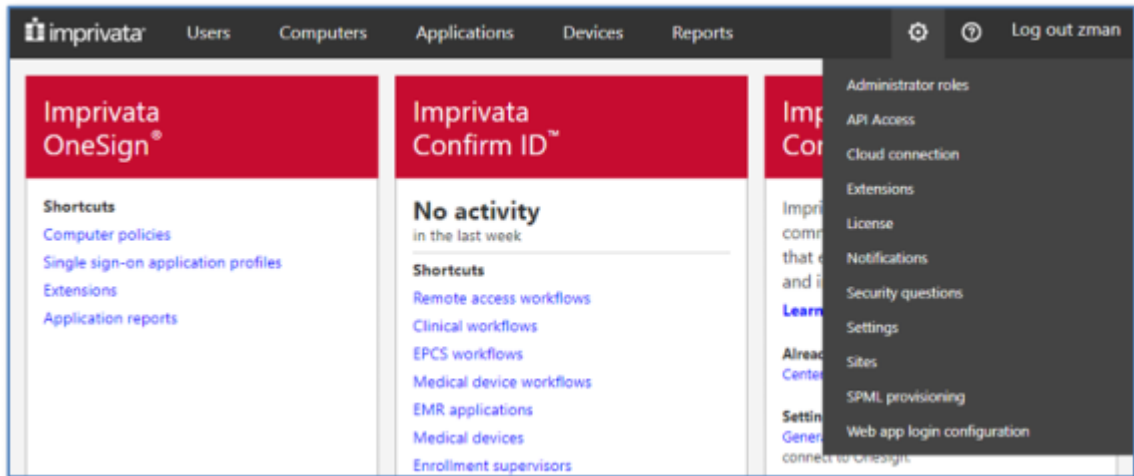
Imprivata Server Configuration

This section highlights the elements required to prepare a system to support Zebra devices. It is not an exhaustive server configuration tutorial.

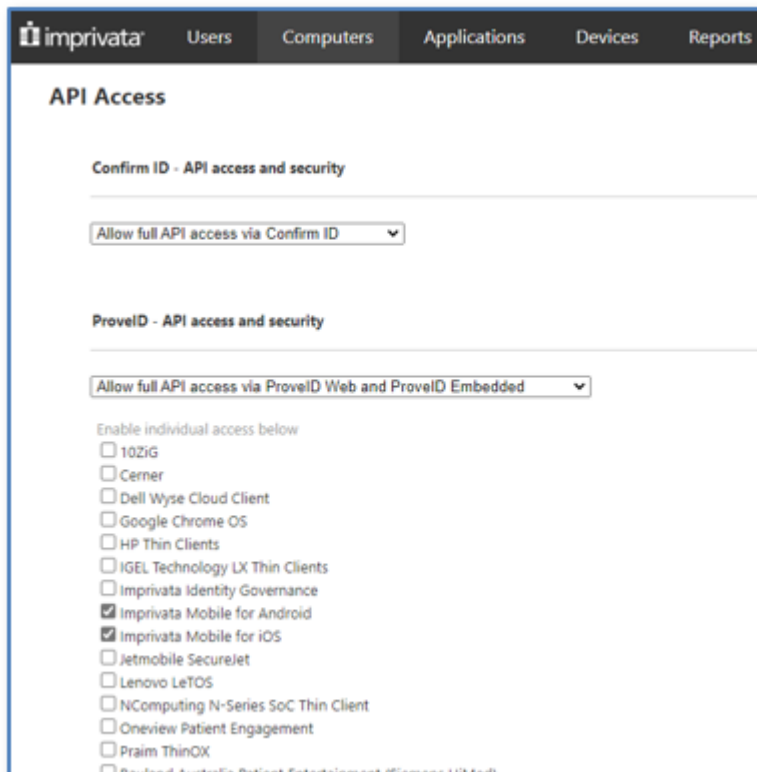
API Access

API access must be enabled for the IMDA to pass credentials to the WFC Profile client. If API access is not enabled, the IMDA generates the `Invalid Mode` error when the card is tapped, and credentials are not passed to the Profile Client.

1. Navigate to **Platform Settings > API Access**.



2. Select the **Imprivata Mobile for Android** and **Imprivata Mobile for iOS** checkboxes in the **ProveID** section.



3. Save the settings.

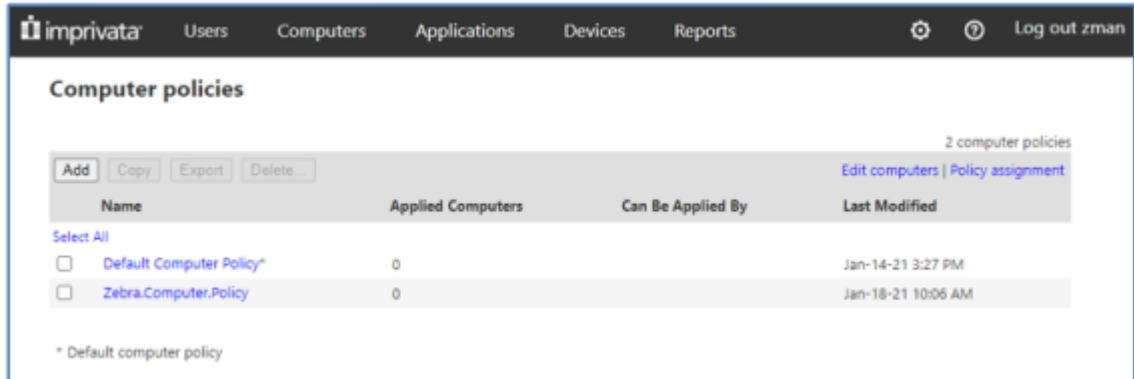
Edit or Create a Computer Policy

Assign a Computer Policy to each user. The assignment is done automatically when the User Import from AD occurs.

Generally, one policy is acceptable for all users. The policy is assigned at User Import and can be changed in each user's profile.

If a PC client is setup for Imprivata One-Sign, then additional attributes are required. For mobile devices, the only change to the default configuration is to enable Device Logging.

1. Click **Computers > Computer Policy**.



2. Select **Yes** for **Enable Agent Logging** for mobile devices.

The screenshot shows a configuration window with the following elements:

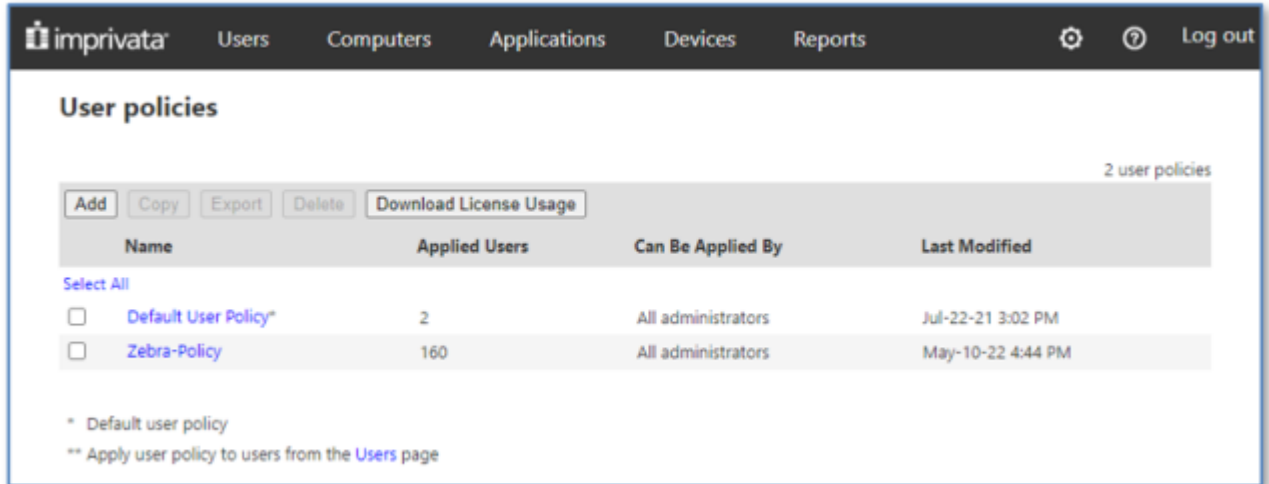
- Configuration 3:** A dropdown menu set to "None" with an information icon (i) to its right.
- Configuration 4:** A dropdown menu set to "None" with an information icon (i) to its right.
- HID card readers:** A section with the text "These settings apply exclusively to HID card readers" and two unchecked checkboxes:
 - Enable legacy mode for HID card readers
 - Program HID 5x27 card reader configurations
- Smart card readers:** A section with one unchecked checkbox:
 - Treat smart card authentications as proximity card authenticationsBelow this checkbox is a blue link labeled "Learn more".
- Agent logging:** A section with the following controls:
 - Enable Agent Logging?** Radio buttons for "Yes" (selected) and "No".
 - Maximum File Size:** A text input field containing "100" followed by the label "Megabytes".
 - Buttons:** "Cancel" and "Save" buttons at the bottom right.

3. Click **Save**.

Edit or Create the User Policy

The user policy is assigned when the user is imported and synchronized.

1. Click **User > User Policy** to add a new policy or edit an existing policy.



2. Add a new policy or edit an existing policy.

The policy options display on the following screens.

3. Select the **Let all administrators apply this policy** and **Password** checkboxes under **Primary Factors**.

User policies - Edit Zebra-Policy

Back to [All User Policies](#) Cancel Save

All users in this policy use the following licenses: Authentication Management and Self-Service Password Reset. Find Applied Users

Policy name: Policy ID: 020A07D7-9EB8-4AF4-8A07-D79EB81AF414

Let all administrators apply this policy

Authentication | Challenges | Self-Service Password/Imprivata PIN Reset | Single Sign-On | Virtual Desktops

Licensed options

- Fingerprint Identification
- Hands Free Authentication
- Imprivata ID for Windows Access

Walk-away security

Provide increased walk-away security using Imprivata ID for presence detection on eligible workstations.

- Allow Secure Walk Away
Requires enrolled Imprivata ID.

Desktop Access authentication

Choose the authentication methods allowed for desktop access.

- Allow offline authentication
- Show greeting notification balloon when users log in

Primary factors

- Password
- Fingerprint

Second factors

- No second factor
- Imprivata ID
- No second factor
- Password
- Imprivata PIN

4. Select the **Proximity Card** checkbox.

Proximity Card No second factor
 Password
 Imprivata PIN
 Fingerprint
 Fingerprint or Password
 Fingerprint or Imprivata PIN

Smart Card or USB token using Active Directory certificate

Choose a keytab file...

Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication

Password No second factor
 Built-in proximity card Password
 Imprivata PIN
 Fingerprint
 Fingerprint or Password
 Fingerprint or Imprivata PIN

Allow use of conditional primary methods for:
[0] : [0]
(0-23 hours) (0-59 minutes)

Smart Card or USB token using external certificate

Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication

Password No second factor
 Built-in proximity card Password
 Imprivata PIN
 Fingerprint
 Fingerprint or Password
 Fingerprint or Imprivata PIN

Allow use of conditional primary methods for:
[0] : [0]
(0-23 hours) (0-59 minutes)

ID token (requires external ID token server)

VASCO OTP token ⓘ

Require password for tokens that do not have a PIN

Answer security questions [View and modify security questions](#)

5. Click **Save**.

The screenshot shows a configuration window titled "Fingerprint" with the following settings:

- Number of sequential failed fingerprint authentication attempts before authentication failure:** 2
- Maximum allowed enrolled fingers:** 2
- Allow users to manage fingerprints**
- VASCO OTP token:**
 - Allow users to enroll VASCO OTP tokens
 - Lock computer if user cancels enrollment
 - Allow Offline Authentication with VASCO OTP token
 - Offline data lifespan:** 14 (1 - 21) days
- Smart card using external certificate:**
 - Allow smart card enrollment and authentication only while certificate is valid

Buttons: **Cancel** and **Save**

Edit or Create the Mobile Device Access Policy

Create a policy to control the behavior of client devices.

1. Select **Computers > Mobile Policy** from the toolbar.

2. Select the **Allow guest mode** checkbox under **Access Management**.

This option allows the user to exit from the IMDA launcher in guest mode without signing in.

Mobile Device Access policy Cancel Save

Access Management

- Allow guest mode**
Provides users with access to an unlocked device without enabling single sign-on capabilities.
- Automatically log out a user**
Set time to log out a user after a period of inactivity.
0 : 30
(0-24 hours) (0-59 minutes)
- Inactivity re-authentication**
Set time to force user to re-authenticate after a period of inactivity.
0 : 30
(0-24 hours) (0-59 minutes)
- Turn on grace period for second authentication factor**
Grace period allows you to not have to enter the second authentication factor for a specified time period.
0 : 0
(0-24 hours) (0-59 minutes)
- Unlock with Imprivata PIN instead of proximity card**
Allows you to use Imprivata PIN to unlock screen for a specified time period after using password as primary factor.
0 : 1
(0-24 hours) (0-59 minutes)

Web Browser Management
When a user logs out, or a user switch is initiated, all open browsers will be automatically closed.

3. Select **Do nothing** under **Web Browser Management**.

Web Browser Management

When a user logs out, or a user switch is initiated, all open browsers will be automatically closed.

Advanced user data clearing
Additional action that can be enabled to ensure all prior user data is removed.

Do nothing

Force stop all browsers

Clear cache on all browsers

Clear data on all browsers

Authentication

Validate stored domain credentials before authenticating
Applies only to non-password authentication methods.

Customization

Select Language:

Allow lock screen notifications
Notifications from other apps will be displayed on the Imprivata Mobile for Android lock screen.
Caution: Notifications may contain sensitive content, such as PHI or private data, and can be read while the device is locked.

Voice call (VoIP) apps (authentication not required to answer call)

List all allowed app packages, comma-separated.

Voice call (VoIP) apps (authentication required to answer call)

List all allowed app packages, comma-separated.

Messaging and other apps

List all allowed app packages, comma-separated.

Allow floating Home button
Applicable for Workspace ONE Launcher configuration.

4. Under the **Authentication** section deselect **Validate stored domain credentials before authenticating**.

5. Select **Allow lock screen customizations** under **Customization**.

Enabling this option enables Workforce Connect notifications to display on the lock screen.

6. Enter the Workforce Connect package name, `com.symbol.wfc.voice`, in the following fields.
 - **Voice call (VoIP) apps (authentication not required to answer call)**
 - **Voice call (VoIP) apps (authentication required to answer call)**
 - **Messaging and other apps**
7. Click **Save**.

Create an Imprivata Directory

Create an Imprivata directory to import users into a unique container within the Imprivata server.

Complete the following steps:

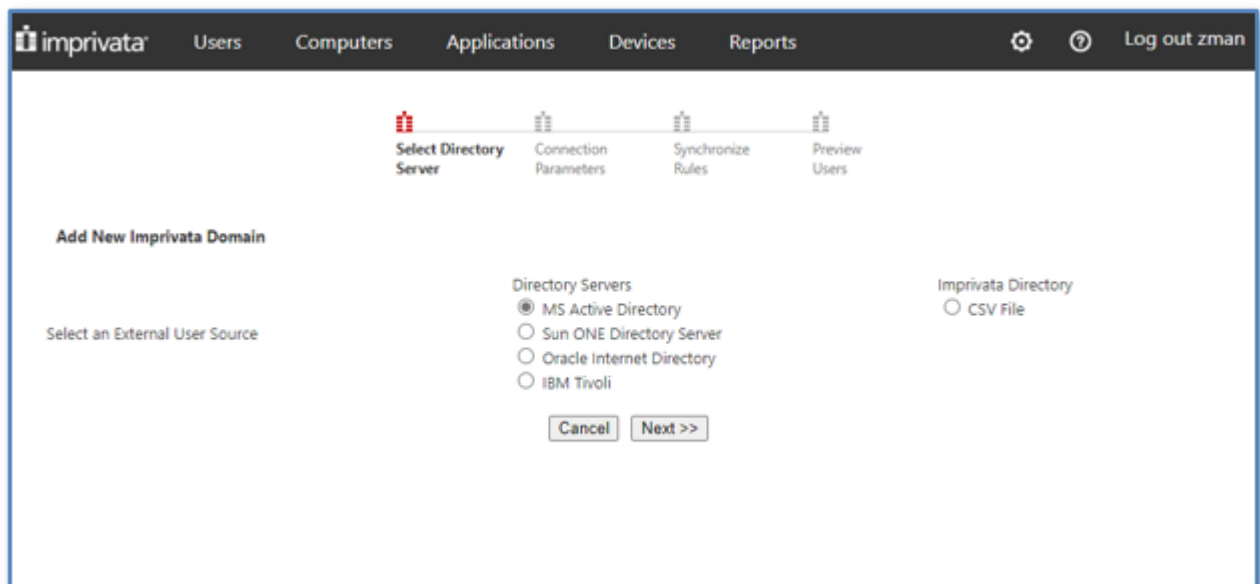
- Create the Imprivata Directory.
- Specify the group of users to import.
- Define synchronization rules.

Users are imported, the application policy is applied, and users are enabled after you complete these steps.

Add a Directory

Create an Imprivata directory by identifying the Active Directory host.

1. Select **Users** > **Directories** from the Imprivata console.



2. Select **MS Active Directory** and click **Next**.

3. Configure the Imprivata Domain to create a new user authentication directory.

The screenshot shows the 'Add New Imprivata Domain' configuration page in the Imprivata web interface. The page has a dark header with the Imprivata logo and navigation tabs: Users, Computers, Applications, Devices, and Reports. On the right side, there are four icons with labels: Select Directory Server, Connection Parameters (highlighted in red), Synchronize Rules, and Preview Users. The main content area is titled 'Add New Imprivata Domain' and contains the following fields and options:

- Domain name:** A text input field with the placeholder text '<enter your domain>'.
Host name: A text input field with the placeholder text '<use dns or IP>'.
Username: A text input field with the placeholder text '<enter valid existing user ID>'.
NetBIOS name: A text input field with a blue 'Look-up' link to its right.
Password: A password input field with masked characters (dots).
- Use TLS for secure communication**
Directory server certificate (1 certificate)
Browse... Upload
- Validate stored domain credentials before authenticating**
Applies only to non-password authentication methods
- Kerberos authentication**
Upload the keytab file if using smart cards with Active Directory certificates or authenticating with Kerberos.
Keytab file (No keytab files)
Browse... Upload

At the bottom right, there are four buttons: Cancel, << Back, Save, and Synchronize Users >>.

- a) Enter the domain name used for the AD server configuration in the **Domain name** field.
- b) Enter the hostname or IP address of the AD server, not the ADFS server, in the **Host name** field.
- c) Enter a valid username in the **Username** field.
- d) Enter a password in the **Password** field.
This user must have permission for AD validation.
- e) Leave the NetBIOS name field blank.
- f) Deselect the **Use TLS for secure communication** if the AD server does not support TLS.
- g) Click the **Look-up** link above the **NetBIOS name** field.

If the information is valid, the NetBIOS name is populated. If the NetBIOS name does not appear then a firewall may be blocking access to the AD server, or the user credentials are invalid.

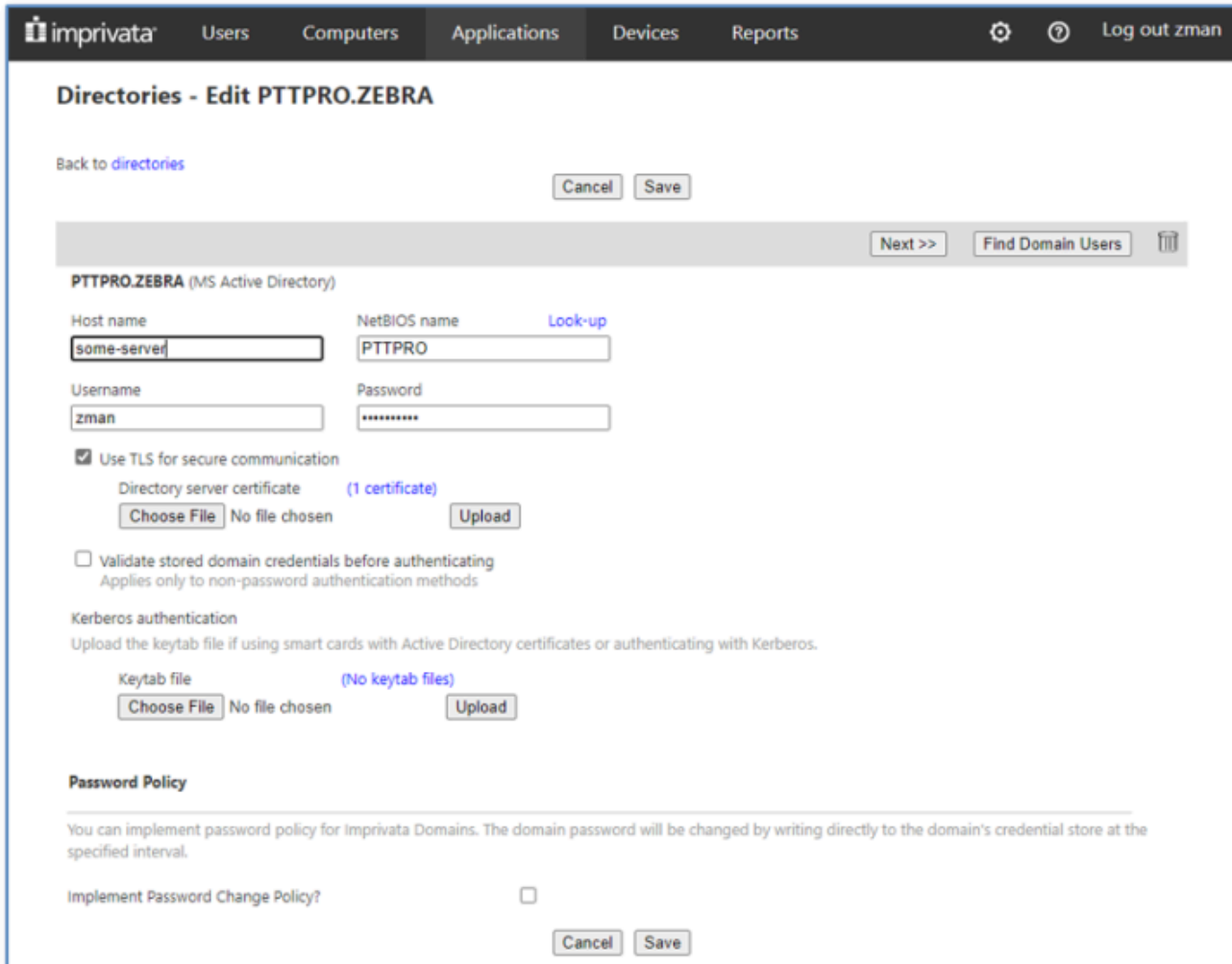
4. Click **Save**.



The screenshot shows the 'Directories' page in the Imprivata interface. It features a table with columns for 'Imprivata Domain', 'Type', 'Total Users', 'Enrolled Users', 'Last Synchronized', and 'Next Synchronization'. There are two entries: 'PTTPRO.ZEBRA' (MS Active Directory) and 'wfc.zebra.com' (Imprivata Directory). An 'Add' button is visible at the top left of the table area.

Imprivata Domain	Type	Total Users	Enrolled Users	Last Synchronized	Next Synchronization
PTTPRO.ZEBRA	MS Active Directory	3	0	Jul-23-20 3:11 PM	Not Scheduled
wfc.zebra.com	Imprivata Directory	30	22		Not Scheduled

5. Select the new directory to advance to the next configuration step and identify users to import.



The screenshot shows the 'Directories - Edit PTTPRO.ZEBRA' configuration page. It includes a navigation bar with 'Users', 'Computers', 'Applications', 'Devices', and 'Reports'. The page title is 'Directories - Edit PTTPRO.ZEBRA'. Below the title, there are buttons for 'Cancel', 'Save', 'Next >>', and 'Find Domain Users'. The main configuration area is for 'PTTPRO.ZEBRA (MS Active Directory)'. It contains fields for 'Host name' (some-server), 'NetBIOS name' (PTTPRO), 'Username' (zman), and 'Password' (masked with asterisks). There is a checked checkbox for 'Use TLS for secure communication' and a file upload section for 'Directory server certificate' (1 certificate) with a 'Choose File' button and 'No file chosen' text. Below that is an unchecked checkbox for 'Validate stored domain credentials before authenticating'. There is also a section for 'Kerberos authentication' with a 'Keytab file' upload section. At the bottom, there is a 'Password Policy' section with a checkbox for 'Implement Password Change Policy?'. 'Cancel' and 'Save' buttons are at the bottom right.

Identify Users to Import

Identify users to import. You can import entire domains, specific OUs, or groups. Consider creating an organizational unit (OU) in AD that includes the users who will use the system.

- Select a method to import users.
 - All users in this domain.
 - Only users in select organizational units.
 - Only users in select groups.

Synchronize users from PTTPRO.ZEBRA

All users in this domain

Only users in select organizational units (0 OUs selected) [Select OUs...](#)

Only users in select groups

- Typical user synchronization (1 group selected) [Select groups...](#)
Synchronize the entire domain structure, including the structure you have not selected.
- Limited user synchronization (0 group selected) [Select groups...](#)
For enterprises with exceptionally large domain structures, limits the domain synchronization to only the groups selected here.

Synchronization settings

These settings are applied to existing users at each synchronization.

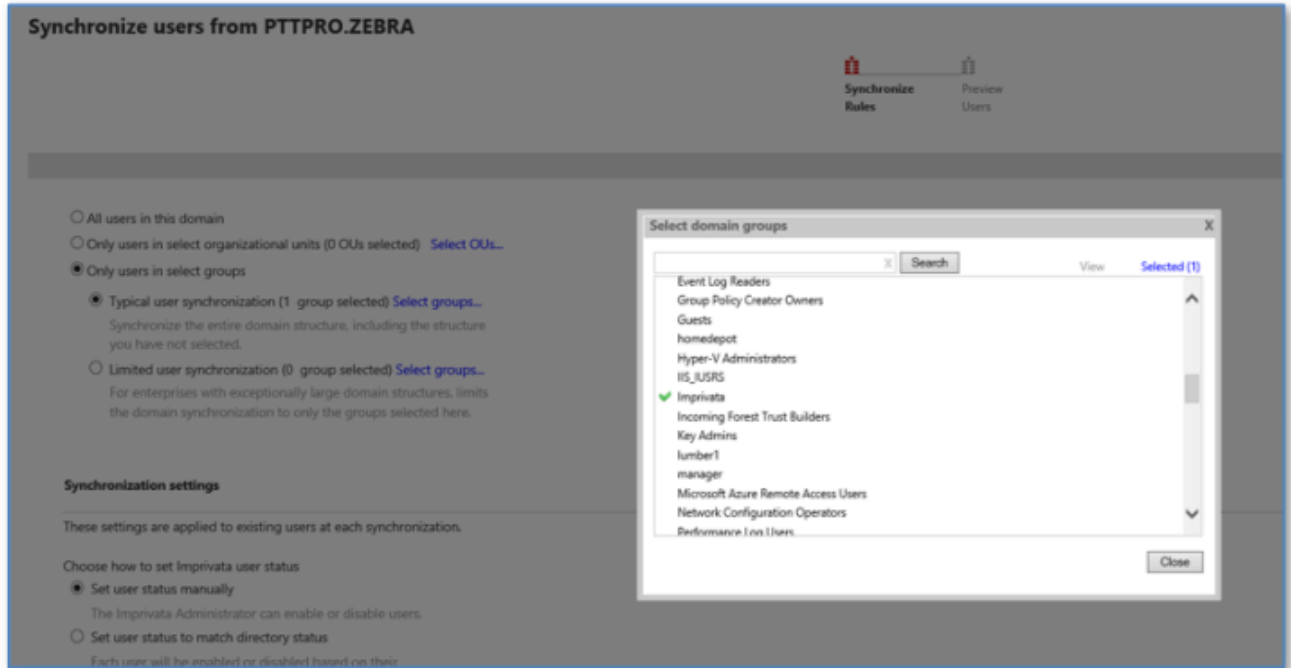
Choose how to set Imprivata user status

Set user status manually
The Imprivata Administrator can enable or disable users.

Set user status to match directory status
Each user will be enabled or disabled based on their directory status and updated automatically.

New Imprivata user settings

Only import users who use Workforce Connect. You can define a specific Group OU to identify these users. In this example , **Only users in select groups** is selected and the **Select domain groups** dialog displays.



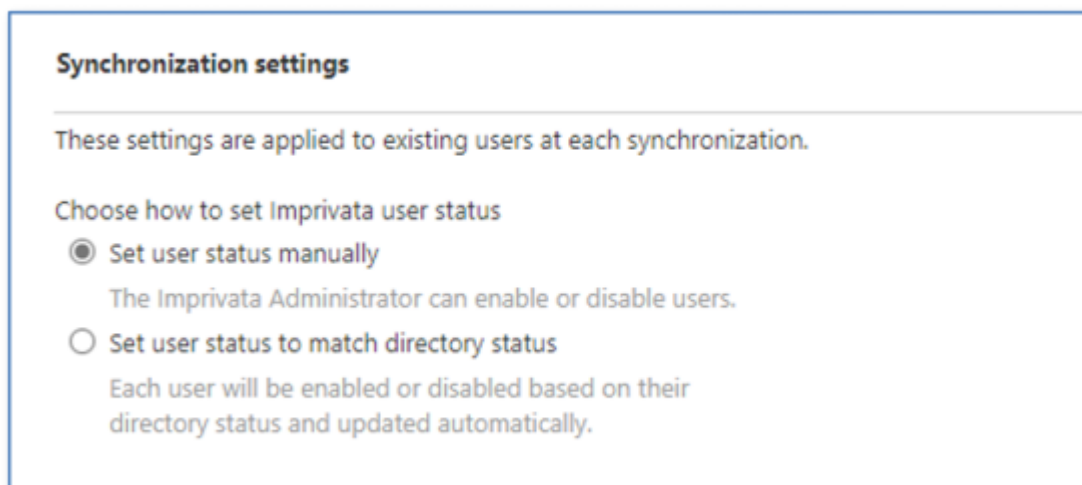
The Imprivata group is selected. This group includes Active Directory users identified as Workforce Connect users.

Synchronize Users

Synchronize the Imprivata server to apply the mobile device access policy after you create the Imprivata Directory and identify the group of users to import.

1. Select a method for setting Imprivata user status.

- Set user status manually.
- Set user status to match directory status.



2. Select the policy to assign to new Imprivata users.

New Imprivata user settings

These settings are applied only to users that are added during synchronization

Choose a policy to be assigned to all new Imprivata users

Zebra-Imp User Policy

Choose the status for new Imprivata users:

Disable new users
New users are initially disabled

Enable new users
New users are initially enabled

Automatically create an email address for each new user

Extended User Attributes

You can specify additional Extended User Attributes to import from the directory server in order to help identify users. Type in the Extended User Attribute name.

Note: Be sure to check the Extended User Attribute name. If it is incorrect, then the attribute value cannot be imported. You will be notified through the system logs.

Automate Synchronization Process

You can automate the synchronization process at a scheduled interval if desired. You may choose not to proceed with the scheduled job.

Automate Synchronization?

3. Select **Enable new users** to apply the user policy.
4. Select the **Automate Synchronization** checkbox.

5. Choose the synchronization configuration.

Automate Synchronization Process

You can automate the synchronization process at a scheduled interval if desired. You may choose not to proceed with the scheduled job if a specified number of users or more will be deleted. Set up a notification for scheduled synchronization if you wish to receive an email when the job runs.

Automate Synchronization?

Do not Synchronize if Users are to be Deleted? Only if the number of users to be deleted exceeds
[Set up event notification?](#)

Synchronize at

Choose the site that performs automated synchronization

6. Click **Save**.
7. Click **Preview Users** to view the user search and the list of users that match the import criteria.

Users Computers Applications Devices Reports

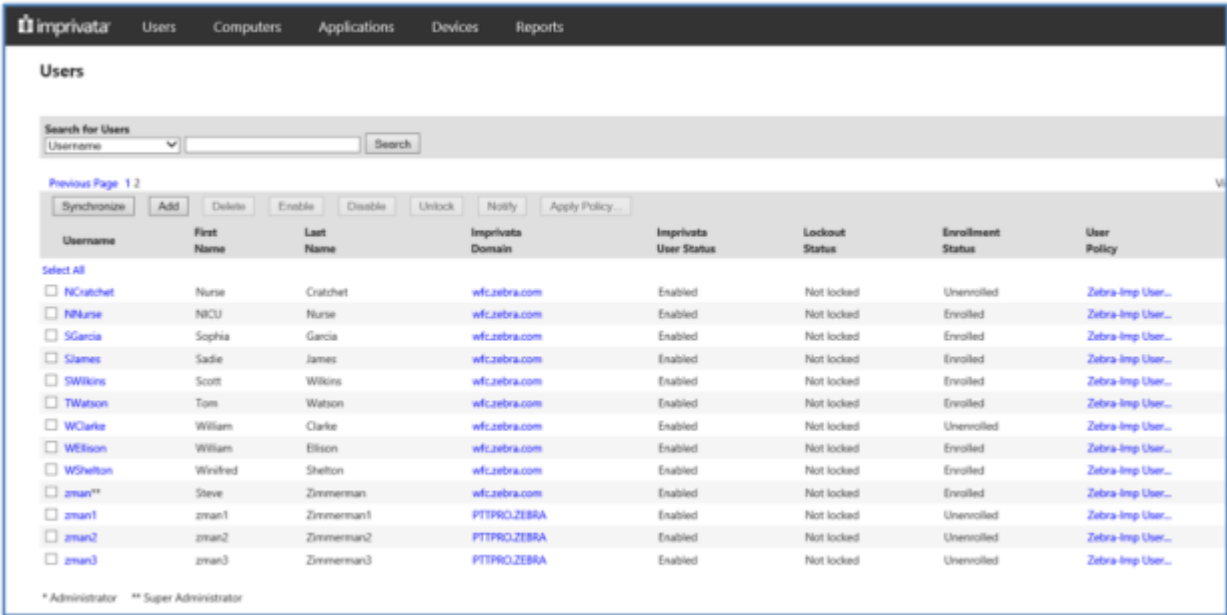
Synchronize users from PTTPRO.ZEBRA

Synchronize Rules
 Preview Users

Users To Be Added
Users To Be Removed

Username	First Name	Last Name
zman1	zman1	Zimmerman1
zman2	zman2	Zimmerman2
zman3	zman3	Zimmerman3

8. Click **Synchronize Now** to add the users to Imprivata.

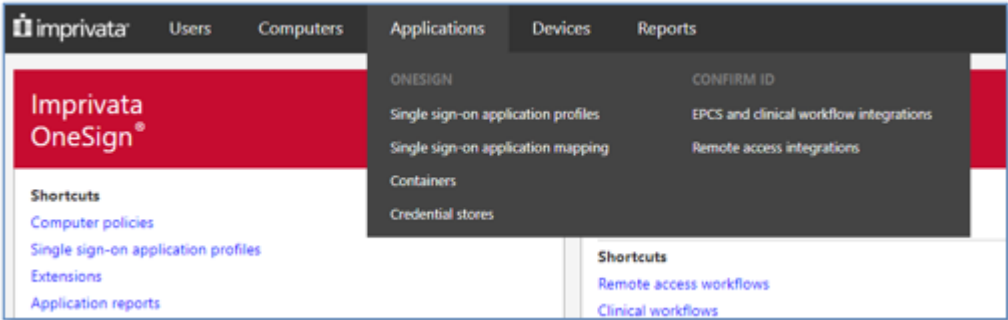


The first time a user taps their badge, they may be prompted for their user name and password to register their card with the system.

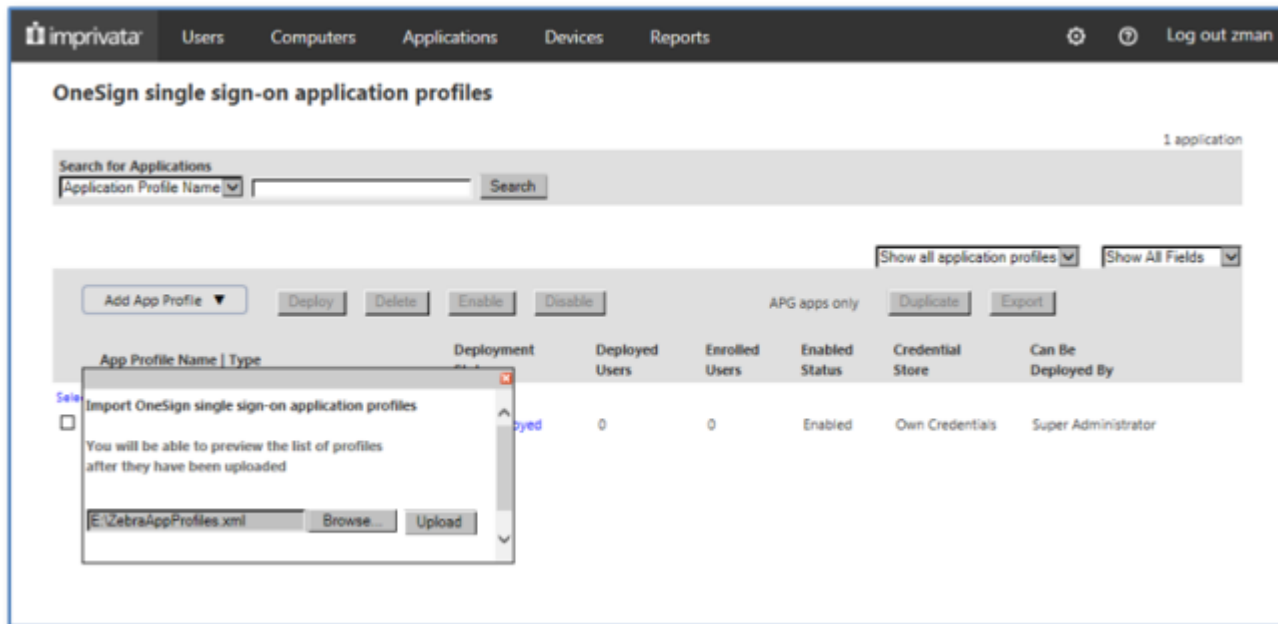
Import the Profile Client Profile

The application profile instructs the identity provider to share credentials with the Profile Client service, com.zebra.dfs. The XML elements shown in the example should not be modified unless instructed by Imprivata Tech Support.

1. Navigate to **Applications > Single sign-on application profiles**.



2. Click **Add App Profile** and click **Browse** to import the `ZebraAppProfiles.xml` file.



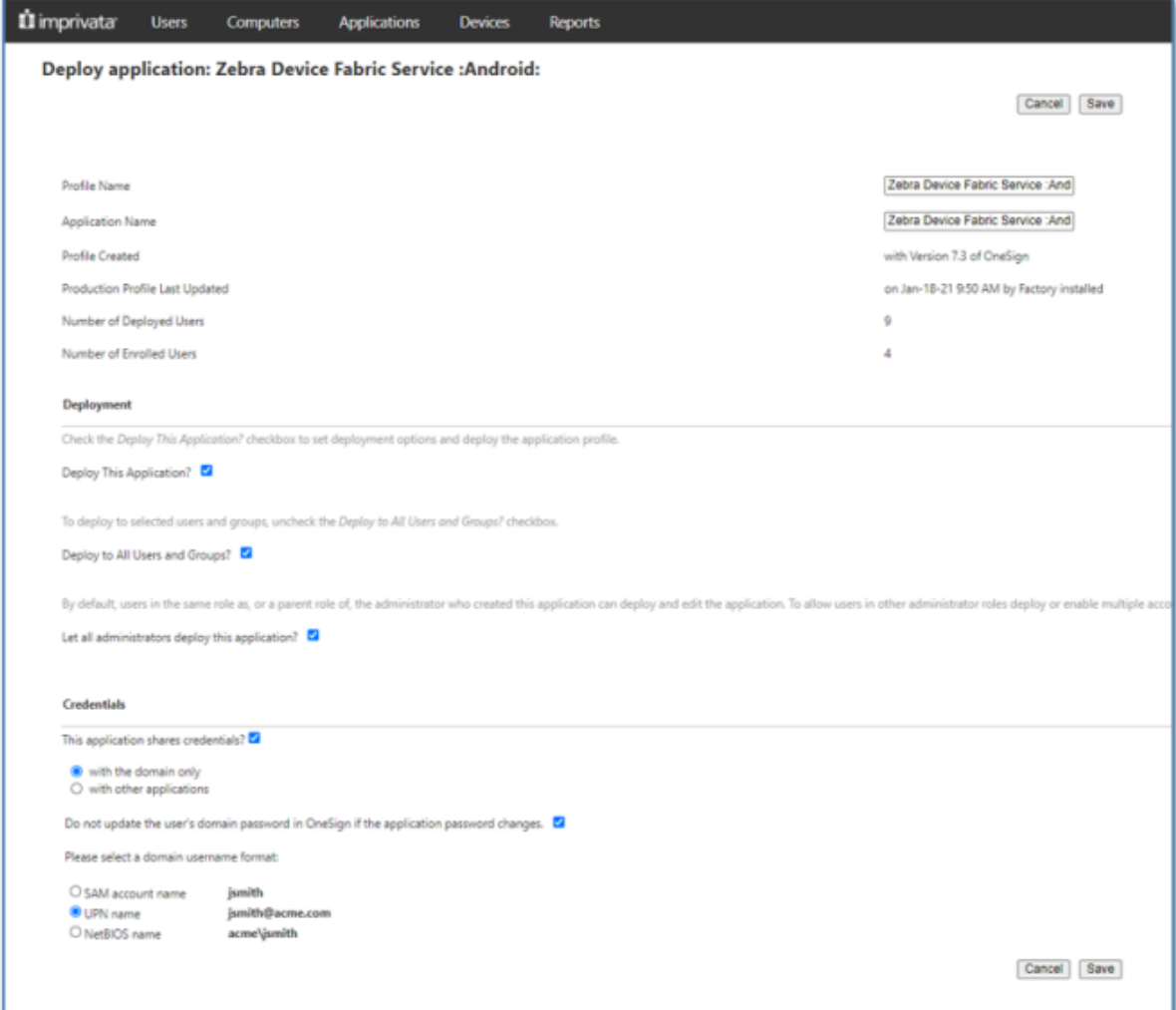
Refer to [Zebra Application Profile](#) for the contents of `ZebraAppProfiles.xml`.

After you import the application profile, the file is listed in the **App Profile Name** column with a deployment status of Not Deployed.

3. Click the **Not Deployed** link to edit the profile and verify the **Deployment** settings.

The following settings must be enabled:

- **Deploy This Application?**
- **Deploy All Users and Groups?**
- **Let all administrators deploy this application?**



The screenshot shows the 'Deploy application: Zebra Device Fabric Service :Android:' configuration page in the Imprivata Profile Manager. The page is divided into several sections:

- Profile Information:** Profile Name, Application Name, Profile Created, Production Profile Last Updated, Number of Deployed Users, and Number of Enrolled Users.
- Deployment:** Contains three checkboxes: 'Deploy This Application?' (checked), 'Deploy to All Users and Groups?' (checked), and 'Let all administrators deploy this application?' (checked).
- Credentials:** Contains three checkboxes: 'This application shares credentials?' (checked), 'Do not update the user's domain password in OneSign if the application password changes.' (checked), and a domain username format selection (UPN name selected).

4. Verify the **Credentials** settings.

The following settings must be enabled:

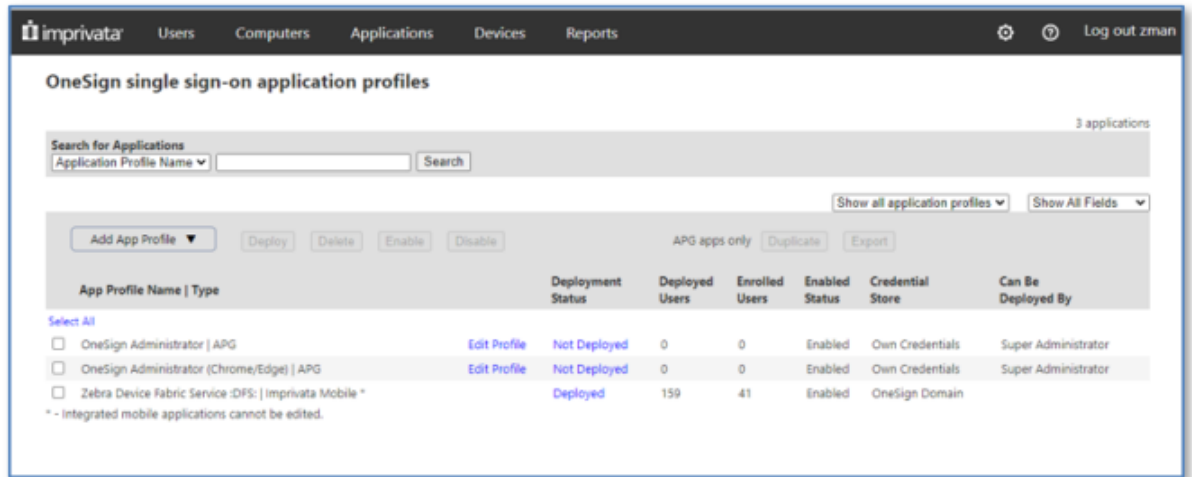
- **This application shares credentials?**
 - **with the domain only**
 - **Do not update the user's domain password in OneSign if the application's password changes.**

5. Select the domain user name format.



NOTE: Profile Manager implementations use UPN format, but there are exceptions.

6. Click **Save**.



The **OneSign single sign-on application profiles** screen displays the deployed profile and lists the number of Deployed Users and the number of Enrolled Users.

Zebra Application Profile

The application profile is an XML file that instructs the IMDA to share credentials with the `com.zebra.dfs` Profile Client service. Do not modify the XML elements of this file unless instructed by Imprivata Tech Support.

The name of the application profile for Zebra devices is `ZebraAppProfiles.xml`.

```
<app desc="Zebra Device Fabric Service :Android:" nm="com.zebra.dfs"
profileType="2" appType="2">
  <env nm="Android" type="100">
    <scn auto="0" dgs="1" nm="">
      <ctl cls="" nm="noAutofill" var="USR"/>
      <ctl cls="" nm="noAutofill" var="PWD"/>
    </scn>
  </env>
```


</app>

Table 1 Application Profile Parameters

Required Parameters	Values
profileType	<ul style="list-style-type: none"> • 0 = OneSign • 1 = Patient Secure • 2 = IMDA <p>A value of 2 is required.</p>
appType	<ul style="list-style-type: none"> • 0 = native • 1 = web • 2 = integrated <p>A value of 2 is required.</p>

Configure the Clients and Profile Manager

Configure the client applications and the Profile Manager (PFM) after configuring the Imprivata server. The client applications include the Imprivata client and the Profile Client.

Configuring the Imprivata Mobile Device Access Client

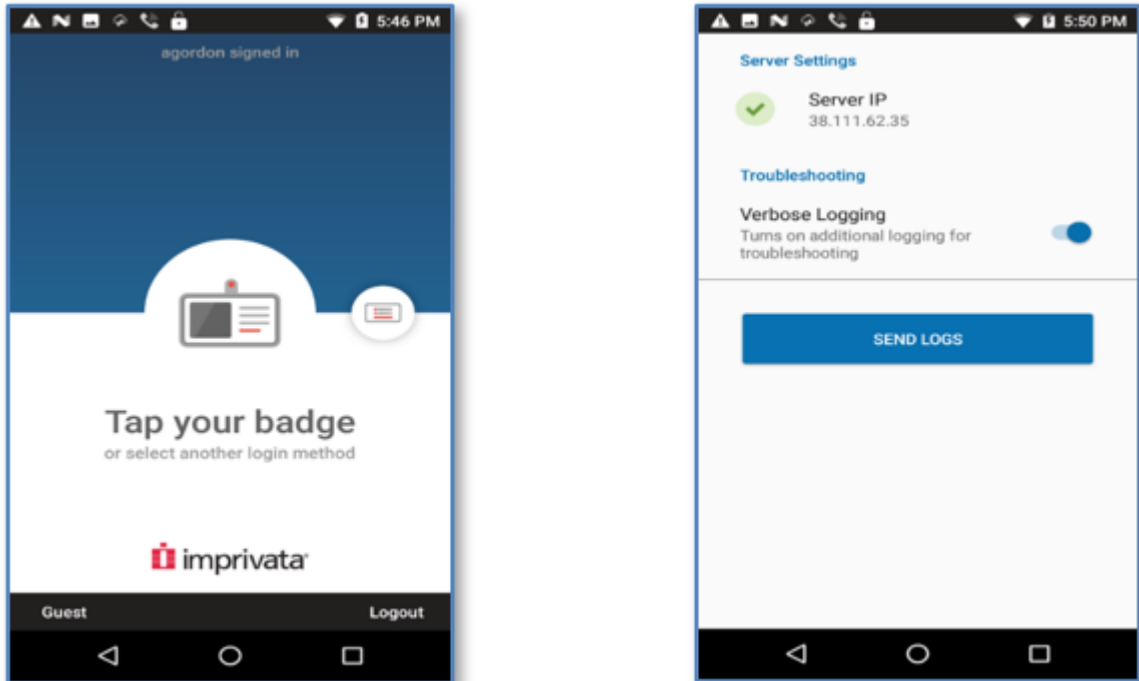
Configure Imprivata Mobile Device Access (IMDA) client to access the Imprivata server.

Complete the following steps to install and configure the IMDA client:

- Install the client and accept the appropriate permissions from the device operating system.
- Turn on the NFC radio on the device.
- Configure the IMDA client with the IP address of the Imprivata server.

Open the IMDA client and tap the blue background ten times to display the client settings and enter the IP address for the Imprivata server.

Figure 2 IMDA Settings



Return to the IMDA main screen after entering the IP address of the Imprivata server.

Configuring the WFC Profile Client

Refer the [Workforce Connect Profile Client Android Configuration and Programmer Guide](#) for configuration information regarding the WFC Profile Client.

Configuring the Profile Manager Tenant

Modify the Profile Manager Customer and Mobile Device options to configure the authentication method.

1. Select **Customer** from the Profile Manager dashboard.

Edit Customer	
CLS Id	sdfsd fsdfsdf
Extension Manager Url	https://asasdasdasdasd.pttpro.zebra.com
Authentication Method *	IMPRIVATA
OAuth Details:	

2. Select IMPRIVATA from the **Authentication Method** drop-down menu.
3. Click **Update**.
4. Select **Device Users** from the **Device User Management** section on the **Dashboard**.
5. Verify that the **Authentication Method** is set to OAUTH2.

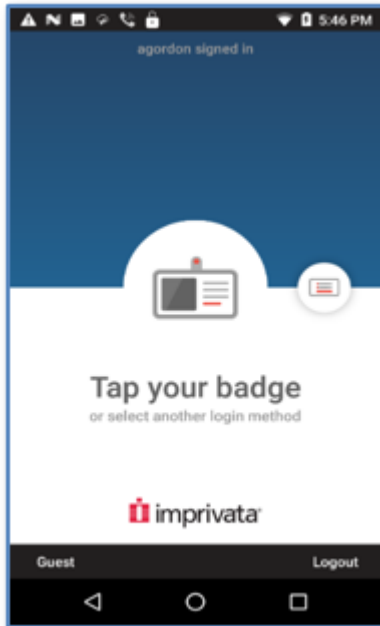
User Name	First Name	Last Name	User Role Levels	User roles	Organization	Department	Force Logout	Authentication Method
jbarber	Jerry	Barber		● wire			true	OAUTH2

Mobile Device Operation

When you start the device with the WFC Profile Client, the Imprivata interface displays.

Tap the NFC card on the back of the device.

Figure 3 Imprivata Screen When Device Starts

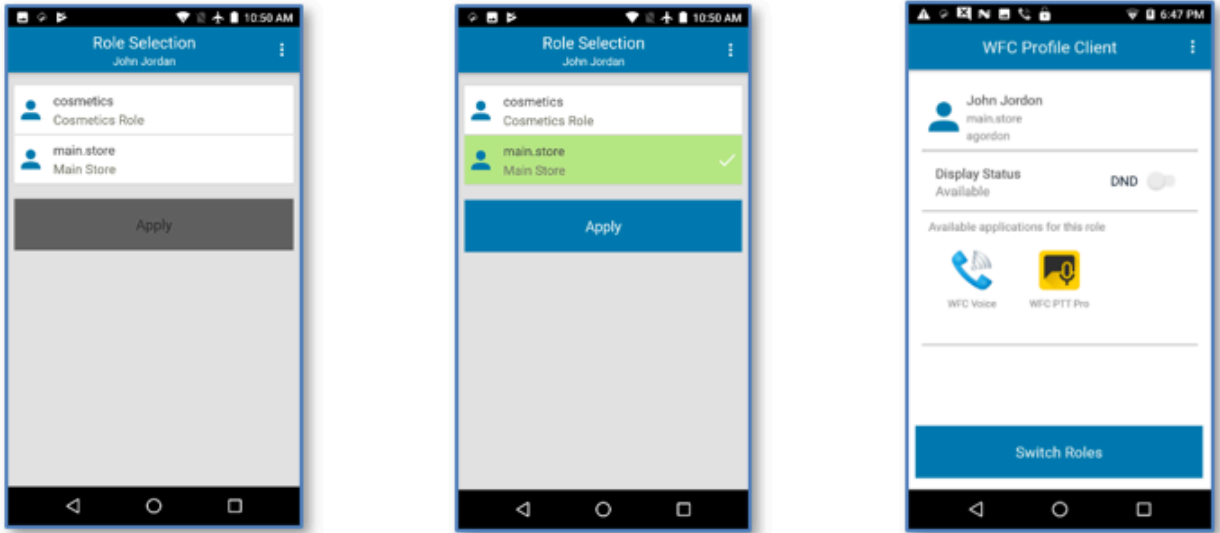


NOTE: NFC services do not automatically start after the device reboots. The Imprivata screen alerts the user to turn on NFC services for the device.

After a user logs in through Imprivata, the Profile Client automatically connects and logs in to Profile Manager. The list of roles available to the user display. The user selects a role and taps **Apply**.

In this example, the Main Store profile is delivered by the Profile Manager to the mobile device. This profile includes the WFC Voice client and the PTT Pro client.

Figure 4 Role Selection in the Profile Client



Revision History

Change	Date	Description
MN-004677-01EN	February, 2023	First version.

