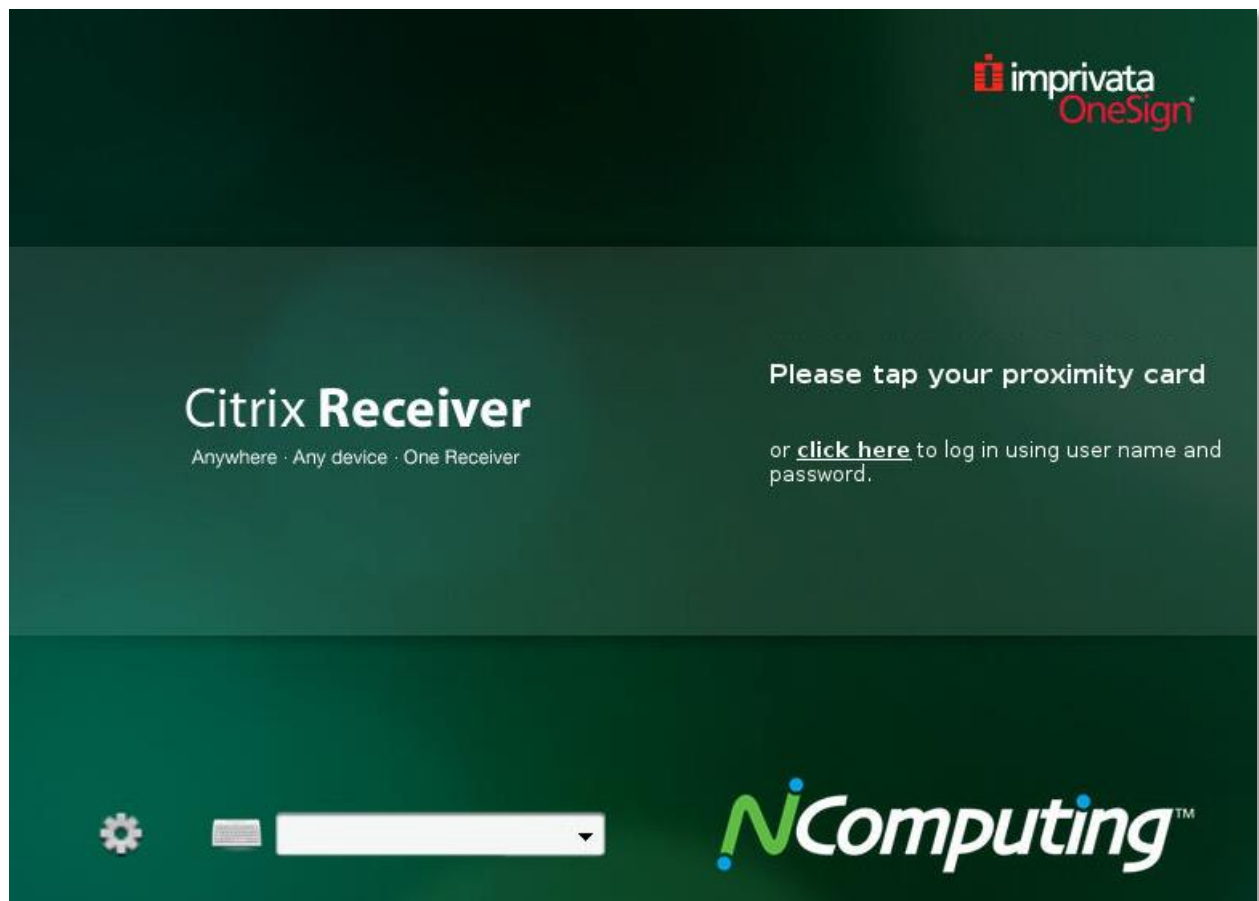




Imprivata OneSign® Integration For N-series Citrix Clients



Important Notices

Please note that reproduction of this User Manual in whole or in part, without express written permission from NComputing, is not permitted.

NComputing reserves the right to make improvements and/or changes to this User Manual and to the products, programs and/or specifications described herein at any time without notice. Information contained in this document may have been obtained from internal testing or from a third party.

NComputing shall not be liable for any direct, indirect, special, incidental or consequential damages in connection with the use of this material. The latest version of this User Manual can be downloaded from the "Documentation" page in the Support section of the NComputing website at:

www.ncomputing.com

Refer to the Limited Hardware Warranty applicable to your region for information on what is and what is not covered by the warranty, your responsibilities, exclusions, and how to obtain service. It is your responsibility to download a copy of the warranty at the time of purchase to keep for your records. The warranty can be downloaded from the "Documentation" page in the Support section of the NComputing website.

This product gives users shared access to computer resources. It is not a computer, and may not support all software applications, especially high-resolution graphics applications or 3D games that are designed to be supported by stand-alone computers. Similarly, it may not support all hardware peripherals that are designed to be supported by stand-alone computers.

Refer to your computer operating system and application software vendors' license agreements for information on using these products with NComputing systems. Additional software licenses may be required.

The NComputing hardware and software products described in this user manual are protected by numerous granted and pending U.S. and international patents. Some components of NComputing products utilize open-source software. Please refer to the GPL Declarations section of this User Manual for more information.

TABLE OF CONTENTS

Important Notices	2
1.0 N-series Overview	4
2.0 Imprivata Setup and Configuration.....	5
2.1 Enable ProveID Web API and Prove ID Embedded	5
2.2 Configure ProveID API Access	6
3.0 N-series Setup and Configuration	7
3.1 Update N-series Device Firmware	7
3.2 Connecting The RFID Card Reader	9
3.3(a) Enabling Imprivata ProveID from the N-series Access Device.....	9
3.3(b) Enabling Imprivata ProveID using vSpace Management Center	10
4.0 Verification and Troubleshooting	12
4.1 N-series Login Screen.....	12
4.2 RFID Device Compatibility	13
4.3 Troubleshooting	13
5.0 Additional Information and Support.....	14
5.1 NComputing Product Documentation	14
5.2 NComputing Technical Support	14
5.3 Additional Information on Citrix products and support	14
5.4 Additional Information on Imprivata products and support	14
Disclaimers and Legal Information	15

1.0 N-series Overview

The NComputing N-series HDX-ready Citrix access device utilizes powerful third-generation Numo™ 3 System on Chip technology to deliver a high-performance, affordable client for Citrix environments.

The N-series is available in three distinct versions; the N400, N500, and N500w. The entry level N400 is the thin client of choice for task workers and those workers with light multimedia needs. The N500 adds client-side video rendering to enable the delivery of full 1080p multimedia content, improved network capabilities, as well as options for dual monitor and wireless connectivity. The N500w further enhances the N-series' capabilities by providing wireless network access, allowing for easy implementation into nearly any environment.



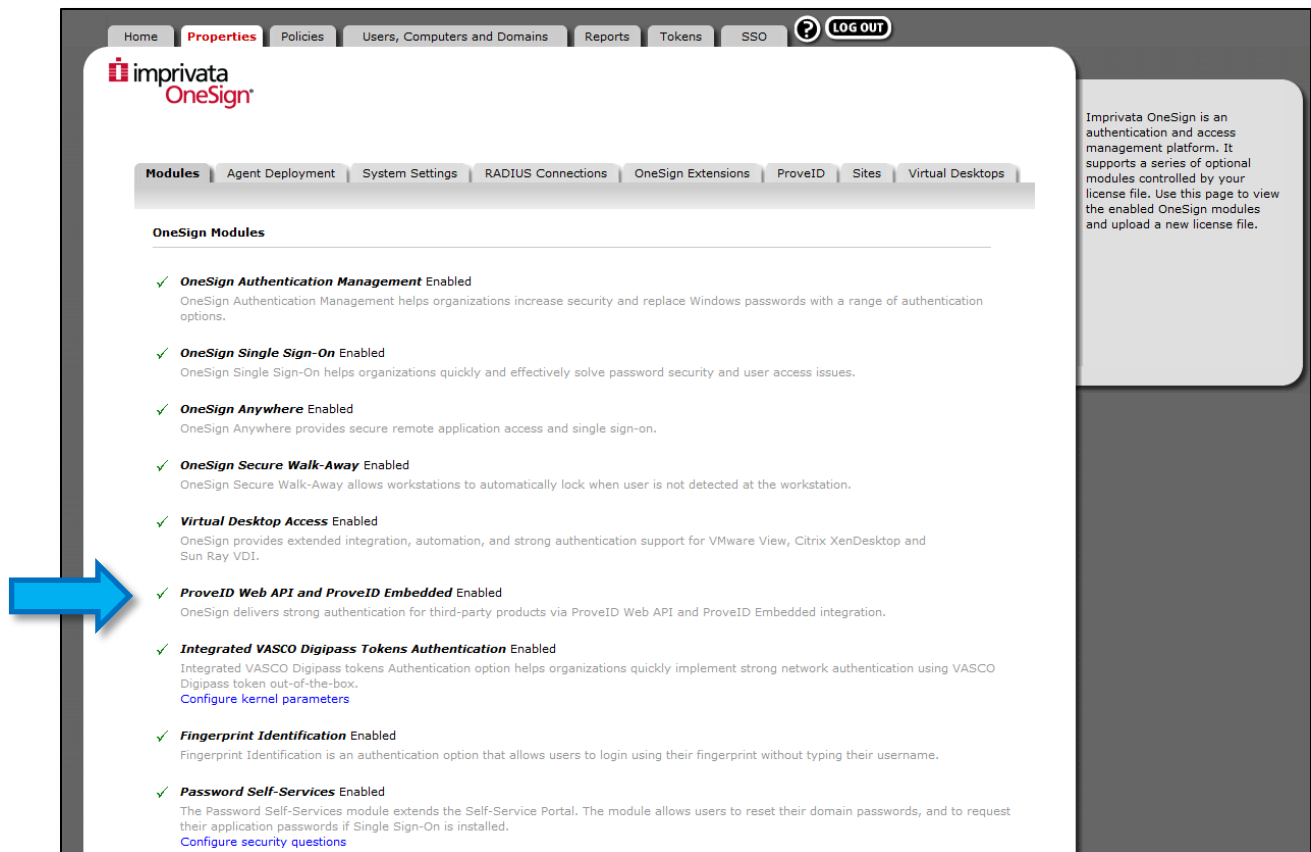
With the addition of Imprivata's OneSign Single Sign-On technology, the N-series offers users a streamlined, low-cost solution for Citrix XenDesktop and XenApp. This implementation guide will walk you through the process of enabling and configuring Imprivata OneSign technology for use with NComputing N-series access devices.

2.0 Imprivata Setup and Configuration

The following sections outline the configuration steps required on the Imprivata server end to enable N-series access devices to make use of OneSign and ProveID technology. Note that compatibility with N-series access devices requires **Imprivata OneSign version 4.6 or newer**.

2.1 Enable ProveID Web API and Prove ID Embedded

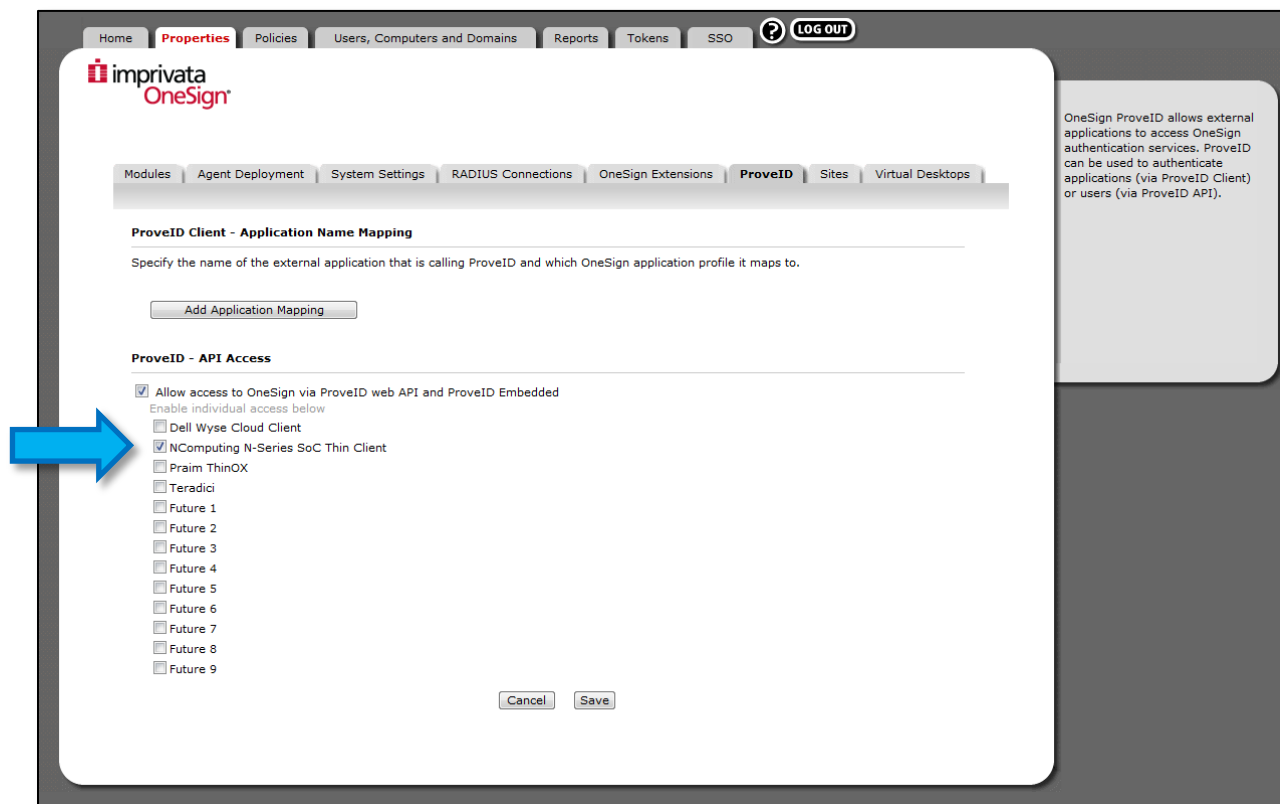
1. From the Imprivata server, open the **Properties Tab** and select **Modules**.



2. Ensure that the **ProveID Web API** and **Prove ID Embedded** feature is enabled, as shown in the image above.

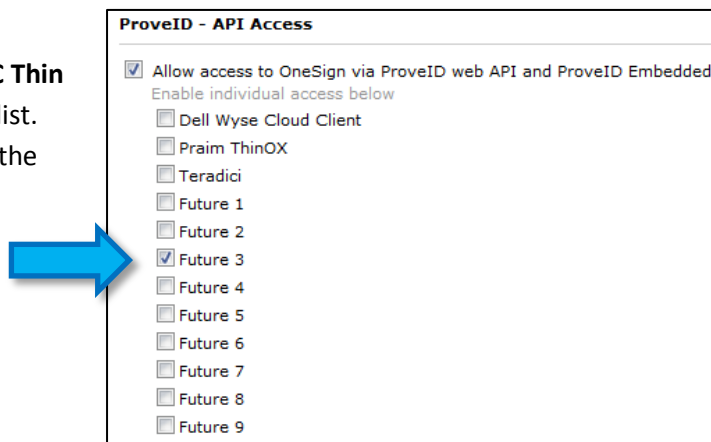
2.2 Configure ProveID API Access

1. From the **Properties Tab**, select **ProveID**.



2. Click the checkbox next to **“Allow access to OneSign via ProveID web API and ProveID Embedded”**.
3. Click the checkbox next to **“NComputing N-Series SoC Thin Client”**.

Note: Certain versions of Imprivata’s OneSign software may not list **“NComputing N-series SoC Thin Client”** as an option in the ProveID – API Access list. For these versions, administrators should select the **“Future 3”** option, as shown to the right:



3.0 N-series Setup and Configuration

The following sections outline the configuration steps required on the N-series device end to enable Imprivata functionality.

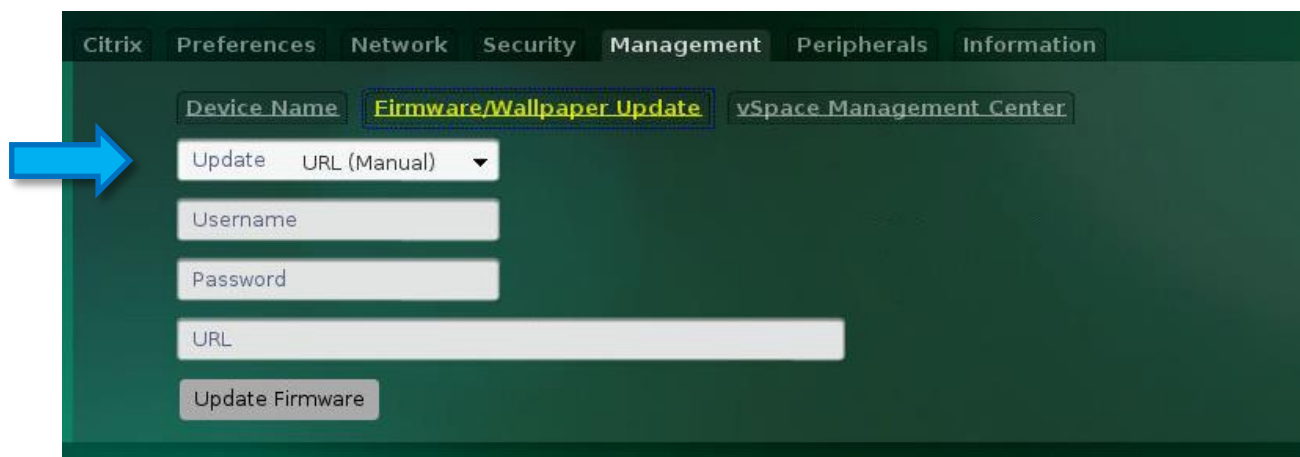
3.1 Update N-series Device Firmware

If you have not done so already, make sure the N-series device(s) that will be using RFID cards are fully updated with the latest firmware. **N-series firmware version 1.4.0.1** will be required to make use of Imprivata technology, along with a small patch provided specifically for Imprivata functionality. The following steps outline the firmware update process.

Proceed to www.ncomputing.com/softwaredownload and select any N-series model from the product drop-down. Click the link marked “**Download Firmware Pack**” under the 1.4.0 release section. This pack will include all of the firmware files from the stock release up through 1.4.0.1, as well as the Imprivata patch file. Be sure to read the latest firmware release notes and README carefully before installation. Once the firmware has been downloaded, it can be applied to the N-series devices in one of two ways; via FTP or using vSpace Management Center. Both methods are outlined below.

Applying Firmware via FTP

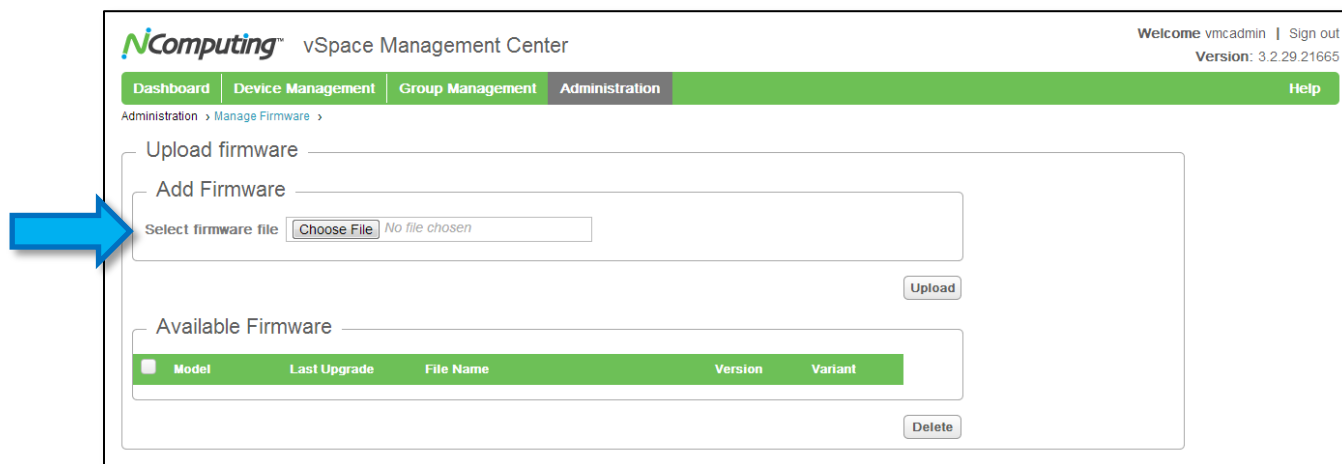
1. Host the N-series firmware in an FTP accessible folder within the same network as the device. If you are not familiar with sharing files across a network in this way, a basic guide on the subject is available at the following URL: <http://www.ncomputing.com/kb/afile/370/303/>
2. Once the file is hosted, open the N-series device’s configuration menu by clicking the **Gear Icon** on the lower left corner of the login screen. Once open, navigate to the **Management Tab** and select “**Firmware/Wallpaper Update**” as shown below.



3. Select **URL (Manual)** from the Update dropdown, and then enter the **URL**, **Username** and **Password** for the FTP source containing the firmware file.
4. Click **Update Firmware** to complete the process. Once the device reboots repeat this process for each of the N-series devices you wish to use and then proceed to section 3.2 of this guide.

Applying Firmware via vSpace Management Center

1. Move the downloaded firmware to your vSpace Management Center server.
2. Open the vSpace Management Center interface, and navigate to the **Administration -> Manage Firmware** page, as shown below.



3. Click the **“Choose File”** button at the top of the screen and navigate to the file’s location within Windows to add this firmware build to your vSpace Management Center database. Click **“Upload”** once you have selected the firmware file.

Once the firmware file appears in the available firmware list at the bottom of this page, you can “push” it to any of your N-series devices on an individual bases, or as part of an updated device profile.

- 4a. To push the firmware as a one-time update to specific devices, navigate to the **Device Management -> Update Firmware** page within vSpace Management Center. Proceed through the prompts selecting the devices you wish to update and the firmware you wish to use, and then confirm the update in the **Summary** section.

- 4b. To add the updated firmware to an existing device profile and automatically update any devices belonging to that profile, navigate to the **Device Management -> Manage Profiles** page within vSpace Management Center and select the desired profile. Click the **Firmware Tab**, and select the firmware you just downloaded. Click **“Apply”** on the Summary tab to complete the update*.

***NOTE:** If you use a profile to distribute the updated firmware, any devices belonging to that profile that are online at the time of the profile change will automatically begin updating their firmware. Any devices that are offline at that time will automatically receive their firmware update the next time they come online.

3.2 Connecting The RFID Card Reader

1. The N-series device features four USB ports; two on the front side of the device and two on the back. With the device powered off, connect your USB RFID card reader to one of the two ports on the front of the device, as pictured below:

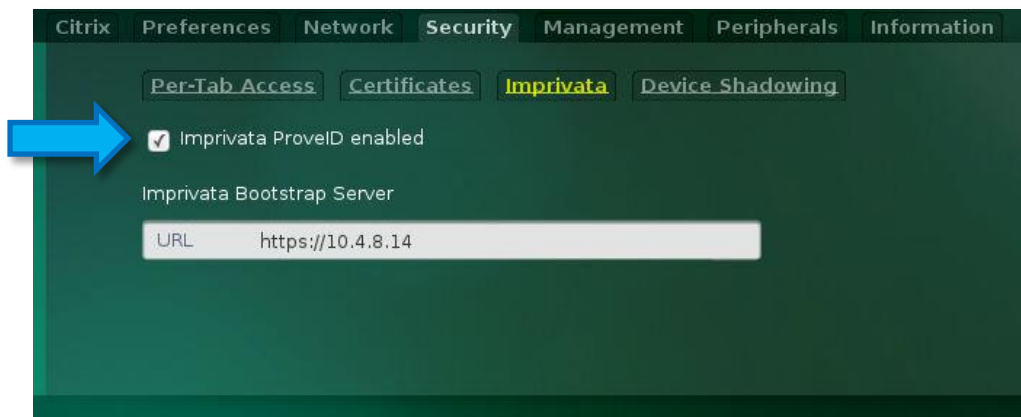


2. Once the reader is connected, power on the N-series device and proceed to the next section.

3.3(a) Enabling Imprivata ProveID from the N-series Access Device

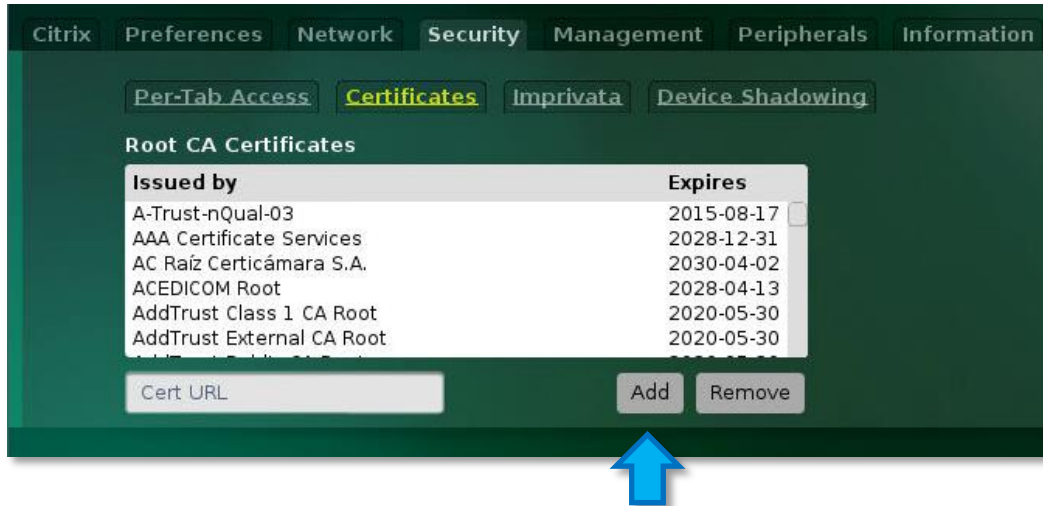
To enable Imprivata functionality from within the N-series device(s), complete the following steps:

1. From the N-series device, open the configuration menu by clicking the **Gear Icon** on the lower left corner of the login screen. Once open, navigate to the **Security** tab and select **Imprivata**, as shown below:



3. Click the checkbox next to **Imprivata ProveID enabled**, and enter the URL or FQDM of your Imprivata server in the **Imprivata Bootstrap Server** field.

4. Next, select **Certificates**, to the left of the Imprivata section.



2. From this menu, add the root certificate from your certificate signing authority using the **Cert URL** and **Add** button as indicated above.* Alternately, you can manually enter the URL of an Imprivata certificate in the Cert URL field using the following format:

`https://<any OneSign Appliance Address>/systemAdmin/ssoCA.crt`

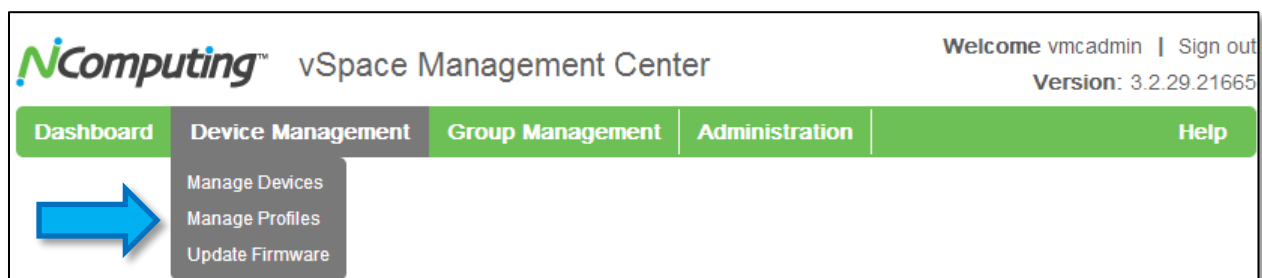
3. Once these settings have been finalized, click the SAVE button at the bottom left of the N-series GUI to return to the login screen.

***Note:** Certificates within the Root CA Certificates list are sorted alphabetically, with the exception of newly added certificates, which appear at the bottom of the list initially.

3.3(b) Enabling Imprivata ProveID using vSpace Management Center

If you would prefer to enable Imprivata on your N-series devices remotely using vSpace Management Center instead of configuring these settings on a per-device basis, you may do so by following these steps:

1. From vSpace Management Center, Select Manage Profiles from the Device Management dropdown, as shown below:



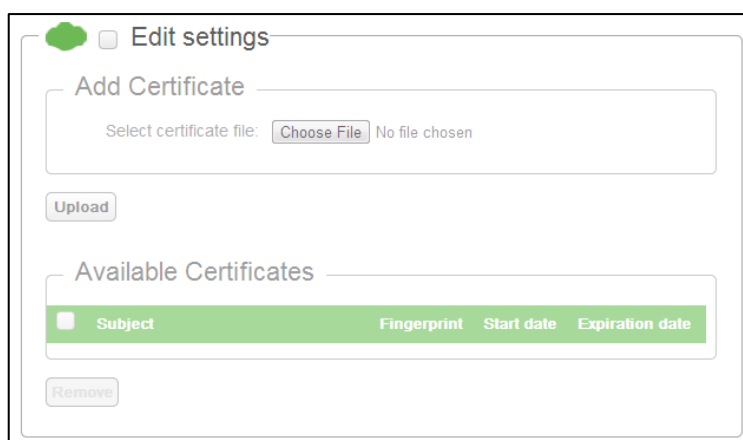
2. From the Manage Profiles menu, create a new profile by first selecting the N-series device model you have deployed, then naming the profile in the Profile Parameters tab.
3. Use the Select Devices tab to select all of the devices you wish to configure using this profile.
4. Select the Security tab from the tabs along the left side of the menu.
5. Use the Imprivata and Certificate fields to complete the configuration steps as outlined in **section 3.4** of this guide.



Imprivata

☐ Imprivata ProvelD enabled

Hostname/IP



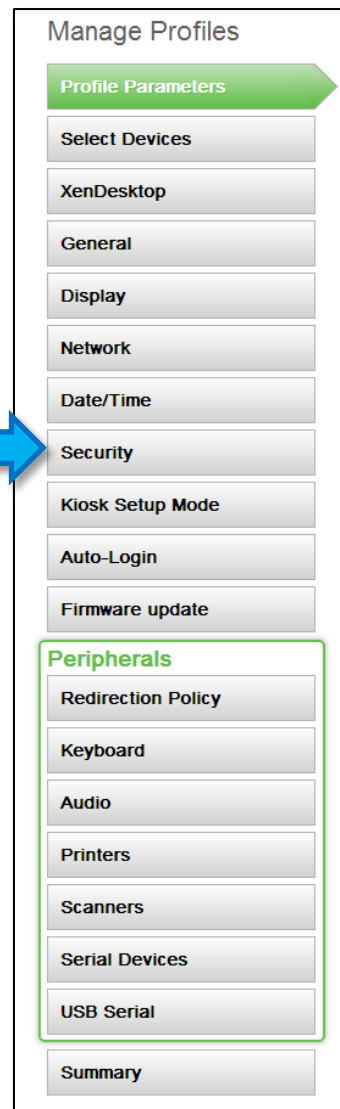
☐ Edit settings

Add Certificate

Select certificate file: No file chosen

Available Certificates

<input type="checkbox"/> Subject	Fingerprint	Start date	Expiration date
<input type="button" value="Remove"/>			



Manage Profiles

Profile Parameters

Select Devices

XenDesktop

General

Display

Network

Date/Time

Security

Kiosk Setup Mode

Auto-Login

Firmware update

Peripherals

Redirection Policy

Keyboard

Audio

Printers

Scanners

Serial Devices

USB Serial

Summary

6. If desired, adjust any other device settings such as display resolution and peripheral settings. Once you are satisfied with the profile settings, select the Summary tab and click “Apply” to push these settings to the devices you have selected.

4.0 Verification and Troubleshooting

The following sections provide a method of testing OneSign functionality on the N-series device, and verifying that the user can log in using an RFID card as well as lock the device in the same manor.

4.1 N-series Login Screen

When the Imprivata feature is enabled on an N-series device, the Login screen will change to display the Imprivata OneSign logo as shown below:



If the N-series device is able to communicate successfully with the Imprivata server, you will see the following text on the login screen:

“Please tap your proximity card or [click here](#) to log in using user name and password”

If the above message is displayed, touch your RFID card to the card reader to log in. For redundancy purposes, you should also verify that you can log in manually by clicking on the text indicated at the N-series login screen and entering your user name and password manually.

4.2 RFID Device Compatibility

The following RFID Card Readers have been tested and confirmed as compatible by NComputing's QA Department:

Make	Model	Model # / SKU
RFIDeas	Air ID Enroll	RDR-7582AKU
RFIDeas	pcProx	RDR-6082AKU
RFIDeas	pcProx Plus	RDR-80582AKU

4.3 Troubleshooting

Symptom ERROR: *"Could not connect to OneSign server!"*

Solution Double-check the information entered in the **Imprivata section of the Security Tab** and ensure that network routing rules are not preventing traffic between the N-series device and the Imprivata bootstrap server. This error message indicates that the device was not able to contact the Imprivata server using the currently entered server address. Refer to **section 3.3 of this guide** for more information on this setting.

Symptom ERROR: *"A network error has occurred!"*

Solution Double-check the N-Series DNS and network settings. This message can be an indication that the device's current network settings are invalid. This message can also appear as a result of the above scenario, wherein the Imprivata bootstrap server settings are not entered correctly.

Symptom ERROR: *"Unknown connection broker error. Please enter fully qualified domain name."*

Solution Check that the network cable is connected firmly to the N-series device. If the device is using a wireless network connection, verify the current wireless network settings. Lastly, double-check the domain information entered on the N-series login screen and confirm that it is valid.

5.0 Additional Information and Support

The following sections provide links to additional product documentation and support resources for NComputing, Citrix, and Imprivata products.

5.1 NComputing Product Documentation

For official NComputing product documentation, visit
<http://www.ncomputing.com/support/documentation>

5.2 NComputing Technical Support

For additional technical documentation, solutions, and how-to's, visit
<http://www.ncomputing.com/kb/>

To request Technical Support for NComputing products, please visit the NComputing Support page at <http://www.ncomputing.com/support>

5.3 Additional Information on Citrix products and support

For additional information and support for Citrix products and environments, visit
<http://www.citrix.com/lang/English/home.asp>

5.4 Additional Information on Imprivata products and support

For additional information and support for Imprivata products, visit
<http://www.imprivata.com/>

Disclaimers and Legal Information

Information contained in this document may have been obtained from internal testing or from a third party. This information is for informational purposes only. Information may be changed or updated without notice. NComputing reserves the right to make improvements and/or changes in the products, programs and/or specifications described herein anytime without notice. All NComputing software is subject to NComputing intellectual property rights and may be used only in conjunction with Genuine NComputing hardware and in accordance to the NComputing End User Licensing agreement and Terms of Use.

www.ncomputing.com

©Copyright 2003-2013 NComputing, Inc. All rights reserved. NComputing is the property of NComputing. Imprivata and OneSign are registered trademarks of Imprivata, Inc. in the U.S. and other countries. The Application Profile Generator and OneSign Agent are trademarks of Imprivata, Inc. Other trademarks and trade names are the property of their respective owners. Specifications are subject to change without notice. Performance may vary, depending on the configuration of the shared computer.