Imprivata® OneSign® Authentication Management comes in a non-intrusive, easy-to-implement appliance that requires no modifications to your network. Users can use strong authentication to access the network more securely. You can implement more secure policies in minutes while OneSign maintains user credentials so you do not have to.

This *OneSign Authentication Management Guide* includes information about the many strong authentication methods available with your Imprivata OneSign system:

- **Chapter 1, OneSign Authentication Methods** introduces the OneSign appliance, authentication methods, and how to deploy OneSign to your enterprise.
- **Chapter 2, Two-Factor Authentication in OneSign** introduces the two-factor authentication feature that strengthens IT security by requiring users to provide a second form of identification for authentication.
- **Chapter 3, Emergency Access Privileges** describes the question-and-answer emergency access feature.
- **Chapter 4, Converging Authentication Management with Physical Access** describes authentication issues relating to OneSign Physical/Logical.
- **Chapter 5, OneSign Secure Walk-Away** describes webcam workstation security.
- **Chapter 6, Configuring OneSign ProveID** describes OneSign’s powerful ProveID feature for ensuring the identity of users at the point of a specific transaction.
- **Chapter 7, Configuring Fingerprint Verification in OneSign** introduces OneSign concepts, including the appliance, authentication methods, and how to deploy OneSign to your enterprise.
- **Chapter 8, Configuring Fingerprint Identification in OneSign** describes how users can authenticate to OneSign with the secure, convenient fingerprint ID system.
- **Chapter 9, Configuring Passive Proximity Card Authentication in OneSign** provides the procedures you need to configure OneSign to work with your proximity card system.
- **Chapter 10, Configuring XyLoc KeyCard Authentication in OneSign** shows how to configure OneSign to work with a XyLoc active proximity card system.
- **Chapter 11, OneSign Authentication for Smart Cards with AD Certificates** shows you how to configure OneSign to work with MS Active Directory smart cards.
- **Chapter 12, OneSign Authentication for Smart Cards with External Certificates** shows you how to configure OneSign to work with third-party smart cards.
- **Chapter 13, Configuring RSA SecurID Token Authentication in OneSign** has procedures for configuring OneSign connections to an RSA SecurID token system.
- **Chapter 14, Configuring PhoneFactor Authentication in OneSign** shows you how to configure OneSign to work with your PhoneFactor system.
- **Chapter 15, Managing VASCO Digipass Tokens** provides the procedures you need to manage access through OneSign’s integrated VASCO VACMAN support.
- **Chapter 16, Managing an Individual Digipass Token** provides the procedures you need to manage Digipass tokens for individual users.
Contacting Imprivata, Inc.

Website http://www.imprivata.com
email support@imprivata.com
Phone Support in North America (800) 935-5958
Outside North America 001-408-987-6072
Sales (877) OneSign (663-7446)
Office address 10 Maguire Road, Lexington, MA 02421-3120,
United States of America

This product is distributed under licenses restricting its use, copying, distribution and decompilation.

Portions of this product are protected under US Patent Number 7,356,705.

OneSign, Imprivata, and the Imprivata logo are registered trademarks of Imprivata, Inc. ProveID and TouchPass APG are trademarks of Imprivata, Inc. in the United States and in other countries.

Under international copyright laws, neither the documentation nor software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part without the prior written consent of Imprivata, Inc., except as described in the license agreement.

The names of companies, products, people, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.
# Table of Contents

Contacting Imprivata, Inc. .......................................................................................................................... ii
Table of Contents ........................................................................................................................................ iii

**Chapter 1 - OneSign Authentication Methods** ...................................................................................... 1
  Password Authentication ............................................................................................................................ 2
  Fingerprint Verification ............................................................................................................................. 3
  Fingerprint Identification .......................................................................................................................... 4
  Passive Proximity Card Authentication .................................................................................................... 5
  XyLoc KeyCard Authentication ............................................................................................................... 6
  Smart Card/USB Token Authentication .................................................................................................... 7
  Authentication with VASCO Digipass and other ID Tokens ..................................................................... 8
  Emergency Access Privileges .................................................................................................................. 9
  Authentication with a OneSign PIN ......................................................................................................... 10

**Chapter 2 - Two-Factor Authentication in OneSign** ................................................................................. 11
  OneSign PIN as a Second Factor for Authentication ............................................................................. 12

**Chapter 3 - Emergency Access Privileges** ........................................................................................... 15
  Assigning and Revoking Emergency Access Privileges ........................................................................ 16
  Revoking Emergency Access Privileges ............................................................................................... 17
  Password Self-Services ............................................................................................................................ 19

**Chapter 4 - Converging Authentication Management with Physical Access** ................................. 21
  Permitting Authentication to OneSign if the Physical Access System is Unreachable ............................ 22

**Chapter 5 - OneSign Secure Walk-Away** .............................................................................................. 23
  OneSign Secure Walk-Away ..................................................................................................................... 24

**Chapter 6 - Configuring OneSign ProveID** ........................................................................................... 27
  Configuring an Application for OneSign ProveID ................................................................................... 28

**Chapter 7 - Configuring Fingerprint Verification in OneSign** .............................................................. 31
  Hardware Requirements .......................................................................................................................... 32
  Assigning Fingerprint Authentication Privileges ................................................................................... 33
  Enrolling Users for Fingerprint Verification .......................................................................................... 34
  Allowing Users to Manage Finger Enrollment Data ............................................................................... 36
  Managing Finger Enrollment Data ........................................................................................................ 37
  Authenticating to OneSign by Finger Biometrics .................................................................................. 38
  OneSign FastPass for Fast, Secure Login ............................................................................................... 39

**Chapter 8 - Configuring Fingerprint Identification in OneSign** .......................................................... 41
  Assigning Fingerprint Identification Privileges .................................................................................... 42
  Authenticating to OneSign via Fingerprint Identification ..................................................................... 43

**Chapter 9 - Configuring Passive Proximity Card Authentication in OneSign** .............................. 45
  Assigning Proximity Card Authentication Privileges ........................................................................... 46
  Enrolling Users for Passive Proximity Card Authentication .................................................................. 47
  Authenticating to OneSign by Passive Proximity Card .......................................................................... 49
  Locking a Shared Workstation ............................................................................................................... 50
  OneSign FastPass for Fast, Secure Proximity Card Login .................................................................... 51

**Chapter 10 - Configuring XyLoc KeyCard Authentication in OneSign** .......................................... 53
  Deploying XyLoc Locks and Readers .................................................................................................... 54
  Configuring OneSign Computer Policies for XyLoc Users .................................................................. 55
  Assigning XyLoc KeyCard Authentication Privileges ......................................................................... 57
  Installing the OneSign Agent with XyLoc Support .............................................................................. 58
  Enrolling for XyLoc KeyCard Authentication ....................................................................................... 59
  Authenticating to OneSign by XyLoc KeyCard ...................................................................................... 60

**Chapter 11 - OneSign Authentication for Smart Cards with AD Certificates** ............................ 61
  Server Configuration Requirements ....................................................................................................... 62
  Uploading the Keytab File to the OneSign Server .................................................................................. 63
  Assigning Smart Card/USB Token Authentication Privileges ............................................................... 64
Authenticating to OneSign via Smart Card or USB Token .......................................................... 65

Chapter 12 - OneSign Authentication for Smart Cards with External Certificates .... 67
   Assigning Smart Card Authentication Privileges ................................................................. 68
   Overriding User Policies on Select Computers ................................................................. 69
   Enrolling for Smart Card Authentication ........................................................................... 70
   Authenticating to OneSign via Smart Card ....................................................................... 71

Chapter 13 - Configuring RSA SecurID Token Authentication in OneSign ............... 73
   Server Configuration Requirements .................................................................................. 74
   Configuring the RSA Authentication Manager to Recognize OneSign ......................... 75
   Configuring OneSign to Recognize the ID Token Server ............................................ 77
   Assigning SecurID Token Authentication Privileges ..................................................... 78
   Enrolling for SecurID Token Authentication .................................................................... 79
   Authenticating to OneSign via SecurID Token ............................................................... 80

Chapter 14 - Configuring PhoneFactor Authentication in OneSign ......................... 81
   Configuring OneSign to Work with a PhoneFactor Server ........................................... 82
   Configuring the PhoneFactor Agent to Recognize OneSign .......................................... 82
   Configuring OneSign to Recognize the PhoneFactor Server ....................................... 84
   Assigning PhoneFactor Authentication Privileges ......................................................... 85
   Authenticating to OneSign via PhoneFactor ................................................................. 86

Chapter 15 - Managing VASCO Digipass Tokens ......................................................... 87
   Reviewing VASCO Kernel Parameters ............................................................................ 88
   Using the Tokens Page ...................................................................................................... 89
   Importing Digipass Tokens .............................................................................................. 90
   Deleting Digipass Tokens ............................................................................................... 91
   Resetting Multiple Digipass Token PINs .......................................................................... 92
   Forcing Digipass ID Token Enrollment .......................................................................... 93
   Using Password with VASCO Digipass OTP ................................................................... 94
   Using Password plus OTP for Remote Authentication .................................................. 95
   Enrolling for Digipass Authentication ............................................................................ 96
   Authenticating to OneSign via Digipass ......................................................................... 97
   Managing an Individual Digipass Token ......................................................................... 98

Chapter 16 - Managing an Individual Digipass Token ................................................... 99
   Changing Token Status ................................................................................................... 100
   Assigning Available Status to a Digipass ....................................................................... 101
   Assigning a Digipass to a User ....................................................................................... 102
   Assigning Lost Status ..................................................................................................... 103
   Changing a Static PIN ..................................................................................................... 104
      User may never change static PIN ............................................................................ 105
      User must change PIN immediately and may change later .................................... 106
      User may change PIN at any time .............................................................................. 107
   Resetting and Changing a Static PIN ........................................................................... 108
   Using Virtual Tokens ...................................................................................................... 109
   Other Operations ............................................................................................................ 110
      Testing a Token’s One-Time Password .................................................................... 111
      Resetting a Disabled Digipass .................................................................................... 114
      Unlocking a Digipass ................................................................................................. 115
   Generating and Viewing a Token Activity Report ....................................................... 116

Index ...................................................................................................................................... 117
OneSign offers an array of administrative tools to simplify and monitor user access to network resources. Authentication methods are the ways a user can authenticate to OneSign. OneSign supports a wide variety of authentication methods:

- **Password Authentication** on page 2
- **Fingerprint Verification** on page 3
- **Fingerprint Identification** on page 4
- **Passive Proximity Card Authentication** on page 5
- **XyLoc KeyCard Authentication** on page 6
- **Smart Card/USB Token Authentication** on page 7
- **Authentication with VASCO Digipass and other ID Tokens** on page 8

This chapter also introduces:

- **Emergency Access Privileges** on page 9
- **Authentication with a OneSign PIN** on page 10

Every user must have at least one authentication method. Users authenticate to OneSign when logging in and unlocking their workstations, and during challenges. Challenges are described in the *OneSign Administrator Guide*. OneSign strong authentication keeps unauthorized people out of your network; however, a valid user might forget or lose an authentication factor; see **Emergency Access Privileges** on page 9.
Chapter 1 - OneSign Authentication Methods

Password Authentication

When you first install OneSign, all users are authorized for password authentication. The default username and password are their current user directory credentials.

You can disallow password authentication for some or all policies; however, all enabled users must have at least one authentication method. Password authentication is often used as a second factor for two-factor authentication.

There is no separate enrollment step for password authentication. All OneSign users automatically enroll the first time they log into Windows after installing the OneSign Agent.

User authentication via password is similar to Windows authentication, except that the user is prompted with the OneSign login screen instead of the Windows login screen:

![OneSign Agent Logon Window Showing Password Authentication](image)

Kerberos Authentication for MS Active Directory Passwords

OneSign supports the choice between native username/password authentication with or without Kerberos for MS Active Directory environments. Kerberos mode offers enhanced authentication speed and additional encryption for password users in OneSign. To establish Kerberos trust between Active Directory and OneSign, you must generate a Kerberos keytab file, as described in the OneSign Administrator Guide.
Fingerprint Verification

OneSign embeds a set of secure, high-performance finger biometric capabilities within the OneSign appliance. With finger biometric authentication, fingerprint matching confirms that users are who they say they are.

Finger Biometric Verification (Standard Module)

OneSign Fingerprint Verification lets users enter their login credentials while adding a layer of security by verifying their identity through a fingerprint swipe. This is a “one-to-one” verification as OneSign checks the fingerprint against the credentials provided by the user.

Finger Biometric Identification (Optional Module)

OneSign optionally supports finger biometric identification. This differs from standard verification in one critical way. With finger biometric identification, the matching algorithm establishes the user's identity from the database of all enrolled users without need for the user to enter a username (no typing is needed). This is a “one-to-many” identification as OneSign checks the fingerprint against all users in the database. Finger biometric identification is introduced in Finger Biometric Identification on page 4.

Finger Biometric Support

OneSign supports multiple types of biometric readers to execute a Windows login. Users enroll and authenticate locally and then can use any fingerprint biometric enabled PC to authenticate with a swipe of a finger.

Finger biometric authentication is reliable and easy.

Two Types of Fingerprint Scanners

Fingerprint authentication is detailed in the OneSign Authentication Management Guide. You can also use a OneSign PIN as an alternative to a password; see the OneSign Authentication Management Guide.
Chapter 1 - OneSign Authentication Methods

Fingerprint Identification

Fingerprint Identification is an optional component of OneSign. The standard finger biometric authentication matches a scanned fingerprint against the records for the individual user, who must enter a valid username along with the fingerprint scan. Easy-to-use Fingerprint Identification identifies the user by comparing the fingerprint to all other fingerprint records. Upon unique identification, the user is authenticated.

Fingerprint Identification is a OneSign optional module. With it, users enabled for fingerprint authentication automatically get the benefit of fast, secure OneSign fingerprint identification without the need to enter a username or select a domain.

Note: If the OneSign Administrator Properties page Modules section does not show Fingerprint Identification as Enabled, then your OneSign license does not include the Fingerprint Identification option.

A OneSign License with the Fingerprint Identification Module Enabled

Fingerprint ID is detailed in the OneSign Authentication Management Guide.
Passive Proximity Card Authentication

OneSign customers can take advantage of pre-existing, low-cost passive facility access cards as a familiar, easy authentication option without re-issuing cards to users. OneSign supports integration for the proximity physical access cards from HID and Motorola/Indala. No OneSign-to-access-card-panel interface is required.

Proximity card authentication can be combined with password, OneSign PIN (as an alternative to a password), or finger biometrics as second factors to provide strong two-factor authentication.

Proximity Cards

Proximity card authentication is detailed in the OneSign Authentication Management Guide.

Note: A proximity card reader is required for this to function.

You can set an option in Computer Policies (Proximity tab) to control whether a proximity card can lock a user’s shared computer screen.
XyLoc KeyCard Authentication

OneSign natively supports XyLoc™ KeyCard active proximity cards from Ensure Technologies. XyLoc is an active RF product that lets users identify themselves merely by approaching a XyLoc Lock-enabled PC. OneSign automatically locks the computer when the user departs. This feature is natively supported and requires no additional software or server to operate.

The XyLoc KeyCard and Lock

XyLoc authentication is detailed in the OneSign Authentication Management Guide.
Smart Card/USB Token Authentication

Smart cards and smart USB tokens provide two-factor authentication by combining a user PIN with a pre-programmed smart card or USB token. Smart cards are good until the expiration date of the digital certificate on the card, normally valid for two or more years.

OneSign is fully compatible with MS Active Directory certificate services and can use any smart card or USB token that contains a MS-compatible login certificate and compatible middleware for MS Active Directory environments using Windows 2000, XP professional, or Vista desktops. OneSign supports x.509 v3 digital certificates for Windows login in Microsoft Active Directory environments via the Windows Local Security Authority and Kerberos. PC/SC-compatible smart token technology is provided with MS Active Directory. Smart cards that comply with the U.S. Department of Defense (DOD) Common Access Card standard are also supported.

In OneSign SSO environments, smart card authentication grants network access and an SSO session in a single step. Smart card-enabled users authenticating to OneSign use a smart card and associated PIN. OneSign makes no difference to the user experience of logging into Windows.

A Smart Card and Smart Card Reader

Smart Card/USB token authentication is detailed for both AD and external certificates in the OneSign Authentication Management Guide.
Authentication with VASCO Digipass and other ID Tokens

OneSign delivers support for VASCO Digipass tokens out-of-the-box and embeds VASCO's VACMAN middleware and management components within the OneSign appliance. There is no separate token management server to purchase or maintain.

![VASCO Digipass Token]

Digipass authentication is detailed in the OneSign Authentication Management Guide.

Using RSA SecurID and SafeWord Tokens

Additionally, sites that have deployed Secure Computing SafeWord or RSA Security SecurID strong authentication tokens can leverage these existing investments. OneSign includes built-in RADIUS integration to Secure Computing's Premier Access and Remote Access Servers and RSA's Authentication Manager for token authentication. OneSign can provide a seamless single-step desktop login using two-factor one-time passcodes for login to any SSO-enabled client/server, web, or legacy application from any OneSign-enabled desktop.

OneSign supports ID token authentication with:
- RSA SecurID® tokens with RSA Authentication Manager®
- Secure Computing SafeWord® tokens with PremierAccess® and RemoteAccess™ servers

![ID Tokens: RSA SecurID Keyfob and Secure Computing SafeWord Token]

ID Token authentication is detailed in the OneSign Authentication Management Guide.

If you are transitioning from RSA SecurID or Secure Computing SafeWord tokens to VASCO Digipass tokens, you can use both SecurID or SafeWord and VASCO Digipass tokens in the same OneSign system.

OneSign also supports PhoneFactor tokenless two-factor authentication.
Emergency Access Privileges

Occasionally users forget or lose their ID tokens, smart cards, or other authentication factors. You can configure emergency access privileges to permit the user access upon answering a number of security questions.

Emergency Access

Emergency Access is detailed in the OneSign Authentication Management Guide.
Authentication with a OneSign PIN

In the authentication configuration for a user security policy, you can configure a OneSign PIN as a second factor (as an alternative to a password) to be used with the primary authentication methods: fingerprint authentication and proximity card authentication. You can configure this feature to require the OneSign users to create and confirm a numeric PIN when they first login.

OneSign PIN Options as a Secondary Factor

See the OneSign Authentication Management Guide for more information.
Two-Factor Authentication in OneSign

OneSign offers a two-factor authentication that strengthens IT security by requiring users to provide a second form of identification for authentication.

Fingerprint identification can be combined with a password or a OneSign PIN as a second factor. Proximity Card authentication can be combined with a password, a OneSign PIN (as an alternative to a password), or finger biometrics as second factors.

VASCO Digipass and other ID tokens are two-factor authentication by nature as they already have PINs assigned to them. Smart card and Smart USB Token authentication can also be used as a two-factor authentication methods.

This chapter contains **OneSign PIN as a Second Factor for Authentication** on page 12.

See the **OneSign Administrator Guide** for more information on assigning authentication methods for user policies.
Chapter 2 - Two-Factor Authentication in OneSign

OneSign PIN as a Second Factor for Authentication

In the authentication configuration for a user policy, you can configure a OneSign PIN as a second factor (as an alternative to a password) to be used with the primary authentication methods: Fingerprint Identification and Proximity Card authentication. This feature lets you configure OneSign to have users create and confirm a numeric PIN when they first enroll or log in.

When you configure a OneSign PIN for use with any primary method, the same settings are applied for use with all other primary methods that employ a OneSign PIN.

Fingerprint Identification Authentication with a OneSign PIN

To configure user policy settings for a OneSign PIN as a second factor with Fingerprint Identification:

1. From the Authentication tab, click **Fingerprint**.
2. Click **OneSign PIN** from the Secondary group.
3. Click **Options...** to open the options dialog box.

OneSign PIN Options as a Secondary Factor for Fingerprint Authentication

4. Set the minimum and maximum lengths for the OneSign PIN (4 to 20 digits).
5. Enable **Force PIN Enrollment** to prompt users to create and verify a new OneSign PIN number upon first login (otherwise, users can enroll at anytime). If users click Cancel in the enroll OneSign PIN login box, they will not be allowed to login.

Once the OneSign PIN is specified, the user is prompted to enter the PIN on subsequent logins after fingerprint or proximity card requirements are met.

6. Enable **Require OneSign PIN Change on Expiration** to have the OneSign Agent force users to change and verify their OneSign PIN numbers when expired.

Users will be prompted to enter their old PIN and will then be prompted to create and verify a new PIN.

7. If you enabled **Require OneSign PIN Change on Expiration**, enter the number of days (1 to 365) for which the PIN number will be valid and click **OK**.

8. Click **Save** at the bottom of the page.

**Proximity Card Authentication with a OneSign PIN**

To configure user policy settings for a OneSign PIN as a second factor with a Proximity Card:

1. From the Authentication tab, click **Proximity Card**.

2. Select **Password or OneSign PIN** from the Secondary group and then click **OneSign PIN**.

3. Click **Options...** to open the options dialog box.
OneSign PIN Options as a Secondary Factor for Proximity Card Authentication

4. Set the minimum and maximum lengths for the OneSign PIN (4 to 20 digits).

5. Enable **Force PIN Enrollment** to prompt the user to create and verify a new OneSign PIN number upon first login. If users click Cancel in the enroll OneSign PIN login box, they will not be allowed to login.

Once the OneSign PIN is specified, the user is prompted to enter the PIN on subsequent logins after fingerprint or proximity card requirements are met.

6. Enable **Require OneSign PIN Change on Expiration** to have the OneSign agent force users to change and verify their OneSign PIN numbers when expired.

Users will be prompted to enter their old PIN and will then be prompted to create and verify a new PIN.

7. If you enabled **Require OneSign PIN Change on Expiration**, enter the number of days (1 to 365) for which the PIN number will be valid and click **OK**.

8. Click **Save** at the bottom of the page.
Emergency Access Privileges

Emergency access privileges let authorized users gain network and SSO access even if they have forgotten a password or lost an ID token or other authentication device. To gain access, the user must correctly answer a number of security questions.

Selecting Emergency Access

You configure the emergency access settings such as:

- the number of questions to answer for successful authentication
- the number to answer when enrolling for emergency access privileges
- how many times a user can take advantage of emergency access in a month

You also control who can have emergency access privileges. Emergency access privileges are granted through the user policies, as described in Assigning and Revoking Emergency Access Privileges on page 16.
Chapter 3 - Emergency Access Privileges

Assigning and Revoking Emergency Access Privileges

You assign and revoke emergency access privileges through the OneSign User Policies that you assign to each user. Emergency access is available only when the user is authenticating to an online OneSign Agent.

User Policy that Permits ID Token Authentication with Emergency Access

You can change the settings of the emergency access options through a dialog that opens when you click the red options link:

Configuring Emergency Access Options

You can set different emergency access settings for different user policies. When you create a new user policy with emergency access privileges, the new policy uses the settings in the default policy as a starting point.
Revoking Emergency Access Privileges

Revoke emergency access privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

User policies are detailed in the OneSign Administrator Guide.

Deleting Emergency Access Enrollment Data for a User

Occasionally a user wants to change the answers to emergency access questions or to select different questions to answer. In this situation, you need to delete the existing data to make way for the new data.

You can delete a user’s emergency access enrollment data from the user record:

Deleting Emergency Access Enrollment Data

Save when you are finished.
Chapter 3 - Emergency Access Privileges

Resetting the Emergency Access Usage Counter

If a user has exhausted the number of emergency access uses permitted by your policy, you can reset the usage counter to 0:

Resetting Emergency Access Enrollment Data

Save when you are finished.

Restricting Emergency Access at Some Computers

You can restrict emergency access at individual computers by deselecting the Emergency Access option in a computer policy applied to the affected computers.

To change the security questions, see the OneSign Administrator Guide.
Password Self-Services

All installations get the OneSign Self-Service Portal, reachable at https://<OneSign IP>/sso/passwordhelp:

A Customized OneSign Self-Service Portal, without the Password Self-Service Option

The Password Self-Services option extends the portal to permit users to change their primary authentication passwords and to review their application credentials (if you have deployed the SSO option):

The OneSign Self-Service Portal with Password Self-Service Option

You can customize the Password Self Services screen with your corporate logo; the procedure is detailed in the OneSign Administrator Guide.
Converging Authentication Management with Physical Access

Imprivata OneSign Physical/Logical integrates building and network access systems for unified enterprise security management by consolidating identities between physical access systems and IT directories. This enables creation and deployment of a single, converged security policy for allowing or denying remote and local network access based on a user’s physical location, user role, and/or employee status.

Coordinating Network Access and Physical Access

OneSign Physical/Logical is fully detailed in the OneSign Physical/Logical Guide. A special authentication issue is detailed in this chapter.

When you use OneSign in conjunction with a physical access system, a situation might arise where the OneSign server is running, but the physical access system is unreachable. You can permit certain users or computers to bypass the physical access system, as described in Permitting Authentication to OneSign if the Physical Access System is Unreachable on page 22.
Chapter 4 - Converging Authentication Management with Physical Access

Permitting Authentication to OneSign if the Physical Access System is Unreachable

User and computer policies that permit or deny network access based upon physical access status require information from the physical access system. If the physical access system is unreachable for any reason, then the physical access side of the equation is unknowable to OneSign.

The default OneSign behavior in this circumstance is to ensure security by prohibiting network access to users who might not have authenticated to the physical access system.

For some users or for some computers that do not require such stringent security measures, you can permit authentication in the event that the physical access system is unreachable. This is also useful if a new user has a network account and is listed in the physical access system, but the accounts have not yet been mapped in OneSign.

To grant network access if the physical access system is unreachable or if a OneSign user has not yet been mapped to an account in the physical access system, create a new User Policy and check the Bypass checkboxes on the Network Access tab.

Permitting Network Access in the Absence of a Physical Access System Connection

For greater security, you can prohibit physical access connections in the User Policies, and then implement this feature for specific computers by using the Override User Policy feature for Local Network Access in a Computer Policy for specific computers.
OneSign Secure Walk-Away closes a critical security gap in the protection of confidential information assets by automating the process of securing the desktop when a user walks away.

OneSign Secure Walk-Away uses a combination of computer vision, active presence detection, and user tracking technologies to identify an authenticated user in front of a workstation, automatically locking the desktop upon the user’s departure and providing instant re-authentication upon their return.

OneSign Secure Walk-Away flexibly supports different user workflows, including shared workstation environments where multiple users require constant fast and secure login and logout to information assets.

Secure Walk-Away is of particular value in clinical settings. Secure Walk-Away enables hospitals to improve patient safety by eliminating the charting errors that can result from an incorrect user logging into a workstation. It also ensures regulatory compliance by taking the burden of desktop security out of the hands of clinicians in a non-intrusive and seamless way.

The Desktop is Active Only While An Authorized User is Present
Chapter 5 - OneSign Secure Walk-Away

OneSign Secure Walk-Away

OneSign Secure Walk-Away automatically secures a user workstation or session when the user leaves the workstation unattended. The system tracks a user's physical presence in front of the workstation using a combination of off-the-shelf webcam hardware, head tracking, and facial recognition technologies.

You configure OneSign Secure Walk-Away from the Agent tab of a Computer Policy:

Configuring OneSign Secure Walk-Away

Before You Begin

Make sure each computer that will support Secure Walk-Away is equipped with a supported web camera. The camera must be properly installed and adjusted for workplace lighting conditions. Users must be trained in the workflow; the OneSign User Information Kit has helpful information for users about OneSign Secure Walk-Away.
Configuring OneSign Secure Walk-Away

To configure Secure Walk-Away:

1. Check the **Automatically lock workstation if user leaves workstation** checkbox.
2. To prevent unauthorized users from gaining access to a computer by disconnecting the camera, check **Lock the workstation after the camera is unplugged or otherwise unavailable**.
3. To secure the workstation when no enrolled user is physically present, check **Lock the workstation if a face is not detected immediately after logging in**.
4. Secure Walk-Away is a change to users’ workflow. Check **Show a tutorial the first time each user logs in** to help educate users about the Secure Walk-Away feature.
5. Set the **countdown to session lock** value. This is the number of seconds after a user is no longer detected before the screen is locked. A user who returns within the countdown period does not have to reauthenticate.
6. Set countdown behavior. Select:
   - **Show the countdown in a notification area balloon**, if you want users to see how soon the session will lock, or
   - **Obscure the desktop during the countdown**, if you want to obscure the desktop until the session lock.
7. Users who often spend a few moments out of camera view while working may find the immediate appearance of a countdown balloon or obscuring the screen a distraction. To delay the appearance of the countdown balloon or the obscured desktop for a few seconds, enter a value in **Delay before countdown appears**.
8. You can enable a grace period for users who frequently leave and return to a Secure Walk-Away-equipped workstation. To enable a grace period, check **Allow visual re-authentication if the same user returns to the workstation within** and enter a value in minutes.

### Secure Walk-Away Technical Specifications for Client Computers

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lighting</td>
<td>50 to 5000 Lux, evenly diffused</td>
</tr>
<tr>
<td>Processor</td>
<td>Pentium 4 Hyperthreaded: 2.4 GHz +, CoreDuo or Core2Duo 1.6 GHz +</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB RAM for Windows XP, 2 GB RAM for Windows 7</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows XP Professional or Windows 7</td>
</tr>
<tr>
<td>Supported Cameras</td>
<td>Logitech Pro 9000, Logitech Pro for Notebooks</td>
</tr>
<tr>
<td>Recommended</td>
<td>Privacy filter, Disable screen saver</td>
</tr>
</tbody>
</table>
Configuring OneSign ProveID

OneSign ProveID is an API that allows an external application to access the OneSign Agent’s authentication services and devices. When triggered by a calling application, OneSign ProveID presents a challenge to verify the user’s identity.

Before you begin

Use the OneSign APG to profile the target application. The list of OneSign application names is generated from the list of OneSign application profiles.

Get the executable application name from the application provider. You will use the exact name used by the application provider when you map it to the OneSign application profile name.

Set Configure ProveID administrator privileges for administrators as needed at Users page>Administrator Roles tab.

Note: OneSign ProveID is only usable with applications that have been explicitly configured by the application provider for use with OneSign ProveID.
Configuring an Application for OneSign ProveID

Configuring an application for OneSign ProveID requires mapping the name used by the application provider to the name used in the OneSign application profile:

1. Open the OneSign Administrator to the Properties page, ProveID tab. The OneSign ProveID tab is on the right end of the Properties page just before the OneSign Sites tab.

![The OneSign ProveID Tab, with no Applications Mapped](image)

2. Enter the application name in the **External Application Name** boxes on the left. OneSign relies upon a text match, so use the *exact name* used by the application provider.

3. From the dropdown list on the right, select the corresponding **OneSign Application Profile Name**.
Mapping an Application to a OneSign Application Profile

You can map multiple applications to a single OneSign application profile. Use the Or... selection to add another mapping to the same OneSign application profile.

Mapping Multiple Applications to a Single OneSign Profile

4. To configure additional applications for OneSign ProveID, click Add Application Mapping and map additional applications as detailed above.
Mapping Another Application to a Different OneSign Application Profile
Configuring Fingerprint Verification in OneSign

This chapter contains:

- **Hardware Requirements** on page 32
- **Assigning Fingerprint Authentication Privileges** on page 33
- **Enrolling Users for Fingerprint Verification** on page 34
- **Allowing Users to Manage Finger Enrollment Data** on page 36
- **Authenticating to OneSign by Finger Biometrics** on page 38
- **OneSign FastPass for Fast, Secure Login** on page 39

**Two-Factor Strong Authentication**

Fingerprint verification can be used in conjunction with a password or a OneSign PIN as a second factor for strong two-factor authentication. When you select **Fingerprint** from the list of primary authentication methods in a user policy, an Options link appears. Click that link to require password authentication or OneSign PIN for users with that security policy.

Fingerprint verification can also be used in conjunction with proximity cards for two-factor authentication. Configure this from the Proximity Card Options. For more on two-factor authentication, see **Two-Factor Authentication in OneSign** on page 11.

**Monitoring and Reporting Fingerprint Verifications**

You can get real-time notifications of many network events, including enrollment for fingerprint. Event notifications are detailed in the **OneSign Administrator Guide**.
Hardware Requirements
To implement finger biometric authentication, workstations must be equipped with fingerprint scanners.

Two Types of Fingerprint Scanners

The fingerprint scanner can be built into a laptop or keyboard, or a USB device that connects to the local computer. It includes a transparent scanning area on which the user places the pad of the fingertip being scanned or swipes the fingertip along the thin strip. As long as one enrolled finger is clean and unscarred, fingerprint scanning is highly reproducible and reliable.

The scanner has no moving parts. The important part is the scanner window or strip. As long as the window or strip is clean, your finger biometric authentication is simple and reliable.

Server Configuration Requirements
OneSign Fingerprint Verification support is handled entirely on the OneSign appliance. There are no connections required to any other servers when you implement fingerprint verification.
Assigning Fingerprint Authentication Privileges

Assign fingerprint authentication and all other authentication methods through the OneSign User Policies that you assign to each user. User policies are detailed in the OneSign Administrator Guide.

A User Policy that Permits Only Fingerprint Verification

Computer Policy Overrides

OneSign permits you to assign computer policies to individual computers. The Override User Policy tab of a computer policy includes an option to allow or to prohibit fingerprint authentication on individual computers. When a user with a user policy that permits fingerprint authentication tries to authenticate to a computer that does not, the computer policy overrides the user policy.

Revoking Fingerprint Authentication Privileges

Revoke fingerprint authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.
Enrolling Users for Fingerprint Verification

Users whose security policies are authorized for fingerprint verification (or for the optional fingerprint identification) get the opportunity to enroll the next time they log into OneSign.

**Note:** All fingerprint data is securely encrypted before it is transmitted and saved. OneSign does not save an image of a fingerprint. Nobody can read the fingerprint data.

To enroll for finger biometrics:

1. After becoming authorized for fingerprint verification or fingerprint identification, use your password to log into OneSign.

2. OneSign logs you into Windows and prompts you to enroll a finger. Accept it and click **Next**.

The Manage Fingerprints screen appears:

![Manage Fingerprints Screen](image)

**Select a Finger for Enrollment**

3. Click a finger to enroll.
A new screen appears:

![Fingerprint Enrollment Screen]

**Scan the Finger for Enrollment**

4. Complete Step 1 by getting three good scans of the finger.

5. Complete Step 2 by scanning the finger again to validate the fingerprint.

6. To enroll more fingers, click **Yes, enroll another finger**. When you have finished scanning fingerprints, click **No, I'm done**.

**Deleting Enrollment Data**

You can delete the enrollment data for fingerprint users from each user's user record.

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Enrolled</th>
<th>Unenrolled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OneSign PIN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DigiProx token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Enrolled</td>
<td></td>
</tr>
<tr>
<td>Proximity Card</td>
<td>Unenrolled</td>
<td></td>
</tr>
<tr>
<td>Smart Card/USB Token (Active Directory certificate)</td>
<td>Unenrolled</td>
<td></td>
</tr>
<tr>
<td>Smart Card (External certificate)</td>
<td>Unenrolled</td>
<td></td>
</tr>
</tbody>
</table>

**Deleting Fingerprint Enrollment Data**
Allowing Users to Manage Finger Enrollment Data

You can allow users to manage their fingerprints after the initial enrollment by editing Fingerprint options in the User Policies. Users with this privilege can enroll additional fingers and un-enroll and re-enroll currently enrolled fingers.

To allow users to manage finger enrollment data:

1. Select the User Policy from the Policies page.
2. In the Fingerprint options, click the checkbox next to Allow users to manage fingerprints:

   Users Are Allowed to Manage Their Fingerprints

   Uncheck the box to prevent users from managing their fingerprints.
3. Click OK and then save the user policy.

See Managing Finger Enrollment Data on page 37 for more information about managing fingerprints.
Managing Finger Enrollment Data

Users can manage their fingerprints from the OneSign Agent menu:

Click Manage Fingerprints

To enroll additional fingers, click the unenrolled finger you wish to enroll.

To re-enroll or un-enroll a finger:
1. Click a enrolled finger. A menu appears:

Select an Finger Enrollment Action from the Menu

2. Select an action from the menu.

See Enrolling Users for Fingerprint Verification on page 34 for information about enrolling fingers.
Authenticating to OneSign by Finger Biometrics

To authenticate via fingerprint scanner:

1. At the OneSign logon window, enter your username and domain. This step is unnecessary if you are using the optional Fingerprint Identification feature, described in Configuring Fingerprint Identification in OneSign on page 41.

   Note: If the Fingerprint option does not appear, then check to be sure the fingerprint scanner is connected to the computer.

2. Select Fingerprint and then click OK. The Fingerprint Scanner screen appears:

   ![The Fingerprint Scanner Screen]

3. Scan any enrolled finger and wait for the system to acknowledge the scan.

4. If a password is configured as a second authentication factor, enter the password and click OK.

   If a OneSign PIN is configured as a second authentication factor, enter the PIN and click the Use OneSign PIN button.

When you have been authenticated, the authentication window closes.
OneSign FastPass for Fast, Secure Login

OneSign FastPass™ allows users fast and secure access to shared workstations with the convenient touch of their fingers. When FastPass is combined with OneSign’s ability to automatically launch applications, sign users into and out of applications and automate Citrix roaming, OneSign provides users with an unprecedented ability to move quickly, unimpeded by access issues.

Users perform a secure, two-part authentication at the beginning of their work shift by scanning their finger and entering a PIN or password as the second factor. Once this two-factor authentication is completed, FastPass starts an authentication grace period, during which the users may access their computer or shared workstations simply by scanning their finger. Users only need to enter their PIN or password again when their grace period expires.

You assign the grace period from an Options link beside the primary authentication method in the User Policy:
Order of Precedence of Related Features

As with all User Policy authentication settings, this can be overridden by local Computer Policies. There is also a Grace Period without Second Factor Challenge setting on the Computer Policy Proximity Card tab that permits grace periods up to 24 hours for proximity cards only.

A Computer Policy setting that explicitly overrides the User Policy takes first precedence (on that computer).

Order of Precedence of Related Features by Policy

<table>
<thead>
<tr>
<th>Feature</th>
<th>Scope</th>
<th>Online Use</th>
<th>Offline Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Policy</td>
<td>Individual users at any computer, unless overridden.</td>
<td>Always in effect. Default setting is 0 min.</td>
<td>Never in effect</td>
</tr>
<tr>
<td>Computer Policy Override of User Policy</td>
<td>Individual computers assigned this policy. User switch has no effect on other users of kiosk.</td>
<td>Always in effect</td>
<td>Never in effect</td>
</tr>
</tbody>
</table>
Configuring Fingerprint Identification in OneSign

Fingerprint Identification is an optional component of OneSign. While finger biometric verification matches a scanned fingerprint against the records for the individual user, convenient Fingerprint Identification identifies the user by comparing the fingerprint to all other fingerprint records. Upon unique identification, the user is authenticated as well.

Fingerprint identification offers great convenience for users, but many factors affect scan quality and accuracy, including number of scanned fingerprints and the cleanliness of the finger and the scanner. Even with diligent attention, the probability of a false reject or a false positive match is always present. Be sure to educate users on the proper use of the Fingerprint Identification feature.

This chapter contains:

- **Assigning Fingerprint Identification Privileges** on page 42
- **Authenticating to OneSign via Fingerprint Identification** on page 43

**Note:** If the OneSign Administrator Properties page License section does not include Fingerprint Identification settings, then your OneSign license does not include the Fingerprint Identification option.

**Hardware and Server Configuration Requirements**

OneSign fingerprint identification is part of OneSign fingerprint authentication. OneSign fingerprint identification support is handled entirely on the OneSign appliance. There are no connections required to any other servers when you implement fingerprint identification.

Implementing OneSign fingerprint identification is easy. Hardware requirements, enrollment, and most other settings and procedures are the same as for fingerprint verification. To implement finger biometric verification, see **Configuring Fingerprint Verification in OneSign** on page 31.

**Monitoring Fingerprint Identifications**

With the Fingerprint Identification module, you get real-time notifications of fingerprint identification suspensions resulting from failed authentication attempts. These and more helpful notifications are detailed in the **OneSign Administrator Guide**.
Assigning Fingerprint Identification Privileges

With OneSign Fingerprint Identification, users enabled for fingerprint verification automatically get the benefit of fast, secure fingerprint identification without the need to enter a username or select a domain. You assign fingerprint authentication and all other authentication methods through the OneSign User Policies that you assign to each user.

A User Policy that Permits Fingerprint Authentication Automatically Permits Fingerprint Identification if you have the Option

Use computer policies to define the parameters for fingerprint ID failure. Too many consecutively failed fingerprint identification attempts will mean that no further fingerprint identifications are allowed for the specified amount of time on the designated workstation.

Computer Policy Fingerprint Identification Suspension Settings

Revoking Fingerprint Identification Privileges

Revoke fingerprint identification privileges the same way you revoke fingerprint verification and all other authentication methods, through the OneSign User Policies that you assign to each user. Simply assign a different policy to the user.
Authenticating to OneSign via Fingerprint Identification

To authenticate via fingerprint only:

1. Log on to the computer. The Imprivata OneSign logon window appears and prompts you to scan your finger:

![The Fingerprint Identification Screen](image)

2. Scan any enrolled finger and wait for the system to acknowledge the scan. When you have been identified, the authentication window closes and you are logged in.

**Note:** Some users may be prompted to provide a valid username to authenticate in large-scale OneSign deployments in which many fingers are enrolled.
Configuring Passive Proximity Card Authentication in OneSign

OneSign supports passive proximity card authentication with most standard proximity cards and USB card-based readers from RFIdeas Inc.

**Note:** OneSign also supports active proximity card authentication with XyLoc KeyCards, detailed in *Configuring XyLoc KeyCard Authentication in OneSign* on page 53.

This chapter contains:

- Assigning Proximity Card Authentication Privileges on page 46
- Enrolling Users for Passive Proximity Card Authentication on page 47
- Authenticating to OneSign by Passive Proximity Card on page 49
- Locking a Shared Workstation on page 50

Proximity Cards

**Hardware Requirements and Server Connections**

Each proximity card-enabled user needs a card, and each computer that supports proximity card authentication requires a card reader. There are no special server configuration steps when implementing proximity card authentication. Microsoft Windows includes the necessary drivers.

**Two-Factor Authentication with Passive Proximity Cards**

For two-factor authentication, you can require proximity cards to be used with password, OneSign PIN, or fingerprint authentication for some or all users via OneSign user policies. See *Two-Factor Authentication in OneSign* on page 11 for more information.

**Monitoring and Reporting Proximity Card Authentications**

You can get real-time notifications of many network events, including enrollment for proximity card. Event notifications are detailed in the *OneSign Administrator Guide*. 
Assigning Proximity Card Authentication Privileges

You assign proximity card authentication and all other authentication methods through the OneSign User Policies that you assign to each user.

Allowing Users to Enroll a Replacement Card

If you restrict the number of cards assigned to each user, you can allow users with this policy to enroll a replacement card when they log in with it. The new card is effective immediately and all other cards assigned to the user are immediately disabled.

Grace Period without Second Factor Challenge

To configure a grace period for a user to re-authenticate without a second factor challenge, see OneSign FastPass for Fast, Secure Proximity Card Login on page 51.

Revoking Proximity Card Authentication Privileges

Revoke proximity card authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

User policies are detailed in the OneSign Administrator Guide.
Enrolling Users for Passive Proximity Card Authentication

Each user with a proximity card must enroll the card to OneSign before using it to authenticate to OneSign. The enrollment process maps the card number to the user’s OneSign user ID.

When a user tries to authenticate to OneSign with an unrecognized proximity card, OneSign shows the proximity card enrollment screen:

![Enroll Proximity Card - Imprivata OneSign](Image)

Enrolling for Proximity Card Authentication

If multiple proximity cards are detected, then you see a list of detected cards so you can select the user account to log into. If a OneSign PIN has been configured, you must enter and confirm a new OneSign PIN.

**Note:** In some cases, the number which is visible in the OneSign Administrator and in the proximity card enrollment screen does not match the number printed on the proximity card. The mapping used internally by OneSign is unique, consistent, and accurate for all OneSign use; there is no need to change or update the card number.

**Note:** If the Proximity Card logon option is grayed out, check to be sure the proximity card sensor is securely plugged into the computer’s USB port.

Deleting Enrollment Data

You can delete the enrollment data for proximity card users from each user’s user record.
Chapter 9 - Configuring Passive Proximity Card Authentication in OneSign

Deleting Proximity Card Enrollment Data
Authenticating to OneSign by Passive Proximity Card

You can require proximity card users to authenticate with the proximity card and password together, proximity card and fingerprint together, or you can permit them to authenticate with the proximity card alone.

![Login with proximity card image](image)

**Authenticating via Proximity Card and Password**

Users who authenticate with a proximity card alone might see the login screen briefly appear and be dismissed with no need for user input.

If your user policy is configured to use a OneSign PIN, you must enter it at login.

If a proximity card is lost, damaged, stolen, or must be taken out of circulation for any other reason, you can disassociate a card from its enrolled user at the user's user record. The disassociated card remains so until another user enrolls to OneSign with it.

Some RFIdaes proximity card readers can beep to acknowledge the users proximity card. Enable this feature in the Proximity Card tab of the computer policy for affected computers.

![Activating the RFIdaes Beep Feature](image)
Locking a Shared Workstation

Users can lock their shared workstation before they leave it by tapping their passive proximity cards on the reader.

On an unlocked shared computer, the OneSign Agent bubble tells the user who is currently logged in. If another user wants to use this workstation, the user can tap the proximity card once to lock the screen and then tap it again to log in.

To allow a user to lock a computer by tapping a passive proximity card on the reader:

1. In Computer Policies, click the Proximity Card tab.

2. Enable the Allow user to lock computer with Passive Proximity Card option (the default is enabled).

A Computer Policy that Lets a User Lock a Shared Workstation with a Passive Proximity Card on this Computer
OneSign FastPass for Fast, Secure Proximity Card Login

OneSign FastPass™ allows users fast and secure access to shared workstations with the convenient touch of their proximity cards. When FastPass is combined with OneSign’s ability to automatically launch applications, sign users into and out of applications and automate Citrix roaming, OneSign provides users with an unprecedented ability to move quickly, unimpeded by access issues.

Users can quickly and securely log on to different workstations in a facility simply by touching their proximity cards on a reader, without having to type their Windows user name and password every time they log on. Users perform a secure, two-part authentication at the beginning of their work shift by touching their ID badge or building access card on a reader and entering a PIN or password as the second factor. Once this two-factor authentication is completed, FastPass starts an authentication grace period (up to 24 hours), during which the users may access other shared workstations simply by touching their card on a reader. Users only need to enter their PIN or password again when their grace period expires.

You assign the grace period from an **Options** link beside the primary authentication method in the User Policy:
Chapter 9 - Configuring Passive Proximity Card Authentication in OneSign

Order of Precedence of Related Features

As with all User Policy authentication settings, this can be overridden by local Computer Policies. There is also a Grace Period without Second Factor Challenge setting on the Computer Policy Proximity Card tab that permits grace periods up to 24 hours for proximity cards only.

A Computer Policy setting that explicitly overrides the User Policy takes first precedence (on that computer).

Order of Precedence of Related Features by Policy

<table>
<thead>
<tr>
<th>Feature</th>
<th>Scope</th>
<th>Online Use</th>
<th>Offline Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Policy Proximity Card tab</td>
<td>Individual computers with this policy, active and passive proximity card only. User switch resets grace period timer.</td>
<td>Only if User Policy has not been set. Default setting is 20 seconds.</td>
<td>Always in effect</td>
</tr>
<tr>
<td>User Policy</td>
<td>Individual users at any computer, unless overridden.</td>
<td>Always in effect.</td>
<td>Never in effect</td>
</tr>
<tr>
<td>Computer Policy Override of User Policy</td>
<td>Individual computers assigned this policy. User switch has no effect on other users of kiosk.</td>
<td>Always in effect</td>
<td>Never in effect</td>
</tr>
</tbody>
</table>
Configuring XyLoc KeyCard Authentication in OneSign

Imprivata OneSign supports active proximity card authentication with XyLoc™ Locks and KeyCards. The Ensure Technologies’ XyLoc wireless PC security solution requires no additional server configuration steps. The OneSign Agent includes the necessary drivers. This chapter contains:

- Deploying XyLoc Locks and Readers on page 54
- Configuring OneSign Computer Policies for XyLoc Users on page 55
- Assigning XyLoc KeyCard Authentication Privileges on page 57
- Installing the OneSign Agent with XyLoc Support on page 58
- Enrolling for XyLoc KeyCard Authentication on page 59
- Authenticating to OneSign by XyLoc KeyCard on page 60

A XyLoc KeyCard

**Hardware Requirements**

Each keycard-enabled user needs a XyLoc KeyCard, and each computer that supports keycard authentication requires a XyLoc Lock and a OneSign Agent with XyLoc support.

**Two-Factor Authentication with XyLoc Cards**

You can use XyLoc KeyCards with password, fingerprint, or a OneSign PIN. See Two-Factor Authentication in OneSign on page 11 for more information.

**Monitoring and Reporting XyLoc KeyCard Authentications**

You can get real-time notifications of many events, including enrollment for proximity card (includes XyLoc card enrollment). These and many more event notifications are detailed in the OneSign Administrator Guide.
Chapter 10 - Configuring XyLoc KeyCard Authentication in OneSign

Deploying XyLoc Locks and Readers

XyLoc KeyCards emit an RFI signal that is read by all XyLock Locks within range. To ensure smooth login-logout activity, it is important to configure settings properly.

Full information for deploying XyLoc Locks and KeyCards is in your XyLoc documentation, but here is some helpful information to get you started.

Deploying XyLoc KeyCards to Users

XyLoc Locks are very sensitive devices. Desktops, computer and other hardware, and even heavy clothing can attenuate the signal enough to result in a lock signal, or the failure to register an unlock event. To the XyLoc Lock, a KeyCard worn below the level of a desktop might seem as far away as a departing user.

It is important to communicate to your users the best way to wear their KeyCards. KeyCards should always be on a shirt pocket, lapel, or on a lanyard around the neck and not below waist level.

Lock and unlock settings based upon a KeyCard worn in an easily-blocked place can make deployment frustrating.

XyLoc KeyCards should be worn high enough to have a relatively uninterrupted view of the XyLoc Lock as the user approaches the Lock. For example, a KeyCard worn on a belt is obscured from the Lock whenever the wearer sits down.

Deploying XyLoc Locks

This section contains some tips for deploying XyLoc Locks on computers that will be used for OneSign. All XyLoc configuration settings referred to below are set in the Computer Policy > Proximity Card tab. Create a computer policy to suit the different needs of different workstation environments (Roaming Cart vs. Nurse Station).

For best results in all environments:

Place the XyLoc Lock on the front of the monitor, with the LED facing the user.

Start with a default Signal Range of 6 and determine the grace period as described in Delay Screen Lock for on page 55.
Configuring OneSign Computer Policies for XyLoc Users

You can customize settings for users who authenticate to this computer by XyLoc KeyCard by configuring Computer Policies for computers with XyLoc Locks:

Grace Period without Second Factor Challenge

If a proximity card is used along with a second authentication method, you can permit a period during which a user can reauthenticate without the second authentication method. The user must use the same proximity card. This provides user convenience at the expense of security.

Delay Screen Lock for

The computer locks when the proximity card is out of the signal range. In an environment that often requires users to be briefly away from the workstation, constant screen locks can be frustrating. You can delay the locking behavior for up to 20 seconds. This permits the user a degree of flexibility at the expense of security.

If the Lock Delay is long enough for a user to go from one workstation to another, then the user could be logged into two workstations simultaneously, to avoid this, determine the maximum lock delay through direct experience with the users. This is most commonly done by measuring the time it takes for the user to leave the workstation, walk around the room, and return to the workstation.

![Computer Policy: Proximity Card Settings](image)
XyLoc KeyCard

**Signal Range** - XyLoc signal range is a dimensionless value related to the strength of the signal at the reader. The computer is locked if no authorized XyLoc KeyCard is detected within the top range, and unlocked if an authorized XyLoc KeyCard is detected within the bottom range. These values often require some careful adjustment based on actual usage; Lock/Unlock values of 10 and 4 are a good start for many common usage scenarios.

**Display a List of Detected Card(s)?** - OneSign can detect the presence of multiple XyLoc KeyCards within authentication range. If no user is logged into the computer, then OneSign displays a list of detected KeyCards. The user selects the KeyCard that corresponds to the user ID to be used for login. You can configure OneSign to display a list of detected cards under different conditions.

**A single card is detected** - When OneSign detects the presence of a single XyLoc KeyCard within authentication range, if no user is logged into this computer, then:

- **Always display the list** - if the computer should always display the detected proximity card. This can be used as a confirmation before login.

- **Always display the list except when the card that locked the computer is detected within grace period** - if there is no need to display the list when the previous user returns within the grace period.

- **No, don’t display the list** - if OneSign can safely assume the card holder is the user to be authenticated, regardless of the grace period.

**Multiple cards are detected** - When OneSign detects multiple KeyCards within authentication range:

- **Always display the list** - to display all detected KeyCards. The user selects from the list which KeyCard to use for authentication to OneSign.

- **Always display the list except when the card that locked the computer is detected within grace period** - to display the detected KeyCards only if none of the detected KeyCards was the last one logged into this computer. If the most recent user returns within the grace period accompanied by other KeyCard users, then the most recent user is reauthenticated automatically.

**Lock the computer after stationary card is detected for** - A XyLoc reader reads constant minute variations in signal strength from a KeyCard carried by a user, even when the user is sitting still. If the signal remains unchanging or at maximum strength for an extended period, then the card may have been abandoned near the reader, creating a security breach. You can instruct OneSign to lock the computer if a XyLoc KeyCard within the unlock signal range exhibits no change in signal strength for a specified period of time.
Assigning XyLoc KeyCard Authentication Privileges

XyLoc KeyCards are active proximity cards. You assign active proximity card authentication through the Proximity Card section of the OneSign User Policies that you assign to each user.

Revoke XyLoc KeyCard authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

User policies are detailed in the OneSign Administrator Guide.
Installing the OneSign Agent with XyLoc Support

You need to include support for XyLoc devices when installing the OneSign Agent on computers to which users will authenticate using their XyLoc KeyCards.

Installing Support for XyLoc Devices
Enrolling for XyLoc KeyCard Authentication

Each user with a XyLoc KeyCard must enroll the card to OneSign before using it to authenticate to OneSign. The enrollment process maps the card number to the user’s OneSign user ID.

When a user tries to authenticate to OneSign with an unrecognized KeyCard, OneSign shows the Proximity Card Enrollment Screen:

Enrolling for KeyCard Authentication

Deleting Enrollment Data

You can delete the enrollment data for XyLoc KeyCard users from each user’s user record.
Chapter 10 - Configuring XyLoc KeyCard Authentication in OneSign

**Authenticating to OneSign by XyLoc KeyCard**

You can require KeyCard users to authenticate with the KeyCard and password together, with the KeyCard and fingerprint together, or you can permit them to authenticate with the KeyCard alone.

When a user is required to authenticate to OneSign with a XyLoc KeyCard and a second authentication method, OneSign detects the KeyCard first:

Users who authenticate with a KeyCard alone may see the login screen briefly appear and be dismissed with no need for user input. If multiple KeyCards are detected, then you see a list of detected cards so you can select the user account to log into.

If a KeyCard is lost, damaged, or stolen, you can disassociate a KeyCard from its enrolled user from the user record. The disassociated KeyCard remains so until another user enrolls to OneSign with it.
OneSign Authentication for Smart Cards with AD Certificates

Smart cards and USB tokens provide two-factor authentication by combining a user PIN with a pre-programmed smart card. Smart cards are good until the expiration date of the digital certificate on the card, normally valid for two or more years.

- Smart cards with certificates issued by an external agency, described in OneSign Authentication for Smart Cards with External Certificates on page 67.
- Smart cards with certificates issued by Active Directory, described in this chapter.

This chapter contains:

- Server Configuration Requirements on page 62
- Assigning Smart Card/USB Token Authentication Privileges on page 64
- Authenticating to OneSign via Smart Card or USB Token on page 65

A Smart Card and Smart Card Reader

Hardware Requirements

Smart card users need smart cards, and workstations need smart card readers. USB token users need a smart USB token and an available USB port on computers that they log into.

Enrolling for Smart Card/USB Token Authentication

There is no separate enrollment step for Active Directory smart cards. Enrolling for smart card/USB token use in Active Directory automatically enrolls the user for use in OneSign.
Chapter 11 - OneSign Authentication for Smart Cards with AD Certificates

Server Configuration Requirements

OneSign supports smart card authentication via the Windows Local Security Authority and Kerberos. PC/SC-compatible smart card/USB token technology are provided with MS Active Directory. The PKI infrastructure must be installed to support Kerberos security and smart card authentication.

There are four steps to configuring OneSign to work with your Microsoft Active Directory Server smart card/USB token system.

1. Before you begin, it is important to be sure the appliance is configured to communicate with the NTP time server on the domain controller that supports the smart card users. Set this on the NTP tab of the Network page on the Appliance Administrator; see the OneSign Appliance Guide.

2. Configure the Microsoft Active Directory Server to recognize OneSign. See Uploading the Keytab File to the OneSign Server on page 63.

3. Configure OneSign to recognize the Microsoft Active Directory Server smart card system, as detailed in Uploading the Keytab File to the OneSign Server on page 63.

4. Create or edit a security policy that permits smart card use, as detailed in Assigning Smart Card/USB Token Authentication Privileges on page 64

Note: Refer to your Microsoft Active Directory Server documentation for additional information about Kerberos v5 security.

![User Policy that Permits Smart Card or USB Token Authentication Only](image-url)
Uploading the Keytab File to the OneSign Server

OneSign does not have a Kerberos trust relationship with the AD server until you generate and upload a keytab file. If you need to generate a keytab file, see Creating a Kerberos Keytab File on Windows 2000 Server and Windows 2003 Server in the OneSign Documentation Library.

To upload the keytab file to the OneSign Server:

1. On the OneSign Domains tab of the Users page, edit the record for the domain that will host the keytab file.

2. Browse to the keytab file and click Upload.

3. The uploaded keytab file will be copied to all appliances in your OneSign enterprise. For best security, destroy the original keytab file. The only copy should be in the OneSign enterprise.

You can view, upload, and delete the keytab file from a domain record. Click the domain name of any MS Active Directory domain to open its record. Near the bottom, at the right end of the Keytab File line is a View Kerberos Keys link.
Assigning Smart Card/USB Token Authentication Privileges

You assign smart card/USB token authentication (and all other authentication methods) through the OneSign User Policies that you assign to each user.

Revoking Smart Card Authentication Privileges

Revoke smart card authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

User policies are detailed in the OneSign Administrator Guide.
Authenticating to OneSign via Smart Card or USB Token

To log into OneSign, the user inserts the card or token into the reader and then enters the associated PIN. All smart card and smart USB token authentication to the domain is handled by the Microsoft GINA, but the user’s OneSign experience is no different from users with any other authentication method.

The authentication process is straightforward. To authenticate via smart card:

1. At the Windows Log On screen:

   ![The Smart Card Login Window](image)

   The Smart Card Login Window

2. Insert the smart card into the smart card reader.

3. Enter your PIN to enable the smart card. Repeated failure to correctly enter the PIN might disable the smart card.

When you have been authenticated, the login window closes.

If you have multiple authentication options, you first see the OneSign login screen. To log in by smart card, ignore the listed options and insert your smart card as above.
OneSign Authentication for Smart Cards with External Certificates

Smart cards provide two-factor authentication by combining a user PIN with a pre-programmed smart card. OneSign supports:

- Smart cards with certificates issued by Active Directory, described in OneSign Authentication for Smart Cards with AD Certificates on page 61.
- Smart cards with certificates issued by an external agency, described in this chapter. OneSign authenticates users through a 3rd-party application rather than Windows.

This chapter contains:

- Assigning Smart Card Authentication Privileges on page 68
- Overriding User Policies on Select Computers on page 69
- Enrolling for Smart Card Authentication on page 70
- Authenticating to OneSign via Smart Card on page 71

Configuring Smart Card Authentication

There are two steps to configuring smart card authentication for your users:

1. Create or edit a user policy that permits smart card use, as detailed in Assigning Smart Card Authentication Privileges on page 68.

2. Create local overrides to smart card use as necessary with a computer policy, as detailed in Overriding User Policies on Select Computers on page 69.
Assigning Smart Card Authentication Privileges

You assign smart card authentication (and all other authentication methods) through the OneSign User Policies that you assign to each user.

Enforcing Smart Card Certificate Validity

You have the option to prohibit authentication with these smart cards if the card certificate has expired. To do this, check the checkbox under options.

Revoking Smart Card Authentication Privileges

Revoke smart card authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.
Overriding User Policies on Select Computers

You can override the User Policy on individual computers with a Computer Policy:

A Computer Policy with the Override User Policy Enabled to Permit Only Smart Card Authentication
Enrolling for Smart Card Authentication

Smart cards with externally-issued certificates cannot be used for authentication to OneSign until the card certificate has been mapped to a OneSign user during an enrollment process. Enrollment occurs during login/unlock process.

1. The user inserts a smart card to authenticate to the network. The PIN dialog appears:

![The Smart Card Login Window]

2. The user enters a valid PIN.

3. OneSign does not recognize the certificate as one mapped to a OneSign user. OneSign displays the "Enroll smart card" caption of the login or unlock dialog and prompts the user to enter a valid domain password.

![The Smart Card Enrollment Window]

4. The user enters username and password. The PIN dialog appears a second time.

5. The user enters a valid PIN. OneSign validates the certificate and maps the User Principal Name from the certificate to the user.
Authenticating to OneSign via Smart Card

To log into OneSign, the user inserts the card or token into the reader and then enters the associated PIN. The user’s OneSign experience is no different from users with any other authentication method.

The authentication process is straightforward. To authenticate via smart card:

1. When the Windows Log On screen appears, insert the smart card into the smart card reader. The Imprivata Smart Card Login window appears:

   ![The Smart Card Login Window](image)

2. Enter your PIN to enable the smart card. Repeated failure to correctly enter the PIN may disable the smart card.

When you have been authenticated, the login window closes.

If you have multiple authentication options, you first see the OneSign login screen. To log in by smart card, ignore the listed options and insert your smart card as above.
Configuring RSA SecurID Token Authentication in OneSign

OneSign supports ID token authentication with RSA SecurID® tokens with RSA Authentication Manager®.

An RSA SecurID Keyfob

This chapter contains:

- **Server Configuration Requirements** on page 74
- **Assigning SecurID Token Authentication Privileges** on page 78
- **Enrolling for SecurID Token Authentication** on page 79
- **Authenticating to OneSign via SecurID Token** on page 80

---

**Note:** You can find additional documentation regarding OneSign integration with RSA SecurID at http://www.RSASecurID.com

---

**Hardware Requirements**

Each user needs a SecurID token. The tokens are powered by an integral battery and require no user maintenance. Tokens last between 2-5 years. There is no reader; the passcode is entered like a password, along with an optional personal PIN.

**Monitoring and Reporting SecurID Token Authentications**

You can get real-time notifications of a variety of network events, including enrollment for ID tokens.
Server Configuration Requirements

To use ID tokens with OneSign, you must configure OneSign to recognize the ID token server, and the ID token server must recognize the OneSign appliances.

Configuring OneSign to work with an ID token server

There are two steps to configuring OneSign to work with an ID token server:

1. Configure the SecurID token server to recognize OneSign, as detailed in Configuring the RSA Authentication Manager to Recognize OneSign on page 75.

2. Configure the OneSign Server to recognize the SecurID token system, as detailed in Configuring OneSign to Recognize the ID Token Server on page 77.

Implementing OneSign in an existing ID Token environment

ID token-enabled users authenticating to OneSign use their domain usernames instead of their ID token system usernames (these may be the same values anyway). In all other ways OneSign makes no changes to the user experience.
Configuring the RSA Authentication Manager to Recognize OneSign

The RSA Authentication Manager cannot communicate with the OneSign appliance until the RSA Authentication Manager has been configured to recognize it. In the RSA Authentication Manager system, appliances must be deployed as Agent Hosts.

To configure the OneSign appliance as an Agent Host:

1. Open the RSA Authentication Manager Admin UI (Start > Programs > RSA Security > RSA Authentication Manager Host Mode).
2. From Agent Host, select Add Agent Host.
3. In the Add Agent Host screen, enter the host name and network address of the OneSign Appliance.

Adding the OneSign Server as an RSA Authentication Manager Agent Host

4. Use the Group Activations or User Activations buttons to activate any groups or users who will be using OneSign.
5. From RADIUS, select Manage RADIUS Server.
6. Expand RSA RADIUS Server Administration menu and select RADIUS Clients.
7. Click Add.

Adding the OneSign Server as an RSA Authentication Manager RADIUS Client

8. Enter the name, description, and IP address of the OneSign appliance.

9. Enter a shared secret encryption key. You will use the key in step 4 of Configuring OneSign to Recognize the ID Token Server on page 77.

10. Repeat Step 1 through Step 9 to configure all other appliances as agent hosts for the RSA Authentication Manager. Use the same value for the encryption key.

Note: Refer to your RSA Authentication Manager documentation for additional information about the RSA Authentication Manager system.
Configuring OneSign to Recognize the ID Token Server

To configure the OneSign Server to recognize the ID token server:

1. On the **ID Tokens** tab on the Tokens page, click the **Add** button. Host Name, Port, and Encryption Key fields appear.

ID Token Server Setup

2. Enter the **host name** (or IP address) for the ID token server.

3. Enter the **authentication port** for the ID token system RADIUS server.

**Note:** The most commonly used authentication ports are 1812 and 1645. You can find the port number in the RSA Authentication Manager Configuration Management tool, under the entry for RADIUS in the Services section.

4. Enter an **encryption key** that you used in **Step 9** of Configuring the RSA Authentication Manager to Recognize OneSign on page 75.

5. You can specify some **Additional time to wait**... to suit the needs of your users. This is probably not necessary; it is intended for PhoneFactor users. PhoneFactor authentication is described in Configuring PhoneFactor Authentication in OneSign on page 81.
Assigning SecurID Token Authentication Privileges

You assign SafeWord token authentication and all other authentication methods through the OneSign User Policies that you assign to each user.

A User Policy that Permits ID Token Authentication with Emergency Access

Revoking ID Token Authentication Privileges

Revoke ID Token authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

User policies are detailed in the OneSign Administrator Guide.
Enrolling for SecurID Token Authentication

Users who have been authorized for SecurID Token authentication get the opportunity to enroll when they log into OneSign so that OneSign can match their RSA identities to their OneSign identities.

To enroll for SecurID token authentication:

1. Log into the computer to invoke a OneSign authentication.
2. Use your password to log into OneSign.
3. OneSign logs you into Windows and offers you the opportunity to enroll for ID Token authentication. Accept it and click Next. The ID Token Enrollment screen appears:

   ![The ID Token Enrollment Screen]

4. Enter the username for the RSA SecurID system.

   **Note:** The ID token system username may not be the same as your Windows username. Your ID token system administrator will know this information.

5. Enter your passcode (with PIN if required).

6. Click OK.
   Authentication is described in Authenticating to OneSign via SecurID Token on page 80.
Authenticating to OneSign via SecurID Token

Once the user has enrolled, the authentication process is straightforward.

To authenticate via your SecurID token:

1. Log into your computer. The OneSign Log On window appears:

   ![The OneSign ID Token Logon Window](image)

   The OneSign ID Token Logon Window

2. Select the **ID Token** radio button at the bottom of the window.

3. In the **Passcode** field, enter your passcode.

When you have been authenticated, the authentication window closes.
PhoneFactor adds a second factor of authentication to your corporate login. Instead of the user entering a passcode from an ID Token, your PhoneFactor server calls the user’s phone with a passcode and instructions for secure authentication. OneSign supports second-factor authentication with PhoneFactor.

OneSign Supports PhoneFactor Authentication

This chapter contains:

- Configuring OneSign to Work with a PhoneFactor Server on page 82
- Assigning PhoneFactor Authentication Privileges on page 85
- Authenticating to OneSign via PhoneFactor on page 86
Chapter 14 - Configuring PhoneFactor Authentication in OneSign

Configuring OneSign to Work with a PhoneFactor Server

There are two steps to configuring OneSign to work with a PhoneFactor server:

1. Configure the PhoneFactor Agent to recognize OneSign, as detailed in Configuring the PhoneFactor Agent to Recognize OneSign on page 82.
2. Configure the OneSign server to recognize the PhoneFactor system, as detailed in Configuring OneSign to Recognize the PhoneFactor Server on page 84.

Configuring the PhoneFactor Agent to Recognize OneSign

The PhoneFactor Agent cannot communicate with the OneSign appliance until the PhoneFactor Agent has been configured to recognize it. In the PhoneFactor Agent, your OneSign appliances must be deployed as RADIUS clients.

To configure the OneSign appliance as a PhoneFactor RADIUS client:

1. Open PhoneFactor Agent (Start >Programs > PhoneFactor > PhoneFactor Agent).
2. From RADIUS Authentication, make sure the Enable RADIUS authentication checkbox is checked.
3. On the Clients tab, below the list of clients, select Add to add the OneSign server as a RADIUS client.
4. In the Add RADIUS Client window, enter the IP address of the OneSign Appliance. Enter a shared secret encryption key. You will use the key in Step 4 of Configuring OneSign to Recognize the PhoneFactor Server on page 84.
Adding the OneSign Server as a PhoneFactor RADIUS Client

5. (Optional) Check **Require PhoneFactor user match**.

6. Click **OK**.

7. Repeat **Step 1** through **Step 6** to configure all other appliances in your OneSign enterprise as RADIUS clients. Use the **same value** for the shared secret.
Configuring OneSign to Recognize the PhoneFactor Server

To configure the OneSign Server to recognize the PhoneFactor server:

1. On the **ID Tokens** tab on the Tokens page, click **Add**. Configuration fields appear.

   ![ID Token Server Setup](image)

2. Enter the **host name** (or IP address) for the ID token server.

3. Enter the **authentication port** for the ID token system RADIUS server.

4. Enter an **encryption key** that you used in Step 4 of [Configuring the PhoneFactor Agent to Recognize OneSign](#) on page 82.

5. It takes some moments for the user to answer the phone and enter the code. Enter a value in the **Additional time to wait...** field to suit the needs of your users.

6. Leave **Enroll users automatically** selected. Use the username format that matches the usernames in the PhoneFactor Agent users list.

7. Click **Save** to save the configuration.
Assigning PhoneFactor Authentication Privileges

You assign PhoneFactor token authentication and all other authentication methods through the OneSign User Policies that you assign to each user.

PhoneFactor authentication is controlled like an ID Token, so PhoneFactor users must have ID Token authentication checked in their User Policies.

A User Policy that Permits PhoneFactor Authentication with Emergency Access

Revoking ID Token Authentication Privileges

Revoke ID Token authentication privileges through the OneSign User Policies that you assign to each user. Create a different user policy and assign it to the user.

OneSign User policies are detailed in the OneSign Administrator Guide.
Authenticating to OneSign via PhoneFactor

Authenticating to OneSign via PhoneFactor is secure, but it is a little tricky. You use your username and password, but you click the ID Token radio button for increased security.

To authenticate via PhoneFactor:

1. Log into your computer. The OneSign Log On window appears:

2. Enter your username and password normally.

Logging into OneSign and OneSign Anywhere with PhoneFactor

3. Select the **ID Token** radio button at the bottom of the window.

4. Click **OK**, and wait for your phone to ring. Within a few moments, your phone will ring with further instructions. When you have been authenticated, the authentication window closes.

**Note:** PhoneFactor is often used as a second factor for authentication to OneSign Anywhere. You can customize the OneSign Anywhere authentication dialog to make it less tricky for your users. This is detailed in the OneSign Anywhere Guide.
Managing VASCO Digipass Tokens

OneSign provides integrated support for VASCO® Digipass® tokens through the Tokens page as an option controlled by your OneSign license. If there is no Tokens tab at the top of the OneSign Administrator page, then it is not a part of your current license.

Integrated VASCO support includes a suite of management tools for all Digipass tokens described in this chapter, and tools for individual tokens described in Managing an Individual Digipass Token on page 99. This chapter includes:

- Reviewing VASCO Kernel Parameters on page 88
- Using the Tokens Page on page 89
- Importing Digipass Tokens on page 90
- Deleting Digipass Tokens on page 91
- Forcing Digipass ID Token Enrollment on page 93
- Using Password with VASCO Digipass OTP on page 94
- Using Password plus OTP for Remote Authentication on page 95
- Enrolling for Digipass Authentication on page 96
- Authenticating to OneSign via Digipass on page 97
- Managing an Individual Digipass Token on page 98

This License Includes the VASCO Integration Module
Chapter 15 - Managing VASCO Digipass Tokens

Reviewing VASCO Kernel Parameters

To review the VASCO kernel parameter values from the VACMAN controller, click Configure Kernel Parameters on the Properties page:

Accessing the VASCO Kernel Parameters Window

Click Click here to configure kernel parameters.

VASCO Kernel Parameters

Note: Consult your VACMAN documentation before changing these values.
Using the Tokens Page

Use the Tokens page to manage Digipass tokens. All Digipass tokens that you import into OneSign appear on the Tokens page.

The Tokens Page

To sort the tokens listed on the Tokens page by token Serial Number, Assignment Status, or Digipass model, click on the column heading.

If you have a long list of tokens, you can search by Serial Number and by Assignment Status (Available, Assigned, and Lost).

When searching by serial number, the search looks for any Digipass serial number that contains the string you type. This means you can type a portion of a serial number to display a list of tokens that include that string.
Importing Digipass Tokens

You can import Digipass tokens at any time. You can have an unlimited number of Digipass tokens on the Tokens page, but you can only enable as many users as you have OneSign licenses.

To import Digipass tokens, you need:

- the shipping code
- a .DPX file

**Note:** If the tokens are configured to support multiple applications, then you need to know which application pertains to .

To import tokens:

1. On the Tokens page, click **Import**. A window appears:

   ![Importing a DPX file with Digipass Token Records](image)

2. Enter the shipping code.

3. Select if the tokens are preconfigured for one application only () or if they are configured for multiple applications. If they are configured for multiple applications, then use the text field provided to enter the application name or number that is reserved for .

4. Browse to and upload the .DPX file.
Deleting Digipass Tokens

You can delete Digipass tokens when you remove the physical tokens from service. If you want to reassign a token, then do not delete the token but instead change its status as described in Changing Token Status on page 100. You can change status to lost, available, or assigned to another user.

To delete Digipass tokens, select them on the Tokens page and click Delete.
Chapter 15 - Managing VASCO Digipass Tokens

**Resetting Multiple Digipass Token PINs**

You can perform a bulk reset operation for multiple Digipass static token PINs, which immediately clears static pins on selected tokens. This feature allows users with new tokens to set their PINs themselves at login.

To reset multiple token pins:

1. On the Tokens page, select multiple tokens.
2. Click **Reset PIN**. A message prompts you to confirm resetting the PINs to zero digits.
3. Click **OK**. The user will need to enter a new PIN at login.
Forcing Digipass ID Token Enrollment

Users who authenticate to OneSign via Digipass must use a Digipass that is enrolled to OneSign. If the Digipass was not preassigned, then the user must self-enroll it before it can be used for authentication. In this case, the user is prompted to enroll at login.

The Digipass Enrollment Dialog

Under normal circumstances, a user authorized for Digipass authentication can defer the Digipass enrollment step indefinitely, always authenticating by password. You can require users to enroll their Digipasses by using the Lock computer if user cancels enrollment? feature in a User Policy.

Forcing ID Token Enrollment

After you save the policy, it will be downloaded to the OneSign Agents of affected users as each Agent reaches its next refresh interval. On authentication to OneSign, the user is prompted to enroll the ID token. The prompt remains for two minutes of inactivity, after which the computer locks, forcing re-authentication.

If this feature is required only on select computers, you can implement this feature through Computer Policies, restricting access to specific computers to enrolled Digipass users.
Using Password with VASCO Digipass OTP

Digipass (One Time Password) OTP plus password authentication provides secure two-factor authentication for PIN-less Digipass users by employing the user's Windows network password as a PIN. You can use the same OneSign User Policy for both types of Digipass users:

**Note:** **OTP+Password authentication is supported only for VASCO Digipass ID tokens. It is not supported for other ID tokens.**

You assign authentication options through User Policies, and you can override them locally with Computer Policies. User Policies and Computer Policies are described in the *OneSign Administrator Guide*.

A User Policy Requiring Password Login in Conjunction with Digipass Passcode

You set remote authentication options separately from local authentication options. Requiring OTP+Password for local authentication does NOT automatically set the same requirement for remote authentication. To require password with OTP for remote authentication, see *Using Password plus OTP for Remote Authentication* on page 95.
Using Password plus OTP for Remote Authentication

You can require password-plus-OTP authentication only for remote users, or permit remote users to use OTP alone. Make the setting in the Remote Network Authentication section.

A User Policy Requiring Password for Remote Login with Digipass
Enrolling for Digipass Authentication

Digipass users must self-enroll or be enrolled by a system administrator. This section describes user self-enrollment. To assign a Digipass to a user, see Assigning a Digipass to a User on page 102.

To self-enroll a Digipass to OneSign:

1. Log into the computer to invoke a OneSign authentication.
2. Use your password to log into OneSign.

OneSign logs you into Windows and offers you the opportunity to enroll for ID Token authentication. Accept it and click Next. The ID Token Enrollment screen appears:

![Image of the ID Token Enrollment screen]

### The Digipass Enrollment Screen

3. In the **serial number** field, enter the serial number of your Digipass. The serial number is located on the back of your token.

4. Enter the passcode on your Digipass in the Passcode field.

---

*Note: If you have a PIN number associated with your Digipass, enter it with your passcode. For more information, contact your Digipass system administrator.*

5. Click **OK** to complete the enrollment process.

You have successfully enrolled your Digipass. For instructions on authenticating to OneSign with your Digipass token, see Authenticating to OneSign via Digipass on page 97.
**Authenticating to OneSign via Digipass**

Once the user has enrolled, the authentication process is straightforward.

To authenticate via Digipass:

1. Log into the computer. The OneSign Log On window appears:

   ![Logging in with a Digipass](image)

   **Logging in with a Digipass**

2. Select the **ID Token** radio button at the bottom of the window.

3. In the **Passcode** field, enter the passcode shown on the Digipass display.

4. Click **OK**.

When you have been authenticated, the authentication window closes.

**Two-Factor Authentication**

If you have a PIN or a password, include it with your passcode. Enter a PIN or a password immediately before the passcode. For example, if the PIN or password is “1234” and the passcode is “98765”, then enter “123498765” in the passcode field.
Managing an Individual Digipass Token

The Digipass record page shows information about a specific Digipass token, including the username of the user currently assigned to it and an image of the token. Each VASCO Digipass has its own VASCO Token page.

You can use OneSign to manage Digipass tokens in many ways. The OneSign tools for managing VASCO Digipass tokens are detailed in Managing an Individual Digipass Token on page 99.

Note: Digipass users can be enabled for Offline Mode through their security policies. For more on offline mode, see the OneSign Administrator Guide.
Managing an Individual Digipass Token

The Digipass detail page shows information about the Digipass, including the username of the user currently assigned to it and an image of the token. You can use to manage Digipass tokens in many ways:

- **Changing Token Status** on page 100
- **Changing a Static PIN** on page 104
- **Using Virtual Tokens** on page 109
- **Other Operations** on page 110
- **Generating and Viewing a Token Activity Report** on page 116

A Token Detail Page

Digipass users can be enabled for Offline Mode through their security policies. For more on offline mode, see the *OneSign Administrator Guide*.
Chapter 16 - Managing an Individual Digipass Token

### Changing Token Status

Every Digipass token must have one of three statuses:

- **Available** tokens are valid, licensed, and ready for use, but not yet assigned to any user. Available tokens cannot be used to authenticate to.

- **Lost** tokens are no longer in the custody of an authorized person, and may be in the possession of an unauthorized person. This is a potential security breach, so tokens with Lost status are disabled. Lost tokens cannot be used to authenticate to.

- **Assigned to a user** have been assigned to an authorized user. These tokens cannot be deleted from OneSign until their status is changed to Available or Lost.

You can change the status of any token at any time, as described in:

- Assigning Available Status to a Digipass on page 101
- Assigning a Digipass to a User on page 102
- Assigning Lost Status on page 103
Assigning Available Status to a Digipass

To assign Available status to a Digipass:

1. From the Tokens page, click the serial number of the Digipass token to open the Digipass token detail page.

2. In the Assignment Status section, select Available:

3. Click Save.
Assigning a Digipass to a User

To assign an available Digipass to a user:

1. From the Tokens page, click the serial number of the Digipass token to be assigned to open the Digipass token detail page.

2. In the Assignment Status section, select Assigned to:

3. Enter the username and domain information of the user.

4. Click Save.

**Note:** If you assign a second token to a user, OneSign automatically unassigns the first token.
Assigning Lost Status

To assign Lost status to a Digipass:

1. From the Tokens page, click the serial number of the Digipass token to open the Digipass token detail page.

2. In the Assignment Status section, select **Lost**: 

![Assigning Lost Status](image)

3. Click **Save**.

When a token is no longer in the custody of an authorized person, then it may be in the possession of an unauthorized person. This is a potential security breach, so tokens with Lost status are disabled.
Changing a Static PIN

Some VASCO Digipass tokens support a static PIN feature. A static PIN is a personal code of preset length that is used in conjunction with the Digipass passcode to permit higher security.

Because the Digipass passcode is dynamic (so it cannot be memorized) and the user’s PIN is static but (under normal circumstances) is never written down, a Digipass token that comes into the hands of an unauthorized user cannot be used to authenticate to your network. In the same way, an intruder who learns a user’s static PIN cannot access the network without having the physical token as well.

If the Digipass supports the VACMAN static PIN feature, then there are three conditions that come preconfigured on the token:

User may never change static PIN on page 105
User must change PIN immediately and may change later on page 106
User may change PIN at any time on page 107

These settings have different security values, so it is important to understand which configurations best suit your users.

There is an additional tool for the administrator:

Resetting and Changing a Static PIN on page 108
User may never change static PIN

Forbidding the user from changing the PIN ensures the PIN is always known to the administrator:

A Digipass with Static PIN Support

This is more a matter of policy than of usability. There is a separate reset function for use when a user changes the PIN and then forgets it or if a token is reassigned. The reset function is detailed in Resetting and Changing a Static PIN on page 108.

These settings are determined by the .DPX file contents set by the manufacturer based on parameters chosen by the Digipass purchaser.
User must change PIN immediately and may change later

Digipass tokens on which the user is required to change the PIN ensures the PIN is known only to the user. The administrator cannot know the PIN after it has been changed.

A Digipass with Static PIN Support that Forces the User to Change the PIN on First Use and Allows the User to Change the PIN at Any Time

If a user changes the PIN and then forgets it, or if a token is reassigned, see Resetting and Changing a Static PIN on page 108.
User may change PIN at any time

Digipass tokens on which the user is permitted but never required to change the PIN makes it possible for the PIN to be known to both the user and to the administrator only until the user changes the PIN. Users are more likely to remember PINs they set themselves.

A Digipass with Static PIN Support that Allows the User to Change the PIN at Any Time

If a user changes the PIN and then forgets it, or if a token is reassigned, see Resetting and Changing a Static PIN on page 108.
Chapter 16 - Managing an Individual Digipass Token

**Resetting and Changing a Static PIN**

If a user changes the static PIN and then forgets it, or if a token is reassigned, you can reset the PIN to nothing at all, a string value of zero length. Not all Digipass tokens support the static PIN feature.

![Resetting a Static PIN](image)

When the PIN has been reset in this manner, the administrator can assign a new PIN by entering and confirming it in the **Change Static PIN** fields.

**Changing a static PIN**

To change the static PIN:

1. Open the token record and scroll down to the Static PIN section.

   ![Changing a Static PIN](image)

   **Note:** Do not click the Reset PIN button.

2. Enter the new PIN in the **New PIN:** field. Confirm the new PIN in the **Confirm PIN:** field. There is no need to enter the old PIN.

3. Click **Change PIN**.

**Users changing the static PIN**

Users can change a PIN in the OneSign ID token login screen in the PIN + Passcode field: enter the old PIN, the passcode, and the new PIN in the following format, with no spaces:

```
OldPINpasscodeNewPINNewPIN
```

If the old PIN was reset (now is of zero length), then enter only:

```
PasscodeNewPINNewPIN
```
Using Virtual Tokens

Virtual tokens are useful when an authorized user has forgotten or lost a Digipass token and needs access to the network.

**Note:** Not all Digipass tokens support the Virtual Token feature. The Virtual Token feature comes programmed into the token, you cannot assign the Virtual Token feature from.

To generate a one-time password:

1. Open the token record and scroll down to the Virtual Token section.

   ![A Digipass with Virtual Token Support](image)

   **A Digipass with Virtual Token Support**

   Click **Generate** to generate a new one-time password.

2. The One-Time Password appears to the right of the button. The one-time password can be used just like the passcode generated by the Digipass token.

   ![Generating a One-Time Password for a Virtual Token](image)

   **Generating a One-Time Password for a Virtual Token**

   **Note:** Do NOT test the new one-time password in the Test One-Time Password field! The Test One-Time Password field is for troubleshooting tokens.

   ![Do Not Test the New One-Time Password](image)
Other Operations

At the bottom of the Digipass token record is a token-sensitive set of other operations. Not all of these operations will appear; their availability depends upon whether or not the token supports them:

If you are testing one-time password functionality on a token, see Testing a Token’s One-Time Password on page 111.

A Digipass can become disabled after passing the inactive days setting (see Reviewing VASCO Kernel Parameters on page 88) or as a result of an accumulation of minor errors over time. If a user’s Digipass has become disabled, the easiest solution is to try resetting it, described in Resetting a Disabled Digipass on page 114.

If a Digipass shows a lock code on its screen, then you can unlock it with the procedure in Unlocking a Digipass on page 115.
Testing a Token’s One-Time Password

When you reassign a token to another user, it is a good idea to test the token first. OneSign permits you to test the token by using it to authenticate against the Test One-Time Password field.

There are two types of one-time password functions, depending on which type of token you are testing:

- Testing a Response-Only Digipass on page 112
- Testing a Challenge-Response Digipass on page 113

The token type is listed on the token information section of the token record:

Identifying the Token Type
Chapter 16 - Managing an Individual Digipass Token

Testing a Response-Only Digipass

It is a good practice to test a Digipass before assigning it to a user.

To test a response-only Digipass:

1. Open the token record for the Digipass to be tested.
2. In the Test One-Time Password field, enter the token PIN and a passcode generated by the token.

A Successful Token Test
Testing a Challenge-Response Digipass

It is a good practice to test a Digipass before assigning it to a user.

To test a challenge-response Digipass:

1. Open the token record for the Digipass to be tested.
2. In the Test One-Time Password line, click **Generate Challenge Code**.

Generating a Challenge Code

3. generates a challenge code:

Testing a One-Time Password for a Challenge-Response Digipass

4. Using the Digipass keypad, enter the challenge code into the Digipass. The Digipass generates a one-time password.
5. Enter the one-time password from the Digipass in the test field.
6. Click **Test**.
Resetting a Disabled Digipass

Each Digipass maintains an internal error counter designed to disable it if it has been misused. Sometimes a Digipass can become disabled through ordinary usage under extraordinary circumstances when the error count gets too high.

To reset a disabled Digipass, push the **Reset Token** button. The error counters are immediately reset to zero.

If resetting the token error counters does not make the token serviceable again, then assign the user a new token.

Resetting the token error counters has no effect on the static PIN. To reset the token static PIN, see **Resetting and Changing a Static PIN** on page 108.
Unlocking a Digipass

If a user locks a Digipass by repeatedly entering the wrong PIN into the token, you can generate a PIN that the user can use to unlock it. This operation can be handled over the telephone.

To unlock a locked Digipass:

1. The token says LOCK and shows a passcode. Enter the passcode in the Unlock Token field.

2. Click **Generate Unlock PIN**. A new PIN appears:

3. Enter the new unlock PIN in the token. This unlocks the Digipass for normal use. The Digipass returns to normal functionality.
Chapter 16 - Managing an Individual Digipass Token

Generating and Viewing a Token Activity Report

A token report is a specific kind of OneSign report that shows Digipass activity for this token for a period of time that you set before running the report.

When you click View Token Report, you are brought to an Add New Report page where you can name the report (if you plan to save it), and specify a date range.

A Token Report

OneSign reports are detailed in the OneSign Administrator Guide.
Index

A
ACE/Server, see RSA Authentication Manager
Agent Host, RSA Authentication Manager, configuring OneSign Server as 75
Assigned to user status, for a Digipass 102
assigning authentication privileges
  fingerprint authentication 33
  ID token 78
  PhoneFactor 85
  proximity card 46
  smart card (AD) 64
  smart card (third-party, government) 68
  XyLoc KeyCard 57
Assignment Status, Digipass 89
Authenticate With Fingerprints screen 38
authentication
  active proximity card 6, 53
  authenticating with a smart card or USB token 65
  Digipass 97
  fingerprint 31
  invoking a OneSign authentication demand 79
  methods of, for users 1
  passive proximity card 5, 45
  password 2
  PhoneFactor 86
  SecurID token 8, 80, 96
  smart card 2, 61, 62, 67
  USB token 2, 61, 62, 67
  XyLoc KeyCard 6, 53
  authentication ports, SecurID 77
Available status, for a Digipass 101

B
beep feature, RFIdeas proximity card readers 49

C
camera, for OneSign Secure Walk-Away 24
certificate, smart card, deleting 68
challenge code, for testing challenge-response-type Digipass 113
changing a Digipass PIN
  user forbidden 105
  user permitted 107
  user required 106
computer policies
  overrides of user policy authentication settings 33
  to bypass unreachable physical access system 22
  XyLoc authentication 55
countdown balloon 25
countdown to session lock 25
Customer Support, Imprivata, contacting ii
delining a user’s smart card certificate 68
deleting Digipass token records 91
deleting emergency access data for a user 17
Digipass
  assigning Available status 101
  assigning Lost status 103
  assigning to a user 102
  deleting 91
determining type 111
disabled 103, 110, 114
derror counters 114
importing into OneSign 90
inactive days setting 110
managing 89
OneSign optional module 87
one-time password 109
record page 98, 99
running an activity report 116
serial number or model 89
static PIN 106, 107
testing OTP before reassignment 111
types of tokens 111
unlocking 115
user forgot or lost, needs access 109
virtual 109
disabled Digipass 110, 114
disabling a smart card accidentally 65
disassociating a proximity card from its enrolled user 49
disassociating a XyLoc KeyCard from its enrolled user 60
drivers, for proximity card use 45

E
emergency access
deleting user data 17
resetting counter 18
revoking 17
emergency access privileges
about 15
assigning and revoking 16
deleting 17
lockouts 18
resetting lockouts 18
restricting at some computers 18
settings for 16
encryption key 77, 84
enrollment
active proximity card 59
fingerprint authentication 34
passive proximity card 47
password 2
Safeword ID token 79
smart card or USB token 61
Ensure Technologies XyLoc cards 6, 53
error counters, Digipass 114

F
fingerprint
authentication privileges, assigning and revoking 33
how to record a fingerprint 38, 43
scanner 3, 32, 33, 35, 42
Fingerprint Enrollment screen 34
Fingerprint Identification (option module) 4, 41
fingerprint scanner, illustrated 32

G
GINA desktop login module 65
grace period for users 25

H
hands image screen 34
hardware requirements
for passive proximity card authentication 45
for SecurID token authentication 73
for smart card authentication 61
for USB token authentication 61
for XyLoc KeyCard authentication 53
HID proximity cards 5

I
ID token
configuration procedure overview 74
configuring OneSign to recognize SecurID
token server 77, 84
configuring RSA Authentication Manager 75
supported tokens 8
identification, fingerprint 3
importing Digipass tokens 90
inactive days setting (VACMAN) 110
Indala proximity cards 5

K
Kerberos security trust, required for smart card authentication 7, 62
keytab file 63

L
limit of emergency access usage, waiving 18
lock code, Digipass 115
lock/unlock a desktop by tapping a proximity card 50
locking a shared workstation 50
Log On window
  fingerprint 38
  PhoneFactor 86
  proximity card 49
  SafeWord 80
  smart card (AD) 65
  smart card (government/third-party) 71
login screen flashing by, with proximity card authentication 49
Lost status, for a Digipass 103

M
Microsoft Active Directory Server, Windows Local Security Authority from 7, 62
multiple applications configured to a Digipass 90
multiple authentication options, when smart card or USB token is an option 65

N
notification, fingerprint identification failure 41

O
OneSign
  authentication methods 1
  Log On window with PhoneFactor 86
  Log On window with SafeWord token 80
  Log On window with smart card 65
  VASCO Integration option 87
OneSign appliance
  as PhoneFactor RADIUS client 83
  as RSA Agent Host 76
OneSign PIN 12, 31
OneSign ProveID
  about 27
  mapping an application 28
  mapping multiple applications 29
OneSign server
  to configure for use with a PhoneFactor system 84
  to configure for use with a SecurID token system 77
  to configure for use with a smart card or USB token system 63
one-time password, for virtual Digipass user 109
one-to-many user identification 4, 42
OTP-plus-password authentication, Digipass local 94
  remote 95
Override User Policy tab, of a computer policy 33

P
passcode 73, 79, 80, 86
password authentication 2
password-plus-OTP authentication, Digipass local 94
  remote 95
PhoneFactor
  configuration procedure overview 82
  configuring OneSign to recognize PhoneFactor 84
  configuring to recognize OneSign 82
  introduction 81
physical access, user policies to bypass temporarily unreachable physical access system 22
PIN, for Digipass, see static PIN
PKI infrastructure 62
port number, for RSA Authentication Manager 77
ProveID, see OneSign ProveID
proximity card
  and two-factor authentication 49
  authentication failure, notification of 45
  grace period 55
  passive proximity card authentication 5, 45
  user enrollment, passive proximity card 47
  user enrollment, XyLoc active proximity card 59
  proximity card, permit user to enroll replacement at login 46

R
RADIUS client, PhoneFactor, configuring OneSign Server as 82
reassigning a Digipass, testing first 111
remote Digipass users 95
replacement proximity card, permit user to enroll at login 46
replacing emergency access questions 17
reporting Digipass activity 116
resetting an individual Digipass token 114
revoking authentication privileges
emergency access 17
fingerprint authentication 33
ID token 78
PhoneFactor 85
proximity card 46
smart card 64, 68
XyLoc KeyCard 57
RFIdeas beep feature 49
RFIdeas, Inc proximity card readers 45
RSA ACE/Server, see RSA Authentication Manager
RSA Authentication Manager
configuring 75
selecting port number for RADIUS service 77
supporting RSA SecurID tokens 73
RSA SecurID tokens 8, 73
Secure Computing PremierAccess
about 8
Secure Computing RemoteAccess
about 8
Secure Computing SafeWord tokens 8
Secure Walk-Away, OneSign 24
SecurID token, about 73
securing a workstation 25
server connections
active proximity card authentication 53
fingerprint authentication 32, 41
passive proximity card authentication 45
RSA ACE/Server 74
shipping code, Digipass 90
signal range, for XyLoc KeyCards 56
smart card
and USB token authentication 62
authentication, not shown on login screen 65
configuration procedure overview 62
illustrated 62
usable period 7
static PIN
changing 108
known to administrator 105
procedure for users to change 108
resetting to zero length 108
unaffected by reset operation 114
unknown to administrator 106
Support, Imprivata, contacting ii
T
tapping a proximity card to lock/unlock a desktop 50
telephone number, Imprivata ii
testing a Digipass 112, 113
testing one-time password on a Digipass 110
token reports (VASCO Integration option only) 116
tokenless two-factor authentication, see PhoneFactor
Tokens page (VASCO Integration option only) 87, 89
tokens, see ID tokens, see also Digipass
tutorial, for OneSign Secure Walk-Away 25
two-factor authentication
with fingerprints 31
with passwords 2
with PhoneFactor 81
with proximity cards 49
with smart cards 61, 67
with USB tokens 61, 67
with XyLoc KeyCard 60
Secure Walk-Away, OneSign 24
unlock PIN, for Digipass token 115
unlocking a locked Digipass 115
USB port 32
user policies, to bypass a physical access system if it is unreachable 22
V
VACMAN
controller 88
static PIN 104
VASCO Integration overview 87
VASCO kernel parameter values 88
verification
fingerprint 31
restricting fingerprint 34
View Kerberos Keys link 63
virtual Digipass 109

W
waiving emergency access limit 18
Windows Local Security Authority 7, 62
wireless PC security, XyLoc 53
workstation, unattended, securing with One-Sign Secure Walk-Away 24

X
XyLoc KeyCard, authentication failure, notification of 53
XyLoc KeyCard, signal range 56
XyLoc Lock 53