VASCO
THE AUTHENTICATION COMPANY

DIGIPASS
authentication

DIGIPASS Authentication for Windows Logon

Product Guide

1.1

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

Trademarks

VASCO®, Vacman®, IDENTIKEY®, aXsGUARD®, DIGIPASS®, and ® are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Table of Contents

1 Overview

1.1 Windows Logon with a DIGIPASS

DIGIPASS Authentication for Windows Logon is a product that allows a User to log on to Windows using a DIGIPASS.

DIGIPASS Authentication for Windows Logon integrates seamlessly with the existing Windows logon system. The User ID is entered along with a One Time Password generated by the DIGIPASS. The existing Windows static password is released and passed to the Windows logon system. The DIGIPASS Authentication for Windows Logon product securely stores the Windows static password using strong encryption.

1.2 What is a DIGIPASS?

A DIGIPASS Authentication for Windows Logon token is a device for providing One Time Passwords to a User.

A DIGIPASS Authentication for Windows Logon token may be provided to each person whom an organization wishes to be able to log into their system using a One Time Password (OTP). The User obtains an OTP from the DIGIPASS Authentication for Windows Logon token to use instead of, or as well as, a static password when logging in.

For more information about DIGIPASS Authentication for Windows Logon, refer to the DIGIPASS section of the IDENTIKEY Server Product Guide.

1.3 How does DIGIPASS Authentication for Windows Logon Work?

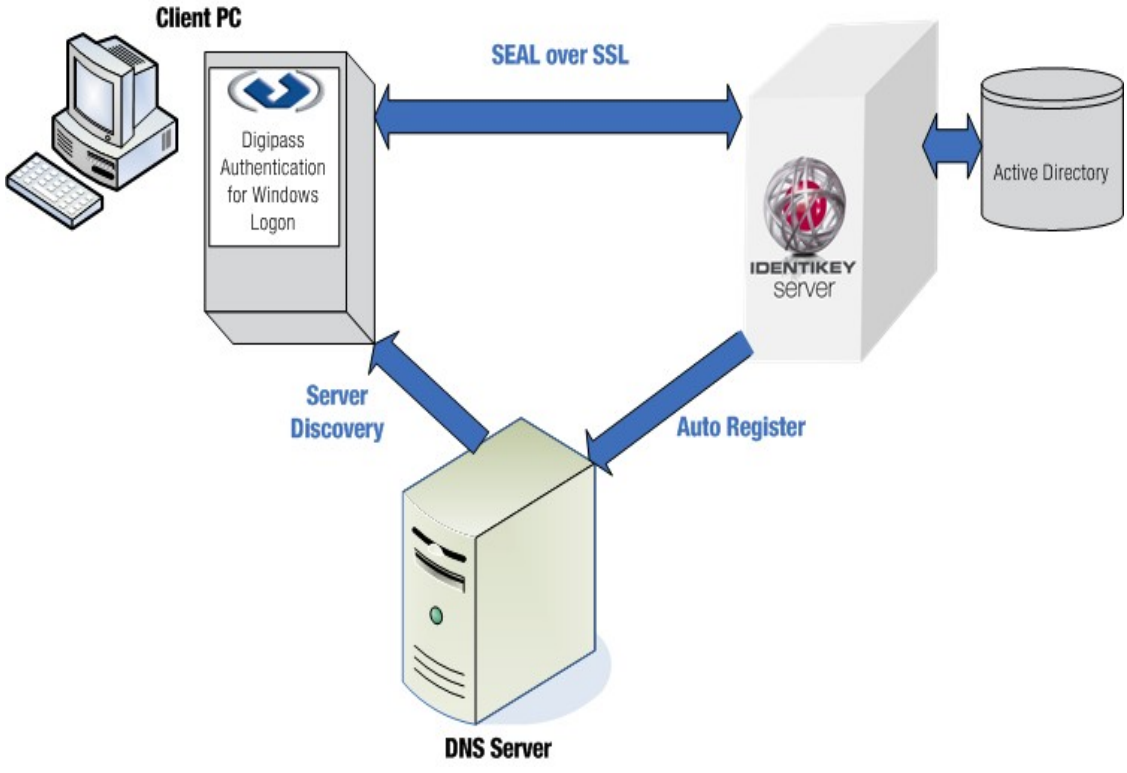

Image 1: DIGIPASS Authentication for Windows Logon Overview Architecture

1.3.1 Components

Client PC

The client PC contains the DIGIPASS Authentication for Windows Logon client module.

Windows Logon Client

The Windows Logon client module collects the authentication credentials entered by the User. It performs a DNS lookup to locate the correct IDENTIKEY Server. The Windows Logon client module delegates OTP validation to IDENTIKEY Server.

IDENTIKEY Server

During advanced installation, the IDENTIKEY Server automatically registers its location with the DNS Server, enabling the Windows Logon client to automatically locate it. The IDENTIKEY Server recieves input from the Windows Logon client and processes the authentication request. It sends the authentication request results back to the client PC.

1.4 DIGIPASS Authentication for Windows Logon Components

DIGIPASS Authentication for Windows Logon consists of Client Components and Server Components. The Client Components are installed on the Client PC and the Server Components are part of IDENTIKEY Server.

1.4.1 Client Components

The Windows Logon Client Module is installed on the Client PC.

The Client Module contains:

- Windows Logon
- Tray Application

For more information, refer to the following sections of the DIGIPASS Authentication for Windows Logon User Manual:

- Understanding DP Windows Logon
- Using DP Windows Logon Tray Agent

1.4.2 Server Components

The DIGIPASS Authentication for Windows Logon Server components are:

- IDENTIKEY Server
- Web Administration Interface
- Active Directory Users and Computers Extension
- Audit Viewer
- TCL Command Line Application
- Password Synchronization Manager (PSM)

Refer to the Server Components section of the IDENTIKEY Server Product Guide for more information.

1.4.3 Communication Protocols

All communication between the DIGIPASS Authentication for Windows Logon and IDENTIKEY Server takes place using SEAL, over SSL.

1.5 Available Guides

The following DIGIPASS Authentication for Windows Logon guides are available:

DIGIPASS Authentication for Windows Logon Product Guide

The Product Guide will introduce you to the features and concepts of DIGIPASS Authentication for Windows Logon and the various options you have for using it.

DIGIPASS Authentication for Windows Logon Getting Started Guide

The Getting Started Guide will lead you through a standard setup and testing of key DIGIPASS Authentication for Windows Logon features.

DIGIPASS Authentication for Windows Logon User Manual

For users of DIGIPASS Authentication for Windows Logon.

DIGIPASS Authentication for Windows Logon Installation Guide

The Installation Guide will help you install and configure DIGIPASS Authentication for Windows Logon to your requirements.

1.5.1 IDENTIKEY Server Guides

The following guides are available for IDENTIKEY Server:

Product Guide

The Product Guide will introduce the features and concepts of IDENTIKEY Server and the various options you have for using it.

Windows Installation Guide

Use this guide when planning and working through an installation of IDENTIKEY Server in a Windows environment.

Linux Installation Guide

Use this guide when planning and working through an installation of IDENTIKEY Server in a Linux environment.

Administrator Reference

In-depth information required for administration of IDENTIKEY Server. This includes references such as data attribute lists, backup and recovery and utility commands.

Getting Started Guide

The Getting Started Guide will lead you through a standard setup and testing of key IDENTIKEY Server features.

Performance and Deployment Guide

Contains information on common deployment models and performance statistics.

Help Files

Context-sensitive help accompanies the Administration Web Interface and DIGIPASS Extension for Active Directory Users and Computers.

SDK Programmers Guide

In-depth information required to develop using the SDK.

2 User Authentication

User One Time Password Authentication can be performed either online or offline

2.1 Online One Time Password Authentication

For Online OTP Authentication the client machine is connected to the Windows Domain and the DIGIPASS OTP is used to logon to the Windows Domain.

Online OTP Authentication is perfomed by the IDENTIKEY Server.

2.1.1 Process

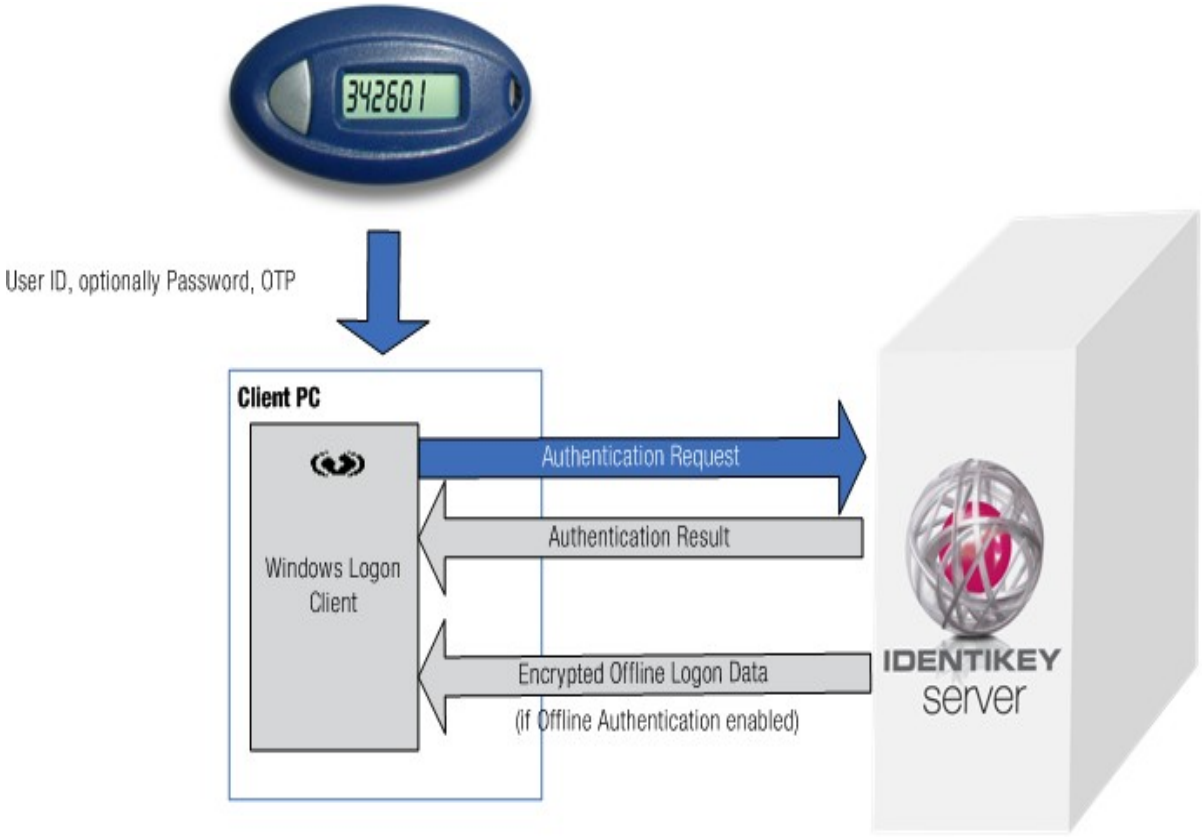

Image 2: Online Authentication Data Flow

Online Authentication begins with the User entering their User ID, Password (optional) and OTP. This passes through the Windows Logon client to IDENTIKEY Server. IDENTIKEY Server validates the authentication credentials and generates an authentication result. This Authentication result includes the Windows static password which is used by the Windows Logon Client to perform a Windows domain logon.

If Offline Authentication is enabled, IDENTIKEY Server also passes encrypted offline logon data back to the Client PC. The encrypted offline logon data is used in Offline Authentication. See 2.2 Offline One Time Password Authentication for further details about Offline Authentication.

2.2 Offline One Time Password Authentication

With Offline One Time Password Authentication the Client machine is not connected to the Windows domain, and the DIGIPASS OTP is used to logon to the local client machine. Offline OTP authentication will authenticate a logon using the Windows Logon client on the Client PC and encrypted offline logon data. This encrypted logon data is generated by IDENTIKEY Server during Online Authentication.

See 2.1 Online One Time Password Authentication for further information about Online Authentication.

2.2.1 Process

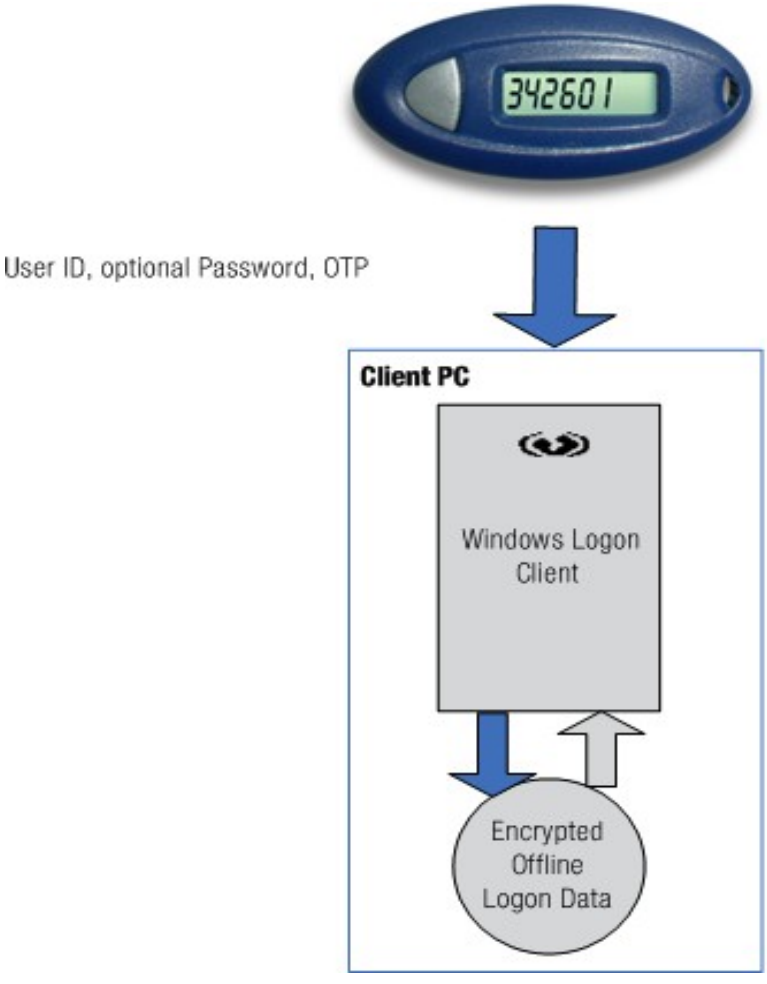

Image 3: Offline OTP Authentication

Offline OTP Authentication begins with the User entering their User ID, optional Password and OTP. These login credentials pass through the Windows Logon client module. The Windows Logon client module performs the following checks:

- Is Offline Authentication Data available for the User? Offline Authentication Data is generated after a successful Online Authentication when Offline Authentication is enabled in the Identikey Windows Logon policy.
- Is the Offline Authentication data still valid? Offline Authentication Data is valid for a limited time for time-based data, or a limited number of logons for event-based data. The time or event limit is defined on the Windows Logon Policy.
- Does the OTP validation succeed with the Offline Authentication Data?

2.2.2 Disable Offline Authentication

When Offline Authentication is disabled for a User, be aware of the following:

- Disabling Offline Authentication for a User means that IDENTIKEY Server will not send any new Encrypted Offline Logon Data to the client PC
- Disabling Offline Authentication for a User means that the User will still be able to use Offline Authentication from the time that it is disabled until the Encrypted Offline Logon Data has expired OR until the User performs their next Online Authentication.

2.3 Force OTP Use

A User may be forced to logon either online or offline using an OTP by utilizing settings in the Windows Logon Client Module. For details on configuring this, refer to the Enforcing DIGIPASS authentication section of the Windows Logon User Manual.

3 DIGIPASS Authentication for Windows Logon Features

3.1 Dynamic Component Registration

IDENTIKEY Server requires a client component to be registered for each incoming authentication request.

> **Note**
>
> Only English ASCII characters are supported for computer names.
>
> Names containing non-ASCII characters, such as Japanese or Chinese, are not supported with Dynamic Component Registration,
>
> Ensure that computer names contain ONLY English ASCII characters.

When Dynamic Component Registration (DCR) is enabled in the Identikey Windows Logon policy, IDENTIKEY Server will dynamically create a client component if no client component is found. The registration method depends on the Windows Group Check set in the policy.

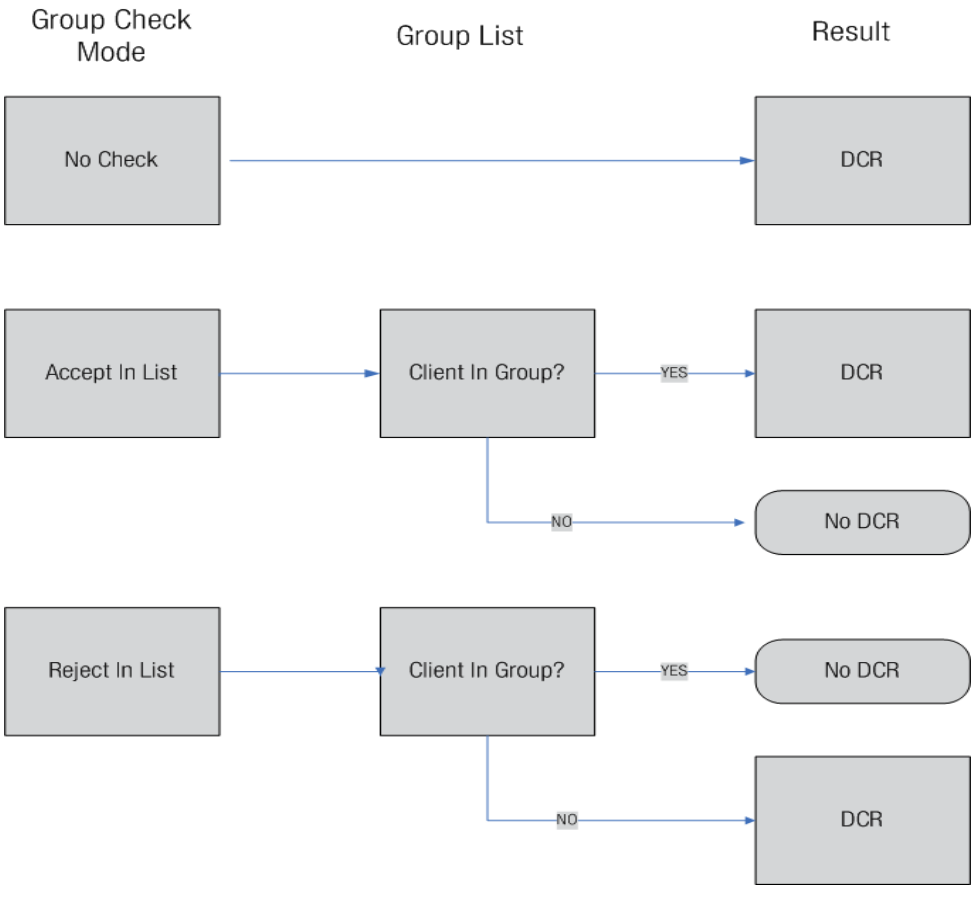

Image 4: DCR Registration

The Windows Logon client component is identified by the following formats:

- Client machine hostname - If DNS based reverse lookup of an IP address is being used with the DNS suffix not set on the client machine.
- Fully qualified domain name (FQDN) - If DNS based reverse lookup of an IP address is being used with the DNS suffix set.

> **Note**
>
> Dynamic Component Registration will fail if a PTR record does not exist on the DNS server for the client machine. A reverse zone must be implemented in order for DCR to function correctly.

3.1.1 Group Check

To enable Group Check to work correctly in Dynamic Component Registration, the server must be able to reach the client machine. Refer to 4.2.1Hostname Resolution . Also ensure that:

- The groups named are in the Active Directory domain. Group Check works with Active Directory domain groups only. It will not work with local Windows groups.
- The group for a client must be defined in the domain that the client will be logging in to. For example, in a parent/child domain setup, if a client is to be used to log in to the child domain, the group must be defined in the child domain.

3.2 Static Password

The DIGIPASS Authentication for Windows Logon relies on the Windows static password to perform the Windows logon. It is therefore important that IDENTIKEY Server is always up to date with the current Windows static password for each user. There are two ways to ensure that the static password is up to date:

- Static Password Synchronization
- Static Password Randomization

3.2.1 Static Password Synchronization

Password Synchronization Manager (PSM) is a product that is installed on the Active Directory domain controller which allows a change of the Windows password to be automatically updated on IDENTIKEY Server. The new Windows password will be reflected as the static password on IDENTIKEY Server.

If IDENTIKEY Server is not available the synchronization will fail.

If the User is not defined on IDENTIKEY Server, only the password on the Domain Controller will be changed.

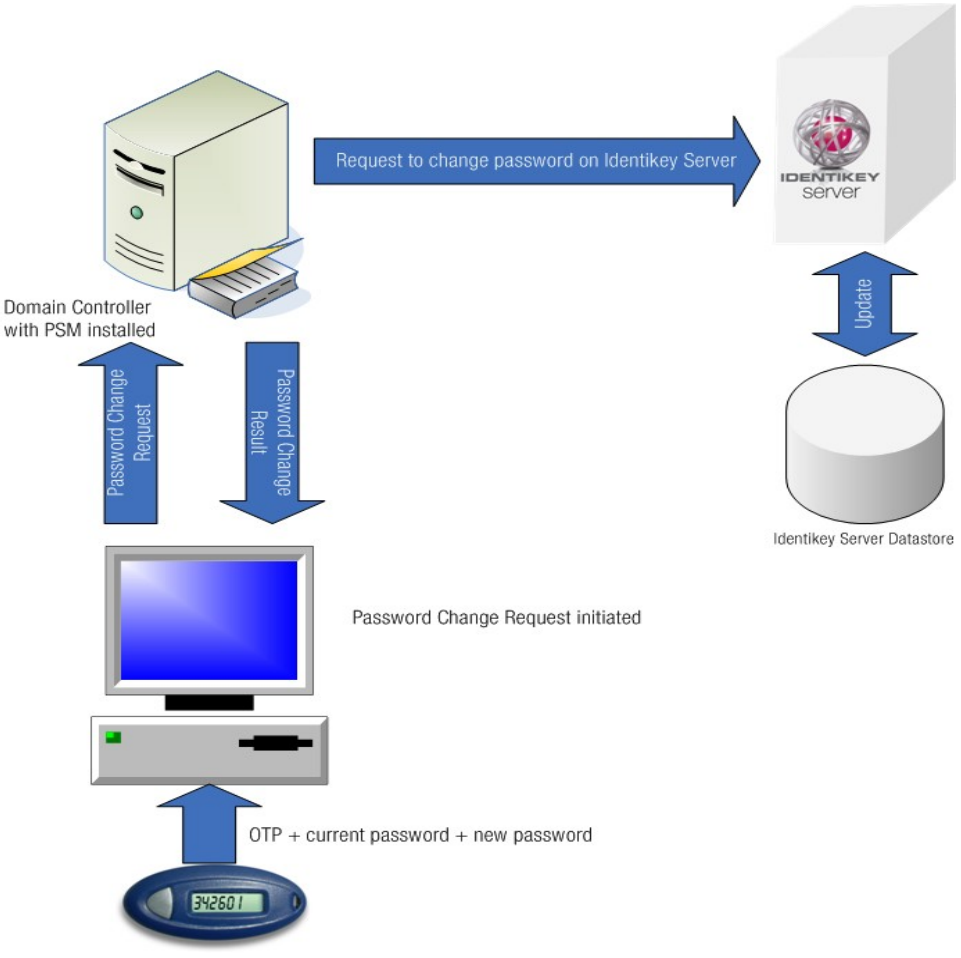

Image 5: Password Synchronization Overview

3.3 Static Password Randomization

3.3.1 Overview

Static Password Randomization means that the User's Windows static password is replaced by a randomly generated password during logon. The User only enters their User ID and the OTP, and the password is generated in the background.

By randomizing the static password, the User is prevented from logging in to Windows on a machine which does not have the DIGIPASS Authentication for Windows Logon installed as the User is unable to enter a correct random password.

Static Password Randomization is enabled on the Identikey Windows Logon policy that is being used.

Static Password Randomization is only available when Windows Back-End Authentication, or Active Directory Back-End Authentication is enabled. Static Password Randomization is not available for ADAM, Tivoli, or Novell e-Directory Back-End Authentication.

3.3.2 Password Format

The format for the new password will meet the following criteria:

- Password length – default length is 16 characters, but default may be overridden by specifying a password length on the Identikey Windows Logon policy
- Character set – the random password will consist of the following character set:
  - a to z
  - A to Z
  - 0 to 9
  - printable symbols - !@#%^&*()'"+=-_[]\|/?<>
- Complexity requirements:
  - The random password must not contain the User's User ID or parts of the User's full name that exceed two consecutive characters.
  - The random password must contain characters from three of the four character set components listed above.

The password complexity requirements are taken from the Microsoft Windows 2003 Active Directory password requirements and guarantee a successful Windows static password.

3.3.3 Use

Static Password Randomization is used to enforce the use of strong authentication on Windows Logon. This may be for the following reasons:

- The User will not be able to log on to a Windows machine without using an OTP.
- The User cannot uninstall the DIGIPASS Authentication for Windows Logon and log on using the Windows Static Password only.
- Regulatory Compliance. Some regulations specify that a strong password must be defined for Windows Logon. The regulations frequently relate to the length of the password, combination of characters in the password, and the frequency with which it must be changed. By using Static Password Randomization better control can be exerted over the regulatory criteria. Generated random passwords can be longer and much more complex than a static password that a User has to remember.

> **Note**
>
> When using Active Directory, a Minimum Password Age is set in Active Directory Group Policy Management. If the static password is reset on Active Directory Users and Computers Extension and Password Randomization is enabled on IDENTIKEY Server, the 'User must change password at next logon' checkbox must be checked. This will avoid authentication failure at the next login due to the password being too young.

3.4 User Locking

Authentications can fail for a number of reasons. The most obvious is that the User does not have authority to use the product they are trying to authenticate themselves with.

Use of incorrect User Ids, passwords, OTPs, or DIGIPASS, will result in Authentication failing, and the offending User Account being locked.

3.4.1 Online Authentication

The number of unsuccessful Online Authentications is limited according to the limit values set on the Identikey Windows Logon policy. If the number of authentications goes beyond that specified, the User will be locked.

3.4.2 Offline Authentication

The number of unsuccessful Offline Authentications is limited, and can be set using Active Directory group policies or using a local registry setting. If the number of authentications goes above that specified in the Active Directory group policy the User will be locked.

3.4.3 Unlock

An error message will appear when a User account has been locked. Follow the instructions in the table below to unlcock the appropriate account in the appropriate location:

Error Message	What To Do
No Offline Authentication Data	Clear offline authenticaiton data (AD or Web Administration Interface) Check DIGIPASS User Account and unlock if necessary User log on and perform online authenticaion. This will renew the offline authentication data.
Back-End Authentication failed	Check Windows Account and unlock if necessary If unlocking doesn't work, reset password in Windows and IDENTIKEY Server
DIGIPASS account locked	Unlock DIGIPASS User Account

A User must be unlocked by an administrator using the Users tab of the Web Administration Interface or Active Directory Users and Computers Extension.

4 Deployment

> **Note**
>
> For any of the following functionality to work, each IDENTIKEY Server must be updated to IDENTIKEY Server 3.1 SR1 or higher.

4.1 What Is Needed?

- Client Module installed on each Windows machine
- Valid license on IDENTIKEY Server(s) to which client machines will be connecting.

4.1.1 IDENTIKEY Server Ports

During deployment of IDENTIKEY Server the following ports should be made available:

- SEAL (SSL) - TCP 20004
- SEAL (non-SSL) - TCP 20003
- MDC Server - TCP 20007
- Live audit - TCP 20006
- SOAP - TCP 8888
- RADIUS Auth - UDP 1812
- RADIUS Auth - UDP 1813

Failure to make these ports available to the installer may lead to problems during deployment and configuration.

4.1.2 Client Ports

The following port must be available on the DIGIPASS Authentication for Windows Logon Client:

- Windows Group Check - TCP 445

4.1.3 DNS Registration

All IDENTIKEY Servers should be registered with the DNS server(s). This allows Server Discovery, if enabled, to work correctly.

4.2 Server Discovery for DIGIPASS Authentication for Windows Logon Client Configuration

Server Discovery is used by the DIGIPASS Authentication for Windows Logon client module to identify the location of the IDENTIKEY Server to be used for authentication.

Server Discovery is configured using the Web Administration Interface ->System Configuration ->Server Discovery tab, or the IDENTIKEY Server Configuration application. For more information about configuring the server discovery option, refer to the How to Set Up IDENTIKEY Server Discovery section of the IDENTIKEY Server Administrator Guide.

4.2.1 Hostname Resolution

When Dynamic Client Registration or Server Discovery is being used, the following process is followed to identify the server required:

1. The client checks to see if the name queried is its own.
2. The client then searches a local Hosts file.
3. DNS servers are queried.

If the above methods fail then NetBIOS name resolution sequence is used as a backup

To aid successful Windows Logon client authentication use one of the following methods:

1. Statically add Hosts to the c:\windows\system32\drivers\etc\hosts file
2. Setup reverse lookup for the network the client belongs to. Entries for the IP address of the clients should already be present. Use nslookup <client ipaddress> to resolve to the hostname of the client
3. Enable the NETBIOS Name Service Discovery port(UDP Port 137).

   In Windows 7, if the firewall is turned on (recommended settings), this port is blocked. To enable this port, Turn on Network Discovery using Network Sharing Center->Advanced sharing settings-><profile being used>, or enable the standard rule named Network Discovery (NB-Name-In) in Windows Firewall Inbound Rules.

4.2.2 Losing Connection Between the Windows Logon client and IDENTIKEY Server

If connection is lost between the Windows Logon client and IDENTIKEY Server when using Server Discovery, the connection will not be re-established automatically. To enable connection to be re-established the DNS cache must be flushed. This will allow the connection to be re-established immediately.

Alternatively, the default behaviour may be changed by modifying a Windows registry setting on the client machine (see http://support.microsoft.com/kb/320760 for further information):

1. Locate following key in the registry - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
2. On the Edit menu, point to New, and then click REG_DWORD.
3. Type ServerPriorityTimeLimit.
4. Press Enter.
5. On the Edit menu, click Modify.
6. Enter 0.
7. Click OK.

4.3 DIGIPASS Authentication for Windows Logon Client Registration Configuration

DIGIPASS Authentication for Windows Logon allows Client components to be registered in two ways:

- Manually using the Web Administration Interface Client Registration page
- Dynamically using Dynamic Component Registation (DCR)

4.3.1 Manual Component Creation

To manually create a DIGIPASS Authentication for Windows Logon client component, use the Web Administration Interface Client Registation page and create a client with client type of IDENTIKEY Windows Logon Client.

4.3.2 Dynamic Component Registration

DIGIPASS Authentication for Windows Logon client components can be registered dynamically on IDENTIKEY Server. DCR must be enabled on the Identikey Windows Logon Policy tab and administered via the Web Administration Interface Policy pages. See 4.2.1 Hostname Resolution for information regarding DNS Hostname resolution for DCR.

4.4 User Locking Configuration

4.4.1 Online Authentication

User Locking can be configured using the Locking Thresholds on the User tab of the Windows Logon policy that is being used.

> **Note**
>
> For further details about the Policy or User settings mentioned below, consult the Help files of the Web Administration Interface.

4.4.2 Offline Authentication

Offline Authentication must first be enabled on the Offline Authentication tab of the Policy or User details on the Web Administration Interface. The Offline Authentication threshold must be set using the Active Directory group policy or local Windows registry settings.

4.5 How to Distribute Client Installation Software

Please refer to the Deploying DIGIPASS Authentication for Windows Logon Client Software using Group Polocy section of the DIGIPASS Authentication for Windows Logon Installation Guide for client installation software distribution options.

4.6 DIGIPASS Token Assignment

In IDENTIKEY Server, DIGIPASS tokens may be assigned to Users in a number of ways, depending on the requirements of your company:

- Auto Assignment
- Self Assingment
- Manual Assignment

> **Note**
>
> DIGIPASS records must be imported into the data store before being assigned to Users.

4.6.1 DUR/Auto Assignment

Auto Assignment allows the IDENTIKEY Server to automatically assign an available DIGIPASS when a User performs a Windows logon using DIGIPASS Authentication for Windows Logon. After the DIGIPASS has been assigned it must be delivered to the User. Users can continue to logon with their static password while they wait for their DIGIPASS to be delivered to them. The length of the period during which they can continue to logon with their static password can be configured in the Web Administration Interface or the Active Directory User and

Computers Extension, and is called the Grace Period. The Windows Logon Client can be configured to notify the end user that a specific DIGIPASS has been assigned.

Auto Assignment can be combined with Dynamic User Registration (DUR). This combination allows IDENTIKEY Server to automatically assign an available DIGIPASS when a User account is created using DUR. The correct DIGIPASS must then be delivered to the User. A grace period is usually set, which allows a number of days in which the User may still log in using only their static password.

See the IDENTIKEY Server Product Guide for further details about DIGIPASS Auto Assignment and DUR settings.

4.6.2 Self Assignment

Self Assignment allows Users to assign themselves a DIGIPASS via a User Self Management Website when using DIGIPASS Authentication for Windows Logon. This enables DIGIPASS to be distributed within an organisation without any administrative work. The end users will typically assign the provided DIGIPASS themselves as part of the Windows Logon process.

See the IDENTIKEY Server Product Guide for further details about Self Assignment and the User Self Management Website.

4.6.3 Manual Assignment

During Manual Assignment a DIGIPASS is assigned to an individual User user by an administrator using the Web Administration Interface or the Active Directory User and Computers Extension. The administrator has the option to specify the grace period during manual assignment.

See the IDENTIKEY Server Product Guide for further details about DIGIPASS Manual Assignment.

5 DIGIPASS Authentication for Windows Logon With IDENTIKEY Server on Linux

If you use DIGIPASS Authentication for Windows Logon with IDENTIKEY Server in a Linux environment, then the funcitonality will be mostly the same as that described above. The differences for a Linux environment are as follows:

- A Windows Back-End is not availabe for a Linux environment.
- Password Randomization
  - Password Randomization can be used with IDENTIKEY Server in a Linux environment with an Active Directory Back-End. Active Directory MUST be installed with SSL enabled to provide an encrypted connection. Password Randomization will not work in this instance with out an encrypted connection.

6 Licensing

DIGIPASS Authentication for Windows Logon must be enabled in the license for IDENTIKEY Server.

6.1 Add License for DIGIPASS Authentication for Windows Logon

> **Note**
>
> IDENTIKEY Server must be upgraded to version 3.1 SR1 or higher before installing the license for DIGIPASS Authentication for Windows Logon.

A license that includes DIGIPASS Authentication for Windows Logon can be loaded during IDENTIKEY Server installation or can be loaded afterwards using the Web Administration Interface.

See the IDENTIKEY Server Product Guide and the IDENTIKEY Server Administrator Reference for further details about Licensing.

7 Technical Support

If you encounter problems with a VASCO product please do the following:

1. Check whether your problem has already been solved and reported in the Knowledge Base at the following URL: http://www.vasco.com/support.
2. If there is no solution in the Knowledge Base, please contact the company which supplied you with the VASCO product.

   If your supplier is unable to solve your problem, they will automatically contact the appropriate VASCO expert.

7.1 Glossary

To understand the way that DIGIPASS Authentication for Windows Logon works, the following concepts must be understood.

GINA

The GINA is the graphical identification and authentication library used by Microsoft Windows 2003 and XP systems, that handles identification and authentication for login. The standard Microsoft-supplied GINA library can be replaced if other authentication methods are to be used, such as DIGIPASS with IDENTIKEY Server.

The VASCO GINA is provided with the client side module for Windows Logon Client Module.

Credential Provider

Windows Vista and Windows 2008 do not use the GINA model. They both use a Credential Provider which, amongst other things, communicates with authentication providers external to Windows. DIGIPASS Authentication for Windows Logon provides a Credential Provider for Windows Vista and Windows 2008.

IDENTIKEY Server

IDENTIKEY Server is a server product designed to support the deployment, use and administration of VASCO's DIGIPASS technology. It can be easily integrated with existing applications using a Software Developer Kit (SDK).

Web Administration Interface

The Web Administration Interface is the web-based administration system for IDENTIKEY Server. The Web Administration Interface is used to administer Users, DIGIPASS, Policies, Clients, Back-End, Organization, Reports and System Settings.

DIGIPASS

A DIGIPASS token is a device for providing One Time Passwords to a User.

A DIGIPASS token may be provided to each person whom an organization wishes to be able to log into their system using a One Time Password (OTP). The User obtains an OTP from the DIGIPASS to use instead of, or as well as, a static password when logging in.

One Time Password

A One Time Password (OTP) is a secure password, generated by a DIGIPASS. An OTP can be used to perform a Windows logon using DIGIPASS Authentication for Windows Logon.

Online Authentication

During online authentication the user logs in to the Windows Domain using an OTP, the one time password is authenticated by IDENTIKEY Server.

Offline Authentication

During an offline authentication the user logs on to the client PC using an OTP when the client PC is not connected to the network. The OTP is authenticated locally on the client PC.

Time Based OTP

One Time Passwords may be time based or event based. A time based DIGIPASS will generate a different OTP for the same input data at different times.

The time based OTP relies on the time on the DIGIPASS and the time on IDENTIKEY Server being synchronized to within an acceptable tolerance.

Event Based OTP

An event based OTP uses a numeric counter which increases every time an OTP is generated. This counter ensures every OTP is unique.

The DIGIPASS and IDENTIKEY Server need to have synchronized event counters. A tolerance for the difference between the event counters can be set on the Identikey Windows Logon policy setting.

Server PIN

A Server PIN may be required in addition to the One Time Password. The Server PIN is entered during login with the OTP - instead of a DIGIPASS PIN, which is entered into the DIGIPASS device. In some cases a new Server PIN may need to be set.

Policy

Policies define how IDENTIKEY Server processes authentication requests. IDENTIKEY Server contains predefined policies for DIGIPASS Authentication for Windows Logon.