aXsGUARD Gatekeeper
Authentication Quick Install Guide
VASCO Products
VASCO Data Security, Inc. and/or VASCO Data Security International Gmbh are referred to in this document as ‘VASCO’. VASCO Products comprise Hardware, Software, Services and Documentation. This document addresses potential and existing VASCO customers and has been provided to you and your organization for the sole purpose of helping you to use and evaluate VASCO Products. As such, it does not constitute a license to use VASCO Software or a contractual agreement to use VASCO Products.

Disclaimer of Warranties and Limitations of Liabilities
VASCO Products are provided ‘as is’ without warranty or conditions of any kind, whether implied, statutory, or related to trade use or dealership, including but not limited to implied warranties of satisfactory quality, merchantability, title, non-infringement or fitness for a particular purpose. VASCO, VASCO DISTRIBUTORS, RESELLERS AND SUPPLIERS HAVE NO LIABILITY UNDER ANY CIRCUMSTANCES FOR ANY LOSS, DAMAGE OR EXPENSE INCURRED BY YOU, YOUR ORGANIZATION OR ANY THIRD PARTY (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF DATA) ARISING DIRECTLY OR INDIRECTLY FROM THE USE, OR INABILITY TO USE VASCO SOFTWARE, HARDWARE, SERVICES OR DOCUMENTATION, REGARDLESS OF THE CAUSE OF THE LOSS, INCLUDING NEGLIGENCE, EVEN IF VASCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR IF THEY WERE FORESEEABLE. OUR MAXIMUM AGGREGATE LIABILITY TO YOU, AND THAT OF OUR DISTRIBUTORS, RESELLERS 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. THIS SECTION WILL NOT APPLY ONLY WHEN AND TO THE EXTENT THAT APPLICABLE LAW SPECIFICALLY REQUIRES LIABILITY DESPITE THE FOREGOING EXCLUSIONS AND LIMITATIONS.

Intellectual Property and Copyright
VASCO Products contain proprietary and confidential information. VASCO Data Security, Inc. and/or VASCO Data Security International Gmbh own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights. No part of these Products may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted by VASCO or its authorized licensee in writing. This document is protected under US and international copyright law as an unpublished work of authorship. No part of it may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted in writing by VASCO or its authorized licensee.

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. Other company brand or product names or other designations, denominations, labels and/or other tags, titles, as well as all URLs (Internet addresses) linked to such designations or communications (irrespective of whether protected by intellectual property law or not), mentioned in VASCO Products may be the trademarks or registered trademarks or be part of any other entitlement of their respective owners.

Radius Disclaimer
Information on the RADIUS server provided in this document relates to its operation in the aXsGUARD Gatekeeper environment. We recommend that you contact your NAS/RAS vendor for further information.

Copyright © 2009 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved.
# Table of Contents

1 **Introduction** .................................................................................................................................................. 7  
   1.1 Audience and Purpose of this Document ................................................................................................. 7  
   1.2 What is the aXsGUARD Gatekeeper? ........................................................................................................... 9  
   1.3 VASCO ....................................................................................................................................................... 9  

2 **Safety and Environmental Information** .................................................................................................... 10  
   2.1 Overview .................................................................................................................................................... 10  
   2.2 Electrical Safety ......................................................................................................................................... 10  
   2.3 Personal, Environmental and aXsGUARD Gatekeeper Safety ...................................................................... 10  
   2.4 Temperature, Power and Humidity ............................................................................................................. 11  
   2.5 Dimensions .............................................................................................................................................. 11  
   2.6 Chassis Rails ............................................................................................................................................. 11  

3 **Before you Begin** .......................................................................................................................................... 12  

4 **Connecting the aXsGUARD Gatekeeper to a Network** .............................................................................. 13  
   4.1 Overview .................................................................................................................................................... 13  
   4.2 Powering on the aXsGUARD Gatekeeper .................................................................................................... 13  
   4.3 Connecting to your Network ....................................................................................................................... 15  
   4.4 Workstation TCP/IP Settings ..................................................................................................................... 15  

5 **Accessing the Administrator Tool** ............................................................................................................ 17  
   5.1 Overview .................................................................................................................................................... 17  
   5.2 Instructions for Logging into the Administrator Tool ................................................................................ 17  

6 **aXsGUARD Gatekeeper Configuration** .................................................................................................... 20  
   6.1 Overview .................................................................................................................................................... 20  
   6.2 Setting the Administrator’s User Name / Password .................................................................................. 20  
   6.3 Entering Customer Information ................................................................................................................ 22  
   6.4 Menu Structure and Navigation ................................................................................................................ 23  
   6.5 Entering the System Information ............................................................................................................... 24  
   6.6 Network Settings: Ethernet Secure LAN Device ....................................................................................... 26  
   6.7 General Settings ....................................................................................................................................... 29  
      6.7.1 Domain Name Server .......................................................................................................................... 29  
      6.7.2 Email Relay ....................................................................................................................................... 29  

7 **Users and Groups** ........................................................................................................................................ 30  
   7.1 Overview .................................................................................................................................................... 30  
   7.2 aXsGUARD Gatekeeper Users .................................................................................................................... 30

© 2009 - VASCO Data Security
7.3 aXsGUARD Gatekeeper Groups.......................................................................................... 30
7.4 Creating and Modifying Groups....................................................................................... 31
  7.4.1 Manually.................................................................................................................. 31
  7.4.2 Automatically via Active Directory......................................................................... 32
7.5 Creating and Modifying Users......................................................................................... 32
  7.5.1 Manually.................................................................................................................. 33
  7.5.2 Automatically via Active Directory......................................................................... 34
8 DIGIPASS Management..................................................................................................... 38
  8.1 Overview...................................................................................................................... 38
  8.2 Importing DIGIPASS Records...................................................................................... 38
    8.2.1 Automatic import.................................................................................................... 38
    8.2.2 Manual import......................................................................................................... 39
  8.3 DIGIPASS Device Testing.............................................................................................. 39
  8.4 Assigning DIGIPASS Devices...................................................................................... 40
  8.5 Unassigning a DIGIPASS Device.................................................................................. 41
  8.6 Deleting DIGIPASS Records......................................................................................... 41
9 RADIUS Server Configuration........................................................................................... 43
  9.1 Overview...................................................................................................................... 43
  9.2 RADIUS Server Setup and Configuration.................................................................... 43
    9.2.1 Adding the RADIUS Client to the Computer list.................................................... 44
    9.2.2 Configuring the RADIUS Server.......................................................................... 46
    9.2.3 RADIUS Server Authentication Policy................................................................. 47
10 What’s Next...................................................................................................................... 48
11 Support........................................................................................................................... 49
  11.1 Overview...................................................................................................................... 49
  11.2 If you encounter a problem......................................................................................... 49
  11.3 Return procedure if you have a hardware failure....................................................... 49
Illustration Index

Image 1: aXs GUARD Gatekeeper AG-3XXX................................................................. 7
Image 2: aXs GUARD Gatekeeper AG-5XXX.......................................................... 7
Image 3: Back of a Typical ...................................................................................... 13
Image 4: Example Stickers Labeling Interfaces on the AG-3XX3......................... 14
Image 5: Example Stickers Labeling Interfaces on the AG-3XX4............................ 14
Image 6: Example Stickers Labeling Interfaces on the AG-5XX6............................. 14
Image 7: Power Button and Power LED.................................................................. 15
Image 8: Command Prompt and Testing TCP/IP Settings...................................... 16
Image 9: Certificate Screen..................................................................................... 18
Image 10: Login Screen........................................................................................... 18
Image 11: Changing the System Administrator Password...................................... 19
Image 12: Creating a System Administrator User.................................................... 21
Image 13: Customer Information............................................................................ 22
Image 14: System > General Screen...................................................................... 23
Image 15: System > General Screen...................................................................... 24
Image 16: Network > Devices > Eth....................................................................... 26
Image 17: Network > Devices > Eth > eth0............................................................... 26
Image 18: Fixed IP Configuration IP Settings.......................................................... 27
Image 19: Network > General............................................................................... 29
Image 20: E-mail>General: SMTP and E-mail Disabled........................................... 29
Image 21: Creating a new group............................................................................. 31
Image 22: Active Directory User and Group Authentication / Synchronization........ 32
Image 23: Creating a New User.............................................................................. 33
Image 24: Directory Services Configuration.............................................................. 35
Image 25: Active Directory Tree............................................................................ 35
Image 26: Synchronized AD Users and Groups...................................................... 37
Image 27: Automatic Status Message................................................................... 38
Image 28: Manually Importing a DPX File............................................................... 39
Image 29: Assigning a record to a User.................................................................. 40
Image 30: Deleting a Record................................................................................... 41
Image 31: RADIUS Server Setup.......................................................................... 44
Image 32: Adding a Host to the Computer List....................................................... 45
Image 33: Adding a RADIUS Client...................................................................... 46
Image 34: Setting the Authentication Policy for the RADIUS Server..................... 47
Index of Tables

Table 1: System General Fields....................................................................................................................25
Table 2: Network > Devices > Eth > eth0 Fields.............................................................................................27
Table 3: Users & Groups > Users > Add User: Fields.....................................................................................33
Table 4: Directory Services > General........................................................................................................36
Table 5: Computer Settings..........................................................................................................................45
Table 6: Authentication > Radius > Clients: Field Descriptions..................................................................46
1 Introduction

1.1 Audience and Purpose of this Document

This Authentication Quick Install Guide explains how to set up the aXsGUARD™ Gatekeeper AG-3XXX or AG-5XXX models (see images below) serving exclusively as an authentication server in your Local Area Network. The document is intended for technical personnel and / or system administrators.

In sections 1.2 and 1.3, we introduce the aXsGUARD Gatekeeper and VASCO®.

In section 2, we provide safety and environmental information. This section must be read before installing your aXsGUARD Gatekeeper.

In section 3, we list the information you need to collect in preparation for installation.
In section 4, we explain how to physically connect the aXsGUARD Gatekeeper to your network. Following successful connection, the aXsGUARD Gatekeeper’s settings can be adjusted by accessing the Administrator Tool.

In section 5, we explain how to access the aXsGUARD Gatekeeper Administrator Tool.

In section 6, we provide instructions for the minimal configurations required to get started.

In section 7, we explain the concepts of users and groups and how to create and modify users and groups on the aXsGUARD Gatekeeper.

In section 8, we explain how to import DIGIPASS® records into the aXsGUARD Gatekeeper, how to test DIGIPASS devices, and how to assign/unassign and delete DIGIPASS records.

In section 9, we explain how to configure and use the aXsGUARD Gatekeeper RADIUS Authentication Server in your network.

In section 10, we list the next configurations required, and where you can read more about them.

In section 11, we explain how to request support, and return hardware for replacement.

An index at the end of the document will help you to find specific information you are searching for.

Other documents in the set of aXsGUARD Gatekeeper documentation include:

- The aXsGUARD Gatekeeper Installation Guide, which provides instructions on how to configure the aXsGUARD Gatekeeper both as an authentication server on your LAN and also as a gateway to the Internet. Minimal settings for modules purchased after first installation of your aXsGUARD Gatekeeper are also explained.

- The aXsGUARD Gatekeeper System Administration How To Guide, which provides detailed information about configuration using the Administrator Tool.

Access to aXsGUARD Gatekeeper guides is provided through the Documentation button in the aXsGUARD Gatekeeper Administrator Tool. A paper copy of the aXsGUARD Gatekeeper Authentication Quick Install Guide is also provided with delivery of the aXsGUARD Gatekeeper.

Further resources available include:

- Context-sensitive help, which is accessible in the aXsGUARD Gatekeeper Administrator Tool through the Help button. This button is permanently available and displays information related to the current screen.

- Training courses covering features in detail can be organized on demand. These courses address all levels of expertise. Please see www.vasco.com for further information.

Welcome to aXsGUARD Gatekeeper security.
1.2 What is the aXsGUARD Gatekeeper?

The aXsGUARD Gatekeeper is an authentication appliance, intended for small and medium sized enterprises. In addition to strong authentication, the aXsGUARD Gatekeeper has the potential to manage all of your Internet security needs. Its modular design means that optional features can be purchased at any time to support, for example, e-mail, Web access and VPN management. The aXsGUARD Gatekeeper can easily be integrated into existing IT infrastructures as a stand-alone authentication appliance or as a gateway providing both authentication services and Internet Security.

Authentication and other features such as firewall, e-mail and Web access are managed by security policies, which implement a combination of rules, for example, whether a user must use a DIGIPASS One-Time Password in combination with a static password for authentication. Rules can be further adjusted with restrictions. Security Policies are applied to specific users or groups of users and can also be applied to specific computers and the entire system.

1.3 VASCO

VASCO is a leading supplier of strong authentication and electronic signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as a global software company for Internet Security serving customers in more than 100 countries, including several international financial institutions. VASCO’s prime markets are the financial sector, enterprise security, e-commerce and e-government.

For further information, please see www.vasco.com.
2 Safety and Environmental Information

2.1 Overview

In this section we provide details important both for the safe use of the aXsGUARD Gatekeeper and also to help maintain the device in a safe environment to keep it fully operational.

Caution
Please read all of this section before starting to install your aXsGUARD Gatekeeper.

2.2 Electrical Safety

Caution
Never disconnect the power supply (power cord) while the appliance is booting up or active, as this may cause system or hardware damage.

Use the exact type of power cord recommended:

- only use a power cord which is certified in compliance with safety regulations
- only use a power cord which is compliant with the AC voltage requirements in your region

Before turning on the power, plug the power cord(s) into a socket which is properly grounded

Before disconnecting the power supply, turn the system off.

Use the exact type of network cable recommended:

- to conform to certification restrictions, only use a network cable with maximum length of 3.0 meters.

2.3 Personal, Environmental and aXsGUARD Gatekeeper Safety

- To avoid back injuries: when lifting the aXsGUARD Gatekeeper, avoid injuries to your back by using your leg muscles. Keep your back straight and bend your knees when lifting the device.

- Protecting the environment: producing the aXsGUARD Gatekeeper involves the extraction and use of natural resources. The product may contain substances which are hazardous for human health and the environment. To reduce the risk of any hazardous substances being released into the environment and to reduce the depletion of natural resources, we encourage you to use appropriate recycling systems. Such systems reuse or recycle most end-of-life materials in a safe way. The 'crossed-bin symbol' invites you to use such systems.
Further information on collection, reuse and recycling is available from your local or regional refuse administration center.

For further information on the aXsGUARD Gatekeeper and the environment, please contact your supplier (see section 11).

**To avoid dropping the aXsGUARD Gatekeeper**: do not lift the device by the chassis handles. These handles are for sliding the aXsGUARD Gatekeeper in and out of the chassis rails only (see section 2.6). Do not carry the aXsGUARD Gatekeeper by these handles.

### 2.4 Temperature, Power and Humidity

VASCO recommends installing the aXsGUARD Gatekeeper in a 'server room' with air conditioning and UPS (Uninterrupted Power Supply). If the equipment is built into a server cupboard, make sure there is sufficient ventilation. Environmental requirements are:

- **Operating Temperature Range**: 10 to 35 degrees Celsius (50 to 95 degrees Fahrenheit)
- **Non-Operating Temperature Range**: -40 to +70 degrees Celsius (-40 to 158 degrees Fahrenheit)
- **Operating Humidity Range**: 8% to 90% non-condensing
- **Humidity Range**: 5% to 95% non-condensing
- **Power Supply**: Thermal control 260 W AC power supply with PFC [24-pin, 4-pin=12V, (2) 4-pin]

### 2.5 Dimensions

<table>
<thead>
<tr>
<th></th>
<th>AG-3XXX</th>
<th>AG-5XXX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>1.7” (43mm)</td>
<td>1.7” (43mm)</td>
</tr>
<tr>
<td>Width</td>
<td>16.8” (426mm)</td>
<td>16.8” (426mm)</td>
</tr>
<tr>
<td>Depth</td>
<td>10” (253mm)</td>
<td>14” (356mm)</td>
</tr>
</tbody>
</table>

### 2.6 Chassis Rails

Chassis rails for storing the aXsGUARD Gatekeeper on a sliding shelf are available for the AG-5XXX model only. These are not included in the VASCO price list. Please consult [www.supermicro.com](http://www.supermicro.com) for compatible chassis rails (part number CSE-PT08).
Before you Begin

Collecting the following information before you start will help to speed up your installation:

- an unused IP address in your network
- the Default Gateway setting in your network
- DNS Server IP address(es) for your network
- DNS Suffix(es) (optional)
- an appropriate network cable, with maximum length of 3.0 meters (see section 2.2)
4 Connecting the aXsGUARD Gatekeeper to a Network

4.1 Overview

In this section we provide step by step instructions to connect the aXsGUARD Gatekeeper to your network.

**Important:**
Please first read the safety information in section 2, check that all the package contents you need (listed on a separate sheet supplied with the aXsGUARD Gatekeeper) have been supplied, and that you have all the information you need for installation (listed in section 3).

4.2 Powering on the aXsGUARD Gatekeeper

Powering the aXsGUARD Gatekeeper on requires the following four steps:

1. Connect the eth0 interface to the network’s hub or switch with an appropriate network cable. The aXsGUARD Gatekeeper has two or more LAN Ethernet interface(s), depending on the chosen configuration and type (AG-3 and AG-5 series). For the AG-3XXX and AG-5XXX models, the default LAN interface is labeled as eth0 (example stickers are shown in the images below: please check the sticker labeling the interfaces on your aXsGUARD Gatekeeper to identify the correct socket).

![Image 3: Back of a Typical aXsGUARD Gatekeeper](image)
Connecting the aXsGUARD Gatekeeper to a Network

Image 4: Example Stickers Labeling Interfaces on the aXsGUARD Gatekeeper AG-3XX3

Image 5: Example Stickers Labeling Interfaces on the aXsGUARD Gatekeeper AG-3XX4

Image 6: Example Stickers Labeling Interfaces on the aXsGUARD Gatekeeper AG-5XX6
2. Connect the aXsGUARD Gatekeeper via the power cable to a supply.

3. Power up the aXsGUARD Gatekeeper by pressing the power switch once (see image below). A green LED lights up.

![Image 7: Power Button and Power LED](image)

4. To check the network is correctly connected, you can verify whether a green light shows at the socket where the network cable is plugged in. If a green light is not visible, check that the network cable is in good working order and correctly plugged into the device labeled as ‘eth0’ on the aXsGUARD Gatekeeper and your network hub or switch.

### 4.3 Connecting to your Network

Installation of the aXsGUARD Gatekeeper requires temporarily isolating a client workstation from the network and linking it to the aXsGUARD Gatekeeper. This involves changing a client workstation IP address to within the specified IP address range for the aXsGUARD Gatekeeper. During the first-time configuration, the aXsGUARD Gatekeeper IP address is modified to within the range of your network (we explain how to do this in section 6.6). The client workstation network settings can then be restored.

The aXsGUARD Gatekeeper is delivered with a default LAN configuration as follows:

<table>
<thead>
<tr>
<th>IP address / Netmask</th>
<th>192.168.250.254/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Host Name</td>
<td>axsguard</td>
</tr>
<tr>
<td>Domain Name</td>
<td>domain.be</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

### 4.4 Workstation TCP/IP Settings

To access the aXsGUARD Gatekeeper, a workstation needs to be temporarily configured with the same TCP/IP settings as the aXsGUARD Gatekeeper.

1. Configure a workstation with the following settings:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.250.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.250.254</td>
</tr>
<tr>
<td>DNS Server</td>
<td>192.168.250.254</td>
</tr>
</tbody>
</table>

2. Once the TCP/IP settings (listed above) are active on a workstation, open a command prompt (Microsoft
Windows) or Terminal (Linux) and run the following command:

```
ping 192.168.250.254
```

If a reply is received as shown in the image above, everything is OK.

If a Request Timed Out or Destination Host Unreachable response is received, please check the following:

- check that the workstation's TCP/IP settings have been entered correctly (see above)
- check that the network cable is in good working order and correctly plugged into the device labeled 'eth0' on the aXsGUARD Gatekeeper and your network hub or switch (see section 4.2).

Once the workstation is correctly configured, the aXsGUARD Gatekeeper Administrator Tool can be accessed through a browser on the workstation, as explained in the following section.

**Note**

Once the network settings on the aXsGUARD Gatekeeper have been configured appropriately, (explained in section 6.6) the workstation IP address can be reconfigured onto the network, and the aXsGUARD Gatekeeper can be accessed from any browser on the network.
Accessing the Administrator Tool

5.1 Overview

Accessing the aXsGUARD Gatekeeper Administrator Tool is possible from any workstation in the same network using a standard Web browser, providing the browser does not have a proxy setup in its browser settings. Access is secured by SSL (Secure Socket Layer) encryption over the HTTPS protocol.

Logging into the Administrator Tool requires the steps described below.

5.2 Instructions for Logging into the Administrator Tool

1. Enter the URL for the Administrator Tool into the browser:

   https://192.168.250.254:82

   **Note**
   1) Remember to include the port number (:82) after the IP address or the connection will fail.

2. As you are accessing a website secured with a self-signed certificate, the browser presents a warning asking you to accept the certificate (see image below) to continue. After the certificate has been accepted, the aXsGUARD Gatekeeper login screen appears (see image 10).

   **Note**
   The procedure for accepting a certificate varies between browsers.
3. Enter the default system administrator’s Username and Password (use lower case only):

   Username:     sysadmin
   Password:     sysadmin

   Press Enter or click on the Log in button to proceed (see image 10).
**Caution**
The default System Administrator (sysadmin) password must be changed as soon as you log on; otherwise the appliance can be accessed by non-authorized users.

4. After a successful login, the status screen is shown, with a warning including a link to the screen where you can modify the default system administrator’s (sysadmin) password (see image below).

![Image 11: Changing the System Administrator Password](image-url)
6 aXsGUARD Gatekeeper Configuration

6.1 Overview

This section covers the practical step by step configuration of the aXsGUARD Gatekeeper to implement the required network security.

6.2 Setting the Administrator's User Name / Password

Caution
The default System Administrator (sysadmin) password must be changed as soon as you log on; otherwise the appliance can be accessed by non-authorized users (see section 5).

The sysadmin user (see section 5) has limited access. This default user can only modify some general system parameters and add/remove or modify users. The first step is to add a new user with full administration privileges to further configure the aXsGUARD Gatekeeper. This also facilitates troubleshooting, since all actions performed by administrators in the Administrator Tool are logged by user name, a useful feature when multiple system administrators exist.

To create a System Administrator user with full administration rights:

1. Log on to the aXsGUARD Gatekeeper as explained in section 5.
2. Navigate to Users & Groups > Users and click on Add new. The screen below is displayed. Fields with a description in bold are mandatory (cannot be left blank).
3. Enter a user name.
4. Enter the user’s full name (optional).
5. Enter and confirm the user’s password. The password should consist of at least 6 characters, some of which are digits. For more information on secure passwords, please refer to the document, aXsGUARD Gatekeeper System Administration How To, which is available via the Documentation button in the Administrator Tool.
6. In the aXsGUARD Gatekeeper Administration tab, select Full Administration.
7. Click on Update / Save.
8. Log off and log on with the newly created administrator credentials.

**Tip**

Mandatory fields are highlighted in bold on screen.

**Note**

A log of the actions performed in the aXsGUARD Gatekeeper Administrator Tool is available under System > Logs > Admin Tool.
6.3 Entering Customer Information

Caution
E-mail addresses must be entered accurately, as they are needed to deliver system-critical information.

Customer information is sent to VASCO back-up servers and automatically entered into the support database. Keeping this information up-to-date helps VASCO to inform you about the latest product updates, features and developments.

After logging on, enter the contact information as requested (see image below).

Information for the Customer, Dealer or preferably both needs to be entered. The Dealer contact tab only displays when ‘dealer’ or ‘both’ is selected for the The aXsGUARD Gatekeeper is managed by field.

Image 13: Customer Information

Tip
1) The screen above can also be accessed by navigating to System > Customer.
2) If you prefer not to receive any mailings from VASCO, uncheck the option 'Please send me all aXsGUARD Gatekeeper and VASCO Data Security technical and informational mailings' on the above screen.
### 6.4 Menu Structure and Navigation

The Administrator Tool interface has three panes (highlighted orange in the image below). The pane across the top is permanently visible; the left pane displays the menu. Selecting a menu or sub menu item displays the corresponding configuration pane to the right for viewing and modifying settings (see image below).

![Image 14: System > General Screen](image)

Navigating the tree menu structure is possible using the following buttons:

- **Collapse**: Clicking on Collapse closes all sub menus, returning the menu to its original state.
- **Plus Sign**: Clicking on the plus sign displays (expands) the sub menu of the selected item. Clicking on the menu item while the sub menu is collapsed also displays the sub menu. (Some menu items, such as Computers, do not have sub menus.)
- **Minus Sign**: Clicking on the minus sign closes (collapses) the sub menu of the selected item. Clicking on the menu item while the sub menu is displayed also closes the sub menu.

**Tip**

In the Administrator Tool, a selectable item can be identified by moving the cursor over it. The cursor changes to a hand-pointing symbol:

For more information on the Administrator Tool menu, please refer to the aXsGUARD Gatekeeper System Administration How To, available through the Documentation button in the Administrator Tool.

Navigation instructions in the rest of this manual use the following format:

```
Navigate to Users & Groups > General
```

This example indicates that you need to expand the main menu topic ‘Users & Groups’ and click on the subtopic ‘General’.
6.5 Entering the System Information

To enter system information:

1. Navigate to System > General. The screen below is displayed.
2. Configure the fields as explained in the table below.
3. Click on Update to finish.

![Image 15: System > General Screen]

**Caution**

1) Changing the default System Administrator (sysadmin) password is critical for security. It should be changed as soon as you log on; otherwise the appliance could be accessed by non-authorized users.

2) The Domain Name is not necessarily the Windows Domain Name (see also the Domain Name field explanation in the table below).

**Note**

1) Fields with a description in bold are mandatory (cannot be left blank).
### Table 1: System General Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>This is the internal (DNS) name of the aXsGUARD Gatekeeper appliance. The name <code>axsguard</code> is used by default. VASCO does not recommend changing this, unless absolutely necessary, in which case no upper cases, special characters or spaces may be used. Changing the hostname requires Advanced Administrator access (see section 6.2).</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter your organization’s name. No upper cases, special characters or spaces may be used. If more than one domain name exists, enter the main Domain Name. This domain becomes the primary domain for the internal DNS server and is used whenever the aXsGUARD Gatekeeper sends an e-mail to the administrator or the outside world. For more information on the aXsGUARD Gatekeeper DNS, please refer to the document, aXsGUARD Gatekeeper System Administration How To, which is available via the Documentation button in the Administrator Tool.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the applicable time zone from the drop-down list.</td>
</tr>
<tr>
<td>System Administrator E-mail address</td>
<td>Enter the System Administrator’s e-mail address. All aXsGUARD Gatekeeper-generated reports are sent to this e-mail address. More than one e-mail address may be entered.</td>
</tr>
<tr>
<td>System Administrator Password</td>
<td>The System Administrator password can be modified here (see section 6.2). The new password should be entered twice. VASCO recommends changing this password immediately after installation, to prevent further use of the default system password.</td>
</tr>
</tbody>
</table>
6.6 Network Settings: Ethernet Secure LAN Device

The next step in configuring the aXsGUARD Gatekeeper is to configure a network device. The default secure LAN device is shown in section 4.2.

To set up the Ethernet Secure LAN Device:

1. Navigate to Network > Devices > Eth.

2. Click on eth0 (secure LAN). The screen below is displayed.
3. Configure the fields as explained in the table below.
4. Click on Update to finish.

Image 16: Network > Devices > Eth

Image 17: Network > Devices > Eth > eth0
Table 2: Network > Devices > Eth > eth0 Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description (optional)</td>
<td>Enter the description of your choice for the selected device.</td>
</tr>
<tr>
<td>Alias Names</td>
<td>Enter additional names for the selected device. A DNS entry will be added in the aXsGUARD Gatekeeper DNS server database for each alias. For more information on the aXsGUARD DNS, please refer to the document, aXsGUARD Gatekeeper System Administration How To, which is available via the Documentation button in the Administrator Tool.</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Keep the Secure option configured.</td>
</tr>
<tr>
<td>Upstream / Downstream Bandwidth</td>
<td>These settings should only be modified when using the Bandwidth Management feature.</td>
</tr>
</tbody>
</table>
| Connection Settings    | Select the applicable option for your network:  
  - If DHCP Client is selected, no extra configuration is required.  
  - If Fixed IP Configuration is selected, additional IP settings need to be added in the IP Settings tab (see image below). The aXsGUARD Gatekeeper’s IP address (as seen by a network segment connected to the Ethernet device) needs to be entered. |

Image 18: Fixed IP Configuration IP Settings

Notes
1) Fields with a description in bold are mandatory (cannot be left blank).
2) As no Internet connectivity is required for an aXsGUARD Gatekeeper serving exclusively for authentication, keep the Interface Type for the eth1 device configured as Not in use.
6.7 General Settings

6.7.1 Domain Name Server

To configure your Domain Name Server (DNS) on the aXsGUARD Gatekeeper:

1. Navigate to Network > General. The screen shown below appears.
2. Enter the name of the DNS server on your LAN.
3. Click on Add and Update to finish.

![Image 19: Network > General](image19)

6.7.2 Email Relay

The aXsGUARD Gatekeeper proactively sends emails to the system administrator. For emails to be sent from the aXsGUARD Gatekeeper requires an email relay server to be configured.

To configure an email relay server:

1. Navigate to E-mail > General.
2. Enter the DNS name or IP address of the SMTP relay server used in your network (see image below).
3. Click on Update to save the settings.

![Image 20: E-mail>General: SMTP and E-mail Disabled](image20)
7 Users and Groups

7.1 Overview

In this section we:
- define aXsGUARD Gatekeeper users and groups.
- explain how to create and modify users and groups on the aXsGUARD Gatekeeper.

Users and groups can be created using the aXsGUARD Gatekeeper Administrator Tool or can be imported and synchronized with a Directory Server, such as Microsoft Active Directory. We explain both methods here.

7.2 aXsGUARD Gatekeeper Users

An aXsGUARD Gatekeeper user is a person who:
- May authenticate with the aXsGUARD Gatekeeper (is registered as a legitimate user on the system).
- Has certain access rights depending on the individual user settings and/or group settings.

7.3 aXsGUARD Gatekeeper Groups

An aXsGUARD Gatekeeper group is:
- A set of users (a group can also contain a single user).
- A unit, based on the location, department, access rights or position within an organization, e.g. accountants, the human resources department or legal department, management, etc.
- Linked to a set of permissions or restrictions which apply to its members.
7.4 Creating and Modifying Groups

In this section, we explain how to create and modify aXsGUARD Gatekeeper groups. Groups are defined in section 7.3. Groups can be created manually in the Administrator Tool, or automatically through synchronization with a Directory Server, such as Microsoft Active Directory.

7.4.1 Manually

To create a new group:

1. Navigate to Users & Groups > Groups.
2. Click on Add new. A screen similar to the image below appears.
3. Enter the group name and a description (optional).
4. Click on Save to finish.

To modify an existing group:

1. Navigate to Users & Groups > Groups.
2. Click on the group name.
3. Modify the group’s settings.
4. Click on Update.
7.4.2 Automatically via Active Directory

Groups can be created automatically by importing and synchronizing with a Directory Server, such as Microsoft Active Directory (AD; see image below). We explain this procedure in section 7.5.2.

**Caution**
Do not modify any Directory Server-specific group settings on the aXsGUARD Gatekeeper. These should be modified on the Directory Server.

![Image](image22.png)

**Image 22: Active Directory User and Group Authentication / Synchronization**

7.5 Creating and Modifying Users

In this section, we explain how to create and modify aXsGUARD Gatekeeper users. aXsGUARD Gatekeeper users are defined in section 7.2.

Users can be created manually in the Administrator Tool, or automatically through synchronization with a Directory Server, such as Microsoft Active Directory.
### 7.5.1 Manually

To create a new user:

1. Navigate to *Users & Groups > Users*.
2. Click on **Add New**. A screen as shown in the image below appears.
3. Enter the information in the user fields as explained in Table 3.
4. Click on **Save**.

![Image 23: Creating a New User](image-url)

#### Table 3: Users & Groups > Users > Add User: Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox / User Name</td>
<td>Enter a name for the user.</td>
</tr>
<tr>
<td>User’s Full Name</td>
<td>Enter the Full Name of the user (optional).</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and confirm a static password. This must not be identical to the user name. An error message appears if the password entered is not sufficiently secure. For more information about password security, consult the aXsGUARD Gatekeeper Authentication How To, which is available through the Documentation button in the Administrator Tool.</td>
</tr>
<tr>
<td>Member of a Group</td>
<td>Assign the user to a group using the select button.</td>
</tr>
<tr>
<td>Has VASCO DIGIPASS</td>
<td>Check this option if the user has a VASCO DIGIPASS device. Select the appropriate DIGIPASS serial number from the list. Detailed information about DIGIPASS assignment is provided in section 8.4.</td>
</tr>
</tbody>
</table>
To modify an existing user:

1. Navigate to Users & Groups > Users.
2. Click on the Mailbox/User Name.
3. Modify the user’s settings as explained in Table 3.
4. Click on Update.

### 7.5.2 Automatically via Active Directory

We explain here the basic steps to import and synchronize users and groups with an Active Directory Server using the aXsGUARD Gatekeeper Directory Services module. Other types of Directory Servers, such as Novell and Generic LDAP are supported, but fall outside the scope of this guide.

For more information on Directory Services, such as the use of LDAP syntax, user / group templates and supported Directory back-end servers, please refer to the aXsGUARD Gatekeeper Directory Services How To, which is available through the Documentation button in the Administrator Tool.

**Caution**

Do not modify any Directory Server-specific user / group settings on the aXsGUARD Gatekeeper. These should be modified on the Directory Server.

To synchronize Active Directory users and groups:

1. Navigate to System > Feature Activation and make sure the Directory Services feature is enabled.
2. Navigate to Directory Services > General. A screen as shown in the image below appears.
3. Make sure the Enable DS lookups option is checked.
4. Enter the settings as explained in Table 4.
5. Click on Update to save your settings.
Enable DS lookups

Server settings
Type of Directory Service: 
Active Directory

Server IP address

Directory Base

DS User with search permission

Password

Integration level
Synchronize group and user objects

Automatically delete users

Add user mail addresses as aliases

Add SMTP ProxyAddresses as mail aliases

Group selection
Directory Base for Group search

Add these groups only

Group patterns

User selection
Directory Base for User search

Only add users with a valid primary group

Only add users which are member of a valid group

Image 24: Directory Services Configuration

Image 25: Active Directory Tree
Table 4: Directory Services > General

<table>
<thead>
<tr>
<th>Field Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable DS Lookups</strong></td>
<td>Checked / Unchecked</td>
<td>Enables / Disables Directory Service synchronization.</td>
</tr>
<tr>
<td><strong>Server Settings</strong></td>
<td>Type of Directory Service</td>
<td>Set the type to <strong>Active Directory</strong>.</td>
</tr>
<tr>
<td></td>
<td>Server IP address</td>
<td>Add the IP address of the Active Directory server and any AD mirrors, if applicable.</td>
</tr>
<tr>
<td></td>
<td>Directory Base (Requires LDAP syntax)</td>
<td>Enter the tree base of the Active Directory server, e.g. dc=my,dc=domain,dc=com</td>
</tr>
<tr>
<td></td>
<td>DS User with search permission (Requires LDAP syntax)</td>
<td>Enter the user name of the user with the necessary Directory Base search permissions, e.g. cn=axsguard,cn=users,dc=my,dc=domain,dc=com</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Enter the user’s password twice.</td>
</tr>
<tr>
<td><strong>Integration Level</strong></td>
<td>Synchronize group and user objects</td>
<td>Check to start the synchronization process. Make sure your user and group templates are configured first, as explained in the aXsGUARD Gatekeeper Directory Services How To, which is available through the Documentation button in the Administrator Tool.</td>
</tr>
<tr>
<td></td>
<td>Automatically delete users</td>
<td>Automatically deletes users who no longer exist on the AD server.</td>
</tr>
<tr>
<td></td>
<td>Add user email addresses as aliases</td>
<td>Imports the AD email addresses as aliases on the aXsGUARD Gatekeeper</td>
</tr>
<tr>
<td></td>
<td>Add SMTP Proxy Addresses as email aliases</td>
<td>Consult the aXsGUARD Gatekeeper Directory Services How To for more information</td>
</tr>
<tr>
<td><strong>Group Selection</strong></td>
<td>Directory Base for Group search (Requires LDAP syntax)</td>
<td>The path from which AD groups are imported, e.g. ou=groups,ou=vancouver,dc=my,dc=domain,dc=com</td>
</tr>
<tr>
<td></td>
<td>Add these groups only</td>
<td>Specify the groups to be imported using the full name or wildcards, e.g. account*</td>
</tr>
<tr>
<td><strong>User Selection</strong></td>
<td>Directory Base for User search (Requires LDAP syntax)</td>
<td>The path from which AD users are imported, e.g. ou=users,ou=vancouver,dc=my,dc=domain,dc=com</td>
</tr>
<tr>
<td></td>
<td>Only add users with a valid primary group</td>
<td>Check to only import users who are members of a valid primary AD group. A valid group is a group within the specified Directory Base for Group search, in other words synchronized on the aXsGUARD Gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>Only add users who are members of a valid group</td>
<td>This option is identical to the option above, except that the user is synchronized if one of their groups is a valid group. (as explained above).</td>
</tr>
<tr>
<td></td>
<td>Both options above are unchecked</td>
<td>All users as specified in the Directory Base for User search are imported.</td>
</tr>
</tbody>
</table>
Notes

1) Synchronization may take a while to complete. The synchronization status can be checked by navigating to Directory Services > Status.

2) For more detailed information, consult the aXsGUARD Gatekeeper Directory Services How To, available through the Documentation button in the aXsGUARD Gatekeeper Administrator Tool.

To view synchronized Active Directory users and groups:

1. Navigate to Users & Groups.

2. Click on Users to view the synchronized AD users. Click on Groups to view the synchronized AD groups.

Synchronized AD users and groups are listed with a special icon next to their name as shown below.

![Synchronized AD Users and Groups](image26.png)
8 DIGIPASS Management

8.1 Overview

In this section, we briefly explain aXsGUARD Gatekeeper DIGIPASS management, including:

- Importing DIGIPASS records to the aXsGUARD Gatekeeper.
- DIGIPASS device testing.
- Assigning, unassigning and deleting DIGIPASS records.

8.2 Importing DIGIPASS Records

Before DIGIPASS devices can be assigned to users and used for authentication, a DIGIPASS DPX file must be imported to the aXsGUARD Gatekeeper.

A DPX file can either be imported automatically or manually. Both procedures are explained below.

8.2.1 Automatic import

When a set of aXsGUARD Gatekeeper DIGIPASS devices has been ordered, the DPX file is automatically uploaded by the VASCO back office to your aXsGUARD Gatekeeper and a message is displayed in the status screen of the Administrator Tool (see below).

Image 27: Automatic DIGIPASS Status Message

To activate the new DPX file:

1. Click on the here link as shown above.
2. On the next screen, click on Apply.
3. To view the list of imported DIGIPASS records, navigate to Authentication > VASCO DIGIPASS > DIGIPASS.
8.2.2 Manual import

A DPX file can also be imported manually through the aXsGUARD Gatekeeper Administrator Tool. This is useful for importing (re-using) DIGIPASS devices and records which have been purchased with other VASCO products.

**Caution**
Importing a DIGIPASS DPX file without a valid license is not allowed. Contact your reseller for more information.

To import a DPX file:

1. Navigate to Authentication > VASCO DIGIPASS > Upload. A screen as shown below appears.
2. Click on Browse and select the DPX file.
3. Enter the provided DPX Transport Key. This is required because encryption is used for transport.
4. Click on Update to finish.
5. To view the list of imported DIGIPASS records, navigate to Authentication > VASCO DIGIPASS > DIGIPASS.

8.3 DIGIPASS Device Testing

The aXsGUARD Gatekeeper is equipped with a DIGIPASS device testing tool. This is useful to test a DIGIPASS device before assigning it to a user, or for troubleshooting.

To test a DIGIPASS device:

1. Navigate to Authentication > VASCO DIGIPASS > DIGIPASS.
2. Click on the serial number for the DIGIPASS device to be tested. The serial number is printed on the back of the DIGIPASS housing.
3. Click on Test OTP (Test One-Time Password).
4. Generate an OTP with the DIGIPASS device and enter the OTP in the DIGIPASS Code field.
5. Click on Test DIGIPASS.
Assigning DIGIPASS Devices

**Caution**
It is possible to assign a single DIGIPASS device to multiple users.
Assigning multiple DIGIPASS devices to a single user is not supported.

To assign a DIGIPASS device to a user:

1. Navigate to *Users & Groups > Users*.
2. Click on the user account to which the DIGIPASS device needs to be assigned.
3. Check the *Has VASCO DIGIPASS* option.
4. Click on *Select*.
5. Select the serial number for the DIGIPASS device to be assigned. The serial number is printed on the back of the device and is composed of digits separated by one or more dashes, depending on the model. The dashes are not displayed in the Administrator Tool (see below).
6. Click on *Update*.

**Image 29: Assigning a DIGIPASS record to a User**

**Tip**
Entering the last few digits of the serial number as a *Search Filter* speeds up the search for a particular DIGIPASS record.
8.5 Unassigning a DIGIPASS Device

A DIGIPASS device can be unassigned if a user is no longer authorized to authenticate, but the aXsGUARD Gatekeeper user data needs to be preserved.

To unassign a DIGIPASS device:

1. Follow steps 1 and 2 as explained in section 8.4.
2. Uncheck the Has VASCO DIGIPASS option.
3. Click on Update to finish.

8.6 Deleting DIGIPASS Records

Caution
Manually imported DIGIPASS records can be deleted by a system administrator (see section 8.2.2).

Automatically imported DIGIPASS records (see section 8.2.1) can only be deleted by the VASCO back office.

A DIGIPASS record cannot be deleted if it is assigned to a user account; it must be unassigned before it can be deleted (see above).

DIGIPASS records can be deleted from the aXsGUARD Gatekeeper, which is useful if the DIGIPASS hardware has been lost or stolen.

To delete a DIGIPASS record:

1. Navigate to Authentication > VASCO DIGIPASS > DIGIPASS.
2. Check the DIGIPASS record to be removed as shown below.
3. Click on Delete.
9 RADIUS Server Configuration

9.1 Overview

This section presents the basic steps to configure and deploy the aXsGUARD Gatekeeper RADIUS Authentication Server in your network.

For more information about the RADIUS protocol and aXsGUARD Gatekeeper RADIUS setups, please refer to the aXsGUARD Gatekeeper Authentication How To, which is available through the Documentation button in the Administrator Tool.

9.2 RADIUS Server Setup and Configuration

The aXsGUARD Gatekeeper acts as a RADIUS Authentication Server in the LAN.

This means that (custom) applications running in your LAN, DMZ or on your corporate gateway can relay authentication to the aXsGUARD Gatekeeper and support DIGIPASS authentication over RADIUS.

The hosts running the custom applications use a pre-shared RADIUS secret (key) to securely relay credentials to the aXsGUARD Gatekeeper (see image below) and must be added to the aXsGUARD Gatekeeper Computer list.

RADIUS configuration requires three steps, which are explained in the following sections:

1. Add the host (RADIUS Client) to the aXsGUARD Gatekeeper Computer list.
2. Configure the aXsGUARD Gatekeeper RADIUS server by adding the RADIUS Client.
3. Set the required Authentication Policy for the aXsGUARD Gatekeeper RADIUS Server.
9.2.1 Adding the RADIUS Client to the Computer list

Caution
The authenticating users on the RADIUS client must also be registered on the aXsGUARD Gatekeeper; otherwise authentication fails (see section 7.5).

To add the RADIUS client to the aXsGUARD Gatekeeper Computer list:

1. Navigate to Computers.
2. Click on Add new. A screen as shown below appears.
3. Enter the settings as explained in Table 5. The other aXsGUARD Gatekeeper Computer settings are not relevant to this setup and are explained in the aXsGUARD Gatekeeper System Administration and Authentication How To guides, which are available through the Documentation button in the Administrator Tool.
4. Click on Save.
RADIUS Server Configuration

Table 5: Computer Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Enter a name for the computer. If an invalid name is provided, an error message is displayed.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the numeric address which identifies the computer in the network, e.g. 192.168.1.50</td>
</tr>
</tbody>
</table>
9.2.2 Configuring the RADIUS Server

To configure the aXsGUARD Gatekeeper as a RADIUS server:

1. Navigate to Authentication > RADIUS > Clients.

2. Click on Add New. A screen as shown below appears.

3. Enter the settings as explained in Table 6.

4. Click on Save.

Table 6: Authentication > Radius > Clients: Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a name (ID) for the new client. An error message appears if an invalid name is entered.</td>
</tr>
<tr>
<td>Description</td>
<td>Add a description for the client (Optional).</td>
</tr>
<tr>
<td>Host name or IP</td>
<td>Select the RADIUS client from the drop-down list. The client should exist in the aXsGUARD Gatekeeper Computer list.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the Shared Secret of the RADIUS Client. (Click A to hide or unhide the shared secret as you type: see image above).</td>
</tr>
</tbody>
</table>
9.2.3 RADIUS Server Authentication Policy

Once the aXsGUARD Gatekeeper RADIUS server has been configured as explained in section 9.2.2, the Authentication Policy to be used needs to be configured. An Authentication Policy determines the type of authentication enforced, e.g. DIGIPASS One-Time Password (OTP) and/or a Static Password.

For more information about Authentication Policies please refer to the aXsGUARD Gatekeeper Authentication How To, available through the permanently available Documentation button in the Administrator Tool.

To configure an Authentication Policy for the RADIUS server:

1. Navigate to Authentication > Services.

2. Click on aXsGUARD Gatekeeper RADIUS Server. A screen as shown below appears.

3. Select the Authentication Policy, e.g. VASCO DIGIPASS.

4. Click on Update to save your settings.

With this configuration, all users authenticating on the RADIUS client (explained in section 9.2) must use a DIGIPASS OTP to authenticate. Other Authentication Policies and Methods are, of course, available. For more information, please refer to the aXsGUARD Gatekeeper Authentication How To, accessible through the permanently available Documentation button in the Administrator Tool.

Image 34: Setting the Authentication Policy for the RADIUS Server
10 What's Next

This guide provides minimal information to support installation and configuration of the aXsGUARD Gatekeeper serving exclusively as an authentication server.

The following documents providing further information are available through the Documentation button in the Administrator Tool:

- **aXsGUARD Gatekeeper System Administration How To**: this document explains the structure of the Administrator Tool, backup & restore and update infrastructures and network functions such as DHCP, NAT, DNS and Routing.

- **aXsGUARD Gatekeeper Authentication How To**: this document explains how to set up local and back-end authentication using policies, rules and restrictions. It also provides detailed instructions on how to configure and use the aXsGUARD Gatekeeper RADIUS Server.

- **aXsGUARD Gatekeeper Directory Services How To**: this document explains how to configure and use the aXsGUARD Gatekeeper Directory Services.

- **aXsGUARD Gatekeeper Reverse Proxy How To**: this document explains the optional module, Application Firewall (Reverse Proxy), and how to secure your Outlook Web Access or Citrix server, for example, with DIGIPASS authentication.
11 Support

11.1 Overview

In this section we provide instructions on what to do if you have a problem, or experience a hardware failure.

11.2 If you encounter a problem

If you encounter a problem with a VASCO product, please follow the steps below:

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.

3. If your supplier is unable to solve your problem, they will automatically contact the appropriate VASCO expert. If necessary, VASCO experts can access your aXsGUARD Gatekeeper remotely to solve any problems.

11.3 Return procedure if you have a hardware failure

If you experience a hardware failure, please contact your VASCO supplier.
Alphabetical Index

Active Directory.......................................................... 34
Administrator Password.............................................. 18, 20, 25
Administrator Tool......................................................... 17, 23, 48
AG-3XXX and AG-5XXX Models....................................... 7, 11, 13
aXsGUARD Gatekeeper.................................................. 9
Chassis Rails................................................................. 11
Configuration Instructions.............................................. 20
Connecting to your Network........................................... 15
Creating and Modifying Groups.................................
   Automatically.......................................................... 32
   Manually.................................................................. 31
Creating and Modifying Users.................................
   Automatically.......................................................... 34
   Manually.................................................................. 33
Customer Information.................................................... 22
DIGIPASS..............................................................
   Assigning.................................................................. 40
   Deleting.................................................................... 41
   Importing.................................................................. 38
   Search Filter............................................................ 40
   Testing.................................................................... 39
   Unassigning.............................................................. 41
   User Setting............................................................... 33
Dimensions................................................................. 11
Documents................................................................. 8, 48
Domain Name............................................................... 24
Domain Name Server.................................................... 29
DPX file.................................................................
E-mail Addresses.......................................................... 22, 25
Electrical Safety............................................................. 10
Email Relay................................................................. 29
Environmental Requirements & Protection.................... 10, 11
Ethernet Secure LAN Device......................................... 26
Further Reading & Configuration................................... 48
General Settings.......................................................... 29
Humidity.................................................................... 11
Knowledge Base........................................................... 49
LAN Interface............................................................... 13
Logs........................................................................... 21
Mailings from VASCO................................................... 22
Menu Structure............................................................... 23
Navigation.................................................................... 23
Network Cable............................................................... 10
Network Settings.......................................................... 26
Personal Safety.............................................................. 10
Power......................................................................... 10, 11, 13
Pre-installation.............................................................. 12
RADIUS Client.............................................................. 44
RADIUS Server............................................................. 43, 46
RADIUS Server Authentication Policy....................... 47
Return Procedure........................................................ 49
Safety ......................................................................... 10
Self-signed Certificate................................................... 17
Shared Secret............................................................... 46
Support........................................................................ 49
Sysadmin Password..................................................... 19, 24
System Information........................................................ 24
Temperature................................................................. 11
Testing TCP/IP Settings.................................................. 16
Training....................................................................... 8
Users and Groups.......................................................... 30
VASCO......................................................................... 9
Workstation TCP/IP Settings.......................................... 15

© 2009 - VASCO Data Security