



## **ViperGuard White Paper**

---

Javelina Software, LLC  
3524 South River Terrace  
Edgewater, MD 21037

Phone 410.798.9907 • Fax 410.798.5425

**Printed: July 2008**

**Copyright Notice**

© Javelina Software, LLC, 2008

All rights reserved. No part of this White Paper may be reproduced in any form or by any means without the express written permission of Javelina Software, LLC.

**Limited Liability**

THIS DOCUMENT MAY CONTAIN TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. ANY DOCUMENTATION WITH RESPECT TO JAVELINA SOFTWARE, LLC SOFTWARE PRODUCTS IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND DOES NOT EXTEND OR MODIFY THE LIMITED WARRANTY EXTENDED TO THE LICENSEE OF JAVELINA SOFTWARE, LLC SOFTWARE PRODUCTS.

**Trademark Acknowledgments**

Microsoft, Microsoft Active Directory, Windows, Windows XP, Windows 2000, Windows 2003 and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other brand and product names are trademarks or registered trademarks of their respective companies.

**Printed in the United States of America.**

## Introduction

It is well known that the most frequent request of the IT help desk is the call to reset a forgotten password. In fact, recent studies have estimated that password related problems comprise as much as 40% of help desk calls. And a recent Gartner Group study has estimated that the cost of those calls in a non-automated environment will range from \$51 to \$147 for the labor alone. Tackling this issue and reducing these costs are the primary goals of ViperGuard.

Meanwhile, the goal of this document is simply to provide you with an overview of the ViperGuard system: an introduction to what it does and how it does it. In addition to a description of its capabilities, each of the major components that comprise the ViperGuard system is described as well as how these components work together.

## Functionality

ViperGuard puts the task of resetting passwords back into the hands of the end-user, thus eliminating entirely those costly help desk calls. To achieve this, the ViperGuard system allows end users to unlock their own accounts and reset their own passwords by simply answering a few previously configured questions. ViperGuard will optionally install a custom logon prompt to the desktop of every user eligible for ViperGuard services. When the custom logon prompt is installed and an end user forgets their password, they simply click on a button on their logon screen (see figure 1) and are instantly linked to the ViperGuard Reset Password web site. The web site steps them through the process of authentication by asking them a few questions and allowing them to select a new password for their account. The web site in turn connects to a secure back end Win32 service which performs all the required authenticating, account unlocking, password resetting, auditing, and emailing.



FIGURE 1. Customized Logon prompt

## Installation

One of the major design goals for ViperGuard was to simplify the installation and management of an otherwise very complicated system. Toward this end, ViperGuard's setup is accomplished in a fairly simple two-step process. First, you must install the ViperGuard console to a Windows XP, Vista or Windows 2003 machine. Then, the first time you launch the Administrator's console itself, you will be presented with a wizard that walks you through an initial installation of ViperGuard onto your network.

The setup wizard leads you step-by-step through configuring each component of the ViperGuard system and, upon completion, installs each of those components including those destined for remote machines. ViperGuard components include web sites, Win32 services, GPO Policies, Active Directory groups and user accounts. The entire installation and configuration can easily be accomplished in less than half an hour and all from a single location. To make the process even simpler, we've linked each step of the installation to an in-depth help system and we've included a ViperGuard Quick Start Guide. Together these aids should provide you with the answers to any questions you have regarding the ViperGuard installation.

## Administration

For installing, configuring, and managing ViperGuard, the administrator is provided with an application called the Administrator's Console (see FIGURE 2). From the console you can expand ViperGuard's coverage on your network, configure your existing installation, run reports on ViperGuard usage, and other administrative tasks.

All installations and un-installations of ViperGuard components to your network are performed by wizards similar to the Setup Wizard in style if not in substance. So there are wizards for adding and removing managed domains, services, websites and desktop applications. Each is easy to navigate and will install all your network components from your workstation.

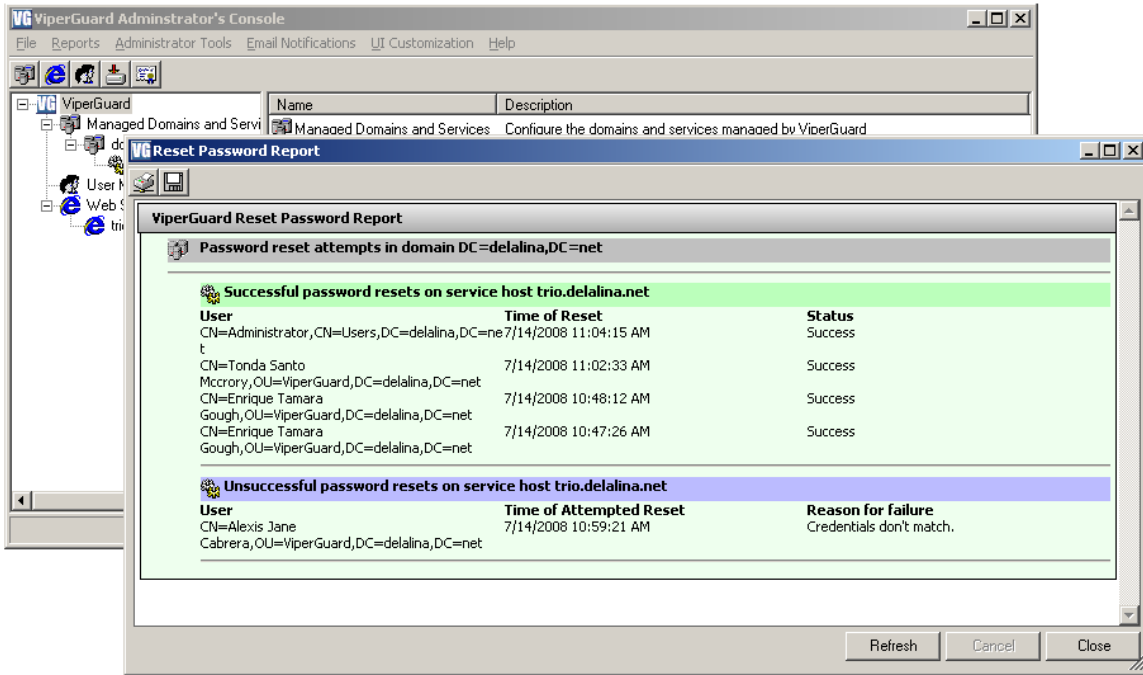


FIGURE 2 – ViperGuard Administrator's Console

## Active Directory Integration

ViperGuard is fully integrated into the Windows 2000/2003 and Active Directory (AD) environment. It does not rely on external databases, but rather stores all enrollment and configuration data in an encrypted format within AD itself, utilizing AD's built in replication and robustness to guarantee the availability and accuracy of the data. Usage of the Administrator's Console is restricted to members of the ViperGuard Admin Group. The Admin Group is an AD object and we rely on AD to enforce security rather than creating a new layer of security and bypassing the built-in mechanisms.

## Connectivity & Platform Support

Because ViperGuard utilizes web sites (see FIGURES 3 & 4) to perform enrolling and password resetting, there are various possibilities for connecting to the system. For example, users can access the system using one of the following methods:

- through a ViperGuard customized logon prompt using their own machine,
- by logging into their own machine with a well known and heavily locked down Help account,
- or, by logging into a special purpose kiosk machine.

And of course, using web sites to interface with ViperGuard also offers platform independence; i.e. a Unix or Apple workstation could access the web sites just as easily as a Windows machine.

## **Hardware and Software Requirements**

Because end users access ViperGuard through a web site, their only requirement is access to an Internet Browser, preferably IE 6.0 or higher. The Administrators Console, ViperGuard Win32 services and ViperGuard websites do have certain hardware and software requirements. These are listed below:

### **Console Pre-requisites**

The ViperGuard Administrators console must be installed to a machine running Windows XP or greater. The machine must be a member of your network and should have at least 40 Mbytes of disk space available.

Note that the logon account you use when running the console determines which domains you can manage. To manage a domain you must have Domain Administrator rights for that domain. If you are logged in with an Enterprise Administrator's account you can manage all domains in your forest.

### **Server Pre-requisites**

Win32 Servers in your network serve as hosts for the ViperGuard Win32 service while IIS servers in your network may serve as hosts for the ViperGuard websites. The requirements for each server type are listed below:

## Web Servers:

- Windows 2000 or higher
- IIS version 5 or higher
- ASP.NET version 1.1
- 10 MB disk space
- On 64 bit operating systems, 32 bit web apps must be enabled

## ViperGuard Service Servers:


- Windows 2000 or higher
- Version 1.1 .Net Framework
- 30 MB disk space

# ViperGuard Websites

Users enroll with ViperGuard using the ViperGuard Enrollment website (see FIGURE 3). To use the website, users enter their Windows credentials, select challenge questions to answer, supply answers to each question, and then submit their answers. The ViperGuard Win32 service fields the requests and writes the users questions and answers in encrypted form to Active Directory.

**Steps to Enrollment**

- Login**
- Select Questions**
- Answer Questions**
- Review Answers**
- Enroll**

 Powered by Javelina Software's **ViperGuard**

### Enroll with ViperGuard

Enter your Windows network name and password. The formats accepted for your name are as follows:

UPN:	YourName@YourDomain.com
NetBIOS:	YourDomainYourName
Fully Qualified Name:	CN=YourName,CN=Users,DC=YourDomain,DC=Com

-----

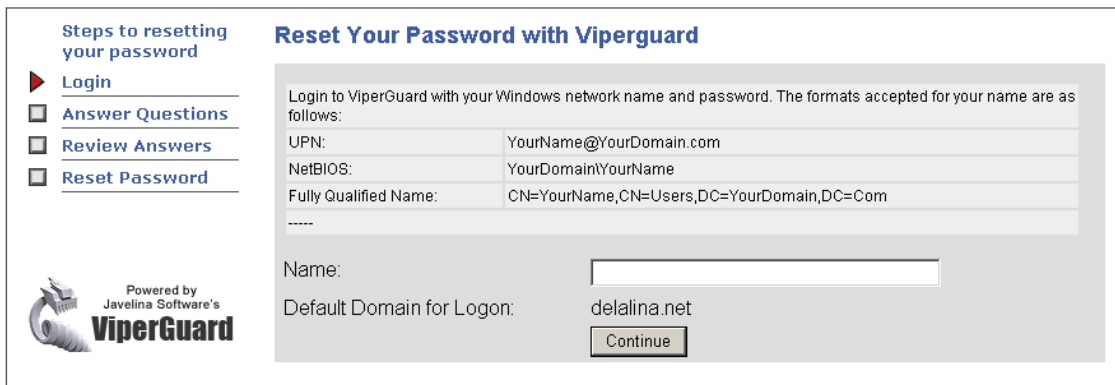
Name:

Password:

Default Domain for Logon: delalina.net

FIGURE 3. Enrollment Website

Users reset their password using the ViperGuard Reset Password website (see FIGURE 4). The user enters his or her Windows name, answers the challenges selected at the time of enrollment, and if the answers match the answers given at enrollment, the user can then change their Windows password and use the new password to log into Windows.



The screenshot shows a web interface for resetting a password. On the left, there is a sidebar with the heading "Steps to resetting your password" and a list of steps: "Login", "Answer Questions", "Review Answers", and "Reset Password". The "Reset Password" step is currently selected. Below the sidebar is the ViperGuard logo, which includes the text "Powered by Javelina Software's ViperGuard". The main content area is titled "Reset Your Password with ViperGuard". It contains a login form with the following fields and values:

UPN:	YourName@YourDomain.com
NetBIOS:	YourDomainYourName
Fully Qualified Name:	CN=YourName,CN=Users,DC=YourDomain,DC=Com

Below the table, there is a "Name:" label followed by an empty text input field. Underneath that is a "Default Domain for Logon:" label followed by the text "delalina.net" and a "Continue" button.

FIGURE 4. Reset Password Website

## ViperGuard Network Architecture

There are four major components that comprise the ViperGuard network architecture: the administrator's console, the Win32 service, the user websites, and the desktop applications (i.e. the custom logon prompt and the enrollment reminder applications). All components are installed and automatically upgraded when necessary from your workstation.

### Administrator's Console

The Administrator's Console, which was previously described in the Administration section, enables the ViperGuard administrator to install and configure every piece of the ViperGuard system. The majority of the configuration information modified by the console, for the services and websites for example, is stored within Active Directory (AD) attributes. This allows us to utilize the built in redundancy, security and distribution of AD. Of

course, the console also interfaces directly with the services in order to control their behavior, such as when broadcasting an email reminder to all un-enrolled users.

## **Services**

ViperGuard utilizes a Win32 service to perform numerous background tasks such as authenticating the users of the ViperGuard websites, changing passwords, sending out emails, et cetera. ViperGuard services are also utilized by the two ViperGuard websites to retrieve challenge questions, set user responses and check user responses against previously stored information.

ViperGuard services have a domain-wide scope. In other words, to provide ViperGuard password management services to users in a domain, there must be at least one ViperGuard service running in that domain. ViperGuard uses the term 'Managed Domain' to refer to any domain that contains one or more ViperGuard services. And though we use the term 'Managed Domain', you can elect to manage OU's within the domain rather than the whole domain.

An initial Managed Domain and service is installed at the time the Setup Wizard is run. Additional services can be added to any Managed Domain from the Administrator's console. Additional Managed Domains can also be added from the console.

## **Websites**

There are two ViperGuard websites that host user functions; the ViperGuard Enrollment website and the ViperGuard Reset Password website. Each website communicates with the ViperGuard service to perform its function.

The ViperGuard Enrollment website presents the user with a set of challenge questions. After authenticating with a name and password, the user enrolls by first selecting any challenge questions he or she wants to answer. Then the user supplies answers to each of the challenge questions selected, plus answers to any challenge questions set by an Administrator as mandatory. A ViperGuard Administrator specifies the minimum number of questions that must be answered and may choose to designate one or more questions that all users must answer. To retrieve the challenges and to submit the answers the website communicates with a ViperGuard service in the user's domain. The service writes the answers submitted by a user in encrypted form to Active Directory.

The ViperGuard Reset Password website presents the user with the same set of challenge questions he or she answered at enrollment. The user's answers to these questions must match the answers given when he or she enrolled. If that is the case, the user is allowed to reset his or her password. As with the enrollment website, the ViperGuard service is utilized to retrieve the challenge questions, and in this case to check the answers submitted against the user's answers at the time of enrollment. The service also takes care of resetting the user's password.

To install a website the administrator simply selects an IIS server from somewhere in the forest to host the ViperGuard web applications. An initial website is installed at the time the Setup Wizard is run. Additional websites can be added from the Administrator's console.

### **ViperGuard Desktop Application (Group Policy Objects)**

ViperGuard can optionally install up to two applications on the desktops of users in a ViperGuard 'Managed Domain'; a custom logon prompt and an Enrollment Reminder. The Enrollment Reminder is an application that allows un-enrolled users to access the ViperGuard Enrollment website via a simple desktop reminder dialog. The custom logon installation includes both the logon prompt and the enrollment reminder application as part of its installation.

Both the enrollment reminder application and the custom logon prompt are delivered to users' desktops by the use of software distribution Group Policy Objects (GPOs) and once installed these GPOs can be viewed by using the supplied Group Policy Management Console application written by Microsoft Corporation. The custom logon prompt is distributed by a GPO named VG\_LogonProviders. The enrollment reminder application is distributed by a GPO named VG\_EnrollmentReminder.

Once installed to a user's machine, each desktop application has a unique purpose. The Enrollment Reminder App (ERA) has 2 responsibilities. Primarily, at user logon and every four hours subsequent to the logon, ERA reads information from Active Directory in order to locate the ViperGuard websites in your forest. This information is subsequently used by both ERA and the ViperGuard logon prompts. ERA's secondary responsibility is to check if the currently logged in user is enrolled with ViperGuard. If the user is enrolled, ERA goes back to sleep. Otherwise, a dialog will appear offering the user the option of enrolling with

ViperGuard now, or being reminded later. If the user chooses to enroll, ERA will launch a web browser loaded with a ViperGuard Enrollment website, and from that point on the user can answer his or her challenge questions and enroll with ViperGuard. If the user decides not to enroll at that time, ERA goes back to sleep. ERA repeats this cycle every 4 hours.

The second desktop application, the custom logon prompt, installs what is known as a GINA extension on Windows 2000/2003/XP or a Credential Provider on Windows Vista. With the Logon Prompt installed, the user has the option to enroll or reset their password with ViperGuard as part of their normal Windows logon experience. Whether it is the GINA extension or the Vista credential provider, both allow the user to get from a Windows Logon prompt to a ViperGuard website (to reset a forgotten password for instance) without ever having to contact a help desk, or use another machine already logged into Windows. The user can access the ViperGuard Reset Password website, answer their challenges and reset their Windows password, return to the Windows logon prompt, and then log in to Windows using their new password.

## Summary

Even though ViperGuard is obviously a complex system of components, the end result for everyone involved is an easy to install, easy to use system. By reducing the number of help desk calls for account unlocks and password resets, ViperGuard effectively lowers the cost of administration and frees help desk technicians for more critical issues. The web-based interface for end-users allows password maintenance from anywhere in the network, while the logon prompt integration provides for the greatest ease of use and simplest means of access. Meanwhile, detailed event logging and event based emails provide for increased security and auditing compliance. And our single point installation of all components through the administrator's console eliminates tedious and lengthy installs.

Hopefully this document has answered all your technical questions regarding the ViperGuard system. But if you have any remaining questions, please contact us at 1-800-397-5484 or email us at [support@javelinasoftware.com](mailto:support@javelinasoftware.com).