SafeNet Authentication Service

Integration Guide

Protecting Microsoft Internet Security and Acceleration (ISA) Server 2006 with SAS

Document Information

Document Part Number	007-012644-001, Rev A
Release Date	July 2009

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft Internet Security and Acceleration Server 2006.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

By default, the Microsoft Internet Security & Acceleration Server 2006 requires that a user provide a correct user name and password to successfully logon to the VPN. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a SafeNet token using the configuration instructions provided below.

Applicability

This guide is applicable to the following:

Security Partner Information	
Security Partner	Microsoft
Product Name and Version	Microsoft Internet Security & Acceleration Server 2006
Protection Category	Remote Access

SAS Server	
Authentication Server	SafeNet Authentication Service
Version	3.2 or higher

Assumptions

It is assumed that SafeNet Authentication Service has been installed and configured and a “Test” user account can be selected in the **Assignment** tab.

Operation

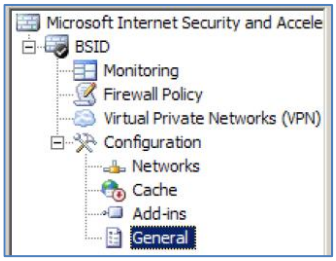
A RADIUS server is specified within the general server configuration section. The VPN connections are then configured to send authentication requests to the SAS RADIUS server. The SAS server then authenticates the provided credentials (Username and OTP), and either grants or rejects the user access.

Prerequisites

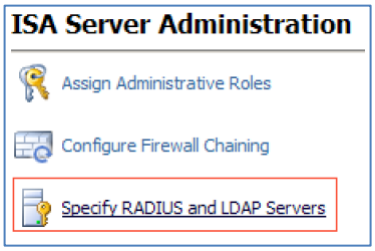
- The SAS agent for Microsoft Internet Authentication Service server (IAS) or Network Policy Server has been installed.
- The Microsoft ISA server must be a valid RADIUS client within your RADIUS server. This will allow RADIUS requests to be sent from Microsoft ISA 2006 to the RADIUS server.

Configuring ISA Server 2006 for Two-Factor Authentication

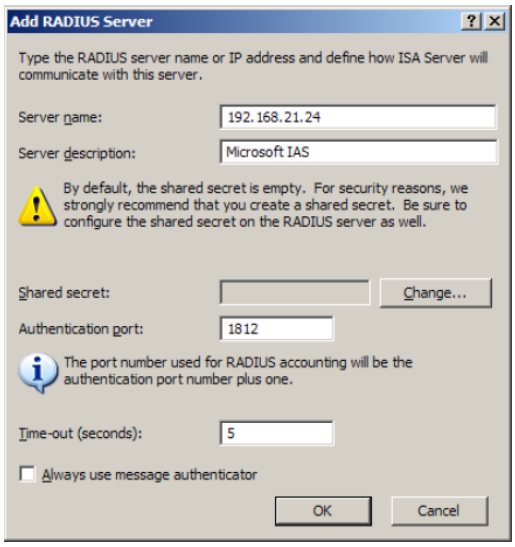
1. Launch the ISA Server Management tool.
2. Expand **(Servername) > Configuration**.
3. Click on General.



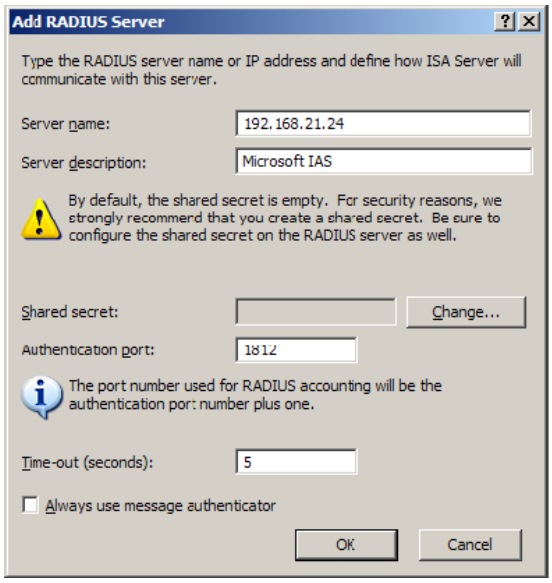
4. Under **ISA Server Administration**, click **Specify RADIUS and LDAP Servers**.



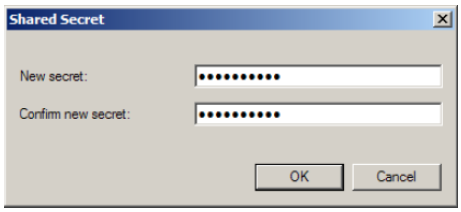
5. On the **RADIUS Servers** tab, click **Add**.



6. In the **Shared Secret** field, click **Change**.



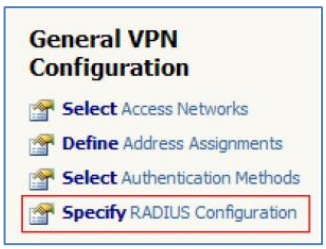
7. Enter the secret in the **New secret** and **Confirm new secret** fields, and then click **OK**.



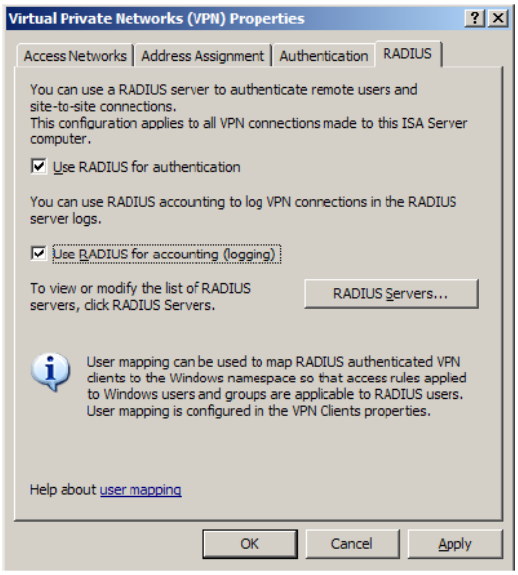
Using the RADIUS Server with VPN Configuration

1. In the ISA Server Management console, click **Virtual Private Networks (VPN)**.

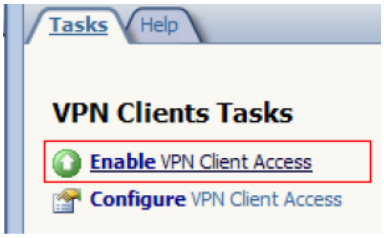
2. In the right pane, click **Specify RADIUS Configuration**.



3. Click the **RADIUS** tab. Select the **Use RADIUS Authentication** and **Use RADIUS for accounting (logging)** options, and then click **OK**.



4. In the right pane, under **VPN**, click **Enable VPN Client Access**.



Troubleshooting

Logging

By default, Microsoft ISA server 2006 has the ability to show live logging information from its reporting features. This should be used as a primary log source to determine authentication issues. Upon requiring more information, the SAS **Snapshot** tab should be used to determine authentication failure cause.

Failed Logons

Symptom	Authentication request is rejected by the VPN client.	
Indication	11/19/2013 12:36:49 PM	Henry Authentication Failure 312212345 192.168.21.120 Invalid PIN
Possible Causes	An incorrect server side PIN is being used.	
Solution	Reset the server-side PIN within the SAS console	

Symptom	Authentication request is rejected by the VPN client.							
Indication	11/19/2013 12:47:24 PM	Henry	Authentication	Failure	312212345	192.168.21.120	Invalid Authentication response	
Possible Causes	An invalid token code is being provided							
Solution	Verify the token code is being typed correctly. Verify the token code is being typed with all correct CaSiNg applied to all characters. The token could be out of sync. Resync the token from within the console manager.							

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	