DualShield
for IIS 6.0
Implementation Guide
(version 5.2)
Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Northway House
1379 High Road
London N20 9LP
United Kingdom

Tel:  +44(0)20 8343 9663
Fax:  +44(0)20 8446 3182
Web:  www.deepnetsecurity.com
Email: support@deepnetsecurity.com
Table of Contents

Overview ................................................................................................................................. 4
Installation ............................................................................................................................... 5
  Installation Prerequisites ................................................................................................. 5
  Installation Procedure ....................................................................................................... 5
Configuration .......................................................................................................................... 6
  Configure Authentication Server .................................................................................. 6
  Configure IIS Server ........................................................................................................ 6
    ASP.NET ........................................................................................................................... 6
    Host Name ........................................................................................................................ 6
    DasWeb Virtual Path ....................................................................................................... 7
  Configure IIS Agent ......................................................................................................... 7
    Protecting an Entire Web Site ....................................................................................... 8
    Protecting Individual Directories .................................................................................. 9
    Protecting Individual Files ............................................................................................ 9
    SSO Server Settings ....................................................................................................... 10
    Advanced Logon Settings .............................................................................................. 10
    Policy Settings ............................................................................................................... 12
    Session Settings ........................................................................................................... 13
    IP Filter ......................................................................................................................... 13
  Configure SSO Logon Service ....................................................................................... 14
Authentication ....................................................................................................................... 15
Appendix A. Outlook Web Access ...................................................................................... 17
Overview

Microsoft Internet Information Server is the world’s most popular web server. DualShield IIS Agent is a plugin component that adds multi-factor authentication to the IIS server. It allows access only to those users who provide multi-factor authentication using a variety of strong authentication tokens provided by DualShield unified authentication platform.

The complete solution consists of the following components:

- DualShield Authentication Server
- DualShield SSO Server
- DualShield IIS Agent

DualShield IIS Agent acts as the bridge that connects the Microsoft Internet Information Server and the DualShield Authentication Server. Technically, DualShield IIS Agent is an ISAPI extension/filter.
Installation

Installation Prerequisites

- Microsoft Internet Information Server 5.0/6.0 installed and operational.

Supported Platforms

- Windows Server 2003, Standard and Enterprise Editions, with Internet Information Services (IIS) 6.0 and .NET 2.0+ installed.
- Windows 2000 Server with Service Pack 4 and Internet Information Services (IIS) 5.0 or 6.0

System Requirements

- Intel Pentium or higher.
- 256 MB of RAM.
- 10 MB of free disk space.
- TCP/IP networking.

Installation Procedure

DualShield Authentication for IIS (DualShield IIS Agent) should only be installed after the DualShield Unified Authentication Platform has been successfully installed and operational.

DualShield IIS Agent should be installed on the same machine on which the Microsoft Internet Information Server (IIS) is installed and operating.

To install the DualShield IIS Agent, simply launch the installer “SetupDualIIS6_x86.exe” on 32-bit Windows Server or “SetupDualIIS6_x64.exe” on 64-bit Windows Server, and then follow the on-screen instruction.

After the DualShield IIS Agent has been successfully installed, you need to restart the IIS server.
Configuration

After the successful installation of the DualShield IIS Agent, you need to configure the following components:

- DualShield Authentication Server
- Microsoft IIS Server
- DualShield IIS Agent

Configure Authentication Server

DualShield authentication server can support multiple applications. Depending on your company’s IT infrastructure and security policy, you may set up different DualShield applications for different types of access. For instance, one application for VPN remote access, one for Windows logon and one for IIS. You can, of course, set up just one application for all types of access.

Once the DualShield application for IIS has been created and configured in the authentication server, you will then need to add to the application those users who are required to be authenticated with two-factor authentication. Each user should be allocated one or more authentication token(s) such as MobileID, SafeID and/or TypeSense etc.

Please refer to the administration guide of the authentication platform for details of how to set up applications, create users and tokens.

Configure IIS Server

ASP.NET

DualShield IIS Agent requires the Microsoft IIS server to support ASP.NET. If your IIS server does not allow ASP.NET then you need to turn on the option.
DasWeb Virtual Path

You may have noticed that a virtual path named DasWeb has been added after the installation of the DualShield IIS Agent. DasWeb is the home directory of the DualShield IIS Agent, and it must be accessible by your users.

Configure IIS Agent

You need to configure the DualShield IIS Agent so that it is connected to the DualShield Single Sign-On (SSO) server. You will also need to configure the Web access authentication settings to specify the web pages or directories that need to be protected.

You administer the DualShield IIS Agent and Web access authentication settings of your IIS web servers through the Internet Information Service Manager (ISM) that has been extended with the DualShield property sheet.

You can protect any type of resource, from an entire web site to individual directories and files.
Protecting an Entire Web Site

In the Internet Service Manager (ISM), right-click the appropriate web site, and click Properties.

1. In the Properties dialog box, click DualShield to display the Web Access Authentication Properties sheet.

2. To enable two-factor authentication on the web site, check the “Enable Two-Factor Authentication on Current Node” option.

3. Check the “Apply Settings to Child Nodes” option, so that all directories and files that belong to the site inherit this protection status.

4. Select the Service Type: Generic

5. Skip to the “URL Bindings” section
Protecting Individual Directories

1. In the Internet Service Manager (ISM), right-click the appropriate directory, and click Properties.

2. In the Properties dialog box, click Deepnet Authentication to display the Web Access Authentication Properties sheet.

3. To protect the directory, check the “Enable Two-Factor Authentication on Current Node” option. All files belong to this directory inherit this protection status.

4. To protect subdirectories that belong to the directory, check the “Apply Settings to Child Nodes” option.

5. Select the appropriate Service Type, e.g. Outlook Web Access, Outlook Anywhere, Outlook ActiveSync or Generic.

6. Skip to the “URL Bindings” section

Protecting Individual Files

1. In the Internet Service Manager (ISM), right-click the appropriate file, and click Properties.

2. In the Properties dialog box, click Deepnet Authentication to display the Web Access Authentication Properties sheet.

3. To protect the file, check the “Enable Two-Factor Authentication on Current Node” option.

7. Select the Service Type: Generic

8. Skip to the “URL Bindings” section
URL Bindings

Any type of resource, such as a website, a directory or a file, to be protected by the DualShield must be given a unique URL. A binding URL must include a binding protocol (HTTP or HTTPS), FQDN and path, i.e.

http://fqdn/path

or

https://fqdn/path

A resource may contain more than one binding if the resource requires different protocols or binding FQDN.

Advanced Logon Settings

If the resource to be protected with DualShield two-factor authentication has its own logon process, then the logon process must be form based. For instance, to add two-factor authentication to the Outlook Web Access (OWA), then the OWA’s logon process must be configured to work in the Form-Based Authentication (FBA) mode. Furthermore, you will need to provide the Advanced Logon Settings to include the information such as the logon and logout URL etc. so that DualShield can interact with the logon form.
The Logon URL, Logout URL and Submit URL can be expressed in plain text string or regular expression (RegEx). If it is expressed in RegEx then it must start with "\" followed by the RegEx pattern string.

Cookies
When a user attempts to logout by clicking the Logout URL, DualShield will clear its own session data and cookies. Normally, the protected resource or application will clear its own session data and cookies too. However, if the application does not clear its own session data and cookies then you can ask DualShield to clear them by providing the names of the cookies.

SSO Server Settings
You need to connect the DualShield IIS Agent to the DualShield SSO Server by providing the SSO server address, port and the application, etc.
Enter your DualShield SSO Server’s address and port number, and click Connect.

**Server Address**
The domain name or IP address of the DualShield SSO Server.

**Server Port**
The TCP/IP port of the Management Service of the DualShield SSO Server. By default, it is 8075.

**SSL**
If you have installed the DualShield Authentication Server with SSL connection, then you must tick this option. Otherwise, do not tick this option.

**Application**
The DualShield application(s) that manages the protected resource and its users.

*Please note that the DualShield SSO Server and Port settings are global to the entire web server whilst the Application settings are local to currently selected resource. In other words, there is only one set of Server Settings but each protected resource can be connected to a set of different applications.*

**Auto Logon**
Some applications, such as Outlook Web Access, Citrix Web Interface, have their own logon interface which authenticates users against Active Directory password. With those types of applications, you would typically configure DualShield IIS Agent to carry out the second factor authentication only, e.g. the token authentication, and leave the first factor, i.e. the Static Password authentication to the application itself. If this is the architecture that you are setting up, then do not check the Auto Logon option.

You can, however, also configure the DualShield IIS Agent to carry out two-factor authentication including token and static password, and ask the DualShield IIS Agent to pass the user’s credentials to the backend application and automatically login the user to the application. In this case, you should check the Auto Logon option.

**Policy Settings**
Click the “Policy...” button to set your authentication policies.
Exempt Local Traffic from Two-Factor Authentication
Local Traffic means traffic originated from the local machine, not the local network.

Session Settings

Normally, a browsing session only expires when the user closes their web browser. For added security, the DualShield IIS Agent allows you to control the expiration time of the current browsing session. You can make the browsing session expire if the user remains idle for the specified expiration time, and to make the session expire after the specified expiration time is reached whether or not the user is idle.

The session settings are global to the entire web server.

IP Filter

If you wish to exempt users from two-factor authentication when they come from an IP address that is trusted, then you should add the users’ IP addresses to the Trusted IP List. All traffic comes from a trusted IP address is exempted from two-factor authentication.
Trusted IP list is local to the currently selected resource. Every protected directory and file inherits the trusted IP list from its parent node, but you can override it by creating a trusted IP list for a selected resource.

**Configure SSO Logon Service**

When a user attempts to access a protected resource, they will be redirected to the DualShield SSO logon pages. By default, the TCP port number of the DualShield SSO logon service is set to 8074. You must configure your firewall settings so that the DualShield SSO Logon service is accessible from the public network.

Note: In IIS 7.0, DualShield IIS Agent has an option that enables you to proxy the SSL Logon pages through the IIS serve, which means that you do not need to allow direct access from the public network to the SSO Logon pages.
Authentication

When a user attempts to access a protected resource and the user has not been authenticated, then the user will be redirected to the DualShield SSO logon pages.

The logon procedure of the protected resources is configured in the DualShield Management Console. You can create a logon procedure that consists of one or more logon steps. In each logon step, you can specify the authenticators that the users can use to authenticate themselves.

For instance, an OWA logon procedure typically consists of two steps.

Step 1

DualShield SSO asks the user to verify by providing credentials of the second factor, e.g. One-Time Password or any other authentication methods that DualShield supports.

Step 2

Once the DualShield SSO has successfully verified the user, it redirects the user to the OWA’s logon page where the user must authenticate themselves with their AD password.

When the DualShield SSO redirects the user to the OWA’s logon page, it also passes the user’s login name and automatically disables the login name entry in the OWA’s logon page. The user does not need to enter their login name again and cannot change the login name. Furthermore, the DualShield SSO will check the login name submitted in the OWA’s logon page and make sure that the login name has not been altered by any means.
Domain\user name: john.smith
Password: 

Security
- Public or shared computer
  Select this option if you use Outlook Web Access on a public computer.
- Private computer
  Select this option if you are the only person who uses this computer.
  Warning: By selecting this option you acknowledge that the computer complies with your organization’s security policy.
Appendix A. Outlook Web Access

This chapter describes the settings for Outlook Web Access for Exchange 2003.

1. To protect OWA with DualShield multi-factor authentication, select the “ExchWeb\bin\auth” virtual path.
2. Right click it and select properties. In the properties box, select the “Deepnet Authentication” page.