



**Deepnet Unified Authentication
for Internet Information Server
User Guide**

**Copyright 2007,
Deepnet Security Limited.**

Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, FlashID, SafeID, SmartID, SmartKey, TypeSense, VoiceSense, MobilePass, DevicePass, RemoteID 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
The Maples Business Centre
144 Liverpool Road
London, N1 1LA
United Kingdom

Tel: +44(0)20 7700 4282
Fax: +44(0)20 7697 8282
www.deepnetsecurity.com
support@deepnetsecurity.com

Table of Contents

Overview 3

Installation 4

 Installation Prerequisites..... 4

 Installation Procedure..... 4

Configuration 5

 Configure Authentication Platform 5

 Configure IIS Agent 6

Protection Settings 7

 Protecting an Entire Web Site..... 7

 Protecting Individual Directories 7

 Protecting Individual Files..... 8

Authentication Settings 8

Session Settings 10

Trusted IP List..... 10

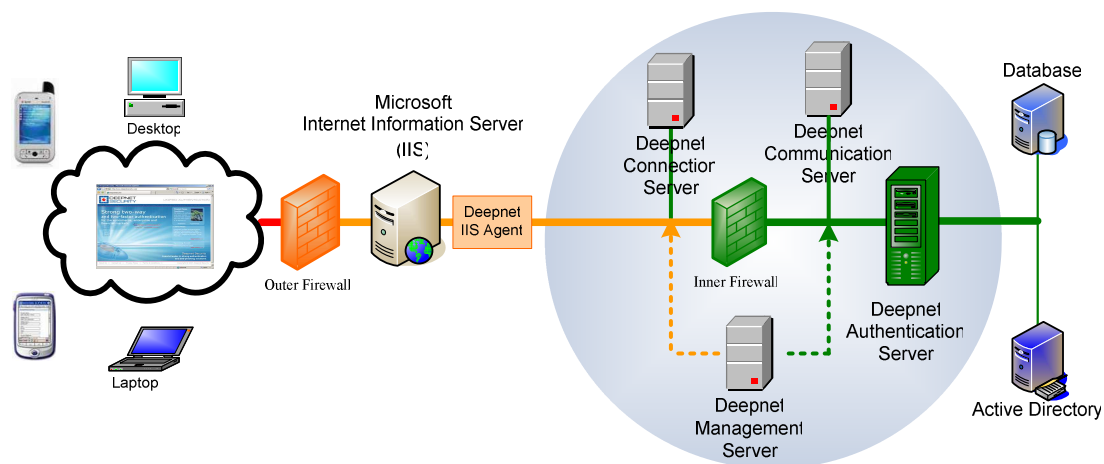
Authentication 11

Customisation 13

Overview

Microsoft Internet Information Server is the world's most popular web server. Deepnet Unified Authentication for IIS allows you to protect selected web servers or web pages with strong two-factor authentication, requiring a user to authenticate with a second factor credential such as one-time password before access to protected web pages is allowed.

Deepnet Unified Authentication for IIS is one of many enterprise solutions that the Deepnet Unified Authentication Platform supports. The following diagram illustrates the typical components involved in the Deepnet Unified Authentication for IIS solution:



The complete solution consists of the following components:

- Deepnet Unified Authentication Platform
- Deepnet IIS Agent

Deepnet IIS Agent acts as the bridge that connects the Microsoft Internet Information Server and the Deepnet Authentication Server. Technically, Deepnet IIS Agent is a ISAPI filter.

Installation

Installation Prerequisites

- Deepnet Unified Authentication Platform installed and registered. Please refer to the User Guide of the Platform for details.
- Microsoft Internet Information Server 5.0 or 6.0 installed and operational.

Supported Platforms

- Windows Server 2003, Standard and Enterprise Editions, with Internet Information Services (IIS) 6.0
- Windows 2000 Server with Service Pack 4 and Internet Information Services (IIS) 5.0

System Requirements

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

Installation Procedure

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

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

To install the Deepnet IIS Agent, simply launch the installer "SetupIIS.exe" and follow the on-screen instruction.

Configuration

After the successful installation of Deepnet Unified Authentication for IIS (Deepnet IIS Agent), you need to configure the following components:

- Authentication Platform
- IIS Agent

Configure Authentication Platform

Deepnet Unified Authentication Platform can support multiple applications. Depending on your company's IT infrastructure and security policy, you may set up different 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 application for IIS has been added to the Authentication Platform, 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, PocketID and/or TypeSense etc.

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

Configure IIS Agent

You need to configure the Deepnet IIS Agent so that it is connected to the Deepnet authentication server. You will also need to configure the Web access authentication settings to specify the web pages that need to be protected.

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

The screenshot shows the 'Default Web Site Properties' dialog box with the 'Deepnet Authentication' tab selected. The dialog is divided into several sections:

- Navigation Tabs:** Directory Security, HTTP Headers, Custom Errors, Web Site, ISAPI Filters, Home Directory, Documents, Deepnet Authentication (selected), ASP.NET, Server Extensions.
- Enable Two-Factor Authentication on Current Node:** (unchecked)
- Apply Settings to Child Nodes:** (unchecked)
- Service Type:** Standard (dropdown menu)
- Deepnet Authentication Section:**
 - Server Address: [Text Field]
 - Server Port: [Text Field] with a 'Change' button
 - Application: [Dropdown Menu]
 - Primary Authenticator: [Dropdown Menu]
 - Require Static Password Authentication: (unchecked)
- Session Section:**
 - Session Expires If Not Used Within: 20 Minutes
 - Session Always Expires After: 720 Minutes
- Trusted IP List Section:**
 - Table with columns 'From' and 'To'.
 - Buttons: Add, Delete
- Bottom Buttons:** OK, Cancel, Apply, Help

Protection Settings

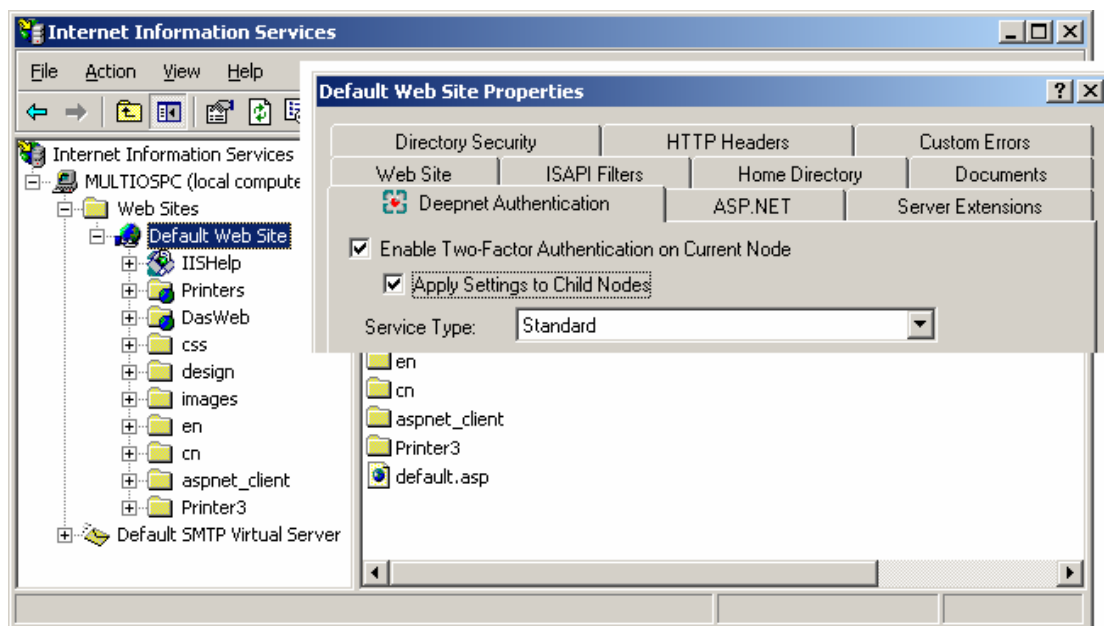
You can protect any type of resource, from an entire web site to individual directories and files.

Protecting an Entire Web Site

To protect all resources of a web site:

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

1. In the Properties dialog box, click Deepnet Authentication to display the Web Access Authentication Properties sheet.
2. To enable Web access 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: Standard
5. Continue to the "Authentication Settings"



Protecting Individual Directories

To protect a specific directory:

1. In the Internet Service Manager (ISM), double-click the appropriate web site.

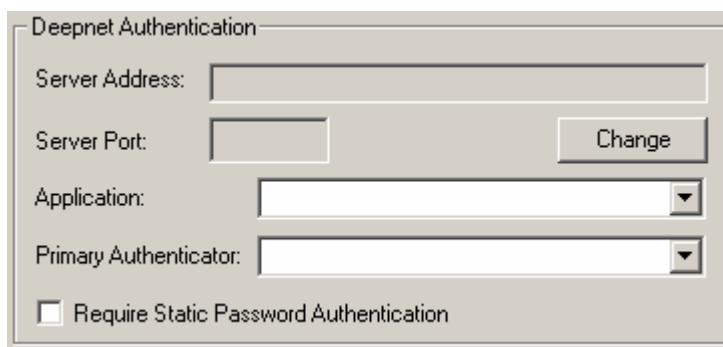
2. Right-click the appropriate directory, and click Properties.
3. In the Properties dialog box, click Deepnet Authentication to display the Web Access Authentication Properties sheet.
4. To protect the directory, check the "Enable Two-Factor Authentication on Current Node" option. All files belong to this directory inherit this protection status.
5. To protect subdirectories that belong to the directory, check the "Apply Settings to Child Nodes" option.
6. If the directory is for Microsoft Server ActiveSync, select Service Type: Server ActiveSync. Otherwise, select Service Type: Standard.
7. Continue to the "Authentication Settings"

Protecting Individual Files

1. In the Internet Service Manager (ISM), double-click the appropriate web site.
2. Right-click the appropriate file, and click Properties.
3. In the Properties dialog box, click Deepnet Authentication to display the Web Access Authentication Properties sheet.
4. To protect the file, check the "Enable Two-Factor Authentication on Current Node" option.
8. Select the Service Type: Standard
9. Continue to the "Authentication Settings"

Authentication Settings

You need to connect the Deepnet IIS Agent to the Deepnet Authentication Server by providing the server address, port and the application, etc.



Deepnet Authentication

Server Address:

Server Port:

Application:

Primary Authenticator:

Require Static Password Authentication

Server Address

The domain name or IP address of the Deepnet Authentication Server.

Server Port

The TCP/IP port of the Deepnet Authentication Server.

Application

The application that manages the protected resource and its users.

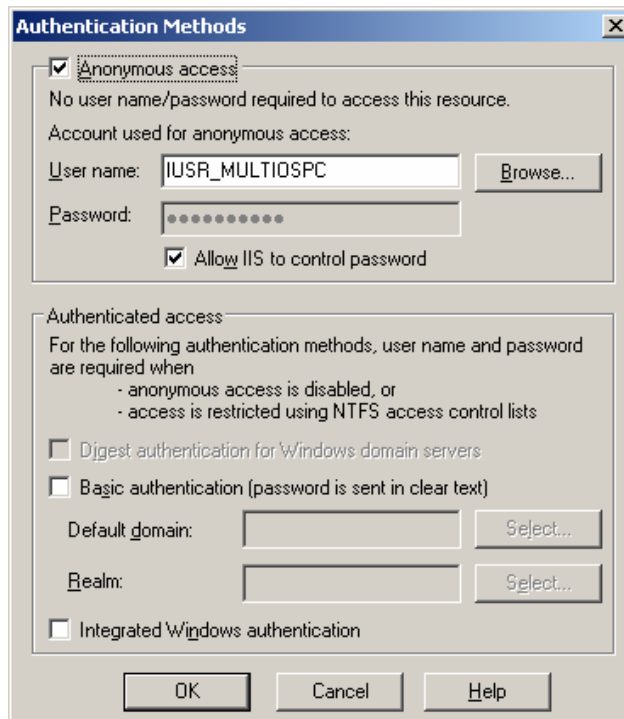
Primary Authenticator

The default authentication method.

Require Static Password Authentication

The "Require Static Password Authentication" feature can be used to replace the "Directory Security" function provided by IIS, providing a consistent user experience in the two-factor authentication process.

If you enable "Require Static Password Authentication" option, during the logon process users will be asked to authenticate their static password first, and then to authenticate their second-factor authentication token. In other words, the Deepnet IIS Agent will carry out two factor authentication, eliminating the need for IIS to authenticate the user. Therefore, you can check "Anonymous access" in the Directory Security settings in ISM.

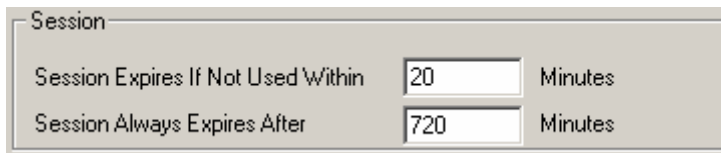


If this option is enabled, you need to make sure that a static password is provided to each user. This can be achieved by either connecting the application to the Active Directory that manages all users or by giving each user a StaticPass token in the Deepnet Authentication Server.

Please note that the Deepnet Authentication Server and Port settings are global to the entire web server whilst the other settings in this section 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 different application etc.

Session Settings

Normally, a browsing session only expires when the user closes their web browser. For added security, the Deepnet 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.

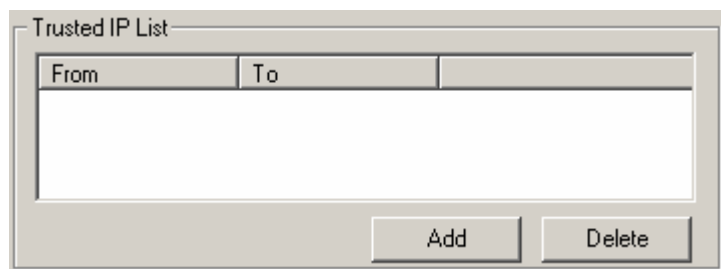


Session		
Session Expires If Not Used Within	20	Minutes
Session Always Expires After	720	Minutes

The session settings are global to the entire web server.

Trusted IP List

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 IP address to the Trusted IP List. All traffic comes from a trusted IP address is exempted from two-factor authentication.



Trusted IP List	
From	To

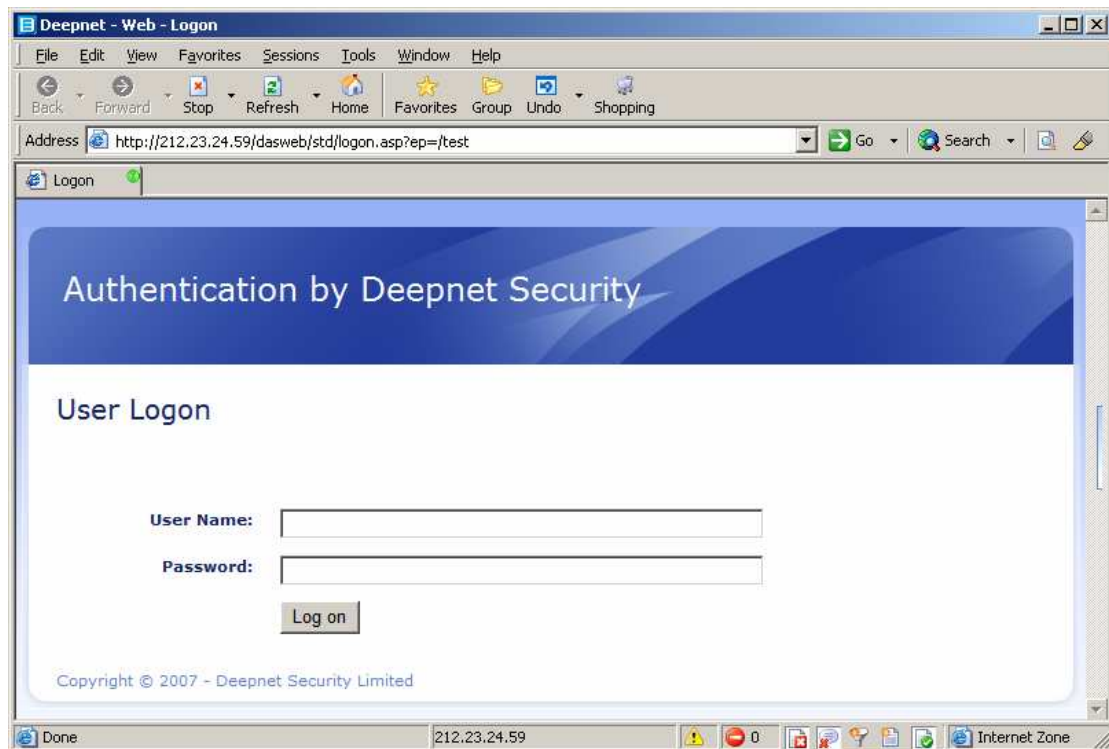
Trusted IP list is local to the currently selected resource. Every protected directory and file inherits the trusted IP list from its parent node, but you can override it by creating a trusted IP list for a selected resource.

Authentication

When a user attempts to access a protected resource, they will be redirected to the two-factor authentication logon pages. Depending on the setting of the "Require Static Password Authentication" option, the user might or might not be asked to authenticate their static password.

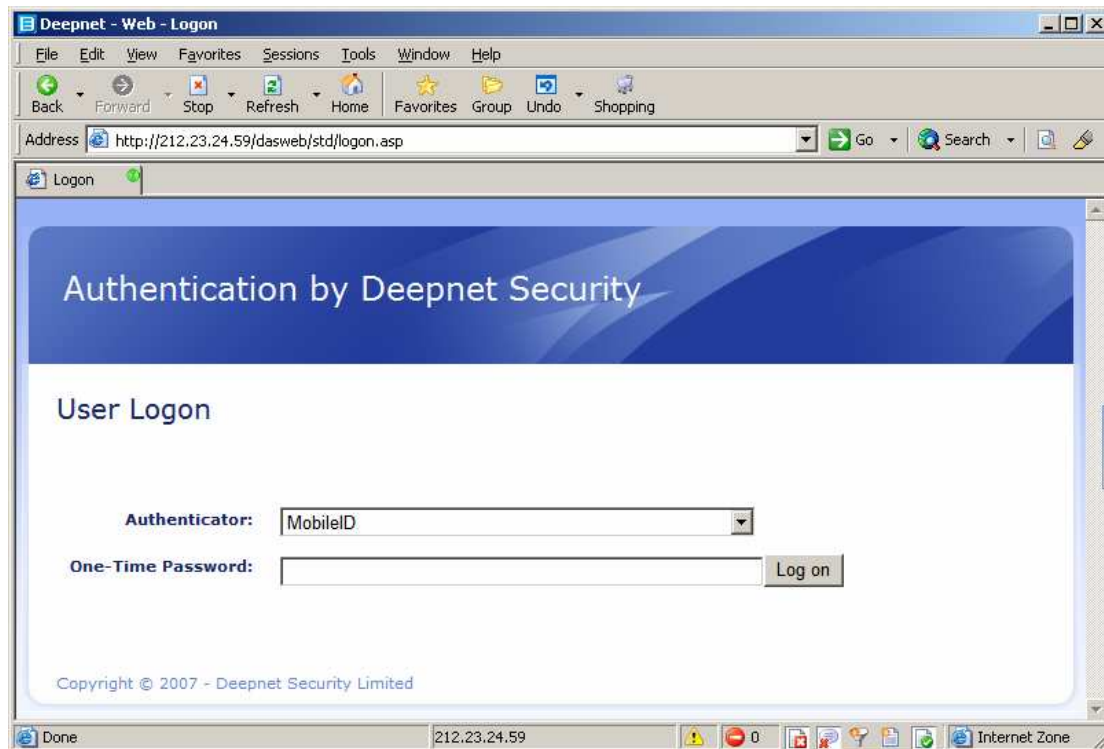
The Static Password Authentication

The first-factor authentication is the same as the traditional static password authentication in which the user is asked to enter their user name and static password.



The Second-Factor Authentication

The second-factor authentication requires the user to provide the credentials generated from their token, such as, a one-time password.



Customisation

The Deepnet IIS Agent software provides default versions of HTML and ASP pages for the two-factor authentication. However, you can customize the web pages to reflect your company's image and administrative needs. You can

- Add a custom greeting message
- Add your own custom graphics
- Change standard buttons to custom graphics
- Display Web access authentication prompts in a language other than English
- Customize the Web access authentication messages

The default web pages are located in /DASWEB/STD directory. Following table lists some of the main pages:

Header.inc	Page header
Footer.inc	Page footer
Main.css	CSS style sheet

To ensure that the IIS Agent will function properly after you have made changes, follow these rules:

1. Copy the original pages into a new directory before making changes to them.
2. Use a text editor to make changes.
3. After you have completed your changes, test the page to make sure they are functioning properly.