Microsoft .NET Passport Integration with Active Directory in IIS 6.0 and Windows .NET Enterprise Server and Windows XP Professional as a Client

Written by Marc Grote
MCP, MCP+I, MCSA, MCSE NT4, MCSE Win2K, MCT, CNA, CCNA, CCA
mailto:grotem@it-training-grote.de

Abstract

The Microsoft Windows .NET Server Operating System and the Internet Information Server (IIS 6.0) provides a new features to map .NET Passport Accounts with Active Directory Accounts in IIS 6.0. This article provides a step by step instruction to implement a .NET Passport to AD mapping.

Introduction

What says Microsoft about .NET Passport:
Microsoft .NET Passport, launched in 1999, is a suite of Web-based services that help make using the Internet and purchasing online easier and faster. .NET Passport provides users with single sign-in (SSI) and fast purchasing capability at a growing number of participating sites, reducing the amount of information users must remember or retype.

.NET Passport helps provide a high-quality online experience for a large user base and uses powerful encryption technologies—such as Secure Sockets Layer (SSL) and the Triple Data Encryption Standard (3DES) algorithm—for data protection. Privacy is a key priority as well, and all participating sites sign a contract in which they agree to post and follow a privacy policy that adheres to industry-accepted guidelines.

Available Services

Here are some of the key services .NET Passport provides:

Single sign in (SSI)

.NET Passport users can create a single sign-in name and password for use across participating .NET Passport sites. In other words, the SSI service provides a common Internet authentication mechanism across participating Web sites. The use of these technologies is important to ensure the integrity of a transaction (for example, making certain that this person is allowed to access a site), and is required by many Web sites, Internet service providers, devices, and computer applications.

The SSI service also enables users to save time and avoid repetitive data entry by storing a limited set of basic demographic information that can, with the user's permission, be easily shared with participating .NET Passport sites when signing into those sites. (Note: The only information required to create a .NET Passport account is an e-mail address and password.)

Kids Passport

Microsoft Kids Passport is a feature of the .NET Passport SSI service and is an example of Microsoft's ongoing initiative to provide children with a positive online experience. The Kids Passport service is designed to provide participating Kids Passport sites with assistance in complying with the parental consent obligations of the Children's Online Privacy Protection Act (COPPA) and provides parents or guardians a way to help manage what .NET Passport profile information their children can share at .NET Passport–participating sites. It also provides additional controls for how Kids Passport–participating sites can collect, use, and share children's profile information.

Scalability

.NET Passport operates at massive scale today.
Live since 1999, .NET Passport is the largest online authentication system in the world—with more than 200 million accounts performing more than 3.5 billion authentications each month. Reliability is very high and a key design consideration for any new features

Licensing

To obtain the necessary credentials for using the Passport service on your live site, you must sign a three-year, non-exclusive Service Agreement.

To request a service agreement, you must send an e-mail message to netservs@microsoft.com. After Microsoft has received the information they will send you a license agreement.

Microsoft .NET Passport is free for end users but not for Enterprises.

There are two fees for licensing Passport: a periodic compliance testing fee of $1,500 US and a yearly provisioning fee of $10,000 US. The provisioning fee is charged on a per-company basis.
For testing purposes you may obtain a free site ID for your .NET Passport test environment. Point your Browser to http://www.netservicesmanager.com.

Passport Registration Process

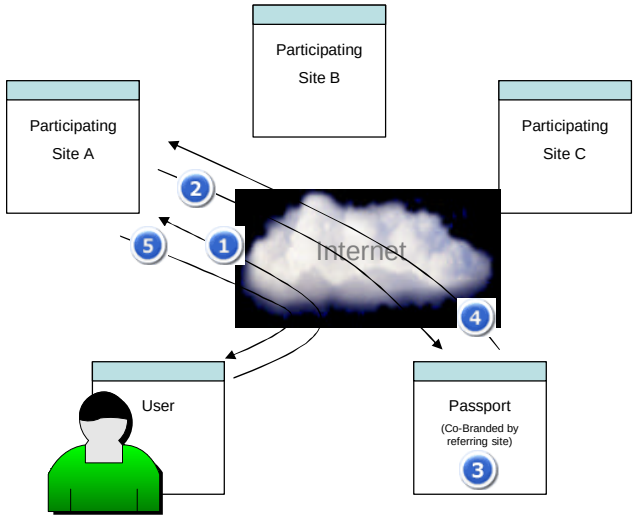

Figure 1: The Registration Process.

1. In this example the user browses to Site A, a participating site or service (or browses to www.passport.com), and they click the “Sign In” button (or click the “Register” button on Passport.com).
2. The user is redirected to a co-branded registration page displaying the registration fields that were chosen by Site A. (The minimum number of fields required is two; email name and password.) Here the user chooses whether or not they want to opt in to share their information with other Passport-enabled sites that they sign in to.
3. The user reads and accepts terms of use (or declines, and the process ends), and submits the form. (On Passport.com the user is shown a congratulations page and sign up process ends here.)
4. The user is then redirected back to Site A with their encrypted authentication ticket and profile information attached.
5. Site A decrypts the authentication ticket and profile information and continues their registration process, or grants access to their site.

NOTE: Sites B and C do not receive any information about the user. The user does not need to download any software. The only requirement is that they use a browser that supports Cookies, SSL, and JavaScript.

(Copied from the .NET Passport Review Guide)

First Step – Configure .NET Passport

The first Step is to configure the .NET Passport mapping for the Standardwebsite. You can find the tool in the %WINDIR%\SYSTEM32 directory with the name MSPPCNFG.EXE.

Create a web site named “Standardwebsite” that corresponds to the website in IIS 6.0

Type in the host name and the IP address of the web site.

The explanation of the other optional parameters can be found in Help and Support Center or in the Microsoft .NET Passport SDK.

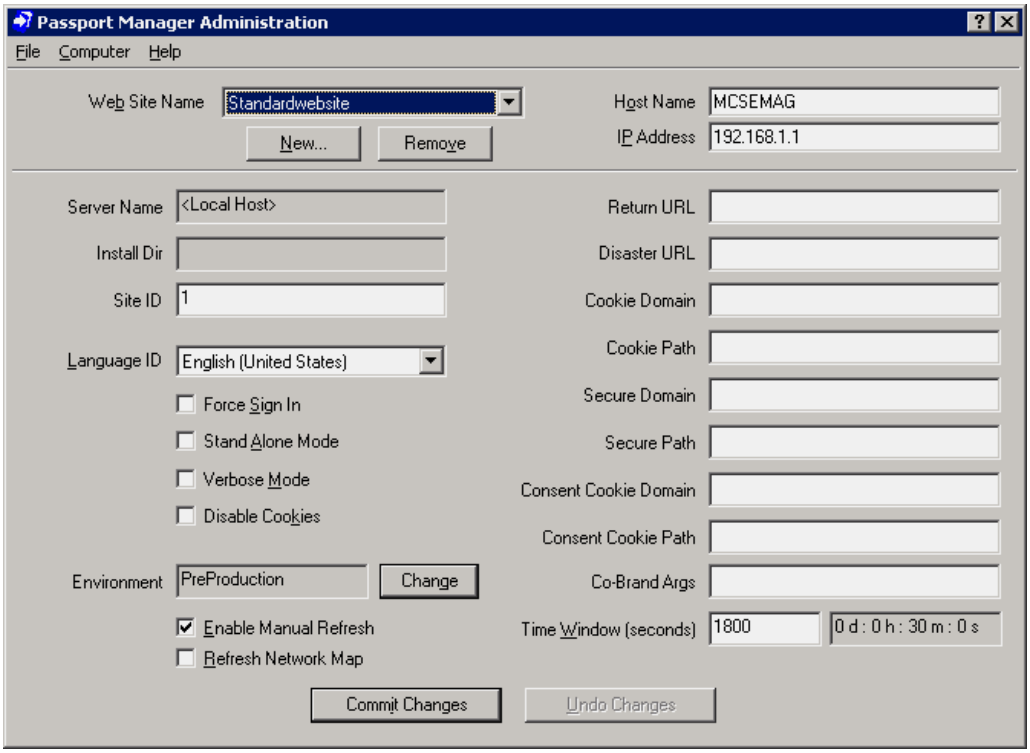

Figure 2: Microsoft .NET Passport Manager Administration Tool

Passport and SSL

Per Default the .NET Passport authentication requires SSL for authentication. This behaviour can be modified via a registry patch.

For the default website:

HKEY_LOCAL_MACHINE\Software\Microsoft\Passport\SecureLevel

For all other websites:

HKEY_LOCAL_MACHINE\Software\Microsoft\Passport\Sites\<SiteName>\
SecureLevel

There are three authentication levels

0 = unspecified – all authentication types are possible
10 = SSL encrypted authentication requests
100 = Authentication via Secure Channel and additional security key

.NET Passport environments

There are two instances of the Microsoft .NET Passport service, which are known as environments. The Preproduction (PREP) environment is used for site development and testing; it enables participating sites to validate their development efforts against .NET Passport servers without granting access to real-world .NET Passport users and profiles. The Production environment is the live .NET Passport service; it is used by all working and approved .NET Passport participating sites after they are publicly deployed. User accounts that exist in the Production environment do not exist in the PREP environment.

The code used to implement a .NET Passport site is the same for both environments. The Passport Manager connects to the instance of the .NET Passport service for which the server is configured. You can switch between environments by configuring your server manually or by using the Passport Manager Administration utility.

Second Step – Configuring the IIS Server for .NET Passport integration

Start Internet Information Manager SnapIn – Expand the Server Object – Web Sites – Properties of the Default Web Site – Directory Security – Edit – Authentication access – Activate ".NET Passport authentication and select the needed domain.

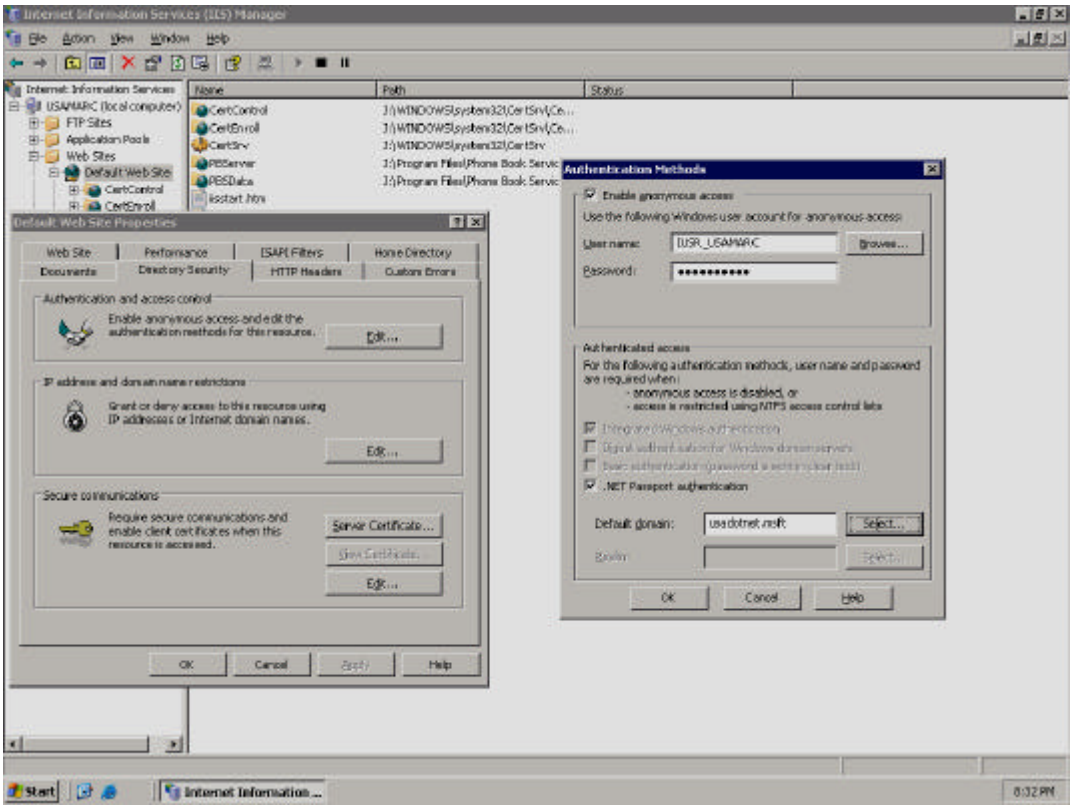

Figure 3: .NET Passport properties in IIS 6.0

Important:

.NET Passport authentication just works if you deselect all other authentication methods except ".NET Passport authentication".

Test-Site

The installation of the Microsoft .NET Passport SDK installs a test site in IIS. You can reach the site at http://servername/passporttest/default.asp

Third Step

.NET Passport Mapping with Active Directory

For a successful .NET Passport – AD mapping you have to map the PUID (the unique ID from a .NET Passport account) with an Active Diretcory account.

The first time mapping is known as “Provisioning”. The Active Directory Schema attribute “altSecurityIdentities” is used for the mapping.

IIS 6.0 use the IIS Metabase flag „AuthFlag“ to define the mapping behaviour. The default mapping is .NET Passport – Active Directory account.

The behaviour can be changed by Metaedit by the following way:

PassportRequireADMapping = Value = 0 – no Active Directory mapping
PassportRequireADMapping = Value = 1 Active Directory mapping
PassportRequireADMapping = Value = 2 Active Directory mapping – if failure error 401 returns

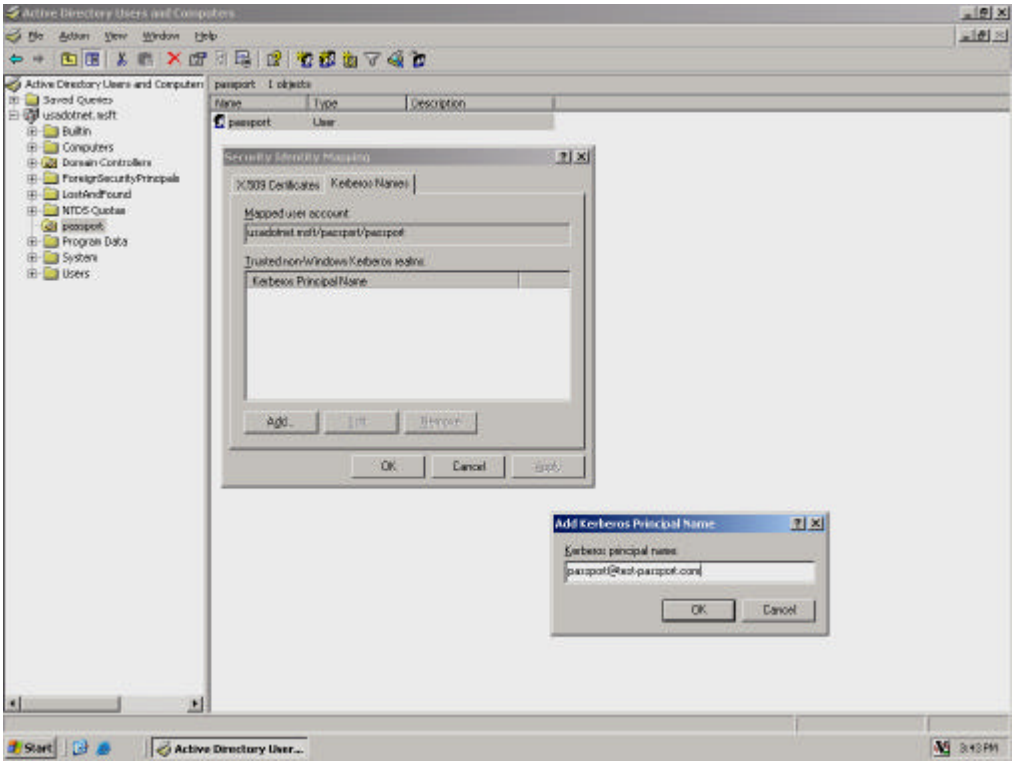

Figure 4: Mapping a PUID (Passport) to Active Directory

.NET Passport SDK

Figure 5: .Installing .NET Passport SDK v2.5

At client side

Connect to the intranet .NET Passport site

Example: http://192.9.200.18

Enter your E-Mail address defined in the user properties in Active Directory and the associated password.

Figure 6: .NET Passport authentication window

It should work and display the desired website.

Related Links

.NET Passport Information
http://www.passport.com

Technical information for .NET Passport
http://www.microsoft.com/netservices/passport

.NET Passport SDK
http://msdn.microsoft.com/downloads/default.asp?URL=/downloads/sample.asp?url=/msdn-files/027/001/885/msdncompositedoc.xml