PROTECTID

Client Authenticated SSL Server Setup Guide for Microsoft Windows IIS

Document: MK-UM-01180405-01-ProtectIDclientAuthSSLsetupIIS.doc



Copyright © 2005 Sentry Project Management All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without the written permission of Sentry Project Management Pty Ltd.

Trademarks: Microsoft and Windows, Windows 95, Windows NT, Windows 98, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation. Netscape, Netscape Communicator and Netscape Messenger are registered trademarks of Netscape Communications Corporation. Novell Groupwise is a registered trademark of Novell Inc. **protectID** is a registered trademark of Sentry Project Management Pty Ltd.

Before you use the protectID product, you must agree to the following terms.

Any use or distribution of the protectID product requires that either you or your supplier have a licence from Sentry Project Management Pty Ltd. Please contact your supplier or support@sentrypm.com for details.

Neither Sentry Project Management nor any other person who has been involved in the creation, production, or delivery of the Software shall be liable to the user or to any other person for any direct, incidental or consequential damages, even if Sentry Project Management has been advised of the possibility of such damages.



Purpose

This document is intended to provide integration support for use of ProtectID smartcards or tokens (ref <u>www.SENTRYpm.com</u>) with client-authenticated SSL on Microsoft Windows IIS-based webservers.

This document describes setup of the IIS server and use of soft certificates at the client PC. Once this setup is complete and the website access is satisfactory, contact Sentry for further advice on installation of Sentry's protectID smartcard- and USB token-based certificates.

The following procedures assume general familiarity with Microsoft Windows systems.



1 Digital certificate client authentication on IIS 5.0 or later

This document assumed that IIS 5.0 or later has already been installed on your PC.

To setup a digital certificate based client authentication on IIS web-server follow the instructions below:

- 1. Generate a Server Certificate Request
- Install a server certificate on IIS web-server. You may obtain the certificate from an external Certification Authority or generate one using your own CA¹.
- 3. Install the CA root certificate used to sign the server certificate.
- 4. Configure IIS to request a client certificate for authentication.
- 5. Obtain client certificates from an external CA or generate client certificates using your own CA.
- 6. Install a root CA certificate used to sign the client certificates.
- 7. Install user/client certificates on IE 6 web-browser.

Generate a Server Certificate Signing Request

SENTRY^{PM}

To generate a Server Certificate Signing Request follow the steps below:

- 1. Click Start -> Settings and click Control Panel.
- 2. Double click the **Administrative Tools** applet icon.
- 3. Double click the Internet Services Manager.



¹ To generate your own certificates you must have a machine with Microsoft Certificate Server installed.



4. Expand your Host name. Right-click the **Default Web site** and then click **Properties**.



5. Click **Directory Security** tab.

escription: De P Address: (All	fault Web Site		
P Address:	11 N		
	(All Unassigned)		
TCP Port: 80 SSL Port: 443			
nnections			
Unlimited			
Elimited To:	10 connections		
onnection Timeout:	900 seconds		
HTTP Keep-Alives En	abled		
Enable Logging			
Active log format:			
W3C Extended Log File	e Format 💌 Properties		

6. Click **Server Certificate** button to launch the Web Server Certificate Wizard.





7. Click **Next** to move past the welcome dialog box.



8. Click Create a New Certificate, and then click Next.

Certificate Wizard		
erver Certificate There are three methods for assigning a cer	tificate to a Web site.	
Select the method you want to use for this (veb site:	
 Create a new certificate. 		
C Assign an existing certificate		
C Import a certificate from a Key Manager	backup file.	
	< Back Nex	t> Cancel



9. Click Prepare the request now, but send it later, and then click Next.



10. Enter the name you wish to appear on the certificate and select 1024 in the **Bit length** drop down list. Click **Next** to continue.

ame and Security Settings	
Your new certificate must have a nam	ie and a specific bit length.
Type a name for the new certificate. T remember.	The name should be easy for you to refer to and
Name:	
Default Web Site	
decrease performance.	
Bit length:	
Bit length:	
Bit length: 1024 Server Gated Cryptography (SGC)	certificate (for export versions only)
Bit length: 1024 Server Gated Cryptography (SGC)	certificate (for export versions only)
Bit length: 1024 Server Gated Cryptography (SGC)	l certificate (for export versions only)
Bit length: 1024 Server Gated Cryptography (SGC)	certificate (for export versions only) < Back Next > Cancel



11. Enter the name of your Organisation and the organisational unit and click Next.

ganization Information	
Your certificate must include inform distinguishes it from other organiza	mation about your organization that ations.
Select or type your organization's	name and your organizational unit. This is typically the
For further information, consult on	dia die name of your division of department.
For rurther information, consult ce	runcation authonity's web site.
Urganization:	
Pinnacle Consulting	
Organizational unit:	
Marketing	•

12. Enter the common name you wish to use. For a server certificate this is usually your domain name.

IS Certificate Wizard		×
Your Site's Common Name Your Web site's common name is its fully gu	ualified domain name.	
5.5	2	
Type the common name for your site. If the name. If the server is on the intranet, you m name.	server is on the Internet, use a valid DN ay prefer to use the computer's NetBIOS	S
If the common name changes, you will nee	d to obtain a new certificate.	
Common name:		
pinnacle-1		
, 		
		10 March 10 Mar



13. Enter the location of your organization and click Next.

graphical Information		
The certification authority requires	the following geographical information.	
Country/Region:		
AUI (Australia) 📃 💌		
State/province:		
New South Wales		-
City/locality:		
Sydney		-
State/province and City/locality mu abbreviations.	ust be complete, official names and may not co	ontain

14. Specify a file name where you want to store the certificate request and click **Next**.

rtificate Request File Name		6
Your certificate request is saved as a text file specify.	with the file name you	
Enter a file name for the certificate request.		
File name:		
c:\certreq.txt		Browse



15. The information that will appear on the certificate will be shown for verification. Click **Next**.

equest File Summary				_
You have chosen to ge	nerate a request file.			
To generate the followin	g request, click Next.			
File name: c:\certreq.t	ĸt			
Your request contains th	e following information:			
Issued To Friendly Name Country / Region State / Province City Organization Organizational Unit	pinnacle-1 Default Web Site AU New South Wales Sydney Pinnacle Consulting Marketing			
		< Back	Next >	Cancel

16. Click **Finish** to complete the Web Server Certificate Wizard.



17. Send the generated certificate request file to a CA of your choice for signing.



2 To install the certificate on the Web server

After you received the certificate back from the CA you need to install it on your web-server.

- 1. Follow step 1 to 7 as described in the previous section.
- 2. Click **Server Certificate** to launch the Web Server Certificate Wizard. Click **Next** to process the certificate you obtained from the CA.

Welcome to the Web Serve	er Certificate Wizard.	×
	Welcome to the Web Server Certificate Wizard This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.	
	Status of your Web server:	
	You have a pending certificate request. Certificate Wizard will help you to process the response from a Certification Authority or to remove this pending request.	
L.	To continue, click Next.	
	< Back Next > Cano	:el

3. Click **Process the pending request and install the certificate**, and then click **Next**.

Certificate Wizard	x
A pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded.	
A certificate request is pending. What would you like to do?	
Process the pending request and install the certificate	
O Delete the pending request	
	1
<back next=""> Canc</back>	el
	ertificate Wizard nding Certificate Request A pending certificate request is a request to which the certification authority has not yet responded. A certificate request is pending. What would you like to do? • Process the pending request and install the certificate • Delete the pending request • Control to the pending request





4. Enter the path and file name of the file that contains the response from the CA, and then click **Next**. The example below will read the certificate from C:\Certs directory.

cess a Pending Request				
Process a pending certificate request I the certification authority's response.	by retrieving the file that contains			
Enter the path and file name of the file containing the certification authority's response.				
Path and file name:				
C:\Certs\Thawte.cer	Browse			

5. Examine the certificate overview, click **Next**, and then click **Finish**.

A certificate is now installed on the web server.



3 Install the CA root certificate used to sign the server certificate

This procedure installs a trusted certificate on IIS 5.0 on Windows 2000 Pro. This section assumed that you already obtained a CA root certificate, which was used to sign the server certificate.

- 1. Start Windows Explorer
- 2. Navigate to the directory, where the CA root certificate file is stored.
- 3. Right click on the certificate file and select **Install Certificate**.
- 4. It will start the Certificate Import Wizard.
- 5. Click **Next** to go pass the Welcome screen.
- 6. Select Automatically select the certificate store based on the type of certificate and click Next.

Windows can automatic	ally select a certifica	te store, or you	ı can specify	a location for
Automatically se	ect the certificate st	ore based on th	ie type of cer	tificate
C Place all certifica	tes in the following s	tore		
Certificate store				
				Browse

- 7. On the next screen click **Finish** to complete the installation of CA root certificate.
- 8. You may be asked, if you trust the certificate issuer. Click Yes, if you are prompted to do so, assuming you received the certificate from a trusted CA.

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.



4 Configure IIS Web Server to use SSL

This procedure uses Internet Information Services (IIS) to configure your Web application's virtual directory to require SSL to access it. This procedure assumed that you have a valid certificate installed on your Web server.

- 1. Follow steps 1 to 6 as described in section 1.
- 2. On the **Default Web Site Properties** dialog box, click **Edit**.

Veb Site	Performance ISAPI Filters Ho	me Directory Document:
Jirectory Se	curity HTTP Headers Custom B	strors Server Extensions
Anonymou	s access and authentication control	
\$	Enable anonymous access and edit the authentication methods for this resource.	Edit
IP address	and domain name restrictions	
	Grant or deny access to this resource usir IP addresses or internet domain names	ng
w.		Edit
Secure col	Require secure communications and	
<u>=0</u>	enable client certificates when this resource is accessed.	Server Certificate
		View Certificate
		Edit

3. Select the Require secure channel (SSL) check box.

ecure Communic	ations	2
Require secure	channel (SSL)	
Require 128-t	it encryption	
Client certificates		
Ignore client d	ertificates	
C Accept client	certificates	
🔿 Require client	certificates	
Client certificates accounts. This a	centricate mapped to Windows user lows access control to resources	Edit
Client certificates accounts. This a using client certific Enable certific Current CTL:	can be mapped to Windows user lows access control to resources cates.	Edit
Client certificates accounts. This a using client certific Enable certific Current CTL:	can be mapped to Windows user lows access control to resources cates.	Edit

- 4. If you want to force strong encryption, select the **Require 128-bit** encryption option.
- 5. Select either Ignore client certificates or Accept client certificates.
- 6. Click OK, and then click OK again.





7. In the Inheritance Overrides dialog box, click Select All, and then click OK to close the properties dialog box.

Your IIS web server is now ready to communicate securely using SSL.

SENTRY^{PM}

5 Configure IIS Web Server to require client certificates

This procedure uses Internet Information Services (IIS) to configure your Web application's virtual directory to require client certificates. This procedure assumes that you have a valid certificate installed on your Web server.

- 1. Follow steps 1 5 in section 3.
- 2. To force your web server to ask for client certificates, select the **Require client certificates** option in Client certificates section.

Require 128-bit encryption Interfective certificates Construct Interfective certificates Accept client certificates Require client certificates Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
lient certificates C Ignore client certificates C Accept client certificates Require client certificates Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
Ignore client certificates Accept client certificates Require client certificates Intervention certificates Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
Accept client certificates Require client certificates Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
 Require client certificates Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates. 	
Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	
Enable certificate trust list	
Sument CTL:	
New Edit.	1
	6 C

- 3. Click OK, and then click OK again.
- 4. In the Inheritance Overrides dialog box, click Select All, and then click OK to close the properties dialog box.



6 Obtain client certificates from an external CA or generate your own client certificates

To obtain a client certificate go to Certification Authority such as Verisign, Thawte, Baltimore, CACert or others.

To generate client certificates from your own CA, you need a machine running Microsoft Certificate Service.





7 Install the CA root certificate

Before you can use a SSL client certificate to access the web-server, which was set up to request client certificate, you must install the root certificate of the CA who signed the client certificate(s).

This procedure installs a trusted certificate on IIS 5.0 on Windows 2000 Pro. This section assumed that you already have a root certificate stored in a .cer file.

Follow instructions in section 3 to install the CA root certificate. The difference is that you must double click the CA root certificate that was used to sign the client certificate(s).

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.



8 Install a Client Certificate

This procedure installs a client-side certificate. **You can use a certificate from any certificate authority,** or you can generate your own certificate using Microsoft Certificate Services. This section assumed that you already have a client certificate from a CA stored in a .cer file

Follow instructions in section 3 to install a client certificate. The difference is you must double click the client certificate file, instead of a CA root certificate file.

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.

Click Finish to complete the wizard. Dismiss the confirmation message box, and then click OK to close the certificate.

