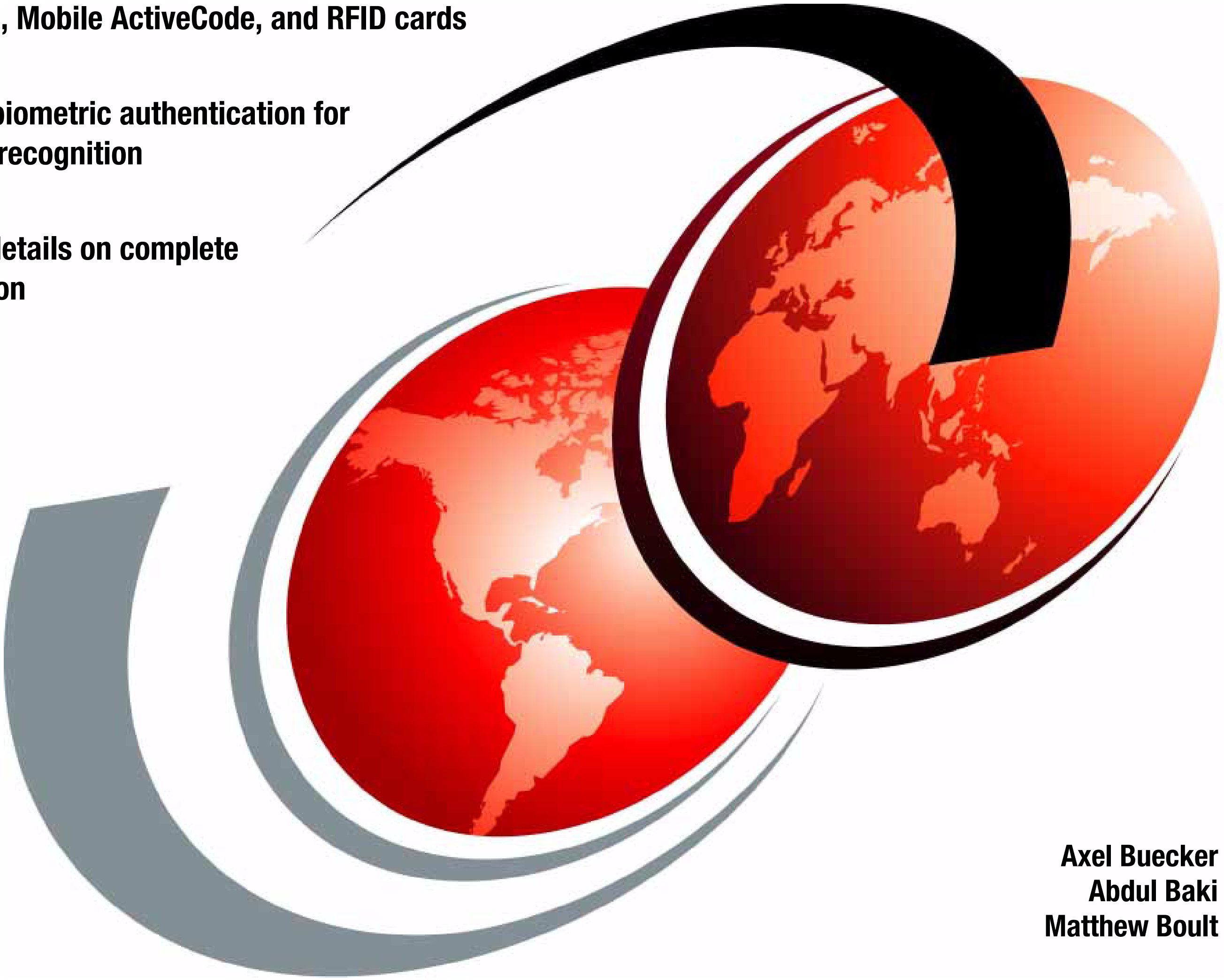
# Configuring Strong Authentication with IBM Tivoli Access Manager for Enterprise Single Sign-On

- Details on external authentication factors for smartcards, Mobile ActiveCode, and RFID cards
- Details on biometric authentication for fingerprint recognition
- Hands-on details on complete configuration



Axel Buecker
Abdul Baki
Matthew Boult

Redpaper

ibm.com/redbooks

International Technical Support Organization

# Configuring Strong Authentication with IBM Tivoli Access Manager for Enterprise Single Sign-On

December 2011

REDP-4808-00

**Note:** Before using this information and the product it supports, read the information in “Notices” on page v.

**First Edition (December 2011)**

This edition applies to IBM Tivoli Access Manager for Enterprise Single Sign-On V8.1.

This document created or updated on December 15, 2011.

# Contents

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information 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 publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DB2®
IBM®
IMS™
Redbooks®
Redpaper™
Redpapers™
Redbooks (logo) ®
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

# Preface

IBM® Tivoli® Access Manager for Enterprise Single Sign-On automates sign-on and access to enterprise applications, eliminating the need to remember and manage user names and passwords. Users log on to Tivoli Access Manager for Enterprise Single Sign-On with a special user ID and password, and then, when they access their secured applications, the Tivoli Access Manager for Enterprise Single Sign-On agent enters their stored credentials automatically without the users needing to do so. Tivoli Access Manager for Enterprise Single Sign-On provides the usual features associated with password security, for example, password length, aging policy, and so forth.

This IBM Redpapers™ publication is based on a set of exercises that was produced for the European Tivoli Technical Conference 2010. It shows how to configure Tivoli Access Manager for Enterprise Single Sign-On to use additional or alternative methods of authentication when users log on to provide a greater degree of security (stronger authentication).

This paper is intended to complement the product documentation and should be read in conjunction with it. In particular, you should refer to the Setup Guide.

## The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

**Axel Buecker** is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in computer science from the University of Bremen, Germany. He has 25 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

**Abdul Baki** is an IT Specialist who works with customers using early versions of IBM Security products as part of his role managing worldwide Beta Programs. He holds a degree in Computer Communication and Networks from the University of Westminster, U.K., and is a member of the British Computer Society. Abdul works at the IBM Hursley development laboratory in Hursley, U.K.

**Matthew Boult** is a Product Introduction Specialist in the IBM SWG Early Programs organization. He is based in Hursley in the U.K. and runs worldwide early programs for Tivoli products, generating feedback to development, creating reference accounts, and promoting sales enablement through early education and the production of intellectual capital. He has more than 30 years of experience in the IT industry and has been working with Tivoli since the acquisition of the company by IBM, initially providing post-sales technical support and later designing and implementing solutions for outsourced customers. He has been working with Tivoli Access Manager for Enterprise Single Sign-On since running the beta program for v8.1 in 2009.

Many thanks to Sven Gossel at charismathics gmbh for providing the smart card middleware, smart cards, and card readers used in producing this IBM Redpaper™.

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

**ibm.com**/redbooks/residencies.html

## Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  **ibm.com**/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

## Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

# Configuring authentication to use smart cards

This chapter explains how to configure an existing Tivoli Access Manager for Enterprise Single Sign-On environment to use smart cards as additional authentication factors.

> **Note:** You can use a USB token instead of a smart card and reader.

This chapter includes the following topics:

## 1.1 Prerequisite environment

To run this exercise, you need the following resources. Refer to the Tivoli Access Manager for Enterprise Single Sign-On product documentation for platform requirements and configuration instructions.

- Integrated Management System Server (IBM IMS™ Server)
  - Microsoft Certificate Server
  - Internet Information Services
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 IMS+ prerequisites
    - IBM WebSphere® Application Server
    - IBM HTTP Server
    - A supported database (for example IBM DB2®)
  - Smart card middleware

  > **Note:** This scenario uses the Charismathics Smart Security Interface (CSSI).

- Client
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 AccessAgent
  - Smart card middleware
  - Initialized smart card and reader or USB token
  - Drivers for reader or token
- Active Directory
  - Domain containing computers and user accounts

## 1.2 Testing smart card compatibility

The Smart Card Compatibility Tool is supplied with Tivoli Access Manager for Enterprise Single Sign-On V8.1 installation files. The tool is installed in the `SCardCompatTool` *`version`* directory.

You can test smart card compatibility in the following way:

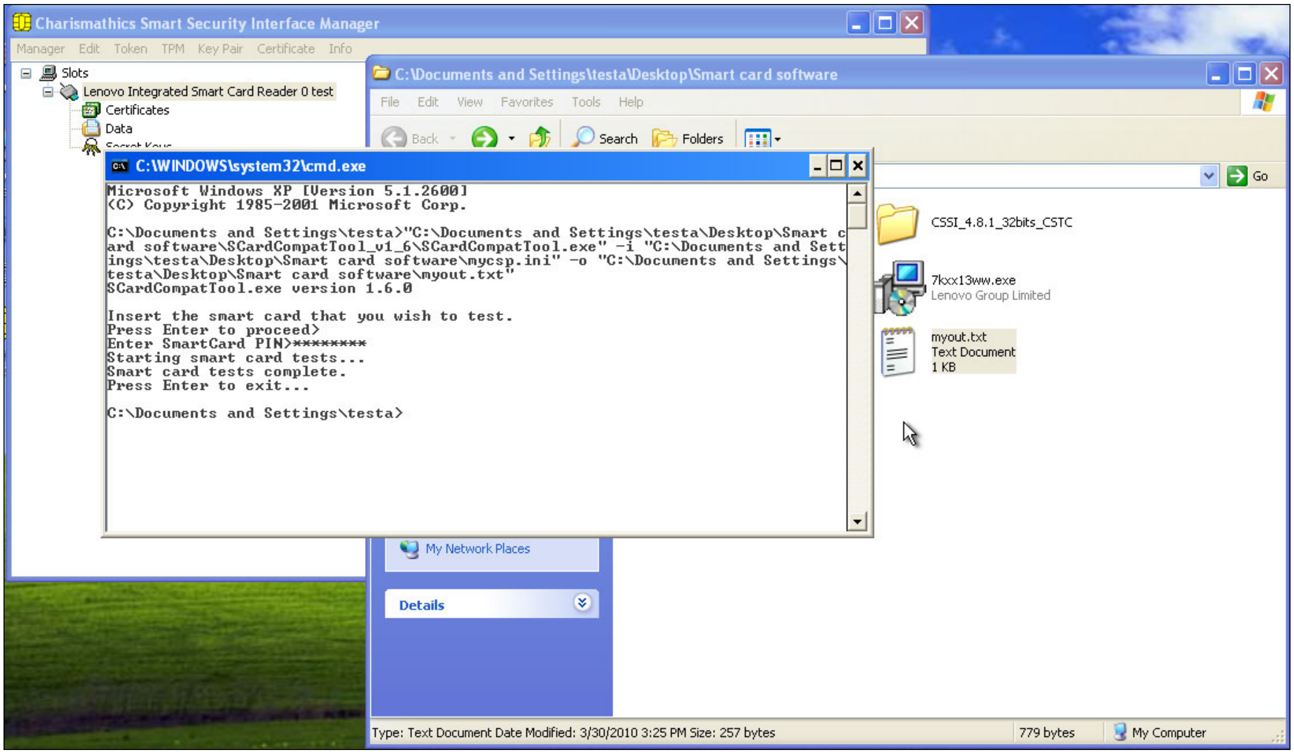
1. Create a `mycsp.ini` configuration file that contains details of the location of the smart card middleware driver, using the supplied `example.ini` file for guidance.
2. Run the following command from the command line:

   ```
   SCardCompatTool.exe -i mycsp.ini -o output_file_name
   ```

   The following prompt appears:

   ```
   Insert the smart card that you wish to test. Press Enter to proceed.
   ```

3. Insert the smart card into the reader, and press Enter. Then, enter the PIN when prompted. Figure 1-1 shows the tests.



Charismathics Smart Security Interface Manager
Manager Edit Token TPM Key Pair Certificate Info
Slots
Lenovo Integrated Smart Card Reader 0 test
Certificates
Data
C:\Documents and Settings\testa\Desktop\Smart card software
File Edit View Favorites Tools Help
Back
Search
Folders
Go
C:\WINDOWS\system32\cmd.exe
CSSI_4.8.1_32bits_CSTC
7kxx13ww.exe
Lenovo Group Limited
myout.txt
Text Document
1 KB
My Network Places
Details
Type: Text Document Date Modified: 3/30/2010 3:25 PM Size: 257 bytes
779 bytes
My Computer

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\testa>"C:\Documents and Settings\testa\Desktop\Smart c
ard software\SCardCompatTool_v1_6\SCardCompatTool.exe" -i "C:\Documents and Sett
ings\testa\Desktop\Smart card software\mycsp.ini" -o "C:\Documents and Settings\
testa\Desktop\Smart card software\myout.txt"
SCardCompatTool.exe version 1.6.0

Insert the smart card that you wish to test.
Press Enter to proceed>
Enter SmartCard PIN>*********
Starting smart card tests...
Smart card tests complete.
Press Enter to exit...

C:\Documents and Settings\testa>
```

*Figure 1-1 Smart card compatibility tool*

4. Verify that the test was successful by examining the output file. If the test is successful, continue to the next section.

> **Note:** You must initialize the smart card or USB token first. This process is outside the scope of this paper. Refer to the smart card middleware documentation for information about how to enable new smart cards.

## 1.3 Configuring the certificate authority

Next, configure the certificate authority (CA) on the IMS Server:

1. Launch the Microsoft Certification Authority by navigating to **Start** → **Administrative Tools** → **Certification Authority**, as shown in Figure 1-2.

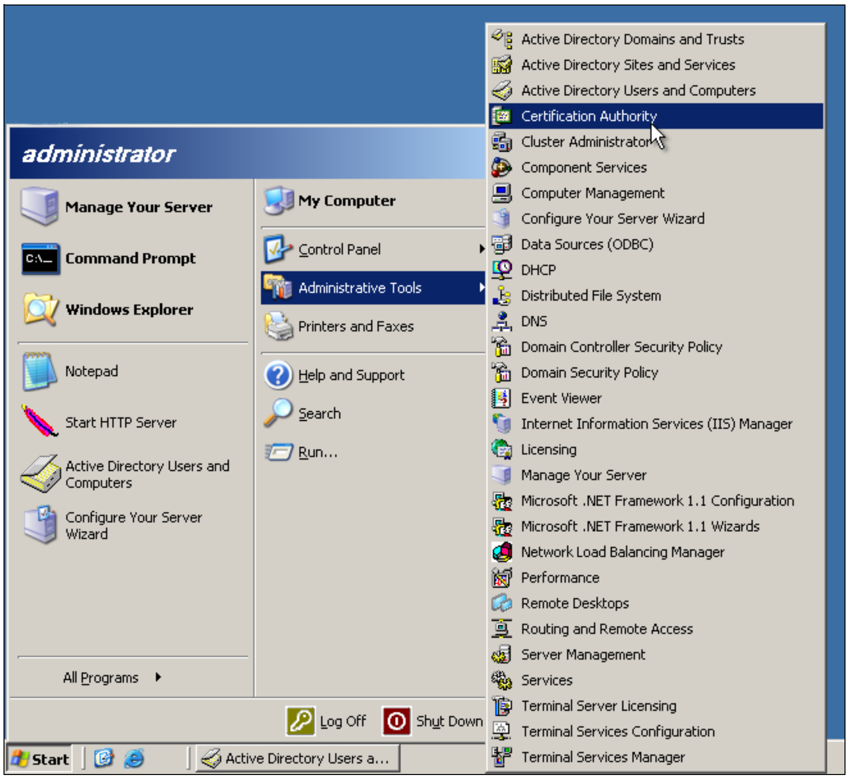
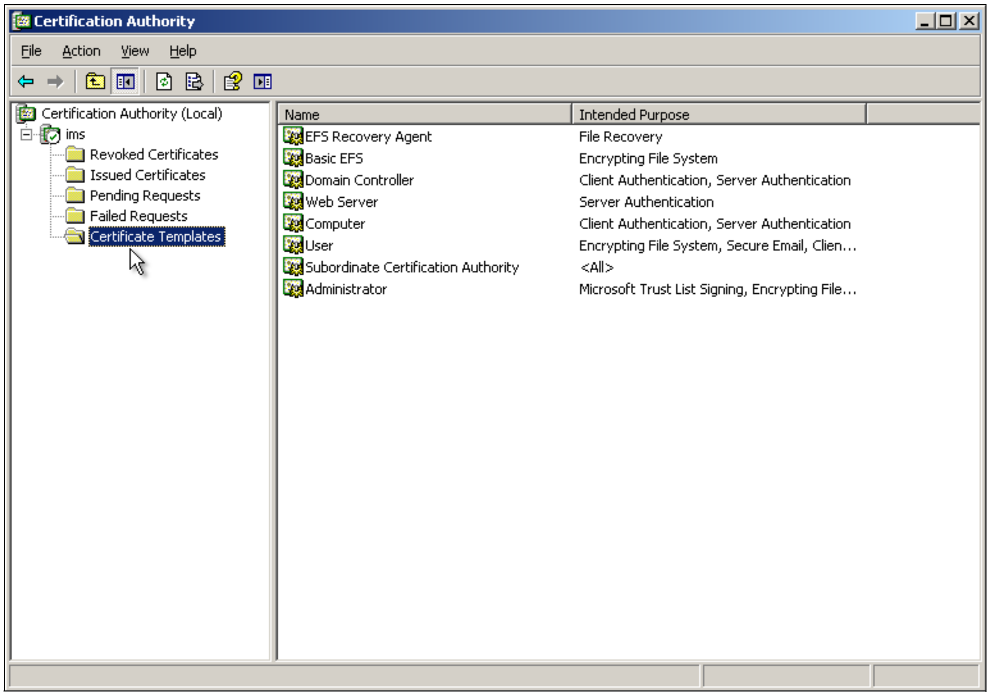

administrator
Manage Your Server
Command Prompt
Windows Explorer
Notepad
Start HTTP Server
Active Directory Users and Computers
Configure Your Server Wizard
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server Wizard
Data Sources (ODBC)
DHCP
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Internet Information Services (IIS) Manager
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Server Management
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Start
Active Directory Users a...

*Figure 1-2 Launching the Microsoft Certification Authority*

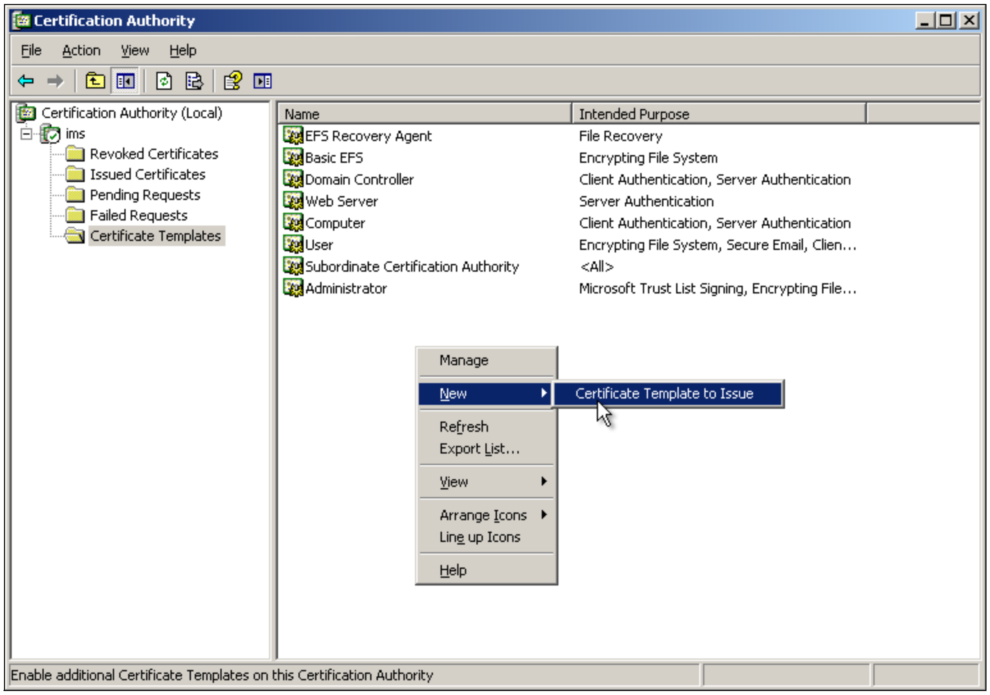
2. A window opens that displays details about the CA. In the left pane, select the CA server, and then select the `Certificate Templates` directory. The available certificate templates are displayed in the right pane, as shown in Figure 1-3.



| Name | Intended Purpose |
|---|---|
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentication |
| User | Encrypting File System, Secure Email, Clien... |
| Subordinate Certification Authority | <All> |
| Administrator | Microsoft Trust List Signing, Encrypting File... |

*Figure 1-3 Available certificate templates*

3. To install the necessary templates (for example, the **Smartcard User** and **Smartcard Logon** templates), right-click in the right pane, and select **New** → **Certificate Template to Issue,** as shown in Figure 1-4.

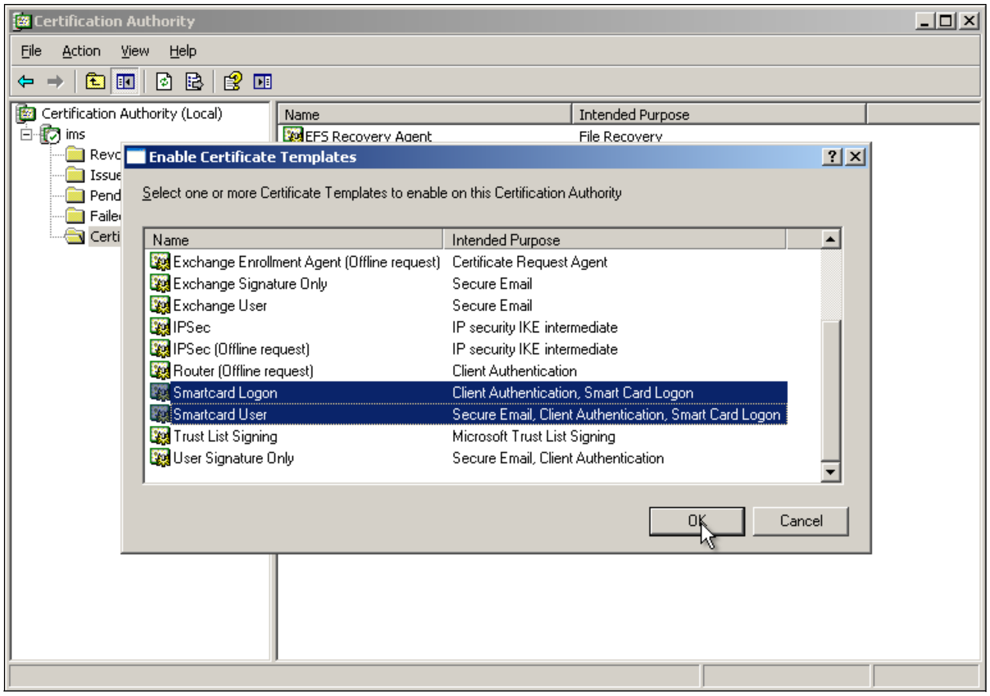


| Name | Intended Purpose |
|---|---|
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentication |
| User | Encrypting File System, Secure Email, Clien... |
| Subordinate Certification Authority | <All> |
| Administrator | Microsoft Trust List Signing, Encrypting File... |

Enable additional Certificate Templates on this Certification Authority

*Figure 1-4 New certificate*

4. A list of available certificate templates appears. Scroll down, and select the **Smartcard Logon** and **Smartcard User** templates, as shown in Figure 1-5. (You can select multiple certificate templates using the Ctrl key.) Click **OK**.

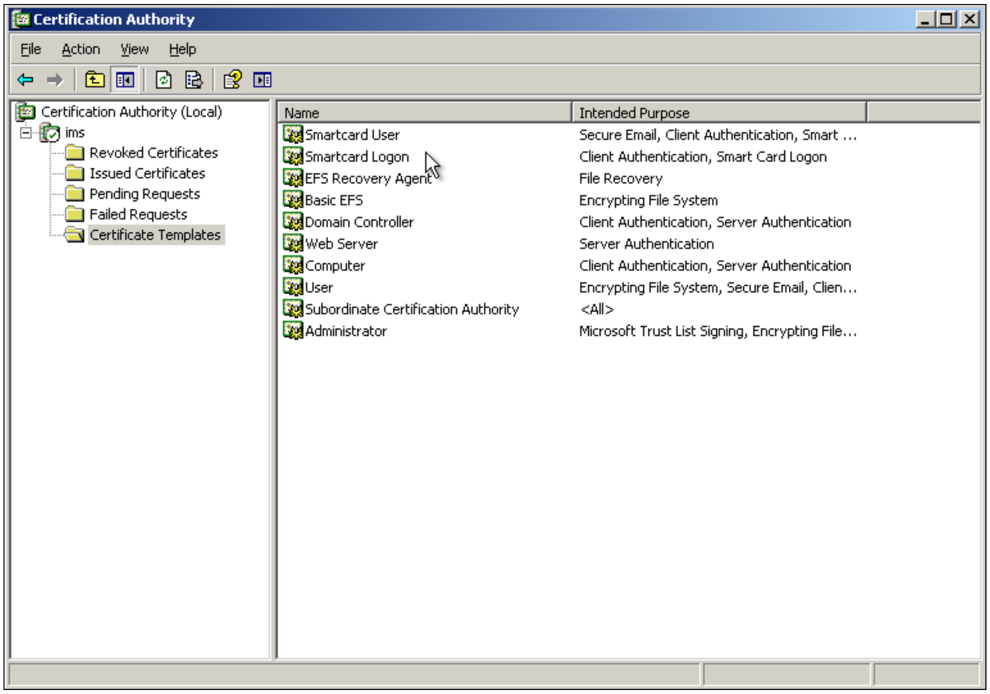


Select one or more Certificate Templates to enable on this Certification Authority

| Name | Intended Purpose |
|---|---|
| Exchange Enrollment Agent (Offline request) | Certificate Request Agent |
| Exchange Signature Only | Secure Email |
| Exchange User | Secure Email |
| IPSec | IP security IKE intermediate |
| IPSec (Offline request) | IP security IKE intermediate |
| Router (Offline request) | Client Authentication |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| Smartcard User | Secure Email, Client Authentication, Smart Card Logon |
| Trust List Signing | Microsoft Trust List Signing |
| User Signature Only | Secure Email, Client Authentication |

*Figure 1-5 Selecting the templates*

The smart card templates are added to the Certificate Template list, and the server is ready to issue certificates, as shown in Figure 1-6.



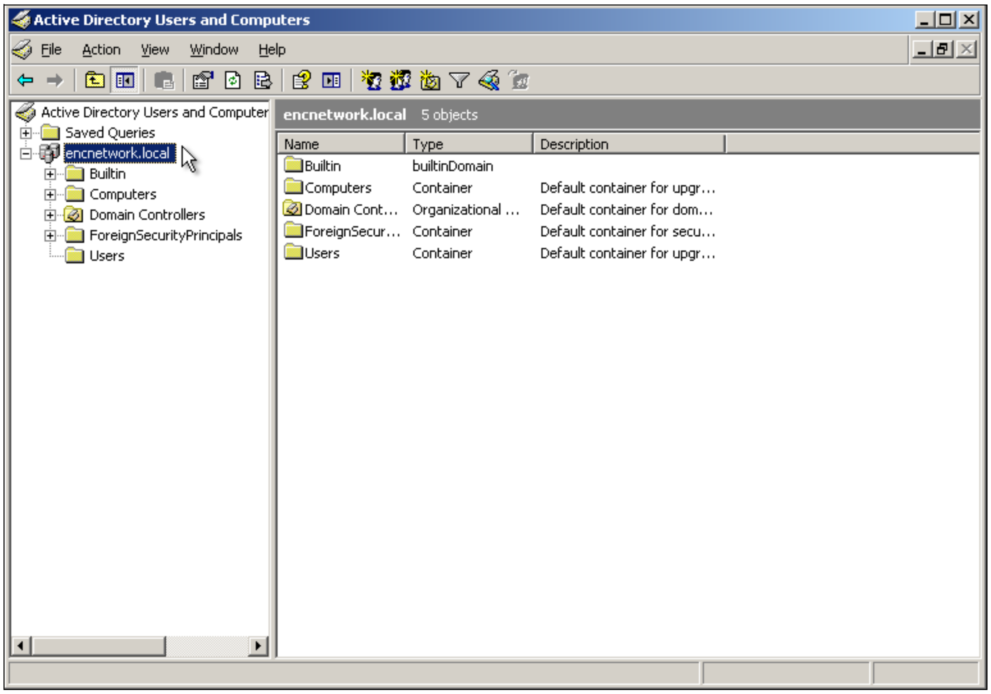
| Name | Intended Purpose |
|---|---|
| Smartcard User | Secure Email, Client Authentication, Smart ... |
| Smartcard Logon | Client Authentication, Smart Card Logon |
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentication |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentication |
| User | Encrypting File System, Secure Email, Clien... |
| Subordinate Certification Authority | <All> |
| Administrator | Microsoft Trust List Signing, Encrypting File... |

*Figure 1-6 Smart card certificates*

# 1.4 Importing the CA root certificate to the IBM HTTP Server truststore, part 1

Now, obtain the CA root certificate by clicking **Start** → **Administrative Tools** → **Active Directory Users and Computers**. The window shown in Figure 1-7 appears.

This scenario uses the Microsoft Certificate Server to obtain the domain name.


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computer
Saved Queries
encnetwork.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

encnetwork.local 5 objects

| Name | Type | Description |
|---|---|---|
| Builtin | builtinDomain | |
| Computers | Container | Default container for upgr… |
| Domain Cont… | Organizational … | Default container for dom… |
| ForeignSecur… | Container | Default container for secu… |
| Users | Container | Default container for upgr… |

*Figure 1-7 Opening the Active Directory*

Next, you need to obtain the Internet Information Services (IIS) server port number. By default, the IIS port number is 80. However, because the IBM HTTP Server already requires port 80, you need to modify the IIS port during installation.

To find the IIS server port number, follow these steps:

1. Go to **Start** → **Administrative Tools** → **Internet Information Services (IIS) Manager**, as shown in Figure 1-8.

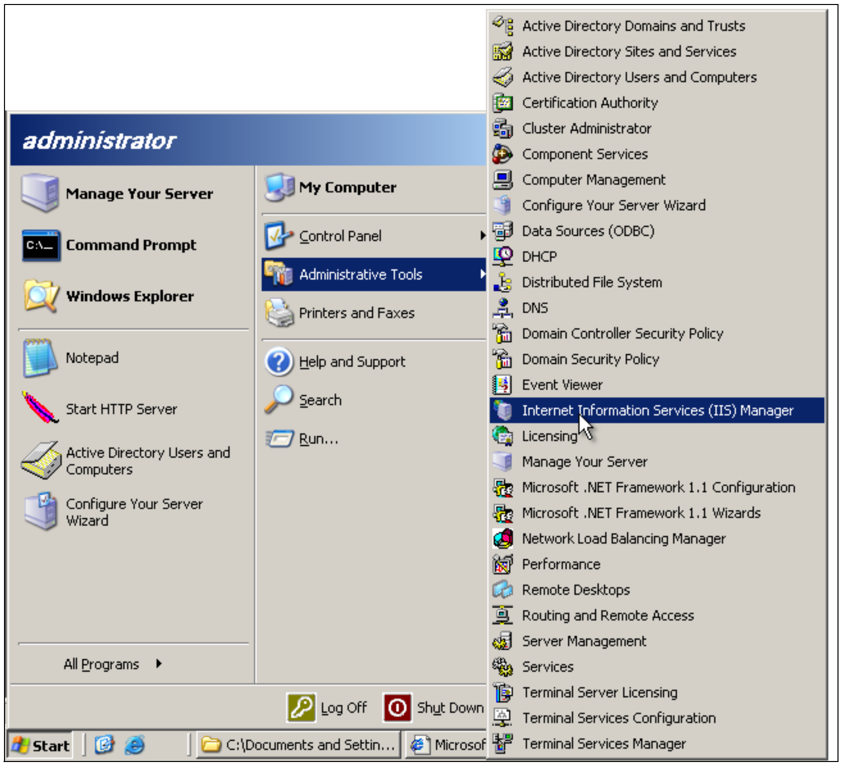
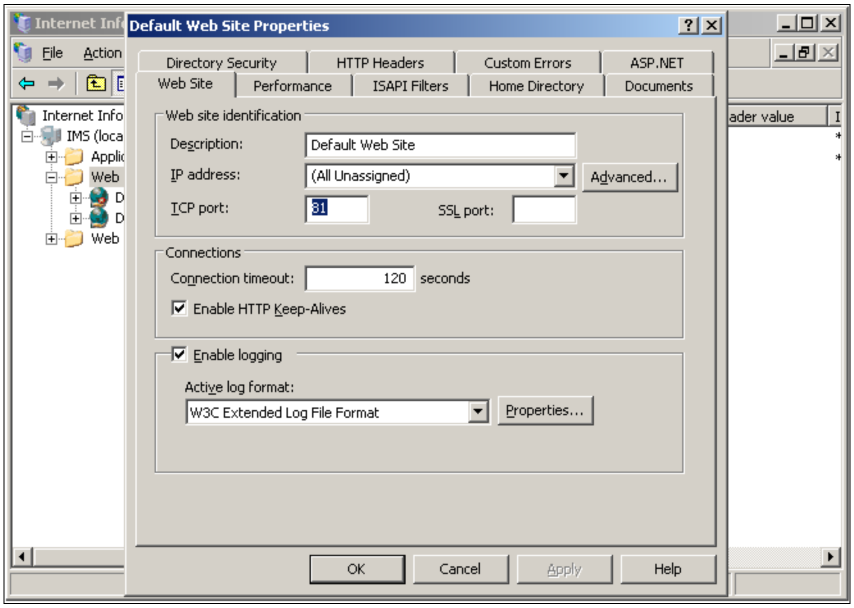

administrator
Manage Your Server
Command Prompt
Windows Explorer
Notepad
Start HTTP Server
Active Directory Users and Computers
Configure Your Server Wizard
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down
Start
C:\Documents and Settin...
Microsof
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server Wizard
Data Sources (ODBC)
DHCP
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Internet Information Services (IIS) Manager
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Server Management
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager

*Figure 1-8 Opening the IIS Manager*

2. Click the plus sign (+) for the server from the left pane.
3. Open the `Web Sites` directory, and right-click **Default Web Site**. If there is more than one website, right-click the one that is available, not the one that is stopped.
4. Select **Properties**. The window shown in Figure 1-9 opens. Several parameters appear, one of which is the TCP port. Note the value of the TCP port. (If the value is 80, change it to 81.



Default Web Site Properties

Web site identification

Description: Default Web Site

IP address: (All Unassigned)

TCP port: 81 SSL port:

Connections

Connection timeout: 120 seconds

☑ Enable HTTP Keep-Alives

☑ Enable logging

Active log format: W3C Extended Log File Format

*Figure 1-9 TCP port value*

## 1.5 Importing the CA root certificate to the IBM HTTP Server trust store, part 2

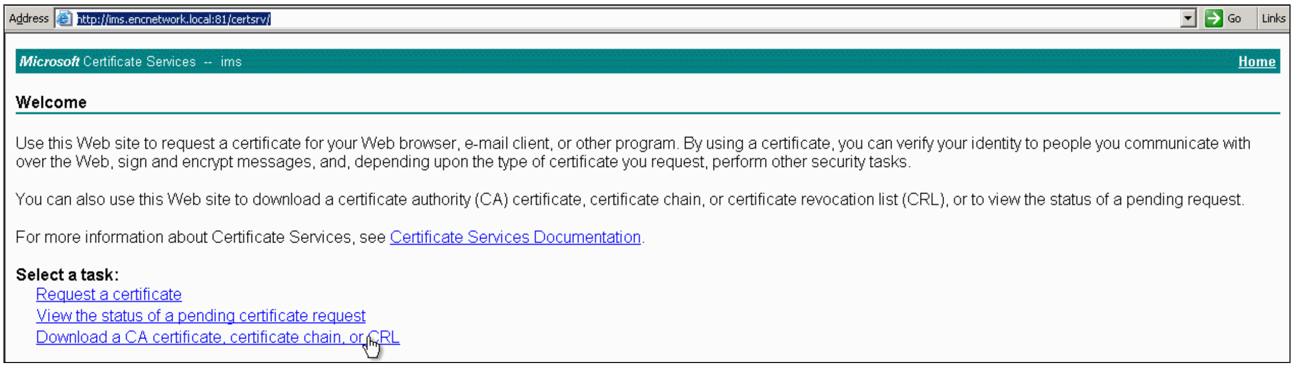
Now that you have determined the domain name and the IIS port number, enter the following address for the certificate server into the browser:

http://*domain_name*:*IIS_port_number*/certsrv

This opens the CA server page and allows certificates to be issued.

Next, follow these steps:

1. Click the **Download a CA certificate, certificate chain, or CRL** link, as shown in Figure 1-10.



Address http://ims.encnetwork.local:81/certsrv/

*Microsoft* Certificate Services -- ims    Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

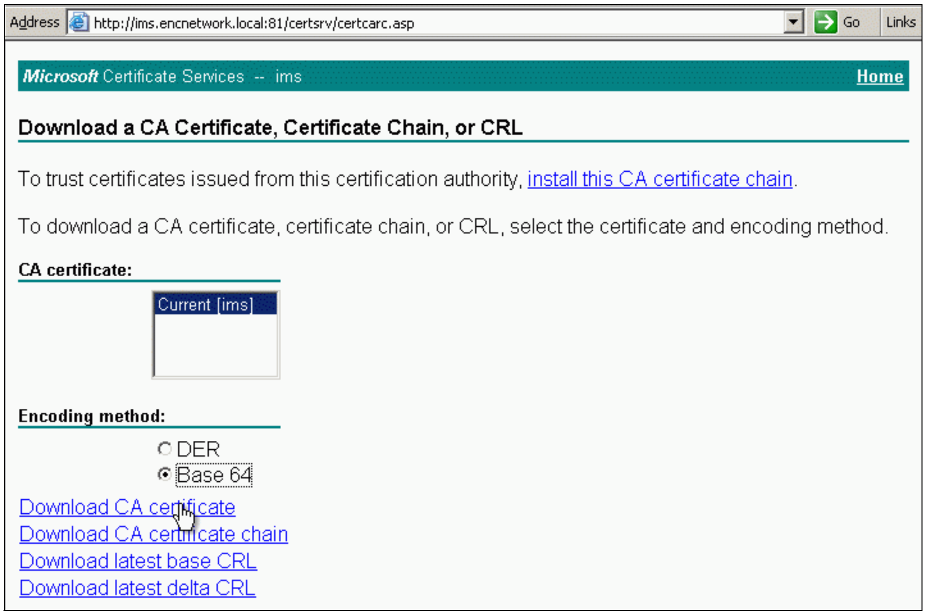
For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

*Figure 1-10   Downloading a certificate*

2. Enter the administrator's user ID and password at the prompt.
3. At the next page, you are prompted to select an encoding method. The following standards are supported:
   - DER
   - Base 64

   This scenario uses the Base 64 standard. Select the **Base 64** option, and click **Download CA certificate**, as shown in Figure 1-11.



Address http://ims.encnetwork.local:81/certsrv/certcarc.asp

*Microsoft* Certificate Services -- ims    Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

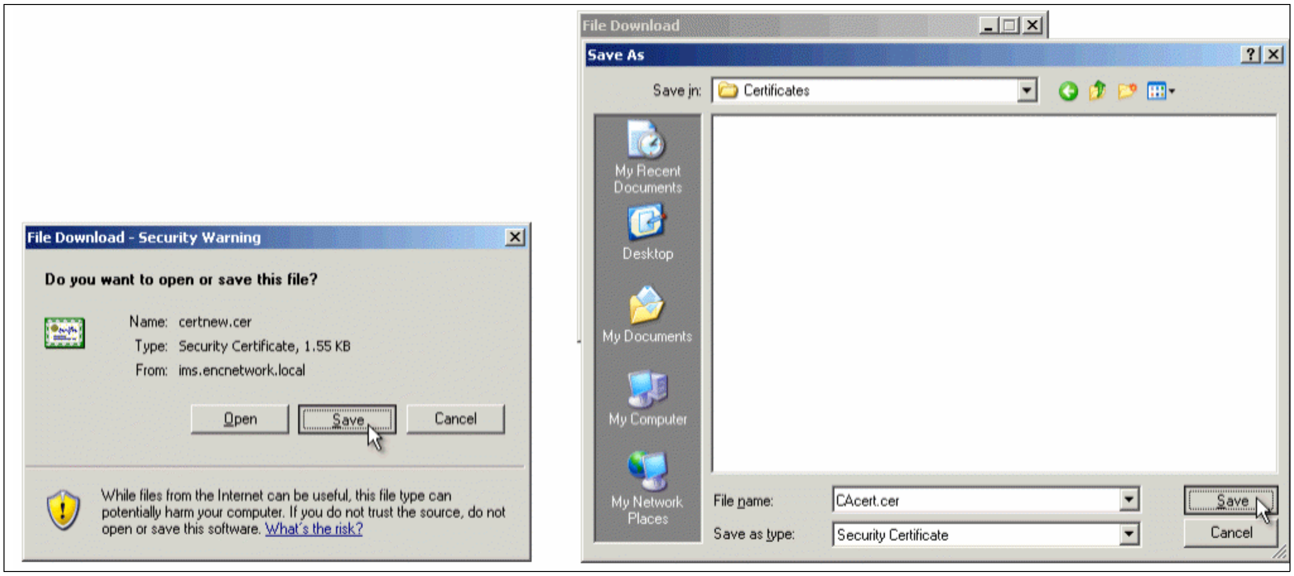
CA certificate:
Current [ims]

Encoding method:
○ DER
● Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

*Figure 1-11   Downloading the Base 64 CA certificate*

4. In the confirmation box, click **Save**, and select the location where you want to save the certificate. Assign a name to the certificate, as shown in Figure 1-12.



File Download - Security Warning

Do you want to open or save this file?

Name: certnew.cer

Type: Security Certificate, 1.55 KB

From: ims.encnetwork.local

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Save As

Save in: Certificates

File name: CAcert.cer

Save as type: Security Certificate

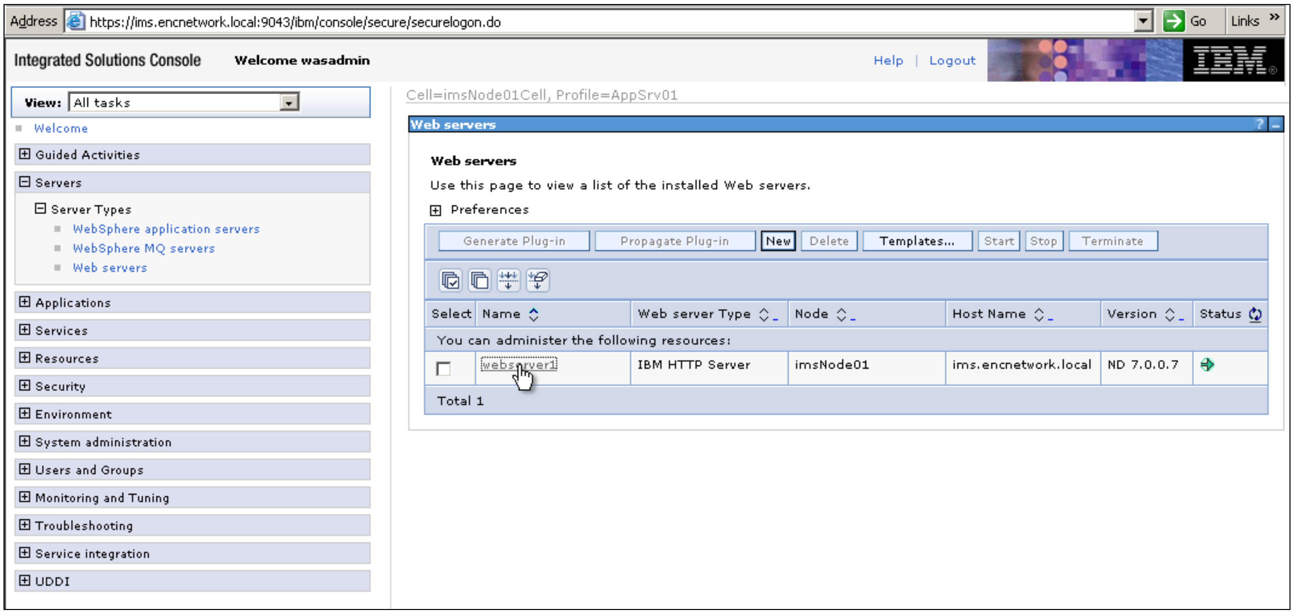
*Figure 1-12 Saving the certificate*

5. After you obtain the root CA certificate, import it into the IBM HTTP Server trust store:

   Navigate to **Start** → **IBM WebSphere** → **Application Server v7.0** → **Profiles** → **AppSrv01** → **Administrative Console.**

   On the left pane, expand **Servers** and then expand **Server Types.** On the right pane, under "Web servers," select the desired server, as shown in Figure 1-13.

> **Note:** At the Administrative Console, you need to enter the WebSphere Application Server administrator credentials.



Address https://ims.encnetwork.local:9043/ibm/console/secure/securelogon.do

Integrated Solutions Console Welcome wasadmin

View: All tasks

Cell=imsNode01Cell, Profile=AppSrv01

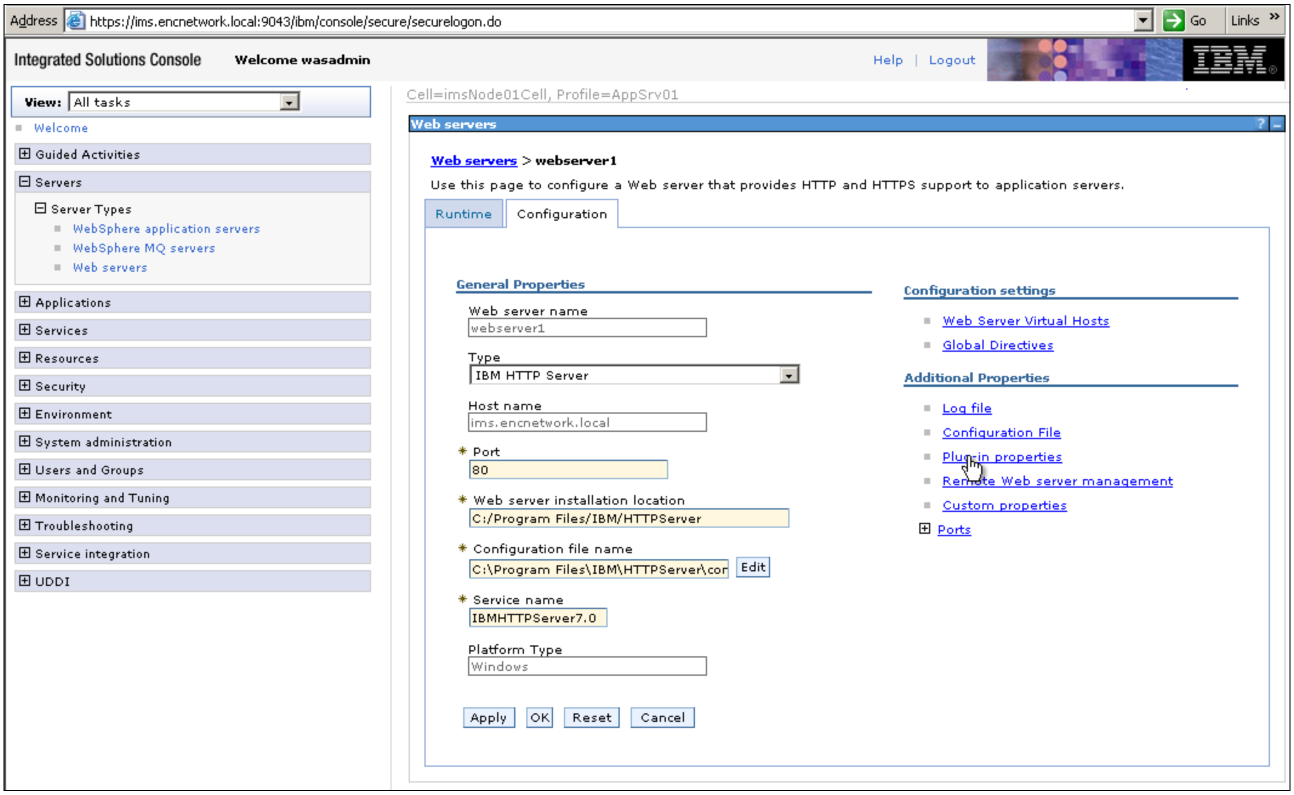
Web servers

Use this page to view a list of the installed Web servers.

| Select | Name | Web server Type | Node | Host Name | Version | Status |
|---|---|---|---|---|---|---|
| You can administer the following resources: | | | | | | |
| □ | webserver1 | IBM HTTP Server | imsNode01 | ims.encnetwork.local | ND 7.0.0.7 | ➔ |
| Total 1 | | | | | | |

*Figure 1-13 Administrative Console*

6. Under the Configuration tab, in the Additional Properties section, click **Plug-in properties**, as shown in Figure 1-14.



Address https://ims.encnetwork.local:9043/ibm/console/secure/securelogon.do

Integrated Solutions Console Welcome wasadmin

Cell=imsNode01Cell, Profile=AppSrv01

Web servers > webserver1

Use this page to configure a Web server that provides HTTP and HTTPS support to application servers.

General Properties

Web server name: webserver1

Type: IBM HTTP Server

Host name: ims.encnetwork.local

* Port: 80

* Web server installation location: C:/Program Files/IBM/HTTPServer

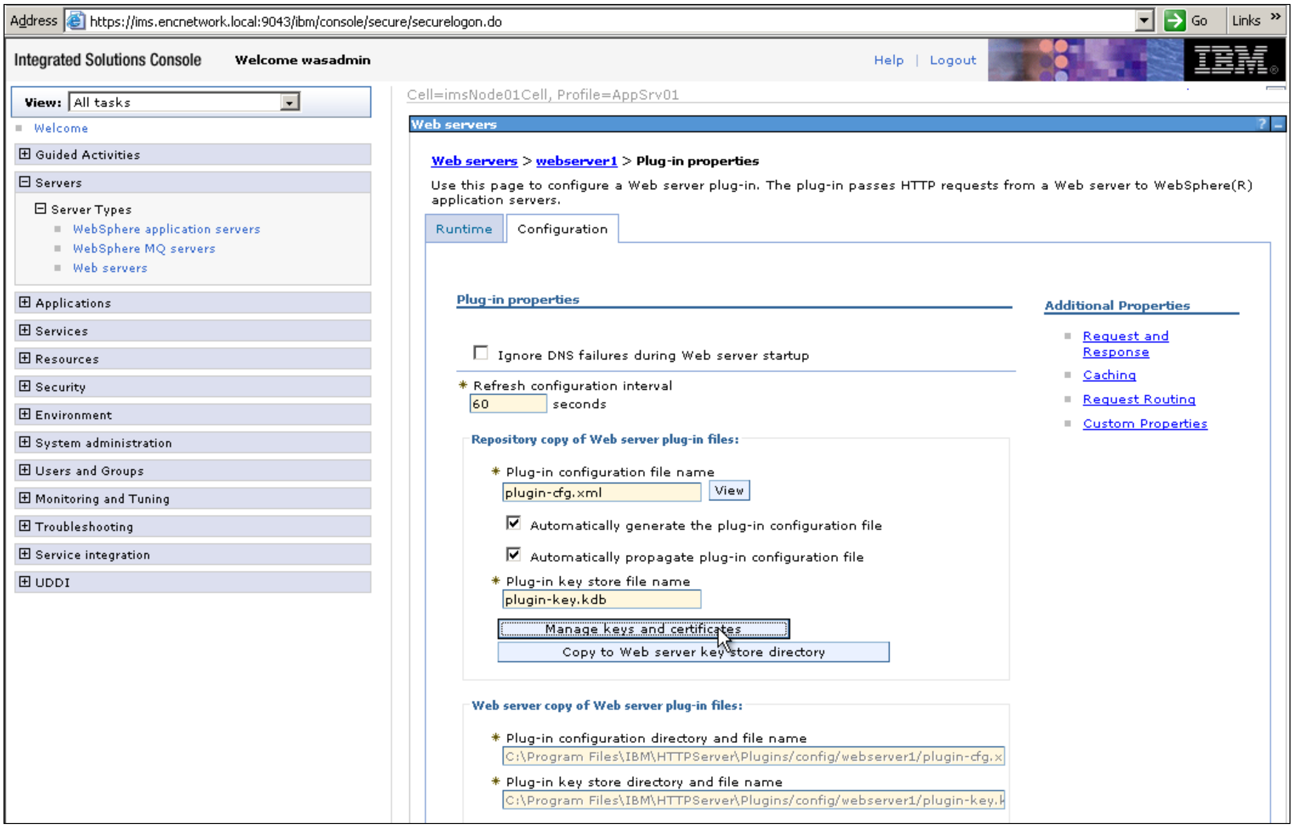
* Configuration file name: C:\Program Files\IBM\HTTPServer\cor

* Service name: IBMHTTPServer7.0

Platform Type: Windows

*Figure 1-14 Selecting Plug-in properties*

7. Click **Manage keys and certificates**, as shown in Figure 1-15.



Web servers > webserver1 > Plug-in properties

Use this page to configure a Web server plug-in. The plug-in passes HTTP requests from a Web server to WebSphere(R) application servers.

Plug-in properties

□ Ignore DNS failures during Web server startup

* Refresh configuration interval: 60 seconds

Repository copy of Web server plug-in files:

* Plug-in configuration file name: plugin-cfg.xml

☑ Automatically generate the plug-in configuration file

☑ Automatically propagate plug-in configuration file

* Plug-in key store file name: plugin-key.kdb

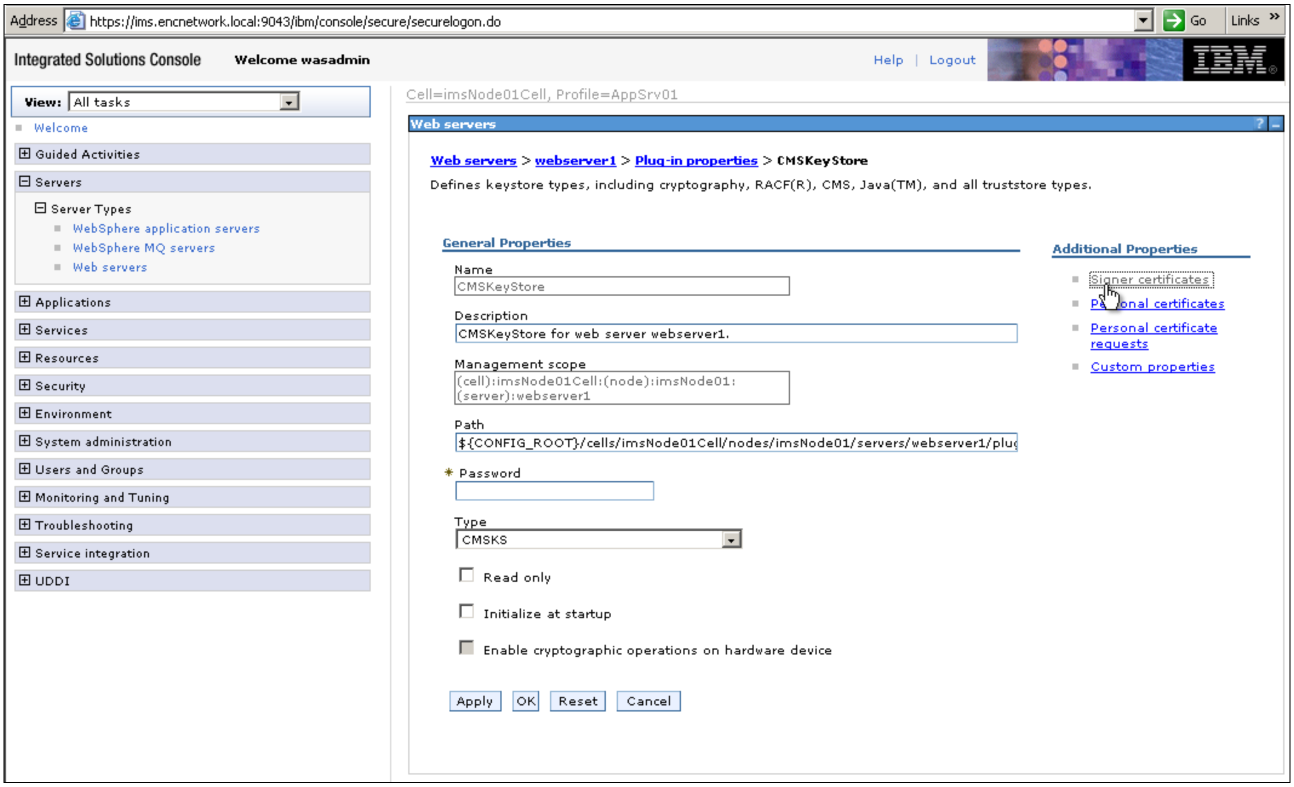
Web server copy of Web server plug-in files:

* Plug-in configuration directory and file name: C:\Program Files\IBM\HTTPServer\Plugins/config/webserver1/plugin-cfg.x

* Plug-in key store directory and file name: C:\Program Files\IBM\HTTPServer\Plugins/config/webserver1/plugin-key.k

*Figure 1-15 Selecting Manage keys and certificates*

8. Then, click **Signer certificates**, as shown in Figure 1-16.



Address https://ims.encnetwork.local:9043/ibm/console/secure/securelogon.do

Cell=imsNode01Cell, Profile=AppSrv01

Web servers > webserver1 > Plug-in properties > CMSKeyStore

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

General Properties

Name: CMSKeyStore

Description: CMSKeyStore for web server webserver1.

Management scope: (cell):imsNode01Cell:(node):imsNode01:(server):webserver1

Path: ${CONFIG_ROOT}/cells/imsNode01Cell/nodes/imsNode01/servers/webserver1/plug

* Password

Type: CMSKS

□ Read only

□ Initialize at startup

□ Enable cryptographic operations on hardware device

Additional Properties

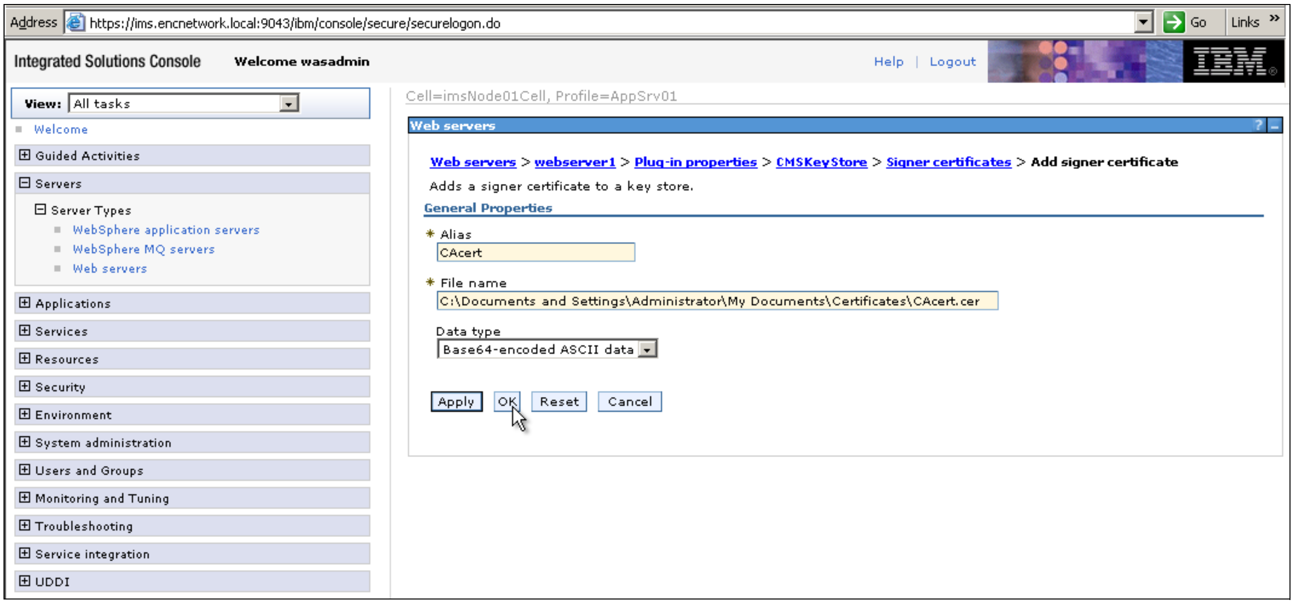
- Signer certificates
- Personal certificates
- Personal certificate requests
- Custom properties

*Figure 1-16 Selecting signer certificates*

9. On the right pane of the next panel, complete the following information:

   – **Alias**: An alias name of your choice
   – **File Name**: Full path of the CA certificate that you created earlier

10. Click **OK**, as shown in Figure 1-17. Save the changes when prompted to do so.



Address https://ims.encnetwork.local:9043/ibm/console/secure/securelogon.do

Cell=imsNode01Cell, Profile=AppSrv01

Web servers > webserver1 > Plug-in properties > CMSKeyStore > Signer certificates > Add signer certificate

Adds a signer certificate to a key store.

General Properties

* Alias: CAcert

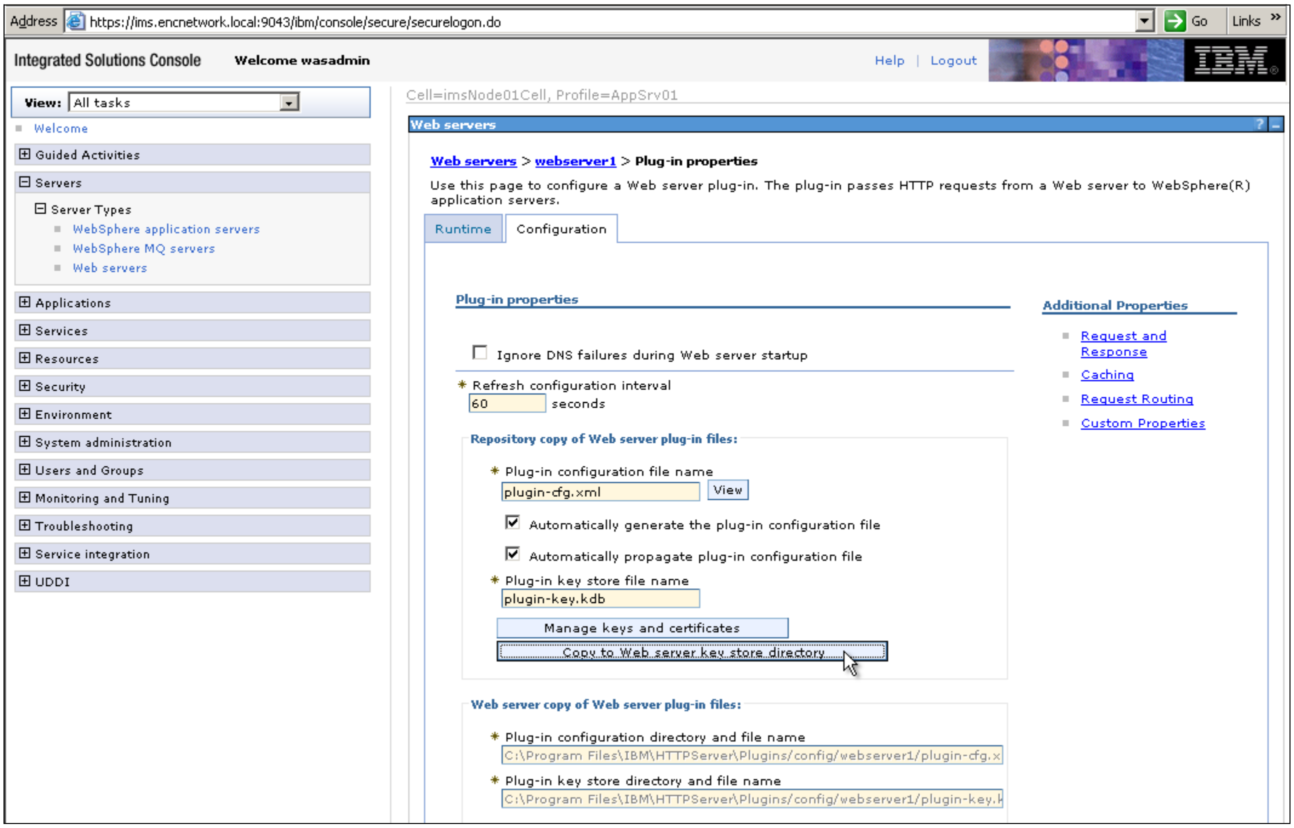
* File name: C:\Documents and Settings\Administrator\My Documents\Certificates\CAcert.cer

Data type: Base64-encoded ASCII data

*Figure 1-17 Copying certificate to web server*

11. On the left pane of the WAS Administrative Console, expand **Servers** and then expand **Server Types**. Select **Web servers**.

    On the right pane, select the desired web server, and then, under "Plug-in Properties," click **Copy to web server key store directory**, as shown in Figure 1-18. The root CA certificate is imported into the IBM HTTP Server trust store.



Use this page to configure a Web server plug-in. The plug-in passes HTTP requests from a Web server to WebSphere(R) application servers.

Plug-in properties

☐ Ignore DNS failures during Web server startup

* Refresh configuration interval: 60 seconds

Repository copy of Web server plug-in files:

* Plug-in configuration file name: plugin-cfg.xml

☑ Automatically generate the plug-in configuration file

☑ Automatically propagate plug-in configuration file

* Plug-in key store file name: plugin-key.kdb

Web server copy of Web server plug-in files:

* Plug-in configuration directory and file name: C:\Program Files\IBM\HTTPServer\Plugins/config/webserver1/plugin-cfg.x

* Plug-in key store directory and file name: C:\Program Files\IBM\HTTPServer\Plugins/config/webserver1/plugin-key.k

*Figure 1-18 Copying to key store*

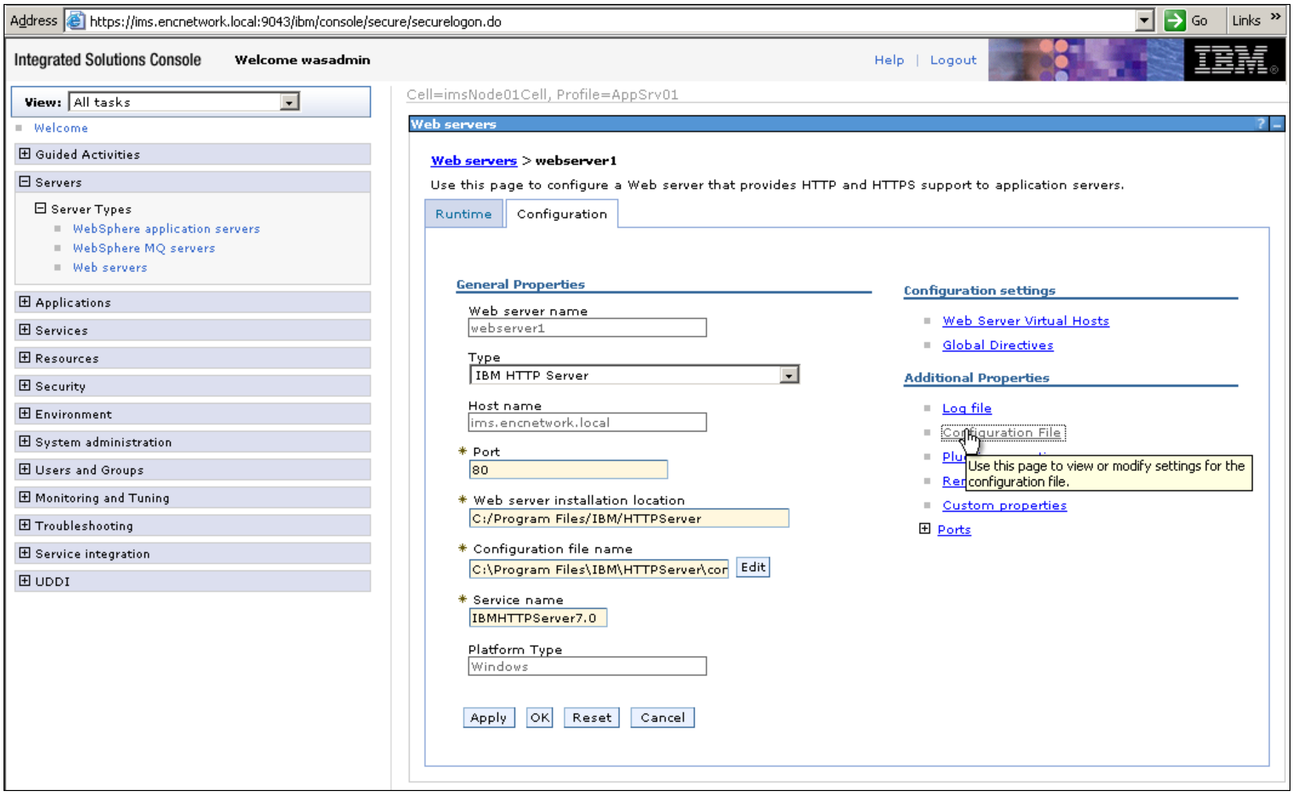
12. Finally, restart the IBM HTTP Server. On the left pane of the WAS Administrative Console, expand **Servers** and then expand **Server Types**. Select **Web servers**.

    On the right pane, select the **webserver1** link, and click **Stop**. After webserver1 stops, select the link again, and click **Start**.

## 1.6 Enabling two-way SSL on IBM HTTP Server

To enable secure communications on the IBM HTTP Server, follow these steps:

1. Log on to the WebSphere Application Server Administrative Console.
2. Then, go to **Server** → **Server Types** → **Web servers** → ***web_server*** → **Configuration file**, as shown in Figure 1-19.



Use this page to configure a Web server that provides HTTP and HTTPS support to application servers.

Web server name: webserver1

Type: IBM HTTP Server

Host name: ims.encnetwork.local

* Port: 80

* Web server installation location: C:/Program Files/IBM/HTTPServer

* Configuration file name: C:\Program Files\IBM\HTTPServer\cor

* Service name: IBMHTTPServer7.0

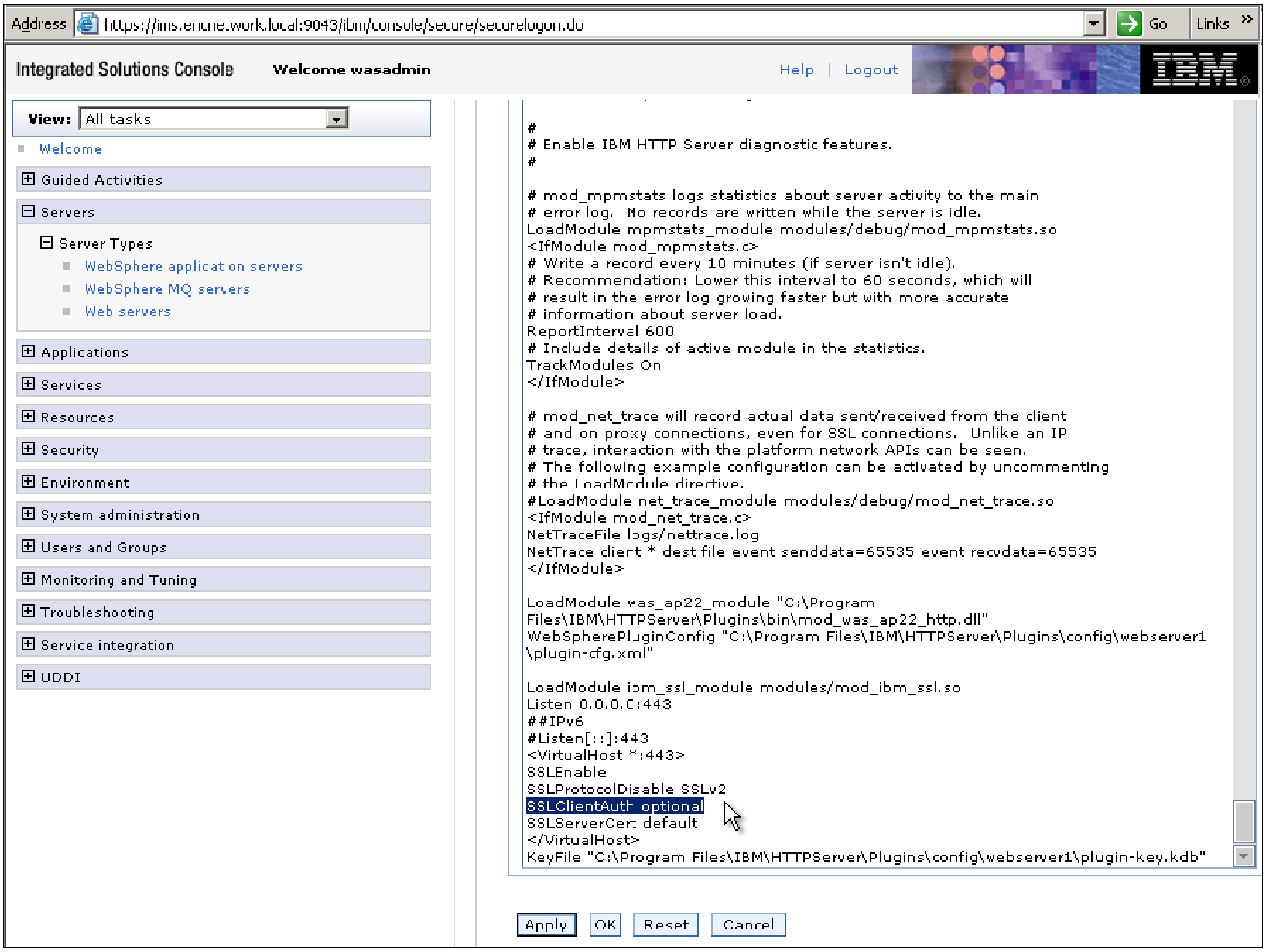
Platform Type: Windows

Use this page to view or modify settings for the configuration file.

*Figure 1-19 Configuration file*

3. Insert the following text between `SSLProtocolDisable SSLv2` and `SSLServerCert default`, as shown in Figure 1-20:

   `SSLClientAuth optional`



```
#
# Enable IBM HTTP Server diagnostic features.
#

# mod_mpmstats logs statistics about server activity to the main
# error log.  No records are written while the server is idle.
LoadModule mpmstats_module modules/debug/mod_mpmstats.so
<IfModule mod_mpmstats.c>
# Write a record every 10 minutes (if server isn't idle).
# Recommendation: Lower this interval to 60 seconds, which will
# result in the error log growing faster but with more accurate
# information about server load.
ReportInterval 600
# Include details of active module in the statistics.
TrackModules On
</IfModule>

# mod_net_trace will record actual data sent/received from the client
# and on proxy connections, even for SSL connections.  Unlike an IP
# trace, interaction with the platform network APIs can be seen.
# The following example configuration can be activated by uncommenting
# the LoadModule directive.
#LoadModule net_trace_module modules/debug/mod_net_trace.so
<IfModule mod_net_trace.c>
NetTraceFile logs/nettrace.log
NetTrace client * dest file event senddata=65535 event recvdata=65535
</IfModule>

LoadModule was_ap22_module "C:\Program
Files\IBM\HTTPServer\Plugins\bin\mod_was_ap22_http.dll"
WebSpherePluginConfig "C:\Program Files\IBM\HTTPServer\Plugins\config\webserver1
\plugin-cfg.xml"

LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
##IPv6
#Listen[::]:443
<VirtualHost *:443>
SSLEnable
SSLProtocolDisable SSLv2
SSLClientAuth optional
SSLServerCert default
</VirtualHost>
KeyFile "C:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb"
```

*Figure 1-20   Entering text*

4. Click **OK**. Then, on the next page, click **OK** again, and click **Save**.

## 1.7 Creating IMS policies for smart card use

To create IMS policies for smart card use, follow these steps:

1. Open a browser, and enter the IMS Server location. On the IMS Server page, select the AccessAdmin option.
2. Enter the login details for the administrator for the IMS Server.
3. On the left pane of the AccessAdmin panel, under Machine Policy Templates, click **New Template**.

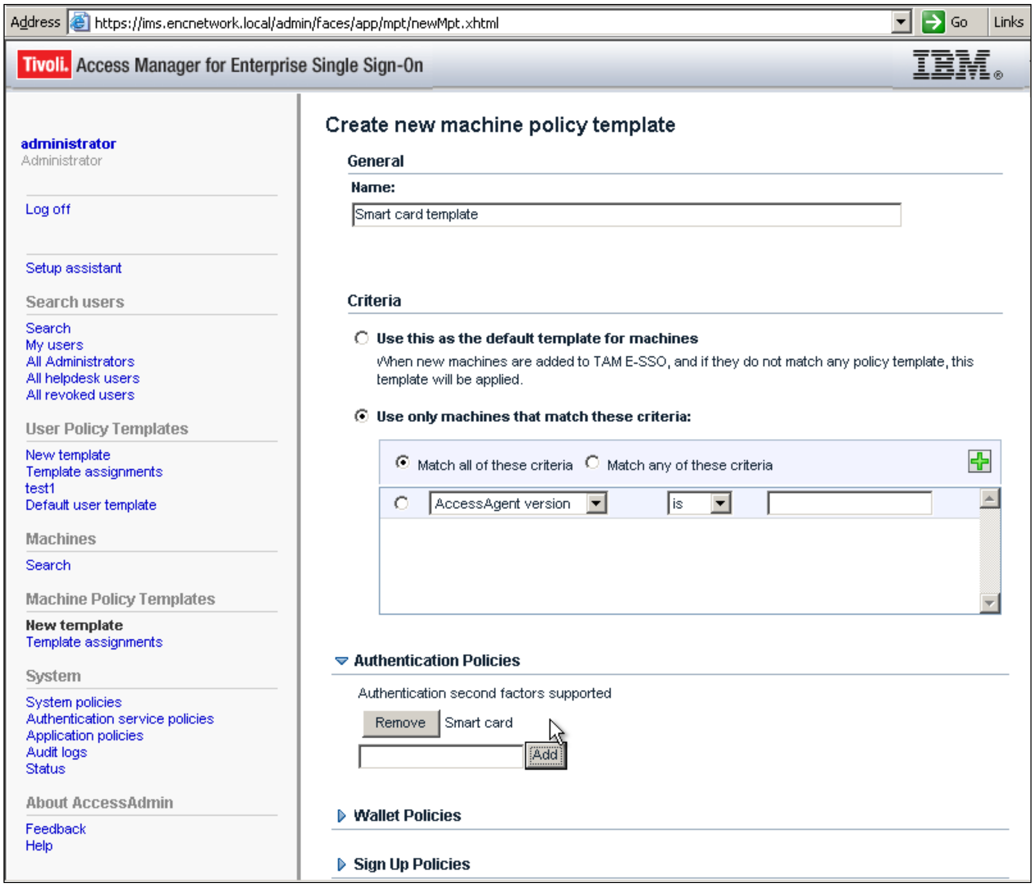
4. On the “Create new policy template” panel, shown in Figure 1-21, enter the following information:

   – **Name**: Name of the template. Assign a meaningful name.

   – **Criteria**: Indication that this template is for specific machines on your domain. Use the default option.

   – **Authentication Policies**: Smart card designation. Enter this into the text box.

5. Click **Add**.



Create new machine policy template

General

Name: Smart card template

Criteria

○ Use this as the default template for machines

When new machines are added to TAM E-SSO, and if they do not match any policy template, this template will be applied.

● Use only machines that match these criteria:

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version is

Authentication Policies

Authentication second factors supported

Remove Smart card

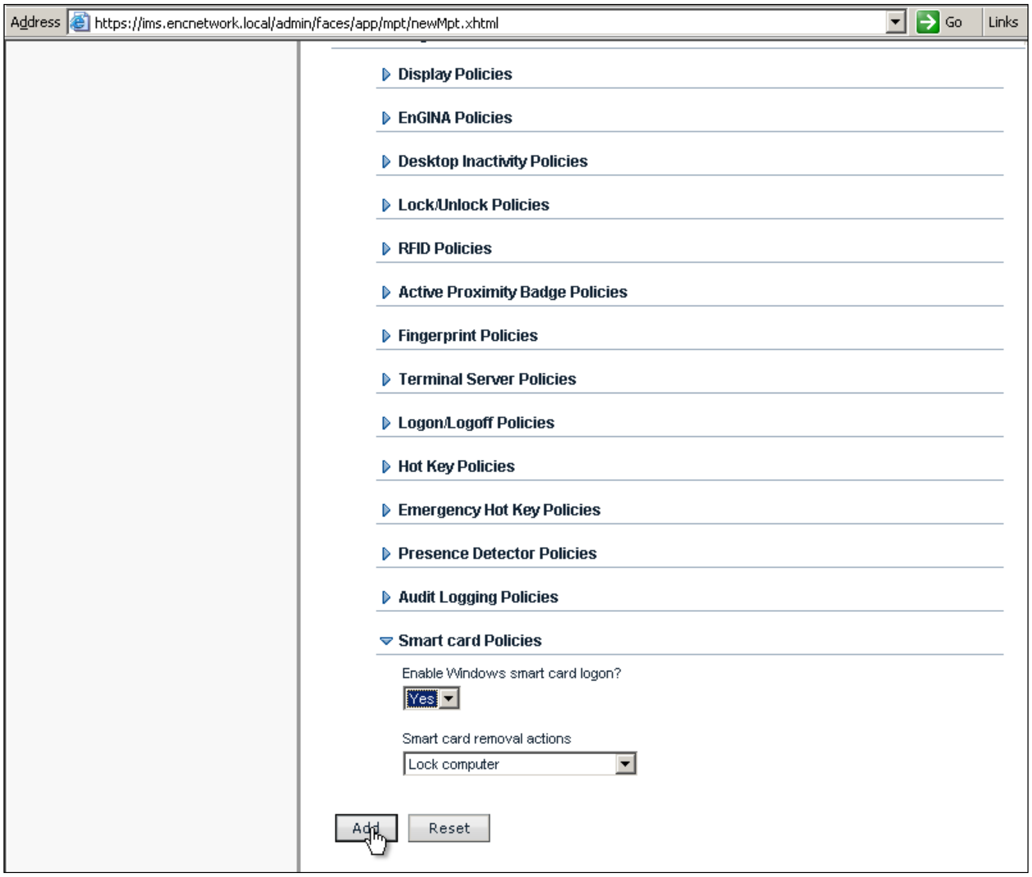
Add

Wallet Policies

Sign Up Policies

*Figure 1-21 Entering the new template information*

6. Next, scroll further down on the “Create new policy template” panel, expand AccessAgent Policies, and click **Smart card policies**.
7. When prompted, select **Yes** to enable Windows smart card logon, and then click **Add**, as shown in Figure 1-22.



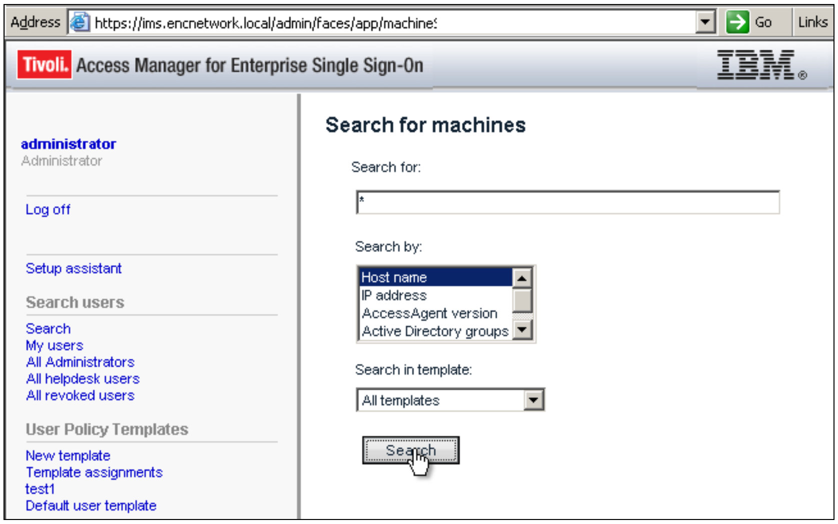
Enable Windows smart card logon? Yes

Smart card removal actions: Lock computer

*Figure 1-22 Adding smart card policies*

## 1.8 Assigning the new template to the client workstation

To assign the new template to the client workstation, go to **Machines** → **Search**. Enter an asterisk (*****) in the "Search for" field and select **Host name** in the "Search by" drop-down. Make sure to select **All templates** in the "Search in template" drop-down list. Then, click **Search** to list the workstations that are connected to the IMS Server using AccessAgent, as shown in Figure 1-23.



Address https://ims.encnetwork.local/admin/faces/app/machine

Tivoli. Access Manager for Enterprise Single Sign-On

administrator
Administrator

Search for machines

Search for: *

Search by: Host name

Search in template: All templates

*Figure 1-23 Listing the workstations connected to the IMS Server using AccessAgent*

Select the desired workstation. Then, from **Machine Template Assignment**, select the **Smart Card policy**, and click **Assign**.

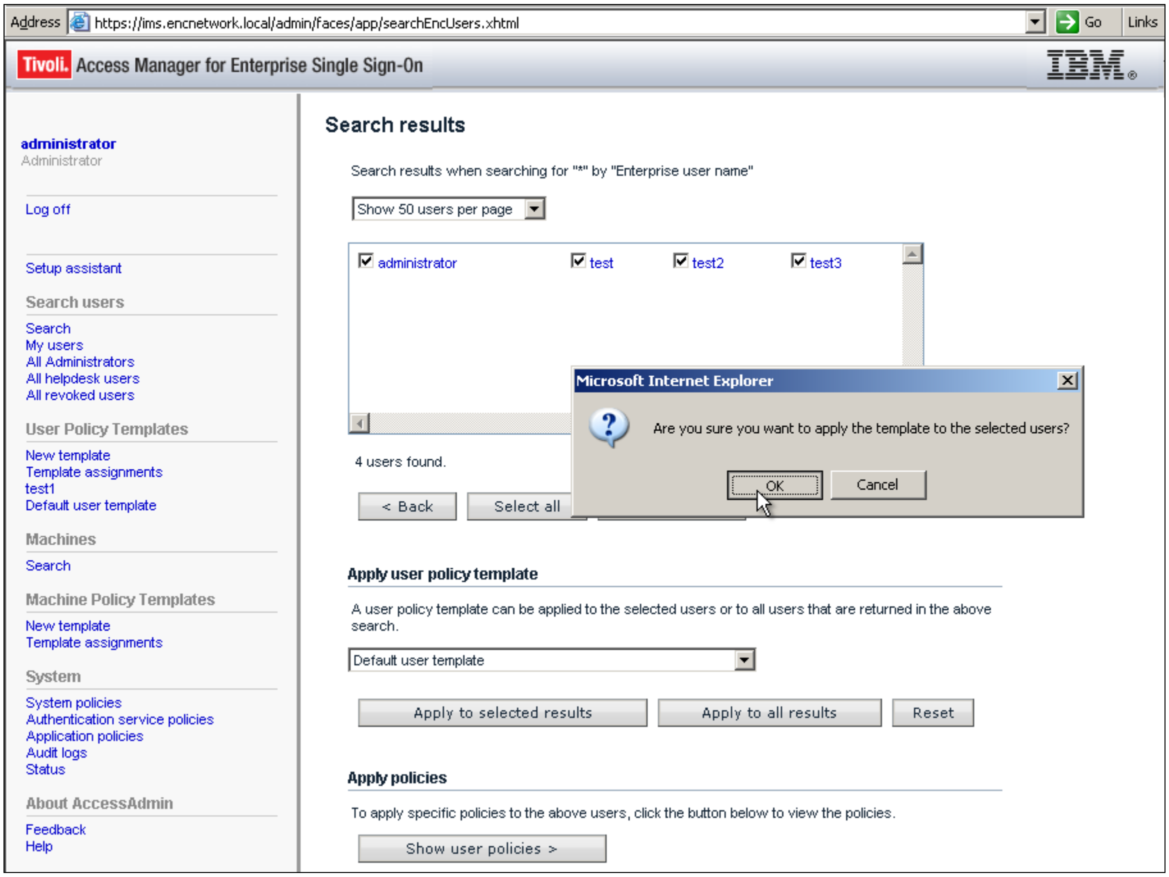
## 1.9 Modifying user default template to accept smart cards for authentication

To modify the user default template to accept smart cards for authentication, follow these steps:

1. Under the "Apply user policy templates" heading, select **Default user template**.
2. On the new panel, click **Authentication Policies**. Then, enable the **Smart card box** option, and click **Update**.
3. Under the "Search users" heading, click the **Search** link. Then, fill in the required fields to narrow down your search and click **Search**.

4. Select the users who require smart card use. Under the **Apply user policy template** heading, select **Default user template** from the drop-down menu, and click **Apply to selected results**.

5. At the confirmation prompt, click **OK**, as shown in Figure 1-24.



Address https://ims.encnetwork.local/admin/faces/app/searchEncUsers.xhtml

Search results

Search results when searching for "*" by "Enterprise user name"

Show 50 users per page

☑ administrator ☑ test ☑ test2 ☑ test3

4 users found.

Microsoft Internet Explorer

Are you sure you want to apply the template to the selected users?

Apply user policy template

A user policy template can be applied to the selected users or to all users that are returned in the above search.

Default user template

Apply policies

To apply specific policies to the above users, click the button below to view the policies.

*Figure 1-24 Confirming modification to template*

6. A status bar displays the progress of applying the user template. When the task is complete, restart WebSphere Application Server, as shown in Figure 1-25.

   To stop WebSphere, select **Start** → **All Programs** → **IBM WebSphere** → **Application Server Network Deployment V7.0** → **Profiles** -> **AppSrv01** → **Stop the server**.

   To restart WebSphere select **Start** → **All Programs** → **IBM WebSphere** → **Application Server Network Deployment V7.0** → **Profiles** → **AppSrv01** → **Start the server**.

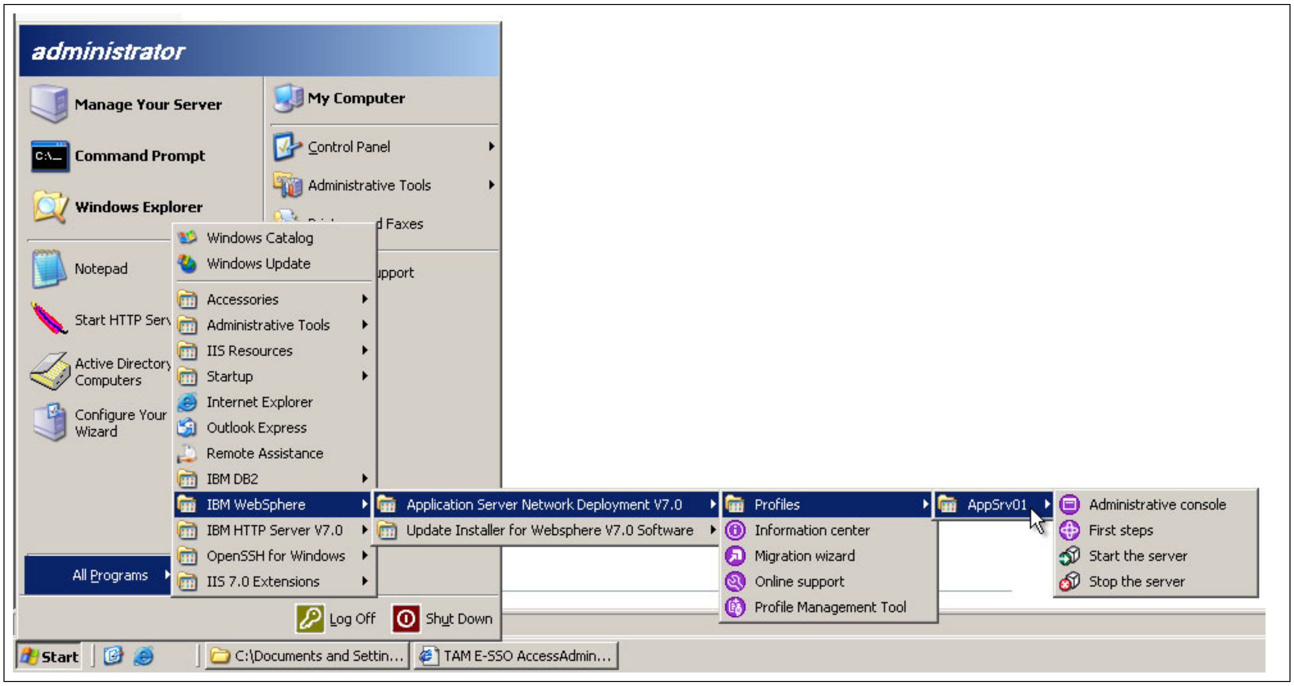


*Figure 1-25 Restarting WebSphere Application Server*

7. The AccessAgent icon on the client system displays a message for the computer to be restarted due to changes on the IMS Server. Restart the computer. The AccessAgent is now ready to allow authentication by smart cards.

## 1.10 Issuing a certificate to a smart card

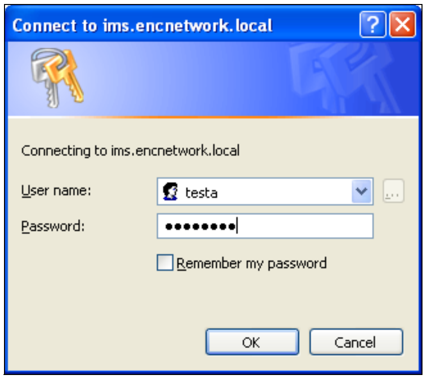
> **Note:** This exercise issues a smart card to the user who logs on, which might not be the case in a real-world scenario.

To issue a certificate to a smart card, follow these steps:

1. On the client system, log on to the Windows system with the ID of the user who requires the smart card use. Do not use AccessAgent to log in.
2. Insert the smart card in the reader or the token in a spare USB slot, as appropriate.
3. Go to the certificate server web page:

   http://*domain_name*:*IIS_port_number*/certsrv

4. Log on using the user’s credentials, as shown in Figure 1-26.



Connecting to ims.encnetwork.local

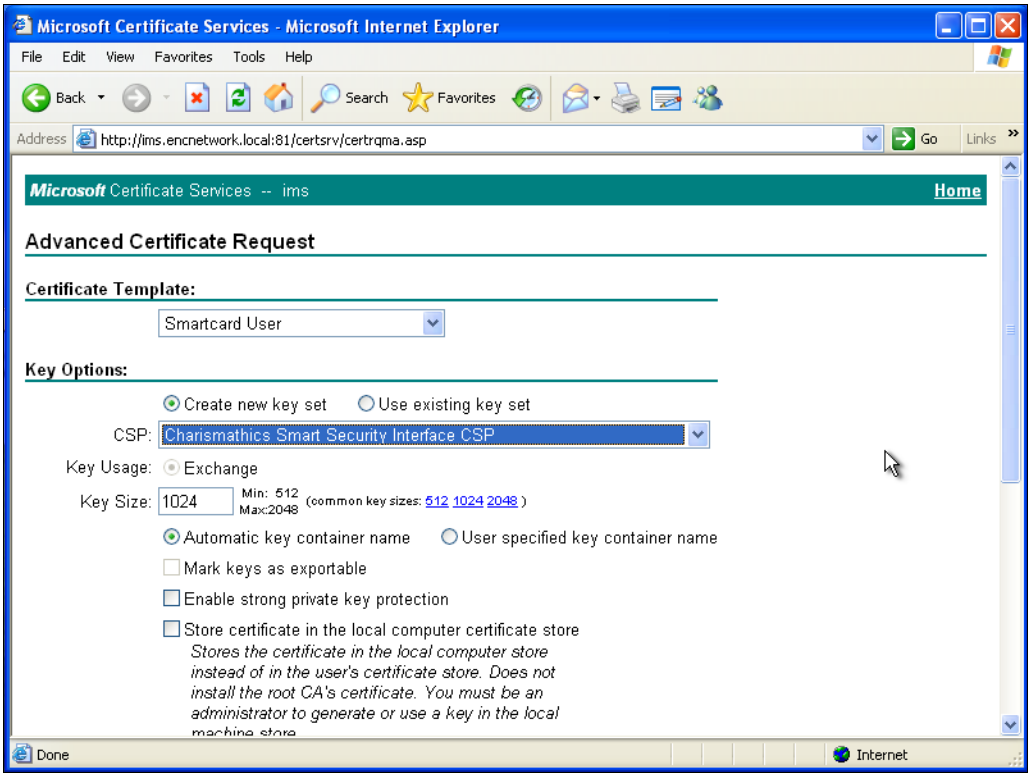
User name: testa

Password: ••••••••

☐ Remember my password

*Figure 1-26 Logging in to issue a certificate*

5. Click **Request a certificate** from the “Select a task” options. Then, select the **Advanced Certificate Request** option, and select the **Create and submit a request to this CA** option.
6. Change only the following parameters, as shown in Figure 1-27:
   - For Certificate Template, use **Smartcard User**.
   - From the CSP drop-down under Key Options, select the relevant middleware that is used within your environment. (This example uses the Charismathics Smart Security Interface CSP.)



Address http://ims.encnetwork.local:81/certsrv/certrqma.asp

Microsoft Certificate Services -- ims Home

Advanced Certificate Request

Certificate Template:

Smartcard User

Key Options:

● Create new key set ○ Use existing key set

CSP: Charismathics Smart Security Interface CSP

Key Usage: ● Exchange

Key Size: 1024 Min: 512 Max:2048 (common key sizes: 512 1024 2048 )

● Automatic key container name ○ User specified key container name

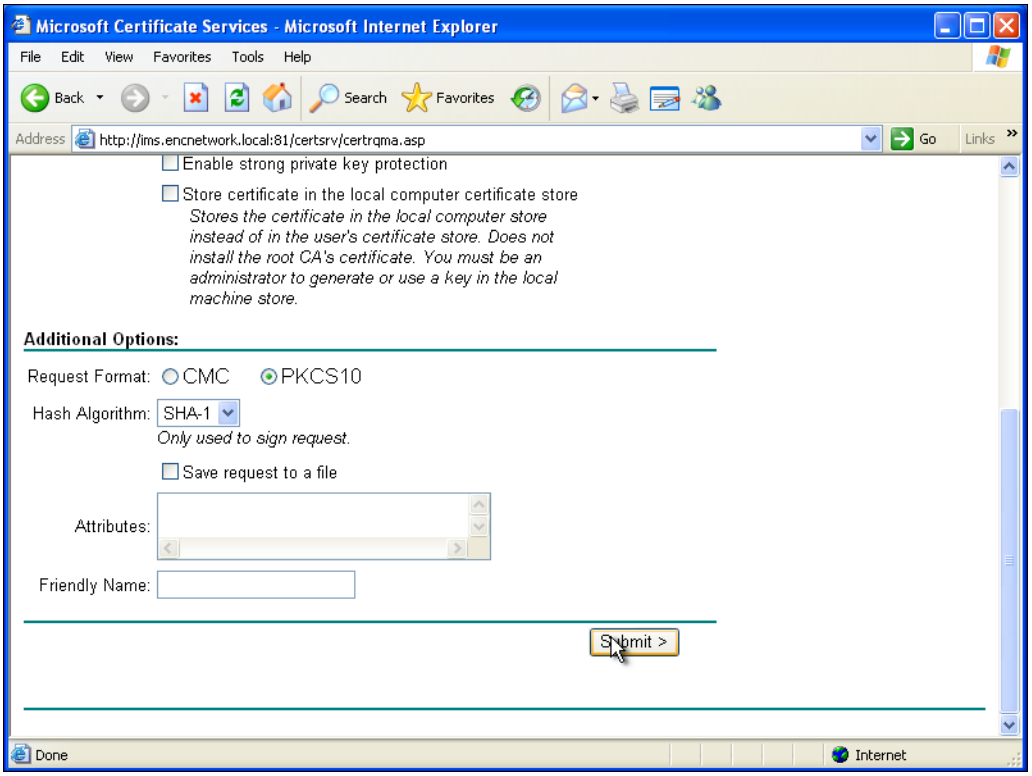
☐ Mark keys as exportable

☐ Enable strong private key protection

☐ Store certificate in the local computer certificate store
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

*Figure 1-27 Changing parameters for requesting certificate*

7. For Request Format under Additional Options, select **PKCS10** (Public Key Cryptography Standard for requesting certificates).
8. Click **Submit**, as shown in Figure 1-28.



Microsoft Certificate Services - Microsoft Internet Explorer

Address http://ims.encnetwork.local:81/certsrv/certrqma.asp

□ Enable strong private key protection

□ Store certificate in the local computer certificate store
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Additional Options:**

Request Format: ○ CMC ● PKCS10

Hash Algorithm: SHA-1
*Only used to sign request.*

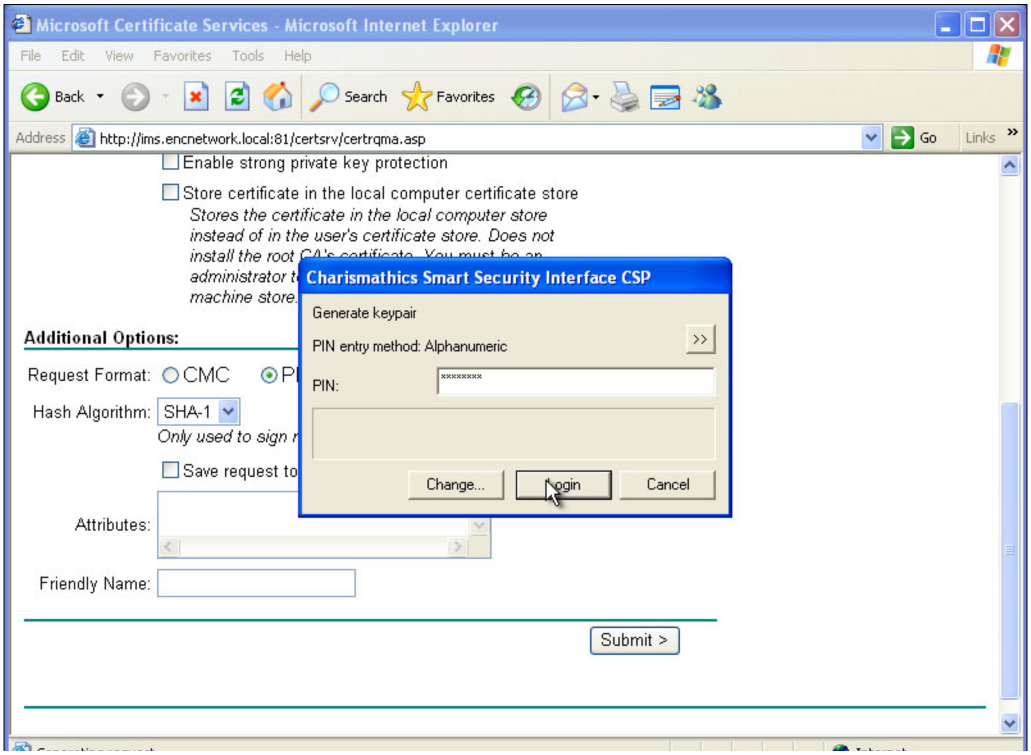
□ Save request to a file

Attributes:

Friendly Name:

*Figure 1-28 Submitting certificate request*

9. If you receive a warning message about a potential scripting violation, click **Yes** to open a window for the appropriate smart card middleware CSP. Then, enter the PIN for the smart card, and click **Login** as shown in Figure 1-29.



Microsoft Certificate Services - Microsoft Internet Explorer

Address http://ims.encnetwork.local:81/certsrv/certrqma.asp

□ Enable strong private key protection

□ Store certificate in the local computer certificate store
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator t… machine store.*

**Additional Options:**

Request Format: ○ CMC ● P…

Hash Algorithm: SHA-1
*Only used to sign r…*

□ Save request to…

Attributes:

Friendly Name:

Charismathics Smart Security Interface CSP

Generate keypair

PIN entry method: Alphanumeric

PIN: ********

*Figure 1-29 Providing login information for the smart card middleware*

The following message appears:

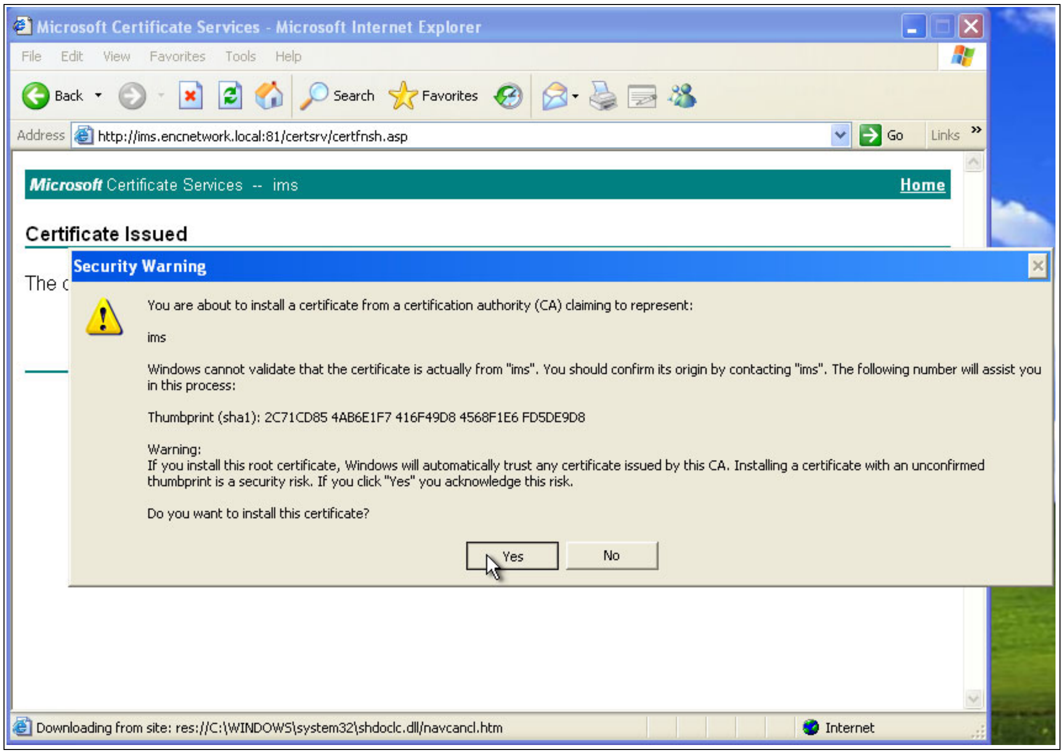
```
Generating Request
```

Then, another message appears:

```
Waiting for Server response
```

These messages might display for two minutes or so.

10. When the Certificate Issued page appears, click **Install this certificate**. When a warning message about a potential scripting violation appears, click **Yes** to continue. Then, when a message appears requesting confirmation for the installation of the certificate from the CA server, click **Yes** again.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://ims.encnetwork.local:81/certsrv/certfnsh.asp
Go
Links
Microsoft Certificate Services -- ims
Home
Certificate Issued
The c
Security Warning
Yes
No
Downloading from site: res://C:\WINDOWS\system32\shdoclc.dll/navcancl.htm
Internet

You are about to install a certificate from a certification authority (CA) claiming to represent:

ims

Windows cannot validate that the certificate is actually from "ims". You should confirm its origin by contacting "ims". The following number will assist you in this process:

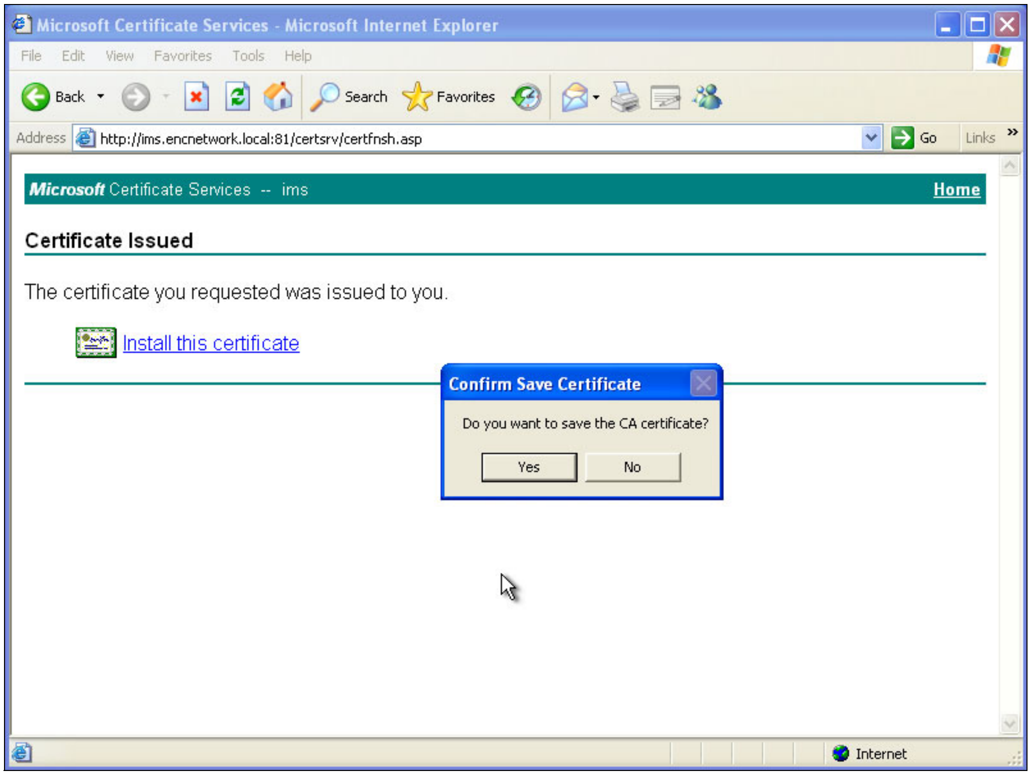
Thumbprint (sha1): 2C71CD85 4AB6E1F7 416F49D8 4568F1E6 FD5DE9D8

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

*Figure 1-30 Accepting a new certificate from your IMS server*

11. Click **Yes** when prompted to save the CA certificate.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Internet

http://ims.encnetwork.local:81/certsrv/certfnsh.asp

Microsoft Certificate Services -- ims Home

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

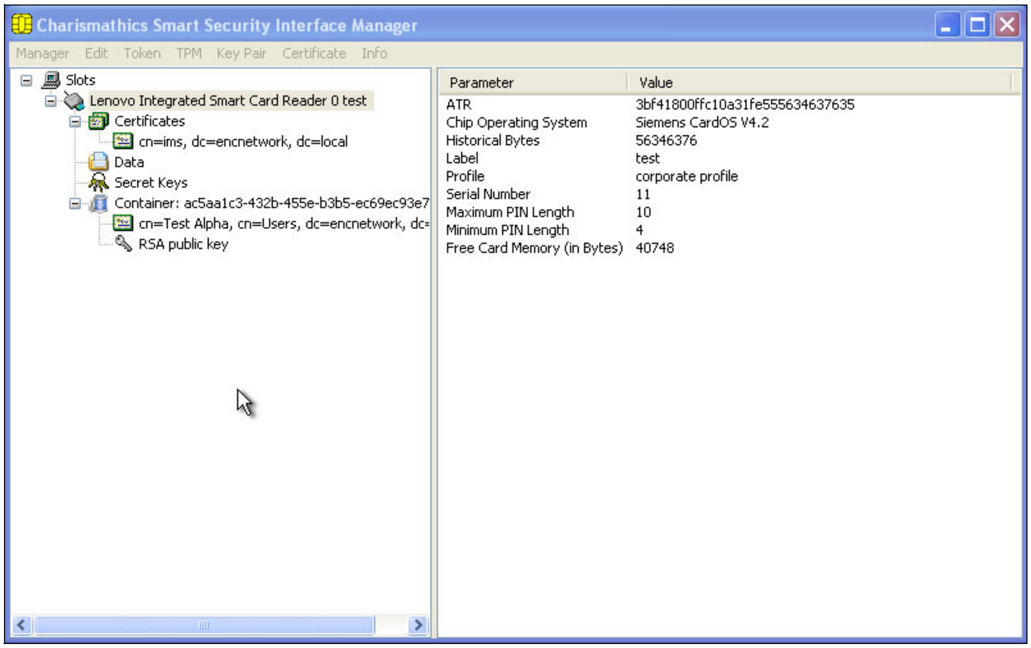
Confirm Save Certificate

Do you want to save the CA certificate?

Yes No

*Figure 1-31 Saving the CA certificate*

12. After the confirmation message appears, open the middleware software and read the smart card contents. Verify that the certificate has been installed. Figure 1-30 on page 26 shows an example of the contents as displayed by the Charismathics Smart Security Interface Manager.


Charismathics Smart Security Interface Manager
Manager Edit Token TPM Key Pair Certificate Info

- Slots
  - Lenovo Integrated Smart Card Reader 0 test
    - Certificates
      - cn=ims, dc=encnetwork, dc=local
    - Data
    - Secret Keys
    - Container: ac5aa1c3-432b-455e-b3b5-ec69ec93e7
      - cn=Test Alpha, cn=Users, dc=encnetwork, dc=
      - RSA public key

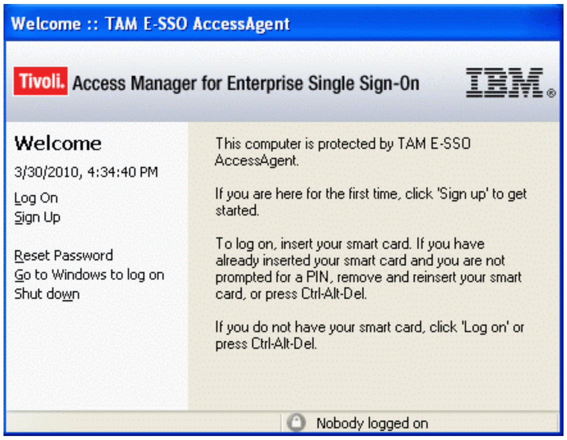
| Parameter | Value |
|---|---|
| ATR | 3bf41800ffc10a31fe555634637635 |
| Chip Operating System | Siemens CardOS V4.2 |
| Historical Bytes | 56346376 |
| Label | test |
| Profile | corporate profile |
| Serial Number | 11 |
| Maximum PIN Length | 10 |
| Minimum PIN Length | 4 |
| Free Card Memory (in Bytes) | 40748 |

*Figure 1-32 Contents displayed by the Charismathics Smart Security Interface*

## 1.11 Registering a smart card to user

To register a smart card to a user, follow these steps:

1. On the client system, insert the smart card into the reader when the AccessAgent logon window is displayed. AccessAgent prompts you for the smart card registration with the user account, as shown in Figure 1-33.



3/30/2010, 4:34:40 PM

This computer is protected by TAM E-SSO AccessAgent.

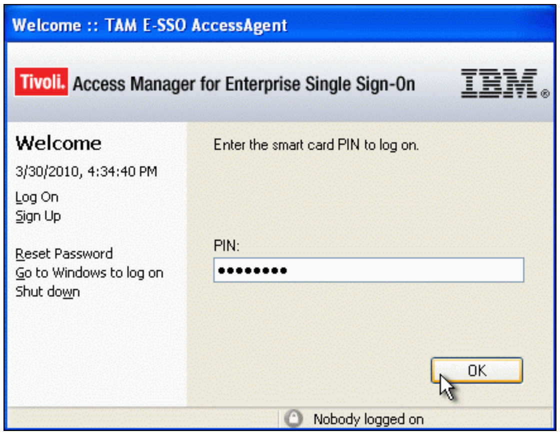
If you are here for the first time, click 'Sign up' to get started.

To log on, insert your smart card. If you have already inserted your smart card and you are not prompted for a PIN, remove and reinsert your smart card, or press Ctrl-Alt-Del.

If you do not have your smart card, click 'Log on' or press Ctrl-Alt-Del.

*Figure 1-33 Smart card registration*

2. Enter the PIN that was assigned to the smart card during the certificate request process, and then click **OK**, as shown in Figure 1-34.



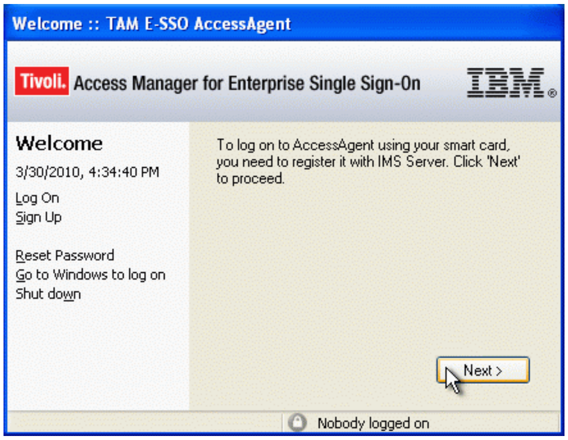
3/30/2010, 4:34:40 PM

Enter the smart card PIN to log on.

PIN: ••••••••

*Figure 1-34 Entering smart card PIN*

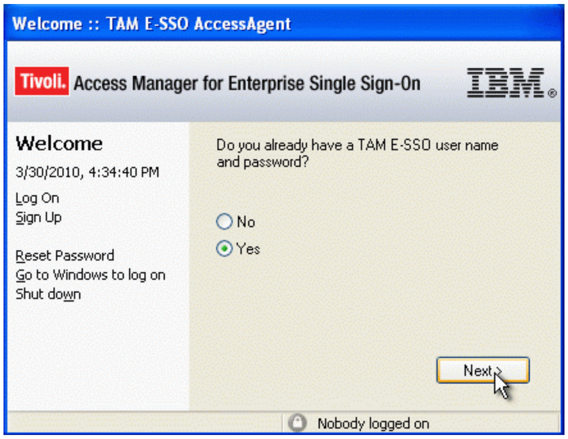
3. A prompt to register the smart card with the IMS Server appears. You can use the smart card with AccessAgent to log on, as shown in Figure 1-35. Then, click **Next**.



To log on to AccessAgent using your smart card, you need to register it with IMS Server. Click 'Next' to proceed.

*Figure 1-35 Logging on with AccessAgent*

4. When prompted, click **Yes** if you have already registered the user to use Tivoli Access Manager for Enterprise Single Sign-On, as shown in Figure 1-36. (Otherwise, click **No** and AccessAgent enrolls the user with the IMS Server.)

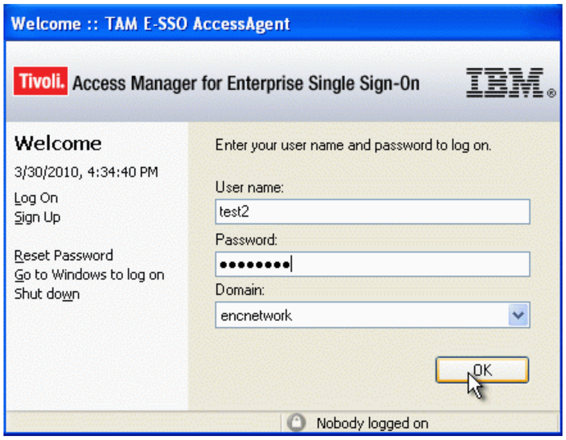


Do you already have a TAM E-SSO user name and password?

○ No
● Yes

*Figure 1-36 Registration to use Tivoli Access Manager for Enterprise Single Sign-On*

5. Enter the account details, as shown in Figure 1-37, and click **OK**.



Enter your user name and password to log on.

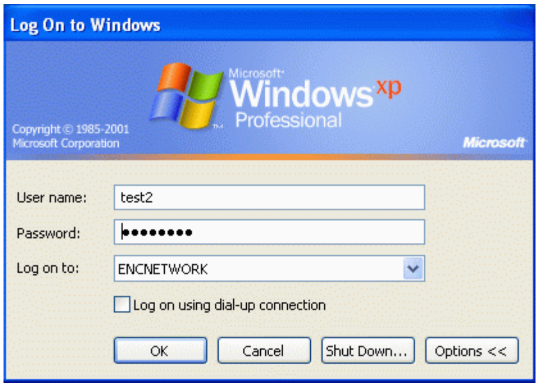
User name: test2

Password: ••••••••

Domain: encnetwork

*Figure 1-37 Entering account details*

The credentials are inserted automatically into the Windows system logon prompt, as shown in Figure 1-38.


Log On to Windows
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft

User name: test2

Password: ●●●●●●●●

Log on to: ENCNETWORK

□ Log on using dial-up connection

OK
Cancel
Shut Down...
Options <<

*Figure 1-38 Windows system logon credentials*

You are now logged on, and your registration for smart card use is complete. If you remove the smart card, you are required to present the smart card and to enter the PIN the next time that you log on with this account.

2

# Configuring authentication to use radio frequency identification cards

This chapter explains how to configure an existing Tivoli Access Manager for Enterprise Single Sign-On environment to use radio frequency identification (RFID) cards as additional authentication factors. It includes the following topics:

- "Prerequisite environment" on page 32
- "Creating and assigning the RFID machine policy template" on page 32
- "Creating an authentication code for the user" on page 35
- "Registering the RFID card to the user" on page 36

## 2.1 Prerequisite environment

To do this exercise, you need the following resources. Refer to the Tivoli Access Manager for Enterprise Single Sign-On product documentation for platform requirements and configuration instructions.

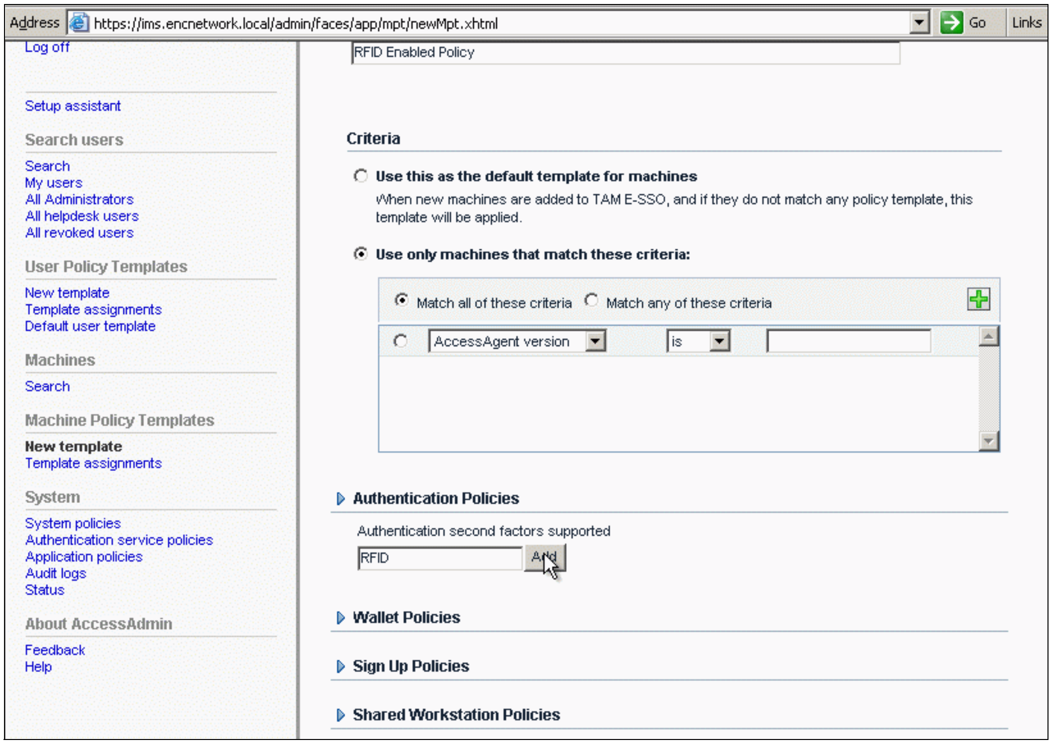
- Integrated Management System Server (IMS Server)
  - Microsoft Certificate Server
  - Internet Information Services
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 IMS+ prerequisites
    - WebSphere Application Server
    - IBM HTTP Server
    - A supported database (for example DB2)
  - Smart card middleware
- Client
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 AccessAgent
  - Smart card middleware
  - Initialized Smart Card and reader or USB token
  - Drivers for reader or token
  - RFID card with reader
  - Drivers for RFID reader

## 2.2 Creating and assigning the RFID machine policy template

To create and assign the RFID machine policy template, follow these steps:

1. Open a browser and enter the IMS Server location. From the IMS Server page, click **AccessAdmin**. Then, enter the login details for the Administrator for the IMS Server.
2. On the AccessAdmin page, under Machine Policy Templates, click **New Template**. Then, enter the following information, as shown in Figure 2-1 on page 33:
   - **Name**: Enter the name of the template. Assign a meaningful name.
   - **Criteria**: Specify the criteria if this template is for specific machines on the domain. Use the default option.
   - **Authentication Policies**: Enter **RFID**.

3. Click **Add**.



Address https://ims.encnetwork.local/admin/faces/app/mpt/newMpt.xhtml

RFID Enabled Policy

Criteria

○ Use this as the default template for machines
When new machines are added to TAM E-SSO, and if they do not match any policy template, this template will be applied.

● Use only machines that match these criteria:

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version | is |

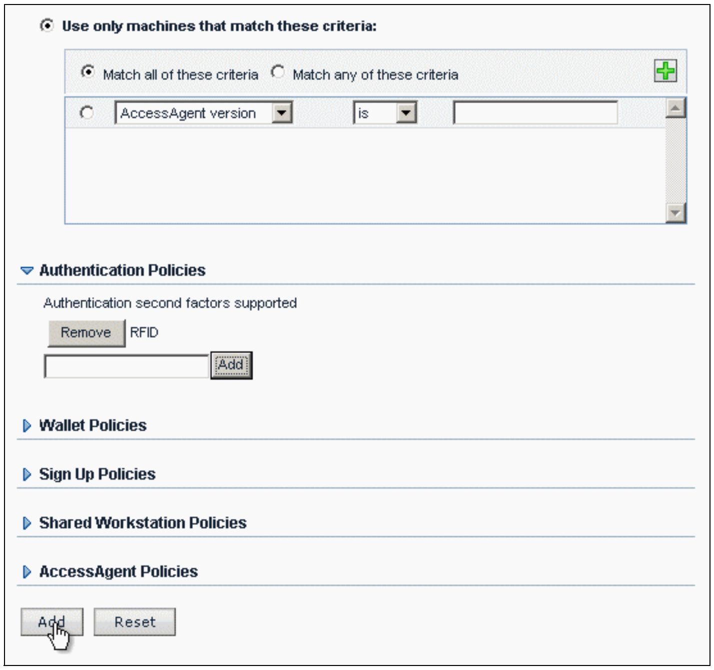
Authentication Policies

Authentication second factors supported

RFID

*Figure 2-1 Entering the new template information*

4. Add the policy template by again clicking **Add**, as shown in Figure 2-2.



● Use only machines that match these criteria:

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version | is |

Authentication Policies

Authentication second factors supported

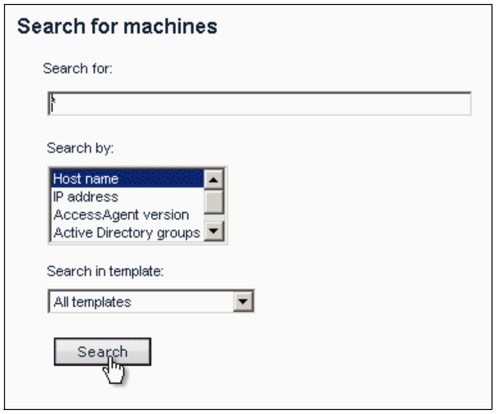
Remove RFID

*Figure 2-2 Adding the template*

5. Now, assign this new template to the client system that will be used when the user with the RFID badge logs on.

   Go to **Machines** → **Search** on the left pane. Enter an asterisk (*) in the “Search for” field and select Host name in the “Search by” drop-down. Make sure to select **All templates** in the “Search in template” drop-down list.

   Then, click **Search** to list the workstations that are connected to the IMS Server using AccessAgent, as shown in Figure Figure 2-3.



Search for machines

Search for: *

Search by: Host name

Search in template: All templates

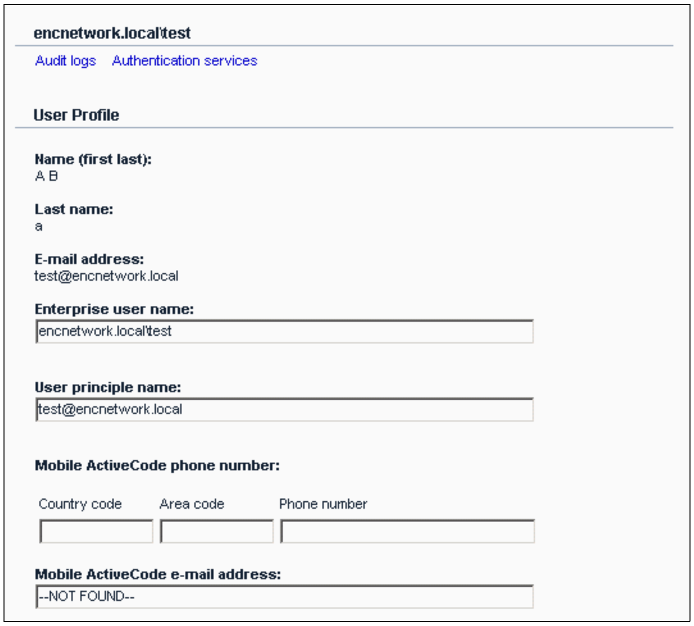
*Figure 2-3 Listing the workstations*

6. Select the workstation. Then, from the Machine Template Assignment list, select the RFID policy, and click **Assign**.

## 2.3 Creating an authentication code for the user

Follow these steps to create an authentication code to permit a user to log on with an RFID badge as an authentication factor:

1. In AccessAdmin, select **IMS Server** → **AccessAdmin** and locate the user you want to create an authentication code for (here, A B) as depicted in Figure 2-4.



**encnetwork.local\test**

**User Profile**

**Name (first last):**
A B

**Last name:**
a

**E-mail address:**
test@encnetwork.local

**Enterprise user name:**
encnetwork.local\test

**User principle name:**
test@encnetwork.local

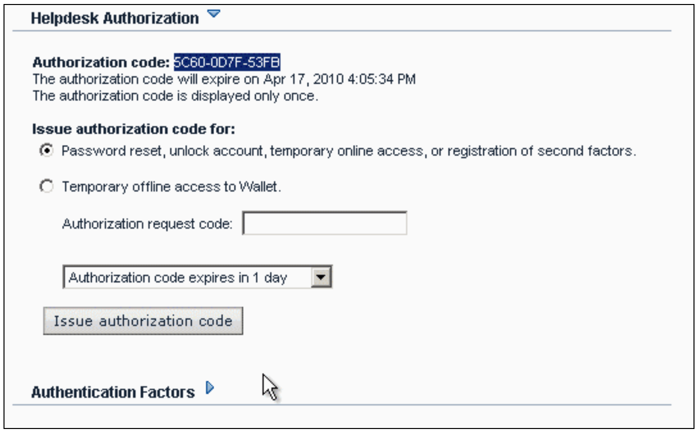
**Mobile ActiveCode phone number:**

| Country code | Area code | Phone number |
|---|---|---|
| | | |

**Mobile ActiveCode e-mail address:**
--NOT FOUND--

*Figure 2-4 Logging on to AccessAgent*

2. Scroll down to Helpdesk Authorization and select **Issue Authorization Code**. Note the code that is generated.



Helpdesk Authorization

**Authorization code:** 5C60-0D7F-53FB
The authorization code will expire on Apr 17, 2010 4:05:34 PM
The authorization code is displayed only once.

**Issue authorization code for:**

● Password reset, unlock account, temporary online access, or registration of second factors.

○ Temporary offline access to Wallet.

Authorization request code:

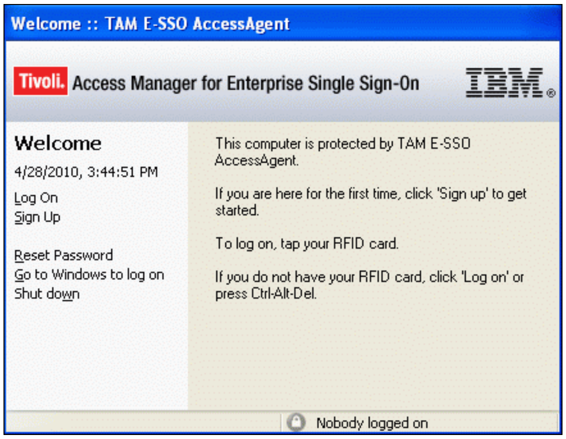
Authorization code expires in 1 day

*Figure 2-5 Issue an authorization code*

## 2.4 Registering the RFID card to the user

To register the RFID card to the user, follow these steps:

1. On the client system, tap your RFID card on the reader when prompted at the AccessAgent logon window. AccessAgent prompts you for the RFID card registration with the user account, as shown in Figure 2-6.



Welcome :: TAM E-SSO AccessAgent

Tivoli. Access Manager for Enterprise Single Sign-On IBM.

Welcome
4/28/2010, 3:44:51 PM

This computer is protected by TAM E-SSO AccessAgent.

If you are here for the first time, click 'Sign up' to get started.

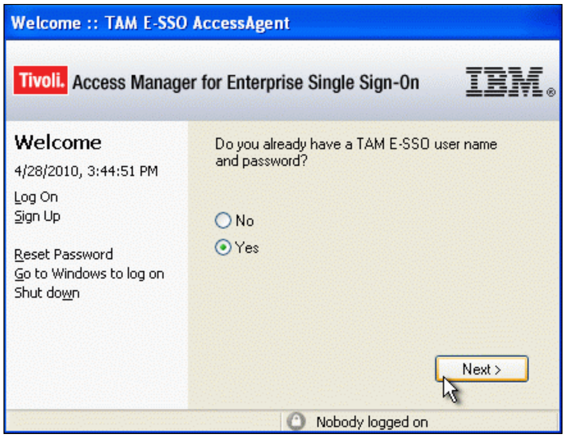
To log on, tap your RFID card.

If you do not have your RFID card, click 'Log on' or press Ctrl-Alt-Del.

Nobody logged on

*Figure 2-6 Prompt to tap RFID card*

2. When prompted, select **Yes** if the user is already registered with Tivoli Access Manager for Enterprise Single Sign-On. (Otherwise, select **No**, and AccessAgent enrolls the user. Then click **Next** as shown in Figure 2-7.



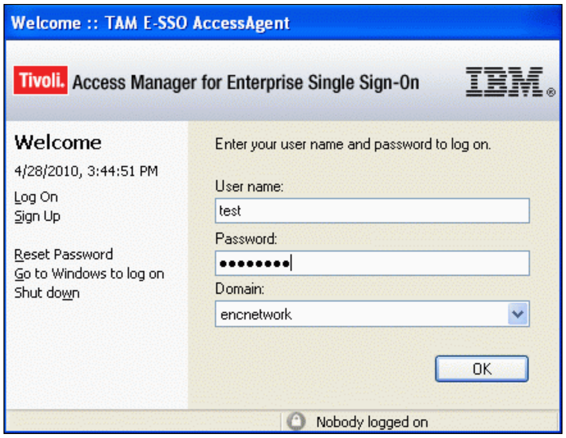
Do you already have a TAM E-SSO user name and password?

○ No

● Yes

*Figure 2-7 Register the RFID card*

3. Enter the account details for User name, Password, and Domain. Then click **OK** as shown in Figure 2-8.



Enter your user name and password to log on.

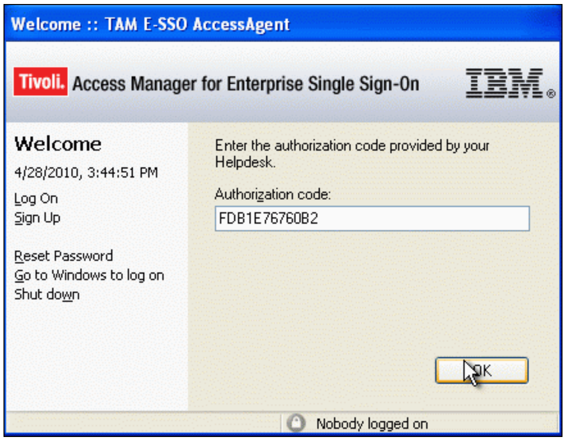
User name: test

Password: ••••••••

Domain: encnetwork

*Figure 2-8 RFID card logon*

4. As shown in Figure 2-9, enter the authorization code that was generated previously (as described in 2.3, “Creating an authentication code for the user” on page 35). The credentials are inserted automatically into the Windows system logon.



4/28/2010, 3:44:51 PM

Enter the authorization code provided by your Helpdesk.

Authorization code: FDB1E76760B2

*Figure 2-9 Entering authorization code*

You are now logged on, and registration for RFID card use is complete. When you log on again with this account, you are required to present the RFID card and enter the password.

# 3

# Configuring authentication to use fingerprint recognition

This chapter explains how to configure an existing Tivoli Access Manager for Enterprise Single Sign-On environment to enable the use of fingerprint readers for logging on to the AccessAgent.

> **Note:** You can use the instructions described in this chapter with supported Digital Persona or UPEK readers. For readers that work with Biokey Biometric Service Provider middleware, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Setup Guide, Version 8.1*, GC23-9692, and adapt these steps as appropriate.

This chapter includes the following topics:

## 3.1 Prerequisite environment

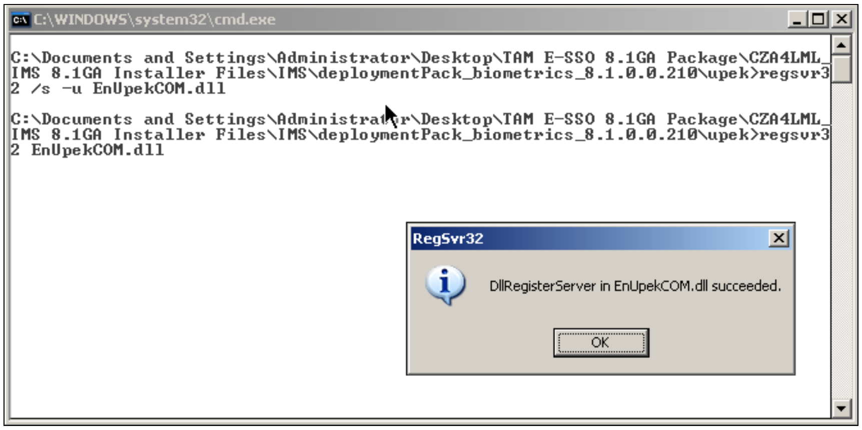
To do this exercise, you need the following resources. Refer to the Tivoli Access Manager for Enterprise Single Sign-On product documentation for platform requirements and configuration instructions.

- Integrated Management System Server (IMS Server)
  - Microsoft Certificate Server
  - Internet Information Services
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 IMS+ prerequisites
    - WebSphere Application Server
    - IBM HTTP Server
    - A supported database (for example DB2)
  - Smart card middleware
  - Drivers for fingerprint reader
- Client
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 AccessAgent
  - Smart card middleware
  - Initialized Smart Card and reader or USB token
  - Drivers for reader or token
  - Fingerprint reader
  - Drivers for fingerprint reader

## 3.2 Configuring the IMS Server

You must install the drivers for the fingerprint reader on both the IMS Server and the client systems before you can use fingerprint authentication. After the drivers are installed, open the `deploymentPack_biometrics_8.1.0.0.`*`xx`* directory from the installation CD, where *`xx`* is the version number.

This directory includes subdirectories. Open the appropriate directory for the reader, and run the relevant `En`*`reader`*`COM.bat` batch file. Refer to Figure 3-1.



```
C:\Documents and Settings\Administrator\Desktop\TAM E-SSO 8.1GA Package\CZA4LML_
IMS 8.1GA Installer Files\IMS\deploymentPack_biometrics_8.1.0.0.210\upek>regsvr3
2 /s -u EnUpekCOM.dll

C:\Documents and Settings\Administrator\Desktop\TAM E-SSO 8.1GA Package\CZA4LML_
IMS 8.1GA Installer Files\IMS\deploymentPack_biometrics_8.1.0.0.210\upek>regsvr3
2 EnUpekCOM.dll
```

DllRegisterServer in EnUpekCOM.dll succeeded.

*Figure 3-1 Configuring the IMS Server for fingerprint authentication*

After the batch file executes successfully, restart WebSphere Application Server, as shown in Figure 3-2.

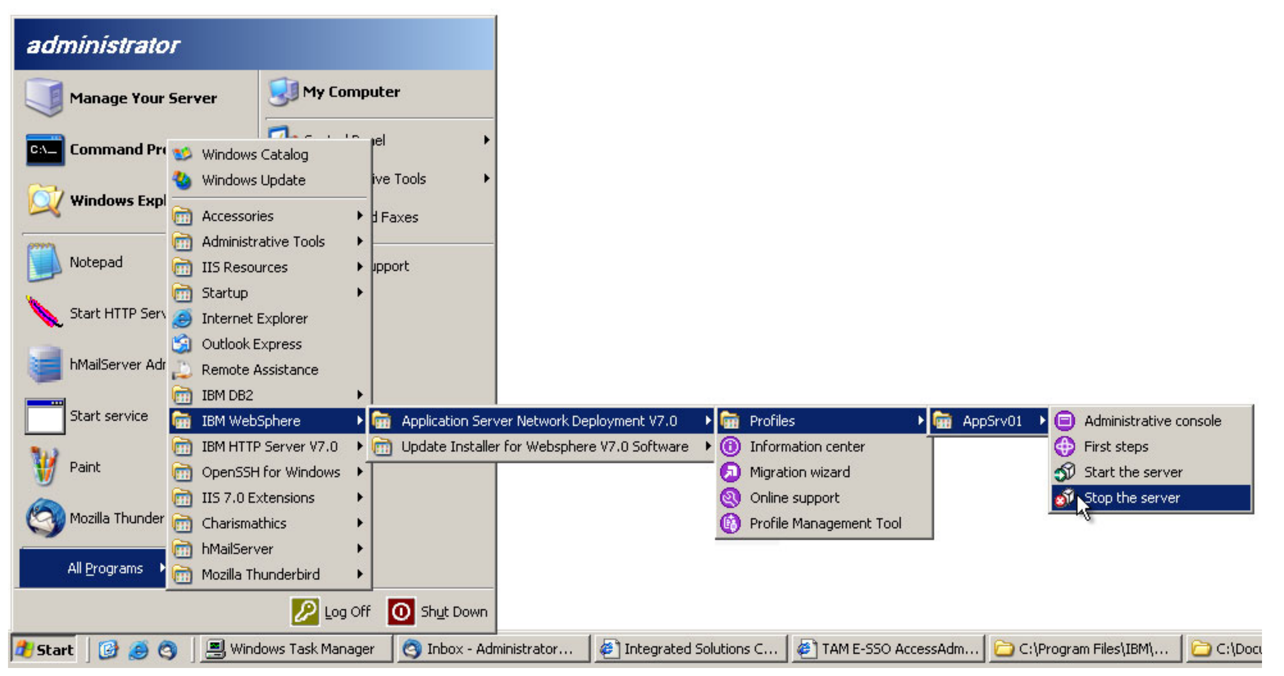


*Figure 3-2 Restarting WebSphere Application Server*

## 3.3 Creating and assigning fingerprint machine policy template

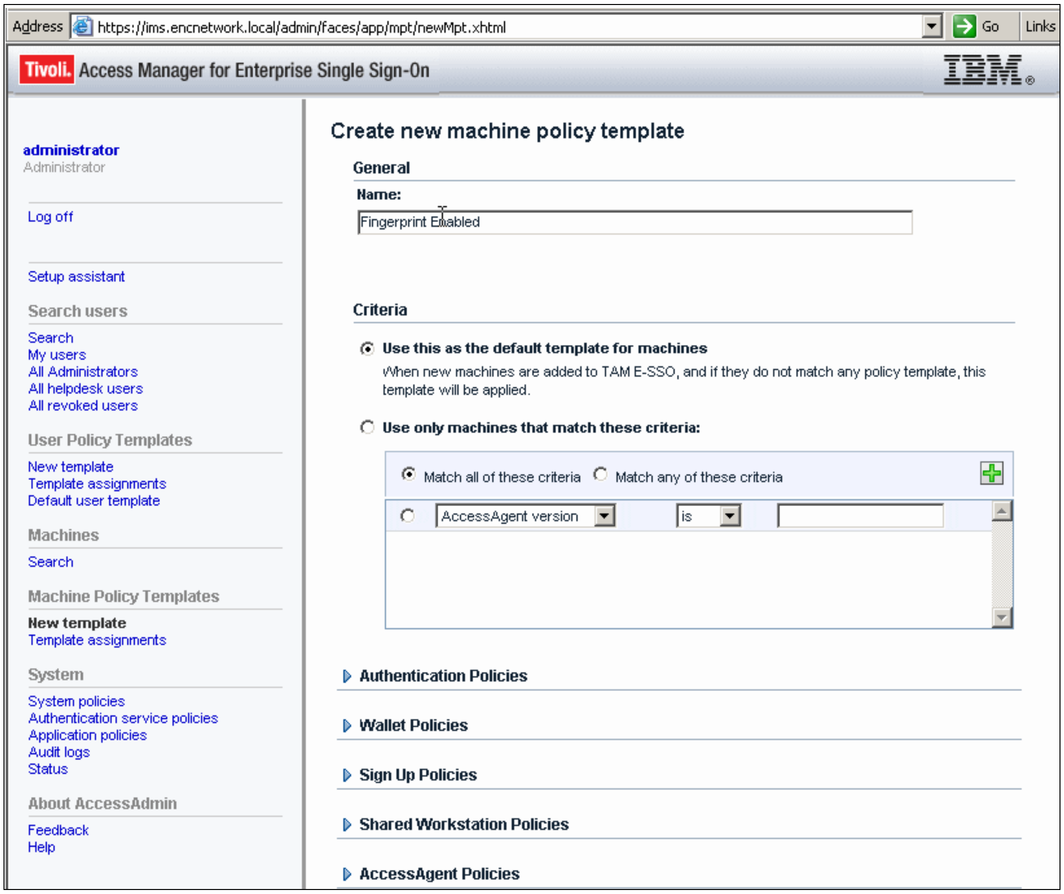
To create and assign a fingerprint machine policy template, follow these steps:

1. Open a browser and enter the IMS Server location. From the IMS Server page, click **AccessAdmin**.
2. Enter the login details for the Administrator for the IMS Server.

3. On the AccessAdmin page, under Machine Policy Templates, click **New Template**. Then, enter the following information, as shown in Figure 3-3:

   – **Name**: Enter the name of the template. Assign a meaningful name.

   – **Criteria**: Specify the criteria if this template is for specific systems on the domain. Use the default option.



Address https://ims.encnetwork.local/admin/faces/app/mpt/newMpt.xhtml

**administrator**
Administrator

Log off

Setup assistant

Search users
- Search
- My users
- All Administrators
- All helpdesk users
- All revoked users

User Policy Templates
- New template
- Template assignments
- Default user template

Machines
- Search

Machine Policy Templates
- **New template**
- Template assignments

System
- System policies
- Authentication service policies
- Application policies
- Audit logs
- Status

About AccessAdmin
- Feedback
- Help

Create new machine policy template

General

**Name:** Fingerprint Enabled

Criteria

● **Use this as the default template for machines**
When new machines are added to TAM E-SSO, and if they do not match any policy template, this template will be applied.

○ **Use only machines that match these criteria:**

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version | is |

▷ Authentication Policies

▷ Wallet Policies

▷ Sign Up Policies

▷ Shared Workstation Policies

▷ AccessAgent Policies

*Figure 3-3 Entering template information*

4. Under the Authentication Policies section, in the “Authentication second factor supported” option, enter `Fingerprint` and click **Add**, as shown in Figure 3-4.

> **Important:** Use the **Add** button. Do not press Return!

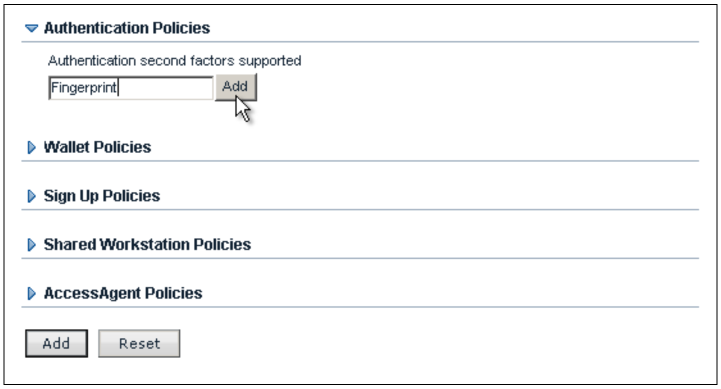


*Figure 3-4 Add fingerprint authentication policies*

5. Scroll down, and add the policy template by clicking **Add**, as shown in Figure 3-5.

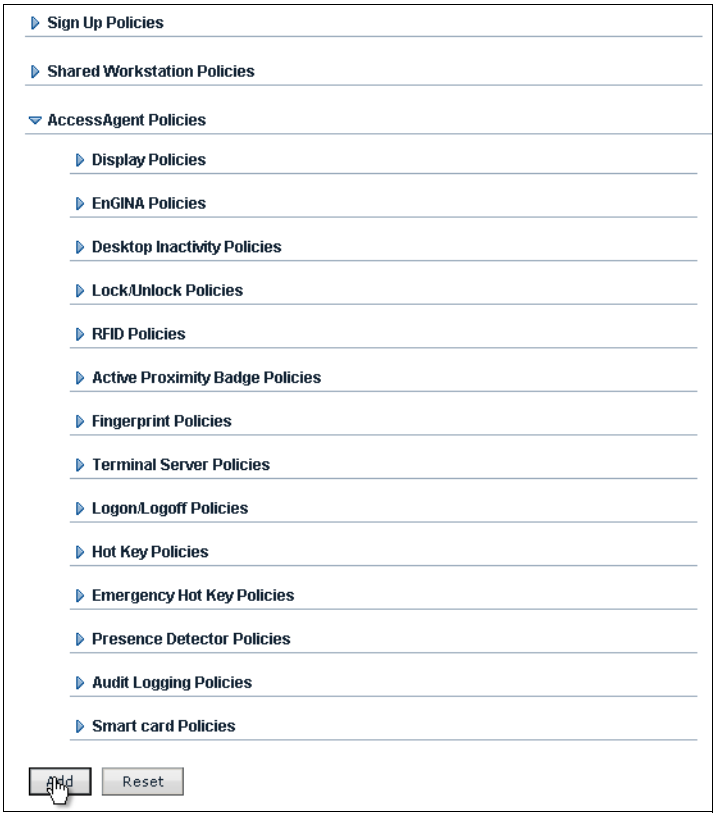
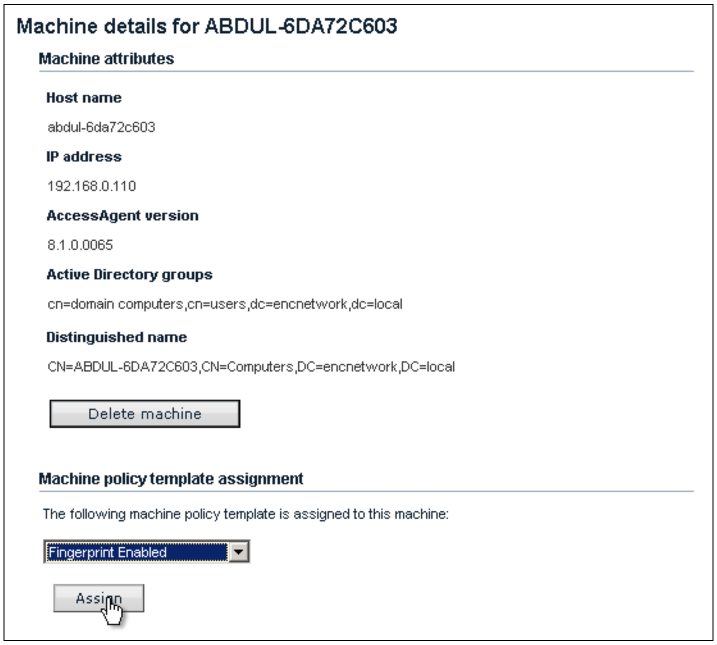


*Figure 3-5 Adding the policy template*

6. Next, assign this new template to the client system that will be used with fingerprint recognition. Go to **Machines** → **Search**, and click **Search** to list the workstations that are connected to the IMS Server. Select the workstation.
7. Then, from the “Machine policy template assignment” section, select the fingerprint policy from the drop-down, and click **Assign** as shown in Figure 3-6.



Machine details for ABDUL-6DA72C603

Machine attributes

Host name

abdul-6da72c603

IP address

192.168.0.110

AccessAgent version

8.1.0.0065

Active Directory groups

cn=domain computers,cn=users,dc=encnetwork,dc=local

Distinguished name

CN=ABDUL-6DA72C603,CN=Computers,DC=encnetwork,DC=local

Machine policy template assignment

The following machine policy template is assigned to this machine:

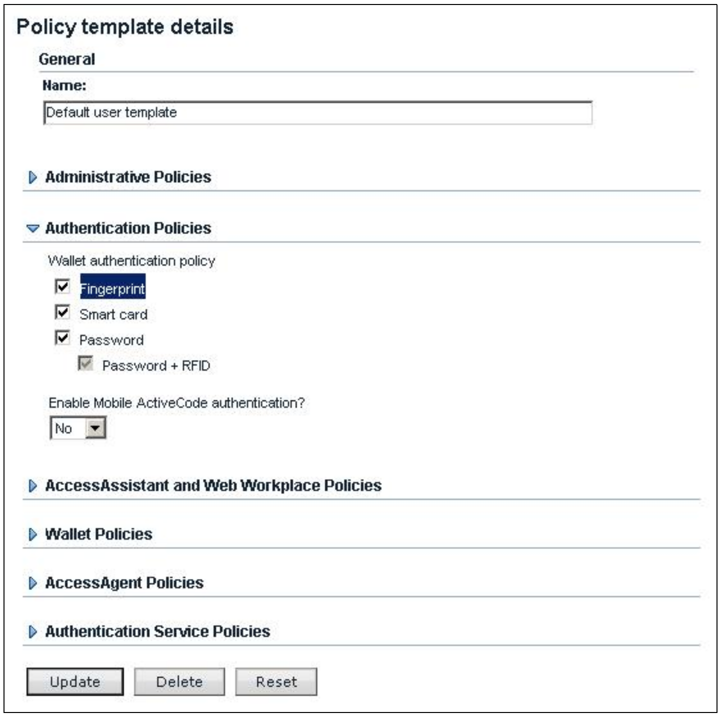
Fingerprint Enabled

*Figure 3-6 Assigning the policy template*

## 3.4 Updating the user template

Next, specify the user or users who can use fingerprint recognition for authentication:

1. Under the User Policy Template heading, click the **Default user template** link to display the details for the default user policy template.
2. Expand the Authentication Policies heading, and select **Fingerprint**, as shown in Figure 3-7. Then, click **Update** at the bottom of the policy template details.



Name: Default user template

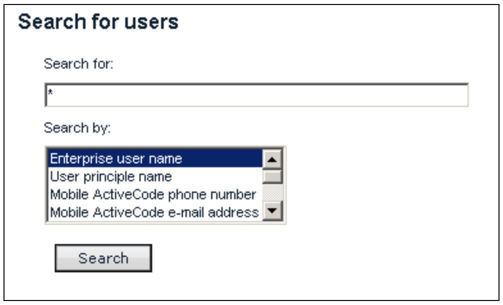
Wallet authentication policy

☑ Fingerprint
☑ Smart card
☑ Password
☑ Password + RFID

Enable Mobile ActiveCode authentication? No

*Figure 3-7 Updating the user template*

3. Click the **Search** button under the Search for Users heading. Then, click **Search**, as shown in Figure 3-8, to list the users who are registered on the IMS Server.

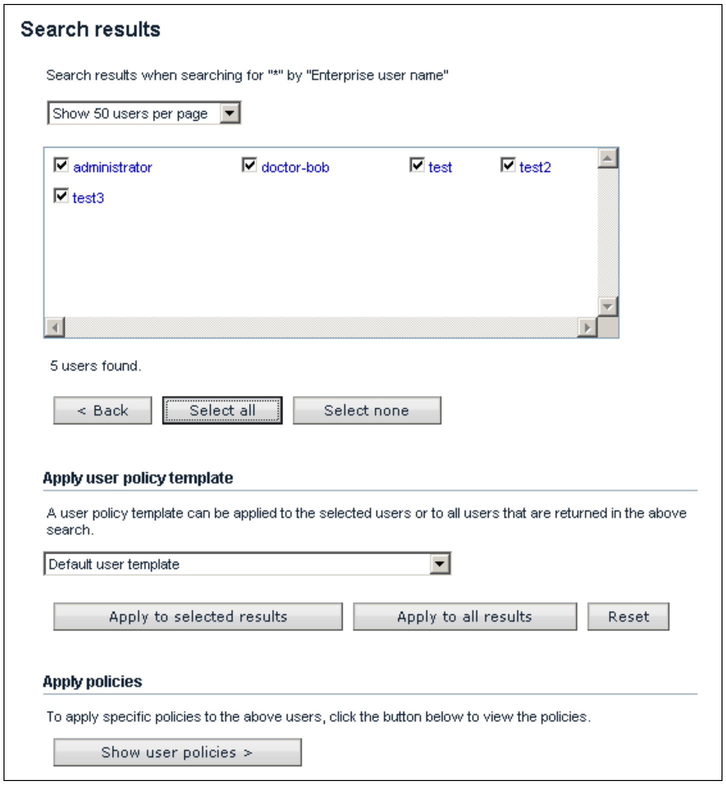

Search for users
Search
Enterprise user name
User principle name
Mobile ActiveCode phone number
Mobile ActiveCode e-mail address

Search for: *

Search by: Enterprise user name

*Figure 3-8 Searching for users*

4. Check the boxes next to the user or users who will use fingerprint authentication, as shown in Figure 3-9.



## Search results

Search results when searching for "*" by "Enterprise user name"

☑ administrator ☑ doctor-bob ☑ test ☑ test2
☑ test3

5 users found.

**Apply user policy template**

A user policy template can be applied to the selected users or to all users that are returned in the above search.

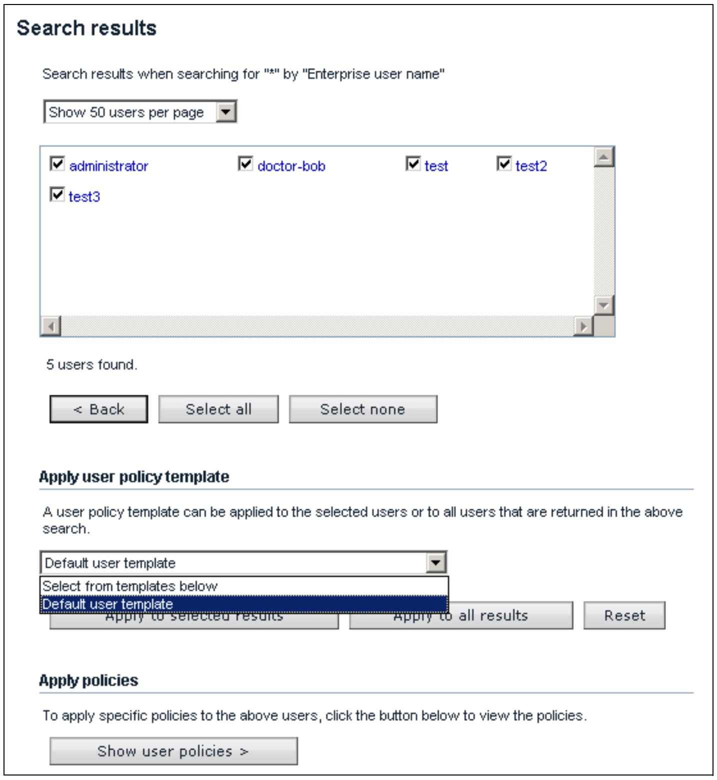
Default user template

**Apply policies**

To apply specific policies to the above users, click the button below to view the policies.

*Figure 3-9 Selecting the user or users*

5. In the “Apply user policy template” section, expand the drop-down menu, and select **Default user template**, as shown in Figure 3-10. Then, click **Apply to selected results**. When prompted to confirm your action, click **OK** to apply the default user template to the selected users.



Search results

Search results when searching for "*" by "Enterprise user name"

Show 50 users per page

☑ administrator ☑ doctor-bob ☑ test ☑ test2
☑ test3

5 users found.

Apply user policy template

A user policy template can be applied to the selected users or to all users that are returned in the above search.

Default user template

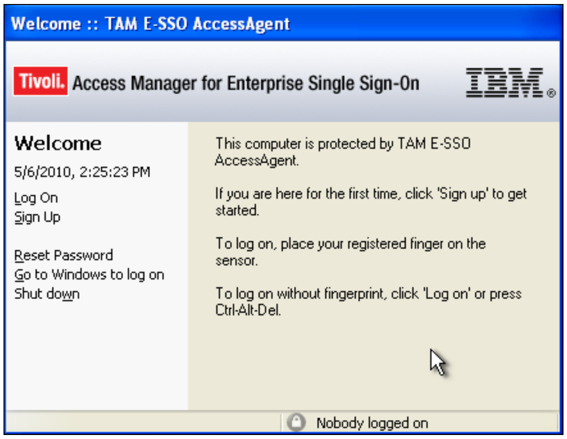
Select from templates below
Default user template

Apply policies

To apply specific policies to the above users, click the button below to view the policies.

*Figure 3-10 Selecting the default user template*

6. A progress bar displays. When the task completes, restart the client machine. The displayed message on the AccessAgent interface on the client workstation will now request a fingerprint to log on, as shown in Figure 3-11.



Welcome :: TAM E-SSO AccessAgent

Tivoli. Access Manager for Enterprise Single Sign-On IBM.

Welcome

5/6/2010, 2:25:23 PM

This computer is protected by TAM E-SSO AccessAgent.

If you are here for the first time, click 'Sign up' to get started.

To log on, place your registered finger on the sensor.

To log on without fingerprint, click 'Log on' or press Ctrl-Alt-Del.

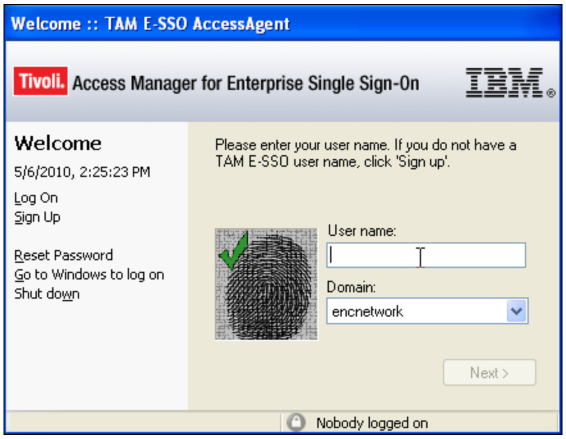
Nobody logged on

*Figure 3-11 Fingerprint requested to log on*

## 3.5 Enrolling the user's fingerprint for authentication

To enroll the user's fingerprint for authentication, follow these steps:

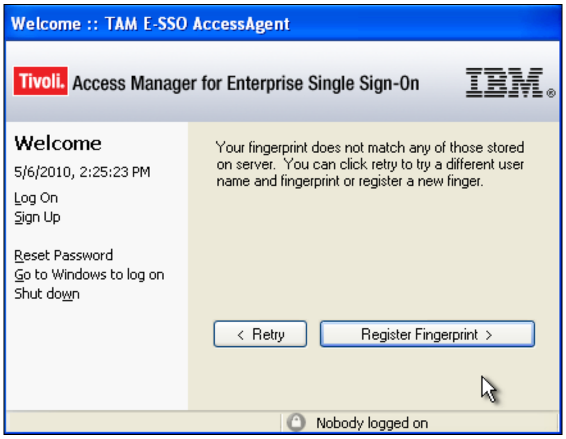
1. Have the user scan his or her finger by moving his or her fingertip across the reader. Enter the appropriate user name at the prompt, as shown in Figure 3-12. Click **Next**.



Please enter your user name. If you do not have a TAM E-SSO user name, click 'Sign up'.

*Figure 3-12 Entering the user name for fingerprint enrollment*

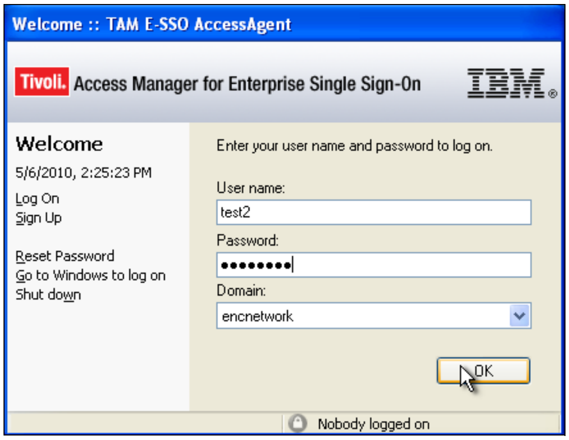
2. Select **Register Fingerprint**, as shown in Figure 3-13.



Your fingerprint does not match any of those stored on server. You can click retry to try a different user name and fingerprint or register a new finger.

*Figure 3-13 Registering fingerprint*

3. Enter the password that is associated with the account, and then click **OK**, as shown in Figure 3-14.



5/6/2010, 2:25:23 PM

Enter your user name and password to log on.

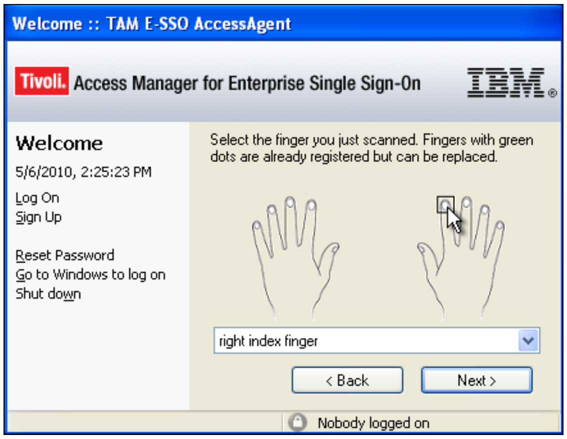
User name: test2

Password: ••••••••

Domain: encnetwork

*Figure 3-14 Enter password*

4. Identify the finger that you scanned from the drop-down, as shown in Figure 3-15.



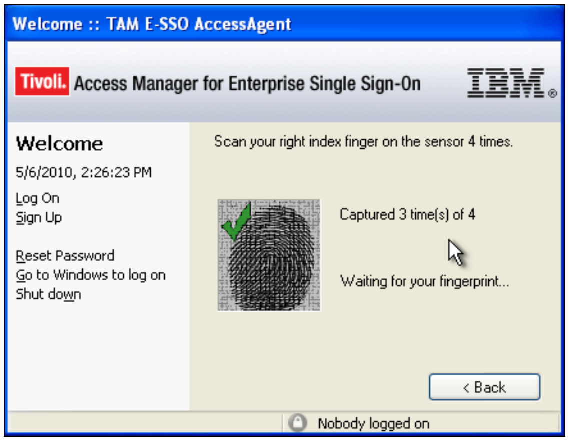
5/6/2010, 2:25:23 PM

Select the finger you just scanned. Fingers with green dots are already registered but can be replaced.

right index finger

*Figure 3-15 Identifying the scanned finger*

5. Scan the finger again as directed, as shown in Figure 3-16.



5/6/2010, 2:26:23 PM

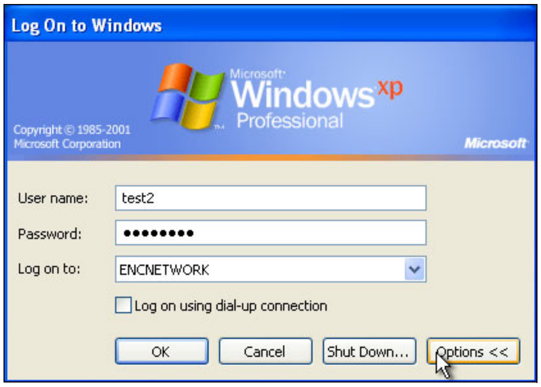
Scan your right index finger on the sensor 4 times.

Captured 3 time(s) of 4

Waiting for your fingerprint...

*Figure 3-16 Scanning user finger*

You are logged on to AccessAgent and to the Windows system, as shown in Figure 3-17. Registration is now complete. You need only to scan the finger that you registered to log on to your account again.



User name: test2

Password: ••••••••

Log on to: ENCNETWORK

□ Log on using dial-up connection

*Figure 3-17 User logged on to the Windows system*

4

# Configuring authentication to use Mobile ActiveCode as a one-time password

This chapter explains how to configure an existing Tivoli Access Manager for Enterprise Single Sign-On environment to use Mobile ActiveCode (MAC) as a one-time password (OTP) for non-AccessAgent authentication.

The authentication is done using AccessAssistant and Web Workplace. AccessAssistant and Web Workplace offer single sign-on without the requirement for an AccessAgent in scenarios where the enterprise applications are web-based. MACs are used to implement second factor authentication for AccessAssistant and Web Workplace.

> **Note:** The steps in this chapter show how to send the OTP using a mail server. If required, you can use short message service (SMS) messages instead of emails. You will need an SMS gateway and will need to adapt these instructions as appropriate.

This chapter includes the following topics:

## 4.1 Prerequisite environment

To do this exercise, you need the following resources. Refer to the Tivoli Access Manager for Enterprise Single Sign-On product documentation for platform requirements and configuration instructions.

- Integrated Management System Server (IMS Server)
  - Microsoft Certificate Server
  - Internet Information Services
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 IMS+ prerequisites
    - WebSphere Application Server
    - IBM HTTP Server
    - A supported database (for example DB2)
  - Smart card middleware
- Mail server
  - An email server and client

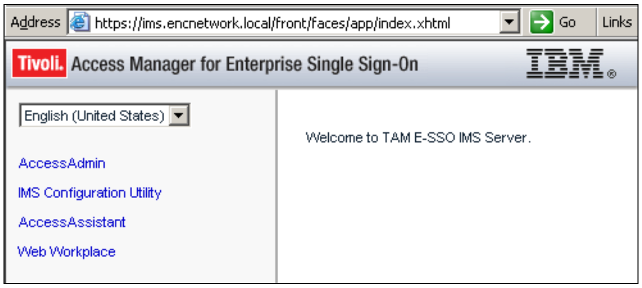
**Note:** The system must be enrolled in the Active Directory domain.

- Client
  - Tivoli Access Manager for Enterprise Single Sign-On 8.1 AccessAgent
  - Smart card middleware
  - Initialized Smart Card and reader or USB token
  - Drivers for reader or token
  - E-mail client

## 4.2 Creating the messaging connector for email

To create the messaging connector for email, follow these steps:

1. Navigate to the IMS Server, and click the **IMS Configuration Utility** link, as shown in Figure 4-1.



Address https://ims.encnetwork.local/front/faces/app/index.xhtml

Welcome to TAM E-SSO IMS Server.

Go
Links
Tivoli. Access Manager for Enterprise Single Sign-On
IBM
English (United States)
AccessAdmin
IMS Configuration Utility
AccessAssistant
Web Workplace

*Figure 4-1 Selecting the connector*

2. On the left menu, under “Advanced settings,” select **Message connectors** to display a drop-down menu on the right. Select **SMTP Messaging Connector** from the menu, as shown in Figure 4-2, and click **Configure**.

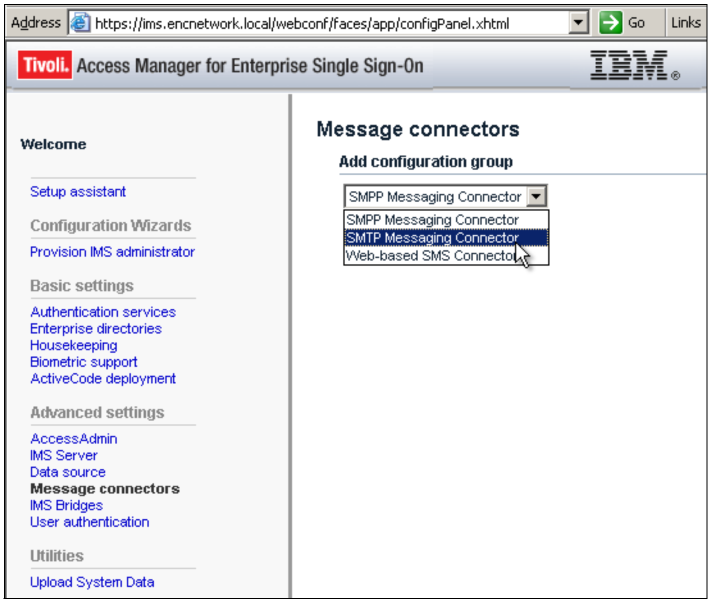
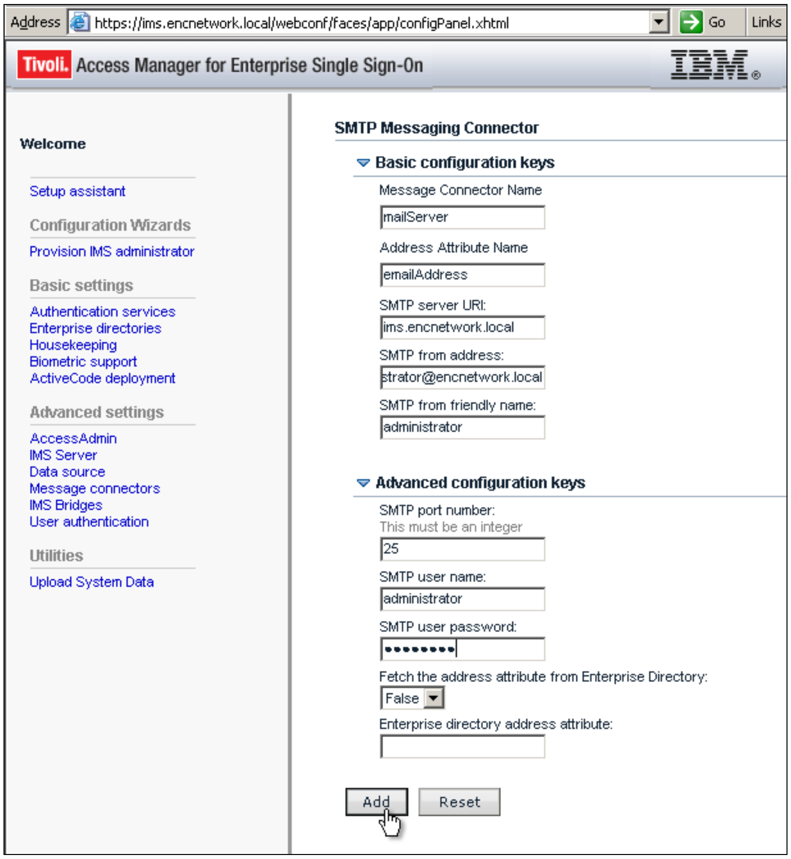


*Figure 4-2 SMTP Messaging Connector*

3. The SMTP messaging connector enables the delivery of MAC through email. Enter the following parameters, as shown in Figure 4-3:
   - **Message Connector Name**: A name of your choice (for example, `mailServer`)
   - **Address Attribute Name**: For example, `emailAddress`
   - **SMTP server URL**:For example, `mailServer.`*`domain name`*
   - **SMTP from address**: For example, `administrator@mailServer.`*`domain name`*
   - **SMTP form friendly name**: Enter a name of your choice (For example, `Admin`)
   - **SMTP port number**: `25`
   - **SMTP user name**: For example, `administrator@mailServer.`*`domain name`*
   - **SMTP user password**: Administrator password
4. After you enter these parameters, click **Add**. The new messaging connector appears.



SMTP Messaging Connector

Basic configuration keys

Message Connector Name: mailServer

Address Attribute Name: emailAddress

SMTP server URI: ims.encnetwork.local

SMTP from address: strator@encnetwork.local

SMTP from friendly name: administrator

Advanced configuration keys

SMTP port number: (This must be an integer) 25

SMTP user name: administrator

SMTP user password: ••••••••

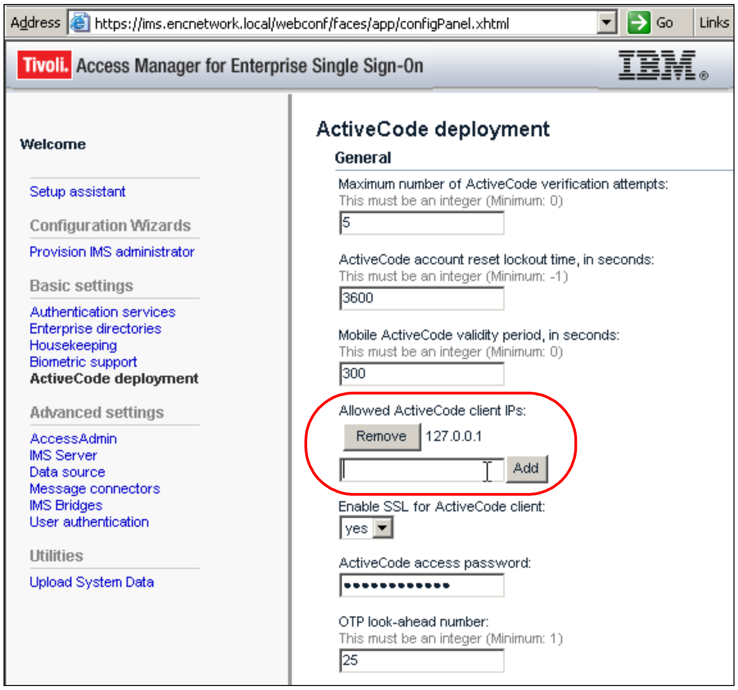
Fetch the address attribute from Enterprise Directory: False

Enterprise directory address attribute:

*Figure 4-3 Entering SMTP messaging connector parameters*

5. Click the **ActiveCode deployment** link. Then, to facilitate communication, add the IP addresses of the following systems under Allowed ActiveCode client IPs, as shown in Figure 4-4:

   – IMS Server
   – Client Machine
   – Mail Server



Address: https://ims.encnetwork.local/webconf/faces/app/configPanel.xhtml

ActiveCode deployment

General

Maximum number of ActiveCode verification attempts:
This must be an integer (Minimum: 0)
5

ActiveCode account reset lockout time, in seconds:
This must be an integer (Minimum: -1)
3600

Mobile ActiveCode validity period, in seconds:
This must be an integer (Minimum: 0)
300

Allowed ActiveCode client IPs:
127.0.0.1

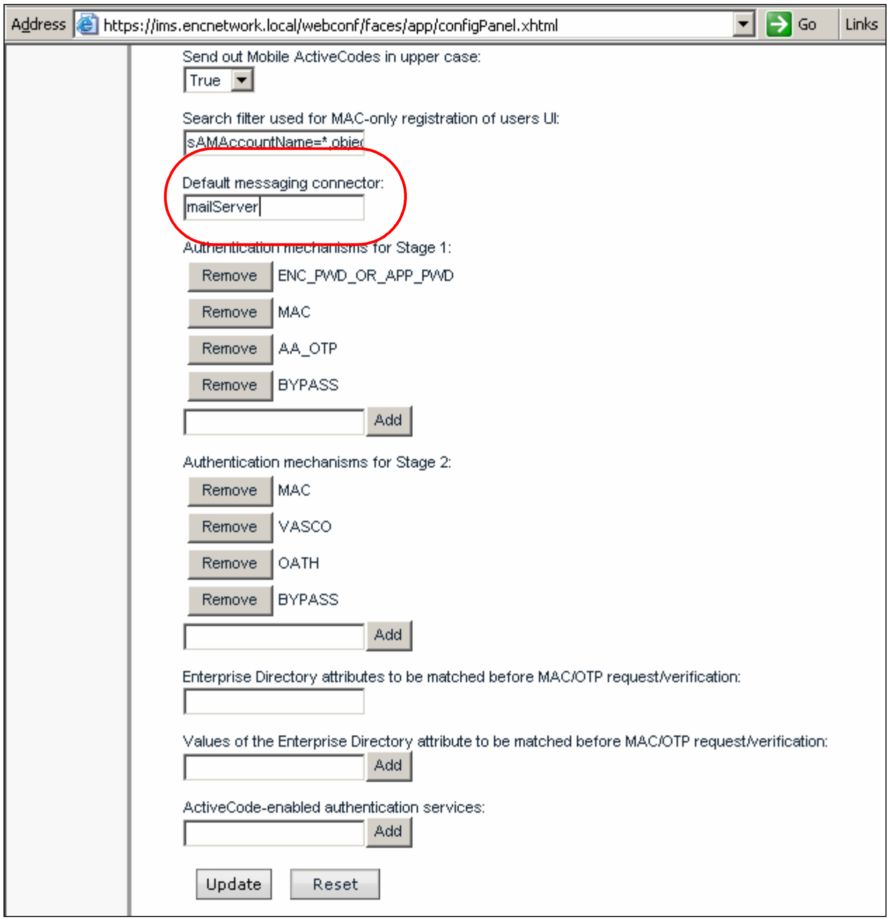
Enable SSL for ActiveCode client:
yes

ActiveCode access password:
••••••••••••

OTP look-ahead number:
This must be an integer (Minimum: 1)
25

*Figure 4-4 Adding ActiveCode client IPs*

6. Scroll down and enter the name of your SMTP messaging connector in the Default Messaging Connector parameter. Then, scroll to the bottom of the page, and click **Update**, as shown in Figure 4-5.



Address https://ims.encnetwork.local/webconf/faces/app/configPanel.xhtml

Send out Mobile ActiveCodes in upper case:
True

Search filter used for MAC-only registration of users UI:
sAMAccountName=*,objec

Default messaging connector:
mailServer

Authentication mechanisms for Stage 1:
ENC_PWD_OR_APP_PWD
MAC
AA_OTP
BYPASS

Authentication mechanisms for Stage 2:
MAC
VASCO
OATH
BYPASS

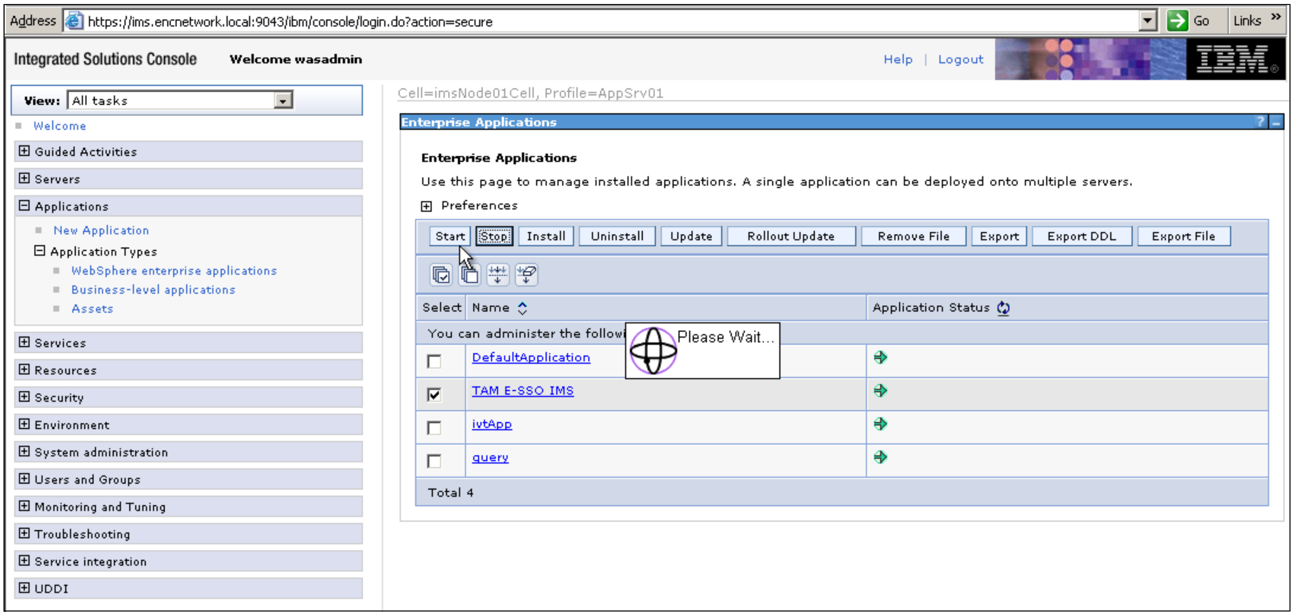
Enterprise Directory attributes to be matched before MAC/OTP request/verification:

Values of the Enterprise Directory attribute to be matched before MAC/OTP request/verification:

ActiveCode-enabled authentication services:

Figure 4-5 Setting default messaging connector

7. Restart the IMS Server from the WebSphere Application Server Administrative Console by clicking **Stop** and then **Start**, as shown in Figure 4-6.



**Enterprise Applications**

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

⊞ Preferences

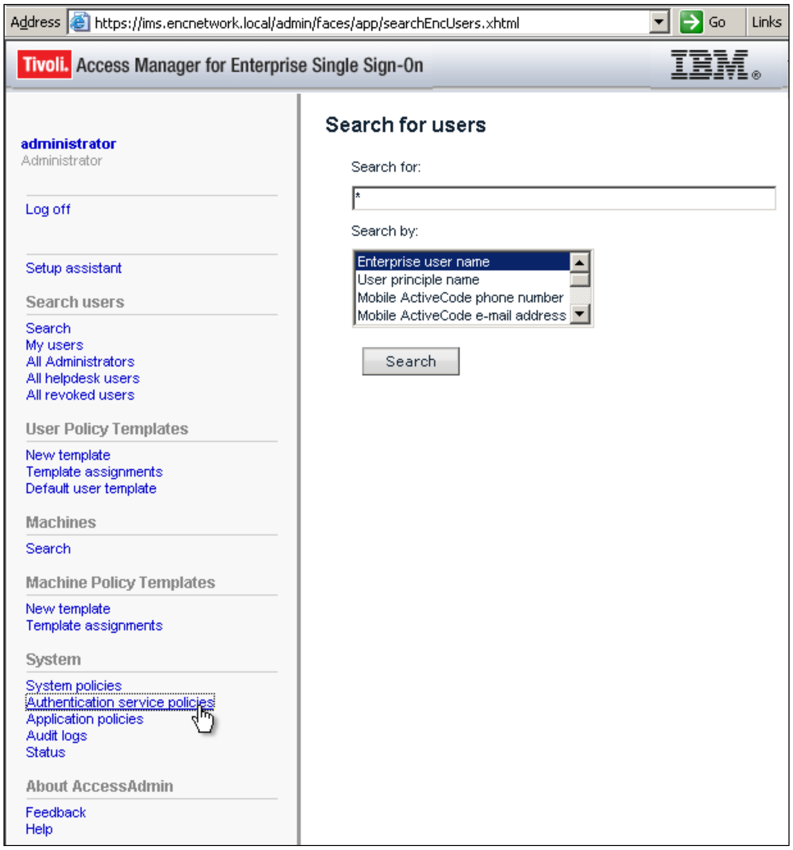
| Select | Name | Application Status |
|---|---|---|
| You can administer the followi | | |
| □ | DefaultApplication | ➔ |
| ☑ | TAM E-SSO IMS | ➔ |
| □ | ivtApp | ➔ |
| □ | query | ➔ |
| Total 4 | | |

*Figure 4-6 Restarting WebSphere Application Server*

## 4.3 Configuring the AccessAssistant to use MAC as second factor authentication

To configure the AccessAssistant to use MAC as a second factor authentication, follow these steps:

1. Navigate to the AccessAdmin page within the IMS Server. On the left menu under the System heading, click the **Authentication service policies** link to list the applications, as shown in Figure 4-7.



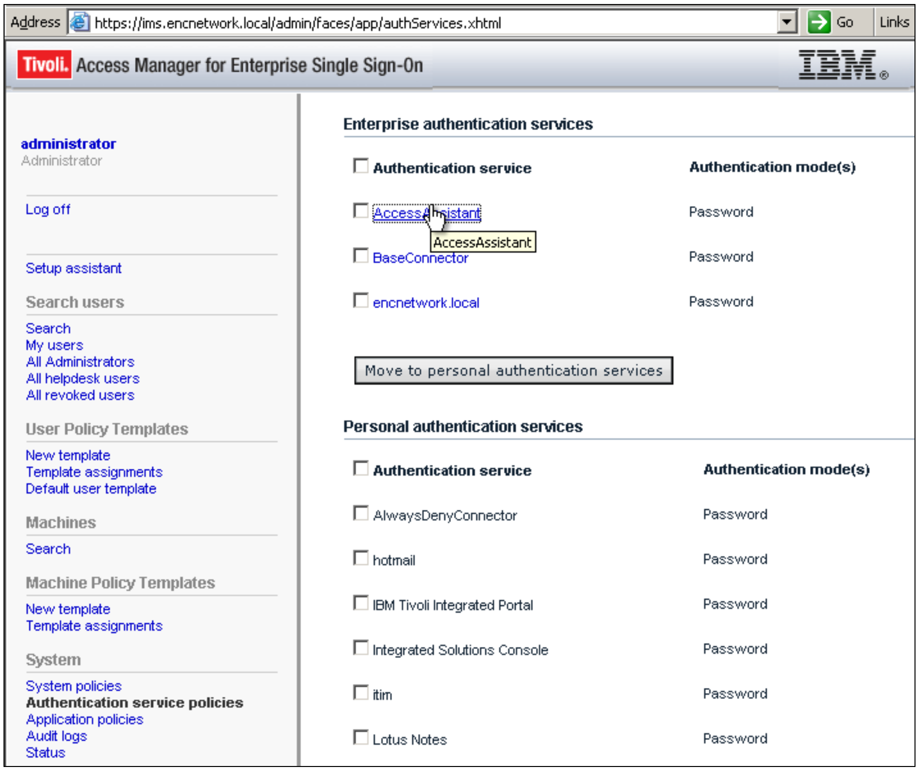
Address: https://ims.encnetwork.local/admin/faces/app/searchEncUsers.xhtml

Search for: *

Search by: Enterprise user name

*Figure 4-7 Selecting AccessAssistant*

2. In the “Personal authentication services” list, select **AccessAssistant** and scroll to the bottom of the page. Click the button **Move to enterprise authentication services**.
3. Now, under the “Enterprise authentication services list,” click the **AccessAssistant** link, as shown in Figure 4-8.



https://ims.encnetwork.local/admin/faces/app/authServices.xhtml

Enterprise authentication services

| □ Authentication service | Authentication mode(s) |
|---|---|
| □ AccessAssistant | Password |
| □ BaseConnector | Password |
| □ encnetwork.local | Password |

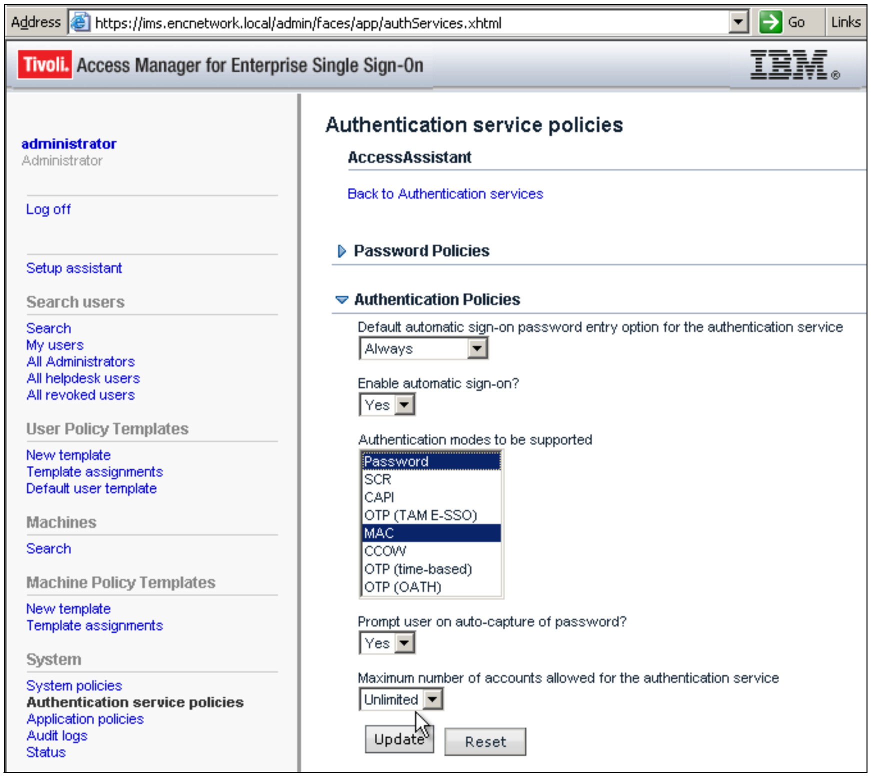
Personal authentication services

| □ Authentication service | Authentication mode(s) |
|---|---|
| □ AlwaysDenyConnector | Password |
| □ hotmail | Password |
| □ IBM Tivoli Integrated Portal | Password |
| □ Integrated Solutions Console | Password |
| □ itim | Password |
| □ Lotus Notes | Password |

*Figure 4-8 Selecting AccessAssistant*

4. The “AccessAssistant Authentication service policies” panel appears. Expand the Authentication Policies menu.

5. In the “Authentication modes to be supported” list, select **Password** and **MAC**, as shown in Figure 4-9. Use the Ctrl key for multiple selections. Then, click **Update**.



Address https://ims.encnetwork.local/admin/faces/app/authServices.xhtml

Tivoli. Access Manager for Enterprise Single Sign-On

Authentication service policies

AccessAssistant

Password Policies

Authentication Policies

Default automatic sign-on password entry option for the authentication service: Always

Enable automatic sign-on?: Yes

Authentication modes to be supported:
- Password (selected)
- SCR
- CAPI
- OTP (TAM E-SSO)
- MAC (selected)
- CCOW
- OTP (time-based)
- OTP (OATH)

Prompt user on auto-capture of password?: Yes

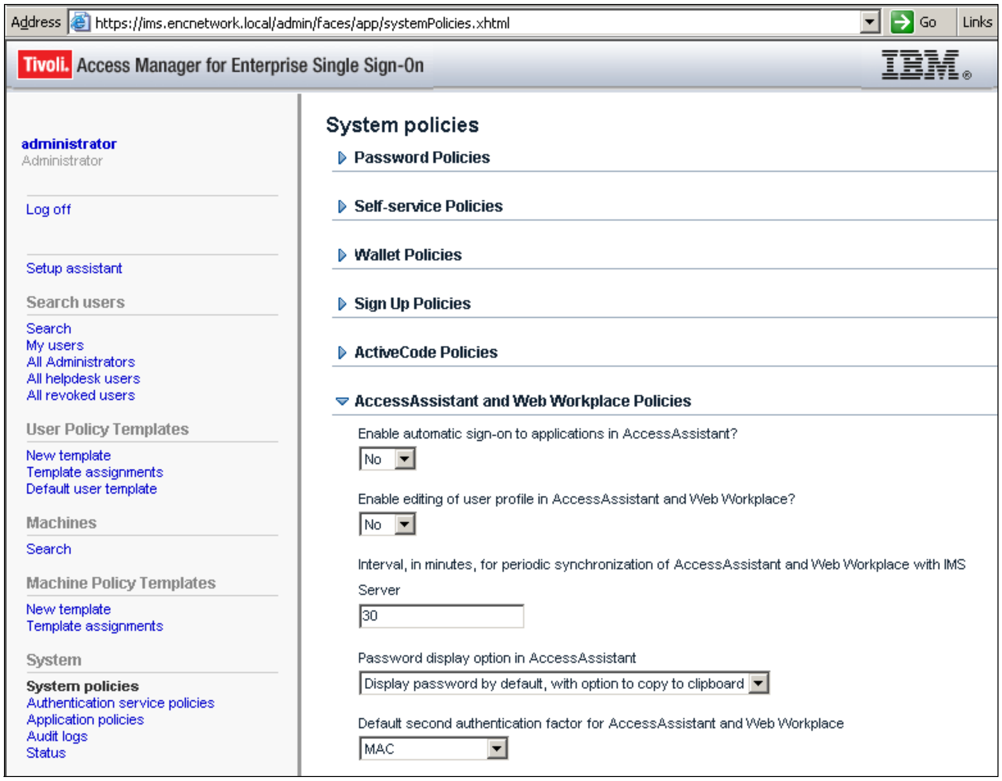
Maximum number of accounts allowed for the authentication service: Unlimited

*Figure 4-9 Selecting MAC and password*

6. After you update the information, click the **Back to Authentication Services** link, and move AccessAssistant back to the “Personal authentication service” list by selecting **AccessAssistant** and clicking **Move to Personal authentication service**.

7. Click the **System policies** link under the System heading in the left pane to display a list of expandable menus. Then, expand the **AccessAssistant and Web Workplace Policies** menu.

8. Select **MAC** from the drop-down list under the “Default second authentication factor for AccessAssistant and Web Workplace” option, as shown in Figure 4-10. Then, scroll down to the end of the page and click **Update**.



https://ims.encnetwork.local/admin/faces/app/systemPolicies.xhtml

System policies

Enable automatic sign-on to applications in AccessAssistant?
No

Enable editing of user profile in AccessAssistant and Web Workplace?
No

Interval, in minutes, for periodic synchronization of AccessAssistant and Web Workplace with IMS Server
30

Password display option in AccessAssistant
Display password by default, with option to copy to clipboard

Default second authentication factor for AccessAssistant and Web Workplace
MAC

*Figure 4-10 System policies*

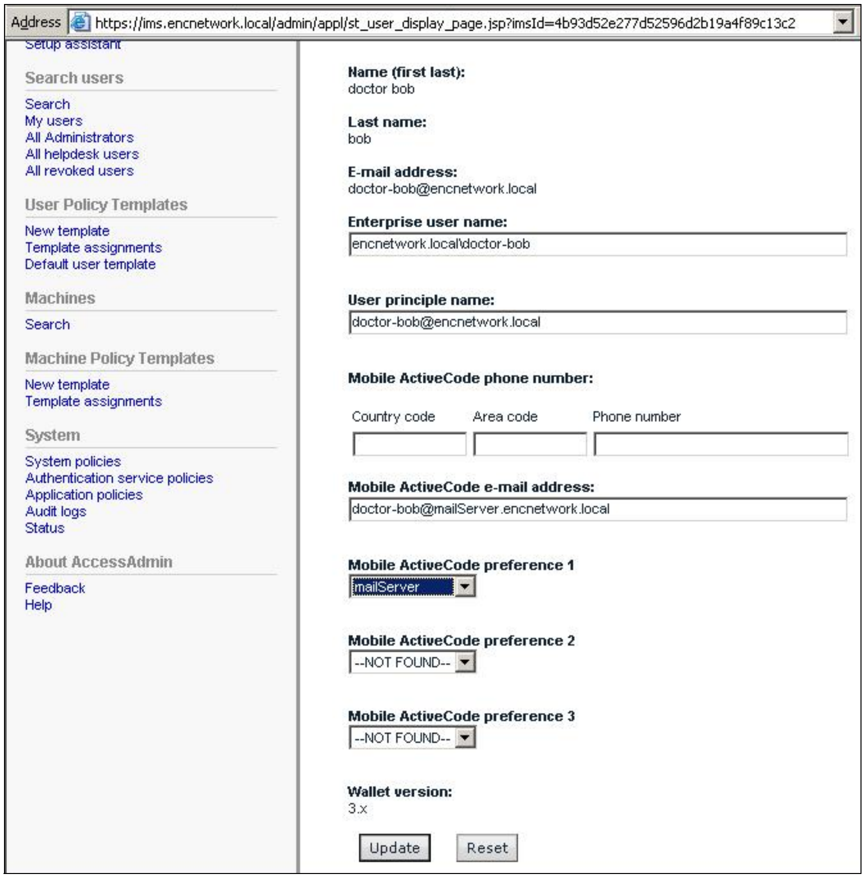
## 4.4 Configuring the user account for MAC use

To configure the user account for MAC use, follow these steps:

1. Navigate to AccessAdmin, search for users, and then select the user account for which you want to set up MAC authentication. Enter the following information, as shown in Figure 4-11:

   – **Mobile ActiveCode email address:** Enter the user's email address to which the MAC will be sent.

   – **Preference:** Enter the name of the of the message connector that you created previously (for example, `mailServer`).



https://ims.encnetwork.local/admin/appl/st_user_display_page.jsp?imsId=4b93d52e277d52596d2b19a4f89c13c2

**Name (first last):**
doctor bob

**Last name:**
bob

**E-mail address:**
doctor-bob@encnetwork.local

**Enterprise user name:**
encnetwork.local\doctor-bob

**User principle name:**
doctor-bob@encnetwork.local

**Mobile ActiveCode phone number:**

Country code | Area code | Phone number

**Mobile ActiveCode e-mail address:**
doctor-bob@mailServer.encnetwork.local

**Mobile ActiveCode preference 1**
mailServer

**Mobile ActiveCode preference 2**
--NOT FOUND--

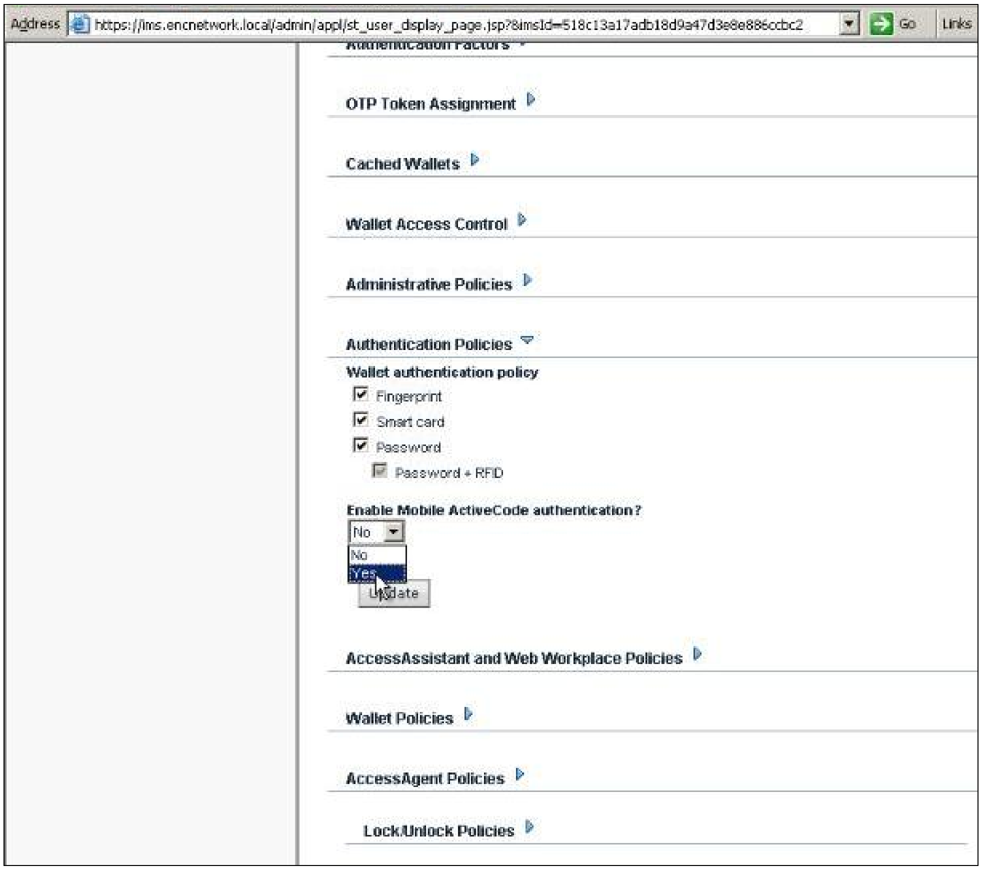
**Mobile ActiveCode preference 3**
--NOT FOUND--

**Wallet version:**
3.x

*Figure 4-11 Entering account information*

2. Then, click the **Update** button.

3. Scroll down to “Authentication Policies” and enable Mobile ActiveCode Authentication, as shown in Figure 4-12, by selecting **Yes** from the drop-down



Address https://ims.encnetwork.local/admin/appl/st_user_display_page.jsp?&imsId=518c13a17adb18d9a47d3e8e886ccbc2

Authentication Factors

OTP Token Assignment

Cached Wallets

Wallet Access Control

Administrative Policies

Authentication Policies

Wallet authentication policy

☑ Fingerprint

☑ Smart card

☑ Password

☑ Password + RFID

Enable Mobile ActiveCode authentication?

No

AccessAssistant and Web Workplace Policies

Wallet Policies

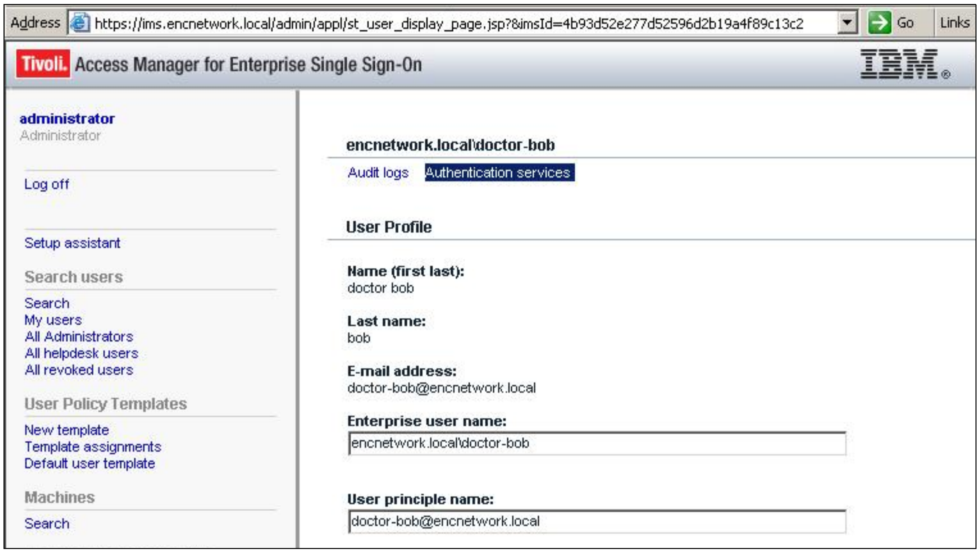
AccessAgent Policies

Lock/Unlock Policies

*Figure 4-12 Enabling Mobile ActiveCode authentication*

4. Click **Update**.

5. Now scroll up, and select **Authentication Services**, as shown in Figure 4-13.



https://ims.encnetwork.local/admin/appl/st_user_display_page.jsp?&imsId=4b93d52e277d52596d2b19a4f89c13c2

encnetwork.local\doctor-bob

User Profile

Name (first last):
doctor bob

Last name:
bob

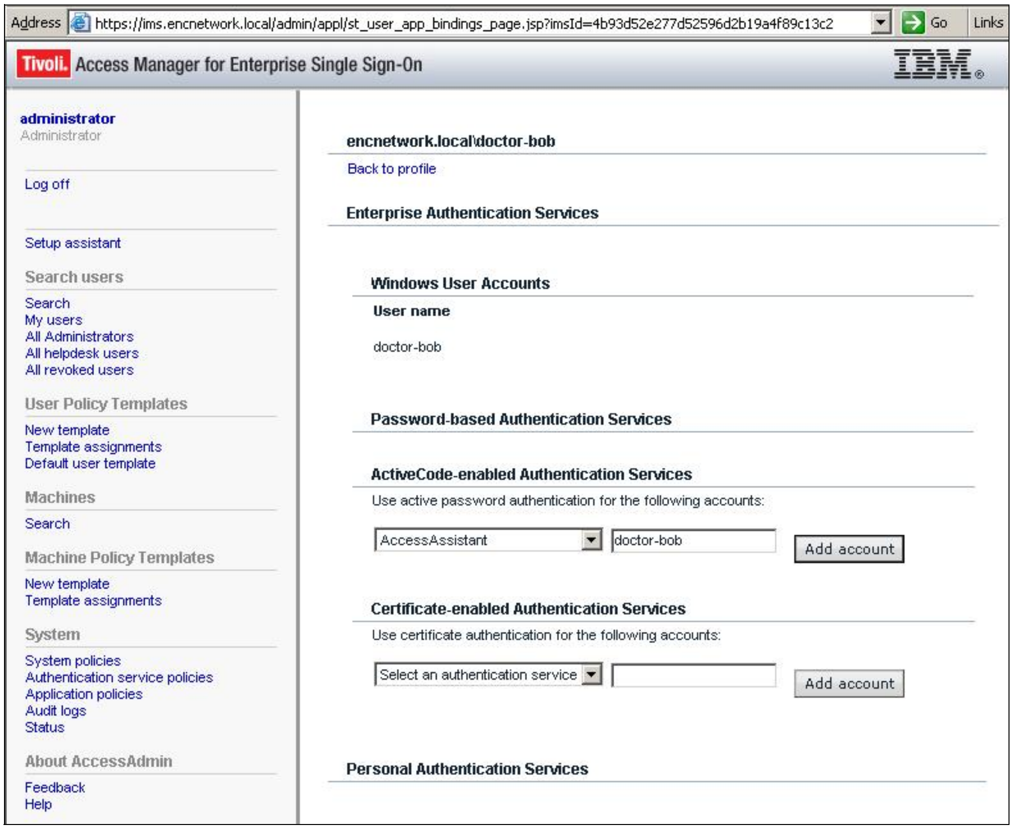
E-mail address:
doctor-bob@encnetwork.local

Enterprise user name:
encnetwork.local\doctor-bob

User principle name:
doctor-bob@encnetwork.local

*Figure 4-13 Authentication Services*

6. Under ActiveCode-enabled Authentication Services, select the **AccessAssistant** authentication service from the drop-down, and enter the account name to which this service is to be applied (in this case, "doctor-bob.") Then, click **Add account** as shown in Figure 4-14.



https://ims.encnetwork.local/admin/appl/st_user_app_bindings_page.jsp?imsId=4b93d52e277d52596d2b19a4f89c13c2

encnetwork.local\doctor-bob

Enterprise Authentication Services

Windows User Accounts

User name

doctor-bob

Password-based Authentication Services

ActiveCode-enabled Authentication Services

Use active password authentication for the following accounts:

AccessAssistant ▼ doctor-bob

Certificate-enabled Authentication Services

Use certificate authentication for the following accounts:

Select an authentication service ▼

Personal Authentication Services

*Figure 4-14 ActiveCode-enabled authentication services*

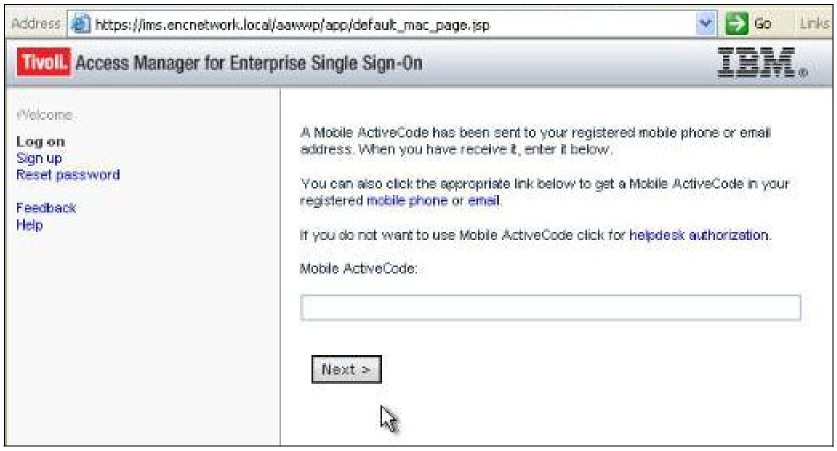
## 4.5 Logging on with MAC

To log on with MAC:

1. Log on to the Windows system with the user account that was configured to use MAC authentication.
2. Open a browser to access the Web Workplace using the following URL:

   *ims_server_domain_name*/aawwp

   If you receive a message about choosing a digital certificate, cancel it.
3. Enter the account details for the user. You are then be prompted for a MAC, as shown in Figure 4-15.



Address https://ims.encnetwork.local/aawwp/app/default_mac_page.jsp
Go
Links
Tivoli. Access Manager for Enterprise Single Sign-On
IBM.
Welcome
Log on
Sign up
Reset password
Feedback
Help
Next >

A Mobile ActiveCode has been sent to your registered mobile phone or email address. When you have receive it, enter it below.

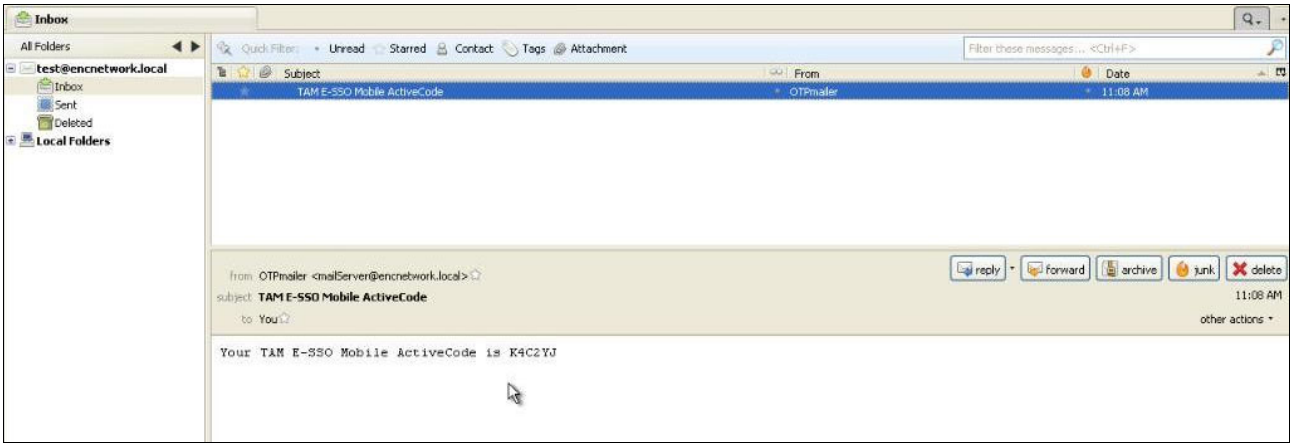
You can also click the appropriate link below to get a Mobile ActiveCode in your registered mobile phone or email.

If you do not want to use Mobile ActiveCode click for helpdesk authorization.

Mobile ActiveCode:

*Figure 4-15 MAC prompt*

4. Do not close this window! To find the MAC, go to the email client, and read the relevant email, as depicted in Figure 4-16.



| Subject | From | Date |
|---|---|---|
| TAM E-SSO Mobile ActiveCode | OTPmailer | 11:08 AM |

from OTPmailer <mailServer@encnetwork.local>

subject TAM E-SSO Mobile ActiveCode

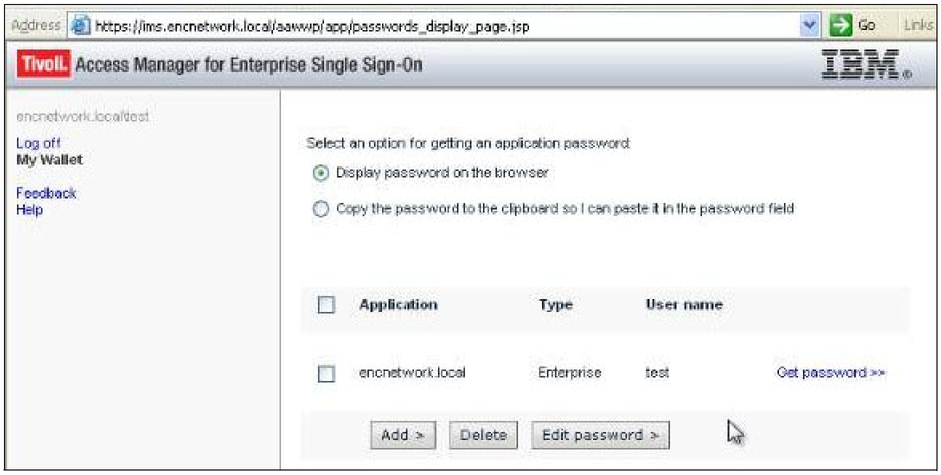
to You

11:08 AM

```
Your TAM E-SSO Mobile ActiveCode is K4C2YJ
```

*Figure 4-16 Obtaining Mobile ActiveCode*

5. Enter the MAC into the prompt. You are presented with AccessAssistant and can view your passwords, as shown in Figure 4-17.


Address
https://ims.encnetwork.local/aawwp/app/passwords_display_page.jsp
Go
Links
Tivoli. Access Manager for Enterprise Single Sign-On
IBM
Log off
My Wallet
Feedback
Help
Add >
Delete
Edit password >

encnetwork.local\test

Select an option for getting an application password

● Display password on the browser

○ Copy the password to the clipboard so I can paste it in the password field

| □ | Application | Type | User name | |
|---|---|---|---|---|
| □ | encnetwork.local | Enterprise | test | Get password >> |

*Figure 4-17 Obtain passwords*

## 4.6 Conclusion

In this Redpaper, we have shown how to configure and use the following authentication factors with Tivoli Access Manager for Enterprise Single Sign-On, for enhanced security:

- Smart Cards
- RFID Cards
- Fingerprint Readers
- Mobile ActiveCodes (a form of one-time password)

# Related publications

We consider the publications that are listed in this section particularly suitable for a more detailed discussion of the topics that are covered in this paper.

## IBM Redbooks publications

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350
- *A Guide to Writing Advanced Access Profiles for IBM Tivoli Access Manager for Enterprise Single Sign-On*, REDP-4767

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

**ibm.com**/redbooks

## Online resources

For all the relevant product documentation you should visit the IBM Tivoli Access Manager for Enterprise Single Sign-On Information Center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc/ic-homepage.html

## Help from IBM

IBM Support and downloads

**ibm.com**/support

IBM Global Services

**ibm.com**/services

# Configuring Strong Authentication with IBM Tivoli Access Manager for Enterprise Single Sign-On

**Details on external authentication factors for smartcards, Mobile ActiveCode, and RFID cards**

**Details on biometric authentication for fingerprint recognition**

**Hands-on details on complete configuration**

IBM Tivoli Access Manager for Enterprise Single Sign-On automates sign-on and access to enterprise applications, eliminating the need to remember and manage user names and passwords. Users log on to Tivoli Access Manager for Enterprise Single Sign-On with a special user ID and password, and then, when they access their secured applications, the Tivoli Access Manager for Enterprise Single Sign-On agent enters their stored credentials automatically without the users needing to do so. Tivoli Access Manager for Enterprise Single Sign-On provides the usual features associated with password security, for example, password length, aging policy, and so forth.

This IBM Redpapers publication is based on a set of exercises that was produced for the European Tivoli Technical Conference 2010. It shows how to configure Tivoli Access Manager for Enterprise Single Sign-On to use additional or alternative methods of authentication when users log on to provide a greater degree of security (stronger authentication).

This paper is intended to complement the product documentation and should be read in conjunction with it. In particular, you should refer to the Setup Guide.

REDP-4808-00