

IBM Security Access Manager
for Versions 6.1, 6.1.1, and 7.0

*Using Kerberos for Windows
Authentication
Exchange Guide*



IBM Security Access Manager
for Versions 6.1, 6.1.1, and 7.0

*Using Kerberos for Windows
Authentication
Exchange Guide*



Note

Before using this information and the product it supports, read the information in “Notices” on page 15

This edition applies to Version 1.1 release i of the IBM Security Access Manager Integration with Kerberos for Windows Authentication and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2010, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	v
About this publication	v
Access to publications and terminology	v
Publication Library	v
IBM Terminology website	vi
Accessibility	vi
Technical training	vi
Support information	vi
Statement of Good Security Practices	vii
Product name updates	vii
 Chapter 1. Introducing the integration	 1
Introduction	1
Using IBM Tivoli Federated Identity Manager	1
Using IBM Security Access Manager Impersonation Authentication Module	2
Integration product version information	2
Network connectivity considerations	3
 Chapter 2. Integration process	 5
Before you start	5
User account ID synchronization or mapping	5
Configuring Microsoft Exchange 2010	5
Exchange Management Console – Outlook Web App	6
Exchange Management Console – Exchange Control Panel	7
Configuring Microsoft Exchange 2013	9
Exchange 2013 Admin Center	10
Exchange Management Console – Outlook Web App	10
Exchange Management Console – Exchange Control Panel	10
Testing the integration	11
Known issues	13
 Notices	 15
Trademarks	17

Preface

About this publication

This guide provides instructions on how to configure your Microsoft Exchange Outlook Web Application (OWA) to enable a single-sign on using Kerberos tokens.

This document assumes that Active Directory is present and IBM® Security Access Manager (previously known as IBM Tivoli® Access Manager) and IBM Tivoli Federated Identity Manager are installed and running on your network. It does not provide details on the installation and administration of these products, except where necessary to achieve integration.

This guide is for those responsible for the installation, deployment, and administration of IBM Security Access Manager, IBM Security Access Manager WebSEAL, and Microsoft Exchange.

Readers must be familiar with the following:

- Microsoft Windows and UNIX operating systems
- Security management
- Lightweight Directory Access Protocol (LDAP) and directory services
- Supported user registries
- Authentication and authorization

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM Security Access Manager Base Installation Guide*
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Security Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Security Access Manager WebSEAL Administrator's Guide*
Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*
Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*
Provides information about configuring and maintaining a Security Access Manager environment.

IBM Tivoli Federated Identity Manager information

- *IBM Tivoli Federated Identity Manager Installation Guide*
Explains how to install, configure, and upgrade IBM Tivoli Federated Identity Manager services.
- *IBM Tivoli Federated Identity Manager Administration Guide*
Describes the concepts and procedures for using IBM Tivoli Federated Identity Manager services.
- *Redbook: Federated Identity Manager and Web Services Security with IBM Tivoli Security Services*
This Federated Identity Redbook covers important aspects of using the IBM Tivoli integrated identity management architecture to build and deploy the IBM Tivoli Federated Identity Manager and Web Services Security components. See www.redbooks.ibm.com.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Chapter 1. Introducing the integration

This chapter has the following sections:

- “Introduction”
- “Integration product version information” on page 2
- “Network connectivity considerations” on page 3

Introduction

This guide provides instructions on how to configure your Microsoft Exchange Outlook Web Application (OWA) to enable a single-sign-on (SSO) with IBM Security Access Manager using Kerberos tokens.

The integration can be achieved by using the IBM Tivoli Federated Identity Manager or the IBM Security Access Manager Impersonation Authentication Module.

Using IBM Tivoli Federated Identity Manager

IBM Security Access Manager and IBM Tivoli Federated Manager can be configured to enable SSO to backend applications by using Kerberos tokens. The Tivoli Federated Identity Manager can be deployed in an IBM WebSphere cluster or running as a stand-alone WebSphere Application Server. Figure 1 depicts the architecture of the environment.

See the *Using Kerberos for Microsoft Windows Authentication Foundation Guide* for instructions on how to configure and manage your Active Directory, IBM Tivoli Access Manager, and IBM Tivoli Federated Identity Manager installations. Install these products to enable single sign-on by using Kerberos tokens.

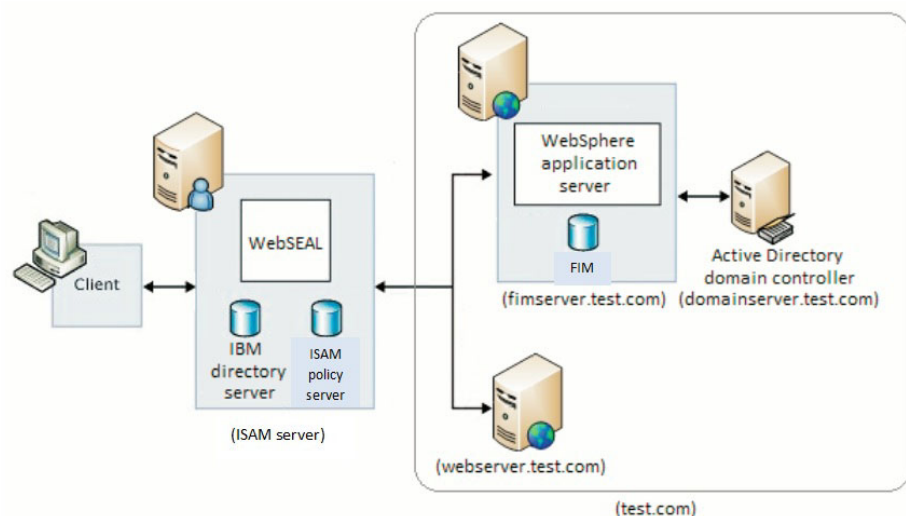


Figure 1. Environment overview using IBM Tivoli Federated Identity Manager

Using IBM Security Access Manager Impersonation Authentication Module

The IBM Security Access Manager Authentication Module is an integration module designed for Microsoft Internet Information Services version 7 and later. This module is designed to run as a native module within Microsoft Internet Information Services.

The purpose of the authentication module is to intercept a generated HTTP header representing an IBM Security Access Manager user and uses it to impersonate their corresponding Windows credential. The impersonation occurs when the authenticate event is fired in the request pipeline. If impersonation succeeds, the Windows credential is consumed by the web application. Figure 2 depicts the architecture of this environment.

See the *Using Impersonation Module for Microsoft Windows Authentication Guide* for information about the configuration and deployment of the impersonation module into the Microsoft Internet Information Service for Microsoft Exchange 2013.

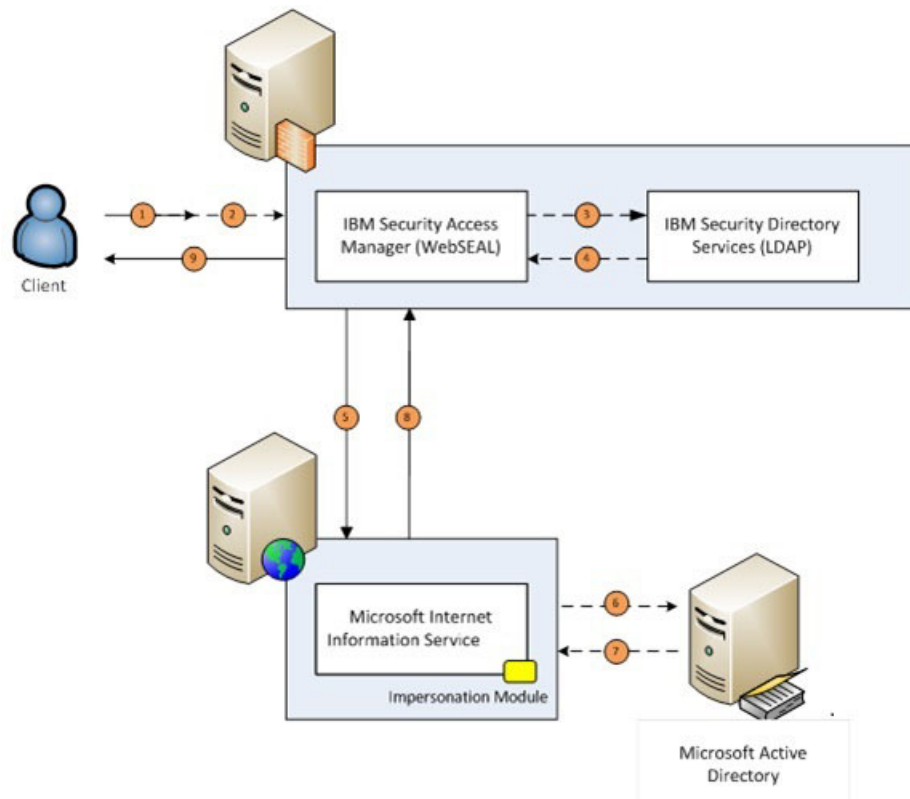


Figure 2. Environment overview using IBM Security Access Manager Impersonation Authentication Module

Integration product version information

For information about the supported product versions, see the Release Notes.

Network connectivity considerations

IBM Security Access Manager services typically run across multiple systems in the network. As such, some network paths must be open for the services to function correctly. All communication is over TCP/IP.

Chapter 2. Integration process

The following sections detail the steps required to achieve this integration.

- “Before you start”
- “Configuring Microsoft Exchange 2010”
- “Testing the integration” on page 11

Before you start

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

Note: Consult the documentation outlined in “Access to publications and terminology” on page v for details on installing and configuring these products.

IBM Security Access Manager

- User registry is configured with a supported registry.
- IBM Security Access Manager Policy Server installed.
- IBM Security Access Manager WebSEAL installed.

IBM Tivoli Federated Identity Manager

- Deployed to an WebSphere® Application Service.
- A Tivoli Federated Identity Manager domain is configured and the runtime is deployed to the domain.

or

IBM Security Access Manager Impersonation Module

- Deployed to Microsoft Internet Information Services
- Install the native module and configure the applet in Microsoft Internet Information Services

Microsoft Exchange

- Installed with Outlook Web Access option.

See “Integration product version information” on page 2 for product details.

User account ID synchronization or mapping

See the *User account ID synchronization or mapping* section in the *Using Kerberos for Microsoft Windows Authentication Foundation Guide* for user account IDs synchronization or mapping between the Tivoli Access Manager user registry and the Microsoft Active Directory.

Configuring Microsoft Exchange 2010

To use Kerberos authentication, the Microsoft Exchange Outlook Web Access (OWA) and Exchange Control Panel (ECP) must be configured.

Exchange Management Console – Outlook Web App

1. From the left pane, expand **Microsoft Exchange On-Premises > Server Configuration > Client Access**.
2. From the right pane, select the **Outlook Web App** tab.

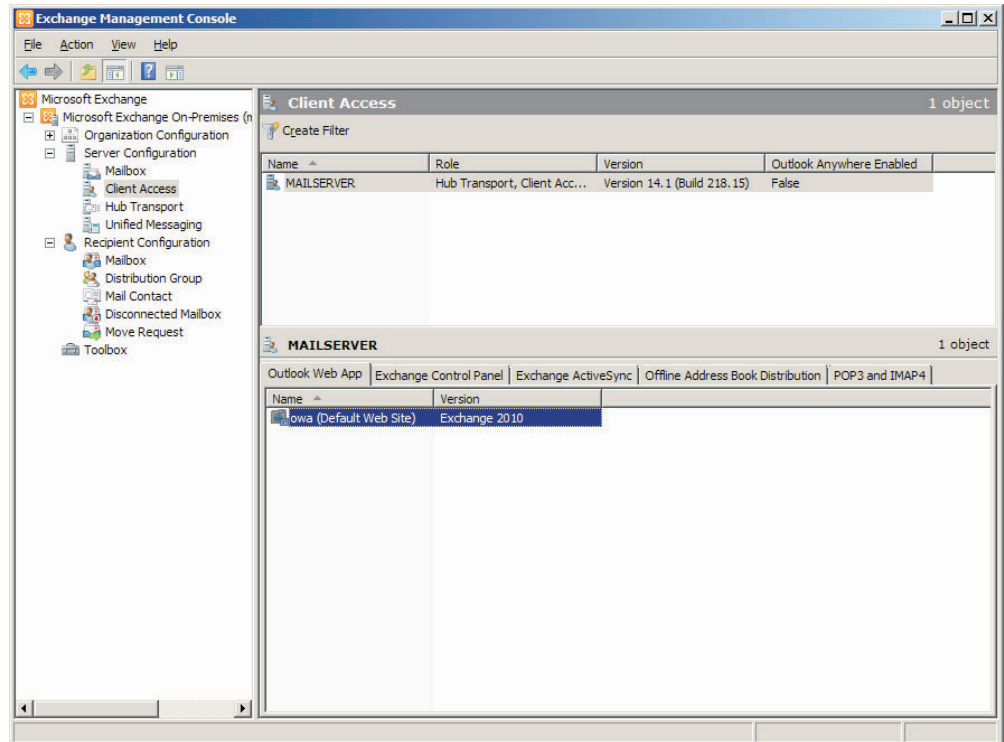


Figure 3. Outlook Web App tab

3. Right-click the **owa (Default Web Site)** item and select **Properties**.
4. On the **Authentication** tab, check **Integrated Windows authentication** and click **OK**.

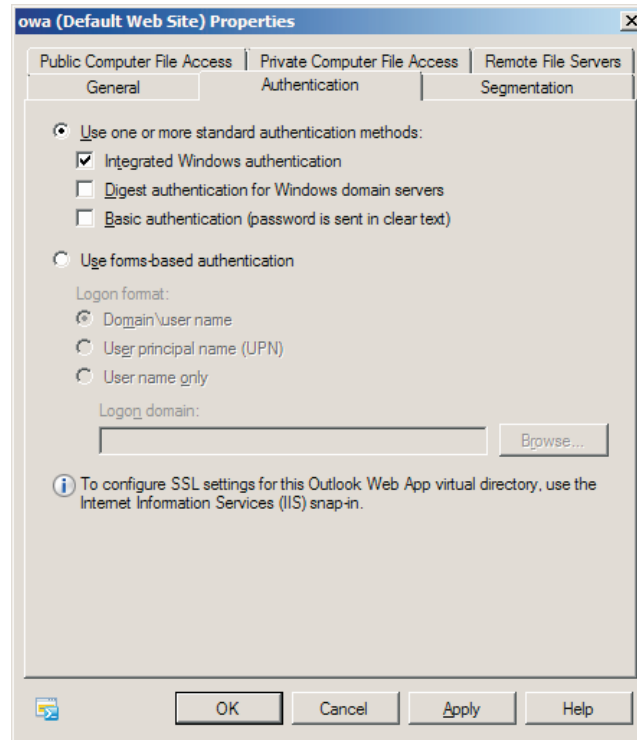


Figure 4. OWA authentication properties

Exchange Management Console – Exchange Control Panel

1. From the left pane, expand **Microsoft Exchange On-Premises > Server Configuration > Client Access**.
2. From the right pane, select the **Exchange Control Panel** tab.

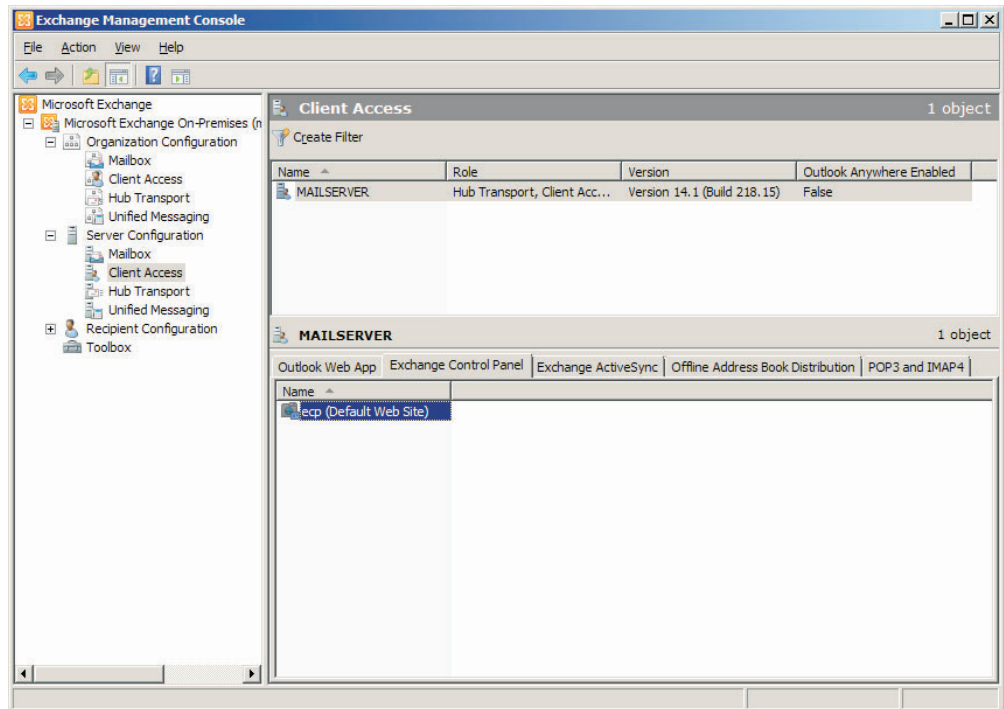


Figure 5. Client Access – Exchange Control Panel

3. Right-click the **ecp (Default Web Site)** item and select the **Properties** from the context menu.
4. On the **Authentication** tab, check **Integrated Windows authentication** and click **OK**.

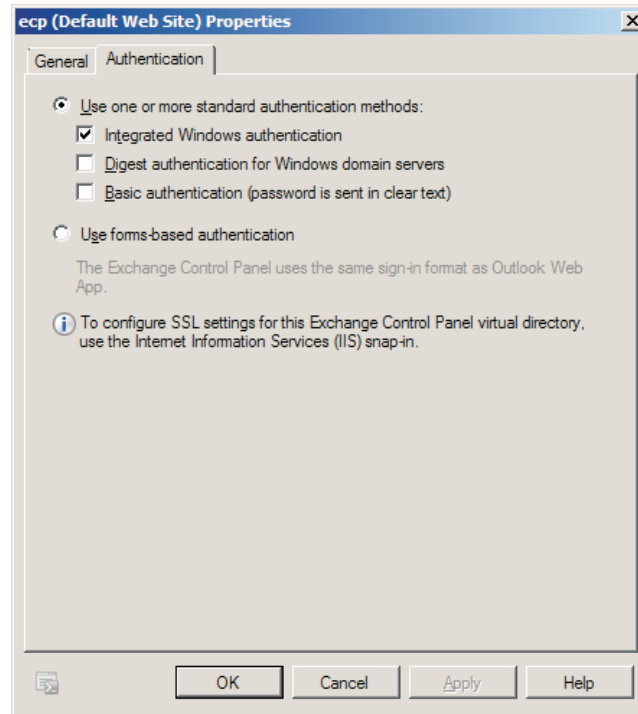


Figure 6. ECP authentication properties

Configuring Microsoft Exchange 2013

Unlike Microsoft Exchange 2010 which uses a MMC snap-in, administration options for Microsoft Exchange 2013 are configured in the web based Administration Center. For example <https://mailserver.test.com/ecp>. Until single sign-on is configured you must navigate to the site directly and not through IBM Security Access Manager. You must provide authentication credentials.

Exchange 2013 Admin Center

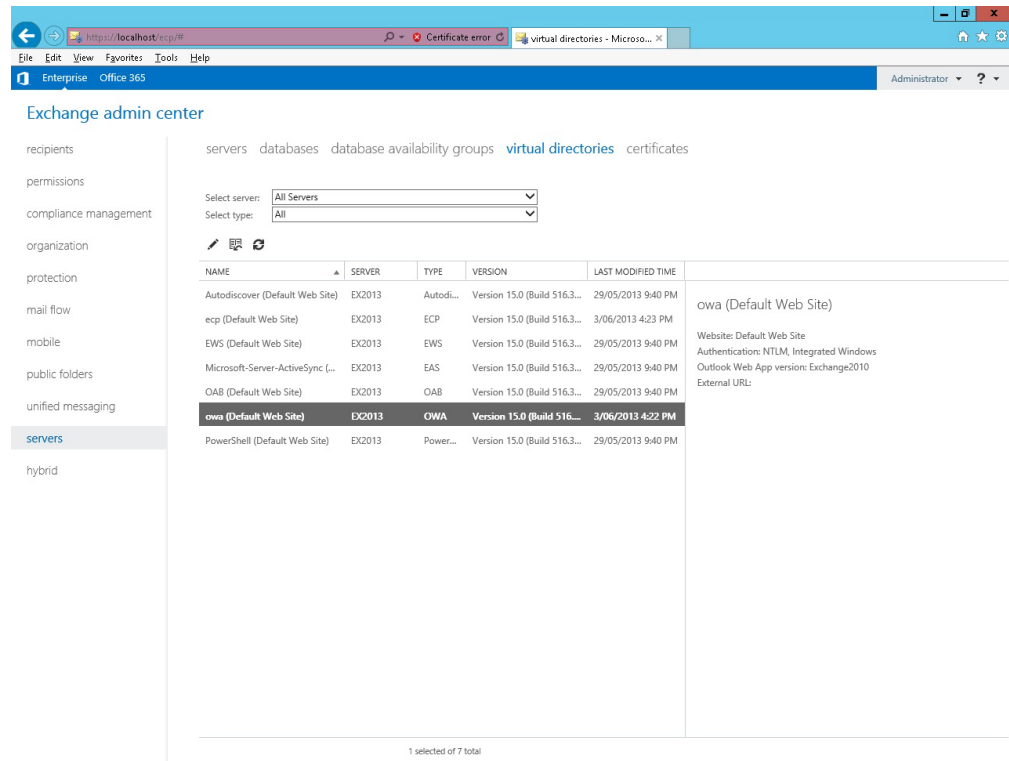


Figure 7. Exchange admin center

Exchange Management Console – Outlook Web App

1. Navigate to the following URL in a browser: <https://<mailserver.test.com>/ecp>.
2. From the **Feature Pane**, click **servers**.
3. Click the **virtual directories** tab.
4. From the table displayed, double-click or click the **Edit** icon on owa (Default Web Site).
5. Click **authentication** from the pop-up browser window.
6. Make sure that **Use one or more standard authentication methods** is selected.
7. Select the **Integrated Windows authentication** check box.
8. Click **Save**.

Exchange Management Console – Exchange Control Panel

1. Navigate to the following URL in a browser: <https://<mailserver.test.com>/ecp>.
2. From the **Feature Pane**, click **servers**.
3. Click the **virtual directories** tab.
4. From the table displayed, double-click or click the **Edit** icon on ecp (Default Web Site).
5. Click **authentication** from the pop-up browser window.
6. Make sure that **Use one or more standard authentication methods** is selected.
7. Select the **Integrated Windows authentication** check box.

8. Click **Save**.

Testing the integration

With the Microsoft Exchange Outlook Web Access configured, the site is now ready to be accessed by using an IBM Security Access Manager username and password.

Note: The IBM Security Access Manager user name must correspond to a user account in Active Directory or be mapped in the Tivoli Federated Identity Manager Kerberos Delegation module to an existing Active Directory user account.

This guide assumes that web requests directed to the Microsoft Exchange server are routed through the IBM Security Access Manager server. An alternative to making DNS changes on a DNS server is to modify the hosts file of the client, at `c:\Windows\System32\drivers\etc\hosts`.

The following example shows sample configuration changes to redirect requests to another computer. The IP address that is associated with the webserver entry is that of the tamserver machine.

```
# 38.25.63.10      x.acme.com # x client host
192.168.60.128    mailserver # routes to WebSEAL (tamserver)
```

1. Complete the required configuration for WebSEAL including junction creation as described in the *Using Kerberos for Microsoft Windows Authentication Foundation Guide* provided with this integration.
2. Ensure that the WebSEAL junction type argument value is **ssl**. Microsoft Exchange Outlook Web Access uses secure sockets layer (SSL) to communicate. See the following **pdadmin** command for an example.

```
pdamin sec_master> s t default-webseald-tamserver virtual create -t ssl
-h mailserver.test.com -Y owa
```

Note:

- The **-Y** parameter is used for single sign-on with IBM Tivoli Federated Identity Manager only. This parameter is not required for the Impersonation Authentication Module.
 - Microsoft Exchange Outlook Web Access uses secure sockets layer (SSL). For single sign-on to function accordingly through WebSEAL, the Microsoft Exchange Outlook Web Access site certificate must be imported into the WebSEAL instance local key store. See the relative WebSEAL administration documentation for the instructions on how to import the certification to its local key store.
3. Browse to the Microsoft Exchange Outlook Web Access URL. The web site URL is displayed on the **General** tab of Figure 4 on page 7.

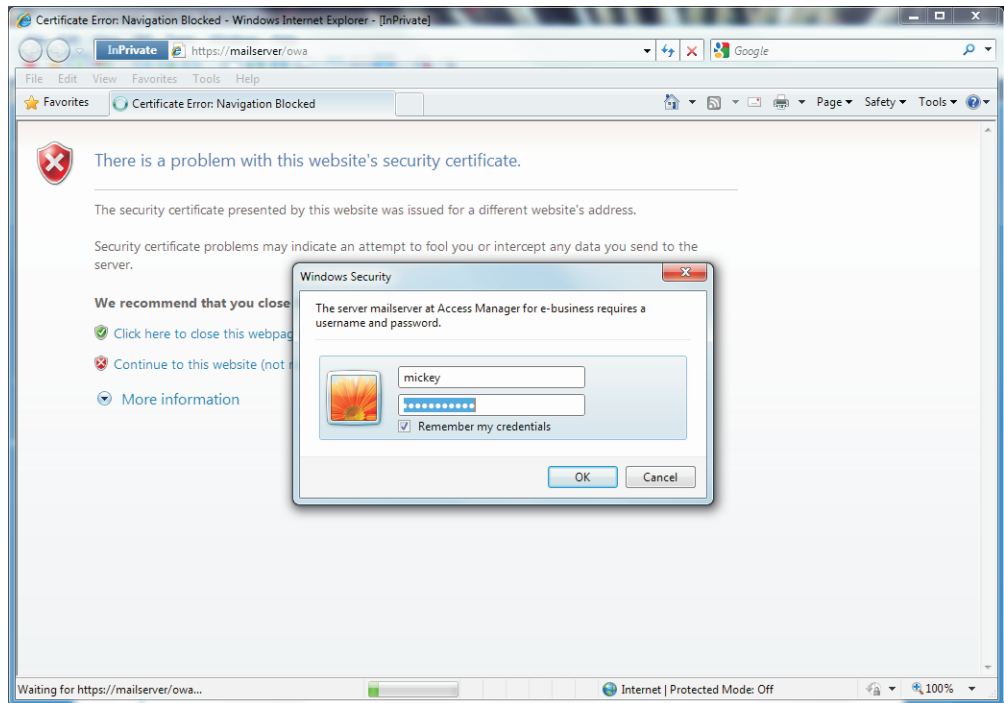


Figure 8. Kerberos Authentication to Exchange through WebSEAL

4. Log in with your user name and password. IBM Security Access Manager authenticates the request, and then issues an RTS request to Tivoli Federated Identity Manager that in turn constructs the Kerberos token. The Kerberos token is passed back to IBM Security Access Manager and forwarded to Microsoft Exchange for Windows Authentication. The Outlook Web Access (OWA) site is then displayed as shown in Figure 9 on page 13.

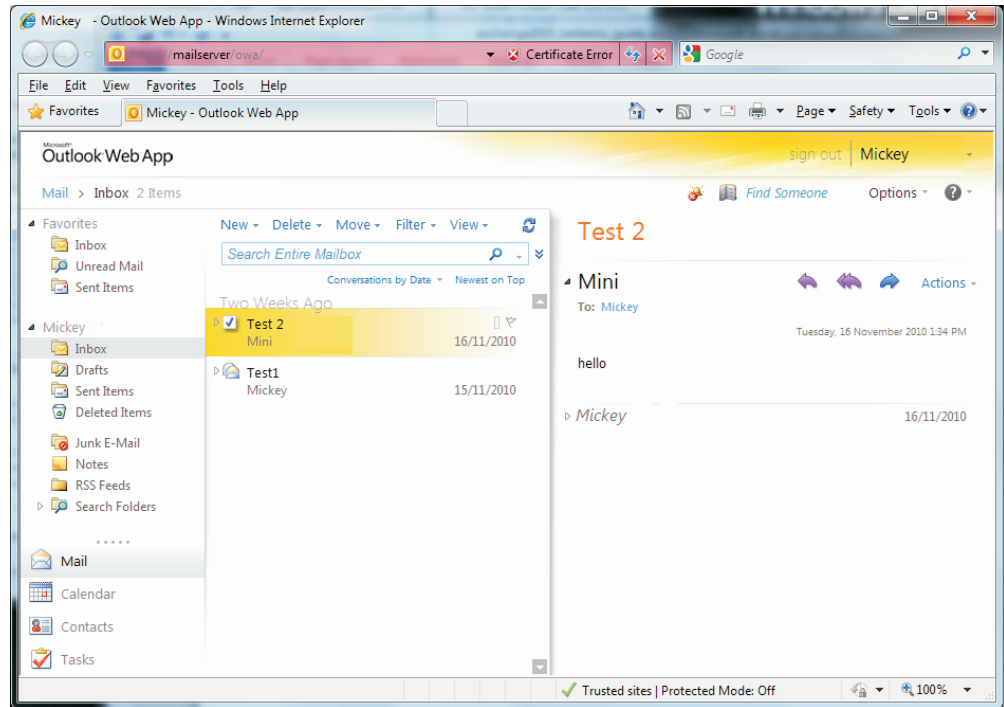


Figure 9. Kerberos authentication to Exchange

Known issues

The IBM Security Access Manager Impersonation Authentication Module is not supported for use with Microsoft Exchange 2010.

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.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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. 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 IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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



Printed in USA