May 2007

# Single Sign-On to Microsoft Exchange 2007 in a clustered environment

## Summary

Users of the SAP NetWeaver Portal can take advantage of Single Sign-On to Web based Microsoft backend systems such as Outlook Web Access using SAP's SSO22KerbMap Module. With Exchange 2007 Microsoft introduces different server roles that enable administrators to easily choose which features are installed on an Exchange server. One of these roles is the Client Access server role that provides access to Microsoft Office Outlook Web Access. In Exchange 2007, Client Access servers support Integrated Windows Authentication for Exchange 2007 virtual directories. As a result the SSO22KerbMap Module can now be installed on a Client Access server rather than on a backend server which was necessary if the filter is used in an Exchange 2003 environment. Exchange 2007 now also offers the possibility to cluster mailboxes, a feature that will likely find a large adoption. We thus investigated a setup that consists out of a Client Access Server and CCR cluster (Cluster Continuous Replication).

## Applies to

- SAP NetWeaver Portal 6.0 SP9 or higher
- Microsoft Active Directory 2003 (forest functional level set to Windows Server 2003)
- Microsoft Exchange 2007 CCR cluster
- SSO22KerbMap Module

## Contact

For feedback or questions you can contact the Collaboration Technology Support Center via the .NET Technologies forum in the .NET interoperability area of SDN. Please check the .NET interoperability area in SDN for any updates or further information.

## Authors Bio

**André Fischer** works at **SAP AG** in the Strategic Alliance Microsoft Team. He is also a member of the CTSC (Collaboration Technology Support Center) that addresses various kinds of interoperability topics regarding SAP and Microsoft solutions. André has specialized in single sign-on, SAP Microsoft Active Directory integration, SAP Exchange Infrastructure BizTalk integration and knowledge management Microsoft Windows integration.

**Jürgen Daiberl** works at **Mircosoft Corp.** as Technical Evangelist at the Developer & Platform Evangelist Team in Redmond. Prior to his role in Redmond he worked at the CTSC (Collaboration Technical Support Center) in Walldorf / Germany, a joint staffed team between Microsoft and SAP. In his current role he is responsible for the Interoperability between Microsoft .NET and SAP NetWeaver on the Application level.


# Contents

## Introduction

Users of the SAP NetWeaver Portal can take advantage of Single Sign-On to Web based Microsoft backend systems using SAP's SSO22KerbMap Module. The SSO22KerbMap Module is frequently used for the integration of Microsoft Exchange Server into a SAP NetWeaver Portal environment.

With Exchange 2007 Microsoft introduces different server roles that enable administrators to easily choose which features are installed on an Exchange server. One of these roles is the Client Access server role that provides access to Microsoft Office Outlook Web Access. In Exchange 2007, Client Access servers support Integrated Windows authentication for Exchange 2007 virtual directories

As a result the SSO22KerbMap Module can now be installed on a Client Access server rather than on a backend server which was necessary if the filter is used in an Exchange 2003 environment.

As availability requirements for eMail have increased over the years so too did the need to guarantee Exchange availability. While client access servers can easily achieve high availability using a scale out strategy backend servers are single points of failure if no additional measures are taken to increase their availability.

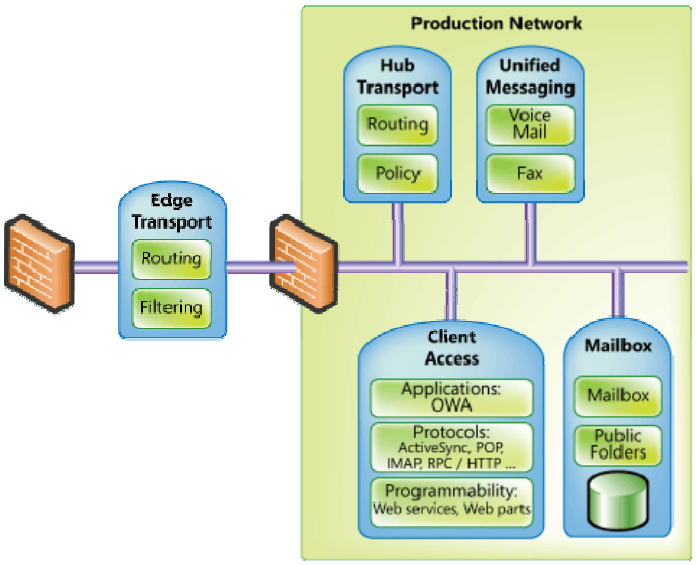
Exchange 2007 now also offers the possibility to cluster mailboxes a feature that will likely find a large adoption. We thus investigated a setup that consists out of a Client Access Server and CCR cluster.

This whitepaper therefore describes the configuration steps that are necessary to implement the SSO22KerbMap Module in a Exchange cluster 2007 environment that leverages a distributed setup that consists out of a Client Access Server and a CCR cluster.

## Exchange 2007

Exchange Server provides a complete messaging system that can run on a single server – meaning that all Exchange services reside on one server, as with the Microsoft Small Business Server product. However, there are significant gains in deployment, management, and security that come from having a flexible, modular system that can be installed across more than one machine. This concept was first introduced in Exchange 2000 Server where a front-end server could be configured to proxy inbound Internet client protocols to the appropriate mailbox server. Front-end servers are optional and can reduce the load on mailbox servers and simplify Microsoft Office Outlook® Web Access (OWA) and Exchange ActiveSync (EAS) user access. Having front-end servers in medium-size and large organizations made Exchange more scalable by concentrating particular tasks on a limited number of servers.

In Exchange Server 2007, role-based deployment has been expanded, allowing you to assign predefined roles to specific servers. These roles allow organizations to control mail flow, increase security, and distribute services, as shown in the following illustration.




Customers would typically customize their Exchange Server 2003 installation, creating specific server roles in a very manual fashion. In Exchange Server 2007, roles are predefined and chosen during installation. The role selected during installation ensures that only the necessary services and components are installed. Not only does this simplify deployment, but it also enables more efficient management and hardware utilization over time.

- **Client Access role**. Similar to the front-end server in earlier versions of Exchange, this server proxies Internet client traffic to the correct mailbox server.
- **Mailbox role**. This role hosts user mailboxes stored in databases that can be replicated or clustered.
- **Hub Transport role**. This role provides internal routing of all messages – from Edge servers, Unified Messaging (UM) servers, or between two users on the same mailbox database. The Hub Transport role is also where messaging policy is enforced for messages moving within and outside the organization.
- **Unified Messaging role**. This role enables PBX integration to allow voice mail and fax messages delivered to Exchange mailboxes, and provides voice dial-in capabilities to Exchange Server.
- **Edge Transport role**. This server resides outside your internal network and provides on-premise e-mail security, antivirus, and anti-spam services for Exchange.

## Client Access Server

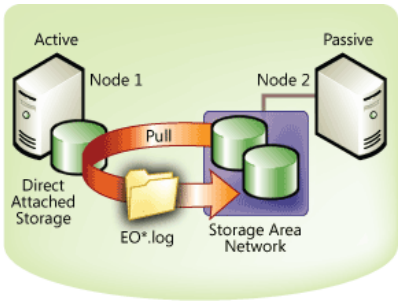
The Client Access server role supports the Microsoft Office Outlook Web Access and Microsoft Exchange ActiveSync client applications, and the Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4rev1 (IMAP4) protocols. The Client Access server role also provides access to free/busy data by using the Availability service and enables clients that are running Microsoft Outlook 2007 and certain mobile

operating systems to download automatic configuration settings from the Autodiscover service.

The Client Access server role accepts connections to your Exchange 2007 server from a variety of different clients. Software clients such as Microsoft Outlook Express and Eudora use POP3 or IMAP4 connections to communicate with the Exchange server. Hardware clients, such as mobile devices, use ActiveSync, POP3, or IMAP4 to communicate with the Exchange server. A Client Access server role must be installed in every Exchange organization.

### CCR cluster (Cluster Continuous Replication)

To provide redundancy for Exchange services and information stores, Exchange Server 2007 provides Cluster Continuous Replication (CCR). Similar to clustering solutions available with earlier versions of Exchange, CCR uses Windows Clustering Services to provide virtual servers and failover capabilities. However, with CCR, shared storage is not required because each node has its own copy of the information stores This allows customers to implement a variety of storage options such as Direct Attached Storage, Serial Attached SCSI, and Storage Area Networks. This solution uses a form of log file shipping that is found in databases such as Microsoft® SQL Server™.




On the active node, transactions are written to the transaction log. When the current transaction log is full, the passive node pulls a copy of the transaction log from the active node to the passive node. A service on the passive node then posts the transactions from the replicated transaction log into the database on the passive node. If the active node fails (either planned or unplanned), the cluster fails over to the passive node that mounts the databases and continues providing Exchange services. Transactions logs on the new active node are then replicated over to the new passive node as needed.

Aside from the benefits of having your databases replicated across multiple nodes, you can also back up the database and transaction logs on the passive node without impacting performance on the active node. After backup is complete on the passive node, and the proper transaction logs are deleted, the transaction logs on the active node are also deleted. The cluster nodes must be on the same subnet, but if the subnet spans physical networks, you can place the active node and passive node in different physical locations. This means that replicating your Exchange databases to a remote disaster recovery site is now possible.

Also, since the reasons for having to restore from backup are reduced with CCR, you may be able to reduce your operating costs by reevaluating your backup strategy and decide if the same schedule, backup type, and number of tapes are needed.

## The SSO22KerbMap Module

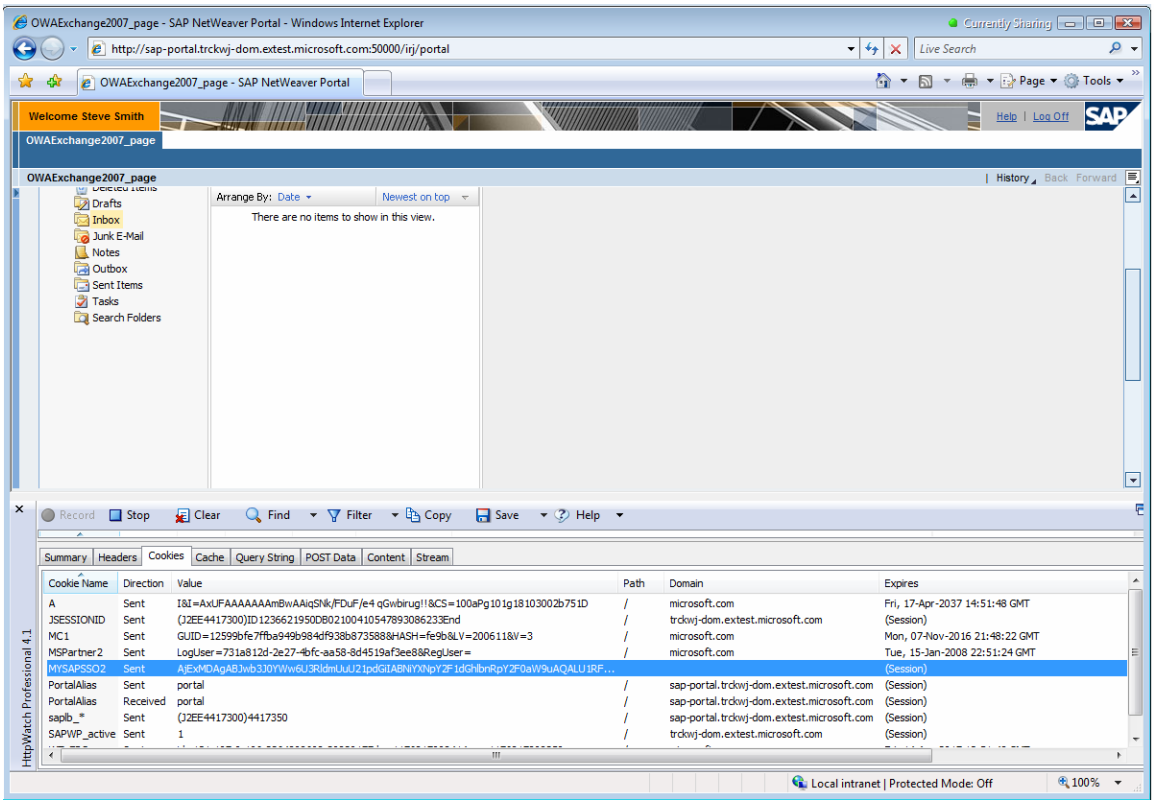
A detailed description of the SSO22KerbMap Module can be found in the collaboration brief *“Using SAP Logon Tickets for SSO to Microsoft-based Web Applications”*.

The ticket bridging mechanism leverages an enhancement of the implementation of the Kerberos protocol that has been introduced by Microsoft with Active Directory 2003.

Using *constrained delegation* a service may request a (constrained) Kerberos ticket on behalf of a user for specified services only. By using *protocol transition* it is possible that the client may be authenticated using other methods than Kerberos. Based on this technology SAP has developed an ISAPI Filter called *SSO22KerbMap Module*.

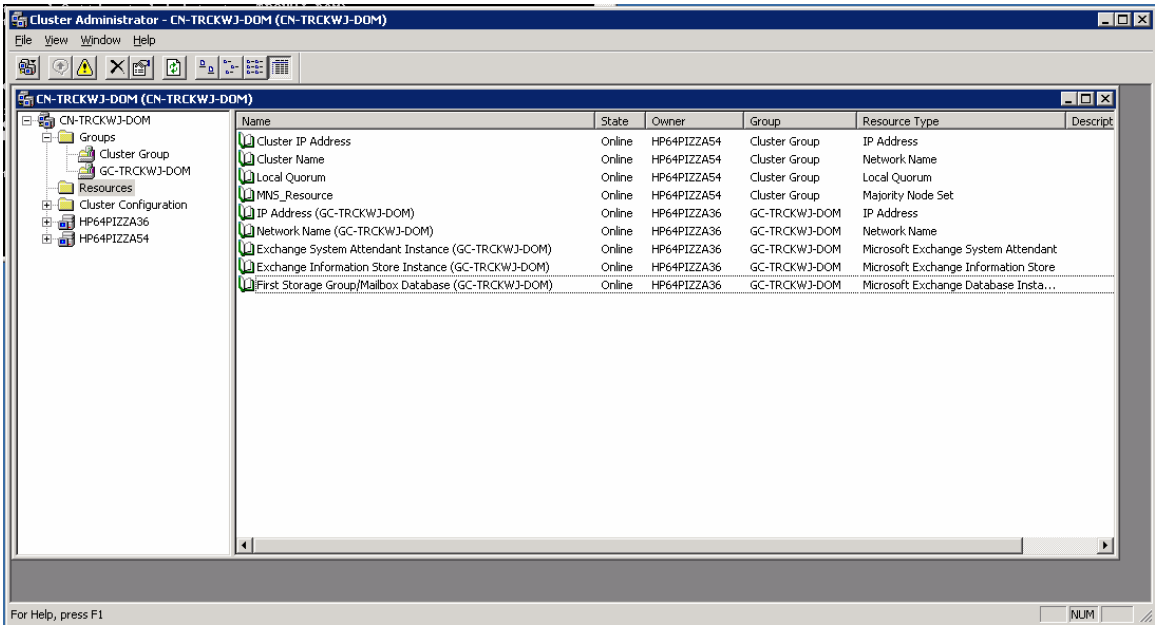
Since Exchange 2007 Client Access Servers support Windows Integrated Authentication the SSO22KerbMap module can be installed on the client access servers rather than on the Exchange backend server which was necessary in the past with Exchange Server 2003.

The following screen shot shows the browser access to Microsoft Outlook Web Access through the SAP NetWeaver Enterprise Portal. Using HTTP Watch it is shown that an SAP Logon Ticket is sent with the HTTP request to the OWA server.




## Integration scenario

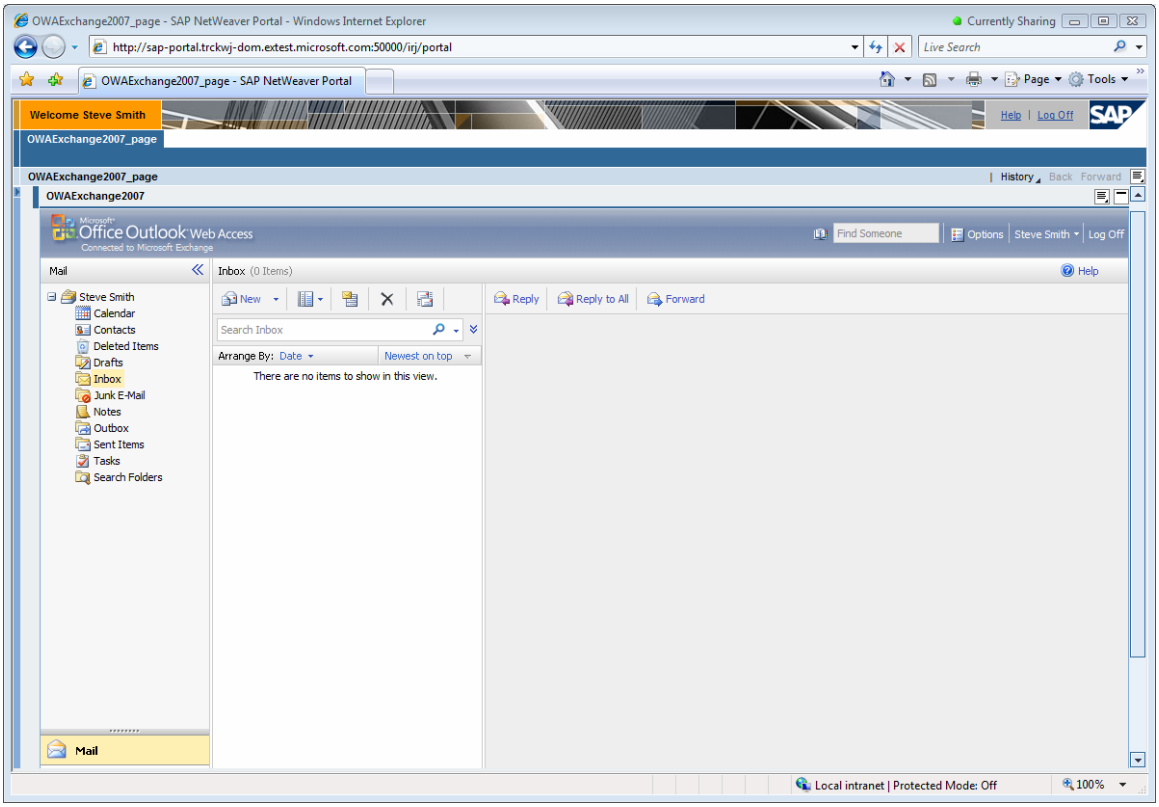
The scenario uses a Microsoft Exchange 2007 landscape that consists out of a client access server and two mailbox servers that are using Cluster Continuous Replication (CCR).




The mailboxes could be accessed using a client access server HP64-SFF120 which was equipped with the SSO22KerbMap Module.
We decided to work with this setup since we assume that several customers will leverage CCR technology to achieve high availability for the mailboxes of their Exchange Servers and because the setup of the SSO22KerbMap Module in a clustered Exchange 2003 environment differs from the setup of a non-clustered environment.
When using a Client Access Server it turns out that there is no difference in the setup of the SSO22KerbMap Module for a clustered and non-clustered Exchange 2007 environment.

## Result

The following screenshots show the successful integration of Microsoft Outlook Web Access 2007 into a SAP NetWeaver Enterprise Portal using the SSO22KerbMap Module and an Application Integrator iView.




## How to Guide section

The following How-To Guide section describes the steps necessary to configure the SSO22KerbMap module on an Exchange 2007 Client Access server.

**Please note:**

This How-To Guide is not meant as a replacement for the official SAP and Microsoft documentations. It is rather meant as a source for information that is specific for the configuration of the SSO22KerbMap Module in an Exchange Server 2007 environment.

The configuration steps can be summarized as follows:

The SSO22KerbMap Module has to be installed on each Client Access Server (if several ones are used).

In contrast to Exchange 2003 there is no difference in the setup if the server that hosts the mailboxes is clustered compared to a setup where a single server installation in the backend is used.

### Step 1: Downloading the installation files

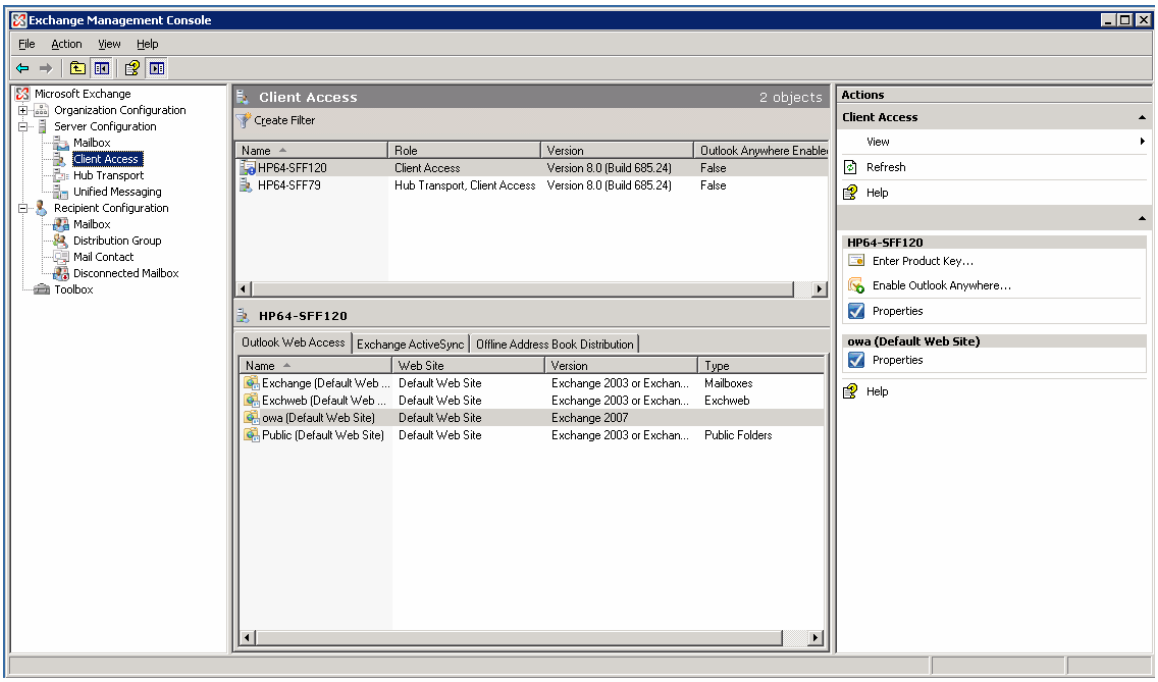
1. Download the most recent version of the SSSO22KerbMap Module and the SAP Logon Ticket Toolkit from SAP Service Marketplace at: http://service.sap.com/patches -> SAP Support Packages and Patches -> Entry

by Application Group -> SAP Technology Components -> SAPSSOEXT -> SAPSSOEXT -> Windows Server on x64 64bit -> SAPSSOEXT_<PL>.SAR and SSO22KerbMap_<PL>.SAR

2. Download the most recent version of SAPSECULIB from SAP Service Marketplace at: http://service.sap.com/patches -> SAP Support Packages and Patches -> Entry by Application Group -> SAP Technology Components -> SAPSECULIB -> SAPSECULIB -> Windows Server on x64 64bit -> SAPSECULIB_<PL>.SAR
3. Download the *verify.pse* file from the SAP Enterprise Portal at *System Administration → System Configuration → Keystore Administration*.

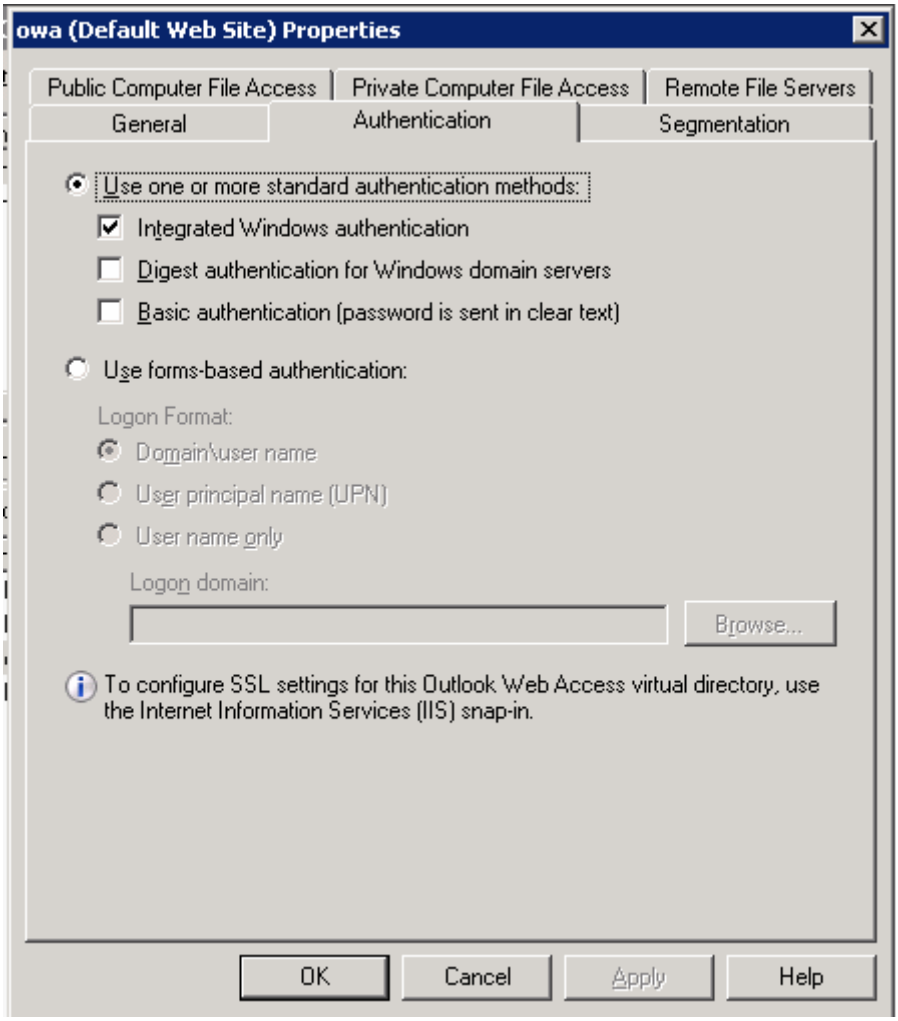
Please note:
Since Exchange Server 2007 is only available on x64 64-bit platforms please be sure to download the files that have to be used for x64 64bit windows platforms.

## Step 2: Configuring Windows Integrated Authentication on the client access server




1. Open the Exchange Management Console.
2. Locate **Server Configuration\Client Access**.
3. On the **Outlook Web Access** tab, open the properties of the virtual directory that you want to configure to use Integrated Windows authentication.
4. Click the **Authentication** tab.
5. Select **Use one or more of the following standard authentication methods**.
6. Select **Integrated Windows authentication**.
7. Click **OK**.

As a result the virtual directory that is used for Outlook Web Access is configured to use Windows Integrated Authentication.




## Step 3: Installing the SSO22KerbMap Module on the Client Access Server

This step includes the following tasks:

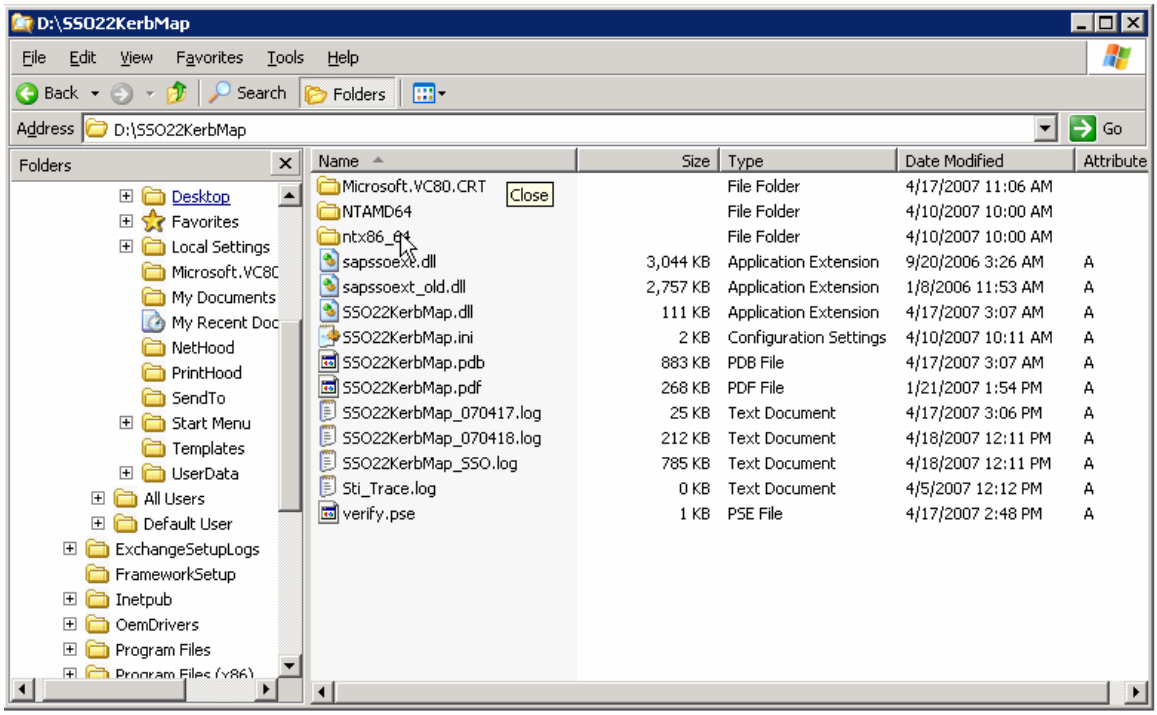
1. Copying the required files for the ISAPI filter to the local directories
2. Determine the SPN used for constrained delegation.
3. Adapt the configuration file SSO22KerbMap.ini
4. Configure the ISAPI Filter in the Internet Information Services Manager
5.

**Copying the required files for the ISAPI filter to the local directories**

1) The following files that have been downloaded in step 1:
   - *SSO22KerbMap.dll*
   - *SSO22KerbMap.pdb*
   - *SSO22KerbMap.ini*

- *sapssoext.dll*
- *verify.pse*

are copied to a local directory on the Client Access Server (in this case *D:\SSO22KerbMap).*




2) The following files that have been downloaded in step 1:
   - *Microsoft.VC80.CRT.manifest*
   - *msvcm80.dll*
   - *msvcp80.dll*
   - *msvcr80.dll*

   are copied to the subdirectory ...*Microsoft.VC80.CRT* in the directory specified in 1) (in this case D:*\SSO22KerbMap\Microsoft.VC80.CRT )* on the Client Access Server.

3) The file *sapsecu.dll* is copied to a directory that is included into the path, for example the %WINDIR%\SYSTEM32 directory.

**Determine the SPN used for constrained delegation.**

1. Log on as a domain administrator.

   ```
   Use the command-line tool setspn.exe

   setspn –L hp64-sff120
   ```

   to list the configured Service Principal Names (SPN) for HOST for the LocalSystem account for the client access server (here: hp64-sff120). The tool will list the Service Principal Name that is registered in Active Directory for the FQDN of the Client Access Server HP64-sff120.

```
HOST/hp64-sff120.TRCKWJ-dom.extest.microsoft.com
```

Please note:
The Setspn.exe tool is included with the Microsoft Windows Server 2003 Support Tools. To install the Windows Support Tools, double-click *Suptools.msi* in the *Support\Tools* folder on the Windows Server 2003 CD.

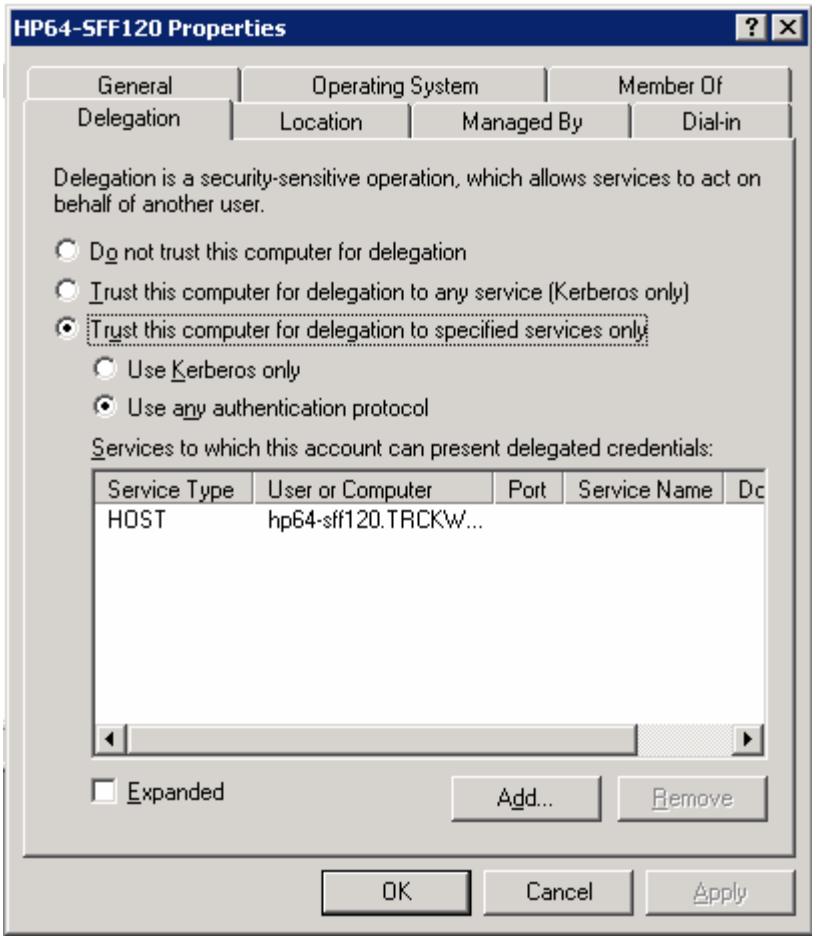
**Adapt the configuration file *SSO22KerbMap.ini***
Now the configuration file SSO22KerbMap.ini on the Client Access Server can be adapted to meet the environment. In our setup the configuration file *SSO22KerbMap.ini* contains the following entries:

```
PseFile: D:\SSO22KerbMap\verify.pse
ServicePrincipalName: HOST/hp64-sff120.TRCKWJ-dom.extest.microsoft.com
FilterPriority: High
SSO2AccountAttribute: sAMAccountName
LogLevel: 3
```

**Configure the ISAPI Filter in the Internet Information Services Manager**
Install the SSO22KerbMap Mapping Filter (the `SSO22KerbMap.dll`) as an ISAPI filter on the website the target application is running on, as follows:

## Step 3: Configure constrained delegation for the Client Access Server in Active Directory

Constrained delegation has to be configured only for the client access server. To do this the *Trusted-to-Authenticate-for-Delegation flag* has to be configured for the computer account of the CAS.



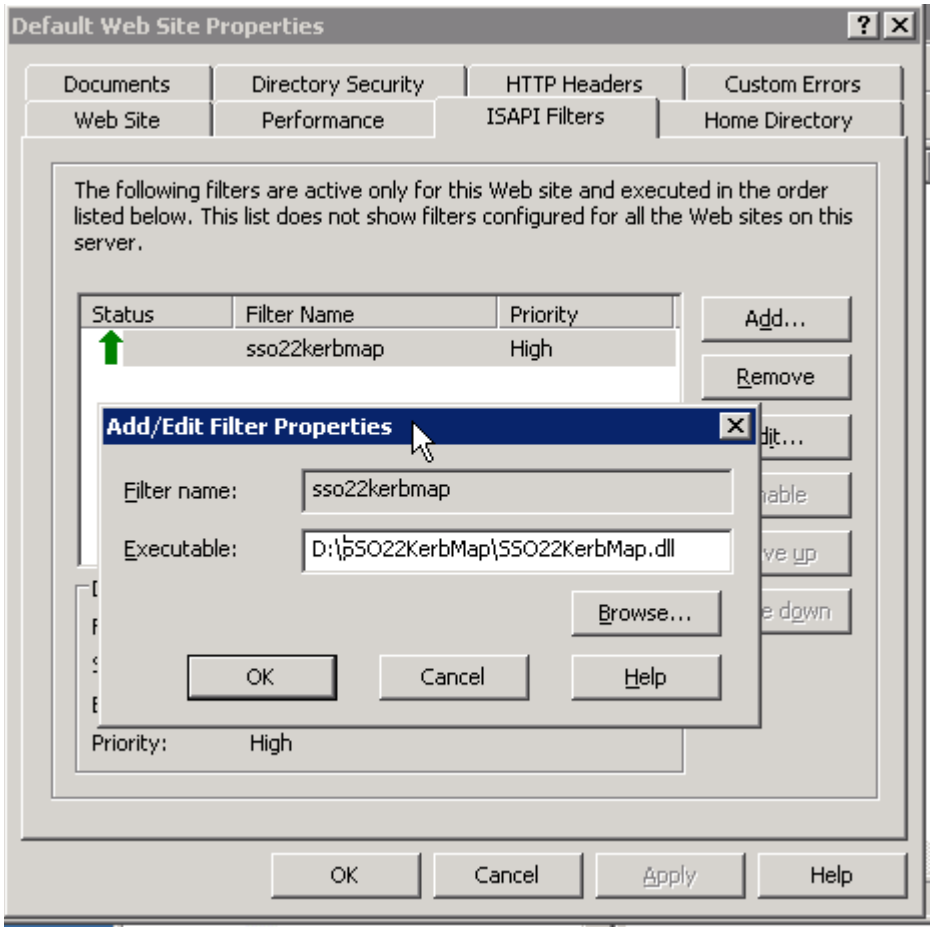

In the following we describe the configuration steps for the computer account of the Client Access Server:

1. Open the MMC *Active directory Users and Computers*.
2. Choose <Your Windows_2003_domain> and locate the computer account of the cluster node (here HP64-SFF120).
3. Right-click the cluster node  and choose Properties.
4. Select Delegation and Trust this computer for delegation to specified services only.
5. Select Use any authentication protocol and choose Add.
6. Select Users or Computers and enter the cluster node that has been selected above as object name (here HP64-SFF120).
7. Choose Check Names and OK.
8. Add the SPN for the HOST service type for your cluster node which was determined in Step 2

Steps 1 to 8 have to be repeated with each client access server if several client access servers are used. Replace the hostname HP64-SFF120 with the hostname of the client access server in the configuration steps described above.

## Step 3: Activation of the ISAPI Filter

After the changes have been done one has to activate the filter.




This has to be done by performing an iisreset. Afterwards you have to access the OWA URL. Only after the filter has been accessed the status will change to green.

## Important Note

Please check SAP Note 735639 *SSO22KerbMap: Known issues* before installing the SSO22KerbMap Module.

At the time of writing of this whitepaper for each server that uses the SSO22KerbMap Module, the Microsoft Hotfix 907524 has to be installed to avoid a memory leak in Windows 2003 caused by Microsoft's *lsass.exe*.

## Conclusion

The SSO22KerbMap Module has only to be installed in the Exchange virtual server of the Client Access Server(s). The setup of the SSO22KerbMap Module for an Exchange Server 2007 CCR Cluster is identical to the setup that is necessary for a CAS together with a single non clustered backend server.

## References


- Note 735639 - SSO22KerbMap: Known issues
  https://service.sap.com/sap/support/notes/735639
- Note 785343 - SSO22KerbMap: Configuration for SSO for Outlook Web Access
  https://service.sap.com/sap/support/notes/785343
- Step-by-Step Guide: SSO22KerbMap ISAPI Module Collaboration Brief "*Using SAP Logon Tickets for Single Sign on to Microsoft based web applications*"
  https://www.sdn.sap.com/irj/servlet/prt/portal/prtroot/com.sap.km.cm.docs/library/unknown/Using%20SAP%20Logon%20Tickets%20for%20SSO%20to%20Microsoft-based%20Web%20Applications.pdf
- A memory leak occurs in the Lsass.exe process after you configure constrained delegation in Windows Server 2003
  http://support.microsoft.com/default.aspx?scid=kb;en-us;907524