Laserfiche Web Access 8 and Kerberos Configuration in a Windows Server 2008 and IIS 7 Environment

White Paper

March 2009

Laserfiche®

The information contained in this document represents the current view of Compulink Management Center, Inc on the issues discussed as of the date of publication. Because Compulink must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Compulink, and Compulink cannot guarantee the accuracy of any information presented after the date of publication.

This chapter is for informational purposes only. COMPULINK MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Table of Contents

1. Overview

Kerberos is an authentication protocol that allows for delegation, which allows you to pass user credentials between different computers. When dealing with the Laserfiche product suite, Kerberos becomes the required authentication protocol when Web Access 8 is running on a different host from the Laserfiche Server and you wish to configure Web Access to allow users to log in using Windows authentication.

Configuring your domain to support Kerberos authentication can be a multi-layered process depending on your specific Laserfiche and network configuration. This paper will list out the possible areas of configuration, starting with the mandatory steps that must be performed for all installations to optional steps that may need to be taken depending on your Laserfiche and network configuration. Here are the possible areas of configuration:

1. Basic configuration involving enabling the Windows Authentication option in IIS and configuring the Laserfiche repository to allow Windows accounts to log in to the repository.
2. Trust the Web server computer for Kerberos delegation.
3. **Optional:** Register SPNs for the Laserfiche Server service domain account. This step is only necessary when the Laserfiche Server is not running under the Local System account.
4. **Optional:** Register SPNs for the application pool identity and trust the application pool identity for Kerberos delegation. By default, SPN registration and Kerberos delegation for the application pool identity is unnecessary in IIS 7. You should only perform the steps described in this section if the Web Access 8 application pool identity is a domain user account plus you specifically want to use the application pool's identity for Kerberos ticket decryption.

Finally, this paper will list out additional resources on the Web for troubleshooting Kerberos, including information on 3rd party tools for diagnosing Kerberos and network issues.

Examples in this whitepaper are based on:

- A Windows Server 2008 domain functional level for Active Directory.
- IIS 7 on Windows Server 2008 Service Pack 1.

Note: The required SPN registrations for setting up Kerberos authentication with IIS 7 differs from the procedure needed with IIS 6. By default, IIS 7 uses a new feature called **Kernel-mode authentication**. This feature streamlines the

Kerberos ticket requesting process such that you no longer need to manually register an SPN for the application pool identity when the IIS application pool is running under that custom domain user.

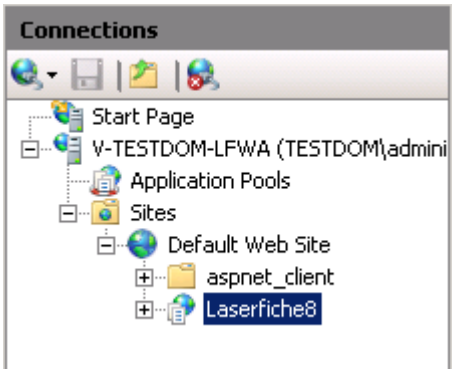
2. Basic Configuration

This section covers steps that must be performed regardless of the specifics of your Laserfiche or network configuration:

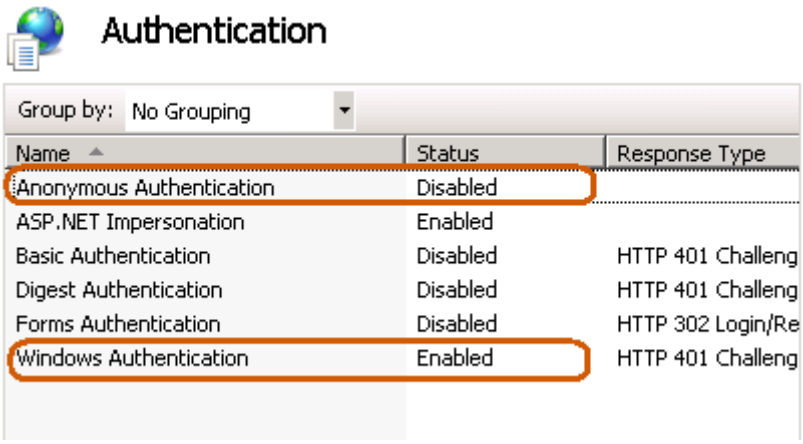
1. Configure IIS to disable anonymous authentication and enable Windows authentication.
2. Configure your Laserfiche repository to trust Windows accounts to log in to the repository.

2.1 Configuring IIS to enable Windows Authentication

1. On the Web Access 8 host computer, Click **Start**, point to **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.
2. In the IIS Manager, expand the tree until you see the Web Access 8 application. By default, the application is named **Laserfiche8**.
3. Click on the **Laserfiche8** item.



4. In the main workspace area, find and double-click the **Authentication** item.
5. In **Authentication**, make sure that the **Anonymous Authentication** item is disabled and that the **Windows Authentication** item is enabled.



2.2 Configure your Laserfiche repository to trust Windows accounts to log in to the repository

1. Load the Laserfiche 8 Administration Console and connect to your repository.
2. Expand the **Users and Groups** item.
3. Select the **Windows Accounts** item.
4. From the **Action** menu, click **New Windows Account**.
5. In the Windows account text box, specify the Windows user or group account that you wish to allow access to the Laserfiche repository.
6. In the Authentication section, select the **Trust: allow access** option.
7. Click **OK** to save your changes.

3. Delegation for the Web Server

By default, when Kernel-mode authentication is enabled, you only need to trust the Web Access host computer for Kerberos delegation.

3.1 Configure Active Directory such that the Web Access host computer is trusted for Kerberos delegation

1. On the domain controller, click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Expand the item for your domain and select the **Computers** item.
3. Locate the computer that is hosting Web Access and view its properties.

4. On the **Delegation** tab, select the **Trust this computer for delegation to any service (Kerberos only)** option.
5. Click **OK** to save your changes.

At this point, if you have performed the steps in section 2 and Laserfiche Server is running under the Local System account, you are finished with enabling Kerberos authentication.

Reminder: IIS 7's Kernel-mode authentication removes almost all situations where you need to manually register SPNs for the application pool identity. This means that even if the identity for the application pool is a domain account, you do not need to register SVNs for that application pool domain account.

This feature is a major departure from IIS 6.0. Please be aware that when dealing with Kerberos configuration, performing IIS 6 instructions with IIS 7 may actually break Kerberos. Due to Kernel-mode authentication, manually registering additional HTTP SPNs for the application pool identity results in duplicate SPNs and prevent Kerberos from functioning.

4. SPN Registration for the Laserfiche Service User (Optional)

The Laserfiche Server can run under the Local System account. When the service runs under the Local System account, you do not need to register SPNs for the Laserfiche Server. SPN registration only becomes necessary if you configure the Laserfiche Server service to run under a domain user account.

SPN registration requires domain administrator priviliges. Use the **setspn.exe** command-line utility configure SPNs.

To register SPNS for the Laserfiche Server Service user

1. As a domain administrator, click **Start** and click **Command Prompt**.
2. Type the following and press ENTER to register the HTTP/*MyLFServer* SPN for the *LFServiceUser* domain account:

   setspn –a HTTP/*MyLFServer LFServiceUser*
3. Repeat the above step with the following commands:

setspn –a HTTP/*MyLFServer.mydomain*.com *LFServiceUser*

setspn –a LaserficheServer/*MyLFServer LFServiceUser*

setspn –a LaserficheServer/*MyLFServer.mydomain*.com *LFServiceUser*

5. Delegation and SPN Registration for the Application Pool Identity (Optional)

By default, Kernel-mode authentication removes the need to worry about the IIS application pool identity for Web Access. You can still choose to set the identity to run as either a domain user account or run as the default Network Service account. However, with Kernel-mode authentication, even if you do choose to configure the application pool to run as a domain user account, you should not need to enable delegation or create SPNs for that user account.

However, certain network configurations may prevent you from using the machine account for Kerberos ticket decryption (e.g., when running IIS in a Web farm). Or you may explicitly want to use the application pool's identity for Kerberos ticket decryption. If you have both configured the Web Access 8 application pool to use a domain identity and you want Kerberos ticket decryption to use that domain identity, you will have to:

- Configure IIS 7 to authenticate using the application pool identity.
- Register SPNs for the application pool identity.
- Trust the application pool identity for Kerberos delegation.

5.1 Configure IIS 7 to authenticate using the application pool identity

Modify the IIS 7 **ApplicationHost.config** file. The file is located at "C:\Windows\System32\inetsrv\config."

Add the "useAppPoolCredentials" attribute to the <windowsAuthentication> element. The final config file should look similar to the following:

```
<system.webServer>
  <security>
    <authentication>
      <windowsAuthentication enabled=”true” user KernelMode=”true”
        useAppPoolCredentials=”true” />
    </authentication>
```

```
    </security>
</system.webServer>
```

For more information, see the following Microsoft article:

http://blogs.msdn.com/webtopics/archive/2009/01/19/service-principal-name-spn-checklist-for-kerberos-authentication-with-iis-7-0.aspx

5.2 Register SPNs for the application pool identity

Register HTTP/*WebServerName* SPNs for the application pool identity. SPN registration requires domain administrator priviliges. Use the **setspn.exe** command-line utility configure SPNs.

To register SPNs for the application pool identity

1. As a domain administrator, click **Start** and click **Command Prompt**.
2. Type the following and press ENTER to register the HTTP/*WebServerName* SPN for the *ApplicationPoolIdentity* domain account:

   setspn –a HTTP/*WebServerName AppPoolUser*
3. Type the following and press ENTER to register the HTTP/*WebServerName.fully-qualified-name* SPN:

   setspn –a HTTP/*WebServerName.domain.com AppPoolUser*

5.3 Trust the application pool identity for Kerberos delegation

1. On the domain controller, click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Expand the item for your domain and select the **Users** item.
3. Select the user acting as the Web Access application pool identity and view its properties.
4. On the **Delegation** tab, select the **Trust this user for delegation to any service (Kerberos only)** option.
5. Click **OK** to save your changes.

6. Troubleshooting Resources

6.1 Understanding Kerberos

Please see the following Microsoft Technet article for a detailed look at the Microsoft Kerberos implementation.

http://technet.microsoft.com/en-us/library/cc772815.aspx

6.2 Logging Kerberos Events to the Windows Event Log

You can modify the registry to enable Windows to write Kerberos-related events to the Windows event log. You can view Kerberos-related events in the system log.

In the

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

registry key, create a DWORD registry value named

LogLevel

Set the value to 1.

For more information, see the following Microsoft Knowledge Base article:

http://support.microsoft.com/kb/262177

6.3 Removing Duplicate SPNs

Service principal names (SPN) must be unique. Duplicate service principal names will prevent Kerberos authentication from properly functioning.

You can use the **setspn.exe** command-line utility to identify and remove duplicate SPNs.

To identify duplicate SPNs

1. As a domain administrator, click **Start** and click **Command Prompt**.
2. Type the following and press ENTER to display any duplicate SPNs:

   Setspn –x

To remove an SPN

1. As a domain administrator, Click **Start** and click **Command Prompt**.
2. Type the following and press ENTER to remove the specified SPN:

   Setspn –D <*SPN*> <*User/Computer Name*>

For example, if the "setspn –x" command showed that the "HTTP/*MyLFServer"* SPN was registered on two accounts: *LFServiceUser* and *IISAppPoolUser*, and the SPN should only be registered on *LFServiceUser*, you would use the following command:

Setspn –D HTTP/*MyLFServer IISAppPoolUser*

Active Directory Explorer

The Microsoft Windows Sysinternals group provides a utility with a graphical user interface for viewing and editing Active Directory objects. See the following link to download Active Directory Explorer.

http://technet.microsoft.com/en-us/sysinternals/bb963907.aspx

You can use Active Directory Explorer to identify and delete duplicate SPNs.

6.4 Viewing and Purging Kerberos Ticket Information

It can also be useful during troubleshooting to be able to view and purge Kerberos ticket information. The Windows Server 2003 Resource Kit Tools include two utilities—Kerbtray.exe and Klist.exe—that provide those capabilities.

Both utilities allow you to view Kerberos ticket information and purge tickets. Kerbtray.exe uses a graphical user interface while Klist.exe is a command-line utility. Klist.exe is slightly more flexible as it allows you to purge an individual ticket while Kerbtray.exe can only purge all tickets on the computer.

See the following Microsoft Download page for details on downloading Kerbtray.exe and Klist.exe.

http://www.microsoft.com/downloads/details.aspx?familyid=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en

6.5 Analyzing Packets

One final option for diagnosing Kerberos problems is to analyze the network traffic between the affected computers. Using your preferred packet analyzer, you can filter for traffic on ports 80 and 88 and see what happens when you try to log in to Web Access.

One commonly used network protocol analyzer is Wireshark. See the following link for more information.

http://www.wireshark.org/

Laserfiche®

Article Title

February 2009

Author: Roger Wu

Editor: Tammy Kaehler

Technical Editor: Michael Allen, David Hale

Compulink Management Center, Inc.

Global Headquarters

3545 Long Beach Blvd.

Long Beach, CA 90807

U.S.A

Phone: +1.562.988.1688

www.laserfiche.com