



Configuring Apache Web Server For Single Sign-On with Likewise 5

IN THIS DOCUMENT

- Setting up an Apache HTTP Server for single sign-on with Likewise 5, Kerberos, and Active Directory.
- Likewise's Apache authentication architecture.
- Generating a keytab file.
- Troubleshooting authentication.
- Dealing with common issues.

REQUIREMENTS

- An Apache HTTP Server 2.0 or 2.2 that supports dynamically loaded modules.
- Likewise Open 5.0 or Likewise Enterprise 5.0, build 3946 or later.
- The Linux or Unix computer running Apache must be using a platform that Likewise supports.
- The Linux or Unix computer that is hosting the Apache web server is joined to Active Directory with Likewise.

Abstract

Likewise Enterprise 5 lets you join Linux and Unix computers running the Apache HTTP Server to Microsoft Active Directory, yielding a range of benefits for users, system administrators, and managers.

Users get single sign-on: They log on once to a workstation that is authenticated through Active Directory and automatically receive Kerberos-based single sign-on for other computers and applications, including the Apache web server. System administrators rest easy with the knowledge that users accessing your intranet through HTTP are securely authenticated with Kerberos 5 and authorized for access to the resources on your Apache web server. Managers see their operational costs drop as their Linux and Unix computers running Apache are centrally managed within Active Directory. Security managers find help in their quest for regulatory compliance.

[This document describes how to configure Likewise and the Apache HTTP Server to provide single sign-on authentication through Kerberos.](#)

About Likewise Enterprise

By joining Linux, Unix, and Mac computers to Active Directory – a secure, scalable, stable, and proven identity management system – Likewise Enterprise gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with group policies. Likewise includes reporting and auditing capabilities that can help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.

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

These documents are for informational purposes only. LIKEWISE SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software
15395 SE 30th Place, Suite #140
Bellevue, WA 98007
USA



Table of Contents

| | |
|---|-----------|
| Introduction | 4 |
| Requirements..... | 4 |
| Configure Apache HTTP Server 2.2 for SSO | 6 |
| Configure Firefox for SSO..... | 8 |
| Configure Internet Explorer for SSO | 10 |
| Troubleshooting..... | 11 |
| Apache Log File | 12 |
| The Microsoft Kerbtray Utility | 12 |
| Klist | 12 |
| Common Problems | 12 |
| Contact Technical Support | 15 |

Introduction

This document describes how to configure Likewise and the Apache HTTP Server to provide single sign-on authentication through Active Directory with Kerberos 5. The instructions assume that you know how to administer Active Directory, the Apache HTTP Server, and computers running Linux.

Single sign-on for the Apache HTTP server uses the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos. SPNEGO is an Internet standard documented in RFC 2478 at <http://www.ietf.org/rfc/rfc2478.txt> and is commonly referred to as the "negotiate" authentication protocol. The Likewise `mod_auth_kerb` module lets an Apache web server running on a Linux or Unix system authenticate and authorize users based on their Active Directory domain credentials.

Important: This topic assumes that you have installed either Likewise Open 5.0 or Likewise Enterprise 5.0, build **3946** or later, on the Linux computer running your Apache HTTP Server and that you have joined the server to Active Directory. With build 3946, Likewise 5.0 began to include the Apache `mod_auth_kerb` module in `/opt/likewise/apache`; the Likewise version of the `mod_auth_kerb` module is required to configure your Apache HTTP Server for single sign-on.

To check whether your build of Likewise Enterprise 5.0 or Likewise Open 5.0 includes `mod_auth_kerb`, confirm that the following components exist:

```
/opt/likewise/apache/2.0/mod_auth_kerb.a  
/opt/likewise/apache/2.0/mod_auth_kerb.so  
/opt/likewise/apache/2.2/mod_auth_kerb.a  
/opt/likewise/apache/2.2/mod_auth_kerb.so
```

Requirements

Likewise Open 5.0 or later or Likewise Enterprise 5.0 or later, build 3946 or later.

- The Linux or Unix computer that is hosting the Apache web server is joined to Active Directory.
- An Apache HTTP Server 2.0 or 2.2 that supports dynamically loaded modules. To check whether your Apache web server supports



dynamically loaded modules, execute the following command and verify that `mod_so.c` appears in the list of compiled modules:

```
httpd -l
```

```
Compiled in modules:
```

```
core.c
```

```
prefork.c
```

```
http_core.c
```

```
mod_so.c
```

For Apache installations that are compiled from the source code, make sure that `--enable-module=so` is specified when `./configure` is executed:

```
./configure --enable-module=so
```

- Your Kerberos libraries must support SPNEGO. For example, MIT Kerberos libraries that are version 1.5 and later support SPNEGO; earlier versions do not. Make sure your Kerberos libraries support SPNEGO by running `ldd`:

```
which httpd
/usr/sbin/httpd
ldd /usr/sbin/httpd
```

In the results, find the line that references `libgssapi`:

```
libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.so.2 (0x00231000)
```

Finally, query the version number of the library and make sure it is **1.5 or later**:

```
rpm -qif /usr/lib/libgssapi_krb5.so.2
```

```
Name       : krb5-libs                               Relocations: (not relocatable)
Version    : 1.5                                     Vendor: Red Hat, Inc.
Release    : 17                                     Build Date: Tue 16 Jan 2007 10:01:00 AM PST
Install Date: Fri 14 Dec 2007 09:09:44 AM PST      Build Host: ls20-bc1-13.build.redhat.com
Group      : System Environment/Libraries          Source RPM: krb5-1.5-17.src.rpm
Size       : 1333337                                License: MIT, freely distributable.
Signature  : DSA/SHA1, Wed 17 Jan 2007 10:57:33 AM PST, Key ID 5326810137017186
Packager   : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
URL        : http://web.mit.edu/kerberos/www/
Summary    : The shared libraries used by Kerberos 5.
Description:
Kerberos is a network authentication system. The krb5-libs package
contains the shared libraries needed by Kerberos 5. If you are using
Kerberos, you need to install this package.
[root@rhel5d sbin]#
```

Configure Apache HTTP Server 2.2 for SSO on RHEL 5

The following instructions demonstrate how to configure Likewise and Apache for SSO on a Red Hat Enterprise Linux 5 computer. The steps vary by operating system and by Apache version. Ubuntu, in particular, uses `apache2` instead of `httpd` for commands, the name of the daemon, the configuration directory, the name of the configuration file, and so forth.

Important: Configuring web servers is complex. Before you deploy your configuration to a production web server, implement and test it in a test environment. More: Before you change your web server's configuration, read and understand the Apache HTTP Server documentation at <http://httpd.apache.org/docs/> and the `mod_auth_kerb` documentation at <http://modauthkerb.sourceforge.net/configure.html>.

1. Determine whether your Apache server is 2.0 or 2.2:

```
httpd -v
```

```
Server version: Apache/2.2.3
Server built:   Nov 29 2006 06:33:19
```

2. Edit your Apache configuration file --
`/etc/httpd/conf/httpd.conf` -- to add a directive to load the Likewise `auth_kerb_module` for your version of Apache. Since my Red Hat computer is running Apache 2.2.3, I have added the 2.2 version of the module to the list after the other `auth` modules (which were already listed in the file):

```
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_kerb_module
/opt/likewise/apache/2.2/mod_auth_kerb.so
```

3. In `/etc/httpd/conf/httpd.conf`, configure authentication for a directory and then restart the web server; example:

```
<Directory "/var/www/html/secure">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
Allow from 127.0.0.0/255.0.0.0 ::1/128
AuthType Kerberos
AuthName "Kerberos Login"
KrbAuthRealms LIKewiseDEMO.COM
Krb5Keytab /etc/apache2/http.ktb
Require valid-user
</Directory>
```

4. Configure your web server for Secure Socket Layer (SSL).

Important: If SSO fails and you have not turned on SSL, your server will prompt you for an ID and password -- which will be sent in clear text. SSL encrypts all data that passes between the client browser and the web server. SSL can also perform Basic Authentication in a secure fashion, providing a fallback mechanism in the event that Kerberos authentication fails. Using SSL is especially important if the protected web site also needs to be accessible from outside the corporate network. For more information, see <http://modauthkerb.sourceforge.net/configure.html>.

5. In Active Directory, create a user account for the Apache web server in the same OU (or, with Likewise Enterprise, cell) to which the Linux computer hosting the web server is joined. Set the password of the user account to never expire. In the examples

that follow, the user account for my Apache web server is named httpUser.

6. On the domain controller, create an RC4-HMAC keytab for the Apache web server by using Microsoft's ktpass utility. For information on ktpass, see <http://technet.microsoft.com/en-us/library/cc776746.aspx>. Example:

```
C:\>ktpass /out keytabfile /princ
HTTP/rhel5d.likewisedemo.com@LIKEWISEDEMO.COM
/pass SkiAlta2008 /mapuser likewisedemo\httpUser
Targeting domain controller: steveh-
dc.likewisedemo.com
Using legacy password setting method
Successfully mapped HTTP/rhel5d.likewisedemo.com
to httpUser.
Key created.
Output keytab to keytabfile:
Keytab version: 0x502
keysize 80
HTTP/rhel5d.likewisedemo.com@LIKEWISEDEMO.COM
ptype 0 (KRB5_NT_UNKNOWN) vno 3 etype 0x17 (RC4-
HMAC) keylength 16
(0x2998807dc299940e2c6c81a08315c596)
```

7. Use secure FTP or another method to transfer the keytab file to the Linux computer that hosts your Apache web server and place the file in the location specified in your <Directory> configuration in httpd.conf. For example, using the configuration shown in Step 3 above, the keytab file would be placed in /etc/apache2/http.ktb.
8. Set the permissions of the keytab file to be readable by the ID under which the Apache web server runs and no one else.

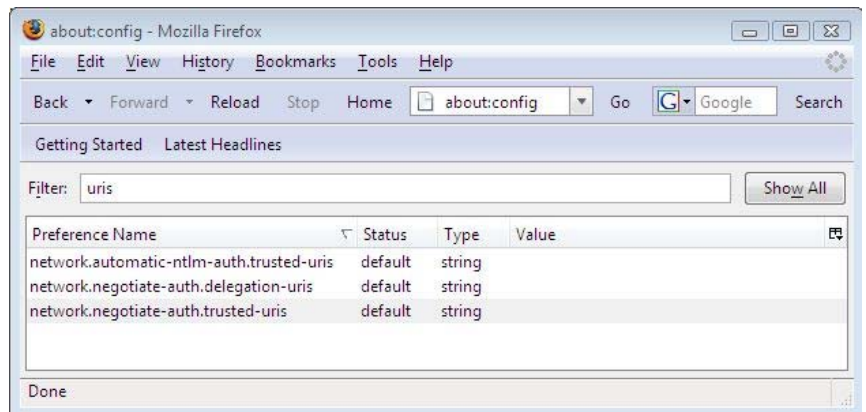
Important: The Kerberos keytab file is necessary to authenticate incoming requests. It contains an encrypted, local copy of the host's key and, if compromised, might allow unrestricted access to the host computer. It is therefore crucial to protect it with file-access permissions.

[Configure Firefox for SSO](#)



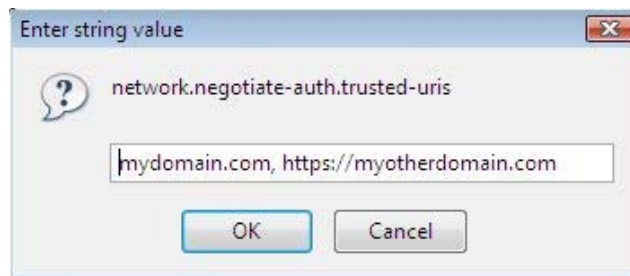
To set up Firefox for single sign-on, you must turn on the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos.

1. Open Firefox.
2. In the **Go** box, type `about:config`, and then click **Go**.
3. In the **Filter** box, type `uris`.



4. Double-click **`network.negotiate-auth.trused-uris`**, enter a comma-separated list of URL prefixes or domains that are permitted to engage in SPNEGO authentication with the browser, and then click **OK**:

Example:



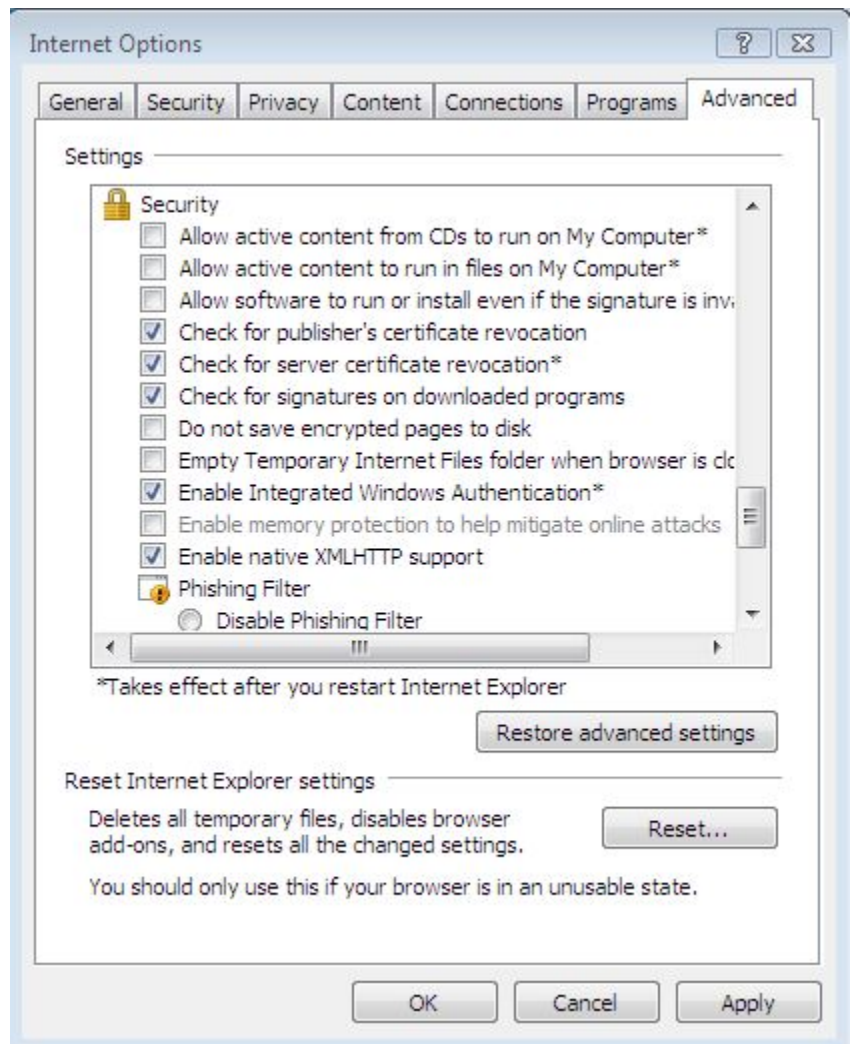
5. Double-click **`network.negotiate-auth.delegation-uris`**, enter a comma-separated list of the sites for which the browser may delegate user authorization to the server, and then click **OK**.

For more information on how to configure Firefox, see <http://grolmsnet.de/kerbtut/firefox.html>.

Configure Internet Explorer for SSO

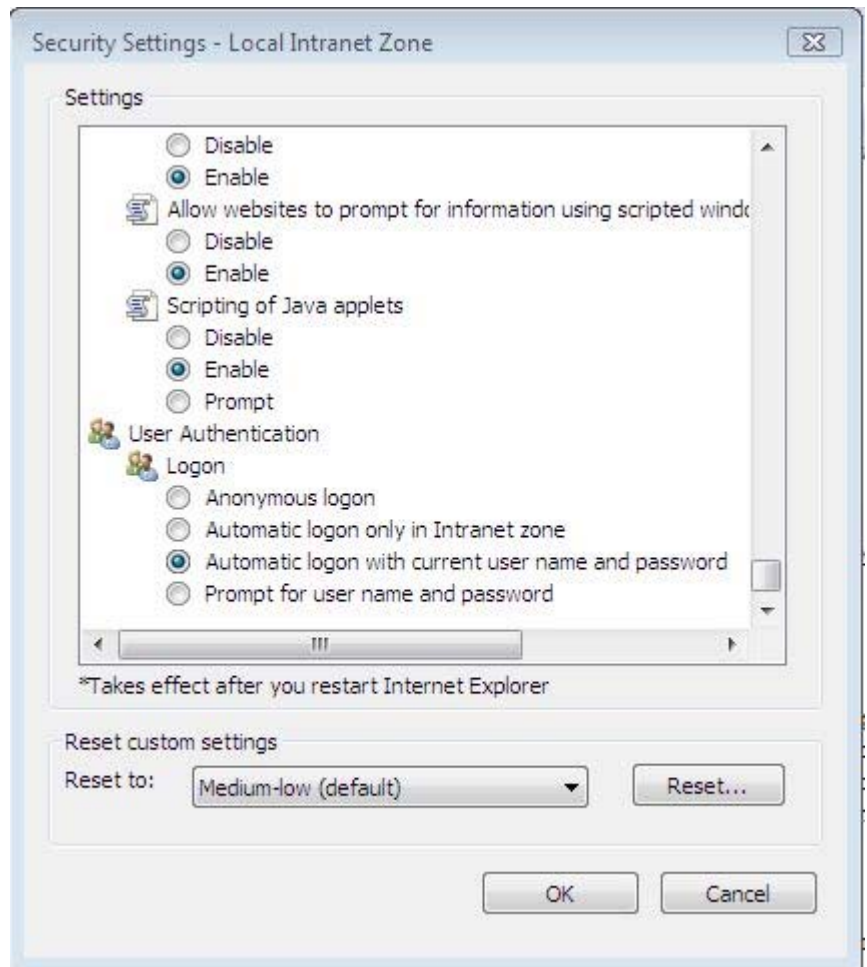
Here's how to configure Internet Explorer 7.0 to use SPNEGO and Kerberos. The settings for other versions of IE might vary; see your browser's documentation for more information.

1. Start Internet Explorer 7.0.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Advanced** tab and make sure that the **Enable Integrated Windows Authentication** box is selected:



4. Click the **Security** tab.

5. Select a zone -- for example, **Local intranet** -- and then click **Custom level**.
6. In the **Settings** list, under **User Authentication**, click **Automatic logon with current user name and password** for a trusted site, or **Automatic logon only in Intranet zone** for a site you added to IE's list of Intranet sites. For more information, see your browser's documentation.



7. Return to the **Security** tab for **Internet Options** and set your web server as a trusted site.
8. Restart Internet Explorer.

There are some tools that can help diagnose problems with Kerberos authentication.

Apache Log File

The location of the Apache error logs is specified in the Apache configuration file under the `ErrorLog` directive. Example directive from `/etc/httpd/conf/httpd.conf` on RHEL 5:

```
ErrorLog logs/error_log
```

The Microsoft Kerbtray Utility

The Microsoft `Kerbtray.exe` utility, part of the Windows 2000 Resource Kit, can verify whether Internet Explorer obtained a Kerberos ticket for your web server. You can download the utility at the following URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en>

Klist

You can use the `klist` utility in `/opt/likewise/bin/klist` to check the Kerberos keytab file on a Linux or Unix computer. The command shows all the service principal tickets contained in the keytab file so you can verify that the correct service principal names appear. Confirm that `HTTP/myserver@MYDOMAIN.COM` and `HTTP/myserver.mydomain.com@MYDOMAIN.COM` appear in the list. It is normal to see multiple entries for the same name.

Example:

```
klist -k krb5_myserver.keytab
Keytab name: FILE:krb5_myserver.keytab
KVNO Principal
-----
-----
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
```

If your service principal names are incorrect, generate a new Kerberos keytab file.

Common Problems

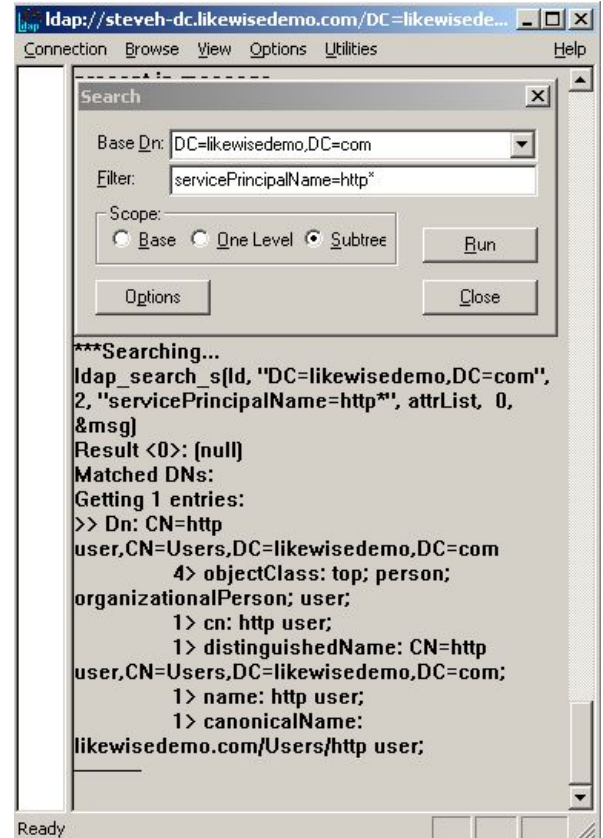


Authentication problems can be difficult to diagnose. First, check all the configuration parameters, including the validity of the keytab file. Second, make sure none of the common problems listed in the following table are sabotaging authentication.

| Problem | Solution |
|--|--|
| The system's clock is out of sync. | The Kerberos standard requires that system clocks be no more than 5 minutes apart. Make sure that the system clocks on the Active Directory domain controller, the Linux or Unix web server, and the client are synchronized. |
| The user accessing the web site is not on the require list | <p>If Kerberos ticket was obtained on the client or the user correctly entered his credentials during the Basic Authentication prompt, it might be because authentication worked but the authorization failed. If so, the Apache error_log will contain a line like this:</p> <pre>access to / failed, reason: user MYDOMAIN\user not allowed access</pre> <p>Add the user to the require user directive or add the user's group to the require group directive.</p> |
| The user accessing the web site is logged on the wrong domain. | <p>If the client user is logged on a domain different from the domain of the web server, one of two things will happen:</p> <p>If the KrbMethodK5Passwd directive is set to on, or was not specified and thus defaults to on, the user will be prompted for credentials.</p> <p>If KrbMethodK5Passwd is set to off, authentication will fail and the Authorization Required page will be displayed.</p> |
| Internet Explorer does | This problem commonly occurs when the |

| | |
|--|--|
| <p>not consider the URL to be part of the Local Intranet zone or the Trusted sites.</p> | <p>web site is accessed by using a URL that includes the full domain name, such as <code>https://myserver.mydomain.com</code>. Internet Explorer tries to obtain Kerberos tickets only for web sites that are in the Local Intranet zone.</p> <p>Try to access the web site by using only the server name, for example <code>https://myserver</code>.</p> <p>Or, you can add the URL to a list of Local Intranet sites or the trusted sites by changing your options in Internet Explorer.</p> |
| <p>The service principal name of the web site is mapped to more than one object in the Active Directory.</p> | <p>Although this problem is rare, it is difficult to diagnose because the error messages are vague. The problem can occur after the <code>ktpass</code> utility was used repeatedly to generate a Kerberos keytab file for the web server.</p> <p>To check for this problem, log on your Active Directory domain controller and open the Event Viewer. Look for an event of type=Error, source=KDC, and event ID=11. The text of the event will be similar to the message below:</p> <p>There are multiple accounts with name <code>HTTP/myserver.mydomain.com</code> of type <code>DS_SERVICE_PRINCIPAL_NAME</code>.</p> <p>To fix the problem, find the computer or user objects that were used to map the service principal name in Active Directory and then use the ADSI Edit to manually remove the <code>"HTTP/myserver.mydomain.com"</code> string from the <code>servicePrincipalName</code> object property.</p> <p>Example of how to find an object named</p> |

HTTP by using Ldap:



Contact Technical Support

For either post-sales technical support or for free technical support during an evaluation period, please visit the Likewise support web page at <http://www.likewise.com/support/>. You can use the support page to register for support, submit incidents, and receive direct technical assistance.

Technical support may ask for your Likewise version, Linux version, and Microsoft Windows version. To find the Likewise product version, in the Likewise Console, on the menu bar, click **Help**, and then click **About**.

ABOUT LIKEWISE

Likewise Software is an open source company that provides audit and authentication solutions designed to improve security, reduce operational costs and help demonstrate regulatory compliance in mixed network environments. Likewise Open allows large organizations to securely authenticate Linux, UNIX and Mac systems with a unified directory such as Microsoft Active Directory. Additionally, Likewise Enterprise includes world-class group policy, audit and reporting modules.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.