# Configuration Guide for Kerberos Deployment of Cisco Unified Videoconferencing Manager Release 7.1

March 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000

Text Part Number: OL-22424-01

*Configuration Guide for Kerberos Deployment of Cisco Unified Videoconferencing Manager Release 7.1*

# CONTENTS

CHAPTER 1

# Deploying Kerberos for Cisco Unified Videoconferencing Manager



## Establishing a Secure Connection

Kerberos is an authentication protocol for nodes communicating over a non-secure network to securely authenticate their identities. Authentication is performed using shared secret keys that can be securely transmitted over an insecure network.

The following parties are involved in the Kerberos authentication:

- Client—The system or user making the request.
- Server—The system that offers a service to systems whose identity can be confirmed.
- Key Distribution Center (KDC)—The system that authenticates credentials and grants service tickets.

When the Kerberos protocol is deployed, a client-to-Cisco Unified Videoconferencing Manager connection is established using this procedure.

**Procedure**

**Step 1** In a browser, enter the address for the Cisco Unified Videoconferencing Manager Administration Web User Interface which is a secured page.

The Cisco Unified Videoconferencing Manager server responds with the “401 Unauthorized” error message.

**Step 2** The browser automatically sends a new modified request to the KDC to request a service ticket.

**Step 3** The browser uses the service ticket to resend a request for connection to the Cisco Unified Videoconferencing Manager.

**Note** By default the service ticket expires after five minutes. This expiry date is configured in the KDC.

**Step 4** The Cisco Unified Videoconferencing Manager server validates the service ticket.

If validation succeeds, the requested page of the Cisco Unified Videoconferencing Manager Administrator web user interface is displayed. If validation fails, the login page is displayed.

**Note** If the browser prompts for a username and password, check the browser security settings. For more information, see "Verifying Browser Settings" section on page 1-2.

# Verifying Browser Settings

Follow this procedure to prepare your internet browser for Kerberos secure connection with the Cisco Unified Videoconferencing Manager Server.

**Procedure**

**Step 1** Select **Tools > Options** in Microsoft Internet Explorer.

**Step 2** Select the **Security** tab.

**Step 3** Select **Local intranet**.

**Step 4** Select **Sites**.

**Step 5** Select the **Advanced** button.

**Step 6** Enter the URL of the Cisco Unified Videoconferencing Manager Server.

**Step 7** Select **Add**.

**Step 8** Select **Close**.

**Step 9** Select **Custom Level**.

**Step 10** Verify **Automatic login only in Intranet zone** is selected under User Authentication > Logon.

**Step 11** Click **OK**.

**Step 12** Select the **Advanced** tab.

**Step 13** Verify **Enable Integrated Windows Authentication (requires restart)** is selected.

**Step 14** Select **OK**.

**Step 15** Select **OK**.

# How to Configure Cisco Unified Videoconferencing Manager to Use Kerberos Protocol



## Creating an Account for Cisco Unified Videoconferencing Manager Server

This procedure describes how to create an account for the Cisco Unified Videoconferencing Manager Server.

### Before You Begin

- Verify the DNS domain name of the Cisco Unified Videoconferencing Manager Server.
- Verify the full hostname (FQDN) of the Cisco Unified Videoconferencing Manager Server.

### Procedure

**Step 1** Select **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

**Step 2** In the left pane, right-click **Users**, and then select **New > User**.

**Step 3** In the New Object - User dialog box, enter the account name for the Cisco Unified Videoconferencing Manager Server.

**Step 4** Click **Next**.

**Step 5** Enter the password.

**Step 6** Select **User cannot change password** option.

**Step 7** Select **Password never expires** option.

**Step 8** Click **Next**.

**Step 9** Click **Finish**.

# Generating a Keytab File

A Kerberos keytab configuration file contains these elements:

- A list of keys analogous to user passwords
- An automatically generated Service Principle Name (SPN) which concatenates the username configured in Creating an Account for Cisco Unified Videoconferencing Manager Server, page 1-3 with the realm.

**Note** A realm is a Kerberos term for the name of a region in which users and services share keys with the Key Distribution Center (KDC). Typically the name is the DNS name in upper case characters.

**Procedure**

**Step 1** Download the Ktpass utility from http://support.microsoft.com/kb/892777 to the Domain Controller.

**Step 2** Start the Ktpass utility.

The command-line interface opens.

**Step 3** Enter this single-line command:

```
C:\>ktpass -princ HTTP/iviewcuvcmserver.dnsname.com@DNSNAME.COM
-mapuser iviewcuvcmserver -pass password -out iviewcuvcmserver.keytab
-crypto rc4-hmac-nt
```

Where

- -princ specifies the name of the SPN, typically composed of the service name, the hostname and the name of the realm. For example, HTTP/iviewcuvcmserver.dnsname.com@DNSNAME.COM.
- -mapuser specifies the user account you created in "Creating an Account for Cisco Unified Videoconferencing Manager Server" section on page 1-3.
- -pass specifies the password.
- -out specifies the name of the keytab file that the Ktpass utility will generate.
- -crypto specifies the cryptographic algorithm the Ktpass utility will use.

**Step 4** Verify that the value of the userPrincipalName attribute in the Active Directory is changed to the same value as the SPN.

**Step 5** Close the command-line interface.

# Verifying a Keytab File

Use the vnexauth.jar utility to verify the generated keytab file if the Kerberos deployment fails to access to the Cisco Unified Videoconferencing Manager.

**Procedure**

**Step 1** Copy the vnexauth.jar file from <Cisco Unified Videoconferencing Manager installation directory>\jboss\server\default\deploy\jbossweb-tomcat55.sar to the location of the keytab file.

**Step 2** Open a command line window.

**Step 3** Enter this command:

```
"<installation directory>\jre_rt\bin\java" -jar vnexauth.jar
<keytab_filename> <address of KDC>
```

The ticket is initialized for the Cisco Unified Videoconferencing Manager Server.

**Step 4** Check the output of the utility to verify the validity of the keytab file:

- The keytab file is valid if the utility confirms that a new ticket is stored in cache file.
- The keytab is not valid if the utility outputs an error stating the identifier does not match the expected value.

# Configuring Cisco Unified Videoconferencing Manager Server for Kerberos

To configure the Cisco Unified Videoconferencing Manager Server for Kerberos, copy the generated keytab file from "Generating a Keytab File" section on page 1-4 to the Cisco Unified Videoconferencing Manager Server.

**Note** Protect the keytab file by storing it on the local disk, to ensure that unauthorized users cannot access it.

**Procedure**

**Step 1** Copy the keytab file generated in the "Generating a Keytab File" section on page 1-4 from the Domain Controller to a directory on the Cisco Unified Videoconferencing Manager Server.

Each keytab file enables one realm to access the Cisco Unified Videoconferencing Manager Server.

For multiple realm access, copy each realm's keytab file into the same directory.

**Note** The keytab file is a binary file. You must transfer it in a way that does not corrupt it.

For example, c:/iviewcuvcmshare.

**Step 2** Create a new text file in the same directory called krb5.conf.

**Step 3** Populate the file with this text:

```
[libdefaults]
default_tkt_enctypes =rc4-hmac
default_tgs_enctypes =rc4-hmac
```

Where

- default_tkt_enctypes and default_tgs_enctypes define the supported session key encryption types.
- rc4-hmac is the default encyption type used by Active Directory server.

**Step 4** Save the file.

**Step 5** Open the *authentication.properties* file, located by default in C:\Program Files\RADVISIONcisco\iVIEW Suitecuvcm\iCM\jboss\bin.

**Step 6** Add these lines to the end of the file:

```
java.security.krb5.conf=c:/iviewcuvcmshare/krb5.conf
vnex.kerberos.keytab.root=c:/iviewcuvcmshare
vnex.kerberos.keytab.list=iviewcuvcmserver.keytab
```

**Note** For multiple realm access, list each of the keytab filenames in the last line, separated by commas.

**Step 7** Restart the Cisco Unified Videoconferencing Manager Server.

**Step 8** To test that the Cisco Unified Videoconferencing Manager Server is correctly configured to use Kerberos protocol:

**a.** Access the Cisco Unified Videoconferencing Manager Administrator web user interface from a different computer.

In this example, use the address http://iviewcuvcmserver.dnsname.com:8080.

**b.** Verify that no errors occur during sign-in.