

Enabling Kerberos in SCOPIA iVIEW Management Suite

Installation Guide Version 7.5



© 2000-2010 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd retains all rights not expressly granted.

This publication is RADVISION confidential. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

For further information contact RADVISION or your local distributor or reseller.

Installation Guide for Enabling Kerberos in SCOPIA iVIEW Management Suite Version 7.5, October 2010

<http://www.radvision.com>

Table of Contents

1 Deploying Kerberos for SCOPIA iVIEW Management Suite

Establishing a Secure Connection	1
Verifying Browser Settings.....	2
How to Configure iVIEW Management Suite to Use Kerberos Protocol	3
Creating an Account for iVIEW Management Suite Server	3
Generating a Keytab File	3
Verifying a Keytab File	4
Configuring iVIEW Management Suite Server for Kerberos	5

1

Deploying Kerberos for SCOPIA iVIEW Management Suite

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.

The sections in this chapter describe the procedures required to set up this protocol with SCOPIA iVIEW Management Suite.

- [Establishing a Secure Connection](#) page 1
- [Verifying Browser Settings](#) page 2
- [How to Configure iVIEW Management Suite to Use Kerberos Protocol](#) page 3

Establishing a Secure Connection

When the Kerberos protocol is deployed, a client-to-SCOPIA iVIEW Management Suite connection is established using this procedure.

Procedure

- Step 1** In a browser, enter the address for the iVIEW Management Suite Administration Web User Interface which is a secured page.
- The iVIEW Management Suite 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 iVIEW Management Suite.

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

Step 4 The iVIEW Management Suite server validates the service ticket.
If validation succeeds, the requested page of the iVIEW Management Suite 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” on page 2](#).

Verifying Browser Settings

Follow this procedure to prepare your internet browser for Kerberos secure connection with the iVIEW Management Suite 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 iVIEW Management Suite 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 iVIEW Management Suite to Use Kerberos Protocol

- [Creating an Account for iVIEW Management Suite Server](#) page 3
- [Generating a Keytab File](#)..... page 3
- [Verifying a Keytab File](#) page 4
- [Configuring iVIEW Management Suite Server for Kerberos](#) page 5

Creating an Account for iVIEW Management Suite Server

This procedure describes how to create an account for the iVIEW Management Suite Server.

Before You Begin

- Verify the DNS domain name of the iVIEW Management Suite Server.
- Verify the full hostname (FQDN) of the iVIEW Management Suite 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 iVIEW Management Suite 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 iVIEW Management Suite Server page 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/iviewserver.dnsname.com@DNSNAME.COM -mapuser iviewserver -pass password -out iviewserver.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/iviewserver.dnsname.com@DNSNAME.COM.
 - -mapuser specifies the user account you created in [“Creating an Account for iVIEW Management Suite Server” on page 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 iVIEW Management Suite.

Procedure

- Step 1** Copy the vnexauth.jar file from <iVIEW Management Suite 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 iVIEW Management Suite 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 iVIEW Management Suite Server for Kerberos

To configure the iVIEW Management Suite Server for Kerberos, copy the generated keytab file from [“Generating a Keytab File” on page 3](#) to the iVIEW Management Suite 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” on page 3](#) from the Domain Controller to a directory on the iVIEW Management Suite Server.

Each keytab file enables one realm to access the iVIEW Management Suite 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:/iviewshare.

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 encryption 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\RADVISION\iVIEW Suite\iCM\jboss\bin.

Step 6

Add these lines to the end of the file:

```
java.security.krb5.conf=c:/iviewshare/krb5.conf  
vnex.kerberos.keytab.root=c:/iviewshare  
vnex.kerberos.keytab.list=iviewserver.keytab
```

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

Step 7

Restart the iVIEW Management Suite Server.

Step 8

To test that the iVIEW Management Suite Server is correctly configured to use Kerberos protocol:

- a. Access the iVIEW Management Suite Administrator web user interface from a different computer.

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

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



www.radvision.com

About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP and 3G networks. With its complete set of standards based video networking infrastructure and developer toolkits for voice, video, data and wireless communications, RADVISION is driving the unified communications evolution by combining the power of video, voice, data and wireless - for high definition video conferencing systems, innovative converged mobile services, and highly scalable video-enabled desktop platforms on IP, 3G and emerging next generation networks. For more information about RADVISION, visit www.radvision.com

USA/Americas

T +1 201 689 6300

F +1 201 689 6301

infoUSA@radvision.com

EMEA

T +44 20 3178 8685

F +44 20 3178 5717

infoUK@radvision.com

APAC

T +852 3472 4388

F +852 2801 4071

infoAPAC@radvision.com