Kaveman Centralized Access (KCA) User Manual

Part Number 950.0029

Revision 03

Kaveman Centralized Access User Manual

Part Number 950.0029 Revision 03

CONTENTS

Contents iv
Figures vi
Tables vii

Introduction 1
Background 1
KCA System Features 1
KCA Benefits 2
KCA System Overview 3
KCA System Components 3
Hardware components 3
Software components 4

Software Installation and Configuration 5
Hardware Requirements 5
Software Installation on the Domain Controller 5
To install the KCA software on the Domain Controller 5
To make the Kaveman.ldf file 5
To modify the schema 5
To change the schema master 6
To install the Active Directory schema Snap-in 6
To run the KCA Snap-in 6
To configure DNS entries for each Kaveman 6
Software Installation on the IIS Server 6
To install the KCA software on the IIS server 6
Creating a New Web Site 7
To create a new web site 7
To configure the new web site 8
To set the Active Server Page for Windows 2003 servers 10
KCA Bridge Configuration 10
KCA Date and Time Synchronization 11
To open the kvmconfig web page 11
To save the tsconfig.txt file 12
To save the config.asp file 12
To execute the timesync.vbs script 12
To configure a Kaveman Access Manager Account 12
To enable Cookies on the IIS Bridge (Windows 2003 Server) 13
Using SSL to Encrypt the Link Between the IIS Server and Kaveman 13
Preparing the Domain Controller 13
To download the OpenSSL for Windows toolkit into the Domain Controller 13
To create a certificate config file 13
To create a Certificate Signing Request 14
To submit a Certificate Request 15
To upload the files to Kaveman 16
To create the Root certificate 16
To get the IIS Server to trust Kaveman 16

Using the KCA Snap-In 17
How it Works 17
Three Easy Steps to Setting up Kaveman Channels 17

Creating Kaveman Objects 17
To create a Kaveman object 18
To identify the Access Manager 20
Grouping Channels 20
Editing Permissions 20
To edit permissions 21
A Simple Example 23
Channel Privilege Report 24
Contact Information 25
Index 26

FIGURES

Figure 1.1 - KCA system overview 3

Figure 2.1 - Creating a new web site 7
Figure 2.2 - Stopping the default web site 8
Figure 2.3 - Configuring the KCA web site 8
Figure 2.4 - Authenticating the KCA web site 9
Figure 2.5 - Application Pool Identities (Windows 2003) 10
Figure 2.6 - Configuring the KCA Bridge 11
Figure 2.7 - Code generated by KCA Bridge configuration 12
Figure 2.8 - Submitting a Certificate Request 15

Figure 3.1 - Kaveman Snap-in screen 18
Figure 3.2 - Creating a new Kaveman object 18
Figure 3.3 - New Kaveman dialog box 19
Figure 3.4 - Selecting Kaveman properties 19
Figure 3.5 - Grouping channels 20
Figure 3.6 - Editing Kaveman permissions 21
Figure 3.7 - Selecting user groups to assign to channels 22
Figure 3.8 - Creating Kaveman objects example 23
Figure 3.9 - Editing permissions example – Kaveman units 23
Figure 3.10 - Editing permissions example – database servers 24
Figure 3.11 - KCA Web Interface Welcome screen 24

TABLES

Table 1.1 - KCA Benefits 2

Table 3.1 - KCA Snap-in definitions 17
Table 3.2 - Summary of Editing Actions 22

1

INTRODUCTION

Background

A Digital V6 Kaveman is a KVM switch that allows up to 6 remote users access to and control of any of the attached servers using a common browser over a TCP/IP network.

Currently, each Kaveman unit is designed to work as a stand alone KVM switch with a separate internal database for user authentication and permission control. Administrators can configure specific access levels for every user for all attached channels within the switch. In an environment where multiple Kaveman switches are deployed to control a number of servers, a centralized user authentication and permission control system means convenience and easy administration of all Kaveman switches.

Using Microsoft Active Directory Services, the KCA (Kaveman Centralized Access) system allows administrators to easily configure access permissions for every channel attached to each Kaveman unit on a network. The system allows centralized access to all channels through a single point of entry, namely a web interface (KCA Web Site). A user logs into the KCA Web Site (configured by the administrator on an IIS Server), is authenticated, and is then presented with a list of channels he has access to, regardless of what Kaveman unit(s) these channels are physically attached to. The entire set of channels attached to all Kaveman units is viewed as being attached to a single virtual Kaveman with up to hundreds of channels.

For an overview of Microsoft Active Directory, please visit http://www.microsoft.com/windows2000/server/evaluation/features/dirlist.asp.

KCA System Features

Stores all user access configuration in Active Directory Tree

- Benefit from existing Microsoft Active Directory Services running on any Windows 2000/2003 Server and store all pertinent data.
- Administrator can use custom KCA Snap-in Console to create Kaveman-related objects within the directory tree. Reference existing users and groups in a tree and assign individual access rights to channels attached to all Kaveman units with a domain.

Provides users with centralized access to all Kaveman channels within a domain

- A single point of entry is provided via web interface (KCA Web Site).
- User logs into web server and is given access only to permitted channels.
- The user is redirected to the appropriate Kaveman and channel when a link on the web interface is selected.

Provides administrators with centralized access management for all channels

- Using the KCA Snap-in, an administrator can assign users/groups specific control over any channels within the entire system. The following access rights can be configured for each user/group:

  - Full Control – User/Group has full control over a channel.
  - No Power – User/Group has full control except for power control.
  - View Only – User/Group has no mouse/keyboard/power control.
- Channels can be grouped logically as well as by their respective Kaveman unit when assigning access rights.

Provides administrators with centralized management of all Kaveman units

- Administrators can manage any Kaveman directly from the KCA web interface.
- The following special features are available and can be performed on all Kaveman units:
  - Synchronize Date and Time – a script that can be executed to automatically synchronize date and time on all Kaveman units within network
  - Synchronize Channel Names – a function on the KCA web site to synchronize channel names on all Kaveman units with the names given in the Active Directory server
  - Upgrade firmware – a function on the KCA web site to upgrade firmware on all Kaveman units found in Active directory.

Provides administrators with session termination capability

- Allows administrator to take control of a channel a user is controlling by terminating his session at any time.
- Users can lock a channel in Java Viewer and prevent other users from viewing/controlling that channel (except in above case).
- Users can see who is currently viewing the channel they are now controlling.
- Administrators can set timeouts for JView and VNC to terminate inactive sessions.
- A **Kill Session Link** is available on the **User Activity** web page.

KCA Benefits

The purpose of Kaveman Centralized Access (KCA) Snap-in is to give administrators a central location to create Kaveman objects for each unit on the network and to configure user access to Kaveman channels. By combining user groups and channel groups, you can make quick and accurate changes to channel privileges.

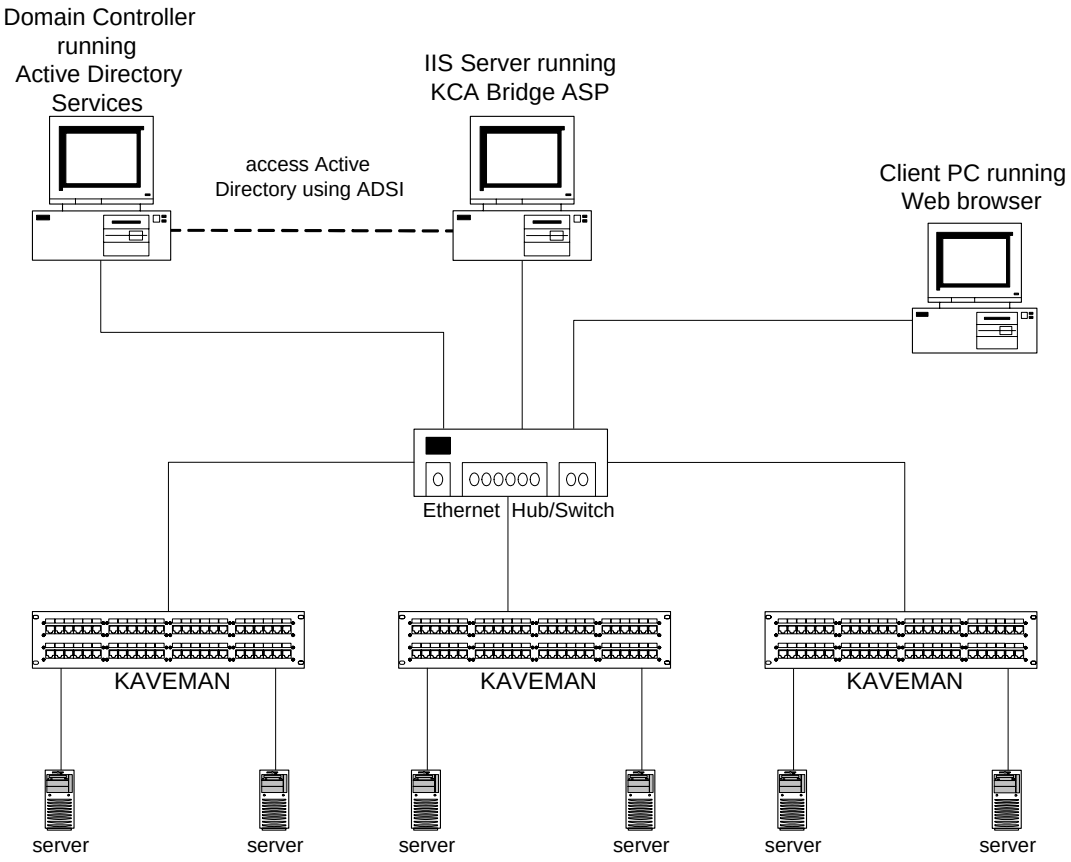
Table 1.1 - KCA Benefits

Kaveman without Active Directory	Kaveman Centralized Access
System administrator must log in to each Kaveman switch to set access to each channel.	System administrator has a central point of access (Active Directory) to configure access by all users.
System administrator must assign a user the same user privileges on all enabled channels of a Kaveman.	System administrator can assign a user or group different privileges on each channel of a Kaveman.
Users must know which Kaveman unit to log into before controlling a channel to assign privileges.	KCA gives users a convenient comprehensive list of all their enabled channels in a virtual “giant Kaveman”.

KCA System Overview

The following diagram depicts the major components required for the KCA system. This diagram displays Kaveman 16 units, however, the layout works equally well with Kaveman 1 and Kaveman 8 units.

Figure 1.1 - KCA system overview



KCA System Components

The following is a description of the KCA system components and their functions.

Hardware components

Client PC – A Windows based computer running a java-enabled web browser. The user logs into the KCA web site, is authenticated, and is presented with a list of all accessible channels. When the user selects a channel, he is transferred to the appropriate Kaveman switch that the selected channel is attached to, and given appropriate control of that channel using the JView applet.

KCA Bridge (running on IIS Web Server) – An IIS web server providing a common entry point for the complete system with a single Universal Resource Locator (URL). When a user logs on to the system, the authentication process begins. The IIS bridge retrieves a list of accessible channels from Active Directory services (based on user group permissions) and presents them to the user. Each accessible channel is presented as a unique URL.

Active Directory Server – A Windows 2000/2003 domain controller running Active Directory Services. This server stores all the Kaveman switches, channel objects, and user data information that the Administrator has created and put in the Active Directory.

Kaveman – Digital V6 Kaveman Switch with attached servers.

Software components

Software installations on the IIS Server and the Domain Controller must be performed in order for the KCA system to function.

Please refer to Software Installation and Configuration on page 5 for more information.

The current version of KCA only supports single domain environments. The DC, IIS, Kaveman, Clients must belong to the same domain.

To access Kaveman Administrator Functions on the KCA web site, you must log in as “administrator”.

2

SOFTWARE INSTALLATION AND CONFIGURATION

Hardware Requirements

The following two Windows-based systems are required for KCA:

- Windows 2000 or Windows 2003 Domain Controller with Active Directory Services and DNS
- Windows 2000 or Windows 2003 server with IIS services (referred to as the IIS Server)

Both machines must be on the same domain or the IIS Server will be unable to search the Directory Tree when a user logs on.

There is a separate software installation for each machine.

Software Installation on the Domain Controller

To install the KCA software on the Domain Controller

1. On the Domain Controller, run **setup.exe** from the DC directory of the Kaveman Centralized Access installation CD-ROM.
2. Follow the on screen instructions, entering the Product Key where required.
   All software components, including DLLs, will be copied and registered. The default target directory is C:\Program Files\DigitalV6\Kaveman.

Set the option for **Every One** to use this application.

To make the Kaveman.ldf file

1. After successfully installing Kaveman Centralized Access to the Domain Controller, click **Start** > **Programs** > **Digitalv6** > **KCA** > **ldifmake.exe**.
   This creates the **Kaveman.ldf** file containing all schema changes (new classes and properties) that are required to support Kaveman Centralized Access.

Running this program does not modify the schema; it only creates the LDF file.

To modify the schema

1. On the Domain Controller, open a DOS window.
2. Navigate to **C:\Program Files\DigitalV6\Kaveman** and verify that the **Kaveman.ldf** file exists.
   If not, go to To make the Kaveman.ldf file on page 5.
3. Enter the following DOS command `ldifde -i -f Kaveman.ldf -v`.
   This will modify the schema by adding all Digital V6 classes and properties.

Running this command modifies the existing schema in your Active Directory. Performing a system backup is highly recommended prior to changing the schema.

To change the schema master

If an error occurs during the schema modification process, you may need to change the schema master to allow modifications to be made on the controller. To change the schema master:

1. Open the schema mmc.
2. Right click **Active Directory Schema**.
3. Select **Operations Master**.
4. Enable the box "**The schema may be modified on this controller**".
5. Go to To make the Kaveman.ldf file on page 5.
   The schema should correctly import all new classes and properties with no errors.

To install the Active Directory schema Snap-in

If the schema Snap-in application is not installed on your Domain Controller, you can install it by doing the following:

1. Open a DOS window.
2. Type `regsvr32 schmmgmt.dll` and press **Enter**.
3. Type `mmc /a` and press **Enter**.
4. Add the Active Directory Schema Snap-in.

To run the KCA Snap-in

1. Click **Start** > **Programs** > **Administrative Tools** > **KCA Snap-in**.

The Snap-in MMC starts and displays the first Kaveman Container object under the root DC object. The administrator can now begin adding new Kaveman objects to the container. Every Kaveman object will have the appropriate number of channels automatically created.

For more information on adding and managing Kaveman related objects, please see Using the KCA Snap-In on page 17.

To configure DNS entries for each Kaveman

Open the DNS service MMC on the Domain Controller and for each new Kaveman unit to be created, enter a DNS entry for that Kaveman and associate the appropriate IP address with it. Configure that IP address on the Kaveman unit.

Software Installation on the IIS Server

To install the KCA software on the IIS server

1. On the IIS Server, run **setup.exe** from the IIS directory on the Kaveman Centralized Access installation CD-ROM.
2. Follow the on screen instructions, entering the Product Key where required.
   All software components, including DLLs, will be copied and registered. The default target directory is C:\Program Files\DigitalV6\KavemanIIS.

Set the option for **Every One** to use this application.

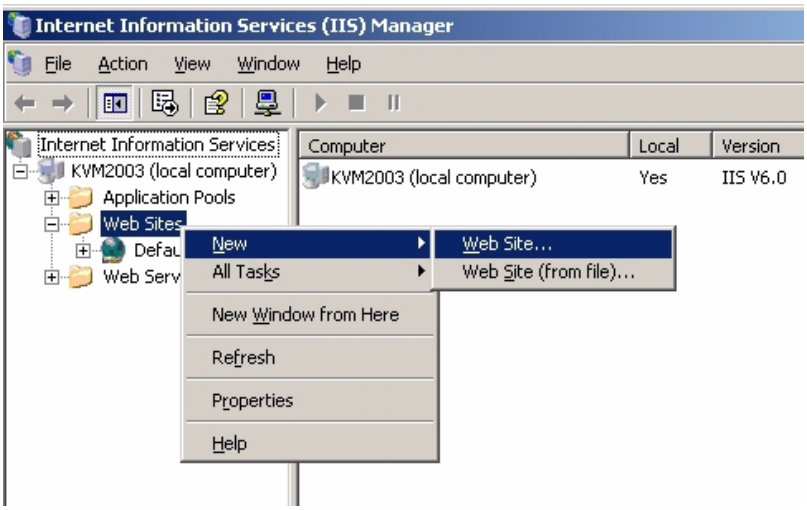
Creating a New Web Site

After the software has been installed on both the Domain Controller and the IIS Server, the next stage is to create and configure the KCA web site.

To create a new web site

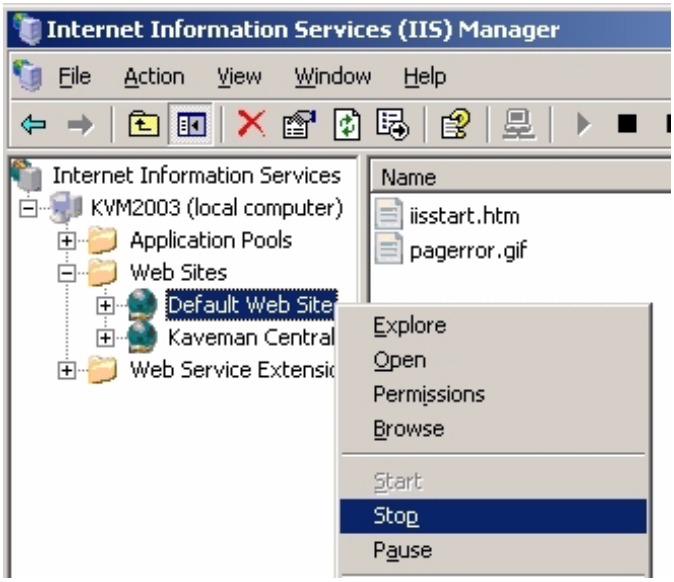
1. Open the Internet Information Services (IIS) Manager.
2. Right click **Web Site** and select **New** > **Web Site**.
   For Windows 2000 Server, right click the machine name and select **New** > **Web Site**.

Figure 2.1 - Creating a new web site



3. Follow the instructions in the **Web Site Creation Wizard**, ensuring you include the following:
   - web site description - **Kaveman Centralized Access**
   - IP address for the web site - **IP address of the IIS**
   - path to the home directory
   - disable the allow anonymous access to the web site box
   - ensure **Read** and **Run Scripts** are enabled
4. Click **Finish** when done.
5. On the IIS Manager, right click **Default Web Site** and select **Stop**.

Figure 2.2 - Stopping the default web site

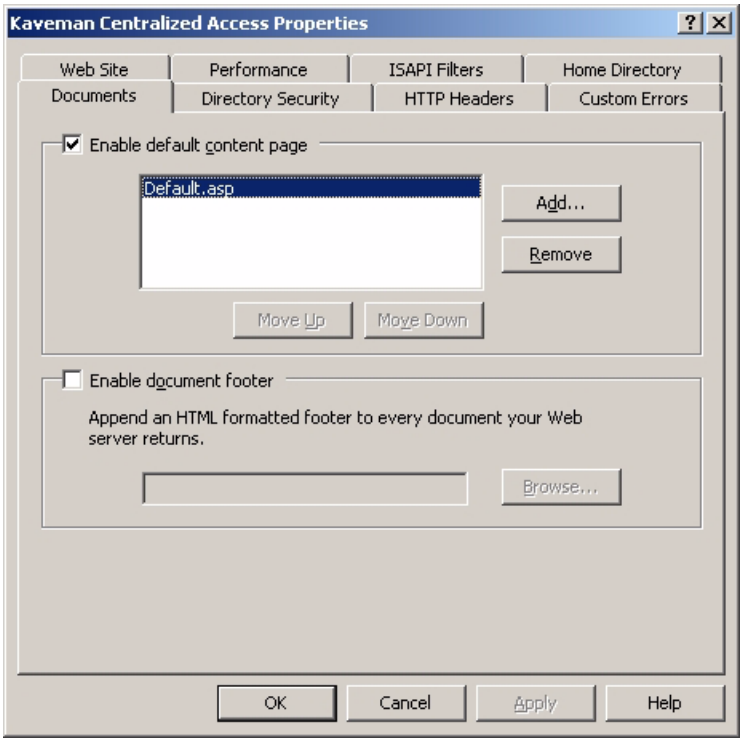


To configure the new web site

After creating the new web site, you must configure it to run Kaveman Centralized Access.

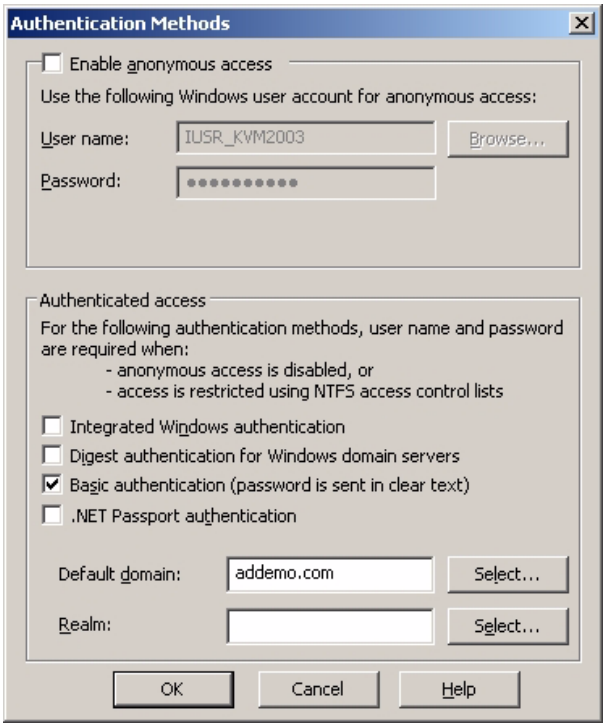
1. Right click the **Kaveman Centralized Access** web site and select **Properties**.
2. On the **Documents** tab, ensure **Enable default content page** (**Enable Default Document** on Windows 2000) is checked and that **Default.asp** is the only file selected.

Figure 2.3 - Configuring the KCA web site



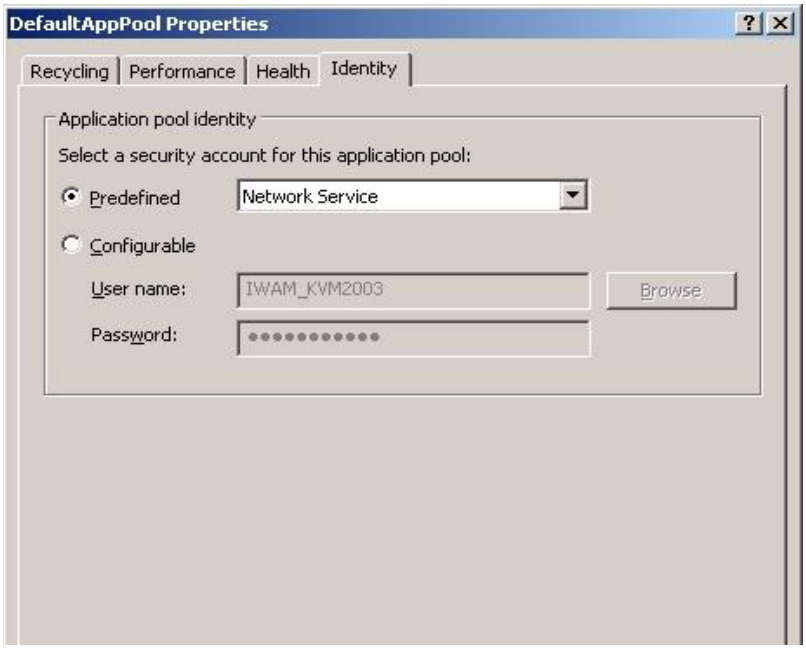
3. On the **Directory Security** tab, click the **Authentication and access control Edit** button.
4. Disable the **Anonymous access** check box, if it is checked.
5. In the **Authenticated access** panel, check only **Basic Authentication** and enter the **Default domain** (e.g. addemo.com)
   In Windows 2000, click the **Edit** button to enter the **Default domain**.

Figure 2.4 - Authenticating the KCA web site



6. For Windows 2000 only - on the **Home Directory** tab, set **Application Protection** to *Low (IIS Process)*.
7. Click OK to save your changes and return to the IIS Manager.
8. For Windows 2003 only - right click **DefaultAppPool** in the **Application Pools** folder and select **Properties**.
9. On the **Identity** tab, choose **Predefined** and select **Network Service** from the list.

Figure 2.5 - Application Pool Identities (Windows 2003)



10. Start the Kaveman Centralized Access web site if it is not already running.

To set the Active Server Page for Windows 2003 servers

1. Select **Web Service Extensions** and change the Active Server Page from **Prohibited** to **Allowed**.

KCA Bridge Configuration

Before a user can successfully log into the IIS Server, the KCA system must be configured. The configuration file, config.asp, will be created and saved in the same directory as the default.asp.

The following information will be required:

- Passphrase
- Account name
- Account password

Passphrase

The passphrase is used to encrypt and decrypt the **Kaveman Access Manager Account** password. The account (name and password) is stored in the Active Directory for each Kaveman object. When a Kaveman object is created (see Using the KCA Snap-In on page 17), the administrator is prompted for this passphrase. The same passphrase must be used in the configuration screen and in the Snap-in screens. Using this passphrase, the Snap-in will encrypt the **Kaveman Access Manager Account** password and write it into the Kaveman object. This account allows the IIS Server to log into the Kaveman and create a special session for use only by the logged in user each time. The user is given authorized access rights to the selected channel.

Account name

The Account Name is used exclusively by the IIS Bridge when searching the Active Directory for a user's channel permissions when a user logs into the IIS Server. For security, set the Kaveman Container security tab to allow read access only to this account. Enter the Active Directory Network Access Account name using both a domain and user name (e.g. "addemo\administrator")

Account password

This is the password for the network account used to read Active Directory.

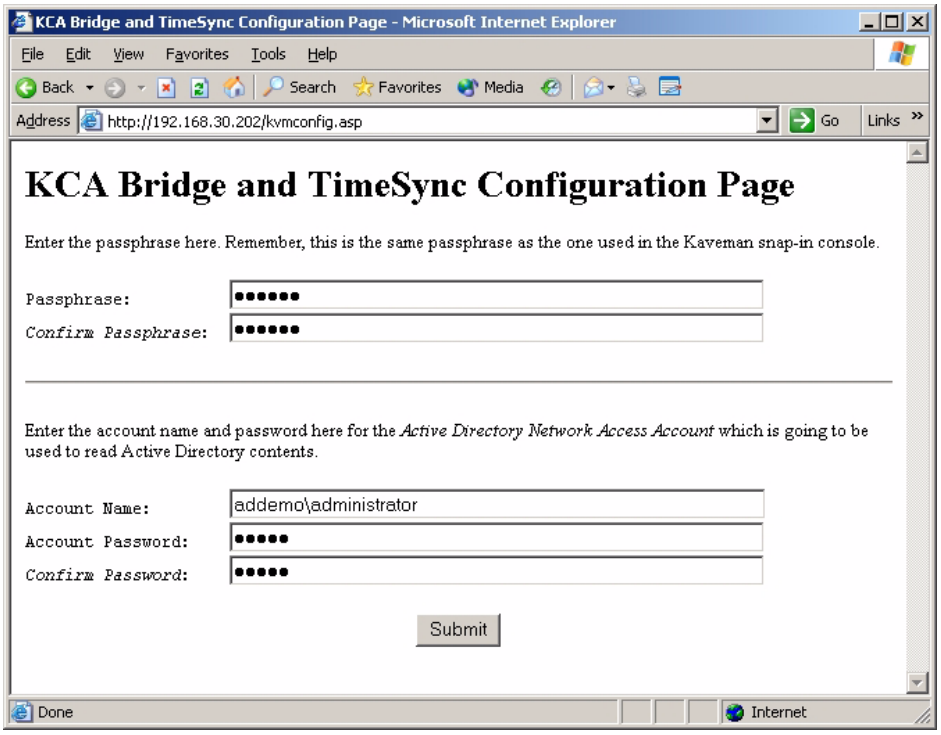
KCA Date and Time Synchronization

During the Bridge configuration process, you will also be able to configure the date and time synchronization feature available on all Kaveman units.The KCA system includes a script called **timesync.vbs** found on the IIS Server at **C:\Program Files\Digitalv6\KavemanIIS**. This script synchronizes the date and time of all Kaveman units found in the Active Directory tree of the root domain.This script can be run manually or automatically using the Windows **Scheduled Tasks** system tool. The date and time is synchronized with the date and time of the IIS Server executing the script.

To open the kvmconfig web page

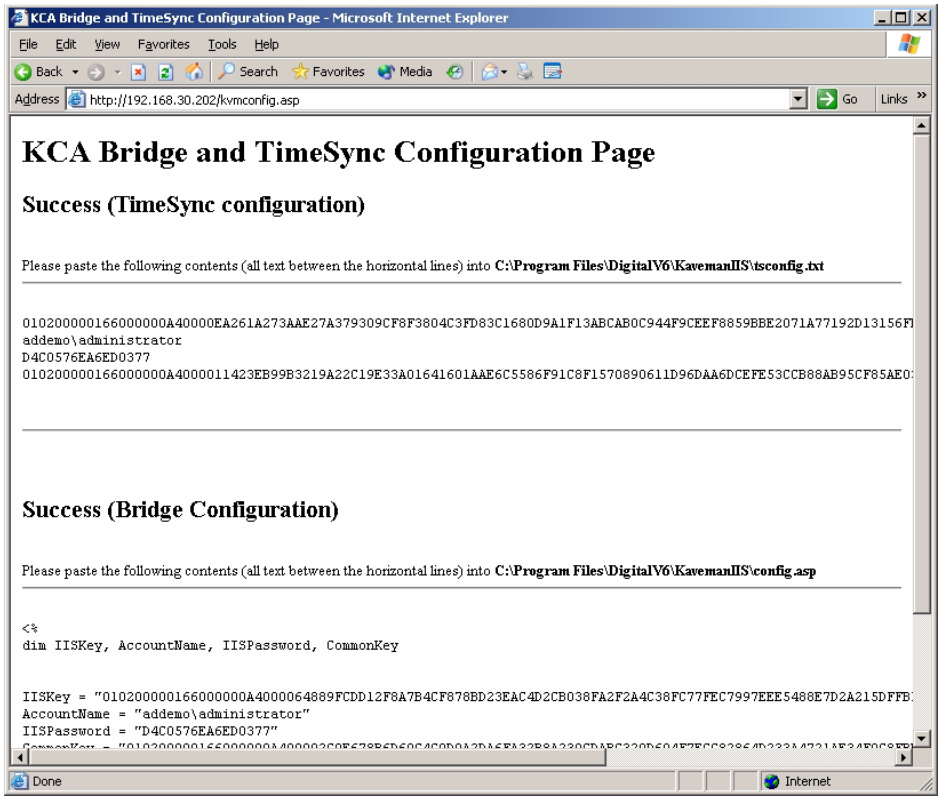
1. Log into the IIS Server and open a web browser.
2. Enter **http://localhost/kvmconfig.asp** in the address bar.
3. When prompted, log in to the **kvmconfig** web page as administrator (or another account configured in Active Directory) The following form appears:

Figure 2.6 - Configuring the KCA Bridge



4. Enter the required information.
5. Click **Submit**.
   The following page is generated.

Figure 2.7 - Code generated by KCA Bridge configuration



To save the tsconfig.txt file

1. Open **C:\Program Files\DigitalV6\KavemanIIS\tsconfig.txt** in Notepad.
2. Copy the tsconfig.txt text block to the file and save.

To save the config.asp file

1. Open **C:\Program Files\DigitalV6\KavemanIIS\config.asp** in Notepad.
2. Copy the config.asp text block to the file and save.

If either tsconfig.txt or config.asp are not generated automatically, create them using Notepad.

To execute the timesync.vbs script

1. From a DOS prompt, go to **C:\Program Files\DigitalV6\KavemanIIS**.
2. Enter the following command `cscript timesync.vbs`.
   Each time the script is run, the results will be appended to the tslog.txt file.

To configure a Kaveman Access Manager Account

1. Invoke the OSD menu and scroll to the **Security settings**.

2. Enter the KCA Access Manager Account and password information.
3. Ensure this account is used every time a new Kaveman object is created (see To identify the Access Manager on page 20).

To enable Cookies on the IIS Bridge (Windows 2003 Server)

1. Log into the bridge machine using the **Active Directory Network Access Account**.
2. Open Internet Explorer.
3. Click **Tools** > **Internet Options**.
4. On the **Security** tab, select **Trusted sites** and click the **Sites** button.
5. Add the Kaveman name to the list of trusted sites.

Using SSL to Encrypt the Link Between the IIS Server and Kaveman

The Kaveman Centralized Access system requires a Secure Sockets Layer (SSL) connection between the IIS Server and the Kaveman unit. This requires an SSL certificate and a private key to be created and copied to each Kaveman that the IIS Server will be accessing. Windows Certificate Services must be installed on the Domain Controller if you are using Windows 2000. The following steps create a certificate and private key.

Preparing the Domain Controller

1. From the **Control Panel**, double click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Install **Internet Information Services (IIS)**.
4. After IIS is loaded, install **Certificate Services**.

Select **Enterprise root CA** as the **Certification Authority type** and add the company and server information when prompted.

To download the OpenSSL for Windows toolkit into the Domain Controller

1. Go to http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7/openssl.zip.
2. Open the file or save it to your local system.
3. Extract the contents of the zipped file to **C:\openssl**.

To create a certificate config file

1. Go to **C:\Program Files\Digitalv6\Kaveman\openssl**.
2. Copy the contents of this folder to **C:\openssl**.
3. Customize the contents to suit your needs.

The following is the contents of the sample file (openssl.cnf). The bold fields can be customized.

```
[req]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name


[req_distinguished_name]
```

```
countryName = CA
countryName_default = CA
countryName_min = 2
countryName_max = 2

stateOrProvinceName = Ontario
stateOrProvinceName_default = Ontario

localityName = Markham
localityName_default = Markham

organizationName = DV6
organizationName_default = DV6
organizationName_max = 64

organizationalUnitName = IT Department
organizationalUnitName_default = IT Department
organizationalUnitName_max = 64

commonName = Kaveman16
commonName_default = Kaveman16
commonName_max = 64

emailAddress = support@digitalv6.com
emailAddress_default = support@digitalv6.com
emailAddress_max = 40
```

The commonName should include the full DNS Host Name (e.g. K16demo1.addemo.com)

To create a Certificate Signing Request

1. 1. From a DOS prompt, go to **C:\OPENSSL**.
2. 2. Enter the following command `create.bat`.
   This batch file performs the following actions

```
openssl req –config openssl.cnf –newkey rsa:1024 –nodes –keyout
Kavemankey.pem –keyform PEM –out Kavemanreq.pem –outform PEM
```

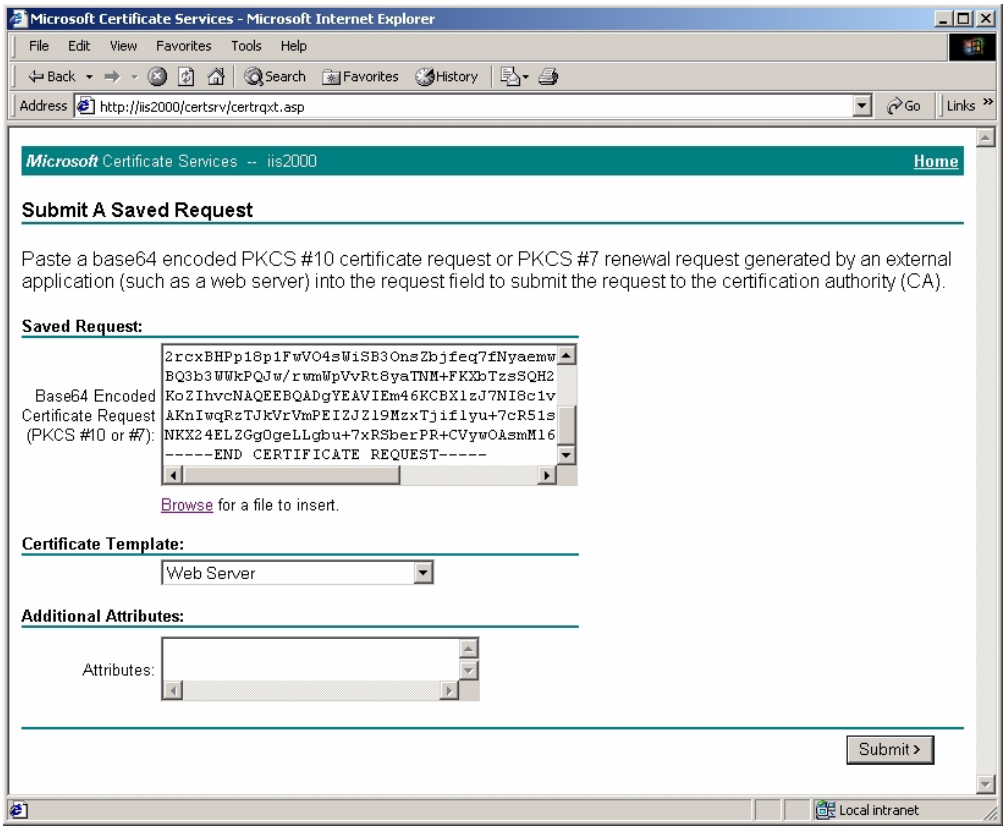
During this process, you will be prompted with a list of options. Press **Enter** to use the default settings you assigned in the openssl.cnf file.

The files **Kavemankey.pem** and **Kavemanreq.pem** have been created and stored in **C:\openssl**.

To submit a Certificate Request

1. On the Domain Controller, copy the contents of Kavemanreq.pem to the clipboard.
2. Open a web browser and enter http://"Name of the Domain Controller machine"/certsrv (i.e.: http://iis2000/certsrv) to access the **certsrv** web site.
3. When prompted, do the following:
   - Login using administrator rights.
   - Select **Request a Certificate**.
   - Select **Advanced request**.
   - Select **Submit a certificate using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.
   - Paste the clipboard contents into the request field of the page.
   - Select **Web Server** from the **Certificate Template** drop down.
4. Click **Submit**.

Figure 2.8 - Submitting a Certificate Request



5. Select **Base 64 encoded** and click **Download CA certificate**.
6. Save the certificate to **C:\Opensss\Kaveman.crt**.

Select **All Files (*.*)** as the **Save as type** to preserve the .crt extension.

To upload the files to Kaveman

1. Rename Kavemankey.pem to Kavemankey.key.
2. On the Kaveman, use the Web interface (**Flash File System**) to delete previous certificates and keys from Kaveman file system.
3. Copy the new Kaveman.crt and Kaveman.key to file system of Kaveman unit.
4. Reboot the Kaveman.

To create the Root certificate

1. On the Domain Controller, open a web browser and enter http://iis2000/certsrv to access the **certsrv** web site.
1. Select **Retrieve the CA certificate or certificate revocation list**, and click **Next**.
2. Select a certificate from the **CA Certificate list**.
3. Click **Download CA certificate**.
4. Save the certificate.

To get the IIS Server to trust Kaveman

1. Copy the Root certificate to the IIS Server.
2. Open **Internet Explorer**.
3. Click **Tools** > **Internet Options**.
4. On the **Content** tab, click the **Certificates** button.
5. On the **Trusted Root Certification Authorities** tab, click the **Import** button.
6. Follow the instructions in the **Certificate Import Wizard**.

3

USING THE KCA SNAP-IN

How it Works

The KCA Snap-in uses existing user accounts to assign privileges. When a user group is added to the Active Directory using the Users and Computers Snap-in, the group becomes available to the KCA Snap-in for the Select Groups dialog. By combining user groups and channel groups, administrators are able to make quick and accurate changes to channel privileges.

The KCA Snap-in further empowers administrators by using DNS. Administrators simply specify the DNS host name of the Kaveman in the Kaveman object itself.

Definitions

Table 3.1 - KCA Snap-in definitions

Administrator	One or more people who use the KCA Snap-in to centrally set up and maintain Kaveman KVM Switch Units, including assignment of their IP addresses, naming of access managers, and assignment of Kaveman channels (servers).
KCA Access Manager Account	The new Kaveman account type, Access Manager, is added to Disabled and Normal. It is required by IIS to log into Kaveman and create a session on behalf of a user.
User or End User	Programmers and others who must have access to or control of a channel in order to maintain or install software, data, etc. on a target server.
KCA Snap-in	A proprietary Microsoft Management Console (MMC) that allows easy management and creation of Kaveman-related objects in the Active Directory tree. This chapter describes how to use this Snap-in interface.

Three Easy Steps to Setting up Kaveman Channels

Administrators must complete three steps to set up Kaveman KVM switches and channel groups:

- Create Kaveman objects
- Create channel groups
- Assign user privileges to channel groups

These three steps are described below, including a simple setup example. The steps and example assume you are using KCA with one or more Kaveman 16 units.

Creating Kaveman Objects

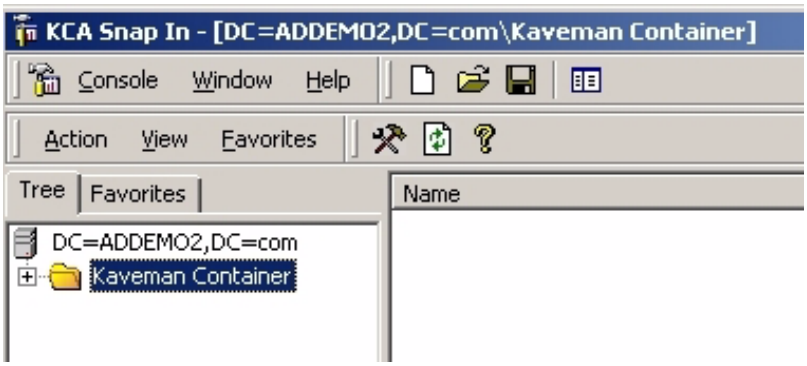
You (the administrator) have a list of Kaveman IP addresses that were locally assigned to each Kaveman (making them all accessible remotely) in a single domain that we will call “addemo2.com”. You should also have or create a predefined set of users and groups. One of the

user IDs on each Kaveman has to have privileges of an Access Manager. You could use a root account for all Kaveman units, but an alternative is to log in to each Kaveman and assign an “access manager” for KCA.

To create a Kaveman object

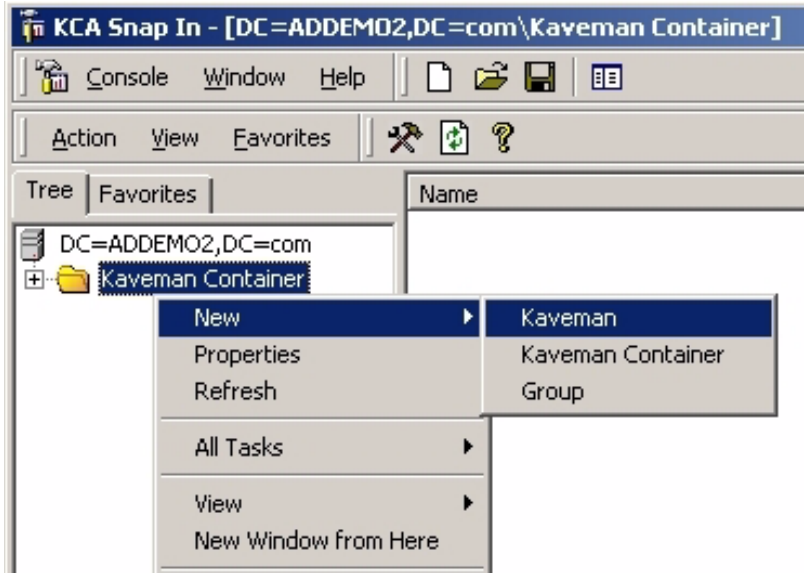
1. Click **Start\Programs\Administrative Tools\KCA Snap-in** to access the **KCA Snap-in** screen.
   The screen displays our initial domain, DC=addemo2, DC=com and a **Kaveman Container** – the beginnings of a tree.

Figure 3.1 - Kaveman Snap-in screen



2. Right click the **Kaveman Container** and click **New** > **Kaveman**. This container holds all Kaveman-related objects and can also contain other Kaveman *containers*.

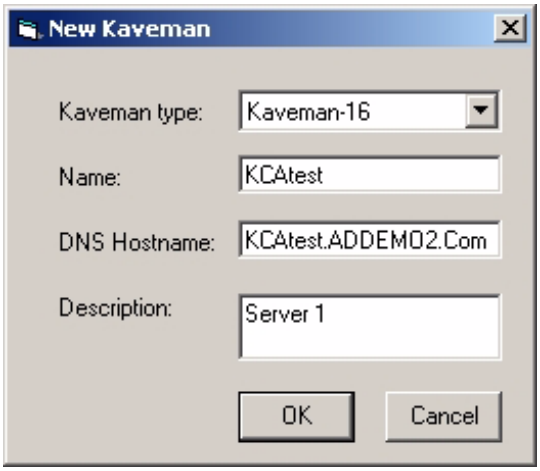
Figure 3.2 - Creating a new Kaveman object



3. On the **New Kaveman** dialog box, enter the following information:
   - **Kaveman type** – select the Kaveman type from the drop down list.

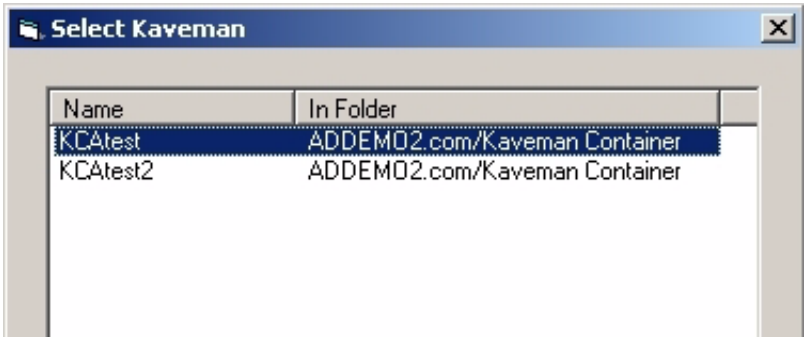
- **Kaveman Name** – a meaningful name within your network environment. Avoiding embedded blanks, underscores, and dashes may reduce typing errors later on. Case is ignored.
- **DNSHostName** – this field is automatically populated with the Kaveman name and the domain to which the Active Directory and KCA are applied (e.g. *KCAtest.addemo.com*, where *KCAtest* is the Kaveman Name and *addemo2.com* is the domain).
- **Description** – a description of the Kaveman object you are creating.

Figure 3.3 - New Kaveman dialog box



4. Click **OK**.
5. The next dialog box asks if you want to copy an existing Kaveman account (object) and password. If there are no existing accounts, you will not see this dialog box.
6. If you click **Yes**, select the Kaveman object you want to copy from the list on the **Select Kaveman** dialog box and click **OK** to finish the object creation.

Figure 3.4 - Selecting Kaveman properties



7. If you click **No**, or if this is the first Kaveman object being created, enter the following information when prompted:
   - Passphrase
   - Kaveman account name
   - Password for this Kaveman

8. Once the Kaveman object has been created, you can rename the 16 channels by right clicking them and choosing **Rename**.

To identify the Access Manager

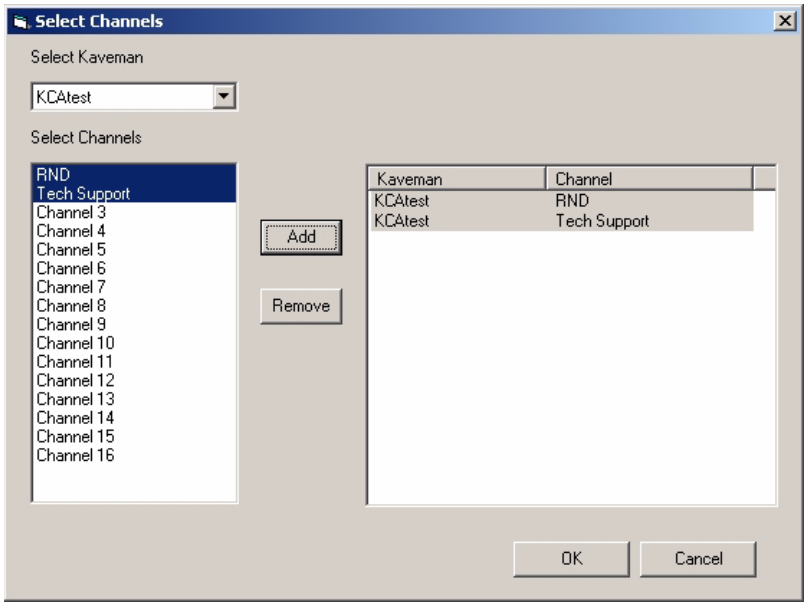
1. Right click the new object and click **Properties**.
2. On the **Advanced** tab, ensure the Access manager account is listed as the **Access ID**. You can change the password and passphrase from the **Advanced** tab.

For more information about setting up the Access Manager account, see To configure a Kaveman Access Manager Account on page 12.

Grouping Channels

1. Right click the container, and click **New** > **Group**.
2. Enter the **Group Name** and **Description** when prompted.
3. In the directory tree, right click the new group icon and click **Properties**.
4. On the **Members** tab, click the **Add** button.
5. On the **Select Channels** dialog box, choose the Kaveman you want from the **Select Kaveman** drop down list.
6. Using **Shift** or **CTRL** click, select the channels you want to assign to this group.
7. Click **Add**.
8. Click **OK** > **OK** to close the screens and save your changes.

Figure 3.5 - Grouping channels



Editing Permissions

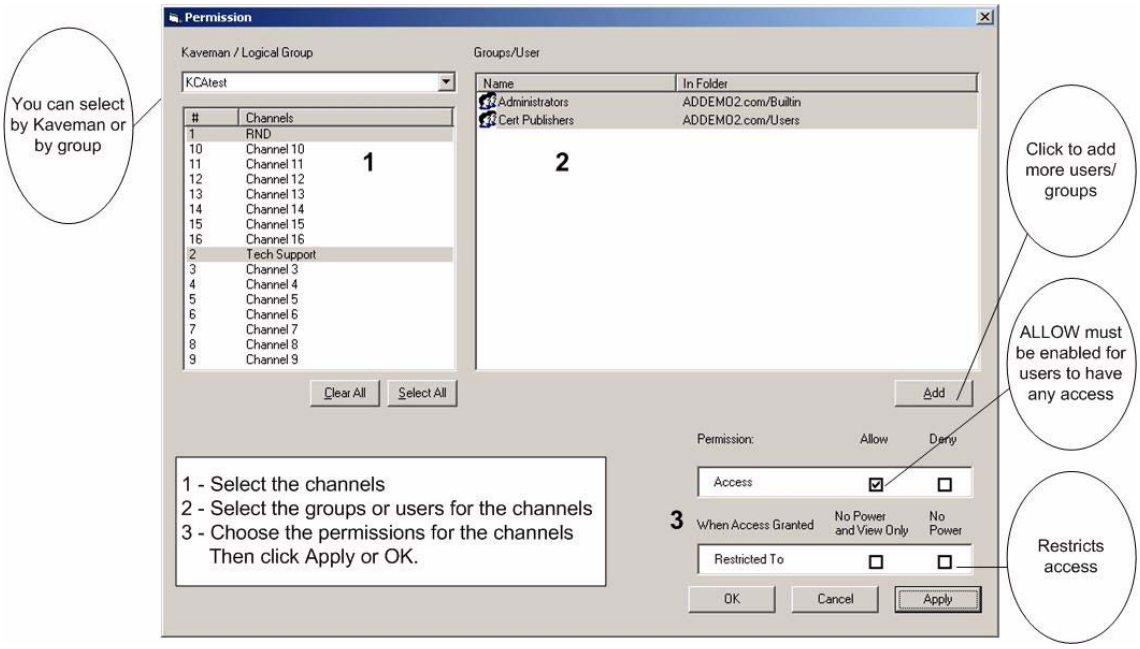
When you create new groups, you will need to edit their permissions and restrictions to certain channels. The **Permission** dialog box lets you associate channel groups with user groups.

The Active Directory standard Snap-in, Users and Computers, lists all the domain's user groups and properties.

To edit permissions

1. Click the **Edit Permissions** icon to get the **Permission** dialog box, which is shown below with sequence numbers 1, 2, 3 indicating the order of selection.

Figure 3.6 - Editing Kaveman permissions



Step 1 – **Select channels**

1. Select the Kaveman or Logical Group from the drop down list.
2. Select the channels you want to grant access to.
   Click **Select All** to select all the channels for that Kaveman or use **Shift** or **CTRL** click to select specific channels.

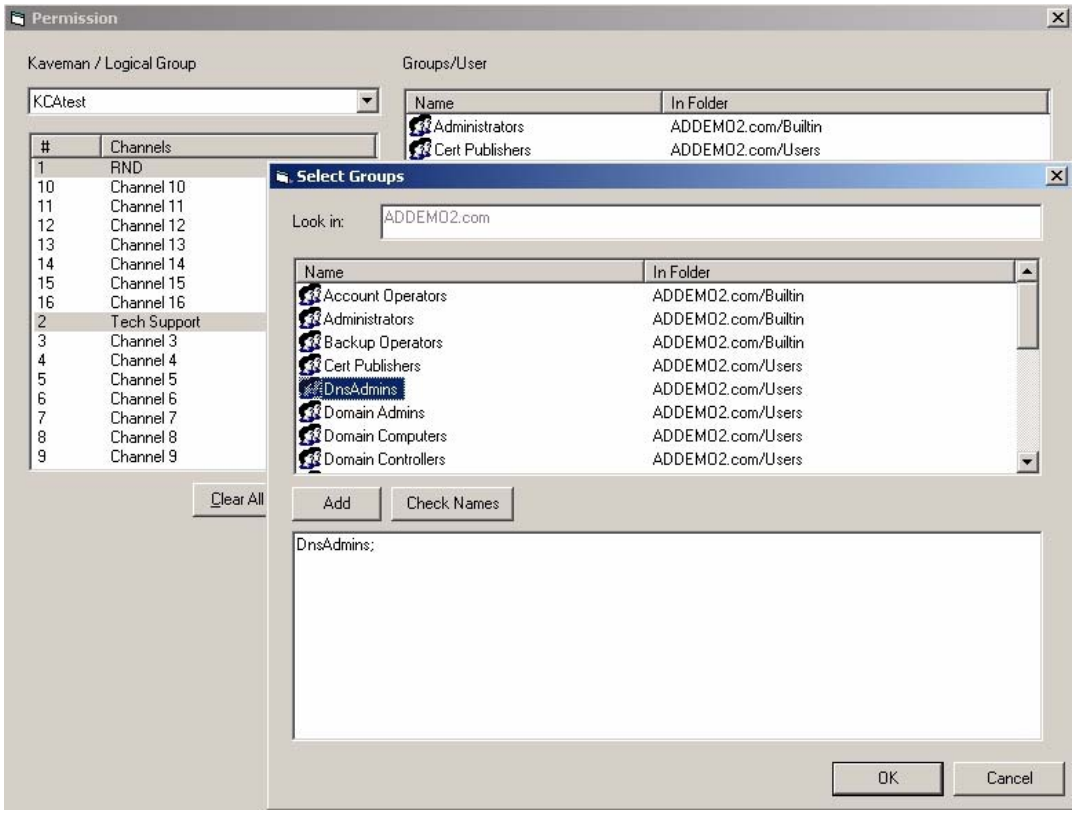
A channel group can span multiple Kaveman units.

Step 2 – **Select user groups**

1. Select the **Groups/User** names (in Pane 2) that you want to apply to the selected channels.
   - To add more user groups to a channel group, select the channel group and click the **Add** button. On the **Select Groups** dialog box, double click the groups you want to add and click **OK**.

If the user or group does not appear in the list, type the name in the lower panel.

Figure 3.7 - Selecting user groups to assign to channels



Step 3 – **Select permissions**

1. In the **Permission** field, check the **Allow** box.
   If you do not check the **Allow** box, the group has no access to the channels.
2. Check either **No Power and View Only** or **No Power** to restrict the access rights of the group, if necessary.
3. Click **Apply** to save the changes and continue editing permissions or click **OK** to save and exit the **Permissions** dialog box.

Summary

Table 3.2 - Summary of Editing Actions

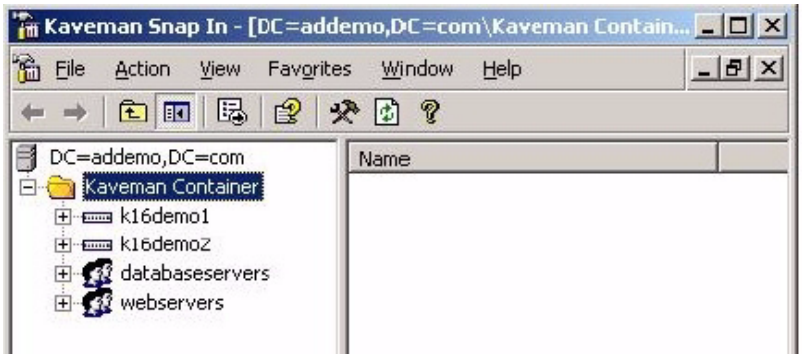
Action	Result
Highlight a user group	Left Pane (1) turns from dark to grey, permissions check boxes get updated.
Select two or more user groups	The user group with lesser privileges imposes them on the other group.
Override permissions	Could allow Control privileges to a View only group.
Clear permissions boxes	The specified user group will be removed from the specified channels.

A Simple Example

The objective of this example is to create two Kaveman units that each have one web server channel and one database channel. You want to assign a user, Wendy, full access to the web server channels, and only view access to the database channels.

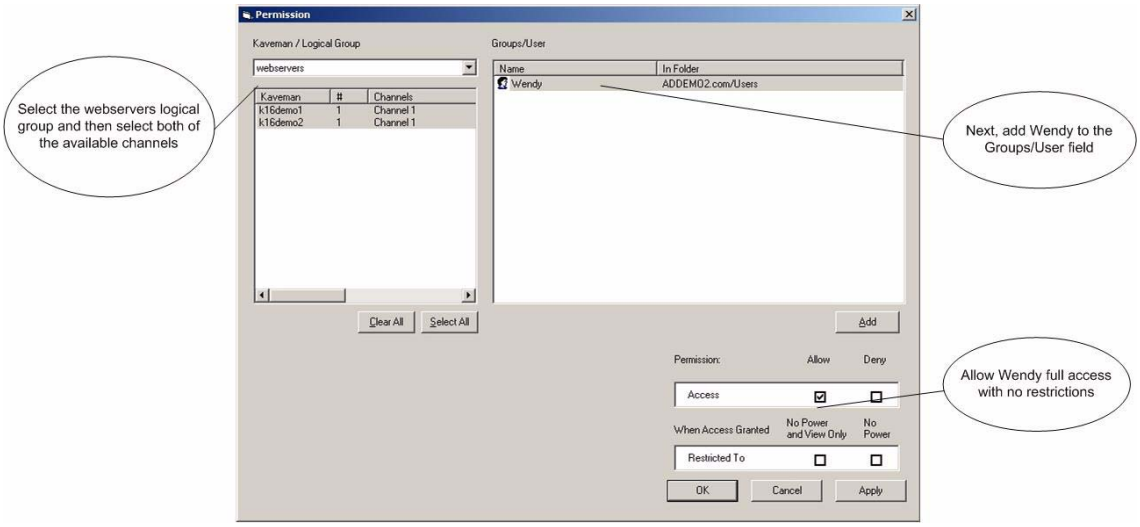
1. Create two Kaveman units (K16demo1 and K16demo2) and two channel groups (database servers and web servers), as shown in the screen below.

Figure 3.8 - Creating Kaveman objects example



2. Grant full access to Wendy on the web servers channel groups on both Kaveman units.

Figure 3.9 - Editing permissions example – Kaveman units



3. Grant view access to Wendy on the database servers channel groups on both Kaveman units.

Wendy can now log in and view all the channels to which she has access. In this example, she has only four channels on two Kaveman units, but in practice she could have any number of channels, grouped and condensed into channel (logical) groups, accessed by scroll bar.

Figure 3.10 - Editing permissions example – database servers

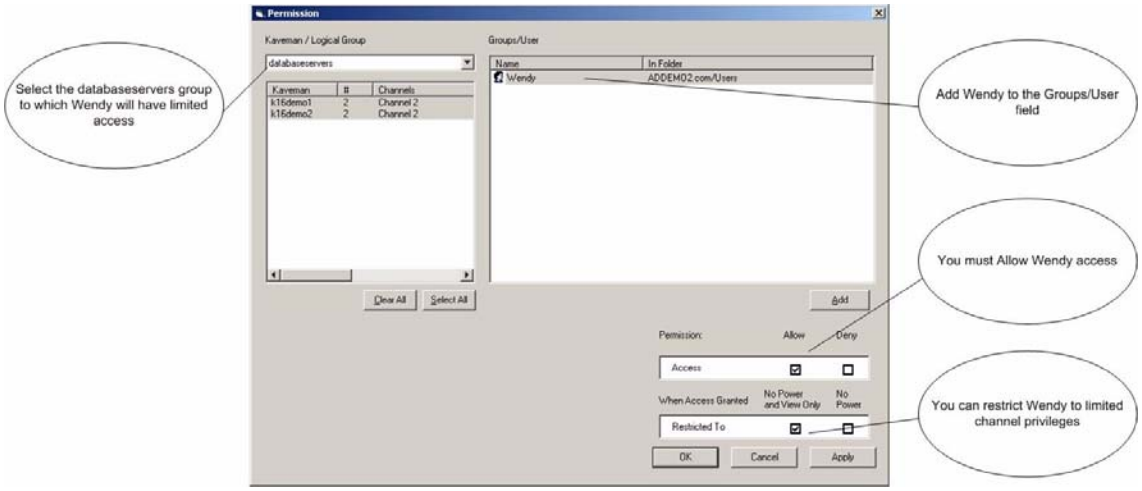
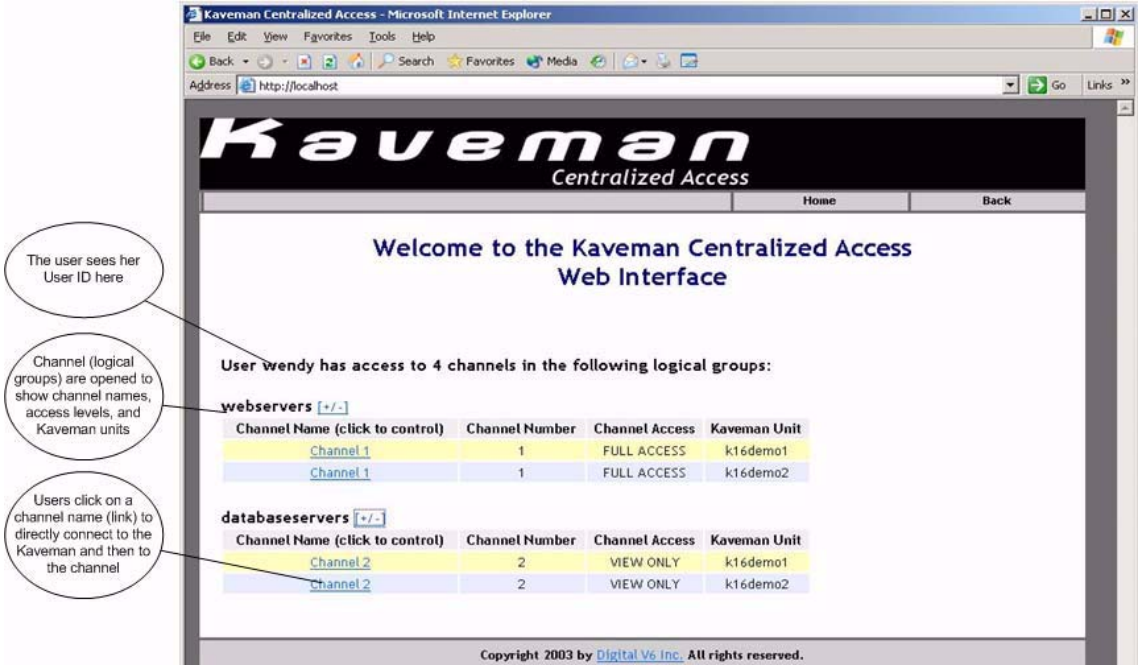


Figure 3.11 - KCA Web Interface Welcome screen



Channel Privilege Report

Automatic seeking and reporting of channel mappings is a major benefit of KCA and Active Directory. Users are able to find all their channel privileges in one place, updated regularly with maximum accuracy, and with no added administrative workload! Hundreds of Kaveman units are compressed into one huge virtual Kaveman with seamless access.

While the virtual Kaveman appears to attach the user through the IIS Web server, the load on this server is actually much reduced by attaching users directly from the target Kaveman with no detour through IIS.

Appendix A

CONTACT INFORMATION

Kaveman products are manufactured and supported by Digital V6 Corp.

Corporate Headquarters

Digital V6 Corp.
3993 14th Avenue
Markham, Ontario
L3R 4Z6
Canada

http://www.digitalv6.com

Phone: 1-905-513-3109

Toll free: 1-866-922-2333

Fax: 1-905-513-3111

General Inquiries: info@digitalv6.com

Support: support@digitalv6.com

Sales Inquiries: sales@digitalv6.com

Index

INDEX

A

Access Manager 20

B

benefits 2

C

certificate request
  creating 14
  submitting 15
certificates 13
  uploading 16
Channel privilege report 24
components
  hardware 3
  software 4
configuring
  DNS entries 6
contacting Digital V6 Corp. 25
creating
  certificate configuration file 13

E

encryption 13

F

features 1

K

Kaveman Access Manager account 12
KCA
  components 3
  system overview 3
  web interface 24
KCA Bridge
  account name 11
  account password 11
  config.asp 12
  configuration 10
  configuring 11
  cookies 13
  kvmconfig.asp 11
  passphrase 10
  timesync.vbs 12
  tsconfig.txt 12
KCA Snap-in 17

O

overview 1

S

schemas
  Active Directory 6
  changing schema master 6
  creating LDF file 5
  modifying 5
security 13
Snap-in
  creating objects 17
  definitions 17
  editing permissions 20
  example 23
  grouping channels 20
  overview 17
software installation
  configuration 5
  domain controller 5
  IIS server 6
synchronizing dates and times 11

W

web site
  configuring 8
  creating new 7
  setting Active Server Page 10